www.takbook.com

کتاب آموزشی
CCNA 200-301

مؤلف: فرشید بابجانی زاده – آزاده تیشه برسر

NAGHOOS
PUBLICATION

www.takbook.com

سرشناسه	:	بابجانی‌زاده، فرشید، ۱۳۶۵-
عنوان و نام پدیدآور	:	کتاب آموزشی CCNA -200-301/مولف فرشید بابجانی‌زاده.
مشخصات نشر	:	تهران : ناقوس ، ۱۳۹۹.
مشخصات ظاهری	:	۷۱۰ص.
شابک	:	۹۷۸-600-473319-9
وضعیت فهرست نویسی	:	فیپا
یادداشت	:	کتابنامه: ص.۷۱۳.
موضوع	:	سیستم عامل اینترنتی سیسکو Cisco IOS
موضوع	:	شبکه‌های کامپیوتری -- آزمون‌ها -- راهنمای مطالعه Computer networks -- Examinations -- Study guides داده‌پردازی -- کارمندان -- گواهی و گواهی‌نامه‌ها Electronic data processing personnel -- Certification
رده بندی کنگره	:	TK۵۱۰۵/۸
رده بندی دیویی	:	۶/۰۰۴
شماره کتابشناسی ملی	:	۷۲۸۰۸۹۲
اطلاعات رکورد کتابشناسی	:	فیپا

www.takbook.com

تقدیم به همسر مهربانم

به جویبارها سوگند در یاد من می‌مانی، به برگ‌های نارنجی پاییزی، به سبد آن میوه های نارس در دل پشت بام‌های دلتنگی، به طعم بی هوایی زردآلو در جاده های سکوت وغمناکی، به پرنده، به پرواز، به شیرینی لبخند رؤیایی، به آسمان، به حیرانه های تنهایی، به تبسم، به خیال، به زیبایی، به عشق، به برگ‌های نارنجی پاییزی در یاد من می‌مانی...

www.takbook.com

www.takbook.com

فهرست مطالب

مقدمه ۱۴

مدارک سیسکو ۱۵

دسته‌ی اول (دستیار یا کارشناس شبکه) ۱۵

دسته‌ی دوم (کارشناس ارشد شبکه) ۱۵

دسته‌ی سوم (متخصص شبکه یا دکترای شبکه) ۱۵

فصل اول ۲۳

مباحث بنیادی شبکه ۲۳

۱-۱ بررسی ساختار شبکه ۲۳

۱-۲ اصول کار با شبکه‌های اترنت ۳۴

۱-۳ بررسی شبکه‌های WAN و IP Routing ۶۰

۱-۴ سوالات فصل اول ۶۷

فصل دوم ۷۰

پیاده‌سازی شبکه‌های Ethernet ۷۰

۲-۱ بررسی دستگاه‌های شبکه ۷۰

۲-۲ بررسی سیستم‌عامل IOS شرکت سیسکو ۷۶

۲-۳ کار با نرم‌افزار Packet Tracer ۸۵

۲-۴ پیکربندی اولیه IOS ۹۰

۲-۵ نحوهی کار با Interface ۹۶

۲-۶ روش‌های دسترسی و رمزگذاری ۹۹

۲-۷ ذخیره اطلاعات دستگاه‌های سیسکو ۱۰۹

۲-۸ سوالات فصل دوم ۱۱۴

www.takbook.com

فصل سوم ۱۲۰
بررسی سوئیچینگ شبکه ۱۲۰
۳–۱ کار با سوئیچ لایهی دوم ۱۲۳
۳–۲ روش‌های انتقال فریم (LAN Switch Types) ۱۲۶
۳–۳ بررسی Loop در سوئیچ ۱۲۸
۳–۴ انواع مد در سوئیچ ۱۳۹
۳–۵ کار با VLAN در سوئیچ ۱۴۱
۳–۶ بررسی Voice VLAN در سوئیچ‌های سیسکو ۱۵۹
۳–۷ کار با EtherChannel در لایه‌ی دوم ۱۶۶
۳–۸ پروتکل‌های EtherChannel ۱۶۷
۳–۸–۱ LACP (Link Aggregation Control Protocol) ۱۶۷
۳–۸–۲ دستور CDP (Cisco discovery Protocol) ۱۷۲
۳–۹ سوالات فصل سوم ۱۷۴
فصل چهارم ۱۷۹
بررسی IPV4 ..... ۱۷۹
۴–۱ الگوهای غیراستاندارد ۱۸۴
۴–۲ اختصاص دادن رنج IP به شبکه سازمان ۱۸۷
۴–۳ بررسی CIDR ۱۹۰
۴–۵ سوالات فصل چهارم ۱۹۵
فصل پنجم ۲۰۴
مسیریابی (IP Routin) ۲۰۴
۵–۱ روش‌های متصل شدن به روتر ۲۰۵
۵–۲ بررسی Routing Table در روتر ۲۰۸

www.takbook.com

۵-۳ بررسی روش Static Route ۲۱۰
۵-۴ بررسی Dynamic Routing ۲۲۸
۵-۵ سوالات فصل پنجم ۲۴۳
فصل ششم ۲۴۹
پروتکل OSPF ۲۴۹
۶-۱ انتخاب بهترین مسیر در OSPF ۲۵۰
۶-۲ بررسی Link State Advertisements ۲۵۱
۶-۳ راه‌اندازی پروتکل OSPF ۲۵۴
۶-۴ روترهای DR و BDR ۲۵۵
۶-۵ کار با Virtual Link در OSPF ۲۶۴
۶-۶ بررسی Passive Interfaces در OSPF ۲۶۸
۶-۷ بررسی دستور Redistribute ۲۶۹
۶-۸ سوالات فصل ششم ۲۷۲
فصل هفتم ۲۷۴
نصب و راه اندازی GNS3 ..... ۲۷۴
۷-۱ اضافه کردن IOS مربوط به روتر در GNS3 ..... ۲۸۴
۷-۲ اضافه کردن لایسنس IOU به نرم‌افزار ۲۸۸
فصل هشتم ۲۹۴
بررسی پروتکل IPV6 ..... ۲۹۴
۸-۱ روش آدرس‌دهی در IPV6 ..... ۲۹۸
۸-۲ انواع آدرس‌های ipv6 ..... ۳۰۰
۸-۳ مسیریابی در IPV6 ..... ۳۰۳
۸-۴ فعال کردن IPV6 روی پروتکل OSPF V3 ..... ۳۰۳

www.takbook.com

۸-۵ سوالات فصل هشتم ۳۰۶

فصل نهم ۳۱۰

شبکه‌های بی‌سیم ۳۱۰

۹-۱ بررسی Basic Service Set (BSS) ۳۱۱

۹-۲ بررسی اجمالی RF ۳۱۷

۹-۳ بررسی معماری Access Point ۳۲۳

۹-۴ معماری AP مبتنی بر Cloud ۳۲۴

۹-۵ معماری Split-MAC ۳۲۵

۹-۶ بررسی کارکرد Wireless LAN Controller ۳۲۹

۹-۷ امنیت در شبکه‌های بی‌سیم ۳۳۰

۹-۸ احراز هویت (Authentication) ۳۳۰

۹-۹ روش‌های تایید اعتبار کاربران در شبکه‌ی بی‌سیم ۳۳۱

۹-۱۰ حریم خصوصی و روشهای یکپارچگی بی‌سیم ۳۳۴

۹-۱۱ بررسی WPA, WPA2, and WPA3 ..... ۳۳۵

۹-۱۲ اتصال به Acces Point سیسکو ۳۳۶

۹-۱۳ راه‌اندازی اولیه‌ی کنترلر LAN بی‌سیم WLC ۳۴۳

۹-۱۴ سوالات فصل نهم ۳۵۳

فصل دهم ۳۵۶

IP Access Control Lists ۳۵۶

۱۰-۱ Access List استاندارد ۳۵۷

۱۰-۲ استفاده از Access-List در پورت مجازی VTY ۳۶۳

۱۰-۳ Access List پیشرفته ۳۶۴

۱۰-۴ سوالات فصل دهم ۳۷۱

www.takbook.com

فصل یازدهم ۳۷۴
امنیت شبکه ۳۷۴
۱-۱۱ فرآیند مدیریت ریسک (Risk Management Process) ۳۷۷
۲-۱۱ شناخت تهدیدات شبکه فعلی ۳۷۸
۳-۱۱ کنترل و نظارت بر دسترسی کاربران ۳۸۱
۴-۱۱ کار با Port Security ۳۸۳
۵-۱۱ ایجاد امنیت در سرویس DHCP ۳۹۳
۶-۱۱ فعال‌سازی تأیید اعتبار در به روزرسانی مسیریابی در OSPF ۴۱۱
۷-۱۱ سوالات فصل یازدهم ۴۱۶
فصل دوازدهم ۴۲۰
IP Services ۴۲۰
۱-۱۲ پروتکل‌های مدیریت دستگاه‌ها ۴۲۰
۲-۱۲ Network Address Translation ۴۲۹
۳-۱۲ Quality of Service (QoS) ۴۳۶
۴-۱۲ Miscellaneous IP Services ۴۶۸
۵-۱۲ سوالات فصل دوازدهم ۴۸۹
فصل سیزدهم ۴۹۶
معماری شبکه ۴۹۶
۱-۱۳ قسمت اول – معماری LAN ۴۹۶
۲-۱۳ معماری WAN ۴۹۶
۳-۱۳ معماری Cloud ۵۷۳
۴-۱۳سوالات فصل سیزدهم ۵۸۰
فصل چهاردهم ۵۸۴

www.takbook.com

Network Automation ۵۸۴
۱۴-۱ SDN و شبکه مبتنی بر کنترلر ۵۸۴
۱۴-۲ APIهای مبتنی بر REST ۵۹۳
۱۴-۳ بررسی Ansible، Puppet و Chef ۶۳۳
۱۴-۵ سوالات فصل چهاردهم ۶۴۸
دستورات دوره‌ی CCNA ۶۵۲
نمودار تبدیل Binary/Hex/Decimal ۶۷۸
پاسخنامه سوالات فصل‌ها ۶۹۰
واژه نامه ۶۹۵
اعداد ۶۹۵
A ۶۹۵
B ۶۹۹
C ۷۰۱
D ۷۰۳
E ۷۰۵
F ۷۰۷
G ۷۰۸
H ۷۰۸
I ۷۰۹
K–L ۷۱۱
M ۷۱۳
N ۷۱۴
O ۷۱۵

www.takbook.com

P ۷۱۶

Q–R ۷۱۸

S ۷۲۰

T ۷۲۲

U ۷۲۳

V ۷۲۴

W ۷۲۶

X–Y–Z ۷۲۸

منابع ۰

www.takbook.com

www.takbook.com

www.takbook.com

مقدمه

با یاری پروردگار نون و قلم بر آن شدیم تا تجربه‌ی سال‌ها فعالیت خویش را در دنیای بی‌حد و مرز شبکه و سیسکو تقدیم مردمانی از جنس دانش کنیم.

هر روزنه‌ای از پیکره‌ی این دنیای وسیع دریچه‌ای است به بی‌کرانگی گستردگی‌های بی‌مانند. این کتاب دربردارنده‌ی ۱۴ فصل است که در پایان هر فصل، سؤالات هر فصل را شامل می‌شود تا ضمن یادگیری دستاوردهای شبکه با زبانی ساده و روان که جای‌جای همراه با تصویر است، دانش پژوه بتواند به صورت خودآموز یافته‌ها را در محک آزمون و خطا قرار دهد و آموخته‌ها ملکه‌ی ذهن گردد.

در این کتاب که نسخه‌ی جدید دوره‌ی CCNA شرکت سیسکو است و با شماره‌ی آزمون ۳۰۱-۲۰۰ معرفی شده است، فصل‌های زیر مورد بررسی قرار خواهد گرفت:

- ✓ **فصل اول – مباحث بنیادی شبکه**
- ✓ **فصل دوم – پیاده‌سازی شبکه‌های** Ethernet
- ✓ **فصل سوم – بررسی سوئیچینگ شبکه**
- ✓ **فصل چهارم – بررسی** IPV4
- ✓ **فصل پنجم – مسیریابی** (IP Routin)
- ✓ **فصل ششم – پروتکل** OSPF
- ✓ **فصل هفتم – نصب و راه‌اندازی** GNS3
- ✓ **فصل هشتم – بررسی پروتکل** IPV6
- ✓ **فصل نهم - شبکه‌های بی‌سیم**
- ✓ **فصل دهم –** IP Access Control Lists
- ✓ **فصل یازدهم – امنیت شبکه**
- ✓ **فصل دوازدهم –** IP Services
- ✓ **فصل سیزدهم – معماری شبکه**
- ✓ **فصل چهاردهم –** Network Automation

در پایان به نام زیستن باید ایستاد؛ زندگی را باید جست، در لابه‌لای حریق‌های سوخته، در عطش‌های ریزبرگ‌های پنهان‌سوز، در هر چه نامش، تجلّی‌گه عشق و عرفان است، در خود زندگی باید جست، باید خواند، مرگ را باور کرد، زنده بود به احترام تمام فصل‌های فراموش‌شده، باید لبریز از وجود شد و پژمرد... زندگی این است، زندگی را باید جست.

www.takbook.com

مدارک سیسکو

سیسکو به‌منظور تعلیم افراد برای طراحی و نگهداری شبکه‌های کامپیوتری، مرکزهای آموزشی تأسیس کرده است. سیسکو مدارکی را برای متخصصین در زمینه‌های مختلف شبکه ارائه می‌کند که شامل این مدارک می‌شود.

دسته‌ی اول (دستیار یا کارشناس شبکه)

Associate یا دستیار، یعنی قرارگرفتن در ابتدای مسیر، گرایش شما هرچه که باشد می‌بایست پیش از اخذ هر مدرک و یا گذراندن هر دوره‌ای، **CCNA** را بگذرانید! تغییرات گسترده‌ای که در سال ۲۰۲۰ ایجاد شده باعث شد تمام مدارک سیسکو که تا قبل از این به صورت جدا از هم بودند به صورت یکجا در یک مدرک ارائه شود و همین موضوع باعث شد کتاب جدیدی که در حال خواندن آن هستید به صورت کلی تغییر پیدا کند.

دوره‌ی CCNA شامل بخش‌های زیر است که در گذشته به صورت جدا از هم اجرا می‌شدند و برای هرکدام مدرک مخصوص به خودش صادر می‌شد.

- CCNA Routing and Switching
- CCDA
- CCNA Data Center
- CCNA Security
- CCNA Service Provider
- CCNA Service Provider Operations
- CCNA Video
- CCNA Voice
- CCNA Wireless

دسته‌ی دوم (کارشناس ارشد شبکه)

این دوره از سطح قبلی بالاتر و کمی سخت‌تر است، دوره‌ی CCNP هم به نسبت CCNA تغییراتی داشته که در لیست زیر مشاهده می‌کند.

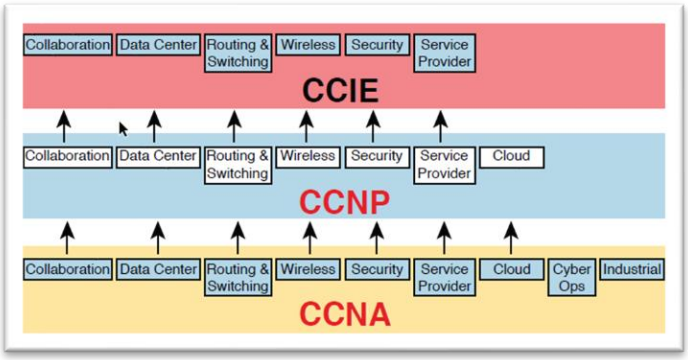
Collaboration (300-070)
Data Center (300-165)
Enterprise (300-401)
Security (300-208)
Service Provider(642-883)

دسته‌ی سوم (متخصص شبکه یا دکترای شبکه)

www.takbook.com

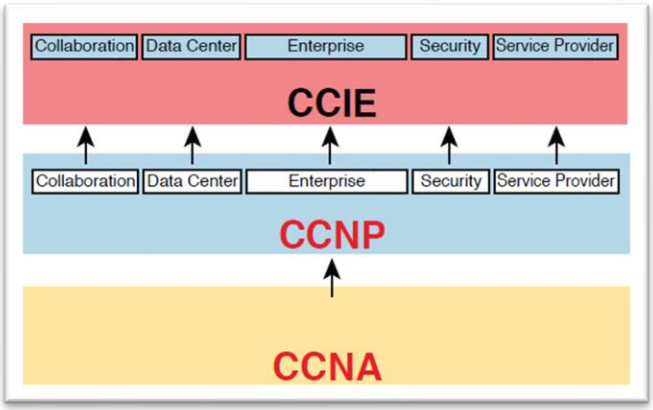
- Collaboration (400-051)
- Data Center (400-151)
- Enterprise (350-401)
- Security (400-251)
- Service Provider(350-801)

در شکل ۱، دوره‌های قدیمی شرکت سیسکو را مشاهده می‌کنید که هر بخش شامل چندین مدرک مختلف بوده است، ولی در حال حاضر این قسمت تغییر کرده است، برای مشاهده تغییرات به شکل ۲ توجه کنید.



شکل 1 - دوره‌های سیسکو

همان‌طور که در شکل ۲ مشاهده می‌کنید دوره‌ی CCNA به صورت یک دوره‌ی کلی درآمده و دیگر از مدارک مختلف خبری نیست، می‌توان گفت این دوره فشرده‌تر شده و در یک دوره خلاصه شده است، دوره‌های CCNP و CCIE هم تغییراتی داشته و به جای Routing and Switching و Wireless مدرک Enterprise جایگزین شده است.



شکل ۲- دوره‌های سیسکو

www.takbook.com

در این کتاب سعی شده است تمام عناوین دوره‌ی CCNA 200-301 که دارای سرفصل‌های گسترده‌تری است بررسی و آموزش داده شود، امتحانی که برای دریافت CCNA نیاز است آن را طی کنید فقط و فقط یک مورد است و آن هم امتحان 200-301 که دارای سرفصل‌های جدید و بیشتری به نسبت قبل است.

برای اینکه امتحان بین‌المللی سیسکو را بگذرانید باید وارد سایت vue.com شوید و زمان و مکان برگزاری امتحان سیسکو را مشخص و هزینه‌ی آن را پرداخت کنید.

نحوه برگزاری آزمون هم به صورت چندگزینه‌ای با یک یا چند پاسخ و به صورت آزمایشگاهی و مجازی است، در قسمت آزمایشگاه شبیه‌سازی شده، یک توپولوژی شبکه با سناریو را مشاهده خواهید کرد و از شما سؤال می‌شود که مشکل مشخص شده را در دستگاه موردنظر پیدا و حل کنید.

برای اینکه از شرایط برگزاری آزمون در سیسکو مطلع شوید بهتر است وارد سایت سیسکو شوید و عبارت "Cisco Certification Exam Tutorial Videos" جستجو کنید که فیلم‌های مربوط به آن را مشاهده خواهید کرد

www.takbook.com

www.takbook.com

www.takbook.com

www.takbook.com

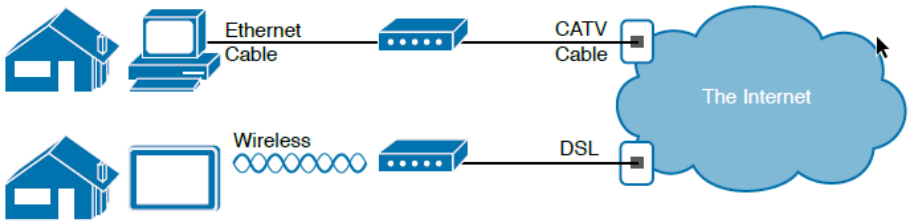
فصل اول

مباحث بنیادی شبکه

شما تازه وارد دنیای شبکه شده‌اید و به مانند اکثر افراد، دیدگاه‌های مختلفی در مورد آن دارید، نظر شما با نظر یک مهندس شبکه می‌تواند بسیار متفاوت باشد، شاید شما شبکه را در اتصال یک خط اینترنت ADSL ببینید.

در شکل ۱-۱، قسمت اول، یک کاربر معمولی با استفاده از سیستم خانگی خود به اینترنت متصل شده است، این ارتباط از طریق کابل و مودم انجام می‌شود که اصولاً از سرعت خوبی برخوردار است.

در قسمت دوم شکل ۱-۱ ، کاربر از طریق موبایل، تبلت، لپ‌تاپ به مودم وایرلس متصل می‌شود و از طریق لینک ADSL به اینترنت متصل می‌شود، فناوری وایرلس که این روزها گسترده‌تر شده بسیار طرف‌دار دارد و مودم‌های Router که برای بخش خانگی طراحی می‌شوند اکثراً از این فناوری پشتیبانی می‌کنند.



شکل ۱- ۱ ارتباط اینترنت

۱-۱ بررسی ساختار شبکه

در ساختار شبکه از دو مدل شبکه استفاده می‌شود.

- مدل OSI
- مدل TCP/IP

www.takbook.com

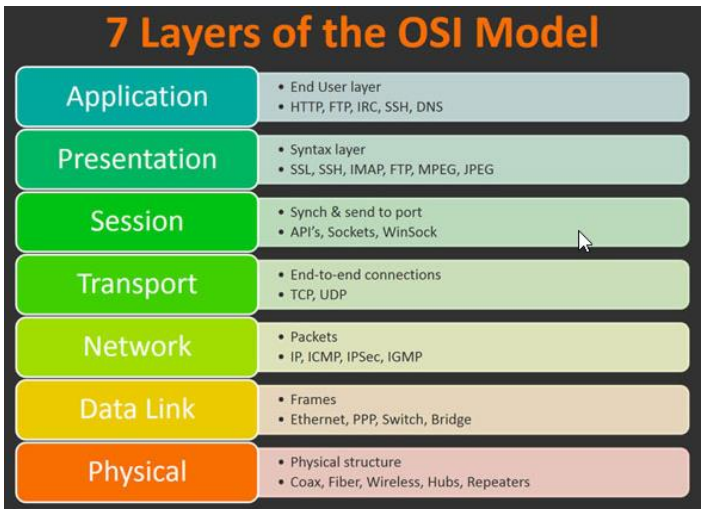
۱-۱-۱ بررسی مدل OSI

این مدل برگرفته از کلمه‌ی Open System Interconnection است و برای ارتباط بین دو کامپیوتر مبدأ و مقصد به کار می‌رود. این مدل در سال ۱۹۸۰ توسط سازمان ISO طراحی و پیاده‌سازی شده است و طبق سالیان متوالی تغییراتی روی آن صورت گرفته است، هرچند که همان ساختار اصلی خود را حفظ کرده است.

این مدل بر اساس یک سری قراردادها با لایه‌ی مقابل خود در کامپیوتر دیگر ارتباط برقرار می‌کند و این کار باعث افزایش سرعت و امنیت در شبکه خواهد شد.

تمام شرکت‌های نرم‌افزاری و سخت‌افزاری طبق این قرارداد محصولات خود را پیاده‌سازی می‌کنند. اگر توجه کرده باشید، بعضی از شرکت‌ها دارای گواهینامه ISO 9001,9002 و غیره می‌باشند، یعنی اینکه طبق استاندارد این سازمان باید کار کنند.

این مدل به صورت قراردادی از هفت لایه‌ی تشکیل‌شده است که هر لایه را برای شما توضیح می‌دهیم:



شکل ۲-۱ مدل OSI

اگر به شکل ۲-۱ توجه کنید، لایه‌های بالاتر به‌صورت نرم‌افزاری می‌باشند و هر چه به طرف لایه‌های پایین‌تر می‌آییم با سخت‌افزار کار داریم.

۱-۱-۱-۱ لایه‌ی Application (کاربردی)

این لایه با برنامه‌های کاربردی روی سیستم عامل که در شبکه کار می‌کنند ارتباط دارند، مانند نرم‌افزارهای مرورگر و انواع سرویس‌های مربوط به شبکه مانند (Telnet – pop3 – mail – ftp - tftp,…)،

www.takbook.com

این لایه اطلاعات دریافتی را قطعه‌قطعه می‌کند تا لایه‌ی پایینی آن بتواند این اطلاعات را درک کند. نظارت بر Error Recovery و Flow control در هنگام ارسال و دریافت اطلاعات بر عهده‌ی این لایه است.

در زیر لیست کامل پروتکل‌هایی که در این لایه کار می‌کنند را مشاهده می‌کنید:

- ✓ AFP, Apple Filing Protocol
- ✓ APPC, Advanced Program-to-Program Communication
- ✓ Telnet
- ✓ SSH
- ✓ FTP
- ✓ TFTP
- ✓ BOOTP
- ✓ SNMP
- ✓ CMOT
- ✓ AMQP, Advanced Message Queuing Protocol
- ✓ Atom Publishing Protocol
- ✓ BEEP, Block Extensible Exchange Protocol
- ✓ Bitcoin
- ✓ BitTorrent
- ✓ CFDP, Coherent File Distribution Protocol
- ✓ CoAP, Constrained Application Protocol
- ✓ DDS, Data Distribution Service
- ✓ DeviceNet
- ✓ eDonkey
- ✓ ENRP, Endpoint Handlespace Redundancy Protocol
- ✓ FastTrack (KaZaa, Grokster, iMesh)
- ✓ Finger, User Information Protocol
- ✓ Freenet
- ✓ FTAM, File Transfer Access and Management
- ✓ Gopher, Gopher protocol
- ✓ HL7, Health Level Seven
- ✓ HTTP, Hypertext Transfer Protocol
- ✓ H.323, Packet-Based Multimedia Communications System
- ✓ IMAP, Internet Message Access Protocol
- ✓ IRC, Internet Relay Chat
- ✓ IPFS, InterPlanetary File System
- ✓ Kademlia
- ✓ LDAP, Lightweight Directory Access Protocol
- ✓ LPD, Line Printer Daemon Protocol
- ✓ MIME (S-MIME), Multipurpose Internet Mail Extensions and Secure MIME
- ✓ Modbus
- ✓ MQTT Protocol
- ✓ Netconf
- ✓ NFS, Network File System
- ✓ NIS, Network Information Service
- ✓ NNTP, Network News Transfer Protocol
- ✓ NTCIP, National Transportation Communications for Intelligent Transportation System Protocol
- ✓ NTP, Network Time Protocol
- ✓ OSCAR, AOL Instant Messenger Protocol
- ✓ POP, Post Office Protocol
- ✓ PNRP, Peer Name Resolution Protocol

www.takbook.com

- ✓ RDP, Remote Desktop Protocol
- ✓ RELP, Reliable Event Logging Protocol
- ✓ RFP, Remote Framebuffer Protocol
- ✓ Rlogin, Remote Login in UNIX Systems
- ✓ RPC, Remote Procedure Call
- ✓ RTMP, Real Time Messaging Protocol
- ✓ RTP, Real-time Transport Protocol
- ✓ RTPS, Real Time Publish Subscribe
- ✓ RTSP, Real Time Streaming Protocol
- ✓ SAP, Session Announcement Protocol
- ✓ SDP, Session Description Protocol
- ✓ SIP, Session Initiation Protocol
- ✓ SLP, Service Location Protocol
- ✓ SMB, Server Message Block
- ✓ SMTP, Simple Mail Transfer Protocol
- ✓ SNTP, Simple Network Time Protocol
- ✓ SSH, Secure Shell
- ✓ SSMS, Secure SMS Messaging Protocol
- ✓ TCAP, Transaction Capabilities Application Part
- ✓ TDS, Tabular Data Stream
- ✓ Tor (anonymity network)
- ✓ Tox
- ✓ TSP, Time Stamp Protocol
- ✓ VTP, Virtual Terminal Protocol
- ✓ Whois (and RWhois), Remote Directory Access Protocol
- ✓ WebDAV
- ✓ X.400, Message Handling Service Protocol
- ✓ X.500, Directory Access Protocol (DAP)
- ✓ XMPP, Extensible Messaging and Presence Protocol
- ✓ Z39.50
- ✓ DNS, Domain Name Services

۲-۱-۱-۱ لایه‌ی Presentation (نمایش)

این لایه اطلاعات دریافتی را از لایه‌ی بالایی خود دریافت می‌کند و آن‌ها را فشرده‌سازی(Compression) و رمزنگاری(encryption) می‌کند و به لایه‌ی پایینی ارسال می‌کند، البته این لایه می‌تواند اطلاعات فشرده‌سازی شده را از حالت فشرده خارج کند (DeCompression) و هم می‌تواند قفل‌گشایی کند(decryption).

در زیر لیست کامل پروتکل‌هایی که در این لایه کار می‌کنند را مشاهده می‌کنید:

- ✓ Apple Filing Protocol (AFP)
- ✓ Independent Computing Architecture (ICA), the Citrix system core protocol
- ✓ Lightweight Presentation Protocol (LPP)
- ✓ NetWare Core Protocol (NCP)
- ✓ Network Data Representation (NDR)
- ✓ Telnet (a remote terminal access protocol)
- ✓ Tox
- ✓ eXternal Data Representation (XDR)
- ✓ X.25 Packet Assembler/Disassembler Protocol (PAD)

www.takbook.com

۳-۱-۱-۱ لایه‌ی Session (جلسه)

در این لایه، ۲ کامپیوتر ارسال و دریافت‌کننده اطلاعات، دور یک میز می‌نشینند و جلسه‌ای باهم برقرار می‌کنند. در این جلسه بر نوع فایل ارسالی بحث و گفتگو می‌شود که این فایل از چه نوعی است، وقتی به نتیجه رسیدند باهم ارتباط برقرار می‌کنند، به این موضوع هم توجه داشته باشید که آغاز و اتمام یک ارتباط از طریق این لایه انجام می‌گیرد.

در زیر لیست کامل پروتکل‌هایی که در این لایه کار می‌کنند را مشاهده می‌کنید:

- ✓ ADSP, AppleTalk Data Stream Protocol
- ✓ ASP, AppleTalk Session Protocol
- ✓ H.245, Call Control Protocol for Multimedia Communication
- ✓ ISO-SP, OSI session-layer protocol (X.225, ISO 8327)
- ✓ iSNS, Internet Storage Name Service
- ✓ L2F, Layer 2 Forwarding Protocol
- ✓ L2TP, Layer 2 Tunneling Protocol
- ✓ NetBIOS, Network Basic Input Output System
- ✓ PAP, Password Authentication Protocol
- ✓ PPTP, Point-to-Point Tunneling Protocol
- ✓ RPC, Remote Procedure Call Protocol
- ✓ RTCP, Real-time Transport Control Protocol
- ✓ SMPP, Short Message Peer-to-Peer
- ✓ SCP, Session Control Protocol
- ✓ SOCKS, the SOCKS internet protocol
- ✓ ZIP, Zone Information Protocol
- ✓ SDP, Sockets Direct Protocol

۴-۱-۱-۱ لایه‌ی Transport (انتقال)

برای توضیح این لایه، باید ۲ نوع ارتباط را برای شما تشریح کنیم:

- Connection Less
- Connection Oriented

۱- در ارتباط connection Less کامپیوتر مبدأ برای کامپیوتر مقصد اطلاعات ارسال می‌کنند، اما کامپیوتر مقصد هیچ‌گونه پیامی (Acknowledge) مبنی بر دریافت اطلاعات به کامپیوتر مبدأ نمی‌دهد. این مدل را می‌توانید در نرم‌افزارهای چت که به صورت صوتی با طرف خود صحبت می‌کنید، مشاهده کنید که با این کار سرعت انتقال اطلاعات به علت عدم دریافت Acknowledge افزایش می‌یابد.

۲- در ارتباط Connection oriented که ارتباط بسیار مهمی است، کامپیوتر مبدأ اطلاعات خود را به کامپیوتر مقصد ارسال می‌کند و منتظر می‌ماند تا کامپیوتر مقصد، پیام Acknowledge را به مبدأ ارسال کند تا متوجه‌ی دریافت اطلاعات در مقصد شود. اگر این کار انجام نشود در طی زمان مشخص، دوباره اطلاعات را برای مقصد ارسال می‌کند، تا زمانی این کار انجام می‌شود که کامپیوتر مقصد Acknowledge را ارسال کند. این روش برای ارتباطات حساس، بسیار کاربرد دارد.

www.takbook.com

Acknowledge یک تأییدی بر دریافت اطلاعات به صورت صحیح است.

در این لایه، این ۲ ارتباط که در بالا توضیح دادم مشخص می‌شود، یعنی طبق فایلی که ارسال می‌شود ارتباط آن هم مشخص می‌شود.

پروتکل‌هایی که در این لایه کار می‌کنند:

- ✓ ATP, AppleTalk Transaction Protocol
- ✓ CUDP, Cyclic UDP[3]
- ✓ DCCP, Datagram Congestion Control Protocol
- ✓ FCP, Fibre Channel Protocol
- ✓ IL, IL Protocol
- ✓ MPTCP, Multipath TCP
- ✓ RDP, Reliable Data Protocol
- ✓ RUDP, Reliable User Datagram Protocol
- ✓ SCTP, Stream Control Transmission Protocol
- ✓ SPX, Sequenced Packet Exchange
- ✓ SST, Structured Stream Transport
- ✓ TCP, Transmission Control Protocol
- ✓ UDP, User Datagram Protocol
- ✓ UDP-Lite
- ✓ µTP, Micro Transport Protocol

۵-۱-۱-۱ لایه‌ی Network (شبکه)

این لایه با ipها سروکار دارد و ip مقصد و مبدأ را به بسته‌ی ارسالی ما اضافه می‌کند و به لایه پایین‌تر می‌فرستد و وظیفایف کامل آن عبارت‌اند از:

۱. کنترل عملکرد زیر شبکه
۲. مسیریابی
۳. QOS
۴. به پیوستن شبکه‌های نا همگن

پروتکل‌هایی که در این لایه کار می‌کنند:

- ✓ IPv4/IPv6, Internet Protocol
- ✓ DVMRP, Distance Vector Multicast Routing Protocol
- ✓ ICMP, Internet Control Message Protocol
- ✓ IGMP, Internet Group Management Protocol
- ✓ PIM-SM, Protocol Independent Multicast Sparse Mode
- ✓ PIM-DM, Protocol Independent Multicast Dense Mode
- ✓ IPsec, Internet Protocol Security
- ✓ IPX, Internetwork Packet Exchange
- ✓ RIP, Routing Information Protocol
- ✓ DDP, Datagram Delivery Protocol

www.takbook.com

- ✓ RSMLT Routed-SMLT
- ✓ ARP, Address Resolution Protocol

۶-۱-۱-۱ لایه‌ی Data Link (داده)

آدرس Mac کارت‌های شبکه که یک شماره اختصاصی است به بسته‌ها اضافه می‌شود. اگر به شکل لایه‌ها تصویر قبلی توجه کنید متوجه‌ی این موضوع خواهید شد.

در کل لایه‌ی Data Link یا پیونددادهٔ به دو زیر لایه‌ی LLC و MAC تقسیم می‌شوند، MAC مخفف کلمه‌ی Media Access Control است و LLC هم مخفف کلمه‌ی Logical Link Control است.

پروتکل‌هایی که در این لایه کار می‌کنند:

- ✓ Address Resolution Protocol (ARP)
- ✓ ARCnet
- ✓ ATM
- ✓ Cisco Discovery Protocol (CDP)
- ✓ Controller Area Network (CAN)
- ✓ Econet
- ✓ Ethernet
- ✓ Ethernet Automatic Protection Switching (EAPS)
- ✓ Fiber Distributed Data Interface (FDDI)
- ✓ Frame Relay
- ✓ High-Level Data Link Control (HDLC)
- ✓ IEEE 802.2 (provides LLC functions to IEEE 802 MAC layers)
- ✓ IEEE 802.11 wireless LAN
- ✓ LattisNet
- ✓ Link Access Procedures, D channel (LAPD)
- ✓ LocalTalk
- ✓ Multiprotocol Label Switching (MPLS)
- ✓ Nortel Discovery Protocol (NDP)
- ✓ OpenFlow (SDN)
- ✓ Split multi-link trunking (SMLT)
- ✓ Point-to-Point Protocol (PPP)
- ✓ Serial Line Internet Protocol (SLIP) (obsolete)
- ✓ Spanning Tree Protocol
- ✓ StarLan
- ✓ Token ring
- ✓ Unidirectional Link Detection (UDLD)
- ✓ and most forms of serial communication.

۷-۱-۱-۱ لایه‌ی Physical (لایه‌ی فیزیکی)

این لایه که پائینترین لایه در مدل OSI است، با سیگنال‌ها و کابل‌ها در ارتباط است و سیگنال را از طریق کابل به کامپیوتر مورد نظر ارسال می‌کند.

در زیر لیست تکنولوژی‌هایی که با لایه‌ی فیزیکی کار می‌کنند را مشاهده می‌کنید:

- ✓ 1-Wire
- ✓ ARINC 818 Avionics Digital Video Bus
- ✓ Bluetooth physical layer
- ✓ CAN bus (controller area network) physical layer

www.takbook.com

- ✓ DSL
- ✓ EIA RS-232, EIA-422, EIA-423, RS-449, RS-485
- ✓ Etherloop
- ✓ Ethernet physical layer Including 10BASE-T, 10BASE2, 10BASE5, 100BASE-TX, 100BASE-FX, 100BASE-T, 1000BASE-T, 1000BASE-SX and other varieties
- ✓ G.hn/G.9960 physical layer
- ✓ GSM Um air interface physical layer
- ✓ IEEE 802.15.4 physical layers
- ✓ IEEE 1394 interface
- ✓ IRDA physical layer
- ✓ ISDN
- ✓ ITU Recommendations: see ITU-T
- ✓ I^2C, I^2S
- ✓ LoRa
- ✓ Low-voltage differential signaling
- ✓ Mobile Industry Processor Interface physical layer
- ✓ Modulated ultrasound
- ✓ Optical Transport Network (OTN)
- ✓ SMB
- ✓ SONET/SDH
- ✓ SPI
- ✓ T1 and other T-carrier links, and E1 and other E-carrier links
- ✓ Telephone network modems — V.92
- ✓ TransferJet physical layer
- ✓ USB physical layer
- ✓ Varieties of 802.11 Wi-Fi physical layers
- ✓ Visible light communication co-ordinated under IEEE 802.15.7
- ✓ X10

۲-۱-۱بررسی مدل TCP / IP

TCP/IP یا Transmission Control Protocol/ Internet Protocol مدلی است که در همه‌ی سیستم‌عامل‌ها کاربرد دارد و بسیار انعطاف‌پذیر است، یکی از ویژگی‌های مهم آن Connection-Oriented است یعنی تا زمانی که تایید اطلاعات را دریافت نکند اطلاعات را ارسال نمی‌کند.

یکی دیگر از ویژگی‌های این شبکه این است که وقتی کلاینتی آدرسی را دریافت کرده آن آدرس تا آخر برای آن کلاینت باقی می‌ماند به جزء اینکه آن کلاینت مسیرش تغییر کند و آدرس را از دست بدهد.

در این مدل از شبکه که با IP سرو کار دارد تغییراتی در لایه‌بندی مشاهده می‌کنید ، در مدل OSI سه‌لایه اول جدا از هم قرار گرفته‌اند ولی در مدل TCP/IP این سه لایه در یک لایه‌ی Application جمع شده‌اند و در آخر هم دولایه مورد نظر در یک لایه‌ی Network Interface قرار گرفتند، در زیر هر چهار لایه را مورد بررسی قرار می‌دهیم.

www.takbook.com

۱-۲-۱-۱ لایه‌ی Application

لایه‌ی Application، بالاترین لایه در پشته‌ی TCP/IP است. تمامی برنامه‌ها و ابزارهای کاربردی در این لایه، با استفاده از لایه‌ی فوق، قادر به دست‌یابی به شبکه خواهند بود. پروتکل‌های موجود در این لایه، به منظور فرمت‌دهی و مبادله‌ی اطلاعات کاربران استفاده می‌گردند. HTTP و FTP دو نمونه از پروتکل‌های هستند که در این لایه کار می‌کنند.

یک نکته که در این لایه باید بدانید این است که این لایه برنامه‌ها را تعریف نمی‌کند بلکه بر روی سرویس‌های آنها عمل می‌کند.

پروتکل HTTP (Hypertext Transfer Protocol)، به منظور ارسال فایل‌های صفحات وب، استفاده می‌گردد که امروزه بسیار گسترده شده و تمام شرکت‌ها نرم‌افزارهای خود را بر روی این بستر پیاده‌سازی می‌کنند تا هم منابع سخت‌افزاری زیادی برای اجرای مشتریان نیاز نباشد و خیلی سریع و امن در دسترس باشد.

پروتکل FTP (File Transfer Protocol)، برای ارسال و دریافت فایل استفاده می‌گردد.

۲-۲-۱-۱ لایه‌ی Transport

لایه‌ی Transport، قابلیت ایجاد نظم و ترتیب و تضمین ارتباط بین کامپیوترها و ارسال داده به لایه‌ی application (لایه‌ی بالای خود) و یا لایه‌ی Internet (لایه‌ی پایین خود) را بر عهده دارد. لایه‌ی فوق، همچنین مشخصه‌ی منحصر به فردی از برنامه‌ای که داده را عرضه نموده است، مشخص می‌نماید. این لایه، دارای دو پروتکل اساسی است که نحوه‌ی توزیع داده را کنترل می‌نمایند.

TCP(Transmission Control Protocol)، پروتکل فوق مسئول تضمین صحت توزیع اطلاعات است.

UDP(User Datagram Protocol) پروتکل فوق، بسیار سریع عمل می‌کند و اطلاعات را به مقصد می‌رساند بدون آنکه تاییدیه‌ای از طرف مقابل خود دریافت کند.

۳-۲-۱-۱ لایه‌ی Internet

لایه‌ی اینترنت، مسئول آدرس‌دهی، بسته‌بندی و روتینگ داده‌ها است. لایه‌ی فوق، شامل چهار پروتکل اساسی است:

- **IP**(Internet Protocol) پروتکل فوق، مسئول آدرسی داده‌ها به‌منظور ارسال به مقصد مورد نظر است.
- **ARP**(Address Resoulation Protocol) پروتکل فوق، مسئول مشخص نمودن آدرس MAC (Media Access Control) کارت شبکه بر روی کامپیوتر مقصد است.
- **ICMP**(Internet Control Message Protocol) پروتکل فوق، مسئول ارائه‌ی توابع عیب‌یابی و گزارش خطا در صورت عدم توزیع صحیح اطلاعات است.
- **IGMP**(Internet Group Managemant Protocol) مسئولیت مدیریت Multicasting در TCP/IP را بر عهده دارد.

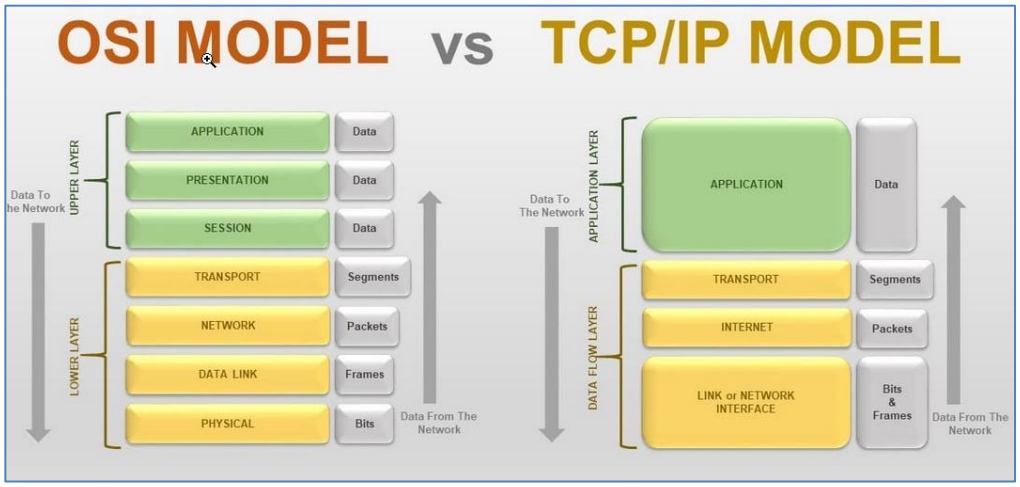
www.takbook.com

۱-۱-۲-۴ لایه‌ی Network

پائین‌ترین لایه در مدل TCP/IP است و با سخت‌افزار سرو کار دارد. لایه‌ی فوق، شامل دستگاه‌های فیزیکی نظیر کابل شبکه و آداپتورهای شبکه است. کارت شبکه (آداپتور) دارای یک عدد دوازده رقمی مبنای شانزده بوده که آدرس MAC، نامیده می‌شود. پروتکل‌های Ethernet ,PPP ,ATM (Asynchronous Transfer Mode)، نمونه‌هایی از پروتکل‌های موجود در این لایه هستند. پروتکل‌های فوق، نحوه‌ی ارسال داده در شبکه را مشخص می‌نمایند.

۱-۱-۲-۵ تفاوت بین مدل OSI و TCP/IP

در این قسمت تفاوت‌های بین این دو مدل را مورد بررسی قرار می‌دهیم، در شکل ۳-۱ تفاوت بنیادی این دو روش را مشاهده می‌کنید.



شکل ۳- ۱ تفاوت بین دو مدل OSI و TCP/IP

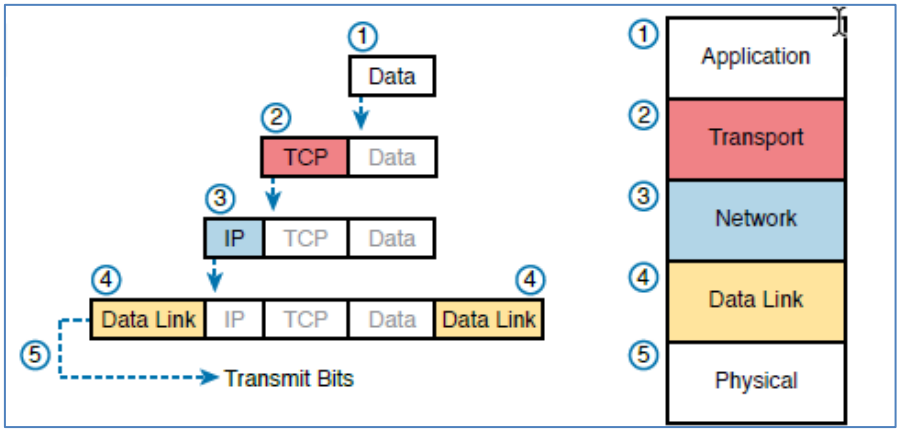
جدول ۱-۱ تفاوت دو مدل

مدل TCP / IP	مدل OSI
توسط ARPANET (شبکه آژانس پروژه تحقیق پیشرفته) ایجاد شده و توسعه یافته است.	توسط ISO (سازمان استاندارد بین المللی) ایجاد و توسعه یافته است.
TCP/IP هیچ نقطه تمایز روشنی بین سرویس ها ، واسط ها و پروتکل‌ها ندارد.	مدل OSI تمایز واضحی بین رابطها ، خدمات و پروتکل‌ها ارائه می‌دهد.
TCP به پروتکل کنترل انتقال اشاره دارد.	OSI به ارتباط بین سیستم‌های باز اشاره دارد.
TCP/IP فقط از لایه‌ی اینترنت استفاده می‌کند.	OSI از لایه‌ی شبکه برای تعریف استانداردهای مسیریابی و پروتکل‌ها استفاده می‌کند.
TCP/IP از یک روش افقی پیروی می‌کند.	OSI از یک روش عمودی پیروی می‌کند.

www.takbook.com

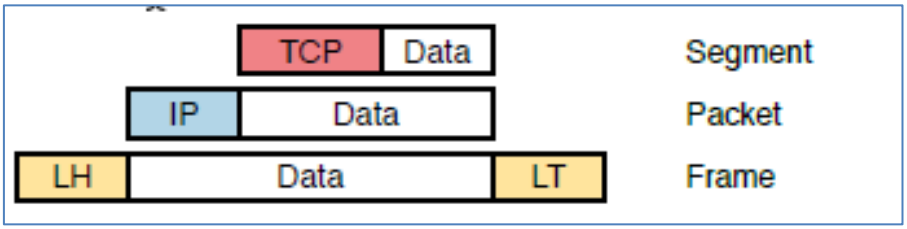
TCP / IP فقط از یک لایه (پیوند) استفاده می‌کند.	مدل OSI از دو لایه جداگانه فیزیکی و داده برای تعریف عملکرد لایه‌های پائین استفاده می‌کند.
TCP / IP چهار لایه دارد.	لایه های OSI دارای هفت لایه هستند.
TCP/IP هم connection-oriented است و هم connectionless.	OSI فقط connection-oriented است.
در TCP، پیوند فیزیکی و داده به عنوان یک لایه میزبان به شبکه واحد ترکیب می شوند.	در مدل OSI ، لایه پیوند داده و فیزیکی لایه های جداگانه ای هستند.
هیچ لایه‌ای برای ارائه و ارائه در مدل TCP وجود ندارد.	لایه های جلسه و ارائه بخشی از مدل TCP نیستند.
قبل از ظهور اینترنت تعریف شده است.	این تعریف پس از ظهور اینترنت است.
حداقل اندازه هدر ۲۰ بایت است.	حداقل اندازه هدر OSI ۵ بایت است.

زمانی که اطلاعات در مدل TCP/IP در حال انتقال هستند در هر مرحله یک بخش به هدر داده مورد نظر اضافه می‌شود که در شکل ۴-۱ چنین موضوعی قابل مشاهده است.



شکل ۴-۱ Data Encapsulation

هر قسمت از این مراحل دارای نام‌های مختلف هستند که در شکل ۵-۱ مشاهده می‌کنید.



شکل ۵-۱ نام مراحل Encapsulation

تفاوت‌های کلیدی بین دو مدل TCP/IP و OSI را در زیر مشاهده می‌کنید:

www.takbook.com

- OSI دارای ۷ لایه است در حالی که TCP / IP دارای ۴ لایه است.
- مدل OSI یک مدل منطقی و مفهومی است که ارتباطات شبکه ای را که توسط سیستم های باز برای اتصال و ارتباط با سایر سیستم ها استفاده می‌شود ، تعریف می‌کند. از طرف دیگر، TCP / IP به شما کمک می‌کند تا تعیین کنید که چگونه یک کامپیوتر خاص باید به اینترنت وصل شود و چگونه می توانید بین آنها اطلاعات را انتقال دهید.
- هدر مدل OSI فقط 5 بایت است در حالی که اندازه هدر TCP / IP برابر 20 بایت است.
- مدل OSI به اتصال به سیستم های باز اشاره دارد در حالی که TCP / IP به پروتکل TCP اشاره دارد.
- مدل OSI به شما در استانداردسازی روتر ، سوئیچ ، مادربرد و سایر سخت‌افزارها کمک می‌کند در حالی که TCP / IP به شما کمک می‌کند تا بین انواع مختلف رایانه ارتباط برقرار کنید.

۱-۲ اصول کار با شبکه‌های اترنت

اکثر شبکه‌های کامپیوتری سازمانی را می‌توانید به دو نوع مختلف تفکیک کرد:

- شبکه‌ی محلی یا همان LAN
- شبکه‌های گسترده و یا همان WAN

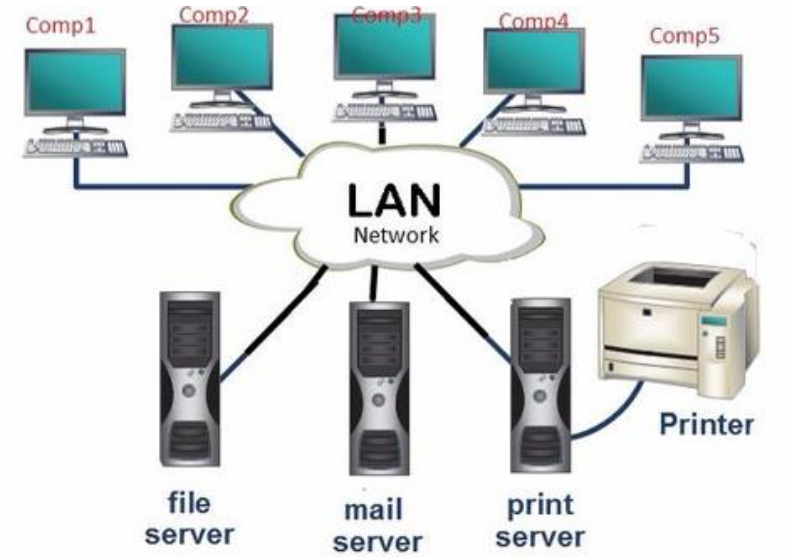
دستگاهایی که در مجاورت هم قرار دارند با استفاده از شبکه‌یLAN به هم متصل می‌شوند و طرف مقابل آن، شبکه‌ی WAN قرار دارد که دستگاه‌هایی که با هم فاصله زیاد داشته باشند را به هم متصل می‌کند مثلاً فاصله یک شهر با شهر دیگر.

۱-۲-۱ انواع شبکه‌های LAN

در این نوع شبکه از کابل‌های مختلفی استفاده می‌شود که این نوع کابل‌ها از نوع مس با کیفیت‌های مختلف وجود دارند که می‌توانند کلاینت‌های مورد نظر را در یک اتاق به هم متصل کنند و اصولاً از کیفیت خوبی برخوردار هستند، البته کابل‌های فیبر نوری را هم می‌توانیم در این دسته قرار دهیم که سرعت کابل‌های معمولی در برابر آنها هیچ است.

نوع شبکه دیگر با عنوان شبکه‌ی بی‌سیم شناخته می‌شود و امروزه از بسیار گسترده شده و رشد کرده است، در این نوع شبکه‌ها از کابل استفاده نمی‌کنند بلکه از امواج رادیویی برای پیوند با دستگاه‌ها استفاده می‌کنند، در ادامه کتاب به صورت گسترده در مورد شبکه بی‌سیم بحث خواهیم کرد.

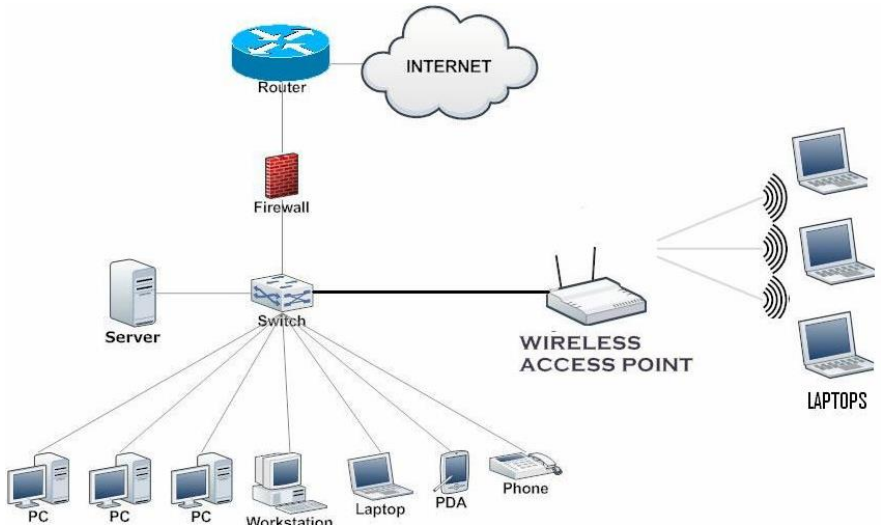
www.takbook.com



شکل ۶- ۱ شبکه‌ی LAN

شبکه‌های SOHO

SOHO مترادف Smal Office/Home Office است که به معنای یک شبکه اداری و خانگی کوچک است که دارای چندین کلاینت،روتر، فایروال و دستگاهای وایرلس است که در شکل ۷-۱ آن را در زیر مشاهده می‌کنید.

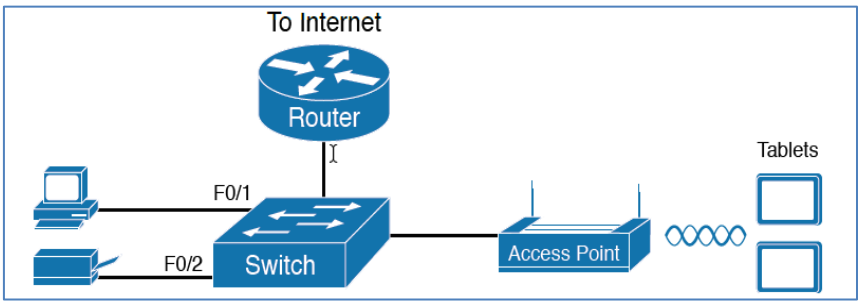


شکل ۷- ۱ شبکه‌ی SOHO

www.takbook.com

در این نوع شبکه‌ها کلاینت‌ها از طریق سوئیچ با کلاینت‌ها و سرورهای دیگر در ارتباط هستند، حتی می‌توان یک AccessPoint برای متصل شدن دستگاه‌های بی‌سیم به شبکه، راه‌اندازی کرد.

امروزه در شبکه‌های خانگی از یک روتر هم به عنوان اینترنت و هم به عنوان سوئیچ استفاده می‌کنند و چند سیستم را از طریق کابل و WIFI به هم متصل می‌کنند، در شکل ۸-۱ یک AccessPoint را مشاهده می‌کنید که به کلاینت‌های WIFI سرویس ارائه می‌دهد.



شکل ۸- ۱ نوع شبکه Small Wired and Wireless

شبکه‌ی LAN بی‌سیم توسط سازمان IEEE تعریف شده و شماره استاندارد آن 802.11 است.

شبکه‌های Enterprise

شبکه‌های سازمانی یک چیزی شبیه به شبکه‌ی SOHO است با این تفاوت که مقیاس آن بسیار بزرگتر از آن است، به عنوان مثال یک ساختمان چند طبقه را در نظر بگیرید که در هر طبقه از یک رک دیواری و سوئیچ برای متصل کردن طبقات استفاده می‌شود، رک‌های دیواری دارای قفل هستند و هر کسی نمی‌تواند به آنها دسترسی داشته باشد.

این مدل رک‌ها در ابعاد کوچک و برای قرار گرفتن سوئیچ‌ها در آن استفاده می‌شود، شاید این مدل رک‌ها را در سازمان‌های مختلف مشاهده کردید، رک‌های دیواری در اندازه‌های ۴، ۶، ۹، ۱۲ یونیت موجود می‌باشند که نمونه‌ای از رک ۹ یونیت را در شکل ۹-۱ مشاهده می‌کنید.

اصولاً این نوع رک‌ها دارای یک عدد فن و چند راهی برق هستند و در بیشتر مدل‌های امروزی، درب آن از هر سه طرف چپ، راست و جلو باز می‌شود.

www.takbook.com

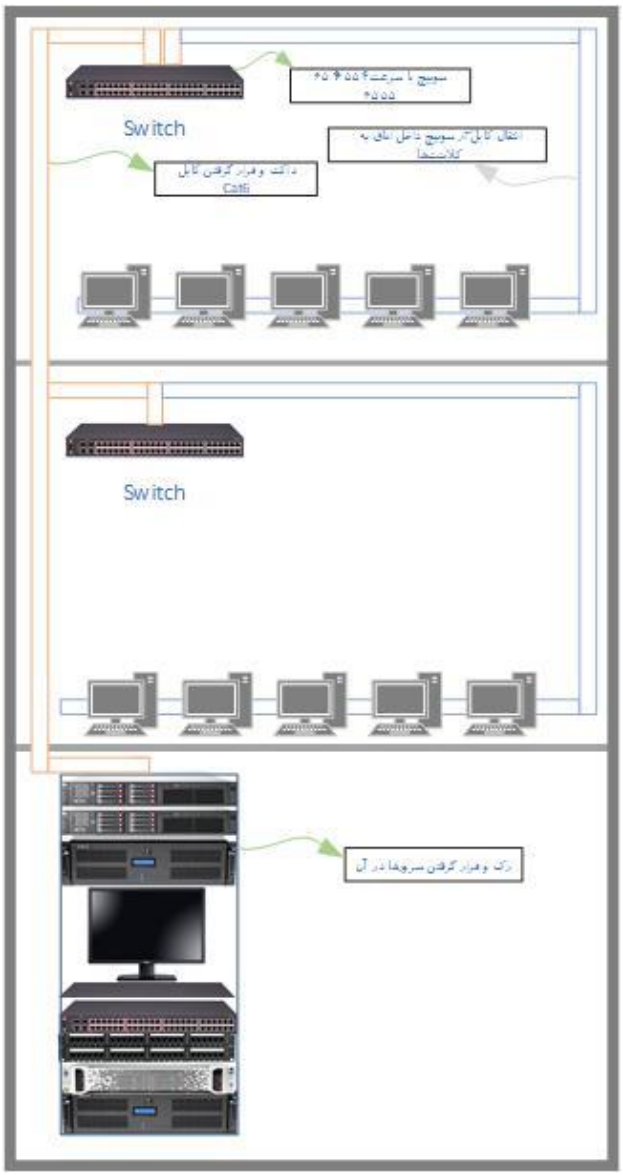
شکل ۹- ۱ *Small Rack*

اصولاً برای راحتی کار کارمندان آن سازمان از دستگاه‌های بی‌سیم هم برای متصل شدن به شبکه استفاده می‌شود.

در شکل ۱۰-۱، یک ساختمان شماتیک را رسم کردیم که در طبقه‌ی همکف آن، اتاق سرور قرار دارد که در داخل این اتاق سرور، یک رک با تعدادی سرور، سوئیچ، پچ پنل و مانیتور قرار دارد، برای اینکه سرعت و کیفیّت کار افزایش پیدا کند از یک سوئیچ با سرعت ۱۰۰۰/۱۰۰/۱۰ استفاده کردیم و کابل شبکه را نیز از نوع CAT6 در نظر گرفتیم، برای انتقال کابل‌ها به طبقات و اتاق‌های دیگر باید از داکت استفاده کنیم.

توجه داشته باشید برای فراگیری این مباحث به صورت تخصصی‌تر باید کتاب مدیر شبکه‌ی دو را از سایت 3isco.ir دریافت و مطالعه کنید.

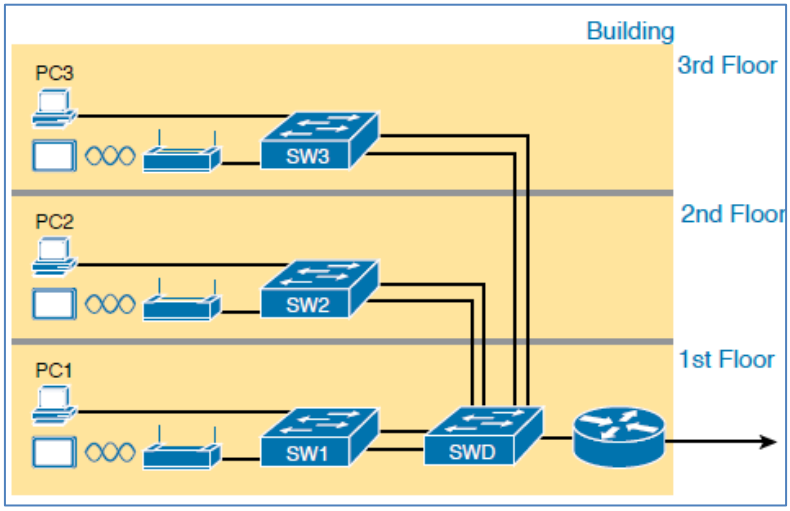
www.takbook.com



شکل ۱۰- ۱ شبکه‌ی LAN در یک ساختمان سه طبقه

در شکل ۱۱-۱ هم یک ساختمان سه طبقه را در نظر بگیرید که در هر طبقه یک سوئیچ قرار دارد و کلاینت‌ها هم از طریق کابل و هم از طریق بی‌سیم به شبکه متصل می‌شوند.

www.takbook.com



شکل ۱۱- ۱ شبکه‌ی LAN در یک ساختمان سه طبقه

کابل‌های اترنت دارای انواع مختلفی هستند و بسته به موادی که در آنها به کار رفته دارای کیفیت‌های مختلف هستند، کابل‌های مسی به نسبت کابل‌های نوری ارزانتر هستند ولی کابل‌های نوری مسافت خیلی زیادی را پشتیبانی می‌کنند و از سرعت بسیار بالایی برخوردارند.

کابل‌های معمولی با پسوند T که اکثراً با نام UTP شناخته می‌شوند و کابل نوری که با پسوند X شناخته می‌شوند، در زیر کابل‌ها با مدل و سرعت مختلف را مشاهده می‌کنید.

اگر توجه کنید کابلی که در ستون informal IEEE standard Name دارای پسوند X است یک کابل Fiber یا همان نوری است.

جدول ۲-۱ Types of Ethernet

Speed	Common Name	Informal IEEE Standard Name	Formal IEEE Standard Name	Cable Type, Maximum Length
10 Mbps	Ethernet	10BASE-T	802.3	Copper, 100 m
100 Mbps	Fast Ethernet	100BASE-T	802.3u	Copper, 100 m
1000 Mbps	Gigabit Ethernet	1000BASE-LX	802.3z	Fiber, 5000 m
1000 Mbps	Gigabit Ethernet	1000BASE-T	802.3ab	Copper, 100 m
10 Gbps	10 Gig Ethernet	10GBASE-T	802.3an	Copper, 100 m

۲-۲-۱ نگاهی به کابل‌ها در شبکه

در این بخش، کابل‌های مختلف را بررسی می‌کنیم و با انواع آن کار می‌کنیم.

کل شبکه‌های امروزی از یکی از گروه‌های کابلی زیر استفاده می‌کند.

- ✓ کابل هم‌محور(coaxial)

www.takbook.com

- ✓ زوج تابیده‌شده(twisted-pair)
- ✓ فیبر نوری(fiber-optic)
- ✓ کابل سریال
- ✓ کابل Console

کابل هم‌محور Coaxial

این نوع کابل معمولاً در بیشتر شبکه‌های امروزی استفاده می‌شود، اما فقط در استفاده‌های خاص در ساده‌ترین شکل آن، کابل coaxial تشکیل‌شده است از یک هسته‌ی ساخته‌شده از مس خالص که توسط روکشی پوشیده شده است. یک روکش فلزی توری مانند و یک روکش بیرونی. هسته‌ی کابل coaxial حامل سیگنال‌های الکتریکی است که در واقع همان اطلاعات ما را تشکیل می‌دهد.

این نوع کابل‌ها از یک روکش توری استفاده می‌کنند که کابل را در برابر امواج مزاحم یا همان Noise دور می‌کند. کلاً این نوع کابل برای ارتباط راه دور استفاده می‌شود، چون در ارتباط راه دور، افت سیگنال ندارد و نسبت به کابل Twisted Pair بهتر است

انواع کابل Coaxial

- ✓ نازک(Thinnet)
- ✓ ضخیم (Thicknet)

کابل نوع Thinnet

Thinnet یک کابل coaxial انعطاف‌پذیر به ضخامت ۰/۲۵ اینچ است.

به خاطر انعطاف و سادگی استفاده، تقریباً در نصب هر نوع شبکه‌ای می‌توان از آن استفاده کرد. این نوع کابل می‌تواند سیگنال را تقریباً ۱۸۵ متر بدون افت سیگنال حمل نماید. کابل thninnet در خانواده‌ای از کابل‌ها به نام RG– ۵۸ قراردارد و امپدانس معادل ۵۰ اهم دارد. امپدانس، مقاومت سیم است که برحسب اهم، اندازه‌گیری شده است. اختلاف اصلی در کابل‌های خانواده‌ی RG– ۵۸، هسته‌ی کابل است که ممکن است به شکل تک رشته یا چند رشته باشد، در شکل ۱۲–۱ و۱۳–۱ دو نمونه از این کابل را مشاهده می‌کنید.

www.takbook.com

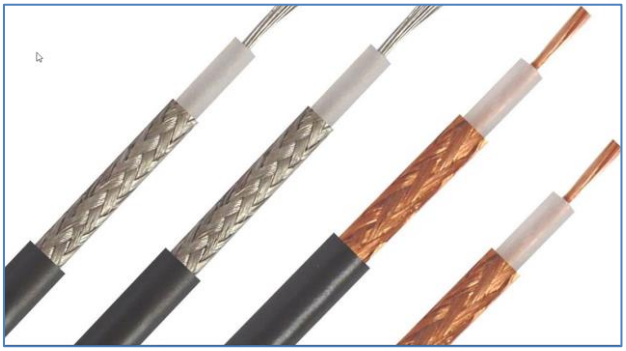
شکل ۱۲- ۱ کابل *Thinnet*

شکل ۱۳- ۱ کابل *Thinnet*

کابل نوع Thicknet

Thicknet یک کابل coaxial ضخیم به قطر ۰/۵ اینچ است. هرچه هسته‌ی مس ضخیم‌تر باشد، به همان اندازه کابل می‌تواند سیگنال را به فاصله‌ی طولانی‌تر حمل کند. این بدین معناست که کابل‌های Thicknet سیگنال را بیشتر از کابل‌های Thinnet می‌توانند حمل کنند. کابل Thinnet می‌تواند سیگنال را تا ۵۰۰ متر حمل کند. توجه داشته باشید که به این کابل Ethernet هم می‌گویند، چون برای اولین بار در این شبکه استفاده شده است. به دلیل اینکه این کابل می‌تواند در فاصله‌ی دورتر سیگنال را انتقال دهند. معمولاً از آن به عنوان ارتباط‌دهنده‌ی چندین شبکه محلی استفاده می‌کنند. به این موضوع هم توجه داشته باشید که این کابل برای انتقال تصاویر متحرک و صوت در فواصل دور استفاده می‌شود، شکل ۱۴-۱ نمونه‌ای از کابل‌های Thicknet را نشان می‌دهد.

www.takbook.com



شکل ۱۴- ۱ کابل Thicknet

انواع connectorهایی که در کابل Coaxial استفاده می‌شوند را می‌توانید در شکل ۱۵-۱ مشاهده کنید.

شکل ۱۵- ۱ connector کابل Thicknet

کارت شبکه‌ای که برای این کابل استفاده می‌شود، مخصوص همین کابل است. به شکل ۱۶-۱ توجه کنید.

شکل ۱۶- ۱ کارت شبکه‌ی کابل Thicknet

www.takbook.com

برای ارتباط کابل Thinnet به کابل Ticknet از وسیله‌ای به نام Tranciver استفاده می‌شود که شکل ۱-۱۷ را مشاهده می‌کنید.

شکل ۱۷- ۱ *Tranciver*

همان‌طور که گفتیم حداکثر طول انتقال سیگنال‌ها توسط این دو نوع کابل coaxial، 185 و 500 متر است و بعد از آن بر روی آن noise تأثیرگذار می‌شود و عملاً کابل از مسیر خارج می‌شود. برای حل این مشکل از وسیله‌ای به نام Repeater استفاده می‌کنند که سیگنال‌ها را تقویت می‌کند و به کابل بعدی می‌فرستد که در شکل ۱-۱۸ این دستگاه را مشاهده می‌کنید.

شکل ۱۸- ۱ *Repeater*

کابل Twisted-pair یا زوج به هم تابیده

در ساده‌ترین شکل، کابل Twisted-pair دارای یک زوج سیم به هم تابیده از مس که دارای روکش است. دو نوع کابل Twisted-pair وجود دارد:

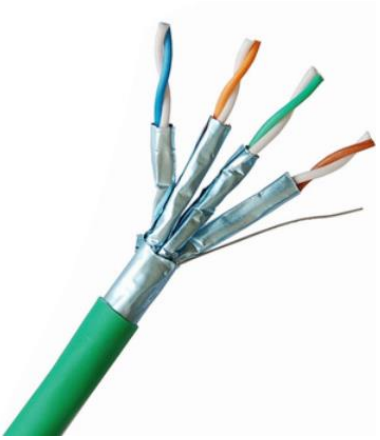
- ✓روکش‌دار یا STP (Shielded Twisted-pair)
- ✓بدون روکش یا UTP(Unshielded Twisted-pair)

این کابل از noiseهای مزاحم با استفاده از پیچیدگی‌هایی که دارد جلوگیری می‌کند، البته استاندارد ساخت این کابل‌ها برای کارخانه‌ها مهم است. اگر این کابل‌ها به‌درستی تابیده نشوند، به مشکل برمی‌خورند.

www.takbook.com

کابل روکش‌دار یا (STP)

این نوع کابل به هم تابیده شده، معمولاً توسط غلافی پوشیده می‌شوند تا در برابر امواج الکترومغناطیسی محافظت شوند. از آنجا که این غلاف‌ها فلزی هستند، می‌توانند نقش سیم ارت را نیز ایفا کنند، اما معمولاً این نوع کابل‌ها دارای رشته سیمی به همین منظور هستند که به آن، سیم تخلیه (drain wire) نیز می‌گویند، در شکل ۲۰-۱ این نوع کابل مشخص شده است.



شکل ۲۰-۱ ***STP Cable***

کابل کاملاً روکش‌دار یا SSTP (Screened Fully shielded Twisted Pair)

این کابل مانند کابل STP است، به‌طوری‌که به غیر از روکش‌های فلزی روی آن یک روکش فلزی دیگر، کل این روکش‌ها را دربرمی‌گیرد که این کابل را به نسبت قوی‌تر و محکم‌تر در برابر ضربه و امواج الکترومغناطیسی کرده است، در شکل ۲۱-۱ این نوع کابل مشخص شده است.

شکل ۲۱-۱ ***SSTP Cable***

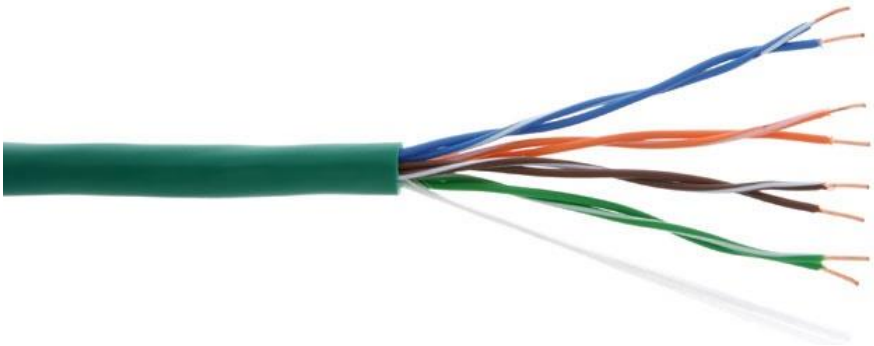
کابل‌های بدون روکش یا UTP (Unshielded Twisted-pair)

www.takbook.com

معمول‌ترین نوع کابل Twisted-pair، نوع بدون روکش آن است که مشخصه‌ی آن " 10 Base T " است که به‌عنوان یکی از محبوب‌ترین نوع کابل‌کشی برای شبکه‌ی LAN شناخته شد. این کابل‌ها در شبکه‌های امروزی استفاده می‌شود، مثلاً مودم ADSL شما از طریق همین کابل به کارت شبکه‌ی کامپیوتر شما متصل می‌شود.

شما می‌توانید این کابل‌ها را در سیستم‌های تلفن خانگی و اداره‌ی مخابرات مشاهده کنید که تمامی از این نوع کابل‌ها استفاده می‌کنند.

این نوع کابل‌ها، بسیار نازک و انعطاف‌پذیر است و به خاطر کوچک بودنشان برای سیم‌کشی به‌صرفه است، اما در برابر ضربه زیاد دوام ندارد، در شکل ۲۲-۱ این نوع کابل مشخص شده است.



شکل ۲۲-۱ ***UTP Cable***

کابل‌های UTP از انواع مختلف تشکیل‌شده‌اند، جدول ۲-۱، انواع کابل‌های UTP را نشان می‌دهد:

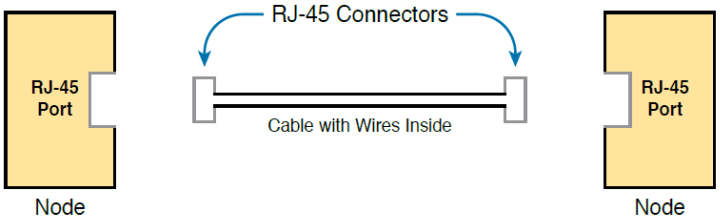
جدول ۳-۱ کابل‌های UTP

توضیحات	موارد استفاده	پهنای باند	نوع	طبقه‌بندی کابل
در توصیه‌های EIA / TIA شرح داده نشده است .برای سیستم های مدرن نامناسب است.	Telephone and modem lines	0.4 MHz		Level 1
در توصیه‌های EIA / TIA شرح داده نشده است .برای سیستم های مدرن نامناسب است.	Older terminal systems, e.g. IBM 3270	4 MHz		Level 2
در EIA / TIA-568 شرح داده شده است .برای سرعت‌های بالاتر از ۱۶ مگابیت در ثانیه نامناسب است و در حال حاضر عمدتاً برای کابل‌های تلفن مورد استفاده قرار می‌گیرد.	10BASE-T and 100BASE-T4 Ethernet	16 MHz	UTP	Cat3

www.takbook.com

Cat4	UTP	20 MHz	16 Mbit/sToken Ring	معمولاً مورد استفاده قرار نمی‌گیرد.
Cat5	UTP	100 MH	100BASE-TX & 1000BASE-T Ethernet	در اکثر شبکه‌های LAN مورد استفاده قرار می‌گیرد.
Cat5e	UTP	100 MHz	100BASE-TX & 1000BASE-T Ethernet	همان طراحی CAT5 است اما با سرعت و عملکرد بهتر از آن.
Cat6	UTP	250 MHz	10GBASE-T Ethernet	معمولاً کابل در فنلاند طبق استاندارد ۲۰۰۲ نصب شده است.
Cat6a		500 MHz	10GBASE-T Ethernet	ISO/IEC 11801:2002 Amendment 2.
Class F	S/FTP	600 MHz	Telephone, CCTV, 1000BASE-TX in the same cable. 10GBASE-T Ethernet.	Four pairs, S/FTP (shielded pairs, braid-screened cable). Development complete - ISO/IEC 11801 2nd Ed. Unofficially, Category 7 cable.
Class Fa		1000 MHz	Telephone, CATV, 1000BASE-TX in the same cable. 10GBASE-T Ethernet.	Four pairs, S/FTP (shielded pairs, braid-screened cable). Development complete - ISO/IEC 11801 2nd Ed. Am. 2. Unofficially, Category 7a cable.

در اکثر مواقع برای متصل شدن کلاینت‌ها به هم از این نوع کابل‌ها (Cat5, Cat5e, Cat6) استفاده می‌شود، در دو سر هر کابل یک کانکتور RJ45 نصب می‌شود و این کانکتور وارد کارت شبکه متصل به کلاینت می‌شود که در شکل ۲۳-۱ این موضوع را مشاهده می‌کنید.



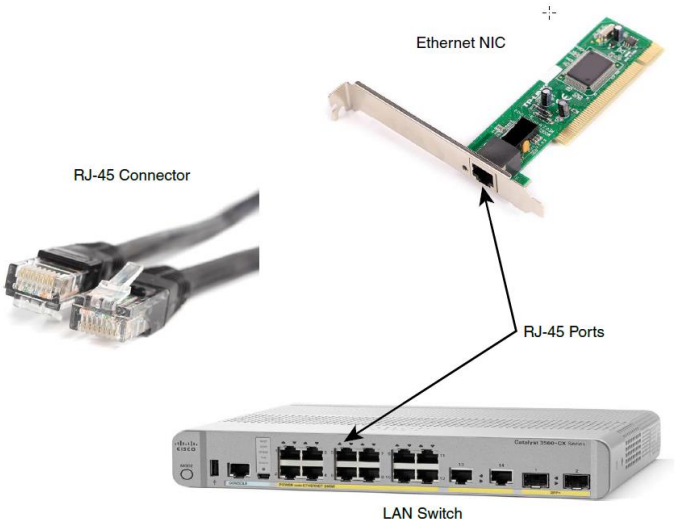
شکل ۲۳-۱ RJ-45 Connectors

کانکتورهای استاندارد برای کابل‌های UTP در شبکه‌های LAN به نام RJ45 هستند که در شکل ۲۴-۱ آن را مشاهده می‌کنید.

www.takbook.com

شکل ۲۴- ۱ *RJ-45 Connectors*

در شکل ۲۵-۱ کارت شبکه، سوئیچ و کابل RJ45 را مشاهده می‌کنید که نحوه ارتباط آنها مشخص شده است.



شکل ۲۵- ۱ *Connection*

سوکت زدن دو سر کابل با RJ45

برای اینکه بر روی کابل‌های UTP یا STP کانکتور RJ45 بزنیم باید به دو نوع کابل توجه کنیم که نحوه ارتباط آنها متفاوت است.

- ✓ **Straight** (به صورت مستقیم – برای دستگاه‌های غیرمشابه)
- ✓ **Cross** (برای به هم بستن دستگاه‌های شبیه به هم)

www.takbook.com

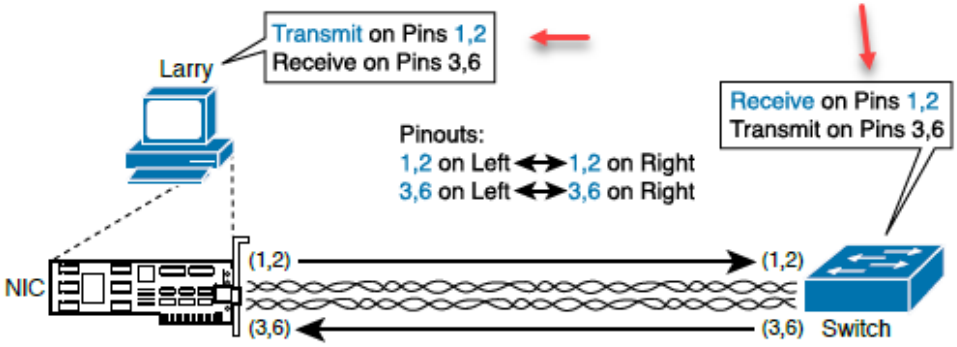
کابل Straight

این نوع کابل برای ارتباط دو وسیله‌ی غیرمشابه مانند سوئیچ و کامپیوتر استفاده می‌شود. باید دو سرکابل را به یک صورت ببندیم، یعنی رنگ‌بندی را تغییر ندهیم، این نوع کابل در آزمایشگاه تست شده و بدون مشکل کار خواهد کرد، در جدول ۳-۱، این موضوع را مشاهده می‌کنید.

جدول ۴-۱، ***Straight Cable***

کابل طرف سوئیچ		رنگ‌بندی	کابل طرف کامپیوتر	
سفید نارنجی	(+TD)	1 — 1	(+TD)	سفید نارنجی
نارنجی	(-TD)	2 — 2	(-TD)	نارنجی
سفید سبز	(+RD)	3 — 3	(+RD)	سفید سبز
آبی	(NC)	4 — 4	(NC)	آبی
سفید آبی	(NC)	5 — 5	(NC)	سفید آبی
سبز	(-RD)	6 — 6	(-RD)	سبز
سفید قهوه‌ای	(NC)	7 — 7	(NC)	سفید قهوه‌ای
قهوه‌ای	(NC)	8 — 8	(NC)	قهوه‌ای

اگر به شکل ۲۶-۱، توجه کنید متوجه ارتباط دو دستگاه سوئیچ و کلاینت خواهید شد، نحوه‌ی ارتباط این دو دستگاه به این صورت است که برای دریافت و ارسال اطلاعات از طریق کابل فقط از رشته‌های شماره‌ی 1,2,3,6 استفاده می‌کنند، به این صورت که مثلاً کلاینت برای ارسال اطلاعات از رشته‌ی 1,2 استفاده می‌کند و سوئیچ از 3,6 و همین‌طور برشکل آن برای دریافت انجام می‌شود.



شکل ۲۶- ۱ *Connection*

www.takbook.com

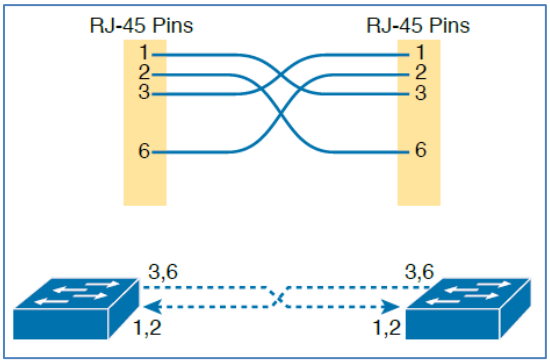
کابل Cross

برای ارتباط دو دستگاه شبیه به هم مثلاً برای ارتباط ۲ کامپیوتر باهم مورد استفاده قرار می‌گیرد، برای این کار باید یک سری تغییرات در هر دو طرف کابل انجام دهید. به جدول ۴-۱، توجه کنید.

جدول ۵-۱ ***Cable Cross***

کابل طرف PC2		رنگ‌بندی	کابل طرف PC1	
سفید سبز	(+TD)		(+TD)	سفید نارنجی
سبز	(−TD)		(−TD)	نارنجی
سفید نارنجی	(+RD)		(+RD)	سفید سبز
آبی	(NC)		(NC)	آبی
سفید آبی	(NC)		(NC)	سفید آبی
نارنجی	(−RD)		(−RD)	سبز
سفید قهوه‌ای	(NC)		(NC)	سفید قهوه‌ای
قهوه‌ای	(NC)		(NC)	قهوه‌ای

این رنگ‌ها در همه‌ی کابل‌ها ثابت است و یک استاندارد است که همه‌ی کارخانه‌های تولیدی، آن را پیروی می‌کنند. در شکل ۲۷-۱ طبق رنگبندی که در بالا مشاهده کردید، ارتباط کمی متفاوت است و پین شماره‌ی 1 به 3 و پین شماره‌ی 6 به 2 و برشکل متصل می‌شود که این موضوع نکته‌ی مهم این کار است.



شکل ۲۷ -۱ *Crossover Ethernet Cable*

در جدول ۶-۱، نحوه‌ی ارتباط دو دستگاه را از طریق کابل مربوطه مشاهده می‌کنید:

جدول ۶-۱ *Cable Connection*

کامپیوتر	روتر	سوئیچ	هاب	

www.takbook.com

هاب	Crossover	Crossover	Straight	Straight
سوئیچ	Crossover	Crossover	Straight	Straight
روتر	Straight	Straight	Crossover	Crossover
کامپیوتر	Straight	Straight	Crossover	Crossover

نکته: کامپیوترهایی که از یک برند کارت شبکه استفاده می‌کنند می‌توانند با کابل Straight هم به هم متصل شوند.

کابل Serial

این کابل‌ها برای ارتباط یک دستگاه، مانند روتر با روتر دیگر به کار می‌رود، که مدل آن RS232 است که فقط برای اتصالات کوتاه که حداکثر ۱۴ یا ۱۵ متر باشد کاربرد دارد، البته برای فواصل طولانی می‌توان از مدل RS485 استفاده کرد.

دو مفهوم کلی برای کابل‌های RS232 وجود دارد:

- ✓ DTE (Data Terminal Equipment)
- ✓ DCE (Data Communications Equipment)

DTEها از یک کانکتور ۹ پین یا ۲۵ پین که به این کانکتور مادگی می‌گویند تشکیل می‌شوند و طرف دیگر DTE هم به همین صورت است که از یک کانکتور ۹ پین یا ۲۵ پین استفاده می‌کند که به آن نرگی می‌گویندکه در شکل ۲۸-۱ هر دو پین ۹ و ۲۵ را مشاهده می‌کنید.

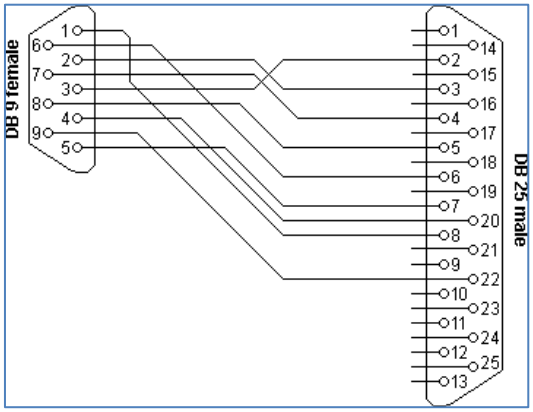
شکل ۲۸- ۱ DTE Serial Cable

تفاوت DCE با DTE

تفاوت این دو در این است که طرف کابلی که DTE است، مربوط به شبکه‌ی خودمان است و طرف دیگر که DCE است مربوط به مخابرات و یا همان Service Provider است که آن‌طرفی که DCE است، باید روی آن سرعت یا همان Clock Rate را تنظیم کند.

در شکل ۲۹-۱ نحوه‌ی بستن کابل‌های ۹ پین و ۲۵ پین را مشاهده می‌کنید.

www.takbook.com



شکل ۲۹- ۱ تفاوت DCE با DTE

کابل‌های سریال به انواع مختلفی تقسیم می‌شوند که در زیر انواع آن‌ها را مشاهده می‌کنید

کابل DTE Smart Serial

این نوع کابل برای ارتباط روترهای DTE استفاده می‌شود.

شکل ۳۰- ۱ DTE Smart Serial Cables

کابل DCE Smart Serial

این نوع کابل برای ارتباط روترهای DCE استفاده می‌شود.

www.takbook.com

شکل ۱-۳۱ *DCE Smart Serial Cables*

کابل E1

این کابل در شبکه‌های Wan بیشترین کاربرد را دارند.

شکل ۱-۳۲ *E1 Cable*

کابل Stacking

این نوع کابل‌ها برای ارتباط سوئیچ‌ها با هم مورد استفاده قرار می‌گیرند.

شکل ۱-۳۳ *Stacking Cable*

www.takbook.com

کابل Console

این نوع کابل که یک‌طرف آن از کانکتور RJ45 و در طرف دیگر از پورت COM استفاده می‌کند و همیشه هم به رنگ آبی است برای اتصال روتر یا سوئیچ به یک کامپیوتر برای تنظیم کردن روتر است. در درس‌های آینده، نحوه‌ی اتصال کامپیوتر به روتر از طریق این کابل بررسی می‌شود.

شکل ۳۴- ۱ Console Cable

کابل Octal

این کابل که برای اتصال مدارهای چندگانه استفاده می‌شود، از کیفیت بالایی برای انتقال اطلاعات برخوردار است.

شکل ۳۵- ۱ Octal Cable

www.takbook.com

۳-۲-۱ بررسی شبکه‌های Ethernet

در جدول ۷-۱، انواع مختلف Ethernet را مشاهده می‌کنید که هر کدام دارای ویژگی‌های مخصوص به خودشان هستند که حداکثر کارایی کابل در ستون Maximum Distance نوشته شده است، امروزه اکثر دستگاه‌ها دارای استاندارد 1000baseX هستند.

جدول ۷-۱، *Ethernet Cable*

Ethernet Standards (IEEE)	Data Rate	Cable Fiber Type	Maximum Distance (IEEE)
Ethernet (10Base-FL)	10 Mbps	50µm or 62.5µm Multimode @ 850nm	2km
Fast Ethernet (100Base-FX)	100 Mbps	50µm or 62.5µm Multimode @ 1300nm	2km
Fast Ethernet (100Base-SX)	100 Mbps	50µm or 62.5µm Multimode @ 850nm	300m
Gigabit Ethernet (1000Base-SX)	1000 Mbps	50µm Multimode @ 850nm	550m
Gigabit Ethernet (1000Base-SX)	1000 Mbps	62.5µm Multimode @ 850nm	220m
Gigabit Ethernet (1000Base-LX)	1000 Mbps	50µm or 62.5µm Multimode @ 1300nm	550m
Gigabit Ethernet (1000Base-LX)	1000 Mbps	9µm Singlemode @1310nm	5km
Gigabit Ethernet (1000Base-LH)	1000 Mbps	9µm Singlemode @1550nm	70km

بررسی 10Base-T

این نوع کابل دارای سرعت ۱۰ مگابایت بر ثانیه بوده که یکی از قدیمی‌ترین استانداردهای شبکه‌ای است و در حال حاضر از آن استفاده نمی‌شود، حرف T در این استاندارد به این معنا است که در این شبکه از کابل‌های UTP استفاده می‌شود که البته در حال حاضر منسوخ شده است.

بررسی 10Base-FL

این نوع از شبکه‌ها که از خانواده‌ی 10BaseT هستند دارای سرعت ۱۰ مگابایت هستند و برای کابل‌های فیبرنوری استفاده می‌شوند، تنها تفاوت آن با 10Base-T این است که می‌تواند تا دو کیلومتر داده‌ها را انتقال دهد که البته در حال حاضر این نوع شبکه‌ها دیگر مورد استفاده قرار نمی‌گیرد و سرعت آن به نسبت شبکه‌های امروزی بسیار کم است.

۴-۲-۱ بررسی شبکه‌ی Fast Ethernet

این استاندارد شبکه دارای سرعت ۱۰۰ مگابایت بر ثانیه بوده و چندین برابر شبکه‌ی قبلی سرعت آن افزایش پیدا کرده است، این استاندارد در شماره‌ی IEEE 802.3u تعریف شده است.

این استاندارد خود به سه قسمت تشکیل می‌شود که عبارت‌اند از 100Base-TX, 100Base-T4, 100Base-FX است.

استاندارد 100Base-TX

در استاندارد 100Base-TX که یک استاندارد عمومی و پرطرفدار است از کابل‌های UTP و STP در آن استفاده می‌شود و سرعت آن ۱۰۰مگابایت بر ثانیه است و حداکثر تا ۱۰۰ متر بهترین پاسخگویی را خواهد داشت.

www.takbook.com

استاندارد 100Base-FX

در استاندارد 100Base-FX از فیبر نوری استفاده می‌شود که حداکثر می‌تواند تا ۱۰ کیلومتر را پشتیبانی کند البته اگر از فیبرهای مخصوص آن استفاده کند.

استاندارد 100Base-T4

در استاندارد 100Base-T4 از کابل‌های UTP با استاندارد CAT 3,4,5 استفاده می‌شود و می‌تواند تا ۱۰۰ مگابایت را پشتیبانی کند، البته در حال حاضر مورد استفاده قرار نمی‌گیرد.

۵-۲-۱ بررسی شبکه‌ی Gigabit Ethernet

استفاده از سرورهای پیشرفته و استفاده از نرم‌افزارهای سنگین باعث شد که سرعت شبکه به صورت کل تغییر و افزایش پیدا کنید، در این استاندارد سرعت به ۱ گیگابایت بر ثانیه افزایش پیدا کرده و در حال حاضر اگر شما یک سیستم کلاینت خریداری کنید حداقل چیزی که دارد یک کارت شبکه‌ی Gigabit Ethernet است که سرعت بسیار بالایی را در شبکه دارا خواهد بود، البته این در صورتی اتفاق می‌افتد که سوئیچ مورد نظر هم از این سرعت پشتیبانی کند.

استاندارد 1000Base-X که خود شامل سه استاندارد 1000Base-SX, 1000Base-LX, 1000Base-CX است.

استاندارد 1000Base-CX که بر روی کابل‌های UTP و STP مورد استفاده قرار می‌گیرد، در شکل ۳۶ - ۱ یک کارت شبکه با تو پورت را مشاهده می‌کنید که دارای استاندارد 1000Base-X است.

شکل ۳۶- ۱ Gigabit Network Card

دو استاندارد 1000Base-SX, 1000Base-LX بر روی فیبر نوری پیاده‌سازی خواهد شد.

۶-۲-۱ فیبر نوری

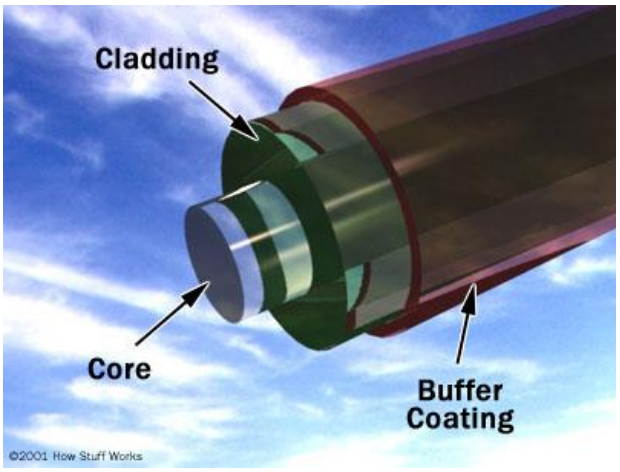
فیبرهای نوری تشکیل شده‌اند از یک استوانه‌ی شیشه‌ای بسیار نازک به نام هسته که توسط لایه‌ی ضخیم‌تر از شیشه پوشیده شده است که به این لایه، Cladding می‌گویند.

www.takbook.com

سرعت انتقال اطلاعات بر روی فیبر نوری، به خاطر استفاده از نور به‌جای سیگنال، خیلی سریع است.

فیبرهای نوری فقط یک‌طرفه هستند و امواج را از یک‌طرف ارسال می‌کنند، به همین دلیل در داخل آن از دو مسیر برای انتقال و دریافت استفاده می‌کنند.

یک فیبر نوری از سه بخش متفاوت تشکیل شده است:



شکل ۳۷- ۱ *Optical Cable*

هسته (Core): هسته‌ی نازک شیشه‌ای در مرکز فیبر که سیگنال‌های نوری در آن حرکت می‌نمایند.

روکش (Cladding): بخش خارجی فیبر بوده که دور تا دور هسته را دربرمی‌گیرد و باعث برگشت نور منشکل‌شده به هسته می‌گردد.

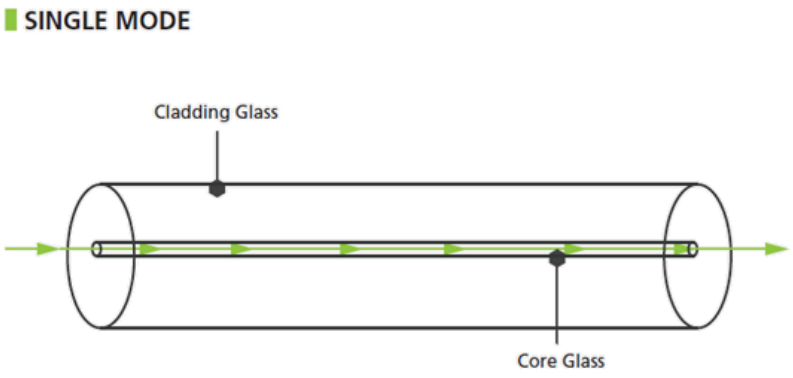
بافر رویه (Buffer Coating): روکش پلاستیکی که باعث حفاظت فیبر در مقابل رطوبت و سایر موارد آسیب‌پذیر است.

فیبرهای نوری در دو گروه عمده ارائه می‌گردند:

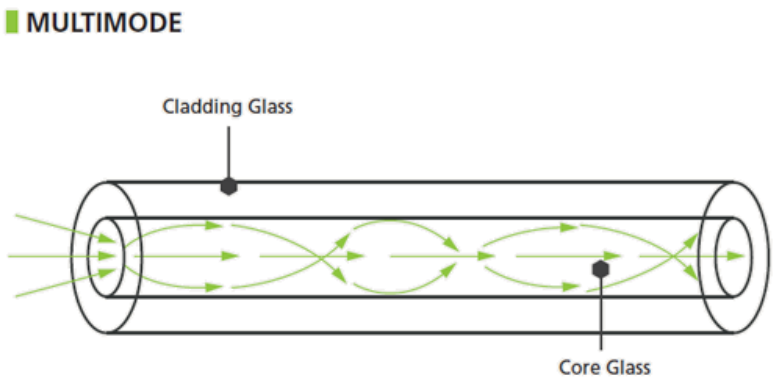
۱- فیبرهای تک‌حالته (Single-Mode)

۲- فیبرهای چندحالته (Multi-Mode)

www.takbook.com



شکل ۳۸- ۱ *Single Mode*



شکل ۳۹- ۱ *Multimode Mode*

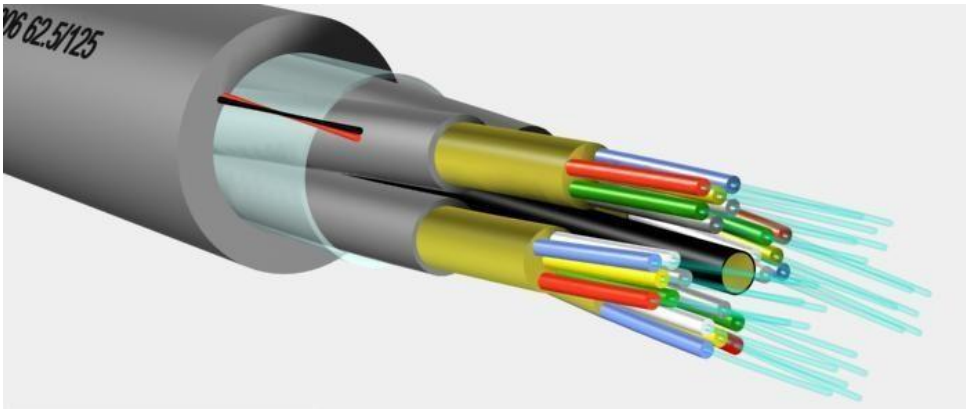
فیبر نوری به سه دسته کلی تقسیم می‌شود:

- ✓ Breakout
- ✓ Distribution
- ✓ Interconnect

۱-۶-۲-۱ فیبرهای نوری Breakout

این کابل امکان خیلی کمی برای خم کردن دارد و چون از تعداد زیاد فیبر تشکیل شده است، این کابل را برای ارتباط Datacenterها مناسب کرده است. از این کابل‌ها برای زیر دریاها و زیر خاک استفاده می‌شود، چون مقاومت آن به علت لایه‌های متعدد محافظتی بسیار زیاد است. در زیر، شکل این کابل را مشاهده می‌کنید.

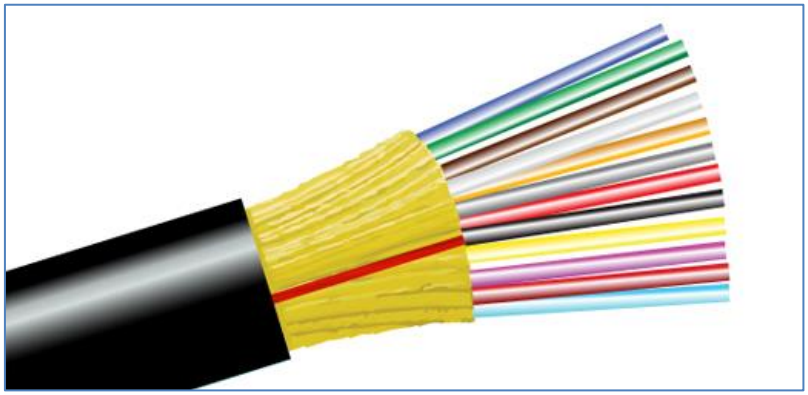
www.takbook.com



شکل ۴۰- ۱ *Breakout Cable*

۲-۶-۲-۱ فیبرهای نوری Distribution

این نوع کابل‌ها به نسبت کابل قبلی کمی خم می‌شوند و تعداد رشته‌ها در آن زیاد است و برای ارتباط کابل‌های Backbone با یک rack به کار می‌رود که شکل آن را می‌توانید مشاهده کنید.



شکل ۴۱- ۱ *Distribution Cable*

۳-۶-۲-۱ فیبرهای نوری Interconnect

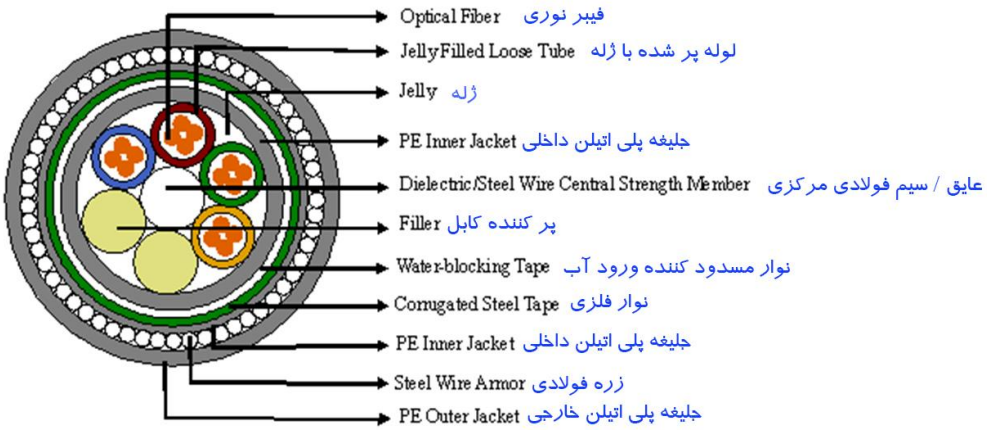
این نوع کابل که از یک پوشش پلاستیکی استفاده می‌کند، امکان خمش بالایی دارند و عموماً در داخل Rack استفاده می‌شود (Rack تجهیزاتی است که در داخل آن روتر، سوئیچ، فایروال و.... قرار می‌گیرد).

www.takbook.com

شکل ۴۲- ۱ *Interconnect Cable*

۴-۶-۲-۱ انواع لایه‌ها در فیبر نوری

فیبرهای نوری در درون خود از چندین لایه تشکیل شده‌اند که هرکدام از آن‌ها، کار خاصی را انجام می‌دهند.



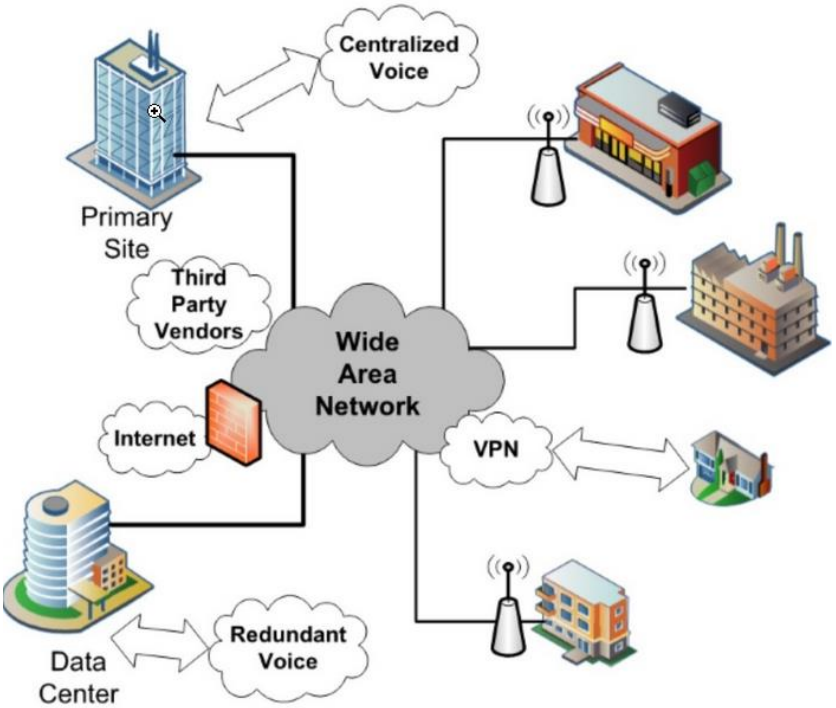
شکل ۴۳- ۱ *Optical Cable Layers*

همان‌طور که در شکل ۴۳-۱، مشاهده می‌کنید، انواع لایه‌های محافظ در این کابل وجود دارد که البته این کابل برای زیر دریاها و زیر خاک بسیار کاربرد دارد. ماده‌ی ژله‌ای که در این کابل وجود دارد، باعث می‌شود فیبر نوری داخل آن کمی متحرک باشد که اگر کمی خمیده شد، مشکلی برای آن پیش نیاید.

www.takbook.com

۱-۳ بررسی شبکه‌های WAN و IP Routing

شما به عنوان یک کاربر در یک سازمان در حال کار هستید و یک روز خاص که از شرکت دور هستید نیاز دارید به داده‌های آن شرکت دسترسی داشته باشید، با استفاده از لپ‌تاپ و از طریق اینترنت به شرکت خود متصل می‌شوید و داده‌های مورد نظر خود را به دست می‌آورید، به این نوع شبکه‌ها که به صورت گسترده و جغرافیایی در دسترس هستند شبکه‌های WAN گفته می‌شود.



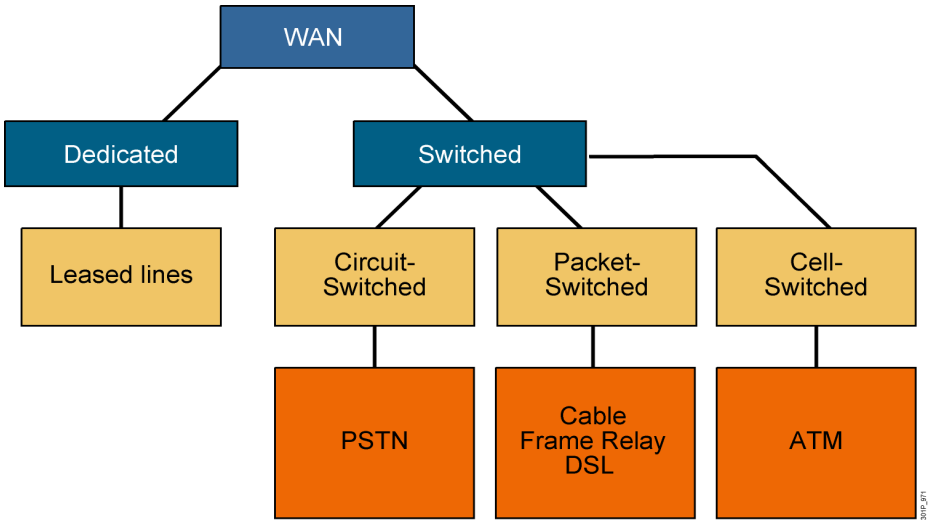
شکل ۴۵- ۱ WAN Networks

در این نوع شبکه‌ها برای پیاده‌سازی آن از خطوط استیجاری استفاده می‌شود که اصولاً در کشور ما این خطوط توسط مخابرات اجاره داده می‌شود که در حال حاضر قیمت آن بسیار گران شده است.

سرویس‌هایی که با آن‌ها می‌توانیم شبکه‌های خود را در نقاط مختلف به هم متصل کنیم و توسط مخابرات ارائه می‌شود، به شرح زیر است:

www.takbook.com

- Leased Line
- Circuit Switching
- Packet Switching
- Cell Switching
- Label Switching



شکل ۴۶- ۱ *WAN Services*

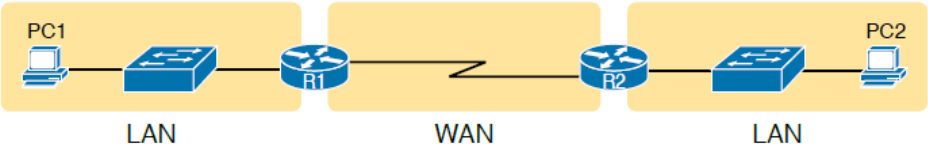
۱-۳-۱ خطوط استیجاری (Leased Line)

این خطوط که توسط مخابرات اجاره داده می‌شود، یک خطوط امن (Secure) محسوب می‌شود و مانند خط تلفن پایدار و ثابت است و پهنای باند آن حدود ۴۵ مگابایت است. برای استفاده از این خطوط باید شرایط زیر برقرار باشد:

- ✓ باید بدانید که مخابرات قابلیت اتصال خطوط استیجاری را در منطقه‌ی شما دارد.
- ✓ باید امکانات سخت‌افزاری و نرم‌افزاری فراهم شود.
- ✓ امنیت شبکه باید بالا باشد، به دلیل نفوذپذیری زیاد به شبکه.

در این نوع شبکه‌ها در هر شبکه‌ی LAN که قرار است به WAN (خط Leased Line) متصل شود از یک فایروال و روتر استفاده می‌کنند تا ارتباط این دو شبکه با هم برقرار شود، در شکل ۴۷-۱، یک شمای کلی از این شبکه را مشاهده می‌کنید.

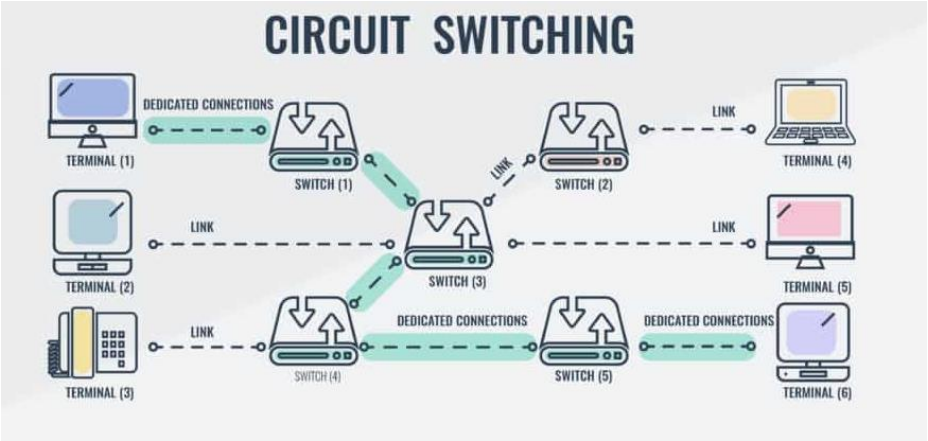
www.takbook.com



شکل ۴۷- ۱ نحوه‌ی ارتباط LAN و WAN

۱-۳-۱-۱ Circuit Switching

در این روش که ازخطوط تلفن و یا ISDN (Intergeated Service Digital Network) استفاده می‌کنند و دو مدار منطقی در هر دو طرف ایجاد شده و ارتباط برقرار می‌شود، اما مشکلی که این روش دارد، این است که در صورتی که هیچ‌گونه اطلاعاتی رد و بدل نشود باز هم خطوط اشغال است تا زمانی که هر دو طرف ارتباط را قطع کنند، مانند تلفن‌های خانگی.

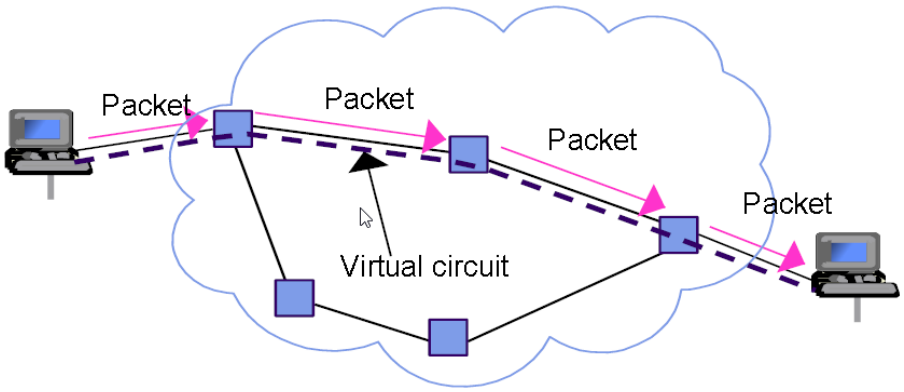


شکل ۴۸- ۱ Circuit Switching

۱-۳-۱-۲ Packet Switching

این سرویس، مانند سرویس مداری نیست که در هر دو طرف از مدار منطقی استفاده کنند، بلکه این سرویس اطلاعات دریافتی را به بسته‌های کوچک‌تر تقسیم می‌کند و به همراه اطلاعات دیگر به شبکه‌ی مورد نظر ارسال می‌کند، شبکه‌های Frame-relay و X.25 از این نوع می‌باشند.

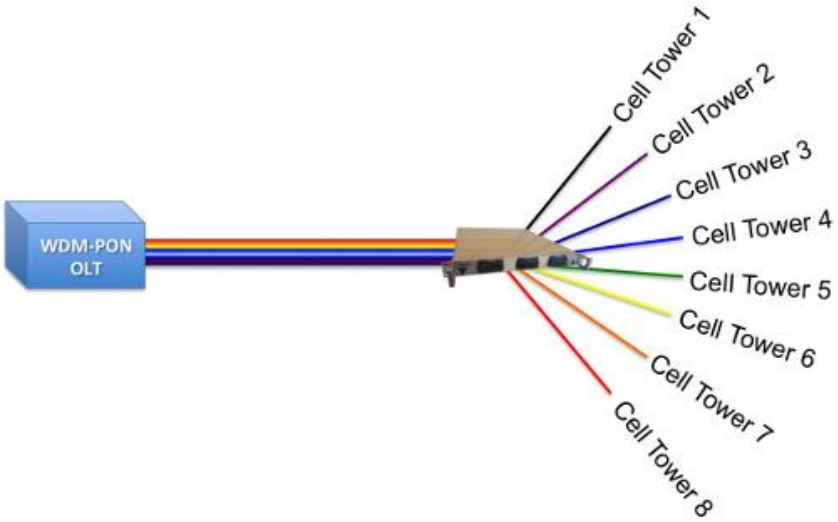
www.takbook.com



شکل ۱-۴۹ *Packet Switching*

۱-۳-۱-۳ Cell Switching

سلولی است شامل مسیر مورد نظر در شبکه که توسط سوئیچ این مسیر انتخاب می‌شود. این شبکه اغلب برای شبکه‌های با سرعت بالا، مانند ستون فقرات استفاده می‌شود؛ پهنای باند آن می‌تواند بین ۵۶ کیلوبایت تا چند گیگابایت باشد. این شبکه بیشتر برای صوت و تصویر استفاده می‌شود.

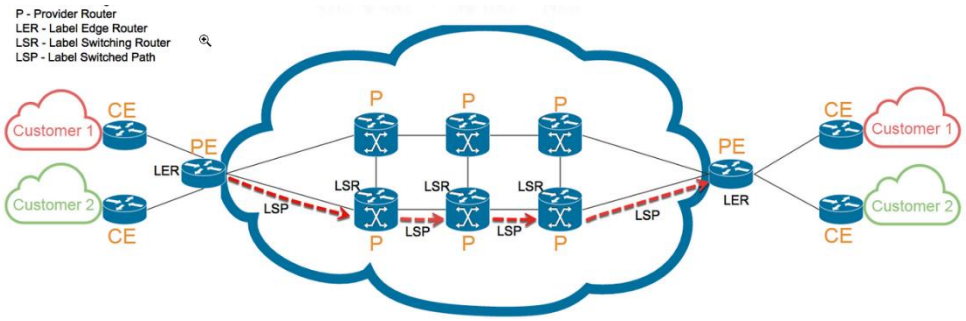


شکل ۱-۵۰ *Cell Switching*

۱-۳-۱-۴ Label Switching

www.takbook.com

در این روش که سریع‌ترین روش موجود است بر روی بسته‌ها برچسب‌گذاری و انتقال داده می‌شود. این روش در لایه‌ی ۲، یعنی لایه‌ی پیوند داده‌ها کار می‌کند. استفاده از برچسب‌گذاری و Multiport فن‌آوری‌های جدید در این زمینه هستند.



شکل ۱-۵۱ *Label Switching*

۲-۳-۱ بررسی پروتکل‌های Leased Line

پروتکل‌های مربوط به خطوط Leased به دو دسته تقسیم می‌شوند:

- ✓ **PPP**
- ✓ **HDLC**

۱-۲-۳-۱بررسی پروتکل PPP

این پروتکل که در یک ارتباط Point To Point کاربرد دارد دارای دو زیر لایه است:

Network Control Protocol یا NCP

این پروتکل وظیفه‌ی بسته‌بندی یا کپسوله کردن پروتکل‌های لایه‌ی Network، مانند IPX, IPv4, IPV6 را دارد.

Link Control Protocol یا LCP

وظیفه‌ی این پروتکل، کنترل برقراری ارتباط بین دو نقطه است. این زیر لایه دارای ویژگی‌های زیر است.

MultiLink

با این ویژگی، Interface که پروتکل PPP روی آن اجرا شده است، می‌تواند پکت‌ها را روی خط‌های مختلف Balance کند.

Error Detection

روشی برای کشف خطا و جلوگیری از Loop است.

Comperession

www.takbook.com

این روش که برای افزایش ظرفیت پروتکل ppp استفاده می‌شود، برای فشرده‌سازی و خارج کردن از حالت فشرده اطلاعات است.

برای اینکه یک ppp با خط دیگر ppp اتصال برقرار کند، نیازمند ۳ مرحله است:

Link Establishment

زمانی که بر روی یک اینترفیس، پروتکل PPP اجرا شده باشد، این پروتکل برای برقراری با اینترفیس مقابل خود یک درخواست ارسال می‌کند که این درخواست دربرگیرنده‌ی **Authentication**، **Comperession** و ... است.

Authentication

در این مرحله، دو متد برای برقراری ارتباط امنیتی استفاده می‌شوند:

PAP (Password Authentication Protocol**)**

این متد از نظر امنیتی، زیاد در سطح بالایی قرار ندارد، آن‌هم به خاطر Clear Text بودن آن است. این متد زمانی استفاده می‌شود که نیاز به امنیت بین دو خط PPP داشته باشیم.

CHAP (Challenge Handshake Authentication Protocol**)**

این متد بسیار پیچیده و با امنیت بسیار بالا نسبت به PAP عمل می‌کند. این متد در سه مرحله کار خود را انجام می‌دهد، در مرحله‌ی اول، روتر درخواست‌کننده‌ی ارتباط یک Challenge Message به روتر مقابل خود ارسال می‌کند، روتر مقابل هم با دریافت پیام روی آن عملیات MD5 را انجام می‌دهد و با یک Response Message به روتر مقابل ارسال می‌کند. در این مرحله، روتر ارسال‌کننده اطلاعات اولیه، پسورد خود را توسط MD5 تبدیل به مقدار مورد نظر می‌کند و این مقدار را با مقدار دریافتی از روتر روبرو مقایسه می‌کند، در صورت تأیید آن، ارتباط برقرار خواهد شد.

۲-۲-۳-۱ بررسی پروتکل HDLC

HDLC مانند پروتکل PPP یک پروتکل برای Encapsulation است که بر روی خطوط استیجاری فعال می‌شود و در لایه دو کار می‌کند.

HDLC در دو نسخه پیاده‌سازی شده است، یکی از نسخه‌ها مختص سیسکو است و به صورت تخصصی برای محصولات سیسکو طراحی شده است.

نسخه‌ی دوم آن که یک نسخه عمومی است که در تمام دستگاه‌های شبکه مورد استفاده قرار می‌گیرد.

در شکل ۵۲-۱ هر دو نسخه پروتکل HDLC را مشاهده می‌کنید که در نسخه Cisco گزینه‌ی Protocol اضافه شده است.

www.takbook.com

شکل ۵۲- ۱ Prtotocole HDLC

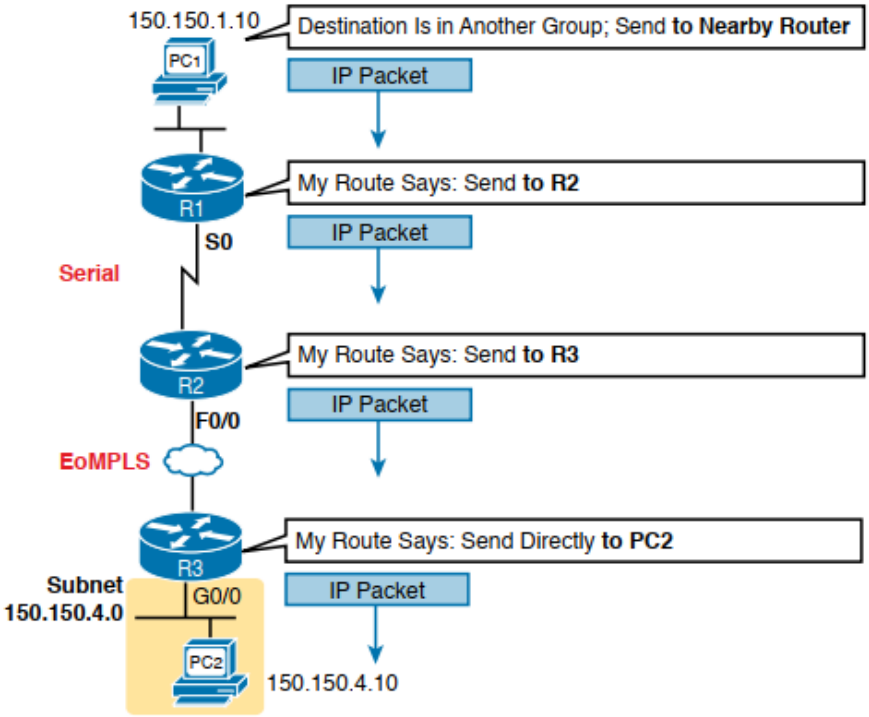
۳-۳-۱ بررسی IP Routing

پروتکل‌های زیادی در طی این چند سال وجود داشته که برای مصارف خاصی استفاده شده ولی در این میان پروتکل TCP/IP بیشترین انعطاف‌پذیری از خود نشان داده است.

TCP/IP به دو پروتکل IPV4 , IPV6 تقسیم می‌شود که پروتکل IP version 4 (IPv4) نسخه‌ی چهار آن است که در حال حاضر بیشترین کاربرد را درشبکه در کل جهان دارد و ورژن IP version 6 (IPv6) که نسخه‌ی جدید آن است و در حال حاضر در حال گسترش در سیستم‌های جهان است، این نسخه از IP از امنیت ویژه‌ای برخوردار است ولی یادگیری آن به نظر می‌رسد سختر باشد.

در شکل ۵۳-۱ یک شکل کلی از کلاینت‌ها و روترها را مشاهده می‌کنید که کلاینت‌ها برای استفاده از IP Packetها از نرم‌افزارهای خاصی در سیستم‌عامل خود استفاده می‌کنند تا از طریق روترها بتوانند بسته را به کلاینت دیگر در شبکه‌ی دیگر برسانند.

www.takbook.com



شکل ۵۳- ۱ *Prtotocole HDLC*

۴-۱ سوالات فصل اول

1.Which of the following protocols are examples of TCP/IP transport layer protocols?
(Choose two answers.)

کدام یک از پروتکل‌های زیر نمونه‌ای از پروتکل‌های لایه‌ی حمل و نقل TCP/IP هستند؟(دو پاسخ را انتخاب کنید)

a. Ethernet
b. HTTP
c. IP
d. UDP
e. SMTP
f. TCP

www.takbook.com

2. Which of the following protocols are examples of TCP/IP data-link layer protocols? (Choose two answers.)

کدام یک از پروتکل‌های زیر نمونه‌ای از پروتکل‌های لایه‌ی پیوند داده TCP/IP هستند؟(دو پاسخ را انتخاب کنید)

a. Ethernet
b. HTTP
c. IP
d. UDP
e. SMTP
f. TCP
g. PPP

3. The process of HTTP asking TCP to send some data and making sure that it is received correctly is an example of what?

فرایندHTTP از TCP درخواست می‌کند که برخی داده‌ها را ارسال کندو از دریافت آن اطمینان حاصل پیدا کند، به کدام یک از گزینه‌ها نزدیکتر است.

a. Same-layer interaction
b. Adjacent-layer interaction
c. OSI model
d. All of these answers are correct.

4. The process of TCP on one computer marking a TCP segment as segment 1, and the receiving computer then acknowledging the receipt of TCP segment 1 is an example of what?

فرآیندی که در آن یک کامپیوتر یک قطعه TCPرا به عنوان بخش ۱ علامت‌گذاری می‌کند و در روبرو سیستم گیرنده پس از تایید، بخش ۱ TCP را می‌پذیرد به کدام گزینه نزدیکتر است؟

a. Data encapsulation
b. Same-layer interaction
c. Adjacent-layer interaction
d. OSI model
e. All of these answers are correct.

5. The process of a web server adding a TCP header to the contents of a web page, followed by adding an IP header and then adding a data-link header and trailer, is an example of what?

روند کار وب سرور که در آن یک هدر TCP به محتویات یک صفحه اضافه می‌شود و به دنبال آن اضافه کردن هدر IP و سپس اضافه کردن یک هدر Data Link و Trailer به کدام گزینه اشاره دارد؟

a. Data encapsulation
b. Same-layer interaction
c. OSI model
d. All of these answers are correct.

6. Which of the following terms is used specifically to identify the entity created when encapsulating data inside data-link layer headers and trailers?

کدام یک از اصلاحات زیر به طور خاص مربوط به شناسایی موجودیت ایجاد شده هنگام استفاده از کپسوله کردن داده‌ها در هدرها و تریلرهای لایه پیوند داده است؟

a. Data
b. Chunk

www.takbook.com

c. Segment
d. Frame
e. Packet

7. Which OSI encapsulation term can be used instead of the term frame?
از کدام اصطلاح می‌توان به جای Frame استفاده کرد؟

a. Layer 1 PDU
b. Layer 2 PDU
c. Layer 3 PDU
d. Layer 5 PDU
e. Layer 7 PDU

8. Which OSI layer defines the standards for cabling and connectors?
کدام لایه‌ی مدل OSI استانداردهای کابل‌کشی و اتصلات را مشخص می‌کند؟

a. Layer 1
b. Layer 2
c. Layer 3
d. Layer 4
e. Layer 5, 6, or 7

9. Which of the following terms are not valid terms for the names of the seven OSI layers? (Choose two answers.)
کدام یک از اصطلاحات زیر نام مناسبی برای هفت لایه‌ی مدل OSI نیست؟ (دو مورد را انتخاب کنید)

a. Application
b. Data link
c. Transmission
d. Presentation
e. Internet
f. Session

10. How do TCP and UDP differ in the way that they establish a connection between two endpoints?
نحوه ارتباط TCP و UDP برای ارتباط بین دو نقطه‌ی پایانی به چه صورت است؟

a. TCP uses the three-way handshake, and UDP does not guarantee message delivery.
b. TCP uses synchronization packets, and UDP uses acknowledgement packets.
c. UDP provides reliable message transfer, and TCP is a connectionless protocol.
d. UDP uses SYN, SYN ACK, and FIN bits in the frame header while TCP uses SYN, SYN ACK,and ACK bits.

www.takbook.com

www.takbook.com

www.takbook.com

فصل دوم

پیاده‌سازی شبکه‌های Ethernet

در این فصل به مهارت‌های مورد نیاز برای راه‌اندازی اولیه دستگاه‌های سیسکو می‌پردازیم.
یک مهندس شبکه برای راه‌اندازی یک شبکه‌ی Ehernet باید با برنامه‌ریزی عمل کند تا در آینده با مشکلی مواجه نشود، این برنامه‌ریزی می‌تواند شامل موارد زیر باشد:

۱. ایجاد طرح کامل از شبکه‌ی سازمان مورد نظر
۲. خرید سوئیچ و ادوات مورد نیاز.
۳. نصب کابل‌ها و ارتباط آن در طبقات.
٤. پیکربندی سوئیچ‌ها و دستگاه‌های مورد نظر شبکه.
٥. و...

امتحان CCNA مهارت‌های لازم برای مهندس شبکه را برای راه‌اندازی و مدیریت دستگاه‌ها، آموزش می‌دهد، اولین مهارت شما قبل از یادگیری باید این باشد که قوانین کار با دستگاه‌ها را بدانید.
مهمترین ویژگی‌های این فصل این است که مطالب آن برای امتحانات بسیار مهم است و باید بسیار خوب در یادگیری آن تلاش کنید.

۲-۱ بررسی دستگاه‌های شبکه

۲-۱-۱ روترها

روترها، دستگاه‌هایی هستند که کار تفکیک شبکه‌ها را انجام می‌دهند و به عنوان یک پل ارتباطی بین دو شبکه مختلف انجام وظیفه می‌کنند. روترها در لایه‌ی ۳ مدل osi کار می‌کنند و با IP ها سر و کار دارند و بسته‌های اطلاعاتی را از یک شبکه به شبکه‌ی دیگر حمل می‌کنند، البته این عمل را از طریق پروتکل‌های مسیریابی انجام می‌دهند که در درس‌های آینده به آن‌ها می‌پردازیم.
یکی از مهم‌ترین کاربردهای روترها جلوگیری از Broadcast است. مسیریاب‌ها با استفاده از پروتکل-های مسیریابی، بهترین مسیر را در شبکه پیدا کرده و از آن مسیر، برای ارتباط با شبکه‌ی دیگر استفاده می‌کنند، در شکل ۲-۱ دستگاه روتر سیسکو را مشاهده می‌کنید.

www.takbook.com

شکل ۱- ۲ روتر سیسکو

یک مسیریاب شبکه از دو بخش عمده سخت‌افزار و نرم‌افزار تشکیل می‌شود. نرم‌افزار مسیریاب شامل سیستم عامل و رابط کاربری است. سیستم عامل معروفی که شرکت سیسکو در مسیریاب‌های خود استفاده می‌کند، IOS نام دارد.

اجزای زیر را برای یک مسیریاب می‌توان نام برد:

- بدنه (شامل کانکتورها و...)
- سخت‌افزار مسیریابی
- رابط‌های شبکه
- سیستم‌عامل
- رابط کاربری

تولیدکنندگان معروف روترها و دستگاه‌های شبکه:

- ✓ Juniper Networks
- ✓ Cisco Systems, Inc
- ✓ Lucent Technologies (Alcatel-Lucent)
- ✓ MRV Communications
- ✓ Mikrotik RouterOS

۲-۱-۲ هاب‌ها

هاب ازجمله تجهیزات سخت‌افزاری است که از آن به منظور برپاسازی شبکه‌های کامپیوتری استفاده می‌شود. گرچه در اکثر شبکه‌هایی که امروزه ایجاد می‌گردد از سوئیچ در مقابل هاب استفاده می‌شود، اما ما همچنان شاهد استفاده از این نوع تجهیزات سخت‌افزاری در شبکه‌های متعددی هستیم.

www.takbook.com

در شکل ۲-۲ دستگاه هاب را مشاهده می‌کنید.

شکل ۲-۲ هاب

به چند موضوع باید در این نوع دستگاه‌ها دقت کرد که عبارت‌اند از:

Domain: تمامی کامپیوترهای عضو یک domain (دامنه)، هر اتفاق و یا رویدادی را که در دامنه اتفاق می‌افتد، مشاهده کرده و یا خواهند شنید.

Collision Domain: در صورت بروز یک تصادف (Collision) بین دو کامپیوتر، سایر کامپیوترهای موجود در domain آن را شنیده و آگاهی‌های لازم در خصوص آن چیزی که اتفاق افتاده است را پیدا خواهند کرد. تمامی کامپیوترهایی که با استفاده از هاب به یکدیگر متصل می‌شوند، عضو یک Collision Domain یکسان خواهند بود (برخلاف سوئیچ).

Broadcast Domain: در این نوع domain، یک پیام broadcast (یک فریم و یا داده که برای تمامی کامپیوترها ارسال می‌گردد) برای هر یک از کامپیوترهای موجود در domain ارسال می‌گردد.

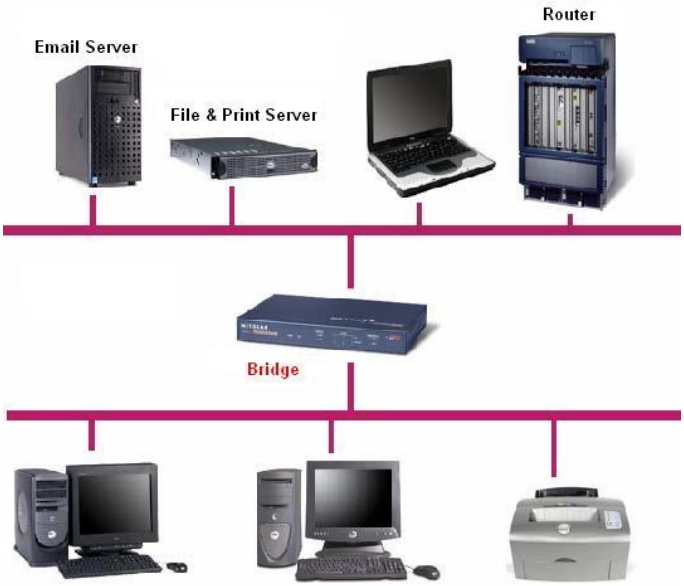
توجه داشته باشید، امروز دستگاه‌هایی که به هاب معروف هستند تغییرات گسترده‌ای کرده و به مانند شکل ۳-۲ از یک هاب برای ارتباط چند مانیتور، کابل شبکه، فلش دیسک و ... استفاده می‌شود که می‌تواند دید خاصی به شما بدهد، چون در جامعه امروز کمتر کسی یا کمتر سازمانی را پیدا می‌کنید که از هاب برای شبکه استفاده کند.

www.takbook.com

شکل ۳- ۲ هاب جدید

۳-۱-۲ پل (Bridge)

شبیه به سوئیچ است، با این تفاوت که از ۲ یا ۴ پورت تشکیل شده است و با آدرس Mac مربوط به دستگاه‌ها کار می‌کند و مانند سوئیچ، دارای جدول برای نگهداری Mac address های شبکه است و برای ارتباط با شبکه‌های Bus استفاده می‌شود، که در شکل ۴-۲ این موضوع را مشاهده می‌کنید.



شکل ۴- ۲ دستگاه Bridge

www.takbook.com

۴-۱-۲ سوئیچ‌ها

سوئیچ برای اتصال دستگاه‌های مختلف از قبیل رایانه، مسیریاب، چاپگرهای تحت شبکه، دوربین‌های مداربسته و ... در شبکه‌های کابلی مورد استفاده قرار می‌گیرد.

از نظرظاهری، سوئیچ همانند جعبه‌ای است متشکل از چندین درگاه Ethernet که از این لحاظ شبیه به هاب (Hub) است، با وجود این‌که هر دوی این‌ها وظیفه‌ی برقراری ارتباط بین دستگاه‌های مختلف را بر عهده دارند، تفاوت از آنجا آغاز می‌شود که هاب، بسته‌های ارسالی از طرف یک دستگاه را به همه‌ی درگاه‌های خود ارسال می‌کند و کلیه‌ی دستگاه‌های دیگر، علاوه بر دستگاه مقصد، این بسته‌ها را دریافت می‌کنند، درحالی‌که در سوئیچ، ارتباطی مستقیم بین درگاه دستگاه مبدأ با درگاه دستگاه مقصد، برقرار شده و بسته‌ها به‌طور مستقیم فقط برای آن ارسال می‌شوند.

این خصوصیت از آنجا می‌آید که سوئیچ می‌تواند بسته‌ها را پردازش کند، در سوئیچ‌های معمولی که به سوئیچ لایه‌ی دوم معروف‌اند، این پردازش تا لایه‌ی دوم مدل OSI پیش می‌رود و نتیجه‌ی این پردازش، جدولی است که در سوئیچ، با خواندن آدرس سخت‌افزاری (MAC) فرستنده‌ی بسته و ثبت Interface ورودی تشکیل می‌شود.

سوئیچ با رجوع به این جدول، عملیات آدرس‌دهی بسته‌ها در لایه‌ی دوم را انجام می‌دهد، بدین معنا که این جدول مشخص می‌کند بسته‌ی ورودی می‌بایست فقط برای درگاه بخصوص ارسال شود.

در شبکه‌های بزرگ Switchها جدول‌های خود را به اشتراک می‌گذارند تا هرکدام بدانند چه دستگاهی به کدام سوئیچ متصل است و با این کار ترافیک کمتری در شبکه ایجاد کنند، در شکل ۲-۵ دستگاه سوئیچ را مشاهده می‌کنید.

شکل ۵- ۲ دستگاه سوئیچ

www.takbook.com

سوئیچ به طور معمول در لایه‌ی دوم مدل OSI کار می‌کند، ولی سوئیچ‌هایی با قابلیت کارکرد در لایه‌ی سوم هم وجود دارد. پرکاربردترین سوئیچ در بین لایه‌های مختلف به‌جز لایه‌ی دوم می‌توان به سوئیچ لایه‌ی سه اشاره کرد که در بسیاری موارد جایگزین مناسبی برای روترها هستند. از سوئیچ می‌توان در یک شبکه‌ی خانگی کوچک تا شبکه‌های بزرگ با Backboneهای چند گیگابایتی استفاده کرد.

مزیت‌ها و قابلیت‌های سوئیچ

- امکان برقراری ارتباط بین چندین دستگاه را به طور مستقیم و هوشمند به ما می‌دهد.
- امکان برقرار ارتباط با سرعت بسیار بالا را فراهم می‌کند.
- امکان نظارت و مدیریت بر عملکرد کاربران را فراهم می‌کند.
- امکان کنترل پهنای باند مصرفی کاربران را فراهم می‌کند.
- امکان تفکیک شبکه به بخش‌های کوچکتر و مشخص کردن نحوه‌ی دسترسی افراد به قسمت‌های مختلف را فراهم می‌کند.

سوئیچ‌ها در انواع مختلف ۸ ، ۱۶ ،۲۴ ،۴۸ پورت وجود دارد. در شکل ۶-۲ یک سوئیچ ۲۹۵۰ مشاهده می‌کنید که دارای ۲۴ پورت است که ۲۴ پورت آن دارای سرعت ۱۰/۱۰۰/۱۰۰۰ هستند و دو پورت آن هم که اصولاً دارای بیشترین سرعت هستند برای ارتباط با دیگر سوئیچ‌ها در یک سازمان مورد استفاده قرار می‌گیرند.

شکل ۶- ۲ سوئیچ ۲۹۵۰ سیسکو

سوئیچ‌ها در دو نوع لایه‌ی ۲ و ۳ قرار دارند، سوئیچ‌های لایه‌ی ۲ سوئیچ‌های معمولی هستند که در بالا باهم بررسی کردیم، اما سوئیچ‌های لایه‌ی ۳ توانایی کار روتر را هم دارند و عملیات روتینگ که در آینده باهم بررسی می‌کنیم را می‌توانند انجام دهند و می‌توان تمام پروتکل‌های Routing را روی این سوئیچ‌ها اجرا کرد. در شکل ۷-۲، سوئیچ 3560 شرکت سیسکو را مشاهده می‌کنید، این سوئیچ یک سوئیچ لایه‌ی ۳ است.

شکل ۷- ۲ سوئیچ ۳۵۶۰ سیسکو

www.takbook.com

۲-۲ بررسی سیستم‌عامل IOS شرکت سیسکو

IOS مخفف کلمه‌ی Internetwork operation cisco است که سیستم‌عامل دستگاه‌هایی مانند روتر و سوئیچ است و کنترل آن از طریق خط فرمان یا همان CLI امکان‌پذیر است. ios هم در این دستگاه‌ها اطلاعات را ذخیره، بازیابی، آدرس‌دهی و ... می‌کند که مانند یک سیستم عامل ویندوز کار می‌کند اما گرافیکی نیست. Ios در انواع مختلفی وجود دارد که در حال حاضر، آخرین ورژن آن (۱۳۹۹/۰۲/۱) IOS 15.5 است.

۲-۲-۱ مراحل روشن شدن دستگاه‌های سیسکو

روتر یا سوئیچ از زمانی که روشن می‌شوند تا زمانی که آماده به کار می‌شوند، از ۷ مرحله عبور می‌کند:

۱. روشن شدن و چک کردن سخت‌افزارهای خود که به آن مرحله‌ی post هم می‌گویند.
۲. بارگذاری فایل boot starp.
۳. پیدا کردن مسیر ios که به‌طور پیش‌فرض روی Flash است.
٤. فایل ios روی Ram اجرا می‌شود.
٥. پیدا کردن تنظیمات ذخیره‌شده.
٦. انتقال تنظیمات Startup config از Nvram به Ram.
۷. اجرا کردن تنظیمات از روی Ram.

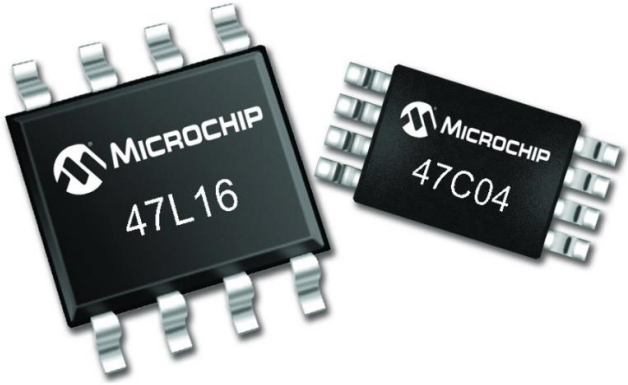
اصولاً روترها از حافظه‌های Rom , Ram , Nvram , Flash تشکیل‌شده‌اند که هرکدام از مراحل بالا با این حافظه‌ها کار می‌کنند.

حافظه‌ی Rom

حافظه‌ای در دل روتر که فقط خواندنی است و قسمت‌های زیر در آن وجود دارد:

- ✓ Boot starp
- ✓ Post
- ✓ Rom Monitor
- ✓ Mini Ios

www.takbook.com



شکل ۸- ۲ حافظه‌ی ROM

- **Boot starp**

این قسمت زمانی که اجرا شود، محل قرارگیری ios را پیدا می‌کند که همان‌طور در مراحل ۷ گانه مشاهده می‌کنید، در مرحله‌ی دوم این فایل اجرا می‌شود و محل IOS را پیدا می‌کند.

- **POST**

این مرحله همان مرحله تست سخت‌افزار است که در مرحله ۱ برای شما معرفی کردیم.

- **Rom Monitor**

بیشترین کاربرد این قسمت در Password Recovery است که با تغییر در رجیستری می‌توانیم Password قرار داده‌شده روی روتر را پاک کنیم.

- **Mini IOS**

این قسمت زمانی اجرا می‌شود که روتر نتواند iOS اصلی را پیدا کند.

حافظه‌ی Ram

یک حافظه‌ی فرّار که با قطع شدن برق، اطلاعات آن پاک‌شده و ذخیره نمی‌شوند، از بین مراحل هفت‌گانه همان‌طور که اشاره کردیم در مرحله‌ی ۴، IOS بر روی Ram اجرا می‌شود،

www.takbook.com

یعنی اینکه فایل IOS به‌صورت فشرده است که از حالت فشرده، خارج شده و روی Ram قرار می‌گیرد و اجرا می‌شود.

شکل ۹- ۲ حافظه‌ی RAM

حافظه Flash

این حافظه، مانند یک هارد دیسک روی روتر است که یک حافظه‌ی دائمی است و اطلاعات ios در آن قرار دارد، در شکل ۱۰-۲، یک Flash disk ، ۶۴ مگابایت شرکت سیسکو را مشاهده می‌کنید که به صورت ماژول بر روی دستگاه‌های روتر و سوئیچ و.... قرار می‌گیرد.

شکل ۱۰- ۲ حافظه‌ی FLASH

حافظه‌ی Nvram

حافظه‌ی دائمی روتر برای ذخیره‌سازی تنظیمات روتر در آن است که زمانی که کاری روی روتر انجام دادیم برای ذخیره باید اطلاعات Ram را به Nvram با دستور خاصی کپی کنیم تا با خاموش شدن روتر و یا سوئیچ، تنظیمات از دست نرود که این تنظیمات می‌تواند آدرس یک اینترفیس یا یک پروتکل برای روتر باشد.

www.takbook.com

شکل ۱۱- ۲ حافظه‌ی Nvram

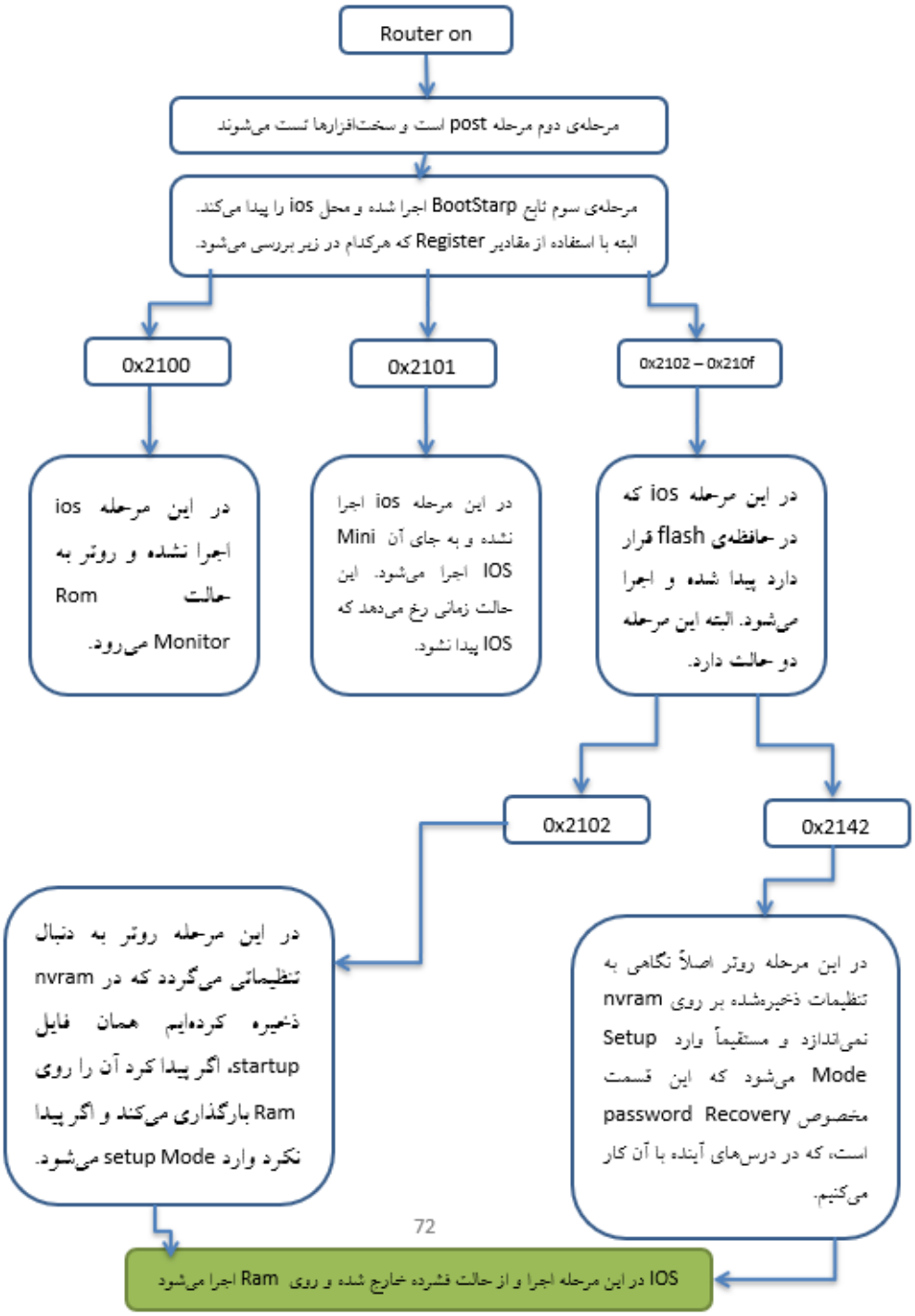
تا به اینجا با روشن شدن یک روتر چندین کار انجام شد که باهم بررسی کردیم. روترها در موقع بوت شدن از چندین کد رجیستری استفاده می‌کنند که هرکدام به مفهوم یک مسیر خاص است.

Configuration register

یک سری اعداد که مسیر اجراشدن روتر را تعیین می‌کنند که برای به دست آوردن این اعداد باید در روتر و خط فرمان از دستور Show Version استفاده کنند.

در شکل ۱۲-۲ کاملاً با این مبحث آشنا خواهید شد.

www.takbook.com



شکل ۱۲-۲ مراحل اجرای IOS سیسکو

www.takbook.com

۲-۲-۲ کار با خط فرمان در دستگاه‌های سیسکو

دستگاه‌های شرکت سیسکو مانند سوئیچ و روتر از طریق خط فرمان یا همان command-line interface (CLI) تنظیم و کنترل می‌شوند، یک مهندس شبکه با وورد به صفحه‌ی VLI با وارد کردن دستورات مشخص که در ادامه یاد میگیرم به دستگاه مورد نظر می‌فهماند که چه کاری باید انجام دهد.

روش‌هایی دیگری هم برای کنترل دستگاه‌های سیسکو وجود دارد، مثلاً می‌توانید از یک سرویس تحت وب برای کنترل آنها استفاده کنید و یا اینکه از نرم‌افزارهای مشخصی که سیسکو برای این کار طراحی کرده استفاده کنید.

۲-۲-۳ نحوه دسترسی به خط فرمان CISCO IOS

برای دسترسی به خط فرمان دستگاه‌های سیسکو، باید از طریق کابل عمل کنید، یعنی اینکه برای اولین بار یک دستگاه را خریداری می‌کنید باید از طریق کابل‌هایی که درون بسته‌ی آن وجود دارد از طریق لپ‌تاپ یا سیستم دیگر به آن متصل شوید.

به مانند شکل ۱۳-۲ اگر به سوئیچ‌ها و روترهای جدید دقت کرده باشید در جلو و یا پشت آنها دو پورت آبی رنگ با عنوان CONSOLE را مشاهده می‌کنید که برای تنظیم اولیه دستگاه باید از آنها استفاده کرد.

شکل ۱۳-۲ پورت کنسول

اگر به تصویر ۱۴-۲ توجه کنید، کابل آبی رنگ کنسول را مشاهده می‌کنید که یک طرف آن پورت RJ45 است و باید به روتر متصل شود و طرف دیگر آن، پورت Com است که باید به سیستم شما متصل شود و از طریق نرم‌افزار خاصی به دستگاه متصل شوید.

www.takbook.com

شکل ۱۴- ۲ پورت و کابل کنسول

اصولاً پورت COM در سیستم‌های جدید و مخصوصاً لپ‌تاپ‌ها وجود ندارد و برای اینکه بتوانیم به روتر یا سوئیچ متصل شویم باید از کابل USB یا تبدیل مخصوص آن استفاده کرد، در شکل ۱۵-۲ یک کابل USB را مشاهده می‌کنید که طرف بزرگتر را به لپ‌تاپ یا سیستم خود متصل می‌کنید و طرف دیگر را به دستگاه روتر یا سوئیچ.

نکته: زمانی که از این نوع کابل استفاده می‌کنید باید نرم‌افزار و یا درایور مربوط به دستگاه مورد نظر را روی سیستم مورد نظر نصب کنید.

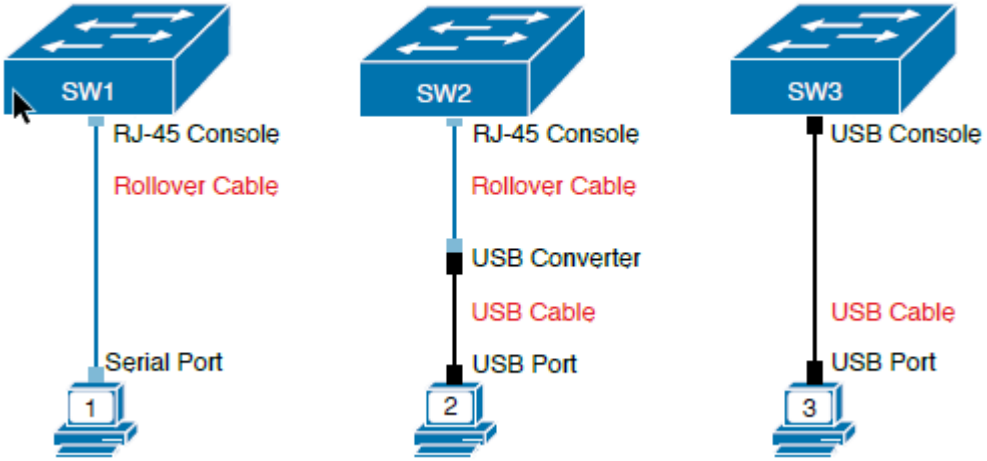
شکل ۱۵- ۲ پورت کنسول USB

اگر چنانچه روتر یا سوئیچ مورد نظر از کابل USB پشتیبانی نمی‌کند و مجبور هستید از کابل Com به RJ45 استفاده کنید می‌توانید برای متصل کردن این کابل به لپ‌تاپ خود از یک مبدیل به مانند شکل ۱۶-۲ استفاده کنید، که این مبدل یک طرفش به پورت USB لپ‌تاپ و طرف دیگر به کابل COM متصل خواهد شد.

www.takbook.com

شکل ۱۶- ۲ پورت COM

در شکل ۱۷-۲ نحوه‌ی اتصال در هر سه روش مشخص شده است.



شکل ۱۷- ۲ نحوه‌ی ارتباط پورت کنسول

بعد از اینکه توانستیم به صورت سخت‌افزاری کابل را به روتر و لپ‌تاپ یا سیستم خود متصل کنیم حالا باید نرم‌افزار مورد نظر را اجرا کنیم و به محیط CLI آن دستگاه متصل شویم.

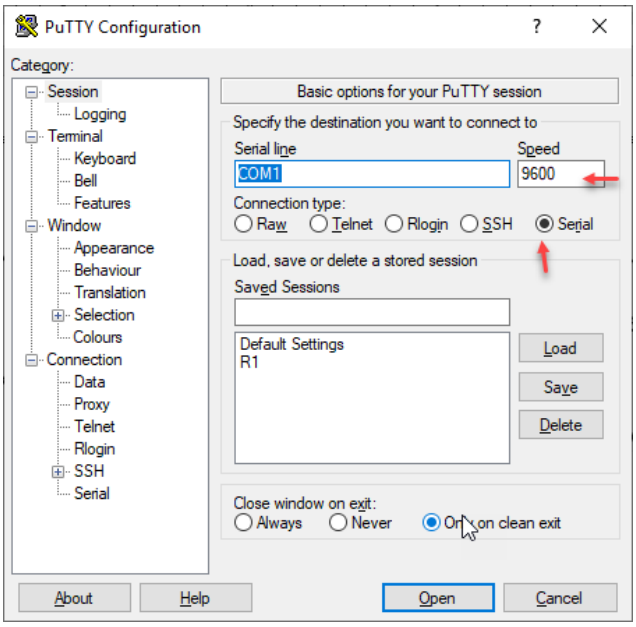
نرم‌افزارهای زیادی برای این کار وجود دارد که می‌توان به SecureCRT، Putty و... اشاره کرد، برای اینکه با عملکرد آنها آشنا شویم نرم‌افزار Putty را از لینک زیر دانلود و اجرا کنید:

https://www.chiark.greenend.org.uk/~sgtatham/putty/latest.html

در شکل ۱۸-۲ نرم‌افزار Putty را مشاهده می‌کنید که دارای چندین گزینه برای برقراری ارتباط با دستگاه‌های مختلف است.

www.takbook.com

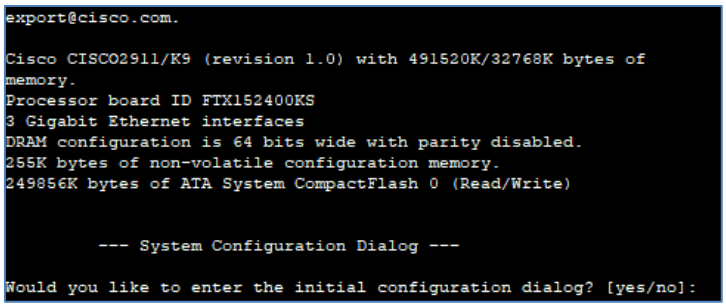
برای متصل شدن به یک سوئیچ یا روتر خام باید پورت Serial را به مانند شکل ۱۸-۲، انتخاب کنید و سرعت پیش‌فرض آن را همان 9600 در نظر بگیرید و بر روی OK کلیک کنید با این کار اگر ارتباط سخت‌افزاری برقرار باشد، این نرم‌افزار به روتر یا سوئیچ متصل خواهد شد.



شکل ۱۸- ۲ نرم‌افزار Putty

بعد از برقراری ارتباط صفحه‌ای به مانند شکل ۱۹-۲، مشاهده خواهید کرد که برای شروع کار از شما سوال می‌کند که آیا مایل هستید برای انجام تنظیمات وارد شوید که باید کلمه Yes را برای آن وارد کنید تا سوالات دیگر از شما پرسیده شود.

شاید شما در منزل یا محل کار خود دستگاه‌های سیسکو در اختیار نداشته باشید و برای اینکه بتوانید با سوئیچ یا روتر کار کنید بهتر است به صورت مجازی و با برنامه‌ی خاصی که برای این کار طراحی شده کار کنید که در ادامه آن را بررسی می‌کنیم.



شکل ۱۹- ۲ ارتباط از طریق پورت COM

www.takbook.com

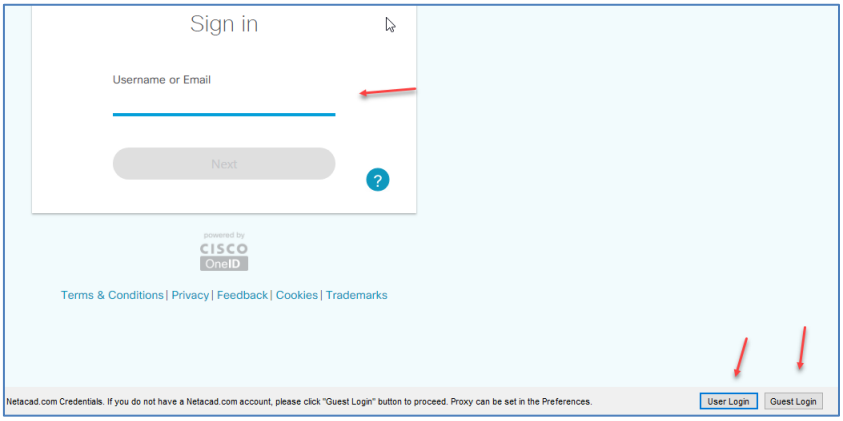
۳-۲ کار با نرم‌افزار Packet Tracer

این نرم‌افزار یکی از بهترین نرم‌افزارهای مجازی‌سازی برای دوره‌ی CCNA بوده و توسط شرکت سیسکو برای دوره‌های درسی که اجرا می‌کند طراحی و پیاده‌سازی شده است، این نرم‌افزار برای دانشجویان دوره‌های درسی مختلف سیسکو کارآمد خواهد بود تا بتوانند از طریق آن به دستگاه‌ها، کابل‌ها و... دست پیدا کنند و یک آزمایشگاه شخصی و مجازی برای خود راه‌اندازی کنند.

برای دانلود این نرم‌افزار می‌توانید از سایت آن یعنی netacad.com استفاده کنید و یا اینکه از سایت‌های داخلی این کار را انجام دهید.

بعد از دانلود، نرم‌افزار را بر روی سیستم خود نصب کنید که مراحل نصب آن ساده بوده و نیاز به توضیح بیشتر ندارد.

اولین صفحه‌ای که بعد از اجرای نرم‌افزار مشاهده می‌کنید شکل ۲۰-۲ است که باید برای ورود به نرم‌افزار یک اکانت در سایت سیسکو داشته باشید تا بتوانید وارد نرم‌افزار شوید، اما ساخت اکانت با محدودیت‌هایی که سیسکو برای ایرانیان گذاشته کمی اذیت کننده است و باید از دکمه‌ی Guest Login برای وورد استفاده کنید که بعد از کلیک بر روی آن باید ۱۵ ثانیه صبر کنید تا وارد نرم‌افزار شوید ولی این گزینه محدودیت‌هایی را به همراه دارد که مقدار زمانی بر روی نرم‌افزار کار کنید مشخص می‌شود.

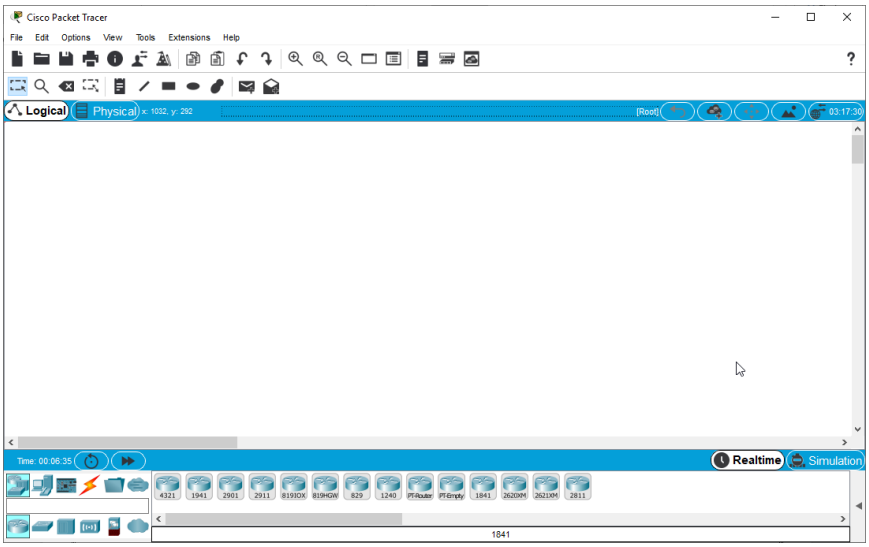


شکل ۲۰-۲ ایجاد اکانت Packet Tracer

یکی از روش‌هایی که بتوانید این پنجره را غیر فعال کنید استفاده از فایل‌های کرکی است که آن را غیرفعال می‌کند و با یک جستجو در اینترنت می‌توانید ورژن مورد نظر خود را پیدا کنید، راه دیگر این است که در فایروال دسترسی این نرم‌افزار را به اینترنت ببندید که با این کار صفحه Login باز می‌شود و بعد از چند ثانیه به صورت اتوماتیک بسته خواهد شد.

www.takbook.com

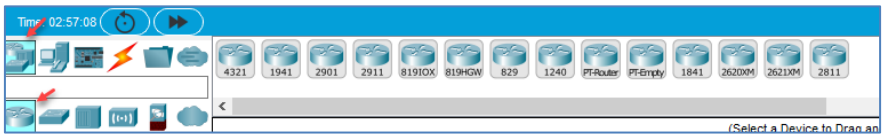
همانطور که در شکل ۲۱-۲ مشاهده می‌کنید نرم‌افزار به درستی اجرا شده است و برای کار آماده است.



شکل ۲۱- ۲ نرم‌افزار Packet Tracer

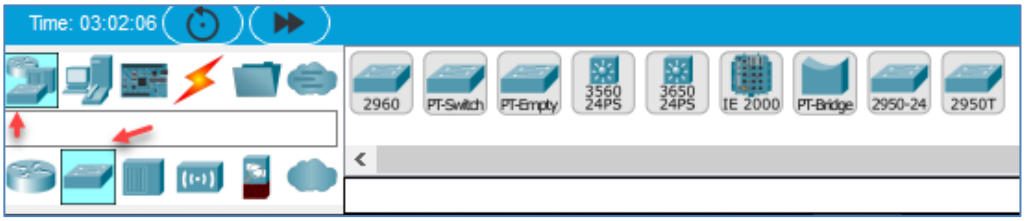
این نرم‌افزار از انواع روترها، سوئیچ‌ها، کابل‌ها، دستگاه‌های بی‌سیم و ... تشکیل شده است که یک دنیای مجازی را برای ما ایجاد می‌کند.

برای مشاهده‌ی لیست روترها در سمت چپ مطابق شکل ۲۲-۲ اول بر روی Network Devices کلیک و بعد بر روی روتر کلیک کنید تا لیست روترهای این نرم‌افزار را به شما نشان دهد.



شکل ۲۲- ۲ ابزار Packet Tracer

در قسمت سوئیچ‌ها هم می‌توانید از چندین مدل مختلف برای سناریو خود استفاده کنید.

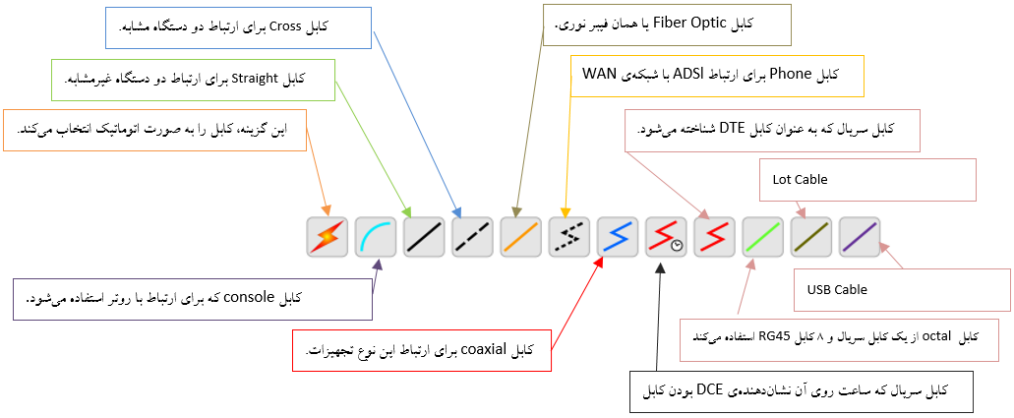


شکل ۲۳- ۲ ابزار Packet Tracer

www.takbook.com

همین‌طور می‌توانید بر روی Hub , Wireless Device , End Device , WAN کلیک کنید و لیست همه‌ی آن‌ها را مشاهده کنید. برای مشاهده لیست کابل‌ها بر روی آیکون کلیک کنید تا لیست کابل‌ها مطابق شکل ۲۴-۲ ظاهر شود.

همان‌طور که مشاهده می‌کنید، انواع کابل در این قسمت وجود دارد، که این کابل‌ها را در درس‌های

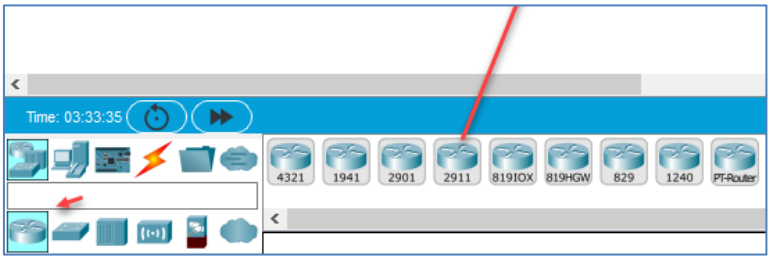


شکل ۲۴- ۲ کابل‌های Packet Tracer

قبلی توضیح دادیم.

برای اینکه با این نرم‌افزار کار کنیم یک روتر را به لیست اضافه می‌کنیم و از طریق یک سیستم یا لپ‌تاپ و از طریق کابل Console به آن متصل می‌شویم تا تنظیمات اولیه آن را انجام دهیم.

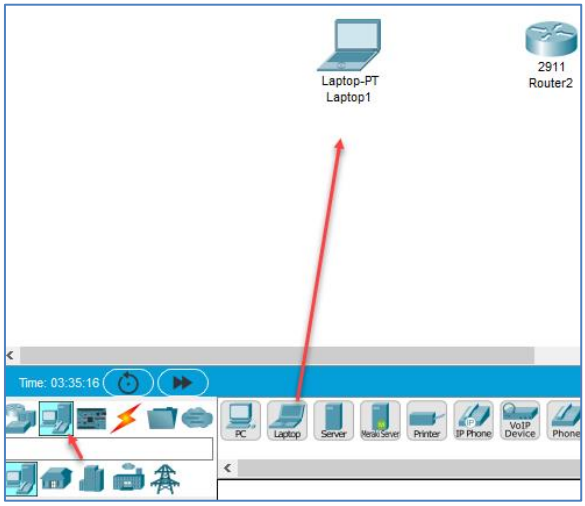
از قسمت پایین نرم‌افزار Packet Tracer ، طبق شکل ۲۵-۲ از سمت چپ بر روی Router کلیک کنید و یک روتر 2911 را انتخاب و به صفحه کار اضافه کنید.



شکل ۲۵-۲ روتر ۲۹۱۱

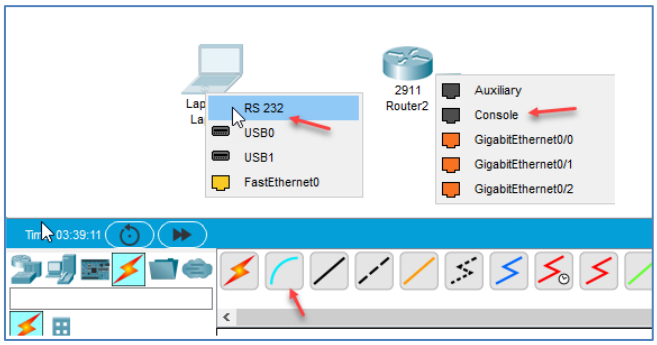
بعداز این کار به مانند شکل ۲۶-۲ یک کامپیوتر را از قسمت End Device انتخاب و به صفحه اضافه کنید.

www.takbook.com



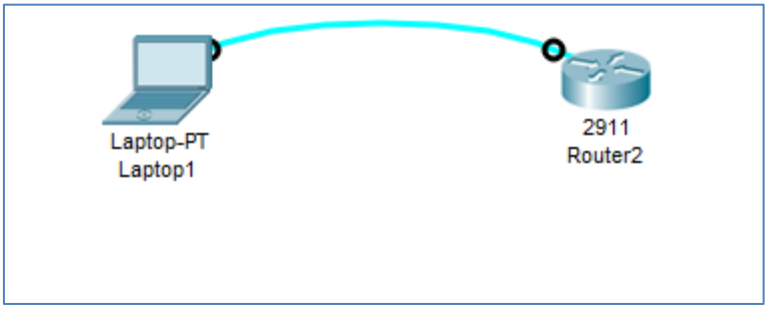
شکل ۲۶-۲ کلاینت

در ادامه از قسمت کابل‌ها باید کابل Console که رنگ آن آبی است را انتخاب و به مانند شکل ۲۷-۲ از پورت RS 232 مربوط به سیستم به پورت Console متصل کنید.



شکل ۲۷-۲ ارتباط از طریق پورت کنسول

شکل ۲۸-۲ ارتباط نهایی را نشان می‌دهد، بعد از متصل شدن کابل، بر روی لپ‌تاپ دوبار کلیک کنید.

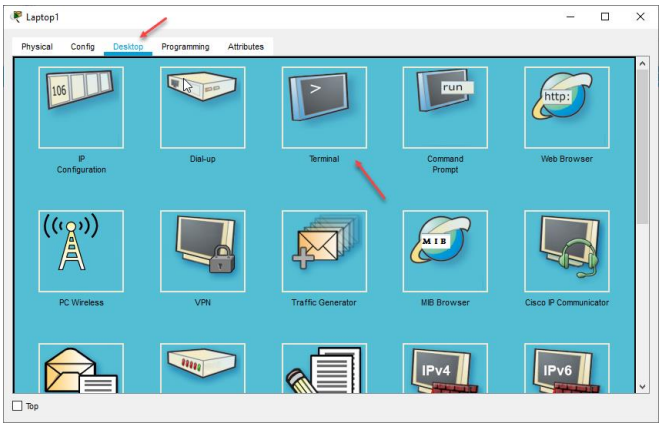


شکل ۲۸-۲ ارتباط از طریق پورت کنسول

www.takbook.com

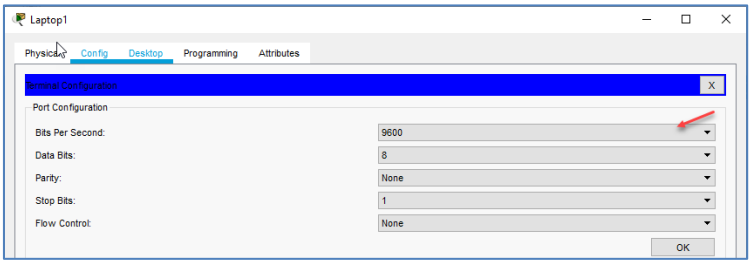
برای وارد شدن به تنظیمات روتر باید از طریق نرم‌افزار Terminal کامپیوتر، این کار را انجام دهید، از تب Desktop گزینه‌ی Terminal را انتخاب کنید.

در شکل ۲۹-۲ وارد تب Desktop شوید و بر روی Terminal کلیک کنید.



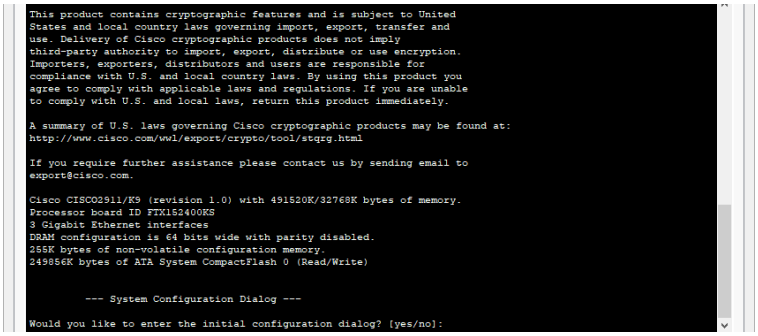
شکل ۲۹-۲ تنظیمات لپ‌تاپ

در شکل ۳۰-۲ باید سرعت ارتباطی را که به صورت پیش‌فرض ۹۶۰۰ است را تغییر دهید ولی این سرعت پیش‌فرض بدون مشکل کار خواهد کرد، پس بر روی OK کلیک کنید.



شکل ۳۰-۲ تنظیمات لپ‌تاپ

با کلیک بر روی OK شکل ۳۱-۲ باز خواهد شد و سوالات پیش‌فرض مطرح خواهد شد و با استفاده از این سوالات می‌توانید دستگاه مورد نظر را تنظیم کنید.



شکل ۳۱-۲ تنظیمات لپ‌تاپ

www.takbook.com

۲-۴ پیکربندی اولیه IOS

در روتر دو نوع پیکربندی وجود دارد:

۱- Setup Mode

۲- Command Line Interface

بررسی Setup Mode

این قسمت اکثراً زمانی به شما نمایش داده می‌شود که هیچ‌گونه تنظیماتی روی روتر در Nvram ذخیره نشده باشد، مثلاً در قسمت قبل که روتر را از طریق کابل console اجرا کردیم، وارد قسمت Setup Mode شده است.

اولین صفحه‌ای که بعد از متصل شدن از طریق کابل Console مشاهده می‌کنید شکل ۲-۳۲ است که از شما برای انجام تنظیمات اولیه درخواست ورود کلمه‌ی Yes می‌کند.

```
Terminal

This product contains cryptographic features and is subject to United
States and local country laws governing import, export, transfer and
use. Delivery of Cisco cryptographic products does not imply
third-party authority to import, export, distribute or use encryption.
Importers, exporters, distributors and users are responsible for
compliance with U.S. and local country laws. By using this product you
agree to comply with applicable laws and regulations. If you are unable
to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to
export@cisco.com.

Cisco CISCO2911/K9 (revision 1.0) with 491520K/32768K bytes of memory.
Processor board ID FTX152400KS
3 Gigabit Ethernet interfaces
DRAM configuration is 64 bits wide with parity disabled.
255K bytes of non-volatile configuration memory.
249856K bytes of ATA System CompactFlash 0 (Read/Write)


         --- System Configuration Dialog ---

Would you like to enter the initial configuration dialog? [yes/no]: yes
```

شکل ۲-۳۲ *Setup Mode*

در شکل ۲-۳۳ از شما پرسیده می‌شود که آیا مایل به تنظیم قسمت‌های مدیریتی روتر هستید؟ که با کلیک بر روی Yes سوالات متعدد دیگری از شما پرسیده خواهد شد که در صفحه‌ی بعد بررسی می‌کنیم.

www.takbook.com


```
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to
export@cisco.com.

Cisco CISCO2911/K9 (revision 1.0) with 491520K/32768K bytes of memory.
Processor board ID FTX152400KS
3 Gigabit Ethernet interfaces
DRAM configuration is 64 bits wide with parity disabled.
255K bytes of non-volatile configuration memory.
249856K bytes of ATA System CompactFlash 0 (Read/Write)


         --- System Configuration Dialog ---

Would you like to enter the initial configuration dialog? [yes/no]: yes

At any point you may enter a question mark '?' for help.
Use ctrl-c to abort configuration dialog at any prompt.
Default settings are in square brackets '[]'.


Basic management setup configures only enough connectivity
for management of the system, extended setup will ask you
to configure each interface on the system

Would you like to enter basic management setup? [yes/no]: Yes
```

Setup Mode شکل ۲-۳۳

نکته: دستوراتی که در این قسمت (Setup Mode) اجرا می‌شوند برای کسانی که برای اولین بار با روتر کار می‌کنند کمی نا آشنا خواهد بود ولی در مبحث بعدی به صورت کلی آنها را فرا خواهیم گرفت.

در سؤال اول از شما نام دستگاه پرسیده می‌شود که شما می‌توانید یک اسم دلخواه وارد کنید.

Enter host name [Router]: R1

در سؤال بعدی از شما رمز عبور درخواست می‌شود، این رمز به صورت Secret است و قابل‌شناسایی برای هرکسی نیست و Hash شده است.

Enter enable secret: cisco

در این قسمت رمز عبور دیگری از شما پرسیده می‌شود که برتری آن کمتر از رمز عبور قبلی است و تا زمانی که رمز عبور قبلی فعال است این رمز کاربردی ندارد.

Enter enable password: ciscoR1

در این قسمت از شما رمز عبور مربوط به پورت ترمینال پرسیده می‌شود که آن را وارد کنید.

Enter virtual terminal password: FR122

این قسمت مربوط به تنظیمات SNMP است که فقط بر روی enter کلیک کنید تا از این قسمت خارج شوید.

Configure SNMP Network Management? [no]:

بعداز اجرای دستور آخر لیست Interfaceهای روتر را نشان می‌دهد.

Current interface summary

Interface	IP-Address	OK?	Method	Status	Protocol
GigabitEthernet0/0	unassigned	YES	manual	administratively down	down

www.takbook.com


```
GigabitEthernet0/1    unassigned    YES manual administratively down down
GigabitEthernet0/2    unassigned    YES manual administratively down down
Vlan1                 unassigned    YES manual administratively down down
```

در این قسمت نام یکی از اینترفیس‌ها را نوشته و بر روی enter کلیک کنید.

Enter interface name used to connect to the

management network from the above interface summary:**GigabitEthernet0/2**

اگر می‌خواهید این Interface را آدرس‌دهی کنید yes را وارد و enter کنید.

Configure IP on this interface? [yes]: **yes**

در این قسمت ip address را وارد و Enter کنید.

IP address for this interface: **192.168.1.1**

در این قسمت از شما subnet Mask مربوط به IP بالا درخواست می‌شود، وارد کنید و بعد enter.

Subnet mask for this interface [255.255.255.0] : **255.255.255.0**

در آخر کار به شما تمام تنظیمات را که انجام داده‌اید، نمایش می‌دهد. و اعلام می‌کند که آیا می‌خواهید تنظیمات را در Nvram ذخیره کنید که با انتخاب گزینه‌ی ۲ این اطلاعات در Nvram ذخیره می‌شود و بعد از خاموش و روشن شدن روتر اطلاعات در حافظه باقی می‌ماند.

The following configuration command script was created:

```
!
hostname r1
enable secret 5 $1$mERr$Wmdu8FSDG1wNa1xa4SQGi.
enable password 21
line vty 0 4
password 2
!
interface Vlan1
shutdown
no ip address
!
interface GigabitEthernet0/0
no shutdown
ip address 192.168.1.1 255.255.255.0
!
interface GigabitEthernet0/1
shutdown
no ip address
!
interface GigabitEthernet0/2
shutdown
```

www.takbook.com


```
no ip address
!
end

[0] Go to the IOS command prompt without saving this config.
[1] Return back to the setup without saving this config.
[2] Save this configuration to nvram and exit.

Enter your selection [2]:
```

بررسی Command Line Interface

اگر در قسمت قبل به جای ورود به قسمت Setup Mode از no استفاده کنید وارد مد Cli یا Command Line Interface می‌شوید که این مد، همان مدی است که ما با آن کار می‌کنیم، در این مد امکانات فوق‌العاده‌ای می‌توانیم داشته باشید و اگر حرفه‌ای شوید، کارهای زیادی می‌توانید روی روتر خود انجام دهید که در ادامه به همه‌ی این مسائل پی خواهیم برد.

۵-۲ کار با مدهای CLI در روتر

Cli از دو مد برای ورود تنظیمات خود استفاده می‌کند.

- ✓ User Mode
- ✓ Privileged Mode

در IOS این مدها برای این تعریف شده‌اند که مثلاً اگر کاربری وارد مد User شود، چقدر توانایی برای کنترل روتر یا سوئیچ دارد و یا اگر وارد مد Privileged شود، چقدر توانایی دارد، که هرکدام را در اینجا مورد بررسی قرار می‌دهیم.

User Mode

این مد، یکی از پائین‌ترین مدها ازنظر سطح دسترسی کاربران به تنظیمات روتر است، حداکثر کاری که یک کاربر می‌تواند در این مد انجام دهد، انجام Monitoring است و به دلیل دستورات کمی که در این مد اجرا می‌شود، سطح دسترسی آن در پائین‌ترین سطح قرار دارد.

Privileged Mode

این مد به نسبت مد قبلی از دسترسی بالاتری برخوردار است و رتبه‌ی آن کمی بالاتر است، چون در این مد، تنظیمات روتر می‌تواند چک شود.

www.takbook.com

حالا می‌خواهیم به صورت واقعی این مدها را در روتر تست کنیم. در نرم‌افزار Packet Tracer روتر را اجرا کنید و در قسمتی که از شما سؤال می‌کند که وارد مد Setup شود کلمه‌ی No را تایپ و بعد، Enter کنید، اولین خطی که بعدازآن می‌بینید، خط زیر است:

```
Router>
```

به نگارش آن توجه کنید این همان قسمت است که به آن User mode می‌گوییم که سطح دسترسی آن پایین است و بیشتر برای مانیتور کردن اطلاعات به کار می‌رود.

برای رفتن به مد بالاتر، یعنی Privileged Mode از دستور enable استفاده می‌کنیم:

```
Router>enable
Router#
```

همان‌طور که در دستور بالا مشاهده می‌کنید با واردکردن دستور enable وارد Privileged Mode شده‌ایم که علامت '#' نشان دهنده‌ی این موضوع است، در این مد می‌توانید کارهای مختلفی انجام دهید، برای خروج از این مد و یا هر مدی از دستور EXIT استفاده کنید:

```
Router#exit
Router>
```

البته در این مد، می‌توانید با دستورات Disable و Logout هم از این مد خارج شوید.

مد Privileged، مد بسیار مهمی است که تنظیمات کامل روتر از طریق این مد و مدهای بعد از آن انجام می‌شود که باید بر روی این مد رمز قرار دهیم تا زمانی که کسی وارد این مد می‌شود از وی رمز درخواست شود.

توجه داشته باشید، دسترسی به یک روتر از راه‌های مختلفی امکان‌پذیر است که می‌توانید بر روی همه آنها رمز عبور قرار دهیم.

قبل از اینکه وارد رمزگذاری روی راه‌های ورود به روتر شویم ، یک سری مسائل باید بررسی شوند.

در **ios** دو مد دیگر به‌جز مدهای گفته‌شده، وجود دارد و آن‌هم، مدهای Global و Interface است، با وارد شدن به مد Global تمام تنظیمات روتر، مانند رمزگذاری روی پورت‌ها، وارد شدن به مد Interface برای آدرس‌دهی به پورت‌ها، راه‌اندازی انواع پروتکل‌ها و هزاران کار دیگر که در این مد انجام می‌شود را می‌توانیم انجام دهیم. برای ورود به این مد، اول وارد مد privileged و بعد، با دستور configure terminal وارد این مد می‌شویم:

```
Router>enable
Router#configure terminal
Router(config)#
```

سیسکو از علامت سؤال برای راهنمایی کاربر استفاده کرده است، مثلاً اگر علامت سؤال را در مد Global وارد کنید، تعداد زیادی دستورات را به ما نشان می‌دهد.

www.takbook.com

Router(config)# **?**

همانطور که در شکل ۳۴-۲ مشاهده می‌کنید، با قرار دادن علامت سوال چندین دستور برای شما به نمایش گذاشته شده است.

```
Router(config)#?
Configure commands:
  aaa                 Authentication, Authorization and Accounting.
  access-list         Add an access list entry
  banner              Define a login banner
  bba-group           Configure BBA Group
  boot                Modify system boot parameters
  cdp                 Global CDP configuration subcommands
  class-map           Configure Class Map
  clock               Configure time-of-day clock
  config-register     Define the configuration register
  crypto              Encryption module
  default             Set a command to its defaults
  do                  To run exec commands in config mode
  dot11               IEEE 802.11 config commands
  enable              Modify enable password parameters
  end                 Exit from configure mode
  exit                Exit from configure mode
  flow                Global Flow configuration subcommands
  hostname            Set system's network name
  interface           Select an interface to configure
  ip                  Global IP configuration subcommands
  ipv6                Global IPv6 configuration commands
 --More--
```

شکل ۳۴-۲ دستورات IOS

در آخر، کلمه‌ی More را مشاهده می‌کنید که به این نکته اشاره دارد، تعداد دستورات در این بخش بیشتر است و اگر بر روی کلید Space روی صفحه‌کلید فشار دهید، بقیه‌ی دستورات را مشاهده خواهید کرد.

حالا کلمه‌ی conf را وارد و بعدازآن، علامت سؤال (؟) وارد کنید:

Router#**con?**
configure connect

همان‌طور که مشاهده می‌کنید با واردکردن علامت سؤال، دو دستور که با حروف con شروع شده‌اند را به ما نشان می‌دهد، این کار زمانی به کار می‌آید که یک کلمه را به صورت کامل در ذهن ندارید که با این کار، به کلمه‌ی موردنظر خود می‌رسید. در ضمن، شما می‌توانید کلمات را به صورت کوتاه شده هم بنویسید، مثلاً برای نوشتن دستور configuration Terminal می‌توانید از دستور کوتاه شده Conf t استفاده کنید.

Router#**conf t**
Router(config)#

www.takbook.com

وقتی مقداری کمی از دستور را تایپ کردید و می‌خواهید در زمان صرفه‌جویی کنید، می‌توانید با فشار کلید **TAB** روی صفحه‌کلید، بقیه‌ی دستور را کامل کنید، خودتان امتحان کنید.

۵-۲ نحوه‌ی کار با Interface

ادوات شرکت سیسکو از interfaceهای مختلفی برای ارتباط با دیگر ادوات شبکه استفاده می‌کنند، بسته به مدل روتر یا سوئیچ از چندین پورت و یا همان Interface تشکیل‌شده‌اند، یک روتر از چندین جای خالی یا همان Slot برای اضافه کردن پورت‌های متفاوت به آن استفاده می‌کند، یعنی اینکه شما می‌توانید پورت‌ها را جداگانه خریداری کرده و به آن اضافه کنید، در ضمن هر Slot روی روتر یا سوئیچ، یک شماره‌ی اختصاصی دارد. اولین Slot شماره‌ی صفر است؛ وقتی شما یک پورت خریداری می‌کنید و وارد Slot یک می‌کنید شماره‌ی آن در روتر مثلاً می‌شود FastEhternet 1/1 که یک اولی برای شماره Slot و یک دومی برای شماره پورت است.

پورت‌ها انواع مختلفی دارند:

- Ethernet
- FastEthernet
- GigaEthernet
- Serial

همانطور که در فصل اول گفتیم پورت‌های Ethernet از سرعت ۱۰ مگابایت پشتیبانی می‌کنند - پورت‌های FastEthernet از سرعت‌های ۱۰ ،۱۰۰ ، مگابایت پشتیبانی می‌کنند و پورت GigaEthernet سرعت‌های ۱۰، ۱۰۰، ۱۰۰۰ پشتیبانی می‌کند.

همان‌طور که در درس‌های قبل در مورد کابل سریال توضیح دادیم، می‌توانیم در ارتباط دو روتر باهم استفاده کنیم که به‌اصطلاح به آن ارتباط Point to Point می‌گویند، می‌توانیم در ارتباط با یک Service Provider هم استفاده کنیم، کابل سریال ویژگی خاصی دارد؛ زمانی که دو روتر می‌خواهند باهم ارتباط برقرار کنند باید از سرعت یکسانی برخوردار باشند، در کابل سریال می‌توانید پهنای باند یا همان BandWidth را تنظیم کنید. کابل‌های سریال از دو ویژگی DTE و DCE برای ارتباط باهم استفاده می‌کنند، یعنی یک سر کابل، DCE و سر دیگر آن DTE است، در طرفی که DCE است باید clock Rate تنظیم شود(Clock Rate سرعت ارتباطی بین دو روتر با استفاده از کابل سریال). حالا چگونه بفهمیم که کدام سر کابل DCE است تا بتوانیم clocke Rate را برای آن تنظیم کنیم، باید از دستور زیر استفاده کنیم:

Router(config)# **show controllers Serial 0/1**

www.takbook.com

با اجرای این دستور، DCE بودن کابل را به ما نشان می‌دهد (در ادامه به صورت کامل به این موضوع خواهیم پرداخت) و بعد از مشخص شدن DCE بودن کابل، باید Clock Rate را بر روی پورت سریال وارد کنیم، که برای این کار، وارد پورت موردنظر شده و دستور زیر را وارد می‌کنیم:

Router(config)# **Clock Rate 64000**

در این قسمت، عدد موردنظر را ۶۴۰۰۰ وارد کردیم که شما می‌توانید اعداد دیگری را هم وارد کنید. برای مشخص کردن این اعداد بعد از دستور clock Rate، یک علامت سؤال قرار دهید تا اعداد مشخص شود.

همان‌طور که گفتیم، یکی دیگر از ویژگی‌های کابل سریال، BandWidth و یا پهنای باند آن است که در انتخاب مسیر برای Routing Protocolها استفاده می‌شود که این مبحث را در درس‌های بعدی می‌آموزید، برای تغییر BandWidth باید وارد پورت سریال شده و از دستور زیر استفاده کرد:

Router(Config)#**Bandwidth 128**

SubInterface (پورت مجازی)

این پورت‌ها، پورت‌های مجازی هستند که روی هر پورت فیزیکی قرار دارند و به صورت 0/0.? هستند.

Router(config)#**interface gigabitEthernet 0/0.?**
<0-4294967295> GigabitEthernet interface number

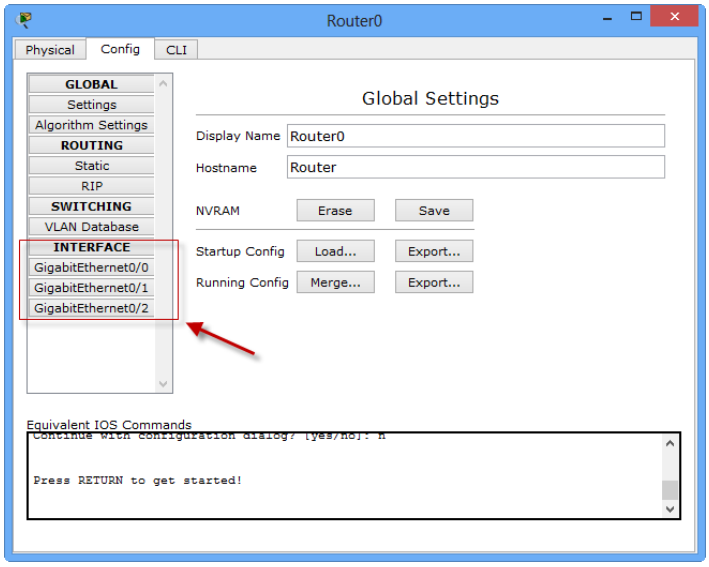
همان‌طور که مشاهده می‌کنید بعد از شماره پورت یک نقطه قرار دادیم و بعد از آن یک علامت سؤال قرارگرفته که تعداد پورت‌های مجازی را 4294967295 نشان می‌دهد. مانند زیر عمل کنید:

Router(config)#**interface gigabitEthernet 0/0.125**

در packet tracer یک روتر ۲۹۱۱ را به صفحه اضافه کنید. بعد بر روی آن کلیک کنید، طبق شکل ۳۵-۲ با رفتن به تب Config می‌توانید interface های مختلف آن را مشاهده کنید.

روی هرکدام که کلیک کنید، می‌توانید آن را خاموش یا روشن و یا آدرس‌دهی کنید که در ادامه با آن کار می‌کنیم.

www.takbook.com



شکل ۳۵-۲ تنظیمات پورت روتر

برای کار با Interfaceها به تب CLI رفته و در مد Privileged دستور زیر را وارد می‌کنیم تا لیست Interfaceهای روی روتر را مشاهده کنید.

```
Router#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol

GigabitEthernet0/0     unassigned      YES unset  administratively down down
GigabitEthernet0/1     unassigned      YES unset  administratively down down
GigabitEthernet0/2     unassigned      YES unset  administratively down down
Vlan1                  unassigned      YES unset  administratively down
```

همان‌طور که مشاهده می‌کنید با واردکردن دستور show ip interface brief لیست interfaceها را برای شما نمایش داده است، بعد با دستور زیر وارد interface موردنظر می‌شویم:

```
Router(config)#Interface  ?
```

بعد از نوشتن دستور Interface، یک علامت سؤال قرار دهید تا انواع interfaceها را به شما نشان دهد. اگر در قسمت قبل، متوجه شده باشید اینترفیس‌های ما از نوع GigaEthernet است، پس ادامه‌ی دستور به این صورت می‌شود:

```
Router(config)#interface gigabitEthernet 0/0
```

با این دستور وارد GigaEthernet 0/0 می‌شویم و می‌توانید کارهای مختلف روی پورت انجام دهیم، می‌خواهیم به این پورت IP address بدهیم برای این کار از دستور زیر استفاده می‌کنیم:

```
Router(config-if)#ip address 192.168.1.1 255.255.255.0
```

www.takbook.com

بعد از IP address باید ip مربوط به این interface را وارد کنیم که در اینجا ۱۹۲.۱۶۸.۱.۱ وارد می‌کنیم بعد، باید Subnet Mask را وارد کنیم که 255.255.255.0 را وارد می‌کنیم، این آدرس، به این Interface داده شد و بعدازاین کار، باید Interface مورد نظر را روشن کنیم. توجه داشته باشد که همه‌ی Interfaceهای روی روتر به صورت پیش‌فرض، خاموش (Shutdown) هستند و باید به صورت دستی روشن شوند، برای این کار از دستور زیر استفاده می‌کنیم:

Router(config-if)#**no shutdown**

با این دستور، پورت موردنظر روشن می‌شود و برای خاموش کردن آن از دستور shutdown استفاده می‌کنیم.

با دستور Show Protocols لیست interfaceهای روتر، فعال و غیرفعال بودن آن‌ها را به ما نشان می‌دهد.

```
Router#show protocols
Global values:
  Internet Protocol routing is enabled
GigabitEthernet0/0 is administratively down, line protocol is down
GigabitEthernet0/1 is administratively down, line protocol is down
GigabitEthernet0/2 is administratively down, line protocol is down
Vlan1 is administratively down, line protocol is down
```

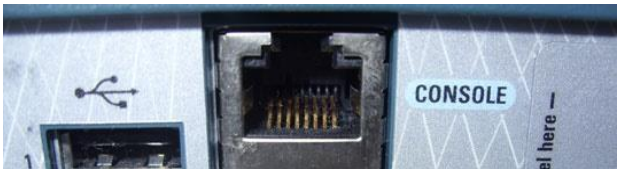
۶-۲ روش‌های دسترسی و رمزگذاری

برای دسترسی به روتر چندین روش وجود دارد که هرکدام را مورد بررسی قرار می‌دهیم:

پورت Console

این همان پورتی است که از طریق کابل Console به روتر متصل شدیم و برای متصل شدن به یک روتر خام است که هیچ‌گونه تنظیماتی روی آن انجام نشده است، برای رمزنگاری این پورت، باید کارهای زیر را انجام دهید.

www.takbook.com



شکل ۳۶-۲ پورت کنسول

وارد مد global شوید و با دستور Line console 0، وارد پورت کنسول شوید. مانند زیر عمل کنید:

Router(config)#**line consol 0**
Router(config-line)#

اصولاً روی روترها، یک پورت کنسول وجود دارد که شماره‌ی آن صفر است.

در این قسمت می‌خواهیم روی این پورت رمز قرار دهیم، باید کارهای زیر را انجام دهیم:

Router(config-line)# **password 123**

برای این کار، از دستور Password و بعدازآن، از یک کلمه‌ی عبور، مانند ۱۲۳ استفاده می‌کنیم که شما می‌توانید به جای این کلمه‌ی عبور (۱۲۳)، کلمه‌ی عبور دلخواهی را وارد کنید.

بعدازاین که رمز را وارد و enter کردیم باید از دستور login استفاده کنیم تا زمانی که می‌خواهیم وارد تنظیمات روتر شویم از ما رمز عبور پرسیده شود، پس به این صورت این دستور را وارد می‌کنیم:

Router(config-line)# **Login**

اگر شما دستور Login را وارد نکنید، هر رمزی را هم روی روتر فعال کنید، باز برای ورود از شما رمز عبور درخواست نمی‌شود، پس به این نکته توجه کنید.

در حال حاضر با واردکردن این دستورات، روی روتر رمز قرار دادیم و زمانی‌که می‌خواهیم از طریق کابل Console وارد User Mode شویم، از شما رمز درخواست می‌شود که در ادامه، نحوه‌ی رمزنگاری پیشرفته‌تر را با هم فرا می‌گیریم، به دلیل اینکه این نوع رمزها، TEXT Base بوده و قابل‌شناسایی و هک شدن هستند.

دستورات دیگری در این پورت وجود دارد که باهم مورد بررسی قرار می‌دهیم:

دستور exec-timeout

زمانی‌که وارد یک مد می‌شوید، اگر مدت زمانی با روتر کار نکنید، در هر مدی که هستید، خارج شده و به مد اول، یعنی UserMode برگشت می‌کند، برای جلوگیری از این کار، باید از دستور زیر در پورت console استفاده کنید:

Router(config-line)#**exec-timeout 0 0**

www.takbook.com

همان‌طور که مشاهده می‌کنید، در این دستور از دو صفر استفاده شده است که اولی برای دقیقه و دومی برای ثانیه است، با صفر کردن هر دو اگر در هر مدی باشید در همان مد ثابت خواهد ماند و خارج نمی‌شود، البته می‌توانید هر زمان که نظر شما است را وارد کنید.

دستور logging synchronous

زمانی در حال تایپ کردن دستورات هستید، روتر به صورت خودکار یک سری اطلاعات را به شما نمایش می‌دهد، مانند فعال شدن یک پورت و یا اجرا شدن یک پروتکل و... که این کار باعث می‌شود دستوراتی که در حال نوشتن هستیم برای آن‌ها مشکلی ایجاد شود و جا به جا شوند. برای جلوگیری از این کار در پورت Console از دستور زیر استفاده کنید:

Router(config-line)#**logging synchronous**

بررسی Enable Password

این نوع رمز برای Privileged Mode است. اگر کاربری بخواهد وارد این مد شود از وی پسورد درخواست می‌شود. برای فعال کردن آن، وارد مد Global می‌شویم و دستور زیر را تایپ و بعد enter می‌کنیم.

Router(config)#**enable password 123**

با این دستور، رمز عبور بر روی مد Privileged فعال می‌شود و زمانی که بخواهید با دستور Enable وارد این مد شوید از شما رمز عبور درخواست می‌شود که به صورت زیر این موضوع را مشاهده می‌کنید.

Router>**enable**
Password:
Router#

توجه داشته باشید در موقع واردکردن رمز عبور، رمز عبور به شما نمایش داده نمی‌شود.

رمزهای عبوری که با دستور Enable Password فعال می‌شوند، زیاد نمی‌توانند امن باشند، چون این رمزها به صورت Text Base بوده و با یک فرمان می‌توانید رمز عبور را مشاهده کنید! برای دیدن رمز عبور از دستور Show Runing-config استفاده کنید، دستور show برای نمایش اطلاعات به کار برده می‌شود، که با این دستور در درس‌های آینده زیاد کار خواهیم کرد، این دستور در مدهای UserMode و Priviliged Mode کار می‌کند، البته در مد Global هم کار می‌کند که باید قبل از این دستور از کلمه‌ی do استفاده کنیم، دستور بعدی که بعد از دستور show به کار بردیم Running-Config است، این دستور اطلاعات حاضر در Ram را به ما نشان می‌دهد، یعنی اینکه هر تنظیماتی که روی روتر انجام شده، در این قسمت قرار دارد. می‌خواهیم با این دستور به شما نشان دهیم که دستور Enable Password زیاد هم امن نیست، این دستور را در مد Privileged وارد کنید.

Router#**show running-config**
Building configuration...

Current configuration : 648 bytes

www.takbook.com

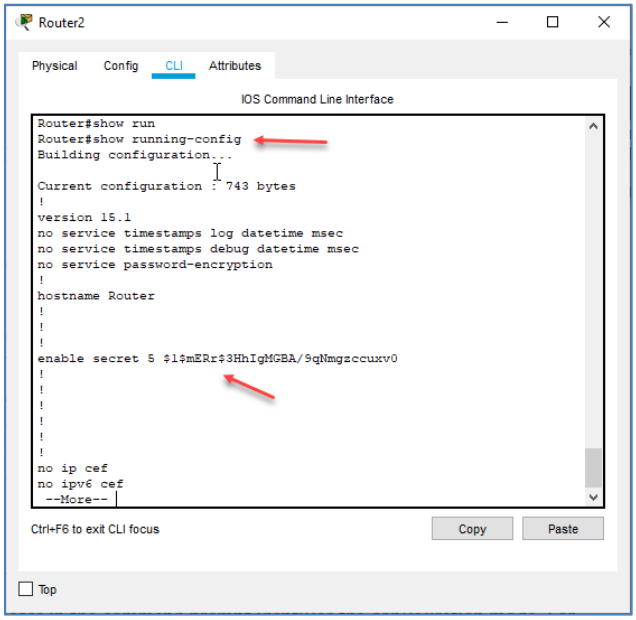

```
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Router
!
!
!
enable password 123
!
!
!
!
!
!
!
!
 --More--
```

همان‌طور که مشاهده می‌کنید با واردکردن دستور Show Running-config، رمز عبور واردشده، نمایش داده شد، پس باید کاری کرد که این رمز به صورت Hashing یا کد شده در این قسمت نمایش داده شود تا کسی نتواند این رمز را مشاهده کند، مانند قبل وارد مد global شوید و کارهای زیر را انجام دهید:

اول از همه، رمز قبلی را که وارد کردیم، حذف می‌کنیم. برای حذف هر دستوری که وارد کردیم، باید قبل از آن دستور، از کلمه‌ی No استفاده کنیم تا دستور مورد نظر حذف شود، برای این کار از دستور No enable password استفاده می‌کنیم، بعد از این کار، از دستور enable Secret 123 استفاده می‌کنیم که رمز عبور را به صورت کد شده درمی‌آورد و برای شما نمایش می‌دهد، بعد از این کار در مد Privileged دستور show Running-config را اجرا کنید، متوجه می‌شوید که رمز عبور ۱۲۳ به صورت کد شده درآمده است.

همانطور که در شکل ۳۷-۲ مشاهده می‌کنید رمز عبور ۱۲۳ به صورت کلی تغییر کرده و به یک کد Hash تبدیل شده است.

www.takbook.com



شکل ۳۷-۲ رمزنگاری در روتر سیسکو

نکته مهم:

زمانی‌که Enable Secret فعال است، Enabel Password روی روتر کاربردی ندارد و اگر هر دو دستور را در یک‌زمان فعال کنید، فقط رمز عبوری که با دستور Enable Secret فعال کردید، جواب می‌دهد .

پورت AUX

این پورت برای ارتباط از راه دور از طریق خط تلفن با روتر استفاده می‌شود که می‌توانیم به روش زیر فعال کنیم:

Router(config)#**Line aux 0**
Router(config-line)#**password 123**
Router(config-line)#**login**

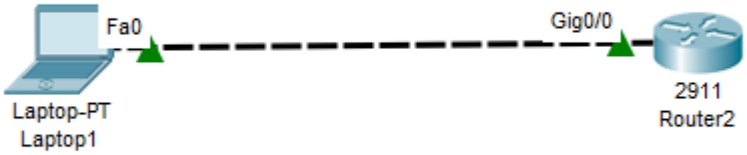
این رمز عبور قبل از وارد شدن به User Mode پرسیده می‌شود.

Telnet

Telnet یکی از راه‌های محبوب برای دسترسی به روتر از راه دور است، که برای فعال کردن آن باید کارهای مختلفی انجام بگیرد، این کار را با مثالی کامل انجام می‌دهیم:

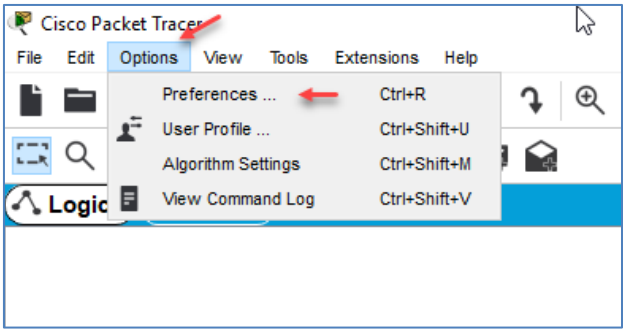
www.takbook.com

یک روتر 2911 و یک Laptop به صفحه اضافه کنید و بعد با کابل Cross پورت Fast Ethernet 0 کامپیوتر را به پورت GigaEthernet0/0 متصل کنید، مانند شکل ۳۸-۲ این کار را انجام دهید.



شکل ۳۸-۲ پورت کنسول

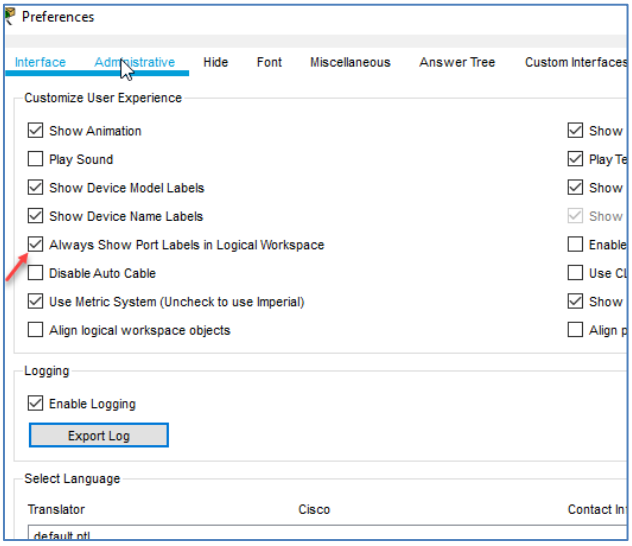
اگر به شکل ۳۸-۲ توجه کنید بر روی کابل، نام Interface هر دستگاه نوشته شده است که برای اینکه این گزینه را در Packet Tracer فعال کنید، باید به مانند شکل ۳۹-۲ وارد منوی Options شوید و بر روی Prefrences کلیک کنید.



شکل ۳۹-۲ تنظیمات Packet Tracer

در شکل ۴۰-۲ باید تیک گزینه‌ی مورد نظر را انتخاب کنید تا نام Interfaceها در صفحه، نمایش داده شود.

www.takbook.com



شکل ۴۰-۲ تنظیمات Packet Tracer

خوب، بعد از این کار بر روی روتر کلیک کنید تا صفحه‌ی موردنظر باز شود وارد مد Global شوید و بعد از آن با دستور زیر پورت GigaEthernet را آدرس‌دهی کنید.

```
Router(config)#interface gigabitEthernet 0/0
Router(config-if)#ip address 192.168.1.1 255.255.255.0
Router(config-if)#no shutdown
```

با دستور interface gigabitEthernet 0/0 وارد interface مورد نظر شده‌ایم، بعد یک ip آدرس به این پورت نسبت داده‌ایم و بعد از این کار پورت موردنظر را با دستور **no shutdown** روشن کرده‌ایم.

پورت موردنظر را آدرس‌دهی و روشن کرده‌ایم، بعد از این کار باید Telnet را فعال کنیم تا بتوانیم از راه دور با استفاده از آدرسی که دادیم به روتر متصل شویم.

برای فعال کردن Telnet باید پورت‌های مجازی VTY را فعال کنیم. VTY مخفف Virtual terminal که از چندین پورت مجازی برای ورود به روتر استفاده می‌کند، مثلاً در روتر ۲۹۱۱ که ما در حال کار با آن هستیم از ۱۵ پورت تشکیل شده است. برای مشاهده این پورت‌ها در مد Global دستور زیر را وارد کنید:

```
Router(config)#line vty ?
<0-15>  First Line number
```

با واردکردن دستور Line Vty و بعدازآن، علامت سؤال به ما تعداد پورت‌های مجازی برای این روتر را نشان می‌دهد که ۱۵ عدد است. شما می‌توانید تمام این ۱۵ پورت را فعال کنید که با این کار ۱۵ نفر در یک‌زمان می‌توانند وارد روتر یا سوئیچ شوند.

در اینجا تمام این ۱۵ پورت را انتخاب و همه‌ی آن‌ها را فعال می‌کنیم، و روی همه آن‌ها رمز قرار می‌دهیم:

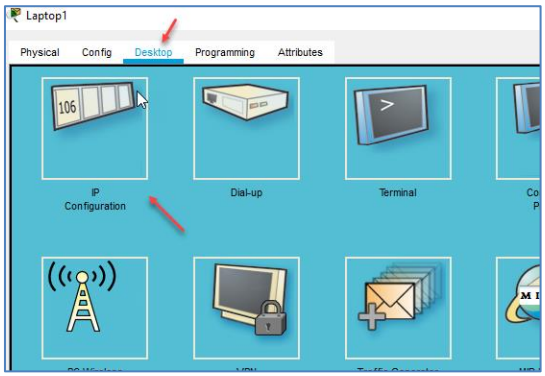
```
Router(config)#line vty 0  15
Router(config-line)#pass 123
```

www.takbook.com


```
Router(config-line)#login
Router(config-line)#
```

تعجب نکنید که به جای نوشتن Password از pass استفاده کردیم، چون همان‌طور که گفتیم در IOS می‌توانیم فرمان‌ها را به صورت کوتاه شده بنویسیم، در قسمت سوم از دستور Login استفاده کردیم که با این دستور به روتر اعلام می‌کنیم که در زمان Telnet رمز عبور را درخواست کن. اگر به جای Login از دستور No Login استفاده کنید، روتر هیچ‌گونه رمزی درخواست نخواهد کرد، پس به این دستور توجه کنید. شما می‌توانید به چند پورت اجازه دسترسی بدهید و به بقیه‌ی پورت‌ها اجازه دسترسی ندهید.

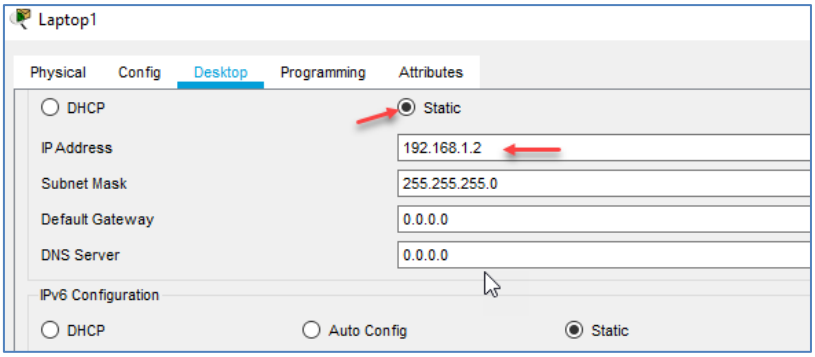
همه‌چیز برای اجرای سرویس Telnet آماده است، بر روی Laptop کلیک کنید و به مانند شکل ۲-۴۱ وارد تب Desktop شوید و بر روی Ip configuration کلیک کنید.



شکل ۲-۴۱ تنظیمات لپ‌تاپ در Packet Tracer

به مانند شکل ۲-۴۲ آدرس IP در رنج روتر وارد کنید.

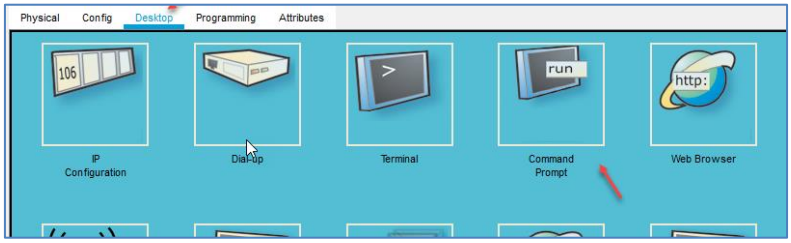
توجه داشته باشید در فصل‌های آینده ورژن‌های مختلف IP را به صورت مفصل بررسی خواهیم کرد.



شکل ۲-۴۲ تنظیمات لپ‌تاپ در Packet Tracer

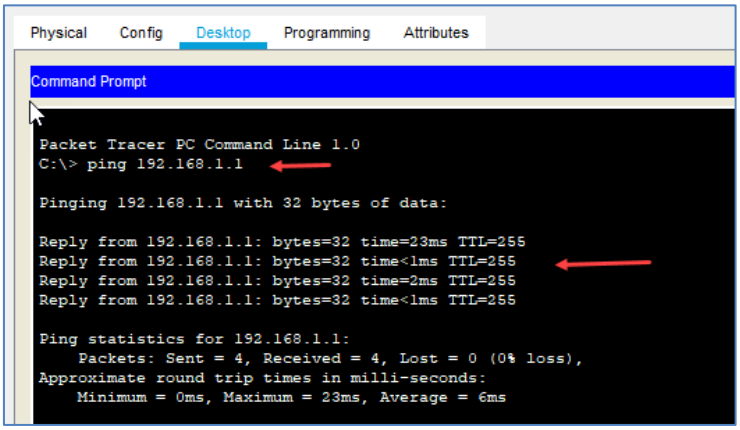
در ادامه کار به مانند شکل ۲-۴۳ بر روی Command Prompt کلیک کنید.

www.takbook.com



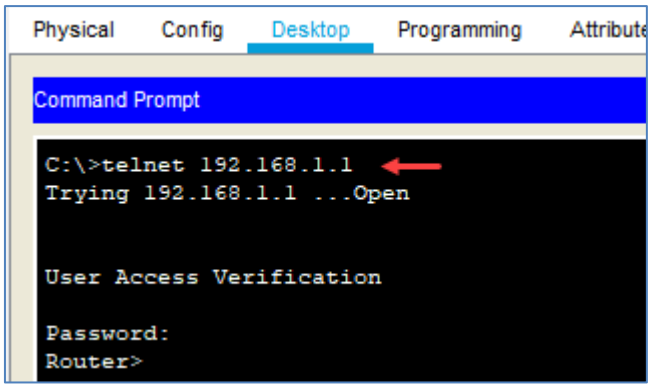
شکل ۴۳-۲ تنظیمات لپ‌تاپ در *Packet Tracer*

در این قسمت با دستور Ping ارتباط با روتر را تست می‌گیریم که همانطور که در شکل ۴۴-۲ مشاهده می‌کنید، ارتباط به درستی شکل گرفته است و Laptop می‌تواند روتر را ببیند.



شکل ۴۴-۲ اجرای دستور *Ping*

در ادامه با دستور Telnet به روتر متصل می‌شویم و رمز عبور ۱۲۳ را وارد می‌کنیم که این موضوع را درشکل ۴۵-۲ مشاهده می‌کنید



شکل ۴۵-۲ اجرای دستور *Ping*

www.takbook.com

شما اگر دستور show Running-config را اجرا کنید، متوجه می‌شوید که تمام رمزهایی را که برای پورت‌های console، AUX و VTY وارد کرده‌ایم در این دستور قابل مشاهده است. به شکل ۴۶-۲ توجه کنید.

```
line con 0
 password 123
!
line aux 0
 password 123
!
line vty 0 4
 password 123
 login
line vty 5 15
 password 123
 login
!
!
!
end

Router(config-line)#
```

شکل ۴۶-۲ اجرای دستور show Running-config

برای این‌که این رمزها یا هر رمزی که داخل IOS وارد می‌کنید، به صورت کد شده (Hash) تبدیل شود از دستور زیر در مد Global استفاده می‌کنیم.

Router(config)# **service password-encryption**

بعد از واردکردن این دستور تمام رمزها به صورت Hash شده یا کد شده درمی‌آید. به شکل ۴۷ -۲، توجه کنید:

همان‌طور که در شکل ۴۷-۲ مشاهده می‌کنید، تمام رمزها به صورت Hash شده درآمده، البته این روش به صورت کامل، روتر را در برابر نفوذ امن نگه نمی‌دارد.

```
line con 0
 password 7 08701E1D
!
line aux 0
 password 123
!
line vty 0 4
 password 7 08701E1D
 login
line vty 5 15
 password 7 08701E1D
 login
!
!
!
end

Router(config)#
```

شکل ۴۷-۲ اجرای دستور show Running-config

www.takbook.com

برای امنیت شبکه در سیستم‌های سیسکو باید کتابی آموزشی CCNA Security را از سایت 3isco.ir دریافت کنید.

نکته: شاید دیده باشید که زمانی در روتر یک دستور را اشتباه وارد می‌کنید روتر به جستجوی آن دستور می‌پردازد، در زیر جمله rn را که کاربردی در روتر ندارد وارد کردیم، اما روتر چنین دستوری ندارد و برای پیدا کردن آن به جستجو می‌پردازد و همین باعث اتلاف وقت می‌شود.

```
Router>rn
Translating "rn"...domain server (255.255.255.255)
%Unknown command or computer name, or unable to find computer address
```

برای جلوگیری از این موضوع وارد مد Global شده و دستور زیر را وارد کنید:

```
Router(config)#no ip domain-lookup
```

با این دستور، روتر دیگر به جستجوی دستورات نمی‌پردازد.

تا اینجا رمز عبور را برای پورت‌ها و مسیرهای مختلف فعال کردیم و نحوه‌ی کد (Hash)کردن آن‌ها را هم یاد گرفتیم، حالا اگر روتر را خاموش کنیم، آیا این تنظیمات روی روتر باقی خواهد ماند؟

به‌هیچ‌وجه این تنظیمات روی روتر باقی نمی‌ماند، چون تمام این اطلاعات در فایلی به نام Running-Config روی Ram قرار دارد و چون Ram حافظه‌ای فرار است، این اطلاعات بعد از خاموش کردن از بین می‌رود، برای حل این مشکل باید این اطلاعات را به یک حافظه غیرموقت ارسال کنیم تا اطلاعات از بین نرود.

۷-۲ ذخیره اطلاعات دستگاه‌های سیسکو

برای اینکه اطلاعاتی که در روتر وارد کردیم را در یک محل نگهداری کنیم دو روش وجود دارد:

- ✓ Nvram
- ✓ TFTP Server

۱- برای ذخیره اطلاعات به حافظه‌ی Nvram، از دستور زیر در مد Privileged استفاده می‌کنیم.

```
Router#copy running-config startup-config
Destination filename [startup-config]?
Building configuration…
[OK]
Router#
```

www.takbook.com

همان‌طور که گفتیم running-config، فایلی است که روی Ram قرار دارد و Startup-config فایل است که بر روی Nvram قرار دارد و با دستور بالا اطلاعاتی که درون فایل running-config قرار دارد وارد startup-config می‌شود.

در قسمت بعدی از شما نام فایل مقصد را می‌پرسد که چیزی وارد نکنید و بعد Enter را زده تا اطلاعات ذخیره شود و حالا اگر روتر را خاموش و بعد روشن کنید اطلاعات آن از بین نمی‌رود.

حذف کردن اطلاعات NVRAM

برای حذف اطلاعات موجود در حافظه‌ی Nvram، باید دستور زیر را در مد Privileged وارد کنید:

Router# **erase startup-config**

بعد از Enter کردن به شما اخطار می‌دهد که آیا مطمئن به پاک کردن اطلاعات موجود در Nvram هستید؟

Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]

اگر Enter کنید، کل اطلاعات موجود در Nvram از بین خواهد رفت. فایل startup-config مربوط به حافظه‌ی Nvram است.

دو دستور دیگر هم برای این کار وجورد دارد که به صورت زیر است:

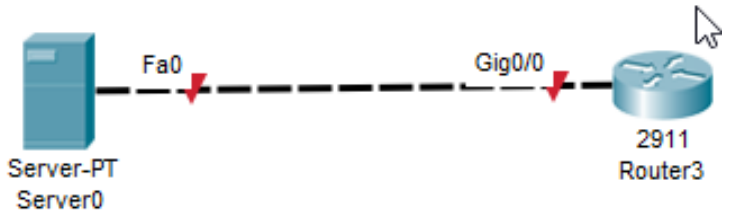
write erase

و

erase nvram:

۲- TFTP Server:

در روش دوم اطلاعات از روتر به یک سرور خارجی منتقل می‌شود و دوباره می‌توان این اطلاعات را از سرور وارد روتر کرد، این کار را باهم انجام می‌دهیم، یک روتر و یک سرور را به لیست اضافه کنید و بعد با کابل Cross این دو را به هم متصل کنید، مانند شکل ۴۸-۲:



شکل ۴۸-۲ TFTP Server

www.takbook.com

اگر به شکل ۴۸-۲ توجه کنید، ورودی پورت یک علامت قرمز رنگ دارد که نشان دهنده‌ی خاموش بودن پورت است، برای اینکه آنها را به رنگ سبز تغییر دهید باید مانند روش‌های قبلی به Interface های روتر و سرور آدرس دهید، که برای روتر آدرس 192.168.1.1 و آدرس 192.168.1.2 را هم برای سرور قرار دهید، بعد وارد روتر شوید و در مد Privileged دستور زیر را وارد کنید:

Router#**copy running-config tftp:**

بعد از واردکردن این دستور از شما آدرس سرور درخواست می‌شود که شما باید آدرس سرور که 192.168.1.2 است را وارد کنید و بعد از Enter، باید نام فایل مقصد را وارد کنید، مانند دستور زیر:

Address or name of remote host []? **192.168.1.2**
Destination filename [Router-confg]? Babajani_Router

با انجام این دستورات اطلاعات از روتر به یک سرور خارجی انتقال داده می‌شود.

کلیدهای ترکیبی

در IOS کلیدهایی طراحی شده است که می‌توانید با فشار آنها عملیاتی را انجام دهید، که لیست آن را در زیر مشاهده می‌کنید:

Ctrl_A باعث می‌شود مکان‌نما به خط آغازین انتقال پیدا کند.
Ctrl_E باعث می‌شود مکان‌نما به انتهای خط برود.
Ctrl_B به اندازه‌ی یک حروف به عقب برگشت می‌کند.
Ctrl_F به اندازه‌ی یک حروف به جلو انتقال داده می‌شود.
Ctrl_D کاراکترهای جلوی مکان‌نما را حذف می‌کند.
Ctrl_U کل خط موردنظر را پاک می‌کند.
Ctrl_W یک کلمه را پاک می‌کند.
Ctrl_Z باعث می‌شود که مکان‌نما در هر مدی که قرار داشته باشد به مد Privileged انتقال پیدا کند.

اگر بر روی کلیدهای جهت بالا و پایین فشار دهید ، آخرین دستوراتی را که وارد کرده اید را می‌توانید مشاهده کنید.

با استفاده از دستورshow history می‌توانید ۱۰ دستور آخر واردشده را مشاهده کنید.

Router#**show history**
en
conf t
show history

تغییر نام روتر (HostName)

www.takbook.com

می‌توانید نام روتر را تغییر دهید تا استفاده از آن برای شما آسان‌تر شود. سعی کنید نام روتر را طبق محلی که قرار دارد تغییر دهید، مثلاً اگر روتر در شهر بابل قرار دارد، نام آن را به بابل تغییر دهید. برای انجام این کار در مد Global، دستور زیر را وارد کنید:

```
Router(config)#hostname babol
babol(config)#
```

همان‌طور که مشاهده می‌کنید، نام روتر به babol تغییر کرده است.

نمایش پیام در زمان ورود به روتر (Banner)

این دستور زمانی به کار می‌رود که بخواهیم برای کسی که وارد روتر می‌شود پیام نمایش بدهیم که برای انجام این کار وارد مد Global می‌شویم و از دستور زیر استفاده می‌کنیم.

```
Router1(config)#banner ?
loginSet login banner
motdSet Message of the Day banner
```

با واردکردن دستور Banner و بعد آن علامت سؤال دو حالت را نمایش می‌دهد که Login برای کاربرانی است که از طریق Telnet وارد روتر می‌شوند و Motd برای کاربرانی است که به صورت مستقیم وارد روتر می‌شوند. در این قسمت از Motd استفاده می‌کنیم:

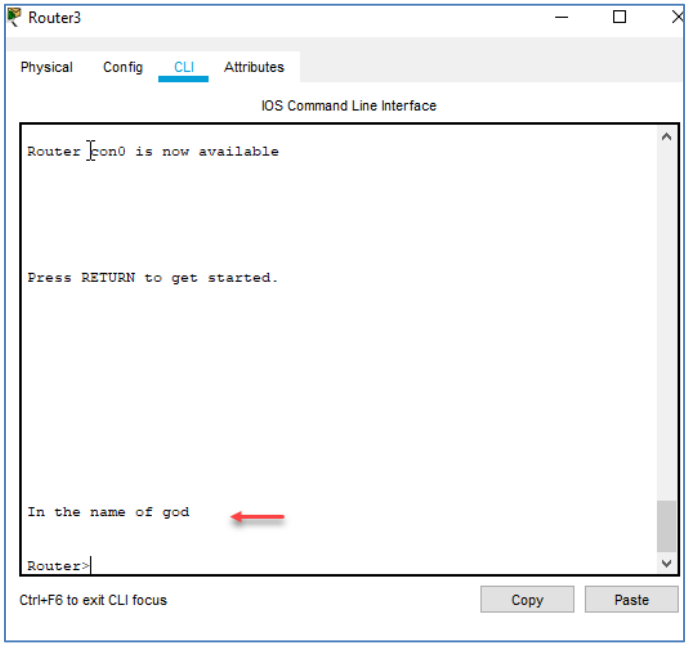
```
Router1(config)#banner motd@
```

در دستور بالا از کلمه‌ی @ استفاده کردیم که به جای آن هر کلمه‌ای می‌توانید قرار دهید. این کلمه، به این معنا است که پیامی که می‌نویسیم، بعد از اتمام پیام اگر این کلمه را در انتهای آن قرار دهید، یعنی اتمام کار و enter کنید، پیام ثبت می‌شود.

```
Router1(config)#banner motd @
Enter TEXT message.  End with the character '@'.
in the name of god @
Router1(config)#
```

banner motd را با هم انجام دادیم، وارد UserMode شوید و قبل از اینکه بخواهیم کاری انجام دهیم پیغام زیر نمایش داده خواهد شد که این موضوع را در شکل ۴۹-۲ مشاهده می‌کنید، این نوع دستورات می‌توانند در کار بسیار کمک کننده باشند و یادآور کار خاصی برای مدیر باشند.

www.takbook.com



شکل ۴۹-۲ *CLI Router*

نوع دیگری از banner وجود دارد که به آن Banner Login می‌گویند. این روش در موقع ورود از طریق Telnet کاربرد دارد. برای فعال کردن آن دستور زیر را وارد کنید.

Router1(config)#**banner login @**
Enter TEXT message. End with the character '@'.
Welcom @

مانند روش قبلی است، فقط به جای Motd، Login قرار می‌دهیم و پیام موردنظر را وارد می‌کنیم.
در زمان Telnet کردن این پیام نمایش داده خواهد شد.

نوشتن توضیحات برای یک Interface

در IOS این امکان وجود دارد که بر روی interface می‌توانید توضیحاتی قرار دهید، برای این کار وارد interface موردنظر می‌شویم و دستور زیر را وارد می‌کنیم:

Router(config-if)#**description connection iran to usa**

بعد از دستور description پیام خود را وارد کنید، مانند مثال بالا.
بعد از انجام این کار برای نمایش این پیام دستور **show Running-config** را در مد privileged وارد کرده و این توضیحات زیر Interface موردنظر نمایش داده می‌شود، مانند دستور زیر:

interface GigabitEthernet0/0
description connection iran to usa

www.takbook.com

تنظیم ساعت و تاریخ روتر

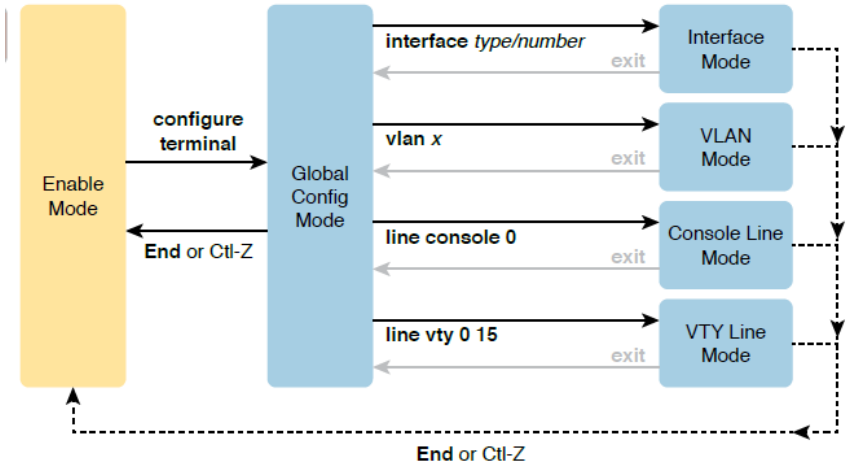
برای اینکه ساعت روتر خود را تنظیم کنید از دستور زیر استفاده کنید:

Router#**clock set 10:20:30 19 sep 2020**

با دستور Clock Set این کار انجام می‌شود و بعد از این دستور ساعت، دقیقه و ثانیه را وارد کنید مانند 10:05:05 و بعدازآن، روز، ماه، سال را وارد کنید مانند 19 Nov 2013، بدین‌ترتیب ساعت و تاریخ روتر تنظیم می‌شود.

تا اینجا دستورات مختلف و اولیه را با هم بررسی کردیم و کاره‌های لازم را بر روی روتر انجام دادیم.

در شکل ۴۹-۲ یک نمای کلی از مدهای مختلف را مشاهده می‌کنید که مثلاً اگر در مد Global باشید با استفاده از کلید ترکیبی CTRL + Z می‌تواند به مد Enable برگردید و یا اگر در مد Interface بودید می‌توانید با دستور exit به مد قبلی آن برگردید یعنی یک قدم عقب‌تر.



شکل ۵۰-۲ *CLI Mode*

۸-۲ سوالات فصل دوم

www.takbook.com

1. In what modes can you type the command show mac address-table and expect to get a response with MAC table entries? (Choose two answers.)

در کدام Mode می‌توانیم دستور show mac address-table را وارد کنیم و نتیجه کار یعنی جدول MAC را مشاهده کنیم؟(دو گزینه انتخاب شود)

a. User mode
b. Enable mode
c. Global configuration mode
d. Interface configuration mode

2. In which of the following modes of the CLI could you type the command reload and expect the switch to reboot?

در کدام یک از Modهای زیر می‌توانید دستور Reload را برای راه‌اندازی مجدد سوئیچ اجرا کنید؟

a. User mode
b. Enable mode
c. Global configuration mode
d. Interface configuration mode

3. Which of the following is a difference between Telnet and SSH as supported by a Cisco switch?

تفاوت بین دو پروتکل SSH و Telnet در کدام گزینه بهتر مشخص شده است؟

a. SSH encrypts the passwords used at login, but not other traffic; Telnet encrypts nothing.
b. SSH encrypts all data exchange, including login passwords; Telnet encrypts nothing.
c. Telnet is used from Microsoft operating systems, and SSH is used from UNIX and Linux operating systems.
d. Telnet encrypts only password exchanges; SSH encrypts all data exchanges.

4. What type of switch memory is used to store the configuration used by the switch when it is up and working?

کدام نوع حافظه برای ذخیره‌سازی اطلاعات پیکربندی سوئیچ مورد استفاده قرار می‌گیرد؟

a. RAM
b. ROM
c. Flash
d. NVRAM
e. Bubble

5. What command copies the configuration from RAM into NVRAM?

کدام دستور زیر برای کپی کردن اطلاعات پیکربندی از RAM به NVRAM است؟

a. copy running-config tftp
b. copy tftp running-config
c. copy running-config start-up-config
d. copy start-up-config running-config
e. copy startup-config running-config
f. copy running-config startup-config

6. A switch user is currently in console line configuration mode. Which of the following would place the user in enable mode? (Choose two answers.)

www.takbook.com

در سوئیچ یک کاربر در حالت پیکربندی در خط کنسول قرار دارد، کدام گزینه کاربر را به حالت enable mode می‌برد؟ (دو گزینه را انتخاب کنید)

a. Using the exit command once
b. Using the end command once
c. Pressing the Ctrl+Z key sequence once
d. Using the quit command

7. Which of the following statements describes part of the process of how a switch decides to forward a frame destined for a known unicast MAC address?

کدام یک از جمله‌های زیر بخشی از فرآیند نحوه تصمیم‌گیری سوئیچ برای ارسال یک Frame برای یک آدرس خاص MAC است؟

a. It compares the unicast destination address to the bridging, or MAC address, table.
b. It compares the unicast source address to the bridging, or MAC address, table.
c. It forwards the frame out all interfaces in the same VLAN except for the incoming interface.
d. It compares the destination IP address to the destination MAC address.
e. It compares the frame's incoming interface to the source MAC entry in the MAC address table.

8. Which of the following statements describes part of the process of how a LAN switch decides to forward a frame destined for a broadcast MAC address?

کدام یک از گزینه‌های زیر در مورد بخشی از فرآیند سوئیچ برای ارسال Frame به یک ادرس MAC Broadcast است؟

a. It compares the unicast destination address to the bridging, or MAC address, table.
b. It compares the unicast source address to the bridging, or MAC address, table.
c. It forwards the frame out all interfaces in the same VLAN except for the incoming interface.
d. It compares the destination IP address to the destination MAC address.
e. It compares the frame's incoming interface to the source MAC entry in the MAC address table.

9. Consider the following output from a Cisco Catalyst switch:

```
SW1# show mac address-table dynamic
Mac Address Table
-------------------------------------------
Vlan Mac Address Type Ports
---- ----------- -------- -----
1 02AA.AAAA.AAAA DYNAMIC Gi0/1
1 02BB.BBBB.BBBB DYNAMIC Gi0/2
1 02CC.CCCC.CCCC DYNAMIC Gi0/3
Total Mac Addresses for this criterion: 3
```

Which of the following answers is true about this switch?

خروجی دستور مورد نظر را در سوئیچ سیسکو مشاهده می‌کنید، کدام یک از گزینه‌های زیر در مورد این سوئیچ درست است؟

a. The output proves that port Gi0/2 connects directly to a device that uses address

www.takbook.com

02BB.BBBB.BBBB.
b. The switch has learned three MAC addresses since the switch powered on.
c. The three listed MAC addresses were learned based on the destination MAC address of frames forwarded by the switch.
d. 02CC.CCCC.CCCC was learned from the source MAC address of a frame that entered port Gi0/3.

10. Imagine that you have configured the enable secret command, followed by the enable password command, from the console. You log out of the switch and log back in at the console. Which command defines the password that you had to enter to access privileged mode?

تصور کنید که دستور enable secret را تنظیم کردید، و به دنبال ان دستور enable password را فعال کردید، در این لحظه از کنسول ارتباطی خارج شده و دوباره به آن متصل می‌شوید، در این لحظه کدام فرمان رمز ورود از شما درخواست می‌شود؟

a. enable password
b. enable secret
c. Neither
d. The password command, if it is configured

www.takbook.com

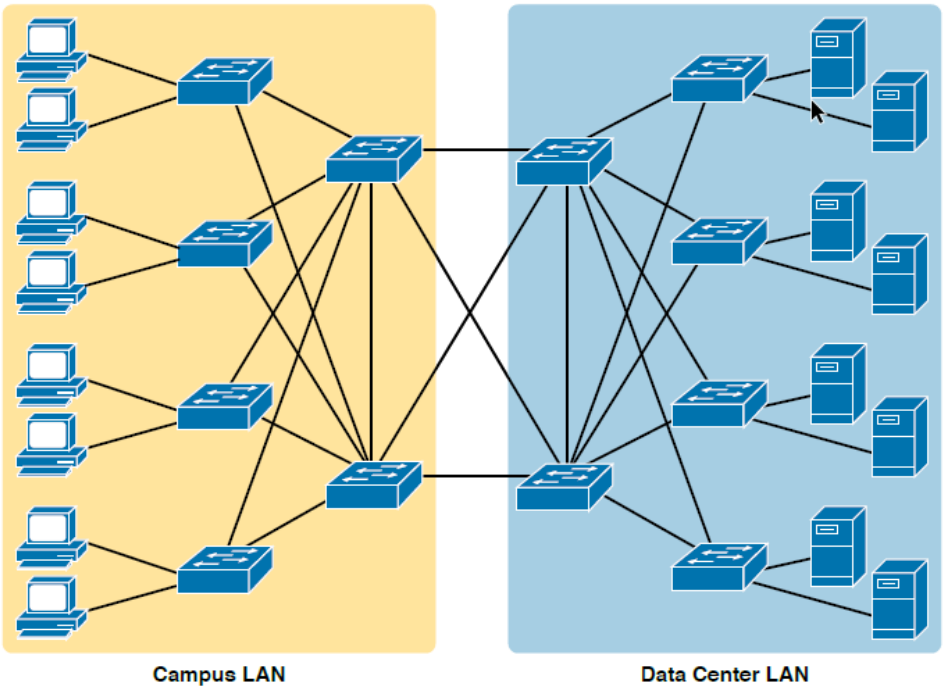
www.takbook.com

www.takbook.com

فصل سوم

بررسی سوئیچینگ شبکه

سوئیچ را می‌توانید قلب تپنده‌ی یک سازمان بنامید، بی شک تنها سخت‌افزاری که برای امر شبکه در همه‌ی سازمان‌ها وجود دارد سوئیچ است که باعث می‌شود که دستگاه‌های مختلف را به هم متصل کند، در شکل ۳-۱ نحوه‌ی ارتباط سوئیچ‌ها در یک دانشگاه (Campus) و یک Data Center را مشاهده می‌کنید.



شکل ۳-۱ *Ethernet LAN*

به طور کلی نقش سوئیچ این است که فریم‌های Ethernet را در شبکه حمل کند، پس کار اصلی یک سوئیچ ارسال درست و به مقصد رساندن فریم است که این مقصد از طریق آدرس MAC مشخص می‌شود.

آدرس‌های MAC در منبع و مقصد هر فریم در سوئیچ مشخص شده است.

سوئیچ‌ها برای انجام این کارها از سه عمل را انجام می‌دهند:

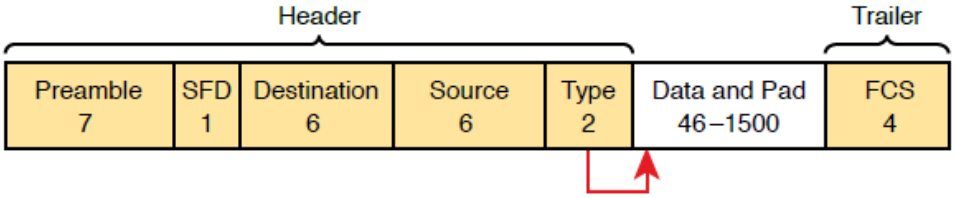
www.takbook.com

۱- تصمیم‌گیری برای ارسال فریم به جلو و یا جلوگیری از آن، که بر اساس آدرس MAC مقصد انجام می‌گیرد.

۲- آماده‌سازی برای ارسال فریم، با بررسی آدرس MAC، منبع فریم دریافت شده، توسط سوئیچ.

۳- آماده‌سازی و ارسال یک کپی از فریم به مقصد مورد نظر با ایجاد یک محیط بدون حلقه در شبکه لایه‌ی دوم با استفاده از پروتکل Spanning Tree Protocol.

در شکل ۲-۳ یک قالب از فریم سوئیچ را مشاهده می‌کنید:



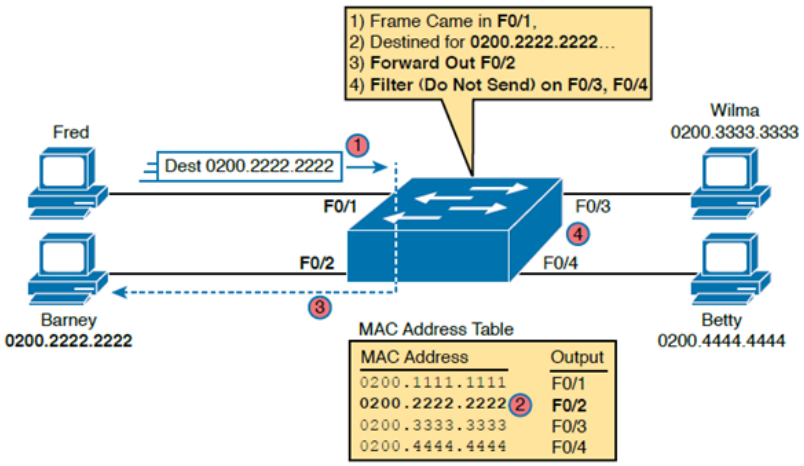
شکل ۲-۳ فریم سوئیچ

همان‌طور که در شکل ۲-۳ مشاهده می‌کنید تمام فریم‌های سوئیچ دارد یک منبع (Source) و مقصد (Destination) یکسان هستند و این دو هر کدام دارای ۶ بایت اطلاعات هستند و مهترین بخش در سوئیچینگ به شمار می‌روند.

هر سوئیچ در شبکه دارای یک جدول است که در آن تمام Mac Addressهای دستگاه‌هایی که به آن متصل شده است قرار دارد.

اگر به شکل ۳-۳ توجه کنید کاربری با نام Fred می‌خواهد اطلاعاتی را به کاربر Barney ارسال کند، اولین کاری که انجام می‌شود این است که سوئیچ مورد نظر جدول Mac خود را بررسی می‌کند و می‌فهمد که آدرس 0200.2222.2222 مربوط به سیستم Barney است و باید اطلاعات را به پورت شماره‌ی F0/2 ارسال کند، با این کار اطلاعات فقط برای فرد مورد نظر (Barney) ارسال شده و پورت‌های 3 , 4 در زمان ارسال فیلتر خواهند شد.

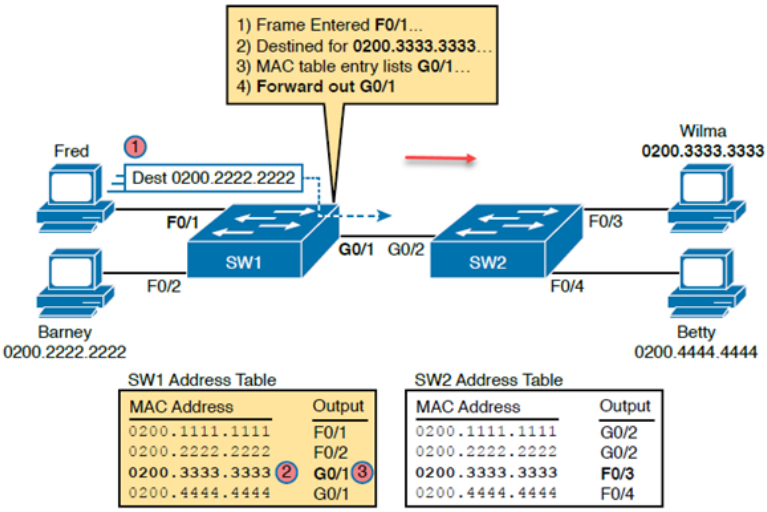
www.takbook.com



شکل ۳-۳ نحوه‌ی ارسال اطلاعات در سوئیچ

اگر از دو سوئیچ در شبکه‌ی خود استفاده کنید، تفاوتی با قسمت قبل ندارد، به خاطر اینکه تمام سوئیچ‌ها دارای جدول MAC هستند و این جداول را بین هم به اشتراک می‌گذارند.

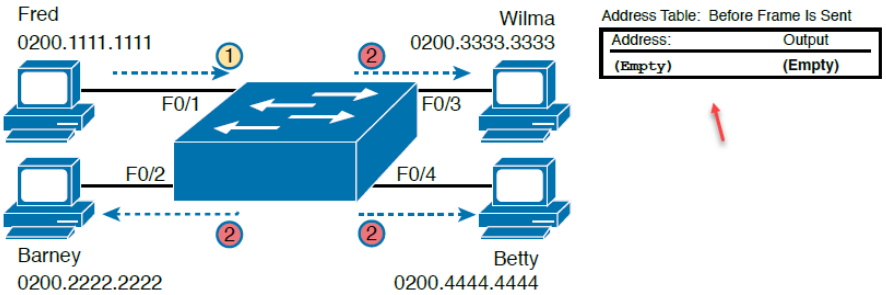
اگر به مانند شکل ۴-۳ کاربر Fred بخواهد اطلاعاتی را به کاربر Wilma ارسال کند سوئیچ SW1 از موقعیت MAC آدرس کاربر Wilma در جدول خود باخبر شده و اطلاعات یا همان فریم مورد نظر را به پورت G0/1 که پورتی است که به سوئیچ SW2 متصل است می‌فرستد و در سوئیچ SW2 طبق جدولی که وجود دارد اطلاعات از طریق پورت F0/3 به کاربر Wilma می‌رسد.



شکل ۴-۳ نحوه‌ی ارسال اطلاعات در سوئیچ

www.takbook.com

حالت دیگری در سوئیچ وجود دارد به نام Broadcast که در این حالت اگر سیستمی بخواهد برای کل سیستم‌هایی که در شبکه وجود دارد اطلاعات ارسال کند، به مانند شکل۵-۳ فریمی که کاربر Fred ارسال می‌کند سوئیچ این فریم را به کل پورت‌های خود ارسال می‌کند.



شکل ۵-۳ نحوه‌ی ارسال اطلاعات در سوئیچ

۱-۳ کار با سوئیچ لایه‌ی دوم

سوئیچ‌ها در لایه‌ی دوم مدل OSI کار می‌کنند. سوئیچ‌ها در انواع مختلف ۸، ۱۶، ۲۴، ۴۸ پورت وجود دارد که با استفاده از آدرس Mac ترافیک را در شبکه انتقال می‌دهند که همین امر این دستگاه را با Hub متمایز کرده است، البته Bridge هم نوعی سوئیچ است، اما با پورت‌های کمتر.

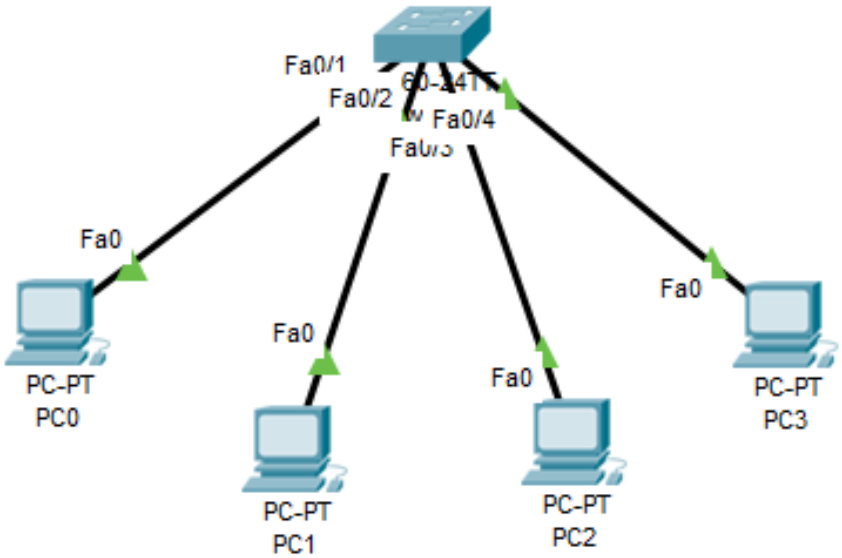
در شکل ۶-۳ یک سوئیچ ۴۸ پورت سیسکو را مشاهده می‌کنید که در لایه دوم مدل OSI کار می‌کند.

شکل ۶-۳ سوئیچ سیسکو

همانطور که بیان کردیم، سوئیچ‌ها از یک جدول استفاده می‌کنند که تمام آدرس‌های MAC دستگاه‌های متصل به خود را در آن جای می‌دهند و از طریق آن کار آدرس‌دهی را انجام می‌دهند.

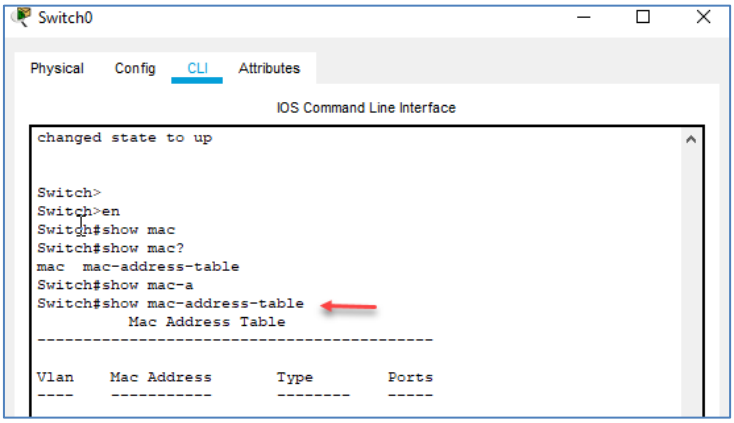
نرم‌افزار Packet tracer را باز کنید و به مانند شکل ۷-۳ یک سوئیچ لایه‌ی دو مانند سری ۲۹۶۰ به همراه چهار Pc به صفحه اضافه کنید.

www.takbook.com



شکل ۷-۳ بررسی سوئیچ لایه‌ی دوم

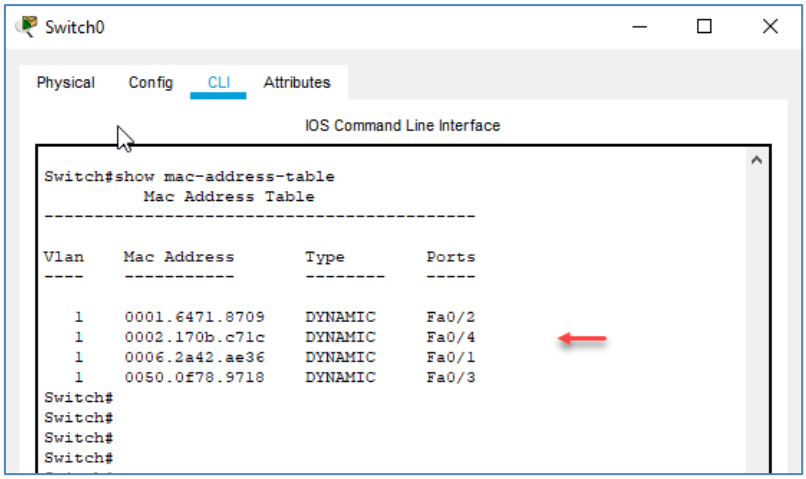
بعد از متصل کردن PCها به سوئیچ مورد نظر، اگر به مانند شکل ۸-۳ وارد سوئیچ شوید و دستور Show mac-address-table را وارد کنید، هیچ MAC آدرسی در لیست وجود نخواهد داشت و در لحظه‌ی اول جدول MAC خالی است.



شکل ۸-۳ تنظیمات سوئیچ

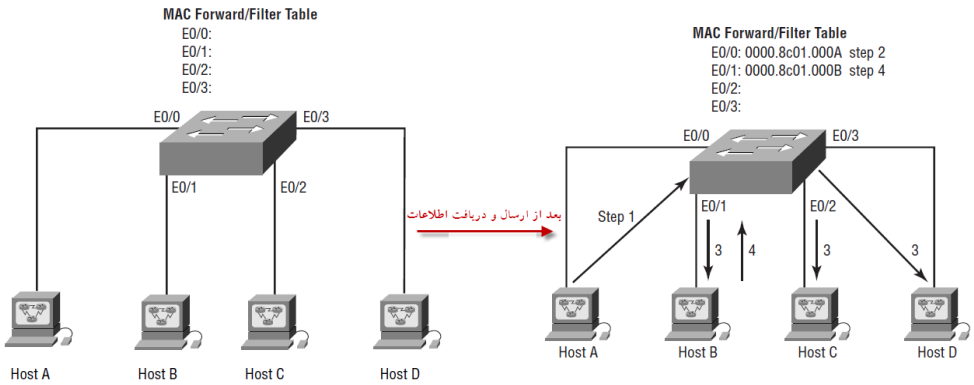
اما اگر در هر Pc یک آدرس IP تنظیم کنید، با این کار یک فریم به سوئیچ ارسال شده و باعث می‌شود که آدرس MAC سیستم‌ها در جدول سوئیچ قرار بگیرد، با این کار سوئیچ به جدول خود نگاهی می‌کند و وقتی مشاهده کرد که آدرس mac این pcها در داخل جدول قرار ندارد آن را در جدول ثبت می‌کند، که این موضوع را در شکل ۹-۳ مشاهده می‌کنید.

www.takbook.com



شکل ۹-۳ تنظیمات سوئیچ

طبق شکل ۱۰-۳، Host A بعد از ارسال اطلاعات Mac آدرس آن در جدول سوئیچ ثبت شد و بعدی Host B است که به محض دریافت اطلاعات، Mac address آن‌هم در جدول سوئیچ ثبت شد و به همین ترتیب این کار ادامه می‌یابد که این موضوع را در شکل ۱۰-۳، مشاهده می‌کنید.



شکل ۱۰-۳ تنظیمات سوئیچ

توجه کنید که سوئیچ برای اینکه برای اولین بار جدول خود را تکمیل کند از Broadcast برای آگاهی از تمام آدرس‌های Mac شبکه استفاده می‌کند و بعد از تکمیل جدول، ارتباط دستگاه‌ها به صورت Unicast انجام می‌شود که این یک ویژگی سوئیچ است و آن را از Hub متمایز می‌کند، مثلاً اگر در شکل ۱۰-۳، Host A بخواهد اطلاعات را به Host D بفرستد، چون سوئیچ از آدرس Mac، Host D خبری ندارد، این پیام

www.takbook.com

را به صورت Broadcast به همه‌ی pc های متصل به سوئیچ ارسال می‌کند و وقتی این کار را انجام داد، تک‌تک آدرس‌های Mac مربوط به pcها در جدول سوئیچ ثبت می‌شوند.

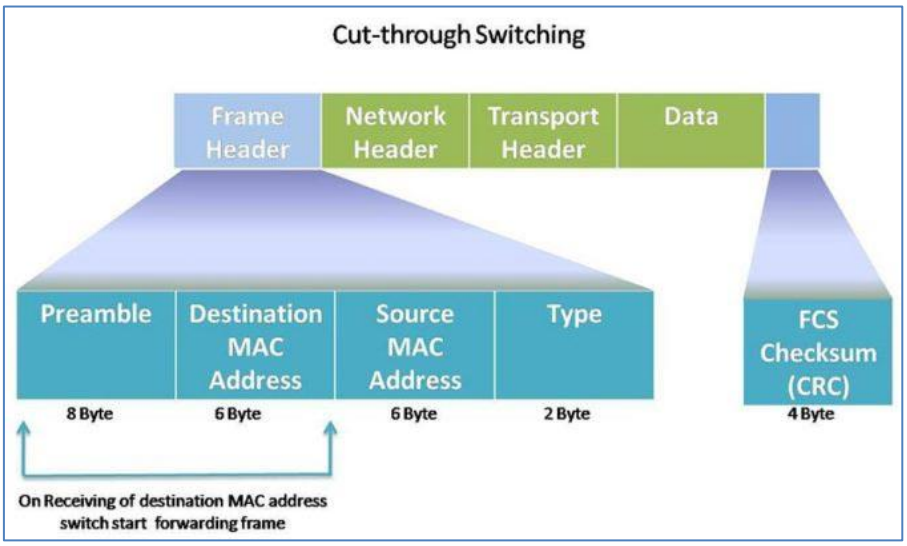
توجه داشته باشید که وقتی Host A بخواهد به Host B اطلاعات ارسال کند، سوئیچ فقط به پورتی که Host B به آن متصل است اطلاعات را ارسال می‌کند و به پورت‌های دیگر کاری ندارد که به این روش، فیلتر کردن فریم‌ها هم گفته می‌شود که در قسمت‌های قبلی آن را بررسی کردیم.

۳-۲ روش‌های انتقال فریم (LAN Switch Types)

سوئیچ از سه روش برای انتقال فریم (اطلاعات) در شبکه استفاده می‌کنند که هرکدام را باهم مورد بررسی قرار می‌دهیم.

۳-۲-۱ روش اول Cut-through (FastForward)

در این روش زمانی که سوئیچ فریمی را که مربوط به یک pc باشد را دریافت کند، سریع آن را از طریق جدول Mac خود به طرف پورت (destination) مورد نظر ارسال می‌کند، این روش بسیار سریع است، چون آدرس مقصد (destination) را در سوئیچ به صورت کامل مورد بررسی قرار نمی‌دهد، یعنی وقتی‌که یک آدرس MAC وارد سوئیچ شد دو قسمت اول مورد بررسی قرار می‌گیرد و سریع به آدرس مقصد ارسال می‌شود که این موضوع را در شکل ۳-۱۱ مشاهده می‌کند.

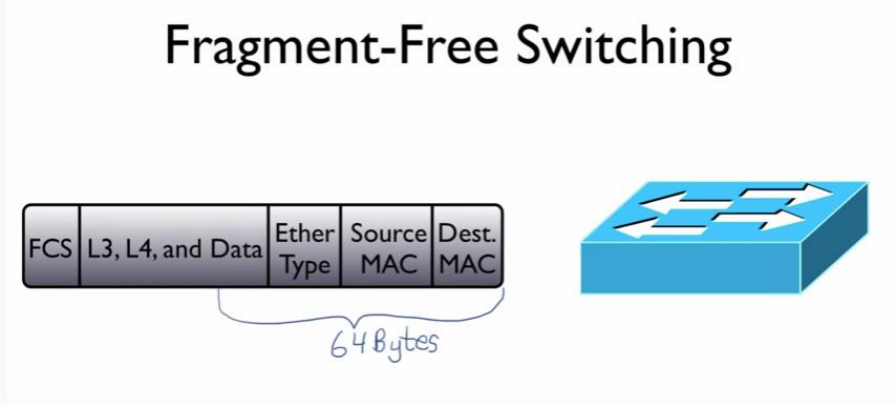


شکل ۳-۱۱ روش Cut-through

www.takbook.com

۳-۲-۲ روش دوم FragmentFree (modified cut-through)

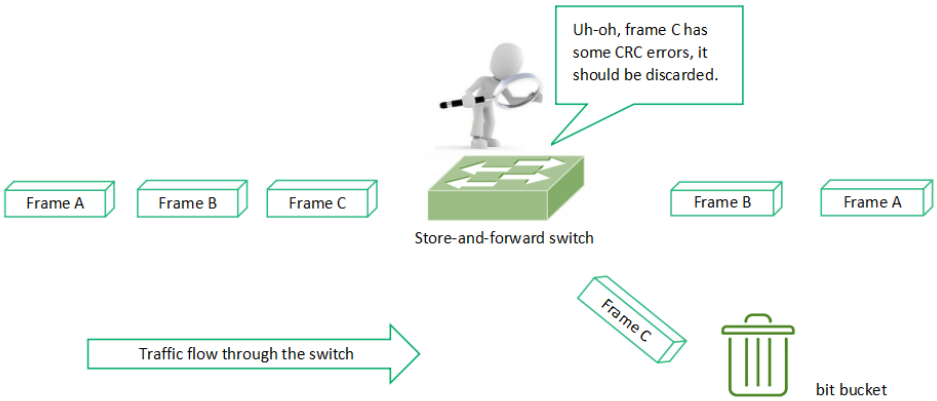
در این روش که کمی سرعت آن به نسبت روش قبلی کمتر است و اصلاح‌شده‌ی روش قبلی است، ۶۴ بیت اول MAC آدرس مقصد (Destination) در سوئیچ مورد بررسی قرار می‌گیرد و از نظر خطا چک می‌شود و اگر مشکلی نداشت به طرف آدرس مقصد ارسال می‌شود، که شکل ۱۲-۳ نمایانگر این موضوع است.



شکل ۱۲-۳ روش *FragmentFree*

۳-۲-۳ روش سوم Store-and-forward

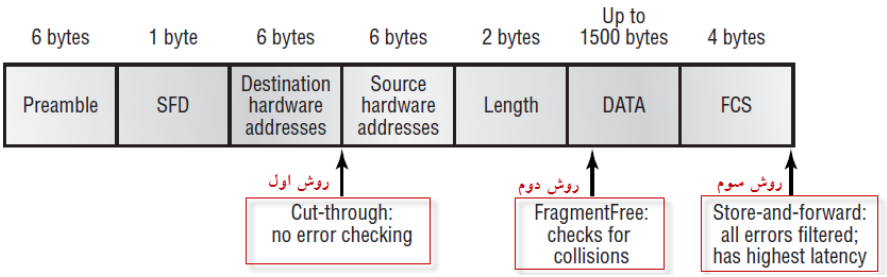
در این روش فریم مورد نظر به صورت کامل دریافت و Buffer می‌شود و در صورتی که الگوریتم CRC خطایی را تشخیص ندهد به آدرس مقصد مورد نظر ارسال می‌شود که البته اگر خطایی داشته باشد، این فریم پس زده می‌شود که این موضوع را در شکل ۱۳-۳ مشاهده می‌کنید.



شکل ۱۳-۳ روش *Store-and-forward*

www.takbook.com

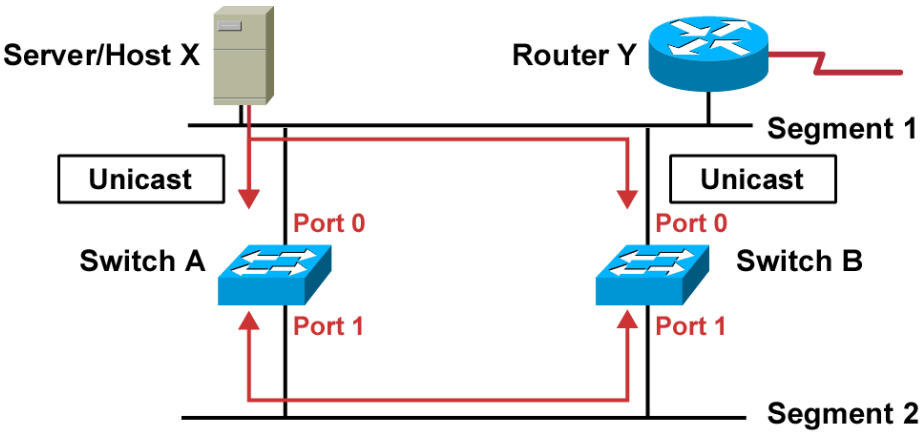
به شکل ۱۴-۳ توجه کنید، این شکل (Frame) هر سه حالت را برای شما نمایش می‌دهد.



شکل ۱۴-۳ *Frame*

۳-۳ بررسی Loop در سوئیچ

به شکل ۱۵-۳ توجه کنید.



شکل ۱۵-۳ بررسی *Loop* در سوئیچ

در شکل ۱۵-۳، Server X در حال ارسال Frame به Router Y است که یک مشکل در سر راه وجود دارد و آن‌هم این است که سوئیچ A و B از دو مسیر مختلف، آدرس MAC سرور X را در جدول خود ثبت کردند و زمانی که بخواهد یک فریم را به روتر مورد نظر ارسال کنند، به علت یکسان بودن فریم دچار بار اضافه در شبکه می‌شوند و در اصطلاح Loop ایجاد می‌شود.

www.takbook.com

۱-۳-۳ روش‌های جلوگیری از loop

STP(Spanning Tree Protocol)
پروتکل STP توسط سازمان IEEE با شماره‌ی 802.1D استاندارد شده است و شرکت سازنده‌ی آن DCE است.

کار این پروتکل این است که وقتی شبکه در Loop قرار می‌گیرد، بعضی از interfaceهای اضافه را خاموش می‌کند و فقط به یک طرف اجازه‌ی ارسال و دریافت اطلاعات می‌دهد.

این پروتکل از الگوریتمی به نام STA (Spanning Tree Algorithm) برای این کار استفاده می‌کند که کار این الگوریتم به این صورت است که کل ساختار شبکه را به صورت یک درخت درآورده و جاهایی را که Loop در آن ایجاد شده، مهار می‌کند. در شکل ۱۶-۳، ۲ سوئیچ با دو لینک به هم متصل شده‌اند و پروتکل STP برای جلوگیری از Loop، یکی از لینک‌ها را از رده خارج کرده است.

شکل ۱۶-۳ مثالی از STP

در این قسمت می‌خواهیم الگوریتم STA را با هم بررسی کنیم، اما قبل از آن باید اجزای آن را مورد بررسی قرار دهیم و از عملکرد آنها مطلع شویم:

Bridge ID
شناسه‌ای است برای تمایز دادن سوئیچ‌ها در پروتکل STP، پس می‌توان گفت با کمک این شناسه، سوئیچ‌ها در یک شبکه قابل تشخیص هستند و اجزای تشکیل‌دهنده‌ی Bridgr Id دو چیز است:

- **Priority**: عددی است روی سوئیچ‌های شرکت سیسکو قرار دارد و به صورت پیش‌فرض ۳۲۷۶۹ است.
- **Mac Address**: آدرس Mac پورت مورد نظر در سوئیچ است.

پس Bridge ID، جمع این دو گزینه می‌شود.
به شکل ۱۶-۳ توجه کنید؛ در سوئیچی که پروتکل STP روی آن اجرا شده است (که با جهت‌نما آن را مشخص کردیم) در مد Privileged دستور زیر را وارد کنید:

Switch# **show spanning-tree**

www.takbook.com


```
VLAN0001
Spanning tree enabled protocol ieee
Root ID    Priority    32769
Address     0001.C9A6.90A3
Cost       19
Port       1(FastEthernet0/1(

Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1(

Address     0090.0C6C.EE69
Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------------------------- -------- --------- --- ---- ----------------

Fa0/1            Root FWD 19        128.1    P2p
Fa0/2            Altn BLK 19        128.2    P2p
Fa0/3            Desg FWD 19        128.3    P2p
```

این اعداد به رنگ قرمز در نتیجه مشخص شده‌اند.

Root Bridge

برای انتخاب یک سوئیچ به عنوان root Bridge تمام Bridge IDهای مختلف سوئیچ‌ها باهم مقایسه می‌شوند و هرکدام که کوچک‌تر بود، همان سوئیچ به عنوان Root Bridge انتخاب می‌شود.

BPDU

فریمی در سوئیچ است که برای انتقال اطلاعات بین سوئیچ‌ها کاربرد دارد و یکی دیگر از ویژگی‌های آن این است که تغییر ساختار شبکه را خیلی سریع به دیگر سوئیچ‌ها در شبکه اطلاع می‌دهد.

Root Port

پورتی است که ارتباط مستقیم با Root Bridge دارد و از طریق آن انتخاب می‌شود.

Designated port

پورتی از سوئیچ است که به عنوان Forwarding انتخاب می‌شود و کار ارسال و دریافت اطلاعات را انجام می‌دهد.

NonDesignated port

برای جلوگیری از loop این پورت shutdown می‌شود.

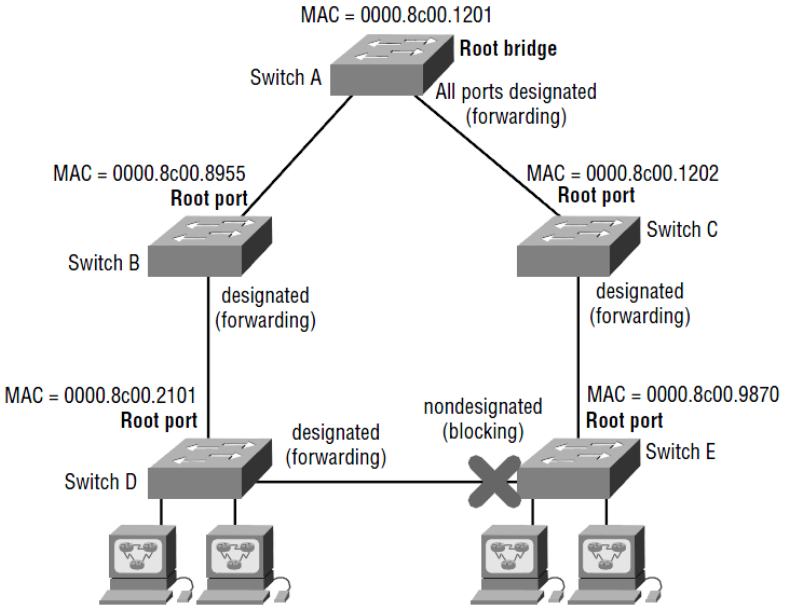
۲-۳-۳ نحوه‌ی کارکرد الگوریتم STA

الگوریتم STA در هر سوئیچ Bridge ID را محاسبه می‌کند و بعد، از طریق BPDU آن را در شبکه تبلیغ می‌کند، بعد Bridge ID خود را با دیگر سوئیچ‌ها مقایسه می‌کند، اگر Bridge ID خودش کمتر از دیگران

www.takbook.com

باشد، Bridge ID خود را در شبکه تبلیغ می‌کند، اما اگر یکی کمتر از خود را پیدا کند آن را در قالب فریم BPDU به دیگر سوئیچ‌ها اعلام می‌کند تا در آخر کار بعد از مقایسه، کمترین Bridge ID به دست آید که آخرین سوئیچ با کمترین Bridge Id به عنوان Root Bridge انتخاب می‌شود. بعد از این کار، نوبت به انتخاب وضعیت پورت‌ها است که چه پورتی در چه وضعیتی قرار دارد.

در شکل ۱۷-۳، تمام مراحل بالا وجود دارد. اگر به شکل توجه کنید، Switch A به علت کوچک‌تر بودنMac Address نسبت به بقیه‌ی سوئیچ‌ها، به عنوان Root bridge انتخاب شده است و هر دو پورت آن به حالت Forwarding رفته است. پورت‌های سوئیچ‌های B و C که به سوئیچ A متصل هستند به عنوان Root Port انتخاب شده‌اند. پورت بعدی سوئیچ‌های B و C به عنوان پورت Forwarding انتخاب شده‌اند و به همین ترتیب بقیه‌ی پورت‌ها انتخاب می‌شوند. برای جلوگیری از loop یکی از پورت‌های سوئیچ E به حالت Nondesignated رفته و Block شده است که البته این پورت به نسبت پورت دیگر دارای cost بیشتر و پهنای باند کمتری بوده است.



شکل ۱۷-۳ مثالی از STP

پس اگر مراحل کار الگوریتم STA را طبق مراحل زیر در نظر بگیریم، متوجه‌ی کار این الگوریتم خواهیم شد.

۱. سوئیچ‌ها، Bridge ID خود را مشخص می‌کنند.
۲. در این مرحله، هر سوئیچ Bridge ID خود را تحت فریم BPDU به دیگر سوئیچ‌ها تبلیغ می‌کند تا پایین‌ترین Bridgr ID مشخص شود و بعدازآن، Root Bridge مشخص می‌شود.

www.takbook.com

۳. باید Designated Port انتخاب شود که پورت‌های متصل به سوئیچ Root Bridge به عنوانDesignated Port انتخاب می‌شوند و کار ارسال و دریافت اطلاعات را انجام می‌دهند. در بین دو سوئیچ هم پورتی که کمترین cost را داشته باشد، به عنوان Designated Port انتخاب می‌شود.
۴. در این مرحله که مرحله‌ی مهمی است در آن قسمت که loop ایجاد می‌شود، یکی از پورت‌ها که پهنای باند کمتر و Cost بیشتر داشته باشد، به عنوان پورت NonDesignated Port انتخاب و Block می‌شود. اگر چنانچه هر دو فاکتور پهنای باند و cost یکی باشد، معیار انتخاب Bridge ID بزرگ‌تر است.

هر پورت سوئیچ دارای پنج وضعیت است:

Blocking
وقتی سوئیچ روشن می‌شود، همه‌ی پورت‌های آن در حالت Block قرار دارند و منتظر هستند تا فریم BPDU به آن‌ها برسد تا وضعیت خود را تغییر دهند.

Listening
در این وضعیت سوئیچ بر طبق فریم‌های BPDU، سوئیچ Root Bridge را انتخاب می‌کند.

Learning
این وضعیت بعد از وضعیت Listening اجرا می‌شود و تمامی مسیرهای موجود در شبکه که در loop قرار ندارد را شناسایی می‌کند. به این موضوع توجه کنید که در وضعیت Listening اگر Mac address جدید به سوئیچ برسد، سوئیچ در جدول آن را ثبت نمی‌کند، اما اگر به وضعیت Learning برسد در جدول خود ثبت می‌کند. در این مرحله، پورت‌های Root Port و Designated Port مشخص می‌شوند.

Forwarding
یک پورت زمانی به این حالت می‌رود که وضعیت قبل را طی کرده باشد، در این حالت، پورت قادر به دریافت و ارسال اطلاعات می‌کند.

Blocking
این حالت زمانی رخ می‌دهد که یک پورت برای جلوگیری از Loop در شبکه باید به حالت Blocking برود، البته در این حالت، پورت Shutdown نمی‌شود، بلکه منتظر فریم‌های BPDU می‌نشیند که اگر تغییری در شبکه رخ داد، دوباره به حالت دیگر تغییر وضعیت دهد.

Disable:
این پورت به صورت دستی توسط مدیر شبکه، shutdown شده است و تا زمانی که توسط مدیر روشن نشود کارایی نخواهد داشت.

www.takbook.com

بررسی چراغ‌های تعبیه شده بر روی سوئیچ:

روی سوئیچ‌ها به ازای هر پورتی که وجود دارد، یک چراغ چشمک‌زن هم وجود دارد که این چراغ به رنگ‌های مختلف نمایانگر می‌شود که هر رنگ آن را باهم مورد بررسی قرار می‌دهیم:

جدول ۱-۳ چراغ‌های سوئیچ

سبز	به این پورت کابلی متصل شده است، اما فعال نشده است.
سبز چشمک‌زن	این پورت فعال و در حال ارسال و دریافت اطلاعات است.
سبز و کهربایی	در این حالت یک collision در سوئیچ رخ داده است.
کهربایی	در این حالت پورت Disable شده، اما به صورت دستی.
off	به پورت کابلی متصل نشده است.

چراغ‌های دیگری هم وجود دارد که در زیر آنهارا بررسی می‌کنیم:

UTL LED: این چراغ‌ها نشان‌دهنده‌ی پهنای باند مصرفی در سوئیچ می‌باشند.

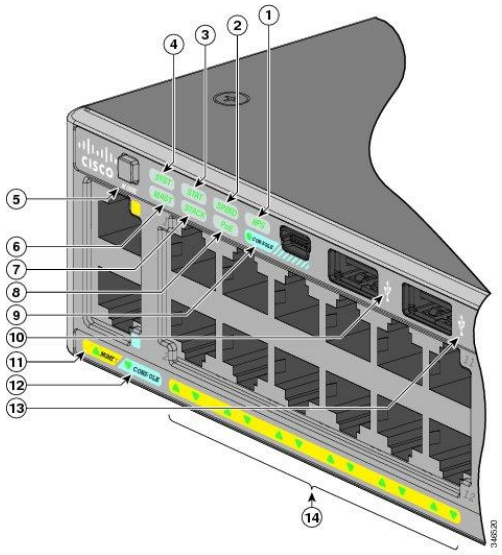
STST LED: زمانی که سوئیچ روشن شود، این چراغ هم روشن می‌شود.

FDUP LED: در این حالت پورت‌ها در دو حالت Half-duplex و Full-duplex قرار دارند و اگر چراغ پورت خاموش باشد، یعنی در حالت Half-duplex قرار دارد و اگر روشن باشد و سبز در حالت Full-duplex قرار دارد.

100 یا Speed Led: این چراغ نشان‌دهنده‌ی سرعت یک پورت است که اگر خاموش باشد، یعنی از ۱۰ مگابایت استفاده می‌کند و اگر روشن و سبز باشد، یعنی از حداکثر سرعت استفاده می‌کند.

در شکل ۱۸-۳ یک شمای کلی از جلوی سوئیچ مدل 2960X را مشاهده می‌کنید که شامل چراغ‌ها و پورت‌های مشخص است که در جدول زیری آن همه چیز مشخص شده است.

www.takbook.com



شکل ۱۸-۳ چراغ‌های تعبیه شده بر روی سوئیچ

جدول ۲-۳ اطلاعات چراغ‌های سوئیچ

شماره	توضیحات
۱	چراغ RPS است که مربوط به پاور سوئیچ است و برای Redundancy کاربرد دارد، یعنی اینکه اگر بر روی سوئیچ از دو پاور هم‌زمان استفاده کنید این چرا غ به کار می‌رود
۲	چراغ SPEED LED نشان‌دهنده‌ی سرعت یک پورت است که اگر خاموش باشد، یعنی از ۱۰ مگابایت استفاده می‌کند و اگر روشن و سبز باشد، یعنی سرعت آن ۱۰۰ مگابایت است و در آخر اگر چراغ سبز خاموش روشن می‌شود سرعت آن از ۱۰۰ تا ۱۰۰۰ مگابایت است.
۳	چراغ STAT LED زمانی که سوئیچ روشن شود، این چراغ هم روشن می‌شود.
۴	چراغ SYS LED اگر روشن نباشد یعنی سوئیچ خاموش است، اگر سبز باشد یعنی سوئیچ در حالت نرمال قرار دارد، اگر در حالت چشمک زن قرار داشته باشد یعنی اینکه سوئیچ در حال اجرای نرم‌افزار است، اگر رنگ آن به کهربایی تغییر کند یعنی اینکه دستگاه در حال اجرا و دریافت نیرو است اما به درستی کار نمی‌کند و در آخر اگر چراغ به صورت کهربایی و چشمک زن باشد یعنی اینکه در شبکه، تامین نیرو و یا ماژول فن مشکل وجود دارد.
۵	دکمه Mode هم برای ریسیت کردن سوئیچ به کار می‌رود که بعد از ریست به حالت Setup Mode خواهد رفت، فقط توجه داشته باشید برای فعال کرن آن باید دکمه را چند ثانیه نگه دارید.

www.takbook.com

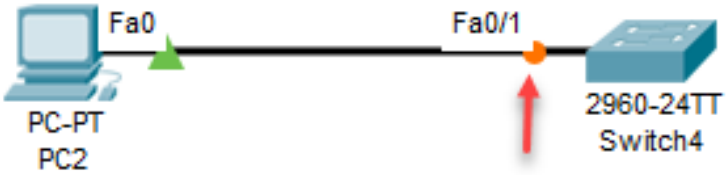
۶	سوئیچ Master به سوئیچی گفته می‌شود که در یک مجموعه به صورت اتوماتیک اطلاعات IOS را بین اعضای جدید اعمال می‌کند یعنی با این کار وقتی یک سوئیچ می‌خواهد به مجموعه‌ای اضافه شود هیچ افتی در سرعت کار پیش نخواهد آمد. چراغ Master LED اگر خاموش باشد یعنی اینکه سوئیچ Master نیست، اگر سبز باشد یعنی اینکه یک سوئیچ Master است.
۷	چراغ STACK نشان دهنده‌ی این است که سوئیچ مورد نظر در یک STACK قرار دارد که این مجموعه‌ی STACK می‌تواند شامل ۸ سوئیچ باشد.
۸	چراغ POE نشان دهنده‌ی این است که پورت مورد نظر فعال شده است، این نوع پورت‌ها دارای برق هم هستند و بیشتر برای دوربین‌های مدار بسته مورد استفاده قرار می‌گیرند، در فصل دوازدهم در مورد این پورت به صورت مفصل بحث خواهیم کرد.
۹	چراغ USB mini-Type B console port زمانی فعال خواهد شد که از کابل Console دستگاه استفاده کنید.
۱۰	پورت USB Type A
۱۱	پورت MGMT یا پورت مدیریتی
۱۲	چراغ CONSOLE
۱۳	پورت USB Type A
۱۴	چراغ تمام پورت‌های سوئیچ که در هر ردیف دو چراغ وجود دارد که چراغ سمت چپ برای پورت بالایی و سمت راست برای پورت پائینی.

۳-۳-۳ بررسی قابلیت PortFast

اگر یک سوئیچ سیسکو را از نزدیک دیده باشید متوجه خواهید شد که زمانی که یک کلاینت یا هر دستگاهی به آن متصل می‌شود مدت زمانی را طول خواهد کشید (۳۰ ثانیه) تا همگرایی با دستگاه مورد نظر انجام شود، ولی این زمان می‌توانند در بعضی موارد اذیت کننده باشد و برای یک سیستم که فقط برای استفاده از منابع شبکه به سوئیچ متصل می‌شود نیاز به این مقدار زمان نیست و می‌توان این زمان را برای آن حذف کرد.

به مانند شکل ۱۹-۳ یک سوئیچ و یک PC را به صفحه اضافه کنید، وقتی از طریق کابل آنها را به هم متصل می‌کنید به صورت پیش‌فرض مدت زمان ۳۰ ثانیه نیاز است تا چراغ زرد رنگ تبدیل به رنگ سبز و فعال شود، برای اینکه این مقدار زمان را کاهش دهیم باید دستوراتی را در سوئیچ وارد کنید.

www.takbook.com



شکل ۱۹-۳ مثالی از STP

وارد سوئیچ مورد نظر شوید و دستور زیر را وارد کنید:

Switch(config)#**interface fastEthernet 0/1**
Switch(config-if)#**spanning-tree portfast**

با دستور بالا وارد پورت FastRthernet 0/1 شدیم و دستور Portfast را بر روی آن فعال کردیم و بعد از آن هر سیستمی که به این پورت متصل شود یک ارتباط بسیار سریع شکل خواهد گرفت.

اما اگر بخواهید این دستور بر روی تمام پورت‌های سوئیچ مورد نظر شما اجرا شود باید دستور زیر را در مد Global وارد کنید:

Switch(config)#**spanning-tree portfast default**

نکته مهم:

زمانی که یک پورت در حالت PortFast باشد پروتکل STP بر روی آن اعمال نخواهد شد و اگر به جای یک PC یک سوئیچ قرار گیرد می‌تواند با ارسال بسته‌های BPDU شبکه را از کار بیندازد، برای جلوگیری از آن باید از قابلیت BPDU Guard استفاده کنید، BPDU Guard یکی از ویژگی‌های سوئیچ‌های سیسکو است که اگر فرد مهاجم بخواهد از طریق یک پورت سوئیچ به شبکه بسته‌های BPDU بفرستد با اجرای این دستور در پورت مورد نظر اگر چنانچه سوئیچ به آن پورت متصل شود و بخواهد فریم BPDU ارسال کند، با فعال بود BPDU Guard، پورت مورد نظر خاموش خواهد شد.

۴-۳-۳ بررسی RSTP در سوئیچ‌های سیسکو

یک پروتکل سریعتر به نسبت STP است، RSTP یا Rapid Spanning Tree Protocol دارای شماره‌ی استاندارد IEEE 802.1w است و این پروتکل با تغییراتی که بر روی آن ایجاد شده است، سرعت کار بسیار افزایش پیدا کرده و پیدا کردن LOOP و خرابی لینک‌ها به سرعت انجام می‌شود.

فرایندی در RSTP با نام Proposal and Agreement وجود دارد که با استفاده از آن Interface که فعال شود سریع شروع به کار خواهد کرد و پورت مورد نظر سریع به حالت Forwarding می‌رود.

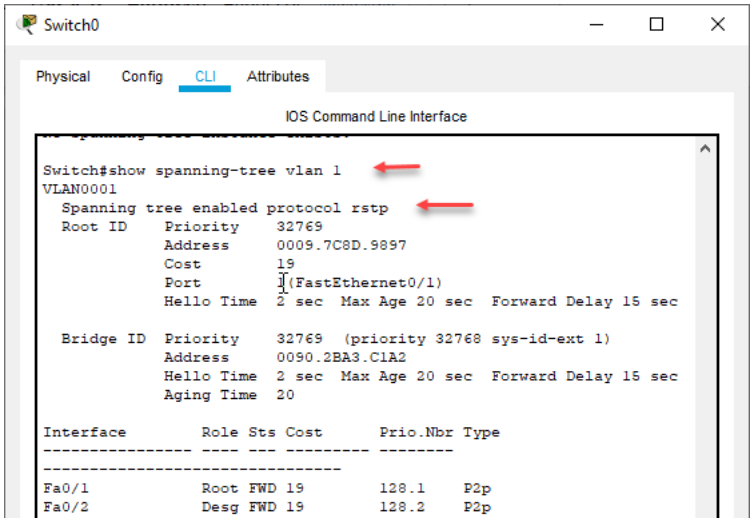
www.takbook.com

اگر یادتان باشد در پروتکل STP پنج حالت را با هم بررسی کردیم، که شامل Disabled, Blocking, Listening ، Learning, Forwarding بوده ولی در پروتکل بهبود یافته RSTP سه حالت اول یعنی (Disabled, Blocking, Listening) به یک حالت تغییر کرده است و نام آن هم Discarding است و دو حالت Learning, Forwarding هم در آن وجود دارد.

در زیر نحوه راه‌اندازی این پروتکل را بررسی می‌کنیم:

switch#**configure terminal**
switch(config)#**spanning-tree mode rapid-pvst**

بعد از فعال کردن پروتکل RSTP با دستور Show spanning-tree vlan 1 می‌توانید در شکل ۲۰-۳ مشاهده کنید که پروتکل مورد نظر فعال شده است، البته به جای VLAN شماره‌ی یک می‌توانید شماره‌ی VLAN مورد نظر خود را وارد کنید.



شکل ۲۰-۳ نتیجه دستور Show spanning-tree vlan 1

پس یکی از دلایلی که سازمان IEEE دست به طراحی RSTP زد این بود که همگرایی یا Convergence پروتکل STP با تنظیمات پیش‌فرض ۵۰ ثانیه است که این زمان در پروتکل RSTP به ۱۰ ثانیه کاهش یافته است که این زمان واقعاً سرعت شبکه را در مقیاس بزرگ افزایش خواهد داد.

در جدول ۳-۳، لیست پورت‌های پروتکل RSTP را مشاهده می‌کنید:

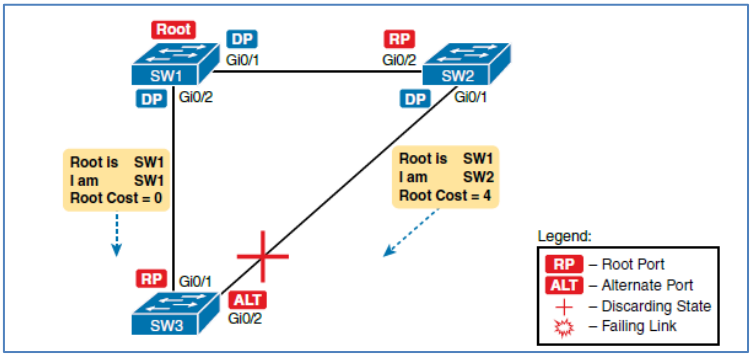
جدول ۳-۳ بررسی پروتکل RSTP

نقش پورت	عملیات

www.takbook.com

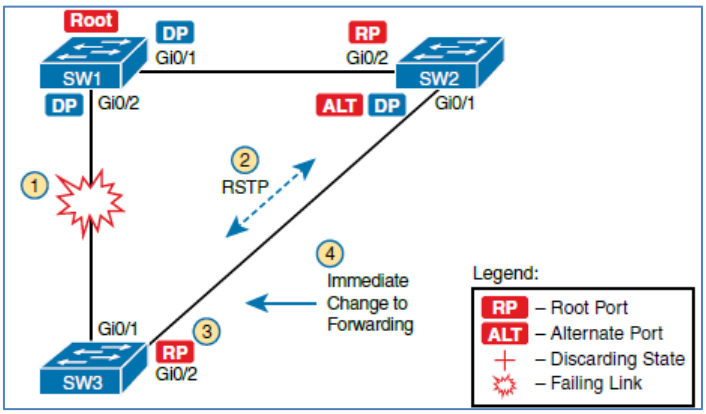
Root port	بهترین مسیر برای رسیدن به سوئیچ root است.
Alternate port	بهترین مسیر جایگزین root port است و در صورت خرابی Root Port این مسیر جایگزین خواهد شد.
Designated port	پورتی از سوئیچ است که به عنوان Forwarding انتخاب می‌شود و کار ارسال و دریافت اطلاعات را انجام می‌دهد.
Backup port	یک مسیر پشتیبان برای Designated port است که در صورت خرابی آن، فعال خواهد شد.
Disabled port	غیر فعال شدن پورت

در شکل ۲۱-۳ سه سوئیچ را مشاهده می‌کنید که Root Port و Alternate Port آن مشخص شده است.



شکل ۲۱-۳ بررسی پروتکل RSTP

اگر پورت Gi0/1 مربوط به سوئیچ SW3 که به پورت Gi0/2 سوئیچ SW1 متصل است خراب شود، نحوه‌ی همگرایی توسط پروتکل RSTP مشخص شده است که پورت Gi0/1 غیر فعال و Gi0/2 در سوئیچ SW3 فعال خواهد شد، که در شکل ۲۲-۳ نتیجه‌ی کار را مشاهده می‌کنید.

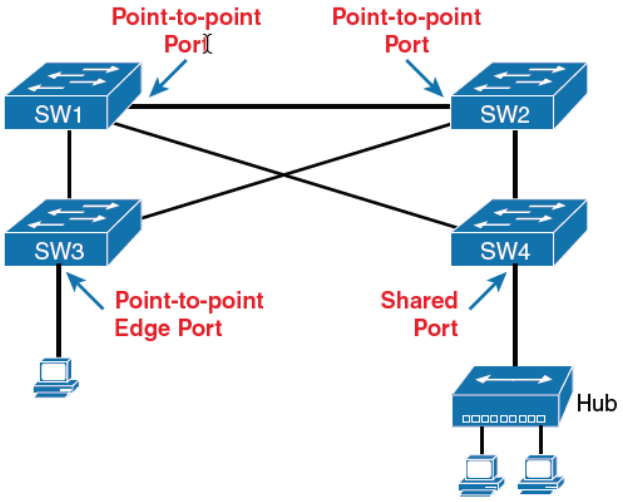


شکل ۲۲-۳ بررسی پروتکل RSTP

www.takbook.com

نکته مهم در پروتکل RSTP این است که زمانی‌که تشخیص دهد یک PC به سوئیچ متصل است آن پورت را به حالت Edge Port تبدیل می‌کند و قابلیت PortFast را روی آن فعال می‌کند، با این کار بسته‌های BPDU دیگر از این پورت دریافت نخواهد شد، اما اگر بر روی یک پورت یک سوئیچ دیگر متصل باشد آن پورت را تبدیل به P2P یا Point to Point می‌کند و بسته‌های BPDU از آن پورت دریافت خواهد شد، این موضوع باعث شده است که سرعت همگرایی به شدت افزایش پیدا کند.

اگر بخواهیم در مورد پورت‌های پروتکل RSTP اشاره‌ای داشته باشیم، می‌توانید شکل ۲۳-۳ را مشاهده کنید که نشان دهنده نحوه ارتباط و نام پورت‌ها است.



شکل ۲۳-۳ بررسی پروتکل RSTP

۳-۴ انواع مد در سوئیچ

سوئیچ از انواع مد در ios استفاده می‌کند که دقیقاً شبیه به روتر است و هیچ فرقی با روتر ندارد.

User Mode

این مد اولین مدی است که وارد سوئیچ می‌شویم و سطح دسترسی آن بسیار محدود است و بیشتر برای Monitoring استفاده می‌شود. وقتی وارد سوئیچ می‌شوید، خط فرمان به صورت زیر مشاهده می‌شود:

Switch>

Privileged Mode

www.takbook.com

برای ورود به این مد از دستور Enable استفاده می‌کنیم و برای خروج از این مد از دستور disable، exit، end استفاده می‌کنیم. این مد به نسبت مد User از سطح دسترسی بالاتری برخوردار است. در این مد می‌توانید تعداد اینترفیس‌های سوئیچ و فعال و غیرفعال بودن آن‌ها را مشاهده کنید و بر روی آن می‌توانید رمز عبور تعریف کنید، چون مد مهمی است.

Switch>**Enable**
Switch#

Global Mode

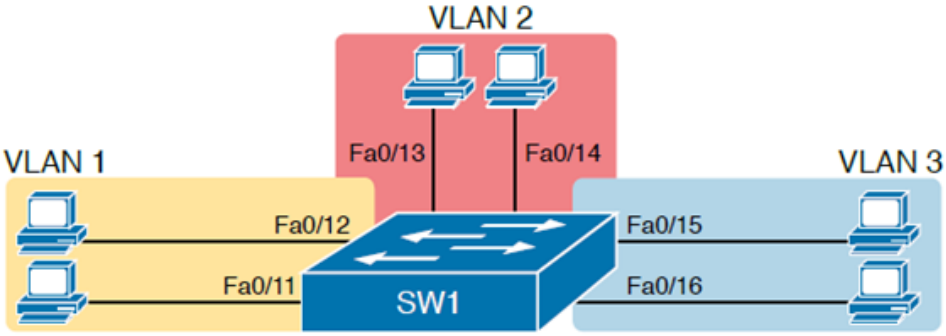
این مد دارای مجوز دسترسی بالایی است، وقتی وارد این مد می‌شوید، می‌توانید تمام تنظیمات سوئیچ را در دست بگیرید و آن‌ها را تغییر دهید. برای ورود به آن، باید از طریق مد Privileged اقدام کنید:

Switch# **Conf terminal**
Switch(Config)#

VLAN (Virtual Link)

وقتی چندین کامپیوتر را به یک سوئیچ متصل می‌کنیم، آن‌ها به راحتی می‌توانند باهم ارتباط داشته باشند و از منابع شبکه استفاده کنند، اما تعداد زیاد کامپیوترها می‌تواند حجم کاری سوئیچ را افزایش دهند، یعنی این‌که تمام سوئیچ‌ها در یک منطقه‌ی کاری باهم در ارتباط هستند و امنیت در این نوع شبکه‌ها بسیار پائین می‌آید، اما می‌توان با تقسیم یک منطقه به چندین منطقه جدا از هم، امنیت را افزایش داد و ترافیک شبکه را به راحتی کنترل کرد.

در شکل ۲۴-۳ سه VLAN را مشاهده می‌کنید که در بر گیرنده‌ی Interfaceهای مشخص هستند که در ادامه در مورد آنها توضیح خواهیم داد.



شکل ۲۴-۳ بررسی پروتکل RSTP

مثال:

شما مدیر شبکه‌ی یک شرکت هستید و این شرکت از ۳ بخش حسابداری، فروش و اداری تشکیل شده است و می‌خواهید این چند اتاق را توسط سوئیچ به هم شبکه کنید که با متصل کردن همه‌ی کامپیوترهای

www.takbook.com

این اتاق‌ها، آن‌ها به هم متصل می‌شوند و می‌توانند به منابع شبکه دسترسی داشته باشند، با این کار ترافیک روی سوئیچ افزایش پیدا می‌کند، چون همه‌ی این کامپیوترها در یک Broadcast Domain قرار دارند و امنیت در این شبکه به خاطر دسترسی همگان به همه‌ی اطلاعات پائین می‌آید. شما که مدیر شبکه هستید، باید کاری انجام دهید که این اتاق‌ها از هم جدا شوند، مثلاً کامپیوتر اتاق حسابداری نتواند با اتاق اداری ارتباط برقرار کند. خوب این کار توسط Vlan انجام می‌شود که همه‌ی کامپیوترهای اتاق حسابداری را می‌توان در یک منطقه قرار داد و باهم در ارتباط باشند و با اتاق‌های دیگر نتوانند در ارتباط باشند با این کار هم امنیت افزایش و هم بار کاری در شبکه کاهش پیدا می‌کند.

۵-۳ کار با VLAN در سوئیچ

برای ایجاد یک VLAN در سوئیچ وارد مد Global شوید و دستور زیر را وارد کنید:

```
Switch(config)# vlan ?
<1-1005>  ISL VLAN IDs 1-1005
```

همان‌طور که در شکل ۲۵-۳ می‌کنید، بعد از تعریف Vlan علامت سؤال قرار دادیم که تعداد Vlanهای قابل ایجاد را نمایش می‌دهد، یعنی می‌توانید از ۱ تا ۱۰۰۵ عدد VLan در یک سوئیچ تعریف کنیم. توجه داشته باشید که VLan 1 را نمی‌توانید ایجاد کنید، چون به صورت پیش‌فرض تمام پورت‌های سوئیچ در این Vlan قرار دارد و به خاطر همین است که تمام پورت‌ها باهم در ارتباط هستند.

اگر دستور show vlan brief را وارد کنید به مانند شکل ۲۵-۳، یک VLAN به شماره‌ی یک را مشاهده می‌کنید که تمام پورت‌های سوئیچ در آن قرار گرفته است.

```
Switch#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                                Gig0/1, Gig0/2
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
Switch#
```

شکل ۲۵-۳ نتیجه دستور show vlan brief

برای تعریف VLAN جدید باید از دستور زیر استفاده کنید:

```
Switch(config)#vlan 20
Switch(config-vlan)#Name Tehran
```

www.takbook.com

در این دستور Vlan شماره‌ی ۲۰ تعریف شده است و بعد از آن، یک اسم از طریق دستور Name به آن نسبت دادیم. برای مشاهده‌ی Vlan که تعریف کردیم و نام این Vlan دوباره از دستور Show استفاده می‌کنیم:

Switch#**show vlan brief**

```
VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                Fa0/21, Fa0/22, Fa0/23, Fa0/24
10   babol                            active
20   Tehran                           active
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005trnet-default                     active
```

همان‌طور که مشاهده می‌کنید، Vlan 20 با نام Tehran تعریف شده است و وضعیت آن فعال است.

اگر بخواهید در مورد شماره‌ی VLAN مشخص شده اطلاعاتی دریافت کنید، می‌توانید از دستور زیر در خط فرمان استفاده کنید:

Switch#**Show vlan id 20**

```
Switch#show vlan id 20

VLAN Name                             Status    Ports
---- -------------------------------- ---------
-------------------------------
20   tehran                           active    Fa0/2

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode
Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- --------
------ ------
20   enet  100020     1500  -      -      -        -    -        0
0

Switch#
```

شکل ۳-۲۶ نتیجه دستور *show vlan brief*

www.takbook.com

۱-۵-۳ قرار دادن پورت در Vlan

برای اینکه پورت‌ها بتوانند در VLAN مورد نظر کار کنند باید آنها را درآن VLAN مشخص شده قرار دهید که این کار به دو صورت انجام می‌پذیرد:

Static

این روش به صورت دستی است و می‌توانیم هر پورتی را در Vlan مورد نظر خود قرار دهید، این روش یکی از امن‌ترین روش‌ها است.

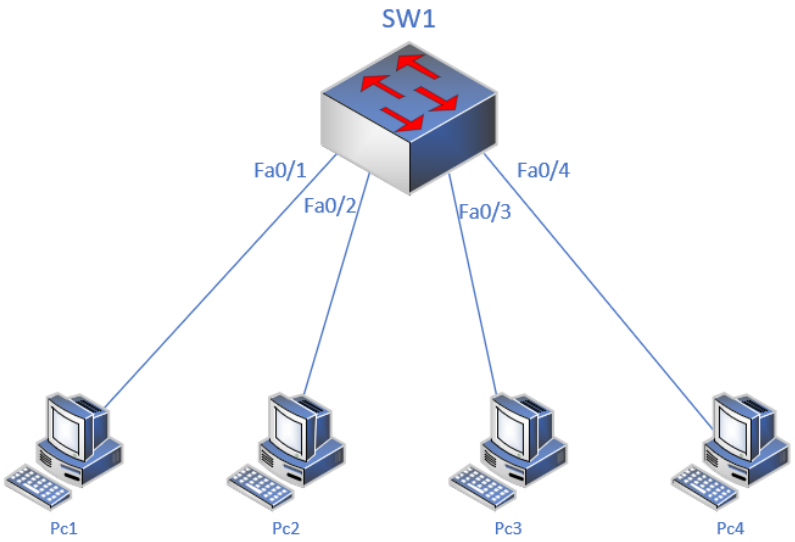
Dynamic

در این روش نسبت دادن پورت به یک Vlan به صورت دستی انجام نمی‌گیرد، بلکه از طریق یک سرور مرکزی با نام VMPS (Vlan Membership Policy Server) ایجاد و مدیریت می‌شوند.

در این قسمت، نحوه‌ی قرار دادن پورت‌های یک سوئیچ را در یک Vlan باهم بررسی می‌کنیم.
هر پورت سوئیچ از دو Mode تشکیل شده است:

- ✓ Access
- ✓ Trunk

تمام پورت‌های یک سوئیچ به صورت پیش‌فرض در مد access قرار دارد. برای اینکه یک پورت را به یک Vlan نسبت دهید، باید از این مد استفاده کنید. با یک مثال، کاملاً به این موضوع پی می‌برید.



شکل ۳-۳۷ Access Mode

www.takbook.com

به مانند شکل ۳۷-۳، یک سوئیچ و ۴ PC را به صفحه اضافه و آن‌ها را به هم متصل کنید و طبق جدول ۴-۳ به کامپیوترها آدرس دهید:

جدول ۴-۳ لیست آدرس‌های PC

Station	IP Address	Subnet Mask
PC1	192.168.1.1	255.255.255.0
PC2	192.168.1.2	255.255.255.0
PC3	192.168.1.3	255.255.255.0
Pc4	192.168.1.4	255.255.255.0

بعد از این‌که آدرس‌دهی کردید، اگر ارتباط بین PC ها را تست کنید، متوجه می‌شوید که همه‌ی آن‌ها باهم در ارتباط هستند. حالا می‌خواهیم از طریق Vlan ارتباط ۲ کامپیوتر Pc1 و Pc2 را با Pc3 و Pc4 جدا کنیم. برای این کار در داخل سوئیچ دو Vlan تعریف می‌کنیم:

```
Switch(config)#vlan 10
Switch(config-vlan)#ex
Switch(config)#vlan 20
Switch(config-vlan)#
```

Vlan های 10 و 20 در داخل سوئیچ ایجاد شده است و حالا باید پورت‌های سوئیچ که Pcها به آن متصل هستند را داخل این Vlan ها قرار دهیم. به شکل توجه کنید، ارتباط پورت‌ها با pcها به صورت جدول ۵-۳، است.

جدول ۵-۳ VLAN مربوط به PC

Station	**Port**	**Vlan**
PC1	Fa0/1	10
PC2	Fa0/2	10
PC3	Fa0/3	20
PC4	Fa0/4	20

طبق جدول ۵-۳، Pcها را درون Vlanهای مورد نظر قرار می‌دهیم؛ برای این کار وارد پورت‌هایی می‌شویم که کامپیوتر مورد نظر به آن متصل است، مثلاً در بالا Pc1 به پورت Fa0/1 متصل است که این پورت باید در Vlan 10 قرار بگیرد:

```
Switch(config)#interface fastEthernet 0/1
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 10
```

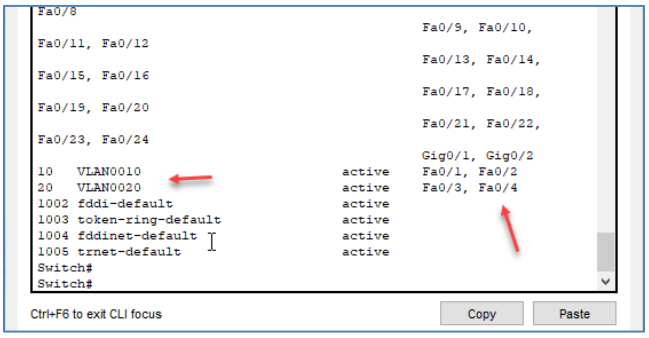
همان‌طور که مشاهده می‌کنید، در قسمت اول وارد پورت Fa0/1 شده‌ایم و بعدازآن از دستورswitchport mode access استفاده کردیم تا مد بر روی Access تنظیم شود و بعدازآن از دستور switchport access vlan 10 استفاده کردیم تا این پورت را وارد Vlan 10 کنیم. بقیه‌ی پورت‌ها هم به صورت زیر انجام می‌شود.

```
Switch(config)#int f0/2
Switch(config-if)# switchport mode access
```

www.takbook.com

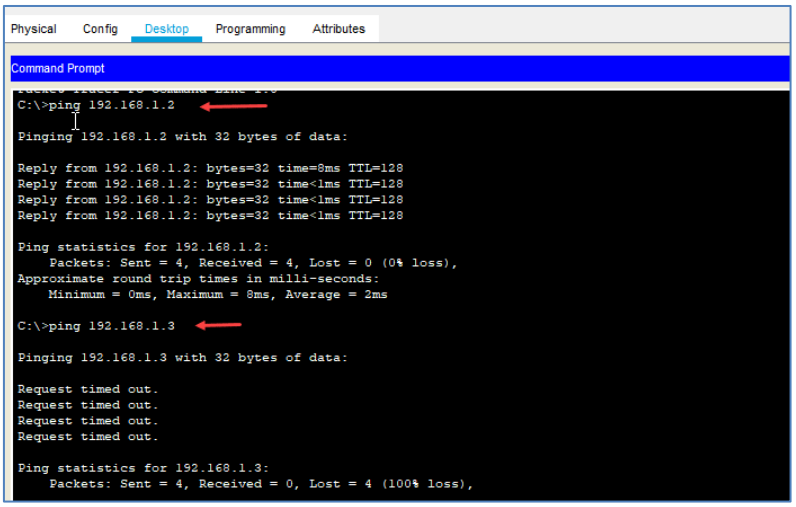
Switch(config-if)# **switchport access vlan 10**
Switch(config-if)#**int f0/3**
Switch(config-if)# **switchport mode access**
Switch(config-if)# **switchport access vlan 20**
Switch(config-if)#**int f0/4**
Switch(config-if)# **switchport mode access**
Switch(config-if)# **switchport access vlan 20**

بعد از اینکه پورت‌های مورد نظر را عضو VLAN مورد نظر کردید با دستور Show vlan brief می‌توانید مشاهده کنید که چهار پورت مورد نظر در VLAN خود قرار گرفته‌اند که در شکل ۳-۳۸ مشخص شده است.



شکل ۳-۳۸ تنظیمات سوئیچ

بعد از اتمام کار به مانند شکل ۳-۳۹ از طریق PC0، PC1 و PC2 را Ping کنید، مشاهده خواهید کرد که سیستم‌هایی که در VLAN هم شماره قرار دارند با هم در ارتباط هستند ولی برشکل آن امکان‌پذیر نیست.



شکل ۳-۳۹ ارتباط بین PC

www.takbook.com

قبل از اینکه به پورت ترانک بپردازیم این نکته را باید بررسی کنیم که وقتی دستور switchport mode ? را وارد کنید سه دستو را به صورت زیر مشاهده می‌کنید.

```
Switch(config-if)#switchport mode ?
access      Set trunking mode to ACCESS unconditionally
dynamic     Set trunking mode to dynamically negotiate access or trunk mode
trunk       Set trunking mode to TRUNK unconditionally
```

در این قسمت سه دستور را مشاهده می‌کنید که دستور Access را در قسمت قبل بررسی کردیم، اما دستور dynamic خود شامل دو قسمت است که در زیر بررسی می‌کنیم:

```
Switch(config-if)#switchport mode dynamic desirable
```

دستور بالا وقتی فعال شود، پورت مورد نظر با ارسال فریم‌های Dynamic Trunking Protocol یا به اختصار DTP سعی می‌کند پورت‌ها را به حالت Trunk ببرد که به صورت پیش‌فرض هم فعال است.

```
Switch(config-if)#switchport mode dynamic auto
```

این دستور وقتی فعال باشد، حالت آن به گوش دادن خط یا همان Listening تغییر می‌کند و اگر خط مقابل در حالت Trunk قرار داشته باشد آن ارتباط تبدیل به Trunkخواهد شد.
در ادامه به صورت کلی مد Trunk را بررسی می‌کنیم و نحوه راه‌اندازی آن را فرا می‌گیریم.

در آخر به این جدول توجه کنید که حالت‌های مختلف یک لینک را نشان می‌دهد که اگر مثلاً interface مورد نظر در حالت Access باشد با Interface دیگر که به آن متصل است باید چه مدی برای آن در نظر بگیرید، که طبق جدول ۶-۳، اگر یک طرف access باشد و طرف دیگر Trunk این عملیات انجام نخواهد شد و لینک مورد نظر کار نخواهد کرد.

Administrative Mode	Access	Dynamic Auto	Trunk	Dynamic Desirable
access	Access	Access	Do Not Use[1]	Access
dynamic auto	Access	Access	Trunk	Trunk
trunk	Do Not Use[1]	Trunk	Trunk	Trunk
dynamic desirable	Access	Trunk	Trunk	Trunk

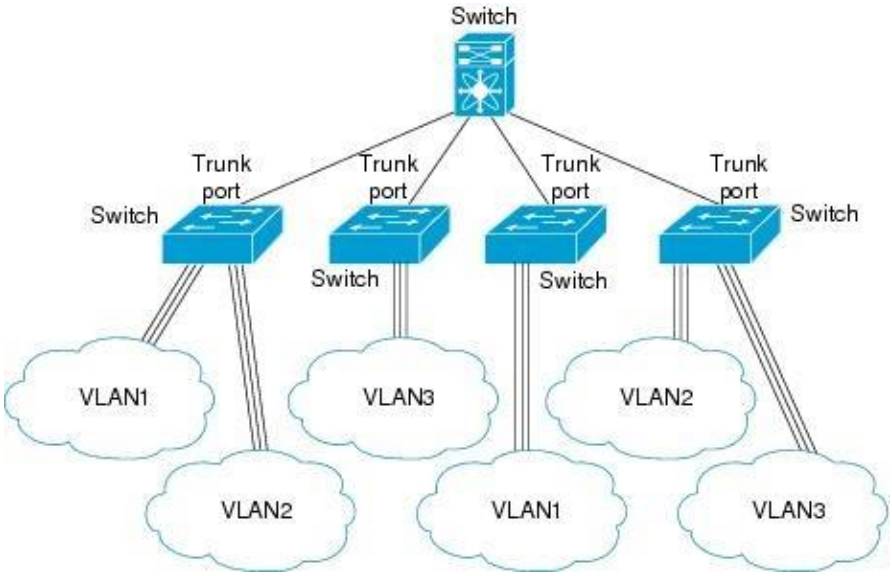
جدول ۶-۳ پورت‌های Switchport

Trunk Mode

قبل تعریف این مد، یک مثال برای درک بهتر این موضوع تعریف می‌کنیم؛ یک ساختمان را در نظر بگیرید که از سه طبقه تشکیل شده است و در هر طبقه از یک سوئیچ برای شبکه کردن کامپیوترها استفاده شده

www.takbook.com

است و تمام سوئیچ‌ها به هم متصل شده‌اند. نکته‌ی مهم در این قسمت این است که در هر طبقه بخش حسابداری، اداری و فروش وجود دارد و می‌خواهیم تمام بخش‌های هر ساختمان باهم در ارتباط باشند؛ برای این کار شما در هر طبقه، مانند مثال قبل برای هر بخش یک Vlan تعریف می‌کنید و پورت‌ها را داخل Vlan مورد نظر قرار می‌دهید، اما یک مشکل وجود دارد این‌که سوئیچ باید با vlanهای دیگر در طبقات مختلف در ارتباط باشند. برای حل این مشکل باید از Trunk استفاده کرد، Trunk روشی برای انتقال Vlanها در سوئیچ‌های مختلف است و با استفاده از آن این مشکل به راحتی حل می‌شود.



شکل ۴۰-۳ بررسی Trunk Mode

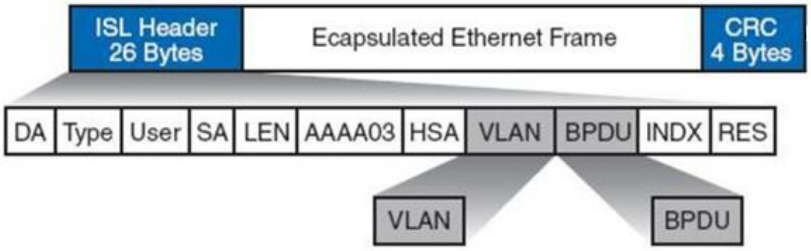
Tag زدن روی فریم‌ها

برای انتقال Vlanها در مد Trunk دو روش وجود دارد که از طریق آن یک Vlan شناسایی می‌شود:

- ✓ 802.1Q
- ✓ ISL(Inter-Switch Link Protocol)

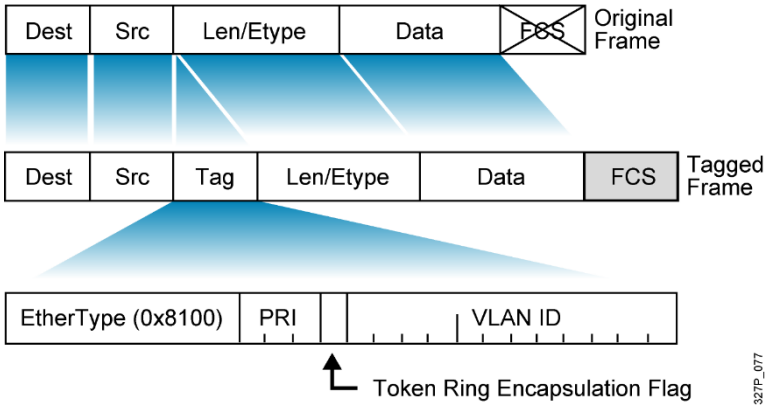
ISL: یک استاندارد برای بسته‌بندی فریم‌ها برای انتقال در یک مسیر یا همان Trunk است که این استاندارد مختص شرکت سیسکو بوده و در سوئیچ‌های امروزی کمتر استفاده می‌شود، در شکل ۳-۴۱ Header پروتکل ISL را مشاهده می‌کنید.

www.takbook.com



شکل ۴۱-۳ استاندارد ISL

802.1Q: یک استاندارد Open Source است و مختص شرکت خاصی نیست و اگر در شبکه‌ی خود از سوئیچ‌های شرکت‌های متفاوت استفاده می‌کنید، برای برچسب زدن روی فریم‌ها باید از این استاندارد استفاده کنید. این پروتکل ساختار فریم‌ها را به کل تغییر می‌دهد، در شکل ۴۲ – ۳ ساختار آن را مشاهده می‌کنید.



شکل ۴۲-۳ استاندارد 802.1Q

فعال کردن پروتکل ISL

این پروتکل به صورت پیش‌فرض روی سوئیچ‌های شرکت سیسکو فعال است.

فعال کردن پروتکل 802.1Q

برای فعال کردن این پروتکل باید وارد interface مورد نظر شوید و دستور زیر را وارد کنید:

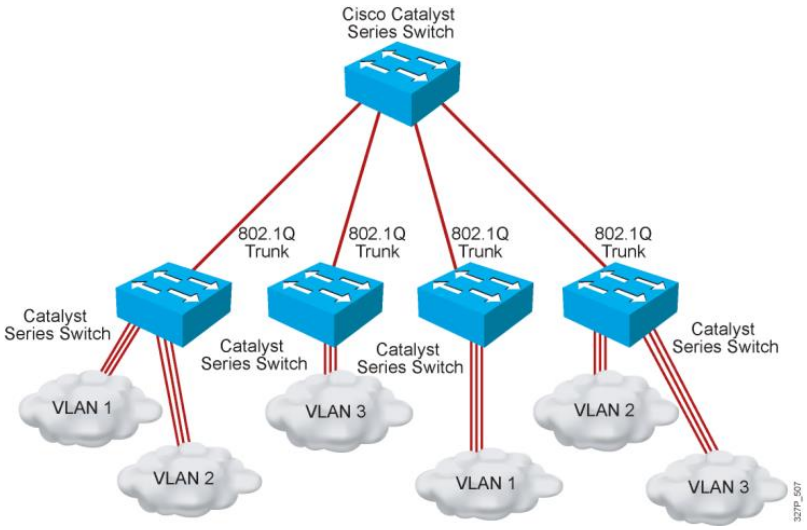
```
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport trunk encapsulation dot1q
```

با اجرای این دستورات، یک سوئیچ تمام Vlanها را برچسب‌گذاری می‌کند و از خود عبور می‌دهد. شاید شما بخواهید به سوئیچ بگوئید که فقط Vlanهای خاصی از وی عبور کنند؛ برای این منظور از دستور زیر استفاده می‌کنیم:

www.takbook.com

Switch(config-if)#**switchport trunk allowed vlan 10**

با این دستور فقط Vlan 10 حق عبور دارد و بقیه Vlanها از این سوئیچ عبور نمی‌کنند.
پس یک پورت در سوئیچ زمانی Trunk می‌شود که بخواهد Vlanها را بین دو دستگاه سوئیچ جابجا کنند.
به شکل ۴۴-۳، توجه کنید:



شکل ۴۴-۳ بررسی حالت Trunk

در شکل ۴۴-۳، سوئیچ‌ها به هم متصل شده‌اند و سوئیچ‌هایی که در زیر قرار دارند از Vlanهای مختلفی تشکیل شده‌اند. برای ارتباط Vlan1 به Vlan1 در سوئیچ دیگر، باید پروتکل Trunk را روی پورت‌های سوئیچ که به سوئیچ اصلی متصل است، اجرا کنیم و بعد 802.1Q را راه‌اندازی کنیم تا عملیات برچسب‌گذاری روی Vlanها را انجام دهد.

نکته:

اگر بخواهید پورت خاصی را برای همیشه در حالت Trunk قرار دهید باید از دستور زیر در آن پورت استفاده کنید:

Switch(config-if)#**switchport nonegotiate**

Native Vlan

همان‌طور که قبلاً گفتیم در تمام سوئیچ‌ها، Vlan1 وجود دارد و قادر به ایجاد و یا حذف آن نیستید، اما وقتی چندین سوئیچ را با پروتکل 802.1Q، Trunk می‌کنید در زمان انتقال بین سوئیچ‌ها روی Vlan 1 هم

www.takbook.com

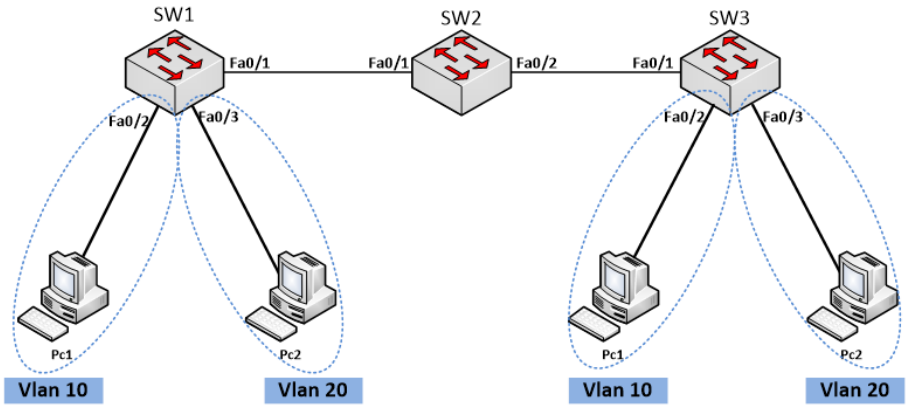
برچسب‌گذاری می‌شود و همین کار باعث استفاده‌ی بیش از حد از پهنای باند شبکه و منابع سوئیچ خواهد شد و برای جلوگیری از این کار باید روی پورتی که Trunk شده است، دستور زیر را وارد کنیم:

Switch(config-if)# **switchport trunk native vlan 1**

با این کار، Vlan1 در پروتکل Trunk انتقال داده نمی‌شود.

برای اینکه بیشتر با بحث Trunk آشنا شوید این مثال را با هم بررسی می‌کنیم.

به مانند شکل ۴۵-۳ در نرم‌افزار Packet Tracer سه سوئیچ و چهار PC را به صفحه اضافه کنید و طبق جدول ۷-۳ آدرس‌های IP مربوط به PCها را وارد کنید.



شکل ۴۵-۳ بررسی حالت Trunk

Station	Ip address	SubnetMask
Pc1	192.168.1.1	255.255.255.0
Pc2	192.168.1.2	255.255.255.0
Pc3	192.168.1.3	255.255.255.0
Pc4	192.168.1.4	255.255.255.0

جدول ۷-۳ پورت‌های Switchport

بعد از این‌که Ip addressها را در pc ها وارد کردیم، نوبت به تعریف Vlan در سوئیچ است. در داخل هر یک از سوئیچ‌ها، Vlanهای ۱۰ و ۲۰ را به صورت زیر تعریف می‌کنیم:

Switch(config)#**vlan 10**
Switch(config)# **vlan 20**

بعد از تعریف Vlan باید پورت‌های متصل به Pc را داخل Vlanهای مشخص‌شده قرار دهیم، مثلاً pc1 باید در Vlan 10 قرار بگیرید؛ برای این کار وارد سوئیچ و بعد، وارد interface fa0/2 که به pc1 متصل است، می‌شویم و آن را طبق دستور زیر داخل Vlan 10 قرار می‌دهیم:

Switch(config)#**int f0/2**
Switch(config-if)#**switchport mode access**

www.takbook.com

Switch(config-if)#**switchport access vlan 10**

بقیه‌ی پورت‌های سوئیچ که به pc متصل است را درون Vlan قرار می‌دهیم.

Switch(config)#**int f0/3**
Switch(config-if)#**switchport mode access**
Switch(config-if)#**switchport access vlan 20**

پورت‌های سوئیچ ۳ را به صورتی که در بالا انجام دادیم، درون Vlan قرار می‌دهیم.

بعد از این‌که این کار را انجام دادید، یک Ping از Pc1 به Pc3 بگیرید و مطمئناً جواب نخواهید گرفت، به خاطر اینکه پروتکل Trunk روی پورت‌های سوئیچ فعال نشده و به همین خاطر ارتباط برقرار نمی‌شود. وارد SW1 شوید و پورتی که به طرف SW2 می‌رود را Trunk کنید:

Switch(config)#**Interface Fa0/1**
Switch(config-if)#**switchport mode trunk**

بعد از این کار، مدل برچسب‌گذاری روی فریم‌ها را باید مشخص کنید که ISL باشد یا 802.1Q که در برنامه‌ی Packet Tracer به صورت پیش‌فرض dot1q است

بقیه‌ی پورت‌های متصل به سوئیچ‌های دیگر را Trunk کنید:

SW2:

Switch(config)#**Interface Fa0/1**
Switch(config-if)#**switchport mode trunk**
Switch(config)#**Interface Fa0/2**
Switch(config-if)#**switchport mode trunk**

SW3:

Switch(config)#**Interface Fa0/1**
Switch(config-if)#**switchport mode trunk**

بعد از این کار، ارتباط بین Vlan ها برقرار می‌شود و pc1 با pc3 باهم ارتباط برقرار می‌کنند.

بعد از این مثال، یک سوال در ذهنتان پیش می‌آید که اگر تعداد سوئیچ‌ها زیاد باشد و ما بخواهیم داخل هرکدام از سوئیچ‌ها vlan تعریف کنیم، کار بسیار وقت‌گیری است. آیا روش دیگری هم وجود دارد؟

بله، روش دیگری هم وجود دارد که می‌توانیم در یک سوئیچ یا هر سوئیچی در شبکه‌ی Vlan تعریف کنید و این Vlanها به صورت خودکار وارد سوئیچ دیگر می‌شوند که به این روش VLAN Trunking Protocol (VTP)می‌گویند.

۳-۵-۲ کار با VTP(VLAN Trunking Protocol)

www.takbook.com

این پروتکل توسط شرکت سیسکو ارائه شده است، اما انحصاری نیست و شرکت‌های دیگر می‌توانند از این پروتکل استفاده کنند. این پروتکل برای مدیریت Vlanها و ایجاد امنیت طراحی شده است. VTP به مدیر شبکه، اجازه‌ی ایجاد، حذف، تغییر نام و ... را می‌دهد. چند ویژگی این پروتکل:

- پیکربندی Vlanها به صورت سریع در همه‌ی سوئیچ‌ها انجام می‌گیرد.
- نظارت کامل بر کار Vlanها در یک زمان.
- ایجاد Vlan به صورت Plug-and-Play.

VTP دارای سه حالت است:

Server Mode

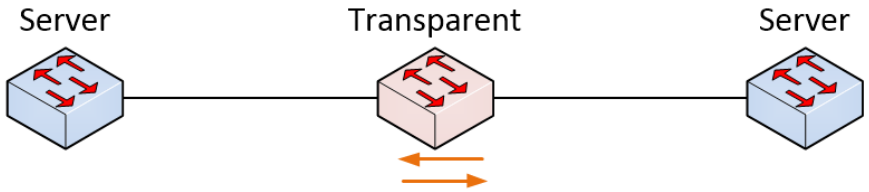
در این حالت یک سوئیچ می‌تواند Vlanها را ایجاد، حذف و به طور کامل مدیریت کند که به صورت پیش‌فرض همه‌ی سوئیچ‌ها در مد Server قرار دارند.

Client Mode

در این حالت سوئیچ به سرور گوش می‌دهد و نمی‌تواند یک Vlan را ایجاد، حذف و مدیریت کند و همه چیز از طریق Server به وی اعمال می‌شود.

Transparent Mode

این سوئیچ فقط Vlanهایی که به وی می‌رسد را از خود عبور می‌دهد و کاری روی آن‌ها انجام نمی‌دهد، اما این سوئیچ می‌تواند Vlan را تعریف و یا حذف کند، اما به کسی اعلام نمی‌کند که این Vlanهای من است! یک سوئیچ خودمختار است و همه‌ی کارها را خودش انجام می‌دهد که این موضوع را در شکل ۴۶-۳ مشاهده می‌کنید.



شکل ۴۶-۳ بررسی Transparent

طبق شکل ۴۶-۳، در بین دو سوئیچ Server یک سوئیچ transparent قرار گرفته است. این سوئیچ فقط Vlanهایی را که از دو سرور برای وی ارسال می‌شود به سوئیچ دیگر انتقال می‌دهد و کاری روی این Vlanها انجام نمی‌دهد، اما خودش می‌تواند vlan ایجاد کند و روی آن‌ها کار کند، ولی VLanهای مربوط به خودش را به کسی نمی‌دهد.

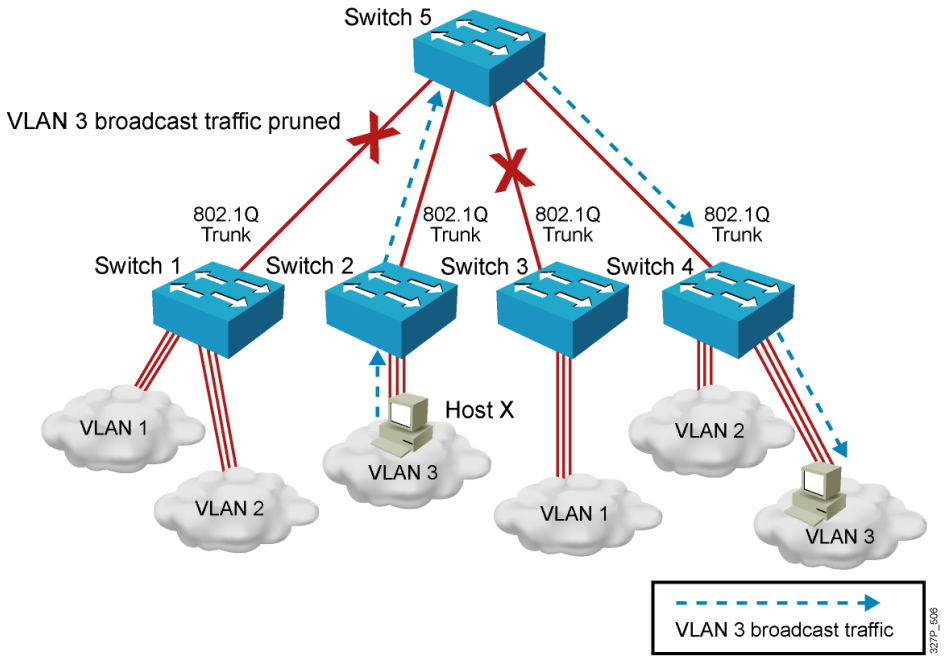
VTP domain

به ناحیه‌ای گفته می‌شود که سوئیچ‌هایی داخل آن عضو هستند و Vlanهای خود را با همدیگر به اشتراک می‌گذارند و سوئیچ‌ها تنها می‌توانند در یک VTP Domain عضو شوند و نمی‌توانند Vlanهای خود را با VTP domain دیگری به اشتراک بگذارند.

www.takbook.com

VTP Pruning

در شکل ۴۷-۳، به سوئیچ 2 یک pc متصل است و در Vlanشماره‌ی 3 قرار دارد و می‌خواهد با pc دیگر در سوئیچ 4 ارتباط برقرار کند. همان‌طور که می‌دانید سوئیچ، بعد از رسیدن درخواست به پورت، خود آن را به صورت Broadcast برای دیگر سوئیچ‌ها که به آن‌ها Trunk شده است، ارسال می‌کند، اما با فعال کردن VTP Pruning این کار انجام نمی‌شود و فقط پیام Broadcast به سوئیچ‌هایی ارسال می‌شود که یکی از پورت‌های آن‌ها در Vlan مورد نظر قرار داشته باشد.



شکل ۴۷-۳ بررسی VTP Pruning

نکاتی در مورد VTP

۱- سوئیچ‌هایی که در نقش سرور هستند می‌توانند VLANها در محدوده‌ی (۱ – ۱۰۰۵) را پیکربندی کنند.

۲- سوئیچ‌هایی که در نقش کلاینت هستند توانایی ایجاد VLAN و پیکربندی آن را نخواهند داشت.

۳- سوئیچ سرور و کلاینت VLANهای دیگر را یاد می‌گیرند .

۴- دستورات VTP را نمی‌توانید در show running-config مشاهده کنید و باید از دستورات دیگر برای این کار استفاده کنید.

نکته مهم:

www.takbook.com

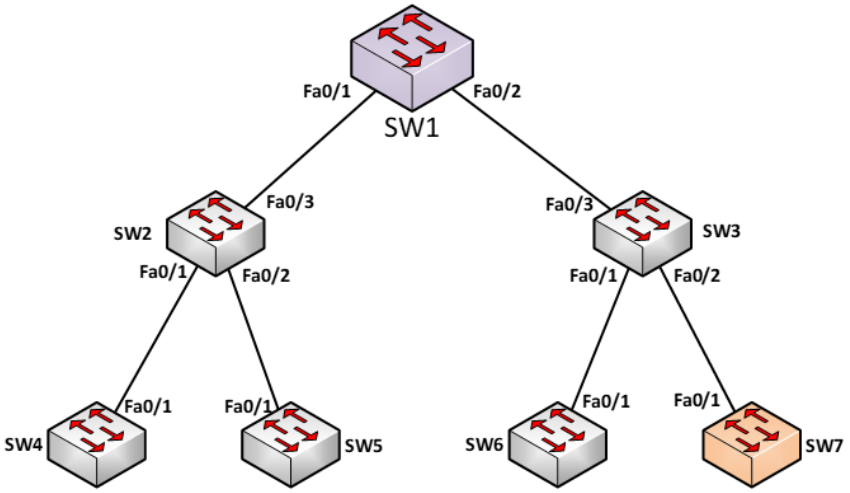
تا زمانی که به صورت کامل کار با دستورات و پیکربندی VTP را فرا نگرفتید نباید در سرویس VTP در شبکه‌ی سازمان خود تغییرات ایجاد کنید، چون باعث می‌شود با یک اشتباه ضربه‌ی سنگینی بر شبکه‌ی LAN سازمان وارد شود و کل شبکه از کار بیفتد، پس سعی کنید برای آزمایش از نرم‌افزارهای مجازی استفاده کنید و یا اگر بخواهید از سوئیچ فیزیکی استفاده کنید بهتر است هیچ لینکی به شبکه اصلی سازمان نداشته باشند.

۳-۵-۳ فعال کردن VTP

برای فعال کردن Vtp باید از دستورات زیر در سوئیچ استفاده کنیم:

Switch# **configure terminal**
Switch(config)# **vtp mode** [server | client | transparent]
Switch(config)# **vtp domain** *domain-name*
Switch(config)# **vtp password** *password*
Switch(config)# **vtp pruning**
Switch(config)# **end**

با توجه به شکل۴۸-۳ با یک مثال این دستورات را داخل آن به کار می‌بریم:



شکل ۴۸-۳ مثالی از VTP

با توجه به شکل ۴۸-۳، سوئیچ SW1 به عنوان سرور و سوئیچ SW7 به عنوان Transparent و بقیه، به عنوان Client هستند.

همیشه به یاد داشته باشید که قبل از ایجاد VTP، حتماً تمام بورت‌های سوئیچ‌ها که به هم متصل هستند را در وضعیت Trunk قرار دهید تا Vlanها بتوانند بین سوئیچ‌ها حرکت کنند، پس در پورت‌های

www.takbook.com

سوئیچ‌ها که به سوئیچ دیگری متصل است دستور زیر را وارد می‌کنیم، مثلاً در سوئیچ یک پورت Fa0/1 آن با پورت Fa0/3 سوئیچ دو در ارتباط است و باید این پورت‌ها در وضعیت Trunk قرار بگیرند:

```
Switch(config)#int f0/1
Switch(config-if)#switchport mode trunk
```

بعد از این‌که در تمام سوئیچ‌ها، پورت‌ها را در وضعیت Trunk قرار دادیم، نوبت به ایجاد VTP است. برای این کار وارد سوئیچ SW1 شوید و دستورات زیر را وارد کنید:

```
Switch(config)# vtp mode server
```

با دستور بالا این سوئیچ به عنوان سرور انتخاب می‌شود، البته این وضعیت به صورت پیش‌فرض فعال است.

در ادامه نام دومین را به cisco تغییر می‌دهیم، توجه داشته باشید تمام سوئیچ‌ها برای ارتباط با هم، باید در یک domain قرار داشته باشند.

```
Switch(config)#vtp domain cisco.com
Changing VTP domain name from NULL to cisco.com
```

با دستور زیر رمز عبور را برای VTP فعال می‌کنیم که گزینه‌ی مهمی در ارتباط با سوئیچ‌های دیگر است. با قرار دادن رمز عبور، کسی دیگر نمی‌تواند بدون اجازه، خودش را عضو این Domain کند. سعی کنید رمز عبور را به صورت پیچیده وارد کنید.

```
Switch(config)#vtp password 123
Setting device VLAN database password to 123
```

با دستورات بالا VTP را روی سوئیچ ۱ فعال کردیم و این سوئیچ به عنوان سوئیچ سرور نقش اصلی را در این شبکه بازی می‌کند. بقیه‌ی سوئیچ‌ها به جز سوئیچ ۷ باید در مد VTP Client قرار بگیرند و اطلاعات را از VTP Server دریافت کنند:

سوئیچ 2:

```
Switch(config)#vtp mode client
Setting device to VTP CLIENT mode.
Switch(config)#vtp password 123
Setting device VLAN database password to 123
Switch(config)#vtp domain cisco.com
Domain name already set to cisco.com.
```

سوئیچ 3:

```
Switch(config)#vtp mode client
```

www.takbook.com


```
Setting device to VTP CLIENT mode.
Switch(config)#vtp password 123
Setting device VLAN database password to 123
Switch(config)#vtp domain cisco.com
Domain name already set to cisco.com.
```

سوئیچ 4:

```
Switch(config)#vtp m c
Setting device to VTP CLIENT mode.
Switch(config)#vtp pass 123
Setting device VLAN database password to 123
Switch(config)#vtp d cisco.com
Domain name already set to cisco.com
```

سوئیچ 5:

```
Switch(config)#vtp m c
Setting device to VTP CLIENT mode.
Switch(config)#vtp pass 123
Setting device VLAN database password to 123
Switch(config)#vtp d cisco.com
Domain name already set to cisco.com.
```

سوئیچ 6:

```
Switch(config)#vtp m c
Setting device to VTP CLIENT mode.
Switch(config)#vtp pass 123
Setting device VLAN database password to 123
Switch(config)#vtp d cisco.com
Domain name already set to cisco.com.
```

سوئیچ 7 را باید در مد Transparent قرار دهیم:

```
Switch(config)#vtp mode transparent
Setting device to VTP TRANSPARENT mode.
Switch(config)#vtp d cisco.com
Domain name already set to cisco.com.
Switch(config)#vtp pass 123
Setting device VLAN database password to 123
```

بعد از اتمام کار، نوبت به تعریف Vlan در سوئیچ SW1 می‌رسد که سوئیچ سرور است. در این سوئیچ، Vlanهای 100، 200، 300 را تعریف می‌کنیم. با اجرای دستور Show vlan brief، می‌توانید لیست Vlanهای ساخته‌شده را مشاهده کنید.

```
Switch#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/3, Fa0/4, Fa0/5, Fa0/6
                                                Fa0/7, Fa0/8, Fa0/9, Fa0/10
```

www.takbook.com


```
                                Fa0/11, Fa0/12, Fa0/13, Fa0/14
                                Fa0/15, Fa0/16, Fa0/17, Fa0/18
                                Fa0/19, Fa0/20, Fa0/21, Fa0/22
                                Fa0/23, Fa0/24, Gig1/1, Gig1/2
100  VLAN0100                     active
200  VLAN0200                     active
300  VLAN0300                     active
1002 fddi-default                 active
1003 token-ring-default             active
1004 fddinet-default              active
1005 trnet-default                active
```

همانطور که گفتیم سوئیچ SW1 سوئیچ سرور است و به خاطر همین موضوع Vlanها را در آن تعریف کردیم. بقیه‌ی سوئیچ‌ها به علتVTP Client بودن Vlanها را از سوئیچ سرور دریافت می‌کنند. اگر شما در سوئیچ 6 دستور Show vlan brief را اجرا کنید، تمام vlanهایی را که در سوئیچ یک ساختیم را در این سوئیچ هم می‌توانید مشاهده کنید:

Switch#**show vlan brief**

```
VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/2, Fa0/3, Fa0/4, Fa0/5
                                                Fa0/6, Fa0/7, Fa0/8, Fa0/9
                                                Fa0/10, Fa0/11, Fa0/12, Fa0/13
                                                Fa0/14, Fa0/15, Fa0/16, Fa0/17
                                                Fa0/18, Fa0/19, Fa0/20, Fa0/21
                                                Fa0/22, Fa0/23, Fa0/24, Gig1/1
                                                Gig1/2
100  VLAN0100                                   active
200  VLAN0200                                   active
300  VLAN0300                                   active
1002 fddi-default                               active
1003 token-ring-default                         active
1004 fddinet-default                            active
1005 trnet-default                              active
```

اگر در سوئیچ 7 دستور بالا را وارد کنید، چیزی مشاهده نمی‌کنید، چون این سوئیچ در مد Transparent قرار گرفته است که آن را توضیح دادیم.

دستور Show Vtp Status

با این دستور اطلاعاتی را درباره‌ی VTP و اجزای آن که روی سوئیچ فعال شده است، مشاهده می‌کنید.

Switch#**show vtp status**

```
VTP Version                     : 2
Configuration Revision          : 3
Maximum VLANs supported locally : 255
Number of existing VLANs        : 8
VTP Operating Mode              : Server
VTP Domain Name                 : cisco.com
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
```

www.takbook.com


```
VTP Traps Generation          : Disabled
MD5 digest                    : 0x5C 0xF1 0xFA 0x4C 0xCB 0x3F 0xB8 0xD3
Configuration last modified by 0.0.0.0 at 3-1-93 00:40:23
Local updater ID is 0.0.0.0 (no valid interface found)
```

دستور Show vtp counters

این دستور تعداد بسته‌های ارسالی و دریافتی پروتکل VTP را به ما نشان می‌دهد.

```
Switch#show vtp counters
VTP statistics:
Summary advertisements received    : 45
Subset advertisements received     : 14
Request advertisements received    : 9
Summary advertisements transmitted : 24
Subset advertisements transmitted  : 14
Request advertisements transmitted : 0
Number of config revision errors   : 3
Number of config digest errors     : 0
Number of V1 summary errors        : 0
```

Summary advertisements: اطلاعاتی است که هر 300 ثانیه توسط Server به بقیه‌ی سوئیچ‌ها در شبکه ارسال می‌شود.

Subset advertisements: شامل تغییرات در یک vlan است و توسط VTP server ارسال می‌شود.

دستور Show vtp Password

رمز عبور قرار داده‌شده روی Vtp Password را نمایش می‌دهد.

```
Switch#show vtp pass
VTP Password: 123
```

با استفاده از دستور show interfaces fastEthernet 0/1 switchport می‌توانید جزئیات کار را در Interface مورد نظر مشاهده کنید.

```
Switch#show interfaces fastEthernet 0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: dynamic auto
Operational Mode: static access
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
```

www.takbook.com

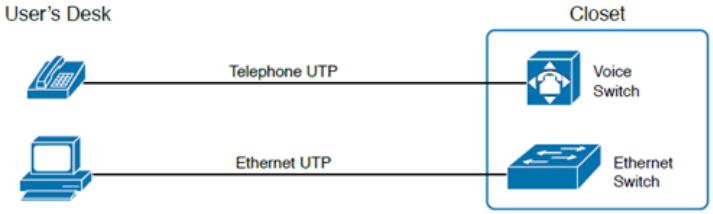

```
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk private VLANs: none
Operational private-vlan: none
Trunking VLANs Enabled: All
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL
Protected: false
Unknown unicast blocked: disabled
Unknown multicast blocked: disabled
Appliance trust: none
```

۳-۶ بررسی Voice VLAN در سوئیچ‌های سیسکو

امروزه استفاده از سرویس‌های Voice در سازمان‌ها بسیار گسترده شده است و در بهبود کارایی آنها بسیار مواثر است.

از طریق تلفن‌های IP می‌توانید بین چند شعبه شرکت خود صوت و تصویر در بستر IP ارسال کنید که این کار توسط سوئیچ انجام می‌شود، در این قسمت می‌خواهیم نحوه پیکربندی آن را بررسی کنیم.

اگر به گذشته برگردیم کاربران برای استفاده از تلفن باید به یک سوئیچ تلفنی که مختص این کار بود متصل می‌شدند و سیستم‌های کامپیوتری آنها هم به مانند شکل ۳-۴۹ به سوئیچ دیگر متصل بود.



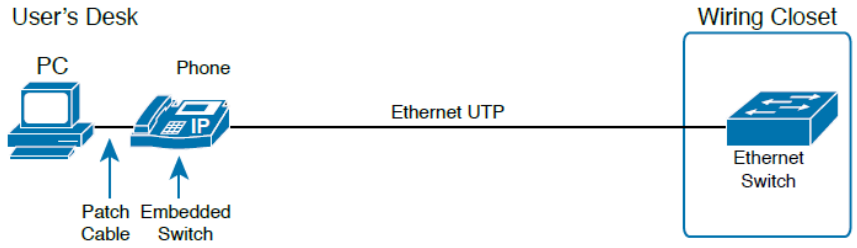
شکل ۳-۴۹ بررسی Voice VLAN

اصطلاح IP telephony به شاخه‌ای از شبکه گفته می‌شود که در آن تلفن‌ها از طریق IP قادر به ارسال و دریافت پکت‌های Voice هستند و از طریق کابل و شبکه Wifi در دسترس قرار می‌گیرند.

شرکت سیسکو برای کنترل و مدیریت IP telphonyهای خود از نرم‌افزاری با نام Cisco Unified Communication استفاده می‌کند که به این گونه نرم‌افزارهای مرکزی، PBX هم گفته می‌شود.

امروزه برای متصل کردن تلفن‌های IP فقط از یک سوئیچ و یک کابل UTP استفاده می‌کنند، در شکل ۳-۵۰، یک PC و یک تلفن ip را مشاهده می‌کنید که اول یک کابل به تلفن متصل می‌شود و در زیر تلفن یک سوئیچ کوچک طراحی شده است که یک خروجی هم می‌توانید به PC متصل کنید که با این کار با یک خط UTPهم تلفن و هم PC دارای IP می‌شوند و از شبکه استفاده می‌کنند.

www.takbook.com



شکل ۳-۵۰ بررسی VTP Pruning

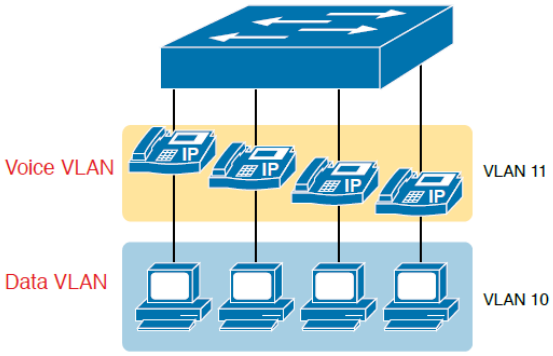
ولی مهمترین نکته در این نوع ارتباط این است که PC و تلفن نمی‌توانند به صورت پیش‌فرض با هم کار کنند، چون PC باید DATA ارسال کند و تلفن هم باید بسته‌های Voice را به شبکه ارسال کند و این کار امکانپذیر نیست جزء اینکه در ادامه آنها را بررسی و تنظیم کنیم.

برای اینکه بتوانیم این دو پکت را از هم جدا کنیم باید روی دو نوع VLAN کار کنیم:

Data Vlan : در این نوع VLAN به مانند قبل اطلاعات عادی PCها از آن عبور می‌کند.

Voice Vlan : در این نوع VLAN اطلاعات تلفن‌های IP عبور می‌کند که اصولا در Header پروتکل 802.1Q علامت‌گذاری می‌شوند.

همانطور که در شکل ۳-۵۱ مشاهده می‌کنید VLANهای تلفن و PC متفاوت است و هر کدام باید در VLAN خود قرار گیرند.

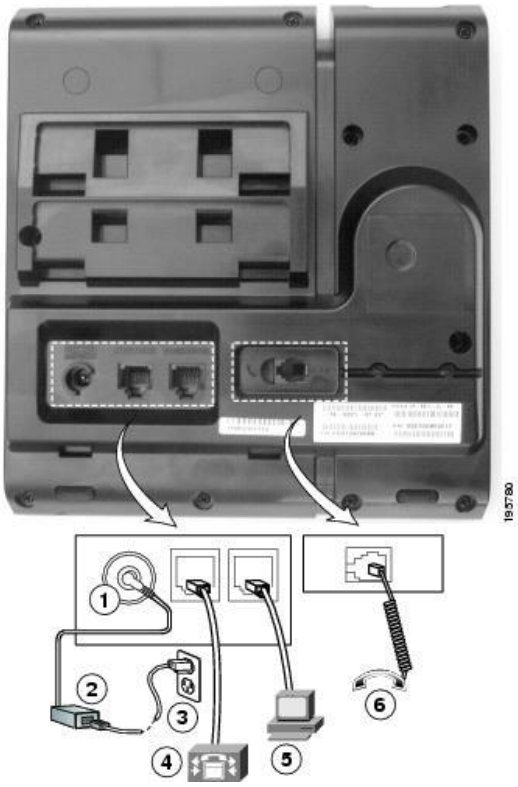


شکل ۳-۵۱ بررسی VTP Pruning

۳-۶-۱ پیکربندی Data Voice VLAN

قبل از اینکه کار پیکربندی را انجام دهید به شکل ۳-۵۲ توجه کنید:

www.takbook.com



شکل ۵۲-۳ *Data Voice VLAN*

شکل ۵۲-۳، نشان دهنده‌ی پشت تلفن IP سیسکو است که دارای چند پورت است که دقیقاً جایگاه آنها مشخص شده است.

پورت اول از سمت چپ برای آداپتور برق ورودی است، پورت دوم که کابل شبکه اصلی که به سوئیچ مادر متصل است به آن اضافه می‌شود، پورت سوم هم برای متصل کردن PC به شبکه است و پورت آخر هم برای متصل شدن به هدفون یا گوشی تلفن است.

دستوراتی که باید در سوئیچ وارد کنید به صورت زیر است:

```
SW1# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SW1(config)# vlan 10
SW1(config-vlan)# vlan 11
SW1(config-vlan)# interface FastEthernet0/1
SW1(config-if)# switchport mode access
SW1(config-if)# switchport access vlan 10
SW1(config-if)# switchport voice vlan 11
```

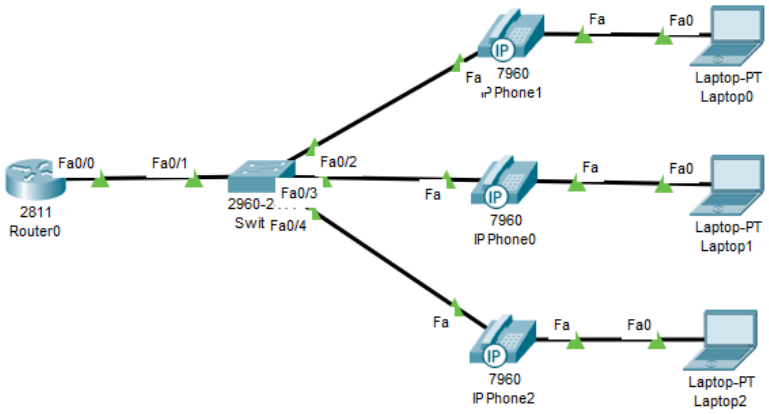
www.takbook.com

در دستورات بالا دو VLANبا شماره‌های 10 و 11 تعریف شده که بعد از آن باید وارد Interfaceهایی شد که به PC و تلفن متصل است و بعد باید دستور switchport mode access را اجرا کنید تا پورت یا پورت‌های مورد نظر به مد access تغییر پیدا کنند و بعد از آن باید با دستور switchport access vlan 10 پکت‌های Data را در VLAN 10 و پکیت‌های Voice را در VLAN11 قرار داد تا این اطلاعات از هم جدا شوند.

مثال:

برای اینکه بهتر این موضوع را درک کنید، یک مثال کامل را در Packet Tracer بررسی می‌کنیم.

نکته: این قسمت فقط برای آگاهی بیشتر شما ارائه شده است، توجه داشته باشید که در این سناریو از سرویس DHCP استفاده شده است که این سرویس در فصل دهم این کتاب بررسی شده است.



شکل ۳-۵۳ مثال Voice VLAN

به مانند شکل ۳-۵۳ سه لپ‌تاپ، سه IP Phone 7960 به همراه یک سوئیچ 2960 و روتر ۲۸۱۱ به لیست اضافه کنید و ارتباط آنها را برقرار کنید، توجه داشته باشید که Ip Phoneها دارای دو پورت هستند که پورت Switch آنها را به سوئیچ و پورت PC را به لپ‌تاپ متصل کنید.

برای شروع کار وارد سوئیچ شوید و تنظیمات زیر را انجام دهید:

در دستور زیر دو VLAN با شماره‌ی 20 , 10 ایجاد شده است که VLAN10 مربوط به Data و VLAN20 مربوط به ترافیک Voice است که برای آنها یک اسم مشخص کردیم.

```
Switch(config)#vlan 10
Switch(config-vlan)#name Data
Switch(config-vlan)#vlan 20
Switch(config-vlan)#name Voice
```

www.takbook.com

برای اینکه VLANها با هم در ارتباط باشند باید Inter Vlan Routing را بر روی روتر پیاده‌سازی کنیم (در مورد Inter VLAN Routing در فصل پنجم به صورت مفصل بحث کردیم) برای همین باید پورت fastEthernet 0/1 که به روتر متصل است را با دستور زیر در حالت Trunk قرار دهیم.

```
Switch(config)#interface fastEthernet 0/1
Switch(config-if)#sw mode trunk
```

در ادامه باید پورت‌هایی که به تلفن متصل شده‌اند را به صورت جداگانه در VLAN10 و VLAN20 قرار دهیم که نوع آنها هم مشخص شده است.

```
Switch(config)#interface range fastEthernet 0/2-4
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 10
Switch(config-if-range)#switchport voice vlan 20
Switch(config-if-range)#no sh
Switch(config-if-range)#exit
```

وارد روتر شوید و دستورات زیر را اجرا کنید:

در دستور زیر وارد پورت fastEthernet 0/0 شوید و آن را روشن کنید:

```
Router(config)#interface fastEthernet 0/0
Router(config-if)#no sh
```

در ادامه کار باید دو پورت مجازی با شماره‌ی VLAN مورد نظر ایجاد و برای آنها آدرس IP وارد کنید که دستورات آن به صورت زیر است، البته این دستور برای VLAN10 است:

```
Router(config)#int fastEthernet 0/0.10
Router(config-subif)#encapsulation dot1Q 10
Router(config-subif)#ip address 192.168.10.1 255.255.255.0
Router(config-subif)#no sh
Router(config-subif)#exit
```

دستورات زیر مربوط به VLAN20 است که برای آن هم آدرس IP در نظر می‌گیریم:

```
Router(config)#int fastEthernet 0/0.20
Router(config-subif)#encapsulation dot1Q 20
Router(config-subif)#ip address 192.168.20.1 255.255.255.0
Router(config-subif)#no sh
```

برای اینکه به لپ‌تاپ‌ها و تلفن‌ها آدرس IP اختصاص دهیم باید سرویس DHCP را فعال کنیم که به این نکته توجه کنید که برای هر VLAN به صورت مجزا باید یک Pool یا رنج شبکه مشخص کنیم:

```
Router(config)#ip dhcp pool Data
Router(dhcp-config)#network 192.168.10.0 255.255.255.0
Router(dhcp-config)#default-router 192.168.10.1
Router(dhcp-config)#exit
```

www.takbook.com


```
Router(config)#ip dhcp pool Voice
Router(dhcp-config)#network 192.168.20.0 255.255.255.0
Router(dhcp-config)#default-router 192.168.20.1
Router(dhcp-config)#option 150 ip 192.168.20.1
Router(dhcp-config)#exit
```

در ادامه باید سرویس Telephony را فعال کنیم، در دستور زیر عدد ۳ مربوط تعداد حداکثر دستگاه‌های تلفن است که این روتر می‌تواند به آنها سرویس دهد، ip source-address هم برای دریافت IP از سرویس DHCP برای تلفن است.

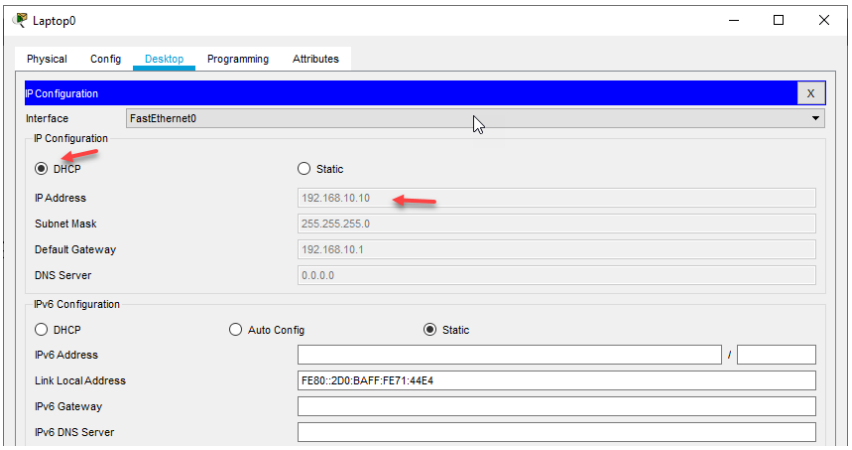
```
Router(config)#telephony-service
Router(config-telephony)#max-dn 3
Router(config-telephony)#max-ephones 3
Router(config-telephony)#ip source-address 192.168.20.1 port 2000
Router(config-telephony)#auto assign 1 to 6
```

بعد از فعال‌سازی سرویس telephony باید شماره‌های تلفن را با دستورات زیر مشخص کنیم:

```
Router(config)#ephone-dn 1
Router(config-ephone-dn)#number 101
Router(config-ephone-dn)#exit

Router(config)#ephone-dn 2
Router(config-ephone-dn)#number 102
Router(config-ephone-dn)#exit

Router(config)#ephone-dn 3
Router(config-ephone-dn)#number 103
Router(config-ephone-dn)#exit
```

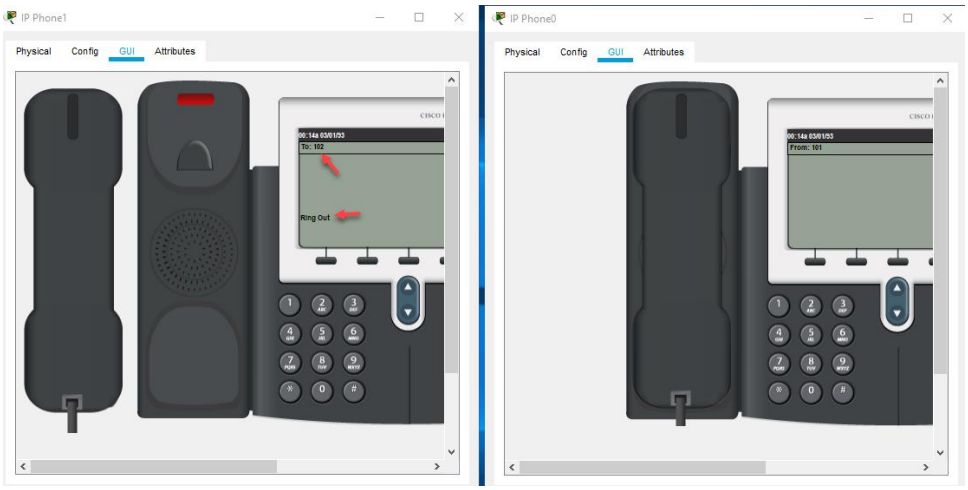
بعد از انجام مراحل بالا اگر وارد یکی از لپ‌تاپ‌ها شوید و قسمت IP را مشاهده کنید، در حالت DHCP آدرس در رنج 192.168.10.0 دریافت کرده است که مربوط به VLAN 10 است که در حالت Access قرار دارد.

www.takbook.com



شکل ۵۴-۳ تنظیمات لپ‌تاپ

وارد تب GUI در IP Phone شوید و شماره‌گیری کنید، به مانند شکل ۵۵-۳ باید تلفن زنگ خورده و می‌توانید گوشی را بردارید.



شکل ۵۵-۳ تنظیمات تلفن IP

www.takbook.com

۳-۷ کار با EtherChannel در لایه‌ی دوم

از کار افتادن شبکه، حتی برای چند لحظه، مشکل‌ساز خواهد بود، برای همین باید از روش‌هایی استفاده کنید تا در زمانی که یک مشکل برای یک کابل ایجاد شد، کل شبکه از رده خارج نشود.
برای اتصال سوئیچ‌ها به هم از چند خط استفاده کنید که اگر یکی یا دو تا از این خط‌ها از کار افتاد، سوئیچ به کار خود روی خط‌های دیگر ادامه دهد؛ برای این کار از EtherChannel استفاده کنید، برای انجام این کار دو سوئیچ به لیست اضافه کنید و ۴ کابل را به این سوئیچ‌ها، مانند شکل ۵۶-۳ متصل کنید:

شکل ۵۶-۳ مثال EtherChannel

همان‌طور که در شکل مشاهده می‌کنید، ۴ کابل به هر دو سوئیچ متصل شده است، اما به خاطر ایجاد Loop، الگوریتم STP فعال‌شده و فقط از یک کابل برای ارتباط با سوئیچ روبرو استفاده کرده است. برای حل چنین مشکلی باید الگوریتم STP طوری تنظیم کنیم که این ۴ کابل را به صورت یک کابل مشاهده کند، لذا از EtherChannel استفاده می‌کنیم.

Etherchannel با ایجاد گروهی از پورت‌های مورد نظر، باعث می‌شود که چند پورت به صورت یک پورت عمل کنند. با این کار باعث ایجاد Redundancy در سوئیچ شده و با قطع شدن یکی از کابل‌ها سوئیچ به کار خود ادامه می‌دهد. این نکته را هم توجه داشته باشید که Etherchannel روی روترها و سرورها هم کارایی دارد.
برای ایجاد EtherChannel چه کاری باید انجام دهیم؟

- پورت‌ها باید یا به صورت Full Duplex و یا به صورت Half Duplex باشند.
- پورت‌ها باید یک نوع داشته باشند، یعنی همگی Fast Ethernet باشند.
- پورت‌ها از سرعت یکسانی برخوردار باشند.
- همگی عضو یک VlAN باشند.
- همگی Trunk باشند که در صورت Trunk بودن، باید در یک Native VLAN قرار داشته باشند.

www.takbook.com

۳-۸ پروتکل‌های EtherChannel

برای ارتباط دو سوئیچ به روش EtherChannel، باید پروتکل‌های مربوط به آن را معرفی کنیم تا دو سوئیچ بتوانند با هم صحبت کنند.

***PAgP** (Port Aggregation Protocol)*

پروتکل PAgP که از ساخته‌های سیسکو است، برای ارتباط دو سوئیچ که EtherChannel روی آن‌ها اجرا شده است، به کار می‌رود. این پروتکل به دو صورت تنظیم می‌شود؛ اگر به صورت Desirable روی سوئیچ اجرا شود به سوئیچ‌های مقابل خود، تقاضای ایجاد Etherchannel می‌دهد، البته به صورت پیش‌فرض بر روی Auto قرار دارد.

۳-۸-۱ LACP (Link Aggregation Control Protocol)

پروتکل LACP می‌تواند ۱۶ پورت را در یک Etherchannel قرار دهد که در یک زمان از ۸ عدد آن استفاده می‌کند و ۸ پورت دیگر به حالت Standby می‌رود و هنگامی‌که یکی از آن‌ها با مشکل مواجه شد، این پورت‌ها جایگزین آن‌ها می‌شوند.

این پروتکل به دو صورت تنظیم می‌شود؛ اگر Active باشد به سوئیچ مقابل خود، تقاضای ایجاد Etherchannel را می‌فرستد و اگر Passive باشد، منتظر می‌ماند و فقط گوش می‌کند.

ایجاد EtherChannel

به مانند شکل ۵۷-۳، دو سوئیچ به صفحه اضافه کنید و به صورت زیر به هم متصل کنید:

شکل ۵۷-۳ مثال EtherChannel

در مرحله‌ی اول، باید وارد هر ۴ پورت به طور هم‌زمان شوید؛ برای این کار وارد سوئیچ ۱ شوید و دستور زیر را وارد کنید.

```
Switch(config)# int range fastEthernet 0/1 - 4
Switch(config-if-range)#
```

www.takbook.com

با دستور int range fastethernet 0/1 - 4 همزمان وارد ۴ پورت شوید و می‌توانید این ۴ پورت را به صورت همزمان کنترل کنید. بعد از این کار، نوبت به تعریف Etherchannel می‌رسد. برای تعریف EhterChannel، باید از دستور Channel-Group استفاده کنیم.

```
Switch(config-if-range)#channel-group ?
 <1-48>  Channel group number
```

با واردکردن دستور Channel-group و قرار دادن علامت سؤال، به شما تعداد Channel-group که می‌توانید ایجاد کنید را نمایش می‌دهد که در این قسمت، شماره‌ی یک را انتخاب می‌کنیم و در ادامه، دستور Mode را قرار می‌دهیم و بعد علامت سؤال که انواع روش‌های ایجاد Channel-Group را نمایش می‌دهد.

```
Switch(config-if-range)#channel-group 1 mode ?
 Enable LACP unconditionally     active
 Enable PAgP only if a PAgP device is detected     auto
Enable PAgP unconditionally   desirable
 Enable Etherchannel only       on
 Enable LACP only if a LACP device is detected    passive
```

در قسمت بالا، انواع مدهای ایجاد channel-Group را مشاهده می‌کنید که مدهای Active وPassive و مدهای Auto و Desirable باهم کار می‌کنند و مد On به صورت جدا کار می‌کند.

کار با مدهای Active و passive

نکته‌ی مهم:

قبل از ایجاد مد Active، این نکته را در نظر داشته باشید که زمانی‌که Active فعال شود، شروع به Negotiation یا مذاکره می‌کند که اگر کسی به وی جواب ندهد، پورت مورد نظر Shutdown می‌شود و از کار می‌افتد، پس سعی کنید اول از Passive استفاده کنید و بعد از آن از Active استفاده کنید.

با دستور زیر وارد چهار پورت سوئیچ شوید و دستور channel-group 1 mode passive را اجرا کنید:

```
SW1(config)# int  rang  f0/1 - 4
SW1(config-if-range)# channel-group 1 mode passive
```

در ادامه کار وارد سوئیچ ۲ شوید و دستور زیر را وارد می‌کنیم:

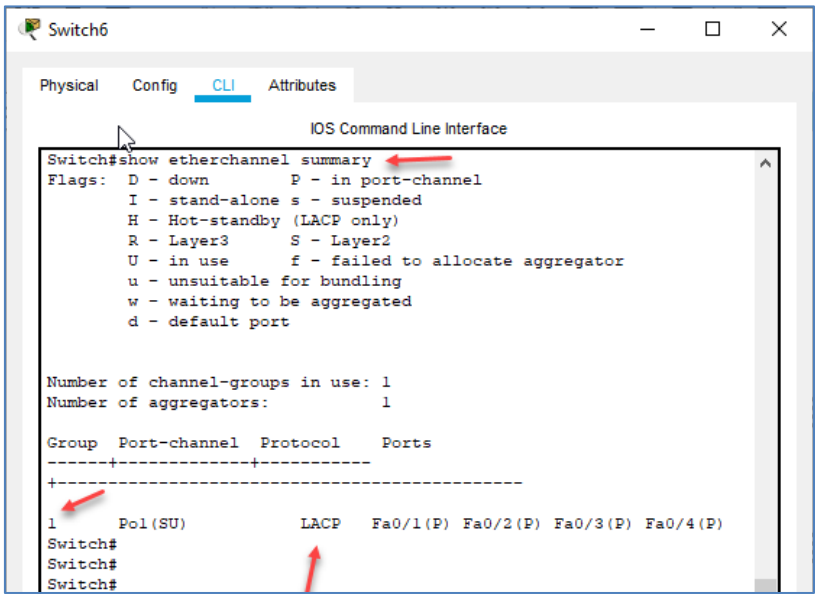
```
SW2(config)# int rang fa 0/1 - 4
SW2(config-if-range)# channel-group 1 mode active
```

بعد از این کار، دو سوئیچ بر روی ۴ خط کار می‌کنند که در شکل ۵۸-۳، این موضوع را مشاهده می‌کنید.

www.takbook.com

شکل ۳-۵۸ مثال *EtherChannel*

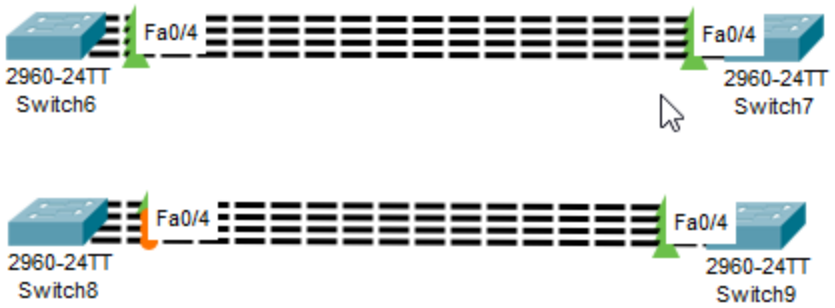
اگر وارد سوئیچ۱ شوید و دستور شکل ۳-۵۹، را وارد کنید اطلاعاتی از channel Group را مشاهده خواهید کرد، در قسمت Group شماره‌ی یک نوشته شده است و در قسمت Protocol نوشته شده LACP که در قسمت قبل توضیح دادیم.



شکل ۳-۵۹ نتیجه‌ی دستور *Show etherchannel summary*

در شکل ۳-۶۰، چهار سوئیچ را مشاهده می‌کنید که چهار کابل به آنها متصل شده است، در دو سوئیچ بالایی Channel-Group فعال شده است و همه لینک‌های آن فعال است ولی در دو سوئیچ پائینی آن این پروتکل فعال نشده است و فقط یکی از پورت‌های Switch8 فعال است و بقیه پورت‌ها برای جلوگیری از Loop بلاک شده‌اند، آن هم به خاطر وجود پروتکل STP است که قبلاً آن را بررسی کردیم.

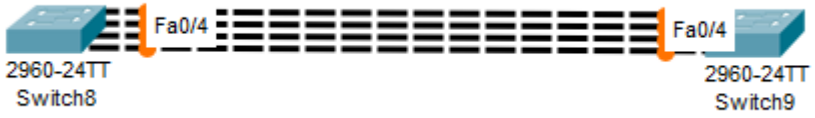
www.takbook.com



شکل ۶۰-۳ مثال Channel-Group

کار با مدهای Auto و desirable

به مانند مثال قبلی دو سوئیچ را به صفحه اضافه کنید و کابل‌های آنها را به هم متصل کنید.



شکل ۶۱-۳ مثال Channel-Group

وارد سوئیچ Switch8 شوید و دستورات زیر را وارد کنید:

```
Switch(config)#interface range fastEthernet 0/1-4
Switch(config-if-range)#channel-group 1 mode auto
```

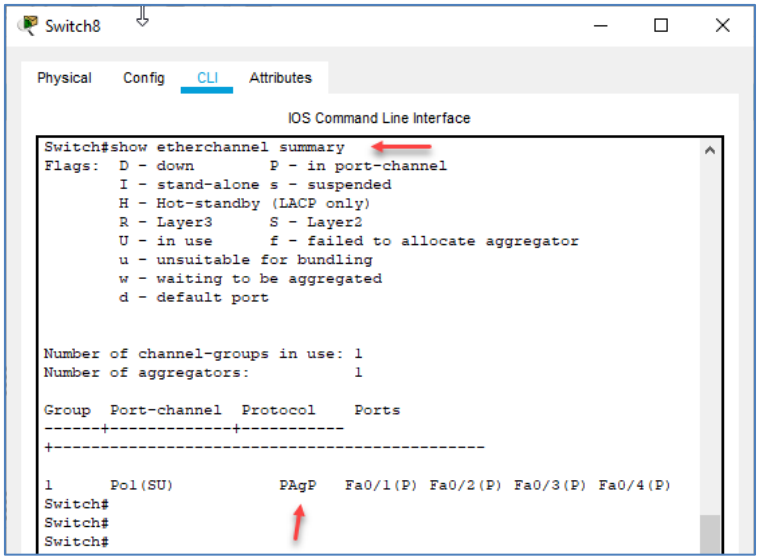
در سوئیچ Switch9 هم دستورات زیر را وارد کنید تا این دو گزینه هم فعال شود:

```
Switch(config)#int range fastEthernet 0/1-4
Switch(config-if-range)#channel-group 1 mode desirable
```

با اجرای دستورات بالا مدهای Auto و desirable نیز بر روی سوئیچ فعال خواهد شد و هر چهار لینک به صورت هم‌زمان کار خواهند کرد.

با اجرای دستور Show etherchannel summary می‌توانید اطلاعات مورد نظر خود را در شکل ۶۲-۳، مشاهده کنید، اگر توجه کنید نوع پروتکل را در این قسمت PAgP در نظر گرفته است.

www.takbook.com

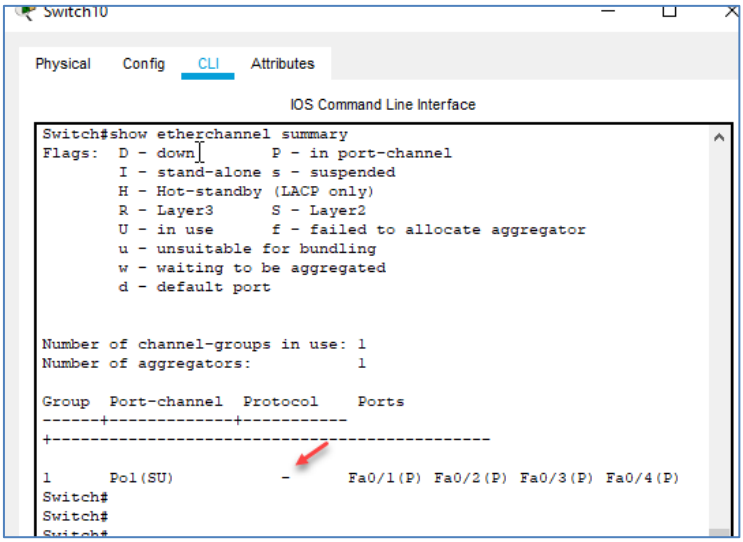


شکل ۶۲-۳ نتیجه‌ی دستور Show etherchannel summary

توجه داشته باشید گزینه ON هم در مدها وجود دارد که خودش به تنهایی کار می‌کند و در هر سوئیچ باید به صورت زیر شود:

Switch(config)#**int ran fastEthernet 0/1-4**
Switch(config-if-range)#**channel-group 1 mode on**

اگر نتیجه کار را به مانند شکل ۶۳-۳، مشاهده کنید در قسمت Protocol هیچ چیزی نوشته نیست و این نشان دهنده‌ی این است که مد در حالت ON است.



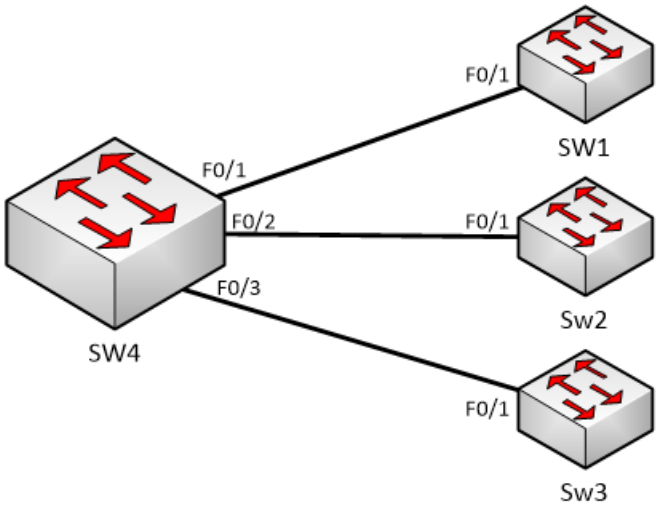
شکل ۶۳-۳ نتیجه‌ی دستور Show etherchannel summary

www.takbook.com

۲-۸-۳ دستور CDP (Cisco discovery Protocol)

این دستور که از سری دستورات شرکت سیکو است، دستگاه‌های متصل به یک روتر یا سوئیچ و ... را نمایش می‌دهد، مثلاً شما وارد شبکه‌ای شده‌اید که از ساختار آن خبر ندارید، می‌توانید با استفاده از این دستور دستگاه‌های متصل به دستگاه مورد نظر را بیابید.

با این مثال کاملاً این موضوع را درک می‌کنید.



شکل ۶۴-۳ مثال CDP

با توجه به شکل ۶۴-۳، از ۴ سوئیچ استفاده می‌کنیم که سوئیچ‌های ۱، ۲ و ۳ به سوئیچ ۴ متصل هستند. زمانی برای شما اتفاق می‌افتد که وارد تنظیمات سوئیچ می‌شوید و می‌خواهید بدانید چه دستگاه‌هایی از چه مدلی به این سوئیچ متصل است، برای این کار از دستور زیر استفاده کنید:

وارد سوئیچ ۴ شوید و در مد Privileged، دستور زیر را وارد کنید:

```
SW4# show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone
Device ID    Local Intrfce   Holdtme   Capability   Platform   Port ID
SW1          Fas 0/1         151       S            2950       Fas 0/1
SW3          Fas 0/3         155       S            2950       Fas 0/1
SW2          Fas 0/2         153       S            2950       Fas 0/1
```

همان‌طور که مشاهده می‌کنید با اجرای دستور show cdp neighbors، لیست سوئیچ‌های متصل به این سوئیچ را با ویژگی‌های سوئیچ‌های مربوطه نمایش داد.

در این دستور شماره‌ی پورت، شماره‌ی دستگاه، نوع دستگاه، پورت ورودی به سوئیچ و مقدار زمانی که طول کشید سوئیچ دستگاه‌های متصل به خودش را شناسایی کند را نمایش می‌دهد.

www.takbook.com

برای اینکه به جزئیات بیشتر در مورد دستگاه‌های متصل شده دست پیدا کنیم از دستور زیر استفاده می‌کنیم:

```
Switch#show cdp neighbors detail

Device ID: Switch
Entry address(es):
Platform: cisco 2960, Capabilities: Switch
Interface: Port-channel1, Port ID (outgoing port): FastEthernet0/1
Holdtime: 169

Version :
Cisco IOS Software, C2960 Software (C2960-LANBASE-M), Version 12.2(25)FX, RELEASE
SOFTWARE (fc1)
Copyright (c) 1986-2005 by Cisco Systems, Inc.
Compiled Wed 12-Oct-05 22:05 by pt_team

advertisement version: 2
Duplex: full
---------------------------

Device ID: Switch
Entry address(es):
Platform: cisco 2960, Capabilities: Switch
Interface: Port-channel1, Port ID (outgoing port): FastEthernet0/1
Holdtime: 169

Version :
Cisco IOS Software, C2960 Software (C2960-LANBASE-M), Version 12.2(25)FX, RELEASE
SOFTWARE (fc1)
Copyright (c) 1986-2005 by Cisco Systems, Inc.
Compiled Wed 12-Oct-05 22:05 by pt_team

advertisement version: 2
Duplex: full
---------------------------
```

پروتکل CDP هر ۶۰ ثانیه یک‌بار، اطلاعات مربوط را به دستگاه‌های متصل به خود ارسال می‌کند و دستگاه‌هایی که این پیام را دریافت می‌کنند در جدولی که معرفی کردیم، این اطلاعات را ذخیره می‌کنند.

www.takbook.com

۹-۳ سوالات فصل سوم

1. In a LAN, which of the following terms best equates to the term VLAN?
در یک شبکه‌ی محلی کدام یک از اصطلاحات زیر با VLAN برابر است؟

a. Collision domain
b. Broadcast domain
c. Subnet
d. Single switch
e. Trunk

2. Imagine a switch with three configured VLANs. How many IP subnets are required, assuming that all hosts in all VLANs want to use TCP/IP?
سوئیچ را با سه VLAN تصور کنید، چند IP subnets نیاز است برای این سه تا VLAN با فرض اینکه همه‌ی میزبان‌ها در کلیه‌ی VLANها می‌خواهند از TCP / IP استفاده کنند.

a. 0
b. 1
c. 2
d. 3
e. You cannot tell from the information provided.

3. Switch SW1 sends a frame to switch SW2 using 802.1Q trunking. Which of the answers describes how SW1 changes or adds to the Ethernet frame before forwarding the frame to SW2?
سوئیچ یک می‌خواهد یک Frame را از طریق پروتکل Trunk 802.1Q به سوئیچ دوم ارسال کند، کدام یک از گزینه‌های زیر نحوه‌ی تغییر یا اضافه کردن به Frame را قبل از ارسال به سوئیچ دوم نشان می‌دهد؟

a. Inserts a 4-byte header and does change the MAC addresses
b. Inserts a 4-byte header and does not change the MAC addresses
c. Encapsulates the original frame behind an entirely new Ethernet header
d. None of the other answers are correct

4. Imagine that you are told that switch 1 is configured with the dynamic auto parameter for trunking on its Fa0/5 interface, which is connected to switch 2. You have to configure switch 2. Which of the following settings for trunking could allow trunking to work? (Choose two answers.)
تصور کنید به شما گفته شده است که پورت Fa0/5 را برای Trunking با پارامتر dynamic auto پیکربندی شده است و به سوئیچ دوم متصل شده است، شما باید سوئیچ دوم را برای این ارتباط پیکربندی کنید، کدام گزینه‌ها را برای این کار باید انتخاب کنید؟ (دو گزینه را انتخاب کنید)

a. on
b. dynamic auto
c. dynamic desirable
d. access
e. None of the other answers are correct.

5. A switch has just arrived from Cisco. The switch has never been configured with any VLANs, but VTP has been disabled. An engineer configures the vlan 22 and name Hannahs-VLAN commands and then exits configuration mode. Which of the following are true? (Choose two answers.)

www.takbook.com

یک سوئیچ سیسکو به دست شما رسیده است و بر روی آن هیچ VLAN پیکربندی نشده و پروتکل VTP هم بر روی آن غیرفعال شده است، یک مهندس بر روی آن یک VLAN با شماره‌ی 22 تعریف می‌کند و یک نام برای آن در نظر می‌گیرد، با این تفاصیل کدام یک از گزینه‌ها درست است؟ (دو مورد را انتخاب کنید.)

a. VLAN 22 is listed in the output of the show vlan brief command.
b. VLAN 22 is listed in the output of the show running-config command.
c. VLAN 22 is not created by this process.
d. VLAN 22 does not exist in that switch until at least one interface is assigned to that VLAN.

6. Which of the following commands identify switch interfaces as being trunking interfaces: interfaces that currently operate as VLAN trunks? (Choose two answers.)

کدام یک از گزینه‌های زیر مشخص می‌کند که یک Interface در حالت Trunk قرار دارد؟

a. show interfaces
b. show interfaces switchport
c. show interfaces trunk
d. show trunks

7. In a switch that disables VTP, an engineer configures the commands vlan 30 and shutdown vlan 30. Which answers should be true about this switch? (Choose two answers.)

پروتکل VTP در سوئیچ غیرفعال شده است، یک مهندس دستورات VLAN 30 و Shutdown Vlan 30 را اجرا می‌کند، کدام پاسخ باید در مورد این سوئیچ درست باشد؟ (دو گزینه را انتخاب کنید)

a. The show vlan brief command should list VLAN 30.
b. The show running-config command should list VLAN 30.
c. The switch should forward frames that arrive in access ports in VLAN 30.
d. The switch should forward frames that arrive in trunk ports tagged with VLAN 30.

8. The show interfaces g0/1 trunk command provides three lists of VLAN IDs. Which items would limit the VLANs that appear in the first of the three lists of VLANs?

دستور زیر لیست VLANها را به ما نشان می‌دهد، کدام یک از گزینه‌های زیر لیست VLAN را محدود می‌کند؟

a. A shutdown vlan 30 global command
b. A switchport trunk allowed vlan interface subcommand
c. An STP choice to block on G0/1
d. A no vlan 30 global command

9. What is the default behavior of a Layer 2 switch when a frame with an unknown destination MAC address is received?

رفتار پیش‌فرض سوئیچ Layer 2 هنگام دریافت یک فریم با آدرس MAC مقصد ناشناخته چیست؟

A. The Layer 2 switch forwards the packet and adds the destination MAC address to its MAC address table.
B. The Layer 2 switch sends a copy of a packet to CPU for destination MAC address learning.
C. The Layer 2 switch floods packets to all ports except the receiving port in the given VLAN.
D. The Layer 2 switch drops the received frame.

www.takbook.com

www.takbook.com

www.takbook.com

www.takbook.com

فصل چهارم

بررسی IPV4

IPV4 یا همان Internet Protocol version 4 در سال ۱۹۸۱ توسط گروه IETF؛ که به گروه ویژه مهندسی اینترنت معروف هستند ایجاد شده است و شماره‌ی جهانی آن RFC 791 است که البته قبل آن RFC 760 بوده است.

هر آدرس IPv4 شامل 32 بیت است که از 4 بخش 8 بیتی تشکیل شده‌است .در نتیجه فضای نشانی آن 2 به توان 32 نشانی است که تعداد آن 4,294,967,296 است.

یک سری از این آدرس‌ها برای مقاصد خاصی مانند شبکه‌های خصوصی (تقریباً ۱۸ میلیون نشانی) و (چند پخشی تقریباً ۲۷۰ میلیون نشانی) رزرو شده‌است که البته به نسبت سیستم‌هایی که هم اکنون وجود دارد تعداد آن زیاد نیست و در حال حاضر هم این نوع آدرس در حال اتمام است.

همان‌طور که گفتیم، IPv4 از چهار قسمت تشکیل شده است که هر بخش، ۸ بیت است و اگر ۸ ضربدر ۴ کنیم، می‌شود 32 بیت، به آدرس زیر توجه کنید.

۱۹۲.۱۶۸.۱.۱

به هر یک از این قسمت‌ها، یک هشت‌تایی یا همان octet می‌گویند. مثلاً در IP بالا به شماره‌ی 192 یک octet می‌گویند.

IPV4 به پنج کلاس تقسیم می‌شوند که در شکل ۱-۴ آنها را مشاهده می‌کنید.

Class A:	1 – 126
Class B:	128-191
Class C:	192- 223
Class D:	224 – 239
Class E:	240 – 255

شکل ۱-۴ کلاس IPV4

www.takbook.com

مثال

192.168.1.1 که عدد اول آن ۱۹۲ است، این IP در رنج کلاس c قرار دارد. به همین صورت اگر Octed اول در یکی از رنج‌های مشخص‌شده‌ی بالا قرار داشته باشد، می‌گوییم که در این کلاس قرار دارد. مثلاً، 10.10.10.1 یک IP در کلاس A است، چون 10 عدد قسمت اول آن است و بین شماره 1-126 قرار دارد.

تذکر: رنج IP کلاس A از 126 - 1 است و شماره‌ی 127 برای تست کارت شبکه به کار می‌رود که همان 127.0.0.1 است و به آدرس loopback معروف است، پس برای استفاده از کلاس A می‌توان از شماره‌ی 1 – 126 استفاده کرد.

توجه داشته باشید که کلاس D برای Multicasting به کار می‌رود، این IPها روی هاست یا همان سیستم تنظیم نمی‌شوند و IPهای کلاس E برای تحقیقات به کار می‌رود و قابل‌استفاده نیست، پس فقط از IPهای کلاس‌های A,B,C برای شبکه خود استفاده می‌کنیم.

IPها به دو دسته تقسیم می‌شوند:

Private Address

این دسته از IP، فقط و فقط در شبکه‌های داخلی به کار می‌روند و در دنیای اینترنت اعتباری ندارند. این نوع از IP ها در هر کلاس وجود دارند که در شکل ۲-۴ مشخص شده‌اند.

Class A:	10.0.0.0
Class B:	172.16.0.0
Class C:	192.168.0.0

شکل ۲-۴ کلاس IPV4

توجه داشته باشید اگر بخواهید دو شرکت در یک شهر را به این آدرس‌های به هم متصل کنید باید از امکاناتی دیگر برای این کار استفاده کنید، مثلاً می‌توانید یک بستر VPN بین دو شرکت ایجاد و بعد از طریق این IP ها با هم در ارتباط باشند.

IPهایی که با این اعداد شروع می‌شوند، مربوط به شبکه‌ی داخلی هستند و اعتباری در اینترنت ندارند. در جدول ۱-۴، لیستی از آدرس‌ها را مشاهده می‌کنید که برای مقاصد خاص طراحی شده‌اند.

www.takbook.com

جدول ۱-۴ لیست آدرس‌های خاص

بلوک آدرس	توضیح	شماره‌ی جهانی
0.0.0.0	شبکه جاری (تنها به عنوان نشانی مبدأ معتبر است)	RFC 1700
10.0.0.0	شبکه خصوصی (شبکه‌ی داخلی)	RFC 1918
127.0.0.0	آدرس بازگشت(Loopback)	RFC 5735
169.254.0.0	Link-Local	RFC 3927
172.16.0.0	شبکه خصوصی	RFC 1918
192.0.0.0	پیکربندی خودکار نشانی برای لایه پیوند (IANA)	RFC 5735
192.0.2.0	TEST-NET-1، مستندسازی و نمونه کد	RFC 5735
192.88.99.0	رله IPv6 به IPv4	RFC 3068
192.168.0.0	شبکه خصوصی	RFC 1918
192.18.0.0	آزمایش‌های محک زدن شبکه	RFC 2544
198.51.100.0	TEST-NET-2، مستندسازی و مثال‌ها	RFC 5737
203.0.113.0	TEST-NET-3، مستندسازی و مثال‌ها	RFC 5737
224.0.0.0	شبکه کلاس D	RFC 3171
240.0.0.0	شبکه کلاس E	RFC 1700
255.255.255.255	پخش گسترده(Broadcast)	RFC 919

Public Address

این دسته از IPها توسط سازمانی به نام IANA رجیستر می‌شوند و بعد از این کار در اینترنت اعتبار دارند. این دسته شامل تمام IPهای کلاس‌های A,B,C است، به غیر از آدرس‌های Privateکه در قسمت قبل باهم بررسی کردیم.

یک IP از دو بخش تشکیل شده است

- ✓ Network address
- ✓ Host address

www.takbook.com

Network Address، به تعداد شبکه‌های موجود و Host address، به تعداد میزبان موجود اشاره دارد.
برای اینکه بتوانیم این دو موضوع را درک کنیم، باید subnet mask را بررسی کنیم.

Subnet Mask

این آدرس، نشان‌دهنده‌ی این است که چه مقدار بیت متعلق به آدرس شبکه و چه مقدار آن، متعلق به میزبان شبکه است.

جدول ۲-۴ آدرس‌های Subnet

Class	IP	Subnet Mask
A	**11.1.5.1**	255.0.0.0
B	**175.1.1.1**	255.255.0.0
C	**192.168.1.1**	255.255.255.0

همان‌طور که در جدول ۲-۴، مشاهده می‌کنید برای هر IP در کلاس مشخص، یک subnet mask تعریف شده است که نشان‌دهنده‌ی تعداد شبکه و هاست است.

اگر به جدول توجه کنید در قسمت Subnet Mask اعداد ۲۵۵ مربوط به Network Address و اعداد 0 مربوط به Host address می‌باشند.

مثلاً اگر IP به شماره 195.1.1.1 به شما بدهند و بگویند subnet Mask آن را مشخص کنید، سریع با نگاه کردن به کلاس‌های IP متوجه می‌شوید که عدد اول این IP در رنج کلاس c قرار دارد وSubnet Mask آن به‌صورت 255.255.255.0 است.

همیشه روال به این صورت نیست که IPها به همین صورت استاندارد در شبکه‌ها نشان داده شوند به این کلاس‌بندی‌ها اصولاً یک الگوی استاندارد می‌گویند، امّا همیشه این‌چنین نیست و الگوی غیراستاندارد هم وجود دارد.

مثلاً آدرس IP زیر را با Subnet آن در نظر بگیرید، طبق جدول ۳-۴ آدرس‌هایی که به آن تعلق می‌گیرد مشخص شده است.

172.16.0.0
255.255.0.0

جدول ۳-۴ لیست ادرس‌های ۱۷۲.۱۶.۰.۰

Subnet	IP Address	Broadcast Address
172.16.0.0	172.16.0.1 – 172.16.0.254	172.16.0.255
172.16.1.0	172.16.1.1 – 172.16.0.254	172.16.1.255
172.16.2.0	172.16.2.1 – 172.16.0.254	172.16.2.255
172.16.3.0	172.16.3.1 – 172.16.0.254	172.16.3.255
172.16.4.0	172.16.4.1 – 172.16.0.254	172.16.4.255
تا . .	تا . .	تا . .

www.takbook.com

.	.	.
172.16.254.0	172.16.254.1 – 172.16.0.254	172.16.254.255
172.16.255.0	172.16.255.1 – 172.16.0.254	172.16.255.255

تذکر

همانطور که قبلاً گفتیم آدرس‌های Broadcast به آدرس‌هایی گفته می‌شود که برای ارسال گروهی پیام مورد استفاده قرار می‌گیرند.

همانطور که گفتیم الگوهایی که در بالا معرفی کردیم یک الگوی استاندارد بوده و تابع قوانین خاص خودش هست، اما الگوی غیر استاندارد هم وجود دارد که با هم آن را بررسی می‌کنیم.

در جدول ۴-۴، اطلاعات کاملتری از سه کلاس A,B,C را مشاهده می‌کنید:

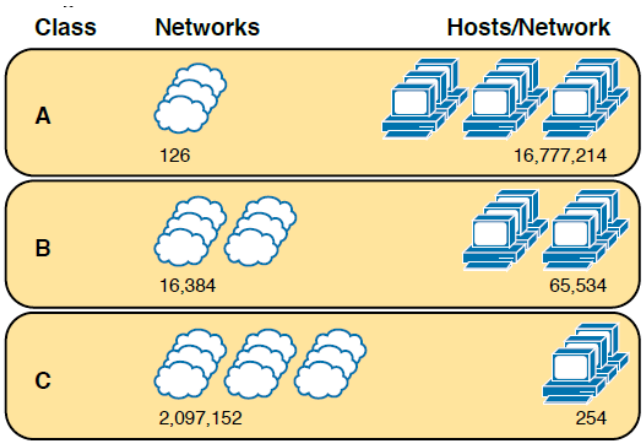
جدول ۴-۴ کلاس A,B,C

	Class A	Class B	Class C
First octet range	1–126	128–191	192–223
Valid network numbers	1.0.0.0–126.0.0.0	128.0.0.0–191.255.0.0	192.0.0.0–223.255.255.0
Total networks	$2^7 - 2 = 126$	$2^{14} = 16,384$	$2^{21} = 2,097,152$
Hosts per network	$2^{24} - 2$	$2^{16} - 2$	$2^8 - 2$
Octets (bits) in network part	1 (8)	2 (16)	3 (24)
Octets (bits) in host part	3 (24)	2 (16)	1 (8)
Default mask	255.0.0.0	255.255.0.0	255.255.255.0

در جدول ۴-۴، می‌توانید در سطر اول رنج شبکه‌ها را مشاهده کنید، در سطر دوم رنج آدرس IP را، در سطر سوم به تعداد کل شبکه‌های موجود اشاره دارد، در سطر چهارم به تعداد کل Hostهایی که پشتیبانی می‌کند اشاره دارد که در شکل ۳-۴، دقیق مشخص شده است که مثلاً در کلاس A تعداد ۱۲۶ شبکه داریم که در آن می‌تواند تا ۱۶ میلیون و ۷۷۷ هزار ۲۱۴ هاست را پشتیبانی کند که این عدد بسیار بزرگ است.

هر چقدر تعداد شبکه بیشتر باشد از آن طرف تعداد هاست آن کمتر خواهد شد که این موضوع را در کلاس C مشاهده می‌کنید.

www.takbook.com



شکل ۳-۴ کلاس A,B,C

برای اینکه بیشتر با Network و HOST کار کنید می‌توانید نگاهی به جدول ۵-۴، بندازید، در این جدول نام کلاس، تعداد شبکه و هاست و در آخر آدرس Network ID و Network Broadcast را مشاهده می‌کنید.

جدول ۵-۴ جزئیات کلاس IPV4

	IP Address	Class	Network Octets	Host Octets	Network ID	Network Broadcast
1	1.1.1.1	A	1	3	1.0.0.0	1.255.255.255
2	128.1.6.5	B	2	2	128.1.0.0	128.1.255.255
3	200.1.2.3	C	3	1	200.1.2.0	200.1.2.255
4	192.192.1.1	C	3	1	192.192.1.0	192.192.1.255
5	126.5.4.3	A	1	3	126.0.0.0	126.255.255.255
6	200.1.9.8	C	3	1	200.1.9.0	200.1.9.255
7	192.0.0.1	C	3	1	192.0.0.0	192.0.0.255
8	191.255.1.47	B	2	2	191.255.0.0	191.255.255.255
9	223.223.0.1	C	3	1	223.223.0.0	223.223.0.255

۴-۱ الگوهای غیراستاندارد

همانطور که گفتیم، به مانند شکل ۴-۴، هر قسمت IP (octet) از هشت عدد تشکیل شده است که می‌تواند صفر یا یک باشد.

www.takbook.com

11110111	11111110	11101011	11000111

شکل ۴-۴ Octed IP

هرکدام از این شماره‌ها در هر بخش دارای یک شماره اختصاصی هستند که به‌صورت زیر است.

1 2 4 8 16 32 64 128 این شماره‌ها، روی هرکدام از چهار بخش بالا به‌صورت جداگانه قرار می‌گیرند.

اولین قسمت از سمت چپ را در زیر مشاهده می‌کنید، به نحوه‌ی قرار گرفتن اعداد توجه کنید.

برای درک بهتر موضوع، به شکل ۵-۴، توجه کنید:

128	64	32	16	8	4	2	1
1	1	1	1	0	1	1	1

شکل ۵-۴ Octed IP

برای به دست آوردن Binary آدرس 192.168.1.1، طبق شماره‌هایی که در هر قسمت به شما گفتیم، عمل کنید.

مثلاً اگر بخواهید شماره‌ی 192 را از بین شماره‌های 1 2 4 8 16 32 64 128 به دست بیاوریم، همیشه از سمت چپ شروع می‌کنیم، می‌گوییم ۱۲۸ از ۱۹۲ کوچک‌تر است، پس زیر ۱۲۸ را ۱ قرار می‌دهیم ، در ادامه اگر ۶۴ را با ۱۲۸ که قبلاً به دست آوردیم جمع کنید می‌شود ۱۹۲ !!! چه جالب ۱۹۲ شد پس زیر ۶۴ هم ۱ قرار می‌دهیم؛ با این حساب، توانستیم شماره‌ی ۱۹۲ را پیدا کنیم، وقتی به شماره‌ی مورد نظر رسیدیم، زیر بقیه‌ی شماره‌ها صفر قرار می‌دهیم. طبق جدول ۶-۴.

جدول ۶-۴ آدرس باینری IPV4

128	64	32	16	8	4	2	1
1	1	0	0	0	0	0	0

پس شماره‌ی باینری به‌دست‌آمده، 11000000 است. بقیه‌ی اعداد هم به‌صورت زیر است.

جدول ۷-۴ آدرس باینری IPV4

192	168	1	1
11000000	10101000	00000001	00000001

اگر به جدول ۸-۴، توجه کنید، دقیقاً عدد باینری به همراه عدد Decimal آن مشخص شده است که می‌تواند به شما کمک کند.

جدول ۸-۴ آدرس باینری IPV4

www.takbook.com

Binary Mask Octet	Decimal Equivalent	Number of Binary 1s
00000000	0	0
10000000	128	1
11000000	192	2
11100000	224	3
11110000	240	4
11111000	248	5
11111100	252	6
11111110	254	7
11111111	255	8

برای اینکه با اعداد Binary و Decimal بیشتر کار کنیم، به جدول ۹-۴، توجه کنید در این جدول و در ستون Binary اعداد باینری، هر قسمت از IP را مشاهده می‌کنید، مثلاً در سطر اول اعداد 11111111 نشان دهنده‌ی عدد 255 است و عدد 11000000 برابر عدد 192 است.

جدول ۹-۴ آدرس باینری IPV4

Binary Mask	Logic	Decimal Mask
11111111 11111111 11000000 00000000	11111111 maps to 255 11000000 maps to 192 00000000 maps to 0	255.255.192.0
11111111 11111111 11111111 11110000	11111111 maps to 255 11110000 maps to 240	255.255.255.240
11111111 11111000 00000000 00000000	11111111 maps to 255 11111000 maps to 248 00000000 maps to 0	255.248.0.0

در یک رنج IP، دو نوع IP قابل‌استفاده نیستند، به مثال زیر توجه کنید (مهم):

IP : 192.168.1.1
Sbnet Mask :255.255.255.0

همان‌طور که آموختید، ۲۵۵ به این نکته اشاره می‌کند که IPهای 192.168.1 ثابت است یعنی همان Network و فقط octet آخر قابل‌تغییر از ۰ تا ۲۵۵ است یعنی همان Host. هر یک از قسمت‌های IP از ۰ تا ۲۵۵ قابل‌تغییر است.

این IP، فقط در قسمت آخر قابل‌تغییر است، بین ۰ تا ۲۵۵، همان‌طور که گفتیم دو IP در هر رنج مانند این IP قابل‌استفاده نیستند. به جدول ۱۰-۴، توجه کنید:

جدول ۱۰-۴ آدرس Network در IPV4

192.168.1.0	Network address

www.takbook.com

IP قابل‌استفاده	192.168.1.1
IP قابل‌استفاده	192.168.1.2
IP قابل‌استفاده	192.168.1.3
	⋮
Broadcast	192.168.1.255

اولین IP به‌عنوان Network address و آخرین IP به‌عنوان Broadcast Address انتخاب می‌شوند و نمی‌توانیم در شبکه از آن‌ها استفاده کنیم.

تذکر

نام دیگر Network address، Net ID است.

مثال: در IP زیر، Net ID و Broadcast ID را به دست آورید:

IP: 172.16.1.1
Subnetmask: 255.255.0.0

در این مثال،IP از رنج کلاس B است. همان‌طور که مشاهده می‌کنید، Subnet mask از دو تا 255 تشکیل شده است پس 2 قسمت اول IP، ثابت(172.16) و دو قسمت بعد قابل‌تغییرند، به این صورت نتیجه می‌دهد که:

Net ID: 172.16.0.0
Broadcast ID: 172.16.255.255

۲-۴ اختصاص دادن رنج IP به شبکه سازمان

شما در یک شرکت کار می‌کنید که از ۳ اتاق حسابداری، فروش و طراحی تشکیل شده است؛ در این اتاق‌ها، چندین کامپیوتر به مانند شکل ۶-۴، وجود دارد.

www.takbook.com

شکل ۶-۴ Octed IP

IP در رنج زیر می‌باشد.

192.168.1.0
255.255.255.0

سریع این IP را در ذهن خود تحلیل کنید، حداکثر IP قابل‌استفاده، ۲۵۵ عدد است .اگر متوجه شده باشید Subnet mask از سه قسمت ثابت تشکیل شده است که فقط گزینه‌ی آخر قابل‌تغییر از ۰ تا ۲۵۵ است.

برای اختصاص دادن IP به این اتاق‌ها، اول از همه، اتاقی را انتخاب می‌کنیم که بیشترین کامپیوتر را دارد که در این مثال، اتاق فروش از ۶۰ کلاینت برخوردار است.
همان‌طور که قبلاً گفتیم در هر قسمت از IP، اعدادی استاندارد و ثابتی وجود دارد.

128 64 32 16 8 4 2 1

همیشه این اعداد را در ذهن خود نگه داشته باشید، کل IP به همین اعداد خلاصه می‌شود و در ادامه، خیلی به آنها نیاز داریم.
شما اول باید ببینید ۶۰ بین کدام یک از اعداد بالا قرار دارد. با کمی دقت متوجه می‌شوید که بین ۳۲ و ۶۴ قرار دارد، چون ما احتیاج به ۶۰ تا IP داریم، پس عدد ۶۴ انتخاب می‌شود.
پس رنج IP به صورت زیر می‌شود:

192.168.1.0 To 192.168.1.63

همان‌طور که گفتیم، دو آدرس از این رنج برای Net ID و Broadcast ID است، یعنی رنج زیر:

Net ID: 192.168.1.0
Broadcast ID: 192.168.1.63

پس با کسر این دوIP، 62 آدرس برای ما می‌ماند که 60تا آدرس آن به کامپیوترها تخصیص داده می‌شود و 2، IP هم برای زمانی که اگر خواستیم کامپیوتر جدید در اتاق اضافه کنیم، به کار می‌بریم.

www.takbook.com

پس رنج IP واقعی می‌شود:

192.168.1.1 – 192.168.1.62

رنج IP را به دست آوردیم؛ ولی Subnet mask مربوط به این IP را به دست نیاوردیم؛ برای این کار همان عدد ۶۴ را که درون شماره‌ها به دست آوردیم منهای ۲۵۶ می‌کنیم (۲۵۶ عددی است که از اعداد ۰ تا ۲۵۵ به دست می‌آید).

256 - 64 = 192

پس Subnet mask برای این IP می‌شود:

255.255.255.192

که ۱۹۲ نشان‌دهنده‌ی 64، IP برای این شبکه است.

اتاق بعدی‌ای که انتخاب می‌شود، اتاق حسابداری است که شامل ۵۰ کامپیوتر است. برای به دست آوردن رنج IP برای این اتاق، از IPهایی که استفاده نشده است، استفاده می‌کنیم.
IPهایی که در اختیارداریم به‌صورت زیر است:

192.168.1.64

به این خاطر، از عدد 64 در آخر این IP استفاده کردیم که 64 تا آدرس به اتاق قبلی داده شده است و قابل‌استفاده نیست.

مانند اتاق قبلی، به 64، IP نیاز دارید، چون 50 بین 32 و 64 قرار دارد، پس 64 انتخاب می‌شود.
IP و Subnet mask برای این اتاق، به‌صورت زیر است:

192.168.1.64 To 192.168.1.127
255.255.255.192

که آدرس Net ID و Broadcast ID به صورت زیر خواهد بود:

Network Address: 192.168.1.64
Broadcast Address: 192.168.1.127

و رنج IP اصلی و قابل استفاده برای Host به صورت زیر است:

192.168.1.65 TO 192.168.1.126

برای اتاق سوم (طراحی)، احتیاج به 14، IP داریم، باید از بین 8 و 16 عدد 16 را انتخاب کنیم، پس IP و subnet mask به صورت زیر می‌شود:

192.168.1.128 To 192.168.1.143

www.takbook.com

255.255.255.240

که آدرس Net ID و Broadcast ID به صورت زیر خواهد بود:

Network Address: 192.168.1.128
Broadcast Address: 192.168.1.143

و رنج IP اصلی و قابل استفاده برای Host به صورت زیر است:

192.168.1.129 TO 192.168.1.142

باید متوجه شده باشید که ما احتیاج به 16، IP داریم، پس برای به دست آوردن Subnet mask باید ۱۶ را از ۲۵۶ کم کنیم تا عدد آخر که ۲۴۰ است به دست بیاید.

با این حساب، جدول IPها نهایی به‌صورت جدول ۱۰-۴، است:

جدول ۱۰-۴ رنج مشخص شده برای هر اتاق

فروش	حسابداری	طراحی
192.168.1.0~63	**192.168.1.64~127**	**192.168.1.128~143**
255.255.255.192	**255.255.255.192**	**255.255.255.240**
64	**64**	**16**

در این رنج‌ها، حداقل هدر رفت IP را داشتیم.

IP ها به دو نوع Class Full و Class Less تقسیم می‌شوند که کلاس‌های A,B,C از نوع Class Full هستند، به این دلیل به آن‌ها Class Full می‌گویند که subnet mask آن‌ها ثابت است و تغییری نمی‌کند، مثلاً 255.255.0.0 که این subnet مربوط به کلاس b است.

نوع دیگری از IPها وجود داردند که به عنوان Class Less شناخته می‌شوند و دارای قوانین ثابتی مانند Class Full نیستند که در ادامه آن را بررسی می‌کنیم.

۴-۳ بررسی CIDR

CIDR یا Class Less Inter-Domain Routing به عنوان IPهای Class Less شناخته می‌شوند، این دسته از IPها برای شرکت‌هایی که ارائه‌دهنده‌ی خدمات اینترنتی هستند(ISP) به کار می‌روند. برای این شبکه‌ها، مهم است که چه مقدار IP را به چه کسی می‌دهند.

IPهایی که به‌عنوان Class Less شناخته می‌شوند، به‌صورت زیر می‌باشند:

172.16.1.1/16

www.takbook.com

یک‌چیز جدید در این IP مشاهده می‌کنید و آن هم، یک slash به همراه یک شماره ۱۶ است که نشان‌دهنده‌ی تعداد شبکه یا همان Net ID است.

بعد از Slash، عددی بین ۱ تا ۳۲ قرار می‌گیرد. این همان عددی است که در ابتدای کار اشاره کردیم، یعنی هر IP از چهار قسمت هشت‌تایی تشکیل‌شده که می‌شود ۳۲ تا، توجه داشته باشید که حداکثر عددی که پشت slash قرار می‌گیرد ۳۰ است، چون ۲ بیت برای host Bite است.

مثال: تعداد Host و Subnet mask رنج IP زیر را به دست می‌آوریم:

192.168.1.1/24

سریع‌ترین روش برای به دست آوردن جواب به‌صورت زیر است:

هر قسمت از IP از هشت بیت تشکیل شده است که به صورت زیر است:

شکل ۷-۴ بررسی IP و Subnet Mask

در مثالی که زدیم 24/ است که اگر به شکل ۷-۴، نگاه کنید 3 تا octet اول را باهم جمع کنیم ۲۴ می‌شود، پس می‌توان IP و Subnet mask را به این صورت نوشت:

192.168.1.0
255.255.255.0

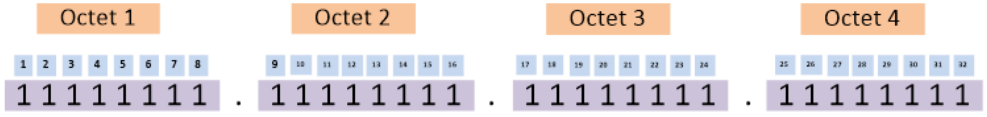
24/ می‌گوید که 3 تا octet اول ثابت باشد و octet آخر تغییر کند.

مثال دیگر :

172.16.1.1/17

اگر به مثال توجه کنید 16 عدد اول را داریم، پس ۲تا عدد اول IP ثابت است که در یک‌گوشه می‌نویسیم 172.16 بعد عدد ۱۷ در octet سوم قرار دارد؛ پس، فقط با octet سوم کار می‌کنیم.

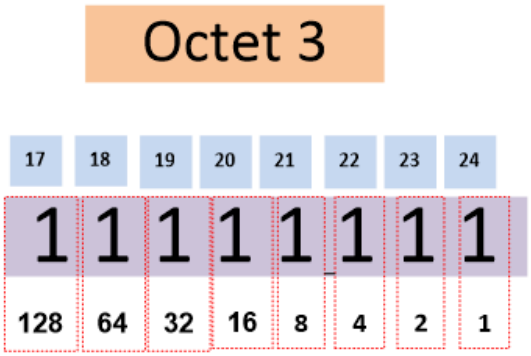
سریع اعداد ۱ ۲ ۴ ۸ ۱۶ ۳۲ ۶۴ ۱۲۸ یادداشت می‌کنیم و بعد از آن، این اعداد را بالای عدد ۱۷ تا ۲۴ از سمت چپ به راست قرار می‌دهیم تا عدد ۱۷ را پیدا کنیم. به شکل ۸-۴، توجه کنید:



شکل ۸-۴ بررسی Octed

www.takbook.com

در شکل ۸-۴، به راحتی می‌توانید درک کنید که 17/ یعنی چه، ببینید سؤال از ما 17/ را می‌خواهد، پس طبق شکل ۸-۴، ما با octed شماره‌ی 3 کار داریم و دو octet اول را به‌صورت ثابت می‌نویسیم، چون تمام اعداد آن ۱ است، پس برای به دست آوردن عدد ۱۷، باید اعداد ۱ ۲ ۴ ۸ ۱۶ ۳۲ ۶۴ ۱۲۸ را یادداشت کرده و از سمت چپ، اعداد ۱۷ تا ۲۴ را به آن‌ها اختصاص دهیم، یعنی عدد اولی که ۱۲۸ باشد، به عنوان عدد ۱۷ است و عدد دوم که عدد ۶۴ باشد، به عنوان عدد ۱۸ است. به شکل ۹-۴، توجه کنید:

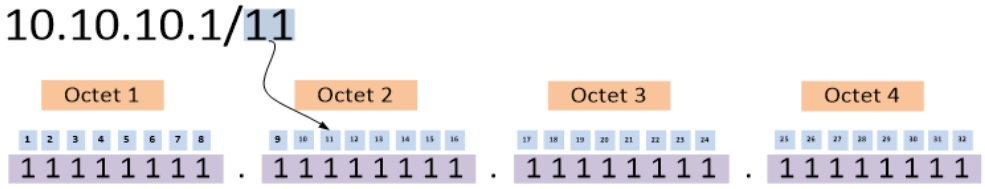


شکل ۹-۴ بررسی Octed

پس ۱۷ همان عدد ۱۲۸ است. این عدد را از ۲۵۶ کم می‌کنیم و Subnet mask **ما به دست می‌آید.**

172.16.0~127.0
255.255.128.0

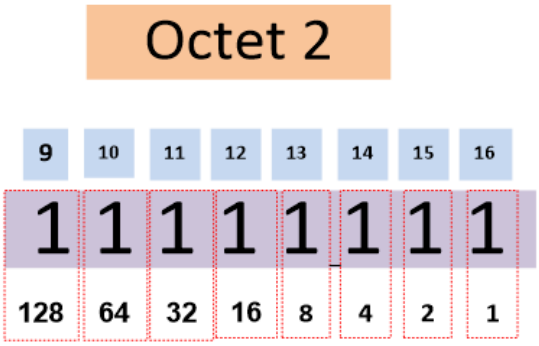
مثال آخر:



شکل ۱۰-۴ بررسی Octed

همان‌طور که در شکل ۱۰-۴، مشاهده می‌کنید 11/ از octed اول رد شده است، پس با octed دوم کار داریم این قسمت از عدد ۹ شروع شده و به ۱۶ ختم می‌شود. عددی که در مثال گفته 11/ است، پس از ۹ و ۱۰ باید بگذریم تا به عدد ۱۱ برسیم. برای این منظور اعداد ۱ ۲ ۴ ۸ ۱۶ ۳۲ ۶۴ ۱۲۸ و از سمت چپ اعداد را با شماره ۹ و بعد ۱۰ و بعد ۱۱ شماره‌گذاری می‌کنیم، مانند شکل ۱۱-۴، عدد زیر ۱۱ که عدد ۳۲ است را از ۲۵۶ کم می‌کنیم که ۲۲۴ به دست می‌آید.

www.takbook.com

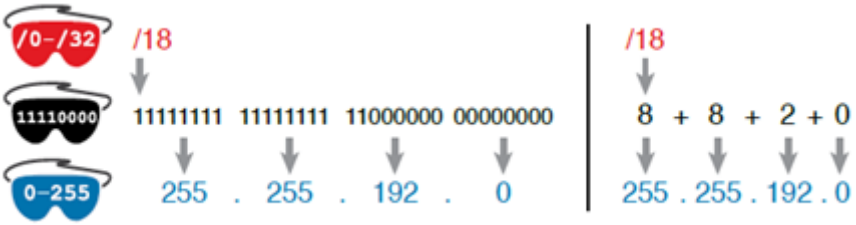


شکل ۱۱-۴ بررسی Octed

10.0~31.0.0
255.224.0.0

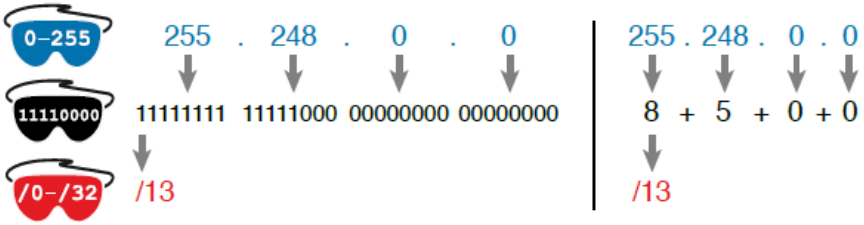
برای اینکه بیشتر با مباحث این بخش آشنا شویم روش‌های دیگری را هم با هم بررسی می‌کنیم.

در شکل ۱۲-۴، عدد 18/ را مشاهده می‌کنید که مشخص شده است این عدد از بین اعداد ۰ تا ۳۲ انتخاب شده است، یعنی اینکه دو قسمت اول Subnet Mask که ۱۶ بیت است ثابت نوشته می‌شود (255.255) و بعد از آن ۲ بیت نیاز است که می‌شود 192 .



شکل ۱۲-۴ بررسی 18/ در IPV4

در شکل ۱۳-۴، جزئیات عدد 13/ را مشاهده می‌کنید.



شکل ۱۳-۴ بررسی 13/ در IPV4

www.takbook.com

جدول ۱۱-۴ را برای شما به عنوان تمرین آماده کردیم که باید اطلاعات آن را تکمیل کنید، در این جدول در قسمت Prefix باید اعداد CIDR را وارد کنید، مثلاً در سطر اول عدد Prefix می‌شود 18/ و قسمت Decimal می‌شود 255.255.192.0 و به همین ترتیب به عنوان تمرین بقیه جاهای خالی را پر کنید.

جدول ۱۱-۴ تمرین CIDR

Prefix	Binary Mask	Decimal
/18	11111111 11111111 11000000 00000000	**255.255.192.0**
		255.255.255.252
/25		
/16		
		255.0.0.0
	11111111 11111111 11111100 00000000	
		255.254.0.0
/27		

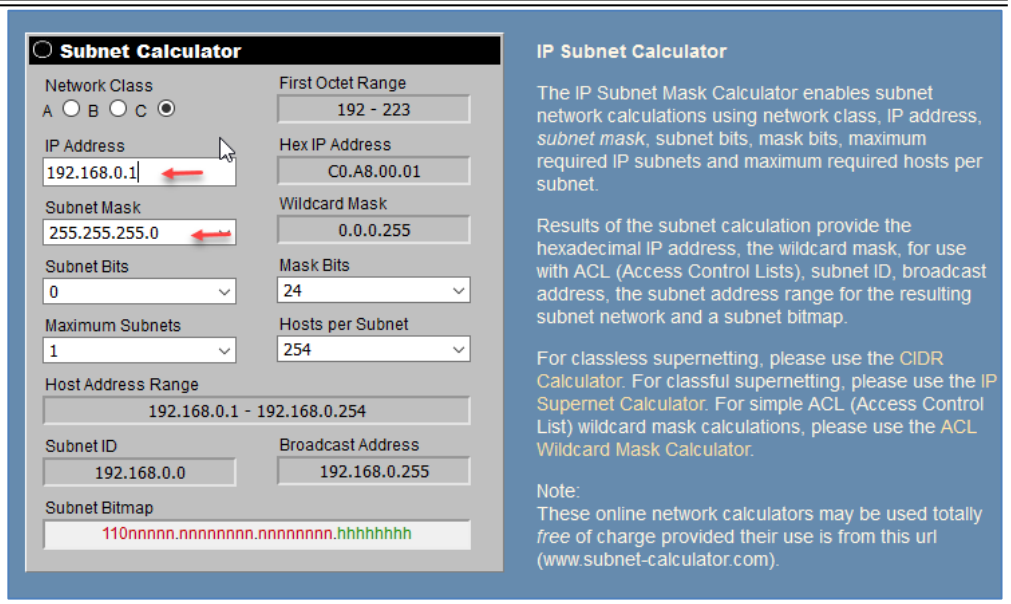
اگر جدول ۱۱-۴، را تکمیل کردید می‌توانید پاسخ آن را در جدول ۱۲-۴، مشاهده کنید:

جدول ۱۲-۴ جواب تمرین CIDR

Prefix	Binary Mask	Decimal
/18	11111111 11111111 11000000 00000000	255.255.192.0
/30	11111111 11111111 11111111 11111100	255.255.255.252
/25	11111111 11111111 11111111 10000000	255.255.255.128
/16	11111111 11111111 00000000 00000000	255.255.0.0
/8	11111111 00000000 00000000 00000000	255.0.0.0
/22	11111111 11111111 11111100 00000000	255.255.252.0
/15	11111111 11111110 00000000 00000000	255.254.0.0
/27	11111111 11111111 11111111 11100000	255.255.255.224

برای اینکه بیشتر با بحث IP ها آشنا شوید، بهتر است سایت‌هایی که برای این منظور طراحی شده است را مشاهده کنید، سایت http://www.subnet-calculator.com یکی از سایت‌های بسیار خوب در این زمینه است که با ورود به آن با صفحه زیر مواجه خواهید شد.

www.takbook.com



شکل ۱۴-۴ بررسی سایت subnet-calculator

در شکل ۱۴-۴، در قسمت IP Address می‌توانید IP دلخواه خود را وارد کنید و در قسمت Subnet Mask هم باید Subnet مربوط به IP خود را انتخاب کنید، با این کار اطلاعات کاملی از رنج IP و دیگر جزئیات را دریافت خواهید کرد.

کلمه Wildcard Mask همان Subnet Mask است اما برشکل آن نوشته می‌شود مثلاً اگر Subten Mask عدد 255.255.0.0 باشد برشکل آن می‌شود 0.0.255.255 از این نوع در ادامه کار و در بحث Ruting استفاده خواهیم کرد.

۵-۴ سوالات فصل چهارم

www.takbook.com

1. Host A is a PC, connected to switch SW1 and assigned to VLAN 1. Which of the following are typically assigned an IP address in the same subnet as host A? (Choose two answers.)

هاست A یک PC است که به VLAN 1 اختصاص داده شده است، در کدام یک از گزینه‌های زیر به طور معمول یک آدرس IP را در همان Subnet هاست A اختصاص می‌دهد؟ (دو گزینه را انتخاب کنید)

a. The local router's WAN interface
b. The local router's LAN interface
c. All other hosts attached to the same switch
d. Other hosts attached to the same switch and also in VLAN 1

2. Why does the formula for the number of hosts per subnet (2H – 2) require the subtraction of two hosts?

چرا فرمول تعداد میزبان در هر Subnet به صورت (2H-2) تفریق نیاز دارد؟

a. To reserve two addresses for redundant default gateways (routers)
b. To reserve the two addresses required for DHCP operation
c. To reserve addresses for the subnet ID and default gateway (router)
d. To reserve addresses for the subnet broadcast address and subnet ID

3. A Class B network needs to be subnetted such that it supports 100 subnets and 100 hosts/subnet. Which of the following answers list a workable combination for the number of network, subnet, and host bits? (Choose two answers.)

یک شبکه کلاس B نیاز به ۱۰۰ زیر شبکه(Subnet) و Hosts دارد، کدام یک از پاسخ‌های زیر ترکیب بهتری برای تعداد بیت‌های شبکه ، زیرشبکه و میزبان است؟ (دو جواب را انتخاب کنید.)

a. Network = 16, subnet = 7, host = 7
b. Network = 16, subnet = 8, host = 8
c. Network = 16, subnet = 9, host = 7
d. Network = 8, subnet = 7, host = 17

4. Which of the following are private IP networks? (Choose two answers.)

کدام یک از گزینه‌های زیر مربوط به IPهای Private است؟(دو گزینه را انتخاب کنید)

a. 172.31.0.0
b. 172.32.0.0
c. 192.168.255.0
d. 192.1.168.0
e. 11.0.0.0

5. Which of the following are public IP networks? (Choose three answers.)

کدام یک از گزینه‌های زیر مربوط به IP Public است؟ (سه گزینه را انتخاب کنید.)

a. 9.0.0.0
b. 172.30.0.0
c. 192.168.255.0
d. 192.1.168.0
e. 1.0.0.0

6. Before Class B network 172.16.0.0 is subnetted by a network engineer, what parts of the structure of the IP addresses in this network already exist, with a specific size? (Choose two answers.)

www.takbook.com

قبل از اینکه یک مهندس شبکه عملیات Subneting را روی آدرس 172.16.0.0 کلاس B انجام دهد کدام بخش از آدرس در حال حاضر مشخص شده است؟ (دو گزینه را انتخاب کنید.)

a. Network
b. Subnet
c. Host
d. Broadcast

7. A network engineer spends time thinking about the entire Class B network 172.16.0.0 and how to subnet that network. He then chooses how to subnet this Class B network and creates an addressing and subnetting plan, on paper, showing his choices.
If you compare his thoughts about this network before subnetting the network to his thoughts about this network after mentally subnetting the network, which of the following occurred to the parts of the structure of addresses in this network?

یک مهندس شبکه زمانی را بر روی Subnting کلاس B برای آدرس 172.16.0.0 صرف می‌کند، و یک برنامه آدرس‌دهی را روی کاغذ پیاده‌سازی می‌کند، قبل از Subneting به نظر رد این آدرس دارد؟

a. The subnet part got smaller.
b. The host part got smaller.
c. The network part got smaller.
d. The host part was removed.
e. The network part was removed.

8. An engineer must configure a /30 subnet between two routes. Which usable IP address and subnet mask combination meets this criteria?

یک مهندس باید subnet /30 را بین دو روتر پیکربندی کند. کدام آدرس IP و MASK این معیارها را برآورده می‌کند؟

a. interface e0/0 description to XX-AXXX:XXXXX ip address 10.2.1.3 255.255.255.252
b. interface e0/0 description to XX-AXXX:XXXXX ip address 192.168.1.1 255.255.255.248
c. interface e0/0 description to XX-AXXX:XXXXX ip address 172.16.1.4 255.255.255.248
d. interface e0/0 description to XX-AXXX:XXXXX ip address 209.165.201.2 225.255.255.252

9. Which network allows devices to communicate without the need to access the Internet?

کدام شبکه اجازه می‌دهد بدون نیاز به دسترسی به اینترنت با دستگاه‌ها ارتباط برقرار کند؟

a. 172.9.0.0/16
b. 172.28.0.0/16
c. 192.0.0.0/8
d. 209.165.201.0/24

10. Figure 15-4, Which statement explains the configuration error message that is received?

با توجه به شکل ۱۵-۴ کدام گزینه در مورد خطای مورد نظر توضیح می‌دهد؟

```
Router(config)#interface GigabitEthernet 1/0/1
Router(config-if)#ip address 192.168.16.143 255.255.255.240
Bad mask /28 for address 192.168.16.143
```

شکل ۱۵-۴ مربوط به شوال شماره‌ی ۱۰

www.takbook.com

a. It belongs to a private IP address range.
b. The router does not support /28 mask.
c. It is a network IP address.
d. It is a broadcast IP address.

www.takbook.com

www.takbook.com

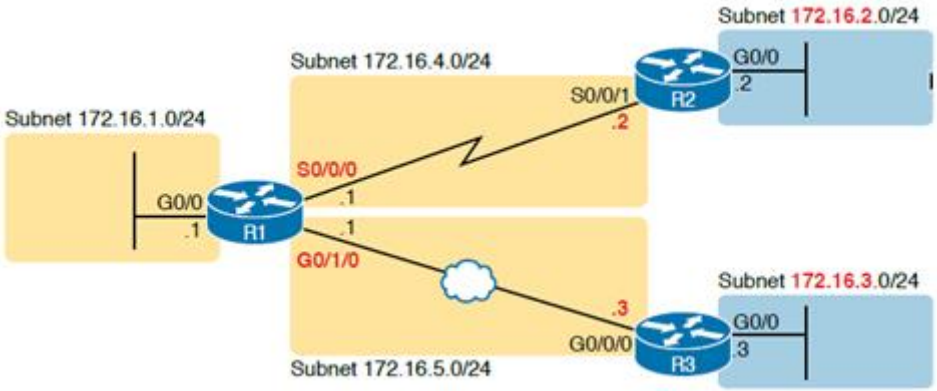
فصل پنجم

مسیریابی (IP Routin)

Routing یا مسیریابی، روشی است برای انتخاب مسیرهای شبکه‌های غیرمحلی و انتقال اطلاعات به شبکه‌ای دیگر که این کار توسط پروتکل‌های مسیریابی انجام می‌شود.

در مسیریابی، بهترین و کوتاه‌ترین مسیر برای ارسال اطلاعات مشخص می‌شود که این کار توسط جدول Routing مشخص و مسیر انتخاب می‌شود، درباره‌ی این موضوعات به‌طور مفصل در ادامه‌ی کتاب بحث خواهیم کرد.

به شکل ۱-۵، توجه کنید، در این سناریو چند روتر را مشاهده می‌کنید که با هم در ارتباط هستند و از رنج IPهای مختلفی برای ارتباط استفاده می‌کنند، مثلاً R1 دارای سه Interface است که هر کدام دارای یک رنج IP جداگانه هستند و این بدان معنا است که روتر نمی‌تواند بر روی Interfaceهای خود آدرس‌هایی در یک رنج داشته باشد.

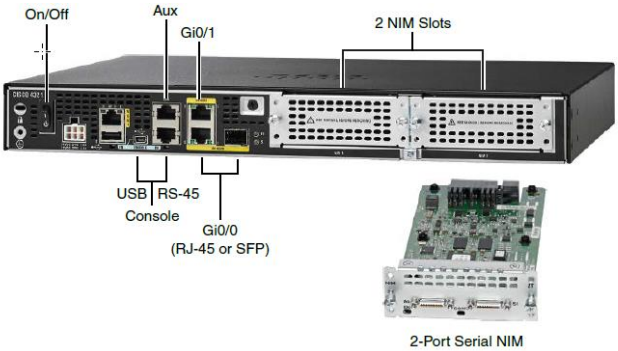


شکل ۱-۵ مسیریابی

امروزه روترها کارهای بیشتری نسبت به مسیریابی انجام می‌دهند، در واقع آنها به عنوان یک پل ارتباطی بین شبکه داخلی سازمان و دنیای اینترنت هستند و می‌توانند هر گونه تغییراتی را در شبکه اعمال کنند، مثلاً از روتر می‌توان به عنوان فایروال استفاده کرد یا اینکه به عنوان Voip آن را تنظیم کرد، انشاالله در این فصل به صورت کامل به آن خواهیم پرداخت.

www.takbook.com

در شکل ۲-۵، روتر سیسکو مدل Cisco 4321 ISR را مشاهده می‌کنید این شکل پشت روتر را به شما نشان می‌دهد، این روتر دارای دو پورت Gigabit Ethernet ست و در قسمت سمت راست آن دو شکاف modular وجود ارد که کارت‌های کوچکی با نام ماژول‌های رابط شبکه در آن قرار می‌گیرند که در همین شکل یک کارت NIM که دارای دو پورت سریال است را مشاهده می‌کنید، پورت‌های دیگر روتر را هم مانند USB, Aux و... مشاهده می‌کنید.



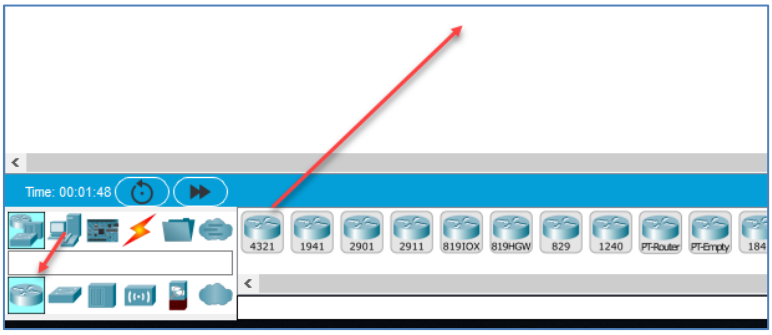
شکل ۲-۵ روتر Cisco 4321 ISR

۱-۵ روش‌های متصل شدن به روتر

متصل شدن به روتر مانند سوئیچ است که دارای پورت Console, Aux, USB و غیره است که باید تنظیمات اولیه را روی آنها انجام داد که این کار را قبلاً انجام دادیم.

راه‌های دیگری مانند Telnet و SSH وجود دارد که می‌توانید از طریق آنها و از راه دور به روتر متصل شوید، یعنی دیگر نیاز نیست برای پیکربندی روتر حتماً در اتاقی که روتر وجود دارد حضور داشته باشید.

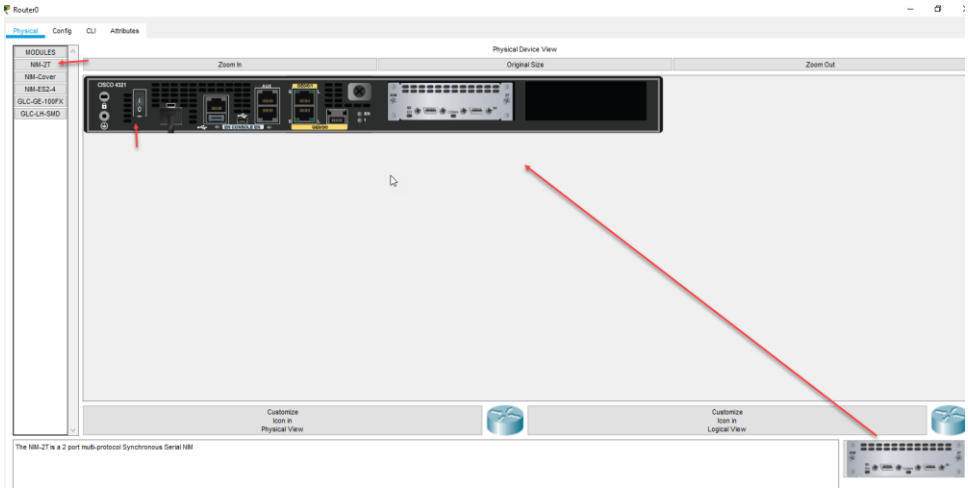
برای استفاده از روتر 4321 به مانند شکل ۳-۵، وارد نرم‌افزار Packet Tracer شوید و از قسمت روتر مدل 4321 را به صفحه اضافه کنید و بر روی آن کلیک کنید.



شکل ۳-۵ روتر ۴۳۲۱ در Packet Tracer

www.takbook.com

طبق شکل ۴-۵، شکل کلی روتر ۴۳۲۱ را مشاهده می‌کنید که برای اینکه بتوانید یک ماژول به آن اضافه کنید اول باید روتر را با کلید مشخص شده در شکل خاموش کنید و بعد از آن NIM-2T را انتخاب کنید تا دو پورت سریال را به روتر اضافه کنید، ماژول سریال مورد نظر را کشیده و در قسمت مشخص شده رها کنید و بعد از آن روتر را روشن کنید.



شکل ۴-۵ اضافه کردن ماژول

وارد تب CLI شوید و دستور زیر را وارد کنید:

```
Router#show ip interface brief
Interface              IP-Address   OK?   Method        Status              Protocol
GigabitEthernet0/0/0   unassigned   YES   unset   administratively down   down
GigabitEthernet0/0/1   unassigned   YES   unset   administratively down   down
Serial0/1/0            unassigned   YES   unset   administratively down   down
Serial0/1/1            unassigned   YES   unset   administratively down   down
Vlan1                  unassigned   YES   unset   administratively down   down
```

در اطلاعاتی که مشاهده می‌کنید، دو پورت GigabitEthernet و دو پورت Serial را مشاهده می‌کنید که تازه به روتر اضافه کردیم، روی هر کدام از این پورت‌ها می‌توانید آدرس IP مورد نظر خود را اضافه و از آن استفاده کنید.

یکی از نکاتی که باید در هنگام کار با روتر بدانید این است که تمام پورت‌های روتر در حالت administratively down قرار دارد و این بدان معنا است که تا زمانی که خودتان با دستور No Shutdown پورت را روشن نکنید آن پورت‌ها خاموش خواهند بود.

برای اینکه اطلاعاتی بیشتری از پورت مورد نظر خود بدست آورید می‌توانید از دستور زیر استفاده کنید:

```
Router#show interfaces gigabitEthernet 0/0/0
GigabitEthernet0/0/0 is administratively down, line protocol is down (disabled)
```

www.takbook.com


```
Hardware is Lance, address is 0003.e4e5.d301 (bia 0003.e4e5.d301)
MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
   reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ARPA, loopback not set
Full-duplex, 100Mb/s, media type is RJ45
ARP type: ARPA, ARP Timeout 04:00:00,
Last input 00:00:08, output 00:00:05, output hang never
Last clearing of "show interface" counters never
Input queue: 0/75/0 (size/max/drops); Total output drops: 0
Queueing strategy: fifo
Output queue :0/40 (size/max)
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
   0 packets input, 0 bytes, 0 no buffer
   Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
   0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
   0 input packets with dribble condition detected
   0 packets output, 0 bytes, 0 underruns
   0 output errors, 0 collisions, 1 interface resets
   0 babbles, 0 late collision, 0 deferred
   0 lost carrier, 0 no carrier
   0 output buffer failures, 0 output buffers swapped out
```

پورت‌های روتر دارای وضعیت‌های مختلف در زمان روشن، خاموش وفعال شدن هستند که در جدول ۱-۱، آنها را بررسی می‌کنیم:

جدول ۱-۵ *وضعیت پورت روتر*

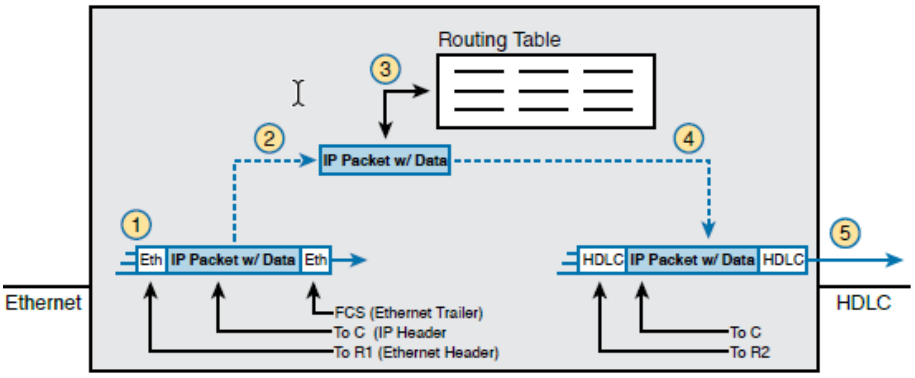
Line Status	Protocol Status	توضیحات
Administratively down	Down	در این وضعیت پورت خاموش بوده و باید با دستور No Shutdown آن را روشن کرد.
Down	Down	در این وضعیت پورت مورد نظر روشن است ولی مشکلی وجود دارد، مثلاً کابل به روتر متصل نیست و نمی‌تواند پورت را فعال کند، یا اینکه سرعت ارتباط با دستگاه دیگر متفاوت است.
Up	Down	این وضعیت زمانی پیش می‌آید که مشکلی در لایه‌ی پیوند داده یا همان data-link باشد، مثلاً در کابل سریال پیکربندی اشتباهی در پروتکل دو طرف انجام شود.
Up	Up	لایه ۱ و لایه دو با هم در حال کار هستند.

www.takbook.com

۵-۲ بررسی Routing Table در روتر

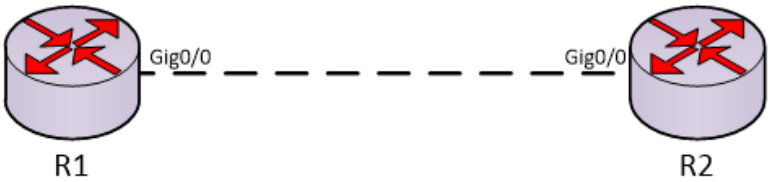
برای انجام Routing در روتر، یک جدول روتینگ وجود دارد که اطلاعاتی در آن ثبت می‌شود که به این جدول Routing Table می‌گویند، این جدول تشکیل شده است از آدرس‌های متصل به روتر و آدرس‌های شبکه‌های غیرمحلی، یعنی از شبکه دیگر.

در شکل ۵-۵، نحوه‌ی قرار گرفتم آدرس‌ها را در جدول Routing مشاهده می‌کنید، زمانی که Frame مورد نظر از طریق کابل ethernet به پورت روتر ارسال می‌شود، بعد از ان اطلاعات از داخل Frame جدا شده و IP مقصد بدست آمده را با IP داخل Routing Table مقایسه می‌کند و بعد در یک Frame جدید جاسازی شده و به پورت دیگر ارسال می‌شود.



شکل ۵-۵ قرار گرفتن آدرس‌ها در جدول روتینگ

با توجه به شکل ۵-۶، این جدول را بررسی می‌کنیم:



شکل ۵-۶ بررسی جدول روتینگ

```
Router#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route
Gateway of last resort is not set
```

www.takbook.com

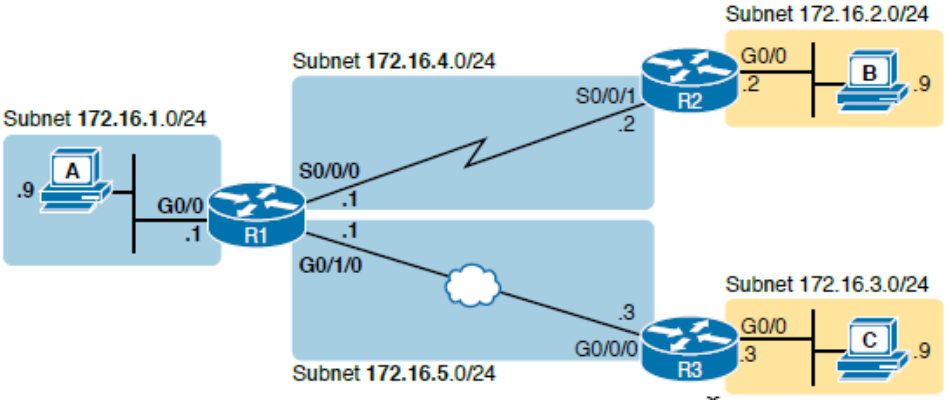
192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C 192.168.1.0/24 is directly connected, GigabitEthernet0/0
L 192.168.1.1/32 is directly connected, GigabitEthernet0/0

در شکل۶-۵، دو روتر به هم متصل شده‌اند. ipهایی که به آن‌ها داده شده در رنج 192.168.1.0 است که همان‌طور مشاهده می‌کنید، این ip به عنوان شبکه‌ی محلی روتر(رنگ قرمز) ثبت شده است. یک کلمه‌ی C اول ip مشاهده می‌کنید که نشان‌دهنده‌ی connected بودن آن است، البته هر حرفی که اینجا نوشته می‌شود در بالا آن کلمه‌ی مربوط به آن نوشته شده است.

این جدول همان جدول **Ip routing** است که در بالا باهم درباره آن صحبت کردیم.

برای اینکه بیشتر با جدول مسیریابی آشنا شویم یک مثال دیگر را با هم بررسی می‌کنیم:

به مانند شکل ۷-۵، سه روتر را به همراه سه PC مشاهده می‌کنید که طبق شکل آدرس‌های آنها مشخص شده است، مثلاً آدرس پورت G0/0 مربوط به روتر R1 برابر است با 172.16.1.1 و به همین صورت بقیه آدرس‌ها مشخص شده است.



شکل ۷-۵ بررسی جدول روتینگ

اگر وارد روتر R1 شوید و دستور زیر را وارد کنید می‌توانید اطلاعاتی را از جدول روتینگ بدست بیاورید.

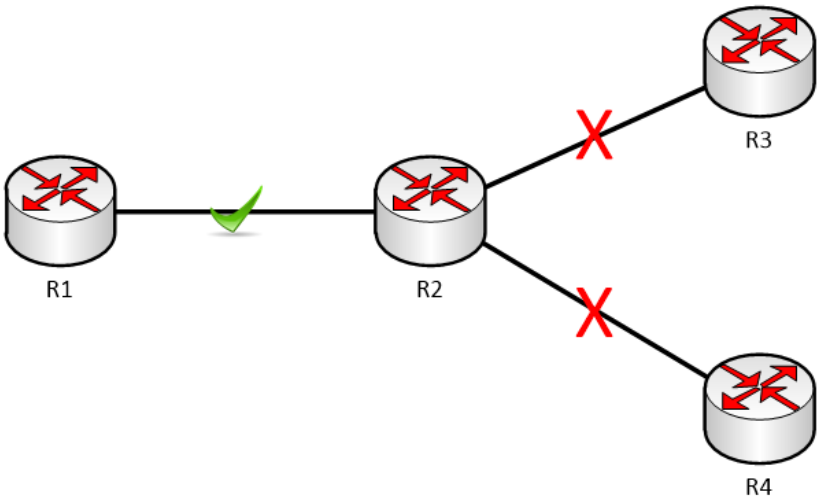
R1# **show ip route**
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
a - application route
+ - replicated route, % - next hop override, p - overrides from PfR
Gateway of last resort is not set
172.16.0.0/16 is variably subnetted, 6 subnets, 2 masks
C 172.16.1.0/24 is directly connected, GigabitEthernet0/0
L 172.16.1.1/32 is directly connected, GigabitEthernet0/0

www.takbook.com

C 172.16.4.0/24 is directly connected, Serial0/0/0
L 172.16.4.1/32 is directly connected, Serial0/0/0
C 172.16.5.0/24 is directly connected, GigabitEthernet0/1/0
L 172.16.5.1/32 is directly connected, GigabitEthernet0/1/0

کلمه C مخفف شبکه‌هایی است که به صورت مستقیم به روتر R1 متصل شده‌اند، و کلمه L مخفف کلمه‌ی Local است که به عنوان شبکه محلی شناخته می‌شود.

لازم است اینجا یک نکته را بررسی کنیم که یک روتر فقط و فقط از شبکه‌های داخل خود که شبکه‌ی محلی است، خبر دارد و از شبکه‌های خارج از آن خبری ندارد. به شکل ۸-۵، توجه کنید.



شکل ۸-۵ بررسی جدول روتینگ

همان‌طور که در شکل ۸-۵ می‌بینید، R1 از اطلاعات شبکه‌ای که به وی متصل است خبر دارد، اما از اطلاعات شبکه‌های دیگر (R3,R4) در روترهای دیگر خبری ندارد. برای حل این مشکل دو راه‌کار وجود دارد؛ برای معرفی شبکه‌های غیر محلی به روترها دو مورد زیر را باید بررسی کنید.

- ✓ Static Route
- ✓ Dynamic Routing

۳-۵ بررسی روش Static Route

در سیستم عامل IOS امکان تعریف مسیرهای Static با استفاده از آدرس‌های IP وجود دارد، معرفی شبکه‌های غیر محلی در Static Route به دو روش انجام می‌گیرد:

- IP Route

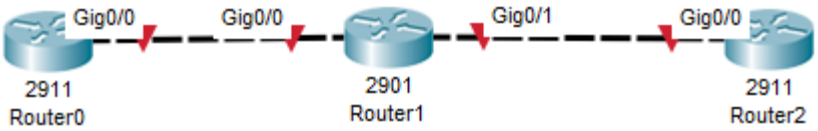
www.takbook.com

- Defualt Route

۱-۳-۵ روش IP Route

در این روش شبکه‌های غیر محلی را به صورت دستی به روتر معرفی می‌کنیم و مشخص می‌کنیم برای رفتن به شبکه مورد نظر از کجا عبور کند.

مثال۱: به مانند شکل ۹-۵، سه روتر وارد صفحه کنید و آن‌ها را با کابل Cross به هم متصل کنید، مانند شکل ۹-۵، ipهای روترها به صورت جدول ۲-۵، وارد کنید .



شکل ۹-۵ بررسی روش IP Route

جدول ۲-۵ آدرس پورت روتر

Router0	Gig0/0	192.168.1.1
Router1	Gig0/0	192.168.1.2
	Gig0/1	192.168.2.1
Router2	Gig0/0	192.168.2.2

وارد Router0 شوید و دستور زیر را وارد کنید:

```
Router(config)#interface gigabitEthernet 0/0
Router(config-if)#ip address 192.168.1.1 255.255.255.0
Router(config-if)#no shutdown
```

وارد Router1 شوید و دستور زیر را وارد کنید:

```
Router(config)# interface gigabitEthernet 0/0
Router(config-if)#ip address 192.168.1.2 255.255.255.0
Router(config-if)#no shutdown

Router(config-if)# interface gigabitEthernet 0/1
Router(config-if)#ip address 192.168.2.1 255.255.255.0
Router(config-if)#no shutdown
```

www.takbook.com

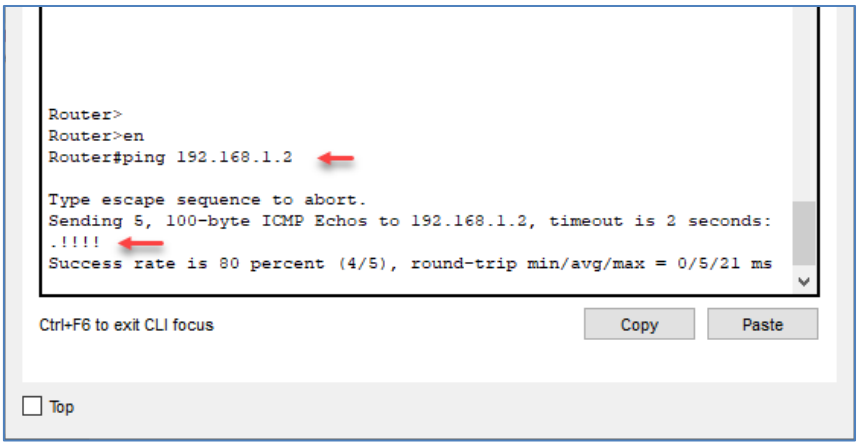
وارد Router2 شوید و دستور زیر را وارد کنید:

Router(config)#**interface gigabitEthernet 0/0**
Router(config-if)#**ip address 192.168.2.2 255.255.255.0**
Router(config-if)#**no shutdown**

برای اینکه متوجه شویم به روترها درست ip داده‌ایم از دستور ping استفاده می‌کنیم. برای این منظور وارد روتر Router0 شوید و در مد Privileged دستور زیر را وارد کنید.

Router# **Ping 192.168.1.2**

با این دستور این تست انجام می‌شود و نتیجه‌ی کار باید به صورت شکل ۱۰-۵، باشد:



شکل ۱۰-۵ Ping گرفتن روتر Router1

علامت ! پشت سر هم به این معنا است که به روتر روبرو متصل شدیم.

شما می‌توانید بعد از اینکه Ip address را در Interface وارد کردید، یک اسم را به ip ارتباط دهید و به جای ip، اسم آن را Ping کنید.

Router(config)# **ip host cisco 192.168.1.2**

همان‌طور که مشاهده می‌کنید نام cisco را به ip ، 192.168.1.2 ارتباط داده‌ایم که برای Ping کردن فقط اسم cisco را Ping می‌کنیم:

Router # **ping cisco**
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.2, timeout is 2 seconds:
.!!!!
Success rate is 0 percent (4/5)

به این موضوع توجه کنید که Router0 فقط به شبکه‌های متصل به خودش دسترسی دارد و این شبکه‌ها را به صورت شبکه‌ی connected در جدول روتینگ خود ثبت می‌کند که در شکل ۱۱ -۵، هم

www.takbook.com

مشخص شده است، اگر به لیست IPها دقت کنید، فقط یک آدرس که مربوط به شبکه داخلی و متصل شده به روتر است مشخص شده است و دیگر آدرس‌ها در لیست وجود ندارند که باید عملیات Routing را روی روتر فعال کنیم.

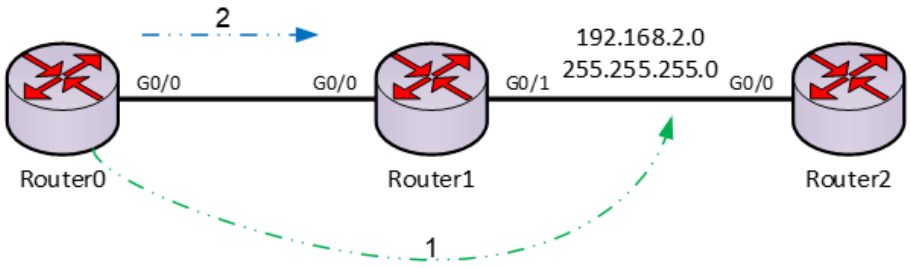
```
Router#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B -
BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS
inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.1.0/24 is directly connected, GigabitEthernet0/0
L       192.168.1.1/32 is directly connected, GigabitEthernet0/0
```

شکل ۱۱-۵ نتیجه دستور Show ip Route

حالا موقع این است که شبکه‌های غیر محلی را به روتر معرفی کنیم، برای معرفی شبکه غیر محلی به روتر باید از دستور Ip Route استفاده کنیم، در Router0 وارد مد Global شده و دستور زیر را وارد می‌کنیم:

Router(config)# **ip route 192.168.2.0 255.255.255.0 192.168.1.2**

این دستور را به این صورت بخوانید (همراه با شکل بخوانید)، بگویید: برو به شبکه 192.168.2.0 با SubnetMask، 255.255.255.0 از 192.168.1.2 عبور کن. در شکل ۱۲-۵، می‌توانید این موضوع را مشاهده کنید.



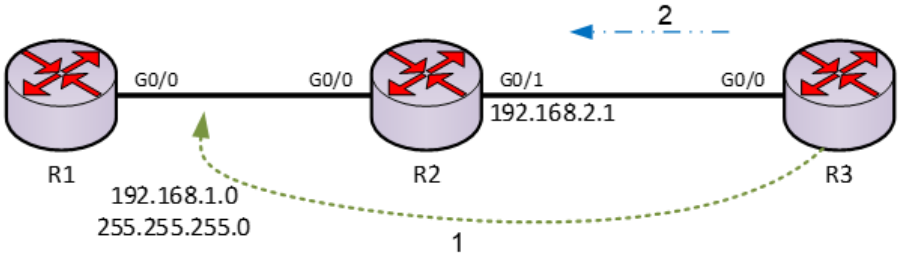
شکل ۱۲-۵ مثال IP Route

www.takbook.com

توجه داشته باشید که این عمل باید از هر دو طرف انجام بگیرد، یعنی اینکه در این مثال در Router2 هم، باید این کار را انجام دهید، اما برشکل قبل، که به صورت زیر باید دستور را در روتر Router2 وارد کنید.

Router(config)# **ip route 192.168.1.0 255.255.255.0 192.168.2.1**

این دستور را به این صورت بخوانید؛ بگویید (شماره‌ی ۱) برو به شبکه‌ی 192.168.1.0 با SubnetMask، 255.255.255.0 از 192.168.2.1 (شماره‌ی ۲) عبور کن. در شکل ۱۳-۵ می‌توانید این موضوع را مشاهده کنید.



شکل ۱۳-۵ مثال IP Route

خوب، حالا اگر شما از Router0 بخواهید، Router2 را Ping کنید، این کار به خاطر فعال کردن IP Route انجام می‌شود.

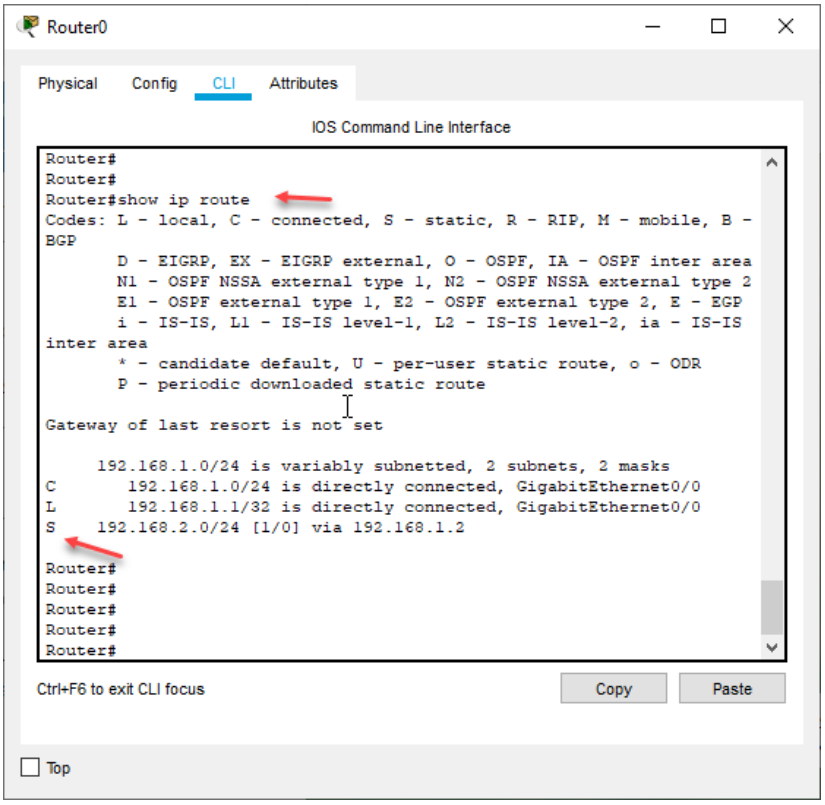
Router# **ping 192.168.2.2**

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/2/13 ms
```

به راحتی توانستیم این کار را انجام دهیم، حالا وقت آن است که سری به جدول روتینگ بزنیم. برای نمایش جدول روتینگ از دستور Show IP Route در مد Privileged استفاده می‌کنیم، مانند زیر:

همان‌طور که در شکل ۱۴-۵، مشاهده می‌کنید، لیست شبکه‌های متصل به روتر را با حروف C مشخص کرده است. اگر توجه کنید، شبکه‌ای با حروف S وجود دارد که S در اینجا به معنای static است و این همان شبکه‌ای است که به صورت دستی تعریف کرده‌ایم.

www.takbook.com



شکل ۱۴-۵ مثال IP Route

نکته: اگر از روترهای قدیمی برای بحث روتینگ استفاده می‌کنید، اگر زمانی interface مورد نظر به هر دلیلیDown (خاموش) شود، ip Route که برای این مسیر ایجاد کرده‌ایم، حذف می‌شود. برای اینکه بعد از Down شدن اینترفیس، IP Route از بین نرود، آخر این دستور از دستور permanent استفاده می‌کنیم، یعنی:

Router(config)#**ip route 192.168.1.0 255.255.255.0 192.168.2.1 Permanent**

۵-۳-۲ Inter Vlan Routing

آیا این موضوع به ذهن شما رسیده که وقتی دو کامپیوتر در دو Vlan متفاوت قرار دارند، راهی وجود دارد که این دو بتوانند باهم در ارتباط باشند؟

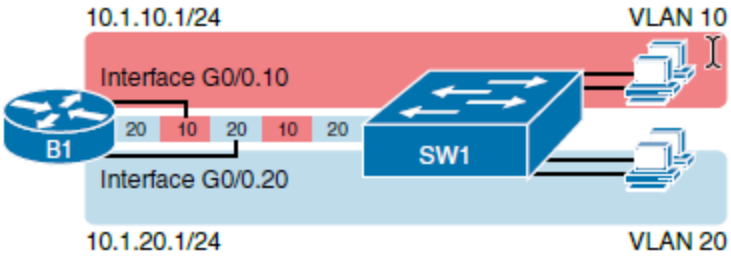
بله این راه از طریق Inter vlan Routing امکان‌پذیر است، یعنی از طریق یک روتر ارتباط Vlanهای تعریف شده در سوئیچ را باهم برقرار می‌کنیم.

www.takbook.com

همان‌طور که می‌دانید سوئیچ‌های لایه‌ی ۲، مانند ۲۹۶۰ قادر به انجام عملیات روتینگ نمی‌باشند و برای همین از روتر برای انجام عملیات روتینگ بین Vlanها استفاده می‌شود.

ارتباط Vlanهای مختلف هم می‌تواند از طریق روتر انجام گیرد و هم از طریق سوئیچ‌هایی که در لایه‌ی ۳ کار می‌کنند.

به شکل ۱۵-۵، توجه کنید، برای انجام عملیات روتینگ روی روتر فقط از یک interface فیزیکی استفاده می‌شود و برای ارتباط با vlanها از پورت‌های مجازی استفاده می‌کنند که قابلیت Encapsulation را دارند. روتر برای انجام عملیات روتینگ باید یک اینترفیس داخل Vlan داشته باشد، یعنی اگر 2 تا vlan داریم، باید 2 تا پورت روتر را به سوئیچ اتصال دهیم که باعث به هدر رفتن پورت‌های روتر و افزایش هزینه می‌شود و به خاطر همین از یک اینترفیس فیزیکی به همراه اینترفیس مجازی داخل آن استفاده می‌کنیم، در شکل ۵-۱۵، یک روتر، یک سوئیچ و PC را مشاهده می‌کنید، در سوئیچ دو VLAN به شماره‌های 10 و 20 تعریف شده است و PCها در این VLANها قرار گرفته است، برای اینکه روتر بتوانید ارتباط بین VLANها را برقرار کند باید از پورت مجازی برای این کار استفاده کند که همانطور که مشاهده می‌کنید دو پورت مجازی بر روی پورت اصلی G0/0 ایجاد شده است.

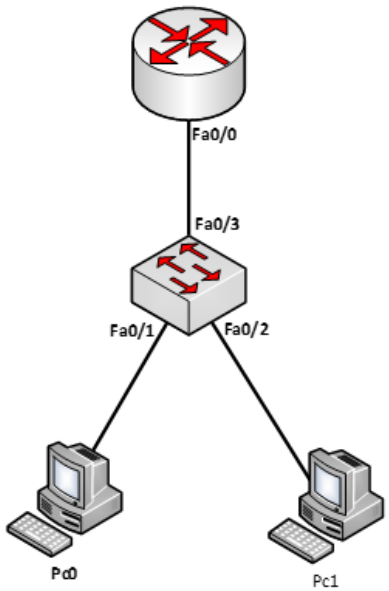


شکل ۱۵-۵ عملیات روتینگ

مثالی از Inter Vlan Routing

مانند شکل ۱۶-۵ ، یک روتر، یک سوئیچ و دو PC را به صفحه اضافه کنید و به صورت زیر به هم متصل کنید:

www.takbook.com



شکل ۱۶-۵ عملیات روتینگ

وارد سوئیچ شوید و پورت متصل به روتر را در Trunk قرار دهید، چون مسئول انتقال Vlanها است:

```
Switch(config)#interface fastEthernet 0/3
Switch(config-if)#switchport mode trunk
```

همان‌طور که می‌دانید dot1q روی سوئیچ‌های سری ۲۵۰۰ به صورت پیش‌فرض فعال است و لازم به واردکردن دستور switchport trunk encapsulation dot1q نیست.

بعد از این کار، دو vlan با شماره‌های ۱۰ و ۲۰ تعریف کنید.

```
Switch(config)#vlan 10
Switch(config-vlan)#exit
Switch(config)#vlan 20
Switch(config-vlan)#exit
```

پورت‌های متصل به pc را داخل Vlan قرار دهید، pc0 داخل Vlan 10 و pc1 داخل Vlan 20.

```
Switch(config)#int f0/2
Switch(config-if)#sw m ac
Switch(config-if)#sw ac vlan 10
Switch(config-if)#int f0/3
Switch(config-if)#sw m ac
Switch(config-if)#sw ac vlan 20
```

حالا وارد روتر شوید و کارهای زیر را انجام دهید:

www.takbook.com

در این سناریو، ما احتیاج به دو Interface مجازی داریم. پورت سوئیچ به پورت G0/0 متصل است، پس Interface مجازی به صورت زیر تعریف می‌شود:

```
Router(config)#interface gigabitEthernet 0/0.10
Router(config-subif)#encapsulation dot1Q 10
Router(config-subif)#ip add 192.168.1.1 255.255.255.0

Router(config-subif)#interface gigabitEthernet 0/0.20
Router(config-subif)#encapsulation dot1Q 20
Router(config-subif)#ip address 192.168.2.1 255.255.255.0

Router(config)#int gigabitEthernet 0/0
Router(config-if)#no shutdown
```

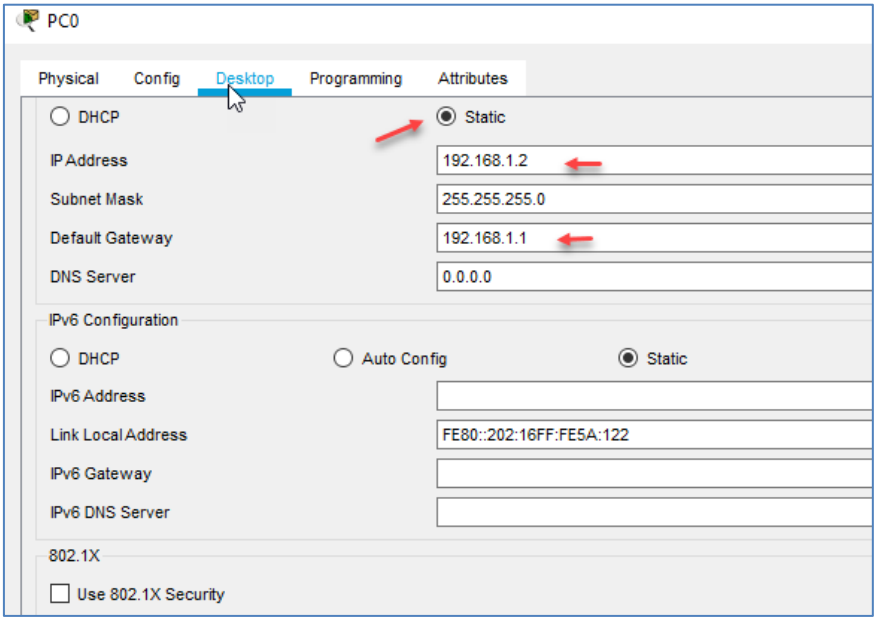
به دقت به دستورات توجه کنید؛ در قدم اول interface gigabitEthernet 0/0.10 را نوشتیم که با این دستور، وارد اینترفیس مجازی با شماره‌ی 10 که روی gigabitEthernet 0/0 قرار دارد، شدیم. بعد از آن، روش برچسب‌زنی را مشخص کردیم، چون در مرحله‌ی Trunk روی سوئیچ، dot1Q را انتخاب کردیم. در این قسمت هم، بعد از encapsulation باید dot1Q قرار داشته باشد. بعد از آن، عدد 10 که نمایانگر Vlan 10 است و ارتباط مستقیم با Vlan 10 دارد و در ادامه، ip address مورد نظر را وارد کردیم و همین کار را در پورت مجازی interface gigabitEthernet 0/0.20 هم انجام دادیم، اما با تغییر شماره‌ی Vlan و شماره‌ی ip، بعد از اتمام کار وارد اینترفیس فیزیکی می‌شویم و آن را فعال می‌کنیم.

تذکر

دستور No Shutdown را در اینترفیس مجازی وارد نکنید، چون پورت اصلی نیست و برای ارتباط باید پورت فیزیکی یا اصلی روشن شود.

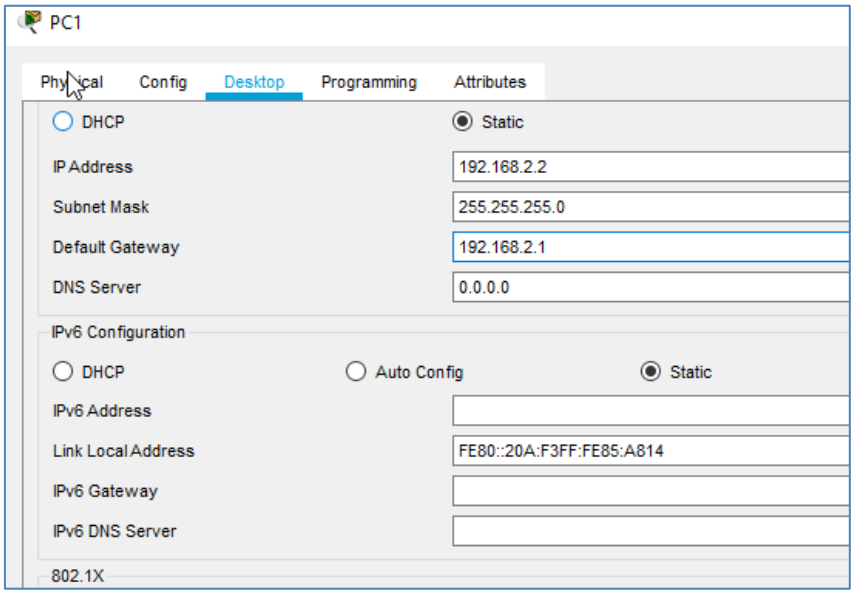
در ادامه وارد pcها شوید و Ip address و Defualt Gateway را برای آن‌ها تعریف کنید، برای PC0 به صورت شکل ۱۷-۵ عمل کنید.

www.takbook.com



شکل ۱۷-۵ تنظیمات PC

برای pc1 به صورت شکل ۱۸-۵، تعریف کنید.



شکل ۱۸-۵ تنظیمات PC

بعد از اتمام کار، دو pc که در Vlanهای مختلف قرار دارند، می‌توانند همدیگر را ببینند. اگر از pc1، pc0 را Pnig کنیم، به صورت زیر جواب می‌دهد:

PC>**ping 192.168.1.2**

www.takbook.com


```
Pinging 192.168.1.2 with 32 bytes of data:

Request timed out.
Reply from 192.168.1.2: bytes=32 time=0ms TTL=127
Reply from 192.168.1.2: bytes=32 time=10ms TTL=127
Reply from 192.168.1.2: bytes=32 time=0ms TTL=127

Ping statistics for 192.168.1.2:
   Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
   Minimum = 0ms, Maximum = 10ms, Average = 3ms
```

۵-۳-۳ روش Defualt Route

شبکه‌ها را در قسمت قبل توانستیم به صورت دستی تعریف کنیم. اگر تعداد شبکه زیاد شود، این کار وقت‌گیر است. متخصصان یک روش دیگر با عنوان Defualt Route معرفی کردند که دیگر لازم نیست تک‌تک شبکه‌های روترها را معرفی کنیم، فقط به روتر می‌گوییم، هر چیزی را که نمی‌داند، بفرست به روتر کناری.

برای انجام این کار در مثال قبلی دستور Ip route را با گذاشتن no در اول آن حذف کنید، مانند زیر:

```
Router(config)#no ip route 192.168.2.0 255.255.255.0 192.168.1.2
Router(config)#no ip route 192.168.1.0 255.255.255.0 192.168.2.1
```

بعد از پاک کردن ip route های قبلی به این صورت دستورات را در **Router0** و **Router2** وارد می‌کنید.

در Router0:

```
Router(config)# Ip Route 0.0.0.0  0.0.0.0  192.168.1.2
```

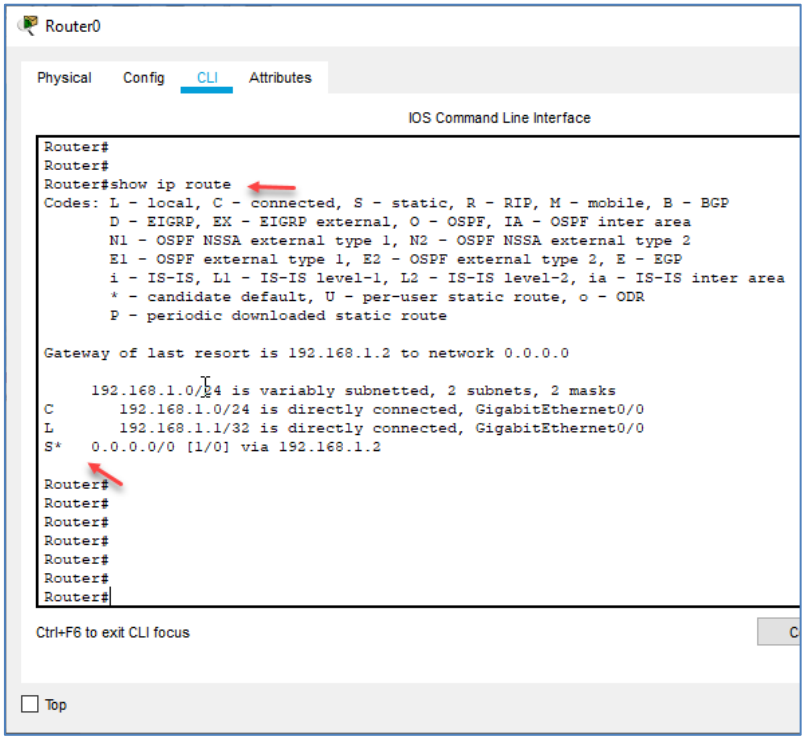
در Router2:

```
Router(config)# Ip Route 0.0.0.0  0.0.0.0  192.168.2.1
```

این دستورات به این صورت است که می‌گوید هر Ip (0.0.0.0) با هر SubnetMask (0.0.0.0) که نمی‌شناسی را بفرست به روتر کناری خودت که به شما متصل است. به این صورت عمل می‌کند که وقتی Router0 بخواهد با روتر Router1 ارتباط برقرار کند، آدرس مقصد را تحویل Router2 می‌دهد و به خاطر اینکه Router1 متصل است به روتر Router2، همین امر باعث می‌شود که کار به نتیجه برسد. در حال حاضر اگر Ping از Router0 به طرف Router2 بزنید، جواب خواهد داد.

در زیر اگر از دستور IP Route در Router0 استفاده کنید یک ستاره بر روی کلمه‌ی S قرار گرفته است که نشان دهنده‌ی Defualt route است.

www.takbook.com



شکل ۱۹-۵ تنظیمات روتر Router0

روش دیگری هم برای اینکه اطلاعات را به مسیر مورد نظر ارسال کنید وجود دارد، مثلاً شکل ۲۰ – ۵ را در نظر بگیرید روتر R1 می‌خواهد شبکه‌های پشت روتر R2 و R3 را مشاهده کند، برای همین می‌توانیم از دستورات زیر استفاده کنیم.

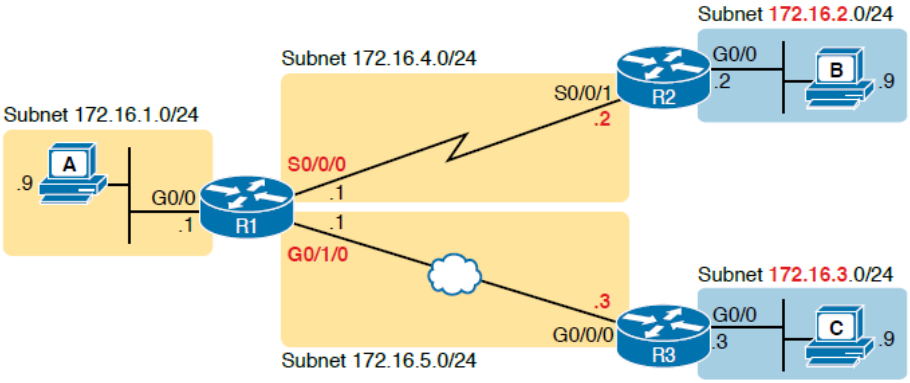
ip route 172.16.2.0 255.255.255.0 S0/0/0

در دستور بالا یک IP Route به شبکه 172.16.2.0 زدیم که خروجی آن را Interface سریال 0/0/0 وارد کردیم، یعنی اینکه حتماً نباید آدرس IP روتر روبرو را وارد کنید.

ip route 172.16.3.0 255.255.255.0 172.16.5.3

اما در دستور بالا برای رسیدن به شبکه‌ی 172.16.3.0 باید از 172.16.5.3 استفاده کند که این دستور را قبلاً بررسی کردیم.

www.takbook.com



شکل ۲۰-۵ مثال Defualt Route

اگر از دستور زیر استفاده کنید مسیر Static که ایجاد کردیم را می‌توانید مشاهده کنید.

R1# **show ip route static**
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
! lines omitted for brevity
Gateway of last resort is not set
172.16.0.0/16 is variably subnetted, 8 subnets, 2 masks
S 172.16.2.0/24 is directly connected, Serial0/0/0
S 172.16.3.0/24 [1/0] via 172.16.5.3

زمانی که از Static Routes در شبکه استفاده می‌کنید شاید با مشکلاتی روبرو شوید که با هم آنها را بررسی می‌کنیم:

۱. مسیرهای استاتیک نادرست که در جدول Routing روتر ثبت شده‌اند، باعث می‌شوند که عملیات به درستی انجام نشود، برای اینکه این موضوع را بررسی کنید باید ببینیم که Subnet Mask یا آدرس شبکه مقصد درست وارد شده است یا خیر، یا می‌توانید بررسی کنیم که آدرس شبکه خروجی درست وارد شده است یا خیر.
۲. مسیر Routing در جدول Routing وجود ندارد، که باید با دستوراتی که گفته شده است، آنها را تعریف کنید، همیشه از دستورات Show برای عیب‌یابی روتر استفاده کنید.
۳. مسیر Routing به درستی در جدول وجود دارد ولی بسته‌ها به مقصد نمی‌رسد و Drop می‌شود که باید مشخص کنید که رابط خروجی یا همان Interface فعال است یا نه.

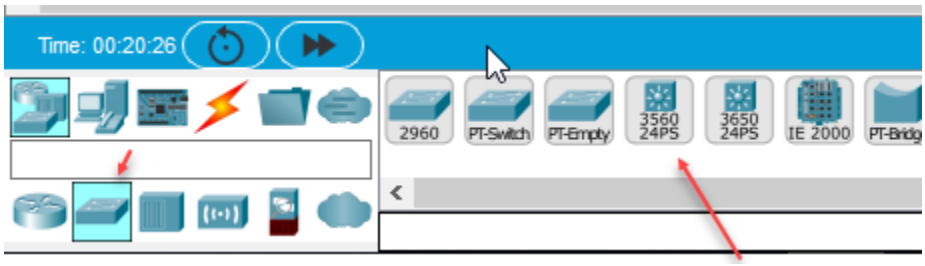
۵-۳-۴ کار با SVI Routing در سوئیچ لایه‌ی سوم

اصولاً سوئیچ‌ها در لایه دو کار می‌کنند و کاری با روتیگ ندارند، اما سوئیچ‌هایی هم وجود دارند که می‌توانند در لایه سوم عمل کنند و کار روتینگ را انجام دهند، پس دیگر نیاز نیست مثل قسمت قبلی از روتر برای InterVlan Routing استفاده کنید بلکه سوئیچ لایه سوم این کار را به خوبی انجام می‌دهد.

برای اینکه بیشتر با سوئیچ لایه سوم آشنا شویم یک مثال کامل را با هم بررسی می‌کنیم.

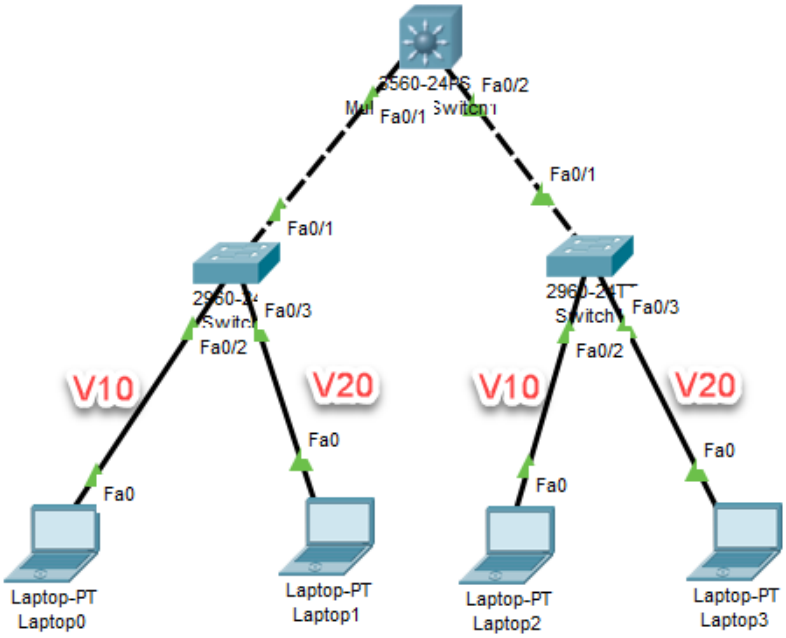
www.takbook.com

به مانند شکل ۲۱-۵، یک سوئیچ لایه سوم (3560) را از قسمت سوئیچ‌ها انتخاب و دو سوئیچ لایه دوم (2960) به همراه 4 لپ تاپ را به صفحه اضافه کنید.



شکل ۲۱-۵ روتر ۳۵۶۰

شکل نهایی سناریو به صورت شکل ۲۲-۵ است، در این سناریو سوئیچ لایه‌ی سوم به عنوان یک روتر عمل می‌کند و عملیات روتیگ بین VLANها را انجام می‌دهد.



شکل ۲۲-۵ مثال Inter VLAN Routing

وارد سوئیچ‌های لایه‌ی دوم (2960) شوید و دستورات زیر را وارد کنید:

```
Switch>enable
Switch#configure terminal
```

www.takbook.com


```
Switch(config)#vlan 10
Switch(config-vlan)#exit

Switch(config)#vlan 20
Switch(config-vlan)#exit
```

در دستورات بالا وارد هر دو سوئیچ لایه‌ی دوم می‌شویم و دو VLAN با شماره‌های 10 و 20 ایجاد می‌کنیم.

در ادامه کار باید وارد Interfaceهای سوئیچ‌ها که به سمت لپ‌تاپ هست شویم و دستورات زیر را وارد کنیم:

```
Switch(config)#interface fastEthernet 0/2
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 10

Switch(config-if)#interface fastEthernet 0/3
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 20
```

در دستورات بالا وارد پورت‌هایی شدیم که به سمت لپ‌تاپ هستند و آنها را در VLAN مورد نظر خود قرار دادیم که در شکل سناریو هم مشخص شده است.

در ادامه کار در همان دو سوئیچ لایه‌ی دوم باید وارد پورتی شوید که به سمت سوئیچ لایه‌ی سوم است و دستورات زیر را وارد کنید:

```
Switch(config-if)#interface fastEthernet 0/1
Switch(config-if)#switchport mode trunk
```

زمانی از پورت Trunk استفاده می‌کنیم که بخواهیم VLANها را در سوئیچ‌ها انتقال بدهیم و عملیات روتیگ بر روی آنها انجام دهیم.

بعد از انجام تنظیمات در سوئیچ‌های لایه‌ی دوم حالا باید تنظیمات مربوط به سوئیچ لایه‌ی سوم را هم انجام دهیم، برای این کار وارد سوئیچ لایه‌ی سوم شوید و دستورات زیر را وارد کنید:

```
Switch(config)#interface fastEthernet 0/1
Switch(config-if)#switchport mode trunk
Command rejected: An interface whose trunk encapsulation is "Auto" can not be configured to "trunk"
mode.

Switch(config)#interface fastEthernet 0/2
Switch(config-if)#switchport mode trunk
Command rejected: An interface whose trunk encapsulation is "Auto" can not be configured to "trunk"
mode.
```

www.takbook.com

در دستور بالا وارد پورت F0/1 شدیم و مد Trunk را فعال کردیم که با پیغامی روبرو شده است، در این پیغام اعلام می‌کند که پورت به صورت پیش‌فرض بر روی Trunk قرار دارد و نیاز به تنظیم دوباره‌ی آن نیست، در پورت F0/2 هم اگر این دستور را وارد کنید با همین پیغام روبرو خواهید شد.

بعد از اجرای دستور بالا باید سرویس Routing را بر روی سوئیچ لایه‌ی سوم فعال و VLAN را در آن تعریف کنید:

```
Switch(config)#ip routing
Switch(config)#vlan 10
Switch(config-vlan)#exit
Switch(config)#vlan 20
Switch(config-vlan)#exit
```

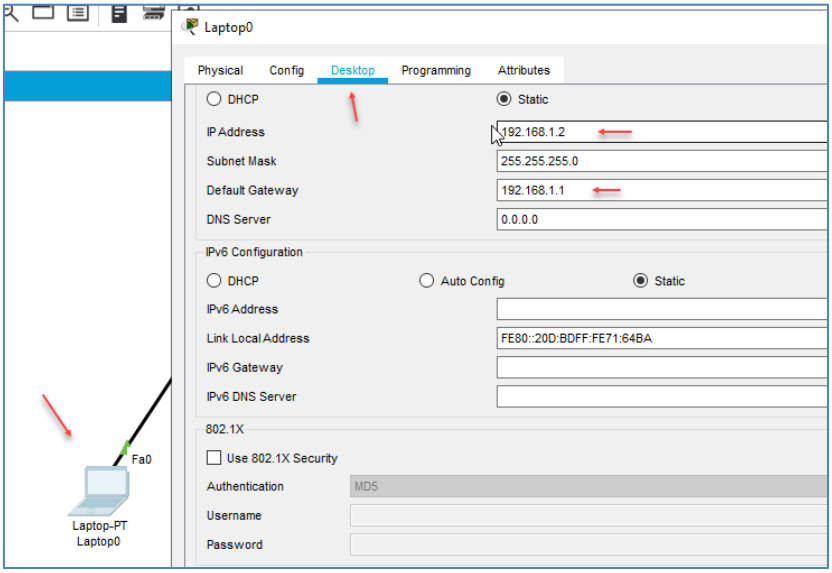
در ادامه کار باید وارد VLANهای مورد نظر شوید و آدرس IP آنها را وارد کنید:

```
Switch(config-if)#interface vlan 10
Switch(config-if)#ip address 192.168.1.1 255.255.255.0
Switch(config-if)#no sh

Switch(config-if)#interface vlan 20
Switch(config-if)#ip address 192.168.2.1 255.255.255.0
Switch(config-if)#no sh
```

بعد از تکمیل هر سه سوئیچ، لایه‌ی دوم و سوم، باید به مانند شکل ۲۳-۵ و ۲۴-۵ وارد لپ‌تاپ‌های مورد نظر شویم و آدرس IP برای آنها در نظر بگیرید تا بتوانند همدیگر را پیدا کنند.

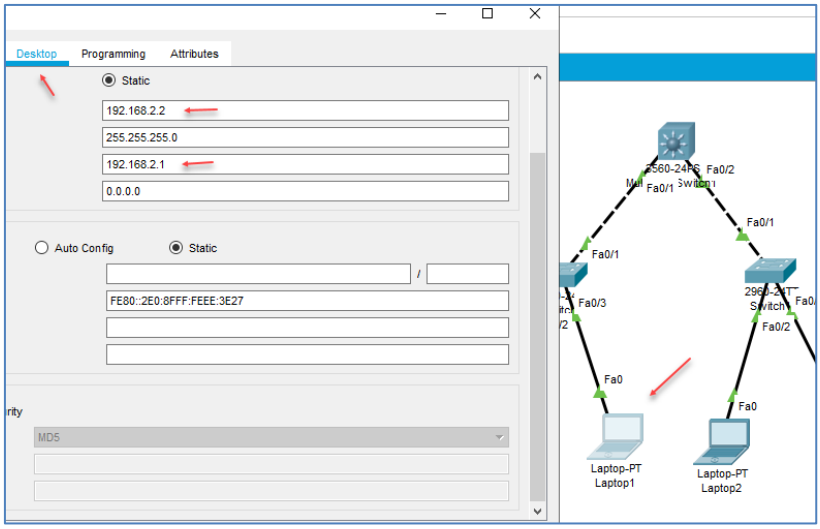
وارد لپ‌تاپ شوید و از تب Desktop آدرس IP مورد نظر را وارد کنید، توجه داشته باشید که هر لپ‌تاپ در کدام VLAN قرار دارد مثلاً لپ‌تاپ (Laptop0) در VLAN شماره‌ی 10 قرار دارد و باید آدرس رنج مشخصی با رنج آدرس سوئیچ لایه‌ی سوم که دستور آن را در قسمت قبل می‌بینید داشته باشد، در قسمت Default Gateway باید آدرس سوئیچ لایه‌ی سوم را که در VLAN شماره‌ی 10 وارد کردیم را وارد کنید.

www.takbook.com



شکل ۲۳-۵ تنظیمات Laptop0

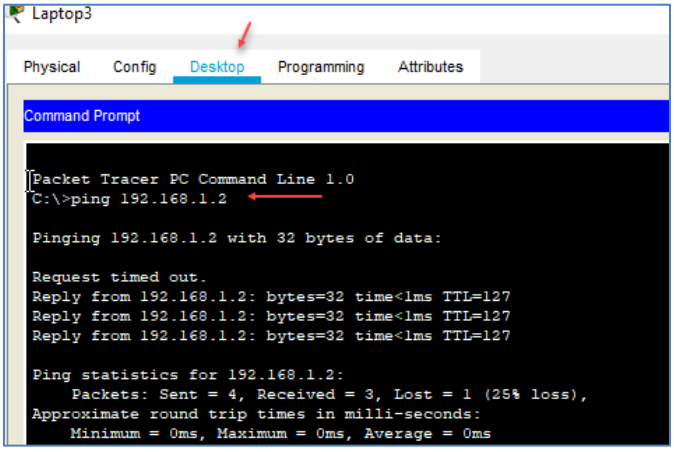
در Laptop1 هم که در VLAN شماره‌ی 20 قرار دارد باید آدرس زیر را وارد و Default Gateway آن را هم 192.168.2.1 در نظر بگیرید که در سوئیچ لایه‌ی سوم در VLAN شماره‌ی 20 وارد کردیم.



شکل ۲۴-۵ تنظیمات Laptop1

اگر بخواهیم سناریوی خود را تست بگیریم می‌توانیم وارد Laptop3 شویم و آدرس Laptop0 را Ping بگیریم که این موضوع به درستی در شکل ۲۵-۵، مشخص شده است.

www.takbook.com

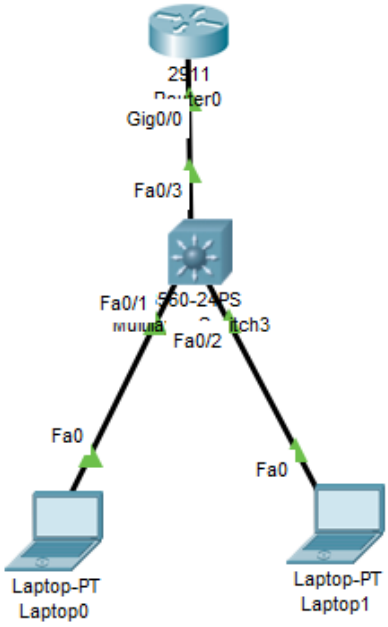


شکل ۲۵-۵ تنظیمات Laptop3

۵-۳-۵ کار با Routed Ports در سوئیچ لایه‌ی سوم

برای اینکه یک سوئیچ را به روتر متصل کنیم باید به صورت زیر عمل کنیم.

در سناریو زیر یک روتر (2911) یک سوئیچ لایه‌ی سوم (3560) و دو لپ تاپ را به مانند شکل ۲۶-۵، به هم متصل کنید.



شکل ۲۶-۵ مثال Routrd Port

www.takbook.com

وارد سوئیچ لایه‌ی سوم شوید و دستوراتی را که در قسمت قبلی وارد کردیم را اینجا هم اجرا کنید، فقط برای اینکه یک پورت سوئیچ را به روتر، برای روتیگ متصل کنیم باید از دستور زیر در سوئیچ استفاده کنیم:

Switch(config)#**interface fastEthernet 0/3**
Switch(config-if)#**no switchport**

بعد از این کار می‌توانید به پورت مورد نظر IP اختصاص دهید تا بتواند با روتر مقابل خودش ارتباط برقرار کند.

Switch(config-if)#**ip address 192.168.3.1 255.255.255.0**
Switch(config-if)#**no sh**

در روتر هم باید دستورات زیر را وارد کنید تا ارتباط برقرار شود.

Router(config)#**interface gigabitEthernet 0/0**
Router(config-if)#**ip address 192.168.3.2 255.255.255.0**

۵-۴ بررسی Dynamic Routing

در این روش دسترسی به شبکه‌های غیر محلی دیگر به صورت دستی انجام نمی‌شود، بلکه به صورت خودکار از طریق Routing Protocolsها انجام می‌شود.
قبل از اینکه بحث را شروع کنیم باید دو موضوع را مشخص کنیم:

Routing Protocol

برای اینکه جدول روتیگ روترها را آپدیت کنیم باید از Routing Protocol استفاده کنیم، مهمترین وظیفه‌ی این نوع پروتکل‌ها انتخاب مسیر درست و سریع، جهت اجرای عملیات روتینگ و ارسال بسته به مقصد مورد نظر است، همانطور که می‌دانید روترها در لایه‌ی سوم مدل OSI کار می‌کنند و برای عملیات روتینگ از پروتکل‌های روتیگ مختلفی استفاده می‌کنند که این روتیگ پروتکل‌ها شامل RIP, EIGRP, OSPF, BGP است، این پروتکل‌ها از طریق الگوریتمی که در خود دارند شبکه‌های خود را به دیگر روترها معرفی می‌کنند و در جدول روتینگ خود این شبکه‌ها را درج می‌کنند.

Routed protocol یا routable protocol

این نوع پروتکل‌ها روش‌های آدرس‌دهی در بسته‌ها مشخص می‌کنند و Routing پروتکل‌ها از طریق آنها می‌توانند بسته مورد نظر را به مقصد برسانند که بهترین مثال در این بخش می‌تواند پروتکل IP باشد.
IOS سیسکو از چندین پروتکل مسیریابی پشتیبانی می‌کند که کار کلی آنها به صورت زیر است:

۱- از روترهای همسایه Subnetهای موجود را یاد می‌گیرد.

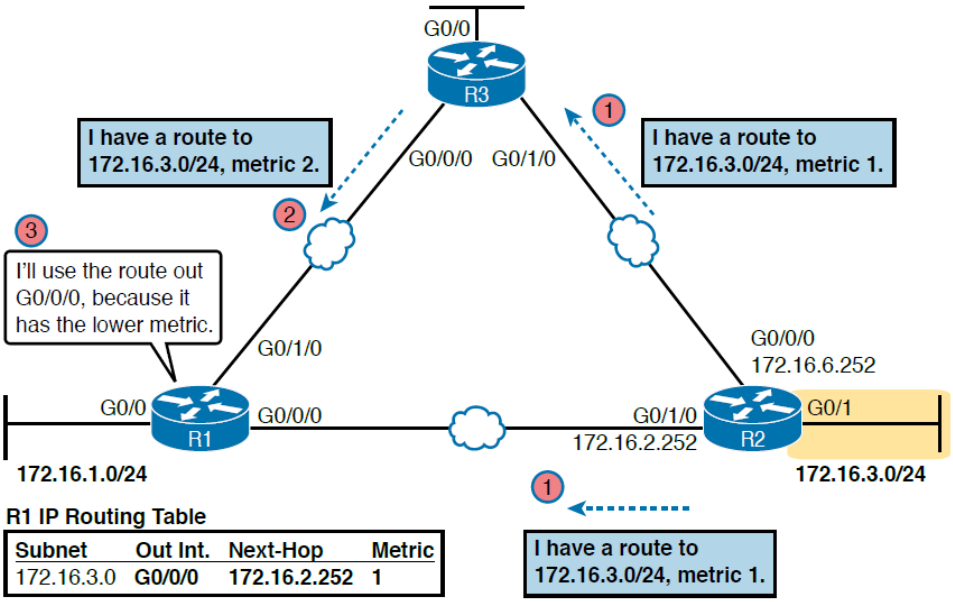
www.takbook.com

۲- به روترهای همسایه Subnetهای موجود در جدول مسیریابی را تبلیغ می‌کند.

۳- اگر برای رسیدن به یک شبکه خاص چند مسیر وجود داشته باشد، بهترین مسیر انتخاب می‌شود که البته با دلایلی که در ادامه روی آن بحث خواهیم کرد.

۴- اگر چنانچه تغییراتی در توپولوژی شبکه ایجاد شود خیلی سریع به دیگر روترها اطلاع می‌دهید.

در شکل ۲۷-۵، یک سناریو متشکل از سه روتر را مشاهده می‌کنید که سه مورد از ۴ مورد بالا را مشخص کرده است، در آن روتر R1 دو مسیر را که مربوط به روتر R2 است را از طریق روتر R2 و R3 یاد می‌گیرد و باید تشخیص دهد که کدام مسیر بهتر است که انتخاب این مسیر را از طریق Metric که در ادامه بررسی می‌کنیم انجام می‌دهد و هر چه این عدد کمتر باشد همان مسیر را انتخاب می‌کند.

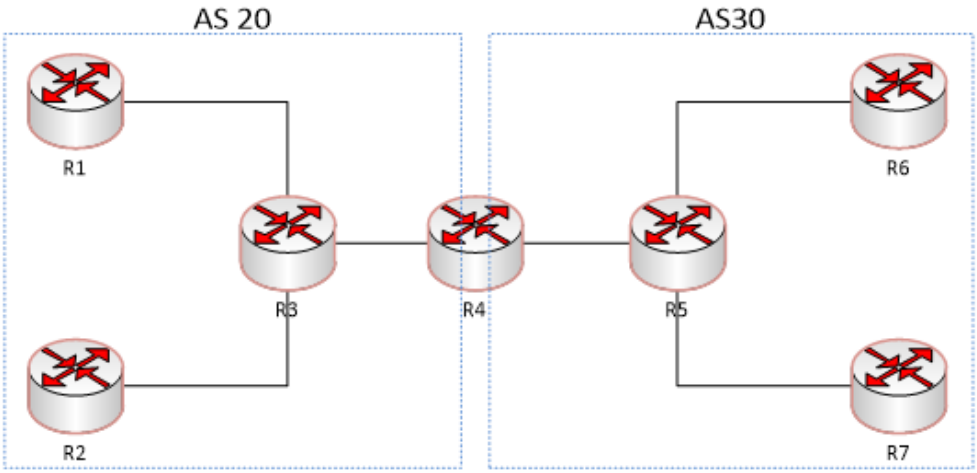


شکل ۲۷-۵ مثال Routrd Port

۱-۴-۵ تعریف Autonomuos System

به مجموعه‌ای از روترها که در یک منطقه قرار دارند گفته می‌شود، که روترها فقط در همان منطقه با هم در ارتباط هستند. اگر به شکل ۲۸-۵، نگاه کنید، متوجه‌ی این موضوع خواهید شد.

www.takbook.com



شکل ۲۸-۵ بررسی Autonomuos System

عدد AS یا همان Autonomous System که با نام ASN هم شناخته می‌شود می‌تواند عددی بین ۰ تا ۶۵۵۳۵ باشد. در ادامه با اجرای یک پروتکل مانند IGP با AS آشنا می‌شوید.

پروتکل‌های مسیریابی بر دو نوع هستند:

- ✓ IGPs(Interior Gateway Protocol)
- ✓ EGPs(Exterior Gateway Protocol)

پروتکل‌های IGPs:

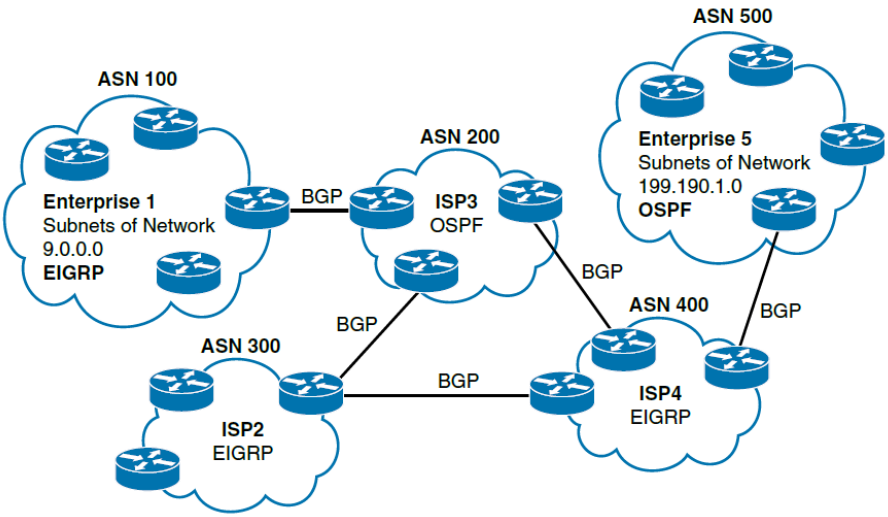
به روتینگ پروتکل‌هایی که داخل یک AS کار می‌کنند و باهم در ارتباط هستند، مانند پروتکل‌های IGRP، RIP، EIGRP و OSPF، پروتکل‌های IGPs گفته می‌شود.

پروتکل‌های EGPs:

روتینگ پروتکل‌هایی که می‌توانند ASهای مختلف را به هم ارتباط دهند، مانند پروتکل BGP پروتکل‌های EGPs گفته می‌شود که به آن‌ها روترهای مرزی هم گفته می‌شود.

در شکل ۲۹-۵، پروتکل‌های IGPs و BGPs را مشاهده می‌کنید که هر کدام در یک ASN خاص با شماره‌ی مشخص قرار دارند.

www.takbook.com



شکل ۲۹-۵ بررسی Autonomuos System

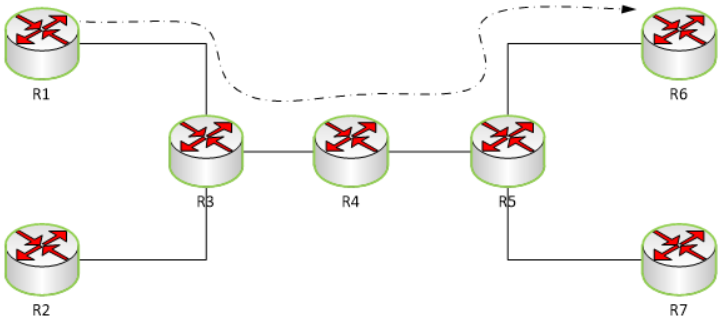
Dynamic Routing به سه دسته‌ی کلی تقسیم می‌شوند که هر ۳ را مورد بررسی قرار می‌دهیم:

- ✓ **Distance Vector**
- ✓ **Link State**
- ✓ **Hybrid**

۲-۴-۵ پروتکل‌های Distance Vector یا بردار فاصله

به پروتکل‌هایی گفته می‌شود که فقط و فقط با روتر کناری خود در ارتباط هستند و تمام اطلاعات خود را به روتر کناری خود منتقل و دریافت می‌کنند.

برای رسیدن به یک شبکه‌ی خاص از یک بردار خطی استفاده می‌کند، مانند شکل ۳۰-۵:



شکل ۳۰-۵ بررسی Distance Vector

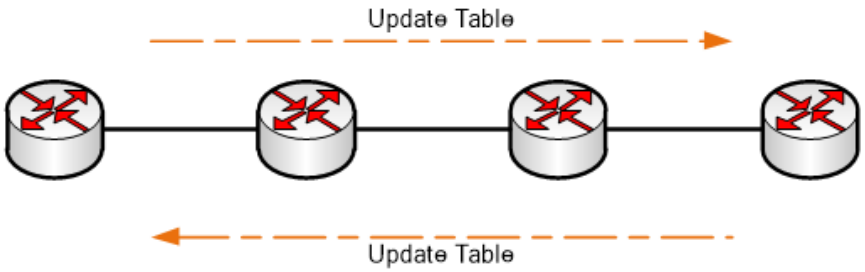
www.takbook.com

در این پروتکل‌ها اگر روتری، روتر کناری خود را بشناسد، می‌تواند بهترین مسیر را از روتر کناری خود دریافت کند. روتینگ پروتکل‌های RIP و IGRP از این نوع هستند.

الگوریتمی که این نوع پروتکل‌ها با آن کار می‌کنند، Bellman_Ford است که ویژگی‌های آن به صورت زیر است:

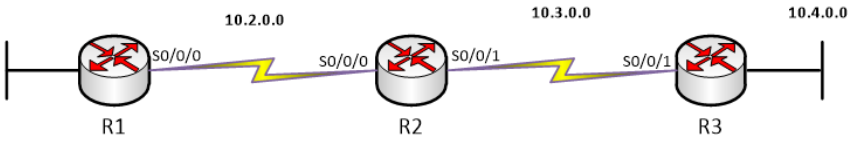
- ساخت جدول Routing برای آدرس‌های شبکه.
- شناسایی شبکه‌های متصل به آن و ثبت در جدول.
- انتقال اطلاعات این جداول به صورت کلی در زمان مشخص که به آن Priodic Update می‌گویند.

به مانند شکل ۳۱-۵، این نوع پروتکل‌ها در جدول روتینگ خود ابتدا، شبکه‌های connect به خود را در جدول درج می‌کنند و بعد از ارتباط با روترهای دیگر؛ بهترین مسیر را انتخاب و در جدول خود درج می‌کنند. روترها جداول خود را به صورت Broadcast به روترهای مجاور خود می‌فرستند که در پروتکل Rip به ip، 255.255.255 و در پروتکل IGRP به ip، 224.0.0.9 فرستاده می‌شود و بعد روتر در پاسخ به روتری که Update فرستاده، اطلاعات جدول خود را به صورت Unicast به این روتر می‌دهد و به همین صورت همه‌ی روترها از کل شبکه‌ی موجود باخبر می‌شوند.



شکل ۳۱-۵ نحوه‌ی ارسال آپدیت

Metric: در جدول روتینگ معیاری وجود دارد به نام متریک که تعداد روترهای سر راه برای رسیدن به شبکه موردنظر را مشخص می‌کند. در یک پروتکل مشخص برای رسیدن به یک شبکه اگر تعداد روترهای سر راه ۳ تا باشد، متریک می‌شود ۳ و به این هم توجه داشته باشید که هر چه متریک کمتر، مسیر بهتر و سریع‌تر است و همان مسیر انتخاب می‌شود.



شکل ۳۲-۵ مثال Metric

جدول ۳-۵ جدول روتینگ

www.takbook.com

Network	Interface	Hop
10.1.0.0	Fa0/0	0
10.2.0.0	S0/0/0	0
10.3.0.0	S0/0/0	1

Network	Interface	Hop
10.2.0.0	S0/0/0	0
10.3.0.0	S0/0/1	0
10.1.0.0	S0/0/0	1
10.4.0.0	S0/0/1	1

Network	Interface	Hop
10.3.0.0	S0/0/1	0
10.4.0.0	Fa0/0	0
10.2.0.0	S0/0/1	1

به شکل ۳۲-۵، توجه کنید، در جدول ۳-۵، برای روتر R1 دو تا از مسیرها، متریک آن صفر در نظر گرفته شده، آن‌هم به خاطر این است که متریک شبکه‌های متصل به روتر، صفر است. توجه داشته باشید به متریک، Hop Count هم می‌گویند. اگر با دقت بیشتر به جدول نگاه کنید، R1 شبکه 10.3.0.0 را با متریک ۱ در جدول خود قرار داده است، آن‌هم به این خاطر است که فقط یک روتر برای رسیدن به این شبکه در سر راه قرار دارد. اگر R1 بخواهد به شبکه‌ی 10.4.0.0 برسد، متریک سر راه را ۲ در نظر می‌گیرد، چون ۲ تا روتر در سر راه تا رسیدن به آن شبکه قرار دارد.

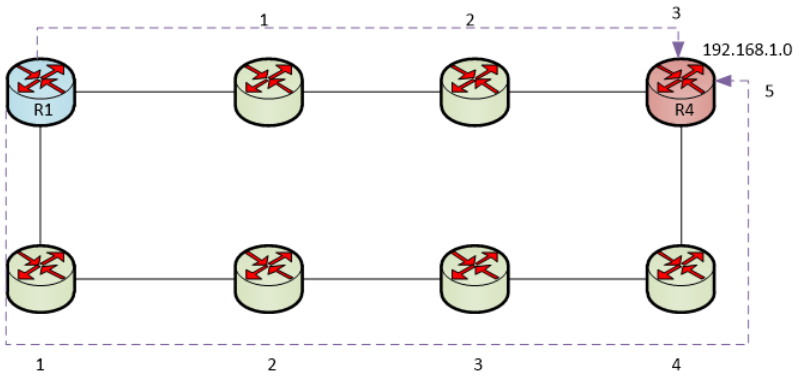
Convergence Time

به مدت‌زمانی گفته می‌شود که یک روتر به حالت پایدار می‌رسد و تمام شبکه‌های خود و اطراف خود را می‌شناسد و در جدول خود ثبت می‌کند.

بعد از این‌که روتر یک، به حالت پایدار رسیده و جدول روتینگ خود را کامل کرده، در طی زمان‌های مشخص تمام جدول روتینگ خود را به صورت Full Update به روترهای دیگر ارسال می‌کند. اگر تغییری در جدول این روتر صورت بگیرد، یا نگیرد این Update ارسال می‌شود. به این روش ارسال اطلاعات که در طی زمانی مشخص صورت می‌گیرد، Priodic Update می‌گویند که این موضوع یکی از مهم‌ترین ویژگی-های پروتکل‌های Distance Vectore است.

۳-۴-۵ روش‌های انتخاب بهترین مسیر

در شبکه‌هایی که با پروتکل Rip راه‌اندازی می‌شوند، انتخاب بهترین مسیر از روی Hop Count یا تعداد روترهای سر راه است. برای درک بهتر این موضوع به این شکل توجه کنید.



شکل ۳۳-۵ انتخاب بهترین مسیر

به دقت به شکل ۳۳-۵، توجه کنید، R1 برای رسیدن به شبکه‌ی 192.168.1.0 دو مسیر سر راه خود می‌بیند. در مسیر بالایی برای رسیدن به شبکه‌ی 192.168.1.0، سه روتر در سر راه قرار دارد، اما در مسیر پایینی

www.takbook.com

پنج روتر در سر راه قرار دارد، پس به این نتیجه می‌رسیم که مسیر بالایی نسبت به مسیر پایینی سریع‌تر و کوتاه‌تر است. در پروتکل Rip که در ادامه با آن آشنا می‌شویم، انتخاب بهترین مسیر از روی متریک و یا همان روترهای سر راه است.

در شبکه‌هایی که با پروتکل IGRP راه‌اندازی می‌شوند، قضیه کمی فرق می‌کند. در پروتکل IGRP برای انتخاب بهترین متریک، چند روش وجود دارد که هر کدام را باهم دیگر بررسی می‌کنیم.

- Bandwidth
- Delay
- Reliability
- Loading
- MTU

در این پروتکل، انتخاب بهترین مسیر از روی متریک صورت نمی‌گیرد، بلکه از روی دو گزینه‌ی اول، یعنی Bandwidth و Delay صورت می‌گیرد که این دو گزینه به نسبت بقیه‌ی گزینه‌ها مهم‌تر هستند. اگر پهنای باند یک مسیر بیشتر باشد، همان مسیر به عنوان بهترین مسیر انتخاب می‌شود.

شکل ۳۴-۵ بررسی Bandwidth و Delay

به شکل ۳۴-۵ توجه کنید، مسیر یک، از پورت‌های FastEthernet استفاده می‌کند و مسیر دوم از پورت‌های GigabitEthernet استفاده می‌کند که پهنای باند FastEthernet، 100000 است و پهنای باند GigabitEthernet، 1000000 است و Delay اولی 100 میلی‌ثانیه و دومی 10 میلی‌ثانیه است و به خاطر بیشتر بودن پهنای باند و کمتر بودن زمان تأخیر، مسیر دوم، یعنی روترهای R4، R5، R6، R3 انتخاب می‌شود.

برای اینکه بتوانید پهنای باند مورد نظر یک پورت را مشاهده کنید، در مد Privileged از دستور زیر استفاده کنید، مثلاً برای پورت GigabitEthernet به این صورت استفاده کنید:

www.takbook.com

Router# **Show interface GigabitEthernet0/0**

همان‌طور که در شکل ۳۵-۵ مشاهده می‌کنید، پهنای باند برای پورت GigaEthernet، 1000000 و Delay ، 10 است.

```
Router#show interfaces g
Router#show interfaces gigabitEthernet 0/0
GigabitEthernet0/0 is administratively down, line protocol is down (disabled)
  Hardware is CN Gigabit Ethernet, address is 0090.2b2d.2101 (bia 0090.2b2d.2101
)
  MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,        Delay
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)                                BandWidth
  Full-duplex, 100Mb/s, media type is RJ45
  output flow-control is unsupported, input flow-control is unsupported
  ARP type: ARPA, ARP Timeout 04:00:00,
  Last input 00:00:08, output 00:00:05, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0 (size/max/drops); Total output drops: 0
  Queueing strategy: fifo
  Output queue :0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     0 watchdog, 1017 multicast, 0 pause input
```

شکل ۳۵-۵ بررسی Bandwidth و Delay

در مورد Administrative Distance کمی صحبت کنیم؛ یک عدد مختص پروتکل‌های شبکه و شبکه‌های **connected** است. به جدول ۴-۵، نگاه کنید:

جدول ۴-۵ Administrative Distance

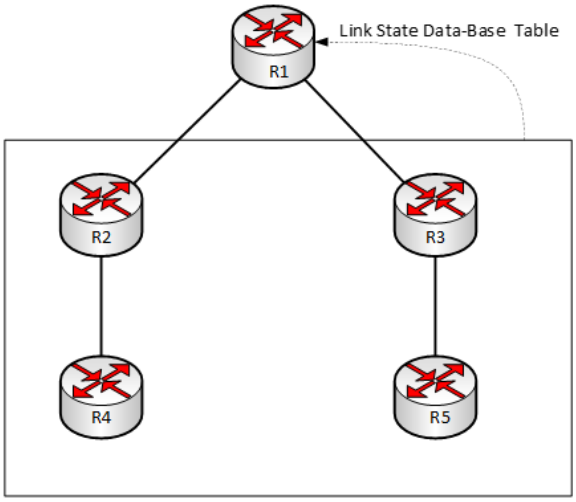
Route Type	Administrative Distance
Connected	0
Static	1
BGP (external routes [eBGP])	20
EIGRP (internal routes)	90
IGRP	100
OSPF IS-IS	110 115
RIP	120
EIGRP (external routes)	170
BGP (internal routes [iBGP])	200
DHCP default route	254
Unusable	255

Administrative Distance، معیار و ملاکی است برای انتخاب یک پروتکل از بین پروتکل‌های مختلف در یک شبکه، مثلاً اگر به یک روتر از دو طرف اطلاعات برسد و یکی از این طرف‌ها Rip با AD 120 و طرف دیگر با IGRP با AD 100 است. برای انتخاب یکی از این مسیرها، مسیری که AD پایین‌تر دارد، انتخاب می‌شود (AD مخفف کلمه‌ی Administrative Distance است) و اطلاعات را از همان مسیر دریافت می‌کند. AD مربوط به static route که به صورت دستی وارد می‌کردیم 1 است.

www.takbook.com

۵-۴-۴ پروتکل‌های Link State

این نوع پروتکل، یک ویژگی عمده دارند و آن هم این است که تصویر کلی از شبکه یا همان گراف کامل از شبکه را دارند، یعنی هر روتر دارای پروتکل‌های Link State، خود را به عنوان ریشه‌ی درخت و بقیه را به عنوان شاخه و برگ حساب می‌کند، اما بدون دور است و به‌این‌ترتیب یک تصویر کلی از شبکه را دارد و از روی همین گراف، بهترین و کوتاه‌ترین مسیر تا شبکه‌ی دیگر را محاسبه و انتخاب می‌کند. به شکل ۳۶-۵، توجه کنید:



شکل ۳۶-۵ Link State

در شکل ۳۶-۵، روتر R1 با استفاده از گراف از نقشه‌ی کل شبکه خبر دارد و بر طبق همین نقشه به بهترین مسیر دست پیدا می‌کند، شاید کمی گیج‌کننده باشد، اما در ادامه، کاملاً با این پروتکل‌ها آشنا می‌شویم، پروتکلی که در این دسته قرار دارند، OSPF(Open Shortest Path First) است که به صورت مفصل روی این پروتکل بحث خواهیم کرد.

پروتکل‌ها از نوع Link State از سه جدول تشکیل شده‌اند:

- Routing Table
- Link state Data-base
- Neighbor Table

در روترهایی که این نوع پروتکل‌ها اجرا می‌شوند، ۳ جدول داخل آن‌ها تشکیل می‌شود که در جدول اول که Neighbor است، اطلاعات شبکه‌های روترهای مجاور در آن ثبت می‌شود و بعد از آن این جدول به صورت آپدیت به روترهای دیگر فرستاده می‌شود و تشکیل جدول Link Sate Data-Base می‌دهند. بعد از آن، الگوریتم بهترین مسیر، با عنوان SPF که مخفف Shortest Path First است، اجرا می‌شود و شبکه را به صورت یک درخت بدون دور درمی‌آورد و بهترین مسیر را به صورت روش‌های خاصی پیدا می‌کند.

پروتکل‌های OSPF و ISIS از دسته پروتکل Link state هستند.

www.takbook.com

۵-۴-۵ کار با پروتکل (Rip)Routing Information Protocol

قبل از شروع کار به این نکته توجه کنید که پروتکل Rip در دوره‌ی جدید دوره‌ی CCNA وجود ندارد و در این قسمت برای اینکه یک ذهنیتی از آن داشته باشید دوباره آن را به صورت کامل بررسی می‌کنیم.

این پروتکل یکی از محبوب‌ترین پروتکل‌های روتینگ و یکی از قدیمی‌ترین آن‌ها هم است. این پروتکل زیرمجموعه‌ی پروتکل‌های Distance Vector است و یک پروتکل IGPs است و در داخل یک AS(Autonomous System) کار می‌کند.

این پروتکل، مخصوص شبکه‌های کوچک است و در شبکه‌های بزرگ بالای ۱۵روتر کاربرد ندارد.

یکی دیگر از ویژگی‌های این پروتکل، این است که جدول روتینگ را به صورت کامل در فواصل زمانی ۳۰ ثانیه به دیگر روترها ارسال می‌کند که به آن Priodic Update می‌گویند که قبلاً روی این موضوع صحبت کردیم.

پروتکل Rip بر دو نوع است:

- ✓ Rip Version 1
- ✓ Rip Version 2

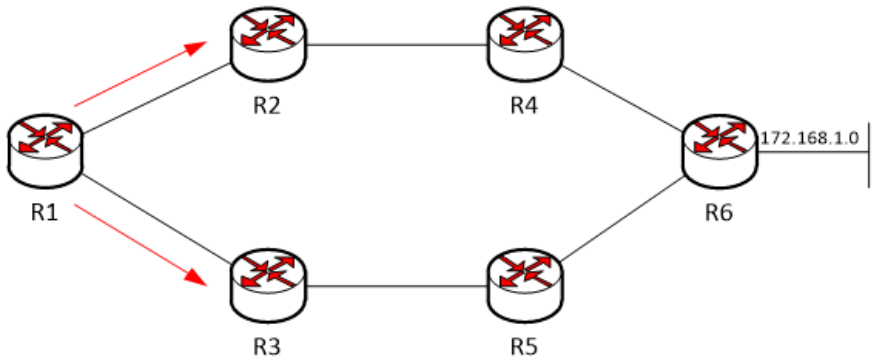
همان‌طور که در مطالب قبلی خواندید، ملاک انتخاب بهترین مسیر در این پروتکل، Hop Count یا روترهای سر راه است. توجه داشته باشید، حداکثر متریک در این پروتکل، ۱۵ است و شما حداکثر روتری که در این پروتکل در یک AS می‌توانید استفاده کنید، ۱۵ عدد است. اگر متریک بیشتر از ۱۵ شود، شبکه غیرقابل‌دسترس خواهد بود.

ویژگی‌های پروتکل Rip در یک نگاه:

- **در فواصل زمانی مشخص (30 ثانیه) کل جدول روتیگ را به صورت Broadcast به روترهای مجاورش ارسال می‌کند (Priodic Update).**
- **جزو پروتکل‌های IGPs است.**
- **حداکثر متریک 15 است.**

یکی دیگر از ویژگی‌های پروتکل Rip، استفاده بهینه از شبکه یا Load Balancing است. اگر دو مسیر با متریک یکسان داشته باشد، اطلاعات را بر روی هر دو مسیر انتقال می‌دهد و این امر باعث افزایش کارایی شبکه می‌شود.

www.takbook.com



شکل ۵-۳۷ Load Balancing

در شکل ۵-۳۷، R1 برای رسیدن به R6 می‌تواند از دو مسیر حرکت کند، چون برای رسیدن به روتر مورد نظر Hop Count سر راه یا روترهای سر راه در هر دو مسیر برابر است، پس از هر دو مسیر به صورتLoad Balancing استفاده می‌کند.

حالا سؤال پیش می‌آید که Rip Version 1 و Rip Version 2 چه تفاوتی باهم دارند؟ برای دریافت جواب به جدول ۵-۳۸، توجه کنید:

RIPv1	RIPv2
Distance vector	Distance vector
Maximum hop count of 15	Maximum hop count of 15
Classful	Classless
Broadcast based	Uses Multicast 224.0.0.9
No support for VLSM	Supports VLSM networks
No authentication	Allows for MD5 authentication
No support for discontiguous networks	Supports discontiguous networks

شکل ۵-۳۸ تفاوت RIPv1 با RIPv2

Rip Version 1 از CIDR و VLSM پشتیبانی نمی‌کند و SubnetMask را به همراه Net ID نمی‌فرستد.

۵-۵-۴-۱ راه‌اندازی پروتکل Rip

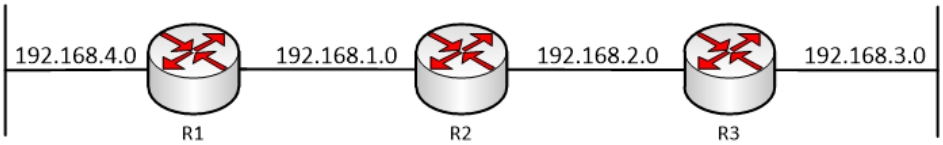
برای راه‌اندازی پروتکل Rip به صورت زیر عمل می‌کنیم:

Router(Config)# **Router Rip**
Router(config-router)# **Netwok** ***Network number***

در قسمت اول وارد مد Global می‌شویم و با دستور Router Rip پروتکل Rip بر روی روتر راه‌اندازی می‌شود و بعدازآن باید شبکه‌های متصل به روتر را به آن معرفی کنیم. با یک مثال به این موضوع پی خواهیم برد.

www.takbook.com

مثال ۲: Packet Tracer را اجرا کرده و 3 روتر مانند شکل ۳۹-۵، به صفحه اضافه کنید و آن‌ها را از طریق کابل به هم متصل کنید و طبق شکل آدرس‌دهی کنید.



شکل ۳۹-۵ مثال RIP

می‌خواهیم در این شبکه، پروتکل Rip راه‌اندازی کنیم؛ بر روی R1 کلیک می‌کنیم و دستورات زیر را در آن وارد می‌کنیم:

Router(config)#**router Rip**
Router(config-router)#**network 192.168.1.0**
Router(config-router)#**network 192.168.4.0**

همان‌طور که مشاهده می‌کنید، با دستور Router Rip، وارد پروتکل Rip شده‌ایم. بعدازآن باید آدرس NET ID شبکه‌های متصل به روتر را معرفی کنیم، شبکه‌هایی که به روتر R1 متصل می‌باشند، 192.168.1.0 و 192.168.4.0 هستند. همین کار را روی روترهای دیگر انجام می‌دهید.

تنظیمات روتر R2:

Router(config)#**router Rip**
Router(config-router)#**network 192.168.1.0**
Router(config-router)#**network 192.168.2.0**

تنظیمات روتر R3:

Router(config)#**router Rip**
Router(config-router)#**network 192.168.2.0**
Router(config-router)#**network 192.168.3.0**

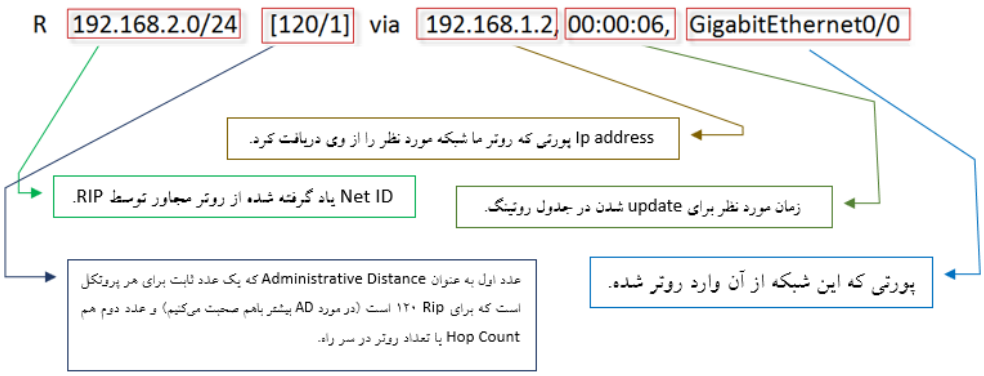
به همین راحتی توانستیم این پروتکل را روی تک‌تک روترها راه‌اندازی کنیم. حالا باید ببینیم جدول روتینگ در چه وضعیتی است. همان‌طور که قبلاً گفتیم این جدول اطلاعات مسیرهای مختلف شبکه‌ها را در خود ذخیره می‌کند. برای نمایش جدول Routing باید از دستور زیر در یکی از روترها استفاده کنیم، وارد مد Privileged می‌شویم و دستور Show IP Route را وارد می‌کنیم، به مانند شکل ۴۰-۵، این کار را در روتر R1 انجام می‌دهیم:

www.takbook.com


```
Router#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.1.0/24 is directly connected, GigabitEthernet0/0
L       192.168.1.1/32 is directly connected, GigabitEthernet0/0
R    192.168.2.0/24 [120/1] via 192.168.1.2, 00:00:01, GigabitEthernet0/0
R    192.168.3.0/24 [120/2] via 192.168.1.2, 00:00:01, GigabitEthernet0/0
     192.168.4.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.4.0/24 is directly connected, GigabitEthernet0/1
L       192.168.4.1/32 is directly connected, GigabitEthernet0/1
```

شکل ۴۰-۵ *نتیجه دستور Show IP Route*

همان‌طور که مشاهده می‌کنید، جدول روتیگ ip addressهای مختلفی را به ما نشان می‌دهد. شبکه‌هایی که با C شروع می‌شوند، شبکه‌های connected و متصل به روتر و شبکه‌ای که با L شروع می‌شود، IP address متصل به روتر است، اما R شبکه‌هایی هستند که از طریق پروتکل Rip وارد جدول شده‌اند و اگر به شکل توجه کنید این شبکه‌ها را از روترهای R2 و R3 یاد گرفته است، مثلاً یکی از این خطها به صورت شکل ۴۱-۵ است:



شکل ۴۱-۵ *بررسی خروجی دستور Show IP Route*

همان‌طور که مشاهده می‌کنید IPها به صورت ClassFull در جدول روتینگ قرار دارند و این موضوع را بیان می‌کند که پروتکل Rip Version 1 از ClassLess پشتیبانی نمی‌کند. امیدوارم درباره‌ی ClassLess در قسمت IPها به‌خوبی مطالعه کرده باشید.

www.takbook.com

به خاطر ClassFull بودن این پروتکل (مثلاً اگر شما ipهایی در رنج کلاس b داشته باشید، مانند این ipهای 172.16.1.0، 172.16.2.0، 172.16.3.0) در این صورت در معرفی Network در پروتکل Rip از این روش استفاده می‌کنید.

Network 172.16.0.0

به خاطر اینکه همه‌ی IP ها در رنج کلاس b بودند، فقط لازم است در موقع تعریف شبکه از Net ID آن استفاده کنید. این Net ID همه‌ی این IP ها را دربرمی‌گیرد. به جدول ۵-۵ توجه کنید.

172.16.0.0/16	172.16.1.0
	172.16.2.0
	172.16.3.0

جدول ۵-۵ Net ID

تایمرها در پروتکل Rip:

- Update Timer
- Invalid Timer
- Holddown Timer
- Flush Timer

Update Timer:

این زمان، همان زمان Priodic Update است و هر ۳۰ ثانیه یک‌بار، کل جدول روتینگ را به صورت Broadcast به ip، 255.255.255.255 می‌فرستد، البته در پروتکل Rip ver2 به صورت Multicast و به IP، 224.0.0.9 می‌فرستد.

Invalid Timer:

این تایمر زمانی اجرا می‌شود که در مورد یک شبکه، هیچ‌گونه اطلاعاتی در زمان 90 ثانیه دریافت نکند، به حالت Hold رفته و در جدول روتینگ مقابل این شبکه، جمله‌ی Posibly Down را درج می‌کند.

Holddown Timer:

این تایمر با تایمر invalid Timer باهم کار می‌کنند، هر موقع در مورد یک شبکه متریک بی‌نهایت را دریافت کند، به حالت Hold رفته و جمله‌ی Posibly Down را در کنار آن شبکه در جدول روتینگ درج می‌کند و زمان آن ۱۸۰ ثانیه است.

Flush Timer:

این تایمر بعد از ۲۷۰ ثانیه که تمام تایمرهای بالا به کار خود پایان دادندآن را از جدول حذف خواهد کرد. اگر update برای شبکه‌ی مورد نظر نرسد، آن را از لیست یا همان Routing Table حذف می‌کند.

این سؤال شاید برای شما پیش آید که آیا می‌شود این تایمرها را تغییر داد؟

www.takbook.com

بله این کار شدنی است و باید وارد پروتکل Rip شده و دستور زیر را وارد کنید:

Router(config-router)# **timers basic ?**
<0-4294967295> Interval between updates
Router(config-router)#**timers basic 10 ?**
<1-4294967295> Invalid
Router(config-router)#**timers basic 10 50 ?**
<0-4294967295> Holddown
Router(config-router)#**timers basic 10 50 90 ?**
<1-4294967295> Flush
Router(config-router)#**timers basic 10 50 90 30**

همان‌طور که مشاهده می‌کنید با دستور Timer basic می‌توان این کار را انجام داد. اولین تایمر همان Priodic Update است که به صورت پیش‌فرض ۳۰ است و شما می‌توانید آن را تغییر دهید. در قسمت دوم، Invalid است که به‌طور پیش‌فرض ۹۰ است و می‌توانید آن را تغییر دهید. در قسمت بعد، Holddown تایمر است که زمان آن ۱۸۰ است و می‌توانید تغییر دهید و قسمت آخر، تایمر Flush است که زمان آن ۲۷۰ ثانیه است و می‌توانید آن را تغییر دهید.

فرمان Debug:

این فرمان برای کنترل و عیب‌یابی به کار می‌رود و برای فعال کردن آن برای پروتکل RIP دستور زیر را در مد Privileged وارد می‌کنیم:

Router# **Debug IP Rip**

این دستور را در مثال بالا در R1 اجرا می‌کنیم:

```
Router#debug ip rip
RIP protocol debugging is on
Router#RIP: ignored v1 packet from 192.168.1.2 (illegal version)
RIP: sending  v2 update to 224.0.0.9 via GigabitEthernet0/0 (192.168.1.1)
RIP: build update entries
      192.168.4.0/24 via 0.0.0.0, metric 1, tag 0
RIP: sending  v2 update to 224.0.0.9 via GigabitEthernet0/1 (192.168.4.1)
RIP: build update entries
      192.168.1.0/24 via 0.0.0.0, metric 1, tag 0
RIP: ignored v1 packet from 192.168.1.2 (illegal version)
RIP: sending  v2 update to 224.0.0.9 via GigabitEthernet0/0 (192.168.1.1)
RIP: build update entries
      192.168.4.0/24 via 0.0.0.0, metric 1, tag 0
RIP: sending  v2 update to 224.0.0.9 via GigabitEthernet0/1 (192.168.4.1)
RIP: build update entries
      192.168.1.0/24 via 0.0.0.0, metric 1, tag 0
```

شکل ۴۲-۵ خروجی دستور Debug IP Rip

همان‌طور که در شکل ۴۲-۵، مشاهده می‌کنید، این دستور اجرا شده است و تمام حرکات پروتکل Rip را در نظر دارد. این پروتکل بعد از زمان‌های مشخص نسبت به ارسال و دریافت اطلاعات اقدام می‌کند. اگر دقیق نگاه کنید، یک ip به شماره‌ی 224.0.0.9 وجود دارد که این ip همان Multicast است که در Rip

www.takbook.com

Version2 کاربرد دارد. این حالت نشان‌دهنده‌ی ارسال جدول روتینگ به این آدرس است، برای اطلاع به روترهای دیگر در شبکه RIP است.

برای اینکه این دستور را غیرفعال کنید از دستور زیر استفاده کنید:

Router#**no debug all**

راه‌اندازی پروتکل Rip Version2:

یکی از ویژگی‌های مهم Rip V2 این است که ClassLess و VLSM را پشتیبانی می‌کند و بهره‌دهی شبکه را افزایش می‌دهد.

برای اینکه در پروتکل rip از این Version استفاده کنید، در داخل Rip دستور Version 2 را وارد کنید، مانند زیر عمل کنید:

Router(config)#**router rip**
Router(config-router)#**version 2**

به همین راحتی پروتکل V1 تبدیل به V2 شد و توانایی پشتیبانی از CIDR و VLSM را دارد.

۵-۵ سوالات فصل پنجم

1. Which of the following installation steps are more likely required on a Cisco router, but not typically required on a Cisco switch? (Choose two answers.)

کدام یک از مراحل نصب زیر بر روی روتر سیسکو انجام می‌شود ولی به طور معمول بر روی سوئیچ انجام نمی‌شود؟ (دو گزینه را انتخاب کنید)

www.takbook.com

a. Connect Ethernet cables
b. Connect serial cables
c. Connect to the console port
d. Connect the power cable
e. Turn the on/off switch to “on”

2. Which of the following commands might you see associated with a router CLI, but not with a switch CLI?

کدام یک از دستورات زیر را می‌شود با CLI مربوط به روتر دید اما در سوئیچ امکان‌پذیر نیست؟

a. The show mac address-table command
b. The show ip route command
c. The show running-config command
d. The show interfaces status command

3. Which answers list a task that could be helpful in making a router interface G0/0 ready to route packets? (Choose two answers.)

کدام یک از گزینه‌های زیر بهترین گزینه برای ایجاد یک Router Interface است که بتواند پکت‌ها را Route کند؟

a. Configuring the ip address address mask command in G0/0 configuration mode
b. Configuring the ip address address and ip mask mask commands in G0/0 configuration mode
c. Configuring the no shutdown command in G0/0 configuration mode
d. Setting the interface description in G0/0 configuration mode

4. The output of the show ip interface brief command on R1 lists interface status codes of “down” and “down” for interface GigabitEthernet 0/0. The interface connects to a LAN switch with a UTP straight-through cable. Which of the following could be true?

خروجی دستور show ip interface brief برای روتر R1 لیستی از Interface ها است که در آن کد down و down برای Interface GigabitEthernet 0/0 مشخص شده است، اگر این پورت روتر را با کابل straight-through به سوئیچ متصل کنیم، کدام یک از گزینه‌های زیر بهترین انتخاب خواهد بود؟

a. The shutdown command is currently configured for router interface G0/0.
b. The shutdown command is currently configured for the switch interface on the other end of the cable.
c. The router was never configured with an ip address command on the interface.
d. The router was configured with the no ip address command.

5. Which of the following commands do not list the IP address and mask of at least one interface? (Choose two answers.)

کدام یک از دستورات زیر آدرس IP و Mask را در خروجی نمایش نمی‌دهد؟(دو جواب را انتخاب کنید)

a. show running-config
b. show protocols type number
c. show ip interface brief
d. show interfaces
e. show version

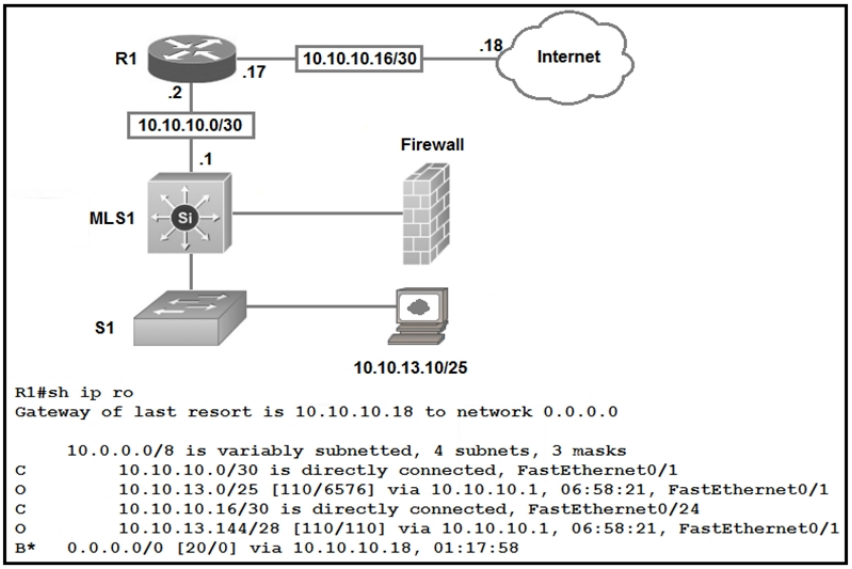
6. Which of the following is different on the Cisco switch CLI for a Layer 2 switch as compared with the Cisco router CLI?

www.takbook.com

کدام یک از گزینه‌هایی زیر تفاوت بین CLI سوئیچ سیسکو لایه دوم را با CLI روتر سیسکو نمایش می‌دهد؟

a. The commands used to configure simple password checking for the console
b. The number of IP addresses configured
c. The configuration of the device's hostname
d. The configuration of an interface description

7. Refer to the exhibit. Which type of route does R1 use to reach host 10.10.13.10/32?
با توجه به شکل ۴۳-۵، روتر R1 برای رسیدن به میزبان 10.10.13.10/32 از کدام نوع استفاده خواهد کرد؟

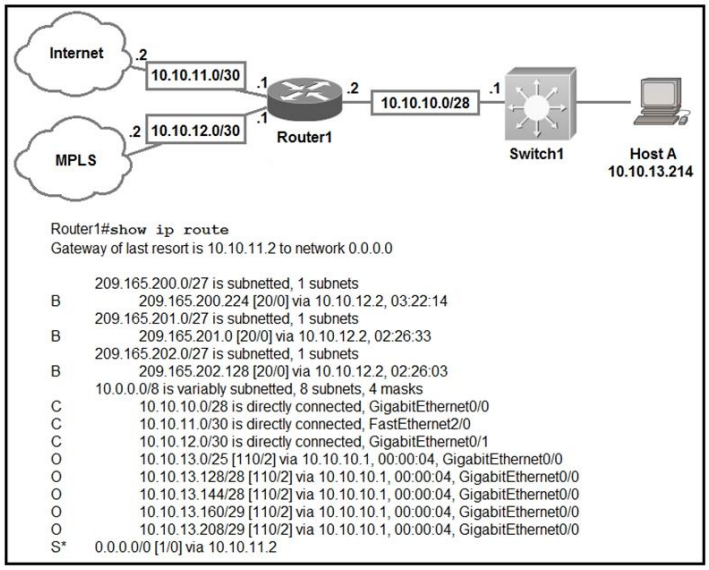


شکل ۴۳-۵ سوال شماره‌ی ۷

a. default route
b. network route
c. host route
d. floating static route

8. Refer to the exhibit. Which prefix does Router1 use for traffic to Host A?
طبق شکل ۴۴-۵، Router1 از کدام پیشوند برای ترافیک Host A استفاده می‌کند؟

www.takbook.com



شکل ۴۴-۵ سوال شماره‌ی ۷

a. 10.10.10.0/28
b. 10.10.13.0/25
c. 10.10.13.144/28
d. 10.10.13.208/29

www.takbook.com

www.takbook.com

www.takbook.com

فصل ششم

پروتکل OSPF

پروتکل OSPF(Open Shortest Patch First) یک پروتکل آزاد است و مختص شرکت خاصی نیست و توسط سازمان IETF در سال ۱۹۸۸ نوشته شده است، مانند EIGRP نیست که فقط در روترهای سیسکو قابل اجرا باشد، بلکه در تمام روترهای شرکت‌های مختلف کاربرد دارد.

پس اگر شما در شبکه‌های خود از روترهای مختلف با برندهای مختلف استفاده کنید، نمی‌توانید روی آن‌ها پروتکل خاص سیسکو یعنی EIGRP اجرا کنید، بلکه فقط باید پروتکل OSPF یا RIP روی آن‌ها run کنید تا بتوانند باهم دیگر ارتباط برقرار کنند.

این پروتکل از مجموعه پروتکل‌های Link state است و زیرمجموعه‌ی پروتکل‌های IGPs است، یعنی داخل یک AS کار می‌کنند.

الگوریتمی که در این پروتکل استفاده می‌شود، Dijkstra است که شبکه را به صورت یک درخت بدون دور در نظر می‌گیرد.

OSPF که در این قسمت بررسی می‌کنیم، Ospf Version 2 است که با IPV4 کار می‌کند و در قسمت IPV6 از OSPF Version 3 استفاده می‌شود.

OSPF از جدولی به نام Link-state Database استفاده می‌کند که کل اطلاعات شبکه یا نقشه‌ی شبکه را برای انتخاب کوتاه‌ترین مسیر در خود ذخیره می‌کند و برای به دست آوردن کوتاه‌ترین مسیر از الگوریتمی به نام SPF استفاده می‌کند و بعد از پیدا شدن مسیر، آن را در جدول دیگری به نام Routing Table ذخیره می‌کند.

OSPF برای ارسال آپدیت از بسته‌هایی به نام LSA (Link-state Advertisement) استفاده می‌کند که اطلاعات جدول خود را به نام Link-state Database به روترهای دیگر ارسال می‌کند.

همانطور که گفتیم پروتکل‌های Distance Vectore برای ارسال Update کل جدول را به روترهای همسایه ارسال می‌کردند که به عنوان Priodic Update بود، اما در OSPF این‌چنین نیست. اگر تغییری در جدول ایجاد شود، این تغییر بلافاصله از طریق LSA که در صفحات قبل توضیح دادیم به بقیه‌ی روترها خبر داده می‌شود و خیلی کم از پهنای باند شبکه استفاده می‌کند، به این آپدیت، Triggered Update می‌گویند که تغییرات را بسیار سریع اعلام می‌کند.

باید گفت: این‌گونه هم نیست که OSPF نخواهد کل جدول را هرگز ارسال نکند، این کار را هر ۳۰ دقیقه یک‌بار انجام می‌دهد که کل جدول Database را به شبکه‌ی مورد نظر ارسال می‌کند.

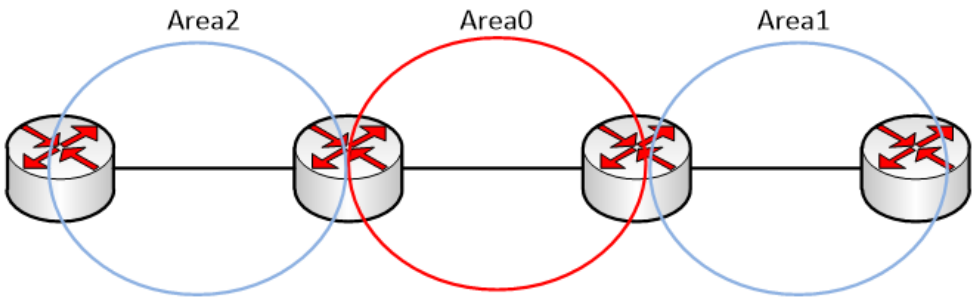
www.takbook.com

این پروتکل برای شبکه‌های بزرگ بسیار کارآمد است و در حال حاضر در حال استفاده در شبکه‌های بزرگ است.

OSPF شبکه‌های بزرگ را به ناحیه‌های(Area) مختلف تقسیم می‌کند که دلایل خاص خودش را دارد:

- با ایجاد ناحیه، سرعت کار این الگوریتم بسیار افزایش پیدا می‌کند.
- کم حجم شدن جدول Routing به خاطر ایجاد ناحیه.
- مدیریت بر چند روتر بهتر از مدیریت بر چندین روتر است.
- با ایجاد ناحیه، اگر یکی از روترها دستکاری یا مشکلی برای آن پیش بیاید، بقیه‌ی روترها در ناحیه‌ی دیگر بدون مشکل به کار خود ادامه می‌دهند.

به شکل ۱-۶، توجه کنید:



شکل ۱-۶ بررسی Area

BackBone Area یا Area0 ناحیه‌ای است که areaهای دیگر به وی متصل می‌شوند و تمام اطلاعات areaهای دیگر باید از این area رد شود، پس این area به‌عنوان BackBone یا ستون فقرات شبکهOSPF شناخته می‌شود. به طور خلاصه می‌توان گفت این area پادشاه همه‌ی area هاست.

اگر دسته‌بندی یا ناحیه در OSPF وجود نداشته باشد، الگوریتم SPF که کار پیدا کردن کوتاه‌ترین مسیر را انجام می‌دهد با مشکل مواجه خواهد شد، چون جدول Database که گراف شبکه در آن قرار دارد، بسیار بزرگ می‌شود. توجه داشته باشید که با ایجاد یک area، الگوریتم SPF فقط در همان Area پردازش خود را انجام می‌دهد و بر کل شبکه تأثیر ندارد، پس الگوریتم SPF(Shortest Path First)، فقط در یک Area پردازش خود را انجام می‌دهد و زمانی که به نتیجه برسد، این نتیجه را با area های دیگر در میان می‌گذارد.

۱-۶ انتخاب بهترین مسیر در OSPF

www.takbook.com

در ospf انتخاب بهترین مسیر از طریق متریکی به نام Cost انجام می‌شود که از طریق الگوریتم SPF کوتاه‌ترین مسیر به دست می‌آید.

این نکته را توجه داشته باشید که هر چه پهنای باند یک خط بیشتر باشد، cost آن کمتر است، پس پهنای باند رابطه‌ی معکوس با cost دارد.

برای به دست آوردن Cost باید 1000000000 را تقسیم بر مقدار پهنای باند کنیم تا عدد مورد نظر به دست آید.

۲-۶ بررسی Link State Advertisements

روترهایی که در پروتکل OSPF قرار دارند دارای یک دیتابیس با عنوان link-state database یا LSDB هستند که پروتکل OSPF با بهره‌گیری از LSA از توپولوژی شبکه آشنا خواهد شد و دیتابیس خود را طبق آن ایجاد و آپدیت می‌کند.

هر LSA دارای یک شماره و یک طول عمر است که به طور پیش فرض ۳۰ دقیقه است.

زمانی که روتر یک Link State Advertisement دریافت می‌کند با دیتابیس LSDB مقایسه می‌شود، اگر LSDB جدید بود به دیتابیس اضافه شده و الگوریتم SPF اجرا می‌شود.

اگر LSA از یک Router ID که قبلا در دیتابیس موجود است باشد Sequence Number آن مقایسه می‌شود و اگر قدیمی‌تر بود از آن صرفه نظر می‌شود. اگر Link State Advertisement قدیمی‌تر باشد LSA جدیدتر که در حافظه موجود است برای فرستنده LSA ارسال می‌شود.

Sequence Number ۳۲ بیت است. اولین مقدار Sequence Number برابر x80000001 است.

Sequence Number به یکی از دو دلیل زیر تغییر می‌کند:

- زمانی که یک Route اضافه یا حذف شود.
- طول عمر LSA تمام به پایان برسد.

انواع LSA

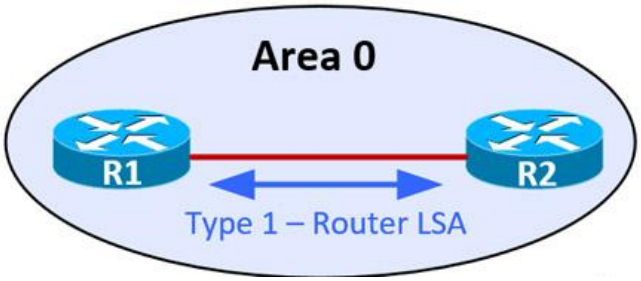
OSPF برای تبلیغ جداول خود از LSAهای مختلف استفاده می‌کند که این LSAها دارای نماد خاصی در جدول مسیریابی هستند.

هر اطلاعاتی که از طریق OSPF به روترهای دیگر اعلام می‌شود به اصطلاح Advertise می‌شود، دارای نوع خاصی است که در header پروتکل از بیت نهم تا شانزدهم به آن اختصاص یافته‌است، این LSAها عبارت‌ند از:

Type 1

همه‌ی روترهای یک ناحیه این نوع داده را ارسال می‌کنند و در آن اطلاعات مربوط به روترهای همسایه و هزینه رسیدن به آنها فهرست می‌شود. این نوع از داده فقط مخصوص همان ناحیه‌ای است که ساخته شده. نام آن را Router Link یا Router LSA گویند، که شکل ۲-۶ نشانگر آن است.

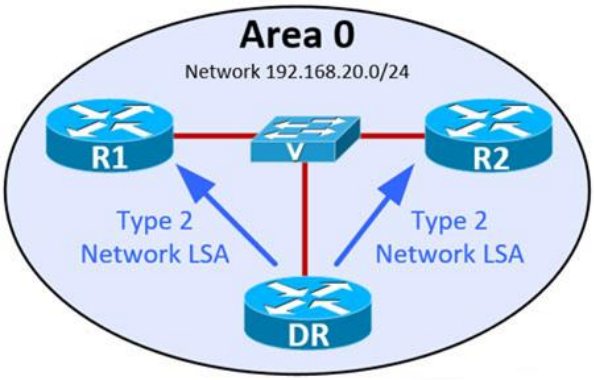
www.takbook.com



شکل ۲-۶ بررسی Type 1 در OSPF

Type 2

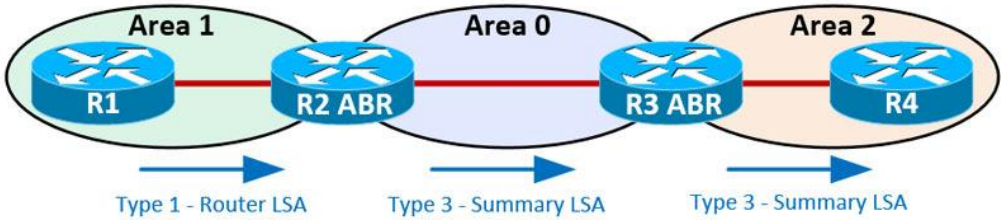
این نوع از LSA توسط روتر برگزیده یا DR (Designated Router) ساخته شده و اطلاعات مربوط به همسایه‌های یک قسمت یا سگمنت مجاور را فهرست می‌کند. این نوع نیز از ناحیه‌ای که در آن ساخته شده فراتر نمی‌رود. نام آن Network Link یا Network LSA است، که شکل ۳-۶ نشانگر آن است.



شکل ۳-۶ بررسی Type 2 در OSPF

Type 3

توسط روترهای مرز ناحیه یا ABR (Area Border Router) ساخته شده و بین ناحیه‌ها ارسال می‌شوند. نام آن Network Summary یا Summary LSA است، که شکل ۴-۶ نشانگر آن است.

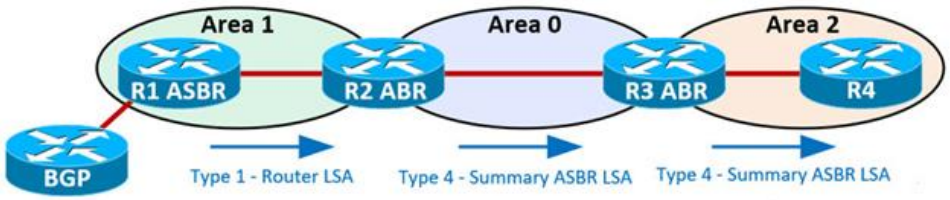


شکل ۴-۶ بررسی Type 3 در OSPF

www.takbook.com

Type 4

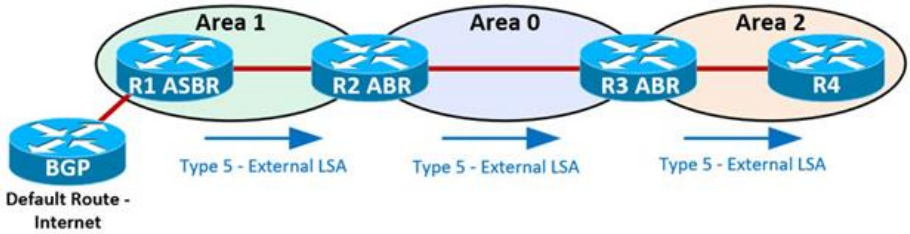
این نوع داده را روتر ABR به ناحیه ستون فقرات شبکه یا Backbone ارسال می‌کند تا حضور یک ASBR را در ناحیه مورد نظر اعلام کند. نام آن ASBR Summary یا Summary LSA است.



شکل ۵-۶ بررسی Type 4 در OSPF

Type 5

توسط روترهای ASBR (Autonomous System Border Router) ساخته می‌شود تا اطلاعات مربوط به مسیرهای خارجی (مسیرهایی که از پروتکل مسیریابی OSPF استفاده نمی‌کنند) به روترهایی اجرا کننده پروتکل OSPF ارسال شود. نام آن External Link یا External LSA است.



شکل ۶-۶ بررسی Type 5 در OSPF

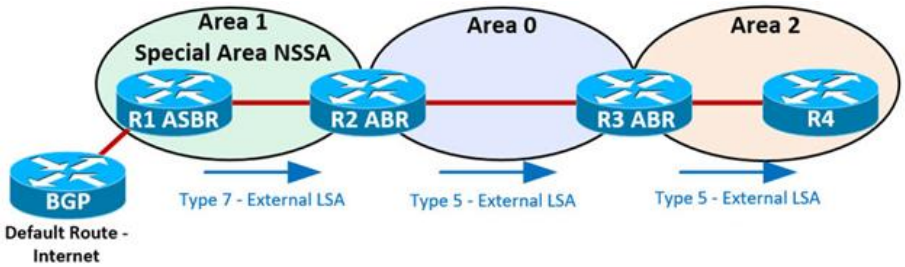
Type 6

در عملیات Multicast در پروتکل OSPF شناخته می‌شود و نام آن هم Multicast LSA است.

Type 7

در ناحیه‌ی Route نوع NSSA خارجی توسط ASBR در همان Area توسط این نوع LSA اعلام می‌شود و توسط ABR به Type 5 تغییر حالت می‌دهد.

www.takbook.com



شکل ۷-۶ بررسی Type 7 در OSPF

نکته: انواع Type دیگر مانند Type 8، Type 9، Type 10 و Type 11 هم وجود دارد که برای گسترش قابلیت OSPF به کار می‌روند و خارج از بحث این کتاب است.

۶-۳ راه‌اندازی پروتکل OSPF

برای فعال کردن پروتکل OSPF باید از دستور زیر به همراه یک Proccess ID استفاده کنیم:

```
Router(Config)# router ospf ?
<1-65535>  Process ID
```

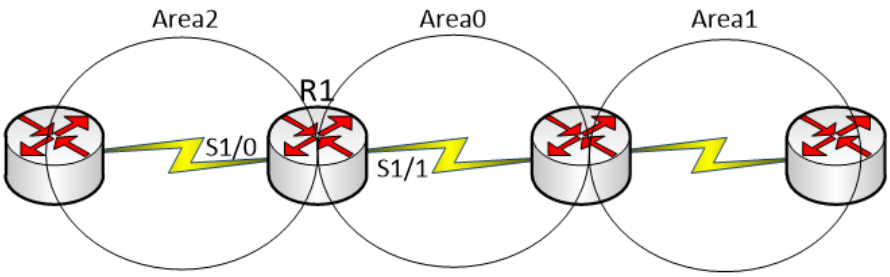
در پروتکل EIGRP، شماره‌ای که اختصاص می‌دهیم، باید در همه‌ی روترها یکی باشد، اما شماره‌ای که به این پروتکل داده می‌شود، لازم نیست که در همه‌ی روترها یکی باشد؛ از شماره ۱ تا ۶۵۵۳۵ می‌توانید اختصاص دهید، پس مانند AS ا نیستند که باید در همه‌ی روترها یکی باشد. این عدد فقط برای متمایز کردن OSPFها باهم است.

برای تعریف کردن NETWORK، باید از روش زیر استفاده کنید.

```
Router(config-router)#Network 192.168.1.1 0.0.0.0  area0
```

برای تعریف شبکه، IP Address را وارد می‌کنیم، بعد Wild Card Mask را و بعدازآن مشخص می‌کنیم که این شبکه در کدام Area یا ناحیه قرار دارد. به شکل ۸-۶، نگاه کنید، اگر توجه داشته باشید Se1/1 مربوط به R1 در area 0 قرار دارد، پس اگر وارد این روتر شدیم در موقع تعریف شبکه در پروتکل OSPF باید آن را داخل Area0 قرار دهیم، مثلاً در سمت دیگر، روتر R1 پورت سریال Se1/0 در area2 قرار دارد که باید در تعریف شبکه‌ی این پورت در Area2 قرار دهیم.

www.takbook.com



شکل ۸-۶ مثال OSPF

در مورد Wild Card Mask گفتیم که این عدد برشکل Subnet Mask است و بعدازآن گفتیم که لازم نیست Wild Card Mask بنویسید، فقط به جای Wild Card Mask از چهار تا صفر استفاده کنید.

Router ID

نشان‌دهنده‌ی یک روتر در شبکه‌ی OSPF است که برای ارتباط روترها باهم در پروتکل OSPF از این شناسه استفاده می‌کنند. از این به بعد Router ID را خلاصه می‌کنیم و از کلمه‌ی RID استفاده می‌کنیم.

این ipها از بین ipهای یک روتر انتخاب می‌شوند که باید بزرگ‌ترین ip آدرس باشد. همان‌طور که می‌دانید این Interfaceها که ip روی آن‌ها قرار داده شده است به صورت فیزیکی می‌باشند و زمانی که Down شوند، بر روی کارکرد پروتکل OSPF تأثیرگذار هستند و باعث مشکل در شبکه می‌شوند. برای حل این مشکل باید از یک Interface مجازی استفاده کرد که هیچ وقت Down نمی‌شود، این اینترفیس، loopback است.

تذکر

اگر از چندین Loopback استفاده کنید، RID از بین آن‌هایی انتخاب می‌شود که بالاترین IP Address را دارند.

۶-۴ روترهای DR و BDR

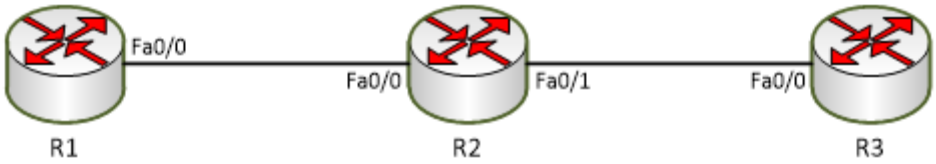
در شبکه‌های تحت OSPF، روتری تحت عنوان DR (Designated Router) وجود دارد که همه‌ی روترهای داخل یک Area، تمام اطلاعات و تغییرات را به این روتر می‌فرستند و این روتر به دیگر روترها اعلام می‌کند. یعنی اینکه هر روتر هر تغییری را به همه‌ی روترها ارسال نمی‌کند که باعث ایجاد بار سنگین در

www.takbook.com

شبکه شود، فقط اطلاعات خود را به روتر اصلی در شبکه، یعنی DR می‌فرستد و DR اطلاعات را پخش می‌کند، اما اگر این روتر از کار بیفتد، چه باید کرد؟ اگر این روتر down شود، روتری که BDR(BackBone Designated Router) است به جای این روتر کار می‌کند و تمام اطلاعات به این روتر ارسال می‌شود.

درصورتی‌که تغییری در شبکه OSPF رخ دهد، این تغییر از طریق LSU به روترهای DR و BDR فرستاده می‌شود، پس توجه داشته باشید که هر چه در روتر DR وجود دارد در روتر BDR هم وجود دارد.

روتر DR و BDR در هر Area وجود دارند، اما بین هر Subnet قرار دارند. به شکل ۹-۶ توجه کنید.



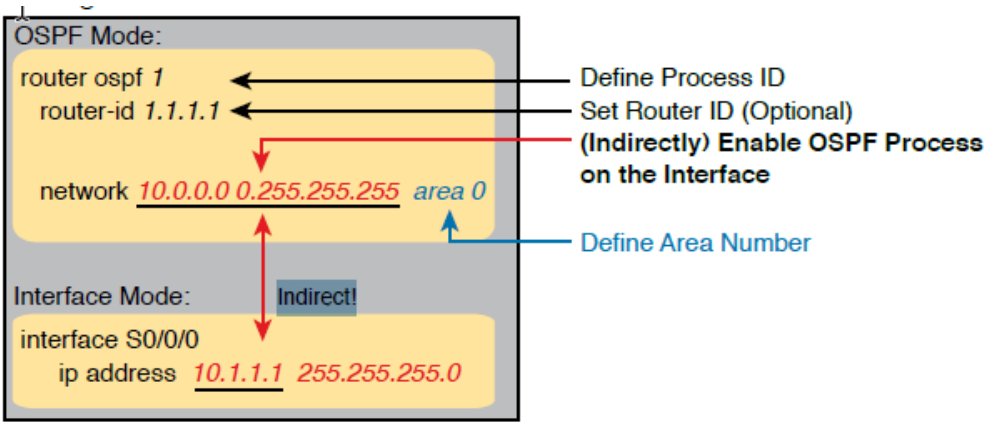
شکل ۹-۶ بررسی روتر DR و BDR

روترهای DR و BDR بین دو Subnet انتخاب می‌شوند، یعنی اینکه در شکل ۹-۶، بین روترهای R1 و R2 یک آدرس 172.16.1.0 وجود دارد که بین این دو روتر، روتری به عنوان DR انتخاب می‌شود که ip address بزرگ‌تری داشته باشد، البته یک فاکتور دیگر در انتخاب روترهای DR و BDR وجود دارد که خیلی مهم‌تر از بقیه‌ی فاکتورها است و آن هم، Priority است که اگر Priority یک روتر از روتر دیگر بزرگ‌تر باشد، همان روتر به‌عنوان DR انتخاب می‌شود، اما به صورت پیش‌فرض Priority=1 است و به خاطر همین از ip address برای انتخاب روترهای DR وBDR استفاده می‌کند.

در شکل ۱۰-۶، یک نمای کلی از پروتکل OSPF را مشاهده می‌کنید که برای تعریف در شبکه می‌توانید از آن استفاده کنید.

در قسمت Network دستور به صورت 10.0.0.0 0.255.255.255 وارد شده است که در قسمت پائین شکل آدرسی که در پورت مورت نظر وارد شده است را مشاهده می‌کنید و می‌توانید تفاوت آن را درک کنید.

www.takbook.com

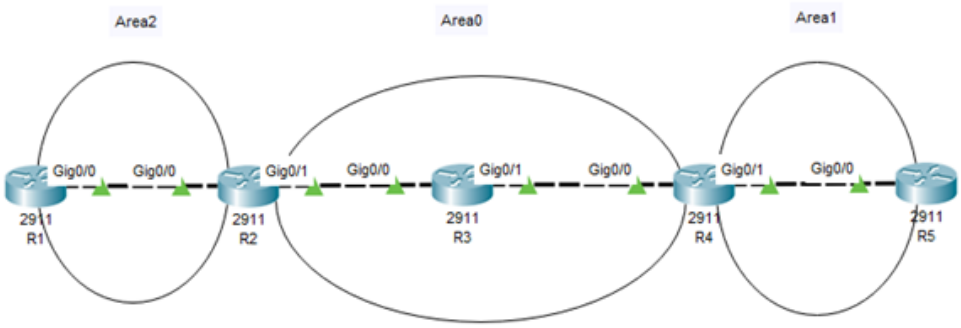


شکل ۱۰-۶ بررسی OSPF

مثال:

در این مثال، نحوه‌ی راه‌اندازی پروتکل OSPF را باهم کار می‌کنیم.

پنج روتر را به لیست اضافه کنید و به صورت زیر به هم متصل کنید.



شکل ۱۱-۶ راه‌اندازی پروتکل OSPF

جدول ۱-۶ آدرس پورت‌ها

	GIG 0/0	GIG 0/1	LoopBack
R1	172.16.1.1/16		150.1.1.1/24
R2	172.16.1.2/16	172.16.2.1/16	150.1.2.2/24
R3	172.16.2.2/16	172.16.3.1/16	150.1.3.3/24
R4	172.16.3.2/16	172.16.4.1/16	150.1.4.4/24
R5	172.16.4.2/16		150.1.5.5/24

www.takbook.com

طبق جدول ۱-۶، آدرس IP را بر روی Interfaceهای روترها Set کنید، بعد از این کار Ping بین روترها را تست بگیرد تا فعال و بدون مشکل باشد و بعد از آن پروتکل OSPF را روی آنها فعال می‌کنیم.

روتر R1:

Router(config)#**router ospf 20**

تعریف Router OSPF 20 که ۲۰ یک شماره‌ی شناسایی برای این پروتکل است که تأثیری در روند کار ندارد ولی باید تعریف شود، می‌توانید یک شماره دلخواه از ۱ تا ۶۵۵۳۵ تعریف کنید

Router(config-router)#**router-id 150.1.1.1**

در این قسمت باید RID روتر را تعریف کنید که این IP مربوط به اینترفیس LoopBack است، پس بعد از ورود به پروتکل OSPF در درجه‌ی اول RID را تعریف کنید.

Router(config-router)#**network 172.16.1.1 0.0.0.0 area 2**

در این قسمت Networkهای مربوط به روتر را تعریف می‌کنیم و می‌گوییم که در کدام area قرار دارد، مثلاً در این قسمت، اینترفیس GIG 0/0 روتر R1 در Area2 قرار دارد. در تعریف Network، اول خود Ip و بعد،Wild Card MASk مربوط به آن را وارد می‌کنیم که همان‌طور که در مطالب قبلی کتاب گفتیم، سعی کنید به جای Wild Card Mask از چهار صفر استفاده کنید (0.0.0.0).

در بقیه‌ی روترها هم همین کار را انجام دهید:

روتر R2:

Router(config)#**router ospf 10**
Router(config-router)#**router-id 150.1.2.2**
Router(config-router)#**network 172.16.1.2 0.0.0.0 area 2**
Router(config-router)#**network 172.16.2.1 0.0.0.0 area 0**

روتر R3:

Router(config)#**router ospf 10**
Router(config-router)#**router-id 150.1.3.3**
Router(config-router)#**net 172.16.2.2 0.0.0.0 area 0**
Router(config-router)#**net 172.16.3.1 0.0.0.0 area 0**

روتر R4:

Router(config)#router ospf 30
Router(config-router)#router-id 150.1.4.4
Router(config-router)#net 172.16.3.2 0.0.0.0 area 0
Router(config-router)#net 172.16.4.1 0.0.0.0 area 1

روتر R5:

Router(config)#router ospf 30
Router(config-router)#router-id 150.1.5.5

www.takbook.com

Router(config-router)#net 172.16.4.2 0.0.0.0 area 1

برای اینکه متوجه شوید پروتکل OSPF بر روی روتر فعال شده است می‌توانید از دستور زیر استفاده کنید، در این دستور Router ID، شماره‌ی OSPF و دیگر اطلاعات را می‌توانید مشاهده کنید.

Router#**show ip protocols**

```
Routing Protocol is "ospf 10"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 150.1.3.3
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    172.16.3.1 0.0.0.0 area 0
    172.16.2.2 0.0.0.0 area 0
  Routing Information Sources:
    Gateway         Distance      Last Update
    150.1.2.2         110      00:23:16
    150.1.3.3         110      00:22:25
    150.1.4.4         110      00:18:26
  Distance: (default is 110)
```

در این قسمت، از طریق فرمان Show Ip Route، نگاهی به جدول روتینگ روتر R1 می‌اندازیم و این دستور را در مد Privileged وارد می‌کنیم:

Router#**show Ip route**

```
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     150.1.0.0/24 is subnetted, 1 subnets
C       150.1.1.0 is directly connected, Loopback0
     172.16.0.0/24 is subnetted, 4 subnets
C       172.16.1.0 is directly connected, FastEthernet0/0
O IA    172.16.2.0 [110/2] via 172.16.1.2, 00:14:31, GigabiteEthernet0/0
O IA    172.16.3.0 [110/3] via 172.16.1.2, 00:11:56, GigabiteEthernet0/0
O IA    172.16.4.0 [110/4] via 172.16.1.2, 00:08:42, GigabiteEthernet0/0
Router(config)#
```

www.takbook.com

همان‌طور که مشاهده می‌کنید، Networkهایی که از طریق OSPF یاد گرفته است به صورت O IA نمایش داده است که O IA، بیانگر OSPF inter area است و نشان‌دهنده‌ی این است که این شبکه را از Area دیگری غیر از area خود یاد گرفته است و اگر یک روتر در area خود چیزی یاد بگیرد، آن را با حرف O ثبت می‌کند، اگر در روتر R2 دستور show ip route را اجرا کنید فقط کلمه‌ی O را در لیست مشاهده می‌کنید

```
Router#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     150.1.0.0/16 is variably subnetted, 2 subnets, 2 masks
C       150.1.2.0/24 is directly connected, Loopback0
L       150.1.2.2/32 is directly connected, Loopback0
     172.16.0.0/16 is variably subnetted, 6 subnets, 2 masks
C       172.16.1.0/24 is directly connected, GigabitEthernet0/0
L       172.16.1.2/32 is directly connected, GigabitEthernet0/0
C       172.16.2.0/24 is directly connected, GigabitEthernet0/1
L       172.16.2.1/32 is directly connected, GigabitEthernet0/1
O       172.16.3.0/24 [110/2] via 172.16.2.2, 00:19:11, GigabitEthernet0/1
O       172.16.4.0/24 [110/3] via 172.16.2.2, 00:15:14, GigabitEthernet0/1
```

توجه داشته باششید که تمام دستوراتی که در مد Privileged اجرا می‌شوند، در مد Global هم اجرا می‌شوند، اما این کار باید از طریق اضافه کردن کلمه‌ی do به اول دستور انجام شود. به مثال زیر توجه کنید.

```
Router(config)#do sh ip int b
Interface              IP-Address      OK? Method Status              Protocol
FastEthernet0/0        172.16.2.2      YES manual up                  up
FastEthernet0/1        172.16.3.1      YES manual up                  up
Loopback0              150.1.3.3       YES manual up                  up
Vlan1                  unassigned      YES unset  administratively down down
```

همان‌طور که مشاهده می‌کنید، دستور **Show Ip Inerface Brief** را هم به صورت کوتاه شده و هم در مد Global با اضافه کردن کلمه‌ی do اجرا کردیم، پس همیشه کلمه‌ی do یادتان باشد و سعی کنید از این کلمه استفاده کنید تا سرعت کار بالا رود.

کلمه‌ی do را زمانی استفاده می‌کنیم که بخواهیم دستوراتی که در مد Privileged اجرا می‌شوند را در مد بالاتر، یعنی Global استفاده کنیم، مانند دستور Ping که در مد Global اجرا نمی‌شود، اما اگر در اول این دستور، کلمه‌ی do قرار گیرد، اجرا می‌شود.

www.takbook.com

دستور Show IP OSPF Database

این دستور را در روتر R3 و در مد Global با اضافه کردن کلمه‌ی do اجرا کنید؛ که شکل۱۲-۶ مشخص کننده‌ی این موضوع است.

```
Router(config)#do sh ip ospf database
            OSPF Router with ID (150.1.3.3) (Process ID 10)

                Router Link States (Area 0)

Link ID         ADV Router      Age         Seq#       Checksum Link count
150.1.4.4       150.1.4.4       409         0x80000003 0x00355a 1
150.1.3.3       150.1.3.3       409         0x80000005 0x00946d 2
150.1.2.2       150.1.2.2       409         0x80000002 0x005744 1

                Net Link States (Area 0)
Link ID         ADV Router      Age         Seq#       Checksum
172.16.3.2      150.1.4.4       409         0x80000001 0x005a26
172.16.2.2      150.1.3.3       409         0x80000001 0x00f586

                Summary Net Link States (Area 0)
Link ID         ADV Router      Age         Seq#       Checksum
172.16.1.0      150.1.2.2       404         0x80000001 0x00956f
172.16.4.0      150.1.4.4       399         0x80000001 0x005ba2
```

در این قسمت RID هایی که داخل یک area شرکت دارند، نمایش داده می‌شود.

شبکه‌های روترهای مجاور که به صورت مستقیم به روتر R3 متصل هستند.

شبکه‌هایی که از Areaهای دیگر وارد این area شده‌اند.

شکل ۱۲-۶ بررسی Database مربوط به OSPF

دستور show ip ospf interface

این دستور، interfaceهای فعال در پروتکل OSPF را نمایش می‌دهد. در روتر R2 این دستور را اجرا می‌کنیم:

```
Router#show ip ospf interface
GigabitEthernet0/1 is up, line protocol is up
  Internet address is 172.16.3.1/24, Area 0
  Process ID 10, Router ID 150.1.3.3, Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 150.1.3.3, Interface address 172.16.3.1
  Backup Designated Router (ID) 150.1.4.4, Interface address 172.16.3.2
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:01
  Index 1/1, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 150.1.4.4  (Backup Designated Router)
  Suppress hello for 0 neighbor(s)
GigabitEthernet0/0 is up, line protocol is up
```

www.takbook.com


```
Internet address is 172.16.2.2/24, Area 0
Process ID 10, Router ID 150.1.3.3, Network Type BROADCAST, Cost: 1
Transmit Delay is 1 sec, State BDR, Priority 1
Designated Router (ID) 150.1.2.2, Interface address 172.16.2.1
Backup Designated Router (ID) 150.1.3.3, Interface address 172.16.2.2
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
  Hello due in 00:00:07
Index 2/2, flood queue length 0
Next 0x0(0)/0x0(0)
Last flood scan length is 1, maximum is 1
Last flood scan time is 0 msec, maximum is 0 msec
Neighbor Count is 1, Adjacent neighbor count is 1
  Adjacent with neighbor 150.1.2.2  (Designated Router)
 Suppress hello for 0 neighbor(s)
```

دستور Show ip ospf neighbor

```
Router#show ip ospf ne

Neighbor ID     Pri   State           Dead Time   Address         Interface
150.1.2.2         1   FULL/DR         00:00:39    172.16.2.1      GigabitEthernet0/0
150.1.4.4         1   FULL/BDR        00:00:37    172.16.3.2      GigabitEthernet0/1
```

شکل ۱۳-۶ اجرای دستور show ip ospf neighbor

با این دستور می‌توانید، DR یا BDR بودن روترهای همسایه را مشاهده کنید. همان‌طور که در شکل ۶-۱۳، مشاهده می‌کنید این دستور در روتر R3 اجرا شده و در نتیجه‌ی آن به ما RID روترهای همسایه را نشان داده است و مشخص کرده است که روتر R2 به عنوان DR و روتر R4 به عنوان BDR انتخاب شده است.

دستور show ip ospf border-routers

```
Router#show ip ospf border-routers
OSPF Process 10 internal Routing Table

Codes: i - Intra-area route, I - Inter-area route

i 150.1.4.4 [1] via 172.16.3.2, GigabitEthernet0/1, ABR, Area 0, SPF 1
i 150.1.2.2 [1] via 172.16.2.1, GigabitEthernet0/0, ABR, Area 0, SPF 1
```

شکل ۱۴-۶ اجرای دستور show ip ospf neighbor

به شکل ۶-۱۴ توجه کنید، این دستور، روترهای همسایه را به ما نشان می‌دهد و Ip address آن‌ها را مشخص می‌کند، و همچنین مشخص می‌کند که ار طریق کدام Interface اطلاعات روتر مورد نظر را یاد گرفته است.

www.takbook.com

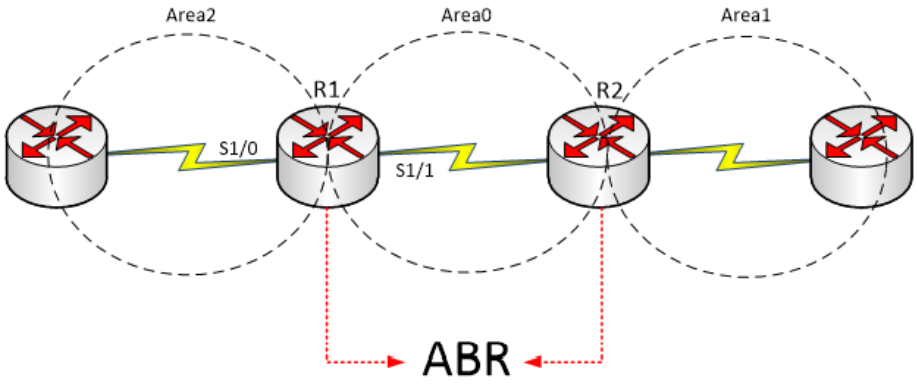
توجه داشته باشید، دستوراتی هستند که در Packet Tracer قابل اجرا نیستند و باید در IOsهای واقعی اجرا شوند، یعنی در نرم‌افزارهایی مانند GNS3 و یا خود دستگاه به صورت فیزیکی، مثلاً دستور شکل ۶-۱۵ در Packet Tracer اجرا نمی‌شود:

```
R1# show ip ospf interface brief
Interface      PID   Area          IP Address/Mask    Cost  State Nbrs F/C
Gi0/0/0        1     0             10.1.12.1/24       1     BDR   1/1
Gi0/1/0        1     0             10.1.13.1/24       1     BDR   1/1
Gi0/2/0        1     0             10.1.14.1/24       1     DR    1/1
Gi0/0.2        1     0             10.1.2.1/24        1     DR    0/0
Gi0/0.1        1     0             10.1.1.1/24        1     DR    0/0
```

شکل ۶-۱۵ اجرای دستور show ip ospf Interface brief

روتر ABR (Area Border Router)

به روتری می‌گویند که بین دو Area قرار دارد و کار انتقال اطلاعات از یک area به area دیگر را بر عهده دارد. به شکل ۶-۱۶، توجه کنید.



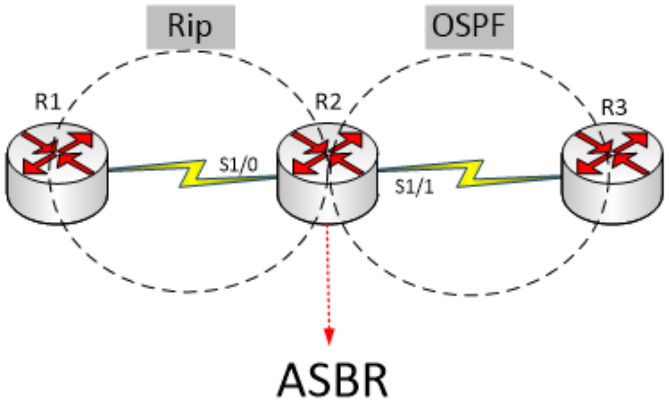
شکل ۶-۱۶ بررسی روتر ABR

همان‌طور که در شکل ۶-۱۶ مشاهده می‌کنید، روترهای R1 و R2 روترهایی هستند که بین دو area قرار دارند و کار انتقال را انجام می‌دهند که به این روترها، روترهای ABR گفته می‌شود.

روتر ASBR (Autonomous System Border Router)

این روتر کار انتقال اطلاعات از یک پروتکل یا یک دومین دیگر به داخل OSPF را انجام می‌دهد. به شکل ۶-۱۷، توجه کنید.

www.takbook.com



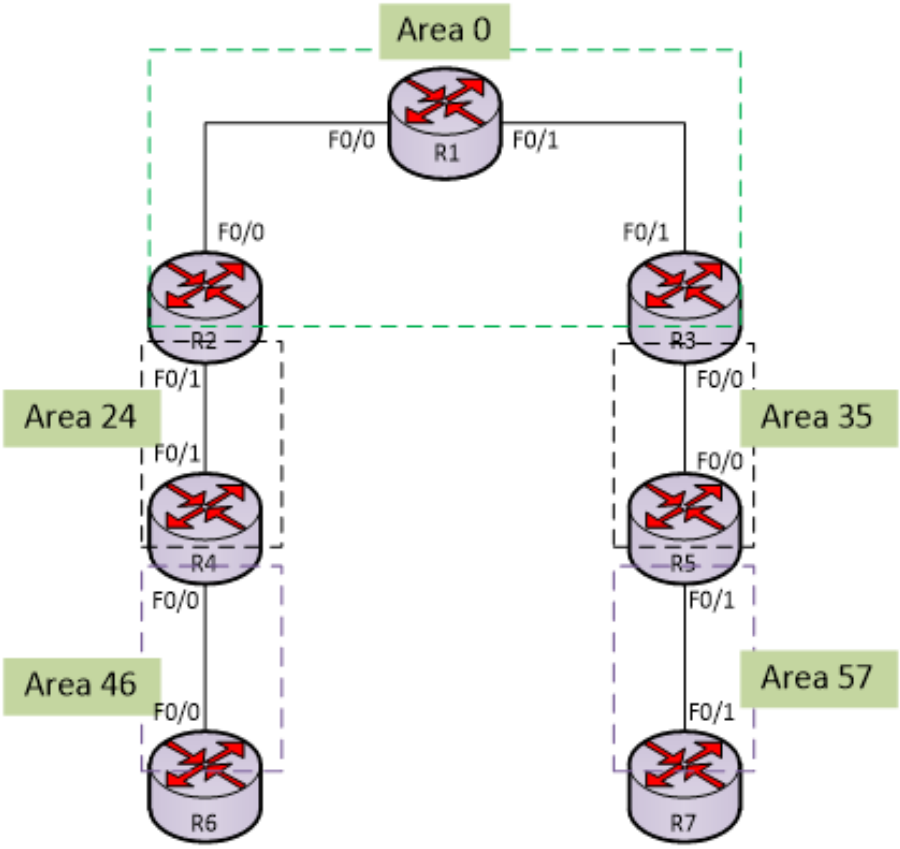
شکل ۱۷-۶ بررسی روتر ASBR

در شکل ۱۷-۶، روتر R2 که بین دو پروتکل قرار دارد و کار ترجمه یا Redistribute را انجام می‌دهد به عنوان روتر ASBR شناخته می‌شود.

۵-۶ کار با Virtual Link در OSPF

همان‌طور که قبلاً بیان کردیم، تمام Areaها باید به Area 0 متصل باشند تا بتوانند اطلاعات خود را انتقال دهند. اگر این Areaها به صورت مستقیم، مانند شکل ۱۸-۶، به Area 0 متصل نباشند، نمی‌توانند داده‌ها را انتقال دهند. برای درک این موضوع یک مثال را باهم بررسی می‌کنیم.

www.takbook.com



شکل ۱۸-۶ مثالی از Virtual Link

در این مثال، Areaهای 46 و 57 نمی‌توانند اطلاعات خود را در شبکه ارسال کنند، به این علت که به Area 0 متصل نیستند. برای حل این مشکل از Area 24,35 که بین این دو Area قرار دارد، کمک می‌گیریم و یک لینک مجازی بین Areaها ایجاد می‌کنیم. برای این کار باید وارد روترهای مرزی شویم که در این مثال برای متصل شدن Area46 به Area0 از روترهای R4 و R2 کمک می‌گیریم و Virtual Link را روی این دو فعال می‌کنیم تا یک پل از Area46 به Area0 زده باشیم.

جدول ip address به صورت زیر است:

جدول ۲-۶ آدرس پورت‌ها

Router	F0/0	F0/1	LoopBack
R1	1.1.12.1/24	1.1.13.1/24	100.1.1.1/24
R2	1.1.12.2/24	1.1.24.2/24	100.2.2.2/24
R3	1.1.35.3/24	1.1.13.3/24	100.3.3.3/24
R4	1.1.46.4/24	1.1.24.4/24	100.4.4.4/24
R5	1.1.35.5/24	1.1.57.5/24	100.5.5.5/24
R6	1.1.46.6/24	…	100.6.6.6/24

www.takbook.com

R7	…	1.1.57.7/24	100.7.7.7/24

بعد از واردکردن IP address در روترها باید پروتکل OSPF را روی تک‌تک روترها فعال کنیم؛
وارد روتر R1 شوید و دستورات زیر را وارد کنید:

```
Router(config)#router ospf 1
Router(config-router)#router-id 100.1.1.1
Router(config-router)#network 1.1.12.1 0.0.0.0 area 0
Router(config-router)#network 1.1.13.1 0.0.0.0 area 0
```

همان‌طور که مشاهده می‌کنید، پروتکل OSPF را روی این روتر فعال و شبکه‌های مربوط به آن را معرفی کردیم در بقیه‌ی روترها هم به صورت زیر عمل می‌کنیم:
وارد روتر R2 شوید و دستورات زیر را وارد کنید:

```
Router(config)#router ospf 1
Router(config-router)#router-id 100.2.2.2
Router(config-router)#network 1.1.12.2 0.0.0.0 area 0
Router(config-router)#network 1.1.24.2 0.0.0.0 area 24
```

وارد روتر R3 شوید و دستورات زیر را وارد کنید:

```
Router(config)#router ospf 1
Router(config-router)#router-id 100.3.3.3
Router(config-router)#network 1.1.13.3 0.0.0.0 area 0
Router(config-router)#network 1.1.35.3 0.0.0.0 area 35
```

وارد روتر R4 شوید و دستورات زیر را وارد کنید:

```
Router(config)#router ospf 1
Router(config-router)#router-id 100.4.4.4
Router(config-router)#network 1.1.24.4 0.0.0.0 area 24
Router(config-router)#network 1.1.46.4 0.0.0.0 area 46
```

وارد روتر R5 شوید و دستورات زیر را وارد کنید:

```
Router(config)#router ospf 1
Router(config-router)#router-id 100.5.5.5
Router(config-router)#network 1.1.35.5 0.0.0.0 area 35
Router(config-router)#network 1.1.57.5 0.0.0.0 area 57
```

وارد روتر R6 شوید و دستورات زیر را وارد کنید:

```
Router(config)#router ospf 1
Router(config-router)#router-id 100.6.6.6
Router(config-router)#network 1.1.46.6 0.0.0.0 area 46
```

www.takbook.com

وارد روتر R7 شوید و دستورات زیر را وارد کنید:

```
Router(config)#router ospf 1
Router(config-router)#router-id 100.7.7.7
Router(config-router)#network 1.1.57.7 0.0.0.0 area 57
```

بعد از اتمام کار، اگر وارد روتر R6 و R7 شوید و دستور **Show Ip Route** را وارد کنید، متوجه می‌شوید هیچ شبکه‌ای را از طریق OSPF یاد نگرفته است.

```
Router#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     1.0.0.0/24 is subnetted, 1 subnets
C       1.1.46.0 is directly connected, FastEthernet0/0
```

همان‌طور که مشاهده می‌کنید، هیچ شبکه‌ای را از طریق پروتکل OSPF یاد نگرفته است، به خاطر این‌که Area 46 و Area 57 به Area 0 متصل نیستند. برای حل این مشکل، یک پل به Area0 می‌زنیم.

ایجاد Virtual Link

برای ایجاد این لینک، باید وارد روترهای R2 و R4 و روترهای R3 و R5 شوید و دستور ساخت Virtual Link را وارد کنید:

وارد روتر R2 شوید و دستور زیر را وارد کنید:

```
Router(config)#router ospf 1
Router(config-router)#area 24 virtual-link 100.4.4.4
```

همان‌طور که مشاهده می‌کنید، اول وارد OSPF 1 شدیم که قبلاً ایجاد کردیم و بعد با دستور area 0 virtual-link 100.4.4.4 به روتر گفتیم که یک Virtual Link برای ارتباط با روتر روبرو که مرز بین Aera دیگر است ایجاد کند، این کار را باید در طرف دیگر هم انجام دهیم، یعنی روتر R4.

وارد روتر R4 شوید و دستور زیر را وارد کنید:

```
Router(config)#router ospf 1
Router(config-router)# area 24 virtual-link 100.2.2.2
```

www.takbook.com

بعد از این‌که در روتر R4 هم این دستور را وارد کردید، ارتباط بین Area 46 و Area0 توسط این لینک برقرار می‌شود. برای درک این موضوع وارد روتر R6 شوید و دستور Show IP Route را وارد کنید:

```
Router# show Ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
     D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
     N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
     E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
     i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
     * - candidate default, U - per-user static route, o - ODR
     P - periodic downloaded static route

Gateway of last resort is not set

    1.0.0.0/24 is subnetted, 5 subnets
O IA    1.1.12.0 [110/3] via 1.1.46.4, 00:00:56, FastEthernet0/0
O IA    1.1.13.0 [110/4] via 1.1.46.4, 00:00:56, FastEthernet0/0
O IA    1.1.35.0 [110/5] via 1.1.46.4, 00:00:56, FastEthernet0/0
C       1.1.46.0 is directly connected, FastEthernet0/0
O IA    1.1.57.0 [110/6] via 1.1.46.4, 00:00:56, FastEthernet0/0
```

روترR6 تمام آدرس‌های شبکه را از طریق OSPF یاد گرفته است. در ادامه باید همین کار را در طرف دیگر وارد کنید، یعنی بین روترهای R3 و R5:

وارد روتر R3 شوید و دستور زیر را وارد کنید:

```
Router(config)#router ospf 1
Router(config-router)#area 35 virtual-link 100.5.5.5
```

وارد روتر R5 شوید و دستور زیر را وارد کنید:

```
Router(config)#router ospf 1
Router(config-router)#area 35 virtual-link 100.3.3.3
```

بعد از اتمام کار، تمام روترها در شبکه قابل شناسایی هستند و می‌توانند همدیگر را ببینند.

۶-۶ بررسی Passive Interfaces در OSPF

یکی از راه‌های که می‌توانید بار کاری بر روی روتر را سبک‌تر کنید این است که بر روی یک Inteeface که نیاز نیست در یک شبکه مانند OSPF فعالیت کند بهتر است قابلیت Hello Packet آن را غیرفعال کنید، که برای این کار باید مثلاً در سناریو قبلی وارد R1 شوید و دستورات زیر را وارد کنید:

```
Router(config)#router ospf 10
Router(config-router)#passive-interface gigabitEthernet 0/1
```

www.takbook.com

با اجرای دستور بالا در OSPF دیگر هیچ پکتی به gigabitEthernet 0/1 ارسال نخواهد شد، توجه داشته باشید اگر اکثر Interfaceهای یک روتر در شبکه شرکت ندارند می‌توانید با دستور زیر همه آنها را غیرفعال و فقط Interfaceهای مورد نظر خود را فعال کنید.

Router(config-router)#**passive-interface default**

بعد از اجرای دستور بالا همه پورت‌ها نمی‌توانند بسته‌ی Hello را دریافت کنند و برای حل این مشکل باید از دستور زیر استفاده کنید:

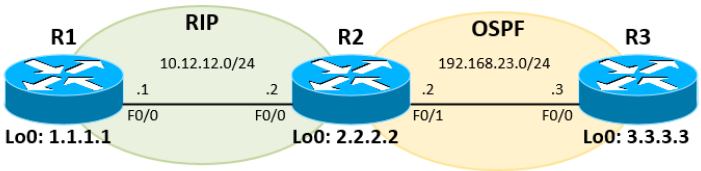
Router(config-router)#**no passive-interface gigabitEthernet 0/0**

۶-۷ بررسی دستور Redistribute

دو پروتکل مسیریابی RIP و OSPF را با هم بررسی کردیم، اگر چنانچه در یک شبکه از هر دو پروتکل استفاده شود، چطوری می‌توان این دو پروتکل را به هم متصل کرد تا بتوانند همدیگر را ببینند؟ برای انجام این کارباید از دستور Redistribute برای ترجمه‌ی دو پروتکل و انتقال اطلاعات به همدیگر استفاده کرد.

برای اینکه با این دستور بیشتر آشنا شوید مثالی را با هم بررسی می‌کنیم.

طبق شکل ۱۹-۶، سه روتر به لیست اضافه کنید و IP آدرس را برای Interfaceهای مورد نظر و Loopback وارد کنید، توجه داشته باشید که بین روترهای R1 و R2 پروتکل RP و بین روترهای R2 و R3 پروتکل OSPF را راه‌اندازی کردیم.



شکل ۱۹-۶ مثالی از Redistribute

بعد از انجام تنظیمات اولیه و راه‌اندازی پروتکل OSPF و RIP وارد روتر R1 شوید و روتر R3 را با دستور زیر تست بگیرید:

```
R1#ping 3.3.3.3 sour 1.1.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 3.3.3.3, timeout is 2 seconds:
Packet sent with a source address of 1.1.1.1
.....
Success rate is 0 percent (0/5)
```

همانطور که در دستور بالا مشاهده می‌کنید، روتر R1 نتوانست روتر R3 را Ping کند.

در زیر تنظیمات انجام شده بر روی هر روتر را مشاهده می‌کنید:

www.takbook.com

در روتر R1 پروتکل RIP راه‌اندازی شده و شبکه‌های مربوط به آن تعریف شده است:

> **تذکر**
> در دستور زیر از علامت (|) استفاده شده است و این به خاطر ایجاد شرط است، یعنی در این دستور به جای اینکه تمام اطلاعات مربوط به فایل Running config را نمایش دهد، فقط اطلاعات مربوط به کلمه‌ی Router را نمایش می‌دهد، کلمه‌ی S هم اول کلمه‌ی Selection است.

```
R1#sh run | s router
router rip
 version 2
 network 1.0.0.0
 network 10.0.0.0
no auto-summary
```

در روتر R2 هر دو پروتکل تعریف شده و شبکه‌های مربوط به هر کدام هم تعریف شده است:

```
R2#sh run | s router
router ospf 1
 network 2.2.2.2 0.0.0.0 area 0
 network 192.168.23.2 0.0.0.0 area 0
router rip
 version 2
 network 10.0.0.0
 no auto-summary
```

در روتر R3 هم پروتکل OSPF را به همراه شبکه‌های آن تعریف می‌کنیم:

```
R3#sh run | s router
router ospf 1
 network 3.3.3.3 0.0.0.0 area 0
 network 192.168.23.3 0.0.0.0 area 0
```

خوب برای این دو پروتکل بتوانند همدیگر را ببینند باید به صورت زیر دستورات را در روتر R2 وارد کنید:

وارد پروتکل OSPF شوید و دستور redistribute rip subnets را وارد کنید.

```
R2(config)#router ospf 1
R2(config-router)#redistribute rip subnets
```

و برای پروتکل RIP هم دستور زیر را وارد کنید:

```
R2(config)#router rip
R2(config-router)#redistribute ospf 1 metric 12
```

همانطور که قبلاً گفتیم در پروتکل RIPباید Hop یا Metric که همان روترهای در سر راه است را مشخص کنیم، که برای اینکه این پروتکل به آسانی کار کنند این عدد را بر روی ۱۲ تنظیم کردیم.

www.takbook.com

در زیر اطلاعات جدول Routing را برای روتر R1 و R3 قبل از اعمال دستور Redistribute مشاهده می‌کنید:

در دستور زیر از حرف b استفاده شده که اول کلمه‌ی begin است، یعنی کلمه‌ای که با Gate شروع می‌شود.

```
R1#sh ip route | b Gate
Gateway of last resort is not set

is subnetted, 1 subnets ۳۲/۱.۰.۰.۰
C      1.1.1.1 is directly connected, Loopback0
is variably subnetted, 2 subnets, 2 masks ۸/۱۰.۰.۰.۰
C      10.12.12.0/24 is directly connected, FastEthernet0/0
L      10.12.12.1/32 is directly connected, FastEthernet0/0

R3#sh ip route | b Gate
Gateway of last resort is not set

is subnetted, 1 subnets ۳۲/۲.۰.۰.۰
O      2.2.2.2 [110/2] via 192.168.23.2, 00:02:14, FastEthernet0/0
is subnetted, 1 subnets ۳۲/۳.۰.۰.۰
C      3.3.3.3 is directly connected, Loopback0
is variably subnetted, 2 subnets, 2 masks ۲۴/۱۹۲.۱۶۸.۲۳.۰
C      192.168.23.0/24 is directly connected, FastEthernet0/0
L      192.168.23.3/32 is directly connected, FastEthernet0/0
```

بعد از انجام عملیات Redistribute فایل Running Config به صورت زیر تغییر خواهد کرد:

```
R1#sh ip route | b Gate
Gateway of last resort is not set

     1.0.0.0/32 is subnetted, 1 subnets
C      1.1.1.1 is directly connected, Loopback0
     2.0.0.0/32 is subnetted, 1 subnets
R      2.2.2.2 [120/12] via 10.12.12.2, 00:00:06, FastEthernet0/0
     3.0.0.0/32 is subnetted, 1 subnets
R      3.3.3.3 [120/12] via 10.12.12.2, 00:00:06, FastEthernet0/0
     10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C      10.12.12.0/24 is directly connected, FastEthernet0/0
L      10.12.12.1/32 is directly connected, FastEthernet0/0
R      192.168.23.0/24 [120/12] via 10.12.12.2, 00:00:06, FastEthernet0/0

R3#sh ip route | b Gate
Gateway of last resort is not set

     1.0.0.0/32 is subnetted, 1 subnets
O E2   1.1.1.1 [110/20] via 192.168.23.2, 00:00:17, FastEthernet0/0
     2.0.0.0/32 is subnetted, 1 subnets
O      2.2.2.2 [110/2] via 192.168.23.2, 00:02:47, FastEthernet0/0
     3.0.0.0/32 is subnetted, 1 subnets
C      3.3.3.3 is directly connected, Loopback0
     10.0.0.0/24 is subnetted, 1 subnets
```

www.takbook.com


```
O E2   10.12.12.0 [110/20] via 192.168.23.2, 00:00:17, FastEthernet0/0
    192.168.23.0/24 is variably subnetted, 2 subnets, 2 masks
C      192.168.23.0/24 is directly connected, FastEthernet0/0
L      192.168.23.3/32 is directly connected, FastEthernet0/0
```

خوب همانطور که در دستور بالا مشاهده می‌کنید تمام شبکه از طریق دو پروتکل به هم معرفی شده است و اگر دوباره دستور اول که برای Ping از R1 به R3 بود را انجام دهیم باید با موفقیت این کار انجام گیرد:

```
R1#ping 3.3.3.3 sour 1.1.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 3.3.3.3, timeout is 2 seconds:
Packet sent with a source address of 1.1.1.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 16/48/68 ms
```

۸-۶ سوالات فصل ششم

1. Which of the following routing protocols is considered to use link-state logic?
کدام یک از گزینه‌های زیر یک پروتکل link-state است؟

a. RIPv1
b. RIPv2
c. EIGRP
d. OSPF

2. Which of the following routing protocols use a metric that is, by default, at least partially affected by link bandwidth? (Choose two answers.)
کدام یک از پروتکل‌های زیر به صورت پیش‌فرض از Metric برای پهنای‌باند بهتر استفاده می‌کند؟ (دو گزینه را انتخاب کنید)

a. RIPv1
b. RIPv2
c. EIGRP
d. OSPF

www.takbook.com

3. Which of the following interior routing protocols support VLSM? (Choose three answers.)

کدام یک از پروتکل‌های زیر از VLSM پشتیبانی می‌کند؟ (سه گزینه را انتخاب کنید)

a. RIPv1
b. RIPv2
c. EIGRP
d. OSPF

4. Two routers using OSPFv2 have become neighbors and exchanged all LSAs. As a result, Router R1 now lists some OSPF-learned routes in its routing table. Which of the following best describes how R1 uses those recently learned LSAs to choose which IP routes to add to its IP routing table?

دو روتر با استفاده از OSPF با هم در ارتباط هستند، و به هم LSA ردوبدل می‌کنند، در نتیجه روتر R1 برخی از مسیرهای آموخته شده توسط پروتکل OSPF را در جدول مسیریابی خود ذخیره می‌کند، حالا سوالی که اینجا باید مطرح کرد این است که چگونه R1 باید بررسی کند که کدام مسیری که آموخته بهترین مسیر است؟

a. Each LSA lists a route to be copied to the routing table.
b. Some LSAs list a route that can be copied to the routing table.
c. Run some SPF math against the LSAs to calculate the routes.
d. R1 does not use the LSAs at all when choosing what routes to add.

5. Which of the following OSPF neighbor states is expected when the exchange of topology information is complete between two OSPF neighbors?

هنگامی که در OSPF بین دو روتر تبادل اطلاعات به صورت کامل انجام بگیرد، کدام یک از گزینه‌های زیر انتظار می‌رود؟

a. 2-way
b. Full
c. Up/up
d. Final

6. A company has a small/medium-sized network with 15 routers and 40 subnets and uses OSPFv2. Which of the following is considered an advantage of using a single-area design as opposed to a multiarea design?

یک شرکت با اندازه‌کوچک یا متوسط را در نظر بگیرید که دارای ۱۵ روتر و ۴۰ Subnet است که از OSPF استفاده می‌کند و نوع طراحی آن یک منطقه یا Single-area است و چند منطقه‌ای استفاده نشده است، بهترین دلیل آن به نظر شما چیست؟

a. It reduces the processing overhead on most routers.
b. Status changes to one link may not require SPF to run on all other routers.
c. It allows for simpler planning and operations.
d. It allows for route summarization, reducing the size of IP routing tables.

7. Routers R1 and R2, with router IDs 1.1.1.1 and 2.2.2.2, connect over an Ethernet WAN link. If using all default OSPF settings, if the WAN link initializes for both routers at the same time, which of the following answers are true? (Choose two answers.)

www.takbook.com

روترهای R1 و R2 ، با شناسه‌های(IDs) ۱.۱.۱.۱ و ۲.۲.۲.۲ ، از طریق لینک Ethernet WAN به هم متصل می‌شوند. اگر از همه تنظیمات پیش‌فرض OSPF استفاده کنید، اگر پیوند WAN همزمان برای هر دو روتر انجام شود ، کدام یک از پاسخ های زیر صحیح است؟ (دو گزینه را انتخاب کنید)

a. Router R1 will become the DR.
b. Router R1 will dynamically discover the existence of router R2.
c. Router R2 will be neither the DR nor the BDR.
d. Router R1's show ip ospf neighbor command will list R2 with a state of "FULL/DR".

8. An engineer connects routers R11 and R12 to the same Ethernet LAN and configures them to use OSPFv2. Which answers describe a combination of settings that would prevent the two routers from becoming OSPF neighbors? (Choose two answers.)

دو روتر R11 و R12 را در نظر بگیرید که از طریق LAN به هم متصل شده‌اند و روی آنها OSPFv2 پیکربندی شده است، کدام پاسخ از همسایه شدن این دو روتر جلوگیری می‌کند؟(دو گزینه را انتخاب کنید)

a. R11's interface uses area 11 while R12's interface uses area 12.
b. R11's OSPF process uses process ID 11 while R12 uses process ID 12.
c. R11's interface uses OSPF priority 11 while R12's uses OSPF priority 12.
d. R11's interface uses an OSPF Hello timer value of 11 while R12's uses 12.

www.takbook.com

www.takbook.com

فصل هفتم

نصب و راه اندازی GNS3

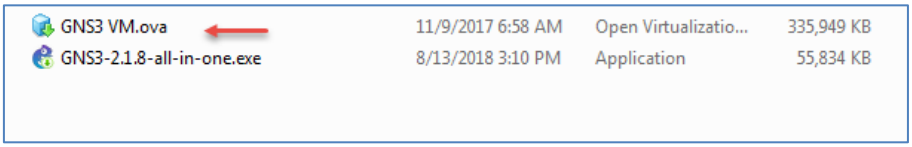
GNS3 یکی از بهترین نرم‌افزارهای مجازی سازی برای دستگاه‌های شبکه خصوصاً سیسکو است است که عملکرد خوبی را دارا است، یکی از مهمترین مشکلات GNS3 در گذشته در زمینه‌ی سوئیچ بوده که عملکرد ضعیفی داشته ولی با روی‌کار آمدن نرم‌افزار IOU این ضعف بر طرف شده و مشکلی از این لحاظ وجود ندارد، در این قسمت می‌خواهیم نحوه نصب و راه اندازی نرم‌افزار GNS3 را بررسی کنیم و IOU را به آن متصل کنیم.

برای شروع کار این دو نرم‌افزار را دانلود کنید:

GNS3 Installation
https://www.gns3.com/software/download GNS3 VMware Workstation

GNS3 VMware Workstation
https://www.gns3.com/software/download-vm

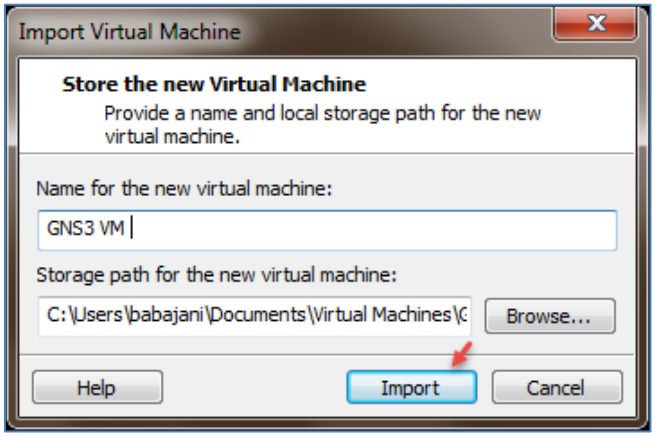
نصب GNS3 ساده بوده و نیاز به توضیح خاصی ندارد ولی فایل GNS3 VMware Workstation به صورت یک فایل فشرده با پسوند ova است به مانند شکل ۱-۷، با کلیک بر روی آن، ماشین مجازی آن بر روی نرم‌افزار VMware Workstation ایجاد خواهد شد، اگر با VMware کار نکردید می‌توانید کتاب آن را از سایت 3isco.ir دانلود و مطالعه کنید.



شکل ۱-۷ ماشین مجازی GNS3

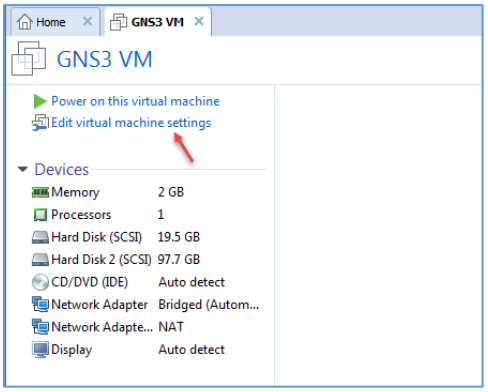
بعد از باز کردن فایل مورد نظر شکل ۲-۷، ظاهر خواهد شد که می‌توانید اسم و آدرس ذخیره شدن آن را تغییر دهید و بر روی کلید Import کلیک کنید تا ماشین مورد نظر ایجاد شود.

www.takbook.com



شکل ۲-۷ ایجاد ماشین GNS3

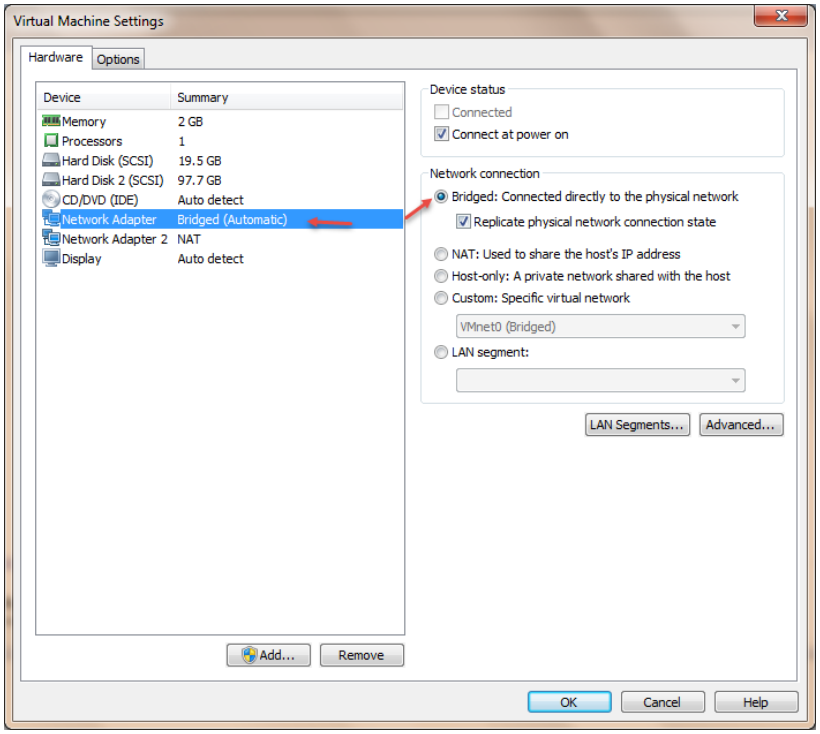
بعد از فعال شدن ماشین برای اینکه تنظیمات خود را بر روی آن اعمال کنید بر روی Edit virtual machine settings که در شکل ۳-۷ مشخص شده است کلیک کنید.



شکل ۳-۷ ایجاد ماشین GNS3

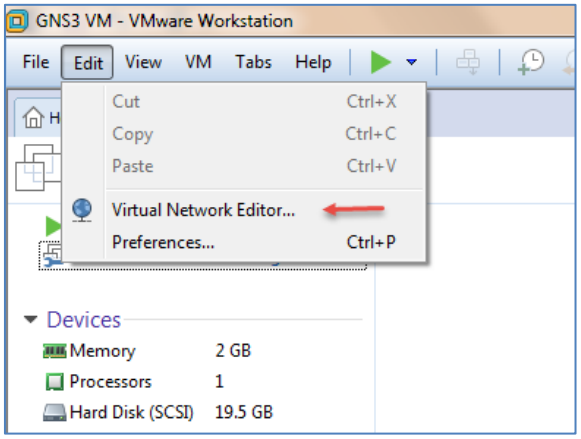
در شکل ۴-۷، می‌توانید مقدار رم و CPU ماشین مورد نظر را برای عملکرد بهتر تغییر دهید که به صورت پیش‌فرض ۲ گیگابایت رم و ۱ هسته CPU به آن اختصاص داده شده است که برای کار ما پاسخگو خواهد بود، در قسمت بعد کارت شبکه مورد نظر را انتخاب کنید و در صفحه باز شده تیک گزینه‌ی Bridged را انتخاب کنید تا این سرور بتواند به شبکه واقعی شما از طریق کارت شبکه اصلی متصل شود.

www.takbook.com



شکل ۴-۷ ایجاد ماشین GNS3

البته برای اینکه تنظیمات مربوط به کارت شبکه‌ها را در نرم‌افزار VMware بررسی کنید به مانند شکل ۵-۷، باید وارد منوی Edit شوید و گزینه‌ی virtual Network Editor را انتخاب کنید.



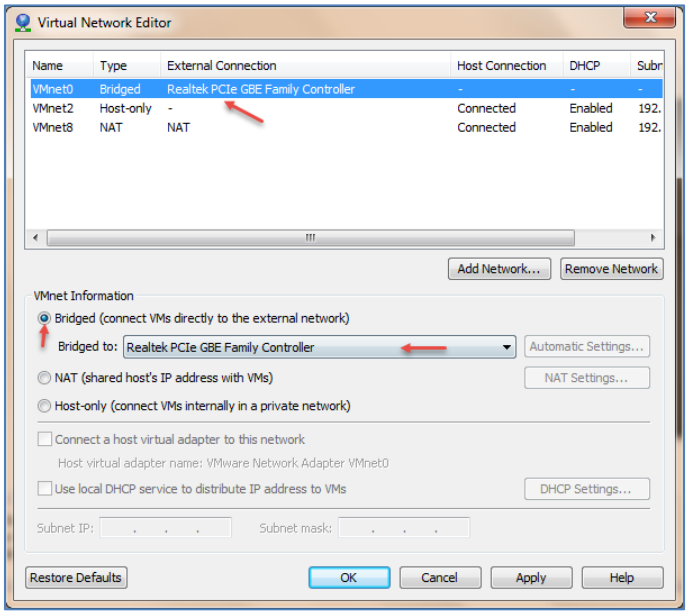
شکل ۵-۷ ایجاد ماشین GNS3

www.takbook.com

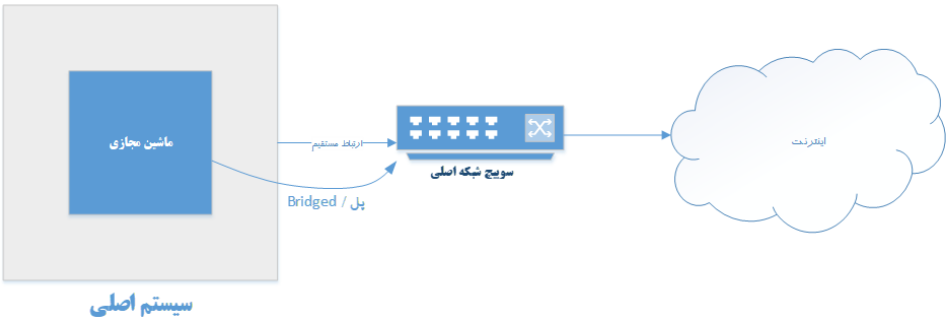
در شکل ۶-۷، باید کارت شبکه VMnet0 را انتخاب کنید و در پایین صفحه گزینه‌ی Bridged را انتخاب و کارت شبکه واقعی سیستم خود را که به شبکه اصلی شما متصل است انتخاب کنید و ب رروی OK کلیک کنید.

تذکر

شما می‌توانید یک شبکه مجازی داشته باشید و از کارت شبکه از نوع Host Only استفاده کنید و نیاز به کارهای بالا نیست.



شکل ۶-۷ ایجاد ماشین GNS3

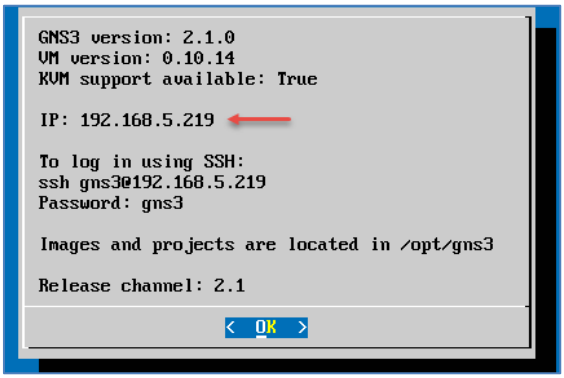


شکل ۷-۷ بررسی مفهوم Bridge

www.takbook.com

اگر به شکل ۷-۷، توجه کنید مفهوم Bridged را بهتر درک خواهید کرد، ماشین مجازی داخل یک سیستم فیزیکی اصلی است که از طریق کارت شبکه‌ای که آن سیستم به دنیای شبکه اصلی ما متصل است از طریق پل یا همان Bridged به شبکه اصلی متصل می‌شود و می‌تواند مثلاً آدرس IP را از سرویس DHCP دریافت کند.

بعد از روشن کرد ماشین و اجرا شدن آن شکل ۸-۷، برای شما ظاهر خواهد شد که اگر تنظیمات مربوط به کارت شبکه را به درستی انجام داده باشید، آدرس IP به آن اختصاص داده خواهد شد که در این شکل آدرس ۱۹۲.۱۶۸.۵.۲۱۹ به آن داده شده است، در قسمت زیر IP دستورات مربوط به متصل شدن با SSH مشخص شده است که نام کاربر یو رمز عبور آن GNS3 است که در ادامه با آن کار خواهیم کرد، تا اینجا توانستیم نرم‌افزار GNS3 را به همراه ماشین مجازی آن فعال کنیم در ادامه باید سوئیچ لایه دو و سه IOU را به GNS3 اضافه کنیم و از آن در این کتاب استفاده کنیم، پس باید به درستی مطالب بعد را انجام دهید تا مشکلی در این زمینه نداشته باشید.



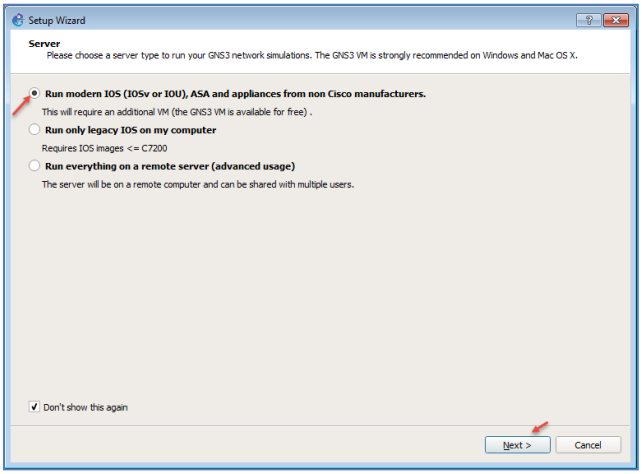
شکل ۸-۷ تنظیمات GNS3

نرم‌افزار GNS3 را اجرا کنید، بعد از اجرا شکل ۹-۷، ظاهر خواهد شد، در این قسمت گزینه‌ی اول را انتخاب و بر روی Next کلیک کنید.

تذکر

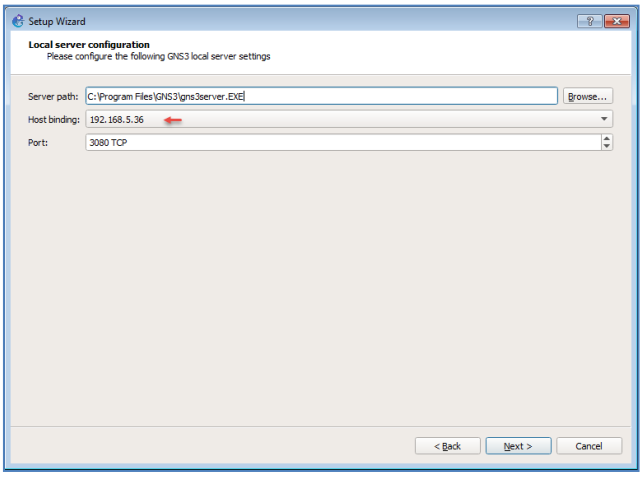
در بعضی موارد در این قسمت و در ادامه با خطاهای مختلف مواجه خواهید شد که این مشکل‌ها بر می‌گردید به تنظیمات آنتی ویروس و فایروال.

www.takbook.com



شکل ۹-۷ تنظیمات GNS3

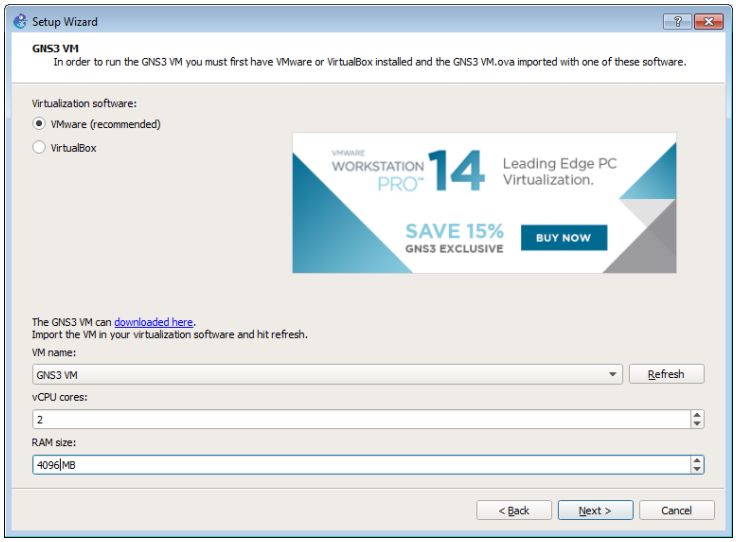
در شکل ۱۰-۷، باید آدرس سروری که نرم‌افزار GNS3 بر روی آن نصب شده است را مشخص کنید، توجه داشته باشید که پورت پیش‌فرض برای اتصال ۳۰۸۰ است.



شکل ۱۰-۷ تنظیمات GNS3

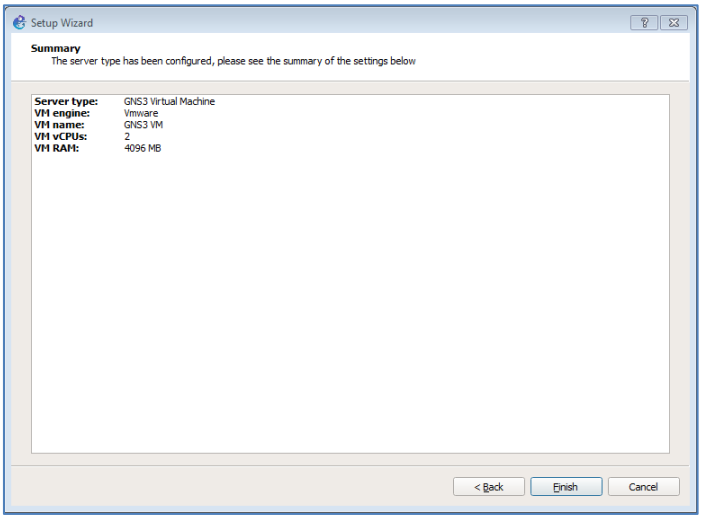
در شکل ۱۱-۷، اگر مراحل راه‌اندازی ماشین مجازی را در قسمت قبل انجام داده باشید این قسمت ماشین مورد نظر را به صورت خودکار شناسایی خواهد کرد، مقدار CPU و مقدار رم را مشخص کرده و بر روی Next کلیک کنید.

www.takbook.com



شکل ۱۱-۷ تنظیمات GNS3

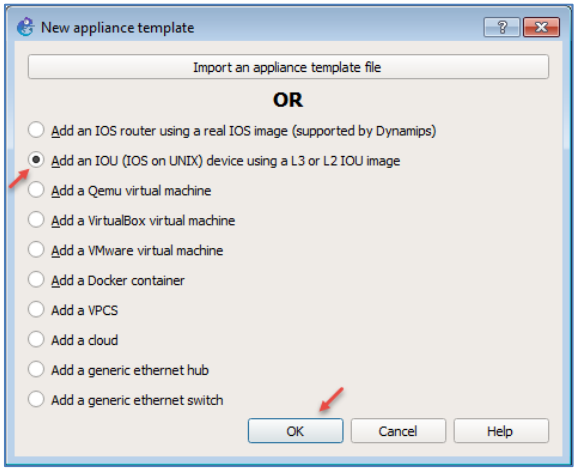
در شکل ۱۲-۷ به ماشین مجازی متصل شدیم و برای ادامه کار بر روی Finish کلیک کنید.



شکل ۱۲-۷ تنظیمات GNS3

بعد از کلیک بر روی Finish شکل ۱۳-۷، ظاهر خواهد شد که باید IOS مربوط به سوئیچ لایه دو و سه را به نرم‌افزار GNS3 اضافه کنیم، برای این کار گزینه‌ی ... Add an IOU را انتخاب کنید و بر روی OK کلیک کنید.

www.takbook.com



شکل ۱۳-۷ تنظیمات GNS3

برای استفاده از IOS مربوط به سوئیچ، دو فایل Image مربوط به سوئیچ لایه دو لایه سه را از لینک زیر دانلود کنید:

Switch L2 & L3:
https://drive.google.com/file/d/0B8tSmsEbVQs-bjVXY3VqMFJrc1E/view

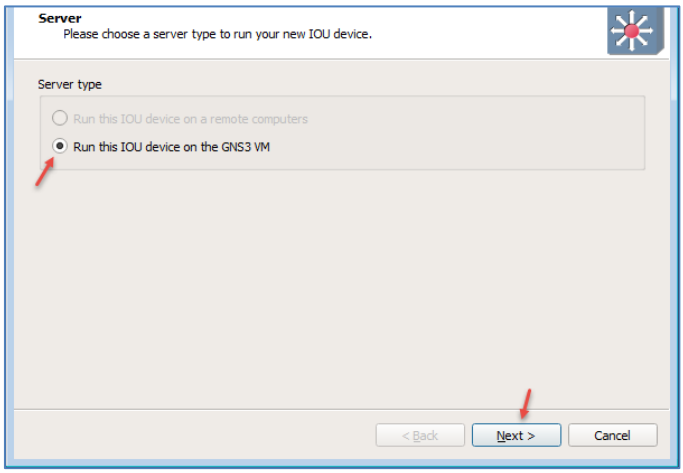
در دو لینک زیر هر دو نسخه‌ی سوئیچ را می‌توانید دانلود کنید:

http://3isco.ir/IOS-3isco.ir/i86bi-linux-l2-adventerprisek9-15.1a-3isco.ir.zip

http://3isco.ir/IOS-3isco.ir/i86bi-linux-l3-adventerprisek9-15.2.4M1-3isco.ir.zip

در شکل ۱۴-۷، گزینه‌ی GNS3 VM به صورت پیش‌فرض انتخاب شده است.

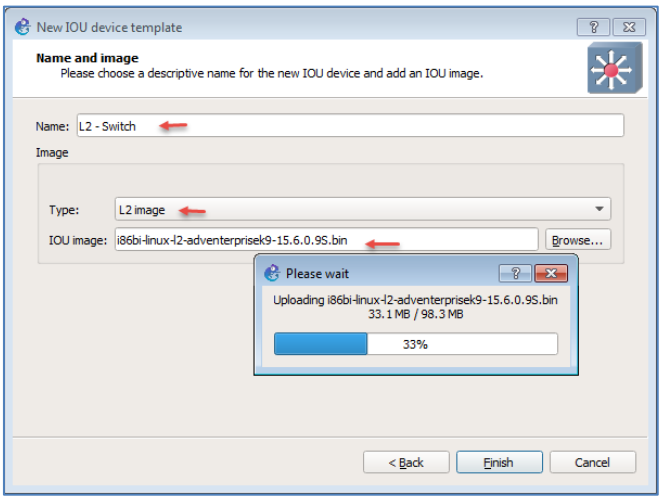
بر روی Next کلیک کنید.



شکل ۱۴-۷ تنظیمات GNS3

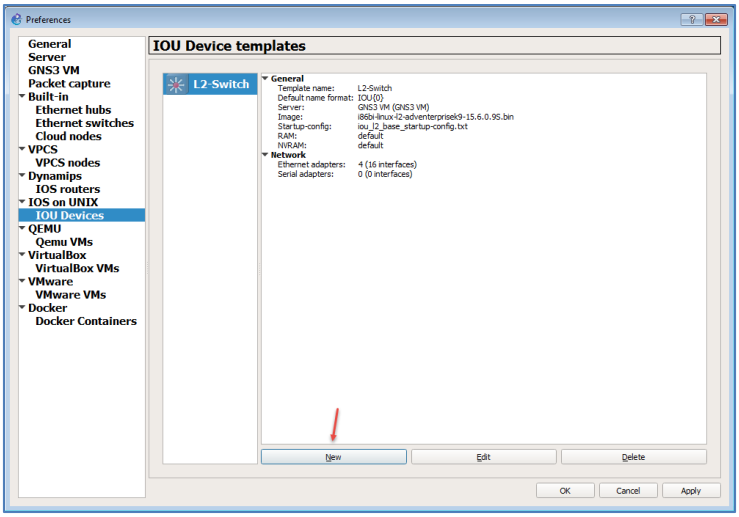
www.takbook.com

در شکل ۱۵-۷، باید دو فایلی که برای سوئیچ سیسکو بوده را به ماشین مجازی معرفی کنید، برای این کار برای سوئیچ لایه دو نام مورد نظر خود را وارد کنید، و در قسمت Type باید گزینه‌ی L2 image را انتخاب کنید و با کلیک بر روی Browse فایل IOS مربوط به آن را انتخاب کنید، با این کار فایل IOS در ماشین مجازی GNS3 آپلود خواهد شد.



شکل ۱۵-۷ تنظیمات GNS3

بعد از کلیک بر روی Finish به مانند شکل ۱۶-۷، سوئیچ لایه دو به لیست مورد نظر اضافه خواهد شد و برای اینکه سوئیچ لایه سه هم به لیست اضافه کنید باید بر روی New کلیک کنید.

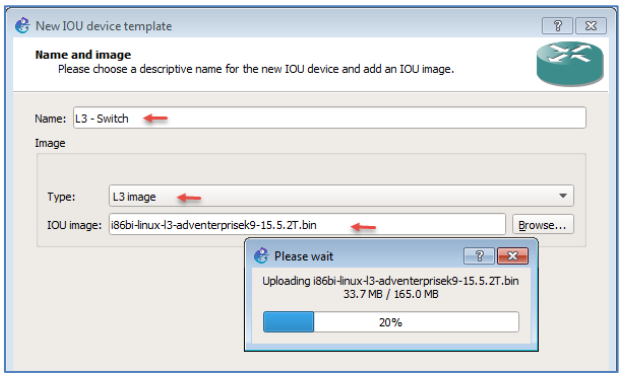


شکل ۱۶-۷ تنظیمات GNS3

www.takbook.com

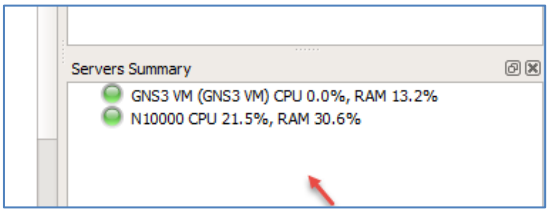
در این صفحه هم نام سوئیچ لایه سه را وارد و فایل IOS آن را به نرم‌افزار معرفی تا در ماشین مجازی آپلود شود.

بعد از اتمام کار به مانند شکل ۱۷-۷، بر روی Finish کلیک کنید.



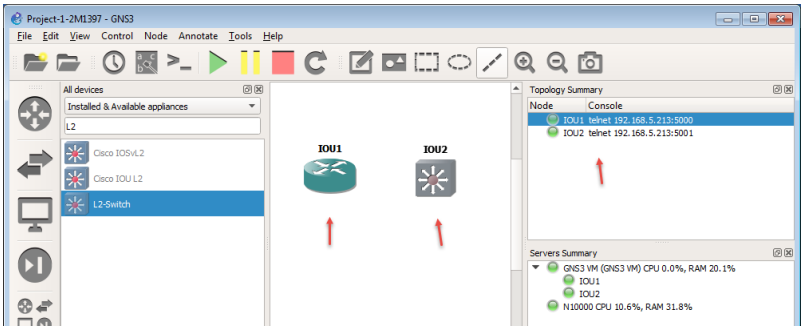
شکل ۱۷-۷ تنظیمات GNS3

با توجه به شکل اگر ۱۸-۷، در نرم‌افزار GNS3 به قسمت Servers Summary توجه کنید، هر دو سرور local و سرور مجازی را به همراه مانیتورینگ سخت‌افزاری آن مشاهده می‌کنید که این موضوع نشان دهنده فعال بودن آن‌ها است.



شکل ۱۸-۷ بررسی قسمت Servers Summary

بعد از اتمام مراحل بالا در قسمت Device به مانند شکل ۱۹-۷، سوئیچ مورد نظر خود را که با اسم مشخص شده ایجاد کردید جستجو کنید و آن را کشیده و در صفحه مورد نظر رها کنید و بعد آنها را روشن کنید، همانطور که مشاهده می‌کنید هر دو سوئیچ لایه دو و سه بدون مشکل روشن شده است.



شکل ۱۹-۷ کار با GNS3

www.takbook.com

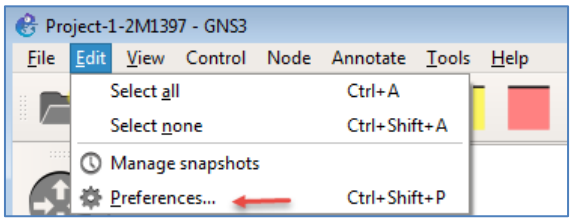
۷-۱ اضافه کردن IOS مربوط به روتر در GNS3

در قسمت قبلی توانستیم، ماشین مجازی راه‌اندازی کنیم و سوئیچ لایه دو و سه را به آن اضافه و به نرم‌افزار اصلی GNS3 اضافه کنیم که همانطور که گفتیم یکی از مشکلات عمده GNS3 در مبحث سوئیچینگ بوده که با این کار مشکلش حل شد و همه دستورات سوئیچ که در ادامه کار خواهیم کرد اجرا خواهد شد، در این قسمت باید IOS مربوط به روتر را هم به نرم‌افزار GNS3 اضافه کنیم، البته نیازی نیست آن را درون ماشین مجازی آپلود کنید، بلکه می‌توانید آن را درون خود نرم‌افزار اصلی آپلود کنید.

برای دانلود IOS 7200 cisco Router می‌توانید از لینک زیر است

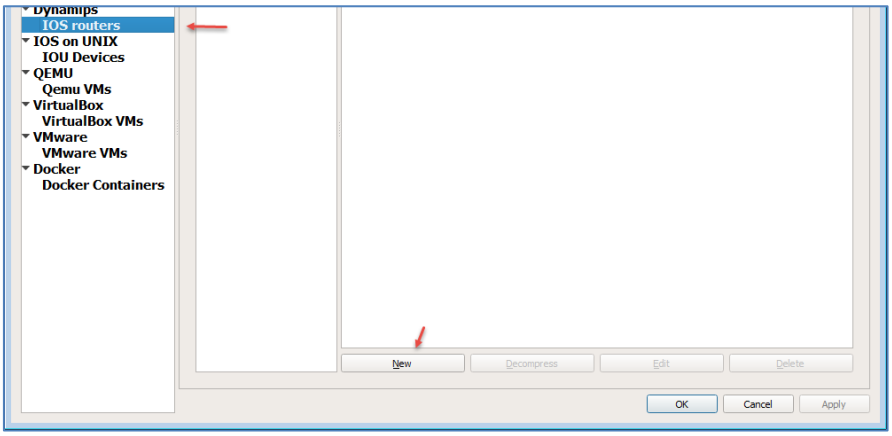
http://ipmanager.ir/r/CISCO/7200/c7200-adventerprisek9-mz.151-4.M.bin

بعد از دانلود IOS مربوط به روتر به مانند شکل ۷-۲۰ وارد منوی Edit شوید و بر روی گزینه‌ی Preferences کلیک کنید.



شکل ۷-۲۰ کار با GNS3

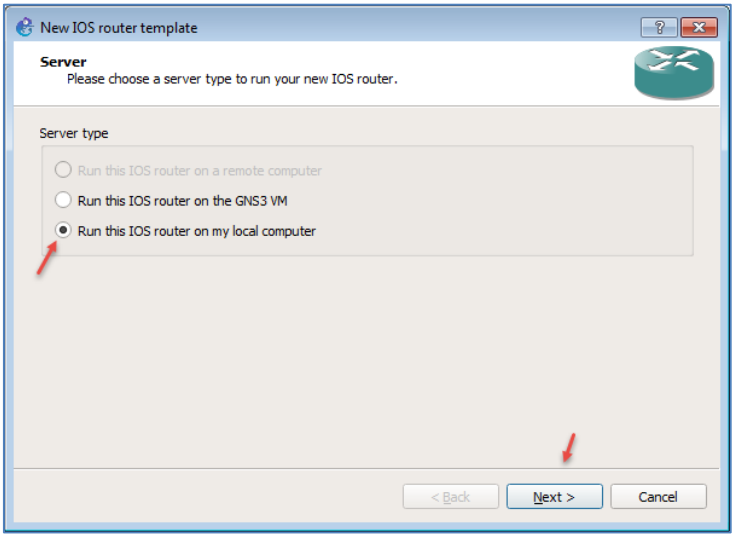
در شکل ۷-۲۱، از سمت چپ وارد قسمت IOS Routers شوید و بر روی New کلیک کنید.



شکل ۷-۲۱ کار با GNS3

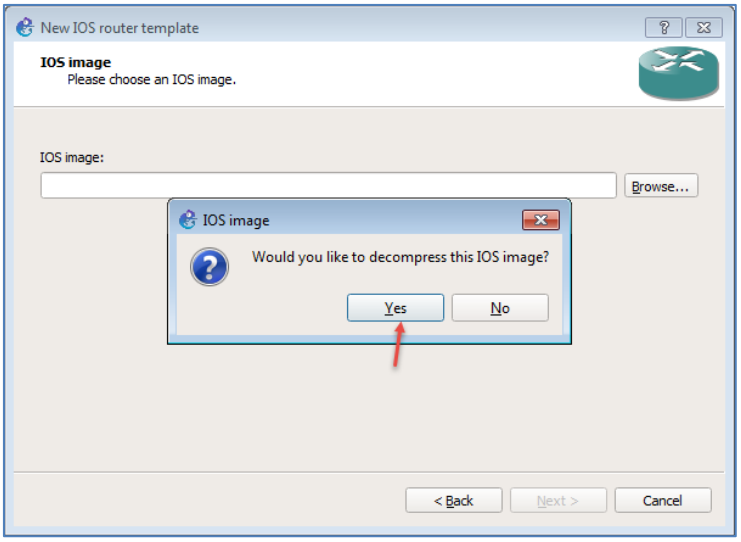
در شکل ۷-۲۲، برای اینکه IOS را بر روی سیستم اصلی اجرا کنیم گزینه‌ی دوم یعنی Local Computer را انتخاب کنید و بر روی Next کلیک کنید.

www.takbook.com



شکل ۲۲-۷ کار با GNS3

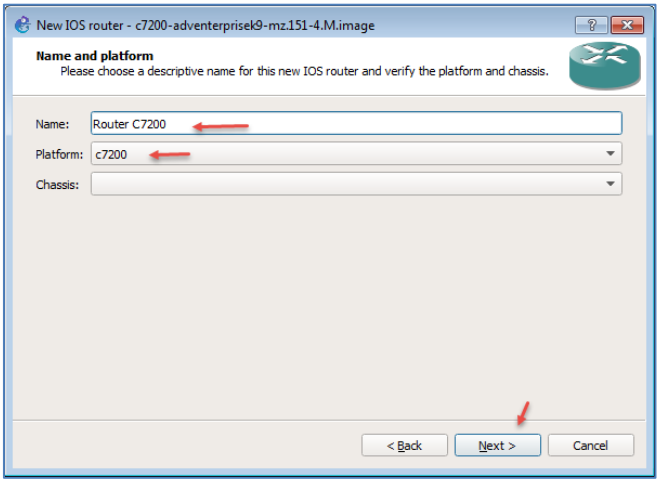
در شکل ۲۳-۷، بر روی Browse کلیک کنید و فایل دانلود شده را به آن معرفی و برای اضافه کردن آن به نرم‌افزار بر روی Yes کلیک و بعد بر روی Next کلیک کنید.



شکل ۲۳-۷ کار با GNS3

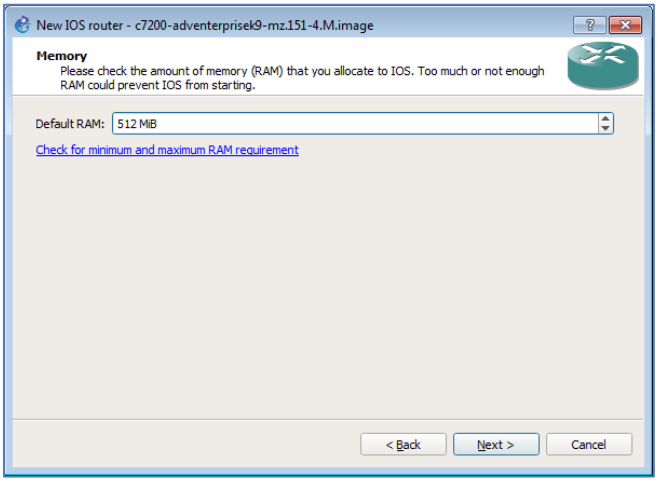
در شکل ۲۴-۷، باید نام روتر را به دلخواه وارد و در قسمت Platform باید مدل روتر را بر روی C7200 قرار دهید و بر روی Next کلیک کنید.

www.takbook.com



شکل ۲۴-۷ کار با GNS3

در شکل ۲۵-۷، بر روی Next کلیک کنید.

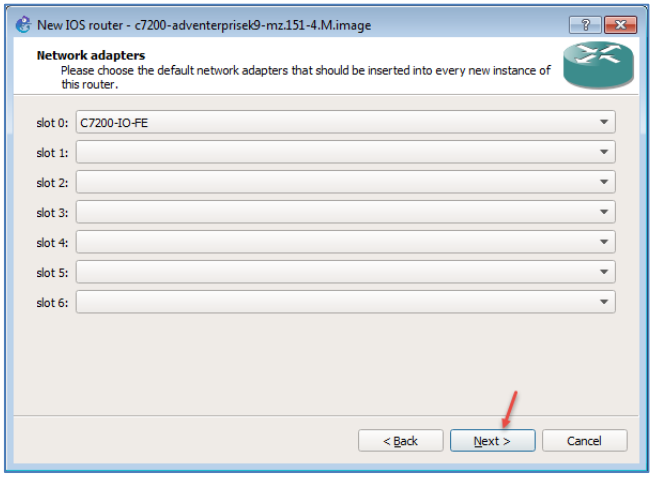


شکل ۲۵-۷ کار با GNS3

در شکل ۲۶-۷، باید Slot مربوط به روتر را انتخاب کنید، که بر روی این Slotها می‌تواند انواع پورت‌ها قرار بگیرد، در حال حاضر Slot پیش‌فرض کفایت می‌کند.

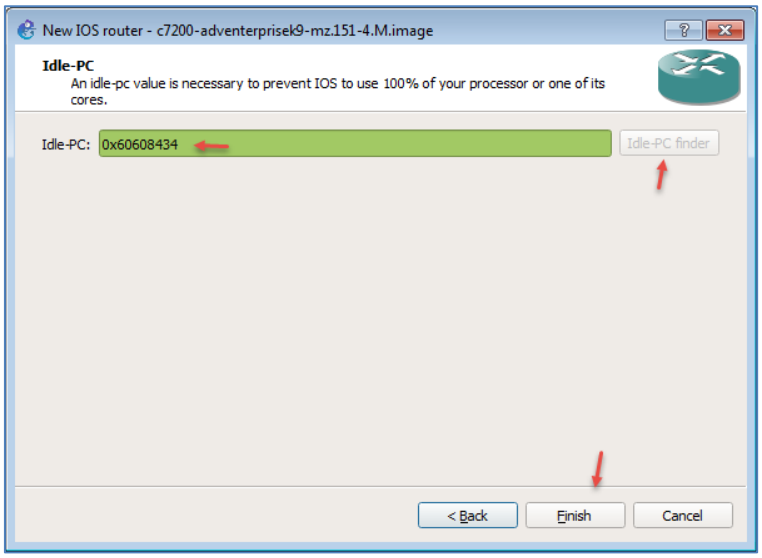
بر روی Next کلیک کنید.

www.takbook.com



شکل ۲۶-۷ کار با GNS3

در شکل ۲۷-۷، باید برای روتر خود یک Idle-PC مشخص کنید، برای این کار بر روی دکمه Idle-Pc finder کلیک کنید، این موضوع کمک می‌کند که مقدار درگیری سرور بسیار کم شود و مشکلی در کار پیش نیاید، اگر این کار را نکنید CPU کاملاً مشغول خواهد شد.

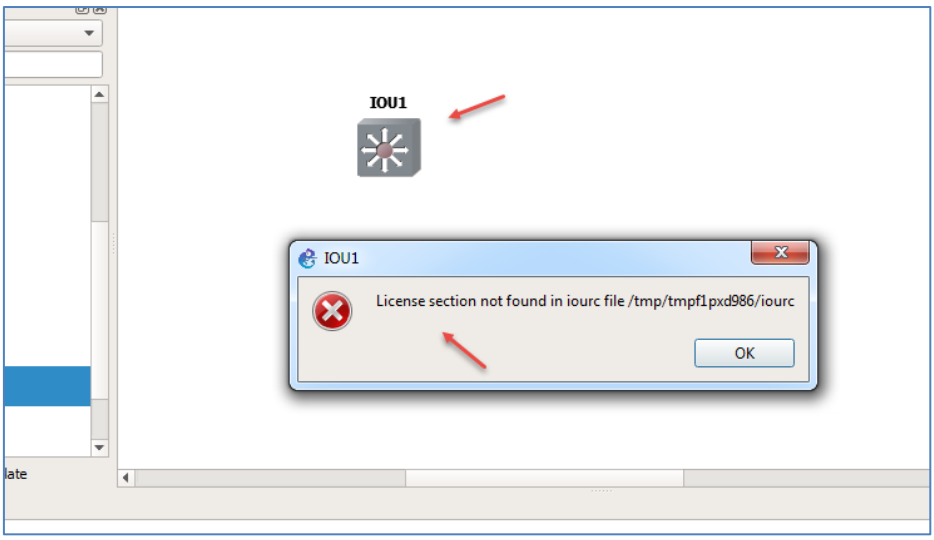


شکل ۲۷-۷ کار با GNS3

www.takbook.com

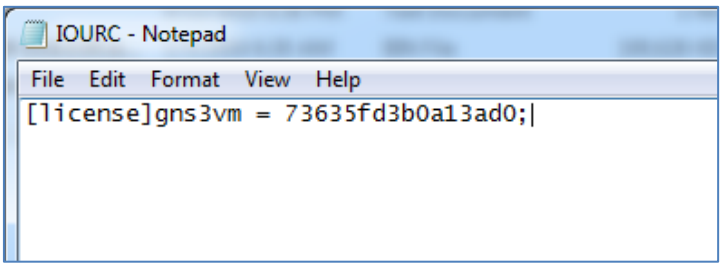
۷-۲ اضافه کردن لایسنس IOU به نرم‌افزار

توجه داشته باشید که برای کار با IOU نیاز به لایسنس دارید که باید در GNS3 وارد کنید، اگر چنانچه به مانند شکل ۷-۲۸، در هنگام روشن کردن دستگاه با خطای زیر مواجه شدید باید به صورت زیر عمل کنید.



شکل ۷-۲۸ کار با GNS3

متن زیر را در یک فایل txt وارد و با هر نامی ذخیره کنید:

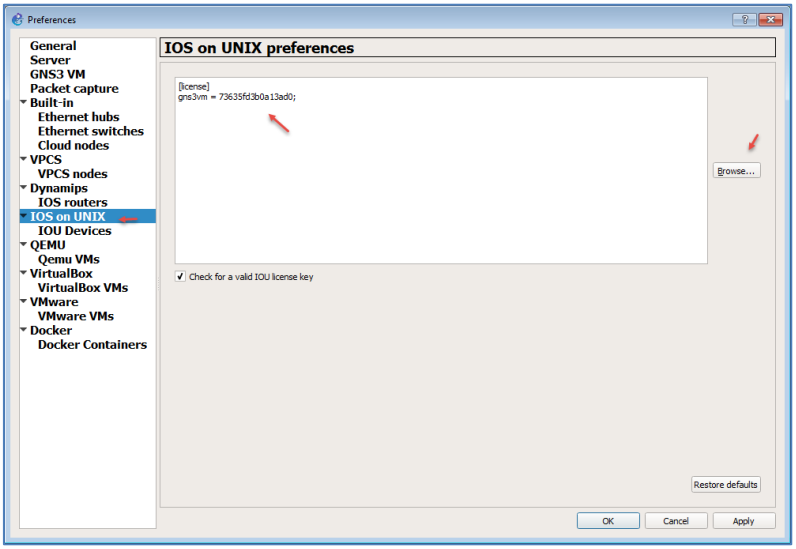


شکل ۷-۲۹ کار با GNS3

```
[license]
gns3vm = 73635fd3b0a13ad0;
```

وارد GNS3 شوید و قسمت Preferences را فعال و به قسمت IOS on UNIX مراجعه کنید و به مانند شکل ۷-۳۰، بر روی Browse کلیک کنید و فایل TXT مربوط به لایسنس را که ایجاد کردید انتخاب و بر روی ok کلیک کنید، با این کار لایسنس IOU فعال و سوئیچ‌ها فعال خواهند شد.

www.takbook.com



شکل ۳۰-۷ کار با GNS3

خوب در این بخش به طور کامل نحوه‌ی نصب و راه‌اندازی GNS3 را با هم بررسی کردیم و در ادامه کتاب از آن استفاده خواهیم کرد.

www.takbook.com

فصل هشتم

بررسی پروتکل IPV6

شبکه‌هایی که با آن‌ها در حال حاضر کار می‌کنیم، بیشتر آن‌ها از IPV4 استفاده می‌کنند، به دلیل تولید بسیار زیاد ادوات الکترونیکی و استفاده‌ی آن‌ها از اینترنت این آدرس‌ها به اتمام رسیده، که همین امر باعث شد که محققان سازمان Internet Engineering Task Force (IETF) مدل جدید آن را با عنوان IPv6 معرفی کنند که بسیار بیشتر از IPV4 آدرس در اختیار جامعه قرار داده است، البته IPV5 هم وجود داشت که به خاطر مشکلاتی که در سر راه قرار داشت، گسترش نیافت و به فراموشی سپرده شد.

ویژگی‌های IPv6

فضای آدرس‌دهی بسیار بزرگ

همان‌طور که می‌دانید، ipv4 از ۳۲ بیت تشکیل شده است، اما ipv6 از ۱۲۸بیت تشکیل شده است که به صورت زیر بیان می‌شود:

2^128 = 340,282,366,920,938,463,374,607,431,770,000,000

این تعداد ip addressهایی است که این پروتکل پشتیبانی می‌کند که واقعاً زیاد است، یعنی در هر مترمربع کره‌ی زمین، چندین هزار آدرس IP اختصاص داده می‌شود.

استفاده نشدن از NAT

همان‌طور که می‌دانید، IPV4 برای خارج شدن از شبکه‌ی داخلی و ورود به اینترنت باید تبدیل به IPهای VALID می‌شد که این کار را با ترجمه‌ی آدرس‌های Invalid به Valid انجام می‌دادیم که به آن NAT می‌گفتند، اما در مورد IPV6 این چنین نیست و روش دیگری برای این موضوع مورد استفاده قرار می‌گیرد.

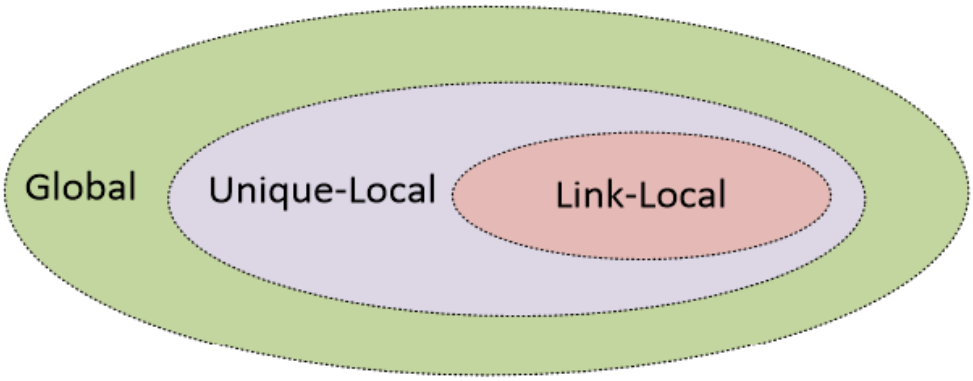
حذف شدن آدرس‌های Broadcast

در این پروتکل، به علت افزایش تعداد آدرس‌های Multicast دیگر خبری از Broadcast نیست و آدرس‌ها به صورت Unicast و Multicast و Anycast هستند.

:Unicast

به آدرس‌هایی گفته می‌شود که برای ارتباط بین یک مبدأ و مقصد استفاده می‌شوند، در شکل ۱ -۸، ساختار آدرس‌های Unicast را مشاهده می‌کنید:

www.takbook.com



شکل ۱-۸ ساختار آدرس‌های Unicast

Global unicast address

به مفهوم، آدرس‌های unicast قابل انتقال در اینترنت است (قابلیت آدرس‌دهی در اینترنت را دارد) و شبیه به نوع متناظر آن در IPv4 می‌باشد، به این نوع آدرس‌ها Aggregatable Address نیز می‌گویند، که به مانند جدول ۱-۸، Subnet آن از سه قسمت 3,45,16 بیت تشکیل شده است که جمعاً می‌شود ۶۴ بیت و قسمت Interface آن هم از ۶۴ بیت تشکیل شده است.

جدول ۱-۸ Global unicast address

3 bits	45 bits	16 bits	64 bits
001	Global Routing Prefix	Subnet ID	Interface ID

این ساختار از قسمت‌های زیر تشکیل شده است:

Unique local address

این آدرس‌ها را با نام Site-Local unicast هم می‌شناسند که قابلیت انتقال در اینترنت را نداشته و عملکرد این نوع آدرس‌ها دقیقاً شبیه به آدرس‌های local یا Private در IPv4 است. به مانند جدول ۲-۸، این آدرس‌ها با ۸ بیت ثابت (FD) شروع می‌شوند و به دنبال آن ۴۰ بیت صفر و سپس 16 بیت مربوط به Subnet ID است که معمولاً آن را هم صفر در نظر می‌گیرند.۶۴ بیت پایانی هم که Interface ID است که برای هر کامپیوتر منحصربه‌فرد است.

جدول ۲-۸ Unique local address

8 bits	40 bits	16 bits	64 bits
FD	Global ID	Subnet ID	Interface ID

www.takbook.com

Link local address

شبیه به آدرس‌های Private یا خصوصی در IPv4 بوده و قابل انتقال در اینترنت نیستند. این آدرس‌ها را می‌توان به اعضای یک شبکه LAN و یا چند LAN مختلف که قصد برقراری ارتباط با یکدیگر دارند، تخصیص داد.

این آدرس‌ها که در غیاب DHCP Server ایجاد می‌شوند، در IPv6 معادل Fe80::/64 هستند. به بیانی دیگر اگر در هنگام تنظیم IP آدرس، در کادر محاوره‌ای Properties کارت شبکه گزینه‌ی obtain IPv6 address automatically را انتخاب کنیم، سیستم عامل به طور خودکار بر اساس تلفیقی از MAC Address مربوط به کارت شبکه با آدرس Link-Local یک آدرس IPv6 به کارت شبکه اختصاص می‌دهد، این آدرس‌ها اصولاً برای رسیدن به گره‌های متصل شده به همان دستگاه مورد استفاده قرار می‌گیرن.

مثلاً در شکل ۲-۸، یک آدرس Link-Local را مشاهده می‌کنید که به یک کارت شبکه تخصیص داده شده است:

شکل ۲-۸ آدرس Link-Local

یکی از نکات مهم در این نوع آدرس‌ها این است که روترها بسته‌هایی که دارای آدرس Link Local باشند به Interfaceهای دیگر انتقال نمی‌دهند، توجه داشته باشید که تمام Interfaceها دارای آدرس link-local هستند.

Multicast

برای ارتباط یک مبدأ با چند مقصد مشخص‌شده استفاده می‌شود که این مقصد در یک گروه قرار دارند؛ این آدرس جایگزین Broadcast در ipv4 شده است. در ادامه، جدول کامل این آدرس‌ها قرار گرفته شده است.

www.takbook.com

Anycast

در این آدرس‌دهی برای مثال روتر شما برای رسیدن به یک سرور چند مسیر را در پیش رو دارد، روتر مسیری را انتخاب می‌کند که کمترین Cost را داشته باشد، پس آدرس Anycast آدرسی است، برای انتخاب بهترین مسیر، تا رسیدن به یک سرور و یا انتخاب یک سرور بین چند سرور یکسان که هزینه‌ی کمتری دارد.

در جدول ۳-۸، تفاوت اصلی بین IPV4 و IPV6 را مشاهده می‌کنید:

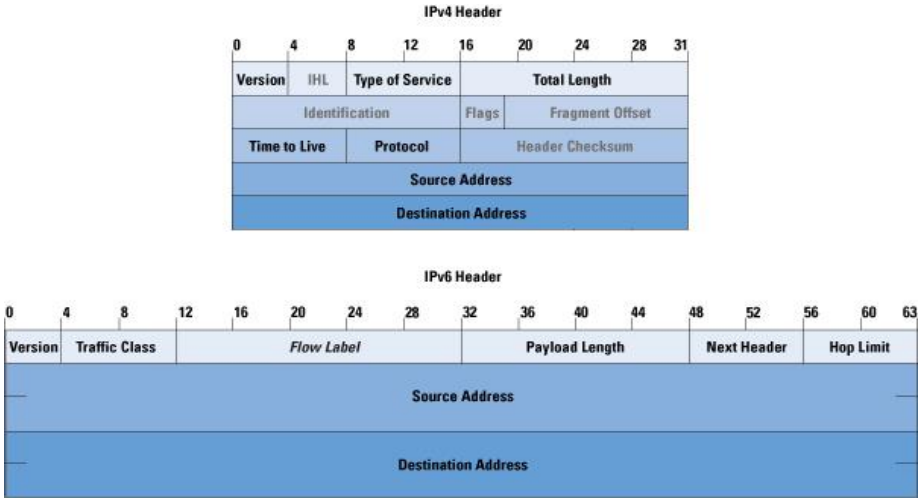
جدول ۳-۸ *تفاون بین IPV4 و IPV6*

IPV4	IPV6
که برابر IPپشتیبانی از ۲ به توان ۳۲ آدرس ۴,۲۹۴,۹۶۷,۲۹۶ آدرس است	پشتیبانی از ۲ به توان ۱۲۸ آدرس که بسیار بسیار زیاد است و می‌شود گفت پایانی ندارد
NATبه خاطر محدودیت فضا باید از پروتکل استفاده کرد.	به NATبه علت داشتن تعداد بالای آدرس از صورت پیش‌فرض استفاده نمی‌شود.
برای اختصاص دادن آدرس به میزبان‌ها باید از استفاده کنند و یا اینکه به DHCPسرویس صورت دستی وارد کنند.	در این ورژن میزبان‌ها دارای آدرس اختصاصی هستند که می‌توانند از آنها استفاده کنند، البته از هم می‌توانید در این پروتکل DHCPسرویس استفاده کنید.
پشتیبانی می‌شود ولی IPSECدر این پروتکل از یک گزینه‌ی اختیاری است که می‌توان از آن از طریق IPاستفاده کرد تا محافظت از بسته‌های رمزگذاری، اعتبارسنجی و .. انجام شود.	IPSECفرض در این پروتکل به صورت پیش پشتیبانی می‌شود و فعال است و نیازی به تنظیم آن نیست.
ARP که در پروتکل broadcastsاستفاده از استفاده می‌شود.	به هیچ عنوان استفاده ARP و broadcastsاز Neighbor و Multicastنمی‌کند ولی به جای آن از استفاده NDP یا همان Discovery Protocol می‌شود.ARP جایگزین NDمی‌کند،
TCP , UDPاز پروتکل لایه ۴ پشتیبانی می‌کند،	TCP , UDPاز پروتکل لایه ۴ پشتیبانی می‌کند،
پشتیبانی می‌کنند.FTP, HTTPار پروتکل‌های	پشتیبانی می‌کنند.FTP, HTTPار پروتکل‌های

تفاوت Headerهای ipv4 و ipv6

ب توجه به شکل ۳-۸، اگر به IPV4 دقیق نگاه کنید، متوجه‌ی پیچیده‌تر بودن آن نسبت به IPV6 می‌شوید، در واقع ipv6 خیلی ساده‌تر از IPV4 است.

www.takbook.com



شکل ۳-۸ تفاوت Headerهای ipv4 و ipv6

هر یک از گزینه‌های موجود در این Header ها را باهم مورد بررسی قرار می‌دهیم:

Version: این فیلد ۴ بیتی بوده و نشان‌دهنده‌ی نسخه‌ی IP موجود است.

Traffic Class: برای مشخص کردن کلاس‌های مختلف و مشخص کردن اولویت پکت‌ها در IPV6 استفاده می‌شود و طول آن 8 بیت است.

Flow Label: طول این فیلد 20 بیت است. یکی از ویژگی‌های آن پشتیبانی از QOS است که یکی از ویژگی‌های جدید در IPV6 است و توانایی مسیریابی ترافیک مشخص را در شبکه می‌دهد و در این کتاب مفصل در مورد آن صحبت می‌کنیم.

Payload Length: طول این بخش 20 بیت است که شامل طول بخش بسته‌ی IPV6 است.

NextHeader: طول این فیلد 8 بیت است که نشان‌دهنده‌ی نوع Header در IPV6 است.

Hop Limit: طول این فیلد ۸ بیت است که برای مشخص کردن تعداد روترهایی است که بسته‌ی اطلاعاتی از آن رد می‌شود، یعنی زمانی‌که این بسته از یک روتر در سر راه رد می‌شود یک شماره از این زمان کم می‌شود و تا زمانی که این شماره به پایان برسد و بسته مورد نظر حذف شود.

Source Address: نشان‌دهنده‌ی آدرس مبدأ است.

DestinationAddress: نشان‌دهنده‌ی آدرس مقصد است.

۸-۱ روش آدرس‌دهی در IPV6

IPV6 از ۱۲۸ بیت تشکیل شده است یعنی از ۸ قسمت ۱۶ بایتی تشکیل شده است که هر قسمت آن به صورت hexadecimal است یعنی از ۰ تا F و توسط (:) هر قسمت از قسمت دیگر جدا می‌شود، در جدول ۸-۴، تبدیل اعداد به Hexadecimal را که مربوط به IPV6 است را مشاهده می‌کنید.

جدول ۴-۸ *تبدیلات اعداد*

www.takbook.com

Decimal	Binary	Hexadecimal
0	0000	0
1	0001	1
2	0010	2
3	0011	3
4	0100	4
5	0101	5
6	0110	6
7	0111	7
8	1000	8
9	1001	9
10	1010	A
11	1011	B
12	1100	C
13	1101	D
14	1110	E
15	1111	F

در زیر یک نمونه از آدرس IPV6 را مشاهده می‌کنید که دارای ۸ بخش است، البته کمی کیج کننده!

2001:0DA8:E800:0000:0260:3EFF:FE47:0001

روش‌هایی را برای کوتاه کردن آن وجود دارد که در این قسمت بررسی می‌کنیم.

روش اول – حذف صفرهای ابتدایی

در این روش هر چه صفر قبل از یک عدد وجود دارد را حذف می‌کنیم:

2001:0DA8:E800:0000:0260:3EFF:FE47:0001

2001: DA8:E800:0: 260:3EFF:FE47: 1

روش **دوم – حذف صفرهای پشت سر هم**

در این روش اگر بین یک کلون " : " چندین صفر وجود داشت، می‌توانید صفرها را حذف کرده و فقط کلون را قرار دهیم. به روش زیر توجه کنید:

www.takbook.com

2001:0000:0000:2260:3EFF:FE47:0001

2001:: 2260:3EFF:FE47:1

همان‌طور که مشاهده می‌کنید به جای صفرهایی که در قسمت ۲ و ۳ قرار داشتند، فقط :: قرار دادیم که همین کار باعث کوتاه شدن این IP شده است.

تذکر

دو بار استفاده از کلون یا :: در یک IP امکان‌پذیر نیست و مشکل ایجاد می‌شود.

در آدرس‌دهی IPV4 اگر یادتان باشد ما از آدرس IP به همراه SubnetMask استفاده می‌کردیم که چنین موضوعی در IPv6 وجود ندارد و به جای آن از Subnet Prefix استفاده می‌کنیم.

در IPV6 چیزی به نام NETMASK وجود ندارد و جایگزین آن Prefix است، در واقع Prefix جداکننده‌ی NET IDاز HOST ID است.

Net ID | Host ID

2014:2015:0000:0000:BC02:0000:0001:0002/64

در مثال بالا ۶۴/ به این معناست که از سمت چپ ۶۴ بیت به جلو برویم و بعد از ۶۴ بیت قسمت HOST IDشروع می‌شود و قبل از آن مربوط به NET ID می‌شود. هر عدد در اینجا معادل ۴ بیت است.

۸-۲ انواع آدرس‌های ipv6

آدرس های Unicast به سه دسته تقسیم می شوند، که در زیر آنها را بررسی می‌کنیم.

فرم کلی Global Unicast:

به آدرس‌های Public در IPv6 گفته می‌شود که در IPv4 هم این آدرس‌ها را داشتیم و در دنیای اینتنرت اعتبار داشتند، در جدول ۵-۸، هدر کلی این آدرس را مشاهده می‌کنید که همه‌ی گزینه‌های آن را بررسی می‌کنیم.

از چپ به راست

جدول ۵-۸ Global Unicast

FP	TLA-ID	RES	NLA-ID	SLA-ID	INTERFACEID
3 بیت	13 بیت	8 بیت	24 بیت	16 بیت	64 بیت

www.takbook.com

FP: نشان‌دهنده‌ی نوع IPV6 است (Format Prefix) ipهای PUBLIC ورژن ۶ در حالت باینری با ۰۰۱ شروع می‌شوند.

TLA-ID: مخفف (Top Level Aggregator Identifire) دسته‌بندی IPهایی هستند که به جاهای بزرگ، مانند قاره‌ها اختصاص پیدا می‌کنند.

RES: یعنی رزرو شده است.

NLA-ID: مخفف (Next Level Aggregator) IPهای منحصربه‌فردی هستند که به جاهای بزرگ، مانند کشورها اختصاص پیدا می‌کنند.

SLA-ID: مخفف (Site Level Aggregator) ipهای منحصربه‌فردی هستند که به جاهای بزرگ، مانند شهرها و سازمان‌های بزرگ اختصاص پیدا می‌کنند.

Ipهای خاصی در **IPV6** وجود دارند که به شرح زیر می‌باشند:

::/128 یک آدرس نامشخص ابتدای یک بایت است که می‌خواهد آدرس Link-Local را مشخص کند.

::/0 این آدرس معادل 0.0.0.0 در IPV4 است و برای مسیریابی به صورت دستی از این آدرس استفاده می‌کنند.

1::/128 این آدرس معادل آدرس LoopBack است که در ipv4 به صورت 127.0.0.1 بوده است و برای تست کارت شبکه و پروتکل TCP/IP استفاده می‌شود.

FE80::/10 آدرس Link Local Unicast است که شبیه به آدرس 169.254.x.x است.

FF00::/8 آدرس‌های مربوط به Multicast است.

آدرس‌های Multicast

این آدرس‌ها جایگزین Broadcast در IPV4 شده‌اند و برای کارهای زیر استفاده می‌شوند:

- برای استفاده در سرویس DHCP.
- اعلام مسیرها در روترها که قبلاً به صورت Broadcast در IPV4 آموختیم.
- برای تقاضاهای روتر.
- و...
- این آدرس‌ها از ۸ بیت پسوند Prefix استفاده می‌کنند که به صورت FF00::/8 است، default Gateway برای کلاینت‌ها وجود ندارد.

در جدول ۶-۸، انواع ipهای multicast برای پروتکل‌ها و سرورها و ... را مشاهده می‌کنید:

جدول ۶-۸ تبدیلات اعداد

توضیحات	Address
همه‌ی گره‌ها در بخش شبکه‌های محلی	ff02::1
تمام روترها در بخش شبکه‌های محلی	ff02::2
برای الگوریتم spf مربوط به OSPFV3	ff02::5
مربوط به همه‌ی روترهای DR در پروتکل OSPF	ff02::6

www.takbook.com

مربوط به پروتکل IS-IS	ff02::8
مربوط به پروتکل RIP	ff02::9
مربوط به پروتکلEIGRP	ff02::a
مربوط به روترهای Protocol Independent Multicast (PIM)	ff02::d
گزارش مربوط به MLDv2 تعریف‌شده در RFC 3810	ff02::16
همه‌ی سرورهای DHCP و Real Agentها در شبکه‌ی محلی	ff02::1:2
تمام میزبان‌های LLMNR (Link Local Multicast Name Resolution) در شبکه‌ی محلی	ff02::1:3
همه‌ی سرورهای DHCP در سایت شبکه‌ی محلی	ff05::1:3
مربوط به Service Discovery Protocol	ff0x::c
مربوط به(Multicast Domain Name System (DNS	ff0x::fb
مربوط به Network Time Protocol	ff0x::101

در آدرس زیر می‌توانید تمام اطلاعات مربوط به آدرس‌های Multicast را مشاهده کنید:

https://www.iana.org/assignments/ipv6-multicast-addresses/ipv6-multicast-addresses.xhtml

IPV6 می‌تواند به صورت خودکار توسط روش‌های زیر تنظیم شود:

Stateful Autoconfiguration
Stateless Autoconfiguration
EUI – 64

Stateful Autoconfiguration

در این روش که سرویس DHCP از آن استفاده می‌کند یک آدرس با طول ۱۲۸ بیت واگذار می‌شود به کلاینت‌ها از طریق سرور واگذار می‌شود، توجه داشته باشید آدرس‌های Stateful و Stateless مکمل همدیگر هستند، مثلاً یک کلاینت می‌تواند از آدرس Stateless استفاده کند ولی برای بدست آوردن دیگر اطلاعات شبکه نیاز به آدرس Stateful دارد.

:Stateless Autoconfiguration

در این روش یک IPV6 که ۱۲۸ بیت است را نصف می‌کند و ۶۴ بین از آن را استفاده و ۶۴ بیت دوم را بعداً استفاده می‌کند، یعنی اینکه ۶۴ بین از یک آدرس واگذار می‌شود و ۶۴ بیت در یک زمان دیگر استفاده می‌شود.

:EUI – 64

در این روش روتر برای اختصاص دادن IP به کلاینت مورد نظر از آدرس Mac کلاینت در IPv6 استفاده می‌کند، به این صورت که ۶۴ بین اول به صورت دستی وارد می‌شود و ۶۴ بیت دوم از طریق Mac address دستگاه مورد نظر استخراج می‌شود، اما آدرس Mac، ۴۸ بیتی است. برای حل این مشکل از مقدار FFFE در وسط آدرس Mac استفاده می‌کنند و به‌این‌ترتیب آدرس مورد نظر به دستگاه مورد نظر داده می‌شود. مثلاً برای واردکردن آدرس به این روش، وارد اینترفیس می‌شویم و از آدرس زیر استفاده می‌کنیم:

www.takbook.com

Router(config-if)# ipv6 address 2011:1111:11::1/64 eui-64

بعد از اینکه آدرس را وارد کردیم با دستور **Show IPV6 Interface Berief** می‌توانیم آدرس اصلی را مشاهده کنیم که به صورت زیر است:

Static Address	Mac Address
2011:1111:11:0:	2D0:97FF:FE51:6A02

همان‌طور که مشاهده می‌کنید در قسمت دوم برای کامل کردن آن، از آدرس Mac دستگاه مورد نظر استفاده کرده است.

۸-۳ مسیریابی در IPV6

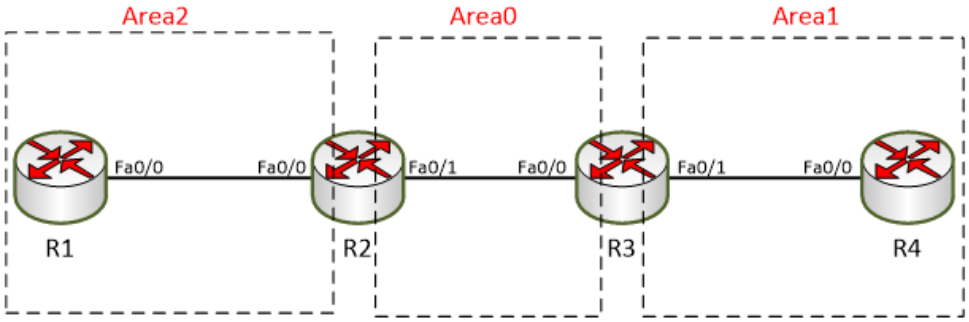
مانند بسیاری از عملکردهای IPV6 مسیریابی هم دقیقاً شبیه به IPV4 انجام می‌شود ولی با کمی تغییر در ویژگی‌های آن، در شکل ۸-۷ پروتکل‌های مسیریابی را مشاهده می‌کنید که در IPV6 می‌توانید از آنها استفاده کنید.

جدول ۸-۷ *پروتکل قابل استفاده در IPV6*

Routing Protocol	Defined By	Notes
RIPng (RIP next generation)	RFC	The "next generation" is a reference to a TV series, *Star Trek: the Next Generation*.
OSPFv3 (OSPF version 3)	RFC	The OSPF you have worked with for IPv4 is actually OSPF version 2, so the new version for IPv6 is OSPFv3.
EIGRPv6 (EIGRP for IPv6)	Cisco	Cisco owns the rights to the EIGRP protocol, but Cisco also now publishes EIGRP as an informational RFC.
MP BGP-4 (Multiprotocol BGP version 4)	RFC	BGP version 4 was created to be highly extendable; IPv6 support was added to BGP version 4 through one such enhancement, MP BGP-4.

۸-۴ فعال کردن IPV6 روی پروتکل OSPF V3

www.takbook.com



شکل ۴-۸ سناریو IPV6 بر روی OSPF

با توجه به شکل ۴-۸، می‌خواهیم با نحوه‌ی کار IPV6 در پروتکل OSPF آشنا شویم. به پروتکل OSPF که IPV6 روی آن فعال می‌شود، OSPF V3 می‌گویند که ورژن سوم این پروتکل است.

وارد روتر R1 می‌شویم و دستورات زیر را وارد می‌کنیم:

```
R1(config)#ipv6 unicast-routing
R1(config)#ipv6 router ospf 100
R1(config-rtr)#router-id 150.1.1.1
R1(config-rtr)#int f0/0
R1(config-if)#ipv6 address 2011:1111:12::1/64
R1(config-if)#ipv6 ospf 100 area 2
R1(config-if)#no shutdown
```

دستورات، مانند گذشته است، فقط زمانی که با دستور ipv6 router ospf 100، پروتکل OSPF را تعریف کردیم و وارد آن شدیم، باید Router-ID را تعریف کنیم. بعدازآن وارد اینترفیس می‌شویم، آدرس را تعریف می‌کنیم و در آخر با دستور ipv6 ospf 100 area 2، پروتکل OSPF را روی این اینترفیس فعال می‌کنیم و در area 2 (طبق شکل) قرار می‌دهیم و بعد با دستور no shutdown، اینترفیس مورد نظر را روشن می‌کنیم.

در بقیه‌ی روترها به صورت زیر، دستورات را وارد کنید:

وارد روتر R2 شوید و دستورات زیر را وارد کنید:

```
R2(config)#ipv6 unicast-routing
R2(config)#ipv6 router ospf 100
R2(config-rtr)#router-id 150.1.2.2
R2(config-rtr)#int f0/0
R2(config-if)#ipv6 address 2011:1111:12::2/64
R2(config-if)#ipv6 ospf 100 area 2
R2(config-if)#no sh
R2(config-if)#int f0/1
R2(config-if)#ipv6 address 2011:1111:23::1/64
R2(config-if)#ipv6 ospf 100 area
R2(config-if)#ipv6 ospf 100 area 0
```

www.takbook.com


```
R2(config-if)#no sh
```

وارد روتر R3 شوید و دستورات زیر را وارد کنید:

```
R3(config)#ipv6 unicast-routing
R3(config)#ipv6 router ospf 100
R3(config-rtr)#router-id 150.1.3.3
R3(config-rtr)#int f0/0
R3(config-if)#ipv6 address 2011:1111:23::2/64
R3(config-if)#ipv6 ospf 100 area 0
R3(config-if)#no sh
R3(config-if)#int f0/1
R3(config-if)#ipv6 address 2011:1111:34::1/64
R3(config-if)#ipv6 ospf 100 area 1
R3(config-if)#no sh
```

وارد روتر R4 شوید و دستورات زیر را وارد کنید:

```
R4(config)#ipv6 unicast-routing
R4(config)#ipv6 router ospf 100
R4(config-rtr)#router-id 150.1.4.4
R4(config-rtr)#int f0/0
R4(config-if)#ipv6 address 2011:1111:34::2/64
R4(config-if)#ipv6 ospf 100 area 1
R4(config-if)#no sh
```

کار به اتمام رسیده است. برای مشخص شدن درستی انجام کار، در یکی از روترها، دستور زیر را وارد کنید:

```
R4(config-if)#do sh ipv6 route
IPv6 Routing Table - 5 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route, M - MIPv6
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
       D - EIGRP, EX - EIGRP external
OI  2011:1111:12::/64 [110/3]
    via FE80::20A:F3FF:FEBA:E802, FastEthernet0/0
OI  2011:1111:23::/64 [110/2]
    via FE80::20A:F3FF:FEBA:E802, FastEthernet0/0
C   2011:1111:34::/64 [0/0]
    via ::, FastEthernet0/0
L   2011:1111:34::2/128 [0/0]
    via ::, FastEthernet0/0
L   FF00::/8 [0/0]
```

www.takbook.com

via ::, Null0

۸-۵ سوالات فصل هشتم

1. Which of the following was a short-term solution to the IPv4 address exhaustion problem?

کدام یک گزینه‌های زیر یک راه‌حل کوتاه مدت برای ظرفیت کم آدرس‌های IPV4 بوده است؟

a. IP version 6

www.takbook.com

b. IP version 5
c. NAT/PAT
d. ARP

2. A router receives an Ethernet frame that holds an IPv6 packet. The router then makes a decision to route the packet out a serial link. Which of the following statements is true about how a router forwards an IPv6 packet?

روتر یک فریم Ethernet را دریافت می‌کند که دارای بسته‌ی IPV6 است بعد از آن روتر تصمیم به ارسال آن بسته از طریق پورت سریال می‌کند، کدام گزینه در مورد ارسال بسته IPV6 درست است؟

a. The router discards the Ethernet data-link header and trailer of the received frame.
b. The router makes the forwarding decision based on the packet's source IPv6 address.
c. The router keeps the Ethernet header, encapsulating the entire frame inside a new IPv6 packet before sending it over the serial link.
d. The router uses the IPv4 routing table when choosing where to forward the packet.

3. Which of the following is the shortest valid abbreviation for FE80:0000:0000:0100:0000:0000:0000:0123?

کدام گزینه کوتاه‌ترین انتخاب برای آدرس FE80:0000:0000:0100:0000:0000:0000:0123 است؟

a. FE80::100::123
b. FE8::1::123
c. FE80::100:0:0:0:123:4567
d. FE80:0:0:100::123

4. Which of the following is the shortest valid abbreviation for 2000:0300:0040:0005:6000:0700:0080:0009?

کدام یک از گزینه‌های زیر کوتاه‌ترین انتخاب برای آدرس 2000:0300:0040:0005:6000:0700:0080:0009 است؟

a. 2:3:4:5:6:7:8:9
b. 2000:300:40:5:6000:700:80:9
c. 2000:300:4:5:6000:700:8:9
d. 2000:3:4:5:6:7:8:9

5. Which of the following is the unabbreviated version of IPv6 address 2001:DB8::200:28?

کدام یک از گزینه‌های زیر آدرس اصلی 2001:DB8::200:28 است؟

a. 2001:0DB8:0000:0000:0000:0000:0200:0028
b. 2001:0DB8::0200:0028
c. 2001:0DB8:0:0:0:0:0200:0028
d. 2001:0DB8:0000:0000:0000:0000:200:0028

6. Which of the following is the prefix for address 2000:0000:0000:0005:6000:0700:0080:0009, assuming a mask of /64?

کدام یک از پیشوندهای زیر برای آدرس 2000:0000:0000:0005:6000:0700:0080:0009 با /64 است؟

a. 2000::5::/64
b. 2000::5:0:0:0:0/64

www.takbook.com

c. 2000:0:0:5::/64
d. 2000:0:0:5:0:0:0:0/64

7. Which command automatically generates an IPv6 address from a specified IPv6 prefix and MAC address of an interface?
کدام دستور زیر به طور خودکار آدرس IPv6 را از پیشوند IPv6 مشخص شده و آدرس MAC یک Interface تولید می کند؟

a. ipv6 address dhcp
b. ipv6 address 2001:DB8:5:112::/64 eui-64
c. ipv6 address autoconfig
d. ipv6 address 2001:DB8:5:112::2/64 link-local

8. When configuring IPv6 on an interface, which two IPv6 multicast groups are joined? (Choose two.)
هنگام پیکربندی یک Interface در IPV6 به کدام دو گروه multicast IPv6 ملحق می‌شوید؟ (دو گزینه را انتخاب کنید)

a. 2000::/3
b. 2002::5
c. FC00::/7
d. FF02::1
e. FF02::2

9. Which IPv6 address type communication between subnets and cannot route on the Internet?
کدام نوع آدرس IPv6 بین زیر شبکه‌ها ارتباط برقرار می‌کند و نمی‌تواند از طریق اینترنت مسیریابی شود؟

a. link-local
b. unique local
c. multicast
d. global unicast

10. Which IPv6 address block sends packets to a group address rather than a single address?
کدام بلوک آدرس IPv6 بسته‌ها را به جای ارسال به یک آدرس واحد به آدرس گروه ارسال می کند؟

a. 2000::/3
b. FC00::/7
c. FE80::/10
d. FF00::/8

www.takbook.com

www.takbook.com

فصل نهم

شبکه‌های بی‌سیم

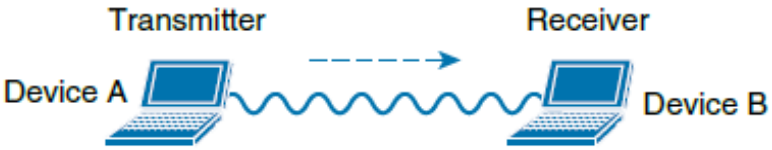
شبکه‌های بی‌سیم (Wireless LANs) به شبکه‌هایی گفته می‌شود که ارتباط بین اجزاء آن بدون سیم صورت می‌گیرد یعنی دیگر نیاز به خرید کابل و سوکت زدن نیست.

اصولاً ارتباط بین دستگاه‌های بی‌سیم از طریق فرکانس‌های رادیویی (RF) انجام می‌گیرد، این نوع ارتباط در لایه‌ی فیزیکی از مدل OSI عمل می‌کند.

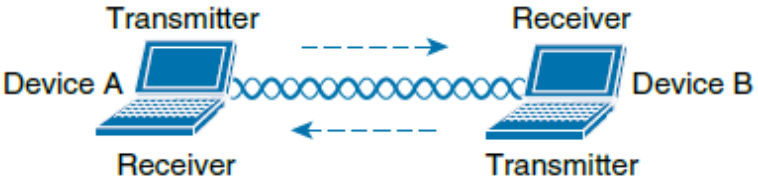
همانطور که دیده‌اید در شبکه‌های سیمی برای اینکه دو دستگاه با هم ارتباط برقرار کنند باید به سیم متصل شوند که این سیستم از رشته‌های فلز یا فیبر نوری تشکیل شده بود، در نوع ارتباط سیمی همه سیستم‌ها در هر نقطه‌ای نمی‌توانستند به شبکه متصل شوند و این یک ضعف بود.

اما در شبکه‌های بی‌سیم این محدودیت برداشته شده و در هر مکانی می‌توانید به شبکه‌های بی‌سیم متصل شوید.

ارتباط بین دستگاه‌های بی‌سیم به صورت یک طرفه و دو طرفه صورت می‌گیرد، که در شکل ۱ -۹، یک دستگاه به عنوان فرستنده (Transmitter) و دستگاه دیگر به عنوان گیرنده (Receiver) عمل می‌کند، اما در شکل ۲-۹، هر دو دستگاه به صورت فرستنده و گیرنده عمل می‌کنند که در ادامه نحوه کار آن را بررسی می‌کنیم.



شکل ۱-۹ ارتباط بین دو دستگاه



شکل ۲-۹ ارتباط بین دو دستگاه

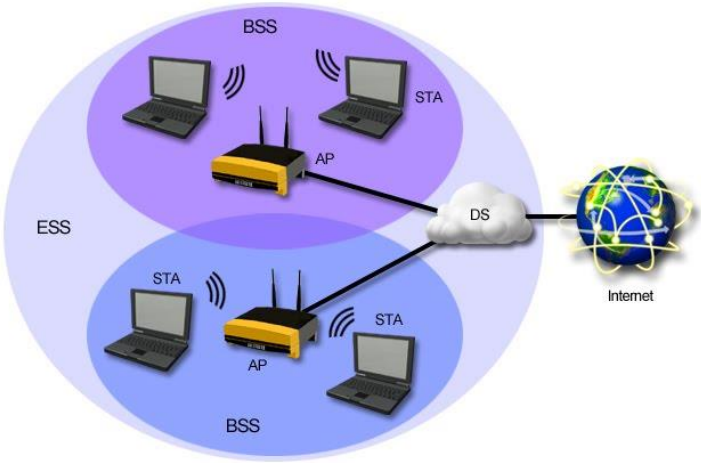
www.takbook.com

اما یکی از مشکلاتی که در این نوع سیستم وجود دارد تداخل در امواج است که در ادامه روی آن بحث می‌کنیم.

شکل ۳-۹ تداخل امواج

۹-۱ بررسی Basic Service Set (BSS)

با توجه به شکل ۴-۹، BSS به دستگاه‌هایی گفته می‌شود که برای متصل شدن به شبکه از یک AccessPoint استفاده می‌کنند و به آن متصل می‌شوند، اصولاً Access Pointها برای ارائه سرویس خود از یک شناسه با نام SSID استفاده می‌کنند که یک نام منطقی است و دستگاه‌ها از طریق آن به AccessPoint یا به طور فراگیرتر WIFI متصل می‌شوند.



***شکل ۴-۹** بررسی BSS*

چند مفهوم دیگر هم در این بخش باید مورد بررسی قرار گیرید:

۱- BSSID یا Basic service set identification به MAC آدرس Access Point اشاره دارد.

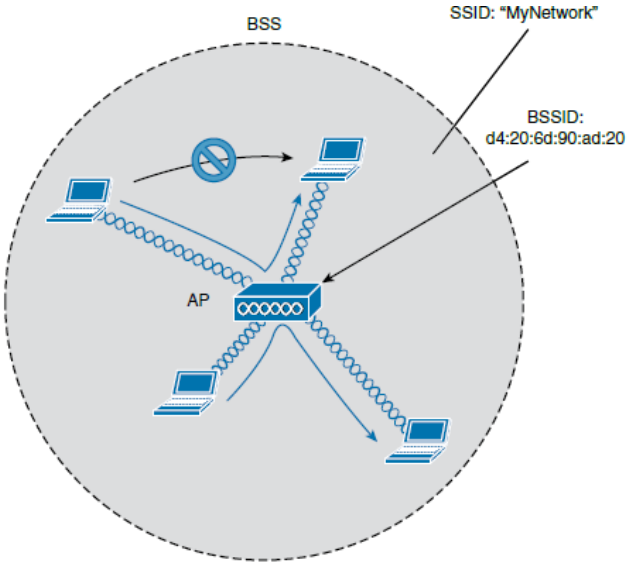
۲- SSID یا Service set identification یک نام برای دسترسی کاربران به Acces Point مورد نظر است که می‌تواند از طرف مدیر تغییر کند و حتی مخفی باشد.

www.takbook.com

۳- BSA یا Basic Service Area به منطقه‌ای گفته می‌شود که دستگاه‌های Access Point قادر به ارسال سیگنال هستند.

۴- ESS یا Extended Service Set به مجموعه‌ای از BSSها گفته می‌شود که دارای نام (SSID) یکسانی هستند که در شکل ۴-۹، این موضوع را مشاهده می‌کنید.

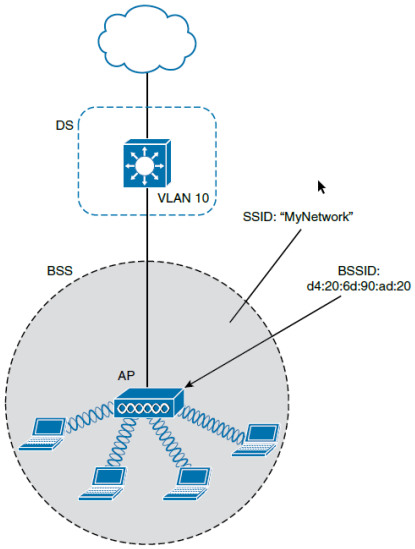
در شکل ۴-۹، جریان ترافیک را به صورت نمادین مشاهده می‌کنید که دستگاه‌ها برای دریافت سرویس از Access Point مرکزی استفاده می‌کنند، که نام SSID آن هم MyNetwork در نظر گرفته شده و دستگاه‌های که در شکل وجود دراند باید به این نام متصل شوند.



شکل ۴-۹ بررسی BSS

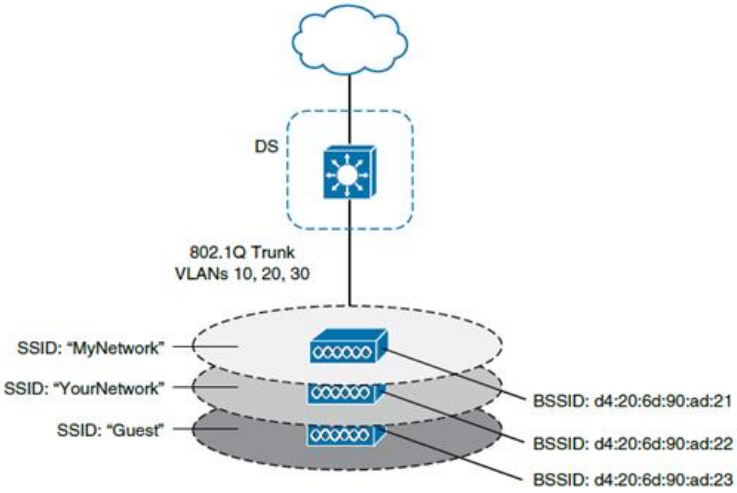
توجه داشته باشید Access Point می‌تواند هم از طریق سیم و هم بی‌سیم به شبکه اصلی سازمان متصل شود و از آن طریق به دستگاه‌های BSS سرویس ارائه دهد که شکل ۵-۹ را مشاهده کنید، توجه داشته باشید که هر SSID را به یک VLAN خاص تخصیص دهید تا کنترل آن راحت تر باشد.

www.takbook.com



شکل ۵-۹ بررسی BSS

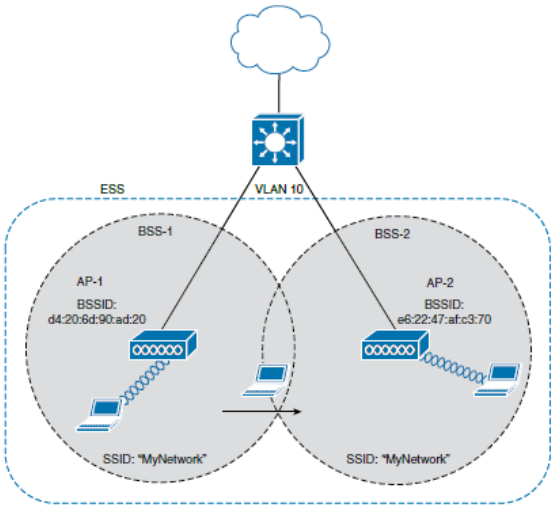
همانطور که در شکل ۶-۹ مشاهده می‌کنید سه VLAN با شماره‌های 10,20,30 ایجاد شده است که برای سه SSID مشخص شده است و به آنها تخصیص داده می‌شود.



شکل ۶-۹ بررسی BSS

اگر در یک سازمان با چندین طبقه مختلف حضور داشته باشید، اصولاً یک Access Point در چندین طبقه کارایی ندارد و سیگنال‌ها در فاصله مشخص به دستگاه‌ها نمی‌رسد و برای حل این مشکل باید از چند Access Point دیگر برای این کار استفاده کرد که دارای SSID یکسان باشند و در یک VLAN قرار داشته باشند که شکل آن را در زیر مشاهده می‌کنید.

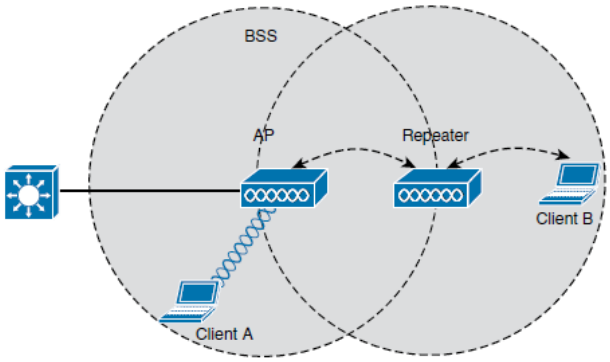
www.takbook.com



شکل ۷-۹ بررسی BSS

دستگاه Repeater

یک Access Point چندین متر مشخص را بسته به نوع سیستم آن پشتیبانی می‌کنید و برای اینکه از مناطق بیشتری پشتیبانی کند می‌توان از دستگاه Repeater استفاده کرد که شکل ۸-۹ در مورد این موضوع است.



شکل ۸-۹ دستگاه Repeater

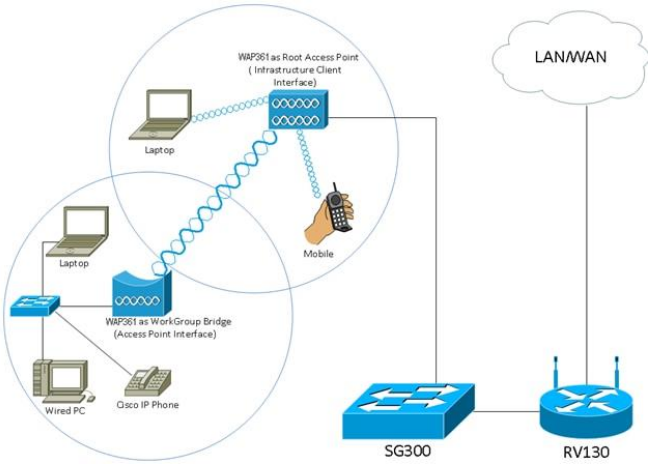
در شکل ۹-۹، یک دستگاه Repeater را مشاهده می‌کنید که دارای ورودی LAN و آداپتور برق است.

www.takbook.com

شکل ۹-۹ دستگاه Repeater

دستگاه Workgroup Bridge

این نوع دستگاه‌ها به سیستم‌هایی که توانایی متصل شدن به سیستم‌های بی‌سیم را ندارند کمک می‌کند تا به این شبکه متصل شود، در شکل ۱۰-۹، یک Access Point با نام WAP361 را مشاهده می‌کنید که دستگاه‌های Laptop و Mobile به آن متصل شده‌اند اما دستگاه‌های دیگر توانایی متصل شدن به این Access Point را ندارند و توسط یک دستگاه Workgroup Bridge که به یک سوئیچ متصل است به آن Access Point متصل می‌شوند.



شکل ۱۰-۹ دستگاه Workgroup Bridge

در کل دو نوع دستگاه Workgroup Bridge وجود دارد:

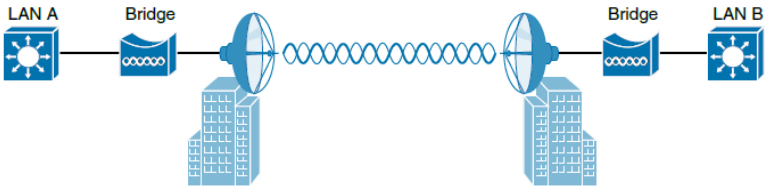
۱- Universal workgroup bridge (uWGB) که یک دستگاه بی‌سیم را به یک دستگاه سیمی متصل می‌کند.

www.takbook.com

۲- Workgroup bridge (WGB) که یک دستگاه بی‌سیم را به چند دستگاه سیمی متصل می‌کند و این نوع دستگاه‌ها مختص شرکت سیسکو هستند.

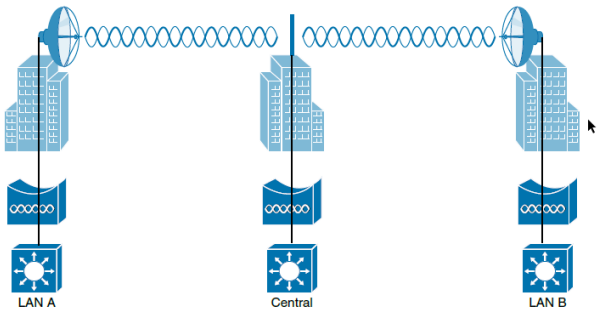
دستگاه Outdoor Bridge

این نوع شبکه‌ها برای ارتباط دو ساختمان در یک شهر استفاده می‌شود که این کار توسط آنتن در هر ساختمان انجام می‌شود که برای اینکه سیسگنال‌ها در یک جهت کنترل شوند از دستگاه‌های bridges استفاده می‌کنند، در شکل ۱۱-۹، یک شبکه‌ی Point to Point را مشاهده می‌کنید.



شکل ۱۱-۹ دستگاه Outdoor Bridge

در شکل ۱۲-۹، یک شبکه‌ی Point to MultiPoint را مشاهده می‌کنید، که در آن سایت یا ساختمان مرکزی از یک آنتن چند کاره یا همه‌کاره برای ارتباط با نقطه‌های مختلف مثلاً در یک شهر استفاده می‌کند و ساختمان‌هایی که قرار است به این ساختمان متصل شوند باید از یک آنتن جهت‌دار استفاده کنند.

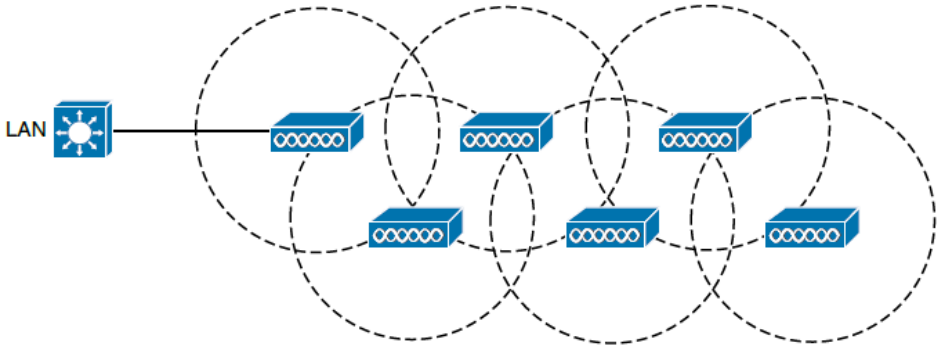


شکل ۱۲-۹ دستگاه Point to MultiPoint

شبکه Mesh

زمانی از این شبکه استفاده می‌شود که محدوده‌ی جغرافیایی بسیار گسترده باشد، در این نوع شبکه از Access Pointهای متعدد کمک گرفته می‌شود تا بتوانند همدیگر را پوشش دهند، به مانند شکل ۱۳ -۹، دستگاه‌های Access Point به صورت زنجیره‌هایی به هم متصل شده‌اند.

www.takbook.com



شکل ۹-۱۳ شبکه Mesh

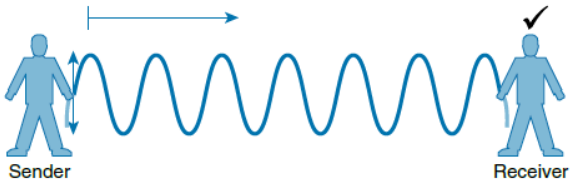
۹-۲ بررسی اجمالی RF

زمانی که دو دستگاه از طریق کابل، یک سیگنال را به همدیگر ارسال می‌کنند، این کار به راحتی انجام می‌گیرد، اما در دستگاه‌های بی‌سیم این کار امکان ندارد چون هیچ کابلی در میان نیست و سیگنال را نمی‌تواند انتقال دهد، پس چگونه می‌توان سیگنال را در هوای آزاد انتقال داد؟

به شکل ۹-۱۴، توجه کنید فرستنده یا همان Sender برای اینکه به گیرنده یا همان Reciver پیام ارسال کند یک طناب در دست خود دارد و یک طرف طناب را بالا نگه می‌دارد، ولی هیچ واکنشی از طرف گیرنده دریافت نخواهد کرد چون گیرنده چیزی متوجه نخواهد شد، خوب چه راه‌کاری برای حل این مشکل باید انجام داد؟

شکل ۹-۱۴ ارسال سیگنال

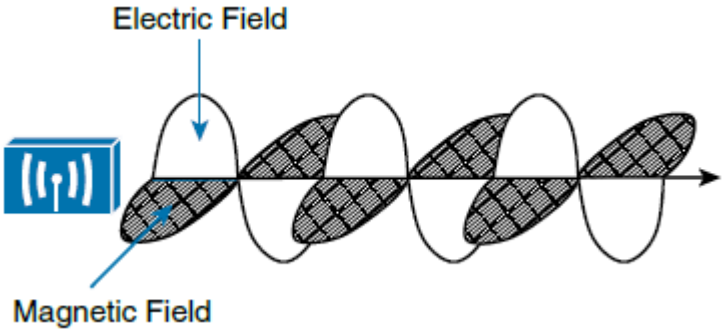
به مانند شکل ۹-۱۵، اگر فرستننده طناب را به صورت یک موج حرکت دهد، طرف دیگر که گیرنده باشد متوجه آن خواهد شد، این همان حرکتی است که دستگاه‌های WIFI انجام می‌دهند و باعث می‌شوند دستگاه‌های ما مانند موبایل امواج را دریافت کنند.



شکل ۹-۱۵ ارسال سیگنال

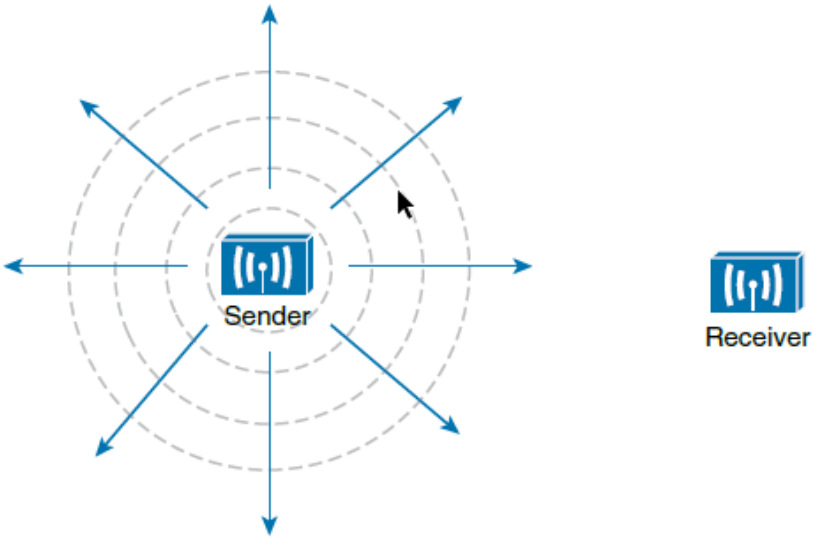
www.takbook.com

به شکل ۱۶-۹، توجه کنید، فرستنده‌ها (transmitter) امواج الکتریکی و مغناطیسی را به صورت موج ارسال می‌کند، که امواج الکتریکی در بالا و امواج مغناطیسی در پائین قرار دارد.



شکل ۱۶-۹ ارسال سیگنال

توجه داشته باشید که امواج الکترومغناطیسی اطلاعات را در جهت مختلف ارسال می‌کنند؛ مثلاً یک دستگاه WIFI را در نظر بگیرید که در خانه شما قرار دارد و امواج ارسال می‌کند، بهترین حالت آن این است که به مانند شکل ۱۷-۹، در تمام جهات امواج را ارسال کند، اما این کار در دنیای واقعی امکان پذیر نیست مثلاً در خانه چندین اتاق قرار دارد که درای دیوار هستند پس باعث می‌شود امواج به صورت شکل ۱۷-۹، پخش نشود.



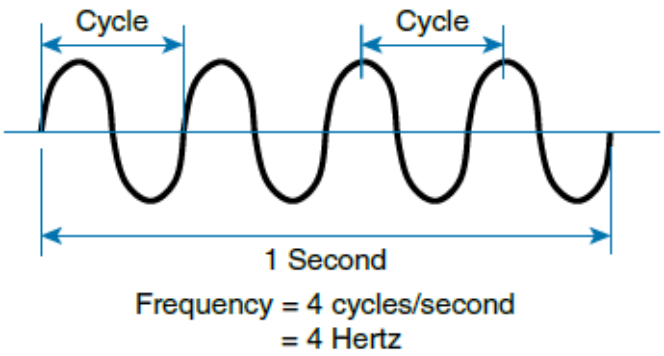
شکل ۱۷-۹ ارسال سیگنال

www.takbook.com

در شکل ۱۸-۹، یک Cycle را مشاهده می‌کنید، منظور از Cycle به تعداد دفعاتی است که موج به صورت سیسنوسی ارسال می‌شود و به این نکته توجه کنید که امواج از هر جایی که شروع می‌شود باید دقیقاً در یک فاصله مشخص قرار گیرد.

اصولاً به این Cycle فرکانس هم گفته می‌شود.

Hertz واحد اندازه‌گیری فرکانس است به یک سیکل کامل در یک ثانیه را Hertz می‌گویند، که در شکل ۱۸-۹، یک سیکل چهارتایی برابر 4 Hertz است.



شکل ۱۸-۹ ارسال سیگنال

در جدول ۱-۹، تعداد واحدهایی که در هر ثانیه انجام میشه دارای واحدهای مختلفی هستند که می‌توانید مشاهده کنید:

جدول ۱-۹ بررسی فرکانس

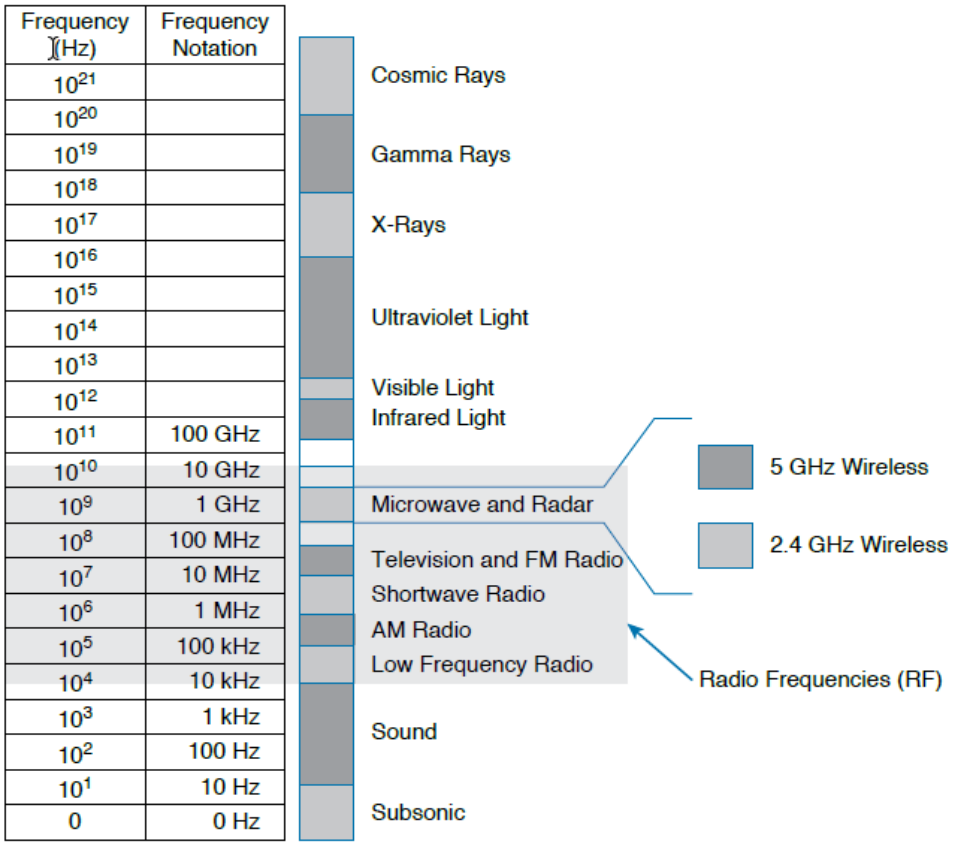
واحد	مخفف	معنی
Hertz	Hz	یک سیکل در ثانیه
Kilohertz	kHz	1000Hz
Megahertz	MHz	1000000Hz
Gigahertz	GHz	1000000000Hz

نکته: محدوده فرکانسی از صفر تا ۱۰به توان ۲۲ است، که پائین‌ترین فرکانس برای گوش انسان قابل شنیدن نیست و بالاترین فرکانس را می‌توان به اشعه X اشاره کرد.

در جدول ۲-۹، فرکانس‌های مختلف را مشاهده می‌کنید، مثلاً Wireless یا همان WIFI درهمان امواج Microwaveو Radar هستند که از 2.4GHZ تا 5GH گسترده هستند، فرکانس‌هایی رادیویی هم در زیر مشخص شده است که فرکانسی 3 kHz to 300 GHz را دارا می‌باشد، که شامل انواع مختلفی از ارتباط رادیویی ، از جمله فرکانس پایین مانند، رادیو AM ، رادیو موج کوتاه ، تلویزیون ، رادیو FM ، مایکروویو ، و رادار است.

جدول ۲-۹ بررسی فرکانس

www.takbook.com



در فرکانس، بعضی از محدوده‌ها دسته‌بندی می‌شوند که به آن BAND می‌گویند، مثلاً فرکانس وایرلس 2.4GHZ از 2.400 تا 2.4835GHz است.

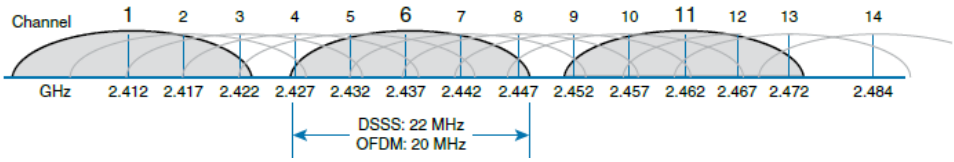
یا باند وایرلس خانگی (LAN) از 5.150 تا 5.825 GHz متغییر است که البته خود شامل ۴ دسته می‌شود که در زیر مشاهده می‌کنید:

5.150 to 5.250 GHz
5.250 to 5.350 GHz
5.470 to 5.725 GHz
5.725 to 5.825 GHz

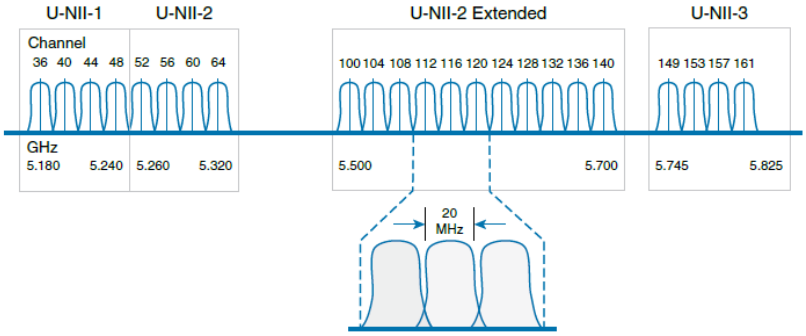
به چهار دسته‌ی بالا توجه کنید، یک محدوده‌ی کوچک بین 5.350 تا 5.470 بین دسته‌ی دوم و سوم وجود دارد که نمی‌توان آن را به عنوان محدوده وایرلس استفاده کرد.

جالب اینجاست که باند 5GHz می‌تواند چندین باند کوچک را در خود جای دهد، در دو شکل ۱۹-۹ و ۲۰-۹، طرح کانال‌ها را برای باند 2.4 و 5GHz نشان می‌دهد.

www.takbook.com



شکل ۱۹-۹ ارسال سیگنال



شکل ۲۰-۹ ارسال سیگنال

فرکانس‌های 2.4 GHz با 5GHz تفاوت‌های متفاوتی دارد، اصولاً از فرکانس 2.4GHz برای مکان‌هایی عمومی و شلوغ استفاده می‌شود، مثلاً اگر بخواهید درب پارکینگ خود را باز کنید از این باند استفاده خواهد شد.

اما فرکانس 5GHz برای ارتباط دو موبایل با هم کاربرد دارد، مثلاً در موبایل‌های امروزی با نرم‌افزار SHAREit برای انتقال اطلاعات استفاده می‌شود که این کار به علت انتقال فایل‌ها با حجم بالا در این فرکانس انجام می‌شود و مشکل آن این است که در فاصله زیاد پاسخگو نخواهد بود و یا اینکه اگر بر سر راه آن، موانع وجود داشته باشد با مشکل روبرو خواهد شد.

برای داخل خانه سعی کنید مودم‌های WIFI خود را بر روی 5GHz قرار دهید تا از امواج مضر 2.4 GHz دور باشید.

با پیشرفت و توسعه WIFI استانداردهای جدیدی برای آن ارائه شده است که قبلاً این استاندارد فقط 802.11 بوده است اما به مرور زمان این استاندارد دست‌خوش تغییراتی شده است که در جدول ۳-۹، آن مشاهده می‌کنید:

همانطور که مشاهده می‌کنید هر یک از استانداردها دارای سرعت‌های محتلفی هستند که در باند فرکانسی خاص خود کار می‌کنند، مثلاً 802.11ax که آخرین استاندارد در این زمینه در سال ۲۰۱۹ است در هر دو فرکانس 2.4 تا 5GHz کارایی دارد و دارای سرعت ۴ برابری از استاندارد 802.11ac است که یک سرعت باورنکردنی را به شما ارائه می‌دهد.

www.takbook.com

جدول ۳-۹ سرعتهای مختلف امواج

Amendment	2.4 GHz	5 GHz	Max Data Rate	Notes
802.11-1997	Yes	No	2 Mbps	The original 802.11 standard ratified in 1997
802.11b	Yes	No	11 Mbps	Introduced in 1999
802.11g	Yes	No	54 Mbps	Introduced in 2003
802.11a	No	Yes	54 Mbps	Introduced in 1999
802.11n	Yes	Yes	600 Mbps	HT (high throughput), introduced in 2009
802.11ac	No	Yes	6.93 Gbps	VHT (very high throughput), introduced in 2013
802.11ax	Yes	Yes	4x 802.11ac	High Efficiency Wireless, Wi-Fi6; expected late 2019; will operate on other bands too, as they become available

توجه داشته باشید دستگاه‌های کاربران دارای استانداردهای مختلفی هستند و برای ارتباط با AP یا همان Access Point باید دارای یک استاندارد مشترک باشند تا بتوانند به هم متصل شوند.

در شکل ۲۱-۹، یک مودم Asus DSL-N16 را مشاهده می‌کنید:

شکل ۲۱-۹ *ارسال سیگنال*

این مودم دارای مشخصات زیر است:

- Wi-Fi Data Rate

802.11b : 1, 2, 5.5, 11 Mbps
802.11g : 6,9,12,18,24,36,48,54 Mbps
802.11n : up to 300 Mbps

www.takbook.com

- Operating Frequency
2.4GHz

باند فرکانسی آن 2.4 GHz است و در شبکه‌های 802.11 b,g,n کارایی دارد.

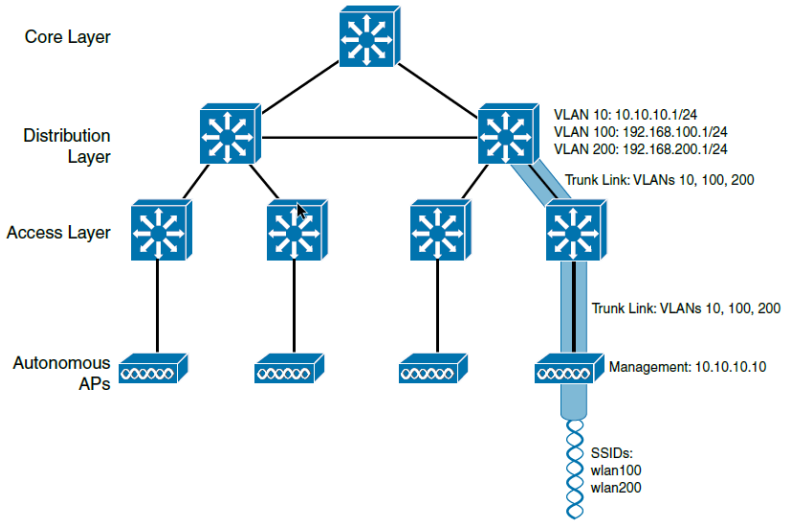
۹-۳ بررسی معماری Access Point

اصولاً کارکرد اصلی یک Access Point انتقال داده‌های بی‌سیم از هوا به شبکه‌ی سیمی است؛ یک access Point می‌تواند، پذیرای انواع دستگاه‌های بی‌سیم باشد به گونه‌ای که این دستگاه‌ها مانند دستگاه‌های با سیم می‌توانند عضو شبکه‌ی دومین شوند و از منابع آن شبکه استفاده کنند.

Access Pointها به عنوان مرکز اصلی یک شبکه بی‌سیم تمام اتصالات را مدیریت و بررسی می‌کنند و دسترسی کاربران به آن را کنترل می‌کنند.

Access Point به صورت خود مختار عمل می‌کند، این دستگاه با سیم به شبکه اصلی متصل می‌شود و بعد از گرفتن اطلاعات لازم مانند آدرس IP، Defualt Gateway به کاربران در آن شبکه سرویس می‌دهند.

در شکل ۲۲-۹، یک شکل کلی از یک شبکه را مشاهده می‌کنید که در آن از چند AP استفاده شده است.



شکل ۲۲-۹ ارسال سیگنال

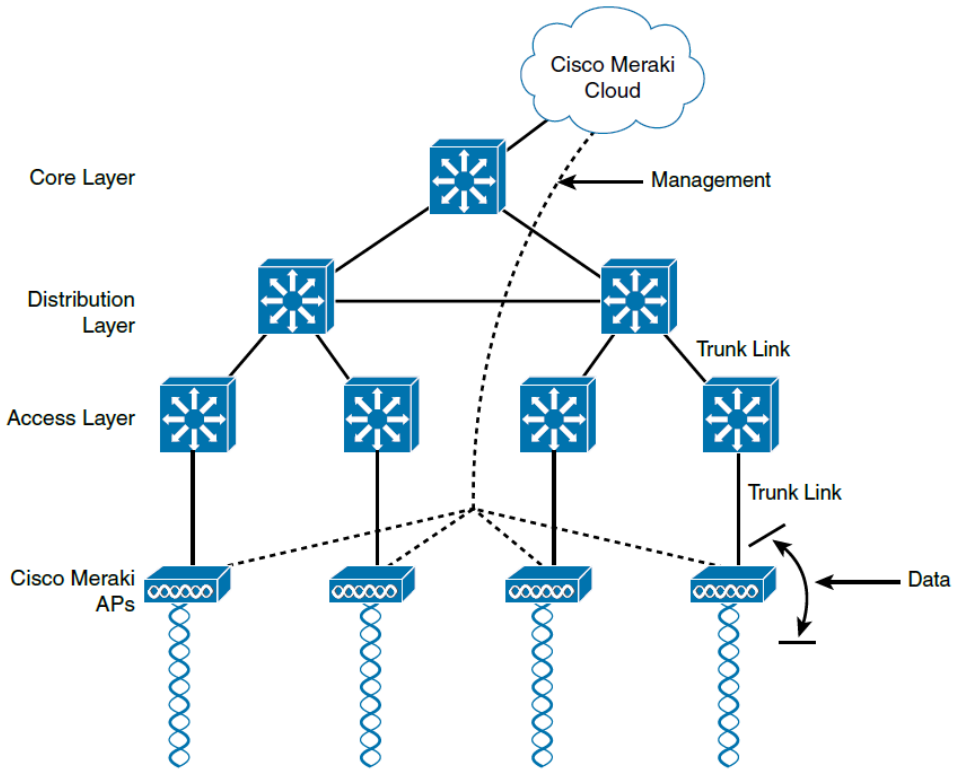
www.takbook.com

۹-۴ معماری AP مبتنی بر Cloud

شما اگر دارای یک هتل باشید برای اینکه به مشتریان خود سرویس اینترنت ارائه دهید باید از Access Pointهای متعددی با تنظیمات یکسان در جای جای هتل استفاده کنید تا بتوان به مشتریان خدمات ارائه داد، اما هیچ فکرش را کردید که چطوری می‌شود این تعداد بالا از AP را مدیریت کرد؟

سیسکو برای اینکه این کار انجام شود، راه حلی را با نام Cisco Meraki معرفی کرده که در آن تمام دستگاه‌های شبکه به صورت همزمان می‌توانند پیکربندی و مدیریت شوند، در زیر یک نمای کلی از این موضوع را مشاهده می‌کنید.

همان‌طور که در زیر مشاهده می‌کنید، این نوع رویکرد به شما این امکان را می‌دهد که بتوانید به راحتی و از راه دور با امنیت کامل تمام دستگاه‌های وایرلس را مدیریت کنید، یعنی نیاز به حضور فیزیکی شما در محل نیست.



شکل ۹-۲۲ معماری AP مبتنی بر Cloud

دو کار مهم دستگاه‌های Meraki در شبکه‌های وایرلس عبارت‌اند از:

۱- control plane

کنترل، پیکربندی و نظارت بر روی Access Point که یکی از مهمترین کاره‌های Meraki است.

۲- data plane

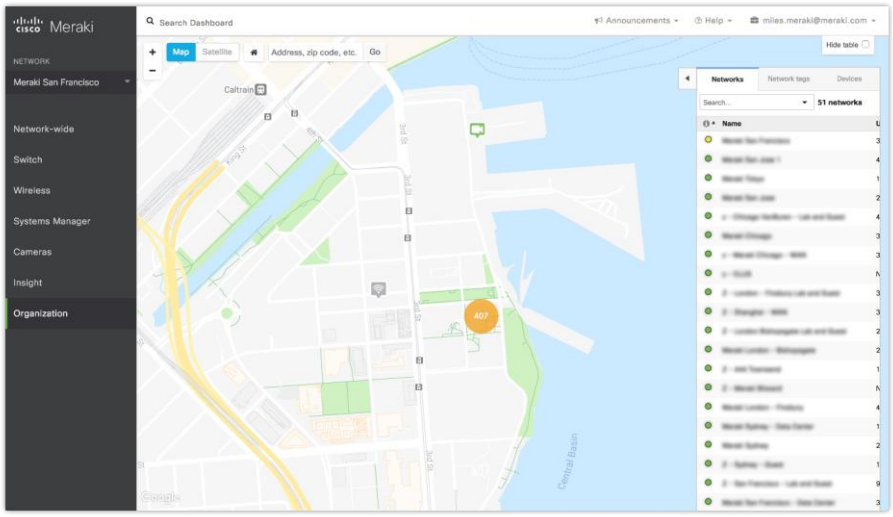
www.takbook.com

نظارت بر روی ترافیک کاربران نهایی که از Access Point استفاده می‌کنند.

در شکل ۲۳-۹، یک نمونه از دستگاه Meraki را مشاهده می‌کنید، که قیمت آن در ایران به نسبت بالا است.

شکل ۲۳-۹ Meraki

در شکل ۲۴-۹، یک نما از داشبورد مدیریتی Meraki را مشاهده می‌کنید:



شکل ۲۴-۹ کنترل پنل Meraki

۹-۵ معماری Split-MAC

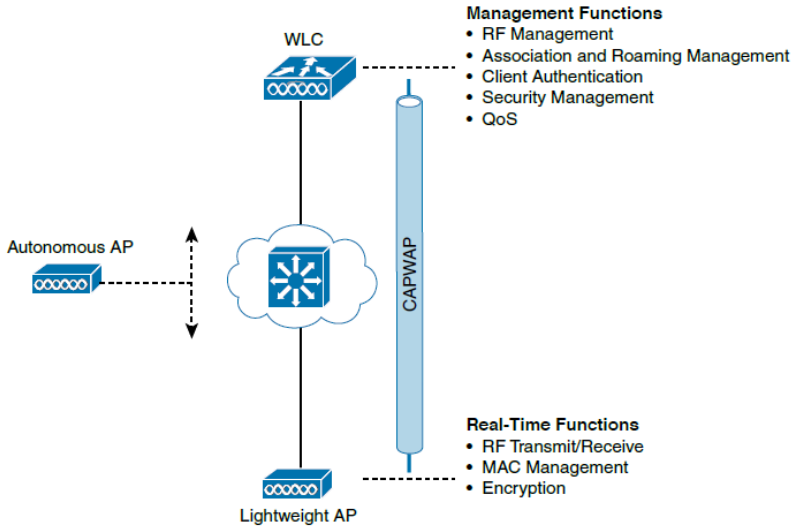
همیشه این موضوع را به یاد داشته باشید که یک Access Point به صورت مستقل عمل می‌کند و این موضوع می‌تواند کار مدیریت آن را سخت کند، شما به عنوان یک مدیر در شبکه باید این توانایی را داشته باشید که بتوانید آنها را مدیریت کنید، از مشکلاتی که یک AP می‌تواند ایجاد کند این است که با دیگر APها تداخل امواج ایجاد کند و همین موضوع باعث می‌شود تا AP به درستی کار نکند و برای اینکه از تداخل بین APها جلوگیری کنید باید توانایی این را داشته باشید تا سطح قدرت آنها را کنترل کنید.

www.takbook.com

یکی از مشکلات دیگری که در بحث AP می‌توان گفت امنیت آن است که هر AP دارای ویژگی‌ها امنیتی مجزا است و باید به درستی پیکربندی و کنترل شود.

برای اینکه بتوانیم هر AP را به درستی مدیریت کنیم باید آنها را به مکان‌ها مشخص انتقال دهیم، در زیر یک AP را مشاهده می‌کنید که فعالیت‌های آن به دو بخش تقسیم شده است، در قسمت بالا مدیریت توابع و در قسمت پائین فرایندهای Real–Time را مشاهده می‌کنید.

توجه داشته باشید که ارتباط بین AP و WLC به صورت امن انجام می‌پذیرد این امنیت توسط پروتکل CAPWAP صورت می‌گیرد.



شکل ۲۵-۹ Meraki

در قسمت پائین یعنی Real-Time برنامه از طریق MAC address یا همان لایه‌ی Media Access Control با کاربران در ارتباط است و بسته‌های عبوری بین آنها رمزنگاری می‌شود. و شامل ارسال و دریافت فریم‌های 802.11 است.

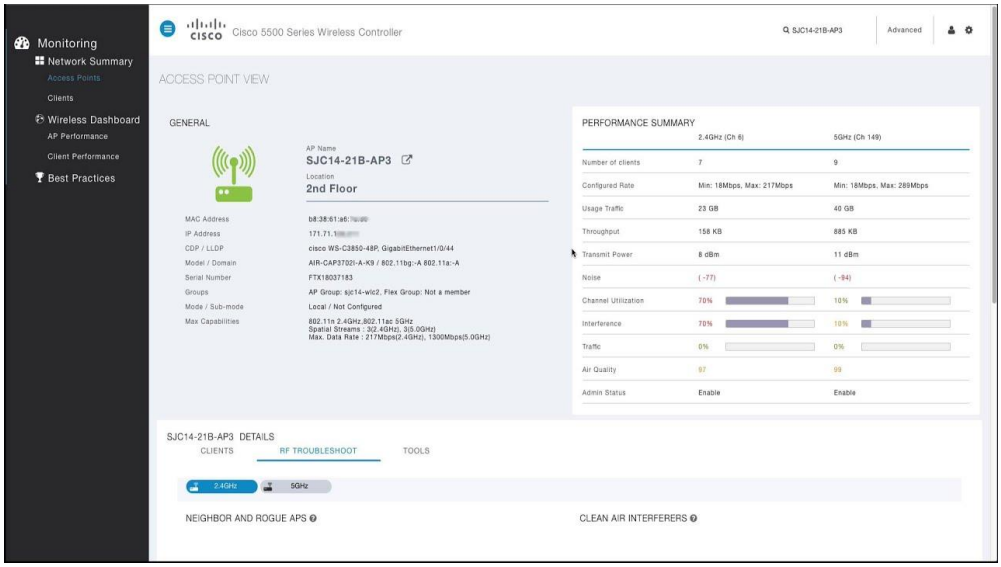
در قسمت بالا یعنی Management Functions با یک کنترلر WLC (Wireless LAN Controller) انجام می‌شود، این نوع دستگاه‌ها می‌توانند تمام Access Pointهای موجود در یک شبکه را مدیریت کنند، با این دستگاه می‌توانید گزارش‌گیری، رفع اشکال، هشدارها و ... را مشاهده کنید.

در شکل ۲۵-۹؛ یک دستگاه سیسکو Cisco 3504 Wireless Controller را مشاهده می‌کنید:

www.takbook.com

شکل ۹-۲۵ *Meraki*

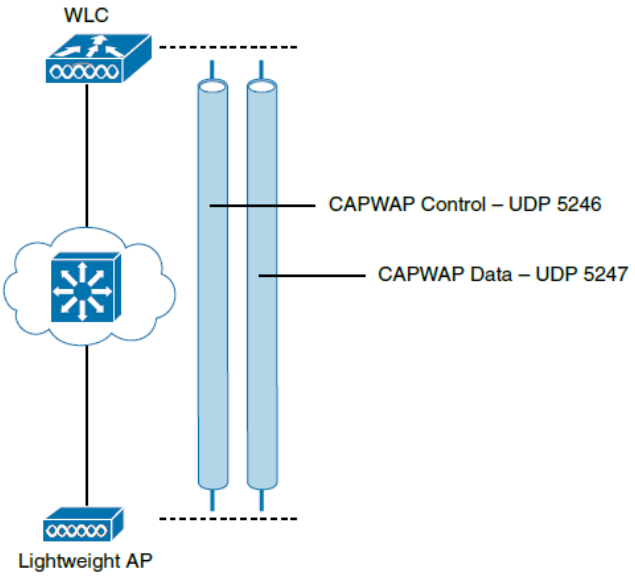
در شکل ۹-۲۶، می‌توانید یک نمای کلی از داشبورد مدیریتی WLC را مشاهده می‌کنید:



شکل ۹-۲۶ *Meraki*

در شکل ۹-۲۷، پروتکل CAPWAP را مشاهده می‌کنید که به صورت دو تونل مجزا کار می‌کنند، در CAPWAP Control از پورت UDP 5246 استفاده می‌شود که ارتباط بین AP و WLC را رمزنگاری می‌کند و به خاطر همین موضوع هر AccessPoint با WLC مختص به خود ارتباط برقرار می‌کند و مهاجم نمی‌تواند به Access Point دسترسی داشته باشد، در CAPWAP Data که با پورت UDP 5247 کار می‌کند اطلاعات کاربران را رمزنگاری می‌کند، به این نکته توجه کنید که به صورت پیش‌فرض رمزنگاری غیر فعال است و باید آن را فعال کنید با فعال کردن آن بسته‌های عبوری توسط(DTLS) Datagram Transport Layer Security امن خواهد شد.

www.takbook.com



شکل ۲۷-۹ Meraki

یکی دیگر از راه‌های ایجاد امنیت بین AP و WLC استفاده از گواهینامه‌های امنیتی است که این دو دستگاه باید گواهینامه‌های x.509 را برای هم تصدیق و تایید کنند که این کار باعث می‌شود که مهاجم نتواند AP جعلی را در WLC ثبت کند.

در زیر کارهایی که یک WLC انجام می‌دهد را مشاهده می‌کنید:

- Dynamic channel assignment

این قابلیت این امکان را می‌دهد که سیگنال‌های RF را به صورت اتوماتیک بر اساس APهایی که در نقطه‌های مختلف قرار دارد مدیریت کند.

- Transmit power optimization

بهینه‌سازی قدرت انتقال، در این قسمت WLC به صورت خودکار قدرت انتقال هر AP را بر اساس نقطه‌ای که حضور دارد مشخص می‌کند تا باعث تداخل با دیگر APها نشود.

- Self-healing wireless coverage

یکی از ویژگی‌های مهم WLC این است که اگر در یک نقطه یک AP ازکار بیفتد، WLC این قابلیت را دارد که سیسگنال‌های APهای اطراف آن را قدرتمندتر کند تا بتوانند نبود آن AP را پوشش دهند.

- Flexible client roaming

یک شرکت را درنظر بگیرید که دارای چند طبقه است و در هر طبقه یک AP وجود دارد و مشتری که در طبقه‌ی اول به AP متصل شده است وقتی به طبقه‌ی پنجم مراجعه کند این قابلیت باعث می‌شود بدون آنکه مشتری متوجه شود خیلی سریع AP آن تغییر کند.

- Dynamic client load balancing

در این ویژگی اگر از چند AP در یک نقطه جغرافیایی استفاده شود کاربران می‌توانند به هر کدام از آنها متصل شوند تا با این کار بار کاری بین APها پخش شود.

www.takbook.com

- RF monitoring

یکی دیگر از ویژگی‌های WLC مدیریت کردن RF در هر AP است که با این کار از تداخل، نویز و سیسگنال‌های دیگران جلوگیری کرد.

- Security management

یکی از بهترین ویژگی‌های WLC ایجاد امنیت در ارتباط با APها است، به کاربران این اجازه را می‌دهد تا بتوانند از یک سرویس دهنده‌ی DHCP معتبر IP دریافت کنند.

- Wireless intrusion protection system

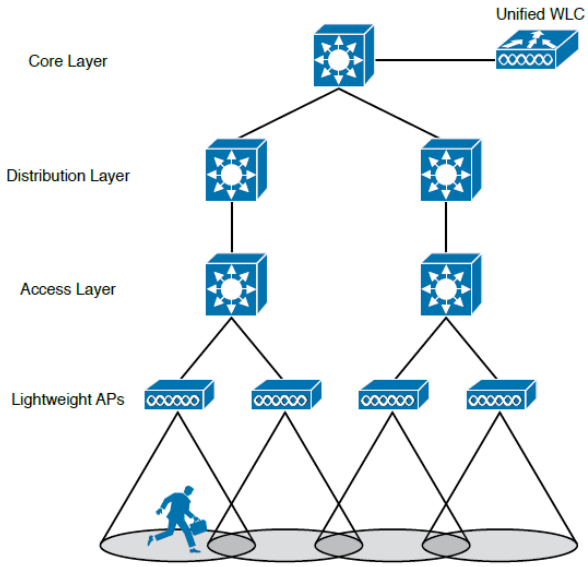
با استفاده از سیستم جلوگیری از نفوذ می‌تواند بر روی داده‌های مشتری یا همان کاربرن نظارت داشته باشد و از داده‌ها و ارتباطات مخرب جلوگیری کند.

۹-۶ بررسی کارکرد Wireless LAN Controller

فرض کنید می‌خواهید WLC را برای پشتبانی از چند AP به کار ببرید، آیا از خود پرسیدید WLC باید در کدام نقطه از شبکه سازمان قرار بگیرد؟

یک از مهمترین بحث‌هایی که در این مورد وجود دارد همین است، یعنی WLC را باید در چه نقطه‌ای از شبکه قرار دهیم.

یک راه این است که WLC را به مانند شکل ۲۸-۹، در مرکز Datacenter یا جایی که اینترنت قرار است به کاربران داده شود قرار دهیم.



شکل ۲۸-۹ Meraki

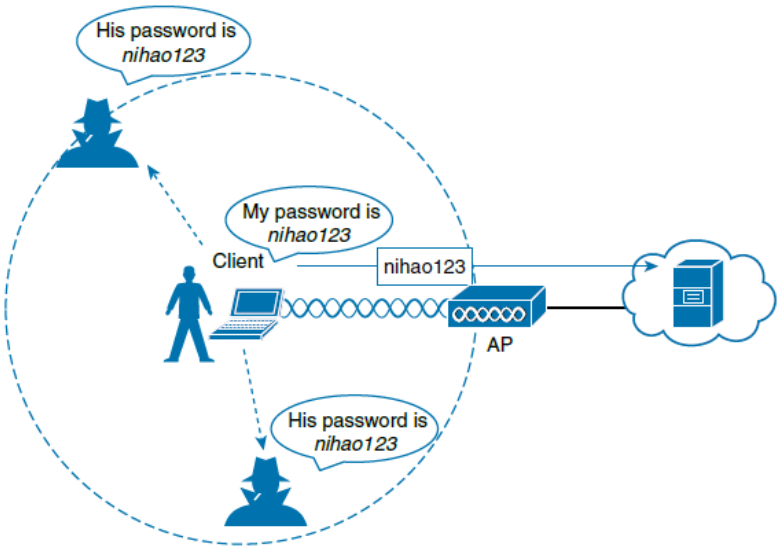
www.takbook.com

۹-۷ امنیت در شبکه‌های بی‌سیم

یکی از بحث‌های مهم در شبکه‌های بی‌سیم حفظ امنیت آن است که باید به درستی و با برنامه‌ریزی کامل انجام شود، همانطور که قبلاً هم بررسی کردیم هر کاربری با هر دستگاه وایرلسی می‌تواند به شبکه AP وصل شود و از خدمات آن استفاده کند، اگر این فرد یک کاربر معمولی نباشد و قابل اعتماد نباشد چه کاری باید انجام داد تا از دسترسی غیرمجاز آن به شبکه جلوگیری شود.

شکل ۲۹-۹، را درنظر بگیرد، که یک AP، با رمز عبور (nihao123) به Client سرویس ارئه می‌دهد، اگر چند نفر دیگر در اطراف آن AP قرار داشته باشند با Capture کردن اطلاعات می‌توانند به این رمز دست پیدا کنند و به AP متصل شوند و از منابع استفاده کنند که این می‌تواند بسیار خطرناک باشد و شبکه‌ی شما را زیر سوال ببرد.

چگونه می‌توانیم داده‌های ارسالی بین Client و AP را محافظت کنیم؟



شکل ۲۹-۹ حفظ اطلاعات

استاندارد 802.11 چارچوبی از مکانیسم‌های امنیتی ارائه کرده که می‌توانیم آنها را برای ایجاد امنیت بهتر و کاملتر استفاده کنیم.

۹-۸ احراز هویت (Authentication)

برای استفاده از شبکه‌ی بی‌سیم مشتریان یا کاربران نهایی (BSS) باید یک SSID که همان نام وایرلس است را پیدا کنند و برای دریافت خدمات به آن متصل شوند که این متصل شدن تابع شرایطی هست که آن را بررسی می‌کنیم، کاربران قبل از متصل شدن باید اول از همه مورد تایید قرار بگیرند، دلیل آن هم

www.takbook.com

این است که هر کسی نتواند با متصل شدن به شبکه‌ی بی‌سیم به اطلاعات شرکت دست پیدا کند، اگر کاربر مورد تایید باشد آن وقت با خیال آسوده‌تری می‌توانیم به ان خدمات ارائه دهیم.

۹-۹ روش‌های تایید اعتبار کاربران در شبکه‌ی بی‌سیم

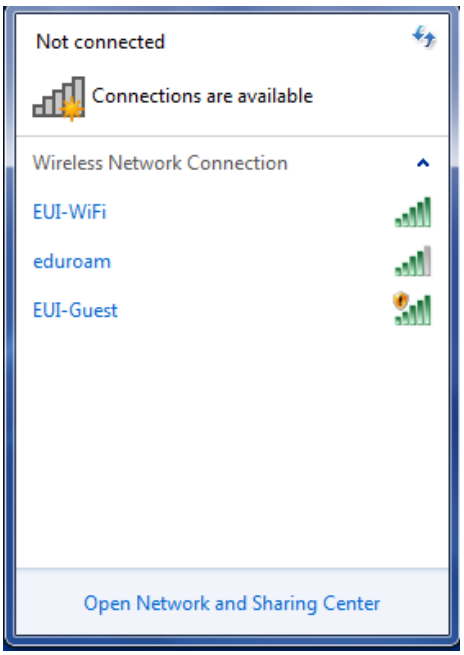
برای اینکه به کاربران خود اجازه‌ی دسترسی به شبکه‌ی بی‌سیم را دهیم راه‌های مختلفی وجود دارد که در این قسمت با هم بررسی می‌کنیم.

Open Authentication

استاندارد 802.11 برای تایید اعتبار مشتری دو استاندارد را ارائه داده است که یکی Open Authentication و دیگری WEP است.

Open Authentication دسترسی آزاد به WLANیا همان شبکه‌ی بی‌سیم را ارائه می‌دهد و مشتری می‌تواند به راحتی با مشاهده SSID مربوط به یک AP به آن متصل شود و از منابع آن استفاده کند که این نوع استاندارد در مکان‌های عمومی که امنیتی مد نظر نیست بیشتر استفاده می‌شود.

در اکثر سیستم‌عامل‌ها این نوع شبکه‌ها را با یک علامت اخطا و یا تعجب مشخص می‌کنند که در شکل ۳۰-۹، این موضوع برای شبکه‌ی EUI-Guest مشخص شده است.



شکل ۳۰-۹ وایرلس بدون امنیت

www.takbook.com

WEP

Wired Equivalent Privacy یا همان WEP یک پروتکل رمزنگاری است که در استاندارد 802.11b تعریف شده است، این پروتکل در سال ۱۹۹۷ معرفی شده است.

پروتکل امنیتی WEP از الگوریتم رمزنگاری RC4 برای ایجاد یک Frame داده‌ی بی‌سیم خصوصی و پنهان استفاده می‌کند که می‌تواند امنیت داده را حفظ کند.

این الگوریتم از یک رشته حروف برای ایجاد کلید رمزنگاری استفاده می‌کند، یعنی اینکه مشتری می‌تواند با وارد کردن این Key یا همان کلید به AP متصل شود.

در کل WEP یک روش امنیتی که با shared-key شناخته می‌شود و یک روش قدیمی برای محرمانگی اطلاعات است، هر چند امروزه کمتر کسی از آن استفاده می‌کند، توجه داشته باشید که کلیدهای WEP می‌توانند بین ۴۰ تا ۱۰۴ بیت باشند.

همانطور که گفتیم این پروتکل ضعیف است و در سال ۲۰۰۱ تعدادی از مشکلات آن شناسایی شد که باعث می‌شد دستگاه‌های بی‌سیم به راحتی هک شوند و در دسترس افراد سودجو قرار بگیرند، برای همین تا سال ۲۰۰۴ روش‌هایی برای پیدا کردن رفع مشکلات و پیدا کردن پروتکل امن‌تر ارائه شد.

نکته آخر اینکه روش WEP به صورت رسمی یک روش ضعیف گزارش شده و امروزه برای تامین امنیت شبکه‌ی بی‌سیم به هیچ عنوان توسعه نمی‌شود.

802.1x/EAP

برای ایجاد امنیت بیشتر روشی تحت عنوان Extensible Authentication Protocol یا EAP ارئه شده است که این خود یک پروتکل مانند WEP نیست بلکه کمک کننده پروتکل‌های امنیتی برای ایجاد امنیت بیشتر است در اصل یک فرآیند در دل پروتکل‌های دیگر است.

روش EAP سه شرط در فرآیند احراز هویت تعریف می‌کند که به صورت زیر است:

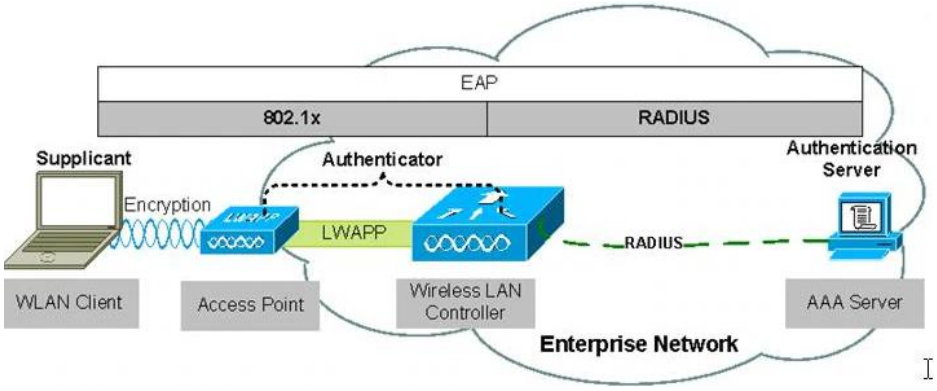
Supplicant : به دستگاه کاربر یا مشتری گفته می‌شود که درخواست دریافت خدمات از AP را دارد.

Authenticator : که اصولاً نحوه دسترسی به شبکه‌ی بی‌سیم را مشخص می‌کند، مانند Access Point.

Authentication Server : این دستگاه هم اجازه‌س استفاده از شبکه را به Supplicant می‌دهد.

در شکل ۳۱-۹، نحوه‌ی ارتباط این سه قسمت را با هم مشاهده می‌کنید.

www.takbook.com



شکل ۳۱-۹ پروتکل EAP

در زیر روش‌های تایید هویت مبتنی بر EAP را مشاهده می‌کنید:

LEAP

برای انجام رفع نقاط ضعف پروتکل WEP شرکت سیسکو روش Lightweight EAP یا همان LEAP را معرفی کرد، در این روش کاربر و سرور هر دو همدیگر را احراز هویت می‌کنند، یعنی به این صورت که کاربر یک رشته مشخص را به سرور ارسال می‌کند و سرور آن رشته را با Shared Secret خود هش می‌کند و برای کاربر ارسال می‌کند، اگر رشته مورد نظر با Shared Secret کاربر که قبلاً برای آن مشخص شده یکی باشد سرور مورد تایید کاربر قرار می‌گیرد.

در مرحله دوم سرور هم یک رشته برای کاربر ارسال می‌کند و کاربر آن را با رمزی که دارد هش می‌کند و برای سرور ارسال می‌کند سرور رشته‌ی ارسالی را با رمز عبور کاربر مقایسه می‌کند و در صورت تایید کاربر هم مورد تایید سرور قرار می‌گیرد و بدین ترتیب ارتباط دو طرفه برقرار می‌شود.

EAP-FAST

سیسکو روش دیگری را برای ایجاد امنیت بهتر با عنوان EAP–Flexible Authentication via Secure Tunneling یا EAP-FAST معرفی کرد که از روش قبلی آن بسیار قویتر و امن‌تر است.

در این روش از Tunnel استفاده می‌شود که در سه فاز انجام می‌گیرد:

فاز 0 :

در فاز صفر یک فایل به صورت دستی یا اتوماتیک بر روی کلاینت مشتری نصب می‌شود، این فایل یک PAC یا Protected Access Credential است که یک اعتبارنامه است برای احراز هویت و به مشتری داده می‌شود.

فاز 1 :

در این مرحله اعتبارنامه یا همان PAC بین کاربر و سرور مورد بررسی قرار می‌گیرد و در صورت تایید، یک Tunnel بین کاربر و سرور ایجاد می‌شود.

www.takbook.com

فاز 2 :

در مرحله آخر هم کاربر نهایی با استفاده از تونل ایجاد شده TLS مورد تایید قرار می‌گیرد.

توجه داشته باشید ایجاد فایل‌های PAC که یک اعتبارنامه است توسط سرورRadius انجام می‌گیرد که در این نوع شبکه‌ها مورد نیاز است.

PEAP

مانند روش EAP-FAST است، روش Protected EAP یا PEAP که کپسوله‌کردن اطلاعات درون پروتکل TLS را پشتبانی می‌کند.

یکی ار روش‌های ایجاد امنیت در آن استفاده از Certificate است که بر روی سیستم‌های کلاینت مشتری نصب می‌شود، اگر چنانچه مشتری، دارای این گواهی یا همان Certificate نباشد باید از دو روش دیگر استفاده کند که شامل این دو مورد است:

MSCHAPv2 : پروتکل احراز هویت Microsoft Challenge Authentication Protocol version 2

GTC: Generic Token Card یک دستگاه سخت‌افزاری که کلمات عبور یک بار مصرف ایجاد می‌کند.

EAP-TLS

این استاندارد ساخت شرکت مایکروسافت است، در این نوع کاربر و سرور همدیگر را احراز هویت می‌کنند، در این روش از RSA Handshake استفاده می‌شود.

EAP-TLS یکی از امن‌ترین روش‌های احراز هویت برای شبکه‌ی بی‌سیم است، در این روش از Certificate و Smart Card هم استفاده می‌شود.

در این روش باید یک سرور ارئه دهنده‌ی گواهینامه CA پیاده‌سازی شود تا بتواند به کاربر و سرور Radius سرویس ارئه دهد.

نکته مهم این است که به خاطر وجود Certificate که باید بر روی تمام دستگاه‌های بی‌سیم نصب شود استفاده از آن زیاد فراگیر نیست، مثلاً دستگاه‌های بی‌سیم پزشکی قابلیت نصب Certficate را ندارند و نمی‌توانند از این روش استفاده کنند.

۹-۱۰ حریم خصوصی و روشهای یکپارچگی بی‌سیم

همانطور که در این فصل بیان کردیم، پروتکل WEP یک پروتکل امنیتی ضعیف بوده و دیگر برای استفاده توسعه نمی‌شود، باید روش‌های دیگری را هم برای رمزنگاری داده پیدا کنیم.

پروتکل TKIP

Temporal Key Integrity Protocol یا TKIP یک پروتکل با امنیت بالاتر به نسبت WEP است، این پروتکل برای ایجاد امنیت از MIC یا همان Message Integrity Check استفاده می‌کند، MIC یک الگوریتم کارآمد

www.takbook.com

است که یک مقدار Hash شده را در فریم ارسالی اضافه می‌کند تا از دستکاری فریم جلوگیری کند، در زیر روش‌های مختلفی که در TKIP استفاده می‌شود را بررسی می‌کنیم:

Time stamp : یک مهر زمانی است که به MIC اضافه می‌شود تا جلوی حملات replay attacks را بگیرد.

Sender's MAC address : MIC آدرس MAC فرستنده را به عنوان مدرک در Frame فرستنده درج می‌کند.

TKIP sequence counter : این ویژگی Frameهایی را که آدرس MAC یکتا ارسال می‌کنند را ضبط می‌کند تا در آینده از حملات احتمالی جلوگیری کند.

Key mixing algorithm : این الگوریتم یک کلید ۱۲۸ بیتی مجزا و یکتا را برای هر Frame در نظر می‌گیرد.

Longer initialization vector : افزایش اندازه‌ی initialization vector از ۲۴ بیت به ۴۸ بیت که این کار باعث جلوگیری از حملات brute-force می‌شود.

پروتکل CCMP

پروتکل Counter / CBC-MAC (CCMP) یک پروتکل امن‌تر از TKIP است، در این پروتکل از دو الگوریتم تشخیص استفاده می‌شود.

۱- AES
۲- Cipher Block Chaining Message Authentication Code (CBC-MAC)

AES یا همان Advanced Encryption Standard یک الگوریتم رمزنگاری پیشرفته است که توسط مؤسسه ملی استاندارد و فناوری آمریکا و دولت آمریکا ایجاد شده و به طور گسترده در سراسر جهان استفاده می‌شود، این روش یک روش امن تا به امروز است و در همه‌ی سیستم‌های امنیتی استفاده می‌شود.

توجه داشته باشید برای استفاده از پروتکل CCMP دستگاه‌های شبکه برای متصل شدن به AP باید دو الگوریتم AES و CBC-MAC را پشتیبانی کنند.

الگوریتم GCMP

پروتکل Galois / Counter Mode Protector (GCMP) یک مجموعه رمزنگاری شده است که چند برابر از الگوریتم CCMP امن‌تر است، این پروتکل از دو الگوریتم برای کار خود استفاده می‌کند:

۱- AES
۲- Galois Message Authentication Code یا GMAC

اصولاً پروتکل GCMP در WPA3 استفاده می‌شود که در ادامه به آن خواهیم پرداخت.

۱۱-۹ بررسی WPA, WPA2, and WPA3

در این قسمت می‌خواهیم بهترین روش‌های امنیتی را برای تنظیم کردن سیستم وایرلس را مشخص کنیم، در حال حاضر سه نسخه از احراز هویت با نام‌های WPA, WPA2, and WPA3 ایجاد شده که هر کدام از دیگری قویتر و بهتر شده است.

www.takbook.com

سایت https://www.wi-fi.org یک انجمن برای دنیای بی‌سیم است که در آن انواع روش‌های ارتباطی با توضیحات آن مشخص شده است که می‌تواند به شما کمک کند، تمام نسخه‌های بالا، اول در آزمایشگاه‌ها تست شدن و توسط همین انجمن مورد تایید قرار گرفتن و بعد از تایید دستگاه‌های بی‌سیم مانند AP یا WLC و... باید با این استانداردها هماهنگ شوند.

اولین نسخه از احراز هویت WIFI با نام WPA بود که با استاندارد 802.11i معرفی شد که از پروتکل TKIP برای رمزنگاری استفاده می‌کرد، اما در ادامه به خاطر ضعف‌هایی که WPA داشت نسخه‌ی دوم آن یعنی WPA2 معرفی شد که با دو الگوریتم قدرتمند AES و CCMP کار می‌کرد.

به مرور زمان برای اینکه قدرت کار افزایش پیدا کند در سال ۲۰۱۸ نسخه‌ی سوم آن یعنی WPA3 معرفی شد که دارای دو الگوریتم AES و GCMP بود.

در جدول ۴-۹، نسخه‌های مختلف احراز هویت را مشاهده می‌کنید که هر کدام دارای ویژگی‌های مختلف هستند.

جدول ۴-۹ نوع رمزنگاری

Authentication and Encryption Feature Support	WPA	WPA2	WPA3*
Authentication with Pre-Shared Keys?	Yes	Yes	Yes
Authentication with 802.1x?	Yes	Yes	Yes
Encryption and MIC with TKIP?	Yes	No	No
Encryption and MIC with AES and CCMP?	Yes	Yes	No
Encryption and MIC with AES and GCMP?	No	No	Yes

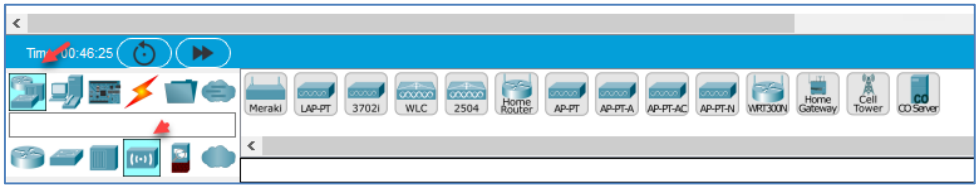
توجه داشته باشید هر سه نسخه WPA از دو حالت تایید مشتری یعنی Pre-Share Keys و 802.1x پشتیبانی می‌کنند، همانطور که می‌دانید یک رمز عبور یا همان کلید که در اینجا Pre-Share Keys یاد می‌شود وجود دارد که باید برای متصل شدن به AP آن را به کاربران خود بدهید، باید همیشه توجه کنید که این کلید را به افراد غیرمجاز ندهید.

۹-۱۲ اتصال به Acces Point سیسکو

خوب تا به اینجا انواع روش‌های احراز هویت و انواع دستگاه‌های موجود برای بحث بی‌سیم را بررسی کردیم و حالا می‌خواهیم به این دستگاه‌ها متصل شویم و تنظیمات خود را روی آن اعمال کنیم.

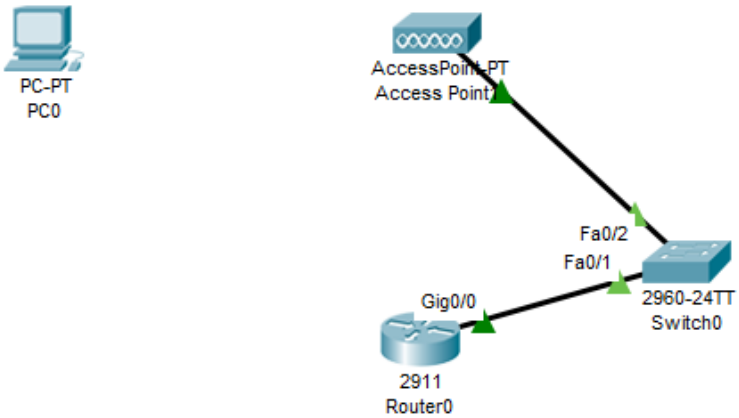
اگر به مانند شکل ۳۲-۹،وارد نرم‌افزار Packet Tracer شوید از قسمت Wireless می‌توانید انواع دستگاه‌های وایرلس مانند AP, Meraki و... را مشاهده کنید که می‌توانید از آنها در پروژه‌های خود استفاده کنید.

www.takbook.com



شکل ۳۲-۹ Packet Tracer

برای اینکه با Accee Point و دیگر وسایل بی‌سیم کار کنیم شکل۳۳-۹، را با هم بررسی می‌کنیم:



شکل ۳۳-۹ مثال وایرلس

یک روتر به همراه سوئیچ، AccessPoint-PT و یک PC را به صفحه اضافه کنید، برای اینکه به دستگاه‌های شبکه‌ی خود به صورت اتوماتیک IP اختصاص دهیم باید در روتر سرویس DHCP را فعال کنیم که دستورات کلی این روتر به صورت زیر است:

```
Router(config)#int gigabitEthernet 0/0
Router(config-if)#ip address 192.168.1.1 255.255.255.0
```

بعد از اجرای دستورات بالا و دادن آدرس به Interface مورد نظر باید سرویس DHCP را فعال کنیم:

```
Router(config)#ip dhcp pool P1
Router(dhcp-config)#network 192.168.1.0 255.255.255.0
Router(dhcp-config)#dns-server 192.168.1.1
```

بعد از تنظیم روتر باید وارد Access Point شوید و تنظیمات آن را تکمیل کنید:

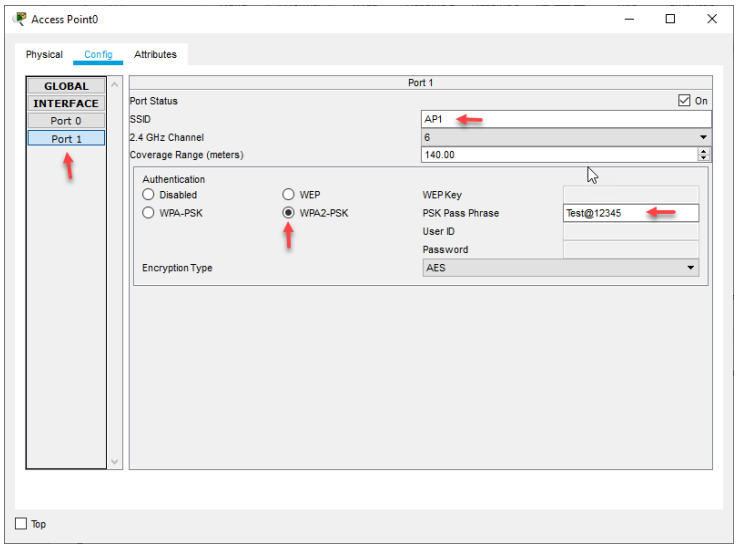
به مانند شکل ۳۴-۹، AP مورد نظر دارای دو پورت است که Port 0 آن به صورت سیمی بوده و به سوئیچ متصل شده است و Port 1 آن به صورت وایرلس است و باید تنظیم شود، بر روی Port 1 کلیک کنید و در صفحه باز شده و در قسمت SSID باید یک نام برای پیدا شدن Access Point وارد کنید که در

www.takbook.com

اینجا API در نظر گرفته شده است، باند فرکانسی آن 2.4 گیگاهرتز در نظر گرفته شده است و نیاز به تغییر آن نیست، در قسمت Coverage Range که مربوط به منطقه تحت پوشش است هر چقدر عدد بیشتر باشد مقدار سیگنالی که برای PC در دسترس خواهد بود بیشتر است.

در قسمت Authentication هم باید یکی از الگوریتم‌های احراز هویت را انتخاب کنید که در اینجا WPA2-PSK انتخاب شده است و یک رمز عبو برای آن در نظر گرفته شده است.

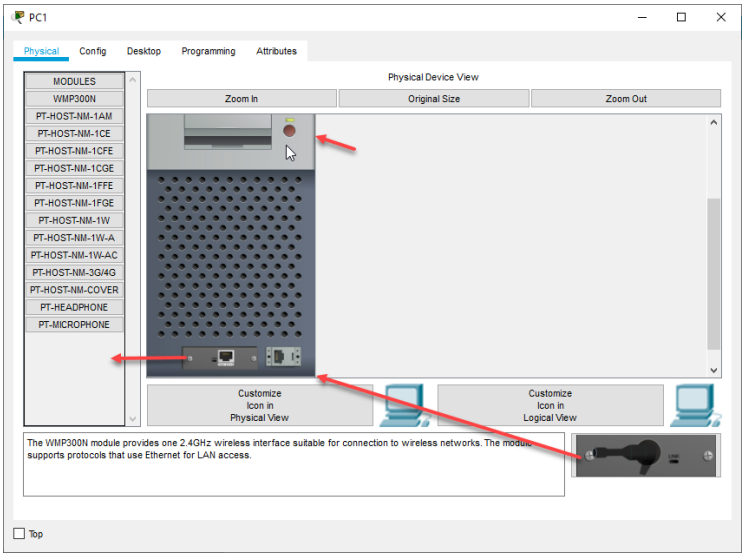
در قسمت Encryption Type می‌توانید نوع الگوریتم رمزگذاری را بین AES و TKIP تغییر دهید.



شکل ۹-۳۴ تنظیمات AP

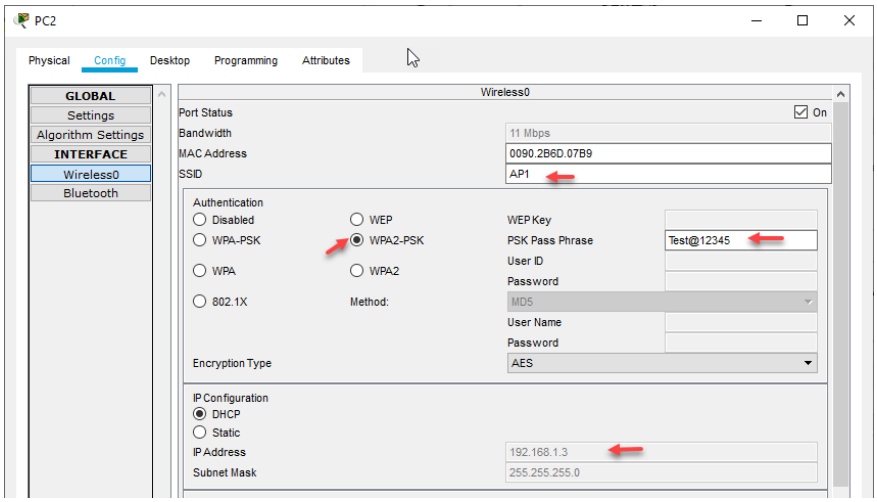
بعد از اینکه AP را تنظیم کردید حالا باید به مانند شکل ۳۵-۹، وارد PC شوید و یک کارت شبکه‌ی بی‌سیم به ان اضافه کنید، برای این کار اول از همه PC را خاموش کنید و اسلات کارت شبکه‌ی Ethernet را از محل مورد نظر خارج و اسلات کارت شبکه‌ی بی‌سیم را به دستگاه اضافه و ان را روشن کنید.

www.takbook.com



شکل ۳۵-۹ تنظیمات PC1

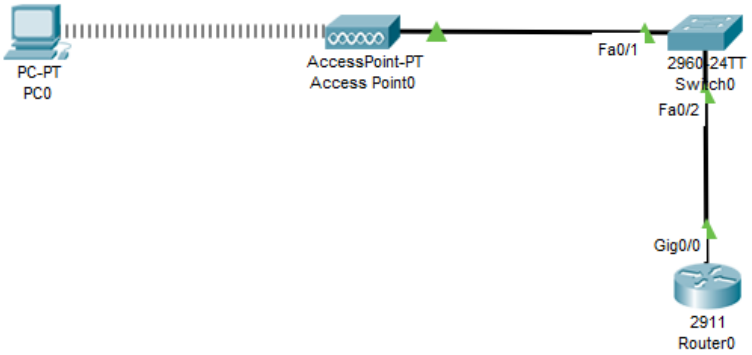
در ادامه کار به مانند شکل ۳۶-۹، وارد تب Config شوید و در قسمت SSID باید نام SSID مربوط به Access Point که وارد کردیم را در این قسمت وارد کنید و از قسمت Authentication هم گزینه‌ی WPA2-PSK را انتخاب و یک رمز عبور برای ان در نظر بگیرید، توجه داشته باشید نوع رمزگذاری باید با AP که AES بود یکی انتخاب شود، بعد از اینکه رمز را وارد کردید، در قسمت DHCP آدرس IP در رنج روتر دریافت خواهد شد.



شکل ۳۶-۹ تنظیمات PC2

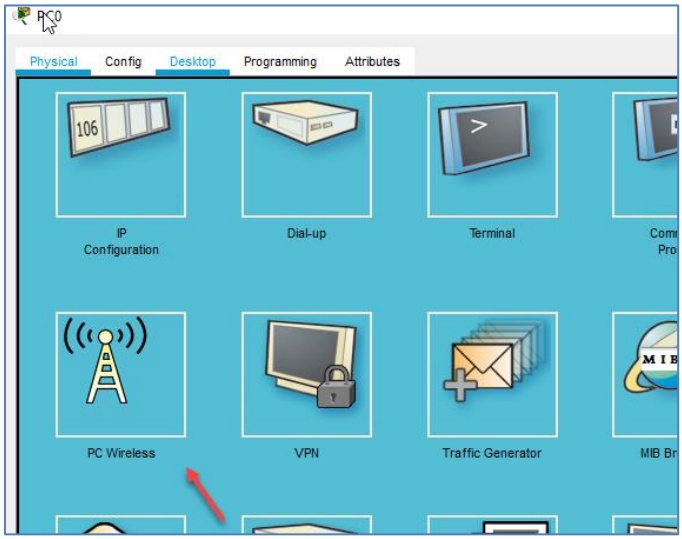
www.takbook.com

شکل نهایی سناریو بعد از تنظیم به صورت شکل ۳۶-۹، تغییر می‌کند، اگر ارتباط بین PC و AP را مشاهده کنید، این ارتباط از نوع Wireless است و با خط‌های پشت سرهم مشخص شده است، اگر از طریق PC روتر را Ping بگیرید این کار امکان پذیر خواهد بود.



شکل ۳۶-۹ سناریو وایرلس

برای اینکه بیشتر با تنظیمان وایرلس در PC آشنا شویم به مانند شکل ۳۷-۹، در تب Desktop بر روی PC Wireless کلیک کنید.



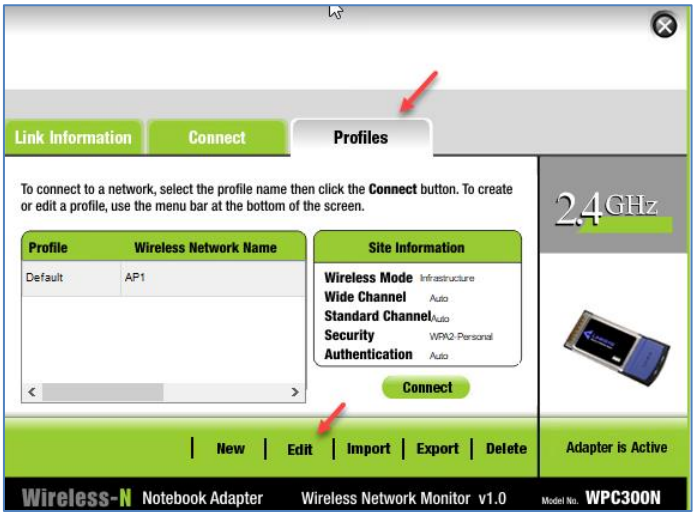
شکل ۳۷-۹ تنظیمات PC0

همانطور که در شکل ۳۸-۹، مشاهده می‌کنید آداپتور Wireless را نشان می‌دهد که دارای سیگنال با کیفیت و یک لینک ارتباطی خوب است، برای اینکه اطلاعات بیشتری از Wireless داشته باشید بر روی More Information کلیک کنید، در این قسمت اطلاعات ارتباطی با AP مشخص شده است.

www.takbook.com

شکل ۳۸-۹ تنظیمات وایرلس

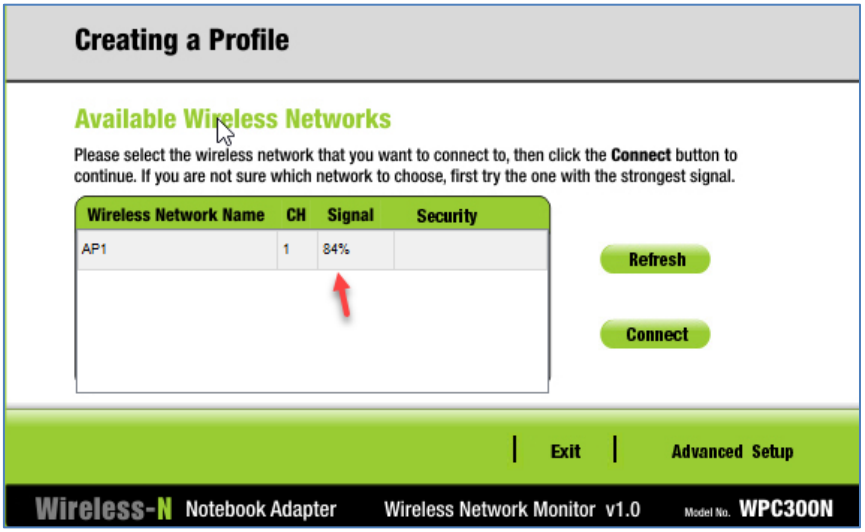
برای اینکه مشاهده کنیم که چه APهایی در اطراف این Pc وجود دارد باید در شکل ۳۹-۹، وارد تب Profiles شوید و بر روی Edit کلیک کنید.



شکل ۳۹-۹ تنظیمات وایرلس

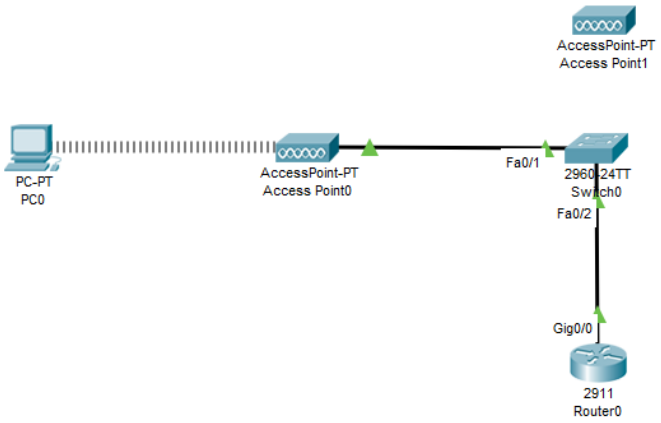
همانطور که در شکل ۴۰-۹، مشاهده می‌کنید یک AP را با نام AP1 پیدا کرده که سیگنال آن ۸۴ درصد است و در دسترس است که ارتباط خوبی خواهد بود، اگر چنانچه در قسمت coverage range در AP عدد را کاهش دهید این درصد تغییر خواهد کرد.

www.takbook.com



شکل ۴۰-۹ تنظیمات وایرلس

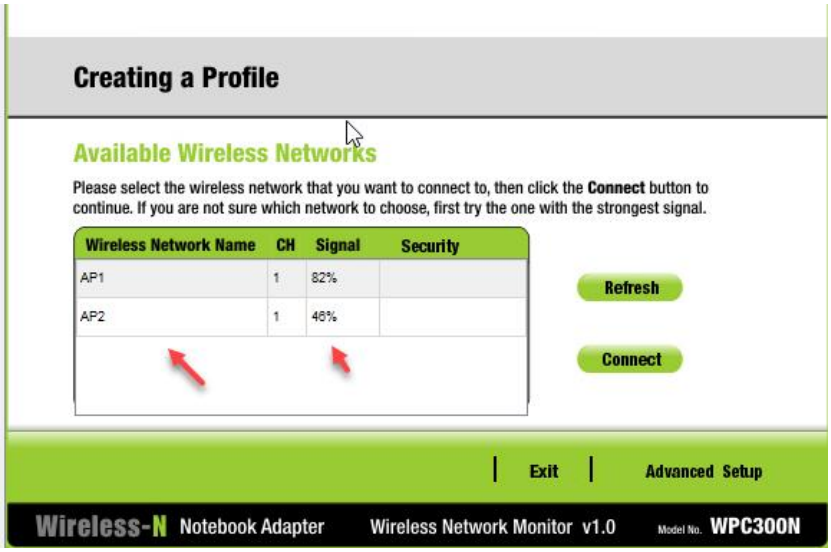
برای اینکه سیگنال‌ها را بررسی کنیم به سناریوی قبلی شکل ۴۱-۹، یک AP جدید اضافه می‌کنیم و نام SSID آن را AP2 در نظر می‌گیریم.



شکل ۴۱-۹ سناریو وایرلس

دوباره وارد PC شوید و همانطور که در شکل ۴۲-۹، مشاهده می‌کنید در قسمت Profile یک AP دیگر با نام AP2 اضافه شده است که دارای سیگنال ضعیف‌تر به نسبت قبلی است چون AP2 در محدوده‌ی دورتری قرار دارد.

www.takbook.com



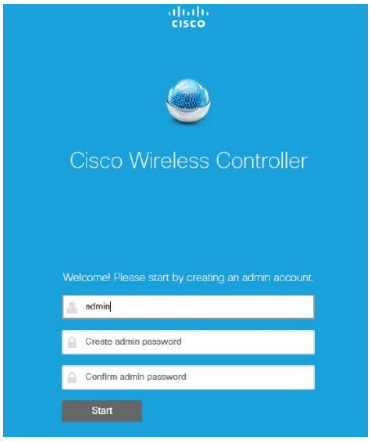
شکل ۴۲-۹ تنظیمات وایرلس

۹-۱۳ راه‌اندازی اولیه‌ی کنترلر LAN بی‌سیم WLC

برای راه‌اندازی WLC، بعد از روشن کردن آن یک IP با آدرس 192.168.1.1 به آن تعلق می‌گیرد و شما باید مرورگر خود را باز کنید و آدرس http://192.168.1.1 را اجرا کنید تا صفحه‌ی WLC باز شود.

صفحه‌ی اولی که باز می‌شود یک Wizard است که به شما کمک می‌کند به سادگی WLC را پیکربندی کنید.

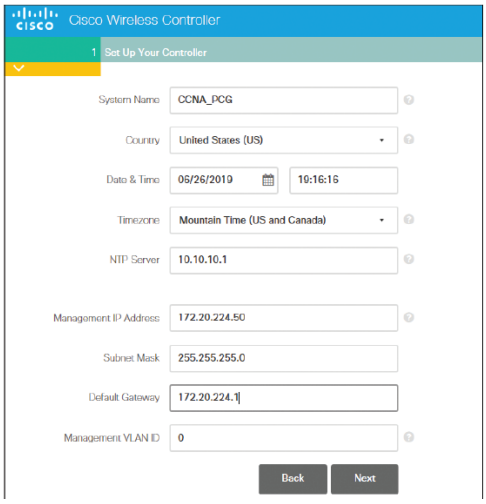
در شکل ۴۳-۹، اولین صفحه‌ی باز شده از شما یک رمز عبور جدید درخواست می‌کند که باید به مانند شکل ۴۲-۹، یک رمز عبور پیچیده وارد و بر روی Start کلیک کنید.



شکل ۴۳-۹ تنظیمات WLC

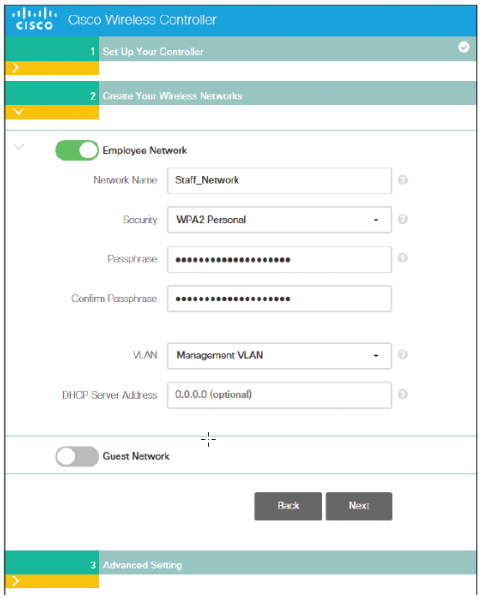
www.takbook.com

در ادامه و در شکل ۴۴-۹، باید اطلاعاتی مانند نام، کشور، تاریخ و ساعت، Timezone، NTP Server همچنین آدرس IP مدیریت، Subnet Mask، Default Gatway را به همراه VLAN ID وارد کنید و بر روی Next کلیک کنید.



شکل ۴۴-۹ تنظیمات WLC

در شکل ۴۵-۹، در قسمت Wireless Networks باید نام SSIDبه همراه نوع احراز هویت که WPA2 است را با یک رمز عبور پیچیده وارد کنید و همچنین می‌توانید در قسمت Guest Network شبکه‌ی مهمانان را فعال کنید و تنظیمات لازم را برای آنها انجام دهید.



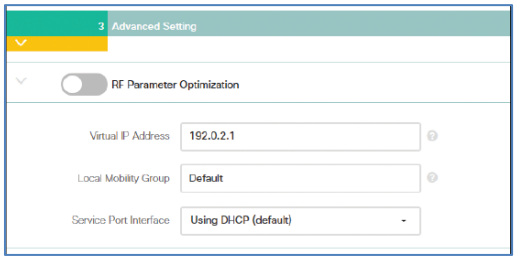
شکل ۴۵-۹ تنظیمات WLC

www.takbook.com

تذکر

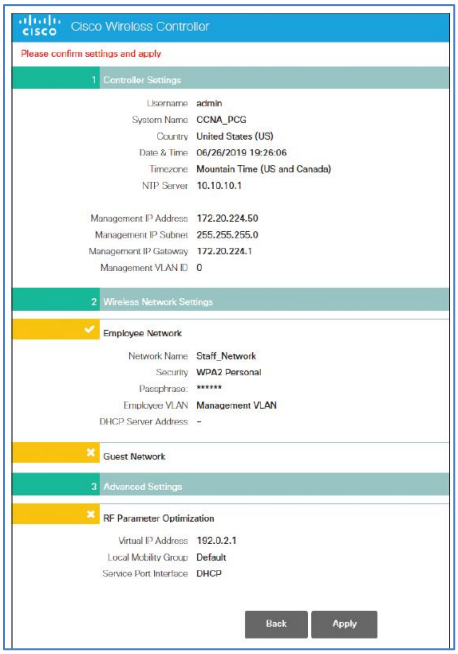
از نقطه نظر امنیتی توسعه‌ای که از طرف سیسکو ارائه شده این است که WLC ها را با WPA2 پیکربندی کنید و رمزگذاری آن را بر روی AES قرا دهید و به هیچ وجه از سایر قسمت‌های امنیتی مانند WEP, WPA/TKIP استفاده نکنید به جزء در مواردی که مشتریان قدیمی دارید که دستگاه آنها با این خطمشی های امنیتی کار می کند.

در شکل ۴۶-۹، می‌توانید تنظیمات مربوط به RF را انجام دهید.



شکل ۴۶-۹ تنظیمات WLC

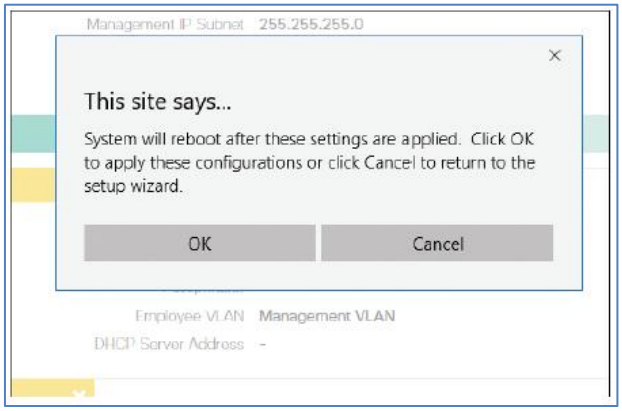
در شکل ۴۷-۹، تنظیمات نهایی را مشاهده می‌کنید و در صورت تایید باید بر روی Apply کلیک کنید.



شکل ۴۷-۹ تنظیمات WLC

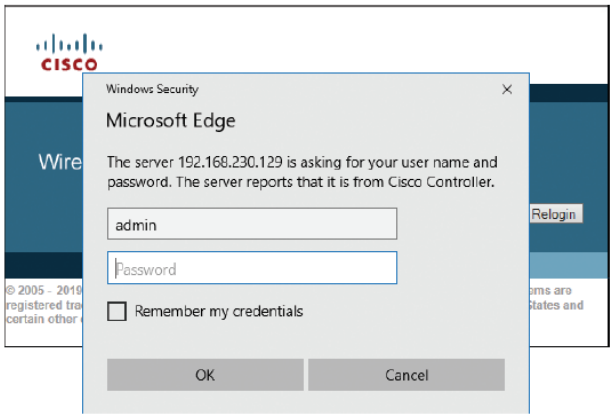
بعد از اینکه در قسمت قبل بر روی Apply کلیک کردید شکل ۴۸-۹، ظاهر می‌شود و به این نکته اشاره دارد که برای اعمال تنظیمات باید دستگاه Restart شود که باید بر روی OK کلیک کنید.

www.takbook.com



شکل ۹-۴۸ تنظیمات WLC

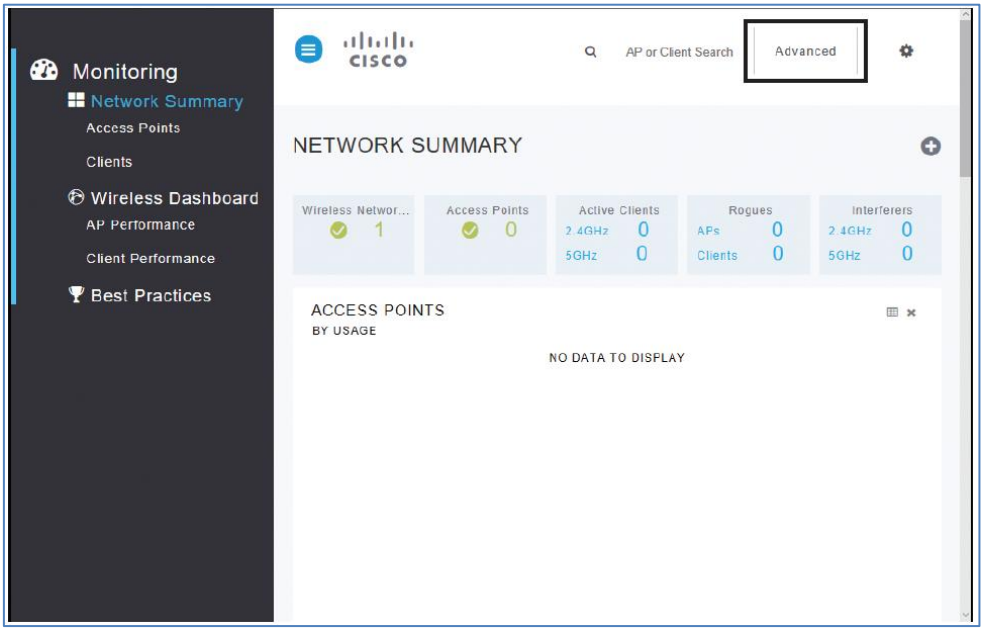
برای ورود باید آدرس مدیریتی WLC را در مرورگر وارد کنید و به مانند شکل ۹-۴۹، نام کاربری و رمز عبوری را که قبلاً تعریف کردید را برای ورود وارد کنید.



شکل ۹-۴۹ تنظیمات WLC

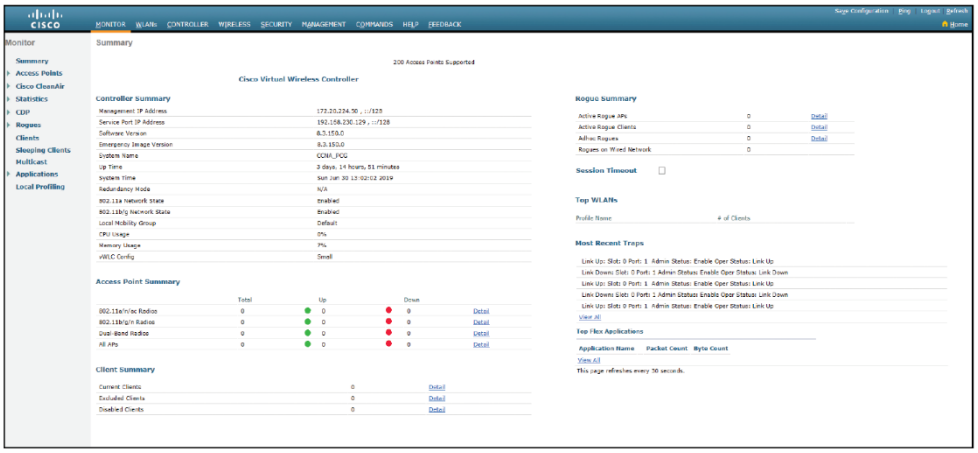
پس از وورد به WLC صفحه‌ی اول آن را به مانند شکل ۹-۵۰، مشاهده می‌کنید که اطلاعاتی از شبکه را به شما نشان می‌دهد، برای انجام تنظیمات وارد Advanced شوید.

www.takbook.com



شکل ۹-۵۰ تنظیمات WLC

در شکل ۹-۵۱، صفحه‌ی Advanced را مشاهده می‌کنید که دارای تنظیمات بی‌شماری است .

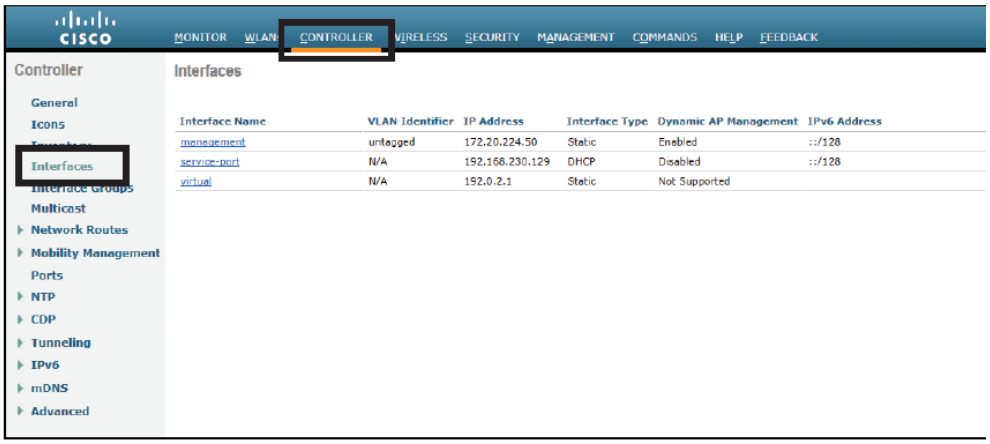


شکل ۹-۵۱ تنظیمات WLC

ایجاد VLAN Interface در WLC

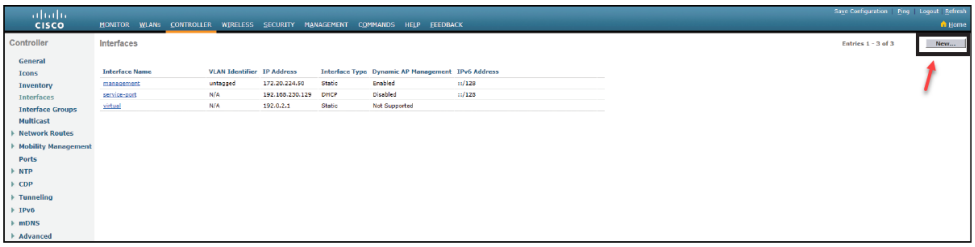
رابط‌های Dynamic Interface به عنوان VLAN Interface هم شناخته می‌شوند، آنها همان VLAN برای مشتری‌های بی‌سیم هستند. این واسطها جریان‌های ارتباطی جداگانه‌ای را ایجاد می‌کنند و به مانند شکل ۹-۵۲، وارد controller شوید و بر روی Interfaces کلیک کنید.

www.takbook.com



شکل ۹-۵۲ تنظیمات WLC

در شکل ۵۳-۹، برای ایجاد VLAN Interface بر روی New کلیک کنید.



شکل ۹-۵۳ تنظیمات WLC

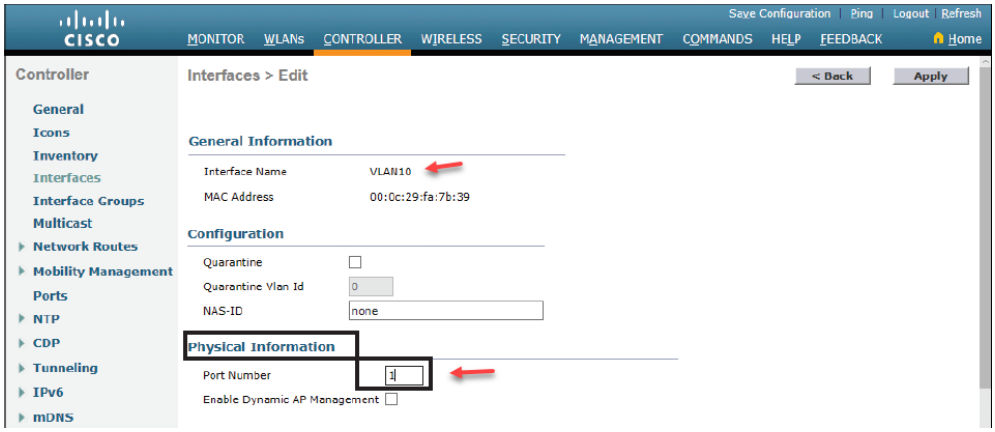
به مانند شکل ۵۴-۹، یک نام و یک شماره‌ی ID برای VLAN خود وارد و بر روی Apply کلیک کنید.

شکل ۹-۵۴ تنظیمات WLC

برای اینکه این Interface مجازی را به Interface فیزیکی ارتباط دهیم باید به مانند شکل ۵۵ -۹ در قسمت physical Information شماره Interface فیزیکی (شماره‌ی یک) را وارد کنید و بر روی Apply کلیک کنید.

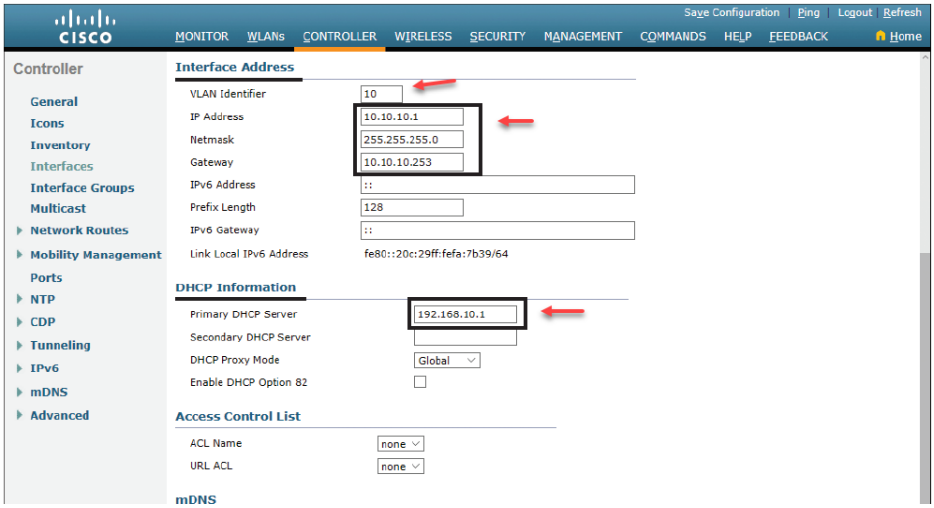
www.takbook.com

توجه داشته باشیدکه بر روی یک interface فیزیکی می‌توانید چندین پورت مجازی قرار دهید.



شکل ۹-۵۵ تنظیمات WLC

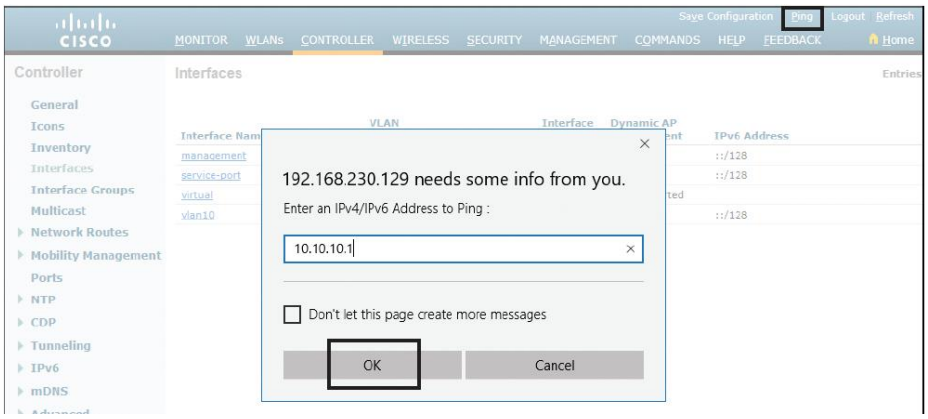
در شکل ۹-۵۶، باید آدرس VLAN 10 را به همراه Gateway آن وارد کنید و در آخر هم آدرس سرور DHCP را وارد کنید و بر روی apply کلیک کنید و بعد از آن WLC را Restart کنید.



شکل ۹-۵۶ تنظیمات WLC

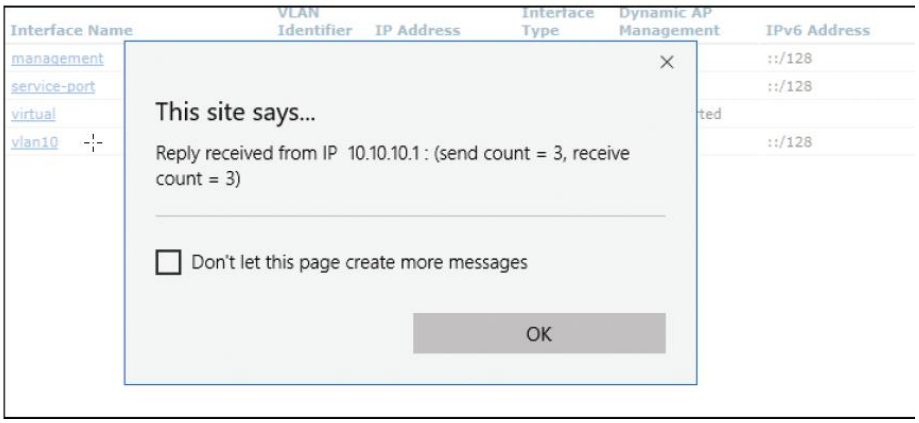
به مانند شکل ۹-۵۷، بعد از ورود به WLC می‌توانید بر روی PING کلیک کنید و آدرس مجازی برای VLAN 10 را تست بگیرید.

www.takbook.com



شکل ۹-۵۷ تنظیمات WLC

همانطور که در شکل ۹-۵۸، مشاهده می‌کنید دستور Ping به خوبی در حال اجرا است.



شکل ۹-۵۸ تنظیمات WLC

تنظیمات DHCP در WLC

برای انجام تنظیمات DHCP در WLC به مانند شکل ۹-۵۹، از قسمت Internal DHCP Server وارد DHCP Scops شوید و بر روی New کلیک کنید.

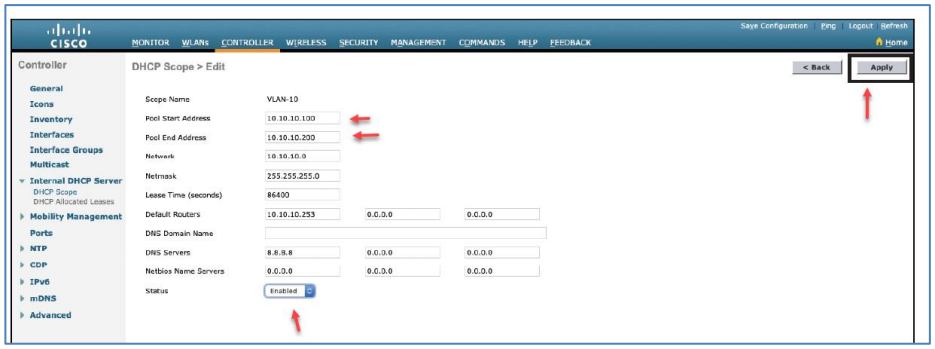
شکل ۹-۵۹ تنظیمات WLC

به مانند شکل ۹-۶۰، نام VLAN-10 را برای آن در نظر می‌گیریم و بر روی Apply کلیک کنید.

www.takbook.com

شکل ۶۰-۹ تنظیمات WLC

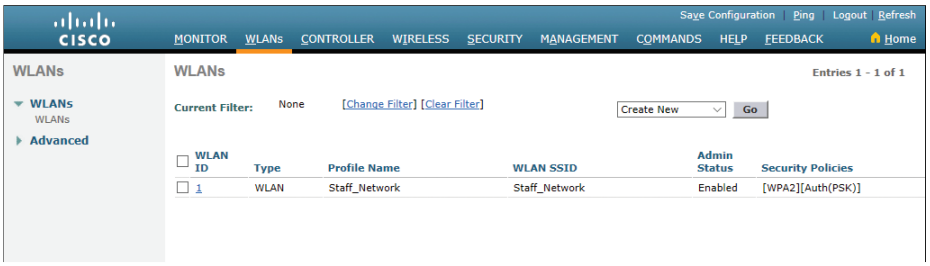
در شکل ۶۱-۹، باید رنج IP آدرس را برای این Pool وارد کنید و بعد در قسمت آخر status را بر روی Enabled قرار دهید و بر روی Apply کلیک کنید.



شکل ۶۱-۹ تنظیمات WLC

پیکربندی WLAN در WLC

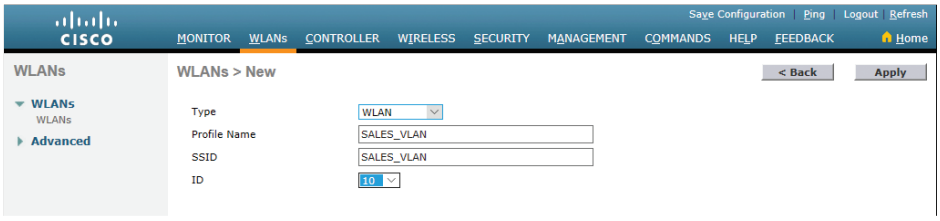
در ادامه کار برای اینکه نیازهای خود را در شبکه فراهم کنیم باید WLAN را در WLC فعال کنیم، برای همین کار به مانند شکل ۶۲-۹، وارد WLANs شوید، در لیست مورد نظر یک WLAN را مشاهده می‌کنید که قبلاً آن را ایجاد کردیم، برای ایجاد WLAN جدید بر روی Go کلیک کنید.



شکل ۶۲-۹ تنظیمات WLC

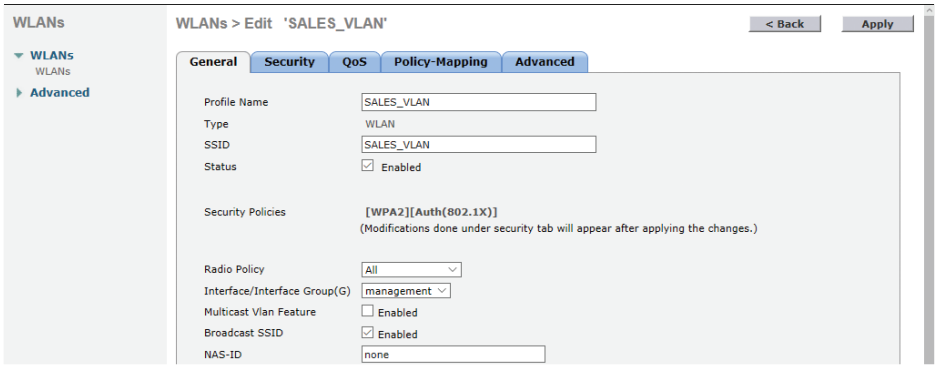
در شکل ۶۳-۹، Type را بر روی WLAN قرا دهید و نام Profile و SSID را وارد کنید و در آخر هم ID را شماره‌ی 10 وارد کنید تا با VLAN 10 که قبلاً ایجاد کردیم مطابقت داشته باشد، در آخر بر روی Apply کلیک کنید.

www.takbook.com



شکل ۹-۶۳ تنظیمات WLC

بعد از ایجاد WLAN وارد آن شوید و به مانند شکل ۹-۶۵، تیک Enable مربوط به قسمت Status را انتخاب کنید تا WLAN فعال شود.

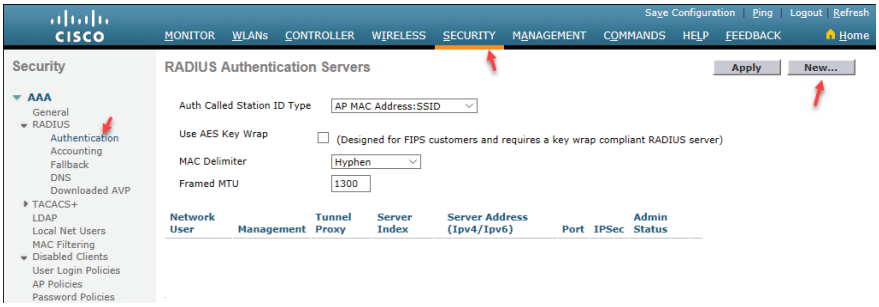


شکل ۹-۶۴ تنظیمات WLC

تعریف RADIUS Server در WLC

همانطور که گفتیم Radius یا Remote Authentication Dial-In User Service یک پروتکل شبکه است که در ورژن جدید آن بر روی پورت ۱۸۱۲ عمل می‌کند و مدیریت تاییدهویت، مجوز و دسترسی را به کاربرانی که می‌خواهند از یک سرویس در شبکه استفاده کنند می‌دهد.

برای تنظیم این پروتکل در WLC به مانند شکل ۹-۶۵، وارد قسمت SECURITY شوید و از قسمت AAA در زیر مجموعه‌ی Radius بر روی Authentication کلیک و در صفحه‌ی باز شده بر روی New کلیک کنید.

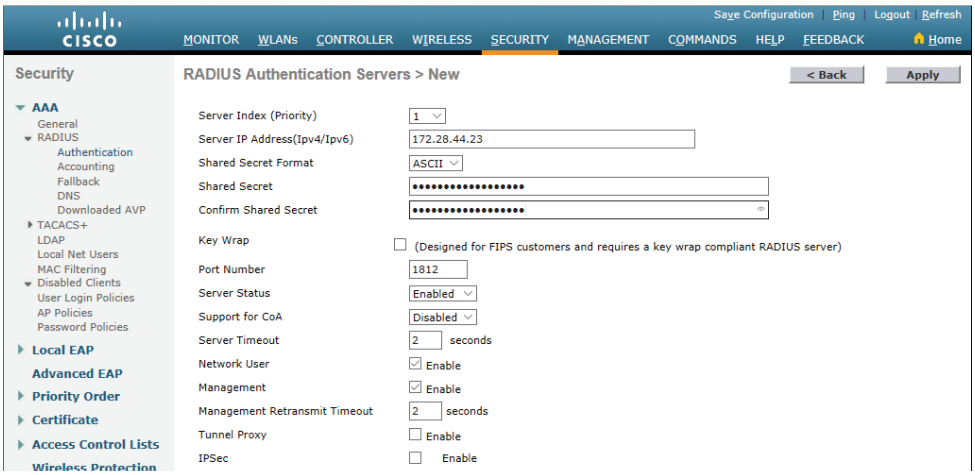


شکل ۹-۶۵ تنظیمات WLC

www.takbook.com

در شکل ۶۶-۹، در قسمت Server IP باید آدرس سرور Radius را وارد کنید و در Shared Secret باید رمز عبوری را که در سرور Radius وارد کردید را اینجا هم وارد کنید و بر روی Apply کلیک کنید تا تنظیمات اعمال شود.

برای راه‌اندازی Radius سرور می‌توانید از نرم‌افزار ACS سیسکو برای این‌کار استفاده کنید.



شکل ۶۶-۹ تنظیمات WLC

۹-۱۴ سوالات فصل نهم

1. Wired Ethernet and Wi-Fi are based on which two IEEE standards, respectively?
کدام یک از گزینه‌های زیر به ترتیب مربوط به استاندارد شبکه‌ی سیمی و بی‌سیم IEEE است؟

a. 802.1, 802.3
b. 802.3, 802.1
c. 802.3, 802.11
d. 802.11, 802.3

2. Devices using a wireless LAN must operate in which one of the following modes?
دستگاهی که از یک شبکه‌ی بی‌سیم استفاده می‌کند باید در کدام حالت قرار داشته باشد؟

a. Round-robin access
b. Half duplex

www.takbook.com

c. Full duplex
d. None of these answers

3. An access point is set up to offer wireless coverage in an office. Which one of the following is the correct 802.11 term for the resulting standalone network?

یک Acess Point برای ارائه پوشش دسترسی در یک دفتر تنظیم شده است. کدام یک از اصطلاح زیر برای یک شبکه‌ی مستقل به کار می‌رود؟

a. BSA
b. BSD
c. BSS
d. IBSS

4.Which one of the following is used to uniquely identify an AP and the basic service set it maintains with its associated wireless clients?

کدام یک از گزینه‌های زیر برای شناسایی Access Point توسط کلاینت وایرلس کاربرد دارد؟

a. SSID
b. BSSID
c. Ethernet MAC address
d. Radio MAC address

5. Which one of the following can be used to provide wireless connectivity to a nonwireless device?

کدام یک از گزینه‌های زیر برای ارتباط وایرلس با دستگاه‌های غیر وایرلس کاربرد دارد؟

a. Wireless repeater
b. Workgroup bridge
c. Transparent bridge
d. Adaptive bridge

6. Which one of the following is not needed in a Cisco outdoor mesh network?

کدام یک از موارد زیر در یک شبکه‌ی مش در فضای باز سیسکو مورد نیاز نیست؟

a. A BSS function
b. Ethernet cabling to each AP
c. A workgroup bridge
d. A backhaul network

7. Which of the following are frequency bands commonly used for Wi-Fi?

کدام یک از باندهای فرکانسی زیر معمولاً برای WIFI استفاده می‌شود؟

a. 2.5 KHz
b. 2.5 MHz
c. 5 MHz
d. 2.5 GHz
e. 5 GHz

8. Which of the following are considered to be nonoverlapping channels?

کدام یک از موارد زیر بعنوان کانال غیر همپوشانی شناخته می شوند؟

a. Channels 1, 2, and 3 in the 2.4-GHz band
b. Channels 1, 5, and 10 in the 2.4-GHz band
c. Channels 1, 6, and 11 in the 2.4-GHz band
d. Channels 40, 44, and 48 in the 5-GHz band

www.takbook.com

9. What is a benefit of using a Cisco Wireless LAN Controller?

استفاده از Wireless LAN Controller شرکت سیسکو چه مزایایی دارد؟

a. It eliminates the need to configure each access point individually.
b. Central AP management requires more complex configurations.
c. Unique SSIDs cannot use the same authentication method.
d. It supports autonomous and lightweight APs.

10. Which statement about Link Aggregation when implementing on a Cisco Wireless LAN Controller is true?

کدام گفته در مورد تجمیع پیوند هنگام اجرای یک کنترلر LAN بی‌سیم سیسکو صحیح است؟

a. The EtherChannel must be configured in "mode active".
b. When enabled, the WLC bandwidth drops to 500 Mbps.
c. To pass client traffic, two or more ports must be configured.
d. One functional physical port is needed to pass client traffic.

www.takbook.com

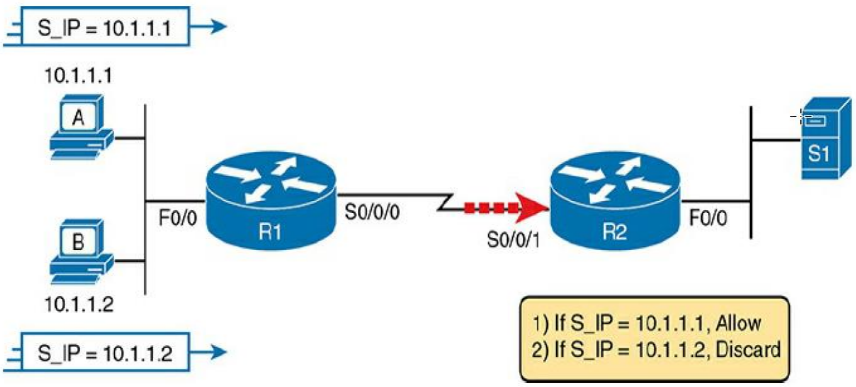
فصل دهم

IP Access Control Lists

از Access List برای مدیریت ترافیک در شبکه استفاده می‌شود، مثلاً شما می‌توانید به یک یا چند کامپیوتر اجازه دسترسی به منابع خاصی از شبکه را ندهید که یکی از مهم‌ترین بخش‌های کار در شبکه است.

مثلاً یک Accee List می‌تواند مشخص کند که بسته‌هایی که آدرس مقصد آنها با آدرس 10.180.0.1 مطابقت دارد اجازه دارند از آن مسیر عبور کنند.

به شکل ۱-۱۰، توجه کنید؛ در این شکل دو PC را مشاهده می‌کنید که می‌خواهند به سرور S1 برسند، برای اینکه محدودیت برای آنها اعمال کنیم باید در روتر R2 یک Access List تعریف کنیم که به IP آدرس 10.1.1.1 که مربوط به کامپیوتر A است دسترسی بدهیم و دیگری را Discard کنیم.



شکل ۱-۱۰ IP Access Control List

دو موضوع که باید در موقع کار با Access List بدانید:

- **Inbound**
- **Outbound**

در ترافیک ورودی یعنی Inbound ابتدا روتر ترافیک مورد نظر را با Access List که توسط شما ایجاد شده است بررسی می‌کند و در صورت تایید آنها را به مقصد ارسال می‌کند و ترافیک Outbound هم در جهت خلاف این عمل کار می‌کند.

www.takbook.com

چند نوع Access List در شبکه داریم:

- Standard numbered ACLs (1–99)
- Extended numbered ACLs (100–199)
- Additional ACL numbers (1300–1999 standard, 2000–2699
- extended)
- Named ACLs
- Improved editing with sequence numbers

۱۰-۱ Access List استاندارد

این نوع از Access Listها از شماره‌های ذکرشده در بالا استفاده می‌کنند و فقط ترافیک‌های مربوط به مبدأ را مورد بررسی قرار می‌دهند. با نحوه‌ی کار این Access List آشنا می‌شویم.

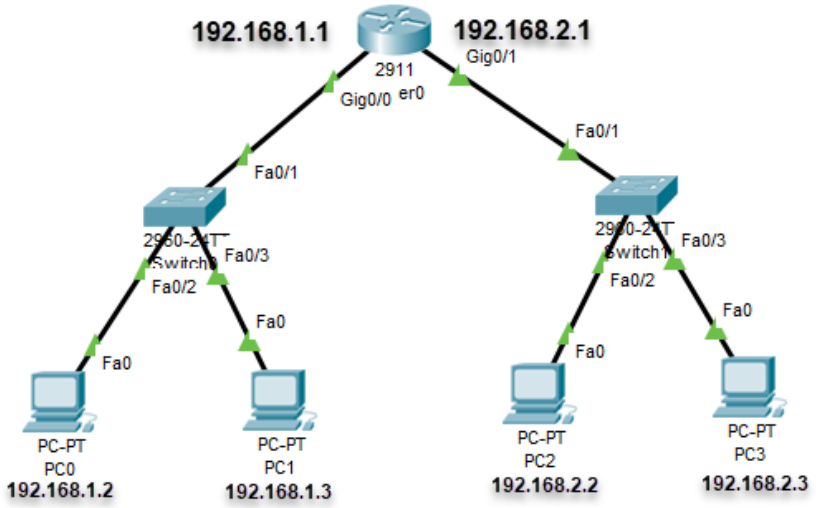
Deny

این دستور در access List برای جلوگیری از دسترسی یک Node خاص به یک شبکه‌ی دیگر است که بسیار پرکاربرد و خطرناک است، به دلیل اینکه با یک اشتباه، شبکه از کار می‌افتد.

Permit

این دستور ضد دستور Deny است و برای دسترسی به شبکه کاربرد دارد.

در شکل ۲-۱۰، می‌خواهیم از دسترسی pc1 به Pc3 و Pc4 جلوگیری کنیم.



شکل ۲-۱۰ سناریو ACL

وارد روتر می‌شویم و دستورات زیر را به ترتیب وارد می‌کنیم:

Router(config)#**ip access-list standard dpc1**

www.takbook.com

در قسمت اول باید access List را تعریف کنیم؛ هم می‌توانیم با نام و هم می‌توانیم با شماره تعریف کنیم که در این قسمت از نام dpc1 استفاده کردیم. شما می‌توانید هر اسم دیگری در این قسمت قرار دهید و یا از شماره استفاده کنید، اما همیشه سعی کنید از نام استفاده کنید که مدیریت آن آسان باشد.

Router(config-std-nacl)#**deny 192.168.1.2 0.0.0.0**

با این دستور، ip address مربوط به pc0 را Deny می‌کنیم. اگر توجه کنید در قسمت اول، دستور Deny و بعد، ip address مربوط به pc0 و بعد از آن که مهم است از Wildcard Mask تأکیدی استفاده کردیم، یعنی استفاده از ۴ تا صفر که تأکید بر Deny کردن همین ip را دارد. اگر Wild Card Mask را به صورت 0.0.0.255 وارد کنیم، یعنی تمام ip address ها در رنج 192.168.1.0 فیلتر شوند، پس سعی کنید از Wild card Mask تأکیدی استفاده کنید.

Router(config-std-nacl)#**permit any**

بعد از Deny حتماً از Permit استفاده کنید، چون به صورت کلی در زمان استفاده از Access List، در آخر تمام این آدرس‌ها، یک دستور Deny any قرار دارد که زمانی که دستورات اول مانند دستور deny 192.168.1.2 0.0.0.0 که در بالا نوشیم با ترافیک همخوانی داشته یا نداشته باشد، بقیه ترافیک به صورت پیش‌فرض Deny خواهد شد و به خاطر همین از Permit Any استفاده می‌کنیم تا بقیه‌ی شبکه اجازه‌ی دسترسی داشته باشند، البته بهتر است به جای استفاده از Permit Any از دستورات مشخص‌تر و محدودتری استفاده کنید.

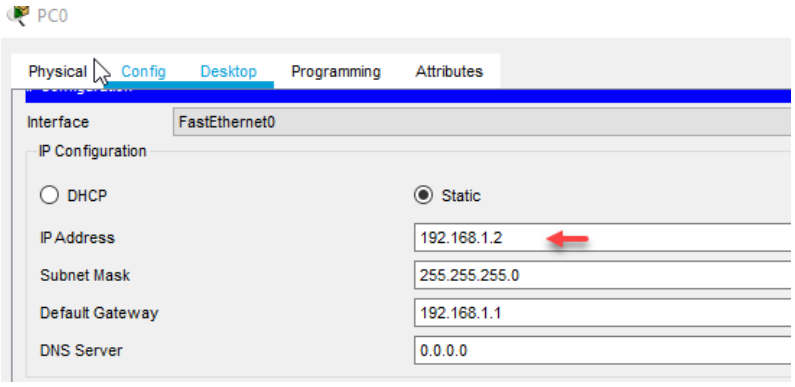
بعد از تعریف کامل access List باید به روتر بگوییم که این فیلترینگ را روی کدام پورت انجام دهد، پس وارد روتر می‌شویم، اگر توجه کنید می‌خواهیم دسترسی pc0 به pc2 و pc3 جلوگیری کنیم، پس باید در پورت Gig0/1 روتر دستور زیر را وارد کنیم:

Router(config)# **int Gig0/1**
Router(config-if)#**ip access-group dpc1 out**

به دستور توجه کنید، ip Access-group را تعریف و بعد از آن، نام Access List که ایجاد کرده‌ایم را وارد می‌کنیم. گفتیم ترافیک این access List در زمان خروج از اینترفیس فیلتر شود. اگر به جای out، گزینه‌ی in را انتخاب می‌کردید، این بدان معنا بود که شما access List را برای شبکه‌ی 192.168.2.0 نوشتید که این امر اشتباه است و این access list عمل نمی‌کند.

توجه داشته باشید آدرس IP را درPC به صورت زیر وارد کنید، مثلاً برای PC0 به صورت شکل ۳-۱۰، باید تعریف شود.

www.takbook.com



شکل ۳-۱۰ تنظیمات PC0

و حالا اگر از pc0 به pc2 و pc3، Ping کنید، با پیام زیر مواجه می‌شوید:

PC>**ping 192.168.2.3**

Pinging 192.168.2.3 with 32 bytes of data:

Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.

و اگر از طریق pc1 بخواهید pc2 و pc3 را Ping کنید، جواب خواهید گرفت.

PC>**ping 192.168.2.3**

Pinging 192.168.2.3 with 32 bytes of data:

Reply from 192.168.2.3: bytes=32 time=1ms TTL=127
Reply from 192.168.2.3: bytes=32 time=0ms TTL=127
Reply from 192.168.2.3: bytes=32 time=0ms TTL=127
Reply from 192.168.2.3: bytes=32 time=0ms TTL=127

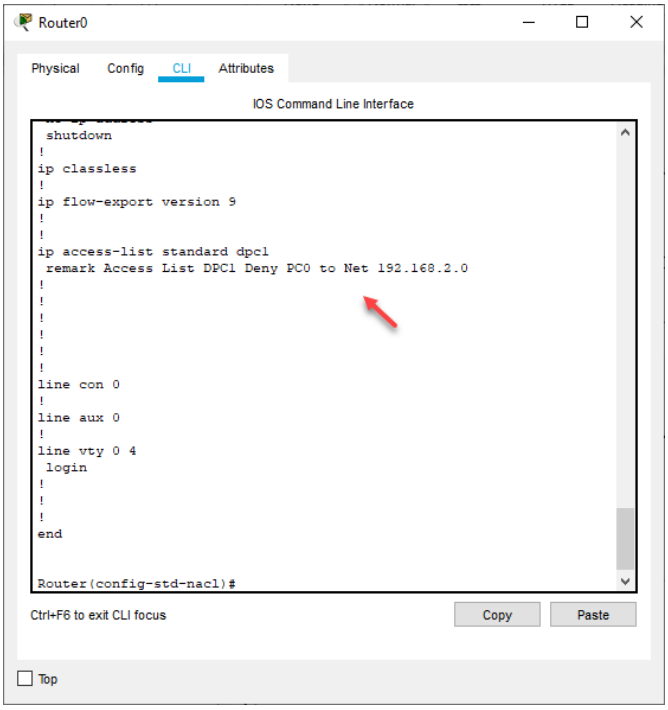
Ping statistics for 192.168.2.3:
  Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
  Minimum = 0ms, Maximum = 1ms, Average = 0ms

برای قرار دادن توضیحات روی یک Access List، باید از دستور Remark درون ACL استفاده کرد، که در دستور زیر اول وارد Access List که با نام dpc1 ایجاد کردیم می‌شویم و بعد دستور Remark و در ادامه توضیحات خود را در مورد آن می‌نویسید.

Router(config)#**ip access-list standard dpc1**
Router(config-std-nacl)#**remark** *Access List DPC1 Deny PC0 to Net 192.168.2.0*

www.takbook.com

به مانند شکل ۴-۱۰، برای مشاهده‌ی این دستور باید وارد Running-config شوید تا این پیام را مشاهده کنید.



شکل ۴-۱۰ تنظیمات روتر Router0

برای اینکه متوجه شوید که دستور مورد نظر کارایی دارد یا نه در روتر دستور show access-lists dpc1 را وارد کنید:

```
Router#show access-lists dpc1
Standard IP access list dpc1
    deny host 192.168.1.2 (8 match(es))
    permit any (8 match(es))
```

اگر به نتیجه‌ی دستور مورد نظر توجه کنید، در قسمت Deny کلمه‌ی match را مشاهده می‌کنید که عدد 8 کنار آن نوشته شده است، این عدد بدان معنا است که ۸ بار پکت از PC0 به سمت شبکه 192.168.2.0 ارسال شده است که Access List مورد نظر آن شناسایی کرده و سیاست مربوطه را بر روی آن پیاده‌سازی کرده.

حالا اگر بخواهیم سیاستی قرار دهیم که PC3 و PC2 نتواند شبکه 192.168.1.0 را ببیند باید به صورت زیر عمل کنیم:

وارد روتر R1 شوید و دستورات زیر را وارد کنید:

www.takbook.com

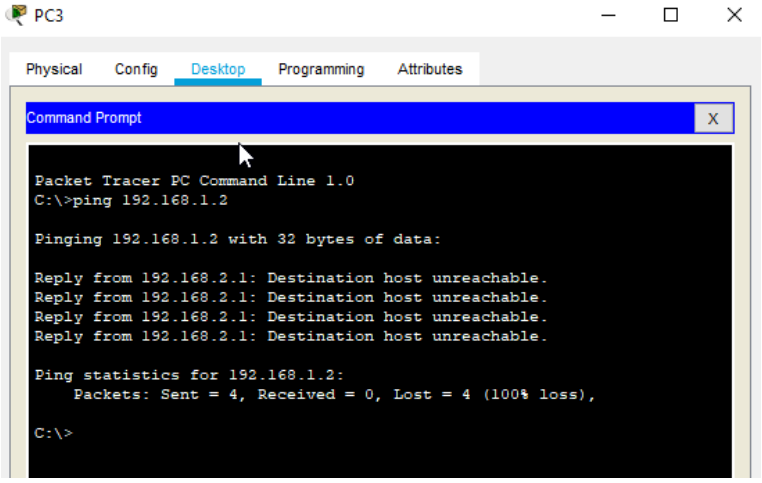

```
Router(config)#ip access-list standard dpc3
Router(config-std-nacl)#deny 192.168.2.0 0.0.0.255
Router(config-std-nacl)#permit any
```

در دستورات بالا به ترتیب یک Access List استاندارد با نام dpc3 ایجاد کردیم و بعد از ورود به آن با دستور Deny زیر شبکه‌ی 192.168.2.0 را برای کل رنج IP آن Deny کردیم و در آخر هم بقیه شبکه‌ها را Permit کردیم.

```
Router(config)#interface gigabitEthernet 0/0
Router(config-if)#ip access-group dpc3 out
```

در ادامه کار وارد Interface مورد نظر که به سمت شبکه 192.168.1.0 است شوید و دستور ip access-group dpc3 out را وارد کنید، با این کار شبکه‌ی 192.168.2.0 نمی‌تواند به شبکه‌ی 192.168.1.0 دسترسی داشته باشد.

به مانند شکل ۵-۱۰، اگر وارد PC3 شوید و PC0 را Ping بگیرید، متوجه خواهید شد که دسترسی به شبکه مورد نظر امکان پذیر نیست.



شکل ۵-۱۰ دستور PING در PC3

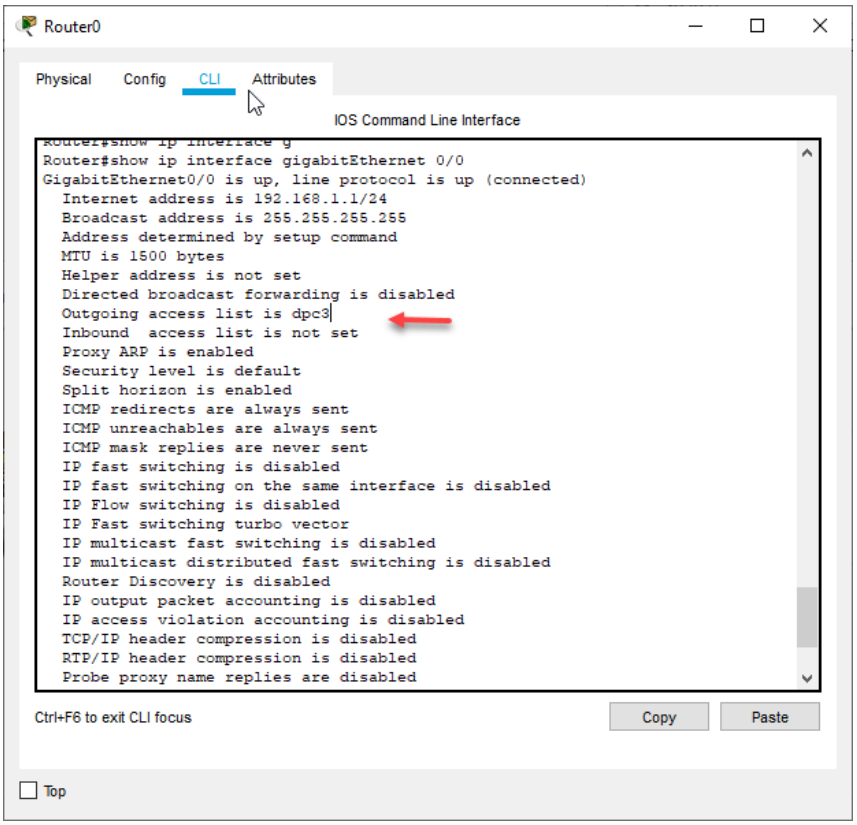
خوب حالا اگر وارد روتر Router0 شوید و دستور show ip access-lists را وارد کنید نتایج زیر را مشاهده می‌کنید:

```
Router#show ip access-lists
Standard IP access list dpc1
    10 deny host 192.168.1.2 (16 match(es))
    20 permit any (8 match(es))
Standard IP access list dpc3
    10 deny 192.168.2.0 0.0.0.255 (8 match(es))
    20 permit any
```

اگر بخواهیم یک Interface را از نظر ورودی و خروجی Access List بررسی کنیم باید از دستور Show ip Interface GigabitEthernet 0/0 استفاده کنیم:

www.takbook.com

به مانند شکل ۶-۱۰، در این دستور که با فلش مشخص شده است Outgoing و Incoming برای Access List مشخص شده است، همانطور که مشاهده می‌کنید Acess List با نام dpc3 بر روی Outgoing فعال شده است.



شکل ۶-۱۰ بررسی ACL

برای اینکه یک access List را پاک کنیم فقط کافی است قبل از دستور ip access-list standard کلمه‌ی no قرار دهیم، که شکل کلی دستور به صورت زیر خواهد بود.

Router(config)#**no ip access-list standard dpc1**
Router(config)#**no ip access-list standard dpc3**

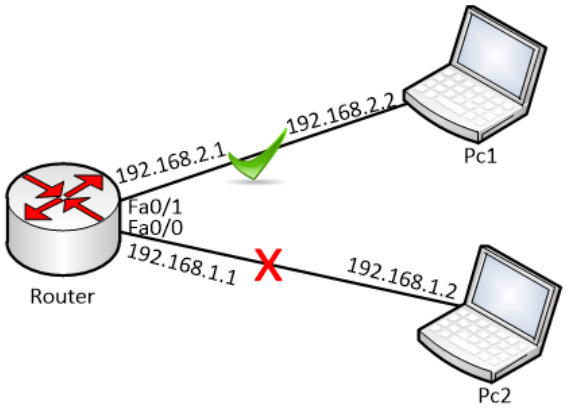
تذکر

ترتیب اجرای دستورات در access List خیلی مهم است و اگر در یک Access List از دو دستور Permit و Denyاستفاده کنید اول از همه دستور Permit اجرا می‌شود و دیگر دستورات بعدی اجرا نخواهند کرد.

www.takbook.com

۱۰-۲ استفاده از Access-List در پورت مجازی VTY

شما می‌توانید با تعریف یک ACCESS List و فعال کردن آن در پورت Vty به یک ip اجازه‌ی Telnet بدهید یا ندهید. برای انجام این کار به مثال زیر توجه کنید:



شکل ۷-۱۰ بررسی ACL در VTY

مانند شکل ۷-۱۰، یک روتر و دو pc به صفحه اضافه و به هم متصل کنید و به پورت‌های مورد نظر ip دهید.

وارد روتر شوید و access-List زیر را وارد کنید:

```
Router(config)#ip access-list standard 10
Router(config-std-nacl)#permit 192.168.1.0 0.0.0.255
```

در دستورات بالا، یک access-list استاندارد با شماره‌ی ۱۰ تعریف کردیم و بعد از آن به شبکه‌ی 192.168.1.0 اجازه دسترسی دادیم و زمانی که یک Permit برای یک شبکه تعریف می‌کنیم، بقیه‌ی شبکه‌ها Deny می‌شوند.

بعد از ایجاد Access-list، وارد پورت Line Vty می‌شویم و telnet را روی پورت‌ها فعال می‌کنیم:

```
Router(config)#line vty 0 15
Router(config-line)#password 123
Router(config-line)#login
Router(config-line)#access-class 10 in
```

در دستور اول وارد پورت VTY 0 15 می‌شویم و بعد، رمز عبور را بر روی پورت‌ها قرار می‌دهیم، سپس با دستور login می‌گوییم که در زمان telnet شدن، رمز عبور را درخواست کند و بعد از آن، با دستور access-class به این پورت می‌گوییم که در زمان telnet شدن، فقط ip addressهایی را قبول کن که access-list 10 می‌گوید.

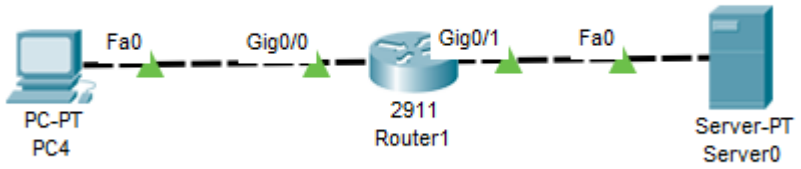
بعد از اتمام کار، اگر از طریق pc1 به روتر telnet کنید، جواب می‌گیرید، اما از طریق pc2 این امکان وجود ندارد.

www.takbook.com

۱۰-۳ Access List پیشرفته

این نوع Access List از شماره‌های ۱۰۰ تا ۱۹۹ و ۲۰۰۰ تا ۲۶۹۹ تشکیل شده است و می‌تواند ترافیک مربوط به مبدأ و مقصد را مورد بررسی قرار دهد، حتی می‌توانید پروتکل‌ها یا برنامه‌های خاص را Deny یا Permit کنید، این Access List در لایه‌ی سوم مدل OSI هم کارایی دارد.

مثال۵: در این مثال می‌خواهیم Telnet را روی روتر راه‌اندازی کنیم و Access List بنویسیم که از دسترسی PC4 به Telnet جلوگیری کند.



شکل ۸-۱۰ سناریو ACL پیشرفته

قبل از ایجاد access List آدرس‌های مربوط به پورت‌ها را وارد و پینگ مورد نظر را بگیرید تا سیستم PC4 بتواند سرور را ببیند.

وارد روتر می‌شویم و به صورت زیر عمل می‌کنیم:

Router(config)#**ip access-list extended PC4toTelNET**

یک Access List extended با نام **PC4toTelNET** را ایجاد کردیم که شما می‌توانید به جای این نام از نام دلخواه یا از شماره‌های ذکرشده در قسمت قبل استفاده کنید.

Router(config-ext-nacl)#**deny tcp 192.168.1.2 0.0.0.0 any eq telnet**

در شکل ۹-۱۰، برای Deny کردن pc4 برای جلوگیری از Telnet، باید پروتکل TCP و پورت 23 که مربوط به Telnet است را Deny کنید. در زیر جدول مربوط به پروتکل‌ها و شماره‌ی پورت‌ها مشخص شده است.

www.takbook.com

Decimal	Keyword	Description	Protocol
0		Reserved	
1-4		Unassigned	
20	FTP-DATA	FTP (data)	TCP
21	FTP	FTP	TCP
23	TELNET	Terminal connection	TCP
25	SMTP	SMTP	TCP
42	NAMESERVER	Host name server	UDP
53	DOMAIN	DNS	TCP/UDP
69	TFTP	TFTP	UDP
70		Gopher	TCP/IP
80	HTTP	WWW	TCP
133-159		Unassigned	
160-223		Reserved	
162		FNP	UDP
224-241		Unassigned	
242-251		Unassigned	

شکل ۹-۱۰ *پورت‌های شبکه*

Router(config-ext-nacl)#**deny tcp 192.168.1.2 0.0.0.0 any eq telnet**

چون در اینجا قرار است که Telnet را برای pc4 ببندیم، از پروتکل TCP طبق جدول و از پورت ۲۳ که مربوط به Telnet است، استفاده می‌کنیم، پس به این صورت بخوانیم که Deny کن، پروتکل TCP را برای هاست 192.168.1.2 با Wild Card mask، 0.0.0.0 و با پورت 23 که مربوط به Telnet است.

بعد از این کار، تمام ترافیک مربوط به 192.168.1.2 فیلتر می‌شود، به خاطر این باید از دستور زیر در آخر کار برای Permit دادن به بقیه‌ی شبکه استفاده کرد.

Router(config-ext-nacl)#**permit ip any any**

با این کار، pc4 می‌تواند با روتر ارتباط داشته باشد و فقط پروتکل Telnet بسته شده است.

اگر یادتان باشد در access List standard همه‌ی ترافیک مربوط به یک دستگاه فیلتر می‌شد و حق دسترسی به هیچ عنوان نداشت، اما در accesslist Extended این چنین نیست و فقط pc2 نمی‌تواند Telnet کند، اما می‌تواند روتر را ping کند.

در ادامه باید این access List را روی پورت روتر فعال کنیم:

Router(config-if)#**ip access-group PC4toTelNET in**

www.takbook.com

پس این دستور به این صورت خوانده می‌شود که Ip access-group PC4toTelNET را بر روی این پورت به صورت ورودی فعال کن، ورودی یعنی این‌که Pc4 در حال ورود به روتر است. اگر از Pc4 به روتر Telnet کنیم، جواب نمی‌دهد.

```
PC>telnet 192.168.2.1
Trying 192.168.2.1 ...
% Connection timed out; remote host not responding
```

اما اگر به روتر ping کنیم، جواب می‌گیریم:

```
PC>ping 192.168.2.1

Pinging 192.168.2.1 with 32 bytes of data:

Reply from 192.168.2.1: bytes=32 time=1ms TTL=255
Reply from 192.168.2.1: bytes=32 time=0ms TTL=255
Reply from 192.168.2.1: bytes=32 time=0ms TTL=255
Reply from 192.168.2.1: bytes=32 time=0ms TTL=255

Ping statistics for 192.168.2.1:
   Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
   Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

دستور Show access-lists

این دستور، تعداد Access List های موجود در روتر را با جزئیات نمایش می‌دهد:

```
Router(config)#do sh ip access-list
Extended IP access list PC4toTelNET
```

توجه داشته باشید که دستورات به صورت خلاصه‌شده وارد شده است و چون در مد Global هستیم، در اول دستور از do استفاده کردیم.

دستور show access-list

با این دستور می‌توانیم جزئیات یک access-list را مشاهده کنیم:

```
Router#show access-lists PC4toTelNET

Extended IP access list PC4toTelNET
   deny tcp 192.168.2.0 0.0.0.255 any eq telnet (24 match(es))
   permit ip any any (8 match(es))
```

مثال دوم

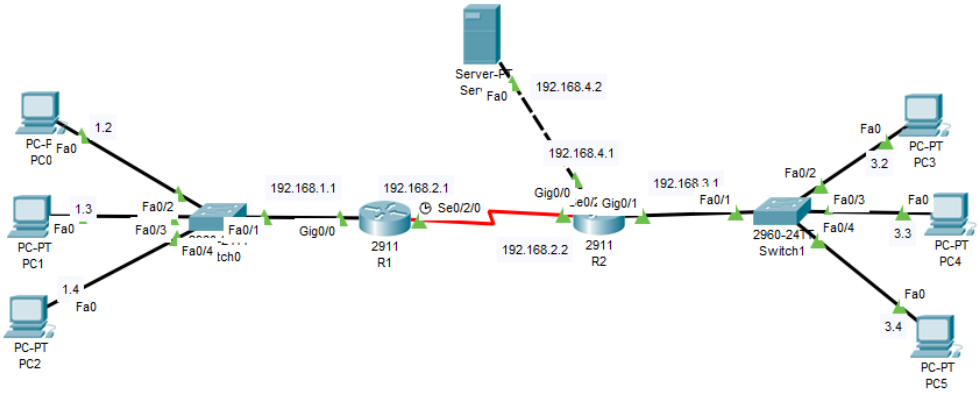
www.takbook.com

برای اینکه بیشتر با Access List پیشرفته آشنا شویم و کار کنیم یک مثال دیگر را با هم بررسی می‌کنیم، به مانند شکل ۱۰-۱۰، می‌خواهیم سه کار را انجام دهیم:

۱- جلوگیری از دسترسی شبکه‌ی 192.168.1.0 به شبکه‌ی 192.168.4.0

۲- اجازه دادن به کلاینت PC3 با آدرس 192.168.3.2 برای دسترسی به سرویس FTP در سرور 192.168.4.2 و جلوگیری از دسترسی دیگر کلاینت‌های شبکه به سرویس FTP .

۳- اجازه دادن به سایر سرویس‌ها در شبکه‌ی 192.168.3.0 .



شکل ۱۰-۱۰ سناریو برای ACL

برای شروع کار وارد کلاینت و سرور شوید و آدرس IP آنها را که در سناریو هم مشخص شده وارد و حتماً Default Gateway را هم وارد کنید.

تنظیمات روتر R1

```
Router(config)#interface gigabitEthernet 0/0
Router(config-if)#ip address 192.168.1.1 255.255.255.0
Router(config-if)#no sh

Router(config)#int serial 0/2/0
Router(config-if)#ip address 192.168.2.1 255.255.255.0
Router(config-if)#clock rate 72000
Router(config-if)#encapsulation ppp
Router(config-if)#no sh

Router(config-if)#router rip
Router(config-router)#network 192.168.1.0
Router(config-router)#network 192.168.2.0
```

تنظیمات روتر R2

www.takbook.com


```
Router(config)#int gigabitEthernet 0/0
Router(config-if)#ip address 192.168.4.1 255.255.255.0
Router(config-if)#sh

Router(config-if)#int gigabitEthernet 0/1
Router(config-if)#ip address 192.168.3.1 255.255.255.0
Router(config-if)#no sh

Router(config)#int serial 0/2/0
Router(config-if)#ip address 192.168.2.2 255.255.255.0
Router(config-if)#encapsulation ppp
Router(config-if)#no sh

Router(config-if)#router rip
Router(config-router)#net 192.168.2.0
Router(config-router)#net 192.168.3.0
Router(config-router)#net 192.168.4.0
```

تا به اینجا روترها را تنظیم و آدرس آنها را مشخص کردیم و برای Routing هم از پروتکل RIP استفاده کردیم تا همه‌ی سیستم‌ها بتوانند همدیگر را ببینند.

اگر از PC0 در شبکه‌ی 192.168.1.0 به PC5 در شبکه‌ی 192.168.3.0 ارتباط برقرار کنید، نتیجه‌ی آن به صورت زیر خواهد بود:

```
C:\>ping 192.168.3.4

Pinging 192.168.3.4 with 32 bytes of data:

Reply from 192.168.3.4: bytes=32 time=2ms TTL=126
Reply from 192.168.3.4: bytes=32 time=1ms TTL=126
Reply from 192.168.3.4: bytes=32 time=1ms TTL=126
Reply from 192.168.3.4: bytes=32 time=3ms TTL=126

Ping statistics for 192.168.3.4:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 1ms, Maximum = 3ms, Average = 1ms
```

حالا می‌خواهیم تنظیمات Access List را روی روترها پیاده کنیم، برای این کار وارد روتر R2 شوید و دستورات زیر را به دقت وارد کنید:

```
Router(config)#access-list 150 deny ip 192.168.1.0 0.0.0.255 192.168.4.0 0.0.0.255
Router(config)#access-list 150 permit tcp 192.168.3.2 0.0.0.0 192.168.4.2 0.0.0.0 eq ftp
Router(config)#access-list 150 deny tcp 192.168.3.0 0.0.0.255 192.168.4.2 0.0.0.0 eq ftp
Router(config)#access-list 150 permit ip any any
```

با دستور اول یک Access List با شماره‌ی 150 ایجاد شده و شبکه‌ی 192.168.1.0 را برای دسترسی به شبکه‌ی 192.168.4.0 بلاک می‌کند.

www.takbook.com

در دستور دوم دسترسی به سرویس FTP را در سرور 192.168.4.2 به کلاینت PC3 که آدرس آن 192.168.3.2 است می‌دهد.

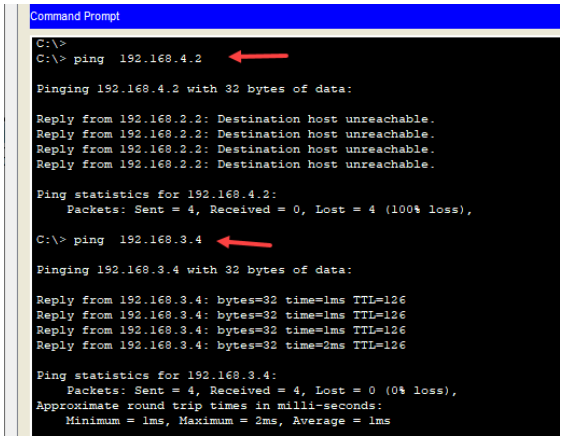
در دستور سوم تمام شبکه 192.168.3.0 را برای دسترسی به سرویس FTP در سرور 192.168.4.2 بلاک می‌کند.

در دستور آخر هم به مانند درس‌های قبلی باید بقیه شبکه را Permit کنید.

بعد از اینکه دستورات Access List را تعریف کردید باید این دستورات را بر روی Interface که به سمت سرور است اعمال کنیم برای همین باید در همین روتر دستور زیر را وارد کنید:

```
Router(config)#interface gigabitEthernet 0/0
Router(config-if)#ip access-group 150 out
```

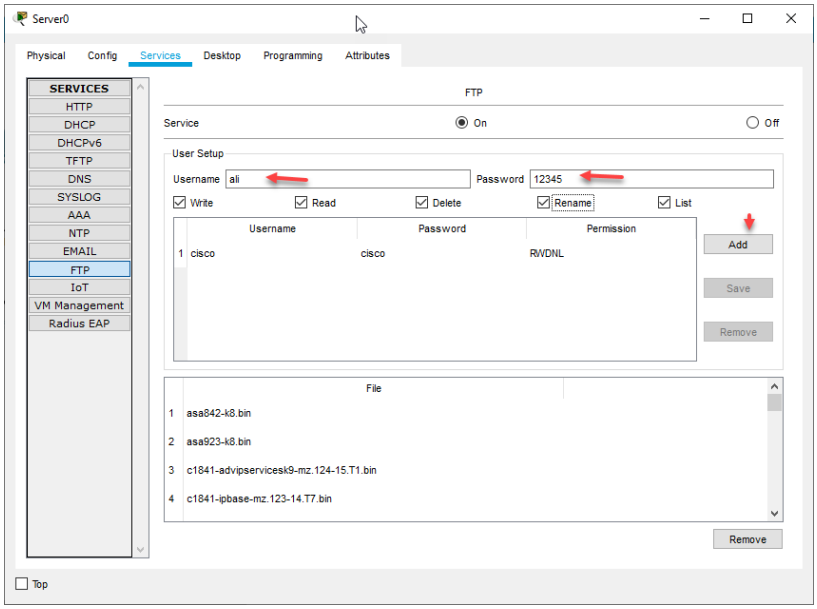
با این دستورات حالا می‌توانیم نتیجه‌ی کار را تست بگیریم، وارد PC2 شوید و آدرس سرور را Ping بگیرید، مشاهده خواهید کرد که پیغام Destination host unreachable می‌دهد ولی اگر شبکه‌ی 192.168.3.0 را بررسی کنید متوجه خواهید شد که عملیات Ping به صورت کامل انجام خواهد شد.



شکل ۱۱-۱۰ تنظیمات PC2

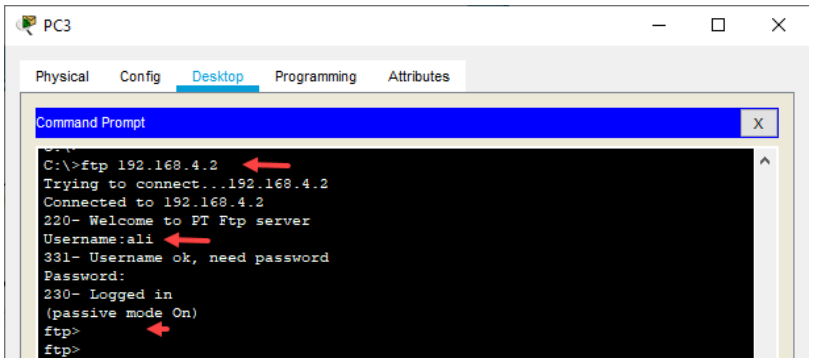
در قسمت قبل، دستور اول از Access List را بررسی کردیم و در ادامه در شکل ۱۲-۱۰، دستور دوم را بررسی می‌کنیم، برای این کار اول وارد سرور شوید و از تب سرویس بر روی FTP کلیک کنید و یک کاربر با نام ali تعریف و رمز عبور آن را مشخص کنید و بر روی Add کلیک کنید تا به لیست اضافه شود.

www.takbook.com



شکل ۱۲-۱۰ تنظیمات Server0

بعد از تعریف کاربر باید به مانند شکل ۱۳-۱۰، وارد PC3 که آدرس آن 192.168.3.2 است و به سرور 192.168.4.2 دسترسی دارد شوید و دستور FTP 192.168.4.2 را اجرا کنید تا به مانند شکل ۱۳-۱۰، از شما نام کاربری و رمز عبور را دریافت و وارد سرویس FTP سرور شود.



شکل ۱۳-۱۰ تنظیمات PC3

اگر در PC5 در شبکه 192.168.3.0 بخواهید به سرویس FTP دسترسی داشته باشید با خطای شکل ۱۴-۱۰، مواجه خواهید شد.

www.takbook.com


```
Packet Tracer PC Command Line 1.0
C:\>ftp 192.168.4.2
Trying to connect...192.168.4.2

%Error opening ftp://192.168.4.2/ (Timed out)
.



(Disconnecting from ftp server)
```

شکل ۱۰-۱۴ تنظیمات PC3

۱۰-۴ سوالات فصل دهم

www.takbook.com

1. Which of the following header fields identify which TCP/IP application gets data received by the computer? (Choose two answers.)

کدام یک از قسمت های هدر زیر مشخص می‌کند که کدام برنامه TCP / IP داده های دریافت شده توسط رایانه را دریافت می‌کند؟ (دو جواب را انتخاب کنید.)

a. Ethernet Type
b.SNAP Protocol Type
c. IP Protocol
d. TCP Port Number
e. UDP Port Number

2. Which of the following are typical functions of TCP?(Choose four answers.)

کدام یک از گزینه‌های زیر عملکردهای معمولی TCP است؟ (چهار جواب را انتخاب کنید.)

a. Flow control (windowing)
b. Error recovery
c. Multiplexing using port numbers
d. Routing
e. Encryption
f. Ordered data transfer

3. Which of the following functions is performed by both TCP and UDP?

کدام یک از توابع زیر توسط TCP و UDP انجام می‌شود؟

a. Windowing
b. Error recovery
c. Multiplexing using port numbers
d. Routing
e. Encryption
f. Ordered data transfer

4. What do you call data that includes the Layer 4 protocol header, and data given to Layer 4 by the upper layers, not including any headers and trailers from Layers 1 to 3? (Choose two answers.)

شما از داده‌هایی استفاده می کنید که شامل هدر پروتکل Layer 4 و داده هایی است که توسط لایه های فوقانی به لایه ۴ داده می‌شود ، کدام یک از گزینه‌های زیر شامل هدر و پیش پرده‌های لایه‌های ۱ تا ۳ نیست؟ (دو جواب را انتخاب کنید.)

a. L3PDU
b. Chunk
c. Segment
d. Packet
e. Frame
f. L4PDU

5. In the URI http://blog.3isco.ir/config-labs, which part identifies the web server?

کدام گزینه سرور وب را مشخص می‌کند؟

a. http

b. blog.3isco.ir
c. 3isco.ir
d. http:// blog.3isco.ir
e. The file name.html includes the hostname.

www.takbook.com

6. Fred opens a web browser and connects to the www.certskills.com website. Which of the following are typically true about what happens between Fred's web browser and the web server? (Choose twoanswers.)

فردی یک مرورگر وب باز می‌کند و به سایت 3isco.ir مراجعه می‌کند، کدام گزینه معمولاً اتفاقات بین سرور وی و کلاینت را نشان می‌دهد. (دو جواب را انتخاب کنید.)

a. Messages flowing toward the server use UDP destination port 80.
b. Messages flowing from the server typically use RTP.
c. Messages flowing to the client typically use a source TCP port number of 80.
d. Messages flowing to the server typically use TCP.

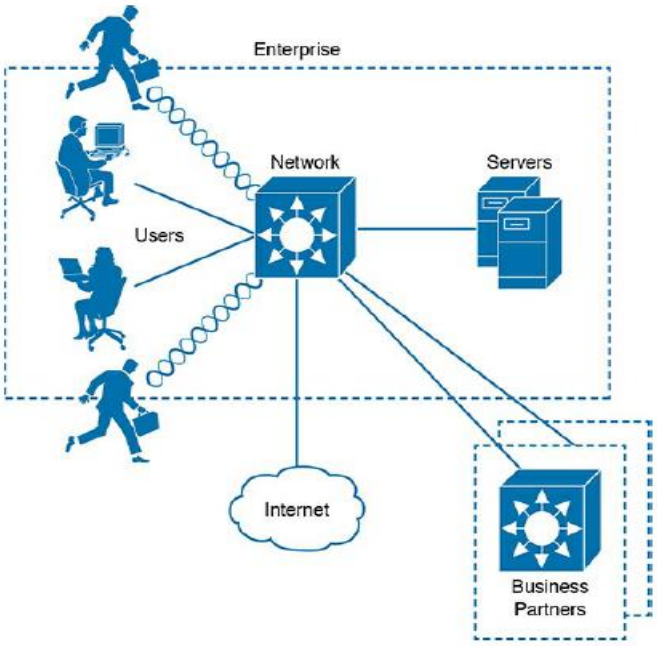
www.takbook.com

فصل یازدهم

امنیت شبکه

یکی از موضوعات مهم در بحث شبکه ایجاد یک لایه امنیتی مناسب برای محافظت از سرورها و دستگاه‌های شبکه مانند روتر، سوئیچ و ... است.

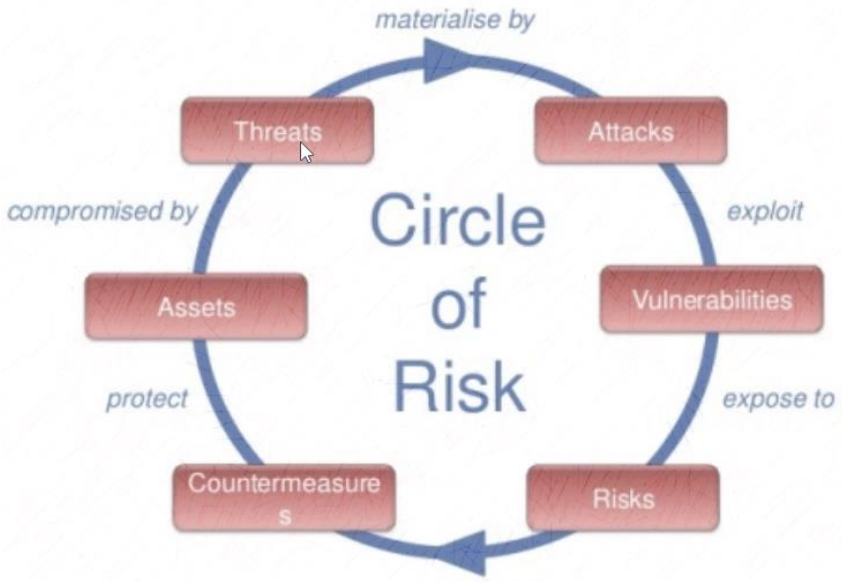
امروزه اکثر شرکت‌های تجاری باید به صورت کامل و قوی با دنیای بیرون ارتباط داشته باشند و این ارتباط از طریق اینترنت صورت خواهد گرفت، یعنی کارمندان می‌توانند از طریق لپ تاپ، موبایل و ... و از طریق قوانینی که مدیرشبکه تعریف می‌کند به شبکه متصل شوند، شاید بخواهید برای مهمانانی که به شرکت می‌آیند یک لینک وایرلس قرار دهید و ایجاد این لینک با مشکلاتی همراه باشد و نتوانید خوب آن را تنظیم کنید و این می‌تواند به شبکه شما ضربه بزند.



شکل ۱-۱۱ /امنیت شبکه

www.takbook.com

برای اینکه یک شبکه را بهتر بشناسیم باید ریسک‌های شبکه را بررسی کنیم که با هم در این قسمت این کار ار انجام می‌دهیم.



شکل ۲-۱۱ / ریسک‌های شبکه

- **منابع یا دارایی‌های سازمان (Assets)**

در این بخش باید منابع با ارزش سازمان مشخص شود، که این منابع می‌تواند شامل داده‌ها، برنامه‌ها و سرورها و... باشد.

در زیر جدولی از منابع موجود را مشاهده می‌کنید.:

جدول ۱-۱۱ منابع شبکه

طبقه‌بندی‌های دولتی	حساس اما غیر طبقه‌بندی شده(SBU) محرمانه راز فوق‌سری
طبقه‌بندی بخش خصوصی و عمومی	حساس خصوصی محرمانه
معیارهای طبقه‌بندی ارزش	سن هزینه جایگزینی

www.takbook.com

	طول عمر مفید

- **آسیب‌پذیری (Vulnerability)**

نقص یا ضعف در طراحی، پیاده‌سازی، بهره‌برداری و مدیریت یک سیستم می‌توانند برای نقض سیاست امنیتی سیستم، مورد سوء استفاده قرار گیرند. اصولاً مهاجمان از آسیب‌پذیری‌هایی که از طریق نرم‌افزار، سخت‌افزار و یا کارمندان به وجود می‌آید می‌توانند به شبکه سازمان حمله کنند، بیشتر سازمان‌های امروزی یک ارزیابی کلی برای شناسایی این آسیب‌پذیری‌ها انجام می‌دهند.

طبقه‌بندی آسیب‌پذیری‌ها به صورت زیر بیان می‌شود:

- Policy flaws (نقص در سیاست سازمان)
- Design errors (طراحی اشتباه)
- Protocol weaknesses (ضعف در پروتکل)
- Misconfiguration (تنظیمات اشتباه)
- Software vulnerabilities (آسیب‌پذیری نرم‌افزار)
- Human factors (عوامل انسانی)
- Malicious software (نرم‌افزارهای مخرب)
- Hardware vulnerabilities (آسیب‌پذیری سخت‌افزاری)
- Physical access to network resources (دسترسی فیزیکی به منابع شبکه)

- **تهدیدات (Threat)**

تهدیدات زمانی رخ می‌دهد که مهاجم در بخش قبلی (**Vulnerability**)، آسیب‌پذیری‌های یک سیستم را شناسایی کند و بتواند از آن طریق به شبکه ما ضربه بزند، یک مثال ساده در این بخش، می‌تواند به اشتراک گذاشتن یک پوشه با دسترسی اشتباه باشد.

- **عامل تهدیدات (Threat agent)**

عامل، کسی است که تهدیدات را به وجود می‌آورد، مثلاً مهاجمی که از ACL یا همان Access List اشتباه استفاده می‌کند می‌تواند عامل تهدید باشد که این عامل‌ها می‌توانند آسیب‌پذیری‌ها را شناسایی و از آنها برای حمله به شبکه استفاده کنند، البته همه عامل‌ها این کار را انجام نمی‌دهند.

- **ریسک (Risk)**

احتمال یک خطر است که توسط یک عامل تعدید (Threat agent) از طریق پیدا کردن یک آسیب‌پذیری در شبکه به وجود می‌آید، کاهش ریسک‌های یک شبکه بسته به سیاست‌هایی دارد که مدیرشبکه پیاده‌سازی می‌کند.

www.takbook.com

روش‌هایی که در اقدام متقابل می‌توان از آنها استفاده کرد شامل موارد زیر است:

۱- اجرایی (Administrative) که شامل استانداردها، رویه‌ها، دستورالعمل‌ها و سیاست‌های سازمان است که باید به صورت کتبی از همه کاربران تعهد گرفت تا خلاف آن عمل نکنند.

۲- فیزیکی (Physical) شامل کنترل‌های فیزیکی دقیق برای تجهیزات شبکه خود است، مثلاً می‌توانید برای اتاق سرور خود از درب‌های ضد سرقت پیشرفته و نسوز استفاده کنید و یا اینکه رک‌های دیواری که در هر طبقه موجود هستند را قفل کنید، طراحی باید به صورتی باشد که کاربران به هیچ قطعه یا سیسمی دسترسی نداشته باشند.

۳- منطقی (Logical) که شامل کنترل‌های منطقی شامل گذرواژه‌ها ، فایروال‌ها ، سیستم‌های پیشگیری از نفوذ، لیست‌های دسترسی ، تونل‌های VPN و... است که کنترل‌های منطقی اغلب به عنوان فنی، گفته می‌شوند.

- **در معرض قرار گرفتن (Exposure)**

وقتی که به یک پوشه به اشتراک گذاشته شده یک دسترسی اشتباه می‌دهید، آن پوشه در معرض تهدیدات قرار خواهد گرفت و امنیت شرکت را زیر سوال خواهد برد.

- **اقدام متقابل (Countermeasure)**

اقدام متقابل، ریسک‌های یک شبکه را کاهش خواهد داد، برای انجام یک کار در شبکه سه موضوع آسیب‌پذیری، تهدیدات و ریسک باید مورد توجه قرار گیرد تا بتوان اقدام متقابل را برای آنها انجام داد.

۱-۱۱ فرآیند مدیریت ریسک (Risk Management Process)

فرآیند مدیریت ریسک شامل یک سرس عملیات است که عبارتند از:

- ✓ شناسایی کردن منابع و ارزش‌های سازمان
- ✓ شناسایی تهدیدات
- ✓ شناسایی آسیب‌پذیری
- ✓ تعیین احتمال حمله
- ✓ شناسایی ضربه
- ✓ تعیین ریسک به عنوان ترکیبی از احتمال و تاثیر.

طبقه‌بندی منابع (Asset Classification)

www.takbook.com

اولین قدم در ارزیابی ریسک‌ها شناسایی منابع و ارزش‌های آن سازمان است، دارایی‌هایی که در یک سازمان وجود دارد مشهود و غیر مشهود است که دارایی‌های مشهود عبارتند از:

کاربران، کامپیوترها، امکانات و منابع.

ولی دارایی‌های غیر مشهود شامل مالکیت معنوی داده‌ها و شهرت سازمانی است.

۲-۱۱ شناخت تهدیدات شبکه فعلی

تهدیدات امروز به طور مداوم در حال تغییر هستند و تهدیدهای جدیدی ظهور می‌کنند، در این قسمت می‌خواهیم به دسته‌های مختلف تهدیدات شبکه بپردازیم:

۱- مهاجمان نهایی (**Potential Attackers**)

که این مورد اشاره دارد به هکرها، تروریست‌ها، کارکنان ناراضی یک شرکت و...

۲- روش‌های حمله (**Attack Methods**)

یک هکر، به هیچ عنوان دوست ندارد شناسایی شود، به خاطر همین از روش‌هایی برای مخفی کردن خود استفاده می‌کند و کارهایی را که در زیر لیست شده است را برای نفوذ به شبکه انجام می‌دهد که شامل:

جدول ۲-۱۱، روش‌های حمله به شبکه

شناسایی (Reconnaissance)	در اولین قدم هکر با استفاده از نرم‌افزار خاصی اقدام به شناسایی آدرسIP و پورت‌های باز شبکه می‌کند تا موارد قابل نفوذ را شناسایی کند.
مهندسی اجتماعی (Social engineering)	یکی از روش‌های ساده برای بدست آوردن اطلاعات یک سازمان است، در این روش هکر با استفاده از کارمندان یک سازمان اقدام به بدست آوردن اطلاعات مهم آن می‌کند، مثلاً می‌تواند با استفاده از ایمیل‌های جعلی از کارمندان اطلاعات بگیرد یا اینکه از فیشینگ کردن وب‌سایت‌های مشخص استفاده کند تا به اطلاعات خود دست پیدا کند.
حداکثر امتیاز (Privilege escalation)	در این روش مهاجم با استفاده از یک کاربر معمولی وارد روتر می‌شود و با استفاده از حملات brute-force شروع به بدست آوردن حداکثر دسترسی می‌کند.

www.takbook.com

در پشتی (Back doors)	مهاجم بعد از ورود به شبکه اقدام به نصب نرم‌افزارهای مخرب بر روی کلاینت یا سرور می‌کند و بعد از آن در هر زمان می‌تواند به اطلاعات آنها دستگاه دست پیدا کند، مانند نرم‌افزارهای Key-logging که تمام اطلاعات ورودی از کیبورد را ذخیره و به آدرس خاصی ارسال می‌کنند.
اجرای کد (Code execution)	در این روش مهاجم توانایی این را دارد که کدها مورد نظر خود را در سرور سازمان شما اجرا کند که این کار یکی از خطرناکترین حملات است این روش با نام Remote Code Execution یا به اختصار RCE شناخته می‌شود.

۳- راه‌های حمله (**Attack Vector**)

این موضوع را به خاطر داشته باشید فرد مهاجم همیشه از بیرون شرکت به شبکه شما حمله نمی‌کند و شاید کسی از داخل شرکت این کار را انجام دهد، شاید کاربر از سر بی‌اطلاعی بخواهد بر روی موضوع خاصی کنجکاوی کند و همان موضوع باعث شود حملات درب پشتی (Back doors) انجام شود. برای جلوگیری از این روش باید سیاست‌های درست پیاده‌سازی شود.

۴- حملات Denial-of-Service

این نوع حملات با نام DOS (Denial-of-Service) و DDOS (Distributed Denial-of-Service) شناخته می‌شود که اصولاً برای از کار انداختن سرور یا سرورها به کار می‌رود، تلاش این نوع حملات برای از کار انداختن سرویس‌های تحت وب مانند هاستینگ و... است که با این کار سایت مورد حمله برای دقایقی یا برای همیشه از کار خواهد افتاد، تفاوت بین حمله DOS با DDOS این است که حمله DOS از طریق یک سیستم انجام می‌شود ولی حمله DDOS که به عنوان حمله توزیع شده شناخته می‌شود با استفاده از چندین سرور انجام می‌گیرد، با این کار روترها، سوئیچ‌ها و دیگر دستگاه‌ها متصل به شبکه با افزایش درخواست‌ها مواجه می‌شوند و همین موضوع باعث می‌شود کارایی CPU افزایش یابد و دستگاه از کار بیفتد.

روش‌های حمله:

تداخل در ارتباط کاربران با شبکه.

ریسیت کردن کانکشن‌های TCP در ارتباط‌ها.

ایجاد تداخل در دستگاه‌های شبکه.

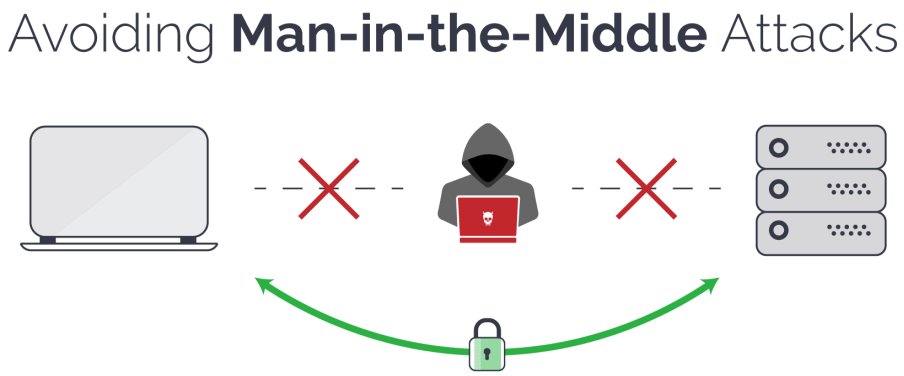
ایجاد اختلال در وضعیت روترها مانند اطلاعات مسیریابی.

مصرف حداکثری منابع مانند پهنای باند، دیسک و...

www.takbook.com

۵- حمله مرد میانی (**Man-in-the-Middle Attacks**)

حملات مرد میانی با نام Bucket Bridge Attack هم شناخته می‌شود، در این نوع حمله مهاجم خود را بین دو سیستم قرار می‌دهد و از روش‌های خاصی برای بدست آوردن اطلاعات سیستم‌ها استفاده می‌کند، این کار با هدف شناسایی و دستکاری داده‌ها انجام می‌شود، این حمله می‌تواند در لایه دو و یا لایه سه اتفاق بیفتد، هدف اصلی این کار، گوش دادن به اطلاعات رد و بدل شده بین دو منبع است.



شکل ۳-۱۱ حمله Man in the middle

۶- سایر روش‌های حمله

۷- *جدول ۳-۱۱ روش‌های حمله*

کانال پنهان (Covert channel)	در این روش اگر شما به عنوان مدیرشبکه اجازه دسترسی به یک وب‌سایت را در فایروال ببندید، کاربر یا مهاجم با استفاده از VPN و ایجاد تونل در شبکه داخلی باعث می‌شود این سیاست شما را دور بزند.
منطقه قابل اعتماد	در این روش اگر در یک فایروال که دارای سه منطقه است و به منطقه خارجی (outside) آن دسترسی کامل دهید، مهاجم با ورود به سرورهای مستقر در منطقه DMZ می‌تواند به سیستم‌های داخل Inside دسترسی پیدا کند.

www.takbook.com

حملات بی رحمانه با رمز عبور Brute-force) ((passwordguessing) attacks	در این روش مهاجم با استفاده از دیتابیسی از کلمه عبور، تلاش می‌کند رمز عبور سیستم را حدس بزند که البته با ایجاد سیاست، تعداد تلاش برای وارد کردن رمز عبور، این مورد حل می‌شود.
Botnet	در این حمله مهاجم در یک سازمان دارای هزاران سیستم آلوده آماده به کار هست و با استفاده از آنها بدون اطلاع صاحبان شرکت شروع به حمله به یک مقصد مشخص می‌کند که از این طریق می‌توان حملات DDOS را انجام داد.

۳-۱۱ کنترل و نظارت بر دسترسی کاربران

یکی از راه‌های مدیریت درست کاربران استفاده از ابزارهای لازم برای نظارت بر روی کار آنها و ایجاد دسترسی مناسب برای دستیابی به منابع شبکه است.

برای ایجاد یکپارچگی در اطلاعات باید سطح دسترسی را برای افراد مشخص کنید تا از افشای اطلاعات در بیرون سازمان جلوگیری شود، سه اصل؛ شناسایی(Identification)، احراز هویت(Authentication)، مجوز دسترسی(Authorization) می‌تواند شما را در این امر بسیار کمک کند.

برای اینکه جلوی دسترسی غیرمجاز به شبکه گرفته شود و کاربرانی که اجازه‌ی دسترسی به شبکه را دارند مشخص شوند بهترین راه استفاده از سیستم AAA یا authentication, authorization, and accounting است.

هدف اصلی AAA این است که چه کسی به چه جایی باید دسترسی داشته باشد و عملکرد آن به چه صورت بوده است یعنی اینکه چه کاربری در چه زمانی وارد شبکه شده است و چه کاری انجام داده است.

حساب‌های کاربری که در AAA ثبت می‌شوند می‌توانند به صورت محلی باشند و یا اینکه از طریق سرویس Active Directory انجام گیرد.

احراز هویت(Authentication)

احراز هویت فرایندی است که توسط آن مشخص می‌شود یک فرد همان کاربر مورد نظر است یا خیر، برای احراز هویت روش‌های مختلفی وجود دارد که می‌توان به نام کاربری و رمز عبور، کارت‌های هوشمند و... اشاره کرد، معمولاً استفاده از Authenticaion می‌تواند برای دسترسی به کنسول روتر، پورت VTY، Auxiliary و... باشد.

www.takbook.com

مجوز دسترسی(Authorization)

در این قسمت بعد از اینکه کاربر مورد نظر از نظر احراز هویت بررسی شد و توانست وارد دستگاه مورد نظر شود باید مجوزهای لازم را برای دسترسی به منابع شبکه برای آن تایین کنید، مثلاً می‌توانید مشخص کنید کاربر در یک ساعت مشخص بتواند وارد شبکه شوند و یا اینکه برای مدیران مشخص کنید که چه چیزی را می‌توانند ببینند و تغییر دهند.

حسابداری و حسابرسی(Accounting and auditing)

کاربر بعد از انجام دو مرحله بالا شروع به کار در شبکه می‌کند و به مسیرهای مختلفی وارد و عملیات خود را انجام می‌دهد، برای اینکه متوجه شویم کاربر به چه مسیری رفته و چه کاری در چه زمانی انجام داده باشند این سرویس را برای آن فعال کنیم، یکی از سیستم‌های حسابرسی می‌توان به عملیات بانکی اشاره کرد که در آن مقدار پول دریافتی و جزئیات آن به صورت دقیق مشخص شده است.

توجه داشته باشید برای اینکه با سرور AAA ارتباط برقرار کنیم باید از پروتکل‌های خاصی استفاده کنیم که این پروتکل‌ها شامل TACACS+ و RADIUS هستند، پروتکل TACACS+ مختص شرکت سیسکو و دیگری عمومی و در همه دستگاه‌ها اجرا می‌شود.

۱۱-۳-۱ پروتکل TACACS+

TACACS+ یا Terminal Access Controller Access-Control System پروتکلی از شرکت سیسکو می‌باشد که از سال ۱۹۹۳ به عنوان یک استاندارد برای احراز هویت به کار گرفته شده است. این پروتکل به صورت پیش‌فرض از پورت ۴۹ (TCP,UDP) برای تبادل ارتباط خود استفاده می‌کند.

۱۱-۳-۲ پروتکل Radius

Radius یا Remote Authentication Dial-In User Service یک پروتکل شبکه است که در ورژن جدید آن بر روی پورت ۱۸۱۲ عمل می‌کند و مدیریت تایید هویت، مجوز و دسترسی را به کاربرانی که می‌خواهند از یک سرویس در شبکه استفاده کنند می‌دهد، این پروتکل مختص شرکت خاصی نیست و به صورت عمومی ارائه شده است و اکثر سیستم‌ها از این پروتکل پشتیبانی می‌کنند.

Radius یک پروتکل سرویس دهنده و گیرنده (Server/Client) است در لایه Application مدل OSI کار می‌کند و برای تبادل اطلاعات از دو پروتکل TCP و UDP استفاده می‌کند، این پروتکل بیشتر بر روی سیستم‌عامل‌های لینوکس و ویندوز پیاده‌سازی می‌شود.

۱۱-۳-۳ تفاوت بین پروتکل Radius و TACACS+

جدول ۱۱-۴ تفاوت Radius و TACACS

	+TACACS	Radius

www.takbook.com

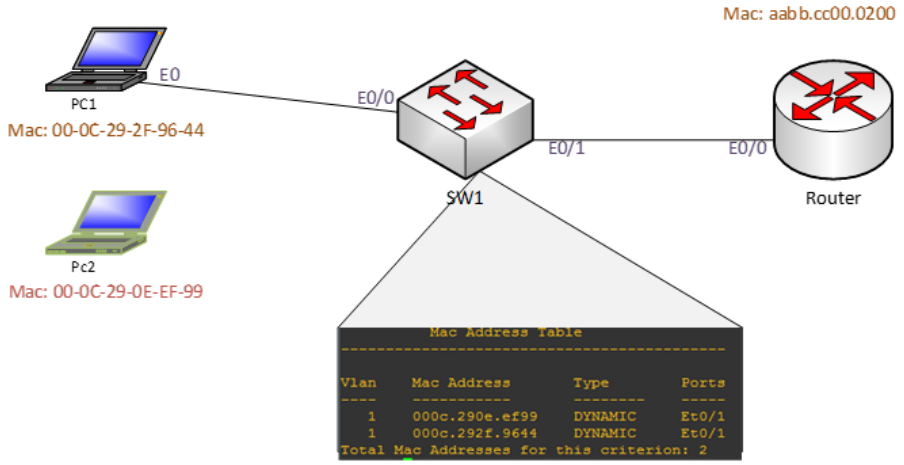
عملکرد	این پروتکل سه فرآیند Authentication، Authorization و Accounting را به صورت جداگانه انجام می‌دهد و عملکرد جداگانه‌ای بر روی آنها دارد.	این پروتکل دو گزینه‌ی Authentication و Authorization را با هم انجام می‌دهد.
استاندارد	مختص شرکت سیسکو است و بسیار خوب عمل می‌کند.	به صورت عمومی در دسترس است و می‌توان روی هر دستگاه پیاده‌سازی شود.
لایه انتقال	بر روی پورت TCP عمل می‌کند.	بر روی پورت UDP عمل می‌کند.
محرمانگی	کل بسته‌های عبوری را رمزنگاری می‌کند و یکی از مهمترین ویژگی‌های آن می‌باشد.	فقط بسته‌هایی که دارای رمز عبور باشند را رمزنگاری می‌کند.
دسترسی	میزان دسترسی کاربران را می‌تواند مشخص کند.	نمی‌تواند.
پشتیبانی	از پروتکل‌های NetBIOS Frame Control Protocols، X.25، AppleTalk، NOVEL NASI پشتیبانی می‌کند.	نمی‌کند

۴-۱۱ کار با Port Security

در این قسمت می‌خواهیم روش امنیتی Port Security را بر روی سوئیچ‌های سیسکو راه‌اندازی کنیم، مثالی که برای این روش می‌توان زد این است که اگر شبکه سازمان خود را در نظر بگیرید و کاربران شما بخواهند از منابع شبکه در سیستمی استفاده کنند که عضو آن شبکه نیست و واقعاً می‌تواند برای شبکه شما بسیار بد و یک ضعف امنیتی بزرگ باشد، اگر کاربر کابل شبکه متصل شده به سوئیچ را به لپ تاپ شخصی خود متصل کند، می‌تواند به منابع شبکه دسترسی پیدا کند.

www.takbook.com

اما شرکت سیسکو برای جلوگیری از دزدیده شدن اطلاعات به این شکل روشی را تحت عنوان Port Security در سوئیچ‌های خود اضافه کرده که اگر چنانچه کاربری از یک سیستم غیرمجاز برای متصل شدن به شبکه استفاده کند، پورت مربوط به آن سیستم در سوئیچ خاموش خواهد شد و فقط توسط مدیر شبکه روشن می‌شود.



شکل ۴-۱۱ بررسی PortSecurity

در شکل۴-۱۱، که برای شما آماده کردیم دو Client به همراه یک سوئیچ و روتر را مشاهده می‌کنید که می‌خواهیم عملیات Port Security را روی آن انجام دهیم، در شکل ۴-۱۱، یک روتر و یک کلاینت به سوئیچ متصل شده‌اند و بعد از اتصال به مانند جدول ۵-۱۱، به پورت‌های آنها IP داده شده است.

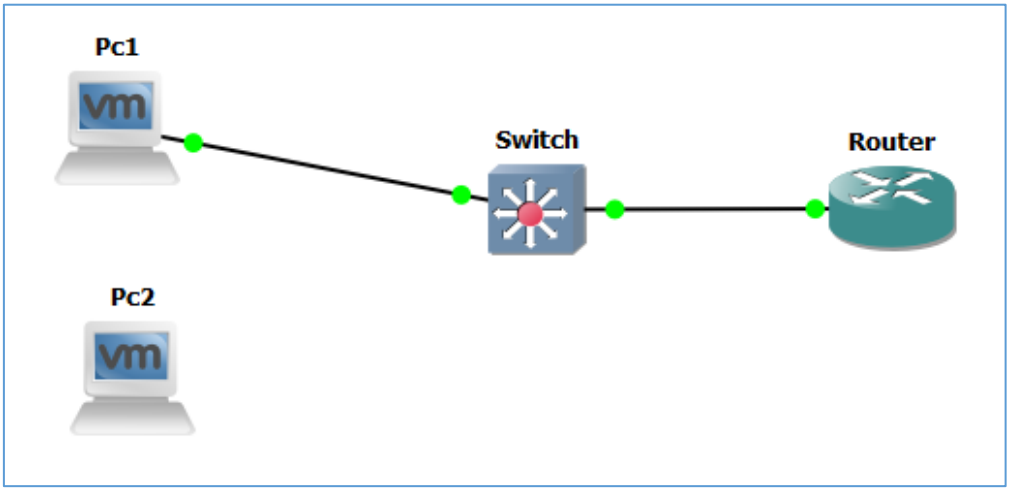
جدول ۵-۱۱ Ip Address

Device	Port	Address
PC1	E0/0	192.168.1.2
Router	E0/1	192.168.1.1

به مانند شکل ۴-۱۱، اگر به جدول MAC Table مربوط به سوئیچ(SW1) نگاه کنید، هر دو مک آدرس مربوط به روتر و کلاینت در آن ثبت شده است، حالا می‌خواهیم در ادامه با اجرای دستور Port Security اجازه ندهیم PC2 به سوئیچ متصل شود.

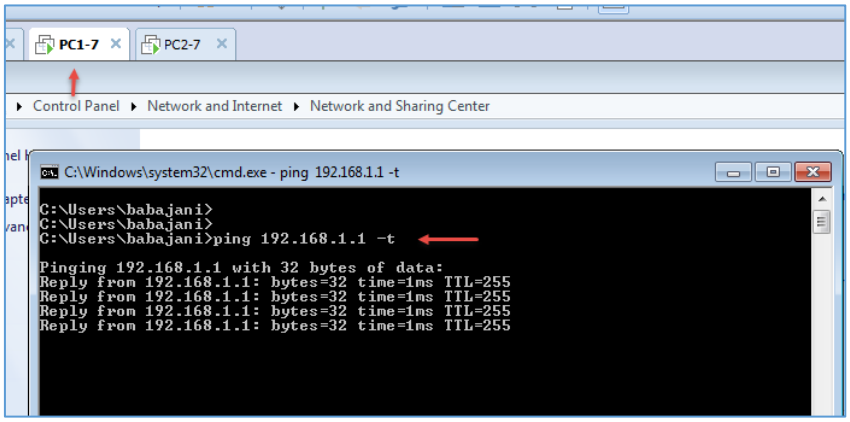
به مانند شکل ۵-۱۱، GNS3 را اجرا کنید و دو کلاینت که قبلاً با هم ایجاد کردیم و بر روی آنها ویندوز ۷ نصب کردیم را به لیست اضافه کنید، و یک سوئیچ لایه ۲ که در شکل با نام Switch مشخص است و یک سوئیچ لایه 3 که با نام Router مشخص شده است را به لیست اضافه کنید، تنظیمات مربوط به IP را بر روی روتر و کلاینت (PC1) که در جدول قبلی وارد کردیم را انجام دهید.

www.takbook.com



شکل ۵-۱۱ سناریو PortSecuirty

بعد از تنظیم IP، مانند شکل ۶-۱۱، وارد کلاینت PC1 شوید و روتر مورد نظر را Ping بگیرید، بعد از اینکه ارتباط اوکی بود به مرحله بعد می‌رویم.



شکل ۶-۱۱ بررسی PC1-7

وقتی یک دستگاه به سوئیچ متصل شود با اولین اتصال و ارسال درخواست به سوئیچ، آدرس Mac آنها در جدولی به نام Mac address Table ذخیره می‌شود و دستور Show Mac Address-Table به شما آدرس‌های Mac دستگاه‌های متصل شده به سوئیچ را نمایش می‌دهد، که این موضوع را در شکل ۷-۱۱، مشاهده می‌کنید.

www.takbook.com


```
Switch#show mac address-table
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
   1    000c.290e.ef99    DYNAMIC     Et0/1
   1    000c.292f.9644    DYNAMIC     Et0/1
Total Mac Addresses for this criterion: 2
Switch#
```

شکل ۷-۱۱ نتیجه دستور Show Mac Address-Table

در جدول ۶-۱۱، دستورات مربوط به Port Security را برای Interface بررسی می‌کنیم:

جدول ۶-۱۱ دستورات PortSecurity

	دستورات	هدف
مرحله اول	Switch(config)# interface interface_id	با این دستور وارد Interface مورد نظر می‌شویم مانند: Interface Fastethernet 0/0
مرحله دوم	Switch(config-if)# switchport mode access	با این دستور پورت مورد نظر به نوع Access تغییر خواهد کرد، توجه داشته باشید به صورت پیش‌فرض تمام پورت‌های سوئیچ بر روی dynamic desirable قرار دارد که بر روی این نوع پورت نمی‌توان Port Security را فعال کرد.
مرحله سوم	Switch(config-if)# switchport port-security	برای فعال کردن Port Security بر روی interface مورد نظر باید از این دستور استفاده کرد.
مرحله چهارم	Switch(config-if)# switchport port-security maximum value	با این دستور می‌توانید مشخص کنید که تعداد مک آدرس‌هایی که بر روی این پورت قرار است فعالیت کنند را مشخص کنید که این عدد می‌تواند بین ۱ تا ۴۰۹۷ باشد که به صورت پیش‌فرض بر روی ۱ قرار دارد.

www.takbook.com

مرحله پنجم	Switch(config-if)# switchport port-security violation {restrict | Protect | shutdown}	از این دستورات هم برای ایجاد نقض در کار استفاده می‌شود یعنی اینکه اگر کاربری از یک MAC آدرس ناآشنا استفاده کند پورت مورد نظر خاموش خواهد شد، این دستور دارای سه گزینه است: Shutdown که به صورت پیش‌فرض فعال است و پورت مورد نظر را خاموش خواهد کرد. Protect در این حالت به بسته‌هایی اجازه‌ی عبور می‌دهد که آدرس Mac آنها در سوئیچ تعریف شده باشد. Restrict این دستور هم به مانند دستور قبلی عمل می‌کند اما در قسمتی از دستور Show Port-Security در ستون Violation شماره‌ی آن را تغییر می‌دهد.
مرحله ششم	Switch(config-if)# switchport port-security limit rate invalid-source-mac	تعیین نرخ بسته‌های اشتباه.
مرحله هفتم	Switch(config-if)# switchport port-security mac-address mac_address	با این دستور می‌توانید به صورت دستی Mac Address سیستمی که قرار است به پورت مورد نظر متصل شود را وارد کنید.
مرحله هشتم	Switch(config-if)# switchport port-security mac-address sticky	این دستور باعث می‌شود که مک آدرس مربوط به سیستم مورد نظر به صورت اتوماتیک در جدول سوئیچ قرار بگیرد و نیاز به ورود به صورت دستی نیست.
مرحله نهم	Switch# show port-security address interface interface_id Switch# show port-security address	نمایش جزئیات عملکرد دستور Port Security به صورت کلی و بر روی Interface .

بعد از آشنایی با دستورات، حالا نوبت آن رسیده که این دستورات را روی سوئیچ پیاده کنیم، برای این کار طبق نقشه‌ای که در صفحات قبل ایجاد کردیم، بر روی سوئیچ مورد نظر دو بار کلیک کنید و دستورات جدول ۷-۱۱را وارد کنید.

جدول ۷-۱۱ اجرای PortSecurity

با این دستور وارد مد Global شوید.	Switch#**configur Terminal**

www.takbook.com

Switch(config)#**interface ethernet 0/0**	با این دستور وارد پورت ethernet 0/0 می‌شویم که به سیستم کلاینت PC1 متصل است.
Switch(config-if)#**switchport mode access**	این دستور مد پورت را به Access تغییر می‌دهد تا دستور Port Security بتواند بر روی آن اجرا شود.
Switch(config-if)#**switchport Port-Security**	دستور switchport Port-Security ویژگی Port Security را بر روی Interface مورد نظر فعال می‌کند.
Switch(config-if)#**switchport Port-Security mac-address sticky**	با این دستور به سوئیچ اعلام می‌کنیم که مک آدرس سیستمی که به این پورت متصل است را دریافت و در جدول ثبت کند.
Switch(config-if)#**switchport Port-Security maximum 1**	در این قسمت باید مشخص کنید در این پورت چند Mac Address قابلیت اضافه شدن به لیست دارند که در این دستور عدد ۱ انتخاب شده و فقط اولین سیستمی که به این پورت متصل شده آدرس Mac آن در لیست قرار می‌گیرد.
Switch(config-if)#**Switchport port-security violation Shutdown**	اگر در دستور قبلی Mac آدرسی به غیر از Mac آدرس سیستم فعلی بخواهد به متصل شود عملیات خاموش شدن پورت روی آن فعال خواهد شد، و فقط مدیر شبکه می‌تواند آن را روشن کند.

بعد از اجرای دستورات بالا و فعال‌سازی قابلیت Port Security می‌توانید با اجرای دستور شکل ۸-۱۱، از وضعیت این دستور با خبر شوید.

Switch(config-if)# **Show Port-Security**

```
Switch(config-if)#do sh port-security
Secure Port  MaxSecureAddr  CurrentAddr  SecurityViolation  Security Action
                (Count)       (Count)          (Count)
--------------------------------------------------------------------------
      Et0/0        1            1                0            Shutdown
--------------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 0
Max Addresses limit in System (excluding one mac per port) : 4096
```

شکل ۸-۱۱ نتیجه دستور show Port-Security

همانطور که در شکل ۸-۱۱، مشاهده می‌کنید بر روی پورت E0/0 این سرویس فعال شده است، در ستون شماره‌ی یک مقدار آدرس مشخص شده است که فقط یک آدرس اجازه دارد در جدول قرار بگیرد،

www.takbook.com

در ستون شماره‌ی دو این یک آدرس توسط Pc1 تکمیل شده است و اگر سیستم دیگری را به آن پورت متصل کنید در قسمت شماره‌ی سه به جای صفر عدد یک قرار خواهد گرفت و بعد در قسمت شماره‌ی چهار هم عملیات Shutdown اجرا خواهد شد. برای اینکه آدرس Mac ذخیره شده بر روی پورت مورد نظر را مشاهده کنید باید از دستور زیر استفاده کنید:

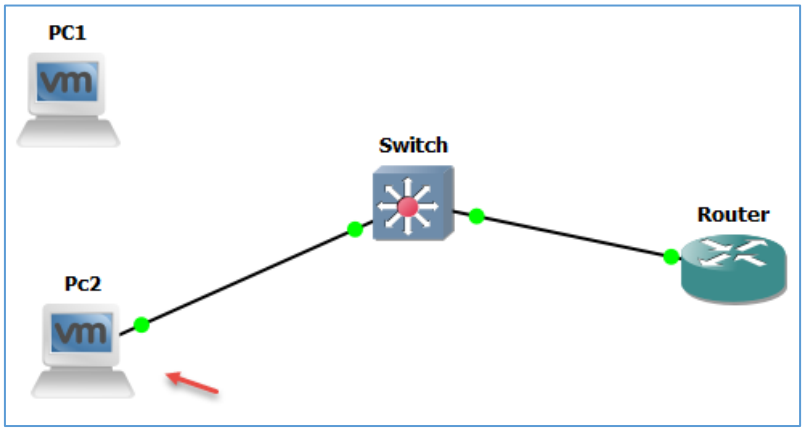
Switch#**show port-security address**

در شکل ۹-۱۱، دستور مورد نظر اجرا و آدرس MAC و شماره پورت آن مشخص شده است.

```
Switch#show port-security address
               Secure Mac Address Table
-----------------------------------------------------------------------------
Vlan    Mac Address       Type                          Ports   Remaining Age
                                                                    (mins)
----    -----------       ----                          -----   -------------
   1    000c.292f.9644    SecureSticky                  Et0/0        -
-----------------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 0
Max Addresses limit in System (excluding one mac per port) : 4096
```

شکل ۹-۱۱ نتیجه دستور show Port-Security address

حالا برای اینکه سرویس Port Security را تست کنیم، طبق شکل ۱۰-۱۱،در پروژه‌ی مورد نظر کابل PC2 را به پورتی متصل می‌کنیم که PC1 به آن متصل بوده است، با اولین پکتی که به سمت سوئیچ ارسال شود پورت مورد نظر خاموش خواهد شد.



شکل ۱۰-۱۱ سناریو PortSecurity

```
Switch(config-if)#
*Sep 16 08:08:48.132: %PM-4-ERR_DISABLE: psecure-violation error detected on Et0/0, putting Et0/0 in err-disab
le state
Switch(config-if)#
*Sep 16 08:08:48.132: %PORT_SECURITY-2-PSECURE_VIOLATION: Security violation occurred, caused by MAC address 0
00c.290e.ef99 on port Ethernet0/0.
*Sep 16 08:08:49.139: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/0, changed state to down
Switch(config-if)#
*Sep 16 08:08:50.134: %LINK-3-UPDOWN: Interface Ethernet0/0, changed state to down
```

شکل ۱۱-۱۱ نتیجه اعمال PortSecurity

www.takbook.com

همانطور که در شکل ۱۱-۱۱، مشاهده می‌کنید سرویس Port Security بر روی پورت E0/0 که آدرس Macآن تغییر کرده اجرا شده است و پورت مورد نظر خاموش شده است و سیستم Pc2 نمی‌تواند از منابع شبکه استفاده کند، البته خود سیستم PC1 هم اگر دوباره به پورت E0/0 متصل شود باز هم پورت مورد نظر خاموش خواهد بود و حتماً باید مدیر مربوطه دستوراتی را که در ادامه بررسی می‌کنیم را اجرا کند تا آن پورت روشن شود.

```
Switch#show port-security
Secure Port  MaxSecureAddr  CurrentAddr  SecurityViolation  Security Action
                (Count)       (Count)          (Count)
--------------------------------------------------------------------------
      Et0/0          1            1                 1          Shutdown
--------------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 0
Max Addresses limit in System (excluding one mac per port) : 4096
Switch#
```

شکل ۱۱-۱۱ نتیجه دستور show Port-security

بعد از اینکه پورت مورد نظر خاموش شد به مانند شکل ۱۱-۱۱، اگر دستور Show Port-Security را اجرا کنید در جلوی زیر ستون چهارم عدد یک قرار گرفته و نشان دهنده این است که تناقضی در MAC آدرس ایجاد شده است.

برای اینکه پورتی که خاموش شده را روشن کنیم دو راه وجود دارد:

۱- حذف کردن دستورات Port Security، که باید قبل از همه‌ی دستورات حرف No را قرار دهید و بعد از این کار پورت مورد نظر را روشن کنید.

۲- یا می‌توانید زمان Recovery را برای سوئیچ تغییر دهید، به این صورت که زمانی که پورت مورد نظر خاموش می‌شود با دستوری مشخص شود که بعد از چه زمانی دوباره به حالت اول برگردد.

Switch(config)#**errdisable recovery cause psecure-violation**

با این دستور تمام پورت‌هایی که بر روی آنها Port Security اجرا شده در حالت Errdisable قرار خواهند گرفت.

Switch(config)#**errdisable recovery interval 60**

در این دستور عدد ۶۰ یعنی ۶۰ ثانیه، بعد از این زمان حالت Errdisable اجرا خواهد شد و پورت مورد نظر روشن خواهد شد، اگر در این ۶۰ ثانیه سیستم Pc1 به سوئیچ متصل شده باشد پورت مورد نظر روشن باقی خواهد ماند و اگر نباشد دوباره آن پورت خاموش می‌شود.

بعد از اجرای دستور بالا در شکل ۱۲-۱۱، بعد از ۶۰ ثانیه قسمت سبز رنگ شکل ۱۲-۱۱، نمایش داده می‌شود و پورت مورد نظر روشن خواهد شد و بعد از این کار MAC آدرس دوباره بررسی خواهد

www.takbook.com

شد اگر با آدرسی که در Port Security ذخیره شده هماهنگ باشد پورت مورد نظر روشن خواهد ماند و اگر درست نباشد دوباره به مانند شکل در قسمت آبی رنگ پورت خاموش خواهد شد.

```
Switch#
*Sep 16 11:09:06.469: %PM-4-ERR_RECOVER: Attempting to recover from psecure-violation err-disable state on Et0/0
Switch#
*Sep 16 11:09:08.469: %LINK-3-UPDOWN: Interface Ethernet0/0, changed state to up
*Sep 16 11:09:09.474: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/0, changed state to up
Switch#
*Sep 16 11:09:54.375: %PM-4-ERR_DISABLE: psecure-violation error detected on Et0/0, putting Et0/0 in err-disable state
Switch#
*Sep 16 11:09:54.375: %PORT_SECURITY-2-PSECURE_VIOLATION: Security violation occurred, caused by MAC address 000c.290e.ef99
 on port Ethernet0/0.
*Sep 16 11:09:55.379: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/0, changed state to down
Switch#
*Sep 16 11:09:56.384: %LINK-3-UPDOWN: Interface Ethernet0/0, changed state to down
Switch#
```

شکل ۱۲-۱۱ نتیجه اعمال دستور errdisable recovery interval 60

۱-۴-۱۱ اضافه کردن MAC آدرس به صورت دستی

شاید بخواهید بر روی یک پورت سوئیچ چند آدرس MAC تعریف کنید، تا همزمان چند دستگاه شبکه بتوانند از آن پورت استفاده کنند، برای تعریف این کار باید به صورت زیر عمل کنید:

اول از همه باید مقدار ورودی MAC آدرس را تغییر دهید، در قسمت قبلی مقدار MAC آدرس را بر روی یک قرار دادیم، که اگر بخواهید مقدار بیشتری را در لیست قرار دهید باید آن مقدار را تغییر دهید:

Switch(config-if)#**switchport port-security maximum 5**

با این دستور می‌توانید به مقدار پنج آدرس MAC به لیست سوئیچ اضافه کنید، توجه داشته باشید برای پاک کردن دستورات می‌توانید از کلمه‌ی No در اول آنها استفاده کنید.

Switch(config-if)#**switchport-security mac-address** 54-04-A6-B1-6C-B0

در این دستور آدرس MAC مورد نظر به صورت دستی به لیست اضافه شده است.

در این قسمت با دستور Show Port-security Address لیست 5 آدرس MAC را مشاهده می‌کنید، اگر به ستون Type نگاهی بیندازید، دو گزینه وجود دارد که یکی Dynamic یعنی همان اتوماتیک و دیگری Configured که به صورت دستی مشخص می‌کند که MAC آدرس به لیست مورد نظر اضافه شده است.

```
Switch(config-if)#do sh port-security address
                Secure Mac Address Table
-----------------------------------------------------------------------------
Vlan    Mac Address       Type                          Ports   Remaining Age
                                                                    (mins)
----    -----------       ----                          -----   -------------
   1    000c.290e.ef99    SecureDynamic                 Et0/0        -
   1    000c.292f.9644    SecureDynamic                 Et0/0        -
   1    0026.5a71.601a    SecureConfigured              Et0/0        -
   1    5404.a6b1.6cb0    SecureConfigured              Et0/0        -
   1    5404.a6b1.fc20    SecureConfigured              Et0/0        -
-----------------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 4
Max Addresses limit in System (excluding one mac per port) : 4096
```

شکل ۱۳-۱۱ نتیجه دستور show port-security address

www.takbook.com

با دستور Show Port-Security interface E0/0 می‌توانید در شکل ۱۴-۱۱، مشاهده کنید که روی پورت Ethernet0/0 سرویس Port Security فعال است یا نه، که در تصویر زیر فعال بودن این سرویس با گزینه‌ی Enabled مشخص شده است.

```
Switch(config-if)#do sh port-security interface E0/0
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 5
Total MAC Addresses        : 5
Configured MAC Addresses   : 3
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 000c.290e.ef99:1
Security Violation Count   : 0
```

شکل ۱۴-۱۱ نتیجه دستور show port-security interface E0/0

۲-۴-۱۱ حذف آدرس MAC بعد از غیر فعال شدن کلاینت

در این قسمت می‌خواهیم روشی را با هم بررسی کنیم که اگر کلاینتی بعد از مثلاً ۱۰ دقیقه ارتباط خود را با سوئیچ قطع کرد، آدرس MAC آن از لیست سوئیچ مورد نظر حذف شود، برای این کار از دستورات زیر استفاده کنید:

Switch(config-if)#**switchport port-security aging time 10**

در دستور بالا مقدار زمان Agin برابر ۱۰ دقیقه قرار گرفته است که این زمان می‌تواند بین ۱ تا ۱۴۴۰ دقیقه متغیر باشد، اگر در این ۱۰ دقیقه ارتباط کلاینت‌ها با سوئیچ قطع شود، آدرس Mac آنها از لیست حذف خواهد شد.

Switch(config-if)#**switchport port-security aging type inactivity**

این دستور نوع Aging را بر روی inactivity قرار می‌دهد، یعنی اینکه از زمان پشتیبانی می‌کند و با دستور قبلی هماهنگ می‌شود.

در شکل ۱۵-۱۱، دو دستور مشخص شده اجرا شده است، بعد از این دستورات ارتباط کلاینت‌ها را با سوئیچ قطع کنید و بعد از ده دقیقه دستور Show Port-security address را اجرا کنید که مشاهده خواهید کرد که دو آدرس MAC که به صورت اتوماتیک به لیست اضافه شده بودند در این قسمت حذف شدند.

www.takbook.com


```
Switch(config-if)#switchport port-security aging time 10
Switch(config-if)#switchport port-security aging type inactivity
Switch(config-if)#do sh port-security address
               Secure Mac Address Table
-------------------------------------------------------------------------------
Vlan    Mac Address       Type                          Ports   Remaining Age
                                                                    (mins)
----    -----------       ----                          -----   -------------
   1    0026.5a71.601a    SecureConfigured              Et0/0        -
   1    5404.a6b1.6cb0    SecureConfigured              Et0/0        -
   1    5404.a6b1.fc20    SecureConfigured              Et0/0        -
-------------------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 2
Max Addresses limit in System (excluding one mac per port) : 4096
```

شکل ۱۵-۱۱ نتیجه دستور show port-security address

طبق شکل ۱۶-۱۱، با اجرای دستور Show Port-Security interface e0/0 در قسمت مشخص شده Aging Time و Aging Type مشخص شده است.

```
Switch(config-if)#do sh port-security interface e0/0
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Shutdown
Aging Time                 : 10 mins
Aging Type                 : Inactivity
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 5
Total MAC Addresses        : 3
Configured MAC Addresses   : 3
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 000c.290e.ef99:1
Security Violation Count   : 0
```

شکل ۱۶-۱۱ نتیجه دستور show port-security interface E0/0

۵-۱۱ ایجاد امنیت در سرویس DHCP

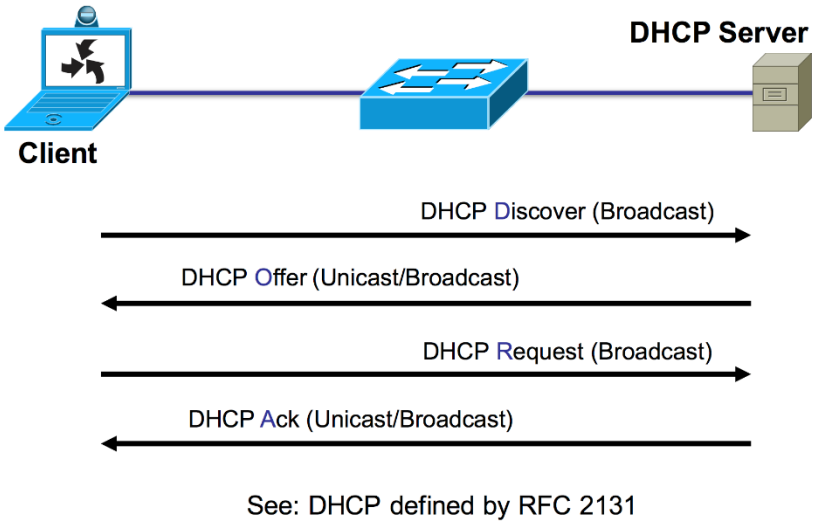
یکی از پرکاربردترین سرویس استفاده شده در شبکه‌های مختلف، سرویس DHCP می‌باشد. این سرویس به صورت پویا به همه کلاینت‌های موجود در شبکه آدرس IP می‌دهد؛ مثلاً اگر در مجموعه‌ی شبکه‌ی خود 200 کامپیوتر داشته باشید، دیگر لازم نیست که پشت تک تک کامپیوترها بنشینید و IP وارد کنید؛ فقط کافی است سرویس DHCP را روی سرور اصلی فعال کنید و کامپیوترها را در حالت دریافت IP به صورت اتوماتیک قرار دهید، تا به همه‌ی کامپیوترها IP در رنج مشخص‌شده تخصیص داده شود.

www.takbook.com

در این قسمت می‌خواهیم روش‌هایی را ارائه دهیم تا مهاجمان با استفاده از ابزارهای موجود نتوانند از طریق این سرویس به منابع شبکه دسترسی داشته باشد، برای ایجاد امنیت نیاز به دستگاه‌های سیسکو مانند سوئیچ دارید تا بتوانید این قابلیت امنیتی را در آن فعال کنید
عملکرد DHCP به چهار قسمت پایه تقسیم می‌گردد:

- اکتشاف(DHCP Discovery)
- پیشنهاد(DHCP Offer)
- درخواست(DHCP Request)
- تصدیق(DHCP Acknowledgement)

این چهار مرحله به صورت خلاصه با عنوان DORA شناخته می‌شوند.



شکل ۱۷-۱۱ بررسی DHCP

۱۱-۵-۱ DHCP Discovery

هر سرویس گیرنده (کاربر) برای شناسایی سرورهای DHCP موجود اقدام به فرستادن پیامی در زیر شبکه خود می‌کند. مدیرهای شبکه می‌توانند مسیریاب محلی را به گونه‌ای پیکربندی کنند که بتواند بسته داده‌ای DHCP را به یک سرور DHCP دیگر که در زیر شبکه متفاوتی وجود دارد، بفرستد. این مهم باعث ایجاد بسته داده با پروتکل UDP می‌شود که آدرس مقصد ارسالی آن ۲۵۵.۲۵۵.۲۵۵.۲۵۵ یا آدرس مشخص ارسال زیر شبکه می‌باشد. کاربر (سرویس گیرنده) DHCP همچنین می‌تواند آخرین IP آدرس شناخته شده

www.takbook.com

خود را درخواست بدهد. اگر سرویس گیرنده همچنان به شبکه متصل باشد در این صورت IP آدرس معتبر می‌باشد و سرور ممکن است که درخواست را بپذیرد. در غیر اینصورت، این امر بستگی به این دارد که سرور به عنوان یک مرجع معتبر باشد. یک سرور به عنوان یک مرجع معتبر درخواست فوق را نمی‌پذیرد و سرویس گیرنده را مجبور می‌کند تا برای درخواست IP جدید عمل کند .

۱۱-۵-۲ DHCP Offer

زمانی که یک سرور DHCP یک درخواست را از سرویس گیرنده دریافت می‌کند، یک IP آدرس را برای سرویس گیرنده رزرو می‌کند و آن را با نام DHCP Offer برای کاربر یا همان گیرنده می‌فرستد. این پیام شامل MAC کاربر؛ IP آدرسی پیشنهادی توسط سرور؛ Subnet Mask IP ،آدرس سروری که پیشنهاد را داده است و...

۱۱-۵-۳ DHCP Request

سرویس گیرنده با یک درخواست به مرحله پیشین پاسخ می‌گوید. یک کاربر می‌تواند پیشنهادهای مختلفی از سرورهای متفاوت دریافت کند. اما فقط می‌تواند یکی از پیشنهادها را بپذیرد. بر اساس تنظیمات شناسایی سرور در درخواست و فرستادن پیام‌ها(identification option) ، سرورها مطلع می‌شوند که پیشنهاد کدام یک پذیرفته شده‌است. هنگامی که سرورهای DHCP دیگر این پیام را دریافت می‌کنند، آن‌ها پیشنهادهای دیگر را، که ممکن است به کاربر فرستاده باشند، باز پس می‌گیرند و آن‌ها را در مجموعه IP های در دسترس قرار می‌دهند.

۱۱-۵-۴ DHCP Acknowledgement

هنگامی که سرور DHCP، پیام درخواست DHCP را دریافت می‌کند، مراحل پیکربندی به فاز پایانی می‌رسد. مرحله تصدیق شامل فرستادن یک بسته داده‌ای (DHCP Pack) به کاربر می‌باشد. این داده بسته‌ای شامل: زمان تخصیص IP یا هرگونه اطلاعات پیکربندی که ممکن بوده‌است که سرویس گیرنده درخواست کرده باشد، می‌باشد. در این مرحله فرایند پیکربندی IP کامل شده‌است.

پیغام‌های DHCP در دیتا گرام‌های UDP حمل می‌شوند و در سمت سرویس دهنده از شماره پورت ۶۷ و در سمت سرویس گیرنده از پورت ۶۸ استفاده می‌کند. پروتکل‌هایی که در ارتباط با DHCP کار می‌کنند شامل IP, BOOTP , UDP, TCP, RARP می‌باشند.

۱۱-۵-۴ پیکربندی سرویس DHCP

سرویس Dynamic Host Configuration Protocol یا DHCP به شما اجازه می‌دهد تا به صورت خودکار به کلاینت‌های خود ip دهید. سرویس بسیار پرکاربرد که با نحوه‌ی راه‌اندازی آن آشنا خواهیم شد.

یک سرور که نقش DHCP را بازی می‌کند از اجزای زیر تشکیل شده است:

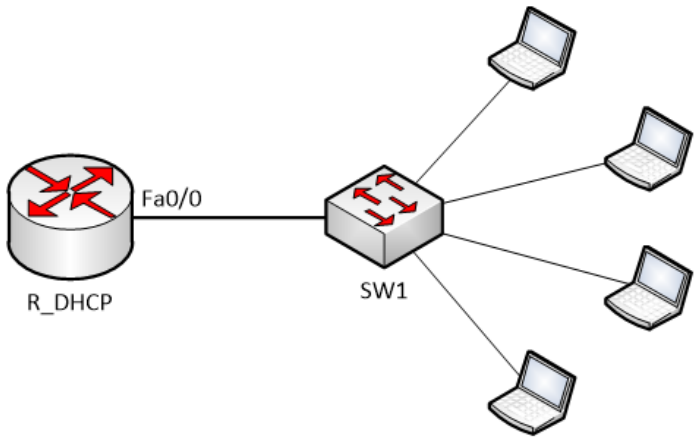
- IP address

www.takbook.com

- Subnet mask
- Domain name
- Default gateway (routers)
- DNS
- WINS information

همه‌ی آن‌ها را می‌توانید بر روی یک DHCP Server فعال کنید تا به کلاینت‌ها داده شود.

مثال۷:



شکل ۱۸-۱۱ سناریو DHCP

طبق شکل ۱۸-۱۱، می‌خواهیم روی روتر R_DHCP، سرویس DHCP را راه‌اندازی کنیم، بعد از راه‌اندازی این سرویس، کلاینت‌ها اگر درخواست آدرس دهند، IPها و اطلاعات را از سرور دریافت می‌کنند.

وارد پورت Fa0/0 شوید و آدرس زیر را در آن وارد کنید:

R_DHCP(config-if)#**ip address 192.168.1.1 255.255.255.0**

بعد، سرویس DHCP را راه‌اندازی می‌کنیم.

R_DHCP(config)#**ip dhcp pool r_dhcp**

با این دستور، DHCP Pool با نام r_dhcp ساخته می‌شود و وارد آن می‌شویم.

R_DHCP (dhcp-config)#**network 192.168.1.0 255.255.255.0**

تعریف رنج ip برای اختصاص دادن به کلاینت‌ها.

R_DHCP(dhcp-config)#**default-router 192.168.1.1**

به کلاینت‌ها می‌گوییم که Default gateway مورد نظر، این روتر است.

www.takbook.com

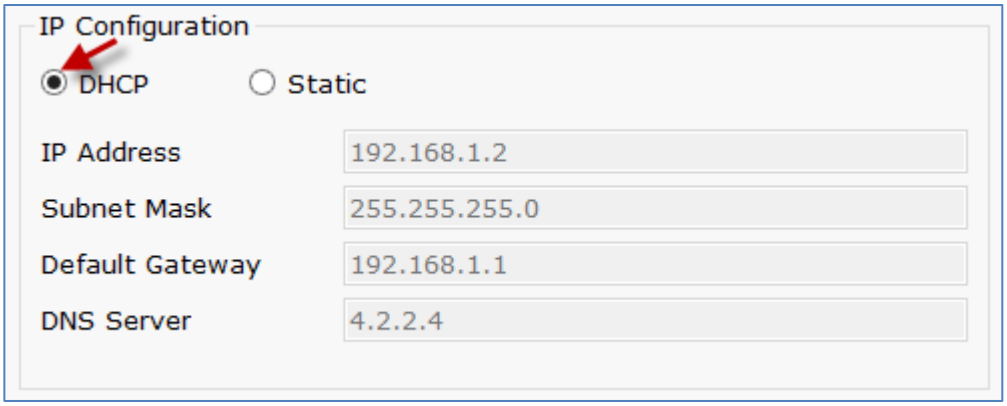
R_DHCP(dhcp-config)#**dns-server 4.2.2.4**

با این دستور، DNS Server را برای کلاینت‌ها تعریف می‌کنیم.

R_DHCP(dhcp-config)#**lease 0 1 05**

این دستور، مقدار زمانی است که به یک کلاینت داده می‌شود و این کلاینت باید در این زمان مشخص با ارسال پکت‌هایی حضور خود را اعلام کند. اگر بعد از پایان این زمان، موجودیت خود را اعلام نکرد، IP اختصاص داده به این کلاینت پس گرفته خواهد شد.

بعد از راه‌اندازی سرویس DHCP باید به کلاینت‌ها بگوییم که ip address را از طریق DHCP به دست بیاورند. به مانند شکل ۱۹-۱۱، در برنامه‌ی packet tracer، وارد pc مورد نظر می‌شویم و از تب Desktop، گزینه‌ی ip Configuration را انتخاب می‌کنیم.

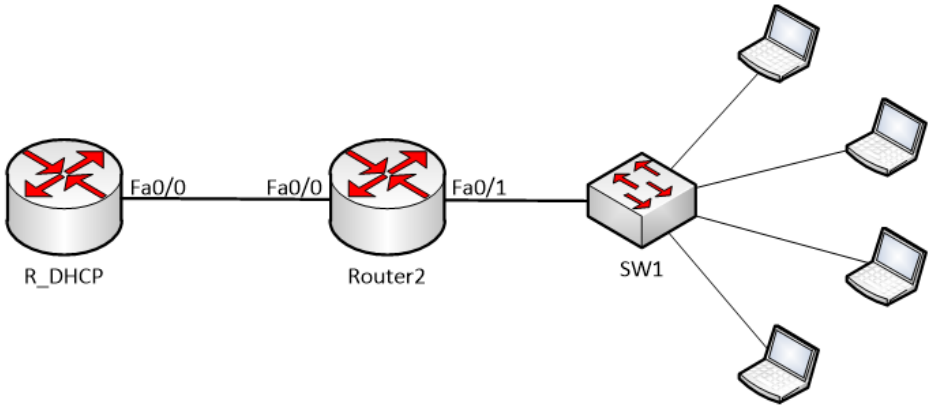


شکل ۱۹-۱۱ تنظیم IP کلاینت

همان‌طور که در شکل ۱۹-۱۱، مشاهده می‌کنید، بعد از انتخاب گزینه‌ی DHCP، به صورت خودکار اطلاعات را از DHCP سرور دریافت کرد.

شاید شما شبکه‌ای داشته باشید که از دو روتر تشکیل شده است و می‌خواهید روی یکی از آن‌ها سرویس DHCP را راه‌اندازی کنید، مانند شکل ۲۰-۱۱، اگر روی روتر R_DHCP، این سرویس را راه‌اندازی کنید کلاینت‌ها نمی‌توانند اطلاعات را از این سرور بگیرند، به خاطر این‌که Router 2 در سر راه قرار دارد و سرویس DHCP برای انجام کار خود از طریق Broadcast، اطلاعات خود را ارسال می‌کند. Router2 جلوی Broadcast را خواهد گرفت و این سرویس کارایی خود را از دست می‌دهد، برای حل این مشکل باید دستوری را در Router 2 اجرا کنید:

www.takbook.com



شکل ۲۰-۱۱ سناریو DHCP

وارد روتر Router2 شوید و در مد Global دستور زیر را وارد کنید:

R_DHCP(config-if)#**ip helper-address 192.168.1.1**

با این دستور، سرویس dhcp به کار خود ادامه می‌دهد و کلاینت‌ها می‌توانند از این سرور اطلاعات را دریافت کنند.

مشکلات امنیتی پروتکل DHCP

همانطور که گفته شد پیغام DHCP Discovery یک پیغام Broadcast است، از این رو در صورتی که بیش از یک سرور DHCP در شبکه موجود باشند، هرکدام از آن سرورها به صورت مجزا به سیستم درخواست کننده پاسخ می‌دهند، در این حالت، سیستمی که پیغام DHCP Discovery را فرستاده است با سروری عملیات را ادامه می‌دهد که پیغام DHCP Offer آن زودتر به دستش رسیده باشد. از این رو در صورتی که یک سرور DHCP تقلبی یا به اصطلاح Rogue DHCP در شبکه وجود داشته باشد درخواست DHCP Discoveryبه آن می‌رسد و شروع به ادامه دادن مراحل سرویس DHCP می‌کند.

در صورتی که DHCP Offer پیشنهاد شده از سمت سرور تقلبی، زودتر از پیغام DHCP Offer پیشنهاد شده از سمت سرور اصلی DHCP برسد، سیستمی که در ابتدا درخواست IP کرده بوده است از یک سرور DHCPمخرب IP را دریافت می‌کند.

دریافت IP از سمت سرور تقلبی به خودی خود مشکلی را ایجاد نمی‌کند، اما حالتی را در نظر بگیریم که حمله کننده تغییراتی را در رنج IP که می‌خواهد به کاربران پیشنهاد بدهد ایجاد کند. تغییرات می تواند به یکی از حالت های زیر به وجود آید:

پیشنهاد کردن رنج شبکه اشتباه

در این نوع حمله، رنج شبکه تغییر کرده و کاربر یک رنج اشتباه را دریافت خواهد کرد. به طور مثال در صورتی که رنج شبکه ما 10.10.10.0 با زیر شبکه‌ی 24 است، حمله کننده یک IP از رنج 192.168.1.0 با زیر

www.takbook.com

شبکه‌ی 26 به آن می‌دهد، با به وجود آوردن این تغییر این سیستم خاص امکان برقراری ارتباط با شبکه داخلی خود را ندارد و کار کردن با آن مختل می‌شود.

تغییر در تنظیمات default gateway

این حمله یکی از انواع حمله‌های ترکیبی به حساب می‌آید. نحوه کار شخص حمله کننده در این روش به این گونه است که در IP پیشنهاد شده به کاربر، IP خودش را به عنوان Default Gateway قرار می‌دهد. در مرحله بعدی حمله کننده با نصب کردن نرم‌افزارهای جاسوسی شبکه مانند Wireshark می‌تواند تمامی ارتباطات آن سیستم را مانیتور کند و از اطلاعات مورد نظر در راستای اهداف غیر قانونی خود استفاده کند.

تغییر در DNS سرور

این روش حمله کردن را می‌توان خطرناک‌ترین نوع حمله در بین این دسته از حملات به شمار آورد. ماهیت حمله به این صورت است که حمله کننده در مرحله اول حمله، یک Website تقلبی مالی، اجتماعی، ایمیل و ... همانند وب سایت‌های شرکت یا فرد مورد نظر را طراحی کرده است. مرحله بعد راه‌اندازی یک DNSسرور تقلبی است بدین صورت که به جای برگرداندن IP واقعی سایت مورد نظر کاربر(مثل Gmail.com، bank.com، IP ...) وبسایت خود را به کاربر انتقال می‌دهد. در این صورت تمامی اطلاعات اکانت کاربر به دست حمله کننده می‌رسد.

روش دیگر مورد استفاده حمله کننده برای تخریب سرویسDHCP

در روش‌های حمله‌ای که در مرحله قبل صحبت شد، فرض بر وجود داشتن همزمان هر دو سرور مخرب و اصلی در شبکه داخلی بود. در این حالت با توجه به زودتر رسیدن یا نرسیدن پیغام DHCP Offer سرور مخرب به کاربران، اطلاعات آن کاربران خاص توسط حمله کننده جاسوسی (Sniff) می‌شود، آیا از دید حمله کننده این روش یک روش بهینه است؟ آیا راه حلی برای sniff تمامی سیستم‌ها وجود دارد؟ پاسخ این‌جاست که در صورتی که سرور اصلی DHCP به گونه‌ای مورد حمله قرار گیرد که قادر به سرویس‌دهی نباشد، تمامی سیستم های درون شبکه را می‌توان تحت کنترل خود داشت.

از این رو از روشی به نام Flooding برای از کار انداختن سرویس DHCP استفاده می‌شود. روش کار به این گونه است که حمله کننده با فرستادن درخواست‌های DHCP Discovery متوالی با MAC Address های تولید شده به صورت تصادفی پایگاه داده‌IPهای سرور DHCP را خالی می‌کند. حالا هنگامی که یک کاربر عادی DHCP Discovery را Broadcast می‌کند، دیگر سرور DHCP اصلی به دلیل موجود نداشتن IP پیغام DHCP Offer را نمی‌فرستد و تنها جواب از سمت سرویس DHCP راه‌اندازی شده توسط حمله کننده به دست کاربر می‌رسد.

نحوه دفاع در برابر حملات به سرورDHCP

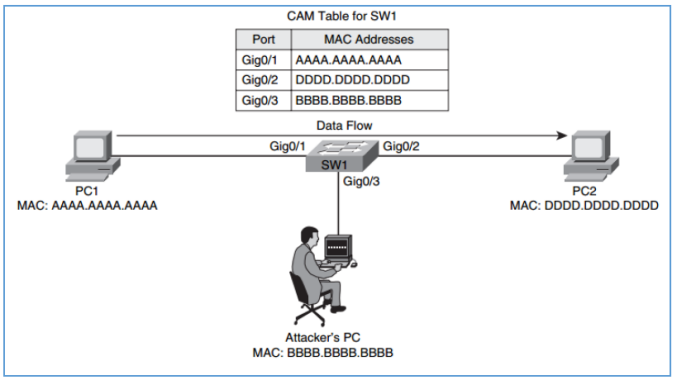
حال که از دید حمله کننده با نحوه‌ی حمله به سرور DHCP آشنا شدیم، نوبت به بررسی راه‌حل‌های دفع حمله است. بدین منظور از دو روش Port-security وDHCP Snooping استفاده می‌شود.

www.takbook.com

تحلیل و بررسی Spoofing MAC Addresses

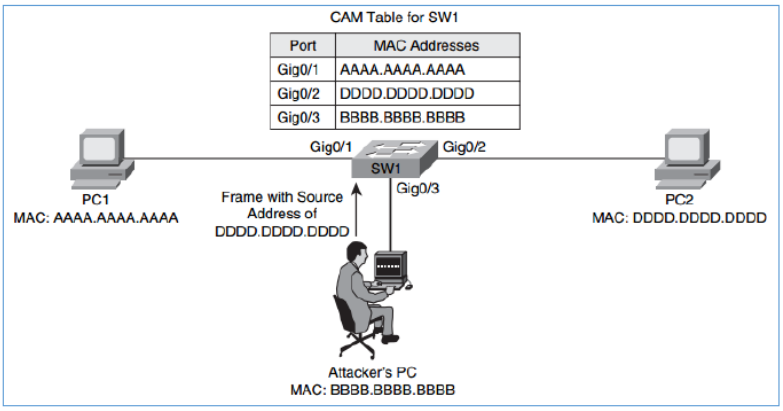
همانطور که می‌دانید آدرس MAC یک آدرس منحصر به فرد می‌باشد و برای هر دستگاه یک آدرس در نظر گرفته خواهد شد، نوع دیگری از حمله جعل کردن آدرس Mac است که در زیر این روش را بررسی خواهیم کرد.

در شکل ۲۱-۱۱، سه سیستم را مشاهده می‌کنید که به سوئیچ متصل شده‌اند و آدرس MAC آنها در جدول سوئیچ ثبت شده است.



شکل ۲۱-۱۱ سناریو Spoofing MAC Addresses

در شکل ۲۲-۱۱، سیستم "Attacker's Pc " با ارسال یک Frame در شبکه آدرس مک جعلی خود یعنی DDDD.DDDD.DDDD که مربوط به PC2 است را به سوئیچ اعلام می‌کند، سوئیچ هم در زمان مشخص شده جدول خود را آپدیت می‌کند و با این کار ترافیکی که قبل از آن به سیستم PC2 ارسال می‌شد به سمت سیستم Attacker's ارسال می‌شود و با این روش اطلاعات به خطر خواهد افتاد.

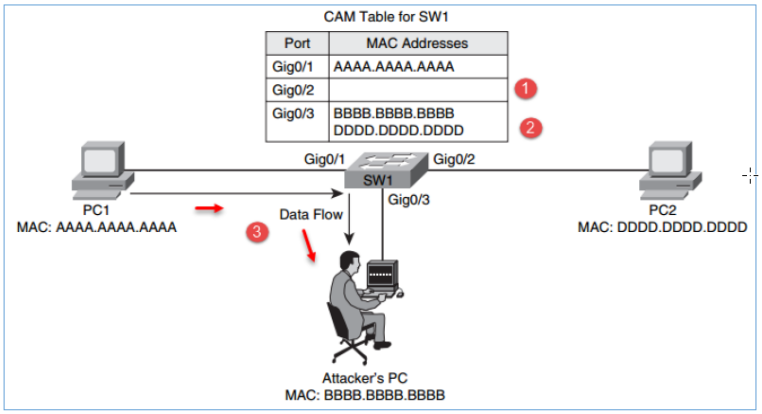


شکل ۲۲-۱۱ سناریو Spoofing MAC Addresses

همانطور که در شکل ۲۳-۱۱، مشاهده می‌کنید، در قسمت اول در جدول سوئیچ آدرس MAC در پورت Gig0/2 که قبلاً به PC2 متصل شده بود خالی شده است و به جای آن در قسمت دوم پورت Gig0/3

www.takbook.com

دارای دو آدرس MAC است که یکی از آنها آدرس MAC جعلی مربوط به PC2 است و در قسمت شماره‌ی سه تمام ترافیک به روتر مهاجم ارسال خواهد شد، در قسمت بعد با استفاده از PortSecurity در سوئیچ امنیت ایجاد خواهیم کرد.

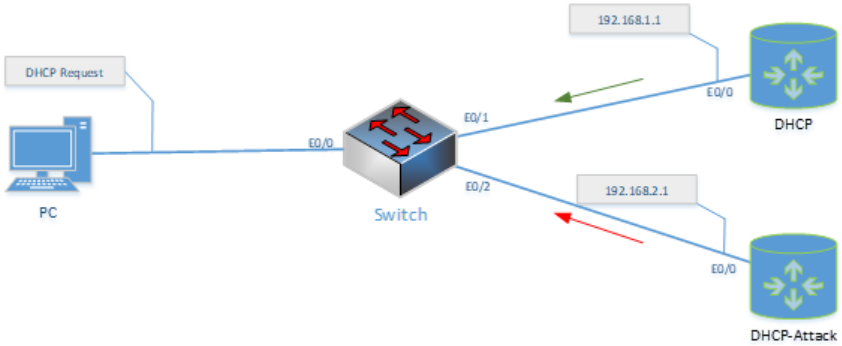


شکل ۲۳-۱۱ سناریو Spoofing MAC Addresses

تحلیل و بررسی DHCP Snooping

حتماً در شبکه‌ی خود از سرویس پرکاربرد DHCP استفاده می‌کنید، یکی از بزرگترین مشکلاتی که این سرویس میتواند ایجاد کند، این است که یک سرویس دهنده‌ی DHCP دیگری به اشتباه یا به صورت عمدی وارد شبکه شود و کلاینت‌های شبکه به اشتباه با سرویس دهنده‌ی جدید ارتباط برقرار می‌کنند و آدرس IP و اطلاعات در این زمینه را از سرور غیرواقعی دریافت می‌کنند، این مورد می‌تواند یکی از انواع حملات به شبکه باشد که برای حل آن باید از ویژگی DHCP Snooping استفاده کرد که در ادامه آن را بررسی خواهیم کرد.

برای شروع شکل ۲۴-۱۱، را پیاده سازی کنید:



شکل ۲۴-۱۱ سناریو DHCP Snooping

www.takbook.com

در شکل ۲۴-۱۱، دو روتر به عنوان سرویس دهنده‌ی DHCP ایفای نقش می‌کنند و PC برای دریافت اطلاعات از DHCP درخواست IP می‌کند، روتری که با نام DHCP در شکل قرار دارد همان DHCP اصلی است که کلاینت PC باید اطلاعات IP را از آن دریافت کند، ولی اگر یک مهاجم یک سرویس DHCP دیگر که در شکل با نام DHCP Attack معرفی شده را در شبکه فعال کند می‌تواند PC را وادار کند تا از اطلاعات آن استفاده کند، برای حل این مشکل باید سرویس DHCP Snooping را فعال کنیم.

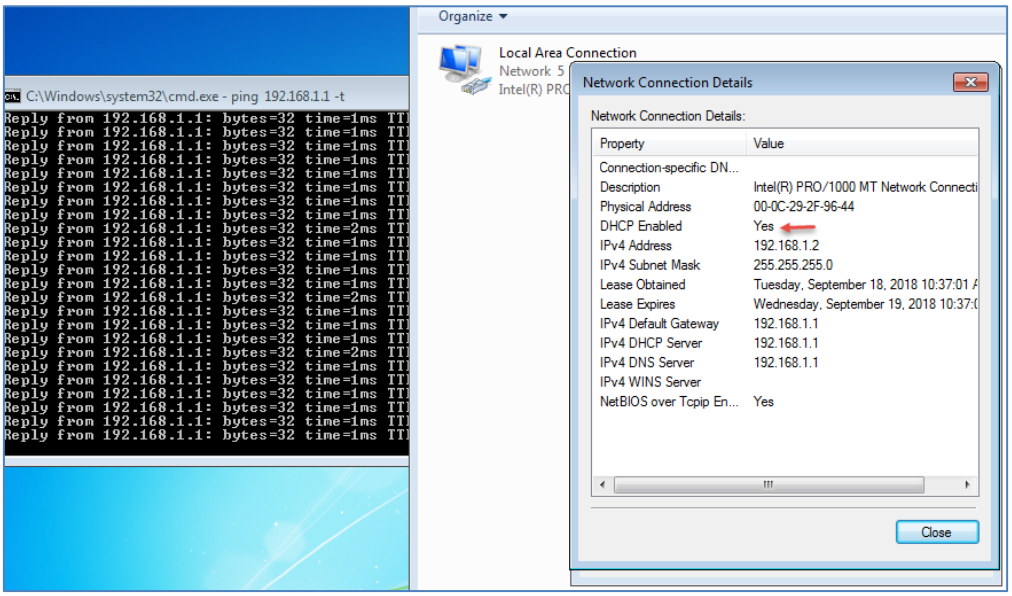
برای شروع، روی هر دو روتر سرویس DHCP را با دستورات زیر فعال می‌کنیم:

تنظیمات روتر DHCP

جدول ۸-۱۱ دستورات DHCP

در این دستور یک Pool با نام P1 ایجاد می‌کنیم.	Switch(config-if)#ip dhcp pool p1
آدرس زیر شبکه مربوط به شبکه DHCP را وارد می‌کنیم.	Switch(config-if)#network 192.168.1.0 255.255.255.0
این قسمت مربوط به تعریف Gateway است.	Switch(config-if)#default-router 192.168.1.1
تعریف سرور DNS که خود سرور DHCP است.	Switch(config-if)#dns-server 192.168.1.1

بعد از اینکه سرویس DHCP فعال شد اگر وارد کلاینت شوید و کارت شبکه را بر روی حالت اتوماتیک قرار دهید به مانند شکل ۲۵-۱۱، IP را از روتر DHCP دریافت خواهد کرد و روتر DHCP را می‌توان Ping کرد.



شکل ۲۵-۱۱ تنظیمات PC

www.takbook.com

تنظیمات روتر DHCP - Attack

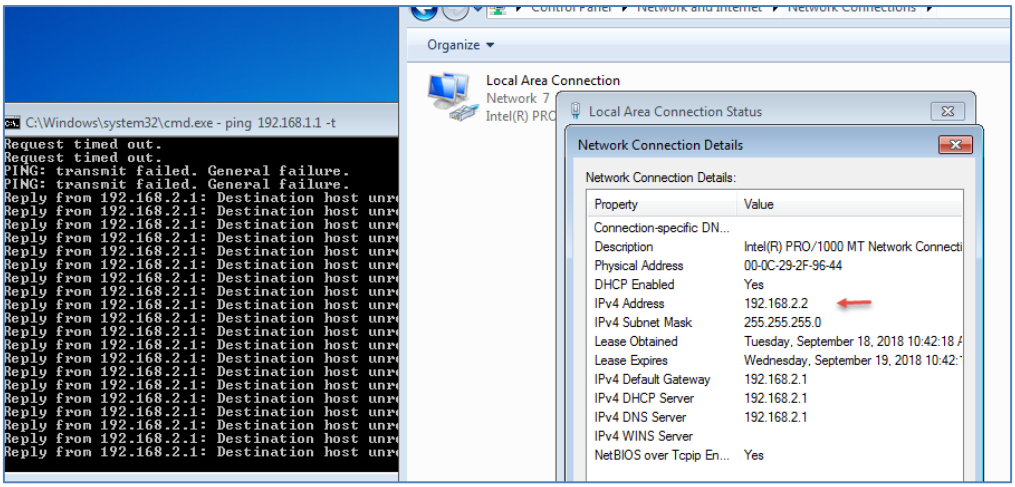
بعد از اینکه روتر DHCP را فعال کردید و کلاینت PC هم از آن IP دریافت کرد، حالا می‌خواهیم روتر دوم را برای DHCP فعال کنیم، برای این کار از دستورات جدول ۹-۱۱، استفاده کنید.

جدول ۹-۱۱ دستورات DHCP

در این دستور یک Pool با نام P2 ایجاد می‌کنیم.	Switch(config-if)#ip dhcp pool p2
آدرس زیر شبکه مربوط به شبکه DHCP را وارد می‌کنیم.	Switch(config-if)#network 192.168.2.0 255.255.255.0
این قسمت مربوط به تعریف Gateway است.	Switch(config-if)#default-router 192.168.2.1
تعریف سرور DNS که خود سرور DHCP است.	Switch(config-if)#dns-server 192.168.2.1

بعد از فعال کردن روتر دوم اگر کارت شبکه مربوط به Pc را غیرفعال و دوباره فعال کنید، طبق شکل ۱۱-۲۶، آدرسی که از شبکه خواهد گرفت یک آدرس جدید در رنج روتر DHCP-Attack است که این همان مشکی است که در قسمت‌های قبلی بیان کردیم.

برای حل چنین مشکلی باید یک سری دستورات را در سوئیچ وارد کنیم تا مشخص کنیم که سرور اصلی DHCP کدام است.

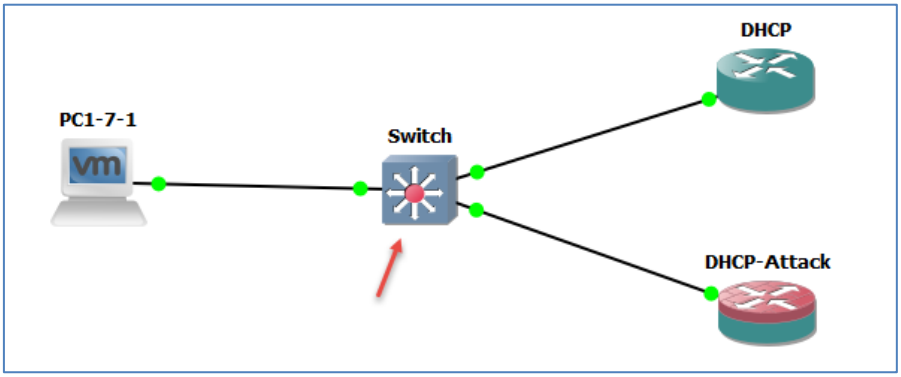


شکل ۱۱-۲۶ تنظیمات PC

همان‌طور که همه‌ی شما در جریان هستید تمام پورت‌های سوئیچ‌ها به صورت پیش‌فرض در Vlan 1 قرار دارند و البته می‌توانید Vlanهای مختلفی تعریف و پورت‌ها را به آن اضافه کنید، برای اینکه سرویس DHCP Snooping را فعال کنیم باید اول این سرویس را روی Vlan اجرا کنیم.

برای شروع کار در شکل ۱۱-۲۷، روی Switch دو بار کلیک کنید تا وارد صفحه Command آن شوید.

www.takbook.com



شکل ۲۷-۱۱ سناریو DHCP Snooping

با دستور Show Vlan brief می‌توانید شماره Vlan را مشاهده کنید که در این قسمت شماره یک است و همه پورت‌ها در آن قرار دارند.

```
Switch(config)#do sh vlan b

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Et0/0, Et0/1, Et0/2, Et0/3
                                                Et1/0, Et1/1, Et1/2, Et1/3
                                                Et2/0, Et2/1, Et2/2, Et2/3
                                                Et3/0, Et3/1, Et3/2, Et3/3
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
Switch(config)#
```

شکل ۲۸-۱۱ نتیجه دستور Show vlan b

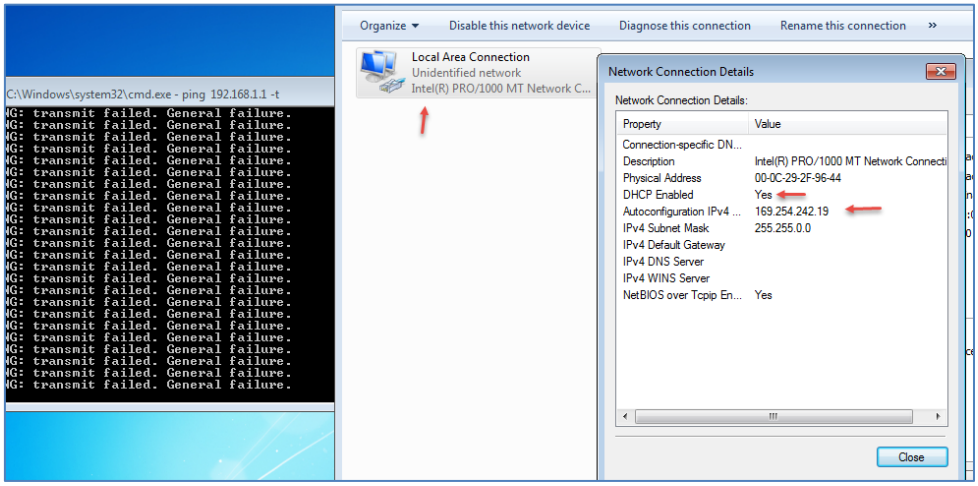
جدول ۱۰-۱۱ دستورات dhcp snooping

با این دستور سرویس DHCP Snooping فعال خواهد شد.	Switch(config)#ip dhcp snooping
با این دستور سرویس Snooping بر روی Vlan1 فعال خواهد شد.	Switch(config)#ip dhcp snooping vlan 1

بعد از فعال کردن دو دستور بالا دیگر هیچ سرویس دهنده‌ی DHCP نمی‌تواند به کلاینت‌ها IP ارائه دهد.

بعد از اینکه دو دستور را در سوئیچ اجرا کردید اگر Pc درخواست IP دهد دیگر سوئیچ به هیچ سرویس دهنده‌ی DHCP این اجازه را نخواهد داد و کلاینت IP اشتباه خواهد گرفت، که این موضوع را در شکل ۲۹-۱۱، مشاهده می‌کنید.

www.takbook.com



شکل ۲۹-۱۱ تنظیمات PC

برای اینکه روتر DHCP اصلی را به سوئیچ معرفی کنیم و بگوییم که این روتر همان روتر DHCP اصلی ما است باید از دستور زیر در پورتی که به روتر DHCP متصل است استفاده کنیم:

Switch(config)#**interface Ethernet 0/2**

با این دستور وارد Interface Ethernet 0/2 که به روتر DHCP متصل شده‌ایم.

Switch(config-if)#**ip dhcp snooping trust**

با این دستور به سوئیچ اعلام می‌کنیم که این پورت که به روتر DHCP متصل است جزو پورت‌هایی باشد که اجازه دارد سرویس DHCP روی آن فعال باشد.

بعد از اینکه پورت مورد نظر را Trust کردید، باید بقیه پورت‌های سوئیچ را Untrust یا غیر قابل اعتماد کنید، برای این کار کافی است وارد پورت مورد نظر شوید و دستو زیر را اجرا کنید:

Switch(config)#**int range e0/3-24**

با این دستور وارد رنجی از پورت که از شماره‌ی ۳ تا ۲۴ است شدیم، البته می‌توانید فقط وارد یک پورت شوید.

Switch(config-if-range)#**no ip dhcp snooping trust**

با این دستور همه پورت‌ها Untrust می‌شوند.

www.takbook.com

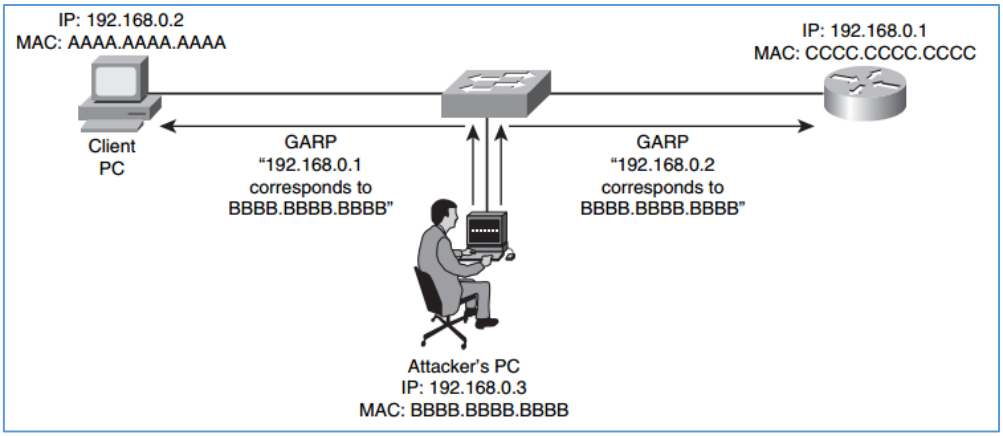
با دستور **show ip dhcp snooping** می‌توانید مشاهده کنید که چه پورت‌هایی فعال و چه پورت‌هایی غیرفعال هستند، اگر به دستور زیر توجه کنید در ستون Trusted گزینه‌ی Yes و No قرار داده شده است.

```
Switch#show ip dhcp snooping
Interface          Trusted   Rate limit (pps)
----------------   -------   ------------------------

Ethernet0/2        yes       unlimited
Ethernet0/1        no        unlimited
```

تحلیل و بررسی Dynamic Arp Inspection

پروتکل ARP که مخفف کلمه‌ی Address Resolution Protocol است، برای تبدیل آدرس IP (لایه‌ی شبکه) به آدرس MAC (لایه‌ی پیوند داده) کاربرد دارد، که این پروتکل یک پروتکل ضروری برای لایه‌ی اینترنت است.

به علت اینکه پروتکل ARP بیشترین کاربرد را دارد، مهاجم‌ها با روش‌های غیرقانونی سعی در دور زدن آن دارند. در شکل ۳۰-۱۱، سیستم "Client PC " را مشاهده می‌کنید که با روتر پیش‌فرض آن 192.168.0.1 در ارتباط است و اطلاعات را با این روتر رد و بدل می‌کند، اگر در این بین یک سیستم مهاجم با نام "Attacker's PC " وجود داشته باشد، برای اینکه خود را به جای سیستم " Client PC " به روتر معرفی کند، با ارسال پیام‌های (GRAP) ARP هم به کلاینت و هم به روتر خود را در وسط کار قرار می‌دهد، مثلاً در این شکل "Attacker's PC " آدرس مک خود را به جای آدرس مک روتر "BBBB.BBBB.BBBB" جا می‌زند و این کار باعث می‌شود که سیستم مورد نظر اطلاعات خود را به مهاجم ارسال کند و به همین ترتیب مهاجم با دستکاری در آن، اطلاعات را به سمت روتر مورد نظر خود ارسال می‌کند؛ این نوع حملات با نام ARP spoofing شناخته می‌شوند و از نوع man-in-the-middle است.



شکل ۳۰-۱۱ سناریو *Dynamic Arp Inspection*

www.takbook.com

توجه داشته باشید که GRAP که به اختصار به نام Gratuitous Address Resolution Protocol شناخته می‌شود کمکی برای شناسایی آدرس IP تکراری در شبکه است که این کار را با ارسال Broadcast در شبکه انجام می‌دهد، باارسال broadcast سیستم‌هایی که در شبکه قرار دارند اگر به این پیغام پاسخ دهند یعنی اینکه آدرس مورد نظر متعلق به آنها است و نمی‌توان از آن استفاده کرد.

در قسمت‌های قبلی از سرویس DHCP snooping استفاده کردیم، زمانی که این سرویس فعال می‌شود یک جدول که شامل آدرس MAC و آدرس IP است ایجاد می‌شود و می‌توانید با کمک این جدول از حملات ARP جلوگیری کنید.

یکی از ویژگی‌های امنیتی در پروتکل ARP استفاده از DAI یا همان Dynamic Arp Inspection است که با استفاده از جدول DHCP snooping بررسی می‌شود که اگر بسته‌ی ARP از پورتی که Trust است دریافت شود، اجازه عبور به آن را می‌دهد و اگر از پورتی دیگر دریافت شود فقط در صورتی که آدرس مک با آدرس IP یکی باشد اجازه عبور را می‌دهد.

برای فعال‌سازی ویژگی Dynamic Arp Inspection به صورت زیر عمل کنید:

برای شروع اول باید DAI را بر روی Vlan مورد نظر خود در سوئیچ اجرا کنید، که دستور آن به صورت زیر می‌باشد.

Switch(config)# **ip arp inspection vlan 1**

بعد از آن باید در Interface که به سوئیچ متصل است دستور زیر را وارد کنید:

Switch(config)#**interface Ethernet 0/2**

Switch(config-if)# **ip arp inspection trust**

توجه داشته باشید به صورت پیش‌فرض ویژگی DAI در همه‌ی پورت‌های سوئیچ در حالت Untrust است و فقط باید در پورت قابل اعتماد که در سوئیچ قرار دارد بر روی Trust قرار بگیرد.

پس در این موضوع یاد گرفتیم که چگونه جلوی مهاجم، که خود را به عنوان یک سیستم میانی جا می‌زند بگیریم، که این کار را با تعریف دستورات مورد نظر در پورت مشخص شده انجام می‌دهیم.

تحلیل و بررسی Private VLAN

در این بخش می‌خواهیم به دنیای VLAN سری بزنیم، همانطور که می‌دانید همه کلاینت‌ها و سرورها برای دسترسی به شبکه به سوییچ متصل می‌شوند و همه پورت‌های سوییچ هم در یک VLAN قرار دارد، ولی بین آنها هیچ امنیتی وجود دارد و همه کلاینت‌ها می‌توانند همدیگر را ببینند، ولی در کل نیازی نیست که کلاینت‌ها بتوانند به یک سری از سرورها دسترسی داشته باشند و باید دسترسی آنها را با استفاده از Private VLAN قطع کرد که این کار را در این قسمت با هم انجام می‌دهیم.

Private VLAN به دو نوع مختلف تقسیم می‌شود که در زیر مشاهده می‌کنید.

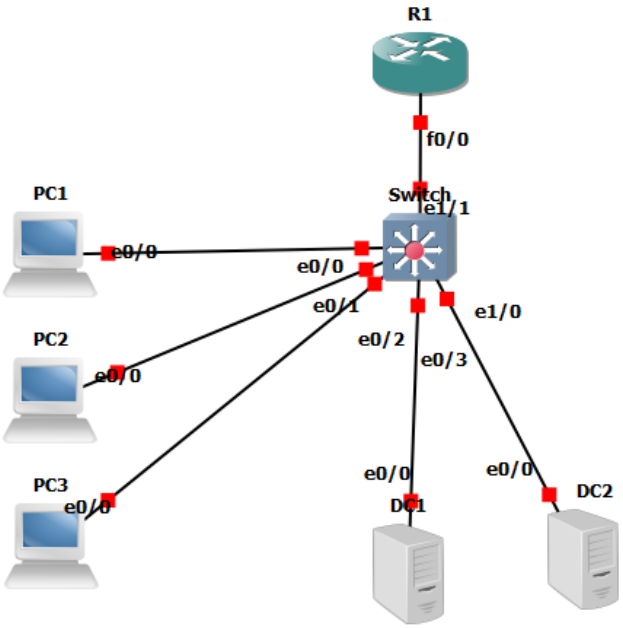
www.takbook.com

Primary VLAN یا همان VLAN اصلی که می‌تواند به همه سرورها و کلاینت‌ها متصل باشد.

Secondary VLAN یا همان VLAN ثانویه خود به دو بخش Isolated و Community تقسیم می‌شود که سیستم‌هایی که در VLAN از نوع Isolated قرار می‌گیرند با هیچ کلاینت یا سروری در ارتباط نخواهند بود و فقط با VLAN از نوع Primary در ارتباط خواهند بود.

کلاینت‌هایی که در VLAN از نوع Community قرار می‌گیرند، فقط می‌توانند با کلاینت‌هایی که در همان VLAN Community قرار دارند ارتباط برقرار کنند، مثلاً ارتباط یک اتاق خاص با هم، البته این نوع VLAN می‌تواند با VLAN از نوع Primary ارتباط داشته باشد.

در این قسمت یک مثال در مورد Private Vlan را با هم بررسی می‌کنیم تا به صورت عملی عملکرد این VLAN را مورد تست قرار دهیم، طبق شکل ۳۱-۱۱، یک روتر، یک سوییچ، دو سرور و سه کلاینت را به لیست GNS3 اضافه کنید.



شکل ۳۱-۱۱ سناریو Private VLAN

در زیر لیست آدرس IP برای هر کدام از سیستم‌ها را مشاهده می‌کنید، طبق جدول به هر یک از سیستم‌ها IP مورد نظر آنها را تخصیص دهید و بعد از این کار دستور Ping را اجرا کنید تا از ارتباط بین آنها مطمئن شوید.

جدول ۱۱-۱۱ تنظیمات IP

System Name	IP Address
R1	192.168.1.1
PC1	192.168.1.2
PC2	192.168.1.3
PC3	192.168.1.4

www.takbook.com

DC1	192.168.1.5
DC2	192.168.1.6

برای اینکه بتوانیم از دستورات Privat Vlan در سوییچ استفاده کنید باید پروتکل VTP را در حالت Transparent قرار دهید تا این دستورات در سوییچ قابل قبول باشد.

```
Switch#conf t
Switch(config)#vtp mode transparen
```

با دستور بالا VTP در حالت Transparent قرار خواهد گرفت.

در ادامه کار سه کلاینت PC1 , PC2 , PC3 را در یک VLAN شماره‌ی ۱۰۰ قرار می‌دهیم و نوع VLAN آن را community در نظر می‌گیریم.

```
Switch(config)#vlan 100
Switch(config-vlan)#private-vlan community
```

در دستور بالا Vlan با شماره ۱۰۰ تعریف شده و نوع آن را community در نظر گرفتیم که در ادامه کار این Vlan را به پورت‌های کلاینت ها تخصیص می‌دهیم.

```
Switch(config)#vlan 200
Switch(config-vlan)#private-vlan isolated
```

در دستور بالا VLAN با شماره‌ی ۲۰۰ ایجاد کردیم که نوع آن را isolated در نظر گرفیم که باید به سرورهای DC1 و DC2 بدهیم.

```
Switch(config)#vlan 300
Switch(config-vlan)#private-vlan primary
Switch(config-vlan)#private-vlan association 100,200
```

با دستور بالا VLAN به شماره‌ی ۳۰۰ از نوع Primary در نظر گرفته شده که باید به پورتی تخصیص دهیم که به سمت روتر ارسال می‌شود، در دستور آخر هم باید مشخص کنیم چه VLanهایی با VLAN Primary در ارتباط هستند.

تا به اینجا سه تا VLAN تعریف کردیم که نوع آنها را مشخص کردیم، حال در ادامه می‌خواهیم پورت‌های هر سیستم را به این VLANها تخصیص دهیم.

```
Switch(config)#interface ethernet 1/1
Switch(config-if)#switchport mode private-vlan promiscuous
Switch(config-if)#switchport private-vlan mapping 300 100,200
```

در دستور بالا وارد پورت ethernet 1/1 که به روتر R1 متصل است، بعد از آن از دستور promiscuous برای معرفی این پورت به عنوان پورت اصلی استفاده می‌کنیم ، در ادامه برای اینکه شماره‌ی VLAN اصلی

www.takbook.com

و فرعی را به این پورت معرفی کنیم از دستور switchport private-vlan mapping 300 100,200 استفاده می‌کنیم که شماره‌ی اول که ۳۰۰ است مربوط به VLAN Primary است که مربوط به همین پورت است و شماره‌های ۱۰۰ و ۲۰۰ که مربوط به VLANهای دیگر است باید به این پورت معرفی کنیم تا دسترسی لازم را به آن داشته باشند.

```
Switch(config-if)#interface range ethernet 0/0-2
Switch(config-if-range)#switchport mode private-vlan host
Switch(config-if-range)#switchport private-vlan host-association 300 100
```

در دستور بالا وارد سه پورتی شدیم که به DC1 ,DC2 ,DC3 متصل شده است، با دستور switchport mode private-vlan host به پورت مورد نظر اعلام کردیم که این سه پورت به کلاینت متصل خواهد شد و دستور switchport private-vlan host-association 300 100 هم برای معرفی VLAN اصلی و فرعی کاربرد دارد.

دستور Host عموماً به سیستم‌هایی داده می‌شود که در شبکه داخلی قرار داشته باشند و بخواهند با دنیای بیرون ارتباط برقرار کنند.

```
Switch(config)#int e0/3
Switch(config-if)#switchport mode private-vlan host
Switch(config-if)#switchport private-vlan host-association 300 200
Switch(config-if)#int e1/0
Switch(config-if)#switchport mode private-vlan host
Switch(config-if)#switchport private-vlan host-association 300 200
```

در دستورات بالا هم وارد دو پورتی شدیم که به سرور DC1 و DC2 متصل شده است و دستور مورد نظر را برای آنها اجرا کردیم.

تا به اینجا توانستیم VLAN مورد نظر را تعریف کنیم و پورت‌های مشخص شده را درون VLAN قرار دهیم، حال اگر بخواهیم کارکرد این عمل را تست بگیریم می‌توانیم از دستور زیر استفاده کنیم:

```
Switch#show vlan private-vlan
Primary  Secondary   Type            Ports
------- --------- ----------------- ----------------------------------------
300      100         community     Et0/0, Et0/1, Et0/2, Et1/1
300      200         isolated      Et0/0, Et0/3, Et1/0, Et1/1
```

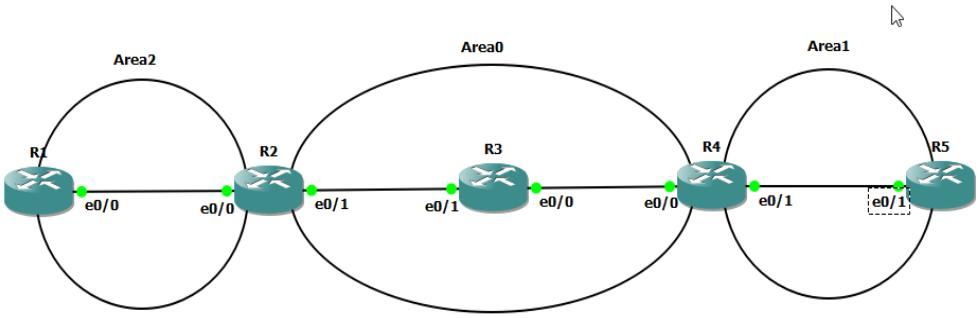
با استفاده از دستور show vlan private-vlan می‌توانید مشاهده کنید که چه VLANهایی به عنوان VLAN اصلی و ثانویه انتخاب شده‌اند و نوع آنها را می‌توانید مشاهده کنید، در قسمت Port هم مشخص شده است که Et0/0 که به عنوان پورت Primary در نظر گرفتیم در هر دو قسمت قرار دارد .

www.takbook.com

۶-۱۱ فعال‌سازی تأیید اعتبار در به روزرسانی مسیریابی درOSPF

، در فصل ششم به طور کامل در مورد پروتکل OSPF صحبت کردیم و نحوه‌ی راه‌اندازی آن را فرا گرفتیم، همانطور که در این فصل بررسی کردیم بحث امنیت یک مبحث بسیار مهم و پیچیده است که در این پروتکل مسیریابی باید اجرایی شود تا ارتباط بین روترها در آن به صورت امن صورت گیرد، برای همین موضع به مثال زیر توجه کنید.

به مانند شکل ۳۲-۱۱، نرم‌افزار GNS3 را اجرا کرده و چهار روتر را به لیست اضافه کنید و به صورت زیر به هم متصل کنید، و طبق جدول آدرس IP را در Interfaceهای مورد نظر وارد کنید.



شکل ۳۲-۱۱ سناریو Private VLAN

جدول ۱۲-۱۱ تنظیمات IP

	E0/0	E0/1	LoopBack
R1	172.16.1.1/24	--------	150.1.1.1/24
R2	172.16.1.2/24	172.16.2.1/24	150.1.2.2/24
R3	172.16.3.1/24	172.16.2.2/24	150.1.3.3/24
R4	172.16.3.2/24	172.16.4.1/24	150.1.4.4/24
R5	-------	172.16.4.2/24	150.1.5.5/24

بعد از تخصیص IPها در روتر باید پروتکل OSPF را راه‌اندازی کنیم:

روتر R1:

Router(config)#**router ospf 20**

تعریف Router OSPF 20 که ۲۰ یک شماره‌ی شناسایی برای این پروتکل است که تأثیری در روند کار ندارد، اما باید تعریف شود.

Router(config-router)#**router-id 150.1.1.1**

www.takbook.com

در این قسمت باید RID روتر را تعریف کنید که این IP مربوط به اینترفیس LoopBack است، پس بعد از ورود به پروتکل OSPF در درجه‌ی اول RID را تعریف کنید.

Router(config-router)#**network 172.16.1.1 0.0.0.0 area 2**

در این قسمت Network های مربوط به روتر را تعریف می‌کنیم و می‌گوییم که در کدام area قرار دارد، مثلاً در این قسمت، اینترفیس Fa0/0 روتر R1 در Area2 قرار دارد. در تعریف Network، اول خود Ip و بعد،Wild Card MASk مربوط به آن را وارد می‌کنیم که همان‌طور که در مطالب قبلی کتاب گفتیم، سعی کنید به جای Wild Card Mask از چهار صفر استفاده کنید (0.0.0.0).

در بقیه‌ی روترها هم همین کار را انجام دهید:

روتر R2:

```
Router(config)#router ospf 10
Router(config-router)#router-id 150.1.2.2
Router(config-router)#network 172.16.1.2 0.0.0.0 area 2
Router(config-router)#network 172.16.2.1 0.0.0.0 area 0
```

روتر R3:

```
Router(config)#router ospf 10
Router(config-router)#router-id 150.1.3.3
Router(config-router)#net 172.16.2.2 0.0.0.0 area 0
Router(config-router)#net 172.16.3.1 0.0.0.0 area 0
```

روتر R4:

```
Router(config)#router ospf 30
Router(config-router)#router-id 150.1.4.4
Router(config-router)#net 172.16.3.2 0.0.0.0 area 0
Router(config-router)#net 172.16.4.1 0.0.0.0 area 1
```

روتر R5:

```
Router(config)#router ospf 30
Router(config-router)#router-id 150.1.5.5
Router(config-router)#net 172.16.4.2 0.0.0.0 area 1
```

در این قسمت، از طریق فرمان Show Ip Route، نگاهی به جدول روتینگ روتر R1 می‌کنیم و این دستور را در مد Privileged وارد می‌کنیم:

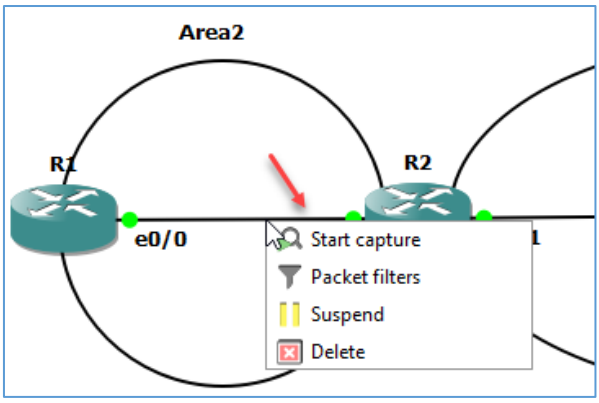
```
R1#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, + - replicated route

Gateway of last resort is not set

     150.1.0.0/16 is variably subnetted, 2 subnets, 2 masks
```

www.takbook.com


```
C       150.1.1.0/24 is directly connected, Loopback0
L       150.1.1.1/32 is directly connected, Loopback0
     172.16.0.0/16 is variably subnetted, 5 subnets, 2 masks
C       172.16.1.0/24 is directly connected, Ethernet0/0
L       172.16.1.1/32 is directly connected, Ethernet0/0
O IA    172.16.2.0/24 [110/20] via 172.16.1.2, 00:03:26, Ethernet0/0
O IA    172.16.3.0/24 [110/30] via 172.16.1.2, 00:02:29, Ethernet0/0
O IA    172.16.4.0/24 [110/40] via 172.16.1.2, 00:01:20, Ethernet0/0
```

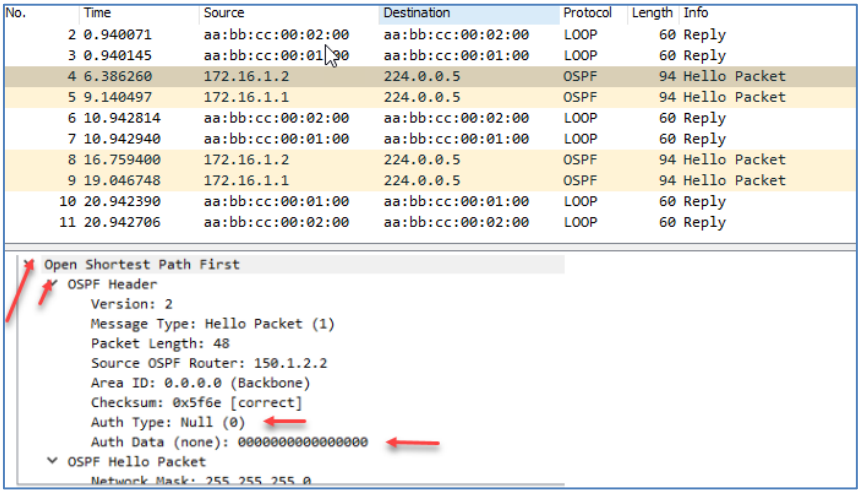
همان‌طور که مشاهده می‌کنید، Network هایی که از طریق OSPF یاد گرفته است به صورت O IA نمایش داده است که O IA، بیانگر OSPF inter area است و نشان‌دهنده‌ی این است که این شبکه‌ها را از Area دیگری غیر از area خود یاد گرفته است و اگر یک روتر در area خود چیزی یاد بگیرد، آن را با حرف O ثبت می‌کند.

برای اینکه متوجه شویم امنیت کار چقدر ارزش دارد به مانند شکل ۳۳-۱۱، بر روی خط ارتباطی بین روتر R1 و R2 کلیک راست کنید و گزینه‌ی Start capture را کلیک کنید تا از طریق Wireshark بتوانیم جزئیات کار را مشخص کنیم.



شکل ۳۳-۱۱ بررسی ارتباط با Wireshark

www.takbook.com



No.	Time	Source	Destination	Protocol	Length	Info
2	0.940071	aa:bb:cc:00:02:00	aa:bb:cc:00:02:00	LOOP	60	Reply
3	0.940145	aa:bb:cc:00:01:00	aa:bb:cc:00:01:00	LOOP	60	Reply
4	6.386260	172.16.1.2	224.0.0.5	OSPF	94	Hello Packet
5	9.140497	172.16.1.1	224.0.0.5	OSPF	94	Hello Packet
6	10.942814	aa:bb:cc:00:02:00	aa:bb:cc:00:02:00	LOOP	60	Reply
7	10.942940	aa:bb:cc:00:01:00	aa:bb:cc:00:01:00	LOOP	60	Reply
8	16.759400	172.16.1.2	224.0.0.5	OSPF	94	Hello Packet
9	19.046748	172.16.1.1	224.0.0.5	OSPF	94	Hello Packet
10	20.942390	aa:bb:cc:00:01:00	aa:bb:cc:00:01:00	LOOP	60	Reply
11	20.942706	aa:bb:cc:00:02:00	aa:bb:cc:00:02:00	LOOP	60	Reply

```
Open Shortest Path First
  OSPF Header
    Version: 2
    Message Type: Hello Packet (1)
    Packet Length: 48
    Source OSPF Router: 150.1.2.2
    Area ID: 0.0.0.0 (Backbone)
    Checksum: 0x5f6e [correct]
    Auth Type: Null (0)
    Auth Data (none): 0000000000000000
  OSPF Hello Packet
    Network Mask: 255.255.255.0
```

شکل ۳۴-۱۱ اطلاعات خط ارتباطی

در شکل ۳۴-۱۱، پروتکل‌های OSPF را مشاهده می‌کنید، اگر یکی از آنها را انتخاب کنید در قسمت Open Shortest path First و قسمت OSPF Header گزینه‌ی Auth Type برابر Null قرار گرفته که نشان دهنده این است که هیچ گونه امنیتی در این پروتکل لحاظ نشده و مهاجم به راحتی می‌تواند روتر خود را به عنوان یک همسایه جدید به Area مورد نظر اعلام کند و کل جدول مسیریابی را تغییر دهد، برای حل این مشکل باید دستورات امنیتی را بین دو یا چند روتر که در یک یا چند Area هستند اعمال کنیم.

برای مثال می‌خواهیم امنیت را بین روتر R1 و R2 برقرار کنیم که برای این کار باید به صورت زیر عمل کنید:

روتر R1:

وارد Interface که در Area1 قرار دارد شوید و دستور زیر را وارد کنید:

```
R1(config-if)#int e0/0
```

با دستور زیر:message-digestفعال کردن الگوریتم

```
R1(config-if)#ip ospf authentication message-digest
```

در دستور زیر عدد یک می‌تواند بین 1 تا 65535 متغیر باشد که در اینجا عدد یک را انتخاب می‌کنیم و توجه کنید در روتر روبرو هم باید همین عدد را انتخاب کنید، بعد از ان الگوریتم MD5 و بعد یک رمز عبور پیچیده برای ان در نظر بگیرید.

```
R1(config-if)#ip ospf message-digest-key 1 md5 Test@12345
```

بعد از اجرای دستور بالا وارد OSPF:شوید و دستور زیر را وارد کنید

```
R1(config-if)#router ospf 20
R1(config-router)#area 1 authentication message-digest
```

www.takbook.com

بعد از اجرای کامل دستورات پیغام زیر را در صفحه مشاهده خواهید کرد که به این نکته اشاره دارد که ارتباط با روتر 150.1.2.2 که همان روتر R2 است قطع شده و دلیل آن هم این است که در R1 الگوریتم و رمز عبور را فعال کردید ولی در روتر R2 انجام ندادید.

*Dec 8 07:33:52.175: %OSPF-5-ADJCHG: Process 20, Nbr 150.1.2.2 on Ethernet0/0 from FULL to DOWN, Neighbor Down: Dead timer expired

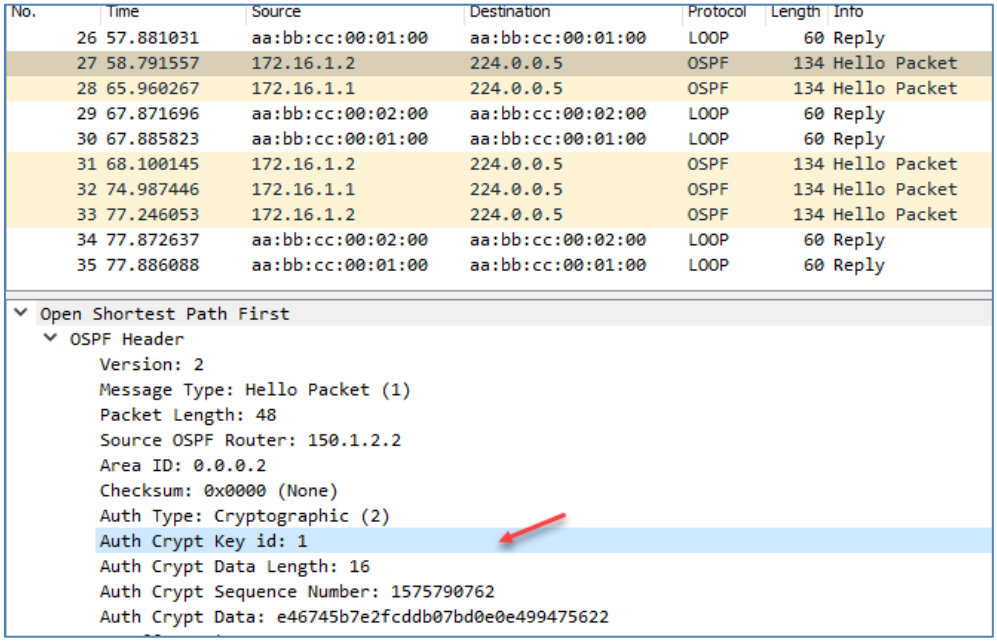
روتر R2 :

در روتر R2 هم دستورات زیر را وارد کنید:

```
R2(config-router)#int e0/0
R2(config-if)#ip ospf authentication message-digest
R2(config-if)#ip ospf message-digest-key 1 md5 Test@12345
R2(config-router)#router ospf 10
R2(config-router)#area 1 authentication message-digest
```

بعد از فعال کردن رمز دوباره ارتباط بین R1 و R2 را با استفاده از نرم‌افزار WireShark ارتباط آنها را بررسی می‌کنیم.

همانطور که در شکل ۳۵-۱۱، مشاهده می‌کنید قسمت OSPF Header به صورت کامل تغییر کرده است و به صورت کامل رمزنگاری شده است، کلمه Auth Crypt در شکل تایید کننده‌ی این موضوع است.



No.	Time	Source	Destination	Protocol	Length	Info
26	57.881031	aa:bb:cc:00:01:00	aa:bb:cc:00:01:00	LOOP	60	Reply
27	58.791557	172.16.1.2	224.0.0.5	OSPF	134	Hello Packet
28	65.960267	172.16.1.1	224.0.0.5	OSPF	134	Hello Packet
29	67.871696	aa:bb:cc:00:02:00	aa:bb:cc:00:02:00	LOOP	60	Reply
30	67.885823	aa:bb:cc:00:01:00	aa:bb:cc:00:01:00	LOOP	60	Reply
31	68.100145	172.16.1.2	224.0.0.5	OSPF	134	Hello Packet
32	74.987446	172.16.1.1	224.0.0.5	OSPF	134	Hello Packet
33	77.246053	172.16.1.2	224.0.0.5	OSPF	134	Hello Packet
34	77.872637	aa:bb:cc:00:02:00	aa:bb:cc:00:02:00	LOOP	60	Reply
35	77.886088	aa:bb:cc:00:01:00	aa:bb:cc:00:01:00	LOOP	60	Reply

```
Open Shortest Path First
  OSPF Header
    Version: 2
    Message Type: Hello Packet (1)
    Packet Length: 48
    Source OSPF Router: 150.1.2.2
    Area ID: 0.0.0.2
    Checksum: 0x0000 (None)
    Auth Type: Cryptographic (2)
    Auth Crypt Key id: 1
    Auth Crypt Data Length: 16
    Auth Crypt Sequence Number: 1575790762
    Auth Crypt Data: e46745b7e2fcddb07bd0e0e499475622
```

شکل ۳۵-۱۱ اطلاعات خط ارتباطی

www.takbook.com

۷-۱۱ سوالات فصل یازدهم

1. Which one of the following terms means anything that can be considered to be a weakness that can compromise security?
کدام یک از اصطلاحات زیر به معنای هر چیزی است که می تواند ضعف در نظر گرفته شود و امنیت را به خطر اندازد؟

a. Exploit
b. Vulnerability
c .Attack
d. Threat

2. An actual potential to exploit a vulnerability is known as which one of the following terms?
بهره‌برداری از یک پتاسنسل یا ضعف در یک شبکه به کدام یک از این اصطلاحات اشاره دارد؟

a. Vulnerability
b. Attack
c. Exploit
d. Threat

3. In a spoofing attack, which of the following parameters are commonly spoofed? (Choose two answers.)
در حمله spoofing ، کدام یک از پارامترهای زیر معمولاً از بین می روند؟ (دوگزینه را انتخاب کنید).

a. MAC address
b. Source IP address
c. Destination IP address
d. ARP address
e. Suppose an attacker sends a series of packets toward

4. a destination IP address with the TCP SYN flag set but sends no other packet types. Which of the following attacks is likely taking place?
یک آدرس IP مقصد با مجموعه پرچم TCP SYN داریم، اما بسته‌ی دیگری ارسال نمی‌شود .کدام یک از حملات زیر احتمالاً رخ داده است؟

a. Spoofing attack
b. Reflection attack
c. Reconnaissance attack
d. Denial-of-service attack
e. None of the choices are correct.

5. In a reflection attack, the source IP address in the attack packets is spoofed so that it contains which one of the following entities?
در حمله‌ی reflection آدرس IP منبع به گونه‌ای جعل شده است، این مورد به کدام گزینه اشاره دارد؟

۱. The address of the attacker

۲. The address of the reflector

۳. The address of the victim

.۴The address of the router

www.takbook.com

۶. During a successful man-in-the-middle attack, which two of the following actions is an attacker most likely to perform?

یک حمله‌ی موفقیت‌آمیز man-in-the-middle توسط مهاجمی انجام می‌شود، اولین کاری که مهاجم بعد از حمله انجام می‌دهد چیست؟

۱. Eavesdrop on traffic passing between hosts

۲. Induce a buffer overflow on multiple hosts

۳. Modify data passing between hosts

۴. Use ping sweeps and port scans to discover the network

۷. Which one of the following is the goal of a bruteforce attack?

هدف یک حمله‌ی bruteforce کدام یک از موارد زیر است؟

۱. Try every possible TCP port until a service answers

۲. Try every possible combination of keyboard characters to guess a user's password

۳. Initiate a denial-of-service operation on every possible host in a subnet

۴. Spoof every possible IP address in an organization

۸. Which one of the following is an example of a AAA server?

کدام یک از موارد زیر نمونه‌ای از سرور AAA است؟

۱. DHCP

۲. DNS

۳. SNMP

۴. ISE

۹. Physical access control is important for which one of the following reasons?

کنترل کردن دسترسی فیزیکی برای کدام یک از دلایل زیر مهم است؟

۱. It prevents unauthorized people from sitting at a corporate user's desk and using their computer.

۲. It prevents users from getting angry and damaging computer equipment.

۳. It prevents unauthorized access to network closets.

۴. It prevents fires from destroying data centers.

www.takbook.com

فصل دوازدهم

IP Services

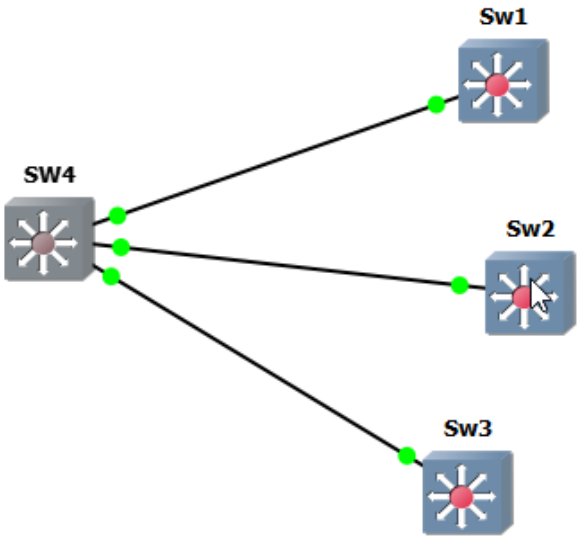
در این فصل می‌خواهیم با سرویس‌هایی که با IP سروکار دارند کار کنیم مانند سرویس NTP, LLDP, CDP و ...

۱-۱۲ پروتکل‌های مدیریت دستگاه‌ها

۱-۱-۱۲ بررسی پروتکل CDP و LLDP

این دو پروتکل برای نمایش لیست دستگاه‌هایی است که به یک روتر یا سوئیچ متصل شده‌اند، CDP یا همان Cisco Discovery Protocol مختص شرکت سیسکو بوده و فقط در دستگاه‌های این شرکت کارایی دارد و LLDP یا همان Link Layer Discovery Protocol یک پروتکل عمومی است که هم در سیسکو و هم در دستگاه‌های دیگر کاربرد دارد.

در این مثال پروتکل CDP را بررسی می‌کنیم و امنیت آن را هم به چالش می‌کشیم.



شکل ۱-۱۲ سناریو CDP

www.takbook.com

در شکل ۱–۱۲، از ۴ سوئیچ استفاده می‌کنیم که سوئیچ‌های ۱، ۲ و ۳ به سوئیچ ۴ متصل هستند. می‌خواهیم بدانید چه دستگاه‌هایی از چه مدلی به سوئیچ SW4 متصل است، برای این کار از دستور زیر استفاده می‌کنیم:

وارد سوئیچ ۴ شوید و در مد Privileged، دستور زیر را وارد کنید:

SW4#**show cdp neighbors**

Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge

S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone,

D - Remote, C - CVTA, M - Two-port Mac Relay

Device ID	Local Intrfce	Holdtme	Capability	Platform	Port ID
Sw1	Eth 0/0	128	R S I	Linux Uni	Eth 0/0
Sw2	Eth 0/1	128	R S I	Linux Uni	Eth 0/1
Sw3	Eth 0/2	129	R S I	Linux Uni	Eth 0/0

همان‌طور که مشاهده می‌کنید با اجرای دستور show cdp neighbors، لیست سوئیچ‌های متصل به این سوئیچ را با ویژگی‌های سوئیچ‌های مربوطه نمایش داد.

در این دستور به ما شماره‌ی پورت، شماره‌ی دستگاه، نوع دستگاه، پورت ورودی به سوئیچ و مقدار زمانی که طول کشید سوئیچ دستگاه‌های متصل به خودش را شناسایی کند را نمایش می‌دهد.
برای اینکه به جزئیات بیشتر در مورد دستگاه‌های متصل شده دست پیدا کنیم از دستور زیر استفاده می‌کنیم:

SW4# **show cdp neighbors detail**

پروتکل CDP هر ۶۰ ثانیه یک‌بار، اطلاعات مربوط را به دستگاه‌های متصل به خود را ارسال می‌کند و دستگاه‌هایی که این پیام را دریافت می‌کنند، این پیام را در جدولی که معرفی کردیم، ذخیره می‌کنند.
یکی از مشکلاتی که این دو پروتکل (CDP , LLDP) دارد این است که مهاجم با گوش دادن به خط ارتباطی آنها می‌تواند به اطلاعات خوبی دست پیدا کند.

وارد سوئیچ شوید و دستور Show lldp را وارد کنید که نتیجه آن را در زیر مشاهده می‌کنید که این پروتکل به صورت پیش‌فرض غیر فعال است و اگر هم فعال بود با دستور no lldp run می‌توانید آن را غیر فعال کنید.

SW4#**show lldp**

www.takbook.com

%LLDP is not enabled

برای غیرفعال کردن پروتکل CDP هم می‌توانید از دستورات زیر استفاده کنید:

SW4(config)#**no cdp run**

با دستور بالا CDP غیر فعال خواهد شد و برای اینکه متوجه شویم دستور به خوبی اجرا شده باید Show cdp را اجرا کنید.

SW4(config)#**do sh cdp**

%CDP is not enabled

برای اینکه CDP را فقط در Interface مشخص، غیرفعال کنید باید از دستورات زیر استفاده کنید:

SW4(config)#**interface ethernet 0/0**

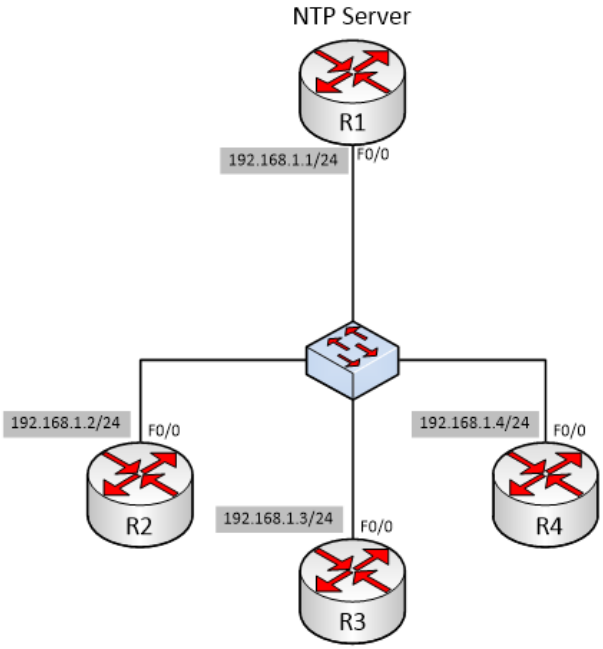
SW4(config-if)#**no cdp enable**

CDP در لایه ۲ عمل می‌کند و می‌تواند اطلاعاتی را برای مهاجمان، به عنوان مثال(نوع دستگاه ، نسخه‌های سخت‌افزاری و نرم‌افزاری ،جزئیات آدرس VLAN و IP و موارد دیگر) ارسال کند که این می‌تواند بسیار نگران کننده باشد.

۲-۱-۱۲ سرویس NTP

از آنجا که زمان، یک فاکتور بسیار مهم در شبکه است و باید تمام اتفاقاتی که در آن روی می‌دهد باید در زمان و تاریخ مشخص در سیستم ثبت شود به خاطر همین از سرویس NTP برای مشخص کردن زمان دستگاه‌ها استفاده می‌کنیم، با یک مثال این پروتکل را بررسی می‌کنیم:

www.takbook.com



شکل ۲-۱۲ سناریو NTP

در شکل ۲-۱۲، R1 به عنوان سرور NTP در نظر می‌گیریم و به بقیه‌ی روترها باید از روتر R1، تنظیمات ساعت و تاریخ را دریافت کنند.

وارد روتر R1 شوید و دستورات زیر را وارد کنید:

R1#**clock set 10:15:00 22 nov 2013**

R1#**configure t**

R1#**configure terminal**

R1(config)#**ntp master 1**

R1(config)#**ntp authentication-key 1 md5 saman 123**

در قسمت اول، ساعت و تاریخ روتر را تنظیم کردیم و بعد وارد مد Global شدیم و دستور Ntp Master 1 را وارد کردیم که با این دستور، این روتر را به عنوان روتر سرور برای پروتکل NTP در نظر می‌گیریم. عدد ۱ که در انتهای دستور مشاهده می‌کنید، می‌تواند از 1 تا 15 و برای مشخص کردن Master مورد نظر باشد و بعدازآن، یک کلید امنیتی تعریف می‌کنیم تا کسی بدون اجازه، زیرمجموعه این سرور نشود.

بعد از مشخص کردن سرور NTP، باید وارد روترهای دیگر شویم و روتر R1 را به عنوان روتر NTP به روترهای دیگر معرفی کنیم:

www.takbook.com

در روترهای R2,R3,R4 دستورات زیر را وارد کنید:

R5(config)#**ntp server 192.168.1.1**

R5(config)#**ntp authentication-key 1 md5 saman 123**

با این دستور، روترها تنظیمات ساعت و تاریخ خود را از سرور، یعنی R1 دریافت می‌کنند. برای مشاهده‌ی این موضوع از دستور زیر استفاده می‌کنیم:

R2#**show ntp status**

Clock is synchronized, stratum 2, reference is 192.168.1.1

nominal freq is 250.0000 Hz, actual freq is 250.0003 Hz, precision is 2**18

reference time is D639AF96.2C66330A (10:25:26.173 UTC Fri Nov 22 2013)

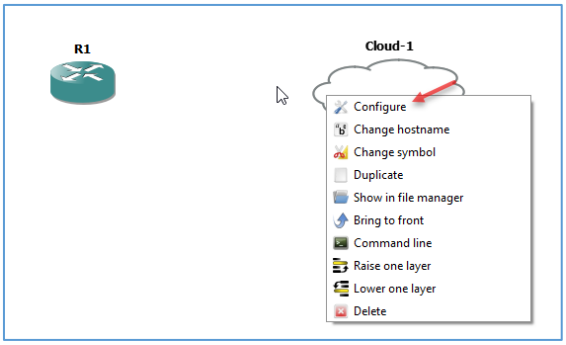
clock offset is 12.7890 msec, root delay is 43.90 msec

root dispersion is 902.04 msec, peer dispersion is 889.22 msec

همان‌طور که مشاهده می‌کنید، وارد روتر R2 شدیم و از دستور **show ntp status** استفاده کردیم که به ما تاریخ و ساعت مورد نظر را نمایش داد.

۳-۱-۱۲ سرویس Log در دستگاه‌های سیسکو

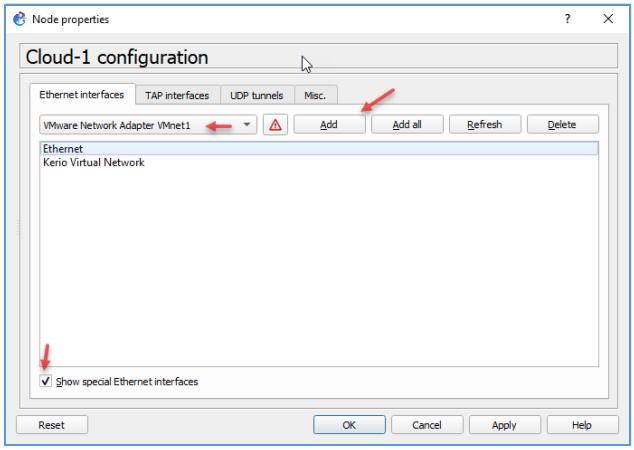
داشتن اطلاعات از رویدادهایی که برای دستگاه‌های شبکه مخصوصاً سوئیچ، روتر، فایروال و... اتفاق می‌افتد بسیار می‌تواند شما را در ارائه گزارش درست و جلوگیری از مشکلات ناشی از آن کمک کند، برای انجام این کار به مانند شکل ۳-۱۲، یک روتر و یک Cloud را به صفحه اضافه کنید و بر روی آن کلیک راست و گزینه‌ی Configure را انتخاب کنید.



شکل ۳-۱۲ تنظیمات GNS3

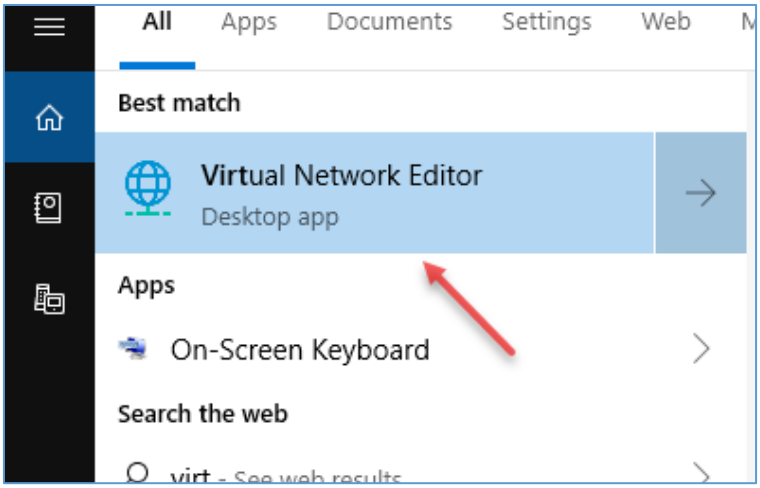
در شکل ۴-۱۲، از قسمت پایین آن تیک گزینه‌ی Show special Ethernet interfaces را انتخاب کنید و بعد از لیست کشویی کارت شبکه مجازی VMnet1 را انتخاب کنید، این کارت شبکه مجازی مربوط به VMware است که می‌توانید رنج IP آن را تنظیم کنید، بر روی ok کلیک کنید.

www.takbook.com



شکل ۴-۱۲ تنظیمات GNS3

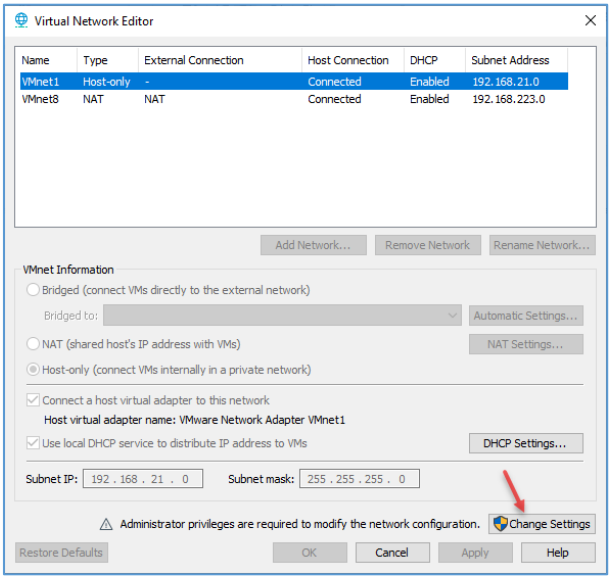
برای اینکه تنظیمات کارت شبکه مجازی را مشاهده کنید به مانند شکل ۵-۱۲، بر روی Start کلیک کنید و سرویس Virtual Network Editor را اجرا کنید.



شکل ۵-۱۲ تنظیمات کارت شبکه مجازی

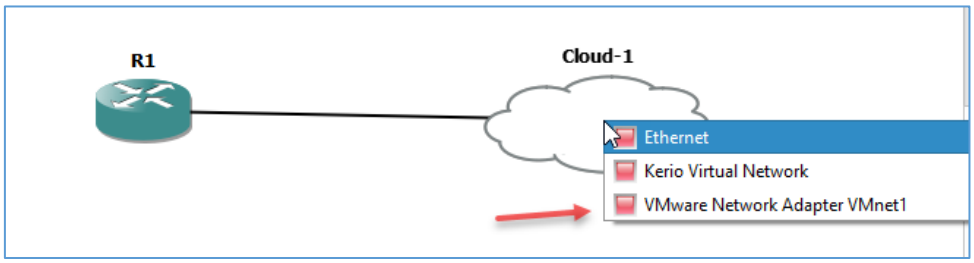
در شکل ۶-۱۲، لیست کارت شبکه مجازی خود را مشاهده می‌کنید، برای اینکه بتوانید آدرس مورد نظر خود را وارد کنید و کارت شبکه را ویرایش کنید باید بر روی Change Settings کلیک کنید.

www.takbook.com



شکل ۶-۱۲ لیست کارت شبکه‌ی مجازی

بعد از تنظیم کارت شبکه در زمان اتصال به Cloud می‌توانید نام کارت شبکه مجازی را به مانند شکل ۱۲-۷، انتخاب کنید.



شکل ۷-۱۲ تنظیمات Cloud در GNS3

برای شروع به روتر R1 آدرس IP می‌دهیم:

R1(config)#**interface ethernet 0/0**

R1 (config-if)#**ip addres 192.168.21.6 255.255.255.0**

R1 (config-if)#**no sh**

همانطور که مشاهده می‌کنید آدرس 192.168.21.6 به روتر R1 تخصیص داده شده است و پورت آن روشن شده است.

www.takbook.com

پس تا به اینجا یک روتر با نام R1 به صفحه اضافه کردیم و آدرس آن را 192.168.21.6 در نظر گرفتیم و آن را به یک Cloud متصل کردیم که می‌توانیم از سیستم واقعی خود به آن روتر دسترسی داشته باشیم، برای اینکه ادامه کار را بررسی کنیم باید یک نرم‌افزار Syslog Server را دانلود و بر روی سیستم خود نصب کنیم.

نرم‌افزاری که برای این کار در نظر گرفتیم نرم‌افزار SolarWinds Kiwi Syslog Server است که می‌توانید آن را از سایت مربوط به آن دانلود کنید، بعد از نصب دو آیکون شکل ۸-۱۲، را مشاهده می‌کنید که یکی برای تحت ویندوز و دیگری برای تحت وب است که در ادامه از هر دوی آنها استفاده خواهیم کرد.

شکل ۸-۱۲ ایکون نرم‌افزار SolarWinds Kiwi Syslog Server

در ادامه کار، دوباره وارد روتر شوید و دستور زیر ار اجرا کنید:

```
R1(config)#logging trap ?
  <0-7>          Logging severity level
  alerts         Immediate action needed          (severity=1)
  critical       Critical conditions              (severity=2)
  debugging      Debugging messages               (severity=7)
  emergencies    System is unusable               (severity=0)
  errors         Error conditions                 (severity=3)
  informational  Informational messages           (severity=6)
  notifications  Normal but significant conditions (severity=5)
  warnings       Warning conditions               (severity=4)
  <cr>
```

با اجرای دستور logging trap ? گزینه‌های مختلف برای اجرای logگیری به شما نمایش داده خواهد شد که جلوی هر یک از آنها عددی وجود دارد که عنوان آن severity در نظر گرفته شده است، مثلاً گزینه‌ی یک مربوط به logهای Alert است و به همین ترتیب گزینه‌های دیگر، اگر گزینه‌ی یک را انتخاب کنید، فقط

www.takbook.com

و فقط Alert برای سرور Syslog ارسال خواهد شد و گزینه‌های دیگر ارسال نخواهند شد ولی اگر گزینه‌ی هفتم را انتخاب کنید همه‌ی گزینه‌های قبل از آن به سرور Syslog ارسال خواهند شد و نیاز نیست تک تک آنها را در این دستور وارد کنید.

R1(config)#**logging trap debugging**

با دستور بالا عملیات Logگیری از سرور با سطح Debugging فعال شده است و ادامه باید اطلاعات را به سرور Syslog ارسال کنیم.

R1(config)#**logging source-interface ethernet 0/0**

در دستور بالا باید مشخص کنیم که اطلاعات Log را به کدام Interface ارسال کنیم، که در این قسمت Interface شماره 0/0 مشخص شده است که به Cloud متصل است.

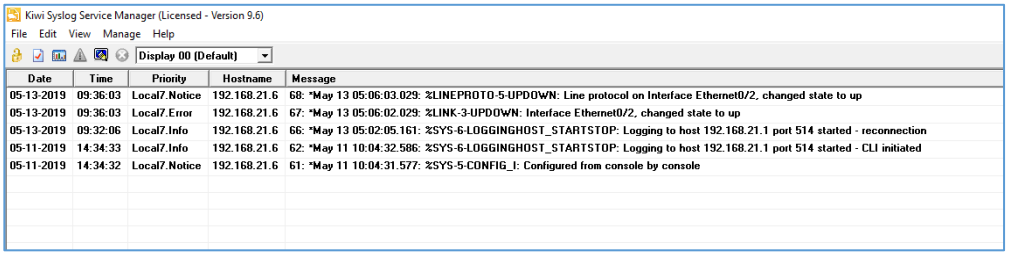
R1(config)#**logging on**

با دستور logging on سرور شروع به Log انداختن می‌کند، یعنی هر کاری که در روتر انجام شود، یک Log برای آن ایجاد خواهد شد.

R1(config)#**logging host 192.168.21.1**

با این دستور مشخص می‌کنیم، که چه سیستمی به عنوان Syslog سرور است، یعنی نرم‌افزار Syslog سرور بر روی آن نصب شده است که در اینجا آدرس آن 192.168.21.1 در نظر گرفته شده است.

حال اگر هر اتفاقی در روتر رخ دهد اطلاعات آن به مانند شکل ۹-۱۲ به نرم‌افزار Kiwi Syslog سرور ارسال خواهد شد.



شکل ۹-۱۲ نرم‌افزار SolarWinds Kiwi Syslog Server

www.takbook.com

Network Address Translation ۱۲-۲

همان‌طور که می‌دانید ipهایی که درون شبکه خود استفاده می‌کنیم، Private هستند و برای ارتباط با دنیای اینترنت باید تبدیل به یک ip valid شوند، ip valid توسط سازمان IANNA رجیستر و تعریف می‌شود و در دنیای اینترنت اعتبار دارد.

در جدول ۱-۱۲، آدرس‌های Private را مشاهده می‌کنید، که همانطور که قبلاً گفتیم این آدرس‌ها در دنیای اینترنت اعتباری ندارند و فقط در شبکه داخلی کاربرد دارند.

جدول ۱-۱۲ IP Private

Range of IP Addresses	Network(s)	Class of Networks	Number of Networks
10.0.0.0 to 10.255.255.255	10.0.0.0	A	1
172.16.0.0 to 172.31.255.255	172.16.0.0 – 172.31.0.0	B	16
192.168.0.0 to 192.168.255.255	192.168.0.0 – 192.168.255.0	C	256

NAT(Network Address Translation) روشی برای ترجمه‌ی Private IP یا درون شبکه به ip valid یا اینترنت است.

IPها در NAT به چهار دسته تقسیم می‌شوند:

- Inside Local : به شبکه‌هایی گفته می‌شود که از Private IP استفاده می‌کنند، مانند شبکه‌ی داخلی. Inside Interface هم وجود دارد که به اینترفیسی گفته می‌شود که در شبکه‌ی Inside Network قرار داشته باشد.
- Inside Global: منظور آدرس‌های valid است که در دنیای اینترنت اعتبار دارند و آدرس‌های شبکه داخلی برای دسترسی به دنیای اینترنت باید از این نوع آدرس‌ها استفاده کنند. Outside interface هم وجود دارد که اینترفیسی است که پورت آن داخل شبکه‌ی Outside قرار داشته باشد.

www.takbook.com

- Outside Local : به آدرس‌هایی گفته می‌شود که دستگاه‌هایی که در شبکه داخلی قرار دارند می‌توانند آدرس‌های شبکه خارجی را ببینند، البته این آدرس‌ها می‌توانند آدرس Private باشد.
- Outside Global : به آدرس‌هایی گفته می‌شود که Public باشند و در دنیای اینترنت اعتبار داشته باشند، مانند آدرس 95.217.198.13 که مربوط به سایت 3isco.ir است.

NAT دارای انواع مختلفی است که در زیر آنها را بررسی می‌کنیم:

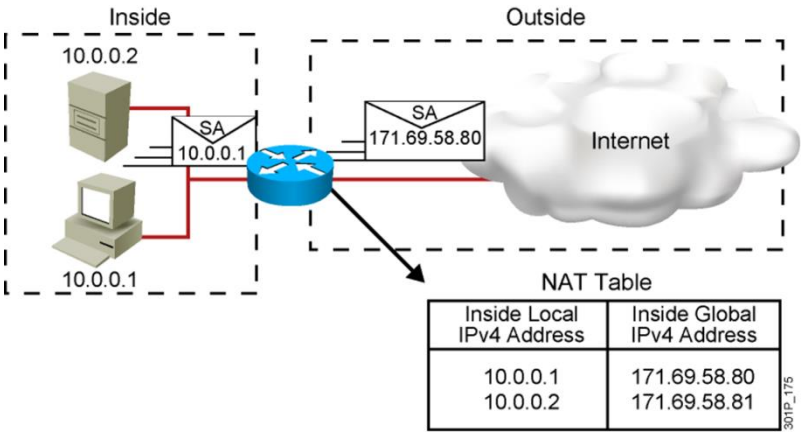
- Static Nat
- Dynamic Nat
- Dynamic Nat With Overload

Static Nat

این روش به صورت دستی انجام می‌شود، یعنی به صورت دستی به روتر می‌گوییم که Private IP داخل شبکه را به ip Valid تبدیل کن.

Dynamic Nat:

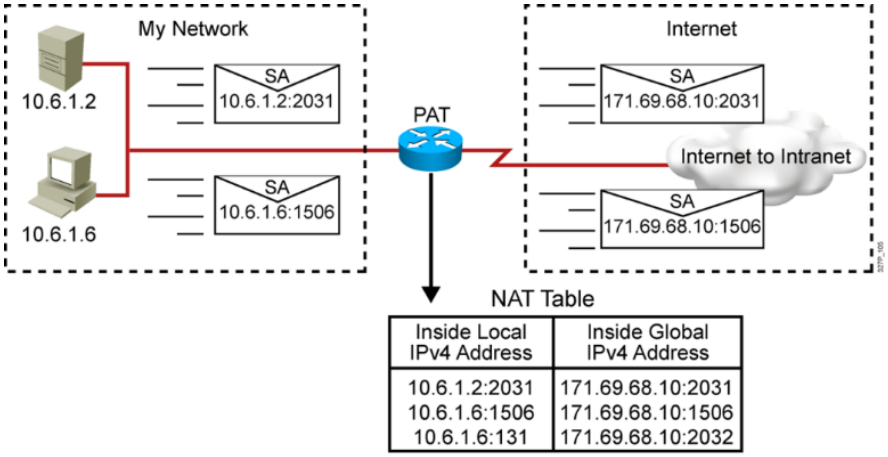
در این حالت، لیستی از Private IP آماده و لیست دیگر از ip Valid آماده می‌شود و روتر به صورت خودکار این دو لیست را در موقع ترجمه در کنار هم قرار می‌دهد و تبدیل می‌کند.



شکل ۱۰-۱۲ بررسی Dynamic NAT

Dynamic Nat With Overload(PAT)

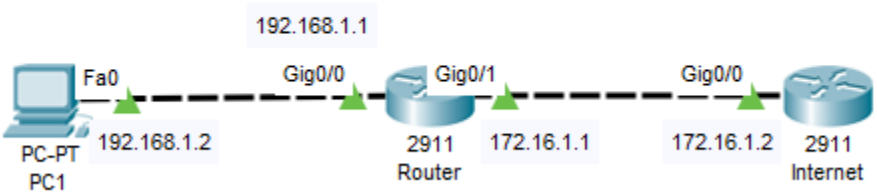
www.takbook.com



شکل ۱۱-۱۲ بررسی PAT

این روش یکی از بهترین روش‌ها در حال حاضر است، به دلیل اینکه شما احتیاج به یک ip valid دارید و تمام Private IP شبکه‌ی داخلی از طریق یک ip valid ترجمه می‌شوند، اما با استفاده از پورت، یعنی این‌که وقتی Private IP می‌خواهد به اینترنت راه پیدا کند از طریق همان ip valid و به همراه یک پورت به اینترنت راه پیدا می‌کند. در ادامه به صورت کامل با این موضوعات کار می‌کنیم.

مثالی از Static Nat:



شکل ۱۲-۱۲ سناریو Static Nat

در شکل ۱۲-۱۲، Pc1 می‌خواهد به اینترنت که در اینجا IP آدرس 172.16.1.2 آدرس VALID است متصل شود و به خاطر invalid بودن ip آن باید ترجمه آدرس به ip valid انجام شود. وارد روتر شوید و دستورات زیر را وارد کنید:

Router(config)#**ip nat inside source static 192.168.1.2 172.16.1.1**

www.takbook.com

این دستور می‌گوید که Ip Nat را روی شبکه داخلی و روی مبدأ فعال کن و به صورت دستی (Static) ip به شماره 192.168.1.2 را به ip valid ، 172.16.1.2 تبدیل کن.

بعد وارد اینترفیس GI0/0 که به سمت شبکه داخلی است می‌شویم و دستور زیر را وارد می‌کنیم:

```
Router(config-if)#ip nat inside
```

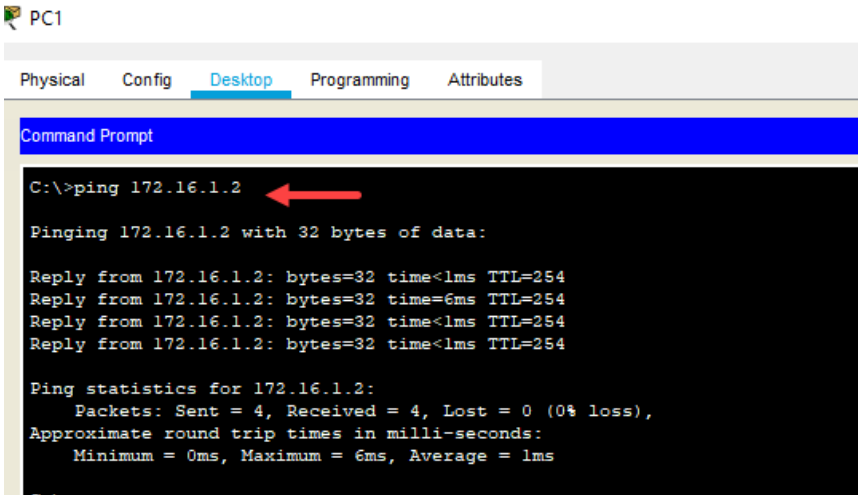
با این دستور Nat روی این اینترفیس فعال می‌شود، در اینترفیس دیگرGI0/1 که به سمت شبکه Outside است دستور زیر را وارد می‌کنیم:

```
Router(config-if)#ip nat Outside
```

بعد از اتمام کار ip مربوط به pc1 برای رفتن به شبکه اینترنت تبدیل می‌شود، می‌توانید با دستور زیر Nat فعال‌شده روی این روتر را مشاهده کنید.

```
Router#show ip nat  translations
Pro  Inside global    Inside local     Outside local    Outside global
---  172.16.1.2       192.168.1.2      ---              ---
```

برای اینکه عمکرد این سرویس را تست یگیریم به مانند شکل ۱۳-۱۱، می‌توانیم از طریق PC1 روتر 172.16.1.2 را Ping بگیریم.



شکل ۱۳-۱۲ Ping router

با ارسال اولین پکت به سمت روتر جدول NAT دچار تغییراتی خواهد شد که در زیر مشاهده می‌کنید:

```
Router(config-if)#do sh ip nat tra
Pro    Inside global     Inside local      Outside local     Outside global
icmp 172.16.1.1:10    192.168.1.2:10    172.16.1.2:10     172.16.1.2:10
icmp 172.16.1.1:13    192.168.1.2:13    172.16.1.2:13     172.16.1.2:13
icmp 172.16.1.1:14    192.168.1.2:14    172.16.1.2:14     172.16.1.2:14
icmp 172.16.1.1:15    192.168.1.2:15    172.16.1.2:15     172.16.1.2:15
icmp 172.16.1.1:16    192.168.1.2:16    172.16.1.2:16     172.16.1.2:16
```

www.takbook.com

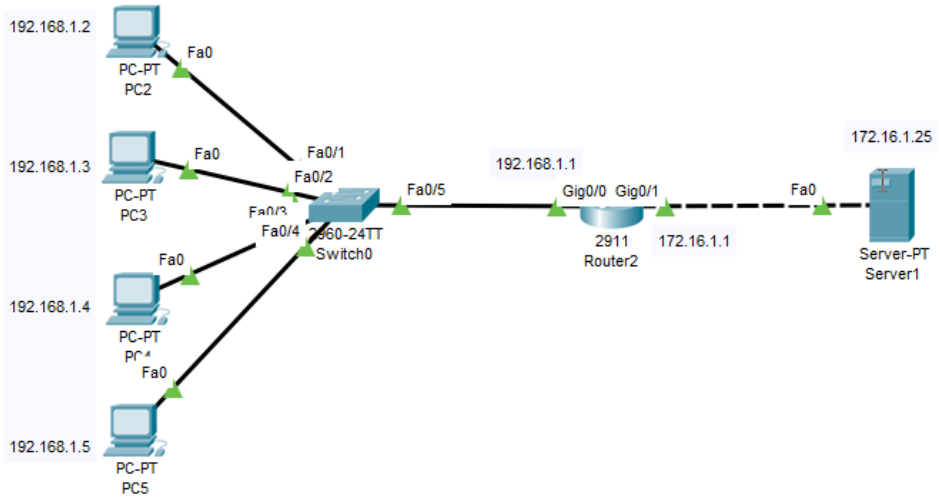
با دستور زیر اطلاعات کامل از Nat روی روتر به دست خواهید آورد:

```
Router#show ip nat statistics
Total translations: 1 (1 static, 0 dynamic, 0 extended)
Outside Interfaces: GigabitEthernet0/1
Inside Interfaces: GigabitEthernet0/0
Hits: 19  Misses: 45
Expired translations: 26
```

اگر به دستور بالا توجه کنید، Hit برابر 19 که تعداد پکت‌های درستی است که انتقال داده شده است و Misses تعداد پکت‌هایی است که مشکل داشته است، شما می‌توانید با مشاهده این دو مورد به کارکرد سرویس خود پی ببرید.

مثالی از Dynamic Nat

Dynamic mappings:



شکل ۱۴-۱۲ سناریو Dynamic Nat

برای استفاده از Dynamic Nat، اول از همه دو چیز تعریف می‌کنیم، یکی ip pool که مجموعه ipهای Valid که در این مثال 5 تا است را در خود نگه می‌دارد و بعد باید یک Access List برای ipهای invalid داخل شبکه خود تعریف کنیم و در آخر این دو را باهم ترکیب کنیم.

به مانند شکل ۱۴-۱۲، وارد روتر شوید و دستور زیر را وارد کنید:

	Start IP	End IP	
Router(config)#**ip nat pool oip**	**172.16.1.1**	**172.16.1.5**	**netmask 0.0.0.248**

www.takbook.com

این دستور را به این صورت بخوانید: ip nat pool ایجاد کن با نام OIP که می‌توانید هر نام دیگری هم قرار دهید و بعد از آن باید ipهای Vlaid را وارد کنید که در قسمت اول، شروع ip و در قسمت بعدی، پایان ip را مشخص کنید، مانند دستور بالا و در قسمت آخر هم Netmask آن را وارد کنید که همان Wild Card mask است. تا این قسمت، ip nat pool را تعریف کردیم و برای ادامه باید access-list را برای شبکه‌ی داخلی تعریف کنیم:

Router(config)#**access-list 10 permit 192.168.1.0 0.0.0.255**

Ipهای داخلی شبکه را در یک access-list قرار می‌دهیم و اجازه‌ی دسترسی به شبکه را به آن‌ها داده‌ایم.

حالا نوبت این است که این دو را به هم ارتباط دهیم:

Router(config)#**ip nat inside source list 10 pool oip**

با این دستور accss-list 10 با pool oip ارتباط برقرار می‌کند و در زمان خروج ipهای تعریف‌شده در access-list به ip تعریف‌شده در pool oip تبدیل می‌شوند.

بعد از این کار وارد اینترفیس می‌شویم و دستورات زیر را وارد می‌کنیم:

Router(config)#**int f0/0**
Router(config-if)#**ip nat inside**
Router(config-if)#**int f0/1**
Router(config-if)#**ip nat outside**

اگر از PCهای مورد نظر سرور 172.16.1.25 را Ping بگیریم نتیجه کار دستور show ip nat translations به صورت زیر خواهد شد.

Router#**show ip nat translations**

Pro	Inside global	Inside local	Outside local	Outside global
icmp	172.16.1.1:5	192.168.1.5:5	172.16.1.25:5	172.16.1.25:5
icmp	172.16.1.1:6	192.168.1.5:6	172.16.1.25:6	172.16.1.25:6
icmp	172.16.1.1:7	192.168.1.5:7	172.16.1.25:7	172.16.1.25:7
icmp	172.16.1.1:8	192.168.1.5:8	172.16.1.25:8	172.16.1.25:8
icmp	172.16.1.2:5	192.168.1.4:5	172.16.1.25:5	172.16.1.25:5
icmp	172.16.1.2:6	192.168.1.4:6	172.16.1.25:6	172.16.1.25:6
icmp	172.16.1.2:7	192.168.1.4:7	172.16.1.25:7	172.16.1.25:7
icmp	172.16.1.2:8	192.168.1.4:8	172.16.1.25:8	172.16.1.25:8
icmp	172.16.1.3:1	192.168.1.3:1	172.16.1.25:1	172.16.1.25:1
icmp	172.16.1.3:2	192.168.1.3:2	172.16.1.25:2	172.16.1.25:2
icmp	172.16.1.3:3	192.168.1.3:3	172.16.1.25:3	172.16.1.25:3
icmp	172.16.1.3:4	192.168.1.3:4	172.16.1.25:4	172.16.1.25:4

www.takbook.com

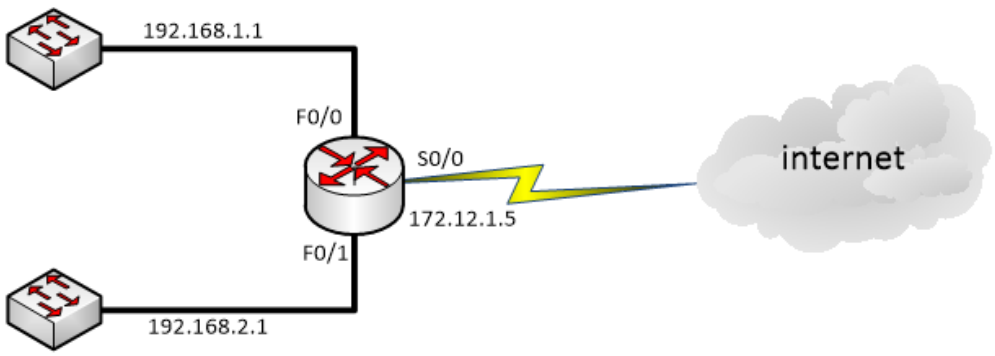
اگر به نتیجه دستور بالا توجه کنید، در قسمت Inside local آدرس IP مربوط به PC که پکت ارسال کرده است را مشاهده می‌کنید، در قسمت inside Global هم آدرس خروجی Router که همان آدرس VALID است و در Pool مشخص کردیم را نمایش می‌دهد و در دو قسمت آخر هم آدرس سرور مقصد را مشاهده می‌کنید.

نتیجه دستور show ip nat statistics به صورت زیر خواهد بود:

```
Router#show ip nat statistics
Total translations: 0 (0 static, 0 dynamic, 0 extended)
Outside Interfaces: GigabitEthernet0/1
Inside Interfaces: GigabitEthernet0/0
Hits: 27  Misses: 28
Expired translations: 28
Dynamic mappings:
-- Inside Source
access-list 10 pool oip refCount 0
 pool oip: netmask 0.0.0.248
      start 172.16.1.1 end 172.16.1.5
       type generic, total addresses 5 , allocated 0 (0%), misses 0
```

مثالی از PAT(Port Address Translation):

در این قسمت نیاز به یک IP Valid است و از طریق پورت، IPها را از هم جدا می‌کند. به شکل ۱۵ –۱۲، توجه کنید:



شکل ۱۵-۱۲ سناریو PAT

در شکل ۱۵–۱۲، دو شبکه‌ی داخلی داریم که باید برای هرکدام یک access-list بنویسیم، وارد روتر می‌شویم و دستورات زیر را وارد می‌کنیم:

```
access-list 1 permit 192.168.1.0 0.0.0.255
access-list 1 permit 192.168.2.0 0.0.0.255
```

www.takbook.com

با دستور بالا، access-list شماره‌ی یک ایجاد شده است که ipهای invalid شبکه‌های داخلی را در خود قرار داده است.

در ادامه دستور زیر را وارد می‌کنیم:

ip nat inside source list 1 interface Serial0 overload

با تعریف دستور بالا، access-list با شماره‌ی 1 که ایجاد کرده‌ایم، انتخاب و روی اینترفیس Serial0 که به طرف شبکه‌ی خارجی است، فعال می‌کنیم و در آخر دستور از overload استفاده می‌کنیم که در زمان خروج، ip را به همراه یک پورت به بیرون ارسال می‌کند.

بعد از آن وارد اینترفیس‌های روتر می‌شویم و nat را فعال می‌کنیم:

Router(config)#**int FastEthernet 0/0**
Router(config-if)#**ip nat inside**

Router(config-if)#**int FastEthernet 0/1**
Router(config-if)#**ip nat inside**

برای interface Serial0/0 که به سمت شبکه‌ی خارجی است دستور زیر را وارد کنید:

Router(config)#**int Serial0/0**
Router(config-if)#**ip nat outside**

نحوه‌ی پاک کردن آدرس‌های موجود در جدول Nat:

Router#**clear ip nat translation ***

با این دستور، کل آدرس‌های موجود در جدول Nat حذف خواهد شد.

Router#**clear ip nat translations inside a.b.c.d outside e.f.g.h**

با این دستور یکی از رکوردهای ایجادشده از جدول Nat حذف خواهد شد، البته باید آدرس IP داخلی و خارجی را مشخص کنید.

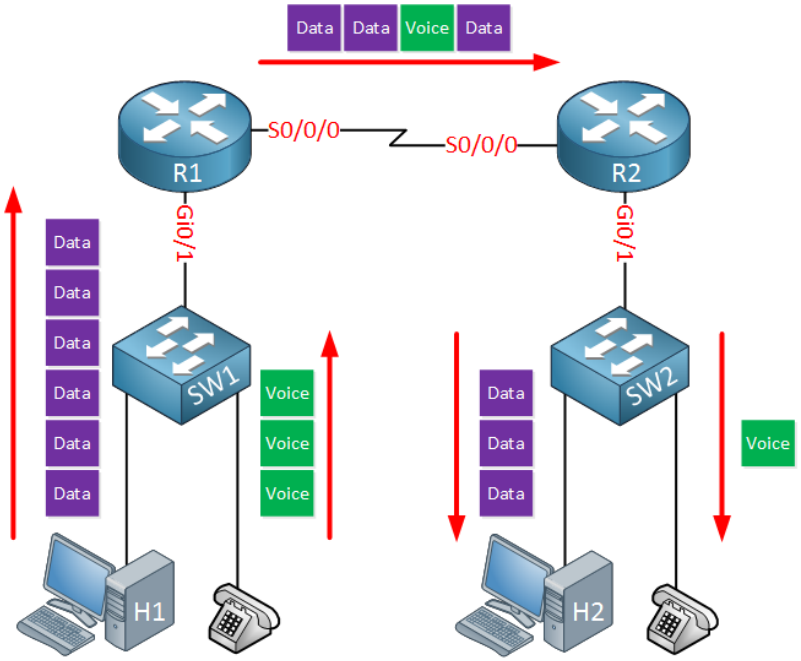
Quality of Service (QoS) ۱۲-۳

دستگاه‌های شبکه واقعاً به نوع ترافیکی که باید Forward کنند اهمیتی نمی‌دهند. سوئیچ شما یک Farme اترنت را دریافت می‌کند و به دنبال آدرس MAC مقصد می‌رود و قاب را به سمت مقصد هدایت می‌کند.

www.takbook.com

همین مورد در مورد روتر شما نیز صدق می‌کند ، یک بسته IP را دریافت می‌کند ، در جدول مسیریابی به دنبال مقصد می‌رود و بسته را به سمت مقصد هدایت می‌کند.

اصولاً روترها و سوئیچ‌ها به صورت یک صف FIFO (First In First Out) عمل می‌کنند و داده‌ها را به مقصد می‌فرستند، برای درک بهتر این موضوع می‌توانید به شکل ۱۶-۱۲ توجه کنید:



شکل ۱۶-۱۲ QOS

در شکل ۱۶-۱۲، یک شبکه کوچک با دو روتر، سوئیچ، کلاینت و دو دستگاه تلفن داریم، برای ارتباط بین این ادوات از پورت Gigabit Ethernet استفاده می‌کنیم به جزء بین دو روتر که از یک پورت سریال استفاده کردیم.

هنگامی که کلاینت و تلفن IP داده‌ها و بسته‌های صوتی را به مقصد خود برای کلاینت و تلفن دیگر ارسال می‌کنند، اما در هنگام ارسال در قسمت لینک سریال بین دو روتر دارای مشکل می‌شوند چون ظرفیت انتقال محدود است و اطلاعات در صف قرار می‌گیرند ولی این صف نامحدود نیست و روتر باید بسته‌های داده یا بسته‌های صوتی را رها (Drop) کند که اگر روتر بسته‌ی صوتی را رها کند طرف مقابل از کیفیت بد صدا شکایت خواهد کرد و یا اگر بسته‌های داده را رها کند کاربر دیگر شکایت خواهد کرد که سرعت انتقال کم است.

QOS یکی از ابزارها در سوئیچ و روتر است که می‌تواند این مشکلات را حل کند و نحوه‌ی برخورد با ترافیک را مشخص می‌کند، مثلاً روتر را طوری تنظیم کنیم که ترافیک صوتی را در اولویت قرار دهد تا صدا بد به کاربر مقصد نرسد.

www.takbook.com

یکی از بخش‌های مهم در شبکه quality Of Service است که برای ایجاد کیفیت بین دو شبکه و یا دو دستگاه مورد استفاده قرار می‌گیرد.

QOS را می‌توانیم به عنوان یک صف یاد کنیم، که در این صف پکت‌هایی وجود دارند که دارای ویژگی خاصی هستند و با اولویت‌هایی که برای آنها در نظر می‌گیرد می‌توانند در جلو یا عقب صف باشند.

QoS اندازه‌گیری کیفیت انتقال و در دسترس بودن سرویس یک شبکه (یا اینترنت) است.

در دسترس بودن خدمات، یک عنصر اساسی برای QoS است. قبل از اجرای موفقیت‌آمیز QoS ، زیرساخت شبکه باید بگونه‌ای طراحی شود که همیشه در دسترس باشد. هدف در دسترس بودن بالا ٪۹۹.۹۹۹ به موقع است.

چرا QoS برای شبکه‌های سازمانی مهم است؟

یک شبکه ارتباطی ستون فقرات هر سازمان موفق را تشکیل می‌دهد. این شبکه‌ها تعداد زیادی برنامه از جمله صدا بدون تاخیر، فیلم با کیفیت بالا و داده‌های حساس بدون تأخیر را انتقال می‌دهند. شبکه‌ها باید خدمات قابل پیش‌بینی، اندازه‌گیری و بعضاً، تضمین شده را برای مدیریت پهنای‌باند، تأخیر، jitter و پارامترهای Loss در یک شبکه، ارائه دهند.

فن‌آوری QoS به مجموعه ابزارها و تکنیک‌ها برای مدیریت منابع شبکه اشاره دارند و به عنوان فن‌آوری کلیدی برای همگرایی (convergence) شبکه در نظر گرفته می‌شوند. هدف QoS این است که همگرایی صدا ، فیلم و داده برای کاربران نهایی شفاف به نظر برسد. برنامه‌ها، Voice، ویدئو و داده‌های حساس ممکن است در شبکه از اولویت خاصی برخوردار شوند تا کیفیت آنها با مشکل روبرو نشود. بنابراین ، QoS یک عنصر مهم و اساسی برای همگرایی شبکه خوب و با کیفیت است.

ابزارهای QoS نه تنها در حفاظت از ترافیک مطلوب هستند بلکه در ارائه خدمات به ترافیک‌های نامطلوب مانند انتشار کرم‌ها نیز مفید هستند.

مدیریت پهنای باند، Delay، Jitter و Loss

سیسکو ابزارهای QoS بسیاری را هم در روتر و هم در سوئیچ‌هایش پیشنهاد می‌کند ، تمام آنها قدرت مدیریت چهار مشخصه‌ی اصلی از ترافیک شبکه را در اختیارتان قرار میدهند :

1. Bandwidth
2. Delay
3. Jitter
4. Loss

پهنای‌باند (Bandwidth)

www.takbook.com

پهنای‌باند یا همان Bandwidth به سرعت یک لینک (بر اساس Bit/s ، بیت بر ثانیه) اشاره می‌کند ، اما همینطور که ما به پهنای باند به عنوان یک سرعت نگاه می‌کنیم ، بهتر است که همچنین به پهنای باند به عنوان ظرفیت یک لینک هم نگاه کنیم. در شرایطی که مشخص می‌شود چه مقدار bit می‌تواند در ثانیه بروی یک لینک ارسال شود، ابزار Qos موجود در آن دستگاه، تحت شبکه مشخص می‌کند که پکت بعدی چه باشد و چه پکتی بعد از آن ارسال شود.

پس دستگاه برای اینکه چه پکتی در مرحله بعد به پهنای باند دسترسی پیدا می‌کند، و یا اینکه چه مقدار پهنای باند (ظرفیت) به هر نوع پکت داده می‌شود، آن را کنترل می‌کند. مثلا ممکن است بخواهید به ترافیک‌های مربوط به یک سرویسی که نیاز به سرعت بالا و عدم قطعی دارند پهنای باند بیشتری بدهید.

تاخیر (Delay)

دو حالت دارد، یا one-way (یکطرفه)، که زمان ارسال تا رسیدن یک پکت به مقصد است و یا round-trip، که مجموع زمانی که طول می‌کشد که بسته ارسال شود و از طرف مقصد هم دوباره بازگشت داده شود یعنی به زبان ساده به مقدار زمانی که طول می‌کشد تا یک پکت بین دو Host ارسال و دریافت شود را round-tripمی‌گویند. و این تاخیرها در بسیاری از جاها می‌تواند حیاتی و بسیار مهم باشد که در ادامه درمورد آن صحبت خواهیم کرد.

جیتر (Jitter)

به مقدار تغییرات ایجاد شده در One-way Delay بین پکت‌های متوالی یک بسته گفته می‌شود. برای درک بهتر، به عنوان نمونه فرض کنید که یک Application صدها پکت به یک مقصد خاص (یک Host) ارسال می‌کند، مقدار one-way delay در ارسال پکت اول ۳۰۰ میلی‌ثانیه، پکت بعدی هم همچنان ۳۰۰میلی‌ثانیه و پکت سوم هم به همین صورت الی آخر. در اینجا Jitter وجود ندارد ، چرا که مقدار one-way delayها یکسان بودند. اما به عنوان مثال اگر پکت اول با ۳۰۰ و دومی با ۳۱۰ و سومی با ۳۵۰ می‌رسید، می‌گفتیم که مقدار Jitter در میان پکت اول و دوم ۱۰ می‌باشد و یا اینکه مقدار Jitter در فاصله پکت دوم و سوم، 40 میلی‌ثانیه است.

www.takbook.com

Loss

به تعداد تعداد پکت‌های از دست‌رفته اشاره دارد. در یک مثال ساده ، فرض کنید که یک اپلیکیشن ۱۰۰ پکت را به سمت یک مقصد ارسال می‌کند و فقط ۹۸ درصد آنها به مقصد تحویل داده می‌شود، در این شرایط می‌گوییم که2%، Loss یا از دست‌رفتگی داشتیم. دلیل پیش‌آمدن Loss می‌تواند خیلی موارد باشد اما اکثرً مردم فکر می‌کنند که دلیل ایجاد Loss، کابل‌کشی بد و دارای نویز و یا اینکه سرویس WAN ضعیف می‌باشد، خب این می‌تواند یکی از دلایل ایجاد Loss باشد. به عنوان مثال اگر در حالت نرمال صف‌های یک Device تحت شبکه Full و پر شوند Loss بیشتری اتفاق می‌افتد ، چراکه دستگاه هیچ جای دیگری ندارد که پکت‌های جدید را قرار دهد، پس پکت‌ها را Discard می‌کند و Loss پیش می‌آید. تعدادی از ابزارهای QoS می‌توانند سیستم صف‌بندی را مدیریت کنند و به کنترل بسته‌ها کمک کنند و از پیش آمدن Loss جلوگیری کنند.

انواع ترافیک

با استفاده از QoS مهندس شبکه می‌تواند بسته به نیازه موجود، با توجه به میزان پهنای باند،Delay، Lossو Jitter ، هر نوع پکت را از نوع دیگری جدا کند.

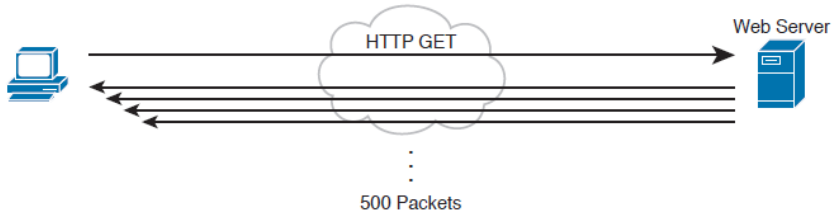
گاهی اوقات نیاز است که که این انتخاب را با توجه به نوع کار و Business خاصی انجام داد، به عنوان مثال نرم‌افزاره سرویس‌دهی مربوط به بانک مرکزی در ۳ نقطه (۳ سرور و Subnet) قرار داشته باشد، با QoS می‌توان در بین این ۳ نقطه ، پکت‌هایی که مربوط به این نرم افزار که در رفت و برگشت هستند را به آن‌ها سرویس‌های بهتر و قدرتمندتری در لینک ارتباطی آن نسبت به بقیه‌ی ترافیک‌ها داد (که همیشه از بابت سرویس‌دهی آن نرم‌افزار ، خیالمان راحت باشد که به عنوان مثال منابع یا مثلا پهنای‌باند، کم نیاورند) به هرحال در موقعیت‌های عادی دیگر، بحث سر این است که چگونه با توجه به طبیعت متفاوت انواع اپلیکیشن‌های مختلف، QoS را اعمال کنیم. برخی برنامه‌ها نیاز به تنظیمات QoS متفاوتی نسبت به بقیه دارند که در ادامه با برخی از تفاوت‌های ابتدایی بر اساس نیازهای هرنوع ترافیک برای QoS ، آشنا میشویم:

DATA Applications

www.takbook.com

در ابتدا یک نرم‌افزار ساده‌ی web application را در نظر بگیرید، با یک کاربر که از یک تبلت و یا یک PC استفاده می‌کند.

کاربر آدرس (URL) را وارد می‌کند تا درخواست یک صفحه‌ی تحت‌وب را ارسال کند. ممکن است فقط نیاز باشد که یک پکت به سمت وب‌سرور ارسال شود اما در پاسخ وب سرور به سمت کاربر ممکن است صدها ویا هزاران پکت ارسال شود (در تصویر زیر،این مثال به خوبی نمایش داده شده است).



شکل ۱۷-۱۲ HTTP Get

خب، تاثیر پهنای باند،delay، jitter و loss بروی این نرم‌افزار تحت‌وب تعاملی چیست؟

در ابتدا پکت‌ها نیاز به ظرفیت مشخصی از پهنای‌باند موجود دارند، از طرف دیگر درمورد delay هم هر کدام از آن بسته‌ها از سمت سرور به سمت کلاینت دارای مقداری one-way delay و همچنین مقداری jitter هستند.

از آن 500 پکتی که در شکل ۱۷-۱۲، نمایش داده شده است، اگر تعدادی از آنها به هر دلیلی از بین بروند، سرور دوباره آنها را ارسال می‌کند اما ممکن است دیگر یکسری از قسمت‌های صفحه‌ی وب مورد نظرما، به درستی نمایش داده نشوند.

درحالی که ابزارهای QoS برای مدیریت پهنای باند و موارد دیگه که در قبل گفته شد تمرکز دارند ، کاربر فقط به کیفیت کلی سرویسی که تجربه می‌کند اهمیت می‌دهد. برای مثال، فقط برایش مهم است که در یک web-application چقدر طول می‌کشد تا بعد از کلیک، چیزی که مدنظرش است را ببیند؟

در اینجور مواقع گفته می‌شود که کاربر به QoE یا Quality of Experience (کیفیت تجربه) اهمیت می‌دهد.

ابزارهای QoS به‌صورت مستقیم می‌توانند بروی jitter, delay, Bandwidth و loss اثر بگذراند و آنها را مدیریت کنند و بصورت کلی می‌بایستی با یکدیگر طوری تنظیم و ترکیب شوند که نتیجه‌ی خوبی بدهند تا بتوانند QoE کاربر را تحت تاثیر قرار دهند.

همچنین می‌توانید از ابزارهای QoS برای ترافیک‌های خیلی مهمتر، QoE بهتری ایجاد کنید ، برای مثال ممکن است برای یک اپلیکیشن خیلی ضروری و حیاتی، صف‌بندی QoS بهتری تدارک ببینید که با این کار، QoEکاربرانِ آن اپلیکیشن را تحت تاثیر قرار می‌دهد.

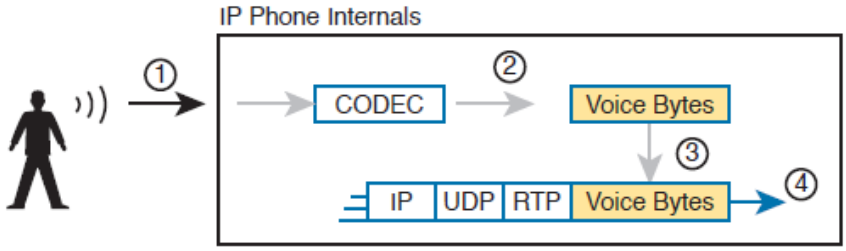
www.takbook.com

از طرف دیگر، یک نرم‌افزار غیرتعاملی (که به آنها batch traffic می‌گویند) مثل برنامه‌های بک‌آپ‌گیری داده‌ها و یا انتقال فایل، نیازمند پیشنیازهای QoS متفاوتی نسبت به اپلیکیشن‌های تعاملی هستند.

Batch Applicationها عموما با توجه به نوعشان داده‌ی بیشتری نسبت به اپلیکیشن‌های تعاملی می‌فرستند اما به دلیل اینکه آن‌طرف هیچکس منتظر نیست، پس مشخصاً مواردی مثل delay و jitterزیاد مهم نیستند. مخصوصاً برای آن نرم‌افزارهایی که وظایف طولانی و سنگینی دارند (مثل انتقال فایل). ابزارهای QoS در اینجا می‌توانند پهنای باند کافی را برای آن نوع ترافیک به صورت جداگانه و بر اساس نیازشان به ظرفیت، ارائه دهند و loss را مدیریت و از ارسال دوباره ی داده ها جلوگیری کنند.

Video and Voice Applications

قبل از هرچیز ، بیایید با مفهومی بنام Flow آشنا شویم. در تعریف ساده می‌توان گفت که به تمام داده‌هایی که در بستر شبکه از یک Application به Application دیگری ارسال می‌شوند، flow می‌گویند. حالا به‌صورت دقیق درمورد Voice در بستر ip (همان VoIP) می‌خواهیم صحبت کنیم، تعریف ساده‌ی VoIP بدین صورت است که صدایی را از طریق تلفن خود تولید و در داخل پکت‌های IP قرار داده و در بستر شبکه به تلفن دیگری ارسال می‌کنید و آن تلفن هم آن صدا را پخش می‌کند (دقیقا مثل تلفن صحبت کردن عادی که در روزمره با آن سروکار داریم، اما اینجا به‌جای خط تلفن، صدا از طریق بستر شبکه انتقال پیدا می‌کند) شکل ۱۲-۸، مواردی که در بالا گفتیم را به صورت مرحله به مرحله نشان می‌دهد:



شکل ۱۲-۱۸ بررسی QOS

۱. کاربر یک تماس برقرار می‌کند و شروع به صحبت کردن می‌کند.
۲. یک chip با نام (codec processes) همان (Digitizes) صدارا به باینری تبدیل کرده و طبق بازه‌ی زمانی آن‌را آماده می‌کند.
۳. تلفن، داده را در IP Packetها قرار می‌دهد.
۴. تلفن پکت را به سمت IP مقصد ارسال می‌کند.

اگر کمی از ریاضی استفاده کنید، می‌بینیم که یک تماس با استفاده از G.711 Codec نیاز به 80kb/s پهنای باند دارد (بدون در نظر گرفتن هدر Data link و trailer overhead)، با جمع زدن هدرها و Payloadهای

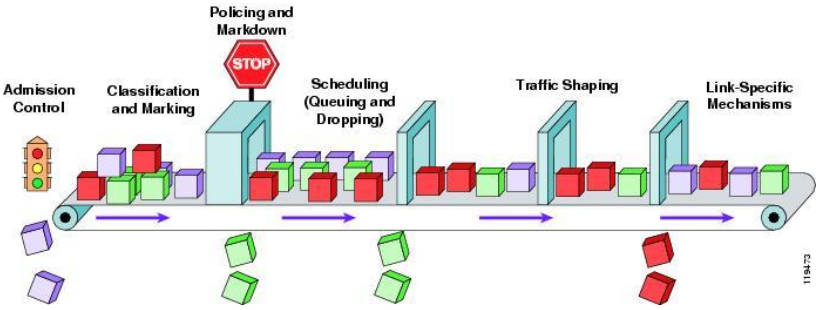
www.takbook.com

مربوط به VoIP (که در تصویر نشان داده شده) ، هر پکت 200 بایت حجم دارد که هرکدام ۲۰ میلی‌ثانیه نگه داشته می‌شوند، پس در مجموع تلفن، هر ثانیه 50 پکت ارسال می‌کند و از آن طرف هر کدام از آن، 50 تا 200 بایت حجم دارد ، پس حدود ۱۰۰۰۰بایت (۸۰۰۰۰ بیت) در ثانیه ارسال می‌شود (که می‌شود 80kb/s). پس می‌توان به راحتی به این نتیجه رسید که VoIP یا یک Flow، نیاز زیادی به پهنای باند قدرتمند ندارد اما با توجه به شدت تعاملی بودنش، نیاز به کیفیت بسیارخوب و قابل توجه‌ی در jitter, delay و loss دارد.

در این بخش دسته‌بندی‌های اصلی مجموعه ابزار Cisco QoS توضیح داده شده و موضوعات زیر را در بر می‌گیرد:

- ابزار طبقه‌بندی و مارک‌گذاری (Classification and Marking tools)
- Policing and Markdown tools
- ابزارهای برنامه‌ریزی (Scheduling tools)
- ابزارهای مربوط به لینک (Link-specific tools)
- ابزارهای AutoQoS
- Call Admission Control tools

سیسکو مجموعه‌ای کامل از ویژگی‌ها و راه‌حل‌های QoS را برای رفع نیازهای متنوع صدا ، فیلم و برنامه‌های مختلف فراهم می‌کند. فناوری Cisco QoS به شما این امکان را می‌دهد که شبکه‌های پیچیده را کنترل کرده و به طرز قابل قبولیف انواع برنامه‌های شبکه و انواع ترافیک را پیش‌بینی کنید. شما می‌توانید با استفاده از این سازوکارها پهنای‌باند، تاخیر، Jitter و Loss را کنترل کنید، در شکل ۱۹-۱۲، یک نمای کلی از ایجاد QOS در سازمان‌ها را مشاهده می‌کنید.



شکل ۱۹-۱۲ نمای کلی QOS

www.takbook.com

۱-۳-۱۲ بررسی CLASSIFICATION AND MARKING

اولین کاری که باید در QOS انجام شود شناسایی ترافیک عبوری است که طبق آن ترافیک باید سیاست‌های کاری خود را روی آن فعال کنیم، بعد از طبقه‌بندی، ابزارهای marking می‌توانند ویژگی‌های یک frame را به یک مقدار جدید تغییر دهند.

می‌توان به زبان ساده‌تر گفت که Marking(علامت گذاری) نوعی ابزار QoS است که پکت‌ها را بر اساس محتوای هدرهای آنها دسته‌بندی (Classification) می‌کند و سپس با استفاده از تغییر دادن تعدادی از بیت‌ها در یکسری فیلدهای خاص در هدرها ، پیغام‌ها را علامت‌گذاری می‌کند .

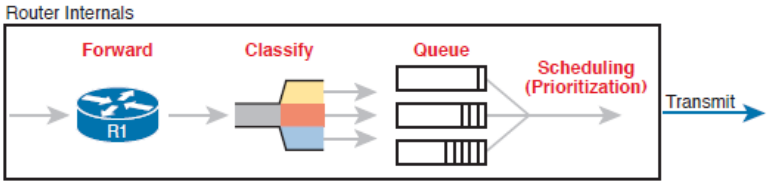
مفاهیمClassification

ابزار QoS دقیقا روی مسیری که پکت‌ها از طریق آن Forward می‌شوند (از طریق یک روتر یا یک سوئیچ) می‌نشیند، **مانند ACL ها**! QoS برروی یک Interface فعال می‌شود و همچنین مانند ACL ها QoS برای یک جهت خاص (بسته‌های ورودی/ بسته‌های خروجی) فعال می‌شوند (مثلا زمانی که بسته درحال خروج از یک Interface است و یا درحال ورود از طریق یک Interface ، مواردی که مدنظرش است را اعمال می‌کند).
قوانین Classification به پروسه‌ی Matchingدر فیلدها اشاره دارد، تا بتواند بر اساس آنها تعیین کند که QoSچه عملکردی باید نشان دهد.
پس بیاید دوباره QoS را با ACL ها مقایسه کنیم:

اکسس‌لیست‌ها یا همانACL ها، دسته بندی (Classification) و Filtering را انجام می‌دهند و هدرهای پکت ها را تطابق می‌دهند و می‌توانند تصمیم بگیرند که چه بازخوردی و actionی برای هر Packet داشته باشند(allow و یا discard)؛ ابزار QoS هم Classification (دسته‌بندی پکت ها را) با Match کردن فیلدهای هدرها انجام می‌دهد و تصمیم می‌گیرد که چه نوع بازخوردی برای QoS داشته باشد (بعدا درمورد این بازخورد ها صحبت خواهیم کرد، مثل queuing، shaping، policing و ...) برای مثال به فرایند Proccessing انجام شده در روتر که در تصویر ۲۰ -۱۲، مشخص شده توجه کنید.

در این حالت یک ابزار صف‌بندی خروجی برروی یک Interface فعال شده است، روترها از ابزار صف‌بندی (Queuing tool) استفاده می‌کنند تا تعدادی از پکت‌ها را در یک صف خروجی قرار دهند و دیگر پکت‌ها را در صف‌های دیگر و به همین صورت الی آخر تا زمانی که Interface و یا Inteface‌های خروجی کاملاً مشغول و درحال ارسال داده باشد(Busy) ، سپس وقتی یک Interface در دسترس قرار گرفت و به‌قول معرف سرش خلوت شد، الگوریتم زمان‌بندیِ ابزارِ صف‌بندی می‌تواند هر پیغام و هر پکت دلخواهی را که می‌خواهد از هر صفی بردارد و یا ترافیک‌ها را بر اساس قوانینی که **مهندس شبکه** برایش تعریف کرده است اولیت‌بندی کند.

www.takbook.com



شکل ۲۰-۱۲ *Classification*

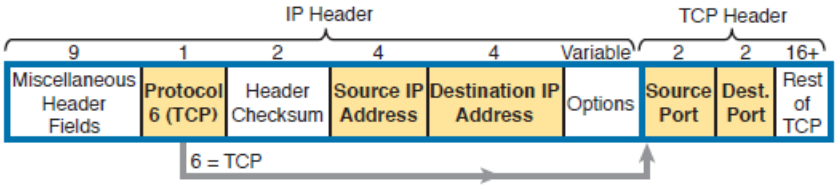
۱. در ابتدا روتر تصمیم به مسیریابی می‌گیرد. (که انجام بدهم یا ندهم).
۲. ابزار صف‌بندی خروجی با استفاده از منطقه classification تصمیم می‌گیرد و تعیین می‌کند که پکتی در کدام صف قرار بگیرد.
۳. روتر بسته‌ها را در صف خروجی پکت‌های درحال خروج نگه می‌دارد تا زمانی که interface برای ارسال بسته‌ی بعدی در دسترس قرار بگیرد.
٤. منطقه زمان بندی ابزار صف‌بندی (queuing tool's scheduling logic) پکت بعدی را انتخاب می‌کند و بصورت بسیار موثری هر بسته را نسبت به بقیه‌ی بسته‌ها اولیت‌بندی می‌کند.

در انتها برای جمع‌بندی نهایی می‌توانید به این صورت نتیجه‌گیری کنیم که ابزار QoS می‌آید در مرحله‌ی اول انواع داده‌ها و بسته‌ها را با استفاده از Marking علامت و برچسب‌گذاری می‌کند و سپس هر نوع داده رو دسته‌بندی کرده و در دسته و یا Class خودش قرار می‌دهد.

در آینده با ابزارهایی آشنا می‌شویم که می‌آیند با توجه به دسته‌بندی‌ها و برچسب‌ها بسته‌ها را اولویت و صف‌بندی می‌کنند و ممکن است به بعضی از آنها پهنای باند بیشتر ویا کمتر بدهند.

همان‌طور که تا الان مشاهده کردید، QoS بسیار شبیه به ACL ها است چراکه عملکرد کاملا مشابهی دارد، به این صورت که شما می‌گویید اگر پکتی با ACL شما match شد، بیاید یک بازخورد (action) خاصی انجام دهد (مثلا Permit کند) و در Qos هم می‌گویید که اگر بسته با موارد پیاده‌سازی شده در Qosتطابق داشت و Match شد، بیاید و فلان بازخورد QoS را انجام بدهد .

در تصویر ۲۱-۱۲، هدر IP و TCP مشاهده می‌شود که در آن تمام فیلدهایی که قابل تطابق (matchable) هستند مشخص شده است .



شکل ۲۱-۱۲ هدر *IP* و *TCP*

حالا به این نکته توجه کنید که ممکن است مهندس شبکه بخواهد بسته‌های لایه‌ی 7 (Application) را هم از یکدیگر جدا و دسته‌بندی کند، مثلا بخواهد به دو نرم‌افزاری که برای بحث Video در شبکه از آن

www.takbook.com

استفاده می‌شود، به هر کدام منابع و QoS Action متفاوتی بدهد. برای بررسی این بسته‌ها در این لایه و دسته‌بندی کردن آنها راه‌کاری که ما پیش‌رو داریم استفاده از NBAR یا همان Network Based Application Recognition می‌باشد NBAR . به راحتی می‌تواند بسته‌ها را دسته‌بندی کند و درClass های متفاوت قرار دهد و در انتها می‌توان آنها را مثل موارد قبل اولیت‌بندی و محدودسازی منابع را برایشان انجام داد.

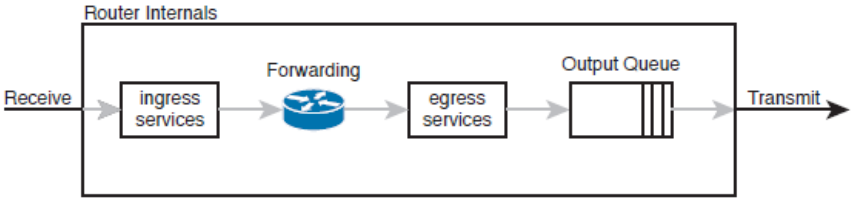
پیاده‌سازی NBAR بسیار ساده بوده و اگر به عنوان مثال بخواهید پکت‌های مربوط به دوربین‌های امنیتی داخل شرکت را از بسته های مربوط به Skype جدا کنید، عدم استفاده از NBAR کارمان را بسیار سخت و پیچیده خواهد کرد.

۱۲-۳-۲ بررسی Queuing و Congestion Management

تمامیDeviceهای تحت شبکه از صف‌بندی (Queuing) استفاده می‌کنند، بدین صورت که دستگاه پیغام را می‌گیرد، برای Forward کردنش تصمیم می‌گیرد و سپس پیغام را ارسال می‌کند ، اما بعضی اوقات Interfaceخروجی مشغول و زیر بار می‌باشد و در دسترس نیست، پس دستگاه پیغام‌های خروجی را در یک صف نگهداری می‌کند تا به محض اینکه Interface در دسترس قرار بگیرد آن‌را ارسال کنند.

سیستم Congestion Management (مدیریت تراکم) به ابزاری در QoS که برای مدیریت صف‌هایی است که پکت‌ها را نگهداری می‌کنند تا زمانی که مسیر خروجی برای آنها باز شود (یا اینکه منابع مورد نیاز آنها در روتر آزاد شود)، اشاره می‌کند؛ اما بحث مدیریت تراکم، یک چیزی فراتر از یک ایده‌ی ساده است که برای بهتر متوجه شدن آن و فهمیدن اینکه چطور کار می‌کند، می‌بایستی به فرآیندهایی که در داخل Device انجام می‌شود نگاه کنید.

برای مثال، تصویر ۲۲-۱۲، که نمایش دهنده‌ی فرآیندهای داخلی یک روتر است را در نظر بگیرید. روتر تصمیم مربوط به Forwarding را می‌گیرد و سپس بسته‌ها را برای قرار گرفتن در صف‌ها آماده می‌کند تا به محض اینکه خروجی در دسترس قرار بگیرد عمل انتقال را انجام دهد. آن طرف بصورت همزمان با این فرآیندها ، روتر ممکن است کارهای دیگری هم انجام دهد. مثل Ingress NAT (ترجمه آدرس داخلی در سمت Interface ورودی) ، Ingress ACL ویا Egress ACL (خروجی) بعد اینکه تصمیم مربوط به Forwarding گرفته شد، و همینطور الی آخر.

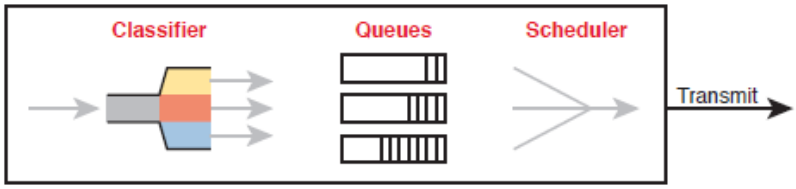


شکل ۲۲-۱۲ هدر IP و TCP

در سیستم مدیریت تراکم شما می‌توانید صف‌های متعددی برای منظورهای مختلف داشته باشید. به عنوان مثال در شکل ۲۲-۱۲، فقط یک صف خروجی ایجاد شده است و از الگوریتم زمان بندی FIFO (مخفف First IN First OUT است، یعنی بسته‌ها به همان ترتیبی که وارد صف می‌شوند ، به همان ترتیب

www.takbook.com

خارج می‌گردند) استفاده می‌شود. اکثر دستگاه‌های تحت شبکه می‌توانند سیستم مدیریت صف با قابلیت پشتیبانی از چندین صف را داشته باشند. برای استفاده از چند صف می‌بایستی پکت‌ها دسته‌بندی و علامت‌گذاری شوند که بتوان مشخص کرد هر بسته در کدام صف می‌بایستی قرار بگیرد. سیستم صف‌بندی نیاز به یک Scheduler هم دارد که مشخص کند در زمان در دسترس قرار گرفتن خروجی، کدام پیغام می‌بایستی ارسال شود.



شکل ۲۳-۱۲ سیستم صف‌بندی

جذاب‌ترین قسمت سیستم صف‌بندی، همین بحث scheduler می‌باشد. با استفاده از scheduler شما می‌توانید prioritization یا همان اولیت‌بندی انجام بدهید و مشخص کنید در زمان در دسترس قرار گرفتن خروجی، چه مواردی اولویت بیشتر و یا کمتری دارند.

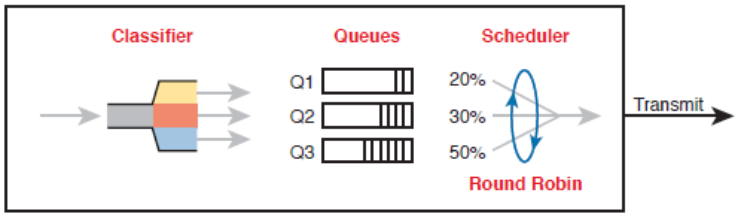
الگوریتم زمانبندی Round Robin : یکی از الگوریتم‌های زمان‌بندی‌ای است که توسط سوئیچ‌ها و روترهای سیسکو استفاده می‌شود. اصولا Round Robin، دوره‌ای را به ترتیب در هر یک از صف‌ها طی می‌کند. در هر دوره به عنوان مثال یک پیام و یا تعداد مشخص‌شده‌ای از بایت‌ها را انتخاب و ارسال می‌کند و به سراغ صف بعدی می‌رود.

یعنی به این صورت که به عنوان مثال تعدادی بایت از صف اول برمی‌دارد و ارسال می‌کند، تعدادی از بایت‌های صف دوم و همچنین تعدادی از بایت‌های صف سوم الی آخر؛ سپس دوباره از اول شروع می‌کند و این پروسه را تا زمانی ادامه می‌دهد که انتقال موارد داخل صف‌ها کاملا انجام شود.

الگوریتم Round Robin همچنین از مفهومی به نام weighting استفاده می‌کند (که عموما با نام weighted round robin شناخته می‌شود). این مفهوم بدین صورت عمل می‌کند که اجازه می‌دهد میزان بایت(هایی) که از صف‌های مختلف برداشته می‌شود، برابر نباشند و به یکسری صف‌ها ، ترجیح و اولویت بیشتری نسبت به بقیه صف‌ها داده شود. به عنوان مثال ، روترها از ابزار محبوبی با نام Class-Based Weighted Fair Queuing ـ (CBWFQ) استفاده می‌کنند تا برای هر دسته‌بندی (Class) ، حداقل پهنای‌باند لازم را فراهم کنند، با پیکربندی این ابزار، در زمان شلوغی، در هر صورتی به دسته بندی مورد نظر حداقل میزان پهنای باند مشخص شده اختصاص داده می‌شود.(ممکن است میزان پهنای باند مصرفی از مقدار مشخص شده بیشتر بشود ، اما کمتر از آن نمی‌شود).

www.takbook.com

ابزار CBWFQ عملاً به مهندسین شبکه اجازه می‌دهد که میزان درصد (٪) مورد نظر خود را از پهنای باند، به هر کلاس اختصاص بدهند. به عنوان مثال همان‌طور که در شکل ۲۴-۱۲، می‌بینید ، الگوریتم Round Robin ۲۰٪ از پهنای‌باند را برای صف اول اختصاص داده است (یعنی یکجورایی قول داده است که از کل پهنای باند موجود ، ۲۰٪اش مختص به این صف می‌باشد،حتی در زمان‌های شلوغی) و ۳۰٪ و ۵۰٪ را به صف دوم و سوم. و بدین صورت داده‌ها را انتقال می‌دهد.



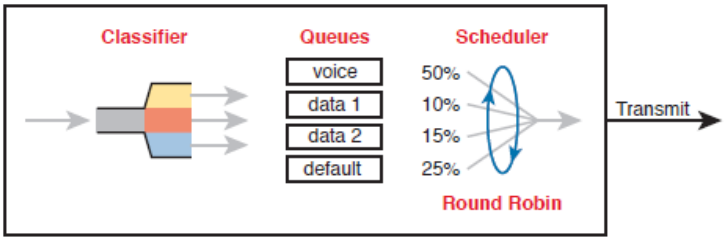
شکل ۲۴-۱۲ الگوریتم Round Robin

.

Low Latency Queuing

در قسمت‌های قبلی کتاب در مورد "Voice and Video Applications" صحبت کردیم که چرا داده‌های ویدئویی و صدا نیاز به Low Latency و زمان تاخیرکم (زمان Delay کم ، Jitter کم ، Loss کم) دارند. متاسفانه الگوریتم Round Robin به تنهایی پیشنهادهای مورد نیاز برای انتقال صدا و تصویر را فراهم نمی‌کند (زمان Delay کم ، Jitter کم، Loss کم) و راهکار ما اضافه کردن LLQ یا همان Low Latency Queuing به زمان‌بند (Scheduler) است.

سیستم Round Robin، تاخیر بسیار زیادی برای بسته‌های Voice (صدا) بهمراه دارد ، برای اینکه متوجه بشوید، تصور کنید که یک پکت Voice از راه می‌رسد و مسیریابی می‌شود که از طریق فلان interface با سیستم صف‌بندی مشخص شده در تصویر ۲۵-۱۲، ارسال شود.



شکل ۲۵-۱۲ الگوریتم Round Robin

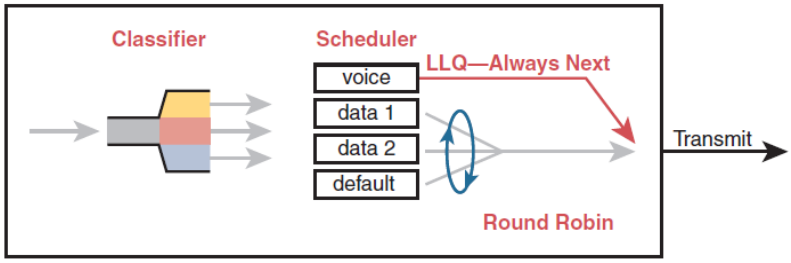
حالا بسته Voice بعدی از راه می‌رسد، همزمان با اینکه RR به سراغ صف دوم (data1) رفته است! حتی با اینکه ۵۰٪ از پهنای باند به صف Voice اختصاص داده شده است ، اما Round Robin تا زمانی که ۳ صف بعدی را پردازش نکند ، آن پکت Voice را ارسال نمی‌کند ، و این موضوع باعث Delay و Jitter می‌شود.

www.takbook.com

راه حل ما که LLQ می‌باشد، می‌آید و به scheduler می‌گوید که برای یکی یا دوتا صف خاص پارتی‌بازی کند و بسته‌هایی را که از راه می‌رسند، بدون معطلی ارسال کند. به این صف‌ها special priority queues گفته می‌شود.

مشکل حل شدJitter ! و Delay بسیار کم می‌شود.

تصویر ۲۶-۱۲، این منطق را به خوبی شرح می‌دهد:



شکل ۲۶-۱۲ الگوریتم Round Robin

ساختار LLQ میزان Delay و Jitter بسیار کم را برای ترافیک فراهم می‌کند ، اما یک مشکلی اینجا وجود دارد ، به تصویر قبل دقت کنید!

فرض کنید که لینک خروجی ما دارای سرعت X بیت در ثانیه است و میزان پکت‌های ارسال voice ، از X بیشتر باشند ! RR هیچوقت نمی‌تواند به صف‌های دیگر هم رسیدگی کند (به این حالت queue starvationیا گرسنگی گفته می‌شود).

۳-۳-۱۲ بررسی Policing & Shaping

در این بخش قرار است که درمورد ۲ راهکار (یا ابزار) QoS صحبت کنیم، این دو مورد یعنی Policing و Shaping یک مقدار هستند در جاهای خاص‌تری استفاده می‌شوند و معمولا در بخش‌های معمولی یک شبکه‌ی عادی دیده نمی‌شوند. این دو، بیشتر در لبه WAN یا همان WAN Edge استفاده می‌شوند.

هر دو سرعت یا همان Rate بیتها و داده‌هایی را که درحال عبور از Device هستند را مانیتور و اندازه‌گیری می‌کنند. یعنی به محض فعال‌سازی آنها، Policer و یا Shaper، سرعت هر پکتی که عبور می‌کند را شمارش و برای خود اندازه‌گیری می‌کنند و هردو تلاش می‌کنند که این سرعت انتقال را (bit rate) کمتر از میزان مشخص شده (پیکربندی شده) و یا به همان میزان پیکربندی شده برسانند و اجازه ندهند که از مقدار مشخص شده بیشتر شود؛ اما بازخورد (Action) یا بهتر است بگوییم روش هر کدام در برابر این موارد متفاوت است، Policer پکت‌هارا discard می‌کند ویا آن‌را remark می‌کند (که این موضوع را در ادامه توضیح می‌دهیم) و shaper پکت‌ها را نگه می‌دارد و در صف‌های تعریف شده قرار می‌دهد (تاخیر ایجاد می‌کند و باعث Delay می‌شود.) در ادامه با هرکدام بصورت کامل‌تر آشنا خواهیم شد.

Policing

www.takbook.com

بصورت کلی اگر بخواهیم بگوییم که Policing دقیقا چه کاری انجام می‌دهد ، بدین صورت است که بروی سرعت ترافیک تمرکز می‌کند و سپس آن‌را با میزان سرعت مشخص شده در Policer مقایسه می‌کند و درصورت عبور این مقدار از حد مجاز، بسته‌های درحال عبور اضافی را دور می‌اندازد (Discard می‌کند). ترافیک با سرعت و حالات متفاوت و گوناگون به deviceها می‌رسد، اگر بخواهید گراف و یا نموداری از bit rate داده‌های ورودی و یا خروجی ایجاد کنید ،نتیجه‌ی شما یک چیزی شبیه گرافه سمت چپ در شکل ۱۲-۲۷، می‌شود (که Policer نموداری مشابه آن‌را از روی داده‌های درحال عبور برای خود ترسیم می‌کند). خط افقی مشخص شده با رنگ آبی، میزان policing rate پیکربندی شده(کانفیگ شده) را نمایش می‌دهد.

شکل ۲۷-۱۲ بررسی Policing

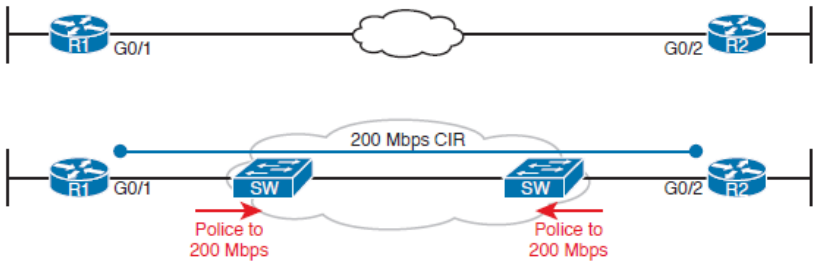
نمودار سمت راست شکل ۲۷-۱۲، نشان می‌دهد که چه اتفاقی می‌افتد اگر Policer تصمیم به اعمال actionو discard کردن پکت‌هایی که از میزان مشخص شده عبور کرده‌اند بگیرد. داده‌هایی که بالای خط افقی را به راحتی می‌بُرَّد.

نمودار سمت راست ، همچنین یک نمونه از اجازهی رخ دادن یک burst (انفجار، شلیک) از ترافیک را نشان می‌دهد. Policer هر از چندگاهی بعد از کم شدن activity یا همان فعالیت، اجازهی یک burst (عبور از میزان مشخص شده) را برای یک زمان کوتاه می‌دهد.

چه زمانی می‌بایست از Policing استفاده کنیم؟

حالا که مقداری با مفاهیم Policing آشنا شدید ، ممکن است برای شما سوال پیش آمده باشد که چطور با discard کردن و از بین بردن پکت‌ها می‌توانیم کیفیت بهتر و QoS در شبکه داشته باشیم و اصلا این Policing به چه دردی می‌خوره؟ چرا که به‌نظر می‌آید بیشتر به شبکه لطمه می‌زنیم و با action هایی که انجام می‌شود، باعث می‌شود که بعضاً پکت‌ها از بین بروند و دوباره ساخته و ارسال شوند، این مورد چگونه به بهتر شدن پهنای‌باند، jitter و delay کمک می‌کند؟ Policing فقط در شرایط خاصی مفید واقع می‌شود، به عنوان مثال در نظر بگیرید که اتصاله شبکهی دو شعبه از کمپانی خود را به‌صورت Point to Pointبر روی بستر MetroEthernet (اتصال WAN بین ۲ روتر لبه شعب شما) فراهم کرده‌اید (شکل ۲۸-۱۲)

www.takbook.com



شکل ۲۸-۱۲ بررسی Policing

عموماً مهندسین شبکه داخل سازمان شما، این ارتباط مابین را به‌صورت یک ابر(Cloud) می‌بینند و به جزئیات آن کاری ندارند که چگونه ارتباطشان بر این بستر فراهم می‌گردد و شبکه را به این صورت در نظر می‌گیرند که انگار دو روتر مستقیماً با استفاده از لینک‌های Ethernet بهم متصل شده‌اند.

حالا از سمت Service Provider ، به قراردادی که این بستر را فراهم کرده است نگاه کنیم. در اینجا ارتباط از طریق یک پورت Gig و CIR (سرعتی که بر روی آن توافق شده و برای آن هزینه پرداخت می‌شود) ۲۰۰ Mgps فراهم شده است که SP آن‌را به تمام مسیرهای خریداری شده اختصاص می‌دهد.

برای یک لحظه فکر کنید که SP با توجه به ده‌ها و صدها مشتری‌ای که دارد و حتی با توجه به اینکه CIRای تعیین شده است، به تمامی آنها اجازهی عبور دیتا به اندازه‌ی پهنای باند قابل پشتیبانی توسط لینک ارتباطی(به عنوان مثال در اینجا ۱۰۰۰mgps یا همان ۱Gbps) را بدهد! این میزان ترافیک زیاد، می‌تواند به راحتی باعث congestion در شبکه و کلی بار ترافیکی زیاد و در نهایت خوابیدن شبکه SP شود.

همچنین ممکن است تعدادی از مشتریان به خود بگویند که SP به هرحال داده ما را انتقال می‌دهد، پس تصمیم به پرداخت به میزان CIR بسیار پایینتری می‌گیرند، گرچه در این شرایط، خوب و بد با هم می‌سوزند و حتی مشتریان خوبی هم که از این شرایط سوء استفاده نمی‌کنند، به همان میزان مشتریان دیگر از مشکل شبکه‌ی SP ، ضرر می‌کنند.

تصویر ما به راحتی راهکار و راه حل این مشکل را هم نمایش می‌دهد ، و آن این است که که SP داده‌های ورودی از سمت شرکت ما را بر اساس CIR مشخص شده و پرداخت شده از سمت مشتری Policeمی‌کند و با اینکار از تمامی مشتریان خود در برابر بازخورد منفی ارسال بیش از حد دیتا از سمت مشتری و یا مشتریان دیگر جلوگیری می‌کند و به هر مشتری ، دقیقا همان میزان پهنای باند و سرعت توافق شده را ارائه می‌دهد.

سیستم Policer همچنین می‌تواند یک action دیگری هم انجام دهد و بسته‌ها را remark کند. بگذارید به این صورت بگوییم که در این سناریوی SP می‌تواند به نحوی به مشتریان خود یک راه‌کار بهتر ارائه بدهد

www.takbook.com

(بجای اینکه پکت هارا از بین ببرد) و همچنین از شبکه ی خودش محافظت کند، پس از یک استراتژی جدید استفاده می‌کند:

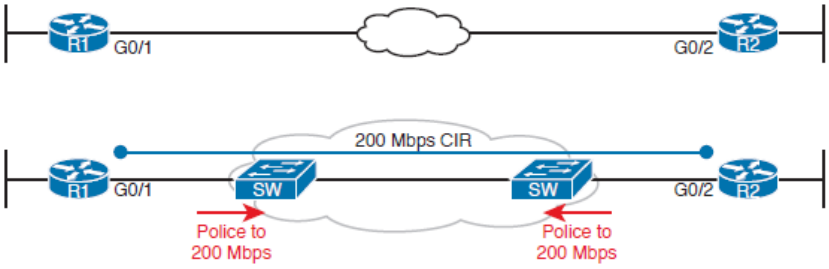
بسته هایی که از میزان مشخص و پیکربنده شده عبور می‌کنند را علامت‌گذاری می‌کند و اجازه می‌دهد آنها وارد شبکه SP شوند.

اگر دیوایس‌های دیگر SP ، سرشان خلوت نبود و زیر باره ترافیکی سنگینی بودند، این بسته‌های علامت‌گذاری شده می‌توانند discard شوند.

در غیر این صورت، یعنی اگر دیوایس‌ها زیر بار سنگینی نبودند و از پس پردازش این پکت‌ها برمی‌آمدند، اجازه‌ی پردازش و عبور این پکت‌ها داده می‌شود.

با این استراتژی، SP قادر است سرویس بهتری را به مشتریان خود ارائه دهد و میزان داده‌ی کمتری را از بین ببرد و همچنین از شبکه خود محافظت کند.

شما یک لینک ۱ گیگابیت از روتر خودتون به سمت Service Provider دارید ، اما با CIR ۲۰۰ Mb/s که شکل ۲۹-۱۲ را مشاهده می‌کنید:



شکل ۲۹-۱۲ بررسی Policing

Service Provider به شما اعلام کرده است که هرزمان، میزان بسته‌های ورودی سمت شما به SP، از میزان مشخص‌شده (CIR) بیشتر شود ، تمامی بسته‌های اضافی را Discard می‌کند. راه‌کاری که ما می‌بایستی برای خود داشته باشیم چیست؟

از یک Shaper استفاده می‌کنیم تا سرعت ترافیک را پایین بیاوریم، به عنوان مثال در این سناریو آن را از ۱ گیگ به ۲۰۰مگابیت (200Mg/ps Shaping Rate) کاهش می‌دهیم.

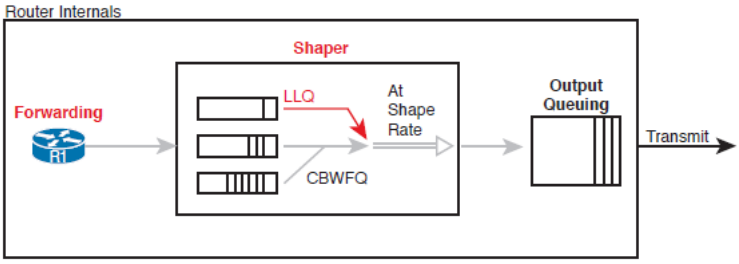
این سناریو (Shaping داده‌ها قبل از ارسال به سمت ISPی که Policing انجام می‌دهد) یکی از استفاده‌های عامیانه‌ی Shaperها است.

Shaperها در شرایط و جاهای دیگری هم می‌توانند مفید واقع شوند ولی بصورت کلی، Shaperها وقتی کاربرد دارند که یک نفعی از کاهش سرعت وجود داشته باشد ، مثل شرایط فعلی در این سناریو، که اگر کمپانی نیاز به سرعت و پهنای‌باند بیشتری داشته باشد ، می‌بایستی هزینه‌ی بیشتری پرداخت کند.

www.takbook.com

Shaper با استفاده از صف‌بندی کردن بسته‌ها (Queuing) سرعت را پایین می‌اورد و سپس یکی یکی به آنها سرویس می‌دهد، اما نه بر اساس در دسترس قرار گرفتنه Interface خروجی، بلکه خود Shaper برای خود بسته‌ها را بر اساس Shaping Rate مشخص شده schedule می‌کند.

پس باید متوجه شده باشید که بحث صف‌بندی انتهایی که بر اساس در دسترس قرار گرفتن Interface انجام می‌شود مرحله‌ی بعد از این موارد می‌باشد و وقتی توسط Shaper، بسته‌ها Shape شدند و قوانین لازمه روی آنها اعمال شد (که از میزان مشخص شده ی Shaping rate عبور نکرده باشند) سپس به سمت مرحله‌ی بعد یعنی Queuingهایی می‌روند (درصورتی که لازم باشند و وجود داشته باشند).



شکل ۳۰-۱۲ بررسی Shaper

بخاطر داشته باشید که ممکن است گاهی اصلا نیاز به صف‌بندی خروجی (همان صف‌بندی(Queuing) نهایی) نباشد.

چراکه برای مثال در این سناریو که مطرح شد، SP بر روی بسته‌های ورودی Policing را اعمال می‌کند و از آن طرف شما هم بر روی تمامی ترافیک خود Shaping را اعمال می‌کنید و لینکتان هم که 1 gb/ps می‌باشد، صف‌های نهایی ممکن است هیچوقت پر نشوند!

Shaperها جایی صف‌هایشان را قرار می‌دهند که شما می‌توانید بر روی آنها از ابزارهای مدیریت Congestion management هم بهره ببرید.کاملا منطقی است که شما از مواردی مانند LLQ ، CBWFQو... را روی این صف‌ها پیاده‌سازی کنید(مانند مثال تصویر ۳۰-۱۲).

تنظیم یک Shaping Time Interval (وقفه زمانی) مناسب برای داده های Voice و Video

مشکل راهکار Shaping این است که با پایین آوردن سرعت Packetها ، باعث ایجاد Delay و احتمالا Jitter بیشتر خواهد شد، چرا که ذات Shaper این است که سرعت را پایین بیاورد.

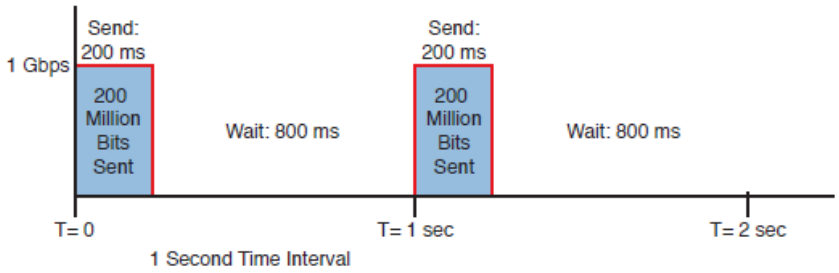
اما شما می‌توانید تنظیمات خاصی را پیکربندی کنید تا روند داخلی Shaper را تغییر دهید، تا بتوانید Delay و Jitter ایجاد شده برای ترافیک‌های Video و Voice را پایین بیاورید.

Time Interval یک Shaper به منطق داخلی و اینکه چگونه Shaper میزان داده را محاسبه و میانگین‌گیری کرده و در یک زمان خاص و یک سرعت خاص ارسال می‌کند ، اشاره دارد. حالا این به چه معناست ؟

www.takbook.com

یک Shaper اصولا به این صورت کار می‌کند که داده را با تمام سرعتی که می‌تواند ارسال می‌کند و سپس دست نگه می‌دارد ... ارسال می‌کند و دست نگه می‌دارد ... ارسال می‌کند و دست نگه می‌دارد. برای مثال در سناریوی فعلی، Shaping، 200Mg/ps بر روی یک روتری که در اینجا دارای Interface، 1Gb/ps است، پیشهاد می‌شود (چرا که CIR ما ۲۰۰ می‌باشد)؛ در اینجا Shaper به این صورت عمل می‌کند که در ۲۰٪ از زمان داده را ارسال می‌کند و سپس ۸۰٪ از زمان را دست‌نگه می‌دارد (زمان همان Interval ما است).

برای مثال شکل ۳۱-۱۲، یک گراف(نمودار) از مفهومی که مطرح شد را نشان می‌دهد. با فرض اینکه Time interval مورد نظر ما در اینجا ۱ ثانیه است. با میانگینِ ۲۰۰ میلیون بیت در ثانیه، Shaper هر ثانیه اجازه خروج ۲۰۰ میلیون بیت را می‌دهد. با توجه به اینکه Interface خروجی 1Gbps است، فقط ۰.۲ ثانیه (یا همان 200 ms) زمان می‌برد تا تمام ۲۰۰میلیون بیت ارسال شوند... سپس Shaper باید تا پایان Time interval (که در اینجا ۱ثانیه است) صبر کند (یعنی ۰.۸ ثانیه یا همان 800 ms بیکار باشد).



شکل ۳۱-۱۲ بررسی Shaper

حالا فکر کنید درست زمانی که Shaper ارسال بسته را برای یک TimeInterval به پایان رسانده است ، یک بسته‌ی Voice ویا Video که به Delay و Jitter بسیار کم نیاز دارند از راه برسد! حتی اگر آن بسته در صف priority قرار گرفته باشد، باز هم برای 800 ms مورد نظر می‌ماند تا Shaper به زمان‌بندی بعدی‌اش برسد. (توجه داشته باشید که حداکثرDelay یک طرفه که برای Voice مشکلی ایجاد نمی‌کند، 150 ms تاخیر است)

راه‌حل ما برای این مشکل، کم کردن میزان Time interval است؛ برای مثال در سناریو فعلی ما، Time intervalهای زیر (که به اختصار به آنها TC هم می‌گویند) می‌توانند استفاده شوند (به تاثیرهای هرکدام هم اشاره شده است):

Tc = 1 second (1000 ms): Send at 1 Gbps for 200 ms, rest for 800 ms
Tc = .1 second (100 ms): Send at 1 Gbps for 20 ms, rest for 80 ms
Tc = .01 second (10 ms): Send at 1 Gbps for 2 ms, rest for 8 ms

وقتی از Shaping استفاده می‌کنید، از Time Interval کوتاهی استفاده کنید (با توجه به توصیه‌هایی که شده است، برای پشتیبانی از داده‌های Voice و Video از Time Interval ، 10 ms استفاده کنید).

www.takbook.com

در انتها به این ۲ نکته هم توجه داشته باشید:

اول اینکه Shaperها همانند Policerها اجازهی یک Burst را بعد از مدتی Inactivity میدهند و دوم اینکه Shaperها بروی اینترفیسهای خروجی فعال میشوند.

۴-۳-۱۲ بررسی Congestion Avoidance

در این مبحث در مورد **جلوگیری از تراکم** ویا همان **Congestion Avoidance** صحبت میکنیم، Congestion Avoidance، یک feature، برای QoS است که با استفاده از discard کردن یکسری از پکتهای استفاده شده در کانکشنهای TCP، تلاش بر کاهشدادن Loss در شبکه را دارد. برای اینکه متوجه شوید که این ابزار به چه صورت عمل میکند، ابتدا میبایستی به فرایند و پروسهی windowing در TCP نگاهی بندازیم و سپس نحوهی عملکرد این سیستم را بررسی کنیم.

مفاهیم TCP Windowing

پروتکل TCP از یک مکانیزمی با نام windowing برای کنترل جریان (Flow)استفاده میکند، هر TCP Receiver(دریافت کننده) یک window به TCP Sender(ارسال کننده) تحویل میدهد "Window" عددی است که نشان میدهد sender (ارسال کننده) قبل از دریافت TCP Acknowledgement از سمتReceiver (دریافت کننده) چه تعداد بایت در طول اتصال TCP یا همان (TCP Connection) میتواند ارسال کند. بخواهیم دقیقتر بگوئیم، window تعداد بایتهای unacknowledged است که sender تا قبل از اینکه وارد پروسهی Stop(توقف) و Wait (انتظار) شود، میتواند ارسال کند.

این مکانیزم به Receiver قدرت کنترل سرعت ارسال دیتایی که توسط sender ارسال میشود را میدهد. هر سگمنت جدیدی که از طرف Receiver به سمت Sender ارسال میشود، باعث ایجاد و تحویل دادن یکwindow جدید میشود که این عدد میتواند کم و یا زیادتر از عدد قبلی (Previous window) باشد. با بالا پایین بردن این عدد ، Receiver میتواند Sender را مجبور به توقفهای طولانیتر کند و یا کاری کند که Sender هیچوقت توقف نکند و دست از ارسال دیتا برندارد!

هر کانکشن TCP، دارای ۲ ارسال کننده و ۲ دریافت کننده است؛ چرا که هر Host دیتاها را هم ارسال و هم دریافت میکند. در این وضعیت فعلی که سعی بر درک این سیستم داریم، شما این اتصال و کانکشن را یکطرفه درنظر بگیرید (بدین معنی که فقط یک host ارسال کننده و دیگری دریافت کننده است) ، در این شرایط در نظر داشته باشید که با وجود یک ارسال کننده و یک دریافت کننده؛ acknowledge ها از طرف دریافتکننده به سمت ارسال کننده ارسال میشوند. زمانی که همه چیز به درستی پیشمیرود، Receiver هربار که دیتاها را acknowledge میکند، سعی میکند که window را بالا ببرد (هربار آنرا دو برابر میکند)؛ در نهایت window به نقطه ای میرسد که Sender هیچوقت نباید دستنگه دارد، Sender مرتباً بستههای TCP Ack را قبل ارسال تمام دادهها درWindow قبل، دریافت میکند. هر acknowledgemen جدید ، یک window جدید به sender تحویل میدهد. همچنین زمانی که TCP Revicer احساس میکند که Loss

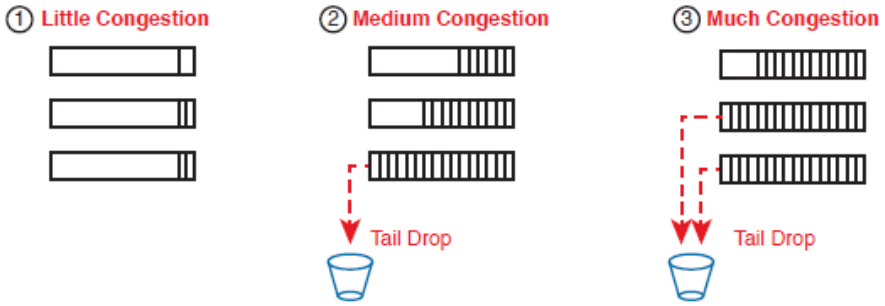
www.takbook.com

درحال اتفاق افتادن است (یعنی زمانی که یک سگمنت TCP را از دست می‌دهد)، برشکل روال بالا را انجام می‌دهد و Window که میخواهد بهSender ارسال کند را Shrink می‌کند. با هر بار اتفاق افتادن این موضوع (از دست رفتن) TCP Segment، عدد (Window) نصف می‌شود که باعث پایین آمدن سرعت و rate فرستنده می‌شود، تا از اتفاق افتادن دوباره این موضوع جلوگیری کند.

حالا برای یک لحظه بیایدQueue های روتر را در نظر بگیریم. بدون ابزارCongestion avoidance ، رویدادی با نام Tail drop باعث بیشترین Drop ها در شبکه می‌شود. شکل ۳۲-۱۲، ایده ی صف‌بندی و همان سیستم Queuing قدیم را نمایش می‌دهد ، اما در سه موقعیت متفاوت :

- تراکم کم(little congestion)
- تراکم متوسط(medium congestion)
- تراکم زیاد(much congestion)

در قسمته سمت چپ شکل ۳۲-۱۲، با تراکم کم، صف‌های خروجی بر روی یک Interface ، هنوز پُر (filled) نشده اند. در قسمت میانی، صف‌های دیگر با پر شدن یک صف، شروع به پر شدن می‌کنند. در این لحظه هر پکتی که برای آن صف از راه برسد، drop می‌شود، چراکه هیچ جایی برای قرار دادن آن پکت وجود ندارد .



شکل ۳۲-۱۲ بررسی صف

بدترین حالتی که می‌تواند پیش بیاید، موقعیتی مشابه قسمت سمت راست یعنی تراکم زیاد می‌باشد، مقدار زیادی tail drop انجام می‌شود و بسته‌های بسیاری از بین می‌روند.

هرچه تراکم بیشتر شود ، تاثیر منفی آن بر ترافیک شبکه هم بیشتر خواهد شد چراکه باعث loss و delay بسیاری می‌شود.

آشنایی‌با Congestion Avoidance Tools (ابزارهای جلوگیری از تراکم)

ابزارهای جلوگیری از تراکم ، همان‌طور که از نامشان مشخص است، تلاش بر جلوگیری از ایجاد تراکم دارند؛ با استفاده از همان مکانیزم windowing در TCP .

www.takbook.com

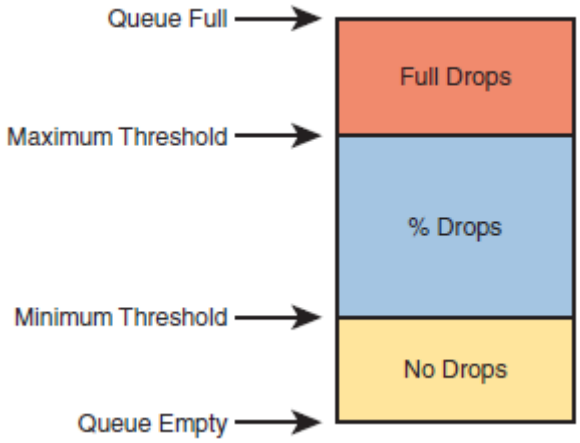
این ابزارها تعدادی از سگمنت‌های TCP را قبل از اینکه صف‌ها پر شوند ، Discard می‌کنند ... به امید آنکه TCP Connection ها، باقی سرعت خود را کم کرده، تراکم را پایین بیاورند و از ایجاد مشکل اصلی یعنی tail dropتعداد زیادی از پکت‌های باقی مانده، جلوگیری کنند.

استراتژی مورد استفاده ساده است : تعدادی از کم اهمیت‌ها را همین الان خودت از بین ببر و امیدوار باش و باعث شو که Device، مقدار بسیار کمتری را در طولانی مدت از بین ببرد.

ابزارهای جلوگیری از تراکم یا همان Congestion avoidance ، هربار عمق صف‌ها را میانگین‌گیری می‌کنند و موقعیتی برای بررسی دقیق‌تر و عمقی‌تر سطح صف‌ها فراهم می‌کنند(شکل ۳۳ –۱۲).

طول شکل ۳۳–۱۲، (طول مستطیل) ، نشان دهنده‌ی عمق صف و یا همان تعداد پکت‌های داخل صف می‌باشد؛ زمانی که عمق صف کم می‌باشد (کمتر از آستانه ی مشخص شده‌ی minimum است) ، ابزارCongestion avoidance ، هیچ کاری انجام نمی‌دهد .زمانی که این عُمق بین آستانهی کم و زیاد (maximumو minimum) باشد، ابزارCongestion avoidance ، درصدی از پکت‌ها را discard می‌کند؛ عموما درصدهای کم مانند ۵٪ ، ۱۰٪ ویا ۲۰٪.

اگر این عمق از آستانیه‌ی maximum عبور کند ، این ابزار تمام پکت‌ها را در عملی که به آن full dropگفته می‌شود ، drop می‌کند.



شکل ۳۳-۱۲ بررسی صف

۵–۳–۱۲ بررسی IP Precedence and DSCP Values

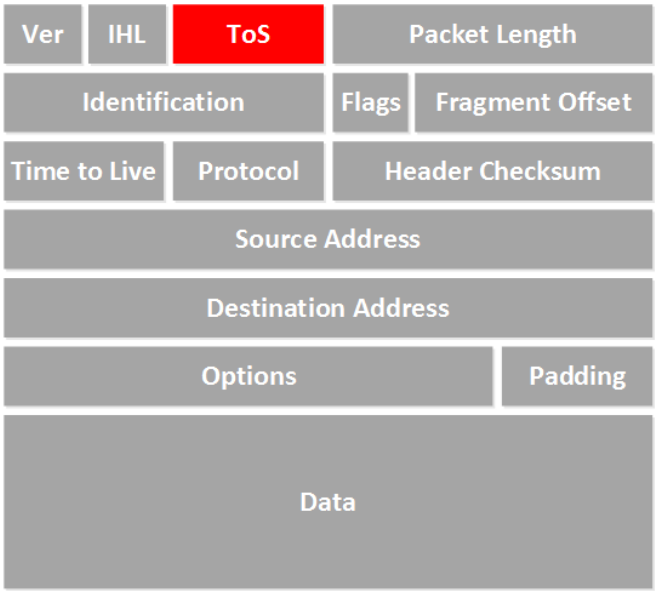
بسته‌های IP فیلدی با نام Type of Service دارند که به بایت TOS نیز معروف است، ایده‌ی اصلی در بایت TOS این بود که ما می‌توانیم اولویت را مشخص کنیم و مسیری را برای توان بالا، تأخیر کم و یک سرویس قابل اطمینان بالا درخواست کنیم.

www.takbook.com

بایت TOS در سال ۱۹۸۱ در RFC 791 تعریف شده است اما نحوه‌ی استفاده از آن در طول سال‌ها تغییر کرده است. این امر باعث می‌شود تا کمی گیج کننده باشد زیرا اصطلاحات زیادی وجود دارد و امروزه بعضی از آنها دیگر مورد استفاده قرار نمی‌گیرند.

بیایید نگاهی به بایت TOS بیندازیم:

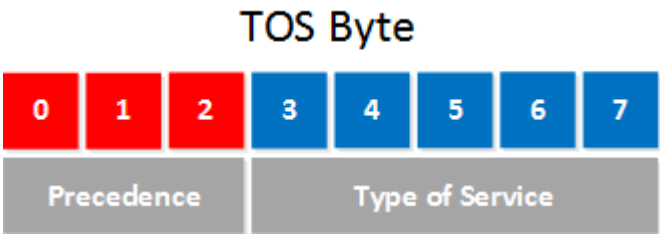
در شکل ۳۴-۱۲، header مربوط به بسته‌ی IP را مشاهده می‌کنید که همه‌ی جزئیات آن مشخص شده است از جمله بایت TOS که در این قسمت روی آن کار خواهیم کرد.



شکل ۱۲-۳۴ *IP Precedence and DSCP Values*

بعضی از دوستان COS (Class of Service) را با TOS (Type os Service) یکی در نظر می‌گیرند و همین موضوع باعث مشکلات می‌شود، توجه داشته باشید که TOS مربوط به Header بسته‌ی IP در لایه‌ی سوم است و COS مربوط به header پروتکل 802.1Q (لایه‌ی دوم) است که COS مربوط به لینک Trunk است، پس هیچ ربطی به هم ندارند.

بررسی ۸ بیت TOS



شکل ۱۲-۳۵ *TOS Byte*

www.takbook.com

به مانند شکل ۳۵-۱۲، سه بیت اول که با نام Precedence مشخص شده‌اند مربوط به تعریف اولویت هستند، به این صورت که هر چقدر مقدار IP بیشتر باشد بسته‌IP مورد نظر مهم‌تر خواهد بود و روتر ابتدا بسته‌هایی دارای اولویت پائین را رها می‌کند.

توجه داشته باشید از TOS یا Type of Service برای تعیین نوع تاخیر، توان و قابلیت اطمینان استفاده می‌شود.

به این موضوع توجه کنید که TOS یک باید در Header بسته‌ی IP است و خود TOS به چند بیت تشکل شده است که این بایت و بیت را با هم مخلوط نکنید تا گیج کننده نباشد.

در جدول ۱-۱۲، لیستی از بیت‌ها و ترکیب‌های احتمالی آورده شده است:

جدول مربوط به بیت Precedence

جدول ۱-۱۲ بیت Precedence

000	Routine
001	Priority
010	Immediate
011	Flash
100	Flash Override
101	Critic/Critical
110	Internetwork Control
111	Network Control

جدول مربوط به بیت Type of Service

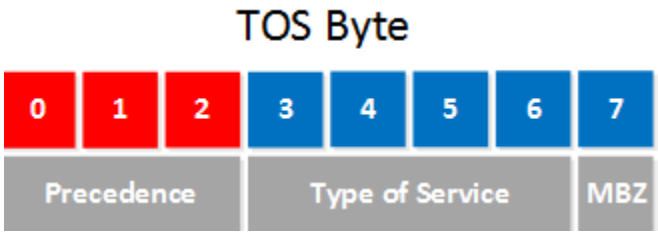
جدول ۲-۱۲ بیت Precedence

Bit 3	0 = normal delay	1 = low delay
Bit 4	0 = normal throughput	1 = high throughput
Bit 5	0 = normal reliability	1 = high reliability
Bit 6-7	Reserved for future use	

جدول ۲-۱۲ بیت Precedence

این تعریف از TOS در سال ۱۹۸۱ بوده و جالب این است که از بیت‌های Type of Service به هیچ عنوان استفاده نشده و فقط از سه بیت اول یعنی بین اولویت استفاده می‌کردند.

بعد از حدود ۱۰ سال در سال ۱۹۹۲، RFC 1349 ایجاد شد که در آن تعریف بایت TOS تغییر کرد، که شکل ۳۶-۱۲را مشاهده می‌کنید:



شکل ۳۶-۱۲ TOS Byte

www.takbook.com

در شکل ۳۶-۱۲، سه بیت اول که مربوط به اولویت یا همان precedence بوده تغییر نکرده ولی بیت‌های Type os Service تغییراتی داشته است.

در Type of Service از چهار بیت برای اختصاص نوع سرویس استفاده می‌کنیم و بیت آخر MBZ نام دارد و این بیت طبق گفته‌ی RFC مورد استفاده‌ی عموم قرار نمی‌گیرد و فقط برای آزمایش‌ها کاربرد دارد و روترها هم این بیت را نادیده می‌گیرند.

در حال حاظر بیت‌های Type os Service به صورت جدول ۳-۱۲، است:

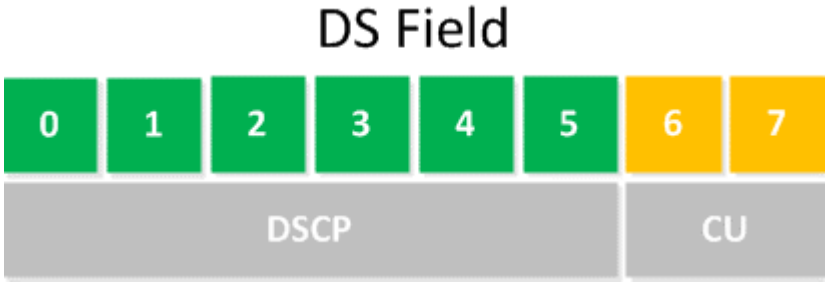
1000	minimize delay
0100	maximize throughput
0010	maximize reliability
0001	minimize monetary cost
0000	normal service

جدول ۳-۱۲ بیت Precedence

در آخر باید گفت که از بیت‌های Type of Service تا به امروز استفاده نشده است و TOS جای خود را به DS یا Differentiated Services داده است.

بررسی Differentiated Services

در سال ۱۹۹۸ تغییراتی ایجاد شد و TOS با شکل و شمایل جدیدی و با نام جدید Differentiated Services ارئه شد که مربوط به RFC2474 است و ۸ بیت آن نیز تغییر کرده است .آنچه در حال حاضر به صورت شکل ۳۷-۱۲ است.



شکل ۳۷-۱۲ TOS Byte

در ابتدا ۶ بیت از قسمت DS برای تنظیم CodPoint یا کد رمزگذاری استفاده می‌شود که بر روی PHP یا همان Per Hop Behavior تاثیر می‌گذارد، منظور از کدگذاری همان DSCP است، به زمان ساده‌تر کد گذاری شبیه به اولویت (precedence) در بایت TOS است.

اگر بخواهیم در مورد PHB بیشتر توضیح دهیم به مانند شکل ۳۸-۱۲، سه روتر پشت سر هم را در نظر بگیرید.

www.takbook.com

شکل ۱۲-۳۸ *TOS Byte*

دو گوشی تلفن و سه روتر را در شکل ۳۸-۱۲، مشاهده می‌کنید، هنگامی که QOS را برای پیکربندی بسته‌های Voip اولویت‌بندی می‌کنیم، باید این کار را در تمام دستگاه‌ها انجام دهیم، اگر در R1 و R3 تنظیمات برای اولویت‌بندی بسته‌های VOIP انجام شود و در روتر R2 نشود باز هم با مشکلات کیفیت بد تماس تلفنی روبرو خواهید بود، پس برای اینکه با مشکلی روبرو نشویم بهتر است این دو روش را انجام دهیم:

۱- استفاده از reservations

هر دستگاه در شبکه برای تماس تلفنی که قرار است برقرار کنید پهنای باند را "رزرو" می‌کند.

۲- اولویت بندی

برای اولویت بندی بسته‌های VoIP ، هر دستگاه را به طور جداگانه پیکربندی کنید.

انجام رزرو به نظر می رسد یک ایده‌ی بسیار خوب است زیرا می‌توانید تضمین کنید که ما می‌توانیم تماس تلفنی برقرار کنیم، اما این یک راه حل بسیار قابل اطمینان نیست، زیرا برای هر تماس تلفنی که می‌خواهید برقرار کنیم چنانچه اگر یکی از روترها اطلاعات رزرو خود را از دست بدهد ، چه اتفاقی رخ می‌دهد؟

۶-۳-۱۲ مثالی QoS Marking در روتر Cisco

در این قسمت نگاهی به مارک‌گذاری (Marking) بسته‌ها می‌اندازیم، برای اینکه بهتر این قسمت را درک کنید یک مثال را با هم بررسی می‌کنیم:

شکل ۱۲-۳۹ مثال *QoS Marking*

به مانند شکل ۳۹-۱۲، سه روتر در یک ردیف قرار دارند و ترافیک از روتر R1 به روتر R3 ارسال می‌شود، برای مشخص کردن ترافیک از روتر R2 استفاده خواهیم کرد، برای اینکه کل شبکه با هم در ارتباط باشند باید در روتر R1 و R3 یک static route بنویسیم که این کار را قبلاً در فصل چهارم به صورت کامل توضیح دادیم.

www.takbook.com

برای ایجاد لیست طبقه‌بندی نیاز به Access List داریم برای همین در زیر یک Acess List در R2 ایجاد می‌کنیم:

```
R2(config)#ip access-list extended TELNET-TRAFFIC
```

با دستور بالا یک ACL از نوع Extended و با نام TELNET-TRAFFIC ایجاد می‌کنیم.

```
R2(config-ext-nacl)#permit tcp any any eq telnet
```

در ادامه وارد Access List شدیم و باید دستور بالا را وارد کنیم، در این دستور به کل شبکه سرویس Telnet را دسترسی می‌دهیم.

در ادامه باید ACL یا همان Access List را به Class-Map متصل کنیم:

```
2(config)#class-map TELNET-TRAFFIC
R2(config-cmap)#match access-group name TELNET-TRAFFIC
```

بعد از انجام کار بالا Class-Map را به policy-map متصل می‌کنید:

```
R2(config)#policy-map MARKING
R2(config-pmap)#class TELNET-TRAFFIC
R2(config-pmap-c)#set ?
  atm-clp        Set ATM CLP bit to 1
  cos            Set IEEE 802.1Q/ISL class of service/user priority
  cos-inner      Set Inner CoS
  discard-class  Discard behavior identifier
  dscp           Set DSCP in IP(v4) and IPv6 packets
  fr-de          Set FR DE bit to 1
  ip             Set IP specific values
  mpls           Set MPLS specific values
  precedence     Set precedence in IP(v4) and IPv6 packets
  qos-group      Set QoS Group
  vlan-inner     Set Inner Vlan
```

با وارد کردن دستور Set و بعد از آن علامت سوال گزینه‌های زیادی را در بالا مشاهده می‌کنید، وقتی نوبت به بسته‌های IP می‌رسد باید از ارزش‌های precedence یا DSCP استفاده کنیم.

```
R2(config-pmap-c)#set precedence ?
  <0-7>          Precedence value
  cos            Set packet precedence from L2 COS
  critical       Set packets with critical precedence (5)
  flash          Set packets with flash precedence (3)
  flash-override Set packets with flash override precedence (4)
  immediate      Set packets with immediate precedence (2)
  internet       Set packets with internetwork control precedence (6)
  network        Set packets with network control precedence (7)
  priority       Set packets with priority precedence (1)
```

www.takbook.com


```
qos-group      Set packet precedence from QoS Group.
routine        Set packets with routine precedence (0)
```

در این دستور عدد 7 یا همان Network را وارد و Enter کنید.

بعد از انجام کار بالا باید در interface FastEthernet 0/0 روتر R2 که به سمت روتر R1 است دستور زیر را وارد کنیم:

```
R2(config)#interface FastEthernet 0/0
R2(config-if)#service-policy input MARKING
```

اگر از طریق روتر R1 به روتر R3 یک ارتباط Telnet برقرار کنیم، نتیجه به صورت زیر خواهد شد:

```
R1#telnet 192.168.23.3
Trying 192.168.23.3 ... Open
```

در ادامه با دستور زیر اطلاعات R2 را مشاهده می‌کنیم:

```
R2#show policy-map interface FastEthernet 0/0
 FastEthernet0/0

  Service-policy input: MARKING

    Class-map: TELNET-TRAFFIC (match-all)
      10 packets, 609 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: access-group name TELNET-TRAFFIC
      QoS Set
        precedence 7
          Packets marked 10

    Class-map: class-default (match-any)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
Match: any
```

همانطور که در نتیجه‌ی دستور بالا مشاهده می‌کنید ۱۰ بسته precedence مشخص شده است.

بیاید ببینم آیا می‌شود برخی از بسته‌ها را با مقدار DSCP علامت‌گذاری کنیم، برای این‌کار می‌خواهیم ترافیک HTTP را علامت بزنیم:

با دستورات زیر یک ACL با نام HTTP-TRAFFIC ایجاد و به ترافیک پورت ۸۰ دسترسی می‌دهیم که همان ترافیک HTTP است.

```
R2(config)#ip access-list extended HTTP-TRAFFIC
R2(config-ext-nacl)#permit tcp any any eq 80
```

در ادامه Class-Map را با دستورات زیر ایجاد می‌کنیم و ACL را به آن ارتباط می‌دهیم:

```
R2(config)#class-map HTTP-TRAFFIC
R2(config-cmap)#match access-group name HTTP-TRAFFIC
```

www.takbook.com

در ادامه Policy-Map را با دستورات زیر ایجاد و Class-Map را به آن ارتباط می‌دهیم:

```
R2(config)#policy-map MARKING
R2(config-pmap)#class HTTP-TRAFFIC
R2(config-pmap-c)#set dscp ?
  <0-63>    Differentiated services codepoint value
  af11      Match packets with AF11 dscp (001010)
  af12      Match packets with AF12 dscp (001100)
  af13      Match packets with AF13 dscp (001110)
  af21      Match packets with AF21 dscp (010010)
  af22      Match packets with AF22 dscp (010100)
  af23      Match packets with AF23 dscp (010110)
  af31      Match packets with AF31 dscp (011010)
  af32      Match packets with AF32 dscp (011100)
  af33      Match packets with AF33 dscp (011110)
  af41      Match packets with AF41 dscp (100010)
  af42      Match packets with AF42 dscp (100100)
  af43      Match packets with AF43 dscp (100110)
  cos       Set packet DSCP from L2 COS
  cs1       Match packets with CS1(precedence 1) dscp (001000)
  cs2       Match packets with CS2(precedence 2) dscp (010000)
  cs3       Match packets with CS3(precedence 3) dscp (011000)
  cs4       Match packets with CS4(precedence 4) dscp (100000)
  cs5       Match packets with CS5(precedence 5) dscp (101000)
  cs6       Match packets with CS6(precedence 6) dscp (110000)
  cs7       Match packets with CS7(precedence 7) dscp (111000)
  default   Match packets with default dscp (000000)
  ef        Match packets with EF dscp (101110)
  qos-group  Set packet dscp from QoS Group.
```

همانطور که در دستورات بالا مشاهده می‌کنید می‌خواهیم از DSCP استفاده کنیم که کد af12 را برای آن انتخاب می‌کنیم.

```
R2(config-pmap-c)#set dscp af12
```

بعد از انجام کار باید یک ترافیکی از نوع HTTP ایجاد کنیم، برای این کار از دستورات زیر استفاده می‌کنیم:

```
R3(config)#ip http server

R1#telnet 192.168.23.3 80
Trying 192.168.23.3, 80 ... Open
```

بعد از انجام کار بالا حالا می‌توانیم اطلاعات Policy-Map را در روتر R2 مشاهده کنیم:

```
R2#show policy-map interface FastEthernet 0/0
 FastEthernet0/0
  Service-policy input: MARKING
    Class-map: TELNET-TRAFFIC (match-all)
      10 packets, 609 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
```

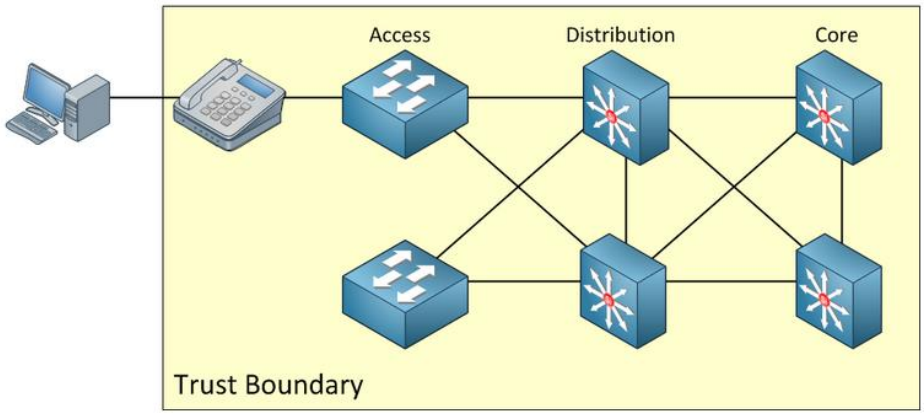
www.takbook.com


```
  Match: access-group name TELNET-TRAFFIC
  QoS Set
    precedence 7
      Packets marked 10
Class-map: HTTP-TRAFFIC (match-all)
  3 packets, 180 bytes
  5 minute offered rate 0 bps, drop rate 0 bps
  Match: access-group name HTTP-TRAFFIC
  QoS Set
    dscp af12
      Packets marked 3

Class-map: class-default (match-any)
  99 packets, 5940 bytes
  5 minute offered rate 0 bps, drop rate 0 bps
   Match: any
```

همانطور که در نتیجه‌ی دستور بالا مشاهده می‌کنید سه بسته Mark شده است.

۷-۳-۱۲ مرز اعتماد QoS در سوئیچ های سیسکو

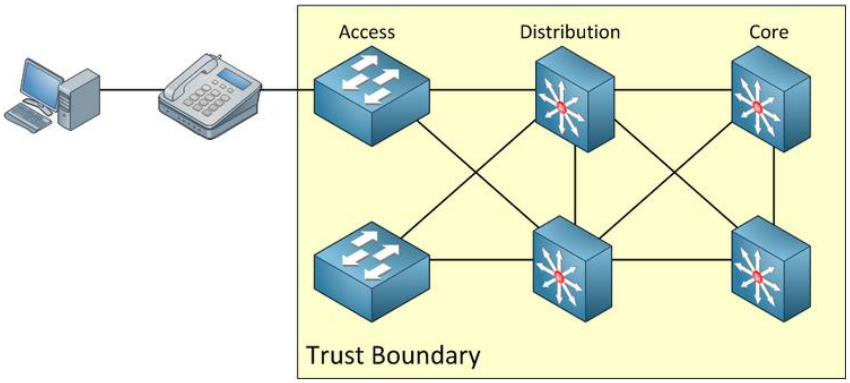
هنگامی که ما QoS را در سوییچ های Cisco پیکربندی می‌کنیم ، باید در مورد مرز اطمینان خود فکر کنیم، به زبان ساده‌تر باید گفت که ما باید به چه دستگاه‌هایی اعتماد کنیم تا عملیات QOS را بر روی آنها انجام دهیم، آیا تلفن IP و یا سوئیچ قابل اعتماد هستند؟



شکل ۴۰-۱۲ Trust Boundary

در شکل ۴۰-۱۲، حاشیه اعتماد در تلفن IP Cisco است ، این بدان معنی است که ما هیچکدام از بسته ها یا فریم‌های Ethernet را در سوئیچ لایه دسترسی متذکر نمی‌کنیم، بلکه تلفن IP تمام ترافیک را علامت‌گذاری می‌کند. توجه داشته باشید که PC خارج از مرز اعتماد QoS است، این بدان معنی است که ما به نشانه‌گذاری PC اعتماد نداریم، اگر بخواهید می‌توانید تمام ترافیک آن را بر روی تلفن IP مشاهده کنید. با توجه به این مسائل به شکل بعدی توجه کنید.

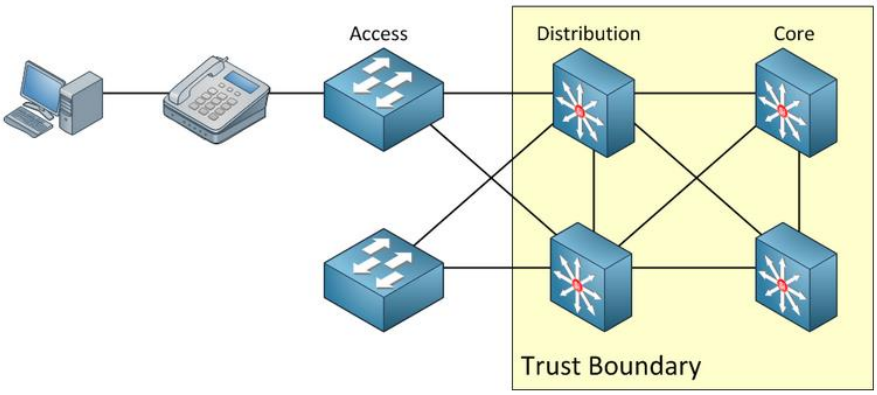
www.takbook.com



شکل ۱۲-۴۱ *Trust Boundary*

در شکل ۴۱-۱۲، ما به هیچ وجه به علامت‌گذاری که توسط تلفن IP انجام می‌شود و به سمت سوئیچ Access ارسال می‌شود اعتمادی نداریم، این بدان معنا است که ما در سوئیچ‌های لایه دسترسی طبقه‌بندی و علامتگذاری (classification and marking) را انجام می‌دهیم.

برای اینکه بیشتر با موضوع آشنا شوید یک مثال دیگر را با هم بررسی می‌کنیم، در شکل ۴۲-۱۲ قبل از تغییرات در سوئیچ لایه‌ی distribution به سوئیچ‌های لایه‌ی Access اعتمادی نداریم، شاید مدیریت سوئیچ‌های لایه‌ی Access شخص دیگری باشد و شاید بخواهید از ارسال بسته یا فریم Ethernet که به سمت سوئیچ های لایه‌ی distribution علامت گذاری شده‌اند جلوگیری کند.



شکل ۱۲-۴۲ *Trust Boundary*

برای اینکه بهتر به این موضوع پی ببرید با هم یک سوئیچ ۳۵۶۰ را برای این کار پیکربندی می‌کنیم، برای فعال‌سازی QOS در سوئیچ باید از دستور زیر استفاده کنید:

3560Switch(config)#**mls qos**

با اجرای دستور بالا تمام بسته‌هایی که مارک‌گذاری و دریافت شده باشد را پاک خواهد کرد و برای اینکه چنین اتفاقی نیفتد بهتر است از دستور زیر استفاده کنید:

3560Switch(config)#**no mls qos rewrite ip dscp**

www.takbook.com

برای اینکه ببینیم یک Interface در چه وضعیتی از QOS قرار دارد باید از دستور زیر استفاده کنید:

3560Switch#**show mls qos interface fastEthernet 0/1**

FastEthernet0/1

trust state: not trusted

trust mode: not trusted

COS override: dis

default COS: 0

DSCP Mutation Map: Default DSCP Mutation Map

Trust device: none

همانطور که در نتیجه‌ی دستور بالا مشاهده می‌کنید ما به هیچ چیز اعتمادی نداریم این یک پیش‌فرض در سوئیچ‌های سیسکو است، ما می‌توانیم بسته‌ها را بر اساس ارزش DSCP، فریم‌های روی مقدار COS و یا می‌توانیم به تلفن IP اعتماد کنیم، برای مثال:

3560Switch(config-if)#**mls qos trust cos**

بعد از تایید و اعتماد به COS باید نتیجه‌ی کار را مشاهده کنید:

3560Switch#**show mls qos interface fastEthernet 0/1**

FastEthernet0/1

trust state: **trust cos**

trust mode: **trust cos**

COS override: dis

default COS: 0

DSCP Mutation Map: Default DSCP Mutation Map

Trust device: none

همانطور که در دستور بالا مشاهده می‌کنید COS در Interface مورد نظر قابل اعتماد شده است.

توجه داشته باشید به صورت پیش‌فرض سوئیچ مقدار DSCP را در Frame بر اساس نقشه‌ی cos-to-dscp تغییر می‌دهد و برای جلوگیری از این کار باید از دستور زیر استفاده کنید:

3560Switch(config-if)#**mls qos trust cos pass-through**

www.takbook.com

کلمه‌ی کلیدی pass-through این اطمینان را به شما خواهد داد که سوئیچ شما مقدار DSCP را بازنویسی نخواهد کرد، برای تنظیم مقدار DSCP در سوئیچ از دستور زیر استفاده کنید:

3560Switch(config-if)#**mls qos trust dscp**

با استفاده از دستور بالا دیگر به COS اعتماد نخواهید کرد و فقط به بسته‌های DSCP که از Interface وارد می‌شود اعتماد خواهید کرد.

3560Switch#**show mls qos interface fastEthernet 0/1**
FastEthernet0/1
trust state: trust dscp
trust mode: trust dscp
COS override: dis
default COS: 0
DSCP Mutation Map: Default DSCP Mutation Map
Trust device: none

اعتماد به مقدار DSCP و COS روی یک Interface می‌تواند مرز اعتماد شما را در سطح سوئیچ تنظیم کند، اما اگر بخواهید مرز اعتماد خود را در تلفن IP Cisco تنظیم کنید چه کاری باید انجام دهید؟

3560Switch(config-if)#**mls qos trust device cisco-phone**

با دستور بالا به سوئیچ خود اعلام می‌کنیم که به تمام مقادیر QOS که از طرف تلفن IP دریافت می‌کند اعتماد کند.

3560Switch#**show mls qos interface FastEthernet0/1**
FastEthernet0/1
trust state: not trusted
trust mode: not trusted
COS override: dis
default COS: 0
DSCP Mutation Map: Default DSCP Mutation Map
Trust device: cisco-phone

۱۲-۴ Miscellaneous IP Services

۱۲-۴-۱ فعال‌سازی سرویس SNMP

سرویس SNMP یا همان Simple Network Management Protocol یک پروتکل برای مدیریت بر عملکرد دستگاه‌های شبکه، سرورها و... است، نسخه‌های SNMP از 1 تا 3 وجود دارد، که نسخه‌ی ۳ آن بیشترین امنیت را دارد.

www.takbook.com

سرویس SNMPv3 دارای سه نوع مدل امنیتی است که در جدول ۴-۱۲، مدل و سطوح امنیتی آن را مشاهده می‌کنید.

جدول ۴-۱۲ سرویس SNMPv3

سطح	احراز هویت	رمزگذاری	نتیجه کار
noAuthNoPriv	نام کاربری	ندارد	فقط از طریق وارد کردن نام کاربری می‌توانید به اطلاعات دست پیدا کنید که این موضوع بسیار می‌تواند خطرناک باشد.
authNoPriv	الگوریتم MD5 و SHA	No	بر اساس الگوریتم‌های احراز هویت MD5 و SHA تایید اعتبار را ارائه می‌دهد.
authPriv	الگوریتم MD5 و SHA	Data Encryption Standard (DES)	بر اساس الگوریتم‌های احراز هویت MD5 و SHA تایید اعتبار را انجام می‌دهد و علاوه بر آن رمزنگاری DES 56 bit را بر اساس استانداردهای CBC-DES و DES-56 ارائه می‌دهد.

برای فعال کردن پروتکل SNMP V3 باید به صورت زیر عمل کنید:

در دستور زیر کلمه 3isco به عنوان گروه معرفی شده است و V3 هم به این معنا است که ورژن snmp استفاده شده برای تنظیم ورژن ۳ است، در ادامه دستور priv را وارد کنید و اگر بعد از آن از علامت سوال استفاده کنید گزینه‌های مختلفی را مشاهده می‌کنید که هر کدام برای مشاهده حالت خاصی از اطلاعات است، مثلاً گزینه‌ی read برای مشاهده اطلاعات است و نمی‌توانید اطلاعات را تغییر بدهید.

www.takbook.com

توجه داشته باشد اگر هیچ کدام از گزینه‌ها را انتخاب نکنید به این معنا است که تمام اطلاعات قابل مشاهده است.

SW4(config)# **snmp-server group 3isco v3 priv**?

access specify an access-list associated with this group

context specify a context to associate these views for the group

match context name match criteria

notify specify a notify view for the group

read specify a read view for the group

write specify a write view for the group

پس دستور نهایی به صورت زیر است:

SW4(config)# **snmp-server group 3isco v3 priv**

دستور نهایی هم به صورت زیر وارد کنید:

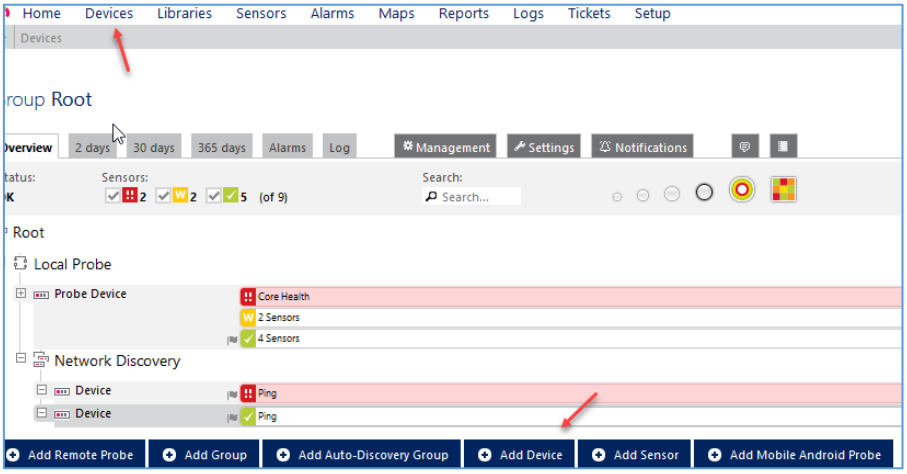
در این دستور یک نام کاربری با عنوان snmp_user وارد کنید و به گروهی را که در مرحله قبل ایجاد کردید در این قسمت وارد کنید بعد از آن باید دو پروتکل برای احراز هویت و کد کردن اطلاعات وارد کنید و رمز عبور آنها را وارد کنید، مثلاً در دستور زیر رمز Test@12345 برای پروتکل MDP و رمز 12345@Test برای پروتکل des است.

SW4(config)# **snmp-server user User1 3isco v3 auth md5 Test@12345 priv des 12345@Test**

بعد از این کار می‌خواهیم عملکرد این پروتکل را تست بگیریم، برای اینکه بتوانیم از پروتکل SNMP استفاده کنیم باید از یک نرم‌افزار مانیتورینگ استفاده کنیم که در اینجا از نرم‌افزار PRTG استفاده می‌کنید، توجه داشته باشید آموزش این نرم‌افزار را می‌توانید از کتاب مدیر شبکه ۱، که بنده آن را تالیف کردم مشاهده کنید.

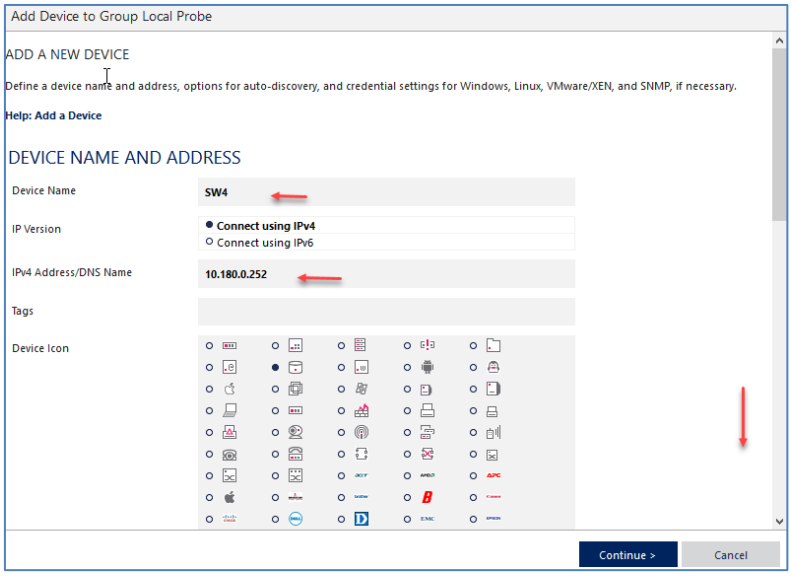
به مانند شکل ۴۳-۱۲، وارد تب Devices در نرم‌افزار PRTG شوید و برای اضافه کردن دستگاه مورد نظر بر روی Add Devices کلیک کنید.

www.takbook.com



شکل ۴۳-۱۲ نرم‌افزار PRTG

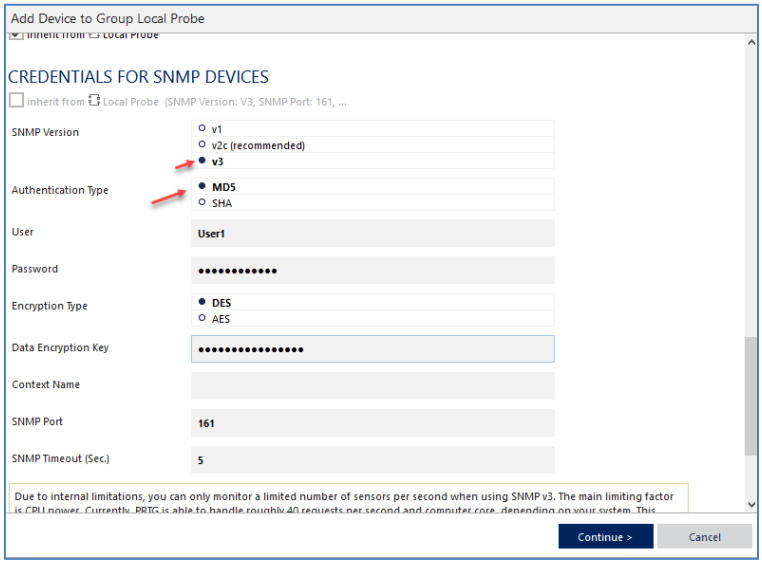
به مانند شکل ۴۴-۱۲، یک نام برای دستگاه خود وارد کنید و در قسمت IPV4 آدرس سوئیچ یا روتر خود را وارد کنید و صفحه را به پائین اسکرول کنید.



شکل ۴۴-۱۲ نرم‌افزار PRTG

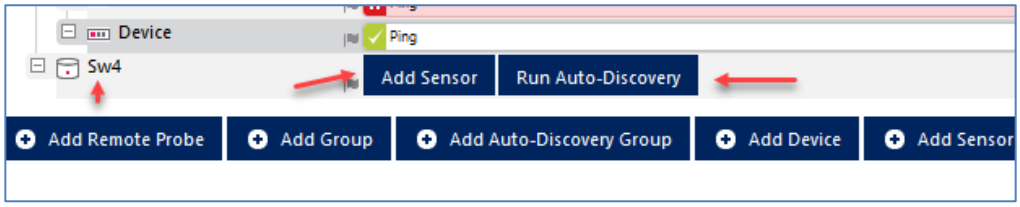
در شکل ۴۵-۱۲، ورژن SNMP را V3 انتخاب کنید و نوع Authentication را MD5 در نظر بگیرید، نام کاربری User1 را که ایجاد کردید در قسمت User وارد کنید و رمز عبور اول که Test@12345 بوده را وارد کنید و در قسمت Encryption Type گزینه‌ی Des را انتخاب و رمز دوم یعنی 12345@Test را وارد کنید و بر روی Continue کلیک کنید.

www.takbook.com



شکل ۴۵-۱۲ نرم‌افزار PRTG

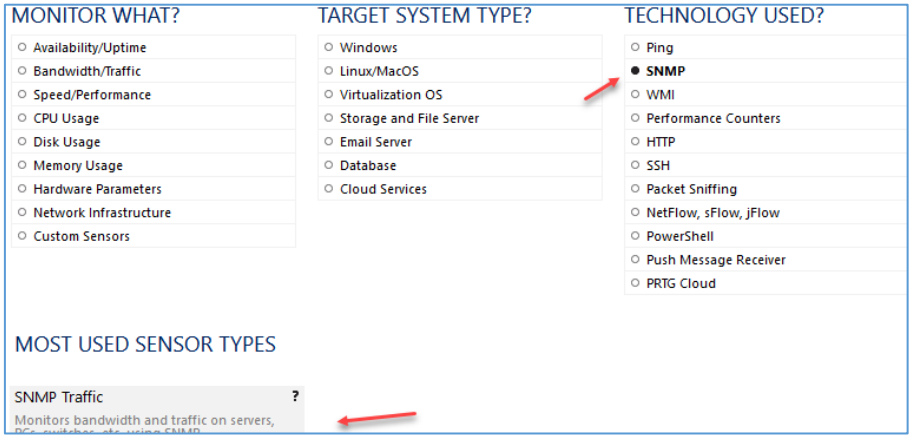
بعد از اضافه کردن دستگاه به لیست به مانند شکل ۴۶-۱۲، باید سنسور مورد نظر را برای آن فعال کنید، یا می‌توانید بر روی Run Auto-Discovery کلیک کنید که این گزینه به صورت اتوماتیک کارها را انجام می‌دهد.



شکل ۴۶-۱۲ نرم‌افزار PRTG

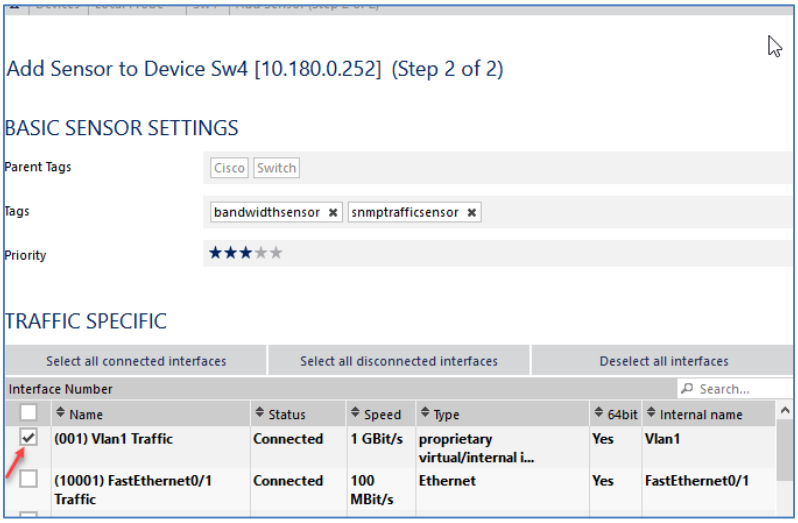
یا اینکه به مانند شکل ۴۷-۱۲، بر روی Add Sensor کلیک کنید تا شکل ۴۷-۱۲، ظاهر شود و در این قسمت گزینه‌ی SNMP را انتخاب کنید و بر روی SNMP Traffic کلیک کنید.

www.takbook.com



شکل ۴۷-۱۲ نرم‌افزار PRTG

همان‌طور که در شکل ۴۸-۱۲، مشاهده می‌کنید لیستی از interfaceها و Vlan را مشاهده می‌کنید که می‌توانید برای مانیتور کردن آنها هر کدام را که مایل بودید انتخاب کنید، در تب Status هم مشخص شده است که کدام interface متصل شده و درحال کار است، بعد از انتخاب بر روی Continue کلیک کنید، بعد از این کار می‌توانید نظارت دقیقی بر روی دستگاه خود داشته باشید.



شکل ۴۸-۱۲ نرم‌افزار PRTG

۲-۴-۱۲ کار با FTP AND TFTP

در این بخش دو پروتکل انتقال فایل FTP و TFTP را مورد بررسی قرار می‌دهیم، با این پروتکل می‌توانید IOS سیسکو را بر روی دستگاه‌های آن قرار دهید و نصب کنید و حتی می‌توانید آنها را آپدیت کنید و از آنها پشتیبان تهیه کنید.

www.takbook.com

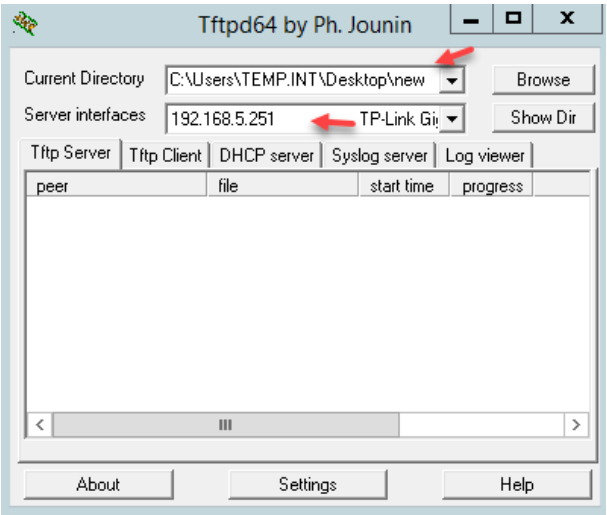
کار با FTP و TFTP در IOS

IOS در دل روتر یا سوئیچ قرار دارد و به عنوان سیستم عامل آن در نظر گرفته می‌شود و برای اجرا بر روی RAM بارگیری می‌شود.

برای اینکه کار پشتبانگیری و قرار دادن فایل IOS را در دستگاه‌های شبکه انجام دهیم می‌توانیم از نرم افزار TFTP که در بازار موجود است استفاده کنیم که ما در اینجا از نرم‌افزار tftpd32 استفاده می‌کنیم، که آن را می‌توانید از لینک زیر دانلود کنید.

http://tftpd32.jounin.net/tftpd32_download.html

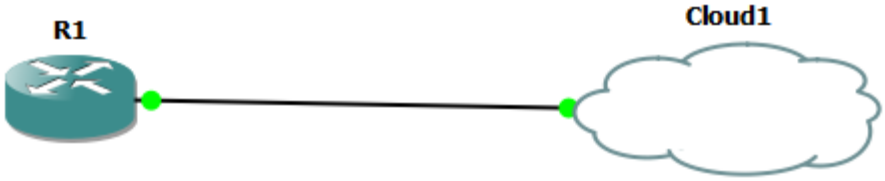
بعد از دانلود به مانند شکل ۴۹-۱۲، باید در قسمت Server interfaces آدرس IP سیستمی که بر روی آن اجرا شده است را انتخاب کنید تا بتوانیم از طریق روتر یا دیگر دستگاه‌های سیسکو به آن متصل شویم، توجه داشته باشید در قسمت Current Directory باید آدرس محل ذخیره‌سازی را مشخص کنید، یعنی این محل هم جایی است که اطلاعات از روتر در آن ذخیره و هم می‌توانیم فایل‌های مورد نظر خود را در آن کپی کنیم تا بتوانیم از طریق روتر آن را برداریم.



شکل ۴۹-۱۲ نرم‌افزار TFTP

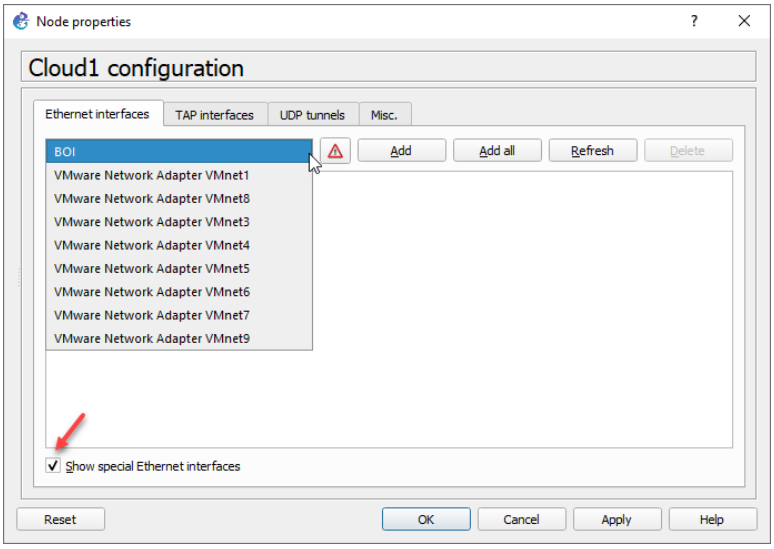
به مانند شکل ۵۰-۱۲، وارد نرم‌افزار GNS3 شوید و یک روتر به همراه یک Cloud به صفحه اضافه کنید، کار Cloud این است که دستگاه‌های داخل نرم‌افزار GNS3 را با شبکه واقعی یا مجازی در سیستم شما ارتباط دهد.

www.takbook.com



شکل ۵۰-۱۲ مثال TFTP

توجه داشته باشید برای اینکه بتوانید شبکه مورد نظر خود را در Cloud تنظیم کنید باید بر روی آن دو بار کلیک کنید و در شکل باز شده‌ی زیر تیک گزینه‌ی Show special Ethernet interfaces را انتخاب کنید و کارت شبکه‌ی خود را به مانند شکل ۵۱-۱۲، انتخاب کنید و بعد از آن می‌توانید روتر را به آن متصل کنید.



شکل ۵۱-۱۲ تنظیمات GNS3

وارد روتر شوید و آدرس IP آن را برای ارتباط با سرور TFTP تنظیم کنید:

```
R1(config)#int fastEthernet 0/0
R1(config-if)#ip address 192.168.5.200 255.255.255.0
R1(config-if)#no sh
```

همانطور که در زیر مشاهده می‌کنید ارتباط با سرور TFTP به درستی برقرار شده است.

```
R1(config-if)#do ping 192.168.5.251
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.5.165, timeout is 2 seconds:
!!!!.
```

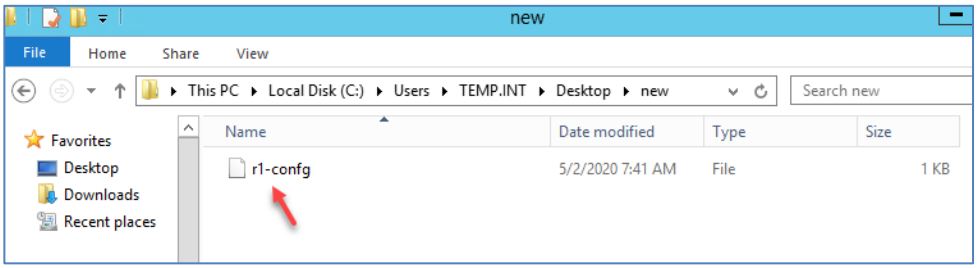
www.takbook.com

برای شروع کار می‌خواهیم اطلاعات Running-Config را در سرور TFTP کپی کنیم، برای این کار باید از دستور زیر استفاده کنید:

در دستورات زیر در قسمت اول دستور copy running-config tftp: برای کپی کردن اطلاعات در TFTP است، در قسمت دوم این دستور باید آدرس سرور TFTP را وارد کنید و در قسمت سوم باید یک اسم برای ذخیره شدن اطلاعات وارد کنید که به صورت پیش‌فرض نام آن r1-confg است.

```
R1#copy running-config tftp:
Address or name of remote host []? 192.168.5.251
Destination filename [r1-confg]?
.!!
851 bytes copied in 5.724 secs (149 bytes/sec)
R1#
```

به مانند شکل ۵۲-۱۲، اگر وارد محل ذخیره‌سازی TFTP سرور شوید فایل r1-confg را مشاهده می‌کنید که به درستی در آن محل ذخیره شده است.



شکل ۵۲-۱۲ تنظیمات GNS3

حالا برای اینکه بتوانیم فایل r1-Config را دوباره در روتر Load کنیم باید از دستورات زیر استفاده کنیم:

در دستور اول باید TFTP و بعد از آن running-config را وارد کنید و در قسمت دوم هم باید آدرس سرور TFTP و در قسمت سوم هم باید نام فایلی که قرار است Load شود را وارد کنید که به مانند زیر دستورات به درستی اجرا می‌شوند.

```
R1#copy tftp: running-config
Address or name of remote host []? 192.168.5.251
Source filename []? r1-confg
Destination filename [running-config]?
Accessing tftp://192.168.5.251/r1-confg...
Loading r1-confg from 192.168.5.251 (via FastEthernet0/0): !
[OK - 851 bytes]

851 bytes copied in 0.280 secs (3039 bytes/sec)
R1#
*May  2 08:02:13.099: %SYS-5-CONFIG_I: Configured from tftp://192.168.5.251/r1-confg by console
R1#
```

www.takbook.com

REDUNDANCY PROTOCOL ۱۲-۴-۳

یکی از بزرگترین مشکلاتی که می‌تواند در شبکه رخ دهد خاموش شدن روتر در شبکه است که با این کار کل شبکه از کار می‌افتد و مقدارس زمان می‌برد تا دستگاه مورد نظر اصلاح شود و دوباره به چرخه بازگردد.

شما به عنوان مدیرشبکه باید تنظیماتی را برای رفع این مشکل انجام دهید تا دیگر شاهد چنین مشکلاتی نباشید.

برای حل این مشکل باید از پروتکل‌هایی که برای این منظور طراحی شده استفاده کنید، پروتکل‌هایی که در این بخش بررسی می‌کنیم، HSRP, GLBP, VRRP است.

HSRP (Hot Standby Router Protcol) ۱۲-۴-۳-۱

اگر شما مدیرشبکه هستید، همیشه سعی کنید Redundancy یا اطمینان کار را در شبکه‌ی خود حفظ کنید. این پروتکل که از ساخته‌های شرکت سیسکو است، با عنوان HSRP به شما این قابلیت را می‌دهد که چند روتر را در یک مجموعه قرار دهید و یکی از این روترها را که روتر اصلی است Active Router، یکی دیگر از روترها به عنوان Standby Router و بقیه‌ی روترها را به عنوان آماده به کار در نظر می‌گیریم. این روترها به عنوان Defualt Gateway کلاینت‌ها در نظر گرفته می‌شوند. اگر زمانی روتری از کار بیفتد، روتر دیگر جایگزین آن می‌شود و باعث ادامه‌ی کار شبکه می‌شود. پورت مربوط به این پروتکل، UDP 1985 است و از آدرس MultiCast، 224.0.0.2 برای انتقال اطلاعات استفاده می‌کند. شماره‌ی گروه آن از ۰ تا ۲۵۵ قابل تخصیص است.

برای انتخاب روتر اصلی در HSRP از Priority استفاده می‌کنند که عددی بین 0-255 است که البته روی همه‌ی روترها و سوئیچ‌های لایه‌ی ۳، 100 است که در صورت برابر بودن Priority، انتخاب روتر Active از روی شماره‌ی ip بزرگ‌تر است.

روترهای Standby، روترهایی هستند که فقط به پیغام‌های روترهای Active که هر ۳ ثانیه ارسال می‌شود، گوش می‌دهند و اگر در مدت 10 ثانیه Hello Packet از طرف روتر Active به روتر Standby نرسد، این روتر فرض می‌کند که روتر Active از کار افتاده و خود را به عنوان روتر Active، فعال می‌کند.

زمان Hold برابر ۱۰ ثانیه است.

می‌توانیم با دستور زیر، زمان‌های Hello و Hold را تغییر دهیم:

SW1 (confing – if)#**standby 1 timers 10 15**

در این دستور Hello برابر ۱۰ و Hold برابر ۱۵ است.

زمانی که روی یک روتر پروتکل HSRP را فعال می‌کنیم در چند حالت قرار می‌گیرد:

1- Disable
2- Init

www.takbook.com

3- Listen
4- Speak
5- Standby
6- Active

هرگاه در یک شبکه، یک روتر به‌عنوان روتر Active شناخته شود و شما روتر دیگری به شبکه با تنظیمات و Priority بهتر متصل کنید، این روتر به‌عنوان Active انتخاب نمی‌شود، اما با دستور زیر می‌توان روتر جدید را به عنوان Active روتر انتخاب کرد.

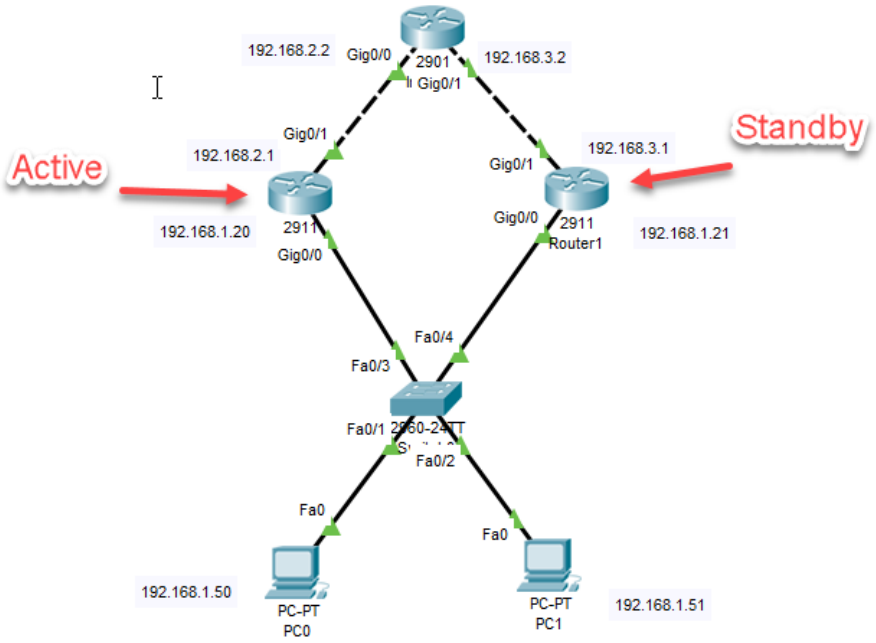
```
R1(config-if)# Standby 1 Preempt
```

این دستور، Active بودن یک روتر را از آن پس می‌گیرد و به روتر دیگر می‌دهد که Priority بهتری دارد.

مثال HSRP

به مانند شکل ۵۳-۱۲، کلاینت‌ها از طریق یک سوئیچ و بعدازآن از طریق روتر وارد اینترنت می‌شوند. در این سناریو دو روتر که به سوئیچ متصل هستند، نقش HSRP را بازی می‌کنند و یکی از روترها به عنوان Active و روتر دیگر به عنوان Standby در نظر گرفته می‌شود و Defualt Gateway را برای کلاینت‌ها مشخص می‌کنند که اگر زمانی یک روتر از کار افتاد روتر دیگر جایگزین می‌شود.

در packet Tracer، شکل ۵۳-۱۲، را ایجاد کنید و کابل‌های مورد نظر را به هم متصل کنید.



شکل ۵۳-۱۲ مثال HDRP

وارد روتر Router0 می‌شویم و تنظیمات مربوط به HSRP را انجام می‌دهیم:

```
Router(config)#interface gigabitEthernet 0/0
Router(config-if)#standby 1 ip 192.168.1.1
Router(config-if)#standby 1 priority 150
%HSRP-6-STATECHANGE: GigabitEthernet0/0 Grp 1 state Speak -> Standby
```

www.takbook.com


```
%HSRP-6-STATECHANGE: GigabitEthernet0/0 Grp 1 state Standby -> Active
Router(config-if)#standby 1 track gigabitEthernet 0/0
```

در دستور اول وارد اینترفیس gigabitEthernet 0/0 شوید، یک آدرس برای این Interface در نظر بگیرید، بعدازآن باید HSRP را با دستور Standby فعال کنید. برای این کار، دستور standby 1 ip 192.168.1.1 را وارد می‌کنیم شماره‌ی ۱ نام گروه مورد نظر است و آدرس 192.168.1.1 هم آدرس DG(Defualt Gateway) است، یعنی روتر روی این آدرس، نقش Defult Gateway را بازی می‌کند. برای این‌که این روتر به‌عنوان روتر اصلی در نظر گرفته شود، باید مقدار priority آن که به صورت پیش‌فرض ۱۰۰ است را به ۱۵۰ تغییر دهیم. بعد از تغییر priority به روتر با دستور Standby 1 preempt می‌گوییم که سریع‌تر به حالت Active سوئیچ کند، مثلاً اگر شما دو روتر داشته باشید، اولی Active باشد و روتر دیگر، standby. اگر Priority روتری که standby است را به ۱۵۰ تغییر دهیم، در حالت کلی باید به روتر Active تغییر کند، اما این کار انجام نمی‌شود. برای حل این مشکل از دستور preempt استفاده می‌کنیم تا حالت Active را از روتر اولی بگیرد و به روتر دومی دهد.

همانطور که در دستورات مشاهده می‌کنید دو پیغام برای تعییر حالت از Standby به Active را مشاهده می‌کنید.

در دستور standby 1 track gigabitEthernet 0/0 در یک فاصله‌ی زمانی مشخص، پورت gigabitEthernet 0/0 توسط Track، Ping می‌شود تا از فعال بودن آن با خبر شود. به محض این‌که لینک مورد نظر down شد. روتر Active تغییر می‌کند و به روتر دیگر داده می‌شود.

در روتر Router0 هم، مانند روتر قبلی همین کار را انجام می‌دهیم:

```
Router(config)#int gigabitEthernet 0/0
Router(config-if)#standby 1 ip 192.168.1.1
Router(config-if)#standby 1 preempt
Router(config-if)#
%HSRP-6-STATECHANGE: GigabitEthernet0/0 Grp 1 state Speak -> Standby
Router(config-if)#standby 1 track gigabitEthernet 0/0
```

در این روتر هم، مانند روتر Router0 دستورات را وارد کردیم. در این روتر نیز از DG، 192.168.1.1استفاده کردیم و از دستور Preempt هم برای تغییر وضعیت سریع استفاده کردیم، که بعد از آن یک پیغام ظاهر شده است که نشان دهنده‌ی Standby بودن این روتر است که با رنگ سبز مشخص کردیم.

با دستور show standby می‌توانید اطلاعات مربوط به HSRP روی روتر مورد نظر را مشاهده کنید، وارد روتر Router0 شوید و این دستور را اجرا کنید؛ اگر به نتیجه دستور توجه کنید روترRouter0 به عنوان روتر Active در نظر گرفته شده است و در قسمت آخر هم مشخص کرده که روتر با آدرس 192.168.1.21 که همان روتر Router1 است به عنوان Standby روتر انتخاب شده است.

```
Router#show standby
```

www.takbook.com


```
GigabitEthernet0/0 - Group 1
State is Active
state changes, last state change 00:26:47 ۱۳
Virtual IP address is 192.168.1.1
Active virtual MAC address is 0000.0C07.AC01
Local virtual MAC address is 0000.0C07.AC01 (v1 default)
Hello time 3 sec, hold time 10 sec
Next hello sent in 2.263 secs
Preemption enabled
Active router is local
Standby router is 192.168.1.21, priority 100 (expires in 8 sec)
Priority 150 (configured 150)
Track interface GigabitEthernet0/0 state Up decrement 10
  Group name is hsrp-Gig0/0-1 (default)
```

با دستور show Standby Brife، می‌توانید اطلاعات سریع در مورد Active و Standby بودن روتر را به دست بیاورید:

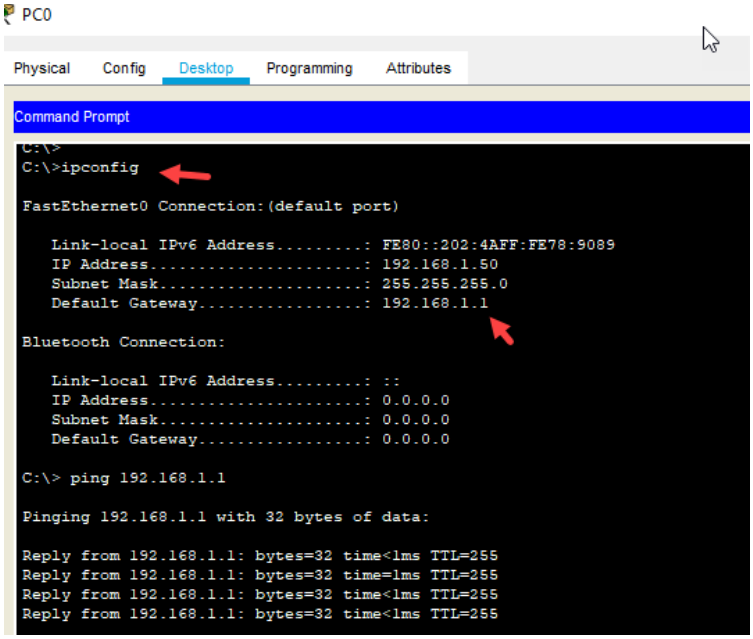
```
Router#show standby brief
                P indicates configured to preempt.
                |
Interface   Grp  Pri P  State   Active      Standby        Virtual IP
Gig0/0       1    150 P Active   local       192.168.1.21   192.168.1.1
```

در حال حاضر روتر Router0 به عنوان Active و روتر Router1 به‌عنوان standby روتر است. زمانی که روتر Router0 از شبکه خارج شود، روتر Router1 جایگزین می‌شود. به این حالت، Redundancy می‌گویند که اطمینان کارایی شبکه را بالا می‌برد.

برای تست این موضوع وارد PC0 شوید و دستور زیر را وارد کنید:

با دستور ipconfig آدرس IP مربوط به PC0 و DG آن را که 192.168.1.1 است را در شکل ۵۴-۱۲ مشاهده می‌کنید.

www.takbook.com

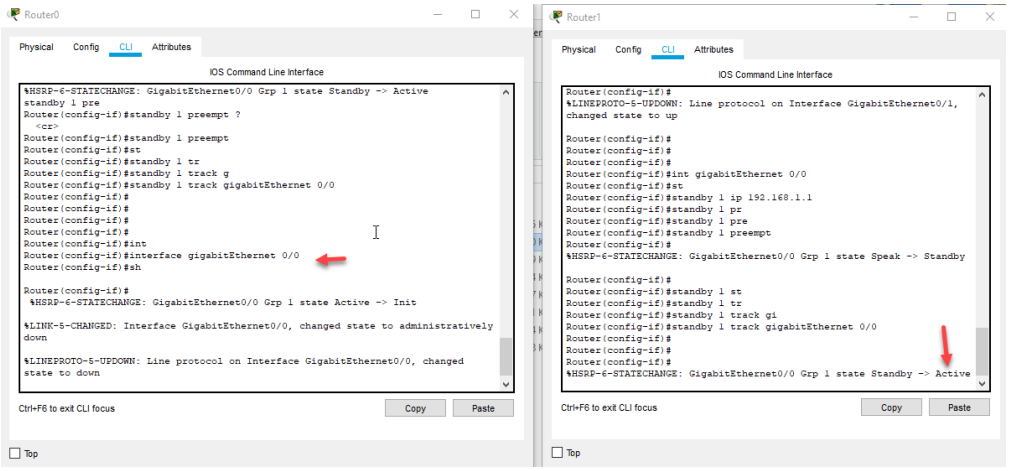


شکل ۵۴-۱۲ تنظیمات PC0

حالا اگر Router0 از شبکه خارج شود باید روتر Active به روتر Router0 نغییر کند، برای انجام این کار وارد Router0 شوید و دستور زیر را وارد کنید:

Router(config-if)#**interface gigabitEthernet 0/0**
Router(config-if)#**sh**

همانطور که در شکل ۵۵-۱۲، مشاهده می‌کنید Interface GigaEthernet 0/0 مربوط به روتر Router0 را خاموش کردیم با این کار روتر Router1 به حالت Active تغییر حالت داده است.



شکل ۵۵-۱۲ تنظیمات روتر

www.takbook.com

در HSRP می‌توانیم روش‌های امنیتی را به کار ببریم که کسی بدون اجازه وارد این شبکه نشود و خودش را به عنوان یک روتر HSRP معرفی نکند.
دو مدل Authentication در HSRP وجود دارد.

۱- Plain Text:

در این روش، امنیت از طریق یک کلمه که می‌تواند حداکثر ۸ کاراکتر باشد، صورت گیرد:

Sw1 (Config-if)# **Standby 1 Authentication babajani**

در هر دو روتر باید این دستور را وارد کنید که در اینجا، کلمه‌ی babajani به‌عنوان رمز عبور برای هر دو روتر است و اگر در هر روتر رمز برقرار باشد، ارتباط برقرار می‌شود، امنیت این روش بسیار پائین بوده و به راحتی توسط نرم‌افزارهای Snif مانند WireShark قابل مشاهده خواهد بود.

۲- MD5:

در این روش که از طریق Hash کردن اطلاعات صورت می‌گیرد، خیلی قوی‌تر و بهتر از روش قبلی است.

Sw1 (Config-if)# **Standby 1 Authentication md5 key-string saman**

این نکته را هم در نظر داشته باشید که دستورات رمزنگاری روی نرم‌افزار Packet Tracer، تعریف نشده و شما باید در نرم‌افزارهای دیگر، مانند GNS3 آنها را اجرا کنید.پ

۲-۳-۴-۱۲ GLBP (Gateway Load Balancing Protocol)

این پروتکل، نسخه‌ی بهبودیافته‌ی پروتکل HSRP است که توسط شرکت سیسکو ارائه شده است و برای Load balancing استفاده می‌شود. کار اصلی این پروتکل به این صورت است که چند روتر در یک Subnet قرار دارند و باید مانند قبل، روی یک IP نقش Defualt Gateway را بازی کنند. روتری که Priority آن بالاتر باشد، می‌شود Active Forwarder، کار این روتر این است که اگر کلاینتی درخواستی به سمت این روتر ارسال کند، این روتر Mac address یکی از روترهایی که در همان گروه قرار دارد را برای کلاینت ارسال می‌کند و در دفعه‌ی بعد، Mac روتر دیگر را می‌فرستد که این کار توسط الگوریتم‌های زیر انجام می‌پذیرد:

الگوریتم Round Robin:

به صورت گردشی عمل می‌کند و به صورت پیش‌فرض فعال است.

الگوریتم Weighted:

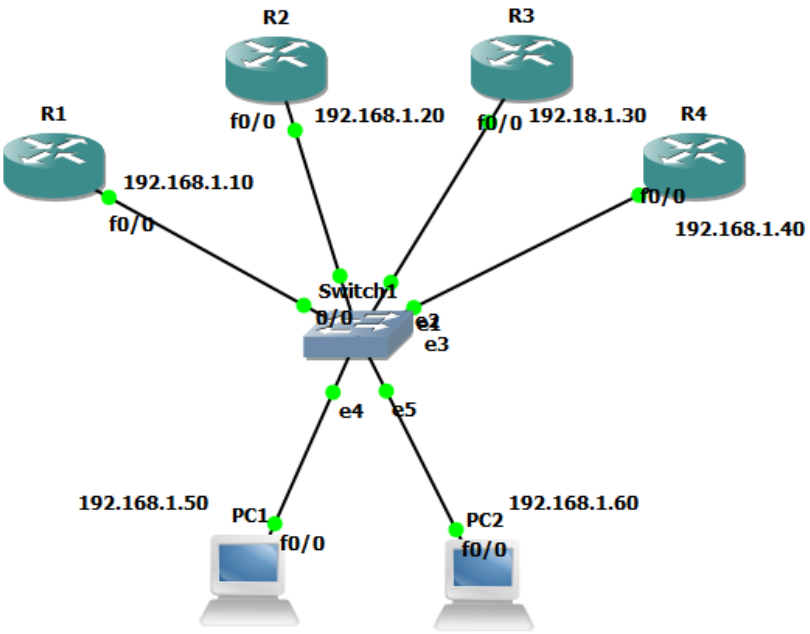
www.takbook.com

این الگوریتم بار کاری را به صورت مساوی بین روترها تقسیم می‌کند.

الگوریتم Host-Dependent:

در این الگوریتم از طریق Access List به روتر می‌گوییم که این کلاینت‌ها از روتر خاصی استفاده کنند.

مثالی از این پروتکل:



شکل ۵۶-۱۲ مثال GLBP

در این مثال، روتر R1 به عنوان روتر Active انتخاب می‌شود و بقیه، به عنوان روتر Standby می‌باشند.

وقتی کلاینت درخواستی را می‌فرستند، در مرحله‌ی اول به روتر R1 می‌رسد و بعد، این روتر Mac address یکی از روترهای گروه خود را به کلاینت مورد نظر می‌دهد و به کلاینت بعدی Mac address روتر دیگر را می‌دهد و همین‌طور ادامه خواهد داشت. در صورت غیرفعال شدن روتر اصلی، روتر دیگر در گروه مورد نظر به جای آن قرار می‌گیرد.

این پروتکل در Packet Tracer پشتیبانی نمی‌شود که برای اجرای آن به صورت مجازی از نرم‌افزار GNS3 در این قسمت استفاده می‌کنیم.

توجه داشته باشید که Interface روتر باید توانایی دریافت چند MAC Address هم زمان را داشته باشد؛ اگر از GNS3 استفاده می‌کنید بهتر است از IOS داخل نرم‌افزار GNS استفاده کنید و از IOU که به صورت VMware Workstation اجرا می‌شود استفاده نکنید.

www.takbook.com

قبل از بررسی سناریو بالا باید Key-Chain را با هم بررسی کنیم، این قابلیت به شما این امکان را می‌دهد که بتوانید برای ایجاد رمز عبور از Life Time استفاده کنید، این بدان معنا است که می‌توانید مشخص کنید که رمز عبور شما تا چه زمانی کارایی داشته باشد و انقضاء شود.

برای ایجاد Key-Chain به صورت زیر عمل کنید:

با دستور زیر یک دسته کلید با نام chain-1 ایجاد می‌کنیم:

```
R1(config)#key chain chain-1
```

در ادامه باید یک Key ایجاد کنیم که شماره‌ی آن از 0 تا 2147483647 متغیر است، توجه داشته باشید در یک دسته کلید می‌توانید چندین Key ایجاد کنید تا امنیت افزایش یابد.

```
R1(config-keychain)#key ?
  <0-2147483647>  Key identifier
R1(config-keychain)#key 20
```

بعد از ایجاد Key با شماره‌ی 20 باید برای آن یک رمز عبور پیچیده در نظر بگیرید که دستور آن به صورت زیر است:

```
R1(config-keychain-key)#key-string Test@12345
```

بعد از ایجاد Key با شماره‌ی 20 و فرار دادن رمز عبور برای آن یک Key دیگر با شماره‌ی 30 برای آن ایجاد می‌کنیم و یک رمز عبور هم برای آن در نظر می‌گیریم

```
R1(config-keychain-key)#key 30
R1(config-keychain-key)#key-string Test@54321
R1(config-keychain-key)#exit
```

Key-chain را باید برای هر چهار روتر ایجاد کنید و بعد در پروتکل GLBP استفاده کنید.

برای فعال‌سازی GLBP هم باید به صورت زیرعمل کنید:

وارد روتر R1 شوید و دستورات زیر را وارد کنید:

وارد Interface FastEthernet 0/0 که به سمت شبکه داخلی است می‌شویم و برای آن IP Address را مشخص می‌کنیم.

```
R1(config)#int fastEthernet 0/0
R1(config-if)#ip address 192.168.1.10 255.255.255.0
R1(config-if)#no sh
```

بعد از فعال‌سازی IP و روشن کردن پورت دستورات زیر را برای GLBP اجرا کنید:

```
R1(config-if)#glbp 1 ip 192.168.1.1
R1(config-if)#glbp 1 priority 150
R1(config-if)#glbp 1 preempt
R1(config-if)#glbp 1 authentication md5 key-chain chain-1
```

www.takbook.com

همان‌طور که مشاهده می‌کنید، مانند پروتکل قبلی یک Defualt Gateway با آدرس 192.168.1.1 مشخص کردیم که روی این آدرس روترها کار خواهند کرد، بقیه دستورات به مانند قبل است با این تفاوت که Authentication از نوع MD5 هم به آن اضافه شده است و در آخر Key-Chain که با نام chain-1 ایجاد کردیم را به آن اضافه می‌کنیم.

در بقیه روترها هم باید همین دستورات را وارد کنید.

تنظیمات روتر R2:

```
R2(config)#key chain chain-1
R2(config-keychain)#key 20
R2(config-keychain-key)#key-string Test@12345
R2(config-keychain-key)#key 30
R2(config-keychain-key)#key-string Test@54321
R2(config-keychain)#exit

R2(config)#int fastEthernet 0/0
R2(config-if)#ip address 192.168.1.20 255.255.255.0
R2(config-if)#no sh

R2(config-if)#glbp 1 ip 192.168.1.1
R2(config-if)#glbp 1 preempt
R2(config-if)#glbp 1 authentication md5 key-chain chain-1
```

تنظیمات روتر R3:

```
R2(config)#key chain chain-1
R2(config-keychain)#key 20
R2(config-keychain-key)#key-string Test@12345
R2(config-keychain-key)#key 30
R2(config-keychain-key)#key-string Test@54321
R2(config-keychain)#exit

R2(config)#int fastEthernet 0/0
R2(config-if)#ip address 192.168.1.30 255.255.255.0
R2(config-if)#no sh

R2(config-if)#glbp 1 ip 192.168.1.1
R2(config-if)#glbp 1 preempt
R2(config-if)#glbp 1 authentication md5 key-chain chain-1
```

تنظیمات روتر R4:

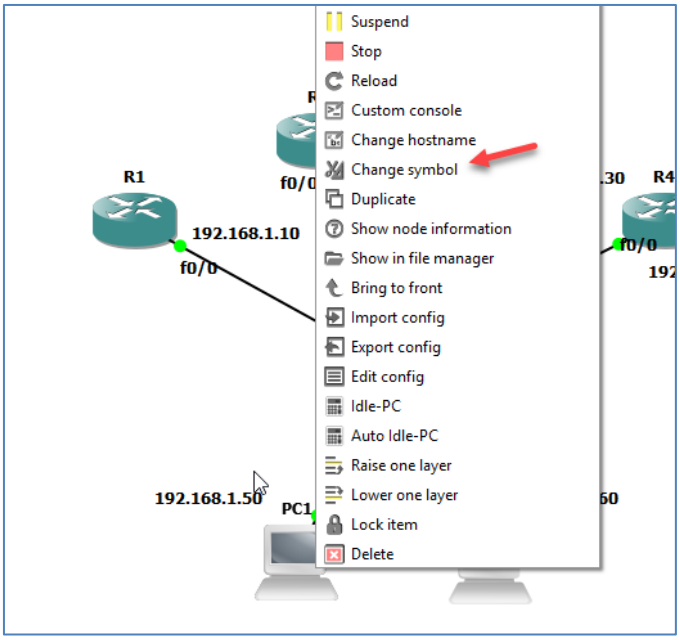
```
R2(config)#key chain chain-1
R2(config-keychain)#key 20
R2(config-keychain-key)#key-string Test@12345
R2(config-keychain-key)#key 30
R2(config-keychain-key)#key-string Test@54321
R2(config-keychain)#exit
```

www.takbook.com


```
R2(config)#int fastEthernet 0/0
R2(config-if)#ip address 192.168.1.40 255.255.255.0
R2(config-if)#no sh

R2(config-if)#glbp 1 ip 192.168.1.1
R2(config-if)#glbp 1 preempt
R2(config-if)#glbp 1 authentication md5 key-chain chain-1
```

با این کار توانستیم پروتکل GLBP را راه‌اندازی کنیم و روترهای می‌توانند روی آدرس مجازی 192.168.1.1 عملیات متصل شدن به DG را انجام دهند.

برای تست این پروتکل باید وارد PC شویم و تنظیمات را بر روی آنها اعمال کنیم؛ توجه داشته باشید که در GNS3 از دو روتر به جای PC استفاده کردیم و به مانند شکل ۵۷-۱۲، فقط Symbol آنهارا به PC تغییر دادیم.



شکل ۵۷-۱۲ تنظیمات GNS3

وارد PC1 شوید و دستورات زیر را وارد کنید:

```
PC1(config)#interface fastEthernet 0/0
PC1(config-if)#ip address 192.168.1.50 255.255.255.0
PC1(config-if)#no sh
```

www.takbook.com

بعد از وارد کردن IP Address برای PC1 باید برای آن Default Gateway را مشخص کنید:

PC1(config)#**ip default-gateway 192.168.1.1**

برای تست برقراری ارتباط با روترها باید یک Ping به آدرس 192.168.1.1 بزنیم، سعی کنید یک Repeat هم برای آن در نظر بگیرید:

PC1#**ping 192.168.1.1 repeat 2000**

با دستور بالا ۲۰۰۰ بار دستور Ping ادامه پیدا می‌کند و در این زمان می‌توانید روترها را خاموش کنید و پروتکل GLBP را تست بگیرید؛ همانطور که مشاهده می‌کنید بدون یک قعطی کار Ping ادامه پیدا کرد.

```
PC1#ping 192.168.1.1 repeat 2000
Type escape sequence to abort.
Sending 2000, 100-byte ICMP Echos to 192.168.1.1, timeout is 2 seconds:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
```

www.takbook.com


```
Redirect time 600 sec, forwarder time-out 14400 sec
Authentication MD5, key-chain "chain-1" (دسته کلید مشخص شده است)
Preemption enabled, min delay 0 sec
Active is local(همین روتر یعنی روتر یک به عنوان روتر اکتیو انتخاب شده است)
Standby is 192.168.1.40, priority 100 (expires in 9.504 sec)
Priority 150 (configured)
Weighting 100 (default 100), thresholds: lower 1, upper 100
Load balancing: round-robin
Group members: (در این قسمت اعضای این گروه را مشاهده می‌کنید که دارای آدرس مک جدا هستند)
  ca01.31e8.0000 (192.168.1.10) local
  ca02.30a0.0000 (192.168.1.20) authenticated
  ca03.060c.0000 (192.168.1.30) authenticated
  ca04.2e88.0000 (192.168.1.40) authenticated
There are 4 forwarders (1 active)
Forwarder 1 (اولین روتری که بعد از غیر فـال شدن روتر اکتیو فعال می‌شود )
  State is Listen
    2 state changes, last state change 01:21:05
  MAC address is 0007.b400.0101 (learnt)
  Owner ID is ca04.2e88.0000
  Redirection enabled, 599.520 sec remaining (maximum 600 sec)
  Time to live: 14399.520 sec (maximum 14400 sec)
  Preemption enabled, min delay 30 sec
  Active is 192.168.1.40 (primary), weighting 100 (expires in 10.720 sec)
  Arp replies sent: 1
Forwarder 2
  State is Active
    3 state changes, last state change 00:22:13
  MAC address is 0007.b400.0102 (default)
  Owner ID is ca01.31e8.0000
  Redirection enabled
  Preemption enabled, min delay 30 sec
  Active is local, weighting 100
  Arp replies sent: 1
Forwarder 3
  State is Listen
  MAC address is 0007.b400.0103 (learnt)
  Owner ID is ca02.30a0.0000
  Redirection enabled, 598.176 sec remaining (maximum 600 sec)
  Time to live: 14398.176 sec (maximum 14400 sec)
  Preemption enabled, min delay 30 sec
  Active is 192.168.1.20 (primary), weighting 100 (expires in 9.536 sec)
Forwarder 4
  State is Listen
  MAC address is 0007.b400.0104 (learnt)
  Owner ID is ca03.060c.0000
  Redirection enabled, 597.536 sec remaining (maximum 600 sec)
  Time to live: 14397.536 sec (maximum 14400 sec)
  Preemption enabled, min delay 30 sec
  Active is 192.168.1.30 (primary), weighting 100 (expires in 8.832 sec)
```

www.takbook.com

با دستور زیر هم می‌توانید مشخص کنید که روتر Active و Standby کدام هستند:

```
R1#show glbp brief
Interface   Grp  Fwd Pri State    Address         Active router   Standby router
Fa0/0       1    -   150 Active   192.168.1.1     local           192.168.1.40
Fa0/0       1    1   -   Listen   0007.b400.0101  192.168.1.40–
Fa0/0       1    2   -   Active   0007.b400.0102  local–
Fa0/0       1    3   -   Listen   0007.b400.0103  192.168.1.20–
Fa0/0       1    4   -   Listen   0007.b400.0104  192.168.1.30–
```

۱۲-۴-۳-۳ VRRP (Virtual Router Redundancy Protocol)

این پروتکل کاملاً شبیه به HSRP است. شماره‌ی گروه در این پروتکل از ۰ تا ۲۵۵ و شماره‌ی Priority از ۰ تا ۲۵۴ است. روتر اصلی به‌عنوان روتر Master در نظر گرفته می‌شود و روترهای فرعی به‌عنوان Backup در نظر گرفته می‌شود. این پروتکل مربوط به سازمان IETF است.

این پروتکل از آدرس 224.0.0.18 استفاده می‌کند و پروتکلی که با آن کار می‌کند، IP Protocol با شماره‌ی پورت 112 است. این پروتکل در هر ۱ ثانیه، پیام‌های خود را ارسال می‌کند و دستور Preempt هم به صورت پیش‌فرض بر روی این پروتکل فعال است.

شاید در شبکه‌ی خود از دستگاه‌هایی غیر از دستگاه‌های شرکت سیسکو استفاده کنید که برای Redundancy حتماً باید از این پروتکل استفاده کنید.

دستورات، کاملاً شبیه به HSRP است. فقط به جای قرار دادن کلمه‌ی HSRP، کلمه‌ی VRRP را جایگزین کنید.

۱۲-۵ سوالات فصل دوازدهم

1. What level of logging to the console is the default for a Cisco device?
سطح Logging به صورت پیش‌فرض برای دستگاه‌های سیسکو چیست؟

a. Informational
b. Errors
c. Warnings
d. Debugging

www.takbook.com

2. What command limits the messages sent to a syslog server to levels 4 through 0?
چه دستوری پیام‌های ارسالی به یک سرور Syslog را به ۰ تا ۴ محدود می‌کند؟

a. logging trap 0-4
b. logging trap 0,1,2,3,4
c. logging trap 4
d. logging trap through 4

3. Which of the following is accurate about the NTP client function on a Cisco router?
کدام یک از موارد زیر در مورد NTP Client درست‌تر است؟

a. The client synchronizes its time-of-day clock based on the NTP server.
b. It counts CPU cycles of the local router CPU to more accurately keep time.
c. The client synchronizes its serial line clock rate based on the NTP server.
d. The client must be connected to the same subnet as an NTP server.

4. The only NTP configuration on router R1 is the ntp server 10.1.1.1 command. Which answers describe how NTP works on the router?
تنها تنظیماتی که برای NTP در روتر انجام شده دستور NTP 10.1.1.1 است، کدام یک از گزینه‌های زیر نحوه‌ی عملکرد سرویس NTP را توصیف می‌کند؟

a. As an NTP server only
b. As an NTP client only
c. As an NTP server only after the NTP client synchronizes with NTP server 10.1.1.1
d. As an NTP server regardless of whether the NTP client synchronizes with NTP server 10.1.1.1

5. Imagine that a switch connects through an Ethernet cable to a router, and the router's host name is Hannah. Which of the following commands could tell you information about the IOS version on Hannah without establishing a Telnet connection to Hannah? (Choose two answers.)
تصور کنید که سوئیچ از طریق کابل Ethernet به روتر متصل شده است و نام روتر هم Hannah است، کدام یک از دستورات زیر می‌تواند بدون اتصال Telnet با Hannah اطلاعاتی در مورد نسخه‌ی IOS در Hannah بدهد؟(دو گزینه را انتخاب کنید)

a. show neighbors Hannah
b. show cdp
c. show cdp neighbors
d. show cdp neighbors Hannah
e. show cdp entry Hannah
f. show cdp neighbors detail

6. A switch is cabled to a router whose host name is Hannah. Which of the following LLDP commands could identify Hannah's model of hardware? (Choose two answers.)
با یک سوئیچ به روتری متصل شده‌ایم که نام آن Aryan است، کدام یک از دستورات LLDP زیر می‌تواند مدل سخت‌افزاری Aryan را نشان دهد؟ (دو گزینه را انتخاب کنید)

a. show neighbors
b. show neighbors Aryan
c. show lldp
d. show lldp interface
e. show lldp neighbors
f.show lldp entry Aryan

www.takbook.com

7. Which command provides this output?

کدام یک از دستورات زیر خروجی شکل ۵۹-۱۲، است؟

```
Router#
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S -Switch, H - Host, I - IGMP, r - Repeater, P - Phone,
                  D - Remote, C - CVTA, M - Two-port Mac Relay

Device ID      Local Interface Holdtime  Capability  Platform    Port ID
10.1.1.2       Gig 37/3        176          R I      CPT 600     Gig 36/41
10.1.1.2       Gig 37/1        174          R I      CPT 600     Gig 36/43
10.1.1.2       Gig 36/41       134          R I      CPT 600     Gig 37/3
10.1.1.2       Gig 36/43       134          R I      CPT 600     Gig 37/1
10.1.1.2       Ten 3/2         132          R I      CPT 600     Ten 4/2
10.1.1.2       Ten 4/2         174          R I      CPT 600     Ten 3/2
```

شکل ۵۹-۱۲ خروجی دستور

a. show ip route
b. show cdp neighbor
c. show ip interface
d. show interface

www.takbook.com

www.takbook.com

www.takbook.com

فصل سیزدهم

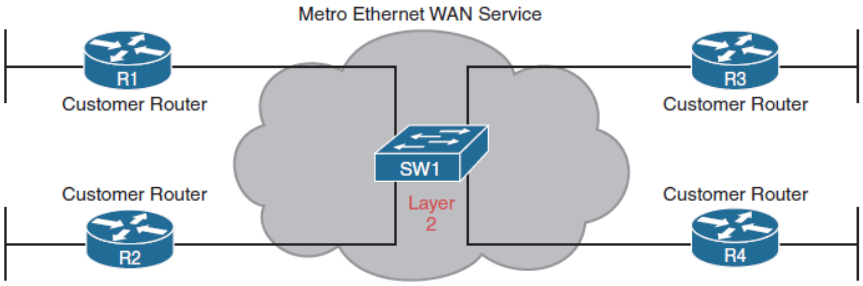
معماری شبکه

۱۳-۲ معماری WAN

۱۳-۲-۱ بررسی Metro Ethernet

Metro Ethernet (MetroE) انواع خدمات WAN را به مشتریان ارائه می‌دهد، سرویس MetroE از پیوندهای فیزیکی Ethernet برای اتصال دستگاه مشتری به دستگاه ارائه دهنده‌ی خدمات استفاده می‌کند. توجه داشته باشید این سرویس یک سرویس لایه‌ی دوم است که در آن سرویس دهنده‌ی WAN فریم‌های اترنت را از یک دستگاه مشتری به دیگری منتقل می‌کند.

در شکل ۱۲-۱۳، چهار سایت مختلف در یک شرکت را مشاهده می‌کنید که این سایت‌ها می‌توانند در یک شهر پخش باشند و توسط یک سوئیچ لایه‌ی دوم و با استفاده از سرویس Metro Ethernet در بستر WAN به هم متصل شده‌اند، اصولاً ارتباط این سایت‌ها توسط فیبر نوری انجام می‌شود.



شکل ۱۲-۱۳ Metro Ethernet

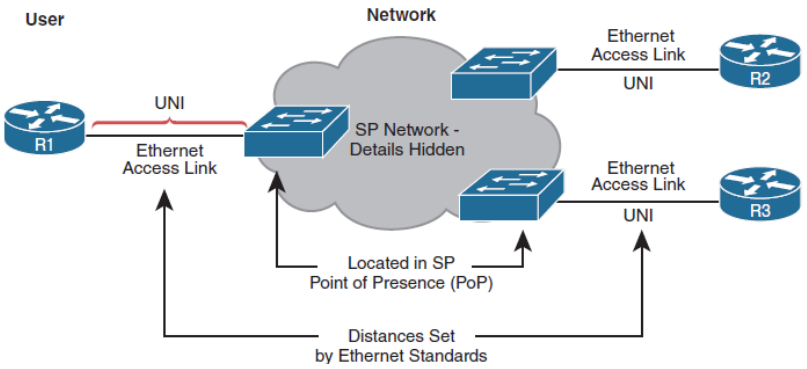
طراحی و توپولوژی Metro Ethernet

از دیدگاه سازمانی برای استفاده از سرویس Metro Ethernet هر سایت یک سازمان، باید حداقل یک لیک برای ارتباط با این سرویس داشته باشد.

نیازی به اتصال هر روتر سازمانی به یک روتر دیگر به طور مستقیم در آن سازمان نیست و این ارتباط به مانند شکل ۱۲-۱۳، خواهد بود.

www.takbook.com

سازمان‌های ارئه دهنده‌ی خدمات شبکه، سعی می‌کنند تا حد امکان دستگاه‌ها یا همان سوئیچ‌های خود را به سایت‌های مشتری نزدیک کنند، این موضوع را در شکل ۱۳-۱۳، مشاهده می‌کنید که SPها سعی کردند برای هر سازمان یک سوئیچ برای ارتباط آنها در مسافت نزدیک در نظر بگیرند.



شکل ۱۳-۱۳ Metro Ethernet

در جدول ۱-۱۳، استانداردهای سازمان IEEE را برای شبکه Metro Ethernet مشاهده می‌کنید.

جدول ۱-۱۳ Metro Ethernet

Name	Speed	Distance
100BASE-LX10	100 Mbps	10 Km
1000BASE-LX	1 Gbps	5 Km
1000BASE-LX10	1 Gbps	10 Km
1000BASE-ZX	1 Gbps	100 Km
10GBASE-LR	10 Gbps	10 Km
10GBASE-ER	10 Gbps	40 Km

خدمات و توپولوژی‌های Metro Ethernet

سازمان MEF استانداردهایی را برای Metro Ethernet تعریف کرده است که مربوط به خدمات شبکه‌ی Metro Ethernet است که در جدول ۲-۱۳، مشاهده می‌کنید:

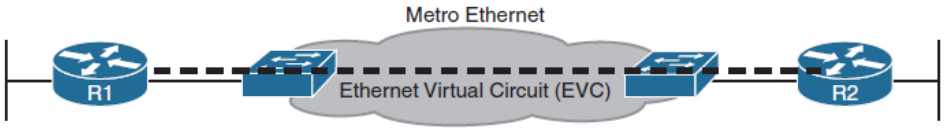
جدول ۲-۱۳ خدمات Metro Ethernet

www.takbook.com

نام سرویس MEF	نام کوتاه شده	توپولوژی استفاده شده	توضیحات
Ethernet Line Service	E-Line	Point-to-point	دو دستگاه مشتری (CPE) می‌توانند فریم‌های Ethernet را که به صورت مفهومی با یک خط leased مشابه هستند، مبادله کنند.
Ethernet LAN Service	E-LAN	Full mesh	این سرویس مانند یک LAN عمل می‌کند ، به این دلیل که همه دستگاه‌ها می توانند فریم‌ها را به تمام دستگاه‌های دیگر ارسال کنند.
Ethernet Tree Service	E-Tree	Hub and spoke; partial mesh; point-to-multipoint	یک سایت مرکزی می‌تواند با مجموعه‌ی مشخصی از سایت‌های از راه دور ارتباط برقرار کند ، اما سایت‌های از راه دور نمی‌توانند مستقیماً با هم ارتباط برقرار کنند.

Ethernet Line Service (Point-to-Point)

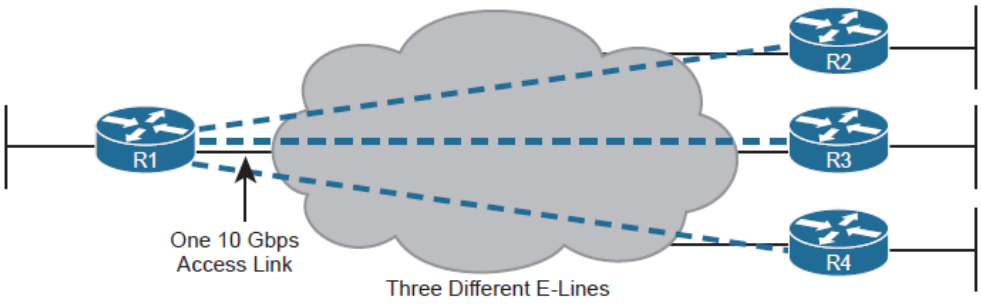
این سرویس یکی از ساده‌ترین سرویس‌ها است که مشتری دو سایت را با لینک‌های دسترسی به هم متصل می‌کند سپس سرویس Metro Ethernet به دو دستگاه اجازه ارسال فریم را می‌دهد، در شکل ۱۴-۱۳، نمونه‌ای از این شبکه را مشاهده می‌کنید.



شکل ۱۴-۱۳ Metro Ethernet

در شکل ۱۵-۱۳، ارتباط یک به چند را در سرویس E-line مشاهده می‌کنید.

www.takbook.com



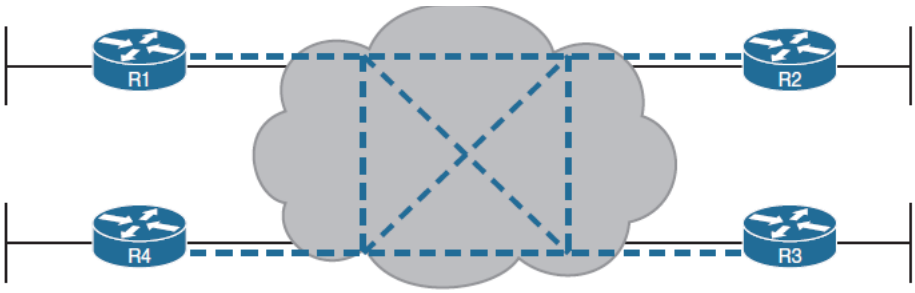
شکل ۱۵-۱۳ *Metro Ethernet*

Ethernet LAN Service (Full Mesh)

یک شرکت را در نظر بگیرید که دارای چندین سایت است و می‌خواهیم از طریق WAN آنها را به هم متصل کنیم، اگر بخواهیم به مانند قسمت قبل از E-Lines استفاده کنیم، مثلاً برای اتصال چهار، پنج و شش سایت شما به ۶، ۱۰ و ۱۵ خط الکترونیکی نیاز دارید فرمول برای محاسبه این خطوط به صورت N(N – 1) / 2 است که مثلاً اگر 20 سایت داشته باشید نیاز به 190 خط الکترونیکی است که این می‌تواند بسیار پرهزینه و زمان‌گیر باشد.

متخصصانی که Metro Ethernet را طراحی کردند به فکر طراحی دیگری با عنوان Ethernet Lan Service و یا همان Full Mesh افتاند که در آن هر دستگاه مستقیم به دستگاه دیگر در سایت دیگر متصل شده است و اجازه‌ی ارسال فریم را دارد.

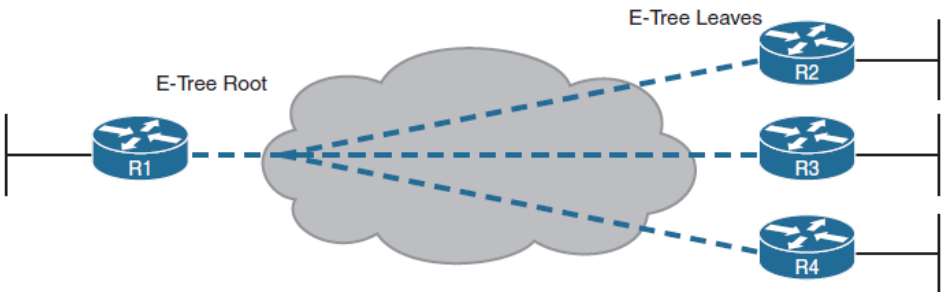
در شکل ۱۶-۱۳، یک شبکه‌ی E-LAN را مشاهده می‌کنید که در آن هر دستگاه در هر سایت مستقیماً می‌تواند با دیگری در ارتباط باشد انگار یک سوئیچ بزرگ در مرکز آن قرار گرفته باشد یعنی اینکه سوئیچ مرکزی (EVC) به هر چهار روتر متصل شده است و به خاطر همین این روترها با هم به صورت مستیقیم در ارتباط هستند و همه‌ی آنها در لایه‌ی سوم شبکه‌ی WAN کار می‌کنند.



شکل ۱۶-۱۳ *Metro Ethernet*

www.takbook.com

در شکل ۱۷-۱۳، شبکه‌ی E-Tree را مشاهده می‌کنید که یک طرح Partial Mesh یا همان مش جزئی است که در آن فقط برخی از روترهای می‌توانند با هم در ارتباط باشند.



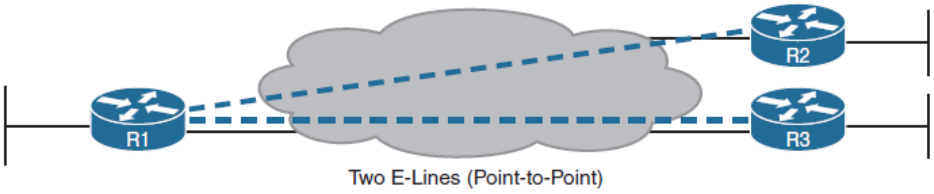
شکل ۱۷-۱۳ شبکه‌ی E-Tree

طراحی لایه‌ی سوم با استفاده از Metro Ethernet

اکنون که شما اصول اولیه خدمات E-Line (نقطه به نقطه)، E-LAN (مش کامل) و E-Tree (point-to-multipoint, hub and spoke) را می‌دانید، در این موضوع برخی از جزئیات طراحی لایه‌ی سوم را هنگام استفاده از خدمات E-Line و E-Tree بررسی می‌کنیم.

در نظر داشته باشید اگر شرکتی از روترها و سوئیچ‌های لایه‌ی سوم استفاده کند مهندسین شبکه چطوری باید آدرس‌های IP و Subnet را تنظیم کنند.

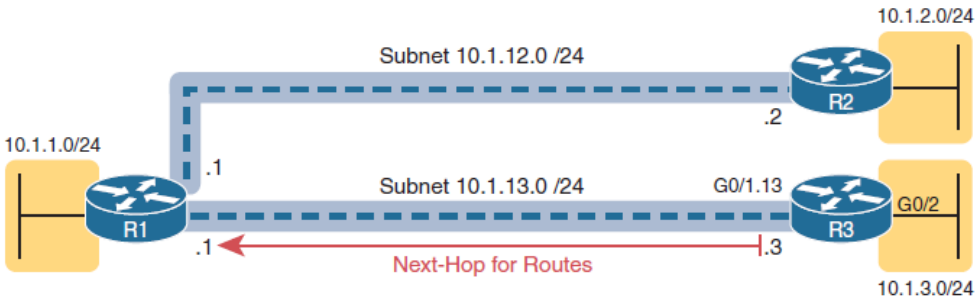
یک شرکت را در نظر بگیرید که به مانند شکل ۱۸-۱۳، از خطوط چندگانه استفاده می‌کند هر یک از این خطوط باید در یک Subnet مجزا قرار داشته باشند.



شکل ۱۸-۱۳ شبکه‌ی E-Tree

شکل ۱۹-۱۳، نحوه صحیح تخصیص IP را به روترها مشخص کرده و در جدول OSPF Routing Table می‌توانید Subnet و Next-hop را مشاهده کنید.

www.takbook.com



R3 Routing Table

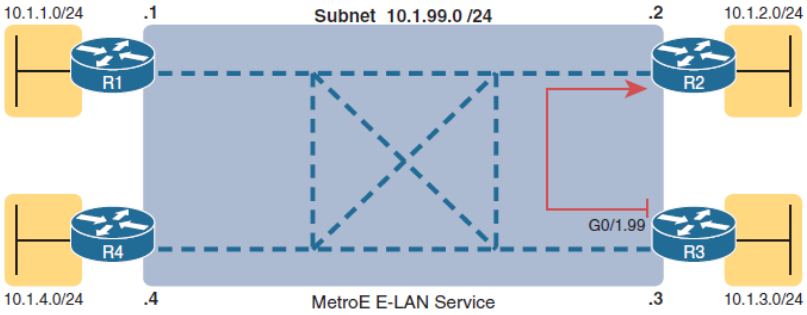
Code	Subnet	Interface	Next-hop
O	10.1.1.0/24	G0/1.13	10.1.13.1
O	10.1.2.0/24	G0/1.13	10.1.13.1
O	10.1.12.0/24	G0/1.13	10.1.13.1
C	10.1.3.0/24	G0/2	N/A
C	10.1.13.0/24	G0/1.13	N/A

شکل ۱۹-۱۳ شبکه‌ی R3 Routing Table

طراحی لایه ۳ با سرویس E-LAN

همانطور که گفتیم در طراحی E-LAN روترها به یک سوئیچ مرکزی متصل می‌شوند و با هم در ارتباط هستند، ولی شما انتظار دارید که آدرس IP در این شبکه در یک Subnet قرار داشته باشد؟

بله تمام روترها در این مجموعه در یک Subnet قرار دارند و می‌توانید از یک پروتکل مسیریابی مانند OSPF هم برای این کار استفاده کنید، این موضوع را در شکل ۲۰-۱۳، مشاهده می‌کنید.



R3 Routing Table (OSPF Routes Only)

Subnet	Interface	Next-hop
10.1.2.0/24	G0/1.99	**10.1.99.2**
10.1.1.0/24	G0/1.99	10.1.99.1
10.1.4.0/24	G0/1.99	10.1.99.4

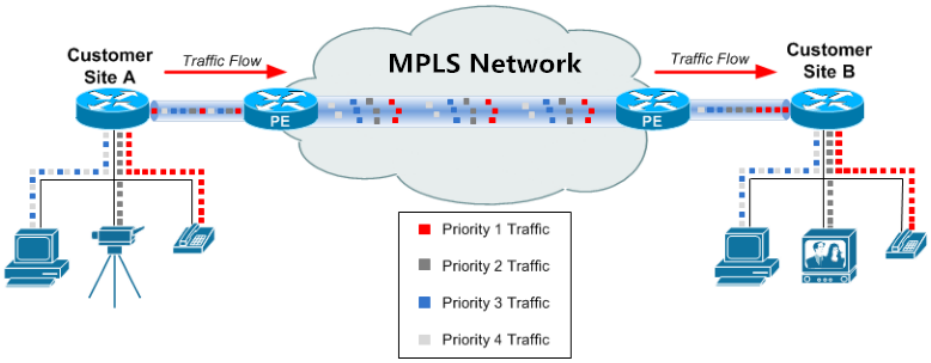
شکل ۲۰-۱۳ شبکه‌ی R3 Routing Table

www.takbook.com

اگر به شکل ۲۰-۱۳، توجه کنید جدول روتر R3 را مشاهده می‌کنید که اولین Next-hop به روتر R2 اشاره دارد و بقیه روترها هم در آن قرار دارند.

۲-۲-۱۳ بررسی Multiprotocol Label Switching (MPLS)

MPLS (Multiprotocol Label Switching) یک تکنولوژی انتقال است، این تکنولوژی چندین سال است که به یک تکنولوژی معروف و محبوب تبدیل شده است. MPLS از یک مکانیزم Label زدن یا برچسب زدن برای ارسال بسته ها در شبکه استفاده می‌کند. در این مقاله می خواهیم این تکنولوژی MPLS را مورد بحث قرار دهیم.



شکل ۲۱-۱۳ Multiprotocol Label Switching (MPLS)

به طور کلی اگر بخواهیم عملکرد MPLS را شرح دهیم عمل سوئچینگ را با استفاده از مکانیزم Label گذاری در بستر روتینگ انجام می‌دهد. یعنی یک بسته در هنگام ورود به شبکه MPLS بر اساس آدرس IPمقصد label گذاری می‌شود و در طول مسیر در لایه دوم و براساس این label هدایت می‌شود تا به مقصد برسد.

MPLS در یک لایه خاص از OSI قرار نمی‌گیرد و عملکرد آن بین لایه‌ی دوم (Data link) و لایه‌ی سوم (Network)قرار می‌گیرد به همین خاطر آن‌را به عنوان یک پروتکل لایه ۲.۵ معرفی می‌کنند.

همانطور که اشاره شده MPLS از مکانیزم Label گذاری روی بسته استفاده می‌کند Labelهای MPLS بین روترها پخش می‌شوند و روترها با استفاده از این labe ها می‌توانند یک نقشه از label های شبکه بدست آورند. این label ها به بسته‌های IP متصل می‌شوند و روترها را قادر می‌سازد که با استفاده از این label ها بدون در نظر گرفتن آدرس IP اقدام به ارسال بسته‌ها کنند. در MPLS بسته‌ها به وسیله Label switching بجای IP switching ارسال می‌شوند.

www.takbook.com

تکنولوژی label switching یک تکنولوژی جدید نیست و شبکه‌های Frame Relay و ATM برای ارسال فریم‌ها و cell ها از آن استفاده می‌کرده‌اند. در Frame Relay و ATM ، در هر hop از شبکه، label تغییر می‌کند و این تفاوت عمده این دو تکنولوژی با ارسال در IP Packet است. زمانی که روتر یک بسته IP را ارسال می‌کند هیچ تغییری در آدرس مقصد بسته انجام نمی‌دهد. در واقعیت labelهای MPLS برای ارسال بسته‌ها، مورد استفاده قرار می‌گیرد و از آدرس IP استفاده نمی‌شود.

برخی مزایای استفاده از MPLS:

در اینجا به صورت خلاصه مزایای استفاده MPLS را در شبکه عنوان می کنیم:

- استفاده از یک زیرساخت شبکه یکپارچه.
- بهتر از IP over ATM است.
- Border Gateway Protocol (BGP)-free core
- بهینه شدن جریان ترافیک
- مهندسی ترافیک
- مدل peer-to-peer برای MPLS VPN

۱-۲-۲-۱۳زیرساخت شبکه یکپارچه

در MPLS ترافیک در هنگام ورود بر اساس مقصد labelگذاری می‌شوند و از یک بستر عمومی عبور داده می‌شوند و این ویژگی یکی از مزایای بزرگ MPLS است. یکی از دلایلی که IP به عنوان پروتکل شبکه جهانی انتخاب شد، این است که بسیاری از تکنولوژی‌های دیگر را می‌توان از آن عبور داد.

اضافه کردن label به بسته‌ها باعث می‌شود که بتوانیم در یک بستر MPLS پروتکل‌های غیر IP را منتقل کنیم، MPLS، می‌تواند IPv4، IPv6، Ethernet، HDLC، PPP و دیگر تکنولوژی‌های لایه دو برای ما منتقل کند.

به ویژگی‌ای که هر نوع فریم لایه دو در بستر MPLS منتقل گردد Any Transport Over MPLS یا AToMگفته می‌شود. روترهای که ترافیک AToM را منتقل می‌کنند نیاز به اطلاع از محتوای آن ندارند و برای ارسال آن تنها نیاز به خواندن Label آن دارند. به زبان ساده می‌توان MPLS را یک روش ساده برای ارسال ترافیک پروتکل‌های مختلف در یک شبکه نامید.

به توجه به تعاریف بالا MPLS این امکان را به Service Provider می‌دهد که انواع پروتکل‌های مورد نیاز مشتریان خود را با استفاده از یک شبکه واحد انتقال دهد.

www.takbook.com

۱۳-۲-۲-۲ Better IP over ATM Integration

در دهه ۹۰ میلادی پروتکل IP توانست از سایر پروتکل‌های لایه سوم مانند AppleTalk ، IPX و DECnet پیشی بگیرد. IP یک پروتکل نسبتا ساده و فراگیر است. ATM به عنوان یک پروتکل لایه دوم نتوانست مطابق انتظار ظاهر شود و بیشترین موفقیت آن در استفاده به عنوان یک پروتکل WAN برای Service Providerها بود.

روش‌های مختلف برای ادغام ATM با IP ارائه شد اما پیاده‌سازی و خطایابی این روش‌ها بسیار سنگین و پیچیده بود. یکی از دلایل بوجود آمدن MPLS جایگزینی یک روش جدید و بهتر برای IP over ATMبود.

۱۳-۲-۲-۳ BGP-Free Core

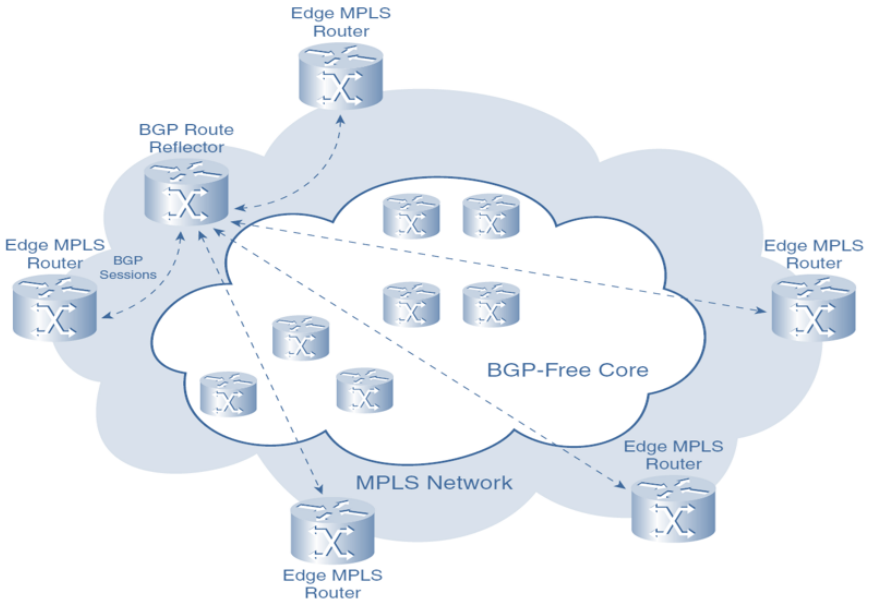
زمانی که شبکه Service Provider می‌خواهد ترافیک را منتقل کند هر روتر باید به مقصد بسته نگاه کند. اگر بسته‌ها به خارج از شبکه Service Provider بخواهد ارسال شود این آدرس‌های خارجی باید در جدول مسیریابی همه روترها وجود داشته باشد. این آدرس‌های خارجی توسط BGP حمل می‌شوند مانند آدرس‌های شبکه مشتریان یا آدرس‌های شبکه اینترنت. این به این معناست که همه روترهای Service Providerباید BGP را اجرا کنند.

اما MPLS این امکان را می‌دهد که ارسال بسته به جای بررسی آدرس IP بر اساس Label صورت گیرد. این label اطلاعاتی است که به روترهای میانی نشان می‌دهد که بسته باید به کدام روتر edge ارسال شود. در نتیجه روترهای Core نیازی به داشتن اطلاعات IP برای ارسال بسته‌ها ندارند و این باعث می‌شود روترهای Core نیازی به اجرای BGP نداشته باشند.

اما روترهای لبه یا همان Edge Router ها همچنان برای ارسال بسته‌ها نیار به بررسی آدرس IP دارند در نتیجه این روترها باید BGP را اجرا کنند.

شکل ۲۲-۱۳، یک شبکه MPLS را نشان می‌دهد که روترهای Edge آن BGP را اجرا کرده اند :

www.takbook.com



شکل ۱۳-۲۲ *Multiprotocol Label Switching (MPLS)*

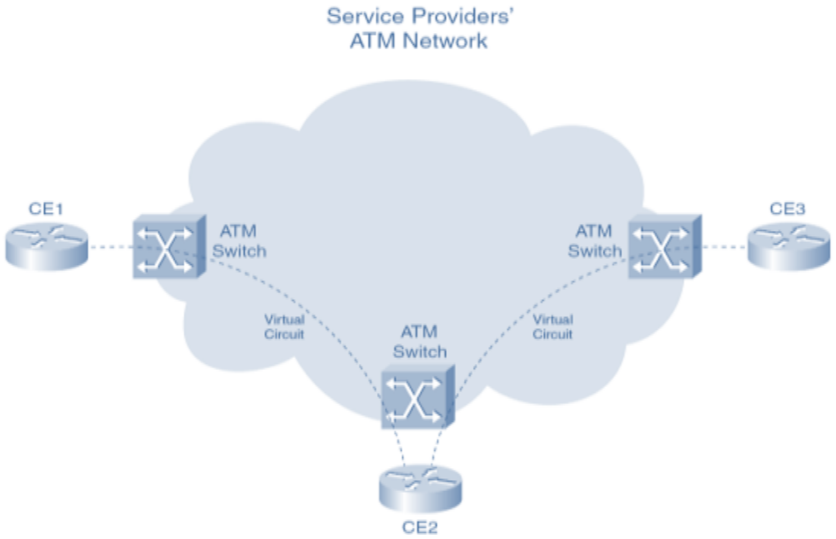
یک ISP را در نظر بگیرد که دارای ۲۰۰ روتر است بدون MPLS باید روی تمام این روترها BGP را اجرا کند اما اگر در این شبکه MPLS پیاده‌سازی شود تنها روترهای Edge که به طور مثال ۵۰ تا هستند نیاز به اجرای BGP دارند.

در شبکه‌های MPLS تمام روترهای Core ارسال بسته‌ها را بدون در نظر گرفتن آدرس IP و تنها با بررسی label بسته انجام می‌دهند و این باعث می‌شود که از بار اجرای BGP و پیچیدگی‌های آن رها شوند. جدول مسیریابی اینترنت یک جدول سنگین است که عدم اجرای آن در روترهای Core باعث می‌شود که روتر به RAM و CPU کمتری نیاز داشته باشد.

۱۳-۲-۲-۴ بهینه شدن جریان ترافیک: (Optimal Traffic Flow)

با توجه به اینکه سوئیچ‌های Frame Relay یا ATM یک دستگاه لایه دو هستند روترها برای اتصال از یک مدارمجازی استفاده می‌کنند. هر روتر برای ارسال ترافیک به صورت مستقیم به هر روتر Edge دیگر باید یک مدارمجازی بین آنها ایجاد گردد. ایجاد این مدارهای مجازی کار خسته‌کننده‌ای است. حال اگر در این شبکه نیاز باشد همه سایت‌ها به یکدیگر ارتباط داشته باشند باید توپولوژی Full Mesh را به وسیله مدار مجازی بین سایت ها ایجاد کنیم که یک کار سنگین و پرهزینه خواهد بود. اگر سایت‌ها مطابق شکل ۱۳-۲۳، (non-Fully Meshed) به یکدیگر متصل باشند ترافیک از CE1 به CE3 از CE2 عبور می‌کند.

www.takbook.com



شکل ۱۳-۲۳ *Optimal Traffic Flow*

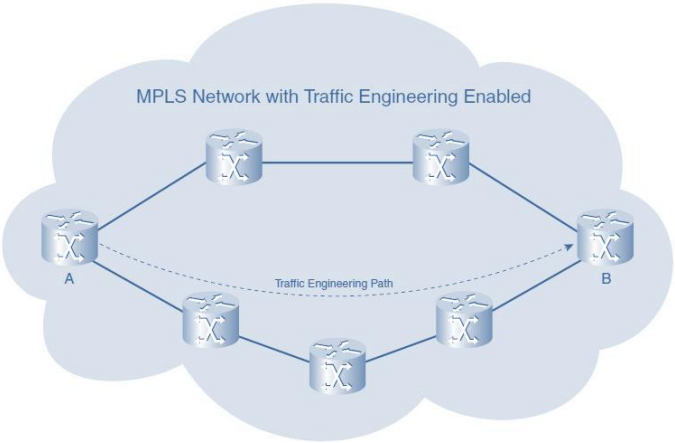
نتیجه این می‌شود که ترافیک یک مسیر انحرافی را دوبار طی می‌کند که باعث هدر رفتن پهنای باند و درگیر شدن روتر CE2 می‌شود.

اما زمانی که MPLS در این شبکه پیاده‌سازی شود ترافیک به صورت مستقیم بین سایت‌ها جریان پیدا می‌کند و باعث بهینه شدن جریان ترافیک بین سایت‌های مشتریان می‌گردد.

۵-۲-۲-۱۳ مهندسی ترافیک: (Traffic Engineering)

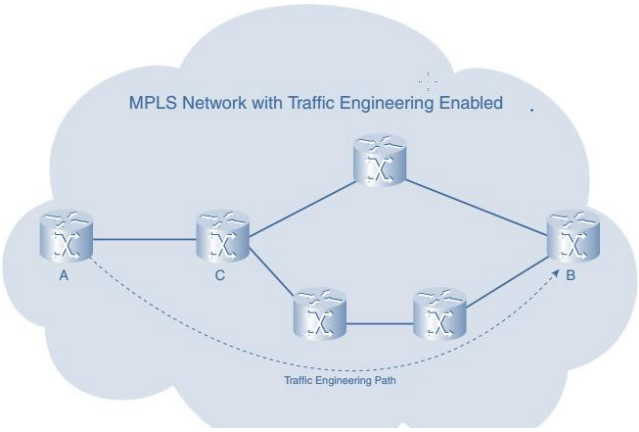
بحث مهندسی ترافیک به منظور استفاده بهینه از زیرساخت شبکه است به این معنا که مهندسی ترافیک بتواند امکان هدایت ترافیک در شبکه را از مسیرهای مختلف غیر از بهترین مسیر را فراهم سازد. بهترین مسیر بر اساس کمترین هزینه توسط IP Routing انتخاب می‌شود. این هزینه توسط پروتکل‌های داینامیک مسیریابی برای پیدا کردن کوتاه‌ترین و بهترین مسیر محاسبه می‌گردد. با استفاده از مهندسی ترافیک MPLS که در شبکه پیاده‌سازی شده باشد شما می‌توانید ترافیک با مقصد خاص یا QoS خاص را از نقطه A به نقطه B از مسیری غیر از بهترین مسیر عبور دهید. در نتیجه ترافیک روی همه لینک‌های موجود تقسیم می‌شود و باعث می‌شود از همه توانایی شبکه به بهترین شکل استفاده شود در شکل ۲۴-۱۳، یک نمونه نمایش داده شده است.

www.takbook.com



شکل ۲۴-۱۳ *Traffic Engineering*

همانطور که در شکل ۲۴-۱۳، می‌بینید شما می‌توانید ترافیک را از نقطه A به B از مسیر پایین انتقال دهید در این مثال مسیر بالا بهترین مسیر بین نقطه A و B است چون مسیر بالا نسبت به مسیر پایین کوتاه‌تر است. در نتیجه برای ارسال ترافیک ما از مسیری استفاده کرده‌ایم که کمتر مورد استفاده قرار می‌گیرد و باعث استفاده بهتر از توان زیرساخت شبکه می‌شود. یک نمونه دیگر در تصویر ۲۵-۱۳، نمایش داده شده است.



شکل ۲۵-۱۳ *Traffic Engineering*

اگر شبکه فوق را یک شبکه IP در نظر بگیریم شما نمی‌توانید تنها با تنظیم روتر A روتر C را مجبور به ارسال ترافیک از طریق مسیر پایین کنید و این روتر C است که تصمیم می‌گیرد که ترافیک را از مسیر بالا یا پایین ارسال کند. اما اگر مهندسی ترافیک MPLS را در این شبکه اجرا کنیم می‌توانیم ترافیک را از روتر A به روتر B از طریق مسیر پایین ارسال کنیم. مهندسی ترافیک روتر C را مجبور به ارسال ترافیک Aبه B از مسیر پایین می‌کند. این کار توسط MPLS امکان‌پذیر است، چون از مکانیزم Label زدن استفاده

www.takbook.com

می‌کند. در این مثال روتر A به عنوان نقطه ورودی شبکه MPLS ما است در نتیجه این روتر مسیر عبور ترافیک را مشخص می‌کند این عمل Source-Based Routing نیز نامیده می‌شود. Label که توسط روتر A به بسته زده می‌شود، باعث می‌شود که بسته از مسیری که توسط روتر A مشخص کرده عبور کند و دیگر روترهای میانی نمی‌توانند مسیر آن را تغییر دهند.

یکی دیگر از مزایای استفاده از مهندسی ترافیک در MPLS، امکان سریع مسیریابی مجدد یا (Fast ReRouting (FRR است. FRR این قابلیت را به ما می‌دهد که در صورت بروز قطعی در لینک یا از دسترس خارج شدن روتر، ترافیک label زده شده را دوباره مسیردهی کنیم این مسیریابی مجدد در کمتر از 50ms صورت می‌گیرد که از سایر استانداردهای روز بسیار سریع‌تر است.

۶-۲-۲-۱۳ VPN Model در پروتکل MPLS

VPN یک شبکه خصوصی مجازی است که روی یک بستر عمومی ایجاد می‌گردد. این شبکه خصوصی باید بتواند تمام سایت‌های مشتری را به یکدیگر متصل کند و به صورت کامل ازVPN های مرتبط با سایر مشتریان جدا باشد. معمولا هر VPN به یک سازمان که دارای چند سایت است اختصاص دارد و سایت‌های سازمان را از طریق VPN روی بستر عمومی Service Provider به یکدیگر متصل می‌کند.

Service Providerها می‌توانند دو نوع عمده VPN را به مشتریان خود ارائه دهند:

- Overlay VPN Model
- Peer-to-Peer VPN Model

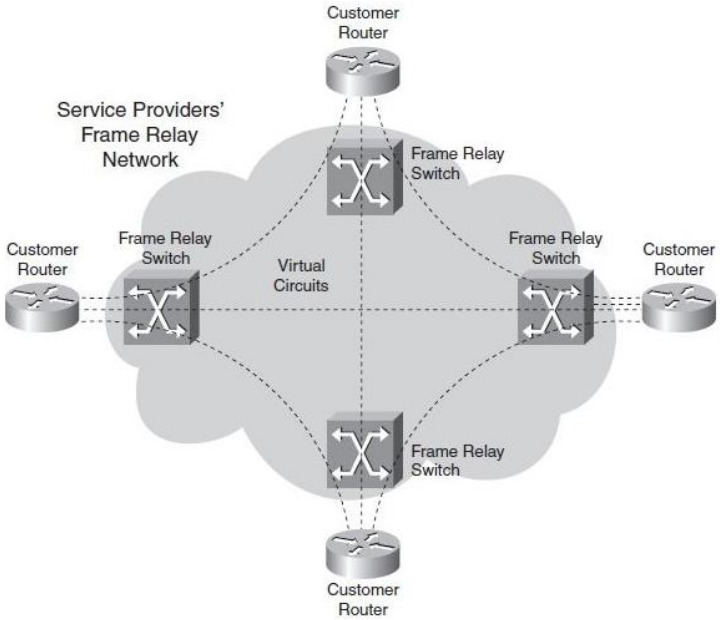
بررسی Overlay VPN Model

Service Provider در Overlay VPN بین روترهای مشتری در شبکه خود سرویس Point to Point یا مداری مجازی (Virtual Circuits) فراهم می‌کند. روترها و سوئیچ‌های Service Provider داده‌های مشتری را در سرتاسر شبکه خود حمل می‌کنند و هیچگونه تبادل Route بین روتر مشتری و روتر Service Provider انجام نمی‌گیرد و این باعث می‌شود که روترهای Service Provider هرگزRoute های مشتری را نبینند.

سرویس Point to Point می‌تواند در لایه یک ، دو و یا سه باشد. نمونه لایه یک آن TDM، E1، E3، Sonet و SDH است و نمونه لایه دو آن X.25 ، ATM و Frame Relay می‌باشد.

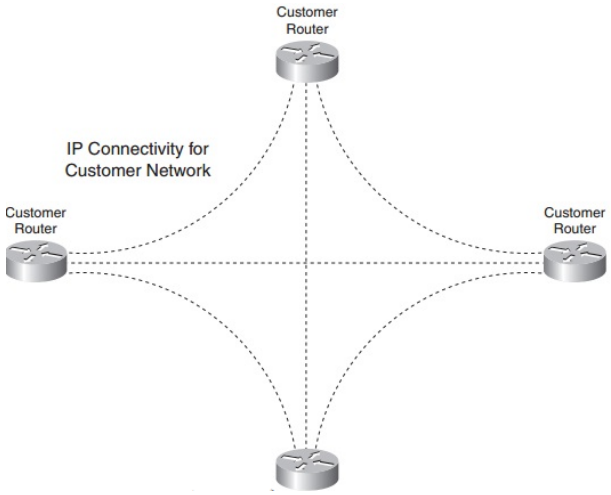
در تصویر ۲۶-۱۳، یک شبکه Overlay را نشان می‌دهد که بر روی بستر Frame Relay ایجاد شده است. سوئیچ های Frame Relay در شبکه Service Provider برای ایجاد مدار مجازی بین روترهای مشتری که در لبه شبکه Frame Relay قرار دارد تنظیم می‌گردند.

www.takbook.com



شکل ۱۳-۲۶ *Overlay VPN Model*

در لایه سوم از دیدگاه روترهای مشتری آنها به صورت مستقیم به یکدیگر متصل هستند در شکل ۱۳-۲۷، از دیدگاه مشتری این ارتباط نمایش داده شده است.

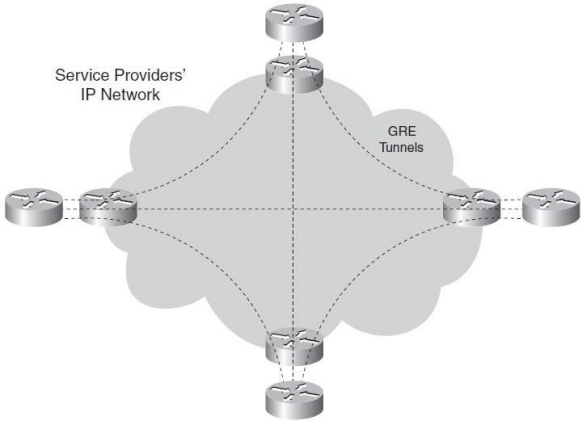


شکل ۱۳-۲۷ *Overlay VPN Model*

شبکه Overlay را می‌توان در لایه سوم ارائه داد و معمولا از GRE Tunnel برای ایجاد شبکه Overlay روی پروتکل IP استفاده می‌شود. این تونل ترافیک را با هدر GRE و یک هدر IP کپسوله می‌کند. هدر GRE برای مشخص شدن پروتکل انتقال استفاده می‌شود و هدر IP برای هدایت بسته‌ها در شبکه Service

www.takbook.com

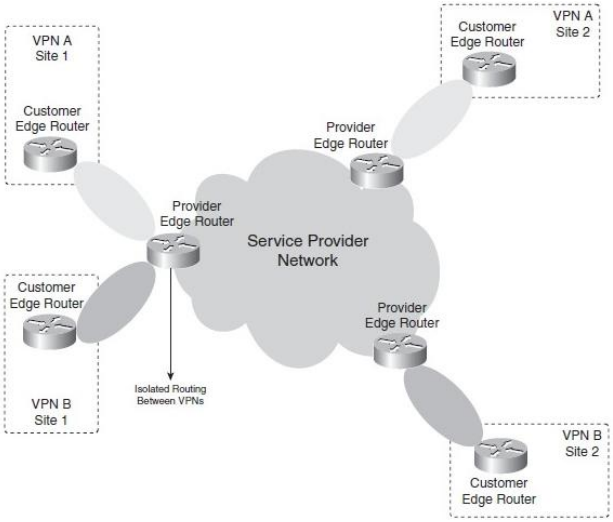
Provider مورد استفاده قرار می‌گیرد. در تصویر ۲۸-۱۳، یک شبکه Overlay با GRE Tunnel را نشان می‌دهد. یکی از مزایای استفاده از GRE Tunnel امکان هدایت ترافیک غیر IP است.



شکل ۲۸-۱۳ *Overlay VPN Model*

بررسی Peer-to-Peer VPN

روترهای Service Provider در مدل Peer to Peer VPN داده‌های مشتری را در شبکه خود حمل می‌کنند و همچنین در مسیریابی ترافیک مشتری، شرکت می‌کند. در تعریف دیگر ، روترهای Service Provider برای مسیریابی ترافیک با روترهای مشتری همکاری می‌کنند که نتیجه آن ایجاد یک رابطه همسایگی بین روترهای مشتری و Service Provider است. در شکل ۲۹-۱۳، نمونه این شبکه نمایش داده شده است:



شکل ۲۹-۱۳ *Overlay VPN Model*

www.takbook.com

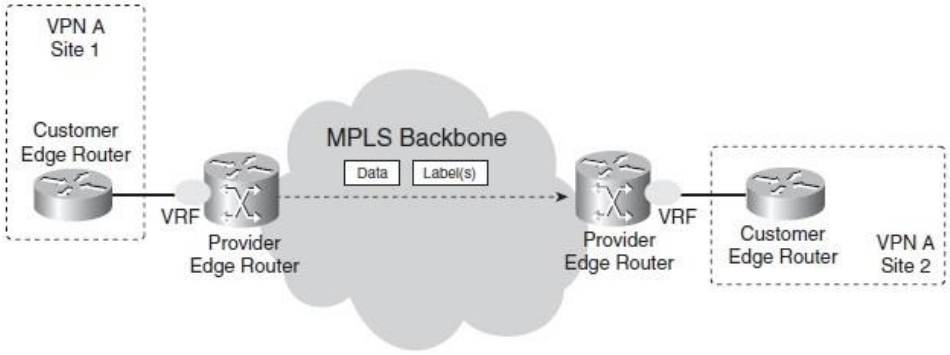
قبل از اینکه MPLS به وجود آید برای ایجاد شبکه Peer to Peer VPN ، مسیریابی IP با Peer کردن روترهای مشتری و Service Provider انجام می‌گرفت. همچنین این شبکه نیاز داشت که حریم خصوصی و ایزوله کردن را برای مشتریان انجام دهد که این کار توسط فیلتر کردن بسته (ACL) برای کنترل داده‌های مشتریان انجام می‌شد. راه دیگر برای اینکار استفاده از فیلتر کردن Route ها بود یا هر دو روش در کنار هم مورد استفاده قرار می‌گرفت.

قبل از ارائه MPLS استفاده از مدل Overlay VPN توسط Service Provider ها معمول‌تر از مدل Peer to Peer VPNبود. مدل Peer to Peer VPN نیاز به تدارکات زیادی داشت چون اضافه کردن یک سایت مشتری نیاز به تنظیمات فراوانی در بسیاری از سایت‌ها به وجود می‌آورد. یکی از کاربرد های MPLS VPN این است که باعث می‌شود مدل Peer to Peer VPN به سادگی پیاده‌سازی گردد.

با استفاده از MPLS امکان حذف و اضافه کردن سایت‌های مشتری به سادگی قابل تنظیم است و نتیجه آن کاهش زمان و حجم تنظیمات است. در MPLS VPN یک روتر مشتری که به آن روتر Customer Edgeگفته می‌شود با حداقل یک روتر Service Provider که به آن Provider Edge گفته می‌شود در لایه سوم با هم Peer می‌شوند.

حریم خصوصی در MPLS VPN با استفاده از VRF(Virtual routing/forwarding) و ارسال بسته‌ها در Backbone شبکه Service Provider با استفاده از label بدست می‌آید. با استفاده VRF از جدا نگه داشتن اطلاعات مسیریابی مشتریان مختلف از یکدیگر اطمینان حاصل پیدا می‌کنیم و در Backbone شبکه مطمئن می‌شویم که ارسال بسته‌ها براساس اطلاعات label صورت می‌گیرد نه اطلاعات آدرس IP .

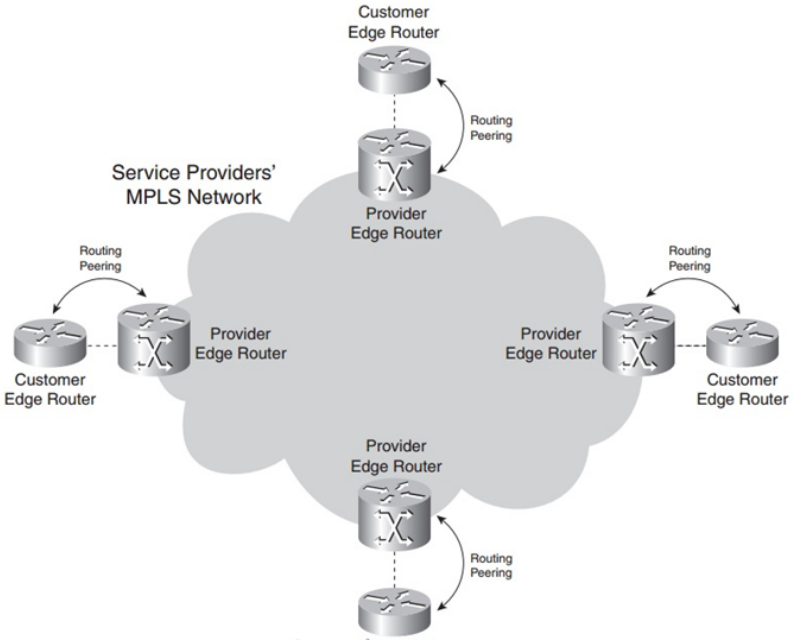
شکل ۳۰-۱۳، مفهوم VRF و ارسال براساس Label در Backbone شبکه در MPLS VPN نمایش داده شده است :



شکل ۳۰-۱۳ بررسی VRF در MPLS

در شکل ۳۱-۱۳، شبکه Peer to Peer VPN در MPLS VPN نمایش داده شده است :

www.takbook.com



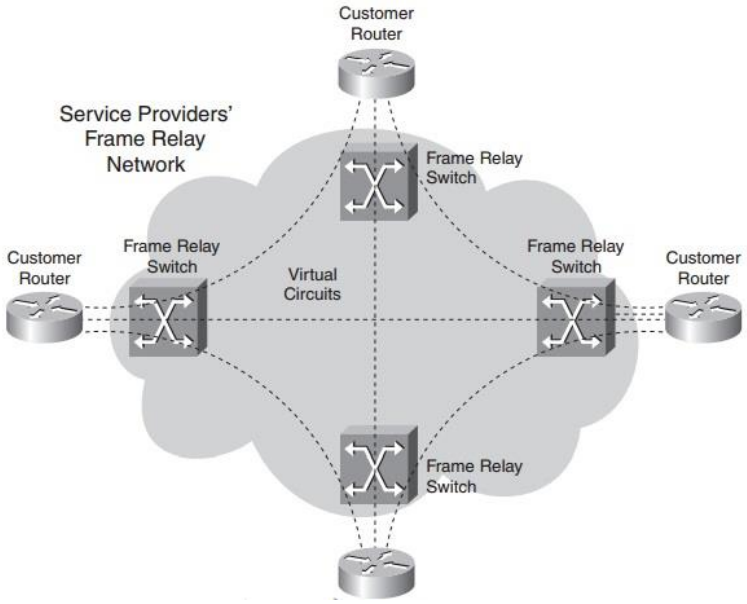
شکل ۳۱-۱۳ *Peer to Peer VPN*

MPLS VPN برای اضافه کردن یک سایت مشتری، فقط روتر PE با CE باید Peer شوند و دیگر نیاز به ایجاد Virtual Circuit در مدل Overlay VPN یا فیلتر کردن بسته‌ها یاRoute ها در مدل Peer to Peer VPN نیست این یک مزیت بزرگ برای Service Provider ها محسوب می‌شود.

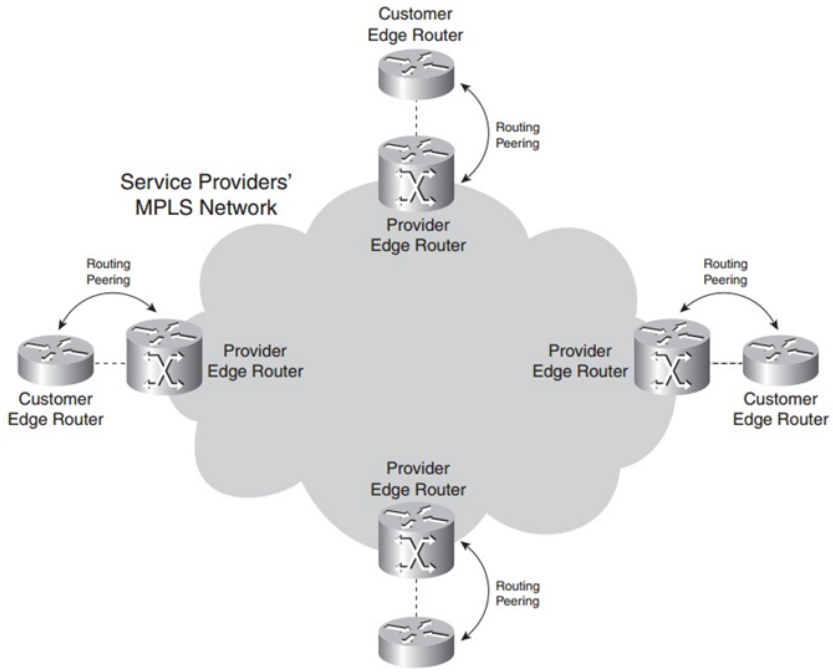
اکثر مشتریان Service Provider ها نیاز به یک شبکه Hub and Spoke دارند و بعضی از مشتریان نیاز به یک شبکه full mesh دارند و بعضی دیگر یک شبکه بین این دو حالت نیاز دارند. مزیت MPLS VPN برای مشتری زمانی ملموس می‌شود که مشتری دارای یک شبکه Full Mesh است.

دو تصویر ۳۲-۱۳ و ۳۳-۱۳، را با یکدیگر مقایسه کنید. در تصویر اول مشتری یک شبکه full mesh روی بستر frame relay دارد و تصویر دوم مشتری یک شبکه full mesh روی بستر MPLS VPN دارد.

www.takbook.com



Peer to Peer VPN شکل ۱۳-۳۲



Peer to Peer VPN شکل ۱۳-۳۳

www.takbook.com

در تصویر اول هر روتر لبه مشتری باید به همه روترهای لبه دیگر خود Peer شود که تعداد آن n-1 می‌شود اما در تصویر دوم هر روتر لبه مشتری تنها با یک روتر لبه Service Provider باید Peer شود.

مزیت دیگر برای Service Provider این است که تنها باید یک link بین روتر PE و CE ایجاد کند در صورتی که Service Provider در مدل Overlay باید بین همه سایت‌های مشتری link یا virtual circuit ایجاد کند. در روش MPLS VPN پیش‌بینی ترافیک و فراهم کردن پهنای باند مورد نیاز برای ترافیک برای یک سایت خیلی راحت‌تر از پیش‌بینی ترافیک برای کل سایت‌ها انجام می‌شود.

تنها معایب روش Peer to Peer VPN نسبت به روش Overlay VPN به شرح زیر است:

- مشتری باید در مسیریابی با Service Provider شریک شود.
- دستگاه های لبه Service Provider بار بیشتری را متحمل می شوند.

اولین عیب روش Peer to Peer VPN این است که باعث می‌شود که مشتری برای مسیریابی با Service Providerباید Peer شود و این باعث می‌شود که مشتری کنترل کاملی روی شبکه خودش نداشته باشد در اینجا منظور مسیریابی در لایه سوم است چون بخشی از این کار توسط Service Provider انجام می‌گیرد و مشتری روی آن کنترلی ندارد.

دومین عیب این روش به Service Provider برمی‌گردد، افزایش بار برای شبکه Service Provider باعث اضافه شدن وظایف روترهای PE می‌شود. Service Provider در گسترش و تبادل اطلاعات مسیریابی مشتریان مسئول است و این روترهای PE هستند که وظیفه حمل به‌موقع دیتا مشتریان را دارند.

برداشت اشتباه:

یکی از دلایل اولیه برای استفاده از label switching نیاز به سرعت بیشتر بوده است چون سرعت IP switchingنسبت به label switching پایین‌تر است. در IP switching روتر، بسته‌های IP را با استفاده از آدرس مقصد بسته که در header بسته قرار دارد و پیدا کردن بهترین مسیر از جدول مسیریابی خود برای آن مقصد ارسال می‌کند. اجرای این مراحل به برند و عملکرد روتر بستگی دارد. به هر حال چون آدرس IPمی‌تواند به صورت unicast یا multicast باشد و از چهار octets تشکیل شده است بررسی آن می‌تواند پیچیده باشد. منظور از پیچیده، این است که تصمیم‌گیری برای ارسال بسته‌های IP می‌تواند زمان‌بر باشد.

اگرچه برخی از مردم تصور می‌کنند که بررسی یک برچسب ساده نسبت به آدرس بررسی IP می‌تواند خیلی سریع‌تر باشد اما در واقع اشتباه است و روتر برای ارسال بسته از ASICs استفاده می‌کند که باعث می‌شود سرعت ارسال همانند label سریع باشد. در نتیجه سرعت بالاتر MPLS یک برداشت اشتباه می باشد.

نکته : قبل از MPLS ، معروفترین پروتکل WAN را می‌توان ATM و Frame Relay نام برد.

نکته : اندازه فیلدی که در فریم ، label را نگه‌داری می‌کند ۳۲ بیت است.

www.takbook.com

۳-۲-۱۳کار با VPN و چرا از آن استفاده می‌کنیم

امروزه اکثر شرکت‌های بزرگ دارای چندین شعبه در سرتاسر کشور یا جهان هستند و ارتباط آنها با هم یک امر بسیار مهم و حیاتی است که این مهم با استفاده از تکنولوژی‌های موجود برقرار می‌شود.

برای اینکه امنیت کاربران و شبکه حفظ شود بهترین راه حل ایجاد یک سرویس VPN برای کارمندان آن شرکت برای دسترسی به اطلاعات آن است تا بدین صورت در مرحله اول امنیت اطلاعات و در مرحله دوم دوری راه تاثیری در روند کار نداشته باشد.

VPN یا همان Virtual private network در اصل یک شبکه‌ی اختصاصی است که از جاهای مختلف دنیا می‌توانند به شبکه اصلی آن سازمان متصل شوند، که این کار از طریق اینترنت امکان‌پذیر است و نیاز به راه‌اندازی یک خط اختصاصی با شعبه‌های مختلف آن سازمان نیست.

زمانی که VPN را برای شرکت خود راه‌اندازی می‌کنید به این معنا است که کاربران با فعال کردن آن یک تونل بین سیستم خودشان و روتر شرکت ایجاد می‌کنند که روی آن انواع پروتکل‌های رمزنگاری فعال شده است و به هیچ عنوان کسی نمی‌تواند به اطلاعات آن دست پیدا کند، چون هر کاربر دارای یک نام کاربری و رمز عبور است که مختص خودش است و کسی دیگری به این اطلاعات دست پیدا نخواهد کرد.

مزایای استفاده از VPN :

- ✓ گسترش محدوده جغرافیائی ارتباطی
- ✓ بهبود وضعیت امنیت
- ✓ کاهش هزینه‌های عملیاتی در مقایسه با روش‌های سنتی نظیرWAN
- ✓ کاهش زمان ارسال و حمل اطلاعات برای کاربران از راه دور
- ✓ بهبود بهره‌وری
- ✓ توپولوژی آسان

در این قسمت می‌خواهیم یک شبکه اختصاصی با VPN ایجاد کنیم و کاربرد آن را فرا بگیریم.

انواع پروتکل‌های VPN

۱- IPsec

مخفف کلمه‌ی IP Security است که برای انتقال اطلاعات به صورت امن طراحی شده است، در این پروتکل از چندین پروتکل استفاده شده تا بسته‌های ارسالی به صورت کاملاً امن به دست گیرنده برسند، البته در این حالت هر دو طرف سرویس‌دهنده و سرویس‌گیرنده باید از یک کلید استفاده کنند تا بین آنها احراز هویت شکل بگیرد، این پروتکل در لایه 3 مدل OSI کار می‌کند و یکی از ویژگی‌های مهم آن این است که زمانی که در لایه 3 کار می‌کند می‌تواند از پروتکل‌های انتقال UDP و TCP به صورت کامل محافظت کند.

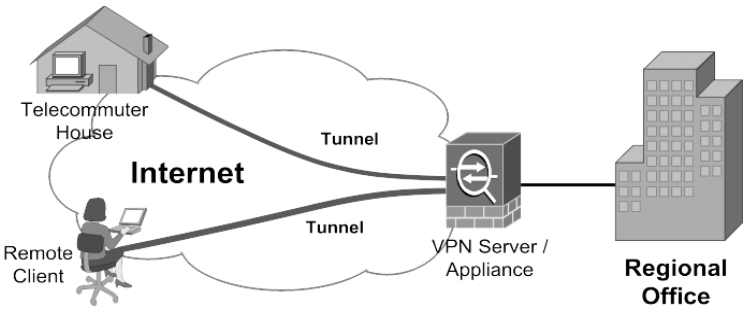
www.takbook.com

۲- SSL
Secure Sockets Layer، این پروتکل بین سرور و کلاینت قرار می‌گیرد و ارتباط را رمزنگاری می‌کند، در بیان دیگر زمانی که یک صفحه وب را با پروتکل HTTP باز می‌کنید اطلاعات به صورت Plain Text ردوبدل می‌شود و همین موضوع باعث می‌شود مهاجم به راحتی از طریق گوش دادن به خط مورد نظر به اطلاعات دست پیدا کنند، به همین خاطر پروتکل HTTPS اجرا شد و اطلاعات آن توسط SSL رمزنگاری شده است تا دیگر هیچ اطلاعاتی درز نکند، توجه داشته باشید که این پروتکل در لایه ۴ مدل OSI کار می‌کند.

انواع VPN

۱- MPLS
Multiprotocol Label Switching یک نوع VPN است که با نام MPLS L3VPN شناخته می‌شود و برای ارتباط چندین سایت در نقاط مختلف کاربرد دارد، در MPLS به صورت پیش‌فرض رمزنگاری وجود ندارد و برای امن کردن آن باید از IPSEC استفاده کنید که در قسمت قبلی به صورت کامل آن را بررسی کردیم.

۲- Remote-access
بعضی از کاربران نیاز دارند تا از راه دور بتوانند به منابع شبکه دسترسی داشته باشند برای همین از VPNهای نوع Remote-Access استفاده می‌کنند، برای ایجاد امنیت در این نوع VPNها از IPSEC و SSL استفاده می‌شود، بسیاری از کسانی که از محصولات سیسکو استفاده می‌کنند از این نوع استفاده می‌کنند، درشکل ۳۴-۱۳، همین موضوع مشخص شده است.



شکل ۳۴-۱۳ Remote Access VPN

۳- **Site-to-site**

www.takbook.com

در این نوع ارتباط شرکتهایی که دارای چندین شعبه در جاهای مختلف دنیا هستند می‌توانند با این فناوری شبکه خود را یکپارچه کنند، در این نوع ارتباط دیگر مشتری نیاز نیست که برای خود یک VPN کانکشن ایجاد کند بلکه روترهای ارتباطی با هم دیگر ارتباط VPN دارند.

شکل ۳۵-۱۳ *Site To Site VPN*

مزایای اصلی استفاده از VPN در MPLS، Site to Site و Remote Access عبارتند از:

- ✓ محرمانه بودن
- ✓ یکپارچگی داده‌ها
- ✓ تأیید اعتبار
- ✓ حفاظت

۱-۳-۲-۱۳ رمزنگاری

رمزنگاری یا همان Cryptography به دانشی گفته می‌شود که در آن اطلاعات به صورت یک کلید رمزنگاری می‌شود، که این کار توسط الگورتم مربوط به آن انجام می‌شود و فقط کسی می‌تواند از این اطلاعات استفاده کند که اطلاعات لازم مانند کلید و الگوریتم مربوط به آن را بداند.

بررسی برخی از اصطلاحات

Decryption

برای آشکارسازی اطلاعات Encryption شده، مورد استفاده قرار می‌گیرد و نام آن را رمزگشایی هم می‌نامند.

Plain text

متن اولیه که رمزنگاری نشده و یک رمز آشکار است و مهاجمان به راحتی می‌توانند به آن دست پیدا کنند.

Cipher

www.takbook.com

الگوریتمی برای رمزگذاری و رمزشکنی است و از سرعت عمل خوبی برخوردار است.

Cryptanalysis

به باز کردن قفل‌های Cipher گفته می‌شود یا خواندن متن قفل شده‌ی آن.

Intruder

در لغت به معنای مزاحم یا مخل است و در رمزنگاری به معنای کسی است که یک کپی از پیام رمزنگاری شده دارد و قصد رمزگشایی آن را دارد. منظور از شکستن رمز، Decrypt کردن آن متن که خود دو نوع است. Active intruder که می‌تواند اطلاعات را روی خط عوض کند و تغییر دهد و passive intruder که فقط می‌تواند اطلاعات روی خط را داشته باشد و قابلیت تغییر آن‌ها را ندارد.

Protocol

به روش یا قراردادی که بین دو یا چند نفر برای تبادل اطلاعات گذاشته می‌شود گفته می‌شود.

Intrusion Points

نقاطی که یک نفوذگر بتواند به اطلاعات با ارزش دست پیدا کند.

Internal Access Point

به سیستم‌هایی گویند که در اتاق یا در شبکه داخلی مستقرند و هیچ امنیتی (LocalSecurity) روی آن‌ها تنظیم نشده باشد و احتمال حمله به آن‌ها وجود دارد.

External Access Point

تجهیزاتی که ما را به شبکه خارجی مانند اینترنت متصل می‌کنند یا Applicationهایی که از طریق اینترنت کار می‌کنند و احتمال حمله به آن‌ها وجود دارد.

Key

به اطلاعاتی گفته می‌شود که با استفاده از آن بتوان cipher text (متنی که cipher شده) را به plain text تبدیل کرد. (یا برشکل) به عبارت ساده یک متن رمز شده توسط یک Key با الگوریتم مناسب، به متن ساده تبدیل می‌شود.

۱۳-۲-۳-۲ کلیدهای متقارن (Symmetric) و نامتقارن (Asymmetric)

۱۳-۲-۳-۱ رمزنگاری کلید متقارن

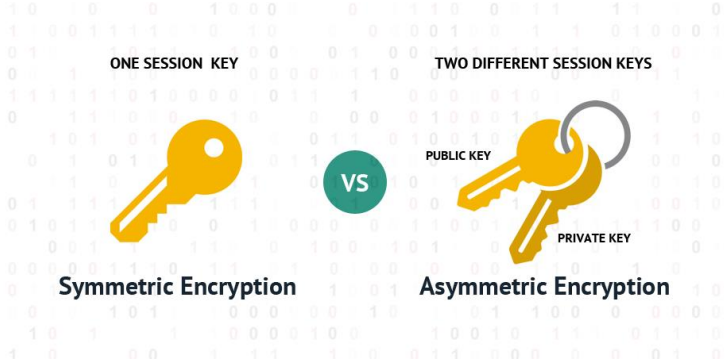
رمزنگاری کلید متقارن یا تک کلیدی، به آن دسته از الگوریتم‌ها، پروتکل‌ها و سیستم‌های رمزنگاری گفته می‌شود که در آن هر دو طرف رد و بدل اطلاعات از **یک کلید رمز یکسان** برای عملیات رمزگذاری و

www.takbook.com

رمزگشایی استفاده می‌کنند. در این قبیل سیستم‌ها، یا کلیدهای رمزگذاری و رمزگشایی یکسان هستند یا با رابطه‌ای بسیار ساده از یکدیگر قابل استخراج هستند.

واضح است که در این نوع از رمزنگاری، باید یک کلید رمز مشترک بین دو طرف تعریف گردد. چون کلید رمز باید کاملاً محرمانه باقی بماند، برای ایجاد و رد و بدل کلید رمز مشترک باید از کانال امن استفاده نمود یا از روش‌های رمزنگاری نامتقارن استفاده کرد. نیاز به وجود یک کلید رمز به ازای هر دو نفرِ درگیر در رمزنگاری متقارن، موجب بروز مشکلاتی در مدیریت کلیدهای رمز می‌گردد.
الگوریتم‌هایی که در Symmetric به کار می‌رود عبارت‌اند از:

- ✓ DES
- ✓ DES3
- ✓ AES
- ✓ IDEA
- ✓ RC2, RC4, RC5, RC6
- ✓ Blowfish



شکل ۳۶-۱۳ کلید متقارن و نامتقارن

رمزنگاری کلید نامتقارن

رمزنگاری کلید نامتقارن، در ابتدا با هدف حل مشکل انتقال کلید در روش متقارن پیشنهاد شد. در این نوع از رمزنگاری، به جای یک کلید مشترک، از یک زوج کلید به نام‌های کلید عمومی و کلید خصوصی استفاده می‌شود. کلید خصوصی تنها در اختیار دارندهٔ آن قرار دارد و امنیت رمزنگاری به محرمانه بودن کلید خصوصی بستگی دارد. کلید عمومی در اختیار کلیهٔ کسانی که با دارندهٔ آن در ارتباط هستند قرار داده می‌شود.

به مرور زمان، به غیر از حل مشکل انتقال کلید در روش متقارن، کاربردهای متعددی برای این نوع از رمزنگاری مطرح گردیده‌است. در سیستم‌های رمزنگاری نامتقارن، بسته به کاربرد و پروتکل مورد نظر، گاهی از کلید عمومی برای رمزگذاری و از کلید خصوصی برای رمزگشایی استفاده می‌شود و گاهی نیز، بر شکل، کلید خصوصی برای رمزگذاری و کلید عمومی برای رمزگشایی به کار می‌رود.

www.takbook.com

دو کلید عمومی و خصوصی با یکدیگر متفاوت هستند و با استفاده از روابط خاص ریاضی محاسبه می‌گردند. رابطهٔ ریاضی بین این دو کلید به گونه‌ای است که کشف کلید خصوصی با در اختیار داشتن کلید عمومی، عملاً ناممکن است.

الگوریتم‌هایی که در Asymmetric به کار می‌روند عبارت اند از:

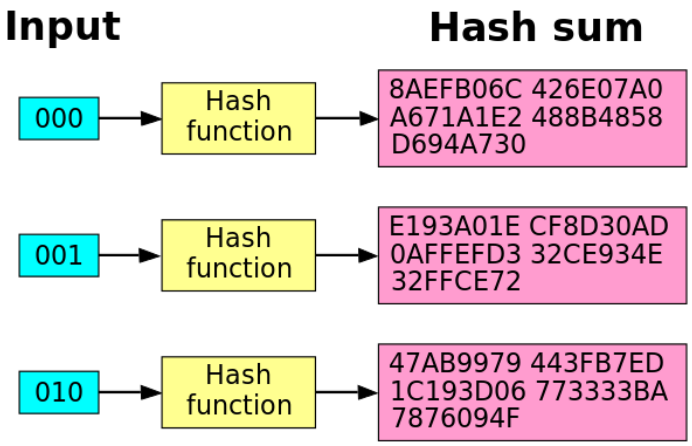
- RSA ✓
- DH ✓
- ElGamal ✓
- DSA ✓
- ECC ✓

مقایسه رمزنگاری کلید متقارن و کلید نامتقارن

اصولاً رمزنگاری کلید متقارن و کلید نامتقارن دارای دو ماهیت متفاوت هستند و کاربردهای متفاوتی نیز دارند. بنابراین مقایسه این دو نوع رمزنگاری بدون توجه به کاربرد و سیستم مورد نظر کار دقیقی نخواهد بود. اما اگر معیار مقایسه، به‌طور خاص، حجم و زمان محاسبات مورد نیاز باشد، باید گفت که با در نظر گرفتن مقیاس امنیتی معادل، الگوریتم‌های رمزنگاری متقارن خیلی سریع‌تر از الگوریتم‌های رمزنگاری نامتقارن می‌باشند.

۱۳-۳-۲-۳ هش کردن (Hashing)

در این روش یک ورودی از اطلاعات دریافت می‌شود و بعد از اجرای یک الگوریتم بر روی آن ورودی تبدیل به اعداد و حروف خواهد شد که در شکل ۳۷- این موضوع را مشاهده می‌کنید که مثلاً با ورود عدد ۰۰۰ و اعمال الگوریتم هش روی آن کد نهایی آن به صورت کامل تغییر کرده و هک کردن آن کاملاً سخت شده است.



شکل ۳۷-۱۳ Hashing

www.takbook.com

انواع الگوریتم‌های هش عبارت‌اند از:

جدول 1-۱۳ – الگوریتم‌های هش

نوع الگوریتم	اندازه
BLAKE-256	256 bits
BLAKE-512	512 bits
BLAKE2s	Up to 256 bits
BLAKE2b	Up to 512 bits
ECOH	224 to 512 bits
FSB	160 to 512 bits
GOST	256 bits
Grøstl	Up to 512 bits
HAS-160	160 bits
HAVAL	128 to 256 bits
JH	224 to 512 bits
MD2	128 bits
MD4	128 bits
MD5	128 bits
MD6	Up to 512 bits
RadioGatún	Up to 1216 bits
RIPEMD	128 bits
RIPEMD-128	128 bits
RIPEMD-160	160 bits
RIPEMD-320	320 bits
SHA-1	160 bits
SHA-224	224 bits
SHA-256	256 bits
SHA-384	384 bits
SHA-512	512 bits
SHA-3 (originally known as Keccak)	arbitrary
Skein	arbitrary
Snefru	128 or 256 bits
Spectral Hash	512 bits
Streebog	256 or 512 bits
SWIFFT	512 bits
Tiger	192 bits
Whirlpool	512 bits

از بین این الگوریتم‌ها بیشترین استفاده از الگوریتم‌های MD5، SHA1، SHA2 می‌شود.

www.takbook.com

۴-۳-۲-۱۳ بررسی IPsec و SSL

IPsec یا همان Internet Protocol security عبارت است از مجموعه‌ای از چندین پروتکل که برای ایمن‌سازی پروتکل اینترنت در ارتباطات بوسیله احراز هویت و رمزگذاری در هر بسته (packet) در یک سیر داده به کار می‌رود. این پروتکل محصول مشترک مایکروسافت و سیسکو است که در نوع خود جالب توجه است.

IPsec بر خلاف دیگر پروتکل‌های امنیتی نظیر SSL, TSL, SSH که در لایه انتقال (لایه ۴) به بالا قرار دارند در لایه شبکه یا همان لایه ۳ مدل مرجع OSI کار می‌کند یعنی لایه‌ای که IP در آن قرار دارد، که باعث انعطاف بیشتر این پروتکل می‌شود به‌طوری‌که می‌تواند از پروتکل‌های لایه ۴، نظیر TCP و UDP نیز محافظت کند.

مزیت بعدی IPsec به نسبت بقیه پروتکل‌های امنیتی نظیر SSL این است که، نیازی نیست که برنامه بر طبق این پروتکل طراحی شود.

الگوریتم‌های رمزنگاری تعریف شده برای استفاده با IPSEC شامل:

- ✓ SHA1 برای حفاظت از صداقت و صحت
- ✓ DES برای محرمانگی
- ✓ AES برای قابلیت اعتماد

IPSEC معمولاً در ارتباط با IPV6 توسعه داده شده و در اصل در تمام پیاده‌سازی‌های استاندارد از IPV6، IPSEC مورد نیاز است. IPSEC برای پیاده‌سازی IPV4 اختیاری است و در IPV4 اغلب برای ایمن‌سازی ترافیک مورد استفاده قرار می‌گیرد.

خانواده پروتکل IPSec شامل دو پروتکل است. یعنی سرآیند احراز هویت یا AH یا همان authentication header و ESP هر دوی این پروتکل‌ها از IPSec، مستقل خواهد بود.

پروتکل AH (Authentication Header)

این پروتکل در اوایل دهه‌ی ۱۹۹۰ در آزمایشگاه تحقیقاتی نیروی دریایی آمریکا ایجاد شد، بطور خلاصه پروتکل AH در واقع تأمین‌کننده سرویس‌های امنیتی زیر خواهد بود:

- ✓ تمامیت داده ارسالی
- ✓ تصدیق هویت مبدأ داده ارسالی
- ✓ رد بسته‌های دوباره ارسال شده

یکی از ویژگی‌های الگوریتم AH جلوگیری از حملات option-insertion در IPV4 است و درIPv6 هم در برابر حملات درج هدر و هم از حملات درج گزینه محافظت می‌کند.

در زیر نمودار بسته AH را مشاهده می‌کنید که چگونه یک بسته AH ساخته و تفسیر می‌شود:

جدول ۲-۱۳ – بسته‌ی AH

www.takbook.com

Authentication Header format					
Offsets	**Octet 16**	**0**	**1**	**2**	**3**
Octet 16	**Bit10**	**0 1 2 3 4 5 6 7**	**8 9 10 11 12 13 14 15**	**16 17 18 19 20 21 22 23**	**24 25 26 27 28 29 30 31**
0	**0**	*Next Header*	*Payload Len*	*Reserved*	
4	**32**	*Security Parameters Index (SPI)*			
8	**64**	*Sequence Number*			
C	**96**	*Integrity Check Value (ICV)*			
		...			

پروتکل Encapsulation Security Payload(ESP)

این پروتکل در اوایل دهه‌ی ۱۹۹۲ در آزمایشگاه تحقیقاتی نیروی دریایی آمریکا ایجاد شد، به عنوان بخشی از یک پروژه تحقیقاتی تحت حمایت DARPA تهیه شد، و توسط گروه IETF SIPP آشکارا منتشر شد.

پروتکل ESP سرویس‌های امنیتی زیر را ارائه می‌کند:

- ✓ محرمانگی
- ✓ احراز هویت مبدأ داده ارسالی
- ✓ رد بسته‌های دوباره ارسال شده

نمودار بسته ESP زیر نحوه ساخت و تفسیر یک بسته ESP را نشان می دهد:

جدول3-۱۳ – بسته ESP

Encapsulating Security Payload format					
Offsets	**Octet 16**	**0**	**1**	**2**	**3**
Octet 16	**Bit10**	**0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15**	**16 17 18 19 20 21 22 23**	**24 25 26 27 28 29 30 31**	
0	**0**	**Security Parameters Index (SPI)**			
4	**32**	**Sequence Number**			
8	**64**	**Payload data**			
...	**...**				
...	**...**				
...	**...**		**Padding (0-255 octets)**		
...	**...**			**Pad Length**	**Next Header**

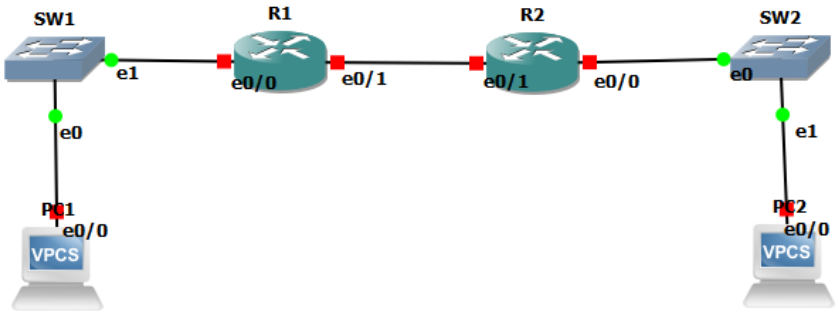
www.takbook.com

...	...	**Integrity Check Value (ICV)**
...	...	...

۵-۳-۲-۱۳ ایجاد VPN در دستگاه‌های سیسکو

۶-۳-۲-۱۳ بررسی Site To Site VPN با استفاده از IPSEC

بعد از بررسی اولیه VPN، در این قسمت می‌خواهیم برای ایجاد VPN از دستگاه‌های سیسکو استفاده کنیم، که این کار را در نرم‌افزار GNS3 انجام می‌دهیم به مانند شکل ۳۸-۱۳، ۴ روتر و دو سوئیچ به صفحه اضافه کنید، توجه داشته باشید PC1 و PC2 همان روتر هستند که با کلیک راست بر روی آنها و انتخاب Change Symbol آیکون آنها را به PC تغییر حالت دادیم، در ادامه به ترتیب تنظیمات مربوط به هر دستگاه را انجام می‌دهیم.



شکل ۳۸-۱۳ Site To Site VPN

تنظیمات مربوط به آدرس IP و انجام Route

تنظیمات روتر R1

R1#**conf t**

R1(config-if)#**int e0/1**

R1(config-if)#**ip address 192.168.1.1 255.255.255.0**

R1(config-if)#**no sh**

R1(config-if)#**int e0/0**

R1(config-if)#**ip address 172.16.1.1 255.255.255.0**

R1(config-if)#**no sh**

www.takbook.com

در دستورات بالا وارد پورت‌های مورد نظر روتر R1 شدیم و آدرس IP را برای آنها مشخص و پورت را روشن کردیم.

تنظیمات روتر R2

R2#**conf t**

R2(config)#**int e0/1**

R2(config-if)#**ip address 192.168.1.2 255.255.255.0**

R2(config-if)#**no sh**

R2(config-if)#**int e0/0**

R2(config-if)#**ip address 172.16.2.1 255.255.255.0**

R2(config-if)#**no sh**

تنظیمات PC1

PC1#**conf t**

PC1(config)#**int e0/0**

PC1(config-if)#**ip address 172.16.1.2 255.255.255.0**

PC1(config-if)#**no sh**

تنظیمات PC2

PC2#**conf t**

PC2(config)#**int e0/0**

PC2(config-if)#**ip address 172.16.2.2 255.255.255.0**

PC2(config-if)#**no sh**

بعد از اینکه با دستور PING ارتباط بین دستگاه‌ها را مطمئن شدید باید از دستور Route برای معرفی شبکه‌ها به هم استفاده کنیم.

برای اینکه از پروتکل‌های مسیریابی هم استفاده کنیم در این قسمت پروتکل EIGRP را فعال می‌کنیم تا شبکه های این دستگاه‌ها به هم معرفی شوند.

روتر R1

R1(config)#**router eigrp 100**

www.takbook.com

R1(config-router)#**network 192.168.1.0**

R1(config-router)#**network 172.16.1.0**

روتر R2

R2(config)#**router eigrp 100**

R2(config-router)#**network 192.168.1.0**

R2(config-router)#**network 172.16.2.0**

کلاینت PC1

PC1(config)#**router eigrp 100**

PC1(config-router)#**net 172.16.1.0**

کلاینت PC2

PC2(config)#**router eigrp 100**

PC2(config-router)#**net 172.16.2.0**

با انجام مراحل بالا اگر از طریق PC1 به PC2 دستور PING را اجرا کنید مطمئناً این دو دستگاه همدیگر را می‌بینند.

PC1#**ping 172.16.2.2**

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 172.16.2.2, timeout is 2 seconds:

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/4/5 ms

یکی از ویژگی‌های IPSEC این است که خط ارتباطی را بین دو روتر یا دستگاه امن می‌کند، اگر در همین حالت این فناوری بین دو خطوط استفاده نشود هر کسی می‌تواند با ابزارهای لازم به اطلاعات گوش دهد و به اطلاعاتی که نیاز دارد دست پیدا کند، مثلاً اگر در PC2 سرویس Telnet را فعال کنید و بخواهید از طریق PC1 به آن دسترسی داشته باشید، فرد مهاجم با استفاده از نرم‌افزارهای Snif مانند Nmap یا Wireshark به اطلاعات شما مانند نام‌کاربری و رمز عبور دست پیدا خواهد کرد که برای حل این مشکل یکی از راه‌های پیشنهادی که بسیار کارایی دارد استفاده از فناوری IPSEC است.

تنظیمات مربوط به IPSEC

تنظیم روتر R1

R1(config)#**crypto isakmp policy 1**

www.takbook.com

با دستور crypto و انتخاب isakmp رمزنگاری بر روی این خط فعال می‌شود.

R1(config-isakmp)#**encryption 3des**

نوع رمزگذاری را می‌توانید با دستور encryption انتخاب کنید که باید یکی از گزینه‌های AES, 3DES, DES را انتخاب کنید که 3DES انتخاب خوبی خواهد بود چون از قدرت رمزگذاری خوبی برخوردار است.

R1(config-isakmp)#**hash md5**

در مورد هشینگ هم در قسمت‌های قبلی صحبت کردیم که گزینه‌ی MD5 را انتخاب می‌کنیم.

R1(config-isakmp)#**authentication pre-share**

در این قسمت باید نوع تایید ارتباط بین دو روتر را مشخص کنید که pre-share انتخاب شده است.

R1(config-isakmp)#**group 2**

در قسمت Group گزینه‌های مختلفی وجود دارد که در زیر لیست آنها را مشاهده می‌کنید:

- Diffie-Hellman group 1 (768 bit)
- 14 Diffie-Hellman group 14 (2048 bit)
- 15 Diffie-Hellman group 15 (3072 bit)
- 16 Diffie-Hellman group 16 (4096 bit)
- 19 Diffie-Hellman group 19 (256 bit ecp)
- Diffie-Hellman group 2 (1024 bit)
- 20 Diffie-Hellman group 20 (384 bit ecp)
- 24 Diffie-Hellman group 24 (2048 bit, 256 bit subgroup)
- 5 Diffie-Hellman group 5 (1536 bit)

گروه شماره‌ی ۲ می‌تواند انتخاب مناسبی باشد، Hellman group برای ایجاد امنیت بین دو نقطه نا امن کاربرد دارد.

توجه داشته باشید که اگر اطلاعات بین روترها بسیار حیاتی و مهم باشد بهتر است که گروهی به غیر از گروه‌های 1,2,5 انتخاب شود چون این گروه‌ها معروف به AVOID هستند و سطح امنیتی مناسبی در برابر تعدیدات ارائه نخواهند داد.

R1(config-isakmp)#**lifetime 86400**

در این قسمت می‌توانید حداکثر زمان فعال بودن ارتباط بین دو دستگاه را مشخص کنید که عددی بین ۱ تا ۸۶۴۰۰ است که در این قسمت بالاترین گزینه انتخاب شده است، این عدد بر حسب ثانیه است.

R1(config)#**crypto isakmp key 123456 address 192.168.1.2**

با این دستور یک رمز عبور ۱۲۳۴۵۶ ایجاد خواهد شد که مربوط به آدرس روتر روبرویی است.

R1(config)#**ip access-list extended 100**

R1(config-ext-nacl)#**permit ip 172.16.1.0 0.0.0.255 172.16.2.0 0.0.0.255**

www.takbook.com

برای اینکه به آدرس شبکه داخلی پشت روترها اجازه عبور بین تونل IPSEC را دهیم باید یک Access-list در هر دو روتر ایجاد کنیم و دسترسی لازم را بدهیم، در دستور بالا یک Access List شماره‌ی ۱۰۰ که از نوع extended است را ایجاد می‌کنیم و در داخل آن به دو شبکه 172.16.1.0 و 172.16.2.0 اجازه عبور می‌دهیم، البته از این Acess List در ادامه استفاده خواهیم کرد.

R1(config)#**crypto ipsec transform-set IPTS esp-3des esp-md5-hmac**

دستور بعدی ایجاد بسته انتقال IPSEC با استفاده از دستور transform-set است که دارای رمزنگاری esp-3des و esp-md5-hmac است، توجه داشته باشید که کلمه IPTS برای این بسته وارد کرده‌ایم که شما می‌توانستید هر نامی برای آن وارد کنید، فقط توجه داشته باشید که از این نام در ادامه استفاده خواهیم کرد.

R1(config)#**crypto map MAP1 10 ipsec-isakmp**

با دستور بالا ارتباط MAP با Ipsec برقرار خواهد شد.

R1(config-crypto-map)#**set peer 192.168.1.2**

با دستور Set peer آدرس روترR2 را وارد می‌کنیم.

R1(config-crypto-map)#**set transform-set IPTS**

با دستور بالا یک بسته با نام IPTS برای Transform-set ایجاد خواهد شد.

R1(config-crypto-map)#**match address 100**

با این دستور Access List که با شماره‌ی ۱۰۰ ایجاد کردیم در این MAP قرار خواهد گرفت.

R1(config-crypto-map)# **int e0/1**

R1(config-if)#**crypto map MAP1**

*May 7 08:33:35.543: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON

در مرحله آخر برای فعال‌سازی MAP باید وارد Interface شوید که به روتر روبریی متصل است که در سناریوی ما پورت e0/1 است، بعد از ورود با دستور crypto map MAP1 فعال‌سازی این دستورات به طور کامل بر روی این پورت انجام می‌شود که در آخر جمله "ISAKMP is ON " نشان دهنده فعال‌سازی آن است.

همه دستورات روتر R1 در یک نگاه

R1(config)#**crypto isakmp policy 1**

R1(config-isakmp)#**encryption 3des**

R1(config-isakmp)#**hash md5**

R1(config-isakmp)#**authentication pre-share**

www.takbook.com

R1(config-isakmp)#**group 2**

R1(config-isakmp)#**lifetime 86400**

R1(config)#**crypto isakmp key 123456 address 192.168.1.2**

R1(config)#**ip access-list extended 100**

R1(config-ext-nacl)#**permit ip 172.16.1.0 0.0.0.255 172.16.2.0 0.0.0.255**

R1(config)#**crypto ipsec transform-set IPTS esp-3des esp-md5-hmac**

R1(config)#**crypto map MAP1 10 ipsec-isakmp**

R1(config-crypto-map)#**set peer 192.168.1.2**

R1(config-crypto-map)#**set transform-set IPTS**

R1(config-crypto-map)#**match address 100**

R1(config-crypto-map)# **int e0/1**

R1(config-if)#**crypto map MAP1**

تنظیم روتر R2

در این قسمت فقط دستورات مربوط به روتر R2 را قرار می‌دهم چون توضیحات آن دقیقاً مانند روتر R1 است با این تفاوت که آدرس IP در آن متفاوت وارد می‌شود.

R2(config)#**crypto isakmp policy 1**

R2(config-isakmp)#**encryption 3des**

R2(config-isakmp)#**hash md5**

R2(config-isakmp)#**authentication pre-share**

R2(config-isakmp)#**group 2**

R2(config-isakmp)#**lifetime 86400**

R2(config)#**crypto isakmp key 123456 address 192.168.1.1**

رمز عبوری که در روتر R1 تعریف کردیم دقیقاً همان رمز را به همراه آدرس روتر روبرو وارد می‌کنیم.

R2(config)#**ip access-list extended 100**

R2(config-ext-nacl)#**permit ip 172.16.2.0 0.0.0.255 172.16.1.0 0.0.0.255**

در دستور بالا آدرس مبدا و مقصد چون از طرف روتر R2 است تغییر کرده است.

R2(config)#**crypto ipsec transform-set IPTS esp-3des esp-md5-hmac**

R2(config)#**crypto map MAP1 10 ipsec-isakmp**

www.takbook.com

R2(config-crypto-map)#**set peer 192.168.1.1**

آدرس روتر R1 را برای ارتباط وارد می‌کنیم.

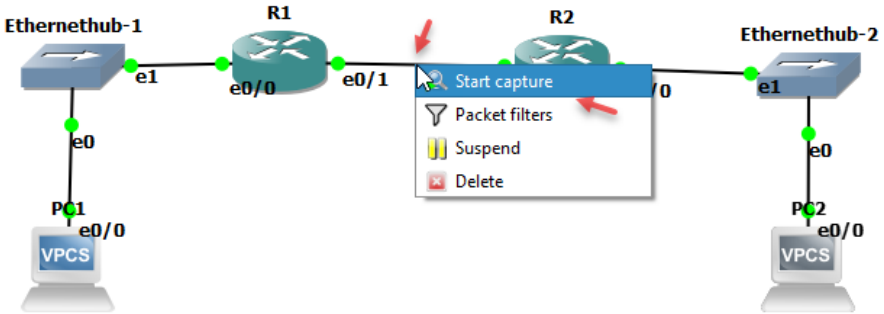
R2(config-crypto-map)#**set transform-set IPTS**

R2(config-crypto-map)#**match address 100**

R2(config-crypto-map)#**int e0/1**

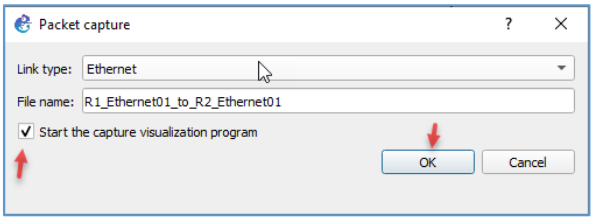
R2(config-if)#**crypto map MAP1**

با انجام این مراحل توانستیم ارتباط بین دو روتر را به صورت کاملاً امن ایجاد کنیم، برای اینکه متوجه شوید که ارتباط بین دو روتر به چه صورت است، به مانند شکل ۳۹-۱۳، باید بر روی لینک بین دو روتر کلیک راست کنید و گزینه‌ی Start Capture را انتخاب کنید، با این کار نرم‌افزار Wireshark برای شما در صوت نصب بودن اجرا خواهد شد.



شکل ۳۹-۱۳ *Site To Site VPN*

در شکل ۴۰-۱۳، تیک گزینه‌ی مورد نظر را انتخاب و بر روی ok کلیک کنید.

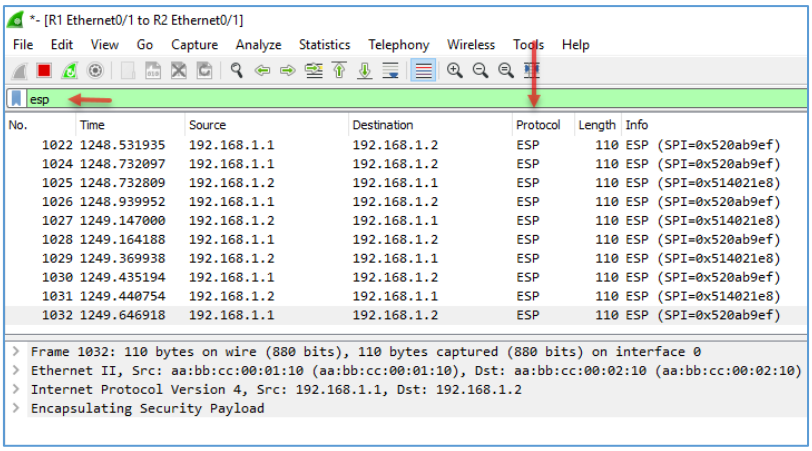


شکل ۴۰-۱۳ *Site To Site VPN*

اگر از PC1 به PC2 دستور Ping را اجرا کنید یا کاری دیگر انجام دهید تمام ارتباط با استفاده از پروتکل ESP (Encapsulating Security Payload) امن شده است و دسترسی به اطلاعات آن امکان‌پذیر نیست

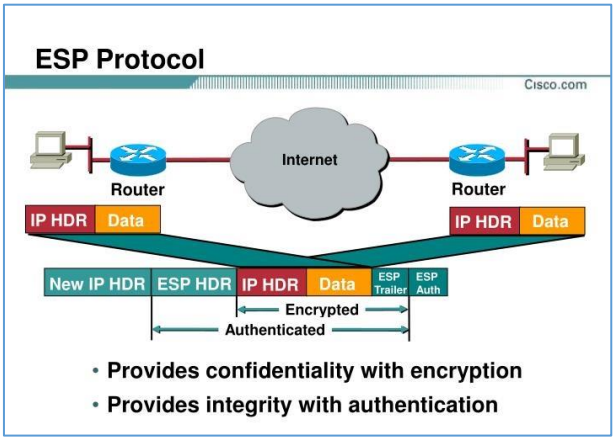
www.takbook.com

که این موضوع را در شکل ۴۱-۱۳، مشاهده می‌کنید، برای مشخص کردن پروتکل ESP بهتر است این کلمه را در فیلترینگ وارد کنید.



شکل ۴۱-۱۳ بررسی پروتکل ESP

در مورد پروتکل ESP می‌توان گفت که این پروتکل سه عملیات رمزنگاری، احرازهویت و محافظت را بر روی داده‌ها انجام می‌دهد، البته ESP از هدر بسته‌ها محافظت نمی‌کند و بسته‌هایی که در داخل بسته‌ی دیگر قرار می‌گیرند را رمزنگاری می‌کند، به طور کل در یک شبکه مبتنی بر IP اول هدر IP قرار می‌گیرد و پشت آن ESP، که در شکل ۴۲-۱۳، هدر کلی ESP را مشاهده می‌کنید.



شکل ۴۲-۱۳ بررسی پروتکل ESP

۷-۳-۲-۱۳ بررسی Remote Access VPNs

این روش با روش Site To Site متفاوت است، در روش قبلی دو روتر در دو منطقه مشخص از طریق VPN به هم متصل می‌شدند و سیستم‌هایی که در هر دو شبکه قرار داشت می‌توانستند با امنیت کامل هم دیگر را ببینند و به اطلاعات هم دسترسی داشته باشند.

www.takbook.com

اما زمانی پیش می‌آید که در یک مکان به غیر از شرکت خود قرار دارید و می‌خواهید به اطلاعات شبکه‌ی شرکت خود دسترسی داشته باشید، در آن موقع باید به فکر راه حل دیگری بود و آن هم استفاده از Remote Access VPN است.

VPNهای Remote Access برای ایجاد یک ارتباط از پروتکل امن Transport Layer Security (TLS) استفاده می‌کنند، TLS امروزه کاربرهای بسیاری دارد اما در اکثر موارد در پروتکل HTTPS از آن استفاده می‌شود.

پروتکل TLS یا همان Transport Layer Security پروتکل ارتباطی امن برای ارتباطات TCP است و هنگامی که با TLS ارتباط برقرار کرده باشد تمام اطلاعات رمزنگاری خواهد شد.

مثلاً برای دسترسی از طریق WEB به اطلاعات مالی شرکت، یک ارتباط HTTPS با پورت 443 با وب سرور شرکت برقرار شده و جلسه‌ای که بین کلاینت شما و وب سرور ایجاد می‌شود توسط پروتکل TLS رمزنگاری می‌شود، اصولاً TLS اطلاعات که بین سرور و کلاینت ردو بدل می‌شود و اطلاعات کاربری کاربران را رمزنگاری می‌کند.

برای اینکه در دستگاه‌های سیسکو این سرویس را داشته باشید نیاز به راه‌اندازی AnyConnect VPN دارید که این نرم‌افزار توسط فایروال سیسکو راه‌اندازی می‌شود، با اینکه این موضوع در سرفصل‌های دوره‌ی CCNA قرار ندارد ولی برای درک بیشتر شما آن را بررسی می‌کنیم.

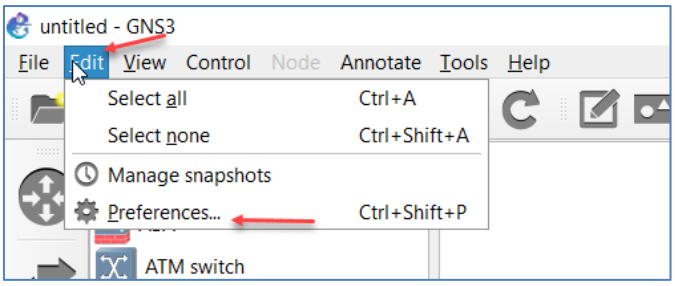
۸-۳-۲-۱۳ نصب و راه‌اندازی فایروال ASA

نکته: این بخش آموزشی در سرفصل‌های این کدام قرار ندارد و فقط برای دریافت بهتر Remote Access VPN بررسی می‌شود.

برای راه‌اندازی فایروال ASA در نرم‌افزار GNS3 باید از فایل qcow2 استفاده کنید، این فایل را می‌توانید از لینک زیر آن را دانلود کنید:

http://dl1.technet24.ir/Downloads/Cisco/ASA/asav9-14-1.qcow2

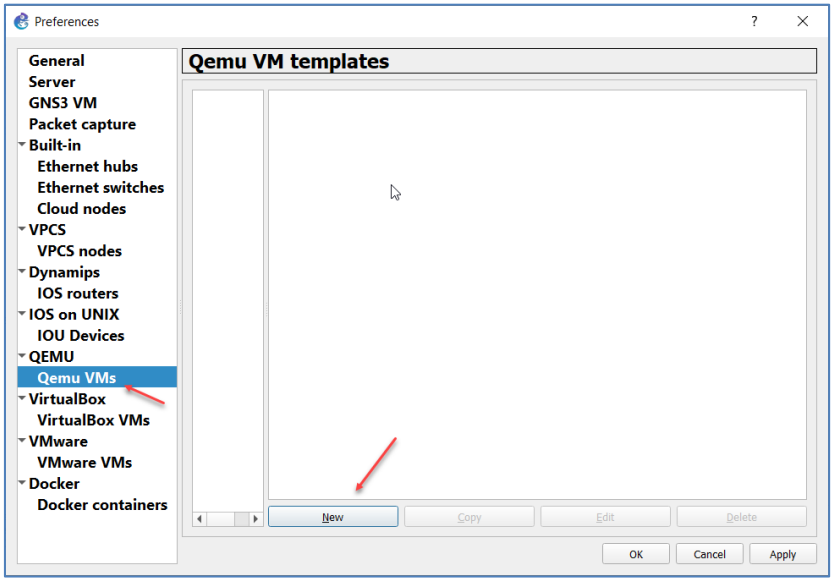
بعد از دانلود فایل مورد نظر، به مانند شکل ۴۳-۱۳، وارد نرم‌افزار GNS3 شوید و از منوی Edit بر روی گزینه‌ی Prefrences کلیک کنید.



شکل ۴۳-۱۳ بررسی GNS3

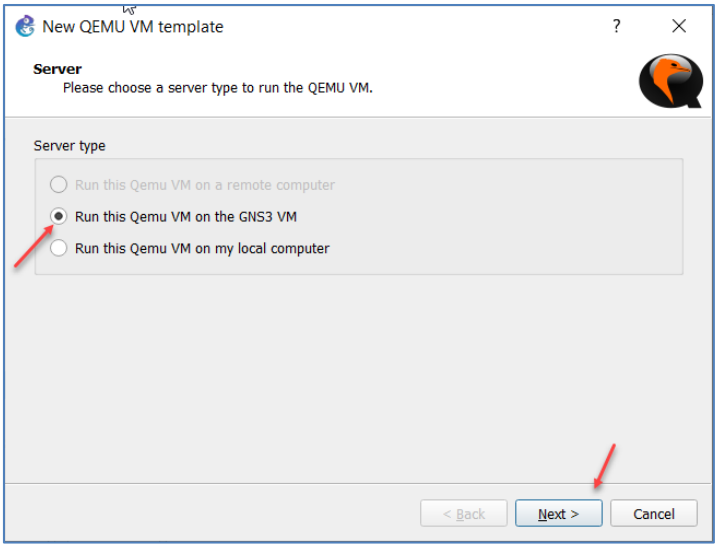
در شکل ۴۴-۱۳، برای اضافه کردن فایل ASA به نرم‌افزار GNS3 باید بر روی New کلیک کنید.

www.takbook.com



شکل ۴۴-۱۳ اضافه کردن فایروال سیسکو

در شکل ۴۵-۱۳، گزینه‌ی Run this Qemu vm on the GNS3 VM را انتخاب کنید تا فایل ASA بر روی ماشین GNS3 آپلود شود.

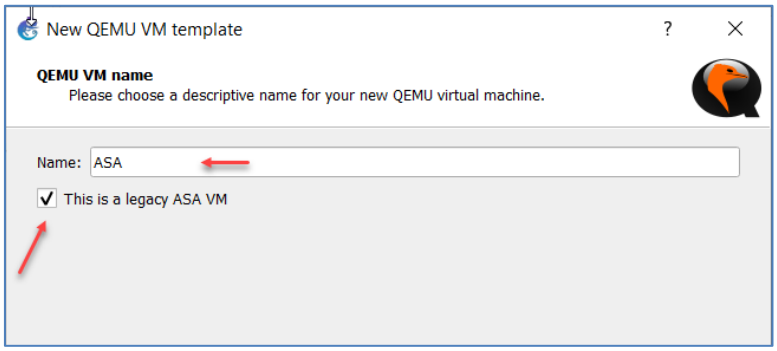


شکل ۴۵-۱۳ اضافه کردن فایروال سیسکو

به مانند شکل ۴۶-۱۳، یک نام برای فایروال خود در نظر بگیرید و تیک گزینه‌ی مورد نظر را هم انتخاب کنید، با این کار تنظیمات اضافه‌تری را در ادامه کار مشاهده خواهید کرد.

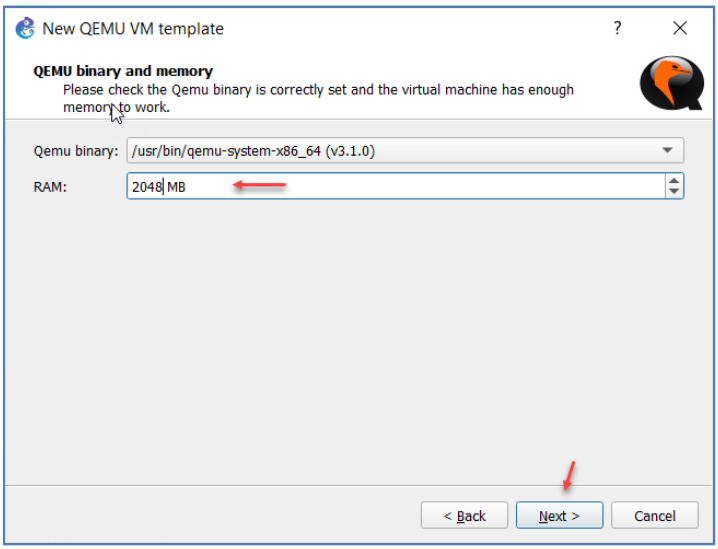
www.takbook.com

چنانچه از ویندوز ۱۰ یا ویندوز سرور ۲۰۱۹ استفاده می‌کنید نیاز به انتخاب این تیک نیست.



شکل ۴۶-۱۳ اضافه کردن فایروال سیسکو

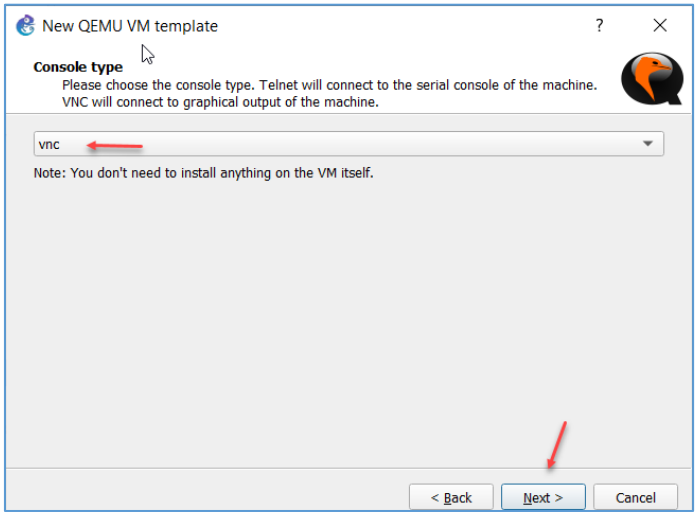
طبق شکل ۴۷-۱۳، مقدار رم مربوط به این دستگاه را مشخص کنید که بهتر است که حداقل ۲ گیگابایت باشد.



شکل ۴۷-۱۳ اضافه کردن فایروال سیسکو

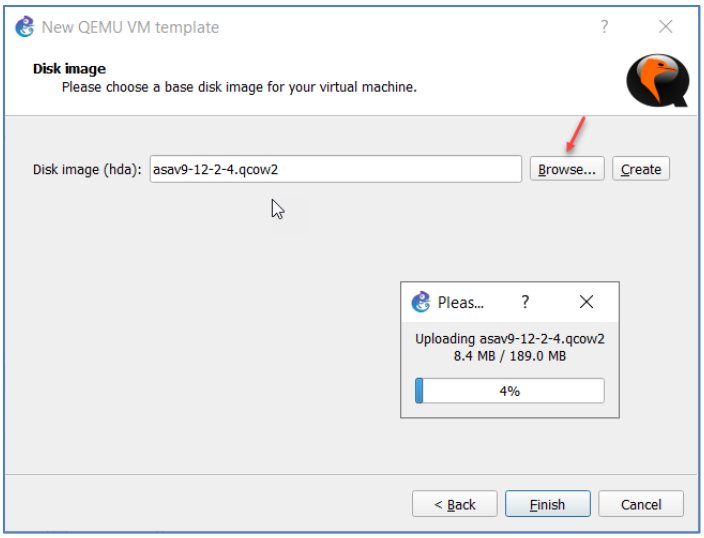
در شکل ۴۸-۱۳، گزینه‌ی VNC را انتخاب کنید، توجه داشته باشید به صورت پیش‌فرض گزینه‌ی Telnet برای آن فعال نشده است و باید بعد از اجرا شدن فایروال آن را فعال کنید.

www.takbook.com



شکل ۴۸-۱۳ اضافه کردن فایروال سیسکو

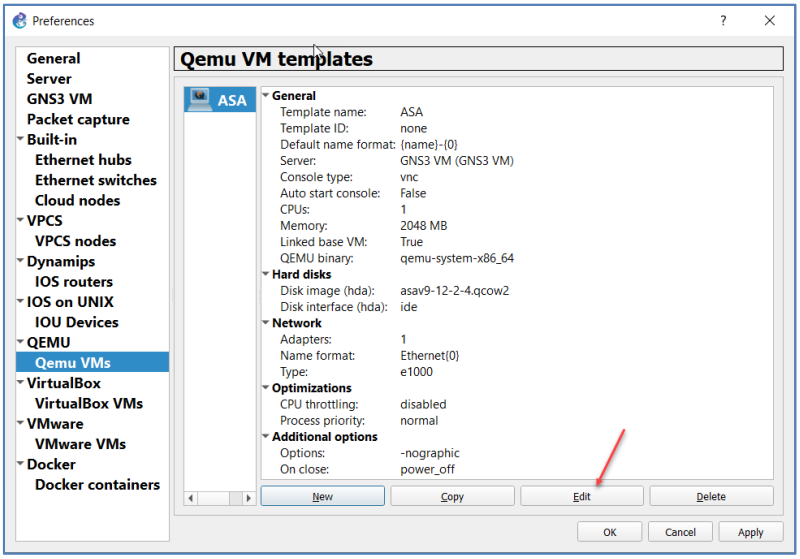
در شکل ۴۹-۱۳، باید بر روی Browse کلیک کنید و فایل دانلود شده مربوط به ASA که با پسوند qcow2 است را انتخاب کنید تا مانند شکل ۴۹-۱۳، آپلود انجام شود.



شکل ۴۹-۱۳ اضافه کردن فایروال سیسکو

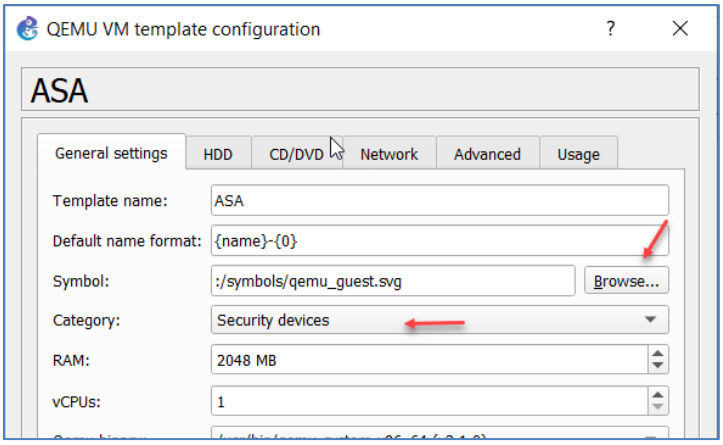
بعد از ایجاد فایروال ASA به مانند شکل ۵۰-۱۳، بر روی Edit کلیک کنید.

www.takbook.com



شکل ۵۰-۱۳ اضافه کردن فایروال سیسکو

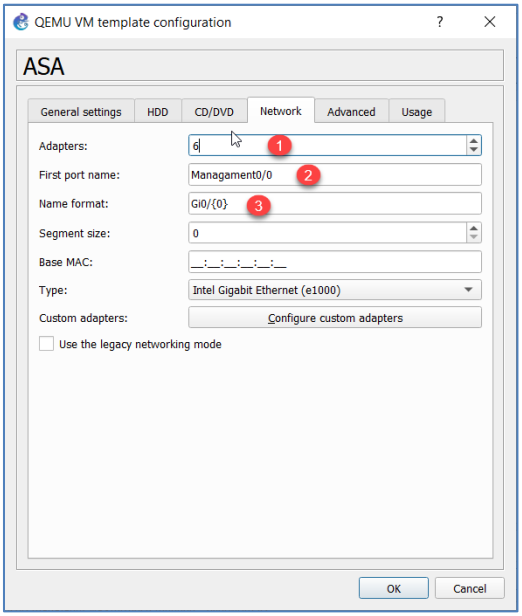
در شکل ۵۱-۱۳، در تب General از قسمت Symbol بر روی Browse کلیک کنید و آیکون مربوط به ASA را از لیست اول انتخاب کنید و از قسمت Category هم گزینه‌ی Secuirty Devices را انتخاب کنید.



شکل ۵۱-۱۳ اضافه کردن فایروال سیسکو

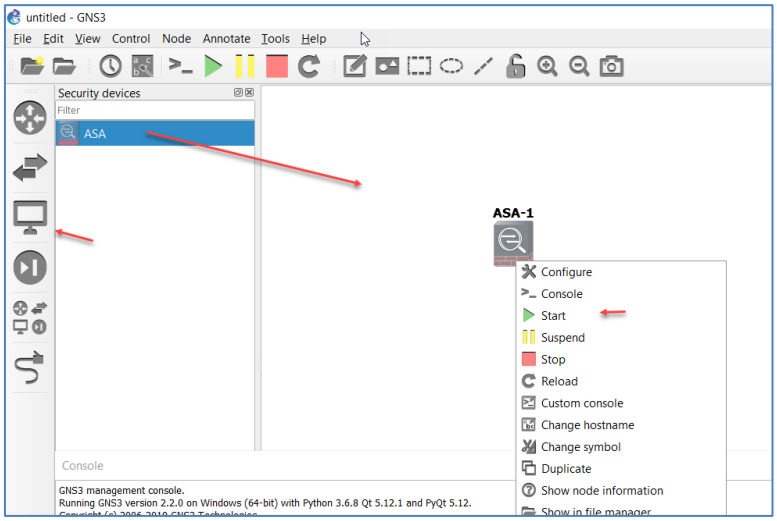
در تب Network و در قسمت Adapters عدد ۶ را وارد کنید تا ۶ کارت شبکه برای این دستگاه در نظر گرفته شود، در قسمت First Port Name نام Management0/0 را وارد کنید، که اولین پورت در ASA است، در قسمت Name format نام G0/{0} را وارد کنید تا ۵ پورت بعدی هم با نام Gigabite اسمگذاری شوند. توجه داشته باشید که اگر تنظیمات شکل ۵۲-۱۳را به درستی انجام ندهید، ASA به خوبی اجرا نخواهد شد.

www.takbook.com



شکل ۵۲-۱۳ اضافه کردن فایروال سیسکو

در شکل ۵۳-۱۳، بعد از ایجاد ASA از قسمت Security Devices آیکون ASA را کشیده و در صفحه رها کنید بر روی آن کلیک راست کنید و گزینه‌ی Start را کلیک کنید تا فایروال ASA روشن شود، اگر بر روی آن دو بار کلیک کنید کنسول VNC باز خواهد شد.

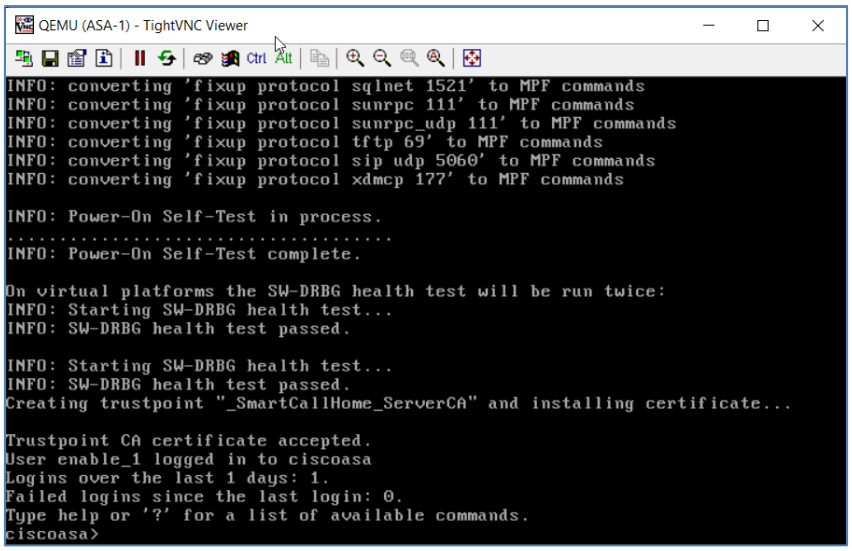


شکل ۵۳-۱۳ اضافه کردن فایروال سیسکو

همانطور که در شکل ۵۴-۱۳، مشاهده می‌کنید فایروال ASA به صورت کامل اجرا شده.

www.takbook.com

توجه داشته باشید در بعضی مواقع فایروال یک بار اجرا و بعد Restart می‌شود و دوباره شروع به بوت می‌کند که مشکلی خاصی نیست.



شکل ۵۴-۱۳ اجرای فایروال سیسکو

۹-۳-۲-۱۳ نصب و راه اندازی ASDM بر روی فایروال

نرم‌افزار ASDM به همراه فایروال ارائه می‌شود و برای تنظیم و ایجاد سیاست‌های سازمانی به صورت گرافیکی کاربرد دارد یعنی با نصب آن دیگر نیازی به وارد کردن اطلاعات به صورت Command نیست، البته همه‌ی دستورات را پشتیبانی نمی‌کند و در بعضی مواقع باید به صورت Command تنظیمات را انجام دهید.

برای شروع، اول باید بر روی Firewall آدرس IP را به صورت دستی و یا اتوماتیک تنظیم کنیم، در دستور زیر وارد Interface Managemet 0/0 می‌شویم و آدرس آن را 192.168.5.28 در نظر می‌گیریم.

ciscoasa(config)# **int management 0/0**

ciscoasa(config-if)# **ip address 192.168.5.28 255.255.255.0**

ciscoasa(config-if)# **nameif mgmt**

INFO: Security level for "mgmt" set to 0 by default.

ciscoasa(config-if)# **no sh**

بعد از وارد کردن IP حتماً باید برای هر Interface یک نام در در نظر بگیریم که این کار را با دستور Nameif mgmt انجام می‌دهیم که mgmt همان نام Interface است که در ادامه در مورد نام اینترفیس بیشتر توضیح خواهیم داد، در آخر هم باید اینترفیس مورد نظر را با دستور no shutdown روشن کنید.

www.takbook.com

در ادامه باید نرم‌افزار ASDM را اجرا کنیم برای این کار اول باید پروتکل HTTP را بر روی سرور فعال کنیم که برای این منظور از دستور زیر استفاده می‌کنیم:
با دستور زیر سرویس HTTP فعال خواهد شد

ciscoasa(config)# **http server enable**

با این دستور به فایروال اعلام می‌کنیم که شبکه ۱۹۲.۱۶۸.۵.۰ می‌تواند به سرویس HTTP دسترسی داشته باشد.

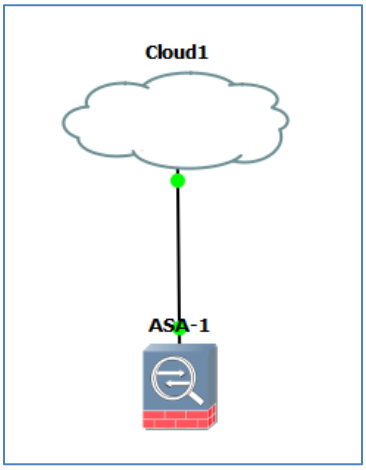
ciscoasa(config)# **http 192.168.5.0 255.255.255.0 mgmt**

برای اینکه دسترسی کامل شود باید پروتکل SSL را بر روی فایروال با دستور زیر فعال کنیم، در این دستور برای امنیت بیشتر از رمزنگاری‌ها و هش‌های مختلفی می‌توانید استفاده کنید.

ciscoasa(config)# **ssl encryption 3des-sha1 rc4-md5 aes256-sha1**

دستور بالا در نسخه‌های قدیمی‌تر ASA کاربرد داشته و در نسخه جدید نیازی به استفاده از این دستور نیست.

توجه داشته باشید برای دسترسی به ASA از طریق شبکه باید به مانند شکل ۵۵-۱۳، یک Cloud به صفحه اضافه کنید و آن را به ASA متصل کنید، فقط توجه داشته باشید که کارت شبکه آن را به درستی انتخاب کنید.



شکل ۵۵-۱۳ اجرای فایروال سیسکو

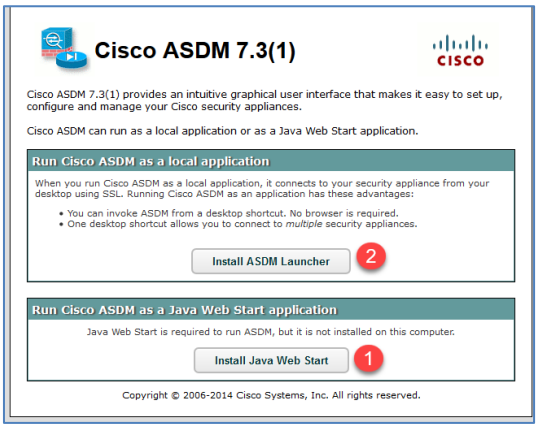
در ادامه وارد مرورگر خود شوید و آدرس زیر را اجرا کنید.

https://192.168.5.28/

بعد از اجرا کردن آدرس بالا شکل ۵۶-۱۳، ظاهر می‌شود که برای شروع کار اول باید گزینه‌ی دوم یعنی جاوا را از سایتش دانلود و نصب کنید، ورژنی که در این کتاب استفاده شده و با این فایروال ASA

www.takbook.com

همخوانی داشته ورژن Java Runtime Enviroment 8 Update 74 (64-bit) بوده که بدون مشکل اجرا شد، بعد از نصب جاوا بر روی شماره‌ی دو کلیک کنید که یک فایل نصبی برای شما دانلود خواهد شد آن را اجرا و نصب کنید و بعد از طریق Desktop یا Start آن را اجرا کنید،

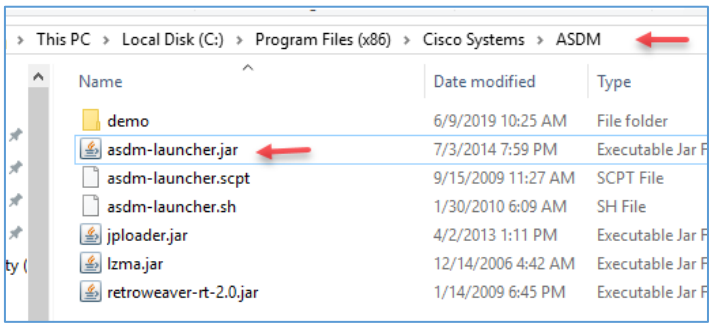


شکل ۵۶-۱۳ اجرای ASDM

اگر در این مسیرها فایل اجرایی را پیدا نکردید می‌توانید وارد آدرس زیر شوید و فایل را اجرا کنید.

C:\Program Files (x86)\Cisco Systems\ASDM

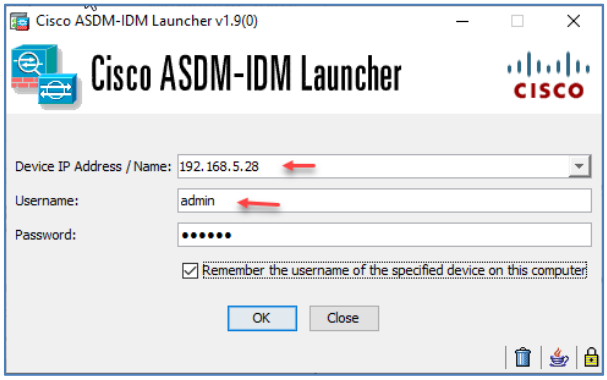
همانطور که در شکل ۵۷-۱۳، مشاهده می‌کنید در آدرس مورد نظر فایل asdm-launcher.jar را اجرا کنید.



شکل ۵۷-۱۳ اجرای ASDM

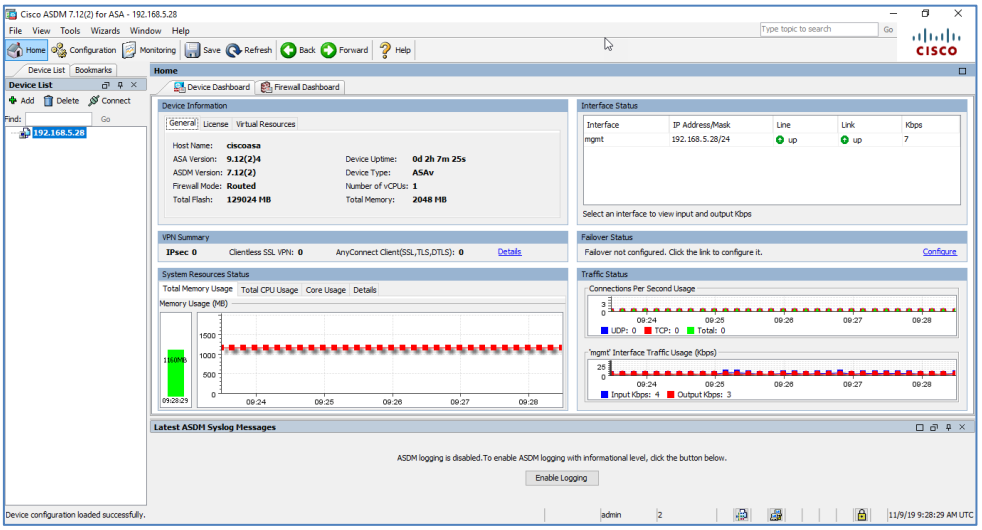
همانطور که در شکل ۵۸-۱۳، مشاهده می‌کنید ASDM-IDM به درستی اجرا شده است که در قسمت اول باید آدرس IP دستگاه ASA را وارد کنید و در ادامه باید یک نام کاربری و رمز عبور در ASA وارد کنید تا بتوانید در این قسمت استفاده کنید.

www.takbook.com



شکل ۵۸-۱۳ اجرای ASDM

همانطور که در شکل ۵۹-۱۳، مشاهده می‌کنید نرم‌افزار ASDM به درستی اجرا شده است، این نرم‌افزار داری بخش‌های مختلفی است، در تب Home داشبوردهای مختلفی را مشاهده می‌کنید، که در قسمت Device Information اطلاعات فایروال مانند نام، ورژن، نوع و ... را مشاهده می‌کنید، در قسمت Interface Status هم Interfaceهای فعال مشخص شده است، همانطور که می‌دانید در حال حاضر فقط یک Interface Management فعال شده است، مقدار مصرف رم و CPU را می‌توانید از قسمت System Resources Status مشاهده کنید، گزینه‌هایی دیگری هم وجود دارند که در صورت نیاز بررسی خواهیم کرد.



شکل ۵۹-۱۳ ASDM

۱۰-۳-۲-۱۳ کار با AnyConnect VPN در ASDM

در نظر بگیرید کارمندان یک سازمان به صورت دوره‌کاری از سرتاسر دنیا قرار است به شبکه داخلی شما متصل شوند و از منابع آن استفاده کنند، این موضوع نیاز به این دارد که امنیت و سرعت آن را

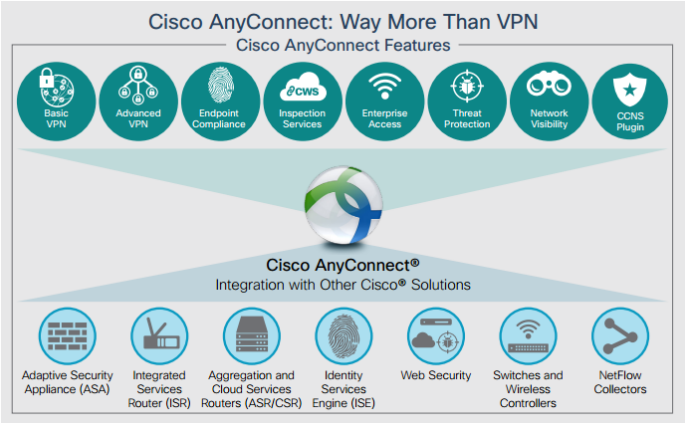
www.takbook.com

تضمین کنید، به خاطر همین موضوع شرکت سیسکو از VPN با نام AnyConnect استفاده کرده است که این امر را تحقق می‌بخشد.

در کنار اینکه شما با استفاده از AnyConnect به شبکه داخلی سازمان خود Remote می‌زنید می‌توانید از دیگر ویژگی‌های امنیتی آن هم استفاده کنید

شعار سیسکو برای این نرم‌افزار این است که به هر نوع دستگاهی در هر زمان و از هر مکان یک دسترسی ایمن و قابل اطمیان دهید.

در شکل ۶۰-۱۳، ویژگی‌های مهم AnyConnect را مشاهده می‌کنید که واقعاً قابل تامل است.

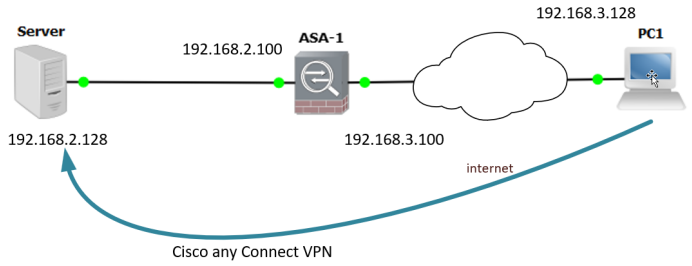


شکل ۶۰-۱۳ ASDM

در شکل ۶۱-۱۳، یک ASA سیسکو به همراه یک سرور و یک کلاینت را مشاهده می‌کنید که Server در شبکه داخلی قرار دارد و PC1 در شبکه outside یا خارجی، می‌خواهیم سرویس Anyconnect را در ASA راه‌اندازی کنیم تا PC1 بتوانید با VPN به شبکه inside یا همان شبکه 192.168.2.0 دسترسی پیدا کند.

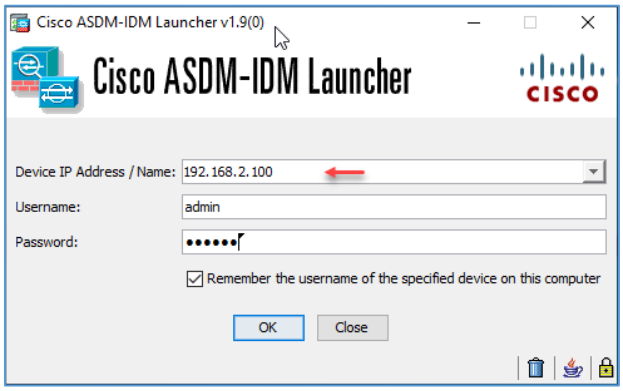
تنظیمات این قسمت، یک دستگاه ASA و سروری که در شبکه Inside قرار دارد یک ویندوز سرور ۲۰۱۲ است که بر روی VMware Workstation فعال شده است و از طریق کارت شبکه VMnet2 به این Cloud متصل شده است، منظور از Cloud همین سرور است که آیکون آن را از ابر به سرور تغییر دادیم، قرار است که Pc1 بتواند بعد از ارتباط anyconnect یک وب سایت را در سرور باز کند.

www.takbook.com



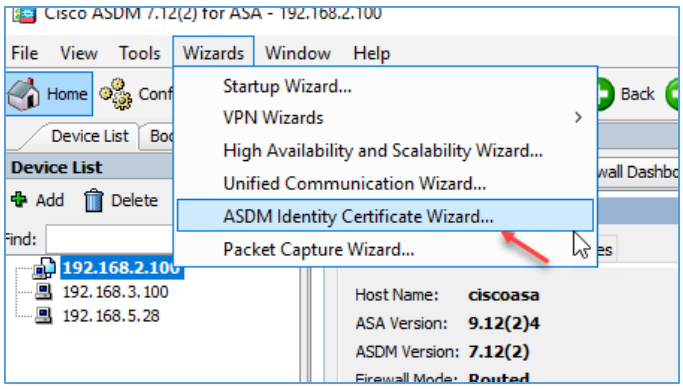
شکل ۱۳-۶۱ *ASA Cisco*

بعد از انجام تنظیمات در فایروال ASA-1 باید به مانند شکل ۶۲-۱۳، از طریق ASDM به آن متصل شویم که از طریق آدرس 192.168.2.100 که بر روی Inisde ست شده است این کار را انجام می‌دهیم.



شکل ۱۳-۶۲ *ASDM Cisco*

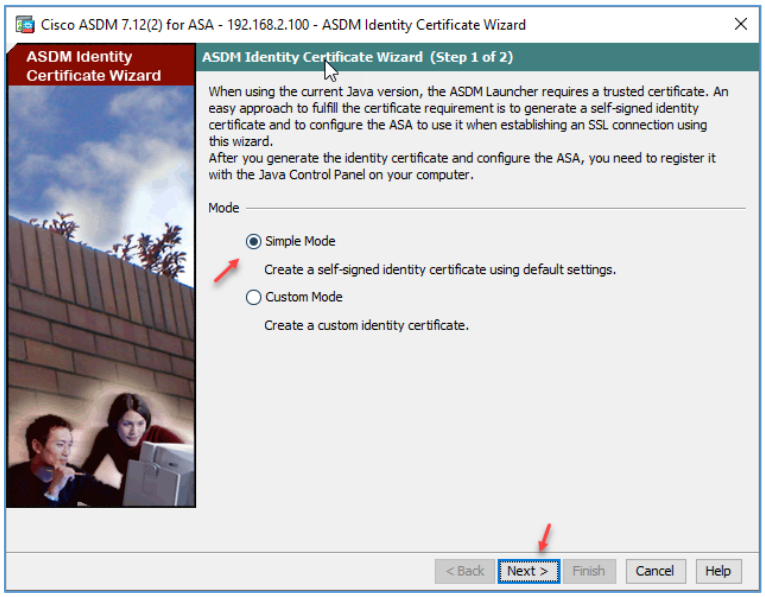
به مانند شکل ۶۳-۱۳، بعد از ورود به ASDM از طریق منوی Wizards گزینه‌ی ASDM identity Certificate Wizard را انتخاب کنید.



شکل ۱۳-۶۳ تنظیمات *AnyConnect VPN*

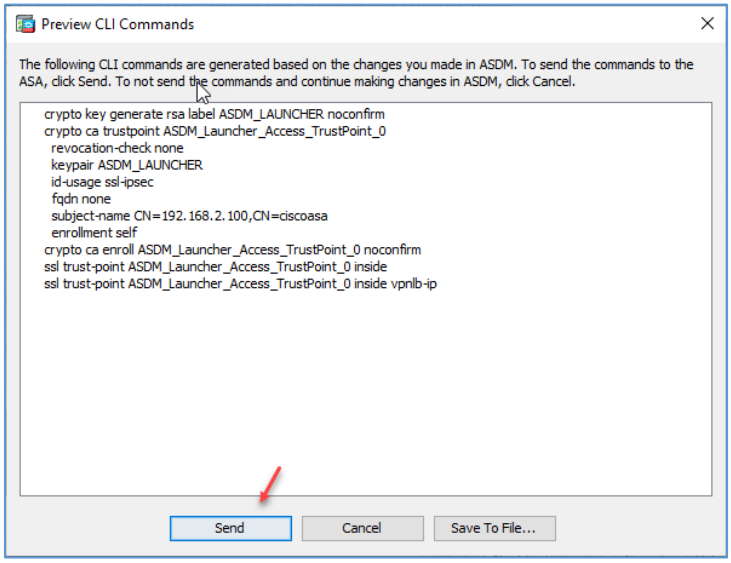
www.takbook.com

در شکل ۶۴-۱۳، در این قسمت گزینه‌ی simple Mode را انتخاب کنید.



شکل ۶۴-۱۳ تنظیمات AnyConnect VPN

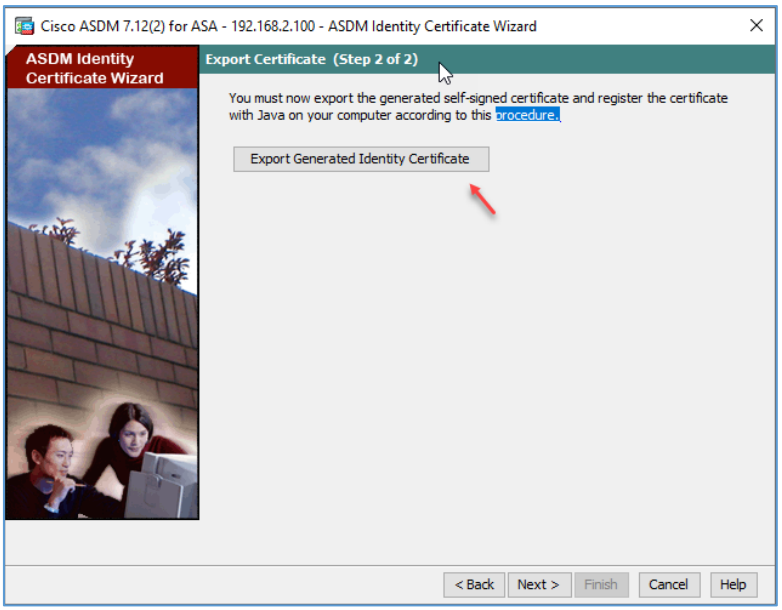
در شکل ۶۵-۱۳، دستوراتی که برای این عملیات مورد نیاز است مشخص شده است، که با کلیک بر روی Send دستورات بر روی فایروال اعمال می‌شود.



شکل ۶۵-۱۳ تنظیمات AnyConnect VPN

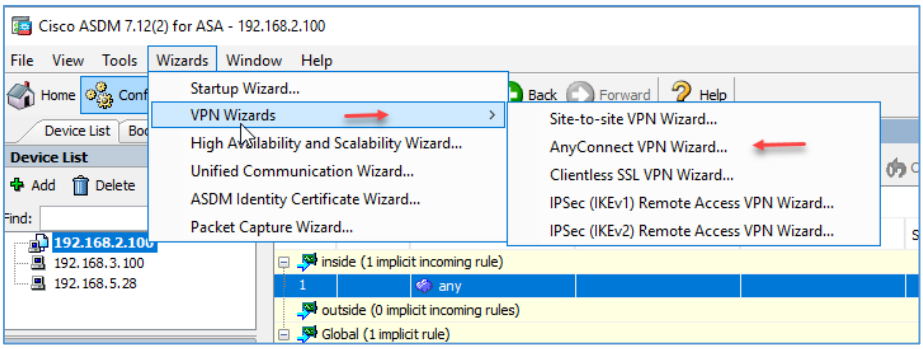
www.takbook.com

در شکل ۶۶-۱۳، هم می‌توانید با کلیک بر روی گزینه‌ی مورد نظر از CA یا همان Certificate ایجاد شده یک Export تهیه کنید.



شکل ۶۶-۱۳ تنظیمات AnyConnect VPN

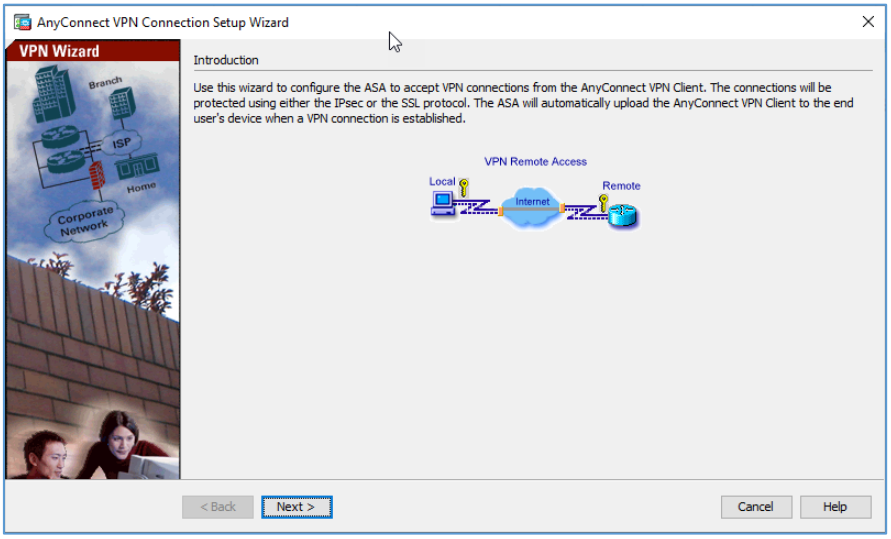
بعد از انجام مراحل بالا به مانند شکل ۶۷-۱۳، وارد منوی Wizards شوید و از قسمت VPN Wizards گزینه‌ی AnyConnect VPN Wizard را انتخاب کنید.



شکل ۶۷-۱۳ تنظیمات AnyConnect VPN

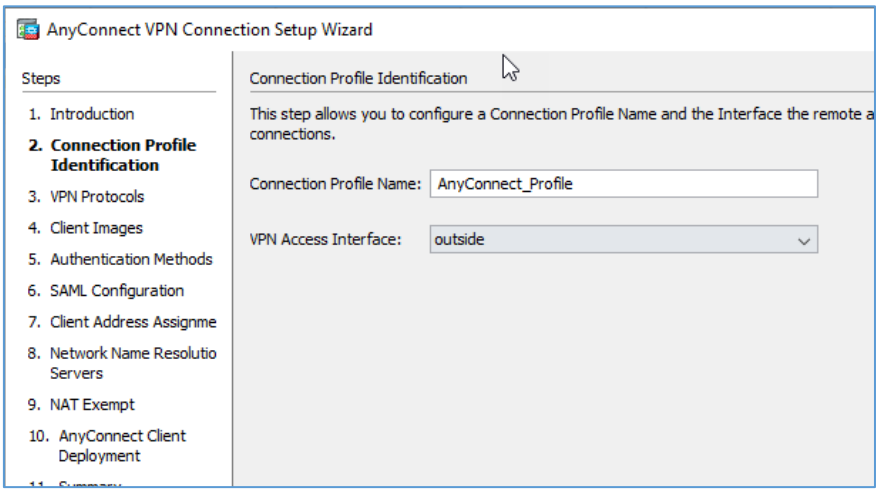
در شکل ۶۸-۱۳، در صفحه اول نحوه ارتباط بین شبکه داخلی و خارجی با شکل مشخص شده است، بر روی Next کلیک کنید.

www.takbook.com



شکل ۶۸-۱۳ تنظیمات AnyConnect VPN

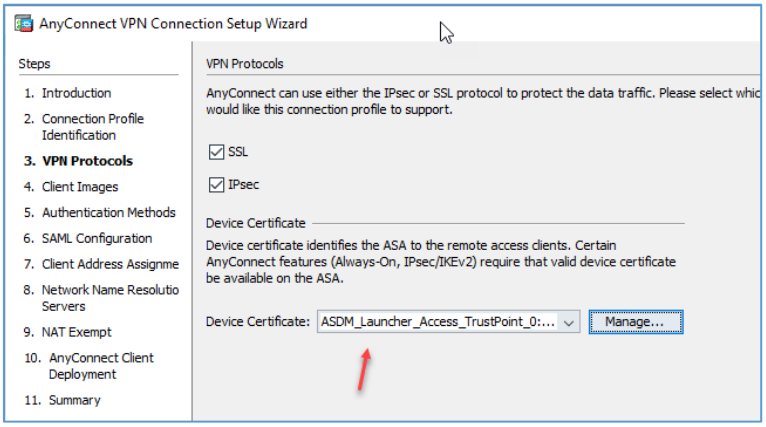
در صفحه‌ی زیر باید یک نام برای Profile خود وارد کنید و در قسمت VPN Access Interface باید مشخص کنید که سرویس VPN بر روی کدام پورت اجازه کار داشته باشد که در اینجا پورت outside که شبکه خارجی است انتخاب شده است.



شکل ۶۹-۱۳ تنظیمات AnyConnect VPN

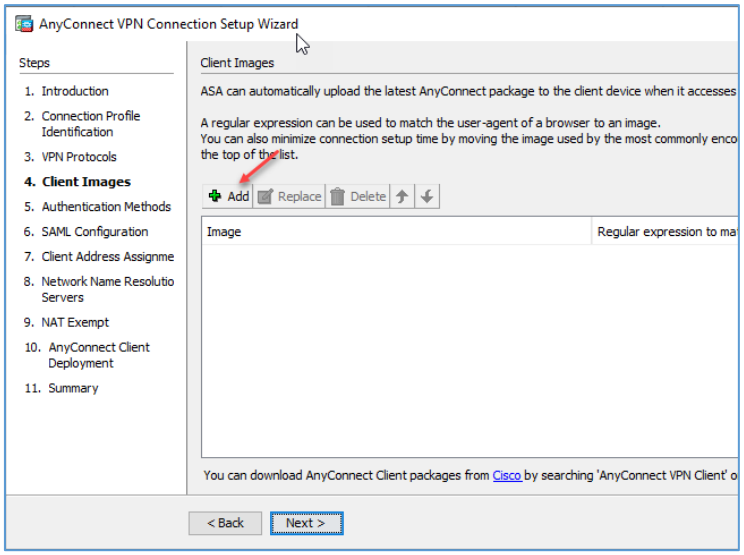
در شکل ۷۰-۱۳، باید تیک هر دو گزینه را انتخاب کنید تا امنیت کار هم از طریق گواهی‌نامه‌ی SSL و هم از طریق IPsec چک شود، در قسمت Device Certificate باید همان گواهینامه‌ای که در قسمت اول این بحث ایجاد کردید را انتخاب و بر روی Next کلیک کنید.

www.takbook.com



شکل ۷۰-۱۳ تنظیمات AnyConnect VPN

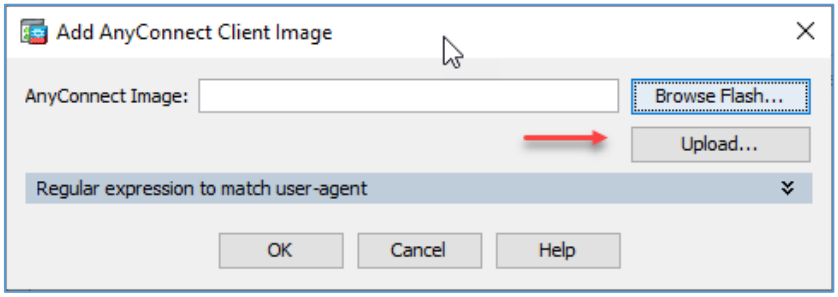
در صفحه‌ی ۷۱-۱۳، باید آخرین پکیج AnyConnect را از سایت سیسکو دانلود و به نرم‌افزار معرفی کنید، فایل Anyconnect باید با پسوند pkg باشد که اگر موفق نشدید آن را از سایت Cisco دانلود کنید؛ می‌توانید از این قسمت دانلود کنید، بعد از دانلود بر روی Add کلیک کنید.



شکل ۷۱-۱۳ تنظیمات AnyConnect VPN

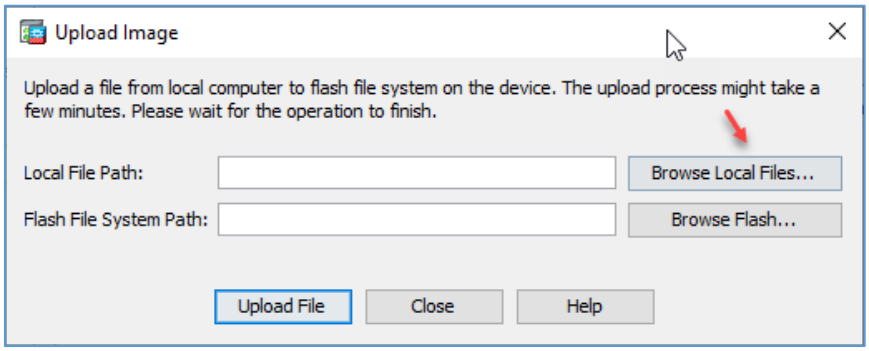
به مانند شکل ۷۲-۱۳، چنانچه فایل از قبل در حافظه Flash دستگاه فایروال موجود باشد باید بر روی Browse Flash کلیک کنید و اگر هم فایل را دانلود کردید بر روی Upload کلیک کنید.

www.takbook.com



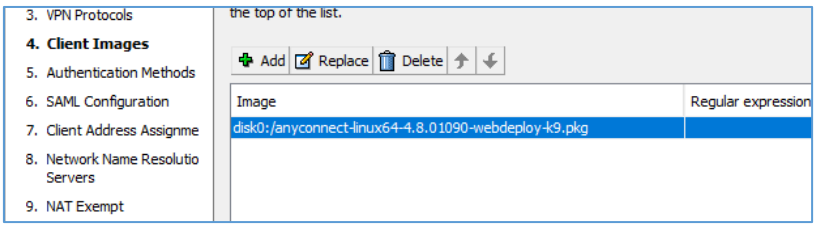
شکل ۱۳-۷۲ تنظیمات AnyConnect VPN

در شکل ۱۳–۷۳، بر روی Browse Local Files کلیک کنید و فایل مورد نظر را انتخاب و Upload کنید.



شکل ۱۳-۷۳ تنظیمات AnyConnect VPN

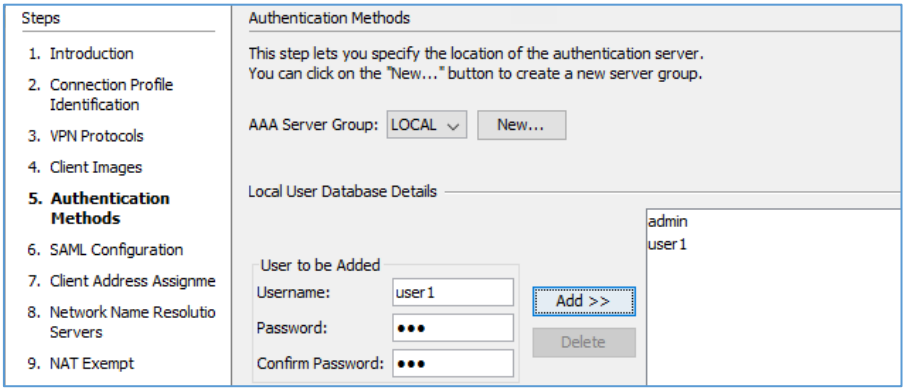
همانطور که در شکل ۱۳–۷۴، مشاهده می‌کنید فایل (anyconnect-win-4.8.01090-webdeploy-k9.pkg) آپلود و به لیست اضافه شده است، برای ادامه کار بر روی Next کلیک کنید.



شکل ۱۳-۷۴ تنظیمات AnyConnect VPN

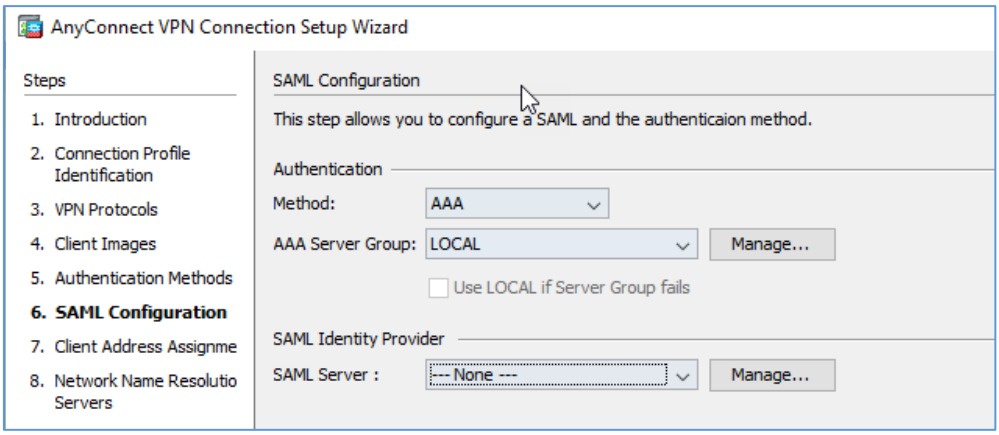
در شکل ۱۳–۷۵، اگر از سرور ACS یا ISE برای بحث احرازهویت استفاده می‌کنید می‌توانید بر روی New کلیک کنید و آدرس سرور را با تنظیمات آن وارد کنید، در غیر این صورت باید نام کاربری و رمز عبور داخلی فایروال را انتخاب کنید، البته در پائین صفحه می‌توانید کاربر دلخواه خود را اضافه یا حذف کنید، توجه داشته باشید کاربر Admin که از قبل ایجاد کرده بودیم در لیست وجود دارد.

www.takbook.com



شکل ۱۳-۷۵ تنظیمات *AnyConnect VPN*

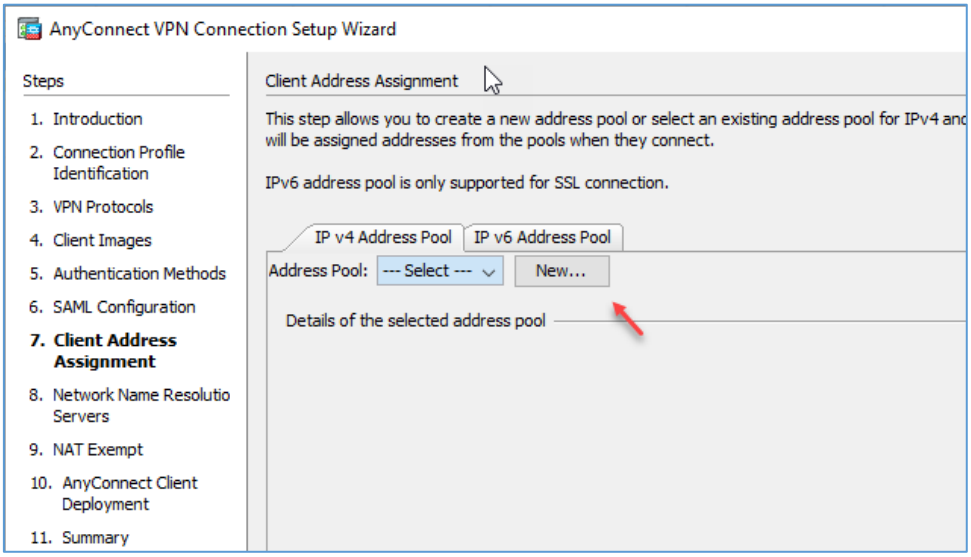
در شکل ۱۳-۷۶، اگر سرور Authentication یا همان احراز هویت داخلی دارید گزینه‌ی Local را انتخاب کنید و یا اگر از سرور خارجی مانند ACS استفاده می‌کنید باید گزینه را تغییر دهید.



شکل ۱۳-۷۶ تنظیمات *AnyConnect VPN*

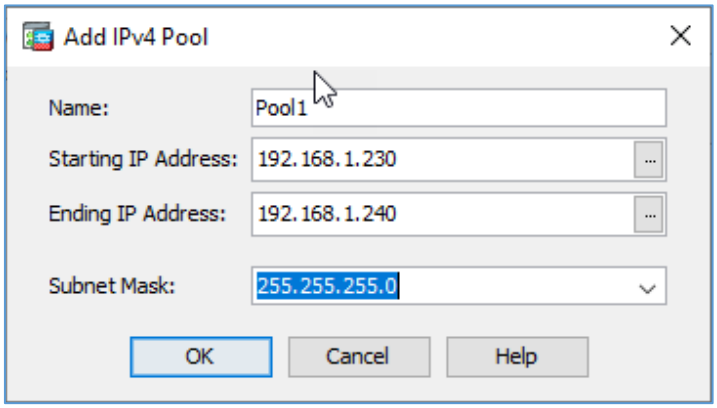
در شکل ۱۳-۷۷، باید یک Pool یا یک رنج IP برای کلاینت‌هایی که می‌خواهند با VPN به شبکه داخلی متصل شوند ایجاد کنید، برای این کار در قسمت IPV4 بر روی New کلیک کنید.

www.takbook.com



شکل ۱۳-۷۷ تنظیمات AnyConnect VPN

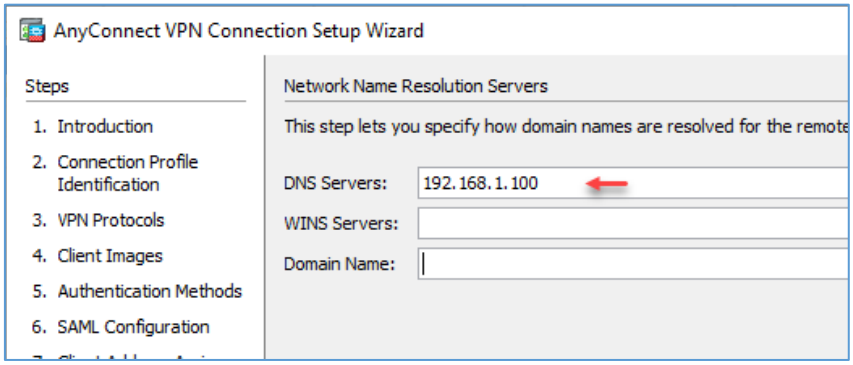
در شکل ۱۳-۷۸، نام، رنج IP و Subnet را برای این Pool مشخص کنید، زمانی که کاربران از AnyConnect برای متصل شدن استفاده کنند یکی از این آدرس‌ها به صورت اتوماتیک به آنها اختصاص داده می‌شود.



شکل ۱۳-۷۸ تنظیمات AnyConnect VPN

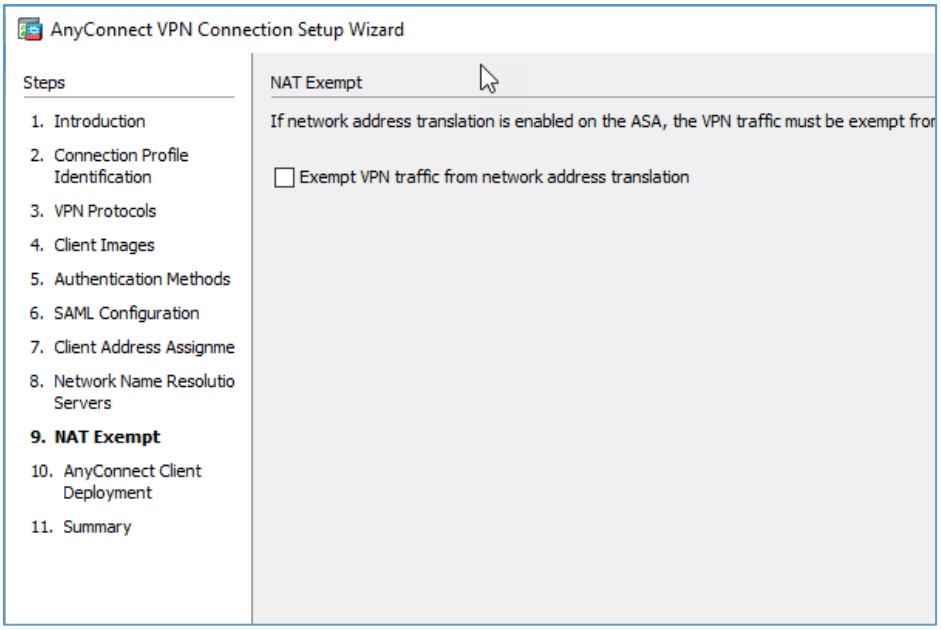
در شکل ۱۳-۷۹، باید آدرس DNS, WINS و نام Domain را مشخص کنید.

www.takbook.com



شکل ۷۹-۱۳ تنظیمات AnyConnect VPN

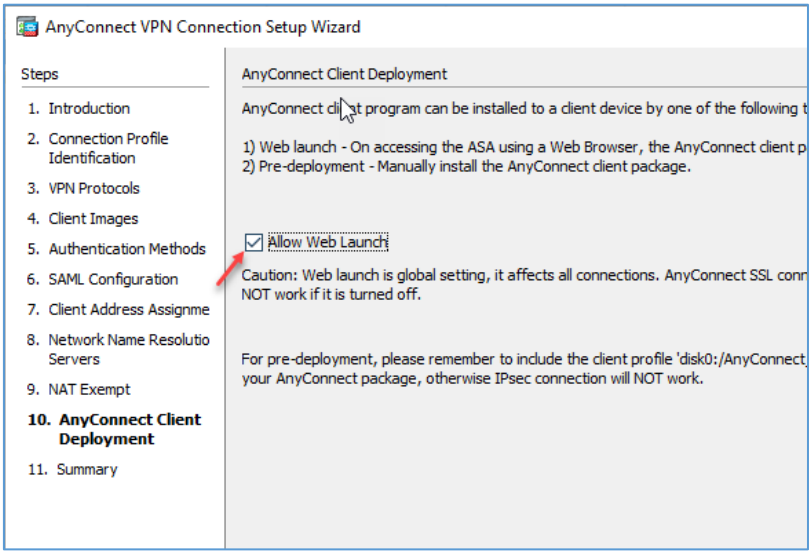
در شکل ۸۰-۱۳، از پروتکل NAT در فایروال خود استفاده می‌کنید برای تبدیل آدرس باید تیک گزینه‌ی مورد نظر را انتخاب کنید تا کارایی آن حفظ شود.



شکل ۸۰-۱۳ تنظیمات AnyConnect VPN

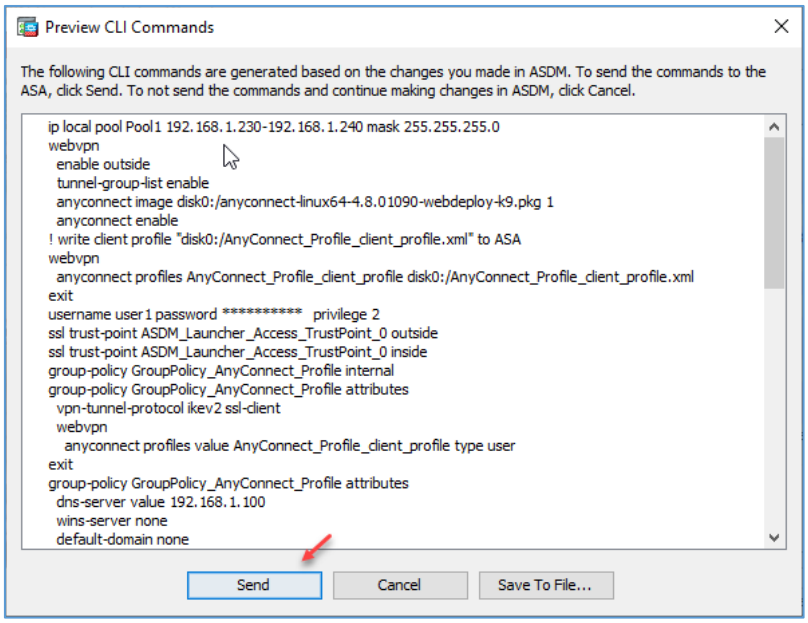
در شکل ۸۱-۱۳، برای اینکه به نرم‌افزار Anyconnect برای کلاینت‌ها دسترسی داشته باشیم می‌توانیم تیک گزینه‌ی Allow Web Launch را انتخاب کنید، بر روی Next کلیک کنید.

www.takbook.com



شکل ۸۱-۱۳ تنظیمات AnyConnect VPN

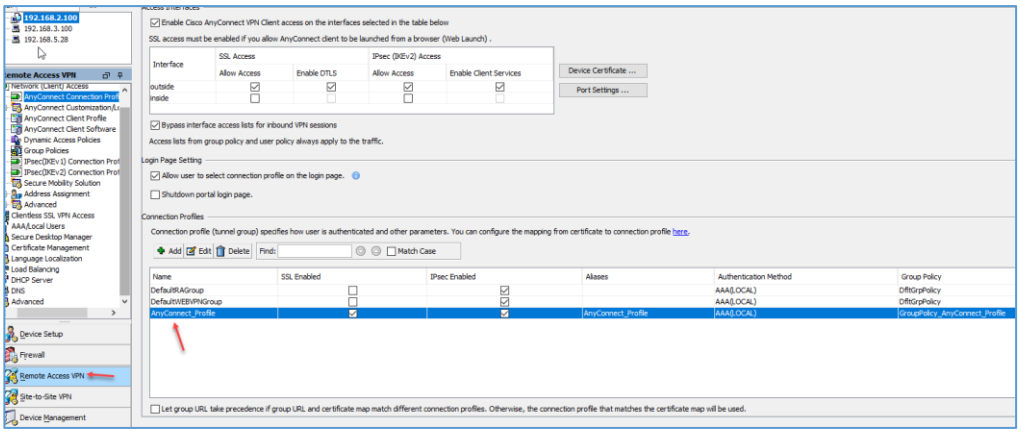
در شکل ۸۲-۱۳، اگر بر روی Finish کلیک کنید، دستورات نهایی به مانند شکل ۸۲-۱۳، ظاهر می‌شوند و با کلیک بر روی Send روی فایروال اعمال می‌شوند.



شکل ۸۲-۱۳ تنظیمات AnyConnect VPN

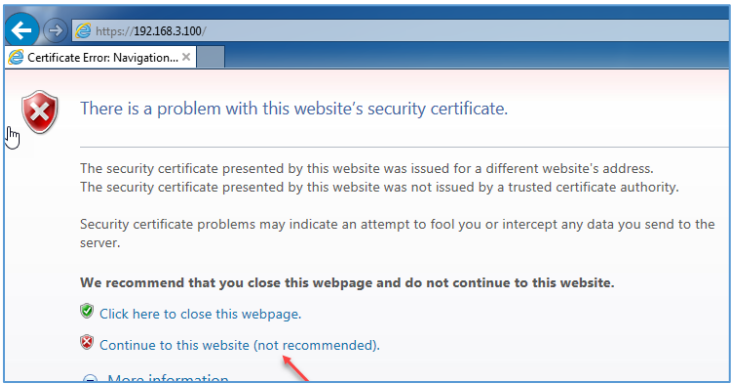
www.takbook.com

همانطور که در شکل ۸۳-۱۳، مشاهده می‌کنید پروفایل مورد نظر برای دسترسی کلاینت‌ها ایجاد شده است و همه چیز برای اتصال کلاینت به فایروال از طریق VPN امکان پذیر است.



شکل ۸۳-۱۳ تنظیمات AnyConnect VPN

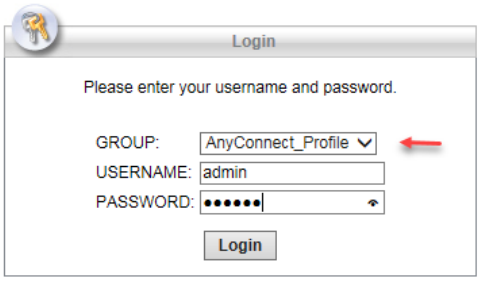
در ادامه باید وارد کلاینت (PC1) شویم و AnyConnect را تست بگیریم، همانطور که گفتیم برای اینکه به نرم‌افزار AnyConnect دسترسی داشته باشیم دو راه وجود دارد، یکی اینکه فایل (anyconnect-win-4.8.01090-predeploy-k9.zip) را دانلود و بر روی کلاینت نصب کنید و یا اینکه یک مرورگر باز کنید و آدرس پورت outside که 192.168.3.100 است را در مرورگر به صورت https://192.168.3.100 وارد کنید که در شکل ۸۴-۱۳، این موضوع را مشاهده می‌کنید با وارد شدن به آدرس فایروال صفحه زیر ظاهر می‌شود که باید بر روی Continue to this website کلیک کنید تا از گواهینامه امنیتی نامعتبر آن صرفنظر کند.



شکل ۸۴-۱۳ تنظیمات AnyConnect VPN

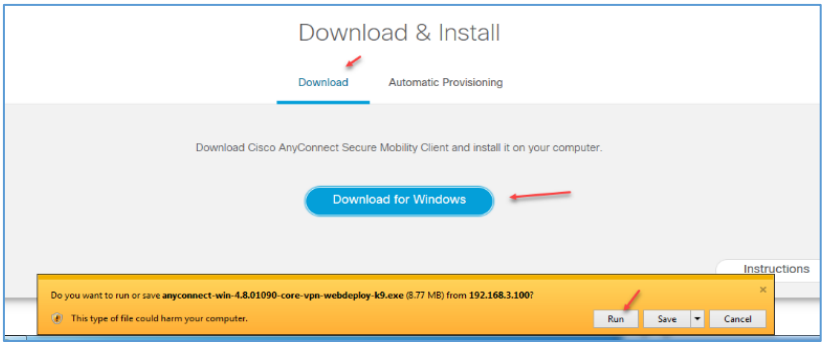
در صفحه بعد که در شکل ۸۵-۱۳، مشاهده می‌کنید، باید پروفایلی را که در قسمت قبل ایجاد کردیم را انتخاب و نام کاربری و رمز عبور تعریف شده در فایروال را وارد و بر روی Login کلیک کنید.

www.takbook.com



شکل ۱۳-۸۵ AnyConnect VPN

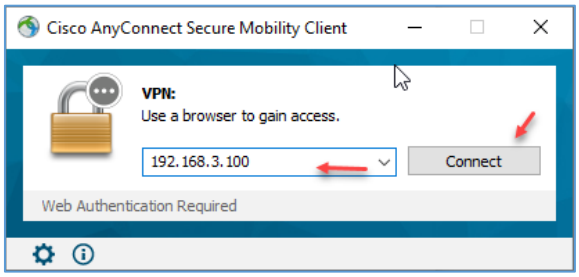
بعد از ورود با شکل ۸۶-۱۳، روبرو خواهید شد، که باید وارد تب Download شوید و بر روی Download for Windows کلیک کنید و در نوار باز شده بر روی Run کلیک کنید و آن را نصب کنید.



شکل ۱۳-۸۶ AnyConnect VPN

در زمان راه‌اندازی AnyConnect باید فایل‌های مربوط به Any Connect که برای ورژن‌های مختلف از سیستم‌عامل است را در فایروال آپلود کنید تا زمانی که در دستگاه‌های مختلف این آدرس سایت را باز می‌کنید ورژن مخصوص به آن برای شما باز شود.

بعد از نصب، آن را اجرا کرده و به مانند شکل ۸۷-۱۳، آدرس outside فایروال را که در اینجا 192.168.3.100 است را وارد کنید و بر روی Connect کلیک کنید.



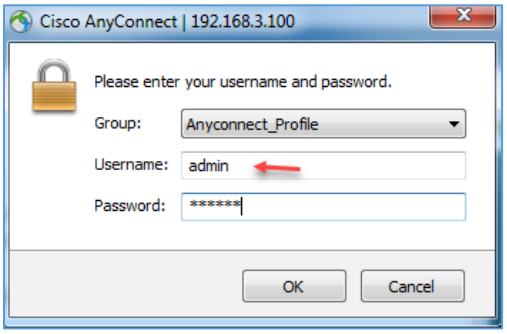
شکل ۱۳-۸۷ AnyConnect VPN

www.takbook.com

در هنگام Connect به علت معتبر نبودن Certificate با اخطار شکل ۸۸-۱۳، مواجه خواهید شد که باید بر روی Connect Anyway کلیک کنید.

شکل ۸۸-۱۳ AnyConnect VPN

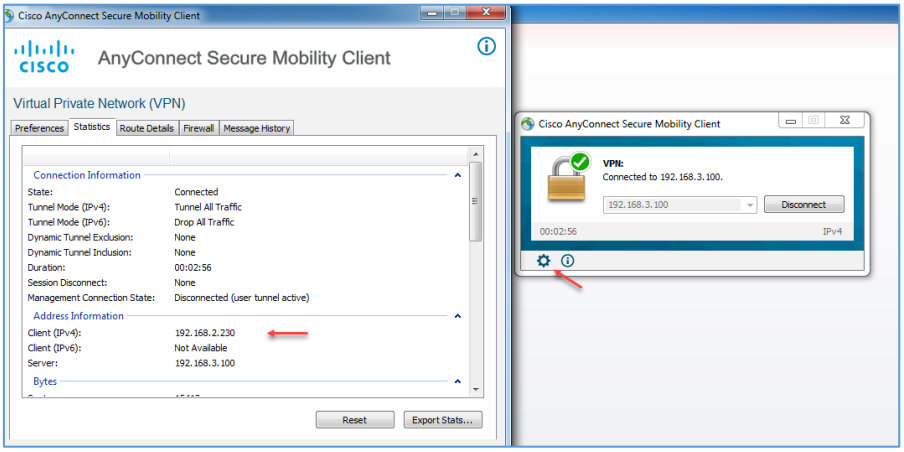
در شکل ۸۹-۱۳، باید پروفایل مورد نظر خود را انتخاب و نام کاربری و رمز عبور تعریف شده را وارد و بر روی OK کلیک کنید.



شکل ۸۹-۱۳ AnyConnect VPN

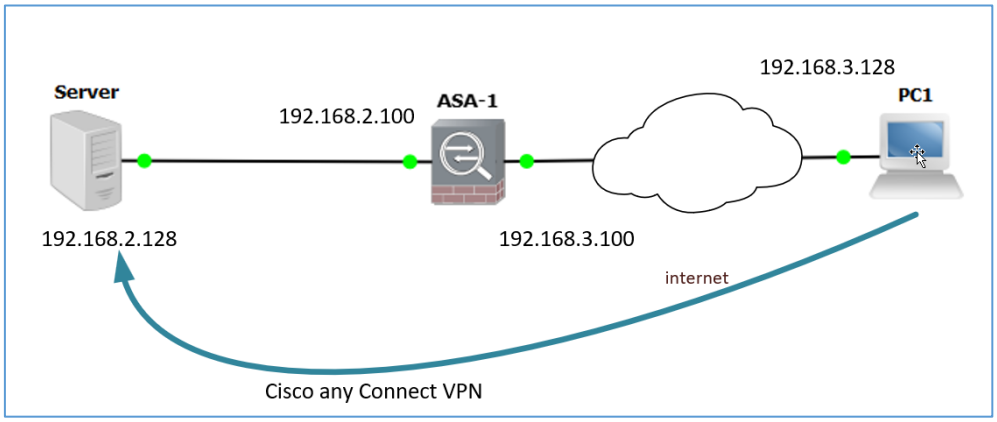
همانطور که در شکل ۹۰-۱۳، مشاهده می‌کنید، VPN متصل شده است و برای اینکه جزئیات آن را مشاهده کنید باید بر روی آیکون مورد نظر کلیک کنید، در تب Statistics آدرس IP، مقدار زمان متصل بودن و بقیه جزئیات نوشته شده است.

www.takbook.com



شکل ۱۳-۹۰ *AnyConnect VPN*

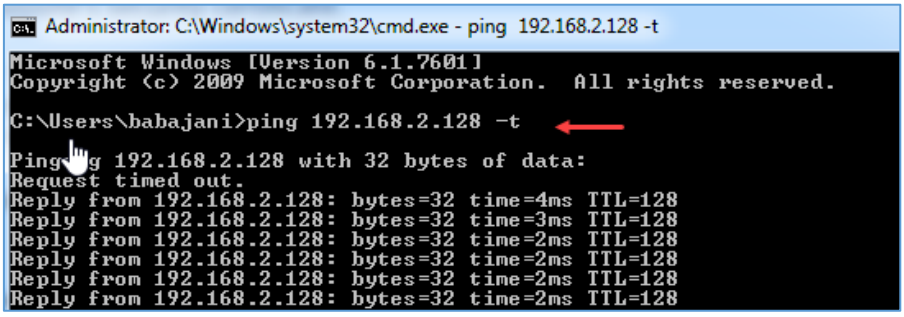
به سناریو خود باز می‌گردیم در این سناریو توانستیم از طریق PC1 با استفاده از AnyConnect VPN به فایروال ASA-1 متصل شدیم و حالا باید شبکه 192.168.2.0 را مشاهده کنیم، برای اینکه بیشتر با کار آشنا شوید، بر روی سرور با آدرس 192.168.2.128 سرویس IIS راه‌اندازی کردیم و می‌خواهیم از طریق PC1 سایت سرور را باز کنیم.



شکل ۱۳-۹۱ *AnyConnect VPN*

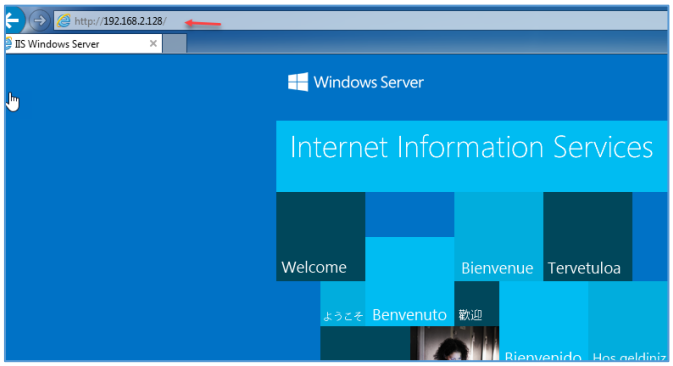
همانطور که در شکل ۹۲-۱۳، مشاهده می‌کنید بعد از متصل شدن VPN توانستیم از طریق PC1 سرور 192.168.2.128 را Ping بگیریم.

www.takbook.com



شکل ۹۲-۱۳ AnyConnect VPN

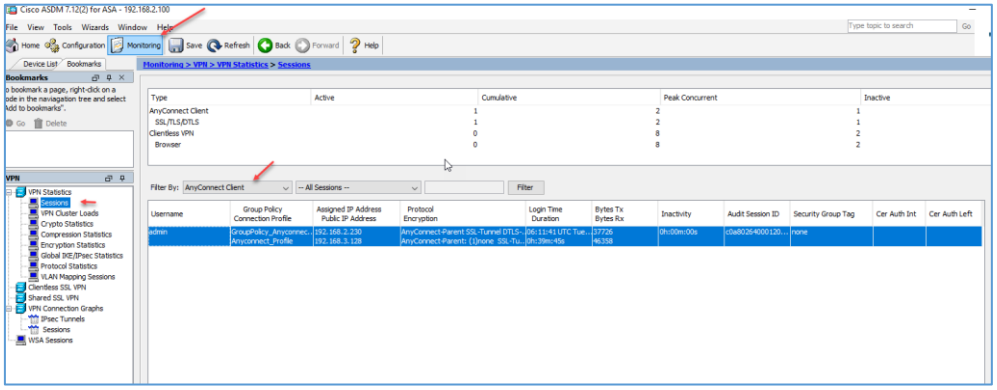
در شکل ۹۳-۱۳، وب سایت سرور را مشاهده می‌کنید که از طریق PC1 توانستیم آن را باز کنیم.



شکل ۹۳-۱۳ AnyConnect VPN

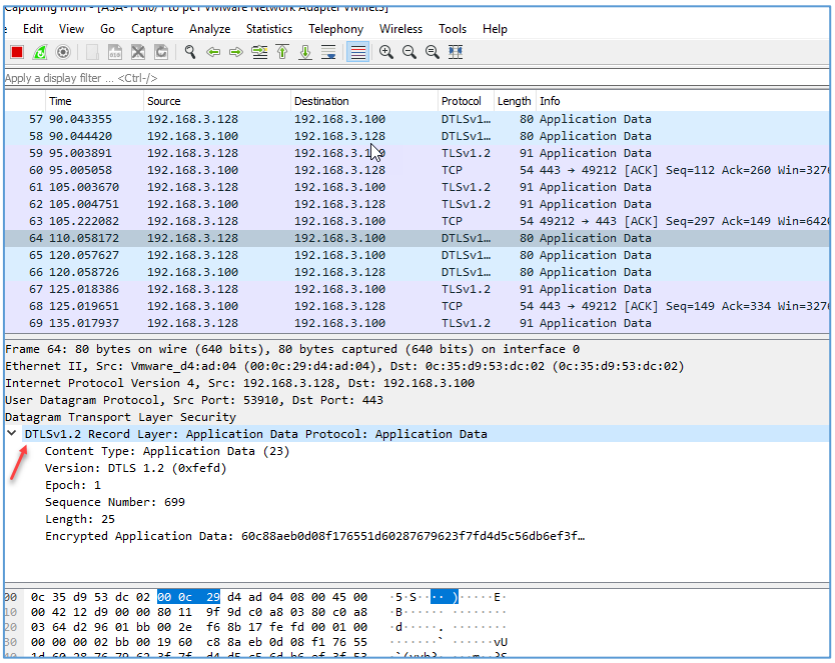
به مانند شکل ۹۴-۱۳، نرم‌افزار ASDM را باز کنید و وارد تب Monitoring شوید، در این صفحه از سمت چپ بر روی VPN کلیک کنید و از بین گزینه‌های موجود بر روی Sessions کلیک کنید، در این قسمت تمام کانکشن‌هایی که به فایروال زده شده مشخص می‌شود، برای اینکه کانکشن مربوط به AnyConnect را مشاهده کنیم باید از قسمت Filter By گزینه‌ی AnyConnect Client را انتخاب کنید که در شکل ۹۴-۱۳، این موضوع مشخص شده است و کانکشنی که از PC1 با آدرس 192.168.3.128 به فایروال زدیم مشخص شده است.

www.takbook.com



شکل ۱۳-۹۴ *AnyConnect VPN*

بعد از ارتباط vpn، برای اینکه جزئیات ارتباط بین کلاینت و فایروال را مشاهده کنیم بر روی خط بین دو دستگاه کلیک راست کنید و گزینه‌ی Start capture را انتخاب کنید، همانطور که در شکل ۹۵-۱۳، مشاهده می‌کنید دو پروتکل DTLS و TLS که برای ارتباط VPN است در حال کار است و اطلاعات بین دو دستگاه را رمزنگاری کرده است، DTLS با UDP و پروتکل TLS با TCP کار می‌کنند.



شکل ۱۳-۹۵ *WireShark*

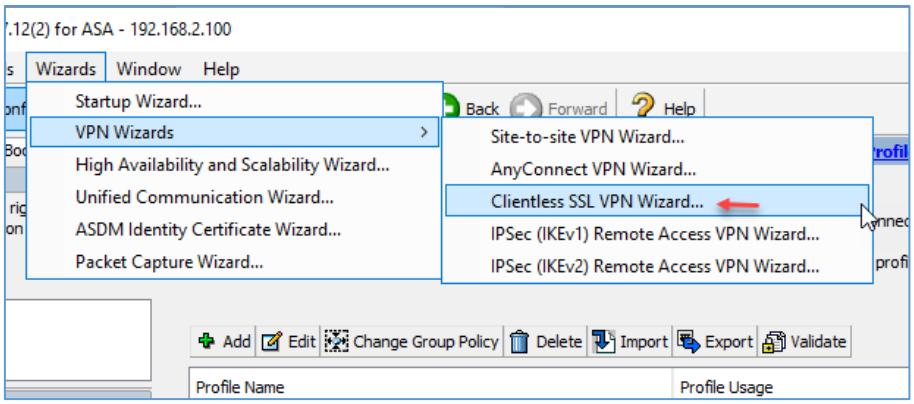
۱۱-۳-۲-۱۳ کار با Clientless SSL VPN در ASDM

در این قسمت بدون اینکه نیازی به ارتباط از طریق VPN داشته باشیم، دسترسی به منابع شبکه داخلی از طریق Web انجام می‌شود، یعنی اینکه می‌توانید سایت‌هایی را مشخص کنید که کاربران با کلیک بر روی

www.takbook.com

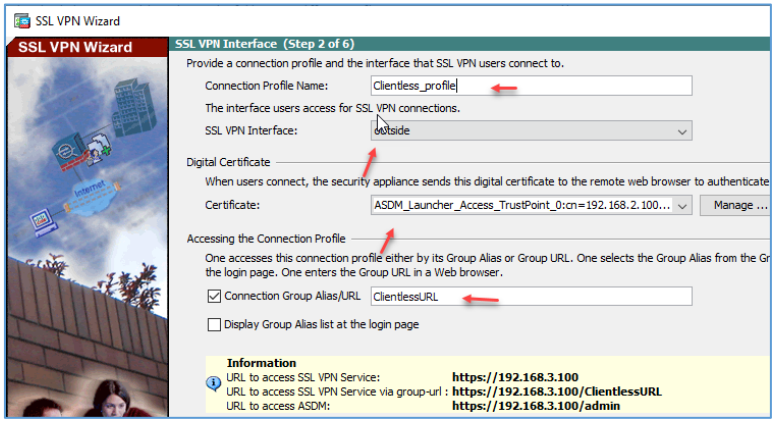
آن صفحه آن سایت را مشاهده کنند و یا اینکه برای File sharing از آن استفاده کنید، البته امنیت این روش از AnyConnect کمتر است.

همان سناریوی قبلی را که بین سه دستگاه PC1، ASA1 و Server بود را در نظر بگیرید، وارد نرم‌افزار ASDM شوید و از منوی Wizards و از قسمت VPN Wizards گزینه‌ی Clientless SSl VPN را انتخاب کنید.



شکل ۹۶-۱۳ *Clientless SSL VPN*

در شکل ۹۷-۱۳، یک نام برای این Profile وارد کنید و Interface که باید بر روی آن سرویس ارائه شود را outside در نظر بگیرید، certificate که در قسمت Anyconnect ایجاد کردیم را انتخاب و در آخر تیک گزینه‌ی مورد نظر را انتخاب و یک نام برای گروه خود وارد کنید، اگر به شکل ۹۷-۱۳، توجه کنید، آدرس‌هایی که برای دسترسی به فایروال نیاز است مشخص شده است، بر روی Next کلیک کنید.

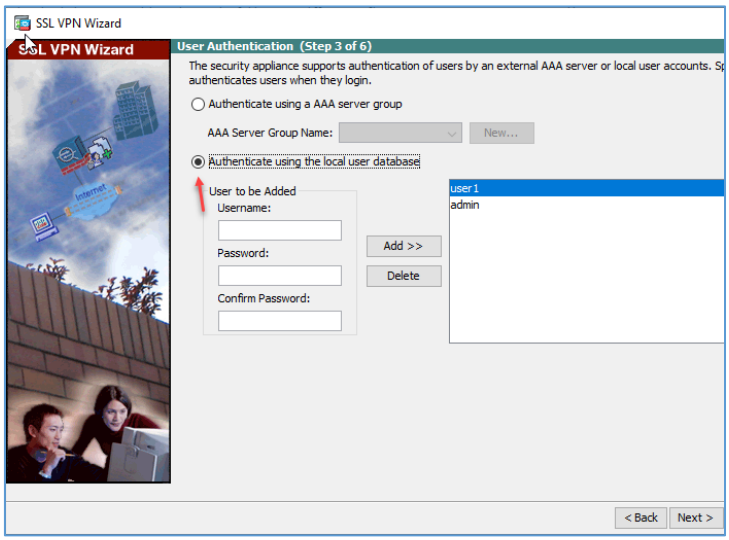


شکل ۹۷-۱۳ *Clientless SSL VPN*

در شکل ۹۸-۱۳، باید مشخص کنید که احراز هویت به چه شکلی مشخص شود، گزینه‌ی اول برای حالتی است که از سرور AAA در شبکه خود استفاده می‌کنید و گزینه‌ی دوم زمانی است که این سرورها

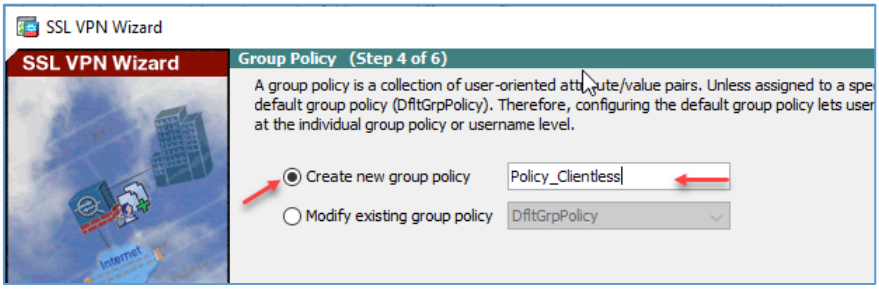
www.takbook.com

را در دسترس ندارید و می‌خواهید از رمز محلی (Local) مربوط به خود فایروال استفاده کنید، البته می‌توانید خودتان کاربران مورد نظر خود را اضافه کنید، ولی سعی کنید در شبکه واقعی یک سرور ACS راه‌اندازی کنید و Active Directory خود را به آن متصل کنید تا کاربران بتوانند با نام کاربری و رمز خودشان وارد فایروال شوند.



شکل ۹۸-۱۳ *Clientless SSL VPN*

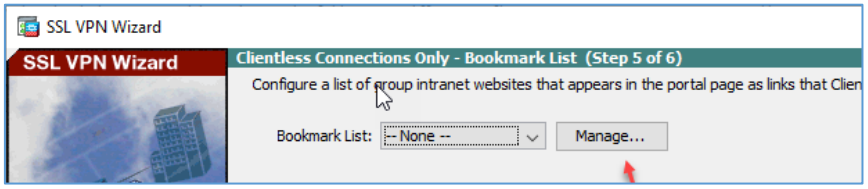
در شکل ۹۹-۱۳، یک Policy جدید ایجاد کنید تا تنظیمات مشخص را بر روی آن اعمال کنیم، نام مورد نظر خود را وارد کنید.



شکل ۹۹-۱۳ *Clientless SSL VPN*

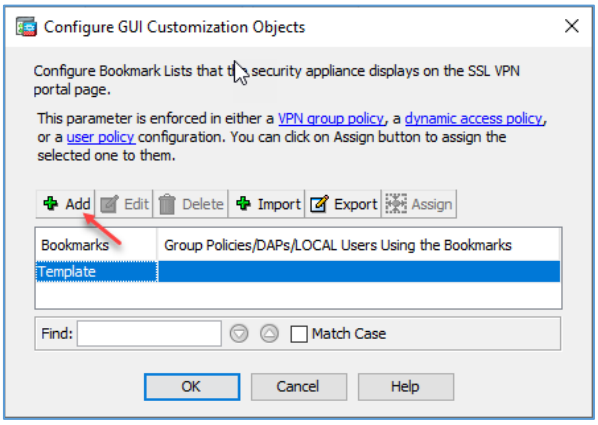
در شکل ۱۰۰-۱۳، باید یک لیست Bokmark از آدرس‌های سرورهای داخلی ایجاد کنید، برای اینکه کاربران زمانی که سایت را باز می‌کنند بتوانند به راحتی به این آدرس‌ها دسترسی داشته باشند.

www.takbook.com



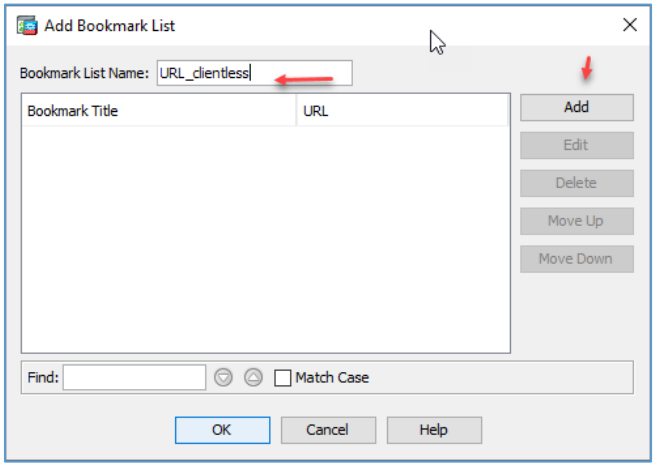
شکل ۱۳-۱۰۰ *Clientless SSL VPN*

در شکل ۱۳-۱۰۱، باید بر روی Add کلیک کنید و Bookmark خود را ایجاد کنید.



شکل ۱۳-۱۰۱ *Clientless SSL VPN*

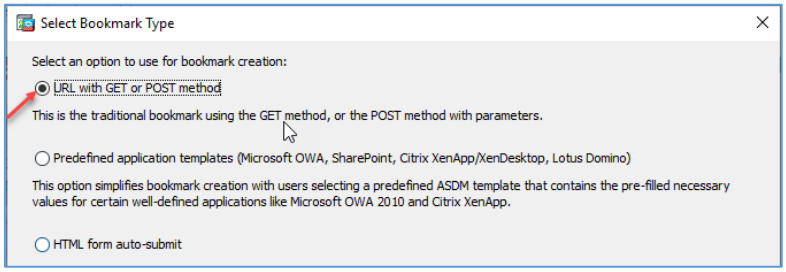
در شکل ۱۳-۱۰۲، باید در این قسمت نام Bookmark خود را وارد و بر روی Add کلیک کنید.



شکل ۱۳-۱۰۲ *Clientless SSL VPN*

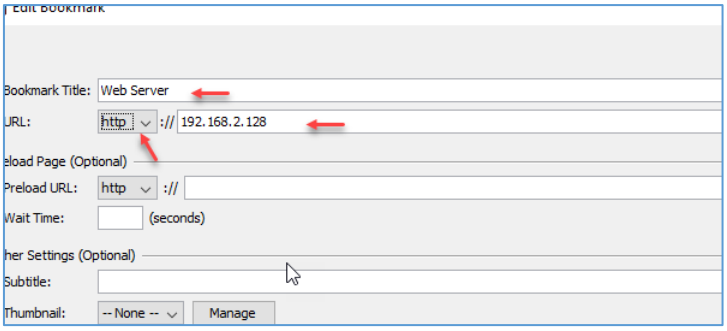
در شکل ۱۳-۱۰۳، گزینه‌ی اول را انتخاب و بر روی OK کلیک کنید.

www.takbook.com



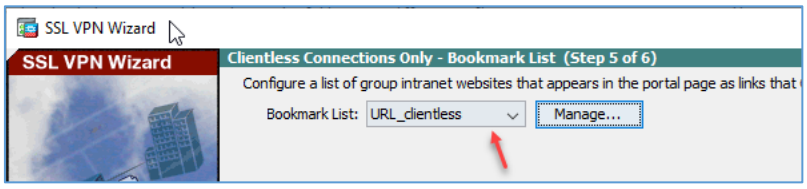
شکل ۱۳-۱۰۳ Clientless SSL VPN

در شکل ۱۳-۱۰۴، باید یک نام برای آدرس خود در نظر بگیرید و در قسمت URL باید پروتکل و آدرس آن را مشخص کنید که در اینجا پروتکل http برای باز کردن وب سایت 192.168. 2.128 انتخاب شده است، بعد از این کار بر روی OK کلیک کنید تا آدرس به لیست اضافه شود.



شکل ۱۳-۱۰۴ Clientless SSL VPN

به مانند شکل ۱۳-۱۰۵، بعد از ایجاد، Bookmark را انتخاب کنید و بر روی Next کلیک کنید در صفحه بعد هم بر روی Finish کلیک کنید تا عملیات انجام شود.



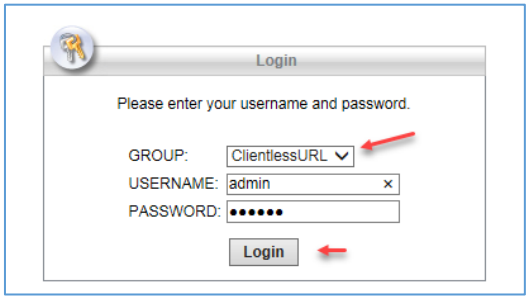
شکل ۱۳-۱۰۵ Clientless SSL VPN

برای تست کار، وارد PC1 شوید و از طریق مرورگر آدرس زیر را اجرا کنید.

https://192.168.2.128

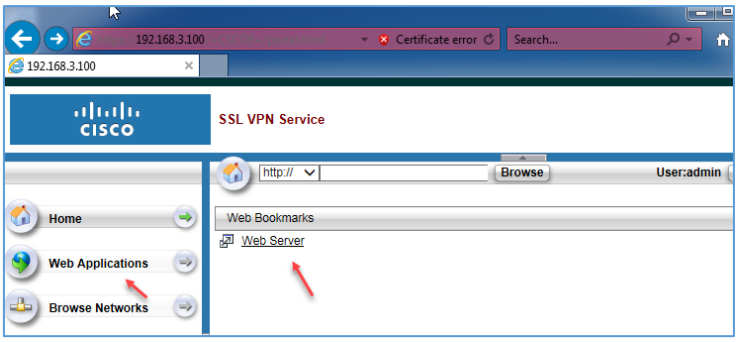
با این کار شکل ۱۳-۱۰۶، ظاهر می‌شود و می‌توانید با نام کاربری و رمز عبور و انتخاب پروفایل مورد نظر وارد سایت شوید.

www.takbook.com



شکل ۱۳-۱۰۶ Clientless SSL VPN

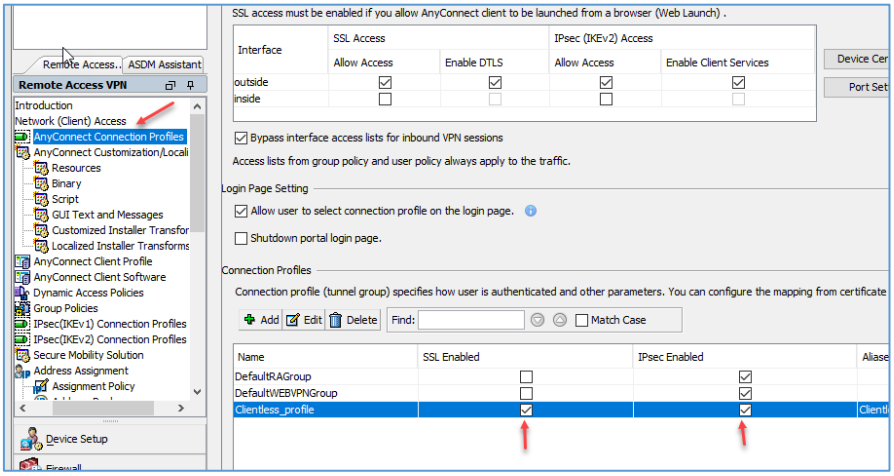
همانطور که در شکل ۱۳-۱۰۷، مشاهده می‌کنید، سایت باز شده است و Bookmark مورد نظر را مشاهده می‌کنید با کلیک بر روی آن می‌توانید سایت مورد نظر را باز کنید، توجه داشته باشید در قسمت بالای آن می‌توانید آدرس دلخواه خود را وارد کنید.



شکل ۱۳-۱۰۷ Clientless SSL VPN

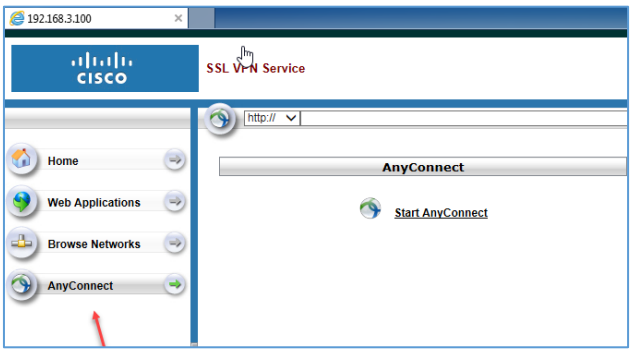
به مانند شکل ۱۳-۱۰۸، اگر هم بخواهید Anyconnect VPN را در لیست سایت فایروال مشاهده کنید باید وارد Remote Access VPN شوید و بر روی AnyConnect Connection Profiles کلیک کنید و از لیست همان Profile مورد نظر که ایجاد کرده بودید را به مانند شکل زیر فعال کنید.

www.takbook.com



شکل ۱۳-۱۰۸ *Clientless SSL VPN*

اگر دوباره وارد سایت شوید گزینه‌ی AnyConnect را هم مشاهده می‌کنید.



شکل ۱۳-۱۰۹ *Clientless SSL VPN*

۱۳-۱ قسمت اول – معماری LAN

تا به اینجا با نحوه‌ی کارکرد سوئیچ‌ها آشنا شده‌اید و یاد گرفته‌اید که چگونه الگوریتم‌های STP و RSTP عمل می‌کنند و همچنین یاد گرفتید که چگونه یک سوئیچ را ازحملات مهاجمان امن نگه داریم.

www.takbook.com

در این بخش می‌خواهیم در مورد طراحی و معماری یک سوئیچ در شبکه صحبت کنیم یعنی می‌خواهیم بدانیم که سوئیچ‌ها در یک شبکه چگونه به هم متصل می‌شوند و نحوه‌ی عملکرد آنها به چه صورت خواهد بود و همچنین چرا یک توپولوژی را به توپولوژی دیگر ترجیح می‌دهیم؟
در این قسمت سه چیز مورد بررسی قرار خواهد گرفت:

۱- در مورد توپولوژی شبکه‌ی Ethernet سیمی و اصطلاحاتی که در لایه‌ی دوم و سوم به کار می‌رود می‌پردازید.
۲- در مورد شبکه‌های SOHO یا همان کوچک / اداری صحبت خواهیم کرد .
۳- و در آخر در مورد سوئیچ‌های POE یا همان Power over Ethernet بحث خواهیم کرد.

۱-۱-۱۳ تجزیه و تحلیل توپولوژی شبکه‌ی LAN دانشگاه

اصطلاح LAN campus یا LAN به پشتیبانی از دستگاه‌های داخل یک ساختمان یا چند ساختمان در مجاورت هم گفته می‌شود.

قبل از اینکه به ادامه موضوعات بپردازیم بهتر است انواع سوئیچ‌ها را بررسی کنیم:

۱- سوئیچ Core

به سوئیچ‌هایی گفته می‌شود که در هسته‌ی مرکزی یک شبکه قرار دارد و از قدرت خوبی در انجام عملیات برخوردار است.

۲- سوئیچ Distribution

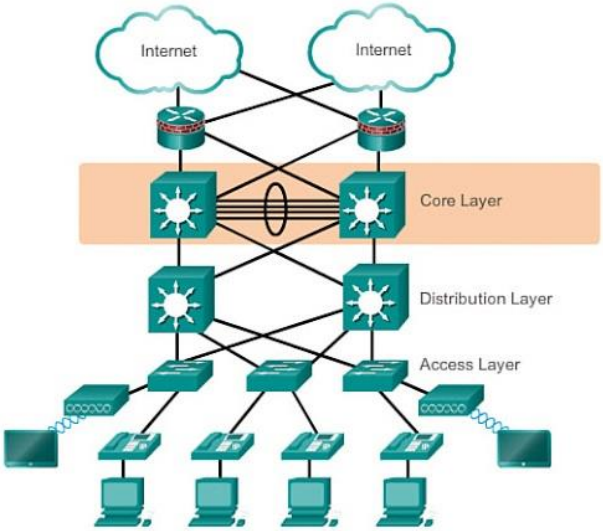
یک سوئیچ رده‌ی میانی است و اصولاً بین سوئیچ Core و سوئیچ Access قرار می‌گیرد و از سرعت خوبی برخورار است.

۳- سوئیچ Access

این نوع سوئیچ برای اتصال به دستگاه‌های شبکه مورد استفاده قرار می‌گیرد و دارای سرعت گیگابایت هستند و از چندین عدد پورت برای پشتیبانی از دستگاه‌های شبکه استفاده می‌کنند.

درشکل ۱-۱۳، نمای کلی سوئیچ‌ها را مشاهده می‌کنید.

www.takbook.com

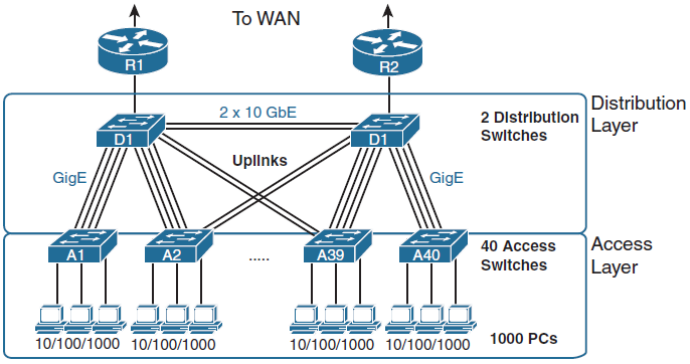


شکل ۱-۱۳ تنظیمات GNS3

برای ادامه کار در زیر با چند اصطلاح در مورد طراحی توپولوژی LAN دانشگاهی آشنا خواهید شد:

۲-۱-۱۳ شبکه‌ی دانشگاهی دو لایه

در شکل ۲-۱۳، یک طراحی از یک شبکه‌ی بزرگ LAN دانشگاهی را مشاهده می‌کنید که در لایه‌ی اول 1000 دستگاه نهایی به 40 سوئیچ متصل شده‌اند که هر سوئیچ دارای ۲۵ پورت است و در لایه‌ی دوم آن سوئیچ‌های Access به سوئیچ‌های Distribution متصل شده‌اند، این نوع سوئیچ‌ها مسیری را به سوئیچ‌های Access نشان می‌دهند تا بتوانند به شبکه دیگر دسترسی داشته باشند، به نحوه‌ی چینش کابل‌ها هم دقت کنید.



شکل ۲-۱۳ شبکه‌ی دو لایه

www.takbook.com

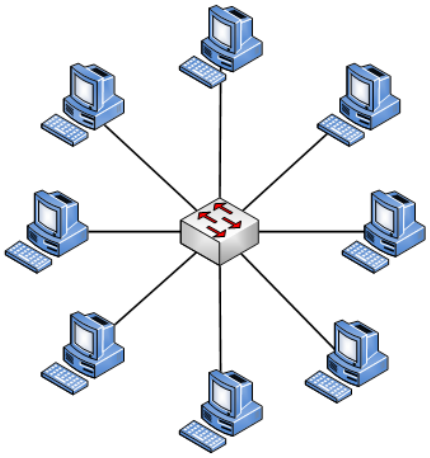
به این موضوع توجه کنید که اصطلاح two-tier و 2-tier یکی در مباحث سیسکو یکی هستند.

انواع اصطلاحات توپولوژی در طراحی Two-Tier

در دنیای شبکه از چندین اصطلاح برای شبکه‌های LAN، WAN استفاده می‌شود که در زیر آنها را بررسی می‌کنیم:

توپولوژی Star (ستاره‌ای)

در این نوع از شبکه، کامپیوترها و یا ادوات دیگر شبکه به‌وسیله‌ی یک دستگاه مرکزی مانند Hub یا Switch به همدیگر متصل می‌شوند که امروزه هم در اکثر جاها از این شبکه استفاده می‌کنند.



شکل ۳-۱۳ شبکه‌ی Star

مزایا

۱- سادگی دسترسی به شبکه.

۲- با ایجاد مشکل در یک کامپیوتر، آن کامپیوتر از مسیر خارج می‌شود و بقیه‌ی شبکه به کار خود ادامه می‌دهد.

۳- می‌تواند در آینده برای شبکه‌های جدیدتر توسعه پیدا کند.

معایب:

۱- درصورتی‌که نقطه‌ی مرکزی شبکه، یعنی Hub یا Switch از کار بیفتد کل شبکه مختل می‌شود.

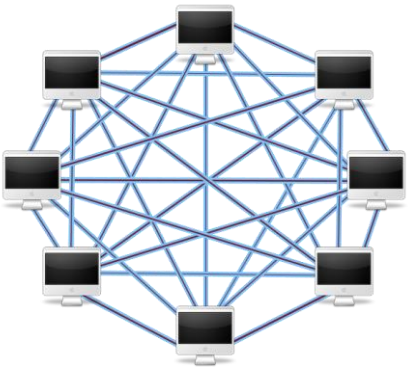
۲- اندازه‌ی کابل به علت دستیابی مستقیم هر کامپیوتر به آن بسیار زیاد است و هزینه را افزایش می‌دهد.

www.takbook.com

توپولوژی mesh (تو در تو)

در این توپولوژی هر گره به‌طور مستقیم، بدون هیچ واسطه‌ای با کلیه‌ی گره‌های دیگر در ارتباط است؛ بنابراین با فرض N گره در توپولوژی، هر گره باید دارای N-1 پورت باشد. اگر یک گره به کلیه‌ی گره‌ها متصل باشد به آن Full Mesh هم می‌گویند و بیشتر در مکان‌های نظامی کاربرد دارد.

Partial mesh هم به مانند Full Mesh است با این تفاوت که ارتباط هر دستگاه با هر دستگاه دیگر در شبکه وجود دارد اما حتماً مستقیم نیست.



شکل ۴-۱۳ شبکه‌ی Mesh

مزایا:

۱- سرعت بسیار بالا.

۲- امنیت بالا.

۳- اگر مشکلی در یک لینک ایجاد شود، تأثیری بر روی شبکه نخواهد داشت.

۴- سادگی در عیب‌یابی.

معایب:

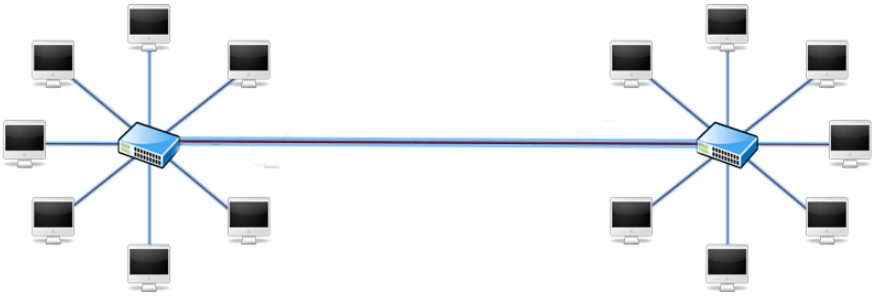
۱- هزینه‌ی بالا به علت استفاده‌ی زیاد از کابل.

۲- هر گره برای اتصال به شبکه، نیاز به چندین interface دارد.

توپولوژی Hybrid (دو رگه)

این شبکه به این علت به نام Hybrid است که در ساختار خود از دو شبکه‌ی Bus و Star استفاده می‌کند.

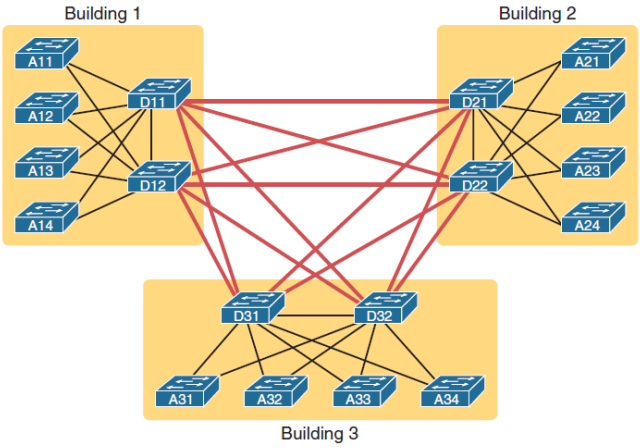
www.takbook.com



شکل ۵-۱۳ شبکه‌ی Hybrid

۳-۱-۱۳ طراحی شبکه‌ی سه لایه‌ی (Three-Tier) دانشگاهی

در طراحی شبکه‌ی دولایه‌ی دانشگاهی همانطور که گفتیم سوئیچ‌های Access به سوئیچهای Distribution متصل شده و بعد از آن به مانند شکل ۶-۱۳، سوئیچ‌های Distribution به صورت Mesh به هم متصل می‌شوند.

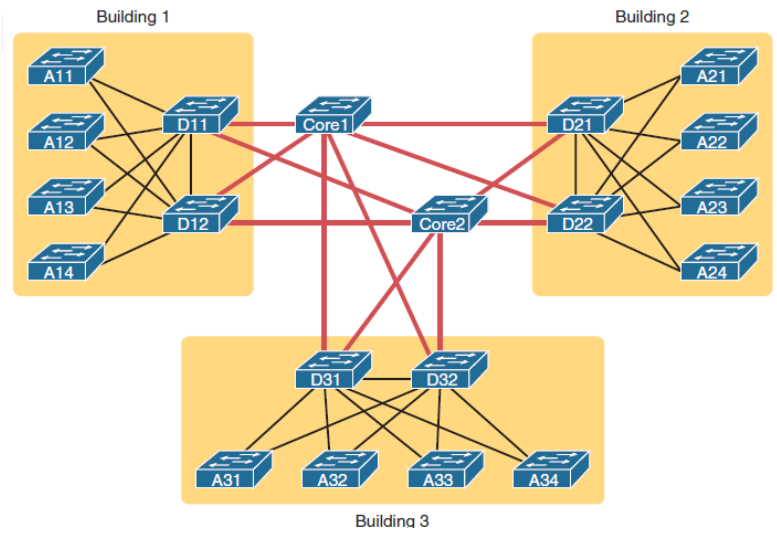


شکل ۶-۱۳ شبکه‌ی دو لایه‌ی دانشگاهی

اما در شبکه‌های امروزی از شبکه‌های سه لایه که در زیر مشاهده می‌کنید استفاده می‌کنند، بسیاری از شرکت‌ها از این روش برای پیاده‌سازی شبکه‌ی خود استفاده می‌کنند و بهترین عملکرد را هم از آن گرفتند، در زیر شبکه‌ی سه لایه را مشاهده می‌کنید که دارای سوئیچ Core هم است که به ساختمان‌های مختلف متصل شده اند.

اصولاً کابل‌کشی در این نوع شبکه‌ها گران‌قیمت خواهد بود و اگر هم بخواهید از کابل‌های فیبر نوری استفاده کنند باید هزینه‌ی بیشتری بپردازند که البته کیفیت کار بسیار بسیار افزایش پیدا خواهد کرد، هر چند که تو کشور ما ایران این چنین هزینه‌هایی انجام نخواهد شد.

www.takbook.com



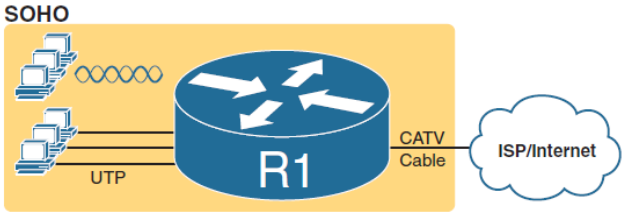
شکل ۷-۱۳ شبکه‌ی سه لایه‌ی دانشگاهی

۴-۱-۱۳ شبکه‌های Small Office/Home Office

بعد از اینکه در مورد طراحی شبکه‌های LAN در محیط دانشگاهی اصطلاحاتی را آموختید حالا در این بخش می‌خواهیم شبکه‌های کوچکتر از نوع LAN را با هم بررسی کنیم.

شبکه‌ی SOHO به طرح‌ها و پیاده‌سازی‌هایی اطلاق می‌شوند که دارای حجم کمی از دستگاه‌ها هستند، مثلاً شامل چند سوئیچ، چند AP، چند روتر و کلاینت هستند.

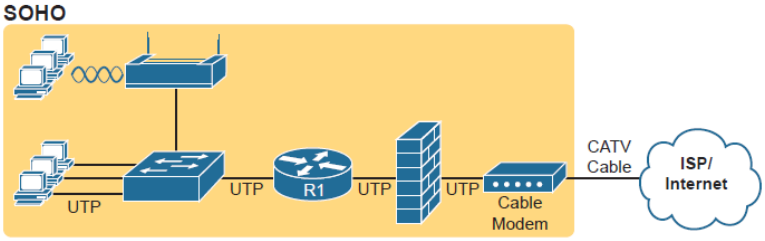
اصولاً کاربران در این نوع شبکه‌های درخانه یا دفتر کار خود با تعداد کمی از این نوع دستگاه‌ها کار می‌کنند، در زیر یک شکل کلی از یک شبکه‌ی کوچک را مشاهده می‌کنید که سیستم‌های نهایی مانند لپ‌تاپ، موبایل و... از طریق کابل و یا از طریق بی‌سیم به روتر متصل می‌شوند و از خدمات آن استفاده می‌کنند، و روتر هم از طریق کابل CATV به شرکت ارائه دهنده‌ی اینترنت متصل می‌شود.



شکل ۸-۱۳ شبکه‌ی Small Office/Home Office

www.takbook.com

همانطور که گفتیم روتر در شبکه‌های SOHO بسیار نقش اساسی دارد و برای اینکه دقیق‌تر ببینیم روتر چه کارهایی انجام می‌دهد می‌توانیم به مانند شکل ۹-۱۳، اجزای آن را مشاهده کنیم:
در این شکل یک روتر را برای شما باز کردیم که دارای سوئیچ، روتر، دیواره‌ی آتش و کابل مودم است.



شکل ۹-۱۳ شبکه‌ی Small Office/Home Office

توجه داشته باشید برای مدیریت AP نیاز به WLC نیست و مدیریت آن توسط کلاینت‌های متصل شده به آن انجام خواهد شد.

۵-۱-۱۳ بررسی Power over Ethernet (PoE)

در یک ساختمان مهندسین برق برای هر دستگاه برقی یک پریز برق و برای لامپ‌ها هم کابل برق مجزا قرار می‌دهند و وسایل برقی با استفاده از آنها روشن می‌شوند.

اما مهندسین شبکه برای اینکه به دستگاه‌های خود برق برسانند یک راه حل بهتری را پیاده‌سازی کردند با عنوان Power over Ethernet (PoE)، زمانی که برخی از دستگاه‌های شبکه را خریداری می‌کنید روی آنها نوشته POE که نشان دهنده‌ی پشتیبانی از این جریان برق در شبکه هستند.
در این تکنولوژی به جای استفاده از سیم‌های جدای برق، فقط از همان کابل شبکه برای برق‌رسانی استفاده خواهد شد و این یعنی صرفه‌جویی در وقت و هزینه.

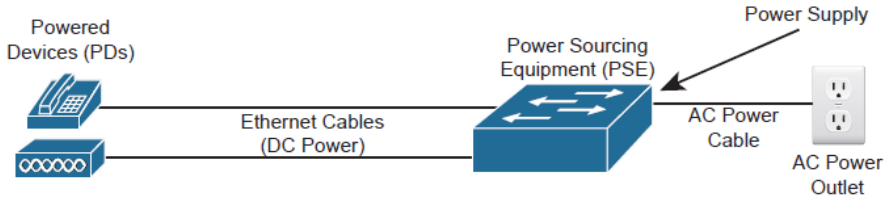
PoE Basics

خانواده استانداردهای تامین کننده‌ی انرژی با نام عمومی Power over Ethernet یا POE شناخته می‌شوند، مثلاً سوئیچ‌هایی برای این موضوع طراحی شده‌اند که پورت آنها قابلیت POE یا برق‌رسانی به دستگاه‌ها را دارد به این نوع دستگاه‌ها PSE یا Power Sourcing Equipment هم گفته می‌شود.

به دستگاه‌هایی که دارای قابلیت POE هستند و از برق دستگاه POE دیگر استفاده می‌کنند PD یا Powered Device گفته می‌شود مانند دوربین‌های مداربسته که POE را پشتیبانی می‌کنند.

www.takbook.com

در شکل ۱۰-۱۳، دو دستگاه که PD هستند را مشاهده می‌کنید که به یک سوئیچ با پشتیبانی از POE متصل شده‌اند.



شکل ۱۰-۱۳ PoE Basics

برای استفاده از دستگاه‌های POE باید یک سری شرایط را مورد بررسی قرار دهید:

۱- از پورت POE زمانی استفاده کنید که مطمئن باشید دستگاه مورد نظر یک PD است و این پورت و برق را پشتیبانی می‌کند.

۲- با استفاده از روش‌های Ethernet autonegotiation و با ارسال سیگنال کم مصرف و نظارت بر سیگنال می‌توان کلاس POE را مشخص کنید و طبق آن می‌توانید مشخص کنید که توان دستگاه چقدر باشد.

۳- دستگاه‌هایی که PD هستند باید کلاس برق آن را مشخص کنید.

۴- مانیتور کردن کلاس پاورها با انجام تست خودکار صدا و هم گوش دادن به پیام‌های CDP و LLDP از دستگاه‌های PD.

در شکل ۱۱-۱۳، سوئیچ سیسکو POE مدل SG350-10P را مشاهده می‌کنید که دارای ۱۰ پورت POE با سرعت گیگابایت است.

شکل ۱۱-۱۳ سوئیچ سیسکو مدل SG350

www.takbook.com

۱۳-۳ معماری Cloud

وقتی به یک سرور فکر می‌کنید چه چیزی به ذهن شما می‌رسد؟ یک سرور با تعداد زیادی رم و چند CPU پرقدرت که بر روی زمین و یا بر روی رک قرار دارند، اما اگر به سیستم‌عامل فکر کنید می‌توانید تصور کنید که بر روی یک ماشین مجازی قرار دارد و در حال اجرا است؟

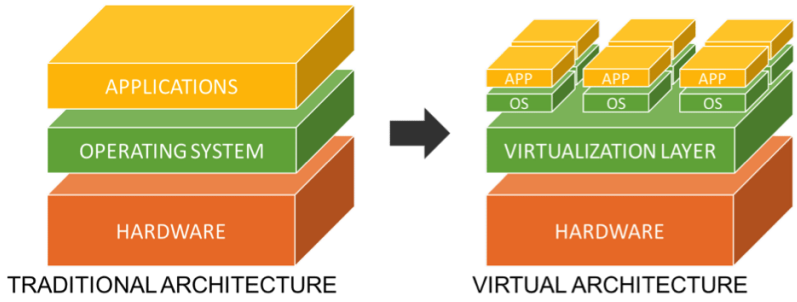
در این قسمت می‌خواهیم در مورد مجازی‌سازی و راه‌های کم کردن هزینه‌ها برای استفاده از از سخت‌افزارهای گران قیمت صحبت کنیم.

۱۳-۳-۱ مجازی سازی (Virtualization)

اصولاً مجازی‌سازی برای ایجاد یک نمونه مجازی یا غیر واقعی از یک سیستم سخت‌افزاری به کار گرفته می‌شود که این موضوع باعث پیشرفت در کار و جلوگیری از اتلاف هزینه خواهد شد، در کل مجازی‌سازی برای یک سازمان و مدیر شبکه آن بسیار بسیار ضروری خواهد بود. در زیر ویژگی‌های مجازی‌سازی را مشاهده می‌کنید:

۱- کاهش هزینه خرید تجهیزات سخت‌افزاری.
۲- متمرکزسازی سرورها در یک مکان.
۳- کاهش هزینه‌های جاری نظیر برق، نگهداری، تعمیرات.
۴- کاهش گرمای تولیدی توسط دستگاه‌ها که به علت مجازی‌سازی به جای استفاده از چند سرور واقعی از یک سرور استفاده می‌شود.
۵- عدم نیاز به فضای زیاد به نسبت حالت اولیه که چندین سرور در یک فضا قرار می‌گرفت.
۶- استفاده از بیشترین ظرفیت تجهیزات سخت‌افزاری.
۷- جابجایی راحت با استفاده از نرم‌افزارهایی که در ادامه مورد بررسی قرار می‌دهیم.
۸- پشتیبان‌گیری راحت از اطلاعات توسط vCenter و نرم‌افزار Veeam.
۹- تسریع امور به خاطر وجود بالقوه دستگاه‌ها و عدم نیاز به صرف زمان برای خرید، نصب و آماده‌سازی.
۱۰- امکان تنظیم و نصب سرورها و تجهیزات مجازی با استفاده از الگو و کپی‌برداری.

www.takbook.com

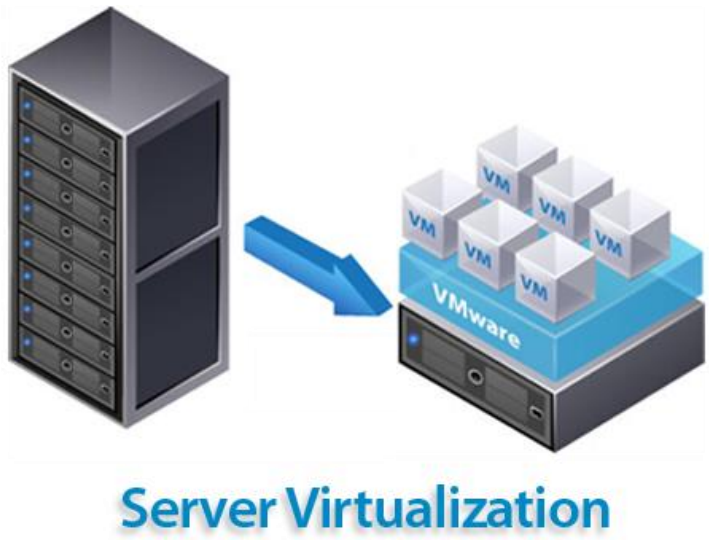


شکل ۱۳-۱۱۰ *Virtualization*

۱۳-۳-۲ انواع مجازی‌سازی‌ها در شبکه

اگر فکر می‌کنید که مجازی‌سازی فقط و فقط برای ماشین مجازی است سخت در اشتباه هستید، بلکه در نوع‌های دیگری هم استفاده می‌شود که در زیر لیست آنها را مشاهده می کنید.

۱۳-۳-۲-۱ مجازی سازی سرور (Server Virtualization)

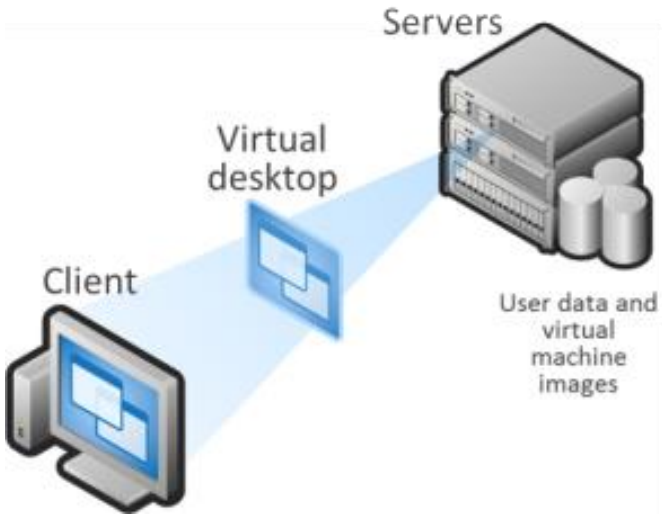


شکل ۱۳-۱۱۱ *Server Virtualization*

به جای خرید چندین سرور فقط یک سرور قدرتمند خریداری می‌شود و سیستم‌عامل‌های مجازی‌سازی یا در اصطلاح hypervisor بر روی آنها نصب می‌شود و بسته به قدرت سخت‌افزاری سرور مورد نظر، می‌توانید چندین سرور مجازی را بر روی آن ایجاد و برای کارهای گوناگون استفاده کنید، با انجام این کار هزینه‌ها کاهش می‌یابد، امنیت اطلاعات افزایش پیدا می‌کند، هزینه‌ی پشتیبانی از سرورها کاهش پیدا می‌کند و چندین کار مهم دیگر که با مجازی‌سازی انجام می‌شود.

www.takbook.com

۲-۲-۳-۱۳ مجازی‌سازی دسکتاپ (Desktop Virtualization)

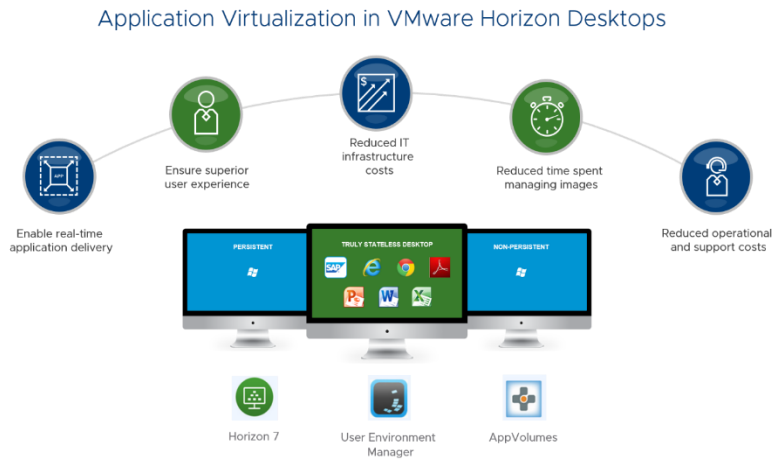


شکل ۱۳-۱۱۲ Desktop Virtualization

هر کاربر دارای یک سیستم Thin client است و این سیستم کوچک و کم هزینه از طریق کارت شبکه و آدرس IP به سرور مجازی و ماشینی که برای این کاربر ایجاد شده متصل می‌شود و به این ترتیب بدون آنکه کاربر متوجه شود وارد سیستم‌عامل خود می‌شود و با آن کار می‌کند، یک ویژگی مهم این کار این است که همه‌ی اطلاعات کاربر بر روی سرور قرار دارد و از این طریق مدیر می‌تواند به راحتی این اطلاعات را کنترل و از آنها پشتبان تهیه کند، با انجام این روش هزینه‌های سخت‌افزاری و انسانی سازمان به شدت کاهش پیدا خواهد کرد.

www.takbook.com

۳-۲-۳-۱۳ مجازی‌سازی نرم‌افزار (Application Virtualization)



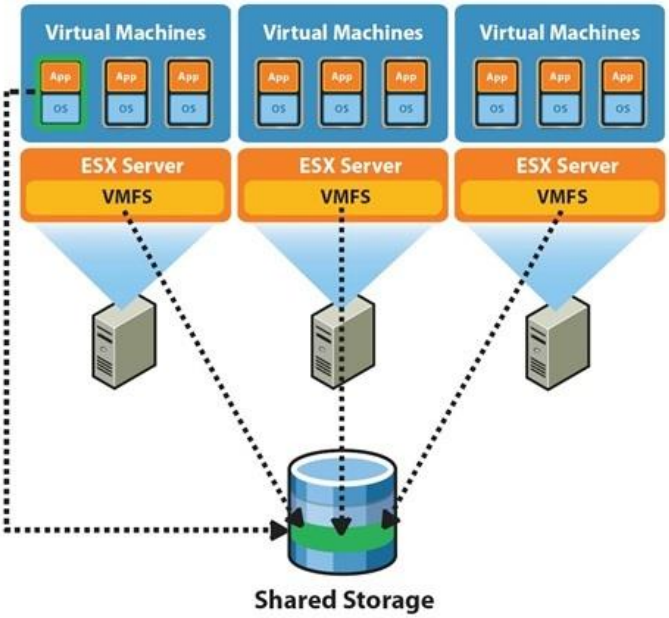
شکل ۱۳-۱۱۳ Application Virtualization

در این مدل از مجازی‌سازی‌ها، بر روی یک یا چند سرور نرم‌افزاری مورد استفاده کاربران مانند نرم‌افزارهای مالی نصب می‌شود و به صورت مجازی با کاربران به اشتراک گذاشته می‌شود، برای اجرای این نرم‌افزارها یک نرم‌افزار Agent که مربوط به همان نرم‌افزار مجازی‌سازی است بر روی سیستم کاربر نصب می‌شود و بعد از آن کاربر با آدرس مشخص شده و از طریق وب می‌تواند به نرم‌افزارهای به اشتراک گذاشته شده دست پیدا کند، از مزایای آن می‌توان به پشتیانی دقیق از نرم‌افزار، متمرکز شدن آن، اجرای نرم‌افزار در هر سیستم با سخت‌افزار پائین و دیگر ویژگی‌هایی که انشاالله در درس‌های آینده به آن می‌رسیم.

۴-۲-۳-۱۳ مجازی‌سازی ذخیره‌سازها (Storage Virtualization)

در این قسمت می‌توانید یک هارد دیسک فیزیکی را به چندین دیسک مجازی تقسیم کنید و بر روی آن اطلاعات قرار دهید، با استفاده از این سرویس به صورت کاملاً بهبود یافته می‌توانید از اطلاعات خود استفاده کنید، پشتیبان تهیه کنید و حتی می‌توانید در SAN هم این نوع مجازی‌سازی را پیاده‌سازی کنید.

www.takbook.com

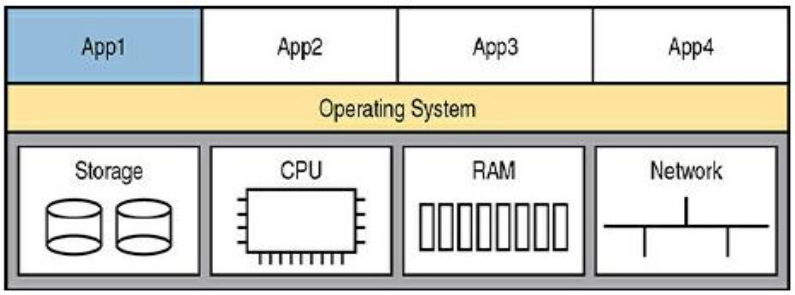


شکل ۱۱۴-۱۳ *Storage Virtualization*

۵-۲-۳-۱۳ مجازی‌سازی شبکه (Network Virtualization)

به صورت خلاصه مجازی‌سازی شبکه را می‌توان به عنوان تکنیک‌هایی برای جداسازی منابع شبکه و محاسباتی، برای واگذاری آن‌ها به یک شبکه مجازی (منطقی)، برای همساز کردن چندین شبکه مجازی قابل برنامه‌ریزی و مستقل، دانست.

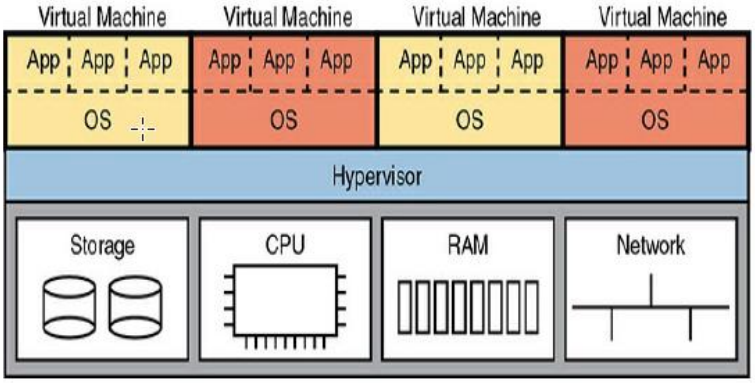
به صورت معمول فکر می‌کنید که یک سرور دارای یک سیستم‌عامل است که از کل منابع آن سرور استفاده می‌کند و بر روی آن نرم‌افزارهای مختلفی نصب شده است



شکل ۱۱۵-۱۳ *Virtualization*

www.takbook.com

اما در بحث مجازی‌سازی، این چنین نیست و به مانند شکل ۱۱۶-۱۳، یک سیستم عامل مجازی‌سازی که اصولاً به آنها Hypervisor می‌گویند بر روی سرور نصب می‌شود و بعد از آن می‌شود بر روی آن چندین ماشین محازی با سیستم عامل‌های مختلف نصب کرد و کارهای مختلفی را بر روی آن انحام داد.



شکل ۱۱۶-۱۳ *Hypervisor*

در زیر چند سیستم‌عامل مجازی‌سازی را مشاهده می‌کنید:

- VMware ESXi
- Microsoft HyperV
- Citrix XenServer
- Red Hat KVM

۶-۲-۳-۱۳ سوئیچ‌های مجازی

یک سرور را در نظر بگیرید که دارای چند پورت است که می‌تواند سیستم‌عامل مورد نظر شما را به شبکه متصل کند، اما اگر بخواهیم سیستم‌عامل مجازی بر روی سرور نصب کنید باید برای ارتباط ماشین‌های مجازی که بر روی آن نصب می‌شوند با شبکه‌ی واقعی یک سوئیچ مجازی راه‌اندازی کنیم، در این بخش قصد نداریم که در مورد مجازی‌سازی شبکه در Hypervisior صحبت کنیم بلکه می‌خواهیم یک دید کلی از آنها بدست آوریم.

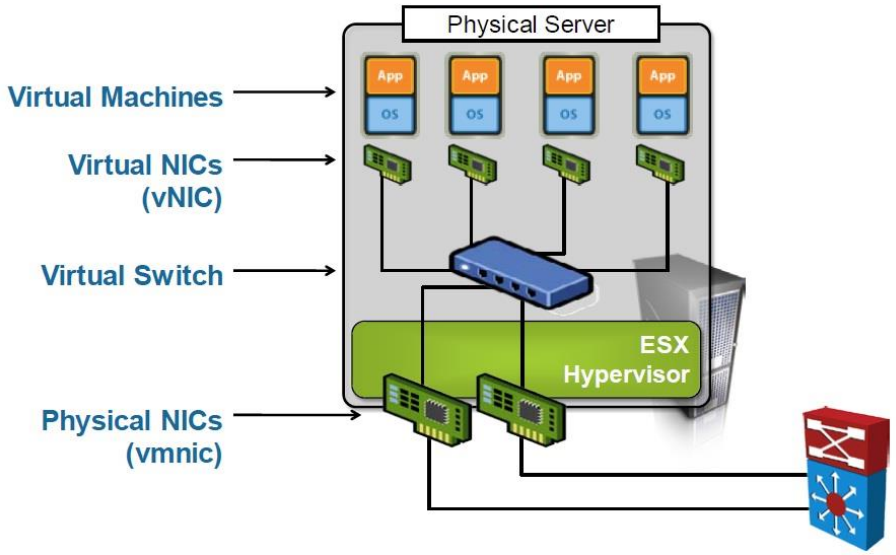
به سوئیچ‌های مجازی به اصطلاح vSwitch یا همان Virtual Switch گفته می‌شود، که به صورت نرم‌افزاری راه‌اندازی می‌شوند و می‌توانند با سوئیچ فیزیکی یا همان پورت فیزیکی سرور ارتباز برقرار کنند.

یکی از محبوب‌ترین Hyprvisior در دنیای مجازی‌سازی VMware ESXi است که در دنیای مجازی‌سازی حرف اول را می‌زند.

در شکل ۱۱۷-۱۳، یک Hypervisor از نوع ESXi را مشاهده می‌کنید که دارای دو کارت شبکه‌ی فیزیکی است که این دو کارت شبکه به یک سوئیچ مجازی Virtual Switch متصل شده‌اند، بعد از آن 4 تا Virtual

www.takbook.com

Nics که کارت شبکه‌ی مجازی داخلی است ایجاد شده است و در آخر به ماشین‌های مجازی تخصیص داده شده است، این یک شکل کلی از سوئیچ مجازی در VMware است.



شکل ۱۱۷-۱۳ ESXi Hypervisor

شرکت سیسکو هم برای اینکه از دنیای مجازی‌سازی عقب نماد یک سری از محصولات خود را به صورت محازی عرضه کرده است مانند همان ASA که در قسمت‌های قبل بررسی کردیم، یا سوئیچ‌های سری Nexus که به صورت مجازی بر روی یک Hyprvisor راه‌اندازی می‌شوند و از آن می‌توانید به عنوان یک سوئیچ واقعی در شبکه استفاده کنید.

سوئیچ‌های مجازی Nexus 1000VE می‌تواند بهترین عملگرد را برای شما به ارمغان بیاورد.

www.takbook.com

۴-۱۳سوالات فصل سیزدهم

1. In a two-tier campus LAN design, which of the following are typically true of the topology design? (Choose two answers.)

در یک طراحی LAN در یک دانشگاه دو طبقه ، کدام یک از موارد زیر به طور معمول در مورد طراحی توپولوژی درست است؟ (دو گزینه را انتخاب کنید.)

a. The design uses a full mesh of links between access and distribution switches.

b. The design uses a partial mesh of links between access and distribution switches.
c. The design uses a partial mesh of links between the distribution and core switches.
d. The end-user and server devices connect directly to access layer switches.

2. In a three-tier campus LAN design, which of the following are typically true of the topology design?(Choose two answers.)

در یک طراحی LAN دانشگاه سه طبقه ، کدام یک از موارد زیر به طور معمول در مورد طراحی توپولوژی درست است؟ (دو گزینه را انتخاب کنید.)

a. The design uses a partial mesh of links between access and distribution switches.
b. The design uses a full mesh of links between access and distribution switches.
c. The design uses a partial mesh of links between the distribution and core switches.
d. The end-user and server devices connect directly to distribution layer switches.

3. Which one answer gives the strongest match between one part of a typical three-tier design with the idea behind the listed generic topology design term?

کدام یک از پاسخ‌های زیر نشان دهنده‌ی یک طراحی سه لایه توپولوژی قوی است؟

a. The access layer looks like a partial mesh.
b. The distribution layer looks like a full mesh.
c. The distribution layer looks like a hybrid design.
d. The access layer looks like a star design.

4. Which answers list criteria typical of a SOHO network? (Choose two answers.)

کدام یک از معیارهای زیر معمولاً مربوط به شبکه‌ی SOHO است؟ (دو گزینه را انتخاب کنید)

a. The AP functions using standalone mode.
b. The AP functions using a split-MAC architecture using a WLC.
c. A single networking device implements the router, switch, AP, and firewall functions.
d. A separate networking device implements each function (router, switch, AP, and firewall).

5. Which answer describes how a LAN switch dynamically chooses the initial power level to apply to a UTP cable with PoE?

کدام پاسخ توصیف می‌کند که یک سوئیچ سطح قدرت را در یک کابل UTP و با استفاده از POE پیدا می‌کند؟

1. Autonegotiation
2. CDP
3. LLDP
4. Preconfigured values

www.takbook.com

6. Which of the following refer to standards that deliver power over all four pairs in a UTP cable?(Choose two answers.)

کدام یک از موارد زیر به این موضوع اشاره دارد که هر کابل UTP توان برق را از هر چهار جفت سیسم تامین می‌کند؟ (دو گزینه را انتخاب کنید)

1. PoE
2. UPoE
3. PoE+
4. UPoE+

7. Which statement identifies the functionality of virtual machines?

کدام یک از گزینه‌های زیر عملکرد ماشین مجازی را مشخص می‌کند؟

a. The hypervisor communicates on Layer 3 without the need for additional resources.
b. Each hypervisor can support a single virtual machine and a single software switch.
c. The hypervisor can virtual physical components including CPU, memory, and storage.
d. Virtualized servers run most efficiently when they are physically connected to a switch that is separate from the hypervisor.

www.takbook.com

فصل چهاردهم

Network Automation

در این فصل در مورد اتوماسیون در شبکه صحبت خواهیم کرد که چطور شرکت‌هایی مانند سیسکو به این فکر افتادن که کارهای شبکه را به صورت یک روال خودکار در بیاورند تا ابزارها و فرایندها به صورت دقیق در زمان مشخص اجرا شود.

در گذشته و تا به امروز برای ایجاد یک شبکه باید از دستگاه‌های مختلفی مانند روتر و سوئیچ استفاده کنید و بر روی آنها تنظیمات خاص خود را انجام دهید تا بتوانند به درستی در شبکه عمل کنند.

در سال ۲۰۱۰ شاهد معرفی شبکه‌ی جدیدی با عنوان Software Defined Networking یا SDN بودیم که یک شبکه بر پایه نرم‌افزار است.

SDN از یک کنترلر استفاده می‌کند، این کنترلر برنامه‌ها را قادر می‌سازند تا به صورت خودکار پیکربندی شوند و شبکه را از طریق رابط برنامه‌نویسی که به آن API می‌گویند کنترل کنند.

در شبکه‌ی سنتی، مهندس شبکه، برای اینکه دستگاه‌های شبکه را پیکربندی کند، باید زمان زیادی را صرف آن می‌کردند، اصولاً شبکه‌های سنتی Closed Platform بودن، یعنی اینکه ما به عنوان مدیرشبکه نمی‌توانستیم به داده‌های داخل یک سخت‌افزار دسترسی داشته باشیم و آن را ویرایش کنیم، ولی با استفاده از SDN و شبکه‌ی مبتنی بر کنترلر مهندسین می‌توانند تغییرات بیشتری را در زمان کمتری اعمال کنند و بسیار قابل انعطاف است.

در شبکه‌های سنتی اگر یک خرابی در یک دستگاه رخ دهد، مقدار زمانی که برای اصلاح آن خرابی نیاز است، بسیار زیاد خواهد بود ولی در شبکه‌های مبتنی بر نرم‌افزار این کار به صورت اتوماتیک و در مدت زمان کوتاهی انجام و رفع خواهد شد.

۱-۱۴ SDN و شبکه مبتنی بر کنترلر

دستگاه‌های شبکه، داده‌ها را به صورت پیام و به طور معمول در فرمت ارتباط داده‌ای مانند Ethernet ارسال می‌کنند. شما در مورد چگونگی کار سوئیچ ها و روترها (router) در تمام مدت آماده‌سازی برای آزمون CCNA آموزش کامل را فرا گرفته‌اید.

در واقع قابلیت برنامه‌نویسی شبکه و شبکه‌سازی نرم‌افزاری (SDN)، این ایده‌ها را به کار می گیرند، بخش‌ها و قسمت‌ها را تجزیه و تحلیل می‌کنند، راه‌هایی را برای بهبود آنها براساس نیازمندی‌های روز پیدا می‌کنند و مجددا این ایده‌ها را به شیوه‌ی جدیدی برای کار در شبکه‌ها ترکیب و فراهم می‌کنند.

www.takbook.com

این اولین بخشی است که محوری‌ترین مفاهیم SDN و قابلیت برنامه‌نویسی شبکه را توضیح می‌دهد. این کار با تجزیه برخی از مؤلفه‌های موجود در دستگاه‌های شبکه سنتی آغاز می‌شود. سپس این بخش توضیح می‌دهد که چگونه برخی نرم‌افزارهای کنترلر متمرکز، به نام کنترل‌کننده(کنترلر)، یک سبک معماری را برای کنترل برنامه‌نویسی‌آسان‌تر یک شبکه ایجاد می‌کنند.

بررسی Data Planes, Control Planes وManagement Planes

درباره‌ی اینکه روتر چه کاری انجام می‌دهد؟ سوئیچ چه کاری انجام می‌دهد؟ و بسیاری ازاین فکر و ایده‌ها که باید به ذهن خطور کند تمرکز کنید.

به عنوان مثال، روترها و سوئیچ‌ها برای ایجاد شبکه‌ها به صورت فیزیکی، با کابل و به صورت بی‌سیم به یکدیگر متصل می‌شوند. آن‌ها پیام‌ها را ارسال می‌کنند: سوئیچ‌ها در فرمت Ethernet و روترها به صورت بسته ارسال می‌کنند. آنها از پروتکل‌های مختلف جهت دریافت اطلاعات استفاده می‌کنند، مانند پروتکل‌های مسیریابی برای یادگیری مسیرهای شبکه در سطوح مختلف. هر کاری که دستگاه‌های شبکه انجام می‌دهند را می‌توان در یک سطح خاص طبقه‌بندی کرد.

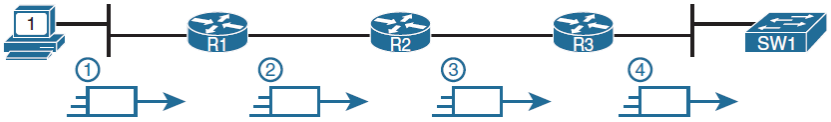
این بخش در مورد نحوه‌ی کار دستگاه‌های شبکه توضیحاتی می‌دهد و سه سطحی را توصیف می‌کند که اغلب برای توصیف چگونگی عملکرد برنامه‌نویسی شبکه استفاده می‌شوند: سطح داده‌ها و اطلاعات، سطح کنترل و بازرسی و سطح مدیریتی.

۱-۱-۱۴ بررسی Data Plane

اصطلاح Data Plane به کارهایی گفته می‌شود که یک دستگاه برای ارسال پیغام در شبکه استفاده می‌کند به عبارت دیگر به دریافت، پردازش و ارسال داده گفته می‌شود.

به مانند شکل ۱-۱۴، روتر R1 در لایه‌ی سوم اطلاعات را در گام اول پردازش می‌کند و به روتر همسایه‌ی خود ارسال می‌کند و همین‌طور تا آخر این کار انجام می‌شود.

می‌توان به معنای دقیق‌تر گفت که Data Plane بسته‌ها را از یک رابط شبکه دریافت می‌کند و تحویل رابط شبکه‌ی دیگر می‌دهد.



شکل ۱-۱۴ Data Plane

در زیر موضوعات مهمی که دستگاه‌های شبکه در Data Plane انجام می‌دهند، مشخص شده است:

- De-encapsulating و re-encapsulating یک پکت در یک فریم Data-link (روتر و سوئیچ لایه‌ی سوم)
- اضافه و حذف کردن هدر 802.1Q (روتر و سوئیچ لایه‌ی سوم)

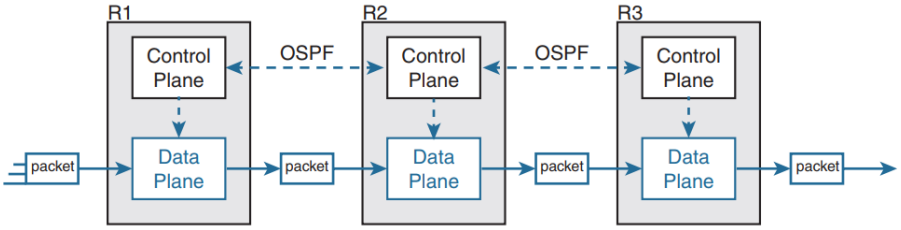
www.takbook.com

- مطابقت دادن(Match) MAC address با جدول MAC Address در سوئیچ لایه‌ی دوم.
- مطابقت دادن Destination IP Address با جدول IP در سوئیچ لایه‌ی سوم و روتر.
- رمزنگاری داده‌ها و اضافه کردن هدر جدید به بسته‌ی IP که بیشتر در شبکه‌های VPN کاربرد دارد.
- تغییر آدرس منبع و مقصد IP برای پردازش‌های پروتکل NAT .
- دور انداختن پیام‌هایی که در لیست‌های Acces List تعریف شدند و اجازه ندارند.

۱۴-۱-۲ بررسی Control Palne

Control Plane را به هر عملی می‌گوییم که قابل کنترل است، مثلاً روترهای برای انجام route نیاز به جدول Routing Table دارند تا DataPlane بتواند عملیات Route را به درستی انجام دهد، و یا اینکه سوئیچ‌ها به آدرس‌های MAC درون جدول MAC address table نیاز دارند تا بتوانند فریم‌ها را به مقصد مورد نظرشان ارسال کنند و... توجه داشته باشید حذف و اضافه کردن اطلاعات در جدول‌ها کار Data Plane است ولی نظارت بر این کار توسط Control Plane انجام می‌شود.

همان‌طور که در شکل ۲-۱۴، مشاهده می‌کنید، Control Plane را می‌توان یک مغز متفکر دانست که یک پروتکل را برای مدیریت ارتباطات فعال می‌کند، که در اینجا پروتکل مسیریابی OSPF فعال شده است و Data Plane هم کار انتقال Packet را انجام می‌دهد، توجه داشته باشید که عملیات Control Plane و Data Plane به صورت جداگانه بر روی هر یک از روترها انجام می‌شود.



شکل ۲-۱۴ Data Plane

نکته: در کل DataPlane نیاز شدیدی به Control Plane دارد و اگر یکی از آنها نباشد عملیات در دستگاه‌های شبکه به خوبی انجام نخواهد گرفت.

کارهایی که Control Plane انجام می‌دهد شامل موارد زیر است:

- IPv4 ARP
- IPv6 Neighbor Discovery Protocol (NDP)
- Switch MAC learning
- STP

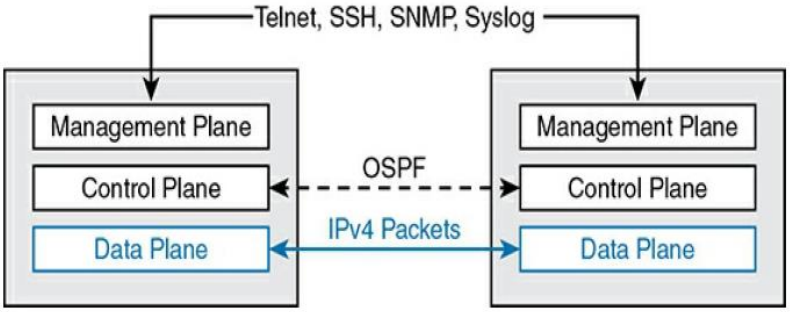
۱۴-۱-۳ بررسی Management Plane

پروتکل مدیریت دستگاه‌های شبکه است، Control Plane به طور خاص با Data Plane در ارتباط بوده و بر روی آن تاثیرگذار است اما Management Plane به صورت مستقیم با Data Palne در ارتباط نیست، ولی

www.takbook.com

در عوض Management Plane شامل پروتکل‌های مدیریتی است که مهندسین‌شبکه بسیار از آنها استفاده می‌کنند.

در شکل ۳-۱۴، چند پروتکل مدیریتی را مشاهده می‌کنید که در Management Plane قرار دارند، همچنین در شکل ۳-۱۴، نحویه چینش پروتکل‌ها را مشاهده می‌کنید.



شکل ۳-۱۴ Management Plane

همانطور که می‌دانید سوئیچ‌ها در ثانیه چندین فریم را Forwardمی‌کنند و اگر تعداد پورت‌های بر روی سوئیچ‌ها را در نظر بگیرید، سویئچ باید در کسری از ثانیه میلیون‌ها فریم را Forward کند، برای مثال اگر شرکت سیسکو بخواهد سرعت موردنیاز Data-plane را محاسبه کند، احتمالا با اعداد زیر مواجه میشود:

- سوئیچ دارای ۲۴ پورت است.
- هر کدام از پورتها دارای ۱۰۰ مگابایت پهنای‌باند هستند.
- فرض کنید طول هرFrame ، ۱۲۵بایت باشد.
- از Full duplex بروی همه پورت‌ها استفاده می‌شود، پس سوئیچ می‌تواند برروی تمامی پورت‌هایش به‌صورت همزمان، انتظار دریافت دیتا داشته باشد.
- نتیجه : هر پورت ۱۰۰۰۰۰ fpsدریافت خواهدکرد(منظور از fps یعنی frames per second) که در کل می‌توان گفت که سوئیچ 2/4 میلیون Frame در ثانیه ارسال می‌کند؛ پسdata-plane باید آمادگی پردازش 2/4 میلیون Frame را برثانیه داشته باشد.

در همین حین که ممکن است 2/4 میلیون عدد بزرگی به نظر برسد، بایدگفت که هیچ‌وقت هدف‌ما، مشخص کردن یک عدد خوب برای داشتن سرعت بالا درdata-plane نبوده است و بجایی آن Switchها نیاز به قدرت پردازشی داشتند که بتواند به‌صورت نرم‌افزاری پردازش‌های بیشتری نسبت بهCPUهای عمومی انجام دهند؛ به همین دلیل سوئیچ‌های سخت‌افزاری همیشه دارای یک سخت‌افزار خاص دیگری در داخل خود هستند که بتوانند پردازش data-plane را به‌صورت جداگانه و به‌خوبی انجام دهد.

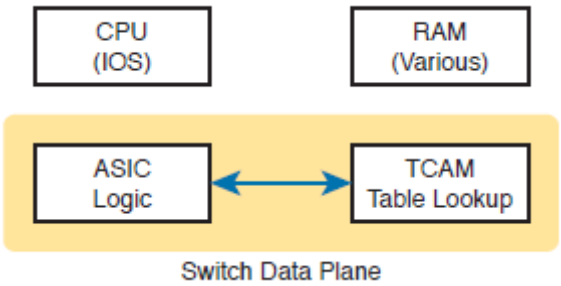
www.takbook.com

۱- باید گفت که منطق Switching در CPU انجام نمی‌شود و این مورد بر عهده‌ی ASIC (Application Specific Integrated Circuit) است، ASIC یک چیپ است که برای یک هدف خاص ایجاد شده است، مثل پردازش بسته‌ها در یک دستگاه تحت‌شبکه.

۲- ASIC باید توانایی این را داشته باشد که Table lookup مربوط به MAC Address Table را انجام دهد، پس برایlookup هرچه‌سریعتر، سوئیچ نیاز به یک حافظه خاص دارد که بتواند دقیقا معادله محتوای MAC Address tableرا در آن نگهداری کند که به این عمل Ternary Content-Addressable memory یا همان TCAM گفته می‌شود.

حافظه TCAM نیازی به ASIC برای جستجوی محتوای یک جدول ندارد و به جای آن ASIC فقط محتوا به فیلدTCAM (برای جستجو) می‌دهد، مثلاً به TCAM یک MAC Address می‌دهد و TCAM موردی که با آن Match می‌شود را بازمی‌گرداند.

درنظر داشته باشید که همه‌ی سوئیچ‌ها دارای یک CPU و Memory هستند. همانطور که در شکل ۴-۱۴، نمایش داده شده است IOS درون CPU اجرا شده و از RAM استفاده می‌کند؛ بیشتر توابع و عملیات Control-planeو Management-plane درون IOS اجرا می‌شوند؛ توابع مربوط بهData-plane و تابع مربوط به Control-plane در داخل ASIC انجام می‌شوند.



شکل ۴-۱۴ Management Plane

به این موضوع توجه کنید که بعضی از روترها از یک سخت‌افزار خاص برای پردازش توابع Data-plane استفاده می‌کنند، برای اطلاعات بیشتر درمورد Hardware data-plane forwarding در روترهای سیسکو، می‌توانید درمورد Quantum Flow Processor مطالعه کنید که تکنولوژی جذابی است.

کنترلرها و کنترل متمرکز

www.takbook.com

بیشتر پردازش‌ها Control-planeهای قدیمی، از یک معماری توزیع‌شده استفاده می‌کنند، یعنی Control-planeتوزیع می‌شود و بر روی دستگاه‌های مختلف اجرا می‌شود؛ برای مثال هر روتر، پردازش مربوط به روتینگ پروتکل OSPF را به‌صورت جداگانه اجرا می‌کند.

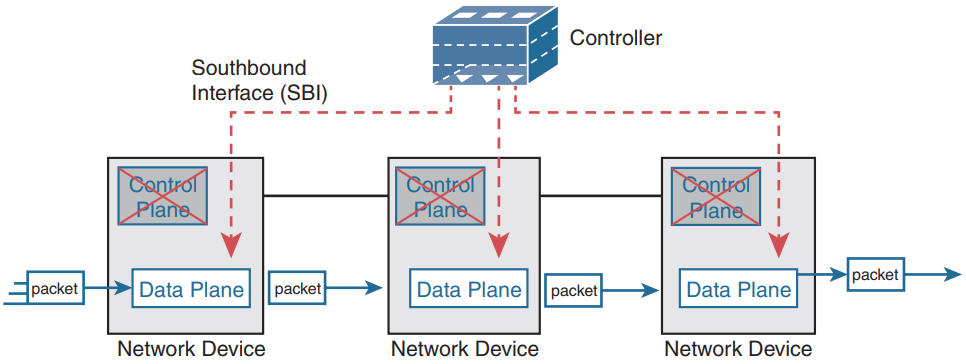
برای اینکه پردازش‌های مربوط به Control-plane های توزیع‌شده، درست کار کند برای ارتباط، از ارسال پیام به یکدیگر استفاده می‌کنند؛ مثلاً پروتکل OSPF در بین روترهای خود، پیام‌های مختلفی مبادله می‌کند.

پس می‌توان گفت شبکه‌های قدیمی از یک Distributed Control-plane استفاده می‌کنند.

برای انجام هر عملکردی در شبکه، مزایا و معایب مختلفی برای معماری‌های توزیع‌شده و متمرکز وجود دارد؛ بسیاری از Control-plane ها، دارای سابقه ی طولانی و خوبی در این موضوع هستند .

باید بدانیم نوشتن یک اپلیکیشن متمرکز، بسیار راحت‌تر از نوشتن یک اپلیکشن توزیع‌شده است؛ به این دلیل که نرم‌افزارهای متمرکز، تمام اطلاعات مورد نیازشان را در یک نقطه و به صورت آماده دارند؛ پس می‌توان گفت که دنیای جدید SDN و Network Programmability بیشتر از یک معماری متمرکز در سرویسی به‌نام کنترلر استفاده می‌کند.

یک کنترلر و یا SDN Controller ، کنترل تجهیزات شبکه را متمرکز می‌کند؛ اینکه چه مواردی به چه اندازه‌ای Centralized شوند، می‌تواند متفاوت باشد. برای توضیح بیشتر ایده‌ی یک کنترلر، تصویر ۵-۱۴، را نگاه کنید، یک SDN Controller تمام عملکردهای مهم Control-plane را متمرکز کرده است.



شکل ۵-۱۴ SDN Controller

در ابتدا Controller در جایی از شبکه قرار می‌گیرد که بتواند به تمام دستگاه‌های داخل شبکه از طریق IP دسترسی داشته باشد و بتواند آنها را ببیند. هرکدام از دستگاه‌های شبکه، دارای یک Data-plane هستند، اما دقت داشته باشید که هیچ کدام از آنها دارای Control-plane نیستند.

www.takbook.com

در تغییرات مربوط به SDN (همانطور که در شکل ۵-۱۴، مشاهده می‌کنید)، کنترلر به صورت مستقیم تمام Data-plane Entry جدول‌های هر دستگاه را برنامه‌ریزی و مقداردهی می‌کند، یعنی دیگر دستگاه‌های ما جدول‌های مربوط به Forwarding را با استفاده از پردازش‌های قدیمی Control-plane توزیع‌شده پُر نمی‌کند.

شکل ۵-۱۴، تنها یک مدل از Network Programmability و SDN را نشان می‌دهد، درحالی که موارد دیگری نیز وجود دارد؛ این تصویر پیش‌زمینه‌ی خوبی برای صحبت کردن در مورد کانسپت‌ها و مفاهیم مهم دیگر است، بخصوص درمورد ایده‌های Southbound Interface (SBI) و Northbound Interface (NBI) که در ادامه در موردشان صحبت خواهیم کرد.

The Southbound Interface

در یک معماری شبکه بر پایه ی کنترلر، کنترلر نیاز به ارتباط با دستگاه‌های داخل شبکه دارد؛ مانند تصویری که در بالا مشاهده کردید، معمولاً Networking Deviceها در نقشه‌ها، مستندات طراحی و معماری‌های شبکه در زیر Controller قرار می‌گیرند.

در بین کنترلر و دستگاه‌های شبکه، یک Interface قرار دارد و با توجه به محل آن Interface در شکل، به آن اینترفیس Southbound Interface یا SBI گفته می‌شود.

API یا Application Programming Interface روشی برای انتقال اطلاعات بین دو نرم‌افزار است یا به بیان دیگر، API یک Interface به یک نرم‌افزار است. برنامه‌ها، داده‌ها را پردازش می‌کنند و API به آنها اجازه می‌دهد که داده‌های خود را جابجا کنند.

پروتکل‌ها معمولاً با یک ساختار مشخص کار می‌کنند، اما API معمولاً دارای کدها، توابع، متغیرها و ساختمان‌داده‌های مختلفی هستند که برنامه ی دیگری در داخل شبکه می‌تواند از آنها استفاده کند.

SBI یک Interface، بین کنترلر و نرم‌افزار روی دستگاه‌های شبکه است و اجازه می‌دهد که این دو با یکدیگر ارتباط داشته باشند، با این هدف که کنترلر بتواند Data-plane دیوایس را مدیریت کند. در یک معماری شبکه که برای Network Programmability ایجاد شده‌است، قابلیت‌های SBIها و APIها، اطلاعات زیادی از توانایی و ضعف‌هایشان در اختیار ما قرار می‌دهند؛ برای مثال ممکن است بعضی از کنترلرها برای یک سری اهداف خاص، تنها اجازه ی استفاده از یک SBI را بدهند، در صورتی که بقیه ی موارد از تعداد زیادی SBI پشتیبانی می‌کنند که این کار باعث می‌شود بتوانیم از SBIهای مختلفی استفاده کنیم.

در زیر، سه نمونه از معماری‌ها را معرفی می‌کنیم که به صورت اتفاقی، SBIهای مختلفی هم دارند:

- Openflow

www.takbook.com

- OpFlex
- CLI

The Northbound Interface

به پیش‌نیازهایی که برای برنامه‌نویسی کنترلر که در تصویر قبل مشخص شده است، دقت کنید. تصویر نشان می‌دهد که کنترلر می‌تواند به Forwarding tableهای دستگاه‌ها، یک Entry اضافه کند، اما باید بدانید که کنترلر از کجا می‌داند که چه چیزی را باید به جدول‌ها اضافه کند؟، به چه صورت عمل کند؟ و قبل از اضافه کردن مقادیر، کنترلر شما به چه اطلاعاتی نیاز دارد تا بتواند مقداری را اضافه کند؟

به احتمال زیاد این اطلاعات را به دست می آورید:

- یک لیست از تمام دستگاه‌ها در شبکه
- قابلیت‌های هر دستگاه
- اینترفیس‌ها و پورت‌های هر دستگاه
- وضعیت فعلی هر پورت
- توپولوژی: هر دستگاه به چه جاهایی متصل شده است و بر روی کدامInterfaceها این ارتباط را برقرار کرده است.
- پیکربندی فعلیIP Address ها، VLANها و...

در یک مدل کنترل متمرکز، کنترلر، بیشتر کارهای مورد نیاز و مربوط به Control-plane را انجام می‌دهد و تمام اطلاعات مفید را از شبکه جمع‌آوری می‌کند (مانند مواردی که در لیست بالا مطرح شد) و در نهایت، خود کنترلر به تنهایی می‌تواند repository یا محلی متمرکز از این اطلاعات را برای شبکه ایجاد کند.

NBI برای یک کنترلر به این صورت است که راه ارتباط مستقیم با کنترلر را برقرار می‌کند تا برنامه‌های دیگر بتوانند از دیتا و زیرمجموعه‌ی آن استفاده کنند.

برنامه‌های گوناگون می‌توانند اطلاعات مختلفی را با استفاده از API کنترلر به دست آورند و نیز NBI به برنامه‌ها اجازه می‌دهد که با استفاده از SBI از قابلیت‌های Controller در ارسال جریان ترافیکی به دستگاه‌ها استفاده کنند.

برای اینکه ببینید NBI در کجا قرار می‌گیرد، در ابتدا در مورد خود Controller دقت کنید؛ کنترلر شما یک نرم‌افزار است که بر روی یک سرور اجرا شده است که می‌تواند یک VM و یا یک سرور فیزیکی باشد.

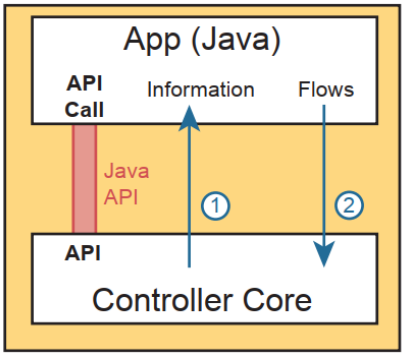
یک نرم‌افزار می‌تواند بر روی همان سروری که کنترلر قرار دارد، اجرا شود و از یک NBI استفاده کند، در نتیجه هر دو نرم‌افزار با استفاده از API می توانند با یکدیگر صحبت کنند.

www.takbook.com

برای مثال به شکل ۶-۱۴، توجه کنید؛ مستطیل نارنجی رنگ، نشان‌دهنده‌ی محل قرار گرفتن «نرم‌افزار کنترلر» است؛ کنترلر با استفاده از زبان Java نوشته شده است و دارای یک Java-based Native API است.

هر فردی می‌تواند به راحتی نرم‌افزاری بنویسد که بر روی این سیستم اجرا شود و از API جاوا کنترلر استفاده کند. نرم‌افزار توانایی آن را دارد که اطلاعات مختلفی را در مورد شبکه بدست آورد و جریان‌های شبکه را مدیریت کند؛ تنها کافی است از کنترلر بخواهد تا Action خاصی را در Forwarding tableهای دستگاه‌ها انجام دهد.

از دیگر API هایی که برای یک کنترلر استفاده می‌شوند، Representational State Transfe (REST) است که به اپلیکیشن‌ها اجازه می‌دهد بر روی Hostهای مختلفی قرار بگیرند و از HTTP برای انتقال پیام در API استفاده کنند.

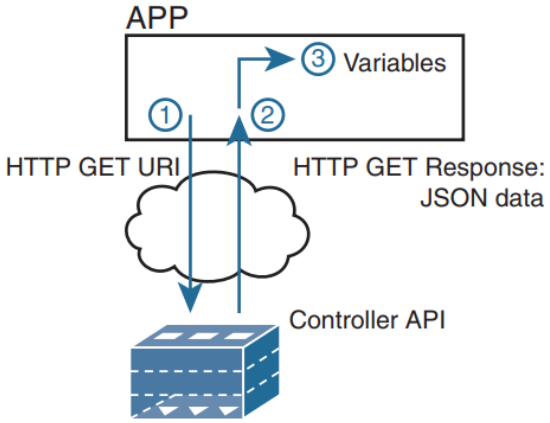


شکل ۶-۱۴ API

هنگامی که شما نمونه‌های مربوط به SDN را مشاهده می‌کنید (مانند تصویر بالا)؛ در این شرایط نیازی نیست که API ، پیام‌ها را در شبکه ارسال کند؛ به این دلیل که هر دو برنامه بر روی یک سیستم مشترک اجرا شده است، اما هنگامی که اپلیکیشن‌های شما بر روی سرورها و سیستم‌های جدا از هم قرار گرفته باشند، نیاز است که API بتواند داده‌ها را در IP ارسال و دریافت کند و اینجاست که RESTFUL APIها به شما کمک می‌کنند.

در شکل ۷-۱۴، ایده‌ی اصلی REST API را نشان می‌دهد؛ نرم‌افزار بر روی یک Host دیگر در بالای تصویر اجرا می‌شود و در مرحله‌ی اول به یک URI خاص، یک درخواست HTTP GET ارسال می‌کند که URIبرای شناسایی یک Object بر روی کنترلر استفاده می‌شود؛ برای مثال ممکن است که URI شما لیستی از Interface های فیزیکی یک دستگاه به همراه وضعیت هر یک از آنها باشد.

www.takbook.com



شکل ۷-۱۴ *REST API*

در مرحله‌ی دوم، کنترلر پیام بازگشت را به صورت یک HTTP GET Response message به همراه Objectارسال می‌کند؛ بیشتر REST API ها، درخواست دریافت یک داده‌ی ساختاریافته را می‌کنند و معمولاً از فرمت‌هایی مانند XML یا JSON برای Network programmability استفاده می‌کنند، مانند مرحله‌ی سوم در شکل ۷-۱۴.

۲-۱۴ APIهای مبتنی بر REST

برنامه‌ها برای برقراری ارتباط از رابطهای برنامه‌نویسی (APIs) استفاده می‌کنند. برای انجام این کار، یک برنامه می‌تواند متغیرها و ساختار داده‌های مورد استفاده توسط برنامه دیگر را یاد بگیرد و انتخاب منطقی بر اساس آن مقادیر داشته باشد، مقادیر آن متغیرها را تغییر دهد و متغیرهای جدید را ایجاد یا حذف کند. APIs به برنامه‌هایی که در رایانه‌های مختلف اجرا می‌شوند، اجازه می‌دهند تا به صورت مشارکتی کار کنند و داده‌ها را برای دستیابی به بعضی از اهداف جابجا و مبادله کنند.

در دنیای API، بعضی از برنامه‌ها دارای API هستند که برنامه‌های دیگر می‌توانند از این API استفاده کنند. توسعه‌دهندگان نرم‌افزار، APIها را به نرم‌افزار خود اضافه می‌کنند تا سایر نرم‌افزارهای کاربردی بتوانند از ابتدایی‌ترین ویژگی‌های آن برنامه استفاده کنند.

هنگام نوشتن یک برنامه، توسعه دهندگان، برخی از کدها را خواهند نوشت، اما اغلب توسعه دهندگان ممکن است با جستجوی APIها در اینترنت، بخش زیادی از کار را انجام دهند، وقتی توسعه دهنده‌ی نرم‌افزار این داده‌ها و توابع را تهیه کند، در این صورت میزان کدهای جدیدی که باید نوشته شود کاهش می‌یابد. در نتیجه، بسیاری از مراکز توسعه‌ی نرم‌افزارهای مدرن، برای درک و یادگیری APIهای جدید، دارای مراجع یا کتابخانه‌هایی هستند، در مورد کتابخانه‌ها باید گفت که کتابخانه یک بسته‌ی برنامه‌نویسی شده‌ی آماده است که می‌توان برای انجام تسک‌ها و وظایف از آن استفاده کرد که بسیار سریع‌تر از

www.takbook.com

نوشتن کد توسط برنامه‌نویس است و اصولاً در هنگام نوشتین یک برنامه با دستوری، کتابخانه مورد نظر فراخوانی می‌شود.

چندین نوع API وجود دارد که هرکدام دارای عملکرد متفاوتی هستند اما در این کتاب به یک نوع API اشاره می‌کنیم که عبارت‌اند از:

Representational State Transfer (REST) – که به دلیل محبوبیت آن به عنوان نوعی از API در برنامه‌های اتوماسیون شبکه استفاده می‌شود.

این بخش از فصل، نگاه دقیق‌تری به APIهای مبتنی بر REST دارد.

APIهای مبتنی بر REST (RESTful)

REST APIs شامل شش ویژگی است که چند دهه پیش توسط خالق آن یعنی Roy Fielding تعریف شده است: (در این سایت می‌توانید اطلاعات خوبی از آن بدست آورید https://restfulapi.net).

۶ ویژگی عبارت‌اند از:

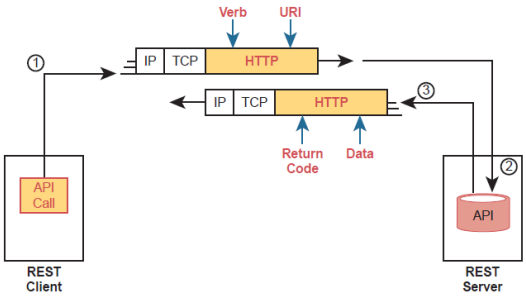
- معماری Server / Client
- عملیات بدون تابعیت
- قابلیت ذخیره‌سازی و غیرقابل ذخیره‌سازی
- ارتباط یک شکل
- دارای لایه یا طبقه
- کدنویسی بر اساس تقاضا

سه مورد اول از این ویژگی‌ها از چگونگی عملکرد REST API ، بدست می‌آید. خیلی راحت می‌توانید، سه ویژگی اول را در کار با شبکه‌های REST API مشاهده کنید، بنابراین چند پاراگراف بعدی توضیحات کمتری برای سه مورد اول می‌دهیم.

معماری Server / Client

برنامه‌های REST مانند بسیاری از برنامه‌ها از مدل معماری Server / Client استفاده می‌کنند. ابتدا ، یک توسعه دهنده‌ی برنامه، یک REST API را ایجاد می‌کند، و آن برنامه هنگام اجرا به عنوان REST Server عمل می‌کند. هر برنامه دیگری می‌تواند با اجرای کدی، باعث ایجاد درخواست از سمت مشتری به سمت سرور، شود و یک تماس REST API (REST Client) برقرار کند. به عنوان مثال ، در شکل ۸-۱۴:

www.takbook.com



شکل ۸-۱۴ REST API

۱. REST client در سمت چپ یک کانکشن REST API را اجرا می‌کند، که پیامی را که به REST Server ارسال می‌شود، تولید می‌کند.

۲. سرور REST در سمت راست دارای کد API است که درخواست را دریافت کرده و تصمیم می‌گیرد که چگونه به آن درخواست پاسخ دهد.

۳. سرور REST، در پیام پاسخ با متغیرهای داده مناسب پیام را تکمیل کرده و به سمت کلاینت ارسال می‌کند.

شکل ۸-۱۴، استفاده از HTTP را نشان می‌دهد، بسیاری از APIهای REST از HTTP استفاده می‌کنند ، استفاده از HTTP یک الزام برای یک API RESTful محسوب نمی‌شود.

عملیات Stateless

ویژگی Stateless، APIهای REST بدین معنی است که REST اطلاعاتی در مورد یک ارتباط API که قبلاً انجام شده است را در حافظه‌ی خود نگه نمی‌دارد. به عبارت دیگر ، از هر درخواست و پاسخ تاریخ گذشته API، در هنگام پردازش استفاده نمی‌کند.

برای مقایسه، پروتکل TCP از یک روش حالت‌پذیر (stateful) استفاده می‌کند، در حالی که UDP از عملیات بدون تابعیت (stateless) استفاده می‌کند.

قابلیت ذخیره‌سازی

برای درک منظور cacheable، در نظر بگیرید هنگام مرور وب‌سایت چه اتفاقی می‌افتد. هنگامی که مرورگر شما یک صفحه جدید وب را باز می‌کند، خود این صفحه شامل موضوعات متنوعی مانند متن، تصاویر،

www.takbook.com

فیلم‌ها، صدا و... است. بعضی از موضوعات به ندرت تغییر می‌کنند ، بنابراین بهتر است فقط یک بار آن را دانلود کنید. در این حالت، سرور آن موضوع را به عنوان cacheable علامت‌گذاری می‌کند. به عنوان مثال ، یک لوگو یا تصویر که در بسیاری از صفحات یک وب‌سایت نشان داده می‌شود تقریباً هرگز تغییر نمی‌کند و احتمالاً قابل ذخیره است.

با این وجود، لیست محصولات جدیدی که در وب‌سایت وارد شده‌اند، قابل ذخیره‌سازی نیستند، چون سرور می‌خواهد هر بار که شما درخواست خود را برای آن ارسال می‌کنید، لیست جدید را بروزرسانی و تهیه کند. APIهای REST نیاز دارند که هر منبع درخواست شده از طریق تماس API، از روش مشخصی برخوردار باشد که با استفاده از آن، منبع را به عنوان قابل ذخیره‌سازی یا غیرقابل ذخیره‌سازی علامت‌گذاری کند .توجه داشته باشید که منابع قابل ذخیره‌سازی با یک بازه زمانی، مشخص شده‌اند، به طوری که مشتری باید بداند چه موقع دوباره یک نسخه‌ی جدید از آن منبع را درخواست کند.

سابقه : داده‌ها و متغیرها

برای درک برخی از موضوعات آینده ، به شما کمک می کند تا ایده اصلی در مورد چگونگی استفاده از زبان های برنامه‌نویسی از متغیرها داشته باشید، هرکسی که مقدار کمی برنامه‌نویسی انجام داده باشد، باید از سابقه‌ی کافی برخوردار باشد، اما برای کسانی که قبلاً برنامه ننوشتند، این موضوع بعدی پیش‌زمینه‌ی کافی در مورد داده‌ها و متغیرهای درون برنامه را به شما می دهد

متغیرهای ساده

برنامه‌ها همه‌ی داده‌های پردازش شده را با همان اقدامات کلی و با نوعی ورودی شروع می کنند. این برنامه برای پردازش به داده نیاز دارد ، بنابراین فرایند ورودی فایل ها را می خواند، سوالات پایگاه داده را به سرور پایگاه داده می فرستد ، یا تماس های API را برای بازیابی داده ها از API برنامه دیگر ایجاد می‌کند. هدف: جمع آوری داده‌هایی که برنامه برای پردازش کار خود نیاز دارد.

سپس برنامه‌ها با انجام مقایسه، تصمیم‌گیری، ایجاد متغیرهای جدید و انجام فرمول‌های ریاضی برای تجزیه و تحلیل داده‌ها ، پردازش داده‌ها را انجام می دهند. تمام این منطق از متغیرها استفاده می‌کنند.

در برنامه‌نویسی ، یک متغیر درواقع یک نام یا برچسب است که دارای مقدار مشخصی است. برای به دست آوردن یک درک کلی نسبت به متغیرهای برنامه‌نویسی ، می‌توانید به متغیرهایی شبیه به متغیرهای معادلات جبر در مدرسه فکر کنید.

مثال زیر برخی از انواع مختلف متغیرها را در یک برنامه Python نشان می دهد (زبان Python امروزه محبوب‌ترین زبان برای نوشتن برنامه‌های اتوماسیون شبکه است). این برنامه با یک نظر (سه خط اول همراه با سه تکه سه گانه) شروع می‌شود و سپس چهار متغیر ایجاد می‌کند و آنها را به مقادیر مختلف

www.takbook.com

اختصاص می‌دهد، و پیغام "The product is -12 " را چاپ می‌کند. زیرا هر نام متغیر یک مقدار واحد دارد که به آن ارتباط دارد. متغیرهای ساده دارای یک نام متغیر و یک مقدار مرتبط هستند، بنابراین ساختار ساده‌ای دارند. مقادیر متغیرهای ساده می‌توانند دارای انواع مختلفی از قالب‌ها باشند ، مانند مثال زیر:

```
'''
Sample program to multiply two numbers and display the result
'''
x = 3
y = -4
z = 1.247
heading = "The product is "
print(heading,x*y)
```

مثال بالا دارای متغیرهایی است که شامل:

- اعداد صحیح بدون علامت (x)
- اعداد صحیح علامت‌دار (y)
- اعداد اعشاری (z)
- متن (heading)

لیست و فرهنگ لغت متغیرها

با وجود اینکه متغیرهای ساده کاربردهای بسیار زیادی دارند، اما برنامه‌ها به متغیرهایی با ساختار داده‌ی پیچیده‌تر نیاز دارند. در برنامه‌نویسی ، یک ساختار داده، مجموعه‌ی مرتبط متغیرها و مقادیر را تعریف می‌کند. به عنوان مثال ، Python از متغیرهای لیست استفاده می‌کند به طوری که به هر متغیر، مقداری که یک لیست از مقادیر است تا یک مقدار واحد، اختصاص داده می‌شود. شما می توانید تصور کنید که یک برنامه اتوماسیون شبکه ممکن است بخواهد لیستی از موارد زیر را داشته باشد:

- لیستی از دستگاه‌های در حال مدیریت.
- لیستی از رابط‌های دستگاه‌ها.
- لیست تنظیمات پیکربندی روی یک رابط.

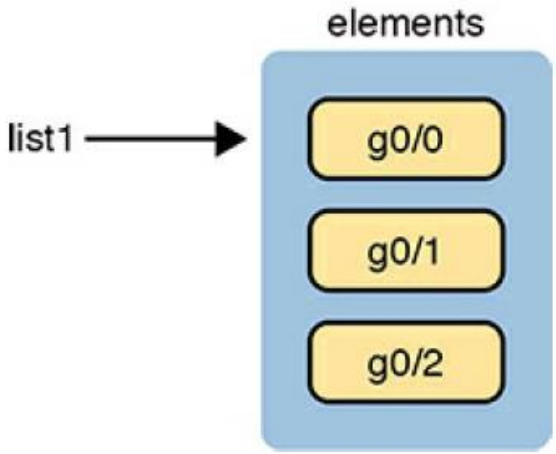
ابتدا متغیری به نام list1 را در مثال زیر نظر بگیرید؛ توجه داشته باشید که خط‌هایی که با یک # شروع می‌شوند، خط توضیح است.

```
# Variable list1 is a list in Python (called an array in Java)
list1 = ["g0/0", "g0/1", "g0/2"]
# Variable dict1 is a dictionary (called an associative array
in Java)
```

www.takbook.com


```
dict1 = {"config_speed":'auto', "config_duplex":"auto",
"config_ip":"10.1.1.1"}
```

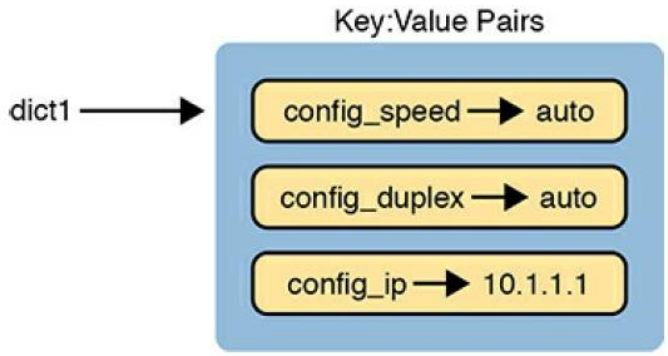
حتی اگر قبلاً کد Python را ندیده باشید، می‌توانید برخی از متغیرهای list1 را حدس بزنید. در این کد list1 را به مقداری اختصاص می‌دهیم که خود یک لیست از سه رشته متن است. توجه داشته باشید که این لیست می‌تواند شامل متن، اعداد صحیح بدون علامت، اعداد صحیح علامت‌دار و غیره باشد. شکل ۱۴-۹، ساختار داده‌ها را بعد از متغیر list1 در مثال بالا نشان می‌دهد. متغیرها به لیست اختصاص داده می‌شوند که این لیست دارای سه لیست عناصر است.



شکل ۹-۱۴ REST API

Python از یک ساختار داده مشابه، به نام فرهنگ لغت(dictionary) پشتیبانی می‌کند. با زبان‌های برنامه‌نویسی مانند Python ، ساختار داده dictionary موارد مترادف را نیز لیست می‌کند: کلیدها (مانند جملات) و مقادیر (مانند تعاریف). شکل ۱۰-۱۴، ساختار یک مقدار فرهنگ لغت را متناسب با متغیر dict1 در انتهای مثال بالایی نشان می‌دهد. توجه داشته باشید که به هر کلید و مقدار آن " key:value " گفته می‌شود.

www.takbook.com



شکل ۱۰-۱۴ REST API

REST APIs and HTTP

APIهایی وجود دارند که به دو برنامه امکان تبادل داده‌ها را می‌دهند. برخی از APIها ممکن است طوری طراحی شوند که واسط بین برنامه‌های در حال اجرا در همان سیستم باشند، بنابراین ارتباط بین برنامه‌ها در یک سیستم‌عامل واحد اتفاق می‌افتد. بسیاری از APIها باید در دسترس برنامه‌هایی باشند که در رایانه‌های دیگر اجرا می‌شوند ، بنابراین یک API، باید نوع پروتکل‌های شبکه که آنها را پشتیبانی می‌کند را تعریف کند. بسیاری از APIهای مبتنی بر REST از پروتکل HTTP استفاده می‌کنند. سازندگان APIهای مبتنی بر REST اغلب HTTP را انتخاب می‌کنند، زیرا منطق HTTP با برخی از مفاهیم تعریف شده، بیشتر مطابقت دارد. HTTP از همان اصول REST استفاده می‌کند یعنی با یک مدل Server / Client کار می‌کند.

اقدامات CRUD نرم افزار و افعال HTTP

صنعت نرم‌افزار برای چهار اقدام اصلی که توسط یک برنامه انجام می‌شود از کلمه‌ی مخفف CRUD استفاده می‌کند، که شامل موارد زیر است:

Create: به مشتری امکان می‌دهد موارد جدیدی از متغیرها و ساختار داده‌ها را در سرور ایجاد کنند و می‌توانند یک کپی از variables, structures, and values را در کلاینت ذخیره کنند.

Read: به مشتری امکان می‌دهد مقدار فعلی متغیرهایی را که در سرور وجود دارد ، بازیابی کند (بخواند) و نسخه‌ای از متغیرها، ساختارها و مقادیر را در کلاینت ذخیره کند.

Update: به مشتری امکان می‌دهد مقدار متغیرهای موجود در سرور را تغییر دهد (به روز کند).

www.takbook.com

Delete: به مشتری این امکان را می‌دهد موارد مختلفی از متغیرهای داده را از سرور حذف کند.

در جدول ۱-۱۴، مقایسه اقدامات CRUD را با REST مشاهده می‌کنید:

جدول ۱-۱۴ CRUD

Action	CRUD Term	REST (HTTP) Verb
Create new data structures and variables	Create	POST
Read (retrieve) variable names, structures, and values	Read	GET
Update or replace values of some variable	Update	PATCH, PUT
Delete some variables and data structures	Delete	DELETE

۱-۲-۱۴ کار با برنامه‌نویسی پایتون در شبکه

می‌توان گفت پایتون یکی از محبوب‌ترین زبان‌های برنامه‌نویسی است که در حین سادگی دارای قدرت بالایی در همه‌ی زمینه‌ها است، یکی از کارهایی که می‌توان با پایتون انجام داد، برنامه‌نویسی سوکت در شبکه است که یکی از راه‌های اتوماتیک‌سازی فرآیند است و امروزه بسیاری از مهندسان شبکه به این سو گرایش پیدا کردند.

www.takbook.com

برای اینکه در شبکه از پایتون استفاده کنید باید پیش‌نیازهایی را قبل آن گذرانده باشید، مثلاً شبکه را به صورت مقدماتی کار کرده باشید، پروتکل‌های شبکه را بشناسید و مهمتر از همه برنامه‌نویسی پایتون را در حد مقدماتی بلد باشید تا بتوانید از کدهایی که در آن استفاده می‌شود سردربیاورید.

در حال حاضر (۲۶ خرداد ۱۳۹۹) آخرین ورژن نرم‌افزار پایتون 3.8.3 است که به صورت رایگان می‌توانید از لینک زیر آن را برای ویندوز و یا دیگر سیستم‌عامل‌ها دانلود کنید:

https://www.python.org/downloads/

بعد از دانلود فایل را اجرا کنید و به مانند شکل ۱۱-۱۴، تیک گزینه‌ی Add Python 3.8 to PATH را انتخاب کنید و بر روی Install Now کلیک کنید.

شکل ۱۱-۱۴ Python

نصب نرم‌افزار به سادگی انجام خواهد شد و بعد از نصب می‌توانید برنامه را به صورت تکی و یا در CMD اجرا کنید، در ادامه می‌خواهیم نحوه‌ی برنامه‌نویسی در شبکه را بیاموزیم.

سوکت چیست:

اولین مبحثی که در این قسمت باید بررسی شود سوکت است، سوکت اصولاً یک پل ارتباطی بین ما و برنامه مورد نظر است که این برنامه می‌تواند یک برنامه کوچک یا سیستم‌عامل باشد، سوکت اولین بار در سال ۱۹۷۱ در ARPANET (سازمان پروژه‌های تحقیقاتی پیشرفته شبکه) آغاز شد و به تدریج گسترش پیدا کرد.

www.takbook.com

اگر بخواهیم درباره سوکت بحث کنیم باید بگوییم که چندین نوع سوکت در دسترس است که بیتشرین آنها دو نوع Connection Oriented و Connection Less هستند، نوع اول Connection Oriented هستند که به سوکت‌های Stream معروفند، که مبتنی بر پروتکل TCP است، یعنی اینکه قبل از مبادله اطلاعات باید یک اتصال مطمئن برقرار شود که اطلاعات به صورت درست و با امنیت به مقصد برسد، از این نوع سوکت برای ارتباط پروتکل هایی همانند FTPوSMTP, HTTP استفاده می‌شود. در سوکت Connection Less که به سوکت‌های Datagram معروفند و مبتنی بر پروتکل UDP هستند، یعنی اینکه قبل از مبادله اطلاعات هیچ امنیتی بین دو مبدأ و مقصدِ برقرار نمی‌شود و فقط سرعت در این ارتباط مهم است، از این نوع سوکت بیشتر برای انتقال صدا و تصویر استفاده می‌کنند.

متداول ترین نوع برنامه‌های سوکت، برنامه‌های مبتنی بر مشتری-سرور (client-server) است که در آن یک طرف به عنوان سرور عمل می‌کند و منتظر ارتباط از طریق مشتری است.

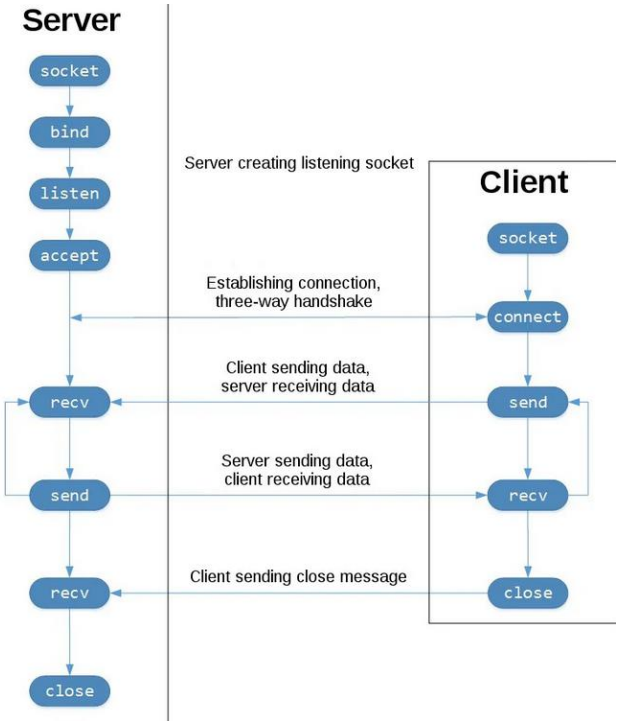
زبان برنامه‌نویسی پایتون دارای ماژول‌های بسیار گسترده‌ای است، در بخش شبکه هم دو ماژول Socket و Scapy بیشترین کاربرد را دارد و در این قسمت از آموزش از آنها استفاده خواهیم کرد.

در زیر توابع اصلی Socket API را مشاهده می‌کنید که هر کدام از آنها برای امر خاصی طراحی شده‌اند:

- `socket()`
- `bind()`
- `listen()`
- `accept()`
- `connect()`
- `connect_ex()`
- `send()`
- `recv()`
- `close()`

در شکل ۱۲-۱۴، نحوه ایجاد توابع را در پایتون مشاهده می‌کنید که کلاینت و سرور برای ایجاد ارتباط به چه صورت عمل می‌کنند.

www.takbook.com



شکل ۱۲-۱۴ Python

بررسی ماژول Socket

برای ایجاد یک سوکت می‌توانید از تابع socket.socket() استفاده کنید، که دستور کلی آن به صورت زیر است:

```
import socket

s= socket.socket (socket_family, socket_type, protocol=0)
```

در دستور بالا، با استفاده از import ماژول Socket صدا زده شد و در ادامه برای ایجاد سوکت باید از تابع socket.socket استفاده کرد که خود این تابع دارای چند قسمت است:

- socket_family: آدرس و پروتکل مورد نظر را نشان می‌دهد.
- socket_type : نوع سوکت را نمایش می‌دهد که می‌تواند SOCK_STREAM یا SOCK_DGRAM باشد.
- protocol : این مورد اختیاری است و معمولا به صورت پیش‌فرض مقدار آن صفر است.

www.takbook.com

برای اینکه بیشتر با این تابع آشنا شویم، یک مثال را با هم بررسی می‌کنیم:

برای اجرای یک کد ساده پایتون در شبکه می‌خواهیم یک پورت را در سرور صدا شده و کلاینت به آن پورت متصل شود، به معنای ساده‌تر باید یک سوکت بر روی پورت فعال کنیم تا به حالت LISTENING برود و بعد یک کلاینت به این پورت پاسخگو خواهد بود.

اولین کد را در سمت سرور وارد می‌کنیم، توجه داشته باشید برای راحتی کار شما سرور و کلاینت را در یک سیستم قرار دادیم تا بتوانیم به صورت سریع این موضوع را تست بگیریم.

```
import socket

s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)

s.bind(("192.168.5.165", 83))
s.listen(1)
connection, client = s.accept()
```

در دستور بالا در خط اول، کتابخانه‌ی socket صدا زده شد، و در خط دوم تابع socket.socket با دو آرگمان صدا زده شده که آرگمان socket.AF_INET برای آدرس‌دهی IPV4 به کار می‌رود و آرگمان socket.SOCK_STREAM برای ایجاد یک ارتباط TCP امن استفاده می‌شود.

در خط سوم با استفاده از تابع bind می‌توان آدرس IP و پورت مورد نظر را تعیین کرد، آدرس IP همان آدرس سیستمی است که در حال کار با آن هستیم و توجه داشته باشید که پورتی که وارد می‌کنید باید بر روی سیستم آزاد باشد و توسط برنامه دیگری استفاده نشود که در اینجا پورت 83 را وارد می‌کنیم، البه برای اینکه بفهمید چه پورتی در سیستم شما در حال استفاده است، باید از دستور زیر در CMD ویندوز خود استفاده کنید:

```
Netstat -a
```

توجه داشته باشید که کلید a- تمام اتصالات TCP فعال و پورت‌های TCP و UDP را که کامپیوتر در آن گوش می‌دهد (listening) را نشان می‌دهد.

www.takbook.com


```
Command Prompt - netstat -a
C:\Users\babajani>netstat -a

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:80             Center:0               LISTENING
  TCP    0.0.0.0:111            Center:0               LISTENING
  TCP    0.0.0.0:135            Center:0               LISTENING
  TCP    0.0.0.0:443            Center:0               LISTENING
  TCP    0.0.0.0:445            Center:0               LISTENING
  TCP    0.0.0.0:902            Center:0               LISTENING
  TCP    0.0.0.0:912            Center:0               LISTENING
  TCP    0.0.0.0:1063           Center:0               LISTENING
  TCP    0.0.0.0:1494           Center:0               LISTENING
  TCP    0.0.0.0:2049           Center:0               LISTENING
  TCP    0.0.0.0:2598           Center:0               LISTENING
  TCP    0.0.0.0:3387           Center:0               LISTENING
  TCP    0.0.0.0:3389           Center:0               LISTENING
  TCP    0.0.0.0:5985           Center:0               LISTENING
  TCP    0.0.0.0:6160           Center:0               LISTENING
  TCP    0.0.0.0:6161           Center:0               LISTENING
  TCP    0.0.0.0:6162           Center:0               LISTENING
  TCP    0.0.0.0:6169           Center:0               LISTENING
  TCP    0.0.0.0:6170           Center:0               LISTENING
  TCP    0.0.0.0:6190           Center:0               LISTENING
  TCP    0.0.0.0:6290           Center:0               LISTENING
  TCP    0.0.0.0:7070           Center:0               LISTENING
  TCP    0.0.0.0:9380           Center:0               LISTENING
  TCP    0.0.0.0:9381           Center:0               LISTENING
  TCP    0.0.0.0:9392           Center:0               LISTENING
```

شکل ۱۳-۱۴ listening

همانطور که در شکل ۱۳-۱۴، مشاهده می‌کنید تمام پورت‌های فعال در سیستم مشخص شده است، برگردیم به کد و خط چهارم که s.listen است که **این تابع میتواند محدودیتی برای تعداد کانکشن های ایجاد شده با سرور را مشخص کند که در این کد عدد 1 در نظر گرفته شده است.** در خط آخر هم منتظر پاسخ از طرف کلاینت می‌نشیند و بعد از دریافت پاسخ کد به اتمام می‌رسد.

بعد از اینکه کد را وارد کردید آن را در یک فایل با نام C1.py ذخیره کنید.

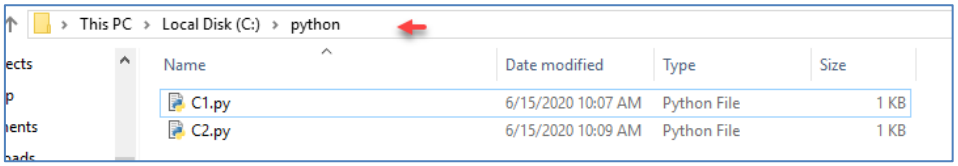
یک فایل دیگر با نام C2.py برای کلاینت ایجاد کنید و کد زیر را در آن وارد کنید.

```
Import socket
s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
s.connect(("192.168.5.165", 83))
```

در خط سوم این کد پاسخ سرور داده می‌شود و یک ارتباط TCP ایجاد می‌شود، برای تست این موضوع باید به صورت زیر عمل کنید:

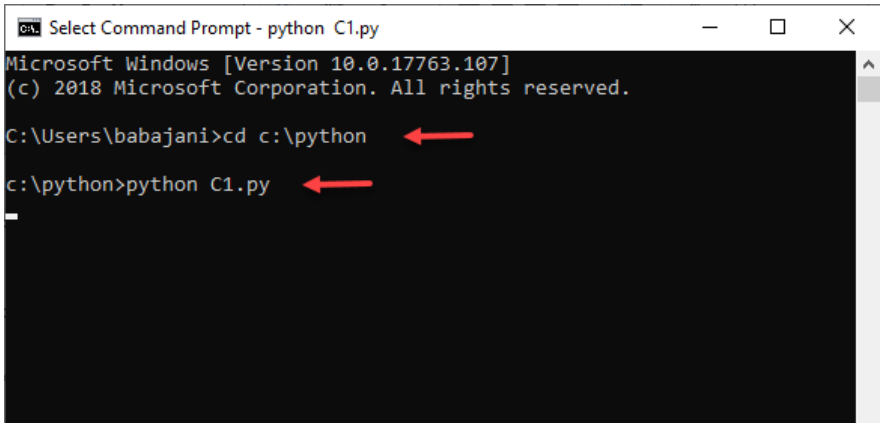
www.takbook.com

همانطور که در شکل ۱۴-۱۴، مشاهده می‌کنید دو فایل مورد نظر ایجاد شده است.



شکل ۱۴-۱۴ فایل‌های پایتون

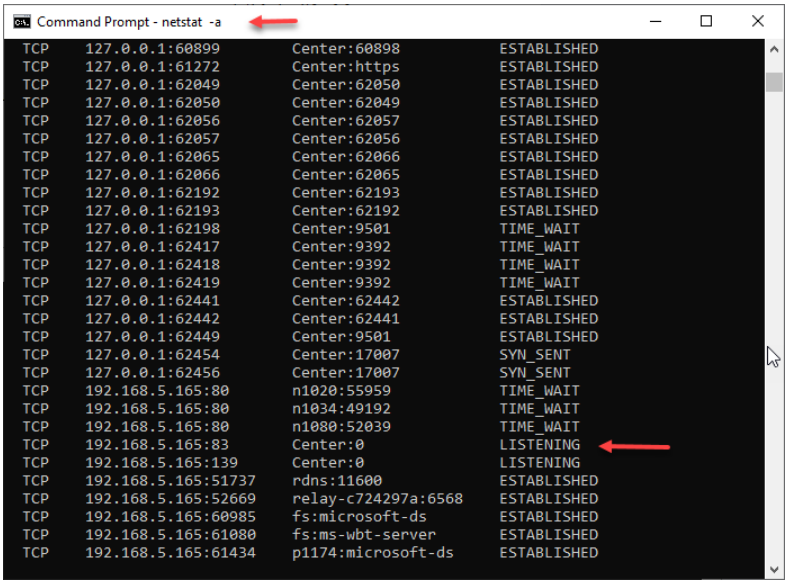
به مانند شکل ۱۵-۱۴، برای اجرای کد اول وارد CMD شوید و با دستور cd c:\python وارد پوشه‌ای شوید که دو فایل در آن قرار دارد و در آخر با دستور python C1.py کدل اول یعنی سرور را اجرا کنید.



شکل ۱۵-۱۴ اجرای فایل پایتون

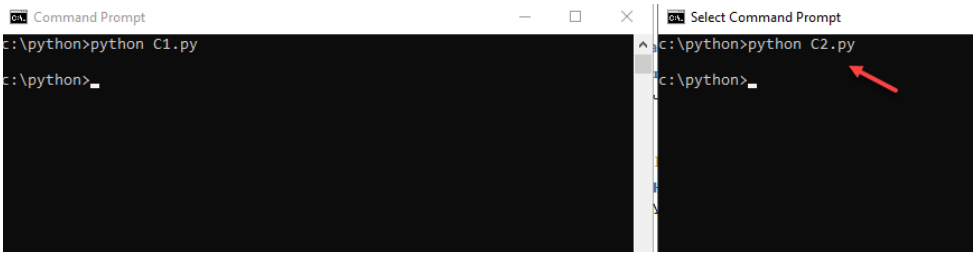
اگر با دستور netstat -a کانکشن‌ها را لیست کنید، همانطور که در شکل ۱۶-۱۴، مشاهده می‌کنید، آدرس IP به همراه پورت 83 را مشاهده می‌کنید که در حالت LISTENING قرار دارند و منتظر پاسخ از سمت کلاینت هستند.

www.takbook.com



شکل ۱۶-۱۴ listening

به مانند شکل ۱۷-۱۴، یک CMD دیگر باز کنید و فایل دوم یعنی C2.py را اجرا کنید، مشاهده می‌کنید که بعد از اجرای C2.py کد C1.py هم به اتمام رسیده است.



شکل ۱۷-۱۴ اجرای فایل پایتون

با این کار توانستیم یک ارتباط ساده با سوکت ایجاد کنیم، توجه داشته باشید چون از یک سیستم برای سرور و هم کلاینت استفاده کردیم می‌توانستید به جای آدرس IP از کلمه‌ی localhost استفاده کنید.

برای اینکه بیشتر با پایتون در شبکه آشنا شوید یک مثال دیگر را هم با هم بررسی می‌کنیم، در سمت سرور کد زیر را وارد کنید:

```
# echo_server.py
import socket

host = ''          # Symbolic name meaning all available interfaces
```

www.takbook.com


```
port = 12345      # Arbitrary non-privileged port
s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
s.bind((host, port))
s.listen(1)
conn, addr = s.accept()
print('Connected by', addr)
while True:
    data = conn.recv(1024)
    if not data: break
    conn.sendall(data)

conn.close()
```

همانطور که در کد بالا مشاهده می‌کنید پورت مورد نظر 12345 در نظر گرفته شده است، در دستور Print در سمت سرور آدرس IP و پورتی که به همراه پروت مورد نظر را که از طریق کلاینت دریافت می‌کند چاپ خواهد کرد، عدد 1024 در شرط While اشاره به اندازه‌ی بافر دارد تا کد در بافر اجرا شود.

کد بالا را با نام C3.py در همان پوشه‌ی Pyhton ذخیره کنید.

کد کلاینت هم به صورت زیر خواهد بود:

```
# echo_client.py
import socket

host = socket.gethostname()
port = 12345                    # The same port as used by the server
s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
s.connect((host, port))
s.sendall(b'Hello, world')
data = s.recv(1024)
s.close()

print('Received', repr(data))
```

در این کد هم پورت را 12345 در نظر گرفتیم، این کد را هم با نام C4.py در همان پوشه ذخیره کنید.
اگر سرور و کلاینت را به همان روشی که قبلاً گفتیم اجرا کنید، نتیجه کار چیزی شبیه به شکل ۱۸ – ۱۴، حواهد بود که در سمت سرور آدر IP و پورت کلاینت مشخص می‌شود و در سمت کلاینت هم کلمه‌ی Hello, Word چاپ خواهد شد.

www.takbook.com

Select Command Prompt

```
C:\python>python C3.py
Connected by ('10.150.157.18', 57241)

C:\python>
```

شکل ۱۸-۱۴ خروجی برنامه

Command Prompt

```
C:\python>python C4.py
Received b'Hello, world'

C:\python>
```

شکل ۱۹-۱۴ خروجی برنامه

۲-۲-۱۴ کار با کتابخانه Netmiko در پایتون

یکی از خصوصیات مهم برنامه نویسی پایتون این است که دارای کتابخانه‌های عظیمی است که توسط افراد یا تیم پایتون برای کارهای مختلف نوشته شده است، در شبکه هم برای کار با دستگاه‌های شبکه مانند دستگاه‌های سیسکو یک کتابخانه‌ی قدرتمند با نام Netmiko وجود دارد که توسط Kirk Byers نوشته شده است، برای دریافت توضیحات بیشتر می‌توانید به سایت زیر مراجعه کنید:

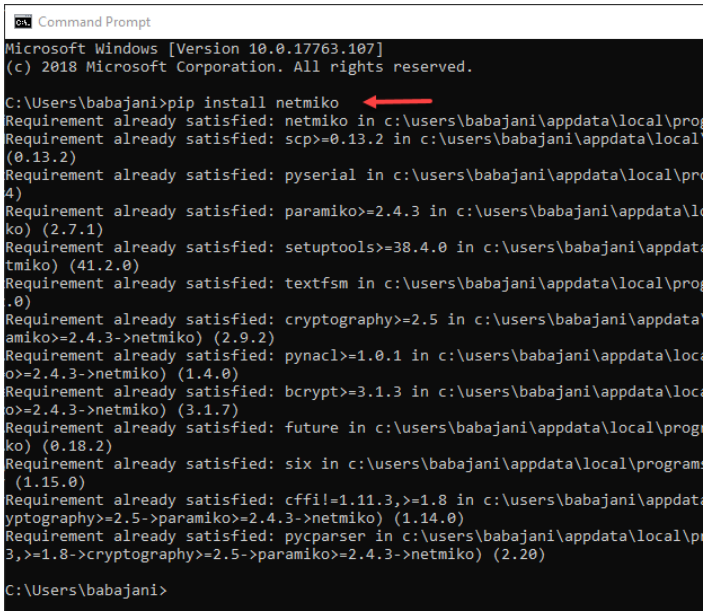
https://pynet.twb-tech.com/blog/automation/netmiko.html

در این کتابخانه شما می‌توانید از طریق دستوراتی که در ادامه مورد بررسی قرار می‌دهیم به روتر سیسکو متصل شوید و دستورات مورد نظر خود را اجرا کنید.

برای شروع کار، اول باید کتابخانه‌ی Netmiko را از اینترنت دانلود و نصب کنیم، برای این‌کار وارد CMD شوید و دستور زیر را وارد کنید. (شکل ۲۰-۱۴)

www.takbook.com

pip install netmiko

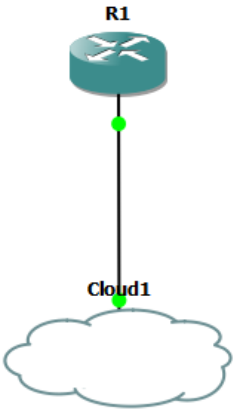


شکل ۲۰-۱۴ خروجی برنامه

همانطور که در شکل ۲۰-۱۴، مشاهده می‌کنید دستور مورد نظر کتابخانه‌ی Netmiko را از اینترنت دانلود و بر روی سیستم نصب کرد، توجه داشته باشید این دستور زمانی اجرا می‌شود که قبل از ام پایتون را بر روی سیستم خود نصب کرده باشد.

بعد از انجام کار بالا وارد GNS3 شوید و یک روتر را برای این کار تنظیم کنید، به مانند شکل ۲۱ - ۱۴ یک روتر به همراه یک Cloud به صفحه اضافه کنید، توجه داشته باشید که این Cloud باید به شبکه‌ی اصلی شما که سیستم بر روی آن فعال است متصل باشد تا بتوانید روتر را ببینید.

www.takbook.com



شکل ۲۱-۱۴ خروجی برنامه

وارد روتر R1 شوید و دستورات زیر را وارد کنید:

در دستور زیر وارد پورت fastEthernet 0/0 شده و آدرس آن را وارد کنید و در آخر پورت را روشن کنید.

R1(config)#**int fastEthernet 0/0**

R1(config-if)#**ip address 192.168.5.10 255.255.255.0**

R1(config-if)#**no sh**

برای اینکه بتوانیم از طریق پایتون به روتر دسترسی داشته باشیم باید سرویس SSH را روی آن فعال کنیم برای این کار دستورات زیر را اجرا کنید:

R1(config)#**ip domain-name 3isco.local**

R1(config)#**crypto key generate rsa**

The name for the keys will be: R1.3isco.local

Choose the size of the key modulus in the range of 360 to 4096 for your

General Purpose Keys. Choosing a key modulus greater than 512 may take

a few minutes.

www.takbook.com

How many bits in the modulus [512]: **1024**

% Generating 1024 bit RSA keys, keys will be non-exportable...

[OK] (elapsed time was 0 seconds)

بعد از فعال کردن سرویس SSH باید وارد پورت VTY شوید و به سرویس SSH اجازه عبور دهید:

R1(config)#**line vty 0 15**

R1(config-line)#**login**

R1(config-line)#**login locald**

R1(config-line)#**transport input ssh**

در آخر هم نام کاربری و رمز عبور را مشخص کرده و رمز عبور Enable را هم مشخص می‌کنیم تا با این کار بتوانیم به روتر دسترسی داشته باشیم.

R1(config)#**username admin password Test@12345**

R1(config)#**enable secret Test@12345**

توجه داشته باشید که برای فعال کردن SSH باید IOS روتر شما از نوع K9 باشد تا بتواند دستور crypto را پشتیبانی کند.

در ادامه کار یک CMD باز کنید و دستور Python را اجرا کنید، با این کار وارد خط فرمان پایتون خواهیم شد و دستورات را به مانند زیر وارد کنید:

>>> **import netmiko**(این دستور کتابخانه مورد نظر را وارد می‌کند)

>>> **dir(netmiko) (**این دستور، تمام دیکشنری‌های مربوط به این کتابخانه را نشان می‌دهد**)**

['BaseConnection', 'CNTL_SHIFT_6', 'ConnectHandler', 'FileTransfer', 'InLineTransfer', 'NetMikoAuthenticationException', 'NetMikoTimeoutException', 'Netmiko', 'NetmikoAuthenticationException', 'NetmikoTimeoutException', 'SCPConn', 'SSHDetect', '__all__', '__builtins__', '__cached__', '__doc__', '__file__', '__loader__', '__name__', '__package__', '__path__', '__spec__', '__version__', '_textfsm', 'a10', 'accedian', 'alcatel', 'apresia', 'arista', 'aruba', 'base_connection', 'calix', 'checkpoint', 'ciena', 'cisco', 'cisco_base_connection', 'citrix', 'cloudgenix', 'coriant', 'dell', 'dlink', 'eltex', 'endace', 'enterasys', 'extreme', 'f5', 'file_transfer', 'flexvnf', 'fortinet', 'hp', 'huawei', 'ipinfusion', 'juniper', 'keymile', 'linux', 'log', 'logging', 'mellanox', 'mikrotik', 'mrv', 'netapp', 'netmiko_globals', 'nokia', 'oneaccess', 'ovs', 'paloalto', 'platforms', 'pluribus', 'quanta', 'rad', 'redispatch', 'ruckus', 'ruijie', 'scp_functions', 'scp_handler', 'sophos', 'ssh_autodetect', 'ssh_dispatcher', 'ssh_exception', 'terminal_server', 'ubiquiti', 'utilities', 'vyos', 'watchguard']

www.takbook.com

دستورات بالا را در شکل ۲۲-۱۴، مشاهده می‌کنید:

```
Administrator: Command Prompt - python
>>> import netmiko
>>> dir(netmiko)
['BaseConnection', 'CNTL_SHIFT_6', 'ConnectHandler', 'FileTransfer', 'InLineTransfer', 'NetMikoAuthenticationException',
 'NetMikoTimeoutException', 'Netmiko', 'NetmikoAuthenticationException', 'NetmikoTimeoutException', 'SCPConn', 'SSHDetec
t', '__all__', '__builtins__', '__cached__', '__doc__', '__file__', '__loader__', '__name__', '__package__', '__path__',
'__spec__', '__version__', '_textfsm', 'a10', 'accedian', 'alcatel', 'apresia', 'arista', 'aruba', 'base_connection', '
calix', 'checkpoint', 'ciena', 'cisco', 'cisco_base_connection', 'citrix', 'cloudgenix', 'coriant', 'dell', 'dlink', 'el
tex', 'endace', 'enterasys', 'extreme', 'f5', 'file_transfer', 'flexvnf', 'fortinet', 'hp', 'huawei', 'ipinfusion', 'jun
iper', 'keymile', 'linux', 'log', 'logging', 'mellanox', 'mikrotik', 'mrv', 'netapp', 'netmiko_globals', 'nokia', 'oneac
cess', 'ovs', 'paloalto', 'platforms', 'pluribus', 'quanta', 'rad', 'redispatch', 'ruckus', 'ruijie', 'scp_functions', '
scp_handler', 'sophos', 'ssh_autodetect', 'ssh_dispatcher', 'ssh_exception', 'terminal_server', 'ubiquiti', 'utilities',
 'vyos', 'watchguard']
>>>
```

شکل ۲۲-۱۴ خروجی دستور dir(netmiko)

خوب همه چیز برای اجرای دستور اصلی آماده است، برای متصل شدن به روتر باید از گزینه‌ی ConnectHandler استفاده کنیم، که این گزینه را در دستور زیر مشاهده می‌کنید:

```
connection1=netmiko.ConnectHandler(ip="192.168.5.10", device_type="cisco_ios", username="admin",
password="Test@12345")
```

در دستور بالا باید آدرس IP، نوع دستگاه، نام کاربری و رمزعبور روتر سیسکو را که در قسمت قبل تنظیم کردیم، وارد کنید، این تنظیمات بعد از اجرا در متغییر connection1 قرار می‌گیرند که در شکل ۲۳-۱۴، این متغییر صدا زده شده و به درستی به دستگاه متصل شده است و در ادامه می‌توانیم از متغیر connection1 استفاده کنیم.

```
Administrator: Command Prompt - python
>>>
>>>
>>> connection1=netmiko.ConnectHandler(ip="192.168.5.10", device_type="cisco_ios", username="admin", password="Test@1234
5")
>>>
>>> connection1
<netmiko.cisco.cisco_ios.CiscoIosSSH object at 0x02BD2E98>
>>>
```

شکل ۲۳-۱۴ صدا زدن متغیر connection1

اگر بخواهیم دیکشنری مربوط به متغییر connection1 را مشاهده کنیم باید از دستور زیراستفاده کنید:

```
dir(connection1)
```

>>> **dir(connection1)**

']RESPONSE_RETURN', 'RETURN', 'TELNET_RETURN', '__class__', '__delattr__', '__dict__',

'__dir__', '__doc__', '__enter__', '__eq__', '__exit__', '__format__', '__ge__', '__getattribute__', '__gt__', '__hash__', '__init__', '__init_subclass__', '__le__', '__lt__', '__module__', '__ne__', '__new__',

www.takbook.com

'__reduce__', '__reduce_ex__', '__repr__', '__setattr__', '__sizeof__', '__str__', '__subclasshook__', '__weakref__', '_autodetect_fs', '_build_ssh_client', '_connect_params_dict', '_first_line_handler', '_lock_netmiko_session', '_modify_connection_params', '_open', '_read_channel', '_read_channel_expect', '_read_channel_timing', '_sanitize_output', '_session_locker', '_session_log_close', '_session_log_fin', '_test_channel_read', '_timeout_exceeded', '_try_session_preparation', '_unlock_netmiko_session', '_use_ssh_config', '_write_channel', '_write_session_log', 'allow_agent', 'allow_auto_change', 'alt_host_keys', 'alt_key_file', 'ansi_escape_codes', 'auth_timeout', 'banner_timeout', 'base_prompt', 'blocking_timeout', 'check_config_mode', 'check_enable_mode', 'cleanup', 'clear_buffer', 'close_session_log', 'commit', 'config_mode', 'device_type', 'disable_paging', 'disconnect', 'enable', 'encoding', 'establish_connection', 'exit_config_mode', 'exit_enable_mode', 'fast_cli', 'find_prompt', 'global_cmd_verify', 'global_delay_factor', 'host', 'is_alive', 'keepalive', 'key_file', 'key_policy', 'normalize_cmd', 'normalize_linefeeds', 'open_session_log', 'paramiko_cleanup', 'passphrase', 'password', 'pkey', 'port', 'protocol', 'read_channel', 'read_until_pattern', 'read_until_prompt', 'read_until_prompt_or_pattern', 'remote_conn', 'remote_conn_pre', 'save_config', 'secret', 'select_delay_factor', 'send_command', 'send_command_expect', 'send_command_timing', 'send_config_from_file', 'send_config_set', 'serial_login', 'serial_settings', 'session_log', 'session_log_record_writes', 'session_preparation', 'session_timeout', 'set_base_prompt', 'set_terminal_width', 'sock', 'special_login_handler', 'ssh_config_file', 'strip_ansi_escape_codes', 'strip_backspaces', 'strip_command', 'strip_prompt', 'system_host_keys', 'telnet_login', 'timeout', 'use_keys', 'username', 'verbose', 'write_channel['

همانطور که در بالا مشاهده می‌کنید، دستوراتی را که می‌توانید برای ارتباط با روتر از آنها استفاده کنید مشخص شده است، برای تست عملکرد آنها از دستور زیر برای نمایش Interfaceهای روتر استفاده می‌کنیم:

```
>>> print(connection1.send_command("sh ip int brief"))

Interface              IP-Address      OK? Method Status            Protocol

FastEthernet0/0        192.168.5.10    YES manual up                up

FastEthernet1/0        unassigned      YES unset  administratively down down
```

همانطور که در دستور بالا مشاهده می‌کنید این روتر دارای دو پورت است که یکی از آنها IP دریافت کرده است، که در شکل ۲۴-۱۴، هم این موضوع را می‌توانید مشاهده کنید.

www.takbook.com


```
Select Administrator: Command Prompt - python
>>> print(connection1.send_command("sh ip int brief"))
Interface              IP-Address      OK? Method Status                Protocol
FastEthernet0/0        192.168.5.10    YES manual up                    up
FastEthernet1/0        unassigned      YES unset  administratively down down
>>>
```

شکل ۲۴-۱۴ خروجی دستور

برای اینکه این دستورات را در یک فایل ذخیره کنیم و آن را صدا بزنیم باید به صورت زیر عمل کنید:

```
import netmiko
connection1=netmiko.ConnectHandler(ip="192.168.5.10",
device_type="cisco_ios", username="admin",
password="Test@12345")
print(connection1.send_command("sh ip int brief"))
connection1.disconnect()
```

دستورات بالا را در یک فایل ذخیره و آن را به صورت شکل ۲۵-۱۴، اجرا کنید:

```
Command Prompt
c:\python>python C4.py
Interface              IP-Address      OK? Method Status                Protocol
FastEthernet0/0        192.168.5.10    YES manual up                    up
FastEthernet1/0        unassigned      YES unset  administratively down down

c:\python>
```

شکل ۲۵-۱۴ خروجی فایل

همانطور که مشاهده می‌کنید، با صدا زدن فایل C4.py که دستورات بالا در آن قرار داشت، خروجی Interfaceهای روتر را به ما نشان داد.

برای اینکه کد برنامه را به شکل زیباتر و قابل فهمتر بنویسیم می‌توانیم از کدهای زیر برای این کار استفاده کنیم:

```
from netmiko import ConnectHandler

# Establish a connection to the router
Connect_Router= {
      'device_type': 'cisco_ios',
```

www.takbook.com


```
        'host':    '192.168.5.10',
        'username': 'admin',
        'password': 'Test@12345',
        'port' : 22,
}
net_connect = ConnectHandler(**Connect_Router)

# Operational Command Example
output = net_connect.send_command('show ip int b')

print(output)
```

در بالا با دستور From فقط گزینه‌ی ConnectHandler را از کتابخانه‌ی netmiko فراخوانی کردیم و دیگر نیاز به فراخوانی کل کتابخانه نیست، بعد از آن یک متغییر رشته‌ای با نام Connect_Router ایجاد می‌کنیم و اطلاعات ارتباطی با روتر را برای ان مشخص می‌کنیم.

بعد از آن نتیجه‌ی دستور ConnectHandler(**Connect_Router) را درون متغییر net_connect ریخته و دستور sh ip int b را ازآن درخواست می‌کنیم و در خروجی چاپ می‌کنیم.

در مجموع استفاده از زبان پایتون به صورت حرفه‌ای در شبکه شما را در ایجاد یک شبکه‌ی کاملاً اتوماتیک کمک خواهد کرد، هر چند در این بخش فقط یک بخش کوچکی از آن را بررسی کردیم ولی با تمرین و پیدا کردن منابع بهتر می‌توانید به بهترین نحو از آن استفاده کنید.

۱۴-۲-۳ بررسی SDN OpenDayLight

OpenDaylight یک نرم‌افزار Framework و یک SDN Controller است که به صورت منبع باز یا Open source توسط بنیاد لینوکس ارئه شده و میزبانی می‌شود که یکی از محبوب‌ترین کنترلر SDN در جهان است.

کنترلر SDN چیست؟

SDN یک فناوری جدید نیست، این فناوری از سال ۱۹۹۶ و برای ایجاد مدیریت کاربر روی ارسال و دریافت، در گره‌های شبکه به‌وجود آمد. برای اینکه SDN پیاده‌سازی شود، دو عامل نیاز بود، یک اینکه باید یک معماری منطقی مشترک بین تمامی سوییچ‌ها و روترها و دیگر تجهیزات شبکه ایجاد شود و دوم اینکه یک پروتکل امن بین SDN و تجهیزات شبکه مورد نیاز است که هر دوی این نیازها توسط پروتکل OpenFlow برطرف شد.

یکی از پروتکل‌هایی که SDN OpenDayLight از آن پشتیبانی می‌کند OpenFlow (نام پروتکل ارتباطی است که امکان پیکربندی سوییچ‌ها و مسیریاب‌های شبکه را از راه دور فراهم می‌کند) است، که برای آزمایش این نرم‌افزار به چند سوئیچ نیاز داریم که از OpenFlow پشتیبانی کنند ولی چون خرید سخت‌افزار گران است می‌توانید از نرم‌افزار مجازی‌سازی Mininet استفاده کنید. Mininet به شما این امکان

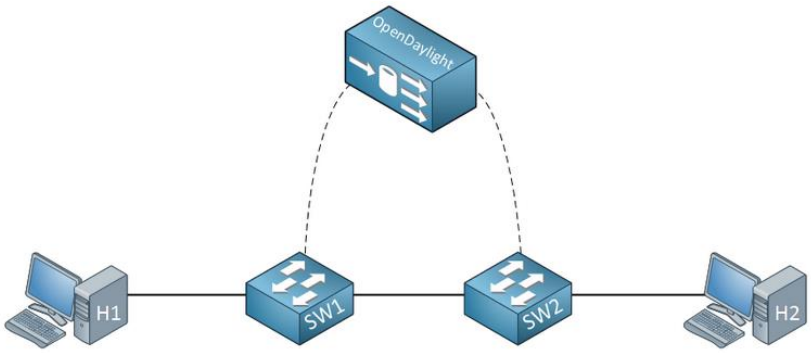
www.takbook.com

را می‌دهد تا با دستگاه‌هایی که از OpenFlow پشتیبانی می‌کنند، یک شبکه مجازی را بر روی سیستم شخصی خود اجرا کنید.

برای اینکه بهتر با این نرم‌افزار آشنا شوید می‌توانید به مثال زیر توجه کنید:

نکته: برای دانلود نرم‌افزار MiniNet می‌توانید از لینک زیر استفاده کنید:

http://mininet.org/download/

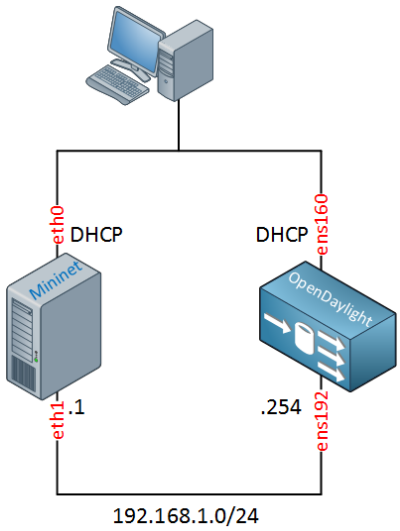


شکل ۲۶-۱۴ *OpenDaylight*

در شکل ۲۶-۱۴، یک کنترلر SDN که همان OpenDaylight باشد را مشاهده می‌کنید به همراه دو سوئیچ که از پروتکل OpenFlow پشتیبانی می‌کنند و درآخر دو میزبان که به سوئیچ‌ها متصل شده‌اند.

برا ادامه کار نیاز به دو ماشین مجازی داریم، یکی Mininet و دیگری OpenDaylight .

www.takbook.com



شکل ۲۷-۱۴ OpenDaylight

در شکل ۲۷-۱۴، دو ماشین مجازی را مشاهده می‌کنید. که در سمت چپ ، سرور Mininet را با دو interface در اختیار داریم. که Interface با نام eth0 ازDHCP Client استفاده می‌کند، در این سناریو از این Interface برای SSH استفاده خواهد شد. Interface با نام eth1 توسط سوئیچ‌های مجازی به کنترل‌کننده OpenDaylightمتصل است.

کنترلر OpenDaylight هم دارای دو Interface است که Interface ens160 برای SSH و برای دسترسی به GUI / API استفاده می‌شود. Interface ens192 برای برقراری ارتباط با سوئیچ‌های مجازی استفاده می‌شود.

یکی از مزیت‌های داشتن Mininet در یک ماشین مجازی مجزا این است که می‌توانید به راحتی شبکه مجازی خود را به کنترلرهای مختلف SDN از راه دور متصل کنید.

نصب OpenDaylight

برای نصب نرم‌افزار OpenDaylight یک ماشین‌مجازی با سیستم‌عامل لینوکس Ubuntu بر روی نرم‌افزار VMware راه‌اندازی کردیم که این ماشین دارای دو کارت شبکه مجازی است که در سناریو به آن اشاره کردیم.

نصب OpenDaylight در این تاریخ شاید با نصب آن در زمان حال شما تفاوت داشته باشد و بهتر است از سایت خود نرم‌افزار نحوه‌ی نصب آن را بررسی کنید، البته اگر در این قسمت به مشکل خوردید.

www.takbook.com

اگر نمی‌خواهید خودتان ماشین مجازی ایجاد کنید، می‌توانید از طریق لینک زیر ماشین آماده شده‌ی آن را دانلود و در VMware اجرا کنید:

https://s3.amazonaws.com/nwlpublic/OpenDayLightBoron.ova

توجه داشته باشید، نام کاربر و رمز عبور ماشین‌ها vmware است.

Network Interface

به صورت پیش‌فرض، تنها Interface که در ماشین OpenDatlight فعال است همان Interface است که از DHCP client استفاده می‌کند و برای اینکه Interface دیگر را فعال کنید باید به صورت زیر عمل کنید:

با استفاده از دستور زیر در لینوکس Ubuntu می‌توانید مشاهده کنید که چند Interface دارید:

$ **ip link**

1: **lo**: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN mode DEFAULT group default qlen 1

link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00

2: **ens160**: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP mode DEFAULT group default qlen 1000

link/ether 00:0c:29:d2:92:c6 brd ff:ff:ff:ff:ff:ff

3: **ens192**: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP mode DEFAULT group default qlen 1000

link/ether 00:0c:29:d2:92:d0 brd ff:ff:ff:ff:ff:ff

همانطور که مشاهده می‌کنید، این ماشین دارای دو کارت شبکه‌ی اصلی با نام‌های ens160 و ens192 است که برای تنظیم Interface دوم باید به صورت زیر عمل کنید:

با دستور زیر وارد تنظیمات شبکه‌ی لینوکس خواهید شد:

$ sudo vim /etc/network/interfaces

به این نکته توجه کنید که vim یک ویرایشگر در لینوکس است که در دستور بالا فایل Interfaces را در مسیر مورد نظر ویرایش می‌کند.

www.takbook.com

بعد از باز شدن فایل در آخر آن متن زیر را وارد کنید:

```
# Second interface

auto ens192

iface ens192 inet static

address 192.168.1.254

netmask 255.255.255.0
```

اطلاعات را با دستور CTRL + X ذخیره کنید و برای اینکه این تنظیمات بر روی لینوکس فعال شود سرور را ریسیت یا از دستور زیر استفاده کنید:

$ **sudo ifup ens192**

نصب JAVA

OPENLight یک نرم‌افزار جاوا است و برای اجرا نیاز به JAVA دارد که باید با دستور زیر در لینوکس نصب کنید:

$ **sudo apt-get install default-jre-headless**

بعد از نصب با دستور زیر فایل مورد نظر را باز کنید:

$ **vim ~/.bashrc**

و خط زیر را برای تنظیم متغییر JAVA_Home اضافه کنید:

```
export JAVA_HOME=/usr/lib/jvm/default-java
```

فایل را ذخیره کرده و با دستور زیر پرونده‌ی bashrc./ را اجرا کنید:

$ **source ~/.bashrc**

در ادامه کار حالا باید نرم‌افزار OpenDaylight را از لینک زیر دانلود و بر روی لینوکس مجازی خود نصب کنیم:

https://www.opendaylight.org/downloads

اگر بخواهید مستقیم از طریق لینوکس دانلود کنید می‌توانید از دستور زیر استفاده کنید:

www.takbook.com


```
$ wget https://nexus.opendaylight.org/content/groups/public/org/opendaylight/integration/distribution-karaf/0.5.0-Boron/distribution-karaf-0.5.0-Boron.zip
```

بعد از دانلود فایل zip باید آن را از حالت فشرده خارج کنیم، اول از همه نرم‌افزار Unzip را با دستور زیر نصب می‌کنیم:

```
$ sudo apt-get install unzip
```

بعد فایل فشرده شده را با دستور زیر از حالت فشرده خارج می‌کنیم:

```
$ unzip distribution-karaf-0.5.0-Boron.zip
```

و در آخر برای اجرای کنترلر از دستور زیر استفاده کنید:

```
$ cd distribution-karaf-0.5.0-Boron/
$ ./bin/karaf
```

OpenDaylight از فناوری karaf container استفاده می‌کند و این امکان را به نرم‌افزار می‌دهد تا همه چیز را از درون یک پوشه اجرا کند، بعد از یک دقیقه اطلاعات زیر ظاهر خواهد شد:

```
Apache Karaf starting up. Press Enter to open the shell now...
100%
[==========================================================
==========]

Karaf started in 69s. Bundle stats: 314 active, 314 total

    ________                        ________                .__
.__         .__      __
    \_____   \ ______   ____    ____ \______ \ _____   ___.__.|   |
|__| ____ |   |___/  |_
     /    |    \\____ \_/ __ \ /    \ |    |  \\__   \<    |   ||   |
|   |/ ___\|   |  \    __\
    /     |     \  |_> >  ___/|    |  \|     `    \/ __ \\___   ||
|_|   / /_/   >    Y   \   |
    \_______   /    __/ \___   >___|  /_______   (____   /
____||____/__\___   /|___|   /__|
            \/|__|         \/      \/         \/      \/\/
/_____/       \/

Hit '<tab>' for a list of available commands
and '[cmd] --help' for help on a specific command.
Hit '<ctrl-d>' or type 'system:shutdown' or 'logout' to
shutdown OpenDaylight.

opendaylight-user@root>
```

www.takbook.com

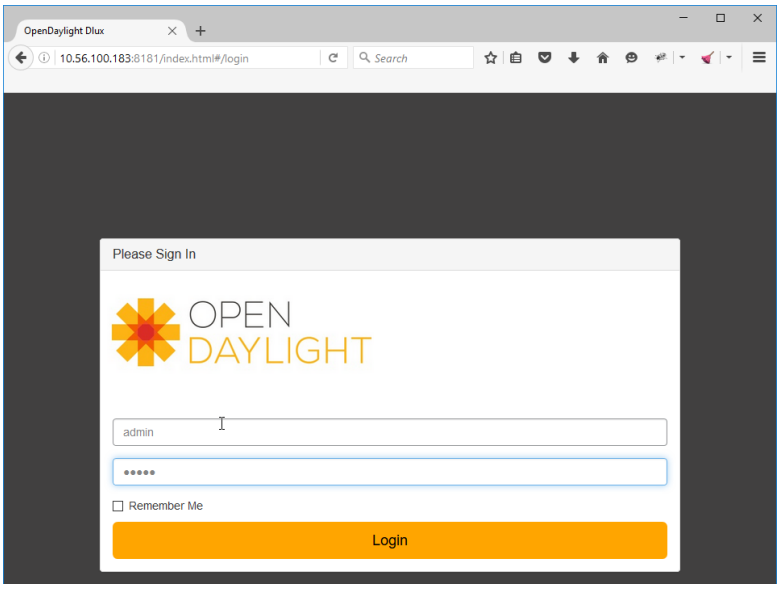
این کنترلر دارای برخی ویژگی‌های اساسی است، ولی برای اینکه بخواهیم کار مفیدی انجام دهیم باید برخی از ویژگی‌های مهم آن را فعال کنیم، در این قسمت می‌خواهیم GUI، RESTCONF API و برخی از قابلیت‌های سوئیچینگ لایه‌ی دوم را برای یادگیری آدرس MAC فعال کنیم، برای این کار باید از دستورات زیر استفاده کنیم:

```
opendaylight-user@root>feature:install odl-restconf odl-l2switch-switch odl-mdsal-apidocs odl-dlux-all
```

برای دسترسی به کنترلر باید از طریق وب عمل کنید و آدرس زیر را اجرا کنید، در دستور زیر به جای کلمه‌ی ip-address-of-opendaylight باید آدرس سرور OpenLight را وارد کنید.

http://**ip-address-of-opendaylight**:8181/index.html#login

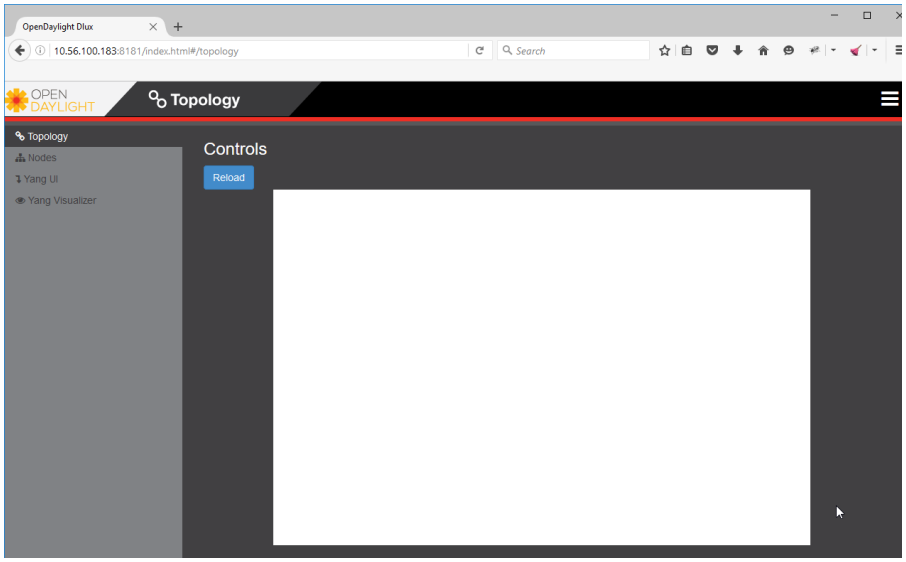
شکل ۲۸-۱۴، صفحه‌ی ورود به نرم‌افزار OpenDaylight را مشاهده می‌کنید، که با نام کاربری و رمز Admin وارد آن شوید.



شکل ۲۸-۱۴ OpenDaylight

بعد از ورود به نرم‌افزار اولین صفحه‌ای که مشاهده می‌کنید به صورت شکل ۲۹-۱۴، خواهد بود، که یک تصویر خالی از توپولوژی را به ما نشان می‌دهد، زیرا هیچ سوئیچی در حال حاضر فعال نیست، که باید با mininet کار کنیم.

www.takbook.com



شکل ۲۹-۱۴ *OpenDaylight*

Mininet

این نرم‌افزار به ما این امکان را می‌دهد تا یک شبکه‌ی مجازی با سوئیچ، روتر و هاست ایجاد کنیم، برای راحتی کار بهتر است ماشین مجازی که در سایت Mininet وجود دارد را از لینک زیر دانلود کنید و بر روی آن کار کنید:

http://mininet.org/download/

برای راحتی کار شما یک VM آماده کردیم که آدرس IP به Interface آن تخصیص داده شده است و نیازی به وارد کردن اطلاعات نیست، برای دانلود می‌توانید از لینک زیر استفاده کنید:

https://s3.amazonaws.com/nwlpublic/Mininet221.ova

بعد از راه‌اندازی ماشین مجازی Mininet باید ببینیم که آیا این ماشین با OpenDaylight ارتباط دارد یا خیر:

$ **ping 192.168.1.254 -c 3**

PING 192.168.1.254 (192.168.1.254) 56(84) bytes of data.

64 bytes from 192.168.1.254: icmp_seq=1 ttl=64 time=0.248 ms

64 bytes from 192.168.1.254: icmp_seq=2 ttl=64 time=0.284 ms

www.takbook.com

64 bytes from 192.168.1.254: icmp_seq=3 ttl=64 time=0.220 ms

--- 192.168.1.254 ping statistics ---

3 packets transmitted, 3 received, 0% packet loss, time 1998ms

rtt min/avg/max/mdev = 0.220/0.250/0.284/0.031 ms

در دستور بالا کلمه c- سه بار Replay را انجام می‌دهد و همانطور هم مشاهده می‌کنید توانستیم ماشین OpenDaylight را از طریق ماشین Mininet ببینیم.

ما با یک چیز ساده شروع خواهیم کرد. توپولوژی‌های زیادی وجود دارد که می توانیم بسازیم اما فعلاً ، اجازه دهید شبکه‌ای بسازیم که:

- دارای دو سوئیچ مجازی است که از پروتکل Openflow پشتیبانی می‌کنند.
- دارای دو میزبان مجازی است.
- از OpenDaylight به عنوان کنترل کننده SDN از راه دور استفاده می‌کند.

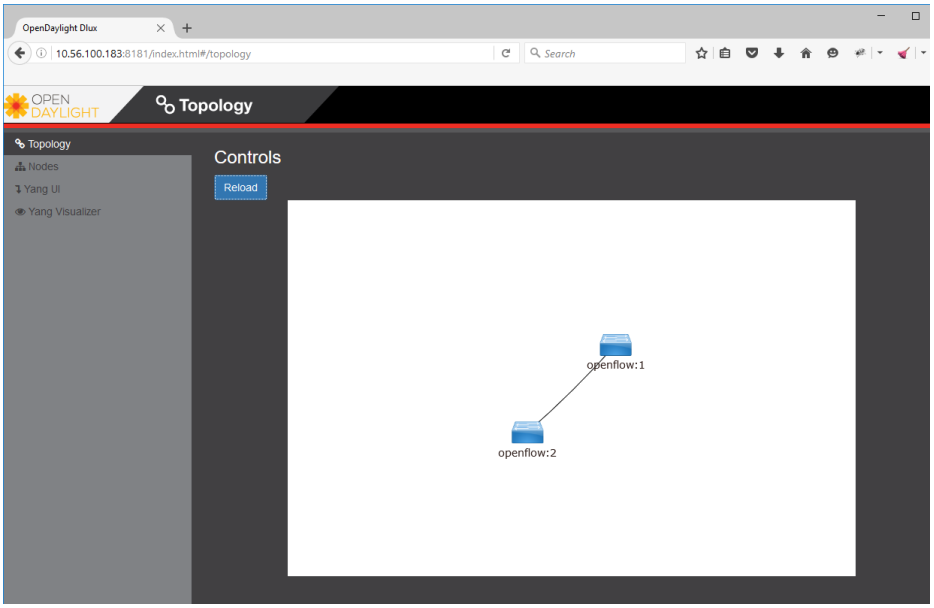
برای راه اندازی این روش می‌توانید از دستور زیر درMininet استفاده کنید:

```
$ sudo mn --topo linear,2 --mac --
controller=remote,ip=192.168.1.254,port=6633 --switch
ovs,protocols=OpenFlow10
*** Creating network
*** Adding controller
*** Adding hosts:
h1 h2
*** Adding switches:
s1 s2
*** Adding links:
(h1, s1) (h2, s2) (s2, s1)
*** Configuring hosts
h1 h2
*** Starting controller
c0
*** Starting 2 switches
s1 s2 ...
```

www.takbook.com


```
*** Starting CLI:
```

همانطور که در نتیجه‌ی دستور بالا مشاهده می‌کنید شبکه مجازی ما اکنون راه‌اندازی شده است و برای مشاهده بهتر کار باید وارد OpenDaylight در مرورگر خود شویم، همانطور که در شکل ۳۰ –۱۴، مشاهده می‌کنید دو دستگاه مجازی Openflow به توپولوژی ما اضافه شده است.



شکل ۳۰-۱۴ *OpenDaylight*

در حال حاضر ما فقط دو سوئیچ را می‌بینیم البته شبکه مجازی ما همچنین دارای دو میزبان است.

Mininet به ما امکان ایجاد ترافیک را می‌دهد. یک روش سریع برای انجام این کار با استفاده از دستور pingall است. همانطور که از نام آن پیداست ، برخی از پینگ‌ها را بین همه دستگاه‌ها ارسال می‌کند:

mininet> **pingall**

*** Ping: testing ping reachability

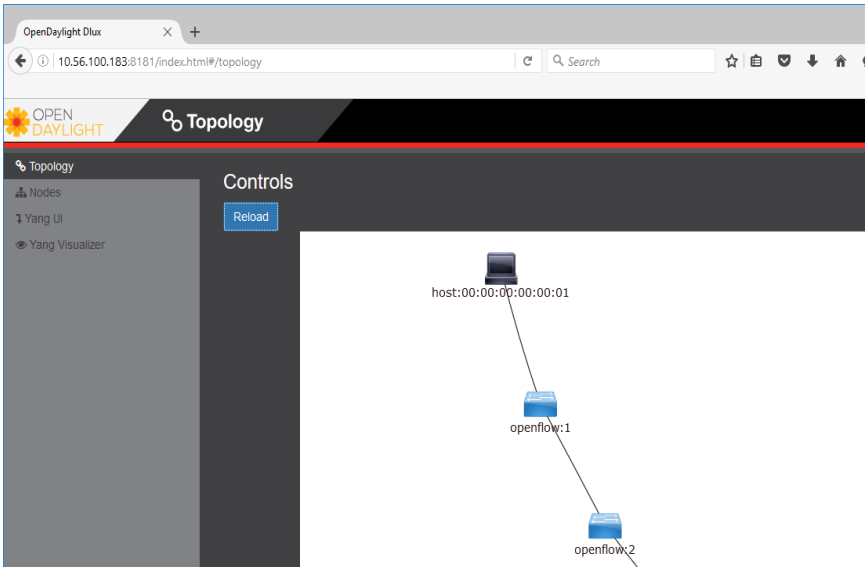
h1 -> h2

h2 -> h1

*** Results: 0% dropped (2/2 received)

www.takbook.com

خوب حالا اگر مرورگر خود را Refresh کنید با شکل ۳۱-۱۴، مواجه خواهید شد که دو هاست هم به صفحه اضافه شده است.



شکل ۳۱-۱۴ *OpenDaylight*

رابط کاربری گرافیکی OpenDaylight خوب است، اما بسیار محدود است. اگر می‌خواهید کنترلر SDN خود را کنترل و پیکربندی کنید باید از API RESTCONF استفاده کنید.

چندین روش مختلف برای استفاده از API وجود دارد، من گزینه‌های مختلفی را به شما نشان خواهم داد. ابتدا بگذارید توضیح دهم که RESTCONF چیست؟

برای چند دهه‌ی گذشته ، ما از CLI برای پیکربندی تجهیزات شبکه خود استفاده کرده‌ایم و بسیاری از ابزارهای اتوماسیون شبکه هم از اسکریپت CLI استفاده می‌کنند، اما CLI برای انسان ایجاد شده است. ما از دستورات show/debug برای تأیید کار خود استفاده می‌کنیم. انجام چنین کاری برای ما بسیار خوب است اما نرم‌افزار چیزی از این دستورات متوجه نخواهد شد. برای اینکه نرم‌افزار این موارد را متوجه شود باید اسکریپت‌نویسی کنید و به مرور زمان هم باید این اسکریپت‌ها را بروزرسانی کنید.

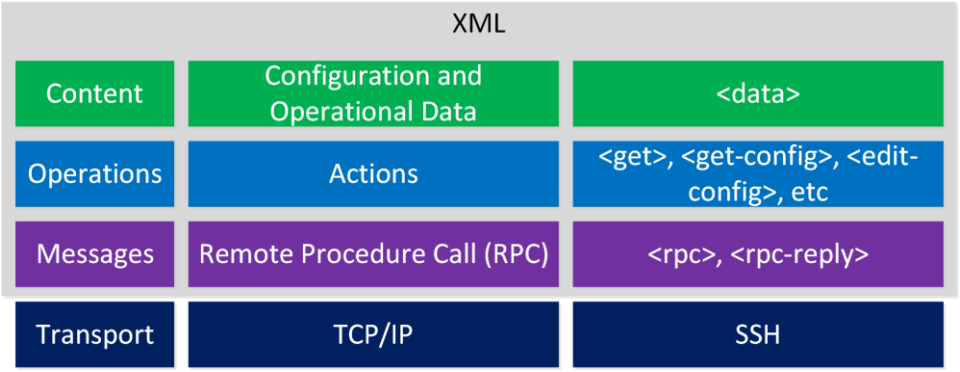
برای آسانتر کردن اتوماسیون شبکه، سازمان IETF، NETCONF را گسترش داد.

NETCONF یک پروتکل مدیریتی است که به ما این امکان را می‌دهد که تنظیمات دستگاه‌های شبکه را نصب، ویرایش و حذف کنیم. از XML برای رمزنگاری داده‌ها و از RPC برای حمل و نقل داده‌ها

www.takbook.com

استفاده می‌شود، که این کار می‌تواند جایگزینی برای CLI برای پیکربندی دستگاه‌های شبکه باشد، همچنین می‌توانید از NETCONF برای دریافت آمار از دستگاه‌های شبکه استفاده کنید.

در شکل ۳۲-۱۴، نمای کلی از لایه‌های مختلف NETCONF را مشاهده می‌کنید:



شکل ۳۲-۱۴ لایه‌های NETCONF

ما از XML به عنوان فرمت داده استفاده می کنیم:

مواردی که می‌خواهیم از یک دستگاه شبکه پیکربندی یا بازیابی کنیم ، در برچسب <data> کپسوله می‌شوند.

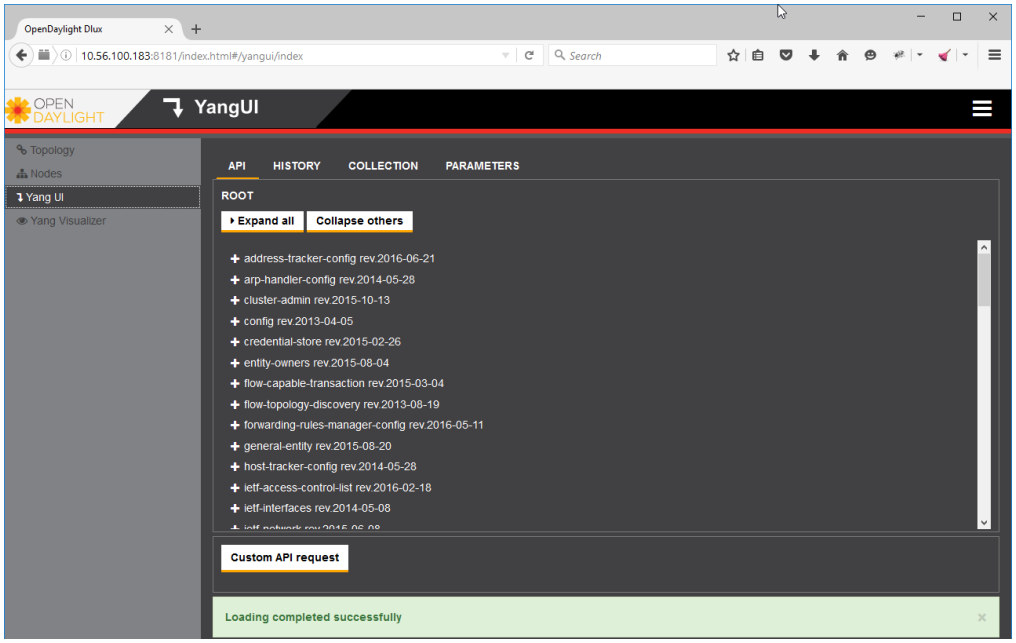
ما NETCONF را بیش از SSH اجرا می‌کنیم.

علاوه بر پروتکل NETCONF از یک زبان مدل‌سازی با نام YANG استفاده می‌کنیم، این زبان مدل‌سازی از یک ساختار سلسله مراتبی استفاده می‌کند و خواندن مطالب را برای انسان آسانتر می‌کند.

برای اینکه زبان YANG بتواند به داده‌ها دسترسی داشته باشد باید از یک رابط API با نام RESTCONF استفاده کنیم.

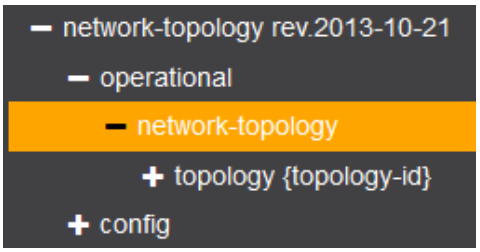
برای دسترسی به YANG می‌توانیم از رابط گرافیکی OpenDayLight استفاده کنیم، برای این کار به مانند شکل ۳۳-۱۴، عمل کنید:

www.takbook.com



شکل ۱۴-۳۳ *OpenDaylight*

همانطور که در شکل ۳۳-۱۴، مشاهده می‌کنید ابزارهای زیادی برای کار وجود دارد، برای تست توپولوژی خود به مانند شکل ۳۴-۱۴، عمل می‌کنیم:



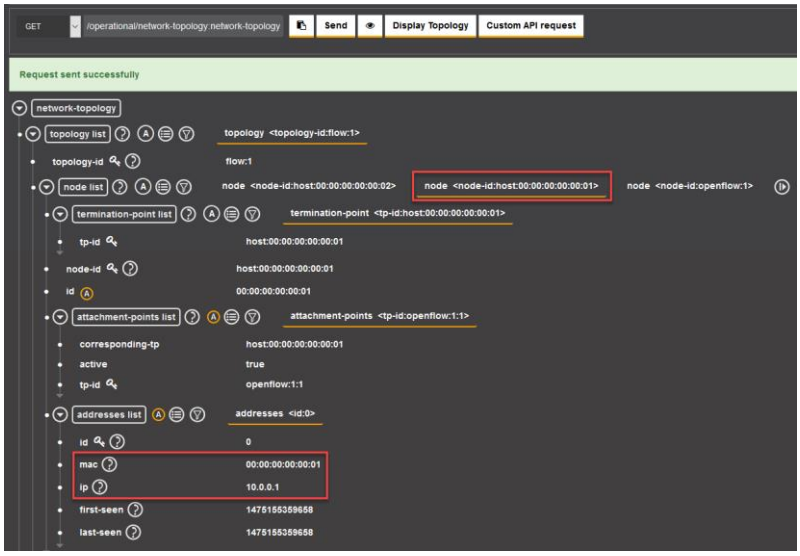
شکل ۱۴-۳۴ *OpenDaylight*

در شکل ۳۵-۱۴، بر روی Send کلیک کنید:

شکل ۱۴-۳۵ *OpenDaylight*

www.takbook.com

بعد از کلیک بر روی Send، توپولوژی شبکه به صورت شکل ۳۶-۱۴، خواهد بود:



شکل ۳۶-۱۴ *OpenDaylight*

در شکل ۳۶-۱۴، می‌توانید اطلاعات مربوط به توپولوژی فعلی ما، از جمله آدرس های MAC و IP میزبان ما را مشاهده کنید.

Postman

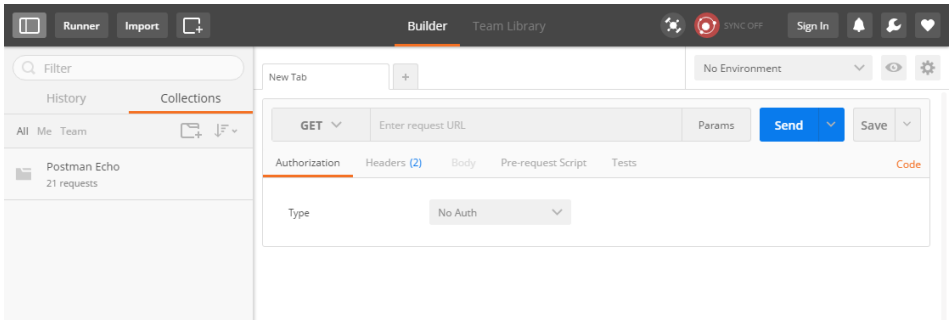
اگر واقعاً بخواهید با RESTCONF API کار کنید ، خیلی مفید نیست، برای جایگزین آن بهتر است از نرم‌افزار Postman برای این کار استفاده کنید که برای دانلود آن می‌توانید از لینک زیر استفاده کنید:

https://www.getpostman.com/

این برنامه به شما این امکان را می‌دهد که با APIها ارتباط برقرار کنید، درخواست‌ها را ذخیره کنید و...

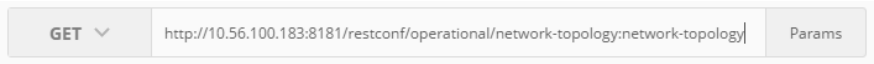
در شکل ۳۷-۱۴، نرم‌افزار Postman را مشاهده می‌کنید:

www.takbook.com



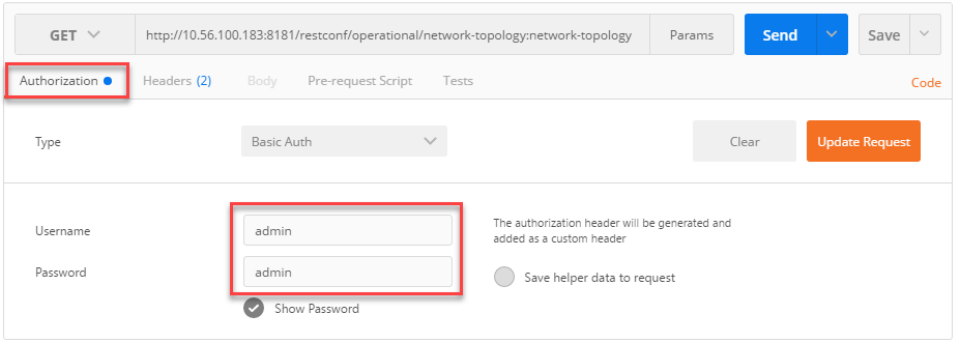
شکل ۱۴-۳۷ *Postman*

آدرسی را که در YANG بدست آوردیم را در این نرم‌افزار هم تست می‌گیریم:



شکل ۱۴-۳۸ *Postman*

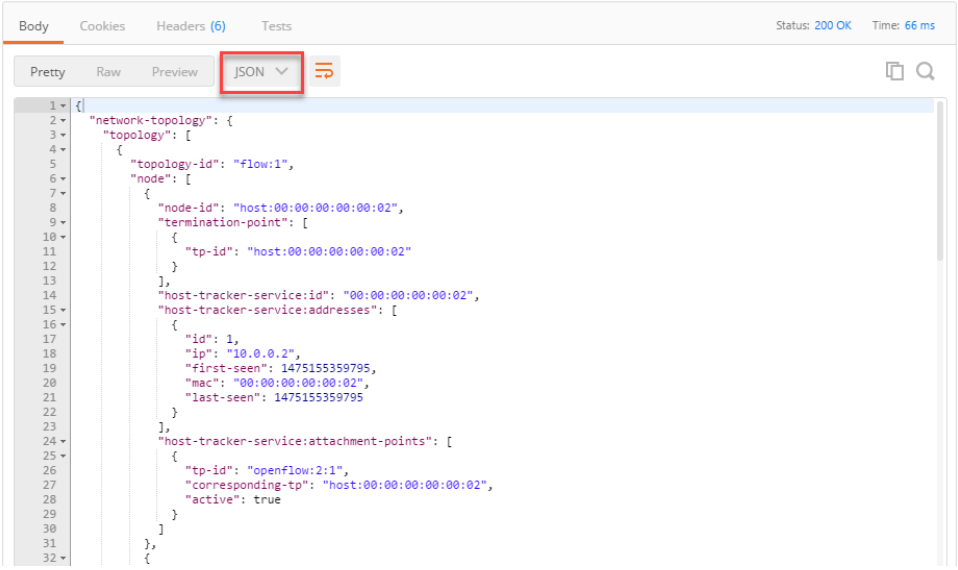
قبل از اینکه بر روی دکمه‌ی Send کلیک کنید باید اعتبارنامه یا همان Certificate برنامه Postman را بر روی سیستم نصب کنید برای این کار باید به مانند شکل ۳۹-۱۴، عمل کنید، توجه داشته باشید که نام کاربری و رمز عبور admin/admin است.



شکل ۱۴-۳۹ *Postman*

به مانند شکل ۴۰-۱۴، بعد از کلیک بر روی دکمه‌ی SEND در قسمت JSON با پاسخ زیر مواجه خواهید شد:

www.takbook.com



شکل ۴۰-۱۴ *Postman*

در شکل ۴۰-۱۴، می‌توانید همان خروجی را ببینید که در Yang UI دیدیم اما این بار ، با فرمت JSON است. یکی از مزایای Postman این است که شما می‌توانید درخواست‌های خود را ذخیره کنید یا مجموعه درخواست‌های دیگران را بارگیری کنید. به عنوان مثال، در اینجا مجموعه‌ای از درخواست‌های OpenDaylight ارائه شده توسط CiscoDevNet را می‌توانید مشاهده کنید:

https://github.com/CiscoDevNet/opendaylight-sample-apps/tree/master/postman-collections

Python

Postman برای همکاری با API بسیار عالی عمل می‌کند، اما یکی از اهداف SDN اتوماسیون شبکه است، برای اینکه بهتر به مسائل پی ببریم یک مثال از پایتون بر روی همان سناریو قبلی که در Postman و Yang UI انجام دادیم، اجرا کنیم.

در زیر کد پایتون را مشاهده می‌کنید که اطلاعات اسکریپت را بازیابی می‌کند و آدرس‌های MAC و IP همه‌ی میزبان‌های شبکه را چاپ می‌کند:

```
import requests

#OpenDayLight RESTCONF API settings.
odl_url =
'http://10.56.100.183:8181/restconf/operational/network-
topology:network-topology'
odl_username = 'admin'
```

www.takbook.com


```
odl_password = 'admin'

# Fetch information from API.
response = requests.get(odl_url, auth=(odl_username,
odl_password))

# Find information about nodes in retrieved JSON file.
for nodes in response.json()['network-topology']['topology']:

    # Walk through all node information.
    node_info = nodes['node']

    # Look for MAC and IP addresses in node information.
    for node in node_info:
        try:
            ip_address = node['host-tracker-
service:addresses'][0]['ip']
            mac_address = node['host-tracker-
service:addresses'][0]['mac']
            print('Found host with MAC address %s and IP
address %s' % (mac_address, ip_address))
        except:
            pass
```

برای اجرای این کد در پایتون باید دستور زیر را در لینوکس وارد کنید:

```
$ python topology_information.py
```

خروجی به صورت زیر خواهد بود:

```
Found host with MAC address 00:00:00:00:00:02 and IP address
10.0.0.2
Found host with MAC address 00:00:00:00:00:01 and IP address
10.0.0.1
```

در این درس آموختم که چگونه کنترلر OpenDaylight و یک شبکه مجازی را با Mininet اجرا کنید. ما همچنین دیده‌ایم که چگونه می‌توانید با استفاده از ابزارهای مختلف مانند یانگ UI ، Postman و اسکریپت پایتون با RESTCONF API کار کنید.

www.takbook.com

۳-۱۴ بررسی Ansible، Puppet و Chef

تا به این قسمت آموختید که چگونه از IOS CLI برای پیکربندی روترها و سوئیچ‌ها استفاده کنید. برای پیکربندی با استفاده از CLI، وارد حالت configuration شوید و دستورات پیکربندی را وارد کنید (دستوری که فایل running-config را تغییر می‌دهد) و در نهایت از حالت پیکربندی خارج شوید.

اگر تصمیم دارید که تغییرات را ذخیره کنید، برای ذخیره تنظیمات در فایل startup-config باید با استفاده از دستور running-config startup-config کار ذخیره را انجام دهید، بعد از آن روتر یا سوئیچ فایل startup-config را به عنوان فایل running-config در RAM بارگذاری می‌کنند.

این فصل در مورد ابزارهایی برای مدیریت پیکربندی (configuration management) دستگاه‌ها بحث می‌کند که فرآیند پیکربندی هر دستگاه را انجام می‌دهد.

در یک شبکه‌ی بزرگ، برای اینکه مدیریت و پیکربندی تمام دستگاه‌های شبکه را انجام دهیم، باید زمانی زیاد را صرف آن بکنیم و این کار می‌تواند مشکلاتی را ایجاد کند. این مشکلات را می‌توان با استفاده از همان فرآیند قدیمی، یعنی استفاده از «حالت پیکربندی در هر دستگاه» به همراه کار پیوسته و پشتکار برطرف کرد. کار در این حالت یعنی به صورت دستی می‌تواند خیلی سخت باشد، بنابراین در بعضی مواقع، شرکت‌ها برای دستیابی به نتایج بهتر، به ابزارهای مدیریت پیکربندی خودکار (automated configuration management)روی می‌آورند.

در بخش اول این فصل، نگاهی کلی به مباحث مربوط به مدیریت پیکربندی می‌پردازیم، به همراه معرفی بعضی از راه‌حل‌های برطرف کردن مشکلات آن، سپس در بخش دوم به جزئیات هر سه ابزار مدیریت پیکربندی یعنی Ansible، Puppet و Chef می‌پردازیم و ویژگی‌های آنها را بررسی می‌کنیم.

در پایان فصل باید بتوانید مشخص کنید که از کدام ابزار مدیریت پیکربندی خودکار در شبکه‌های مدرن استفاده می‌کنید.

چالش‌ها و راه‌حل‌های پیکربندی دستگاه‌های شبکه

به یک شبکه تولیدی فکر کنید. چه کسی می‌تواند پیکربندی دقیق برای هر دستگاه را در یک شبکه مشخص کند؟ آیا اطلاعاتی که در فایل running-config وجود دارد با اطلاعاتی که در گذشته در فایل startup-config وجود دارد یکی است؟ یک نفر مثلاً مهندس شبکه تغییراتی را در فایل پیکربندی دستگاه انجام می‌دهد بدون اینکه کسی از این کار با خبر شود، چگونه می‌توانیم مشخص کنیم که چه کسی در چه زمانی اطلاعات فایل پیکربندی را تغییر داده است و مهمتر از همه چه چیزی تغییر کرده است؟

www.takbook.com

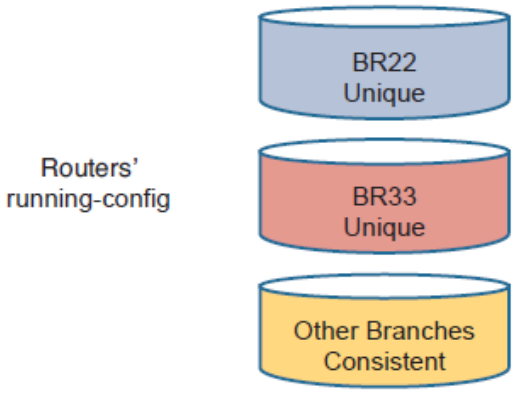
همانطور که در فصل‌های قبل بررسی کردیم در دوره‌ی CCNA آموختیم که چگونه یک دستگاه را با استفاده از دستور Configure Terminal، پیکربندی کنیم، تا بعد از آن فایل running-config تغییر کند و چگونه می‌توان فایل running-config را در فایل startup-config کپی یا ذخیره کرد. شرکت‌هایی که یک مهندس شبکه دارند ممکن است مدیریت تنظیمات دستگاه را به اندازه کافی خوب انجام دهند، به خصوص اگر تنظیمات دستگاه شبکه اغلب تغییر نکند. اما ، هرچه یک شرکت به سمت مهندسان شبکه‌های متعدد حرکت می‌کند و تعداد و تنوع دستگاه‌ها را افزایش می‌دهد ، با افزایش نرخ تغییرات، مدیریت پیکربندی به صورت دستی دارای مشکلاتی می‌شود که می‌تواند یک ضعف بزرگ در آن شرکت باشد.

این بخش در مورد برخی از موارد مدیریت پیکربندی بحث می‌کند تا بدین ترتیب درک کنید که چرا شرکت‌ها برای سروکار داشتن با پیکربندی دستگاه‌ها، به افرادی که با تجربه باشند و شیوه‌های خوب را به کار بگیرند، احتیاج دارند. در ادامه کار، بخش دیگری از ویژگی‌هایی را که می توانید در ابزارهای مدیریت پیکربندی خودکار پیدا کنید، به تفصیل بیان می‌کنیم.

۱-۳-۱۴ افت عملکرد پیکربندی (configuration drift)

یک شرکت بزرگ را در نظر بگیرد، که به دو مهندس شبکه، آرین و آریانا، نیاز دارد. آنها هر دو تجربه و همکاری خوبی با هم دارند. اما پیکربندی شبکه فراتر از چیزی است که هر شخص بتواند از حافظه خود استفاده کند و با وجود دو مهندس شبکه ، ممکن است جزئیات مختلفی را به خاطر نسپارند یا حتی در مواردی اختلاف نظر داشته باشند. مثلاً یکی از شب‌ها آریانا در مورد یک مشکل در شبکه‌ی سازمان، تماسی دریافت می‌کند. او از طریق لپ‌تاپ خود وارد شبکه شده و با تغییری که در پیکربندی روتر شعبه BR22 انجام می‌دهد، مشکل را برطرف می‌کند. آرین، مهندس‌ارشد، درمورد مشکل دیگری در ساعت ۴ بامداد تماسی دریافت می‌کند و تنظیمات مربوط به روتر شعبه BR33 را تغییر می‌دهد. روز بعد آنقدر سرشان شلوغ می‌شود می‌شود که نه آرین و نه آریانا از تغییراتی که ایجاد کرده‌اند هیچ اطلاعی نمی‌دهند. آن‌ها تغییرات در سیستم مدیریت تغییر خود مستند می‌کنند که جزئیات هرگونه تغییر را به صورت لیست نشان می‌دهد، اما کارشان زیاد شده و سرشان شلوغ می‌شود و این موضوع هرگز مطرح نمی‌شود و هیچ یک از آنها برای ماه‌ها تغییرات را ذکر نمی‌کنند. این داستان نشان می‌دهد که چگونه افت عملکرد پیکربندی رخ می‌دهد (configuration drift)، شکل ۴۱-۱۴، ایده اصلی را نشان می‌دهد، دو روتر فعلی با پیکربندی کمی متفاوت از روترهای شاخه دیگر مشخص شده است.

www.takbook.com



شکل ۴۱-۱۴ عملکرد پیکربندی

اگر فقط از ابزارهای سنتی پیکربندی دستی استفاده کنید، افت عملکرد پیکربندی به یک مشکل بسیار بزرگتر تبدیل می‌شود.

به عنوان مثال:

- فرآیند پیکربندی دستی روی دستگاه، تاریخچه تغییرات را دنبال نمی‌کند: مثلاً کدام خطوط تغییر کرده است، چه چیزی در هر خط تغییر کرده، چه پیکربندی قدیمی حذف شده یا اینکه چه کسی پیکربندی را تغییر داده است.
- سیستم‌های خارجی استفاده شده، توسط فرآیندهای مدیریت سیستم‌های خوب ، مانند نرم‌افزاراهای فروش بلیط و نرم افزار مدیریت تغییر ، ممکن است جزئیات کار را ثبت کنند. در حالی که آنهایی که خارج از پیکربندی قرار گرفته‌اند برای آنکه بفهمند چه چیزی تغییر کرده است، نیاز به تجزیه و تحلیل دارند. آنها همچنین به یک نیروی انسانی متکی هستند که به طور مداوم و صحیح روندهای عملیاتی را دنبال کند. در غیر این صورت ، یک مهندس نمی تواند کل تاریخچه تغییرات در یک پیکربندی را پیدا کند.
- مراجعه به داده های تاریخی در سیستم‌های مدیریت تغییر، اگر دستگاه در طی یک دوره زمانی تغییراتی را انجام داده باشد ، ضعیف عمل می‌کند.

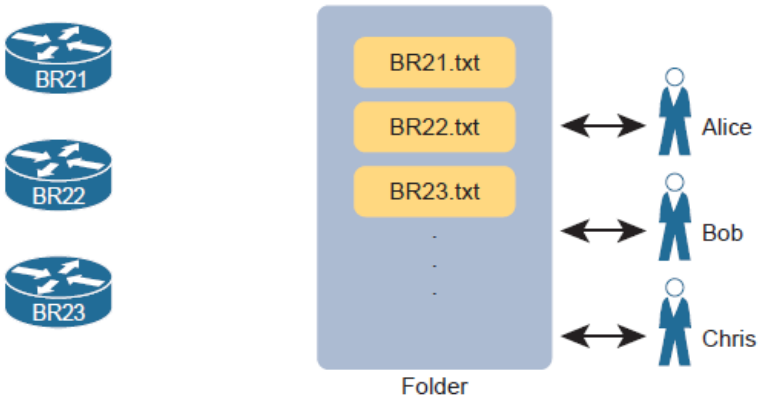
۲-۳-۱۴ فایلهای پیکربندی متمرکز و کنترل نسخه

مدل پیکربندی دستی برای یک نفر که یک دستگاه را مدیریت می‌کند، حس بسیار خوبی دارد. با استفاده از آن مدل، یک مهندس شبکه می‌تواند از پیکربندی startup-config به عنوان پیکربندی ایده‌آل استفاده کند. در صورتی که نیاز به تغییر باشد، مهندس شبکه وارد حالت پیکربندی شده و فایل running-config را به

www.takbook.com

روز می‌کند. سپس مهندس این تغییرات را در فایل startup-config ذخیره می‌کند و این تغییرات رابه عنوان پیکربندی ایده‌آل قبول دارد. مدل پیکربندی دستی برای هر دستگاه، و در شبکه‌های بزرگتر، با صدها یا حتی هزاران دستگاه شبکه، یا با چند مهندس شبکه کارایی ندارد. به عنوان مثال ، اگر یک تیم تنظیمات راه‌اندازی هر دستگاه را به عنوان تنظیم ایده‌آل می‌داند، اگر یکی از اعضای تیم، پیکربندی را تغییر دهد (مثل آرین و آریانا که در داستان قبلی برسری کردیم)، در این صورت هیچ سابقه‌ای در مورد تغییر وجود نخواهد داشت که این یک مشکل بزرگ خواهد بود.

در فایل پیکربندی نمی‌توانید مشخص کنید که چه چیزی تغییر کرده است، در چه زمانی، یا چه کسی آن را تغییر داده است و این روند در مورد تغییر به کل تیم اطلاع داده نمی‌شود. اولین قدم برای مدیریت بهتر پیکربندی، این است که بسیاری از شرکت‌های متوسط و بزرگ پیکربندی‌ها را در یک مکان مرکزی ذخیره کنند. در ابتدا، ممکن است ذخیره کردن پرونده‌ها به صورت مرکزی یک کار ساده برای نگه داشتن نسخه‌های پشتیبان از پیکربندی هر دستگاه است. آنها مطمئناً پرونده‌ها را در یک پوشه مشترک قرار می‌دهند که برای کل تیم شبکه قابل دسترسی باشد، که در شکل ۴۲-۱۴، این موضوع را مشاهده می‌کنید.



شکل ۴۲-۱۴ عملکرد پیکربندی

کدام یک از فایل‌های بالا منبع اصلی تنظیمات دستگاه‌ها در شبکه است؟ فایل‌های پیکربندی هنوز در هر دستگاه وجود دارند، اما در حال حاضر در یک سرور مرکزی ذخیره شده‌اند و مهندسان می‌توانند پیکربندی دستگاه و همچنین فایل‌های متنی موجود در سرور را تغییر دهند. به عنوان مثال ، اگر نسخه پیکربندی BR21 در دستگاه با فایل موجود در سرور متفاوت باشد ، کدام نسخه باید به عنوان تنظیم ایده‌آل که تیم هم بر روی آن نظر دارد برای این دستگاه در نظرگرفته شود؟

در عمل، شرکت‌ها هر دو رویکرد را اتخاذ می‌کنند، در برخی موارد، شرکت‌ها همچنان از فایل‌های پیکربندی موجود در دستگاه به عنوان منبع اصلی استفاده می‌کنند ، در صورتی که دستگاهی از کار بیفتد باید پرونده‌ی دیگر جایگزین آن شود، فایل‌های پیکربندی در سرور اصلی به عنوان نسخه پشتیبان استفاده

www.takbook.com

می‌شوند. مهندسان می‌توانند هنگام استفاده از فایل متمرکز به عنوان منبع اصلی، از بسیاری از ابزارهای مدیریت پیکربندی استفاده کنند و در واقع پیکربندی‌ها را راحت تر و با دقت بیشتری مدیریت کنند.

به عنوان مثال، ابزارهای مدیریت پیکربندی، از نرم افزار کنترل نسخه استفاده می‌کنند تا تغییرات در فایل‌های پیکربندی در سرور متمرکز را ردیابی کنند، و مشخص کنند، چه کسی یک پرونده را تغییر داده، چه خطها و کاراکترهای خاصی تغییر کرده است، چه زمانی این تغییر رخ داده است و غیره. ابزارها همچنین به شما این امکان را می‌دهند که اختلافات بین نسخه‌های مختلف پرونده‌ها را با گذشت زمان مقایسه کنید، همانطور که در شکل ۴۳-۱۴، نشان داده شده است.

شکل ۴۳-۱۴ ابزار مدیریت پیکربندی

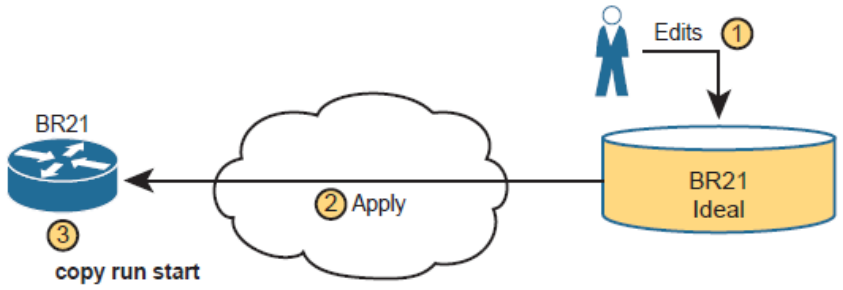
شکل ۴۳-۱۴، نمونه‌ای از مقایسه بین دو نسخه از یک فایل پیکربندی را نشان می‌دهد. دو خط برجسته بالا با علائم منفی، خطوط تغییر یافته را نشان می‌دهند در حالی که دو خط برجسته پایین با علائم مثبت، نسخه‌های جدید هر خط را نشان می دهند. نرم افزار کنترل نسخه، بسیاری از مشکلات عدم‌ردیابی تغییر در خود دستگاه‌ها را برطرف می‌کند. شکل ۴۳-۱۴، خروجی است از سایت محبوب (GitHub (www.github.com)) . GitHub حساب‌های رایگان و پولی ارائه می دهد و از نرم‌افزار منبع باز (Git) برای انجام توابع کنترل نسخه استفاده می‌کند.

۳-۳-۱۴ نظارت بر پیکربندی و اجرا

با یک سیستم کنترل نسخه در یک مکان مرکزی یا یک سرور مرکزی، یک تیم شبکه می‌تواند کار بهتری را برای ردیابی تغییرات و پاسخ دادن به اینکه چه کسی و در چه زبانی چه چیزی را تغییر داده است بدهد.

www.takbook.com

با این حال، استفاده از آن مدل ، چالش‌های دیگری را ارائه می دهد که می‌توان با استفاده از یک ابزار مدیریت پیکربندی خودکار، بهترین راه حل را ارائه داد. با استفاده از این مدل جدید، مهندسان باید با ویرایش فایل‌های پیکربندی، مرتبط در مکان ذخیره مرکزی، تغییراتی ایجاد کنند. سپس ابزار مدیریت پیکربندی می‌تواند همانطور که در شکل ۴۴-۱۴، نشان داده شده است، جهت کپی یا اعمال پیکربندی در دستگاه هدایت شود. پس از اتمام این روند، فایل پیکربندی مرکزی و پیکربندی Running-Config (و Startup-Config) باید یکسان باشند.



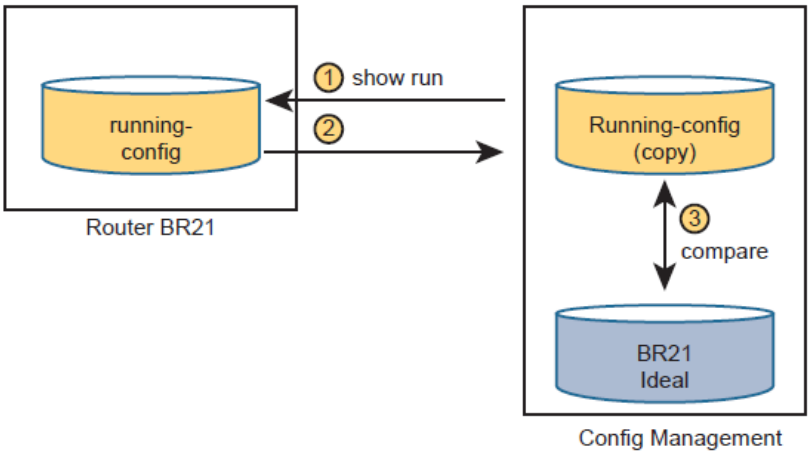
شکل ۴۴-۱۴ ابزار مدیریت پیکربندی

استفاده از مدلی که در شکل ۴۴-۱۴، نشان داده شده است، هنوز خطراتی دارد. به عنوان مثال، مهندسان شبکه باید با استفاده از ابزارهای مدیریت پیکربندی، تغییراتی ایجاد کنند، اما آنها هنوز هم توانایی ورود به هر دستگاه و ایجاد تغییرات دستی در هر دستگاه را دارند. بنابراین، در حالی که ایده استفاده از ابزار مدیریت پیکربندی با مکان ذخیره متمرکز، جذاب به نظر می‌رسد، در نهایت کسی مستقیماً به دستگاه دسترسی داردو تنظیماترا تغییر می‌دهد که این کار جالب نخواهد بود. تغییرات پیکربندی صحیحی که قبلاً انجام شده ممکن است با تغییرات بعدی اشتباه شوند. به عبارت دیگر، سرانجام، ممکن است افت عملکرد پیکربندی که در قسمت قبل توضیح دادیم رخ دهد.

ابزارهای مدیریت پیکربندی می‌توانند تنظیمات دستگاه را کنترل کنند تا تشخیص دهند که پیکربندی دستگاه با پیکربندی ایده‌آل مورد نظر تفاوت دارد یا نه، و سپس دستگاه را پیکربندی مجدد کنند یا به کارکنان مهندسی شبکه اطلاع دهند تا این تغییرات را انجام دهند. این ویژگی ممکن است به عنوان نظارت بر پیکربندی یا اجرای پیکربندی نامیده شود ، به ویژه اگر ابزارها به طور خودکار پیکربندی دستگاه را تغییر دهند.

شکل ۴۵-۱۴، ایده‌ی کلی در مورد نظارت بر پیکربندی را نشان می‌دهد. نرم‌افزار مدیریت پیکربندی خودکار یک نسخه از پیکربندی در حال اجرا دستگاه را درخواست می‌کند، همانطور که در مراحل ۱ و ۲ نشان داده شده است. آنها اختلافاتی دارند (افت عملکرد پیکربندی). در هر پیکربندی، ابزار این پیکربندی را اصلاح می‌کند یا در مورد افت عملکرد پیکربندی به کارکنان اطلاع می‌دهد.

www.takbook.com



شکل ۴۵-۱۴ ابزار مدیریت پیکربندی

۴-۳-۱۴ الگوهای پیکربندی و متغیرها

به وظایف دستگاه‌های شبکه در یک سازمان، فکر کنید. با تمرکز بر روی روترها، که اغلب هم به WAN و هم به یک یا چند شبکه محلی LAN وصل می‌شوند، سایت‌های کوچکتر، مانند شعب یک اداره، ممکن است دارای روترهای کوچکی باشند که شاید با یک رابط WAN و یک رابط شبکه LAN کار کنند. با این وجود، شما ممکن است تعداد زیادی از آن روترها در شبکه داشته باشید.

برای هر مجموعه‌ای از دستگاه‌هایی که در یک سازمان فعال هستند، اصولاً تنظیمات مشابه‌هی بر روی آن‌ها قرار گرفته است. به عنوان مثال ، مجموعه‌ای از روترهای دفاتر یک شعبه ممکن است تنظیمات یکسانی برای برخی از خدمات IP مانند NTP یا SNMP داشته باشند. در صورت استفاده از پیکربندی OSPF Interface، روترها در همان منطقه OSPF و با شناسه Interface یکسان می‌توانند پیکربندی OSPF یکسانی هم داشته باشند.

مثال:

مثال زیر گزیده‌ای از پیکربندی یک روتر را نشان می‌دهد که قسمت‌های مشخص شده‌ی پیکربندی آن برجسته شده است. تمام بخش‌های دیگر که برجسته نشده است، می‌تواند در تمام روترهای شعبه دیگر از همان مدل (با همان شماره Interface) یکسان باشد. یک شرکت ممکن است ده‌ها یا صدها روتر در شعبه‌های مختلف با پیکربندی تقریباً یکسان داشته باشد.

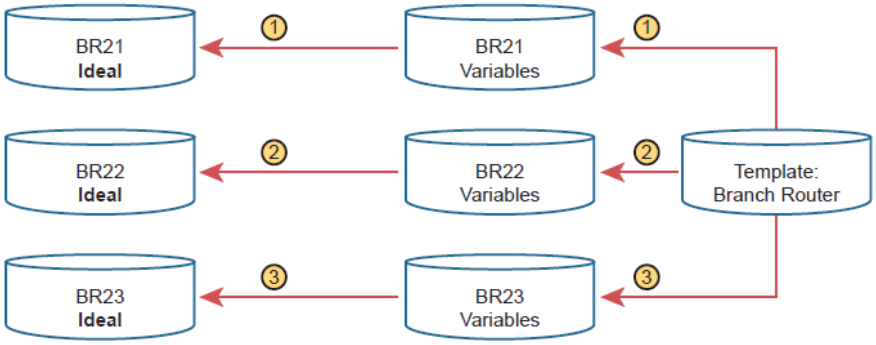
hostname **BR1**

www.takbook.com


```
!
interface GigabitEthernet0/0
ip address 10.1.1.1 255.255.255.0
ip ospf 1 area 11
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/1/0
ip address 10.1.12.1 255.255.255.0
ip ospf 1 area 11
!
router ospf 1
router-id 1.1.1.1
```

ابزارهای مدیریت پیکربندی می‌توانند اجزای یک پیکربندی را به قسمت‌های مشترک برای کلیه دستگاههای موجود در آن نقش (template) در مقابل قطعات منحصر به فرد برای هر یک از دستگاه‌ها (متغیرها) جدا کنند. مهندسین می‌توانند فایل template استاندارد را برای نقش دستگاه به عنوان یک فایل جداگانه از فایل متغیر هر دستگاه ویرایش کنند. سپس ابزار مدیریت پیکربندی می‌تواند قالب (template) و متغیرها را پردازش کند تا فایل پیکربندی ایده‌آل برای هر دستگاه ایجاد شود، همانطور که در شکل ۴۶-۱۴، نشان داده شده است، پرونده‌های پیکربندی برای روترهای شعبه BR21، BR22 و BR23 ساخته شده‌اند.

www.takbook.com



شکل ۴۶-۱۴ پرونده‌های پیکربندی

برای توضیح بیشتر شکل ۴۶-۱۴، یک فایل الگویی را نشان می‌دهد که می‌تواند توسط Ansible برای پیکربندی نشان داده شده در مثال قبلی استفاده شود. هر ابزار، مشخص می‌کند که برای هر نوع پرونده چه زبانی را باید مورد استفاده قرار دهیم، که در اینجا می‌توان از زبان Jinja2 برای نمونه‌ها استفاده کرد. این الگو از پیکربندی در مثال قبل تقلید می‌کند ، بجز قرار دادن نام‌های متغیر در داخل دسته های براکت‌های دوگانه، به زبان ساده‌تر فقط جاهایی تغییر می‌کند که در زیر مشخص شده‌اند.

```
hostname {{hostname}}

!

interface GigabitEthernet0/0

ip address {{address1}} {{mask1}}

ip ospf {{OSPF_PID}} area {{area}}

!

interface GigabitEthernet0/1

!

interface GigabitEthernet0/1/0

ip address {{address2}} {{mask2}}

ip ospf {{OSPF_PID}} area {{area}}

!
```

www.takbook.com


```
router ospf {{OSPF_PID}}

router-id {{RID}}
```

برای تهیه مقادیر برای یک دستگاه، Ansible خواستار تعریف فایل‌های متغیر با استفاده از YAML است، همانطور که در مثال زیر نشان داده شده است، به جای کلماتی که در بالا مشخص کردیم، متغیرهای زیر قرار می‌گیرند، مثلاً به جای hostname نام BR1 قرار می‌گیرد.

```
---

hostname: BR1

address1: 10.1.1.1

mask1: 255.255.255.0

address2: 10.1.12.1

mask2: 255.255.255.0

RID: 1.1.1.1

area: '11'

OSPF_PID: '1'
```

به نظر می رسد جداسازی پیکربندی‌ها در یک فایل templates و متغیر کار اضافی باشد، اما استفاده از templatesها مزایای بزرگی دارد. به طور خاص:

- نمونه‌ها تمرکز خود را برای داشتن تنظیمات استاندارد برای هر نقش دستگاه افزایش می‌دهند و به جلوگیری از تمرکز پوسته (دستگاه‌های پیکربندی شده منحصر به فرد) کمک می‌کنند.
- دستگاه‌های جدید می‌توانند به سادگی و با کپی کردن یک فایل متغیر در هر دستگاه و تغییر مقادیرآن، با نقش موجود سازگار و مستقر شوند.
- نمونه‌ها امکان عیب‌یابی آسان‌تر را دارند زیرا مشکلات عیب‌یابی با یک الگوی (templates) استاندارد باید مشکلات مربوط به همه دستگاه‌هایی که از همان الگو استفاده می‌کنند را پیدا کرده و برطرف کنند.
- ردیابی نسخه‌های فایل برای نمونه در مقابل فایل‌های متغیر، امکان عیب‌یابی آسان را نیز فراهم می‌کند. برای یافتن تغییرات در تنظیمات دستگاه به طور جداگانه از الگوی استاندارد پیکربندی استاندارد ، می‌توان مشکلات مربوط به یک دستگاه را بررسی کرد.

www.takbook.com

۱۴-۳-۵ ANSIBLE, PUPPET, AND CHEF BASICS

این فصل به موضوع آزمون و تست می پردازد و قابلیت‌های سه ابزار مدیریت پیکربندی را بررسی می‌کند:

- Ansible
- Puppet
- Chef

بخش اصلی این فصل توانایی‌های هر سه ابزار مدیریت پیکربندی را شرح می‌دهد. بخش دوم با تمرکز بر اصطلاحات و قابلیت‌های مهم آنها، به بررسی برخی از ویژگی‌های هر ابزار می‌پردازد.

Ansible، Puppet و Chef بسته‌های نرم افزاری هستند. شما می‌توانید این سه بسته‌ی نرم‌افزاری را خریداری کنید. با این وجود، همه آنها گزینه‌های رایگان مختلفی هم دارند که به شما امکان می‌دهد که آنها را دانلود کرده و در مورد این ابزارها تست و آزمایش کنید، گرچه ممکن است نیاز به اجرای یک سیستم عامل Linux داشته باشید، زیرا برخی از ابزارها در سیستم‌عامل ویندوز اجرا نمی شوند.

۱۴-۳-۵-۱ Ansible

برای استفاده از Ansible (www.ansible.com)، باید Ansible را روی برخی از رایانه‌ها نصب کنید: Mac، Linux یا Linux VMv که در یک هاست ویندوز از طریق نرم‌افزارهای مجازی‌سازی اجرا می‌شود. شما می‌توانید از نسخه رایگان منبع آزاد استفاده کنید یا از نسخه سرور قابل پرداخت Tower Ansible استفاده کنید. پس از نصب ، چندین فایل متنی مانند موارد زیر ایجاد می‌شود:

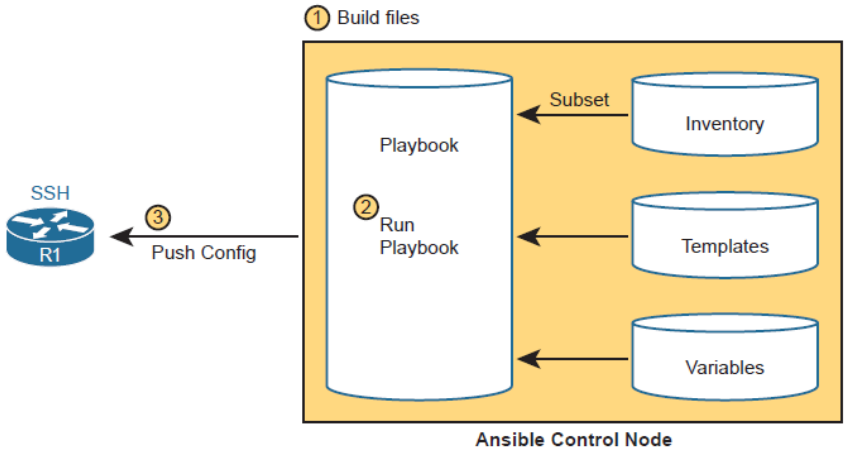
- Playbooks: این پرونده‌ها اقدامات و منطق‌هایی را در مورد کارهایی که Ansible باید انجام دهد فراهم می‌کند.
- Inventory: این پرونده‌ها نام دستگاه را به همراه اطلاعات مربوط به هر دستگاه، مانند نقش دستگاه، ارائه می‌دهند.
- Templates: با استفاده از زبان Jinja2 ، نمونه‌ها، پیکربندی دستگاه را با متغیرها نشان می‌دهند.
- Variables: با استفاده از YAML که یک زبان برای طبقه‌بندی داده برای قابل خواندن کردن برای انسان است و بیشتر برای فایل‌های پیکربندی مورد استفاده قرار می‌گیرد، این فایل می‌تواند متغیرهایی را که Ansible در نمونه‌ها جایگزین می‌کند، لیست کند.
- Static or Local: در این حالت هاست‌ها درون فایل //etc//ansible//hosts قرار می‌گیرند.

از آنجا که Ansible برای مدیریت دستگاه‌های شبکه به کار می‌رود، از یک معماری agentless (بدون عامل) استفاده می‌کند. این بدان معناست که Ansible به هیچ عاملی (agent) در حال اجرا بر روی دستگاه

www.takbook.com

در شبکه اعتماد ندارد. در عوض، Ansible برای ایجاد تغییرات و استخراج اطلاعات در دستگاههای شبکه، به پروتکل SSH و یا NETCONF متکی است.

Ansible بر پایه زبان پایتون ساخته شده و از فرمت YAML که یک زبان پیکربندی ساده هست استفاده می‌کند، یادگیری این زبان برنامه‌نویسی بسیار آسان است.



شکل ۱۴-۴۷ Ansible

Ansible می‌تواند هم تنظیمات پیکربندی را انجام دهد (پیکربندی دستگاه‌ها پس از ایجاد تغییرات در پرونده‌ها) و هم نظارت بر پیکربندی(در اقع بررسی برای یافتن اینکه آیا پیکربندی دستگاه مطابق با پیکربندی ایده‌آل در گره کنترل است یا خیر). با این حال، همان‌طور که در شکل ۱۴-۴۷؛ مشاهده می‌شود معماری Ansible به طور طبیعی متناسب با تهیه تنظیمات است. برای انجام نظارت بر پیکربندی، Ansible از ماژول‌های منطقی استفاده می‌کند که تفاوت پیکربندی‌ها را تشخیص داده و لیست می‌کند، پس از آن راه‌کاری مشخص می‌کند که چه اقدامی انجام شود (پیکربندی یا اطلاع رسانی).

توجه داشته باشید بحث Ansible بسیار گسترده است و کتاب‌های زیادی برای این موضوع به نگارش در آمده است که می‌توانید آنها را مطالعه کنید.

۱۴-۳-۵-۲ Puppet

استفاده از Puppet (www.puppet.com) ، مانند Ansible، با نصب Puppet روی لینوکس شروع می‌شود. شما می‌توانید آن را، روی هاست لینوکس خود نصب کنید، اما برای اهداف تولید، به طور معمول آن را روی یک سرور لینوکس بنام Master Puppet نصب خواهید کرد. مانند Ansible، می‌توانید از نسخه رایگان منبع آزاد با نسخه‌های پولی موجود آن استفاده کنید. شما می‌توانید یادگیری Puppet را بدون یک سرور جداگانه برای یادگیری و آزمایش شروع کنید.

www.takbook.com

پس از نصب، Puppet از چندین فایل متنی مهم با مؤلفه‌های مختلف مانند موارد زیر استفاده می‌کند:

Manifest: این یک فایل متنی قابل خواندن توسط انسان در Puppet است، با استفاده از زبانی که توسط Puppet تعریف شده است، برای تعریف وضعیت پیکربندی ایده‌آل یک دستگاه استفاده می‌شود.

Resource, Class, Module: این اصطلاحات به مؤلفه‌های Manifest اشاره دارد که بزرگترین مؤلفه (ماژول) از کلاس‌های کوچکتر تشکیل شده است، که به نوبه خود از منابع تشکیل شده‌اند.

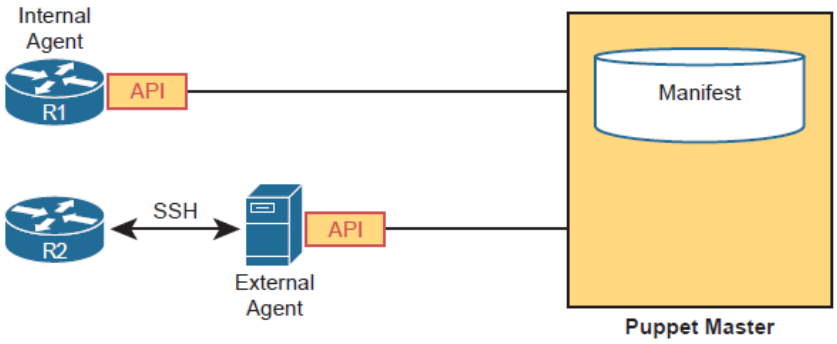
Templates: با استفاده از یک زبان domain-specific Puppet، این پرونده‌ها به Puppet اجازه می‌دهند با جایگزین کردن متغیرها در نمونه، Manifests (و ماژول‌ها ، کلاس‌ها و منابع) را تولید کند.

یک راه برای فکر کردن در مورد تفاوت بین رویکرد Ansible در مقابل رویکرد Puppet این است که راه کارهای Ansible از یک زبان ضروری استفاده می‌کنند ، در حالی که Puppet از یک زبان اعلانی استفاده می‌کند.

به عنوان مثال، Ansible، لیست وظایف و گزینه‌های مبتنی بر نتایج را انجام می‌دهد، مانند "پیکربندی تمام روترهای شعبه در یک مکان و در صورت بروز خطا، کارهای اضافی را برای آن دستگاه انجام می‌دهد." در عوض، Manifest **برای** Puppet باید وضعیت نهایی را که یک دستگاه دارد را اعلام کند، Manifest که توسط مهندس ساخته شده است، وضعیت نهایی را تعریف می‌کند و Puppet وظیفه دارد که بدون نیاز به مجموعه مشخصی از مراحل انجام شده، این پیکربندی را برای دستگاه ایجاد کند.

Puppet معمولاً برای پشتیبانی از دستگاه شبکه از یک معماری مبتنی بر Agent استفاده می‌کند. برخی از دستگاه‌های شبکه پشتیبانی از Puppet را از طریق یک Agent انجام می‌دهند. با این حال، هر سیستم‌عامل Cisco از عوامل Puppet پشتیبانی نمی‌کند ، بنابراین Puppet با استفاده از یک عامل پروکسی که بر روی میزبان خارجی اجرا می‌شود، این مشکل را حل می‌کند (به نام عملیات بدون Agent). سپس عامل خارجی از SSH برای ارتباط با دستگاه شبکه استفاده می‌کند ، این موضوع را می‌توانید در شکل ۴۸-۱۴ مشاهده کنید.

www.takbook.com



شکل ۴۸-۱۴ *Puppet*

در هر وب‌سایت Puppet، Puppet هم از یک معماری بدون Agent پشتیبانی می‌کند و هم اینکه معماری بدون Agent مورد استفاده از یک عامل خارجی در دستگاه شبکه است، همانطور که در قسمت پایین شکل ۱۴–۴۸ نشان داده شده است.

زمانی که به manifest مجهز باشد، جمله‌ای مانند "این دستگاه باید از حالت پیکربندی استفاده کند" را اعلام می‌کند، Puppet از یک مدل کشش (pull) استفاده می‌کند تا این تنظیمات در دستگاه ظاهر شود، همانطور که در شکل ۴۹–۱۴، نشان داده شده است، پس از نصب، این مراحل انجام می‌شود:

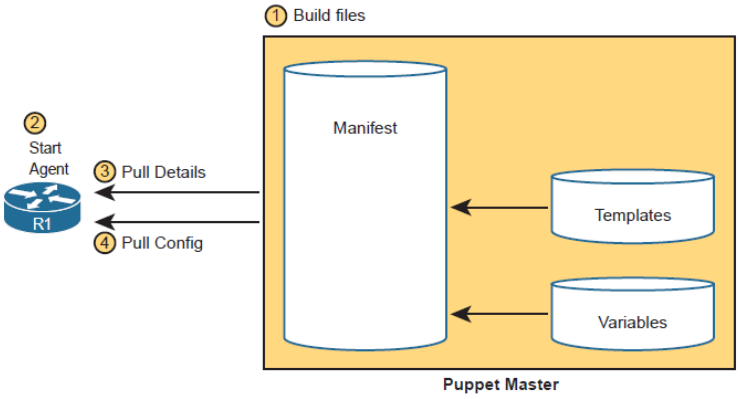
مرحله ۱. مهندس تمام پرونده‌ها را در سرور Puppet ایجاد و ویرایش می‌کند.

مرحله ۲. مهندس agent یا Proxy agent را برای هر دستگاه تنظیم و فعال می‌کند.

مرحله ۳. Agent جزئیات سرور را از طریق Manifest دریافت می‌کند، که به عامل می‌گوید پیکربندی باید همانی باشد که خودش می‌گوید.

مرحله ۴. اگر پیکربندی دستگاه Agent باید به روز شود ، نماینده Puppet برای به دست آوردن همه جزئیات مورد نیاز ، کارهای اضافی را انجام می‌دهد ، یا این که عامل پیکربندی دستگاه را به روز می‌کند.

www.takbook.com



شکل ۱۴-۴۹ *Puppet*

۱۴-۳-۵-۳ Chef

Chef، (www.chef.io)، همانند Ansible و Puppet ، به عنوان بسته‌های نرم افزاری ارائه شده است و می‌توانید آن را دانلود و استفاده کنید. Chef کالاهای مختلفی را ارائه می‌دهد که Chef Automate محصولی است که بیشتر مردم به آن به عنوان Chef اشاره می‌کنند. مانند Puppet، Chef را به عنوان سرور (به نام حالت سرور-مشتری) اجرا می‌کنیم.

پس از نصب Chef، چندین فایل متنی با اجزای مختلف مانند موارد زیر ایجاد می‌شود:

Resource: اشیاء پیکربندی که وضعیت آنها توسط Chef مدیریت می‌شود. به عنوان مثال، مجموعه‌ای از دستورات پیکربندی برای دستگاه شبکه.

Recipe: منطق Chef روی منابع اعمال می‌شود تا تعیین کنند که چه موقع، چگونه و چطور باید در برابر منابع عمل کنند.

Runlist: لیست مرتب شده‌ای از دستور العمل‌هایی که باید در برابر یک دستگاه خاص اجرا شوند، در نظر داشته باشید که Chef از معماری مشابه Puppet استفاده می‌کند. برای دستگاه‌های شبکه، در هر دستگاه مدیریت شده عامل را اجرا می‌کند.

عامل نظارت بر پیکربندی را به این منظور انجام می دهد که مشتری، دستورالعملها و منابع را از سرور Chef گرفته و سپس پیکربندی خود را تنظیم می‌کند تا در هنگام همگام‌سازی با جزئیات موجود در آن دستورالعمل‌ها و لیست‌های دیگر، همگام شود.

www.takbook.com

البته توجه داشته باشید که Chef نیاز به کد مشتری Chef دارد و بسیاری از دستگاه‌های Cisco از مشتری Chef پشتیبانی نمی‌کنند، بنابراین به احتمال زیاد شاهد استفاده بیشتر از Ansible و Puppet برای مدیریت پیکربندی دستگاه Cisco خواهید بود.

خلاصه ابزارهای مدیریت پیکربندی

هر سه ابزار مدیریت پیکربندی که در اینجا ذکر شده است ، از پایگاه خوبی از کاربران و نقاط قوت متفاوتی برخوردار هستند. در مورد استفاده از آنها برای مدیریت پیکربندی دستگاه شبکه، به نظر می‌رسد Ansible بیشترین استفاده و علاقه‌مندی را داشته باشد، بعد از آن هم Puppet و Chef بیشترین استفاده را بین کاربران دارند. معماری بی‌نظیر و استفاده از SSH ، طیف گسترده‌ای از دستگاه‌های Cisco را پشتیبانی می‌کنند. مدل بی‌سیم Puppet همچنین پشتیبانی گسترده‌ای را برای دستگاه های Cisco ایجاد می‌کند. جدول ۱۴-۲، تعدادی از رایج‌ترین ایده ها در مورد هر یک از سه ابزار مدیریت پیکربندی خودکار را مشخص کرده است. توجه داشته باشید که ستون Puppet یک عامل دستگاه را فرض می‌کند.

جدول ۲-۱۴ تفاوت سه ابزار

Action	Ansible	Puppet	Chef
Term for the file that lists actions	Playbook	Manifest	Recipe, Runlist
Protocol to network device	SSH, NETCONF	HTTP (REST)	HTTP (REST)
Uses agent or agentless model	Agentless	Agent*	Agent
Push or pull model	Push	Pull	Pull

۵-۱۴ سوالات فصل چهاردهم

1. A Layer 2 switch examines a frame's destination MAC address and chooses to forward that frame out port G0/1 only. That action occurs as part of which plane of the switch?

سوئیچ Layer 2، آدرس MAC مقصد را بررسی می‌کند و تصمیم می‌گیرد که آن Frame را فقط از پورت G0 / 1 عبور دهد. این عمل در کدام Plane از سوئیچ اتفاق می‌افتد؟

a. Data plane

www.takbook.com

b. Management plane
c. Control plane
d. Table plane

2. A router uses OSPF to learn routes and adds those to the IPv4 routing table. That action occurs as part of which plane of the switch?

روتر از OSPF برای یادگیری مسیرها استفاده می‌کند و آن‌ها را به جدول مسیریابی IPv4 اضافه می‌کند. این عمل به عنوان در کدام Plane از سوئیچ اتفاق می‌افتد؟

a. Data plane
b. Management plane
c. Control plane
d. Table plane

3. A network uses an SDN architecture with switches and a centralized controller. Which of the following terms describes a function or functions expected to be found on the switches but not on the controller?

یک شبکه از یک معماری SDN با سوئیچ ها و یک کنترلر متمرکز استفاده می‌کند. کدام یک از اصطلاحات زیر یک عملکرد یا کارکردهایی را که انتظار می‌رود در سوئیچ‌ها پیدا شوند نشان می‌دهد اما روی کنترلر نیست؟

a. A northbound interface
b. A southbound interface
c. Data plane functions
d. Control plane functions

4. Which of the following controllers (if any) uses a mostly centralized control plane model?

کدام یک از کنترل کننده‌های زیر (در صورت وجود) از یک مدل control plane متمرکز استفاده می‌کند؟

a. OpenDaylight Controller
b. Cisco Application Policy Infrastructure Controller (APIC)
c. Cisco APIC Enterprise Module (APIC-EM)
d. None of these controllers uses a mostly centralized control plane.

5. To which types of nodes should an ACI leaf switch connect in a typical single-site design? (Choose two answers.)

a. All of the other leaf switches
b. A subset of the spine switches
c. All of the spine switches
d. Some of the endpoints
e. None of the endpoints

www.takbook.com

6. Which answers list an advantage of controller-based networks versus traditional networks? (Choose two answers.)

کدام پاسخ‌ها مزیت شبکه‌های مبتنی بر کنترلر را نسبت به شبکه‌های سنتی لیست می کند؟ (دو جواب را انتخاب کنید.)

a. The ability to configure the features for the network rather than per device
b. The ability to have forwarding tables at each device
c. Programmatic APIs available per device
d. More consistent device configuration

7. Which two conditions must be met before SSH can operate normally on a Cisco IOS switch? (Choose two.)

قبل از اینکه سرویس SSH را فعال کنید، کدام گزینه‌ها را باید قبل از آن اماده کنیم؟(دو گزینه راانتخاب کنید)

a. IP routing must be enabled on the switch.
b. A console password must be configured on the switch.
c. Telnet must be disabled on the switch.
d. The switch must be running a k9 (crypto) IOS image.
e. The ip domain-name command must be configured on the switch.

www.takbook.com

www.takbook.com

دستورات دوره‌ی CCNA

نگاه کلی به دستورات و نحوه‌ی نوشتن و کار کردن با آن‌ها:

Router>enable Router>enab Router>en	می‌توانید دستورات را به صورت کامل و یا به صورت چند کلمه بنویسید، مثلاً در دستور روبرو کلمه‌ی enable , enab, en یک عملکرد را از خود نشان می‌دهند
Router#configure terminal Router#config t	به جای نوشتن یک کلمه به صورت کامل آن را خلاصه کنید.
Router#sh Tab = Router#show	بعد از نوشتن چند کلمه از یک دستور، بر روی کلید TAB فشار دهید تا دستور کامل نوشته شود.
Router#?	با نوشتن علامت سوال، لیست همه‌ی دستورات در مد مورد نظر نمایش داده می‌شود.
Router#c? clear clock	با نوشتن یک کلمه و بعدازآن نوشتن علامت سؤال، لیست دستوراتی که با این کلمه وجود دارد، نمایش داده می‌شود.
Router#cl? clear clock	نمایش دستوراتی که با حروف cl شروع می‌شوند.
Router#clock % Incomplete Command	این پیام زمانی نمایش داده می‌شود که یک دستور را به صورت کامل وارد نکرده باشیم.
Router#clock ? set	با گذاشتن علامت سؤال بعد از Clock دستورات بعدازآن نمایش داده می‌شود.
Router>enable Router#	با دستور enable در مد User وارد مد بعدی، یعنی مد Privileged می‌شویم.
Router#exit or Router>exit	با دستور Exit در دو مد اول از همه‌ی مدها خارج می‌شوید، در واقع،Sign Out می‌کنید.

www.takbook.com

با نوشتن دستور exit از interface خارج شده و به مد قبلی برمی‌گردیم.	Router(config-if)#exit Router (config)#
با این دستور در مد Privileged از آن خارج و به مد User می‌رویم.	Router#disable Router>
با این دستور اگر در مد user و Privileged باشیم از آن‌ها به طور کامل خارج می‌شویم.	Router#logout
با این دستور وارد Setup Mode می‌شوید.	Router#setup
نمایش اطلاعات درباره‌ی IOS روتر.	Router#show version
نمایش اطلاعات حافظه‌ی Flash روتر.	Router#show flash
لیست ۱۰ دستور آخر که وارد کرده‌ایم را به ما نشان می‌دهد.	Router#show history

انواع مد در دستگاه‌های سیسکو:

User mode	Router>
Privileged mode	Router#
Global configuration mode	Router(config)#
Interface mode	Router(config-if)#
Subinterface mode	Router(config-subif)#
Line mode	Router(config-line)#
Router configuration mode	Router(config-router)#

با این دستور می‌توانید نام روتر یا سوئیچ را تغییر دهید.	Router(config)#hostname Cisco
نام تغییر کرده.	Cisco(config)#

www.takbook.com

Router(config)#enable password cisco	فعال کردن Password.
Router(config)#enable secret class	فعال کردن secret password.
Router(config)#line con 0	وارد شدن به پورت console.
Router(config-line)#password console	رمزگذاری در پورت console.
Router(config-line)#login	فعال کردن رمز گذاشته شده بر روی پورت با این دستور.
Router(config)#line vty 0 4	وارد شدن به پورت Vty که ۵ پورت است.
Router(config-line)#password telnet	رمزگذاری در پورت Vty.
Router(config-line)#login	فعال کردن رمز گذاشته‌شده بر روی پورت با این دستور.
Router(config)#line aux 0	وارد شدن به پورت auxiliary.
Router(config-line)#password backdoor	رمزگذاری در این پورت.
Router(config-line)#login	فعال کردن رمز گذاشته‌شده بر روی پورت با این دستور.
Router(config)#service password-encryption	فعال کردن سرویس کد کردن رمز عبور تا امنیت روتر افزایش پیدا کند.
Router(config)#no service password-encryption	غیرفعال کردن این امکان.
Router#show ?	تمام دستورات که با دستور show اجرا می‌شود را نمایش می‌دهد.
Router#show interfaces	نمایش اطلاعات تمام Interface های روتر یا سوئیچ.
Router#show interface serial 0	نمایش اطلاعات یک اینترفیس سریال.
Router#show ip interface brief	نمایش همه‌ی اینترفیس‌ها به همراه اطلاعاتی از قبیل ip address و روشن یا خاموش بودن پورت.

www.takbook.com

Router#show controllers serial 0	با این دستور متوجه می‌شویم که کدام طرف از کابل سریال DTE است یا DCE.
Router#show clock	نمایش ساعت دستگاه.
Router#show hosts	نمایش اطلاعات کش روتر در مورد Ipaddress ها و...
Router#show users	نمایش همه کاربرانی که به روتر متصل هستند.
Router#show arp	نمایش جدول پروتکل ARP.
Router#show protocols	نمایش اینترفیس‌های روتر که در لایه‌ی ۳ کار می‌کنند.
Router#show startup-config	نمایش تنظیمات ذخیره‌شده در حافظه‌ی NVram.
Router#show running-config	نمایش اطلاعات ذخیره‌شده در Ram.
Router(config)#int s0	وارد شدن به interface با شماره‌ی صفر.
Router(config-if)#exit	خارج شدن از اینترفیس.
Router(config)#int e0	وارد شدن interface مورد نظر.
Router(config)#int s0/0	وارد شدن به اینترفیس Serial 0/0.
Router(config-if)#description Link to ISP	برچسب‌گذاری روی اینترفیس Serial 0/0.
Router(config-if)#ip address 192.168.10.1 255.255.255.0	آدرس‌دهی به اینترفیس.
Router(config-if)#clock rate 56000	تعیین نرخ انتقال.
Router(config-if)#no shut	روشن کردن اینترفیس.
Router(config)#banner motd # This is a securesystem. Authorized Personnel Only! # Router(config)#	Banner یک پیغام ایجاد می‌کنیم تا کسانی که قصد ورود به روتر را دارد، یعنی قبل از مد UserMode برای آن‌ها نمایش داده شود. # این علامت برای قطع کردن دستور است.

www.takbook.com

Router(config)#clock timezone EST 5	مشخص کردن منطقه‌ی جهانی، عدد 5 در اینجا به معنای این است که ساعت شما با ساعت جهانی چقدر فاطله دارد.
Router(config)#ip host london 172.16.1.3	نسبت دادن یک نام (london)به یک ip address و ارتباط با آن.
Router#ping london	Ping کردن آدرس london.
Router(config)#no ip domain-lookup	زمانی که یک دستور را به اشتباه وارد کردید، روتر دنبالش می‌گردد و وقت‌گیر است. با این دستور از این کار جلوگیری می‌کنیم.
Router(config)#line con 0	وارد پورت console شوید.
Router(config-line)#logging synchronous	با فعال شدن این دستور از نمایش پیام‌های خودکار در هنگام تایپ دستورات جلوگیری می‌کند.
Router(config-line)#exec-timeout 0 0	این دستور مدت‌زمان قرار گرفتن در یک مد را به بی‌نهایت تبدیل می‌کند.
Router#copy run start	ذخیره کردن تنظیمات از Ram به Nvram.
Router#copy run tftp	ذخیره کردن تنظیمات از Ram به یک سرور.
Router#erase start	حذف تنظیمات ذخیره‌شده در Nvram.
Router(config)#ip route 172.16.20.0 255.255.255.0 172.16.10.2	با این دستور یک شبکه‌ی غیرمحلی را به روتر معرفی می‌کنیم.

شماره‌ی Administrative Distance برای پروتکل‌های مختلف:

Route Type	Administrative Distance
Connected	0
Static	1
EIGRP Summary Route	5
EBGP	20

www.takbook.com

Route Type	Administrative Distance
EIGRP (Internal)	90
IGRP	100
OSPF	110
IS-IS	115
RIP	120
EGP	140
On-Demand Routing	160
EIGRP (External)	170
iBGP (External)	200
Unknown	255

پروتکل OSPF:

Router#show ip route	این دستور برای نمایش جدول روتینگ استفاده می‌شود.
Router(config)#router ospf 123 Router(config-router)#	فعال کردن پروتکل OSPF با شماره‌ی ۱۲۳.
Router(config-router)#network 172.16.10.0 0.0.0.255 area 0	تعریف شبکه‌ی مربوط به روتر و قرار دادن آن داخل Area0.
Router(config)#interface loopback 0	وارد شدن به اینترفیس loopback.
Router(config-if)#ip address 192.168.100.1 255.255.255.255	تعریف ip address در loopback.
Router(config)#int S0/0	وارد شدن در interface Serial 0/0.
Router(config-if)#ip ospf priority 50	تغییر priority به ۵۰ برای خارج شدن روتر از حالت DR یا BDR.
Router(config)#int s 0/0	وارد شدن در interface Serial 0/0.
Router(config-if)#bandwidth 128	تغییر پهنای باند اینترفیس مورد نظر.

www.takbook.com

Router(config-if)#ip ospf cost 1564	تغییر cost مربوط به یک interface برای استفاده در OSPF.
Router(config)#router ospf 456	
Router(config-router)#area 0 authentication	فعال کردن Authentication بر روی یک area که رمز عبور در آن به صورت clear Text است.
Router(config-if)#ip ospf authentication-key fred	قرار دادن رمز برای پروتکل ospf.
Router(config)#router ospf 456	
Router(config-router)#area 0 authentication message-digest	فعال کردن MD5 برای hash کردن password.
Router(config-if)#ip ospf message-digest-key 1 md5 fred	تعریف رمز عبور به همراه MD5.
Router(config-if)#ip ospf hello-interval timer 20	تغییر تایمر Hello به ۲۰ ثانیه.
Router(config-if)#ip ospf dead-interval 80	تغییر تایمر Dead به ۸۰ ثانیه.
Router(config)#ip route 0.0.0.0 0.0.0.0 s0/0	تعریف ip Route.
Router(config-router)#default-information-originate	تزریق Default Route به پروتکل Ospf.
switch#show version	نمایش اطلاعاتی از نرم‌افزار و سخت‌افزار سوئیچ.
switch#show flash:	جزئیان ios سوئیچ.
switch#show mac-address-table	نمایش جدول MAC address سوئیچ.
switch#show running-config	نمایش اطلاعات ذخیره‌شده در حافظه‌ی ram.
switch#show start	نمایش اطلاعات ذخیره شده در حافظه‌ی NVRAM.
switch#show post	نمایش حالت Post سوئیچ.

www.takbook.com

switch#show vlan	نمایش تنظیمات Vlan.
switch#show interfaces	نمایش اطلاعات interface های سوئیچ.
switch#show interface vlan1	نمایش اطلاعات Vlan1.
switch#delete flash:vlan.dat	حذف VLAN database از روی حافظه‌ی Flash.
Switch#erase startup-config	حذف اطلاعات حافظه‌ی Nvram.
Switch#reload	ریسیت کردن سوئیچ.
Switch(config)#hostname 2900Switch	تغییر نام سوئیچ.
2900Switch(config)#enable password cisco	فعال کردن رمز عبور.
2900Switch(config)#enable secret class	فعال کردن secret password روی سوئیچ.
2900Switch(config)#line con 0	وارد شدن به console mode.
2900Switch(config-line)#login	درخواست دریافت رمز عبور صادر شود.
2900Switch(config-line)#password cisco	گذاشتن رمز عبور بر روی console.
2900Switch(config-line)#exit	خروج از console mode.
2900Switch(config-line)#line aux 0	ورود به auxiliary mode.
2900Switch(config-line)#login	درخواست دریافت رمز عبور صادر شود.
2900Switch(config-line)#password cisco	فعال کردن رمز عبور روی پورت auxiliary.
2900Switch(config-line)#exit	خروج از auxiliary mode.
2900Switch(config-line)#line vty 0 4	ورود به پورت مجازی VTY.
2900Switch(config-line)#login	درخواست دریافت رمز عبور صادر شود.
2900Switch(config-line)#password cisco	فعال کردن رمز عبور روی پورت VTY.
2900Switch(config-line)#exit	خروج از VTY mode.

www.takbook.com

2900Switch(config)#int vlan1	وارد شدن در Vlan1.
2900Switch(config-if)#ip address 172.16.10.2 255.255.255.0	ثبت ip address در این Vlan.
2900Switch(config-if)#exit	
2900Switch(config)#ip default-gateway 172.16.10.1	ثبت default-gateway برای این سوئیچ.
2900Switch(config-if)#description Finance VLAN	قرار دادن توضیحات در یک interface خاص.
2900Switch(config-if)#speed 10	تعیین سرعت ۱۰ مگابایت.
2900Switch(config-if)#speed 100	تعیین سرعت ۱۰۰ مگابایت.
2900Switch(config-if)#speed auto	تعیین سرعت به صورت اتوماتیک.
X900Switch(config)#ip http server	فعال کردن سرویس http روی سوئیچ.
X900Switch(config)#ip http port 80	اختصاص دادن پورت به سرویس http.
2900Switch(config)#mac-address-table static aaaa.aaaa.aaaa fa0/1 vlan 1	قرار دادن پارامتر در Mc Address.
2900Switch(config)#no mac-address-table static aaaa.aaaa.aaaa fa0/1 vlan 1	حذف کردن پارامتر در Mc Address.
2950Switch(config-if)#switchport port-security	فعال کردن port-security.
2950Switch(config-if)#switchport port-security mac-address sticky	دریافت اطلاعات آدرس mac از دستگاه متصل به پورت.
2950Switch(config-if)#switchport port-security maximum 1	مشخص کردن حداکثر تعداد دستگاه‌های متصل به پورت.
2950Switch(config-if)#switchport port-security violation shutdown	دسترسی غیر مجاز باعث shutdown شدن پورت می‌شود.
2900Switch#show port security	نمایش اطلاعات مربوط به port security.

www.takbook.com

2900#show spanning-tree brief	نمایش اطلاعات پروتکل STP.
Switch(config)#int fa 0/11	
Switch(config-if)#channel-group x mode on	ایجاد Channel-Group با مد on.
2950Switch(config)#vlan 10	ایجاد Vlanبا شماره‌ی ۱۰.
2950Switch(config-vlan)#name Accounting	نام‌گذاری Vlan.
2950Switch(config-vlan)#exit	خروج از vlan.
2900Switch(config-if)#switchport mode access	تبدیل پورت به حالت access.
2900Switch(config-if)#switchport access vlan 2	قرار دادن پورت در vlan 2.
2900Switch(config-if)#int fa0/3	وارد شدن به پورت Fa0/3.
2950Switch(config)#int range fa 0/1 - 4	وارد شدن به چند پورت هم‌زمان و ایجاد تغییرات روی آن.
2900Switch#delete flash:vlan.dat	حذف فایل Vlan.dat از روی حافظه‌ی Falsh.
2900Switch(config-if)#no switchport access vlan 3	خروج پورت از vlan 3 و انتقال آن به Vlan1.
2900Switch#vlan database	حذف Vlan Database.
2900(vlan)#no vlan 3	حذف Vlan با شماره ۳.
2900Switch#show vlan	نمایش جزئیات یک Vlan.
2900Switch#show vlan brief	نمایش جزئیات سریع از vlan.
2900Switch#show interfaces	نمایش اطلاعات interface مورد نظر.
2900Switch#debug sw-vlan packets	عیب‌یابی vlan.

www.takbook.com

2900Switch(config-if)#switchport mode trunk	فعال کردن وضعیت Trunk روی پورت مورد نظر.
2900Switch(config-if)#switchport trunk encapsulation isl	نحوه‌ی برچسب‌گذاری روی فریم‌ها.
2950Switch(config-if)#switchport mode trunk	فعال کردن وضعیت Trunk روی پورت مورد نظر.
29x0Switch#show int fa 0/1 switchport	نمایش اطلاعات witchport روی یک پورت.
2950Switch(config)#vtp mode client	تبدیل سوئیچ به VTP Client.
2950Switch(config)#vtp mode server	تبدیل سوئیچ به VTP Server.
2950Switch(config)#vtp mode transparent	تبدیل سوئیچ به VTP Transparent.
2950Switch(config)#vtp domain academy	تعیین دومین برای سوئیچ.
2950Switch(config)#vtp password catalyst	فرار دارد رمز عبور برای VTP.
2950Switch(config)#vtp v2-mode	تعیین ورژن VTp.
2950Switch(config)#vtp pruning	فعال کردن قابلیت Pruning.
29x0Switch#show vtp status	نمایش اطلاعات دومین.
29x0Switch#show vtp counters	نمایش اطاعات بسته‌های ارسالی و دریافتی در VTP.
Edmonton(config)# ntp server 209.165.200.254	با ساتفاده از این دستور روتر ساعت خود را با سرور NTP به آدرس 209.165.200.254 هماهنگ می‌کند.
Edmonton(config)# ntp server 209.165.200.234 prefer	در صورت داشتن چندین سرور NTP با دستور prefer می‌توانیم NTP دلخواه خود را انتخاب کنیم.
Edmonton(config-if)# ntp disable	عملکرد NTP را در یک Interface غیرفعال می‌کند، بهتر است از این دستور در پورت‌هایی که به شبکه‌ی خارجی متصل است استفاده کنید.

www.takbook.com

Edmonton(config)# ntp master stratum	برای هماهنگ‌سازی دستگاه‌ها با ساعت اتمی مورد استفاده قرار می‌گیرد که این نوع سرورهای NTP دارای یک ساختار سلسله مراتبی هستند که به آنها Stratum گفته می‌شود، Stratum 1 مستقیماً به سرور اتمی متصل است و Stratum 2 به سرور Stratum 1 متصل است.
Edmonton(config)# ntp max-associations 200	حداکثر تعداد peer-and-client در NTP که یک روتر می‌تواند از آن استفاده کند از ۰ تا ۴,۲۹۴,۹۶۷,۲۹۵ است که عدد پیش‌فرض آن ۱۰۰ است.
Edmonton(config)# access list 101 permit udp any host a.b.c.d eq ntp	ایجاد یک لیست دسترسی برای سرور NTP برای دسترسی به یک آدرس خاص که این Access List باید در جهت ورودی قرار بگیرد.
Edmonton(config)# ntp peer 172.16.21.1	یک دستگاه IOS را برای همگام‌سازی ساعت نرم‌افزار با همسایه‌ی خود که آدرس 172.16.21.1 است تنظیم می‌کند.
Edmonton(config)# ntp peer 172.16.21.1 version 2	یک دستگاه IOS را برای همگام‌سازی ساعت نرم‌افزار با همسایه‌ی خود که آدرس 172.16.21.1 است تنظیم می‌کند البته یا استفاده از نسخه‌ی دوم که کلاً سه نسخه از NTP وجود دارد از ۲ تا ۴ .
Edmonton(config)# ntp peer 172.16.21.1 source loopback 0	یک دستگاه IOS را برای همگام‌سازی ساعت نرم‌افزار با همسایه‌ی خود که آدرس 172.16.21.1 است تنظیم می‌کند، به این نکته توجه کنید که بهتر است آدرس منبع را آدرس Loopback 0 قرار دهید چون هیچ وقت خاموش نمی‌شود.
NTPServer(config)# ntp authentication-key 1 md5 NTPpa55word	یک کلید احراز هویت NTP را تعریف می‌کند، که شماره ۱ آن یک کلید تایید اعتبار است که می‌تواند عددی بین ۱ تا ۴,۲۹۴,۹۶۷,۲۹۵ باشد.
NTPServer(config)# ntp authenticate	احراز هویت NTP را فعال می‌کند.
NTPServer(config)# ntp trusted-key 1	تعریف می‌کند که کدام کلیدها برای تأیید اعتبار NTP معتبر هستند .شماره کلیدی در اینجا باید با شماره

www.takbook.com

	کلیدی که در دستور تأیید اعتبار کلید ntp تعریف کرده اید مطابقت داشته باشد.
NTPClient(config)# ntp authentication-key 1 md5 NTPpa55word	یک کلید احراز هویت NTP را تعریف می‌کند.
NTPClient(config)# ntp server 192.168.200.1 key 1	سرور NTP را که نیاز به تأیید اعتبار دارد در آدرس ۱۹۲.۱۶۸.۲۰۰.۱ تعریف می‌کند و شماره کلید همتا را به عنوان کلید ۱ مشخص می‌کند.
Edmonton(config)# access-list 1 permit 10.1.0.0 0.0.255.255	تعریف لیست دسترسی که آدرس‌هایی با منبع 10.1.x.x اجازه عبور دارند.
Edmonton(config)# ntp access-group peer 1	یک گروه دسترسی برای کنترل دسترسی NTP ایجاد می‌کند و لیست دسترسی با شماره‌ی یک را اعمال می‌کند. کلمه کلیدی همتا دستگاه را قادر می‌سازد درخواست‌های زمان و نمایش داده‌های کنترل NTP را دریافت کند و خود را با سرورهای مشخص شده در لیست دسترسی، همگام‌سازی کند.
Edmonton(config)# ntp access-group serve 1	یک گروه دسترسی برای کنترل دسترسی NTP ایجاد می‌کند و لیست دسترسی با شماره‌ی یک را اعمال می‌کند. کلمه کلیدی همتا دستگاه را قادر می‌سازد درخواست‌های زمان و نمایش داده‌های کنترل NTP را دریافت کند و خود را با سرورهای مشخص شده در لیست دسترسی، همگام‌سازی نکند.
Edmonton(config)# ntp access-group serve-only 1	یک گروه دسترسی برای کنترل دسترسی NTP ایجاد می‌کند و لیست دسترسی با شماره‌ی یک را اعمال می‌کند. کلمه کلیدی فقط دستگاه را قادر می‌سازد درخواست‌های زمان را از سرورهای مشخص شده در لیست دسترسی دریافت کند
Edmonton(config)# ntp access-group query-only 1	یک گروه دسترسی برای کنترل دسترسی NTP ایجاد می‌کند و لیست دسترسی با شماره‌ی یک را اعمال می‌کند، کلمه‌ی کلیدی query-only دستگاه را قادر

www.takbook.com

	می‌سازد فقط از نمایشگرهای کنترل NTP از سرورهای مشخص شده در لیست دسترسی دریافت کند.
Edmonton# show ntp associations	وضعیت انجمن های NTP را نشان می‌دهد.
Edmonton# show ntp associations detail	اطلاعات دقیق درباره هر انجمن NTP را نشان می‌دهد.
Edmonton# show ntp status	وضعیت NTP را نشان می دهد .این دستور نشان می‌دهد که آیا ساعت روتر با سرور NTP خارجی هماهنگ شده است یا خیر.
Edmonton# debug ip packets	بررسی می‌کند که بسته‌های NTP دریافت یا ارسال می‌شوند یا خیر.
Edmonton# debug ip packet 1	خروجی debug را به ACL 1 محدود می‌کند.
Edmonton# debug ntp adjust	
Edmonton# debug ntp all	خروجی debug را برای تنظیم ساعت NTP نشان می‌دهد.
Edmonton# debug ntp events	تمام وقایع NTPرا نمایش می‌دهد.
Edmonton# debug ntp packet	debug بسته NTP را نشان می دهد.
Edmonton# debug ntp packet detail	جزئیات بسته‌های debug ntp را نمایش می‌دهد.
Edmonton# debug ntp packet peer a.b.c.d	نمایش debugging برای همسایه‌ی a.b.c.d
Switch(config)# errdisable recovery interval seconds	زمان Recover شدن را میتوانید بین ۳۰ تا ۸۶۴۰۰ ثانیه انتخاب کنید که به صورت پیش‌فرض بر روی ۳۰۰ ثانیه قرار دارد.
Switch# show errdisable recovery	اطلاعات مربوط به دستور errdisable Recovery را نمایش می‌دهد.
Switch# show interfaces status err-disabled	نمایش اطلاعات err-disabled بر روی Interface های سوئیچ.

www.takbook.com

Switch# clear errdisable interface interface-id vlan [vlan-list]	VLANهایی که دارای error-disabled بودند را دوباره فعال می‌کند.
Switch(config)# ip dhcp snooping	فعال کردن snooping
Switch(config)# ip dhcp snooping vlan 20	DHCP snooping را در VLAN شماره‌ی ۲۰ فعال می‌کند
Switch(config)# ip dhcp snooping vlan 10-35	DHCP snooping را در VLAN شماره‌ی ۱۰ تا ۳۵ فعال می‌کند.
Switch(config)# ip dhcp snooping vlan 20 30	DHCP snooping را در VLAN شماره‌ی ۲۰ تا ۳۰ فعال می‌کند.
Switch(config)# ip dhcp snooping vlan 10,12,14	DHCP snooping را در VLAN شماره‌ی ۱۰، ۱۲ و ۱۴ فعال می‌کند.
Switch(config)# ip dhcp snooping vlan 10-12,14	DHCP snooping را در VLAN شماره‌ی۱۰ تا ۱۲ و ۱۴ فعال می‌کند.
Switch(config)# ip dhcp snooping information option	ویژگی شماره‌ی ۸۲ سرویس DHCP Snooping را فعال می‌کند، با فعال‌سازی آن اطلاعات اضافه‌تری در هنگام ارسال به بسته اضافه خواهد شد.
Switch(config-if)# ip dhcp snooping trust	مشخص می‌کند که Inteface مورد نظر قابل اعتماد است، این مورد در زمانی مورد استفاده قرار می‌گیرد که باید پورت متصل به سرور DHCP را Trust کنید.
Switch(config-if)# ip dhcp snooping limit rate 75	تعداد بسته‌هایی که در هر ثانیه یک Interface می‌تواند دریافت کند را مشخص می‌کند. سیسکو ۱۰۰ بسته در هر ثانیه را غیر مجاز می‌داند.
Switch(config)# ip dhcp snooping verify mac-address	با این دستور به سوئیچ اعلام می‌کنیم که آدرس MAC فرستنده در یک بسته‌ی DHCP که از یک پورت غیر

www.takbook.com

قابل اعتماد دریافت می‌شود با آدرس سخت‌افزاری مشتری در بسته مطابقت دارد.	
پیکربندی DHCP snooping را برای سوئیچ نشان می‌دهد.	Switch# show ip dhcp snooping
فقط اتصالات پیکربندی شده بصورت پویا را در بانک اطلاعاتی اتصال DhCP نشان می‌دهد.	Switch# show ip dhcp snooping binding
اتصالات پیکربندی شده بصورت پویا و استاتیک را نشان می‌دهد.	Switch# show ip source binding
برای مشاهده وضعیت شماره‌ی ۸۲ در همه‌ی Interfaceها می‌توانیم از این دستور استفاده کنیم.	Switch# show running-config
مشاهده وضعیت arp inspection بر روی Interface .	Switch# show ip arp inspection interfaces
مشاهده وضعیت arp inspection بر روی VLAN شماره‌ی ۱۰ .	Switch# show ip arp inspection vlan 10
مشاهده آماری وضعیت arp inspection بر روی VLAN شماره‌ی ۱۰ .	Switch# show ip arp inspection statistics vlan 10
Enables DHCP snooping, globally	Switch(config)# ip dhcp snooping
DHCP Snooping را در VLAN شماره‌ی ۱۰ تا ۲۰ فعال می‌کند.	Switch(config)# ip dhcp snooping vlan 10-20
فعال کردن arp inspection در VLAN شماره‌ی ۱۰ تا ۲۰.	Switch(config)# ip arp inspection vlan 10-20
با این دستور arp inspection بسته‌هایی که آدرس MAC فرستنده با آدرس MAC فرستنده مشخص شده در Ethernet header یکی نباشد این بسته Drop خواهد شد.	Switch(config)# ip arp inspection validate src-mac

www.takbook.com

Switch(config)# ip arp inspection validate dst-mac	با این دستور arp inspection بسته‌هایی که آدرس MAC گیرنده با آدرس MAC گیرنده‌ی مشخص شده در Ethernet header یکی نباشد این بسته Drop خواهد شد.
Switch(config)# ip arp inspection validate ip	با این دستور arp inspection آدرس‌های IP نامعتبر و غیر منتظره مانند 0.0.0.0، 255.255.255.255 و تمام آدرس‌های multicast را Drop می‌کند.
Switch(config)# interface fastethernet0/24	رفتن به حالت Interface شماره‌ی fastethernet0/24
Switch(config-if)# ip dhcp snooping trust	قابل اعتماد کردن پورت مورد نظر برای dhcp snooping .
Switch(config-if)# ip arp inspection trust	قابل اعتماد کردن پورت مورد نظر برای arp inspection.
Router(config-if)#int fa 0/0.1	ساختن interface مجازی با شماره‌ی 0/0.1
Router(config-subif)#encapsulation dot1q 10	نسبت دادن این پورت به Vlan 10 با برچسب‌گذاری dot1q.
Router(config-subif)#ip address 192.168.10.1 255.255.255.0	واردکردن IP address در اینترفیس مجازی.
Router(config)#boot system flashimage-name	اجرای ios از روی ایمیج مورد نظر.
Router(config)#boot system tftpimage-name172.16.10.3	اجرای ios از روی سرور TFTP.
Router(config)#boot system rom	اجرای IOS از روی Rom.
copy tftp running-config	انتقال اطلاعات از سرور TFTP به Ram.
copy tftp startup-config	انتقال اطلاعات از سرور TFTP به Nvram.
show startup-config	نمایش اطلاعات ذخیره‌شده روی Nvram.
erase startup-config	پاک کردن Nvram.

www.takbook.com

copy run start	انتقال اطلاعات از Ram به Nvram.
copy run tftp	انتقال اطلاعات از Nvram به Ram.
show run	نمایش اطلاعات ذخیره‌شده روی ram.
router#show version	نمایش ورژن ios روتر یا سوئیچ.
router(config)#config-register 0x2142	تغییر شماره‌ی رجیستر با دستور confreg.
Router#show cdp	نمایش دستگاه‌های متصل.
Router#show cdp neighbors	نمایش دستگاه‌های متصل .
Router#show cdp neighbors detail	نمایش دستگاه‌های متصل با جزئیات کامل.
Router#show cdp entry word	نمایش دستگاه‌های متصل با استفاده از نام دستگاه.
Router#show cdp entry *	نمایش همه دستگاه‌های متصل
Router#show cdp interface	نمایش اینترفیسی که CDP روی آن فعال شده است
Router#show cdp interface x	نمایش اینترفیسی که CDP روی آن فعال شده است
Router#show cdp traffic	نمایش ترافیک مربوط به CDP
Router(config)#cdp holdtime x	تغییر ساعت holdtime در CDP
Router(config)#cdp timer x	تغییر ساعت ارسال آپدیت در CDP
Router(config)#cdp run	فعال کردن CDP.
Router(config)#no cdp run	غیرفعال کردن فرمان CDP.

www.takbook.com

Router(config-if)#cdp enable	فعال کردن CDP روی یک اینترفیس خاص.
Router(config-if)#no cdp enable	غیرفعال کردن CDP روی یک اینترفیس خاص.
Router#clear cdp counters	ریسیت کردن شماره‌ی counters در CDP.
Router#clear cdp table	حذف جدول CDP.
Router#debug cdp adjacency	مانیتور کردن اطلاعات CDP مربوط به همسایه.
Router#debug cdp events	مانیتور کردن تمام رویدادهای CDP.
Router#debug cdp ip	نمایش اطلاعات CDP مربوط به یک ip خاص.
Router#debug cdp packets	مانیتور کردن پکت‌های مربوط به CDP.
Router#traceroute 172.168.20.1	نمایش روترهای سر راه تا رسیدن به ip مورد نظر.
Router#TRace paris	نمایش روترهای سر راه تا رسیدن به Host مورد نظر.
Router#show ip route	نمایش جدول Route.
Router#show ip route protocol	نمایش اطلاعات جدول روتینگ بر طبق یک پروتکل خاص مانند Rip و Eigrp.
Router#show ip route w.x.y.z	نمایش اطلاعات route در مورد یک آدرس خاص.
Router#show ip route connected	نمایش اطلاعات روترهای متصل به این روتر.
Router#show ip route static	نمایش static Route.
Router#show ip route summary	نمایش اطلاعات کامل از جدول route.
Router(config)#ip route 0.0.0.0 0.0.0.0 172.16.20.1	فعال کردن Ip Route برای روتر که هر چه نمی‌داند را بفرستد به ip 172.16.20.1.

www.takbook.com

Router#show ip route	نمایش جدول روتینگ.
Router#debug telnet	نمایش اطلاعات رد و بدل شده دستور Telnet.
Router#show interface serial 0/0	نمایش وضعیت پورت سریال ۰/۰
Router#clear counters	پاک کردن همه‌ی شمارنده‌ها.
Router#clear counters interface type/slot	پاک کردن شمارنده‌ی مربوط به یک اینترفیس خاص.
Corp(config)#ip nat pool scott 64.64.64.70 64.64.64.126 netmask 255.255.255.128	فعال کردن Pool برای یک رنج ip خاص که مربوط به ip Valid است.
Corp(config)#access-list 1 permit 172.16.10.0 0.0.0.255	ساخت access-list و مجوز دادن به ip های در رنج مورد نظر.
Corp(config)#ip nat inside source list 1 pool scott	متصل کردن pool و Access-list مورد نظر در کنار هم.
Router(config)#int fa 0/0	وارد شدن به interface مورد نظر برای فعال کردن nat.
Router(config-if)#ip nat inside	فعال کردن nat بر روی اینترفیس داخلی شبکه.
Router(config-if)#ip nat Outside	فعال کردن nat بر روی اینترفیس خارجی شبکه.
Corp(config)#ip nat inside source list 1 interface serial 0/0 overload	فعال کردن access-list بر روی یک اینترفیس مورد نظر به صورت Overload (Pat).
Corp(config)#ip nat inside source static 172.16.10.5 64.64.64.65	فعال کردن Static Nat.
Router#show ip nat translations	نمایش اطلاعات مربوط به آدرس‌های مربوط به NAT.
Router#show ip nat statistics	نمایش کامل اطلاعات NAT.
Router#clear ip nat translations inside a.b.c.d outside e.f.g.h	حذف اطلاعات nat مربوط به آدرس خاص.

www.takbook.com

Router#clear ip nat translations *	پاک کردن کامل اطلاعات مربوط به جدول translations.
Router#debug ip nat	فعال کردن Debug برای Nat.
Router#debug ip nat detailed	نمایش اطلاعات پکت‌های مربوط به Nat به صورت کامل.
Router(config)#ip dhcp pool academy	تعریف کردن Dhcp Pool و فعال شدن آن.
Router(dhcp-config)#network 172.16.10.0 255.255.255.0	تعریف کردن رنج Ip برای DHCP .
Router(dhcp-config)#default-router 172.16.10.1	تعریف کردن Default-Route برای کلاینت‌ها.
Router(dhcp-config)#dns-server 172.16.10.10	تعریف کردن Dns Server برای کلاینت‌ها.
Router(dhcp-config)#netbios-name-server 172.16.10.10	تعریف کردن Netbios برای کلاینت‌ها.
Router(dhcp-config)#domain-name 3isco.ir	تعریف کردن Domain برای کلاینت‌ها.
Router(dhcp-config)#lease 14 12 23	حداکثر زمان در اختیار قرار گذاشتن ip address به یک کلاینت.
Router(dhcp-config)#lease infinite	زمان نامحدود برای پس گرفتن ip address از کلاینت.
Router(config)#ip dhcp excluded-address 172.16.10.1 172.16.10.9	اختصاص ندادن رنج ip مورد نظر به کلاینت‌ها.
Router(config)#no service dhcp	غیرفعال کردن سرویس DHCP.
Router(config)#service dhcp	فعال کردن سرویس DHCP.
Router#show ip dhcp binding	نمایش اطلاعات سرویس DHCP.
Router#show ip dhcp server statistics	نمایش اطلاعات مربوط به ارسال و دریافت اطلاعات از طریق DHCP.

www.takbook.com

نمایش رویدادهای مربوط به DHCP.	Router#debug ip dhcp server events
انتقال اطلاعات مربوط به یک DHCP سرور به یک اینترفیس خاص. توجه داشته باشید که زمانی که ip helper-address فعال می‌شود، بر روی ۸ پورت UDP عملیات Broadcast را انجام می‌دهد که عبارت‌اند از: TFTP (port 69) DNS (port 53) Time service (port 37) NetBIOS name server (port 137) NetBIOS datagram server (port 138) Boot Protocol (BOOTP) client and server datagrams (ports 67 and 68) TACACS service (port 49) اگر بخواهید بعضی از این پورت‌ها را ببندید باید از دستور زیر استفاده کنید: no ip forward-protocol udp x که در دستور بالا به جای حرف x باید شماره‌ی پورت مورد نظر را وارد کنید. و برای باز کردن پورت‌های دیگر UDP می‌توانید از دستور زیر استفاده کنید: ip forward-protocol udp x	Router(config-if)#ip helper-address 172.16.20.2
با گزینه‌ی ۶۶ می‌توانید آدرس IP سرور TFTP را مشخص کنید.	Router(dhcp-config)# option 66 ip 10.1.1.250
با گزینه‌ی ۱۵۰ می‌توانید نام سرور TFTP را مشخص کنید.	Router(dhcp-config)# option 150 ip 10.1.1.250
با گزینه‌ی ۱۵۰ می‌توانید نام دو سرور TFTP را مشخص کنید.	Router(dhcp-config)# option 150 ip 10.1.1.250 10.1.1.251
مشخص کردن default route در سرویس DHCP با گزینه‌ی ۳ .	Router(dhcp-config)# option 3 ip 10.1.1.1
لیستی از تمام اتصالهای ایجاد شده را نشان می دهد.	Router# show ip dhcp binding

www.takbook.com

Router# show ip dhcp binding w.x.y.z	پیوندها مربوط به آدرس مشخص شده (w.x.y.z) را نمایش می‌دهد.
Router# clear ip dhcp binding a.b.c.d	یک اتصال خودکار را از بانک اطلاعات سرور DHCP پاک می‌کند.
Router# clear ip dhcp binding	پاک کردن اتوماتیک تمام اتصالات خودکار.
Router# show ip dhcp conflict	لیستی از آدرس‌های شبیه به هم که در سرور DHCP قرار گرفته‌اند.
Router# clear ip dhcp conflict a.b.c.d	پاک کردن آدرس شبیه به هم در بانک اطلاعاتی DHCP که با هم Conflict دارند.
Router# clear ip dhcp conflict *	پاک کردن تمام آدرس‌هایی که با هم Conflict دارند.
Router# show ip dhcp database	فعالیت اخیر را در پایگاه داده DHCP نمایش می‌دهد.
Router# show ip dhcp pool	اطلاعات مربوط به poolها را در DHCP نشان می‌دهد.
Router# show ip dhcp pool name	اطلاعات مربوط به نام Pool را در DHCP نشان می‌دهد.
Router# clear ip dhcp server statistics	تمام اطلاعات مربوط به statistics را از پایگاه داده پاک می‌کند.
Router# debug ip dhcp server {events | packet | linkage | class}	نمایش اطلاعاتی از پردازش‌هایی در مورد آدرس‌های Leased و برگشتی.
Router#config t	وارد شدن به مد Global.
Router(config)#int s 0/0	وارد شدن به اینترفیس سریال ۰/۰
Router(config-if)#encapsulation hdlc	فعال کردن برچسب‌گذاری به روش HDLC.

www.takbook.com

Router(config-if)#encapsulation ppp	فعال کردن برچسب‌گذاری به صورت PPP.
Router(config)#username routerb password cisco	تعریف UserName و Password.
Router(config)#int s 0/0	ورود به پورت سریال s0/0
Router(config-if)#ppp authentication pap	فعال کردن الگوریتم رمزنگاری PAP.
Router(config-if)#ppp authentication chap	فعال کردن الگوریتم رمزنگاری CHAP.
Router(config-if)#ppp authentication pap chap	فعال کردن الگوریتم‌های رمزنگاریPAP و CHAP.
Router(config-if)#ppp authentication chap pap	فعال کردن الگوریتم‌های رمزنگاریCHAP و PAP.
Router(config-if)#ppp pap sent-username routerb password cisco	تعریف نام کاربری و رمز عبور روتر روبرو.
Router#show interfaces serial x	نمایش اطلاعات اینترفیس سریال.
Router#show controllers serial x	نمایش اطلاعات مربوط به اینترفیس سریال برای مشخص کردن DCE و DTE بودن کابل مورد نظر.
Router#debug serial interface	نمایش رویدادهای مربوط به اینترفیس سریال.
Router#debug ppp	نمایش رویدادهای مربوط به پروتکل PPP.
Router#debug ppp packet	نمایش رویدادهای مربوط به پکت‌های پروتکل PPP.
Router#debug ppp negotiation	نمایش رویدادهای مربوط به پروتکل PPP.
Router#debug ppp error	نمایش پکت‌های مشکل دار در پروتکل PPP.
Router#debug ppp authentication	نمایش رویدادهای مربوط به پکت‌هایی که دارای احراز هویت هستند.
Router(config)#int s 0/0	وارد شدن به اینترفیس سریال ۰/۰

www.takbook.com

Router(config-if)#encapsulation frame-relay	فعال کردن Frame Relay روی اینترفیس سریال مورد نظر.
Router(config-if)#frame-relay lmi-type {ansi | cisco | q933a}	مشخص کردن نوع پروتکل Frame Relay برای ارتباط در روترهای شرکت‌های مختلف.
Router(config-if)#frame-relay interface-dlci 110	تعریف شماره‌ی DLCI 110 بر روی اینترفیس مورد نظر.
Router(config-if)#frame-relay map ip 192.168.100.1 110 broadcast	تعریف آدرس با شماره‌ی DLCI روتر دیگر در یک ارتباط Frame Relay.
Router(config-if)#no frame-relay inverse arp	غیرفعال کردن حالت خودکار Invers Arp.
Router(config-subif)#int s 0/0.103 point-to-point	ساخت اینترفیس مجازی با حالت Point To Point
Router(config-subif)#ip address 192.168.20.1 255.255.255.0	تخصیص دادن IP address به اینترفیس مجازی.
Router(config-subif)#frame-relay interface-dlci 103	تعریف DLCI برای این اینترفیس.
Router(config)#access-list 10 permit 172.16.0.0 0.0.255.255	فعال کردن AL 10 و اجازه‌ی عبور دادن IP Address 172.16.0.0.
access-list	دستور Access List.
Router(config)#access-list 10 permit any	این Access List با شماره‌ی ۱۰ به همه‌ی آدرس‌ها اجازه عبور می‌دهد (Any یعنی همه).
Router(config)#int fa0/0	وارد شدن به اینترفیس مورد نظر.
Router(config-if)#ip access-group 10 in	فعال کردن Access List شماره‌ی ۱۰ روی اینترفیس مورد نظر به صورت in.
Router#show access-lists	نمایش Access List های تعریف‌شده روی روتر.
Router#show access-list access-list-number	نمایش Access List با شماره‌ی مورد نظر.

www.takbook.com

Router#show access-list name	نمایش Access List با اسم مورد نظر.
Router(config)#access-list 110 per677itt cp 172.16.0.0 0.0.0.255 192.168.100.0 0.0.0.255 eq 80	اجازه‌ی عبور به شبکه مورد نظر برای دسترسی به پروتکل HTTP که پورت آن ۸۰ است.
Router(config)#access-list 110 deny tcp any 192.168.100.7 0.0.0.0 eq 23	فعال کردن access List Estended برای جلوگیری از IP adderss 192.168.100.7 برای دسترسی به Telnet.

www.takbook.com

نمودار تبدیل
Binary/Hex/Decimal

نمودار زیر سه سیستم رایج مورد استفاده در شبکه را نشان می دهد: decimal, hexadecimal و binary .
بعضی از اعداد را به راحتی به یاد می‌آورید، برای اینکه در فعالیت‌های روزانه خود از آنها بسیار استفاده می‌کنید. برای یادآوری شماره‌های دیگر می‌توانید به این نمودار مراجعه کنید.

Decimal Value	Hexadecimal Value	Binary Value
0	00	0000 0000
1	01	0000 0001
2	02	0000 0010
3	03	0000 0011
4	04	0000 0100
5	05	0000 0101
6	06	0000 0110
7	07	0000 0111
8	08	0000 1000
9	09	0000 1001
10	0A	0000 1010
11	0B	0000 1011
12	0C	0000 1100
13	0D	0000 1101
14	0E	0000 1110
15	0F	0000 1111
16	10	0001 0000

www.takbook.com

17	11	0001 0001
18	12	0001 0010
19	13	0001 0011
20	14	0001 0100
21	15	0001 0101
22	16	0001 0110
23	17	0001 0111
24	18	0001 1000
25	19	0001 1001
26	1A	0001 1010
27	1B	0001 1011
28	1C	0001 1100
29	1D	0001 1101
30	1E	0001 1110
31	1F	0001 1111
32	20	0010 0000
33	21	0010 0001
34	22	0010 0010
35	23	0010 0011
36	24	0010 0100
37	25	0010 0101
38	26	0010 0110
39	27	0010 0111
40	28	0010 1000
41	29	0010 1001

www.takbook.com

42	2A	0010 1010
43	2B	0010 1011
44	2C	0010 1100
45	2D	0010 1101
46	2E	0010 1110
47	2F	0010 1111
48	30	0011 0000
49	31	0011 0001
50	32	0011 0010
51	33	0011 0011
52	34	0011 0100
53	35	0011 0101
54	36	0011 0110
55	37	0011 0111
56	38	0011 1000
57	39	0011 1001
58	3A	0011 1010
59	3B	0011 1011
60	3C	0011 1100
61	3D	0011 1101
62	3E	0011 1110
63	3F	0011 1111
64	40	0100 0000
65	41	0100 0001
66	42	0100 0010

www.takbook.com

67	43	0100 0011
68	44	0100 0100
69	45	0100 0101
70	46	0100 0110
71	47	0100 0111
72	48	0100 1000
73	49	0100 1001
74	4A	0100 1010
75	4B	0100 1011
76	4C	0100 1100
77	4D	0100 1101
78	4E	0100 1110
79	4F	0100 1111
80	50	0101 0000
81	51	0101 0001
82	52	0101 0010
83	53	0101 0011
84	54	0101 0100
85	55	0101 0101
86	56	0101 0110
87	57	0101 0111
88	58	0101 1000
89	59	0101 1001
90	5A	0101 1010
91	5B	0101 1011

www.takbook.com

92	5C	0101 1100
93	5D	0101 1101
94	5E	0101 1110
95	5F	0101 1111
96	60	0110 0000
97	61	0110 0001
98	62	0110 0010
99	63	0110 0011
100	64	0110 0100
101	65	0110 0101
102	66	0110 0110
103	67	0110 0111
104	68	0110 1000
105	69	0110 1001
106	6A	0110 1010
107	6B	0110 1011
108	6C	0110 1100
109	6D	0110 1101
110	6E	0110 1110
111	6F	0110 1111
112	70	0111 0000
113	71	0111 0001
114	72	0111 0010
115	73	0111 0011
116	74	0111 0100
117	75	0111 0101

www.takbook.com

118	76	0111 0110
119	77	0111 0111
120	78	0111 1000
121	79	0111 1001
122	7A	0111 1010
123	7B	0111 1011
124	7C	0111 1100
125	7D	0111 1101
126	7E	0111 1110
127	7F	0111 1111
128	80	1000 0000
129	81	1000 0001
130	82	1000 0010
131	83	1000 0011
132	84	1000 0100
133	85	1000 0101
134	86	1000 0110
135	87	1000 0111
136	88	1000 1000
137	89	1000 1001
138	8A	1000 1010
139	8B	1000 1011
140	8C	1000 1100
141	8D	1000 1101
142	8E	1000 1110

www.takbook.com

143	8F	1000 1111
144	90	1001 0000
145	91	1001 0001
146	92	1001 0010
147	93	1001 0011
148	94	1001 0100
149	95	1001 0101
150	96	1001 0110
151	97	1001 0111
152	98	1001 1000
153	99	1001 1001
154	9A	1001 1010
155	9B	1001 1011
156	9C	1001 1100
157	9D	1001 1101
158	9E	1001 1110
159	9F	1001 1111
160	A0	1010 0000
161	A1	1010 0001
162	A2	1010 0010
163	A3	1010 0011
164	A4	1010 0100
165	A5	1010 0101
166	A6	1010 0110
167	A7	1010 0111
168	A8	1010 1000

www.takbook.com

169	A9	1010 1001
170	AA	1010 1010
171	AB	1010 1011
172	AC	1010 1100
173	AD	1010 1101
174	AE	1010 1110
175	AF	1010 1111
176	B0	1011 0000
177	B1	1011 0001
178	B2	1011 0010
179	B3	1011 0011
180	B4	1011 0100
181	B5	1011 0101
182	B6	1011 0110
183	B7	1011 0111
184	B8	1011 1000
185	B9	1011 1001
186	BA	1011 1010
187	BB	1011 1011
188	BC	1011 1100
189	BD	1011 1101
190	BE	1011 1110
191	BF	1011 1111
192	C0	1100 0000
193	C1	1100 0001

www.takbook.com

194	C2	1100 0010
195	C3	1100 0011
196	C4	1100 0100
197	C5	1100 0101
198	C6	1100 0110
199	C7	1100 0111
200	C8	1100 1000
201	C9	1100 1001
202	CA	1100 1010
203	CB	1100 1011
204	CC	1100 1100
205	CD	1100 1101
206	CE	1100 1110
207	CF	1100 1111
208	D0	1101 0000
209	D1	1101 0001
210	D2	1101 0010
211	D3	1101 0011
212	D4	1101 0100
213	D5	1101 0101
214	D6	1101 0110
215	D7	1101 0111
216	D8	1101 1000
217	D9	1101 1001
218	DA	1101 1010
219	DB	1101 1011

www.takbook.com

220	DC	1101 1100
221	DD	1101 1101
222	DE	1101 1110
223	DF	1101 1111
224	E0	1110 0000
225	E1	1110 0001
226	E2	1110 0010
227	E3	1110 0011
228	E4	1110 0100
229	E5	1110 0101
230	E6	1110 0110
231	E7	1110 0111
232	E8	1110 1000
233	E9	1110 1001
234	EA	1110 1010
235	EB	1110 1011
236	EC	1110 1100
237	ED	1110 1101
238	EE	1110 1110
239	EF	1110 1111
240	F0	1111 0000
241	F1	1111 0001
242	F2	1111 0010
243	F3	1111 0011
244	F4	1111 0100

www.takbook.com

245	F5	1111 0101
246	F6	1111 0110
247	F7	1111 0111
248	F8	1111 1000
249	F9	1111 1001
250	FA	1111 1010
251	FB	1111 1011
252	FC	1111 1100
253	FD	1111 1101
254	FE	1111 1110
255	FF	1111 1111

www.takbook.com

www.takbook.com

پاسخنامه سوالات فصل‌ها

نکته: سعی کنید قبل از اینکه پاسخ سوالات را مشاهده کنید، خودتان به سوالات پاسخ دهید تا بتوانید خود را محک بزنید.

فصل اول	سوال اول	گزینه‌ی D , F
	سوال دوم	گزینه‌ی A , G
	سوال سوم	گزینه‌ی B
	سوال چهارم	گزینه‌ی B
	سوال پنجم	گزینه‌ی A
	سوال ششم	گزینه‌ی D
	سوال هفتم	گزینه‌ی B
	سوال هشتم	گزینه‌ی A
	سوال نهم	گزینه‌ی C , E
	سوال دهم	گزینه‌ی A

فصل دوم	سوال اول	گزینه‌ی A , B
	سوال دوم	گزینه‌ی B
	سوال سوم	گزینه‌ی B
	سوال چهارم	گزینه‌ی A
	سوال پنجم	گزینه‌ی F
	سوال ششم	گزینه‌ی B , C
	سوال هفتم	گزینه‌ی A
	سوال هشتم	گزینه‌ی C
	سوال نهم	گزینه‌ی D
	سوال دهم	گزینه‌ی B

فصل سوم	سوال اول	گزینه‌ی B

www.takbook.com

	سوال دوم	گزینه‌ی D
	سوال سوم	گزینه‌ی B
	سوال چهارم	گزینه‌ی A , C
	سوال پنجم	گزینه‌ی A , B
	سوال ششم	گزینه‌ی B , C
	سوال هفتم	گزینه‌ی A , B
	سوال هشتم	گزینه‌ی B
	سوال نهم	گزینه‌ی C

فصل چهارم	سوال اول	گزینه‌ی A , D
	سوال دوم	گزینه‌ی D
	سوال سوم	گزینه‌ی B , C
	سوال چهارم	گزینه‌ی A , C
	سوال پنجم	گزینه‌ی A , D , E
	سوال ششم	گزینه‌ی A , C
	سوال هفتم	گزینه‌ی B
	سوال هشتم	گزینه‌ی D
	سوال نهم	گزینه‌ی B
	سوال دهم	گزینه‌ی D

فصل پنجم	سوال اول	گزینه‌ی B , E
	سوال دوم	گزینه‌ی B
	سوال سوم	گزینه‌ی B , C
	سوال چهارم	گزینه‌ی A
	سوال پنجم	گزینه‌ی C , E
	سوال ششم	گزینه‌ی B

www.takbook.com

	سوال هفتم	گزینه‌ی B
	سوال هشتم	گزینه‌ی D

فصل ششم	سوال اول	گزینه‌ی D
	سوال دوم	گزینه‌ی C , D
	سوال سوم	گزینه‌ی B , C , D
	سوال چهارم	گزینه‌ی C
	سوال پنجم	گزینه‌ی B
	سوال ششم	گزینه‌ی C
	سوال هفتم	گزینه‌ی B , D
	سوال هشتم	گزینه‌ی A , D

فصل هشتم	سوال اول	گزینه‌ی C
	سوال دوم	گزینه‌ی A
	سوال سوم	گزینه‌ی D
	سوال چهارم	گزینه‌ی B
	سوال پنجم	گزینه‌ی A
	سوال ششم	گزینه‌ی C
	سوال هفتم	گزینه‌ی C
	سوال هشتم	گزینه‌ی D , E
	سوال نهم	گزینه‌ی B
	سوال دهم	گزینه‌ی D

فصل نهم	سوال اول	گزینه‌ی C
	سوال دوم	گزینه‌ی B
	سوال سوم	گزینه‌ی C
	سوال چهارم	گزینه‌ی B

www.takbook.com

	سوال پنجم	گزینه‌ی B
	سوال ششم	گزینه‌ی B
	سوال هفتم	گزینه‌ی E
	سوال هشتم	گزینه‌ی D
	سوال نهم	گزینه‌ی A
	سوال دهم	گزینه‌ی D

فصل دهم	سوال اول	گزینه‌ی D , E
	سوال دوم	گزینه‌ی A , B , C , F
	سوال سوم	گزینه‌ی C
	سوال چهارم	گزینه‌ی C , F
	سوال پنجم	گزینه‌ی B
	سوال ششم	گزینه‌ی C , D

فصل یازدهم	سوال اول	گزینه‌ی B
	سوال دوم	گزینه‌ی D
	سوال سوم	گزینه‌ی A , B
	سوال چهارم	گزینه‌ی D
	سوال پنجم	گزینه‌ی C
	سوال ششم	گزینه‌ی A , C
	سوال هفتم	گزینه‌ی B
	سوال هشتم	گزینه‌ی D
	سوال نهم	گزینه‌ی C

فصل دوازدهم	سوال اول	گزینه‌ی D
	سوال دوم	گزینه‌ی C

www.takbook.com

	سوال سوم	گزینه‌ی A
	سوال چهارم	گزینه‌ی C
	سوال پنجم	گزینه‌ی E , F
	سوال ششم	گزینه‌ی B
	سوال هفتم	گزینه‌ی D , E

فصل سیزدهم	سوال اول	گزینه‌ی B , D
	سوال دوم	گزینه‌ی A , C
	سوال سوم	گزینه‌ی D
	سوال چهارم	گزینه‌ی A , C
	سوال پنجم	گزینه‌ی A
	سوال ششم	گزینه‌ی B , D
	سوال هفتم	گزینه‌ی C

فصل چهاردهم	سوال اول	گزینه‌ی A
	سوال دوم	گزینه‌ی C
	سوال سوم	گزینه‌ی C
	سوال چهارم	گزینه‌ی A
	سوال پنجم	گزینه‌ی C , D
	سوال ششم	گزینه‌ی A , D
	سوال هفتم	گزینه‌ی D , E

www.takbook.com

واژه نامه

اعداد

10/100 یک مرجع کوتاه شده برای پورت‌های Ethernet که دارای سرعت‌های ۱۰ و ۱۰۰ مگابایت بر ثانیه است.

10/100/1000 یک مرجع کوتاه شده برای پورت‌های Ethernet که دارای سرعت‌های ۱۰ و ۱۰۰ و ۱۰۰۰ مگابایت بر ثانیه است.

10BASE-T نشان دهنده‌ی مشخصات کابل Ethernet با سرعت ۱۰ مگابایت است که اصولاً در کابل‌های سری 3,4,5 قرار دارد و دارای مسافت تقریبی ۱۰۰ متر یا ۳۲۸ پا است است و حداکثر طول آن ۱۰۰ متر است.

1000BASE-T نامی برای استاندارد IEEE Gigabit Ethernet که از چهار جفت سیم مسی تشکیل شده است و سرعت ۱ گیگابایت یا همان ۱۰۰۰ مگابایت را به ارمغان می‌آورد و تا ۱۰۰ متر می‌تواند باشد.

2-way state ارتباط با روترهای همسایه در پروتکل OSPF.

802.11a استاندارد شبکه‌های بی‌سیم با استفاده از طیف U-NII و رمزگذاری OFDM با سرعت ۵۴ مگابایت بر ثانیه.

802.11b استاندارد IEEE برای شبکه‌های بی‌سیم با استفاده از طیف ISM و رمزنگاری DSSS با سرعت ۱۱ مگابایت بر ثانیه.

802.11g استاندارد IEEE برای شبکه‌های بی‌سیم با استفاده از طیف ISM و رمزنگاری DSSS و OFDM با سرعت ۵۴ مگابایت بر ثانیه.

802.11n استاندارد IEEE برای شبکه‌های بی‌سیم با استفاده از طیف ISM و رمزنگاری OFDM با سرعت ۱۵۰ مگابایت بر ثانیه با سه آنتن مجزا.

802.1Q پروتکل استاندارد IEEE برای Trunking Vlan که شامل پروتکل RSTP نیز می‌شود.

802.1x An استاندارد IEEE که دسترسی میتنی بر پورت را برای دستگاه‌های سیمی و بی‌سیم تعریف می‌کند.

100BASE-T نامی برای استاندارد EEE Fast Ethernet که دارای دو جفت سیسم است و سرعت ان ۱۰۰ مگابایت بر رو ثانیه.

A

AAA از سه قسمت Authentication, Authorization, Accounting تشکیل شده است که کار احراز هویت، بررسی دسترسی و ثبت وقایع را انجام می‌دهد.

www.takbook.com

AAA server سروری که اطلاعات امنیتی را در اختیار دارد و خدمات مربوط به کاربر را ارائه می‌دهد مانند ورود به سیستم، احراز هویت، مجوز و حسابداری.

ABR مربوط به روتر Area Border که در OSPF کاربرد دارد.

Access Interface یک اصطلاح در طراحی شبکه است که به پورت‌های سوئیچ گفته می‌شود که دستگاه‌هایی مانند PC به آن متصل می‌شوند، یعنی دستگاه‌هایی که نیاز به استفاده از پورت Trunk ندارند.

Access layer در طراحی شبکه‌ی دانشگاهی یا شبکه‌ی campus به کار می‌رود و برای متصل شدن دستگاه‌های نهایی مانند سرور و دستگاه‌های کاربران کاربرد دارد.

Access Control Entry (ACE) یک خط در یک لیست کنترل دسترسی(ACL) .

Access interface یک اصطلاح در طراحی شبLAN ، که به یک Interface سوئیچ متصل به دستگاه های کاربر نهایی اشاره دارد و به گونه‌ای تنظیم شده است که از VLAN Trunking استفاده نکند.

Access layer در یک طراحی LAN دانشگاه ، سوئیچ‌هایی که مستقیماً به دستگاه‌های نقطه انتهایی (سرورها ، دستگاه‌های کاربر) متصل می‌شوند و همچنین به سوئیچ‌های لایه توزیع وصل می‌شوند.

Access link در Frame Relay به پیوند سریال فیزیکی به یک دستگاه DTE در Frame Relay اشاره دارد که معمولا سوئیچ و روتر را به یک سوئیچ Frame Relay متصل می‌کند.

Access link (WAN) پیوند فیزیکی بین Service Provider و مشتری که دسترسی به شبکه‌ی SP را به سایت مشتری فراهم می‌کند.

Access rate به سرعت ارسال بیت‌ها بر روی Access Link.

Accounting مربوط به قسمت AAA در بخش امنیت که برای ظبط عملکرد کاربران یا دستگاه مورد استفاده قرار می‌گیرد..

ACI بخش Application Centric Infrastructure (ACI) را بررسی کنید.

ACL یا Access control list که همان لیست کنترل دسترسی است و برای کنترل جریان بسته‌ها به کار می‌رود و از طریق روتر پیکربندی می‌شود.

Active Directory مجموعه محبوب سرویس احراز هویت و دایرکتوری مایکروسافت که بخشی از آن مربوط به تایید اعتبار **کاربر است**.

Agent یک سرویس نرافزاری کوچک و خاص که اصولاً برای نرم‌افزارهای بزرگ طراح می‌شود تا بتوانند اطلاعات و دسترسی‌هایی را به سیستم کاربر داشته باشند.

Agent-based architecture یک ابزار برای مدیریت پیکربندی یک نرم‌افزار است که در داخل دستگاه استفاده می‌شود.

Agentless architecture به معماری یک نرم‌افزار گفته می‌شود که نیاز به Agent در دستگاه دیگری نداشته باشد ولی در عوض از سایر روش‌های ارتباطی مانند SSH یا NETCONF استفاده می‌کند.

Amplification attack به یک حمله اشاره دارد که در آن با تولید و انعکاس حجم عظیمی از ترافیک به سمت قربانی باعث از کار افتادن شبکه قربانی می‌شود.

www.takbook.com

Ansible برای مدیریت دستگاه‌های شبکه به کار می‌رود، از یک معماری agentless (بدون نماینده) هم استفاده می‌کند.

Ansible template یک فایل متنی، به زبان Jinja2 ، که پیکربندی شده است، اما نام‌های متغیر را جایگزین مقادیر می‌کند و بعد از آن آنها را لیست می‌کند، بنابراین Ansible می‌تواند پیکربندی‌های استاندارد را برای چندین دستگاه از همان قالب ایجاد کند.

Antivirus نرم‌افزاری که فایل‌های در حال انتقال را رصد می‌کند تا به دنبال محتوایی باشد که شامل ویروس هستند.

Application Centric Infrastructure (ACI) راه حل SDN مرکز داده که شامل مفاهیم سیساست‌های کنترل کننده APIC است.

Enterprise Module (APIC-EM) نرم‌افزاری که در یک شبکه‌ی سازمانی برای دستگاه‌های سیسکو نقش کنترلر را بازی می‌کند.

Application Policy Infrastructure Controller (APIC) نرم‌افزاری که نقش کنترلر را ایفا می‌کند و برای استخراج Policy و Audit Log از آن استفاده می‌شود.

Application programming interface (API) یک مکانیزم نرم‌افزاری که اجزای یک نرم‌افزار را قادر می‌سازد تا با هم ارتباط برقرار کنند.

Application Visibility and Control (AVC) یک دستگاه فایروال با ویژگی‌های پیشرفته از جمله امکان اجرای بسیاری از ویژگی‌های امنیتی مرتبط در همان دستگاه فایروال (IPS، شناسایی بدافزار ، VPN)، همراه با بازرسی بسته‌ها با برنامه Application Visibility و کنترل (AVC) و امکان انجام URL فیلترینگ.

Application-specific integrated circuit (ASIC) مدارهای مجتمعی هستند که به منظور انجام عملیات خاص، طراحی و بهینه‌سازی شده‌اند . به عنوان مثال یک پردازنده که در گوشی موبایل مورد استفاده قرار می‌گیرد نمونه‌ای از این نوع تراشه‌ها است. استفاده از تراشه‌های ASIC به افزایش کارایی سیستم منتهی می‌شود. در مقابل، پردازنده‌ها با وجود انعطاف‌پذیری از قابلیت‌های لازم برخوردار نیستند . FPGAها راه حلی برای ایجاد یک سیستم با انعطاف‌پذیری بالا و کارایی مورد نیاز می‌باشند . در ASICهای اولیه از فناوری آرایه گیت استفاده می‌شد. اولین برنامه تجاری موفق در سال‌های ۱۹۸۱ و ۱۹۸۲ در رایانه‌های ۸ بیتی سری ZX اتفاق افتاد.

Address Resolution Protocol – ARP یک پروتکل اینترنتی که برای ارتباط آدرس IP و آدرس MAC کاربرد دارد که در RFC 826 تعریف شده است.

ARP ACL یک ویژگی در پیکربندی سوئیچ که جهت آدرس MAC و IP را تعریف می‌کند که می‌تواند به طور مستقیم برای فیلتر کردن استفاده شود.

www.takbook.com

ARP request یک پیغام ARP برای درخواست اطلاعات از میزبان دیگر در همان لینک پیوند داده است.

ARP table لیستی از آدرس‌های IP همسایگان در همان VLAN، به همراه آدرس‌های MAC آنها.

ASAv فایروال سیسکو که به صورت مجازی به جای سخت‌افزار سیسکو کار می‌کند و اصولاً در یک سرور ابری و در دیگر محیط‌های مجازی مورد استفاده قرار می‌گیرد.

Access Point (AP) یک دستگاه بی‌سیم که در یک منطقه‌ی جغرافیایی مشخص به مشتریان خدمات بی‌سیم ارائه می‌دهد.

Accounting یک قسمت از بحث امنیتی است که برای ذخیره کردن کارهایی که یک کاربر در شبکه انجام می‌دهد به کار می‌رود، مثلاً می‌توانیم مشاهده کنیم که کاربر چه تغییری در شبکه ایجاد کرده است.

Ad hoc network بحثی در وایرلس است که مربوط به خدمات IBSS است و باید این قسمت را مطالعه کنید.

Address block به مجموعه‌ای از آدرس‌های IPV4 گفته می‌شود که که اغلب برای CIDR تعریف می‌شود.

Adjacent-layer interaction به مفهوم ارتباط یک لایه با لایه مجاور خود است.

Administrative distance یک عدد مختص پروتکل‌های شبکه و شبکه‌های connected است.

ADSL یک فناوری که برای ارائه سرویس با پهنای باند بالا به مشتریان استفاده می‌شود و در حال حاضر هم بسیار گسترده در حال استفاده است.

All-nodes multicast address یک آدرس چند بخشی در IPV6 است، FF02::1 برای ارسال بسته‌ها به کلیه دستگاه‌های عضو شبکه‌ی محلی کاربرد دارد.

All-routers multicast مربوط به آدرس Multicast است که آدرس FF02 :: 2 برای ارسال اطلاعات به دستگاه‌ها کاربرد دارد.

Alternate port یک پورت جایگزین است درپروتکل RSTP یا Rapid Spanning Tree Protocol است که این پروتکل دارای شماره‌ی استاندارد IEEE 802.1w و این پروتکل با تغییراتی که بر روی آن ایجاد شده باعث شده سرعت کار بسیار افزایش پیدا کند و پیدا کردن LOOP و خرابی لینک‌ها به سرعت انجام شود.

Anycast address – Anycast آدرسی است برای انتخاب بهترین مسیر تا رسیدن به یک سرور و یا انتخاب یک سرور بین چند سرور یکسان که هزینه‌ی کمتری دارد.

Area Border Router (ABR) روتری است که در OSPF استفاده می‌شود و بین Area یا منطقه‌های مختلف برای تبادل اطلاعات قرار می‌گیرد.

ARP یا Address resolution protocol که هدف آن در شبکه پیدا کردن mac آدرس متناظر با هر IP آدرس است.

ARP table لیستی از آدرس‌های همسایه در یک VLAN به همراه آدرس MAC آنها که در حافظه نگهداری می‌شود.

www.takbook.com

ARPANET سازمان پروژه‌های تحقیقاتی پیشرفته شبکه که اولین شبکه سوئیچیگ بسته‌های اطلاعات در دنیا بود و پس از مدتی تبدیل به اینترنت جهانی شد.

ASBR این روتر کار انتقال اطلاعات از یک پروتکل یا یک دومین دیگر به داخل OSPF را انجام می‌دهد.

Asymmetric یکی از فناوری‌های دسترسی به اینترنت است، مانند DSL , cable , modems که نرخ آنتقال پائین دست از بالادست بالاتر است.

Authentication در حوزه‌ی امنیت استفاده می‌شود و فرآیندی برای تایید هویت اشخاص است که یک نمونه از آن سیستم AAA است.

Authentication server (AS) بر اساس بانک اطلاعاتی که از کاربران وجود دارد، کاربران یا مشتری را تایید اعبار می‌کند، در شبکه‌های بی‌سیسم سرور RADIUS این کار را انجام می‌دهد.

Authenticator یک سیستم مانند WLC است که به عنوان تایید کننده عمل می‌کند و دسترسی کاربران را به شبکه تایید می‌کند.

Authorization در حوزه‌ی امنیت به کار می‌رود و فرآیندی برای تعین حقوق دسترسی کاربران یا دستگاه خاص به شبکه است که این کار در سیستمی مانند AAA انجام می‌شود.

Autonegotiation برای اطمینان پیدا کردن دو گره یا نود برای ارتباط درست با یکدیگر.

Autonomous AP یک Access Point بی‌سیم که به صورت مستقل کار می‌کند و دارای یک BSS است و به DS متصل می‌شود.

Autonomous system به مجموعه‌ای از روترها که در یک منطقه قرار دارند، گفته می‌شود که روترها فقط در همان منطقه باهم در ارتباط هستند.

Auxiliary port یک پورت فیزیکی که بر روی روتر تعبیه شده و برای ارتباط از راه دور استفاده می‌شود.

(AAA)- authentication, authorization, accounting سروری که اطلاعات امنیتی را در اختیار دارد و خدمات مرتبط با ورود به سیستم کاربر، به‌ویژه احراز هویت، مجوز و حسابرسی را ارائه می‌دهد.

Authoritative DNS server سرور DNS که آدرس مربوط به یک نام دامنه (A Record) را برای آن دامنه لیست می‌کند.

Autonomous system number (ASN) عدد AS یا همان Autonomous System که با نام ASN هم شناخته می‌شود می‌تواند عددی بین ۰ تا ۶۵۵۳۵ باشد و در پروتکل‌های BGP و EIGRP مورد استفاده قرار می‌گیرد.

B

Backbone Area یا **Area0** ناحیه‌ای است که areaهای دیگر به وی متصل می‌شوند و تمام اطلاعات areaهای دیگر باید از این area عبور کند، پس این area به‌عنوان BackBone یا ستون فقرات شبکه OSPF شناخته می‌شود.

www.takbook.com

back-to-back link به ارتباط لینک سریال بین دو روتر اشاره دارد، که یک سر آن DTE و دیگری DCE است.

Backup designated router همه‌ی روترهای داخل یک Area، تمام اطلاعات و تغییرات را به روتر BR می‌فرستند و این روتر به دیگر روترها اعلام می‌کند و اگر این روتر خراب شود روتر جایگزین آن BDR یا backup designated router خواهد بود.

backup port در پروتکل RSTP استفاده می‌شود و به عنوان یک پورت پشتیبان عمل می‌کند که در صورت خرابی پورت اصلی این پورت شروع به کار می‌کند.

band طیف متفاوت فرکانس‌ها در وایرلس.

Bandwidth مرجع سرعت یک لینک یا خط در شبکه است .

basic service set (BSS) خدمات ارائه شده‌ی توسط یک Access Point به یک یا چند مشتری.

Basic service set identifier (BSSID) یک آدرس MAC منحصر به فرد که برای شناسایی Access Point استفاده می‌شود.

binary mask به Subnet آدرس IPV4 اشاره دارد که به عنوان یک شماره‌ی باینری ۳۲ بینی نوشته می‌شود.

blocking state در پروتکل STP عمل می‌کند و در آن هیچ پیام دریافتی پردازش و خارج نمی‌شود به جز پیام‌های STP .

BPDU یا Bridge protocol data unit نام عمومی برای پیام‌های پروتکل STP است.

BPDU Guard یکی از ویژگی‌های سوئیچ‌های سیسکو است که اگر فرد مهاجم بخواهد از طریق یک پورت سوئیچ به شبکه، بسته‌های BPDU بفرستد با اجرای این دستور در پورت مورد نظر اگر چنانچه سوئیچ به آن پورت متصل شود و بخواهد فریم BPDU ارسال کند، با فعال بود BPDU Guard، پورت مورد نظر خاموش خواهد شد.

Bridge ID (BID) یک شناسه‌ی ۸ بیتی برای سوئیچ‌ها است که در STP و RSTP استفاده می‌شود.

bridge protocol data unit یا BPDU

Broadcast address به طور کلی هر آدرسی که نماینده تمام دستگاه‌ها باشد می‌تواند به همه دستگاه‌ها پیام ارسال کند، مثلاً در آدرس مک، آدرس FFFF.FFFF.FFFF و در IPV4 آدرس 255.255.255.255 است.

Broadcast Domain که در آن یک دستگاه فرستنده یک کپی از داده‌هایی را که قصد ارسال در شبکه را دارد برای همه‌ی دستگاه‌های آن شبکه ارسال خواهد کرد.

Broadcast frame یک فریم Ethernet با معنی FFFF.FFFF.FFFF به آدرس مقصد ارسال شده است که این قاب باید به تمام میزبان‌های آن شبکه‌ی LAN تحویل داده شود.

Broadcast subnet هنگام subnet کردن کلاس A, B, C در قسمت CLASSFUL ارزش آن یک و در قسمت subnet broadcast هم ارزش عدد آن یکسان است.

brute-force attack در این روش مهاجم با استفاده از دیتابیسی از کلمه عبور، تلاش می‌کند رمز عبور سیستم را حدس بزند که البته با ایجاد سیاست، تعداد تلاش برای وارد کردن رمز عبور، این مورد حل می‌شود.

www.takbook.com

C

Cable Internet یک فناوری برای دسترسی به اینترنت است که به طور معمول از کابل تلوزیون با نام CATV استفاده می‌کند که برای و ارسال و دریافت داده و فیلم مناسب است.

CAPWAP یک استاندارد امنیتی است که برای ایجاد یک ارتباط امن بین AP و WLC کاربرد دارد.

cell یک مساحت جغرافیایی که توسط AP تحت پوشش قرار گرفته است و همچنین به عنوان basic service area شناخته می‌شود.

Centralized WLC deployment مربوط به بخش WLC است.

Certificate authority (CA) یک نهاد قابل اعتماد که گواهینامه‌های دیجیتال تولید و امضاء می‌کند.

Channel-group یک اصطلاح سیسکو است که در آن سوئیچ‌ها از دسته‌ای از لینک‌ها برای ارتباط با هم استفاده می‌کنند.

CIDR یا Class Less Inter-Domain Routing به عنوان IPهای Class Less شناخته می‌شوند، این دسته از IPها برای شرکت‌هایی که ارائه‌دهنده‌ی خدمات اینترنتی هستند(ISP) به کار می‌رود. برای این شبکه‌ها، مهم است که چه مقدار IP را به چه کسی می‌دهند.

CIDR mask اصطلاح دیگر برای Prefix mask است.

CIDR notation مربوط به موضوع Prefix است.

Cladding مربوط به فیبر نوری است که در لایه‌ی دوم قرار دارد که برای بازگرداندن نور به داخل هسته کاربرد دارد.

Classful addressing مفهومی در IPV4 است که یک آدرس IP را در شبکه تعریف می‌کند و شامل سه بخش network, subnet, و host است.

Classful IP network شبکه IPV4 کلاس A, B, C است که به دلیل قوانینی که دارد یک شبکه‌ی کلاسی نامیده می‌شوند.

Classful routing protocol اطلاعات Mask را به همراه Subnet ارسال نمی‌کند و در آن از VLSM پشتیبانی نمی‌شود.

Classless addressing مفهومی در IPV4 که یک آدرس IP در زیر شبکه را تعریف می‌کند که این آدرس شامل دو بخش Subnet و Host است.

Classless interdomain routing مربوط به آدرس‌دهی IPV4 است و یک استراتژی برای واگذاری آدرس جهانی برای حفظ اندازه‌ی IPV4 است.

Classless prefix طیف گسترده‌ای از آدرس‌های عمومی IPV4 که توسط CIDR تعریف شده است.

Classless prefix length mask یا طول پیشوند که هنگام تعریف یک پیشوند بدون کلاس استفاده می‌شود.

Classless routing protocol یکی از ویژگی‌های پروتکل مسیریابی است، پروتکل‌های مسیریابی Subnet Mask را در آپدیت‌های خود ارسال می‌کنند و در نتیجه هرگونه نیاز را برطرف می‌کنند.

www.takbook.com

CLI Command-line interface که واسطه‌ای بین کاربر و دستگاه است که کاربر را قادر می‌کند با دستگاه تعامل داشته باشد.

Clock rate به سرعت کابل سریال اشاره دارد.

Clock source دستگاهی که سایر دستگاه‌های موجود، سرعت خود را با استفاده از لینک‌های هم‌زمان با این دستگاه تنظیم می‌کنند.

Clocking روند دریافت سیگنال از طریق کابل یا از طریق پین‌های یک کابل سریال.

Cloud-based AP یک AP بی‌سیم که کاملاً شبیه به یک AP مستقل است، اما دارای صفحه مدیریتی و عملکرد کنترلی از طریق اینترنت است.

Cloud-based WLC deployment طراحی یک شبکه‌ی بی‌سیم که WLC را در مرکز شبکه قرا می‌دهد، و به عنوان یک ماشین مجازی در بخش ابر خصوصی یک مرکز داده قرار دارد.

Collapsed core design به شبکه‌ی دانشگاهی اشاره دارد که در آن از سوئیچ مرکزی استفاده نمی‌شود و در عوض از چندین سوئیچ در جای جای آن استفاده شده است.

Collision domain به مجموعه‌ای از فریم‌هایی که توسط چندین کارت شبکه در یک زمان ارسال می‌شود و باعث برخورد به هم می‌شوند گویند.

Command-line interface به توضیح CLI مراجعه کنید.

Configuration mode بخشی از نرم‌افزار Cisco IOS است که برای اجرای دستورات پیکربندی مورد استفاده قرار می‌گیرد.

Connected یک کد وضعیت است که توسط سوئیچ نشان داده می‌شود و وضعیت Interfaceها را مشخص می‌کند.

Console port سوکتی در روتر یا سوئیچ که برای پیکربندی اولیه IOS کاربرد دارد و اصولاً یک کابل آبی رنگ است.

Contiguous network توپولوژی شبکه‌ای که در آن Subnet شبکه‌ی X از Subnet شبکه‌ی دیگر جدا نمی‌شود.

Convergence مقدار زمانی که پروتکل‌ها به تغییرات در شبکه واکنش نشان می‌دهند که این واکنش‌ها می‌تواند در مورد از بین بردن مسیرهای اشتباه و ارائه بهترین مسیر در جدول Routing باشد.

core در کابل‌کشی فیبر نوری، سیلندر مرکزی کابل است و از فایبرگلاس ساخته شده است، و از طریق آن نور عبور می‌کند.

core design به شبکه‌ی دانشگاهی گفته می‌شود که سوئیچ‌های Access را به سوئیچ‌های distribution متصل می‌کند و سوئیچ‌های distribution به عنوان سوئیچ اصلی عمل می‌کند و به دستگاه‌های داخل شبکه خدمات ارائه می‌دهد.

Counter/CBC-MAC Protocol (CCMP) یک طرح امنیتی بی‌سیم مبتنی بر 802.11i از یک حالت AES برای رمزگذاری و از CBC-MAC برای یکپارچگی داده استفاده می‌کند.

www.takbook.com

Crossover cable برای ارتباط ۲ دستگاه شبیه به هم مثلاً برای ارتباط ۲ کامپیوتر باهم مورد استفاده قرار می‌گیرد، برای این کار باید یک سری تغییرات در هر دو طرف کابل انجام دهید.

CSMA/CD (Carrier Sense Multiple Access/Collision Avoidance) در شبکه‌های کامپیوتری، روش دسترسی چندگانه در شبکه‌های بی‌سیم است. نودی که قصد ارسال اطلاعات دارد باید مدت زمان مشخصی را به کانال گوش دهد و تشخیص دهد که آیا نود دیگری قصد ارسال اطلاعات بر روی کانال را در حوزه بی‌سیم مربوط به خودش دارد یا خیر. اگر کانال «آزاد» باشد، سپس نود اجازه می‌یابد تا فرایند ارسال را آغاز کند، اما اگر کانال «مشغول» باشد، نود مذکور فرایند ارسال را به زمان رندوم دیگری موکول می‌کند. به محض اینکه مبادله اطلاعات آغاز شد، باز این امکان وجود دارد که ارسال واقعی اطلاعات رخ ندهد.

CSU/DSU یک نوع دستگاه سخت‌افزاری مانند مودم که Frameهای شبکه LAN را به Frameهای شبکه WAN تبدیل می‌کند.

D

Data VLAN نوع دیگری از VLAN است که در شبکه و در کلایت و سرور مورد استفاده قرار می‌گیرد و همیشه در کنار VLAN Voice قرار دارد.

Database Description نوع بسته OSPF که توضیحات مختصری را در مورد LSDB ارئه می‌دهد.

DCE یا Data communications equipment از منظر لایه‌ی فیزیکی Clock را روی ارتباطات WAN ارئه می‌دهد.

DDN قسمت dotted-decimal notation بررسی شود.

Dead Interval در پروتکل OSPF یک تایمر برای هر همسایه وجود دارد که اگر روتر همسایه بسته‌ی Hello را دریافت نکند آن ارتباط با شکست مواجه خواهد شد.

Decimal mask یک mask زیر شبکه‌ی IPv4 که با علامت‌گذاری dotted-decimal نوشته شده است .مثلاً، 255.255.255.0.

de-encapsulation در سیستم‌هایی که داده‌ها را از طریق شبکه دریافت می‌کند، فرآیندی که در آن دستگاه هدرهای لایه پایین را تفسیر می‌کند و با پایان یافتن هر سربرگ، هدر را حذف می‌کند و PDU با لایه بعدی بالاتر را آشکار می‌کند.

default gateway/default router در یک میزبانIP ، آدرس IP برخی از روترهایی که در آن وجود دارد میزبان بسته‌هایی را ارسال می‌کند که آدرس مقصد بسته روی یک زیر شبکه غیر از زیر شبکه محلی باشد.

default mask به Mask استفاده شده در کلاس‌های A, B, C گفته می‌شود که ۲۵۵.۰.۰.۰ برای کلاس A و ۲۵۵.۲۵۵.۰.۰ برای کلاس B و ۲۵۵.۲۵۵.۲۵۵.۰ برای کلاس C است.

default route برای ارسال بسته‌ها به یک مسیر جدید که قابل شناسایی در شبکه‌ی فعلی نست.

default VLAN به VLAN شماره‌ی یک اشاره دارد.

www.takbook.com

switchport access vlan vlan-id interface یک دستور subcommand در سوئیچ سیسکو است و به صورت پیش‌فرض برای اختصاص دادن یک پورت به یک Interface کاربرد دارد.

designated port پورتی از سوئیچ است که به عنوان Forwarding انتخاب می‌شود و کار ارسال و دریافت اطلاعات را انجام می‌دهد.

designated router در شبکه‌های تحت OSPF، روتری تحت عنوان DR (Designated Router) وجود دارد که همه‌ی روترهای داخل یک Area، تمام اطلاعات و تغییرات را به این روتر می‌فرستند و این روتر به دیگر روترها این تغییرات را اعلام می‌کند.

DHCP یا Dynamic Host Configuration Protocol این سرویس به صورت پویا به همه کلاینت‌های موجود در شبکه آدرس IP اختصاص می‌دهد.

DHCP client یک سرویس در کلاینت‌ها است که برای دریافت آدرس IP، درخواست خود را به سرور DHCP ارسال می‌کنند.

Dijkstra Shortest Path First (SPF) algorithm یک الگوریتم link-state است که برای مسیریابی در پروتکل استفاده می‌شود و با تجزیه و تحلیل LSDB بهترین مسیر با کمترین هزینه را پیدا می‌کند.

directed broadcast address مربوط به broadcast address است.

disabled port در الگوریتم STP کاربرد دارد و این پورت غیرفعال شده است.

discarding state مربوط به وضعیت Interface در پروتکل RSTP است که در آن هیچ فریمی پردازش و ارسال نمی‌شود به استثنای پیام‌های RSTP.

discontiguous network به توپولوژی شبکه‌ای اشاره دارد که Subnet آن با Subnet شبکه‌ی دیگر متفاوت است.

distance vector به پروتکل‌هایی گفته می‌شود که فقط و فقط با روتر کناری خود در ارتباط هستند و تمام اطلاعات خود را به روتر کناری خود منتقل و دریافت می‌کنند و برای رسیدن به یک شبکه‌ی خاص از یک بردار خطی استفاده می‌کند.

distribution layer در طراحی شبکه‌ی دانشگاهی استفاده می‌شود که در آن سوئیچ‌هایی که به لایه‌ی دسترسی متصل می‌شوند به عنوان کارآمدترین وسیله برای اتصال لایه‌ی دسترسی به دیگر بخش‌های شبکه هستند.

distribution system (DS) به شبکه‌ی سیمی که به یک access Point متصل شده است و ترافیک را بین شبکه‌ی سیسمی و بی‌سیم حمل می‌کند گویند.

DNS یا Domain Name System سرویسی برای تبدیل اسم به IP و بلشکل است.

DNS Reply به بیغامی که در سرویس DNS در جواب درخواست کلاینت برای دریافت IP ارسال می‌شود گویند.

DNS Request پیامی که توسط یک کلاینت یا مشتری به سرور DNS ارسال می‌شود تا یک نام مشخص را که مربوط به یک ادرس خاص است درخواست کند.

www.takbook.com

dotted-decimal notation (DDN) مربوط به فرمت آدرس‌دهی در IPV4 است که در آن از نقطه برای جداسازی آدرس IP استفاده می‌کنند.

DSL modem دستگاهی که با استفاده از استانداردهای DSL به خط تلفن متصل می‌شود و جهت انتقال اطلاعات و دریافت داده استفاده می‌شود.

DTE یا Data terminal equipment که در روتر و بر روی پورت سریال فعال می‌شود.

dual stack یک حالت عملکردی که در هاست و روتر بر روی IPV4 و IPV6 اجرا می‌شود.

duplex mismatch زمانی که یک دستگاه از منطق full-duplex استفاده کند و دستگاه دیگری از half-duplex استفاده کند این مشکل به وجود می‌آید.

duplicate address detection (DAD) اصطلاحی است که در IPV6 استفاده می‌شود.

E

EAP Flexible Authentication by Secure Tunneling (EAP-FAST) احراز هویت سیسکو که مبتنی بر EAP است و از PAC به عنوان یک اعتبار برای احراز هویت خارجی و از یک تونل TLS برای احراز هویت استفاده می‌کند.

EAP Transport Layer Security (EAP-TLS) روشی برای احراز هویت که از گواهینامه‌ی دیجیتال برای این کار استفاده می‌کند که این گواهینامه هم در سرور قرار دارد و هم در کلاینت که ارتباط این دو هم از طریق یک تونل TLS است.

EIGRP یا Enhanced Interior Gateway Routing Protocol نسخه‌ی پیشرفته‌ی پروتکل IGRP است که ساخته شرکت سیسکو است که بسیار عملکرد خوبی در همگرایی دارد.

EIGRP version 6 این ورژن از پروتکل EIGRP در IPV6 کاربرد دارد.

embedded WLC deployment طراحی یک شبکه بی‌سیم که WLC را در لایه دسترسی قرار می‌دهد.

Enable mode یک Mode در روتر یا سوئیچ که در آن کاربر می‌تواند از قدرتمندترین دستورات برای تنظیم روتر یا سوئیچ استفاده کنید.

encapsulation واژه encapsulation را برای توصیف عملیات اضافه کردن headers و trailers در دیتا یا داده است.

encryption رمزنگاری داده با استفاده از الگوریتم خاص برای جلوگیری از دیدن اطلاعات توسط افراد ناشناس.

enterprise mode مربوط به استاندارد 8021x که نیاز به تایید اعتبار EAP برای WPA, WPA2, WPA3 است.

enterprise router یک روتر کامل با تمام امکانات مانند Route, Wireless Access Point و ... که نقش کلی را در شبکه بازی می‌کند.

www.takbook.com

error detection فرایند کشف خطا یک فریم سطح داده‌ی پیوند، که در طول زمان تغییر داشته است یا خیر، برای انتقال این فرآیند به طور معمول از یک قسمت Frame Check Sequence (FCS) در پیش پرده datalink استفاده می‌کند.

error disabled یک حالت برای Interface سوئیچ است که می‌تواند نتیجه‌ی یکی از ضعف‌های امنیتی سوئیچ باشد.

error recovery هنگامی که برخی از داده های انتقال یافته با موفقیت دریافت نشوند این داده‌ها را دوباره ارسال می‌کند تا با موفقیت دریافت شود.

EtherChannel با ایجاد گروهی از پورت‌های مورد نظر، باعث می‌شود که چند پورت به صورت یک پورت نمایش داده شود. با این کار باعث ایجاد Redundancy در سوئیچ شده و با قطع شدن یکی از کابل‌ها سوئیچ به کار خود ادامه می‌دهد.

EtherChannel Load Distribution انتخاب یک لینک ارتباطی در سوئیچ برای انتقال Frame در عملیات Etherchannel.

Ethernet یک استاندارد در شبکه‌ی LAN است.

Ethernet address یک عدد ۶۴ بیتی است که معمولاً به صورت 12-digit هگزادسیمال نوشته می‌شود و برای شناسایی گره‌های اترنت در شبکه به کار می‌رود.

Ethernet frame اصطلاحی که به هدر DataLink و Trailer اشاره دارد.

Ethernet Line Service (E-Line) یک سرویس carrier/metro است که توسط MEF تعریف شده است که یک اتصال نقطه به نقطه بین دو کلاینت را ارئه می‌دهد.

Ethernet link اصطلاح عمومی برای ارتباط دو گره در شبکه که البته مهم نیست از چه نوع کابل‌کشی استفاده کرده باشند.

Ethernet over MPLS (EoMPLS) اصطلاحی که به طور خاص به چگونگی ارائه خدمات اشاره دارد که می‌توانید از پروتکل MPLS برای ایجاد سرویس WAN استفاده کنید.

Ethernet port یک اصطلاح عمومی که برای ارتباط با هر گره است و به طور معمول در سوئیچ‌ها با نام NIC یا LAN شناخته شده و به آن کابل شبکه متصل می‌شود.

EtherType به یک field در Ethernet header اشاره دارد که این قسمت نوع بسته‌بندی یا همان encapsulated را مشخص می‌کند.

EUI-64 مربوط به IPV6 است که یک شناسه منحصر به فرد با طول ۶۴ بیت است.

extended ping یک دستور در IOS که در آن دستور پینگ علاوه بر IP مقصد گزینه‌های دیگری را هم می‌پذیرد.

extended service set (ESS) چندین Access Point که توسط یک سوئیچ اصلی به هم متصل می‌شوند.

Extensible Authentication Protocol (EAP) یک چارچوب تأیید هویت استاندارد که توسط انواع روشهای تأیید اعتبار استفاده می‌شود.

www.takbook.com

F

Fast Ethernet یک نام مشترک برای کلیه‌ی استانداردهایی که داده‌ها را حداکثر با سرعت 100 مگابایت انتقال می‌دهند.

fiber-optic cable نوعی از کابل‌کشی که در آن از فیبر شیشه‌ای به عنوان واسطه استفاده می‌کنند و از طریق آن می‌توان نور را انتقال داد.

filter به طور کلی، یک فرآیند یا دستگاهی که از ویژگی‌های خاصی مانند آدرس منبع، آدرس مقصد یا پروتکل استفاده می‌کند، و ترافیک شبکه را نمایش می دهد و تعیین می‌کند که آیا بر اساس معیارهای تعیین شده، می توانید آن ترافیک را به جلو هدایت کرد یا اینکه آن را از بین ببرد.

firewall دستگاه امنیتی که بسته‌های عبوری را بین قسمت‌های ایمن شبکه و نا امن هدایت و مدیریت می‌کند.

flash memory نوعی از حافظه‌ی دائمی برای خواندن و نوشتن است و از هیچ قسمت متحرکی در آن استفاده نمی‌شود و همین موضوع باعث شده است که اطلاعاتی که بر روی آن قرار می‌گیرد همیشه بدون مشکل حفظ شود و به مرور از بین نرود.

floating static route یک مسیر IP Static که از اولویت بالاتری به نسبت مسیرهای دیگر برخوردار است و اصولاً در شبکه‌های کوچک استفاده می‌شوند.

Forward ارسال یک فریم دریافت شده از Interface دیگر به یک مقصد خاص.

forward delay مربوط به زمان در پروتکل STP است و به طور پیش‌فرض ۱۵ ثانیه است و مشخص می‌کند تا چه زمانی یک Interface باید به اطلاعات دریافتی گوش دهد و آنها را یاد بگیرد.

forward route از دیدگاه یک میزبان به مسیری که یک بسته از آن میزبان به میزبان دیگر سفر می‌کند گویند.

forward secrecy یک روش تبادل کلید در پروتکل WPA3 است که از حمله‌ی مهاجمان جلوگیری می‌کند که در آن از Pre-shared Key استفاده می‌شود.

forwarding state حالتی است در STP و RSTP که در آن یک Interface بدون محدودیت کار خواهد کرد.

frame اصطلاحی که به هدر و trailer پیونددداده اشاره دارد که به علاوه آن عملیات encapsulated را بین هدر و Trailer انجام می‌دهد.

Frame Check Sequence یک فیلد که در بسیاری از Trailerهای پیوند داده وجود دارد و بخشی از فرآیند پیدا کردن خطا است.

full duplex به طور کلی به ارتباط دو طرفه‌ی دو دستگاه که می‌توانند همزمان داده‌ها را ارسال و دریافت کنند گویند.

full state در پروتکل OSPF کاربرد دارد و به بخش LSDB مربوط می‌شود.

full update مربوط به پروتکل‌های مسیریابی IP است که در آن پروتکل مسیریابی با بروزرسانی، تمام مسیرهای شناخته شده را لیست می‌کند.

www.takbook.com

fully adjacent مفهومی در OSPF است که در آن دو روتر همسایه در حالت کامل قرار گرفته‌اند و اطلاعات را به هم ارسال کرده‌اند.

fully adjacent neighbor به دو روتر همسایه اشاره دارد که این دو روتر LSDBهای خود را مستقیماً با هم ردوبدل کرده‌اند.

G

Galois/Counter Mode Protocol (GCMP) یک روش رمزگذاری قوی است که در مدل امنیتی بی‌سیم WPA3 استفاده می‌شود.

Gigabit Ethernet یک نام مشترک برای کلیه استانداردهای IEEE که داده‌ها را تا 1 گیگابایت بر ثانیه ارسال می‌کنند.

global routing prefix به یک مجموعه منحصر به فرد از IPهای ورژن 6 اشاره دارد که یک سازمان می‌تواند در شبکه‌ی خود استفاده کند.

global unicast address یک مجموعه از آدرس‌های IPV6 Unicast است که توسط سازمان‌های IANA/ICANN ثبت شده است و به ISPها داده می‌شود.

H

half duplex هرگونه ارتباط که در آن یک دستگاه به صورت یک طرفه داده ارسال کند.

HDLC – High-Level Data Link Control پروتکل لایه پیونددادهٔ که برای همگرایی ایجاد شده و توسط سازمان ISO ارائه شده است.

Hello (Multiple definitions) پروتکل مورد استفاده در روترهای OSPF که برای کشف، ایجاد و ارتباط با همسایه مورد استفاده قرار می‌گیرد، همچنین در پروتکل EIGRP استفاده می‌شود.

Hello BPDU در پروتکل STP و RSTP مورد استفاده قرار می‌گیرد و برای شناسایی bridge ID، فرستنده‌ی bridge ID و Cost است.

Hello Interval یک تایمر زمانی که در پروتکل EIGRP و OSPF مورد استفاده قرار می‌گیرد و مشخص می‌کند که روتر چند بار باید پیغام Hello ارسال کند.

Hello timer در پروتکل STP مورد استفاده قرار می‌گیرد و در آن سوئیچ اصلی یا root باید hello BPDU را ارسال کند.

history buffer در یک روتر یا سوئیچ سیسکو، چندین دستور آخر که کاربر در مد EXEC و configuration وارد می‌کند را در حافظه نگه می‌دارد و کاربر می‌تواند از آنها استفاده کند.

hop count همان متریک استفاده شده در پروتکل RIP است، که در در جدول روتینگ معیاری وجود دارد به نام متریک که تعداد روترهای سر راه برای رسیدن به شبکه موردنظر را مشخص می‌کند.

host به هر دستگاهی که از IP استفاده می‌کند گویند.

www.takbook.com

host address به آدرسی IP که به هر کارت شبکه‌ی کلاینت داده می‌شود می‌گویند.

host part اصطلاحی که برای توصیف بخشی از آدرس IPV4 مورد استفاده قرار می‌گیرد که برای شناسایی میزبان از یک Subnet است.

host route مسیری با Mask /32 که به واسطه‌ی آن یک آدرس برای یک هاست مشخص می‌شود.

hostname یک نام برای میزبان IP است.

Hub – Hubها دستگاه‌هایی هستند مانند سوئیچ با این تفاوت که یک ابزار ساده هستند بدون هیچ نوع مدیریتی همه ترافیک دریافتی را منتشر می‌کنند.

I

IANA سازمانی که کار اختصاص دادن اعداد در اینترنت را دارد، سازمانی که دارای حق واگذاری شماره‌هایی که در اینترنت کاربرد دارد است مثلاً آدرس‌های IPV4 و IPV6 و ....

ICANN یک شرکت اینتنرتی برای نام‌ها و شماره‌های اختصاصی است، این سازمان زیر مجموعه‌ی سازمان IANA است و برای نظارت بر واگذاری آدرس‌های عمومی IPV4 و IPV6 منصوب شده است.

ICMP یا Internet Control Message Protocol پروتکلی در لایه‌ی TCP/IP است که برای گزارش خطاها و اطلاعاتی در مورد بسته‌ی IP بکار می‌رود.

ICMP echo reply یک نوع پیام ICMP که به طور اختصاصی برای دستور PING استفاده شده و برای مشخص کردن اتصال در یک شبکه کاربرد دارد، این پیغام زمانی که دستور Ping پیغام Icmp echo را ارسال کرده است منتظر آن است.

ICMP echo request یک نوع پیام ICMP که به طور اختصاصی برای دستور PING استفاده شده و برای مشخص کردن اتصال در یک شبکه کاربرد دارد، با این دستور درخواست را به میزبان دیگر ارسال و منتظر جواب می‌نشیند.

IEEE موسسه مهندسان برق و الکترونیک است که یک سازمان حرفه‌ای است و یکی از فعالیت‌های آن ایجاد استانداردهای مختلف برای شبکه است.

IEEE 802.1 AD استاندارد IEEE که معادل آن عملکرد EtherChannel سیسکو است.

IEEE 802.11 استاندارد IEEE برای شبکه‌های بی‌سیم.

IEEE 802.1Q مربوط به پروتکل Trunking VLAN و یکی از استانداردهای IEEE و مربوط به Native VLAN است.

IEEE 802.2 استاندارد IEEE که زیر لایه‌ی LLC از پیوند داده را مشخص می‌کند.

IEEE 802.3 مجموعه‌ی از پروتکل‌های LAN که در شبکه‌ی امروزی شناخته می‌شود.

IEEE 802.3 AD استاندارد IEEE که معادل عملکرد Etherchannel در سیسکو است.

IETF سازمانی با عنوان کار گروه مهندسی اینترنت، IETF بعنوان سازمان اصلی که به صورت مستقیم بر روی استانداردهای جدید TCP/IP کار می‌کند.

www.takbook.com

inactivity timer مربوط به Timer جدول آدرس MAC سوئیچ است.

independent basic service set (IBSS) یک شبکه‌ی بی‌سیم بداهه است که بین دو یا چند دستگاه بدون AP یا BSS تشکیل می‌شود و همچنین به عنوان یک شبکه‌ی Ad Hoc شناخته می‌شود.

infrastructure mode حالت operating mode در AP که یک BSS را برای مشتری‌های بی‌سیم فراهم می‌کند.

Integrated Services Router (ISR) به روترهای ISR مراجعه کنید.

interface bandwidth در OSPF کاربرد دارد و برای محاسبه‌ی هزینه‌ی متریک در یک Interface استفاده می‌شود.

interface-local scope مفهومی در IPV6 است که بسته‌های ارسال شده به یک آدرس، با استفاده از این محدودیت نباید از رابط فیزیکی خارج شود و باید در درون میزبان فرستنده نگه داشته شود.

interior gateway protocol (IGP) یک روتینگ پروتکل است که برای مسیریابی در یک سیستم مستقل طراحی شده است.

interior routing protocol مترادف پروتکل interior gateway است.

Internal Border Gateway Protocol (iBGP) استفاده از روتینگ پروتکل BGP بین دو روتر در ASN یکسان با قواعد متفاوت در مقایسه با BGP خارجی.

internal router مفهومی در OSPF است که یک روتر با تمام Interfaceها در همان Area قرار دارد.

Internetwork Operating System سیستم‌عامل سوئیچ‌ها و روترها که اکثر ویژگی‌های روتر و سوئیچ را در اختیار ما قرار می‌دهند.

Inter-Switch Link (ISL) پروتکل Trunking VLAN اختصاصی شرکت سیسکو که سال‌ها پیش 802.1q را پیش می‌برد.

IP پروتکل اینترنت، پروتکل لایه‌ی شبکه در پشته‌ی TCP / IP.

IP address (IP version 4) یک آدرس ۳۲ بیتی است که به میزبان‌ها داده می‌شود، هر آدرس شامل یک Network Number، Subnet Number و Host Number است.

IP address (IP version 6) یک آدرس ۱۲۸ بیتی است که به میزبان‌ها اختصاص داده می‌شود، این سری از IPها بسیار گسترده هستند و تعداد زیادی از میزبان‌ها را پشتیبانی می‌کنند.

IP subnet زیربخش‌های یک شبکه‌ی کلاس A,B,C که توسط مدیر شبکه پیکربندی شده است، زیر شبکه‌ها این امکان را می‌دهند، به جای استفاده از چندین شبکه از یک شبکه کلاس A,B,C استفاده کنید.

IP version 4 پروتکل اینترنت نسخه ۴ یا به اختصار IPv4، چهارمین بازبینی پروتکل اینترنت (IP) و نخستین نسخه‌ایست که به گستردگی به کارگرفته شد. این نسخه از پروتکل در هسته روش‌های شبکه‌بندی بر پایه استانداردها در اینترنت است. هرچند به کارگیری نسخه ششم پروتکل اینترنت (IPv6) تا تاریخ ۲۰۱۰ آغاز شده‌است، IPv4 پراستفاده‌ترین پروتکل اینترنت است.

IP version 6 پروتکل اینترنت نسخه ۶ یا به اختصار IPv6 جدیدترین نسخه پروتکل اینترنت (Internet Protocol)است که ارتباط‌های اینترنتی بر پایه آن شکل می‌گیرد. این نسخه قرار است جای نسخه ۴ این پروتکل (IPv4) را که هم‌اکنون استفاده می‌شود را بگیرد.

www.takbook.com

IPv4 address exhaustion فرآیندی که برای IPV4 Public استفاده می‌شود و به آدرس‌های Public جهانی اشاره دارد که روز به روز در حال اتمام هستند و در حال حاضر هم به اتمام رسیده‌اند.
IPv6 address scope به مفهوم چگونگی ارسال بسته‌های IPV6 توسط میزبان‌ها و روترها در یک شبکه‌ی IPV6 اشاره دارد که شامل interface-local, link-local, site-local و... است.
IPv6 administrative distance معیار و ملاکی است برای انتخاب یک پروتکل از بین پروتکل‌های مختلف در یک شبکه، مثلاً اگر به یک روتر از دو طرف اطلاعات برسد و یکی از این طرف‌ها Rip با AD 120 و طرف دیگر با IGRP با AD 100 است. برای انتخاب یکی از این مسیرها، مسیری که AD پایین‌تر دارد، انتخاب می‌شود (AD مخفف کلمه‌ی Administrative Distance است) و اطلاعات را از همان مسیر دریافت می‌کند. AD مربوط به static route که به صورت دستی وارد می‌کردیم 1 است.
IPv6 host route یک مسیر با MASK /128 که به کمک این MASK مسیری را برای یک آدرس هاست IPV6 نشان می‌دهد.
IPv6 local route مسیری که به جدول مسیریابی IPV6 اضافه شده است برای آدرس IP یک Inetrafce روتر با MASK /128 .
IPv6 neighbor table معادل IPV6 در جدول ARP است. جدولی که آدرس‌های IPV6 میزبان‌ها را در همان لینک به همراه آدرس‌های MAC مطابق با آنها لیست می‌کند.
ISL یک پیوند بین سوئیچ، که یک پروتکل اختصاصی سیسکو است و اطلاعات VLAN را به عنوان جریان ترافیک بین سوئیچ و روتر حفظ می‌کند.
ISO که معادل International Organization for Standardization (سازمان بین‌المللی استانداردسازی) است و مسئولیت طیف گسترده‌ای از استانداردها ازجمله استانداردهای شبکه را بر عهده دارد، ISO مدل مرجع OSI را توسعه داده است که یک مدل مرجع شبکه است.

K–L

keepalive ویژگی اختصاصی روترهای سیسکو که در آن، روتر پیام‌ها را به صورت دوره‌ای به عنوان وسیله‌ای برای اطلاع روتر همسایه می‌فرستد که مشخص می‌شود که روتر اول هنوز در حال کار است.
known unicast frame یک Frame اترنت که آدرس MAC مقصد آن در جدول آدرس MAC سوئیچ ذکر شده است، بنابراین سوئیچ آن Frame را از طریق Interface مشخص شده در جدول، ارسال می‌کنند.
L2PDU واحد داده‌ی پروتکل لایه‌ی دوم که اغلب frame نامیده می‌شود.

www.takbook.com

L3PDU واحد داده پروتکل لایه ۳ .اغلب Packet نامیده می‌شود .داده‌های گردآوری شده توسط پروتکل Layer 3 شامل هدرهای Layer 3 و داده‌های لایه بالا کپسوله شده است ، اما شامل هدرها و تریلرهای لایه پایین‌تر نمی‌شوند.

L4PDU واحد داده پروتکل لایه ۴. اغلب segment نامیده می‌شود. داده‌های گردآوری شده توسط پروتکل Layer 4، شامل هدرهای Layer 4 و داده های لایه بالا کپسوله شده ، اما شامل هدر و تریلر سطح پائین نیست.

LACP یا Link Aggregation Control Protocol یک پروتکل پیام‌رسانی است که توسط IEEE 802.3ad تعریف شده است و دو دستگاه همسایه را قادر می‌سازد تا بتوانند بفهمند که چند لینک موازی متصل به هم دارند و سپس می‌توانند تصمیم بگیرند که کدام پیوندها را در یک EtherChannel قرار دهند.

Layer 2 EtherChannel (L2 EtherChannel) یک EtherChannel که به عنوان یکی از پورت‌های سوئیچ در لایه‌ی دوم عمل می‌کند.

Layer 3 EtherChannel (L3 EtherChannel) یک EtherChannel که به عنوان یک درگاه مسیریابی عمل می‌کند، و به همین ترتیب با استفاده از منطق حمل و نقل Layer 3 سوئیچ استفاده می‌شود.

Layer 3 protocol پروتکلی که دارای خصوصیات لایه‌ی سوم مدل OSI است و آدرس‌دهی و مسیریابی در شبکه را تعریف می‌کند، IPV4 و IPV6 پروتکل‌های لایه‌ی سوم هستند.

learning فرایندی که توسط سوئیچ‌ها برای کشف آدرس‌های MAC استفاده می‌شود.

learning state حالت یک پورت در STP است.

leased line این خطوط که توسط مخابرات اجاره داده می‌شود، یک خطوط امن (Secure) محسوب می‌شود و مانند خط تلفن پایدار و ثابت است و پهنای باند آن حدود ۴۵ مگابایت است.

lightweight AP یک AP بی‌سیم که به کاربران سرویس ارائه می‌دهد ولی برای کنترل آن باید به یک کنترل‌کننده‌ی بی‌سیم متصل شود.

Lightweight EAP (LEAP) یک روش امنیتی در سیسکو است که در این روش کاربر و سرور هر دو همدیگر را احراز هویت می‌کنند، یعنی به این صورت که کاربر یک رشته مشخص را به سرور ارسال می‌کند و سرور آن رشته را Shared Secret خود هش می‌کند و برای کاربر ارسال می‌کند، اگر رشته مورد نظر با Shared Secret کاربر که قبلاً برای آن مشخص شده یکی باشد سرور مورد تایید کاربر قرار می‌گیرد.

link state این نوع پروتکل، یک ویژگی عمده دارند و آن‌هم این است که تصویر کلی از شبکه یا همان گراف کامل از شبکه را دارند، یعنی هر روتر دارای پروتکل‌های Link State، خود را به عنوان ریشه‌ی درخت و بقیه را به عنوان شاخه و برگ حساب می‌کنند، اما بدون دور است و به این ترتیب یک تصویر کلی از شبکه را دارد و از روی همین گراف، بهترین و کوتاه‌ترین مسیر تا شبکه‌ی دیگر را محاسبه و انتخاب می‌کند.

www.takbook.com

link-local address یک آدرس IPV6 از نوع Unicast است که با FE80 شروع می‌شود.

link-local multicast address یک آدرس IPV6 از نوع Multicast که با FF02 شروع می‌شود.

link-state advertisement (LSA) OSPF روترها برای تبلیغ جداول خود از LSAهای مختلف استفاده می‌کند.

link-state database (LSDB) روترهایی که در پروتکل OSPF قرار دارند دارای یک دیتابیس با عنوان link-state database یا LSDB هستند.

Link-State Request یک بسته در OSPF که برای درخواست یک روتر همسایه برای ارسال یک LSA خاص استفاده می‌شود.

Link-State Update بسته OSPF که برای ارسال LSA به روتر همسایه استفاده می‌شود.

listening state یکی از وضعیت‌های پورد در STP را نشان می‌دهد که از حالت Blocking به حالت forwarding می‌رود.

local broadcast IP address مربوط به آدرس 255.255.255.255 در IPV4 که به عنوان یک آدرس Broadcast شناخته می‌شود، توجه داشته باشید که روترها این نوع بسته‌ها را ارسال نمی‌کنند.

local mode حالت پیش‌فرض یک برنامه Cisco lightweight در Access Point که می‌تواند چند BSS را در چند کانال خاص ارائه دهد.

local route مسیری که به جدول مسیریابی روتر اضافه شده است که شامل نام Interface و آدرس IPV4 با ماسک 32/ است.

M

MAC یا Media Access Control که برای شبکه‌های اترنت تعریف شده است و استاندارد آن IEEE 802.3 است.

MAC address یک آدرس لایه‌ی پیوند داده است که برای هر دستگاهی که دارای یک کارت شبکه است تعلق می‌گیرد. این آدرس‌ها با نام MAC و دارای ۶ بایت هستند و توسط سازمان IEEE کنترل می‌شوند، همچنین به عنوان یک آدرس سخت افزاری، یک آدرس لایه MAC و یک آدرس فیزیکی شناخته می‌شود.

MAC address table یک جدول که در سوئیچ لایه‌ی دوم کاربرد دارد که در آن آدرس‌های MAC دریافتی وارد شده و سوئیچ بر اساس آن تصمیم می‌گیرد اطلاعات را به کدام آدرس ارسال کند، این همان تفاوت سوئیچ و هاب است.

MaxAge یک تایمر در پروتکل STP، که سوئیچ وقتی بسته‌ی Hellos را از سوئیچ root دریافت نمی‌کند چقدر باید صبر کند.

maximum paths در CISCO IOS به تعداد مسیرهای بر سر راه بر اساس هزینه اشاره دارد.

www.takbook.com

MD5 hash یک الگوریتم خاص ریاضی که برای استفاده در پروتکل‌های امنیتی مورد استفاده قرار می‌گیرد که روترها و سوئیچ‌ها برای ایمن کردن ارتباطات خود از این الگوریتم استفاده می‌کنند.

media access control (MAC) layer در لایه دوم مورد استفاده قرار می‌گیرد و می‌توان بین کنترلر LAN بی‌سیم و یک AP از آن استفاده کرد تا یک معماری split-MAC ایجاد شود.

mesh network مربوط به شبکه‌ی بی‌سیم است و در یک منطقه‌ی بزرگ بدون استفاده از کابل‌کشی استفاده می‌شود.

message integrity check (MIC) یک ویژگی برای تشخیص دستکاری در محتویات یک Fram است.

message of the day یک نوع banner که می‌توان در هنگام ورود به روتر و سوئیچ سیسکو تعریف شود.

metric یک واحد اندازه‌گیری که توسط الگوریتم‌های مسیریابی مورد استفاده قرار می‌گیرد و برای تعیین بهترین مسیر برای استفاده از ترافیک برای رسیدن به یک مقصد خاص است.

Mobility Express WLC deployment مربوط به طراحی شبکه‌ی بی‌سیم در ارتباط WLC با یک AP .

Multiarea در OSPF ورژن ۲ و ۳ کاربرد دارد و مربوط به ایجاد چندین Area است.

Multilayer switch به سوئیچی که توابع مسیریابی در لایه‌ی سوم را انجام می‌دهد.

Multimode fiber نوعی کابل فیبر نوری که به خوبی با فرستنده‌هایی مانند LED کار می‌کند که چندین زاویه نور را به هسته کابل ساطع می‌کنند، این نوع کابل دارای هسته‌ی بزرگتر هستند.

N

Name Resolution فرآیندی که یک میزبان IP، آدرس IP مربوط به یک نام میزبان را کشف می‌کند گویند، اغلب شامل ارسال درخواست DNS به سرور DNS است.

Name server سروری متصل به شبکه که برای شناسایی نام و آدرس IP به کار می‌رود.

NAT یا Network Address Translation مکانیزمی برای کاهش نیاز به IP آدرس Valid که در دنیای اینترنت اعتبار دارد، به این صورت که یک شرکت با داشتن تنها یک آدرس Valid می‌تواند با استفاده از این سرویس کل شبکه‌ی داخلی خود را به اینترنت متصل کند.

Native VLAN وقتی چندین سوئیچ را با پروتکل 802.1Q، Trunk می‌کنید در زمان انتقال بین سوئیچ‌ها روی Vlan 1 هم برچسب‌گذاری می‌شود و همین کار باعث استفاده‌ی بیش از حد از پهنای باند شبکه می‌شود و برای جلوگیری از این کار باید روی پورتی که Trunk شده است، native VLAN را فعال کنیم.

Neighbor در پروتکل‌های مسیریابی به روتری که یک روتر با آن تصمیم دارد مبادله اطلاعات را انجام دهد گویند.

www.takbook.com

Neighbor Advertisement (NA) پیامی که توسط پروتکل کشف همسایه **IPv6 (NDP)** تعریف شده است، برای اعلام آدرس MAC میزبان به سایر همسایگان استفاده می‌شود.

Neighbor Discovery Protocol (NDP) بخشی از مجموعه پروتکل‌های IPv6 است که برای کشف و تبادل اطلاعات در مورد دستگاه‌های موجود در همان زیر شبکه (همسایگان) استفاده می‌شود. به طور خاص، جایگزین پروتکل IPv4 ARP است.

Neighbor Solicitation (NS) پیامی که توسط پروتکل کشف همسایه IPv6 (NDP) تعریف شده است، برای درخواست از همسایه برای پاسخ دادن به یک آگهی همسایه، که در آن آدرس MAC همسایه وجود دارد ، پاسخ می دهد.

Neighbor table مربوط به پروتکل‌های OSPF و EIGRP که لیستی از روترهایی که به وضعیت همسایه رسیده‌اند.

Network broadcast address در IPv4، یک آدرس خاص در هر شبکه وجود دارد که می‌تواند برای پخش یک بسته در کلیه میزبان‌ها در همان شبکه استفاده شود مانند 10.255.255.255 که این آدرس یک آدرس Broadcast برای شبکه‌ی 10.0.0.0 است.

Network ID شماره‌ای که یک شبکه‌ی IPV4 را مشخص می‌کند، با استفاده از یک علامت اعشاری (نقطه) کلاس هر شبکه را مشخص می‌کنیم.

network interface card (NIC) به کارت شبکه در هر سیستم گفته می‌شود که گاهی اوقات به صورت یک کارت خارجی استفاده می‌شود و یا بر روی مادربرد تعبیه می‌شود.

Network LSA - OSPF برای تبلیغ جداول خود از LSAهای مختلف استفاده می‌کند که این LSAها دارای نماد خاصی در جدول مسیریابی هستند، هر اطلاعاتی که از طریق OSPF به روترهای دیگر اعلام می‌شود به اصطلاح Advertise می‌شود، دارای نوع خاصی است که در header پروتکل از بیت نهم تا شانزدهم به آن اختصاص یافته‌است.

Network number عددی که از نشان‌های اعشاری (نقطه) استفاده می‌کند مانند آدرس‌های IP .

Networking model یک اصطلاح عمومی است که به هر مجموعه پروتکل و استانداردهای جمع آوری شده در یک گروه‌بندی جامع که در صورت رعایت دستگاه‌های موجود در یک شبکه ، امکان ارتباط با همه دستگاه‌ها را می‌دهد، مانند TCP/IP و OSI.

NVRAM یا رم غیر ولتاژ، نوعی از حافظه با دسترسی تصادفی (RAM) که حتی در صورت قطع برق، محتویات خود را حفظ می‌کند.

O

www.takbook.com

open authentication یک روش احراز هویت ۸۰۲.۱۱ که به مشتریان این امکان را می‌دهد بدون داشتن هیچ‌گونه اعتبارنامه‌ای ، با AP ارتباط برقرار کنند.
Organization-local scope مربوط به IPV6 که بسته‌های ارسالی به یک آدرس با استفاده از این محدودیت فقط باید در شبکه داخلی سازمان ارسال شوند.

OSI این مدل برگرفته از کلمه‌ی Open System Interconnection است و برای ارتباط بین دو کامپیوتر مبدأ و مقصد به کار می‌رود. این مدل در سال ۱۹۸۰ توسط سازمان ISO طراحی و پیاده‌سازی شده است و طبق سالیان متوالی تغییراتی روی آن صورت گرفته است، هرچند که همان ساختار اصلی خود را حفظ کرده است.

OSPF پروتکل OSPF(Open Shortest Patch First) یک پروتکل آزاد است و مختص شرکت خاصی نیست و توسط سازمان IETF در سال ۱۹۸۸ نوشته شده است، مانند Eigrp نیست که فقط در روترهای سیسکو قابل اجرا باشد، بلکه در تمام روترهای شرکت‌های مختلف کاربرد دارد.
OSPF version 2 نسخه‌ای از پروتکل OSPF که مختص IPV4 است و نه IPV6 و حدوداً ۲۱ سال است که در حال استفاده است.
OSPF version 3 نسخه‌ی سوم پروتکل OSPF که برای IPV6 طراحی شده است.

P

Packet یک گروه‌بندی منطقی از بایت‌ها که شامل هدر لایه شبکه و داده‌های Encapsulated است، اما بطور خاص هیچ هدر و پیش پرده‌ای را در زیر لایه شبکه قرار نمی‌دهد.
PagP پروتکل PAgP که از ساخته‌های سیسکو است، برای ارتباط دو سوئیچ که EtherChannel روی آن‌ها اجرا شده است، به کار می‌رود.
Partial mesh توپولوژی شبکه‌ای که در آن بیش از دو دستگاه می‌توانند از نظر فیزیکی با هم ارتباط برقرار کنند ولی حتماً نباید این ارتباط به صورت مستقیم باشد.
passive interface یکی از راه‌های که می‌توانید بار کاری بر روی روتر را سبک‌تر کنید این است که بر روی یک Inteeface که نیاز نیست در یک شبکه مانند OSPF فعالیت کند بهتر است قابلیت Hello Packet آن را غیرفعال کنیم که برای این کار باید passive interface را بر روی پورت فعال کرد.
patch cable یک کابل اترنت کوتاه که دو سر آن سوکت RJ45 زده شده است و اصولاً برای ارتباط داخل رک و برای سرور، روتر، سوئیچ و ... استفاده می‌شود.
PDU یا Protocol data unit یک اصطلاح در OSI که به طور کلی به گروه‌بندی اطلاعات توسط یک لایه‌ی خاص مدل OSI اشاره دارد.

www.takbook.com

periodic update مربوط به پروتکل‌های مسیریابی است که در آن بروزرسانی‌ها به صورت منظم در یک زمان مشخص برای دیگر روترها تبلیغ می‌شود، که این ویژگی در پروتکل‌های مسیریابی distance vector کاربرد دارد.

personal mode استفاده از کلید Pre-shared در WPA, WPA2 و WPA3.

ping دستوری برای مشخص کردن ارتباط با یک هاست در شبکه و یا اینترنت که مربوط به پروتکل ICMP است.

Port در TCP و UDP عددی منحصر به فرد وجود دارد که مربوط به سرویس و یا برنامه‌ی خاصی است و از آن برای ارتباط در شبکه استفاده می‌شود.

PortChannel به مجموع لینک‌ها که می‌توانند در یک زمان بین دو سوئیچ برقرار شوند گویند، یعنی اینکه به جای داشتن یک لینک از چند لینک همزمان استفاده می‌شود و اگر یکی از لینک‌ها خراب شود ارتباط بین دو سوئیچ قطع نخواهد شد.

PortFast یک ویژگی در پروتکل STP که اگر فعال شود سریعاً پورت به حالت بی‌درنگ می‌رود و از حالت‌های listening و learning صرفه‌نظر می‌کند.

Prefix (prefix ID) در IPV6 برای جداکردن NET ID از HOST ID به کار می‌رود و در IPV4 هم رنج IP را مشخص می‌کند.

prefix length در IPv6 ، تعداد بیت‌های پیشوند IPv6 است.

prefix mask اصطلاحی برای توصیف یک Subnet MASK در IPv4 است با یک (/) نمایش داده می‌شود و به دنبال آن یک عدد اعشاری است، عدد اعشاری تعداد باینری‌های یک MASK است.

spanning-tree vlan x root {primary | secondary} این دستور باعث می‌شود تا سوئیچ یک تنظیم Priority جدید را انتخاب کند که این کار باعث می‌شود سوئیچ تبدیل به Root Switch در شبکه شود.

Private addresses آدرس‌های IP در شبکه A، B و C که در سازمانهای خصوصی مورد استفاده قرار می‌گیرند و در دنیای اینترنت اعتباری ندارند.

Private IP network هر یک از شبکه‌های IPv4 کلاس A، B، یا C مطابق با RFC 1918 تعریف شده ، برای استفاده در داخل یک شرکت در نظر گرفته شده‌اند اما به عنوان شبکه‌های IP عمومی استفاده نمی‌شود.

Protected access credential (PAC) داده‌های ویژه‌ای که به عنوان اعتبار احرازهویت در EAP-FAST مورد استفاده قرار می‌گیرند.

Protected EAP (PEAP) روشی برای احراز هویت که از یک گواهی در AS برای احراز هویت خارجی و یک تونل TLS برای احراز هویت داخلی استفاده می‌کند. مشتریان می‌توانند اعتبار خود را از طریق MS-CHAPv2 یا GTC تهیه کنند.

Protected Management Frame (PMF) سرویس ارائه شده توسط WPA3 که از مجموعه‌ای از Frameها و مدیریت قدرتمند ۸۰۲.۱۱ محافظت می‌کند ، برای جلوگیری از فریب کارکردهای AP.

www.takbook.com

public IP address آدرس IP که بخشی از شماره شبکه ثبت شده است که توسط آژانس IANA به سازمان‌ها اختصاص داده می‌شود و فقط همان سازمان باید از آن رنج آدرس استفاده کند.

Public IP network به هر شبکه‌ی IPV4 که شامل کلاس‌های A، B، C هستند که به یک سازمان اختصاص داده شده است به طوری که آدرس‌ها در شبکه از طریق اینترنت در دسترس هستند و می‌توان از طریق اینترنت بسته‌ها را ارسال کرد.

Public Key Infrastructure (PKI) یک سیستم Enterprise که گواهی‌های دیجیتالی را برای تأیید اعتبار مشتری ایجاد و ابطال می‌کند، گزینه PVST And STP در سوئیچ‌های سیسکو که نمونه ای از این دست هستند.

Q–R

Quartet مجموعه‌ای از چهار رقم Hex در یک آدرس IPV6 .

RADIUS server یک سرور برای تأیید اعتبار،که از 802.1x برای تأیید اعتبار مشتریهای بی سیم استفاده می‌کند.

RAM یا Random-access memory یک حافظه‌ی دسترسی تصادفی، نوعی از حافظه فرار که توسط یک ریزپردازنده قابل خواندن و نوشتن است.

Rapid PVST+ گزینه‌ای در STP است و در سوئیچ‌های سیسکو استفاده می‌شود که نمونه ای از RSTP را برای هر VLAN ایجاد می‌کند و اختصاصی سیسکو است.

Rapid Spanning Tree Protocol (RSTP) در استاندارد IEEE 802.Iw تعریف شده است و یک نسخه‌ی بهبود یافته از پروتکل STP را تعریف می‌کند که خیلی بهتر و سریعتر از STP استاندارد 802.Id است.

Reference bandwidth در OSPF ، یک مقدار قابل تنظیم برای فرآیند مسیریابیOSPF است که هنگام محاسبه متریک استفاده می‌شود.

Regional Internet Registry یک سازمان برای مدیریت جغرافیایی آدرس IPV4 در سطح جهان.

Repeater A دستگاهی که سیگنال‌های دریافتی را تکرار و دوباره انتقال می‌دهد، که می‌تواند یک منطقه بی‌سیم گسترده را پوشش دهد.

Reverse route از دیدگاه میزبان، برای بسته‌هایی که از میزبان دیگر به این میزبان ارسال می‌شود را گویند.

RFC یا Request for Comments سندی که به عنوان وسیله اصلی برای برقراری اطلاعات در مورد پروتکل‌های TCP / IP استفاده می‌شود. برخی RFCها توسط گروه معماری اینترنت (IAB) به عنوان استاندارد اینترنت تعیین می‌شوند و برخی دیگر اطلاعاتی هستند.

www.takbook.com

RIP پروتکل اطلاعات مسیریابی، پروتکل interior gateway (IGP) که از منطق distance vector و تعداد روترهای در سر راه به عنوان متریک استفاده می‌کند. RIP نسخه ۲ (RIPv2) جایگزین نسخه قدیمی RIP (RIPv1) 1 شد، و RIPv2 از ویژگیهای بیشتری از جمله پشتیبانی از VLSM بهره می‌برد.

RJ-45 یک نوع اتصال دهنده‌ی کابل که مورد استفاده برای کابل‌کشی شبکه است. شبیه به اتصال RJ-11 است که برای سیم‌کشی تلفن در خانه‌ها استفاده می‌شود. RJ-45 امکان اتصال هشت سیم را فراهم می‌کند.

roaming فرایندی که یک مشتری بی‌سیم برای تغییر مکان از یک AP به AP دیگر در منطقه دیگر استفاده می‌کند.

ROM یا Read-only memory نوعی حافظه غیر فرار که توسط ریزپردازنده قابل خواندن است اما نمی‌توان روی آن بنویسد.

ROMMON یک نام کوتاه‌تر برای ROM Monitor است، که یک سیستم‌عامل سطح پایین است که می تواند برای تعمیر و نگهداری، اگر مورد نیاز شد در روترهای Cisco بارگیری شود، از جمله بازیابی رمز عبور و بارگذاری یک IOS جدید در هنگام خراب شدن حافظه فلش.

Root switch در STP و RSTP ، سوئیچی که به دلیل داشتن Bridge ID پائین به عنوان Root Switch انتخاب می‌شود و در نتیجه می‌تواند، بسته‌های BPDU دوره‌ای (پیش‌فرض، ۲ ثانیه) ارسال کند.

Routed port مربوط به سوئیچ لایه‌ی سوم است که یک پورت سوئیچ را می‌توان به یک پورت روتر تبدیل کرد.

routed protocol پروتکل‌هایی را تعریف می‌کند که می توانند توسط روتر مسیریابی شوند.

Router Advertisement (RA) پیامی که توسط پروتکل IPv6 Neighbor Discovery (NDP) تعریف شده است، توسط روترها برای اعلام آمادگی خود برای عمل به عنوان روتر IPv6 در یک لینک استفاده می‌شود. این اطلاعات می‌تواند در پاسخ به پیام قبلاً دریافت شده NDP روتر (RS) ارسال شوند.

Router ID (RID) در EIGRP و OSPF، یک عدد ۳۲ بیتی است، که به صورت آدرس IP است و مشخص کننده‌ی هر روتر است.

Router LSA در پروتکل OSPF کاربر دارد و نوعی LSA است که روتر برای توصیف خود و شبکه‌های متصل به آن ایجاد می‌کند.

Router Solicitation (RS) پیامی تعریف شده توسط پروتکل IPv6 Neighbor Discovery Protector (NDP) ، برای درخواست از هر روتر برای پاسخ، شناسایی روتر، به علاوه سایر تنظیمات پیکربندی (پیشوندها و طول پیشوند) استفاده شده است.

Routing protocol مجموعه ای از پیام ها و پردازش‌هایی که با آنها روتر می تواند اطلاعات مربوط به مسیرها را برای دستیابی به کل شبکه بدست آورد. نمونه‌هایی از پروتکل‌های مسیریابی شامل پروتکل مسیریابی پیشرفته Interior Gateway (EIGRP) ، Open Shortest Path First (OSPF) و پروتکل اطلاعات مسیریابی (RIP) است.

www.takbook.com

S

Secondary root مربوط به پیکربندی سوئیچ است، در زمان پیکربندی، این دستور باعث می‌شود که سوئیچ اولویت اصلی خود را روی ۲۸،۷۶۲ تنظیم کند.

Secure Shell (SSH) در لایه‌ی application کار می‌کند، با استفاده از تبادل کلید رمزگذاری و رمزگذاری یک ارتباط امن را با سرور ایجاد می‌کند.

Serial cable این کابل‌ها برای ارتباط یک دستگاه، مانند روتر با روتر دیگر به کار می‌رود، که مدل آن RS232 است که فقط برای اتصالات کوتاه که حداکثر ۱۴ یا ۱۵ متر باشد کاربرد دارد، البته برای فواصل طولانی می‌توان از مدل RS485 استفاده کرد.

Serial interface نوعی رابط در روتر، که برای اتصال به برخی از انواع پیوندهای WAN، به ویژه خطوط اجاره‌ای و پیوندهای دسترسی Frame Relay استفاده می‌شود.

Service set identifier (SSID) رشته متن که برای شناسایی یک شبکه بی‌سیم استفاده می‌شود.

Shortest path first (SPF) algorithm الگوریتم SPF که در پروتکل OSPF کاربرد دارد و برای پیدا کردن بهترین مسیر استفاده می‌شود.

Simultaneous Authentication of Equals (SAE) یک روش احراز هویت بسیارقوی که در WPA3 برای تأیید اعتبار مشتری و AP استفاده می‌شود و از حملات جلوگیری فرهنگ لغت (dictionary) برای کشف کلیدهای pre-shared جلوگیری می‌کند.

Single-mode fiber نوعی کابل فیبر نوری که به خوبی با فرستنده‌ها مانند لیزر کار می‌کند به طوری که یک زاویه نور به هسته کابل ساطع می‌کنند ، در مقایسه با کابل‌های فیبر چند حالته دارای هسته کوچکتر هستند.

Site-local scope مفهومی در IPv6 است که بسته‌های ارسال شده به یک آدرس با استفاده از این Scope یا محدوده باید توسط روترها ارسال شوند، اما از طریق پیوندهای WAN به سایت‌های دیگر ارسال نمی شوند.

SOHO router اصطلاحی که به یک روتر به عنوان بخشی از شبکه یک سازمان داده می‌شود که اصولاً در خانه‌ی یک کارمند و یا در دفتر کار کوچک قرار دارد و اصولاً کار سوئیچ، روتر، وایرلس و ... با هم انجام می‌دهد.

Spanning Tree Protocol (STP) پروتکل STP توسط سازمان IEEE با شماره‌ی 802.1D استاندارد شده است و شرکت سازنده‌ی آن DCE است. کار این پروتکل این است که وقتی شبکه در Loop قرار می‌گیرد، بعضی از interfaceهای اضافه را ShutDown می‌کند و فقط به یک طرف اجازه‌ی ارسال و دریافت اطلاعات می‌دهد.

www.takbook.com

این پروتکل از الگوریتمی به نام STA (Spanning Tree Algorithm) برای این کار استفاده می‌کند که کار این الگوریتم به این صورت است که کل ساختار شبکه را به صورت یک درخت درآورده و جاهایی را که Loop در آن ایجاد شده، مهار می‌کند.

Standard access list لیستی از دستورات پیکربندی روتر که در آن اگر بسته‌ای با IP منبع مطابقت داشته باشد طبق قانونی که برای آن تعریف می‌کنیم یا به آن بسته اجازه عبور داده می‌شود و یا اینکه آن بسته Drop (رها) می‌شود.

Star topology توپولوژی شبکه‌ای که در آن نقاط انتهایی در یک شبکه توسط پیوندهای Point to Point به یک دستگاه مرکزی مشترک متصل می شوند.

Startup-config file در سوئیچ‌ها و روترهای IOS سیسکو، نام پرونده‌ای است که در حافظه NVRAMقرار دارد و پیکربندی دستگاه را که در صورت بارگیری مجدد یا روشن شدن آن، در حافظه RAM بارگذاری می‌کند.

Stateful DHCPv6 در این نوع آدرس سرویس DHCP پیگیری می‌کند که کدام آدرس از نوع IPV6 به کلاینت داده شده است.

Stateless address autoconfiguration (SLAAC) ویژگی‌ای در IPv6 که در آن یک میزبان یا روتر می‌تواند بدون نیاز به Stateful DHCP server یک آدرس IPv6 unicast داشته باشد.

Static route یک مسیر IP در روتر که توسط کاربر ایجاد می‌شود و برای پیکربندی مسیر در روتر محلی است.

station (STA) یک سرویس گیرنده ۸۰۲.۱۱ که با یک BSS همراه است.

STP یا Shielded twisted-pair که یک نوع کابل‌کشی است و دارای لایه‌ی محافظت شده است و برای کاهش تداخل الکترومغناطیسی (EMI) است.

Straight-through cable به کابل مستقیم گفته می‌شود که سیسم متصل شده در پین یک به سیسم متصل شده به پین دو در سمت دیگر متصل می‌کند و به همین ترتیب تا سیسم آخر به همان ردیف در سر دیگر متصل می‌شود.

subinterface به Interface مجازی در داخل یک Interface اصلی اشاره دارد.

subnet به زیرشبکه‌هایی از کلاس A,B,C که توسط یک مدیر شبکه پیکربندی شده باشد گویند، این زیرشبکه‌ها به ما این امکان را می‌دهند به جای داشتن چندین شبکه از یک شبکه‌ی کلاس A,B,C بتوانیم استفاده کنیم.

subnet broadcast address یک آدرس خاص در هر Subnet، که بزرگترین آدرس IP در آن Subnet است و به گونه‌ای طراحی شده است که بسته‌های ارسال شده به این آدرس باید به تمام میزبان‌های آن Subnet تحویل داده شود.

www.takbook.com

Subnet mask در واقع وظیفه تفکیک دو قسمت Host و Network را از یکدیگر دارد. Subnet Mask یک رشته ۳۲ بیتی است که از چپ به راست دارای بیت‌های صفر و یک است.

subnetting فرایند تقسیم یک شبکه کلاس A، B یا C به گروه‌های کوچکتر به نام زیر شبکه‌ها است.

Summary LSA در OSPFv2، نوعی LSA است، که توسط روتر Area Border Router (ABR) ساخته می‌شود، برای معرفی یک Subnet در روترهای دیگر کاربرد دارد.

Supplicant یک موجودیت 802.1x است که به عنوان نرم‌افزار در یک دستگاه مشتری وجود دارد و درخواست دسترسی به شبکه را دارد.

T

T1 نام خطوط مخابراتی مخصوص است. بر روی هر خط T1 تعداد ۲۴ خط تلفن معمولی شبیه‌سازی می‌شود، هر خط T1 می‌تواند حامل 1.5 مگابایت پهنای باند باشد.

Transmission Control Protocol یک پروتکل TCP/IP مربوط به لایه‌ی انتقال که انتقال داده را به صورت قابل اعتماد انجام می‌دهد.

Transmission Control Protocol/Internet Protocol یک نام مشترک برای مجموعه پروتکل‌هایی که توسط وزارت دفاع آمریکا در دهه ۱۹۷۰ برای حمایت از ساخت کارگاه‌های اینترنتی در سراسر جهان تهیه شده است، TCP و IP دو پروتکل شناخته شده در مجموعه هستند.

Telnet یک پروتکل شبکه است که مخفف Terminal Network بوده و برای ارتباط با یک دستگاه از طریق خط فرمان (Command Prompt) است.

Temporal Key Integrity Protocol (TKIP) یک پروتکل با امنیت بالاتر به نسبت WEP است، این پروتکل برای ایجاد امنیت از MIC یا همان Message Integrity Check استفاده می‌کند، MIC یک الگوریتم کارآمد است که یک مقدار Hash شده را در فریم ارسالی اضافه می‌کند تا از دستکاری فریم جلوگیری کند.

trace – Short for traceroute از این دستور برای پیدا کردن مسیرهایی که بسته از آنها عبور می‌کند تا به مقصد برسد، استفاده می‌شود و بیشتر برای عیب‌یابی مسیریابی بین میزبان‌ها انجام می‌شود.

traceroute برنامه‌ای که در بسیاری از سیستم‌ها وجود دارد و مسیری را که یک بسته به مقصد می‌فرستد، را ردیابی می‌کند .بیشتر برای اشکال‌زدایی مشکلات مسیریابی بین میزبان‌ها استفاده می‌شود.

transceiver اصطلاحی که از کلمات فرستنده و گیرنده تشکیل شده است.

trunk روشی برای انتقال Vlanها در سوئیچ‌های مختلف است.

trunk interface قرار دادن پورت سوئیچ بر روی Trunk برای ارتباط برقرار کردن با سوئیچ دیگر برای انتقال VLAN.

www.takbook.com

trunking – VLAN trunking نیز گفته می‌شود، روشی که در آن با استفاده از پروتکل سیسکو ISL یا پروتکلIEEE(802.1Q) استفاده می‌شود که برای پشتیبانی از چندین VLAN است و اجازه می‌دهد تا از طریق آن ترافیک VLAN بین سوئیچ عبور کند.

Twisted-pair محیط انتقال متشکل از دو سیم عایق‌بندی شده که سیم‌ها در یک مارپیچ به دور یکدیگر پیچیده شده‌اند. یک مدار الکتریکی بر روی جفت سیم جریان می‌یابد و جریان در جهت‌های مخالف بر روی هر سیم قرار می‌گیرد ، که به طور قابل توجهی تداخل بین دو سیم را کاهش می دهد.

U

unicast address بطور کلی، هر آدرس در شبکه که نماینده یک دستگاه یا رابط واحد است.

unicast IP address آدرس IP که یک رابط واحد را نشان می‌دهد، درIPv4 ، این آدرس‌ها از محدوده کلاس A ، B و C هستند.

unified WLC deployment طراحی شبکه بی‌سیم که WLC را بطور مرکزی در یک توپولوژی شبکه قرار می‌دهد.

unique local address یک نوع آدرس IPv6 unicast که جایگزینی برای آدرس‌های Private در IPv4 است.

UDP – User Datagram Protocol پروتکل لایه انتقال که از نوع Connectionless است.

Unified Computing System (UCS) نام تجاری سیسکو برای محصولات سخت افزاری سرور خود است.

Universal Power over Ethernet (UPoE) یک استاندارد PoE است و همانطور که در اصلاح IEEE 802.3btدر استاندارد 802.3 تعریف شده است ، از چهار جفت سیم برای تأمین برق با حداکثر ۶۰ وات استفاده می‌کند.

Universal Power over Ethernet Plus (UPoE+) یک استاندارد PoE است، همانطور که در اصلاحیه IEEE 802.3bt در استاندارد 802.3 تعریف شده است ، از چهار جفت سیم برای تأمین برق با حداکثر ۱۰۰ وات استفاده می‌کند.

untrusted port این ویژگی مربوط به سرویس DHCP snooping است.

UPoE یا Universal Power over Ethernet که یک استاندارد PoE خاص است که در IEEE 802.3bt تعریف شده است و از چهار جفت سیسم برای تامین برق با حداکثر ۶۰ وات استفاده می‌کند.

www.takbook.com

URL یا Uniform Resource Locator اصطلاح بسیار رایج که یک متن با فرمت خاص برای ارتباط آن با آدرس IP به کار می‌رود، به عنوان مثال http://www.3isco.ir/ که با پروتکل (HTTP) کار می‌کند و نام میزبان (www.3isco.ir) است.

user network interface (UNI) اصطلاحی که در انواع استانداردهای WAN به کار می رود ، از جمله Metro Ethernet / Carrier، استانداردهای ارتباط برقرار کردن دستگاه مشتری با دستگاه WAN را از طریق لینک دسترسی تعریف می‌کند.

Username Secret مرجع گذرواژه تنظیم شده بر روی نام کاربری مخفی و رمز عبور ، که نام کاربری و رمز عبور رمزگذاری شده را تعریف می‌کند و برای ساختن یک نام کاربری محلی برای روتر یا سوئیچ استفاده می‌شود.

update timer یک بازه‌ی زمانی برای مشخص کردن ارسال آپدیت از طریق پروتکل‌های مسیریابی.

User mode این مد، یکی از پائین‌ترین مدها ازنظر سطح دسترسی کاربران به تنظیمات روتر است، حداکثر کاری که یک کاربر می‌تواند در این مد انجام دهد، انجام Monitoring است و به دلیل دستورات کمی که در این مد اجرا می‌شود، سطح دسترسی آن در پائین‌ترین سطح قرار دارد.

Unshielded twisted-pair - UTP نوعی کابل‌کشی، استاندارد شده توسط Telecommunications Industry Association (TIA) که دارای جفت‌های به هم پیوسته‌ی سیم مسی (به طور معمول چهار جفت) است و هیچ‌گونه محافظی در خارج از سیم ندارد.

V

Virtual LAN (VLAN) گروهی از دستگاه‌ها، متصل به یک یا چند سوئیچ، VLANها به سرپرستان سوئیچ این امکان را می دهند تا دستگاه‌های متصل به سوئیچ‌ها را بدون نیاز به سوئیچ‌های فیزیکی جداگانه، به VLANهای جداگانه تفکیک کنند و از مزایای طراح جداسازی ترافیک بدون هزینه خرید سخت افزار اضافی استفاده کنند.

Variable در برنامه‌ها یک روشی برای اختصاص دادن یک نام به یک مقدار وجود دارد تا بر اساس آن، برنامه بتواند به مقدار مورد نظر از طریق اسم ارجاع پیدا کند، آن را تغییر دهد و یا آن را با سایرین مقایسه کند.

Version control software به برنامه‌هایی اشاره دارد که فایل‌ها را برای تغییرات آنها ردیابی می‌کند، با این کار کاربران می‌توانند نسخه‌های هر پرونده را در طول تاریخ خود مقایسه کنند تا تفاوت‌ها را مشاهده کنند.

www.takbook.com

Violation mode مربوط به یکی از حالت‌های امنیتی پورت است که پورت را در حالت shutdown, restrict, protect قرار می‌دهد.

Virtual CPU (vCPU) در یک محیط سرورمجازی، یک هسته یا پردازنده CPU (پردازنده) اختصاص داده شده به یک ماشین مجازی (VM) توسط Hypervisor .

Virtual machine نمونه‌ای از سیستم‌عامل در حال اجرا بر روی سخت افزار سرور است که از یک hypervisorبرای اختصاص زیر مجموعه‌ی سخت‌افزار سرور مانند CPU، RAM، دیسک و شبکه استفاده می‌کند.

Virtual network function (VNF) هر عملکردی که در یک شبکه انجام شود (به عنوان مثال روتر ، سوئیچ ، فایروال) که به عنوان یک وسیله فیزیکی اجرا نمی‌شود بلکه به عنوان یک سیستم عامل در یک سیستم مجازی(برای مثال ، یکVM اجرا می‌شود).

Virtual NIC (vNIC) در یک محیط سرورمجازی، یک کارت رابط شبکه (NIC) که توسط یک ماشین مجازی استفاده می‌شود، و سپس به برخی سوئیچ‌مجازی (vSwitch) که در همان میزبان کار می‌کند متصل می‌شود گویند.

Virtual private network (VPN) یک شبکه خصوصی مجازی است که روی یک بستر عمومی ایجاد می‌گردد. این شبکه خصوصی باید بتواند تمام سایت‌های مشتری را به یکدیگر متصل کند و به صورت کامل ازVP های مرتبط با سایر مشتریان جدا باشد. معمولا هر VPN به یک سازمان که دارای چند سایت است اختصاص دارد و سایت‌های سازمان را از طریق VPN روی بستر عمومی Service Providerبه یکدیگر متصل می‌کند.

Virtual Router Redundancy Protocol (VRRP) این پروتکل کاملاً شبیه به HSRP است. شماره‌ی گروه در این پروتکل از ۰ تا ۲۵۵ و شماره‌ی Priority از ۰ تا ۲۵۴ است. روتر اصلی به‌عنوان روتر Master در نظر گرفته می‌شود و روترهای فرعی به‌عنوان Backup در نظر گرفته می‌شود. این پروتکل مربوط به سازمان IETF است.

virtual switch (vSwitch) یک سوئیچ مجازی است که برای ارائه سرویس سوئیچ به ماشین مجازی کاربرد دارد.

virus بدافزارهایی که خود را به برنامه های دیگر تزریق می کنند و سپس از طریق مداخله کاربر پخش می شوند.

VPN client یک نرم‌افزار که در سیستم‌های شخصی هر کاربر وجود دارد و برای ارتباط با پروتکل‌های مورد نیاز شبکه و از راه دور استفاده می‌شود.

vulnerability ضعفی که می‌تواند برای به خطر انداختن امنیت یک شبکه به کار رود.

www.takbook.com

VXLAN – Virtual Extensible LAN یک پروتکل محفظه انعطاف‌پذیر که برای ایجاد تونل‌ها استفاده می‌شود.

VLAN configuration database نام دسته‌بندی شناسه‌های VLAN و نام‌های موجود در سوئیچ سیسکو.

VLAN interface یک مفهوم پیکربندی در داخل سوئیچ‌های سیسکو است، که به عنوان واسط بین IOS که روی سوئیچ کار می‌کند و یک VLAN که در داخل سوئیچ پشتیبانی می‌شود، مورد استفاده قرار می‌گیرد تا سوئیچ بتواند یک آدرس IP به VLAN اختصاص دهد و بسته‌های IP را در آن VLAN ارسال کند.

VLAN Trunking Protocol (VTP) این پروتکل توسط شرکت سیسکو ارائه شده است، اما انحصاری نیست و شرکت‌های دیگر می‌توانند از این پروتکل استفاده کنند. این پروتکل برای مدیریت Vlanها و ایجاد امنیت به کار برده می‌شود. VTP به مدیر شبکه، اجازه‌ی ایجاد، حذف، تغییر نام VLAN و ... را می‌دهد.

Voice VLAN این VLAN مختص ارسال Voice است و در سوئیچ باید آن را تنظیم کرد.

VoIP یا Voice over IP انتقال ترافیک صوتی در داخل بسته‌های IP از طریق شبکهVTP .

VTP client mode یکی از سه حالت عملیاتی در VTP در سوئیچ است که سوئیچ‌ها از طریق آن با نام‌های VLAN و شماره‌های آن از سوئیچ‌های دیگر مطلع می‌شوند ، اما نمی‌توانند به صورت مستقیم اطلاعات VLAN را پیکربندی کنند.

VTP server mode یکی از سه حالت عملیاتی در VTP که سوئیچ‌ها در حالت سرور می‌توانند VLAN ها را پیکربندی کنند، سوئیچ‌های دیگر را در مورد تغییرات اطلاع دهند و درباره تغییرات VLAN از سوئیچ‌های دیگر مطلع شوند.

VTP transparent mode یکی از سه حالت عملیاتی در VTP که در این حالت سوئیچ‌ها در حالت transparent می‌توانندVLAN های خود را پیکربندی کنند، اما در مورد تغییرات دیگر سوئیچها چیزی یاد نمی‌گیرند ولی VLANها را از خود عبور می‌دهند.

W

web server نرم‌افزاری که در رایانه کار می‌کند، صفحات وب را ذخیره می‌کند و آن صفحات وب را برای مشتری‌های وب (مرورگرهای وب) که درخواست صفحات وب می‌کنند ، ارسال می‌کند.

wide-area network (WAN) بخشی از شبکه بزرگتر که عمدتاً از فن‌آوری لایه‌ی یک و دو استفاده می‌کند، سایت‌هایی را که معمولاً بسیار دور از هم قرار دارند به همدیگر متصل می‌کند.

Wi-Fi Alliance یک مجموعه خصوصی جهانی برای وضع استانداردهای شبکه‌های WIFI است.

www.takbook.com

Wi-Fi Protected Access (WPA) اولین نسخه از احراز هویت WIFI با نام WPA بود که با استاندارد 802.11i معرفی شد که از پورتکل TKIP برای رمزنگاری استفاده می‌کند.

wildcard mask مربوط به MASK مورد استفاده در Access List و پروتکل‌های OSPF و EIGRP .

window تعداد بایت های ارسال شده را بدون دریافت تأییدیه نشان می‌دهد.

Wired Equivalent Privacy (WEP) یک پروتکل رمزنگاری است که در استاندارد 802.11b تعریف شده است، این پروتکل در سال ۱۹۹۷ معرفی شده است، پروتکل امنیتی WEP از الگوریتم رمزنگاری RC4 برای ایجاد یک Frame داده‌ی بی‌سیم خصوصی و پنهان استفاده می‌کند که می‌تواند امنیت داده را حفظ کند، این الگوریتم از یک رشته حروف برای ایجاد کلید رمزنگاری استفاده می‌کند، یعنی اینکه مشتری می‌تواند با وارد کردن این Key یا همان کلید به AP متصل شود.

wired LAN یک شبکه‌ی محلی LAN که اطلاعات را از طریق سیسم بین دستگاه‌های شبکه ارسال می‌کند.

wireless LAN یک شبکه‌ی محلی بی‌سیم، که اطلاعات را از طریق امواج رادیویی انتقال می‌دهد.

wireless LAN Controller (WLC) دستگاهی برای کنترل چندین AP مختلف در یک سازمان به صورت همزمان.

WLAN client یک وسیله بی‌سیم است که می خواهد به منظور برقراری ارتباط با سایر دستگاه‌های بی‌سیم ، به یک نقطه دسترسی بی سیم دسترسی پیدا کند.

workgroup bridge (WGB) یک دستگاه بی‌سیم را به چند دستگاه سیمی متصل می‌کند و این نوع دستگاه‌ها مختص شرکت سیسکو هستند.

WPA Version 2 (WPA2) دومین نسخه از احراز هویت WIFI با نام WPA2 بود که با استاندارد 802.11x معرفی شد که از پروتکل TKIP برای رمزنگاری استفاده می‌کند و معرفی روش CCMP که به عنوان جایگزینی برای TKIP بود.

WPA Version 3 (WPA3) نسخه‌ی سوم استاندارد که در سال ۲۰۱۸ معرفی شد در این استاندارد نیاز به کلید Pre-Shared یا احراز نوع 802.1x دارد و دارای دو الگوریتم AES و GCMP است.

WAN edge این دستگاه (به طور معمول روتر) در سایت‌های سازمانی که به پیوندهای WAN خصوصی متصل می‌شوند استفاده می‌شود.

WAN service provider شرکتی که خدمات WAN خصوصی را به مشتریان ارائه می دهد.

watering hole attack حمله گودال آب به حمله‌ای گفته می‌شود که مهاجمان با ایجاد حفره‌های آبی برای قربانی سعی دارند با اجرای اسکریپتی به صورت کاملاً مخفیانه قربانی را به سمت آن گودال‌ها هدایت کنند و از این طریق به سیستم قربانی نفوذ کنند.

web server نرم‌افزاری که در رایانه کار می‌کند، صفحات وب را ذخیره می‌کند و آن صفحات وب را برای مشتری‌های وب (مرورگرهای وب) که صفحات وب را درخواست می‌کنند ارسال می‌کند.

www.takbook.com

well-known port یک شماره پورت TCP یا UDP که برای استفاده توسط یک برنامه خاص رزرو شده است.

whaling یک تکنیک فیشینگ است و به دنبال افراد درای سابقه‌ی بالا می‌گردد تا بتوانند انها را از طریق لینک به سایت‌های مخرف دنبال کنند.

wildcard mask یک MASK که در دستورات ACL و دستورات OSPF و EIGRP استفاده می‌شود.

window تعداد بایت های ارسال شده را بدون دریافت تأییدیه نشان می دهد.

worm بدافزارهایی که از یک سیستم به سیستم دیگر منتقل می‌شوند و همه‌ی سیستم‌ها را به صورت اتوماتیک آلوده می‌کند.

X–Y–Z

XML (eXtensible Markup Language) یک زبان نشانه‌گذاری است که به عنوان یک زبان سریال‌سازی داده‌ها مفید است.

YAML (YAML Ain't Markup Language) یک زبان سریال‌سازی داده‌ها که توسط انسان به راحتی قابل خواندن است و توسط Ansible استفاده می‌شود.

zero-day vulnerability به یک آسیب‌پذیری امنیتی اشاره دارد، از روزی که این آسیب‌پذیری شناسایی شده تا روزی که آن آسیب‌پذیری توسط مسئول آن نرم‌افزار حل شود و آن را رفع کند.

www.takbook.com

www.takbook.com

منابع

- CCNA 200-301 Official Cert Guide, Volume 1 - Wendell odom
- CCNA 200-301 Official Cert Guide Volume 2 - Wendell odom
- CiscoPress_CCNA-200-301-Portable-Command-Guide-5th-Edition_2 - Scott Empson
- CCNA Self-Study: CCNA Portable Command Guide -Scott Empson
- CCNA Cisco Certified Network AssociateStudy Guide 5th Edition - Todd Lammle
- CCNP - Routing Study Guide -Todd Lammle – Sean Odom – with kevin wallac
- CCNP Routing - Kevin Wallace
- CCNP Switching - Kevin Wallace
- CCNP Routing and Switching TSHOOT - Kevin Wallace
- http//cisco .com
- http://forum.ciscoinpersian.com
- https://virgool.io - سجاد غفاریان - QOS
- https://cisco.tosinso.com– جعفر قنبری شوهانی - MPLS
- https://networklessons.com/