**عنوان سند:** مقدمه ای بر **IP Version 6**

**ارائه دهنده:** بهروز عباس زاده

**تاریخ ارائه:** ۸۳/۱۰/۲۱

**گروه کاری : IPV6**

**گروه مطالعاتی : IP**

**اصلاح کننده :** بهروز عباس زاده

**تاریخ اصلاح:** ۸۳/۱۱/۲

**منابع:** مقالات اینترنت

# بنام خدا

## IP Version 6

**مقدمه**

IPv6 را بعضي وقتها توليد بعدي IP هم مي گويند ، البته براي بسياري از شبكه هاي خصوصي فوايد به روز كردن نسخه IP از 4 به 6 هنوز آشكار نشده است ، راستي با اين همه خصوصيات خوبي كه **IPv4** داراست چه نيازي براي به روز كردن آن از نسخه 4 به نسخه 6 مي باشد ؟

يكي از عمومي ترين مزايا و منافع IPv6 گستردگي و ازدياد فضاي آدرس آن است و اين نسخه از IP از فضاي آدرس دهي 128 بيتي استفاده مي كند در صورتيكه IPv4 از فضاي آدرس دهي 32 بيتي استفاده مي نمود .

هرچند كه IPv4 به وفور و گستردگي در شبكه هاي خصوصي خيلي بزرگ مورد استفاده قرار مي گيرد ، IPv6 داراي فوايد زيادي براي اين شبكه ها مي باشد از جمله اين فوايد مي توان به Security بالاي آن در لايه شبكه ، بهبود و تقليل جداول مسيريابي ( routing table ) ( و در نتيجه كاهش حافظه و پردازنده لازم براي روترها ) و بهبود بخشيدن به استفاده از آدرس دهي اتوماتيك براي كاربران متحرك ( mobile users ) اشاره نمود .

IPv6 داراي تاريخچه متفاوتي براي اينترنت مي باشد ، نقشه ها و آمارها نشان مي دهد كه افزارها و دستگاههاي گيرنده آدرس IP (دستگاههايي كه مي توانند IP آدرس داشته باشند ) روز به روز بصورت تواني در حال افزايش است بطوريكه حتي كالا هاي مورد استفاده توسط خانواده ها و مصرف كنندگان نيز قابل آدرس دهي اينترنتي مي شوند ، اين كار به فضاي آدرس دهي بيشتري نياز دارد و به اين دليل بطور اختصار نحوه برخورد فرم فعلي IPv6 با اين مسئله را بررسي مي كنيم .

**پيش گفتار ( Background )**

با اين تصميم كه اينترنت بطور جدي نياز به ظرفيت و فضاي آدرس دهي بالايي دارد گروه معماري اينترنت ( The Internet Architecture Board ) سه پيشنهاد ( proposal ) اصلي در اين زمينه ارائه نمود .

اولين پيشنهاد تحت عنوان TUBA ( TCP and UDP over Bigger Addresses ) بود ، اين پيشنهاد بر اساس سوئيچينگ IP بر روي CLNP ( The Connection-Less Network Protocol ) بعنوان پروتكل لايه اينترنت بود ، CLNP يك پروتكل OSI مي باشد كه داراي آدرس 20 هشت تايي ( 20 octet ) مي باشد و تمامي پروتكل هاي مسيريابي تعريف شده را پشتيباني مي كند ، اين پروتكل مورد قبول واقع نشد زيرا CLNP در آن زمان هم ( زمان پيشنهاد ) يك پروتكل قديمي و غير موثر محسوب مي شد و حتي در بازار IPv4 هم بصورت يك پروتكلي كه بطور گسترده در بازار پروتكل هاي IP كاربرد داشته باشد مورد قبول نبود .

پيشنهاد دوم IPV7 ناميده مي شد كه بعداً به TP/IX تغيير نام داد و سر انجام آن را CATNIP ناميدند ، اين پيشنهاد بر اساس اين ايده پايه ريزي شده بود كه يك بسته اطلاعاتي ( packet ) با شكل ( format ) مشترك تعريف شود كه با IP ، CLNP و IPX سازگاري داشته باشد ، اين پيشنهاد بعلت عدم رشد سريع آن مورد توجه و استقبال واقع نشد .

سومين و آخرين پيشنهاد كه موفقترين آنها نيز بود با عنوان IP در IP زندگي خود را آغاز نمود ، اساس اين پيشنهاد اين بود كه در آن براي اينترنت دو لايه جداگانه تعريف مي كنند يكي بعنوان لايه زيرساخت ( backbone ) و ديگري بعنوان لايه گسترش محلي ( local deployment ) .

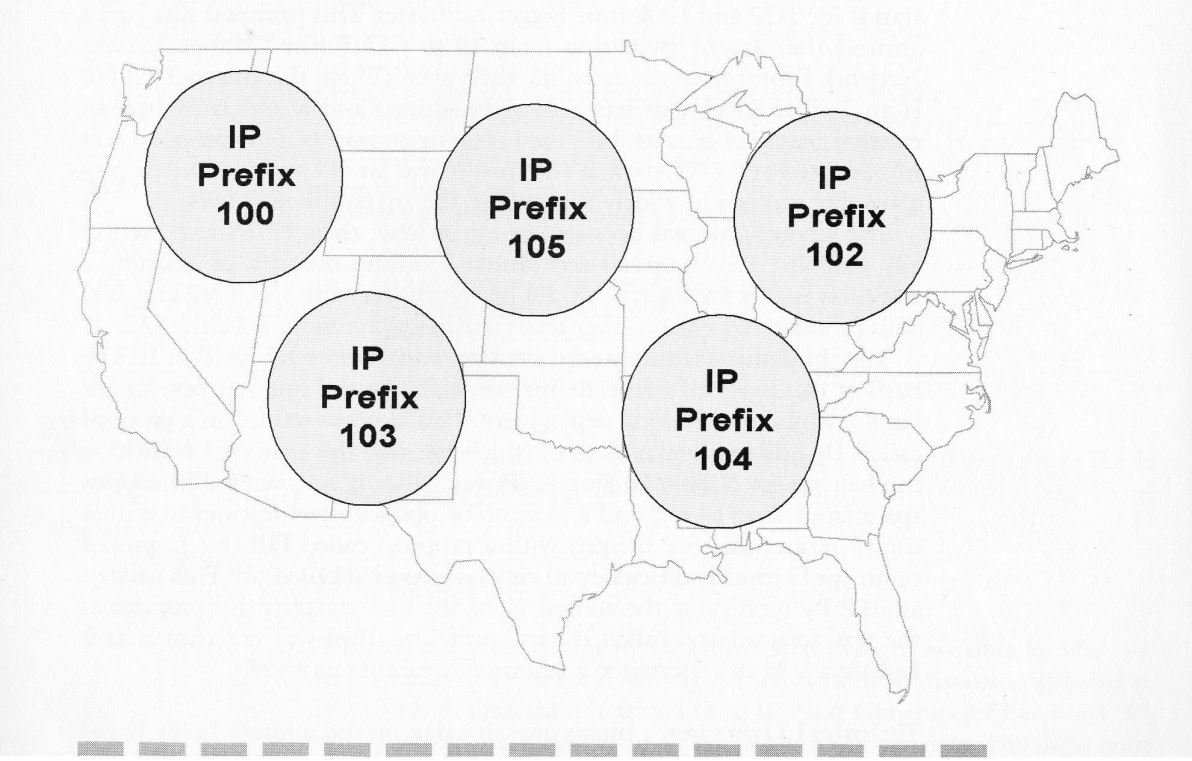
در اين پيشنهاد در اقع يك نوع بسته بندي ( encapsulation ) آدرس IP صورت گرفته است كه مكانيزم خوبي براي انتقالIP ساده ( simple IP ) نيز مي باشد ، انتقال آدرسها با اين روش از IPv4 به راحتي انجام مي گيرد اين روش در واقع به افزايش فضاي آدرس دهي IP از 32 بيتي به 64 بيتي و از بين بردن بعضي از مشخصه هاي منسوخ شده IPv4 براي كاهش اندازه هدرهاي ( header ) پروتكل IP مي باشد ، SIP را با پيشنهادي كه به آن PIP مي گفتند تركيب دادند و اثرات

مسيريابي IPv4 را بهبود بخشيدند و پيشنهاد جديدي را ارائه نمودند كه آن را SIPP ناميدند (Simple IP Pulse ) ، با تغييرات به وجود آمده و با گسترش فضاي آدرس IAB اين پيشنهاد را پذيرفت و با اعمال تغييرات ديگري روي آن بعدها آن را IPv6 ناميد ، از اسم IPV5 استفاده نكردند چون قبلا از آن در جاي ديگر و براي پروتكل جاري ديگر استفاده شده بود .

**مرور تكنيكی ( Technical overview )**

افزايش فيلد آدرس قسمت آسان كار مي باشد كپي كردن اطلاعات با حجم بزرگتر با استفاده از آدرسهاي IP ( توانايي روترها براي جابجا كردن اطلاعات از مبدا به مقصد ) در اينترنت يك دردسر و مشكل واقعا بزرگ و پيچيده اي است و تنها تكنيك شناخته شده براي حمل اطلاعات يك سيستم در اينترنتي كه روز به روز بزرگتر مي شود تكنيك مسيريابي سلسله مراتبي مي باشد در صورت عدم وجود روش بهتر و كاراتر سيستم مسيريابي اينترنت ( هم در فضاي IPv4 و هم در فضاي IPv6 ) نياز مبرم به روش و تكنيك مسير يابي سلسله مراتبي دارد ، اگرچه روش مسيريابي سلسله مراتبي داراي درجه اطمينان وقابليت بالايي مي باشد لكن محدوديتهايي نيز در آن وجود دارد كه باعث مي شود تاثير بهينه نداشته باشد يكي از مهمترين اين محدوديتها نيازي است كه اختصاص دادن آدرس بتواند توپولوژيهاي لايه هاي پايين شبكه را نيز پشتيبانی نمايد.

يكي از موارد عملي كه در اين مورد مي توان به آن اشاره نمود اختصاص دادن آدرسهاي IP با توجه به محدوديتهاي جغرافيايي مي باشد كه مشابه اين مفهوم در شبكه تلفني وجود دارد و مي دانيد كه چگونه يك كد محلي ( area code ) به نواحي




جغرافيايي بخصوص اختصاص مي دهند ، اين مفهوم در شكل1 تشريح شده است .

**شكل 1**

(( آدرس دهي سلسله مراتبي : با اين نوع آدرس دهي ISP ها درمحل جغرافيايي خود يك prefix تنظيم شده ( يك كد از پيش تعيين شده ) دارند . با تغيير دادن محل ISP يا تغيير دادن محل اتصال فيزيكي آنها به اينترنت بايستي شماره گذاری آدرس سلسله مراتبي مجددا انجام پذيرد تا موثر واقع شود . ))

بنابراين اگر يك شبكه محل اتصال خود به شبكه اينترنت را تغيير دهد بايستي آدرس دهي خود را نيز تغيير دهد ، اگر يك شركت محل ISP خود را عوض نمايد اين كار بلافاصله مشخص و آشكار خواهد شد زيرا آن شركت براي داشتن ارتباط ممتد و

موثر با شبكه جهاني اينترنت نياز به تغيير سلسله آدرس هاي خود دارد لذا يك پيش شرط ضروري براي مسيريابي سلسله مراتبي دسترسي عملي به تكنولوژيهاي مور د نياز براي شماره گذاري مجدد ( تغيير دادن آدرسها ) مي باشد در IPv6 شماره گذاري مجدد توسط توانايي هاي روش پيكربندي اتوماتيك خيلي راحتتر از IPv4 انجام مي شود و با فعال كردن يك ميزبان ( host ) در IPv6 عمل شماره گذاري اتوماتيك خيلي راحتتر از IPv4 و بدون دخالت انسان انجام ميشود اگرچه پيكربندي اتوماتيك , پيكربندي ميزبانها را ساده تر و راحتتر انجام مي دهد حسن و فايده اصلي آن توانايي نگهداري سلسله مسيرهاي موثر در شبكه جهاني اينترنت مي باشد .

براي ساده كردن شماره گذاري مجدد يك ميزبان در IPv6 ، نياز به ميزبانهايي است كه اين ميزبانها قابليت تنظيم كردن چند آدرس را روي يك اينترفيس فراهم مي كنند ، اين كار مشابه مفهوم گذاشتن دو آدرس IP روي يك اينترفيس ( مثلا Cisco ) مي باشد كه با استفاده از دستور secondary IP address امكانپذير است ، مكانيزم IPv6 براي گذاشتن چند آدرس بر روي يك اينترفيس سواي روشهاي فوق مي باشد IPv6 داراي اين قابليت است كه با استفاده از آن بتوان يك آدرس valid ( معتبر ) ، deprecated ( نيمه معتبر ) يا invalid ( نا معتبر ) را بر روي يك اينترفيس گذاشت يك ميزبان از آدرس valid هم براي ارتباط موجود و هم براي تثبيت كردن يك ارتباط جديد مي تواند استفاده نمايد ، بصورت تعريف شده ( by default ) يك ميزبان از آدرس depricated فقط براي برقراري ارتباط موجود استفاده مي كند ولي از اين آدرس براي برقراري ارتباط جديد نمي تواند استفاده نمايد و بالاخره اگر يك ميزبان از آدرس invalid استفاده نمايد نه مي تواند از آن براي ارتباط جديد استفاده كند و نه براي برقراري ارتباط موجود ، در پروسه تغيير دادن مجدد آدرس ها ميزبانهايي كه داراي آدرس IPv6 هستند و آدرس آنها بصورت deprecated باشد ميزبان يك آدرس valid جديد را از طريق يكي از مكانيزمهاي پيكربندي اتوماتيك آدرس IPv6 بدست مي آورد ، در نتيجه تمامي ارتباطات تازه از آدرس جديد استفاده خواهند كرد .

پيكربندي اتوماتيك آدرس دهي در IPv6 هم با مكانيزمهاي با كيفيت بالا و هم با مكانيزمهاي با كيفيت پايين پشتيباني مي شود ، پيكربندي اتوماتيك با كيفيت بالا براساس DHCP مي باشد كه بصورت اختصاصي براي IPv6 تعريف شده است ، پيكربندي اتوماتيك با كيفيت پايين نياز به نگهداري سرورهاي ( servers ) DHCP را

حذف مي كند ، با پيكربندي اتوماتيك با كيفيت پايين انتظار ميرود كه يك ميزبان آدرس IPv6 خود را با پيش شماره ( prefix ) زير شبكه كه آن ميزبان با استفاده از پيدا كردن همسايه ها ( neighbor discovery ) از روترهايي كه مانند همان ميزبان در آن شبكه هستند بدست آورد .

اختصاص دادن آدرس جديد براي يك دستگاه يا افزار تنها قسمتي از كار و برنامه مي باشد ، ميزبانهاي زيادي وجود دارند كه تغيير آدرس آنها توسط متدها و روشهاي تغيير آدرس موجود كه در زير به آنها اشاره مي كنيم امكان پذير نمي باشد :

١ – به روز رساني ديتا بيس هاي DNS ها ( Domain Name System ) براي تمامي گره هايي ( nodes ) كه آدرس آنها تغيير يافته است و همچنين به روز رساني اطلاعات آدرس هاي سرورهاي DNS ( DNS servers ) با سايت مربوطه .

٢ – آدرس دهي مجدد در مواردي همچون تغيير اطلاعات پيكربندي روترها براي مثال ليست فيلترهاي كنترل و دسترسي ( access control list filters ) و اطلاعات دستيابي .

٣ – بعضي از كاربردهاي TCP/IP كه در اطلاعات پيكربندي به آنها اشاره شده است ( ديتا بيس هاي پيكربندي ) و با دستور ip address بيان شده اند .

٤ – اگر ديتا بيس هاي كنترل كننده ( مجوز دهنده ) ايستگاههاي كاري ( clients ) با يك آدرس IP بخصوص پيكربندي شده باشند تغيير آدرس سايت مستلزم تغيير اطلاعات پيكربندي است كه توسط ايستگاههاي كاري ( clients ) نگهداري ميشود .

هيچكدام از حالتهاي فوق توسط الگوها و روشهاي تغيير آدرس در دسترس و موجود تحت پوشش قرار نمي گيرند ، نگهداري سلسله مراتبي موثر بوسيله تغيير آدرسي كه توضيح داده شد مشكل اجرايي مهمي را باعث مي شود .

**هدرهاي ( Header ) IPv6 چگونه كار مي كنند ؟**

IPv6 بسياري از ويژگيهاي اصلي پروتكل IPv4 را دارا مي باشد ، اينترنت موفقيتهاي لازم را كسب نخواهد كرد مگر اينكه بسياري از عيب ها و نقص هاي مهم و قابل توجه موجود در طراحي IPv4 را كنار بگذاريم بنابراين هدرهاي IPv6 داراي شباهتهاي زيادي در مقايسه با هدرهاي IPv4 مي باشد ، هدر هاي IPv6 تركيبي از 64 بيت هستند كه بوسيله دو فيلد 128 بيتي يعني آدرس مبداء و آدرس مقصد احاطه شده است ، 64 بيت اشاره شده از فيلدهاي زير تشكيل شده است :

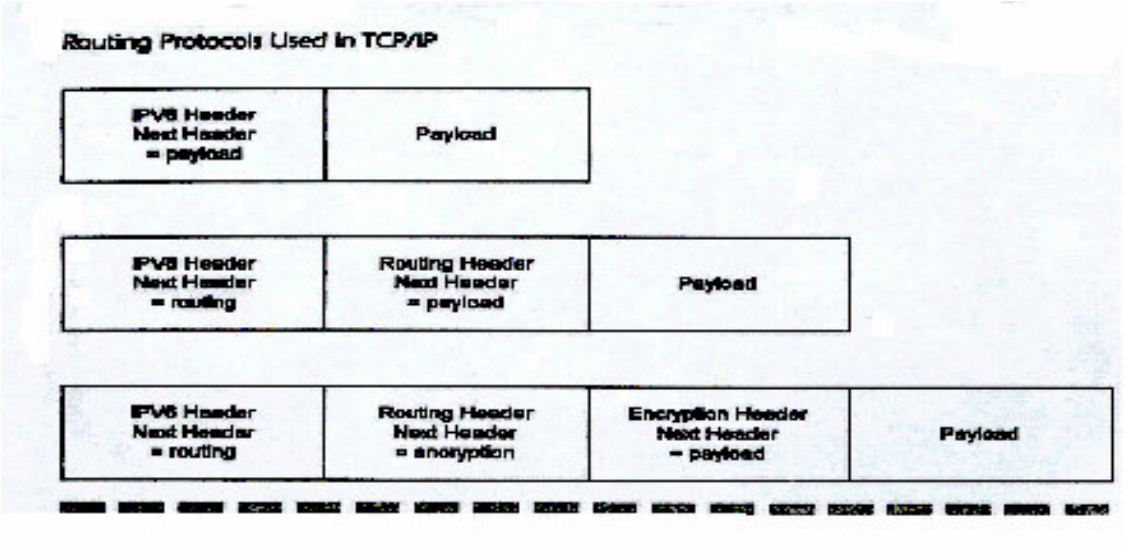
- Version
- Class
- Flow lable
- Legth of payload
- Type
- Hop limit

برخلاف هدر های IPv4 که شکل و فرمت ثابت دارند هدرهای IPv6 دارای شکل ثابت نبوده و از انعطاف پذیری بیشتری برخوردار است این کار باعث مي شود هدر هايي كه در IPv4 استفاده مي شدند ساده تر گردند زيرا IPv4 يك شكل و فرمت ثابت به همه هدرها اختصاص مي دهد و تصحيح كننده ها و چك كننده هاي هدر ( header checksum ) را جابجا مي كند و اين پروسه و عمل را در همه جهش ها ( hop ) تكرار مي كند .

مهمترين قسمت اين تغييرات جابجايي و برداشتن پروسه و مرحله تقسيم بندي جهش به جهش ( hop to hop) مي باشد ، قبلا ممكن بود يك ميزبان اطلاعات خود را از طريق چندين محيط و مسير از مبداء به مقصد بفرست ، زيرا اين احتمال وجود داشت كه بسته اي ( packet ) كه ارسال شده به اندازه اي بزرگ باشد كه بعضي از محيط ها نمي توانند آن را جابجا كنند ، بعنوان مثال ارسال يك بسته از محيط شبكه با توپولوژي حلقه – نشانه ( Token-Ring ) كه ماكزيمم اندازه بسته آن 4k است به يك شبكه با استاندارد اترنت ( Ethernet ) كه حد اكثر اندازه بسته آن 1.5 k مي باشد ، در اين حالت روتري كه دو نوع محيط را به همديگر متصل مي كند بسته اصلي را تقسيم خواهد كرد ، اين اتفاق در IPv6 نخواهد افتاد زيرا IPv6 از پروسه اي كه تشخيص دهنده MTU مسير ( path MTU ) گفته مي شود استفاده مي كند و بنابراين مطمئن است كه هيچ نوع تقسيم بندي لازم نيست .

با وجود اينكه IPv6 داراي مفهوم هدر بسيار ساده اي است ولي با اين وجود مفهوم توسعه هدر ( header extension ) را نيز پشتيباني مي كند ، زماني كه توسعه هدر ها مورد استفاده قرار مي گيرد بيت انتهايي هر هدر وظيفه هدر بعدي را كه بايد جريان يابد مشخص مي كند مگر در حالتي كه نوبت هدر آخري (

payload ) که نقطه نهايي جريان را نشان مي دهد برسد ، اين مفهوم در شكل 2شرح داده شده است




.

شكل 2

گستردگي هدرها

هدر هاي گسترش يافته اي كه قابل دسترسي هستند عبارتند از :

- Routing header
- Fragment header
- Authentication header
- Encrypted security payload
- Destination option header

**آدرس دهی در IPv6 (IPv6 addressing)**

در IPv4 از روش معروف هشت تايي براي آدرس دهي استفاده مي كرديم و با استفاده از آن كلاس هاي آدرس A ، B و C را تعريف مي كرديم و با توجه به ماسك زير شبكه اي ( subnet mask ) كه اعمال مي كرديم مي -توانستيم شبكه ، زير شبكه و شماره هاي گره ها ( node number ) را تشخيص دهيم

IPv6 مقداري با اين مفهوم متفاوت است و ما اين تفاوت را در اينجا توضيح خواهيم داد .

در IPv6 سه روش آدرس دهي وجود دارد كه عبارتند از unicast ، multicast و anycast و حالت broadcast يا پخشي وجود ندارد ، unicast مانند ارتباط نقطه به نقطه ( point to point ) مي باشد و يك بسته فقط به يك آدرس مشخص ارسال مي شود نه به آدرس هاي ديگر و اين آدرس به يك اينترفيس مشخص و ثابت در شبكه اختصاص پيدا مي كند ، حالت multicast به پروسسي اشاره مي كند كه در آن يك بسته به تعدادي از گيرنده ها ارسال مي شود اين كار متفاوت با حالت broadcast است زيرا در حالت broadcast بسته ارسال شده به تمامي افزارها و دستگاههاي موجود در زير شبكه كه broadcast به آنها دلالت دارد تحويل داده مي شود ولي در حالت multicast ارسال بسته فقط براي تعداد محدودي از افزارها كه از قبل تنظيم شده اند صورت مي گيرد بنابراين افزارهايي بسته را دريافت مي كنند كه حالت multicast براي آنها از قبل تعريف شده باشد ، حالت anycast مشابه multicast است با اين اختلاف كه بسته تنها به اولين افزاري كه در گروه anycast مي تواند بسته را دريافت كند تحويل داده مي شود و به تمامي افزارهاي موجود در گروه anycast تحويل داده نخواهد شد .

قراردادي كه براي نشان دادن و نوشتن آدرسهاي 128 بيتي در IPv6 بكار مي رود استفاده از بلوكهايي از 4 عدد هگزادسيمال ( Hexadecimal ) است كه با علامت كولن ( : ) از همديگر جدا مي شوند ، يك مثال در زير آورده شده است .

FEDC:CD56:6543:7896:F123:2344:9877:7654

نوشتن اين اعداد مقداري پرزحمت است البته نه براي كاربراني كه در هر حالت مي توانند از نام ميزبان ( host ) بجاي آدرس آن استفاده كنند بلكه براي مديراني كه مجبورند اين اعداد را براي پيكربندي فايل ها و ديتا بيس ها و افزارها بنويسند ، براي خلاصه كردن اين عدد نويسي مطابق قرارداد از نوشتن صفرهاي سمت چپ آدرس جلوگيري مي كنند اين كار بسيار مفيد واقع خواهد شد مخصوصا در روزهاي اول عمر IPv6 كه مقدار زيادي از فضاي آدرس از صفرها تشكيل شده است ، قرارداد خذف كردن صفرهاي سمت چپ به عدد نويسي با دو كولن ( double colon ) معروف است و آن به اين معنا است كه اگر دو كولن در يك آدرس نشان داده

شود آن آدرس را با وارد کردن صفرها بین دو کولن بـه 128بیـت مـي رسـانیم مثـال زیر این عمل را نشان مي دهد .

0000:0000:0000:0000:1111:2222:3333:4444

که مي توان آدرس فوق را بصورت زیر نشان داد .

::1111:2222:3333:4444

در نوشـتن اعـدا مربـوط بـه آدرس هـاي IPv6 مـي تـوان یـك پیـشوند ( prefix ) آدرس همانطور که در IPv4 استفاده مي شـد تعریـف نمـود ، در IPv4 همـانطور کـه دیدید تعداد بیتهایي که بعنوان پیشوند به آدرس اضافه مي شد و آدرس زیر شـبکه ( subnet ) را مشخص مي کرد را مي توانستیم با استفاده از علامت / ( slash ) از آدرس جدا کنیم ، مثال زیر یـك آدرس کـلاس B بـا تعـداد بیتهـاي 24 ( کـه معـادل بـا ماسك زیر شبکه 255.255.255.0 مي باشد) را نشان مي دهد .

173.8.4.3/24

از همان روش درIPv6 نیز مي توان استفاده کرد مثال زیرنشان مي دهد که اولین 64 بیتي که بعنوان پیشوند ( prefix ) مي باشد در جدول مـسیریابي بـراي مـشخص کردن قسمتهاي مجزا و انحصاري شبکه استفاده مي شود .

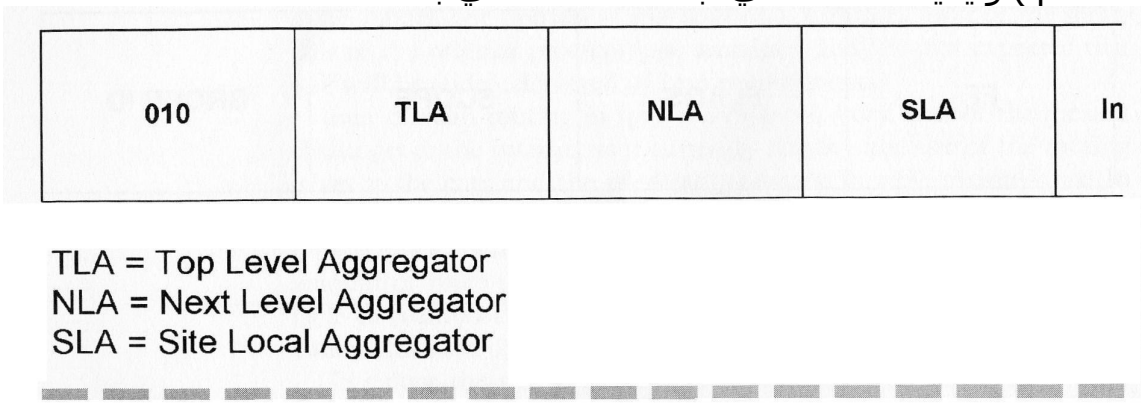
FEDC::1234:2345:2222/64

**آدرس های Unicast**

شکل و فرمت آدرس هاي unicast جهاني براي استفاده در یك گره ( node) IPv6 در شکل3 نشان داد ه شده است اولین سه بیت که بصورت 010 مي باشد نشان مي دهد که این آدرس یك آدر س unicast جهاني قابل قبول مي باشد فیلدهاي بعدي همگي فیلدهاي با طول ثابت هستند که فهرست و تهیه کننده ID هاي با طول متغیر در IPv6 با تجسم قبلي را جایگزین مي کند .

با13 بیت که براي Top Level Aggregator در نظر گرفته شده است اختصاص دادن TLA ، 2^13=8192 امکانپذیر است و انتظار مي رود که این تعداد آدرس براي پوشش دادن به نقط اصلي دسترسي به هسته اینترنت در آینده کافي باشد و اختصاص هر

كدام از اين TLA ها در حالت فيزيكي معادل با يك فراهم كننده زيرساخت ( backbone provider ) و يا يك نقطه اصلي تبادل اطلاعات مي باشد .




شكل 3

- شكل يك آدرس unicast

NLA ( Next Level Aggregator ) معادل است با يك ISP بخصوص و SLA ( Site Local Aggregator ) معادل است با قسمتي از يك سايت مشخص و يا محل قرار گرفتن يك كاربر انتهايي . با استفاده از اين روش NLA و TLA ممكن است تغيير يابد اما SLA و ID مربوط به اينترفيس ثابت باقي خواهند ماند .

درحقيقت ID مربوط به يك اينترفيس يك شماره منحصر به فرد جهاني است كه از فرم استاندارد IEEE EUI-64 استفاده مي كند . استاندارد IEEE EUI-64 بر پايه استفاده از آدرس معروف48 بيتي استاندارد IEEE 802 بنا شده است كه به آدرس فيزيكي يا MAC address ( Medum Access Control ) معروف بوده و يك آدرس واحد جهاني است و با استفاده از يك آدر سMAC ميتوان يك آدرس EUI-64 ، 64 بيتي با اضافه كردن اعداد هگزا دسيمال FF و FE بين هشت تايي هاي سوم و چهارم آدرس MAC اصلي بدست آورد .

همانطور كه در IPv4 آدرس هاي بخصوصي وجود داشت در IPv6 هم آدرس هاي بخصوصي وجود دارد ، مثلا آدرس 127.0.0.1 در IPv4 بعنوان آدرس loopback استفاده مي شود در IPv6 هم آدرسهاي بخصوص جالبي مانند بعضي از آدرسهاي غير مشخص ، آدرس loopback ، آدرسهاي site local و link local وجود دارد .

آدرس غير مشخص ( unspecified ) در IPv6 آدرسي است كه تمامي بيتهاي آن صفر ( 0 ) باشد ممكن است از آن براي آدرس مبداء يك ايستگاه بتوان استفاده نمود قبل از اينكه آن ايستگاه IP آدرس بخصوصي را گرفته باشد .

آدرس loopback در IPv6 عدد ساده 1 مي باشد كه مي توان آن را به شكل ::1 نوشت ، سازمانهايي كه مي خواهند شبكه داخلي خود را با استفاده از تكنولوژي

IPv6 اجرا كنند مي توانند از آدرسهاي site local استفاده كنند ، آدرس دهي با استفاده از site local پيش شماره ( prefix ) مخصوص خود را دارد كه عبارت است از 1111 1110 11 .

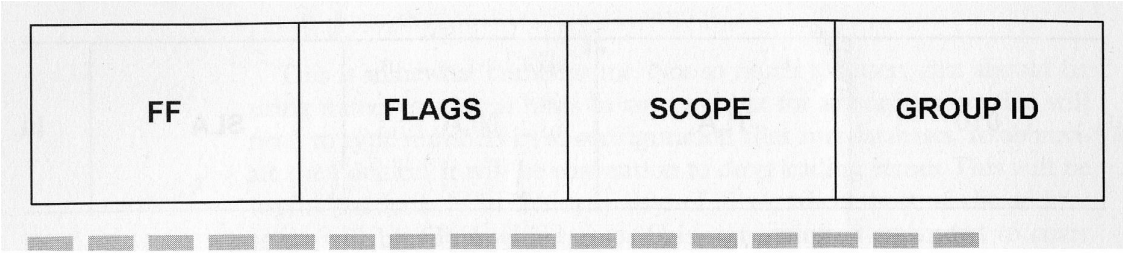
آدرس site local كامل شامل پيش شماره مخصوص خود ، تعدادي از صفرها ،ID زير شبكه و ID اينترفيس مي باشد .

دستگاهها و افزارهايي كه توسط آدرس پايه تهيه كننده و يا آدرس site local پيكربندي نشده اند ممكن است از آدرس هاي link local استفاده كنند كه شامل كد يا پيش شماره هاي محلي (local prefix ) (10 1110 1111 ) ، تعدادي از صفرها و ID اينترفيس مي باشد .

**آدرسهای Multicast و Anycast**

IPv4 از سال 1988 زماني كه آدرسهاي كلاس D و IGMP Internet Group ( Multicast Protocol ) پيشنهاد شده است حالت multicast را پشتيباني كرده است ، IPv6 با قابليتهاي multicast ساخته شده است و اين قابليتها در داخل پروتكل ICMP موجود در IPv6 طراحي شده است .

شكل آدرس multicast مربوط به IPv6 در شكل 4 نشان داده شده است كه شامل هشت بيت ( 8 bit ) يك ( 1 ) بصورتFF ، چهار بيت ( 4 bit ) پرچم ( flag ) و چهار بيت (4 bit ) scope و صدودوازده بيت (112 bit) group ID مي باشد ، تمامي طول فيلد پرچم يك آدرس گذرا و بي ثبات است و از آن بعنوان آدرس دائمي و هميشگي استفاده نميشود ( مانند آدرس هايي كه براي شبكه هاي آزمايشي مانند MBONE استفاده مي شود ) ، از فيلد scope جهت محدود كردن توسعه و افزايش بسته هاي ( packet ) حالت multicast استفاده مي كنند مانند مجزا نگهداشتن ويدئو كنفرانس محلي بجاي اينكه آن را از طريق شبكه جهاني اينترنت منتقل نماييم .




شكل 4

- شكل و فرمت يك آدرس multicast در IPV6

مثالهايي از آدرسهاي multicast عبارتند از FF02::1 كه براي آدرس دهي تمامي گره ها بكار مي رود و FF02::5 كه براي مشخص كردن تمامي روترهايي كه با پروتكل OSPF كار مي كنند به كار مي رود .

Anycast خيلي جديد مي باشد و آدرسهاي معروفي مانند تركيبات آدرسهاي multicast در حالت anycast مورد استفاده قرار مي گيرد ، اختلاف بين multicast و anycast در اين است كه بسته anycast به نزديكترين افزار و وسيله تحويل مي شود كه آن افزار و وسيله عضو گروه anycast مي باشد و اين وظيفه و عمل مي تواند در مشخص كردن چيزهايي شبيه نزديكترين زمان يا نام server در شبكه باشد .

## مسيريابی در داخل و خارج دامنه Inter and Intra Domain Routing

مسيريابي در داخل دامنه ها براي مديريت شبكه هاي خصوصي يكي از معروفترين و مهمترين نوع مسيريابي ها مي باشد ملاحظه نموديم كه براي مسيريابي داخل دامنه با يك Autonomus System در IPv4 از نسخه هاي مختلف پروتكل هاي مسيريابي مانند RIP ، OSPF ، IGRP و ديگر پروتكل ها استفاده مي شود .

گروه كاري IETF پروتكل RIP و OSPF را به روز مي كنند تا مسيريابي درIPv6 را اصلاح كنند و ما ميتوانيم انتظار داشته باشيم كه نسخه هاي مختلف IPv6 پروتكل هاي مختلف مسيريابي مانندCisco EIGRP را هم پشتيباني كند .

به روز كردن OSPF خيلي راحتتر است زيرا همانطور كه يك آدرس 32 بيتي در IPv4 در ديتابيس مسيريابي ظاهر ميشود در IPv6 نيز يك آدرس 128 بيتي ظاهر

خواهد شد . پروتكل RIP در IPv6 براي به روز كردن جدول مسيريابي همانند IPv4 از روش distance vector استفاده مي كند و همانند خاصيت broadcasting يا پخشهاي به روز رساني با پروتكل UDP كه هر 30 ثانيه يك بار اطلاعات و محتويات جداول مسيريابي را به همسايه ها مي فرستد عمل ميكند ، چون بسته هاي به روز رساني پروتكل RIP خيلي كوچك هستند قسمت اعظم پروتكل بدون تغيير باقي مي ماند ، بنابراين انتظار نمي رود كه پروتكل مسيريابي RIP در IPv6 گستردكي و تغييرات زيادي داشته باشد ، مسير يابي بين ناحيه ها در IPv6 داستان ديگري دارد ، يكي از مشكلات اصلي در شبكه جهاني اينترنت اين است كه اندازه آن روز به روز بزرگتر و بزرگتر مي شود بنابراين اندازه جداول مسيريابي در هستة شبكه بزرگتر مي شود و نگهداري اين جداول و مديريت كردن آنها خيلي سخت و دشوار است .

در سال 1995 اينترنت با خطر جدي مواجه بود بطوريكه اكثر ارتباطات آن با مشكل مواجه شده بود و ارزيابي و درست كردن آن نيز كار بسيار سختي بود ، در آن موقع شركت Cisco يك روش سريع و آسان براي جلوگيري از مشكلات فوق ارائه كرد ، مطابق اين روش اندازه اطلاعات به روز رساني مسيرها ( route updates ) كه به شبكه اينترنت ارسال مي شد كاهش پيدا مي كرد و اين باعث كم شدن محاسبات جداول مسيريابي در روترهاي مركزي شبكه اينترنت و كاهش حجم جداول مسيريابي تشكيل يافته و در نتيجه كاهش عرض باند ( bandwidth ) مصرفي براي انتقال اين جداول مسيريا بي مي شد .

براي كاهش حجم و اندازه جداول مسيريابي روترهاي موجود در هسته مركزي اينترنت بايد اطلاعات موجود در آنها فشرده شود ، امروزه متراكم سازي به مواردي مانند اختصاص دادن آدرس شبكة كلاس **C** ، 195.X.X.X مثلا به اروپا ميباشد كه اين عمل به روترهاي موجود در كل شبكه اينترنت اجازه مي دهد كه در هر كجاي دنيا كه باشند تنها يك مسير فشرده براي دسترسي به تمامي زير شبكه هاي كلاس C اشاره شده ، در جداول مسير يابي خود داشته باشند بجاي آنكه مسيرهاي منحصر به فرد و مجزايي براي هر كدام از اين زير شبكه ها كه همگي در يك ناحيه هستند داشته باشند .

مسيريابي بين ناحيه ها ( Inter Domain ) در IPv6 بر اساس خاصيت سلسله مراتبي آدرسهاي تهيه كنندگان سرويس اينترنت انجام گرفته است تا با استفاده از آن

بتوان حجم جداول مسيريابي روترهاي هسته مركزي شبكه اينترنت را كاهش داد ، اين تصور اوليه در مورد طرح و نقشه مرتب كردن آدرس دهي در IPv6 توپولوژي شبكه را راحتتر ميكند ، بعلاوه بروزرساني بين نواحي هم در IPv6 با استفاده از پروتكل مسير يابي بين ناحيه ها ( Inter Domain Routing Protocol ) انجام مي شود كه اين خود حركت مهم وعظيمي است براي رهايي از وضعيت كنوني كه با استفاده از پروتكلBGP4 انجام مي شود . علت اين كه BGP4 در دنياي IPv6 استفاده نمي شود اين است كه BGP4 در آدرس دهي 32 بيتي به سختي بهينه مي شود بنابراين نمي توان به راحتي آن را براي آدرس دهي 128 بيتي اصلاح نمود .

تفاوت اصلي و عمده BGP با IDRP به شرح زير است :

- BGP از TCP براي ارسال پيغامهاي به روز رساني استفاده مي كند در صورتي كه IDRP از سرويس داده گرام ( Datagram service ) براي اين منظور استفاده مي كند .
- BGP از شمارة سيستم خودگردان ( Autonomous System ) 16 بيتي براي تشخيص ناحيه ( Domain ) استفاده مي كند در صورتيكه IDRP از كدهاي محلي كه از آدرسهاي با طول متغير تشكيل شده است استفاده ميكند .
- IDRP مسيرهاي مربوط به سيستم هاي خود گردان ( Autonomous System Path ) را با استفاده از جمع آوري و خلاصه كردن مسيرها فشرده مي سازد .

## پيدا كردن همسايه Neighbor Discovery

عمل پيدا كردن همسايه (Neighbor Discovery ) در شبكه هاي IPv6 فعل و انفعالي را كه بين گره ها ي موجود در آن شبكه اتفاق مي افتد را شرح مي دهد ، براي مثال جهت ارسال يك بسته اطلاعاتي ( Packet ) به يك شبكه دور دست دستگاه و افزاري كه بسته را توليد مي كند جهت ارسال آن نياز به آدرس روتري كه داراي آدرس جهش ( hop ) بعدي است دارد ، در IPv4 اين كار با استفاده از پروتكل ARP(Address Resolution Protocol) انجام مي گرفت كه اين پروتكل

ليستي از آدرسهاي محيطي ( مانند MAC ) را نگهداري مي كرد و به آدرسهاي IP مربوطه ارتباط مي داد .

در اين مورد IPv6 پيشرفت زيادي داشته است ، تمامي مكانيزمهايي كه به روابط و اثرات متقابل بين روترها و ميزبانها ( hosts ) در يك قسمت از شبكه مربوط مي شود تنها در يك پروتكل خلاصه شده است و آن عبارتست از پروتكل پيدا -كردن همسايه يا NDP ( Neighbor Discovery Protocol ) كه اين پروتكل درواقع جايگزين مناسبي براي پروتكل هاي ARP ( Address Resolution Protocol ) و ICMP ( Internet Control Message Protocol ) در IPv4 مي باشد كه در مد پيشرفته براي تشخيص روترها با قابليت و كارايي بهتر و بالاتر به كار مي رود .

برخلاف IPv4 كه در آن تحصيل و تفكيك كردن آدرسها از لايه IP تا لايه ديتا لينك بر اساس خاصيت پخشي ( broadcast ) پروتكل ARP مي باشد در IPv6 اين عمل با استفاده از خاصيت multicast انجام مي شود و اين كار باعث مي شود كه وقفه هاي ( interrupt ) ناشي از تفكيك پذيري آدرسها در گره هاي شبكه تا حد قابل توجهي تقليل يابد .

IPv6 پيغامهايي را كه ICMP منعكس مي كند با پيغامهاي ND جايگزين مي كند ، براي پشتيباني كردن از چندين زير- شبكه در يك قسمت از شبكه فيزيكي IPv6 محدوديت پذيرش پيغامهاي منعكس شده را كمتر كرده است و به هر ميزبان اجازه مي دهد كه اين پيغامها را بدون توجه به اينكه از كجا منعكس شده و همچنين بدون توجه به اينكه آيا جهش (hop ) بعدي ( كه در آن پيغام مشخص شده ) در همان زير شبكه اي است كه ميزبان در داخل آن قرار دارد يا نه ، بپذيرد ، بعلاوه برخلاف IPv4 كه در آن پيغامهاي منعكس شده از پروتكل ICMP فقط مي تواند يك روتر را مشخص كند ، آدرس مقصدي كه توسط پيغامهاي منعكس شده از پروتكل ND حمل مي شود مي تواند يك روتر يا حتي مقصد نهايي يعني يك ميزبان را هم مشخص كند ، براي جلوگيري از موارد اضافي در نگاشتن ( mapping ) آدرسها از لايه IP به لايه ديتا لينك پيغامهاي منعكس شده ND هم شامل آدرس IPv6 و هم شامل آدرس لايه ديتا لينك مقصد مي باشد .

يكي از مشكلات مشترك كه بين يك ميزبان با روتري كه بعنوان اولين جهش ( hop ) مي باشد اتفاق مي افتد مشكل مشخص كردن خطاهاي روتر ( تشخيص روتر خراب dead router ) مي باشد ، جهت به حداقل رساندن خطاهاي ناشي از خرابي روترها در شبكه ، ND يك مكانيزم صريح و روشني را پيشنهاد كرده است بطوريكه به يك گره اجازه مي دهد (آن گره مممكن است روتر باشد يا ميزبان ) كه تشخيص دهد آيا گره هاي ديگر در قسمتهاي مختلف همان شبكه ( هم روتر و هم ميزبان ) بالا (up ) مي باشد يا نه .

در مقايسه با IPv4 اطلاعات آدرس دهي كه توسط ND منتقل مي شود time out ( اتمام زمان ) را مشخص مي كند ، اين time out كه توسط فرستنده هاي اطلاعات مشخص مي شود به آنها اجازه مي دهد كه مستقيما زمان زندگي ( life time ) اطلاعات خود را كنترل كنند ، انتظار مي رود كه اين ويژگي از اهميت بخصوصي برخوردار باشد، مخصوصا در حالتي كه اطلاعات نسبتا متحرك (dynamic) باشد ( بعنوان مثال براي ميزبانهاي متحرك - mobile host) .

ND ميزبانهايي را كه داراي اطلاعاتي مانند ماكزيمم جهش (hop–count) مي باشد را فراهم مي كند كه اين ميزبانها در بسته هايي كه به بيرون فرستاده مي شوند و همچنين در بعضي از پارامتر هاي بخصوص لايه ديتا لينك مانند MTU ( Maximum Transmission Unit ) مورد استفاده قرار مي گيرند .

از آنجايي كه ND رابطه متقابل بين گره ها ( روترها و ميزبانها ) در قسمتهاي مختلف يك شبكه را بهبود مي بخشد لازم نيست همه اين اصلاحها توسط اين پروتكل در دسترس باشد ، بسياري از وظايفي كه توسط ND تامين مي شود بر اين تصور استوار است كه لايه ديتا لينك قابليت و توانايي هاي multicast را با روش و اسلوب ساده و خاص ( مشابه آنچه كه در استاندارد اترنت وجود دارد ) ، پشتيباني كند . محيط هايي كه لايه ديتا لينك آنها multicast را پشتيباني نمي كند مانند شبكه هاي ATM ( Asynchronous Transfer Mode ) يا سيستم هايي كه نسبتا گران قيمت هستند ، استفاده از سرورهاي multicast براي پشتيباني كردن كامل پروتكل ND در آنها قائدتا ممكن است بهينه نباشد .

## انتقال از IPv4 به IPv6 The Transmission from IPv4 to IPv6

تهيه يك روش انتقال با قابليت مديريتي از IPv4 به IPv6 يك موفقيت قطعي براي IPv6 محسوب مي شود ، در طي مدت انتقال ضروري به نظر مي رسد كه حالت سازگاري با روترها و ميزبانهايي كه بر اساس IPv4 نصب شده اند و در حال حاضر در حال كار هستند حفظ شود و به كاركرد آنها لطمه اي وارد نشود زيرا خيلي به سختي مي توان پيش بيني كرد كه اين انتقال چقدر طول مي كشد و مي توان تصور كرد كه پيدا كردن چنين سازگاريي به زمان خيلي زيادي نياز دارد .

در حقيقت بسياري از پيشگوييها براي انتقال به پروتكل هاي پيشرفته IP در آينده نزديك اتفاق خواهد افتاد در حالي كه اينترنت از IPv4 به IPv6 در حال انتقال است ، تا حدود ساده اي مي توان انتقال را مركب از دو جزء زير دانست ، اولي انتقال به ميزبانهاي IPv6 و دومي انتقال به پروتكل هاي مسيريابي و چگونگي مسيريابي در IPv6 .

انتقال به ميزبانهاي IPV6 بر اساس اين فرضيه است كه هر ميزبان داراي دو پشته ( stack ) خواهد بود كه عبارتند از IPV6 و IPv4 ، هر ميزباني داراي دو وظيفه و عمل خواهد بود مثل اينكه دو ميزبان مجزا از هم هستند و يكي از آنها با IPv6 و ديگري با IPv4 كار مي كنند و يك API (Application Programming Interface ) بر روي اين ميزبان نصب خواهد شد كه هم IPv4 و هم IPv6 را پشتيباني مي كند و ارتباط بين آن دو را بر قرار مي كند ، API مورد نظر شبيه API هايي خواهد بود كه هم اكنون در دنياي IPv4 به مورد اجرا در مي آيند .

اجراي پشته IPv6 در ميزبانها و گسترش دادن توانايي API ها در IPv6 يكي از مراحل و گامهاي ضروري براي انتقال به IPv6 محسوب مي شود ، البته اين مراحل به اين معني نيستند كه IPv6 را مفيد و كارا جلوه دهند ، در حقيقت عليرغم اينكه تابحال تعداد قابل ملاحظه اي از برنامه هاي كاربردي شبكه ها به API ها ي سازگار با IPv6 منتقل شده است ولي باز هم تصور استفاده گسترده از IPv6 غير واقعي به نظر مي رسد .

بنابراين از نظر و ديدگاه يك ميزبان نتيجه پشتيباني از IPv6 مشابه منتشر كردن و انتقال تمامي پشته هاي TCP/IP از لايه شبكه به لايه كاربرد مي باشد و مقدار تلاشي كه براي كامل كردن اين موضوع لازم است و همچنين توانايي و پتانسيل لازم براي رفع عيب مقدماتي نرم افزارها بعنوان نتيجه اين اصلاح ، تلاش و كوششي است كه نبايد آن را ناچيز پنداشت .

انتقال به مسيريابي IPv6 بعنوان گسترش دادن روترها تلقي مي شود به شرطي كه اين روتر ها بتوانند عمل مسيريابي و به جلو راندن بسته ها (packet ) را هم در IPv4 و هم در IPv6 انجام دهند ، پروتكل هاي مسيريابي كه انتظار مي رود در IPv6 مورد استفاده قرار گيرد ( همانطور كه قبلا مورد بررسي قرار گرفت ) در واقع گسترش يافته پروتكل هاي مسيريابي موجود در IPv6 مي باشد ، بنابراين انتظار مي رود كه مسئله و مشكل قابل ملاحظه اي در سيستم مسيريابي IPv6 نداشته باشيم ، جهت به حداقل رساندن وابستگي انتقال به پروتكل هاي مسيريابي IPv6 تصور مي شود كه هيچگونه پيوستگي بين قسمتهاي مختلف IPv6 در دنياي اينترنت وجود ندارد ، ارتباط ميزبانها در محدوده IPv6 و در قسمتهاي مختلف شبكه با ايجاد تونل هاي بخصوصي صورت مي گيرد ، اين تونل ها ترافيكs IPv6 را با استفاده از بسته هاي IPv4 جابجا مي كند ، بنابراين استفاده از تونلهايي كه بتواند ترافيك IPv6 را بر روي روترهايي كه با پروتكل IPv4 كار مي كنند را منتقل نمايند يكي از اجزاء ضروري در انتقال مسيريابي از IPv4 به IPv6 مي باشد .

IPv6 به دو نوع از اين تونلها اجازه دسترسي مي دهد (IPv6 داراي دو نوع تونل مي باشد) ، تونلهايي كه بصورت خودكار ( automatic ) ايجاد مي شوند و تونلهايي كه بصورت دستي ( manually ) پيكربندي مي شود ، در تونلهاي خودكار به پيكربندي دستي مجزا و تك به تك نيازي نيست هرچند كه استفاده از تونلهاي خودكار نياز به دو پيش نياز دارد .

آدرس هاي IPv6 ميزبانها كه از طريق تونلهاي خودكار قابل دسترسي هستند بايد با IPv4 سازگار باشند و همچنين آدرسهاي IPv4 كه براي تشكيل آدرسهاي IPv6 ميزبانها مورد استفاده قرار مي گيرند بايستي قابل مسيردهي باشند ، بعلاوه

استفاده از تونلهاي خودكار در حال حاضر فقط براي حالتي تعريف مـي شـود كـه نقطـه انتهايي در طرف مقابل تونل ميزبان باشد زيرا استفاده از تونل خودكار بين روترها تعريف نـشده اسـت ، توانـايي ايجـاد تونلهـاي خودكـار بـين هـر جفـت از ميزبـان IPv6 كـه آدرسIPv6 آنها بـا آدرسIPv4 آنهـا سـازگار باشـد بـه ميزبانهـا اجـازه مـي دهـد كـه از بسته بندي ( encapsulation ) IPv6 براي نقل و انتقال اطلاعات نقاط انتها به انتهاي ( end-to-end ) از IPv4 اسـتفاده كنـد بـدون آن كـه بـراي پـشتيباني كـردن IPv6 بـين ميزبانها به روتر نيازي داشته باشد اين كار انتقال آدرس هاي ميزبان IPv6 را بـدون نيـاز به به روز كردن جداول مسيريابي از IPv4 به جداول مـسيريابي IPv6 آسـانتر و راحتتـر مي كند .

## امنيت در IPv6 IPv6 Security

امنيت يكي از مشخصات داخلي پروتكل IPv6 است كه شامل هر دو مورد تصديق ( Authentication ) و رمز -نگاري ( Encryption ) در لايه IP پروتكل جديد است ، هر چند IPv6 داراي فرايندي براي Authorization كه در دامنه برنامه هاي كاربردي قرار دارد نمي باشد .

IETF داراي سازماني است كه به گروه كاري (working group) امنيت در IP ( IP Sec ) معروف است و اين سازمان وظيفه دارد كه مكانيزمهاي امنيتي مورد نياز در لايه هاي مختلف IP را هم در IPv6 و هم در IPv4 جهت گسترش و بهبود استاندارد هاي مورد نياز بر عهده گيرد ، اين گروه همچنين وظيفه دارد پروتكل هاي مديريتي كليدي عمومي ( Key Management Protocols ) را جهت استفاده بيشتر در شبكه جهاني اينترنت توسعه و گسترش دهد .

تصديق ( Authentication ) اين قابليت را به گيرنده بسته مي دهد كه مطمئن شود كه آدرس مبداء معتبر بوده و بسته در طول زمان انتقال دچار تغيير و دستكاري نشده است .

رمز نگاري ( Encryption ) اطمينان حاصل مي كند كه تنها گيرنده اصلي بسته بتواند به محتويات آن دسترسي داشته باشد بعبارت ديگر رمزنگاري باعث مي شود كه تنها گيرنده اي به محتويات بسته دسترسي داشته با شد كه بسته به آن اسال شده است . براي بررسي و تحليل اين مزايا يك سيستم كليدي بكار گرفته مي شود كه به موجب آن فرستنده ها و گيرنده ها بر روي يك مقدار كليدي كه مورد استفاده قرار مي گيرد با هم به توافق مي رسند ، سيستم مديريت كليدي عمومي كه توسط طراحان IPv6 پذيرفته شده است مكانيزم ISAKMP-OAKLEY مي باشد ، ISAKMP مخفف كلمات Internet Security Association and Key Management Protocol است كه روشهاي اجراي عمومي پروتكل مديريت كليدي را تامين مي كند ، پيغامهاي ISAKMP با استفاده از پروتكل UDP رد وبدل مي شوند و از شماره پورت 500 ا ستفاده مي كنند ، ISAKMP اجاز مي دهد كه چندين نوع از مكانيزمهاي تغييرات كليدي مورد استفاده قرار گيرد اما در محيط IPv6 به نظر مي رسد كه پيشنهادهاي OAKLEY داراي سازگاري بيشتري مي باشد .

علاوه بر سيستم كليدي كه در بالا اشاره شد گيرنده ها و فرستنده ها بايد در بعضي از موارد در مورد تغيير و ايجاد تعدادي از پارامترها ي امنيتي با همديگر به توافق برسند تا بتوانند با تركيب آنها هر چه بيشتر امنيت را بالا ببرند ، از جمله اين پارامترها مي توان به كليدهاي اشاره شده ( key ) ، الگوريتم تصديق ( Algorithm Authentication ) ، الگوريتم رمزنگاري ( Encryption Algorithm ) و ساير پارامترها مانند طول عمر ( life time ) يك كليد اشاره نمود .

با به هم پيوستن و تركيب روشهاي امنيتي فوق و استفاده از آنها گيرنده ها فقط بسته هايي را باز خواهند كرد كه آن بسته ها از روشهاي امنيتي منحصر به فرد اشاره شده براي رسيدن به آن گيرنده استفاده كرده باشند ، با اين روش هر كدام از بسته هاي تصديق و رمزنگاري شده يك پارامتر امنيتي مرجع بنام SPI ( Security Parameter Index ) با خود حمل خواهد كرد ، بعنوان نمونه SPI انتخاب شده توسط گيرنده چگو نگي ساخت بسته و اين كه آن بسته چگونه به مقصد برسد را مشخص مي كند .

در عمل ، تصديق ( Authentication ) در دنياي IPv6 از طريق يكي از روشهاي گسترش هدرهاي عمومي كه قبلا مورد بررسي قرار گرفت و به هدر تصديق ( Authentication Header ) معروف است انجام مي شود ، ديتاي مورد نياز براي تصديق با انجام چند عمل رياضي بر روي آدرس مبداء و همچنين روي تعدادي از فيلدهاي هدرIP به دست مي آيد ، ديتاي به وجود آمده را به محتواي بسته اصلي اضافه كرده سپس آن را ارسال مي كنند .

الگوريتم مورد نياز براي توليد مقادير رمزنگاري شده ( كه بعنوان checksum از آنها ياد مي شود ) بر پايه روش MD5 ( Message Digest 5 ) استوار است كه در واقع نوع ديگري از الگوريتم خلاصه كردن پيغام مي باشد .

اين الگوريتم خيلي سختتر از آن است كه كسي بتواند آن را دستكاري نمايد ، تغييراتي در آن اعمال كند و يا مطمئن شود كه بدون دخالت آدرس مبداء بسته مورد نظر بصورت سالم و دستكاري نشده به مقصد رسيده است يا نه ، هدر تصديق ( Authentication Header ) payload را رمزنگاري نمي كند ، بنابراين در اين مرحله بسته ها آسيب پذير هستند و ممكن است كه هنوز توسط كساني كه گيرنده واقعي بسته نيستند خوانده شوند ، براي جلوگيري از اين كار هدر ESP ( Encrypted Security Payload ) مورد استفاده قرار مي گيرد ، ESP هميشه اولين هدر بعد از هدر IPv6 است چون اطلاعات payload و تصديق را رمز نگاري مي كند ، مدل از پيش تعيين شده براي رمزنگاري بر اساس استاندارد رمزنگاري ديتا ( Data Encryption Standard ) مي باشد كه به Cipher Block chaining معروف است .

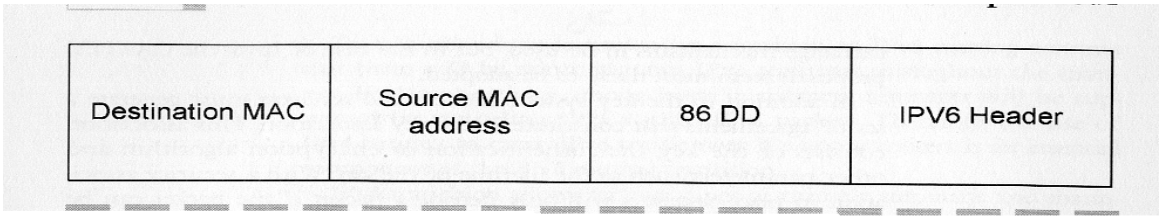
وظايف امنيتي پيشرفته در لايه IP پروتكل IPv6 انجام ميشود و بيشتر براي ارتباط بين كامپيوترهاي متحرك ( mobile computer ) ، ارتباط بين ميزبانهاي با امنيت بالا و امن ساختن ساير ارتباطات و عمليات شبكه مانند پيدا كردن همسايه ها و تغيير اطلاعات مسيرها و ... بكار ميرود ، البته توجه به اين نكته ضروري است كه تجربه نشان داده است عمل رمزنگاري مسيرها تا حد قابل توجهي بار پردازشگر مسيريابها را زياد خواهد كرد ، مخصوصا اگر در لينكها خرابي ايجاد شده باشد باعث ايجاد حالت Triggered-updates خواهد شد و محاسبه مسير ها مجددا تكرار خواهد شد.

# IPv6 در لایه دیتا لینک توپولوژیهای مختلف

همانطور که قبلا اشاره شد فرایند پیدا کردن همسایه در محیط هاي مختلف قابل اجرا مي باشد ، اختلاف کمي در چگونگي ساخته شدن بسته هاي IPv6 در لایه دیتا لینك توپولوژي بخصوص وجود دارد که در زیر تعدادي از آنها را مورد بررسي قرار مي دهیم .

**الف ) Ethernet**

Ethernet ساده ترین حالت مي باشد بنابراین ابتدا آن را بررسي مي کنیم ، یك بسته Ethernet که دیتاي IPv6 را حمل مي کند شبیه بسته اي خواهد بود که در شکل 5 نشان داده شده است ، همانطور که قبلا مورد بررسي قرار گرفت هدرهاي Ethernet II داراي یك فیلد مخصوصي است که پروتکل لایه شبکه را که در بسته هاي Ethernet وجود دارد مشخص مي کند ، IPv6 براي مقدار دهي فیلد بخصوص فوق از عدد هگزا دسیمال86DD استفاده مي کند .




شکل 5

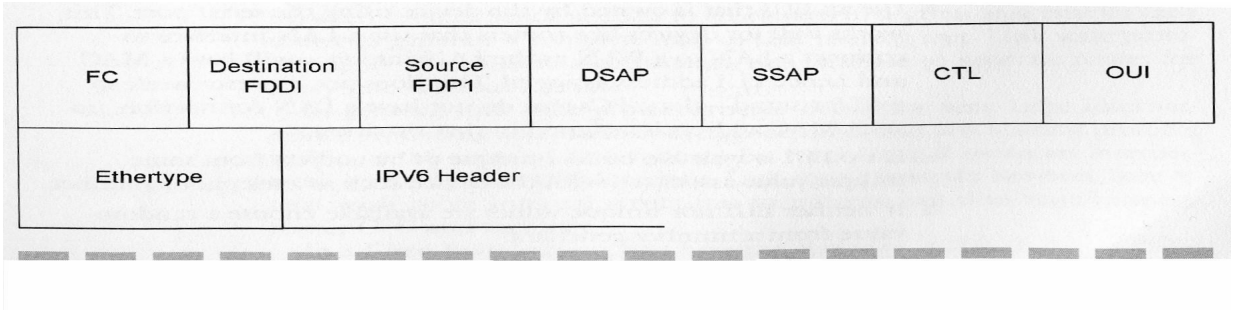
- بسته های توپولوژی Ethernet در IPv6

در محیط Ethernet آدرس IPv6 هر ایستگاه کاري از ترکیب ( Link Local Prefix LLP ) ، (که توسط یك سرور آدرس محلي اختصاص داده میشود) و آدرس 64 بیتي EUI اینترفیس استنتاج میشود ، این آدرس سپس به عنوان آدرس مبداء در هدر IPv6 مورد استفاده قرار مي گیرد ، آدرس لایه دیتا لینك یك افزار در یك قسمت از

شبکه با استفاده از روشهاي عادي پيدا کردن همسايه که قبلا به آنها اشاره شد ، مشخص خواهد شد .

**ب) FDDI**

IPv6 در محيط FDDI با اختلاف خيلي جزيي شبيه Ethernet مي باشد ، FDDI يك محيط حلقه اي بسته با شمارشگر گردشي حلقه ها است که مدار خود را از طريق حلقه فيزيکي مي بندد و گره هاي ( nodes ) FDDI را به همديگر متصل ميکند ، هر فريم شامل دو هدر FDDI و LLC مي باشد و همانطور که در شکل 6 نشان داده شده است بر هدر IPv6 تقدم دارند .




شکل 6

- بسته هاي توپولوژي FDDI در IPv6

تشکيل آدرس IPv6 توپولوژي FDDI دقيقا به همان روش تشکيل آدرس IPv6 توپولوژي Ethernet مي باشد ، يعني آدرسهاي اينترفيسهاي FDDI با ترکيب پيش شماره محلي لينك ( LLP ) و آدرس 64 بيتي EUI لايه ديتا لينك تشکيل مي شود .

بقيه فيلدهاي بسته را مي توان به شکل زير توصيف کرد :

FC کد فريم FDDI است که مي توان مقدار آن را از 50 تا 57 ، HEX قرار داد ، و براي تعيين و تعريف تقدم يك فريم در حلقه از آن استفاده مي شود آدرس هاي مبدا و

مقصد ( Destination and Source Address ) همان آدرس 48 بيتي است كه به اينترفيس اختصاص داده شده است.

DSAP و SSAP مخفف Destination and source Service Access point مي باشد و به مقدار HEX 33 ست مي شوند .

فيلد CTL كه به فيلد كنترل كننده لايه ديتا لينك ( Link Level Control ) معروف است به مقدار 03 ست مي شود تا اطلاعاتي را كه داراي هيچگونه شماره و ترتيبي نيستند را مشخص كند .

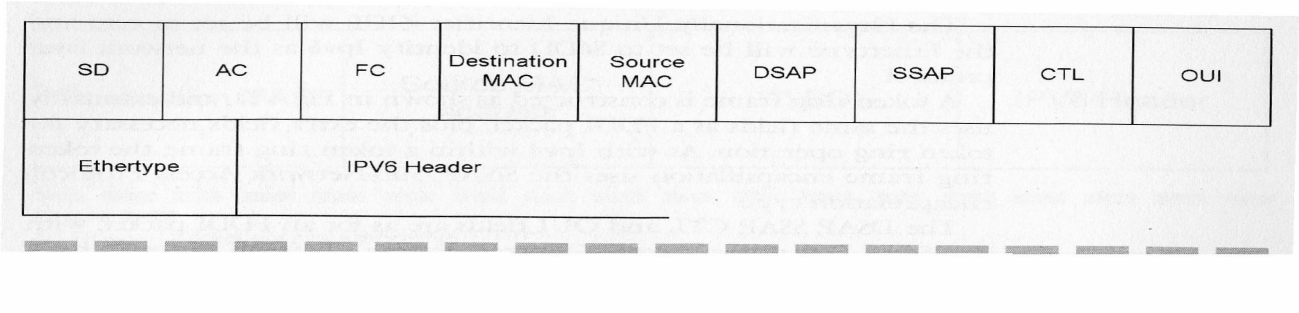
OUI (Organizationally unique Identifier) را 0 قرار مي دهند.

Ethertype به 86DD ست شده است تا مشخص شود كه پروتكل لايه شبكه IPv6 مي باشد .

**ج ) Token – Ring**

فريم هاي توپولوژي حلقه نشانه ( Token-Ring ) همانطور كه در شكل7 نشان داده شده است ساخته مي شوند ، و چنانكه مي بينيد از همان فيلدهايي كه بسته FDDI استفاده مي كرد بعلاوه فيلدهاي اضافي مورد نياز براي عملكرد توپولوژي حلقه نشانه استفاده مي كند .

همانند بسته بندي ( Encapsulation ) توپولوژي حلقه نشانه در IPv4 ، بسته بندي فريم هاي آن درIPv6 نيز با استفاده از روش بسته بندي SNAP ( Subnetwork Access protocol ) انجام مي شود




شكل 7

- بسته هاي توپولوژي Token Ring در IPv6

فيلدهاي OUI , CTL , SSAP , DSAP همانند فيلدهاي بسته FDDI مي باشند ولي Start Delimiter , Access Control , , Frame check , Frame control Sequence , Frame Status در آنها مطابق استاندارد حلقه ـ نشانه خواهد بود ، اينترفيس حلقه نشانه از آدرس 48 بيتي يعني آدرس MAC براي ساختن آدرس هاي EUI استفاده ميكند تا بتواند آدرس هاي IPv6 را به صورت نرمال تشكيل دهد .

محيط توپولوژي حلقه نشانه را مي توان با استفاده از فيلد اطلاعات مسيريابي RFI ( Routing Information Field ) مبداء گسترش داد ، در اين محيط ها RFI مستقيما بعد از آدرس MAC مبداء وارد مي شود .

**د ) PPP**

پروتكل نقطه به نقطه يا PPP ( Point to point Protocol ) براي انتقال بسته هاي IPv6 از روي لينك هاي سريال مورد استفاده قرار مي گيرد ، PPP يك پروتكل ديتا لينك مي باشد كه مانند Ethernet چندين پروتكل لايه شبكه را پشتيباني مي كند ، يك ارتباط PPP با مبادله پيغامي بين دو ديتا لينك شروع مي شود و قبل از اينكه ارتباط بين دو لايه شبكه تثبيت شود،كامل مي شود . جهت برقراري ارتباط در IPv6 ، پروتكل كنترل IPv6 ( IPv6 Control Protocol ) لازم است پروسه مبادله پيغامها را كامل كند .

IPv6 CP شبيه تنظيم كردن پروتكل كنترل لينكPPP ( PPP Link Control Protocol ) مي باشد و در اين حالت توسط ايستگاه انتهايي براي مبادله كردن عملگرهاي IPv6

مانند الگوريتم فشرده سازي (Compression Algorithem ) مورد استفاده قرار مي گيرد ، IPv6 CP از عدد 8057 هگزا دسيمال براي فيلد پروتكل PPP استفاده مي كند و به محض اينكه IPv6 CP مبادله اطلاعات خود را كامل كرد بسته هاي IPv6 از مقدار 0057 هگزا دسيمال براي فيلد پروتكل استفاده مي كنند .

جالبترين قسمت IPv6 در پروتكل PPP اختصاص دادن يك آدرس IPv6 به يك اينترفيس مي باشد ، در پروتكل هاي لايه ديتا لينك قبلي اشاره شده يك آدرس EUI جهاني منحصر به فرد وجود داشت كه نشان مي داد آدرس جهاني IPv6 اختصاص داده شده به اينترفيس منحصر به فرد است ، براي اينترفيسهاي سريال همچون آدرسي اختصاص داده نشده است ، براي تحت پوشش قرار دادن اين حالت اينترفيسهاي PPP از 64 بيت استفاده مي كند كه به (***Interface Token***) معروف است و اطمينان حاصل مي كند يك اينترفيس در طرفين لينك PPP از آدرس منحصر به فرد استفاده مي كند ، اين Token ، 64 بيتي با كد محلي (Prefix ) 64 /:FE80 تركيب مي شود تا يك آدرس لينك محلي را جهت استفاده در لينك PPP تشكيل دهد .

جهت ساختن يك Token اينترفيس در IPv6 چهار انتخاب وجود دارد :

١ ـ استفاده از آدرس EUI اي كه به خود افزار اختصاص داده شده است و از آن براي پورت سريال مي توان استفاده نمود ، اين روش بيشتر براي افزارها و تجهيزاتي به كار مي رود كه مانند روترها داراي يك اينترفيس LAN هستند و داراي يك آدرسMAC بوده و بنا براين داراي آدرسEUI نيز مي باشند، اين مورد به خوبي كار نمي كند مخصوصا در موردPC هاي Stand – alone كه داراي ارتباط شبكه محلي نيستند ، بنابراين داراي آدرسMAC نيز نخواهند بود .

٢ ـ اگر آدرس EUI در دسترس نباشد يك آدرس 64 بيتي واحد از روي مقادير منحصر به فرد اختصاص يافته به افزارها ( unique value ) مانند شماره تلفن و ... بسازيد .

٣ ـ اگر نه EUI و نه مقادير منحصر به فرد اختصاص يافته به افزارها ( unique value ) در دسترس نباشند يك مقدار تصادفي ( random value ) براي ساختن آدرس انتخاب كنيد .

٤ - اگر هيچكدام از روشهاي فوق براي ساختن آدرس در دسترس نباشد و قادر به ساختن آدرس نباشيد ، آدرس مبدا IPv6 را 0 ( صفر ) قرار دهيد .

زماني كه هر اينترفيس تصميم بگيرد كه از Token خود براي برقراري ارتباط استفاده كند اينترفيس طرف مقابل PPP تصور خواهد كرد كه مقدار Token اختصاص داده شده به اينترفيس هاي ديگر با Token آن متفاوت است و لذا ارتباط را برقرار خواهد كرد .