عنوان مقاله :عناوين پيشرفته MPLS

گروه مطالعاتی : IP

گروه کاری : MPLS

ارايه دهنده : هايده عادلي

تاريخ ارايه :۸٤/۱/۲۲

سرپرست گروه کاری :احمد آقا ميرزايي

اصلاح کننده : هايده عادلي

تاريخ اصلاح : ۸٤/۲/۳

مرجع :فصل پنجم کتاب MPLS and VPN Architecture

فصل پنجم : عناوين پيشرفته MPLS

تااين نقطه ، اين كتاب روي توضيح مفاهيم ومكانيزمهايي كه معماري MPLS را مي سازند متمركز شده بود، اما هدف ازاين فصل ارائه اطلاعات بيشتر درموردچند عنوان پيشرفته تركه شمادرهنگام اجراي اين معماري مواجه مي شويد ، ميباشد.

شاخصهايي كه دراين فصل ارائه شده اند،ويژه معماري MPLS بوده ووابسته به هر اجرايي، فارغ از استفاده از ويژگيهاي پيشرفته اي مانند VPN درون اين ساختار، ميباشد.شاخص هاي بيشتري كه جهت اجراي موفقيت آميز معماري MPLS/VPN بسيار مهم ميباشند، را مي توانيد در فصل ۱۳- "شاخص هاي اجراي MPLS/VPN" بيابيد.

قبلاً ديده ايد كه چگونه برچسبهاي MPLS بين همسايه هاي TDP/LDP مجاور گردش مي يابند. بهرحال، ممكن است لازم باشدكه گسترش اين اطلاعات رابه همسايه هاي مشخصي محدود كنيم ياحتي اعلام كلي اطلاعات رابلوكه كنيم. اين فصل به اين امكان نگاهي مي اندازد وبررسي مي كند كه چرا اين ويژگي هنگام اجراي MPLS مي تواند مفيد باشد.اين فصل همچنين نگاهي دارد به اينكه درسيستمهاي سيسكو .INC ، بكارگيري معماري MPLS چگونه مي تواندبابسته هاي بزرگ درانواع معيني از واسطه ها (MEDIA)كه ماكزيمم واحدانتقالي (MTU) دارند كه به طورپيش فرض اجازه افزودن برچسب MPLS به بسته هاي بزرگتر از 1500 بايت رانمي دهد، رفتاركند.

سرانجام ، اين فصل آناليز مي كند كه چگونه MPLS مي تواند لوپهاي ارسالي (Forwarding) راكشف وازآنها جلوگيري كند ومشخص مي كند كه چگونه تراكم اطلاعات مسيريابي IP مي تواند برعملكرد شبكه تاثيربگذارد.

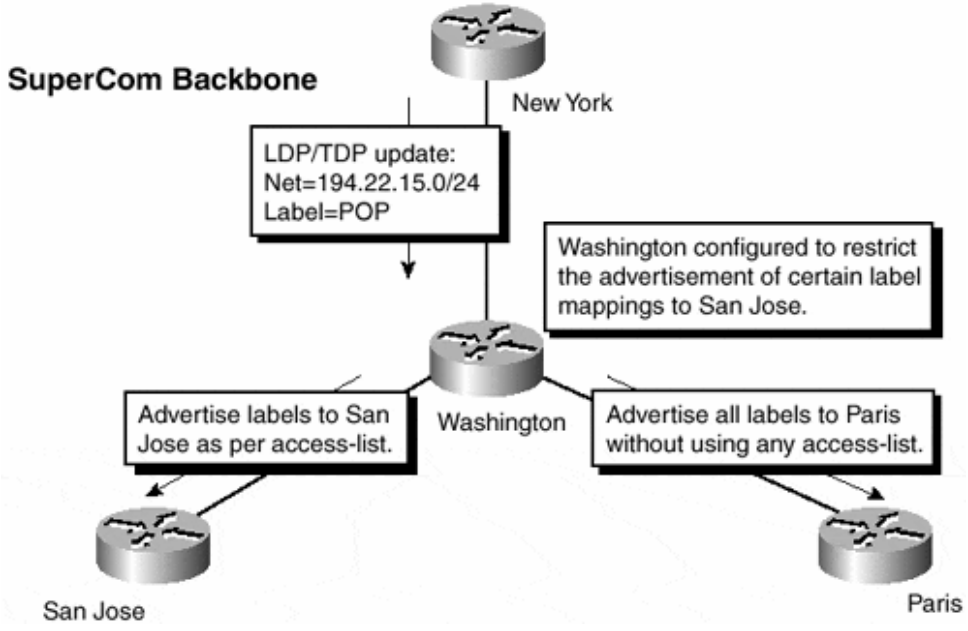
كنترل گسترش نگاشت برچسب

درفصل ۲ ، "عملكرد MPLS درFrame-mode" ، ديديد كه يك پروتكل دروازه داخلي IGP درشبكه MPLS جهت كشف اطلاعات پسوند IP كه با يك كلاس مساوي ارسالي FEC مشخص مرتبط است، بكار ميرود. بعدازاينكه LSR اين اطلاعات راكشف كرد، ممكن است يك برچسب به FEC متصل شود وبه كليه همسايه هاي بالا رونده LDP/TDP بسته به اينكه مدانتشار برچسب پائين رونده ياپائين رونده براساس تقاضا فعال باشد، اعلام گردد.

تصميم چسباندن برچسب به يك FEC به مد كنترلي فعال بستگي دارد. دومدكنترلي وجوددارد: سفارشي ومستقل. فصل ۲ نشان ميدهد وقتي شما مدكنترلي LSP كه مدپيش فرض براي ATM-LSR ميباشد، رااجرامي كنيد، يك LSR فقط به شرطي يك برچسب به يك FEC مشخص مي زند، كه LSR خروجي براي آن FEC باشد، ياقبلاً برچسب الصاق شده اي رابراي آن FEC از LSR پرش بعدي دريافت كرده باشد. اگرشما مد مستقل رابكار ببريد كه درحالت Frame-mode MPLSپيش فرض ميباشد، يك LSR ، مستقل ازبرچسبي كه بايد از LSR پرش بعدي دريافت كند يك برچسب به يك FEC الصاق مي كند.اين شبيه به مسيريابي IP براساس وضعيت لينك، كه درآن هر روتر جدول مسيريابي خودش رامستقلاً مي سازد، ميباشد.

درمعماري MPLS بخاطر روشي كه برچسبها به FEC الصاق مي شوند ، نمي توانيم FEC ها رامحدود كنيم كه كداميك برچسب مرتبط به خود داشته باشند وكداميك نداشته باشند. بنابراين اگر سوئيچينگ برچسب به يك FEC مشخص موردنظر نباشد (ممكن است زماني باشدكه درحالت مهاجرت به معماري MPLS است) ، شمانياز به مكانيزمي داريد كه بتواند اعلان عمومي نگاشت برچسبها رافيلتر كند ،به طوريكه يك همسايه LSR بالا رونده نتواند نگاشت برچسب براي يك FEC مشخص را دريافت كند. بدون اطلاعات اين نگاشت برچسب، LSR بالا رونده نمي تواند به يك FEC مقصد، برچسبي سوئيچ كند وبنابراين بايد بسته ها رابراساس اطلاعات جدول مسير دهي ، مسيريابي كند. كه شكل ۱-۵ اين تكنيك راتشريح مي كند.

شكل ۱-۵ كنترل پخش برچسب بين LSR هاي مجاور
زيرساخت SUPERCOM



شمادرشكل ۱-۵ مي بينيد كه LSR واشينگتن براي محدود كردن اعلان عمومي نگاشت برچسب به LSR سن خوزه و نه پاريس پيش بيني شده است اين پيكر بندي بوسيله بكارگيري دستور عمومي tag-switching advertise-tags حاصل شده است .جدول ۱-۵ گردد اين دستور رانشان ميدهد.

جدول ۱-۵. tag-switching advertise-tags Command Syntax

هدف	دستور
فیلتر کردن نگاشت برچسب به Peerهای TDP/LDP براساس پسوندهای مقصد که دریک لیست دسترسی استاندارد مشخص شده اند.	**tag-switching advertise-tag** [**for** *ccess-list-for- definition prefixes*] [**to** *access-list-for-TDP/LDP-peers*]

جدول ۱-۵ نشان میدهد که دوآرگومان **tag-switching advertise-tags** دردستور وجوددارد. آرگومان for ، ليست دسترسي رابكار مي بندد كه پسوندهاي IP مقصد چه مجاز وچه غيرمجاز رامشخص مي كند. آرگومان to ازليست دسترسي كه مشخص مي نمايد به كدام همسايه هاي TDP/LDP بايد آرگومان for قبلي اعمال شود، استفاده مي كند. ليست دسترسي مشخص شده درآرگومان to بايدبامشخصه TDP/LDP همسايه مطابقت داشته باشد اين مشخصه مي تواند بادستور show tag-switching tdpneighborنمايش داده شود. همانگونه كه درمثال ۱-۵ نشان داده شده است كه درآن مشخصه TDP همسايه در نماي چاپ highlight شده است.

توجه:

بسيارمهم است كه مطمئن شويم آدرسهاي ثابت براي مشخصه TDP/LDP استفاده شده اند. بنابراين ،مطمئن شويد كه يك آدرس loopback براي استفاده بعنوان مشخصه دردسترس ميباشد. اگر چندين loopback استفاده شده ، ازدستور tag-switching tdp router-id براي اينكه مشخص كنيد كدام آدرس loopback بعنوان مشخصه TDP/LDP بكار رود، استفاده نمائيد .

درمثال ۲-۵ مي توانيد لزوم پيكر بندي براي LSR واشينگتن را ببينيد .

مثال ۱-۵ دستور *tag-switching tdp neighbor*

```
washington# show tag-switching tdp neighbor

Peer TDP Ident: 194.22.15.2:0; Local TDP Ident 194.22.15.3:0
        TCP connection: 194.22.15.2.12226 – 194.22.15.3.711
        State: Oper; PIEs sent/rcvd: 122/117; ; Downstream
        Up time: 01:37:24
        TDP discovery sources:
            ATM0/0/0.1
       Addresses bound to peer TDP Ident:
          10.1.1.13         194.22.15.2
```

مثال ۲-۵ ، مثال پيكربندي tag-switching advertise-tags

```
hostname Washington
!
tag-switching advertise-tags for 1 to 2
tag-switching tdp router-id Loopback0
!
interface Loopback0
ip address 194.22.15.3 255.255.255.255
!
interface ATM0/0/0
no ip address
no atm ilmi-keepalive
!
interface ATM0/0/0.1 point-to-point
description ** interface to San Jose **
ip address 10.1.1.14 255.255.255.252
atm pvc 1 20 20 aal5snap
tag-switching ip
!
interface Ethernet0/1/0
description ** interface to Paris **
ip address 10.2.1.22 255.255.255.252
tag-switching ip
!
interface POS2/0/0
description ** interface to New York **
ip address 10.1.1.21 255.255.255.252
tag-switching ip
!
access-list 1 permit 194.22.15.0 0.0.0.255
access-list 1 deny any
access-list 2 deny 195.22.15.1
```

دستور **tag-switching advertise-tags** مي تواند فقط وقتي كه MPS درحالت Frame - mode درحال كاراست،استفاده شود. اين بدان معناست كه اگرلينك بين دو LSRازطريق يك اينترفيس LC- ATM برقرار باشد، آن گاه فيلتر كردن نگاشت برچسب ممكن نيست.

توجه:

خوب است بدانيدكه مي شود درپيكربندي روتر واشينگتن يك اينترفيس ATM بكاربرد وبه روترسن خوزه متصل كرد. بهرحال اين اينتر فيس يك اينتر فيس LC- ATM نيست، بنابراين يك فروم ATM سنتي PVC دراينترفيس بين دو روتر پيكربندي شده است. دراينحالت، روتر براي آن اينترفيس مشخص بصورت فريم مد كار مي كند.اگرچه اين ، يك اينترفيس ATM است وبنابراين دستور **tag-switching advertise-tags** عمل مي كند.

دليل اين محدوديت اين است كه روتر درزمان كاردر اينترفيس LC-ATM مدكنترلي LSP سفارشي وانتشار پائين رونده براساس تقاضاي برچسب رابكار مي گيرد. هنگام بكارگيري

اين مدعملكرد، منابع اينترفيس بعنوان برچسب بكار مي روند. درمورد ATM اينها جفتهاي VPI/VCI هستند وبعنوان مدارهاي مصنوعي برچسب (LVCs) شناخته شده اند.فصل ۳ ، "عملكرد MPLS درCell-mode"، درمورد LVC ها بحث مي كند. اين ترتيب براي آن است كه اگراعلان عمومي نگاشت برچسب فيلتر شده، آنگاه كل ترافيك درلينك به مدار مجازي كنترل (VPI 0 VCI 32) فرستاده مي شود. اين بخاطر آن است كه پسوند مقصد در LFLB بصورت untagged نشان داده شده وكل ترافيك به طرف آن پسوند مسيريابي مي شود. ازآنجا كه پرش بعدي براي پسوند مقصدبسته به طرف همسايه پائين دستي كه ازطريق مدارمجازي كنترل دردسترس است،اشاره خواهدكرد، كل ترافيك اين مسير رادنبال مي كند. اين يك عملكرد رضايت بخش نيست، چراكه مدارمجازي براي كنترل پيغام رساني وترافيك پروتكل مسيريابي بكارميرود. وبراي حمل ترافيك IP مناسب نيست.

فشرده سازی MPLS درلینک اترنت

يكي از موضوعات پيرامون بكارگيري فشرده سازي MPLSپياده سازي لينكهاي اترنت (اترنت ، اترنت سريع يا گيگابيت اترنت) درتوپولوژيي كه فشرده سازي اترنت راپشتيباني مي كند :اترنت ،802.3 (بايابدون يك هدر(header) 802.2) يا SNAP، ميباشد.هرنوع واسطه اي حداكثر اندازه فريمي معادل با ۱۵۱۸ اكتت (به جز Preamble يا SFD) واندازه طول داده اي (payload) كه از ۴۶ اكتت تا۱۵۰۰ اكتت (۱۴۹۲ درحالت فشرده سازي SNAP) دارد.

فصل پيشين تشريح مي كرد كه استفاده از MPLS دريك شبكه باعث افزايش اندازه بسته ها مي شود ،كه اين مربوط به افزودن برچسب هايي به پشته برچسب ميباشد.طول هر هدربرچسب ENTRY، ۴ اكتت است. اين يعني اگريك بسته با طول داده، ۱۵۰۰ اكتتي دريافت شود ويك هدر برچسب به پشته اضافه شود،آنگاه فريم بايد بايك طول داده طول ۱۵۰۴ اكتتي ارسال شود. بخاطر محدوديت حداكثر اندازه فريم درانواع مختلف واسطه هاي اترنتي ،اين باعث اشكال مي شود. زيرا MTU دراين لينكها كوچكتراز اندازه بسته نشان داده شده است.

توجه:

درحال حاضر استاندارد گيگابيت اترنت اندازه فريم رابه ۱۵۱۸ اكتت محدودمي كند،اگرچه اكنون بعضيVendorها، فريمهاي خيلي بزرگ راپشتيباني مي كنند كه درآنها فيلد ديتاتا ۴۴۷۰ يا۹۰۰۰ اكتت مي تواند گسترش يابد. افزايش طول فيلددیتا درفريم اترنت منجربه اين مي شود كه نتوانيم كاملاً تشخيص دهيم كه آيايك بسته مشخص يك بسته 802.3 است يابسته فشرده شده اترنت نوعΠ . اين به اين دليل است كه نوع / طول فيلد اگركمتراز۱۵۳۵ اكتت (وبنابراين ، يك فريم 802.3 و 802.3 به اضافه 802.2 يا SNAP) باشد،بعنوان طول واگربيشتر از ۱۵۳۵ اكتت (ودرنتيجه فشرده سازي اترنت Π) باشد، بعنوان نوع، تفسير مي شود.نتيجه اين است كه فريمهاي بزرگ درواسطه(media) ازنوع اترنت، فقط بافشرده سازي اترنت Π بهتركار مي كند. مطالعات بيشتردرحال انجام است تامشخص كند كه چگونه فشرده سازيهايي غيراز اترنت Π دراترنت گيگابيت بكارگيريم .اگرچه تازمان نوشتن اين كتاب هنوز نتايج محكمي بدست نيامده است.

كشف MTU **مسير** IP

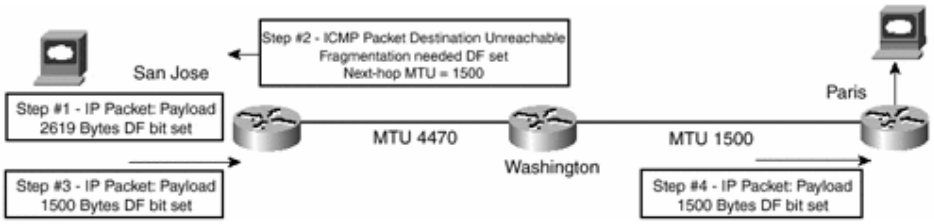
امـروزه بيـشترميزبانهاي IP اسـتفاده از مكـانيزم كـشف MTU مـسير رامطـابق بـا RFC 1191 "كشف MTU مسير"،پشتيباني مي كنند.مكانيزم توصيف شده در RFC به يك ميزبان IP اجازه ميدهد،حداكثر MTU مجاز درطول مسير ازمقصد تامبدأ رابصورت دنياميك كشف كند.
ايده اصلي درپشت كشف MTU مسير ،اين است كه ميزبـان مبـدأ درابتـدافرض مـي كنـد كـه MTU مسيردريك اتصال مشخص برابربا اولين پرش است وتمام ديتا گرامها درآن مـسيررابابيت DFست شده (قطعه قطعه نكنdont fragment) مي فرستد . هيچ ديتا گرام فرسـتاده شـده اي بزرگتراز MTU اولين پرش نخواهدبود. ميزبانهايي كه از اين پروسه استفاده نمي كنند،نبايد ديتاگرامهايي بزرگتر از ۵۷۶ اكتت بفرستند.

توجه:

درمورد پروتكل كنترل انتقال (TCP) ،وقتي يك جلـسه بايـك وسـيله راه دور برقـرار مـي شـود، حداكثرسايـــزoption بخش (segment) پرسش مـي شـود. دودسـتگاه درگيـر دربرقـراري ايـن جلسه مقدار حداكثر سايزقطعه (MSS) ICP خودرا مبادله مي كنند كه به طـور نرمـال بامقـدار MTU محلي، منهاي ۴۰ اكتت (هدر TCP وهدر IP) تعيين مي شـود. مقـدار MTU كـوچكتر در پروسه كشف بعنوان MTU مسير بكار ميرود.

وقتي يك روتر بسته اي رادريافت مي كند كه بزرگتر از MTU اينترفيس خروجي به طرف مقصد بـسته ورودي بـوده وبيـت DF دربـسته سـت شـده باشـد، يـك پيغـام "ICMP مقـصد غيرقابـل دسترس است"،باكد ۴(قطعه سازي(fragmentation)لازم بوده و DF ست شده است) ، به سمت مبداء بسته پس مي فرستد .
پروسه كشف MTU مسير به نتيجه اين پيغام بـراي تعيـين حـداكثر انـدازه بـسته اي كـه مـي تواند درمسير به سوي يك مقصد مشخص فرستاده شود،بستگي دارد.شكل ۲-۵ ايـن فرآينـد راتشريح مي كند.

شكل ۲-۵ مكانيزم كشف MTU مسير



وقتي شمااين فرآيند رااجرا كنيد، بسته ها مي تواننـد بـه طورموفقيـت آميـزدر سـتون فقـرات MPLS (Backbone) بدون قطعه قطعه شدن ارسال شوند. بهرحال هـر LSR مـي توانـد بـسته هاي برچسب گذاري شده يانشده را اگربزرگتر از MTU خروجـي بـوده وبيـت DF درآنهـا سـت نشده باشد، قطعه قطعه كند.

اگربيت DF ست شده باشد LSR بافرستادن يك پيغام ICMP "مقصد غيرقابل دسترس "باكد" قطعه سازي لازم بوده و DF ست شده است"، بامكانيزم كشف MTU مسير تطبيق مي يابد. تمام اين كارها درست خواهدبود،اگر هرمكانيزم بامكانيزمهاي توصيف شده قبلي،تطبيق داشته باشد. بهرحال، واقعيت اين است كه بعضي ميزبانهااز مكانيزم كشف MTU مسير استفاده نكرده وديتاگرامهايي كه بزرگتر از ۵۷۶ اكتت را مي فرستند. علاوه براين بعضي ديوارهاي آتش پيغام هاي ICMP "غيرقابل دسترس "كه بطور موثري مكانيزم كشف MTU رامي شكند، مي فرستند. بخاطراين مسئله جهت اطمينان ازارسال موفقيت آميز بسته ها درشبكه درمحيط MPLS ،به مكانيزم بهتري كه به فريمهاي با طول داده بزرگتر از ۱۵۰۰ اكتت اجازه عبور مي دهد، نيازميباشد.

توجه:

بعضي از مطالب مربوط به كشف MTU باجزئيات بيشتر در draft-ietf-tcpimpl-pmtud بحث شده اند. شمامي توانيد اين متن رادر وب سايت IETF بيابيد: http://www.ietf.org/ids.by.wg/tcpimpl.html

سيستمهاي سيسكو دراين مورد راهكارهايي رامعرفي كرده اند كه به پورت اترنت دريك روتر اجازه پشتيباني از بسته هاي MPLSبا طول داده بزرگتر از۱۵۰۰ اكتت رامي دهد.اين باافزايش MTU پورت اترنت به ۱۵۲۶ اكتت كه از ماكزيمم اندازه استاندارد فريم اترنت كه ۱۵۱۸ اكتت است به اضافه ۸ اكتت براي دوسطح ازبرچسبهاي MPLS تشكيل مي شود ،قابل حصول است.درحال حاضر اين تعداد برچسب كافي است و ازعملكرد MPLS و VPN هاي فعال شده با MPLS پشتيباني مي كند ، امايك عمق دلخواه ازپشته برچسب راپشتيباني نمي كند. مطالعه بيشتر درحال انجام است وعمق پشته برچسب ممكن است درآينده افزايش يافته وامكان ارائه سرويسهايي كه نياز به عمق پشته برچسب بزرگتر ازدو دارند ، ايجادشود. اين راهكار به بسته هايي كه بابيت DF ست شده ، دريافت شده اند ، بستگي دارد.در draft-ietf-tcpimpl-pmtud اين افزايش اندازه طول داده طول بعنوان" ماكزيمم اندازه واقعي طول داده فريم" شناخته شده است.

مقاله قبلي بيان مي كند، براي بسته هايي كه DF آنهاست نشده است، كه هر LSR بايد پارامترهاي پيكربندي را پشتيباني كندكه بعنوان "اندازه ماكزيمم ديتاگرام IP برچسب گذاري شده "،شناخته شده است.
(بخش ۳,۲ از draft-ietf-mpls-label-encaps رابببينيد) اين پارامتر براي ورود به حوزه MPLS (domain) بكارميرود، به طوري كه اگربسته بزرگتر ازماكزيمم اندازه MTU برچسب گذاري وپيكربندي شده باشد، مي تواند درلبه (edge) شبكه قطعه قطعه شود. اين بدان معناست كه اندازه MTU بايدبراي تمام لينكهاي ستون فقرات ثابت شود، به طوري كه بشوددرمورد اين مقدار تصميم گيري كرد. فايده اين آن است كه بسته قبل از ورودبه حوزه MPLS، قطعه قطعه مي شود ونيازي به قطعه قطعه شدن بيشتر درستون فقرات MPLS ندارد.

درسيستمهاي MPLS سيسكو اين پارامتر بااستفاده از دستور tag-switching mtu دراينترفيس خروجي پيكربندي مي شود اين دستور اندازه MTU اينترفيس رابطور پيش فرض تنظيم مي كند .اگربسته هايي دريافت شوند كه خيلي بزرگ باشند، همانگونه كه دردستور tag-switching mtu مشخص شده، بايدبدون قطعه قطعه شدن به جايي درشبكه MPLS ارسال شوند وبيت DF شان ست نمي شود. آنگاه قبل ازارسال به خارج از اينترفيس، قطعه قطعه مي شوند. فايده اين كار آن است كه قطعه قطعه كردن نبايد درحوزه MPLS اتفاق بيفتد وبه لبه شبكه محدود مي شود.

توجه:

علاوه بر اين ،دستور tag-switching mtu درارتباط باافزايش حداكثر اندازه MTU اترنت ("حداكثر اندازه واقعي طول داده فريم ") ضروري ميباشد. اگراين دستوررا ست نكنيد، هربسته ورودي كه اندازه طول داده بزرگتر ازاندازه حداكثرفريم پيش فرض براي اينترفيس خروجي (مثلاً درمورد اترنت Π ، اين اندازه وقتي برچسبهاي MPLS به پشته وارد مي شوند ۱۵۰۰ اكتت است)دارد ،دور انداخته شده ويك پيغام ICMP به مقصد فرستاده مي شود. اين امر حتي اگر اينترفيس بتواند اين اندازه هاي بزرگ فريمها را پشتيباني كند، اتفاق مي افتد به اين خاطر اين فرمان رادرتمام اينترفيسهاي اترنت كه براي حمل بسته هاي فشرده شده MPLS پيكربندي شده اند، فعال كنيد.

توجه:

اينترفيستهاي اترنت تنها اينتر فيسهايي نيستند كه درآنها MTU كوچكتر ازاندازه فريم منتج بعداز افزودن برچسبهاي MPLS ميباشد .اين بدان معناست كه فرمان tag-switching mtu فقط به اينترفيسهاي اترنت محدود نمي شود وبايد براي هر اينترفيسي كه احتمال افزايش حداكثر MTU تنظيم شده براي آن وجوددارد، پيكربندي شود.

سوئيچهای اترنت و MPLS MTU

همانگونه كه دربخش قبلي بحث شد، MTU مربوط به بسته هاي IP به اندازه هربرچسب MPLS كه به آن اضافه مي شود، ۴ اكتت افزايش مي يابد. درمورد استفاده از هرامكاني از MPLS (MPLS پايه، VPN يامهندسي ترافيك) اندازه يك بسته MPLS مي تواند ازحداكثر اندازه فريم اترنت كه ۱۵۱۸ اكتت است، تجاوز كند. بخش قبلي نشان داد كه اين مشكل تاحدودي باتغييردر LSR وتوانا كردن آن درارسال فرمهايي بزرگتر از۱۵۱۸ اكتت حل شده است.

اين راهكار خوب است اگر LSR ها ازطريق كابلكشي اترنتي بصورت پشت به پشت (back to back) بهم متصل شده باشند. بهرحال اگرشما ازيك سوئيچ لايه ۲ براي ساختن يك بخش (segment) اترنتي استفاده كنيد، آنگاه اين وسيله هم بايدقادر به ارسال فريمهايي كه بزرگتر از۱۵۱۸ هستند، باشد. دربيشترموارد ونه درهمه موارد اين عملاً واقعي نيست وسوئيچ فريم رادور انداخته ويك GIANT (فريم غول پيكر) گزارش مي كند.

توجه:

بعضي سوئيچهاي لايه ۲ سيسكو بطورپيش فرض ،ازفريمهاي خيلي بزرگ giant پشتيباني مي كنند وبعضي نمي كنند .اگر پشتيباني نكنند، راهكارهايي وجوددارد كه سوئيچها راقادر به عبور فريمها بكند. شمامي توانيداين راهكارهاراز سيستمهاي سيسكو. TAC,INC (مركز پشتيبان فني) تقاضا ودريافت كنيد.

چگونگی کشف وجلوگیری از لوپ در MPLS

يك موضوع مهم هنگام اجراي معماري MPLS، توجه به توانايي آن درکشف وجلوگيري ازارسال لوپ به داخل توپولوژي ميباشد. يك لوپ ارسالي دريك شبكه IPفرايندي است كه باآن يك روتر، بسته رادر يك مسيراشتباه (تاآنجا كه همسايه هايش مورد توجه قرار مي گيرند) ، به يك مقصد مشخص برپايه اطلاعات موجوددر جدول مسيريابي اش، پس مي فرستد.اين مي تواند درزمان گذر همگرا، هنگامي كه پروتكلهاي مسيريابي ديناميك بكار مي روند ،اتفاق بيافتد يادراثر پيكربندي اشتباه، كه باعث مي شود روتر به روتر ديگري كه عملاً پرش بعدي صحيحي براي يك مقصد مشخص نميباشد، اشاره كند.

درموردمعماري MPLS بايد هم به واحد كنترل(control plane) وهم به واحد ديتا(data plane) واينكه جلوگيري ازلوپ درستون فقرات فريم مد وسلول مدچگونه انجام مي شود، توجه كنيد. شماهم چنين بايد بدانيد كه هر كدام چگونه لوپهاي ارسالي راتشخيص داده وباآنها چه رفتاري مي كنند .

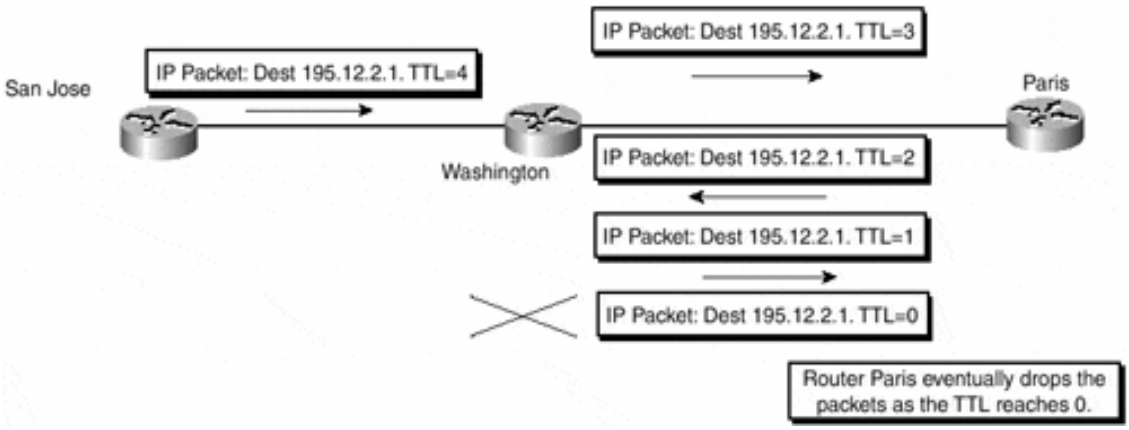
تشخیص لوپ وجلوگیری از آن در MPLS Frame–mode

هنگاميكه كه درفصل ۲ نشان داده شد ،برچسبها درزمان فعال بودن پياده سازي MPLS frame-mode بابكارگيري مدكنترلي مستقل به FEC هاي مشخصي الصاق مي شوند. وقتي شمااز اين مداستفاده مي كنيد،برچسبها براساس اينكه FEC در جدول مسيريابي LSR وجوددارد، به FEC هاالصاق مي شوند. بابكارگيري اين روش الصاق FEC ، مي توانيدLSPاها رادرشبكه MPLS ايجادكنيد. شماباعلم به اين موضوع مي توانيد بفهميد كه چگونه هر LSR مي تواند لوپهاي ارسالي راشناسايي وازآنها جلوگيري نمايد.

Frame–mode: تشخیص لوپ واحد دیتا

دريك شبكه استاندارد مسيريابي شده IP لوپهاي ارسالي باامتحان فيلد TTL بسته IP ورودي، شناسايي مي شوند. بااستفاده ازاين فيلد، هرروتر درمسير بسته مقدار آن را واحد ۱ كاهش مي دهد. اگرفيلد به ۰ برسد بسته دورانداخته شده ولوپ ارسالي شكسته مي شود. شكل ۳-۵ اين مكانيزم راتشريح مي كند.

شكل ۳-۵ كشف لوپ بااستفاده ازTTL دريك شبكهIP



همانگونه كه شكل ۳-۵ نشان ميدهد، يك لوپ بين روترهاي واشينگتن وپاريس ايجاد شده است .ازآنجا كه هرروتر مقدارفيلد TTL را ۱ واحد كاهش مي دهد، عاقبت لوپ كشف شده وبسته لوپ دورانداخته مي شود (دراين مثال توسط روتر پاريس). مكانيزم مشابهي در واحد ديتا درپيياده سازي MPLS درframe-mode بكار مي رود.
هر LSR دريك LSP مشخص، هرزمان كه يك فريم MPLS ورودي راارسال مي كند، فيلد TTL مربوط به هدر MPLS راكاهش داده و هربسته اي كه TTL آن به 0 برسد رادور مي اندازد.

توجه:

اين مطلب براي هر اينتر فيس ATM نيزكه MPLS رامستقيماً باهرسوئيچ ATM فعال نمي كند ،صحيح ميباشد .اين به خاطر آن است كه يك PVC دراين اينترفيس بعنوان پرش بعدي قلمداد مي شود، اگرچه ممكن است ازيكسري سوئيچهاي ATM عبوركند.

Frame–mode: جلوگيري ازلوپ درواحد كنترل

واضح است كه كشف لوپهاي ارسالي، يك عمل بسيار ضروري ميباشد. البته اين نيزلازم است ، كه LSR قادربه جلوگيري ازاين لوپهاي ارسالي ،قبل از اينكه اتفاق بيفتند،باشد. اين فعاليت جلوگيري، بايددر واحد كنترل يعني جايي كه LSP ها ايجاد مي شوند، حاصل شود.
دريك شبكه استاندارد مسيريابي شده IP ،جلوگيري ازلوپهاي ارسالي وظيفه پروتكل مسيريابي داخلي است زيراهر LSR در پياده سازي MPLS در frame-mode مشابه اين پروتكل هاي مسيريابي رابراي تكميل جدول مسيريابي اش بكار مي برد . اطلاعاتي كه براي تشكيل LSP هادرشبكه بكارميرود، شبيه اطلاعات شبكه استاندارد مسيريابي شده IP ميباشد. به اين دليل پياده سازي MPLS در frame-mode براي اطمينان حاصل كردن ازاينكه اطلاعات موجوددرجدول مسيريابي LSR، بدون لوپ هستند، به پروتكلهاي مسيريابي تكيه مي كند . اين دقيقاً كاري است كه يك شبكه استاندارد مسيريابي شده IP انجام مي دهد.

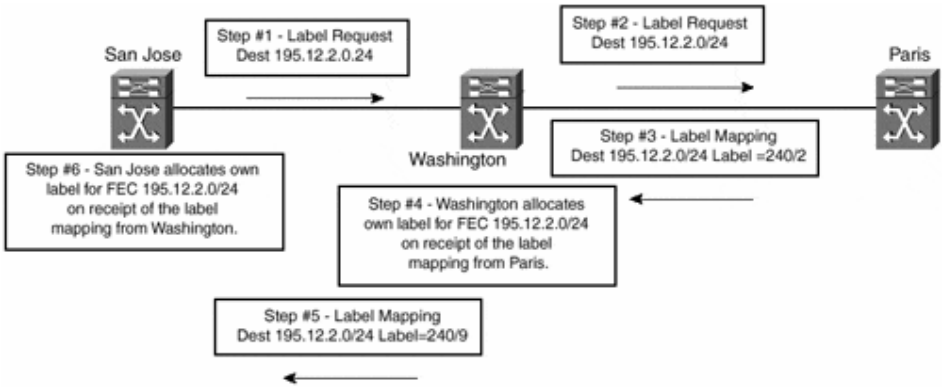
کشف لوپ وجلوگیری از آن در MPLS در Cell–mode

وقتي كه شما MPLS رادرسوئيچها وورترهاي ATM كه اينتر فيسهاي LC-ATM رابكار مي بندند، اجرا مي كنيد، مكانيزم بكاررفته دركشف وجلوگيري ازلوپ در پياده سازي frame-mode براي اين نوع محيط كافي نخواهدبود. اين بخاطر آن است كه در هدريك سلول ATM ،مفهوم TTL وجودندارد وروش ديگري براي تخصيص وانتشار برچسبها بكارميرود. بنابراين مكانيزمهاي جديد مختص به محيط ATM ،براي اجراي موفقيت آميز MPLS دراين نوع شبكه ها نيازميباشد.
براي اينكه ببينيد كشف وجلوگيري ازلوپ چگونه در يك محيط ATM انجام مي شود، به هردوواحد ديتا وكنترل MPLS توجه كنيد، تابدانيد چگونه ازحالت بكارگيري frame-mode متمايز مي شوند.

Cell–mode: كشف / جلوگيري ازلوپ درواحد كنترل

همانگونه كه درفصل ۲ عملكرد MPLS در frame-mode بحث شد ،هنگاميكه MPLS دراينترفيسهاي LC-ATM وسوئيچهاي ATM پياده ميشود، واحدكنترلي به طور پيش فرض پروسه انتشار پائين رونده براساس تقاضاي برچسبها رابصورت تخصيص سفارشي برچسب بكارمي گيرد.اين، يعني تخصيص وانتشار برچسبها براساس تقاضا وبراساس حضور يك FEC مشخص درجدول آدرس دهي ATM-LSR صورت ميگيرد. كه اين خود بدان معناست كه يك ATM-LSR مي تواند به هر FEC، مستقل ازاينكه قبلاً ازهمسايه پائين دستي ATM-LSR نگاشت برچسبي دريافت كرده يانه، برچسبي اختصاص دهد. درهر حالت، اگردرخواست شود، يك پيغام تقاضاي برچسب به همسايه پائين دستي ، براي يك FEC مشخص فرستاده مي شود، تانگاشت برچسب آن FEC ارسال شود. يك تفاوت عمده بين دو روش وجوددارد : هنگاميكه شمامدكنترلي مستقل رابكار مي گيرد، ATM-LSR فوراً نگاشت برچسب رابه منبع پيغام تقاضا برمي گرداند. اما هنگامي كه مدكنترلي سفارشي رابكار مي بريد، ATM-LSR قبل از تخصيص وارسال نگاشت برچسب خودش به مبداپيغام تقاضاي برچسب، منتظر رسيدن نگاشت برچسب از همسايه پائين دستي اش مي شود.
نتيجه هر دواين روشها اين است كه اگر چه ATM-LSR هنوزبه پروتكل مسيريابي داخلي براي تكميل جدول مسيريابي اش بستگي دارد، علاوه براين به تكميل موفقيت آميز مكانيزم سيگنالينگ نيز وابسته است، تابتواند يك LSP براي يك FEC معين ايجادكند. براي فهم اينكه چرا اين نتيجه حاصل مي شود وچرا واحد كنترلي MPLS درcell-modeگسترش يافته، چگونگي تخصيص وانتشاربرچسب(براي سهولت كنترل سفارشي رابكار ببريد) درمثالهاي نشان داده شده درشكل ۴-۵ رامرور كنيد .

شكل ۴-۵ مدكنترلي سفارشي وپائين رونده براساس تقاضا



همانگونه كه درشكل ۴-۵ مي بينيد، وقتي كه ATM-LSR درسن خوزه مي خواهد يك LSP براي FEC 195.12.2.Q/24 راه اندازي كند ،جدول مسيريابي محلي اش رابراي يافتن پرش بعدي براي FEC كنترل مي كند. بعدازاينكه اين پرش بعدي (باامتحان اطلاعات همسايگي LDP/TDP)رامشخص كرد، مي تواند بفهمد كه كدام همسايه LDP/TDP اين پرش بعدي رابعنوان اينترفيس مستقيماً متصل خوددارد .آنگاه ATM-LSR لبه در سن خوزه يك پيغام تقاضاي برچسب به همسايه پائين دستي پرش بعدي خود مي فرستد. كه در مثال ATM-LSR واشينگتن ميباشد. اين پيغام تقاضاي برچسب، گام به گام درشبكه MPLS سفر مي كند وناگهان به ورودي ATM- LSR براي FEC195.12.2.0/24، كه در مثالATM- LSR پاريس است، ميرسد.

ATM- LSR پاريس يك پيغام نگاشت برچسب بالاروندە ،درجواب پيغام تقاضاي برچسب مي فرستدكه تازمان رسيدن به ورودي ATM-LSR بصورت آبشاري در LSP به عقب برميگردد.وقتي كه اين فرآيند كامل شد، LSR براي عبورترافيك آماده است .اين روش خوب كارمي كند، فقط مشكل اين است كه هم تقاضاي برچسب وهم پيغامهاي نگاشت برچسب مي توانند به واسطه اطلاعات غلط مسريابي به طورپيوسته بين ATM-LSR ها هدايت شوند. اين شرايط مشابه شرايط مثال TTL قبلي است ويك لوپ ارسالي از اطلاعات كنترلي ايجادمي كند مطمئناً اين حالت مطلوب نميباشد زيرامكانيزمهاي اضافي درواحد كنترل براي جلوگيري ازاين اتفاق لازم ميباشد.

توجه:

احتمال وقوع يك لوپ ارسالي ازاطلاعات كنترلي فقط هنگامي كه شما يك ATM-LSR غيرقابل ادغام را پياده سازي مي كنيد، آشكار است. زيرايك ATM- LSR وقتي كه بايدحداقل دوLSR رادريك FEC ادغام كند، تبديل به يك ATM- LSR ادغام مي شود وبراي پشتيباني از ادغام VC پيكربندي مي شود. بنابراين هنگامي كه اولين تقاضاي برچسب براي يك FEC معين دريافت ميگردد، فقط يكي ازشرايط قبلي برآورد مي شود وپروسه هاي ATM-LSR غيرقابل ادغام بكارمي رود.اگرتمام شرايط برآورده شود ديگربدون توجه به اينكه براي تقاضاي اوليه برچسب، نگاشت برچسبي دريافت شده، پيغام تقاضاي برچسبي ارسال نخواهدشد.

اين مكانيزم درمورد استفاده از شمارش پرش TLV كه شامل شمارش تعداد ATM-LSR ها يكي كه تقاضاي برچسب ياپيغام نگاشت برچسب ازآنها عبور ميكند، ميباشد.هنگامي كه يك ATM-LSR ،يك پيغام تقاضاي برچسب دريافت مي كند ،اگر ATM- LSR ورودي براي FEC پيغام نباشد، يابرچسبي براي FEC نداشته باشد،پيغام تقاضاي برچسب خودش را ايجادكرده وآن را به ATM- LSR پرش بعدي مي فرستد اين پرش بعدي ATM-LSR، دوباره باآناليز جدول مسيريابي تعيين مي شود.

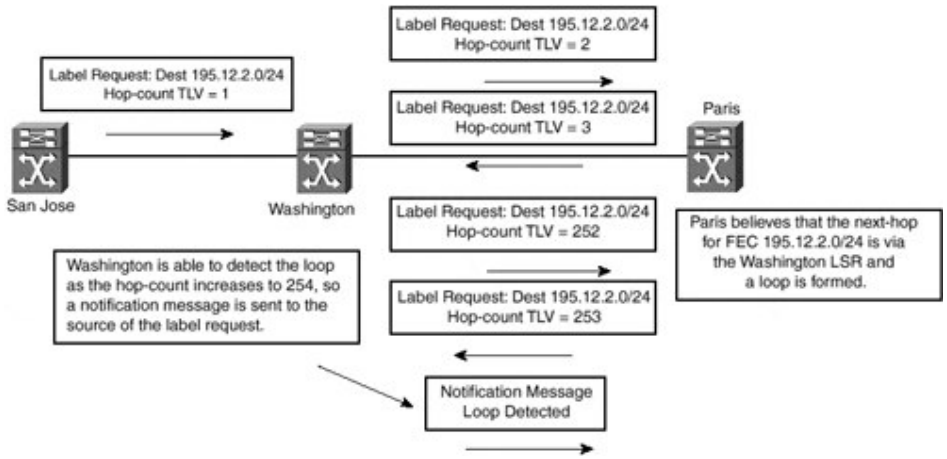
توجه :

در پياده سازي فعلي TDP، سيسكو يك شي شمارنده پرش رابعنوان بخشي از تقاضاي برچسب TDP وپيغامهاي نگاشت برچسب بكارمي برد. اين مكانيزم شبيه TLV شمارنده پرش LDP است كه دربخش ۲۰۸ " كشف لوپ " در draft-ietf-mpls-ldp توصيف شده وتوسط پياده سازي LDP سيسكو پشتيباني مي شود.

اگرپيغام اصلي تقاضاي برچسب شامل يك شي/ TLV شمارنده پرش باشد، ATM-LSR نيز يكي در پيغام تقاضاي برچسب خودش خواهدداشت، اماشمارنده پرش رايك واحد افزايش مي دهد. اين برعكس عملكرد ،TTL كه درآن TTL يك واحد كاهش مي يافت، ميباشد. اگرچه همان مفهوم تعدادحداكثر پرشها مورداستفاده قرارميگيرد.

وقتي يك ATM-LSR يك پيغام نگاشت برچسب دريافت مي كند، اگرآن پيغام شامل يك شي/ TLV شمارنده پرش باشد،اين شي/ TLV شمارنده پرش نيزيك واحد افزايش مي يابد. درحالي كه نگاشت برچسب محلي بالاروندە ارسال مي شود.وقتي يك ATM-LSR كشف مي كند كه تعـــداد پرش به يك مقدار حداكثر تنظيم شده (۲۵۴ در پياده سازي سيسكو) رسيده ، مي فهمد كه پيغام درلوپ افتاده است .آنگاه يك پيغام " اخطار كشف لوپ"، به منبع تقاضاي برچسب ياپيغام نگاشت برچسب مي فرستد.بااستفاده از اين مكانيزم يك لوپ ارسالي قابل تشخيص وبعداً قابل جلوگيري است .
شكل ۵-۵ اين فرآيند راتشريح مي كند.

شكل ۵-۵ فرآيند شمارش پرش شي/TLV



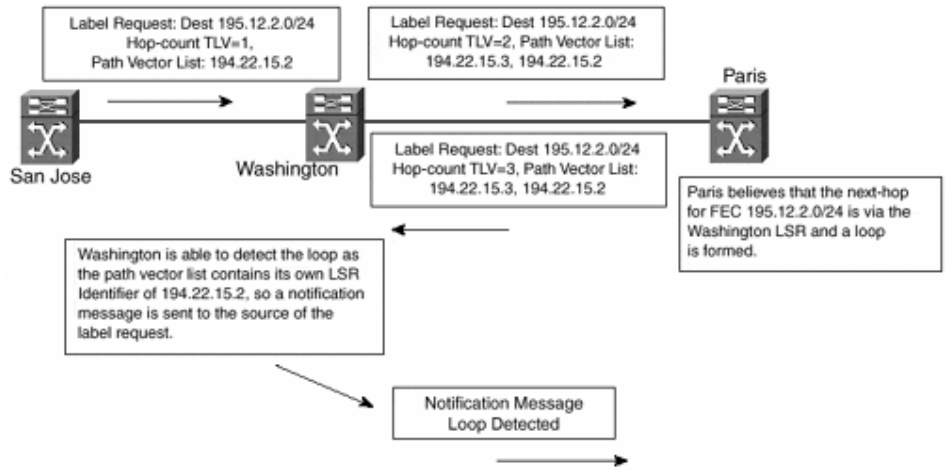
يك مشكل روش شمارش پرش درکشف لوپ اين است که زمان کشف لوپ بخاطر اينکه تعداد پرش تاتشخيص لوپ بايد به ۲۵۴ برسد، بسيارزياد مي شود.

توجه :

تعداد پرش در پياده سازي سيسکو بطور پيش فرض ۲۵۴ پرش است. اما شما مي توانيد آن رابافرمان tag-switching atm maxhopsتغيير دهيد. بااستفاده از اين فرمان شما مي توانيد حداکثر تعداد پرشها راکاهش دهيد. بنابراين مقدارزمان موردنياز تاکشف لوپ دراطلاعات کنترلي کاهش مي يابد .

به اين دليل draft-ietf-mpls-ldp يك مکانيزم بردارمسير که مورداستفاده ازبردار مسير TLV فراهم مي آورد که مي تواند لوپ مربوط به مسيري که پيغام ازآن عبور مي کند را کشف نمايد.اين شبيه به مفهوم روشي است که BGP-4 لوپها را دريك AS_PATH کشف مي کند، امادرمورد MPLS شاخص LSR بکارميرود. بااستفاده ازاين مکانيزم، هر ATM-LSR هرزمان که پيغامي بامحتواي بردار مسير TLV منتشر مي کند، شاخص LSR خودش را به ليست بردارمسير مي افزايد . اگرپيغا مي بامحتواي شاخص LSR خود LSR -ATM درليست بردارمسير دريافت گردد، لوپ کشف شده وپيغام اخطار کشف لوپ به مبداء پيغام پس فرستاده مي شود.شكل ۶-۵ اين فرآيند رانشان ميدهد.

شكل ۶-۵ مكانيزم جلوگيري ازلوپ بابردارمسير TLV

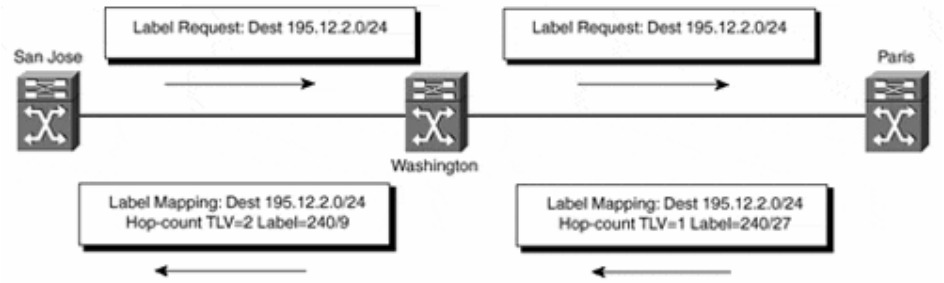


همانطوريكه شكل ۶-۵ نشان ميدهد، شاخص LSR مربوط به هر ATM-LSR باحركت درشبكه به پيغام تقاضاي برچسب افزوده مي شود. بخاطر اطلاعات غلط، ATM-LSR واشينگتن تصور مي كند كه پرش بعدي براي FEC195.12.2.0/24 ازطريق ATM-LSR پاريس ميباشد ،اما ATM-LSR پاريس فكرمي كند كه پرش بعدي براي FEC195.12.2.0/24 از طريق ATM- LSR واشينگتن است .اين باعث تشكيل يك لوپ مي شود. ATM- LSR واشينگتن مي تواند با ديدن شاخص LSR خودش درپيغام تقاضاي برچسب، لوپ راكشف كند.

Cell –mode **كشف لوپ درواحد ديتا**

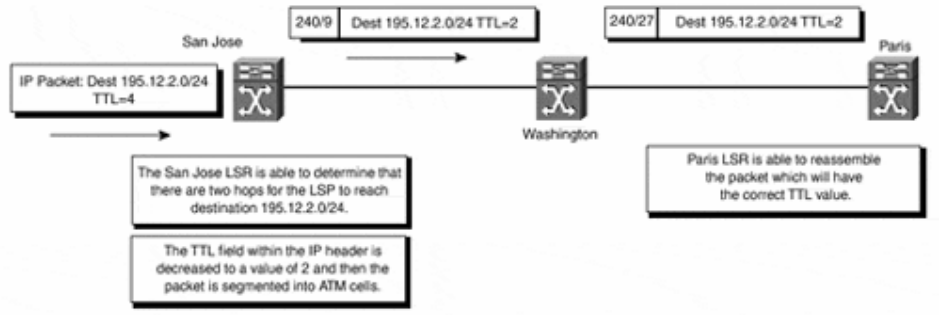
قبلاً آموختيد كه در هدريك سلول TTL,ATM وجود ندارد اين يعني مكانيزمي كه قبلاً جهت كشف لوپهاي ارسالي در MPLS فريم مد توصيف شد، درحالت cell-mode كاربردي ندارد.
دربخش قبلي ديديد كه بااستفاده ازيك شي/ TLV شمارنده پرش درپيغامهاي تقاضاي برچسب يانگاشت برچسب كه بين LSR ها ردوبدل مي شود مي توان از لوپهاي ارسالي درواحد كنترل جلوگيري كرد.نتيجه اين است كه هر ATM-LSR اطلاعات ضروري براي تشخيص تعداد پرشهاي لازم جهت رسيدن به نقطه ورودي ATM يك LSP رادارد واين اطلاعات مي تواند درواحد ديتاي پياده سازي cell-mode MPLS استفاده شود. شكل ۵-۷ انتشار اطلاعات شمارش پرشها بين ATM-LSR هارانشان مي دهد.

شكل ۵-۷ افزايش تعدادپرشها بين ATM- LSR ها



مثال شكل ۵-۷ نشان مي دهد كه ATM- LSR لبه در سن خوزه مي تواند تعيين كندكه يك بسته براي رسيدن به نقطه ورودي LSP براي FEC195.12.2.0/24 بايد دو پرش انجام دهد.
باداشتن اين اطلاعات، ATM-LSR لبه درسن خوزه مي تواند فيلد TTL يك بسته IP ورودي راقبل از تقسيم بسته به سلولهاي ATM پردازش كند.شكل ۵-۸ اين فرآيند رانشان مي دهد.

شكل ۵-۸ پردازش TTL بسته IP قبل ازفرآيندSAR



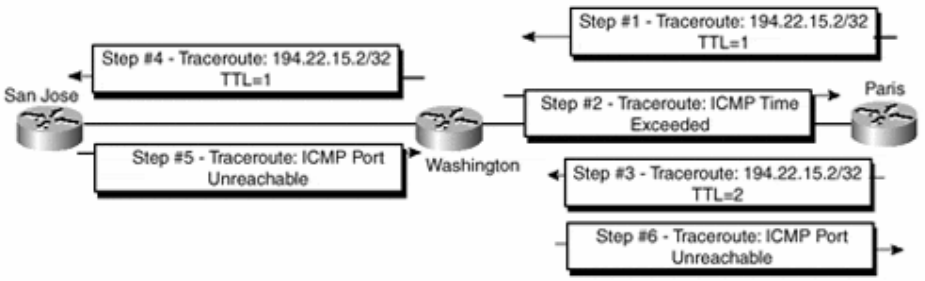
شكل ۵-۸ نشان ميدهد كه وقتي يك بسته IP به مقصد ميزباني درشبكه 195.12.2.0/24 به ATM-LSR لبه درسن خوزه ميرسد IP TTL درزمان تقسيم به سلولها (segmentation)به تعداد پرشهاي ضروري براي رسيدن به نقطه پاياني LSP كاهش مي يابد. وقتي ATM-LSR درپاريس بسته IP اصلي را بازسازي مي كند، فيلد TTL موجوددر هدر IP محتوي مقدارصحيح TTL كه نشانگر تعداد پرشهايي كه بسته ازآنها عبوركرده، ميباشد.

مشكل اين روش اين است كه به هر حال هنگام رديابي مسير دربخش ATM شبكه، خرق عادت مي شود .كاهش MPLS/IP TTL به اندازه ۱ واحد براي جلوگيري از لوپهاي ارسالي كافي است .در پياده سازي معماري MPLS توسط سيسكو ATM-LSR لبه، TTL راقبل از تقسيم فريم به سلولها بدون توجه به تعداد پرشها، ۱ واحد كاهش مي دهد. بااستفاده ازاين روش، شما مي توانيد درنواحي ازشبكه كه فريم ارسال مي كنند، شامل لبه ابر ATM به TTL اعتماد كرده و فرض نمائيد كه فرآيندهاي كنترل (همانگونه كه دربخش قبلي بحث شد) ، دربخش ATM شبكه از لوپها جلوگيري مي كنند.

رديابی مسير دريک شبکه MPLS

امكان رديابي مسيريك وسيله اشكال زدايي مفيداست كه به شما اجازده رديابي مسيري كه يك بسته ازمنبع IP تامقصد IP طي مي كند، را مي دهد اين وسيله به طور گسترده اي درجامعه IP استفاده مي شود وبنابراين اگرچه معماري MPLS رفتار ذاتي كار رديابي مسيررا تغيير نمي دهد، هدايت بسته هاي رديابي مسير راباكمي تفاوت بايك شبكه IP نرمال انجام ميدهد. دريك محيط IP نرمال ، پياده سازي رديابي مسير سيسكو، همانگونه كه درشكل ۵-۹ تشريح شده انجام مي شود.

شكل ۹-۵ عملكرد رديابي مسير دريك شبكه IP



همانگونه كه شكل ۹-۵ نشان مي دهد ،عملكرد رديابي مسير دريك شبكه IP به ترتيب زير مي تواند خلاصه شود. اين قدمها استفاده ازرديابي مسير راهم در شبكه IP وهم در شبكه MPLS ميسر ميسازند.

گام ۱ ، مبداء رديابي مسيريك بسته IP رابا TTL مساوي ۱ وپورت UDP مقصد مساوي ۳۳۴۳۴ به يك مقصد مشخص مي فرستد.

گام ۲ ، اولين روتر درمسير بسته يك پيغام ICMP "زمان ازحدمجاز تجاوز كرد (exceeded time)" ، به مبداء بسته پس مي فرستد. اين بخاطر آن است كه TTL بسته IP ، بعداز اينكه روتر آن را ۱ واحدكاهش داد، به صفر ميرسد.

گام ۳ ، مبداء دومين بسته را اين بار باTTL مساوي ۲ مي فرستد، اولين روتر دراولين گام بسته رامسيريابي مي كند. وقتي به روتر دوم درمسير ميرسد دوباره يك پيغام ICMP "زمان ازحدمجاز تجاوز كرد"، ارسال مي شود.(گام ۳ وگام ۴)

گام ۴ ، اين پروسه ادامه مي يابد (با افزايش ۱ واحدي TTL درهربار تكرار توسط مبداء) تااينكه به مقصد نهايي بسته يا حداكثر تعداد پرشها برسد (مقدار پيش فرض ۳۰ پرش است). روتر مقصدنهايي (ياميزبان) يك پيغام ICMP "پورت دردسترس نيست"، به مبداء پس مي فرستد بابكارگيري پيغامهاي جواب ICMP، مبداء مي تواند بگويد كه آيا جواب ازيك روتر عبوري است ياباز مقصدنهايي بسته. (گام ۵ وگام ۶)
مطمئناً اين پروسه دريك ستون فقرات IP نرمال، جايي كه تمام روترهاي عبوري ، اطلاعات روترهاي خارجي را حمل مي كنند كافي است بهرحال همانگونه كه درفصل ۲ بحث شد ، دريك شبكه MPLS مطلوب است كه اطلاعات روترهاي خارجي حمل نشود وفقط ترافيك سوئيچ براي BGP پرش بعدي اين مقصدهاي خارجي، برچسب بخورد .اين درمورد استفاده رديابي مسيرمشكلاتي راپيش مي آورد:

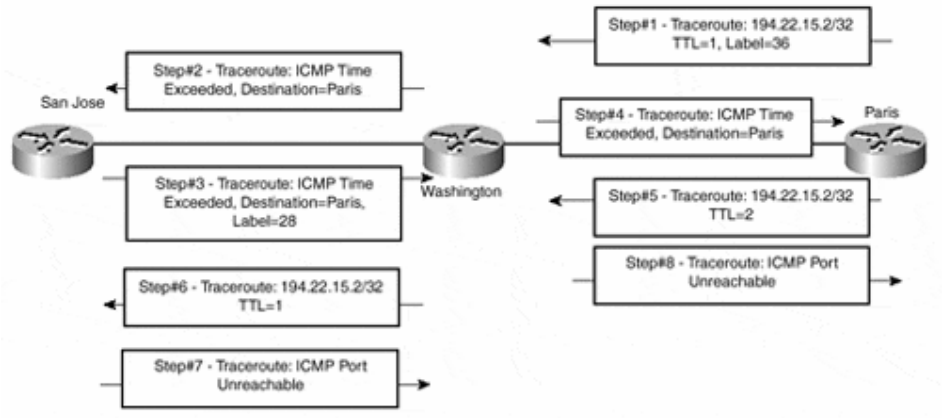
- رديابي مسيربه اين واقعيت كه آدرس مبداء بسته رديابي مسير توسط هرروتري كه نيازبه پاسخگويي به بسته بايك پيغام ICMP دارد قابل دستيابي است، بستگي دارد .
- افزايش TTL بايددرشبكه براي فعاليت رديابي مسير امكان پذير باشد.

توجه:

اين مطلب به طوركامل در draft-ietf-mpls-lable-encops بخش ۲,۳,۲ "تونل آدرسهاي خصوصي درستون فقرات عمومي" بحث شده است.

به خاطر اينكه آدرس مبداممكن است دردسترس نباشد (مثلاً در VPN ياوقتي كه هسته شبكه اطلاعات مسيريابي BGP را حمل نمي كند) ،درمحيط MPLS شما مي توانيد ،دوباره ازپشته برچسب بسته اصلي براي برچسب زني به پيغامهاي ICMP به سمت مبداء استفاده كنيد. اين يعني بسته ها مي توانند به مقصد اصلي فرستاده شوند كه بعداً ازآنجا مي توانند درشبكه MPLS به مبدا اصلي پس فرستاده مي شوند. درمثال نشان داده شده درشكل ۹-۵ ،اين رفتار باعث مي شود روتر واشينگتن پيغام ICMP "زمان ازحدمجاز تجاوز كرد" (گام ۲ درشكل ۹-۵) ، رابه روتر سن خوزه بفرستد كه آن هم بسته را به روتر واشينگتن باپشته برچسبي براي رسيدن به روتر پاريس پس مي فرستد. شكل ۱۰-۵ اين فرآيند را نشان ميدهد.

شكل ۱۰-۵ رديابي مسيردر محيطMPLS



شكل ۱۰-۵ نشان ميدهد كه اگرچه TTL بسته ورودي (گام ۱) به صفر ميرسد، روتر واشينگتن مي تواند بااستفاده از پشته برچسب اصلي بسته پيغام ICMP "زمان ازحدمجاز تجاوز كرد"، رابه روتر پاريس پس بفرستد.درمثال ۳-۵ چند debug خروجي براي نشان دادن اين فرآيند درعمل آمده است. آدرسهاي نشان داده شده 10.2.1.21 (آدرس اينترفيس روترپاريس كه آن را به واشينگتن متصل مي كند) 10.1.1.13 (آدرس اينترفيس سن خوزه كه آن را به واشينگتن متصل مي كند) و 194.22.15.2 (آدرس اينترفيس loopback درروتر سن خوزه) ميباشد.

مثال ۳-۵ ردیابي مسیردر شبکه MPLS

Paris# **debug ip icmp**
Paris# **traceroute 194.22.15.2**

Type escape sequence to abort.
Tracing the route to 194.22.15.2

1 10.2.1.22 4 msec 0 msec 0 msec
2 10.1.1.13 4 msec * 0 msec

ICMP: dst (10.2.1.21) port unreachable rcv from 10.1.1.13

Washington# debug ip icmp
Washington# debug tag packet

TAG: Et0/1/0: recvd: CoS=0, TTL=1, Tag(s)=36
TAG: AT0/0/0.1: xmit: (no tag)

ICMP: time exceeded (time to live) sent to 10.2.1.21 (dest was 194.22.15.2)

TAG: Et0/1/0: recvd: CoS=0, TTL=1, Tag(s)=36
TAG: AT0/0/0.1: xmit: (no tag)

ICMP: time exceeded (time to live) sent to 10.2.1.21 (dest was 194.22.15.2)

TAG: Et0/1/0: recvd: CoS=0, TTL=1, Tag(s)=36
TAG: AT0/0/0.1: xmit: (no tag)

ICMP: time exceeded (time to live) sent to 10.2.1.21 (dest was 194.22.15.2)

TAG: Et0/1/0: recvd: CoS=0, TTL=2, Tag(s)=36
TAG: AT0/0/0.1: xmit: (no tag)

TAG: Et0/1/0: recvd: CoS=0, TTL=2, Tag(s)=36
TAG: AT0/0/0.1: xmit: (no tag)

TAG: Et0/1/0: recvd: CoS=0, TTL=2, Tag(s)=36
TAG: AT0/0/0.1: xmit: (no tag)

San Jose# debug ip icmp

ICMP: dst (194.22.15.2) port unreachable sent to 10.2.1.21
ICMP: dst (194.22.15.2) port unreachable sent to 10.2.1.21

توجه:

draft-ietf-mpls-icmp براي اينكه رديابي مسير شامل اطلاعات برچسب mpls هم شود، اضافاتي به آن مي افزايد، كه بسيارمفيد بوده و اطلاعاتي نه فقط درموردمسيري كه بسته طي مي كند، بلكه درمورد برچسبهاي MPLSي كه در آن مسير استفاده مي شود،نيز فراهم مي آورد.

اگرچه توصيفات قبلي تمام عمليات ضروري براي كاركردن رديابي مسير درمحيط MPLS frame-mode را فراهم مي كند، شماباید به تاثيرات رديابي مسيردرشبكه MPLS كه توپولوژي آن با ATM-LSR ها ساخته شده است ،توجه كنيد.

فصل ١ ،" بازنگري معماري MPLS "يك ATM-LSR رابعنوان LSR باتعدادي اينترفيس LC-ATM كه سلولهاي بين اين اينترفيسها راباستفاده ازبرچسبها ي موجود درفيلد VPI/VCI هدايت مي كند،تعريف مي نمايد. نتيجه اين است كه TTL درهدر يك سلول ATM دردسترس نميباشد وبنابراين نمي تواند درهرگام درشبكه كنترل شود. به همين دليل وقتي ATM-LSR ها درمسير هستند، بابخش ATM شبكه بعنوان يك پرش IP رفتار مي شود.

توجه :

Draft-ietf-mpls-atm درمورد كنترل TTLدرمحيط ATM دربخش ١" كنترلTTL " بحث مي كند.

توجه:

شما مي توانيد TTL رادريك شبكه frame-mode بااستفاده ازفرمان propagate -ttl ip switching -tag[NO] غيرفعال كنيد. فصل ١٣ به تفضيل در مورداين فرمان بحث مي كند.

وقتي اين فرمان غيرفعال است ،فيلد ipttl درزمان اعمال برچسب درفيلد TTL MPLS كپي نمي شود ومقدار 255 بجاي آن درج ميگردد. اين عمل به طور موثري رديابي مسيررا درشبكه MPLS غيرفعال مي كند وخروجي فرمان رديابي مسير پرشهاي غير MPLS (پرشهايي كه بسته IP ارسال مي شود) درخروجي رانشان ميدهد.

توجه:

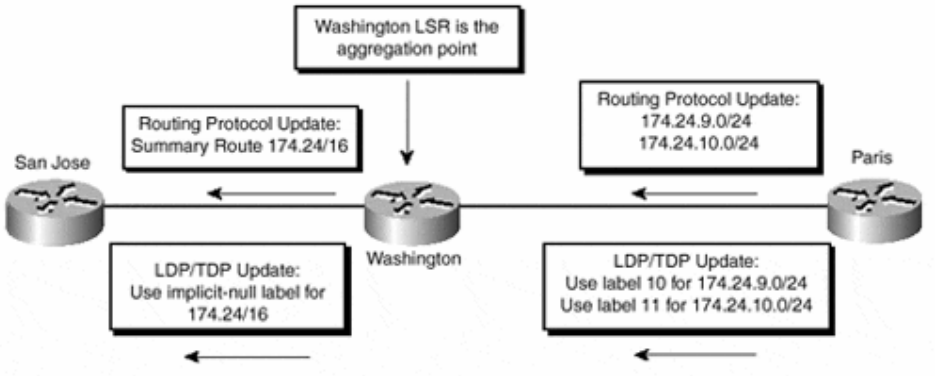
بخاطر هر پيغام ICMP زمان تجاوز كرد،كه درهنگام استفاده ازپشته برچسب اصلي بسته اضافه مي شود، خروجي تاخيري كه رديابمسيرنشان ميدهد، ديگر معنادار نخواهدبود. زيرا تاخير دقيقي كه بسته درهنگام عبـــوراز ستون فقرات باآن روبرو شده است رامنعكس نمي كند.

خلاصه سازی مسیردر یک شبکه MPLS

درهر پياده سازي براساس IP ،چه درآن از پروتكلهاي مسيريابي IP استفاده شود، يا IP درشبكه MPLS فعال باشد ،خلاصه سازي مسير بخش مهمي از ساختار شبكه ميباشد. خلاصه سازي مسير مكانيزم ضروري براي كاهش اندازه جدول مسيريابي لايه ۳، بادسته بندي تعدادي پسوند دريك مسيرخلاصه كمتر مشخص، رافراهم مي كند كه به كاهش مقدار حافظه موردنياز توسط وسايل درشبكه وكاهش overhead درزمان محاسبات مسير درتوپولوژي شبكه كمك مي كند.

دريك پياده سازي MPLS ،اين خلاصه سازي مي تواند تعداد برچسبها راكاهش دهد زيرا فقط يك برچسب براي خلاصه سازي مسير لازم است. شما مي توانيد مثالي درمورد خلاصه سازي وانتشار برچسب مربوطه رادرشكل ۱۱-۵ ببينيد.

شكل ۱۱-۵ خلاصه سازي مسيردرشبكه MPLS



درشكل ۱۱-۵ مي بينيد كه LSR واشينگتن دوپسوند 24/، 174.24.10.0/24, و174.24.9.0/24 از LSR پاريس، ازطريق پروتكل مسيريابي داخلي اش دريافت مي كند.ISR واشينگتن براي فرستادن يك مسيرخلاصه، پيكربندي شده است كه هردومسير خاص تر كه از ISR پاريس فرامي گيرد راپوشش مي دهد.

بابكارگيري اين پيكربندي، ISR واشينگتن نقطه تجمعي براي ISR هايي كه مسير خلاصه رابكار مي برند، مي شود. اين يعني هر LSP كه مسيرخلاصه رابكار مي برد،لازم است به LSR واشينگتن ختم شود. نتيجه اين است كه LSR واشينگتن ،نيازبه امتحان برچسب سطح دوم هربسته داردونسبت به آنچه مي يابد، به عمل انجام شده وابستگي مي يابد. اگريك برچسب وجود داشته باشد، LSR بسته ها رابراساس برچسبش سوئيچ مي كند. اگربرچسبي وجود نداشته باشد، LSR نيازبه امتحان اطلاعات هدرلايه ۳ براي كلاسه بندي مجدد بسته دارد.

بخاطر ضرورت كلاسه بندي مجدد بسته ها درنقطه تجمع، تاكيد مي شود كه وسيله اي كه تجميع ايجاد مي كند، يك سوئيچ ATM نباشد.اين بدان دليل است كه يك سوئيچ ATM هيچ سخت افزاري براي پردازش اطلاعات لايه ۳ كه توسط آنها هربسته اي رامجدداً كلاسه بندي مي كند، ندارد وفقط از VPI/VCI ورودي بعنوان مرجع تشخيص پورت خروجي و VPI/VC1 خروجي كه بايد براي سلول ورودي بكاررود، استفاده مي كند.

توجه:

خلاصه بندي هنگام استفاده درمحيط MPLS/VPN نيز كاربردهاي عمده اي دارد.فصل ۱۳ به تفضيل دراين مورد بحث مي كند.

خلاصه:

اين فصل درمورد عناوين پيشرفته MPLS كه شديداً براي پياده سازي يك ستون فقرات MPLS ضروري اند، بحث كرد. اما هنگام طراحي وعيب يابي پيشرفته شبكه بكار نمي آيد.

شما مي توانيد مكانيزمهاي پيشرفته اي در IOS سيسكو رابدين ترتيب، كنترل كنيد:

- انتشار كنترل شده برچسب، جايي كه شما مي توانيد باكنترل اينكه ISR كدام برچسبها رابه همسايه هاي دربالا دستي اش اعلام مي كند ، كاملاً مشخص كنيد كدام بسته ها برچسب گذاري شده اندوكدام بسته ها مسيريابي IP.
- MPLS- MTU دريك بخش LAN درتركيب با MTU افزايش يافته فيزيكي درهمان بخش، كه به بسته هاي IP باحداكثر اندازه اجازه مي دهد درواسطه ازنوع اترنت بعنوان فريمهاي غول پيكر بدون قطعه قطعه شدن، افزايش يابند.
- افزايش IP TTL كه باآن شما مي توانيد، كنترل كنيد كه آيا يك ميزبان انتهايي متصل به يك شبكه MPLS مي تواندعمل رديابي مسير درشبكه انجام دهد.
- پارامتر atm maxhopsكه به شما اجازه مي دهد، جلوگيري ازايجاد لوپ را درمحيط هاي ATM كاملاً تنظيم كنيد.

Glossary

Advertisement	اعلان عمومی
Assign	الصاق کردن
Architecture	معماری
Control plane	واحد کنترل
Data plane	واحد دیتا
Deploy	اجرا-انجام –پیاده سازی
Down-streem	پایین رونده
Forwarding	ارسال
Forwarding loop	لوپهای ارسالی
Fragmentation	قطعه قطعه کردن
Guideline	شاخص
Hop	پرش
Implementation	پیاده سازی –بکارگیری
Independent control	کنترل مستقل
label	برچسب
Ordered control	کنترل سفارشی
Payload	طول داده
Up-streem	بالا رونده
Workaround	راهکار