Official Cert Guide

Advance your IT career with hands-on learning

Hands-On Labs

Review Exercises

Config Checklists

CCNA 200-301

Volume 1

WENDELL ODOM,
CCIE® NO. 1624 EMERITUS

ciscopress.com

نهال را "باران" باید، تا سیرابش کند از آب حیات و "آفتاب "باید، تا بتاباند نیرو را و "محکم" کند شاخه های تازه روییده را؛ بسی شایسته است از استاد محترم و توانا جناب آقای مهندس منتخبی و دوستانم که همواره نگارنده را مورد لطف و محبت خود قرار داده‌اند و برای گردآوری اطلاعات دوره CCNA اینجانب را یاری نموده‌اند، تقدیر و تشکر نمایم. توفیقات روز افزون ایشان را توأم با صحت و سعادت از خداوند متعال خواستارم.

مهدی شاه‌محمدی – تابستان ۱۴۰۲

MENU

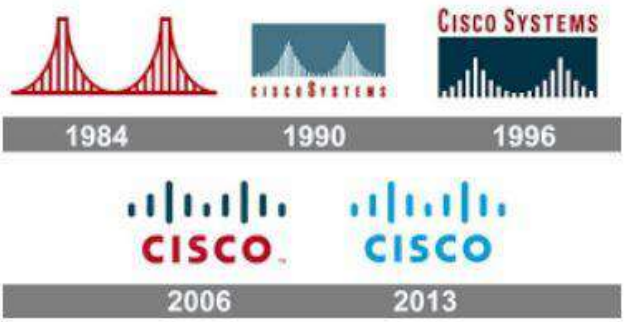
About CISCO Company

شرکت «سیسکو سیستمز» (Cisco Systems) کمپانی آمریکایی تولیدکننده تجهیزات شبکه (Network) است که مرکز آن در شهر سن خوزه، کالیفرنیا در ناحیه مشهور به سیلیکان ولی در ایالت کالیفرنیا قرار دارد. این کمپانی محصولات وابسته به شبکه و ارتباطات را مدل سازی می کند و با سه نام تجاری گوناگون سیسکو، لینکسیس و ساینتیفیک آتلانتا به فروش می‌رساند. در ابتدا، سیسکو تنها روترهای چند پروتکل را تولید میکرد ولی امروز محصولات سیسکو را در خدمات شبکه می‌توان پیدا کرد.

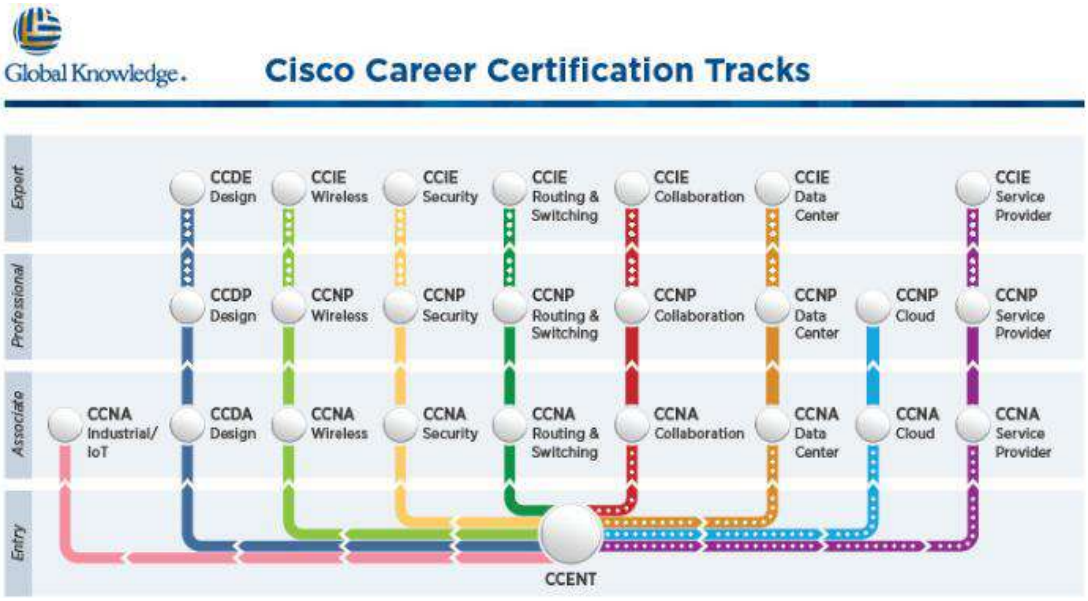
لیونارد بوساک و سندی لرنر (دارای گواهینامه لیسانس از دانشگاه ایالتی کالیفرنیا، فوق لیسانس اقتصاد سنجی از دانشگاه کلرمونت و فوق لیسانس علوم کامپیوتر از دانشگاه استنفورد)، زوجی که در مبحث کامپیوتر دانشگاه استنفورد کار می کردند، Cisco را در سال ۱۹۸٤ تأسیس کردند.

با وجود اینکه Cisco نخستین شرکتی نبود که Router(رهیاب) مدل سازی و تولید می کرد، اولین شرکتی بود که یک Router چند پروتکل موفق تولید می کرد که اجازه پیوند بین پروتکل های مختلف شبکه را می دهد.

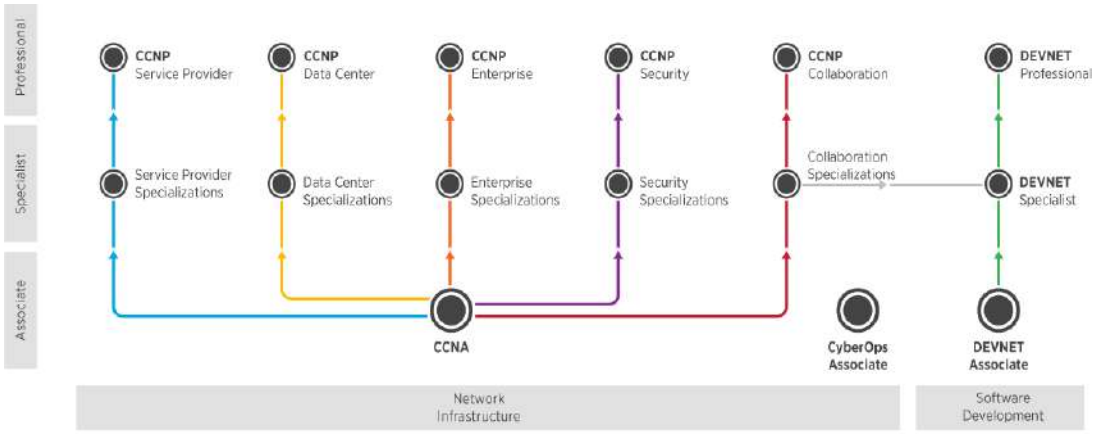
نام «سیسکو» مخفف سانفرانسیسکو است. با توجه به اظهارات جان مرگریج، کارمند ۳٤ ساله و مدیر سابق شرکت، موسسان کمپانی زمانی که داشتند به سمت ساکرامنتو رانندگی می کردند تا کمپانی را به ثبت برسانند، با عکس پل گلدن گیت در نور خورشید مواجه می شوند و اسم و سمبل کمپانی را بر این اساس انتخاب می کنند.



Cisco Certification



Before



Now

Switch & Switching

Types of Cisco switch:

سوئیچ های سیسکو انواع مختلفی دارند و برای کاربردهای متفاوتی طراحی شده‌اند. مثلا سوئیچ های کاتالیست برای شبکه‌های محلی و سوئیچ های Nexus برای دیتاسنترها. به طور کلی انواع سوئیچ های سیسکو به صورت زیر است:

1. Fixed switch →

سوئیچ های fixed محبوب‌ترین سوئیچ ها در بازار هستند. این سوییچ ها می‌توانند هم مدیریتی باشند و هم غیرمدیریتی و برای تمام شبکه ها با هر سایزی استفاده می‌شوند.

پورت ها در سوییچ های fixed انواع مختلفی از نظر سرعت و اتصال دارند اما معمولا دارای حداقل سرعت 1Gbpsهستند و انواع اتصال شامل RJ45یا فیبر نوری است. اتصال چند سوئیچ fixed به هم از طریق کابل شبکه مثل Cat6 یا فیبر نوری امکان‌پذیر است تا پورت trunk بین آنها به وجود بیاید.

1. Cisco Catalyst 2960 Series
2. Cisco Catalyst 2960-S Series
3. Cisco Catalyst 3560 Series
4. Cisco Catalyst 3560-E Series
5. Cisco Catalyst 3560-X Series
6. Cisco Catalyst 3750 Series
7. Cisco Catalyst 3750-E Series
8. Cisco Catalyst 3750-X Series
9. Cisco Catalyst 4900 Series
10. Cisco Catalyst 2975 Series

سوئیچ ۲۹۶۰

2. Modular switch →

بر خلاف سوئیچ fixed سوئیچ ماژولار با افزودن ماژول روی کیس قابل توسعه و ارتقا است یعنی می‌تواند پورت‌های بیشتری به آنها اضافه کرد و کارایی بیشتری از آنها توقع داشت. این مدل سوئیچ که با نام blade نیز شناخته می‌شود، معمولا در کیس‌های بزرگ عرضه می‌شوند و با افزودن هر ماژول امکان افزودن پورت و افزودن کاربر فراهم می‌شود. اغلب این مدل سوئیچ ها در لایه سوم هم کار می‌کنند و می‌توانند به عنوان روتر استفاده شوند. استفاده از آنها بیشتر در شبکه‌های سازمانی و اینترپرایزها و دیتاسنترها است.

1. Cisco Catalyst 4500 Series
2. Cisco Catalyst 6500 Series
3. Cisco Nexus 7000 Series

3. Stackable switch →

سوئیچ Stackable ترکیبی از سوئیچ fixed و ماژولار است یعنی برخی مدل‌های سوئیچ fixed می‌توانند با دیگر سوئیچ‌های سیسکو هم مدلشان ترکیب شوند. این سوئیچ های fixed با کابل مخصوصی از قسمت پشت به هم وصل می‌شوند و با هم کار می‌کنند به طوری که انگار یک سوییچ داریم اما با تعداد پورت بیشتر کار می کند.

فناوری Cisco StackWise چیست؟

روشی نوآورانه برای به‌کارگیری تجمیعی سوییچ‌ها است که اجازه می‌دهد منابع مختلف را با یکدیگر ترکیب کرده و در قالب یک مفهوم واحد در اختیار کلاینت‌های شبکه قرار داد. البته این فناوری قابلیت پشتیبانی و متصل کردن حداکثر ۹ سوئیچ را به عنوان یک واحد سوئیچینگ یکپارچه دارد. این دستگاه‌ها از طریق کابل stack که قابلیت انتقال 400Gb/s دیتا را دارد، به هم به صورت شکل بالا متصل می‌شوند. این فناوریextendشدن(توسعه پیدا کردن) و Redundancy(برای مدیریت spof) را تسهیل میکند. بعد از stack کردن آدرس اینترفیس ۳ قسمتی می‌شود(قسمت اول=شماره سوئیچ – قسمت دوم= شمارهline – قسمت سوم= شماره پورت).

Interface TYPE Stack/Module/Number → Interface Gi 2/0/1

نکته۱: با کنسول که به سوئیچ استک شده متصل میشویم، به تعداد سوئیچ داریم ولی با Telnet یک سوئیچ داریم.

نکته۲: طول کابل Stack نهایتا ۵ متر است. هنگامی که تعدادی سوییچ را با کابل Stack به یکد یگر متصل می کنیم یکی از سوییچ‌ها بعنوان Master Stackشناخته می شود و سایر سوئیچ‌های موجود در آن Stack بعنوان سوئیچ‌های Slave شناخته می شوند.

4. PoE switch →

PoE مخفف Power over Ethernet است و سوئیچ PoE بر اساس تکنولوژی PoE کار می‌کنند. در PoE، برق و دیتا در یک کابل منتقل می‌شوند یعنی دیتا به صورت موازی یا برق به گیرنده می‌رسد. انعطاف‌پذیری از ویژگی‌های سوئیچ های PoE است.

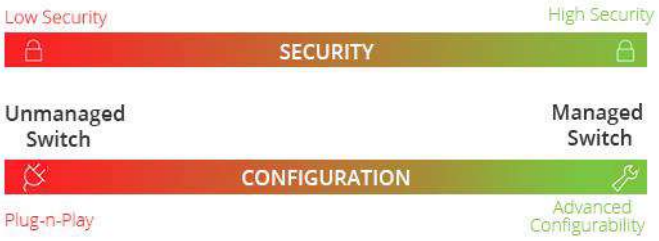
5. Fiber optic switch →

اگر برای اتصال از فواصل طولانی نیاز دارید به عنوان مثال بیش از ۱۰۰ متر که کابل اترنت معمولی کافی نمی باشد، باید از کابل فیبر نوری استفاده کنید. پورت‌های فیبر نوری را SFP – Small Form Factor Pluggable می‌نامند. پورت‌های فیبر نوری برای اتصال سوئیچ ها در یک طبقه ساختمان و یا ساختمان‌هایی با فواصل چند کیلومتر از هم استفاده می‌شوند.

6. Unmanaged Switch →

سوئیچ های غیرمدیریتی اغلب در شبکه‌های خانگی و شرکت‌های کوچک استفاده می‌شوند چون بلافاصله پس از نصب، شروع به کار می‌کنند. با Unmanaged Switch ها می‌توان دستگاه‌های اترنت را به راحتی با هم ارتباط داد. این سوئیچ ها برای برقراری ارتباط، فقط به کابل نیاز دارند و با کانفیگ ثابتی به بازار می‌آیند. سوئیچ های غیرمدیریتی فقط می‌توانند دستگاه‌های یک VLAN را به هم وصل کنند و فقط اتصال لایه ۲ را فراهم می‌کنند. سوئیچ های غیرمدیریتی باعث می‌شوند دستگاه‌های اترنت به صورت خودکار و اتوماتیک با دیگر دستگاه‌ها ارتباط برقرار کنند. از مدل‌های غیرمدیریتی سیسکو می‌توان به Cisco Business 110 Series اشاره کرد

تفاوت اصلی بین سوئیچ های مدیریتی و غیر مدیریتی، توانایی کانفیگ کردن سوئیچ و اولویت‌دهی به ترافیک LAN است تا مهم‌ترین اطلاعات در اولویتِ ارسال قرار گیرند .



7. managed Switch →

سوئیچ‌های مدیریتی سیسکو (Managed switches) امنیت، امکانات و انعطاف‌پذیری را در اختیار کاربران قرار می‌دهند، زیرا می‌توانید آن‌ها را به‌گونه‌ای پیکربندی کنید که شبکه خود را به شکل اختصاصی دربیاورید.

سفارشی سازی شبکه باعث می‌شود تا مدیریت و کنترل شبکه راحت‌تر شود و همچنین کیفیت خدمات برای کسانی که به شبکه دسترسی دارند، بسیار مطلوب خواهد بود. مدل‌های سری Cisco 350X،Cisco 550X و Cisco Business 350 در دسته‌ی سوئیچ‌های مدیریتی قرار دارند.

ویژگی‌های مهم سوئیچ های مدیریتی:

Quality of Service – QoS

شامل اولویت‌دهی به ترافیک شبکه است که با اختصاص اولویت بالاتر به ترافیکِ مهم‌تر است. این کار منجر به افزایش کارایی شبکه می‌شود. بدین ترتیب از داده‌های حساس به تاخیر (Delay Sensitive Data) مانند Real Time Voice پشتیبانی می‌شود.

Virtual LANs

VLANها امکان گروه‌بندی دستگاه‌ها را به صورت منطقی می‌دهد تا ترافیک را بین این گروه‌ها ایزوله کند حتی اگر ترافیک در یک شبکه فیزیکی رد و بدل شود. این دسته‌بندی و ایزوله کردن باعث کاهش ترافیک غیرضروری در شبکه می‌شود.

Redundancy

با وجود افزونگی وRedundancy ، اگر اتصال یا کابلی در شبکه قطع شود، با ایجاد مسیر جایگزین برای داده و ترافیک، از بروز قطعی در شبکه و Downtimeجلوگیری می‌شود Redundancy .در شبکه با استفاده از پروتکل STP یا Spanning Tree Protocol فراهم می‌شود. یعنیSTP ، افزونگی مسیر را در شبکه ایجاد می‌کند و در عین حال از ایجاد لوپ جلوگیری می‌کند. الگوریتمSTP ، چند مسیر اکتیو را بین سوئیچ ها ایجاد می‌کند اما در هر لحظه، بین دو دستگاه، فقط یک مسیر اکتیو قابل استفاده است. در نتیجه لوپ و حلقه ایجاد نمی‌شود و لینک‌های افزونه به عنوان بکاپ وجود دارند.

Port Mirroring

مانیتورینگ پورت در تشخیص خطا و مشکل در شبکه استفاده می‌شود. Port Monitoring، ترافیک شبکه را کپی کرده و به یک پورت در همان سوئیچ می‌فرستد تا تحلیلگر شبکه، آن را تحلیل کند. بدین صورت عیب یابی مشکلات شبکه با ترافیک تستی روی پورت‌ها و یا سگمنت‌های دیگر انجام می‌شود. مزیت آن چیست؟ شما با این ویزگی می‌توانید بدون اینکه شبکه را از دسترس خارج کنید، اقدام به عیب یابی شبکه تان کنید.

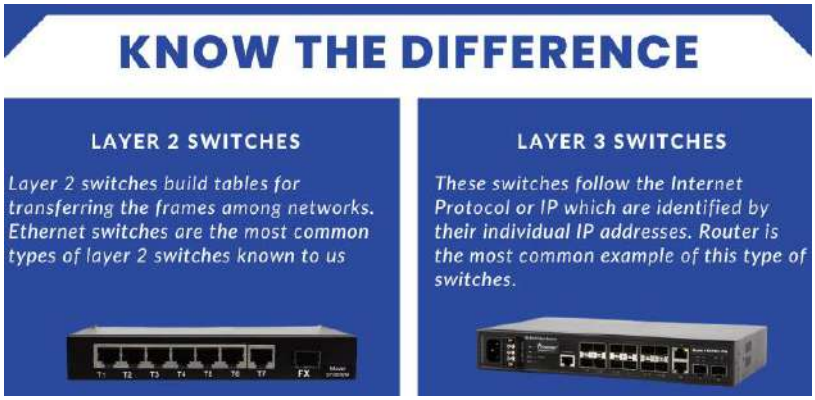
8. Smart Switch →

قابلیت‌های سوئیچ های اسمارت چیزی بین سوئیچ مدیریتی و غیر مدیریتی است یعنی سوئیچ های هوشمند دارای قابلیت‌های ابتدایی مدیریتی هستند و برخی سطوح امنیتی را فراهم می‌کنند اما نسبت به سوئیچ های مدیریتی، اینترفیس مدیریتی آسان‌تر و قابلیت‌های مدیریتی محدودتری دارند. این سوییچ ها دارای قابلیت‌های مهمی مانند پیکربندی VLAN و speed/duplex control و SNMP هستند. کاربرد Smart Switch ها در LAN هایی است که از Allocation و Data Transfer پشتیبانی می‌کنند.

9. Layer 3 Switch →

سوئیچ ها معمولا در لایه دوم مدل OSI یعنی لایه Data Network کار می‌کنند و وظیفه آن انتقال فریم‌های اترنتی از یک پورت به پورت دیگر است. اما سوئیچ های پیشرفته دیگری داریم که بسته‌های IP را مسیریابی می‌کنند درست مانند روتر شبکه. این سوئیچ‌ها را سوییچ لایه ۳ می‌نامیم چون در لایه ۳ از مدل OSI کار می‌کنند و ترکیبی از دستگاه لایه ۲ و ۳ هستند.

نرم افزار سوئیچ لایه ۳ از سوئیچ لایه ۲ پیشرفته‌تر است و می‌تواند پروتکل‌های مسیریابی دینامیک مانند RIP و OSPF را اجرا کند. در سوئیچ لایه ۲ می‌توان چند VLAN را کانفیگ کرد اما مسیریابی بین این VLAN ها توسط خود سوئیچ ممکن نیست. اما در سوئیچ لایه ۳ می‌توان چند VLAN را کانفیگ کرد و خودِ سوئیچ می‌تواند مسیریابی شبکه در سطح IP را بین VLAN ها فراهم کند. این تکنیک را مسیریابی داخل inter-vlan routing می‌نامند.



10. Data center Switch →

سوئیچ های دیتاسنتری ویژگی‌های خاصی دارند تا بتوانند کارایی و سرعت بسیار بالا، ظرفیت بیشتر در پورت، امنیت، QoS و غیره را فراهم کنند. بهترین نمونه از سوئیچ های دیتاسنتری سوئیچ سیسکو سری Nexus است. با این سوئیچ ها می‌توان مجازی سازی و مفهوم SDN – Software Defined Network را به راحتی پیاده سازی کرد.

SDN روشی برای شبکه سازی است که از پروتکل‌های باز مانند OpenFlow برای کنترل نرم افزار در لبه شبکه استفاده می‌کند و برای کنترل دسترسی به سوئیچ‌ها و روترها استفاده می‌شود.

The difference between Cisco switches :

تفاوت سوئیچ های سیسکو در تکنولوژی‌هایی است که هر کدام پشتیبانی می‌کنند. مثلا:

- ✓ پشتیبانی یا عدم پشتیبانی از PoE وPoE+
- ✓ ماژولار یا مستقل یا Stackable بودن
- ✓ LANLiteیا LANBase بودن
- ✓ Fast Ethernetیا Gigabit Ethernet بودن
- ✓ دسکتاپی یا رک مونت بودن
- ✓ مدیریتی یا غیرمدیریتی یا اسمارت بودن
- ✓ سرعت و تعداد پورت‌ها
- ✓ پشتیبانی از فیبر نوری و...

Port status Led :

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:

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.

Cisco Catalyst Switches :

در برند سوئیچ‌های Cisco Catalyst برای شبکه‌هایLAN ، شرکت سیسکو سری‌ها و خانواده‌های گوناگونی از سوئیچ را تولید می‌کند. هر یک از این سری سوئیچ‌ها، شامل تعداد ویژه‌ای از مدل‌های سوئیچ می‌باشد، که ویژگی‌های شبیه به هم دارند. شباهت‌هایی نظیر نسبت قیمت به کارایی، همچنین شباهت‌های سخت‌افزاری.

برای مثال، سری سوئیچ‌های ۲۹۶۰ XR-یکی از سری سوئیچ‌های شرکت سیسکو می‌باشد. شرکت سیسکو، سری سوئیچ‌های ۲۹۶۰ XR-را به عنوان سوئیچ‌های کاملا برجسته، با قیمت پایین در رده‌ی سوئیچ‌های کابلی برای شبکه‌های بزرگ و تجاری، وارد بازار کرده است. این به این معناست که شما می‌توانید از این سوئیچ‌ها، به عنوان سوئیچ‌های لایه دسترسی یا Access در طراحی شبکه‌های خود، استفاده کنید.

شکل زیر تصویری از ۱۰ مدل مختلف از سری سوئیچ‌های ۲۹۶۰–XR شرکت سیسکو را نشان می‌دهد. از یک از سری سوئیچ‌های این شرکت، شامل چندین مدل سوئیچ می‌شوند، که شامل ترکیبی از قابلیت‌ها می‌باشند. برای مثال، برخی از این سوئیچ‌ها دارای ۴۸ پورت UTP RJ-45 می‌باشند، همچنین این پورت‌ها می‌توانند به صورت اتوماتیک از استانداردهای (10 Mbps) 10BASE-T یا (100 Mbps) 100BASE-T و یا 1000BASE-T (1 Gbps) استفاده کنند.

10Base-T (10 Mbps – Ethernet)

100 Base-T (100Mbps – Fast Ethernet)

1000Base-T (1000Mbps – Gigabit Ethernet)

در سوئیچ‌های سیسکو، هر پورت یا اینترفیس، شامل یک نوع و شماره می‌باشد، و از این اطلاعات می‌توان در دستورات سوئیچ استفاده کرد. منظور از نوع اینترفیس، Ethernet، Fast E، Gig E و ... می‌باشد، که در واقع نشان دهنده سرعت هر اینترفیس می‌باشد. نوع اینترفیس، سریع‌ترین سرعتی که اینترفیس می‌تواند پشتیبانی کند را نشان می‌دهد. برای مثال، یک اینترفیس ۱۰/۱۰۰/۱۰۰۰ (که می‌تواند از سرعت‌های ۱۰ Mbps، ۱۰۰ Mbps و یا ۱۰۰۰ Mbps پشتیبانی کند) به نام اینترفیس Gig Ethernet شناخته می‌شود، و سرعتی که در این لحظه استفاده می‌کند، مد نظر نیست.

برای شماره‌گذاری منحصر به فرد هر یک از این اینترفیس‌ها، برخی از سوئیچ‌های Catalyst، از دو شماره به صورت x/y استفاده می‌کنند، در حالی که برخی دیگر از سوئیچ‌ها از سه رقم به شکل x/y/z استفاده می‌کنند. برای نمونه، دو اینترفیس ۱۰/۱۰۰/۱۰۰۰ در مدل‌های قدیمی‌تر سیسکو با نام‌های Gigabit Ethernet 0/0 و Gigabit Ethernet 0/1 شناخته می‌شدند، ولی در مدل‌های جدیدتر ۲۹۶۰–XR از نام‌های Gigabit Ethernet 1/0/1 و Gigabit Ethernet 1/0/2 استفاده می‌شود.

عدد اول یعنی شماره لاین / عدد دوم یعنی شماره پورت

IOS :

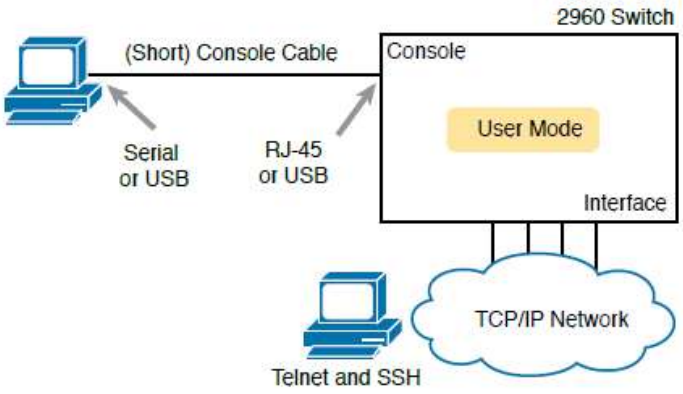
مانند هر سخت‌افزار کامپیوتری دیگری، سوئیچ‌های سیسکو نیز به نوعی از سیستم عامل نیاز دارند. سیسکو، این سیستم عامل را Internetwork Operating Systemیا **IOS** می‌نامد.

IOS شرکت سیسکو برای سوئیچ‌های Catalyst، وظیفه پیاده‌سازی و کنترل منطق و عملکرد این سوئیچ‌ها را بر عهده دارد. علاوه بر کنترل کارایی و رفتار سوئیچ، IOS سیسکو یک رابطی را برای مهندس شبکه محیا می‌کند، که به آن CLI گفته می‌شود. رابط **CLI** در IOS سیسکو به کاربر اجازه می‌دهد، با استفاده از یک نرم‌افزار شبیه‌ساز ترمینال (Terminal Emulator)، متن وارد شده توسط کاربر را دریافت کند. زمانی که کاربر کلید Enter را می‌زند، این نرم‌افزار متن وارد شده را به سوئیچ ارسال می‌کند. سوئیچ نیز این متن را بررسی کرده و در صورتی که متن وارد شده، یک دستور بود، آن را اجرا کرده و سپس پاسخ آن را به نرم‌افزار شبیه ساز ترمینال برمی‌گرداند.

Terminal Emulation Programs :
Putty
Super Putty
Hyper Terminal
Secure CRT

رابط CLI سوئیچ‌های سیسکو از طریق روش‌های محبوبی به نام کنسول (Console)، Telnet، و SSH قابل دسترسی است. دو روش Telnet و SSH برای دسترسی به سوئیچ از شبکه IP که در آن سوئیچ در آن قرار دارد استفاده می‌کنند.

به طور کلی کنسول نیازمند یک ارتباط فیزیکی مستقیم مابین سوئیچ و یک کامپیوتر و یک نرم‌افزار می‌باشد. در طرف دیگر، Telnet و SSH فقط نیازمند نرم‌افزار موجود بر روی کامپیوتر می‌باشند، اما این روش‌ها متکی بر شبکه TCP/IP مابین سوئیچ و کامپیوتر، برای انتقال اطلاعات می‌باشند.



The difference between Cisco ios versions :

Comparison	LAN Lite	LAN Base	IP Base	IP Services
Scale of business	Small	Small-to-medium	Medium-large	Large
Layer 2	Yes	Enterprise access	Complete access	Complete access
Layer 3	No	Yes	Enterprise access	Complete access
Security	Basic	Enterprise access Security	Complete access Security	Complete access Security
QoS	Basic	Enterprise access QoS	Complete access QoS	Complete access QoS

CLI :

شرکت سیسکو برای محصولات خود از جمله روترها و اکثر مدل‌های سوئیچ‌های Catalyst LAN از مفهومی به نام Command-Line Interface یا CLI استفاده می‌کند. CLI یک رابط متنی است که در آن مهندس شبکه، دستورات را به صورت متنی وارد کرده و سپس کلید Enter را می‌زند. با زدن این کلید، دستورات به سوئیچ یا روتر ارسال شده و بر روی دستگاه اجرا می‌شود. گاهی اوقات هم پیامی در نتیجه این دستورات برای کاربر برگشت داده می‌شود.

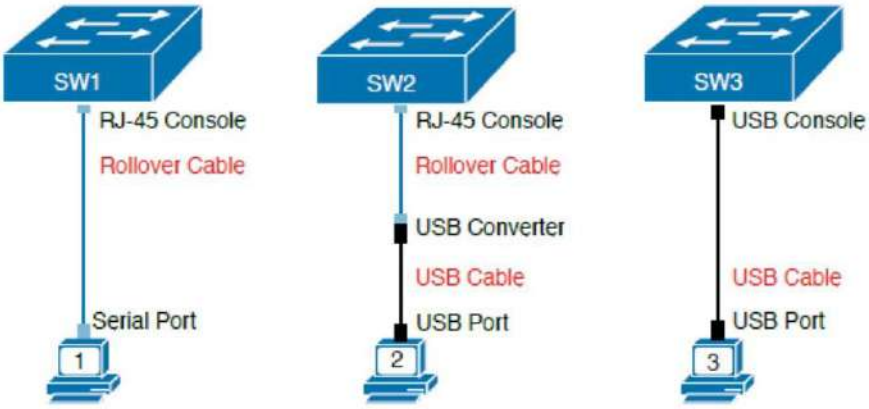
سوئیچ‌های Catalyst شرکت سیسکو همچنین از روش دیگری برای پیکربندی و نظارت این سوئیچ‌ها، پشتیبانی می‌کنند. برای مثال، مهندسین شبکه می‌توانند از یک رابط وب برای اتصال به سوئیچ استفاده کنند. در این روش، مهندس شبکه، یک مرورگر وب را باز کرده و به وب سروری که بر روی سوئیچ در حال اجرا می‌باشد، متصل می‌شود. این سوئیچ‌ها همچنین می‌توانند توسط یک نرم‌افزار مدیریت شبکه، کنترل و مدیریت کرد.

Cabling the Console Connection :

پشت دستگاه های سیسکو پورت کنسول قرار دارد. زمانی از این پورت استفاده می شود که برای اولین بار می خواهیم پیکربندی سوییچ یا روتر را انجام دهیم. در لحظه فقط یک نفر می تواند به دستگاه متصل شود و باید نزدیک دستگاه باشد. بدلیل اینکه در ابتدا روتر یا سوییچ هیچگونه تنظیمات شبکه ای ندارد و به همین دلیل نمی تواند برای متصل شدن به آن از SSH یا Telnet ویا HTTPS استفاده کرد.

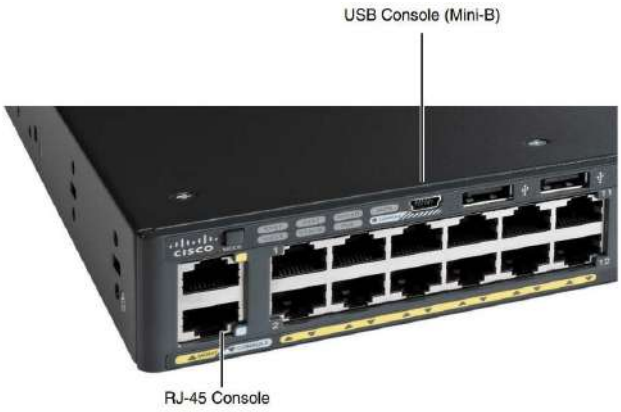
برای اینکه بتوانیم به کنسول دستگاه متصل شویم از کابل Console Cable - DB-9 Female (RS232) بعنوان کابل کنسول یا Cable Over Rollمعروف است استفاده میکنیم. یک سر این کابل سوکت ٤٥ RJ است که به پورت کنسول روتر یا سوییچ وصل می شود و سمت دیگر به پورت سریالCOM کامپیوتر متصل میشود، که قرار است روتر یا سوییچ را پیکربندی کند. به این نوع ارتباط Access Local می گویند.

اکثر کامپیوترهای امروزی از استاندارد کابل‌های USB برای استفاده از کابل کنسول پشتیبانی می‌کنند. شرکت سیسکو در روترها و سوئیچ‌های جدید خود از پورت USB برای اتصال کابل کنسول استفاده می‌کنند.



روترها و سوئیچ‌های قدیمی‌تر که پورت کنسول RJ-45دارند، نمی‌توانند به صورت مستقیم با کامپیوتر ارتباط برقرار کنند(شکل وسط). برای اتصال یک کامپیوتر جدید که از پورت سریال پشتیبانی نمی‌کند به یک روتر یا سوئیچ قدیمی، باید از یک مبدل USB استفاده کرد، که کابل کنسول قدیمی را به کابل USBتبدیل می‌کند.

****نکته: زمانی که از یک مبدل USB کنسول استفاده می‌کنید، نیاز است تا نرم‌افزاری را بر روی سیستم عامل کامپیوتر خود نصب کنید، تا سیستم عامل متوجه شود که انتهای این کابل USB یک کابل کنسول می‌باشد.



برای نمونه، سری سوئیچ‌های XR-۲۹۶۰، از هر دو مدل پورت‌های کنسول RJ-45 و USBپشتیبانی می‌کنند و فقط از یکی از این پورت‌ها می‌توان در لحظه استفاده کرد. توجه داشته باشید که در پورت کنسول USB از نوع mini-B استفاده می‌شود.

*سوال: چرا برخی از سوئیچ‌ها مانند ۲۹۶۰ کلید on/off ندارند؟

چون سوئیچ‌ها عمدتا در نزدیکی End user ها قرار دارند، به همین شاید عمدا یا سهوا از این کلید استفاده شود. به همین خاطر چون سوئیچ‌ها همیشه باید در دسترس باشند از گذاشتن این کلید خودداری کرده اند.

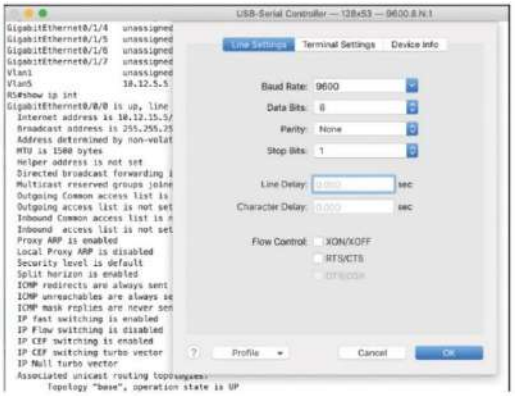
Accessing the Cisco IOS CLI :

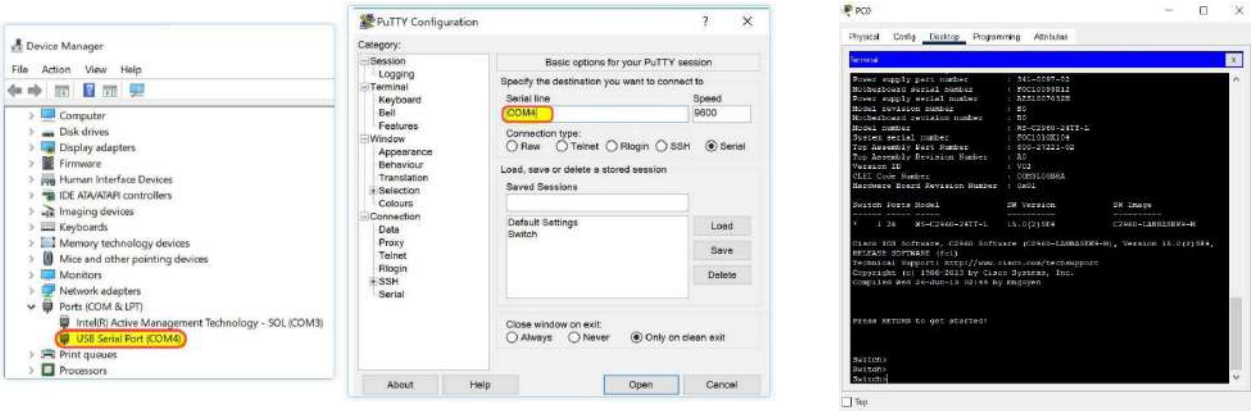
(A) Local Device Access Configuration:

بعد از اتصال فیزیک کامپیوتر به پورت کنسول و نصب برنامه شبیه ساز ترمینال، نرم‌افزار شبیه ساز ترمینال باید به گونه‌ای تنظیم شود که تنظیمات پورت سریال کامپیوتر، با تنظیمات پورت سریال سوئیچ با یکدیگر همخوانی داشته باشند. تنظیمات پیشفرض پورت کنسول به شرح زیر می‌باشد، و زمانی که شما نرم‌افزار شبیه ساز ترمینال را اجرا می‌کنید باید تنظیمات زیر را در آن وارد کنید.

نظیمات مربوط به ترمینال برای اتصال از طریق کنسول:

- Baud Rate: 9600 bit/second
- Data Bits: 8-bit ASCII
- Parity: No parity bits
- Stop Bits: 1 stop bit
- No hardware flow control





نکته۱: در برنامه Putty باید توجه داشته باشیم که serial line با com سریال متصل به PC برابر باشد.

نکته۲: برای اینکه متوجه شویم سیستم ما کدام پورت COM را شناسایی کرده، وارد Manager Device می شویم.

(B) Remote Device Access Configuration:

در اکثر مواقع بعد از پیکربندی Router یا Switch نیاز داریم که از راه دور به دستگاه دسترسی داشته باشیم تا در صورت نیاز جهت پیکربندی یا رفع عیب به دستگاه متصل شویم، مثال در نظر بگیرید شما یک یا چند Device را در سطح یک شهر یا کشور پیکربندی کرده اید و پس از این کار باید به مشترکین خود خدمات پشتیبانی ارائه دهید. در صورتی که از راه دور دسترسی به این دستگاه را نداشته باشید، هنگامی که نیاز به ایجاد تغییر در پیکربندی دستگاه یا رفع عیب باشید باید جهت دسترسی به دستگاه مسیر زیادی را طی کنید که مستلزم وقت و هزینه زیادی خواهد بود. جهت حل این مشکل سیسکو از پروتکل هایی مانند SSH,Telnet استفاده می کند:

نکته: SSH در مقابل Telnet امنیت بیشتری دارد چون SSH هنگام انتقال ترافیک ابتدا آن را رمزنگاری می کند سپس ترافیک را ارسال می کند، اما Telnetترافیک را به همان شکل اصلی خود یا Plane Text ارسال می کند.

(BA) Telnet

تلنت از جمله پروتکل‌های بحث‌برانگیز است که سرپرستان شبکه علاقه زیادی به آن دارند، اما کارشناسان امنیتی سعی دارند دسترسی به این سرویس را غیرفعال کنند و کارشناسان شبکه را متقاعد کنند گزینه‌های جایگزین را به جای آن استفاده کنند. تلنت سرویسی از نوع tcp است که از پورت ۲۳ استفاده می‌کند و در لایه ۵ کار میکند. تلنت به دلیل این‌که اطلاعات را در قالب یک متن ساده(clear text) و بدون استفاده از هیچ مکانیزم رمزنگاری انتقال می‌دهد، به هکرها اجازه می‌دهد بدون مشکل به شنود و سرقت اطلاعات بپردازند. با این‌حال، به دلیل سهولت استفاده راهکار فوق هنوز هم از جانب سرپرستان شبکه برای اتصال به سوییچ استفاده می‌شود.

- **مراحل دسترسی به سوییچ از طریق تلنت:**

۱. تخصیص آدرسIP (به همراه Subnet mask) روی شبکه محلی مجازی اول(اینترفیس logical) (VLAN1) و روشن کردن آن(چون پیش فرض خاموش می‌باشد)

۲. ویرایش نام سوئیچ در صورت تمایل (Switch(config)#hostname Switch1)

۳. فعال کردن سرویس تل نت(<> line vty) و رمزگذاری

٤. رمزگذاری Enable mode

٥. write

Telnet Configuration :

1 – IP address Assignment

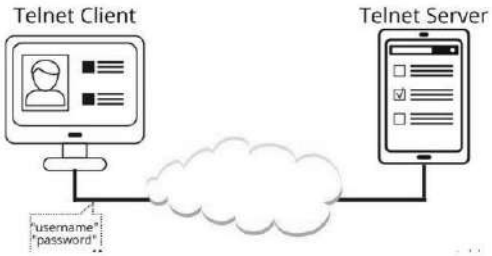
```
switch(config)#interface vlan <>
switch(config-if)#ip address <IP> <Subnet Mask>
switch(config-if)#no shutdown
switch(config-if)#exit
```

2 – User Mode Security ➔ Line VTY

```
switch(config)#line VTY <>
switch(config-line)# {password | secret } <>
switch(config-line)#login
switch(config-line)#exit
```

OR

```
switch(config)#username <> {password | secret } <>
switch(config)#line VTY <>
switch(config-line)#login local
switch(config-line)#exit
```



3 – Privilege Mode Security

```
switch(config)#enable {password | secret } <>
```

نکته۱: 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 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
```

یعنی شما میتوانید تمام این۱۵ پورت را فعال کنید که با این کار ۱۵ نفر در یکزمان میتوانند وارد روتر یا سوئیچ شوند.

نکته۲: سوئیچ چون لایه دو هستش و اینکه در این لایه IP تعریف نشده است پس ما نمیتوانیم به interfaceهای physical آیپی اختصاص بدیم. به همین خاطر به سراغ اینترفیس Logical (interface vlan<>)میرویم. (به صورت پیش این اینترفیس(vlan1) روی سوئیچ‌ها وجود دارد که پیش فرض خاموش می‌باشد.)

نکته۳: دستور show interface status برای دیدن وضعیت اینترفیس‌های فیزیکال است. برای اینکه وضعیت اینترفیس های لاجیکال هم مشاهده شود باید از دستور show ip interface brief استفاده کنیم.

```
SWT_TEH#show ip interface brief
Interface              IP-Address      OK? Method Status                Protoc
FastEthernet0/1        unassigned      YES manual up                    up
FastEthernet0/2        unassigned      YES manual down                  down
FastEthernet0/3        unassigned      YES manual down                  down
FastEthernet0/4        unassigned      YES manual down                  down
FastEthernet0/5        unassigned      YES manual down                  down
FastEthernet0/6        unassigned      YES manual down                  down
FastEthernet0/7        unassigned      YES manual down                  down
FastEthernet0/8        unassigned      YES manual down                  down
FastEthernet0/9        unassigned      YES manual down                  down
FastEthernet0/10       unassigned      YES manual down                  down
FastEthernet0/11       unassigned      YES manual down                  down
FastEthernet0/12       unassigned      YES manual down                  down
FastEthernet0/13       unassigned      YES manual down                  down
FastEthernet0/14       unassigned      YES manual down                  down
FastEthernet0/15       unassigned      YES manual down                  down
FastEthernet0/16       unassigned      YES manual down                  down
FastEthernet0/17       unassigned      YES manual down                  down
FastEthernet0/18       unassigned      YES manual down                  down
FastEthernet0/19       unassigned      YES manual down                  down
FastEthernet0/20       unassigned      YES manual down                  down
FastEthernet0/21       unassigned      YES manual down                  down
FastEthernet0/22       unassigned      YES manual down                  down
FastEthernet0/23       unassigned      YES manual down                  down
FastEthernet0/24       unassigned      YES manual down                  down
GigabitEthernet0/1     unassigned      YES manual down                  down
GigabitEthernet0/2     unassigned      YES manual down                  down
Vlan1                  192.168.1.100   YES manual up                    up
```

```
SWT_TEH#show interfaces status
Port      Name               Status       Vlan       Duplex  Speed Type
Fa0/1                        connected    1          auto    auto  10/100BaseTX
Fa0/2                        notconnect   1          auto    auto  10/100BaseTX
Fa0/3                        notconnect   1          auto    auto  10/100BaseTX
Fa0/4                        notconnect   1          auto    auto  10/100BaseTX
Fa0/5                        notconnect   1          auto    auto  10/100BaseTX
Fa0/6                        notconnect   1          auto    auto  10/100BaseTX
Fa0/7                        notconnect   1          auto    auto  10/100BaseTX
Fa0/8                        notconnect   1          auto    auto  10/100BaseTX
Fa0/9                        notconnect   1          auto    auto  10/100BaseTX
Fa0/10                       notconnect   1          auto    auto  10/100BaseTX
Fa0/11                       notconnect   1          auto    auto  10/100BaseTX
Fa0/12                       notconnect   1          auto    auto  10/100BaseTX
Fa0/13                       notconnect   1          auto    auto  10/100BaseTX
Fa0/14                       notconnect   1          auto    auto  10/100BaseTX
Fa0/15                       notconnect   1          auto    auto  10/100BaseTX
Fa0/16                       notconnect   1          auto    auto  10/100BaseTX
Fa0/17                       notconnect   1          auto    auto  10/100BaseTX
Fa0/18                       notconnect   1          auto    auto  10/100BaseTX
Fa0/19                       notconnect   1          auto    auto  10/100BaseTX
Fa0/20                       notconnect   1          auto    auto  10/100BaseTX
Fa0/21                       notconnect   1          auto    auto  10/100BaseTX
Fa0/22                       notconnect   1          auto    auto  10/100BaseTX
Fa0/23                       notconnect   1          auto    auto  10/100BaseTX
Fa0/24                       notconnect   1          auto    auto  10/100BaseTX
Gig0/1                       notconnect   1          auto    auto  10/100BaseTX
Gig0/2                       notconnect   1          auto    auto  10/100BaseTX
```

نکته٤: برای دیدن اطلاعات لایه دو و لایه سه اینترفیس لاجیکال (vlan1) به ترتیب از دستورات show interface vlan1 و show ip interface vlan1 استفاده میکنیم.

```
SWT_TEH#sh int vlan1
Vlan1 is up, line protocol is up
  Hardware is CPU Interface, address is 000c.cfa4.d880 (bia 000c.cfa4.d880)
  Internet address is 192.168.1.100/24
  MTU 1500 bytes, BW 100000 Kbit, DLY 1000000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 21:40:21, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); 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
     1682 packets input, 530955 bytes, 0 no buffer
     Received 0 broadcasts (0 IP multicast)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     563859 packets output, 0 bytes, 0 underruns
     0 output errors, 23 interface resets
     0 output buffer failures, 0 output buffers swapped out
```

```
SWT_TEH#show ip int vlan1
Vlan1 is up, line protocol is up
  Internet address is 192.168.1.100/24
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Outgoing access list is not set
  Inbound  access list is not set
  Proxy ARP is enabled
  Local Proxy ARP is disabled
  Security level is default
  Split horizon is enabled
  ICMP redirects are always sent
  ICMP unreachables are always sent
  ICMP mask replies are never sent
  IP fast switching is disabled
  IP fast switching on the same interface is disabled
  IP Null turbo vector
  IP multicast fast switching is disabled
  IP multicast distributed fast switching is disabled
  IP route-cache flags are None
  Router Discovery is disabled
  IP output packet accounting is disabled
  IP access violation accounting is disabled
  TCP/IP header compression is disabled
  RTP/IP header compression is disabled
  Probe proxy name replies are disabled
  Policy routing is disabled
  Network address translation is disable
  WCCP Redirect outbound is disabled
  WCCP Redirect inbound is disabled
  WCCP Redirect exclude is disabled
  BGP Policy Mapping is disabled
```

نکته۵: معمولا IP تلنت و ssh را به صورت دستی تنظیم میکنند و از dhcp دوری میکنند، چون نیاز است ip ثابت بماند.

نکته٦: هر اینترفیس سوئیچ،چه فیزیکال و چه لایجال، دارای مک آدرس مجزاست.

نکته۷: telnet به دلیل clear textبودن، مورد استفاده قرار نمیگرد و ssh جایگزین آن است.

(BB) SSH

یکی از بهترین مکانیزم‌های اتصال به سوئیچ های سیسکو به‌کارگیری یک حالت ایمن و اتصال بر مبنای پروتکل رمزنگار SSH است. مزیت روش فوق در مقایسه با تلنت Telnet در این است که اطلاعات به شکل رمزنگاری شده مبادله می‌شوند. در نتیجه اگر هکری موفق شود به هر شکل ممکن (نفوذ به شبکه بر مبنای بردار حمله مرد میانی) به شبکه نفوذ کند، دیگر قادر نخواهد بود اطلاعات را در قالب یک متن ساده مشاهده کند. پروتکل SSH در حالت پیش‌فرض از پورت ۲۲ استفاده می‌کند.

مراحل دسترسی به سوییچ از طریق ssh :

۱. تنظیم IP و Subnet maskمدیریتی (+ No shutdown کردن vlan مدنظر)

۲. یک) ساخت نام کاربری و گذرواژه دو) تنظیم پیکربندی Line VTY

۳. Enable password

٤. تنظیم نام دستگاه (switch(config)#hostname) و نام دامنه (myswitch(config)# ip domain-name meti.com) (ثبت بودن یا نبودن دامنه اهمیت ندارد.)

۵. ساخت کلید RSA (myswitch(config)# crypto key generate rsa) (سایز کلید میتواند بین ۳٦۰ الی ۲۰٤۸ باشد، که به صورت پیش فرض این مقدار ۵۱۲ تعریف شده که قابل تغییر میباشد.)

```
SWT_TEH(config)#crypto key generate ?
  rsa  Generate RSA keys
SWT_TEH(config)#crypto key generate rsa
The name for the keys will be: SWT_TEH.ccna.com
Choose the size of the key modulus in the range of 360 to 2048 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [512]:
```

SSH Configuration :

1 – IP address Assignment

```
switch(config)#interface vlan <>
switch(config-if)#ip address <IP> <Subnet Mask>
switch(config-if)#no shutdown
switch(config-if)#exit
```

2 – User Mode Security ➔ Line VTY

```
switch(config)#username <> {password | secret } <>
switch(config)#line VTY <>
switch(config-line)#login local
switch(config-line)#exit
```

3 – Privilege Mode Security

```
switch(config)#enable {password | secret }  <>
```

4 – Hostname Configuration

```
switch(config)#hostname <>
```

5 – Domain name Configuration

```
switch(config)#ip domain-name <>
```

6 – RSA Key generation Configuration

```
switch(config)#crypto key generate rsa
```

Show user
Show ip ssh
Show ssh

نکته: برای دیدن userهایی که به دستگاه متصل شدن از دستور show user در محیط enable استفاده میشود.

نکته: برای بدست آوردن اطلاعاتی همچون مدت زمان timeoutیوزر در حالت Ssh، از دستور show ip ssh استفاده می شود.

نکته : اگر بخواهیم مشخص کنیم کدام یوزرها از ssh و کدام یوزرها از telnet استفاده کنند، درsubmod line vty از دستور Tranport input استفاده میکنیم. (پیش فرض روی All(هم sshهم telnet) می‌باشد.)

```
SWT_TEH(config-line)#transport input ?
  all      All protocols
  none     No protocols
  ssh      TCP/IP SSH protocol
  telnet   TCP/IP Telnet protocol
```

Cisco Memory Types - Storing Switch Configuration Files :

انواع حافظه دستگاه‌های سیسکو به ترتیب زیر است:

۱ :**RAM(Random Access Memory)**- حافظه فرار RAM که نام دیگر آن حافظه ی Running Config است ، حافظه ای در سیسکو است که دارای سرعتی بسیار بالا است ، وظیفه این حافظه ذخیره فایل Running – Configuration است . به این معنی که تمامی Configuration تعریف شده برای دستگاه ، در فایلی به نام Running – Configuration ، که داخل رم قرار دارد ، ذخیره می شود .

باید دانست امکان از بین رفتن این حافظه با restart شدن سیسکو وجود دارد ، این اتفاق مشابه اتفاقی است که با قطع شدن برق برایRAM میافتد. از RAM برای نگهداری تنظیمات زمانیکه دستگاه در حال روشن شدن است به عنوان یک حافظه موقت می توان استفاده کرد .

برای دیدن محتویات این حافظه ازدستور Show Running config در محیط Enable استفاده می کنیم.

۲ :**Nv RAM(Non-Volatile Random Access Memory)** - حافظه غیرفرار و ماندگار است، خودش در غالب فایل Config.text داخل Flashذخیره می‌شود، فقط چون در قالب یک حافظه جداگانه در حافظه RAM بالا می‌آید، به آن Nv RAM گفته می‌شود. نام دیگر حافظه NV-RAM ، حافظه Start-up Config است . Configuration ها و پس ازذخیره در Running Configuration در پایان کار و همچنین تنظیمات پیشفرض دستگاه(مثل shut بودن اینترفیس‌های روتر و ...) بر روی Start-up Configuration ریخته می شوند تا برای همیشه ذخیره شوند و از بین نروند . تفاوت عمده Ram و nvRam که میتوان اشاره کرد این است که با شروع دوباره (restart) و یا قطع برق اطلاعات از بین نمیرود . با دستور **Show startup-config** در محیط Enable می توانیم محتویات آن را ببینیم. برای انتقال حافظه RAM به NVRAM از دو دستور زیر در محیط Enable استفاده می کنیم:

Copy Running-Config Startup-Config

یا

Write

```
Switch#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
```

```
Switch#write
Building configuration...
[OK]
```

برای پاک کردن حافظه نیز در محیط Enable از دستور زیر استفاده میکنیم:

#erase startup-config

```
Router#erase startup-config
Erasing the nvram filesystem will remove all configuration files! Continue?
[confirm]
[OK]
Erase of nvram: complete
%SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram
Router#reload
Proceed with reload? [confirm]
```

۳ :**ROM(Read Only Memory)** - حافظه ای است فقط خواندنی و البته دائمی. در دستگاه‌ها Cisco، ROM بوت شدن دستگاه را برعهده دارد و مشخصات دستگاه و پارامترهای Boot دستگاه را نشان می‌دهد ، در واقع نشان می‌دهد که IOS دستگاه چیست و از کجا باید شروع به Load شدن کند. در قسمت های زیر وجود دارد :

-POST (Power On Self-Test): وظیفه آن تست قسمت های سخت افزاری و اصلی دستگاه است.

-Boot Strap Programتوسط Register Number ، مراحل بوت دستگاه را مشخص می کند . ابتدا به سراغ فلش می رود و IOS را بوت می کند و داخل RAM می ریزد . سپس به سراغ NV RAM می رود و Start-up Config را که کانفیگ های اولیه دستگاه است را داخل رم میریزد و دستگاه شروع به کار می‌کند.

- ROM Monitor: IOS کوچکی است که در مواقع ضروری امکان انجام کارهای مدیریتی را محدودی می‌کند . به طور مثال در زمان فراموشی رمز عبور دستگاه.

- RxBoot : با استفاده از دستورات این قسمت میتوانید یک IOS جدید نصب کنید.

٤ :**Flash** - مثل فلش‌های معمولی است که داخل دستگاه قرار داده شده است. در Router های Cisco می‌توانیم این فلش را بیرون بیاوریم که با این کار، سیستم بدون سیستم عامل (IOS) می‌شود. حافظه فلش شامل Image کاملی از سیستم عامل (IOS) می باشد. به کمک این حافظه شما می توانید سیستم عامل روتر خود را تغییر و یا ارتقا بدهید در ضمن محتویات این حافظه با خاموش شدن دستگاه پاک نمی شود و ثابت باقی می ماند. با دستور Show Flash میتوانیم محتویات فایلهای flash را ببینیم.

```
Switch#show flash:
Directory of flash:/

    1  -rw-     4414921          <no date>  c2960-lanbase-mz.122-25.FX.bin
    2  -rw-        1076          <no date>  config.text

64016384 bytes total (59600387 bytes free)
```

نکته۱: وقتی که به دستگاه وصل می‌شویم و می‌خواهیم شروع به کار کردن با IOS کنیم چیزی جلوی ما قرار می‌گیرد به نام CLI که از طریق آن می‌توانیم دستورهای مربوط به دستگاه را بنویسیم، هر کاری که در این محیط انجام می‌دهیم، داخل Running Config اتفاق می‌افتد که دستورات را اجرا می‌کند. اما اگر دستگاه را خاموش و روشن کنیم این حافظه از بین می‌رود، مگر اینکه دستورات را در فایلی به نام Config.text ذخیره کنیم. این فایل داخل Flash ذخیره می‌شود، هر بار که دستگاه بالا می‌آید محتویات این فایل را روی حافظه RAM لود می‌کند و در Running config نمایش داده می‌شود.

نکته۲: همچنین برای مشاهده اطلاعات سخت افزاری و نرم افزاری دستگاه روتر و سوئیچ سیسکو میتوان از دستورالعمل زیر استفاده کرد:

router> show version

Memory	Volatile / Non-Volatile	Stores
RAM	Volatile	• Running IOS • Running configuration file • IP routing and ARP tables • Packet buffer
ROM	Non-Volatile	• Bootup instructions • Basic diagnostic software • Limited IOS
NVRAM	Non-Volatile	• Startup configuration file
Flash	Non-Volatile	• IOS • Other system files

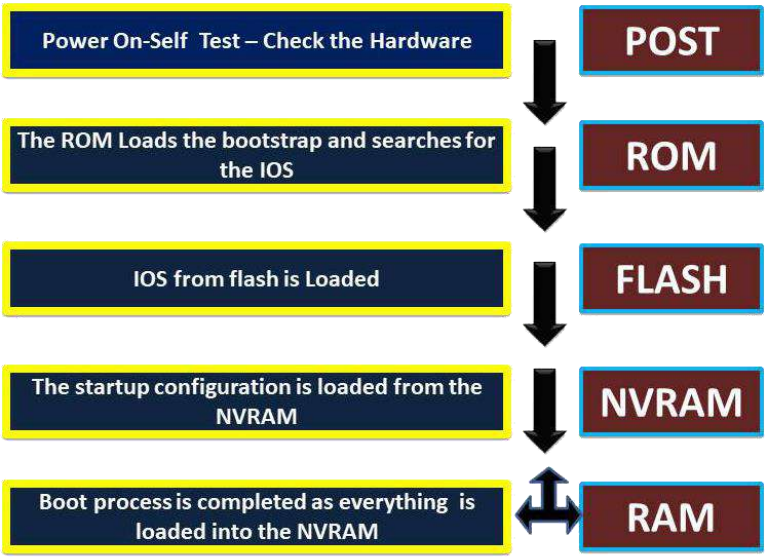
Cisco boot steps :

۱. Power همانند یک سیستم معمولی کامپیوتری، روتر و سوئیچ به محض روشن شدن، فرآیند POST که مخفف Power On Self-Test است را انجام می دهدPOST .تمامی سخت افزارهای موجود بر روی دستگاه را تست می کند و از صحت عملکرد آنها اطمینان حاصل میکند.

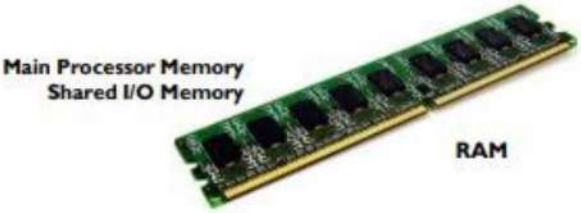
۲. در مرحله بعدی برنامه bootstrap که در ROM ذخیره شده است باید سیستم عامل IOS را از Image ای که در حافظه Flash یا سرور TFTPوجود دارد Load کند.

۳. بعد از اینکه ios سیستم boot شد، تنظیمات پیش فرض(مثل: سرعت، خاموش روشن بودن پورت ها و ...) و config ذخیره شده در حافظه غیر فرارnvram (اصلاحاً starup config) قرار دارد ، باید در حافظه فرارRam(اصلاحاًrunning config) قرار بگیرد.

۴. زمانیکه Startup Configuration بصورت کامل Load شد ، IOS به شما خط فرمان User Mode را نمایش می دهد.



نکته: طبیعتاً سوئیچ و روتر تازه به کارگیری شده، startup config خالی است، ولی running config با آمدن پیش فرض های دستگاه از nvram به Ram محتوای پیش فرض را نشان میدهد.



Types of modes :

سوئیچ از انواع مد استفاده می‌کند که دقیقاً شبیه به روتر است و هیچ فرقی با روتر ندارد. (به دلیل سطح دسترسی، امنیت، ویژگی های زیر لایه‌ها)

User Mode (User EXEC Mode) :

این مد اولین مدی است که وارد روتر و سوئیچ میشویم و سطح دسترسی آن بسیار محدود است. تمامی سه روش نحوه اتصال به محیط CLI (Telnet, SSH, Console)، کاربر را به این مد منتقل می‌کند و بیشتر برای Monitoring و Trouble

shooting استفاده میشود. در این سطح، به کاربر اجازه داده می‌شود که برخی از تنظیمات اعمال شده را مشاهده کند ولی نمی‌تواند چیزی را تغییر دهد. وقتی وارد سوئیچ میشوید، خط فرمان به صورت زیر مشاهده میشود:

```
Switch>
```

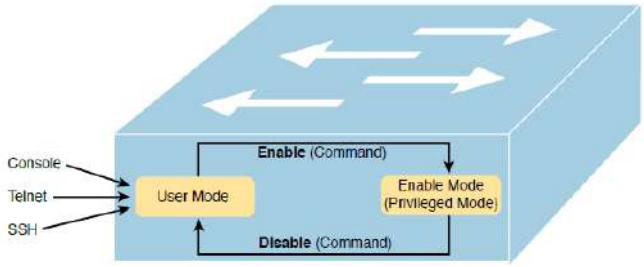
Enable Mode (Privileged Mode or User EXEC Mode) :

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

```
Switch>
switch> enable
Switch# disable
Switch>
```

در این مُد همه دستورات user mode موجود است بعلاوه چندین دستور دیگر. همچنین چندین دستور مدیریتی مثل reload داریم.

در این مُد برای Monitoring و Trouble shooting بشدت استفاده میشود.



Configuration Mode (Global Mode):

این مد دارای مجوز دسترسی بالایی است و پیکربندی(config) دستگاه از این مد و زیرسطح های آن استفاده می‌شود.به همین خاطر وقتی وارد این مد میشوید، میتوانید تمام تنظیمات سوئیچ را دردست بگیرید و آنها را تغییر دهید. برای ورود به آن، باید از طریق مد Privileged اقدام کنید:

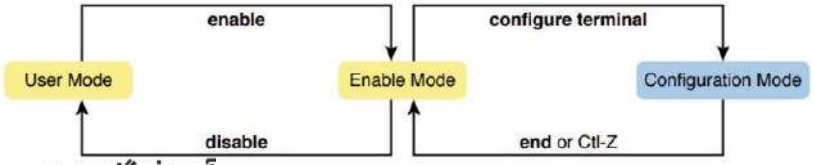
```
Switch>
switch> enable
Switch# Configure Terminal
Switch(config)# exit
Switch#
```

-در این مُد دیگر دستورات Monitoring و Trouble shooting نداریم و دستورات صرفا برای Config دستگاه میباشد.

- برای برگشت به مدهای قبلی ازctl-z یا ctl-c یا exit استفاده می‌شود.

- دستوراتی که در configuration mode اجرا می‌شوند، فایل پیکربندی حال حاضر سوئیچ را بروزرسانی می‌کنند. این تغییرات بر روی پیکربندی، زمانی اعمال می‌شوند که شما کلید Enter را فشار دهید. زمانی که یک دستور پیکربندی را وارد می‌کنید، مراقب باشید.

دستور عوض کردن نام دستگاه:



```
Router>ena
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname Zeljko
Zeljko(config)#
Zeljko#
```

نکته :در محیط Global اگر بخواهیم دستورات Enable mode را اجرا کنیم، کافیست قبل دستور از عبارت do استفاده کنیم. (دراین حالت auto complete و help نداریم ولی میتوانیم از حروف اول دستورات استفاده کنیم(به شرط اینکه آن حروف مشابه دیگری نداشته باشند(یونیک باشد).))

SWT_TEH(config)#do write or SWT_TEH(config)#do wri

زیرسطح‌های configuration mode و مفاد آن:

بهترین راه برای یادگیری زیرسطح‌ها، استفاده از آنها است. ولی ابتدا باید نگاهی به مثال‌های زیر داشته باشید. برای نمونه، دستور interface یکی از پرکاربردترین دستورات می‌باشد که با استفاده از آن، به یکی از زیرسطح‌های CLI منتقل می‌شویم. برای مثال، کاربر با وارد کردن دستور interface FastEthernet 0/1 در محیط CLI وارد زیرسطح اینترفیس می‌شود. زمانی که در این زیرسطح هستید، اگر از ? برای کمک استفاده کنید، تنها دستوراتی برای شما نمایش داده می‌شود که در پیکربندی اینترفیس‌ها کاربرد دارند. دستوراتی که در زیرسطح‌ها استفاده می‌شوند، زیر دستور یا subcommand نامیده می‌شوند، و در این مورد ویژه، زیردستورات اینترفیس نامیده می‌شوند.

```
Switch# configure terminal
Switch(config)# hostname Fred
Fred(config)# line console 0
Fred(config-line)# password hope
Fred(config-line)# interface FastEthernet 0/1
Fred(config-if)# speed 100
Fred(config-if)# exit
Fred(config)#
```

در مثال بالا موارد زیر نشان داده شده است:(جابه‌جایی مابین سطح‌های مختلف IOS)

انتقال از enable mode به global configuration mode با استفاده از دستور configure terminal

به کمک دستور hostname Fred در configuration mode ، نام دستگاه پیکربندی می‌شود.

انتقال از config mode به console line config mode با استفاده از دستور line console 0 (برای پیکربندی تنظیمات مربوط به پورت کنسول).

پیکربندی کلمه عبور ساده hope ، برای پورت کنسول (با استفاده از زیردستور password hope).

انتقال از console configuration mode به interface configuration mode با استفاده از دستور interface type number.

تنظیم سرعت ۱۰۰ Mbps برای اینترفیس Fa0/1 با استفاده از زیردستور speed 100

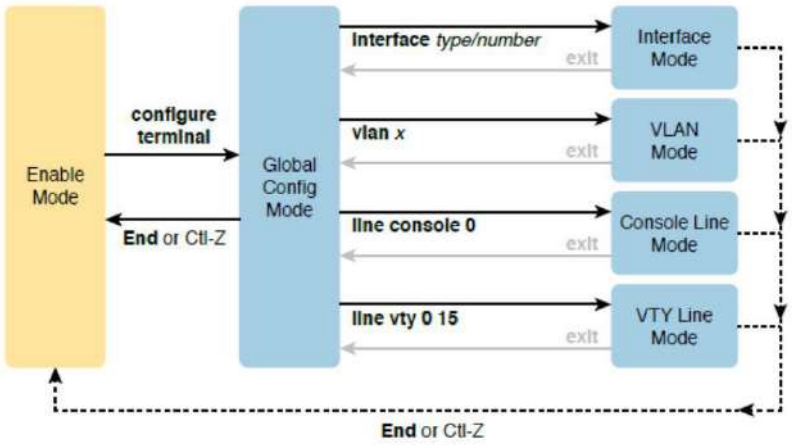
انتقال از interface configuration mode به global configuration mode با استفاده از دستور exit

نکته: در دستور interface در مد گلوبال، می‌توانیم برای هر اینترفیس یک اسم مجزا (دستورdescription) ، سرعت مجزا(دستورspeed) و نوع ارتباط (دستورduplex)تعریف کنیم.

```
Switch#show interfaces status
Port      Name               Status       Vlan       Duplex  Speed Type
Fa0/1     meti               notconnect   1          a-half  a-10  10/100BaseTX
Fa0/2                        notconnect   1          auto    auto  10/100BaseTX
Fa0/3                        notconnect   1          auto    auto  10/100BaseTX
Fa0/4                        notconnect   1          auto    auto  10/100BaseTX
Fa0/5                        notconnect   1          auto    auto  10/100BaseTX
```

کلمات داخل پرانتز در خط فرمان، نشان دهنده سطح یا زیرسطح جاری می‌باشد. برای مثال، زمانی که وارد configuration mode می‌شوید، ابتدا خط فرمان به (config) تغییر می‌کند، که به معنای این است که شما در global configuration mode هستید. سپس دستور line console 0 ، خط فرمان را به (config-line) تغییر می‌دهد. هر بار که خط فرمان به همراه زیرسطح تغییر می‌کند به این معنی است که شما به یک زیرسطح دیگر منتقل شده‌اید. جدول زیر پرکاربردترین خط فرمان‌ها در زیرسطح‌ها را نشان میدهد.

خط فرمان	نام زیرسطح	دستوراتی که برای ورود به این سطح نیاز است
hostname(config)#	Global	اولین سطح پس از زدن دستور configure terminal می‌باشد
hostname(config-line)#	Line	line console 0 line vty 0 15
hostname(config-if)#	Interface	interface typenumber
hostname(vlan)#	VLAN	vlan number



وارد و خارج شدن از سطح‌های مختلف IOS

نکته: روش هایی که به دستگاه سیسکویی می‌توان دسترسی داشت:

- ✓ CTYکه همان دسترسی از طریق کنسول می‌باشد.
- ✓ TTYدسترسی به کنسول از طریق Access Server است.
- ✓ VTYدسترسی به صورت Telnet و یا SSH است.
- ✓ AUXدسترسی از طریق مودم می‌باشد.

LAN Switch Interface Status Codes :

وضعیت و کدهای اینترفیس‌ها:

Disable : این پورت به صورت دستی توسط مدیر شبکه، shutdown شده است و کاری در شبکه انجام نمیدهد.

Connected : هم لایه یکی هم لایه دوئی برقرار است.

Not connected: این پورت فیزیکالی روشن است ولی چیزی به آن وصل نیست.

Err-disable: در مباحث آینده آشنا می‌شویم.

Line Status	Protocol Status	Interface Status	Typical Root Cause
administratively down	down	disabled	The **shutdown** command is configured on the interface.
down	down	notconnect	No cable; bad cable; wrong cable pinouts; speed mismatch; neighboring device is (a) powered off, (b) **shutdown**, or (c) error disabled.
up	down	notconnect	Not expected on LAN switch physical interfaces.
down	down (err-disabled)	err-disabled	Port security has disabled the interface.
up	up	connected	The interface is working.

Securing the Switch CLI (Local & Remote) :

۱. ایمن کردن **user mode** و **Privileged Mode** با رمزهای عبور ساده:

(**Securing User Mode and Privileged Mode with Simple Passwords**)

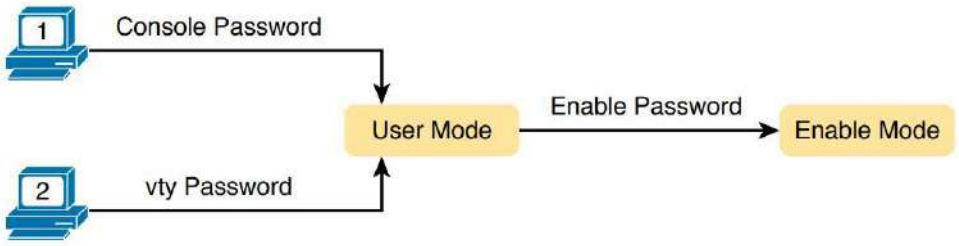


Figure 6-1 *Simple Password Security Concepts*

الف) ست کردن پسورد برای پورت کنسول **Console** (برای ورود به **user mode** بلافاصله بعد از زدن کابل **console**)

```
switch#configure terminal
switch(config)#line console <>
switch(config-line)#password <>
switch(config-line)#login
switch(config-line)#exit
switch(config)#
```

در صورتی که قصد دارید password را برای Line Console حذف کنید، در Line Console عبارت no password را تایپ کنید .

ب) اعمال رمزعبور برروی محیط **enable** (**Global**):

```
switch#configure terminal
switch(config)#enable {password | secret }  <>
```

نکته۱ : در اینجا ما به دو روش می توانیم پسورد را وارد کنیم، اگر بزنیم enable password پسورد به صورت رمز نشده در running config نمایش داده می شود و اگر از enable secret استفاده کنید پسورد شما به صورت یک متن هش(hash) شده و رمز شده نمایش داده می شود.پس اگر از تنظیمات show running-config بگیریم رمزهای password به صورت تکتس اصلی(Clear text) نشان داده میشود ولی secret با الگوریتم md5 کد شده هستند. البته به جای Secret میتوان از "password 5" استفاده کرد.

```
Switch# configure terminal
Switch(config)# enable secret love
!
! At Step 2 in the checklist, enter console configuration mode, set the
! password value to "faith" and enable simple passwords for the console.
! The exit command moves the user back to global config mode.
!
Switch#(config)# line console 0
Switch#(config-line)# password faith
Switch#(config-line)# login
Switch#(config-line)# exit
!
! The next few lines do basically the same configuration, except it is
! for the vty lines. Telnet users will use "hope" to login.
!
Switch#(config)# line vty 0 15
Switch#(config-line)# password hope
Switch#(config-line)# login
Switch#(config-line)# end
Switch#

Switch# show running-config
!
Building configuration...

enable secret 5 $1$OwtI$A58c2XgqWyDNeDnv51mNR.
!
interface FastEthernet0/1
!
interface FastEthernet0/2
!
! Several lines have been omitted here - in particular, lines for
! FastEthernet interfaces 0/3 through 0/23.
!
interface FastEthernet0/24
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
line con 0
 password faith
 login
!
line vty 0 4
 password hope
 login
!
line vty 5 15
 password hope
 login
```

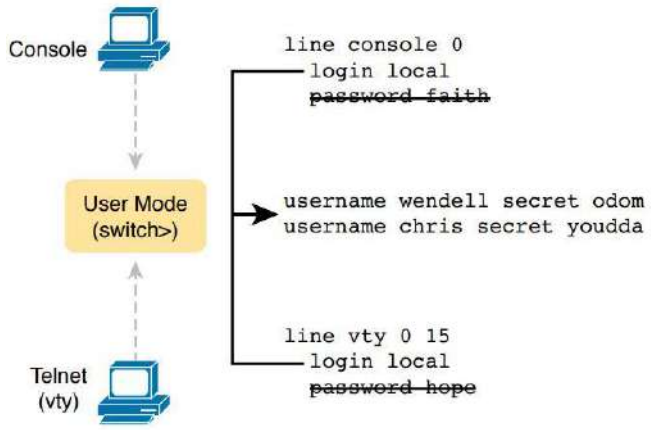
نکته۲: زمانی که از enable password و enable secret به صورت هم زمان استفاده میکنید، فقط enable secret کار میکند.

نکته۳: برای راه اندازی لاین های **Telnet**و **SSH**حتما می‌بایست برروی محیط enable رمز عبور اعمال نمایید.

۲. ایمن کردن دسترسی به **Usermode** با **usernames** و **Passwords** محلی:

(**Securing User Mode Access with Local Usernames and Passwords**)

الف) ست کردن username & password :



در این روش ما ابتدا username و password می‌سازیم و سپس به Line Console می‌گوییم کلمه و رمز عبور را از localسیستم تایید کند. هنگامی که قصد داریم برای هر کارمند یک username وpassword برای ورود به Line Console ایجاد کنیم از این روش استفاده می‌کنیم.

```
switch#configure terminal
switch(config)#username <> password <>
switch(config)#line console <>
switch(config-line)#login local
switch(config-line)#exit
switch(config)#
```

```
SW2# telnet 10.9.9.19
Trying 10.9.9.19 ... Open


User Access Verification

Username: wendell
Password:
SW1> enable
Password:
SW1# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SW1(config)#^Z
SW1#
*Mar 1 02:00:56.229: %SYS-5-CONFIG_I: Configured from console by wendell on vty0
(10.9.9.19)
```

- **جهت غیرفعال کردن** نیز به ابتدای Login Local یک No اضافه می‌کنیم.

```
Switch(config)#line console 0
Switch(config-line)#no login local
Switch(config)#exit
```

۳. ایمن کردن دسترسی به **Usermode** با سرورهای احراز هویت خارجی:

(Securing User Mode Access with External Authentication Serverss)

وقتی تعداد سوئیچ و روترها زیاد میشود، برای مدیریت یوزرنیم و پسوردها میتوانیم به جای استفاده از یک نام کاربری و رمز عبور از یک سرور با عنوان AAA که مخفف کلمات Authentication یا احراز هویت ، Authorization یا سطح مجاز دسترسی و Accounting یا قابلیت حسابرسی استفاده کنیم که بصورت مرکزی این سه عملیات را انجام خواهد داد .

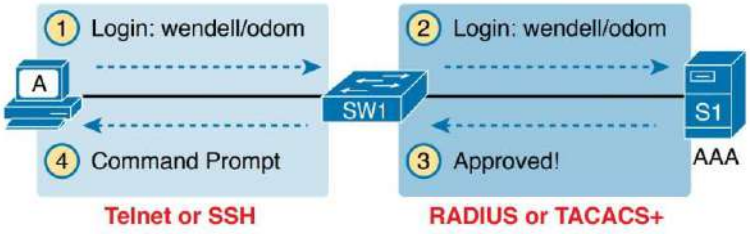


Figure 6-4 *Basic Authentication Process with an External AAA Server*

با استفاده از سرور AAA برای احراز هویت، سوئیچ (یا روتر) به سادگی پیامی را به آن ارسال می کند. از سرور AAA سوال می کند که آیا نام کاربری و رمز عبور مجاز است یا خیر، و سرور AAA پاسخ می دهد.
سوئیچ و سرور AAA معمولاً از پروتکل RADIUS یا TACACS+ استفاده می‌کنند که هر دو رمز عبور را هنگام عبور از شبکه رمزگذاری می‌کنند.

٤. ایمن سازی دسترسی از راه دور با **Secure Shell** :

(Securing Remote Access with Secure Shell)

نکته۱: در صورتی که از دستور زیر استفاده کنید، با استفاده از رمزنگاری معروف به type 7 تمام پسوردهای رمز نشده ما را رمزنگاری می‌کند. حتی رمز دستورات enable password و line console

Switch(config)#service password-encryption

نکته۲: زمانیکه وارد یک مد میشوید، اگر مدت زمانی با روتر یاسوئیچ کار نکنید، در هر مدی که هستید، خارج شده و به مد اول، یعنی UserMode برگشت میکند، برای تغییر زمان این حالت دستور exec-timeout را اعمال میکنیم(درون<> باید مدت زمان گذاشت). برای جلوگیری از این کار(یعنی تبدیل به زمان بی نهایت)، باید در انتهای این دستور 00 (اولی برای دقیقه و دومی برای ثانیه است) قرار دهیم.

swtich (config-line)# exec-timeout <>

نکته۳: 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 پورتConsole از دستور logging synchronous استفاده کنید.

```
swtich (config-line)# logging synchronous
```

نکته۴: یکی از راه‌های جرم‌یابی یوزرنیم‌ها استفاده از دستور زیر است. این دستور به ما ۱۰(قابل تغییر است) دستور اخیر این یوزر لیست میکند.

```
switch#show history
```

دستور زیر هم تمامی کاربرانی که به روتر یا سوئیچ متصل شده‌اند را نمایش می‌دهد:

```
Switch#show users
    Line       User       Host(s)              Idle       Location
*  0 con 0     ali        idle                 00:00:00

  Interface    User               Mode         Idle     Peer Address
```

دستور سطح دسترسی یوزرها :

۰ تا ۱۵ سطح دسترسی داریم که هر که سطح دسترسی بالاتر میرود میزان دسترسی به سطوح CLI بیشتر است. میزان این سطح دسترسی‌ها قابل تغییر هستند و می‌شود برای هر عدد(۰-۱۵) تعریف کرد(مانند شکل زیر).

```
Switch(config)#username meti pr
Switch(config)#username meti privilege ?
  <0-15>  User privilege level
Switch(config)#username meti privilege 15 pas
Switch(config)#username meti privilege 15 password 123456
Switch(config)#
Switch(config)#us
Switch(config)#username jafar pr
Switch(config)#username jafar privilege 0 pas
Switch(config)#username jafar privilege 0 password 123456
```

```
Switch(config)#privilege conf
Switch(config)#privilege configure l
Switch(config)#privilege configure level ?
  <0-15>  Privilege level
Switch(config)#privilege configure level 10
```

The difference between Hashing and Encryption:

Swh-1(config)#service password-encryption	type7
Swh-1(config)#username Ali Secret Ali	secret=type5(MDF)
Swh-1(config)#username Ahmad password 8 ahmad	8=type8

رمز Type5

این روش پسورد و رمزگذاری سوئیچ سیسکو در حدود سال ۱۹۹۲ معرفی شد. این روش از یک الگوریتم هش بسیار ساده خلاصه پیام (Message-Digest 5) MD5 اســتفاده میکند که قابلیت تکرار ۱۰۰۰ MD5 تا ۳۲ بیت را دارد. با این حال الگوریتم MD5مورد تایید مو سسه ملی فناوری و ا ستانداردها آمریکا (NIST) نیست. با این حال ا ستفاده از رمز Type5 زمانی تو صیه میشود که سخت افزار سیستم از نرم افزارها و قابلیت رمزگذاری ۶،۸ و یا ۹ پشتیبانی نمی‌کند.

رمز Type7

این روش از یک جانشین الفبایی ساده رمز Vigenere با یک کلید سخت کد و شناخته شده عمومی استفاده میکند. این روش را میتوان با استفاده از ابزارهای موجود در اینترنت بلافاصله تبدیل به یک متن ساده کرد. همچنین رمزهای عبور در این مدل به صورت رشته‌های رمزگذاری شده در فایل پیکربندی ذخیره می‌شوند. NSA اکیدا توصیه میکند از نوع ۷ استفاده نکنید.

رمز Type8

با توسعه سیستم عامل‌های سیسکو پس از سال ۲۰۱۳، مدل Type8 را می‌توان نسخه‌ی ارتقا یافته‌ی Type4دانست. گذرواژه‌های نوع ۸ با تابع استخراج کلید، مبتنی بر رمز عبور نسخه an 80bit-salt2 ، SHA-256 ، PBKDF2 ، ۲۰،۰۰۰ تکرار هش عمل می‌کنند که در مقایسه با انواع رمزهای قبلی، ایمن‌تر هستند. و همچنین پسوردها به صورت هش در فایل پیکربندی ذخیره میشوند.

Table: Cisco password types

Password type	Ability to crack	Vulnerability severity	NSA recommendation
Type 0	Immediate	Critical	**Do not use**
Type 4	Easy	Critical	**Do not use**
Type 5	Medium	Medium	Not NIST approved, use only when Types 6, 8, and 9 are not available
Type 6	Difficult	Low	Use only when reversible encryption is needed, or when Type 8 is not available
Type 7	Immediate	Critical	**Do not use**
Type 8	Difficult	Low	**Recommended**
Type 9	Difficult	Low	Not NIST approved

CLI Help Features:

جدول زیر به طور خلاصه قابلیت کمک گرفتن هنگام تایپ دستور موجود در CLI را نشان می‌دهد. توجه داشته باشید که در ستون اول، " command" نشانگر هر دستوری است. به همین ترتیب، " parm" نیز نشانگر پارامتر مربوط به دستور است. برای مثال، در سطر دوم command ? نوشته شده است، که به این معنی است که دستوراتی مانند show? و copy? تایپ شوند، در ادامه لیستی نمایش داده می‌شود که در آن دستوراتی که می‌توانند در ادامه تایپ شوند، را نشان می‌دهد.

چیزی که تایپ می‌کنید	کمکی که به شما می‌شود
?	کمک برای تمامی دستورات موجود در سطح جاری را نمایش می‌دهد.
command ?	با یک فاصله میان ? و command، سوئیچ لیستی از تمامی پارامترهای اول مربوط به دستور را نمایش می‌دهد.
com?	تمامی دستوراتی که با com شروع می‌شوند را نمایش می‌دهد.
command parm?	تمامی پارامترهایی که با نیمه‌ی تایپ شده، شروع می‌شوند، را نمایش می‌دهد. (توجه کنید که فاصله‌ای میان param و ? نیست.)
command parm«Tab»	با فشردن کلید Tab از روی صفحه کلید، IOS مابقی پارامتر را به صورت اتوماتیک تایپ می‌کند. با این فرض که از یک دستور یا پارامتر به اندازه‌ای تایپ شده که با سایر دستورات تداخل نداشته باشد.
command parm1	اگر یک فاصله قبل از علامت ? باشد، CLI لیستی از پارامترهای بعدی موجود را نمایش می‌دهد.

زمانی که علامت سوال را وارد می‌کنید، IOSد ستگاه بیدرنگ واکنش ن شان داده و نیازی نی ست که شما کلید Enter یا کلیدهای دیگر را ف شار دهید. اطلاعاتی که توسط ابزار کمک، نمایش داده می شود، نسبت به سطح جاری متغیر می‌باشد. برای مثال، زمانی که در سطح user mode علامت سوال تایپ کنید، فقط دستوراتی که در user mode مجاز هستند برای شما نمایش داده می‌شود.

```
Router>?
Exec commands:
  <1-99>      Session number to resume
  connect     Open a terminal connection
  disable     Turn off privileged commands
  disconnect  Disconnect an existing network connection
  enable      Turn on privileged commands
  exit        Exit from the EXEC
  logout      Exit from the EXEC
  ping        Send echo messages
  resume      Resume an active network connection
  show        Show running system information
  ssh         Open a secure shell client connection
  telnet      Open a telnet connection
  terminal    Set terminal line parameters
  traceroute  Trace route to destination
```

```
Router>show ?
  arp           Arp table
  cdp           CDP information
  class-map     Show QoS Class Map
  clock         Display the system clock
  controllers   Interface controllers status
  crypto        Encryption module
  dot11         IEEE 802.11 show information
  flash:        display information about flash: file system
  frame-relay   Frame-Relay information
  history       Display the session command history
  hosts         IP domain-name, lookup style, nameservers, and host table
  interfaces    Interface status and configuration
  ip            IP information
  ipv6          IPv6 information
  lldp          LLDP information
  policy-map    Show QoS Policy Map
  pppoe         PPPoE information
  privilege     Show current privilege level
  protocols     Active network routing protocols
  queue         Show queue contents
  queueing      Show queueing configuration
  sessions      Information about Telnet connections
  ssh           Status of SSH server connections
  tcp           Status of TCP connections
  terminal      Display terminal configuration parameters
  users         Display information about terminal lines
  version       System hardware and software status
  vlan-switch   VTP VLAN status
  vtp           Configure VLAN database
```

```
Router>show  ip ?
  arp         IP ARP table
  bgp         BGP information
  dhcp        Show items in the DHCP database
  eigrp       IP-EIGRP show commands
  interface   IP interface status and configuration
  nbar        Network-Based Application Recognition
  ospf        OSPF information
  protocols   IP routing protocol process parameters and statistics
  rip         IP RIP show commands
  route       IP routing table
  ssh         Information on SSH
```

سیستم عامل IOS سیسکو دستوراتی که شما وارد می‌کنید در حافظه تاریخچه خود نگه می‌دارد، به صورت پیشفرض ۱۰ دستور آخر نگه داری می‌شود. CLI به شما این اجازه را می‌دهد تا این لیست را بررسی کرده و در صورت نیاز آن را تغییر دهید و سپس آن را مجدد بر روی سوئیچ اعمال کنید. این قابلیت به شما کمک می‌کند تا سرعت تایپ خود را افزایش دهید. (جدول زیر)

کلیدهای صفحه کلید	تاثیر کلید
کلید بالا یا Ctrl + P	آخرین دستور وارد شده را نمایش می‌دهد. اگر مجدد همین کلید را فشار دهید، دستور ماقبل آخرین دستور را خواهید دید، تا زمانی که حافظه آن به پایان رسد.
کلید پایین یا Ctrl + N	اگر در تاریخچه زیاد به عقب رفته‌اید، با این کلید می‌توانید به سمت جلو بروید و آخرین دستورات وارد شده را مشاهده کنید.
کلید چپ یا Ctrl + B	این کلید، نشانگر خط فرمان را به سمت عقب می‌برد و شما می‌توانید کاراکترهای قبلی را تغییر دهید بدون این که کاراکترهای جلویی را پاک کنید.
کلید راست یا Ctrl + F	این کلید، نشانگر خط فرمان را به سمت جلو می‌برد، بدون این که کاراکتری را پاک کنید.
کلید Backspace	با فشار دادن این کلید، در جایی که نشانگر خط فرمان قرار دارد، یک کاراکتر را پاک می‌کند.

: Techniques for writing commands in the CLI environment=======

- در هر Mode که باشیم با گرفتن ؟ می‌توانیم تمام دستورات آن Mode را ببینیم. مثلاً اگر بخواهیم ببینیم که چه دستوراتی با e شروع می شوند ?e را وارد می‌کنیم(قابلیت Auto complete).

- اگر قصد وارد کردن دستور Enable را داریم برای راحتی کار می‌توانیم ۲ کار انجام دهیم. یا en را وارد کرده و بعد Enter یا از En+Tab استفاده کنیم.(در دستورات به شرطی این قابلیت قابل استفاده است که آن دستور Unique باشد.)
- برای غیر فعال کردن یک future، قبل از هر دستوری No گذاشته می‌شود. مثلا برای روشن کردن یک interface قبل از کلمه shutdown عبارت no قرار میدهیم. No shut down .
- اگر دستوری را اشتباه بزنیم و ۲۵۵/۲۵۵/۲۵۵/۲۵۵ را ببینیم، این اعداد یعنی دستور وارد شده نامفهوم بوده و از طریق اینترنت در حال جستجو است و چون به اینترنت دسترسی ندارد آن را Broadcast کرده است، در این مواقع برای اینکه بتوانیم سریع‌تر از این حالت خارج شویم از ترکیب دکمه‌های Ctrl+Shift+6 استفاده می‌کنیم.

```
Switch#sdfsdg
Translating "sdfsdg"...domain server (255.255.255.255) % Name lookup aborted
```

برای غیر فعال کردن آن از دستور زیر استفاده میکنیم.

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

- اگر در یک سوئیچ Interface Fast Ethernet 0/1 داشته باشیم، عدد اول (صفر) همان شماره Module است و عدد دوم (یک) شماره Portاست. شماره Port در Switch از یک شروع می‌شود اما در Router از صفر شروع می‌شود.
- برای جابجایی پوینت (نقطه select شده) از کلیدهای جهت دار یا Arrow keys استفاده میشود چون موس قابل استفاده نیست.
- برای قرار گرفتن در انتها و ابتدای یک دستور به ترتیب از ctl+E و ctl+A استفاده میشود.

```
SWT_TEH#sh int vlan1
Vlan1 is up, line protocol is up
  Hardware is CPU Interface, address is 000c.cfa4.d880 (bia 000c.cfa4.d880)
  Internet address is 192.168.1.100/24
  MTU 1500 bytes, BW 100000 Kbit, DLY 1000000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 21:40:21, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); 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
     1682 packets input, 530955 bytes, 0 no buffer
     Received 0 broadcasts (0 IP multicast)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     563659 packets output, 0 bytes, 0 underruns
     0 output errors, 23 interface resets
     0 output buffer failures, 0 output buffers swapped out
```

MTU & MSS

در شبکه های Ethernet بیشترین(max) سایز(Size) بسته(Packet) لایه ۳ (که همانPDU است)، B۱۵۰۰ و در لایه ۲، ۱۵۱۸بایت میباشد که به آن MTU می گویند.

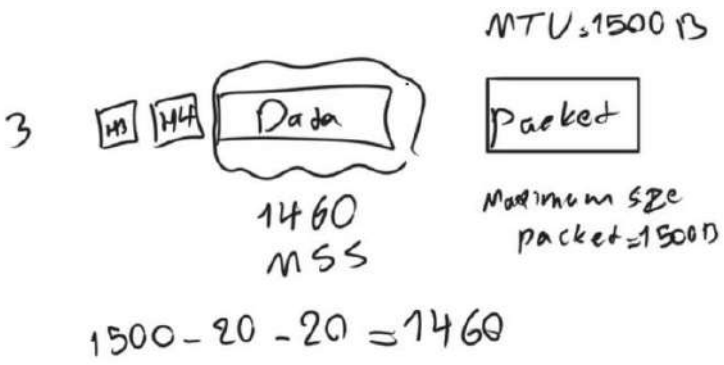
MTU (Maximum Transmission Unit): حداکثر اندازه واحد قابل انتقال یک بسته(Packet) بر روی یک لینک ارتباطی می باشد.

MSS (Maximum Segment Size): حداکثر سایزی که Data از لایه ٤ به لایه ٣ یا لایه سه به لایه دو می تواند وارد شود را گویند.

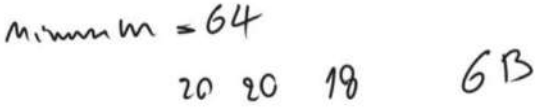
در مثال زیر اگر هدر لایه سه و لایه چهار را هر کدام در بیشترین حالت خود یعنی ٢٠ بایت در نظر بگیریم،MSS دیتا نمی‌تواند بیش از ١٤٦٠ بایت باشد.

MTU=H4+H3+data

MSS=MTU-H4-H3



نکته١: در لایه دو minimum MTU size ٦٤بایت می‌باشد. در این حالت نباید دیتا از ٦بایت کمتر باشد و اگر این حال پیش آید، با Padding یک مشت صفر و یک اضافه میکند که حجم دیتا به ٦ بایت برسد.



نکته٢: اگر بسته اطلاعاتی یا Packet ای اندازه ای بزرگتر از اندازه MTU داشته باشد، سیستم بصورت خودکار بسته را Fragment یا تکه تکه کرده و تبدیل به تکه های کوچکتر می کند و در قسمت های بعدی ارسال خواهد کرد .

نکته٣: MTU بطور دستی قابل تغییر است.

مثال محاسبه MTU مسیر google.com :

```
C:\Users\meti>ping google.com -l 1700 -f

Pinging google.com [216.239.38.120] with 1700 bytes of data:
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.
```

```
Pinging google.com [216.239.38.120] with 1466 bytes of data:
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.
```

```
Pinging google.com [216.239.38.120] with 1465 bytes of data:
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.
```

```
C:\Users\meti>ping google.com -l 1464 -f

Pinging google.com [216.239.38.120] with 1464 bytes of data:
Reply from 216.239.38.120: bytes=68 (sent 1464) time=95ms TTL=109
Reply from 216.239.38.120: bytes=68 (sent 1464) time=70ms TTL=109
Reply from 216.239.38.120: bytes=68 (sent 1464) time=71ms TTL=109
Reply from 216.239.38.120: bytes=68 (sent 1464) time=73ms TTL=109

Ping statistics for 216.239.38.120:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 70ms, Maximum = 95ms, Average = 77ms
```

Mss= 1464 این عدد یعنی میزان دیتای ورودی از لایه سه به لایه دو

MTU= 1464+H3(20) + (16 =پروتکل های مجزا مسیر) =1500

چون ping بسته icmp ارسال میکند، هدر لایه٤ نداریم چون در لایه ٣ کار میکند. به همین خاطر در محاسبات بالا از H4 استفاده نشد.

Interface Counters for Layer 1 Problems :

CRC: ممکن است ارتباطی داشته باشیم که loss Pocket داشته باشیم یا کند باشد یا Gitter یا Delay ، که CRC آن را نمایش می دهد. عمدتا مشکل فیزیکی است مثل خرابی cord Patch, panel Patch ، ماژول ، کانکتور ، کابل یا نویز مثل رد شدن سیم برق از کنار کابل شبکه.

هنگامی که با دستورات show به اطلاعات اینترفیس‌ها دست پیدا می‌کنیم، به عبارات زیر برمیخوریم:

- ✓ Runts: یعنی بسته‌هایی که در این اینترفیس منتقل می‌شوند کمتر از 64B است.
- ✓ Giants: یعنی بسته‌هایی که در این اینترفیس منتقل می‌شوند بیشتر از 1500B است. به فریم هایی که حجم آن از 1500B بیشتر باشد را jumbo frame میگویند .
- ✓ Throttles:
- ✓ Input error: مجموع اخطارهای این اینترفیس.
- ✓ Overrun: بسته‌هایی که مجدد ارسال شده‌اند.
- ✓ Jitter: در تمام شبکه‌ها تاخیر وجود دارد مخصوصا در شبکه‌هایWAN . معمولاً تاخیر ۱۰ میلی ثانیه بین بسته‌ها تاخیر خوبی است، اما جیتر بالا و افزایش این عدد به ۵۰ میلی ثانیه باعث سختی پردازش دیتا در کامپیوتر مقصد می‌شود.
- ✓ Delay: دیلی در شبکه یعنی زمانی که سیگنال لازم دارد در شبکه منتقل شود. این زمان هم می‌تواند ثابت باشد و هم متغیر. تعریف ساده تر : مدت زمانی که طول می‌کشد تا بسته از یک نقطه به نقطه دیگر برود.
- ✓ Packet loss: بسته های از دست رفته.

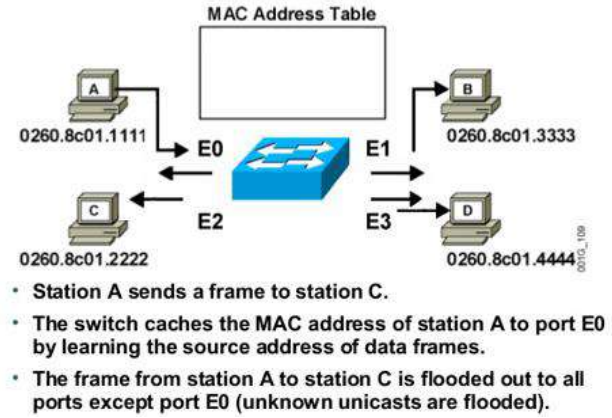
LAN Switching Concepts :

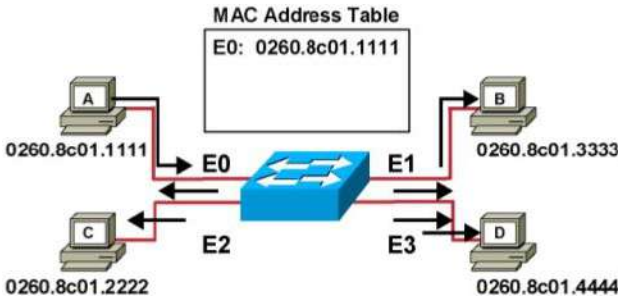
بررسی اجمالی منطق switching (Overview of Switching Logic) :

سوئیچ ها به طور کلی سه کار اساسی را انجام میدهند:

۱)سوئیچ‌ها بر اساس source mac-address، learning انجام می‌دهند. عمل Learning به بیان ساده یعنی اینکه کدام Mac در کدام پورت سوئیچ قرار گرفته تا بتواند ترافیک را از آن پورت عبور دهد.

زمانی که سوئیچ یک فریم را دریافت نمود، آدرس MAC فرستنده آن را با اطلاعات موجود در جدول MAC-Address مقایسه کرده و در صورت نبود مشابه آن، آدرس مزبور را به همراه شماره پورتی که فریم از راه آن پورت وارد سوئیچ شده است در جدول پورت خود ثبت خواهد کرد. اما اگر مشابه آدرس رسیده در جدول موجود باشد ،شماره پورت فریم رسیده با مورد موجود در جدول مقایسه خواهد شد که اگر تفاوتی مشاهده گردید، اطلاعاتی که در جدول وجود دارد به وسیله اطلاعات جدید به روز خواهند گردید.



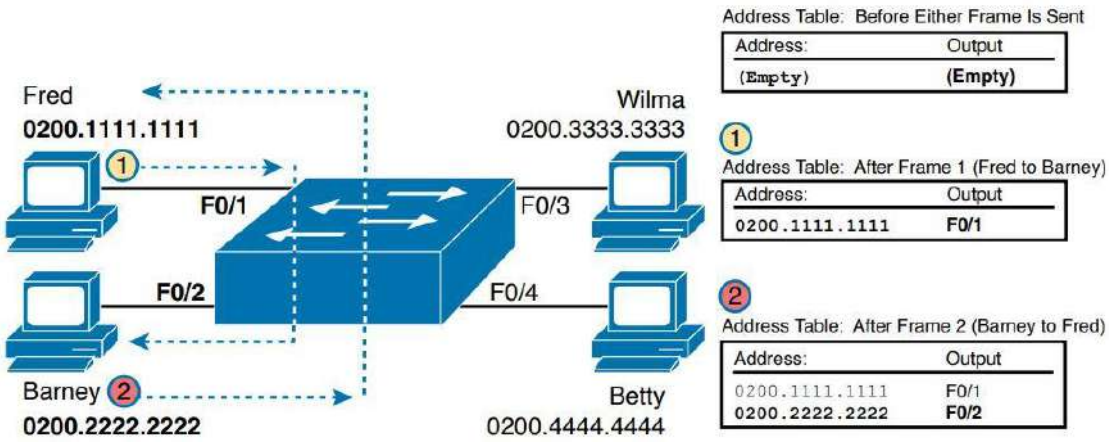


مثال۱: فرض کنید در ابتدا جدول MAC خالی است، بنابر این به محض دریافت اولین فریم توسط سوئیچ عمل Learning انجام می شود. به این صورت که فرض کنید کامپیوتر A می خواهد ترافیکی به سمت کامپیوتر C ارسال کند. اولین کاری که سوئیچ می کند عمل Learningاست! یعنی وقتی فریمی دریافت می کند، در جدول Mac خود از آن پورتی که فریم را دریافت کرده آنرادرجدول ثبت می کند. یعنی چون فریم را از پورت شماره E0 خود دریافت کرده است و اطلاعاتی از آن در جدول موجود نیست دو عمل اساسی انجام می دهد: مورد اول ابتدا آدرس مک ایستگاهی که برای سوئیچ ترافیک ارسال کرده است رادر جدول مک خود Cache می کند.

مورد دوم اینکه چون مقصد را در جدول خود یافت نمی‌کند ترافیک موردنظر را بر روی تمام پورت های خود Flood می‌کند (Broadcast میکند).

بدین ترتیب عملیات Learning انجام می‌شود. با این کار سوئیچ از این لحظه به بعد می داند که اگر ترافیکی دریافت کند که مقصد آن ۲۲۲۲.۳۳۳۳.۴۴۴۴ باشد باید آن را بر روی پورت ۲ خود ارسال کند.

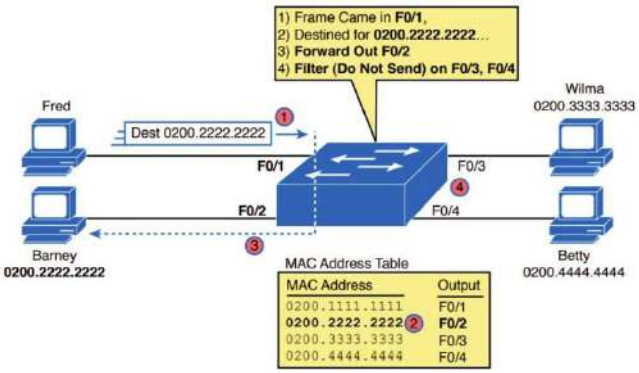
مثال۲(پروسه پر شدن mac address table) : در مثال زیر پورت F0/1 با مک 0200.1111.1111 قصد ارسال به پورت F0/2 با مک 0200.2222.2222 را دارد. سوئیچ در ابتدای کار با دریافت فریم از F0/1 مک آدرس Fred را در جدول مک آدرس ثبت میکند. بعد از پاسخ Barney سوئیچ از طریف پورت F0/2 متوجه مک 0200.2222.2222 میشود و آن را وارد جدول میکند.



۲) سوئیچ‌ها بر اساس Dst mac-address، Forwarding انجام می‌دهند. عمل Forwarding با فرض اینکه سوئیچ یک Mac Table دارد چگونه می تواند این عمل انتقال ترافیک از یک Port به یک Mac خاص را انجام دهد.

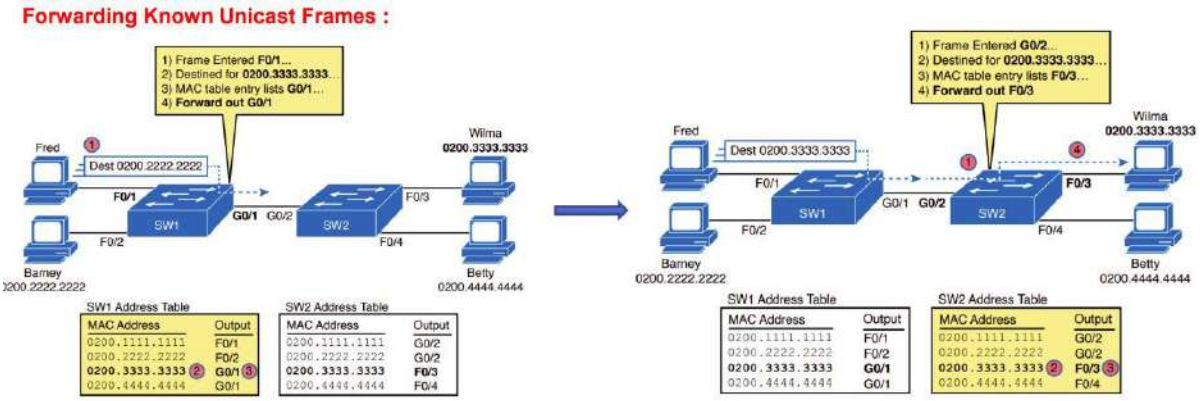
سوئیچ های اترنت، ۳ نوع فورواردینگ دارند:

یک) Know Unicast : در این حالت اطلاعات(مک و آیپی) مبدا و مقصد را میدانیم. همانطورکه از نامش مشخص است سوئیچ مقصد را با توجه به Mac Table خود می داند (اصطلاح Unicast یعنی مقصد یک ایستگاه می باشد).

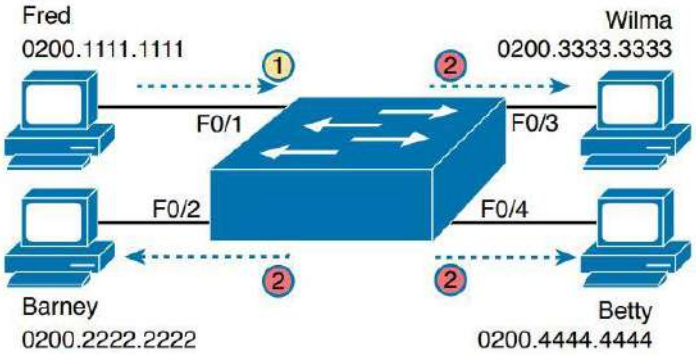


مثال۱: فرض کنید فریمی از F0/1 به سوئیچ می رسد که مقصد آن 0200.2222.2222 می باشد. با توجه به Mac Table سویچ آن را فقط به پورت F0/3 فوروارد می کند.

مثال۲:



دو) UnKnow Unicast : تصور کنید پورت F0/1 قصد ارسال به پورت F0/3 با مک آدرس 0200.3333.3333 را دارد. با این شرایط سوئیچ با این مسله مواجه می شود که فریمی دریافت کرده که آدرس مک آن را در جدول خود ندارد و نمی داند که مقصد آن کجاست! در چنین شرایطی سویچ فریم مورد نظر را به تمام پورت های خود فوروارد(Flood) می‌کند (غیر از آن پورتی که فریم را از آن دریافت کرده است)



Address Table: Before Frame Is Sent

Address:	Output
(Empty)	(Empty)

سه) Broadcast : در این حالت وقتی فریمی به سوئیچ برسد و آدرس مقصد آن ffff:ffff:ffff باشد همانند Unknow Unicast عمل کرده و آن را بر روی تمام پورت های خود Flood می کند.

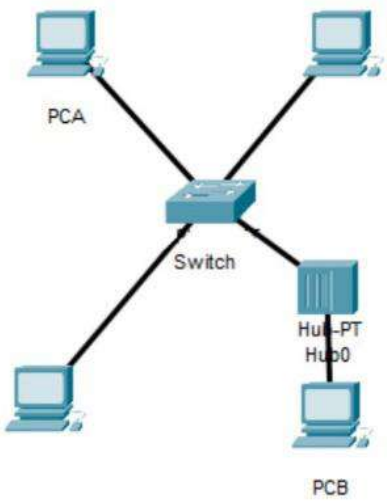
۳) STP – در مباحث آینده آشنا خواهیم شد.

نکته۱: سوئیچ تمام لایه های TCP/IP را متوجه میشود، ولی Learning و forwarding را براساس mac address انجام میدهد. به همین خاطر به سوئیچ دستگاه لایه دوئی میگویند.

نکته۲: Mac address Table = Switching Table = Bridging Table = CAM Table (Content Address Memory Table)

نکته۳: برای پاک کردن جدول Mac address از دستور clear mac address-table استفاده می‌کنیم.

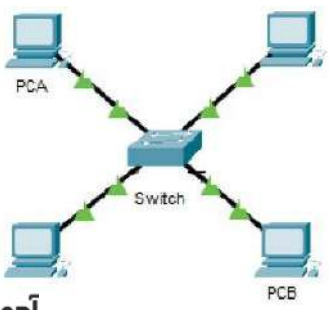
نکته٤: عمر mac adderss table ۵ دقیقه است.



** اگر سوئیچ از پورتی مک سیستمی را learn کرده باشد، اگر سیستم(NIC جدید= mac جدید) همان پورت را مستقیم Connected Directory عوض کنیم(یا ادمین down shut کند)، به سرعت مک قبلی حذف و مک جدید جایگزین میشود. اما اگر سیستم قدیم و جدید با واسطه(مثلا hub) به سوئیچ متصل شده باشد، در صورت تعویض تا ۵ دقیقه اتصال برقرار نمیشود، چون mac آدرس قبلی در جدول مک آدرس همچنان موجود است(یعنی اگر ارتباط بین Hub , PcBقطع شود ، سوئیچ هیچ LOG نمی دهد و جدول Mac هنوز مک این interface را نگه داشته و اگر بسته ارسال شود ، سوئیچ آن را فوروارد می کند و روی هاب Drop می شود و تا زمان Mac age timeیا همان ۵ دقیقه ، PcB Macرا نگه می دارد) که اگر بخواهیم قطعی باقی نماند باید از clear mac adsress table استفاده کنیم تا سوئیچ mac سیستم جدید را دریافت کند.

ARP (Address Resolution Protocol) :

ARP پروتکلی است برای یافتن Address Mac از طریق ip مورد استفاده قرار می گیرد. زمانیکه یک دستگاه با دستگاه دیگر در شبکهLAN ارتباط برقرار می کند، برای آن دستگاه نیاز به Address Mac دارد و دستگاه از پروتکل ARP جهت دستیابی به Address Mac مربوط به آن دستگاه استفاده می‌کند.



مثال: فرض کنید PCA میخواهد با PCB ارتباط برقرار کند.

قبل اینکه بسته icmp شکل بگیرد، arp شکل میگیرد(برای بدست آوردن DST Mac address). اطلاعات بسته اولیه Arp به صورت ذیل است:

Src IP: IP PC A Src Mac address: Mac address PC A F0/1

Dst IP: IP PC B Dst mac address: FFFF.FFFF.FFFF PC B F0/2

سوئیچ در مرحله اول learning میکند، یعنی مک pc A را در جدول مک آدرس قرار میدهد.

Mac Pc A F0/1

در مرحله دوم چون مک آدرس PC B را نمیداند، (FFFF.FFFF.FFFF یعنی بسته باید برای پیدا شدن مک آدرس به همه پورت ها ارسال شود)بسته را به همه پورت‌ها به غیر از پورتی که از آن بسته را دریافت کرده است Flood(Broadcast) میکند. همه سیستم‌ها وقتی بسته را دریافت کردند، اطلاعات لایه دوئی(mac ad) و لایه سه‌ی (ip) را مقایسه میکنند. اگر مطابقت نداشت، آن بسته را دور می‌ریزند، ولی در صورت برابری IPخود با Dst ip، بسته جدید ARP را به صورت زیر اصلاح میکند:

Src IP: IP PC B Src Mac address: Mac address PC B F0/2

Dst IP: IP PC A Dst mac address: Mac address PC A F0/1

و همچنین PC B جدول Arp خود را به صورت زیر برای خود تشکیل میدهد :

Arp table / IP A mac address table B

وقتی این بسته به سوئیچ میرسد، از پورتF0/2 مک دستگاه B را در جدول خود قرار میدهد .

Mac Pc A F0/1

Mac Pc B F0/2

سپس براساس Dst mac addressی که در جدول خود دارد، بسته را به سمت PC A ارسال میکند.

بعد از رسیدن بسته، PC A نیز جدول arp خود را به صورت زیر تشکیل میدهد:

Arp table / IP B mac address table B

بعد از اینکه PC A مک PC B را متوجه شد، آنگاه Icmp با خیال راحت بسته اصلی خود را به مقصد خود یعنی PC B ارسال میکند.

نکته۱: عمر arp table ٤ ساعت است. این بدان معنا است اگر به عنوان مثال در پورتی اطلاعاتی رد و بدل نشد بعد از ٤ ساعت پاک میشود ولی اگر منتقل شد این زمان تمدید میشود. (این زمان مانند ساعت شنی عمل میکند)

نکته۲: Arp هم از نوع فوروارد Unknow unicast میباشد.

نکته۳: برای پاک کردن جدول arp سیستم، در cmd از دستور arp –d استفاده می شود.

نکته٤: برای مشاهده جدول arp سیستم، در cmd از دستور arp –a استفاده می شود.

نکته۵: arp به دو صورت staticو dynamic ایجاد می‌شود. برای اضافه کردن مک به صورت دستی، در cmd از دستور arp –s استفاده می‌شود.

Arp -s	10.0.0.3	90-02-7b-c

نکته٦: برای اینکه یک بسته به دست همه اعضای شبکه در broadcast که دادیم به همه برسد باید تمام بیت های host را یک قرار دهیم. مک آدرس ٤٨ بیت می باشد که در مبنای ١٦ نماش داده می شود یا HEX یعنی هر ٤ کاراکتر را یک کاراکتر HEX در نظر می گیرد. اینجا چهارتا ۱ رو کنار هم قرار دهیم و تبدیل کنیم به HEX ، عددی که به HEX بدست می آید۱۵ می‌شود که اینجا ۱۲ تا Fخواهیم داشت.

BIN 1111 => HEX=F

1111 1111 1111 1111 1111 1111 1111 1111 1111 1111 1111 1111

F F F F F F F F F F F F

نتیجه: 48bit FFFF.FFFF.FFFF.FFFF

Application specific integrated circuit (Asic) :

سیسکو جدول های Mac را تشکیل می دهد تا بتواندforwarding Traffic را انجام دهد که این جدول ها در RAM ذخیره می شوند که باید پردازش شوند و بعد بسته فورورد شود. در دستگاه های دیگر CPU این وظیفه را دارد، اما سیسکو به ازای هر پورت یک CPU سخت افزاری جداگانه به نام Asic در نظر گرفته ، به همین علت سرعت forwarding تجهیزات سیسکو بالاست و به اصطلاح Wire speed عمل می کنند.

Virtual Local Area Network (VLAN) Concept :

ما در لایه سه با جدا کردن NetIDها توانستیم broadcast domainها راجدا کنیم. ولی لایه دو چی؟ ما اگر فقط broadcast domain را در لایه سه جدا کرده باشیم، در صورت نیاز به broadcast، سوئیچ بسته را به همه پورت‌ها ارسال می‌کند. به دلیل اینکه تمام پورت‌های یک سوئیچ در یک broadcast domain هستند و سوئیچ ترافیک را بر حسب لایه دو فورورد میکند. که این امر باعث کاهش امنیت می‌شود.

برای جدا کردن Broadcast domainها در سطح لایه دو از مکانیزم logical ویلن (vlan) استفاده میکنیم. Vlan یعنی شبکه محلی مجازی. هر VLAN یا LANهای مجازی، مانند یک LAN فیزیکی یک حوزه Broadcast مستقل را برای جدا نمودن ترافیک بخش‌های مختلف تشکیل خواهد داد. برای مثال در یک شرکت، برای جدا کردن ترافیک کامپیوترهای واحد حسابداری از ترافیک کامپیوترهای واحد فروش یا هر بخش دیگری. برای این منظور کامپیوترهای واحد حسابداری در یک VLAN و کامپیوترهای واحد فروش در یک VLAN دیگر قرار خواهند گرفت در این صورت ارتباطی بین کامپیوترهای واحد فروش و کامپیوترهای واحد حسابداری وجود نخواهد داشت.

نکته۱: هر سوئیچی قابلیت پشتیبانی از VLAN را نخواهد داشت ولی SWTICHهای CISCO توانمندی VLAN را پشتیبانی می‌کنند.

نکته۲: VLAN1 معروف به Default VLAN است که به‌صورت پیش‌فرض بر روی کلیه Swtichها ایجاد شده و کلیه پورت‌های Swtich در عضویت VLAN1 هستند.

نکته۳: هر VLAN با یک شماره که به VLAN ID معروف است شناسایی خواهد شد. سوئیچ‌های Catalyst سیسکو رنج گسترده‌ای از VLANها را از VLAN1 تا VLAN4094 را پشتیبانی خواهند کرد. به دلیل اینکه برای vlan، ۱۲ بیت در نظر گرفته شده است. این یعنی

2^12 حالت. یعنی ما میتوانیم 4096 ویلن داشته باشیم(۰ تا ٤۰۹٥) که ۰ و ٤۰۹٥ رزور است و Vlan1 و vlan1002 تا vlan1005 استفاده شده است. پس در نهایت ما می‌توانیم vlanهای ۲ تا ۱۰۰۱ و ۱۰۰٦ تا ٤۰۹٤ را استفاده کنیم.

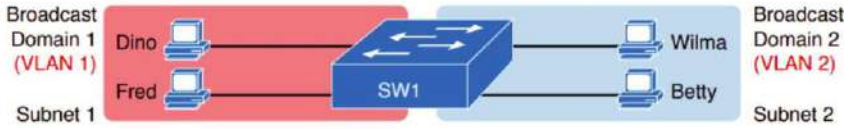
```
Switch(config)#vlan ?
  <1-4094>  ISL VLAN IDs 1-1005
```

```
VLAN Name                                Status
---- ----------------------------------- ---------
1    default                             active

1002 fddi-default                        active
1003 token-ring-default                  active
1004 fddinet-default                     active
1005 trnet-default                       active
```

نکته٤: هر VLAN مانند یک LAN فیزیکی دارای یک رنج IP Address مستقل به خود است.

نکته٥: برای جدا کردن Broadcast domainها نیاز به اضافه کردن سوئیچ جدید نیست. با مکانیزم vlan این امکان با یک سوئیچ به راحتی فراهم است.

Creating Two Broadcast Domains with Two Physical Switches and No VLANs



Creating Two Broadcast Domains Using One Switch and VLANs

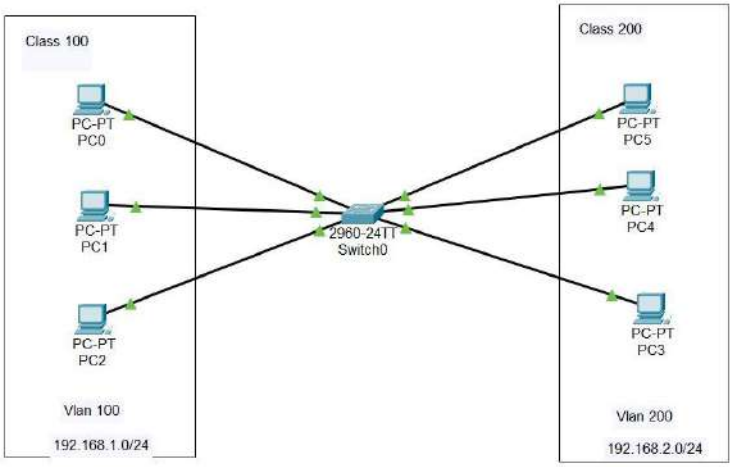
نکته۷: برای مشاهده وضعیت vlanهای یک سوئیچ از دستور show vlan استفاده می‌کنیم. همچنین با دستور show vlan brief خلاصه‌ای از وضعیت vlanها نشان داده می‌شود.

```
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#show vlan

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

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1    enet  100001     1500  -      -      -        -    -        0      0
1002 fddi  101002     1500  -      -      -        -    -        0      0
1003 tr    101003     1500  -      -      -        -    -        0      0
1004 fdnet 101004     1500  -      -      -        ieee -        0      0
1005 trnet 101005     1500  -      -      -        ibm  -        0      0

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------

Remote SPAN VLANs
------------------------------------------------------------------------------

Primary Secondary Type              Ports
------- --------- ----------------- ------------------------------------------
```

ساخت و نامگذاری vlanها :

```
Switch(config)#vlan 100
Switch(config-vlan)#na
Switch(config-vlan)#name CLASS_100
Switch(config-vlan)#vla
Switch(config-vlan)#vlan 200
Switch(config-vlan)#nam
Switch(config-vlan)#name CLASS_200
```




```
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
100  CLASS_100                         active
200  CLASS_200                         active
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
```

همانطور که مشاهده میشود vlanها تشکیل شده ولی هنوز پورت‌ها به عضویت vlanها درنیامده اند.

نکته: برای حذف یک vlan از دستور Switch(config)#no VLAN-ID استفاده می‌کنیم.

عضویت PORTهای سوئیچ در VLANها:

با دستور interface وارد اینترفیس موردنظر خودتان می‌شوید و با استفاده از دستور switchport access vlan ID می‌توانید Vlan انتخابی خود را برای آن اینترفیس انتخاب کنید.

با این دستور به پورت اعلام می کنیم که به یک device end متصل شده و باید ترافیک یک vlan را از خود عبور دهد.

نحوه انتخاب اینترفیس‌ها:

- ✓ انتخاب پورت بصورت تکی:

Switch>enable

Switch#configure terminal

Switch(config)#**interface fastEternet 0/1**

Switch(config-if)#**switchport access vlan 20**

Switch(config-vlan)#exit

✓ انتخاب چند پورت بصورت انتخابی:

```
Switch>enable
Switch#configure terminal
Switch(config)#interface fastEternet 0/5,0/10,0/15
Switch(config-if)#switchport access vlan 20
```

✓ انتخاب پورت ها بصورت ترتیبی و پشت سر هم

```
Switch(config)#interface range fastEternet 0/15-0/24 or (0/1-3)
Switch(config-if-range)#switchport access vlan 20
```

ادامه مثال بالا:

```
Switch(config)#interface range fastEthernet 0/1-3
Switch(config-if-range)#sw
Switch(config-if-range)#switchport as
Switch(config-if-range)#switchport ac
Switch(config-if-range)#switchport access v
Switch(config-if-range)#switchport access vlan 100
```

```
Switch(config)#interface range fastEthernet 0/4-6
Switch(config-if-range)#sw
Switch(config-if-range)#switchport ac
Switch(config-if-range)#switchport access v
Switch(config-if-range)#switchport access vlan 200
```

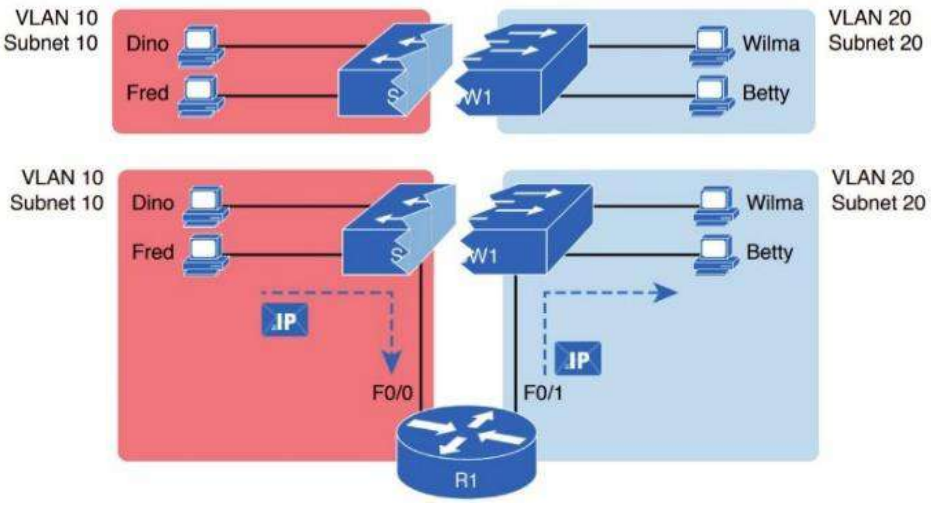
```
Switch#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    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
100  CLASS_100                        active    Fa0/1, Fa0/2, Fa0/3
200  CLASS_200                        active    Fa0/4, Fa0/5, Fa0/6
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
```

Forwarding Data Between VLANs:

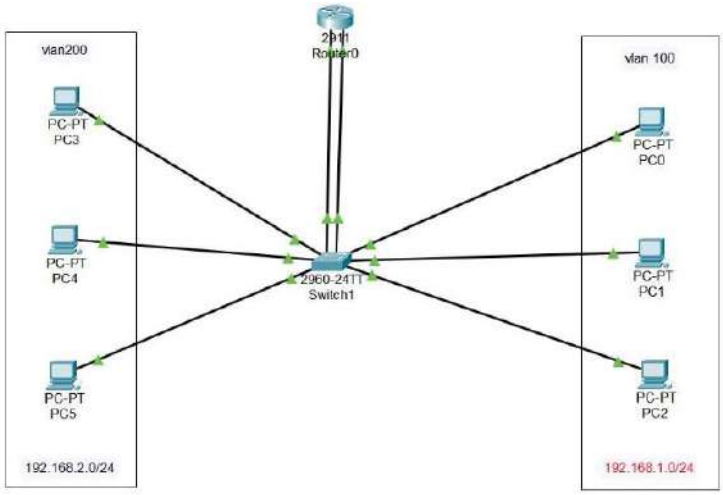
حال اگر بخواهیم دو شبکه جدا شده گاهی با هم ارتباط داشته باشند، به روش‌های زیر عمل میکنیم: برای اینکار ما باید از دستگاهی استفاده کنیم که لایه سه بفهمد(مثل روتر و MLS) که بتواند ارتباط بین networkها را برقرار کند.

* روش یک (Roas=Router on a stick):

در این روش به ازای هر vlan، یک پورت سوئیچ را به روتر وصل کرده‌ایم.



مثال:



در ابتدا پورت‌هایی که به روتر متصل شده‌اند را جداگانه اول به مد Accese تبدیل میکنیم، دوم به مُد vlan accessهای موجود را فراخوان میزنیم.

(Creating VLANs and Assigning Access VLANs to an Interface)

```
Switch(config)#interface gigabitEthernet 0/1
Switch(config-if)#sw
Switch(config-if)#switchport m
Switch(config-if)#switchport mode ac
Switch(config-if)#switchport mode access
Switch(config-if)#sw
Switch(config-if)#switchport ac
Switch(config-if)#switchport access v
Switch(config-if)#switchport access vlan 100
```

```
Switch(config)#interface gigabitEthernet 0/2
Switch(config-if)#sw
Switch(config-if)#switchport m
Switch(config-if)#switchport mode ac
Switch(config-if)#switchport mode access
Switch(config-if)#sw
Switch(config-if)#switchport ac
Switch(config-if)#switchport access v
Switch(config-if)#switchport access vlan 200
Switch(config-if)#
```

در مرحله بعد به سراغ روتر می‌رویم. ابتدای کار پورت مورد نظر روتر را no shut می‌کنیم. در ادامه روی هر پورت روتر یک IP (که همان getway هر network میباشد- معمولا اولین یا آخرین IP address را به عنوان getway تعیین می‌کنند)

```
Router(config)#interface gigabitEthernet 0/1
Router(config-if)#no
Router(config-if)#no sh
Router(config-if)#no shutdown

Router(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to up

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

```
Router(config)#interface gigabitEthernet 0/2
Router(config-if)#no sh
Router(config-if)#no shutdown

Router(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/2, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/2, changed state to up

Router(config-if)#ip
Router(config-if)#ip ad
Router(config-if)#ip address 192.168.2.1 255.255.255.0
```

برای دیدن وضعیت اینترفیس های روتر از دستور show ip interface brief استفاده میشود.

```
Router#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0     unassigned      YES unset  administratively down down
GigabitEthernet0/1     192.168.1.1     YES manual up                    up
GigabitEthernet0/2     192.168.2.1     YES manual up                    up
Vlan1                  unassigned      YES unset  administratively down down
```

```
C:\>ping 192.168.2.40

Pinging 192.168.2.40 with 32 bytes of data:

Request timed out.
Reply from 192.168.2.40: bytes=32 time=1ms TTL=127
Reply from 192.168.2.40: bytes=32 time=3ms TTL=127
Reply from 192.168.2.40: bytes=32 time=1ms TTL=127

Ping statistics for 192.168.2.40:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 3ms, Average = 1ms
```

در نهایت مشاهده می‌شود که PC0 از vlan100، PC5 Ping در Vlan200 را دارد. یعنی می‌توانند به همدیگر بسته ارسال کنند.

نکته۱: دستور switchport لایه دوئی میباشد و روتر accces vlan و... را متوجه نمیشود.

نکته۲: در صورتی که vlan از قبل ایجاد شده نباشد وارد کردن دستور switchport access vlan 100 باعث ایجاد VLAN 100 می شود.

نکته۳: این روش عملی است ولی غیر منطقی. همچنین مقرون به صرفه نیست، چون پورت‌های روتر محدود است. اصلا قرار نیست End user ها به روتر متصل شوند.

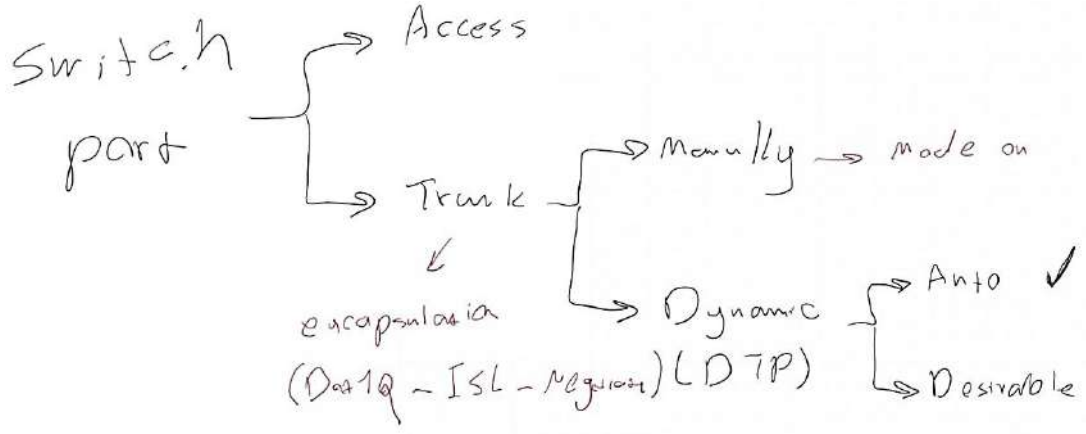
* روش دو (روش منطقی روش قبل):

(VTP) VLAN Trunking Protocol :

در روش قبلی ما هر پورت را Access یک vlan می‌کردیم که هر پورت vlan مربوط به خود را عبور می‌داد. در این روش ما از Trunk mode استفاده میکنیم که از پورت خود ترافیک چندین vlan را به طور همزمان عبور میدهد.

هر پورت سوئیچ از دو Mode تشکیل شده است:

(static(on) & dynamic (auto&desirable)) Trunk & Access



Access :	**NOT Send , NOT Accept**
Dynamic Auto:	**NOT Send , Accept**
Dynamic Desirable :	**Send , Accept**
Trunk :	**Send**

Access : اگر پورت در این حالت قرار بگیرد، ترافیک vlan را عبور می‌دهد و Trunk نمی‌شود.

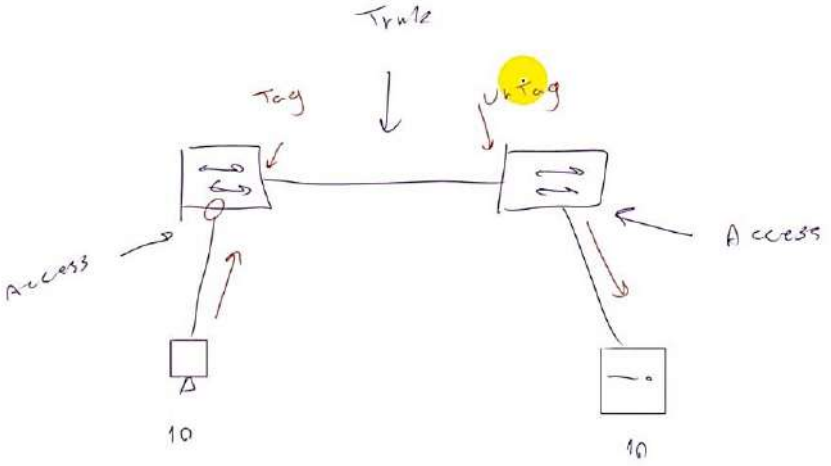
Trunk : اگر پورت را در این حالت قرار بدهیم یعنی پورت باید ترافیک همه vlanها را همزمان با زدن Tag انتقال دهد.

Dynamic auto : این حالت دستوری به طرف مقابل نمی‌دهد، ولی اگر دستوری دریافت کند عمل می‌کند. یعنی اگر طرف مقابل درخواست کند که ارتباط Trunk برقرار کنیم قبول می‌کند.

Dynamic desirable : هم درخواست Trunk شدن می‌دهد، هم اگر دستوری برای برقراری Trunk دریافت کند می‌پذیرد.

Command Option	Description
access	Always act as an access (nontrunk) port
trunk	Always act as a trunk port
dynamic desirable	Initiates negotiation messages and responds to negotiation messages to dynamically choose whether to start using trunking
dynamic auto	Passively waits to receive trunk negotiation messages, at which point the switch will respond and negotiate whether to use trunking

نکته: tag و untag در Trunk به صورت زیر انجام میشود: (این Tagها به header ،encapsulation می‌شوند .)



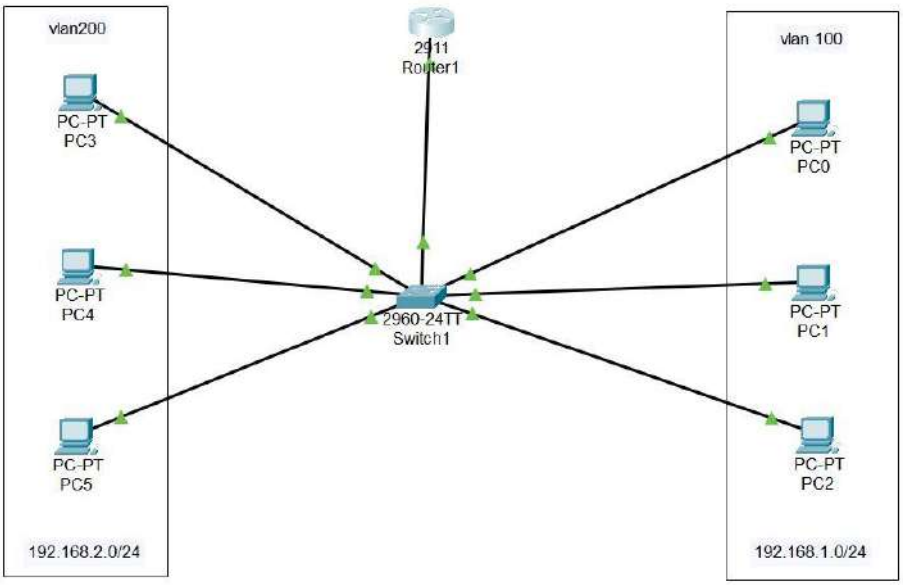
نکته۱: تمام پورتهای یک سوئیچ به صورت پیشفرض در مد access قرار دارد. برای اینکه یک پورت را به یک Vlanنسبت دهید، باید از این مد استفاده کنید.

نکته۲: با توجه به جدول بالا، دو پورت مقابل نمی‌توانند یک طرف access و طرف دیگر Trunk باشد.

نکته۳: تمام پورت‌های سوئیچ در حالت dynamic port هستند. یعنی دو پورت مقابل هم negotitation می‌کنند تا ببینند در نهایت چه modeی را استفاده کنند(حالت‌های زیر رخ می‌دهد).

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

مثال :



در ابتدای کار وارد interfaceای می‌شویم که به روتر متصل شده است. اینترفیس را به حالت Trunk میبریم.

```
Switch(config)#interface gigabitEthernet 0/1
Switch(config-if)#switchport mode trunk
```

به سراغ روتر می‌رویم. در شروع کار اینترفیس را روشن می‌کنیم.

```
Router(config)#interface gigabitEthernet 0/1
Router(config-if)#no shutdown
```

توجه : روتر اینترفیس logicalای دارد که وابستگی به اینترفیس physical دارد(یعنی اگر اینترفیس فیزیکال down بشه، همه اینترفیس های لایجال down میشوند.). این اینترفیس تگ vlan را برخلاف خود روتر و اینترفیسش میفهمد. این اینترفیس sub interface نامیده میشود که به صورت زیر ساخته میشود(تعداد ساخت Sub ineterfaceها نامحدود است). بعد از ساخت با دستور encapsulation به sub interface تگ vlan فهمانده می‌شود. در نهایت به این sub اینترفیس IP داده میشود (این IP همان getway نتورک‌هاست).

```
Router(config)#interface gigabitEthernet 0/1.100
Router(config-subif)#encapsulation dot1Q 100
Router(config-subif)#ip address 192.168.1.1 255.255.255.0
```

```
Router(config)#interface gigabitEthernet 0/1.200
Router(config-subif)#encapsulation dot1Q 200
Router(config-subif)#ip address 192.168.2.1 255.255.255.0
```

```
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  up                    up
GigabitEthernet0/1.100 192.168.1.1     YES manual up                    up
GigabitEthernet0/1.200 192.168.2.1     YES manual up                    up
GigabitEthernet0/2     unassigned      YES unset  administratively down down
Vlan1                  unassigned      YES unset  administratively down down
```

نکته: برای برگردان یک interface به حالت پیش‌فرض، از دستور Default int gig 0/X استفاده می‌کنیم:

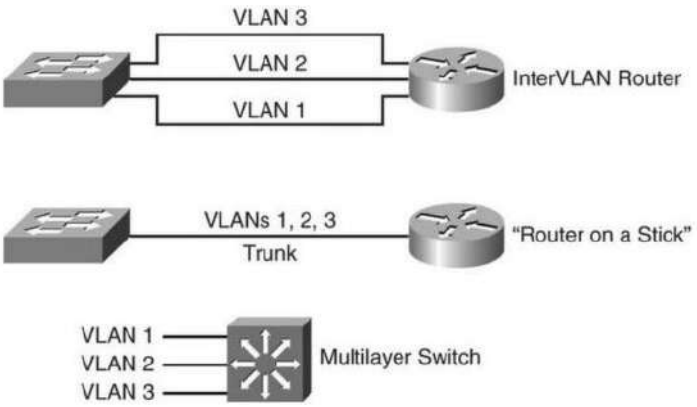
```
Switch(config)#default interface g
Switch(config)#default interface gigabitEthernet 0/1
Building configuration...
```

نکته: برای مشاهده اطلاعات مربوط به حالت Trunk از دستور show interfaces trunk استفاده می‌شود.

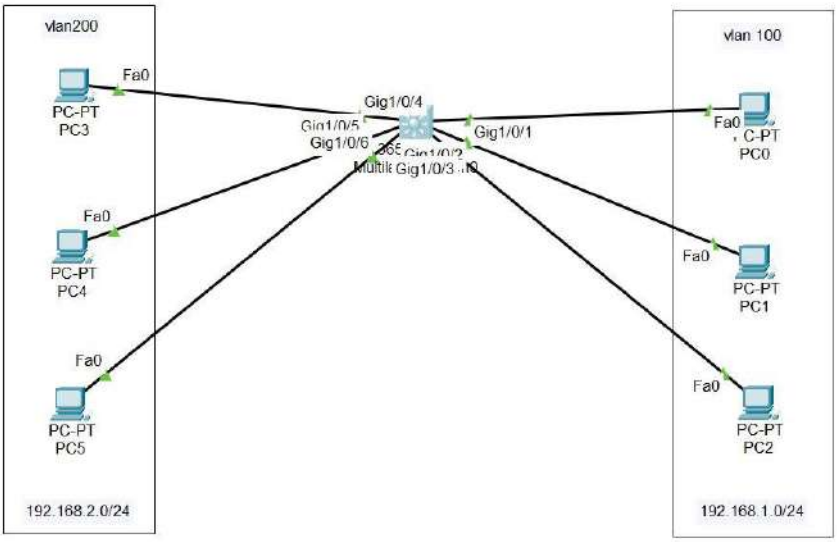
```
Switch#show interfaces trunk
Port        Mode         Encapsulation  Status        Native vlan
Gig0/1      on           802.1q         trunking      1

Port        Vlans allowed on trunk
Gig0/1      1-1005

Port        Vlans allowed and active in management domain
Gig0/1      1,100,200

Port        Vlans in spanning tree forwarding state and not pruned
Gig0/1      1,100,200
```

* روش سه :

در service providerها و large scaleها به دلیل اینکه حجم ترافیک‌ها بالاست، اگر از روش های قبل استفاده کنیم بخاطر رفت و آمد ترافیک‌ها headache ایجاد میشود(هم برای دستگاه هم ترافیک). به همین خاطر گفتند برای حل این مسئله به دستگاهی نیاز داریم که هم switching انجام دهد هم Routing. به دستگاهی به اسم MLS (multilayer switch) رسیدند.



مثال:



در ابتدای کار vlan می‌سازیم. سپس interfaceها را عضو این vlanها می‌کنیم.

```
Switch(config)#interface range gigabitEthernet 1/0/1-3
Switch(config-if-range)#sw
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 100
```

```
Switch(config)#interface range gigabitEthernet 1/0/4-6
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 200
```

```
Switch#show vlan

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Gig1/0/7, Gig1/0/8, Gig1/0/9, Gig1/0/10
                                                Gig1/0/11, Gig1/0/12, Gig1/0/13, Gig1/0/14
                                                Gig1/0/15, Gig1/0/16, Gig1/0/17, Gig1/0/18
                                                Gig1/0/19, Gig1/0/20, Gig1/0/21, Gig1/0/22
                                                Gig1/0/23, Gig1/0/24, Gig1/1/1, Gig1/1/2
                                                Gig1/1/3, Gig1/1/4
100  class100                         active    Gig1/0/1, Gig1/0/2, Gig1/0/3
200  class200                         active    Gig1/0/4, Gig1/0/5, Gig1/0/6
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
```

توجه: همانطور که vlan1 و interface vlan1 به طور پیش‌فرض روی دستگاه سوئیچ موجود است، ما می‌توانیم به ازای ساخت هر vlan x، یک interface vlan x بسازیم. برای ساخت interface vlan حتماً باید vlan آن را بسازیم(بلعکس مانعی ندارد).

SVI (Interface VLan)=Switch virtual interface

مرحله بعد به سراغ ساخت interface vlan و دادن IP به آن می‌رویم. توجه شود که این interface شات‌دان نیست(برخلاغ interface vlan1)

```
Switch(config)#interface vlan 100
Switch(config-if)#
%LINK-5-CHANGED: Interface Vlan100, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan100, changed state to up

Switch(config-if)#ip
Switch(config-if)#ip ad
Switch(config-if)#ip address 192.168.1.1 255.255.255.0
```

```
Switch(config)#interface vlan 200
Switch(config-if)#
%LINK-5-CHANGED: Interface Vlan200, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan200, changed state to up

Switch(config-if)#ip ad
Switch(config-if)#ip address 192.168.2.1 255.255.255.0
```

در آخر هم دستور IP Routing را برای برقراری ارتباط لایه سه‌ی interfaceها وارد می‌کنیم.

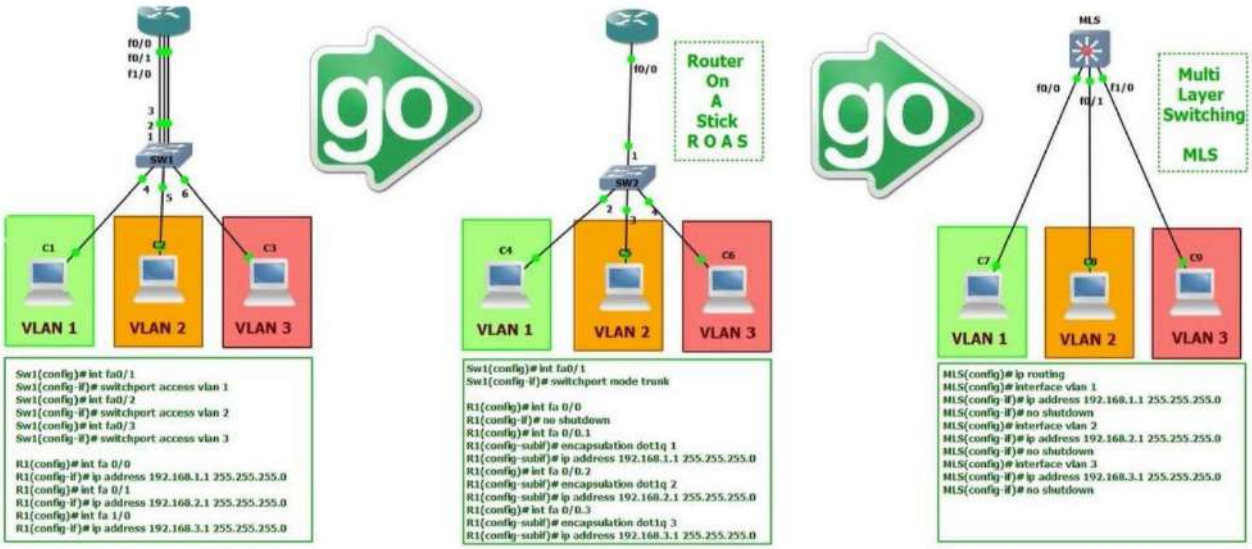
```
Switch(config)#ip routing
```

```
Switch#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet1/0/1   unassigned      YES unset  up                    up
GigabitEthernet1/0/2   unassigned      YES unset  up                    up
GigabitEthernet1/0/3   unassigned      YES unset  up                    up
GigabitEthernet1/0/4   unassigned      YES unset  up                    up
GigabitEthernet1/0/5   unassigned      YES unset  up                    up
GigabitEthernet1/0/6   unassigned      YES unset  up                    up
GigabitEthernet1/0/7   unassigned      YES unset  down                  down
GigabitEthernet1/0/8   unassigned      YES unset  down                  down
GigabitEthernet1/0/9   unassigned      YES unset  down                  down
GigabitEthernet1/0/10  unassigned      YES unset  down                  down
GigabitEthernet1/0/11  unassigned      YES unset  down                  down
GigabitEthernet1/0/12  unassigned      YES unset  down                  down
GigabitEthernet1/0/13  unassigned      YES unset  down                  down
GigabitEthernet1/0/14  unassigned      YES unset  down                  down
GigabitEthernet1/0/15  unassigned      YES unset  down                  down
GigabitEthernet1/0/16  unassigned      YES unset  down                  down
GigabitEthernet1/0/17  unassigned      YES unset  down                  down
GigabitEthernet1/0/18  unassigned      YES unset  down                  down
GigabitEthernet1/0/19  unassigned      YES unset  down                  down
GigabitEthernet1/0/20  unassigned      YES unset  down                  down
GigabitEthernet1/0/21  unassigned      YES unset  down                  down
GigabitEthernet1/0/22  unassigned      YES unset  down                  down
GigabitEthernet1/0/23  unassigned      YES unset  down                  down
GigabitEthernet1/0/24  unassigned      YES unset  down                  down
GigabitEthernet1/1/1   unassigned      YES unset  down                  down
GigabitEthernet1/1/2   unassigned      YES unset  down                  down
GigabitEthernet1/1/3   unassigned      YES unset  down                  down
GigabitEthernet1/1/4   unassigned      YES unset  down                  down
Vlan1                  unassigned      YES unset  administratively down down
Vlan100                192.168.1.1     YES manual up                    up
Vlan200                192.168.2.1     YES manual up                    up
```

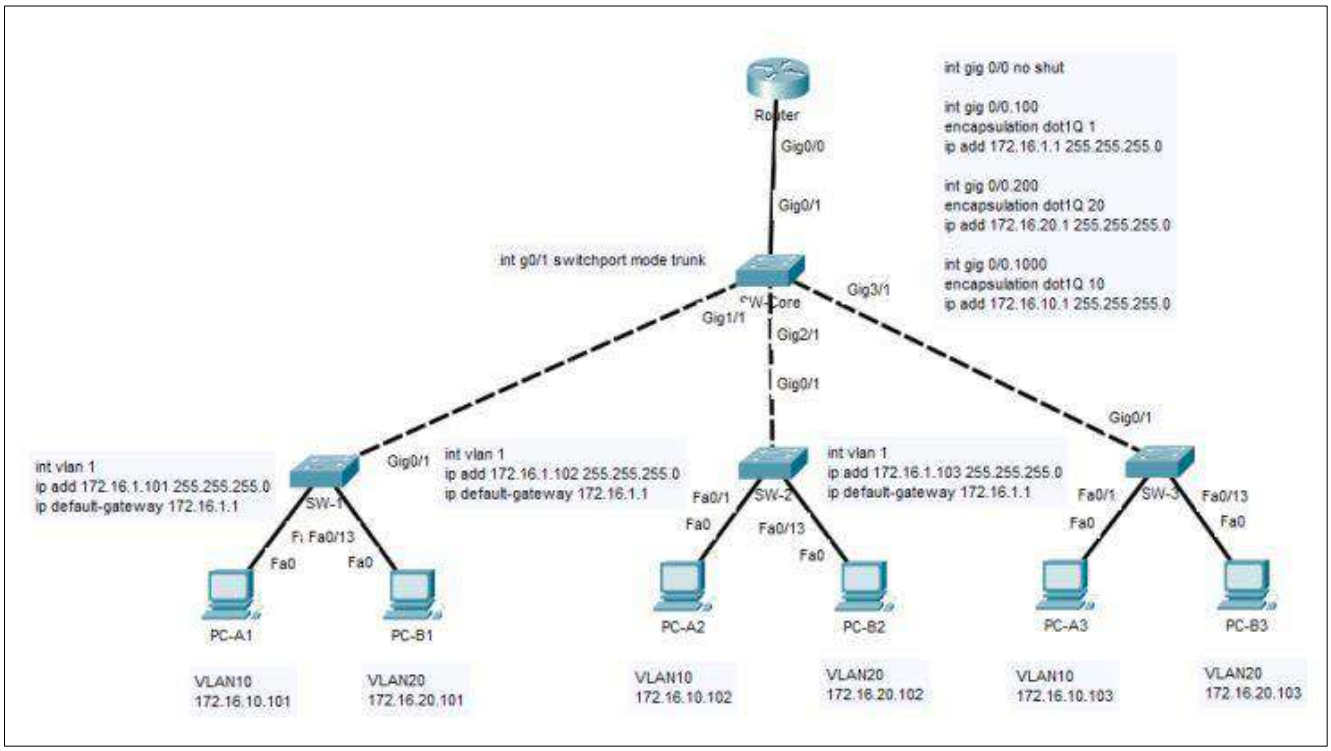
```
C:\>ping 192.168.1.10

Pinging 192.168.1.10 with 32 bytes of data:

Request timed out.
Reply from 192.168.1.10: bytes=32 time=1ms TTL=127
Reply from 192.168.1.10: bytes=32 time<1ms TTL=127
Reply from 192.168.1.10: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.1.10:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

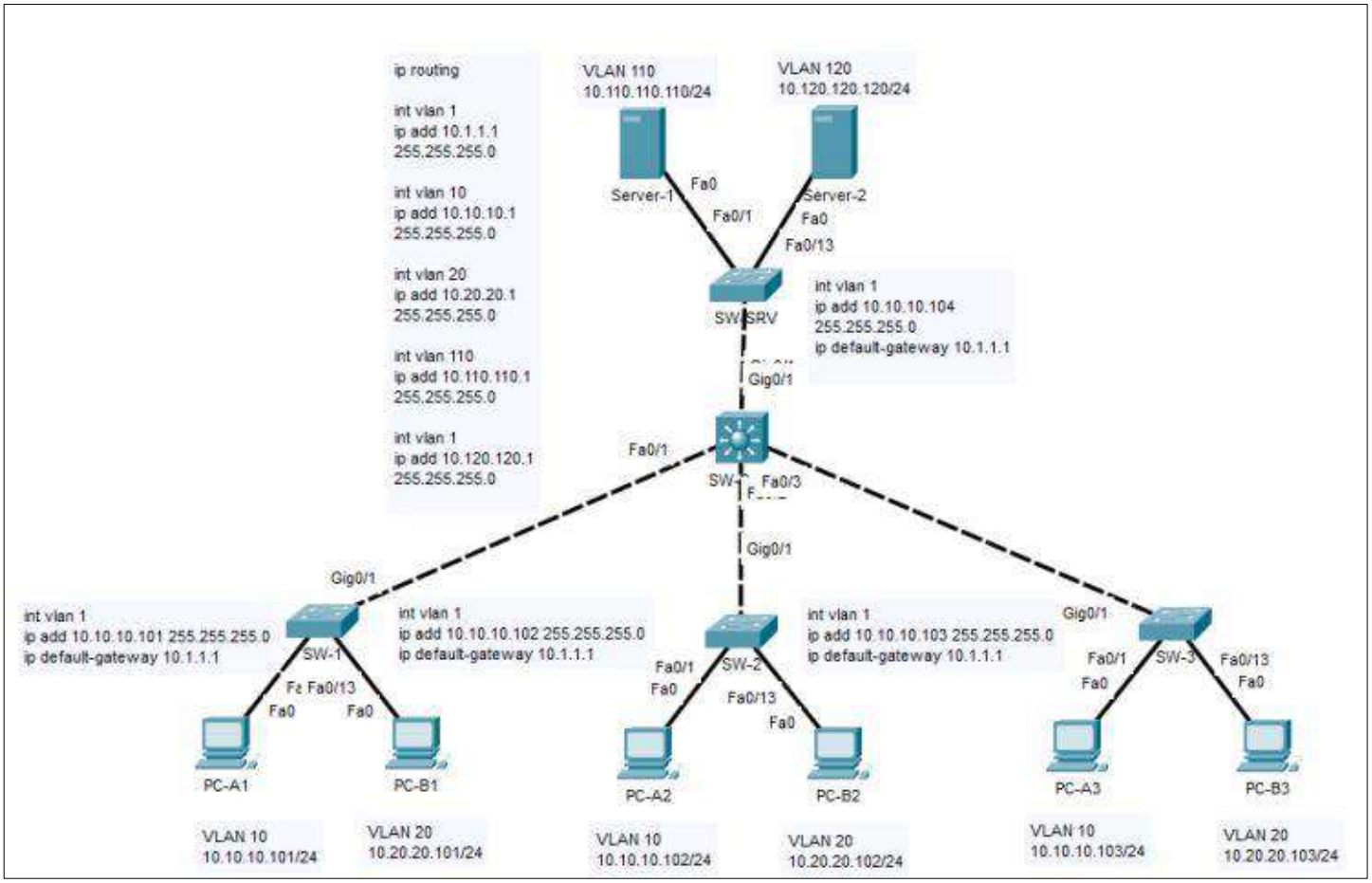
ارتباط برقرار شد.

خلاصه ای از ۳ حالت :

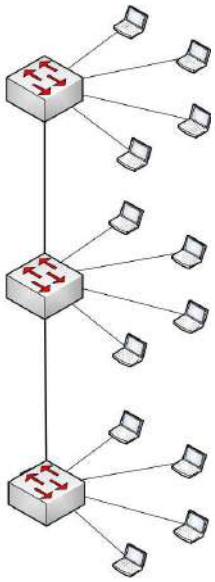


نمونه سناریو :





Trunk Mode :



قبل تعریف این مد، یک مثال برای درک بهتر این موضوع تعریف میکنیم؛ شما مدیر شبکه‌ی یک ساختمان هستید و این ساختمان از سه طبقه تشکیل شده است و در هر طبقه از یک سوئیچ برای شبکه کردن کامپیوترها استفاده شده 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، 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 vlan های دیگر در طبقات مختلف در ارتباط باشند. برای حل این مشکل باید از Trunk استفاده کرد، Trunkروشی برای انتقال Vlan ها در سوئیچ‌های مختلف است و با استفاده از آن این مشکل به راحتی حل میشود.

Tag زدن روی فریم‌ها: برای انتقال Vlan ها 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 که این استاندارد مختص شرکت سیسکو بوده و به صورت پیشفرض در برخی دستگاه‌های لایه ی دوم این شرکت فعال است. بسیار سنگین و مجموعا 30 B هدر به بسته اضافه می کند.

802.1Q: یک استاندارد Source Open 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. مجموعا ٤ بایت دارد که ۱۲ بیت را به VLAN تخصیص داده.

فعال کردن پروتکل **ISL** و **802.1Q** : این پروتکل به صورت پیشفرض روی سوئیچ‌های شرکت سیسکو فعال است. 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 Vlan ها را برچسبگذاری میکند و از خود عبور میدهد.

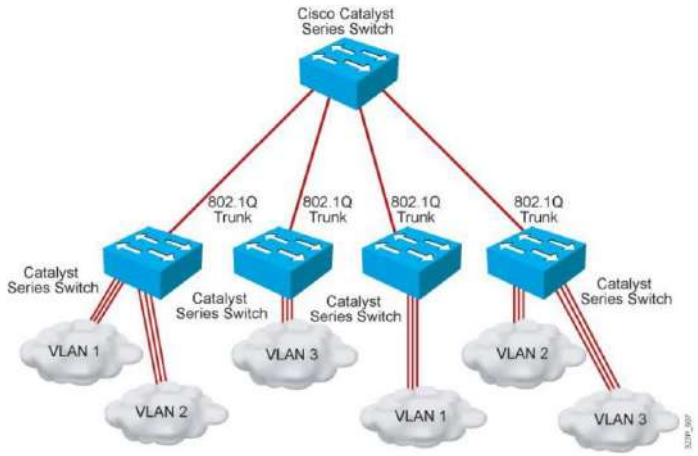
**توجه: شاید شما بخواهید به سوئیچ بگوئید که فقط Vlan های خاصی از وی عبور کنند(یا فلان vlan عبور نکند)؛ برای این منظور از دستور (<> Allow vlan) استفاده میکنیم:

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

با این دستور فقط Vlan ۱۰ حق عبور دارد و بقیهVlan ها از این سوئیچ عبور نمی‌کنند.

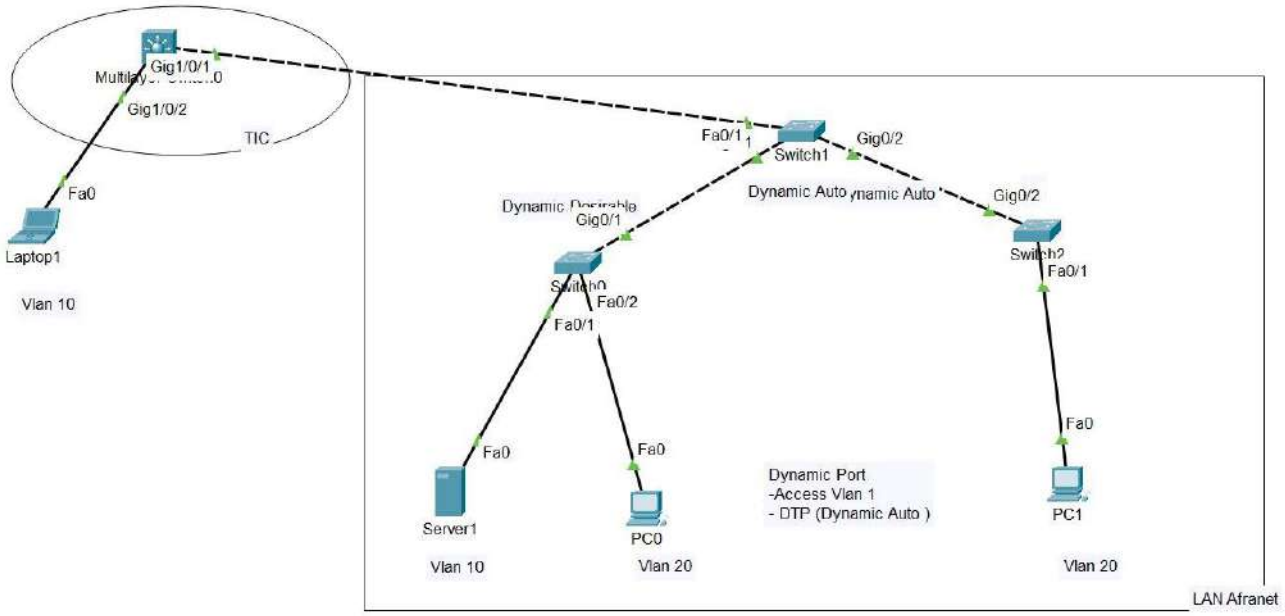
پس یک پورت در سوئیچ زمانی Trunk میشود که بخواهد Vlan ها را بین دو دستگاه سوئیچ جابجا کنند. به شکل توجه کنید:

در این شکل، سوئیچ‌ها به هم متصل شده‌اند و سوئیچ‌هایی که در زیر قرار دارند از Vlan های 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 Q802.1 را راه‌اندازی کنیم تا عملیات برچسب‌گذاری روی Vlan ها را انجام دهد.



Allow Vlan :

سناریو:



در مثال بالا شرکتی مانند افرانت شبکه ای لایه دو تشکیل داده است که بسترهای ارتباطی آن vlan است. فرض میکنیم شرکت اصلی افرانت در تهران و server آن در date center اصفهان است. پس نیاز داریم برای ارتباط این دو، شبکه لایه ۲ برقرار کنیم. دو طرف برای ارتباط از مخابرات سرویس یا پورت لایه ۲ گرفته‌اند یعنی ارتباط از طریق vlan برقرار می‌کنند.

طبیعتا date center برای ارتباط بین سوئیچ و ... Vlan بندی دارد. همچنین با vlanبندی سوئیچ ۰ و سوئیچ ۲، pc0و PC1 با هم ارتباط دارند. (نکته: برای اینکه سوئیچ ۱ vlanهای سوئیچ ۲و ۰ را بفهمد و Tag و untag کند باید همه vlanهای طرفین را در خود ساخته باشد. یعنی vlan20 باید در سه سوئیچ ساخته شده باشد تا ارتباط برقرار شود.)

بعد از مشخص شدن mode های سوئیچ ۱ ، مشخص شد که همه vlanهای ۱۰ و ۲۰ و ۱ از fa/01 به سمت مخابرات Trunk میشوند ولی ما نمیخواهیم جز vlan 10 که سرور است ، از شبکه خارج شد (در شکلg را F در نظر بگیریم).

```
Switch#show interfaces trunk
Port        Mode         Encapsulation  Status        Native vlan
Gig0/1      desirable    n-802.1q       trunking      1

Port        Vlans allowed on trunk
Gig0/1      1-1005

Port        Vlans allowed and active in management domain
Gig0/1      1,10,20

Port        Vlans in spanning tree forwarding state and not pruned
Gig0/1      1,10,20
```

برای allow کردن vlanی(حذف کردن، اضافه کردن و...) به سوئیچ از دستور زیر استفاده می‌کنیم:

```
Switch(config)#interface fastEthernet 0/1
Switch(config-if)#switchport trunk ?
  allowed  Set allowed VLAN characteristics when interface is in trunking mode
  native   Set trunking native characteristics when interface is in trunking
           mode
Switch(config-if)#switchport trunk allow vlan ?
  WORD     VLAN IDs of the allowed VLANs when this port is in trunking mode
  add      add VLANs to the current list
  all      all VLANs
  except   all VLANs except the following
  none     no VLANs
  remove   remove VLANs from the current list
Switch(config-if)#switchport trunk allow vlan
```

Word یعنی **vlan** معرفی میکنم

Add یعنی یک **vlan** جدید اضافه میکنم

All یعنی همه **vlan** ها **trunk** باشند

Except یعنی همه به غیر از **vlan x**

None یعنی هیچ **vlan**ی

Remove یعنی پاک کردن **vlan x**

نکته: در صورت اضافه کردن vlan حتی باید از دستور add استفاده کنیم. در صورت عدم استفاده،vlan جدید روی vlanهای قبلی overwrite میشود.

```
Switch#show interfaces trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/1       on           802.1q         trunking      1
Gig0/1      auto         n-802.1q       trunking      1
Gig0/2      auto         n-802.1q       trunking      1

Port        Vlans allowed on trunk
Fa0/1       10
Gig0/1      1-1005
Gig0/2      1-1005

Port        Vlans allowed and active in management domain
Fa0/1       10
Gig0/1      1,10,20,400
Gig0/2      1,10,20,400

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/1       none
Gig0/1      1,10,20,400
Gig0/2      1,10,20,400
```

نتیجه نهایی مشخص میشود که سوئیچ ۱ با پورت f0/1 فقط Vlan 10 را از خود عبور میدهد.

نکته: در تعیین allow vlan میتوان vlanها را بصورت بازه‌ای مشخص کرد. مانند :

```
Switch(config-if)#switchport trunk allowed vlan 100-200
```

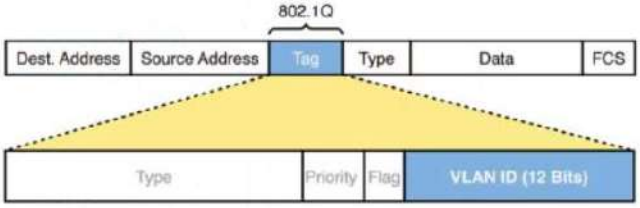
The 802.1Q and ISL VLAN Trunking Protocols:

ISL

- ISL is an Cisco proprietary protocol.
- Supports up to 1000 Vlans
- Original frame is encapsulated and a new header is inserted during encapsulation process.
- A 26 byte header and a 4 byte FCS (frame check sequence) are inserted. Hence a total of 30 Bytes of overhead.
- ISL tags frames from native Vlans.
- ISL is less preferred in networks because of its high overhead value which is added to each Ethernet frame.

802.1Q

- It is an IEEE Standard.
- 802.1q supports 4096 Vlans.
- IN 802.1q encapsulation process, a 4 byte tag is inserted into original frame and FCS (Frame Check Sequence) is re-calculated.
- 802.1q does not tag frames from native Vlans.



نکته۱: یکی از معایب پروتکل ISL مقدار بالای آن بود. (26+4=30B)

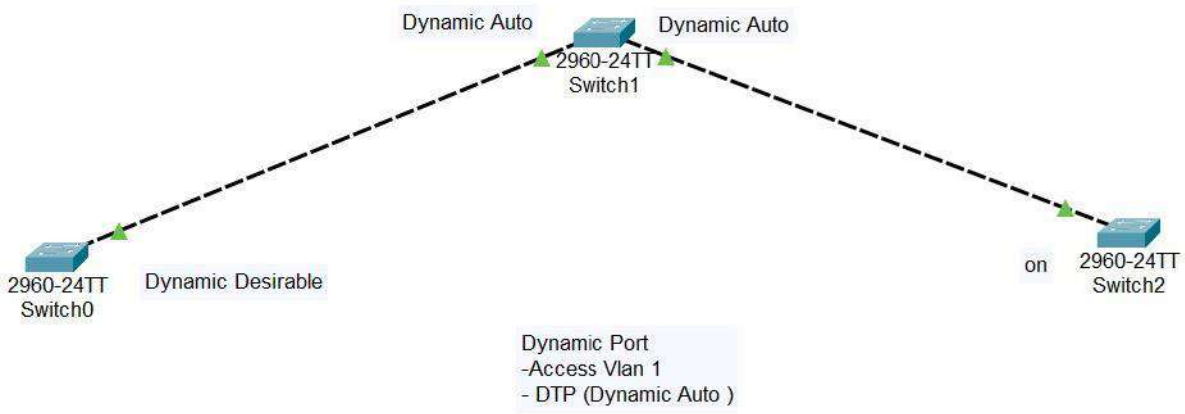
نکته۲: در هدر لایه دو تگ 1Q. قرار دارد که در این تگ ۱۲ بیت برای vlan اختصاص داده‌اند. که به اصلاح Tagزدن روی فریم‌ها گفته میشود.

نکته۳: همچنان برخی از سوئیچ‌های سیسکو ISL را ساپورت میکنند.

Types of trunk modes :

* پورت‌های سوئیچ Dynamic Port هستند. یعنی هم Access vlan1 می‌باشد(یعنی ترافیک vlan1 را از خود عبور دهد)، هم DTP(Dynamic trunk protocol) از نوع Auto (یعنی اگر درخواستی از طرف مقابل برای Trunking بیاید قبول میکند)روی هر پورت پیشفرض فعال است. ما وقتی دستورات switch mode access or Trunk را میدهیم، در واقع فقط ما قابلیت dynamic بودن را از پورت می‌گیریم ولی قابلیت negotiation را خیر(نکته امنیتی پورت). بهتر است mode هر پورت سوئیچ را مشخص کنیم که access است یا Trunk.

مثال برای فهم بیشتر حالت های مختلف Trunk شدن پورت‌ها:



در شکل بالا مشاهده می‌کنید که تمام پورت های سوئیچ‌ها dunamic auto میباشند.(در این حالت همه پورت‌های موجود همگی access میشوند(dynamic auto در مقابل dynamic auto دو طرف Access میشوند)). در ادامه پورت سوئیچ 0 را به حالت dynamic desirable پورت سوئیچ 2 را به حالت static Trunk(on) تبدیل می‌کنیم.

نکته: با دستورshow int g/01 switchport اطلاعات لایه دوئی قابل مشاهده است که اطلاعاتی از قبیل mode و negotiation موجود است.

```
Switch#show interfaces gigabitEthernet 0/1 switchport
Name: Gig0/1
Switchport: Enabled
Administrative Mode: dynamic auto
Operational Mode: static access
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: On
```

سطر سوم: یعنی این پورت لایه دو است

سطر چهارم: یعنی تنظیمات پیش فرض mode، dynamic auto بوده

سطر پنجم: یعنی modeای که در واقع برای این پورت اتفاق می‌افته

سطر ششم: یعنی از چه استانداردی استفاده میشه

سطر هشتم : یعنی قابلیت negotiation فعال است که می توان غیر فعالش کرد(در صورتی که نخواهیم از DTP استفاده کنیم).

سوئیچ 0 :

تغییر mode به desirable :

```
Switch(config)#int g 0/1
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
Switch(config-if)#switchport mode dynamic ?
  auto       Set trunking mode dynamic negotiation parameter to AUTO
  desirable  Set trunking mode dynamic negotiation parameter to DESIRABLE
Switch(config-if)#switchport mode dynamic desirable
```

مشاهده نتیجه تغییر mode :

```
Switch#show interfaces trunk
Port        Mode         Encapsulation  Status        Native vlan
Gig0/1      desirable    n-802.1q       trunking      1

Port        Vlans allowed on trunk
Gig0/1      1-1005

Port        Vlans allowed and active in management domain
Gig0/1      1

Port        Vlans in spanning tree forwarding state and not pruned
Gig0/1      1
```

سطر اول میگوید اینترفیس g0/1 با mode desirable، negotiation کرده و با 802.1q توافق رسیده و در نهایت Trunkشده است.

حال سوئیچ1 که desirable auto بود ، با توجه به درخواست پورت سوئیچ0 مبنی بر ایجاد ارتباط Trunk ، حال Trunk شده است . شکل زیر مشاهده می‌کنید(دستور روی سوئیچ 1) :

```
Switch#show int g 0/1 switchport
Name: Gig0/1
Switchport: Enabled
Administrative Mode: dynamic auto
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
```

سوئیچ 2 :

```
Switch#show interfaces trunk
Port        Mode         Encapsulation  Status        Native vlan
Gig0/1      auto         n-802.1q       trunking      1

Port        Vlans allowed on trunk
Gig0/1      1-1005

Port        Vlans allowed and active in management domain
Gig0/1      1

Port        Vlans in spanning tree forwarding state and not pruned
Gig0/1      1
```

تغییر mode به on :

```
Switch(config)#interface gigabitEthernet 0/2
Switch(config-if)#sw
Switch(config-if)#switchport mo
Switch(config-if)#switchport mode tr
Switch(config-if)#switchport mode trunk
```

مشاهده نتیجه تغییر mode :

```
Switch#show interfaces trunk
Port        Mode         Encapsulation  Status        Native vlan
Gig0/2      on           802.1q         trunking      1

Port        Vlans allowed on trunk
Gig0/2      1-1005

Port        Vlans allowed and active in management domain
Gig0/2      1

Port        Vlans in spanning tree forwarding state and not pruned
Gig0/2      1
```

سطر اول میگوید اینترفیس g0/1 سوئیچ 2 با mode static(on)، با استاندارد 802.1q توافق رسیده و در نهایت Trunkشده است.

حال سوئیچ1 که desirable auto بود ، با توجه به درخواست پورت سوئیچ2 مبنی بر ایجاد ارتباط Trunk ، حال Trunk شده است . شکل زیر مشاهده می‌کنید(دستور روی سوئیچ 1):

```
Switch#show interfaces gigabitEthernet 0/2 switchport
Name: Gig0/2
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
```

سوئیچ 1:

```
Switch#show interfaces trunk
Port        Mode         Encapsulation  Status        Native vlan
Gig0/1      auto         n-802.1q       trunking      1
Gig0/2      auto         n-802.1q       trunking      1

Port        Vlans allowed on trunk
Gig0/1      1-1005
Gig0/2      1-1005

Port        Vlans allowed and active in management domain
Gig0/1      1
Gig0/2      1

Port        Vlans in spanning tree forwarding state and not pruned
Gig0/1      1
Gig0/2      1
```

نتیجه نهایی mode سوئیچ ۱ را مشاهده میکنید.

دو پورت فعال با پورت مقابل خود negotiation کرده‌اند و encapsulation 802.1q را انتخاب کردند و در نهایت با توجه به گفتگوی دو طرفه، دو پورت های این سوئیچ trunk شده اند.

*نکته: در حالت access mode برای بحث امنیتی زمانیکه بخواهیم port را force کنیم تا با پورت دیگری به طور ناخواسته وارد negotiation نشود میتوانیم آن را با دستور زیر غیر فعال کنیم:

لازم است بدانیم پیشفرض negotiation فعال است. در صورت فعال کردن آن کافیست عبارت No را در ابتدای دستور زیر بیاوریم.

```
Switch(config)#int fastEthernet 0/1
Switch(config-if)#swi
Switch(config-if)#switchport ?
  access          Set access mode characteristics of the interface
  mode            Set trunking mode of the interface
  nonegotiate     Device will not engage in negotiation protocol on this
                  interface
  port-security   Security related command
  priority        Set appliance 802.1p priority
  protected       Configure an interface to be a protected port
  trunk           Set trunking characteristics of the interface
  voice           Voice appliance attributes
Switch(config-if)#switchport non
Switch(config-if)#switchport nonegotiate
```

Deleting settings and Valns in Cisco switches :

مشکل اینجاست که با حذف تنظیمات ذخیره شده در Startup configuration همه تنظیمات به غیر Vlan از بین می روند، پس به این معنی است که حذف تنظیمات پیکربندی شده روی سوئیچ چیز دیگر و حذف Vlan ها مقوله دیگری است. البته با حذف Startup configuration، تمامی پورت‌های سوئیچ که عضو Vlan های دیگری هستند از آن Valn ها حذف می‌شوند و به Vlan پیشفرض خود سوئیچ انتقال پیدا می کنند ولی خود VLANهای ایجاد شده(که با نام فایل Vlan.dat را که در حافظه Flashسوئیچ وجود دارد) حذف نمی‌شوند و باید دستی آنها را خودتان حذف کنید.

اگر دستورshow flash را در مود privilege اجرا کنید، این فایل را مشاهده خواهید کرد(البته اگر روی سوئیچ Vlan ای وجود داشته باشد).

```
Switch#show flash:
Directory of flash:/

    1  -rw-     4670455          <no date>  2960-lanbasek9-mz.150-2.SE4.bin
    3  -rw-         616          <no date>  vlan.dat
```

1) Deleting the switch configuration

ما فقط باید تنظیمات ذخیره شده در startup-configuration را حذف کرده و سوئیچ را ریستارت کنیم. همانطور که مشاهده می کنید، کافیست در مود privilegeدستور زیر را اجرا کنید. پس از اجرای دستور زیر، پیغام تایید حذف را هم Enter کنید. بدین ترتیب کلیه تنظیمات از nvram حذف شدند ولی هنوز در Runing-config این تنظیمات وجود دارد که کافیست فقط سوئیچ را ریستارت کنید تا کاملا از بین برود. پس با دستور Switch#reload سوئیچ را ریستارت می کنیم.

```
Switch#erase startup-config
```

2) Deleting the switch Vlans

در این مرحله نوبت به حذف Vlan ها می رسد. چون اگر دستور زیر را اجرا کنید، خواهید دید که Vlan ها حذف نمی شوند. همچنین مشاهده میشود که اصلا پورتی در عضویت این Vlan ها نیست ولی خود Vlan ها حذف نشده اند.

```
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
10   VLAN0010                         active
```

شما می توانید این فایل را از حافظه flash سوئیچ حذف کرده و سوئیچ را reload کنید تا Vlan ها حذف شوند. برای این منظور از دستور زیر استفاده کنید.

```
Switch#delete vlan.dat
```

اگر دوباره دستور Show flash را اجرا کنید، می بینید که هیچ اثری از فایل Vlan.dat نیست.

```
Switch#show flash:
Directory of flash:/

    1  -rw-     4670455          <no date>  2960-lanbasek9-mz.150-2.SE4.bin
```

VLAN Trunk Protocol (VTP) :

زمانی که قصد ساختن vlan ها را داریم انجام این عملیات در شبکه هایی که تعداد سوییچ های آن زیاد باشد , معرفی اینvlan ها به تک‌تک سوئیچ‌ها کاری بسیار دشوار و زمانبر است. برای حل این مساله سیسکو اقدام به معرفی پروتکلی به نام vtp نمود. کار vtp انتقال vlan های مختلف به سوئیچ هایی است که در جوار یکدیگر قرار دارند که به آن vtp domain میگویند. این پروتکل اختصاصی سیسکو است(Cisco Proprietary) که به طور کل از آن برای تبادل اطلاعات دیتابیس VLAN بین سوئیچ های یک VTP دامین استفاده می‌شود.

پروتکلی است client-serverی که مخصوص سیسکوست. در این روش یک سوئیچ به عنوان سوئیچ مرجع و مابقی سوئیچ‌ها به عنوان سوئیچ مقلد معرفی می‌شوند. به طور کل هر تنظیماتی که روی سوئیچ مرجع(server) اعمال کنیم، روی سوئیچ‌های مقلد(client) هم اعمال خواهد شد.

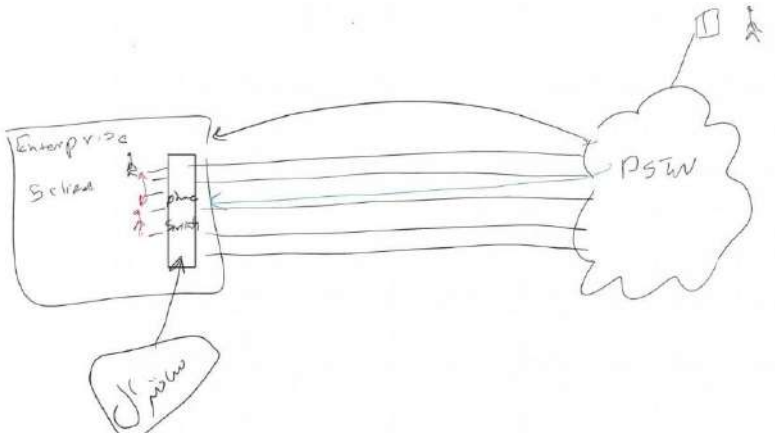
VTP Pruning :

قابلیتی است که می‌توان به وسیله آن ترافیک اضافه مثل Broadcast را کاهش داد. به این صورت که سوئیچ تمام پورت های Trunk خود را چک می کند و مشخص می‌کند که از هر پورت به چه VLAN هایی می رسد. به طور پیش فرض این ویژگی غیر فعال است. در صورت فعال کردن این ویژگی روی یک سوئیچ این ویژگی بر تمام سوئیچ‌های دامین فعال خواهد شد.

Voice Vlan :

قدیم الایام به عنوان مثال وقتی یک شرکت enterprise در سطح Lan با ۵ user داشتیم، برای ارتباط تلفنی یوزرها، ما باید ۵ خط تلفن از PSTN(مخابرات) خریداری میکردیم. مخابرات تا شرکت ٤ سیم دودویی می‌آورد، آنوقت ما هم این ۵ سیم را به داخل شرکت منتقل میکردیم. در نهایت به ازای هر user یک تلفن با شماره خط متفاوت اختصاص میدادیم. دو مشکل داشتند: ۱) اگر از بیرون به یکی از این userها تماس گرفته میشد خط busy(مشغول) میشد و باقی‌userها نمی‌توانستند تماس بگیرند. ۲) اگر user1 و user2 قصد داشتند تماس داخلی برقرار کنند، ترافیک به pstn میرفت و برمیگشت که این عمل هزینه‌ساز بود(cost).

به همین دلیل به سراغ دستگاهی (phone swich) رفتند که مشکلات cost و busy را نداشت که به نمونه ای متداول آن به نام سانترال می‌توان اشاره کرد.

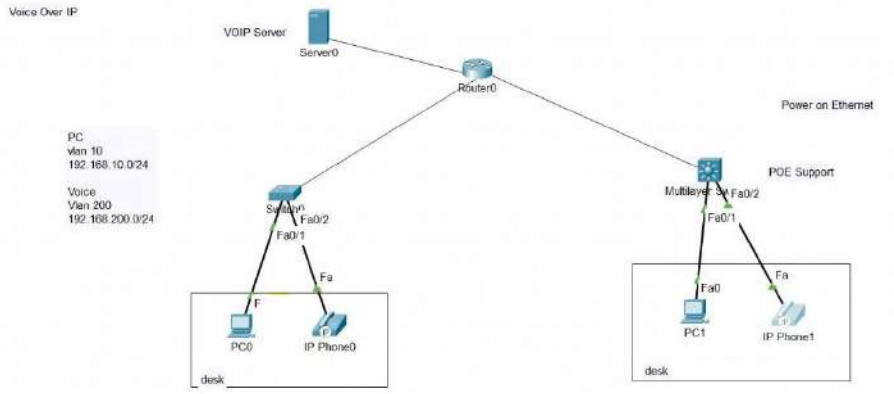


نکته ای که باید توجه میشد این بود که ما برای هر user برای اتصال به این سانترال، باید متراژ بالایی کابلی کشی می‌کردیم(که هزینه‌ور بود). نکته بعد اینکه ما اگر میخواستیم این شبکه را به عنوان مثال تبدیل به شبکه WAN با ۲۰۰۰ user در مکان‌های متفاوت میکردیم، آیا این روش جوابگو بود؟ خیر. چون این سیستم تا حدی قابل گسترش هستند و منطقی نبود.

به همین منظور سیسکو برای حل این مشکل، تلفنی(IP Phone) را طراحی کرد که آنالوگ نیست وTCP/IPمی‌فهمد(چون قرار استData جابجا شود).

تلفن‌های سیسکو برای این که بتوانند VLANهای ساخته شده روی سوییچ را بفهمند و اطلاعات را متناسب با آن VLANها ارسال و دریافت کنند ، از قابلیت CDP که مختص تجهیزات سیسکو می‌باشد استفاده می‌کنند . این بدان معناست کهIP Phone تگ vlan میفهمد. CDP مخفف عبارت Cisco Discovery Protocol می‌باشد که به تجهیزات سیسکو این امکان را می‌دهد تا اطلاعاتی را از همسایگان سیسکویی خود به دست آورند . بنابراین اگر این قابلیت روی سوییچ شما فعال نیست کافیست به زیر پورت‌های مربوطه رفته و کامند cdp enable را وارد کنید .

مثال:

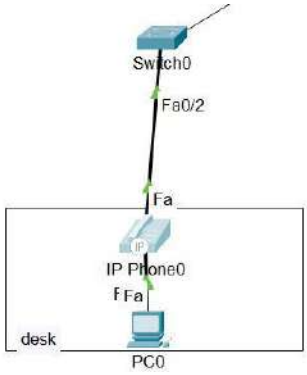


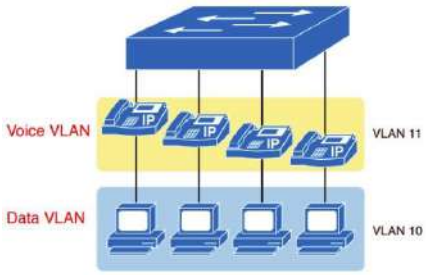
Config سوئیچ0 :

ساخت vlanهای مورد نیاز و access کردن Port ها به vlanهای خود.

** نکته:

در بسیاری از سازمان‌ها برای هر کاربر تنها یک نود شبکه یا یک کابل شبکه در نظر گرفته می‌شود ، بنابراین در چنین مواردی امکان اتصال تلفن و کامپیوتر کاربران به دو پورت یا دو VLAN جداگانه وجود ندارد . درست در همین نقطه می‌توانیم به کمک Voice VLAN این مشکل را حل کنیم. برای این منظور تلفن‌های ویپ عموما دو پورت اترنت در بخش پشتی خود دارند ، یکی از پورت‌ها برای اتصال تلفن به سوییچ شبکه بوده و دیگری برای اتصال کامپیوتر کنار تلفن به بستر شبکه در نظر گرفته شده است.





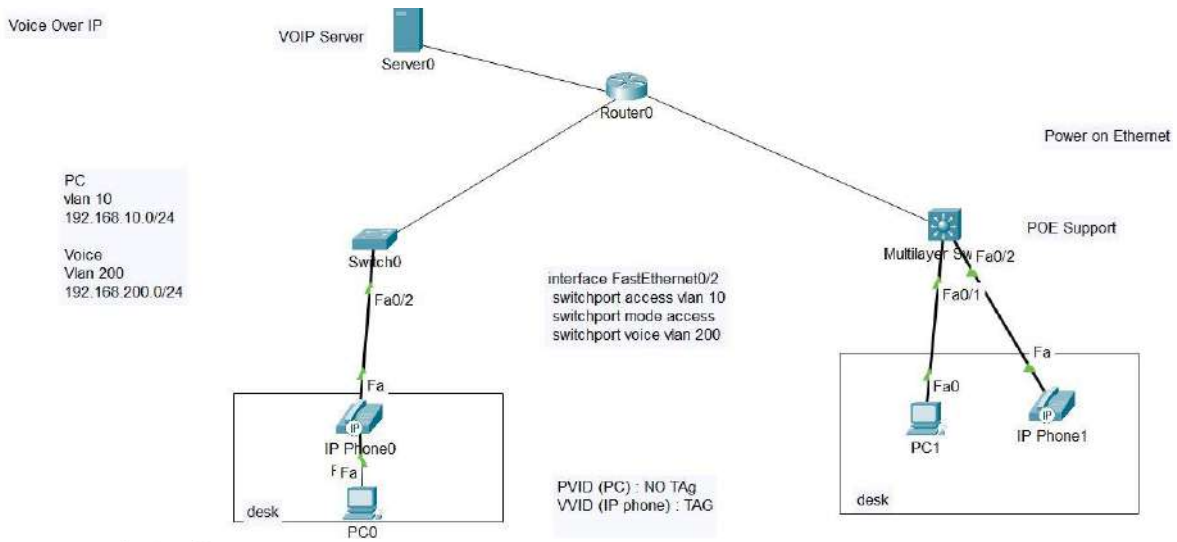
زمانی که شما کامپیوتر و تلفن کاربران را به صورت ذکر شده به سوییچ سازمان متصل می‌کنید، تلفن شما در حقیقت نقش یک سوییچ دو پورت را برای شما بازی می‌کند و این تلفن با ایجاد یک ارتباطی که شاید بتوان آن را مینی ترانک نامید ، ارتباط Data و Voice شما را به صورت جداگانه روی VLANهای مربوطه برقرار می‌کند.

نکته۱: معمولا برای این که سرعت UP شدن پورت سوییچ بالا برود ، کارشناسان شبکه قابلیت PortFast را روی پورت‌هایی که به تلفن و کامپیوترها متصل است فعال می‌کنند .(به یاد داشته باشید که فعال کردن PortFast روی پورت‌هایی که به سوئیچ‌ها یا برخی دیگر از تجهیزات شبکه متصل هستند می‌تواند برای شبکه مخرب باشد ، بنابراین این قابلیت را فقط روی پورت‌های متصل به کامپیوتر و تلفن فعال کنید.)

نکته۲: زمانی که در سناریو خود از تلفن غیر سیسکویی استفاده می کنید، به دلیل غیر فعال بودن پروتکل CDP باید کامنت‌های Voice vlan را وارد نمایید.

نکته۳: IP Phoneها به دو صورت روشن می‌شوند: ۱) توسط adaptor ۲) استفاده از قابلیت poe برخی سوئیچ‌ها(Poe support)

مثال:



می‌دانیم که سوئیچ یا access mode است یا Trunk. وقتی به pc متصل می‌شود، چون PC درک و فهمی از Tag و unTag ندارد، پس باید پورت سوئیچ Access باشد. حال طبق مثال، چطور پورت بفهمد ترافیکی که به سمتش می‌آید، برای PC است یا IP phone؟

از طرفی هم می‌دانیم که سوئیچ اگر access میشود، فقط می‌تواند Access یک vlan باشد. اما به طور استثنا سوئیچ سیسکو می‌تواند همزمان به طور جداگانه Access دیتا و voice شود.

طبق دستورات زیر عمل میکنیم:

```
Switch(config)#interface fastEthernet 0/2
Switch(config-if)#switchport mode access

Switch(config-if)#switchport access vlan 10
Switch(config-if)#switchport voice vlan 200
```

show running-config که گرفته شود مشاهده می‌شود که در این interface دو Vlan، Access شده‌اند که data و voice به طور همزمان منتقل می‌شوند.

```
interface FastEthernet0/2
 switchport access vlan 10
 switchport mode access
 switchport voice vlan 200
```

با بررسی اطلاعات لایه دوئی سوئیچ هم نشان می‌دهد که این interface access vlan100، و voice vlanی هم که دارد ۲۰۰ است.

```
Switch#show interfaces fastEthernet 0/2 switchport
Name: Fa0/2
Switchport: Enabled
Administrative Mode: static access
Operational Mode: static access
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: 10 (VLAN0010)
Trunking Native Mode VLAN: 1 (default)
Voice VLAN: 200
```

نکته: دیتایی که از طرف pc به سمت سوئیچ حرکت میکند بدون Tag است. یعنی وقتی به ip phone میرسد بدون tag است و ip phone نیز دیتای آن را بدون tag به سوئیچ ارسال میکند که سوئیچ متوجه ارسال ترافیک از pc می‌شود. که اصطلاحاً به آن **PVID** (Port vlan ID) گویند. همچنین IP Phone نیز دیتای خود را با Tag به سوئیچ ارسال میکند که سوئیچ متوجه ارسال Data از IP phone میشود. که اصطلاحاً به آن **VVID** (Voice vlan ID) می‌گویند.

خطوط دیجیتال:

- ✓ خط E1 : این خط معادل اروپایی خط T1 آمریکایی است . نرخ انتقال داده آن 2/048 mbps است. دارای ۳۲ کانال kbps64 است که ۳۰ عدد از کانال‌ها برای انتقال صوت و دو عدد دیگر برای همگام‌سازی و سیگنال‌دهی استفاده میشود.
- ✓ خط T1: در ژاپن و آمریکا استفاده می‌شود، نرخ انتقال داده آن 1/544 mbps بوده و ۲۴ کانال صوتی دارد.

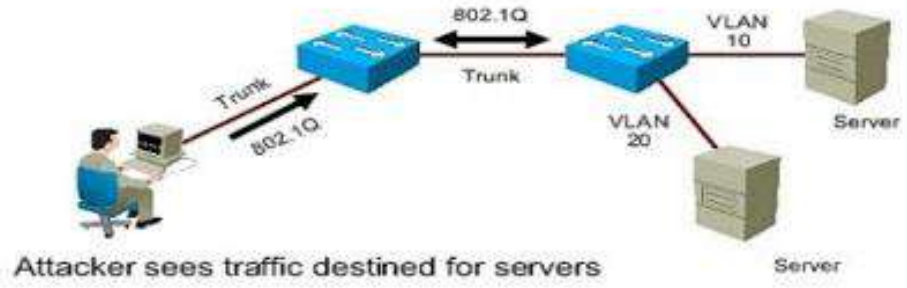
Native Vlan :

وقتی در سوئیچ‌ها اقدام به ساخت vlan و فعال‌سازی پروتکل802.1q می‌کنیم، به فریم‌های داده یک هدر اضافه می‌شود که دارای یک tag مربوط به vlan خاص خود می‌باشد، اما اگر در این شبکه فریمی وجود داشته باشد که دارای این هدر نیست باید به Vlan ای منتصب شود که این فریم‌ها متعلق به آن است که به این native vlan گفته می‌شود. این اتفاق زمانی رخ می‌دهد که پورت در حالت Trunk باشد و از پروتکل 802.1q استفاده کند. معمولاً native vlan ها همان vlan های شماره یک هستند که بصورت پیش فرض بر روی سوئیچ‌ها وجود دارد.

به معنای دیگر در صورتی که Native Vlan بر روی یک پورت به صورت مثال ۱ تعریف شده باشد در صورتی که پکتی از آن پورت وارد سوییچ شود و دارای tag مربوط به Vlan ها نباشد آن را جزو پکتهای مربوط به Vlan 1 در عملیات switching به حساب می‌آورد. این vlan دارای یک مشکل بزرگ امنیتی است که میتوان آن را هک کرد که به آن vlan hopping گفته می‌شود.

VLAN Hopping :

VLAN Hopping یکی از تکنیک‌های حمله و تست نفوذ در شبکه است که به مهاجم اجازه می‌دهد تقسیم‌بندی‌های شبکه را دور بزند. روشی برای حمله به شبکه با ارسال بسته ها به پورت است.



- این حمله در دو صورت Switch Spoofing و double tagging قابل انجام میشود:

- **Switch Spoofing:**

این حمله زمانی قابل انجام است یک پورت سوییچ متصل شده به یک end-device مانند کامپیوتر و لپ تاپ درحالت trunk قرار داشته باشد در این صورت فرد مهاجم با ارسال ترافیک‌های مخرب موجب میتواند به دیگر vlan ها دسترسی پیدا کند و حمله MITM صورت گیرد.

نکته*: در سوییچ پورت ها به صورت Default درحالت Dynamic قرار دارند و فرد مهاجم با مذاکره به سوییچ می تواند آن پورت را در حالت trunk قرار دهد.

نحوه جلوگیری: ۱) غیر فعال کردن ترانک پورت های متصل به سوییچ به سمت end-device ها (تبدیل به access mode) ۲) جلوگیری از امکان DTP (dynamic trunk protocol)

```
Switch1(config)# interface gigabitethernet 0/3
Switch1(config-if)# switchport mode access
```

&

```
Switch1(config)# interface gigabitethernet 0/4
Switch1(config-if)# switchport trunk encapsulation dot1q
Switch1(config-if)# switchport mode trunk
Switch1(config-if)# switch port nonegotiate
```

- **Double tagging:**

در native vlan ها که بصورت پیش فرض vlan 1 هستند بسته ها بدون tag ارسال میشوند ،در صورتی که Native Vlan بر روی یک پورت تعریف شده باشد وقتی که پکتی از آن پورت وارد سوییچ شود و دارای tag مربوط به Vlan ها نباشد آن را جزو پکتهای مربوط به Vlan 1در عملیات سوییچینگ به حساب می آورد.Vlan1 در تمامی سوئیچ ها بدون معرفی قابل عبور می باشد.

در اینجا هکر به vlan1 رفته وکنار تگ۱ یک تگ ۱۰ میچسباند , سویچ هنگام process به تگ ۱۰ نگاه میکند و انرا به سمته vlan10 هدایت میکند. برای جلوگیری از این کار میتوان native vlan را از vlan1 تغییر داد ویا Native vlan را با تگ ارسال کنیم. این تگ باید طوری انتخاب شود که بعدها قابل استفاده نباشد.

نحوه جلوگیری: برای جلوگیری از حملات Vlan-hopping با استفاده از قابلیت double tagging از قابلیت Native VLAN برای ارسال ترافیک کاربر استفاده نکنید. اینکار را می توانید با ایجاد یک VLAN که هیچ پورتی به آن اضافه نشده است انجام دهید و از این VLAN فقط برای استفاده به عنوان Native VLAN باشد (Native VLAN نیز با Tag ارسال شود.)

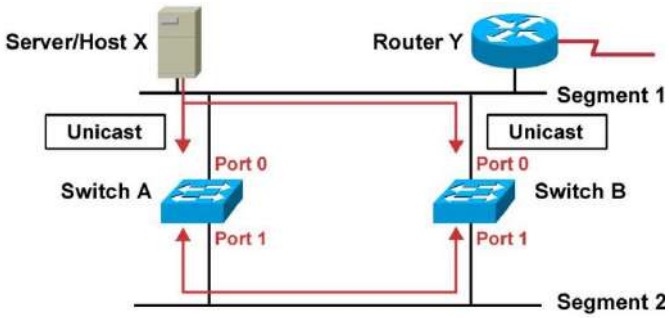
```
Switch1(config)# interface gigabitethernet 0/4
Switch1(config-if)# switchport trunk native vlan 400
```

«ابزارهای هک امنیت شبکه»

Yersiniaیکی از محبوب‌ترین ابزارهای هک امنیت شبکه برای سیستم عامل‌های مشابه یونیکس است. هدف اصلی این ابزار هک VLANو سوءاستفاده از نقاط ضعف در پروتکل‌های شبکه زیر است:

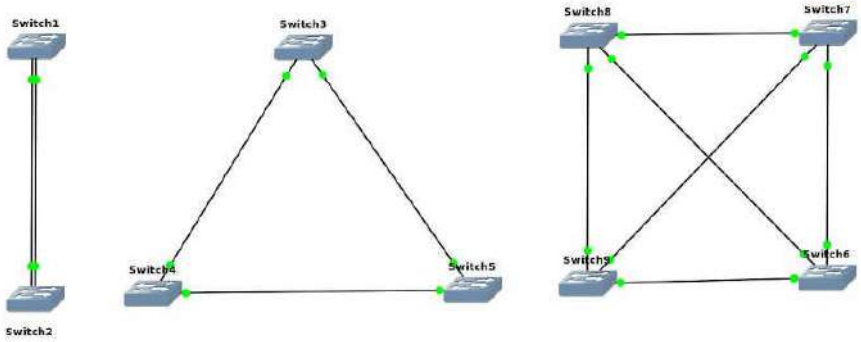
- Cisco Discovery Protocol
- Cisco Inter-Switch Link
- DTP
- Dynamic Host Configuration Protocol
- Hot Standby Router Protocol
- IEEE 802.1Q
- IEEE 802.1X
- Spanning Tree Protocol
- VLAN Trunk Protocol

Loop :



در شکل روبرو، ServerX در حال ارسال Frame به RouterY 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.

به طور کلی هرگاه چند Switch را طوری به یکدیگر متصل کنیم که یک حلقه بسته به وجود بیاید ، می‌گوییم یک Loop ایجاد شده است.



Spanning Tree (STP) :

:STP Concepts

STP پروتکل جلوگیری از Loop (Loop detection) در لایه دو می‌باشد.

اگر در یک LAN که دارای مسیر های redundant می‌باشد، پروتکل STP فعال نباشد، loopهای نامحدودی در شبکه به وجود می آید که این امر می تواند باعث down شدن شبکه شود. در حالی که اگر در همان LAN پروتکل STP فعال باشد، سوئیچ ها برخی از پورت ها را بلاک می کنند و اجازه عبور اطلاعات از آن پورت ها را نمی‌دهند تا در شبکه loop ایجاد نشود.

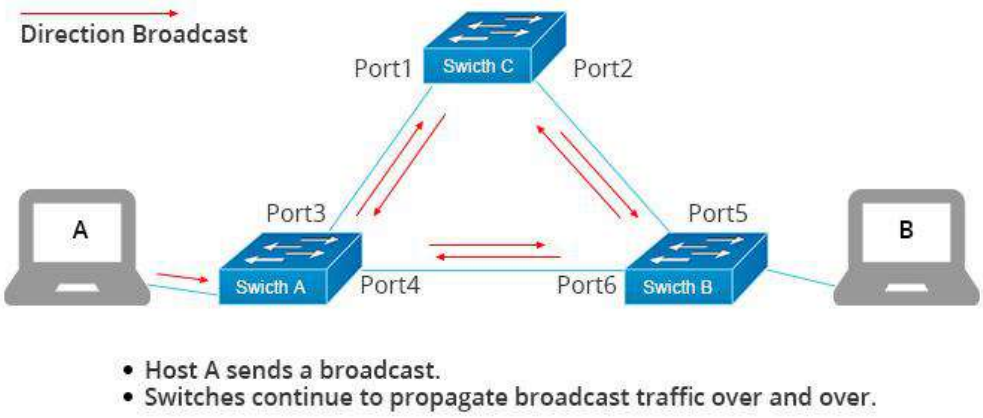
بدون استفاده از STP همه این لینک های redundant (اضافی) همزمان با هم فعال هستند. و باعث به وجود آمدن مشکلات زیادی می‌شوند ازجمله :

مشکل	توضیحات
Broadcast storm	ارسال مکرر یک frame بر روی یک لینک، ظرفیت قابل ملاحظه ای از لینک را اشغال می کند
MAC table instability	به روزرسانی مکرر جدول مک آدرس سوئیچ ها با ورودی های اشتباه بر اثر چرخش frameها، که باعث ارسال frameها به مقصد اشتباه می شود
Multiple frame transmission	یکی از جنبه های تاثیرات چرخش frameها که باعث می شود کپی های مختلفی از frame به مقصد برسد و آن device را گیج کند

❖ **Broadcast Storm** یا طوفان **Broadcast**:

زمانی که در یک شبکه دارای Loop بسته ای Broadcast می شود ، تا بینهایت بین Switch ها منتقل می‌شود و همینطور تعداد آن افزایش میابد. این عمل آنقدر ادامه پیدا می کند که یک Broadcast storm ایجاد می شود. افزایش این بسته های Broadcast منابع زیادی از Switch های ما را اشغال می کند و باعث افزایش بار شبکه می شود که در نهایت باعث کندی یا قطعی شبکه شود.

زمانی که یک Broadcast storm اتفاق میوفتد، frameها مانند مثال پایین به چرخیدن ادامه می‌دهند تا زمانی که تغییراتی به وجود آید (مثلاً شخصی یکی از پورت ها را خاموش کند، سوئیچ را reload کند یا کاری کند که loop از بین برود).



❖ **MAC Address Table Instability** یا ناپایداری جدول مک آدرس:

همانطور که دیدید Frame ها در شبکه هایی که دارای Loop هستند مدام می چرخند. به همین دلیل جدول Mac Address سوئیچ ها همیشه درحال آپدیت شدن به صورت اشتباه است.

مثلا در شکل بالا اگر کامپیوتر A با مک آدرس AAA یک بسته Broadcast را با استفاده از پورتی که به سوئیچ A متصل است در شبکه ارسال کند ، این بسته وارد یک Loop می شود. زمانی که همین بسته دوباره وارد port3 سوئیچ A می شود. سوئیچ دوباره جدول Mac Address خودرا آپدیت می‌کند. زیرا مک آدرس AAA را روی port3 خود دریافت کرده است. که این عمل باعث ناپایدار شدن جدول مک آدرس سوئیچ ها می شود. که می تواند باعث ارسال Frame ها به مقصد اشتباه شود.

مثال دیگر: همانطور که در شکل پایین مشاهده می‌کنیم، sw3 مک آدرس Bob را از Fa0/13 به mac address table خود اضافه کرده است. حالا فرایند switch learning را در نظر بگیرید، frame ارسالی پس از یک دور چرخیدن از طریق پورت Gi0/1 وارد سوئیچ SW3 می‌شود. سوئیچ SW3 متوجه می‌شود که frame وارد شده از پورت Gi0/1، مک آدرس مبداءBob را دارد، بنابراین جدول مک آدرس خود را به روز می‌کند. پس از به روز رسانی جدول مک آدرس، سوئیچ SW3 هم دیگر نمی‌تواند به درستی frameها را به سیستم Bob برساند. برای مثال در این حالت اگر یک frame که مقصد آن Bob باشد به سوئیچ SW3 برسد (خارج از frameهایی که در داخل loop افتاده اند) ، سوئیچ SW3 به اشتباه frame را روی پورت Gi0/1 به سوئیچ SW1 ارسال می‌کند ، نتیجه ی این اشتباه یک loop است که ترافیک زیادی را در شبکه ایجاد می‌کند.

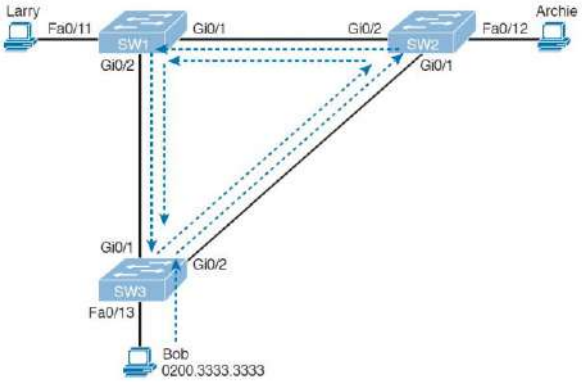
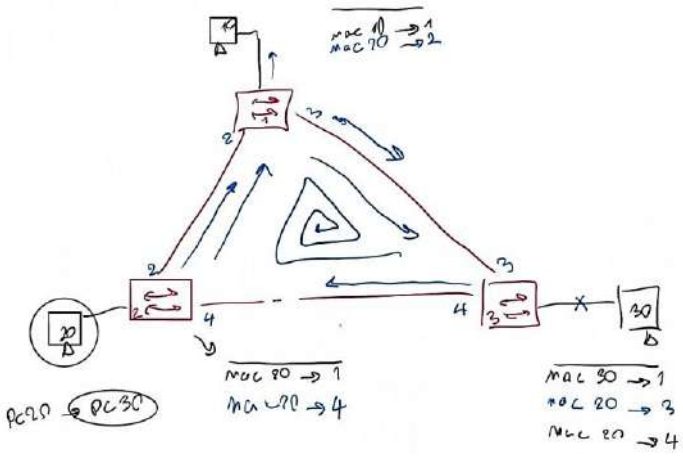


Figure 2-1 *Broadcast Storm*

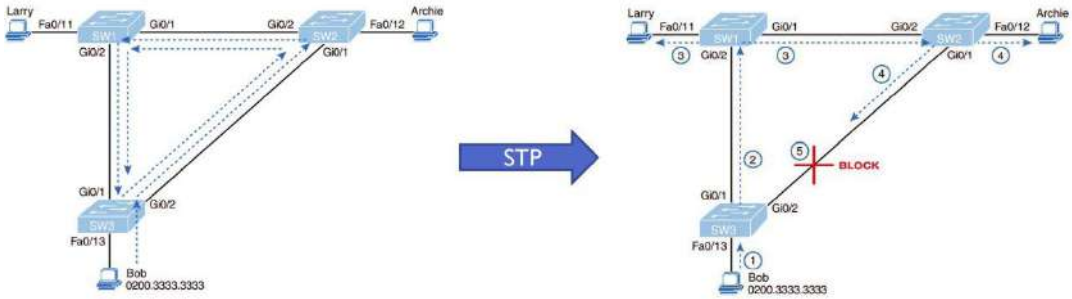
❖ **Multiple Frame Transmission** :

یکی دیگر از مشکلاتی که Loop در شبکه ایجاد میکند ، Multiple Frame Transmission می باشد. یعنی ممکن است یک Frame چندین بار به دست یک Device در شبکه برسد و مشکلاتی را به وجود آورد.



What Spanning Tree Does:

پس ما برای حل این مشکلات، نیاز به پروتکلی به نام STP داریم که طبق الگوریتمی Physical همین ارتباط برقرار باشد ولی به صورت logical یکی از لینک ها(portها) را به صورت موقت Block میکند . تا loop اتفاق نیافتد.



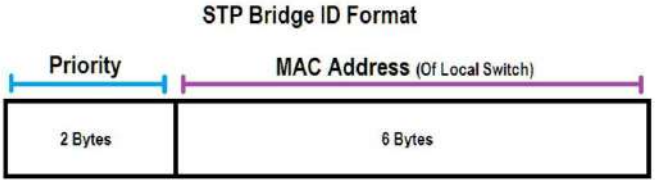
نکته: توجه کنید که وضعیت STP یک پورت، دیگراطلاعات مربوط به پورت را تغییر نمی‌دهد. برای مثال با تغییر وضعیت خود تغییری در وضعیت های trunk/access و connected/not-connectedایجاد نمی‌کند. وضعیت STP یک مقدار جدا از وضعیت های قبلی دارد و اگر در حالت بلاک باشد پورت را از پایه غیر فعال می‌کند .

How Spanning Tree Works:

(نحوه عملکرد STP)

فرآیند STA (spanning tree algoritm) با انتخاب یک سوئیچ به عنوان root شروع می‌شود. برای اینکه روند انتخاب را بهتر متوجه شوید، شما باید با مفهوم پیام هایی که بین سوئیچ ها تبادل می‌شود و فرمت شناساگری که برای شناسایی هر سوئیچ استفاده می‌شود آشنا شوید:

Bridge ID (BID) : یک مقدار ۸ بایتی(٦٤بیتی) برای شناسایی هر سوئیچ می‌باشد. Bridge ID به دو بخش ۲ بایتی (Priority) که مشخص کننده اولویت و حق تقدم است و ٦ بایتی که system ID نامیده می‌شود و همان مک آدرس هر سوئیچ(مک آدرس interface vlan1) است، تقسیم می‌شود. استفاده از مک آدرس این اطمینان را می‌دهد که bridge ID هر سوئیچ یکتا خواهد بود.




```
Switch#show interfaces vlan 1
Vlan1 is administratively down, line protocol is down
  Hardware is CPU Interface, address is 000a.41d5.7c52 (bia 000a.41d5.7c52)
```

نکته: Priority دو بایت(١٦ بیت) است. یعنی 2^{16} حالت (که میشود ٦٥٥٣٦). مقدار Priority در سوئیچ‌های سیسکو به صورت پیشفرض ٣٢٧٦٩(٣٢٧٦٨+١) میباشد. از آنجایی که مک آدرس سوئیچ ها معیار مناسبی برای انتخاب سوئیچ root نمی‌باشد بهتر است به صورت دستی مقدار اولویت را تغییر دهیم تا سوئیچی که می‌خواهیم، به عنوان سوئیچ root انتخاب شود. (٠ تا ٦٥٥٣٥). البته باید این اعداد مضربی از 4996 باشد.

Table 10-3 STP/RSTP Configurable Priority Values

Decimal Value	16-bit Binary Equivalent	Decimal Value	16-bit Binary Equivalent
0	0000 0000 0000 0000	32768	1000 0000 0000 0000
4096	0001 0000 0000 0000	36864	1001 0000 0000 0000
8192	0010 0000 0000 0000	40960	1010 0000 0000 0000
12288	0011 0000 0000 0000	45056	1011 0000 0000 0000
16384	0100 0000 0000 0000	49152	1100 0000 0000 0000
20480	0101 0000 0000 0000	53248	1101 0000 0000 0000
24576	0110 0000 0000 0000	57344	1110 0000 0000 0000
28672	0111 0000 0000 0000	61440	1111 0000 0000 0000

چرا Priority پیشفرض (۳۲۷۶۸+۱=۳۲۷۶۹) میشود؟ با توجه به جدول بالا و شکل زیر، Priority از دو قسمت تشکیل شده است. اگر بیت های Prioriy را کنار هم قرار دهیم (مانند شکل بالا)، ٤ بیت اول متعلق به حالت های Priority multiple می‌باشد که ۱٦=2^4 حالت دارد، مابقی بیت‌ها هم متعلق به شماره Vlan(به اصلاح System id extension گفته میشود).

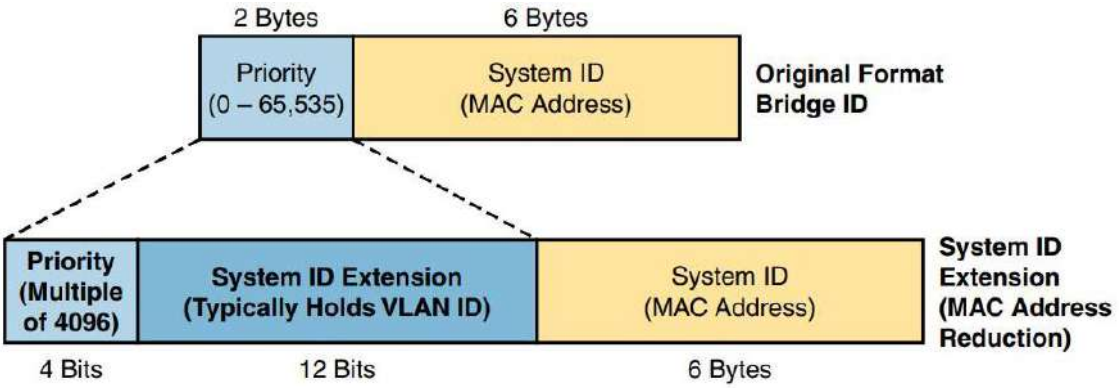


Figure 10-4 *STP System ID Extension*

جواب سوال: چون در سوئیچ ها به صورت پیشفرض vlan1 ساخته شده، به همین دلیل هنگام محاسبه priority ، شماره vlan (۱) را به Priority multiple اضافه میکند. باینری و نحوه محاسبه vlan20 و vlan1به صورت زیر میشود:

32788= (2^{15}+0+0+0+0+0+0+0+0+0+0+2^4+0+2^2+0+0) 1000 0000 0001 0100 vlan20

32769= (2^{15}+0+0+0+0+0+0+0+0+0+0+0+0+0+0+1) 1000 0000 0000 0001 vlan1

BPDU (Bridge Protocol Data Unit) : پیام هایی که برای تبادل اطلاعات مربوط به پروتکل STP بین سوئیچ ها استفاده می شود، BPDU نام دارد. رایج ترین BPDU ، که Hello BPDU نام دارد، تعدادی از اطلاعات که شامل BID سوئیچ ها نیز می‌شود را لیست و ارسال می‌کند. با استفاده از BID درج شده روی هر پیام، سوئیچ ها می‌توانند تشخیص دهند که هر پیامHello BPDU از طرف کدام سوئیچ است.

مثال زمانیکه یکی از لینک‌ها down می‌شود و یا یک لینک جدید اضافه می شود یا یک سو یچ جدید اضافه می‌شود و درنهایت یکی از سوئیچ های شبکه fail می‌شود ، سوئیچ های لایه دو با استفاده از Frameهای BPDU همدیگر را از به وجود آمدن چنین شرایطی آگاه می‌کنند، با استفاده از این اطلاعات جدید الگوریتم STP مجدداً شروع به کار و اجرا می‌کند و توپولوژی جدید بدون Loop را ایجاد می کند. STP و BPDU به سریعتر شدن فرآیند Convergence در مسیریابی بین شبکه ای بسیار کمک می کنند. Convergence در واقع مدت زمانی است که شبکه باید تغییرات جدید را تجزیه و تحلیل و تغییرات جدید را اعمال و اجرایی کند. به فرآیند ایجاد و ارسال کردنFrame های BPDU در اصطلاح فنی BPDU Advertisementگفته می‌شود.

جدول زیر اطلاعات کلیدی مربوط به Hello BPDU را نشان می‌دهد:

Table 9-4 Fields in the STP Hello BPDU

Field	Description
Root bridge ID	The bridge ID of the switch the sender of this Hello currently believes to be the root switch
Sender's bridge ID	The bridge ID of the switch sending this Hello BPDU
Sender's root cost	The STP/RSTP cost between this switch and the current root
Timer values on the root switch	Includes the Hello timer, MaxAge timer, and forward delay timer

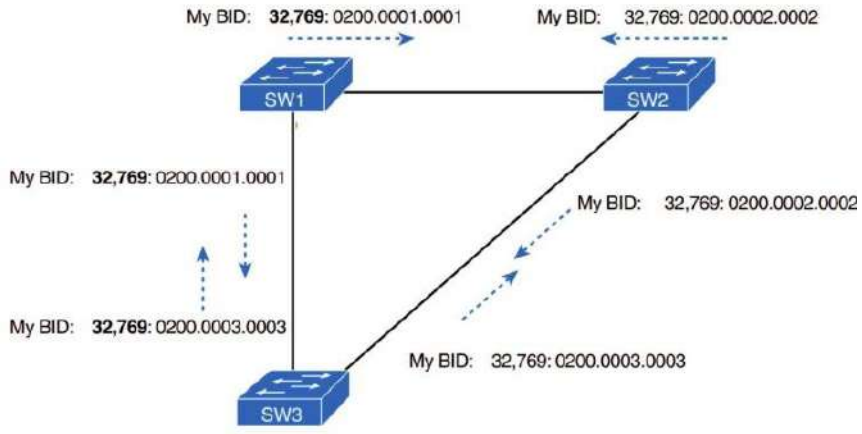
مواردی که باید در STP انتخاب شود:

1 - Elect Root Bridge [RB] -> Lowest BID

سوئیچ ها در شروع به‌گونه‌ای عمل می‌کنند که انگار آنها Root Bridge هستند و بسته‌های اطلاعاتی Root Bridge یا همان BPDU را هر دو ثانیه یک‌بار ارسال می‌کنند و سعی می کنند خود را به عنوان سوئیچ root (RB) به سوئیچ های مجاور خود معرفی کنند.

پس چگونه برنده و بازنده مشخص می‌شود؟

سوئیچ ها با استفاده از BIDهای موجود در پیام های BPDU، سوئیچ root را انتخاب می‌کنند. سوئیچی که عدد BID آن مقدار کمتری را داشته باشد به عنوان سوئیچ root انتخاب می‌شود. با توجه به اینکه بخش اول عدد BID مقدارPriority می‌باشد، سوئیچی که مقدار Priority پایین تری داشته باشد به عنوان سوئیچ root انتخاب می‌شود. برای مثال اگر سوئیچ های اول و دوم به ترتیب دارای Priority های ٤٠٩٦ و ٨١٩٢ باشند، بدون در نظر گرفتن مک آدرس سوئیچ ها که در به وجود آمدن BID هر سوئیچ موثر است، سوئیچ اول به عنوان سوئیچ root انتخاب خواهد شد و اگر مقدار Priority دو سوئیچ برابر شد، سوئیچی که مک آدرس آن مقدار کمتری را داشته باشد به عنوان سوئیچ root انتخاب می‌شود. در این حالت به علت یکتا بودن مک آدرس، حتما یک سوئیچ انتخاب خواهد شد. پس اگر مقدار Priority دو سوئیچ برابر باشد و مک آدرس آنها ۰۲۰۰,۰۰۰۰,۰۰۰۰ و ۰۹۱۱,۱۱۱۱,۱۱۱۱ باشد، از سمت چک نظیر به نظیر مقایسه می‌شود و سوئیچی که دارای مک آدرس ۰۲۰۰,۰۰۰۰,۰۰۰۰ است، به عنوان سوئیچ root انتخاب می‌شود، چون کاراکتر دومش کمتر است.



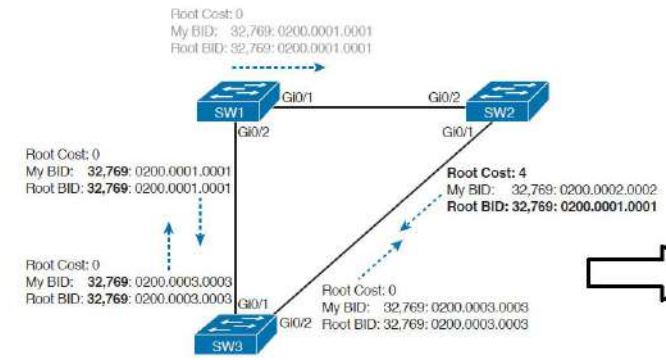


Figure 2-3 *Beginnings of the Root Election Process*

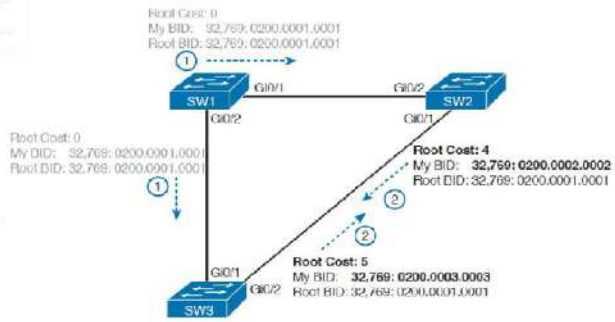


Figure 2-4 *SW1 Wins the Election*

در فرآیند انتخاب سوئیچroot ، سوئیچ ها از طریق فرستادن پیام های Hello BPDU که BID خود را در این پیام ها به عنوان root BID قرار داده اند، سعی می کنند خود را به عنوان سوئیچ root به سوئیچ های مجاور خود معرفی کنند. اگر یک سوئیچ پیامی را دریافت کند که BID کمتری نسبت به BID خودش داشته باشد، آن سوئیچ دیگر خود را به عنوان سوئیچ root معرفی نمی‌کند، به جای آن شروع به ارسال BPDU دریافتی که دارای BIDبهتری است می‌کند (مانند رقابت های انتخاباتی که یک نامزد به نفع نامزد هم حزبش که موقعیت بهتری دارد، از رقابت در انتخابات خارج می‌شود). در نهایت تمامی سوئیچ ها به یک نظر نهایی می‌رسند که کدام سوئیچ BID کمتری دارد و همه آن سوئیچ را به عنوان سوئیچ root انتخاب می‌کنند.

توجه : در مقایسه دو پیام Hello با هم، پیامی که BID کمتری دارد، superior Hello و پیامی که BID بیشتری دارد، inferior Hello نام دارد.

تصویر ۳-۲ آغاز فرایند انتخاب سوئیچ root را نشان می‌دهد، در ابتدای این فرایند SW2 همانند باقی سوئیچ ها خود را به عنوان سوئیچ root معرفی می‌کند. SW2 پس از دریافت Hello مربوط به SW1 متوجه می‌شود که SW1 شرایط بهتری را برای root بودن دارد، پس شروع به ارسال Hello دریافتی از SW1 می‌کند. در این حالت سوئیچ SW1 خود را به عنوان root معرفی می‌کند و SW2 نیز با آن موافقت می‌کند اما سوئیچ SW3 هنوز سعی می کند که خود را به عنوان سوئیچ root معرفی کند و Hello BPDUهای خود را ارسال می‌کند.

دو نامزد هنوز باقی ماندند: SW1 وSW3 . از آنجایی که SW1 مقدار BID کمتری دارد، SW3پس از دریافت BPDU مربوط بهSW1 ، SW1 را به عنوان سوئیچ root می پذیرد و به جای BPDU خود، BPDUدریافتی از SW1 را به سوئیچ های مجاور ارسال می‌کند.

پس از اینکه فرایند انتخاب تکمیل شد، فقط سوئیچ root به تولید پیام های Hello BPDU ادامه می‌دهد. سوئیچ های دیگر این پیام ها را دریافت می‌کنند و BID فرستنده و root cost را تغییر می‌دهند و به باقی پورت ها ارسال می‌کنند. در تصویر ٤-۲ ، در قدم اول سوئیچ SW1 پیام های Hello را ارسال می‌کند، در قدم دوم سوئیچ های SW2 و SW3 به صورت مستقل تغییرات را روی پیام های دریافتی اعمال می کنند و آن ها را روی پورت های خود ارسال می‌کنند.

```
Switch#show spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID     Priority    24577
              Address     000A.41D5.7C52
              Cost        19
              Port        25(GigabitEthernet0/1)
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    28673  (priority 28672 sys-id-ext 1)
              Address     0090.0CC4.D724
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------
Fa0/2            Desg FWD 19        128.2    P2p
Gi0/1            Root FWD 19        128.25   P2p
```

نکته۱: برای دیدن اطلاعات مربوط به STP مانند RB و BID از دستور Switch#Show spanning-Tree استفاده میکنیم.

نکته۲: BPDU هر ۲ ثانیه ارسال می‌شود(فقط از سوئیچ RB). در صورتی که به مدت ۲۰ ثانیه(دهمین بار) سوئیچ ها BPDU دریافت نکنند به منزله قطع شدن Root Bridge خواهد بود و مراحل انتخابات مجدد انجام خواهد شد.

نکته۳: در دستور بالا عدد مقابل Port شناسه‌ایست که همان شماره Port است. این سوئیچ ۲۶ پورته است که ۲۵امین پورت آن g0/1 است.

نکته٤: سوئیچ هایی که در یک STP هستند، باید Hello time یکسان داشته باشند که پیشفرض 2 است.

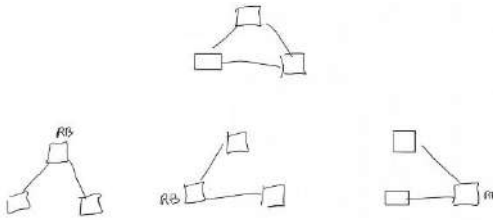
نکته۵: بعد از شکل گرفتن STP ، فقط RB میتواند BPDU تولید کند. مابقی سوئیچ ها فقط در نقشForwarding این PBDU ظاهر می‌شوند.

نکته٦: [RB]نقطه شروع درخت که به آن سوئیچ ریشه گفته می شود و بقیه سوئیچ های غیر ریشه را [Non RB] می‌گویند.

تغییر RB(Root bridge) :

برای این کار کافیست Priority ها را تغییر دهیم(mac addressها که قابل تغییر نیستند):

```
Switch(config)#spanning-tree vlan () priority ()
% Bridge Priority must be in increments of 4096.
% Allowed values are:
 0    4096  8192  12288 16384 20480 24576 28672
 32768 36864 40960 45056 49152 53248 57344 61440
```



البته گاهی شاید بخواهیم فقط RB swX باشد و نخواهیم درگیر اعداد Priority شویم. با دستورات زیر میتوانیم اولویت اول و دوم برای سوئیچ ها را به طور مستقیم اعمال کنیم. خود دستگاه با محاسبه Priority اولویت ها را تغییر میدهد(مثلا برای اولویت اول یک قدم نسبت به priority قبلی و برای اولویت دو ، دو قدم نسبت به Priroty اول، Priority را به عقب بر میگرداند.)

Switch(config)#spanning-tree vlan 200 root primary	با این دستور سوئیچ را به عنوان روت اصلی برای vlan مورد نظر انتخاب می‌کند
Switch(config)#spanning-tree vlan 200 root secondary	با این دستور سوئیچ را به عنوان روت دوم (جایگزین) برای vlan مورد نظر انتخاب می‌کند

2 - Select Root Port Per SWH [RP] -> Lowest Cost to RB

پس از انتخاب سوئیچ root، در مرحله ی بعدی، پروتکل STP برای سوئیچ های nonroot (همه ی سوئیچ ها به جز سوئیچ RB) یکRP (Root port) انتخاب می‌کند. RP هر سوئیچ، پورتی است که کمترین cost را برای رسیدن به سوئیچ root (RB)دارد. در واقع RP پورت اصلی یک سوئیچ است که آن را به سوئیچ روت (RB) برساند. در واقع **Port**ی میشود **RP** که،از سوئیچ روت **BPDU** با مجموع **Cost** کمتر دریافت کند.

هر پورت سوئیچ که کمترین میزان RPC (Root Port Cost) را داشته باشد به‌عنوان Root Port تعیین‌میشود. مقدار cost بر اساس نوع کابل ارتباطی در نظر گرفته شده است. هر چه سرعت ارتباط(بستگی به نوع کابل دارد) بیشتر باشد میزان cost کمتر و در نتیجه احتمال RP شدن Port بیشتر است.

Path Cost Method

Ethernet Speed	IEEE Cost: 1998 (and Before)	IEEE Cost: 2004 (and After)
10 Mbps	100	2,000,000
100 Mbps	19	200,000
1 Gbps	4	20,000
10 Gbps	2	2000
100 Gbps	N/A	200
1 Tbps	N/A	20

STP/RSTP Short **MST Long**

*نکته۱: اگر شما در حال استفاده از یک کابل شبکه 1گیگا بیتی هستند، STP هزینه را بر اساس سرعت واقعی در حال استفاده محاسبه می‌کند. یعنی اگر یک پورت گیگا بیتی بعد از negotiate با سرعت ۱۰۰ مگابیت در ثانیه کار کند، هزینه آن ۱۹ شناسایی خواهد شد نه ٤.

نکته۲: [RP] انتخاب یک پورت به ازای هر سوئیچ که نزدیک به RB باشد.

نکته۳: زمانی که BPDU تولید و از دستگاه خارج می شود Cost محاسبه نمی شود، در واقع زمانی محاسبه می شود که وارد پورت می شود. در نتیجه زمانی که RB بسته BPDU را ارسال می کند Cost آن صفر می باشد و به دست طرف مقابل که می‌رسد Speed Operational که دارد (سرعتی که با دستور Speed ادمین ست کرده) Cost را محاسبه می کند.

نحوه محاسبه RPC :

در شکل روبرو فرض میکنیم sw1 به عنوان RB انتخاب شده است.

سوئیچ SW3 برای ارسال frame ها به سوئیچ root ، می‌تواند از دو مسیر استفاده کند: G0/1و G0/2. برای هر یک از پورت ها، RPC رسیدن به سوئیچ root برابر است با مجموع cost خروج از پورت هایی که frame ارسالی، برای رسیدن به سوئیچ root از آن ها عبور می‌کند (در این محاسبه، هزینه ورود به پورت ها حساب نمی‌شود). مجموع(Total) cost هر پورت را مشاهده میکنید. از آنجاییکه مسیری که دارای RPC کمتری برای رسیدن به سوئیچ root می‌باشد از پورت Gi0/1 خارج می‌شود، سوئیچ SW3 این پورت را به عنوان root port انتخاب می‌کند. سوئیچ ها با سپری کردن فرایندی متفاوت به همین نتیجه می‌رسند.

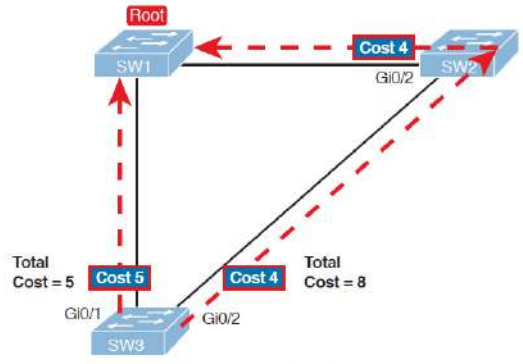


Figure 2-5 *How a Human Might Calculate STP Cost from SW3 to the Root (SW1)*

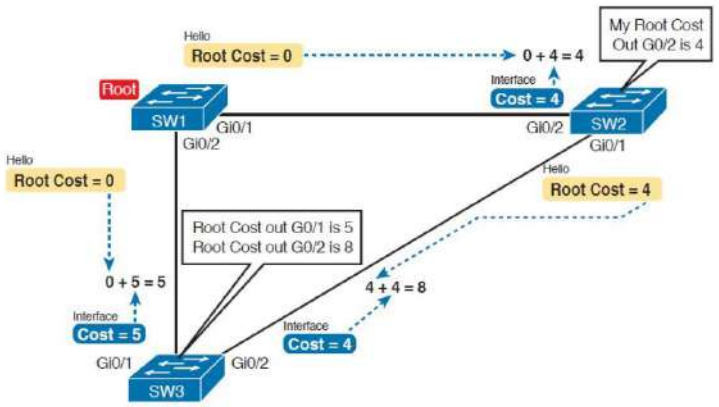
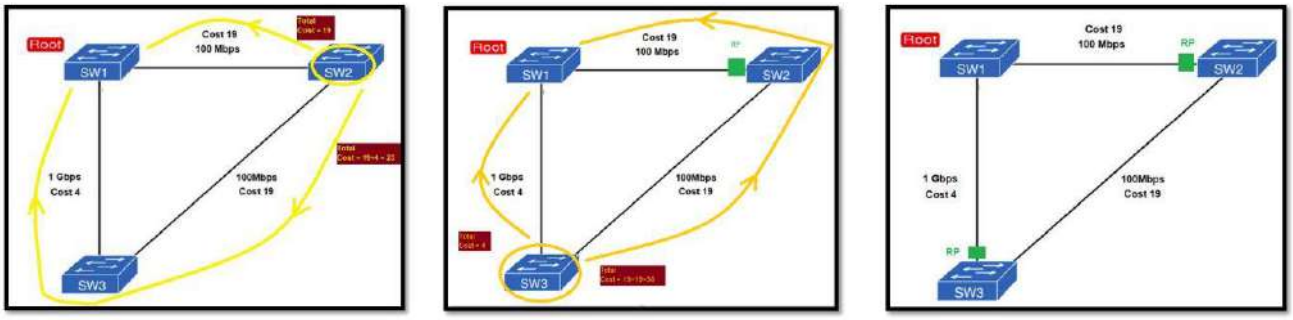


Figure 2-6 *How STP Actually Calculates the Cost from SW3 to the Root*

توجه شود که cost پورتهای خروجی RB

صفر می باشد.

در نهایت :



تغییر مقدار Cost :

برای تغییر cost هم میتوان سرعت انتقال interface را جابجا کرد ، هم مقدار مستقیم cost. تغییر سرعت روی data plane تاثیر میذارد ولی تغییر cost روی control plane (یعنی تاثیری روی data rate ما ندارد). تغییر cost برای این استفاده میشود که ما بخواهیم مسیر رسیدن سوئیچ به سوئیچ دیگر را تغییر بدهیم.

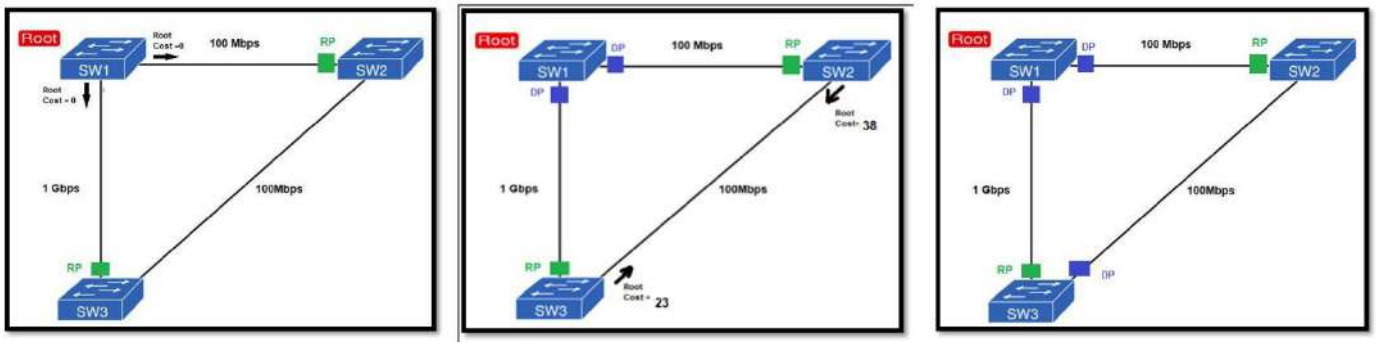
Change Cost :

Indirect :
change speed under interface

direct :
interface () spanning-tree cost ()

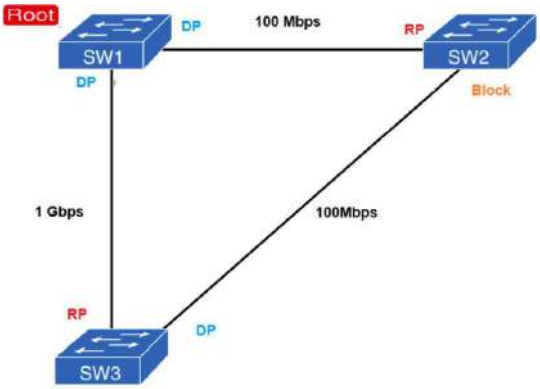
3 – Select Designated Port per Link [DP]

پس از انتخاب سوئیچroot ، در سوئیچ هایnonroot ، تمامroot port ها مشخص شدند و در وضعیت forwarding قرار گرفتند. مرحله نهایی پروتکل STP برای تکمیل توپولوژیSTP ، انتخاب designated port در هر LAN segment است. در هر بخش (segment)ازLAN ، پورت سوئیچی که کمترین root cost را دارد و به آن بخش از LAN متصل استDP(Designated port) نامیده می شود. در واقع DP پورتی است در هرLAN segment ، BPDU با Cost کمتر ارسال کند .



نکته : پورت‌های RB و پورت‌های مقابل پورت‌های RP همیشه در حالت DP هستند.(با محاسبه قابل اثبات هستند)

4 – select Blocked Port based on STP



در نهایت پورت هایی که وضعیتشان مشخص نشده در وضعیتblocking قرار می گیرند. درواقع در حالتی که یک پورت نه Root و نه Designated باشد آن پورت در حالت blocking قرار می‌گیرد.

نکته۱ : BLK State نه ترافیک را عبور می‌دهد و نه از آن پورت MAC Learning می‌کند.

```
Switch#show spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID     Priority    24577
              Address     000A.41D5.7C52
              Cost        19
              Port        25(GigabitEthernet0/1)
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    28673  (priority 28672 sys-id-ext 1)
              Address     0090.0CC4.D724
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------
Fa0/2            Desg FWD 19        128.2    P2p
Gi0/1            Root FWD 19        128.25   P2p
```

سرانجام نقش و وضعیت پورتهای یکی از سوئیچ‌ها را به عنوان نمونه مشاهده میکنید.

نقش و وضعیت port ها در STP :

Port State

==========

Role : RP/DP State : FWD

Role : Block(alternative) State :BLK

STP Tie Breaker :

گره های STP در انتخاب RP :

به طور کل برای انتخاب RP مراحل زیر به ترتیب طی می‌شود. هر شرط صدق کرد به سراغ شرط بعد نمی‌رویم.

Root Port Selection

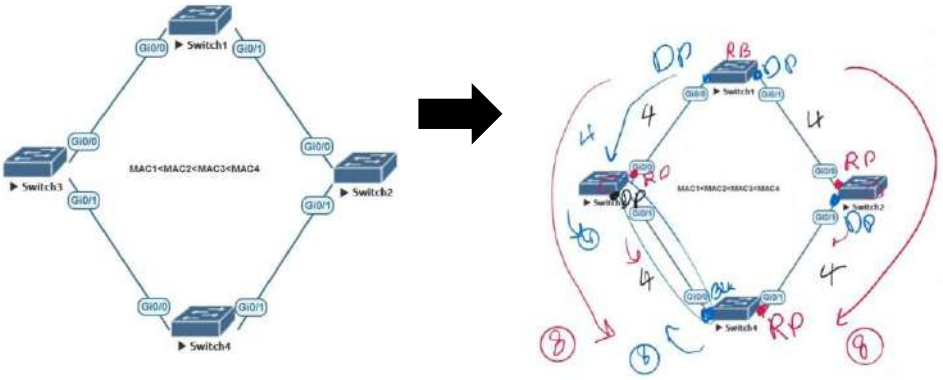
1 – Lowest Cost To RB

2 – Lowest Sender BID ➔ BID = Priority:MAC (Def Prio=32768) (2 byte, 6 byte)

3 – Lowest Sender Port-ID ➔ PID = Priority.Port NUM (Def Prio=128) (1 byte, 1 byte)

4 – Lowest Local Port-ID

حالت اول:



مراحلstp شکل بالا: مرحله اول که RB مشخص است چون Sw1 BID از همه کمتر است. مرحله دوم(بررسی پورتهای swh3) ، Gi0/0 سوئیچ۳، BPDU با Cost4 از سمت RBدریافت میکند (به دلیل اینکه gi0/0سوئیچ۱،BPDU با costصفر ارسال و چون ارتباط 1G است، gi0/0 سوئیچ۳ BPDU با cost4 دریافت میکند)، ولی Gi0/1سوئیچ۳، BPDU با Cost(4+4+4=12) از سمت RBدریافت میکند. پس پورتG0/0سوئیچ۳ RP است. مرحله سوم(بررسی پورتهای swh2)، Gi0/0 سوئیچ۲، BPDU با Cost4 از سمت RBدریافت میکند، ولی Gi0/1سوئیچ۲،BPDUبا Cost(4+4+4=12) از سمت RBدریافت میکند. پس پورتG0/0سوئیچ۳ RP است. اما در مرحله چهارم(بررسی پورت‌های swh4)، پورت‌های سوئیچ٤ هردو BPDU با Cost(4+4=8) دریافت میکنند. حال کدام RP است ؟!

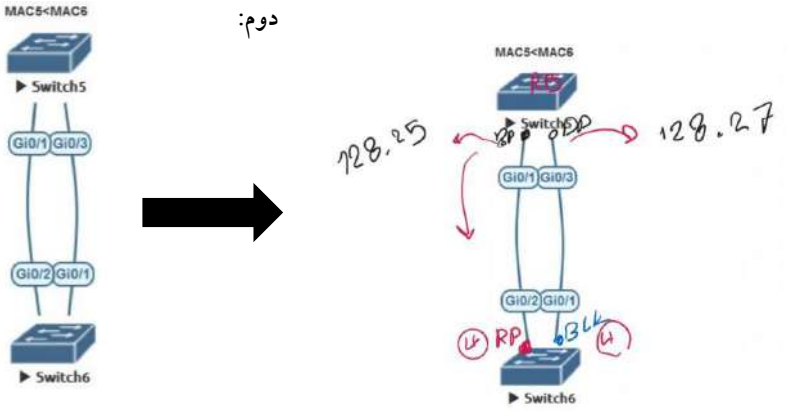
در این حالت شرط اول(جدول بالا) که نمیتواند تصمیم ساز بشود. به سراغ شرط دوم می‌رویم. در این حالت Portی RP میشود که sender BID کمتری (Lowest Sender BID) داشته باشد. پس چون Swt3 < Swt2 BID است، swt4 gi0/1 میشود RP ما.

2 – Lowest Sender BID ➔ BID = Priority:MAC (Def Prio=32768) (2 byte, 6 byte)

مرحله پنجم(انتخاب DP)، میدانیم که روبروی هر DP،RP قرار دارد(همچنین می‌دانیم پورت‌های RB همیشهDP می‌باشد.) . پس پورت های باقیمانده سوئیچ‌های۱ و ۲ DP شدند. مرحله ششم (انتخاب DP لینک بین سوئیچ‌های ۳و٤)، swt3 gi0/1 BPDU با cost

4 و gi0/0 BPDU swt4 با cost 8 به سمت همدیگر ارسال میکنند. حال Portی میشود DP که cost کمتری ارسال میکند. پس در این شکل gi0/1 میشود DP ما. در ادامه هر Portی که باقیماند میشود Block port.

حالت دوم:



مراحل stp شکل بالا: مرحله اول که RB مشخص است چون BID Sw5 از BID Sw6 کمتر است. مرحله دوم، در سوئیچ nonroot bridge باید RP مشخص کنیم. شرط اول: gi0/2 و gi0/1 sw6 هر دو BPDU یکسان دریافت میکنند. پس این شرط قابل استفاده نیست. شرط دوم: sender BID هر دو Port یکسان هستند در نتیجه شرط Lowest Sender BID قابل استفاده نیست. شرط سوم: در این حالت Portی میشود RP که PID (Port Id) پورت سوئیچی که BPDU ارسال میکند کمتر باشد(Lowest Sender Port-ID). پس چون PID Gi0/1 Swt5 < PID Gi0/3 Swt5 است،Port مقابل gi0/2 swt5 میشود RP ما.

3 – Lowest Sender Port-ID ➔ PID = Priority.Port NUM (Def Prio=128) (1 byte . 1 byte)

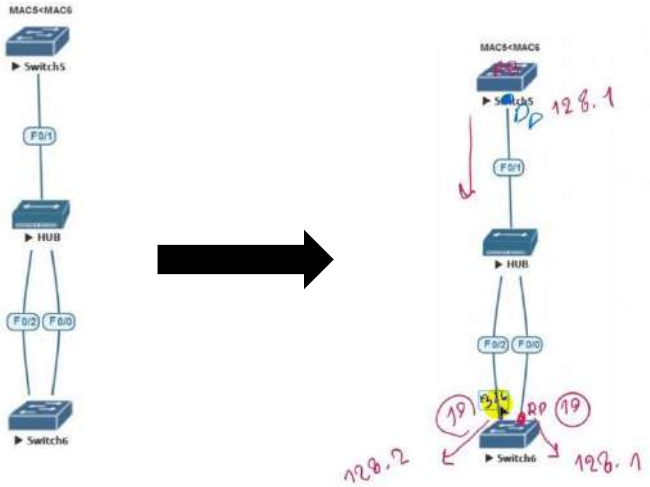
پورت های RB که همگی DP هستند. فقط یک Port باقی میماند که آن هم Block Port است.

**نکته: PID پیشفرض ۱۲۸ است که اعداد بین ۰ _۲۵۵ قابل تخصیص هستند

برای تغییر PID(البته فقط Priority) از دستور زیر استفاده میکنیم:

```
switch(config-if)#spanning-tree vlan <> port-priority <>
```

حالت سوم:



مراحلstp شکل بالا: مرحله اول Sw5 میشودRB، چون BID Sw5<BID Sw6 . مرحله دوم، در سوئیچ nonroot bridge باید RP مشخص کنیم. شرط اول: Sw5 یک BPDU با Cost 0 ارسال میکند. وقتی به Portهای swt6 میرسد، Cost برای هر دو Port میشود ۱۹. پس با این شرط نمیتوان RP را مشخص کرد. شرط دوم هم نمیشود چون یک BPDU sw ارسال میکند که آن هم پورت RB است. شرط سوم: ما در این سناریو یک پورت در حال ارسال BPDU است پس شرط سوم قابل تشخیص نیست. شرط چهارم: مبنا را خود Sw6 قرار میدهیم. در این حالت Portی میشود RP که PID کمتری داشته باشد. طبق سناریو PID F0/0 < PID F0/2 پس پورت Sw6 F0/0 میشود RP ما.

4 – Lowest Local Port-ID

پورت های RB که همگی DP هستند. فقط یک Port باقی میماند که آن هم Block Port است.

گره های STP در انتخاب DP :

به طور کل برای انتخاب DP مراحل زیر به ترتیب طی می‌شود. هر شرط صدق کرد به سراغ شرط بعد نمی‌رویم.

Designated Port Selection

---

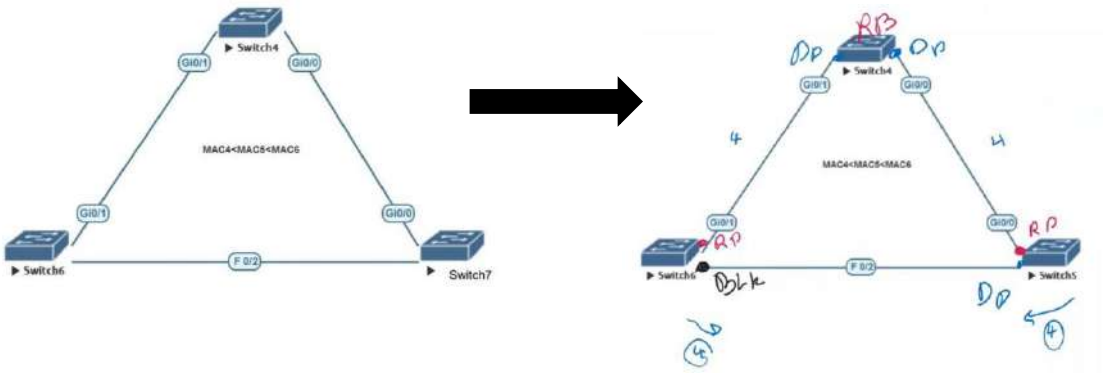
1 – Lowest Cost To RB

2 – Lowest Sender BID ➔ BID = Priority:MAC (Def Prio=32768)

(2 byte, 6 byte)

3 – Lowest Local Port-ID

حالت اول:

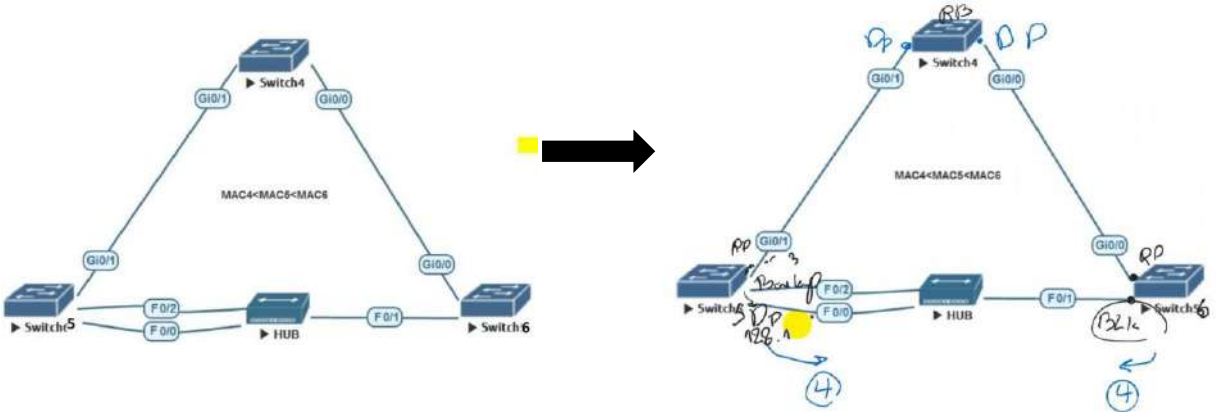


مراحل stp شکل بالا: مرحله اول Sw4 میشودRB چون BIDاش از همه کمتر است. مرحله دوم: BPDUی که به swt6 Gi0/1 وارد میشود، cos4 دارد ولی BPDUی که به swt6 F0/2 وارد میشود Cost(4+19) دارد. پس swt6 Gi0/1 میشود RP. در swt5 هم به همین صورت. در نهایت swt5 Gi0/0میشود RP. مرحله سوم:Portهای RB که همگی DP هستند.در نهایت فقط پورت‌های link lan بین swt5 و swt6 مانده. شرط اول قابل تشخیص نیست چون دو پورت با cost4یکسان BPDU ارسال میکنند. شرط دوم: Portی

میشود DP که Lowest Sender BID باشد. در این سناریو چون BID swt5 > BID swt6 است، پس پورت Swt5 F0/2 میشود DP ما. مرحله چهارم. در نهایت یک لینک باقی ماند که آن هم Block port است.

2 – Lowest Sender BID → BID = Priority:MAC (Def Prio=32768)

حالت دوم:



مراحل stp شکل بالا: مرحله اول Sw4 میشودRB چون BID اش از همه کمتر است. مرحله دوم: در مرحله دوم: BPDUی که به swt5 Gi0/1 وارد میشود، cos4 دارد ولی BPDUی که به swt5 F0/2 وswt5 F0/2 وارد میشود cost بیشتری دارد. پس swt5 Gi0/1 میشود RP. در swt6 هم به همین صورت. در نهایت swt6 Gi0/0 میشود RP. مرحله سوم: (روی link بین hub وswt) شرط اول برقرار نمیشود چرا که هر دو پورتBPDU با cost ٤ ارسال میکنند(یکسان است). شرط دوم: این شرط هم برقرار نیست چون هر دو Port دارای BID یکسانی هستند. شرط سوم: مبنا را خود Sw5 قرار میدهیم. در این حالت Portی میشود DP که PID کمتری داشته باشد. طبق سناریو PID F0/0 < PID F0/2 پس پورت Sw5 F0/0 میشود DP ما.

3 – Lowest Local Port-ID

در نهایت swt6 F0/1 میشود block port و Swt f0/2 میشود Backup port.

** نکته: block port جایگزین RP و backup port جایگزین DP است.

Root port Replace X → ALTN
Designated port Replace X → Backup

نکته:

Data Plane	**ترافیکی که بین ارتباطات شبکه ارسال می شود**
Control Plane	**بسته های کنترلی مثل BPDU**
Management Plane	**بسته هایی مثل Telnet یا SSH**

Weak points STP:

- داشتن یک STP برای کل شبکه باعث کاهش مصرف منابع می شود.
- داشتن یک STP باعث ایجاد محدودیت هایی می شود.

- لینک های Redundant یا جایگزین بین سوئیچ ها مسدود می شوند و از توان آنها برای Load Balancing نمی توان استفاده کرد.

Types of STP protocols :

: CST 802.1D

پیش تر در سوئیچ ها، روش پیش فرض CST یا Common Spanning Tree بوده است. در حال حاضر این ورژن مورد استفاده نیست. در این روش که استفاده از آن بیش از یک دهه کنار گذاشته شده است، یک root bridge برای تمام VLANها میشود. پس از استفاده از این روش، به سرعت مشخص گردید این روش بایستی ارتقا داده شود و به ازای هر VLAN یک RB نیاز است.

: PVST و PVST+ 802.1Q

اگر به ازای هر VLAN یکبار spanning-tree را راه ندازی کنیم به آن PVST می گوییم. اگر در لینکی کهencapsulation اش برا ساس ISL با شد، امکان اجرای CST و PVST با یکدیگر وجود ندارد. اما، PVST+بین سوئیچ هایی که CST را اجرا کرده و گروهی دیگر که PVST را اجرا کرده اند، امکان فهم اطلاعات بین طرفین را ایجاد میکند.

: MST 802.1S

در روش MST، به جای مفهوم VLAN از instance استفاده میکنیم و RB به ازای آن مشخص میشود. به مجموعه ای از VLAN ها یک instance گفته میشود. علت ا ستفاده از این روش زیاد شدن تعداد VLAN ها ست که بار محا سباتی سوئیچ را بسیار زیاد خواهد کرد. به طور معمول، در شـــبکه ها، تعدادVLAN ها به عدد ۱۰۰ نزدیک هم نمیشـــود. اما، این تعداد در شـــبکه هایی مانند دیتاسنترهای بزرگ، شبکه های زیرساختی ارائه دهنده سرویس مانند مخابرات و ...، کاملا متداول است.

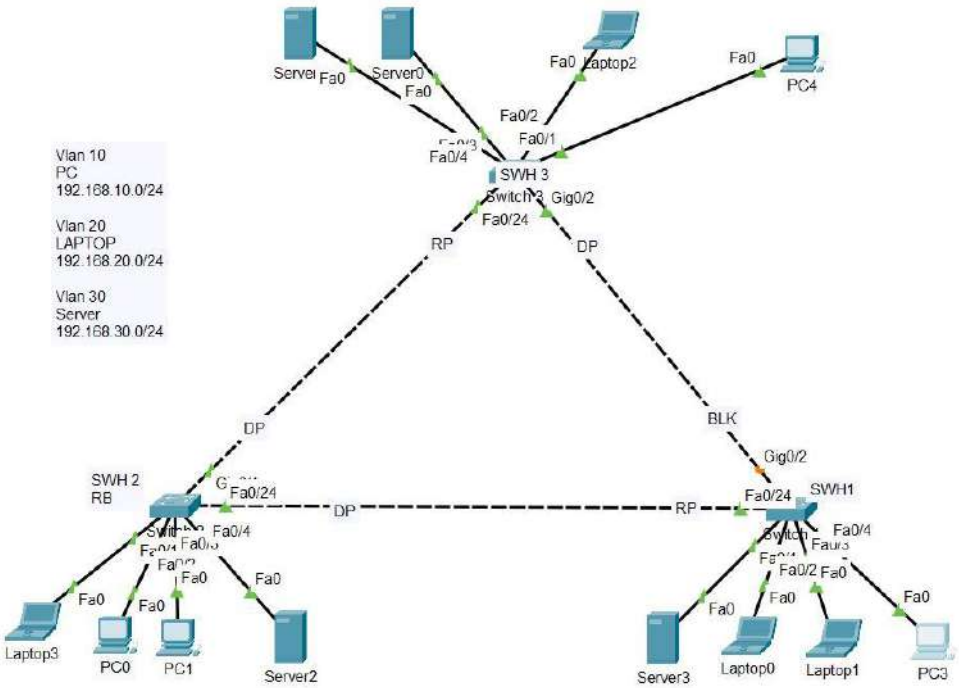
PVSTP (per vlan spanning tree protocol) :

سیسکو یک نسخه اختصاصی را پیشنهاد می دهد که دارای انعطاف پذیری بیشتری نسبت به STP است. در STP برای کل شبکه یک درخت داریم و برای کل شبکه بدون در نظر گرفتنVLAN ها انتخاب انجام می شود. اما در PVST ما برای هر VLAN یک STP اجرا می شود و برای هر VLANیک درخت ایجاد می شود و انتخابات را برای هر VLAN به صورت جداگانه انجام می گیرد و به این شکل جریان ترافیک بهبود می یابد. یعنی یک سوئیچ در یک VLAN به عنوان Root Bridge نقش ایفا می کند و همان سوئیچ می تواند نقش یک سوئیچ معمولی را برای یک VLAN دیگر ایفا کند که به اینکار **Load Balancing** میگویند.

PVST: برای هر vlan یک پروسه STP اجرا میکنه . اختصاصی سیسکو هست . با پروتکل ISL که مخصوص سیسکو هست کار می کنه.

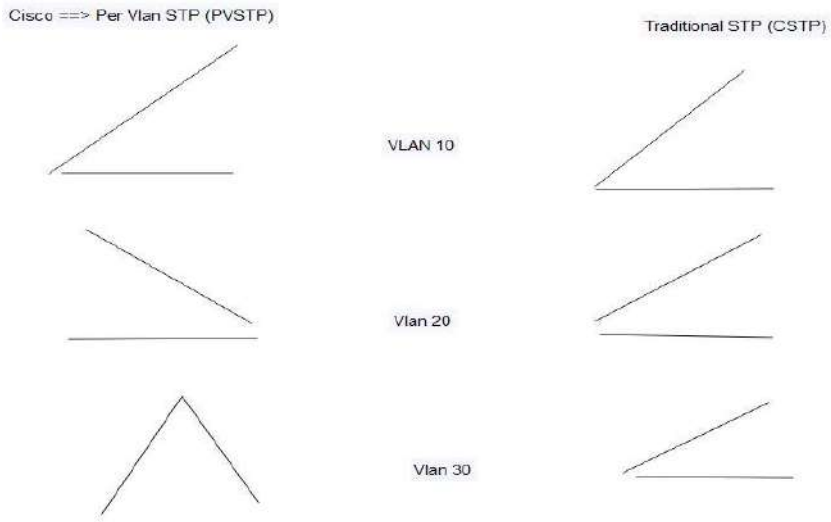
PVST +: مثل PVST هست با این تفاوت که پروتکل های 802.1Q و ISL رو پشتیبانی می کنه .

مثال برای فهم بیشتر PVSTP:



برای مثال بالا به دستگاه‌ها(pc,server,laptop) IP میدیم. روی سه سوئیچ سه vlan (۱۰ / ۲۰ /۳۰) میسازیم(show vlan brief میزنیم چک میکنیم آیاvlan ها ساخته شدن یا خیر). پورت های سوئیچ ها را بهtrunk mode تبدیل میکنیم(فرق نمیکند دست خودمونه trunk trunk/ trunk auto / desirable auto)(با دستور show interface trunk چک میکنیم آیا vlanهای ساخته شدن allow اینترفیس‌ها شده‌اند یا خیر). روی هر سوئیچ، روی portهایی که به end userها وصل شده‌اند switch mode access را میزنیم و در ادامش همان دستگاه را access آن vlan میکنیم(show interface status میزنیم چک میکنیم آیا دستگاه‌ها (Port) access ویلن مدر نظر شدند یا خیر).

می‌دانیم که در شکل بالا پروتکل stp فعال شده. اجزای Stp (RB ،RP ، DP و BP) هم روی شکل مشخص کرده‌ایم. ما اگر از Traditional STP (CSTP) استفاده کنیم، Topology همه vlanها برای data palne به صورت زیر(سمت راست) عمل میکنند:



فرض کنید laptop سوئیچ ۱ میخواهد بسته ای را به laptop سوئیچ ۳ برساند. این بسته با توجه به بلاک بودن swh2 gi0/2، حتما باید بسته خود را از مسیر swh f0/24 برساند. این کار منطقی‌ست؟ خیر. ما برای حل این مشکل STP، باید RB را به نسبت vlanها انتخاب کنیم(برای هر vlan سوئیچ روت مجزا تعیین شود). در نتیجه logical topology ما به نسبت هر Vlan متفاوت میشود(شکل سمت چپ) . ما با این کار هم از ظرفیت پهنای باند به خوبی استفاده میکنیم ، هم Spof را مدیریت بهتری میکنیم، هم مکانیزم مدیریت loopلایه دو را همچنان برقرار داریم که نمیگذاریم loop در شبکه اتفاق بیفتد. به این پروتکلی که برقرار کردیم PVSTP گفته میشود.

نکته: در سوئیچ ها سیسکو Pvstp به طور پیشفرض روشن است. (دستورshow running-config)

```
spanning-tree mode pvst
```

* حل سناریو: RB سرورها(vlan30) بشود swh 3 . RB لپ‌تاپ‌ها(vlan20) بشود swh 1. RB کامپیوترها(vlan10) بشود swh2.

راهکار این سناریو پروتکل PVSTP است.

قبل از اینکه سناریو را انجام دهیم، اگر دستور show spanning-tree را بزنیم، متوجه میشویم که با توجه به اینکه روی سوئیچ ها پروتکل pstv فعال است، برای هر vlan (۱ و ۱۰ و ۲۰ و ۳۰) جدا گانه stp تشکیل شده است، ولی نتایج یکسان است(چون RBو ...یکسان هستند). حال به سراغ تفکیک آن ها میرویم:

مرحله اول) برای سرورها به سراغ swh3 می‌رویم. با یکی از دستورات زیر vlan 30 را به logical topology دلخواه تبدیل میکنیم.

Swich(config)#spanning-tree vlan <> root Primary

Or

Swich(config)#spanning-tree vlan <> priority <>

مرحله دوم) مرحله قبل را برای سوئیچ های دیگه هم انجام میدهیم (به نسبت خواسته سناریو)

قبل از اعمال pvstp، با دستور show spanning-tree همه نتایج vlans یکسان بود، ولی بعد از اعمال pvstp ، logical topology هر vlan متفاوت شده است.

برای اثبات این حرف به شکل های زیر توجه کنید.

برای vlan10 ، swh2 ، برای vlan20،swh1 و برای Vlan30، swh3 RB هستند. همچنین وضعیت و نقش هر Portسوئیچ به نسبت هر Vlan تغییر کرده‌اند.

```
VLAN0010
  Spanning tree enabled protocol ieee
  Root ID     Priority    24586
              Address     0002.1713.94B9
              This bridge is the root
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    24586  (priority 24576 sys-id-ext 10)
              Address     0002.1713.94B9
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/2            Desg FWD 19        128.2    P2p
Fa0/3            Desg FWD 19        128.3    P2p
Fa0/24           Desg FWD 19        128.24   P2p
Gi0/1            Desg FWD 19        128.25   P2p
```

```
VLAN0020
  Spanning tree enabled protocol ieee
  Root ID     Priority    24596
              Address     00E0.8F85.C523
              Cost        19
              Port        24(FastEthernet0/24)
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    32788  (priority 32768 sys-id-ext 20)
              Address     0002.1713.94B9
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/1            Desg FWD 19        128.1    P2p
Fa0/24           Root FWD 19        128.24   P2p
Gi0/1            Altn BLK 19        128.25   P2p
```

```
VLAN0030
  Spanning tree enabled protocol ieee
  Root ID     Priority    24606
              Address     0060.5CA7.D70C
              Cost        19
              Port        25(GigabitEthernet0/1)
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    32798  (priority 32768 sys-id-ext 30)
              Address     0002.1713.94B9
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/4            Desg FWD 19        128.4    P2p
Fa0/24           Altn BLK 19        128.24   P2p
Gi0/1            Root FWD 19        128.25   P2p
```

Timers in STP :

STP از سه تایمر در عملیات های خود استفاده می کند و این زمان بندی توسط Root Bridge در پیام های Configuration BPDU به بقیه اعلام میگردد.

- **Hello Time 2** ثانیه : زمان ارسال Configuration BPDU توسط RB
- **Froward Delay 15** ثانیه : مدت زمان هر کدام از حالت های Learning وListening
- **Max Age 20** ثانیه : طول عمر BPDU

نکته : زمان Convergence (همگرایی) در STP معمولا بین ۳۰ تا ۵۰ ثانیه است .

Convergence after change in STP topology :

منطق STP در هنگام Stable بودن شبکه این است که پروسه ارسال Hello را چک کند که در حالت Normal باشد و هنگامی که پروسه ارسال Hello تغییر کرد ، نیاز است که STP عکس العمل نشان دهد و بر اساس توپولوژی جدید تصمیم گیری نماید .

منطق **STP** در هنگامی که توپولوژی شبکه **Stable** می باشد:

- Root Bridge به صورت پریودیک براساس Hello Time دو ثانیه ای BPDU را ساخته و ارسال می کند.
- تمام سوییچ های Non Root Bridge به صورت منظم یک کپی برابر اصل از BPDU سوییچ Root را از روی Root Port دریافت میکند.
- تمام سوییچ ها BPDU را UPDATE و از طریق Designated Port ارسال میکنند.
- سوییچ ها از طریق پورت Block ، BPDU را ارسال نمی کنند.
- پورتی از سوییچ که به حالت Blocking رفته است به صورت متناوب از پورت Designated اون Segment ، یک کپی از BPDU را دریافت می‌کند .

**اگر اختلالی در هر یک از رویدادهای فوق رخ می دهد ، STP متوجه می شود که توپولوژی تغییر کرده و نیاز به Convergence دارد. مثلا سوییچ (Root Bridge) Root ممکن است خاموش شود که با این اتفاق بقیه سوییچ ها هیچ BPDU ای را دریافت نمیکنند و پس از اینکه MAX Timer منقضی شد (به صورت پیش فرض ۲۰ ثانیه)، دوباره سوییچ بر اساس منطق STP، Root جدید را انتخاب می کنند که این عمل را همگرایی STP گویند.

Details of STP messages :

همانطور که گفته شد به اطلاعات یا Message هایی که در لایه ۲ بین سوییچ ها مبادله می‌شود، پیام‌های BPDU گفته می‌شود.۲ گونه Message یا پیام در STP بین سوییچ ها رد و بدل می‌شود :

۱. Configuration BPDU :برای محاسبات Spanning Tree استفاده می‌شود.

۲. TCN BPDU:برای اعلان تغییرات پیش آمده در ساختار شبکه استفاده می‌شود .

۳.TCA BPDU (Topology Change Acknowledgement) : تایید دریافت TCN BPDU است.

نکات:

- پیام Configuration BPDU از Root Bridge به بقیه سوئیچ ها ارسال می‌شود.

- پیام TCN (Topology change Notification) از سوییچ‌ها به سمت Root Bridge (هنگام تغییر) ارسال می‌شود.

- در یک شبکه سالم و Stable اکثر پیام‌های STP از نوع Configuration BPDU هستند.

Field	Byte	Description
Protocol ID	۲	همیشه صفر است .
Version	۱	همیشه صفر است .
Type	۱	برای Configuration BPDU برابر صفر و برای TCN برابر یک است .
Flags	۱	LSB = Topology Change (TC) flag MSB = Topology Change Acknowledgment (TCA) flag
Root BID	۸	BID مربوط به Root Bridge فعلی
Root Path Cost	۴	Root Path Cost تا Root Bridge مشخص میکند .
Sender BID	۸	فرستنده PBDU را تا Root Bridge مشخص میکند .
Port ID	۲	مشخص کننده پورت ارسال کننده این BPDU
Message Age	۲	زمان تولید Message در Root Bridge
Max Age	۲	طول عمر صحت یک Configuration BPDU
Hello Time	۲	زمان بندی بین ارسال Configuration BPDU ها
Forward Delay	۲	زمان بندی Listening , Learning

نکته : TCN فقط شامل ۳ فیلد ابتدایی است.

Topology change check in STP :

به هنگام بروز هرگونه تغییر وضعیت در پورت و ایجاد اشکال یا اتصال یک Segment به Lan، STP باید با خبر و دست به کار شود و محاسبات لازم را صورت بدهد .یک سوییچ تغییر را از سمت Root Port به سمت Root Bridge ارسال و گزارش میکند و سوییچ های دریافت کننده پیام تغییر ، به فرستنده تغییرات ، پیام Ack را ارسال میکنند (به قولی رسید میدن که پیام رو دریافت کردن) . سوییچ فرستنده تا زمانی که Ack را دریافت نکند دست بردار نیست و همچنان به ارسالTCNمبادرت می‌کند. سوئیچ دریافت‌کنندهTCN، رسیدنTCNرا اطلاع میدهد تا دیگرTCNفرستاده نشود.

هنگامی که یک تغییر در وضعیت یک پورت سوییچ به وقوع می‌پیوندد، سوئیچ این تغییر را به صورت TCN از طریق Root Port بهRoot Bridge ارسال می‌کند.(TCN حاوی جزییات تغییر نیست بلکه یک خبر درباره یک تغییر است).

حالا نوبت سوئیچ بالایی است که با ارسال TCN سوئیچ‌های دیگر را از تغییر مطلع سازد و در این حالت یک گام به Root Bridge نزدیک‌تر شده و مراحل "رسید و ارسال" ACK مطابق بالا تکرار می‌گردد .در نهایت پیام به Root Bridge می‌رسد .

Root Bridge به محض دریافت TCN، Topology Change ACK را ارسال می کند و در هنگام ارسال Configuration BPDU بعدی، Topology Change Flag را که مشخص کننده تغییر در شبکه است را علامت می زند. فایده ارسال این علامت این است که سوییچ ها به محض دریافت Topology Change Flag در Configuration BPDU زمان طول عمر Bridging Table رو به میزان Forward Delay کاهش می‌دهند یعنی ۳۰۰ ثانیه به ۱۵ ثانیه کاهش پیدا میکند و در این مدت اگر فریمی از Mac Address خاصی دریافت نشود از جدول حذف می‌شود.

به طور خلاصه "هنگامی که پورتی به هر دلیل فعال یا غیر فعال میشه ، سوییچ هر ۲ ثانیه یک فریم TCN رو از Root Port خودش به سمت سوییچ بالا دستی ارسال می کند تا زمانیکه یک پیام ACK از اون سوییچ بالا دستی دریافت کند (مطمئن بشه که پیام TCN بهش رسیده) این روند همینطور ادامه پیدا میکند تا به دست سوییچ Root برسد .

سپس Root Bridge یک Configuration BPDU را که Flag آن ۱ شده به همه پورت های خودش ارسال میکند .مابقی سوییچ ها با دریافت این BPDU و مشاهده flag یک شده , عمر تمام رکورد های جدول Mac خود رو به Forward Delay یعنی ۱۵ ثانیه تغییر می دهد. هنگامی که تغییری درتوپولوژی شبکه ایجاد می گردد احتمال تغییر در Cam Table بسیار زیاد است و با این کار باعث می شود آدرس های Mac جدول زودتر Update شود و در این ۱۵ ثانیه به سایر دستگاه‌ها اجازه داده می شود تا Mac Address خود را Update کنند ."

نکته: دلیل اینکه سوییچ سریعا و بلافاصله جدول Mac خود را پاک نمیکند این است که ممکن است بسیاری از رکورد ها صحیح باشد و با پاک کردن کل جدول توسط سوییچ ها در لحظاتی Unicast های ناشناخته ای در شبکه Flood شود و شبکه را مختل کند.

Introducing different types of change in Topology :

معرفی انواع مختلف تغییر در Topology :

۱. **Direct Tolpology Changes** (تغییرات توپولوژی مستقیم)

اگر یک تغییری نسبت به سوئیچی که پورت بلاک در شبکه دارد اتفاق بیافتد، یعنی یکRP یا DP است قطع شود و پورتBLK بخواهد جایگزین آن شود، دو فاز ۱۵ ثانیه ای را طی می‌کند که به آن Forward Delay phase می‌گویند.

**نکته: در STP پورتی که FWD ا ست اگر نیاز با شد به پورت BLK تبدیل شود بدون تعلل انجام می‌گیرد چون در غیر این صورت در شبکه Loop ایجاد می‌شود.

----- مراحل تغییر وضعیت پورت **BLK** به **FWD** :

دو مرحله دارد (۳۰ثانیه): مرحله اول LSN ، عمرکوردهای جدول MAC Add Table ۱۵ ثانیه می‌گذرد و بعد از ۱۵ ثانیه جدول MACپاک می‌شود. بعد از ۱۵ثانیه LSN وارد مرحله Learning می شود. ۱۵ ثانیه صبر می‌کند تا Address MAC های جدید را از پورت های جدید یاد بگیرد و ترافیک FWD شود.

مراحل تبدیل پورت بلاک به فوروارد 30s BLK -> LSN -> LRN -> FWD

مراحل تبدیل پورت فوروارد به بلاک 0s FWD -> BLK

۲. **Indirect Topology Changes** (تغییرات توپولوژی غیر مستقیم)

در این حالت تغییرات روی ســـوئیچی که پورت بلاک ندارد رخ می‌دهد. در indirect علاوه بر مدت زمان ۳۰ ثانیه مدت زمان دیگری هم صرف می شود و بیش از ۳۰ ثانیه قطعی خواهیم دا شت. Max Age Time به اندازه ۲۰ ثانیه صبر می‌کند که مطمئن شود قطعی که در شبکه اتفاق افتاده، قطعی لحظه ای نباشد.

Max Age Time(20s) + Listening(15s) + Learning(15s) + BPDU(Hello time=2s) = 52Sec

۳. insignnificant Topology Changes (تغییرات توپولوژی ناچیز)

تشخیص تغییرات بی‌اهمیت در توپولوژی شبکه. هر کامپیوتری که در شبکه روشن و یا خاموش می‌شود و یا هر لینکی که از هر کامپیوتر قطع و یا وصل می‌شود منجر به UP و DOWN شدن یکی از پورت‌های سوئیچ می‌شود. سوئیچ تغییر مورد نظر را از نوع DIRECTتشخیص می دهد و وارد پروسه همگرایی STP می شود، این در حالی است کهEnd user ها در ایجاد LOOP نقشی ندارند، زیرا لینک های REDUNDANT بین سوئیچ‌ها وجود دارند و همان‌ها سبب ایجاد LOOP خواهند شد که باید در پروتکل STPلحاظ شوند. پروتکل STP تغییرات پورت‌هایACCESS(متصل به End userها) را نادیده می‌گیرد و وارد پروسه همگرایی نمی‌شود. البته باید توجه کرد که با فعال کردن ویژگی PORTFAST روی پورت‌های ACCESS ، پروتکل STP، تغییرات ایجاد شده روی پورت‌های PORTFAST را از دسته‌بندی بی‌اهمیت خارج می‌کند و آنجا تغییرات این پورت بسیار مهم می‌شود چرا که اگرBPDUای روی آن پورت ها در یافت شود باعث ایجاد LOOP خواهد شد.

ممکن است اتفاقی یکی از پورت‌های سوئیچ قطع شود (مثلاً دستمان اتفاقی به Patch cord خورد یا کانکتور آن شل بوده) و بعد بلافاصله آن را وصل کنیم. روی سوئیچ پورت بلاک برای اینکه به فوروارد تغییر وضعیت پیدا کند حداقل ۳۰ ثانیه طول می‌کشد. همه پورت‌ها در مرحله اول پس از روشن شدن بلاک هستند که بعد از آن DP می شوند و یا بلاک باقی می مانند. بعد از هرقطعی و وصل شدن الگوریتم STP در کل شبکه مجدد اجرا می شود و این شرایط ایده آل نیست زیرا پهنای باند و دستگاه را درگیر می‌کند.

وضعیت پورت ها در STP :

STP State \ Action	RCV BPDU	SND BPDU	LRN MAC	FWD MAC
Disable	N	N	N	N
Block	Y	N	N	N
Listening	Y	Y	N	N
Learning	Y	Y	Y	N
Forward	Y	Y	Y	Y

Disable: BPDU دریافت و ارسال نمی‌کند، Mac Learn نمی‌کند و ترافیک فوروارد نمی‌کند.

Block: BPDU دریافت می‌کند، چون باید متوجه تغییرات شبکه باشد، اما BPDU ارسال نمی کند، Learn MAC نمی‌کند و ترافیک فوروارد نمی کند.

Listening: BPDU دریافت و ارسال می کند، اما MAC Learn نمی‌کند و ترافیک فوروارد نمی‌کند.

Leraning: BPDU دریافت و ارسال می‌کند، MAC Learn می‌کند اما ترافیک فوروارد نمی کند چون درحال یادگیری مک آدرس است.

Forward: BPDU دریافت و ارسال می‌کند، MAC Learn می‌کند و ترافیک را ارسال می کند.

Port Fast :

ویژگی اختصاصی سیسکو برای بهبود سرعت تبادل اطلاعات در STP می باشد که باعث می شود Forward Delay phase را، روی پورتی که به End Device متصل شده را حذف کنیم. پورت بدون گذشتن از وضعیت های مختلف، به طور مستقیم در حالت Forwarding قرار می گیرد. طبق دستور زیر :

```
Switch(config)# int fa < >
Switch(config)# spanning-tree portfast
```

این قابلیت را فقط می‌توان روی اینترفیس‌های Non Trunk فعال کنیم و پورت اگر به دستگاه لایه۲ مثل سوئیچ یا بریج وصل باشد و BPDU ارسال کند و BPDUای که ارسال می‌کند شرایط بهتری داشته باشد اصطالحا BPDU Superior ارسال کند و آن سوییچ RB شود (Mac یا priority پایین‌تری داشته باشد) خطرناک هست چون توپولوژی کل شبکه را تغییر می‌دهد و تمام ترافیک سمت آن ارسال می شود و کل شبکه قطع می‌شود.

به همین راحتی به همین سادگی شبکه یک Provider قطع میشه ☺

BPDU Guard :

زمانی که BPDU Guard را فعال می‌کنیم، اگر روی پورت سوئیچ BPDU دریافت شود، ارسال روی این پورت متوقف می‌شود و پورت غیرفعال می شود. کاربرهای نهایی که به پورت های سوئیچ متصل هستند نباید روی این پورت BPDUارسال کنند. این تنظیمات باید روی پورت‌های access که به دستگاه‌های نهایی متصل هستند اعمال شود و از اتصال سوئیچ غیر مجاز به شبکه جلوگیری می‌کند. با اینکار می توان جلوی تغییر در توپولوژی STPرا گرفت.

مثال زیر نحوه اعمال BPDU Guard را نمایش می‌دهد:

```
SW(config)#interface fastethernet <>
SW(config-if)#spanning-tree bpduguard enable
```

نکته۱: درمحیط Global با اجرای دستور زیر بجای اینکه روی هر پورت جداگانه بزنیم، بصورت پیشفرض روی همه پورت‌ها فعال می شود و بعد روی پورت‌هایی که نمی خواهیم BPDU Guard فعال باشد، بجای enable باید disable بنویسیم.

```
SW(config)#spanning-tree portfast bpduguard default
```

نکته۲: چرا پروتکل STP خاص SWITCHING است و چرا از بین ۳ لینک سوئیچ ، یکی از پورت ها در یکی از لینک‌ها باید بلاک شود، در حالی که در Routing ما مشکل LOOP را نداریم و می‌توانیم بین روترهایمان مسیرهای متفاوتی داشته باشیم؟ روترها مانع از عبور بسته‌ها broadcast می‌شوند درحالیکه ماهیت سوئیچ‌ها متفاوت از روتر است چون سوئیچ از طریق همین بسته های broadcastمانندARPجدولMacخودرا کامل می‌کنند.

نکته۳: نمایش پورتی که err -disable شده و علت آن را به ما نمایش می دهد:

```
Switch# show interface status err-disable
```

حال، برای اینکه از وضعیت disable-err خارج شود یکبار باید پورت را خاموش و روشن کنیم. یک مکانیزم دیگر هست که سوییچ را بررسی می‌کند که اگر مشکل حل شده باشد، پورت را روشن کند که به آن err-recovery می‌گویند که بصورت پیشفرض فعال نیست، اما-err disable فعال است.

Rapid Spanning Tree Protocol (RSTP) :

همانطورکه گفته شد، به صورت کلی درSTPزمانی بین۳۰ تا ۵۲ثانیه طول میکشد تاconvergenceدر شبکه صورت گیرد،مخصوصاً زمانیکه تغییر کوچکی درساختار شبکه رخ می‌دهد،می‌بایست این زمان سپری شود تا مجدداً کل شبکه با پروتکلstp همگرا شود. این زمان، زمان بسیار زیادی است وجهت برطرف کردن این مشکلRapid stpبراساس استانداردIEEE W802.1 W بوجود آمد تازمان convergence را به ٦ ثانیه(3Hello) برساند!

انواع وضیعت **RSTP** تا رسیدن به وضعیت مطلوب پورت :

در STP پنج وضعیت disabled , blocking , listening , learning و forwarding داشتیم ولی در RSTP سه وضعیت زیر را داریم:

۱) **Discarding:** این وضعیت فقط BPDU دریافت می‌کند. این وضعیت در RSTP در واقع ترکیبی است از سه وضعیت listening , blocking , disabled در STP است. در این وضعیت frameها Drop می‌شوند و هیچMac addressای Learn نمی‌شود و به دلیل سرعت بالای پروتکل RSTP وضعیت listening احساس نیاز نشده و پورت سریعاً به حالت negotiate در میاید.

۲) **Learning**: علاوه بر دریافت BPDU ، ارسال BPDU را انجام می‌دهد و جدول MAC را نیز بروز می‌کند. در این وضعیتframe ها dropمی‌شوند ولی mac address ها را در سوئیچ نگهداری میکند یا به اصطالح learn میشوند.

۳) **Forwarding**: در این حالت سوئیچ فعالیت طبیعی خودش را انجام میدهد و frameهای ورودی بر اساسmac addressهایی که در سوئیچ learn شده اند ، فرستاده می شوند.

نقش های پورت در**RSTP** :

- Root Port: پورتی که از طریق آن با کمترین Cost به Bridge Root می‌رسیم.
- Designated Port: پورتی که میتواند یک سوئیچ دیگر را با کمترین Cost به Root Bridge برساند.
- Alternate port: پورت Backup برای RP .
- Backup port: پورتBackup برای Designated port.
- Disabled port: پورت غیرفعال که در Spanning Tree استفاده نمی شود.
- Edge port : پورتی که به End User متصل است.

عملکرد BPDU ها در RSTP :

برای سازگاری بیشتر پروتکل RSTP با STP همچنان BPDU ها بر اساس استاندارد 802.1q فرستاده می شوند. BPDU ها هر ۲ ثانیه یکبار برای همسایه‌ها از طریق تمام پورت‌ها ارسال میشود و زمانیکه به اندازه ۳ پکت BPDU جوابی از همسایه مورد نظر دریافت نگردد، پورت در نظر میگیرد که همسایه‌ای وجود ندارد و پورت به وضعیت learning می‌رود.

RSTP Convergence :

Covergence به مرحله ای گفته میشود که در لحظه اول تمامی سوئیچ ها خودشان را root switch در نظر میگیرند و شروع به ارسال BPDU می کنند، پس از ارسال و دریافت BPDU ها از سوئیچ های دیگر، root switch در شبکه انتخاب می‌شود و دیگر هیچ سوئیچی BPDU ارسال نمی‌کند مگر سوئیچ Root.

در واقع **Convergence** دو مرحله دارد:

- ✓ انتخاب سوئیچ **root** یا همان **RB**.
- ✓ انتخاب وضعیت پورت یعنی همان **root port , Designated port , Alternate port , Backup port.**

Port types (انواع پورت‌ها) :

Edge Port : همانطور که از نام پورت پیداست، منظور پورتهایی هستند که به Hostها یا PC ها در شبکه متصل هستند و در واقع لبه شبکه را تشکیل می‌دهند. برای جلوگیری از ارسال BPDU ها Port fast را فعال می کنیم ، BPDU Gaurdو Loop Guard را نیز انتخاب می‌کنیم.

Root Port : پورتی از یک سوئیچ سیسکو که جهت برقراری ارتباط با RB مورد استفاده قرار میگیرد را RP می‌نامند. در واقع برای برقراری ارتباط با RB تنها از یک مسیر استفاده میشود و انتخابRP مناسب به cost مسیرهای موجود برای دستیابی بهRB بستگی دارد.

point-to-Point Port : برای اتصال دو سوئیچ به یکدیگر استفاده میشود، زمانی که دو سوئیچ به صورت مستقیم به یکدیگر متصل هستند در نظر گرفته می‌شود که پورت‌ها به صورت Full duplex با یکدیگر negotiate کنند، اگر وضعیت Half duplex باشد، بدین معناست که بین دو سوئیچ deviceهای دیگری هم وجود دارد (در حالت half duplex دیگر پورت‌ها را point to Point نمی‌نامیم).

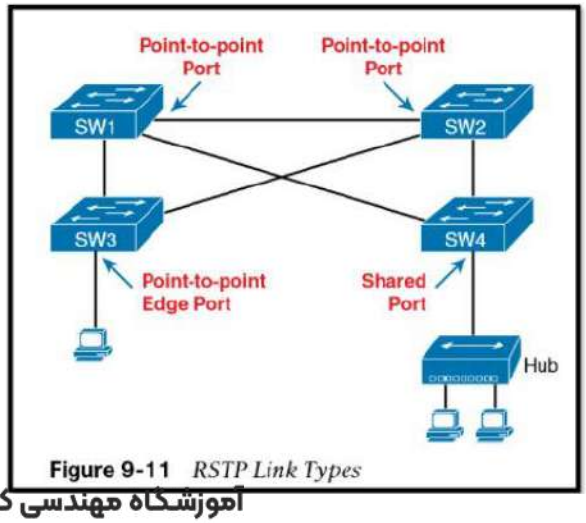


Figure 9-11 *RSTP Link Types*

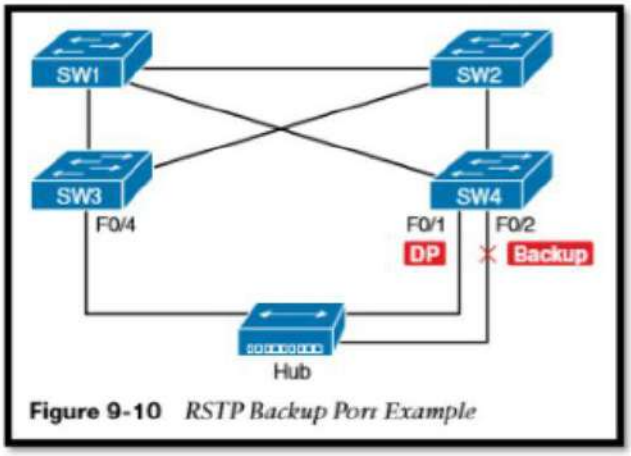


Figure 9-10 *RSTP Backup Port Example*

در جدول زیر وضعیت RSTP با CST مقایسه شده است:

Classic Spanning-Tree	Rapid Spanning-Tree	Port active in topology?	Learns MAC addresses?
Blocking	Discarding	No	No
Listening	Discarding	Yes	No
Learning	Learning	Yes	Yes
Forwarding	Forwarding	Yes	Yes

تنظیمات RSTP :

برای فعال کردن RSTP بر روی یک پورت که نقش Edge Port را در شبکه ایفا می کند، می‌بایست از دستور زیر استفاده کنید:

```
Switch(config-if)# spanning-tree portfast
```

اما برای فعال کردن RSTP بر روی یک پورت که نقش Point to Point را دارد و قرار است با سوئیچ مجاور به صورتFull Duplex کار کند ، از دستور زیر استفاده می‌کنیم:

```
Switch(config-if)# spanning-tree link-type point-to-point
```

تنظیمات RP+ یا Rapid Per-Valan spanning tree protocol (RVSTP)

برای فعال کردن RPVST بر روی کل سوئیچ سیسکو از دستور زیر استفاده کنید :

```
Switch(config)#spanning-tree mode rapid-pvst
```

برای برگشتن به حالت پیش فرض PVST از دستور زیر استفاده میکنیم:

```
Switch(config)# spanning-tree mode pvst
```

```
To change STP mode
==========================================
Switch(config)#spanning-tree mode [pvst I rapid-pvst I mst ]
```

نکته: در حالتی که RPVST سوئیچ شما، PVST را هم ساپورت می‌کند، در واقع شما هم stp که بر مبنای IEEE 802.1D است را ساپورت می‌کنید و هم RSTP را، که به صورت ایده‌آل برای سوییچ فعال می‌باشد.

عیب بابی پروتکل RSTP :

برای عیب‌یابی و بررسی وضعیت RSTP از دستور زیر استفاده میکنیم:

Switch# show spanning-tree vlan vlan-id

Multiple Spanning Tree (MST) :

زمانی تعدادVLAN ها خیلی زیاد باشند و ما از PVST یا Per-VLAN RSTP استفاده کرده باشیم، برای هر VLAN نیاز به محاسبه جداگانه دارد که باعث مصرف زیاد CPU و RAM می‌شود. برای برطرف کردن این مشکل ما از MST استفاده می‌کنیم. به این صورت که VLAN هایی که قرار است RB یکسانی داشته باشند را در یک instance قرار می‌دهیم، به طور مثال vlan های ۱۱ تا ۲۰ را در ۱ instance و ۲۱ تا ۳۰ را در ۲ instance قرار می‌دهیم.

نکته۱ : امکان ساخت حداکثر ۱۶ تا instance وجود دارد.

نکته۲: MST که فعال شود، ۰ instance ایجاد می شود و تمام vlan ها به صورت پیش فرض عضو این instance می‌شوند.

نکته۳ : به کلیه سوئیچ هایی که MST را اجرا کنند و در یک ناحیه قرار بگیرند به اصطلاح MST Region گفته می‌شود.

تاریخچه STP به صورت خلاصه:

Name	Based on STP or RSTP?	# Trees	Original IEEE Standard	Config Parameter
STP	STP	1 (CST)	802.1D	N/A
PVST+	STP	1/VLAN	802.1D	pvst
RSTP	RSTP	1 (CST)	802.1w	N/A
Rapid PVST+	RSTP	1/VLAN	802.1w	rapid-pvst
MSTP	RSTP	1 or more*	802.1s	mst

Spanning Tree Protocols						
	Legacy STP	PVST	PVST+	RSTP	RPVST+	MST
Algorithm	Legacy ST	Legacy ST	Legacy ST	Rapid ST	Rapid ST	Rapid ST
Defined By	802.1D-1998	Cisco	Cisco	802.1w, 802.1D-2004	Cisco	802.1s, 802.1Q-2003
Instances	1	Per VLAN	Per VLAN	1	Per VLAN	Configurable
Trunking	N/A	ISL	802.1Q, ISL	N/A	802.1Q, ISL	802.1Q, ISL

EtherChannel :

فناوری اترچنل (EtherChannel) توسط کالپانا (Kalpana) در اوایل دهه‌ی ۱۹۹۰ اختراع شد اما در سال ۱۹۹٤ کمپانی سیسکو این سیستم را از وی خریداری کرد. سپس در سال ۲۰۰۰ انجمن مهندسان برق و الکترونیک (IEEE) نسخه‌ی 802.3ad اترچنل که یک نسخه‌ی استاندارد باز بود را تصویب کرد. به Etherchannel، Portchannel یا Bonding هم گفته میشود.

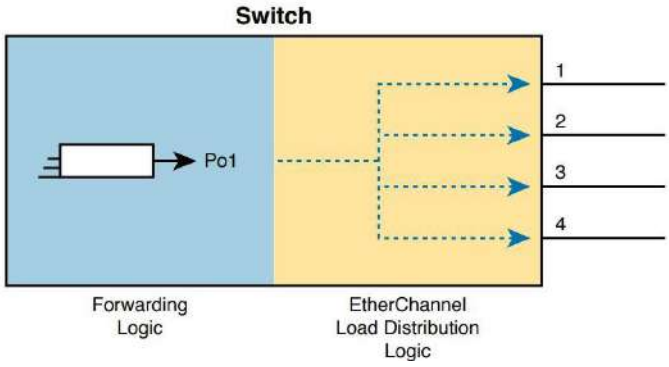
تکنولوژی EtherChannel همچنین به عنوان:

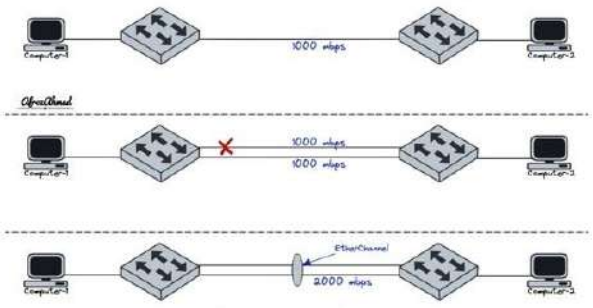
- NIC Teaming در مایکروسافت
- Link Aggregation در سیسکو
- Ethernet Bridge در لینوکس

شناخته می‌شود.

EnterChannel (که به آن **logical link** نیز گفته می‌شود،) توانمندی می‌باشد که اجازه می‌دهد چندین پورت فیزیکی سوئیچ در یک گروه منطقی قرار بگیرند که به منظور دسترسی به پهنای باند بالاتر و ایجاد تحمل خطا در اتصالات بین سوئیچ‌ها استفاده می‌شود. همچنین با پیوند پورت‌ها اگر هر کدام از پورت‌ها به هر دلیلی غیرفعال (failover) شوند، عملکرد سیستم متوقف نخواهد شد و پورت دیگر جایگزین آن می‌شود.

*توجه شود که به طور معمول Tree Spanning لینک های جایگزین را مسدود می کند اما EtherChannels قابلیت **Load Balancing** را بدون مسدود کردن پورت ها برای ما ایجاد می کند. مدلی که دستگاه برای load balance استفاده می‌کند Per session است.

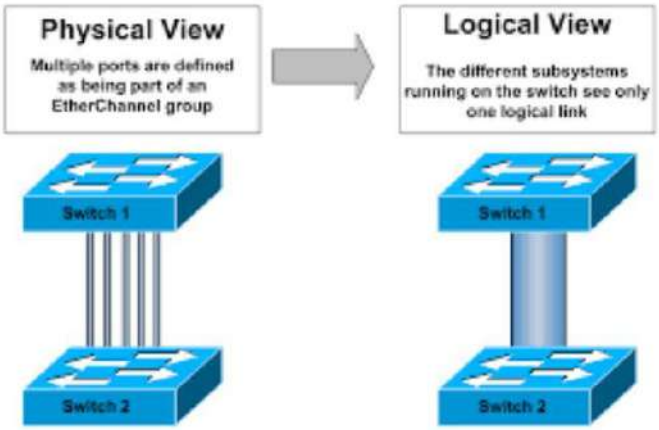




مثال یک: در این لابراتور بین دو سوئیچ سیسکو ما دو پورت فیزیکی را که هر کدام با سرعت 1G کار می کنند در داخل یک گروه منطقی به نام-Channel Groupقرار خواهیم داد که حال این پورت منطقی از مجموعه پهنای باند دو لینک فیزیکی استفاده می کند و پهنای باند معادل 2G برای این اتصال منطقی بوجود می آید که در صورت قطع شدن هر یک از اتصالات فیزیکی داخل این گروه، حمل اطلاعات توسط سایر اتصالات موجود در گروه انجام می‌گیرد.

شما در گروه EnterChannel می‌توانید از پورت‌های Fast Ethernet و GigabitEthernet بر روی سوئیچ‌ها استفاده کنید که میزان پهنایی باند اتصال شما بین سوئیچ‌ها افزایش یابد. مثلا دو یا چهار یا هشت پورت فیزیکی را داخل یک گروه قرار می‌دهید.

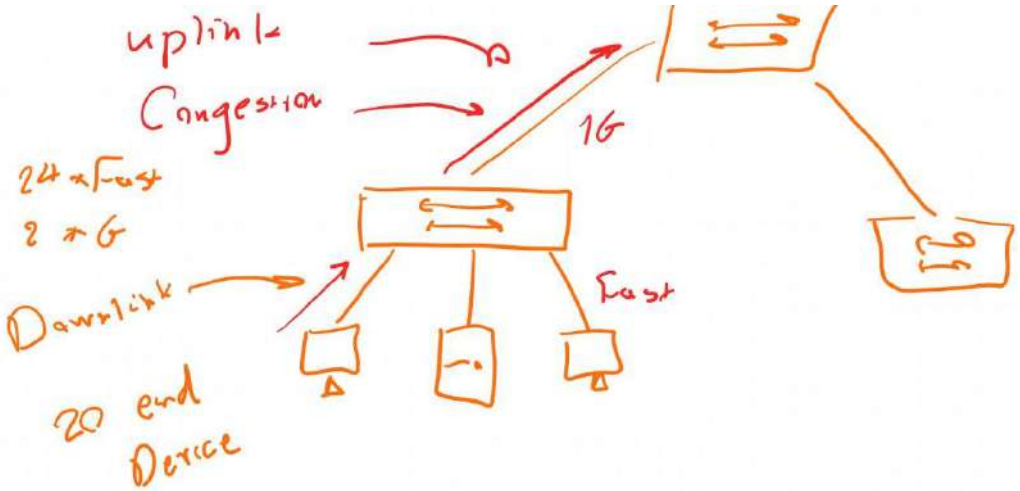
مثال دو: فرض کنید یک شرکت دارای دو سوئیچ است که از طریق یک پورت Fast Ethernet به یکدیگر متصل شده اند. بعد از مدتی این شرکت گسترش پیدا می کند و دیگر لینک Fast Ethernet جوابگوی نیاز آنها نخواهد بود. اگر یک پورتFast Ethernet دیگر را بین این دو سوئیچ متصل کنیم پروتکلTree Spanning برای جلوگیری از ایجاد Loop در شبکه یکی از این دو پورت را Block می کند. یکی از راه حل ها ، خرید یک سوئیچ دارای پورت Gigabit Ethernet است که اینکار مقرون به صرفه نیست. راه حل منطقی استفاده از EtherChannel است.

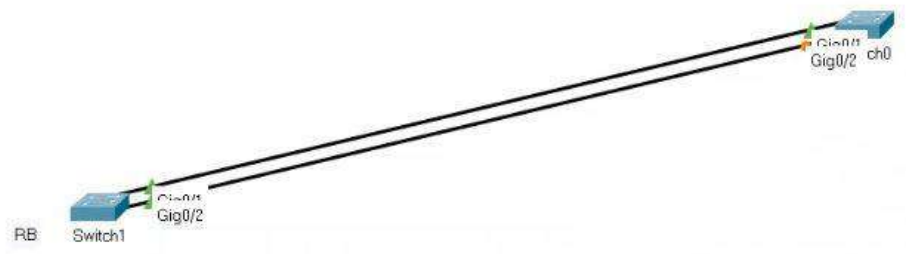


تنها موردی که در استفاده از این تکنولوژی باید در نظر گرفت داشتن پورت های آزاد است. ترافیک براساس MAC Address یا IP Address یا Port Address مبدا یا مقصد بین لینک ها تقسیم می‌شود و از طریق Config Mode قابل تنظیم است.

Switch(config)#port-channel load-balance {dst-ip|Srt-ip|dst-mac|srt-mac| src-dst-ip| dst-dst-ip}

مثال سه: فرض کنید End Device 20 با ارتباط Fast Ethernet به سوئیچی با ۲۴ پورت fast و ۲ پورت Gig به عنوان ارتباط Downlink متصل شده اند. این سوئیچ را نیز به سوئیچ دیگری با ارتباط 1 Giga Ethernet به عنوان ارتباط Uplink متصل میکنیم. فرض میکنیم هر دستگاهی به طور میانگین 60Mbps تبادل دیتا دارد(ارسال و دریافت). به این صورت میزان پهنای باند downlink ما از 1G فراتر خواهد رفت (مثلا G۱,۲). در این سناریو ما روی لینک بین سوئیچ یک و سوئیچ دو Congection (سر رفتن ، پُرشدن) خواهیم داشت. فرض کنیم یک اتوبان ده لاین داریم که میخواهیم دوازده خودرو همزمان عبور کنند. که مقدور نیست. برای حل مشکل شاید بشود در یک لاین دو خودرو را جای دهیم تا مشکل حل شود. دستگاه ها هم همچنین قابلیتی دارند که به buffer (مخزن)گفته میشود. این مخزن دیتاهایی که امکان ارسال دریافت برای آن ها در زمان مقدور نیست در آن قرار میگیرند که طبق متدهایی که موجود است بسته ها را به طور الویت ارسال و دریافت میکند. این اتفاق باعث تاخیر، delay ، packet lost خواهد شد که برای شبکه خوب نیست. برای حل این مشکل میتوان بین دو سوئیچ یک پورت 1G اضافه کرد. اما چونstpفعال است، خودکار یکی از پورتهای ما block میشود. برای رفع این مشکل به سراغ مفهومEtherchanelمیرویم که این دو ارتباطPhyisicalرا به یک ارتباطLogicalتبدیل کند.





پروتکل های مدیریتی EnterChannel:

برای مدیریت اتصال EtherChannel دو نوع پروتکل وجود دارد:

۱. **PAgP** (Port Aggregation Protocol) :

Port Aggregation Control Protocol
==========
- CISCO Prop.
- Auto / Desirable
- Auto Not send , just accept
- Desirable Send and Accept
- Max 8 port

- پروتکل انحصاری شرکت سیسکو (در صورتی می توانید از این پروتکل استفاده کنید که تجهیزات دو طرف اتصال شما Cisco باشد)

-دارای مُدهای Auto (درخواست ارسال نمیکند و فقط درخواست میپذیرد) و desirable (هم درخواست ارسال میکند هم دریافت میپذیرد).

- در این پروتکل فقط ۸ پورت میتوانند در Etherchannel قرار بگیرند.

نکته : نحوه تقسیم ترافیک بین پورت ها در EtherChannel به تعداد پورت ها بستگی دارد و قابل تغییر نیست. برای تقسیم مساوی ترافیک بهتر است تعداد لینک ۲، ٤، ۸ تا(2^n) باشد. در جدول زیر این مقادیر نشان داده شده است.

Number of Ports in the EtherChannel	Load Balancing
8	1:1:1:1:1:1:1:1
7	2:1:1:1:1:1:1
6	2:2:1:1:1:1
5	2:2:2:1:1
4	2:2:2:2
3	3:3:2
2	4:4

۲. **LACP** (Link Aggregation Control Protocol) :

Link Aggregation Control Protocol
==========
- IEEE 802.3ad
- Passive / Active
- Passive Not send , just accept
- Active Send and Accept
- Max 16 port but 8 port active

-این پروتکل مربوط به شرکت سیسکو نیست ولی توسط شرکت سیسکو و سایر شرکت‌های دیگر پشتیبانی می‌شود.

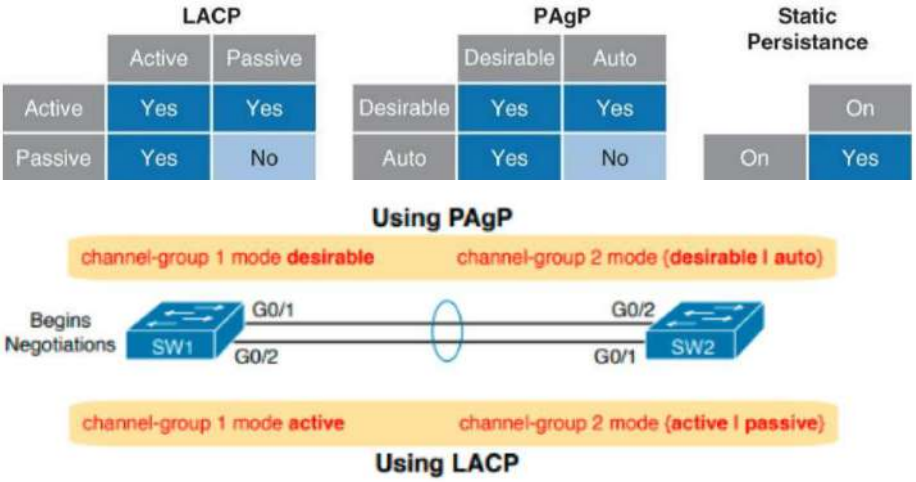
- طبق استاندارد 802.3ad فعالیت می‌کند.

-دارای مُدهای Passive (درخواست ارسال نمیکند و فقط درخواست میپذیرد) و active (هم درخواست ارسال میکند هم دریافت میپذیرد).

- max شانزده پورت میتوانند Etherchannel شوند ولی هشتای آن ترافیک روی آن قرار می‌گیرد.

نکته: مُد Static هم وجود دارد که هیچ پروتکل خاصی نیازی ندارد و مذاکره بین پورت اترنت به صورت دستی انجام می‌شود.

حالت‌هایی که برای مُدهای میتواند رخ دهد:



نکات Etherchanel:

- در پیکربندی EnterChannel ترتیب قرارگیری پورت‌های فیزیکی نباید حتماً به ترتیب یا پشت سر هم باشد یا حتما پورت‌ها بر روی یک Moduleقرار داشته باشند بلکه درصورتی که پورت‌ها به ترتیب پشت سر هم قرار نداشته باشند هم می‌توانند در داخل یک گروه قرار بگیرند.

- همه پورت های شرکت کننده در EnterChannel باید دارای یک سرعت و Duplex یکسان و همچنین Enable وفعال باشند.

- Accessیا Trunk یکسان

- Encapsulation (ISL یا 1.q) ، Allow vlan ، native vlan یکسان

- مدل Stp یکسان (stp، pvstp ،Rstp)

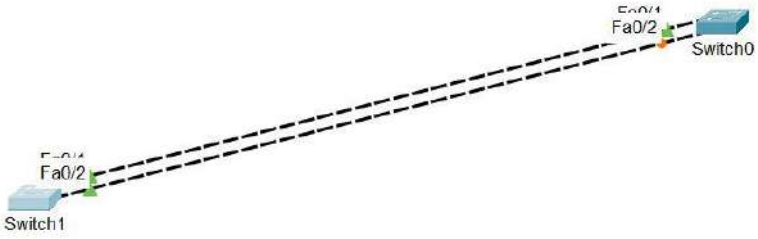
- در EnterChannel پروتکل LACPو PAgP با یکدیگر سازگار نمی باشند. (پروتکل مورد استفاده همه پورت‌ها باید یکی باشد.)

- حداکثر تعداد پورت هایی که می‌توان به EtherChannel اضافه کرد ۸پورت می‌باشد. یعنی حداکثر پهنای باندی که ما میتوانیم به آن دست پیدا کنیم، در Fast Ethernet پهنای باند ۸۰۰Mbps ، در Gigabit Ethernet پهنای باند 8 Gbps و درTen Gigabit Ethernet پهنای باند ۸۰Gbps خواهد بود.

- در صورت استفاده از EtherChannel در لایه سوم، IP را تنها به پورت منطقی اختصاص دهید نه به پورت های فیزیکی به صورت تک.

- تنظیماتی که روی Port Channel اعمال می کنیم روی تمام پورت ها مربوطه تاثیر می گذارد ولی تنظیماتی که شما به یک اینترفیس فیزیکی اعمال می کنید تنها روی همان اینترفیس تاثیر میگذارد.

پیکربندی EtherChannel :



Layer 2 EtherChannel

باید یک اینترفیس منطقی ایجاد و اینترفیس های فیزیکی مد نظر را به آن اضافه کنید.

مرحله۱) برای ایجاد Port Channel از دستور زیر استفاده می کنیم:

```
Switch(config)#interface port-channel ?
  <1-6>  Port-channel interface number
Switch(config)#interface port-channel 2
```

<1-6> به این معنی‌ست که در این دستگاه ۱ تا ٦ شماره می‌توان Portchannel داشت. همچنین اهمیت ندارد این شماره برای مابقی Port channelها یکسان باشد یا خیر. فقط برای Tshoot بهتر است یکسان باشند.

show interface status که گرفته شود وضعیت اینترفیس های فیزیکال را نشان میدهد. اینترفیس portchannel هم جزوی از این اینترفیس‌های فیزیکال می‌باشد، که در ابتدای کار notconnected است.

```
Switch#show interfaces status
Port      Name               Status       Vlan       Duplex  Speed Type
Po2                          notconnect   1          auto    auto
Fa0/1                        connected    1          auto    auto  10/100BaseTX
Fa0/2                        connected    1          auto    auto  10/100BaseTX
Fa0/3                        notconnect   1          auto    auto  10/100BaseTX
Fa0/4                        notconnect   1          auto    auto  10/100BaseTX
Fa0/5                        notconnect   1          auto    auto  10/100BaseTX
```

مرحله۲) برای اضافه کردن پورت های مورد نظر از دستور زیر استفاده می کنیم:

```
Switch#conf terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#int range fast 0/1-2
Switch(config-if-range)#channel-group 2 mode ?
  active     Enable LACP unconditionally
  auto       Enable PAgP only if a PAgP device is detected
  desirable  Enable PAgP unconditionally
  on         Enable Etherchannel only
  passive    Enable LACP only if a LACP device is detected
Switch(config-if-range)#channel-group 2 mode passive
```

همچنان با گرفتن show int status متوجه میشویم که interface portchannel، notconnected است. چرا؟ چون طرف مقابل را هنوز config نکردیم.

مرحله سوم) ساخت interface portchannel و اضافه کردن interfaceهای سوئیچ مقابلش

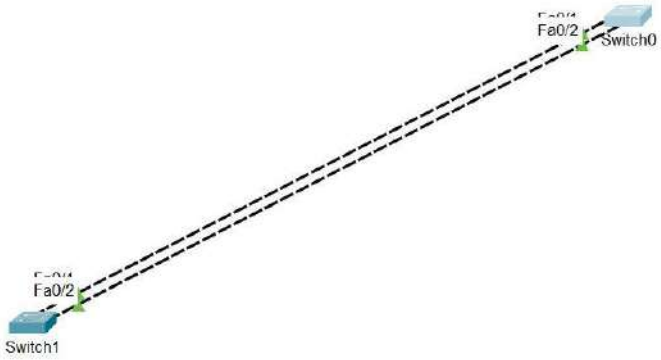
```
Switch(config)#interface port-channel ?
  <1-6>  Port-channel interface number
Switch(config)#interface port-channel 2
```

طبق مد انتخابی برای سوئیچ قبلی، فقط باید مد active برای این سوئیچ انتخاب میشد.

```
Switch(config)#interface range fast 0/1-2
Switch(config-if-range)#channel-group 2 mode active
```

حالا با گرفتن show int status متوجه میشویم که interface portchannel، connected شده است.

```
Switch(config)#do show int status
Port      Name               Status       Vlan       Duplex  Speed Type
Po2                          connected    1          auto    auto
```



مشاهده میشود که بعد از اعمال etherchannel هیچکدام از پورت‌ها blk نمی‌مانند.

دستور تغییر یا تعیین پروتکل مدیریتی Portchannel :

```
Switch(config)#int range fastEthernet 0/1-2
Switch(config-if-range)#channel-protocol ?
  lacp  Prepare interface for LACP protocol
  pagp  Prepare interface for PAgP protocol
```

نکته: جهت دیدن وضعیت EtherChannel از دستورات زیر استفاده کنید.

Switch#show etherchannel

```
Switch#show etherchannel
                Channel-group listing:
                ----------------------

Group: 2
----------
Group state = L2
Ports: 2 Maxports = 16
Port-channels: 1 Max Port-channels = 16
Protocol:   LACP
```

Switch#show etherchannel summary

```
Switch#show etherchannel summary
Flags:  D - down        P - in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate aggregator
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port


Number of channel-groups in use: 1
Number of aggregators:           1

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------------

2      Po2(SU)          LACP    Fa0/1(P) Fa0/2(P)
```

کدSU در سطر آخر یعنی:

S(اترچنل لایه ۲) و U(در حال استفاده)

قبل از اینکه up بشه ، SD بوده

S(اترچنل لایه ۲) و D(down)

Switch#show etherchannel load-balance

```
Switch#show etherchannel load-balance
EtherChannel Load-Balancing Operational State (src-mac):
Non-IP: Source MAC address
  IPv4: Source MAC address
```

Switch#show spanning-tree

```
Switch#show spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID     Priority    32769
              Address     0001.C90D.8CD7
              This bridge is the root
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    32769  (priority 32768 sys-id-ext 1)
              Address     0001.C90D.8CD7
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Po2              Desg FWD 9         128.27   Shr
```

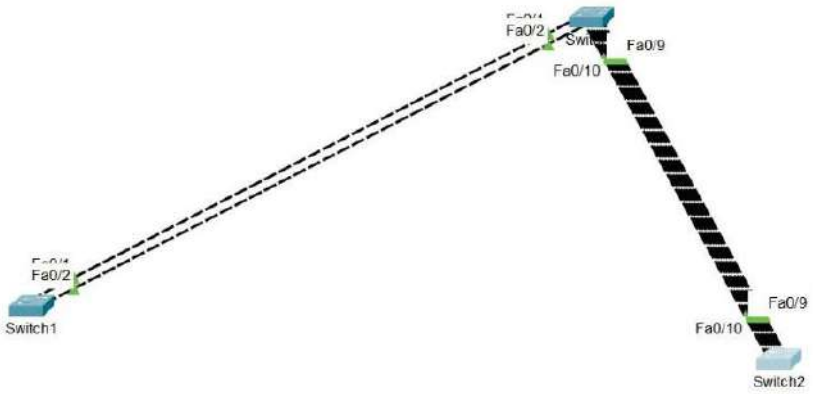
Layer 3 EtherChannel


```
switch(config)# interface TYPE MOD/NUM
switch(config-if)# no switchport
switch(config-if)# ip address A.B.C.D  E.F.G.H

sw1(config)# interface gi0/1
sw1(config-if)# no switchport
sw1(config-if)# ip address 192.168.1.1 255.255.255.0

sw2(config)# interface gi0/1
sw2(config-if)# no switchport
sw2(config-if)# ip address 192.168.1.2 255.255.255.0
```

Routing-Protocol

```
switch(config)# interface TYPE MOD/NUM
switch(config-if)# no switchport

Manual/PAgP/LACP

switch(config-if)# channel-group GRP_NUM mode on
switch(config-if)# ip address A.B.C.D E.F.G.H
```

مثال دوم:



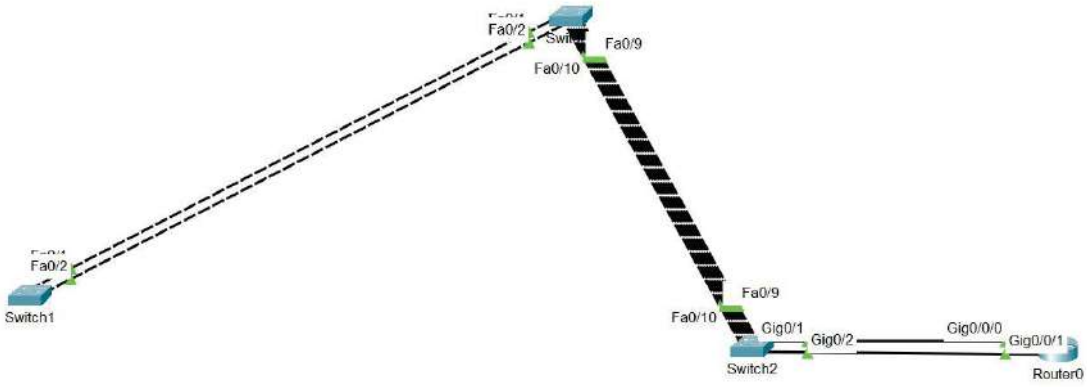
دسته راست به همان روشی که گفته شد

وضعیت سوئیچ میانی بعد از etherchannel :

```
Switch#show etherchannel summary
Flags:  D - down        P - in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate aggregator
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port


Number of channel-groups in use: 2
Number of aggregators:           2

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------------

2      Po2(SU)           LACP   Fa0/1(P) Fa0/2(P)
3      Po3(SU)           PAgP   Fa0/3(P) Fa0/4(P) Fa0/5(P) Fa0/6(P) Fa0/7(P) Fa0/8(P) Fa0/9(P) Fa0/10(P)
```

Show سوئیچ0

مثال سوم: وارد کردن روتر به سناریو



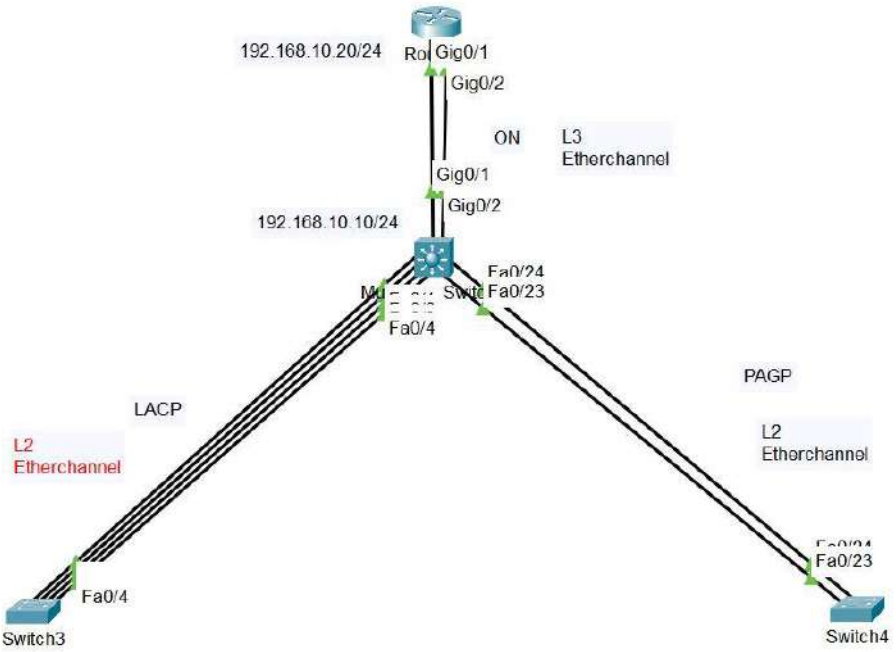

```
Switch#show etherchannel summary
Flags:  D - down        P - in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate aggregator
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port


Number of channel-groups in use: 2
Number of aggregators:           2

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------------

3      Po3(SU)           PAgP   Fa0/3(P) Fa0/4(P) Fa0/5(P) Fa0/6(P) Fa0/7(P) Fa0/8(P) Fa0/9(P) Fa0/10(P)
5      Po5(SU)           -      Gig0/1(P) Gig0/2(P)
```

Show سوئیچ 2

نکته۱: اگر سوئیچ به روتر به حالت Ethechannel به هم متصل شده باشند و ارتباط inter vlan ایجاده کرده باشیم، باید برای ارتباط بجای sub interface ،sub interface portchannel بسازیم.

نکته۲: ما هر تغییری بخواهیم روی اینترفیس های عضو portchannel اعمال کنیم، باید دستورات را روی Switch(config)#interface portchannel<number po> اعمال میکنیم. مانند: trunk،native vlan ، allow vlan و... .

مثال چهارم:



بازوی چپ و بازوی راست همانند مثال های قبل etherchannel در سطح لایه2 را تنظیم میکنیم(بازوی راست PAGP و بازوی چپ LACP). بازوی بالای mls را باید در سطح لایه سه etherchannel را تنظیم کنیم.

مرحله اول: ساخت<> portchannel

مرحله دو: رفتن به پورت های مربوطه ، سپس اجرای دستور no switchport (چون میخواهیم از این پورتها در لایه سه استفاده کنیم.) . همچنین فراموش نکنیم باید برای interface portchannel نیز دستور no switchport را اجرا کنیم.

مرحله سوم: عضویت اینترفیس‌ها به این portchannel (مثل قبل)

توجه: با گرفتن etherchannel summary، متوجه میشویم که portchannelی که ساختیم کُد RU مقابلش درج شده است. این به معنی آن است که این portchannel در لایه سه کار میکند.

```
Switch#show etherchannel summary
Flags:  D - down        P - in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate aggregator
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port


Number of channel-groups in use: 3
Number of aggregators:           3

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------------

1      Po1(SU)         LACP      Fa0/1(P) Fa0/2(P) Fa0/3(P) Fa0/4(P)
2      Po2(SU)         PAgP      Fa0/23(P) Fa0/24(P)
3      Po3(RU)         -         Gig0/1(P) Gig0/2(P)
```

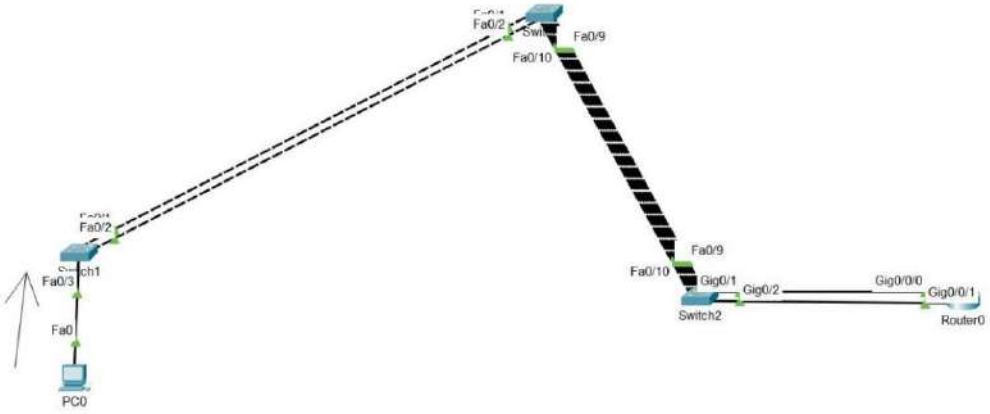
مرحله چهار(روتر): روشن کردن پورت‌ها و ساخت portchannel و عضویت پورت‌ها در این portchannel .

مرحله پنج: حال میتوانم به interface portchannel دو طرف ipبدهیم.

EtherChannel Load Distribution :

نحوه توزیع بار در **Etherchannel**:

یکی از مباحث مهمی که باید در EtherChannel مورد بررسی قرار گیرد نحوه ی توزیع بار بر روی لینک هایی که Aggregate شده اند میباشد. اگر تصور کرده اید که ترافیک ها بر روی لینک ها بصورت متوازن ارسال می شوند کاملا در اشتباه هستید برای توزیع بار در بین لینک هایی که Aggregate شده اند الگوریتم های متفاوتی وجود دارند که براساس الگوریتم های موجود توزیع بار بر روی لینک ها صورت می گیرد. به عنوان مثال درسناریوی زیر PC0 میخواهد دیتایی را به swh1 برساند. این سوئیچ بر اساس چه پارامتری متوجه میشود که این دیتا را از کدام پورت etherchannel باید ارسال کند؟



به طور پیشفرض این سوئیچ براساس src-mac ترافیک را روی پورت‌ها ارسال میکند

```
EtherChannel Load-Balancing Operational State (src-mac):
Non-IP: Source MAC address
  IPv4: Source MAC address
  IPv6: Source MAC address
```

شاخص های **load balance** به شرح ذیل میباشد که قابل تغییر هستند:

Configuration Keyword	Math Uses...	Layer
src-mac	Source MAC address	2
dst-mac	Destination MAC address	2
src-dst-mac	Both source and destination MAC	2
src-ip	Source IP address	3
dst-ip	Destination IP address	3
src-dst-ip	Both source and destination IP	3
src-port	Source TCP or UDP port	4
dst-port	Destination TCP or UDP port	4
src-dst-port	Both source and destination TCP or UDP port	4

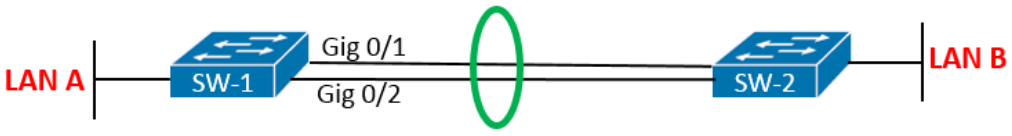
نحوه تغییر load-balance با دستور زیر :

```
Switch(config)#port-channel load-balance ?
  dst-ip        Dst IP Addr
  dst-mac       Dst Mac Addr
  src-dst-ip    Src XOR Dst IP Addr
  src-dst-mac   Src XOR Dst Mac Addr
  src-ip        Src IP Addr
  src-mac       Src Mac Addr
```

نکته : هر سوئیچ فقط می‌تواند load-balance ارسالی از خود را به دیگر دستگاه‌ها را config کند و در قبال دریافت دیتا از سوئیچ‌های دیگر اختیاری ندارد.

Source IP Address: اگر برای توزیع بار در EtherChannel از الگوریتم Source IP Address استفاده کنیم، سوییچ از ۳۲ بیت Source IP Address برای توزیع بار استفاده می کند. این توزیع بار کاملا بستگی به این دارد که چند لینک را با یکدیگر Aggregateکرده‌ایم.

اگر ۲ لینک را با یکدیگر Aggregate کنیم سوییچ از آخرین بیت Source IP برای توزیع بار بر روی لینک ها استفاده می‌کند از آنجایی که هر بیت دو حالت می تواند داشته باشد، یا ۰ باشد و یا ۱، پس برای دو لینک تنها یک بیت کفایت می‌کند. به تصویر زیر دقت کنید:



فرض کنیم دیتایی قرار است از سمت LAN A توسط کلاینتی با آدرس ۱۹۲,۱۶۸,۱,۱۰ به سمت LAN B ارسال شود دیتا زمانی که به سوییچ می رسد از آنجایی که پورت های Gig 0/1 و Gig 0/2 باهم Aggregate شده اند سوییچ به الگوریتم توزیع بار EtherChannelنگاهی می اندازد. الگوریتم مورد استفاده ی ماSource IP Address می‌باشد. در نتیجه سوییچ به بررسی آدرس Source IPمی پردازد آدرس ۱۹۲,۱۶۸,۱,۱۰ بصورت باینری معادل مقدار زیر می باشد:

۱۱۰۰۰۰۰۰,۱۰۱۰۱۰۰۰,۰۰۰۰۰۰۰۱,۰۰۰۰۱۰۱۰

از ۳۲ بیت آدرس بالا تنها بیت آخر برای ما اهمیت دارد بیت آخر در حال حاضر ۰ می باشد پس به راحتی متوجه نحوه ی توزیع بار بر روی لینک ها می شویم. به عنوان مثال سوییچ اینگونه بیان می کند که اگر آخرین بیت آدرس Source IP برابر با ۰ باشد دیتا باید از لینک Gig 0/1 ارسال شود و اگر آخرین بیت برابر با ۱ باشد دیتا باید از Gig 0/2 ارسال شود.

– اگر ٤ لینک را با یکدیگر Aggregate کنیم سوییچ از ۲ بیت آخر Source IP برای توزیع بار بر روی لینک ها استفاده می کند. چرا که با ۲ بیت می توانیم چهار حالت داشته باشیم.

۰۰۰۰۰۰۰۰,۰۰۰۰۰۰۰۰,۰۰۰۰۰۰۰۰,۰۰۰۰۰۰۰۰

۰۰۰۰۰۰۰۰,۰۰۰۰۰۰۰۰,۰۰۰۰۰۰۰۰,۰۰۰۰۰۰۰۱

۰۰۰۰۰۰۰۰,۰۰۰۰۰۰۰۰,۰۰۰۰۰۰۰۰,۰۰۰۰۰۰۱۰

۰۰۰۰۰۰۰۰,۰۰۰۰۰۰۰۰,۰۰۰۰۰۰۰۰,۰۰۰۰۰۰۱۱

برای مثال اگر دو بیت آخر برابر با ۰۰ باشند سوییچ دیتا را از لینک اول ارسال کرده، اگر دو بیت آخر برابر با ۰۱ باشند سوییچ دیتا را از لینک دوم ارسال کرده، اگر دو بیت آخر برابر با ۱۰ باشند سوییچ دیتا را از لینک سوم ارسال کرده و اگر دو بیت آخر برابر با ۱۱ باشند سوییچ دیتا را از لینک آخر یعنی لینک چهارم ارسال می کند.

- اگر ۸ لینک را با یکدیگر Aggregate کنیم سوییچ از ۳ بیت آخر Source IP برای توزیع بار بر روی لینک ها استفاده می کند چرا که با ۳ بیت می توانیم هشت حالت داشته باشیم.

۰۰۰۰۰۰۰۰,۰۰۰۰۰۰۰۰,۰۰۰۰۰۰۰۰,۰۰۰۰۰۰۰۰

۰۰۰۰۰۰۰۰,۰۰۰۰۰۰۰۰,۰۰۰۰۰۰۰۰,۰۰۰۰۰۰۰۱

۰۰۰۰۰۰۰۰,۰۰۰۰۰۰۰۰,۰۰۰۰۰۰۰۰,۰۰۰۰۰۰۱۰

۰۰۰۰۰۰۰۰,۰۰۰۰۰۰۰۰,۰۰۰۰۰۰۰۰,۰۰۰۰۰۰۱۱

۰۰۰۰۰۰۰۰,۰۰۰۰۰۰۰۰,۰۰۰۰۰۰۰۰,۰۰۰۰۰۱۰۰

۰۰۰۰۰۰۰۰,۰۰۰۰۰۰۰۰,۰۰۰۰۰۰۰۰,۰۰۰۰۰۱۰۱

۰۰۰۰۰۰۰۰,۰۰۰۰۰۰۰۰,۰۰۰۰۰۰۰۰,۰۰۰۰۰۱۱۰

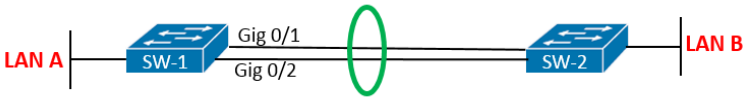
۰۰۰۰۰۰۰۰,۰۰۰۰۰۰۰۰,۰۰۰۰۰۰۰۰,۰۰۰۰۰۱۱۱

برای مثال اگر سه بیت آخر برابر با ۰۰۰ باشند سوییچ دیتا را از لینک اول ارسال می کند، اگر سه بیت آخر برابر با ۰۰۱ باشند سوییچ دیتا را از لینک دوم ارسال می کند و الی آخر.

Destination IP Address: اگر برای توزیع بار در EtherChannel از الگوریتم Destination IP Address استفاده کنیم، سوییچ از ۳۲ بیت Destination IP Address برای توزیع بار استفاده می کند این توزیع بار کاملا بستگی به این دارد که چند لینک را با یکدیگر Aggregate کرده ایم. نحوه ی توزیع بار در این الگوریتم دقیقا مشابه با الگوریتم Source IP Address می باشد، با این تفاوت که به جای استفاده از آدرس Source IP از آدرس Destination IP برای محاسبات توزیع بار استفاده می کند.

ترکیبی از Source IP Address و Destination IP Address : در این حالت سوییچ از ۳۲ بیت Source IP Address به همراه ۳۲ بیت Destination IP Address برای توزیع بار استفاده می کند. این توزیع بار کاملا بستگی به این دارد که چند لینک

را با یکدیگر Aggregate کرده ایم نحوه ی توزیع بار در این الگوریتم به این صورت می باشد که همانند الگوریتم Source IP براساس تعداد لینک ها تعداد بیت هایی که مورد بررسی قرار میگیرند مشخص می شود. به مثال زیر دقت کنید:Address



اگر ۲ لینک را با یکدیگر Aggregate کنیم سوییچ از آخرین بیت Source IP و Destination IP برای توزیع بار بر روی لینک ها استفاده می کند. فرض کنید دیتایی قرار است از سمت LAN A توسط کلاینتی با آدرس ۱۹۲,۱۶۸,۱,۱۰ به سمت کلاینتی با آدرس ۱۹۲,۱۶۸,۱,۱۱ که در LAN B قرار دارد ارسال شود. دیتا زمانی که به سوییچ می رسد از آنجایی که پورت های Gig 0/1 و Gig 0/2 باهم Aggregate شده اند سوییچ به الگوریتم توزیع بار EtherChannel نگاهی می اندازد.

الگوریتم مورد استفاده ی ما ترکیبی از Source و Destination آدرس IP می باشد در نتیجه سوییچ به بررسی آدرس Source IPو Destination IP می پردازد آدرس ۱۹۲,۱۶۸,۱,۱۰ که آدرس Source می باشد بصورت باینری معادل مقدار زیر می باشد:

۱۱۰۰۰۰۰۰,۱۰۱۰۱۰۰۰,۰۰۰۰۰۰۰۱,۰۰۰۰۱۰۱۰

آدرس ۱۹۲,۱۶۸,۱,۱۱ که آدرس Destination می باشد بصورت باینری معادل مقدار زیر می باشد:

۱۱۰۰۰۰۰۰,۱۰۱۰۱۰۰۰,۰۰۰۰۰۰۰۱,۰۰۰۰۱۰۱۱

در این تصویر بین دو سوییچ ما دو لینک داریم در نتیجه سوییچ تنها به یک بیت آخر توجه می کند اما کدام بیت؟ بیت مربوط به آدرس Source و یا بیت مربوط به آدرس Destination ؟ در حقیقت به هیچکدام. ابتدا سوییچ مقدار باینری شده‌ی آدرس های Sourceو Destination را باهم **XOR** کرده و سپس آخرین بیت حاصل از XOR را برای توزیع بار استفاده می کند.

۱۱۰۰۰۰۰۰,۱۰۱۰۱۰۰۰,۰۰۰۰۰۰۰۱,۰۰۰۰۱۰۱۰

XOR

۱۱۰۰۰۰۰۰,۱۰۱۰۱۰۰۰,۰۰۰۰۰۰۰۱,۰۰۰۰۱۰۱۱

=

۰۰۰۰۰۰۰۰,۰۰۰۰۰۰۰۰,۰۰۰۰۰۰۰۰,۰۰۰۰۰۰۰۱

در خروجی بالا بیت آخر حاصل از XOR برابر با ۱ قرار گرفته است. حال ممکن این ترافیک یعنی از مبدا ۱۹۲,۱۶۸,۱.۱۰ به مقصد ۱۹۲,۱۶۸,۱,۱۱ از لینک Gig 0/1 ارسال شود و اگر دیتای دیگری به سوییچ رسید که آخرین بیت حاصل از XOR آن برابر با ۰ بود از لینک دوم ارسال شود.

اگر ٤ لینک را با یکدیگر Aggregate کنیم، سوییچ از ۲ بیت آخر Source IP و Destination IP بصورتXOR شده برای توزیع بار بر روی لینک ها استفاده می کند چرا که با ۲ بیت می توانیم چهار حالت داشته باشیم.

اگر ۸ لینک را با یکدیگر Aggregate کنیم سوییچ از ۳ بیت آخر Source IP و Destination IP بصورتXOR شده برای توزیع بار بر روی لینک ها استفاده می کند چرا که با ۳ بیت می توانیم هشت حالت داشته باشیم.

Source MAC Address: اگر برای توزیع بار در EtherChannel از الگوریتم Source MAC Addressاستفاده کنیم، سوییچ از ٤٨ بیت Source MAC Address برای توزیع بار استفاده می کند این توزیع بار کاملا بستگی به این دارد که چند لینک را با یکدیگر Aggregate کرده ایم نحوه ی توزیع بار در این الگوریتم دقیقا همانند الگوریتم Source IP Address می باشد.

Destination IP Address: اگر برای توزیع بار در EtherChannel از الگوریتمDestination MAC Address استفاده کنیم، سوییچ از ٤٨ بیت Destination MAC Address برای توزیع بار استفاده می کند. این توزیع بار کاملا بستگی به این دارد که چند لینک را با یکدیگر Aggregate کرده ایم. نحوه ی توزیع بار در این الگوریتم دقیقا همانند الگوریتمDestination IP Address می باشد.

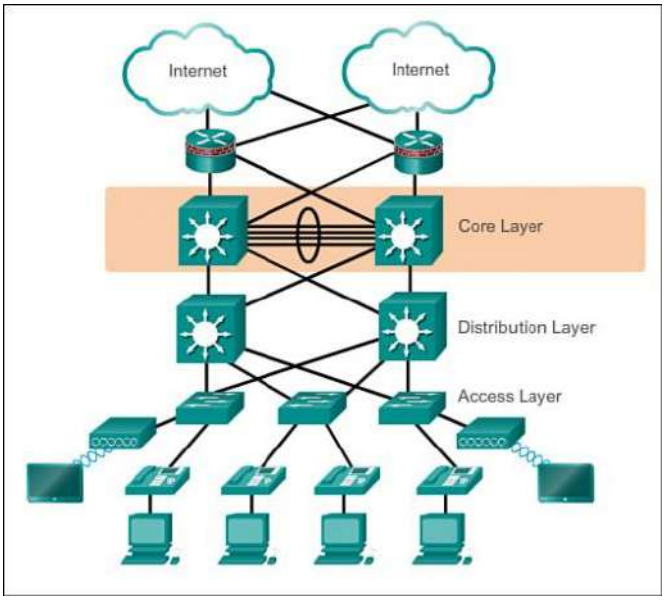
ترکیبی از Source MAC Address و Destination MAC Address : در این حالت سوییچ از ٤٨ بیت Source MAC Address به همراه ٤٨ بیت Destination MAC Address برای توزیع بار استفاده می‌کند. این توزیع بار کاملا بستگی به این دارد که چند لینک را با یکدیگر Aggregate کرده ایم. نحوه ی توزیع بار در این الگوریتم دقیقا همانند الگوریتم ترکیبی از Source IP Addressو Destination IP Address می باشد.

TCP/UDP Port Numbers: در این الگوریتم می توان نحوه ی توزیع بار را براساس شماره ی پورت مشخص کرد. برای مثال می توان گفت ترافیک هایی که مقصدشان سرویس های وب یعنی پورت های ۸۰ و ٤٤٣ می‌باشد از یک لینک ارسال شوند و ترافیک های دیگر از لینکی دیگر. (این الگوریتم در تمامی سوییچ ها پشتیبانی نمی شود.)

نکته: دستور تشخیص اینکه متوجه شویم دیتای ما از کدام پورت Portchannel خارج میشود:

```
SW1# test etherchannel load-balance interface po1 mac 0200.0000.0001 0200.1111.1111
Would select Gi1/0/22 of Po1

SW1# test etherchannel load-balance interface po1 mac 0200.0000.0001 0200.1111.1112
Would select Gi1/0/22 of Po1

SW1# test etherchannel load-balance interface po1 mac 0200.0000.0001 0200.1111.1113
Would select Gi1/0/22 of Po1
```

Port Security :



مکانیزیمی امنیتی است که که به ما کمک می‌کند در لایه دو کنترل مناسبی داشته باشیم و بتوانیم جلوی بسیاری از حملات را بگیریم. Port Security کنترل می‌کند که چندMAC addressروی یک پورت اجازه استفاده دارند.

بر اساس طراحی سه لایه‌ای سیسکو، دسترسی ها از طریق لایه Access ایجاد می‌شود که عمده مشکلات امنیتی به دلیل عدم کنترل این دسترسی‌ها صورت می‌پذیرد.

برای جلوگیری از اینکه کاربر نتواند دستگاه های مختلف را به سوئیچ وصل نکند میتوان از port security استفاده کرد و براساس MAC address این محدودیت را برای هر پورت اعمال کرد. همچنین port security می‌تواند شبکه را در برابر نرم افزارهای مخرب که می توانند هزاران فریم را در شبکه با MAC Addressهای متفاوت ارسال کنند محافظت کند.

Switchport Security در سوئیچ‌های اترنت، از اتصال کامپیوترهای بیگانه به شبکه جلوگیری می‌کند. سوییچ آدرس **MAC** کامپیوتر فرستنده قاب (Frame) اترنت را از هدر آن خوانده و با لیست آدرس های MAC مجاز که از قبل ایجاد و به سوییچ معرفی شده تطبیق می‌دهد. اگر سوییچ آدرس MAC مورد نظر را غیر مجاز تشخیص دهد، از ورود ترافیک به شبکه جلوگیری می‌کند.

به‌عنوان مثال می‌توان مشخص کرد چه تعداد دستگاه‌هایی می‌توانند از طریق یک پورت به سوئیچ متصل شوند. یا اینکه مشخص کرد چه آدرسی می‌تواند از یک پورت سوئیچ استفاده کند.

با استفاده از Port Security می‌توان کامپیوترهایی را که به یک پورت سوئیچ متصل می‌شوند از جهات مختلفی محدود کرد. شاید در شبکه نیاز باشد که تعداد محدودی کامپیوتر به سوئیچ وصل شوند یا اگر کاربری لپ‌تاپ خود را به شکل فیزیکی به سوئیچ متصل کرد، ارتباط برقرار نشود.

*نکته۱: رفتار پیش‌فرض سوییچ سیسکو در مواجهه با ترافیکی که آدرس مک فرستنده آن معتبر نیست، این است که پورت را shut می‌کند. ادمین سوئیچ می‌بایست برای دوباره فعال کردن اینترفیسی که توسط port security غیرفعال شده است، اینترفیس را یک بار shut و سپس no shut کند.

نکته۲: کانفیگ Port Security فقط روی پورت‌های Access mode در سطح سوئیچ‌های access (سوئیچ‌هایی که در سطح end deviceها فعالیت میکنند) اعمال می‌شود.

نکته۳: به صورت پیشفرض مکانیزم Port security ، disable میباشد.

نکته٤: اینترفیس به روش‌های زیر macها را learn می‌کند:

- ✓ **Dynamic** حالت معمولی که تمام Address MAC ها یاد می گیرد و اجازه اتصال می دهد اما اگر دستگاه reload شود پاک می‌شود .
- ✓ **Static** تنها به Address MAC هایی که ما تعیین می‌کنیم اجازه دسترسی می‌دهد.
- ✓ **Sticky** به صورت اتوماتیک Address MAC ها را ثبت می کند با این تفاوت که این تعداد آدرس ها ثبت شده محدود هستند.

دستورات Port security:

```
2950(config)# interface fastethernet|gigabit 0/port_# (1)
2950(config-if)# switchport mode access (2)
2950(config-if)# switchport port-security (3)
2950(config-if)# switchport port-security maximum value (4)
2950(config-if)# switchport port-security violation protect|restrict|shutdown (5)
2950(config-if)# switchport port-security mac-address MAC_address (6)
2950(config-if)# switchport port-security mac-address sticky (7)
```

(1) در ابتدا باید به اینترفیسی وارد شوید که قصد دارید تا محدودیت‌های امنیتی را بر روی آن‌ها اعمال کنید.

(2) با استفاده از این حالت، اینترفیس در حالتAccessقرار می‌گیرد.توجه داشته باشید که کلاینت‌ها به اینترفیس‌هایAccessمتصل می‌شوند.

(3) ویژگی Port Security با استفاده از دستور سوم فعال می‌شود.

(4) با استفاده از دستور چهارم می‌توان بیشترین تعداد کامپیوتری که می‌توانند به پورت متصل شوند را مشخص کرد. (به طور پیش فرض ۱ است، و تا ۱۳۲ میتوان آن را مقداردهی کرد).

(۵) با استفاده از دستور بعد می‌توان مشخص کرد که اگر تعداد کامپیوترهای متصل شده به پورت از تعداد MAX که در دستور قبل مشخص شده بیشتر شود، چه محدودیتی اعمال شود. (به طور پیش فرض محدودیت shuudown است).

(٦) با این دستور می بایست آدرس فیزیکی مورد نظر خود را مشخص نماییم تا تنها این آدرس مجاز محسوب شود و دسترسی این آدرس فیزیکی به شبکه برقرار گردد. در نظر داشته باشید اگر قصد مجاز نمودن ۲ آدرس را داشته باشیم می بایست این دستور را ۲ بار استفاده نموده و آدرس های مورد نظر خود را وارد نماییم . اگر از حالت پیش فرض استفاده نمودیم و تنها یک آدرس مجاز شد تنها یک آدرس فیزیکی را وارد خواهیم نمود.

(۷) اگر تعداد زیادی آدرس فیزیکی وجود دارد و یا پیدا نمودن این آدرس ها برای ما دشوار است می توان از قابلیت Sticky نیز استفاده نمود و دستگاه به صورت اتوماتیک اولین آدرس هایی که روی پورت های مد نظر ما یاد می گیرد را به عنوان آدرس مجاز شناسایی نماید. به منظور این کار به جای دستور(mac) از دستور sticky استفاده می نماییم.

محدودیت های قابل اعمال برایPort Security :

Protect: در این حالت ترافیک مربوط به دستگاه غیر مجاز Drop می شود و هیچ logی را ثبت نمی‌کند.

Restrict : همانند حالت قبل ترافیک مربوط به دستگاه غیر مجاز Drop می شود و علاوه بر این Log نیز تولید می کند.

ShutDown: سخت گیرانه‌ترین حالت می باشد که با دریافت ترافیک غیرمجاز پورت مربوطه در حالت Err-Disable قرار می‌گیرد و پورت خاموش می شود و برای خارج کردن آن از این حالت باید وارد تنظیمات سوئیچ شد و پورت مورد نظر را خاموش و روشن کرد.

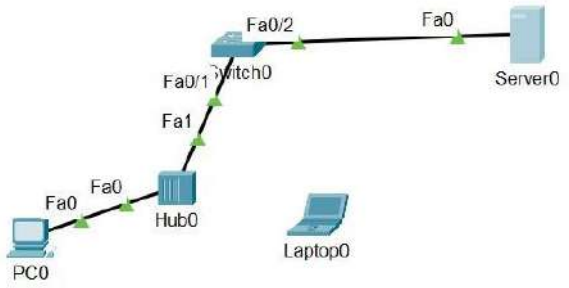
نکته: با دستور زیر می توانید این کار را به صورت خودکار انجام دهید:

Switch(config)#errordisable recovery cause secure-violation

Option on the switchport port-security violation Command	Protect	Restrict	Shutdown
Discards offending traffic	Yes	Yes	Yes
Sends log and SNMP messages	No	Yes	Yes
Disables the interface by putting it in an err-disabled state, discarding all traffic	No	No	Yes

مثال ۱:

قصد داریم در این سناریوی ناامن(با وجود hub)، روی اینترفیس fa0/1 با دستور port security محدودیت ایجاد کنیم که در صورت اضافه شدن laptop به hub ، محدودیت ها اعمال شود.



قبل از اعمال محدودیت های غیر پیشفرض، با گرفتن show port-security تنظیمات اعمال شده به شرح ذیل است :

```
Switch#show port-security
Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security Action
                 (Count)       (Count)         (Count)
-------------------------------------------------------------------------
      | Fa0/1      ۲ 1         ۳ 0              ۴ 0        ۵ Shutdown
-------------------------------------------------------------------------
```

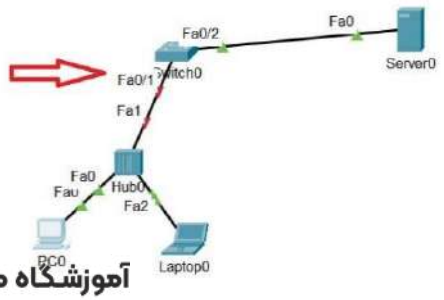
این جدول میگوید که (۱) روی f0/1 مکانیزم port-security فعال است.(۲) ماکزیمم تعداد سیستمی که به این اینترفیس می‌توانند متصل شود "یک" است.(پیشفرض یک بود) (۳) در این لحظه صفر سیستم learn شده است.(٤) تعداد رخداد امنیتی که رخ داده صفر است. (۵) محدودیت این port security در صورت برخورد با اتفاق امنیتی shutdown است.(پیش فرض shبود)

```
Switch#show port-security address
              Secure Mac Address Table
-------------------------------------------------------------------------
Vlan    Mac Address       Type                        Ports   Remaining Age
                                                                  (mins)
----    -----------       ----                        -----   -------------
-------------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 0
Max Addresses limit in System (excluding one mac per port) : 1024
```

چون بسته ارسال نشده است، همچنان جدول secure mac address table همچنان خالی است

```
Switch#show port-security address
              Secure Mac Address Table
-------------------------------------------------------------------------
Vlan    Mac Address       Type                        Ports   Remaining Age
                                                                  (mins)
----    -----------       ----                        -----   -------------
1       0060.5CD9.9061    DynamicConfigured FastEthernet0/1          -
-------------------------------------------------------------------------
```

بعد از ارسال و دریافت اولین بسته، جدول فوق به صورت روبرو خواهد شد:



در ادامه با اتصال یک device دیگر متوجه میشویم که interface0/1، shutdown و وضعیتش err-disable میشود.

```
%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to administratively down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down
```

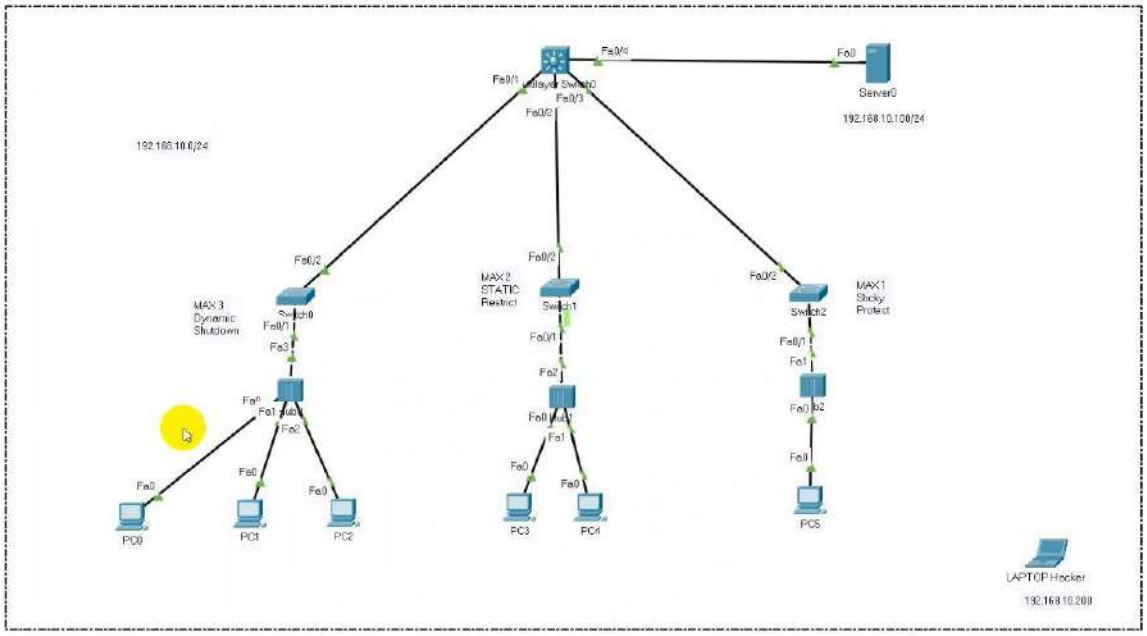
```
Switch#show interfaces status
Port      Name               Status       Vlan       Duplex  Speed Type
Fa0/1                        err-disabled 1          auto    auto  10/100BaseTX
```

```
Switch#show port-security
Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security Action
                (Count)       (Count)        (Count)
---------------------------------------------------------------------
        Fa0/1        1           0                1          Shutdown
```

نکته: برای پاک کردن جدول secure mac address table از دستور زیر استفاده میکنیم:

Switch#clear port-security address

مثال ۱:



**سوال کلی : به نظر شما راهی برای دور زدن port security وجود دارد ؟! بله . با روش اسکوف hacker می‌تواند macaddress جعلی یکی از pcها را برای خود تنظیم کند و سپس وارد شود.

**نکته: جهت مشاهده و بررسی تنظیمات Port Security از دستورات زیر استفاده می‌کنیم:

```
show mac address-table
show port- security
show port- security interface TYPE MOD/NUM
show mac address-table secure
show interface status err-disable
Clear port-security
```

نکته: در صورتی که بخواهیم MAC آدرس هایی که از طریق Sticky آنها را پیدا کرده ایم را حذف کنیم از دستورات زیر استفاده می‌کنیم:

Switch#clear port-security all

Switch#clear port-security sticky interface fastEthernet 0/1

Dynamic Host Configuration Protocol (DHCP) :

پروتکل DHCP یکی دیگر از پروتکل های مدل IP/TCP میباشد که در لایه application مورد استفاده قرار میگیرد.

هر دستگاه یا هر اینترفیس که از IP/TCP استفاده می کند ، برای استفاده از شبکه و ارتباطات خود نیاز به یکIP دارد، که این IP را میتوان به دو صورت زیر به دستگاه اختصاص داد:

1. Static :

در این حالت اختصاص IP به صورت دستی انجام می‌گیرد. یعنی روی هر دستگاه کاربر خودش یک IP مشخص کند. اختصاص IP به صورت Static مزایای و معایب خاص خودش را دارد که به برخی از آنها اشاره می‌کنیم:

-مزایا:

- هر دستگاه دقیقا مشخص است که از چه IP استفاده می‌کند.
- به لحاظ امنیتی استفاده از روش Static بهتر است چون در این روش کلاینت‌ها را بهتر می‌توان کنترل کرد.
- نیاز به راه‌اندازی و استفاده از سرویس خاصی ندارد.
- نگه داری و عیب‌یابی ساده‌تر انجام می‌شود.

-معایب:

- برای آینده‌نگری و عدم بروز مشکل باید برای سیستم آدرس‌دهی ، یک برنامه دقیق و مشخص داشته باشیم.
- در صورتی که تعداد دستگاه زیاد باشند نیاز به وارد کردن IP به صورت دستی روی تک تک دستگاه است که کار مشکلی است.
- احتمال استفاده شدن یک IP برای دو دستگاه وجود دارد که نتیجه آن IP Conflict و مختل شدن عملکرد دستگاه ها است.
- در صورت نیاز به تغییر در سیستم آدرس دهی این تغییرات باید روی تک تک دستگاه ها انجام شود.

نکته: معمولاً دستگاه هایی که در شبکه یک سرویس خاص را ارائه می دهند از Static IP استفاده می کنند، چون کلاینت‌ها از این سرویس استفاده می کنند درنتیجه نباید IP این دستگاه ها تغییر کند، روترها و سرور ها از این دسته می باشند.

2. Dynamic :

در این حالت اختصاص IP به صورت خودکار و توسط سرویسDHCP انجام می‌گیرد. این پروتکل وظیفه مدیریت سیستم آدرسی‌دهی شبکه را برعهده می‌گیرد. DHCP این اجازه را به دستگاه‌های شبکه می‌دهد که درخواست برای دریافت IP داشته باشند. DHCP را می‌توان روی تجهیزات مختلف مانند روتر ، سوئیچ ، ویندوز سرور ، مودم و... راه‌اندازی کرد و به آن DHCP Server گفته می‌شود و کلاینتی که درخواست IP می کند را DHCP client می‌نامند.

نکته: اکثر مدیران شبکه حتی فکر این را نمی کنند که از تجهیزات سیسکو مانند روتر و سویچ سیسکو می توانند به عنوان DHCP سرور استفاده کنند. البته فراموش نکنید که این قابلیت با نسخه های جدید از IOS های سیسکو ارائه شده است و با سری محصولات Catalyst 3550 و 3750 ارائه شده است .

معایب و مزایای استفاده از DHCP :

-مزایا:

- ✓ آدرس دهی به صورت خودکار و سریع انجام می شود.
- ✓ برای مکان‌هایی که کاربران آن افراد ثابتی نیستند بسیار مناسب است.
- ✓ مدیریت سیستم آدرسی دهی و رنج IP آدرس مورد استفاده توسط سرویس DHCP به صورت خودکار انجام می شود.
- ✓ احتمال Conflict IP و مختل شدن عملکرد دستگاه ها بسیار کم است.
- ✓ در صورت نیاز به تغییر در سیستم آدرس دهی این تغییرات به سادگی انجام می شود.

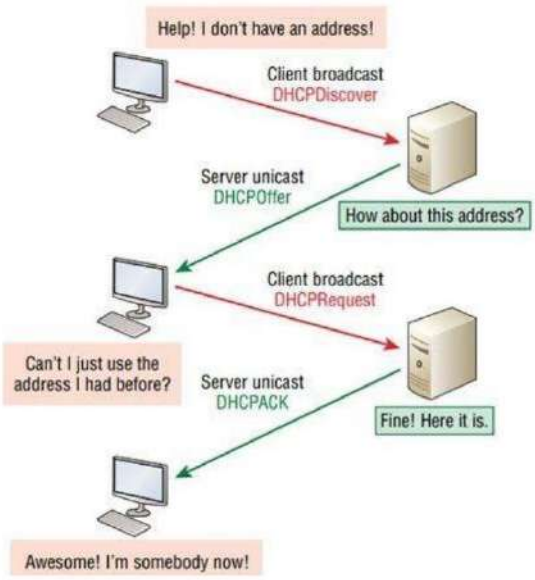
- معایب:

- ✓ نیاز به نگه داری دارد.
- ✓ دستگاه ها ، IP مشخصی ندارند در نتیجه کنترل آنها مشکل است.
- ✓ امکان حمله DHCP Spoofing برای این سرویس وجود دارد.
- ✓ برای راه اندازی نیاز به یک DHCP Server داریم. در صورتیکه تجهیزات موجود در شبکه این را قابلیت نداشته باشند باید یک دستگاه به این منظور تهیه شود.
- ✓ برای همه تجهیزات مثل سرورها نمی‌توان از DHCP استفاده کرد.

نحوه عملکردDHCP :

برای DHCP Server یک رنج IP مشخص می‌شود(استخر Pool ID = ID) که از این رنج IP برای اختصاص به کلاینت‌ها استفاده می‌کند. DHCP Server علاوه بر مشخص کردن IP برای کلاینت، می‌تواند Gateway IP ، DNSو ... را به کلاینت اعلام کند.

برای دریافت IP بین DHCP Client و DHCP Server چهار بسته رد و بدل می‌شود:



زمانی که یک کلاینت به شبکه متصل می‌شود، از رنج IP شبکه و DHCP Server بی خبر است، یک بسته به عنوان DHCP Discover به آدرس MAC کلاینت و مقصد ffff.ffff.ffff و IP مبدا ۰،۰،۰،۰ و IP مقصد ۲۵۵،۲۵۵،۲۵۵،۲۵۵ به صورت Broadcastروی شبکه ارسال می‌کند. DHCP Server با دریافت این بسته به عنوان پاسخ یک بسته به عنوان offer ارسال می کند که حاوی اطلاعاتی مانندIP ، Default Gateway و ... می باشد. DHCP Client با دریافت بسته offer و بررسی اطلاعات آن، به عنوان تایید یک بسته Request ارسال می‌کندDHCP Server . با دریافت بسته Request به عنوان تایید این مراحل و اختصاصIP ، یک بسته Ack ارسال می‌کند و به این ترتیب مراحل اختصاص IP پایان می‌پذیرد.

SRC Port DHCP =67 & 68

[DHCP-Discovery][UDP=>DST=67 SRC=68][PT=17 SRC-IP=0.0.0.0 DST-IP=255.255.255.255] [SRC-MAC=Client DST-MAC=FFFF.FFFF.FFFF

نکته: اگر DHCP SERVER از دسترس خارج شود، ویندوز برای ارتباط موقت از رنج رزور APIPA برای دادن IP به خود استفاده میکند. APIPA یک روش IP موقت است که روش جالبی نیست چون ممکن است duplicate IP اختصاص بدهند.

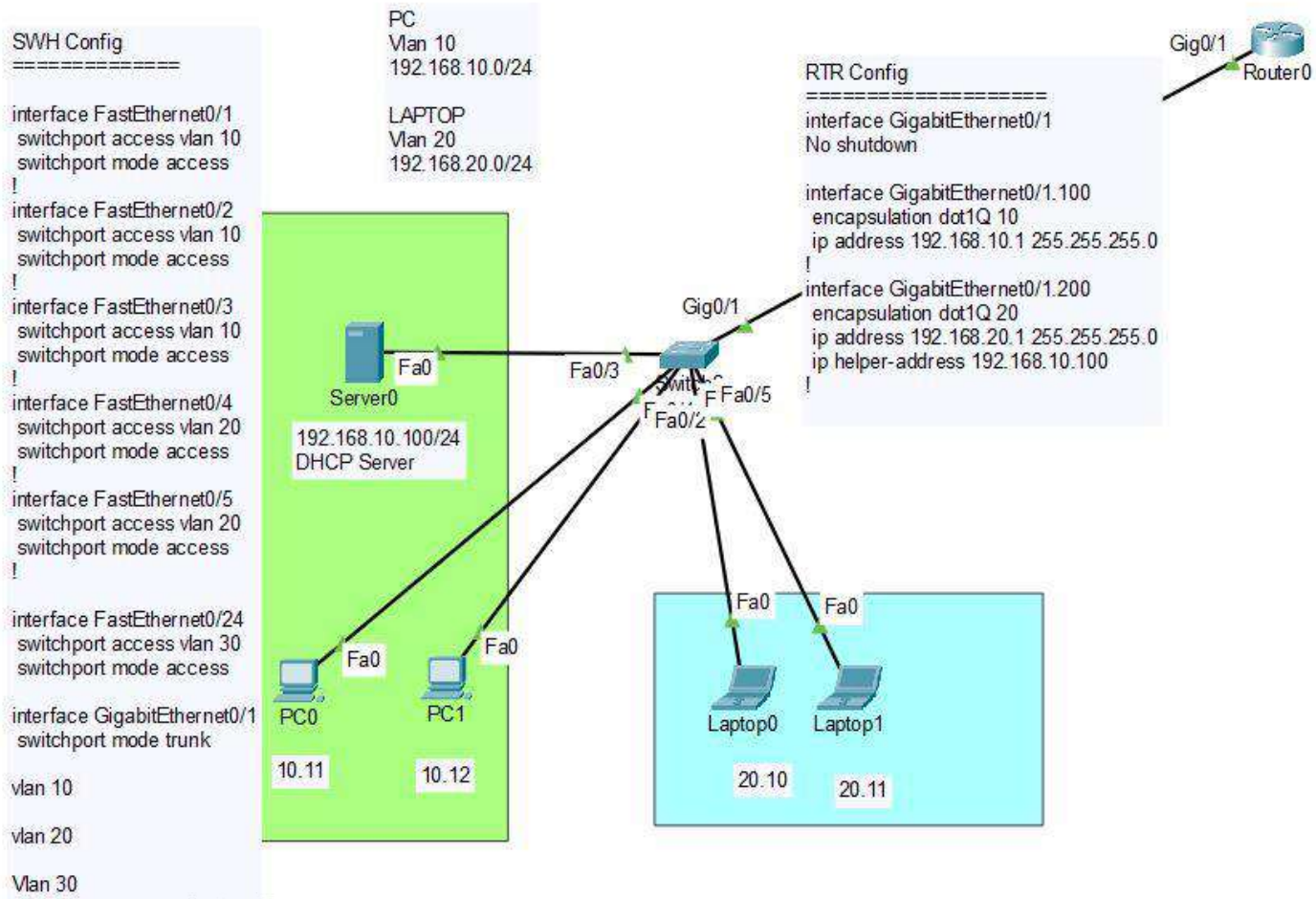
Range APIPA: 169.254.0.0 => 169.255.255.255

فعال کردن DHCP در تجهیزات سیسکو:

DHCP Relay Agent:

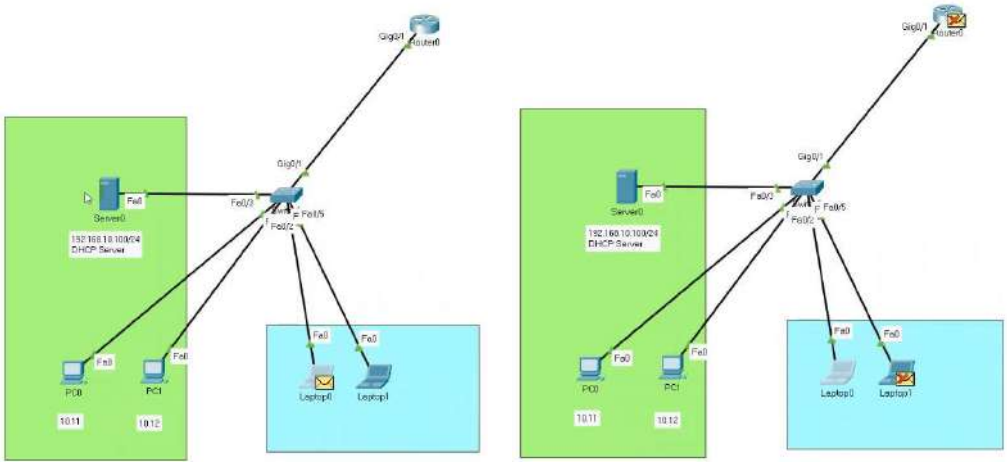
همانطور که می‌دانیم، بسته DHCP به صورت Broadcast ارسال می شوند حالا شبکه ای را در نظر بگیرد که DHCP Server آن در شبکه‌ای localنیست و در یک شبکه دیگر قرار دارد، که باعث می شود درخواست های کلاینت‌ها به دست DHCP Server نرسد(در بین شبکه ها روتر قرار دارد و یکی از وظایف روتر جلوگیری از ارسال بسته های Broadcast از یک شبکه به شبکه دیگر است). DHCP Relay Agent این مشکل را برای ما حل می کند. دستگاهی که به عنوان DHCP Relay Agent عمل می کند بسته های درخواستی کلاینت که به صورت Broadcast است را به سمت DHCP Server به صورت unicast ارسال می کند. در واقع DHCP Relay Agent به عنوان یک واسطه بین کلاینت و سرور کار می‌کند.

مثال۱: تعیین DHCP وقتی server خارج از شبکه (vlan) باشد:



در اینجا ما یک توپولوژی را مشاهده می نماییم که دو vlan به عنوان DHCP Client وجود دارند که هیچ آدرس IP روی آن‌ها تنظیم نشده. همچنین یک DHCP Server را با آدرس ۱۹۲,۱۶۸,۱,۱۰۰ داریم که در vlan20 قرار دارد. و یک روتر ROAS داریم که قصد داریم این روتر نقش DHCP Relay Agent را ایفا کند.

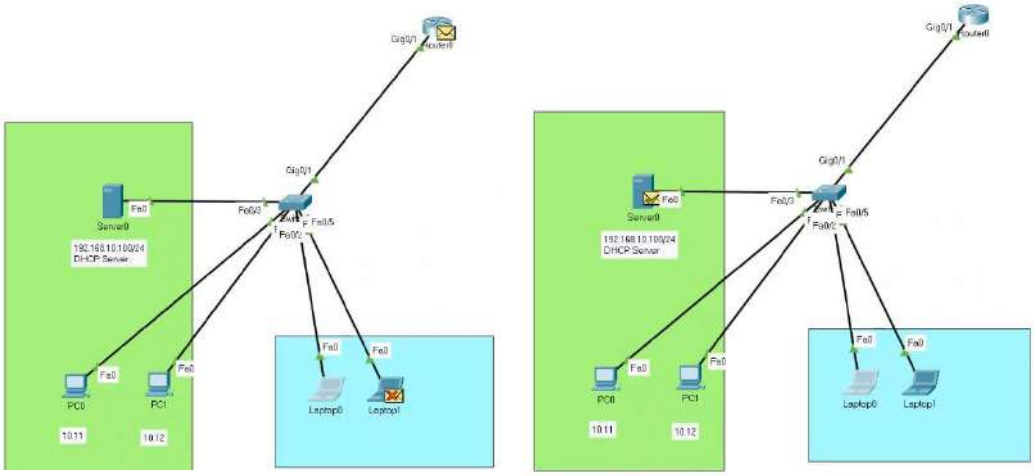
بعد از vlanبندی و تعیین mode اینترفیس‌های سوئیچ، قصد داریم به Laptop0 از طریق DHCP SERVER آیپی بدهیم. پیام Discoverتوسط DHCP Client (laptop0)به صورت Broadcast انتشار می یابد تا مشخص شود که آیاDHCP Server به سوئیچ ما متصل شده یا خیر. سوییچ به محض اینکه پیام را از کلاینت دریافت می‌نماید آن را در شبکه Broadcastمی کند. که این پیام همه پخش شده در این توپولوژی به اینترفیس‌های عضو vlan20 (laptop1)و همچنین به روتر ارسال می‌گردد(سوئیچ بسته DHCP را به vlan10 ارسال نمیکند). در ادامه اعضای Vlan20 و روترآن را Drop میکنند. (یکی از وظایف روتر جلوگیری از ارسال بسته های Broadcast از یک شبکه به شبکه دیگر است)



حال میخواهیم broadcast کلاینت‌ها به دستserver برسد، چون ما که نمیتوانیم به ازای هر vlan یک DHCP Server بگذاریم. برای اینکار ابتدا DHCP(Pool IP) را روی Server قرارمیدهیم. بعد باید به روتر تعریف شود که اگر بسته Broadcastی DHCP به subinterfaceت رسید، آن را بهIP ی برسان که نقشDHCP Server دارد. به این کار DHCP Relay Agent میگویند.

در این حالت روتر دیگر بسته را Drop نمیکند و بسته را به سمت server که در Vlan10قرار دارد به صورت unicast میرساند.

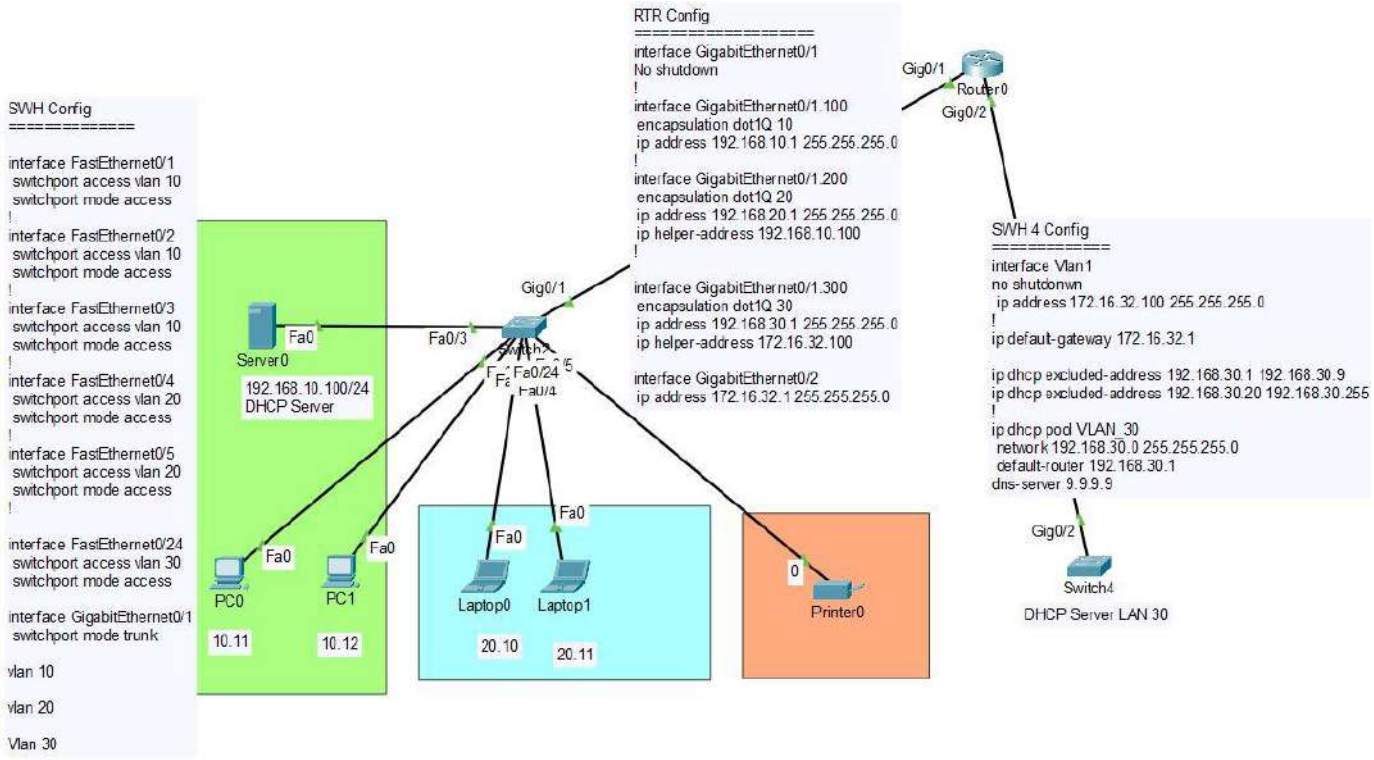
*نکته: در ابتدا بسته به صورت broadcast ارسال میشود، ولی در برگشت چون مبدا و مقصد کامل مشخص شده است، این بسته به صورت unicast ارسال خواهد شد. یعنی در برگشت بسته از server به سوئیچ و سپس از سوئیچ به روتر میرسد. روتر بر اساس dst بسته را به سمت مقصد میرساند.



توجه: مراحل Dora باید کامل طی شود تا DHCP به کلاینت مورد نظر IP تخصیص دهد.

مثال۲: DHCP Server شدن سوئیچ سیسکو خارج از شبکه:

در این مثال می‌خواهیم برای پرینتر از سوئیچ ٤ به صورت DHCP آیپی بگیریم



از تجهیزات سیسکو مانند روتر و سوئیچ می توان به عنوان Server DHCP استفاده کرد. برای اینکار از دستورات زیر استفاده می کنیم:

برای ارتباطات لایه ۳ سوئیچ، باید روی اینترفیس vlan1 آیپی set کنیم(no shut فراموش نشود).

در ادامه یک Pool ایجاد می کنیم(ایجاد و نامگذاری):

```
Switch(config)# ip dhcp pool VLAN_30
```

حالا باید رنج شبکه ای که می خواهیم از آن به کلاینت IP اختصاص دهیم را مشخص کنیم:

```
Switch(dhcp-config)# network 192.168.30.0 255.255.255.0
```

تنظیم جهت default-router بادستور Default Gateway :

```
Switch(dhcp-config)# default-router 192.168.30.1
```

تنظیم جهت domain-name بادستور dns-server :

```
Switch (dhcp-config)# domain-name 9.9.9.9
```

مدت زمان نگه داری IP را براساس روز مشخص می کنیم:

```
Switch (dhcp-config)# lease 9
```

اگر بخواهیم بخشی از رنج IP را برای موارد خاص مثل سرورها رزرو کنیم از دستور زیر استفاده می‌کنیم:

Switch (config)# ip dhcp excluded-address 192.168.30.1 192.168.30.9

Switch (config)# ip dhcp excluded-address 192.168.30. 20 192.168.30.255

دستورات مشاهده تنظیمات:

Switch#Show ip dhcp pool

```
Switch#show ip dhcp pool

Pool VLAN_30 :
 Utilization mark (high/low)    : 100 / 0
 Subnet size (first/next)       : 0 / 0
 Total addresses                : 254
 Leased addresses               : 1
 Excluded addresses             : 2
 Pending event                  : none

 1 subnet is currently in the pool
 Current index        IP address range                  Leased/Excluded/Total
 192.168.30.1         192.168.30.1      - 192.168.30.254    1    / 2      / 254
```

Tatal addresses:تعداد آیپی قابل تخصیص

Leased addresses:تعداد آیپی تخصیص داده شده

Excluded addresses:تعداد رنج آیپی خارج شده

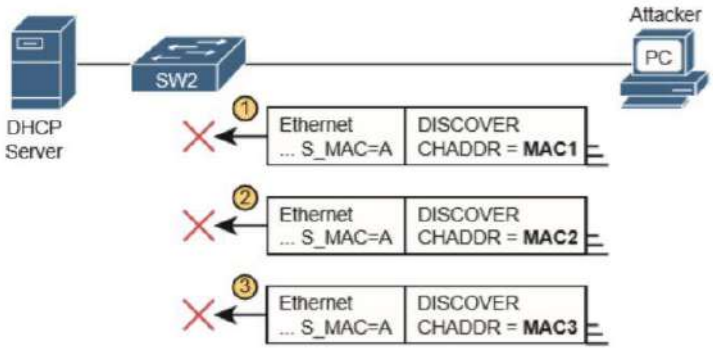
DHCP Snooping :

Snooping = جاسوسی

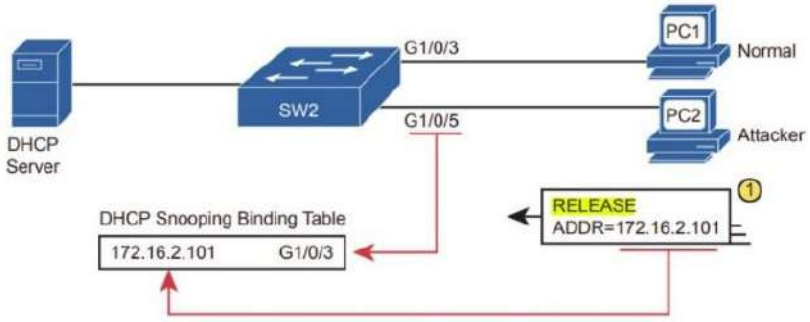
Spoofing =جعل

– متداول‌ترین حملات مربوط به DHCP عبارتند از:

DHCP Starvation: این حالت جهت از کار انداختن سرویس DHCP مورد استفاده قرار می گیرد. به این صورت که مهاجم تعداد زیادی DHCP Request جعلی ایجاد می کند و باعث می شود که کل محدود IP تعیین شده برای DHCP سرور پر شود یا تعداد این DHCP Request انقدر زیاد می شود که سرور توان پاسخگویی به آن را نداشته باشد. این حمله معمولاً مقدمه‌ی حمله‌ی DHCP spoofing است. به خارج کردن سرویس از دسترس Denial-of-Service [DOS] گفته می‌شود.



DHCP Server Spoofing: در این حمله، که بعد از حمله DHCP starvation انجام می‌شود، مهاجم یک سرور DHCP جعلی با پیکربندی متفاوت از سرور اصلی راه‌اندازی می‌کند. این پیکربندی متفاوت شامل گیت‌وی و DNS متفاوت است. به عنوان مثال گیت‌وی جدید می‌تواند سیستم خود مهاجم باشد. در این حالت ترافیک کاربران سمت سیستم مهاجم ارسال می‌شود و او می‌تواند حمله man-in-the-middle را انجام دهد. به عنوان مثال در این حمله مهاجم می‌تواند کاربران را سمت یک وب سایت جعلی هدایت کرده و حمله فیشینگ را نیز انجام دهد.



نکته : در صورتی که DHCP سرور روی سوئیچ فعال باشد این حمله صورت نخواهد گرفت.

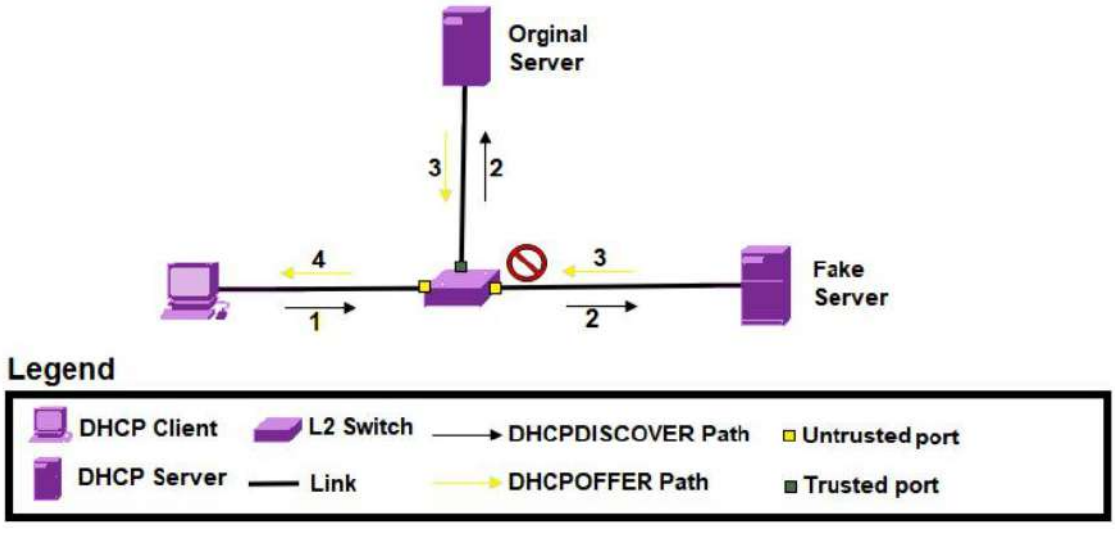
یک فرد مهاجم با DHCP سرور های تقلبی مشکلاتی را می تواند برای شبکه به وجود آورد که عبارتند از:

- تغییر دادنIP
- تغییر Default gateway
- از بین بردن DHCP Server اصلی
- تغییر در DNS

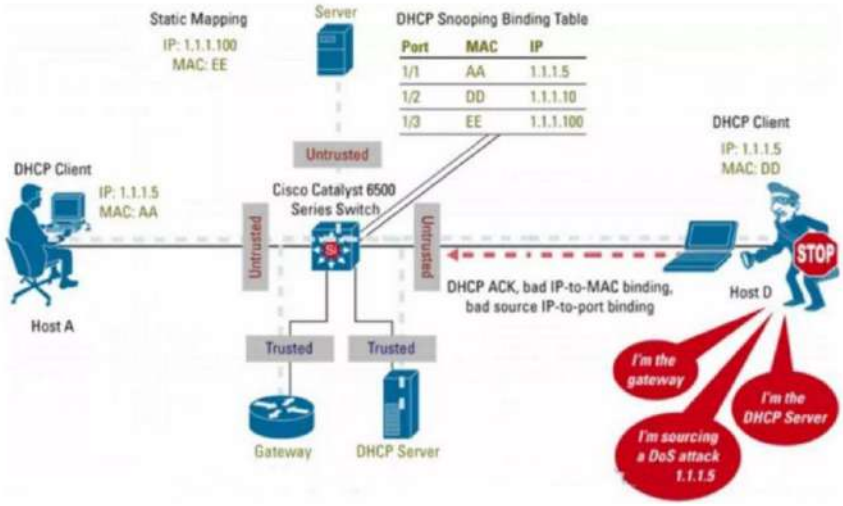
برای جلوگیری از این حملات از DHCP Snooping استفاده می کنیم و به صورت زیر عمل می کند :

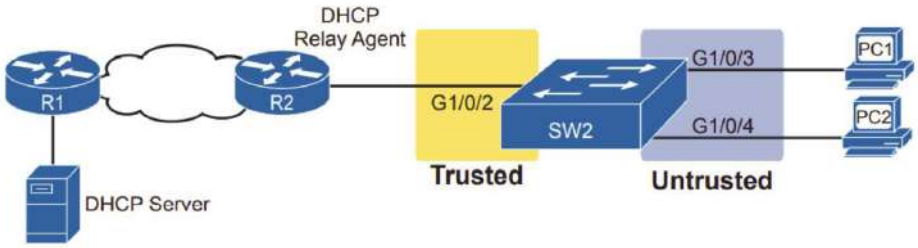
-برای جلوگیری از DHCP Starvation برای پورت ها مشخص می کنیم که در هر ثانیه اجازه دارند به چه تعداد DHCP Request دریافت کند(Limit Rate) و یا استفاده از قابلیت Port Security (با استفاده از این روش، Mac Address های مشخصی در یک پورت خاص در شبکه اجازه دسترسی دارند. در این صورت دیگر فرد مهاجم قادر به ارسال بسته های حاوی در خواست IP با چند Mac Address را نخواهد بود.).

-برای جلوگیری از DHCP Server Spoofing ، پورت مربوط به سرور DHCP شناسایی و در حالت Trusted قرار می‌گیرد و بقیه پورت‌ها در حالت Untrusted قرار می‌گیرند. سوئیچ در صورتی که بسته‌های مربوط به سرور DHCP را از پورت Untrust دریافت کند آن را drop می‌کند.



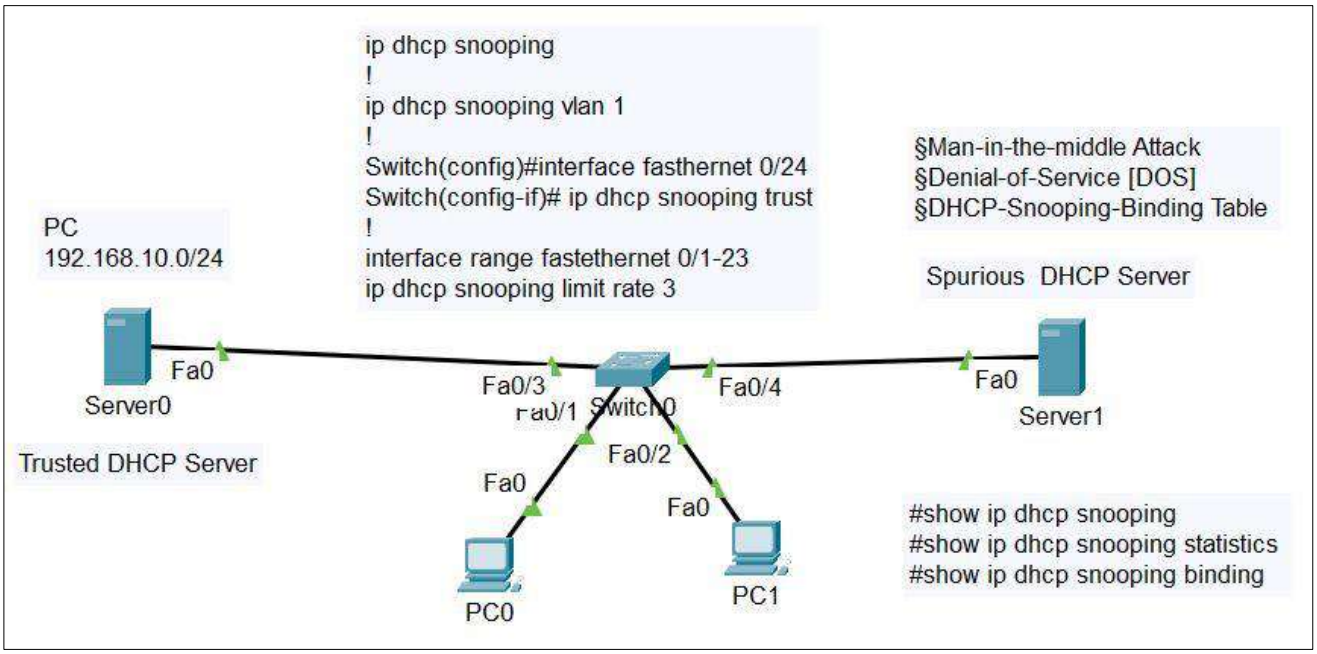
در این روش سوئیچ با چک کردن بسته‌های سرور DHCP جدولی به نام Binding Table می‌سازد که حاوی Mac Address، آدرس IP، شماره ویلن و شماره پورت است. در صورتی که سوئیچ بسته‌هایی از آی‌پی و MAC اشتباه دریافت کند، آن‌ها را drop می‌کند.





نحوه اعمال دستورات DHCP Snooping:

مثال:



در ابتدا DHCP Snooping را فعال می کنیم.

```
Switch(config)#ip dhcp snooping
```

سپس VLAN مربوطه را مشخص می کنیم.

```
Switch(config)#ip dhcp snooping vlan 1
```

وارد اینترفیس متصل به DHCP سرور می شویم و آنرا به عنوان trust معرفی می کنیم.

```
Switch(config)#interface fasthernet 0/24
Switch(config-if)# ip dhcp snooping trust
```

حالا باید مشخص کنیم که باقی پورت ها در هر ثانیه اجازه ارسال چند DHCP Request را دارند.

```
Switch(config)#interface range fastethernet 0/1-23
Switch(config-if)#ip dhcp snooping limit rate 3
```

جدول DHCP Snooping :

```
Switch#show ip dhcp binding
```

```
Switch#SHow IP DHcp Snooping Binding
MacAddress          IpAddress        Lease(sec)  Type           VLAN  Interface
------------------  ---------------  ----------  -------------  ----  ------------------
00:60:70:7D:E1:9E   192.168.10.11    86400       dhcp-snooping  1     FastEthernet0/1
00:60:70:03:96:1A   192.168.10.10    86400       dhcp-snooping  1     FastEthernet0/2
Total number of bindings: 2
```

GARP (Gratuitous Address Resolution Protocol) :

پروتکل ARP یا Address Resolution Protocol یک پروتکل لایه دو است، که کار آن به دست آوردن آدرس لایه دو یا همان آدرس فیزیکی مقصد، معروف به MAC، از روی آدرس لایه سه-ای یعنی IP است.

فرض کنید کامپیوتر A که IP آن 192.168.1.100/24 است، قصد دارد بسته‌ای به کامپیوتر B که IP آن 192.168.1.200/24 است ارسال کند. آدرس فیزیکی یا همان MAC Address کامپیوتر A برابر باAA.AA.AA.AA.AA.AA است. هنگام تشکیل بسته در لایه دو نیاز به Destination-MAC یا همان آدرس MAC مقصد دارد. در ابتدا کامپیوتر A به جدول ARP خود که معروف به ARP Cache یا ARP Table است نگاه می‌کند. در این جدول آدرس‌های IP با آدرس‌های MAC متناظر یا Bind شده‌اند. یعنی MAC آدرسی برای این IP آدرس موجود است. کامپیوترها به کمک این جدول می‌توانند بسته‌های خود را کامل کرده و ارسال کنند.

حال اگر کامپیوتر A هیچ اطلاعی از آدرس MAC کامپیوتر B نداشته باشد، یعنی در جدول خود آدرس MACکامپیوتر B را نداشته باشد باید چه کند؟ جواب ساده است. باید ARP ارسال کند و خواستار آدرس MACکامپیوتر B شود.

GARP چیست؟

وقتی شما آدرس IP خود را عوض می‌کنید، ARP Table تمام کامپیوترهای دیگر باید آپدیت شوند. در این هنگام کامپیوتری که آدرس IP خود را عوض کرده GARP ارسال می‌کند. در این حالت کامپیوتر آدرس IP خود را ARP می‌زند تا جدول بقیه را آپدیت کند. این اتفاق زمانی که کارت شبکه فعال شده و یا آدرس IP از DHCP Server دریافت می‌کند نیز می‌افتد تا از Duplicate IP جلوگیری کند.

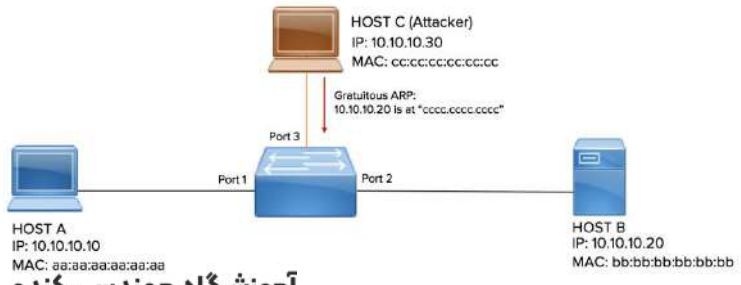
در واقع GARP یک ARP Request است که به صورت broadcast در شبکه منتشر میشود. وقتی کامپیوتر به صورت static یا dynamic دارای یک آدرس IP جدید میشود؛ آن را از طریق پیام GARP به تمام کامپیوترهای حاضر در broadcastdomain و vlan خود خبر میدهد. در پیام GARP، کامپیوتر به دنبال فهمیدن MAC هیچ کامپیوتری نیست؛ بلکه هدف از ارسال پیام GARP این است که جدول ARP کامپیوترهای شبکه بروزرسانی شود.

اگر GARP ارسال نشود چه می‌شود؟

فرض کنید آدرس آی پی ۱۹۲,۱۶۸,۱,۱۰ متعلق به PC ۱ است. ادمین شبکه این آدرس IP را از تنظیمات کارت شبکه PC ۱حذف میکند و همین آدرس را به کامپیوتر PC ۲ اختصاص میدهد. دیگر کامپیوترهای حاضر در شبکهLAN ، از قبل در جدول ARP خود آدرس ۱۹۲,۱۶۸,۱,۱۰ را مرتبط با آدرس مک کامپیوتر PC۱ثبت کرده اند. حالا اگر PC ۲ آدرس IP جدیدش را همراه با آدرس مک خود برای سایر کامپیوترها broadcast نکند، سوییچ اترنت ترافیک ارسالی به مقصد ۱۹۲,۱۶۸,۱,۱۰ را بر اساس مک آدرس PC۱ مسیردهی می‌کند. بنابراین ترافیک برای PC۲ ارسال نمی‌شود.

معرفی حمله ARP Spoofing و ARP Poisoning (سمی کردن) و روش مقابله با آن:

پروتکل ARP عمل تبدیل IP به MAC را برای ما انجام می‌دهد و مهاجم از این پروتکل برای حمله خود سود می‌برد. در این روش مهاجم با استفاده از پروتکل ARP یک بسته GARP ارسال می‌کند. به طور مثالIP Address گیت وی شبکه را با MAC آدرس خود را اعلام می کند و سیستم های موجود در شبکه اطلاعات مربوط به ARP خود را با اطلاعات جدید بروز می کند و از این پس ترافیک خارج از شبکه خود را تحویل مهاجم می دهند و اگر مهاجم بعد از بدست آوردن اطلاعات مورد نیاز خود ترافیک به گیت وی اصلی ارسال کند، کاربران از این اتفاق بی خبر خواهند بود (man in the middle). با این روش مهاجم سعی نمی کند که دسترسی بقیه سیستم ها را به اینترنت و منابع دیگر مسدود کند، بلکه فقط جهت حرکت داده ها را تغییر می‌دهد.



در شکل روبرو میزبان‌هایA ، Bو C به پورت‌های ۱، ۲ و ۳ سوئیچ متصل گردیده‌اند. هنگامی که دستگاه A نیاز به برقراری ارتباط با دستگاه B دارد، یک درخواست ARP برای تعیین آدرس MACمرتبط با آدرس IP دستگاه(10.10.10.20) B ، به

صورت همه پخشی ارسال می نماید. هنگامی که میزبان B پاسخ می دهد، سوئیچ و میزبان A کَش‌های ARP خود را با آدرس IP 10.10.10.20 و آدرس MAC bb:bb:bb:bb:bb:bb تکمیل می‌نمایند. میزبان C می تواند کش ARP سوئیچ و میزبان A را در مورد میزبان B با پخش پاسخ های ARPجعلی مسموم نماید. بسته های جعلی ARP از میزبان C ادعا می کنند که آدرس IP 10.10.10.20 مربوط به آدرس MAC cc:cc:cc:cc:cc:ccمی باشد.

اکنون سوئیچ و میزبان A از آدرس cc:cc:cc:cc:cc:cc به عنوان آدرس MAC مقصد جهت ارسال ترافیک به میزبان B استفاده می نمایند. سوئیچ اکنون تمام ترافیک مربوط به آدرس IP 10.10.10.20 را به پورت ۳ که متصل به دستگاه مهاجم است هدایت می نماید. میزبان C اکنون با موفقیت خود را در جریان ترافیک از میزبان A به میزبان B قرار داده است، که یک شکل کلاسیک از حمله Man-in-the-Middle می باشد.

ARP inspection:

Dynamic:

برای جلوگیری از این حملات از DAI(Dynamic ARP inspection) استفاده می شود. DAI می تواند با DHCP Snooping کار کند تا جلوی این حمله را بگیرد. درDAI پورت های trusted و untrusted مشخص می شود و IP Address و MAC بسته های دریافتی ARP را با استفاده از دیتابیس DHCP Snooping بررسی می کند. پورت‌های Access باید به عنوان untrusted و پورت های متصل به روتر و دستگاه های که نمی‌خواهد بسته های ARP آنها چک شوند را در حالت trusted قرار می دهیم. *** باید در نظر داشت که DAI بر پایه مکانیزم DHCP Snooping می باشد. ***

Static:

با استفاده از Access Control List (ACL)

نکته: پروتکل ARP Inspection را روی سوئیچ‌هایی استفاده میکنند که به End userها متصل شده‌اند.

زمانی که ARP inspection را فعال می کنیم چه اتفاقی می افتد؟

مجدد همه پورت‌های سوییچ untrusted می‌شود و زمانی که روی هر پورت یک بسته ARP ارسال شود سوییچ هدر بسته را باز می کند و طبق جدول dhcp binding بررسی میکند که Mac بسته و Mac که در جدول قرار دارد یکی باشد، در غیر این صورت بسته را دور میریزد.

از دستورات زیر برای فعال کردن این قابلیت استفاده می شود:

```
Switch(config)# ip arp inspection vlan z
```

با استفاده از دستور زیر پورت را در حالت trusted قرار داده می شود.

```
Switch (config)#interface fastethernet 0/1
Switch(config-if)# ip arp inspection trust
```

Forward,Drop,DHCP Drop,ACL Drop های بسته تعداد مشاهده

Switch#show ip arp inspection statistics

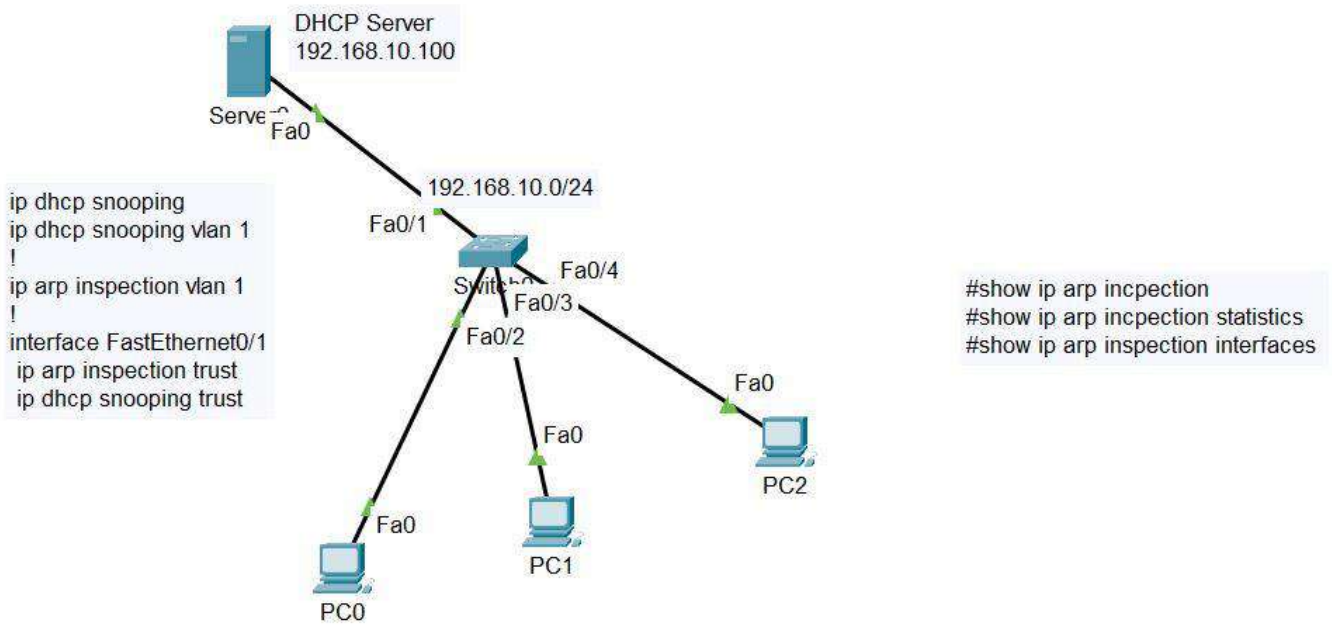
Switch#show ip arp inspection interface fast 0/1

نکته: بصورت پیشفرض روی هر اینترفیس که inspection فعال می کنیم اینتروالی که دارد در لحظه ۱۵ بسته می تواند ارسال کند اگر بیشتر ارسال کند drop می شود.

برای تغییر محدودیت از دستور زیر استفاده می شود که در tracer packet غیر فعال است :

ip arp inspection limit rate <count>

مثال:




```
Switch#show ip arp inspection interfaces
Interface          Trust State       Rate (pps)     Burst Interval
---------------    -----------       ----------     --------------
Fa0/1              Trusted                   15                  1
Fa0/2              Untrusted                 15                  1
Fa0/3              Untrusted                 15                  1
Fa0/4              Untrusted                 15                  1
Fa0/5              Untrusted                 15                  1
```

```
Switch#show ip arp inspection statistics

 Vlan      Forwarded        Dropped      DHCP Drops      ACL Drops
 ----      ---------        -------      ----------      ---------
    1              0              0               0              0

 Vlan   DHCP Permits    ACL Permits   Source MAC Failures
 ----   ------------    -----------   -------------------
    1              0              0                     0

 Vlan   Dest MAC Failures   IP Validation Failures
 ----   -----------------   ----------------------
    1                   0                       0
```

```
Switch#show ip arp inspection

Source Mac Validation      : Disabled
Destination Mac Validation : Disabled
IP Address Validation      : Disabled

 Vlan     Configuration    Operation   ACL Match          Static ACL
 ----     -------------    ---------   ---------          ----------
    1     Enabled          Active

 Vlan     ACL Logging      DHCP Logging      Probe Logging
 ----     -----------      ------------      -------------
    1     Deny             Deny              Off

 Vlan      Forwarded        Dropped      DHCP Drops      ACL Drops
 ----      ---------        -------      ----------      ---------
    1              0              0               0              0

 Vlan   DHCP Permits    ACL Permits   Probe Permits   Source MAC Failures
 ----   ------------    -----------   -------------   -------------------
    1              0              0               0                     0

 Vlan   Dest MAC Failures   IP Validation Failures   Invalid Protocol Data
 ----   -----------------   ----------------------   ---------------------
    1                   0                       0                       0
```

```
Switch#show ip arp inspection vlan 1

Source Mac Validation      : Disabled
Destination Mac Validation : Disabled
IP Address Validation      : Disabled

 Vlan     Configuration    Operation   ACL Match          Static ACL
 ----     -------------    ---------   ---------          ----------
    1     Enabled          Active

 Vlan     ACL Logging      DHCP Logging      Probe Logging
 ----     -----------      ------------      -------------
    1     Deny             Deny              Off
```

Error Disabled & Error Recovery :

There are various reasons for the interface to go into errdisable. The reason can be:

- Duplex mismatch
- Port channel misconfiguration
- BPDU guard violation
- UniDirectional Link Detection (UDLD) condition
- Late-collision detection
- Link-flap detection
- Security violation
- Port Aggregation Protocol (PAgP) flap
- Layer 2 Tunneling Protocol (L2TP) guard
- DHCP snooping rate-limit
- Incorrect GBIC / Small Form-Factor Pluggable (SFP) module or cable
- Address Resolution Protocol (ARP) inspection
- Inline power

```
(config)# errdisable detect cause <>

#show interfaces TYPE <> status
#show interface status err-disabled
```

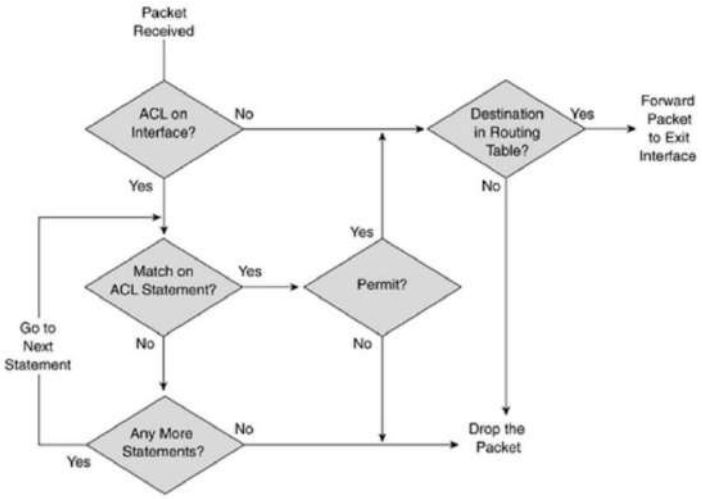
```
(config)#errdisable recovery cause <>
(config)#errdisable recovery interval <sec>

#show errdisable recovery
```

Err-disable برخلاف Error-Recovery پیشفرض فعال است.

Access Control List :

Access Control list یا ACL یک فیلتر است که به وسیله آن می توانیم جریان ترافیک را کنترل کنیم که چه بسته‌هایی اجازه ورود یا خروج از شبکه را دارند یا خیر. این فیلتر معمولاً توسط مدیر شبکه تعیین و مورد استفاده قرار می‌گیرند تا به این وسیله بتواند کنترل و امنیت بیشتر را برای شبکه خود فراهم کند. این فیلترها را می‌توان روی بسیاری از دستگاه‌های شبکه مانند روتر و سوئیچ مورد استفاده قرار داد.

نحوه عملکردACL :

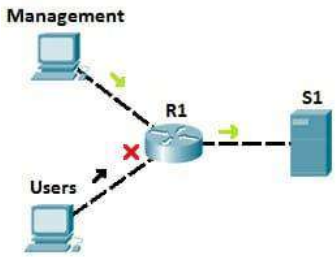


برای اینکه نحوه عملکردACLها را بهتر درک کنیم یک نگهبان که جلوی یک در بسته مستقر است را تصور کنید. نگهبان براساس دستورالعملی که به او داده شده اجازه عبور به افراد را می‌دهد. به طور مثال به او یک لیست داده شده که فقط این افراد اجازه ورود دارند. افراد که می خواهند از این در عبور کنند نام آنها توسط نگهبان با لیست خود مطابقت داده می‌شود و در صورتی که نام آنها در لیست بود به آنها اجازه عبور از در را می‌دهد در غیر اینصورت فرد اجازه عبور از در را نخواهد داشت .

ACLها با استفاده از آیتم های مختلف مانند آدرس مبدا و مقصد ، پورت مبدا و مقصد ، نوع پروتکل و ... می‌تواند عمل فیلترینگ را روی بسته‌های ورودی یا خروجی یک پورت برای ما انجام دهد. زمانی که یک بسته به دستگاه می‌رسد، در صورت وجودACL ، اطلاعات موجود در Headerبسته را بررسی می‌کند و با آیتم‌های تعریف شده درACL مقایسه می‌کنند و نسبت به آن اجازه یا عدم عبور به بسته را می‌دهد.

در اینجا برای اینکه شما با مفهوم ACL بیشتر آشنا شوید،با یک مثال آن را توضیح می دهیم.به شکل زیر توجه کنید:

بیائید اینگونه در نظر بگیریم که سرورS1 ، یک سرور حاوی اسناد و اطلاعات مهم می باشد که فقط دسترسی به این اطلاعات برای مدیران شرکت مجاز است. ما می توانیم با استفاده از دستورات اکسس لیست به شکلی روتر R1 را پیکربندی کنیم که فقط ترافیک هایی که از سمت شبکهManagement به سمت سرور ارسال می شوند اجازه عبور داشته باشند و در غیر اینصورت مابقی ترافیک ها بلاک شوند .این مسئله باعث می شود که ما مطمئین شویم تنها کاربرانی که احراز هویت شده اند می توانند به S1 دسترسی داشته باشند.



چه زمانی از **ACL** استفاده می کنیم؟

- ✓ جهت مقاصد امنیتی
- ✓ محدود کردن ترافیک برای افزایش کارایی شبکه
- ✓ جهت کنترل بسته های مربوط به پروتکل های مسیریابی
- ✓ چه نوع ترافیکی اجازه عبور یا عدم عبور دارند
- ✓ جداسازی برخی ترافیک های خاص به منظور عملیات خاص مانند QoS
- ✓ اعمال محدودیت های زمانی
- ✓ و...

شرایط ACL (Condition) :

وقتی ورودی ACL را تعریف می کنید ، به اطلاعات لازم نیاز خواهید داشت:

- Sequence Number: مشخص سازی با استفاده از شماره
- ACL Name: ACL را با استفاده از یک نام تعریف کنید. به جای استفاده از توالی اعداد ، برخی از روترها ترکیبی از حروف و اعداد را امکان پذیر می کنند.
- Remark: برخی از روترها به شما امکان می دهند تا توضیحات را در ACL اضافه کنید، که می تواند به شما در شناسایی و نحوه کارکرد دقیق کمک کند.
- Statement: مشخص سازی Deny و یا permit بودن.
- Network Protocol: مشخص سازی نحوه برخورد بر اساس پروتکل.
- Source or Destination: مشخص سازی مبدا و مقصد.
- Log: برخی از تجهیزات میتوانند گزارش نیز تولید کنند.
- سایر معیارها: ACLهای پیشرفته به شما امکان می دهند تا از اولویت نوع خدمات (ToS) ، اولویت IP ، و کدگذاری خدمات متفاوت (DSCP) استفاده کنید.

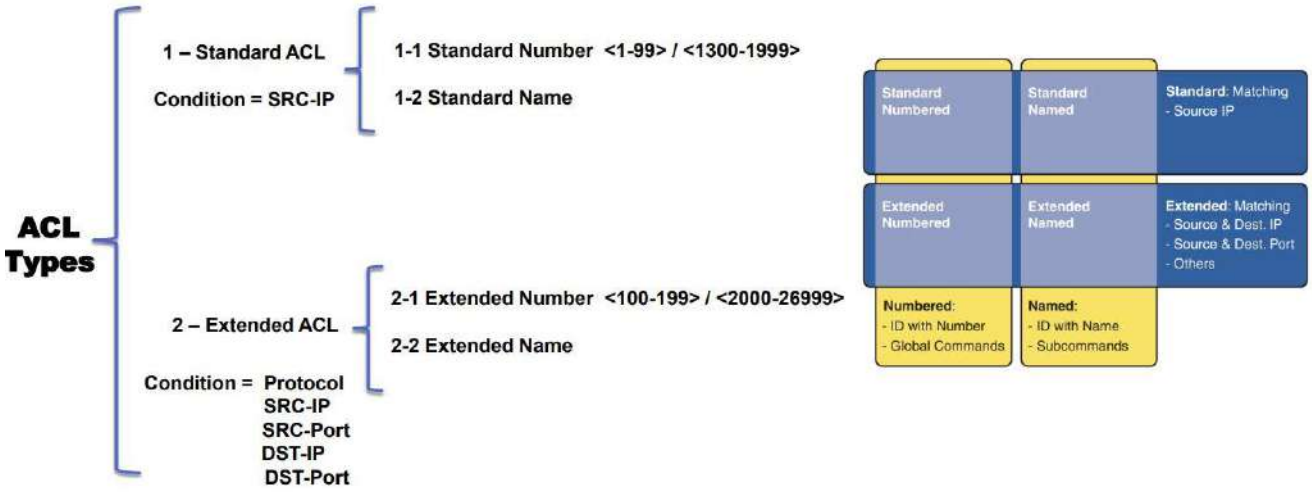
Access Control List’s Actions :

- Permit اجازه عبور به بسته را می دهد.
- Deny اجازه عبور به بسته را نمی دهد.

انواع معرفی Access Control List :

- Standard ACLs
- Extended ACLs
- Reflexive ACLs
- Time-Base ACLs
- Established ACLs

سیسکو دو نوع Access control list با نام های Standard ACL و Extended ACL معرفی کرده است. Standard ACL قدیمی ترین و ساده ترین نوع Access List است که در نسخه ۸,۳ IOS سیسکو ارائه شده است.



: Standard ACL

ترافیک بسته‌ها را به وسیله مقایسه آدرس مبدا (source IP) با آدرس تعریف شده در ACL کنترل می‌کند و action که می‌تواند داشته باشد Deny/Permit است. در همه نسخه‌ها، برایStandard ACL می‌توان یک عدد از۱تا۹۹در نظر گرفت. از نسخه ۱۱,۲ IOS سیسکو امکان تعریف Standard ACLبه وسیله نام فراهم شد و همچنین از نسخه۱۲,۰,۱ سیسکو محدوده عددی بین ۱۳۰۰ تا ۱۹۹۹ برای Standard ACL اضافه شد.

**نکته:

هر Access list میتواند چندین فرمان داخل خود داشته باشد. هر خط فرمان دارای شماره‌هایی به نام sequence است که ترتیب اعمال آنها را مشخص می‌کند. به صورت پیش فرض زمانی که چندین دستور در یک لیست وارد میکنیم، sequenceها با فاصله‌ی ۱۰ تایی انتخاب میشوند. شماره sequence ها را می‌توان به دلخواه تعیین کرد.

به این دلیل شماره گذاری شده که دستورات لیست، به ترتیب اجرا شود،به این صورت که به عنوان مثال روی روتر یک list access standard در جهت in bound تعریف شده، SRC Ip که بسته ارسال کرده را خط به خط باlist access بررسی می کند با اولین خطی که match شود طبق آن action انجام می دهد(permit/deny) .

نکته۱: جهت مدیریت bandwith و resourseها بهتر است تا جای ممکن فیلترینگ در نزدیکترین دستگاه در مبدا صورت گیرد که منابع سخت افزاری و پهنای باند کمتری اشغال شود.

نکته۲: بسته ها تنها تا زمانی کهRuleهایی که شما تعریف کرده اید مطابقت داشته باشند، اعمال خواهد شد. مثلا چند خط رول داشته باشید با اولین رولی که که ترافیک مطابقت داشته باشد، همان اعمال خواهد شد وسایر خطوط در نظر گرفته نمی شود.

*نکته۳: در انتهای هرACL، Deny وجود دارد. یعنی بسته اطلاعاتی با هیچکدام از رول های شما مطابقت نداشته باشند، بسته discard خواهد شد.

: Inbound & Outbound

ACLها در global configuration mode ایجاد شده و سپس آنها را باید فعال نمود. برای کنترل ترافیک انتقالی از راه اینترفیس ها، ACLها را باید روی اینترفیس موردنظر فعال نماییم. در هنگام فعال نمودن ACLهای ایجاد شده باید نوع ترافیکی را که تحت تاثیر قرار خواهد گرفت را مشخص نماییم. ترافیک عبوری را میتوان در دو گروه عمده قرار داد:

Inbound access lists(لبه ورودی): هنگامی که یک access list بر روی بسته های inbound یا ورودی یک اینترفیس اعمال شود، ابتدا بسته ها بر اساس آنچه که در access list تعیین شده، پردازش می شوند و سپس به سمت اینترفیس خروجی Route می شوند.

Outbound access lists(لبه خروجی): هنگامی که یک access list در خروجی یک اینترفیس اعمال و استفاده شود، ابتدا بسته به آن اینترفیس Route می‌شود و سپس پردازش بر اساس رول موجود در access list در خروجی آن اینترفیس اعمال می شود.

نکته:

در ترافیک ورودی روتر اطلاعات رسیده را ابتدا باACLهای تعیین شده در روی اینترفیس مربوطه مقایسه کرده و سپس اقدام به ارسال آنها به مقصد خود می کند. اما در ترافیک خروجی یا outbound ، روتر اطلاعات رسیده را ابتدا به مقاصد خود ارسال کرده و سپس اقدام به مقایسه آنها با ACL مربوطه می‌نماید. یکی از محدودیت‌هایی که استفاده ازACL داراست این است که نمی توان ترافیکی که خود روتر آنها را ایجاد کرده به وسیلهACL ها فیلتر نمود.

برای مثال اگر از دستورات ping و یا traceroute در روی روتر استفاده کرده و یا اقدام به برقراری ارتباط telnet از روتر خود به سمت دستگاه‌های دیگر نماییم، نمی توان این ترافیک ها را به وسیلهACLها فیلترگذاری کرد. اما اگر روتر دیگری اقدام به ping کردن و یا برقراری ارتباط telnet با روتر ما نماید و یا از طریق روتر ما، دستگاه دیگری را هدف قرار دهد، می توان از ACL بهره برد.

نحوه تعریف ACL Standard در حالت عددی:

Ip access-list stadard {number} = number-list-access عدد بین ۱ تا ۹۹ یا ۱۳۰۰ تا ۱۹۹۹

deny|permit اجازه عبور یا عدم اجازه

مشخص کردن IP به یکی از سه روش زیر:

- Host یک آدرس IP مشخص می کنیم مانندHost۱,۱.۱۹۲,۱۶۸
- Any هر IP آدرسی
- source source-wildcard تعیین یک بازه IP به همراه Wildcard Mask

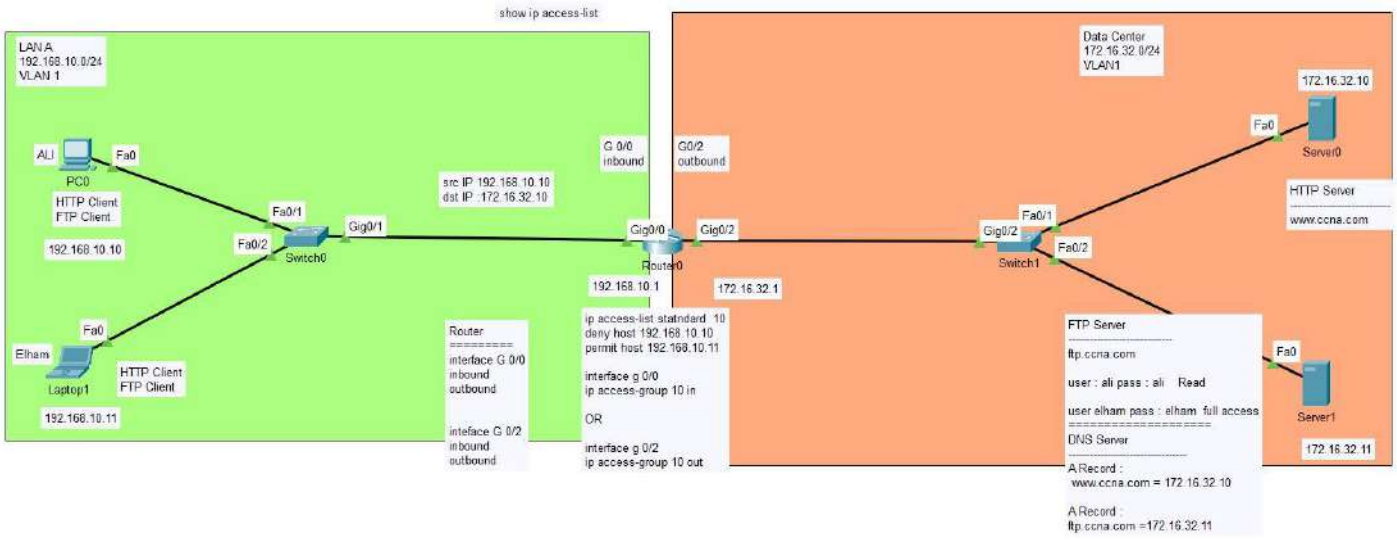
نحوه تعریف ACL Standard با استفاده از نام:

مانند حالت عددی است فقط به جای عدد از name استفاده میکنیم.

IP Access-list {standard|extended} name

deny|permit {host | source source-wildcard | any}

مثال :



قبل از اعمال ACLها ، به PC و Laptop و Serverها IP داده شده است. با تنظیمات HTTP روی Srv0 و تنظیمات FTP و DNSروی Srv1، سرورها را به عنوان HTTP server و FTP Server و DNS server معرفی کرده‌ایم. همچنین PC و Laptop کلاینت‌های ما هستند. در ادامه G0/0 , G0/1 روتر را No shut و IP به عنوان Getway به هر کدام جداگانه اختصاص دادیم(معمولا اولین و یا آخرین آدرس IP هر شبکه را به عنوان Getway انتخاب میکنند). سپس این Getway را به کلاینت‌ها و سرورها هم اختصاص دادیم. در این حالت همه Deviceها Ping همگی را دارند.

به نظرتان PC0 میتواند HTTP srv0 را با آدرس www.ccna.com را باز کند؟ خیر. چون Dns را روی کلاینت ها set نکردیم که بتواند آدرس را به IP تبدیل کند.

حال میخواهیم تنظیماتی را اعمال کنیم که Ali به data center دسترسی نداشته باشد ولی Elham بالعکس.

در ابتدا ما باید قوانین(ایجاد لیست) را تنظیم کنیم و سپس نسبت به سناریو، به interfaceها ابلاغ کنیم.

Router(config)#Ip access-list

Router(config-std-nacl)# Ip access-list standard 10 10لیست اکسس ساخت

Router(config-std-nacl)#deny host 192.168.10.10 دسترسی عدم

Router(config-std-nacl)#permit host 192.168.10.11 دسترسی

```
Router#show ip access-lists
Standard IP access list 10
    10 deny host 192.168.10.10
    20 permit host 192.168.10.11
```

نکته: بعد از هر قانونی، دستگاه به هر دستور یک Sequence اختصاص می‌دهد که به نوعی ترتیب اعمال قوانین را نشان میدهد.(ضریبی از 10)

حال به نظرتان بعد ایجاد لیست قوانین، PC0 میتواند با SRVها ارتباط داشته باشد یا خیر(از روتر میتواند عبور کند یا خیر)؟ بله میتواند. چون هنوز لیست به اینترفیس ابلاغ نشده است.

نحوه ابلاغ:

در این سناریو هم میشود inbound g0/0 اعمال کرد، هم Outbound g0/2.ولی بهتر است inbound باشد تا به روتر وارد نشود که ترافیک اضافی را روتر تحمل کند.

interface g 0/0

ip access-group 10 in

OR

interface g 0/2

ip access-group 10 out

```
Router(config)#int gig 0/0
Router(config-if)#ip access-group {number} {in|out}
```

حال اگر با PC0 ، srv را Ping کنید نتیجه ذیل را مشاهده میکنیم:

```
C:\>ping 172.16.32.10

Pinging 172.16.32.10 with 32 bytes of data:

Reply from 192.168.10.1: Destination host unreachable.
Reply from 192.168.10.1: Destination host unreachable.
Reply from 192.168.10.1: Destination host unreachable.
Reply from 192.168.10.1: Destination host unreachable.

Ping statistics for 172.16.32.10:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

همچنین اگر با **Laptop1** ، **srv** را **Ping** کنید نتیجه ذیل را مشاهده میکنیم:

```
C:\>ping 172.16.32.10

Pinging 172.16.32.10 with 32 bytes of data:

Request timed out.
Reply from 172.16.32.10: bytes=32 time=10ms TTL=127
Reply from 172.16.32.10: bytes=32 time<1ms TTL=127
Reply from 172.16.32.10: bytes=32 time<1ms TTL=127
```

****نکته:

اگر access list خالی بنویسیم در واقع خالی نیست اما آن را خالی می بینیم، بصورت پیشفرض ته هر access list یک خط نا نوشته وجود دارد(any deny). اگر لیست بررسی شد و هیچ خطی مچ نشده خط آخر any deny اجرا می شود.

در مثال بالا اگر access listی ایجاد شود اما قانونی داخلش قرار ندهیم، سپس آن را به g0/0روتر ابلاغ کنیم، PC و laptop هر دو deny میشوند. یعنی هیچ پیامی اجازه ورود به این interface را ندارد.

ip access-list standard LAN_A or ip access-list standard 10

خالی

---

interface g 0/0

ip access-group LAN_A in or ip access-group 10 in

نکته: دستور حذف access list (برای مثال قبل)

Router(config)#int gig 0/0

Router(config-if)#no ip access-group 10 in

Router(config)#no ip access-list standard 10

نکته: دستور حذف و جایگزین کردن قانون در Access list 10

Router(config)#ip access-list standard 10

Router(config-std-nacl)#no 5 خط(سکوئنس) ۵ حذف گردد

Router(config)#15 permit host 192.168.10.12 خط ۱۵ با دستور مدنظر اضافه گردد

نکته: برای اینکه یادمان نرود فلان خط Accessلیست برای چه کاری است، میتوان از remark زیر access-list10 استفاده کرد.

Router(config)#ip access-list standard 10

Router(config-std-nacl)#**remark** PC_ALI

نکته: برای log گرفتن از جابجایی بسته در خط مد نظر (بدرد Tsoot میخورد):

Router(config-std-nacl)#permit 192.168.10.18 **log**

در هنگام استفاده ازACL ها باید چند نکته را مدنظر قرار دهید که در ادامه این موارد را مورد بررسی قرار داده ایم:

- ✓ تنها یک ACL را می توان برروی ترافیک های Inbound و یک ACL برروی ترافیک های Outbound تعریف کنید.

- ✓ ACLها را به نحوی تعریف کنید که فیلترهای کلی در ابتدای لیست قرار داشته باشند و فیلترهای جزئی در انتهای لیست.
- ✓ شروط ACL را نمی‌توان تغییر داد و در صورت نیاز باید کل ACL را حذف کرده و مجددا آن را ایجاد نمایید.ACL هایی که از نوع Namedهستند از این قانون مستثنی هستند.
- ✓ در صورتی که در انتهای ACL از دستور permit any استفاده نشود و پکت ها با شروط مشخص شده مطابقت نداشته باشد، پکت دور ریخته (Drop) خواهد شد.
- ✓ ACLها تنها به ترافیک هایی اعمال خواهد شد که از روتر عبور میکنند، پس درنتیجه ترافیک هایی که از روتر تولید و ارسال می‌شوند باACL ها محدود نخواهند شد.
- ✓ ACLهایی که از نوع Extended هستند را تا حد ممکن برروی روترهای نزدیک به مبدا تعریف کنید، چرا که با استفاده از این دسته ازACL ها میتوان جزئیات بیشتری از پکت ها را مورد بررسی قرار داد و فیلترهای بیشتری را اعمال نمود. این موضوع باعث می شود تا ترافیک های قرار گرفته برروی لینک به حداقل ممکن برسد و از پهنای باند استفاده موثر گردد.
- ✓ اولویت لیستها، از بالا به پایین میباشد. روش متداول در نوشتن لیستها به صورت نوشتن لیستهای permit و سپس لیستهای deny میباشد.

Wilcard Mask :

در تعریفACL ها به جای استفاده از Subnet Mask از **Wildcard Mask** استفاده می شود که بیان کننده تعداد بیت ها از آدرس می باشد که باید در ACLمورد بررسی قرار بگیرند و به عبارت دیگر مشخص کننده قسمتی از آدرس IP Address می باشد که باید در ACL مورد بررسی قرار بگیرد(تشخیص بیت‌های مهم و غیر مهم).

Wildcard Maskدقیقا برعکس Subnet Mask می باشد(به جایbit های ۱ در subnet mask ما از بیت های صفر در wildcard mask و به جای بیت های صفر در subnet mask از بیت های یک در wildcard mask استفاده می کنیم).برای مثال فرض کنید که 255.255.0.0 mask را در اختیار داریم. اگر این ماسک را در مبنای ۲ بنویسیم خواهیم داشت:

255.255.0.0 = 11111111.11111111.00000000.00000000

سرانجام اگر این subnet mask را تبدیل به wildcard mask نماییم، نتیجه به صورت زیر خواهد بود:

00000000.00000000.11111111.11111111

که در این صورت تبدیل این آدرس به حالت دسیمال یا مبنای ۱۰ آدرس 0.0.255.255 به دست خواهد آمد. در این مثال wildcard mask به روتر می‌گوید که فقط ۱۶ بیت از اول آدرس IP باید با ۱۶ بیت از آدرس مشخص شده در هریک از قانون های ACL یکسان باشد تا آن قانون روی پیام رسیده اجرا گردد. در غیر اینصورت، روتر به بررسی قانون‌های بعدی خواهد پرداخت. دو نوع مخصوص از wildcard mask وجود دارد:

0.0.0.0

255.255.255.255

ماسک اولی به روتر می گوید که تمامی ۳۲ بیت آدرس پیام رسیده باید با آدرس مشخص شده در لیست ACL برابر باشد تا اینکه قانون موردنظر روی آن اجرا شود. برای همین هم اگر wildcard mask برابر با ۰،۰،۰،۰ باشد، به نام hostنامیده می شود.یک مثال ساده میزنیم:

اگر قانون موجود در ACLرا به صورت مقابل داشته باشیم:

192.168.1.1 0.0.0.0

به این معنی است که روتر دقیقا بدنبال آدرس ۱۹۲،۱۶۸،۱،۱ در بین پیامهای رسیده می گردد که اگر هیچ مشابهی پیدا نشود، روتر موارد بعدی موجود در لیست ACL را بررسی می نماید. بعد از اینکه لیست ACL را به صورت0.0.0.0 192.168.1.1 تنظیم نمودیم، روتر به طور اتوماتیک آن را به حالت 192.168.1.1 **host**در خواهد آورد.

ماسک دوم (۲۵۵،۲۵۵،۲۵۵،۲۵۵) به روتر می‌فهماند که همه آدرسهایی که وارد روتر می شوند قابل پذیرش بوده و قانون مزبور روی همه پیام‌های ورودی اجرا خواهند شد. معمولا این نوع را به صورت آدرس IP برابر با ۰،۰،۰،۰ و Wildcard Mask برابر با ۲۵۵،۲۵۵،۲۵۵،۲۵۵ در داخل ACL مشخص می کنیم: ۲۵۵،۲۵۵،۲۵۵،۲۵۵ 0.0.0.0که روتر آن را به صورت 0.0.0.0 any در خواهد آورد. آدرس IP نوشته شده در این فرمول اهمیت چندانی نداشته و می توان هر آدرسی را بدلخواه وارد نمود.

مثلا میتوان نوشت: ۲۵۵،۲۵۵،۲۵۵،۲۵۵ ۱۹۲،۱۶۸،۱،۱۴۵ که در این حالت نیز روتر صرف نظر از آدرسی که مشخص شده است، به علت ماسک داده شده، همه آدرس ها را قبول خواهد کرد. برای اینکه بهتر بتوانید با Wildcard Mask آشنا شوید، چند مثال را در این باره مطرح می کنیم. جدول زیر برخی از آدرس های **IP** و **Wildcard Mask** را نشان می دهد.

IP Address	Wildcard mask	توضیحات
۰.۰.۰.۰	۲۵۵.۲۵۵.۲۵۵.۲۵۵	تمامی آدرس ها پذیرفته خواهند شد
۱۷۲.۱۶.۱.۱	۰.۰.۰.۰	پیام رسیده حتما باید دارای آدرس ۱۷۲.۱۶.۱.۱ باشد تا قانون موردنظر در روی آن اجرا گردد.
۱۷۲.۱۶.۱.۱	۰.۰.۰.۲۵۵	قانون مزبور بر روی پیام های رسیده از شبکه 172.16.1.x
۱۷۲.۱۶.۲.۰	۰.۰.۱.۲۵۵	قانون مزبور بر روی پیامهایی که دارای آدرس ۱۷۲.۱۶.۲.۰/۲۳
۱۷۲.۱۶.۰.۰	۰.۰.۲۵۵.۲۵۵	قانون مزبور بر روی پیامهایی که دارای آدرس 172.16.x.x می باشند اجرا می گردد

مثال wild-card:

فرض کنید ما یک شبکه با ۱۰،۰،۰،۰ و ۲۵۵،۲۵۵،۲۵۵،۲۴۰ mask Subnet داریم. ما می خواهیم یک ACL برای این شبکه ایجاد کنیم که کل شبکه به یکسری منابع دسترسی نداشته باشند. برای این کار در ACL ما نیاز به اختصاص دادن Mask Wilcard برای آن Subnet داریم. ابتدا باینری mask Subnetبه صورت زیر محاسبه میکنیم: 255.255.255.240=11111111.1111111.1111111.11110000

Wild-card: 00000000.00000000.00000000.00001111

در مرحله بعد یه جمع ساده می سازیم ،به آخرین Octet نگاه کنید. برای Mask Wilcard فقط یک ها را جمع می بندیم: 8+4+2+1=15

بنابراین WilcardMask ما ۰،۰،۰،۱۵ خواهد بود.

Extended ACL :

در ACL Standard ما تنها می توانیم بر اساس آدرس مبدا ، بسته ها را کنترل کنیم ولی ACL Extended میتواند کنترل را براساس آدرس مبدا و مقصد ، شماره پورت مبدا و مقصد ، نوع پروتکل انجام دهد، در نتیجه Extended ACL به عنوان یک ابزار قدرتمند برای مدیران برای کنترل ترافیک محسوب می شود. در همه نسخه‌ها ، برای Extended ACL میتوان یک عدد از ۱۰۰ تا ۱۹۹ در نظر گرفت. از نسخه IOS ۱۱,۲ سیسکو امکان تعریف Extended ACL به وسیله نام فراهم شد و همچنین از نسخه IOS ۱۲,۰,۱ سیسکو محدود عددی بین 2000 تا 2699 برای ACL Extended اضافه شد.پارامترهای که می توان توسط Extended ACL کنترل کرد:

- ✓ آدرس IP مبدا
- ✓ آدرس IP مقصد
- ✓ شماره پورت مبدا
- ✓ شماره پورت مقصد
- ✓ نوع پروتکل

```
Router(config-ext-nacl)#deny ?
  ahp     Authentication Header Protocol
  eigrp   Cisco's EIGRP routing protocol
  esp     Encapsulation Security Payload
  gre     Cisco's GRE tunneling
  icmp    Internet Control Message Protocol
  ip      Any Internet Protocol
  ospf    OSPF routing protocol
  tcp     Transmission Control Protocol
  udp     User Datagram Protocol
```

```
Router(config-ext-nacl)#permit icmp host 192.168.10.10 host 172.16.32.10 ?
  <0-256>               type-num
  echo                  Echo (ping)
  echo-reply            Echo reply
  host-unreachable      Host unreachable
  net-unreachable       Net unreachable
  port-unreachable      Port unreachable
  protocol-unreachable  Protocol unreachable
  ttl-exceeded          TTL exceeded
  unreachable           All unreachables
```

پروتکل ICMP را میشود فیلترش را جزئی‌تر نوشت.

نحوه تعریف**Extended ACL** : عدد و **name** -----> مثال این دستور در شکل زیر آمده است:

(config)# IP Access-list {standard|extended} name(or 100_199 & 2000_2699)

(config-ext-nacl)# {permit|deny} protocol source [Source port] destination [destination port]

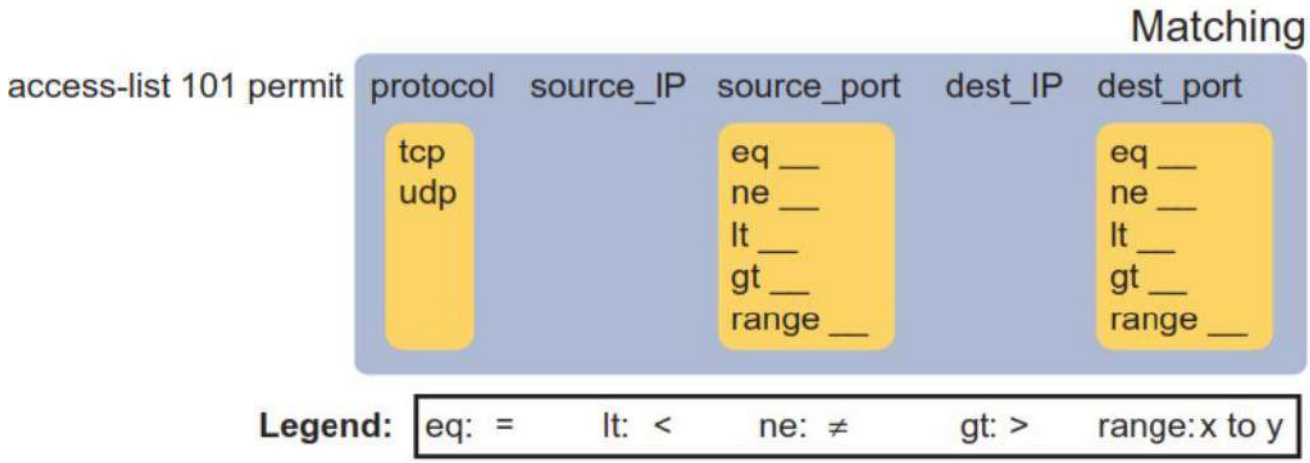
Router(config)#interface fastEthernet 0/0

Router(config-if)#ip access-group 101 in

نکته:

هنگامی که یک دستور ACL Extended شامل کلمه کلیدی tcp یا udp باشد، به SRC PORT / DST PORT اشاره دارد.

برای انجام مقایسه شماره پورت از کلمات کلیدی: equal, not equal , less than , greater than , range استفاده می شود.




```
Router(config-ext-nacl)#deny tcp host 192.168.10.10 host 172.16.32.10 ?
  eq             Match only packets on a given port number
  established    established
  gt             Match only packets with a greater port number
  lt             Match only packets with a lower port number
  neq            Match only packets not on a given port number
  range          Match only packets in the range of port numbers
  <cr>
```

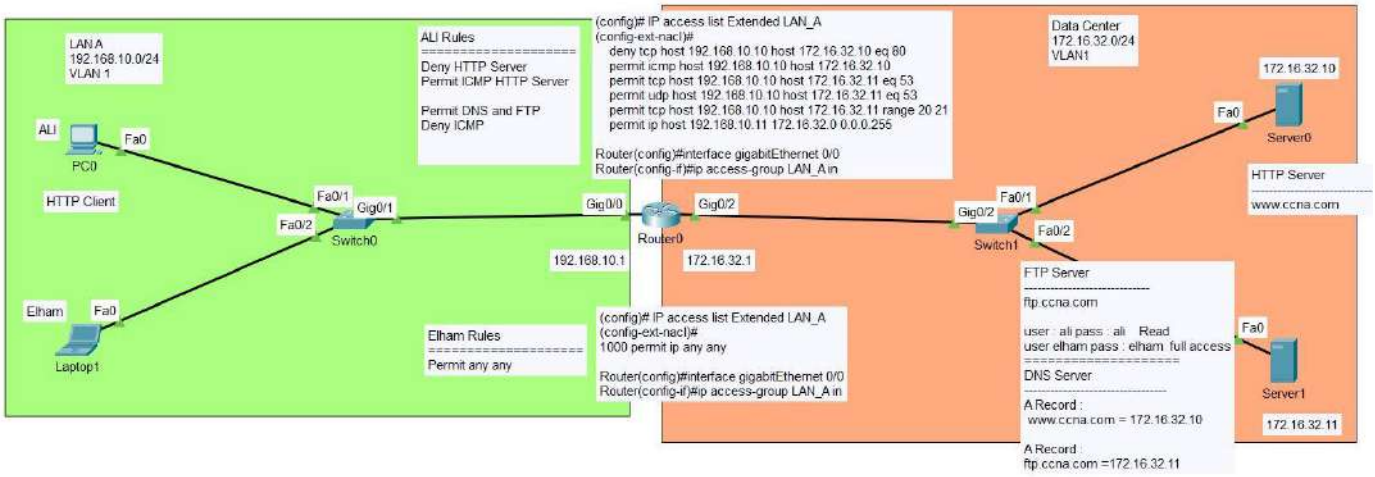
لیست پورت های مهم و شناخته شده UDP و TCP :

Port Number(s)	Protocol	Application	access-list Command Keyword
20	TCP	FTP data	ftp-data
21	TCP	FTP control	ftp
22	TCP	SSH	—
23	TCP	Telnet	telnet
25	TCP	SMTP	smtp
53	UDP, TCP	DNS	domain
67	UDP	DHCP Server	bootps
68	UDP	DHCP Client	bootpc
69	UDP	TFTP	tftp
80	TCP	HTTP (WWW)	www
110	TCP	POP3	pop3
161	UDP	SNMP	snmp
443	TCP	SSL	—
514	UDP	Syslog	—
16,384–32,767	UDP	RTP (voice, video)	—

نکته: sequence بندی مانند ACL standard است.

مثال:

ACL برای Ali و Elham طبق شکل



نتیجه: علی طبق قانون ولی الهام با همه IPها می‌تواند با سرورها ارتباط داشته باشد.

```
Extended IP access list LAN_A
    10 deny tcp host 192.168.10.10 host 172.16.32.10 eq www
    20 permit icmp host 192.168.10.10 host 172.16.32.10
    30 permit tcp host 192.168.10.10 host 172.16.32.11 eq domain
    40 permit udp host 192.168.10.10 host 172.16.32.11 eq domain
    50 permit tcp host 192.168.10.10 host 172.16.32.11 range 20 ftp
    1000 permit ip any any
```

*** نکته : در این سناریو برای Elham یک دستور کلی را اعمال کردیم که بسیار خطرناک است. چون هر سیستمی بتواند به سوئیچ وصل شود میتواند به سرورها دسترسی داشته باشد.

برای جلوگیری از اینکار، دستور را کمی جزئی تر مینویسیم. برای اینکار میتوان از **wild-card** برای مشخص کردن بیت‌های اهمیت دار استفاده کرد. مثلا دستوری اعمال میکنیم که مشخص شود ۲۴ بیت اول IP مهم هستند و اگر قرار است IPی با سرورها ارتباط داشته باشد باید ۲۴ بیت اول آن برابر باشد.

در ابتدا خط ۱۰۰۰ را حذف میکنیم. Router(config-ext-nacl)#no 1000

Router(config-ext-nacl)#permit ip host 192.168.10.11 172.16.32.0 **0.0.0.255**

این خط یعنی : IP الهام اگر به هر IPی که ۲۴ بیت اولش(بیت‌های با اهمیت) برابر 172.16.32 بود می تواند متصل شود.

یعنی الهام به هر دو سرور می‌تواند متصل شود.

```
Router#show access-lists
Extended IP access list LAN_A
    10 deny tcp host 192.168.10.10 host 172.16.32.10 eq www
    20 permit icmp host 192.168.10.10 host 172.16.32.10
    30 permit tcp host 192.168.10.10 host 172.16.32.11 eq domain
    40 permit udp host 192.168.10.10 host 172.16.32.11 eq domain
    50 permit tcp host 192.168.10.10 host 172.16.32.11 range 20 ftp
    60 permit ip host 192.168.10.11 172.16.32.0 0.0.0.255
```

** نکته: اگر به جای host از 0.0.0.0 (wildcard) +IP استفاده کنیم، سیستم عامل host در نظر میگیرد. IP رو هم اگر خالی بدون Host یا Wildcard بنویسیم ، Host در نظر می‌گیرد.

سوال :

در مثال بالا اگر یک سرور دیگر با IP 172.16.32.12 به سوئیچ یک وصل کنیم، ارتباطات علی، الهام و سیستم جدید با IP 192.168.10.13 به این سرور را تشریح کنید.

- الهام کامل متصل است چون دردستور ذکر شد که فقط ۲۴ بیت اول بایدباشد(مابقی مهم نیست)که با IP سرور جدید تطابق دارد.

- علی کامل قطع است چون خطی برای این ارتباط تعریف نشده است و هر IP غیر خط با به صورت خودکار Deny می‌شود.

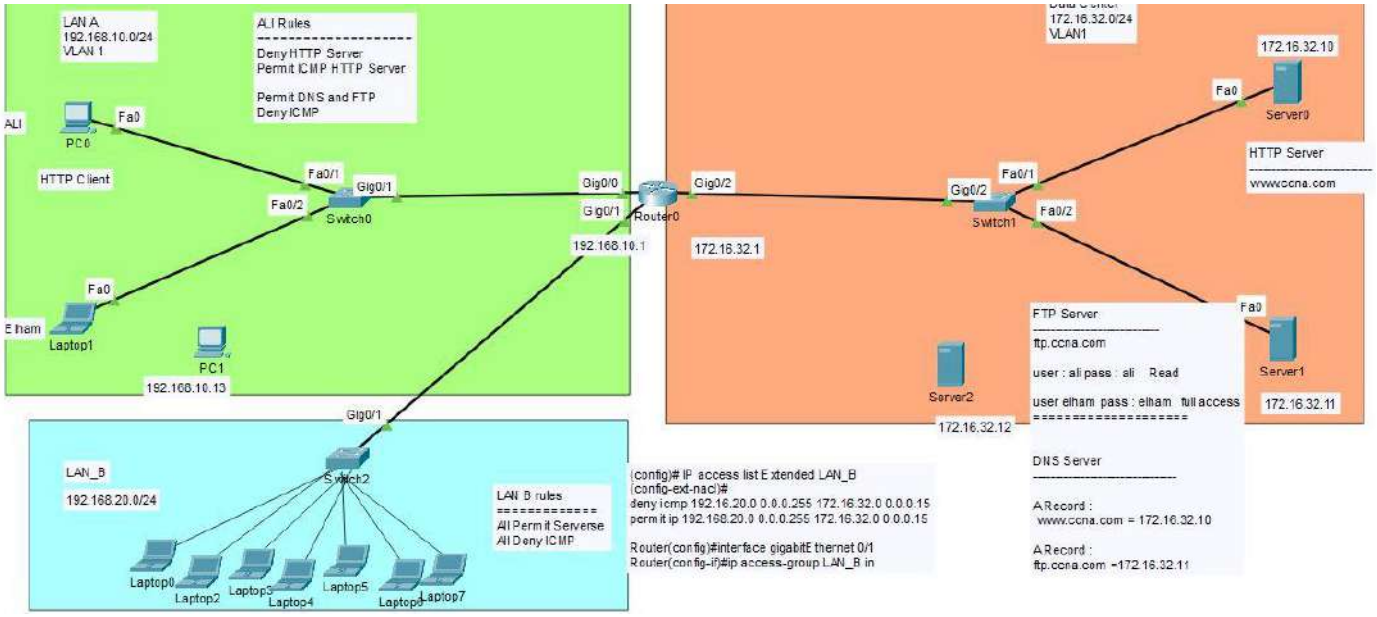
- سیستم جدید هم ارتباطی ندارد ، چون با خط آخر که deny any Ip مچ شده است.

مثال۲:

بهترین کار(رول نویسی) برای اضافه کردن LAN_B چیست؟

می‌توان رول‌های Aclقبلی را به Acl lan B اضافه کرد. ولی چند رول نوشته شده(اضافه هم خواهد شد) که شاید تداخل بخورد و اصلاً شاید استفاده نشود. شدنی است ولی منطقی نیست. یا حتی میتوان در مسیر outیک Acl مشترک داشت(برای هردو) ولی همچنان مشکل قبل پابرجاست.

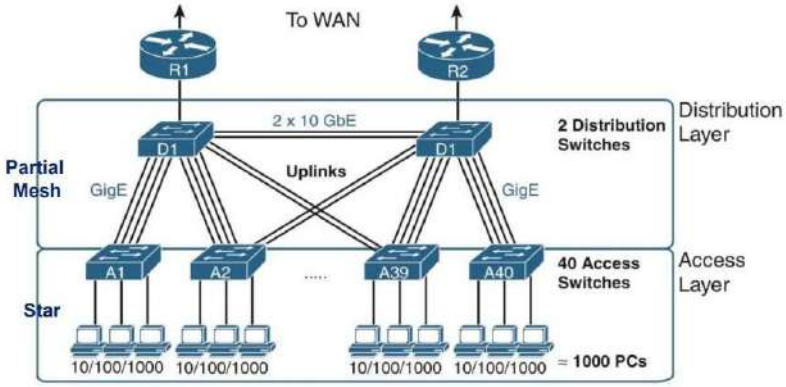
نکته: رول‌های درخواستی این مثال به ترتیب (permit کردن همه Ipها برای سرویس‌ها و deny کردن همه Ip ها برای ICMP) است. نکته اینجاست که اگر ما ابتدا رول اول را بنویسیم، رول دوم اجرا نمیشود. چرا؟ چون وقتی IP ها را در سطح لایه سه و چهار permit میکنیم(که Icmpهم شامل میشود) ، دیگر دستور deny کردن ipها برای icmp نامعتبر میشود چون اولویت با خط اول است. پس باید ابتدا رول deny را بنویسیم، بعد permit (برای این سناریو).




```
Extended IP access list 150
    10 deny icmp 192.16.20.0 0.0.0.255 172.16.32.0 0.0.0.15
    20 permit ip 192.168.20.0 0.0.0.255 172.16.32.0 0.0.0.15
```

Enterprise Campus Network Desiqn :

Two-Tier Campus Design (Collapsed Core)



نکته: دلیل اینکه در این راهکار سوئیچ‌های A1 و A2 و A39 و... را برای ارتباط با هم به صورت قطاری بهم متصل نمیکنند این است که اگر یکی از سوئیچ‌ها از دسترس خارج شود، ارتباط بین سوئیچ‌های چپ و راستی از هم قطع می‌شود. ثانیا اگر بخواهیم برای رفع این مشکل، همه سوئیچ‌های موجود در لایه Access را بهم متصل کنیم(کابل n(n-1)/2(mesh))، دیگر portی باقی نمی‌ماند که بخواهیم End deviceها را به سوئیچ‌ها وصل کنیم. ثالثا با وصل کردن همه سوئیچ ها بهم ، پروتکل stp ارتباط یکی از مابین‌ها را block می‌کند. رابعاً شاید فاصله بین سوئیچ‌ها زیاد باشد که این عمل را دشوار و بی‌منطق می‌کند.

نکته۱: این نوع طراحی اصولاً برای مکان‌هایی در نظر گرفته می‌شود که تعداد End-Deviceها در این نوع از شبکه‌ها به تعداد حداکثر ۲۰۰ می‌رسد. در لایه distribution فقط می‌توان دو سوئیچ قرار داد.

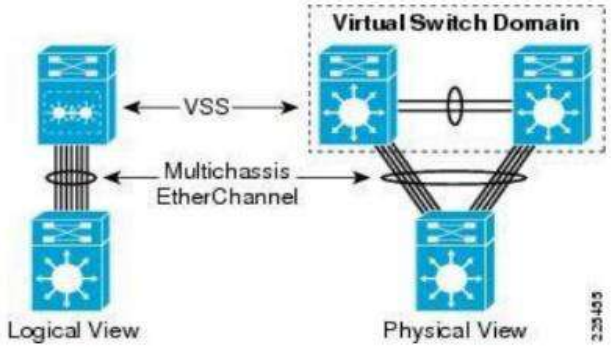
نکته۲: به ارتباطات لایه Access،downlink و به لایه distribution،uplink گفته می‌شود.

نکته۳: در این مدل در لایه Distribution، یکی از سوئیچ باید RB Primary و دومی RB secondary باشند (بخاطرSTP).

نکته٤: در این مدل ارتباط بین لایه Access و distribution لایه دوئی می‌باشد.(البته لایه سه‌ی هم می‌تواند باشد)

نکته٥: همه ارتباطات A2 , A1 به D1 و... bundle شده اند(Etherchannel). A2 هم به D1 و هم به D2 متصل شده است. این شرایط درصورتی Recommended (توصیه شده) است که سوئیچ‌های D1,2 stack شده باشند(در سوئیچ‌های Catalyst با روش virtual stack مثلVSSیا physical stack مثل stack wise و در سوئیچ‌های Nexus با روش VPC)، چونSTPیکی از ارتباطات راBlk میکند.

نکته٦: به این فناوری که تعدادی Port با D1 و تعدادی Port با D2 اترچنل میکنیم، Multichassis Etherchannel (MEC) گفته می‌شود.

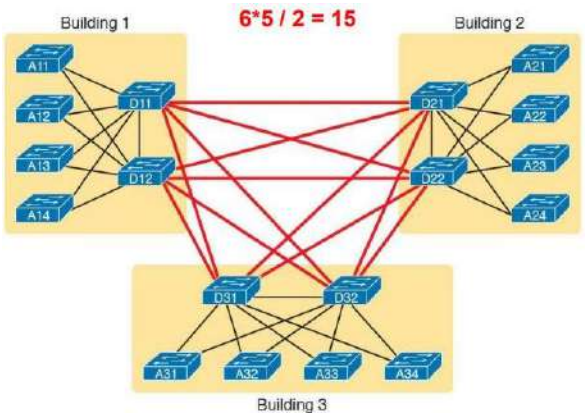


نکته۷: در سال ۲۰۱۰ ، شرکت سیسکو از فناوری‌های Virtual-port-channel (VPC) سوئیچ‌های Nexus دیتاسنترها و از Multichassis EtherChannel (MEC) سوئیچ‌های catalyst برای غلبه بر محدودیت stp رونمایی کرد.

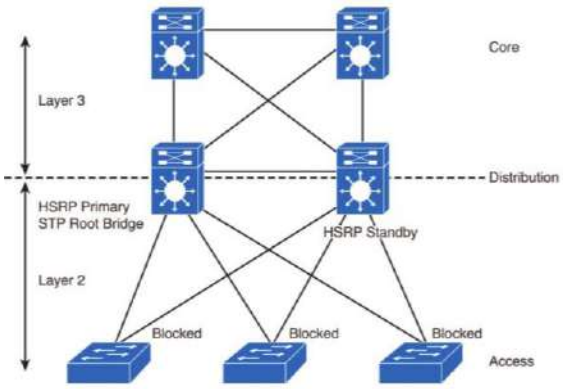
نکته۸: سوئیچ‌های Cisco Catalyst۶۵۰۰ به بالا از Virtual Switching System(VSS) و خانواده سوئیچ‌های Cisco Nexus از Virtual Port Channel(VPC) برای ساخت MEC پشتیبانی می‌کنند. همچنین سوئیچ‌های Cisco Catalyst۳۸۵۰ نیز قادر به پشتیبانی از معماری MEC هستند. البته در این حالت باید از StackWise برای اتصال سوییچ‌ها استفاده کنید.

نکته۹: مشکل این ساختار چه بود؟

با توجه به شکل مقابل اگر بنا باشد طبق فرم بالا چندین شبکه lan را به هم متصل کنیم، از آنجایی که لایه distribution در جهت ارتباط بین سوییچ‌ها و داشتن REDUNDANCY به هم متصل شوند (ارتباط Mesh Full)، با این کار تعداد پورت‌های سوییچ‌های distribution هدر می رود و از یک جایی به بعد محدود می شویم و نمی توانیم شبکه را توسعه دهیم، به همین دلیل به سراغ معماری سه لایه‌ی رفتند.



Three-Tier Campus Design (Core)



- دارای سه لایه Core ، Distribiotion و Access

-لایه core برای اتقای شبکه ایجاد میشود، که میتواند MLS باشد یا روتر.

-لایه Access تا Distribution همچنان layer2 است، ام ارتباطات بین coreها با هم، Coreها و Distributionها layer3 است.

- در این معماری اگر stack داشته باشیم port block نداریم، در غیر این صورت داریم.

نکته: در طراحی دو لایه‌ای، لایه Core و Distribution با یکدیگر ادغام می‌شوند و تشکیل لایه جدیدی به نام Collapsed را می‌دهند و از دستگاه‌های کمتری استفاده می‌کنند که باعث کاهش هزینه ها شود.

سوییچ های مورد استفاده در لایه Access

Table 1-3 *Common Access Layer Switch Platforms*

	Catalyst Model	Max Port Density	Uplinks	Max Backplane	Other Features
	2960-X	384 (Up to 8 48-port switches in a stack)	2 10GE or 4 1 Gigabit Ethernet per switch	80 Gbps	RIP, OSPF available for routed access layer; PoE+
	3650	432 (Up to 9 48-port switches in a stack)	2 Gigabit Ethernet or 4 10GE	160 Gbps	Full-featured routing available, integrated wireless controller, PoE+
	3850	432 (Up to 9 48-port switches in a stack)	4 Gigabit Ethernet, 4 10GE	480 Gbps	Full-featured routing available, integrated wireless controller, PoE+, UPoE
	4500E	384 (Up to 8 48-port modules per chassis)	Up to 12-port 10GE per module	928 Gbps	Dual supervisors, full-featured routing available, integrated wireless controller, PoE+, UPoE

سوییچ های مورد استفاده در لایه Distribution :

Table 1-4 *Common Distribution and Core Layer Switch Platforms*

	Catalyst Model	Max Port Density	Max Backplane	Other Features
	4500-X	80 10GE	1.6 Tbps	Dual-chassis Virtual Switching System (VSS) redundancy
	4500E	96 10GE or 384 Gigabit Ethernet	928 Gbps	Dual supervisors
	6807-XL	40 40Gbps, 160 Gigabit Ethernet, 480 Gigabit Ethernet	22.8 Tbps	Dual supervisor, dual-chassis VSS redundancy

ICMP :

پروتکل icmp که مخفف عبارت internet control message protocol است که در فارسی آن را پروتکل کنترل پیام‌های اینترنتی ترجمه می‌کنند. همانطور که می‌دانیم IP مکانیزم داخلی برای ارسال پیام‌های کنترلی و خطا ندارد. به همین دلیل پروتکلی مانند ICMP مورد نیاز است. به همین خاطر پروتکل icmp یک بخش جدانشدنی از پروتکل ip است. بطورکل icmp جهت خطایابی در کامپیوترها، روترها و هاست، بررسی وجود سیگنال و به طور کلی بررسی وضعیت ارتباطی بین روتر و سرورها مورد استفاده قرار می‌گیرد.

در مدل ۵ لایه‌ای شبکه، این پروتکل همانند پروتکل ip در لایه‌ی network قرار می‌گیرد، اما نوع کارکرد آن شبیه پروتکل‌های لایه transport می‌باشد.

ICMP با پروتکل های ارسال مانند TCP و UDP تفاوت دارد که در واقع برای تبادل اطلاعات بین سیستم‌ها به کار نمی‌رود. پیام‌های ICMP به منظور تشخیص یا کنترل پروسه‌ها یا یافتن خطاهای Ip ، اورهای ICMP مستقیما به Src address IPدر پاکت پیام منشا می‌رود.

داده های پیغام‌های ICMP درون هدر IP کپسوله (Encapsulated) می‌شوند که به این معناست که هدر داده نگار ICMP پس از اطلاعاتIPV4/6می‌آیند. اولین بخش هدر بسته ICMP شامل پارامترهایی است که به دستگاه‌های شبکه در شناسایی پیغام های خطا یا کوئری کمک می کند.

در میان ۳۲ بیت اول، ۸ بیت اول نوع پیغام را مشخص می کنند؛ ۸ بیت بعدی کد پیغام را تعیین می‌کنند؛ و بیت‌های باقی مانده صحت داده ها را با اطلاعاتی به اثبات می رسانند.

بنابراین، سه فیلد اطلاعاتی شامل: انواع ICMP، کد ICMPو Checksumمی شوند:

ICMP Header Format

Offsets	Octet	0								1								2								3							
Octet	Bit	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	Type								Code								Checksum															
4	32	Rest of Header																															

انواع ICMP:

این انواع مشخص کننده هدف بسته ICMPهستند؛ پس به طور خلاصه به دستگاه مقصد اطلاع می دهد که به چه دلیلی این پیغام را دریافت کرده است. حدودا بین ۰ تا ۲۵۵ نوع پیغامICMPوجود دارد که هر نوع یک اطلاعات خاصی را ارائه می‌دهد. برخی از مهم‌ترین انواع ICMP عبارتند از:

۱. Echo Replyبرای پینگ استفاده می‌شود.
۲. Destination is unreachableمقصد غیرقابل دسترسی است.
۳. Source quenchبه این معنی است که روتر بیش از حد بار دارد.
٤. Redirectاین نشانگر استفاده از روتر دیگر است.
۵. Echo Requestمشابه ۱، برای پینگ استفاده می‌شود.
٦. Router advertisement replyپاسخ آگهی روتر.
۷. Router solicitationدرخواست روتر.
۸. Time Exceededزمان بیشتر است. این برای traceroute استفاده می‌شود.
۹. و...

کد ICMP :

کد ICMP اطلاعات جامع‌تری در خصوص پیغام‌های ارسالی فراهم می‌کند. برای مثال، ICMP نوع ۳ با کد ۰-۱۵ مشخص می‌کند که چرا مقصد در دسترس نیست که یعنی اگر کد ۰ باشد، به این دلیل است که شبکه در دسترس نیست. به همین شکل برای نوع ۳ کد۱، پیغام مشخص‌کننده این است که هاست در دسترس نیست.

به همین ترتیب، کد ۰ نوع ۸ و کد ۰ نوع ۰ نمایانگر پیغام های echo-request و echo reply هستند. به همین دلیل، هر نوع پیغام با کد یکسان می‌تواند اطلاعات شبکه‌ای متفاوتی را بیان کند.

: Checksum

مجموع یا checksumیک مکانیزم شناسایی خطاست که از صحت داده‌ها اطمینان حاصل می‌کند. مقدار checksumنمایانگر بیت‌های موجود در پیغام انتقالی است. ارسال‌کننده در پیغام خود مجموع داده‌ها را شمارش کرده و دریافت‌کننده نیز هنگام دریافت این مجموع را می‌شمارد. این فرآیند برای مقایسه مجموع اصلی با مجموع دریافتی است.

موارد کاربرد ICMP :

Ping :

پینگ یک دستور است که برای در دسترس بودن شبکه و تأخیرات بین دو دستگاه از پیغام‌های echo-request و ICMP echo-reply استفاده می‌کند. این کارکرد به سادگی با تخمین تعداد کل بسته های ارسالی و دریافتی و درصد Packet lossها، در دسترس بودن سرور مقصد را مشخص می‌کند.

این کارکرد علاوه بر این به شناسایی حداکثر حجم واحد های انتقالی (MTU) نیز کمک می‌کند.

ping <ip_address>

Traceroute :

Traceroute نیز یک کامند لاین دیگر است که از پیغام های echo-request و ICMP echo-reply و یک متغیر TTLبرای ردیابی مسیر بین مبدا و مقصد استفاده می کند. این روش برای شناسایی تأخیرات پاسخ‌دهی نیز مناسب بوده و با ارسال کوئری های متعدد به هر پرش (Hop) از دقت آن اطمینان حاصل می کند.

چطور از ICMP برای ایجاد یک حمله DDoS استفاده می‌شود؟

در ادامه به سه مورد از انواع حملات DDoS که توسط ICMP ایجاد می‌شوند، اشاره خواهیم کرد:

- ICMP flood attack

یک سیل پینگ یا ping flood، زمانی است که یک مهاجم در تلاش است تا دستگاه قربانی را با ارسال بسته های بی‌شمار Echo-request از کار بیاندازد. به صورتی که دستگاه مجبور است تمام این بسته‌ها را پردازش کرده و به آنها پاسخ دهد. این موضوع باعث مصرف بیش از حد منابع پردازشی شده و دسترسی کاربران مجاز را مخدوش می‌کند.

- Ping of death attack

یک حمله ping of deathزمانی رخ می دهد که مهاجم یک پینگ بزرگتر از حد مجاز یک بسته به سمت دستگاه قربانی ارسال می کند. این موضوع دستگاه را کند کرده و یا باعث هنگ کردن آن می شود. این بسته در مسیر خود به سمت مقصد، به قسمت های کوچک‌تری تقسیم می‌شود؛ اما زمانیکه مقصد آن را مجدداً کنار هم قرار می‌دهد، سایز بسته باعث وقوع یک buffer overflow می‌شود.

این نوع حملات در حال حاضر بسیار متداول هستند، اما دستگاه های مدرن جلوی اینگونه حملات مقاوم هستند.

- Smurf attack

در یک حمله smurf مهاجم با یک آدرس IP سرقت رفته، یک بسته ICMP ارسال می‌کند. تجهیزات شبکه به بسته پاسخ می‌دهند. که پاسخ ها را به سمت IP سرقت رفته ارسال می‌کنند؛ این موضوع قربانی را با حجم وسیعی از بسته‌های ناخواسته مواجه می کند.

ICMPتنها پروتکلی نیست که در حملات لایه ۳ مورد استفاده قرار می گیرد؛ مهاجمین از بسته های GREنیز در گذشته استفاده می کردند.

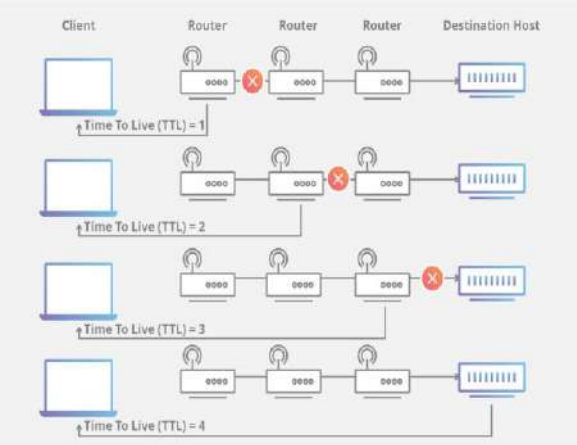
به طور کلی حملات DDoSدرصدد از کار انداختن تجهیزات و زیرساخت های شبکه‌ای هستند؛ البته بجز حملات لایه اپلیکیشن که تنظیمات وب را مورد هدف قرار می‌دهند.

TTL (Time to Live) :

TTLیا Time to Live یک مقدار است که به مدت زمان فعال بودن یک بسته یا یک داده، بر روی یک کامپیوتر یا شبکه اشاره دارد. معنای TTL، یا طول عمر یک بسته، به موضوع و حوزه فعالیت آن بسته بستگی دارد. برای مثال، در بستر بسته های IP یا پروتکل اینترنت، TTLمقداری است که به یک روتر شبکه اطلاع می‌دهد که این بسته از چه مدت در شبکه بوده و تا چه زمانی می‌تواند عمر کند. در واقع TTLبه عنوان یک Timestamp یا شمارنده ای عمل می‌کند که به هر بسته ضمیمه می‌شود. زمانی که طول عمر از پیش تعریف شده یا شمارنده منقضی شود، یک بسته یا مجدداً اعتباردهی می‌شود و یا به کلی نادیده گرفته می‌شود.

TTL چطور کار می کند؟

ادمین ها می توانند TTL را بر روی هر مقداری بین ۱ تا ۲۵۵ تنظیم کنند. البته هر سیستم عامل از یک سری مقادیر پیش‌فرض مشخصی پشتیبانی می‌کند.



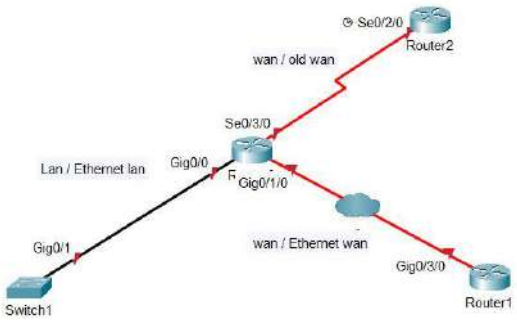
زمانی که بسته‌ای از روتر خارج می‌شود، روتر از مقدار TTL یک شماره کم می‌کند؛ سپس بسته به سمت مقصد بعدی خود در شبکه حرکت می‌کند. زمانی که مقدار TTL صفر باشد، پس از آخرین کسری، بسته توسط روتر به دور انداخته می‌شود. در این لحظه یک پیام ICMP یا پروتکل پیام کنترل اینترنت، به سمت هاست یا میزبان اولیه ارسال می‌شود.

در کنار محدودسازی طول عمر یک بسته،TTLمشخص می‌کند که آن بسته چه مدت در چرخه بوده و تا چه زمانی درون شبکه در جریان خواهد بود.

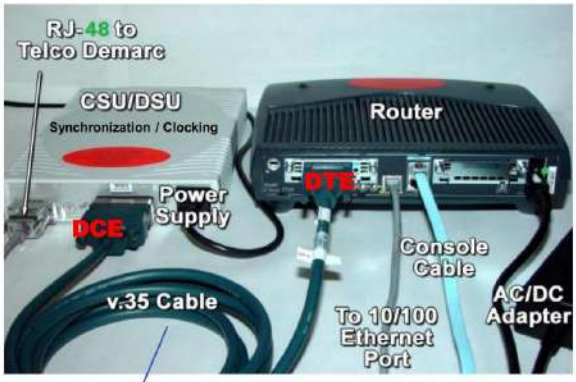
نکته طلایی: در شبکه‌ها management plane ، control plane(protocols) و (دیتای اصلی) data plane همگی از یک بستر عبور می‌کنند. معمولاً در شبکه‌ها نمیتوان DPو CP را از هم جدا کرد، ولی معمولاً سعی میکنند MP را از بقیه جدا کنند. به این حالت OOBM(Out of band managment) گویند. در صورت کنار هم بودن این سه مورد INband management گفته میشود. در بعضی از دستگاه‌ها portی به نام management موجود است که کلا cpu و... جدا دارند که در صورت attack و درگیر شدن resource بتواند مدیریت کند.

Router & Routing

WANs & IP Routing :

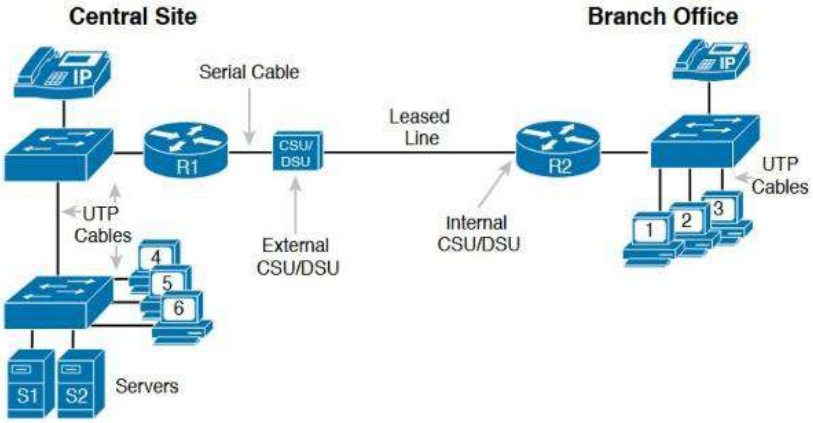


Router :



تاریخچه:

قـدیم: **Router**های قدیمی در صورت ارتباط با شبکه wan(سریال)، باید به دستگاهی به نام CSU(channel service unit) DSU/(Data service unit) با کابلی به نام V.35 متصل میشد (به قسمت متصل به روتر DTE(Data Terminal Equipment) و به قسمت متصل به DSU/CSU، DCE(Data Communications Equipment) گفته میشود). همچنین دستگاه DSU/CSU با کابل RJ-48 (کاملا مشابه با RJ45) به شبکه wan متصل می‌شود.



کار DSU/CSUها

Synchronization / Clocking بود. چون فاصله زیاد بوده، دیتا هنگامی که رد و بدل میشد، به تاخیر و delay دچار میشد. این دستگاه با در نظر گرفتن تاخیر، بین شبکه و provider این تاخیر را sync میکرده و زمانی را در نظر میگرفت.

که delayصورت نگیره و در صورت delayداشتن sync بشوند.

نکته: در روترهای امروز line cartها جایگزین DSU/CSU و کابل V.35 شده‌اند.

انواع ماژول‌های روتر :

جدید:

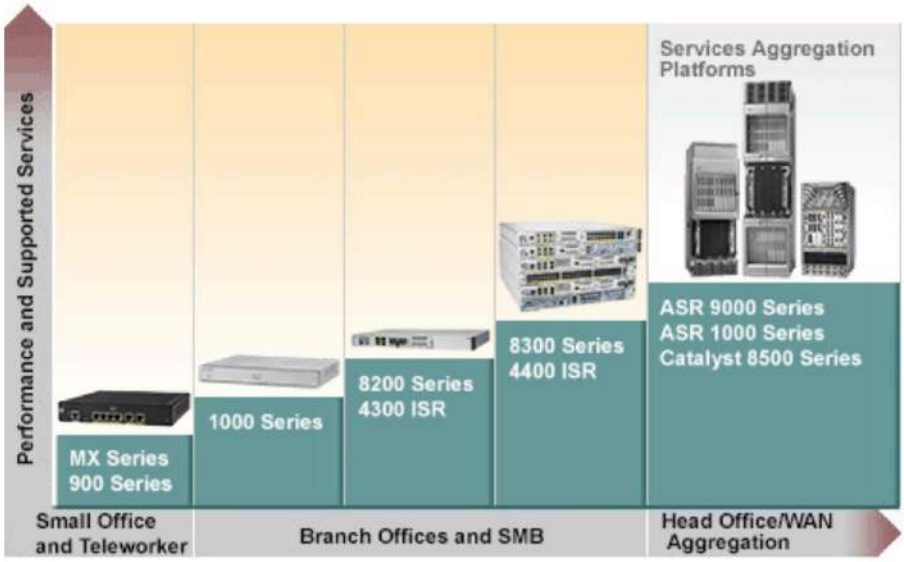
تفاوت روترهای سری (Integrated Services Router) ISR و سری (Aggregation Services Router) ASR :

روتر سری ISR در مکان‌هایی استفاده می‌شود که نیازمندی‌های آن شبکه کوچک و کم(Enterprise) هستند ، مانند مشاغل و دفاتر کوچک یا متوسط ، شعب شرکت‌ها و بانک‌ها و ... و این درحالی است که سری ASR برای نیاز شبکه های مقیاس بزرگ همانند شرکت‌های بسیار بزرگ یا ارائه دهندگان خدمات اینترنت و ... استفاده می‌شود.

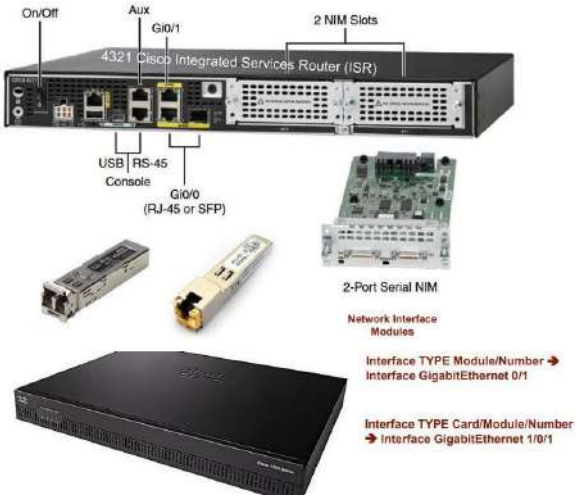
سری ISR در مکان هایی که معمولاً نیازمند سرویس و پهنای باند کم هستند ، استفاده می شود و چندین سری روتر ISRوجود دارد که توسط شرکت سیسکو معرفی شده است که شامل سری ۸۰۰ ISR ، سری ۱۹۰۰ ISR ، سری ISR ۲۹۰۰، سری ۳۹۰۰ ISR و سری ۴۰۰۰ ISR و ... هستند و سیستم عامل آن ها IOS نامیده می شود.

روتر سری ASR در مکان هایی که معمول نیازمند سرویس و پهنای باند بالا هستند ، استفاده می شود و چندین سری روتر ASR وجود دارد که توسط شرکت سیسکو معرفی شده است که شامل سری ۹۰۰ ASR ، سری ۱۰۰۰ ASR و سری ۵۰۰۰ ASR و ... هستند و سیستم عامل آن ها IOS XE نامیده می شود.

روترهای سری ASR	روترهای سری ISR	پارامترهای ساده مقایسه
طراحی شده جهت شبکه های بزرگ و ارائه دهنگان خدمات اینترنتی	طراحی شده جهت شبکه های کوچک و متوسط	موارد قابل استفاده
سیسکو IOS-XE و IOS-XR	سیسکو IOS	سیستم عامل مورد استفاده
عدم دسترسی به سیستم ابری (در بعضی مدل ها قابلیت دسترسی)	قابلیت دسترسی به سیستم ابری	دسترسی به سیستم ابری
قابلیت پردازش سرعت تا 100 گیگابیت بر ثانیه (متفاوت در برخی مدل ها)	قابلیت پردازش سرعت تا 10 گیگابیت بر ثانیه (متفاوت در برخی مدل ها)	قابلیت پردازش سرعت
تعداد پورت زیاد و قابلیت افزایش پورت (توسط ماژول)	تعداد پورت کم و قابلیت کم افزایش پورت ها (توسط ماژول)	تعداد پورت ها و قابلیت افزایش دادن پورت ها (توسط ماژول)



نکته: در دستگاه‌های ISR اگر بخواهیم کارتی را اضافه کنیم باید ابتدا آن را خاموش کنیم(hog plug نیستند) ولی سری‌های ASR و Chassis به این صورت نیستند. برای اضافه کردن ماژول خاموش و روشن بودن دستگاه اهمیتی ندارد.



شمایل یک روتر :

برای سری روترهایی که نمی‌توان کارت اضافه کرد(روترهای fix)، آدرس پورت دو قسمتی(قسمت اول: شماره لاین و قسمت دوم شماره پورت)، ولی برای سری روترهایی که میتوان کارت یا ماژول اضافه کرد(ASRها) آدرس پورت سه قسمتی(قسمت اول: شماره لاین، قسمت دوم: شماره کارت یا ماژول، قسمت سوم: شماره پورت) می‌باشد.

برقراری ارتباط از طریق پورت**Console** :

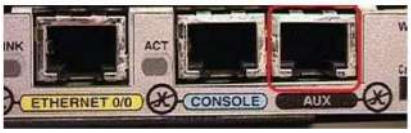
پورت کنسول زمانی مورد استفاده قرار می‌گیرد که شما نمی‌توانید تحت شبکه به روتر خود متصل شوید ، معمولاً زمانیکه برای اولین بار روتر خود را می‌خواهید پیکربندی کنید و در مدار شبکه قرار دهید از این پورت استفاده می‌کنید.

برقراری ارتباط از طریق پورت**Auxiliary** :

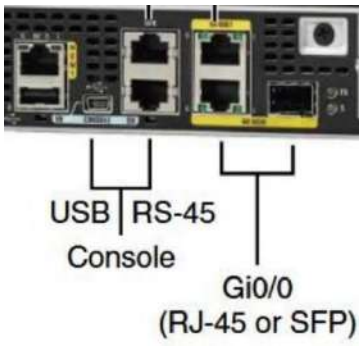
با استفاده از این پورت شما می توانید یک دستگاه مودم را به روتر خود وصل کنید و شخصی که قصد پیکربندی روتر را دارد نیز با استفاده از مودمی که در اختیار دارد به مودمی که به پورت **AUX** روتر متصل شده است ، وصل می‌شود.

و می‌توانند همانند حالتی که با استفاده از پورت کنسول شما روتر را پیکربندی می کنید از طریق مودم خود و از راه دور روتر را پیکربندی کند . در واقع این پورت برای برقراری ارتباط با روتر از راه دور اما بدون استفاده از بستر شبکه‌ای می باشد.

شاید برای شما هم با توجه به تصویر زیر جای تعجب باشد که چگونه کابل شبکه به مودم متصل می شود زیرا اندازه پورت **AUX** همانند کابل های شبکه است ، مودم با استفاده از یک **Connector** خاص یا بهتر بگوییم یک مبدل به روتر متصل می‌شود و کار می کند که شما احساس کنید با پورت کنسول روتر کار می‌کنید ، به تصویر زیر دقت کنید که یک پورت **AUX** را نشان می دهد که با استفاده از یک کابل **RJ** به روتر متصل شده است.



نکته ۱:

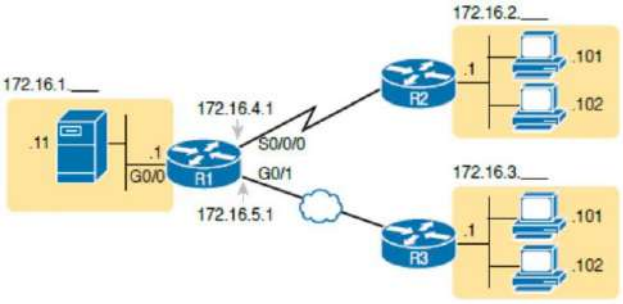


Media Typeروی پورت های روتر مشترک هستند که بصورت پیش فرض ٤٥ **RJ** می‌باشد.

جهت تغییر به فیبر باید از دستور **type-media sfp** استفاده کنیم و یا تغییر به ٤٥. **RJ**.

نکته ۲:

همه پورت‌های روتر پیشفرض **shut** است که با دستور **no shut** می‌توان آن‌ها را روشن کرد.




```
R1# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)# interface G0/0
R1(config-if)# ip address 172.16.1.1 255.255.255.0
R1(config-if)# no shutdown
R1(config-if)# interface S0/0/0
R1(config-if)# ip address 172.16.4.1 255.255.255.0
R1(config-if)# no shutdown
R1(config-if)# interface G0/1/0
R1(config-if)# ip address 172.16.5.1 255.255.255.0
R1(config-if)# no shutdown
R1(config-if)# ^Z
R1#
```

```
Router(config)#interface <>
Router(config-if)# [no] shutdown
Router(config-if)# ip address <IP> <MASK>
Router(config-if)# Duplex <>
Router(config-if)# Speed <>
Router(config-if)# Description <TXT>

Router# show ip interface brief
Router# show interface <>
Router# show protocols <>
```

-نحوه روشن و خاموش کردن پورت

-نحوه ip و mask دادن به port

-نحوه تنظیمات speed , duplex

-نحوه عوض کردن اسم روتر

-Showها

Router VS Switch :

■ User and Enable (privileged) mode

■ Entering and exiting configuration mode, using the configure terminal, end, and exit commands and the Ctrl+Z key sequence

■ Configuration of console, Telnet (vty), and enable secret passwords

■ Configuration of Secure Shell (SSH) encryption keys and username/password login credentials

■ Configuration of the hostname and interface description

■ Configuration of Ethernet interfaces that can negotiate speed using the speed and duplex commands

■ Configuration of an interface to be administratively disabled (shutdown) and administratively enabled (no shutdown)

■ CLI help, command editing

■The meaning and use of the startup-config (in NVRAM), running-config (in RAM)

■ The configuration of IP addresses differs in some ways, with switches using a VLAN interface and routers using an IP address configured on each working interface.

■ Many Cisco router models have an auxiliary (Aux) port, intended to be connected to an external modem and phone line to allow remote users to dial in to the router, and access the CLI, by making a phone call. Cisco switches do not have auxiliary ports.

■ Router IOS defaults to disallow both Telnet and SSH into the router because of the typical router default setting of transport input none in vty configuration mode.

■ Cisco Layer 2 switches support the show mac address-table command, while Cisco routers do not.

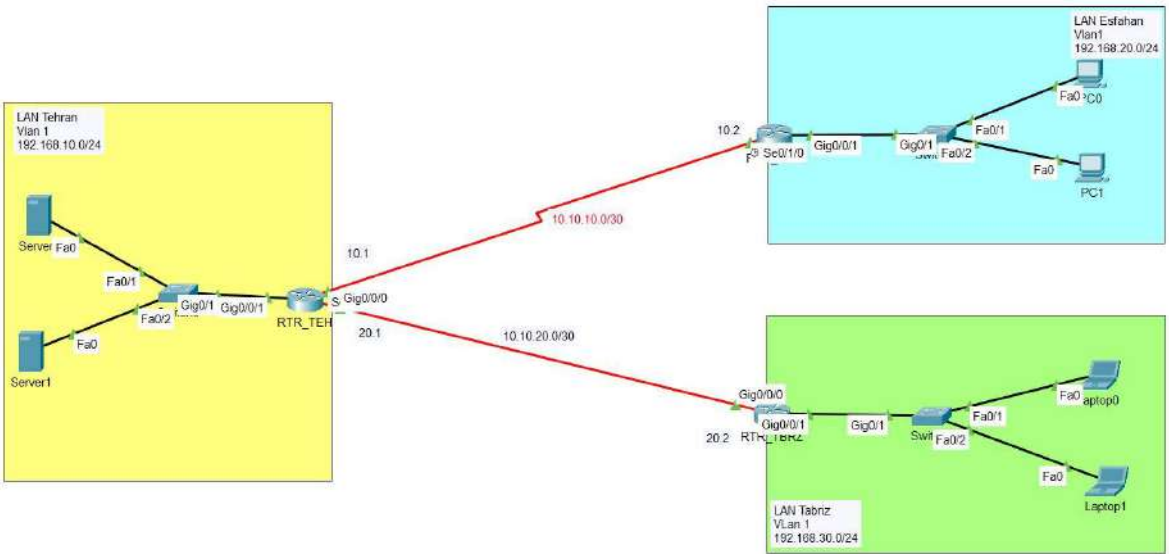
■ Cisco routers support the show ip route command, while Cisco Layer 2 switches do not.

■ Cisco Layer 2 switches use the show interfaces status command to list one line of output per interface (and routers do not), while routers use the show ip interface brief command to list similar information (but switches do not)

Route Concept :

هر روتر بصورت پیشفرضnetworkهایی که به آن متصل هستند را متوجه می‌شود و ipهایی که در همان networkروی هر دست روتر set شده را می‌داند. به عنوان مثال در شکل زیر روتر اصفهان از شبکه پشت خود و IPهایی که به دسته‌های خود متصل شده‌اند مطلع است. همچنین Getway PC1 روتر اصفهان را ping دارد ولی نمیتواند laptop1 یا server1 در شهرهای دیگر را ping کند.

نکته اینکه getway صرفاً برای ارتباط با شبکه‌های دیگه‌ست، در صورت ارتباط صرفا داخلی نیاز به getway نداریم.




```
RTR_TEH#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

     10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
C       10.10.10.0/30 is directly connected, Serial0/1/0
L       10.10.10.1/32 is directly connected, Serial0/1/0
C       10.10.20.0/30 is directly connected, GigabitEthernet0/0/0
L       10.10.20.1/32 is directly connected, GigabitEthernet0/0/0
     192.168.10.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.10.0/24 is directly connected, GigabitEthernet0/0/1
L       192.168.10.1/32 is directly connected, GigabitEthernet0/0/1
```

با دستور show ip route روتر teh، میگوید که شبکه 10.10.10.0/30را از ports0/1/0وشبکه 10.10.20.0/30 را از port g0/0/0 یاد گرفته‌ام (C=connected).

همچنین با Port و IP 10.10.10.1/32 s0/1/0 با شبکه esf و با Port و IP 10.10.20.1/32 g0/0/0 با شبکه TBZ ارتباط گرفته‌ام(local=L یعنی خود پورتهای روتر) .

از طریق port g0/0/1 شبکه 192.168.10.0/24 یاد گرفته‌ام و Ip adderss که با این شبکه ارتباط دارم 192.168.10.1/32 میباشد.

در شکل بالا اگر به end deviceها getway نداده باشیم، و بخواهیم از pc1 بسته‌های icmp به سمت server1 ارسال کنیم ، بسته ها در ابتدای کار دور ریخته میشوند و پیام Request timed out دریافت می‌شود، چون مسیری برای خود ندارد. همچنین در صورت تعریف getway برای end deviceها ، مجدد اگر بخواهیم از pc1 بسته‌های icmp به سمت server1 ارسال کنیم، بسته‌ها به دست getway میرسد ولی چون مسیری برای رسیدن به شبکه تهران و سپس به سرور۱ (با توجه به جدول routing tabel)تعریف نشده است از سمت getwayروتر اصفهان پیام Reply from 192.168.20.1: Destination host unreachable دریافت میشود.

برای ارتباط این دو باید در Routing table مسیری را تعریف کنیم.

Routing table or Routing information base (RIB) :

روترها برای مسیریابی از جداول روتینگ استفاده می‌کنند. #show ip route

تمامی Routerها و بطورکلی دستگاه‌هایی که می‌توانند وظیفه مسیریابی بسته‌های اطلاعاتی را در شبکه برعهده بگیرند و از پروتکل IPپشتیبانی می‌کنند دارای Routing Table می‌باشند.

جدول مسیریابی شامل اطلاعات ضروری برای ارسال بسته اطلاعاتی به سمت بهترین مسیر به مقصد آن است. هر بسته اطلاعاتی شامل مبدا و مقصد آن میباشد. وقتی بسته اطلاعاتی توسط گیرنده (که می‌تواند روتر باشد) دریافت می‌شود و آن بسته اطلاعاتی یا پکت را باز می‌کند و اگر مشاهده کرد که آدرس مقصد در جدول مسیریابی‌اش قرار دارد، آن را به شبکه مورد نظر هدایت می‌کند، اما اگر بسته اطلاعاتی مربوط به آن شبکه نبود، آن را به بهترین مسیر برای رسیدن آن بسته به مقصدش هدایت می‌کند. جدول مسیریابی همچنین دارای اطلاعاتی مثل Hop می‌باشد که روترهای بعدی را از رسیدن بسته به مقصد مطلع میسازند(**Hop** نشان دهنده تعداد روترهایی است که بسته اطلاعاتی برای رسیدن به مقصد نهایی‌اش باید از آنها عبور کند.).

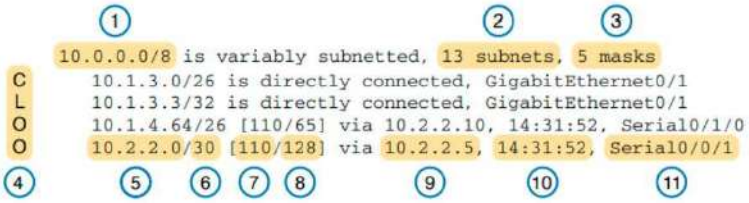
----- یک جدول مسیریابی ساده شامل اطلاعات زیر میباشد:

- Destination یا مقصد : که بیانگر آدرس IP مقصد بسته اطلاعاتی است.
- Next hop: آدرس IP روتری که بسته اطلاعاتی باید به آن فوروارد یا ارسال شود.
- Interface: آدرس IP اینترفیس یا پورتی که روتر پس از دریافت بسته اطلاعاتی به آن ارسال می‌کند تا به دست دیگر روتر (HOP)ها در شبکه برسد.
- Metric: متریک به زبان ساده پارامتری است که بهینه‌ترین Route برای هدایت بسته اطلاعاتی انتخاب می‌شود. هر چه میزان cost کمتر باشد آن بسته توسط Route مربوط به مقصد ارسال می‌شود.
- Subnet: که بیانگر آدرس زیر شبکه یا Subnet Mask ای است که به اینترفیس روتر تخصیص داده شده است.

نکته: جداول مسیریابی هم به صورت دستی static می‌توانند نگهداری و مدیریت شوند و هم بصورت dynamic(خودکار). جداول مسیریابی که در دستگاه‌های روتر به صورت static تعریف می‌شوند تنها توسط مدیر شبکه قابل تغییر است، اما در Dynamic routingجداول مسیریابی توسط پروتکل‌های مسیریابی که روی روترها راه‌اندازی و پیکربندی می‌شود ایجاد و نگهداری می‌شوند.

Router# show ip route

Item	Idea	Value in the Figure	Description
1	Classful network	10.0.0.0/8	The routing table is organized by classful network. This line is the heading line for classful network 10.0.0.0; it lists the default mask for Class A networks (/8).
2	Number of subnets	13 subnets	The number of routes for subnets of the classful network known to this router, from all sources, including local routes—the /32 routes that match each router interface IP address.
3	Number of masks	5 masks	The number of different masks used in all routes known to this router inside this classful network.
4	Legend code	C, L, O	A short code that identifies the source of the routing information. *O* is for OSPF, *D* for EIGRP, *C* for Connected, *S* for static, and *L* for local. (See Example 16-8 for a sample of the legend.)
5	Prefix (Subnet ID)	10.2.2.0	The subnet number of this particular route.
6	Prefix length (Mask)	/30	The prefix mask used with this subnet.



7	Administrative distance	110	If a router learns routes for the listed subnet from more than one source of routing information, the router uses the source with the lowest administrative distance (AD).
8	Metric	128	The metric for this route.
9	Next-hop router	10.2.2.5	For packets matching this route, the IP address of the next router to which the packet should be forwarded.
10	Timer	14:31:52	For OSPF and EIGRP routes, this is the time since the route was first learned.
11	Outgoing interface	Serial0/0/1	For packets matching this route, the interface out which the packet should be forwarded.

Static Routing :

Static Routing نوعی از مسیریابی است که دستگاه روتر با استفاده از Route هایی که در Routing Table آن دارد و بصورت دستی در روتر Learn یا تعریف شده است بسته اطلاعاتی را به سمت مقصد هدایت می‌کند. در بسیاری از موارد route staticها به صورت دستی توسط مدیر شبکه در Routing Table روتر پیکربندی می‌شوند. برخالف Dynamic routing مسیریابی استاتیک ثابت هستند و تا زمانیکه تغییری در ساختار فیزیکی شبکه (مانند اضافه شدن یا حذف شدن یک روتر از شبکه) بوجود نیامده است بدون تغییرات باقی می‌مانند.

– مزایای استفاده از Static routing :

a. از static routing می‌توان برای تعیین یک مسیر پیش‌فرض خروج بسته اطلاعاتی در صورت نبود آدرس مقصد آن بسته در Routing Tableروتر استفاده کرد. که به این مسیر پیشفرض Default Route نیز میگویند.
b. از static routing می‌توان در شبکه های کوچک که نیاز به یک یا دو Route دارند استفاده کرد.
c. از static routing می‌توان در مواقعی استفاده کرد که Dynamic routing در دسترس نباشد. به این معنی که می‌توان به عنوان یک Backup routing یا بهتر است بگوییم به عنوان یک مکمل در کنار Dynamic routing از آن استفاده کرد.
d. از static routing می‌توان به عنوان یک کمک برای انجام عملیات Routing از یک پروتکل مسیریابی به پروتکل مسیریابی دیگر بهره برد .(Routing Redistribution)
e. سربار روی CPU روتر وجود ندارد.
f. پهنای باند بلااستفاده بین پیوندها وجود ندارد.
g. فقط مدیر شبکه می تواند مسیرها را اضافه کند.

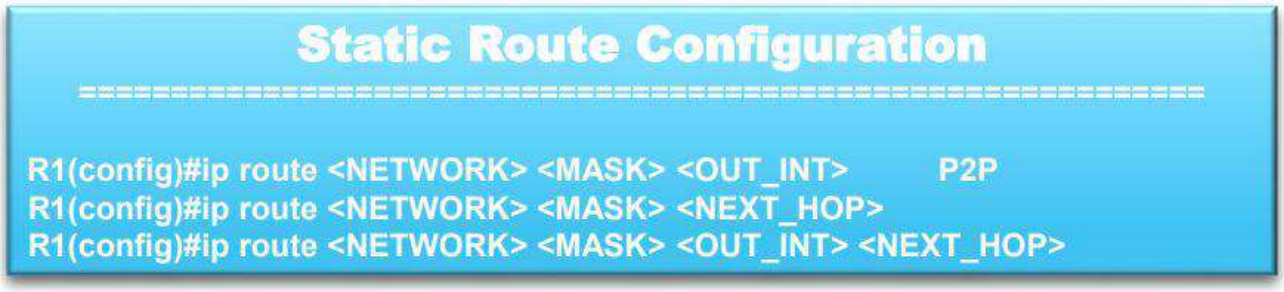
– معایب استفاده از Static routing :

a) Human errorدر بسیاری از موارد static route ها بصورت دستی در روتر تعریف می‌شود که این خود مستعد بروز اشتباهات فردی است. اگر تنها یک Route به اشتباه در روتر وارد شود عملیات مسیریابی در کل شبکه از کار می‌افتد.
b) Fault toleranceمسیریابی استاتیک از قابلیت Fault tolerance یا تحمل خرابی پشتیبانی نمی‌کند. به این معنی که اگر یکی از روترها در شبکه خراب شود یا تغییری در ساختار فیزیکی شبکه ایجاد شود دیگر ترافیک قابل مسیریابی در شبکه نمی‌شود. در نتیجه شبکه غیر قابل استفاده می‌شود و تا زمانی‌که مشکل برطرف نشده باشد کل شبکه فلج می‌شود.
c) Administrative distanceمسیرهای استاتیک یا Static route ها بر dynamic route ها تقدم دارند به این معنی که Static routeها ممکن است مانع از کارکرد مناسب پروتکل‌های مسیریابی یا Routing Protocolها شود که راهکار این مشکل تغییر دادن مقدار AD پروتکل مسیریابی است.
d) Administrative overheadمسیرهای استاتیک در هر روتر باید بصورت دستی پیکربندی شود. این پیکربندی‌ها مدت زمان زیادی صرف می‌کند در صورتیکه تعداد روترها در شبکه زیاد باشد. همچنین تغییر دادن این تنظیمات نیز می‌تواند مستعد اشتباهات زیادی باشد و در کل ناکارامد نباشد.
e) سرپرست باید نحوه اتصال هر روتر را بداند.

f) گزینه ایده آل برای شبکه های بزرگ نیست زیرا زمان زیادی را صرف می کند.

g) هرگاه لینک خراب شود تمام شبکه از کار می افتد که در شبکه های کوچک امکان پذیر نیست.

نحوه پیکربندی Static routing در روتر های سیسکو:



برای نوشتن یک دستور ip route ساده، تنها نیاز است که فرمان ip route را نوشته و ابتدا آدرس network و یا host مقصد (prefix) را وارد کنیم. در ادامه باید که mask subnet مربوط به مقصد (mask) را نوشت.

نکته: برای یک host خاص باید که mask subnet مربوط به آن را ۲۵۵.۲۵۵.۲۵۵.۲۵۵ بنویسیم که میتوان ننوشت.

در صورتی که subnet خود را برای ipای که host هر subnet بجز ۳۲/ وارد شود پیغام خطای Inconsistent% mask and address نشان داده خواهد شد . در گام بعدی میبایست ip address مربوط به روتر next-hop و یا interface که packet ها می‌توانند برای رسیدن به next-hop استفاده کنند نوشته شود.

دستور زیر یک مثال ساده از نوشتن Ip route می باشد:

Ip route 172.16.0.0 255.255.0.0 Ethernet 0

Ip route 172.16.0.0 255.255.0.0 192.168.1.2

اما یکی از تفاوت های اصلی این دو فرمان در نحوه نمایش route مورد نظر در routing table است.

نکته۱: برای مشاهده staticها route به تنهایی می‌توان از فرمان show ip route static استفاده کرد.

نکته۲: هنگامی که از exit interface (پورت خروجی از روتر)استفاده شود ، router به شکل Directly Connected در routing table نمایش داده می شود.

Prefix/mask is directly connected, exit-interface example: 172.16.0.0/24 is directly connected, Serial1/0

```
S       192.168.10.10/32 is directly connected, Serial0/1/0
```

اما زمانی که از next-hop استفاده شود، route مورد نظر در جدول routing به شکل زیر نمایش داده می شود که این قالب بهتر از قالب قبلی‌ست.

prefix [AD/metric]via ip-next-hop example : 15.1.1.0 [1/0] via 172.16.0.2

```
s       192.168.20.10/32 [1/0] via 10.10.10.2
```

علاوه بر نحوه نمایش ، استفاده از exit-interface وnext-hop در نوشتنstatic routes، تفاوت‌های محسوسی با یکدیگر دارند. هنگامی در نوشتن static route از next-hop استفاده شود، روتر به طور پیش‌فرض هر ٦٠ ثانیه یکبار next-hop را چک می‌کند و در صورت عدم دریافت جواب route را از routing table حذف می‌کند. برای تغییر این زمان می‌توان از فرمان زیر استفاده کرد:

Ip route static **adjust-time number**

در دستور فوق ، number عددی بین ١ تا ٦٠ ثانیه است. در صورت استفاده از exit-interface تنها زمانی route از routing table حذف می‌شود که exit-interface به نحوی fail شود. به طور مثال interface مربوطه shutdown شود.

همانطور که اشاره شد در نوشتن static route می‌توان هم به exit-interface مثل Serial0 و همnext-hop استفاده کرد. اما همیشه استفاده از next-hop به جای exit-interface پیشنهاد می‌شود . در صورتی کهstatic route به یک broadcast interface مثل Ethernetاشاره کند، route مربوط به آن تنها زمانی در routing table قرار می‌گیرد که interface مربوط به آن up باشد. به علاوه routerفرض می‌کند محدوده تمام ip هایی که از طریق static route اشاره شده به صورت directly connect هستند و روتر برای ارسال به هر destination که درstatic route به آن اشاره شده است یک ARP ارسال می‌کند. نمونه چنین route زیر می باشد:

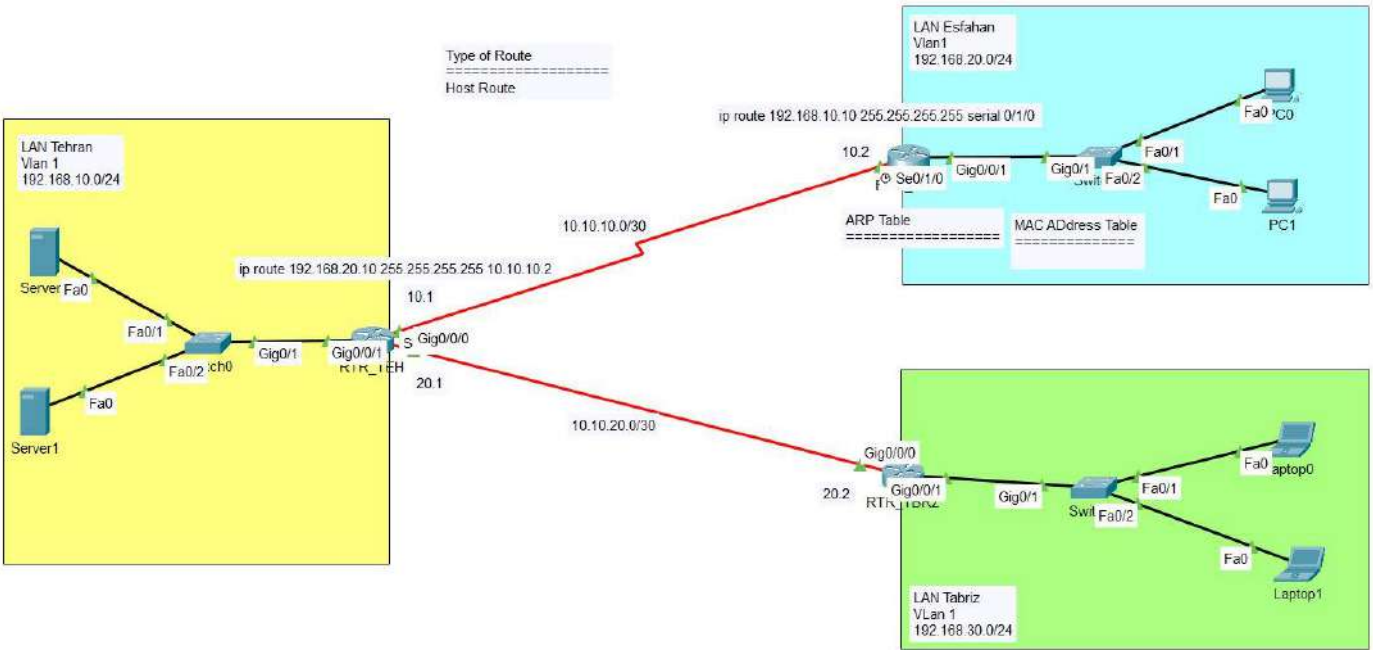
Ip route 0.0.0.0 0.0.0.0 Ethernet0

در صورتی که packet های زیادی برای دستیابی به destination های کثیری از این فرمان استفاده کنند ، CPU Utilizationروتر بسیار بالا می‌رود و یک جدول arp cache بسیار بزرگ ایجاد می‌شود که می‌تواند حتی روتر را overloadکند. اضافه کردن numerical addressو به بیان واضح تر IP مربوط به next-hop دو مزیت عمده دارد: یکی اینکه از ارسال arpها جلوگیری می‌کند و دوم اینکه در صورت down شدن آنinterface ، از طریق route recursive سعی در پیدا کردن route دسترسی به آن ip می‌کند. برای نوشتن این نوع route می‌بایست که interfaceو next-hop هر دو نوشته شوند. مثال آن در زیر نوشته شده است:

Ip route 0.0.0.0 0.0.0.0 **Ethernet0 172.16.0.2**

**استفاده از exit-interface به تنهایی فقط زمانی پیشنهاد می‌شود که نوع interface خروجیpoint-to-point باشد. یکی از مرسوم ترین interface point-to-point ها serial interface ها می‌باشد.

مثال: Host route – مسیریابی تک Host (مسیریابی PC0 به Srv0)



به روتر تهران گفته شد که اگر میخواهی اطلاعاتی را از deviceی در شبکه تهران به host PC0 با IP 192.168.20.10 255.255.255.255 برسانی باید به (in)interface se0/1/0 با IP 10.10.10.2 بسپاری.

```
S       192.168.20.10/32 [1/0] via 10.10.10.2
```

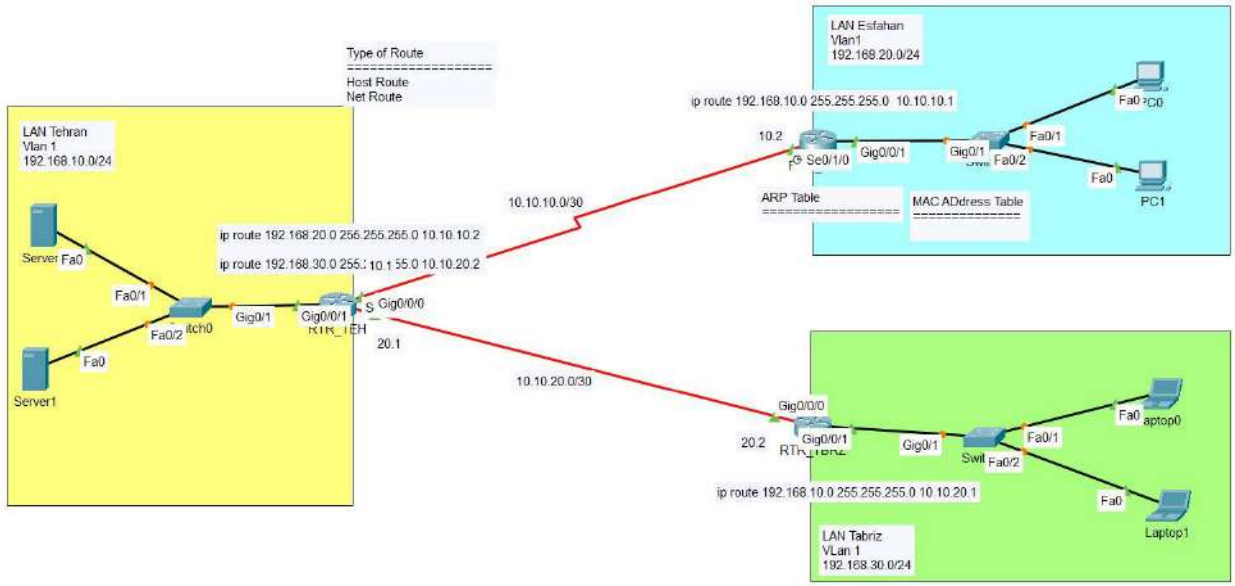
از طرفی هم به روتر اصفهان گفته شد اگر میخواهی اطلاعاتی را از deviceی در شبکه اصفهان به host srv0 با IP 192.168.10.10 255.255.255.255 برسانی باید به (out)se0/1/0 بسپاری. (به این صورت هم میشود نوشت: باید به (in)interface se0/1/0 با IP 10.10.10.1 بسپاری.)

```
S       192.168.10.10/32 is directly connected, Serial0/1/0
```

نکته: برای تشکیل جدول روتینگ و برقراری ارتباط، باید دو طرف کانفیگ شوند.

نکته: در این سناریو چون مقصد تک host است، subnet mask 255.255.255.255 میباشد. یعنی این مسیریابی فقط مختص این تک host است.

مثال: Net route – مسیریابی کل شبکه اصفهان به تهران و بالعکس – مسیریابی کل شبکه تبریز به تهران و بالعکس



به روتر اصفهان گفته شد اگر میخواهی اطلاعاتی را از deviceی در شبکه اصفهان به شبکه تهران با IP 192.168.10.0 255.255.255.0 برسانی(این subnet یعنی حتما سه octed اول برابر باشد) باید به interface se0/1/0(in) با IP 10.10.10.1 بسپاری.

ip route 192.168.10.0 255.255.255.0 10.10.10.1

```
S    192.168.10.0/24 [1/0] via 10.10.10.1
```

به روتر تبریز گفته شد اگر میخواهی اطلاعاتی را از deviceی در شبکه تبریز به شبکه تهران با IP 192.168.10.0 255.255.255.0 برسانی باید به interface gi0/0/0(in) با IP 10.10.20.1 بسپاری.

ip route 192.168.10.0 255.255.255.0 10.10.20.1

```
S    192.168.10.0/24 [1/0] via 10.10.20.1
```

به روتر تهران گفته شد که اگر میخواهی اطلاعاتی را از deviceی در شبکه تهران به شبکه اصفهان با IP 192.168.20.0 255.255.255.0 برسانی باید به interface se0/1/0(in) با IP 10.10.10.2 بسپاری.

ip route 192.168.20.0 255.255.255.0 10.10.10.2

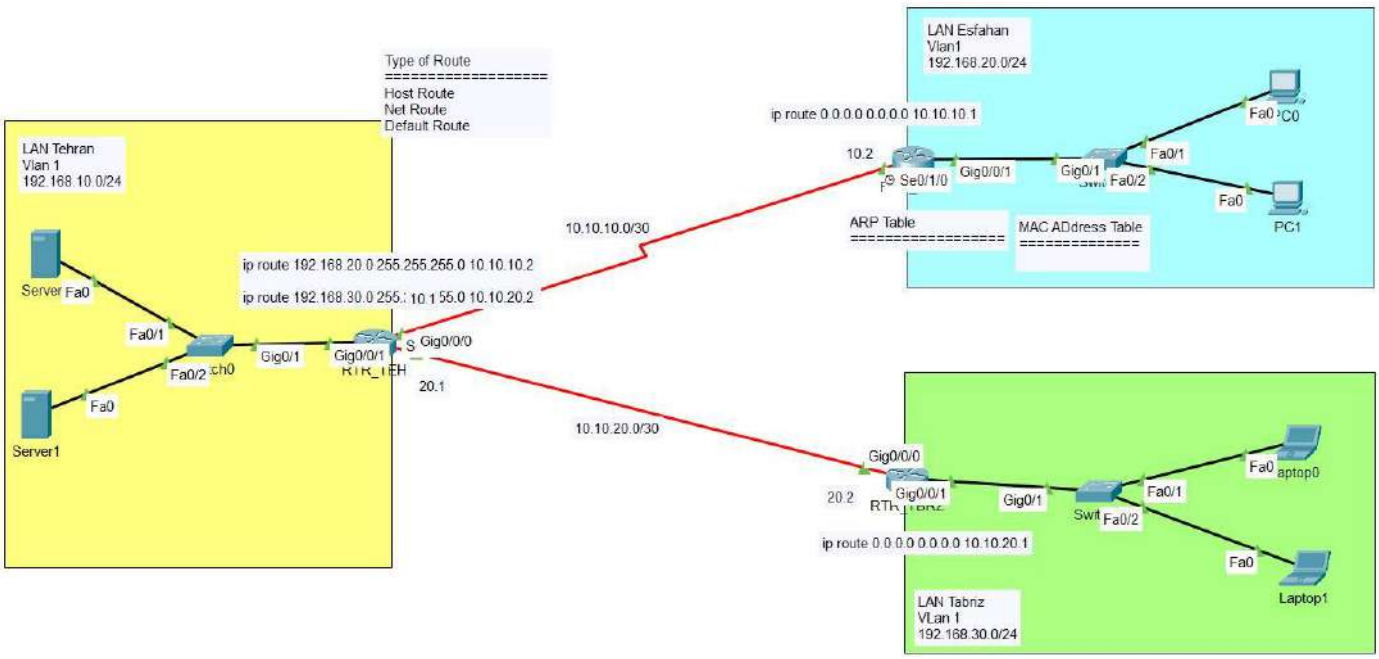
```
S    192.168.20.0/24 [1/0] via 10.10.10.2
```

همچنین به روتر تهران گفته شد که اگر میخواهی اطلاعاتی را از deviceی در شبکه تهران به شبکه تبریز با IP 192.168.30.0 255.255.255.0 برسانی باید به interface gi0/0/1(in) با IP 10.10.20.2 بسپاری.

ip route 192.168.30.0 255.255.255.0 10.10.20.2

```
S    192.168.30.0/24 [1/0] via 10.10.20.2
```

مثال: **Default route** – مسیریابی غیر مستقیم کل شبکه تبریز به اصفهان و بالعکس – سپردن مسیر به روتری که مسیر هدف مارا بلد است



ابتدا همه دستورات روتینگ روتیر اصفهان و تبریز را حذف می‌کنیم (با قرار دادن no قبل دستور روتینگ). در ادامه :

به روتر اصفهان گفته شد که اگر میخواهی اطلاعاتی را از deviceی در شبکه اصفهان به شبکه تبریز برسانی باید به interface (in)se0/1/0 با IP 10.10.10.1 (تهران) بسپاری. که برسونه تبریز(هر کی با هر subnetی: 0.0.0.0 0.0.0.0)

ip route 0.0.0.0 0.0.0.0 10.10.10.1

```
S*   0.0.0.0/0 [1/0] via 10.10.10.1
```

همچنین به روتر تبریز گفته شد که اگر میخواهی اطلاعاتی را از deviceی در شبکه تبریز به شبکه اصفهان برسانی باید به (in)interface gi0/0/0 با IP 10.10.20.1 (تهران) بسپاری. که برسونه به اصفهان

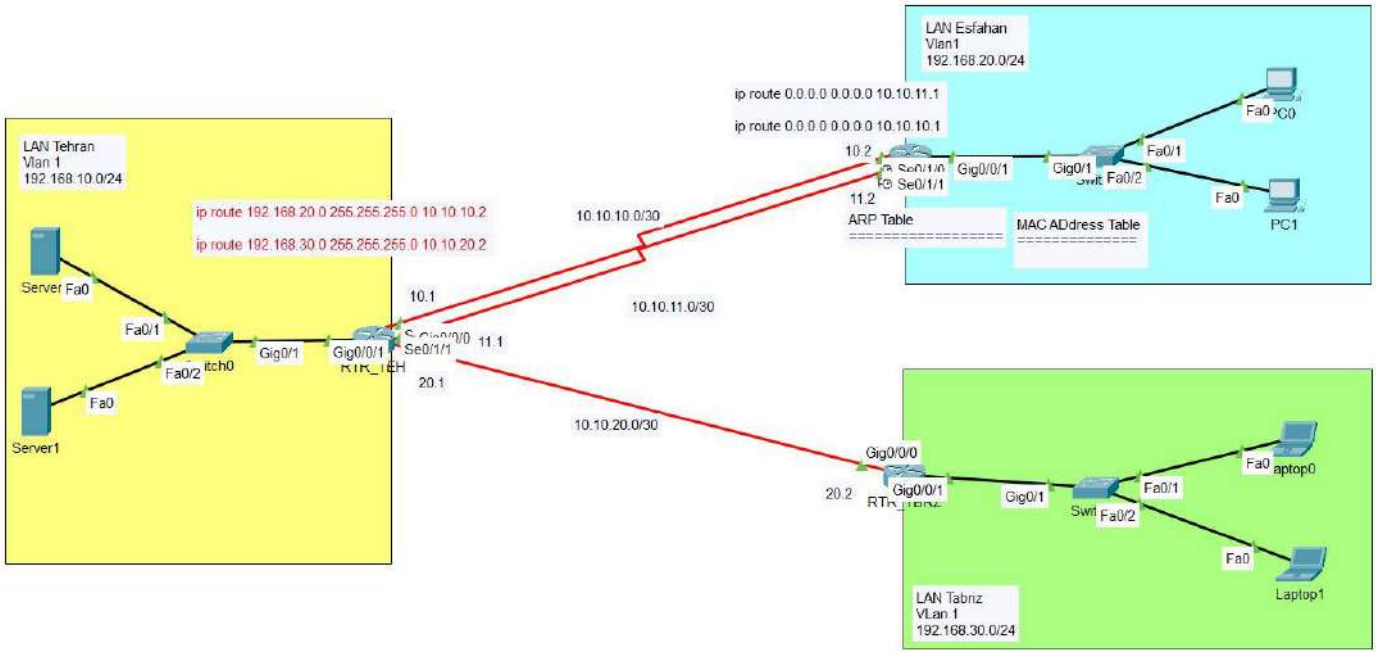
ip route 0.0.0.0 0.0.0.0 10.10.20.1

```
S*   0.0.0.0/0 [1/0] via 10.10.20.1
```

مثال: ECMP (Equal-Cost Multi-Path) / یعنی به ازای یک مقصد یکسان چندین مسیر با cost یکسان وجود داشته باشد، تمام این مسیرها کشف شده و بین آن ها برای ارسال ترافیک load sharing صورت گیرد. ECMP معمولاً برای افزایش پهنای باند و redundancy صورت میگیرد.

پس در این روش، هر forwarder (روتر) به ازای هر مقصد معینی چندین next-hop داشته و از روش‌هایی به منظور مشخص کردن آن که از کدام next-hop برای ارسال یک پکت مشخص باید استفاده شود، استفاده مینماید. ساده ترین روش

برای انجام این عمل آن است که مثلاً پکت اول از لینک اول، پکت دوم از لینک دوم و الی آخر ارسال شوند. اصطلاحاً به این روش per -packet load balancing گفته می شود.

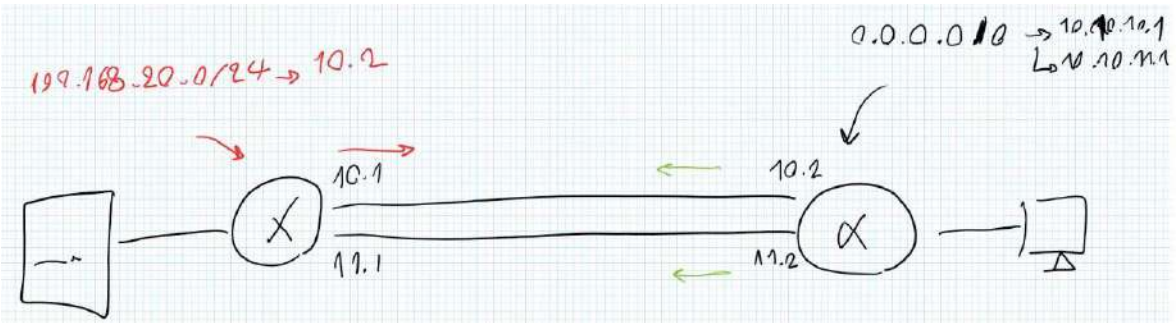


به روتر esf گفته شد برای ارسال هر بسته از شبکه خود دو مسیر داری(10.1 و 11.1). در این حالت یک packet از لینک اول و یک packet از لینک دوم و الی آخر ارسال میشود. به این حالت ECMP گفته میشود.

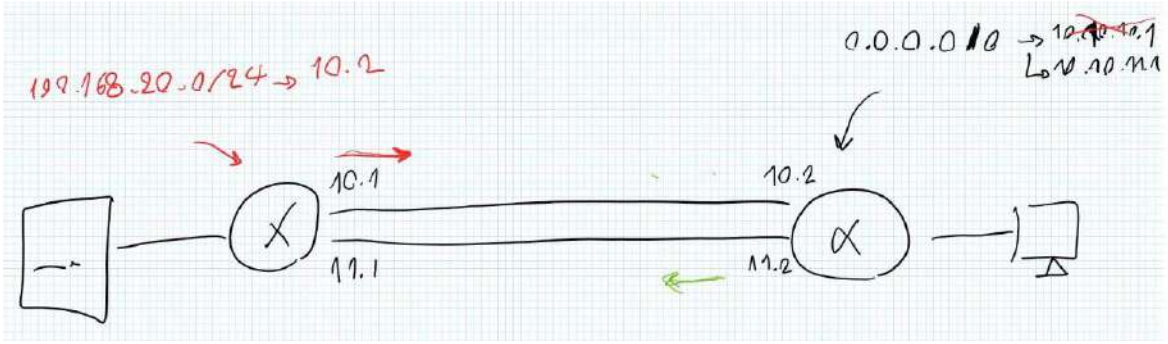
```
S*    0.0.0.0/0 [1/0] via 10.10.11.1
                [1/0] via 10.10.10.1
```

در این حالت در صورت قطع شدن interface ارتباط همچنان برقرار است و از لینک دوم استفاده میکند. در صورت shut شدن، مسیر از جدول روتینگ حذف خواهد شد.

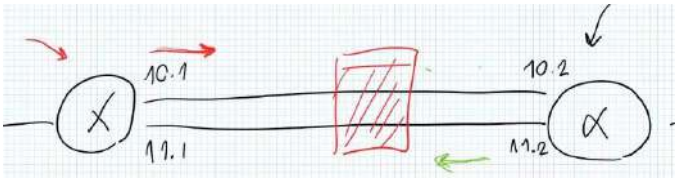
نکته اینه ما فقط مسیر esf به teh را دو مسیر تعریف کردیم. به همین خاطر همچنان برای برگشت از مسیر 10.10.10.2 (لینک ابتدایی) برمیگردد. به این صورت:

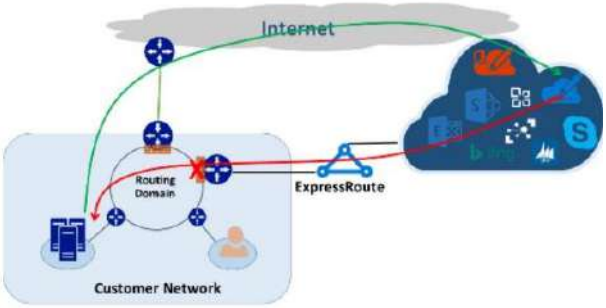


حالت مسیر نامتقارن (Asymetric Routing) - یعنی مسیر رفت و برگشت یکسان نباشد. به این صورت:



توجه:در Asymmetric زمانی به مشکل میخوریم که در بین روتر ها فایروال یا cash server داشته باشیم. ارتباطی برقرار میشه که اگر درخواستی از روی یک ip و پورت رفت جوابش هم جوابش هم از روی همون برگرده، در غیر این صورت اگر ارتباط یک طرفه بیاد سمتش فکر میکنه attack و آن بسته را drop میکنه.





نکته: به حالتی که مسیر رفت و برگشت یکسان است symmetric routing گفته میشود .

*نکته: شروط Routing Table

1. Next Hop Reachability
2. Longest Prefix Match
3. Administrative Distance
4. Metric

1-روشن و برقرار بودن interface connected= next hop

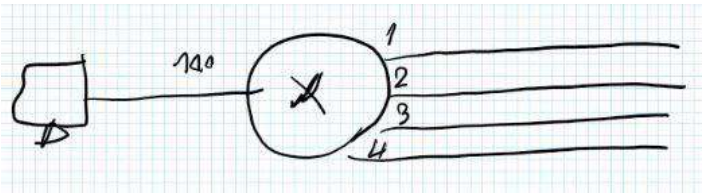
2- LPM=**longest Prefix match** :

Route ی اولویت دارد که انطباق بیشتری با Dst Ip (بیت به بیت)که در بسته موجود است داشته باشد.

مثال:

Routing Table

192.0.0.0/8	E1
192.1.0.0/16	E2
192.1.1.0/24	E3
0.0.0.0/0	E4



– اگر بسته‌ای با Dst IP 192.1.1.100به روتر برسد، بسته از کدام مسیر عبور میکند؟ E3 چون E4 در octetاول ، E1 در octed2 ، E2 هم در octed3 کنار میروند.

– اگر بسته‌ای با Dst IP 192.168.1.100به روتر برسد، بسته از کدام مسیر عبور میکند؟E1 چون E2 میگوید که حتما باید دو octed اولش192.1 و E3میگوید که حتما باید سه octed اولش 192.1.1 باشد که Dst IP به این صورت نیست (192.168). پس E2و E3 کنار میروند.

– اگر بسته‌ای با Dst IP 193.1.1.100به روتر برسد، بسته از کدام مسیر عبور میکند؟ E4 چون این مسیر میگوید که اگر مسیری برای Dst IP نداشتید(Eهای 1,2,3 هیچکدام انطباق ندارند) ، از مسیر من(هر چی = 0.0.0.0) عبور دهید.

3-Administrative Distance:

در Routing table داخل براکت دو عدد وجود دارد که قسمت اول آن Administrative Distance هست.

```
C       192.168.20.0/24 is directly connected, GigabitEthernet0/0/1
L       192.168.20.1/32 is directly connected, GigabitEthernet0/0/1
S*   0.0.0.0/0 [1/0] via 10.10.10.1
                [1/0] via 10.10.11.1
```

بیشتر پروتکل های مسیریابی برای خود یک ساختار Metric و الگوریتم خاص دارند که شاید اصلاً با پروتکل‌های دیگر تناسبی نداشته باشد. در شبکه‌ای که از چندین پروتکل مسیریابی مختلف استفاده می‌شود، تبادل اطلاعات در خصوص مسیرهای موجود و همچنین قابلیت تشخیص بهترین مسیر از بین چندین پروتکل مسیریابی موجود مهمترین اولویت است.

Administrative Distance قابلیتی است که روترها با استفاده از آن می‌توانند بهترین مسیر در میان دو یا چندین شبکه‌ای که از پروتکل های مسیریابی مختلف استفاده می‌کنند برای رسیدن به یک مقصد مشخص را بیابند.

بعد از Reachable و up بودن اینترفیس Next hop ،و انتخاب Specific Route تر (LPM)، حالا اگر چند تاroute به ازای مقصد باقی مانده بود، routeی ارجح‌تر می‌باشد که Administrative Distance کمتری داشته باشد.Route هایی که بصورت استاتیک استفاده می کنیم بصورت پیشفرض یک هستند(به صورت دستی قابل تغییر هستند)، connected بصورت پیشفرض صفر است. اگر در نهایت چندین Route ماند که Distance Administrative آنها برابر شد، ECMP شکل میگیرد.

نکته: به همین دلیل اگر static route خواستیم بزنیم interface انتخاب کنیم و connected شودAdministrative Distance صفر می شود و میتواند loop ایجاد کند بنابراین اصوال next hop استفاده می کنیم.

پارامترAdministrative Distance اولین شرطی است که یک Router زمانی که دو پروتکل مسیریابی مختلف، اطلاعات مسیریابی مربوط به یک مقصد مشخص را ارائه می‌کنند، برای پیدا کردن بهترین مسیر از بین این دو یا چند پروتکل مسیریابی بررسی می‌کند. در واقع معیاری برای درست بودن و موثق بودن مبدا اطلاعات مسیریابی می‌باشد.

نکته مهم در Administrative Distance این است که Local Significance است، یعنی اهمیت و معنی آن فقط روی همان روتر معتبر است و با Update شدن Routing به روترهای دیگر Advertise نمی شود.

هر چقدر مقدار یا Value ای که به پروتکل در Administrative Distance داده می شود کمتر باشد به معنی این است که پروتکل مورد نظر قابل اعتمادتر است، برای مثال اگر یک روتر یک Route به یک شبکه مشخص دریافت کند که در آن هم پروتکل OSPF با Administrative Distanceپیشفرض ۱۱۰ وجود داشته باشد و هم IGRP با Administrative Distance پیشفرض ۱۰۰ ، روتر مورد نظر ما مسیری که IGRP به آن معرفی می‌کند را به دلیل Reliabilityبیشتر انتخاب می‌کند و این بدین معناست که روتر نسخه Routeمربوط به IGRP را درRouting Table خود اضافه می کند.

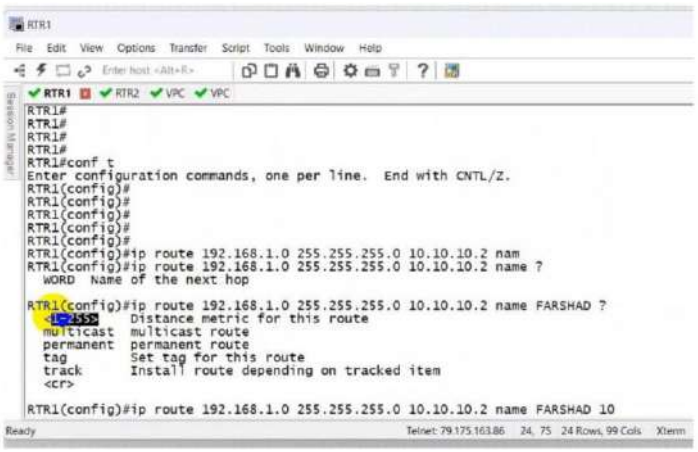
اگر به هر دلیلی شما موفق به دریافت اطلاعات مربوط به IGRP نشدید (مثلا روتر در آن لحظه خاموش شده باشد)، نرم افزار بصورت خودکار اطلاعات مربوط به مسیرهایی که OSPF ایجاد کرده است را استفاده می‌کند تا زمانیکه اطلاعات IGRP مجددا در دسترس باشند.

مقادیری که به عنوان Value به پروتکل‌های مختلف بصورت پیشفرض داده می‌شود از عدد ۰ تا ۲۵۵ متغیر می‌باشد. عدد ۰ بالاترین اولویت و به معنای بالاترین Reliability و عدد ۲۵۵ به معنای پایین‌ترین حد Reliability می باشد. در Static Route سعی می کنیم زیر ۸۰ انتخاب کنیم چون در Dynamic Route مقدار value از ۹۰ به بالا می باشد.

Route Source	Default Distance Values
Connected interface	0
Static route	1
Enhanced Interior Gateway Routing Protocol (EIGRP) summary route	5
External Border Gateway Protocol (BGP)	20
Internal EIGRP	90
IGRP	100
OSPF	110
Intermediate System-to-Intermediate System (IS-IS)	115
Routing Information Protocol (RIP)	120
Exterior Gateway Protocol (EGP)	140
On Demand Routing (ODR)	160
External EIGRP	170
Internal BGP	200
Unknown*	255

جدول روبرو لیست مقادیر AD پیشفرض پروتکل‌هایی است که سیسکو از آنها پشتیبانی می کند:

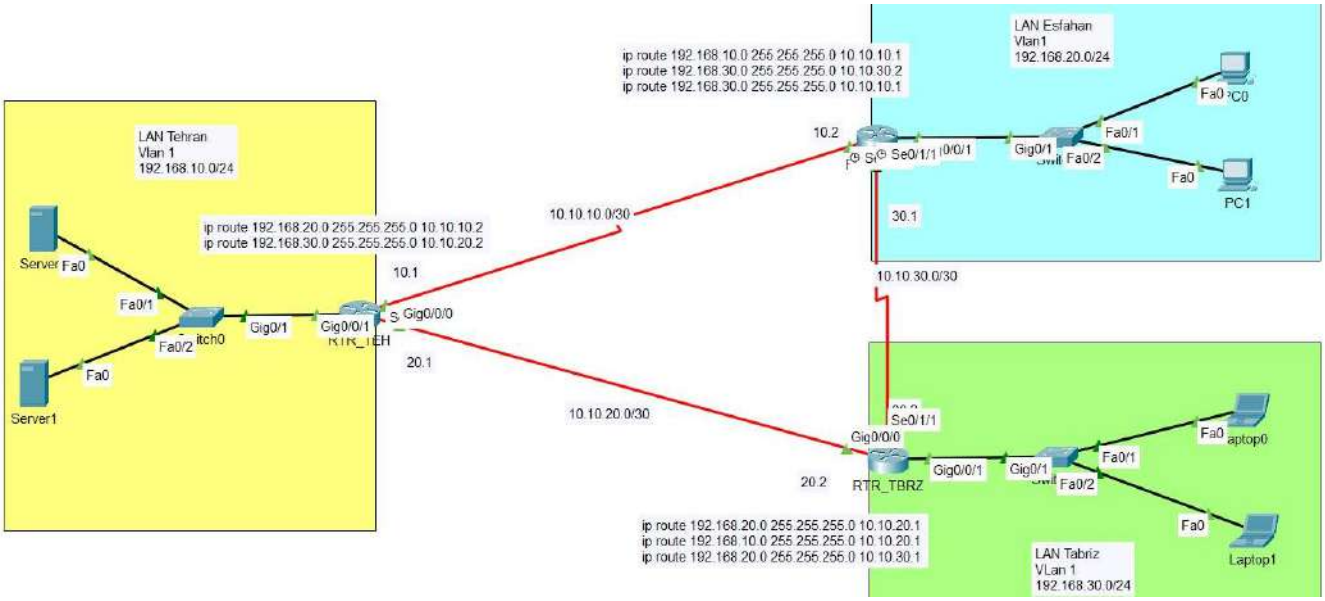
تغییر **Administrative Distance** بصورت دستی:



نکته: اگر به اشتباه روی روتری آدرس شبکه پشت خودش را مسیری تنظیم کنیم، همچنان ping داریم، چرا؟ چون مسیر با اولویت‌تری در جدول روتینگ ما موجود است (C table). یعنی چون AD کانکتد صفر است و مسیری که تنظیم کردیم AD آن یک است. به همین خاطر اولویت connected بهتر است.

Metric-4:

مثال: ADN – مسیریابی غیر مستقیم کل شبکه تبریز به اصفهان و بالعکس – سپردن مسیر به روتری که مسیر هدف مارا بلد است



با توجه به کانفیگ روی شکل، شبکه اصفهان از طریق 10.1 با تهران و تبریز ، همچنین از طریق 30.2 نیز با تبریز ارتباط دارد.

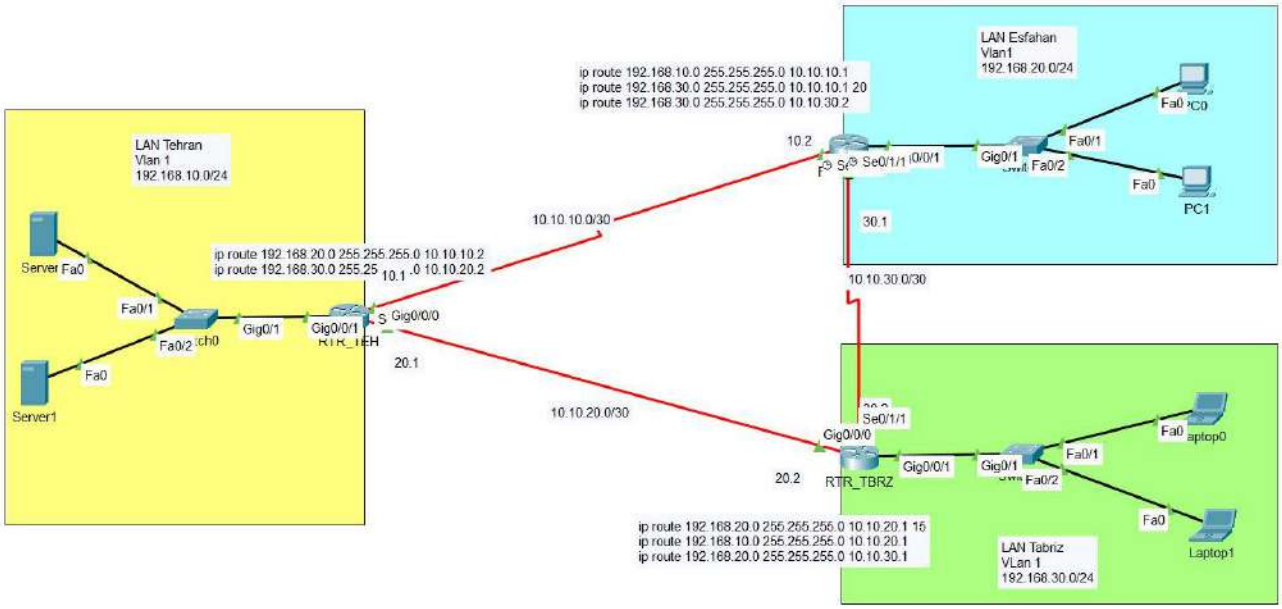
شبکه تبریز از طریق 30.1 و 20.1 با اصفهان و از طریق 20.1 با تهران ارتباط دارد.

در کل تبریز و اصفهان از دوست مسیر طبق مکانیزمECMP با هم ارتباط دارند (چون AD یکسانی دارند. هر دو یک هستند.)

حال اگر بخواهیم اولویت یک مسیر را نسبت به مسیر دوم تغییر دهیم، باید Administrative Distance را تغییر دهیم. اگر Administrative Distance یک مسیر را بیشتر کنیم ، مسیر دوم اولویت بیشتری پیدا میکند چون AD کمتری دارد.

برای اینکار در انتهای آدرس روتی که میخواهیم اولویت کمتری داشته باشد، عددی بیشتر از یک را درج میکنیم. به صورت زیر:

تفسیر مسیر اصفهان به تبریز: این بدان معناست که به طور کل این ارتباط دو مسیر دارد ولی ارتباط از 30.2 اولویت بیشتری نسبت به 10.1دارد که در صورت قطع این ارتباط، مسیر 10.1جایگزین 30.2 میشود.



نکته: Route اولویت دوم درRouing table تا زمانیکه اولویت اول از دسترس خارج نشود نشان داده نمی‌شود و فقط اولویت اول موجود است.

```
S    192.168.30.0/24 [1/0] via 10.10.30.2
```

نکته: به این حالت **Floating Static Route** گفته می‌شود.

یعنی یک Route را شناور بذاریم، میتواند چند Static Route با ADهای متفاوت نوشت، یا می‌توان یک یا چند Static Route به همراه یک Dynamic Route بنویسیم. در داینامیک Administrative Distance ها متفاوت است و اولویت‌هایش از ۹۰ به بالا شروع می‌شود.

برای مثال ، در یک شبکه ، یک آپلینک اینترنت و یک لینک بکاپ وجود دارد ، میخواهیم ، در صورت قطع ارتباط اصلی ، ارتباط از طریق لینک بکاپ برقرار شود.

*** یکی از سناریوهای پرکاربرد در ایران ، بدین ترتیب است که اکثر ISPها ، علاوه بر ارتباط رادیویی با uplink خود که مثلا میتواند ماکروویو باشد ، یک ارتباط اینترنتی نیز بر روی فیبر هم با ISP بالادست خود ، یا مخابرات دارند ، خب البته که ماکروویو ارجح است ، چون تاخیر کمتری داشته و همچنین به ISP ، بار اضافی over head تحمیل نمی‌کند، ولی در هر صورت ، اگر این لینک down شود ، می‌بایست ترافیک به شکل خودکار از روی لینک فیبر و یا همان اینترنت ، یا هر لینک دوم دیگری ، عبور کند ، البته هم برای send این کار را کرد و هم receive که می‌تواند BGP peering باشد .

نکته۱ : اگر کلمه permanent یا persistent را به انتهای Route اضافه کنیم، باعث می‌شود route ای که شما اضافه می کنید در Routing tableروتر حتی بعد از خاموش و روشن شدن یا دچار مشکل شدن روتر باقی بماند. می‌دانیم که روت‌ها بر اثر خاموش و روشن شدن از بین می‌روند.

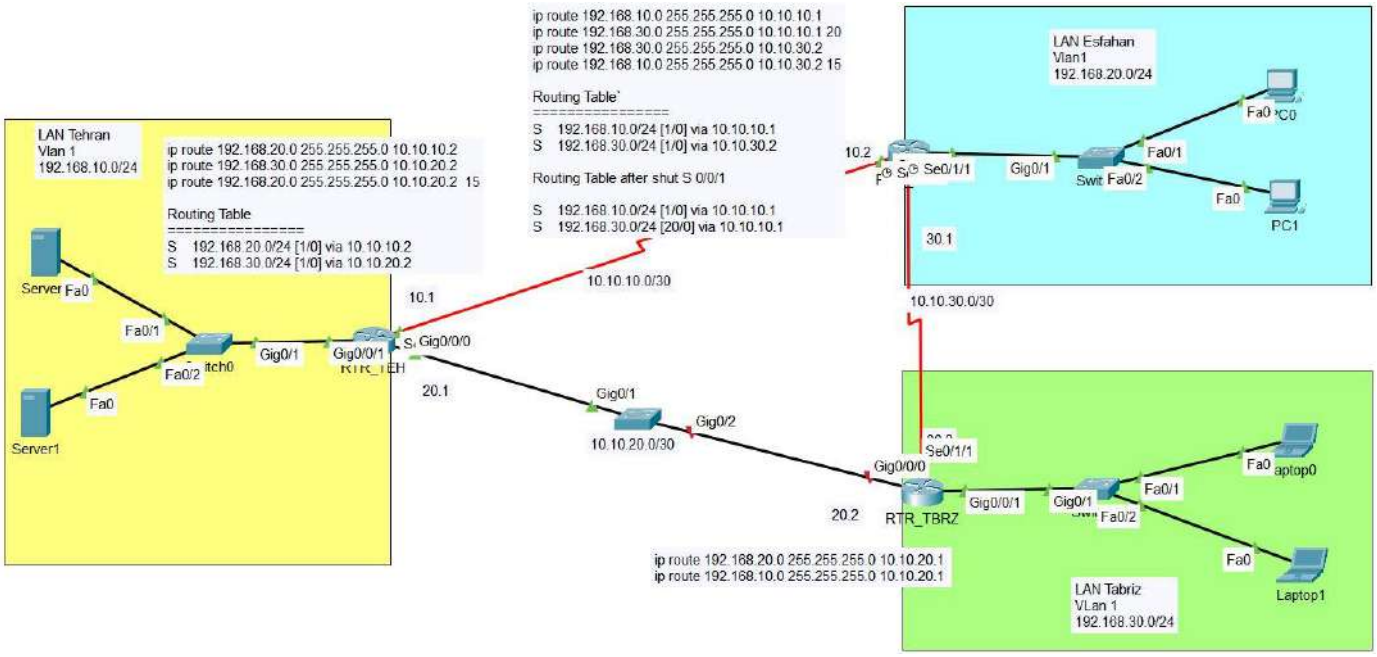
```
ip route 10.1.1.1 255.255.255.255 serial0 permanent
```

نکته۲ : با کمک کلمه name می‌توان برای route یک نام تعیین کرد. استفاده از نام تعیین شده کمک می‌کند تا زمانیکه routeهای زیادی داریم، به راحتی آن‌را در configuration file پیدا کنیم. مثال زیر کاربرد این فرمان را نشان می‌دهد:

```
ip route 172.0.0.0 255.0.0.0 10.0.0.1 name Tehran2Shiraz
show running-config | in Tehran2Shiraz          <-  (eve)
```

نکته۳: Static Route نسبت به تغییرات شبکه پشت خود مطلع می‌شود ولی نسبت به تغییرات شبکه های دیگر خیر(indirect topology change) ! که این مسئله ایراد مهم این روش است. روتر به طور کلی فقط direct change topology را متوجه میشود.

مثال: Static Route **Indirect Topology Change**



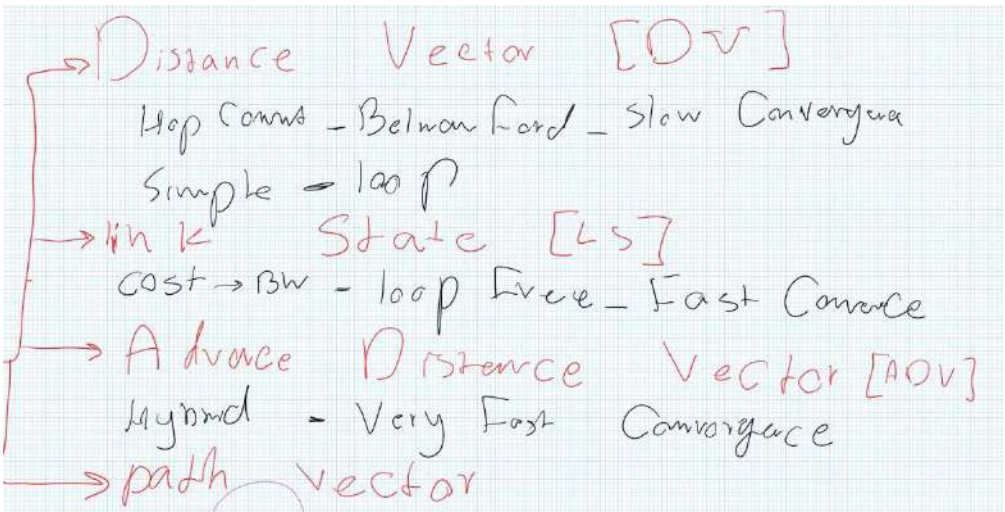
در مثال بالا روت‌های ارتباط بین تهران و اصفهان نوشته شده است(به ازای هر روتر، دو مسیر با اولویت های متفاوت). همانطور که نوشته شده است، در جدول روتینگ فقط اولویت اصلی تا قبل از حذف لینک ارتباطی نمایش داده می‌شود.

روتر اصفهان هنگام قطع راه های ارتباطی متصل به خود را متوجه میشود و به سرعت نسبت به اصلاح جدول روتینگ (جایگزین کردن روت با اولویت دوم با اولویت اول(چون مسیر از دسترس خارج شده است)). (direct)

اما در صورتیکه لینک بین روتر تبریز و سوئیچ قطع شود، روتر اصفهان و حتی روتر تهران متوجه نخواهند شد و این مسیر را از Routing table خود حذف نمی‌کنند(indirect) .

Dynamic Routing :

انواع پروتکل مسیریابی بر اساس عملکرد :



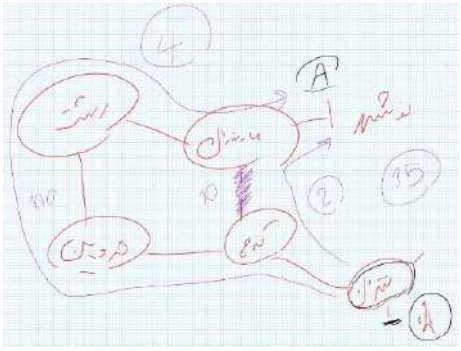
پروتکل های Distance Vector (DV) :

پروتکل‌های Distance Vector با استفاده از دو فاکتور مسافت (Distance) و جهت (Vector) کار روتینگ را انجام می‌دهند. پروتکل‌های Distance Vector جدول مسیریابی خود را برای تمامی همسایگانی که به طور مستقیم به آن‌ها متصل هستند، در فواصل زمانی مشخص و با پهنای باند بالایی انتشار می‌دهند و به آرامی همگرا می‌شوند. هنگامی که یک مسیر از دسترس خارج می شود، تمام روترهای شبکه باید جدول های مسیر یابی خود را بر اساس اطلاعات جدید به روز کنند.

متریک(معیار بررسی بهترین مسیر) آن Hop Count (تعداد روترهای مسیر) است ومشکل این پروتکل‌ها این است که هر روتر مجبور است که اطلاعات جدیدی را به همسایگان خود اطلاع دهد، در نتیجه مدت زمان زیادی طول میکشد تا همه روترها دید دقیقی از شبکه داشته باشند. این پروتکل‌ها از subnet mask های ثابت استفاده می‌کنند که مقیاس پذیر نیستند و حداکثر از 15 Metric Value پشتیبانی می‌کند یا به عبارتی فقط ۱۵ عدد Hop Count (تعدا روتر مسیر)را پشتیبانی می‌کند. اگر تعداد Hop Count ها بیشتر از عدد ۱۵ شود این شبکه را به عنوان شبکه غیر قابل دسترس یا Unreachable در نظر می‌گیرد.

این پروتکل از الگوریتم بلمن‌فورد (Bellman-Ford) برای محاسبه مسیر استفاده می‌کند. الگوریتم بلمن‌فورد یک الگوریتم برای محاسبه کوتاه‌ترین مسیر است. این پروتکل خیلی کُند هستند (slow convergence)، یعنی اگر تغییری در شبکه اتفاق بیافتد خیلی دیر متوجه می شوند(بین ۳۰ثانیه تا ۷ دقیقه و ۳۰ ثانیه زمان می‌برد متوجه شود)، اما simple هستند و راحت پیاده سازی و اجرا میشوند و ادمین زیاد درگیر دیزاین نمی شود. این پروتکل‌ها مستعد Loop هستند.

به عنوان مثال اگر مسیری با پهنای باند بالا ولی تعداد روترهای مسیر موجود باشد، این پروتکل مسیر با پهنای باند کمتر ولی تعداد روتر های کمتر را انتخاب میکند.



این پروتکل هیچ دیدی نسبت به کل Topology ندارد و صرفا روترهایی که به خود متصل هستند را می‌شناسد. در این شکل نوشهر می‌داند روتر مازندران به خودش متصل است ولی روتر تهران نمی‌داند چه روتری به نوشهر متصل است و صرفا این را می‌داند که برای رسیدن به نوشهر دو مسیر موجود است و بهترین مسیر، مسیر کرج میباشد.

به طور کل نسبت به روتر همسایه دید دارد. البته نا گفته نماند networkهای شبکه را می‌شناسد ولی مسیرهای رسیدن به مقصد را دید ندارد.

پروتکل های Link State (LS) :

Link state از سه فاکتور ترافیک شبکه، سرعت Link و فاصله به طور هم زمان و نه مجزا برای انتخاب بهترین مسیر استفاده می‌کند و همین عوامل باعث می‌شوند که Link State بسیار پیچیده‌تر از Distance Vector باشد. متریک آن cost است(که ارتباط مستقیم با Bw دارد- هرچه bw بیشتر،cost کمتر و در نتیجه مسیر بهتر) و از الگوریتم دایجسترا (Dijkstra) استفاده می‌کند.

پروتکل‌های Link state اطلاعات مسیریابی را تنها در زمان بروز تغییرات انتشار می‌دهند، به همین دلیل به صورت موثر از پهنای باند استفاده می‌کنند. در این حالت روترها به جای جدول مسیریابی، تنها تغییرات را انتشار می‌دهند، در نتیجه باعث افزایش سرعت همگرایی

می‌شود. پروتکل مسیریابی اطلاعات جدید را در اختیار تمام همسایگان در یک شبکه قرار می‌دهد و تلاش می کند تا با اطلاعات مسیریابی جدید شبکه را همگرا کنند.

این پروتکل‌ها از subnet masks با طول متفاوت استفاده می‌کنند که هم مقیاس پذیر هستند و هم مسیریابی را بهتر انجام می‌دهند. آنها همچنین نسبت به پروتکل های مسیریابی distance vector به CPU و حافظه بیشتری نیاز دارند و پیکربندی آن سخت تر می باشد. از پروتکل های Link State معمولاً در شبکه های بزرگ و متوسط استفاده خواهد شد. است.

این پروتکل‌ها خیلی سریع هستند (Fast convergence)یعنی اگر تغییری در شبکه اتفاق بیافتد خیلی سریع متوجه می‌شوند. در این پروتکل‌ها امکان اتفاق Loopصفر است.

این پروتکل‌ها نسبت به کل شبکه دید دارند. یعنی در شکل بالا روتر تهران میداند که نوشهر به روتر مازندران وصل است و دو مسیر برای رسیدن به نوشهر (از کرج و قزوین) وجود دارد و بر اساس الگوریتم خود بهترین مسیر را بر اساس ترافیک، مسافت و سرعت link انتخاب می کند.

پروتکل هایAdvance Distance Vector (Hybird) :

متریکی که استفاده می‌کند ترکیبی از چند پارامتر است و ترکیبی از پروتکل های DV وLS هستند، به همین دلیل به آن Hybird می‌گویند (ترکیبی از سادگی DV و دقت LS ها). هر کدام از این دو نوع دارای مزایایی می‌باشند که در اینجا پروتکل‌های ADV مجموعه ای از مزایای دو پروتکل را در خود دارند و به همین دلیل امروزه در اکثر شبکه های بزرگ از این دسته پروتکل‌ها برای روتینگ استفاده می‌شود.

متریک ADVها از چند پارامتر استفاده می‌کنند و در فرمول زیر قرار و بهترین مسیر را انتخاب می‌کند، اما دید کاملی از کل توپولوژی شبکه ندارد .

K1 = Bandwidth [1]
K2 = Load [0]
K3 = Delay [1]
K4 = Reliability [0]
K5 = Additional Reliability [0]

$$\text{Metric} = \left[\left(K1 \times \frac{10^7}{BW_{min}} + \frac{K2 \times BW_{min}}{256 - load} + K3 \times \sum delays\right) \times \frac{K5}{K4 + reliability}\right] \times 256$$

With $K5$ defaulted to 0, the equation $\frac{K5}{K4 + reliability}$ will be set to 1

$$\text{Metric} = \left[\left(1 \times \frac{10^7}{BW_{min}} + \frac{0 \times BW_{min}}{256 - load} + 1 \times \sum delays\right) \times 1\right] \times 256$$

$$\text{Metric} = \left(1 \times \frac{10^7}{BW_{min}} + \frac{0 \times BW_{min}}{256 - load} + 1 \times \sum delays\right) \times 256$$

$$\text{Metric} = \left(\frac{10^7}{BW_{min}} + \sum delays\right) \times 256$$

Competitive Metric

** اگر به ازای رسیدن به یک مقصدی بیش از یک مسیر داشته باشیم، یکی از آنها Best باشد، مسیر بکاپ را هم در توپولوژی نگه می‌دارد اما درDVوLS اینطور نیست. که این سرعت تغییرات در Topology را بیشتر می‌کند.

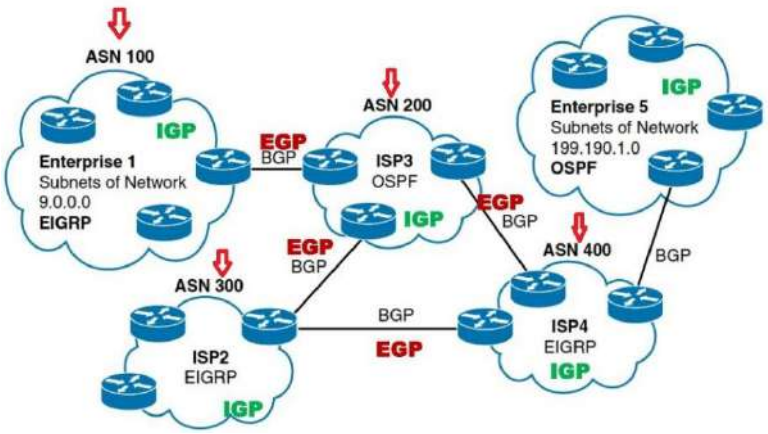
این پروتکل‌ها خیلی خیلی سریع هستند (very Fast convergence)یعنی اگر تغییری در شبکه اتفاق بیافتد خیلی بسیار سریع متوجه می‌شوند.

پروتکل های Path Vector :

رفتار آنها شبیه به DV هست اما اینجا متریک نداریم و پارامترهای مختلف که شبیه به متریک هستند را داریم.

Autonomous System:

Autonomous system یا AS به مجموعه ای از شبکه‌ها گفته می شود که در یک حوزه مدیریتی واحد قرار دارند. این مجموعه می‌تواند شبکه‌های موجود در یکISPباشد یا یک شبکهWANبزرگ سازمانی. مثل بانک ملی ، شاتل و ...، ولی مجموعه‌هایی مانند کندو ASN نیستند چون خودمختار نیستند و سرویس‌هایی از ISP ها ... می‌گیرند و وابسته به یک ASN است. Autonomoous systemها میتوانند شماره(Number) داشته باشند هم نداشته باشند.



دسته بندی dynamic Routing protocolها از لحاظ اینکه داخل ASها کار می‌کنند یا بین ASها (Purpose):

- ✓ **IGP** (Interior Gateway Protocol) :

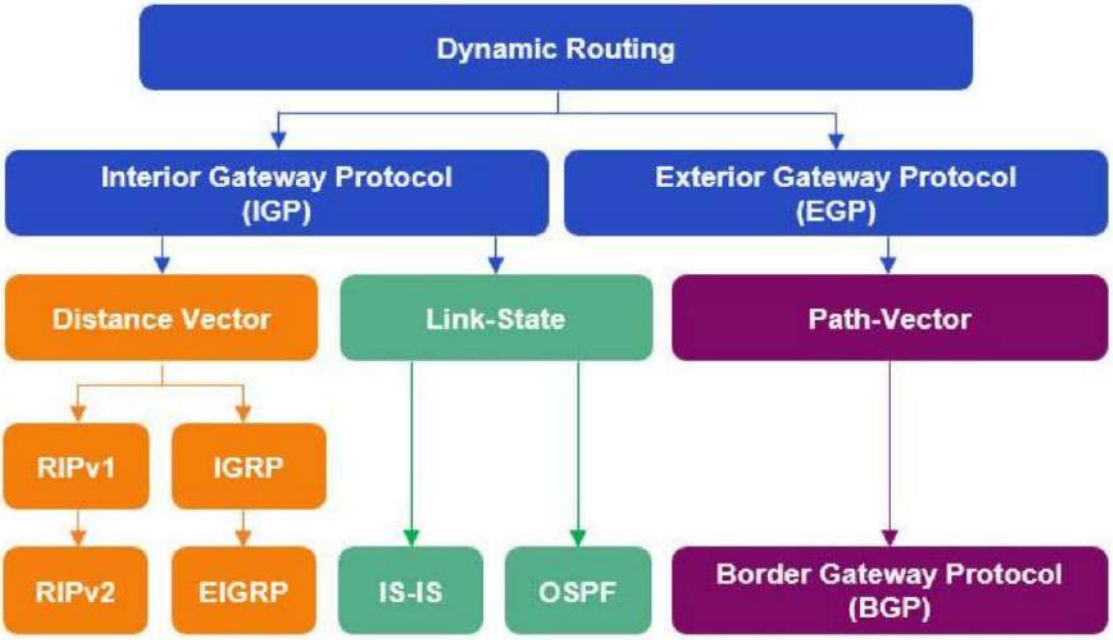
درون یک AS استفاده می شوند که (LS,ADV,DV) جزو این دسته هستند. مثل شبکه ایرانخودرو، شرکت نفت و ...

- ✓ **EGP** (Exterior Gateway Protocol) :

بین AS ها استفاده می شوند که Path Vector جزو این دسته هست.

IGP Intera-AS
- RIPv1 / v2 → Expired (V1 Classfull) / weak → Routing Information Protocol
- IGRP → Expired (Classfull) → Cisco Prop. → Interior Gateway Routing Protocol
- EIGRP → Strong → Cisco Prop. → Enhanced Interior Gateway Protocol
- OSPF → Strong → Standard → Open Shortest Path First
- ISIS → very Strong → Standard → Intermediate System - Intermediate System

EGP Inter-AS
- BGP : Border Gateway Protocol



The Various Routing Protocols

Features	RIP v1	RIP v2	IGRP	OSPF	EIGRP
Classful / Classless	Classful	Classless	Classful	Classless	Classless
Metric	Hop	Hop	Composite (bw and delay)	Cost 100,000/BW	Composite (bw and delay)
Periodic Advertisement	30 seconds	30 seconds	90 seconds	none	30 seconds
Advertising Address	255.255.255.255 (broadcast)	224.0.0.9 (multicast)	255.255.255.255 (broadcast)	224.0.0.5 224.0.0.6 (multicast)	224.0.0.10 (multicast)
Administrative Cost	120	120	100	110	Internal: 90 External: 170
Category	Distance Vector	Distance Vector	Distance Vector	Link State	Hybrid

فقط دو پروتکل آخر (EIGRP و OSPF) در حال حاضر مورد استفاده قرار می‌گیرند.

Feature	RIPv2	EIGRP	OSPF
Classless/sends mask in updates/supports VLSM	Yes	Yes	Yes
Algorithm (DV, advanced DV, LS)	DV	Advanced DV	LS
Supports manual summarization	Yes	Yes	Yes
Cisco-proprietary	No	Yes[1]	No
Routing updates are sent to a multicast IP address	Yes	Yes	Yes
Convergence	Slow	Fast	Fast

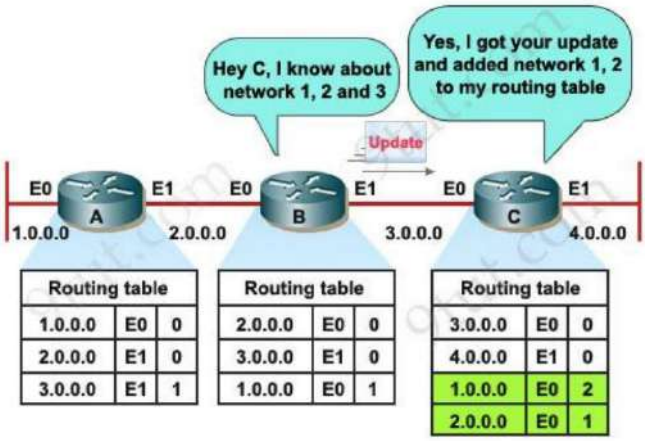
RIP (Routing Information Protocol):

RIP یک پروتکل قدیمی و عمومی می‌باشد که جزء دسته پروتکل‌های IGP (Interior getway protocol) است که در شبکه هایی با اندازه کوچک کارایی بالایی دارد و از رده پروتکل‌های DV (Distance vector) می باشد و فاقد مکانیزم احراز هویت می‌باشد یعنی اگر روتری این پروتکل را فعال کند می‌تواند کل Routing شبکه را داشته باشد .

ملاک انتخاب بهترین مسیر در این پروتکل hop count می باشد که بیشترین مقداری که برای متریک در این پروتکل در نظر گرفته شده است، ۱۵ می باشد و در صورتی که از این مقدار بیشتر شود، مسیر غیرقابل دسترس خواهد بود.

full update در این پروتکل هر ۳۰ ثانیه یکبار در شبکه بصورت Broadcast از اینترفیس‌های متصل به روتر خارج شده و به روترهای مجاور ارسال می‌شود. (به همه روترها، چه روتری که درمسیر باشد چه نباشد، چه تغییر داشته باشد یا نداشته باشد. واقعا چرا!؟ ☺)

* در صورتیکه روتر چند مسیر با متریک یکسان به یک شبکه پیدا کند، ترافیک را بین این مسیرها تقسیم می‌کند. بنابراین در این حالت از منابع شبکه و پهنای باند موجود به خوبی استفاده می‌شود. RIP به صورت پیش‌فرض توانایی پشتیبانی ٤ مسیر با متریک یکسان جهت load balancing را دارد.



RIP Version 2 :

این پروتکل هم از نوع Distance Vector می‌باشد ولی پیشرفته‌تر از RIPV1 است. پروتکل RIP Ver1 از Multicasting به جای Broadcast استفاده می‌کند، اما قابلیت کار به صورت Broadcast را نیز دارا می‌باشد. پروتکل RIP Ver1 یک پروتکل Classless می‌باشد و VLSM را پشتیبانی می‌کند. RIP Ver1 همچنین از احراز هویت پشتیبانی می‌کند که این توانمندی باعث می‌شود که روترها قبل از آپدیت جدول مسیریابی و رد و بدل کردن اطلاعات مسیریابی یکدیگر را احراز هویت نمایند و بعد از تکمیل پروسه احراز هویت، جدول‌های مسیریابی را بین یکدیگر مبادله کنند. در این پروتکل انتخاب بهترین مسیر بر اساس HOP Count با تعداد روترها موجود در مسیر محاسبه می شود. همان ۳۰ ثانیه RIP1 همچنان پارجاست.

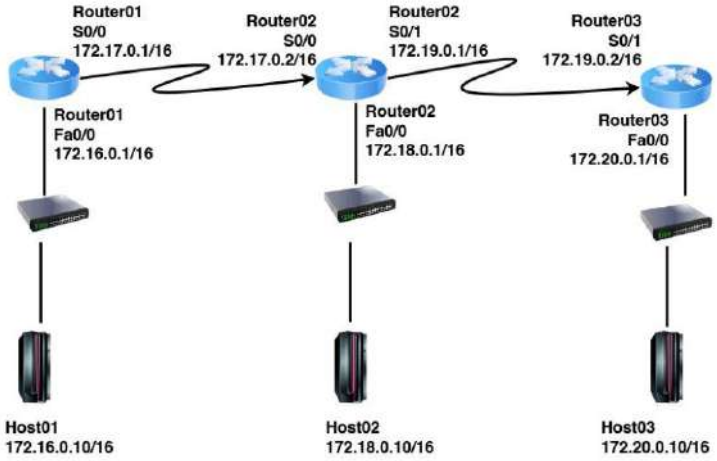
همانطور که گفته شد روترها، update Routing Table را به صورت multicast به روترهای دیگر(هدف) می‌رسانند. یعنی روی دسته‌های روترها IP با رنج set multicast می‌کنیم تا بتوانند فقط این اطلاعات را به روترهایی که صرفا در مسیر خود هستند ارسال کنند.

Class	High order bits	Start ip address	End ip address
A	0	0.0.0.0	127.255.255.255
B	10	128.0.0.0	191.255.255.255
C	110	192.0.0.0	223.255.255.255
Multicast	1110	224.0.0.0	239.255.255.255
Experimental	1111	240.0.0.0	255.255.255.255

IGRP (Interior Getway Routing protocol):

IGRP یک زیرمجموعه از پروتکل interior gateway vector-distance است که توسط CISCO توسعه یافته است. برای غلبه بر محدودیت‌های RIP معرفی شده است. معیارهای مورد استفاده عبارتند از: بار، پهنای باند، تاخیر،MTU و قابلیت اطمینان. به طور گسترده‌ای توسط روترها برای تبادل داده‌های مسیریابی در یک سیستم autonomous استفاده می‌شود.

این نوع پروتکل مسیریابی برای اندازه شبکه های بزرگ از RIP بهتر است، زیرا پس از هر ۹۰ ثانیه به صورت Broadcast پخش می‌شود و حداکثر تعداد پرش ۲۵۵ است. این به شما کمک می‌کند تا شبکه های بزرگتری را در مقایسه با RIP مدیریت کنید. IGRP همچنین به طور گسترده‌ای مورد استفاده قرار می گیرد، زیرا در برابر ایجاد حلقه Loop در مسیریابی مقاوم است، زیرا هنگام تغییر مسیر در شبکه خاص به طور خودکار به روز می‌شود. همچنین گزینه ای برای بارگیری تعادل ترافیک در مسیرهای هزینه متریک مساوی یا نابرابر ارائه شده است.



OSPF (Open Shortest Path First):

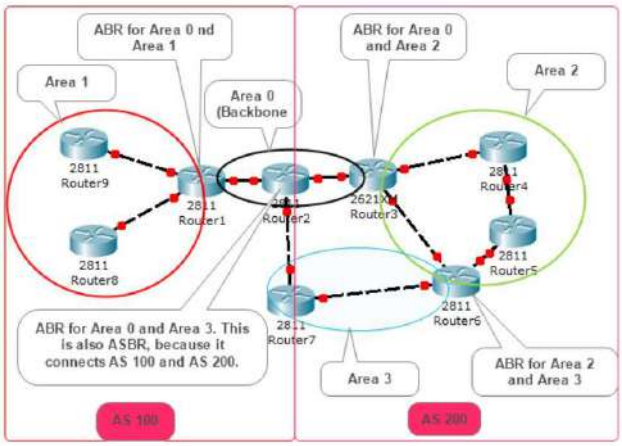
یک پروتکل(لایه۳) مسیریابی Link state است که درون یک AS(Autonomous System)کار می کند و می‌تواند ترافیک‌های مربوط به پروتکل IP را مدیریت کند . تقریبا همه روترهایی که در دنیا وجود دارند از پروتکل OSPF پشتیبانی می‌کنند (استاندارد RFC2328). این پروتکل مسیریابی از الگوریتم Shortest Path First یا SPF برای جلوگیری از به وجود آمدن Loop Routing در توپولوژی شبکه‌ها استفاده می‌کند و به نوعی یک شبکهLoop Free ایجاد می‌کند.OSPF فرآیندConvergence سریعی دارد و از طرفی قابلیت Incremental Update را نیز با استفاده از LSA فراهم می‌کند. در OSPF روترها هر ۱۰ ثانیه Hello برای برقراری همسایگی ارسال می‌کنند.

224.0.0.5
224.0.0.6
(multicast)

مجموعه روترهایی که OSPF را اجرا می‌کنند به بخش‌هایی تحت عنوان Area تقسیم می‌شوند. یک شبکهOSPF باید یک Area0 داشته باشد و علاوه بر آن می‌تواند Areaهای دیگری نیز داشته باشد. الگوریتم SPF در هر Area اجرا می‌شود و همچنین مسیرهای ناحیه ای بین Areaها رد وبدل می‌شوند. به صورت پیش‌فرض توانایی پشتیبانی ٤ مسیر با متریک یکسان جهت load balancing را دارد.

در OSPF دو سطح وجود دارد:

Area0 به عنوان ناحیه انتقال طراحی شده است و Areaهای دیگر به آن متصل می‌شوند.Area های دیگر باید به صورت مستقیم به Area0متصل شوند و از طریق Area0 به دیگرAreaها دسترسی پیدا کنند.



EIGRP (Enhanced Interior Gateway Routing Protocol):

یک پروتکل(لایه۳) مسیریابی ترکیبی است که پروتکل‌های مسیریابیDV و پروتکل‌های مسیریابی link-state را ارائه می‌دهد. پروتکل مسیریابی فرم کامل EIGRPپروتکل مسیریابی پیشرفته داخلی است. پروتکل‌های مشابهی را که IGRPبا استفاده از معیارهای ترکیبی مشابهIGRPهدایت می‌کند، که به شبکه کمک می‌کند بهترین مقصد مسیر را انتخاب کند. این پروتکل هر ۳۰ ثانیه Hello برای برقراری همسایگی ارسال می‌کند.

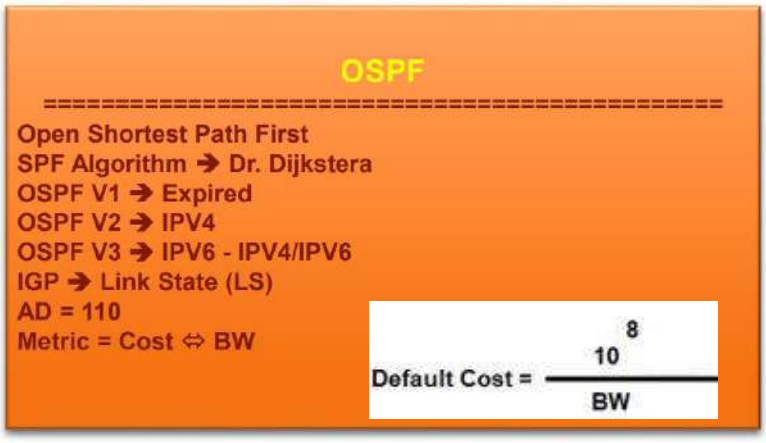
Although Cisco created EIGRP and has kept it as a proprietary protocol for many years, Cisco chose to publish EIGRP as an informational RFC in 2013. This allows other vendors to implement EIGRP, while Cisco retains the rights to the protocol.

224.0.0.10
(multicast)
Internal: 90
External: 170

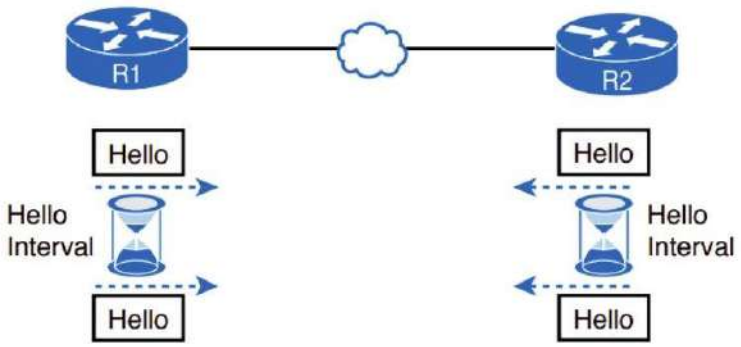
BGP (Border Getway Protocol):

BGP آخرین پروتکل مسیریابی اینترنت است که به عنوان distance path vector protocol(DPVP)طبقه‌بندی می‌شود. این نوع پروتکل مسیریابی هنگام ایجاد تغییرات، داده‌های جدول روتر به روز شده را ارسال می‌کند. بنابراین هیچ auto-discovery از تغییرات توپولوژی وجود ندارد، به این معنی که کاربر باید BGP را به صورت دستی پیکربندی کند.

OSPF Concepts and Operation :



در زمان طراحی ospf سرعت شبکه Mbps100 بوده = ۱۰ به توان ۸



- The Hello message follows the IP packet header, with IP protocol type 89.
- Hello packets are sent to multicast IP address 224.0.0.5, a multicast IP address intended for all OSPF-speaking routers.
- OSPF routers listen for packets sent to IP multicast address 224.0.0.5, in part hoping to receive Hello packets and learn about new neighbors.

OSPF قابلیت periodic update دارد، یعنی هر چند دقیقه یکبار هم یک آپدیت کلی ارسال می کند(پیشفرض هر۳۰دقیقه). پیغام هایی که OSPF ارسال می‌کند LSA(Advertisement State Link) نامیده می‌شوند، اما در برخی منابع PDU(Unit Data Protocol)نامیده شده است.پس اگر تغییری در شبکه اتفاق بیافتد، در قالب پیغام‌های LSA اطلاع‌رسانی می‌شود. پیغام های LSA به آدرس Multicast 224.0.0.5 ارسال می‌شود، پس باید درون فایروال این آدرس را برای OSPF باز بگذاریم.

هر روتر LSA دریافتی را پس از ذخیره کردن برای همسایه‌ها Forward می‌کند، منتها محدوده ی Forward درون همان Area است. روترها LSAها را درونLSDB(Link state data base) روی روتر ذخیره می‌کنند (LSDB معادل همانTopology Tableپروتکل EIGPRمی‌باشد). درون LSDB الگوریتم Dijkstra's (یکی از الگوریتم‌های پیمایش گراف) بهترین مسیرها را برای مقصدهای مختلف بدست می‌آورد و این مسیرهای منتخب درون Routing Table قرار می‌گیرند(که به آن Forwarding Database هم گفته می‌شود) و هر روتر براساس موقعیت و مکان خودش، بهترین مسیر را از LSDBانتخاب می کند. (بهترین مسیر برای همه روترها همیشه یکسان نیست، بلکه براساس Position و شرایط آن روتر انتخاب می‌شود).

روتری که در OSPF شرکت می‌کند، اولین کاری که باید انجام دهد این است که اطلاعات همسایه ها را نگهداری کند. برای این کار قطعا یک Neighbor Data Base خواهد داشت (که Adjacency Data Base هم نامیده می‌شود). بعد از شناختن همسایه‌هایی که روی آنها OSPF اجرا شده است و در حال ارسال و دریافت LSAهستند، LSDB و به تبع آن Routing Table هم تکمیل می شود. (نکته: هنگام T-Shoot در OSPF ابتدا باید دید کهNeighborها را شناخته باشد.)

: LoopBack Interface

interface loopback یک اینترفیس Virtual یا Logical است که در روترهای سیسکو با Commandی ساده می‌توانید آن را ایجاد کرده و از آن استفاده کنید. با توجه به اینکه اینترفیس هایloopback، اینترفیس مجازی هستند، پس اینترفیسی مانند اینترفیس های فیزیکی مانند، Gigabit interface و یا Fast Ethernet ها نیستند.

واقعا هدف از ایجاد کردن Loopback Interface چیست؟ این Interface نه به پورت‌ها یا Interfaceهای فیزیکی روتر سیسکو متصل می‌شود و نه شبکه‌ای می‌تواند به آن متصل شود، در واقع به نظر می‌رسد وجود چنین Interface ی فقط باعث هدر رفتن آدرس‌های IPموجود در شبکه شود، اما برخلاف تصوری که می‌شود کاربردهای زیادی دارد.

اگر با ویندوز کار کرده باشید با آدرس Loopback تاحدودی آشنایی دارید که بصورت آدرس ۱۲۷.۰.۰.۱ در کامپیوتر وجود داشت و شما با Ping کردن این آدرس در واقع ترافیک را به داخل کارت شبکه مجددا بازگشت می‌دادید و به این روش تنظیمات TCP//IPرا تست می‌کردید. در روترهای سیسکو آدرس‌های IPای که بصورت Loopbackتعریف می‌شوند به هیچ interface فیزیکی متصل نمی شوند که شما بخواهید آن را ببینید.

در واقع Loopback Interface یکی از ابزارهای قدرتمند است که در هر زیرساختاری می تواند مورد استفاده قرار بگیرد و مهمترین ویژگی این Interface این است که هیچوقت down نمی‌شود مگر اینکه خود دستگاه بصورت کامل خاموش شود. این پایداری باعث می‌شود فرآیندهایی که نیاز به آدرس IP برای شناسایی دستگاه های شبکه دارند براحتی با استفاده از Loopback Interface دستگاه های شبکه را شناسایی کنند و در واقع Loopback Interface به عنوان یک Identifier یا شناسه در شبکه می‌تواند مورد استفاده قرار بگیرد. یکی از پرکاربردترین استفاده‌هایی که از Loopback Interface می‌شود در پروتکل مسیریابی OSPF است ، آدرس IP که شما برای Loopback Interface انتخاب می‌کنید در واقع تعیین کننده OSPF RID در این پروتکل است که می توان به آن ۳۲/ ip بدهیم.

Loopback interface برای telnet و ssh زدن هم کاربرد خوبی دارد.

بصورت پیشفرض روترها دارای loopback interface نیستند و در واقع این قابلیت روی آنها فعال نشده است ، اما شما می توانید براحتی آن را ایجاد کنید ، ساختار دستوراتی که باید برای ایجاد کردن loopback interface در روتر سیسکو بکار بروند به شکل زیر می باشد:

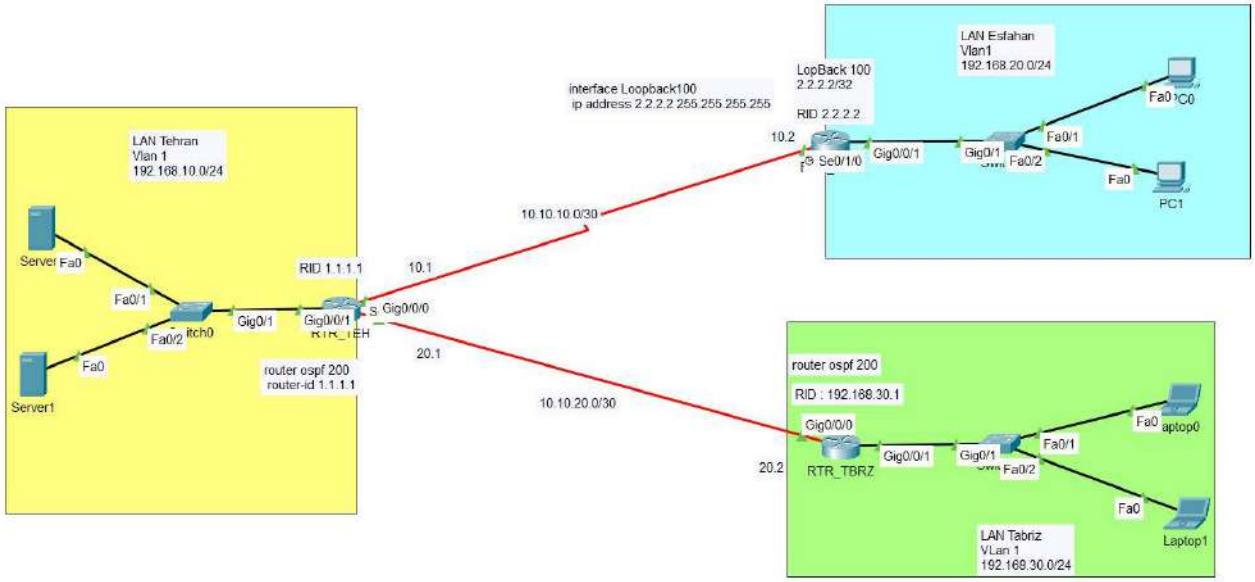
```
Router(Config)#int loopback (loopback_interface_number)
Router(Config-if)#ip address (ip_address) (subnet_mask)
```

Router ID :

هر روتری که در شبکه‌های OSPF قرار بگیرد به یک OSPF Router ID یا Identifier منحصر به فرد نیاز دارد. Router ID برای شناسایی یک روتر در شبکه‌های مبتنی بر پروتکل مسیریابی OSPF استفاده می‌شود و هر روتر برای اینکه در شبکه بصورت مشخص شناسایی شود برای خود دارای یک Router ID است. ID Router یک عدد خاص نیست بلکه یک آدرس IPV4 است (یک عدد ۳۲ بیتی باینری/ 1-65535). اگر OSPF Router-ID به صورت دستی تنظیم نشود، روتر یکی از آدرس‌های IP اختصاص داده شده به روتر را به عنوان آن Router-IDاستفاده می کند.

هر روتر در OSPF یک شناسه ۳۲ بیتی دارد که به یکی از روش های زیر قابل مشخص شدن است:

- ✓ ۱. دستی
- ✓ ۲.بزرگترین یا کوچکترین (بسته به سازنده روتر شما) اینترفیس Loop Back logical روتر به عنوان RID در نظر گرفته می شود.
- ✓ ۳.بزرگترین یا کوچکترین (بسته به سازنده روتر شما) اینترفیس nonLoop Back را در نظر می گیرد (اینترفیس باید در حالت up باشد).



در این سناریو،

روتر تهران به صورت دستی RID گرفته است (دستور زیر روتر درج شده)

روتر اصفهان بعد از فعال کردن اینترفیس لوپ_بک و Ip گرفتن، از طریق همین اینترفیس ، RID را مشخص کرده است.

اگر چندتا ip loopback داشت باشیم، کوچکترین یا بزرگترین Ip میشود RID.

```
RTR_ESF#sho ip protocols

Routing Protocol is "ospf 200"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 2.2.2.2
```

روتر تبریز نیز با توجه به اینکه روی این روتر اینترفیس لوپ بک وجود ندارد و به صورت دستی نیز RID تعریف نشده است، سراغ روش سوم یعنی انتخاب RID از بزرگترین اینترفیس up روتر رفته است.

```
RTR_TBRZ#sho ip interface brief
Interface              IP-Address
GigabitEthernet0/0/0   10.10.20.2
GigabitEthernet0/0/1   192.168.30.1
GigabitEthernet0/0/2   unassigned
Serial0/1/0            unassigned
Serial0/1/1            10.10.30.2
Vlan1                  unassigned
```

نکته۱: این عدد ospf بین روترها باید یکسان باشد؟ خیر، ولی برای desiqn معمولا اصولی یک عدد یکسان قرار میدهند.

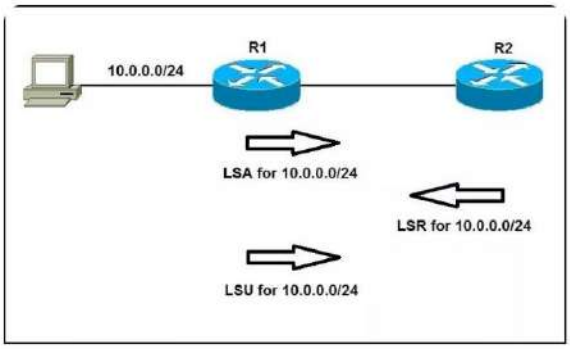
نکته۲: اگر RID را بعد از فعال شدن OSPF تغییر دهیم همان RID قبلی استفاده می‌شود مگر اینکه پروسه OSPF را Reset کنیم.

نکته۳: بهتر است که RID را براساس مقادیری تعیین کنیم که نشان‌دهنده آن روتر باشد تا در زمان‌های مانیتورینگ و خطایابی با استفاده از این RID متوجه شویم که منظور کدام روتر است.

LSA :

Link-State Advertisement به یک سری از بسته‌ها در پروتکل‌های مسیریابی link-state گفته می‌شود که وظیفه انتشار دادن اطلاعات موجود(Touting و Topology) در جدول مسیریابی (Routing Table)یک روتر را به سایر همسایه های (Neighbors)خود در یک روند مسیریابی پویا (Dynamic Routing Process) برعهده دارد.

زمانی که دو روتر همسایه تصمیم به تبادل اطلاعات مسیربابی خود می‌گیرند، هر یک از این روترها یک پکت LSA شامل اطلاعات خود درمورد توپولوژی شبکه را به همسایه خود ارسال می‌کند. روتر دریافت کننده این اطلاعات را با دیتابیس خود از شبکه که به آن LSDB (Link State Data-Base) می‌گویند نگاه می‌کند و در صورتیکه اطلاعات دریافتی در این دیتابیس وجود نداشته باشد، پکت درخواست اطلاعات کامل آنLSA را که به آن LSR (Link-State Request) میگویند را به همسایه‌ای که پکت ابتدایی را از آن دریافت کرده است ارسال می‌کند و روتر مقابل نیز اطلاعات تکمیلی را تحت عنوان LSU (Link State Update) برای آن ارسال می‌کند.



OSPF Packet Type :

OSPF PACKET TYPE		DESCRIPTION
1	Hello	- Use to discover neighbors, and to establish and maintains adjacencies - OSPF header + Network Mask + Hello and Dead Intervals + Options Field + Router Priority + DR/BDR addresses + List of discovered neighbors.
2	Database Description	- Describes the contents of the topological database. - OSPF header + packet seq. # + link-state advertisement header.
3	Link State Request	- Sent by a router when it detects that portions of its database are out of date and during initial sync. - Used to request link state update. - OSPF header + fields that uniquely identify the database information that the router is requesting
4	Link State Update	- Carries one or more link-state advertisements - Sent as a response to a Link State Request
5	Link State Ack.	- Response to link-state update packets - Validates that the update packets have been received successfully. - OSPF header + link-state advertisement header

پنج نوع بسته مختلف در پروتکل مسیریابی OSPF وجود دارد:

Hello_1 : با استفاده از این پیام یک روتر قادر به شناسایی روترهای همسایه خواهد شد و بعد از شناسایی بین آن‌ها رابطه مجاورت برقرار می‌شود. هر ۱۰ ثانیه دوره‌ای ارسال می‌شود تا همسایه‌ها را پیدا کرده و ارتباط را برقرار کند. اگر hello ها دریافت نشوند، همسایگی از بین می‌رود. هر روتر یک Dead Interval دارد که به صورت پیشفرض چهار برابر زمان ارسال دوره‌ای Hello Packet آن می‌باشد (پیشفرض ٤٠ ثانیه) و مشخص می‌کند که چه مدت باید منتظر دریافت Hello از سمت Neighbor بمانیم و پس از گذشتن این مدت همسایگی از بین می‌رود. علت استفاده از Dead Interval این است که بلافاصله پس از دریافت نکردن یکhello کل توپولوژی به هم نخورد، روتر باید منتظر بماند چراکه شاید Packet Lost اتفاق افتاده باشد یا مشکل موقتی دیگری است.

توصیه می‌شود جایی که شبکه‌ی ما زیاد Stable نیست مقدار Dead Interval را بیشتر بگذاریم.

2ـ Database Description یا DBD : با استفاده از این پیام به روز بودن اطلاعات جدول LSDB یک روتر توسط روتر همسایه مورد بررسی قرار خواهد گرفت.

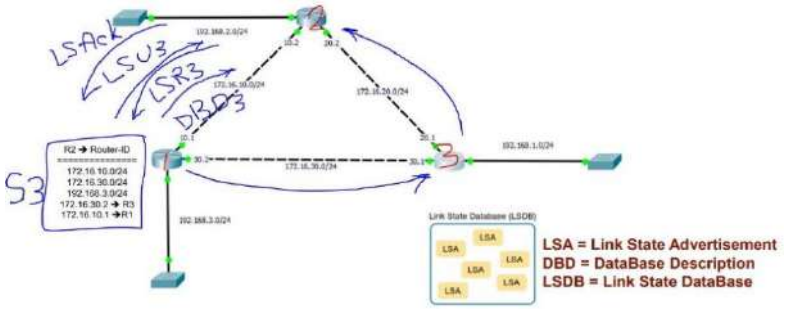
وقتی دو روتر تازه همسایه شدند، باید چک شود که آیا LSDBهایشان یکی است یا خیر. به عبارت دیگر کاربرد DBD برای Data Base Synchronization است. DBD کل LSDB را نمی‌فرستد بلکه تنها یک خلاصه‌ای از آن را ارسال می‌کند.

3ـ Link state request یا LSR : یک روتر با ارسال این پیام از سایر روترها درخواست دریافت اطلاعات مسیریابی می‌کند.

زمانیکه یکDBDدریافت می‌شود ممکن است تعدادی از اطلاعات درون آن برای روتر شناخته باشد. پس یک LSRبرای فرستنده DBD ارسال می‌شود تا در قالب یکLSU ، اطلاعات کامل (یعنی LSDB) مسیرهای خواسته شده دریافت شود.

4ـ Link state update یا LSU : پاسخی خواهد بود که روتر به درخواست پیام LSR ارسال میکند و با استفاده از پیام LSU اطلاعات درخواستی را برای روتر درخواست‌کننده ارسال می‌کند. (یعنی ارسال LSDB کامل)

5ـ Link state Acknowledgment یا LSAck : بعد از دریافت پیامDBD ، LSR، LSU، روتر دریافت‌کننده پیام، با ارسال پیام LSAck برای روتر ارسال کننده پیام، دریافت صحیح پیام را تأیید خواهد کرد.



توضیح شکل بالا:

بعد از برقراری همسایگی(neighbor)، هر روتر بعد از فهم وضعیت لینک خود (LS)، وضعیت خود را به بقیه روترها تبلیغ می‌کند (LSA). به عنوان مثال در شکل بالا، روتر1LSA خود را به روترهای3 رو2 تبلیغ می‌کند. هر روتر با مجموع LSAخود و DBDهایی که به سمتش ارسال می‌شود LSDB را تشکیل می‌دهد. روترها قبل ارسال LSDBها ، پیغام یا بسته سبک و کوچکی به نام DBD با sequence number آن LSDB به سمت روتر مقصد ارسال می‌کند که بفهمد آخرین update را دارد یا خیر. اگر روتر هدف Update بود که هیچ(LSDB ارسال نمی‌شود)، ولی اگر Update نبود، روتر هدف به روتر مبدا LSR ارسال می‌کند. روتر مبدا LSDB را در قالب LSU به روتر هدف ارسال می‌کند. روتر هدف هم برای اطلاع از صحت دریافت LSDB، یک LSACT به مبدا ارسال می‌کند. Router1 همین مراحل را برای Router3 طی می‌کند. نتیجه اینکه وقتی روترهای ۲ و ۳ به هم DBD ارسال می‌کنند، با توجه به اینکه هر دو روتر Update هستند، دیگر نیاز به ارسال LSDB نیست. همین مراحل آنقدر بین روترها انجام می‌شود که LSDBها یکسان شوند.

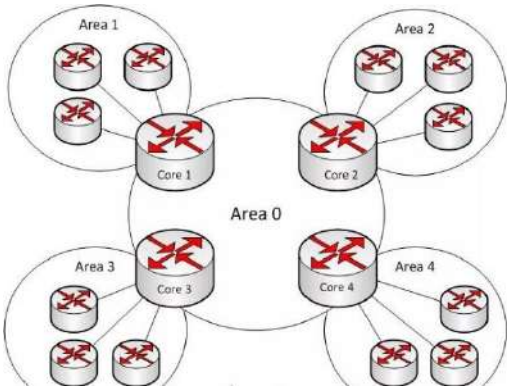
نکته۱: در ospf ابتدا جدول همسایگی تشکیل می‌شود. سپس با توجه به همسایگی، LSDBها ارسال می‌شوند تا یکسان شوند و Topology Table شکل بگیرد. سپس با اعمال الگوریتم‌ها در Topology Table، بهترین مسیر انتخاب می‌شود و در نهایت جدول Routing table به نتیجه می‌رسد.

Becoming Neighbors ➔ Exchanging Database ➔ Adding The best Route
Neighborship Table LSDB Routing Table

نکته۲: پیغامی مثل Hello نیاز به Ack ندارد چون مداوم در بازه‌های زمانی ارسال می‌شود، اما وقتی LSU داریم حتما باید در جواب Ack بفرستیم. تمامی پنج Packet در OSPF به صورت لایه سومی توسط بسته‌های IP ارسال می‌شوند، یعنی OSPF از UDP و TCP استفاده نمی‌کند و مکانیزم خاص خود را دارد. شما یکFrame دارید که Headerو trailer دارد، داخلFrameیک قسمتی به نام Header IP وجود دارد و درون آنProtocol ID Number مشخص شده است که مقدار آن ۸۹ می‌باشد تا هر روتری که این بسته را گرفت بفهمد که OSPF است.

نکته۳: هر LSA یک Sequence Number دارد که براساس آن Sequence Number جواب هایAckارسال می‌شود، یعنی در LSA برای تشخیص جدیدترین آپدیت‌ها از Sequence Number استفاده می‌شود. همچنین هر LSA یک MaxAge دارد، یعنی مدت زمانیکه آن LSA معتبر خواهد بود که به صورت پیشفرض یک ساعت است. پس اگر آپدیتی دریافت نکند، پس از ۶۰ دقیقه آن LSA نامعتبر می‌شود. همچنین به صورت پیشفرض هر ۳۰دقیقه یکبار OSPF کل LSDB ای که دارد را درون شبکه Deploy(گسترش) می‌کند.

Area Concept in OSPF:



شبکه‌ای که توسط پروتکل **OSPF** ایجاد می‌شود، به مجموعه‌ای از شبکه‌های کوچکتر تقسیم‌بندی می‌شود که در اصطلاح فنی به هر کدام از این شبکه‌های کوچکتر یک Area یا ناحیه گفته می‌شود. از ساختار Area برای جلوگیری از بزرگ شدن LSDBاستفاده می‌کنند. تعداد روتر توصیه شده برای هر Area حداکثر50روتر می‌باشد. البته نمی‌شود گفت که OSPF برای مدیریت شبکه به دنبال ساختار Area رفته است، چراکه وقتی حجم LSDB بالا برود، کار الگوریتم برای محاسبه دشوار می‌شود، زیرا شبکه خیلی پیچیده شده و تغییرات زمان‌بر است که این مطلوب نیست.

OSPF از طراحی‌های سلسله مراتبی یا موروثی در شبکه که در اصطلاح فنی به آنها Hierarchical Network گفته می‌شود پشتیبانی می‌کند. **OSPF** این اجازه را به ما می‌دهد که شبکه‌های خود را در دو لایه سلسله مراتبی طراحی کنیم.

یک روتر مستقر در یک OSPF Area اطلاعات دقیقی در خصوص توپولوژی‌های شبکه‌های بیرون از Areaخود ندارد. از مهمترین مزایای طراحی شبکه‌های **OSPF** بصورت Multi-Area می‌توان به موارد زیر اشاره کرد:

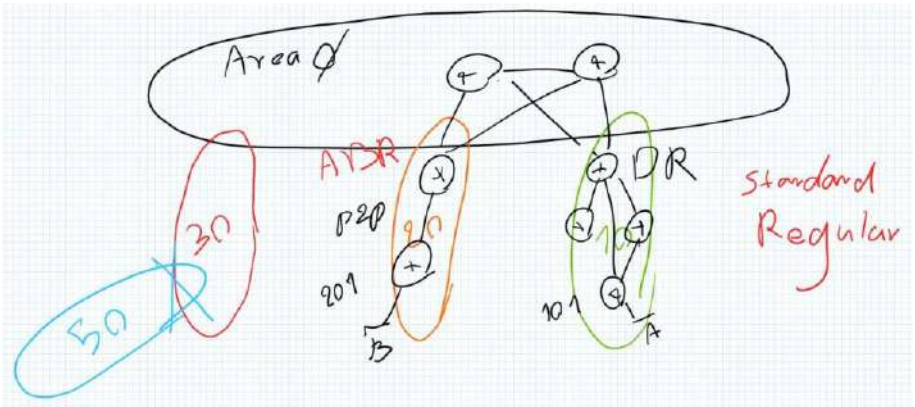
- روترهای موجود دریک OSPF Area فقط Link State Database (LSDB) را در محدوده خود Share می‌کنند.
- نیازمندی‌های مربوط به میزان استفاده از RAM و CPU برای LSDB ها در روترها نسبتاً کمتر است.
- زمانیکه در توپولوژی شبکه تغییری ایجاد شود، روترها برای محاسبه کردن بهترین مسیر بایستی مجددا الگوریتم SPF را اجرا کنند ، الگوریتم SPF حتما زمانیکه در توپولوژی شبکه تغییری ایجاد می‌شود، بایستی در همانArea اجرا شود.به

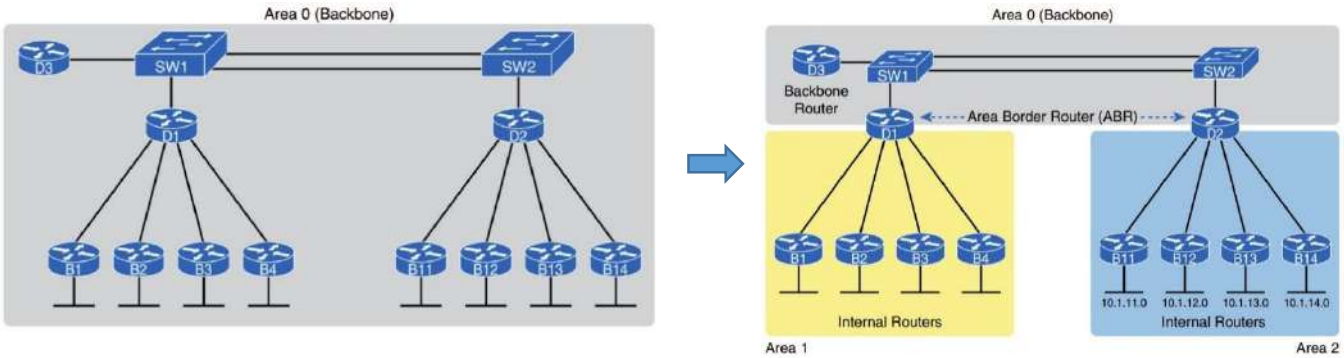
همین خاطر نکته مثبت در استفاده ازAreaها این است که با توجه به کوچکتر بودن یک Area نسبت به کل شبکه، در هر بار تغییر در توپولوژی‌ها نیاز به اجرای SPF کمتر و کمتر می‌شود.

- **Router Summarization** دستی فقط می‌تواند بر روی ABRها و ASBRها اجرا شود و به Areaها اجازه می‌دهد که بتوانند Routing Table های همدیگر را بصورت خلاصه دریافت کنند.

چند نوع Area در OSPF وجود دارد؟

- ✓ Backbone Area : همان Area 0 است که تمامArea ها دیگر باید به آن متصل شوند.
- ✓ Regular (Or Normal) Area : Areaهای غیر Area 0 که دیتابیس آنها شامل هر دو مسیرهای داخلی و خارجی است. یک Area Normalنمی‌تواند به صورت پیشفرض ترافیک سایر Area Normalها را عبور دهد. هر Area یک LSDB منحصربه خود دارد که روی تمام روترهای عضو آن باید یکسان باشد.
- ✓ Stub Area: دیتابیس اینArea ها فقط شامل مسیرهای داخلی و یک Default Route می باشد.
- ✓ Totally Stubby Area: اختصاصی شرکت سیسکو می باشد و دیتابیس آن شاملRoute های Area خودش و یک Default Routeمی باشد.
- ✓ Not-so-stubby area (NSSA): دیتابیس آن شاملRoute های داخلی و مسیرهای Redistributed شده و Default Route می باشد.
- ✓ Totally NSSA: اختصاصی شرکت سیسکو است دیتابیس آن شاملRoute های Area خودش و مسیرهای Redistributed شده و Default Route می باشد.



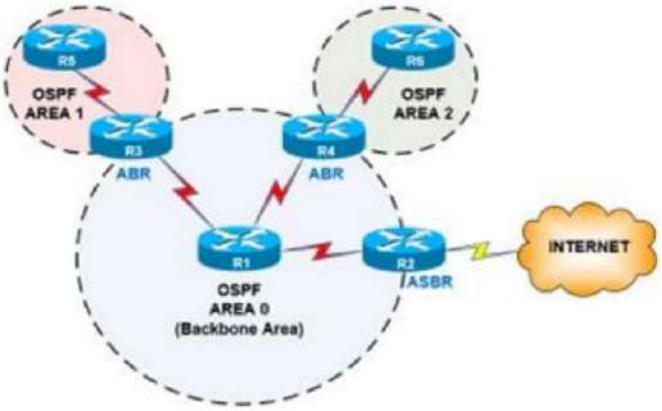


به منظور پیاده‌سازی Area بندی ابتدا می‌بایست با قوانین موجود در آن آشنا شوید:

- دو نوع Area وجود دارد، یک Backbone Area و سایر Area ها. Backbone Area ناحیه‌ای است که سایر Area ها به آن متصل می‌شوند.
- مابین سایر Area ها نباید اتصالی وجود داشته باشد. یعنی یک Area برای دیدن Area دیگر باید از طریق Backbone Area این کار را انجام دهد.
- بین Backbone Area می بایست پیوستگی وجود داشته باشد.

آشنایی با واژگان در Multi Area:

- به روترهایی که در مرز بین Area ها قرار دارند ABR گفته می‌شود. یک سمت این روترها در Area Backbone قرار دارد و سمت دیگر آن در سایر Area . معمولاً ABR بین Area0 و Normal Area ها می باشد.
- به روترهایی که درون Backbone Area قرار گرفته اند، Backbone Router گفته می‌شود.
- به روترهایی که درون سایر Area ها قرار گرفته اند Internal Router گفته می‌شود.
- به روتری که بخشی از اطلاعات را می‌خواهد از خارج از شبکه OSPF وارد کند، ASBR یا Autonomous System Boundary Router گفته می شود.



نکته۱: Backbone که همان Area0 می‌باشد در واقع هسته‌ی اصلی Routing Protocol ما است. به همین خاطر روترهای درون Area0 با د از قدرت بالایی برخوردار باشند، چراکه تمام ترافیک Routing شبکه باید از آن عبور کند (حداکثر تعداد روتر توصیه شده درون یک area ۵۰روتر می‌باشد).البته Area0 هسته است اما نه هسته‌ی شبکه، بلکه هسته‌ی Routing Protocol است، یعنی ترافیک سایر Routing Protocol ها کاری با Area0 ندارند.

نکته۲: LSDB یک Area با هیچ Area دیگری یکسان نیست. بین دو Area جزئیات تمام مسیرها ردوبدل نمی‌شود چون کاربردی نیست، بلکه تنها اطلاعات بهترین مسیر مدنظر داده می‌شود. توصیه شده است که یک روتر حداکثر عضو سه Area باشد.

نکته۳: در Multi Area ها یک نوع LSA دیگر وجود دارد که به آن LSA Type 3 گفته می‌شود که توسط ABR تولید شده و به منظور ارائه شبکه‌های یک Area به Area دیگر تولید می‌شود و LSID آن برابر با Subnet Network هر شبکه می‌باشد. این بسته‌ها به تعداد شبکه‌های موجود در Area تولید می‌شوند و در روند اجرای الگوریتم SPF دخالتی ندارند.

در جدول روتینگ OSPF هر روت دارای یک شناسه است که در زیر مشخص شده اند:

- مسیرهایی که با O مشخص شده‌اند آنهایی هستند که با LSA های T1 و T2 ساخته شده‌اند.
- مسیرهایی که با OIA مشخص شده‌اند آنهایی هستند که با LSA Type 3 ایجاد شده‌اند.
- مسیرهایی که با OE1 و OE2 مشخص شده‌اند آنهایی هستند که با ASBR تولید شده‌اند.

پیکربندی این مدل از OSPF نیز همانند ساختار Single Area می باشد اما به چیزی که باید توجه شود نحوه Area بندی و قرار دادن Network ها درون Area های خودشان می‌باشد.

OSPF Configuration :

OSPF Configuration Steps

1 – Enabling OSPF and Process-ID

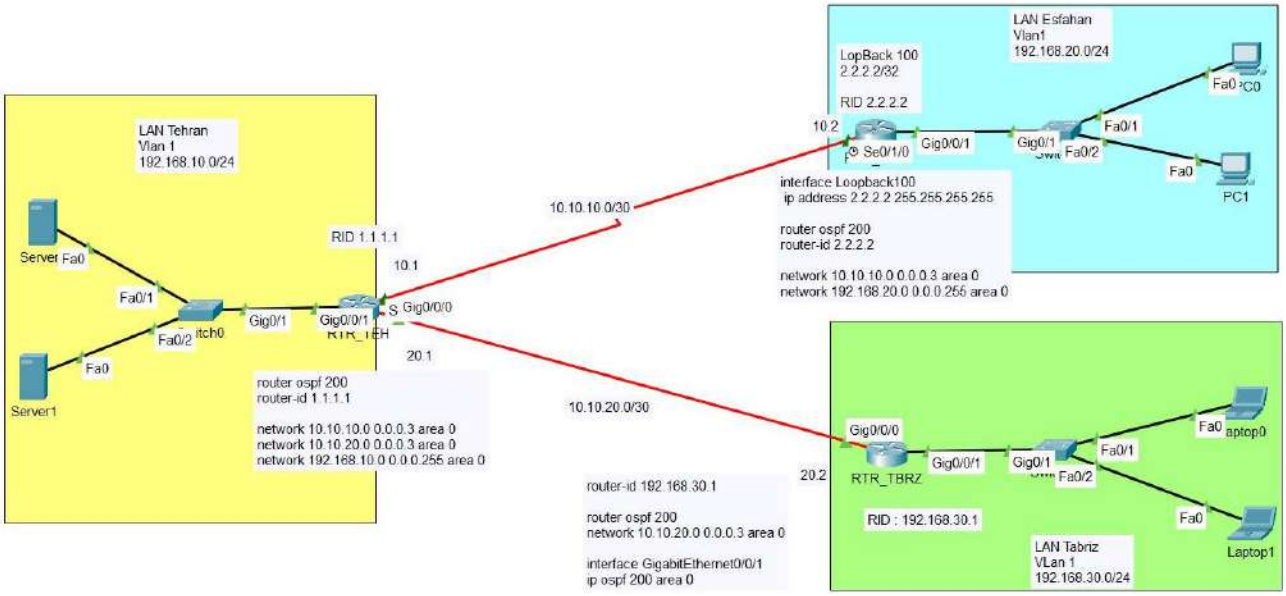
2 – Configure RID
* Its can be select Manually or Automatically

3 – Adding OSPF Networks

3-1 – Network Command → Traditional
3-2 – Interface Command → Explicit

```
Show ip protocols
Show ip ospf
Show ip ospf interface [brief]
Show ip ospf neighbor
```

مثال:



۱)بعد از انتخاب RID (Router-ID) توسط یکی از روش‌های گفته شده، ۲) مرحله بعد باید همسایگی‌ها تعریف شوند(برای برقرای همسایگی باید دو طرف config شوند).

دستور برقراری Neighbor :

در مثال بالا، برای روتر تهران دو همسایگی و برای روتر اصفهان و تبریز هر کدام یک همسایگی تعریف شده است.

network 10.10.20.0 0.0.0.3 area 0 network 10.10.10.0 0.0.0.3 area 0 network 10.10.10.0 0.0.0.3 area 0
network 10.10.20.0 0.0.0.3 area 0

بررسی نتیجه همسایگی تهران:

```
RTR_TEH#sho ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
192.168.30.1      1   FULL/DR         00:00:31    10.10.20.2      GigabitEthernet0/0/0
2.2.2.2           0   FULL/  -        00:00:31    10.10.10.2      Serial0/1/0
```

۳) مرحله بعد network هایی که روی هر روتر وجود دارد را در ospf به بقیه advertise کنیم.

Traditional Configuration :

معرف مستقیم شبکه متصل به روتر به صورت مستقیم

network 192.168.10.0 0.0.0.255 area 0 network 192.168.20.0 0.0.0.255 area 0

Router(config)# router ospf < Proccess-ID>
Router(config-router)# router-id <A.B.C.D> [Optional]
Router(config-router)# network <A.B.C.D> <WC-MASK> area <AREA-ID>

explicit Configuration:

هر networkی که به این دسته روتر متصل شود، به ospf وارد میشود. برای روتر تبریز همینکارو کردیم.

```
interface GigabitEthernet0/0/1
ip ospf 200 area 0
```

Router(config)# router ospf < Proccess-ID>
Router(config-router)# router-id <A.B.C.D> [Optional]

Router(config)# interface <type> <>
Router(config-if)# ip ospf <Process-ID> area <AREA ID>

نکته: نحوه دیدن Routing table یک روتر ؟ به عنوان مثال روتر تهران:

```
RTR_TEH#sh 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

     10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
C       10.10.10.0/30 is directly connected, Serial0/1/0
L       10.10.10.1/32 is directly connected, Serial0/1/0
C       10.10.20.0/30 is directly connected, GigabitEthernet0/0/0
L       10.10.20.1/32 is directly connected, GigabitEthernet0/0/0
     192.168.10.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.10.0/24 is directly connected, GigabitEthernet0/0/1
L       192.168.10.1/32 is directly connected, GigabitEthernet0/0/1
O    192.168.20.0/24 [110/65] via 10.10.10.2, 00:48:06, Serial0/1/0
O    192.168.30.0/24 [110/2] via 10.10.20.2, 01:31:31, GigabitEthernet0/0/0
```

نکته۱: خط یکی مونده به آخر : داخل [] عدد اولی AD که ospf ۱۱۰ است . عدد دومی metric است که با توجه به اینکه Gig خروجی کاستش (cost) ۱ و serial خروجی کاستش ٦٤ است، نتیجه میشود ٦٤+۱=٦٥

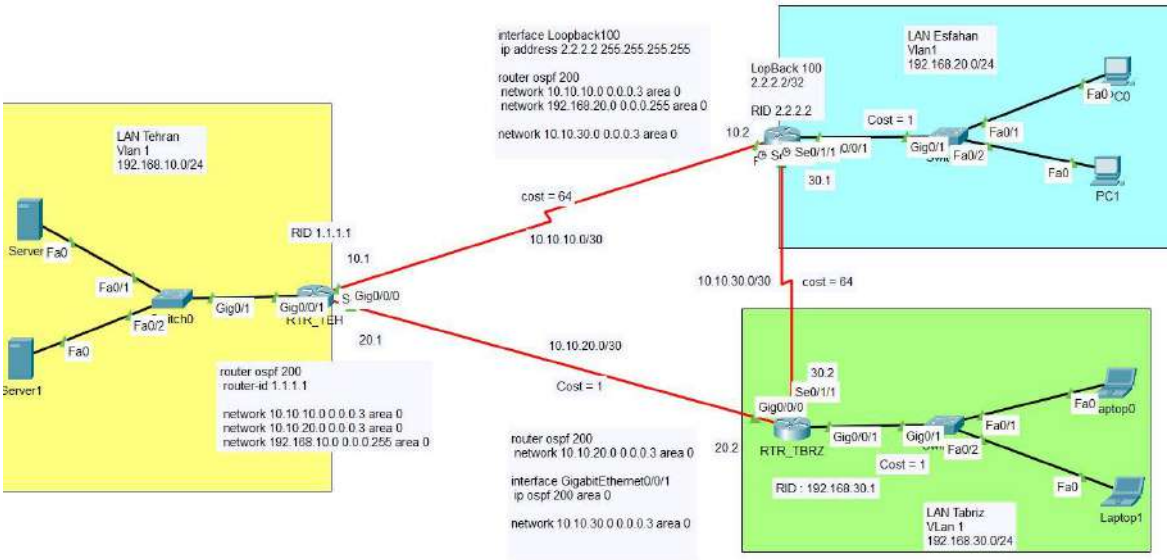
و خط آخر : داخل [] عدد اولی AD که ospf ۱۱۰ است . عدد دومی metric است که با توجه به اینکه Gig خروجی کاستش (cost) ۱ و gigخروجی دومی کاستش همچنین ۱ است، نتیجه میشود ۱+۱=۲

نکته۲: در بعضی از دستگاه‌ها اگر به جای WC-mask از subnet-mask استفاده کنیم، خودش تبدیل به Wc-mask میکند.

نکته۳: نحوه دیدن جدول ospf یک روتر ؟

```
RTR_TEH#sh ip route ospf
O    192.168.20.0 [110/65] via 10.10.10.2, 00:02:19, Serial0/1/0
O    192.168.30.0 [110/2] via 10.10.20.2, 00:01:44, GigabitEthernet0/0/0
```

مثال : ارتباط بین اصفهان و تبریز



در ادامه مثال قبل، ابتدا به برقراری همسایگی اصفهان و تبریز پرداختیم.

حال، هم اصفهان و هم تبریز برای رسیدن به هم دو مسیر دارند. با توجه به metric مسیر، بهترین مسیر(مجموعهcost =>کمترین) برای مسیر هر روتر انتخاب میشود.

O 192.168.30.0 [110/65] via 10.10.30.2, 00:15:53, Serial0/1/1
O 192.168.30.0 [110/66] via 10.10.10.1, 00:15:53, Gig0/0/0

در این مثال راه رسیدن اصفهان به تبریز به دو صورت است. به دلیل اینکه مسیر 30.2 متریک کمتری (64+1=65) نسبت به مسیر 10.1(64+1+1=66) دارد پس مسیر بهتر شناخته می‌شود. به همین جهت فقط این مسیر در جدول روتینگ نشان داده میشود.

```
O    192.168.30.0 [110/65] via 10.10.30.2, 00:15:53, Serial0/1/1
```

نکته۱: اگر در روتر اصفهان interface se 0/1/1 به هردلیلی قطع یا خاموش شود، به سرعت مسیر بعدی جایگزین میشود. همچنین اگر روشن و وصل شود، این اتفاق به سرعت به حالت اول برمی‌گیردد. خوبی ospf این است که برای برگشت به مسیر قبلی recalculator نمی‌کند، چون مسیر Back up را ذخیره کرده است.

نکته۲: برای اینکه یک مسیر را بهتر یا بدتر کنیم که مسیر ترافیک را جابجا کنیم، میتوانیم متریک را تغییر دهیم.

روش اول تغییر BW است. با کاهش BW در نتیجه cost بیشتر میشود و در نهایت metricبالاتر می‌رود (که به سوی بدتر شدن مسیر پیش می‌رود). اما این کار پیشنهاد نمی‌شود. نکته اینکه تغییر BW زیر اینترفیس هیچ تاثیری روی ترافیکی که روی آن اینترفیس عبور می‌کند ندارد، چون صرفا برای control plain است. اما در پروتکل‌هایی که استفاده می‌کنیم مثل stp این BW لحاظ می‌شود . روش دوم تغییر مستقیم همان اینترفیس است. بدانیم که این کار را Localی انجام می‌دهد، یعنی روی روترهای دیگر اعمال نمی‌شود. BW که برای اینترفیس سریال در نظر گرفته شده ۱۵۴۴ هست که با دستور زیر می‌توانیم مشاهده کنیم:

Change Cost of OSPF :

```
R1(config)#interface <type> <>
R1(config-if)#ip ospf cost <1-65535>

R1(config)#interface <type> <>
R1(config-if)#bandwidth <>
```

Change Maximum-Path in ospf (Default 4):

```
R1(config)#router ospf <>
R1(config-router)#maximum-paths <1-32>
```

تغییر BW با دستور زیر :

```
RTR_ESF(config)#Interface serial 0/1/1
RTR_ESF(config-if)#bandwidth 500
```

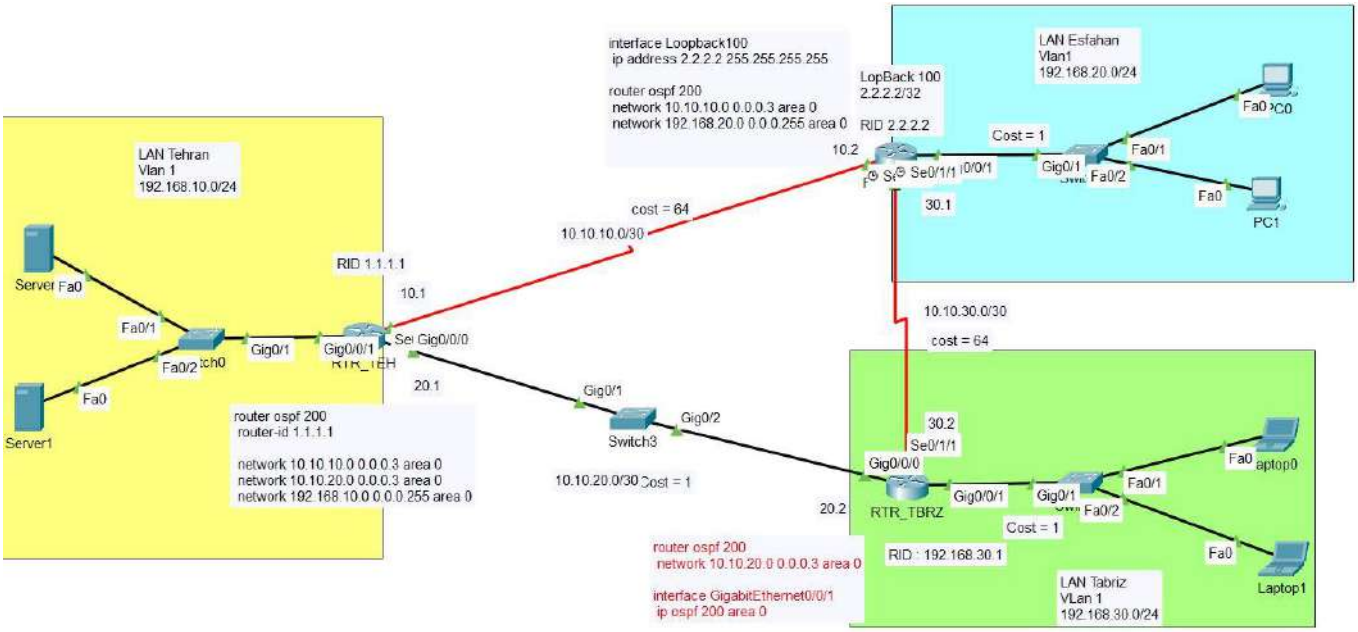
یا تغییر Cost با دستور زیر :

```
TRT_TBRZ(config)#interface serial 0/1/1
RTR_ESF(config-if)#ip ospf cost 100
```

حال با توجه به تغییرات، مسیر مستقیم اصفهان به تبریز با متریک جدید(۱+۱۰۰=۱۰۱) و مسیر اصفهان به تبریز از 10.1 با متریک (64+1+1=66) هستند. با این تفاسیر مسیر backup سابق، به مسیر اصلی تبدیل می‌شود. یعنی اصفهان برای رسیدن به تبریز باید

از تهران عبور کند. **نکته اینکه همانطور که گفتیم این تغییرات localای است، به همین خاطر تبریز برای رسیدن به اصفهان از مسیر 30.1 می رسید، نه از مسیر تهران(مگر اینکه costیا BW آن را تغییر دهیم.

مثال: Dynamic Route **Indirect Topology Change**

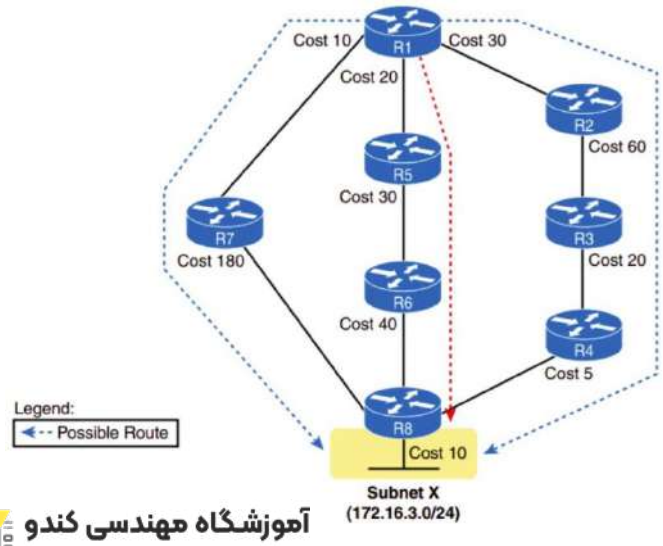


در مثال بالا Routeهای ارتباط بین تهران و اصفهان نوشته شده است(به ازای هر روتر، دو مسیر با اولویت های متفاوت). همانطور که نوشته شده است، در جدول روتینگ فقط اولیت اصلی تا قبل از حذف لینک ارتباطی نمایش داده می‌شود.

روتر اصفهان هنگام قطع راه‌های ارتباطی متصل به خود را متوجه می‌شود و به سرعت نسبت به اصلاح جدول روتینگ (جایگزین کردن روت با اولویت دوم با اولویت اول(چون مسیر از دسترس خارج شده است)) اقدام می‌کند. (direct or indirect).

در حال حاضر مسیر اصفهان به تبریز از تهران است. مسیر تبریز به اصفهان هم direct میباشد. در صورت قطعی بین روتر تهران و سوئیچ، روتر تهران به سرعت متوجه می‌شود، و سریعا مسیر backup را جایگزین می‌کند.

مثال: درجه اهمیت cost در ospf



در ospf، cost خروجی از اینترفیس محاسبه می‌شود.

مثل در شکل روبرو متریک مسیر وسط ۲۰+۳۰+۴۰+۱۰ میباشد.

Table 20-3 Faster Interfaces with Equal OSPF Costs

Interface	Interface Default Bandwidth (Kbps)	Formula (Kbps)	OSPF Cost
Serial	1544 Kbps	100,000 / 1544	64
Ethernet	10,000 Kbps	100,000 / 10,000	10
Fast Ethernet	100,000 Kbps	100,000/100,000	1
Gigabit Ethernet	1,000,000 Kbps	100,000/1,000,000	1
10 Gigabit Ethernet	10,000,000 Kbps	100,000/10,000,000	1
100 Gigabit Ethernet	100,000,000 Kbps	100,000/100,000,000	1

نحوی تبادل اطلاعات Topology چگونه است؟

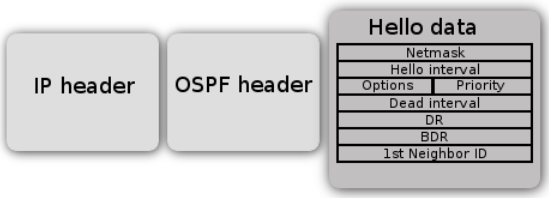
- ***شبکه های Point to Point***
- ***شبکه های Multi Access (Broadcast)***
- شبکه هایNBMA
- شبکه های Point to Multipoint (P2MP)
- شبکه های(Point to Multipoint nonbroadcast (P2MNB

**نکته : از روی نوع لینک امکان تشخیص نوع شبکه فراهم می‌شود. به طور مثال Fastethernet به عنوان یک شبکه Multi Access و Serial به عنوان یک شبکه Point to Point در نظر گرفته می‌شود.

مراحل ایجاد همسایگی :

در OSPF در ابتدا باید با روترهای مجاور همسایه شد و اطلاعات آنها در جدول همسایگی قرار گیرد که به دو دلیل زیر انجام می گیرد:

- از فعال و زنده بودن روتر همسایه مطمئن شود.
- شرایط همسایگی بین دو روتر بررسی شود.



**نکته :تشکیل همسایگی در OSPF توسط بسته های Hello انجام می گیرد. هر 10ثانیه یکبار این بسته ها ارسال می شوند و اگر 40ثانیه (Dead Time)از همسایه خود Hello دریافت نکند همسایه خود را غیرفعال و مرده درنظر می گیرد.

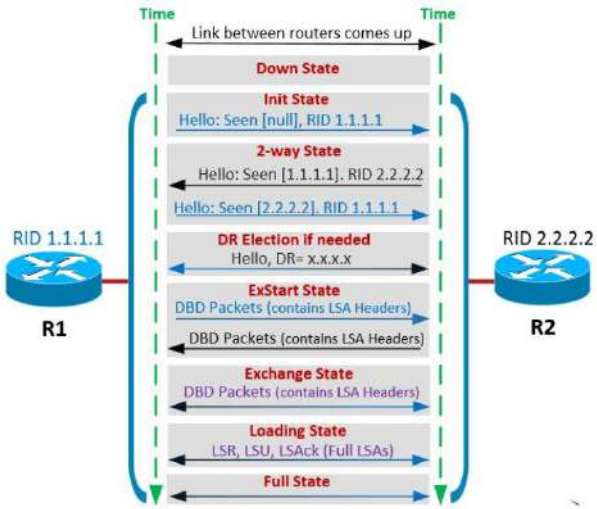
OSPF Network Type	Default HelloInterval	Default RouterDeadInterval
Broadcast	10 seconds	40 seconds
Non-broadcast	30 seconds	120 seconds
Point-to-Point	10 seconds	40 seconds
Point-to-Multipoint	30 seconds	120 seconds
Point-to-Multipoint Non-broadcast	30 seconds	120 seconds
Loopback	N/A	N/A

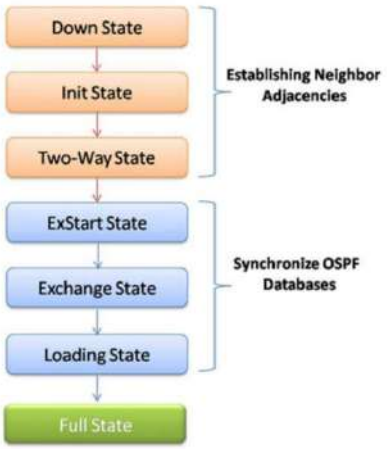
پارامترهایی که برای همسایگی مورد بررسی قرار می گیرد:

Requirement	Required for OSPF	Neighbor Missing if Incorrect
Interfaces must be in an up/up state.	Yes	Yes
Access control lists (ACL) must not filter routing protocol messages.	Yes	Yes
Interfaces must be in the same subnet.	Yes	Yes
They must pass routing protocol neighbor authentication (if configured).	Yes	Yes
Hello and hold/dead timers must match.	Yes	Yes
Router IDs (RID) must be unique.	Yes	Yes
They must be in the same area.	Yes	Yes
OSPF process must not be shut down.	Yes	Yes
Neighboring interfaces must use same MTU setting.	Yes	No
Neighboring interfaces must use same OSPF network type.	Yes	No

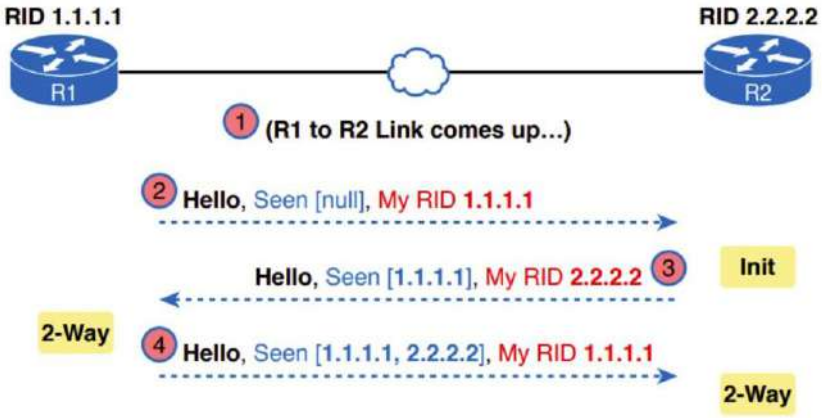
۱. داشتن Hello interval برابر
۲. داشتن Dead interval برابر
۳. داشتن شماره Area یکسان
٤. داشتن Sunbnet mask یکسان
٥. داشتن Subnet number یکسان
٦. Authentication مشابه (احراز هویت)
۷. نداشتن RID برابر
۸. Stub area flag
۹. Down نبودن OSPF
۱۰. ACL نباید بسته‌های مرتبط به Routing را فیلتر کرده باشد.
۱۱. داشتن MTU برابر

OSPF States :





Early Neighbor States :



حالت همسایگی با **down** شروع می‌شود، بدین معنی که دربازه مورد انتظار، بسته hello از همسایه دریافت نشده است (بسته رد و بدل نشده یا اصلا روتر روبرو config نشده). به محض دریافت بسته hello از روتر همسایه (بسته حاوی RID خود و همسایه‌ها)، حالت همسایگی از down به initialized (**init**) تغییر می‌کند.

حالت همسایگی initialized با یک همسایه بدین معنی است که بسته hello از آن همسایه دریافت شده است. یکی از فیلدهای بسته hello، neighbor-list یا لیست همسایه‌هایی است که روی آن لینک، hello از آنها دریافت شده است. اگر بسته hello از همسایه ای دریافت کنیم که در فیلد neighbor-list، نام روتر دریافت کننده hello وجود نداشته باشد، بدین معنی است که روتر همسایه بسته hello ارسالی روتر را دریافت نکرده است. اما چنانچه روتر همسایه نیز بسته hello ارسالی ما را دریافت کرده باشد، آنگاه دو طرف پارامترهای تشکیل همسایگی را که در بالا به آنها اشاره شده است، چک می‌کنند و در صورتیکه این پارامترها بین روترهای همسایه یکسان بوده و یا مطابقت داشته باشد، همسایگی از حالت Init به حالت 2-way تغییر می‌کند.

به عبارت دیگر وقتی حالت همسایگی با روتر همسایه به 2-way تغییر می‌کند که دو طرف همدیگر را شناسایی نموده اند و پارامترهای همسایگی نیز بین آنها مطابقت داشته باشد. همسایگی2-way بین روترهای همسایه شروع پروسه انتقال اطلاعات بین روترهای همسایه است. در این مرحله ارتباط به صورت unicast انجام می‌شود.

حالت های فوق تنها حالت های همسایگی نیستند. از این مرحله به بعد نیز حالت های همسایگی دیگری تا تشکیل همسایگی کامل وجود دارد. اما با توجه به اینکه این حالت‌ها بعد از شروع انتقال اطلاعات اتفاق می‌افتد، آنها را در بخش معرفی خواهیم نمود.

خلاصه ای از حالت‌های همسایگی در OSF تا قبل از انتقال اطلاعات Data base:

حالت همسایگی	توصیف
down	بدین معنی است که در زمان dead time از این همسایه hello دریافت نشده است.
attempt	بدین معنی است که این روتر در حال ارسال hello به همسایه مورد نظر است. این حالت فقط وقتی معنی دارد که همسایگی دستی تعریف شده باشد که در شبکه های از نوع non-broadcast کاربرد دارد و در بخش انواع شبکه ها در ospf در همین فصل در مورد آنها صحبت خواهیم نمود
init	حالت Init بدین معنی است که از این همسایه hello دریافت شده است اما همسایه هنوز از این روتر دریافت نکرده است و یا آنکه پارامترهای همسایگی مطابقت ندارد. اگر پارامترهای همسایگی حالت Init بدین معنی است که از این همسایه hello دریافت شده است اما همسایه هنوز از این روتر دریافت نکرده است و یا آنکه پارامترهای همسایگی مطابقت ندارد. اگر پارامترهای همسایگی مطابقت نداشته باشد، در این حالت به صورت دائمی باقی می ماند مطابقت نداشته باشد، در این حالت به صورت دائمی باقی می ماند
۲way	این حالت همسایگی بدین معنی است که دو روتر همسایه همدیگر را شناسایی نموده اند و پارامترهای همسایگی نیز مطابقت دارد.

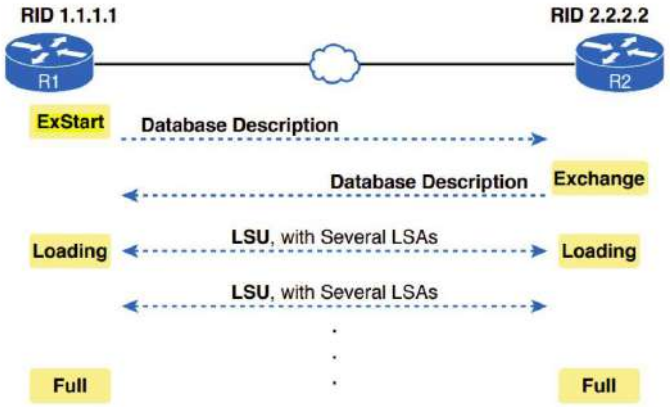
حالت های همسایگی در OSPF تا قبل از انتقال اطلاعات دیتابیس

همانطور که در جدول فوق دیده می شود حالت همسایگی attempt نیز اضافه شده است که فقط وقتی کاربرد دارد که همسایه به صورت دستی تعریف شده باشد. در بخش انواع شبکه ها در OSPF مشاهده خواهیم نمود که در شبکه های از نوع non-broadcast حتما باید همسایگی به صورت دستی تعریف شود. در حالت همسایگی دستی بسته hello به آدرس unicast ارسال می‌گردد (برخلاف معمول که بسته‌های hello به آدرس multicast 224.0.0.5 ارسال می شود).

***نکته: در OSPF زمانیکه روی هر روتری روی هر دست آن همسایگی را فعال می‌کنیم یک224.0.0.5 ip multicast در کنارip unicast یکه ما Set کردیم فعال می‌شود.

Exchange Database:

بعد از فرآیند همسایگی و قبل از Exchange Database، اگر شبکه Broadcast باشد، ابتدا مراحل DR Election و BDR انجام می‌شود، ولی اگر شبکه P2P باشد، مستقیم از همسایگی وارد Exchange database می‌شود.



این توضیحاتی که داده شد، قبل از ExStart است. Exchange Database از Exstart شروع می‌شود. ExStart همان مراحل DBD->LSR->LSU->LSAct است. در مرحله قبل وقتی از روتر مقابل درخواست LSU میشود، مرحله Exchange آغاز میشود. وقتی همه دیتاها و Updateهای روترها به هم Sync شدند و به مرحله Loading رسیدند، همسایگی ما Fullخواهد شد.

توجه:

قبل از انجام exchange Database و انتخابات BDR,DR ، در این مرحله MTU Discovery انجام می‌دهد و MTU مسیر بین دو روتر باید یکسان باشد ، ولی اگر MTU یکسان نباشد، همسایگی برقرار می‌شود و تا مرحلهTwo Way پیش می‌رود اما دیگر قادر به exchange دیتابیس نیستند(همسایگی برقرار میشود، ولی exchange Database انجام نمی‌شود). این کار را بدلیلperformanceانجام می‌دهد، MTU مسیر رادiscovery می کند که بداند سایز دیتابیس‌هایی می‌خواهد بین خود و طرف مقابل جابجا کند ماکزیمم چقدر می‌تواند باشد. اگر یک بسته ای را با یک سایزی ارسال کنیم و طرف مقابل MTU کمتری داشته باشد و در نتیجه MSS آن هم کمتر می‌شود و بخواهد بسته را Segmentation انجام دهد Performance کاهش می‌یابد پس در نتیجه برای

اینکه سایز بسته‌هایی که ما ارسال می‌کنیم برای طرف مقابل با سایز بسته‌هایی که قرار است دریافت کند یکی باشد و نخواهد Segmentationانجام دهد MTU باید یکسان باشد.

معرفی وضعیت های مختف روتر در پروتکل OSPF برای T-Shoot:

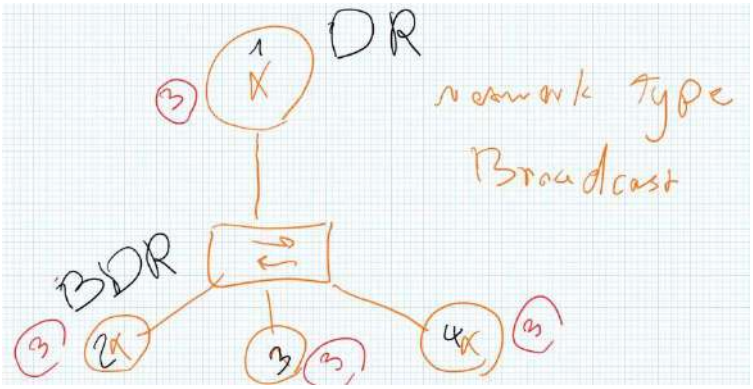
- **Down State**: یعنی همسایگی برقرار نیست. مثلا پیش می‌آید که شما تمام تنظیمات را درست انجام داده‌اید و حتی ping همسایه را هم دارید ولی وضعیت همسایگی برقرار نیست، در این حالت قطعا Hello Packet ها در طول مسیر Drop شده‌اند و رنج Multicast 224.0.0.5باز نیست.
- **Initialize**: یعنی برای اولین بار یک Hello Packet دریافت شده است. پس از اینکه روتر دوم اولین Hello را دریافت کرد، برای فرستنده‌ی آن یک hello از جنس Unicast می‌فرستد تا درخواست همسایگی اجابت شود. به همین علت است که Hello Packet ها نیاز به LSAck ندارند.
- **Two Way**: یعنی هر دو طرف قبول کردند که باهم همسایه باشند.
- **Exstart**: علت استفاده از الویت Router ID در این مرحله، انتخاب شروع کننده ی ارسال DBD است، چون هر دو روتر همزمان نمی توانند برای هم DBD ارسال کنند و یکی باید فرآیند را آغاز کند.
- **Exchange State**: پس از همسایگی نوبت به همگام سازیLSDBها رسیده‌است. حالت Exchange هنگامی است که بالاترین RID شروع به ارسال DBD می کند. هر دو روتر پس از دریافتDBDبرای هم LSAck میفرستند.
- **Loading State**: در این مرحله چک می‌شود که با LSR چه اطلاعاتی را باید درخواست دهد و از LSU دریافت کند. پس از این که هر روتر خلاصه ای از LSDB همسایه اش را دریافت کرد، حال آن Record هایی که ندارد را درخواست می کند.
- **Full**: یعنی LSDB ها هم همگام سازی شده اند.

نکته۱: خلاصه ای از وضعیت LSA ها هر ۳۰ دقیقه یکبار در شبکه ارسال می‌شود. تا هر روتری که دید Record خاصی را ندارد با LSR درخواست کند تا با LSU دریافت کند. وقتی که یک LSA مجددا دریافت می‌شود Life Time آن Refresh می شود.

نکته۲: قبلا گفتیم که برای پیدا کردن بروزترین LSA باید SeqNumber ها چک شود، اما اگرSeqNumber ها برابر باشد، باید CheckSumهای آن ها مقایسه شود و آن LSA ای که عدد CheckSum بالاتری داشته باشد، بروزتر است. اگر CheckSum ها نیز یکی بود، Age Timeبررسی می‌شود که کدام Age کمتری دارد. لازم به ذکر است که SeqNumber یک عدد ۳۲ بیتی است و به صورت هگزادسیمال نمایش داده می شود.

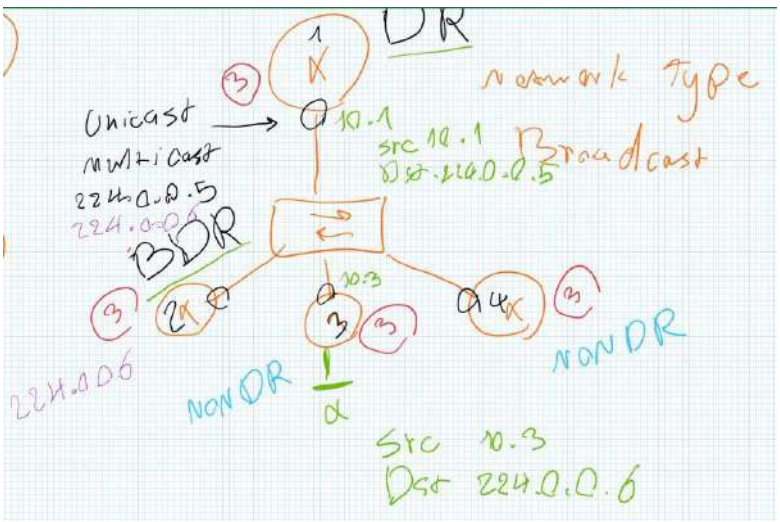
DR & BDR in OSPF:

در شبکه‌هایی که بستر ارتباطی بین روترهای شبکه مشترک(Multi access) است، انجام عمل همسایگی و تبادل اطلاعات بین همه، باعث ایجاد بار زیاد و درگیر کردن تجهیزات می‌شود. برای جلوگیری از این مشکل ، ارتباط و تبادل اطلاعات دو به دو انجام نمی‌شود و یک روتر به عنوان Designated Router (DR) انتخاب می‌شود و وظیفه بروز نگه‌داشتن همه روترها را دارد که اطلاعات را به nonDRها(DRouter) ارسال می‌کند. در این حالت سایر روترهایی که درون این Broadcast Domain هستند، LSDBهای خود را به DR ارسال می‌کنند. DRیک نقطه حساس در شبکه است و اگر این روتر از کار بیافتد(SPOF)، شبکه نیز مختل می شود. برای جلوگیری از این مشکل یک روتر به عنوان Backup Designated Router یا BDR در نظر گرفته می‌شود و به طور دائم ، فعال و زنده بودن DR را چک می‌کند و در صورت بروز مشکل اطلاعات الزام برای DRشدن را دارد. نکته اینکه اگر یک روتر جدید به این سوئیچ متصل شود، با سایر روترها همسایه می‌شود، اما برای تکمیل LSDB خود فقط با DR کار دارد. به طور ساده DRرا به عنوان ریشه یک درخت در نظر بگیرید که همه روترها (شاخه ها) به آن متصل می شوند و از طریق آن اطلاعات را رد و بدل می کنند.



نحوه صحبت کردن با هم :

قبلا گفته شدRIP ورژن یک، اطلاعات را broadcast می‌کرد. یعنی روتری که RIP هم نداشت updateهای RIP را دریافت می‌کرد. در ورژن دو یک multicast ip addressی قرار دادند که بعد از آن برای همه IGPها وجود داشت. همچنین گفتیم در OSPF وقتی برای هر دست روتر همسایگی را فعال میکنیم (فارغ از Traditionalیا explicit)، در کنار IP unicastای که ما قرار دادیم، یک IP multicast 224.0.0.5 نیز فعال می‌شود. در کل هر اینترفیس روتری که ospf فعال می‌شود، در یک multicast groupی قرار می‌گیرند که این IP multicast روی آنها فعال است.



حال فرض می‌کنیم روتر۳ یک network a به خود متصل است. به عنوان مثال می‌خواهد به روترهای دیگر خبر دهد که network a قطع شده است. اگر این روتر بخواهد اطلاعاتش را به 224.0.0.5 ارسال کند، باز همان مشکل شلوغی و... رخ می‌دهد و اطلاعات به دست همه می‌رسد. نکته اینکه در networkهای broadcast در کنار ip224.0.0.5، ip 224.0.0.6 در روترهای DR و BDR ایجاد می‌شود. به همین خاطر از src10.3 اطلاعتش به DST 224.0.0.6 که فقط DR و BDR عضوش هستند می‌رسد. (نکته اینکه BDR به دلیل Sync بودن با DR، فقط گوش میکند و کاری نمی‌کند). سپس DR بعد از دریافت Updateها ، از Src10.1 به DST 224.0.0.5 اطلاعات را به non-DRها (Other DR) ارسال می‌کند.

M1 = 224.0.0.5 All OSPF Enabled Interface
M2 = 224.0.0.6 DR/BDR

**نکته: بر خلاف شبکه های Broadcastی، در شبکه های Point to Point مانند Serial نیاز به DR و BDR نیست(اما در صورت نیاز قابل تغییر هستند). همچنین در بین ارتباط سریال نمیتوان Swt گذاشت.

```
RTR_TBRZ#sh ip os interface gigabitEthernet 0/0/0

GigabitEthernet0/0/0 is up, line protocol is up
  Internet address is 10.10.20.2/30, Area 0
  Process ID 200, Router ID 192.168.30.1, Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State DR, Priority 1
```

```
RTR_ESF#sh ip ospf interface serial 0/1/1

Serial0/1/1 is up, line protocol is up
  Internet address is 10.10.30.1/30, Area 0
  Process ID 200, Router ID 2.2.2.2, Network Type POINT-TO-POINT, Cost: 200
  Transmit Delay is 1 sec, State POINT-TO-POINT,
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
```

** نکته: دستور نمایش فقط قسمت ospf روتر در eve :

RTR#show run | section router ospf

```
RTR4#sh run | section router ospf
router ospf 100
router ospf 300
 router-id 4.4.4.4
 network 192.168.1.0 0.0.0.255 area 0
```

نکته:

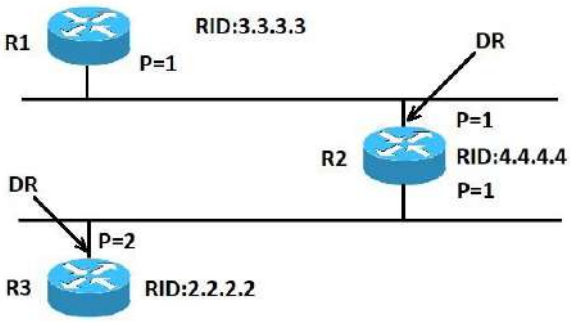
RTR2(config-router)#network 0.0.0.0 0.0.0.0 area 0 همسایه شو هر آی پی داری که روهرچیزی

این روش زیاد مناسب نیست و سطح امنیت پایینی دارد، زیرا اگر یک روتر دیگر اضافه کنیم آن هم می‌تواند همسایه شود، اگر طرف مقابل هکر باشد بسته های hello ارسالی را دریافت می‌کند و می‌تواند روی روتر خود ospf اجرا کند و دیتابیس را دریافت کند و توپولوژی شبکه ما را بدست بیاورد.

نحوه انتخاب DR و BDR در OSPF :

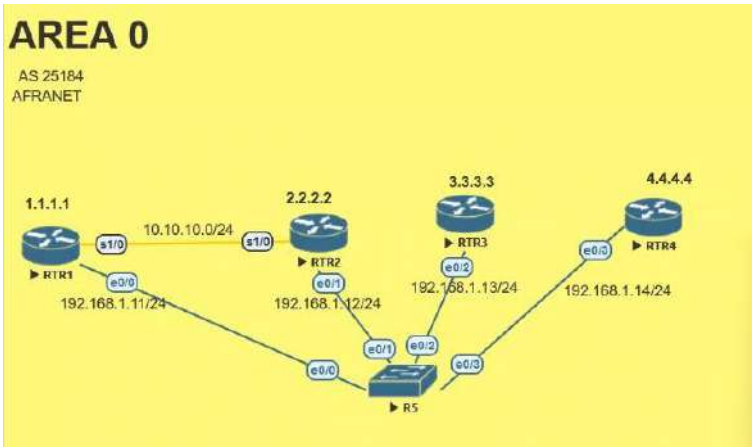
```
DR-Election
============================
1 – Highest OSPF Priority (Def. = 1)
2 – Highest OSPF Router-ID
```

انتخاب DR و BDR از طریق پروتکل hello انجام می‌شود. بسته‌های Hello از طریق بسته‌های multicast در هر ناحیه مبادله می‌شوند. روتری که بیشترین **OSPF priority** را در یک ناحیه دارد به عنوان روتر DR در آن ناحیه انتخاب می‌شود. فرآیند مشابهی نیز برای انتخاب روتر BDR تکرار می‌شود. در صورت تساوی اولویت‌ها در روترها، روتری که بیشترین **RID** را دارد، پیروز خواهد شد. اولویت(Priority) OSPF برای اینترفیس به صورت پیش فرض برابر با ۱ است.



در تصویر روبرو روترهای R1 و R2 اولویت های یکسانی دارند، اما RID مربوط به روتر R2 بیشتر است. در نتیجه در آن ناحیه روتر R2به عنوان DR انتخاب می شود. روتر R3 نسبت به روتر R2 از اولویت بالاتری برخوردار است، در نتیجه در آن ناحیه روتر R3 به عنوان DR انتخاب می شود.

مثال: بررسی انتخاب DR و BDR




```
RTR1#sh ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
2.2.2.2           1   FULL/BDR        00:00:33    192.168.1.12    Ethernet0/0
3.3.3.3           1   FULL/DROTHER    00:00:33    192.168.1.13    Ethernet0/0
4.4.4.4           1   FULL/DROTHER    00:00:33    192.168.1.14    Ethernet0/0
2.2.2.2           0   FULL/           00:00:31    10.10.10.2      Serial1/0
```

با دستور show ip ospf neighbor ابتدا همسایگی را مشاهده می‌کنیم. توجه کنید که priority سریال را صفر قرار داده است (مابقی یک، چون ارتباط مابقی Rj45 است.) پس ما اگر ما نخواهیم بین دو روتر DR BDR Election انجام شود، یکی از راه‌ها این است که میتوانیم Priority دو طرف را صفر قرار دهیم. یا network را از broadcast به Point to point تغییر میدهیم. (چون یکی از دلایل دیر Up شدن اینترفیس، همین DR BDR election است، می‌توان صرف نظر کرد. مثلا بین روتر با ارتباط فیبر).

Change Priority of interface :
R1(config)#interface <type> <>
R1(config-if)#ip ospf priority <1-256>

Or

```
R1R10(config if)#ip ospf network point to point
```

در مثال بالا، RTR1 را به عنوان DR و RTR2 را به عنوان BDR نشان داده شده است. سوال: مگر بنا نبود با Priority یکسان، آن روتری بشود DR که RID بیشتری داشته باشه؟ الان باید RTR4 بشود DR و RTR3 بشود BDR. چه شد پس ؟

نکته اینجاست کهDR BDR Election قابلیت مقایسه ندارند. یعنی اگر روتری شد DR و روتر دیگری به عنوان BDR انتخاب شدند، ولی در ادامه روتری اضافه شد که Priority یا RID بیشتری داشت، اینطور نیست که DR و DBR تغییر کنند!!!! در کل هر روتری به عنوان DR و DBR انتخاب شوند، تا زمان Down شدن باقی می‌مانند.

پس دلیل اینکه RTR1 شده DR و DBR RTR2 ، به خاطر این است که درابتدا از این روترها شروع به config زدن کرده‌ایم. حال اگر بخواهیم DR BDR Election واقعی (براساس Priorityو RID) انجام شود، باید Ospf یکبار Down و Up شود.

#Router ospf <>
#Shutdown
#No shut down

```
RTR1(config)#router ospf 25184
RTR1(config-router)#
RTR1(config-router)#
RTR1(config-router)#
RTR1(config-router)#shu
RTR1(config-router)#shutdown
```

چون ospf روتر یک را up و Down کردیم، DR از روی این روتر برداشته شد و به BDR (که RTR2 بود)تحویل داده شد. حال RTR4 به دلیل بالا بودن RID به عنوان BDR انتخاب شده است. مابقی روترها به عنوان nonDR انتخاب شده اند.

```
RTR1#sh ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
2.2.2.2           1   FULL/DR         00:00:36    192.168.1.12    Ethernet0/0
3.3.3.3           1   2WAY/DROTHER    00:00:31    192.168.1.13    Ethernet0/0
4.4.4.4           1   FULL/BDR        00:00:32    192.168.1.14    Ethernet0/0
2.2.2.2           0   FULL/  -        00:00:32    10.10.10.2      Serial1/0
```

نکته: این روش توصیه نمیشود، بهتر است همسایگی (neighbor) را Up و Down کنیم.

به همین خاطر، در RTR2 دستور clear ip ospf <> process را می‌زنیم. در این حالت RTR4 که BDR بود می‌شود DR و RTR3 که نسب به بقیه RID بیشتری دارد، به عنوان DBR انتخاب می‌شود.

```
Neighbor ID     Pri   State           Dead Time   Address         Interface
2.2.2.2           1   2WAY/DROTHER    00:00:39    192.168.1.12    Ethernet0/0
3.3.3.3           1   FULL/BDR        00:00:37    192.168.1.13    Ethernet0/0
4.4.4.4           1   FULL/DR         00:00:36    192.168.1.14    Ethernet0/0
2.2.2.2           0   FULL/  -        00:00:36    10.10.10.2      Serial1/0
```

نکته۱: اصولاً روتری را DR قرار می‌دهند که Performance و ظرفیت و ... بالایی دارند. همچنین روتری که پیشفرض به عنوان DR انتخاب می‌شود را معمولاً دست نمی‌زنند.

** نکته۲: مقدار priority برابر با ۰ ، نشان دهنده ی آن است که آن اینترفیس به عنوان DR یا BDR انتخاب نشده است (DR BDR Election صورت نمی‌گیرد)

نکته۳: زمانی DR و BDR حضورشان نقض می‌شود(یعنی باید DR و DBR جایگزین انتخاب شود) که همسایگی روترها با روتر DR از دست برود (از دست دادن یک بسته Hello ملاک نیست و حتماً باید همسایگی به طور کل قطع شود) .

Metric calculation in OSPF :

پروتکل مسیریابی OSPF نیز همانند همه دیگر پروتکل‌های مسیریابی ترافیک را همواره روی بهترین مسیر ارسال می‌کند. بهترین مسیر در همه پروتکل‌های مسیریابی مسیری است که متریک آن کوچکتر باشد. معیار متریک در OSPF پهنای باند همه لینک های مسیر است. به عبارت دیگر پهنای باند همه لینک‌های مسیر در متریک نهایی OSPF تاثیرگذار است.

بدیهی است که معیار متریک در OSPF بهترین معیار نیست. در پروتکل EIGRP فقط کمترین پهنای باند مسیر در متریک نهایی EIGRP تاثیر گذار است که نسبت به OSPF که پهنای باند همه لینک‌های مسیر را مد نظر قرار می‌دهد، واقعی‌تر است. زیرا پهنای باند واقعی مسیر شما، کمترین پهنای باند مسیر خواهد بود.

اما پهنای باند چگونه در متریک نهایی محاسبه می‌شود؟ در OSPF متریک برابر با جمع cost همه لینک های مسیر است. cost هر لینک نیز رابطه معکوس با پهنای باند آن لینک دارد. به عبارتی هر چه پهنای باند لینک بیشتر باشد، costآن نیز کمتر خواهد بود. به صورت پیش‌فرض مقدار cost هر لینک بر اساس فرمول زیر محاسبه می‌شود که در آن پهنای باند مرجع ۱۰۰ Mbpsاست.

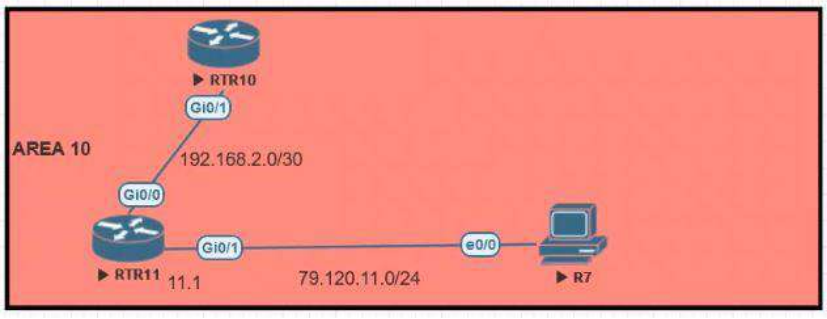
$$\text{Default Cost} = \frac{10^8}{BW}$$

به صورت پیش فرض لینکی که پهنای باند آن ۱۰۰ Mbpsاست، مقدار cost آن ۱ خواهد بود. لینکی با پهنای باند ۱۰ Mbpsدارای cost با مقدار ۱۰ است cost .لینک‌هایی که پهنای باند آن 1Gbpsو یا ۱۰ Gbpsاست، اعشاری خواهد شد که البته در این صورت cost آن ۱ در نظر گرفته می‌شود. پیشنهاد می‌شود. برای رفع این مشکل در شبکه‌هایی که لینک‌های با پهنای باند ۱ Gbpsو یا بالاتر وجود دارد، پهنای باند مرجع را از 100Mbpsبه عددی بالاتر مثلا ۱ Gbpsو یا ۱۰ Gbpsتغییر دهیم.

برای تغییر پهنای باند مرجع از دستور auto-cost reference-bandwidth mbps در محیط router ospfاستفاده کنید. فقط توجه کنید که در صورت تمایل به تغییر پهنای باند مرجع، در همه روترهای شبکه این تغییر را اعمال نمایید.

```
R1(config-router)#auto-coust refrence-bandwidth REF-BW[M}
```

مثال :




```
O        79.120.11.0 [110/2] via 192.168.2.2, 00:00:02, GigabitEthernet0/1
```

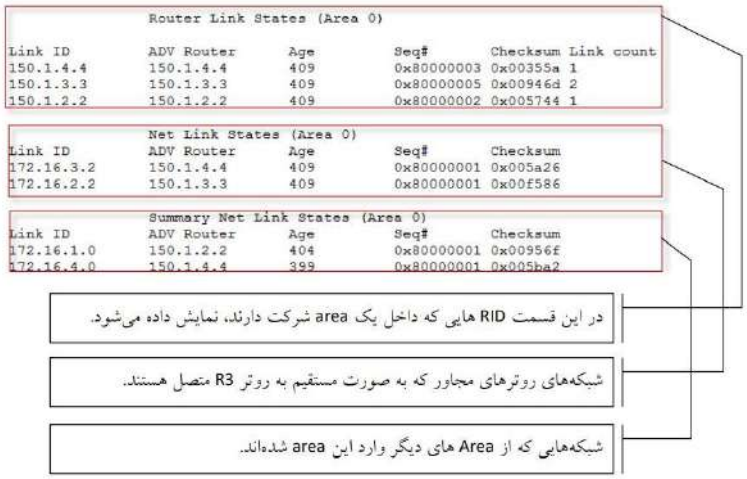
در ارتباطات گیگ، چون مبنای متریک بر حسب fastethernet در نظر گرفته شده، همان ۱۰ به توان ۸ میباشد. برای تغییر آن از دستور زیر استفاده میکنیم. در این مثال ما معیار متریک را به 10^{10} تغییر میدهیم.

```
RTR11(config-router)#auto-cost reference-bandwidth 10000
```

```
79.120.11.0 [110/[illegible]] via 192.168.2.2, 00:00:22, GigabitEthernet0/1
```

نکته: از ارتباطات Fast به بالا متریک را تغییر میدهیم تا مسیر بهتر و بدتر را تشخیص بدهند.

دستورShow IP OSPF Database:

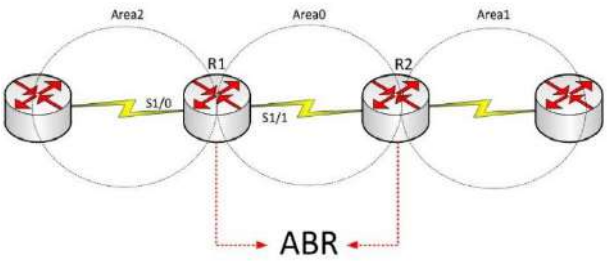


دستورshow ip ospf border-routers :

این دستور، روترهای همسایه را به ما نشان می‌دهد و IP address آنها را مشخص می‌کند.

```
Router#show ip ospf border-routers
OSPF Process 10 internal Routing Table
Codes: i - Intra-area route, I - Inter-area route
i 150.1.2.2 [1] via 172.16.2.1, FastEthernet0/0, ABR, Area 0, SPF 1
i 150.1.4.4 [1] via 172.16.3.2, FastEthernet0/1, ABR, Area 0, SPF 1
```

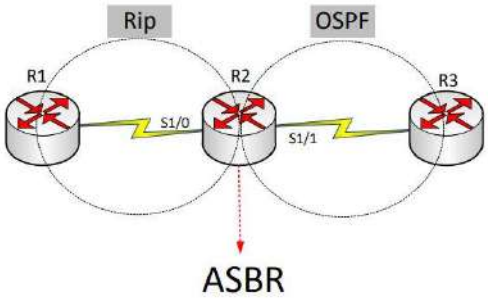
روتر(ABR (Area Border Router:



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 زیر توجه کنید. همانطور که در شکل زیر مشاهده می‌کنید، روترهای R1وR2 روترهایی هستند که بین دو area قرار دارند و کار انتقال را انجام می‌دهند که به این روترها، روترهای ABR گفته می‌شود.

روتر(Autonomous System Border Router) ASBR:

به روتری که بخشی از اطلاعات را می‌خواهد از خارج از شبکه OSPF وارد کند ASBRگویند.



OSPF LSA Type:

شماره LSA	نام LSA	ارسال کننده LSA	محتویات LSA	تعداد LSA	محدوده ارسال LSA	شناسه LSA یا Link ID
Type 1	Router	همه روترها	جزئیات لینک	هر روتر یک LSA	داخل Area	router-id روتر ارسال کننده
Type 2	Network	روتر DR	جزئیات شبکه Transit	هر شبکه یک Transit LSA	داخل Area	آدرس IP روتر DR
Type 3	Summary	روترهای ABR	مسیر شبکه های خارج از Area	هر شبکه یک LSA	بین Area ها	آدرس شبکه
Type 4	ASBR Summary	روترهای ABR	دسترسی به ASBR	هر ASBR یک LSA	غیر Area Backbone	router-id روتر ASBR
Type 5	External	روتر ASBR	مسیر شبکه های خارج از OSPF	هرشبکه یک External LSA	کل شبکه OSPF	آدرس شبکه خارجی
Type 6	Group Membership	مربوط به پروتکل MOSPF است. در روترهای سیسکو پشتیبانی نمی شود.				
Type 7	NSSA External	روتر ASBR در NSSA Area	مسیر شبکه های خارج از OSPF	هرشبکه یک External LSA	کل شبکه OSPF	آدرس شبکه خارجی

Type 8	Link Local in OSPFV3	همه روترها	شبکه های متصل به لینک	هر لینک یک LSA	داخل لینک	Interface-Id
Type 9	Intra-Area-Prefix in OSPFV3	همه روترها	شبکه های داخل Area	هر روتر یک LSA	داخل Area	Refrence to LSA Type 1/2

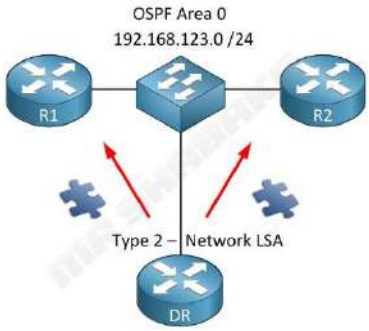
Router LSA.1 :

Type1 از LSA است که توسط روترها ردوبدل می‌شود و مربوط به همان منطقه است (این LSA همان LSAی است که همه روترها ایجادش می‌کنند، فارغ از نوع Area). روتر شامل وضعیت لینک، Router ID، اطلاعات IP و وضعیت فعلی رابط است. اگر روتر به چندین منطقه متصل باشد، Type1 جداگانه LSA رد و بدل می‌شود. این نوع LSA همچنین نشان می‌دهد که آیا هر پیوند یک اتصال-point-to-pointاست، اتصال به یک شبکه حمل و نقل (transit network)، اتصال به stub area یا پیوند مجازی virtual link است.

Link ID	Description	Link Type
Neighbor router ID	Point to Point Connection to another router	1
IP address of DR	Connection to transit network	2
IP Network	Connection to Stub network	3
Neighbor router ID	Virtual Link	4

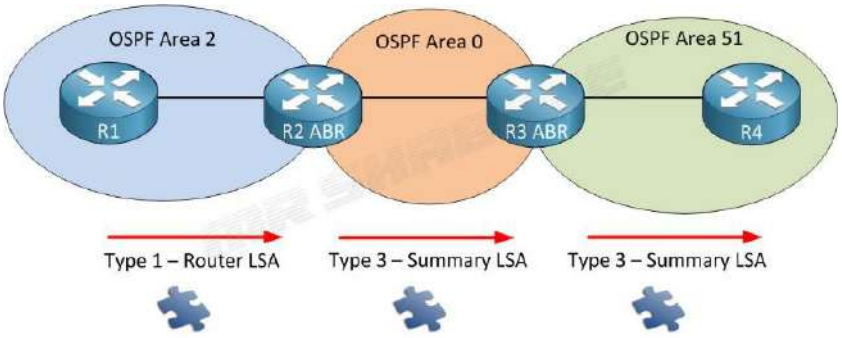
Network LSA .2 :

این نوع Type2 LSA است که توسطDR فقط به سایر روترهای موجود در همان Area (broadcast or multi-access network) ارسال می‌شود. اینها شامل اطلاعاتآیپیDR,BDRو همچنین وضعیت روترهای دیگری هستند که بخشی از همان شبکه هستند. به یاد داشته باشید_ DRمسئول توزیع اطلاعات مسیریابی به سایر روترهای موجود در همان منطقه broadcast area است. نکته اینکه هرگز این LSA از Areaخارج نمی‌شود.



Summary LSA .3 :

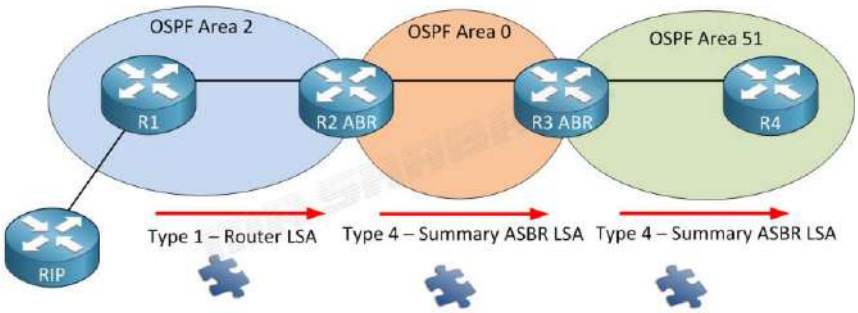
این یک نوع Type3 LSA است که توسط ABRدر مناطقی غیر از محل زندگی تولید می‌شود(multi areaها). پایگاه داده توپولوژیکی که ABR از مناطق دیگر دریافت می کند، Backbone Areas تزریق می‌شود. این شامل اطلاعات IP و RID ازABRی است که این LSAرا تبلیغ می‌کند. در کل اگر ABR بخواهد Updateها و Area regular را به Backbone area برساند از این LSA استفاده می‌کند.



4. Summary ASBR LSA :

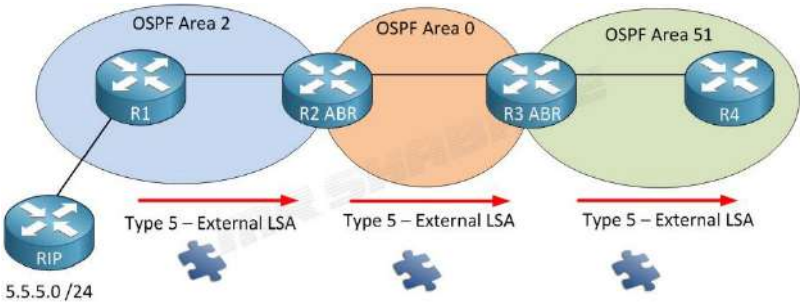
ABR(Area Border Routers) این نوع LSA را به سمت منطقه دیگری غیر از منطقه ای که در آن تولید شده است ارسال می‌کند .این LSAها توسط ABR تولید می‌شوند تا مسیر رسیدن بهASBRرا به دیگران بگویند. در این مثال ما R1 را داریم که در حال توزیع مجدد اطلاعات از روتر RIP به OSPF است. این باعث می شود R1 به یک ASBR تبدیل شود.

آنچه اتفاق می‌افتد این است که R1 کمی در LSAروتر قرار می‌گیرد تا خود را به عنوان ASBR معرفی کند. هنگامی که R2 که یک ABRاست این LSA روتر را دریافت می کند، یک LSA نوع ٤ ایجاد می کند و آن را به Area 0 می رساند. این LSA همچنین به سایر مناطق که مورد نیاز است ارسال می‌شود و بنابراین تمام روترهای OSPF می دانند که کجا ASBR را پیدا کنند.



External LSA.5

این LSA ها توسط ASBR برای تبلیغ مسیرهای AS(Autonomous System)دیگر به غیر از OSPFتولید می شوند. مسیرها را به مقصد خارج از AS توصیف می‌کند. در شکل زیر توپولوژی مانند قبل است اما رنج IP 5.5.0/24 را به روتر RIP خود اضافه کردیم. این رنج IPدر OSPF توزیع می‌شود . روتر R1 یا همان ASBR از این امر مراقبت کرده و یک LSA نوع ٥ برای این امر ایجاد می‌کند. فراموش نکنید که برای یافتن R1 هنوز به LSA نوع ٤ نیاز داریم. اگر تاکنون redistribution با OSPF را امتحان کرده‌اید، ممکن است ورودی های O E1 یا E2 را دیده باشید. این ها همان External LSA هستند.

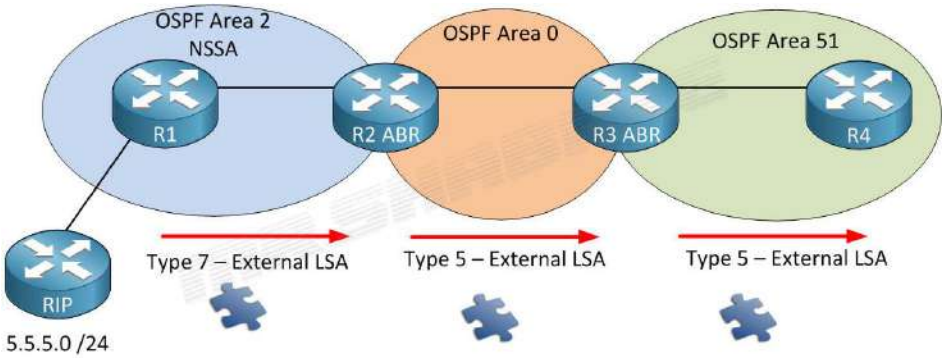


Multicast OSPF LSA:_6

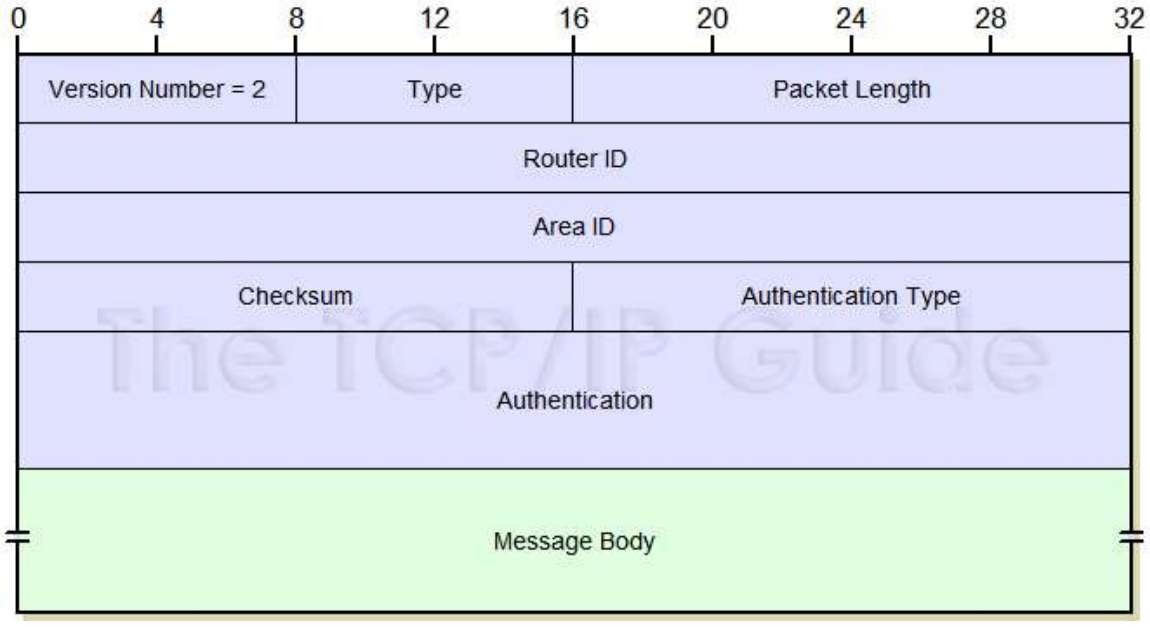
از انواع LSA در OSPF است که این LSA در تجهیزات سیسکو دیگر کاربرد آنچنانی ندارند و انتظار می‌رود که در آینده‌ای نه چندان دور این LSA منسوخ شود. این LSA برای Multicast OSPF (MOSPF) طراحی شده است. پروتکلی که از multicast routing در OSPFپشتیبانی می‌کند.

Not-so-stubby area LSA:_7

NSSA areaها اجازه کار به type 5 external LSA ها نمی‌دهند. در این توپولوژی همچنان R1 بعنوان ASBR اطلاعات مسیرها را از RIPبه داخل OSPF وارد می‌کند. از آنجایی که type 5 اجازه کار ندارند، از type 7 استفاده می کنیم. سپس R2 این Type 7را به Type 5تبدیل کرده و به سایر area ها ارسال می کند.

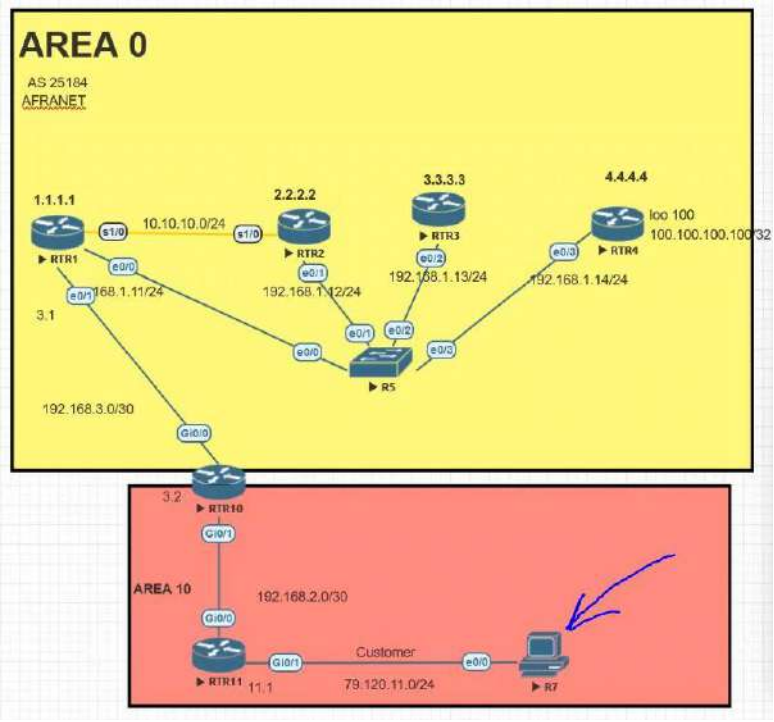


OSPF Header :



** نکته: ospf نسبت به Area خودش Topologyها را بلد است، و از طریق ABR است که networkها را بلد است.

ospf authentication :



در سناریوی روبرو، R7 به عنوان مشتری، اگر بخواهد کارهای خرابکارانه انجام دهد، می‌تواند به همه Topologyهای همه Area دست پیدا کند. برای جلوگیری از این کار، اولین راهکار تنظیمات ospf authentication است.

انواع احراز هویت در **OSPF** :

به صورت کلی دو حالت احراز هویت در OSPF وجود دارد:

Type1: در این روش از احرازهویت که از آن به عنوان Simple Authentication نیز یاد می‌گردد، احراز هویت به صورت غیرامن و تنها به صورت Clear Text انجام خواهد گرفت.

Type2: در این روش، احراز هویت OSPF با رمزنگاری MD5 انجام خواهد شد.

Two types of authentication can be used:

1. **clear text authentication** – clear text passwords are used

Router(config-if)#ip ospf authentication-key PASSWORD
Router(config-if)# ip ospf authentication

2. **MD5 authentication** – MD5 authentication is used. This type of authentication is more secure because the

Router(config-if)# ip ospf message-digest-key <> md5 <VALUE>
Router(config-if)# ip ospf authentication message-digest

به صورت پیش‌فرض هیچ احرازهویتی در OSPF انجام نمی‌گیرد. باید دقت داشت چنانچه قصد استفاده از احراز هویت در OSPFرا داریم، روترها باید بر سر نوع احراز هویت اتفاق نظر داشته باشند. این قابلیت وجود دارد که بنا به نیاز یکی از مکانیزم‌های احراز هویت را فقط روی یکی از اینترفیس‌های روتر فعال نمود تا احراز هویت OSPF تنها بر روی یک اینترفیس انجام پذیرد. همچنین این نکته حائز اهمیت است، چنانچه احراز هویت را به صورت عمومی فعال نمایید و در عین حال بر روی اینترفیس هم

احراز هویت فعال شود، اولویت با تنظیمات اینترفیس خواهد بود. همواره به دلیل رمزنگاری استفاده از احراز هویت Type2 که از MD5 بهره می‌گیرد، پیشنهاد می‌شود.

در مثال بالا ما میدانیم میخواهیم بین RTR10 و RTR11 همسایگی برقرار شود، ولی نمیخواهیم RTR11 با R7 همسایه باشد تا در معرض حملات خرابکارانه قرار بگیرد. پس عملیات رمزگذاری بین RTR11 و R7 فنی است ولی منطقی نیست.

از طرفی ما نمیتوانیم g0/1 را از ospf حذف کنیم، چون شبکه باید از این network شناخت داشته باشد. همانطور که میدانیم برای برقراری همسایگی، دو طرف بسته های hello ارسال می‌کنند. اگر ما جلوی ارسال hello از RTR11 به R7 را بگیریم مشکل حل می‌شود. پس به router ospf <> می‌رویم و با دستور زیر می‌گوییم که نسبت به این اینترفیس (logical یا physical) خنثی (Passive) باش. حال از طرف R7 برای برقرای همسایگی Hello ارسال می‌شود ولی از RTR11 جواب برای همسایه شدن دریافت نمی‌کند.

```
RTR11(config)#router ospf 25184
RTR11(config-router)#
RTR11(config router)#
RTR11(config-router)#
RTR11(config-router)#
RTR11(config-router)#pas
RTR11(config-router)#passive-interface g 0/1
```

پس بهتر است بجای Authentication ، از این روش استفاده کنیم.

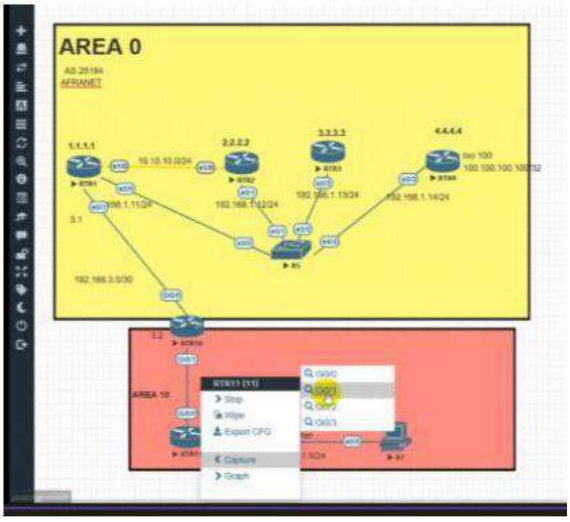
نکته۱: شاید این دستور برای اینترفیس‌هایی که نمی‌خواهیم بسته Hello ارسال شوند زیاد باشد. برای رفع این مشکل، می‌توانیم همه اینترفیس ها را" Passive به غیر از فلان اینترفیس در نظر بگیریم". طبق دستور زیر : دراین دستور گفته ایم که همه اینترفیس‌ها به غیر از g0/0 باید Passive باشند.

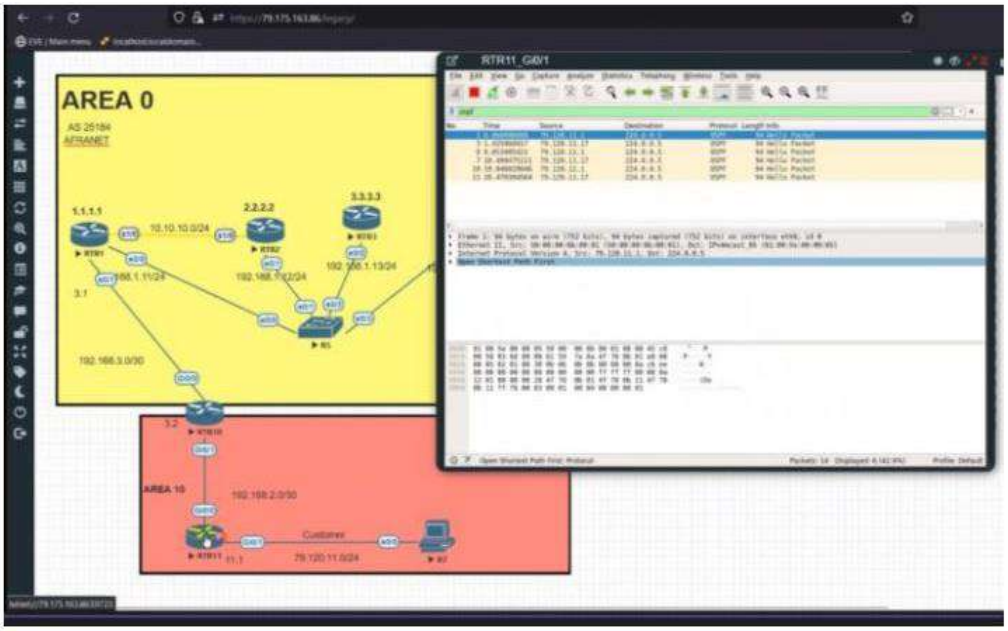
```
RTR11(config router)#no passive interface g 0/0
```

نکته۲: دستور برگرداندن به حالت اول :

```
RTR11(config-router)#passive-interface defau|t
```

کپچر کردن یک اینترفیس با استفاده از نرم افزار**Wireshark** در **Eve** :

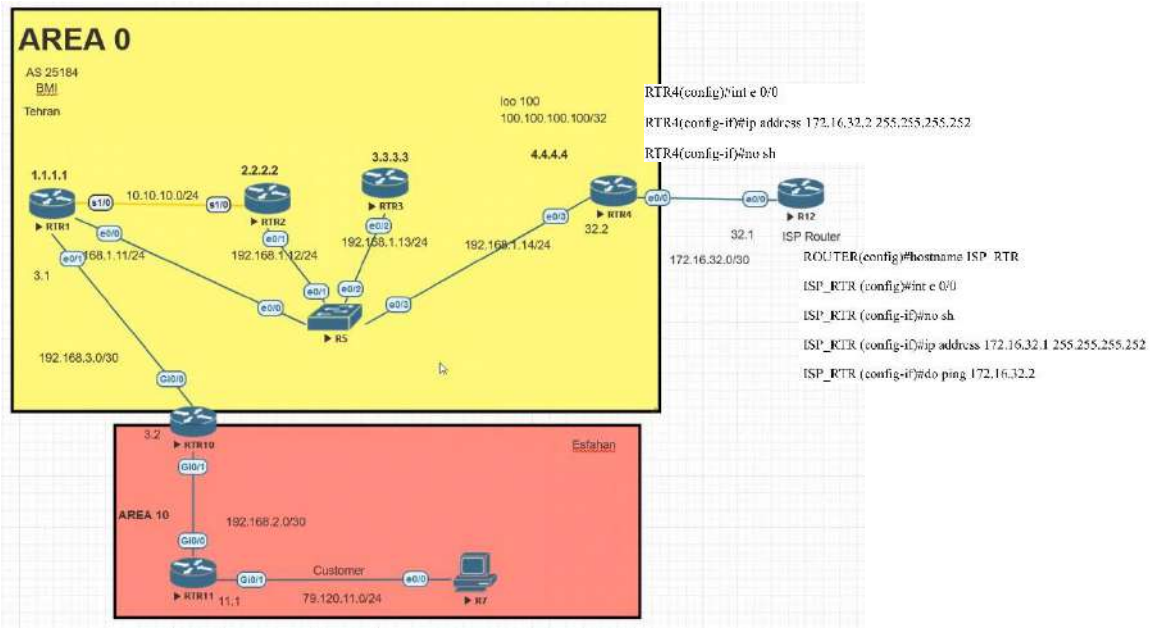




Default Routes:

اگر روتر برای بسته اطلاعاتی که به دستش می رسد مسیر مشخصی نداشته باشد، بسته را برایDefault Route ارسال می‌کند (البته اگر در روتر، Default Route پیکربندی شده باشد).

مثال : در این مثال می‌خواهیم شبکه Enterpriseی را به یک Provider متصل کنیم.



ایجاد یک default route : RTR4(config)#ip route 0.0.0.0 0.0.0.0 172.16.32.1 name TO_PROVIDER

بدان معناست که RTR4 از طریق جدول مسیریابی، مسیرهای استاتیک و داینامیکی که می‌داند را مسیریابی می‌کند و مسیرهایی که نمی‌شناسد را از default route استفاده می‌کند که مسیرش را تکمیل کند.

```
S*      0.0.0.0/0 [1/0] via 172.16.32.1
```

نکته: روتری که به شبکه خارجی متصل شده، **edge** شبکه می‌باشد (جایی که سرویس را به یوزر delivere می‌کنیم یا به شبکه دیگری وصل می‌شویم لبه شبکه می‌گویند)

توجه: در این سناریو، فرض کنید صدتا روتر داریم، به دلیل اینکه خود روترها مستقیم با Provider ارتباط نداشتند، باید به تک تک روترها می‌گفتیم Default Route را به RTR4 بده ، RTR4 هم از طریق Default Route به provider میرساند. که این کار مشکل است(ما از رفتار Dynamic استفاده میکنیم که رفتارهای Static را کنار بگذاریم.)

برای اینکار باید روتر Edge (RTR4) به بقیه اعلام کند که به یک شبکه دیگر وصل می‌باشد و ارتباطش از طریق default routeمی‌باشد، که اگر روتری برای مسیریابی به سمت مقصدی که در جدول مسیریابی وجود نداشت ، به این روتر بسپارد. با این default route می‌توانند match شوند و دیگر نیاز نیست روی همه روترها default route بصورتی دستی inject شود. RTR4 با LSA Type5 به بقیه روترها می‌فهماند که چنین Defaul Routeی دارد.

```
RTR4(config)#router ospf 200
RTR4(config-router)#default-information orginate
```

```
Router(config)# router ospf < Proccess-ID>
Router(config-router)# default-information orginate [always]
```

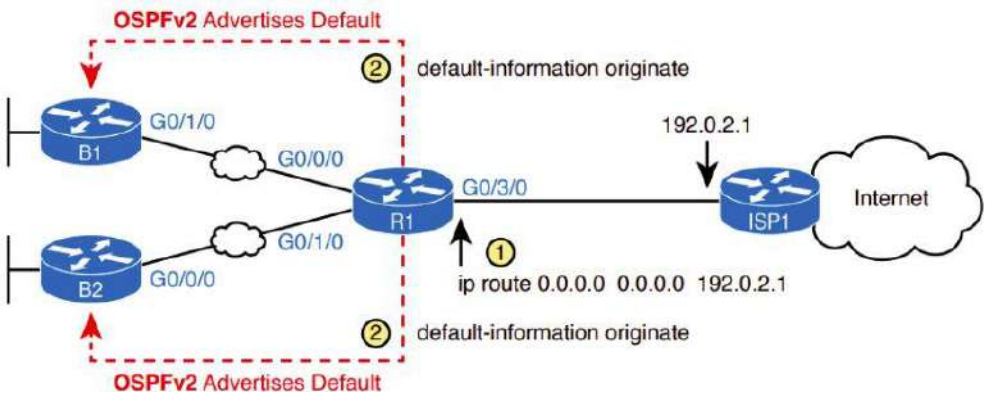
حال با دستور show ip route ، در همه روترها مسیریابی زیر دیده می‌شوند.(فقط اینترفیس‌های خروجی متفاوت است)

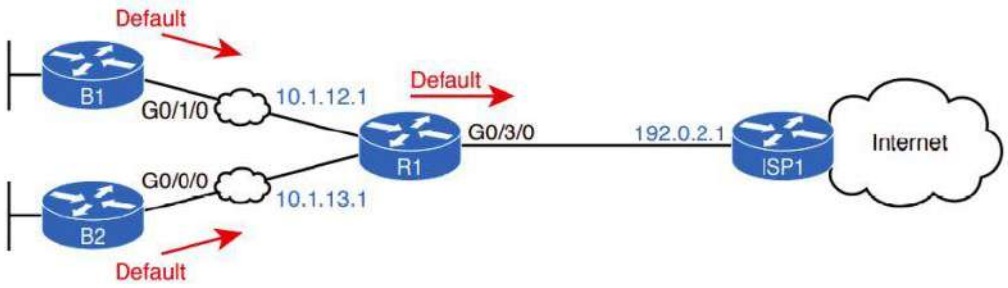
```
O*E2  0.0.0.0/0 [110/1] via 192.168.1.14, 00:00:04, Ethernet0/2
```

E2یعنی Default Routeی قرار است ما را به network خارجی مسیریابی کند.

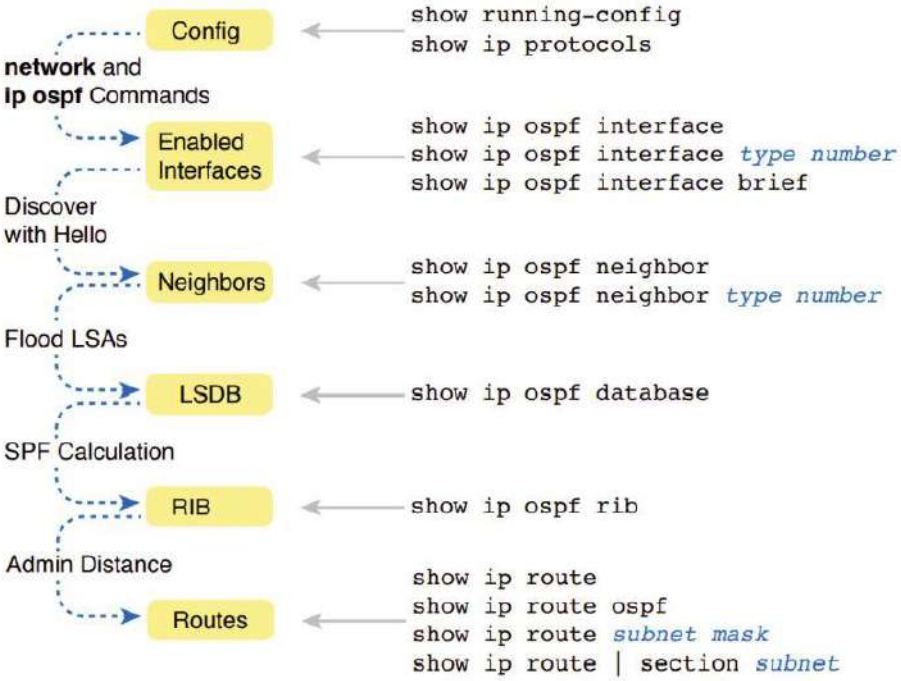
نکته: در این سناریو اگر RTR4 خاموش شود، Default Route از جدول روتینگ حذف میشود و درنتیجه به روترهای دیگر یاد داده نخواهد شد.

خلاصه ای از Default Route :

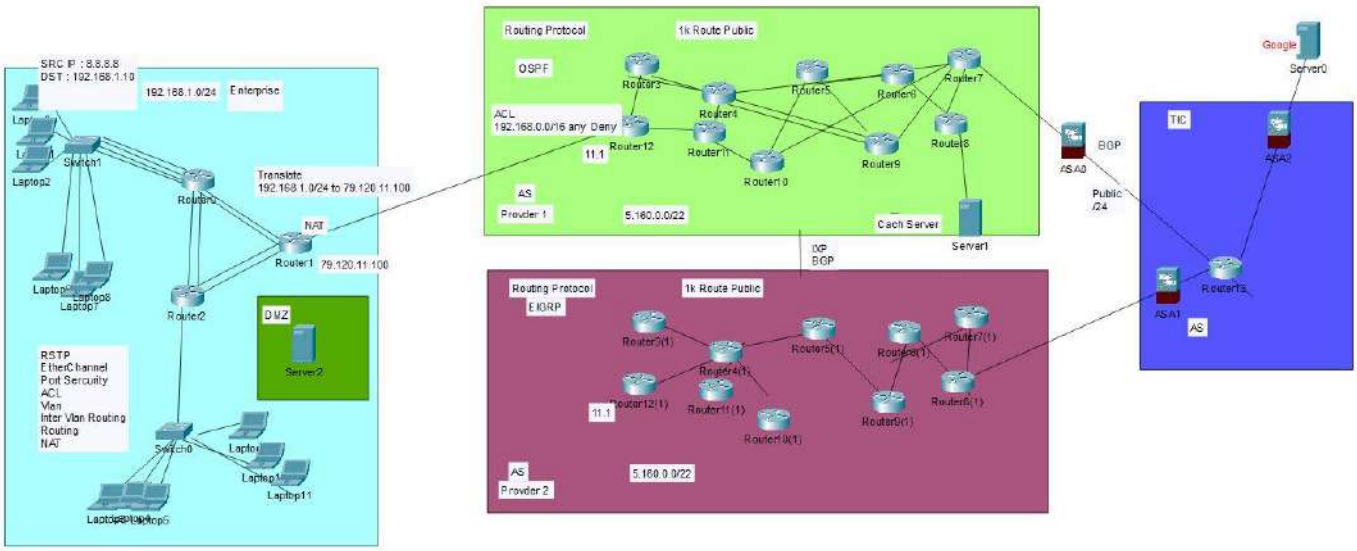




OSPF T-shoot Command :



ISP and TIC Topology Enterprise and :



شرح تصویر بالا :

قسمت آبی آسمانی به عنوان یک Enterprise معرفی شده است که سرویس‌ها و پروتکل‌هایی که نوشته شده، درون آن فعال شده‌اند. به شبکه Enterprise در این سطح را campus گفته می‌شود. حال این سازمان نیاز به اینترنت دارد. خود سازمان نمی‌تواند از شرکت ارتباطات زیر ساخت(TIC=Telecommunication Infrastructure Company) که انحصاری متصدی تامین کننده سرویس اینترنت کشور است، این امکان را فراهم کند. Providerها از طریق مجوز FCP (Fixed Communications Provider= ارائه‌دهنده سرویس‌های اینترنتی و ارتباطی ثابت) می‌توانند اینترنت را از این شرکت دریافت کنند و در اختیار مشتریان قرار دهند. به دلیل بحث‌های حاکمیتی و نظارت و فیلترینگ، تعمین‌کننده پهنای باند اینترنت صرفاً به عهده یک شرکت(TIC) گذاشته شده است که در تمام دنیا این موضوع وجود دارد. TICایران از شرکت‌هایی از قبیل TAFA ،Delta ، omen و ... پهنای باند اینترنت کشور تامین می‌شود.

قسمت سبز رنگ، اولین Providerی است که شبکه Enterprise قصد دریافت سرویس اینترنت را دارد. به عنوان مثال رنج Private IP شبکه Enterprise،192.168.1.0/24 است. به همین خاطر شبکه Provider یک ACL روی اینترفیسی که به شبکه En متصل است قرار داده است که نتواند همچین رنج Ipای وارد شبکه خود شود. ولی یک IP برای ارتباطش با Enتخصیص داده است(مثلا IP Public 79.120.11.1به اینترفیس خود و 79.120.11.100 به اینترفیس روتر Edge). در این حالت شبکه En برای ارتباط با Provider باید NAT انجام دهد(تبدیل IP Praivate به IP Public).

قسمت بنفش رنگ، دومین Providerی است که شبکه Enterprse برای spof و redundancy سرویس دریافت می‌کند. شبکه‌های Provider و ارائه‌دهندگان خدمات اینترنتی، از طریق یک زیرساخت فیزیکی به نامInternet exchange point یا IXP (که از پروتکل BGP استفاده می‌کنند) می‌توانند ترافیک اینترنت را بین شبکه‌های خود مبادله کنند.

هر کدام از این Providerها با IPهایی که به شبکه En اجاره داده‌اند در ارتباط هستند. حال سوال اینجاست چه زمانی شبکه Enterprise نیاز به IP public اختصاصی خود است؟!

همانطور که می‌دانید به طور کل IP گرفتن به دو صورت شکل می‌گیرد: یک اینکه مستقیم از Provider اجاره می‌کنیم(که عمدتاً به این صورت است)، دو اینکه وقتی سازمانی AS و IP های اختصاصی Public نیاز داشته باشد، باید مستقیم از RIPE آیپی بگیرد (ناگفته نماند همچنان این سازمان‌ها نمی‌توانند مستقیم سرویس از شرکت‌های زیرساخت بگیرند و همچنان این وظیفه به عهده FCPهاست و صرفاً راه ارتباطی خود و FCPها، آیپی های Public اختصاصی خود است).

حال با این توضیحات، فرض می‌کنیم شبکه Enterprise ما سروری دارد که خدمات Snapfood را ارائه می‌دهد. در ابتدای کار شرکت اسنپ برای آدرس اینترنتی www.snapfood.ir دو public IP از دو Provider می‌گیرد و برای این آدرس اینترنتی و IPها Recordی در DNS Serverها ثبت می‌کند که Userها بتوانند به شرکت snap متصل شوند(تعدادی از Userها با IP اول و مابقی هم با IP دوم به snap متصل می‌شوند). حال اگر Provider1 قطع شود چه اتفاقی می‌افتد؟ Userهایی که از طریق این Provider به اسنپ متصل می‌شدند، به مدت ۳ روز نمی‌توانند به snapp کانکت شوند (۳ روز برای update کردن valid نبودن IP Provider1 برای این Address زمان می‌برد). از آنجایی که available بودن سرویس برای اسنپ خیلی اهمیت دارد، پس برای این شرکت به مقرون به صرفه‌است که IP و AS مستقل خود را داشته باشد. حال با داشتن IP Public اختصاصی میتواند هر زمان Provider خود را به سرعت بعد از قطعی یکی از Providerها تغییر دهد.

به عنوان مثال laptop1 می‌خواهد با server google ارتباط برقرار کند. هدری که تشکیل میدهد که مثلاً Src IP آن 192.168.1.10 و DSTاش ۸.۸.۸.۸ خواهد بود. Src mac مک خود لپ تاب و Dst mac مک Getway اینترفیس Router0 خواهد بود. به Router0 که می‌رسد هدر تغییر میکند(این تغییرات تا انتها ادامه دارد). در ادامه Router0چون برای 8.8.8.8 مسیری ندارد، آن را به Defulte Route میسپارد. در روتر Edge (Router1)، عملیات Nat با تبدیل آیپی 192.168.1.10 به 79.120.11.100 انجام می‌شود(فراموش نکنیم Router1 دارای Nat table است و می‌داند که IPای تبدیل به چه IPای شده است). هنگامیکه بسته به Router12 Provider می‌رسد، این روتر Routing table خود را بررسی می‌کند که آیا برای Dst IP 8.8.8.8 مسیری دارد یا خیر. چون ندارد پس با Defulte Route Provider مچ می‌شود و بسته به Router7 (Edge Router)، روتر متصل به شرکت زیر ساخت (TIC) می‌رسد. Router7 نیز بسته را به Router13 TIC می‌رساند. این روتر در جدول مسیریابی، مسیری را برای رسیدن به 8.8.8.8 دارد و در نهایت به سرور گوگل می‌رساند. حال Google میخواهد پاسخ دهد. هدر را به Src IP 8.8.8.8 و Dst IP 79.120.11.100 تغییر می‌دهد. در ابتدا بسته را به Router13 می‌رساند. این روتر مسیری برای 79.120.11.100 دارد چون Provider از طریق پروتکل BGP، Networkها را به Router13 ،Advertise کرده است(پروتکل‌هایی IGP توان این حجم از اطلاعات برای انتقال به TIC را ندارد، به همین خاطر از پروتکل EGP(BGP) استفاده می‌شود). پس بسته وقتی به Router7 می‌رسد، طبق Routing table بسته را به Router1می‌رساند. در نهایت بعد از پروسه Nat ، بسته از طریق Routing Table شبکه Enterprise به Laptop1 می‌رسد.

نکته: طبق تصویر، دستگاه‌های فیلترینگ بین Provider و TIC قرار می‌گیرند که هم می‌توانند در شرکت TIC قرار بگیرند هم در خود Providerها.

نکته: Providerها برای کاهش پرداخت هزینه‌های پهنای باند به شرکت زیر ساخت و همچنین افزایش سرعت خدمات به Customerها، از Cach server استفاده می‌کنند که این سرورها را معمولا در لبه شبکه خود قرار می‌دهند.

نکته: به دلیل محدودیت IPV4ها در شبکه، چند راهکار ارائه شده است:

Short Term : کوتاه مدت–>

- ✓ CIDR –> استفاده از IP classless و Subnet mask
- ✓ استفاده از IP private برای شبکه های داخلی و IP Public برای شبکه اینترنت . در حال حاضر قیمت یک IP Public سالانه ۵۰ دلار می‌باشد.
- ✓ NAT –> پروتکل لایه۳ئی که IPهای Private را به Public برای ورود به دنیای اینترنت تبدیل میکند.
- ✓ و..

Long Term : بلند مدت–> مهاجرت به IPV6

Internet Assigned Numbers Authority(IANA) :

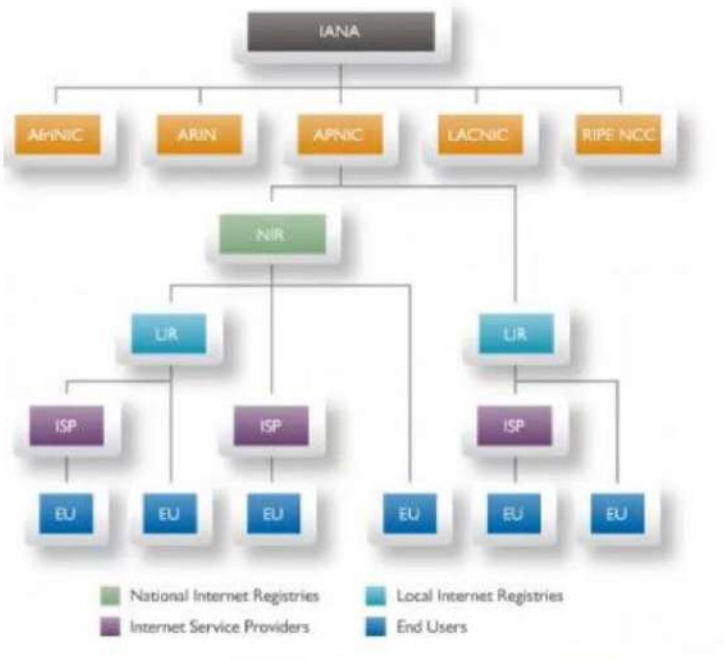
مرجع و نهاد واگذاری اعداد در اینترنت(IP،AS،Port و...) است. پیش از برپایی ICANN برای این منظور، IANA در ابتدا به وسیله جان پوستِل از مؤسسه علوم اطلاعات دانشگاه کالیفرنیای جنوبی، تحت قراردادISI/USC با وزارت دفاع ایالات متحده مدیریت می‌شد، تا اینکه آیکان برای دریافت این مسئولیت تحت قراردادی با وزارت بازرگانی ایالات متحده ایجاد شد.

کل کره زمین به پنج region جداگانه تقسیم‌بندی شده که به آن Registry Internet Regional (RIR)گفته می‌شود.

در سطح کرده زمین پنج RIR وجود دارد: APNIC, ARIN, RIPE NCC , LACNIC, AFRINIC که از این بین RIPE برای اروپا و خاورمیانه به حساب می‌آید که ایران نیز شامل آن است.

سازمان‌هایی مانند ایران خودرو و بانک ملی و حتی Providerها که بخواهند IP و AS مستقل و Public داشته باشند، باید از RIPE درخواست IP و Public AS کنند که باید ماهانه یا سالانه هزینه‌های بالایی پرداخت کنند. به این نوع شبکه‌ها LIR (Local internet Registry) گفته می‌شود.

برای درک بهتر، یک شرکت را در نظر بگیرید. مثال اسنپ که سرویسی را می‌خواهد ارائه کند، باید به یک یا دو Provider وصل شود. حال برای اینکه سرویس را در سطح اینترنت Publish کند، دو روش دارد: یا IP را از Provider اجاره کند یا IP/AS مستقل داشته باشد و مالکیت آن را داشته باشد و هزینه بیشتری باید بپردازد، اما اگر Provider Service دچار اختلال و قطعی شد امکان جابجایی ترافیک شبکه را بین Providerها دارد و همیشه سرویس در دسترس است.

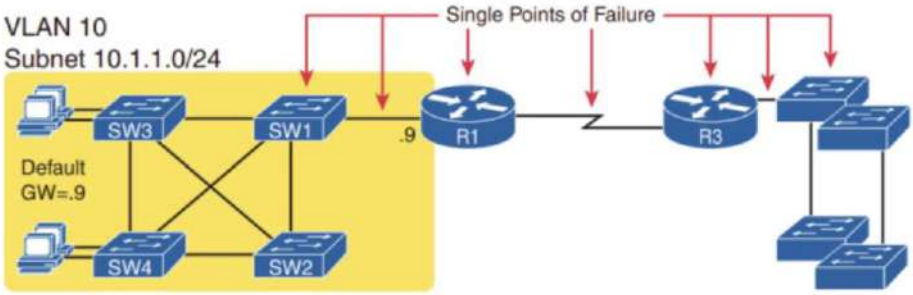


First Hop Redundancy Protocol (FHRPs) :

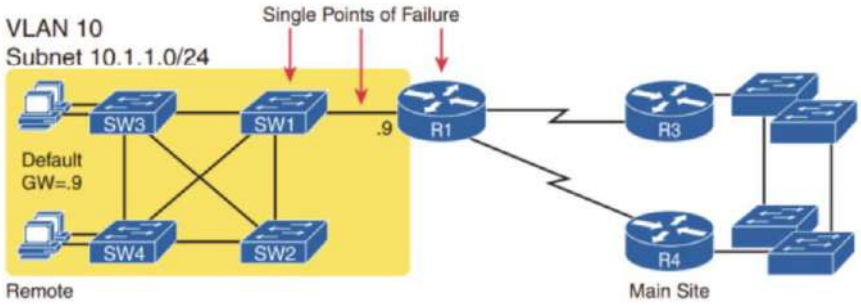
در شبکه‌های با مقیاس بزرگ از مدل طراحی سه لایه‌ای سیسکو که شامل لایه‌های Core, Distribution و Access است استفاده شده و برای افزایش Availability یا در دسترس بودن از تکنیک‌های مختلفRedundancy استفاده می‌شود. در اکثر این شبکه‌ها Redundancy در لایه‌های Distribution و Core دیده می‌شود.

بعضاً در سازمان‌ها با وجود قابلیت استفاده از پروتکل‌های FHR در سوئیچ‌های لایه Distribution، از تکنیک تنظیم چندین Default Gatewayروی کلاینت‌های مختلف استفاده می‌شود، یعنی روی بخشی (معمولاًنصفی)از کلاینت‌ها آدرس IP اینترفیس یکی از سوئیچ‌های لایه Distribution را تنظیم می‌کنند و روی بخش دیگری از کلاینت‌ها آدرس آی پی اینترفیس سوئیچ دوم را تنظیم می‌کنند. اگرچه این روش باعث ایجاد Load Balancing و تا حدودیRedundancyدر شبکه می‌شود، ولی در صورت قطعی یکی از لینک‌ها یا خرابی یکی از سوئیچ‌ها، دسترسی نیمی از کلاینت‌ها به کل شبکه قطع خواهد شد.

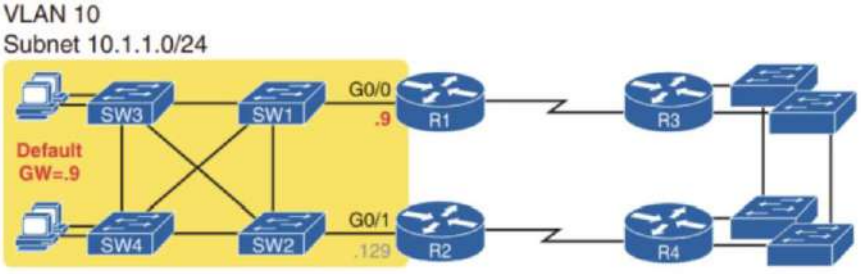
FHRP ها پروتکل‌هایی هستند که با ایجاد یک اینترفیس مجازی این مشکل را حل کرده و باعث ایجاد Redundancy و در نتیجه High Availabilityدر لایه Distribution می‌شوند. عملکرد هر سه پروتکل HSRP, VRRPو GLBP از دید کلاینت‌ها تقریباً شبیه به هم بوده و کلاینت‌ها این دو یا چند سوئیچ لایه توزیع را به صورت یک سوئیچ می‌بینند. در حالت کلی در تمامی این سه پروتکل، یک IP Address و Mac Address به صورت مجازی انتخاب می‌شود.



شناسایی SPF

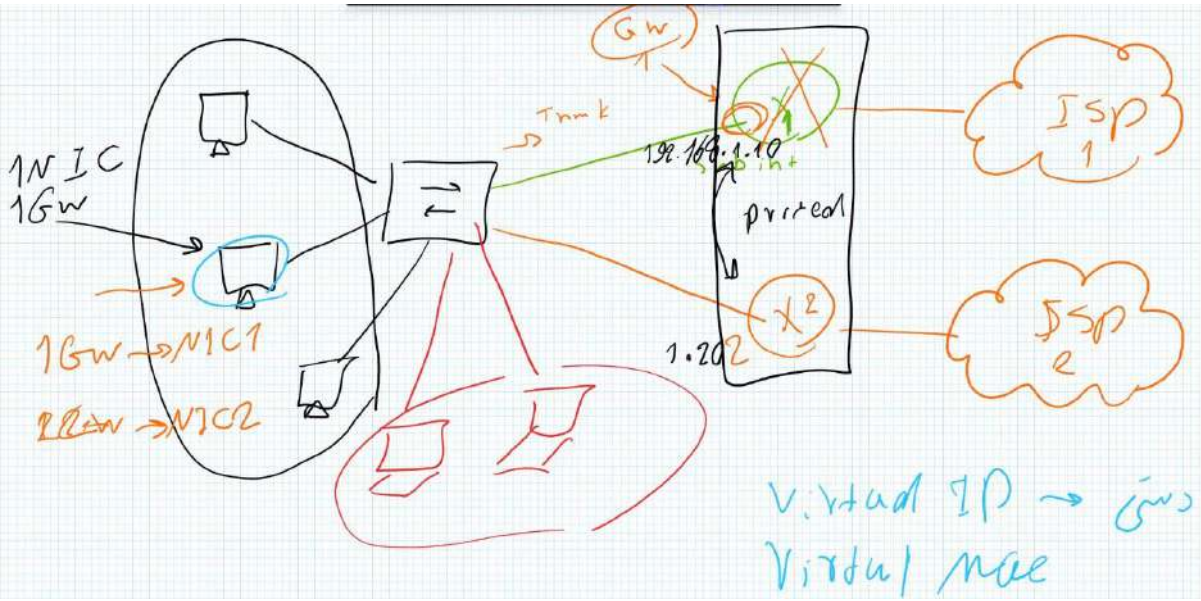


اضافه کردن یک Provider



اضافه کردن یک روتر جهت Redundancu

متوجه شدیم که با اضافه کردن روتر مشکل حل نشد و رویclient ها نمی‌تواند دو Default Gateway تنظیم کند و پروتکل HSRP را جهت رفع مشکل پیاده سازی می کند.



FHRP Protocols :

پروتکل Hot Standby Router Protocol – HSRP که اختصاصی سیسکو است در سال 1998 معرفی شده است.

پروتکل Virtual Router Redundancy Protocol – VRRP که یک پروتکل استاندارد است

پروتکل Gateway Load Balancing Protocol – GLBP یک پروتکل جدیدتر از سیسکو می باشد.

Acronym	Full Name	Origin	Redundancy Approach	Load Balancing Per...
HSRP	Hot Standby Router Protocol	Cisco	active/standby	subnet
VRRP	Virtual Router Redundancy Protocol	RFC 5798	active/standby	subnet
GLBP	Gateway Load Balancing Protocol	Cisco	active/active	host

Hot Standby Router Protocol (HSRP) :

یک پروتکل استاندارد سیسکو است؛ که جهت ایجاد High Availability (HA) در شبکه ارائه شده است، این پروتکل از طریق ایجادRedundancyدر First-Hop ، برایIPهاستهای رویIEEE802 LAN، با یک Gateway پیش‌فرض تنظیم شده است. در واقع HSRPترافیک IP را بدون هیچگونه وابستگی به در دسترس بودن هر یک از روترها، مسیریابی می‌نماید. این امر باعث فعال نمودنِ گروهی از Interfaceهای روتر می‌شود که ظاهر یک روتر مجازی یا Gateway پیشفرض را به هاستهای روی یک LAN می‌دهد. هنگامی‌که HSRP روی یک شبکه یا Segment پیکربندی می‌گردد، یک آدرس مجازی MAC و یک IP آدرس می‌سازد که در گروهی از روترهای پیکربندی شده به اشتراک گذاشته می‌شود. HSRP به دو یا چند روتر پیکربندی شده بر اساسHSRP اجازه

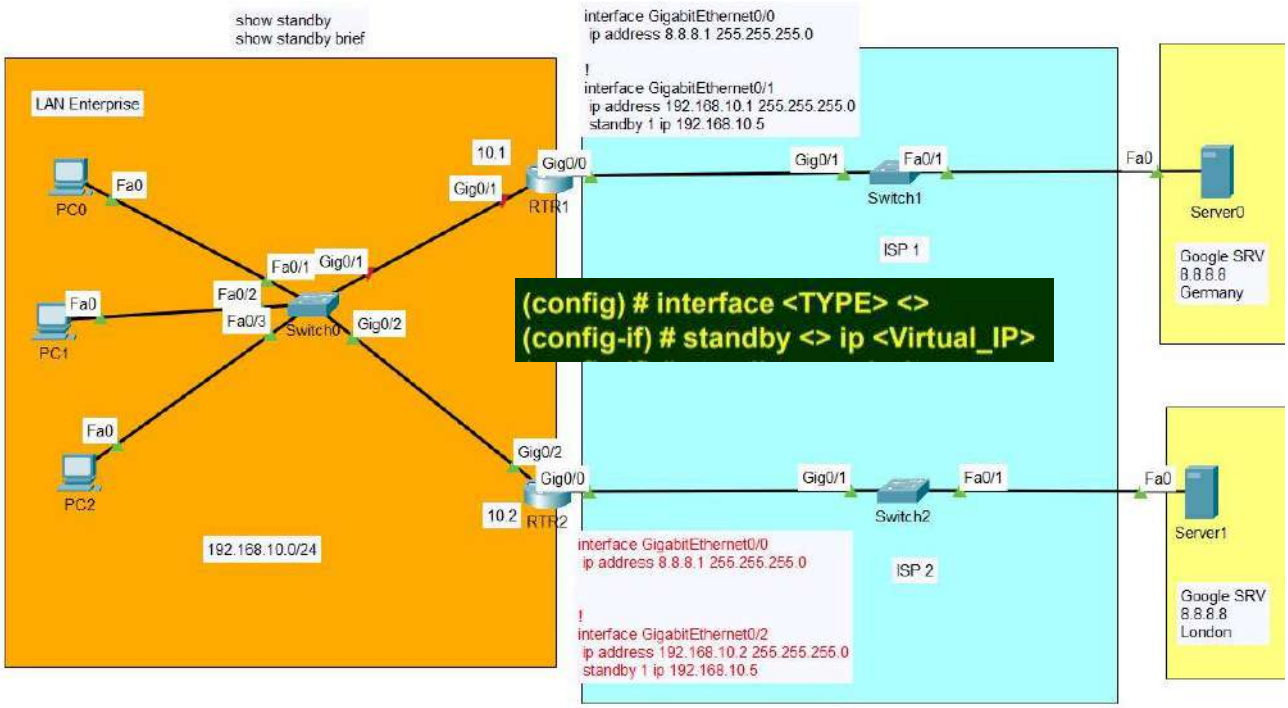
میدهد که ازMAC یا IP یک روتر مجازی استفاده نمایند .در واقع، این روتر مجازی وجود ندارد، بلکه هدف مشترک روترهایی است که برای ارائه‌ی پشتیبانی به یکدیگر، تنظیم شده‌اند .یکی از روترها به عنوان روتر Active و دیگری به عنوان روتر Standby انتخاب می‌شود، روتر Standby، کنترل MAC گروه و IP را، در صورتی که روتر Active از کار بیافتد، به عهده می‌گیرد.

Version	HSRP V1 (Default)	HSRP V2
Group numbers	0 to 255	0 to 4095
Multicast address	224.0.0.2	224.0.0.102 or FF02::66
Virtual MAC address	0000.0C07.AC00 - 0000.0C07.ACFF (last two digits group number)	**IPv4** 0000.0C9F.F000 to 0000.0C9F.FFFF **IPv6** 0005.73A0.0000- 0005.73A0.0FFF (last three digits group number)
Support for MD5 authentication	No	Yes

پیکربندیHSRP :

یکی از راه‌های رسیدن به Uptime تقریباً ۱۰۰ درصدی، استفاده از HSRP است که Redundancy شبکه را برای شبکه های مبتنی بر IP فراهم کرده و رفع مشکل ارسال و دریافت ترافیک کاربر پس از خرابی اولین Hop، در تجهیزات Edge شبکه و مدارهای دسترسی را تضمین می‌نماید.

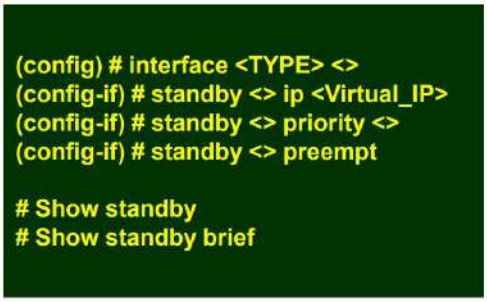
مثال ۱:



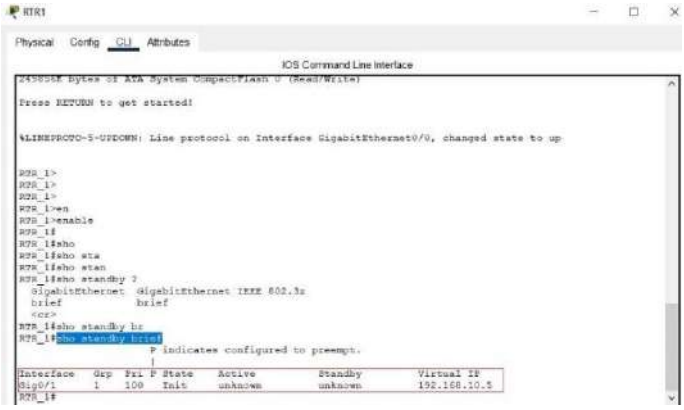
نکته۱: Group-number دو روتر باید یکسان باشد (در این سناریو ۱ در نظر گرفت شده است)

نکته۲: دلیل اینکه ما از virtual (Ip , mac) استفاده می‌کنیم این است که نمیتوان به Clientها دو Getway تخصیص داد.

نکته۳: برای انتخاب حالتstandby,activeروتر، دو قسمت در نظر گرفته می‌شود. قسمت اول priority عددی بین0 تا 255 که بصورت پیش‌فرض همه روترها عدد۱۰۰ در نظر گرفته شده که ادمین قادر به تغییر این مقدار می‌باشد. روتریActiveمی‌شود کهprorityبالاتری داشته باشد، اگر باpriorityنتوانست انتخاب کند، بزرگترینIP Interface را در نظر می‌گیرد، اما قابلیت مقایسه فعال نیست، یعنی اگر روتری که IP کمتری داردActive شود و روتری که Interface IP بزرگتری دارد وارد شود تا زمانی که روتری که Active هست fail نشود اتفاقی نمی‌افتد. هر ۳ثانیه یکبار بین یکدیگر بسته‌های Hello ارسال می‌کنند و ۱۰ثانیه Dead Timeدر نظر گرفته شده که قابل تنظیم(تغییر) می‌باشد.



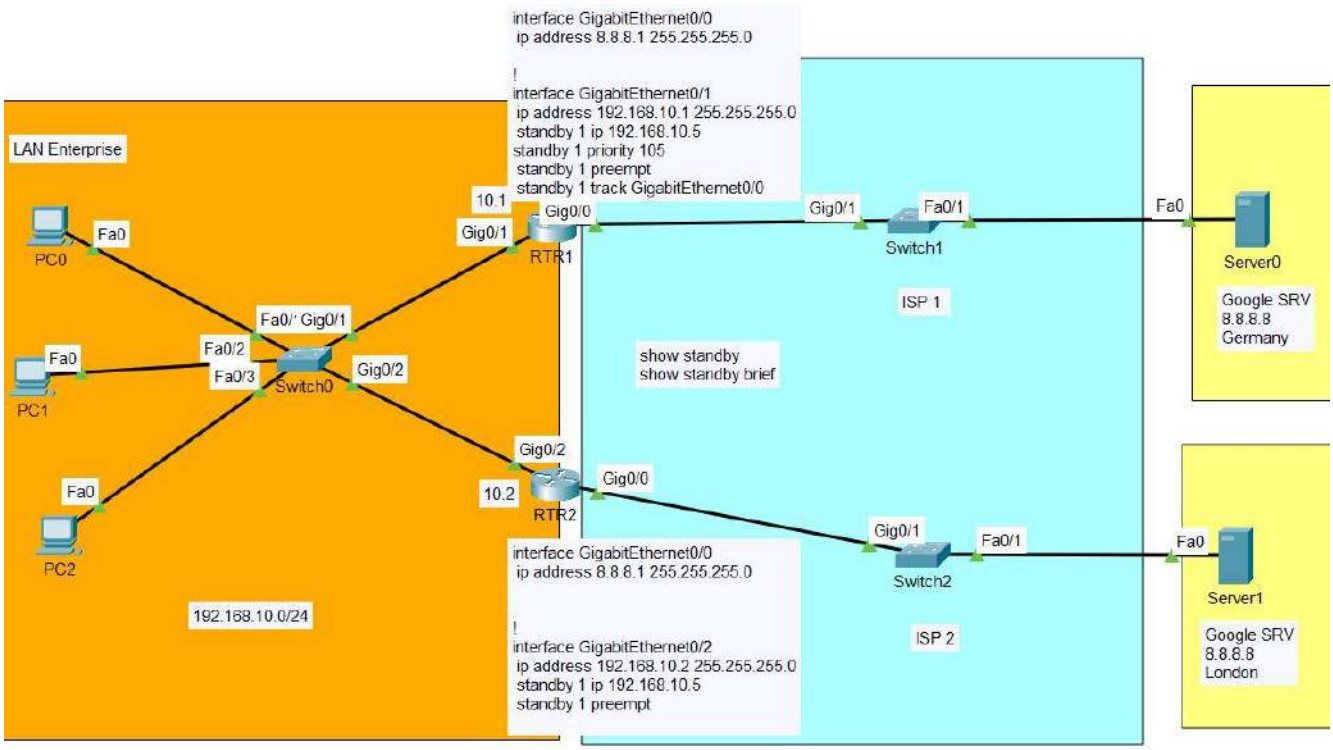

```
RTR_1#show standby
GigabitEthernet0/1 - Group 1
  State is Init (interface down)
  Virtual IP address is 192.168.10.5
  Active virtual MAC address is unknown
    Local virtual MAC address is 0000.0C07.AC01 (v1 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 1.180 secs
  Preemption disabled
  Active router is unknown
  Standby router is unknown
  Priority 100 (default 100)
  Group name is hsrp-Gig0/1-1 (default)
```



نکته٤: در این سناریو دلیل اینکه RTR1 به عنوان Active معرفی شده، این است که Priority یا interface بیشتری نسبت به RTR2 دارد.

نکته٥: این سناریو فقط Redundancy خروجی به سمت شبکه Enterprise را حل می‌کند و در صورت قطعی اینترفیس‌های خروجی به سمت Provider به مشکل میخورد و RTR بعدی متوجه نمی‌شود و دسترسی کامل قطع می‌شود.

مثال۲: در صورت قطعی اینترفیس خروجی روتر



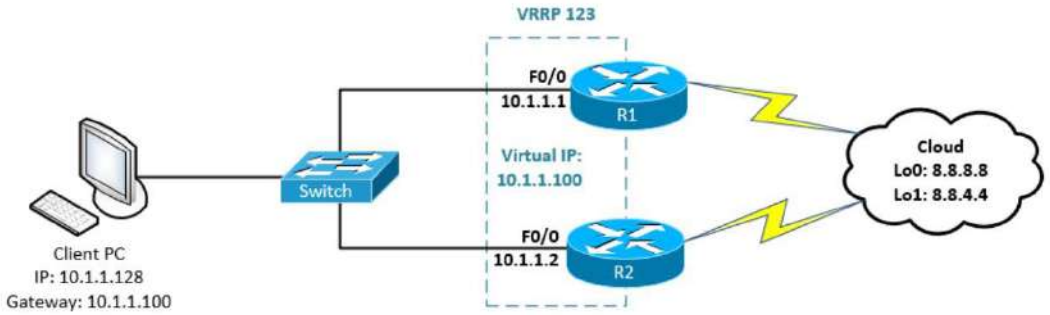
روی RTR1 مقدار priority را بصورت دستی تغییر می‌دهیم اما تا زمانی که قابلیت مقایسه یا preemption فعال نشود اتفاقی نمی‌افتد (ابتدا دستور Priority و سپس دستور Preemption زده میشود). یعنی روی روتری که می‌خواهیم اکتیو باشد و الویت بالاتری دارد قابلیت مقایسه را فعال می کنیم.

این تنظیمات در سطح Redundancy Getway بود.

حال اگر دست دیگر روتر یعنی اینترفیسی که سمت Provider هست قطع شود درکی از آن ندارد. برای حل این مشکل از راهکار زیر استفاده می‌کنیم. در این حالت زمانیکه اینترفیسNot Connected یا Shutdown شود با دستور standby <> track <interface> بصورت خودکار از مقدار Priority 10تا کم می کند که جایActive و Standby تغییر کند. در ادامه برای اینکه این دستورات را RTR2 هم متوجه شود، فقط دستور Preemption زده میشود.

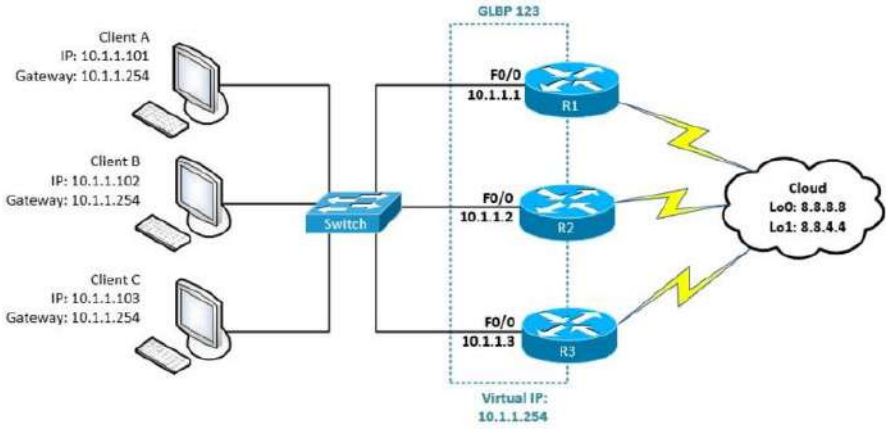
**نکته۶: دستور Track یعنی اینترفیس من فعال باشد تا زمانیکه که اینترفیس خروجی روتر <> هم فعال باشد.

پروتکل **Virtual Router Redundancy Protocol – VRRP** :



این پروتکل توسط IETF به صورت عمومی منتشر شده و قابل استفاده در تمامی سوئیچ‌ها با هر برندی می‌باشد. نحوه عملکرد کلی آن شبیهHSRPبوده و درموارد جزئی تفاوتی با آن دارد. در این پروتکل می‌توان از آدرس اینترفیس فیزیکی هم به عنوان آدرس انتخابی مجازی استفاده کرد، ولی در HSRP چنین قابلیتی وجود نداشت. هرچند این کار توصیه نمی‌شود ولی می‌توان استفاده کرد. همچنین در این پروتکل بر خلافHSRPچندین سوئیچ یا اینترفیس می‌توانند در گروه به صورتStandbyمنتظر به دست گرفتن کنترل اینترفیس مجازی بمانند.

پروتکل **Gateway Load Balancing Protocol – GLBP** :



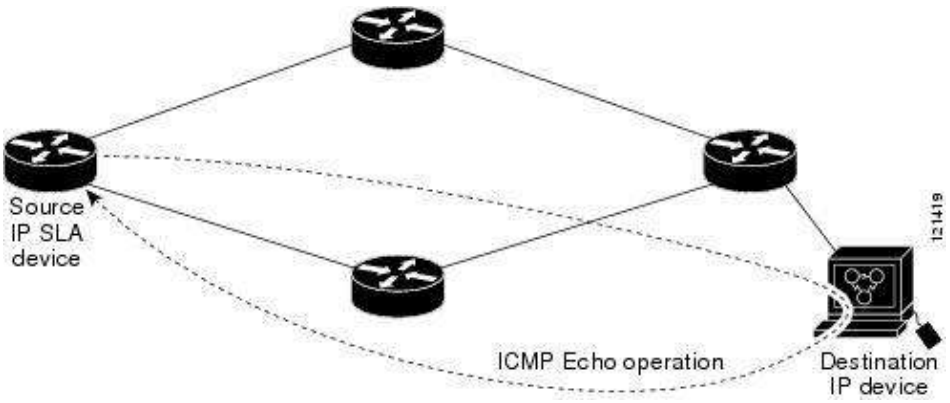
پروتکلGLBP، پروتکل اختصاصی شرکت سیسکو است و بصورت دیفالت از ۳ روش برایLOAD-BALANCE استفاده می‌کند. این پروتکل را در سطح روتر در خیلی از IOSها می‌توانیم داشته باشیم، اما در زمینه MLSها در سوئیچ های ٤٥٠٠،٦٥٠٠ محدود شده‌ایم. این پروتکل برای برداشتن محدودیت‌هایی که در پروتکل HSRP و VRRPبا آن مواجه بودیم معرفی شد.

در پروتکل های HSRP و VRRP ما تنها یک روترACTIVE داشتیم که ترافیک از طریق آن به خارج از شبکه (اینترنت) ارسال می‌شد و سایر روترها منتظر بودند تا روتر ACTIVEی ، FAILشود تا جایگزین آن شوند.

همچنین در پروتکل‌های HSRP وVRRP وقتی کلاینت‌هایی که برای GATEWAY آنها VIRTUAL IP تخصیص داده شده بود و حالا برایVIRTUAL MAC آنها، ARP REQUEST ارسال می‌کردند، تنها روتر ACTIVEدر HSRPوMASTERدر VRRPجوابگو بودند و برای آنها درARP REPLY ارسالی، MAC VIRTUAL را معرفی می‌کردند، اما در پروتکل GLBP ، وقتی کلاینت‌ها برای مک VIRTUAL IPای ، ARP REQUEST ارسال می کنند، روتر AVGپاسخگو است و در هر بار ARP REQUESTکلاینت‌ها،VIRTUAL MACیکی ازFORWARDERها را معرفی می‌کند که البته براساس یکسری الگوریتم، این روش اختصاص VIRTUAL MAC متفاوت است.

IP SLA (Internet Protocol Service Level Agreement) :

IP SLA یک قابلیت بسیار مفید در IOS و تجهیزات سیسکو می‌باشد، این قابلیت کمک می‌کند تا به صورت لحظه‌ای و Real time از تمام داده‌ها و اطلاعات دستگاه و شبکه یک گزارش تهیه نماید.



در واقع IP SLA به ما امکان بررسی و جمع‌آوری اطلاعات در مورد میزان تاخیر پکت‌ها،Packet Delay ، میزان Packet Loss ، برقراری ارتباطات، میزان Jitter ،کیفیت صدا در ارتباطات voip ،بررسی یک مسیر به شکلhop by hop ، در دسترس بودن یک سرویس و .. که تمامی این امکانات باعث می‌شود که میزان پایداری شبکه و کیفیت سرویس QOS بالا رفته و از Down Time ها و network outageها به شکل قابل ملاحظه ای کاسته شود.

همچنین با ابزارهایی نظیرSNMPو نرم‌افزارCiscoWorks Internetwork Performance Monitorو یا حتی نرم‌افزارهایthird part امکان بررسی و جمع آوری اطلاعات در زمینه کارکرد شبکه و کیفیت سرویس فراهم می‌آورد.

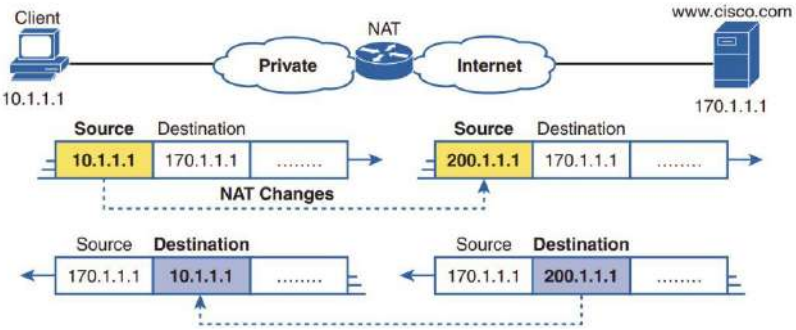
بعد از مدتی که شما از IP SLA استفاده کنید به داده‌های نورمال شبکه خود دست پیدا می‌کنید که به آن**Baseline** نیز گفته می‌شود، حال اگر وضعیت داده‌های عادی و نورمال شما تغییری پیدا کند و کمتر یا بیشتر حد نورمال خودش شود، این تغییرات به شما اطلاع داده می‌شود. برای نمونه ممکن است شما از شرکتی اینترنت دریافت کرده اید و یک قرار داد هم بین خود نوشته‌اید تا کمتر از یک میزان پهنای باند یا قطعی نداشته باشد، با بررسی اطلاعت به دست آمده از IP SLA می‌توانید مشخص کنید که این شرکت به شما درست خدمات داده است یا خیر.

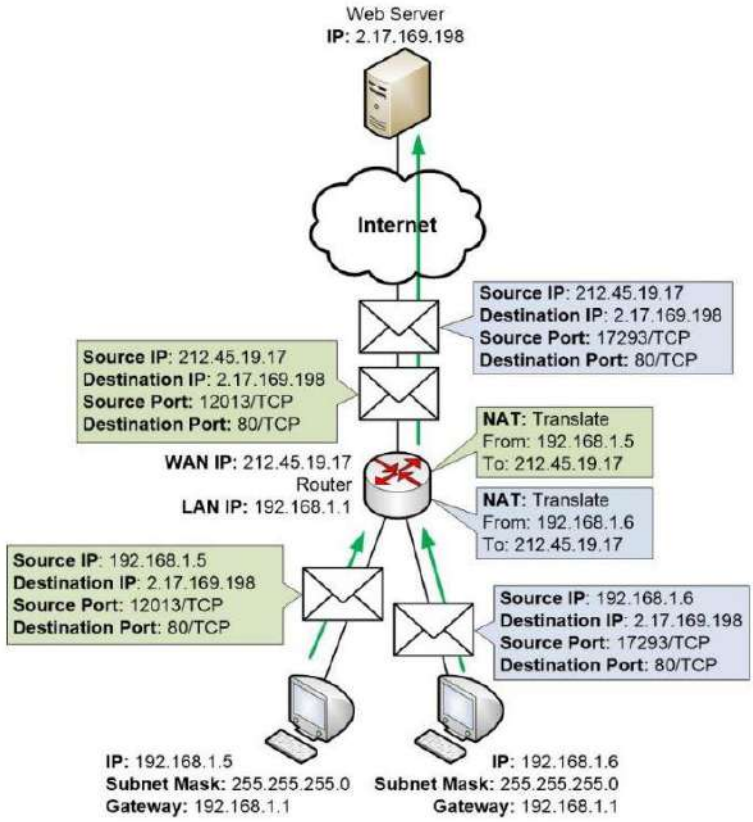
در واقع IP SLA یکسری اطلاعت خام مانند SPAN به ما می‌دهد که ما به کمک نرم افزار های مانیتورینگ مانند – PRTG Solarwinds – OPManager – Nagios XI – Zabbix– Datadog – Logic Monitorو نرم افزارهای دیگر که به آن ها NMS یا Network management software نیز گفته می‌شود می‌توانیم گزارشی تهیه کنیم که یک مدرک برای اثبات کیفیت سرویسی است.

Network Address Translation (NAT) :

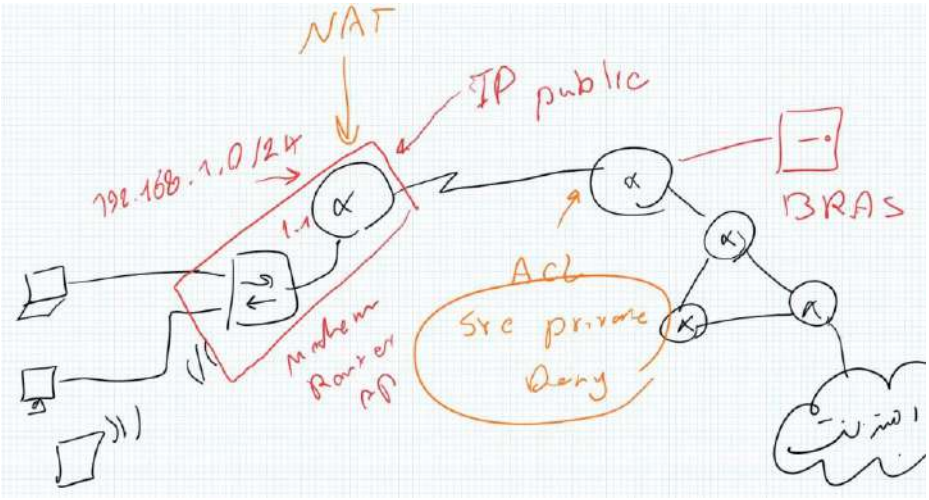
IPv4 نسخه چهارم پروتکل اینترنت نسبت به تقاضای فعلی شبکه به لحاظ تعداد IP محدود می‌باشد. به همین دلیل امکان درنظر گرفتن IP برای تمام تجهیزاتی که به اینترنت می‌خواهند متصل شود وجود ندارد. علاوه بر این محدودیت، استفاده ازIPهای معتبر موجود در اینترنت نیاز به پرداخت هزینه است.

NAT برای برطرف شدن این مشکلات ارائه شد. در شبکه‌های محلی از IP Private استفاده می‌شود و برای شبکه تعداد محدودی IPمعتبر (Public) گرفته می‌شود و با استفاده از سرویس NAT ارتباط دستگاه‌ها به اینترنت برقرار می‌شود.





به طور مثال یک شبکه را در نظر بگیرد که دارای ۲۰ دستگاه است که می خواهند از اینترنت استفاده کنند. با استفاده از سرویس NATبه جای اینکه برای هر دستگاه یکIP Publicتهیه شود، کلا یکIP Publicتهیه می‌شود و برای دستگاه‌هاIP Privateدرنظر گرفته می‌شود واین دستگاه‌ها با استفاده از یکIP Publicبه اینترنت متصل می شوند. با اینکار در مصرفIPو هزینه صرفه‌جویی می‌شود.



محدوده آدرس‌های آی پی IP Private :

10.0.0.0 تا 10.255.255.255

172.16.0.0 تا 172.31.255.255

192.168.0.0 تا 192.168.255.255

موارد استفاده ازNAT :

- صرفه‌جویی در مصرف IP و هزینه.
- زمانی که بخواهیم IP را به دلایلی عوض کنیم.
- زمانی که شبکه داخلی از IP Private استفاده می‌کند.
- برقراری ارتباط بین دو شبکه که دارای رنج IP یکسانی هستند.
- نخواهیم رنج IP که در شبکه مورد استفاده قرار می‌گیرد از بیرون دیده شود.
- زمانیکه مقصد، رنج IP داخلی شبکه ما را نمی‌شناسد.

معرفی مفاهیمNAT :

Address Local Inside : آدرس‌هایی که برای شبکه داخلی مورد استفاده قرار می‌گیرد.

Addres Global Inside :آدرس‌هایی که دستگاه‌های داخلی شبکه با آن از بیرون دیده می‌شوند(IP Public).

Address Local Outside: آدرس‌هایی که دستگاه‌های داخل شبکه، دستگاه‌های خارج از شبکه را با آن می‌بینند و می‌تواند آدرس Privateباشد. نکته‌ای که وجود دارد این آدرس از طریق شبکه داخلی قابل مسیریابی است.

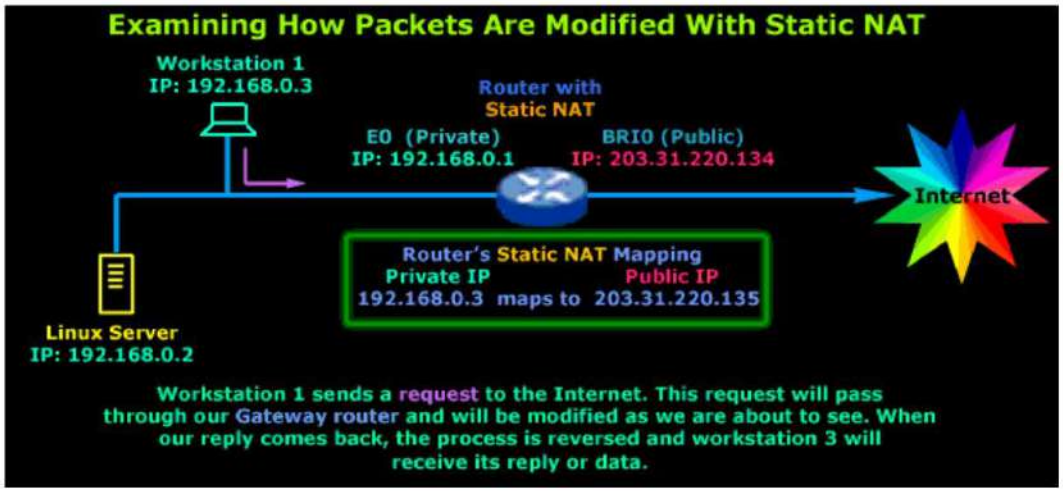
Address Global Outside :آدرس‌های Public مربوط به دستگاه‌های بیرون از شبکه ، که ما با آنها ارتباط برقرار می‌کنیم، مانند IP Publicسرور سایت.

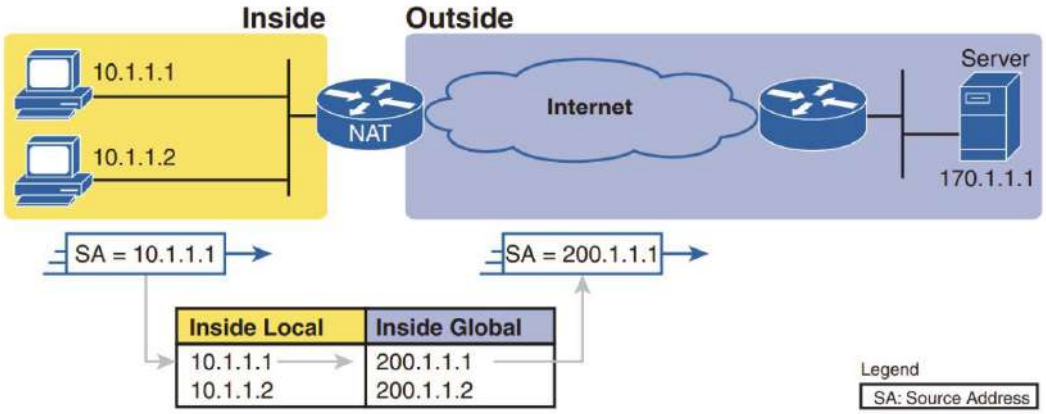
Types Of NAT :

- ✓ Static NAT
- ✓ Dynamic NAT
- ✓ Overloaded (PAT)

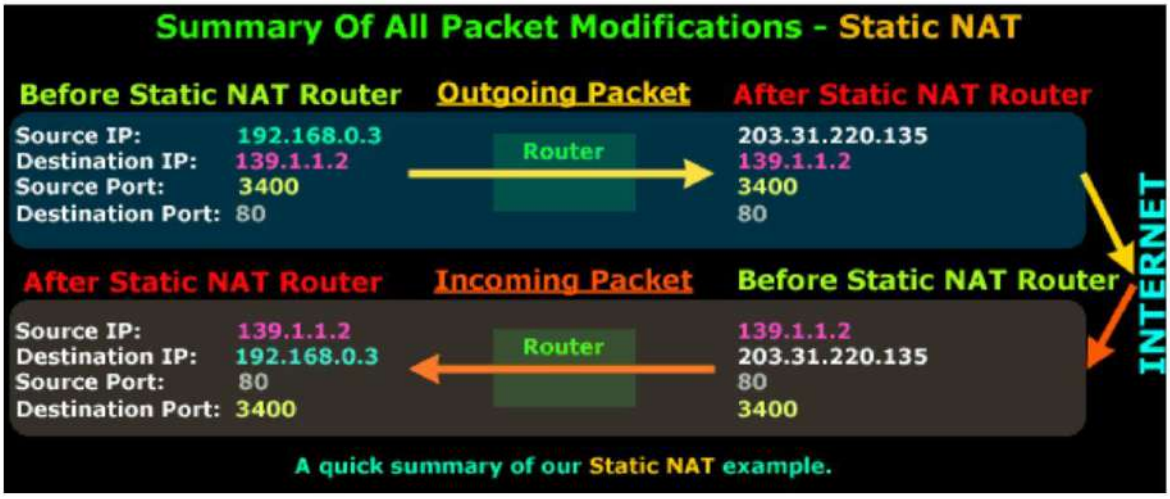
Static NAT :

در این روش یک آدرس Private را تبدیل به یک آدرس Public می کند، یا به عبارتی یک دستگاه از شبکه داخلی به یک IP از شبکه خارجی تبدیل می شود.

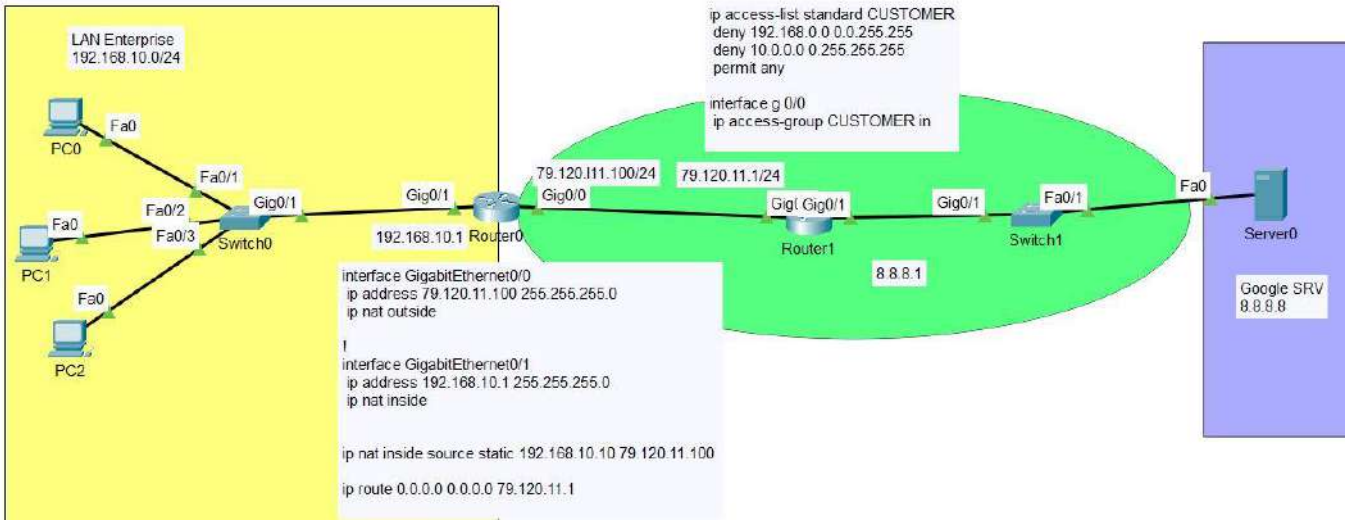




در این روش NAT به صورت یک به یک انجام می‌شود. اگر شما ۱۰۰ کاربر داخلی و ۱۰۰ آدرس global داشته باشید، می‌توانید از این روش استفاده کنید و برای هر یوزر مشخص کنید از چه آدرس global می‌تواند استفاده کند. به صورت معمول ما به اندازه کافی آدرس global برای هر کاربر نداریم. استفاده معمول از روش static NAT برای یک سرور در شبکه داخلی یا محیط DMZ است و می‌خواهیم به کاربران سطح اینترنت دسترسی به این سرور را بدهیم و با استفاده از static NAT می‌توانیم این دسترسی را فراهم کنیم.



مثال: static Nat



نکته۱: Provider یک IP از طریق DHCP یا بصورت دستی به ما اختصاص داده، در این سناریو

79.120.11.100 255.255.255.0

نکته۲: برای اینکه PC بتواند با سرور ارتباط برقرار کند باید روی روتر route مورد نظر را وارد کنیم. همچنین اگر هر مسیری که در جدول مسیریابی نداشت، با Default Route به provider می‌دهد.

RTR_EDGE (config)#ip route 0.0.0.0 0.0.0.0 79.11.120.1

نکته۳: Provider یک ACL به نام Customer نوشته و مثلا آیپی های Private شبکه موجود را Deny کرده که رد نشوند.

RTR_PROVIDER(config)ip access-list standard CUSTOMER

RTR_PROVIDER(config-std-nacl)deny 192.168.0.0 0.0.255.255

RTR_PROVIDER(config-std-nacl)deny 10.0.0.0 0.255.255.255

RTR_PROVIDER(config-std-nacl)permit any

RTR_PROVIDER(config)int g 0/0

RTR_PROVIDER(config-if)ip access-group CUSTOMER in

نکته٤:

Step 1 Use the ip nat inside command in interface configuration mode to configure interfaces to be in the inside part of the NAT design.
Step 2 Use the ip nat outside command in interface configuration mode to configure interfaces to be in the outside part of the NAT design.
Step 3 Use the ip nat inside source static inside-local inside-global command in global configuration mode to configure the static mappings

Router0 RTR_EDGE (config)#int g 0/1

RTR_EDGE (config-if)#**ip nat inside**

RTR_EDGE (config-if)#exit

RTR_EDGE (config)#int g 0/0

RTR_EDGE (config-if)#**ip nat outside**

RTR_EDGE (config-if)#exit

RTR_EDGE (config)#**ip nat inside source static 192.168.10.10 79.120.11.100**

RTR_EDGE #show ip nat

نکته٤: در روش استاتیک مشکل رفع شد، اما به ازای هر کلاینت باید یک IP Public تهیه کنیم که منطقی نیست. به همین خاطر به سراغ NAT Dynamic می‌رویم.

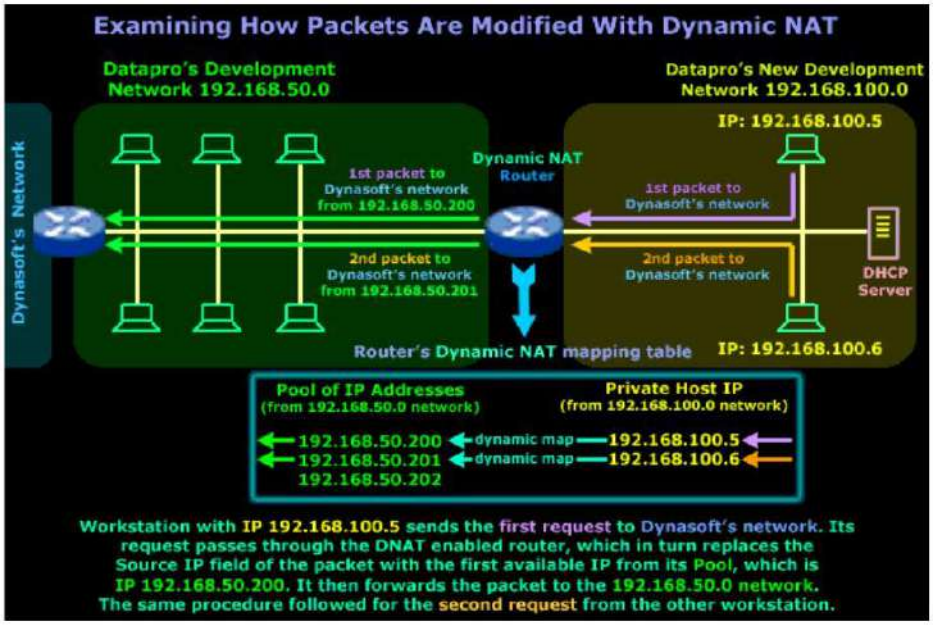
Dynamic NAT :

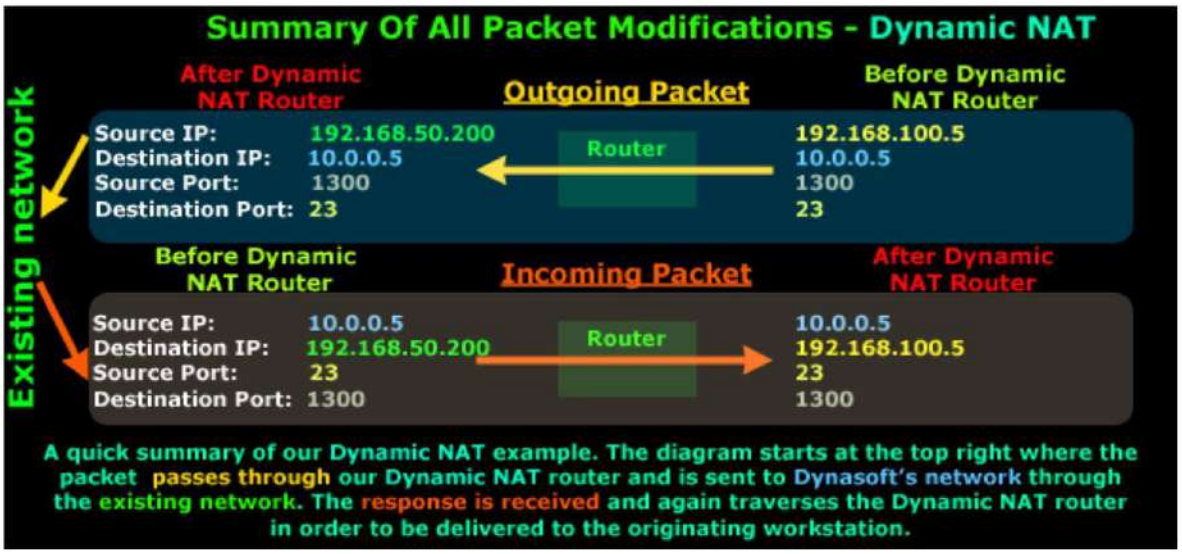
IPهایی که از Provider گرفته شده را در NAT Pool قرار می دهیم .

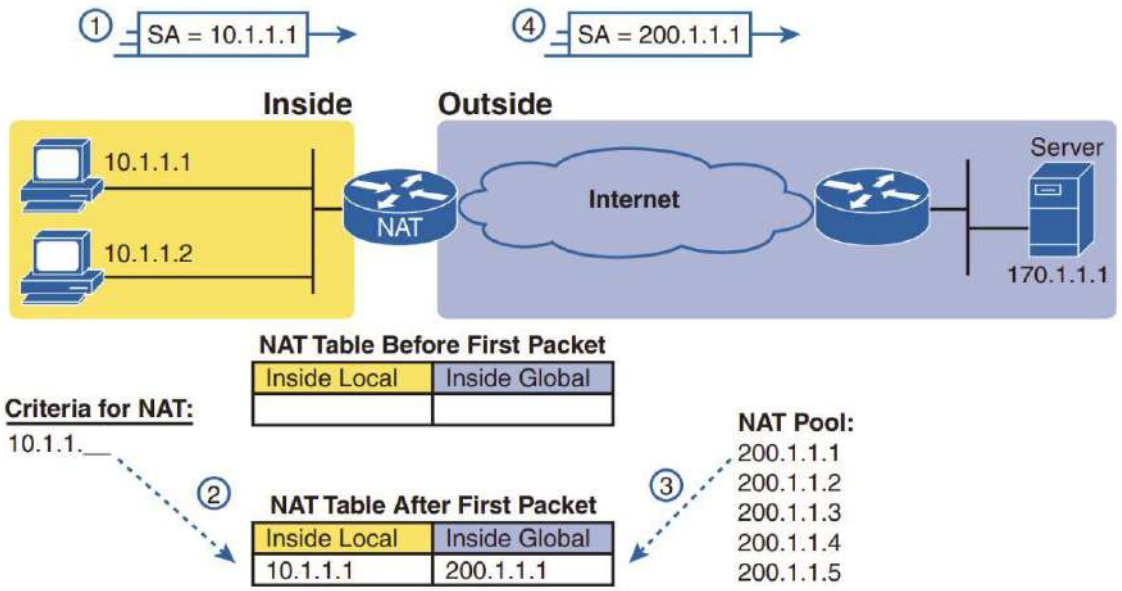
در این روش یکpool (رنج) از IP Public را به یک رنج از IP Private شبکه داخلی اختصاص می‌دهیم. در این حالت تعداد IPهای داخلی و خارجی باید برابر باشد.

نکته:NATکردن براساس پارامترهای دیگر مانند پروتکل ، اینترفیس ، مقصد و ... امکان پذیر است، برای این حالت، به جای Standard ACLاز Extended ACL استفاده می‌کنیم .

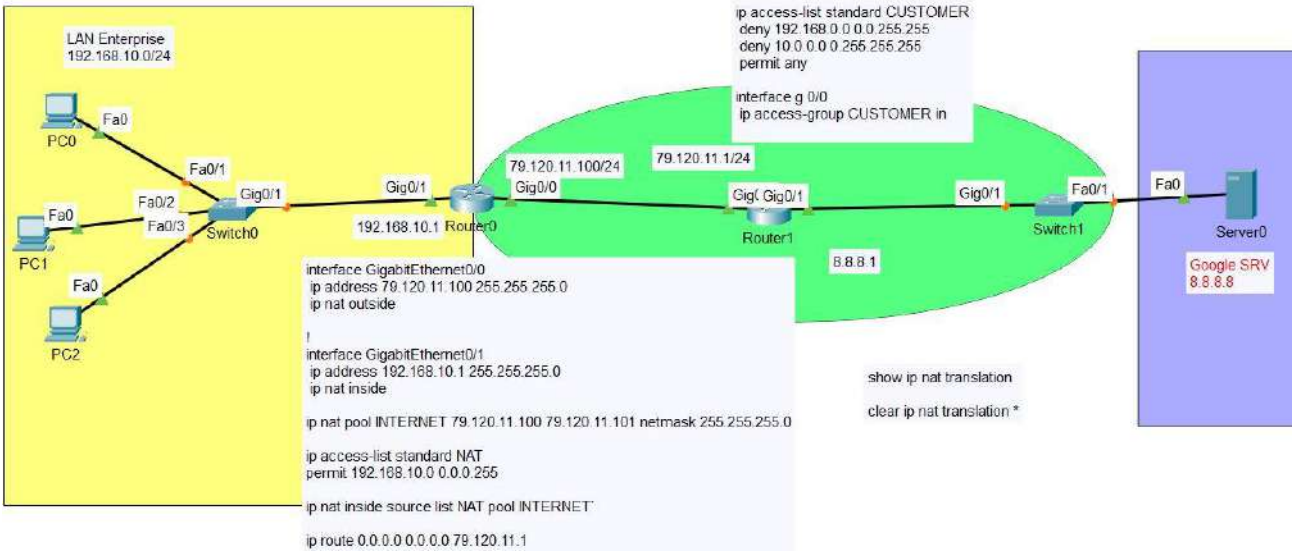
در این حالت ما یک رنج از آدرس های global داریم و تنها این رنج آدرس‌ها را به شبکه داخلی اختصاص می‌دهیم تا زمانیکه هر دستگاه نیاز به استفاده از اینترنت را داشت از آنها استفاده کند. به طور مثال، یک کاربر می‌خواهد از اینترنت استفاده کند با شروع به کار او یک آدرس global از این رنج به او اختصاص داده می‌شود و این کاربر با استفاده از این آدرس global ارتباطش با اینترنت برقرار می‌شود. بعد از یک بازه زمانی کاربر کارش با اینترنت به اتمام می‌رسد و دیگر نیاز به استفاده از اینترنت را ندارد. در این دستگاهی مثل روتر که عمل NAT را انجام می‌دهد، بعد از یک بازه زمانی مشخص در صورت عدم استفاده آدرس global این آدرس را آزاد خواهد کرد که سایر دستگاه‌ها بتوانند از آن استفاده کنند.







مثال : Dynamic NAT



در ابتدای کار NAT static قبلی را غیر فعال میکنیم.

RTR_EDGE (config)no ip nat inside source static 192.168.10.10 79.120.11.100

Step 1 Use the ip nat inside command in interface configuration mode to configure interfaces to be in the inside part of the NAT design (just like with static NAT).
Step 2 Use the ip nat outside command in interface configuration mode to configure interfaces to be in the outside part of the NAT design (just like with static NAT).
Step 3 Configure an ACL that matches the packets entering inside interfaces for which NAT should be performed.
Step 4 Use the ip nat pool name first-address last-address netmask subnet-mask command in global configuration mode to configure the pool of public registered IP addresses
Step 5 Use the ip nat inside source list acl-number pool pool-name command in global configuration mode to enable dynamic NAT. Note the command references the ACL (step 3) and pool (step 4) per pre

Ipهایی که از Provider گرفتیم را در Nat Pool قرار می‌دهیم.

RTR_EDGE (config)#**ip nat pool INTERNET 79.120.11.100 79.120.11.101 netmask 255.255.255.0**

یک Standard List Access به نام NAT می نویسیم

RTR_EDGE (config)#ip access-list standard NAT

RTR_EDGE (config-std-nacl)#permit 192.168.10.0 0.0.0.255

در نهایت فعالسازی List NAT برای Pool INTERNETی که ساختیم.

RTR_EDGE (config)#**ip nat inside source list NAT pool INTERNET**

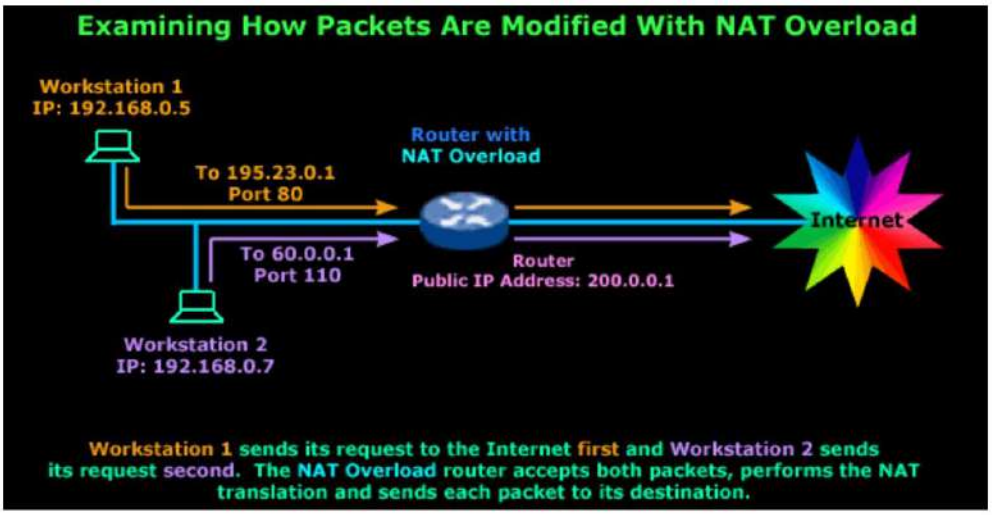
نکته: این روش بهینه‌تر از روش Static بود، ولی تعداد IP که می‌توانستیم Nat کنیم محدود بود. چون Provider که نمی‌تواند به عنوان مثال IP 24/ در اختیار ما قرار دهد . به همین خاطر به سراغ روشPAT می‌رویم.

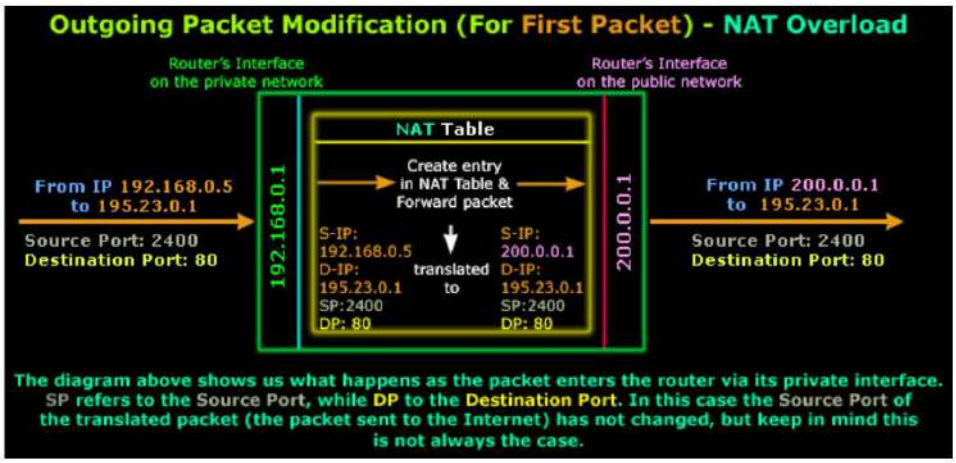
PORT ADDRESS TRANSLATION (PAT) / OVERLOAD NAT:

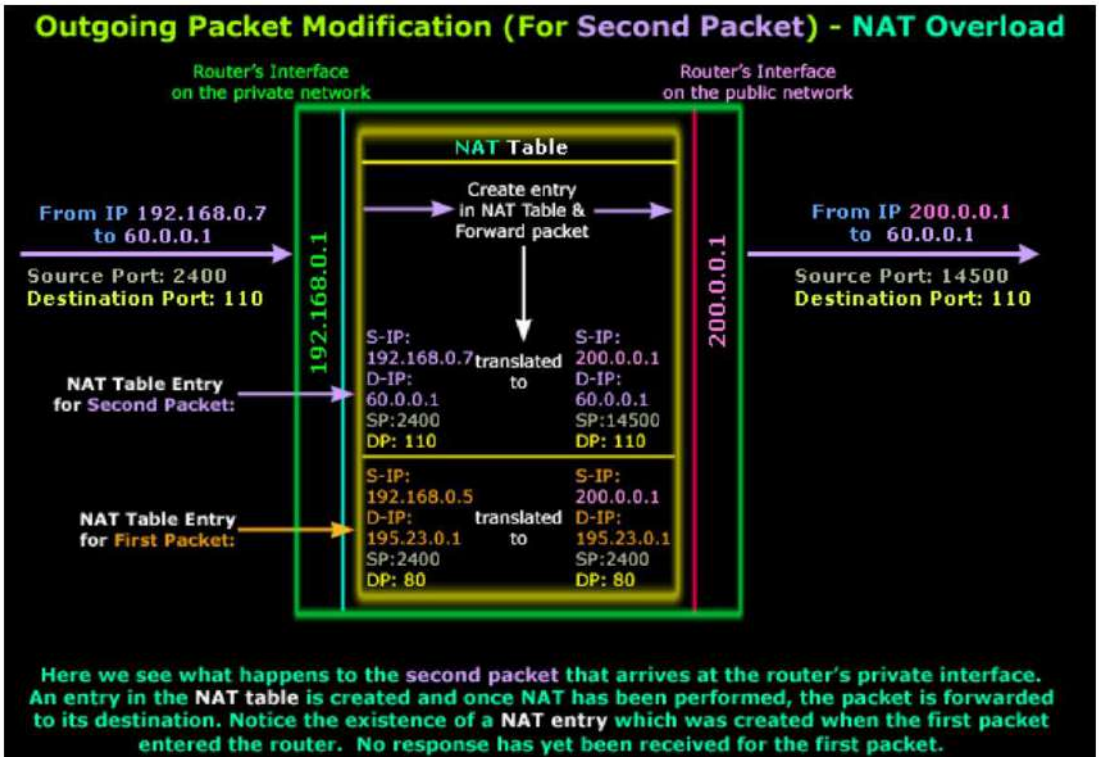
این روش مشابه Dynamic NAT می‌باشد با این تفاوت که به تعداد دستگاه‌هایی که می‌خواهند از اینترنت استفاده کنند نیاز به IP نداریم و تعداد می‌تواند کمتر و یا حتی یک عدد باشد.

این روش برای بیشتر کاربرانی که به اینترنت متصل می‌شوند استفاده می شود. در این روش از مزیت Dynamic NAT که تنها به کاربرانی که نیاز به استفاده از اینترنت دارند آدرس Global اختصاص داده می‌شود استفاده می‌کند و در کنار آن با استفاده از شماره پورت‌های مورد استفاده در ارتباط، امکان استفاده چندین کاربر را از یک آدرس Global فراهم می‌کند. در این روش دستگاهی که عمل PAT را انجام می‌دهد، اطلاعات پورت و IPها را ردیابی می‌کند و براساس آنها جدولNAT را تشکیل می‌دهد.

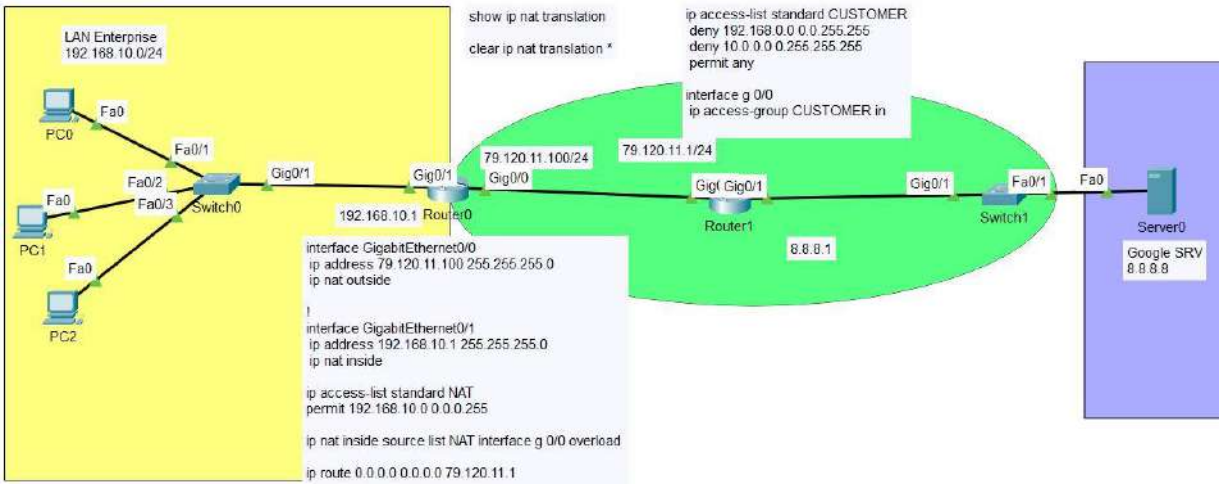
مقدار پورت کنار IP قرار داده می شود که ۱۶ بیت می باشد یعنی 2^{16}=65536 حالت، در نتیجه با یک IP Public که از Provider می‌گیریم این تعداد Client را می توانیم NAT کنیم.







مثال: Overload NAT



چون یک IP از Provider گرفتیم دیگر نیازی به Pool NAT نداریم. اگر بخواهیم Pool NAT را حذف کنیم باید کانفیگ NAT را پاک کنیم، زیرا در حال حاضر Pool NAT ما Used هست اجازه پاک کردن آن را نمی دهد.

RTR_EDGE (config)#no ip nat pool INTERNET 79.120.11.100 79.120.11.101 network 255.255.255.0

خطا: %pool INTERNET use,cannot destroy .

در نتیجه اول خط NAT را پاک می کنیم

RTR_EDGE (config)#clear ip nat translation *

RTR_EDGE (config)#no ip nat inside source list NAT pool INTERNET

RTR_EDGE (config)#no ip nat pool INTERNET 79.120.11.100 79.120.11.101 network 255.255.255.0

NAT همان ACL که نوشتیم می‌باشد

RTR_EDGE (config)#ip nat inside source list NAT interface g 0/0 overload

دستور آخر می‌گوید: میخواهیم NAT کنیم. چه چیز را؟ inside را . چه قسمتیشو؟ soureش را. از روی چه لیستی؟ لیستی که به اسم NAT ساختیم. روی اینترفیس G0/0. در انتها اگر overload زده نشود، یک بسته ارسال می‌شود و تمام. پس باید در انتها overload را وارد کنیم. Overloadدر اصل port را هم اضافه می‌کند.

حال اگر از هر PC بسته‌های ICMP(مثال Ping) با IP و PORT متفاوت ارسال کنیم، میبینیم کهIP همه سیستم‌ها هنگام خروج از RTR0 به IP public یکسان ولی Portهای متفاوت تبدیل میشوند.

توجه شود که این Portها از روتر خارج نمی‌شوند و Local درون روتر باقی می‌مانند. جدولی تشکیل می‌دهد که اگر پاسخ بسته آمد مقصد(داخل شبکه) را بداند.

```
RTR_EDGE#sh ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
icmp 79.120.11.100:1   192.168.10.10:1    8.8.8.8:1          8.8.8.8:1
icmp 79.120.11.100:2   192.168.10.10:2    8.8.8.8:2          8.8.8.8:2
```

نکته: در شبکه‌های بزرگ نباید همه Clientها را با یک IP به خارج از شبکه (NAT) ارسال کرد(مخصوصاً سرویس‌های مهم). شاید به خاطر سهل‌نگاری یا خرابکاری یک یوزر، این IP از مقصد بلاک شود. پس سعی شود در شبکه ها IP ها را Scop Scop کنیم و با NAT با IP های متفاوت به خارج از شبکه هدایت کنیم.

Carrier Grade Network Address Translation (CGNAT) :

ماژول CGNAT (CGN) امکان پیاده‌سازی انواع مختلفی از تکنیک‌های Tunneling مورد استفاده بین شبکه‌های IPv4 و IPv6 شامل DS-lite ، RD6، MAP ،MAP-E، و LW406 را فراهم می‌نماید. این ماژول با ارائه کارایی بسیار بالا در شبکه‌های Enterpriseو Carrier-grade ، به خوبی نیازمندی‌های مرتبط با یک شرکت ارائه‌دهنده سرویس‌های اینترنتی را برآورده می‌کند. همچنین با استفاده از ماژولCGN، امکان پیکربندی و پیاده‌سازی انواع مختلفی از تکنیک‌های Address Translation شامل NAT44 و NAT64 با استفاده از تکنیک هایDeterministic ، NAPT (Network Address & Port Translation) ، PBA (Port Block Allocation) به‌صورت Reverse-proxy و Forward-proxy فراهم خواهد شد. علیرغم آنکه امکان استفاده از ماژول CGN به تنهایی نیز وجود دارد، ولی استفاده از این ماژول در کنار ماژول LTM وAFM نیز منجربه فراهم شدن قابلیت مجزا نمودن سرویس‌های مختلف و اعمال Security Policy مختلف به ازای هر سرویس و درنهایت ارسال/دریافت ترافیک به واسطه IPv4 Tunnels و یا IPv6 Tunnels تحتNAT Policy دلخواه می‌باشد.

***به طور خلاصه Provider به شبکه‌های خود IP public می‌دهد که IP private خود را به آن تبدیل کنند تا از اینترنت بهره ببرند. با توجه به محدودیت IP و همچنین هزینه بالای آن، Provider ها از مکانیزمی به نام CGNAT استفاده می‌کنند و این IP public را مجدد به IP public دیگری تبدیل میکند و سمت شبکه اینترنتIPV4,6 هدایت می‌کند.

between 100.64.0.0 To 100.127.255.255 : Range IP CGNAT

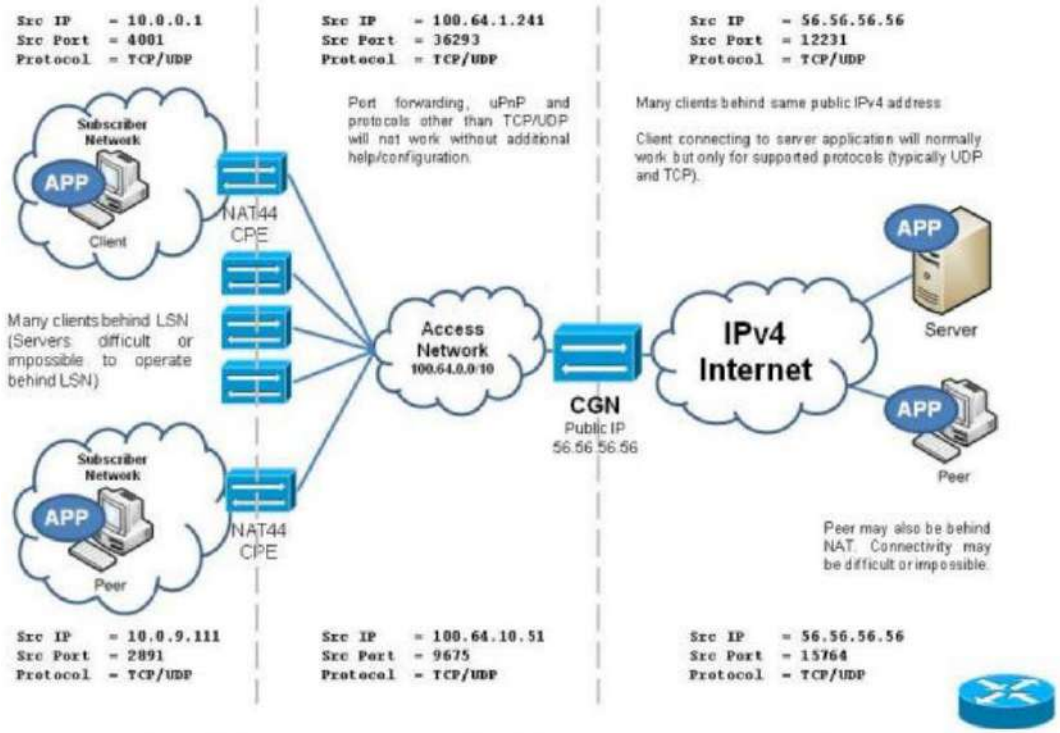
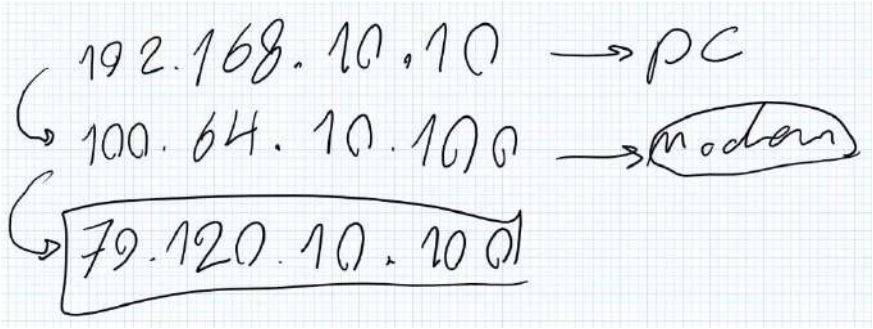


Figure 3.3 - The Internet and Access Networks with the Introduction of CGN

نکته: CGNAT میتواند ۲ یا ۳ بار یک IP را NAT کند که به آن NAT44 و NAT444 گفته می‌شود (به علت کمبود)

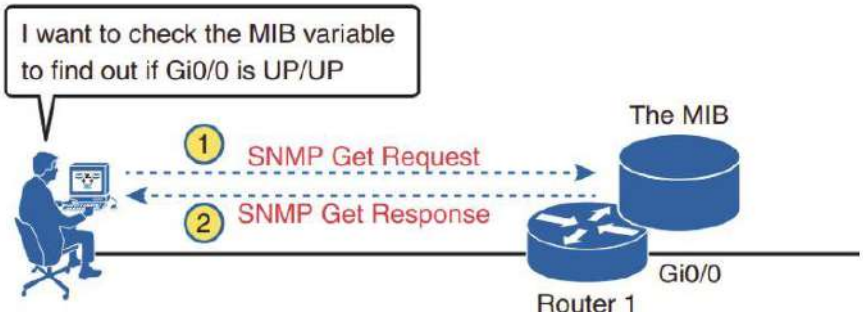
به عنوان مثال :



Simple Network Management Protocol (SNMP) :

در بسیاری از شبکه‌های کامپیوتری نرم افزارهای مانیتورینگ وجود دارند. با این نرم افزارها می‌توان به بررسی اطلاعات کامل و دقیق از تمامی بخش‌های شبکه پرداخت. تمامی این نرم افزارها با استفاده از پروتکل‌های مختلفی مثل NetFlow، ICMP، ARPو از همه مهم‌تر SNMP اقدام به اسکن و بررسی شبکه می‌کنند.

پروتکل SNMP یکی از پروتکل‌های لایه Application(یا لایه5 TCP/IP با پورت UDP162 , UDP161) است (که clientی server رفتار می‌کند) که امکان نقل و انتقال اطلاعات مدیریتی را بین عناصر شبکه ایجاد می‌کند. این پروتکل به طور وسیعی برای مانیتورینگ و مدیریت اجزاء شبکه استفاده می‌شود. بسیاری از وندورها، تجهیزات تولیدی خود را به پروتکل SNMP مجهز می‌کنند تا امکان نظارت بر عملکرد آنها به کمک نرم افزارهای مانیتورینگ فراهم شود. در حال حاضر سه نسخه از پروتکل SNMP وجود دارد: SNMPv1، SNMPv3 .و SNMPv2.



نکته: این پروتکل بر روی Deviceهایی که این قابلیت را پشتیبانی می‌کند صورت می‌گیرد.

با استفاده از نرم افزارهای زیر می‌توان مانیتورینگ کرد:

Zabix، PRTG ، SolarWinds ، Cacti و...

- SNMPv1 :

امنیت این ورژن پروتکل SNMP بسیار پایین است. هنگامی که ارسال جواب از سمت SNMP Agent به NMS در حال انتقال است، به راحتی می‌توان جواب را تغییر داد. در واقع این نسخه فقط community-based است.

- SNMPv2 :

این ورژن پروتکل SNMP شامل سه نوع است که در مجموع امنیت بهتری از ورژن ۱ دارد.

SNMPv2c : نسخه ای از ورژن ۲ است که فقط community-based است.

SNMPv2u : نسخه ای از ورژن ۲ است که فقط user-base است، یعنی میتوانید جهت احراز هویت، نام کاربری تعریف کنید.

نکته : در این ورژن می‌توانید به جای ارتباط Write-Read با Read Only بهره ببرید تا دیتاها توانایی تغییر نداشته باشند.

- SNMPv3 :

این ورژن ایمن‌ترین، کامل‌ترین و همچنین پر دردسرترین ورژن پروتکل SNMP است .

در SNMPv3 بسته ها کاملاً Encrypt می‌شوند. همچنین user-base است و NMS نیاز به رمزی برای احراز هویت دارد.

اجزای اصلی پروتکل SNMP:

- ✓ SNMP Manager
- ✓ Managed Devices
- ✓ SNMP Agent
- ✓ Management Information Base (MIB)

SNMP Manager: که با نام Network Management System(NMS) هم شناخته می‌شود، وظیفه برقراری ارتباط و تبادل اطلاعات با SNMP Agentهای فعال در تجهیزات شبکه را بر عهده دارد. به زبان ساده‌تر، یکSNMP Manager کامپیوتری است که بر روی آن یک نرم‌افزار مانیتورینگ شبکه نصب شده است و وظیفه مانیتورینگ شبکه را بر عهده دارد. وظایف یک SNMP Manager به طور عمده عبارتند از :

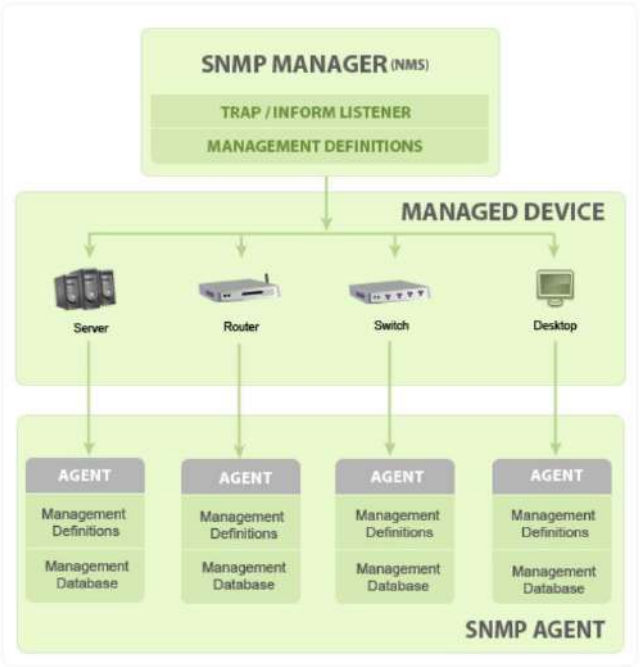
- ارسال پرس‌وجو به Agentها
- دریافت پاسخ از Agentها
- ست کردن متغیرها در Agentها
- دریافت پیغام‌های Trap از Agent ها

Managed Devices : منظور از Managed Device همه دستگاه‌های شبکه هستند که بر روی آنها SNMP Agent فعال شده باشد، مثل روترها، سوئیچ‌ها، سرورها و فایروال‌ها.

SNMP Agent : یک SNMP Agent در اصل برنامه‌ای است که بر روی تجهیزات شبکه کار گذاشته شده تا قابلیتSNMP را به آنها اضافه کند و وظیفه اصلی آن پاسخ دادن به درخواست‌های ارسال شده از طرفSNMP Manager است. وقتی SNMP Agent روی یک دستگاه فعال می‌شود، شروع به ثبت شاخص‌ها و اطلاعات دستگاه به صورت Local می‌کند و این اطلاعات را در دسترس NMSها (SNMP Manager) قرار می‌دهد.

این Agentها می‌توانند استاندارد باشند. مثل (Net-SNMP) یا مخصوص یک وندور باشند مثل (HP Insight Agent) . به طور کلی وظایف یک SNMP Agent عبارتند از:

۱. جمع‌آوری اطلاعات مدیریتی از دستگاهی که روی آن نصب شده است.
۲. نگهداری و فراخوانی اطلاعات مدیریتی بر اساس MIB مربوطه.
۳. ارسال سیگنال به NMS شبکه.



MIB- Management Information Base یا پایگاه داده اطلاعات مدیریتی : هر SNMP Agent دارای یک پایگاه داده برای معرفی و توصیف پارامترهای قابل نظارت و اندازه‌گیری است. به عبارتی SNMP Managerها از این پایگاه داده جهت ارسال درخواست به Agent ها برای دریافت پارامترهای مورد نظر و همچنین تفسیر پاسخ‌ها مطابق با تعاریف صورت گرفته توسط وندور استفاده می‌کنند. به زبان ساده، یک MIB یک پایگاه داده متنی است که فهرست پارامترهای قابل مانیتورینگ روی دستگاه را مشخص می‌کند و زبان مشترک بین Agent و Managerاست، شاید بتوان گفت فایل‌های MIB مجموعه‌ای از سوالاتی است که یک NMS می تواند از دستگاه تحت مانیتورینگ بپرسد.

**به طور کلی SNMP Agent شامل یک Database یا پایگاه است که به آن MIB می گویند.

نکته: تمامی اطلاعاتی یک دستگاه می‌تواند از خود به سمت NMS ارسال کند، به شکل یک Tree در آن قرار دارد. به هر یک از اطلاعاتی که در MIB قرار دارد OID یا Object identifier گفته می‌شود که شامل آدرس آن Tree میباشد. در نتیجه، تمامی اطلاعاتی که درون MIBوجود دارند، OID نام دارد. برای دریافت اطلاعات یک OID باید آدرس آن را به سمت SNMP Agent توسط پروتکل SNMP ارسال کنید.

انواع MIB ها در پروتکل SNMP :

MIBها به دو دسته Public و Private تقسیم می‌شوند:

MIBهایPublic : در تمام دستگاه‌ها قالب یکسانی دارند و پشتیبانی می‌شوند. مثل MIBهای RFC1759 که برای تمامی پرینترها است و یا RFC1213 که اطلاعات شبکه‌ی دستگاه را می‌دهد که درون تمامی دستگاه‌ها وجود دارد.

MIBهایPrivate : توسط شرکت سازنده دستگاه‌ها ارائه می‌شوند و فقط در دستگاه‌های آن ها وجود دارد. مثل MIBیCISCO-VTP- MIBکه فقط درون دستگاه های سیسکو وجود دارد.

انواع درخواست های پروتکلSNMP :

از NMS به SNMP Agent با استفاده از درخواست‌ها و فرمان‌های زیر می‌توان مقادیر MIB ها را دریافت کرد:

Get--- > جهت دریافت دیتای یک OID خاص

Get next---> جهت دریافت دیتای یک آدرس بعد از آخرین آدرس GET شده.

Set---> برخی از OIDها در حالت Write-Read قرار دارند که از NMS می‌توان مقدار آن OID را توسط این فرمان تغییر داد.

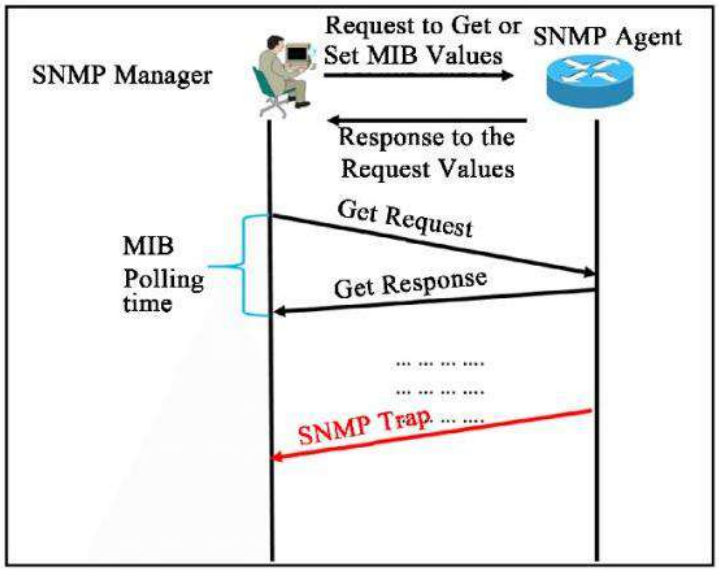
Getbulk---> جهت دریافت دیتا از جدولی که تعداد زیادی OID دارد که هر OID شامل چندین خروجی است.

Trap---> یک نوع Notification از وضعیت SNMP Agent برای NMSها بدون Acknowledge.

Inform---> همان Trap می‌باشد با این تفاوت که دارای Ack است و می‌توانید از ارسال بسته اطمینان حاصل کنید.

:SNMP Trap

یک سری دیتا مشخص شده می‌باشد که به صورت اعلان و به طور خودکار و بدون نیاز به ارسال درخواست، ازSNMP Agent یا همان Device Managed برای NMS ارسال می‌شود.



برای فعال‌سازی این ابزار باید آدرس NMS را به دستگاه بدهید تا بداند که دیتای Trap برای کی ارسال شود.

نکته: برای فعال‌سازی Trap در دستگاه‌ها و Managed Deviceها باید SNMP فعال باشد. Trap وضعیت روشن یا خاموش بودن Interface ها، خاموش یا روشن شدن دستگاه‌ها، مشکلات و وضعیت در لحظه تجهیزات و دستگاه‌ها را در لحظه به NMS ارسال می‌کند.

Time Setting Configuration :

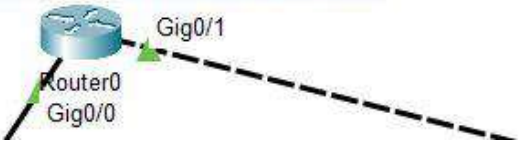
```
Router(config)#clock timezone <TEH> <3 30>
Router#clock set 20:49:50 24 Sep 2015


Router#show clock
```

The following example specifies that summer time starts on the first Sunday in April at 02:00 and ends on the last Sunday in October at 02:00. The **recurring** keyword indicates that the rules apply every year.

```
router(config)# clock summer-time PDT recurring 1 Sunday April 2:00 last Sunday October 2:00
```

مثال: تنظیم Time به صورت دستی

```
Router(config)#int g 0/0
Router(config-if)#no sh
Router(config-if)#ip address 192.168.10.1 255.255.255.0
Router#show clock
Mon Mar 1 1993

Router#clock set 20:49:50 24 Sep 2015 `
```



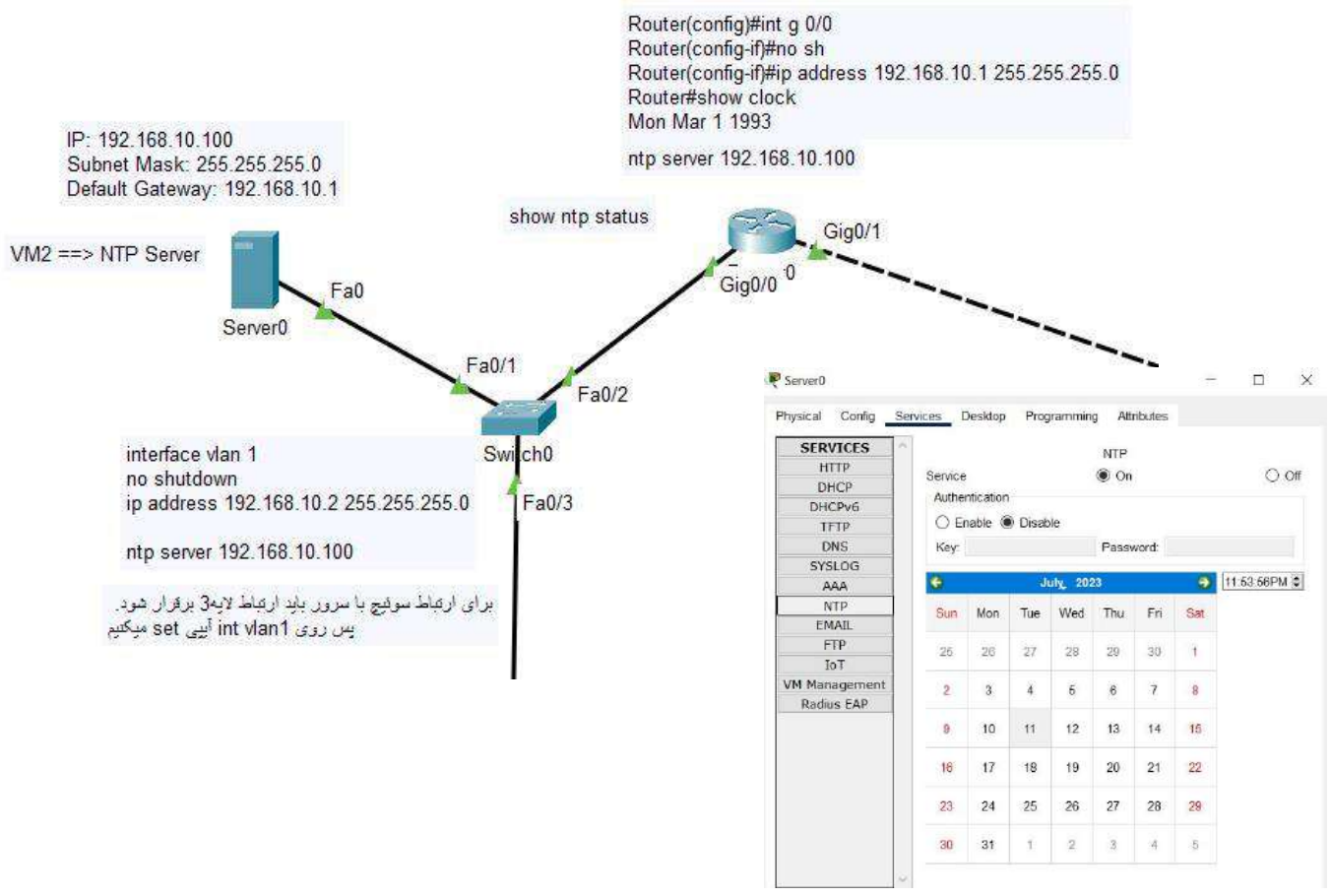
نکته : در مثال قبل اگر تعداد Deviceها زیاد شوند، Set کردن Time دشوارتر می‌شود. به همین دلیل به سراغ **پروتکل NTP** (Network Time Protocol) رفتند.

```
Router(config)#ntp server <NTP IP ADDRESS> [prefer]

Router#show ntp status
Router#show ntp association
```

UDP 123

– در این روش، NTP را روی سرور فعال می‌کنیم و در در صورت اصلاح زمان و تاریخ ، همه Deviceها خودشان را Sync می‌کنند.

مثال: تنظیمات زمان با NTP




```
Router#show ntp status
Clock is synchronized, stratum 16, reference is 192.168.10.100
nominal freq is 250.0000 Hz, actual freq is 249.9990 Hz, precision is 2**24
reference time is E8299B84.00000251 (11:48:20.593 UTC Fri Jul 7 2023)
clock offset is 5.00 msec, root delay is 11.00  msec
root dispersion is 50.28 msec, peer dispersion is 0.12 msec.
loopfilter state is 'CTRL' (Normal Controlled Loop), drift is - 0.000001193
ago.
```

Startum اولویت ntp به حساب می آید

System Message Logging (Syslog) :

Logging type:

UDP 514

Keyword	Numeral	Description	
Emergency	0	System unusable	Severe
Alert	1	Immediate action required	
Critical	2	Critical Event (Highest of 3)	Impactful
Error	3	Error Event (Middle of 3)	
Warning	4	Warning Event (Lowest of 3)	
Notification	5	Normal, More Important	Normal
Informational	6	Normal, Less Important	
Debug	7	Requested by User Debug	Debug

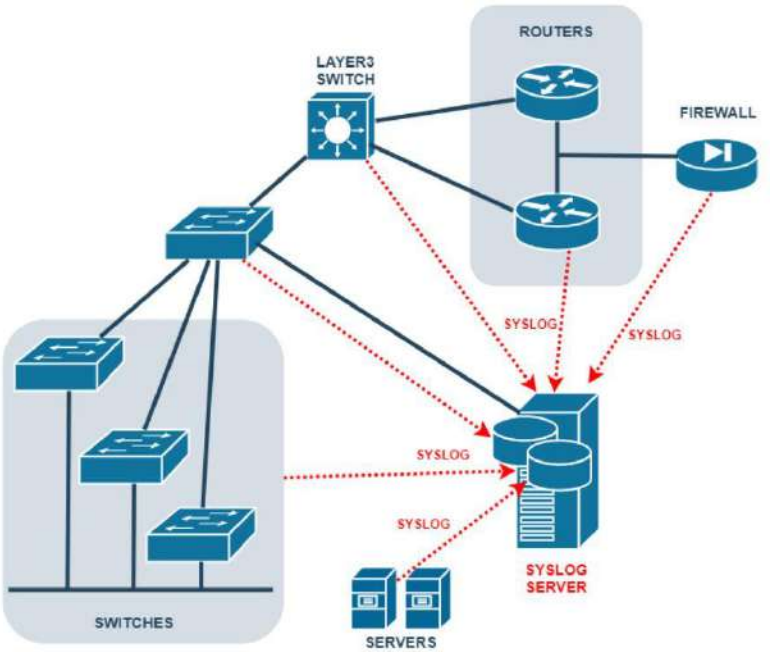
Service	To Enable Logging	To Set Message Levels
Console	logging console	logging console *level-name* | *level-number*
Monitor	logging monitor	logging monitor *level-name* | *level-number*
Buffered	logging buffered	logging buffered *level-name* | *level-number*
Syslog	logging host *address* | *hostname*	logging trap *level-name* | *level-number*

Log Message Format:

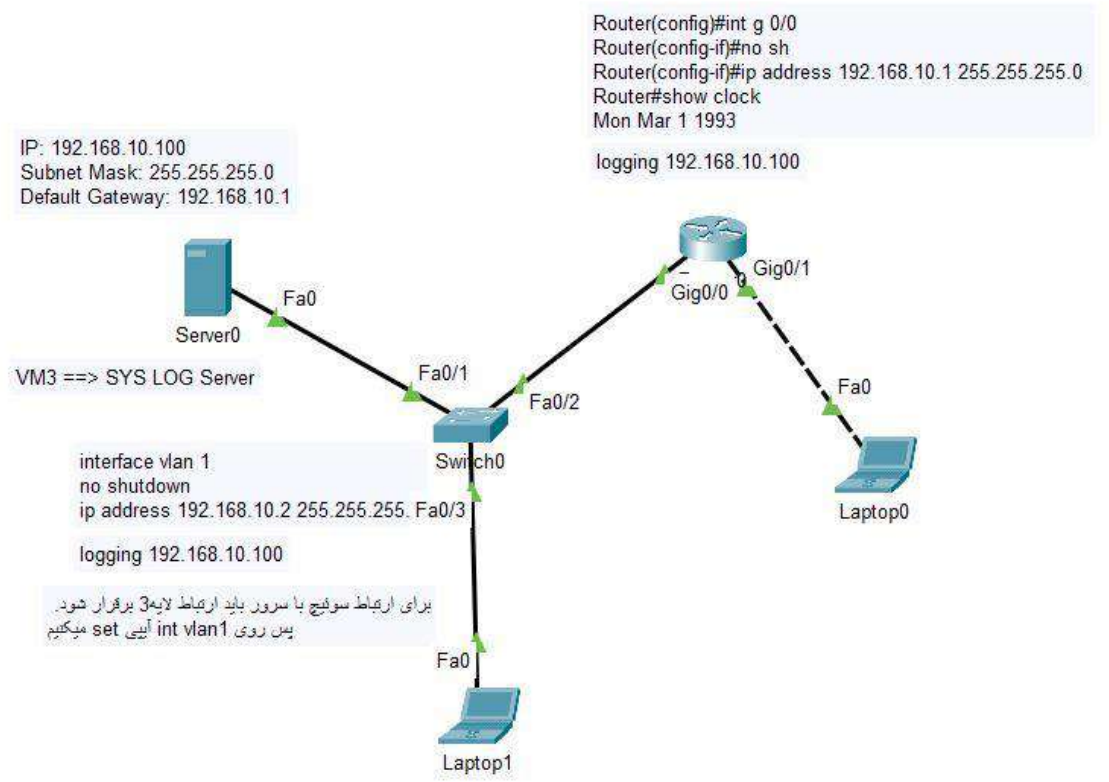
*Dec 18 17:10:15.079: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to down

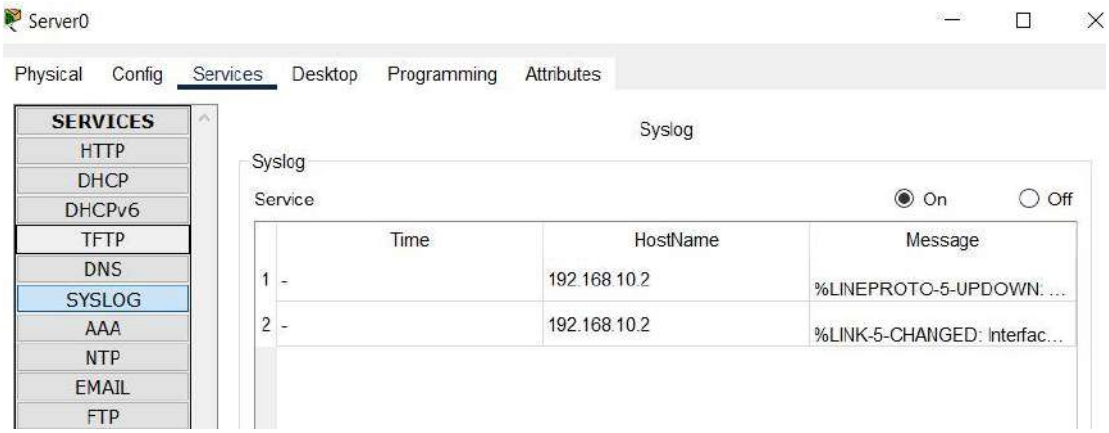
Notice that by default on this particular device, we see the following:

A timestamp: *Dec 18 17:10:15.079
The facility on the router that generated the message: %LINEPROTO
The severity level: 5
A mnemonic for the message: UPDOWN
The description of the message: Line protocol on Interface FastEthernet0/0, changed state to down



مثال:





نرم افزارهایی مانند: kiwi، PRTG ، syslog watcher و...

Cisco Discovery Protocol (CDP) :

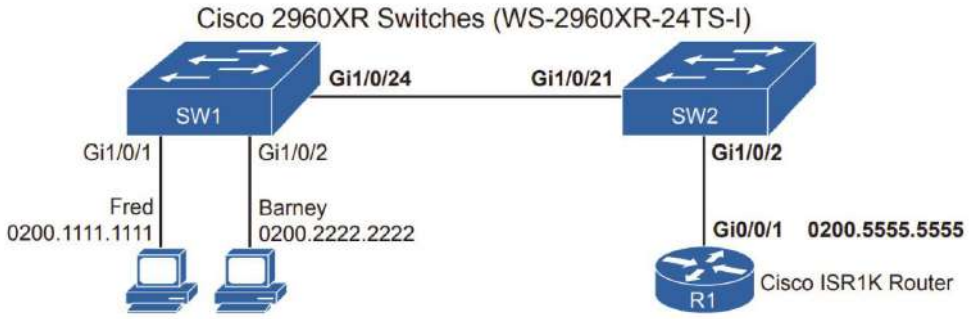
سیسکو CDP را در سال ۱۹۹٤ معرفی کرد که یک مکانیزم برای مدیریت سیستم می‌باشد که بتواند به صورت خودکار در مورد دستگاه متصل به شبکه اطلاعات کسب کند(برای بدست آوردن Topology شبکه). CDP روی دستگاه های سیسکو (روتر ، سوئیچ ، تلفن و ...) اجرا می‌شود. استفاده از CDP باعث می‌شود که دستگاه‌های شبکه به صورت دوره‌ای اطلاعات خود را به یک آدرس Multicast در

شبکه ارسال کنند. در نتیجه این امکان را برای سایر دستگاه‌ها یا نرم افزارها فراهم می‌کند که به اطلاعات ارسالی توسط این پروتکل دست پیدا کنند. به مرور زمان بهبودهایی در این پروتکل بوجود آمد تا قابلیت های آن افزایش یابد.

CDP (Cisco Discovery Protocol) is a Cisco proprietary protocol which has been in use on Cisco devices for many years. If CDP is enabled, a device will send out information about itself using the multicast MAC address 01-00-0c-cc-cc-cc

برنامه های کاربردهایی مانند Vocie به این پروتکل وابسته شدند تا بتوانند به درستی کار کنند. این وابستگی باعث بروز مشکلاتی در ارتباط با سایر برندها شد. بنابراین برای ارتباط بین تجهیزات برندهای مختلف نیاز به یک پروتکل استاندارد احساس شد. پروتکل استانداردی که تعریف شد LLDP می باشد که به عنوان بخشی از AB 802.1می‌باشد که بصورت استاندارد قابلیت discovery را فراهم می‌کند. همچنین یک بهبود تحت عنوانMedia Endpoint Discovery (MED) برای برنامه های Voice برای آن ارائه شد.

این پروتکل به صورت پیش فرض روی دستگاه‌ها فعال است و پیشنهاد می‌شود که CDP را روی پورت‌های غیرقابل اطمینان و پورت‌هایی که نیاز به این پروتکل ندارند غیر فعال شود. CDP در لایه دو عمل می‌کند و می‌تواند اطلاعاتی مانند نوع دستگاه، نسخه نرم افزار و سخت افزار ، اطلاعات IP و VLAN و ... را در اختیار مهاجم قرار دهد. در مثال زیر نحوه تنظیم و همچنین غیرفعال کردنCDP را به صورت global و به ازای اینترفیس نمایش داده است.



Command	Description
show cdp	States whether CDP is enabled globally and lists the default update and holdtime timers
show cdp interface [*type number*]	States whether CDP is enabled on each interface, or a single interface if the interface is listed, and states update and holdtime timers on those interfaces
show cdp traffic	Lists global statistics for the number of CDP advertisements sent and received

```
SW2# 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              Gig 1/0/21        155              S I   WS-C2960X Gig 1/0/24
R1               Gig 1/0/2         131            R S I   C1111-8P  Gig 0/0/1

Total cdp entries displayed : 2
```

[no] cdp run	Global command that enables and disables (with the no option) CDP for the entire switch or router.
[no] cdp enable	Interface subcommand to enable and disable (with the no option) CDP for a particular interface.
cdp timer *seconds*	Global command that changes the CDP send timer (the frequency at which CDP sends messages).
cdp holdtime *seconds*	Global command that changes how long CDP waits since the last received message from a neighbor before believing the neighbor has failed, removing the neighbor's information from the CDP table.

نکته: بهتر است برای امنیت بیشتر، در Global، CDP را غیر فعال کنیم و صرفا زیر اینترفیس‌هایی که در شبکه هستند آن را فعال کنیم.

```
router(config)#no cdp run
router(config)#interface fastethernet 0/0
router(config-if)#no cdp enable
```

*** توجه: اگر Device روبرو سیسکویی نباشد باید از **LLDP** استفاده کنیم.

LLDP (Link Layer Discovery Protocol) is a vendor-neutral standard defined by the IEEE in 802.1AB. It allows devices from different manufacturers to learn information about each other and behaves similarly to CDP. LLDP uses Ethernet frames and is usually sent to one of several multicast MAC addresses (01:80:c2:00:00:0e, 01:80:c2:00:00:03 or 01:80:c2:00:00:00) with the Ether type 0x88CC.

Command	Description
[no] lldp run	Global command to enable and disable (with the no option) LLDP for the entire switch or router.
[no] lldp transmit	Interface subcommand to enable and disable (with the no option) the transmission of LLDP messages on the interface.
[no] lldp receive	Interface subcommand to enable and disable (with the no option) the processing of received LLDP messages on the interface.
lldp timer *seconds*	Global command that changes the LLDP send timer (the frequency at which LLDP sends messages).
lldp holdtime *seconds*	Global command that changes how long LLDP waits since the last received message from a neighbor before believing the neighbor has failed, removing the neighbor's information from the LLDP table.

Password Recovery :

Password recovery of Cisco routers:

پسورد روتر سیسکو یا همان کلمه عبور، اولین لایه محافظت از روتر سیسکو در مقابل دسترسی‌های غیرمجاز است. گاهاً پیش آمده که نیاز به بازیابی کلمه عبور روتر سیسکو (ریست پسورد روتر سیسکو) داشته باشید. برای مثال روتر سیسکو دست دوم خریداری کرده اید یا کلمه عبور روتر سیسکو فراموشتان شده.

مراحل بازیابی کلمه عبور روتر سیسکو بسیار آسان و سریع است. مراحل کار بدین ترتیب است:

-قدم اول: کابل کنسول را به روتر متصل کرده و نرم افزار putty را SecureCRT را باز کنید.

- قدم دوم: روتر را خاموش و روشن کنید؛ پیش از decompress شدنIOS (حدودا ٦٠ ثانیه اول روشن شدن روتر)، کلید PauseBreak+Ctrlیا C+Shift+Ctrl را بزنید تا وارد محیط Rommon شوید .

- قدم سوم: دستور confreg 0x2142 را وارد کرده و با اجرای دستور reset، روتر را دوباره راه اندازی کنید.

-

```
rommon 1>confreg 0x2142
rommon 2>reset
```

روتر Reboot و فاقد تنظیمات بالا می‌آید. حال وارد Enable Mode شده و دستور زیر را وارد کنید تا تنظیمات Startup-config بر روی running-config کپی شود:

```
Router>enable
Router#copy startup-config running-config
```

نکته: توجه داشته باشید در صورتی که دستور را به صورت copy running-config Startup-config وارد کنید، تمامی تنظیمات روتر پاک خواهد شد.

پس از کپی شدن تنظیمات بر روی روتر، پسورد را تغییر دهید

```
Router(config)#enable password 1234
```

در مرحله آخر با استفاده از دستور زیر ، به حالت قبل برمی‌گردیم :

```
Router (config)#config-register 0x2102
```

نکته: تمامی اینترفیس های فیزیکی بعد از این عملیات به حالت administrative shut درخواهد آمد که نیاز به up کردن دستی خواهد داشت.

1 – To initiate the password recovery procedure, connect the rollover cable to the console port, then power the router off and back on. As soon as you receive a prompt showing the boot process, hit Ctrl-Break:

2 – Now, to skip our password-protected configuration, we instruct the router to by-pass the configuration located in NVRAM during bootup, and reset the router:

```
rommon 1 > confreg 0x2142    (by Def. 0x2102)
rommon 2 > reset
```

```
R1#show version | include register
Configuration register is 0x2102
```

3 - The router will now reset and start its normal bootup process, however, the current configuration will be ignored. When the bootup is complete, you will be prompted to 'enter the initial configuration dialog', answer 'no':

```
Router> enable
Router# copy startup-config running-config
Destination filename [running-config]? (hit enter)

Router# configure terminal
Router(config)# enable password <>
Router(config)# enable secret <>
Router(config)# line console 0
Router(config-line)# password <>
Router(config)# username <> privilege 15 secret <>
```

4 – Lastly, we need to change the 'configuration register' so the router will load the newly modified configuration next time it reboots, save our settings and reboot the router

```
Router(config)# config-register 0x2102

Router(config)# exit
Router# copy running-config startup-config
Destination filename [startup-config]? (hit enter)
Router# reload
```

```
R1#show version | include register
Configuration register is 0x2102
```

The default value is 0x2102, what does this mean? Let's break it down:

Hexadecimal	2	1	0	2
Binary	0010	0001	0000	0010
Bit Number	15 14 13 12	11 10 9 8	7 6 5 4	3 2 1 0

The 0x part means that we are looking at hexadecimal characters. 2102 is the default setting that tells the router to use a console speed of 9600 baud and to load the Cisco IOS image from flash memory.

- bit 13 tells the router to boot the default ROM software if network boot fails.
- bit 8 disables break.
- bit 1 tells the router to boot the first system image in onboard flash memory.

Bit 5, 11 and 12 are used to change the baud rate. If you don't touch these settings then the default will be 9600 baud.

Password recovery of Cisco :

در برخی از موارد ممکن است پسورد ورود به کنسول سوئیچ سیسکو را فراموش کرده‌اید و یا شخص دیگری این پسورد را تعیین کرده و به او دسترسی ندارید. اگر به تنظیمات سوئیچ خود نیاز ندارید. در این شرایط یا باید کلید Mode سوئیچ را به مدت ۱۵ ثانیه نگه دارید تا تمامی تنظیمات سوئیچ حذف شده و سوئیچ reset Factory شود (سوئیچ به حالت کارخانه برگرد)، ولی اگر به تنظیمات سوئیچ نیاز دارید، باید آن را recovery passwordکنید.

پسورد ریکاوری سوئیچ با روتر تفاوت دارد، برای پسورد ریکاوری سوئیچ مراحل زیر را انجام دهید:

۱. پورت کنسول را به سوئیچ متصل کرده و نرم افزار putty را SecureCRT را باز کنید.

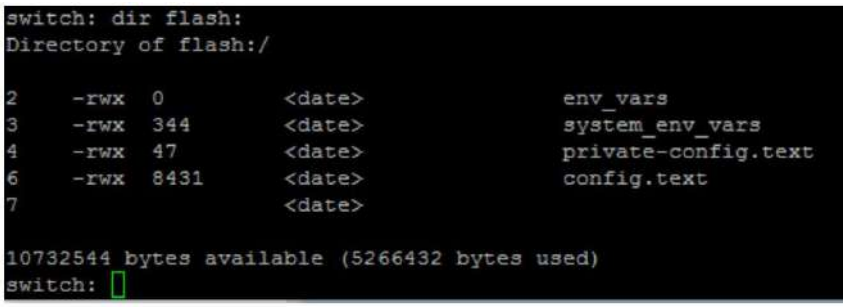
۲. سوئیچ را خاموش کرده، کلید Mode را بین ۳۰ تا ٤٠ ثانیه نگه داشته و سوئیچ را روشن کنید تا قبل ازextract کردن IOS ، وارد محیط ریکاوری شود. عبارت"switch:" بر روی کنسول مشاهده می‌کنید:

۳. در این مرحله، سوئیچ هنوز Flash خود را detect نکرده است. با توجه به اینکه تنظیمات سوئیچ در Flash قرار دارد، با اجرای دستور زیر، flashرا Detect خواهد کرد:

Switch: Flash_init

٤. پس از شناسایی Flash، محتویات آن را با اجرای دستور زیر مشاهده کنید:

Switch: dir flash:



**نکته: در صورتی که دستور no service password recovery بر روی سوئیچ اجرا شده باشد، پیغامی ظاهر می‌شود که recovery password غیرفعال شده و تنها راه Recover کردن پسورد، حذف تمامی Config است.

۵. حال باید فایل Config.text را به نام دیگری Rename کنید، برای انجام این کار از دستور زیر استفاده کنید:

Switch: rename flash:config.text flash:config.old

٦. پس از Rename کردن فایل Config، با اجرای دستور boot، سوئیچ را reboot کنید.

Switch: boot

۷. پس از بوت شدن سوئیچ، سوئیچ خام و فاقد تنظیمات می‌باشد، برای بازگرداندن تنظیمات، از دستورات زیر استفاده کنید، دستور اول نام فایل Config را به فرمت اصلی بر می‌گرداند و دستور دوم تنظیمات شما را که در فایلConfig.txt قرار دارد به مموری یا-running configمنتقل می‌کند.

```
Switch# rename flash:config.old flash:config.text
Switch# copy flash:config.text system:running-config
```

۸. پس از بازگرداندن تنظیمات، پسورد را تغییر داده و تنظیمات را ذخیره کنید.

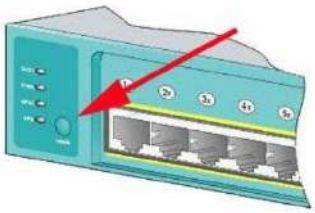
Step 1: Connect your PC or terminal into the switch console port with the blue console cable.

Step 2: Open up a Hyperterminal for emulation and set the speed to 9600 baud.

Step 3: Unplug the power cable to the switch.

Step 4: Press and hold the **MODE** button on the front of the switch and plug the power cable back into the switch at the same. After the power cable has been plugged in, wait a couple of seconds and then release the **MODE** button.

Step 5: Your display on your HyperTerminal should look like this… **switch:**



Step 6: Enter these commands into the switch
•switch: **flash _init**
•switch: **load_helper**
•switch: **dir flash:**

Directory of flash:
•13 drwx 192 Mar 01 1993 22:30:48 c2960-mz-124-0.0.53
•11 -rwx 5825 Mar 01 1993 22:31:59 config.text
•18 -rwx 720 Mar 01 1993 02:21:30 vlan.da

•switch: **rename flash:config.text flash:config.text.old**
•switch: **boot**

Step 7: Once the switch reboots, answer **NO** to "Would you like to enter system configuration dialog? [Yes/No]:

Step 8: Get into the privilege prompt.
•Switch**>enable**
•Switch**#rename flash:config.text.old flash:config.text**
•Switch**#copy flash:config.text system:running-config**
•Source filename [config.text]?
•Destination filename [running-config]?
•Press **Enter** to copy

Step 9: Get into global configuration
•Switch#conf t
•Switch (config)**#enable secret password**
•Enter the password you would like

Step 10: Return to Privilege mode and save your config
•Switch (config)**#exit**
•Switch**#copy run start**

IOS Upgrade / Downgrade :

روترهای سیسکو هم مانند سیستم عامل‌هایی که استفاده می‌کنیم هر چند وقت یکبار باید بروزرسانی شوند و یا یک نسخه جدید از آنها روی روتر نصب شود. این فرآیند می‌تواند به دلایل مختلفی انجام شود، برای مثال ممکن است شما سخت افزار یا ماژول جدیدی به روتر خود اضافه کنید و بر همین اساس IOS شما هم باید این ماژول را پشتیبانی کند و یا اینکه قابلیت جدیدی از نظر نرم افزاری به IOS ها اضافه شده است که شما با

بروزرسانی به IOS جدید می‌توانید از این قابلیت جدید استفاده کنید و در نهایت اگر Bug ای در IOS های قدیمی وجود داشته است و در IOS جدید برطرف شده است.

شما می توانید با بروز رسانی به IOS جدید این Bug را برطرف کنید ، توجه کنید که IOS مثل ویندوز شما ممکن است بعد از مدت ها کارکرد دچار اختلال یه به اصطلاح فنی Corrupt شود و این بهترین گزینه است که بعد از چند وقت IOS خود را از اول نصب کنید.خوب قبل از اینکه به سراغ آموزش برویم یک سری نیازمندی های اولیه و تذکر ها وجود دارد که شما باید آنها را رعایت کنید. حتما به اندازه و ظرفیت حافظه Flash موجود روی روتر یا سویچ خود دقت کنید.

ممکن است اندازه حافظه Flash موجود روی روتر شما به اندازه ای نباشد که IOS جدید بتواند بر روی آن نصب شود بنابراین این مورد را حتما بررسی کنید. شما می توانید IOS خود را از طریق یک TFTP سرور موجود روی شبکه نصب و بروز رسانی کنید. نرم افزارهای رایگان زیادی وجود دارند که شما براحتی با استفاده از آنها می توانید یک TFTP سرور راه اندازی کنید.

بعد از اینکه TFTP سرور را در شبکه راه اندازی کردید از برقراری ارتباط با TFTPسرور اطمینان حاصل کنید. حالا فایل Image مربوط به IOSمربوطه را در TFTP سرور کپی کنید.

دقت کنید که برای بروز رسانی IOS روتر بصورت کلی دو روش وجود دارد: دستورالعمل اول برای روترهایی است که دارای حافظه Flash داخلی یا Internal Flash هستند و دستورالعمل دوم برای روترهایی است که از حافظه Flash Card های PCMCIA استفاده می کنند.

دستورالعمل بروز رسانی **IOS** روترهای سیسکو با استفاده از **Internal Flash**

۱. با استفاده از تنظیمات پیش‌فرض یک ارتباط کنسولی با دستگاه برقرار کنید (9600 baud rate, 8 databit ,no flow control)
۲. با استفاده از دستور Ping ارتباط بین روتر و TFTP سرور را آزمایش کنید. البته قبل از آن مطمئن شوید که Range آدرس IP شما با Rangeآدرس IP سرور TFTP یکسان باشد.
۳. با توجه به اینکه فرآیند Upgrade در حافظه Flash انجام می شود و تنظیمات روتر در NVRAM ذخیره می‌شود، این دو چندان ارتباطی با هم ندارند، اما بهتر است قبل از اینکه فرآیند Upgrade را انجام دهید، از تنظیمات و پیکربندی‌های روتر خود Backup بگیرید، چون در زمان Upgrade معمولاً نیست چه اتفاقی برای روتر بیوفتد. همچنین از IOS فعلی که بر روی روتر قرار دارد نیز یک Backup تهیه کنید تا زمانیکه در صورت احتمال IOS در زمان بروز رسانی دچار اختلال شد بتوانید از IOS قبلی استفاده کنید.
٤. با استفاده از دستور زیر فرآیند Upgrade را شروع کنید: ITPRO-Router#copy tftp flash

حالا شما به چیزی که در پایین مشاهده می‌کنید ، از شما آدرس IP سرور TFTP پرسیده خواهد شد :

Address or name of remote host []? XXX.XXX.XXX.XXX

بعد از وارد کردن آدرس TFTP سرور از شما نام فایل IOS ای که قرار است از TFTP کپی شود از شما مشابه پایین پرسیده می‌شود:

Source filename []? cXXXX-X-XX.XXX-XX.bin

به این نکته توجه کنید که اسم فایل IOS که می‌خواهید وارد کنید کاملا Case Sensitive است و باید دقت کنید که عین حروف را بدون کوچکترین تغییری وارد کنید. بعد از این مرحله از شما در خصوص نام فایلی که قرار است بر روی روتر مقصد قرار بگیرد سوال خواهد شد ، همانطور که در پایین مشاهده می‌کنید:

Destination filename []? cXXXX-X-XX.XXX-XX.bin

پیشنهاد می شود که این فایل را نیز همانند همان فایلی نامگذاری کنید که در TFTP سرور قرار گرفته است تا به سادگی این فایل و فایلی که روی روتر قرار گرفته است را بتوانیم مقایسه کنیم. حالا همانطور که در پایین مشاهده می کنید از شما سئوال می شود که آیا می خواهید فایل های موجود در حافظه Flashحذف شود یا خیر ؟ اگر فضای خالی به اندازه کافی روی Flash دارید ، ترجیحا IOS قبلی را حذف نکنید ، ممکن است بعدا به آن نیاز پیدا کنید.

Erase flash: before copying? [confirm]

بعد از تایید روتر شروع به کپی کردن فایل Image مربوط به IOS از TFTP سرور به داخل روتر می‌شود و یا برحسب انتخاب شما شروع به حذف و خالی کردن حافظه Flash می‌کند:

```
Erasing the flash filesystem will remove all files! Continue? [confirm]y
Erasing device… eeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeee
eeeeeeeeee …erased
Erase of flash: complete
Loading cXXXX-X-XX.XXX-XX.bin from XXX.XXX.XXX.XXX (via Ethernet0/0): !!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - xxxxx/yyyyyyy bytes]

Verifying checksum… OK (0xAC8A)
xxxxxx bytes copied in xx.xx secs (yyyy bytes/sec)
```

فرآیند کپی کردن IOS ممکن است چندین دقیقه بر حسب نوع شبکه‌ای که دارید زمان ببرد. در طی زمان کپی کردن پیام هایی نمایش داده می‌شود که نمایانگر فایل‌هایی است که به آنها دسترسی پیدا می‌شود. علامت تعجب یا ! به معنای این است که فرآیند کپی شدن در حال انجام است همانطور که در بالا مشاهده می‌کنید. هر کدام از علامت های تعجب به معنای کپی شدن ۱۰ بسته اطلاعاتی یا Packetمی باشد که با موفقیت کپی شده است. بعد از اینکه فرایند کپی به درستی انجام شد یک Checksum تایید یاVerification Checksum به داخل حافظه Flash روتر نوشته می‌شود.

۵. قبل از اینکه روتر را Reload کنید بایستی از دو چیز مطمئن شوید. اولین نکته این است که باید مطمئن شوید که configuration registerروتر شما مقدار 0×2102 است. برای بررسی این مورد کافیست دستورshow versionرا وارد کنید .اگر configuration registerشما مقدار 0×2102 را نمایش نمی دهد و هر چیزی به غیر از این است بایستی آن را بصورت دستی با استفاده از دستور زیر تبدیل به 0×2102 کنیم :

Router(config)#config-register 0×2102

دومین نکته ای که بایستی به آن توجه کنید (البته زمانیکه به سیستم گفته‌اید که Flash را پاک نکند) این است که روتر نباید از IOS قبلی بوت شود و شما باید به روتر بگویید از IOS قبلی استفاده نکند ، با استفاده از دستور اول زیر ، روتر شما از IOS قبلی سیستم دیگر استفاده نمی‌کند و با استفاده از دستور دوم روتر از IOSای که برایش تعریف می‌کنید بوت خواهد شد :

```
Router(config)#no boot system
Router(config)#boot system flash cXXXX-X-XX.XXX-XX.bin
```

۶. اگر دستور reload را در این مرحله وارد کنید، روتر از شما می‌پرسد که آیا می‌خواهید تنظیمات را ذخیره کنم یا خیر؟ در این مرحله شما باید بسیار دقت کنید و دلیلش هم این است که اگر روتر در boot mode قرار بگیرد، روتر دیگر قادر به انجام عملیات routing نخواهد بود. بنابراین در این هنگام ترجیحاً تمامی تنظیمات موجود در running-config را بر روی startup-config ذخیره کنید تا در زمان bootاین تنظیمات از بین نرود. توجه کنید زمانی تنظیمات را ذخیره کنید که همه تنظیمات را می توانید در خروجی دستور show run مشاهده کنید. به هر حال تایید را با y انجام دهید و ادامه دهید.

```
Router#reload
System configuration has been modified. Save? [yes/no]: y
Building configuration…
[OK]
Proceed with reload? [confirm]y
```

۷. برای اینکه مطمئن شوید Image جدید بصورت کامل در روتر Load شده است دستور show version را وارد کنید.

```
00:22:25: %SYS-5-CONFIG_I: Configured from console by console
Cisco Internetwork Operating System Software
IOS ™ CXXXX Software (CXXXX-X-X), Version XX.X(XX), RELEASE SOFTWARE (fc1)
Copyright (c) 1986-2002 by cisco Systems, Inc.
Compiled Mon 25-Mar-02 20:33 by xxxxx
Image text-base: 0x80008088, data-base: 0x80828788

ROM: System Bootstrap, Version xx.x(x)XA4, RELEASE SOFTWARE (fc1)

XXXX uptime is 22 minutes
System returned to ROM by reload
System image file is "flash: cXXXX-X-XX.XXX-XX.bin "     <<< Check it here
```

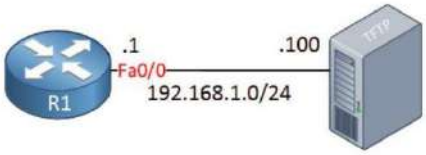
۸. روتر شما به IOS جدید بروزرسانی شد!

1 – Once you downloaded the IOS image, check if you have enough space left on your flash memory:

```
R1#show flash:
1    1119 Sep 29 2015 11:11:52 +00:00 r1-r2-r3.cfg
2    1184 Dec 3 2014 15:14:06 +00:00 R1-R2-ASA1-ASA2.cfg

3862364160 bytes available (137428992 bytes used)
```

2 – When we want to copy something to or from this router, we have to use the copy command:

```
R1#copy tftp: flash:
Address or name of remote host [ ]? 192.168.1.200
Source filename [ ]? c2800nm-adventerprisek9-mz.151-4.M12a.bin
Destination filename [c2800nm-adventerprisek9-mz.151-4.M12a.bin]?
```



3 - The transfer has completed, let's take a look at our flash memory:

```
R1#show flash: | include .bin
8    67926080 Apr 2 2015 14:21:46 +00:00 c2800nm-adventerprisek9-mz.151-4.M10.bin
25   67929600 Nov 4 2016 12:11:22 +00:00 c2800nm-adventerprisek9-mz.151-4.M12a.bin
```

4 – Most routers will select the first filename that they find on the flash memory so in our case, it means it would boot the older IOS image. We can change this with the boot system command:

```
R1(config)#boot system flash:c2800nm-adventerprisek9-mz.151-4.M12a.bin
```

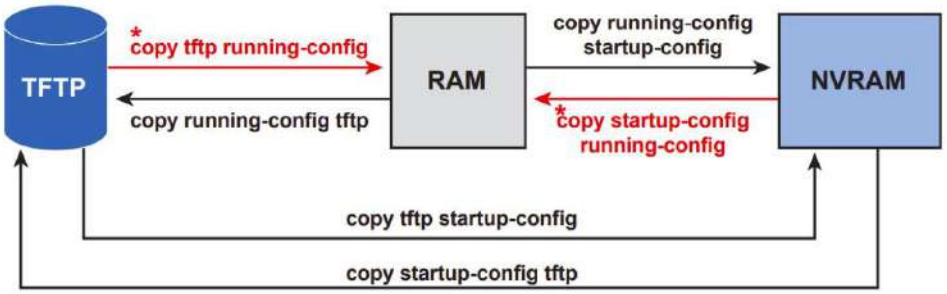
5 – Let's reload the router:

```
R1#reload

System configuration has been modified. Save? [yes/no]: yes
Building configuration...

[OK]
```

6 - Once the router has reloaded, verify that we are running the new IOS image:

```
R1#show version
```

Backup /Restore :



1 - Traditional Configuration Backup and Restore with the copy Command

2 - Alternatives for Configuration Backup and Restore

2-1 – First we need to configure where we want to store our configuration archives. When you use the path command you can see what options we have:

```
Router(config)#archive
Router(config-archive)#path ?
  flash:  Write archive on flash: file system
  ftp:    Write archive on ftp: file system
  http:   Write archive on http: file system
  https:  Write archive on https: file system
  pram:   Write archive on pram: file system
  rcp:    Write archive on rcp: file system
  scp:    Write archive on scp: file system
  slot0:  Write archive on slot0: file system
  tftp:   Write archive on tftp: file system
```

2-2 – Normally an external location would be a good idea but to keep things simple I will use the flash memory of my router:

```
Router(config-archive)#path flash:router-backup
```

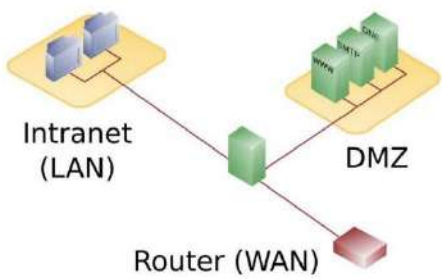
2-3 – I will also configure a schedule, for example to create a configuration archive each 24 hours:

```
Router(config-archive)#time-period 1440
```

Demilitarized Zone (DMZ) :

در جریان جنگی که بین کره‌شمالی و جنوبی پیش آمده بود (سال ۱۹۵۰ میلادی)، در پیشنهادی که از طرف سازمان ملل به دو کشور شد، قرار بر این شد که در میان مرز این کشور قسمتی را به عنوان منطقه غیرنظامی یا Demilitarized Zone انتخاب کنند تا مردم بتوانند از آن برای زندگی و امرار معاش بدون وارد شدن ساختار نظامی و جنگ استفاده کنند و همین مورد بین دو کشور توافق شد. مردم از این منطقه به عنوان منطقه ارتباطی بین دو کشوری که در حال جنگ بودند و به یکدیگر اعتماد نداشتند استفاده می‌کردند، اما در محیطی که به هیچیک از دو کشور صدمه ای وارد نشود.

در یک ساختار DMZ ساده در یک شبکه معمولی ، یک سرور یا کامپیوتر که در اینجا به عنوان Host معرفی می‌شود در محیط DMZ قرار می گیرد و تمامی درخواست‌هایی که کاربران داخلی برای برقراری ارتباط با خارج از شبکه دارند را دریافت می‌کند، این سرور بعد از دریافت این بسته‌های درخواست(مثال درخواست وب سایت) آنها را به سمت شبکه عمومی یا اینترنت هدایت می‌کند و سپس پاسخ این درخواست‌ها را در همان Session ای که توسط کاربر داخلی ایجاد شده بود برای وی ارسال می‌کند، توجه کنید که در این طراحی ساده، هیچگونه ترافیکی نمی‌تواند از شبکه بیرونی به شبکه داخلی وارد شود.

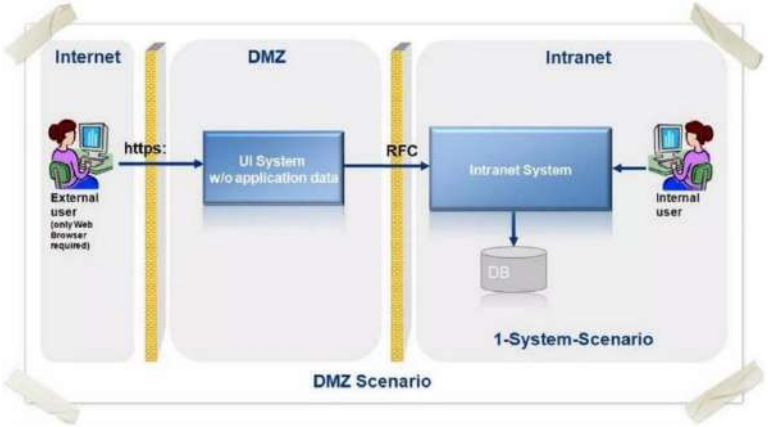


کاربرانی که در شبکه اینترنت یا خارجی قرار دارند صرفا می‌توانند بهHost ای که برای DMZ استفاده می‌شود دسترسی پیدا کنند و به هیچ عنوان به شبکه داخلی دسترسی نخواهند داشت. یکی دیگر از کارهایی که در اینHostمی‌تواند انجام شود این است که صفحات وب‌ای که قرار است از طرف سازمان بر روی اینترنت در معرض دسترسی قرار بگیرند می توانند بر روی این Host قرار بگیرند. اما توجه کنید که DMZ به شبکه داخلی نیز در این حالت دسترسی نخواهد داشت. شما فرض کنید که در این حالت یک هکر قصد حمله به وب سایت سازمان را دارد ، حتی اگر موفق به هک این صفحات شود، به اطلاعات خاصی در خصوص شبکه داخلی و اطلاعات خصوصی سازمان دست پیدا نخواهد کرد. بدون شک یکی از بهترین تجهیزات شبکه ای که برای استفاده ویژه در ساختار DMZ مورد استفاده قرار می‌گیرد تجهیزات فایروال شرکت سیسکو می باشد.

اگر بخواهیم از نظر امنیتی DMZ را تعریف کنیم، می‌توان آن را به نوعی تنظیمات پیشرفته در فایروال‌های شبکه نیز معرفی کنید. در تنظیمات DMZ اکثر کامپیوترهایی که در شبکه LAN قرار گرفته اند در پشت فایروال قرار می‌گیرند که این فایروال به شبکه اینترنت یا شبکه عمومی متصل شده است. از طرفی یک یا چندین سرور نیز در محلی بعد از فایروال قرار می‌گیرند ، یعنی در شبکه داخلی نیستند ، این سرورهایی که در بعد از فایروال قرار میگیرند ، درخواست های کاربران داخلی را همانطور که اعلام شد از شبکه داخلی دریافت کرده و سپس آنها را به شبکه اینترنتی که به آن متصل هستند ارسال می‌کنند ، این دقیقا همان مفهوم امنیتی است که مد نظر است، خاطرتان هست که در جنگ بین کره شمالی و جنوبی یک شهر به عنوان محل رابط بین دو کشور انتخاب شد که در آن جنگی در کار نبود ، این را دقیقا در شبکه نیز می توانید تصورکنید .

توجه کنید که شما واژه DMZ را در بسیاری از تجهیزات شبکه اعم از روترهای اینترنتی خانگی نیز مشاهده می‌کنید اما آنها واقعا DMZ نیستند بلکه صرفا قابلیت پشتیبانی از این نوع تنظیمات هستند که در تجهیزات شبکه دیده شده است. این نوع تجهیزات با طراحی واقعی DMZدر ساختارهای سازمانی به کلی تفاوت دارند ، آنها صرفاً چند Rule ساده در تنظیمات روتر خانگی هستند ، اما در DMZ های سازمانی، سرورها و تجهیزات حرفه ای در طراحی DMZ استفاده می‌شود .

در حوزه امنیت اطلاعات ممکن است DMZ به عنوان Perimeter Network نیز مطرح شود که نام دیگر همین نوع طراحی شبکه است. در اکثر سازمان‌های دولتی و حتی شرکت‌ها، سرویس‌هایی وجود دارد که سازمان‌ها قصد دارند به بیرون از شبکه ارائه دهند، مثال وب سایت یا پورتال سازمانی ، سرویس ایمیل ، سرویس میزبانی وب یا حتی سرویسDNS. فرض کنید که این سرویس‌ها را در درون شبکه داخلی قرار بدهید و به کاربرانی که از اینترنت قصد استفاده از این سرویس‌ها را دارند اجازه ورود به شبکه داخلی را بدهید، این خود یک نقطه ضعف امنیتی می‌باشد، بنابراین همیشه برای اینگونه سرویس‌های عمومی استفاده از طراحی DMZ توصیه می‌شود.

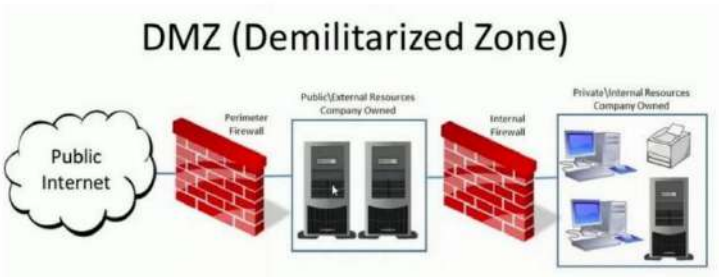


در چنین شرایطی شما سرویس‌ها و سرورهای مورد نظر خود را در محیط DMZ قرار می‌دهید و ارتباط محدودی با شبکه داخلی برای آنها ایجاد می‌کنید، ارتباطی که در سطح بسیار کم و با درصد خطر کمتری نسبت به ارتباطات معمول شبکه باشد. طراحی DMZ برای محافظت از حملاتی است که از بیرون سازمان به سرویس‌ها انجام می‌شود و معمولاً در این نوع طراحی خطرات شبکه داخلی سازمان از جمله Spoofing و Sniffing و ... دیده نمی‌شود.

سرویس‌هایی که نیازمند دسترسی عمومی می‌باشند را در این منطقه از شبکه قرار می‌دهیم که مهمترین و معروفترین سرویس‌هایی که در قسمت DMZ شبکه قرار می‌گیرند به شکل زیر می‌باشند:

- سرویس دهنده های وب یا Server Web ها
- سرویس دهنده های ایمیل یا Server Mail ها
- سرویس دهنده های Voip
- سرویس دهنده های FTP

نکته‌ای که در اینجا بسیار مهم است، این است که وب سرورهای سازمانی معمولاً صفحات ایستا نیستند که صرفاً چند صفحه باشند، بلکه صفحات دینامیکی هستند که در پس زمینه خود دارای یک پایگاه داده اطلاعاتی می‌باشند، این وب سرورها بایستی بتوانند از این پایگاه داده استفاده کنند، قاعدتاً اگر این پایگاه داده را در خود محیط DMZ قرار بدهید، کار اشتباهی خواهد بود. در این حالت پایگاه داده مورد نظر را یا در شبکه داخلی و پشت فایروال قرار می‌دهند و یا در پشت یک فایروال و در شبکه ای در همان طراحی DMZقرار می‌دهند. در این حالت اگر هکری موفق به نفوذ به وب سایت شود، صرفاً به صفحات وب سایت دسترسی پیدا می‌کند و نمی‌تواند داده‌ها و اطلاعات موجود در پایگاه داده را که در پشت فایروال دیگری قرار دارد را مورد هجوم قرار دهد.



سرویس‌های ایمیل یا همان Server Email ها نیز دارای اطلاعات کاربری و پایگاه داده خاص خود می‌باشند که آنها نیز بایستی محافظت شوند. همانطور که در طراحی قبلی اشاره کردیم آنها را نیز در پشت یک فایروال جداگانه قرار می‌دهیم، توجه کنید که معمولاً سرویس‌دهنده‌های ایمیل از سرویسی به نامWebmailپشتیبانی می‌کنند که می‌توان از طریق وب به آنها دسترسی داشت، شما می‌توانید ایمیل سرور خود را در پشت فایروال DMZ قرار داده و از طریق امکانی به نام Publishing صفحه وب ایمیل را برای دسترسی عمومی Publishکنید.

توجه کنید که ایمیل سرورهایی که به این شکل هستند هم ترافیک ورودی و هم ترافیک خروجی ایمیل‌ها را بایستی به درستی مدیریت کنند، طراحی DMZ ها با توجه به سرویس‌های موجود در شبکه متغیر هستند و DMZ یک ساختار ایستا و ثابت نمی‌باشد. به دلیل مسائل امنیتی و همچنین مسائل مانیتورینگ در یک محیط تجاری، بیشتر سازمان‌ها و شرکت‌ها در محدوده DMZ خود یک Server Proxy راه اندازی می‌کنند. راه اندازی این سرور در این محیط دارای مزایا به شرح زیر می‌باشد:

- اجبار کردن کاربران داخلی برای استفاده از Server Proxy برای استفاده از اینترنت
- کاهش نیاز به پهنای باند اضافی بر روی شبکه اینترنت به علت استفاده از قابلیت cache در پروکسی سرور
- ساده‌سازی فرآیند ضبط و مانیتورکردن استفاده کاربران از اینترنت
- متمرکزسازی فرآیند فیلترکردن وب سایت‌ها و محتویات وب

ممکن است در اینجا این سئوال پیش بیاید که حال اگر نیاز به این باشد که کاربری بتواند از بیرون به شبکه داخلی دسترسی پیدا کند، آیا ساختار DMZ این امکان را به وی می‌دهد یا خیر؟ در پاسخ به این سئوال بایستی بگوییم که سرویسی به نام Proxy Reverse وجود دارد که امکان دسترسی پیدا کردن کاربران خارجی به منابع داخلی شبکه را فراهم می‌کند، همانطور که Server Proxy به کاربران داخلی سرویس می‌دهد ، Proxy Reverseعکس این عمل را انجام می‌دهد ، یعنی به کاربران خارجی دسترسی داخلی را می‌دهد.

برای مثال فرض کنید که شما در ساختار DMZ خود یک سرویس ایمیل دارید و کاربران اینترنتی از آن استفاده می‌کنند، اما مدیر همین سرور تصمیم می‌گیرد به این سرور که در شبکه داخلی قرار داشته و توسط فایروال Publish شده است دسترسی پیدا کند، چه مشکلی پیش می آید ؟ با استفاده از Proxy Reverse شما می‌توانید به وی اجازه برقرار ارتباط Remote به سرور مورد نظر را بدهید. توجه کنید که در چنین حالت‌هایی برای کاهش خطرات موجود شما از فایروال‌های لایه هفتم یا Firewall Layer Application ها استفاده می‌کنید تا درصد بروز حملات به سرورها از طریق Proxy Reverse را کاهش دهید. این روش امن‌ترین روش برقراری ارتباط از خارج شبکه به داخل آن می‌باشد.

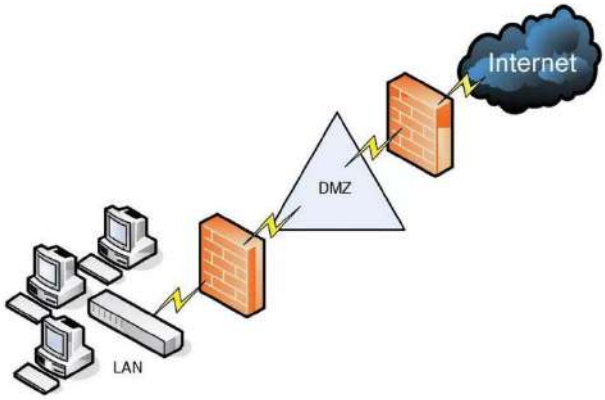
معماری های مختلف در ساختارDMZ

همانطور که اشاره کردیم روش‌های زیادی برای طراحی DMZ وجود دارد و هرکس می‌تواند با توجه به شرایط موجود طراحی ویژه سازمان خود از این روش را داشته باشد. شما می‌توانید در طراحی‌های DMZ از یک فایروال با سهکارت شبکه، یا از چندین فایروال جداگانه استفاده کنید. البته اینها طراحی‌های ساده‌ای از DMZ هستند، DMZ می‌تواند در ابعاد بسیار گسترده آنقدر بزرگ و پیچیده شود

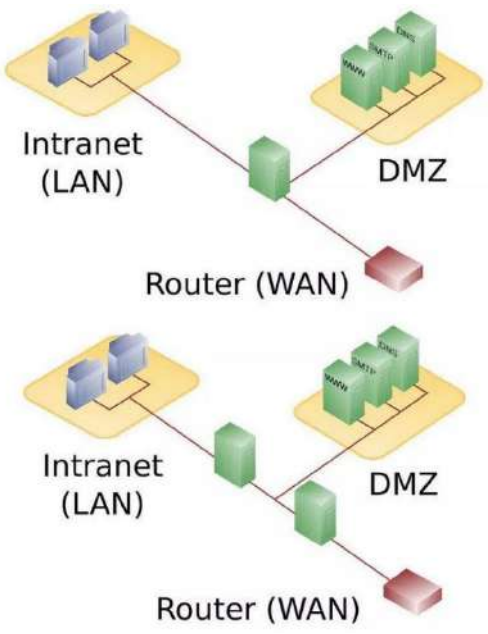
که واقعاً در حد این مقاله نمی‌باشد. اینکه چگونهDMZ را طراحی میکنید کاملاً به نیازمندی‌های سازمانی شما بستگی دارد. در ادامه دو نوع از روش‌های معمولی که DMZطراحی می‌شود را برای شما شرح می دهیم:

- ✓ DMZبا استفاده از یک فایروال

در این حالت شما یک فایروال سخت‌افزاری یا نرم‌افزاری دارید که دارای حداقل سه کارت شبکه می‌باشد که طراحی DMZ شما در این سه کارت شبکه جای می‌گیرد. ارتباط خارجی شما که به اینترنت و شبکه ISP متصل می‌شود، به درون کارت شبکه اول متصل می‌شود. شبکه داخلی شما به کارت شبکه دوم موجود و درنهایت شبکه DMZ شما نیز به کارت شبکه سومی که بر روی فای روال قرار دارد متصل می‌شود. در اینجا فایروال ما یکSPOF ایجاد کرده است ، به این معنی که با ازبین رفتن این فایروال یا بروز اختلال در آن، کلیه شبکه‌هایی که به آن متصل شده‌اند دچار مشکل خواهند شد. همچنین اگر ترافیک بین شبکه‌ها زیاد باشد، این فایروال به تنهایی ممکن است نتواند سرویس‌دهی را انجام دهد و شبکه شما کند شود. به هر یک از این کارت شبکه‌ها در اصطلاح یک Zone یا محدوده گفته می‌شود. معمولاً برای نمایش این ساختار برای مستندسازی از رنگ بنفش برای شبکه داخلی، سبز برای شبکه DMZ و قرمز برای شبکه اینترنت استفاده می‌شود.



- ✓ DMZ با استفاده از دو فایروال



استفاده از دو عدد فایروال در طراحی DMZ یکی از امن‌ترین طراحی‌های موجود در DMZ را به شما ارائه می‌دهد. اولین فایروال که به آن firewall end-front هم گفته می‌شود به گونه‌ای تنظیم می‌شود که ترافیک را از شبکه اینترنت دریافت و به آن ارسال می‌کند، این ترافیک قاعدتاً ابتدا به Zoneای که به DMZ معروف است متصل می‌شود. فایروال دوم به گونه‌ای تنظیم می‌شود که ترافیک ورودی و خروجی به شبکه داخلی را مدیریت می‌کند و در اصطلاح به آن firewall end-back گفته می‌شود.

این طراحی از امنیت بیشتری برخوردار است، دلایل مختلفی برای اثبات این موضوع وجود دارد. ایجاد مشکل و خرابکاری در دو فایروال طبیعی است که از یک فایروال سخت‌تر است و یک هکر به ناچار بایستی انرژی بیشتری برای هک این سرورها بگذارد. اگر فایروال‌های مورد استفاده در این طراحی از دو نوع مختلف باشند، درجه امنیتی را بالاتر خواهند برد، وجود نقطه ضعف امنیتی در یکی از سرورها باعث بروز مشکل در سرور دیگری یا فایروال دیگری نخواهد شد.

برای مثال فرض کنید که در چنین طراحی ، به عنوان end-front فایروال نرم افزاری TMG و به عنوان فایروال داخلی یا end-back فایروال سیسکو ASA قرار داده اید، حال اگر نقطه ضعف امنیتی بر روی TMG وجود داشته باشد و هکر بتواند به منطقه DMZ نفوذ کند، به دلیل عدم وجود همین نقطه ضعف در فایروال ASA حمله در همین نقطه باقی خواهد ماند.

Data Center Design :

دیتاسنتر و اتاق سرور استاندارد:

سرورها باید در اتاق سرور استاندارد مستقر شوند، چون امنیت فیزیکی و کنترل محیطی را به طور بهینه میتوان ارائه کرد؛ سرورهایی که در این اتاق قرار می‌گیرند باید تمام الزامات امنیتی در آنها رعایت شود.

اتاق سرور:

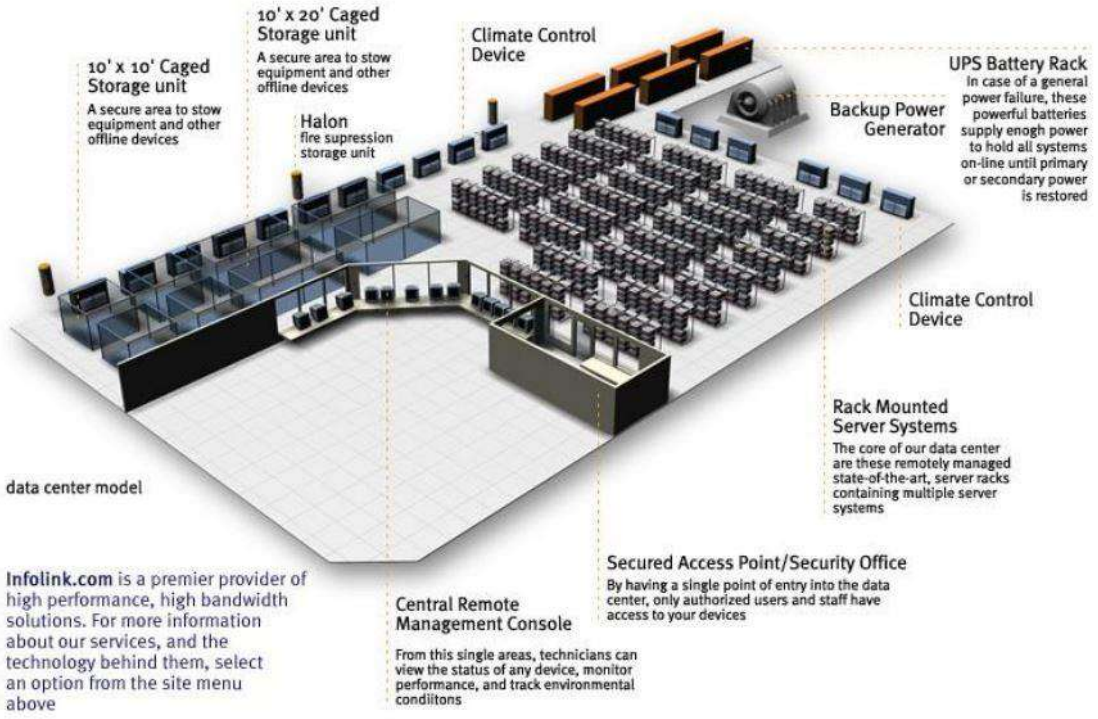
هر اتاقی که یک یا چند کامپیوتر برای ارائه خدمات برای گروهی از کاربران از طریق شبکه دارد، یک اتاق سرور نامیده می‌شود. این دامنه‌ای از اتاق سرور کوچک تا دیتاسنترهای بزرگ‌تر می‌باشد.

دیتاسنتر:

دیتاسنتر یا مراکز داده، مجموعه‌ای از تجهیزات سخت‌افزاری و نرم‌افزاری است با زیرساخت‌های امنیتی، اطلاعاتی که برای نگه‌داری و پشتیبانی از سرویس‌های تحت شبکه اینترنت، اینترانت، اکسترانت استفاده می‌شود، دیتاسنتر یا مرکز داده و یا اتاق سرور در حقیقت محل نگه داری داده های تحت وب است.

شرکت‌های ارائه‌دهنده خدمات تحت وب با اجاره قسمتی از مراکز داده یا همان دیتاسنتر، به صورت مستقیم یا غیر مستقیم، قسمتی از دیتا سنتر را با نام سرور تهیه می‌کنند و اقداماتی در جهت بهینه سازی سرور تهیه شده انجام می‌دهند و با اتصال سرور به اینترنت، امکان میزبانی وب سایت‌ها بر روی این فضا فراهم می‌شود. بنابراین دیتاسنتر محلی است که صدها و یا هزاران سرور را در رک ها rack ، کیج ها Cage و اتاق‌های مختلف جای می‌دهد.

ساختمان دیتاسنتر از بخش‌های مختلفی مانند اتاق کنترل، اتاق سرور، ژنراتورها، تاسیسات خنک سازی، انبار سخت افزار، اتاق UPS و Battery backup ، اتاق نگه‌داری از وسایل اطفای حریق، اتاق مدیریت شبکه تشکیل می‌شود، هرچند که با توجه به نیازها، طراحی و امکانات و زیرساخت برای هر مرکز داده کاملاً میتواند متفاوت باشد.



استانداردهای دیتاسنتر

دیتاسنتر بر اساس چندین نوع استاندارد تعبیه شده است که اینک به بررسی دونوع TIA942و BICSI می‌پردازیم: در سال ۲۰۱۰ استاندارد bisci2010 منتشر شد و در سال ۲۰۱۱ نسخه نهایی اصلاح شده آن منتشر شد. استاندارد TIA942زمانی تنها مرجع استاندارد ساخت مرکز داده بود که به خودی خود تنها بخش‌های Telecommunicationمرکز داده را پوشش می‌داد و اشاراتی نیز به سایر استانداردها داشت.

استاندارد TIA942را زمانیکه مطالعه کردیم، تعداد زیادی علامت سوال در ذهن‌ها بوجود می‌آمد که برای رفع آنها نیاز بود به مراجع و مآخذ اعلام شده در استاندارد مراجعه نموده و پاسخ سوالات خود را دریابیم.

استاندارد BICSI محدوده وسیع‌تری را در حوزه دیتاسنتر پوشش می‌دهد. مثلاً در استانداردTIA942 اشاره مختصری به بحث سرمایش شده است، اما در BICSI صفحات زیادی به توضیحات این مقوله اختصاص یافته است.

استانداردBICSIبرای ساخت یک دیتاسنتر تمام عیار منتشر شده است.در این استاندارد به جزئیات زیادی توجه شده. مثلاً به آب ورودی ساختمان،قطر لوله وحتی محل جمع‌آوری زباله‌ها نیز توجه شده است.در ابتدا محدوده (Scope)تعریف و واحدهای مورد استفاده توضیح داده شده وسپس به عنوان اولین مبحثPlanning Spaceمطرح می‌گردد.

قبل از ایجاد دیتاسنتر باید موارد زیر را در نقشه آن به طور کامل در نظر بگیریم:

- ✓ **تهیه نقشه مهندسی ساختمان**
- ✓ **مسیرگذاری کف وسقف جهت کابل کشی برق و شبکه**
- ✓ **فاصله قرارگیری رک‌ها از هم**

موقعیت:

مکانی باید انتخاب شود که بتوان از کنترل‌های فیزیکی و محیطی مطمئن شد. مکان باید در برابر آتش، سیل و سایر خطرات مشابه، ایمن باشد. اتاق سرور استاندارد درجایی قرار دارد که سر وصدا در کار دفاتر و اتاق‌ها خلل ایجاد نکند.

امنیت محیط:

تمام اتاق های سرور باید دیوارهای محکم از سقف تا کف داشته باشند. در بخش‌هایی که کف کاذب یا سقف کاذب وجود دارد، دیوار باید تا زیر کف کاذب و بالای سقف کاذب کشیده شود تا مانع از ورود اشخاص شود. رک‌های دارای قفل یا قفسه هم برای امنیت استفاده می‌شود .

دسترسی فیزیکی:

دسترسی فیزیکی به اتاق سرور استاندارد باید تنها محدود به چند نفر شود که اجازه دسترسی را به طور قانونی دارند. استفاده از کارت‌خوان یا قفل الکترونیک برای اجازه دسترسی نسبت به کلیدهای مرسوم، پیشنهاد می‌شود؛ اگر از کلید استفاده می‌شود، باید عبارت "عدم کپی‌برداری"، روی آن حک شود. لیست افراد مجاز برای ورود باید حداقل هر فصل توسط صاحبان دیتاسنتر بررسی شود. باید کلیدها یا کارت های دسترسی گم شده یا دزدیده شده مشخص شوند. استفاده از دوربین‌های مدار بسته برای کنترل و ثبت ورود و خروج و کار در این فضا پیشنهاد می‌شود. ثبت زمان ورود، زمان خروج، هدف از دسترسی فیزیکی توسط بازدیدکنندگان یا پرسنل مجاز باید مشخص شود. بازدیدکنندگان باید کارت شناسایی داشته باشند. بازدیدکنندگان توسط پرسنل مجاز در تمامی زمان‌ها باید اسکورت شوند.

ملاحظات و بررسی‌های ساختاری:

اتاق سرور استاندارد باید در جایی مستقر باشد که بتواند وزن تمام سیستم‌ها از جمله سیستم هایی که قرار است در آینده نصب شود را تحمل کند. اندازه چارچوب در باید مناسب بردن و آوردن تجهیزات باشد. برای ساختار جدید، درها باید ۴۲ اینچ عرض و ۹ فوت ارتفاع داشته باشند. اگر لولا خارج از اتاق است، درها باید از پین های قفل لولا استفاده کنند.

سقف اتاق باید حداقل ۹ فوت ارتفاع داشته باشد.

اتاق سرور استاندارد نباید پنجره رو به بیرون داشته باشد.

ترتیب چیدمان تجهیزات باید به گونه ای باشد که فضای مناسب در اطراف رک‌ها داشته باشد.

٤ فوت از جلو و ۳ فوت از عقب پیشنهاد می‌شود.

برق اتاق سرور باید مدارهای مناسب برای تمام تجهیزات به همراه یک یا چند مدار اضافی در صورت آسیب رسیدن به مدار اصلی را داشته باشد. سیستم‌های مهم و اصلی باید به UPS و یا برق ژنراتور بسته به الزامات کسب و کار متصل باشد. UPS و یا ژنراتور برق باید حداقل سالانه تست شود و بر اساس خصوصیات و ویژگی‌های تولیدکننده نگهداری شود.

اتاق های بزرگ باید سوئیچ خاموش اضطراری داشته باشند. باید رویه‌های مربوطه در اتاق نصب شود و توضیح دهید که در هنگام قطعی برق چکار باید انجام داد. باید سیستم نورپردازی اضطراری هم داشته باشند.

کنترل درجه حرارت:

اتاق سرور استاندارد باید کنترل درجه حرارت مناسب برای حفظ دمای اتاق بر اساس محدودیت تعریف شده برای سخت افزارهای موجود در اتاق را داشته باشد. باید تهویه هوای مناسب برای حفظ درجه حرارت بین ٦٥ – ۷۰ درجه فارنهایت داشته باشد. کنترل‌های محیطی باید مجهز به سیستم‌های هشداردهنده در هنگام بروز مشکل باشند. برای اتاق‌های بزرگ، سیستم‌ها و تجهیزات خنک‌کننده باید برای حداکثرسازی کارآیی نصب شود.

اتاق سرور، قلب هر کسب و کار است. بدون مدیریت پیوسته و کارآمد داده، ذخیره و انتشار، بیشتر کسب و کارها نمی‌توانند به درستی کار کنند و اگر برای سیستم مشکلی ایجاد شود، نمی‌توان کار کرد. اهداف اساسی در خصوص طراحی اتاق سرور باید کارآیی و ثبات همراه با تجهیزات در سطوح بهینه باشد. در این مقاله به پنج نکته که در هنگام طراحی اتاق سرور باید به آنها توجه شود اشاره می‌کنیم:

فضای باز، تمیز و با تهویه مناسب:

اتاق سرور استاندارد باید تمیز، بدون گرد و غبار باشد و تهویه مناسب داشته باشد. سرورها و سایر کامپیوترها به طور طبیعی گرما ایجاد می‌کنند و تهویه نامناسب می‌تواند منجر به گرمای بیش از حد و خرابی شود. در طراحی اتاق سرور مطمئن شوید که فضای کافی بین واحدها برای نظافت منظم و دسترسی راحت برای تعمیر و نگهداری با حداقل فضاهای غیرقابل دسترسی که گرد و غبار روی هم انباشته می‌شود، وجود دارد.

کنترل های محیطی و لوازم خنک کننده مناسب:

هر چه تهویه و خنک‌سازی بیشتری برای سرورها فراهم شود، کمتر احتمال دارد بیش از حد گرم شوند. مطمئن شوید که کنترل‌های محیطی و تخلیه موثر را برای طراحی اتاق سرور در نظر گرفته‌اید. لوازم جانبی بسیاری در بازار وجود دارند تا به تسهیل خنک‌سازی کمک کنند، از جمله کف کاذب، کابینت های خود خنک کننده و IRC.

تامین برق اضطراری:

مهم است که سیستم الکتریکی اتاق سرور برای ادامه کار در حین اختلال در برق، طراحی شود. همچنین مهم است مطمئن شد که برق برای واحدهای شما، به درستی توزیع شده است. ژنراتورهای بک‌آپ و باتری‌ها به سالم ماندن تامین برق ادامه می‌دهند و واحدهای توزیع برق می‌توانند مقدار درستی از برق را در تمام زمان‌ها به مکان مناسب منتقل کنند.

جلوگیری از بهم ریختگی سیم‌ها:

بخش کلیدی دیگر طراحی اتاق سرور، مسیریابی موثر و مناسب کابل و سیم‌ها است. در هم و برهمی سیم‌ها، حوادثی هستند که آماده هستند هر زمانی رخ دهند. مطمئن شوید که مسیر مناسبی مشخص کرده‌اید تا سیم‌ها و اتصالات بتوانند بدون خطر قطعی، کشیدن و کندن منتقل شوند و مطمئن شوید که نقشه اتصالات را ترسیم کرده‌اید تا متخصصین فناوری اطلاعات بدانند که در چه جایی مشکلات را شناسایی کرده و به آنها دسترسی پیدا کنند.

فراهم سازی محیط کار با کیفیت:

در هنگام طراحی اتاق سرور استاندارد، فراموش نکنید که به فکر کارکنان فناوری اطلاعات باشید. مطمئن شوید که یک فضای کار با طراحی خوب، روشن و مطابق با ارگونومی فراهم می‌کنید تا کارکنان فناوری اطلاعات بتوانند به راحتی و به طور موثر بر آن نظارت داشته باشند.

مشخصات محیطی:

- اتاق نباید پنجره داشته باشد.
- فضا به اندازه کافی برای رشد و توسعه آتی، بزرگ باشد.
- سقف باید حداقل نه فوت ارتفاع داشته باشد.

مشخصات تجهیزات:

- رک های کامپیوتر باید حداقل ٤٢ اینچ فاصله داشته باشند.
- تمام رک ها باید مجهز به امکانات لرزه ای مناسب باشند.
- تجهیزات محاسباتی باید حداکثر شدن الکتریکی ۳۰۰ وات در هر مربع فوت را داشته باشند.
- در اتاق سرور باید بر آتش، دود، آب و رطوبت نظارت داشت.

مشخصات خنک سازی:

- از تجهیزات خنک سازی با فن های متغیر سرعت استفاده شود.
- سیستم های خنک سازی از کف با حداقل ارتفاع ٢٤ اینچ با توانایی تحمل بار رک های سرور و تجهیزات نیاز است.

مشخصات سیستم های الکتریکی:

- تجهیزات کامپیوتری و HVAC باید پانل های برق جداگانه داشته باشند.
- نباید هیچ تجهیزات پشتیبانی که گرما تولید می کند، وجود داشته باشد.
- برق جداگانه باید برای دیتاسنتر موجود باشد.

تجهیزات اتاق سرور:

هک و افشای داده‌ها، کسب و کارها را مجبور کرده تا درباره حریم خصوصی داده یا محرمانگی دوباره فکر کنند که چگونه می‌توانند داده‌ها را از دست هکرها حفظ کنند. با ایجاد بخش فناوری اطلاعات در شرکت به جای استفاده از خدمات آنلاین، می‌توان بسیاری از مسائل امنیتی مربوط به داده را حفظ کرد، این امر مستلزم استفاده از تجهیزات اتاق سرور استاندارد است. با تمرکز بر خدمات آنلاین، این کار می‌تواند برای کسب و کارهای کوچک، ترسناک باشد. علاوه بر این، منابعی که برای کمک طراحی شده‌اند می‌خواهند از تاسیسات در اندازه متوسط استفاده کنند که ممکن است ضرورتاً برای اتاق سرور کوچک، به اندازه کافی خوب نباشد.

با درک برخی اصول، ایجاد اتاق سرور دیگر یک فرآیند محرمانه نخواهد بود. در اینجا به برخی نکات اشاره شده است:

تجهیزات رک ، اهمیت دارند

برای کسب و کارهای کوچک چندان رایج نیست تا عملیات خود را با استفاده از سخت افزار سرور و دستگاه‌های شبکه روی قفسه یا میز انجام دهند. اگرچه چنین کاری، ارزان است، اما مقداری زیادی از تجهیزات با رشد شرکت، توسعه می‌یابند. تجهیزات همچنین کاملاً برای بررسی فیزیکی، باز هستند و گرد و غبار، ریختن مایعات یا حتی برخورد با سیم‌ها برای تجهیزات بسیار خطرناک است.

رک سرور، برای تمام فصول است

قبل از خرید رک سرور، خوب است که در ابتدا خصوصیات اصلی را درک کنید. رک‌های سرور با واحدهای رک سنجیده می شوند. یک واحد رک معادل ۱،۷۵ اینچ (٤٤،٤٥ میلی متر) ارتفاع دارد. سوئیچ‌های شبکه در کل ۱ تا ۲ واحد هستند. سرورها می‌توانند بین ۱ تا ٤ واحد داشته باشند.

سرورها را برای کاهش صدا، ایزوله کنید

سازمان‌ها بدون اتاق‌های اختصاصی برای تجهیزات سرور می‌خواهند صدا را کنترل کنند. یک اتاق کوچک با پارتیشن هم ارزش هزینه دارد. گذشته از کاهش یا حتی حذف صدای تجهیزات، اتاقی برای تجهیزات فناوری اطلاعات می‌تواند به جلوگیری از سرقت یا دستکاری تجهیزات کمک کند.

مدیریت سیم ها، ضروری است

تنظیم و راه‌اندازی رک سرور، چیزی بیشتر از بستن چند تا پیچ و مهره است. در مدیریت مناسب کابل ها نمی توان اغراق کرد چون هر بخش از تجهیزات در رک با کابل های اترنت بهم متصل شده اند. در کنار سیم کشی بین کابینت‌ها، رساندن کابل به نقاط LAN برای کامپیوترها، دوربین های مدار بسته و سایر تجهیزات شبکه در رک، اهمیت دارد. علاوه بر نصب پانل، همیشه یک بند کابل داشته باشید تا کابل‌ها را بهم ببندید. بند استاندارد کابل، ارزان هستند.

تمامی تجهیزات باید دارای برچسب باشند

یک پرینتر لیبل خریداری کنید. تمامی سرورها و تجهیزات شبکه باید با نام های توصیفی منحصر به فرد و آدرس های آی پی شان برچسب گذاری شوند. همچنین برای سایر تجهیزات اتاق سرور مثل کیبورد، سوئیچ ویدئو و ماوس، تجهیزات NAS، روترها، دستگاه های بک آپ داده و تجهیزات اتاق سرور دیگر هم باید برچسب داشته باشند.

توضیحات مشروح که رویه های مهم مرتبط با تجهیزات را توصیف می کند باید تایپ و به کابینت سرور با چسب یا آهنربا متصل شود. این نوشته ها باید به دستور العمل های عملیاتی مهم مرتبط با شبکه، بک آپ داده یا خاموش کردن تجهیزات در هنگام بروز قطعی برق اشاره کند.

اگر برنامه دارید تا از یک جفت سوئیچ شبکه و سیستم ذخیره ((NASاستفاده کنید، باید درجه حرارت را با تجهیزات مرتبط کاهش دهید، چرا که با افزایش درجه حرارت تجهیزات اتاق سرور، طول عمر آنها کم شده و باعث بروز قطعی یا خسارت می شود.

یکی دیگر از تجهیزات اتاق سرور ، سیستم تهویه هوا می باشد که کسب و کارها باید حداقل دو دستگاه در اتاق سرور با مدارهای جداگانه نصب کنند.

سینی کابل و لدر برای کابل کشی

سینی‌های کابل باید به نحوی اجرا شود که جلو مسیر هوا را در زیر کف کاذب سد نکند. سینی های زیر کف کاذب ممکن است به صورت چند طبقه طراحی شوند تا فضای کمتری را اشغال نموده و ظرفیت بیشتری را عرضه نماید . سینی های فلزی باید به سیستم ارت مرکز داده متصل شود.

سینی کابل حداکثر با عمق ۱۵ سانتی متر مجاز است. مسیر سینی کابل های زیر کف کاذب در هنگام طراحی باید با سایر تاسیسات نصب شده زیر کف کاذب هماهنگی لازم را داشته باشد . کابل ها درون سینی باید فیکس شود و لیبل شماره کابل مطابق استاندارد نصب شود.

سینی ها باید در قالب چند استاندارد مهم پیاده سازی شوند ، از جمله:

–نارسانایی در برابر بارها

–تحمل وزن بالا

–غیر قابل اشتعال

–مقاومت در برابر ضربه

– دارای عمر مطلوب و بالا

–ایده آل برای انواع آب و هوا ها

– و سینی ولدرهای کابل با ورق استیل مقاوم در برابر مواد شیمیایی باشد.

کنترل تردد و دوربین های امنیتی:

برای کنترل دسترسی ورودی و خروجی افراد مجاز و بر روی مبادی ورودی وبرخی از مبادی خروجی سایت مرکز داده سیستم های کنترل دسترسی نصب خواهد شد ، برای مبادی خروجی از کارت های مغناطیسی با بیومتریک استفاده یا از Push Button استفاده می شود.

همچنین دوربین های امنیتی نیز پوشش نسبتا کاملی با توجه به نیاز کارفرما در فضای مرکز خواهد داشت. صفحه نمایشی که برای نظارت تصاویر دوربین های مداربسته استفاده می شوند معمولا مانیتورهای حادثه یا نقطه‌ای نامیده شده و اجازه می‌دهند که اطلاعات تصاویر بدون خطا و در لحظه دیده بانی شوند و مانیتورهای حادثه مستقیماً باید روبروی اپراتور و در فاصله‌ی تقریبی0.5 تا 1.5متری و با اندازه قطر 9-16 اینچی (40–22cm) از وی نصب شوند.

درب اتاق سرور:

امنیت اتاق سرور بسیار حائز اهمیت است. از این رو باید اکثر الزامات ضروری در این اتاق رعایت شود تا از آسیب‌ها و خسارات احتمالی جلوگیری شود. گزینه‌های مختلفی برای سیستم‌های امنیتی درب اتاق سرور وجود دارد. سه سیستم وجود دارد: قفل های صفحه کلید دار، قفل‌های کارتی و قفل های بیومتریک.

قفل های صفحه کلید دار، یک صفحه کلید عددی در نزدیکی دستگیره درب اتاق سرور دارند که کاربر باید یک پین کد برای باز کردن در وارد کند. قفل های کارتی که در بیشتر هتل ها استفاده می شود به یک کارت با نوار مغناطیسی برای باز کردن درب نیاز است مثل کارت های اعتباری. سیستم های بیومتریک معمولا سیستم خواندن اثر انگشت برای قفل دارند که کاربر انگشت خود را برای اجازه دسترسی روی آن قرار می دهد.

اگرچه تمام این سیستم ها اساسا مکانیکی هستند اما به کنترل های متمرکز نیاز دارند که معمولا می توان از طریق شبکه کامپیوتری انجام داد. بزرگ ترین مزیت کارت خوان ها این است که نوار مغناطیسی را می توان تنها برای اجازه دسترسی کارکنان خاصی فعال کرد. وقتی که آن کارکنان، شرکت را ترک کنند، کارت را می توان بدون دسترسی فیزیکی به قفل، غیر فعال کرد.

قفل های صفحه کلید دار هم به صورت مکانیک و هم به صورت الکترونیک هستند که هر قفل حدودا بین ۱۰۰ تا ۱۵۰ دلار بسته به برند و مارک آن قیمت دارد.

یک نکته: مطمئن شوید که صفحه کلیدهای مکانیکی، چندین گزینه تغییر راحت کد را داراست. این نوع قفل برای درب اتاق سرور اماکنی مناسب است که افراد کمی به آنجا تردد دارند مثل اتاق سرور مدارس.

قفل بدون کلید یا ورود با کد الکترونیک برای درب اتاق سرور امروزه بسیاری از اشکال قفل های بدون کلید و قفل های کد دار الکترونیک در ساختمان ها به چشم می خورد. برخی از آنها سیستم های پیچیده ترین دارند که گران تر هم هستند. این سیستم ها به یک کاربر نیاز دارند تا کد ورودی را برای دسترسی جهت ورود وارد کند. آسیب پذیری مشهود این سیستم ها این است که اگر کد هیچ وقت تغییر نکند، کل افراد در نهایت کد را می دانند. وقتی این اتفاق رخ دهد، انگار که اصلا هیچ دربی وجود ندارد. تعیین یک فرد برای قفل‌ها یا امنیت خارجی به شما کمک می‌کنند تا اگر شما هم یکی از افرادی هستید که به اتاق سرور وارد می‌شوید، کد دسترسی خود را به صورت بازه‌ای از طریق سیستم‌های قفل بدون کلید تغییر دهید. با وجود چنین سیستم‌هایی، می‌توانید کدهای مختلف برای کارکنان مختلف تعیین کنید. بدین ترتیب، اگر کسی شرکت را ترک کند می‌توانید کد دسترسی او را غیرفعال کنید.

کارت های کنترل دسترسی قدرتمند ترین شیوه برای نظارت بر دسترسی به نقاط مهم و حساس، سیستم های کارتی کنترل دسترسی روی درب اتاق سرور است. سیستم هایی با ویژگی های کامل هستند که با ساختار ساختمان یکپارچه شده اند و حقوقی که برای یک شخص جهت ورود به اتاق سرور مشخص شده را رد یا تایید می کند (که به کدام شخص تخصیص یافته است). چنین سیستم هایی می توانند هر چیزی را از HVAC، آسانسورها و درب‌ها گرفته تا حتی سیستم های نور پردازی، پیکربندی کند. سیستم های کارتی کنترل دسترسی، بهترین مزیت را به شرکت‌های بزرگ ارائه می‌کنند. شرایط را در موقعیت‌های خاص، تغییر کارکنان و غیره کنترل می کنند. برخی حتی رابط‌های نرم افزاری دارند که از طریق آنها می توان کنترل کرد. سیستم‌های کارتی کنترل دسترسی، انعطاف پذیری بسیاری دارند. برخی از آنها با انواع جدیدتری از این تکنولوژی‌ها، دستگاه‌های رابط انسان دارند تا در ارتباط با سیستم‌های کارتی کار کنند.

سیستم مانیتورینگ اتاق سرور:

در عصر حاضر اتاق سرور درهر سازمان قلب تپنده آن می‌باشد و هرگونه اشکال درعملکردآن باعث ازکار افتادن سیستم‌ها و ایجاد خسارت فراوان به آن سازمان را در پی خواهد داشت، بطوریکه در بعضی مواقع این خسارات جبران‌ناپذیر می‌باشند. انتخاب تجهیزات مناسب اتاق سرور یکی از راهکارهای کنترل کار کرد صحیح و بهینه این قلب تپنده می‌باشند. اما یکی از مهمترین عوامل در عملکرد صحیح این تجهیزات وجود شرایط مناسب محیطی همچون دما رطوبت و ولتاژ مناسب است. نکته مهم دیگر، وضعیت امنیت و ایمنی اتاق سرور می‌باشد که در آن را در ماقبل دستبرد حریق و ... حفظ نماید. بسیاری از حوادثی که در اتاق سرور رخ می‌دهد قابل پیشگیری می‌باشند. نظارت و مانیتورینگ عوامل محیطی اتاق سرور نیز یکی از مهمترین وظایف مسئولین اتاق سرور است.

سیستم مانیتورینگ اطلاعات لازم جهت کنترل وضعیت محیط را دراختیار شما قرار می‌دهد و در مواقعی مانند نفوذ رطوبت گاز و دود قطع ولتاژ دمای بالا و ... هشدارهای لازم و از قبل تعیین شده را برای شما ارسال کند. این کار می‌تواند توسط ارسال اخطار به نرم افزار مرکزی، ارسال پیامک، ایمیل فعال کردن، زنگ هشدار و ...صورت پذیرد و یا اقدامی را در صورت رسیدن به آستانه بحران و خطر انجام دهد. به عنوان مثال در صورت افزایش بیش از دما سیستم تهویه را فعال نماید. در صورت نیاز می‌توان برای تامین سطح امنیت بیشتر سیستم کنترل تردد و دوربین مدار بسته را به خدمت گرفت.

اتاق‌های سرور از معدود مکان‌هایی هستند که حساسیت ویژه ای دارند، چرا که تمامی اطلاعات و ارتباطات یک مجموعه به اتاق سرور وابسته است. معمولاً سرورهای موجود در شرکت‌ها و سازمان‌ها می بایست به صورت شبانه‌روزی سرویس‌دهی گردد ، این امر مستلزم ایجاد شرایط محیطی مناسب و نظارت مداوم می‌باشد تا در صورت بروز هر گونه اشکال، بلافاصله اقدامات لازم در خصوص فعال نگاه داشتن صورت پذیرد. از این رو استفاده ازسیستم کنترل و نظارت بر اتاق سرور امری ضروری می‌باشد. شما می‌توانید با وجود این سیستم، تمام تجهیزات، دستگاه‌ها و سنسورهای موجود در اتاق را با استفاده از تلفن همراه یا پنل ، کنترل و تمامی آلارمها و خطاها را دریافت و نسبت به رفع آن بدون حضور در محل اقدام نمایید.

– فعال شدن آزیر صوتی در محل و ارسال آلارم هشدار بر روی تلفن همراه و پنل کاربری در صورت افزایش دما ، رطوبت و یا مشکل در سیستم سرمایش.

– کنترل تردد و جلوگیری از ورود غیر مجاز با استفاده از درب های مجهز به قفل دیجیتالی با قابلیت شناسایی اثر انگشت و...

– اعمال فرایند های ویژه بصورت اتوماتیک و هوشمند برای کنترل دما : مانند روشن کردن کولر رزرو و یا هواساز، برای جلوگیری از خسارات وارده .

– دریافت دستور مدیر اتاق سرور را در برای قطع برق ، آب و راه اندازی مجدد و یا غیره .

– ارسال دما و رطوبت فعلی اتاق سرور بر روی تلفن همراه و پنل کاربری با قابلیت زمان بندی.

– دریافت آلارم از سنسورهای آتش و دود ، نشت گاز ، ضربه و ورود غیر مجاز ، قطع برق ، نوسان برق و ...

– کنترل برق اتاق سرور و نحوه کارکرد یو پی اس و تجهیزات برق اضطراری ، توسط تلفن همراه و پنل کاربری در شرایط بحرانی .

– کنترل و مدیریت دمای سویچ ها ، رکها و دیگر تجهیزات با قابلیت دریافت خطاهای شبکه و... .

امکانات سیستم :

–قابلیت کارکرد دستگاه بصورت آفلاین بدون نیاز به کامپیوتر

–امکان اجرای فرامینی خاص توسط اس ام اس

-امکان کنترل درب های ورودی با استفاده از قفل های دیجیتالی با امکان دسترسی به قفل با اثر انگشت،اسکن چشم و کد٤ تا٨ رقم

-امکان کنترل عوامل محیطی مانند دما ، رطوبت ، دود و گاز

-امکان هشدار بصورت پیام کوتاه، تماس تلفنی، آژیر و ایمیل

-قابلیت فعال سازی سیستمهای مختلف توسط ارسال پیام کوتاه

-دارای چندین خروجی (رله) جهت کنترل ادوات جانبی

-امکان ثبت تصویر افراد وارد شده به اتاق سرور

-امکان تعریف و ارسال پیام کوتاه به چند نفر بطور همزمان

-امکان کنترل ارتباط و خاموش کردن چندین سرور توسط نرم افزار مرکزی در مواقع خاص

-مانیتور کردن ریست شدن سرور توسط نرم افزار و ارسال پیام کوتاه

–مانیتور کردن قطع و وصل شدن برق توسط نرم افزار و ارسال پیام کوتاه

-مانیتور کردن قطع و وصل شدن UPS توسط نرم افزار و ارسال پیام کوتاه

-قابلیت ارتباط با سیستم کنترل دسترسی و بازکردن در توسط پیام کوتاه

-قابلیت کنترل سرویس های ویندوز سرور اعم از DNS, DHCP و...

-امکان دریافت وضعیت اتاق سرور با استفاده از پیام کوتاه

-گزارش گیری های مختلف تحت وب و شبکه محلی

UPS اتاق سرور:

اتاق‌های سرور بخش مهمی از هر شرکت یا سازمان را تشکیل می‌دهد و از این رو بایستی در ساخت آن استانداردهای لازم موردتوجه قرار گیرد و مشکلی در نهایت به وجود نیاید. اتاق سرورها شامل فناوری‌های مختلفی می‌شوند که به شکل دستگاه در اختیار افراد نظارت کننده قرار می‌گیرد. یکی از دستگاه‌های اتاق سرور UPS است. این دستگاه که در اتاق‌های سرور به کار گرفته می‌شود موجب عملکرد نرمال سرورها حین قطع و وصل شدن جریان خواهد شد.

اتاق‌های سروری که بدون UPS باشند قطعاً با مشکل قطع و وصلی برق سرورها از کار افتاده یا دچار آسیب‌هایی می‌شوند که بایستی به وسیله UPS آن را برطرف ساخت. افزود یک دستگاه UPS بسته به حجم سرورها داشته باید برای هر تعداد سرور یک دستگاه UPS

تهیه کرد، زیرا اگر حجم سرورها بسیار بوده و دستگاه UPS کوچکی در نظر گرفت قطعا نمی‌تواند پاسخگو نیاز و برطرف کننده مشکل قطع و وصل شدن جریان برق باشد.

بسیاری از شرکت‌ها یا سازمان‌ها برای اتاق سرور خود یک UPS تهیه می‌کنند تا اتاق سرور آنها به عنوان اتاق سرور UPS شناخته شود. البته هزینه کمی نیز نداشته و یک گزینه بزرگ برای اتاق سرور است که با افزودن آن می‌توان ایمنی و استاندارد لازم را به اتاق سرور افزود. بنابراین می‌توان به کمک چنین دستگاهی شدت جریان برق را در سرورها به شکل نرمالی برقرار کرده و خطر قطعی را از دستگاه ها دور داشت.

در حقیقت اتاق سرور UPS به اتاقی گفته می‌شود که شامل دستگاه UPS برقرارکننده شدت جریان برق نرمال در حین قطعی کامل یا تغییر نوسان می‌شود. بنابراین وجود دستگاه UPS در کنار اتاق سرور ضروری بوده و موجب جلوگیری از بروز هرخطری ناشی از قطعی برق می‌شود.

برق امر حیاتی برای یک اتاق سرور محسوب می‌شود که نبود آن حتی موجب حذف حافظه بخشی از داده ها می شود که در نهایت ضررهایی را برای شرکت یا سازمان موردنظر به دنبال دارد. بنابراین نباید در هنگام ایجاد اتاق سرور از استفاده دستگاه UPS صرف نظر کرد.

این دستگاه ها البته هزینه بسیاری نداشته اما ایمنی یک اتاق سرور را بالا می برند. بنابراین اکثر شرکت ها یا سازمان ها با به کارگیری اتاق سرور در کنار سرورها دستگاه UPS را خریداری کرده و به کار می گیرند. به نوعی این دستگاه را یک منبع تغذیه بی وقفه می‌دانند. این دستگاه مخفف Uninterruptible power supply که همان منبع تغذیه بی وقفه محسوب شده و مدت ها می تواند در کنار اتاق سرور به کار گرفته می شود. بنابراین این نوع دستگاه وجودی ضروری در اتاق سرور داشته باید آن را یکی از استانداردهای اتاق سرور به شمار می رود.

شرکت‌ها و سازمان بزرگ بیشتر به استفاده از دستگاه Uninterruptible power supply می‌پردازند تا ایمنی بیشتری را فراهم آورده و از آسیب رسیدن به دستگاه جلوگیری کنند.

به هر حال اگر به دنبال ایجاد اتاق سرور هستید قطعا این دستگاه را در کنار اتاق به کارگیرید تا اتاق سرور UPS ایجاد نمایید.

دمای اتاق سرور:

اتاق سرور، اتاقی است که هوای مطبوع دارد و به عملیات مداوم سرورهای کامپیوتری تخصیص یافته است. کل ساختمان یا ایستگاهی که به این کار اختصاص یافته، دیتاسنتر نام دارد. دمای اتاق سرور ، یکی از فاکتورهایی است که بر مصرف انرژی و اثر محیطی اتاق سرور تاثیر می گذارد. در نواحی که هوا خنک است و برق قابل تجدید بسیاری دارند، اثرات زیست محیطی معتدل تر است. از این رو کشورهایی با شرایط مطلوب مثل کانادا، فنلاند، سوئد و سوئیس سعی دارند شرکت های بیشتری را برای استقرار اتاق های سرور خود در این کشورها جذب کنند.

در سرتاسر دنیا، شرکت ها برای ذخیره و پشتیبانی از داده های حساس بی شمار به اتاق های سرور متکی هستند. به منظور برآورده سازی تقاضای مشتری، سرورها باید پیوسته آنلاین حفظ شوند. این تجهیزات، گرمای زیادی را ایجاد می کنند که اگر بررسی نشود، می توانند اثر معکوسی بر عملکرد آن داشته باشد. بنابراین اوپراتورهای اتاق های سرور باید دمای بهینه را حفظ کنند تا مطمئن شوند که این سیستم ها کار خود را به درستی انجام می دهند.

وقتی یک اتاق سرور، خیلی گرم باشد، تجهیزات خیلی راحت بیش از حد گرم می شوند و منجر به از بین رفتن داده های ذخیره شده می شود. این مشکل برای یک سازمان، فاجعه به حساب می آید که به این اطلاعات برای انجام کسب و کار خود متکی است. بنابراین در اتاق های سرور از سیستم های خنک سازی برای خنک کردن اتاق سرور و جلوگیری از گرمای بیش از حد تجهیزات استفاده می شود.

تجهیزات شبکه و کامپیوتر برای عملیات در یک دامنه دمایی نسبتا محدود طراحی شده است. برای اطمینان از عملیات قابل اعتماد و طولانی تر شدن عمر قطعات ، شما باید مطمئن شوید که دما در آن دامنه باقی می ماند. حتی چند درجه گرما می تواند یک تراشه سرور را از بین ببرد.

هزینه خرابی سرور می تواند قابل توجه باشد. فکر کنید به خاطر این خرابی چقدر ضرر می کنید؟ هزینه جایگزینی هم وجود دارد. تجارت الکترونیک را از دست می دهید، جزییات اطلاعات مشتریان را از دست می دهید، زمان کارکنان هدر می رود و متحمل خیلی هزینه های مرتبط دیگر می شوید.

توصیه های عمومی مطرح می کنند که دما نباید پایین تر از ۱۰ درجه سانتی گراد (۵۰ درجه فارنهایت) یا بالای ۲۸ درجه سانتی گراد (۸۲ درجه فارنهایت) باشد اما بهتر است که دما را بین ۲۰ – ۲۱ درجه سانتی گراد (۷۱–۶۸ درجه فارنهایت) نگه داشت.

چگونه بر دمای اتاق سرور نظارت داشته باشیم؟

شما باید دمای اتاق سرور استاندارد را همیشه کنترل کنید و بر آن نظارت داشته باشید، به ویژه در شب و آخر هفته ها که هیچ کس در آنجا نیست. سیستم هایی برای این کار موجود است. باید دما را در نقاط مختلف اتاق بسنجید تا ببینید که کجا گرم است. سنجش دما باید خودکار و قابل اعتماد باشد. سیستم ها باید از هشدار به صورت های مختلف مثل ایمیل یا اس ام اس پشتیبانی کنند.

در تعیین بهترین دمای اتاق سرور، چندین فاکتور از جمله اندازه اتاق و تعداد سرورها باید در نظر گرفته شود. این اطلاعات می تواند به اوپراتورها در تصمیم گیری پیرامون بهترین دما کمک کند. وقتی که بهترین دما شناسایی شد، اوپراتورهای اتاق سرور باید بر سیستم های کنترل دما نظارت داشته باشند تا مصرف انرژی و خنک سازی حفظ شود.

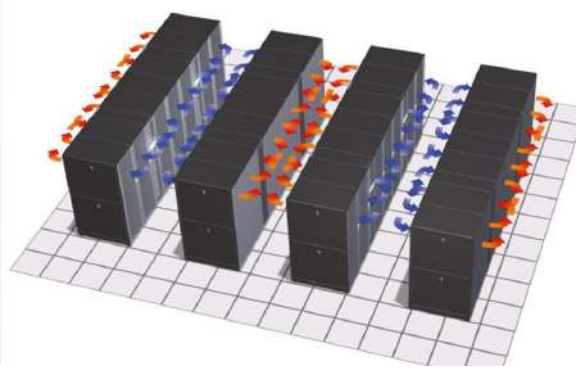
سیستم تهویه:

انتخاب سیستم خنک کننده بر اساس نوع و سطح درجه بندی مرکز داده انجام می گیرد. باید از تکنولوژی استفاده شود که قادر به کاهش بار تهویه هوا در اتاق سرور استاندارد باشد زیرا قبل از آنکه گرما در فضای اتاق سرور پخش شود جمع آوری و به خارج از اتاق سرور منتقل شود.

راه های توزیع هوای سرد به سه دسته براساس تجهیزات تقسیم بندی می شود:

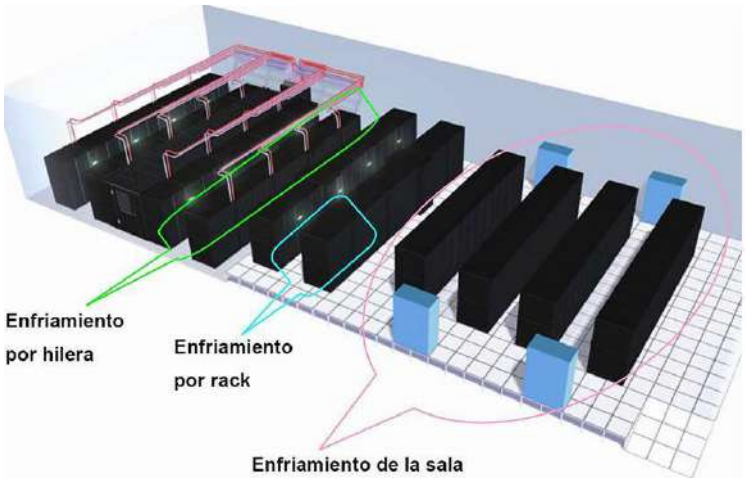
Row oriented:

سیستم توزیع سرمایش در میان رک ها بالا و پایین کف کاذب یا در بین ردیف ها استفاده میشود ، رک های ظرفیت بالاتر در یک ردیف و رک های با ظرفیت پایین ر یک ردیف دیگر نگهداری می شود.



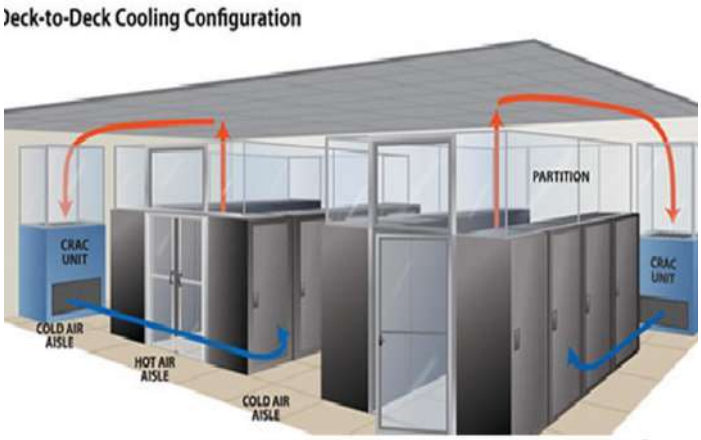
Room Oriented:

سیستم سرمایشی که برای کل فضای دیتا سنتر در نظر گرفته می شود و به ساختار اتاق و ارتفاع سقف وابسته است. مکانیزم آن به این شکل است که هوای گرم و سرد را با یکدیگر ترکیب می کند تا به دمای مناسب دیتا سنتر برسد.

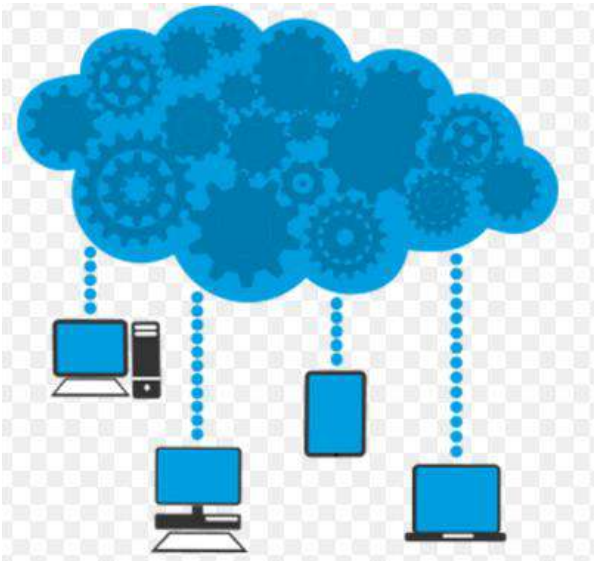


Rack Oriented:

سیستم سرمایش در داخل رک قرار می گیرد و وظیفه تنظیم دمای هر رک را به عهده دارد تا دمای رک را همواره در دمای تنظیم شده نگه دارد و به طور کلی فارغ از وابستگی به تغییرات دمای اتاق می باشد.



اتوماسیون اتاق سرور:



اتاق سرور یکی از مکان های مهم شرکت ها و سازمان ها محسوب می شود که بایستی تجهیزات نگهداری مختلفی برای کنترل آن در نظر گرفت. از این رو کمپانی های سعی می کنند با استفاده از اتوماسیون اتاق سرور در این زمینه نگهداری کاملی از چنین مکانی داشته باشند. بنابراین بوسیله اتوماسیون اتاق سرور می توان کنترل بی نقصی داشت و در طول زمان تنها با سرویس دهی اتوماسیون برای همیشه شاهد نگهداری حرفه ای اتاق سرور بود.

اتوماسیون اتاق سرور جهت کنترل و نظارت روی عملکرد سرورها به کار گرفته می شود تا بتوان در صورت به وجود آمدن مشکلی در سرورها سریعا به آن رسیدگی کرد و مانع از گسترش مشکل آنها شد. موضوعی که بسیاری از شرکت ها به آن توجه داشته مانع از فراگیر شدن مشکل می شوند. از طریق اتوماسیون اتاق سرور یا همان سیستم کنترل و نظارت، می توان از هر گونه تغییر شرایط در اتاق سرور با خبر شد. در این میان باید به تغییر شرایط دمایی، رطوبتی، وجود دود و گاز در اتاق اشاره داشت. بوسیله چنین اتوماسیونی می توان عملکرد سریع در حل مشکل داشت.

سیستم کنترل و نظارت یا همان اتوماسیون اتاق سرور استاندارد یکی از تجهیزات اصلی نگهداری اتاق های سروری شرکت ها و سازمان ها به شمار می روند، بنابراین بدون وجود آن خطر بزرگی این مکان ها را تهدید می کند و خسارت های بزرگی را نیز برای این کمپانی

های به دنبال خواهد داشت. از این رو بایستی به طور حتم اتوماسیون ها در اتاق های سرور به کار گرفته شوند تا نظارت همیشگی روی سرورها داشت و مانع از به وجود آمدن مشکلات شد.

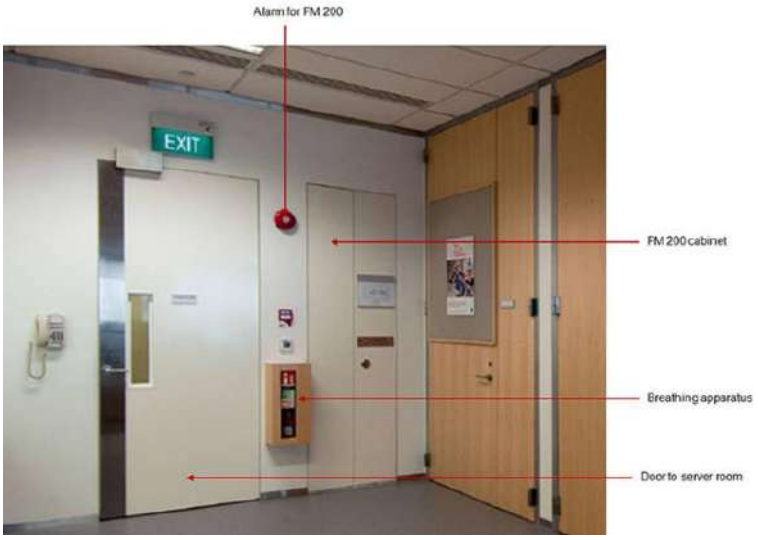
برخی از کمپانی هایی که فاقد چنین اتوماسیونی هستند نظارت ناقصی روی سرورها داشته و از این رو باید هزینه های بسیاری جهت حل مشکل متحمل شوند. هنگامی که مشکلی به وجود می آید سیستم نظارت یا همان اتوماسیون به شکل ارسال پیامک، برقراری تماس، ارسال ایمیل و برخی از این دست به افراد تعیین شده در سیستم ارسال می شود. از این رو افراد معین شده در صورت به وجود آمدن مشکلی در این رابطه اطلاعی کسب کرده و به حل سریع آن می پردازند.

یکی دیگر از ویژگی های بارز و قابل توجه این نوع سیستم خاموش و روشن نمودن سرور و روشن کردن تهویه با ارسال پیامک است که کمک شایانی جهت حل مشکل می کند.

بنابراین وجود اتوماسیون در اتاق سرور استاندارد می تواند موجب ایمنی کامل اتاق ها شده و نگهداری کاملی به دنبال خواهد داشت. اتاق های سرور همانطور که گفته شد مرکز اسناد و اطلاعات شرکت ها و سازمان ها به شمار می روند. از این رو بایستی نظارت کامل و حرفه ای روی آنها صورت گیرد و در غیر این صورت شاهد آشکار شدن مشکلات متعددی خواهیم بود که اگر در اسرع وقت حل نشود، مشکلات بزرگ دیگری را به دنبال خواهد داشت.

به هر حال وجود اتوماسیون در یک اتاق سرور ضروری بوده و شرکت ها/سازمان ها/ادارات نیز باید توجه بسیاری به آن داشته باشند، در غیر این صورت پیامدهای خوبی به دنبال نخواهد بود

سیستم های اطفاء حریق مناسب جهت دیتاسنترها و اتاق های سرور:



در درجه اول گازهای تمیز همچون FM-200، Novec 1230، Inert Gas و سایر گازهای ذکر شده دراستاندارد NFPA 2001، پیشنهاد می شود. همچنین استفاده از سیستم های Oxygen Reduction و Watermist جهت استفاده در اتاق سرور با محدودیت هایی روبرو است که می بایست مورد بررسی بیشتری قرار گیرد. استفاده از سیستم آیروسل ((Aerosolدر اتاق سرور به عنوان گزینه اصلی توصیه نمی شود.

خصوصیات کلی یک سیستم اطفاء حریق مناسب از نوع **Total Flooding** در اتاق سرور استاندارد شامل موارد زیر است:

- قدرت اطفاء کنندگی در کلاس C و A حریق
- قابلیت نفوذ پذیری بالا
- نداشتن پسماند
- عایق الکتریسیته
- نداشتن خطر جانی برای افراد
- سرعت عملکرد و برگشتن سریع سیستم به حالت نرمال
- آسیب نرساندن به تجهیزات
- تناسب مالی با ارزش دیتا و سخت افزار مورد استفاده
- امکان جایگزینی سریع پس از عملکرد

مضرات اتاق سرور استاندارد:

اتاق سرور یکی از بخش های مهم هر سازمان و شرکت محسوب می شود که باید نگهداری کاملی از آنها صورت گیرد. در این میان اگرچه فوایدی از اتاق سرور می توان مشاهده کرد امامضرات اتاق سرور را نیز باید در نظر گرفت. سازمان ها و شرکت ها باید توجه کاملی به مضرات اتاق سرور داشته باشند زیرا ممکن است در نهایت خطرات و ضررهای بزرگی را برای طرف های مقابل به دنبال داشته باشند.

از جمله مضرات اتاق سرور باید به تهدیداتی اشاره کرد که همیشه اتاق های سرور را دنبال می کنند. این تهدیدات که باید آنها را مضرات اتاق سرور نیز محسوب کرد شامل عوامل متعددی می شوند که باید به افزایش درجه دما، رطوبت بالا هوا، جنبش ، قطعی برق و سرقت اشاره کرد.

البته هر یک از عوامل فوق توضیحاتی داشته که در ادامه می توانید بیشتر درباره آنها اطلاعات کسب کنید:

۱– جنبش

حرکات ناخواسته در اتاق سرور استاندارد آسیبی به هارد سرورها وارد می کند که در نتیجه داده ها موجود در آن را با مشکل ایجاد خواهد کرد. حرکت افراد، حرکت وسایل نقلیه و برخی از این قبیل موجب می شود تا حرکت های ناخواسته ای را به دنبال داشته که– فرجام بدی دارد. این حرکت های ناخواسته که به آن ارتعاش نیز گفته می شود، درایوهای سرور را دچار اختلال می کند که این اختلال ممکن است به حذف داده های درون سرور بیانجامد. بنابراین نباید به حرکت کردن در اتاق های سرور پرداخت و بایستی بیشتر کارها را به شکل آهسته انجام داد.

۲– قطعی برق

قطع برق یکی از بزرگترین عوامل تهدید کننده اتاق سرور است. زیرا هارد درایو سرورها بوسیله برق می توانند انرژی داشته و فعال باشند و قطعی مکرر می تواند آسیب بزرگی را به این درایوها وارد کند. آسیبی که همچون جنبش می تواند موجب پاک شدن داده های درون هارد سرور شود. از این رو بایستی سیستم هوشمندی را به کار گرفته تا از قطعی برق جلوگیری کرده تا آسیبی متوجه سرورها نشود.

۳– رطوب هوا

رطوبت یکی از تهدیدات مهم هر اتاق سرور است. رطوبت بالای هوا موجب می شود تا سخت افزارهایی چون پردازنده و درایوهای سرور دچار پوسیدگی شده که در نهایت نابودی آنها را به دنبال دارد. بنابراین بایستی مانع از به وجود آمدن رطوب در این اتاق ها شد زیرا ضرر بزرگی را به وجود خواهد آورد.

٤– افزایش دما

دما یکی از مهم های تهدید اتاق سرور استاندارد به شمار می رود. با افزایش درجه دما اتاق سرور، سخت افزار سرورها دچار اختلالی شده که ناشی از افزایش دما آنها بوده و بایستی با استفاده از سیستم خنک کننده این موضوع را حل کرد. با افزایش دما سرورها ممکن است در سخت افزار آن مشکلی ایجاد شده و داده ها پاک شوند.

۵– سرقت

برخی افراد برای ضربه زدن به شرکت یا سازمانی سعی می کنند با رجوع به بخش اتاق سرور آن که داده های مهمی را در بر می گیرد، به این اتاق آسیبی وارد کرده و اطلاعات را به سرقت ببرد. از این رو موجب شده تا داده های مهم نابود و سرور دچار اختلالی شود که سازمان یا شرکت موردنظر را با مشکل بزرگی رو به رو خواهد ساخت. بنابراین باید افراد و سیستم نظارتی برای این نوع اتاق ها به کار گرفته شود.

Vocabulary واژگان			
Implementing	پیاده سازی	Redistribution	توزیع مجدد
debug	اشکال زدایی	Significance	اهمیت
Overview	بررسی اجمالی	**Floating**	شناور
Aggregation	تجمع	Utilization	استفاده
Integrated	یکپارچه	recursive	بازگشتی
Autonomoous system	سیستم خودمختار		

Imprtant sites	
Check-host.net	

Cheat Sheets :

BGP · PART 1

packetlife.net

Attributes

	Name	Description
Well-known Mandatory · Must be supported and propagated		
1	**Origin**	Origin type (IGP, EGP, or unknown)
2	**AS Path**	List of autonomous systems which the advertisement has traversed
3	**Next Hop**	External peer in neighboring AS
Well-known Discretionary · Must be supported; propagation optional		
5	**Local Preference**	Metric for internal neighbors to reach external destinations (default 100)
6	**Atomic Aggregate**	Includes ASes which have been dropped due to route aggregation
Optional Transitive · Marked as partial if unsupported by neighbor		
7	**Aggregator**	ID and AS of summarizing router
8	**Community**	Route tag
Optional Nontransitive · Deleted if unsupported by neighbor		
4	**Multiple Exit Discriminator (MED)**	Metric for external neighbors to reach the local AS (default 0)
9	**Originator ID**	The originator of a reflected route
10	**Cluster List**	List of cluster IDs
13	**Cluster ID**	Originating cluster
--	**Weight**	Cisco proprietary, not communicated to peers (default 0)

About BGP

Type	Path Vector
eBGP AD	20
iBGP AD	200
Standard	RFC 4271
Protocols	IP
Transport	TCP/179
Authentication	MD5

Terminology

Autonomous System (AS)
A logical domain under the control of a single entity

External BGP (eBGP)
BGP adjacencies which span autonomous system boundaries

Internal BGP (iBGP)
BGP adjacencies formed within a single AS

Synchronization Requirement
A route must be known by an IGP before it may be advertised to BGP peers

Packet Types

Open	**Update**
Keepalive	**Notification**

Path Selection

	Attribute	Description	Preference
1	**Weight**	Administrative preference	Highest
2	**Local Preference**	Communicated between peers within an AS	Highest
3	**Self-originated**	Prefer paths originated locally	True
4	**AS Path**	Minimize AS hops	Shortest
5	**Origin**	Prefer IGP-learned routes over EGP, and EGP over unknown	IGP
6	**MED**	Used externally to enter an AS	Lowest
7	**External**	Prefer eBGP routes over iBGP	eBGP
8	**IGP Cost**	Consider IGP metric	Lowest
9	**eBGP Peering**	Favor more stable routes	Oldest
10	**Router ID**	Tie breaker	Lowest

Neighbor States

Idle · Neighbor is not responding
Active · Attempting to connect
Connect · TCP session established
Open Sent · Open message sent
Open Confirm · Response received
Established · Adjacency established

Troubleshooting

```
show ip bgp [summary]
show ip bgp neighbors
show ip route [bgp]
clear ip bgp * [soft]
debug ip bgp [...]
```

Influencing Path Selection

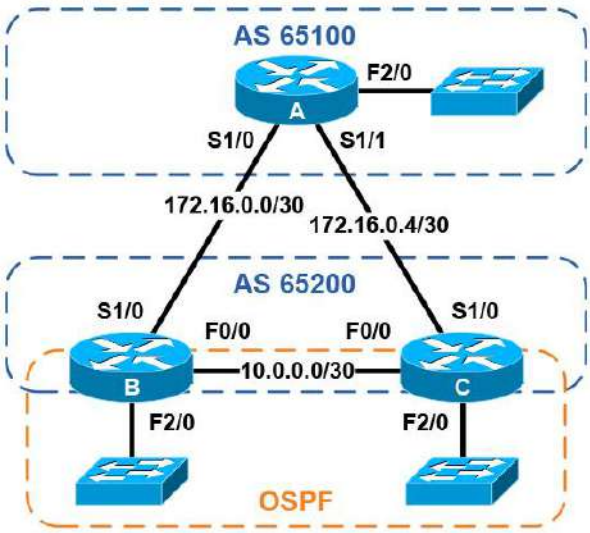
Weight	`neighbor 172.16.0.1 weight 200`	**Local Preference**	`bgp default local-preference 100`
MED	`default-metric 400`	**Route Map**	`neighbor 172.16.0.1 route-map Foo`
Ignore AS Path	`bgp bestpath as-path ignore`	**Ignore Cost Communities**	`bgp bestpath cost-community ignore`

by Jeremy Stretch v2.1-r1

BGP · PART 2

packetlife.net

Configuration Example



Router A

```
interface Serial1/0
 description Backbone to B
 ip address 172.16.0.1 255.255.255.252
!
interface Serial1/1
 description Backbone to C
 ip address 172.16.0.5 255.255.255.252
!
interface FastEthernet2/0
 description LAN
 ip address 192.168.1.1 255.255.255.0
!
router bgp 65100
 no synchronization
 network 172.16.0.0 mask 255.255.255.252
 network 172.16.0.4 mask 255.255.255.252
 network 192.168.1.0
 neighbor South peer-group
 neighbor South remote-as 65200
 neighbor 172.16.0.2 peer-group South
 neighbor 172.16.0.6 peer-group South
 no auto-summary
```

Router B

```
interface FastEthernet0/0
 description Backbone to C
 ip address 10.0.0.1 255.255.255.252
!
interface Serial1/0
 description Backbone to A
 ip address 172.16.0.2 255.255.255.252
!
interface FastEthernet2/0
 description LAN
 ip address 192.168.2.1 255.255.255.0
!
router ospf 100
 network 10.0.0.1 0.0.0.0 area 0
 network 192.168.2.1 0.0.0.0 area 1
!
router bgp 65200
 no synchronization
 redistribute ospf 100 route-map LAN_Subnets
 neighbor 10.0.0.2 remote-as 65200
 neighbor 172.16.0.1 remote-as 65100
 no auto-summary
!
access-list 10 permit 192.168.0.0 0.0.255.255
!
route-map LAN_Subnets permit 10
 match ip address 10
 set metric 100
```

Router C

```
interface FastEthernet0/0
 description Backbone to B
 ip address 10.0.0.2 255.255.255.252
!
interface Serial1/0
 description Backbone to A
 ip address 172.16.0.6 255.255.255.252
!
interface FastEthernet2/0
 description LAN
 ip address 192.168.3.1 255.255.255.0
!
router ospf 100
 network 10.0.0.2 0.0.0.0 area 0
 network 192.168.3.1 0.0.0.0 area 2
!
router bgp 65200
 no synchronization
 redistribute ospf 100 route-map LAN_Subnets
 neighbor 10.0.0.1 remote-as 65200
 neighbor 172.16.0.5 remote-as 65100
 no auto-summary
!
access-list 10 permit 192.168.0.0 0.0.255.255
!
route-map LAN_Subnets permit 10
 match ip address 10
 set metric 100
```

Router A Routing Table

```
     172.16.0.0/30 is subnetted, 2 subnets
C       172.16.0.4 is directly connected, S1/1
C       172.16.0.0 is directly connected, S1/0
C    192.168.1.0/24 is directly connected, F2/0
B    192.168.2.0/24 [20/100] via 172.16.0.2
B    192.168.3.0/24 [20/100] via 172.16.0.2
```

Router B Routing Table

```
     172.16.0.0/30 is subnetted, 2 subnets
B       172.16.0.4 [20/0] via 172.16.0.1
C       172.16.0.0 is directly connected, S1/0
     10.0.0.0/30 is subnetted, 1 subnets
C       10.0.0.0 is directly connected, F0/0
B    192.168.1.0/24 [20/0] via 172.16.0.1
C    192.168.2.0/24 is directly connected, F2/0
O IA 192.168.3.0/24 [110/2] via 10.0.0.2, F0/0
```

by Jeremy Stretch

v2.1-r1

Cisco IOS Versions

packetlife.net

IOS Nomenclature

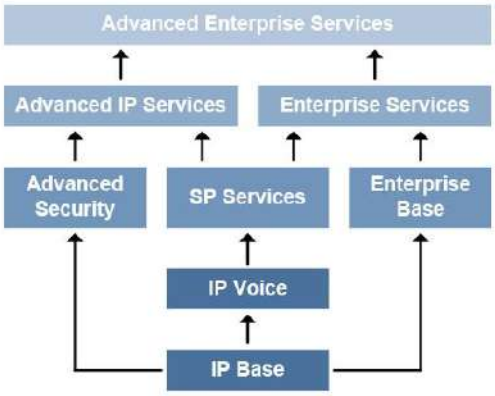
Mainline 12.4(7a)
- Maintenance Release
- Individual Release
- Numbered Version

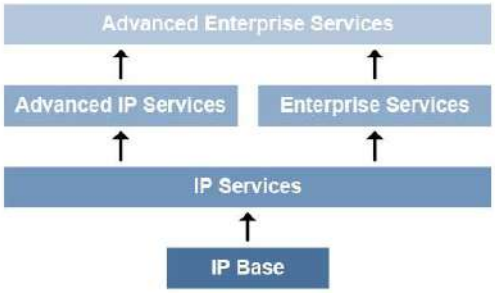
T Train 12.4(9)T1
- Maintenance Release
- Individual Release
- New Feature Identifier
- Numbered Version

S Train 12.2(25)SEB4
- Release
- Individual Release
- Numbered Version

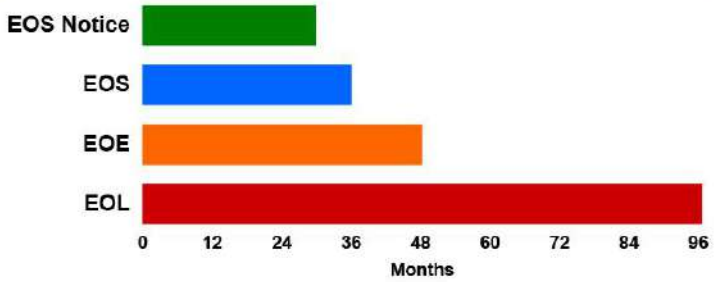
IOS XR 3.2.1
- Major Release
- Minor Release
- Maintenance Release

IOS Package Trees





Release Lifecycle



First Customer Shipment (FCS)
The release is made available to Cisco customers on CCO

EOS Notice
Notification of upcoming EOS

End of Sale (EOS)
The release is no longer orderable or included in manufactured shipments

End of Engineering (EOE)
The last day for software fixes; only TAC assistance is offered from this point

End of Life (EOL)
The last day for TAC support; release becomes obsolete; upgrade is only option for continued support

IOS Filename

c3725-entbase-mz.124-6.T.bin
- Hardware
- Feature Set
- Memory Location
- Compression Format
- Maintenance Release
- Individual Release
- T Designator

Deployment Classifications

Early Deployment (ED)
Offers new feature, platform, or interface support

General Deployment (GD)
A major release considered qualified for deployment on critical devices

Limited Deployment (LD)
A major release prior to reaching its GD milestone

Deferred (DF)
Known defective images; should not be installed

IOS Version Verification

```
show version
dir <filesystem>:
verify <filesystem>:<image>
```

by Jeremy Stretch v2.0

COMMON PORTS

packetlife.net

TCP/UDP Port Numbers

7	Echo	554	RTSP	2745	Bagle.H	6891-6901	Windows Live
19	Chargen	546-547	DHCPv6	2967	Symantec AV	6970	Quicktime
20-21	FTP	560	rmonitor	3050	Interbase DB	7212	GhostSurf
22	SSH/SCP	563	NNTP over SSL	3074	XBOX Live	7648-7649	CU-SeeMe
23	Telnet	587	SMTP	3124	HTTP Proxy	8000	Internet Radio
25	SMTP	591	FileMaker	3127	MyDoom	8080	HTTP Proxy
42	WINS Replication	593	Microsoft DCOM	3128	HTTP Proxy	8086-8087	Kaspersky AV
43	WHOIS	631	Internet Printing	3222	GLBP	8118	Privoxy
49	TACACS	636	LDAP over SSL	3260	iSCSI Target	8200	VMware Server
53	DNS	639	MSDP (PIM)	3306	MySQL	8500	Adobe ColdFusion
67-68	DHCP/BOOTP	646	LDP (MPLS)	3389	Terminal Server	8767	TeamSpeak
69	TFTP	691	MS Exchange	3689	iTunes	8866	Bagle.B
70	Gopher	860	iSCSI	3690	Subversion	9100	HP JetDirect
79	Finger	873	rsync	3724	World of Warcraft	9101-9103	Bacula
80	HTTP	902	VMware Server	3784-3785	Ventrilo	9119	MXit
88	Kerberos	989-990	FTP over SSL	4333	mSQL	9800	WebDAV
102	MS Exchange	993	IMAP4 over SSL	4444	Blaster	9898	Dabber
110	POP3	995	POP3 over SSL	4664	Google Desktop	9988	Rbot/Spybot
113	Ident	1025	Microsoft RPC	4672	eMule	9999	Urchin
119	NNTP (Usenet)	1026-1029	Windows Messenger	4899	Radmin	10000	Webmin
123	NTP	1080	SOCKS Proxy	5000	UPnP	10000	BackupExec
135	Microsoft RPC	1080	MyDoom	5001	Slingbox	10113-10116	NetIQ
137-139	NetBIOS	1194	OpenVPN	5001	iperf	11371	OpenPGP
143	IMAP4	1214	Kazaa	5004-5005	RTP	12035-12036	Second Life
161-162	SNMP	1241	Nessus	5050	Yahoo! Messenger	12345	NetBus
177	XDMCP	1311	Dell OpenManage	5060	SIP	13720-13721	NetBackup
179	BGP	1337	WASTE	5190	AIM/ICQ	14567	Battlefield
201	AppleTalk	1433-1434	Microsoft SQL	5222-5223	XMPP/Jabber	15118	Dipnet/Oddbob
264	BGMP	1512	WINS	5432	PostgreSQL	19226	AdminSecure
318	TSP	1589	Cisco VQP	5500	VNC Server	19638	Ensim
381-383	HP Openview	1701	L2TP	5554	Sasser	20000	Usermin
389	LDAP	1723	MS PPTP	5631-5632	pcAnywhere	24800	Synergy
411-412	Direct Connect	1725	Steam	5800	VNC over HTTP	25999	Xfire
443	HTTP over SSL	1741	CiscoWorks 2000	5900+	VNC Server	27015	Half-Life
445	Microsoft DS	1755	MS Media Server	6000-6001	X11	27374	Sub7
464	Kerberos	1812-1813	RADIUS	6112	Battle.net	28960	Call of Duty
465	SMTP over SSL	1863	MSN	6129	DameWare	31337	Back Orifice
497	Retrospect	1985	Cisco HSRP	6257	WinMX	33434+	traceroute
500	ISAKMP	2000	Cisco SCCP	6346-6347	Gnutella		
512	rexec	2002	Cisco ACS	6500	GameSpy Arcade		
513	rlogin	2049	NFS	6566	SANE		
514	syslog	2082-2083	cPanel	6588	AnalogX		
515	LPD/LPR	2100	Oracle XDB	6665-6669	IRC		
520	RIP	2222	DirectAdmin	6679/6697	IRC over SSL		
521	RIPng (IPv6)	2302	Halo	6699	Napster		
540	UUCP	2483-2484	Oracle DB	6881-6999	BitTorrent		

Legend

- Chat
- Encrypted
- Gaming
- Malicious
- Peer to Peer
- Streaming

IANA port assignments published at **http://www.iana.org/assignments/port-numbers**

by Jeremy Stretch — v1.1

EIGRP

packetlife.net

Protocol Header

8	16	24	32
Version	Opcode	Checksum	
Flags			
Sequence Number			
Acknowledgment Number			
Autonomous System Number			
Type	Length		
Value			

Metric Formula

$$256 * (K_1 * \text{bw} + \frac{K_2 * \text{bw}}{256 - \text{load}} + K_3 * \text{delay}) * \frac{K_5}{\text{rel} + K_4}$$

- **bw** = 10^7 / minimum path bandwidth in kbps
- **delay** = interface delay in µsecs / 10

EIGRP Configuration

Protocol Configuration

```
! Enable EIGRP
router eigrp <ASN>

 ! Add networks to advertise
 network <IP address> <wildcard mask>

 ! Configure K values to manipulate metric formula
 metric weights 0 <k1> <k2> <k3> <k4> <k5>

 ! Disable automatic route summarization
 no auto-summary

 ! Designate passive interfaces
 passive-interface (<interface> | default)

 ! Enable stub routing
 eigrp stub [receive-only | connected | static | summary]

 ! Statically identify neighoring routers
 neighbor <IP address> <interface>
```

Interface Configuration

```
! Set maximum bandwidth EIGRP can consume
ip bandwidth-percent eigrp <AS> <percentage>

! Configure manual summarization of outbound routes
ip summary-address eigrp <AS> <IP address> <mask> [<AD>]

! Enable MD5 authentication
ip authentication mode eigrp <AS> md5
ip authentication key-chain eigrp <AS> <key-chain>

! Configure hello and hold timers
ip hello-interval eigrp <AS> <seconds>
ip hold-time eigrp <AS> <seconds>

! Disable split horizon for EIGRP
no ip split-horizon eigrp <AS>
```

Attributes

Type	Distance Vector
Algorithm	DUAL
Internal AD	90
External AD	170
Summary AD	5
Standard	Cisco proprietary
Protocols	IP, IPX, Appletalk
Transport	IP/88
Authentication	MD5
Multicast IP	224.0.0.10
Hello Timers	5/60
Hold Timers	15/180

K Defaults	
K_1	1
K_2	0
K_3	1
K_4	0
K_5	0

Packet Types	
1	Update
3	Query
4	Reply
5	Hello
8	Acknowledge

Terminology

Reported Distance
The metric for a route advertised by a neighbor

Feasible Distance
The distance advertised by a neighbor plus the cost to get to that neighbor

Stuck In Active (SIA)
The condition when a route becomes unreachable and not all queries for it are answered; adjacencies with unresponsive neighbors are reset

Passive Interface
An interface which does not participate in EIGRP but whose network is advertised

Stub Router
A router which advertises only a subset of routes, and is omitted from the route query process

Troubleshooting

```
show ip eigrp interfaces
show ip eigrp neighbors
show ip eigrp topology
show ip eigrp traffic
clear ip eigrp neighbors
debug ip eigrp [packet | neighbors]
```

by Jeremy Stretch v2.1

First Hop Redundancy

packetlife.net

Protocols

Hot Standby Router Protocol (HSRP)
Provides default gateway redundancy using one active and one standby router; standardized but licensed by Cisco Systems

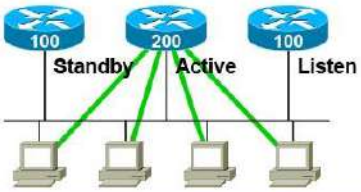
Virtual Router Redundancy Protocol (VRRP)
An open-standard alternative to Cisco's HSRP, providing the same functionality

Gateway Load Balancing Protocol (GLBP)
Supports arbitrary load balancing in addition to redundancy across gateways; Cisco proprietary

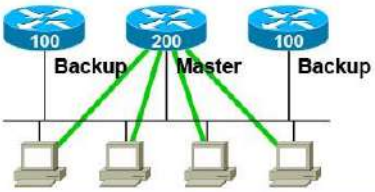
Attributes

	HSRP	VRRP	GLBP
Standard	RFC 2281	RFC 3768	Cisco
Load Balancing	No	No	Yes
IPv6 Support	Yes	No	Yes
Transport	UDP/1985	IP/112	UDP/3222
Default Priority	100	100	100
Default Hello	3 sec	1 sec	3 sec
Multicast Group	224.0.0.2	224.0.0.18	224.0.0.102

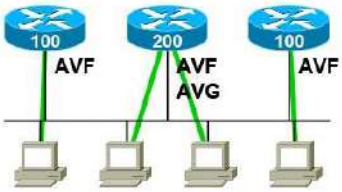
HSRP



VRRP



GLBP



HSRP Configuration

```
interface FastEthernet0/0
 ip address 10.0.1.2 255.255.255.0
 standby version {1 | 2}
 standby 1 ip 10.0.1.1
 standby 1 timers <hello> <dead>
 standby 1 priority <priority>
 standby 1 preempt
 standby 1 authentication md5 key-string <password>
 standby 1 track <interface> <value>
 standby 1 track <object> decrement <value>
```

VRRP Configuration

```
interface FastEthernet0/0
 ip address 10.0.1.2 255.255.255.0
 vrrp 1 ip 10.0.1.1
 vrrp 1 timers {advertise <hello> | learn}
 vrrp 1 priority <priority>
 vrrp 1 preempt
 vrrp 1 authentication md5 key-string <password>
 vrrp 1 track <object> decrement <value>
```

GLBP Configuration

```
interface FastEthernet0/0
 ip address 10.0.1.2 255.255.255.0
 glbp 1 ip 10.0.1.1
 glbp 1 timers <hello> <dead>
 glbp 1 timers redirect <redirect> <time-out>
 glbp 1 priority <priority>
 glbp 1 preempt
 glbp 1 forwarder preempt
 glbp 1 authentication md5 key-string <password>
 glbp 1 load-balancing <method>
 glbp 1 weighting <weight> lower <lower> upper <upper>
 glbp 1 weighting track <object> decrement <value>
```

HSRP/GLBP Interface States

Speak · Gateway election in progress

Active · Active router/VG

Standby · Backup router/VG

Listen · Not the active router/VG

VRRP Interface States

Master · Acting as the virtual router

Backup · All non-master routers

GLBP Roles

Active Virtual Gateway (AVG)
Answers for the virtual router and assigns virtual MAC addresses to group members

Active Virtual Forwarder (AVF)
All routers which forward traffic for the group

GLBP Load Balancing

Round-Robin (default)
The AVG answers host ARP requests for the virtual router with the next router in the cycle

Host-Dependent
Round-robin cycling is used while a consistent AVF is maintained for each host

Weighted
Determines the proportionate share of hosts handled by each AVF

Troubleshooting

`show standby [brief]`	`show vrrp [brief]`
`show glbp [brief]`	`show track [brief]`

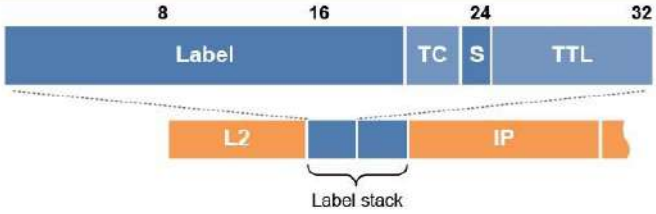
by Jeremy Stretch

v2.0

FRAME MODE MPLS

packetlife.net

Protocol Header



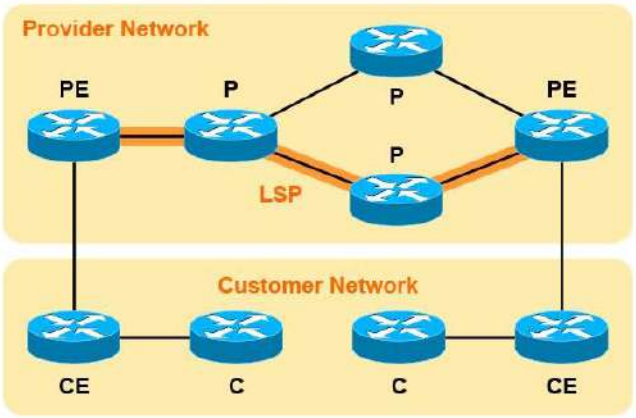
Label (20 bits) · Unique label value

Traffic Class (3 bits) · CoS-mapped QoS marking

Bottom of Stack (1 bit) · Indicates label is last in the stack

Time To Live (8 bits) · Hop counter mapped from IP TTL

Label Switched Path



Customer (C) · IP-only routers internal to customer network

Customer Edge (CE) · C routers which face PE routers

Provider Edge (PE) · LSRs on the MPLS-IP boundary

Provider (P) · MPLS-only LSRs in provider network

MPLS Configuration

```
! Enable CEF
ip cef

! Select label protocol
mpls label protocol ldp

! Enable MPLS on IP interfaces
interface FastEthernet0/0
 ip address 10.0.0.1 255.255.255.252
 mpls ip
 ! Raise MPLS MTU to accommodate multilabel stack
 mpls mtu 1512
```

Conceptual Components

Control Plane
Facilitates label exchange between neighboring LSRs using LDP or TDP (includes the LIB)

Forwarding/Data Plane
Forwards packets based on label or destination IP address (includes the FIB and LFIB)

Label Protocols

	LDP	TDP
Hello Address	224.0.0.2	255.255.255.255
Hello Port	UDP/646	UDP/711
Adjacency Port	TCP/646	TCP/711
Proprietary	No	Cisco

Terminology

Label Distribution Protocol (LDP)
Standards-based label distribution protocol defined in RFC 3036

Tag Distribution Protocol (TDP)
Cisco's proprietary predecessor to LDP

Label Switching Router (LSR)
Any router performing label switching (MPLS)

Label-Switched Path (LSP)
The unidirectional path through one or more LSRs taken by a label-switched packet belonging to an FEC

Forwarding Equivalence Class (FEC)
A group of packets which are forwarded in an identical manner, typically by destination prefix and/or traffic class

Label Information Base (LIB)
Contains all labels learned by an LSR via a label distribution protocol

Forwarding Information Base (FIB)
Routing database for unlabeled (IP) packets

Label FIB (LFIB)
Routing database for labeled (MPLS) packets

Interim Packet Propagation
An LSR temporarily falls back to IP routing while waiting to learn the necessary MPLS label(s)

Penultimate Hop Popping (PHP)
The second-to-last LSR in an LSP removes the MPLS label so the last LSR only has to perform an IP lookup

Troubleshooting

`show mpls interfaces`	`show mpls ldp bindings [detail]` (LIB)	`show ip cef [detail]` (FIB)
`show mpls ldp neighbors`	`show mpls forwarding-table [detail]` (LFIB)	`debug mpls […]`

by Jeremy Stretch v2.0

IEEE 802.1X

packetlife.net

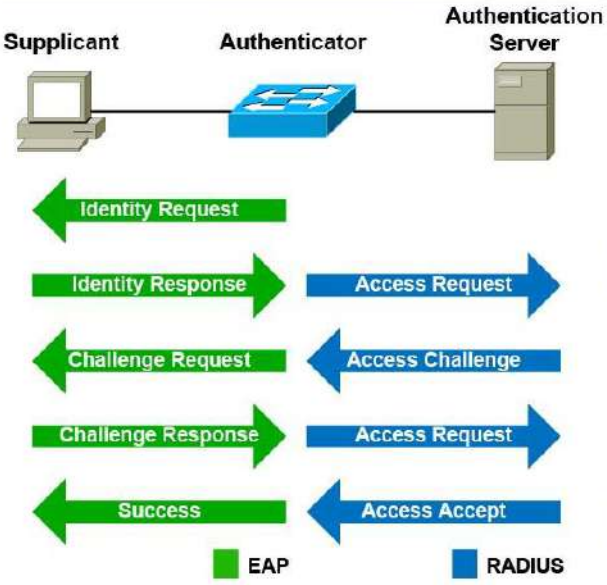
802.1X Header

1	1	2	
Version	Type	Length	EAP

EAP Header

1	1	2	
Code	Identifier	Length	Data

EAP Flow Chart



Configuration

Global Configuration

```
! Define a RADIUS server
radius-server host 10.0.0.100
radius-server key MyRadiusKey
! Configure 802.1X to authenticate via AAA
aaa new-model
aaa authentication dot1x default group radius
! Enable 802.1X authentication globally
dot1x system-auth-control
```

Interface Configuration

```
! Static access mode
switchport mode access
! Enable 802.1X authentication per port
dot1x port-control auto
! Configure host mode (single or multi)
dot1x host-mode single-host
! Configure maximum authentication attempts
dot1x max-reauth-req
! Enable periodic reauthentication
dot1x reauthentication
! Configure a guest VLAN
dot1x guest-vlan 123
! Configure a restricted VLAN
dot1x auth-fail vlan 456
dot1x auth-fail max-attempts 3
```

Terminology

Extensible Authentication Protocol (EAP)
A flexible authentication framework defined in RFC 3748

EAP Over LANs (EAPOL)
EAP encapsulated by 802.1X for transport across LANs

Supplicant
The device (client) attached to an access link that requests authentication by the authenticator

Authenticator
The device that controls the status of a link; typically a wired switch or wireless access point

Authentication Server
A backend server which authenticates the credentials provided by supplicants (for example, a RADIUS server)

Guest VLAN
Fallback VLAN for clients not 802.1X-capable

Restricted VLAN
Fallback VLAN for clients which fail authentication

802.1X Packet Types

0	EAP Packet
1	EAPOL-Start
2	EAPOL-Logoff
3	EAPOL-Key
4	EAPOL-Encap-ASF-Alert

EAP Codes

1	Request
2	Response
3	Success
4	Failure

Interface Defaults

Max Auth Requests	2
Reauthentication	Off
Quiet Period	60s
Reauth Period	1hr
Server Timeout	30s
Supplicant Timeout	30s
Tx Period	30s

EAP Req/Resp Types

1	Identity
2	Notification
3	Nak
4	MD5 Challenge
5	One Time Password
6	Generic Token Card
254	Expanded Types
255	Experimental

Port-Control Options

force-authorized
Port will always remain in authorized state (default)

force-unauthorized
Always unauthorized; authentication attempts are ignored

auto
Supplicants must authenticate to gain access

Troubleshooting

```
show dot1x [statistics] [interface <interface>]
dot1x test eapol-capable [interface <interface>]
dot1x re-authenticate interface <interface>
```

by Jeremy Stretch v2.0

IEEE 802.11 WLAN · PART 1

packetlife.net

IEEE Standards

	802.11a	802.11b	802.11g	802.11n
Maximum Throughput	54 Mbps	11 Mbps	54 Mbps	300 Mbps
Frequency	5 GHz	2.4 GHz	2.4 GHz	2.4/5 GHz
Modulation	OFDM	DSSS	DSSS/OFDM	OFDM
Channels (FCC/ETSI)	21/19	11/13	11/13	32/32
Ratified	1999	1999	2003	2009

WLAN Types

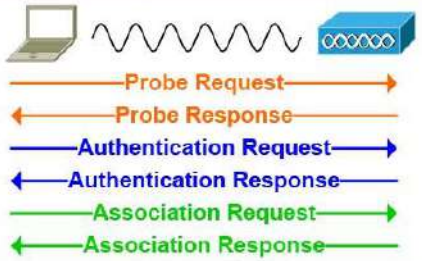
Ad Hoc
A WLAN between isolated stations with no central point of control; an IBSS

Infrastructure
A WLAN attached to a wired network via an access point; a BSS or ESS

Frame Types

Type	Class
Association	Management
Authentication	Management
Probe	Management
Beacon	Management
Request to Send (RTS)	Control
Clear to Send (CTS)	Control
Acknowledgment (ACK)	Control
Data	Data

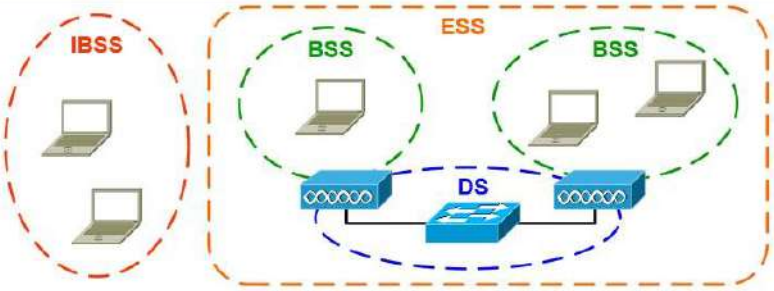
Client Association



Modulations

Scheme	Modulation	Throughput
DSSS	DBPSK	1 Mbps
	DQPSK	2 Mbps
	CCK	5.5/11 Mbps
OFDM	BPSK	6/9 Mbps
	QPSK	12/18 Mbps
	16-QAM	24/36 Mbps
	64-QAM	48/54 Mbps

WLAN Components



Basic Service Area (BSA)
The physical area covered by the wireless signal of a BSS

Basic Service Set (BSS)
A set of stations and/or access points which can directly communicate via a wireless medium

Distribution System (DS)
The wired infrastructure connecting multiple BSSs to form an ESS

Extended Service Set (ESS)
A set of multiple BSSs connected by a DS which appear to wireless stations as a single BSS

Independent BSS (IBSS)
An isolated BSS with no connection to a DS; an *ad hoc* WLAN

Measuring RF Signal Strength

Decibel (dB)
An expression of signal strength as compared to a reference signal; calculated as $10\log_{10}$(signal/reference)

dBm · Signal strength compared to a 1 milliwatt signal

dBw · Signal strength compared to a 1 watt signal

dBi · Compares forward antenna gain to that of an isotropic antenna

Terminology

Basic Service Set Identifier (BSSID)
A MAC address which serves to uniquely identify a BSS

Service Set Identifier (SSID)
A human-friendly text string which identifies a BSS; 1-32 characters

Carrier Sense Multiple Access/Collision Avoidance (CSMA/CA)
The mechanism which facilitates efficient communication across a shared wireless medium (provided by DCF or PCF)

Effective Isotropic Radiated Power (EIRP)
Net signal strength (transmitter power + antenna gain - cable loss)

by Jeremy Stretch v2.2

IEEE 802.11 WLAN · PART 2

packetlife.net

Distributed Coordination Function (DCF)

Interframe Spacing

Short IFS (SIFS)
Used to provide minimal spacing delay between control frames or data fragments

DCF IFS (DIFS)
Normal spacing enforced under DCF for management and non-fragment data frames

Arbitrated IFS (AIFS)
Variable spacing calculated to accommodate differing qualities of service (QoS)

Extended IFS (EIFS)
Extended delay imposed after errors are detected in a received frame

Encryption Schemes

Wired Equivalent Privacy (WEP)
Flawed RC4 implementation using a 40- or 104-bit pre-shared encryption key (deprecated)

Wi-Fi Protected Access (WPA)
Implements the improved RC4-based encryption Temporal Key Integrity Protocol (TKIP) which can operate on WEP-capable hardware

IEEE 802.11i (WPA2)
IEEE standard developed to replace WPA; requires a new generation of hardware to implement significantly stronger AES-based CCMP encryption

Quality of Service Markings

WMM	802.11e	802.1p
Platinum	7/6	6/5
Gold	5/4	4/3
Silver	3/0	0
Bronze	2/1	2/1

Wi-Fi Multimedia (WMM)
A Wi-Fi Alliance certification for QoS; a subset of 802.11e QoS

IEEE 802.11e
Official IEEE WLAN QoS standard ratified in 2005; replaces WMM

IEEE 802.1p
QoS markings in the 802.1Q header on wired Ethernet

Client Authentication

Open · No authentication is used

Pre-shared Encryption Keys
Keys are manually distributed among clients and APs

Lightweight EAP (LEAP)
Cisco-proprietary EAP method introduced to provide dynamic keying for WEP (deprecated)

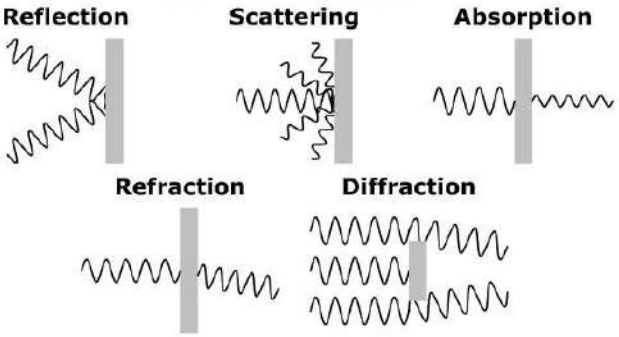
EAP-TLS
Employs Transport Layer Security (TLS); PKI certificates are required on the AP and clients

EAP-TTLS
Clients authenticate the AP via PKI, then form a secure tunnel inside which the client authentication takes place (clients do not need PKI certificates)

Protected EAP (PEAP)
A proposal by Cisco, Microsoft, and RSA which employs a secure tunnel for client authentication like EAP-TTLS

EAP-FAST
Developed by Cisco to replace LEAP; establishes a secure tunnel using a Protected Access Credential (PAC) in the absence of PKI certificates

RF Signal Interference



Antenna Types

Directional · Radiates power in one focused direction

Omnidirectional
Radiates power uniformly across a plane

Isotropic
A theoretical antenna referenced when measuring effective radiated power

by Jeremy Stretch v2.2

Unicast Routing Protocols Comparison

	RIP	EIGRP	OSPF	IS-IS	BGP
Type	Distance Vector	Distance Vector	Link State	Link State	Path Vector
Algorithm	Bellman-Ford	DUAL	Dijkstra	Dijkstra	Path Selection
Admin Distance	120	90/170 (external)/5 (summary)	110	115	20/200 (IBGP)
Standard	RFCs 2080, 2453	Cisco proprietary	RFCs 2328, 5340	ISO 10589, RFC 1142	RFC 4271
Supported Protocols	IPv4, IPv6	IPv4, IPv6, IPX, Appletalk	IPv4, IPv6	IPv4, IPv6, CLNP	IPv4, IPv6
Transport	UDP/520	IP/88	IP/89	Layer 2	TCP/179
Authentication	Plain, MD5	MD5	Plain, MD5, AH (v3)	Plain, MD5	MD5
Multicast Address	224.0.0.9	224.0.0.10	224.0.0.5-6	N/A	N/A

RIP

RIP Implementations

RIPv1
Original RIP implementation, limited to classful routing (obsolete)

RIPv2
Introduced support for classless routing, triggered updates, and multicast announcements (RFC 2453)

RIPng (RIP Next Generation)
Extends RIPv2 to support IPv6 routing (RFC 2080); functions very similarly to RIPv2 and is subsequently as limited

Terminology

Split-Horizon
Mitigates routing loops by ensuring a route is never advertised back to the neighbor from which it was learned

Poison Reverse
Learned routes are advertised back to their originator as explicitly invalid

Troubleshooting

```
show ip[v6] protocols
show ip[v6] rip database
debug ip rip { database | events }
debug ipv6 rip [interface]
```

RIP Configuration

Interface Configuration

```
interface type number
 ! Enable RIPng on the interface
 ipv6 rip name enable
 ! Configure manual route summarization
 ip summary-address rip IPv4-address subnet-mask
 ipv6 rip name summary-address IPv6-prefix
 ! Enable MD5 authentication (RIPv2 only)
 ip rip authentication mode md5
 ip rip authentication key-chain key-chain
```

RIP Configuration

Global Configuration

```
! Enable RIPv2 IPv4 routing
router rip
 version 2
 ! Disable RIPv2 automatic summarization
 no auto-summary
 ! Designate RIPv2 interfaces by network
 network IPv4-network
 ! Identify unicast-only neighbors
 neighbor IP-address
 ! Originate a default route
 default-information originate
 ! Designate passive interfaces
 passive-interface {interface | default}
 ! Modify equal-cost load balancing
 maximum-paths 1-16
 ! Modify timers
 timers basic update invalid hold flush
! Enable RIPng IPv6 routing
ipv6 router rip name
 ! Toggle split-horizon and poison-reverse
 [no] split-horizon
 [no] poison-reverse
```

EIGRP

Metric Formula

$$256 * (K_1 * \textbf{bw} + \frac{K_2 * \textbf{bw}}{256 - \textbf{load}} + K_3 * \textbf{delay}) * \frac{K_5}{\textbf{rel} + K_4}$$

- **bw** = 10^7 / minimum path bandwidth in kbps
- **delay** = interface delay in µsecs / 10

Packet Types	Default K Values
1 Update	K_1 1
3 Query	K_2 0
4 Reply	K_3 1
5 Hello	K_4 0
8 Acknowledge	K_5 0

Terminology

Reported Distance
The metric for a route advertised by a neighbor

Feasible Distance
The distance advertised by a neighbor plus the cost to get to that neighbor

Stuck In Active (SIA)
The condition when a route becomes unreachable and not all queries for it are answered; adjacencies with unresponsive neighbors are reset

Passive Interface
An interface which does not participate in EIGRP but whose network is advertised

Stub Router
A router which advertises only a subset of routes, and is omitted from the route query process

Default Timers

	LAN (>T1)	WAN (<=T1)
Hello	5 sec	60 sec
Hold	15 sec	180 sec

Troubleshooting

```
show ip[v6] eigrp {interfaces | neighbors }
show ip[v6] eigrp topology
clear ip[v6] eigrp [AS-number] neighbors
debug ip[v6] eigrp [neighbor]
```

EIGRP Configuration

Global Configuration

```
! Enable EIGRP for an autonomous system
[ipv6] router eigrp AS-number

! Specify a router ID formatted in IPv4 dotted-decimal
[eigrp] router-id router-ID

! Disable automatic classful summarization (IPv4 only)
no auto-summary

! Enable EIGRP on interfaces by network (IPv4 only)
network IPv4-address wildcard-mask

! Modify maximum paths for equal-cost load balancing
maximum-paths 1-16

! Configure multiplier for unequal-cost load balancing
variance 1-128

! Configure K values to manipulate the metric formula
metric weights 0 k1 k2 k3 k4 k5

! Explicitly identify neighbors on NBMA links
neighbor IP-address interface

! Designate passive interfaces
passive-interface {interface | default}

! Enable stub routing
[eigrp] stub [receive-only | connected | static | summary | redist]
```

Interface Configuration

```
interface type number

! Enable EIGRP for IPv6 on the interface
ipv6 eigrp AS-number

! Set the maximum bandwidth EIGRP can consume (can be >100%)
ip[v6] bandwidth-percent eigrp AS-number 1-999999

! Configure manual summarization of outbound routes
ip summary-address eigrp AS-number IPv4-address subnet-mask [AD]
ipv6 summary-address eigrp AS-number IPv6-prefix [AD]

! Enable MD5 authentication
ip[v6] authentication mode eigrp AS-number md5
ip[v6] authentication key-chain eigrp AS-number key-chain

! Modify interface hello and hold timers
ip[v6] hello-interval eigrp AS-number seconds
ip[v6] hold-time eigrp AS-number seconds

! Toggle split horizon
[no] ip[v6] split-horizon eigrp AS-number
```

CISCO IOS INTERIOR ROUTING PROTOCOLS

PART3

OSPF

OSPFv2 Link State Advertisements

Router Link (Type 1)
Lists neighboring routers and the cost to each; flooded within an area

Network Link (Type 2)
Generated by a DR; lists all routers on an adjacent segment; flooded within an area

Network Summary (Type 3)
Generated by an ABR; advertises routes between areas

ASBR Summary (Type 4)
Injected by an ABR into the backbone to advertise the presence of an ASBR in a non-backbone area

External Link (Type 5)
Generated by an ASBR and flooded throughout the AS to advertise a route external to OSPF

Group Membership (Type 6)
Used by Multicast OSPF; unsupported by IOS

NSSA External Link (Type 7)
Generated by an ASBR in a not-so-stubby area; converted into a type 5 LSA by the ABR when leaving the area

OSPFv3 Link State Advertisements

Name	v2 Equiv.
0x2001 Router LSA	Type 1
0x2002 Network LSA	Type 2
0x2003 Inter-area prefix LSA	Type 3
0x2004 Inter-area router LSA	Type 4
0x4005 AS-external LSA	Type 5
0x2006 Group membership LSA	Type 6
0x2007 Type-7 LSA	Type 7
0x0008 Link LSA	N/A
0x2009 Intra-area prefix LSA	N/A

Network Types

	Nonbroadcast (NBMA)	Multipoint Broadcast	Multipoint Nonbroadcast	Broadcast	Point-to-Point
DR/BDR Elected	Yes	No	No	Yes	No
Neighbor Discovery	No	Yes	No	Yes	Yes
Hello/Dead Timers	30/120	30/120	30/120	10/40	10/40
Defined By	RFC 2328	RFC 2328	Cisco	Cisco	Cisco
Supported Topology	Full Mesh	Any	Any	Full Mesh	Point-to-Point

Router Roles

Internal Router
All interfaces reside within the same area

Backbone Router
A router with at least one interface in area 0

Area Border Router (ABR)
Connects two or more areas

AS Boundary Router (ASBR)
Connects to additional routing domains (redistribution to or from other protocols)

Area Types

Standard Area
Default OSPF area type

Stub Area
External link (type 5) LSAs are replaced with a single default route

Totally Stubby Area
Type 3, 4, and 5 LSAs are replaced with a default route

Not-So-Stubby Area (NSSA)
A stub area containing an ASBR; type 5 LSAs are converted to type 7 within the area

External Route Types

E1
Considers the cost to the advertising ASBR plus the external cost of the route

E2 (Default)
The external cost of a route as seen by the ASBR; internal OSPF cost is not considered

Troubleshooting

```
show ip[v6] ospf [process] interface
show ip[v6] ospf [process] neighbor
show ip[v6] ospf border-routers
show ip[v6] ospf database [LSA-type]
show ip[v6] ospf virtual-links
debug ip[v6] ospf [...]
```

Virtual Links

- Tunnel formed to join two areas across an intermediate
- Both end routers must share a common non-stub area
- At least one end must reside in area 0
- Transition tool; not ideal for permanent designs

Metric Formula

$$\text{cost} = \frac{\textit{reference-bandwidth}}{\textit{link speed}}$$

Adjacency States

1 Down	**5** ExStart	**2** Attempt	**6** Exchange
3 Init	**7** Loading	**4** 2-Way	**8** Full

Message Types

1 Hello	**4** LS Update	**2** DB Descr.	**5** LS Ack
3 LS Request			

DR/BDR Election

- The DR serves as a common point for all adjacencies on a multiaccess segment
- The BDR also maintains adjacencies with all routers in case the DR fails
- Does not occur on point-to-point or multipoint links
- Default priority (0-255) is 1; highest priority wins; 0 cannot be elected
- DR preemption will not occur unless the current DR is reset

OSPF Configuration

Global Configuration

```
! Create an OSPF process
[ipv6] router ospf process-ID
! Specify a router ID formatted as IPv4 dotted-decimal
router-id router-ID
! Modify the default reference bandwidth
auto-cost reference-bandwidth speed-in-mbps
! Assign interfaces to areas by network (OSPFv2)
network IPv4-address wildcard-mask area area
! Identify neighbors for NBMA links (OSPFv2)
neighbor IPv4-address [cost 1-65535]
! Configure summaries on area border routers
area area range { IPv4-address subnet-mask | IPv6-prefix }
! Summarize external routes (ASBRs only)
summary-address IPv4-address subnet-mask [not-advertise]
summary-prefix IPv6-prefix [not-advertise]
! Originate a default route
default-information originate [always]
! Designate stub, totally stubby, or not-so-stubby areas
area area { stub | nssa } [no-summary]
! Create a virtual link
area area virtual-link router-ID
```

Interface Configuration

```
interface type number
! Enable OSPF on the interface
ip[v6] ospf process-ID area area
! Identify neighbors for NBMA links (OSPFv3)
ipv6 ospf neighbor IPv6-address
! Set interface cost manually
ip[v6] ospf cost 1-65535
! Configure DR election priority
ip[v6] ospf priority 0-255
! Specify network type (broadcast, point-to-point, etc.)
ip[v6] ospf network type
! Modify interface hello and dead intervals
ip[v6] ospf hello-interval seconds
ip[v6] ospf dead-interval seconds
! Enable MD5 authentication (OSPFv2)
ip ospf authentication message-digest
ip ospf message-digest-key key-id md5 key-string
! Enable IPsec authentication (OSPFv3)
ipv6 ospf auth ipsec spi spi-number { md5 | sha1 } string
```

CISCO IOS INTERIOR ROUTING PROTOCOLS

PART4

Integrated IS-IS

NSAP Addressing

Interdomain Part (IDP)
Portion of the address used in routing between autonomous systems; assigned by ISO

Domain-Specific Part (DSP)
Portion of the address relevant only within the local AS

Authority and Format Identifier (AFI)
Identifies the authority which dictates the format of the address

Initial Domain Identifier (IDI)
An organization belonging to the AFI

High Order DSP (HODSP)
The area within the AS

System ID
Unique router identifier; 48 bits for Cisco devices (often taken from an Ethernet MAC address)

NSAP Selector (SEL)
Identifies a network layer service; always 0x00 in a NET

ISO Routing Levels

Level 0 Used to locate end systems
Level 1 Routing within an area (IS-IS)
Level 2 Routing between areas (IS-IS)
Level 3 Inter-AS routing

Terminology

Type-Length-Value (TLV)
Variable-length modular datasets carried by PDUs

IS-IS Hello (IIH)
Establish and maintain neighbor adjacencies

Link State PDU (LSP)
Carry TLVs encompassing link state information

Sequence Number Packet (SNP)
Used to request and advertise LSPs; can be complete (CSNP) or partial (PSNP)

Network Entity Title (NET)
Unique router ID; includes area ID

Designated Intermediate System (DIS)
A pseudonode responsible for emulating point-to-point links across a multi-access segment

Adjacency Requirements

- Interface MTUs must match
- Levels must match
- Areas must match (if level 1)
- System IDs must be unique
- Authentication must succeed

DIS Election

- Highest-priority interface elected
- Highest SNPA (e.g. MAC or DLCI) breaks tie
- Highest system ID breaks SNPA tie
- Default interface priority is 64
- Current DIS may be preempted, unlike OSPF

Network Types

Broadcast	**Point-to-Point**
DIS Elected Yes	No
Neighbor Discovery Yes	Yes
Hello/Dead Timers 10/30	10/30

Troubleshooting

```
show [clns | isis] neighbors      show isis [database | spf-log]
show clns interface               debug [clns | isis] [...]
show isis [ipv6] topology
```

IS-IS Configuration

Global Configuration

```
! Enable IS-IS routing
router isis
 ! Specify one or more NET addresses
 net NET
 ! Set global routing level (default level-1-2)
 is-type { level-1 | level-1-2 | level-2-only }
 ! Configure IPv4 route summaries
 summary-address IP-address subnet-mask [level]
 ! Configure IPv6 route summaries
 address-family ipv6
  summary-prefix IPv6-prefix [level]
 ! Originate a default route
 default-information originate
```

Interface Configuration

```
interface type number
 ! Enable IS-IS on an interface
 ip[v6] router isis
 ! Specify interface routing level
 isis circuit-type { level-1 | level-1-2 | level-2-only }
 ! Set interface metric
 isis [ipv6] metric { 1-16777214 | maximum }
 ! Designate the network as point-to-point
 isis network point-to-point
 ! Configure DIS election priority
 isis priority 0-127 [ level-1 | level-2 ]
 ! Modify interface hello and dead intervals
 isis hello-interval seconds [ level-1 | level-2 ]
 isis hello-multiplier 3-1000 [ level-1 | level-2 ]
 ! Enable MD5 authentication
 isis authentication mode md5
 isis authentication key-chain key-chain
```

IOS IPv4 Access Lists

packetlife.net

Standard ACL Syntax

```
! Legacy syntax
access-list <number> {permit | deny} <source> [log]

! Modern syntax
ip access-list standard {<number> | <name>}
 [<sequence>] {permit | deny} <source> [log]
```

Actions

permit	Allow matched packets
deny	Deny matched packets
remark	Record a configuration comment
evaluate	Evaluate a reflexive ACL

Extended ACL Syntax

```
! Legacy syntax
access-list <number> {permit | deny} <protocol> <source> [<ports>] <destination> [<ports>] [<options>]

! Modern syntax
ip access-list extended {<number> | <name>}
 [<sequence>] {permit | deny} <protocol> <source> [<ports>] <destination> [<ports>] [<options>]
```

ACL Numbers

1-99 **1300-1999**	IP standard
100-199 **2000-2699**	IP extended
200-299	Protocol
300-399	DECnet
400-499	XNS
500-599	Extended XNS
600-699	Appletalk
700-799	Ethernet MAC
800-899	IPX standard
900-999	IPX extended
1000-1099	IPX SAP
1100-1199	MAC extended
1200-1299	IPX summary

TCP Options

ack	Match ACK flag
fin	Match FIN flag
psh	Match PSH flag
rst	Match RST flag
syn	Match SYN flag
urg	Match URG flag
established	Match packets in an established session

Logging Options

log	Log ACL entry matches
log-input	Log matches including ingress interface and source MAC address

Source/Destination Definitions

any	Any address
host <address>	A single address
<network> <mask>	Any address matched by the wildcard mask

IP Options

dscp <DSCP>	Match the specified IP DSCP
fragments	Check non-initial fragments
option <option>	Match the specified IP option
precedence {0-7}	Match the specified IP precedence
ttl <count>	Match the specified IP time to live (TTL)

TCP/UDP Port Definitions

eq <port>	Equal to	**neq <port>**	Not equal to
lt <port>	Less than	**gt <port>**	Greater than
range <port> <port>	Matches a range of port numbers		

Miscellaneous Options

reflect <name>	Create a reflexive ACL entry
time-range <name>	Enable rule only during the given time range

Applying ACLs to Restrict Traffic

```
interface FastEthernet0/0
 ip access-group {<number> | <name>} {in | out}
```

Troubleshooting

```
show access-lists [<number> | <name>]
show ip access-lists [<number> | <name>]
show ip access-lists interface <interface>
show ip access-lists dynamic
show ip interface [<interface>]
show time-range [<name>]
```

by Jeremy Stretch v2.0

IPsec

packetlife.net

Protocols

Internet Security Association and Key Management Protocol (ISAKMP)
A framework for the negotiation and management of security associations between peers (traverses UDP/500)

Internet Key Exchange (IKE)
Responsible for key agreement using asymmetric cryptography

Encapsulating Security Payload (ESP)
Provides data encryption, data integrity, and peer authentication; IP protocol 50

Authentication Header (AH)
Provides data integrity and peer authentication, but not data encryption; IP protocol 51

IPsec Modes

Transport Mode
The ESP or AH header is inserted behind the IP header; the IP header can be authenticated but not encrypted

Tunnel Mode
A new IP header is created in place of the original; this allows for encryption of the entire original packet

Configuration

ISAKMP Policy

```
crypto isakmp policy 10
 encryption aes 256
 hash sha
 authentication pre-share
 group 2
 lifetime 3600
```

ISAKMP Pre-Shared Key

```
crypto isakmp key 1 MySecretKey address 10.0.0.2
```

IPsec Transform Set

```
crypto ipsec transform-set MyTS esp-aes 256 esp-sha-hmac
 mode tunnel
```

IPsec Profile

```
crypto ipsec profile MyProfile
 set transform-set MyTS
```

Virtual Tunnel Interface

```
interface Tunnel0
 ip address 172.16.0.1 255.255.255.252
 tunnel source 10.0.0.1
 tunnel destination 10.0.0.2
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile MyProfile
```

Encryption Algorithms

	Type	Key Length (Bits)	Strength
DES	Symmetric	56	Weak
3DES	Symmetric	168	Medium
AES	Symmetric	128/192/256	Strong
RSA	Asymmetric	1024+	Strong

Hashing Algorithms

	Length (Bits)	Strength
MD5	128	Medium
SHA-1	160	Strong

IKE Phases

Phase 1
A bidirectional ISAKMP SA is established between peers to provide a secure management channel (IKE in main or aggressive mode)

Phase 1.5 (optional)
Xauth can optionally be implemented to enforce user authentication

Phase 2
Two unidirectional IPsec SAs are established for data transfer using separate keys (IKE quick mode)

Terminology

Data Integrity
Secure hashing (HMAC) is used to ensure data has not been altered in transit

Data Confidentiality
Encryption is used to ensure data cannot be intercepted by a third party

Data Origin Authentication
Authentication of the SA peer

Anti-replay
Sequence numbers are used to detect and discard duplicate packets

Hash Message Authentication Code (HMAC)
A hash of the data and secret key used to provide message authenticity

Diffie-Hellman Exchange
A shared secret key is established over an insecure path using public and private keys

Troubleshooting

```
show crypto isakmp sa
show crypto isakmp policy
show crypto ipsec sa
show crypto ipsec transform-set
debug crypto {isakmp | ipsec}
```

by Jeremy Stretch v2.0

IPv4 MULTICAST

packetlife.net

Layer 2 Addressing

239.142.57.6

11101111 10001110 00111001 00000110

01-00-5E-0E-39-06

00000001 00000000 01011110 00001110 00111001 00000110

Terminology

Reverse Path Forwarding (RPF)
Verifies that multicast traffic travels in the reverse direction of unicast traffic, away from the tree root

Cisco Group Management Protocol (CGMP)
A proprietary protocol used by switches to obtain multicast membership information for end hosts (deprecated)

Internet Group Management Protocol (IGMP)
Hosts send IGMP requests to local routers to join multicast groups

IGMP Configuration

IGMP Support	`Router(config-if)# ip igmp [version <#>]`
IGMP Snooping	`Switch(config)# ip igmp snooping`

Protocol Independent Multicast (PIM)

Dense Mode
The initial tree encompasses all multicast routers; after a period of time, routers without IGMP members prune back branches

Sparse Mode
The tree is grown from a central rendezvous point out to the multicast source and recipients

Sparse-Dense Mode
Allows a PIM-enabled interface to function in either sparse or dense mode per group

PIMv1
Provides automatic RP discovery with Auto-RP (Cisco proprietary)

PIMv2
Automatic RP discovery is accomplished by the bootstrap router (BSR) method (standard)

PIM Configuration

```
ip multicast-routing
!
interface FastEthernet0/0
 ip pim {sparse-mode | dense-mode | sparse-dense-mode}
 ip pim version {1 | 2}
```

RP Configuration

Manual	`ip pim rp-address <IP>`
Auto-RP Mapping Agent	`ip pim send-rp-discovery scope <TTL>`
Auto-RP Candidate	`ip pim send-rp-announce <interface>`
BSR Candidate	`ip pim bsr-candidate <interface>`
BSR RP Candidate	`ip pim rp-candidate <interface>`

Group Ranges

224.0.0.0/24	Local network control
224.0.1.0/24	Internetwork control
232.0.0.0/8	Source-specific
233.0.0.0/8	GLOP (RFC 3180)
239.0.0.0/8	Admin-scoped

Common Groups

224.0.0.1	All hosts
224.0.0.2	All routers
224.0.1.39	Cisco RP Announce
224.0.1.40	Cisco RP Discovery

Distribution Trees

Shared
A common set of links which carry all multicast traffic; statically configured

Source-Rooted
Provides the shortest paths from the source to receivers

IGMP

IGMPv1
Original IGMP specification

IGMPv2
Adds support for dynamic leave requests and querier election to original IGMP

IGMPv3
Adds multicast source filtering to v2

IGMP Snooping
A switch passively inspects IGMP requests to determine which hosts should receive multicast traffic

IGMP Troubleshooting

```
show ip igmp
show ip igmp group
show ip igmp interface
show ip igmp snooping
ip igmp join-group
```

PIM Troubleshooting

```
show ip mroute
show ip pim interface
show ip pim neighbor
show ip pim rp [mapping]
show ip rpf <IP>
```

by Jeremy Stretch v2.0

IPv4 Subnetting

packetlife.net

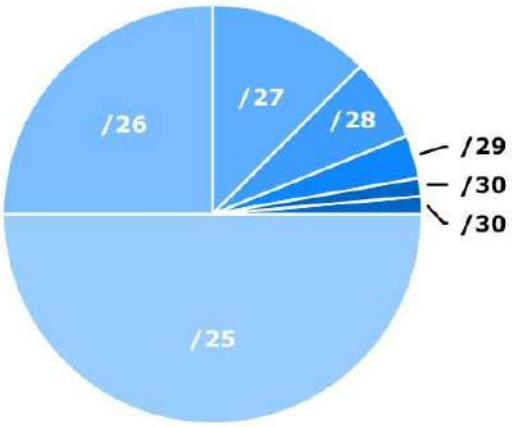
Subnets

CIDR	Subnet Mask	Addresses	Wildcard
/32	255.255.255.255	1	0.0.0.0
/31	255.255.255.254	2	0.0.0.1
/30	255.255.255.252	4	0.0.0.3
/29	255.255.255.248	8	0.0.0.7
/28	255.255.255.240	16	0.0.0.15
/27	255.255.255.224	32	0.0.0.31
/26	255.255.255.192	64	0.0.0.63
/25	255.255.255.128	128	0.0.0.127
/24	255.255.255.0	256	0.0.0.255
/23	255.255.254.0	512	0.0.1.255
/22	255.255.252.0	1,024	0.0.3.255
/21	255.255.248.0	2,048	0.0.7.255
/20	255.255.240.0	4,096	0.0.15.255
/19	255.255.224.0	8,192	0.0.31.255
/18	255.255.192.0	16,384	0.0.63.255
/17	255.255.128.0	32,768	0.0.127.255
/16	255.255.0.0	65,536	0.0.255.255
/15	255.254.0.0	131,072	0.1.255.255
/14	255.252.0.0	262,144	0.3.255.255
/13	255.248.0.0	524,288	0.7.255.255
/12	255.240.0.0	1,048,576	0.15.255.255
/11	255.224.0.0	2,097,152	0.31.255.255
/10	255.192.0.0	4,194,304	0.63.255.255
/9	255.128.0.0	8,388,608	0.127.255.255
/8	255.0.0.0	16,777,216	0.255.255.255
/7	254.0.0.0	33,554,432	1.255.255.255
/6	252.0.0.0	67,108,864	3.255.255.255
/5	248.0.0.0	134,217,728	7.255.255.255
/4	240.0.0.0	268,435,456	15.255.255.255
/3	224.0.0.0	536,870,912	31.255.255.255
/2	192.0.0.0	1,073,741,824	63.255.255.255
/1	128.0.0.0	2,147,483,648	127.255.255.255
/0	0.0.0.0	4,294,967,296	255.255.255.255

Decimal to Binary

Subnet Mask		Wildcard	
255	1111 1111	0	0000 0000
254	1111 1110	1	0000 0001
252	1111 1100	3	0000 0011
248	1111 1000	7	0000 0111
240	1111 0000	15	0000 1111
224	1110 0000	31	0001 1111
192	1100 0000	63	0011 1111
128	1000 0000	127	0111 1111
0	0000 0000	255	1111 1111

Subnet Proportion



Classful Ranges

A	0.0.0.0 – 127.255.255.255
B	128.0.0.0 - 191.255.255.255
C	192.0.0.0 - 223.255.255.255
D	224.0.0.0 - 239.255.255.255
E	240.0.0.0 - 255.255.255.255

Reserved Ranges

RFC 1918	10.0.0.0 - 10.255.255.255
Localhost	127.0.0.0 - 127.255.255.255
RFC 1918	172.16.0.0 - 172.31.255.255
RFC 1918	192.168.0.0 - 192.168.255.255

Terminology

CIDR
Classless interdomain routing was developed to provide more granularity than legacy classful addressing; CIDR notation is expressed as /XX

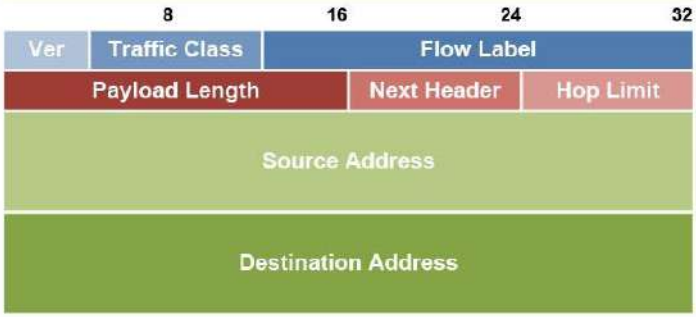
VLSM
Variable-length subnet masks are an arbitrary length between 0 and 32 bits; CIDR relies on VLSMs to define routes

by Jeremy Stretch v2.0

IPv6

packetlife.net

Protocol Header



Version (4 bits) · Always set to 6

Traffic Class (8 bits) · A DSCP value for QoS

Flow Label (20 bits) · Identifies unique flows (optional)

Payload Length (16 bits) · Length of the payload in bytes

Next Header (8 bits) · Header or protocol which follows

Hop Limit (8 bits) · Similar to IPv4's time to live field

Source Address (128 bits) · Source IP address

Destination Address (128 bits) · Destination IP address

Address Types

Unicast · One-to-one communication

Multicast · One-to-many communication

Anycast · An address configured in multiple locations

Address Notation

· Eliminate leading zeros from all two-byte sets

· Replace up to one string of consecutive zeros with a double-colon (::)

Address Formats

Global unicast

Link-local unicast

Multicast

EUI-64 Formation

· Insert 0xfffe between the two halves of the MAC

· Flip the seventh bit (universal/local flag) to 1

Multicast Scopes

1	Interface-local	**5**	Site-local
2	Link-local	**8**	Org-local
4	Admin-local	**E**	Global

Special-Use Ranges

::/0	Default route
::/128	Unspecified
::1/128	Loopback
::/96	IPv4-compatible*
::FFFF:0:0/96	IPv4-mapped
2001::/32	Teredo
2001:DB8::/32	Documentation
2002::/16	6to4
FC00::/7	Unique local
FE80::/10	Link-local unicast
FEC0::/10	Site-local unicast*
FF00::/8	Multicast

* Deprecated

Extension Headers

Hop-by-hop Options (0)
Carries additional information which must be examined by every router in the path

Routing (43)
Provides source routing functionality

Fragment (44)
Included when a packet has been fragmented by its source

Encapsulating Security Payload (50)
Provides payload encryption (IPsec)

Authentication Header (51)
Provides packet authentication (IPsec)

Destination Options (60)
Carries additional information which pertains only to the recipient

Transition Mechanisms

Dual Stack
Transporting IPv4 and IPv6 across an infrastructure simultaneously

Tunneling
IPv6 traffic is encapsulated into IPv4 using IPv6-in-IP, UDP (Teredo), or Intra-Site Automatic Tunnel Addressing Protocol (ISATAP)

Translation
Stateless IP/ICMP Translation (SIIT) translates IP header fields, NAT Protocol Translation (NAT-PT) maps between IPv6 and IPv4 addresses

by Jeremy Stretch v2.0

IS-IS · PART 1

packetlife.net

Protocol Header

4			8	12	16
IRPD				Packet Length	
Version/Protocol ID Extension				ID Length	
R	R	R	PDU Type	Version	
Reserved				Maximum Area Addresses	
Type				Length	
Value ...					

NSAP Addressing

	Interdomain Part			Domain-Specific Part	
NSAP	AFI	IDI	HODSP	System ID	SEL
Condensed	Area				
Example	47	0005.80ff.f800.0000	0001	0000.0c00.1234	00

Interdomain Part (IDP)
Portion of the address used in routing between autonomous systems; assigned by ISO

Domain-Specific Part (DSP)
Portion of the address relevant only within the local AS

Authority and Format Identifier (AFI)
Identifies the authority which dictates the format of the address

Initial Domain Identifier (IDI)
An organization belonging to the AFI

High Order DSP (HODSP)
The area within the AS

System ID
Unique router identifier; 48 bits for Cisco devices (often taken from a MAC address)

NSAP Selector (SEL)
Identifies a network layer service; always 0x00 in a NET address

Network Types

	Broadcast	Point-to-Point
DIS Elected	Yes	No
Neighbor Discovery	Yes	Yes
Hello/Dead Timers	10/30	10/30

Troubleshooting

`show ip route`	`show isis spf-log`
`show ip protocols`	`debug isis spf-events`
`show [clns|isis] neighbor`	`debug isis adjacencies-packets`
`show [clns|isis] interface`	`debug isis spf-statistics`
`show isis database`	`debug isis update-packets`

Attributes

Type	Link-State
Algorithm	Dijkstra
Metric	Default (10)
AD	115
Standard	ISO 10589
Protocols	IP, CLNS
Transport	Layer 2
Authentication	Plaintext, MD5

Routing Levels

Level 0	Used to locate end systems
Level 1	Routing within an area
Level 2	Backbone between areas
Level 3	Inter-AS routing

Terminology

Type-Length-Value (TLV)
Variable-length modular datasets

Link State PDU (LSP)
Carry TLVs encompassing link state information

Sequence Number Packet (SNP)
Used to request and advertise LSPs; can be complete (CSNP) or partial (PSNP)

Hello Packet
Establishes and maintains neighbor adjacencies

Designated Intermediate System
A pseudonode responsible for emulating point-to-point links across a multi-access segment

Adjacency Requirements

- Interface MTUs must match
- Levels must match
- Areas must match (if level 1)
- System IDs must be unique
- Authentication must succeed

DIS Election

- Highest-priority interface elected
- Highest SNPA (MAC/DLCI) breaks tie
- Highest system ID breaks SNPA tie
- Default interface priority is 64
- Current DIS may be preempted

by Jeremy Stretch v2.0

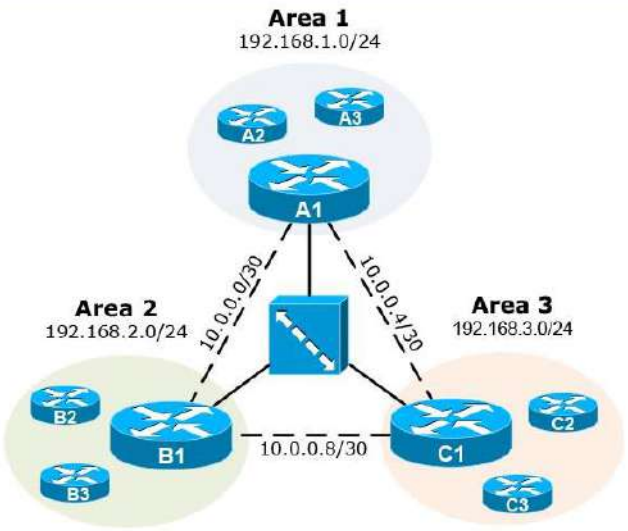
IS-IS · PART 2

packetlife.net

TLV Types

	Name	Use		Name	Use		Name	Use
1	Area Addresses	Hello, LSP	**6**	IS Neighbors	Hello, L2 LSP	**128**	IP Internal Reach.	LSP
2	IS Neighbors	LSP	**8**	Padding	Hello	**129**	Protocols Supported	Hello, LSP
3	ES Neighbors	L1 LSP	**9**	LSP Entries	SNP	**131**	IDRPI	SNP, L2 LSP
5	Prefix Neighbors	L2 LSP	**10**	Authentication	All	**132**	IP Interface Address	Hello, LSP

Configuration Example



Router A1

```
interface FastEthernet0/0
 description Area 1
 ip address 192.168.1.1 255.255.255.0
 ip router isis
 isis circuit-type level-1
!
interface Serial1/0
 no ip address
 encapsulation frame-relay
!
interface Serial1/0.1 point-to-point
 description To Area 2
 ip address 10.0.0.1 255.255.255.252
 ip router isis
 isis circuit-type level-2-only
! MD5 authentication (keychain not shown)
 isis authentication mode md5
 isis authentication key-chain <keychain>
 frame-relay interface-dlci 101
!
interface Serial1/0.2 point-to-point
 description To Area 3
 ip address 10.0.0.5 255.255.255.252
 ip router isis
 isis circuit-type level-2-only
 frame-relay interface-dlci 102
!
router isis
 net 49.0001.0000.0000.00a1.00
```

Router A2

```
interface FastEthernet0/0
 description Area 1
 ip address 192.168.1.2 255.255.255.0
 ip router isis
 isis circuit-type level-1
!
router isis
 net 49.0001.0000.0000.00a2.00
```

Router B1

```
interface FastEthernet0/0
 description Area 2
 ip address 192.168.2.1 255.255.255.0
 ip router isis
 isis circuit-type level-1
!
interface Serial1/0
 no ip address
 encapsulation frame-relay
!
interface Serial1/0.1 point-to-point
 description To Area 1
 ip address 10.0.0.2 255.255.255.252
 ip router isis
 isis circuit-type level-2-only
! MD5 authentication (keychain not shown)
 isis authentication mode md5
 isis authentication key-chain <keychain>
 frame-relay interface-dlci 101
!
interface Serial1/0.2 point-to-point
 description To Area 3
 ip address 10.0.0.9 255.255.255.252
 ip router isis
 isis circuit-type level-2-only
 frame-relay interface-dlci 103
!
router isis
 net 49.0002.0000.0000.00b1.00
```

Router B2

```
interface FastEthernet0/0
 description Area 2
 ip address 192.168.2.2 255.255.255.0
 ip router isis
 isis circuit-type level-1
!
router isis
 net 49.0002.0000.0000.00b2.00
```

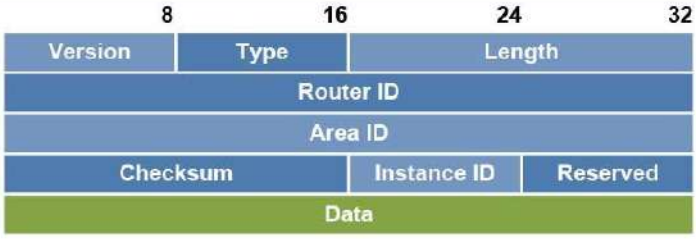
by Jeremy Stretch

v2.0

OSPF · PART 1

packetlife.net

Protocol Header



Link State Advertisements

Router Link (Type 1)
Lists neighboring routers and the cost to each; flooded within an area

Network Link (Type 2)
Generated by a DR; lists all routers on an adjacent segment; flooded within an area

Network Summary (Type 3)
Generated by an ABR and advertised among areas

ASBR Summary (Type 4)
Injected by an ABR into the backbone to advertise the presence of an ASBR within an area

External Link (Type 5)
Generated by an ASBR and flooded throughout the AS to advertise a route external to OSPF

NSSA External Link (Type 7)
Generated by an ASBR in a not-so-stubby area; converted into a type 5 LSA by the ABR when leaving the area

Router Types

Internal Router
All interfaces reside within the same area

Backbone Router
A router with an interface in area 0 (the backbone)

Area Border Router (ABR)
Connects two or more areas

AS Boundary Router (ASBR)
Connects to additional routing domains; typically located in the backbone

Area Types

Standard Area
Default OSPF area type

Stub Area
External link (type 5) LSAs are replaced with a default route

Totally Stubby Area
Type 3, 4, and 5 LSAs are replaced with a default route

Not So Stubby Area (NSSA)
A stub area containing an ASBR; type 5 LSAs are converted to type 7 within the area

External Route Types

E1 · Cost to the advertising ASBR plus the external cost of the route

E2 (Default) · Cost of the route as seen by the ASBR

Troubleshooting

`show ip [route | protocols]`	`show ip ospf border-routers`
`show ip ospf interface`	`show ip ospf virtual-links`
`show ip ospf neighbor`	`debug ip ospf […]`

Attributes

Type	Link-State
Algorithm	Dijkstra
Metric	Cost (Bandwidth)
AD	110
Standard	RFC 2328, 2740
Protocols	IP
Transport	IP/89
Authentication	Plaintext, MD5
AllSPF Address	224.0.0.5
AllDR Address	224.0.0.6

Metric Formula

$$\text{cost} = \frac{100{,}000\ \text{Kbps}^*}{\textbf{link speed}}$$

* modifiable with
`ospf auto-cost reference-bandwidth`

Adjacency States

1 Down	**5** Exstart
2 Attempt	**6** Exchange
3 Init	**7** Loading
4 2-Way	**8** Full

DR/BDR Election

· The DR serves as a common point for all adjacencies on a multiaccess segment

· The BDR also maintains adjacencies with all routers in case the DR fails

· Election does not occur on point-to-point or multipoint links

· Default priority (0-255) is 1; highest priority wins; 0 cannot be elected

· DR preemption will not occur unless the current DR is reset

Virtual Links

· Tunnel formed to join two areas across an intermediate

· Both end routers must share a common area

· At least one end must reside in area 0

· Cannot traverse stub areas

by Jeremy Stretch v2.1

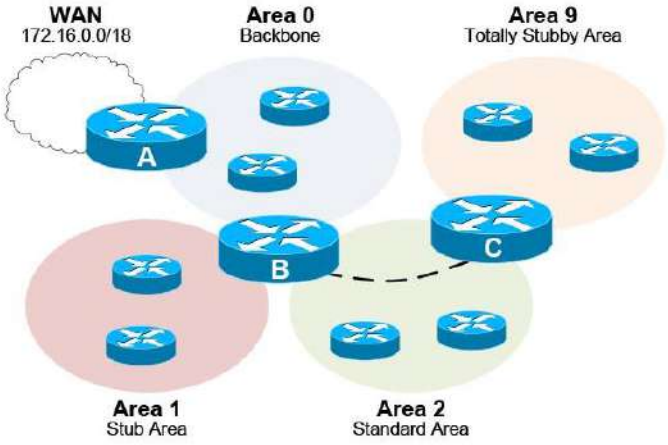
OSPF · PART 2

packetlife.net

Network Types

	Nonbroadcast (NBMA)	Multipoint Broadcast	Multipoint Nonbroadcast	Broadcast	Point-to-Point
DR/BDR Elected	Yes	No	No	Yes	No
Neighbor Discovery	No	Yes	No	Yes	Yes
Hello/Dead Timers	30/120	30/120	30/120	10/40	10/40
Defined By	RFC 2328	RFC 2328	Cisco	Cisco	Cisco
Supported Topology	Full Mesh	Any	Any	Full Mesh	Point-to-Point

Configuration Example



Router A

```
interface Serial0/0
 description WAN Link
 ip address 172.16.34.2 255.255.255.252
!
interface FastEthernet0/0
 description Area 0
 ip address 192.168.0.1 255.255.255.0
!
interface Loopback0
 ! Used as router ID
 ip address 10.0.34.1 255.255.255.0
!
router ospf 100
 ! Advertising the WAN cloud to OSPF
 redistribute static subnets
 network 192.168.0.0 0.0.0.255 area 0
!
 ! Static route to the WAN cloud
ip route 172.16.0.0 255.255.192.0 172.16.34.1
```

Router B

```
interface Ethernet0/0
 description Area 0
 ip address 192.168.0.2 255.255.255.0
 ip ospf 100 area 0
!
interface Ethernet0/1
 description Area 2
 ip address 192.168.2.1 255.255.255.0
 ip ospf 100 area 2
 ! Optional MD5 authentication configured
 ip ospf authentication message-digest
 ip ospf message-digest-key 1 md5 FooBar
 ! Give B priority in DR election
 ip ospf priority 100
!
interface Ethernet0/2
 description Area 1
 ip address 192.168.1.1 255.255.255.0
 ip ospf 100 area 1
!
interface Loopback0
 ip address 10.0.34.2 255.255.255.0
!
router ospf 100
 ! Define area 1 as a stub area
 area 1 stub
 ! Virtual link from area 0 to area 9
 area 2 virtual-link 10.0.34.3
```

Router C

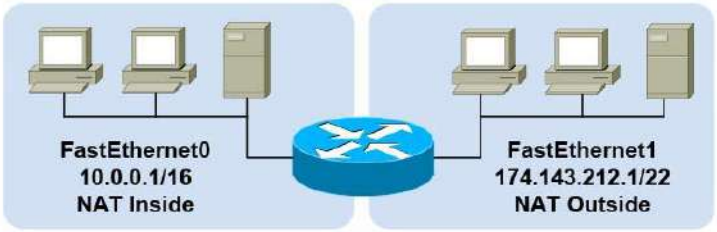
```
interface Ethernet0/0
 description Area 9
 ip address 192.168.9.1 255.255.255.0
 ip ospf 100 area 9
!
interface Ethernet0/1
 description Area 2
 ip address 192.168.2.2 255.255.255.0
 ip ospf 100 area 2
 ! Optional MD5 authentication configured
 ip ospf authentication message-digest
 ip ospf message-digest-key 1 md5 FooBar
 ! Give C second priority (BDR) in election
 ip ospf priority 50
!
!
!
!
!
!
interface Loopback0
 ip address 10.0.34.3 255.255.255.0
!
router ospf 100
 ! Define area 9 as a totally stubby area
 area 9 stub no-summary
 ! Virtual link from area 9 to area 0
 area 2 virtual-link 10.0.34.2
```

by Jeremy Stretch v2.1

NETWORK ADDRESS TRANSLATION

packetlife.net

Example Topology



Address Classification

Inside Local	An actual address assigned to an inside host
Inside Global	An inside address seen from the outside
Outside Global	An actual address assigned to an outside host
Outside Local	An outside address seen from the inside

NAT Boundary Configuration

```
interface FastEthernet0
 ip address 10.0.0.1 255.255.0.0
 ip nat inside
!
interface FastEthernet1
 ip address 174.143.212.1 255.255.252.0
 ip nat outside
```

		Perspective: Local	Perspective: Global
Location	Inside	Inside Local	Inside Global
Location	Outside	Outside Local	Outside Global

Static Source Translation

```
! One line per static translation
ip nat inside source static 10.0.0.19 192.0.2.1
ip nat inside source static 10.0.1.47 192.0.2.2
ip nat outside source static 174.143.212.133 10.0.0.47
ip nat outside source static 174.143.213.240 10.0.2.181
```

Dynamic Source Translation

```
! Create an access list to match inside local addresses
access-list 10 permit 10.0.0.0 0.0.255.255
!
! Create NAT pool of inside global addresses
ip nat pool MyPool 192.0.2.1 192.0.2.254 prefix-length 24
!
! Combine them with a translation rule
ip nat inside source list 10 pool MyPool
!
! Dynamic translations can be combined with static entries
ip nat inside source static 10.0.0.42 192.0.2.42
```

Port Address Translation (PAT)

```
! Static layer four port translations
ip nat inside source static tcp 10.0.0.3 8080 192.0.2.1 80
ip nat inside source static udp 10.0.0.14 53 192.0.2.2 53
ip nat outside source static tcp 174.143.212.4 23 10.0.0.8 23
!
! Dynamic port translation with a pool
ip nat inside source list 11 pool MyPool overload
!
! Dynamic translation with interface overloading
ip nat inside source list 11 interface FastEthernet1 overload
```

Terminology

NAT Pool
A pool of IP addresses to be used as inside global or outside local addresses in translations

Port Address Translation (PAT)
An extension to NAT that translates information at layer four and above, such as TCP and UDP port numbers; dynamic PAT configurations include the **overload** keyword

Extendable Translation
The **extendable** keyword must be appended when multiple overlapping static translations are configured

Special NAT Pool Types

Rotary	Used for load balancing
Match-Host	Preserves the host portion of the address after translation

Troubleshooting

```
show ip nat translations [verbose]
show ip nat statistics
clear ip nat translations
```

NAT Translations Tuning

```
ip nat translation tcp-timeout <seconds>
ip nat translation udp-timeout <seconds>
ip nat translation max-entries <number>
```

Inside Destination Translation

```
! Create a rotary NAT pool
ip nat pool LoadBalServers 10.0.99.200 10.0.99.203 prefix-length 24 type rotary
!
! Enable load balancing across inside hosts for incoming traffic
ip nat inside destination list 12 pool LoadBalServers
```

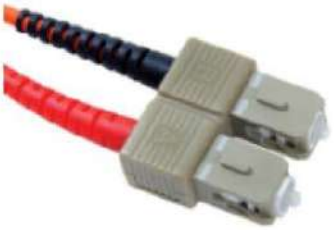
by Jeremy Stretch v1.0

PHYSICAL TERMINATIONS

packetlife.net

Optical Terminations

ST (Straight Tip)



SC (Subscriber Connector)

LC (Local Connector)

MT-RJ

Wireless Antennas

RP-TNC

RP-SMA

Copper Terminations

RJ-45

RJ-11

RJ-21 (25-pair)

DE-9 (Female)

DB-25 (Male)

DB-60 (Male)

GBICs

1000Base-SX/LX

1000Base-T

Cisco GigaStack

1000Base-SX/LX SFP

1000Base-T SFP

X2 (10Gig)

by Jeremy Stretch

v1.1

POINT-TO-POINT PROTOCOL

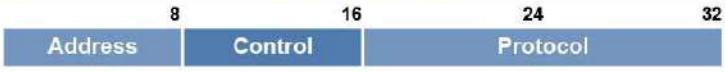
packetlife.net

PPP Components

Link Control Protocol (LCP)
Provides for the establishment, configuration, and maintenance of a PPP link. Protocol-independent options are negotiated by LCP.

Network Control Protocol (NCP)
A separate NCP is used to negotiate the configuration of each network layer protocol (such as IP) carried by PPP.

PPP Header



LCP Header

Authentication Protocols

Plaintext Authentication Protocol (PAP)
Original, obsolete authentication protocol which relies on the exchange of a plaintext key to authenticate peers (RFC 1334).

Challenge Handshake Authentication Protocol (CHAP)
Authenticates peers using the MD5 checksum of a pre-shared secret key (RFC 1994).

Extensible Authentication Protocol (EAP)
Provides MD5-based authentication similar to CHAP (RFC 3748). Could be expanded to support other EAP mechanisms as well.

General PPP Configuration

```
! Configure a peer account if authentication will be used
username peer-hostname password password

! Configure a local IP address pool if needed
ip pool name first-IP last-IP

interface Serial0/0
 ! Enable PPP encapsulation
 encapsulation ppp
 ! Enable CHAP and/or PAP for authentication
 ppp authentication { chap | pap } [ chap | pap ]
 ! Enable compression
 compress { predictor | stac }
 ! Enable peer IP address assignment (server side)
 peer default ip address { pool name | IP-address }
 ! Enable IP address negotiation (client side)
 ip address negotiated
```

Multilink PPP Configuration

```
! Create the multilink interface
interface Multilink1
 ip address IP-address subnet-mask
 ppp multilink group group

! Assign physical interfaces to the multilink group
interface Serial0/0
 encapsulation ppp
 ppp multilink group group
```

PPP Summary

Standard	RFC 1661
Interfaces	Asynchronous serial, synchronous serial, ISDN, HSSI

PPP Features

Protocol Multiplexing · Multiple NCPs

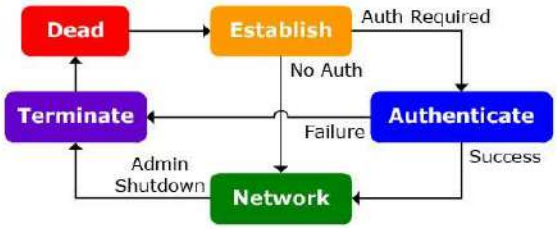
Optional Authentication · PAP/CHAP

Optional Compression · Stacker/predictor

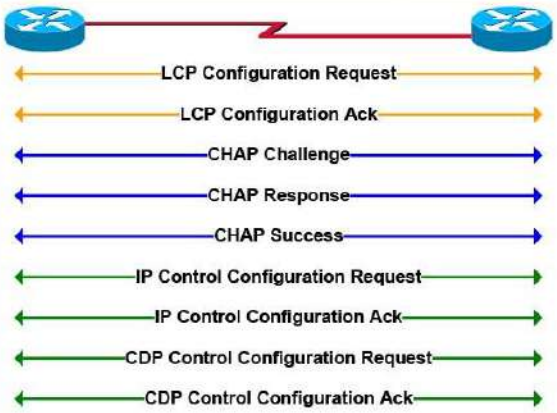
Loopback Detection · Provided by LCP

Load Balancing · Multilink PPP

Connection Phase Flowchart



PPP Connection Example



PPP Compression Algorithms

Stacker
Replaces repetitive data with symbols from a dynamic dictionary (more processor-intensive)

Predictor
Attempts to predict sequential data (more memory-intensive)

Troubleshooting

```
show ppp multilink
debug ppp authentication
debug ppp { negotiation | packet }
```

by Jeremy Stretch

v1.2

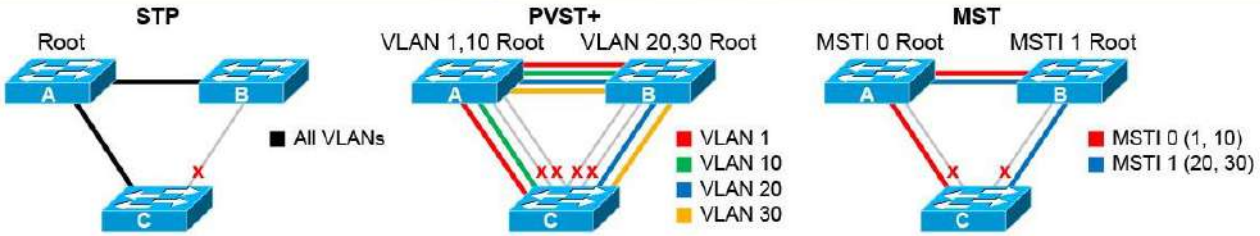
SPANNING TREE · PART 1

packetlife.net

Spanning Tree Protocols

	Legacy STP	PVST	PVST+	RSTP	RPVST+	MST
Algorithm	Legacy ST	Legacy ST	Legacy ST	Rapid ST	Rapid ST	Rapid ST
Defined By	802.1D-1998	Cisco	Cisco	802.1w, 802.1D-2004	Cisco	802.1s, 802.1Q-2003
Instances	1	Per VLAN	Per VLAN	1	Per VLAN	Configurable
Trunking	N/A	ISL	802.1Q, ISL	N/A	802.1Q, ISL	802.1Q, ISL

Spanning Tree Instance Comparison



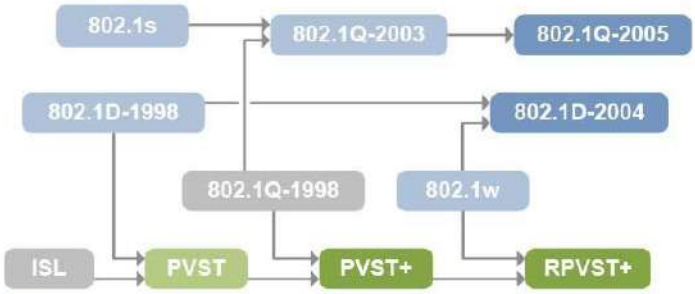
BPDU Format

Field	Bits
Protocol ID	16
Version	8
BPDU Type	8
Flags	8
Root ID	64
Root Path Cost	32
Bridge ID	64
Port ID	16
Message Age	16
Max Age	16
Hello Time	16
Forward Delay	16

Default Timers

Hello	2s
Forward Delay	15s
Max Age	20s

Spanning Tree Specifications



IEEE

- **IEEE 802.1D-1998** · Deprecated legacy STP standard
- **IEEE 802.1w** · Introduced RSTP
- **IEEE 802.1D-2004** · Replaced legacy STP with RSTP
- **IEEE 802.1s** · Introduced MST
- **IEEE 802.1Q-2003** · Added MST to 802.1Q
- **IEEE 802.1Q-2005** · Most recent 802.1Q revision

Cisco

- **PVST** · Per-VLAN implementation of legacy STP
- **PVST+** · Added 802.1Q trunking to PVST
- **RPVST+** · Per-VLAN implementation of RSTP

Link Costs

Bandwidth	Cost
4 Mbps	250
10 Mbps	100
16 Mbps	62
45 Mbps	39
100 Mbps	19
155 Mbps	14
622 Mbps	6
1 Gbps	4
10 Gbps	2
20+ Gbps	1

Port States

Legacy ST	Rapid ST
Disabled	Discarding
Blocking	
Listening	
Learning	Learning
Forwarding	Forwarding

Port Roles

Legacy ST	Rapid ST
Root	Root
Designated	Designated
Blocking	Alternate
	Backup

Spanning Tree Operation

1. **Determine root bridge**
   The bridge advertising the lowest bridge ID becomes the root bridge
2. **Select root port**
   Each bridge selects its primary port facing the root
3. **Select designated ports**
   One designated port is selected per segment
4. **Block ports with loops**
   All non-root and non-desginated ports are blocked

by Jeremy Stretch v3.0

SPANNING TREE · PART 2

packetlife.net

PVST+ and RPVST+ Configuration

```
spanning-tree mode {pvst | rapid-pvst}

! Bridge priority
spanning-tree vlan 1-4094 priority 32768

! Timers, in seconds
spanning-tree vlan 1-4094 hello-time 2
spanning-tree vlan 1-4094 forward-time 15
spanning-tree vlan 1-4094 max-age 20

! PVST+ Enhancements
spanning-tree backbonefast
spanning-tree uplinkfast

! Interface attributes
interface FastEthernet0/1
 spanning-tree [vlan 1-4094] port-priority 128
 spanning-tree [vlan 1-4094] cost 19

 ! Manual link type specification
 spanning-tree link-type {point-to-point | shared}

 ! Enables PortFast if running PVST+, or
 ! designates an edge port under RPVST+
 spanning-tree portfast

 ! Spanning tree protection
 spanning-tree guard {loop | root | none}

 ! Per-interface toggling
 spanning-tree bpduguard enable
 spanning-tree bpdufilter enable
```

MST Configuration

```
spanning-tree mode mst

! MST Configuration
spanning-tree mst configuration
 name MyTree
 revision 1

 ! Map VLANs to instances
 instance 1 vlan 20, 30
 instance 2 vlan 40, 50

! Bridge priority (per instance)
spanning-tree mst 1 priority 32768

! Timers, in seconds
spanning-tree mst hello-time 2
spanning-tree mst forward-time 15
spanning-tree mst max-age 20

! Maximum hops for BPDUs
spanning-tree mst max-hops 20

! Interface attributes
interface FastEthernet0/1
 spanning-tree mst 1 port-priority 128
 spanning-tree mst 1 cost 19
```

Bridge ID Format

4	12	48
Pri	Sys ID Ext	MAC Address

Priority
4-bit bridge priority (configurable from 0 to 61440 in increments of 4096)

System ID Extension
12-bit value taken from VLAN number (IEEE 802.1t)

MAC Address
48-bit unique identifier

Path Selection

1. Bridge with lowest root ID becomes the root
2. Prefer the neighbor with the lowest cost to root
3. Prefer the neighbor with the lowest bridge ID
4. Prefer the lowest sender port ID

Optional PVST+ Ehancements

PortFast
Enables immediate transition into the forwarding state (designates edge ports under MST)

UplinkFast
Enables switches to maintain backup paths to root

BackboneFast
Enables immediate expiration of the Max Age timer in the event of an indirect link failure

Spanning Tree Protection

Root Guard
Prevents a port from becoming the root port

BPDU Guard
Error-disables a port if a BPDU is received

Loop Guard
Prevents a blocked port from transitioning to listening after the Max Age timer has expired

BPDU Filter
Blocks BPDUs on an interface (disables STP)

RSTP Link Types

Point-to-Point
Connects to exactly one other bridge (full duplex)

Shared
Potentially connects to multiple bridges (half duplex)

Edge
Connects to a single host; designated by PortFast

Troubleshooting

```
show spanning-tree [summary | detail | root]
show spanning-tree [interface | vlan]
show spanning-tree mst […]
```

by Jeremy Stretch

v3.0

RIP

packetlife.net

RIP Implementations

RIPv1
Original RIP implementation, limited to classful routing (obsolete)

RIPv2
Introduced support for classless routing, authentication, triggered updates, and multicast announcements (RFC 2453)

RIPng (RIP Next Generation)
Extends RIPv2 to support IPv6 routing (RFC 2080); functions very similarly to RIPv2 and is subsequently as limited

Protocols Comparison

	RIPv1	RIPv2	RIPng
IP	IPv4	IPv4	IPv6
Admin Distance	120	120	120
UDP Port	520	520	521
Classless	No	Yes	Yes
Adv. Address	Broadcast	224.0.0.9	FF02::9
Authentication	None	Plain, MD5	None

RIPv2 Configuration

```
! Enable RIPv2 IPv4 routing
router rip
 version 2

 ! Disable RIPv2 automatic summarization
 no auto-summary

 ! Designate RIPv2 interfaces by network
 network network

 ! Identify unicast-only neighbors
 neighbor IP-address

 ! Originate a default route
 default-information originate

 ! Designate passive interfaces
 passive-interface {interface | default}

 ! Modify timers
 timers basic update invalid hold flush
```

RIPng Configuration

```
! Enable IPv6 routing
ipv6 unicast-routing

! Enable RIPng IPv6 routing
ipv6 router rip name

 ! Toggle split-horizon and poison-reverse
 [no] split-horizon
 [no] poison-reverse

 ! Modify timers
 timers basic update invalid hold flush
```

Attributes

Type	Distance Vector
Algorithm	Bellman-Ford
Admin Distance	120
Metric	Hop count (max 15)
Standard	RFCs 2080, 2453
Protocols	IPv4, IPv6
Transport	UDP
Authentication	Plaintext, MD5
Multicast IP	224.0.0.9/FF02::9

Terminology

Split Horizon
A rule that states a router may not advertise a route back to the neighbor from which it was learned

Route Poisoning
When a network becomes unreachable, an update with an infinite metric is generated to explicitly advertise the route as unreachable

Poison Reverse
A router advertises a network as unreachable through the interface on which it was learned

Timer Defaults

Update	30 sec	**Flush**	240 sec
Invalid	180 sec	**Hold-down**	180 sec

RIPv2 Interface Configuration

```
! Configure manual route summarization
ip summary-address rip network mask

! Enable MD5 authentication (RIPv2 only)
ip rip authentication mode md5
ip rip authentication key-chain key-chain
```

RIPng Interface Configuration

```
! Enable RIPng on the interface
ipv6 rip name enable

! Configure manual route summarization
ipv6 rip name summary-address prefix
```

Troubleshooting

```
show ip[v6] protocols
show ip[v6] rip database
show ip[v6] route rip
debug ip rip { database | events }
debug ipv6 rip [interface]
```

by Jeremy Stretch v1.1

TCPDUMP

packetlife.net

Command Line Options

`-A`	Print frame payload in ASCII	`-q`	Quick output
`-c <count>`	Exit after capturing **count** packets	`-r <file>`	Read packets from **file**
`-D`	List available interfaces	`-s <len>`	Capture up to **len** bytes per packet
`-e`	Print link-level headers	`-S`	Print absolute TCP sequence numbers
`-F <file>`	Use **file** as the filter expression	`-t`	Don't print timestamps
`-G <n>`	Rotate the dump file every n seconds	`-v[v[v]]`	Print more verbose output
`-i <iface>`	Specifies the capture interface	`-w <file>`	Write captured packets to **file**
`-K`	Don't verify TCP checksums	`-x`	Print frame payload in hex
`-L`	List data link types for the interface	`-X`	Print frame payload in hex and ASCII
`-n`	Don't convert addresses to names	`-y <type>`	Specify the data link type
`-p`	Don't capture in promiscuous mode	`-Z <user>`	Drop privileges from root to **user**

Capture Filter Primitives

`[src|dst] host <host>`	Matches a host as the IP source, destination, or either
`ether [src|dst] host <ehost>`	Matches a host as the Ethernet source, destination, or either
`gateway host <host>`	Matches packets which used **host** as a gateway
`[src|dst] net <network>/<len>`	Matches packets to or from an endpoint residing in **network**
`[tcp|udp] [src|dst] port <port>`	Matches TCP or UDP packets sent to/from **port**
`[tcp|udp] [src|dst] portrange <p1>-<p2>`	Matches TCP or UDP packets to/from a port in the given range
`less <length>`	Matches packets less than or equal to **length**
`greater <length>`	Matches packets greater than or equal to **length**
`(ether|ip|ip6) proto <protocol>`	Matches an Ethernet, IPv4, or IPv6 protocol
`(ether|ip) broadcast`	Matches Ethernet or IPv4 broadcasts
`(ether|ip|ip6) multicast`	Matches Ethernet, IPv4, or IPv6 multicasts
`type (mgt|ctl|data) [subtype <subtype>]`	Matches 802.11 frames based on type and optional subtype
`vlan [<vlan>]`	Matches 802.1Q frames, optionally with a VLAN ID of **vlan**
`mpls [<label>]`	Matches MPLS packets, optionally with a label of **label**
`<expr> <relop> <expr>`	Matches packets by an arbitrary expression

Protocols

`arp`	`ip6`	`slip`
`ether`	`link`	`tcp`
`fddi`	`ppp`	`tr`
`icmp`	`radio`	`udp`
`ip`	`rarp`	`wlan`

TCP Flags

`tcp-urg`	`tcp-rst`
`tcp-ack`	`tcp-syn`
`tcp-psh`	`tcp-fin`

Modifiers

`!` or `not`	
`&&` or `and`	
`||` or `or`	

Examples

`udp dst port not 53`	UDP not bound for port 53
`host 10.0.0.1 && host 10.0.0.2`	Traffic between these hosts
`tcp dst port 80 or 8080`	Packets to either TCP port

ICMP Types

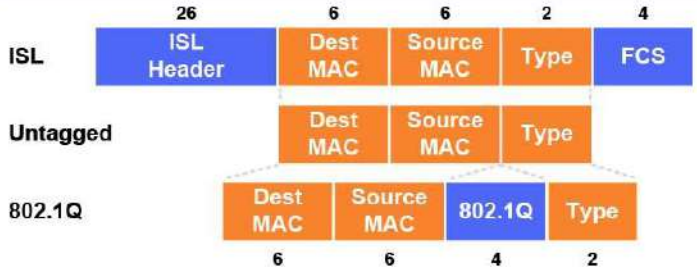
`icmp-echoreply`	`icmp-routeradvert`	`icmp-tstampreply`
`icmp-unreach`	`icmp-routersolicit`	`icmp-ireq`
`icmp-sourcequench`	`icmp-timxceed`	`icmp-ireqreply`
`icmp-redirect`	`icmp-paramprob`	`icmp-maskreq`
`icmp-echo`	`icmp-tstamp`	`icmp-maskreply`

by Jeremy Stretch v2.0

VLANs

packetlife.net

Trunk Encapsulation



VLAN Creation

```
Switch(config)# vlan 100
Switch(config-vlan)# name Engineering
```

Access Port Configuration

```
Switch(config-if)# switchport mode access
Switch(config-if)# switchport nonegotiate
Switch(config-if)# switchport access vlan 100
Switch(config-if)# switchport voice vlan 150
```

Trunk Port Configuration

```
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk encapsulation dot1q
Switch(config-if)# switchport trunk allowed vlan 10,20-30
Switch(config-if)# switchport trunk native vlan 10
```

SVI Configuration

```
Switch(config)# interface vlan100
Switch(config-if)# ip address 192.168.100.1 255.255.255.0
```

VLAN Trunking Protocol (VTP)

Domain
Common to all switches participating in VTP

Server Mode
Generates and propagates VTP advertisements to clients; default mode on unconfigured switches

Client Mode
Receives and forwards advertisements from servers; VLANs cannot be manually configured on switches in client mode

Transparent Mode
Forwards advertisements but does not participate in VTP; VLANs must be configured manually

Pruning
VLANs not having any access ports on an end switch are removed from the trunk to reduce flooded traffic

VTP Configuration

```
Switch(config)# vtp mode {server | client | transparent}
Switch(config)# vtp domain <name>
Switch(config)# vtp password <passsword>
Switch(config)# vtp version {1 | 2}
Switch(config)# vtp pruning
```

Trunk Types

	802.1Q	ISL
Header Size	4 bytes	26 bytes
Trailer Size	N/A	4 bytes
Standard	IEEE	Cisco
Maximum VLANs	4094	1000

VLAN Numbers

0	Reserved	**1004**	fdnet
1	default	**1005**	trnet
1002	fddi-default	**1006-4094**	Extended
1003	tr	**4095**	Reserved

Terminology

Trunking
Carrying multiple VLANs over the same physical connection

Native VLAN
By default, frames in this VLAN are untagged when sent across a trunk

Access VLAN
The VLAN to which an access port is assigned

Voice VLAN
If configured, enables minimal trunking to support voice traffic in addition to data traffic on an access port

Dynamic Trunking Protocol (DTP)
Can be used to automatically establish trunks between capable ports (insecure)

Switched Virtual Interface (SVI)
A virtual interface which provides a routed gateway into and out of a VLAN

Switch Port Modes

`trunk`
Forms an unconditional trunk

`dynamic desirable`
Attempts to negotiate a trunk with the far end

`dynamic auto`
Forms a trunk only if requested by the far end

`access`
Will never form a trunk

Troubleshooting

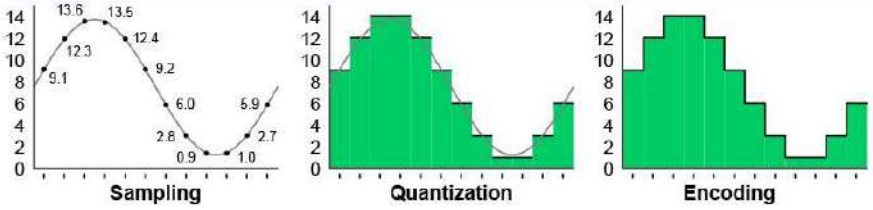
```
show vlan
show interface [status | switchport]
show interface trunk
show vtp status
show vtp password
```

by Jeremy Stretch v2.0

VOIP BASICS

packetlife.net

Pulse Code Modulation (PCM)



Sampling
8000 discrete signal measurements are taken at equal intervals every second

Quantization
The level of each sample is rounded to the nearest expressible value

Encoding
Digital values are encoded as binary numbers for encapsulation

Compression (Optional)
The digital signal is compressed in real time to consume less bandwidth

Power Over Ethernet (PoE)

Cisco Inline Power (ILP)
Pre-standard; employs a 340 kHz tone to detect devices; power needs communicated via CDP

IEEE 802.3af
Detects power requirements of PoE device by the line resistance present

IEEE 802.3at
Uses LLDP to negotiate delivery of up to 25 watts in .10 W intervals

IEEE 802.3af Classes

0	15.4 W	**3**	15.4 W
1	4 W	**4**	Reserved
2	7 W		

Voice Codecs

	MOS	Bandwidth	Complexity	Free
G.722 SB-ADPCM	4.13	48-64 kbps	Medium	Yes
G.711 PCM	4.1	64 kbps	Low	Yes
iLBC	4.1	15.2 kbps	High	Yes
G.729 CS-ACELP	3.92	8 kbps	High	No
G.726 ADPCM	3.85	32 kbps	Medium	Yes
G.729a CS-ACELP	3.7	8 kbps	Medium	No
G.728 LD-CELP	3.61	16 kbps	High	No

Signaling Protocols

ITU-T H.323
Originally designed for multimedia transmission over ISDN; mature and widely supported; peer-to-peer call control

Session Initiation Protocol (SIP)
Text-based, similar in nature to HTTP; defined in RFC 3261; peer-to-peer call control

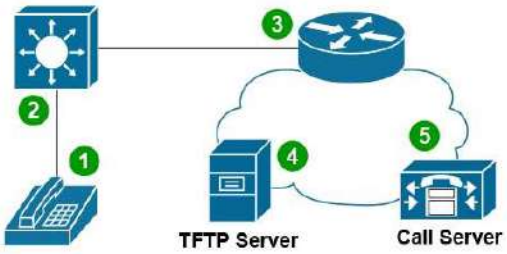
Media Gateway Control Protocol (MGCP)
Employs centralized call control; defined in RFC 3661

Skinny Client Control Protocol (SCCP)
Cisco-proprietary; limited support on gateways; centralized control

Calculating Required Bandwidth

	G.711/Ethernet Example		
Codec Payload (Bitrate × Sample Size)	64 Kbps × 20 msec		160 B
L2 Overhead	Ethernet (18) + 802.1Q (4)	+	22 B
L3 Overhead	IP (20)	+	20 B
L4 Overhead	UDP (8) + RTP (12)	+	20 B
Packets per Second	1000 msec / 20 msec	×	50 pps
Total Bandwidth			88.8 Kbps

IP Phone Boot Process



1. Power Over Ethernet (Optional)
Power is supplied via IEEE 802.3af/at or Cisco ILP

2. VLANs Learned via CDP or LLDP
Voice and data VLANs communicated via CDP/LLDP

3. IP Assignment via DHCP
The phone sends a DHCP request in the voice VLAN; the response includes an IP and DHCP option 150

4. Configuration Retrieved via TFTP
The phone retrieves its configuration from one of the TFTP servers specified in the DHCP option

5. Registration
The phone registers with the call server(s) specified in its configuration

Access Switch Port Configuration

```
interface FastEthernet0/1

 ! Configure data and voice access VLANs
 switchport access vlan <VLAN>
 switchport voice vlan <VLAN>

 ! Trust ingress QoS markings
 mls qos trust cos

 ! Optionally pre-allocate power for the port
 power inline static [max <wattage>]
```

by Jeremy Stretch

v1.0

WIRESHARK DISPLAY FILTERS · PART 1

packetlife.net

Ethernet

eth.addr	eth.len	eth.src
eth.dst	eth.lg	eth.trailer
eth.ig	eth.multicast	eth.type

IEEE 802.1Q

vlan.cfi	vlan.id	vlan.priority
vlan.etype	vlan.len	vlan.trailer

IPv4

ip.addr	ip.fragment.overlap.conflict
ip.checksum	ip.fragment.toolongfragment
ip.checksum_bad	ip.fragments
ip.checksum_good	ip.hdr_len
ip.dsfield	ip.host
ip.dsfield.ce	ip.id
ip.dsfield.dscp	ip.len
ip.dsfield.ect	ip.proto
ip.dst	ip.reassembled_in
ip.dst_host	ip.src
ip.flags	ip.src_host
ip.flags.df	ip.tos
ip.flags.mf	ip.tos.cost
ip.flags.rb	ip.tos.delay
ip.frag_offset	ip.tos.precedence
ip.fragment	ip.tos.reliability
ip.fragment.error	ip.tos.throughput
ip.fragment.multipletails	ip.ttl
ip.fragment.overlap	ip.version

IPv6

ipv6.addr	ipv6.hop_opt
ipv6.class	ipv6.host
ipv6.dst	ipv6.mipv6_home_address
ipv6.dst_host	ipv6.mipv6_length
ipv6.dst_opt	ipv6.mipv6_type
ipv6.flow	ipv6.nxt
ipv6.fragment	ipv6.opt.pad1
ipv6.fragment.error	ipv6.opt.padn
ipv6.fragment.more	ipv6.plen
ipv6.fragment.multipletails	ipv6.reassembled_in
ipv6.fragment.offset	ipv6.routing_hdr
ipv6.fragment.overlap	ipv6.routing_hdr.addr
ipv6.fragment.overlap.conflict	ipv6.routing_hdr.left
ipv6.fragment.toolongfragment	ipv6.routing_hdr.type
ipv6.fragments	ipv6.src
ipv6.fragment.id	ipv6.src_host
ipv6.hlim	ipv6.version

ARP

arp.dst.hw_mac	arp.proto.size
arp.dst.proto_ipv4	arp.proto.type
arp.hw.size	arp.src.hw_mac
arp.hw.type	arp.src.proto_ipv4
arp.opcode	

TCP

tcp.ack	tcp.options.qs
tcp.checksum	tcp.options.sack
tcp.checksum_bad	tcp.options.sack_le
tcp.checksum_good	tcp.options.sack_perm
tcp.continuation_to	tcp.options.sack_re
tcp.dstport	tcp.options.time_stamp
tcp.flags	tcp.options.wscale
tcp.flags.ack	tcp.options.wscale_val
tcp.flags.cwr	tcp.pdu.last_frame
tcp.flags.ecn	tcp.pdu.size
tcp.flags.fin	tcp.pdu.time
tcp.flags.push	tcp.port
tcp.flags.reset	tcp.reassembled_in
tcp.flags.syn	tcp.segment
tcp.flags.urg	tcp.segment.error
tcp.hdr_len	tcp.segment.multipletails
tcp.len	tcp.segment.overlap
tcp.nxtseq	tcp.segment.overlap.conflict
tcp.options	tcp.segment.toolongfragment
tcp.options.cc	tcp.segments
tcp.options.ccecho	tcp.seq
tcp.options.ccnew	tcp.srcport
tcp.options.echo	tcp.time_delta
tcp.options.echo_reply	tcp.time_relative
tcp.options.md5	tcp.urgent_pointer
tcp.options.mss	tcp.window_size
tcp.options.mss_val	

UDP

udp.checksum	udp.dstport	udp.srcport
udp.checksum_bad	udp.length	
udp.checksum_good	udp.port	

Operators	Logic	
eq or ==	and or &&	Logical AND
ne or !=	or or ||	Logical OR
gt or >	xor or ^^	Logical XOR
lt or <	not or !	Logical NOT
ge or >=	[n] […]	Substring operator
le or <=		

by Jeremy Stretch v2.0

WIRESHARK DISPLAY FILTERS · PART 2

packetlife.net

Frame Relay

fr.becn	fr.de
fr.chdlctype	fr.dlci
fr.control	fr.dlcore_control
fr.control.f	fr.ea
fr.control.ftype	fr.fecn
fr.control.n_r	fr.lower_dlci
fr.control.n_s	fr.nlpid
fr.control.p	fr.second_dlci
fr.control.s_ftype	fr.snap.oui
fr.control.u_modifier_cmd	fr.snap.pid
fr.control.u_modifier_resp	fr.snaptype
fr.cr	fr.third_dlci
fr.dc	fr.upper_dlci

PPP

ppp.address	ppp.direction
ppp.control	ppp.protocol

MPLS

mpls.bottom	mpls.oam.defect_location
mpls.cw.control	mpls.oam.defect_type
mpls.cw.res	mpls.oam.frequency
mpls.exp	mpls.oam.function_type
mpls.label	mpls.oam.ttsi
mpls.oam.bip16	mpls.ttl

ICMP

icmp.checksum	icmp.ident	icmp.seq
icmp.checksum_bad	icmp.mtu	icmp.type
icmp.code	icmp.redir_gw	

DTP

dtp.neighbor	dtp.tlv_type	vtp.neighbor
dtp.tlv_len	dtp.version	

VTP

vtp.code	vtp.vlan_info.802_10_index
vtp.conf_rev_num	vtp.vlan_info.isl_vlan_id
vtp.followers	vtp.vlan_info.len
vtp.md	vtp.vlan_info.mtu_size
vtp.md5_digest	vtp.vlan_info.status.vlan_susp
vtp.md_len	vtp.vlan_info.tlv_len
vtp.seq_num	vtp.vlan_info.tlv_type
vtp.start_value	vtp.vlan_info.vlan_name
vtp.upd_id	vtp.vlan_info.vlan_name_len
vtp.upd_ts	vtp.vlan_info.vlan_type
vtp.version	

ICMPv6

icmpv6.all_comp	icmpv6.option.name_type.fqdn
icmpv6.checksum	icmpv6.option.name_x501
icmpv6.checksum_bad	icmpv6.option.rsa.key_hash
icmpv6.code	icmpv6.option.type
icmpv6.comp	icmpv6.ra.cur_hop_limit
icmpv6.haad.ha_addrs	icmpv6.ra.reachable_time
icmpv6.identifier	icmpv6.ra.retrans_timer
icmpv6.option	icmpv6.ra.router_lifetime
icmpv6.option.cga	icmpv6.recursive_dns_serv
icmpv6.option.length	icmpv6.type
icmpv6.option.name_type	

RIP

rip.auth.passwd	rip.ip	rip.route_tag
rip.auth.type	rip.metric	rip.routing_domain
rip.command	rip.netmask	rip.version
rip.family	rip.next_hop	

BGP

bgp.aggregator_as	bgp.mp_reach_nlri_ipv4_prefix
bgp.aggregator_origin	bgp.mp_unreach_nlri_ipv4_prefix
bgp.as_path	bgp.multi_exit_disc
bgp.cluster_identifier	bgp.next_hop
bgp.cluster_list	bgp.nlri_prefix
bgp.community_as	bgp.origin
bgp.community_value	bgp.originator_id
bgp.local_pref	bgp.type
bgp.mp_nlri_tnl_id	bgp.withdrawn_prefix

HTTP

http.accept	http.proxy_authorization
http.accept_encoding	http.proxy_connect_host
http.accept_language	http.proxy_connect_port
http.authbasic	http.referer
http.authorization	http.request
http.cache_control	http.request.method
http.connection	http.request.uri
http.content_encoding	http.request.version
http.content_length	http.response
http.content_type	http.response.code
http.cookie	http.server
http.date	http.set_cookie
http.host	http.transfer_encoding
http.last_modified	http.user_agent
http.location	http.www_authenticate
http.notification	http.x_forwarded_for
http.proxy_authenticate	

by Jeremy Stretch v2.0

دوستان عزیز در این جزوه تمام تلاش خود را کرده‌ام تا بتوانم موضوعات این دوره را به صورت ساده، کامل و کاربردی برای شما عزیزان بیان کنم. در صورت هرگونه میتوانید از طریق ارتباطات زیر با من در تماس باشید. به امید موفقیت‌های روز افرون...

Email : shahmohammadi301@gmail.com

LinkedIn : https://linkedin.com/in/mahdi-shahmohammadi-74ba05100

Telegram : https://t.me/mahdish59

Phone : +989355531775