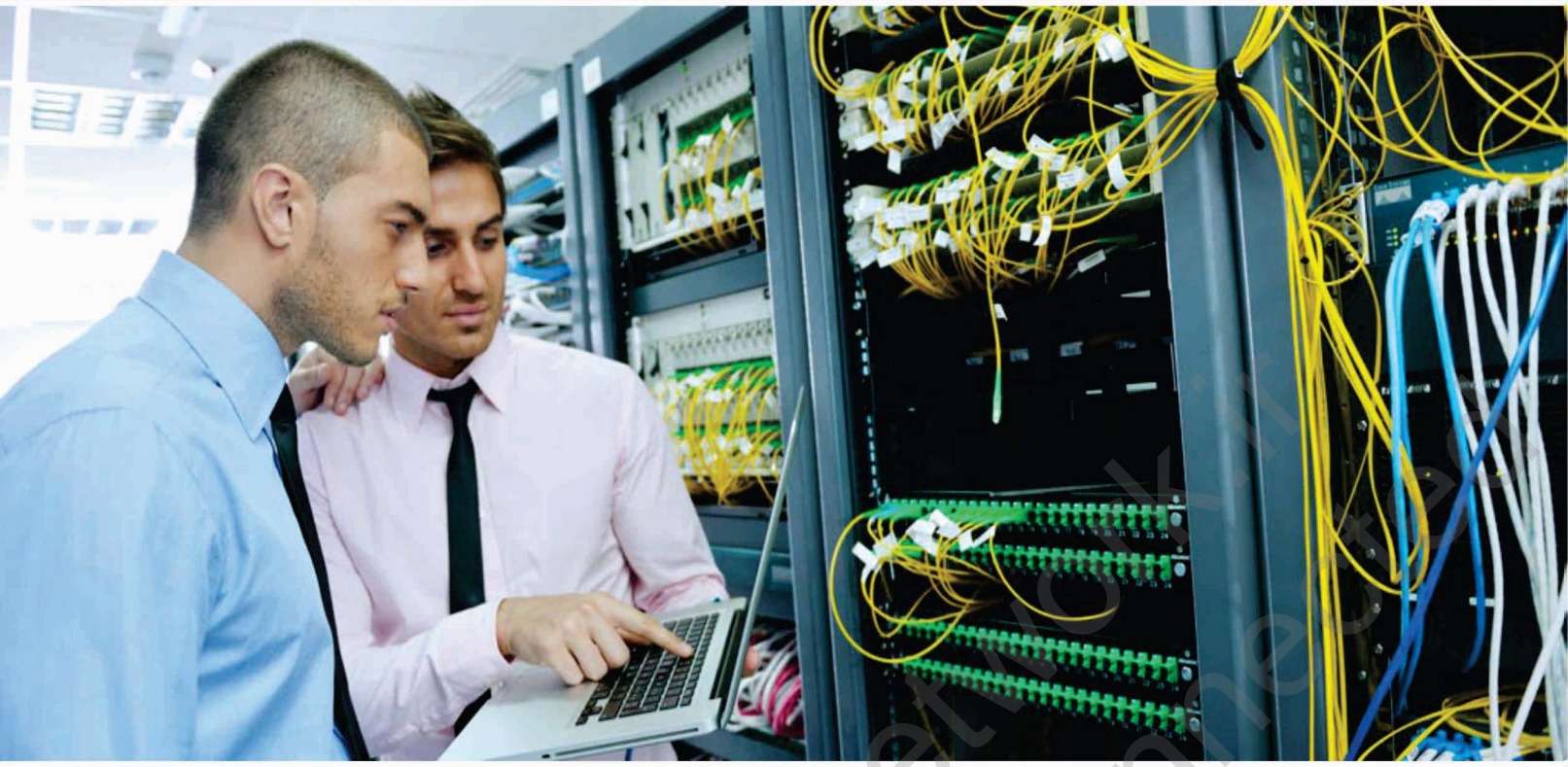


جزوه ۱.۱

CCNA

مدرس دوره : مهندس فرزاد حیدری

تهیه کننده : دانیال نامورکهن

بهار ۱۳۹۵

SEMATEC
مرکز آموزش های تخصصی سماتک

درود و سپاس

پایه و اساس مطالب گردآوری شده در این جزوه بر مبنای آموزه های دریافتی اینجانب در محضر استاد گرانقدر مهندس فرزاد حیدری در موسسه آموزشی سماتک بوده است. شایان ذکر است با توجه به گستردگی و حجم مطالب پیرامون موضوع دوره آموزشی و نیز جهت تکمیل این مستند به منظور درک مطلوبتر مطالب، از کلیه منابع اطلاعاتی در دسترس (کتاب, اینترنت ، نسخ قبلی جزوه و ...) متناسب با بضاعت شخصی استفاده گردیده است. در اینجا لازم می دانم از کلیه پدید آورندگان, تهیه کنندگان، نویسندگان منابع فوق در دنیای مجازی و غیرمجازی صمیمانه تشکر نموده و برایشان موفقیت و کسب مدارج علمی بالاتر آرزو نمایم.

بدون تردید این جزوه دارای کمبود و کاستی های نیز می باشد که ضمن عذر تقصیر، خواهشمند است در رفع آن مساعدت و یاری نمایید.

با تقدیم و تجدید احترام – دانیال نامورکهن
Daniel.Namvar-kohan@gmail.com
بهار ۱۳۹۵

ویرایش	سطح ویرایش	شـــــــرح ویرایش
۱,۱	اصلاح	دستورات مربوط به پیکربندی VTP صفحه ۳۳ و OSPF صفحه ۷۲

با تشکر از دانشجویان و خوانندگان این جزوه که با مسئولیت پذیری به انتقال اشکالات و ارتقاء کیفی این جزوه کمک می نمایند.

فصل اول

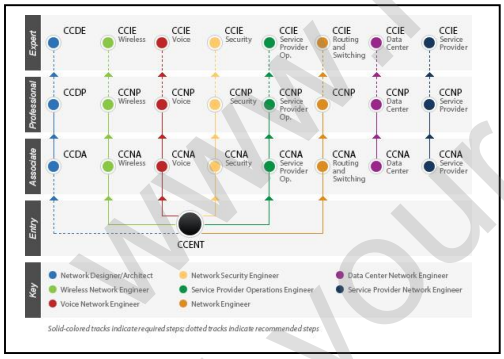
آشنایی با CISCO

شرکت سیسکو سیستمز (Cisco Systems) شرکت آمریکایی تولیدکننده تجهیزات شبکه (Network) است که مرکز آن در شهر سن‌خوزه، کالیفرنیا در ناحیه معروف به سیلیکان ولی در ایالت کالیفرنیا قرار دارد. این شرکت محصولات مربوط به شبکه و ارتباطات را طراحی می‌کند و با سه نام تجاری مختلف سیسکو، لینکسیس و ساینتیفیک آتلانتا به فروش می‌رساند. در ابتدا، سیسکو فقط روترهای چند پروتکل تولید می‌کرد ولی امروز محصولات سیسکو را در همه جا از اتاق نشیمن گرفته تا شرکت‌های ارائه دهنده خدمات شبکه می‌توان پیدا کرد. دید سیسکو این است «تغییر روش زندگی، کار، بازی و آموزش».

لن بزاک و سندی لرنر (دارای مدرک لیسانس از دانشگاه ایالتی کالیفرنیا، فوق لیسانس اقتصادسنجی از دانشگاه کلرمونت و فوق لیسانس علوم کامپیوتر از دانشگاه استنفورد)، زوجی که در بخش کامپیوتر دانشگاه استنفورد کار می‌کردند، Cisco را در سال ۱۹۸۴ تأسیس کردند. بزاک نرم‌افزار روترهای چند پروتکل را که توسط ویلیام یاگر(یک کارمند دیگر که کارش را سالها قبل از بزاک شروع کرده بود) نوشته شده بود تکمیل کرد.

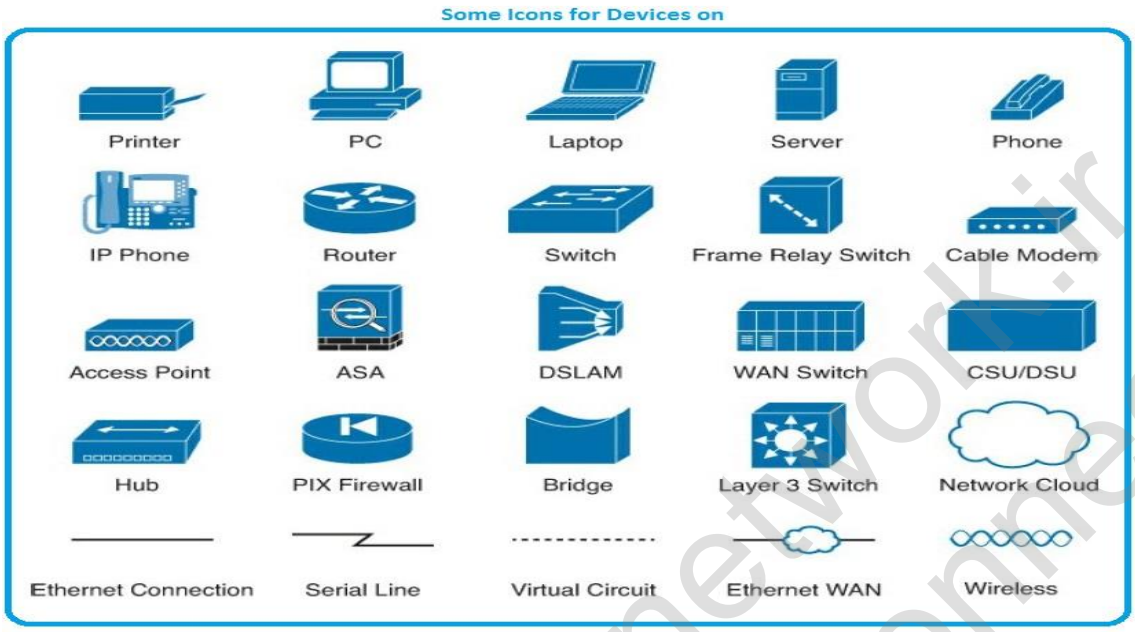
با وجود اینکه Cisco اولین شرکتی نبود که Router طراحی و تولید می‌کرد، اولین شرکتی بود که یک Router چند پروتکل موفق تولید می‌کرد که اجازه ارتباط بین پروتکل‌های مختلف شبکه را می‌دهد. از زمانی که پروتکل اینترنت (IP) به یک استاندارد تبدیل شد، اهمیت Router های چند پروتکل کاهش یافت. امروزه بزرگ‌ترین روترهای Cisco طراحی شده‌اند تا بسته‌های IP و فریمهای MPLS را هدایت کنند. در ۱۹۹۰، شرکت به سهامی عام تبدیل شد و سهام آن در بازار بورس نزدک عرضه شد. بزاک و لرنر با ۱۷۰ میلیون دلار از شرکت خارج شدند و بعد از مدتی جدا شدند. زمان انفجار اینترنت در ۱۹۹۹، Cisco شرکت Cerent واقع در کالیفرنیا را با قیمت ۷ میلیارد دلار خریداری کرد. این شرکت گرانترین خرید Cisco در آن زمان بود. تنها خرید گرانتر مربوط به ساینتیفیک آتلانتا می‌باشد.

شناخت هرم سیسکو ، دوره ها و گواهینامه ها



Network Engineer Path			Certification Exam
5	CCA	Cisco Certified Architect	
4	CCIE	Cisco Certified Internetwork Expert	
3	CCNP	Cisco Certified Professional	300-101 Route, 300-115 Switch, 300-135 TShoot
2	CCNA	Cisco Certified Associate	(ICND1:100-101, ICND2:200-101) or (200-120)
1	CCENT	Cisco Certified Entry Networking Technician	ICND1:100-101

نمادها و الگوهای نگارش

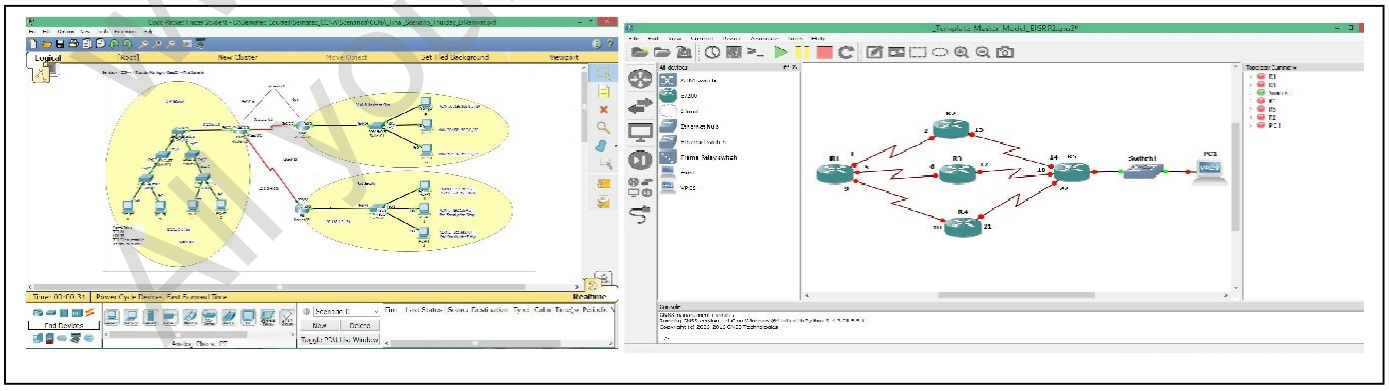


- نگارش دستورات با حروف کوچک مشخص خواهد شد.
- نگارش پارامترهای دستور که می بایست با توجه به نیاز کاربر مشخص نماید با حروف بزرگ درج می گردد.
- پارامترهای انتخابی که در صورت نیاز استفاده می شود در داخل آکولاد {} قرار خواهد گرفت.
- پارامترهای انتخابی یک از چند که در می بایست یکی از گزینه ها حتماً انتخاب استفاده شود در داخل آکولاد < > قرار خواهد گرفت.

مثال :

Switch(Config)# interface {range} TYPE / MOD NUM
Switch(Config)# hostname <HOSTNAME>
Switch# show < run | flash | ip | mac | …. >

- نرم افزارهای مورد استفاده در طول دوره Packet-Tracer (۸۵٪) و GNS3 (۱۵٪) و برخی ابزارهای کمکی



آشنایی با سوییچ (Switch) – بخش اول:

سوئیچ شبکه یک دستگاه شبکه کامپیوتری است که نقطه‌های شبکه یا دستگاه های شبکه را به یکدیگر وصل می‌نماید. این واژه معمولا به دستگاه چند پورته‌ای اطلاق می‌شود که پردازش و انتقال داده را در لایه‌ی دوم مدل OSI انجام می‌دهد. سوئیچ هایی که معمولا در لایه‌ی سوم یا بالاتر پردازش را انجام می‌دهند، معمولا سوئیچ چند لایه یا سوئیچ لایه ۳ خوانده می‌شوند. اولین سوئیچ اترنت، توسط Kalpana در سال ۱۹۹۰ معرفی شد.

سوئیچ یک وسیله‌ی ارتباط از راه دور است که پیام ها را از هر وسیله‌ای که به آن وصل است دریافت میکند و سپس آن را تنها برای دستگاه هدف ارسال میکند. این کار سوئیچ را یک وسیله هوشمند تر نسبت به هاب میکند (که پیغامی را دریافت میکند و آن را برای تمام دستگاه‌های موجود در شبکه ارسال میکند). سوئیچ شبکه، یک نقش کامل را در بیشتر شبکه‌های مدرن محلی اجرا می‌کند. شبکه‌های متوسط به بزرگ معمولا یک یا چند سوئیچ مدیریت شده را شامل می‌شوند.

سوئیچ برای اتصال دستگاهای مختلف از قبیل رایانه, مسیریاب, چاپگرهای تحت شبکه، دوربین‌های مدار بسته و .... در شبکه‌های کابلی مورد استفاده واقع می‌شود. در شکل ظاهری سوئیچ همانند جعبه ایست متشکل از چندین درگاه اترنت که از این لحاظ شبیه هاب (Hub) می‌باشد، با وجود آنکه هر دو این‌ها وظیفه برقراری ارتباط بین دستگاه‌های مختلف را بر عهده دارند، تفاوت از آنجا آغاز می‌شود که هاب بسته‌های ارسالی از طرف یک دستگاه را به همهٔ درگاه‌های خود ارسال می‌کند و کلیه دستگاه‌های دیگر علاوه بر دستگاه مقصد این بسته‌ها را دریافت می‌کنند در حالیکه در سوئیچ ارتباطی مستقیم بین درگاه دستگاه مبدا با درگاه دستگاه مقصد برقرار شده و بسته‌ها مستقیما فقط برای آن ارسال می‌شود.

این خصوصیت از آنجا می‌آید که سوئیچ می‌تواند بسته‌ها را پردازش کند، در سوئیچ‌های معمولی که به *سوئیچ لایه دوم* معروفند این پردازش تا لایه دوم مدل OSI پیش می‌رود و نتیجه این پردازش جدولی است که در سوئیچ با خواندن آدرس سخت‌افزاری (MAC) فرستنده بسته و ثبت درگاه ورودی تشکیل می‌شود. سوئیچ با رجوع به این جدول عملیات آدرس دهی بسته‌ها در لایه دوم را انجام می‌دهد، بدین معنا که این جدول مشخص می‌کند بسته ورودی می‌بایست فقط برای کدام درگاه ارسال شود. در شبکه‌های بزرگ Switchها جدول‌های خود را به اشتراک می‌گذارند تا هر کدام بدانند چه دستگاهی به کدام سوئیچ متصل است و با این کار ترافیک کمتری در شبکه ایجاد کنند.

سوئیچ بطور معمول در لایه دوم مدل OSI کار می‌کند ولی سوئیچ‌هایی با قابلیت کارکرد در لایه‌های مختلف حتی لایه هفتم هم وجود دارد.پرکاربردترین سوئیچ در بین لایه‌های مختلف بجز لایه دوم می‌توان به *سوئیچ لایه سه* اشاره کرد که در بسیاری موارد جایگزین مناسبی برای روتر می‌باشند. از سوئیچ می‌توان در یک شبکه خانگی کوچک تا در شبکه‌های بزرگ با Backbone های چند گیگابایتی استفاده کرد. برخی مزیت‌های و قابلیت‌های سوئیچ :

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

سوییچها به اشکال متعددی با توجه به موضوع قابل دسته بندی می باشند، برخی از این دسته بندیها عبارتند :

- از نظر ابعاد و اندازه متناسب با محل قرارگیری (Size and Form Factor) : Standalone , Rack-mounted
- از نظر نوع پردازش : Layer 2 (Work with Mac-Address) , Layer 3 (Work with IP-Address & Mac-Address), Multilayer
- از نظر گزینه های کنترلی و قابل تنظیم(Network Switch Configuration Option): Fully Managed, Partially Managed and Unmanaged
- از نظر تعداد پورت (Number of LAN port): 16, 24, 32, 48, daisy chaining
- از نظر حداکثر میزان انتقال داده (Maximum data Rate) : 10 ,100 Mbps, 1 , 10 Gbps

heydari.farzad@gmail.com نام مدرس دوره: مهندس فرزاد حیدری
تهیه و گردآوری: دانیال نامورکهن

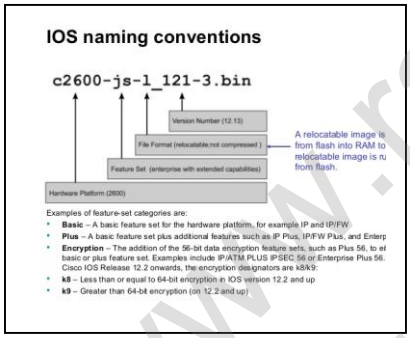
آشنایی اولیه با روتر (Router):

Router یکی از دیوایس های مورد استفاده در شبکه می باشد که در لایه ی سوم OSI (لایه Network) کار می کند. Router بین شبکه های مختلف مسیر یابی می کند. شرکت های زیادی هستند که تجهیزات شبکه مانند Router و دیگر دیوایس های مورد استفاده را تولید می کنند به این سبب Router ها نیز برند ها و مدل های مختلفی دارند اما همانطور که همه می دانیم بهترین شرکت تولید کننده تجهیزات شبکه، شرکت Cisco است که نه تنها تجهیزات بلکه صادر کننده علم شبکه به دنیا نیز می باشد. Routing علمی است که Cisco به دنیا معرفی کرد و کاریست که روتر ها برایمان انجام می دهند. به طور کلی Routing به معنی ارسال بسته از مبدا به مقصد بر اساس پروتکل ها ،آدرس لایه سومی (IP) و Routing Table یک روتر می باشد. روترها را می توان به دو گروه عمده سخت افزاری و نرم افزاری تقسیم نمود:

روترهای سخت افزاری : روترهای فوق ، سخت افزارهائی می باشند که نرم افزارهای خاص تولید شده توسط تولید کنندگان را اجراء می نمایند (در حال حاضر صرفا" به صورت black box به آنان نگاه می کنیم).نرم افزار فوق ، قابلیت روتینگ را برای روترها فراهم نموده تا آنان مهمترین و شاید ساده ترین وظیفه خود که ارسال داده از یک شبکه به شبکه دیگر است را بخوبی انجام دهند . اکثر شرکت ها ترجیح می دهند که از روترهای سخت افزاری استفاده نمایند چراکه آنان در مقایسه با روترهای نرم افزاری، دارای سرعت و اعتماد پذیری بیشتری می باشند.

روترهای نرم افزاری : روترهای نرم افزاری دارای عملکردی مشابه با روترهای سخت افزاری بوده و مسئولیت اصلی آنان نیز ارسال داده از یک شبکه به شبکه دیگر است. یک روتر نرم افزاری می تواند یک سرویس دهنده NT ، یک سرویس دهنده نت ور و یا یک سرویس دهنده لینوکس باشد . تمامی سیستم های عامل شبکه ای مطرح ،دارای قابلیت های روتینگ از قبل تعبیه شده می باشند .

به IOS خوش آمدید ؟



این کلمه برگرفته از Internetwork Operating System ، نرم افزاری است که از آن به منظور کنترل روتینگ و سوئیچینگ دستگاه های بین شبکه ایی استفاده می گردد. آشنائی با IOS برای تمامی مدیران شبکه و به منظور مدیریت و پیکربندی دستگاه هایی نظیر روتر و یا سوئیچ الزامی است.

یک روتر و یا سوئیچ بدون وجود یک سیستم عامل قادر به انجام وظایف خود نمی باشند (همانند یک کامپیوتر). شرکت سیسکو، سیستم عامل Cisco IOS را برای طیف گسترده ای از محصولات شبکه ای خود طراحی و پیاده سازی نموده است. نرم افزار فوق، جزء لاینفک در معماری نرم افزار روترهای سیسکو می باشد و همچنین به عنوان سیستم عامل در سوئیچ های Catalyst ایفای وظیفه می نماید. بدون وجود یک سیستم عامل ، سخت افزار قادر به انجام هیچگونه عملیاتی نخو اهد بود . این سیستم عامل سرویس های شبکه ای زیر را ارائه می نماید :

- عملیات روتینگ و سوئیچینگ
- دستیابی ایمن و مطمئن به منابع شبکه
- قابلیت توسعه و تغییر پیکربندی شبکه

شیوه های اتصال به سوییچ (سوییچ / روتر)

IOS یک تکنولوژی کلیدی است که از آن در اکثر خطوط تولید محصولات شرکت سیسکو استفاده می گردد. عملکرد IOS با توجه به نوع دستگاه های بین شبکه ای متفاوت می باشد.جهت دستیابی به محیط IOS از روش های متعددی استفاده می گردد :

Connect	Connection	Cable	Software	Description
Console	• Serial • Serial-USB • USB	• Rollover • USB-USB	• Hyper Terminal • Tera Term • Putty • Secure CRT • Telnet • SSH	در این روش با استفاده از یک اتصال سریال با سرعت پائین، کامپیوتر/ ترمینال را مستقیماً به پورت کنسول سوییچ یا روتر متصل می نمایند. برای دستیابی به بخش رابط کاربر روتر و یا سوئیچ از یک برنامه ترمینال استفاده می گردد. HyperTerminal متداولترین گزینه در این رابطه می باشد.
Dialup	• Serial • Serial-USB • USB • AUX	•Rollover •USB-USB	• Hyper Terminal • Tera Term • Putty • Secure CR • Telnet • SSH	در این روش با استفاده ازمودم و از طریق پورت کمکی (AUX) با سوییچ / روتر ارتباط برقرار می گردد.
Network	• Net Port • http • https	•Cat xx	• Telnet • SSH	در این روش می توان از یک اتصال شبکه جهت برقراری ارتباط استفاده نمود.

- **استفاده از Telnet** : یک از زیرپروتکلهای، پروتکل TCP/IP تحت شبکه است که در اینترنت و شبکه‌های محلی استفاده می‌شود. این شبکه در سال ۱۹۶۹ توسعه یافت. بیشتر تجهیزات شبکه‌ای و سیستم‌های عاملی که دارای مدل مرجع اینترنتی هستند، تل‌نت را پشتیبانی می‌کند.Telnet یک پروتکل سرویس دهنده و سرویس گیرنده‌است و براساس انتقال ارتباطی عمل می‌کند. این TCP به صورت ۲۳ Port است. اگر چه telnet می‌تواند TCP/IP را بر NCP اجرا کند. پروتکل‌ها چند پسوند دارند و هر یک استاندارد اینترنت می‌باشند. IETF به ۲۷ STD اشاره می‌کند. ۳۲ STB نیز در تعریف پسوندها کاربرد داشته‌است. دیگر پسوندهای IETF یک استاندارد هستند. کارشناسان ایمنی مانند موسسه Sans و اعضای Compoos معتقدند که استفاده از Telnet برای ثبت راه دور می‌تواند در شرایط عادی متوقف شود. این به دلایل زیر گزارش شده‌است. Telnet نمی‌تواند رمزبرداری داده‌های ارسال شده را انجام دهد.

- **استفاده از SSH (Secure Shell)** : SSH یکی از زیر پروتکل های، پروتکل TCP/IP است که به عنوان ابزاری مناسب برای مدیریت و دسترسی به شبکه از راه دور است. این پروتکل، داده‌ها را به صورت رمز شده میان دو میزبان انتقال می‌دهد. پروتکل SSH ابتدا برای سیستم‌های عامل یونیکس و لینوکس ساخته شد تا جایگزینی برای Telnet و دیگر ابزارهای نا امن راه دور باشد. پروتکل‌های قدیمی از ساز و کارهای امنیتی استفاده نمی‌کردند و هر شخصی می‌توانست به راحتی با شنود کردن، به اطلاعات بسیار ارزشمندی مانند نام کاربری و کلمه¬عبور راه دور دست یابد. پروتکل SSH با رمز کردن اطلاعات در حین انتقال، مانع استراق سمع توسط دیگران می‌شود. در واقع این پروتکل یک تونل ارتباطی رمز شده میان دو میزبان به وجود می‌آورد تا داده‌ها تبادل شوند. بنابراین حتی در صورت به دست آوردن اطلاعات میان این دو میزبان، امکان بهره برداری از آن‌ها وجود ندارد. با پروتکل SSH می‌توان امنیت ارتباط را در سراسر یک شبکه نا امن (مانند اینترنت) فراهم کرد.

heydari.farzad@gmail.com نام مدرس دوره: مهندس فرزاد حیدری
تهیه و گردآوری: دانیال نامورکهن

سطوح متعدد رابط کاربر (Interface Level)

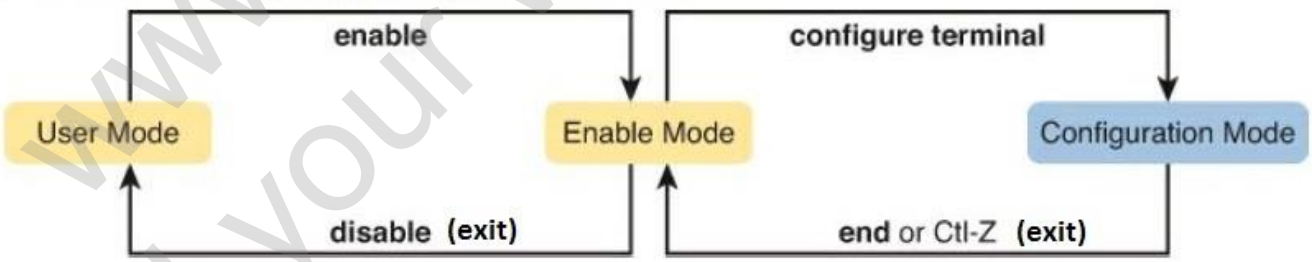
بر خلاف اینترفیس های گرافیکی رایج (GU: Graphic User Interface) و مورد استفاده به دلایل تکنیکی و امنیتی سیستم عامل IOS از یک اینترفیس خط دستوری (Command-Line Interface) استفاده می نماید.

اینترفیس خط دستور و یا CLI سوییچ/ روتر سیسکو از یک ساختار سلسله مراتبی hierarchical تبعیت می نماید. ساختار فوق کاربران را ملزم می نماید که برای انجام هر نوع عملیات خاص به یک mode بخصوص وارد شوند. مثلاً برای پیکربندی یک اینترفیس سوییچ / روتر، کاربر می بایست به mode پیکربندی اینترفیس (interface configuration mode) وارد شود. هر mode دارای یک prompt مختص به خود می باشد که با مشاهده آن می توان دستورات مربوطه به آن سطح را تایپ و استفاده نمود.

IOS ، یک سرویس مفسر دستور با نام EXEC را ارائه می نماید. پس از درج هر دستور ، EXEC صحت آن را بررسی و پس از تائید آن را اجراء می نماید. نرم افزار IOS در جهت افزایش امنیت، دو سطح متفاوت دستیابی user EXEC mode و privileged EXEC mode با ویژگی زیر را برای سرویس مفسر دستور (EXEC) در نظر می گیرد:

Prompt mode	Level Name	Description
Switch> Router> [1]	**User Exec Mode** (View Mode)	در این mode کاربر صرفاً می تواند تعداد محدودی از دستورات مانیتورینگ را اجراء نماید. در این مد دستورات ساده قابل اجراست و نمی توان دستوراتی را که باعث تغییر در پیکربندی روتر می گردند، اجراء نمود. امکان تعبیه تدابیر امنیتی جهت دسترسی و ورود به این سطح توسط کاربر ارشد امکانپذیر می باشد.
Switch# Router#	**Privilege Exec Mode** (Enable mode)	در این mode می توان به تمامی دستورات عملیاتی، اجرایی و مانیتورینگ دستیابی داشت. برای استفاده از این mode و در جهت افزایش امنیت، می توان سوییچ را بگونه ای پیکربندی نمود که کاربران را ملزم به درج نام و رمز عبور جهت دستیابی به سوییچ/ روتر نماید.
Switch(config) Router(config)	**Configuration Mode** (Global Mode)	کلیه تنظیمات و پیکربندی سوییچ/روتر با استفاده از دستورات در این mode میسر می باشد. در این mode نیز با توجه به نوع دستورات به صورت سلسله مراتبی به لایه های دیگری نیز وارد خواهید شد که در آن لایه دستورات و ضوابط مربوط به همان لایه لازم الاجراست که در جای خود به هر کدام از آنها پرداخته خواهد شد.

- استفاده از نرم افزارهای شبیه ساز محیطی (Simulator / Emulator) : به منظور طراحی، پیاده سازی، انجام تنظیمات و اجرای شبکه های متعدد استفاده از یک محیط مجازی توصیه می گردد. استفاده از نرم افزار های Packet Tracer یا GNS3 برای انجام سناریوهای کلاسی و حتی سازمانی پیشنهاد می گردد.



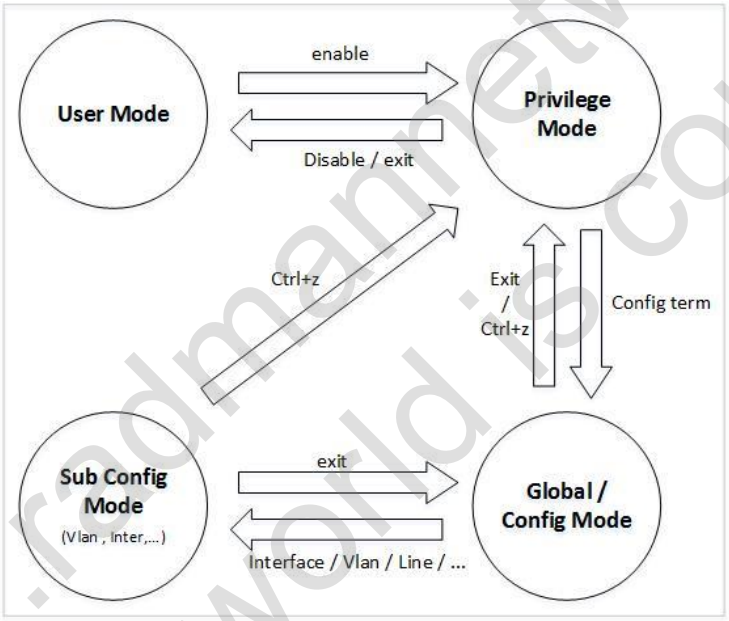
نکات قابل توجه در محیط و سطوح متعدد CLI و تایپ Commands

- غیرحساس به شکل حروف در تایپ دستورات با حروف کوچک و بزرگ (case insensitive)
- حساس به شکل حروف در تایپ و نامگذاری متغیرها با حروف کوچک و بزرگ (case sensitive)
- تکمیل کننده خودکار دستورات commands و پارمترهای آن (Auto-Complete) با فشردن کلید Tab بعد از تایپ چند حرف اولیه
- مفهوم بودن و اجرایی شدن دستورات و پارامترهای مربوطه فقط با تایپ بخشی از آن با توجه به وضعیت پارامتر قبلی
- استفاده از علامت ? جهت دریافت فهرست command های قابل انتخاب با توجه به Mode ، سطح و نوع دستورات اولیه
- چنانچه پیغام خطا زیر مشاهد شد جهت رفع قفل شدن صفحه کلید (hang) در هنگام تایپ و کار در محیط CLI از کلیدهای ترکیبی CTRL+Shift+6 استفاده می شود.

Translating "x x x x "...domain server (255.255.255.255)

چنانچه دستور وارد شده معتبر و یا صحیح نباشد با توجه به نوع خطا پیغام متناسب ظاهر می گردد. لطفاً پیام خطا خوانده شود.

نحوه جابجایی و تغییر محیط در سطوح متعدد سوییچ




```
Switch> enable                          */  ena
Switch# configure Terminal              */ conf  t
Switch(config)# exit                    */ exi
Switch# disable                         */ disa / exi
Switch> exit                            */ exi
-----------------------
Switch> enable                          */  ena
Switch# configure Terminal              */ conf  t
Switch(config)# ctrl+z                  */ press Ctrl +z
Switch>
```

روش ومراحل رمز گذاری به روی Console:

در بخش قبل به روشها و چگونگی اتصال به سوییچ اشاره شد حال به جزییات بیشتر روش اتصال به سوییچ از طریق کنسول و انجام تنظیمات آن که منوط به حضور فیزیکی admin در سایت و اتصال از طریق کابل Rollover میسر می باشد پرداخته می شود. پس از اتصال کابل و استفاده از یک نرم افزار ترمینال دستورات زیر قابل اجرا می باشد.

```
Switch> enable
Switch# configure terminal
Switch(config)# line console 0
Switch(config-line)# password PASSWORD
Switch(config-line)# login
Switch(config-line)# exit
```

جهت حذف رمز از Console می بایست وارد سطح کنسول شد و دستور No را به قبل از دستور Password اضافه نمود.

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

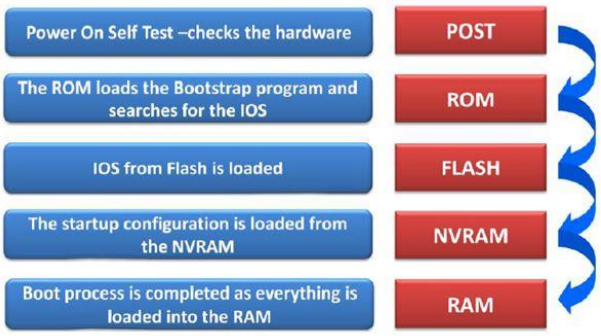
تغییر نام سوییچ و برگشت به حالت Default:

```
Switch(config)# hostname NAME

Switch(config)# hostname S01-Cisco
S01-Cisco(config)#
---------------------------------------------------
Switch(config)# no hostname
Switch(config)#
```

با در دست داشتن رمز کنسول به منظور بالا بردن ضریب امنیتی در محیط IOS همچنین می توان برای ورود به سطح Privilege کد رمز (Password) تعبیه کرد تا هر گونه تغییر و تنظیم پارامترهای IOS سوییچ بدست admin صورت گیرد. با انجام مراحل زیر می توان به این مهم دست یافت. همانند روش های اشاره شده در قبل، جهت حذف کد رمز از دستور no قبل از دستور اصلی استفاده می گردد.

```
Switch(config)# enable password PASSWORD
*/
Switch(config)# enable password 123456
*/
Switch(config)# no password
```

انواع حافظه در سوییچ / روتر:



سوییچ و روترهای سیسکو نیز همانند کامپیوتر ها دارای حافظه هستند که به عنوان فضایی برای ذخیره سازی IOS و فایل های کانفیگ ، اینترفیس های شبکه و ... مربوط به آنها و یا حتی لود شدن خود IOS و خیلی چیز های دیگر استفاده میشود. Admin شبکه با استفاده از دستورات متعدد مدیریت حافظه را بعهده گرفته و نسبت به کپی ، حذف، بروزرسانی و بارگذاری مجدد حافظه اقدام نماید. حافظه در این دو سخت افزار به چهار نوع دسته بندی می شوند:

Memory	IOS word	Description
ROM		براساس تنظیمات سازنده وظیفه شناخت و انجام هماهنگی مابین قطعات داخلی دستگاه را درر زمان Boot را بعهده دارد. در دستگاههای قدیمی سیسکو محل نگهداری IOS بود، ولی بعده ها شامل قسمت هایی شد که وظیفه راه اندازه و بوت را بر عهده دارند.
Flash	Flash	شبیه HDD و یا EPROM در کامپیوتر است، سیستم عامل بر روی آن نصب شده و اطلاعات ذخیره شده با قطع برق از بین نمی رود. در ابتدا Flash ها به صورت SIMM با ظرفیت های پایین بودند که بر روی بورد اصلی روتر نصب میشدند ، مثلا AS5300 یا Cisco 2500 – 2600 ، در حال حاضر اکثر Flash های روتر های سیسکو به صورت کارت های compact flash با ظرفیت های بالا بسته به پشتیبانی و نیاز روتر سیسکو به راحتی از بیرون روتر و بدون نیاز به باز کردن کیس روتر و حتی خاموش کردن روتر سیسکو قابل تعویض و ارتقاع هستند ، برای مثال روتر های سری ۱۸۰۰ – ۱۹۰۰ – ۲۸۰۰ – ۲۹۰۰ – ۳۸۰۰ – ۳۹۰۰ از این نوع
RAM	Running-config	Random Access Memory: همانند حافظه موقت در کامپیوتر است و با قطع جریان برق تمام تنظیمات و اطلاعات موجود در آن پاک خواهد شد. (Non-Permanent) این نوع حافظه به صورت ماژول های DRAM بر روی برد اصلی روتر و یا supervisor engine قابل نصب و ارتقاء است و هر روتر دارای سقف مجاز حداکثری نصب RAM بسته به مدل و سری میباشد .
NVRAM	Startup-config	یا همان Non-Volatile Random Access Memory در واقع محلی برای ذخیره سازی Startup Config دستگاه است ، در واقع پس از لود شدن IOS ، کانفیگ دستگاهو یا همان Startup Config از روی NVRAM خوانده میشود و هرگاه کانفیگ تغییر و ذخیره شود ، این تغییرات بر روی NVRAM ذخیره میشود ، ضمنان vlan database نیز بر روی NVRAM قرار دارد . ذکر این نکته حائز اهمیت است که ، Running Config بر روی RAM قرار دارد تا زمانی که با فرمان ذخیره سازی بر روی NVRAM ذخیره شود ، در غیر این صورت با قطع و وصل برق ، تغییرات اعمال نشده و آخرین Config موجود از روی NVRAM لود خواهد شد . شایان ذکر است به صورت پیش فرض هیچگونه اطلاعاتی در این حافظه موجود نیست.

دستورات IOS جهت مشاهده اطلاعات و ذخیره سازی تنظیمات انجام شده در سوییچ و روتر:

Switch# show running-config	نمایش آخرین محتویات حافظه RAM
Switch# show startup-config	نمایش محتویات حافظه NVRAM (کلیه تنظیمات)
Switch# show flash	نمایش محتویات Flash (IOS)
Switch# copy running-config startup-config	ذخیره سازی محتویات حافظه RAM به NVRAM با دریافت تاییدیه
Switch# copy startup-config running-config	ذخیره سازی محتویات حافظه NVRAM به RAM با دریافت تاییدیه (reset)
Switch# write	ذخیره سازی محتویات حافظه RAM به NVRAM بدون دریافت تاییدیه

ایجاد صفحه هشدار ورودی با استفاده از Banner:

تعبیه یک جمله اخطار دهنده در هنگام ورود به شبکه و ارائه هشدارهای لازم به نفوذ کننده با استفاده از دستور زیر امکانپذیر می باشد. در مطالبی که درج می شود نباید هیچگونه اشاره ای به نام شبکه، نام سازمان ، نوع و مدل دستگاه و ... نمود. (motd: Message Of The Day)

Switch(config)# banner motd " ATTENTION MESSAGE"

Banner های دیگری هم وجود دارد که کمتر مورد استفاده قرار می گیرد.

- پیام برای اعضای شبکه: banner exec
- پیام در خاتمه کار : banner logout

```
Switch(config)# banner motd "
*** Unauthorized Use or Access Prohibited ***
        For Authorized Official Use Only
 You must have explicit permission to access or
 configure this device. All activities performed
 on this device may be logged, and violations of
 this policy may result in disciplinary action, and
 may be reported to low enforcement authorities.

 There is no right to privacy on this device."
```

فصل دوم

Virtual LAN در سوییچ ونحوه تنظیم آن – بخش اول

اول از همه باید مفهوم درست VLAN ، VLAN مخفف Virtual Local Area Network هست یعنی شبکه محلی مجازی ، همانطور که می دانیم هر شبکه محلی برای خودش تنها یک محدوده Broadcast داره که ترافیک محدوده خودش رو در در این محدوده نگه میداره و اگر ما بتونیم بصورت مجازی یک شبکه محلی ایجاد کنیم در حقیقت توانستیم یک محدوده Broadcast یا Broadcast Domain ایجاد کنیم و این باعث می شود که ترافیک شبکه به حالت مطلوبتری کنترل بشود.

وقتی با یک سویچ سیسکو کار می کنید، محدوده کاری آن با نام VLAN 1 مشخص میشود این VLAN به صورت پیش فرض در سوییچ های سیسکو تعریف شده است.. تمامی پورت های سویچ بصورت پیش فرض به این VLAN متصل هستند . ایجاد کردن VLAN باعث میشود سرعت و کارایی سوییچ و شبکه افزایش پیدا نماید و با تفکیک نمودن پورت ها به VLAN های مختلف این کار انجام پذیر می باشد.

```
Switch(config)# interface vlan 1
Switch(config-if)# ip address IP_ADDRESS  NET_MASK
Switch(config-if)# no shutdown                    */ <- active telnet ( shutdown : inactive Telnet)
Switch(config-if)# exit
*/
Switch(config)# interface vlan 1
Switch(config-if)# ip address 192.168.1.1 255.255.255.0
Switch(config-if)# no shutdown                    */ <- active telnet ( shutdown : inactive Telnet)
Switch(config-if)# exit
```

رمزگذاری با سطح امنیتی بالاتر:

اگر در هنگام نمایش حافظه که با دستور show r دقت کرده باشید تمامی رمزهای تعبیه شده برای console و vty قابل مشاهده می باشد و قطعاً ای روش و سطح امنیتی می تواند در آینده ما را با مشکلات جدی روبرو سازد بدین خاطر از سرویس password encryption که به صورت پیش فرض فعال نمی باشد استفاده خواهیم کرد. با انجام این دستور encryption کلاس ۷ فعال می گردد.

```
Switch(config)# enable password PASSWORD
Switch(config)# service password-encription
```

با نمایش و مشاهده حافظه متوجه خواهید شد که دیگر رمزها همانند گذشته خوانا و قابل استفاده نمی باشند. البته این الگوریتم نیز به سادگی و با استفاده از نرم افزارهای موجود در بازار و اینترنت رمز گشایی می شود. پس چه باید کرد ؟

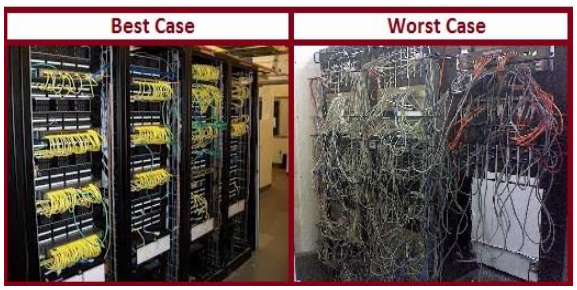
برای رفع این مشکل، سیسکو یک الگوریتم مطمین تر نسبت به الگوریتم سطح ۷ خود ارائه داده است به نام MD5 (Message Digest 5) این الگوریتم هم در آینده نزدیک شاید قابل رمزگشایی باشد ولی در حال حاضر خیلی سخت و دشوار و ناممکن به نظر می رسد. با استفاده از این الگوریتم دیگر نیاری به دستور encryption نخواهیم داشت. چنانچه قبلا رمزگذاری انجام شده باشد الگوریتم MD5 به دلیل ارجح بودن تمامی رمزگذاریهای قبلی را نیز بروزرسانی و تحت پوشش قرار می دهد.

استفاده از خاصیت و سرویس secret برای line vty و line console:

بدلیل عدم وجود دستورات secret در محیط vty و console ابتدا می بایست یک بانک اطلاعاتی database ورودی مشخص کرده و vty و console را به آن معرفی کنیم.

```
Switch(config)# username NAME {secret / password} PASSWORD      */ secret is more secure
Switch(config)# username user1 secret 123456                    */ create database
Switch(config)# line vty 0 15                                   */ Fifteen Terminal is Available to access
Switch(config-line)# login local                                */ use of database
Switch(config-line)# exit
-------------------------------------------------------------------------------
Switch(config)# line console 0
Switch(config-line)# login local                                */ use a link of database
Switch(config-line)# exit
```

راه اندازی Telnet بر روی سوییچ:



امروزه متناسب با رشد و گسترش کمی و کیفی شبکه های کامپیوتری، ارائه سرویسهای عملیاتی و پشتیبانی به منظور حفظ، نگهداری و توسعه پایدار منابع اطلاعاتی و شبکه نیز در درجه بالایی از اهمیت قرار گرفته است. Admin و تیم فنی مجموعه می بایست از هر نقطه امکان پاسخگویی به نیازها و درخواست های مجموعه را داشته باشند. حتی در بهترین شرایط، امکان حضور فیزیکی admin شبکه در سایت، دسترسی به rack و یافتن پورت مورد نظر روی سوییچ مورد نظر با توجه به تعداد سوییچها و اتصالات مربوطه ریسک بالایی را به همراه خواهد داشت.

را متوجه کابل البته در اکثر مواقع برخی مواقع دسترسی به Rack و اتصال کابل به یکی از سوییچها بدین منظور استفاده از سرویسهای موجود و قابل پشتیبانی در IOS سوییچ دسترسی از راه دور از طریق خطوط شبکه و عدم نیاز به حضور فیزیکی در سایت را برای کادر فنی و admin فراهم می سازد. Telnet به صورت پیش فرض بر روی سوییچ فعال نیست و در ابتدا می بایست از طریق Console و انجام تنظیمات مربوطه آن را فعال نمود. پس از آن admin با توجه به نوع تنظیمات انجام شده و زیرساخت شبکه از هر نقطه ای امکان دسترسی به منابع شبکه را خواهد داشت. چنانچه تمرین های بخشهای قبل را بخوبی فرا گرفته باشید هم اکنون به راحتی آماده فعالسازی telnet خواهید بود.

1- Set IP address on vlan
2- Set parameter & configure terminal / terminals
3- Set password to safe access
4- Set IP on Your PC

*/----------

***/ 1**

```
Switch(config)# interface vlan 1
Switch(config-if)# ip address IP_ADDRESS  NET_MASK
Switch(config-if)# no shutdown                                  */ <- active telnet ( shutdown : inactive Telnet)
Switch(config-if)# exit
```

***/ 2**

```
                                                                */ Virtual TeletYpe
Switch(config)# line vty 0 15                                   */ Fifteen Terminal is Available to access
Switch(config-line)# password PASSWORD
Switch(config-line)# login
Switch(config-line)# exit
```

***/ 3**

```
Switch(config)# enable password PASSWORD
```


heydari.farzad@gmail.com نام مدرس دوره: مهندس فرزاد حیدری
تهیه و گردآوری: دانیال نامورکهن

***/1**

```
Switch(config)# interface vlan 1
Switch(config-if)# ip address 192.168.1.1 255.255.255.0
Switch(config-if)# no shutdown                    */ <- active telnet ( shutdown : inactive Telnet)
Switch(config-if)# exit
```

***/ 2**

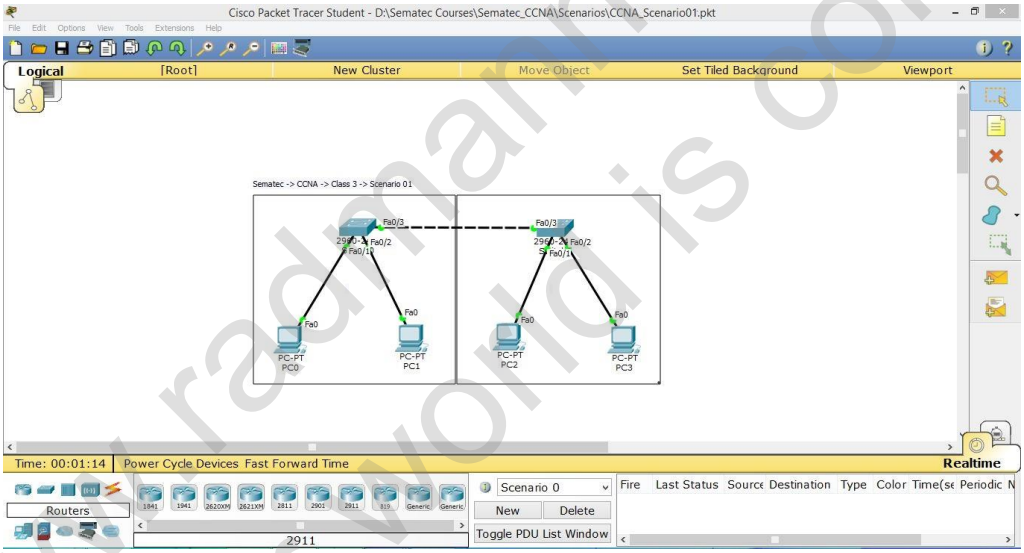
```
Switch(config)# line vty 0 15                     */ Fifteen Terminal is Available to access
Switch(config-line)# password 12345               */ limitation , case sensitive
Switch(config-line)# login
Switch(config-line)# exit
```

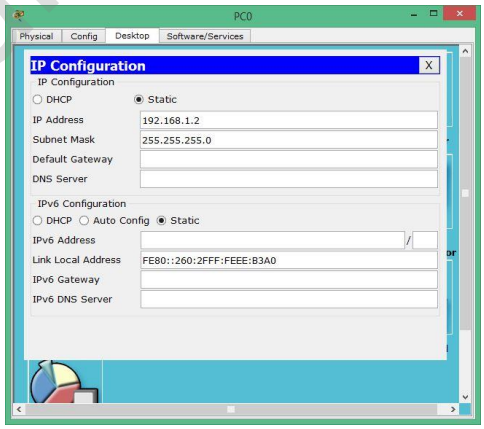
***/ 3**

```
Switch(config)# enable password 67890             */ no limitation , case sensitive
```

در نسخه های قدیمی IOS با انجام تنظیمات vty همزمان ۵ نفر می توانستند از Telnet استفاده نمایند ولی در نسخ جدید ۱۶ نفر به صورت همزمان می توانند از این سرویس استفاده نمایند. به همین دلیل line vty در هنگام خروجی دستور show r به شکل تفکیک شده نمایش داده می شود.

Line vty 0 4
Line vty 5 15





heydari.farzad@gmail.com نام مدرس دوره: مهندس فرزاد حیدری
تهیه و گردآوری: دانیال نامورکهن

آشنایی با پورت های Ethernet سوییچ ونحوه تنظیم آن:

همانطور که در فصل اول اشاره شد، سوییچها از لحاظ شکل ظاهری با مدل های گوناگون و تعداد پورت های (Interfaces) ثابت یا متغیر ، متناسب با نیاز مشتری تولید و مورد استفاده قرار می گیرد. از نظر ماهیتی نیز هر پورت (Interface) گونه های متعددی دارد که در هر سوییچ با توجه به نیاز از یک یا چند نوع آن تعبیه شده است.

انواع سوییچ از لحاظ تعداد پورت

No	Type	Description
1	Fix	تعداد پورتها در این نوع ثابت بوده و امکان کاهش و افزایش وجود ندارد. (13,16,24,48,Daisy-Chaining)
2	Modular	قابلیت اضافه کردن پورت به این نوع از سوییچ ها امکانپذیر می باشد. ۴۵۰۰ و ۶۵۰۰

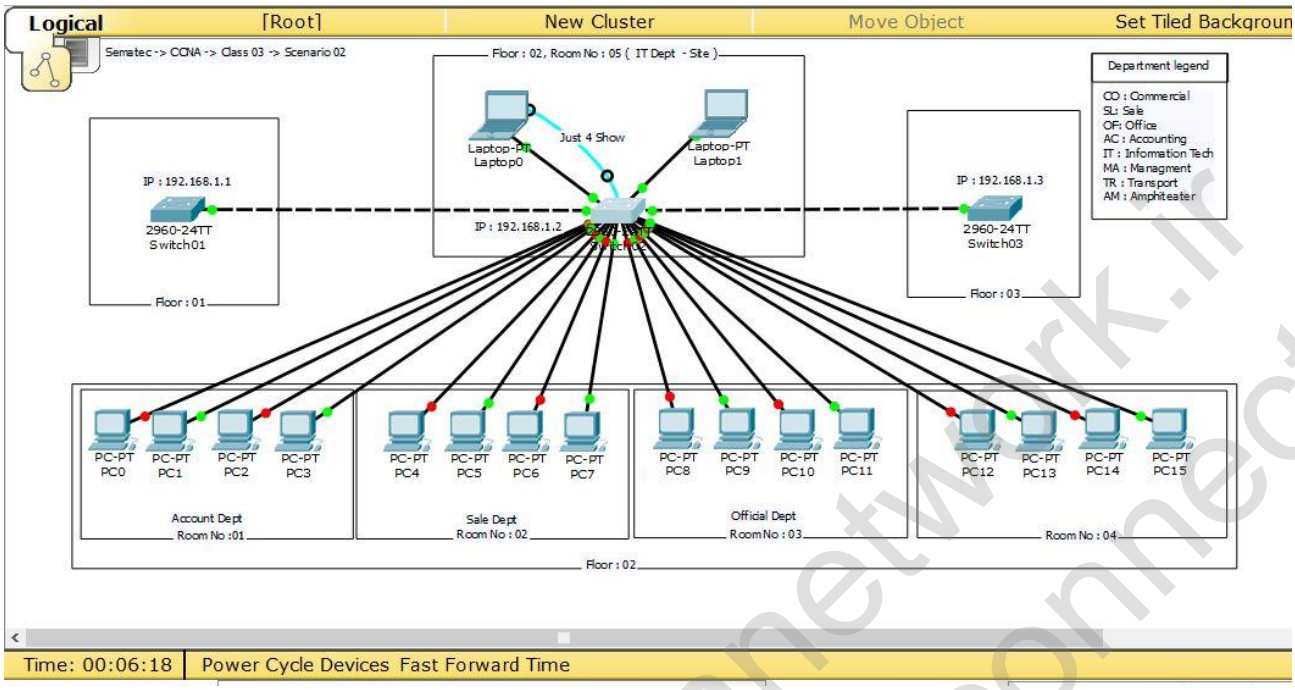
انواع پورت از لحاظ سرعت

No	Interface TYPE	Speed (Mbps)	Module	Number
1	Ethernet	10	0 - n	1 - n
2	Fast Ethernet	100	0 – n	1 - n
3	Gigabit Ethernet	1000	0 - n	1 - n
4	Ten Gigabit Ethernet	10,000	0 - n	1 - n

به هر پورت در سوییچ Interface گفته می شود و به صورت پیش فرض تمامی آنها فعال (no shutdown) می باشند. انجام هر گونه تنظیم روشن / خاموش ، نام گذاری ، اختصاص توضیح و ... می تواند هم به صورت تک و هم به صورت گروهی range صورت پذیرد.

```
Switch(config)# interface TYPE MOD/NUM                    */ Enter to Interface / port
Switch(config-if)# description DESCRIPTION                */ Set description on interface /port
Switch(config-if)# no shutdown                            */ Activate an Interface
Switch(config-if)# shutdown                               */ Deactivate an Interface
*/ Sample
Switch(config)# interface FastEthernet 0/1
Switch(config-if)# description SW1-F01R02-Sale
*/
Switch(config)# interface range TYPE MOD/NUM1-NUM2        */ Enter to a range of Interfaces (Sequential)
*/ Sample
Switch(config)# interface range FastEthernet 0/1-10
*/                                                        */ enter to a range of Interfaces (Random)
Switch(config)# line interface range TYPE MOD/NUM1-NUM2 , TYPE MOD/NUM1-NUM2 , …
*/ Sample
Switch(config-if)# interface range FastEthernet 0/1-5 , range GigabitEthernet 0/1-2
```

- غیر فعال/خاموش کردن Interface (توصیه می شود Interface هایی که از آنها ستفاده نمی شود در وضعیت خاموش قرار گیرند.)



Switch01># show run

```
!
interface FastEthernet0/1
 description F02-AC-R01-N01
 shutdown
!
interface FastEthernet0/2
 description F02-AC-R01-N02
!
interface FastEthernet0/3
 description F02-AC-R01-N03
 shutdown
!
interface FastEthernet0/4
 description F02-AC-R01-N04
!
interface FastEthernet0/5
 description F02-SL-R02-N05
 shutdown
!
interface FastEthernet0/6
 description F02-SL-R02-N06
!
interface FastEthernet0/7
 description F02-SL-R02-N07
 shutdown
!
interface FastEthernet0/8
 description F02-SL-R02-N08
!
interface FastEthernet0/9
 description F02-OF-R03-N09
 --More--
```

فصل سوم

آشنایی با سوییچ – (مفاهیم و اصطلاحات کار با سوییچ) - بخش دوم:

همانطور که می دانید یک شبکه شامل نود (Node) یا ایستگاه کاری ، واسطه های ارتباطی (Wired or wireless) و تجهیزات مخصوص شبکه مانند روتر و سوییچ و هاب ها می باشد. در محیط اینترنت ، تمامی این اجزا با هم کار می کنند تا شما بتوانید اطلاعاتی را از کامپیوتر خود برای کامپیوتر دیگری به آنسوی دنیا بفرستید. سوئیچ ها ، از قسمت های اساسی بیشتر شبکه ها می باشند. دستگاه مذکور این امکان را برای چندین کاربر فراهم می سازد تا در یک زمان واحد از طریق شبکه اطلاعات را برای هم ارسال کنند. سوئیچ ها به نودهای مختلف موجود در شبکه اجازه می دهد مستقیماً و با یک روش آسان و کارآمد به یک نود دیگر متصل شوند. سوییچ هایی که ارتباط مجزایی را برای هر یک از نودهای شبکه ایجاد می کنند به LAN Switches معروف می باشند. زمانیکه قسمت های مختلف در یک شبکه بخواهند با هم صحبت کنند سوئیچ ها وارد عمل می شوند.

روشهای متعدد در شبکه جهت ارسال Packet :

Unicast: در این نوع آدرس دهی انتقال اطلاعات از یک نود به آدرس نود دیگر را unicast می گویند.

Multicast: در آدرس دهیMulticast یک نود ، یک بسته اطلاعاتی را برای گروهی می فرستد که اعضای این گروه بسته های آدرس دهی شده را دریافت می کنند. به طور مثال ممکن است یک روتر Cisco اطلاعات دست اول را به تمامی روترهای Cisco دیگر ارسال دارد.

Broadcast: یک نود بسته اطلاعاتی را برای ارسال به تمامی نودهای موجود در شبکه در نظر گرفته و می فرستند که به این عمل broadcast می گویند.

سوییچ عمل مسیریابی در شبکه را چگونه و به چه روش هایی انجام می رساند؟

همانطور که گفته شد یک سوئیچ می تواند در نحوه برقراری ارتباط بین نودها تغییر اساسی ایجاد کند .سوئیچ ها معمولاً با استفاده از آدرس های MAC در لایه دوم مدل مرجع OSI که دیتا لینک است کار می کند. یکی از ضروری ترین عواملی است که در نحوه کار شبکه دخالت دارد. هرگاه یکی از Node ها بخواهد اطلاعاتی را ارسال کند و گیرنده آن را نشناسد، در این صورت یک Packet اعلان همگانی یا Broadcast به تمامی Node ها ارسال می کند. به طور مثال اگر کامپیوتر جدیدی وارد مجموعه Node های شبکه شود در این صورت توسط یک Packet Broadcast حضور خود را به تمامیNode ها اطلاع می دهد .Hub ها و سوئیچ ها هر بسته اطلاعاتی اعلان همگان (Broadcast Packet) دریافت شده را به تمامی سگمنت های موجود در محدوده اعلان ارسال می کنند .

Packet-Switching :سوئیچ ها بر مبنای Packet-Switching کار می کنند و بین سگمنت هایی که از نظر بعد مکانی از هم به حد کافی دور می باشند، ارتباط برقرار می سازد. بسته های اطلاعاتی وارده در buffer نگهداری می شوند. آدرس های MAC در قسمت هدر فریم نگهداری می شوند. آدرس های مذکور که در این قسمت قرار دارد ، خوانده می شوند و با جدول مک سوئیچ (MAC Table) مقایسه می گردند. همچنین فریم اترنت در یک شبکه LAN قسمتی به نام Payload دارد. که شامل MAC Address مبدا و مقصد می باشد. همانطور که قبلا گفته شد سوئیچ آدرس مک مبدا و مقصد را چک کرده و در صورتیکه آدرس مقصد را در جدول مک آدرس های خود داشت برای مقصد ارسال می کند.

منظور از حافظه بافر در سوئیچ چیست؟

حافظه بافر یک ناحیه ذخیره سازی اختصاص داده شده، برای رسیدگی به داده های عبوری می باشد. بافرها معمولاً برای دریافت و ذخیره سازی اطلاعات پراکنده، که پشت سر هم توسط دستگاه های سریعتر، ارسال می شود را دریافت می کنند و تفاوت سرعت را جبران می نمایند. اطلاعات ورودی ذخیره می شوند تا هنگامی که تمام داده های گرفته شده قبلی فرستاده شوند. این حافظه در سوئیچ به اشتراک گذارده می شود.

۱- **سوئیچ های Packet-based** برای تعیین مسیر ترافیک از یکی از سه روش زیر استفاده می کند:

- Cut-through
- Store-and-forward
- Fragment-free

Cut-through: در این روش ، سوئیچ آدرس های MAC را به محض دریافت بسته می خواند و سپس ۶ بایت MAC اطلاعات مربوط به آدرس را ذخیره کرده و با وجود اینکه ما بقی بسته ها در حال رسیدن به سوئیچ می باشند ، اقدام به ارسال بسته مذکور به سمت Node مقصد می نماید.

Store-and-forward: سوئیچی که از این روش استفاده می کند ، ابتدا تمام اطلاعات داخل بسته را دریافت و نگهداری می کند و قبل از ارسال بسته مورد نظر به دنبال خطای CRC (Cyclic redundancy Check) و یا مشکلات دیگر می گردد. در صورتی که بسته دارای خطایی باشد آن بسته را کنار می گذارد. در غیر اینصورت سوئیچ آدرس کارت شبکه گیرنده را جستجو کرده و سپس آن را برای Node مقصد ارسال می دارد.

بیشتر سوئیچ ها همزمان از دو روش فوق استفاده می کنند مثلاً ابتدا از روش Cut-through استفاده کرده ولی به محض برخورد با یک خطا ، روش خود را تغییر می دهد و به شیوه Store-and-forward عمل می کند ، از آنجائیکه روش Cut-through قادر به اصلاح خطا نمی باشد در نتیجه سوئیچ های کمتری از این روش استفاده می کنند ولی از سرعت بالاتری برخوردار است.

Fragment-free: سوئیچ ها از این روش کمتر استفاده می کنند. این روش مانند روش اول می باشد با این تفاوت که در این شیوه ، سوئیچ قبل از ارسال بسته ، ۶۴ بایت اول آن را نگه می دارد این کار به خاطر آن است که بیشتر خطا و برخوردها در طول اولین ۶۴ بایت بسته اطلاعاتی اتفاق می افتد.

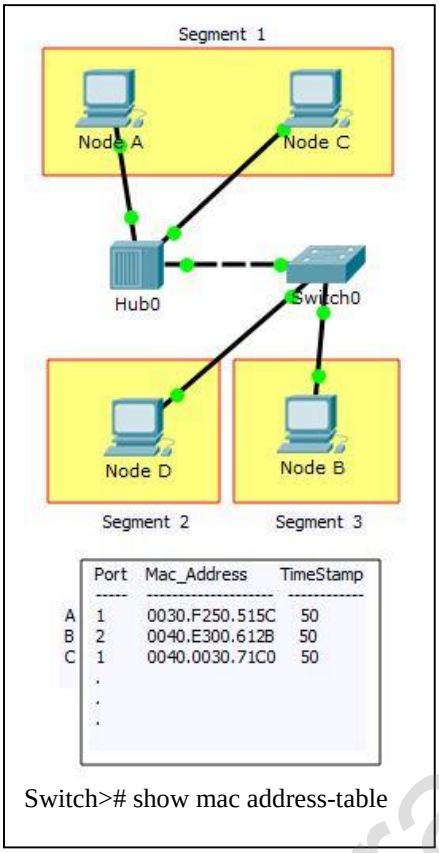
۲- **Switch Configurations** : سوئیچ های LAN از نظر شکل فیزیکی با هم متفاوتند ، در حال حاضر ، سوئیچ ها دارای سه شکل عمده می باشند :
Shared memory: این نوع از سوئیچ ها ، بسته رسیده را در یک حافظه مشترک یا buffer نگهداری می کند. این buffer در بین تمامی درگاه های سوئیچ تقسیم می شود نگهداری می کنند و سپس Packet را از طریق درگاه مناسب برای سمت Node مقصد ارسال می کنند.
Matrix: این نوع سوئیچ ها دارای یک شبکه خطوط داخلی (ماتریکس) با پورت های ورودی و خروجی می باشند. زمانیکه وجود یک بسته اطلاعاتی در پورت ورودی تشخیص داده شود ، آدرس کارت شبکه (MAC) با جدول جستجوی موجود در سوئیچ(MAC Table) مقایسه می شود تا در نهایت بسته مذکور به پورت خروجی مورد نظر هدایت شود. بنابر این سوئیچ در حد فاصل بین این دو پورت یک خط ارتباطی ایجاد کرده و آن دو پورت را به هم متصل می کند.
Bus Architecture: در این دسته از سوئیچ ها یک بافر برای هر یک از درگاه ها در نظر گرفته شده است. که گذرگاه اطلاعات را کنترل می کند.

۳- **Transparent Bridging:** اکثر سوئیچ ها از سیستمی موسوم به Transparent Bridging استفاده می کنند تا جداولی جهت جستجوی آدرس بسازند. سیستم مذکور یک تکنولوژی می باشد که امکان می دهد تا سوئیچ همه آنچه که در مورد موقعیت Nodeها در شبکه باید بداند را بدون دخالت مدیر شبکه (network administrator) می آموزند. این سیستم دارای پنج قسمت زیر می باشد :

- Learning
- Flooding
- Forwarding
- Filtering
- Aging

حال قدم به قدم با مراحل فوق آشنا می شویم: همانطور که در شکل ۳ مشاهده می کنید سوئیچ به شبکه اضافه شده است و سگمنت های مختلف به آن متصل هستند.

Learning: کامپیوتر A که در سگمنت ۱ قرار دارد ، اطلاعاتی برای کامپیوتر B واقع در سگمنت ۳ ارسال می کند. پس سوئیچ اولین بسته اطلاعاتی را از روی Node A دریافت می کند. آدرس کارت شبکه یا MAC Address آن را می خواند و آن را در جدول مک خود به ثبت می رساند. از این پس سوئیچ به محض دریافت یک بسته اطلاعاتی که آدرس مقصد دستگاه ، Node A آدرس دهی شده باشد می تواند Node A را با توجه به آدرس موجـود بیاید. به این عملیات Learning می گویند. یعنی به محض دیدن یک MAC Address جدید سوییـچ آن را یادداشت می کند و آن را یاد می گیرد.



Switch># show mac address-table

Flooding: با توجه به اینکه سوئیچ ، مک آدرس Node B را نمی شناسد، یک بسته که به اصطلاح به آن Unkown Unicast گفته می شـود را را به تمـامی سگمنت ها به استثنـای سـگمنت ۱ می فرستد. هرگاه سوئیچ برای یافتن یک Node مشخص بسته را به تمامی سگمنت ها بفرستد در اصطلاح به این عمل Flooding می گویند.

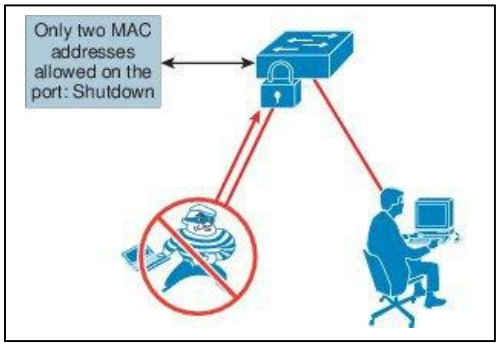
Forwarding : در این مرحله بسته را دریافت کرده و بسته ای را برای شناسایی به سمت Node Aمی فرستد. بسته ارسالی از سوی Node B به سوئیچ می رسد و سوئیچ نیز آدرس کارت شبکه Node Bرا به لیست MAC Table خود در سگمنت ۳ اضافه می کند. از آنجائیکه سوئیچ ، آدرس Node A را از قبل می داند در نتیجه بسته را مستقیماً به Node A می فرستد. چون سگمنتی که Node Aمتعلق به آن است با سگمنتی که Node B به آن تعلق دارد با هم متفاوت می باشند. در نتیجه سوئیچ می باید این دو سگمنت را به هم مربوط سازد و سپس اقدام به ارسال بسته نماید که به این عمل Forwarding می گویند. بسته دیگری از سوی Node A به سمت Node B ارسال می گردد، بسته ابتدا به سوئیچ می رسد، سوئیچ نیز آدرس Node B را می داند و بسته را مستقیماً به Node Bمی فرستد.

Filtering: Node C اطلاعاتی را برای Node A می فرستد. آدرس Node C به سوئیچ نیز از طریق HUB، ارسال می شود و سوئیچ آدرس Node C را نیز به لیست آدرس های خود در سگمنت A اضافه می کند. پیش از این ، سوئیچ آدرس مربوط به Node A را می دانست و مشخص می سازد که این Node ها A و C هر دو در یک سگمنت مشابه قرار دارند ، پس برای ارسال اطلاعات از Node C به Node A دیگر نیازی نیست تا سوئیچ سگمنت۱ را با سگمنت دیگری مرتبط سازد. بنابراین سوئیچ در حین انتقال اطلاعات بین Node های درون یک سگمنت عکس العملی از خود نشان نمی دهد که به این عمل Filtering می گویند.

Aging: مراحل learning وFlooding ادامه می یابد تا اینکه سوئیچ مک آدرس تمامی Node ها را به لیست خود اضافه کند. بیشتر سوئیچ ها برای نگهداری لیست آدرس ها از حافظه زیادی برخوردارند. اما برای استفاده بهتر از این حافظه سوئیچ آدرس های قدیمی را از جدول پاک می کند و برای جلوگیری از اتلاف وقت در آدرس های قدیمی به دنبال آدرسی نمی گردد. برای انجام این کار از تکنیکی موسوم به Aging بهره می گیرد. اساساً وقتی اطلاعات یک Node وارد جدول سوئیچ می شود یک Timestamp در مقابل آن اطلاعات نوشته می شود و با دریافت هر بسته اطلاعاتی دیگر، آن بر چسب زمان(Timestamp) به روز می شود. سوئیچ دارای قابلیتی است که پس از مدتی در صورت عدم فعالیت Node، اطلاعات مربوط به آن را پاک می کند. این قابلیت باعث میشود تا فضای قابل توجهی از حافظه برای اطلاعات و پکت های دیگر اختصاص داده شود.

در نمونه ای که ملاحظه کردید، دو Node A و Node C یک سگمنت را بین خود تقسیم می کنند حال آنکه سوئیچ برای هر یک از Node های B و D یک سگمنت مستقل میسازد. در یک شبکه ایده آل LAN-Switched هر یک از Node ها دارای یک سگمنت جداگانه می باشد که خصیصه مذکور ، احتمال برخورد بین بسته های اطلاعاتی و همچنین نیاز به فیلترینگ را حذف می کند.

ایجاد تدابیر امنیتی بر روی پورت های سوییچ (Port Security)



در طراحی یک شبکه ، در نظر گرفتن مباحث امنیتی آن دارای اهمیت ویژه است چون در زمان حمله ، شبکه دچار مشکلاتی مختلفی مانند از کار افتادن بخشی یا کل شبکه ، افشاء اطلاعات محرمانه سازمان ، دستکاری در اطلاعات و ... می شود. برای جلوگیری از بروز این حملات ما باید طرح و برنامه درستی برای شبکه خود در نظر بگیریم.

یکی از مسائل در حال رشد که امروزه مدیران شبکه با آن برخورد می‌کنند نحوه کنترل دسترسی افراد به شبکه داخلی سازمانشان می‌باشد. به عنوان مثال آیا هر شخصی می‌تواند وارد سازمان شده، laptop خود را به پریز شبکه متصل کرده و به شبکه داخلی دسترسی داشته باشد؟ ممکن است جواب شما به این پرسش این باشد که هر پریز شبکه روی دیوار به سوئیچ متصل نیست. ولی اگر شخصی کابل اترنت را از PC در حال کاری جدا کند و به شبکه متصل شود چطور؟ شاید این سناریو غیر ممکن به نظر بیاید ولی این اتفاق بارها در سازمان‌های مختلف پیش آمده است. مسئله‌ای که بیش از هرچیز در این مورد نگران کننده است ویروس‌ها و wormهای مختلفی است که PC شخص غیر مجاز متصل شده به شبکه ممکن است داشته باشد. Switchport security برای حل این مشکل به شما کمک می‌کند. در ادامه به بررسی ویژگی‌های Cisco"s Port Security خواهیم پرداخت.

Port Security یکی از خصوصیتهای کنترل ترافیک لایه ۲ در سوئیچهای Catalyst سیسکو می باشد. دلیل استفاده از Port Security این است که به شما این امکان را میدهد که به تعداد خاصی از آدرسهای مک مبداء اجازه ورود به پورت رابدهید. در ساده‌ترین حالت Port Security آدرس MAC متصل به پورت سوئیچ را به خاطر می‌سپارد و فقط به همان آدرس MAC اجازه برقراری ارتباط با پورت سوئیچ را می‌دهد. اگر آدرس MAC دیگری بخواهد از طریق همان پورت به شبکه متصل شود، پورت مذکورغیرفعال می‌شود. اکثر اوقات مدیران شبکه سوئیچ را طوری تنظیم می‌کنند که یک SNMP trap به سیستم مانیتورینگ مبنی بر غیر فعال شدن یک پورت به دلایل امنیتی فرستاده شود.

اگر چه پیاده‌سازی راه‌حل های امنیتی همیشه شامل یک trade-off می‌باشد و لی این کاهش سهولت در مقابل افزایش امنیت سیستم می‌باشد. وقتی شما از Port Security استفاده می‌کنید می‌توانید از دسترسی دستگاه‌های مختلف به شبکه جلوگیری کنید و این امر موجب افزایش امنیت می‌شود. ولی از طرف دیگر فقط مدیر شبکه است که می‌تواند پورت را فعال کند و این امر در جایی که به دلایل مجاز قرار به تغییردستگاه‌ها باشد ایجاد مشکل می‌کند.

با وارد کردن ابتدایی‌ترین دستور، تنظیمات پیش فرض که اجازه دسترسی فقط به یک آدرس MAC (آدرس دستگاهی که اولین بار به پورت سوئیچ وصل شده است.)می‌باشد، اعمال می‌گردد. و در صورتی که دستگاه دیگری بخواهد با آن پورت ارتباط برقرار کند، پورت سوئیچ خاموش می‌شود. ولی قطعاً تنظیمات پیش فرض مد نظر شما نمی‌باشد.

```
Switch(config)# interface {range} TYPE MOD/NUM or NUMs
Switch(config-if)# switchport mode access                                   */ set port to access mode
Switch(config-if)# switchport port-security                                 */ open port
Switch(config-if)# switchport port-security mac-address {MAC_ADDRESS | sticky}      */set MAC
Switch(config-if)# switchport port-security maximum MAX_NO                  */ MAX_NO : 1- 132
Switch(config-if)# switchport port-security violation < shutdown | restrict | protect >      */ defaut :shutdown
Switch># show port-security
Switch># show port-security address
*/
Switch(config-if)# switchport port-security 0001.96D7.7026                  */set MAC
Switch(config-if)# switchport port-security maximum 4                       */se Max_NO
```

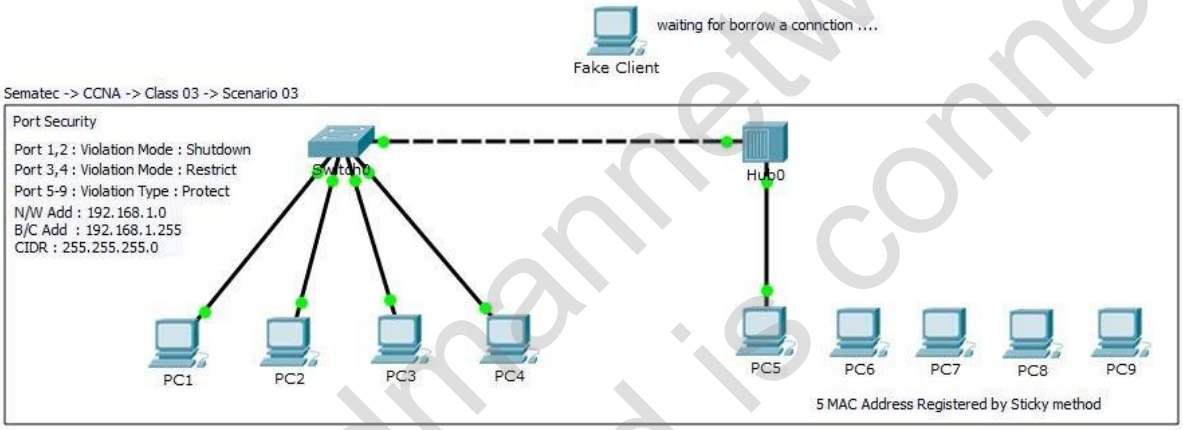

heydari.farzad@gmail.com نام مدرس دوره: مهندس فرزاد حیدری
تهیه و گردآوری: دانیال نامورکهن

- **Mac_Address**: با بدست آوردن Mac-Address یا Physical Address کامپیوتر خود با استفاده از دستور ipconfig /all و وارد نمودن آن، به پورت اعلام می کنید که به جز این آدرس، Mac-Address دیگری امکان استفاده از این پورت اختصاصی را ندارد.
- **Sticky**: با اعمال این تنظیم، به محض اینکه اولین دستگاه به این پورت متصل شود MAC آن در حافظه پورت ذخیره می گردد.
- **Max_NO** : تعداد حافظه هایی که برای ذخیره MAC-Address ها در هر پورت تعیین می گردد. به عبارت ساده تر تعداد دستگاههای که می توانند از این پورت سوییچ استفاده نمایند.
- **Violation**: به منظور تعیین واکنش به خطای ایجاد شده بر روی پورت از یکی از گزینه های موجود این دستور استفاده می شود.

Shutdown: (پیش فرض): اینترفیس در حالت error-disabled قرار میگیرد و تمام ترافیک ورودی را بلاک میکند. برای خروج پورت از این وضعیت باید پورت را shutdown و سپس no shutdown نمود.

Restrict: فریم هایی که از مک آدرس بدون مجوز برسد را حذف میکند و دسترسی متوقف می گردد همراه با ثبت Violation syslog message

Protect: فریم هایی که از مک آدرس بدون مجوز برسد را حذف میکند و دسترسی متوقف می گردد و بدون ثبت Violation syslog message




```
Switch01#show port-security
Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security Action
               (Count)       (Count)       (Count)
---------------------------------------------------------------------
        Fa0/1         1             1             0         Shutdown
        Fa0/2         1             1             0         Shutdown
        Fa0/3         1             1             0         Restrict
        Fa0/4         1             1             0         Restrict
        Fa0/5         5             5             0          Protect
---------------------------------------------------------------------
Switch01#
Switch01#show port-security address
                Secure Mac Address Table
---------------------------------------------------------------------------
Vlan    Mac Address       Type                  Ports           Remaining Age
                                                                  (mins)
----    -----------       ----                  -----           -------------
1       000C.CF60.D11D  SecureConfigured        FastEthernet0/1         -
1       0001.C766.577B  SecureConfigured        FastEthernet0/2         -
1       00D0.BA06.8DB2  SecureConfigured        FastEthernet0/3         -
1       00E0.8F65.C81A  SecureConfigured        FastEthernet0/4         -
1       0006.2AD5.7BE8  SecureSticky            FastEthernet0/5         -
1       000C.8517.513B  SecureSticky            FastEthernet0/5         -
1       0030.F2B6.1664  SecureSticky            FastEthernet0/5         -
1       0060.4768.9972  SecureSticky            FastEthernet0/5         -
1       00D0.D385.61B3  SecureSticky            FastEthernet0/5         -
---------------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 4
Max Addresses limit in System (excluding one mac per port) : 1024
Switch01#
```

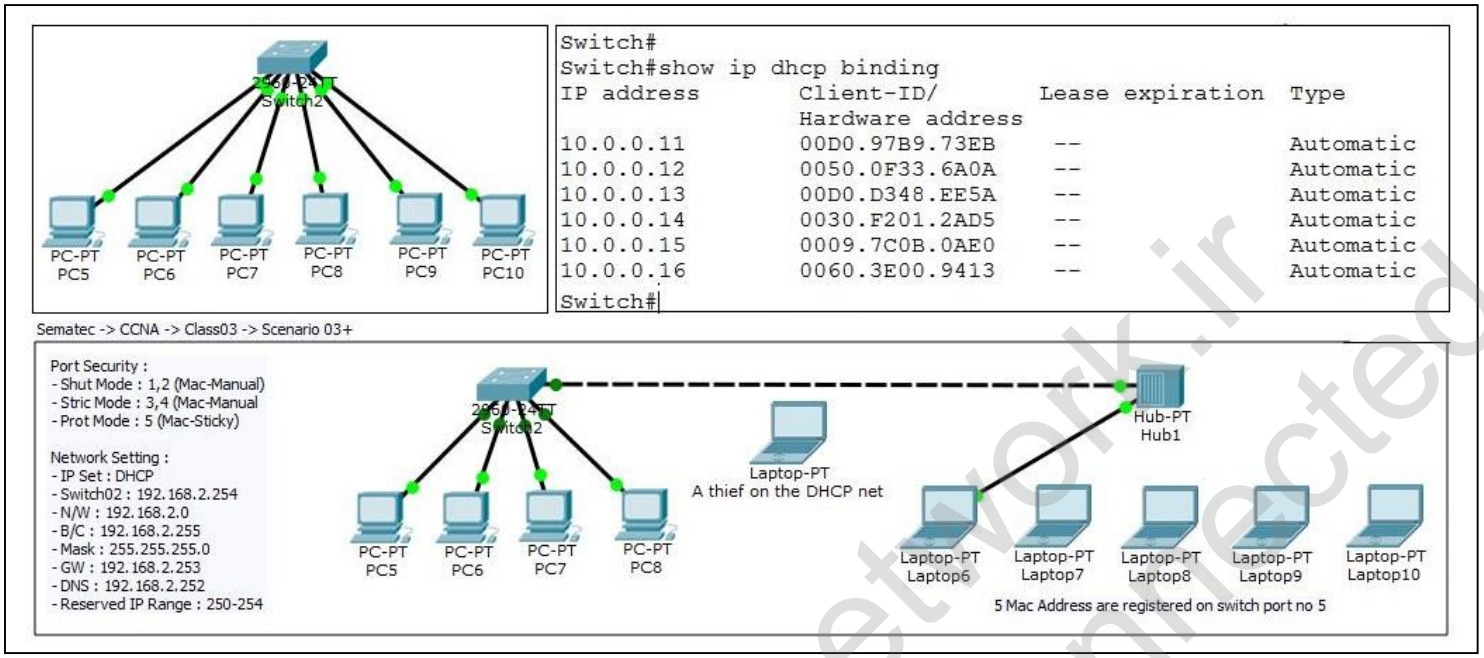
آشنایی و پیاده سازی DHCP (Dynamic Host Configuration Protocol):

DHCP یکی از پر کاربرد ترین سرویس های شبکه است که در خفا و پس زمینه مسئول اختصاص آدرس های IP به کلاینت های شبکه است ، این سرویس جزء لاینفک شبکه های بزرگ و کوچک بوده و از ابتدایی ترین تراکنش های ارتباطی در شبکه های LAN است. هنگامی که شما یک کلاینت را به یک شبکه مرتبط میکنید و یا با یک سرور / سوییچ ارتباط برقرار میکنید ، پس از احراز هویت ، دریافت آدرس IP از ابتدایی ترین واکنش هاست. استفاده از DHCP علاوه بر افزایش کارایی شبکه به افزایش چشمگیر امنیت در شبکه های مبتنی بر سیسکو می انجامد. بدین ترتیب که به عنوان یک مدیر شبکه امکان مدیریت و رصد مشکلات به سادگی امکان پذیر است ، و همچنین از مشکلاتی نظیر IP Conflict ، خطای انسانی و دسترسی غیر مجاز به آدرس های IP جلوگیری به عمل می آید. پیاده سازی DHCP بر روی روتر ها و سوییچ های سیسکو به سادگی امکان پذیر بوده و ترافیک و بار (load) چندانی را به دستگاه تحمیل نمی نماید.

- نکته : به سوییچ باید Static IP داشته باشد تا در صورت هر بار خاموش و روشن شدن سوییچ IP آن تغییر ننماید.

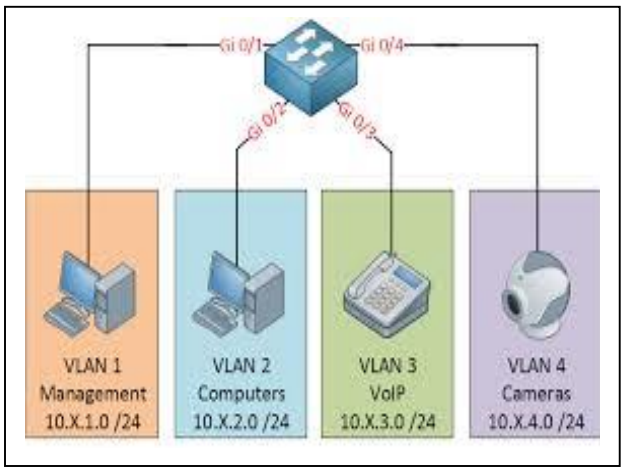
۱- اختصاص IP به سوییچ
۲- تعیین و مجزا نمودن یک محدوده IPs برای مصارف خاص
۳- اختصاص یک نام برای شبکه DHCP مورد نظر
۴- اختصاص Net_ID و Net_Mask شبکه
۵- اختصاص IP به Default Gateway
۶- اختصاص IP به DNS
۷- نمایش و مشاهده نتیجه تنظیمات

```
Switch(config)# interface vlan 1
Switch(config-if)# ip address IP_ADDRESS NET_MASK                    */ 1
Switch(config-if)# no shutdown
Switch(config-if)# exit
*/
Switch(config)# ip excluded-address START_IP_ADDRESS END_IP_ADDRESS          */ 2
*/
Switch(config)# ip dhcp pool POOL_NAME                               */ 3
Switch(dhcp-config)# network NET_ID NET_MASK                         */ 4
Switch(dhcp-config)# default-router IP_ADDRESS                       */ 5
Switch(dhcp-config)# dns-server IP_ADDRESS                           */ 6
Switch(dhcp-config)# ctrl+z
Switch# show ip dhcp binding                                         */ 7
-----------------------------------------------------
Switch(config)# interface vlan 1
Switch(config-if)# ip address 10.0.0.1 255.255.255.0                */ 1
Switch(config-if)# no shutdown
Switch(config-if)# exit
*/
Switch(config)# ip excluded-address 10.0.0.1 10.0.0.10               */ 2
*/
Switch(config)# ip dhcp pool First_LAN                               */ 3
Switch(dhcp-config)# network 10.0.0.0 255.255.255.0                  */ 4
Switch(dhcp-config)# default-router 10.0.0.2          */ 5 – Choose IP from exclude range
Switch(dhcp-config)# dns-server 10.0.0.3              */ 6 – Choose IP from exclude range
```



فصل چهارم

Virtual LAN در سوییچ ونحوه تنظیم آن – بخش دوم



ەمانطور که در بخش یک اشاره گردید، در واقع vlan این امکان را می دهد که کامپیوتر های متصل به سوییچ را به شکل منطقی در گروه های مختلفی قرار دهیم. هر گروه دارای حوزه های Broadcast جداگانه می باشدو ترافیک شبکه ها را از هم جدا می باشد.

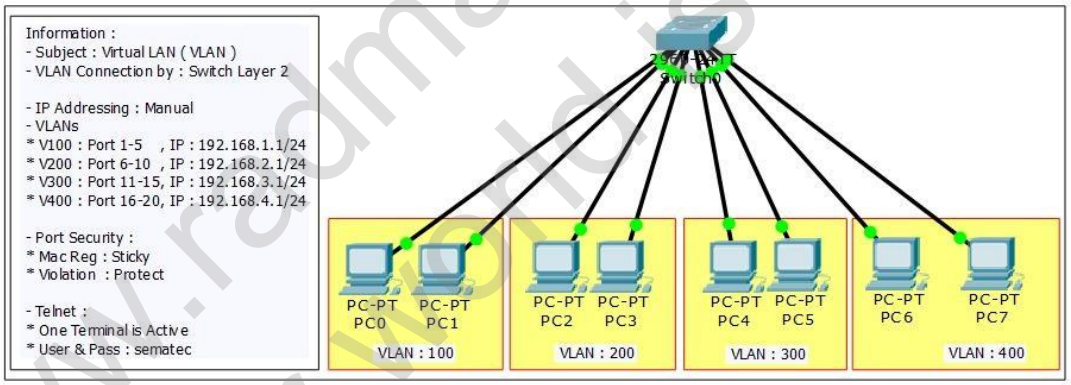
چه تعداد VLAN می توانیم داشته باشیم : در عمل چندین رنج VLAN وجود دارد. رنجهای VLAN بین ۰ تا ۴۰۹۵ میباشد که فقط برای استفاده سیستم رزرو شده است.به غیر از VLAN 1 که به عنوان VLAN پیش فرض در نظر گرفته شده است که شما نمی توانید آن را حذف یا ویرایش کنید .موضوع مهمی که باید بدانید این است که شما میتوانید VLAN پیش فرض خود را در سوئیچ تغییر دهید بنابرین نمیتوانیم به این عبارت بسنده کنیم که VLAN 1 همیشه VLAN پیش فرض است. VLAN های رنج ۲ تا ۱۰۰۱ VLAN های هستند که شما به صورت عادی از این رنج میتوانید استفاده کنید. VLAN های رنج ۱۰۰۲ تا ۱۰۰۵ برای FDDI و token ring رزرو شده است که نمیتوانیم آنها را حذف کنیم.در آخر رنج ۱۰۰۶ تا ۴۰۹۴ به عنوان VLAN های توسعه یافته (extended VLANs) شناخته میشوند که بصورت معمولی قابل استفاده نیست.

VLAN_ID	Name	Description
1	Default VLAN	Configurable – Not Removd
2 - 1001	Normal VLAN – (Free)	Manageable by user
1002 - 1005	FDDI – Token Ring	Expired
1006 - 4094	Extended VLAN	Reserved for

Vlan کمک می کند که ما یک شبکه برزگ را به چند تا شبکه کوچک تر تقسیم کنیم. هر vlan در یک broadcast domain جدید کمک میکند تا از توفانهای broadcast جلوگیری کنیم. ترافیک های ناشناخته MAC unicast یک مشکل در شبکه های بزرگ می باشد جای که سوئیچ ها فرستنده Packet را نمیشناسند و به همین خاطر Packect ها را بر روی همه پورت ها میفرستند یا اصطلاحاً flood میکنند. حل این مشکل به راحتی و با طراحی کردن vlan امکانپذیر می باشد. با توجه به آموخته های قبلی در ساخت و معرفی VLAN 1 در برقراری ارتباط از طریق Telnet مراحل زیر جهت ایجاد و تنظیم VLAN ارائه می شود :

۱. ایجاد VLAN و اختصاص نام به آن
۲. اختصاص پورت یا پورتها به VLAN مورد نظر (راه میانبر : می توان مرحله ۱ را انجام نداد و در این مرحله ایجاد VLAN و اختصاص پورت به VLANرا همزمان به عمل آورد و نامگذاری VLAN_ID را به زمان بعد موکول کرد.)
۳. نمایش و مشاهده تنظیمات و پورت ها

```
Switch(config)# vlan VLAN_ID                          */ 1 - Create VLAN
Switch(config-vlan)# name VLAN_NAME                   */ 1 - Set VLAN Name (Default VLANxxxx)
Switch(config-vlan)# exit
*/
Switch(config)# interface {range} TYPE MOD/NUM | NUMs
Switch(config-if)# switchport access vlan VLAN_ID     */ 2- Set port/ports into vlan_id |.
                                                      */ 2- create VLAN in short way with Default Name: VLAN0003
Switch(config-if)# exit
*/
Switch># show vlan brief                              */ It shows: VLAN_ID , VLAN_NAME, STATUS, PORTS
Switch># show run
*/----------------------------------------
Switch(config)# vlan 10                               */ 1 - Create VLAN
Switch(config-vlan)# name Cisco-V10                   */ 1 - Set VLAN Name
Switch(config-vlan)# exit
*/
Switch(config)# interface range FastEthernet 0/1-5
Switch(config-if)# switchport access vlan 10          */ 2 - Set port/ports into vlan_id
Switch(config-if)# exit
```




```
Switch01>
Switch01>show vlan brief

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                                 Gig0/1, Gig0/2
100  100                               active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                 Fa0/5
200  200                               active    Fa0/6, Fa0/7, Fa0/8, Fa0/9
                                                 Fa0/10
300  300                               active    Fa0/11, Fa0/12, Fa0/13, Fa0/14
400  400                               active    Fa0/15, Fa0/16, Fa0/17, Fa0/18
                                                 Fa0/19, Fa0/20
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
Switch01>
```

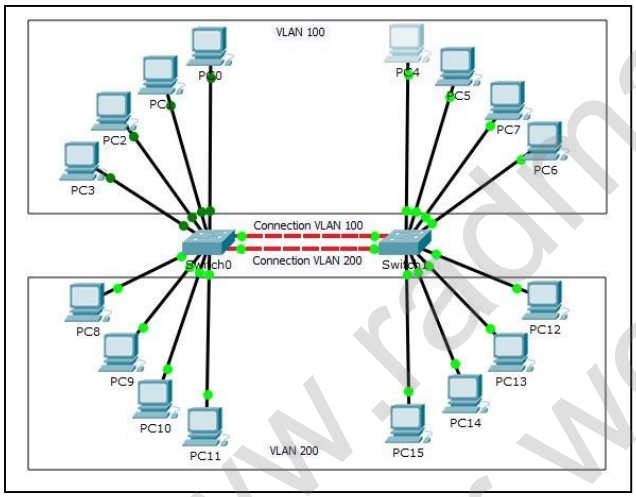
حذف VLAN

چنانچه نیاز به حذف VLAN های ایجاد شده داشته باشید، ابتدا می بایست پورت ها را از VLAN خارج نمایید (حذف کنید) و سپسVLAN را حذف کنید در غیر اینصورت پورت هایی که داخل VLAN استفاده شده است غیرفعال (Deactive) می شود و یا اصطلاحاً گم می شود و حتی در خروجی دستور show vlan brief هم قابل مشاهده نخواهند بود. در صورت فراموش نمودن VLAN_ID می توان با دستور show run و مشاهده پورت ها اطلاعات مورد نیاز جهت خارج نمودن پورتها را از VLAN مربوطه بدست آورد. مراحل صحیح حذف پورت یا پورتها از VLAN حذف VLAN طبق دستورا زیر می باشد.

```
*/
Switch(config)# interface {range} TYPE MOD/NUM | NUMs
Switch(config-if)# no switchport access vlan VLAN_ID      */ 1- Erase port/ports from vlan_id |.
Switch(config-if)# exit
*/
Switch(config)# no vlan VLAN_ID                           */ 2 - Remove VLAN
```

اتصال دو سوییچ یا سوییچ ها به همدیگر – ارتباط VLAN ها با پورت Trunk

پورت Trumk در واقع پورت یا پورت هایی از سوئیچ است که امکان ارتباط سوئیچ های مختلف را با یکدیگر فراهم می آورد. این پورت کلیه ترافیک هایی را که از VLAN های مختلف ایجاد می شود به خارج منتقل می کند. یک پورت می تواند به عنوان ترانک در یک سوئیچ تعریف گردد. نحوه تنظیم این پورت سوئیچ ترانک را بر مبنای پروتکل ۸۰۲,۱q بیان می شود.



فرض کنید دو سوییچ دارید که ۵ پورت اول هر کدام را به VLAN 100 اختصاص داده اید و ۵ پورت دوم سوییچ ها را به VLAN 200، این VLAN ها نیاز به تبادل اطلاعات مابین هم دارند. ساده ترین شکل برای حل این مشکل تهیه یک کابل و اختصاص دادن یکی از ۵ پورت هر سوییچ جهت برقراری VLAN ها با هم است. ارتباط برقرار خواهد شد و VLAN ها می توانند ابا هم تبادل اطلاعان داشته باشند ولی این روش بک مشکل دارد ؟!؟

اگر چند VLAN داشته باشیم باید به ازای هر VLAN یک کابل ارتباطی استفاده کنیم. اینجا هم کابل و هم پورت ها به صورت نادرستی از مورد استفاده قرار می گیرند. جهت رفع این مشکل باید از Trunk (شاه سیم، صندوق) استفاده گردد. Trunk فقط ترافیک بین VLAN ها را حمل و به عهده دارد و با چیز دیگری کار ندارد. همانند صندوق عقب اتومبیل، کاری به محتویات آن نداریم، اتومبیل فقط آن محموله را حمل می کند. در صورتیکه پورت Trunk ساخته نشده باشد، دستور زیر هیچ خروجی نخواهد داشت. در استفاده از قابلیت Trunk فقط یک پورت به ازای هر سوییچ وظیفه اتصال و تبادل اطلاعات را بهعده خواهد گرفت.

```
Switch># show interface trunk
```

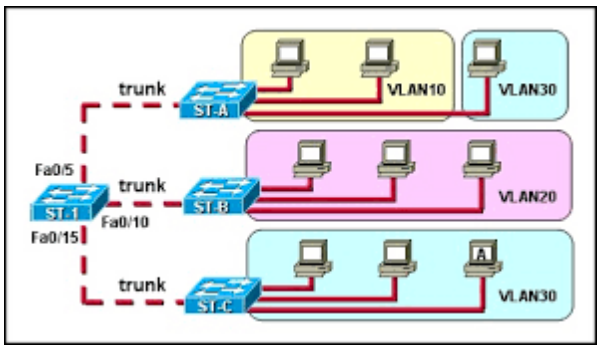
طریقه ساخت پورت Trunk بر روی Interface یا پورت مورد نظر

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

- به دلیل اینکه Trunk Port وظیفه حمل ترافیک را بعهده دارد معمولاً استفاده از پورت های Gig (سرعت بالاتر) توصیه می شود.

heydari.farzad@gmail.com نام مدرس دوره: مهندس فرزاد حیدری
تهیه و گردآوری: دانیال نامورکهن

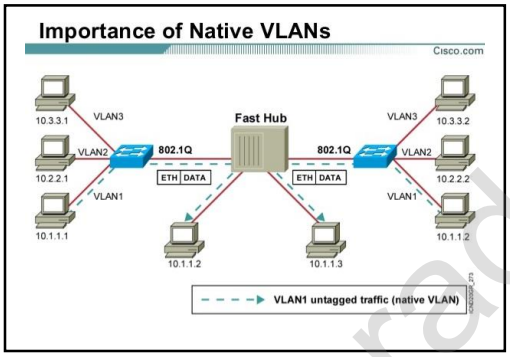
پروتکل های مورد استفاده در Trunk



سوییچ ها از طریق یک Tag متوجه می شوند که کدام بسته برای کدام VLAN است و از کدام پورت می آید. دو پروتکل برای انجام عملیات tag گذاری در سوییچ تعبیه شده اند.

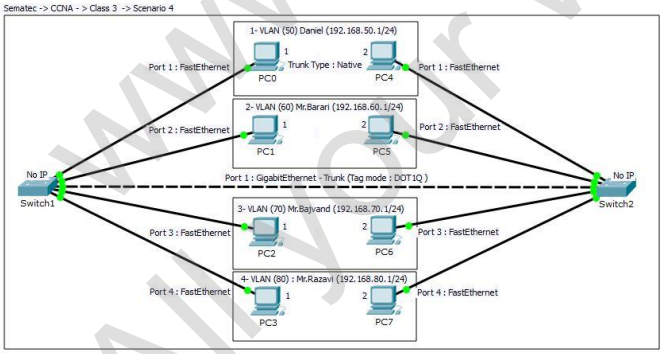
- ISL: این پروتکل مخصوص سیسکو است (Cisco Proprietery) و به دلیل اینکه سایز هر کدام از Tag بسته های آن ۳۰ بایت بود و باعث ایجاد ترافیک و Oevrhead در شبکه می شد، دیگر کمتر مورد استفاده قرار می گیرد.
- DOT1q یا (802.1q): این پروتکل به صورت همگانی است و سایز Tag بسته های آن ۴ بایت است.
- توضیح اینکه قبل از اینکه پورت Trunk را راه اندازی کنیم باید نوع پروتکل مورد استفاده را مشخص شود. انجام این کار در سوییچ هایی که هر دو پروتکل را پشتیبانی می کنند الزامیست. (CISCO Model: 3650)

Switch(config-if)# switchport trunk encapsulation {<dot1q> | <isl>}



Native VLAN: در مجموعه ها و شبکه هایی که تعداد دستگاه ها زیاد است، Admin شبکه می تواند با دریافت گزارشات آماری از ترافیک شبکه و بررسی آنها مشخص نماید که کدام VLAN حجم بیشتری از ترافیک شبکه را به خود اختصاص داده است. به منظور تسریع در تبادل بسته های این VLAN و کاهش ترافیک شبکه، Admin می تواند با استفاده از Native VLAN به این پروتکل اعلام نماید تا Tag گذاری بر روی بسته های این VLAN را متوقف نماید (UnTag). طبعاً فقط یک VLAN از VLAN های موجود در شبکه قادر به استفاده از این سرویس خواهد بود. تنظیم برای بهره مندی از این سرویس می بایست بر روی تمامی سوییچ ها صورت پذیرد. بدیهی است اجرای این دستور بر روی interface منتخب برای Trunk انجام خواهد شد.

Switch(config-if)# switchport trunk native vlan VLAN_ID



- نکته : پروتکل ISL از Native VLAN پشتیبانی نمی کند.

هشدار : وقتی یک VLAN را Native کرده باشیم احتمال نفوذ یک هکر وجود دارد بدین شکل که وی VLAN بدون Tag را یافته و یک بسته اضافه می کند سپس سوییچ ها بسته را به مقصد مورد نظر می رسانند.

فصل پنجم

مدیریتVLAN ها بر روی پورت Trunk

به صورت پیش فرض تمامی VLAN ها مجوز (Allow) استفاده از پورت Trunk را دارا می باشند. این بدان معناست که کلیه ترافیک ها از پورت Trunk عبور می نمایند. حال با توجه به توضیح فوق می خواهیم در جایگاه Admin مدیریت این ترافیک را بعهده گرفته و بنا به صلاحدید تغییرات مورد نیاز را نسبت به VLAN های موجود بر روی پورت Trunk انجام دهیم، بدین منظور دستورات زیر ارائه می شود:

- دستور به شکل کلی

```
Switch01(config-if)# switchport trunk allowed vlan {add | remove | except | VLAN_ID } or {no | all}
```

```
Switch01(config-if)# switchport trunk allowed vlan VLAN_ID          */ Only this VLAN on trunk
Switch01(config-if)# switchport trunk allowed vlan add  VLAN_ID     */ Add a VLAN to Trunk
Switch01(config-if)# switchport trunk allowed vlan remove VLAN_ID   */ Remove a VLAN from Trunk
Switch01(config-if)# switchport trunk allowed vlan except VLAN_ID   */ All VLANs add ,except this VLAN
Switch01(config-if)# switchport trunk allowed vlan no               */ Remove all VLANs from Trunk
Switch01(config-if)# switchport trunk allowed vlan all              */ Add all VLANs to Trunk
```

Switch01# show vlan brief

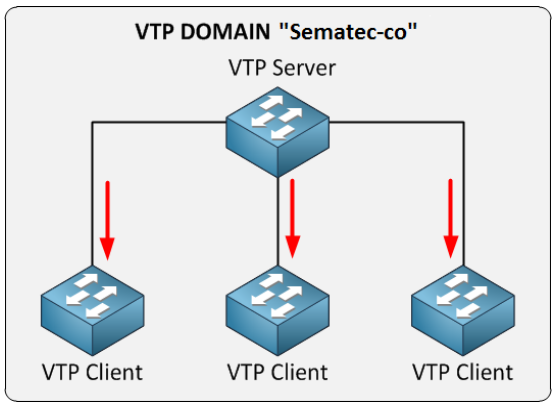
```
Switch01(config-if)#do show vlan brief

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    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
                                                 Gig0/2
50   Daniel                            active    Fa0/1
60   Mr.Barati                         active    Fa0/2
70   Mr.Bajvand                        active    Fa0/3
80   Mr.Razavi                         active    Fa0/4
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
Switch01(config-if)#
```

Switch01# show interfaces trunk

```
Switch01)# show interface trunk
Port        Mode         Encapsulation  Status        Native vlan
Gig0/1      on           802.1q         trunking      50

Port        Vlans allowed on trunk
Gig0/1      1-69,71-1005

Port        Vlans allowed and active in management domain
Gig0/1      1,50,60,80

Port        Vlans in spanning tree forwarding state and not pruned
Gig0/1      1,50,60,80
Switch01)#
```


heydari.farzad@gmail.com نام مدرس دوره: مهندس فرزاد حیدری
تهیه و گردآوری: دانیال نامورکهن

(VLAN Trunking Protocol) :VTP



در VLaning اگر شبکه شما بیش از یک سوئیچ داشته باشد باید VLan ها در همه سوئیچ ها تعریف شوند. از طرفی اگر شما یک شبکه بزرگ با تعداد زیادی کلاینت و سوئیچ های شبکه باشد، فرایند تعریف VLan ها در همه سوئیچ ها می تواند بسیار زمان بر و خسته کننده شود.

برای حل این معضل سیسکو پروتکلی به نام VTP را ابداع کرد. با فعال سازی و تعریف این پروتکل VLan ها بصورت خودکار در شبکه به تمام سوئیچ هایی که تنظیمات VTP مورد نیاز جهت دریافت VLan در آنها انجام شده باشد ارسال خواهد شد. سوئیچ های یک شبکه در تعاریف VTP می توانند در سه وضعیت client، server و یا transparent قرار گیرند.

VTP پروتکل اختصاصی سیسکو است که از آن برای تبادل اطلاعات VLAN Database بین سوئیچ های یک VTP Domain استفاده می شود و با کمک این پروتکل برای ایجاد یا حذف یک VLAN نیاز نیست که اینکار را روی تمام سوئیچ ها انجام دهید فقط کافیست روی یکی از سوئیچ ها (Server) این کار را انجام دهید این پروتکل روی باقی سوئیچ ها تغییرات شما را اعمال می کند. VTP Domain یک گروه مدیریتی است که تمام سوئیچ های عضو این گروه باید دارای نام Domain و تنظیمات یکسان باشند در غیر اینصورت اطلاعات VLAN Database بین آنها تبادل نمی شود.

پروتکل VTP برای تبادل اطلاعات از یک عدد تحت عنوان Revision Number استفاده می کند و بسته های خود را به عنوان VTP Advertisement روی پورت های Trunk خود ارسال می کند. هر سوئیچ هر ۵ دقیقه یکبار و یا در هنگام تغییر در Databse خود اقدام به ارسال Advertisement می کند. همانطور که بیان شد در هر Advertisement یک عدد تحت عنوان Revision Number وجود دارد که به ازای هر تغییر در Database یک واحد به آن اضافه می شود.

- انواع Adertisement

۱. Summary: بسته ای که حاوی اطلاعاتی مانند نام Domain و Revision Number است.
۲. Subset : بسته حاوی اطلاعات (update)
۳. .Reques: زمانی که یک Client یک بسته Summary دریافت می کند بعد از چک کردن محتویات آن با تنظیمات خود، اگر مقدار Revision Number بسته از مقدار خود بیشتر بود یک Request ارسال می کند و درخواست یک Subset می کند. همچنین در صورت ریست کردن یا تغییر نام Domain این بسته ارسال می شود.

- نحوه عملکرد:

زمانی که یک سوئیچ یک بسته Summary دریافت کند مقدار Revision Number ان را با مقدار خود مقایسه می کند. اگر مقدار Revision Number بزرگتر از مقدار خود بود یک Request ارسال می کند و درخواست Subset می کند و Database خود را با Subset دریافتی بروز می کند. اگر مقدار برابر بود، از Summary صرف نظر می کند و اگر مقدار Revision Number کوچکتر از مقدار خود بود یک Subset حاوی اطلاعات Database خود که جدیدتر است را برای سوئیچ همسایه خود ارسال می کند.

VTP Versions

نسخه	توضیحات و ویژگی ها
۱	نسخه پیش فرض سوئیچ می باشد. زمانی که در حالت Transparent است در صورت دریافت Advertisement ، نسخه و نام Domain را چک می کند در صورت مطابقت با مشخصات خود Advertisement ها را ارسال می کند.
۲	از شبکه های Token Ring پشتیبانی می کند. زمانی که در حالت Transp!arent است بدون در نظر گرفتن نسخه و نام Domain ، Advertisement ها را ارسال می کند. Consistency check: زمانی که اطلاعات جدیدی از طریق CLI یا SNMP ایجاد شود مواردی مانند نام VLAN چک می شود.در صورت استفاده از نسخه دو تمامی سوئیچ های VTP Domain باید بتوانند از این نسخه پشتیبانی کنند. در نسخه دوم تنها یک سوئیچ نقش سرور را ایفا می کند و مابقی در نقش Client عمل می کنند. نمایش Password در هر Mode !
۳	بهبود مکانیزم احراز هویت، از VLAN رنج Extended (۱۰۰۶ تا ۴۰۹۴) پشتیبانی می کند. پشتیبانی از Private VLAN ،ایجاد مکانیزم Primary Server و Secondary Server ،امکان غیر فعال کردن VTP روی پورت Trunk ، نمایش Password فقط روی Server Mode

- نکته : نسخه سوم در Cisco IOS Release 12.2 (۵۲) و بعد از ان قابل دسترس است.

- انواع نقش ها در VTP

همانطور ک در ابتدای این بخش اشاره شد سوئیچ های یک شبکه در تعاریف VTP می توانند در سه وضعیت قرار گیرند :

۱. **Server**: نقش پیش فرض سوئیچ ها است. سوئیچی که دارای این نقش است دارای تمام امکانات است می تواند Vlan بسازد ، پاک کند و یا تغییر نام دهد. هر ۵ دقیقه یکبار و یا در هنگام تغییر در VLAN Database خود Advertisement ارسال می کند. در هر VTP Domain حداقل باید یک سوئیچ دارای نقش Server باشد.

۲. **Client**: صاحب این نقش نمی تواند VLAN ایجاد یا حذف کند اما می تواند تنظیمات VTP خود را تغییر دهد. در این حالت هر ۵ دقیقه یکبار Advertisement ارسال می کند.

۳. **Transparent**: صاحب این نقش می تواند VLAN بسازد یا پاک کند اما تنها به صورت Localy (فقط روی این سوئیچ اعمال می شود). در این حالت بروز رسانی اطلاعات Database با دیگر سوئیچ ها انجام نمی شود و همچنین Advertisement ارسال نمی کند اما در صورت دریافت Advertisement اگر از نسخه یک VTP استفاده کند نام Domain و نسخه Advertisement را چک می کند در صورت مطابقت با مشخصات خود آن را ارسال می کند اما در نسخه دوم محتویات Advertisement را چک نمی کند و آنرا ارسال می کند.

نکات ضروری که باید در هنگام کار با ساختار VTP در نظر گرفته شود:

- مدل سه لایه ای شبکه: لایه سرور که در نقش Core قرار دارد، لایه پخش کننده یا Distribute و آخرین لایه که کاربران یا Users به آن دسترسی دارند Access نام دارد.
- Mode پیش فرض هر سوییچ Server می باشد.
- Domain بیان شده در مبحث VTP ارتباطی به Network Domain ندارد.
- Transparent Mode همانطور که اشاره شد فقط وظیفه عبور ترافیک را بعهده دارد. از سوییچ های تعریف شده در این Mode جهت دسترسی به سوییچ های بیشتر در Client mode و افزایش پورت ها استفاده می شود.
- هنگامیکه از Password استفاده نشود هر شخصی می تواند به راحتی با اتصال یک سوییچ به کلیه اطلاعات VLAN ها دسترسی پیدا نماید. پیشنهاد می گردد در زمان معرفی ساختار VTP بر روی سوییچ ها Domain و Password همزمان تنظیم و در نظر گرفته شود
- بدیهی است با تعاریف و مفاهیم ارائه شده امکان ساخت VLAN بر روی سوییچ مستقر در Client Mode از جانب IOS پیغام خطا دریافت خواهید نمود. "VTP VLAN Configuration not allowed when device in Client Mode"
- هنگامیکه سوییچ در Server Mode تعریف شود پیغام مشاهده می شود. "Device Mode Already VTP Server"
- هنگامیکه سوییچ در Client Mode تعریف شود پیغام مشاهده می شود. "Setting Device to Transparent | Client Mode"

heydari.farzad@gmail.com نام مدرس دوره: مهندس فرزاد حیدری
تهیه و گردآوری: دانیال نامورکهن

- هنگامیکه Domain بر روی تعریف شود پیغام مشاهده می شود. ”Changing VTP Domain name from NULL to xxxx”
- چنانچه تنظیم Password قبل از تنظیم و معرفی Domain انجام شود پیغام خطاای زیر دریافت خواهد شد

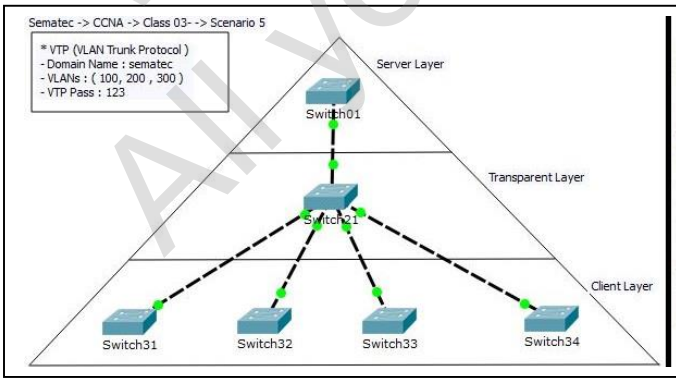
”The VTP Password cannot be set for null Domain”

اختصاص پورت ها به VLAN باید به صورت دستی انجام شود.

- هنگامیکه برای بار اول یک سوییچ را به ساختار VTP متصل کنیم و پورت متصل شده را در وضعیت Trunk قرار دهید سوییچ به صورت خودکار VTP Domain را از Server دریافت خواهد کرد. (اگر Domain Name Switch قبلاً تغییر نکرده باشد و Null باشد.)
- هشدار : چنانچه یک Switch را از انبار جهت استفاده و استقرار در VTP در نظر گرفته اید، قبل از هر چیز باید به Revision Number آن توجه نمایید. در غیر اینصورت اگر RN این سوییچ از سوییچ همسایه یا Server بالاتر باشد کلیه اطلاعات VLAN های شما از بین خواهد رفت. ولی اگر RN کوچکتر باشد مشکلی را برای شبکه شما بوجود نخواهد آورد و بروزرسانی توسط نزدیکترین سوییچ انجام خواهد شد.
- جهت Reset نمودن Revision Number ابتدا با کابل Console به سوییچ متصل شده و با تغییر Mode دادن سوییچ و برگشت مجدد به Mode قبلی عمل Reset انجام می شود.
- در VTP مدیریت بر روی پورت وجود ندارد.
- پورت هایی که مابین سوییچ ها وظیفه انتقال ترافیک شبکه را عهده دار هستند باید حتماً در وضعیت Trunk تنظیم شوند.

دستورات ایجاد VTP:

```
Switch01(config)# vtp mode {Server | Transparent | Client }
Switch01(config)# vtp domain DOMAIN_NAME
Switch01(config)# vtp password PASSWORD
Switch01># vtp show vtp status
/*
Switch01(config)# vtp mode server
Switch01(config)# vtp domain name Sematec
Switch01(config)# vtp password 123456
/*
Switch21(config)# vtp mode transparent
/*
Switch31(config)# vtp mode server
Switch31(config)# vtp domain name Sematec
Switch31(config)# vtp password 123456
Switch01># vtp show vtp status
```




```
Switch01#
Switch01#show vtp stat
VTP Version                     : 2
Configuration Revision          : 6
Maximum VLANs supported locally : 255
Number of existing VLANs        : 8
VTP Operating Mode              : Server
VTP Domain Name                 : sematec
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0x39 0xCF 0xAB 0xC0 0x4E 0x0E 0xDB
Configuration last modified by 0.0.0.0 at 3-1-93 00:13:17
Local updater ID is 0.0.0.0 (no valid interface found)
Switch01#
```

Dynamic Trunking Protocol (DTP)

این پروتکل مخصوص IOS است (CISCO Proprietery) و به صورت Dynamic پورت سوییچ را برای ما Trunk میکند. در بخش های قبل با دو وضعیت یا Mode که برای پورت قابل تنظیم است، آشنا شده اید.

۱- Access: این پورت درون یک VLAN کار می کند و ترافیک یک VLAN را انتقال می دهد.

۲- Trunk: این پورت تمامی ترافیک های VLAN ها را انتقال می دهد و عضو هیچ VLAN بخصوصی نیست.

Administrative or DTP Mode

No	Mode	Description
1	Dynamic Auto	پیشنهاد Trunk شدن را به پورت دیگر نمی دهد ولی درخواست پورت دیگر را برای Trunk شدن می پذیرد.
2	Dynamic Desirable	هم پیشنهاد Trunk شدن را به پورت دیگر می دهد و هم درخواست پورت دیگر را برای Trunk شدن می پذیرد.
3	Trunk	قطعاً چون در وضعیت Trunk است به پورت دیگر پیشنهاد Trunk شدن می دهد.
4	Aceess	به پورت دیگر Trunk شدن پیشنهاد نمی دهد و پیشنهاد هم نمی پذیرد.

بررسی نتایج برقراری دو پورت در حالت های متعدد DTP

DTP Negotiated Interface / Operational Modes

	Dyanamic Auto	Dynamic Desirable	Trunk	Access
Dyanamic Auto	Access	Trunk	Trunk	Access
Dynamic Desirable	Trunk	Trunk	Trunk	Access
Trunk	Trunk	Trunk	Trunk	LC[1]
Access	Access	Access	LC[1]	Access

[1] **LC**:Limited Connectivity

- تمامی سوییچ ها به صورت پیش فرض در Dynamic Auto می باشند.
  به دلایل امنیتی از DTP استفاده نمیشود.
- هنگامیکه کابل به پورت سوییچ متصل نیست، پورت در وضعیت Down است.
- حرف n اضافه شده در فیلد Encapsolution در خروجیshow interface trunk نشان دهنده Negotiate نمودن پورت برای Trunk است.
- برای جلوگیری از سوء استفاده احتمالی و امنیت بیشتر تمامی پورت های استفاده نشده را به Access Mode تغییر دهید و پورت هایی که برای Trunk در نظر گرفته شد اند نیز به Trunk Mode تغییر یابند تا اجازه مذاکره نداشته باشند.
- از دستور Switcport nonegotiate از انجام مذاکره بین دو پورت جلوگیری می نماید.

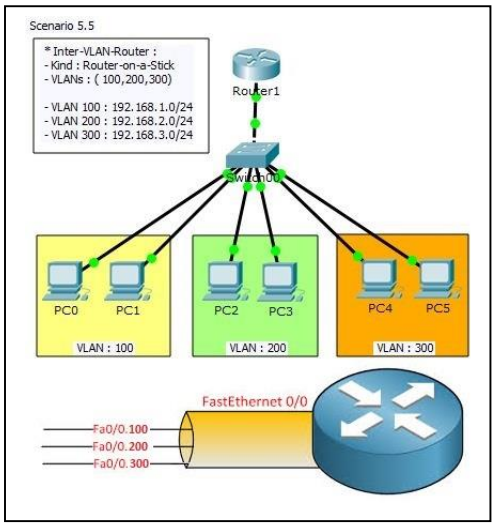
دستورات برای تنظیم پورت :

```
Switch01(config-if)# switchport mode dynamic auto          */ Dynamuc-Auto Mode
Switch01(config-if)# switchport mode dynamic desirable     */ Dynamuc-Desirable Mode
Switch01(config-if)# switchport mode trunk                 */ Trunk Mode
Switch01(config-if)# switchport mode access                */ Access Mode
Switch01(config-if)# switchport nonegotiate        */ No Negotiate ( First Change to Access)
```

فصل ششم

Inter-VLAN چیست و نحوه پیاده سازی و تنظیم آن

وقتی VLAN بر روی Switch ساخته می شود در واقع Broadcast-domain را به واحد های کوچکتری داخل لایه ۲ یا همان Switched internetwork تقسیم بندی می گردد. (با اختصاص Port هایی از Switch برای هر Subnetwork). به صورت پیش فرض Host هایی که درون یک VLAN قرار دارند نمیتوانند با Host های دیگری که درون VLAN دیگری قرار دارند ارتباط برقرار کنند. جهت برقراری VLAN ها با هم از دو روش استفاده می گردد : (Inter-vlan communication)



۱- **Router-on-Stick**: Subinterface در واقع یک Virtual Interface یا رابط مجازی می باشد که از طریق آن شما می تواند یک Interface فیزیکی روتر سیسکو را به چندین Interface مجازی یا Virtual تبدیل کند. طبیعی است که یک Subinterface در روترهای سیسکو از Physical Interface ای که از آن مشتق شده است داده های خود را ارسال و دریافت می کند. Subinterface ها می توانند برای موارد مختلفی مورد استفاده قرار گیرند. اگر شما یک روتر دارید که دارای یک Interface فیزیکی است اما می خواهید این روتر ترافیک بین دو Subnet مختلف IP را Route کند کافیست بر روی این Interface فیزیکی دو عدد Interface مجازی یا Subinterface ایجاد کنید و به هر کدام از این Subinterface ها یک آدرس IP از Subnet ای که می خواهید را بدهید و در نتیجه شما می توانید ترافیک بین این دو شبکه را Route کنید. به هر حال یک Subinterface دقیقا می تواند عملکردی مشابه یک Interface فیزیکی روتر را داشته باشد.

بخش روتر:

- فعال کردن پورت FastEthernet روتر (شماره گذاری پورت های روتر از صفر آغاز می شود و به صورت پیش فرض همه غیرفعال می باشند.)
- معرفی Subinterface ها به تفکیک هر VLAN
- تعیین نوع Tag گذاری Frame ها
- اختصاص IP به Interface مورد نظر

```
Router(config) # interface TYPE MOD/NUM.VLAN_ID
Router(config-subif) # encapsulation dot1q VLAN_ID
Router(config-subif) # ip address IP_ADDRESS NET_MASK
*/
Router(config) # interface FastEthernet 0/0
Router(config-if) # no shut
Router(config-if) # exit
Router(config) # interface FastEthernet 0/0.100
Router(config-subif) # encapsulation dot1q 100
Router(config-subif) # ip address 192.168.1.1 255.255.255.0
Router(config-subif) # exit
```

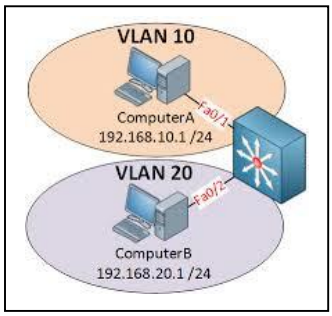
```
*/ Another VLANs , 10 , 200 , 300 , ….
*/ ….
*/ set ip address for each VLAN  ( like Default Gateway )
```

بخش سوییچ : (سوییچ لایه ۲)

- Trunk نمودن پورت متصل به Router
- اختصاص پورت ها به VLANها

```
Switch(config)# switchport mode trunk
Switch(config)# interface { range} TYPE MOD/NUMs
Switch(config-if)# switchport access vlan VLAN_ID
```

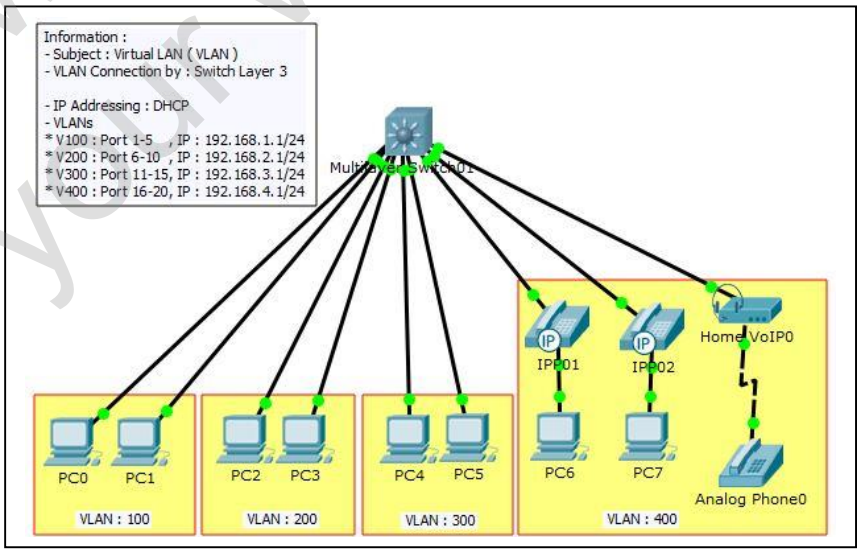
۲- استفاده از سوییچ لایه ۳: (Switch Layer 3)



برای چیره شدن بر مشکلاتی مانند ازدیاد Broadcast ها و مدیریت لینک های بیشتر ، شرکت سیسکو سویچ های مدل کاتالیست ۳۵۵۰، ۳۵۶۰ ، ۳۷۵۰ ، ۴۵۰۰۰ و ۶۵۰۰ را معرفی کرد . این سویچ های این قابلیت را دارا هستند که می توانند ارسال بسته ها را با قابلیت های سخت افزاری یک مسیریاب انجام دهند. سویچ های لایه سوم علاوه بر اینکه قابلیت های سویچ های لایه دوم را نیز دارا هستند در همان دستگاه سخت افزاری قابلیت های مسیریابی را نیز تعبیه کرده اند ، با اینکار هزینه های یک سازمان بسیار پایین می آید زیرا نیازی به خرید مسیریاب های اضافی برای استفاده از قابلیت های VLAN نخواهند داشت. مراحل و دستورات ارتباط VLAN با استفاده از سوییچ لایه ۳ :

- ساخت و ایجاد VLAN ها
- اختصاص IP به هر VLAN
- اختصاص پورت interface ها به هر VLAN
- فعال کردن توانایی مسیریابی سوییچ

```
Switch(config) # interface vlan VLAN_ID                    */ Build VLAN
Switch(config-if) # ip address IP_ADDRESS NET_MASK         */ Set IP Address for each VLAN (Like DG)
Switch(config) # ip routing                                */ Routing Between VLANs same Router
*/
Switch(config)# interface { range} TYPE MOD/NUMs                */ Enter to port / ports
Switch(config-if)# switchport access vlan VLAN_ID               */ set interfaces in each VLAN
*/
Switch(config) # interface vlan 100
Switch(config-if) # ip address 192.168.1.1 255.255.255.0
Switch(config-if) # exit
Switch(config) # interface FastEthernet 0/1
Switch(config-if) # switchport access vlan 100
Switch(config-if) # exit
Switch(config) # ip routing
```



آشنایی با CDP (Cisco Discovery Protocol):

CDP که مخفف کلمات Cisco Discovery Protocol است به معنای پروتکل شناسایی سیسکو می باشد ، این پروتکل همانطور که از نامش نیز پیداست توسط خود شرکت سیسکو تهیه و تدوین شده است و در لایه دوم از مدل OSI یا Datalink کار می کند. کاربرد اصلی CDP به اشتراک گذاری اطلاعات در خصوص Device های سیسکو ای که بصورت مستقیم به روترهای سیسکو متصل شده اند ، این اطلاعات مواردی از قبیل نوع سیستم عامل یا IOS مورد استفاده و آدرس IP مربوط به دستگاه می باشد.

بصورت پیش فرض پیام هایی که توسط Cisco Discovery Protocol یا CDP از همسایه های روتر یا Neighbor ها دریافت می شود برای سایر دستگاه های موجود در شبکه ارسال نمی شود و این بدین معناست که CDP فقط اطلاعات را به دستگاه های می دهد که بصورت مستقیم یا Directly به روتر متصل شده اند. هدر کدام از دستگاه ها و تجهیزات شرکت سیسکو که از پروتکل CDP پشتیبانی کند می تواند پیام های دریافتی از تجهیزات همسایه خود را در محلی درون دستگاه ذخیره سازی کند ، شما می توانید این پیام ها را در روترهای سیسکو با استفاده از دستور show cdp neighbors مشاهده کنید. تجهیزات شرکت سیسکو ای که از CDP پشتیبانی می کنند و پیام های CDP را دریافت می کنند پیام های CDP خود را به آدرس Multicast ای به شکل C:CC:CC:CC۰۱:۰۰:۰ ارسال می کنند. پیام های CDP هر ۶۰ ثانیه یکبار بر روی Interface های روتری که از قابلیت Subnetwork Access Protocol یا SNAP هدر پشتیبانی می کنند ارسال می شود. توجه کنید که همه interface های لایه دوم توانایی استفاده از SNAP را ندارند. رسانه هایی که از CDP پشتیبانی می کنند معمولا شبکه هایی از نوع Ethernet، Token Ring، FDDI، PPP، HDLC، ATM و Frame Relay می باشند. اطلاعاتی که در پیام ها یا Packet های CDP وجود دارد به شکل زیر است :

۱- اطلاعات نسخه نرم افزار IOS
۲- اسم دستگاه در صورت وجود
۳- قابلیت های سخت افزاری دستگاه از قبلی Routing و Switching
۴- سازنده دستگاه و سخت افزار
۵- آدرس IP دستگاه مورد نظر
۶- Interface ای که از آن برای ارسال Cisco Discovery Protocol استفاده می شود.

Switch(config) # show cdp run

```
Switch21#show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone
Device ID     Local Intrfce   Holdtme    Capability   Platform     Port ID
Switch01      Gig 0/1          172           S       2960         Gig 0/1
Switch32      Fas 0/24         172           S       2960         Fas 0/24
Switch01      Gig 0/2          172           S       2960         Gig 0/1
Switch21#
```

- با در نظر گرفتن این نکته که اطلاعات بسته های CDP برای PC های متصل به سوییچ قابل فهم نمی باشد و این بسته ها Drop می شوند. بنابراین می توان با حذف این بسته ها از ترافیک شبکه اقدام نمود. برای غیرفعال کردن ارسال بسته های CDP توسط سوییچ بر روی پورت ها از دستور زیر استفاده می شود:

Switch(config) # no cdp enable

- از آنجایی که CDP به صورت پیش فرض فعال می باشد و برخی سازمان ها نسبت به مسائل امنیتی حساسیت بیشتری دارند می توان به شکل کامل با دستور زیر اجرای آن را بر رویIOS متوقف نمود.

Switch(config) # no cdp run *\/ Starting CDP : cdp run

- هشدار : در صورت استفاده از سوییچ با قابلیت PoE (Power on Ethernet – 15.4 Volt) و تلفن های دارای IP Phone در محیط کار استفاده از دستور no cdp run باعث قطع کامل تلفن ها خواهد شد.

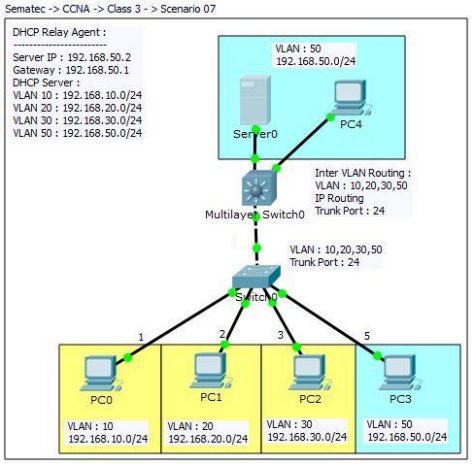
heydari.farzad@gmail.com نام مدرس دوره: مهندس فرزاد حیدری
تهیه و گردآوری: دانیال نامورکهن

فصل هفتم

ارتباط با سوییچ با SSH

همانطور که در بخش اول اشاره شد هنگامی که Admin پیکربندی یک دستگاه Cisco را انجام می دهد، در ابتدا باید از کابل کنسول (Rollover) استفاده کند و به‌طور مستقیم به دستگاه وصل شود تا به این ترتیب کنترل دستگاه را در اختیار بگیرد. مراحل و دستورات زیر به منظور پیکر بندی پروتکل SSH بر روی محصولات سیسکو ارائه می شود.

```
Switch(config) # hostname HOSTNAME                          */ 1- Change hostname
Switch(config) # line vty 0 15
Switch(config-line) # transport line SSH                    */ 2- Set input to SSH only
Switch(config-line) # login local                           */ 3- Set line vty login
Switch(config-line) # exit
*/
Switch(config) # line console 0
Switch(config-line) # logining synchronous                  */ 4- Set message on consol
Switch(config-line) # login local                           */ 5- Set console login
Switch(config-line) # exit
*/
Switch(config) # interface vlan 1
Switch(config-if) # ip address IP_ADDRESS NET_MASK          */ 6- Set ip for vlan 1
Switch(config-if) # no shut
Switch(config-if) # exit
*/
Switch(config) # username USER_NAME secret PASSWORD         */ 7- Set user name on database
Switch(config) # enable secret PASSWORD                     */ 8- Set enable password
Switch(config) # service password-encryption secret PASSWORD */ 9- Set enable password
Switch(config) # ip domain-name DOMAIN_NAME                 */ 10- Set a domain
Switch(config) # crypto key generate rsa      */11 – RSA Cryptography – A Policy Key (Rivest-Shamir-Adleman)
The name for the keys will be: networks.blog
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]: 1024
 % Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

Switch# show ip ssh                                         */ show ssh situation on switch (enable/disable)
*/ on PC
Set ip address and default gateway on your PC
ssh –L USERNAME IP_ADDRESS
```



DHCP Relay Agent: در فصل دوم مفاهیم و تنظیمات DHCP ارائه شد. در این قسمت به ارتباط مابین VLAN های متعدد در شبکه که از سرویس DHCP استفاده می کنند. خواهیم پرداخت. البته در سازمان های بزرگ از سرویس DHCP بر روی سوییچ ها استفاده نمی شود بلکه بر روی یک سرور (Microsoft یا Linux) ایجاد و پیکربندی می شود.

Relay Agent در حقیقت یک قابلیت در سویچ های لایه سوم یا روترها می باشد که درخواست های آدرس IP یا Broadcast را از Client ها دریافت کرده و بصورت Unicast برای DHCP سرورهای تعریف شده روی آن ارسال می کند، طبیعی است که Client ها و Server ها در چنین شبکه ای در یک Subnet قرار ندارند و بصورت فیزیکی هم ممکن است از هم جدا باشند، در واقع وظیفه اصلی Relay Agent ارسال درخواست به سرور و پاسخ دادن به Client می باشد. فرآیند ارسال یا Forwarding در Relay Agent تا حدودی با فرآیند Forwarding معمولی که در IP Router ها انجام می شود متفاوت است، بگونه ای در IP Routing معمولی ساختار Packet ارسالی و دریافتی چندان تغییر نمی کند اما در Relay Agent بعد از اینکه بسته Broadcast از طریق پیام DHCP Client دریافت شد روتر یک Packet یا یک پیام جدید ایجاد می کند و برای DHCP ارسال می کند، Router یا سوییچ لایه ۳ درخواست را از یک طرف بصورت Broadcast دریافت و از طرف دیگر بصورت Unicast برای سرور DHCP ارسال میکند.

- ✓ یک DHCP در VLAN خود فقط به scope خود جواب می دهد که IP Address کارت شبکه DHCP جز آن قرار دارد.
- ✓ در صورتی که بخواهید DHCP به VLAN های دیگر نیز IP Address بدهد کافی است که برای هر VLAN یک scope در DHCP تعریف کنید سپس به وسیله دستور IP helper بر روی روتر یا سوییچ لایه ۳، پکت های Broadcast دریافتی را به شکل Unicast به سمت DHCP بفرستید.
- ✓ زمانی که برای هر VLAN یک scope تعریف می کنید باید Default Gateway آن VLAN را در رنج IP Address آن scope بر روی DHCP معرفی نمایید.

۱- تنظیمات Server ، اختصاص IP,Subnet Mask, Default Gateway

۲- تنظیمات DHCP Sever، ایجاد Scope ها و معرفی محدوده IP برای هر Inter VLAN

۳- معرفی VLAN ها بر روی سوییچ لایه ۳ و اختصاص DG برای هر VLAN

۴- تنظیم Forwarding بر روی سوییچ لایه ۳ و برقراری ارتباط InterVLAN ها با DHCP

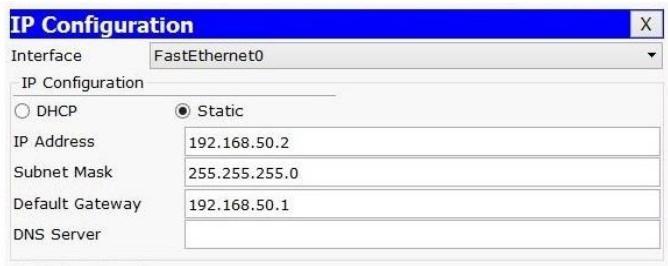
```
Switch01(Config-if)# ip  helper-address IP_Address        */ DHCP Server IP Address
Switch01(Config-if)# ip  helper-address 192.168.50.2      */ DHCP Server IP Address
```

۵- Trunk کردن Interface مابی سوییچ ها

۶- اختصاص پورت یا پورت ها به هر VLAN بر روی سوییچ لایه ۲

۷- تنظیم و اختصاص IP و سایر مشخصات به هر Client از طریق DHCP

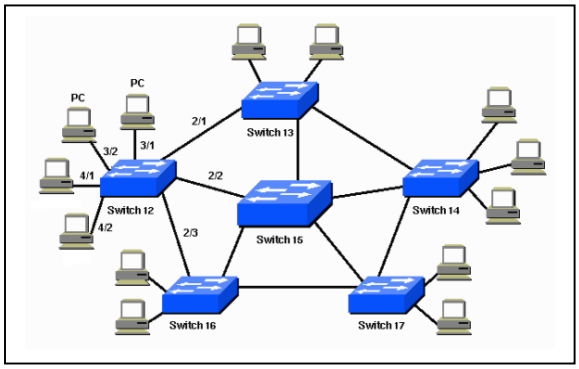
Pool Name	Default Gateway	DNS Server	Start IP Address	Subnet Mask	Max User	TFTP Server
VLan50	192.168.50.1	0.0.0.0	192.168.50.3	255.255.255.0	200	0.0.0.0
VLan30	192.168.30.1	0.0.0.0	192.168.30.2	255.255.255.0	200	0.0.0.0
VLan10	192.168.10.1	0.0.0.0	192.168.10.2	255.255.255.0	200	0.0.0.0
VLan20	192.168.20.1	0.0.0.0	192.168.20.2	255.255.255.0	200	0.0.0.0
serverPool	0.0.0.0	0.0.0.0	192.168.50.0	255.255.255.0	512	0.0.0.0



heydari.farzad@gmail.com نام مدرس دوره: مهندس فرزاد حیدری

تهیه و گردآوری: دانیال نامورکهن

پروتکل درخت پوشا یا (STP:Spanning Tree Protocol)



در طراحی شبکه داشتن لینک جایگزین (Redundant) یک ویزگی محسوب می شود که در صورت از کار افتادن لینک اصلی از لینک جایگزین جهت جلوگیری از وقفه در جریان ترافیک استفاده می شود اما Ethernet قابلیت تشخیص لینک جایگزین و غیر فعال کردن آن تا زمان مورد نیاز را ندارد در نتیجه باعث ایجاد یک چرخه می شود و ترافیک Broadcast دائم در این مسیر در حال چرخش است و به مقدار آن اضافه می شود و به اصطلاح باعث ایجاد Loop در شبکه می شود و ۳ اتفاق بر روی شبکه رخ خواهد داد که در نهایت با پر شدن پهنای باند و درگیر شدن تجهیزات، شبکه ظرف مدت ۳ تا ۵ دقیقه Down خواهد شد. سه اتفاق اشاره شده عبارتند از :

۱- **Broadcast Storm**: به دلیل ارسال پیاپی بسته های ARP در شبکه و ایجاد Loop این پدیده در شبکه رخ می دهد.

۲- **Mac-Address-Table Instability**: با ارسال بسته ARP برای PC ها (FLOOD) سوییچ Mac دستگاه ها را در جدول خود ثبت می کند و پس از مدتی دچار سر در گمی و بی ثباتی می شود که این Mac دریافتی از PC را روی پورت ۱ خود ثبت کند یا ۲ (Learn). جدول نگهداریMac دائماً در حال تغییر است و چنانچه مشکل فوق مدت زمان زیادی به طول بیانجامد پورت غیرفعال می شود و Mac-Flapping رخ می دهد.

۳- **Multiple Framing**: همزمان دو Frame با یک مشخصات برای پورت ارسال می شود. نرم افزارهای امنیتی نصب شده روی شبکه به دلیل احتمال خطر Attack روی شبکه یکی از بسته ها را Drop می کنند. بودن و نبودن این اتصال به عنوان مسیر جایگزین شبکه را در کوتاه مدت و دراز مدت با مشکل مواجه می سازد ، پس چاره مار چیست ؟

Spanning Tree پروتکلی است استاندارد (802.1D) که با تشخیص مسیر جایگزین یا مسیر دوم آنرا تا زمانی که مورد نیاز نیست مسدود می کند. بنابراین طراح شبکه می تواند ضمن جلوگیری از بوجود آمدن Loop (Loop Free) در شبکه دو یا چند مسیر را بین سوئیچ های خود در نظر بگیرد، یک مسیر را به عنوان مسیری اصلی Active و باقی مسیرها به عنوان Standby در نظر گرفته می شود و در صورت قطع شدن مسیر اصلی مسیر Standby به سرعت جایگزین مسیر اصلی شده و ترافیک را منتقل می کند. و به این شکل یک شبکه با قابلیت اطمینان بیشتر خواهیم داشت.

STP چگونه کار می کند ؟

این پروتکل دارای الگوریتمی است که طی آن عملیات تصمیم گیری صورت می گیرد تا مشخص شود کدامیک از لینکهای شبکه در حالت Forwarding و کدامیک در حالت Blocking قرار گیرد. این تصمیم گیری براساس چند عامل صورت می پذیرد که مهمترین آنها عبارتند از :

الف) اگر یک Switch بعنوان سوئیچ اصلی شناسایی شود تمام لینکهای متصل به آن در حالت Forwarding قرار خواهند گرفت.

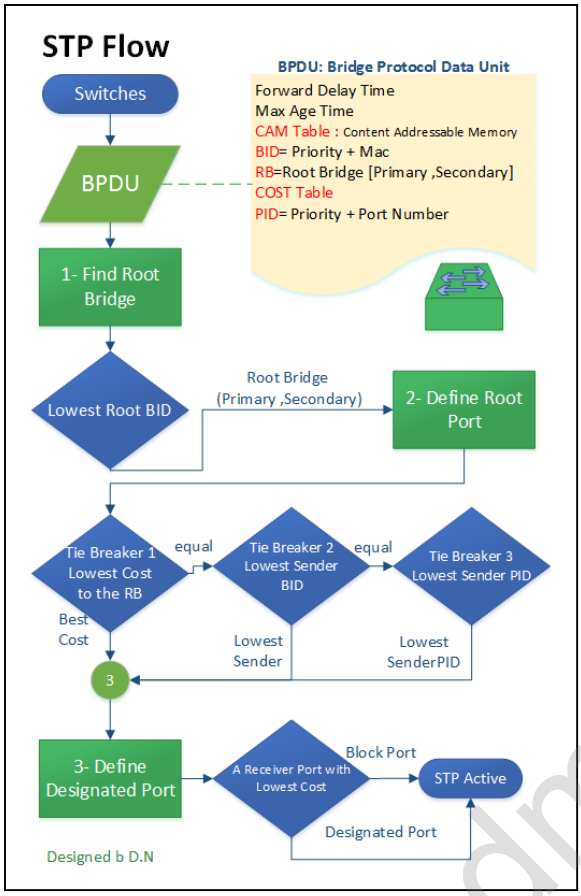
ب) اگر چندین سوئیچ به سوئیچ x متصل باشند ، سوئیچ x تنها لینکی را در حالت هدایت قرار می دهد که کمترین و کوتاهترین هزینه را تا سوئیچ اصلی دارا باشد.

ج) لینکی از یک Switch که کمترین هزینه را با سوئیچ اصلی دارا است در حالت هدایت قرار خواهد گرفت.

- در صورتی که وضعیت لینک در حالتی غیر از موارد فوق باشد ، STP آن لینک را Block خواهد کرد.
- نکته قابل ملاحظه در STP این است که این پروتکل نیز مانند اکثر پروتکل های دیگر قابلیت همگرائی دارد. بدین مفهوم که در صورت قطع یک ارتباط و یا ایجاد تغییر در مسیر و جابجائی فیزیکی سوئیچ ها و ارتباطات، این مسیرها و وضعیتها متعاقباً متناسب با وضعیت فعلی تغییر خواهند کرد.

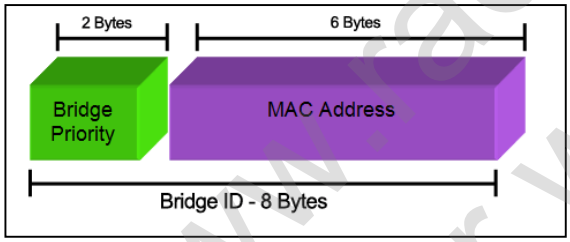
فصل هشتم

سه مرحله اصلی STP برای انجام کار



۱. **Select Root Bridge**: (انتخاب رئیس شبکه) در تمام شبکه حتماً یک سوییچ رئیس وجود دارد و تمامی ترافیک ها از آن عبور می کند. این انتخاب بر اساس و معیار (BID : Bridge ID) انجام می شود که شامل Priority و Mac-Address می باشد. هر سوییچ که دارای BID کمتری باشد به عنوان Root Bridge شناخته می شود. شایان ذکر است که تمامی سوییچ ها به طور پیش فرض Priority یکسانی دارند و آن عدد 32768 می باشد. سوالی که مطرح می شود، این است که اگر تمام سوییچ ها یک Prioriy دارند پس معیار انتخاب Root Bridge چیست؟ پاسخ این سوال Mac-Address است ولی اگر این سوییچ انتخاب شده به عنوان Root Bridge سوییچ متوسط و قدیمی تر در شبکه بوده و Admin بخواهد سوییچ جدیدتر و با کارایی بالاتر را جایگزین آن کند، چه باید کرد؟ برای رفع این مشکل Admin می تواند با تغییر عدد Priority ، سوییچ مورد نظر خود را به عنوان Root Bridge تعیین نماید.

Switch01 # show spanning-tree *⁄ Dispalay STP Information



- به دلیل اضافه شدن شماره VLAN به Priority عدد ۳۲۷۶۸ یک رقم افزایش داشته است. STP در VLAN 1 ایجاد شده بنابر این عدد ۳۲۷۶۹ قابل مشاهده می باشد.
- به منظور انتخاب یک سوییچ به عنوان Root Bridge یک عدد در مضرب ۴۰۹۶ را کمتر از Priority دیگر سوییچ ها قرار می دهیم.
- به هیچ عنوان Priority نباید صفر باشد. زیرا امکان تعیین سوییچ دیگر به عنوان Root Bridge امکانپذیر نخواهد بود مگر اینکه مجدداً صفر را به عددی بزرگتر تغییر دهیم.
- با استفاده از دستور زیر می توان Priority را با در نظر گرفتن تمامی موارد فوق الذکر تغییر داد. اعدادب با مضرب ۴۰۹۶ (4096, 8192, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, …)

Switch(config)#spanning-tree vlan VLAN_ID priority PRIORITY_NUM

- استفاده از no در ابتدای دستور فوق وضعیت را به حالت پیش فرض بر می گرداند.
- جهت تعیین سوییچ رئیس و نیز جایگزین آن به عنوان معاون علاوه بر تعیین عدد Priority می توان از Macro نیز استفاده نمود. بدین شکل که برای رئیس گزینه Primary [(4096*2)-32768] و برای جایگزین Secondary [(4096*1)-32768] را در دستور زیر در نظر گرفت. (اولویت Macro بیش از Priority می باشد)

Switch(config)#spanning-tree vlan VLAN_ID root { primary | secondary }

بسته BPDU - (Bridge Protocol Data Unit) نام بسته های ارسالی STP می باشد که تا قبل از مشخص شدن Root Bridge کلیه سوییچ ها این بسته را ارسال می کنند ولی به محض مشخص شدن RB فقط RB این بسته را ارسال می کند. (هر ۲ ثانیه) BID هم در همین بسته قرار گرفته است.

۲. **Select Root Port**: (انتخاب بهترین مسیر) Root Port پورتی است که بهترین مسیر (Root Path Cost to RB) را تا Root Bridge دارد. هر سوییچ یک Root Port دارد ولی Root Bridge فاقد Root Port می باشد زیرا کمترین هزینه را دارا می باشد.

پروتکل STP با گوش دادن به پیامهای رد و بدل شده میان Switch ها و آنالیز آنها متوجه درجه اهمیت دستگاههای متصل به سوئیچ می شود. بطور معمول همه سوئیچ ها بعد از اتصال به یکدیگر با بسته BPDU به یکدیگر پیام می دهند و ادعا می کنند که من سوئیچ اصلی هستم و همه لینک های من باید در حالت هدایت قرار بگیرند اما از آنجا که همه سوئیچ ها به یکدیگر این پیغام را می دهند، این پیام ها توسط خودشان آنالیز می شود و به نتیجه می رسند که کدامیک از لینک ها از درجه اهمیت بیشتری نسبت به بقیه برخوردار می باشد.

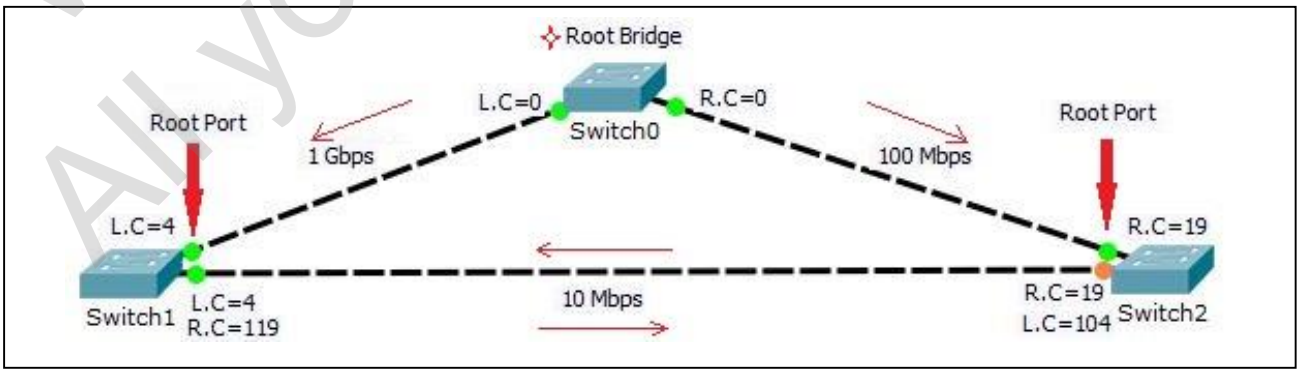
در پیامهای BPDU شماره Switch به همراه آدرس فیزیکی آن برای بقیه سوئیچ ها ارسال می شود و هریک از سوئیچ ها پیام های BPDU دریافتی را با یکدیگر مقایسه می کند و سوئیچ هائی را که دارای شماره و آدرس کوچکتر می باشد را بعنوان کم هزینه ترین و سوئیچ اصلی انتخاب می کنند جالب اینجاست که اگر یکی از سوئیچ ها بفهمد که مثلاً Switch شماره ۳ از بقیه سوئیچ هائی که می شناسد بهتر و کم هزینه تر است از آن به بعد تبلیغ Switch شماره ۳ را می کند و به سوئیچ های همسایه خود می گوید شماره ۳ اصلی است این روند تا آنجا ادامه پیدا می کند که تمامی سوئیچ های شبکه در اصلی بودن یکی از سوئیچ ها به توافق برسند. در این زمان طبق شرایط ذکر شده تمامی لینکهای آن را در حالت هدایت قرار می دهند و سوئیچهای متصل به آن، لینک واسط خود با آن را فعال نگه می دارند. حالا بحث بین لینکهای دیگر شروع می گردد.

هزینه دستیابی این لینکها به سوئیچ اصلی در فرآیند تشخیص Switch اصلی محاسبه شده است و در این لحظه با یک بررسی کلی ، کم هزینه ترین لینکها در حالت Forwarding قرار می گیرند و مابقی بلوکه می شوند قابل ذکر است که هزینه لینک ها را می توان بصورت دستی در سوئیچ تعریف کرد ولی بطور استاندارد هزینه لینک های مختلف بصورت زیر است.

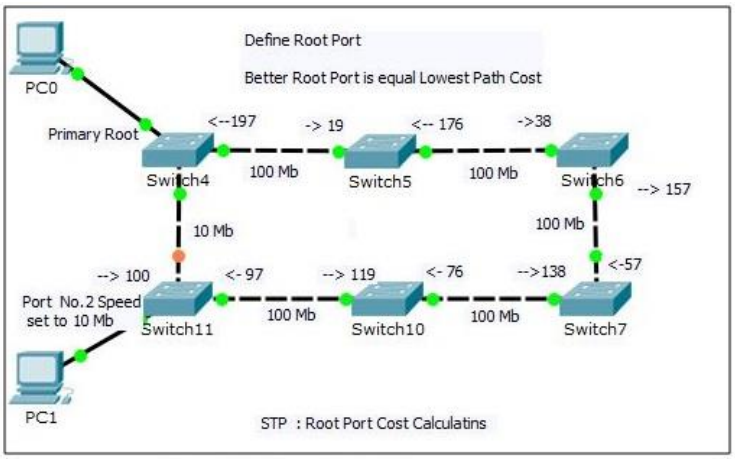
Speed (Bandwidth)	Scale	STP Cost Value
10	Mbps	100
100	Mbps	19
1	Gbps	4
10	Gbps	2

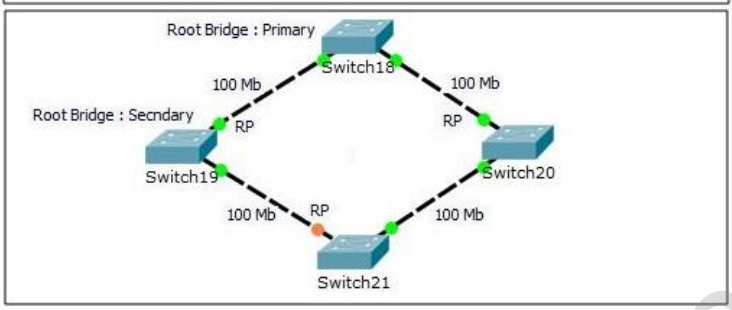
برای هر مسیر یک Path Cost محاسبه می گردد. نحوه محاسبه Path Cost بر اساس استانداردهای ارائه شده توسط موسسه IEEE است. بمنظور محاسبه مقدار Path Cost ، ۱,۰۰۰ مگابیت در ثانیه (یک گیگابیت در ثانیه) را بر پهنای باند سگمنت متصل شده به پورت، تقسیم می نمایند. بنابر این یک اتصال ۱۰ مگابیت در ثانیه، دارای Cost به میزان ۱۰۰ است (۱,۰۰۰ تقسیم بر ۱۰). بمنظور هماهنگ شدن با افزایش سرعت شبکه های کامپیوتری استاندارد Cost نیز اصلاح می گردد. جدول مقابل مقادیر STP Cost را نشان می دهد.

- باید به ازای هر سوییچ یک Root Port پیدا کنیم.
- قبل از دریافت بسته ارسالی از Root Bridge توسط سوییچ هزینه برابر صفر است، با توجه به نوع کابل و سرعت آن هزینه محاسبه می شود. پورتی که کمترین هزینه را داشته باشد به عنوان Root Port انتخاب می شود. هزینه ها در داخل بسته BPDU قرار دارد.



heydari.farzad@gmail.com نام مدرس دوره: مهندس فرزاد حیدری
تهیه و گردآوری: دانیال نامورکهن





❖ نمونه ای برای تمرین محاسبه و تعیین Root Port

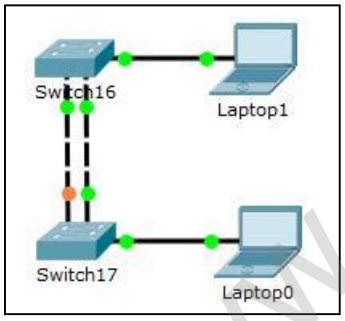
- تعیین Root Bridge
- تعیین Root Port ها
- هزینه یابی اجزاء مسیر
- محاسبه مسیر ۱ موافق گردش ساعت : PC0 به PC1
- محاسبه مسیر ۲ معکوس گردش ساعت : PC1 به PC0
- تعیین نقطه بلاک
- تعیین بهترین مسیر

❖ نمونه ای برای تعیین Root Port & Secondary RB

- تعیین Root Port ها
- هزینه یابی اجزاء مسیر
- محاسبه مسیر ۱ و ۲
- تعیین نقطه بلاک
- تعیین بهترین مسیر

Tie Breaker: در شرایطی که cost هر دو مسیر مشابه باشد، اولویت دیگری یا اصطلاحاً Tie Breaker باید مورد استفاده قرار گیرد و آن Lowst Sender BID است. در این حالت چنانچه BID فرستنده کمتر باشد به عنوان Root Port انتخاب می شود.

دراینجا Root Bridge ، Cost و Sender BID یک سوییچ است، حال چه باید کرد؟



در این وضعیت از Tie Breaker سوم استفاده می کنیم و Lowest Sender PID مربوط به پورت سوییچ فرستنده بسته BPDU در نظر گرفته می شود. چنانچه بخواهیم در انتخاب صورت گرفته بنا به دلایلی تغییراتی اعمال کنیم می توان با تغییر Port ID که از P[riority و شماره پورت تشکیل شده است استفاده کرده و اولویت دیگری را برای انتخاب Root Port تعیین کنیم. Priority مضربی از ۱۶ است و لازم به ذکر نیست که تنظیم دستور زیر می بایست بر روی پورت یا Interface مورد نظر انجام شود.

Switch(config-if)#spanning-tree vlan VLAN_ID port-priority PRIORITY_NUM

۳. **Select Designated Port**: (انتخاب پورت برتر) پورتی است که بسته BPDU را با کمترین Cost دریافت می کند. این پورت در Packet Tracer با رنگ سبز نشان داده می شود. تا اینجا تمامی پورت ها و سوییچ ها نقش و عنوان را به خود اختصاص داده اند به غیر از یک پورت که در وضعیت Block قرار گرفته (Block Port) و به نقشی با عنوان Alternate را به خود اختصاص می دهد تا در زمان مقتضی جایگزین Root Port شود. این پورت در برنامه Packet Tracer با رنگ نارنجی مشخص شده است که در مثال های فوق نمونه های متعددی از آن را می توانید مشاهده نمایید.

```
Switch#show spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID     Priority    32769
              Address     0009.7C42.76B2
              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     0009.7C42.76B2
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Gi0/2            Desg FWD 4         128.26   P2p
Gi0/1            Desg FWD 4         128.25   P2p

Switch#
```


heydari.farzad@gmail.com نام مدرس دوره: مهندس فرزاد حیدری
تهیه و گردآوری: دانیال نامورکهن

STP State : هر پورتی که در STP شرکت می کند ۵ وضعیت را دارا می باشد.

۱. **Blocking:** پورت برای مدت ۲۰ ثانیه در حالت Blocking باقی می ماند و در این مدت فقط به BPDU ها گوش داده و آنها را پردازش می کند و مابقی فریم ها را Drop می کند. در واقع سوییچ منتظر است تا اطلاعاتی راجع به Root Bridge ، Root Port، Designated Port کسب کند.

۲. **Listening:** پس از اتمام ۲۰ ثانیه یک RP یا DP به مدت ۱۵ ثانیه به وضعیت Listening می رود و به BPDU گوش داده و آنها را پردازش می کند و مابقی فریم ها را Drop می کند. بقیه پورت ها در حالت Block هستند.

۳. **Learning:** پورت های RP و DP از وضعیت Listening خارج شده و به مدت ۱۵ ثانیه به وضعیت Learning می روند و Mac Table و CAM Table را Update می کند اما سوییچ هنوز فریم ها را Forward نمی کند. البته در این وضعیت نیز به BPDU گوش می دهد و آنها را پردازش می کند.

۴. **Forwarding:** در نهایت پورتی که در وضعیت learning بود به وضعیت forward می رود و همزمان با ارسال فریم ها عمل پردازش و بروز رسانی جداول را نیز انجام میدهد.

۵. **Disable:** پورت که در این وضعیت باشد در فرآیند STP شرکت نمی کند. (خاموش بودن پورت، عدم اتصال کابل، غیر فعال بودن پورت توسط Aamin). مدت ۳۰ تا ۵۰ ثانیه برای همگرایی مابین سوییچ ها در این فرآیند صرف می شود که با استفاده از قابلیت PortFast می توان کاری کرد تا پورت های Access (Only Connect to PC) مستقیماً به حالت Forwarding بروند.

```
Switch(config-if) spanning-tree portfast trunk
Switch(config-if) spanning-tree portfast disable
```

R	STP State	Receiveing & BPDU Processing	Sending BPDU	Receiveing & Frame Processing	Sending Frame	Receive & Update Mac & CAM Tables
۱	**Blocking**	Yes	No	No	No	No
۲	**Listening**	Yes	Yes	No	No	No
۳	**Learning**	Yes	Yes	Yes	No	Yes
۴	**Forwarding**	Yes	Yes	Yes	Yes	Yes
۵	**Disabled**	No	No	No	No	No

- Forward Delay Time: از این طریق سوییچ متوجه می شود شبکه Loop Free است.
- Max Age Time : ۲۰ ثانیه زمانی است که هر سوییچ در شبکه ارسال می کند و در صورت عدم پاسخ خودش را رییس اعلام می کند.
- Hello Time: بسته ای است که RB هر دو ثانیه ارسال می کند.
- BPDU Guard: چنانچه به پورتی که جهت اتصال به PC از امکان PortFast نیز استفاده کرده یک سوییچ متصل کنیم، پورت مربوطه کاملاً down می شود. راه اندازی مجدد آن با Shutdown , No shutdown کردن آن انجام می گیرد.

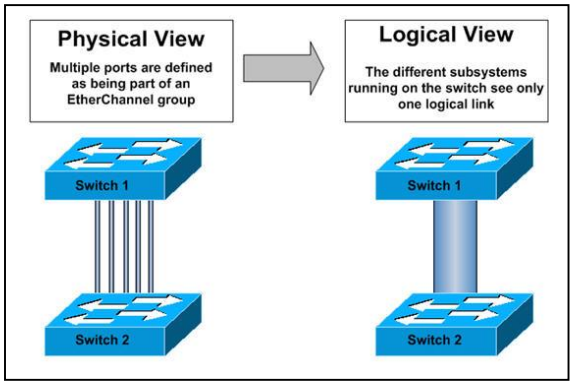
```
Switch(config-if)# Spaning-tree bpduguard enable
Switch(config-if)# Spaning-tree bpduguard disableS
```

STP Mode:

- Traditional
- Advance PVST

فصل نهم

Aggregation: (EtherChannel)



لینک های Ethernet با استاندارد های متفاوت معرفی شده اند که مشخصات متفاوتی دارند. یکی از مهمترین مشخصات آن که انگیزه پیشرفت را ایجاد کرده همواره سرعت آنها بوده است .Ethernet در حال حاضر با استاندارد های 1G,10Gو10M,100M,1000M موجود است که طبیعتاً برای لینک های با پهنای باند بیشتر می بایست هزینه بیشتری برای تجهیزات و لینک های ارتباطی متحمل شد. علاوه بر هزینه ممکن است media ارتباطی نظیر فیبر برای سرعت بالاتر وجود نداشته باشد.

پس در موارد نیاز به سرعت بیشتر باید به دنبال راه چاره گشت .گاهی اوقات ما بین ۲ عدد switch یا یک router و یک switch نیاز به برقراری یک ارتباط Redundant داریم. به صورتی که هنگام قطع شدن یکی از لینک های ارتباطی لینک دومی وجود داشته باشد تا در مدار آمده و سرویس دهی را ادامه دهد.

برای پاسخ به مشکلات فوق تکنولوژی Etherchannel ابداع گردید که تحت استاندارد ۸۰۲,۳ معرفی شده است. این استاندارد اتصال دو switch را توسط دو الی هشت لینک ارتباطی ممکن می سازد. در ابتدا شرکت سیسکو Etherchannel را با پروتکل Port Aggregation Protocol عرضه کرد و پس از آن IEEE استاندارد ۸۰۲,۳ با نام Link Aggregation Control Protocol معرفی نمود. PAgP تنها بین تجهیزات سیسکو قابل استفاده است و LACP به صورت استاندارد در ما بقی تجهیزات کاربرد دارد. لازم به ذکر است که تجهیزات سیسکو نیز از LACP پشتیبانی میکنند.

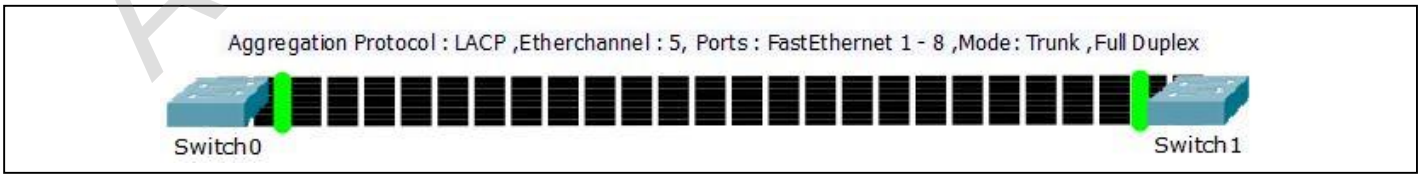
نکته:

- در صورت وجود Bottleneck از Aggregation استفاده می شود.
- پورت های انتخابی باید دارای سرعت همسان باشند.
- Aggregation از پورت های Ethernet پشتیبانی نمی کند.
- تمامی پورت ها از نظر Duplex باید در یکی باشند. (Half / Full)
- وضعیت پورت ها (mode) باید یکی باشند. (Access / Trunk)
- Lacp می تواند تا ۱۶ پورت را تجمیع کند ولی فقط ۸ پورت آن Active هستند و مابقی به صورت Backup در نظر گرفته می شود.

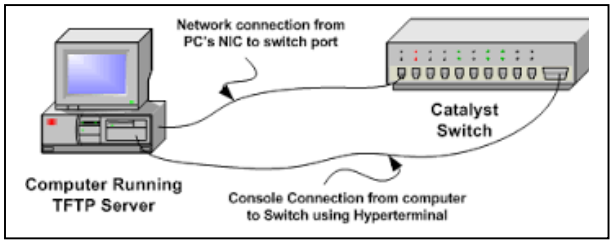
Switch1(Config-if)# interface range TYPE MOD/NUM
Switch1# show run

Type	Protocol	Command	Best Practice	
Manual		(config-if)# channel-group NUM mode on	On	On
Dynamic *	**PAgP** (Port Aggregation Protocol) Cisco Propriety	(config-if)# channel-protocol PAgP */ (optional) (config-if)# channel-group NUM mode <desirable | auto>	Desirable	Auto
	LACP (Link Aggregation Control Protocol)	(config-if)# channel-protocol LACP */ (optional) (config-if)# channel-group NUM mode <Active | Passive>	Active	Passive

(Negotiation Protocol)



مدیریت سیستم عامل سوییچ (IOS)



همانطور که در ابتدای جزوه اشاره شد IOS (برگرفته از Internetwork Operating System)، نرم افزاری است که از آن به منظور کنترل روتینگ و سوئیچینگ دستگاه های بین شبکه ای استفاده می گردد . آشنائی با IOS برای تمامی مدیران شبکه و به منظور مدیریت و پیکربندی دستگاه هائی نظیر روتر و یا سوئیچ الزامی است. یک روتر و یا سوئیچ بدون وجود یک سیستم عامل قادر به انجام وظایف خود نمی باشند (همانند یک کامپیوتر). شرکت سیسکو، سیستم عامل Cisco IOS را برای طیف گسترده ای از محصولات شبکه ای خود طراحی و پیاده سازی نموده است. نرم افزار فوق، جزء لاینفک در معماری نرم افزار روترهای سیسکو می باشد و همچنین به عنوان سیستم عامل در سوئیچ های Catalyst ایفای وظیفه می نماید. بدون وجود یک سیستم عامل، سخت افزار قادر به انجام هیچگونه عملیاتی نخو اهد بود. فرآیند راه اندازی روتر با استقرار برنامه Bootstrap ، سیستم عامل و یک فایل پیکربندی در حافظه آغاز می گردد. در صورتی که سوییچ / روتر نتواند یک فایل پیکربندی را پیدا نماید، Setup mode فعال و پس از اتمام عملیات در این mode ، می توان یک نسخه backup از فایل پیکربندی را در حافظه NVRAM ذخیره نمود.

تغییر و نصب IOS یا سیستم عامل سوئیچ و روتر سیسکو یکی از مواردی است که توسط مدیر شبکه کامپیوتری یک سازمان صورت می گیرد. دلیل اینکار را می توان در موارد زیر خلاصه کرد :

- مانند بقیه نرم افزارها ، سیستم عامل دستگاه ها نیز دارای نقاط ضعف امنیتی هستند که به مرور توسط تولید کنندگان شناسایی شده و در نسخه های جدید سیستم عامل اصلاح می شوند.
- اضافه شدن امکانات جدید به سیستم عامل همواره مد نظر ایجاد کنندگان سیستم عامل بوده است.
- همیشه بروزبودن و بروزنگهداشتن دستگاه ها به عنوان یک وظیفه همیشه مدنظر مدیران شبکه می باشد.

ویژگی نرم افزار IOS

شرکت سیسکو تاکنون نسخه های متفاوتی از نرم افزار IOS را پیاده سازی نموده است . هر نسخه دارای ویژگی های مختص به خود می باشد .علیرغم تنوع بسیار گسترده IOS برای دستگاه های سیسکو ، ساختار اولیه دستورات پیکربندی در آنان مشابه می باشد و در صورت کسب مهارت لازم به منظور پیکربندی و اشکال زدائی یک دستگاه خاص، می توان از تجارب موجود در ارتباط با سایر دستگاه ها نیز استفاده نمود. اسامی در نظر گرفته شده برای هر یک از نسخه های IOS از سه بخش عمده تشکیل می گردد :

محیطی که image بر روی آن اجراء می گردد.
ویژگی منحصربفرد image
محل اجراء image و وضعیت فشرده بودن آن

با استفاده از Cisco Software Advisor می توان ویژگی های خاصی از IOS را انتخاب نمود. نرم افزار فوق یک ابزار محاوره ای است که پس از نمایش وضعیت موجود، امکان انتخاب گزینه هائی متناسب با واقعیت های شبکه را فراهم می نماید.

یکی از مهمترین مواردی که در زمان انتخاب یک IOS image جدید می بایست به آن توجه گردد ، سازگاری آن با حافظه فلش و RAM است . نسخه های جدیدتر عموماً دارای امکانات بیشتری بوده و به حافظه بیشتری نیز نیاز خواهند داشت. با استفاده از دستور Show version می توان وضعیت image موجود و حافظه فلش را مشاهده نمود. قبل از نصب یک نسخه جدید از نرم افزار OS ، می بایست وضعیت حافظه آن به منظور اطمینان از وجود ظرفیت کافی، بررسی گردد . برای مشاهده میزان حافظه RAM ، از دستور Show version استفاده می گردد.

heydari.farzad@gmail.com نام مدرس دوره: مهندس فرزاد حیدری
تهیه و گردآوری: دانیال نامورکهن

تهیه نسخه پشتیبان و ارتقاء سیستم عامل دستگاه سیسکو

قبل از نصب و بروزرسانی سیستم عامل دستگاه سیسکو از تنظیم های دستگاه های سیسکو خود نسخه پشتیبان تهیه نمایید. قدم اول در بروزرسانی تهیه آخرین ویرایش سیستم عامل ، دانلود آن است. برای این منظور می توانید به لینک زیر مراجعه نموده و سیستم عامل متناسب به دستگاه سیسکو خود را دانلود نمایید.

http://www.cisco.com/tacpage/sw-center/index.shtml

در این نوشتار IOS 3560 به عنوان نمونه انتخاب شده است. با اجرای دستور زیر تنظیمات موجود در حافظه را ذخیره نمایید.

```
cisco# write memory
cisco# copy running-config startup-config
```

از وجود فضای لازم در Flash memory اطمینان حاصل نمایید و از Startup Configuration نسخه پشتیبانی تهیه کنید. شما از دستور Show flash برای دیدن فضای Flash Memory می توانید استفاده کنید.

در اینجا باید TFTP Server راه اندازی نمایید تا بتوانید ازتنظیمات نسخه پشتیبان تهیه کنید، Image دستگاه را ذخیره کنید و در آخر بروزرسانی را انجام دهید. برای نصب TFTP بخاطر داشته باشید که IP در محدوده IP سوییچ استفاده کنید و همچنین Gateway مناسب برای دستگاه سیسکو و کامپیوتر خود انتخاب کنید. ذخیره سازی تنظیمات بصورت زیر خواهد بود.

```
cisco# copy startup-config tftp
Address or name of remote host []? 10.10.10.2
Destination filename [startup-config]?
!!
۱۲۷۸ bytes copied in 0.100 secs
```

تهیه Image از نسخه IOS موجود به صورت زیر خواهد بود.

```
cisco# copy flash: tftp:
Source filename []? xxxxx-xx-xx.121-x.XB
Address or name of remote host []? 10.10.10.2
Destination filename [xxxxx-xx-xx.121-x.XB]?
```

پس از تهیه نسخه پشتیبان از تنظیمات و سیستم عامل، نوبت آن است که نسخه جدید IOS را بارگذاری کنید. برای این منظور از دستور زیر استفاده کنید.

```
cisco#copy tftp: flash
Address or name of remote host []? 10.10.10.2
Source filename []? c3560-ipbasek9-mz.122-40.SE.bin
Destination filename [c3560-ipbasek9-mz.122-40.SE.bin]?
Accessing tftp://10.10.10.2/c3560-ipbasek9-mz.122-40.SE.bin....
Loading c3560-ipbasek9-mz.122-40.SE.bin from 10.10.10.2 (via Vlan1)
OK - 8295106 bytes
bytes copied in 124.571 secs (66589 bytes/sec) ۸۲۹۵۱۰۶
```

پس از اتمام نصب و انتقال IOS ، دستگاه خود را مجدد بوت نمایید تا از اجرا شدن آخرین نسخه IOS مطمئن شوید.

```
cisco(config)# boot system flash:/c3560-ipbasek9-mz.122-40.SE.bin
```

اکنون دستگاه خود را Reload نمایید.

```
cisco# reload
```

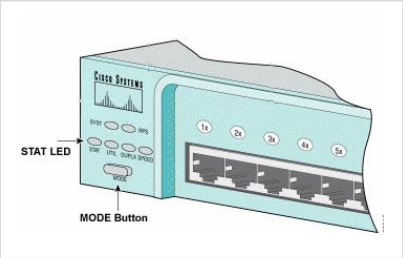
پس از بوت شدن دستگاه سیسکو خود باید از اینکه آخرین نسخه IOS نصب شده است اطمینان حاصل نمایید لذا از دستور زیر استفاده کنید.

```
cisco# show version
```

پس از انجام این تنظیمات شما دارای سیستم عامل جدید در دستگاه سیسکو خود خواهید شد.

Switch Password Recovery

با توجه به اینکه هر سازمان به تناسب مسئولیت و جایگاه خود از منابع و تجهیزات گوناگونی استفاده می نماید و حدود دسترسی و لایه های امنیتی متعددی را با در نظر گرفتن استانداردهای فنی به منظور حفاظت و حراست از آنها در سازمان پیاده سازی و اجرا می کند، برخی مواقع به دلیل برخی مشکلات و یا خطاهای انسانی بروز رسانی مستندات و آرشیو فنی انجام نمی شود و به همین دلیل راه کارهای خاصی برای خروج از چالش بوجود آمده توسط تولیدکنندگان تجهیزات در سیستم ها تعبیه شده است که عمومیت نداشته و می بایست به مستندات فنی محصول مورد نظر و یا مکاتبه با تولید کننده اقدام نمود. قطعاً تا کنون با راهکارهای امنیتی متعدد ارائه شده به منظور دسترسی به سوییچ و انجام تنظیمات بر روی آن آشنا شده اید. با فرض اینکه Admin و نماینده او تنها کسانی هستند که به صورت فیزیکی امکان حضور و یا دسترسی به منابع و تجهیزات شبکه را دارند این راهکارها قابل انجام می باشد.



سیسکو قابلیتی را در سوییچ قرار داده است که Admin می تواند پس از روشن کردن سوییچ و آماده به کار شدن آن با نگاه داشتن کلید Mode به مدت بیست ثانیه اقدام به Reset نمودن سوییچ نماید. شایان ذکر است پس از این عمل کلیه تنظیمات و Config های انجام شده بر روی سوییچ کاملاً حذف خواهد شد و تنها با برگرداندن نسخه پشتیبان احتمالی دسترسی و برگرداندن تنظیمات امکان پذیر خواهد شد.

اما اگر بخواهیم فقط رمز فراموش شده را حذف کنیم و کلیه تنظیمات دست نخورده باقی بماند چه باید کرد؟ بخاطر داشته باشید که حذف تنظیمات یک سوییچ در یک سازمان می تواند هزینه و لطمات زیادی را به همراه داشته باشد. بدین خاطر سعی خواهیم کرد تا با استفاده از روش دیگری به رفع این مشکل بپردازیم.

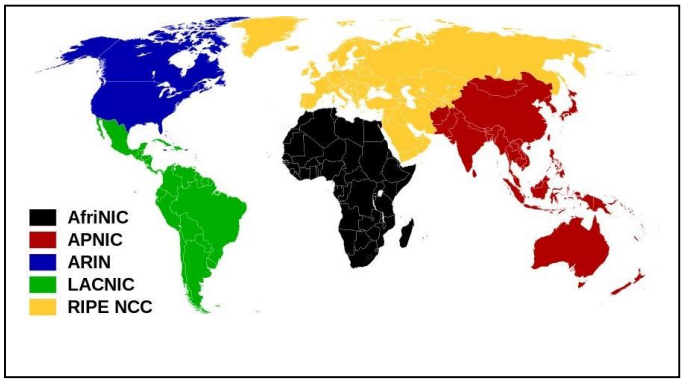
```
C2955 Boot Loader (C2955-HBOOT-M) Version 12.1(0.0.514), CISCO DEVELOPMENT TEST
VERSION
Compiled Fri 13-Dec-02 17:38 by madison
WS-C2955T-12 starting...
Base ethernet MAC Address: 00:0b:be:b6:ee:00
Xmodem file system is available.
Initializing Flash...
flashfs[0]: 19 files, 2 directories
flashfs[0]: 0 orphaned files, 0 orphaned directories
flashfs[0]: Total bytes: 7741440
flashfs[0]: Bytes used: 4510720
flashfs[0]: Bytes available: 3230720
flashfs[0]: flashfs fsck took 7 seconds.
...done initializing flash.
Boot Sector Filesystem (bs:) installed, fsid: 3
Parameter Block Filesystem (pb:) installed, fsid: 4

*** The system will autoboot in 15 seconds ***
Send break character to prevent autobooting.


!--- Wait until you see this message before
!--- you issue the break sequence.
!--- Ctrl+Break is entered using Hyperterm.


The system has been interrupted prior to initializing the flash file system to finish
loading the operating system software:

flash_init
load_helper
boot
switch:
```

ابتدا از طریق کنسول به سوییچ متصل می شویم و جهت اطمینان اطلاعات running-config را ذخیره می نماییم. هنگامیکه ما اطلاعات حافظه را از طریق copy و یا دستور wr دخیره می کنیم، فایلی به نام config.text در nvram سوییچ ساخته می شود و رمزها نیز در آن ذخیره شده است. برای دور زدن این فایل سوییچ را خاموش کرده و همزمان با روشن کردن مجدد آن، کلید Mode را برای ۵ ثانیه فشرده و نگاه می داریم (نیازی به فشار زیادی نیست!). پس از آن سوییچ وارد محیط دیگری می شود که محیط IOS نیست و سوییچ آمادگی خود را با نشان دادن ": switch" مشخص می نماید. در هر مرحله می توان از دستور dir برای مشاهده فهرست فایل های موجود بر روی سوییچ استفاده نمود. دستور flash_init را تایپ و اجرا کرده تا برخی از تنظیمات اولیه IOS اجرا شود. دستور ip_helper در برخی مدل های قدیمی کارآیی دارد. پس از آن با دستور rename فایل flash:config.text را به flash:config.old تغییر نام می دهیم. سپس دستور boot را تایپ و اجرا می کنیم. در برخی از سوییچ ها چون فایل config وجود ندارد ممکن است برای انجام تنظیمات سوالی پرسیده شود که به آن پاسخ منفی بدهید. پس از این مرحله Admin می تواند با rename نمودن فایل config.old به config.text تنظیمات گذشته سوییچ را از حذف نجات دهد ولی هنوز کارهای دیگری باقیست و یک اشتباه می تواند تمام مراحل طی شده را از بین ببرد. Admin بایستی فایل flash:config.text را بر روی system:running-config کپی نموده و سپس نسبت به تغییر رمزهای ورود به سوییچ و یا رمز ورود به مرحله global اقدام نماید و در خاتمه عملیات از دستور wr و یا copy running-config startup-config استفاده می کنیم. برای اطمینان خاطر سوییچ را مجدداً راه اندازی می نماییم.

```
Switch#copy flash:config.text system:running-config
Destination filename [running-config]?

!--- Press Return or Enter.

1131 bytes copied in 0.760 secs
Sw1#
```

فصل دهم

یادآوری IPV4:



در ابتدا که استاندارد های شبکه وب تعریف گردید، از اعدادی بر مبنای ۳۲ بیت برای ایجاد شماره های IP استفاده شد که به آن، آدرس های اینترنتی نسخه ۴ می گویند (IPv4 یا Internet Protocol Version 4)، در این نسخه که هم اکنون نیز در حال استفاده است، از ترکیب اعداد بر مبنای ۳۲ بیت نهایتا تا سقف ۴,۳ میلیارد (۴,۲۹۴,۹۶۷,۲۹۶) آدرس اختصاصی قابل ایجاد است، از طرفی در این نسخه از آدرس های پروتکل اینترنت تعداد ۱۸ میلیون آدرس برای شبکه های شخصی (private networks شامل سری ۱۰,۰,۰,۰ الی ۱۰,۲۵۵,۲۵۵,۲۵۵ تعداد ۱۶۷۷۷۲۱۶ آی پی آدرس، ۱۷۲,۱۶,۰,۰ الی ۱۷۲,۳۱,۲۵۵,۲۵۵ تعداد ۱۰۴۸۵۷۶ آی پی آدرس و ۱۹۲,۱۶۸,۰,۰ الی ۱۹۲,۱۶۸,۲۵۵,۲۵۵ تعداد ۶۵۵۳۶ آی پی آدرس) و ۲۷۰ میلیون آدرس نیز برای کامپیوترهای میزبان شبکه (multicast) اختصاص داده شد (multicast به طور ساده به معنی تکنیکی است که در آن با اختصاص یک IP به یک ابر سرور، امکان پشتیبانی از تعداد زیادی سرورهای زیر مجموعه با آن فراهم می شود، multicast ها در واقع به نوعی سرورهای اصلی وب محسوب می شوند).

ساختار IP نسخه ۴

از لحاظ بررسی ساختاری، IP های نسخه چهار از چهار قسمت مجزا تشکیل می شوند که بین آنها یک نقطه (.) قرار می گیرد، در هر قسمت نیز می توان از یک عدد ۱ تا ۳ رقمی استفاده کرد (۸ بیت) که شامل ۰ تا ۲۵۵ می شود (این اعداد بر مبنای باینری محاسبه شده اند)، به طور مثال: ۴۶,۲۱,۸۸,۱۶۶ یا به فرض آی پی پیش فرض ابزارهایی که به شبکه متصل نیستند به صورت ۱۲۷,۰,۰,۱ است که به آن localhost نیز می گویند، به این ترتیب هر وسیله ای که به اینترنت متصل می شود، دارای یک شماره شناسایی خاص و یکتا است که موقعیت آن را (یا در بیشتر موارد موقعیت سرویس دهنده آن را) مشخص می کند، اما شاید این سوال به ذهنتان برسد که کشور و موقعیت کاربر را چگونه از شماره آی پی آن بدست می آورند؟ پاسخ این است که اطلاعات هرIP از دو قسمت تشکیل شده است، قسمت مربوط به شبکه یا سرور و قسمت مربوط به وسیله ای که به شبکه متصل است، به طور مثال سه قسمت اول یک IP ممکن است نشانگر ISP باشد که به شما سرویس اینترنت ارائه می دهد و عدد آخر نشانگر شماره وسیله ای است که به آن سرویس دهنده متصل شده است، لذا ممکن است چند IP متفاوت به شکل نمونه زیر از یک خدمات دهنده اینترنت داشته باشیم:

۴۶,۲۱,۸۸,۱۶۸ - ۴۶,۲۱,۸۸,۱۶۷ - ۴۶,۲۱,۸۸,۱۶۶

از آنجایی که اطلاعات سرویس دهنده اینترنت و مالک حقیقی آی پی در منبع رسمی، مستقل و بین المللی ارائه دهنده مجوز آدرس های اینترنتی ICANN یا (International Company for the Assignment of Names and Numbers) ثبت شده است، لذا هویت آن نیز مشخص و در دسترس است و از طرفی اطلاعات مشترکین نیز درISP موجود است، لذا اگر شرایط اقتضاء کند، می توان موقعیت دقیق کاربر را مشخص کرد (البته برای عموم معمولا تنها موقعیت ISP قابل ردیابی است، اما برای سازمانهای امنیتی، موقعیت کاربران نیز در شرایطی قابل دستیابی است)، باید توجه داشت که معمولا ISP ها از پروتکل DHCP یا (Dynamic Host Configuration Protocol) استفاده می کنند، بدین معنی که با هر بار اتصال شما به اینترنت، به صورت داینامیک یکی از آدرس های آزاد شده به شما اختصاص پیدا می کند و با قطع اتصال، ممکن است IP مورد نظر به فرد دیگری اختصاص داده شود، لذا IP در این نوع خود، یک شماره همیشگی نیست و در هر اتصال معمولا متفاوت خواهد بود (به این نوع آی پی ها به اصطلاح داینامیک می گویند).

کلاس های مختلف IP، راهنما و نحوه تبدیل از باینری به دسیمال و بالعکس و نیز روش and نمودن دو IP در جداول زیر درج گردیده است.

Class	Binary	Start Address	End Address	Octet1 8 bit	Octet2 8 bit	Octet3 8 bit	Octet4 8 bit	Network Formula	Host Fomula
A	10000000	1.0.0.0	127.255.255.255	11111111	00000000	00000000	00000000	2^(8-1)	(2^24)-2
B	11000000	128.0.0.0	191.255.255.255	11111111	11111111	00000000	00000000	2^(8-2)	(2^16)-2
C	11100000	192.0.0.0	223.255.255.255	11111111	11111111	11111111	00000000	2^(8-3)	(2^24)-2
D	11110000	223.0.0.0	239.255.255.255	Mulicast					
E	11111000	240.0.0.0	255.255.255.255	Resereved					

.

Class	Defaul Subnet Mask				CIDR
A	255	0	0	0	/8
B	255	255	0	0	/16
C	255	255	255	0	/24

Class	Private IP Addresses Start	End	Networks
A	10.0.0.0	10.255.255.255	1
B	172.16.0.0	172.16.255.255	16
C	192.168.0.0	192.168.255.255	256

.

bit position and its vlaue							
8	7	6	5	4	3	2	1
2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
128	64	32	16	8	4	2	1
۱۲۸	۰	۰	۰	۰	۰	۰	۰
۱۹۲		۰	۰	۰	۰	۰	۰
۲۲۴			۰	۰	۰	۰	۰
۲۴۰				۰	۰	۰	۰
۲۴۸					۰	۰	۰
۲۵۲						۰	۰
۲۵۴							۰
۲۵۵							

.

IPv4 Calculation																															
11000000								**10101000**								**00010100**								**00000001**							
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	32
8	7	6	5	4	3	2	1	8	7	6	5	4	3	2	1	8	7	6	5	4	3	2	1	8	7	6	5	4	3	2	1
128	64	32	16	8	4	2	1	128	64	32	16	8	4	2	1	128	64	32	16	8	4	2	1	128	64	32	16	8	4	2	1
1	**1**	**0**	**0**	**0**	**0**	**0**	**0**	**1**	**0**	**1**	**0**	**1**	**0**	**0**	**0**	**0**	**0**	**0**	**1**	**0**	**1**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**1**
192								**168**								**20**								**1**							

.

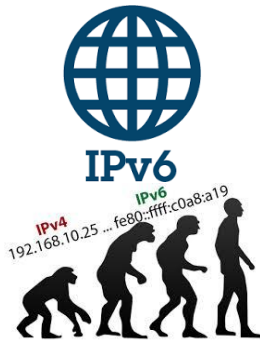
And				/20	172								16								180								163							
۰	۰	=	0	Mask	255								255								248								0							
۱	۰	=	0	IP	1	0	1	0	1	1	0	0	0	0	0	1	0	0	0	0	1	0	1	1	0	1	0	0	1	0	1	0	0	0	1	1
0	1	=	0	Mask	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0
۱	۱	=	1	And	1	0	1	0	1	1	0	0	0	0	0	1	0	0	0	0	1	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0
Net_ID					172								16								176								0							
First_IP					172								16								176								1							
Last_IP					172								16								208								254							
Broadcast					172								16								208								255							
Next Net_ID					172								16								209								0							

آدرس Loopback : ۱۲۷,۰,۰,۱

heydari.farzad@gmail.com نام مدرس دوره: مهندس فرزاد حیدری

تهیه و گردآوری: دانیال نامورکهن

IP نسخه ۶ چیست؟



با توجه به افزایش دستگاه‌هایی که از پروتکل اینترنت استفاده می‌کنند، در آینده نزدیک هیچ آی پی آدرس نسخه ۴ ای آزاد باقی نخواهد ماند. بنابراین برای افزایش تعداد آی پی های آزاد، نسخه ۶ آن با نام IPv6 طراحی شد؛ این نسخه در مقابل نسخه ۴ دارای دامنه بسیار گسترده‌ای است. به دلیل تازه بودن این نسخه، استفاده از آن گسترده نیست و نسخه ۴ تقریباً به صورت کامل نیازهای آی پی آدرس را تامین می‌کند. به عبارت دیگر تقریباً ۹۶ درصد کل ترافیک اینترنت از آی پی آدرس های نسخه ۴ استفاده می‌کنند. اما در آینده نزدیک حتماً به این نسخه از آی پی ها نیاز خواهیم داشت.

مفاهیم IP نسخه ۶:

- ✓ آدرس دهی های IPv6 به صورت ۱۲۸ بیتی می باشند که بر خلاف آدرس دهی های IPv4 که ۳۲ بیتی می باشند تعداد زیادی آدرس IP را در اختیار قرار می دهند.
- ✓ تعداد آدرس IP در IPv6 چیزی در حدود ۳۴۰,۲۸۲,۳۶۶,۹۲۰,۹۳۸,۴۶۳,۴۶۳,۳۷۴,۶۰۷,۴۳۱,۷۶۸,۲۱۱,۴۵۶ می باشد.
- ✓ ویژگی های متعددی به این نسخه از آدرس دهی اضافه گردید که شامل موارد زیر می باشند:
  - ✓ ویژگی های خاص آدرس دهی بدون نیاز به DHCP یا Static Addressing
  - ✓ پشتیبانی از Renumbering
  - ✓ پشتیبانی از Mobility در تغییرات شبکه به صورت سیار و مباحث Routing
  - ✓ استفاده از آدرس های Public مستقل از ISP ها (عدم تغییر آدرس Public شما با تغییر سرویس دهنده اینترنت شما)
  - ✓ عدم نیاز به NAT و PAT
  - ✓ استفاده از ویژگی IPSec در هدر این آدرس دهی ها و امن شدن آینده اینترنت
  - ✓ بهینه سازی در ساختار Header این نوع IP
  - ✓ عدم حضور Broadcast در این ساختار آدرس دهی
  - ✓ وجود ابزارهای متعدد برای مهاجرت از IPv4 به IPv6 و یا استفاده از هر دو در یک شبکه

ساختار IP نسخه ۶:

در نسخه ۶، آی پی آدرس ها یک عبارت ۱۲۸ بیتی (شامل ۸ بخش ۱۶ بیتی) بوده و هر بخش یا Quarter به وسیله کاراکتر دو نقطه (:) از هم جدا می‌شوند. ساختار IPv6 نسبت به IPv4 پیچیده تر بوده و یک IP آدرس نسخه ۶ مانند عبارت زیر است:

F0A0:9002:E051:0000:0000:0000:C91D:۲۶۰۱

خلاصه سازی اول: درصورتی که در ابتدای بخش رقم صفر (۰) قرار بگیرد، می‌توان آن را نادیده گرفت برای مثال آدرس F925:00C4 می‌تواند تبدیل به F925:C4 شود. دقت کنید که این تنها یک مثال است و فقط دو بخش مورد بررسی قرار گرفته است.

خلاصه سازی دوم : بخش‌هایی که به وسیله کاراکتر کولون ":" از هم جدا می‌شوند، شامل اعداد و حروف استاندارد هگزادسیمال (حروف A, B, C, D, E, F) که از محدوده ۰۰۰۰ تا FFFF قابل تغییر هستند. برای راحتی در خواندن این عبارت، قسمت‌هایی که دارای چهار رقم صفر هستند می‌توانند حذف شوند. توجه کنید که این خلاصه سازی در طول آدرس آی پی فقط یک بار می‌تواند انجام شود. بنابراین ساده شده آی پی آدرس بالا، عبارت زیر است:

F0A0:9002:E051::C91D:۲۶۰۱

همان طور که گفته شد این عبارت‌ها برای کامپیوتر هیچ مفهومی نداشته و باید تبدیل به عبارت باینری شوند. در این تبدیل مقادیر هر بخش به یک عبارت ۱۶ بیتی تبدیل می‌شود. یعنی تبدیل شده باینری عبارت بالا کد زیر است:

0010011000000001:1111000010100000:1001000000000010:1110000001010001:0000000000000000:0000000000:1100100100011101

دلیل این که هر بخش تبدیل به یک عبارت ۱۶ بیتی می‌شود، این است که هر کاراکتر در هر بخش با توجه به جدول تبدیل هگزادسیمال، به یک عبارت چهار رقمی باینری تبدیل می‌شود. یعنی بخش اول (۲۶۰۱) تبدیل به ۰۰۱۰۰۱۱۰۰۰۰۰۰۰۰۱ می‌شود. بنابراین با کنار هم قرار دادن این ۴ رقم، ما در هر بخش ۱۶ بیت خواهیم داشت. با استفاده از جدول تبدیل هگزادسیمال به باینری زیر، می‌توانید به راحتی آدرس IPv6 را به باینری تبدیل کنید:

جدول هگزادسیمال (Hexadecimal) باینری (Binary)

Bin	0000	0001	0010	0011	0100	0101	0110	0111	1000	1001	1010	1011	1100	1101	1110	1111
Hex	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**A**	**B**	**C**	**D**	**E**	**F**

نحوه آدرس دهی در IPv6:

نحوه آدرس دهی (Addressing) که مولتی کستینگ (Multicasting - چند بخشی) نیز نامیده می‌شود، روش و تکنولوژی‌ای است که برای ارسال یک پاکت داده به چندین مقصد در طی یک فرایند ارسال در داخل یک شبکه مورد استفاده قرار می‌گیرد. با استفاده از قابلیت مولتی کستینگ پهنای باند مصرف شده در داخل شبکه کاهش یافته و زمان فرایند ارسال به چندین مقصد و همچنین فشار پردازشی داخل شبکه به شدت بهینه خواهد شد. طبق استاندارد RFC3307 نحوه مسیر دهی در پروتکل اینترنت ورژن ۶ به سه حالت زیر تقسیم می‌شود:

Unicast: روش انتقالی است که در آن داده‌ها از یک مبدا به تنها یک مقصد مشخص در داخل شبکه فرستاده می‌شوند؛ مانند آن که به صورت مستقیم به یک شخص مشخص نامه می‌فرستیم.

Anycast: روش انتقالی است که در آن مقصد به یک گروه مشخص ازگره‌ها (Nodes) که ممکن است در مکان‌های مختلفی باشند پاکت را مسیر دهی می‌کند اما در آن مسیر یاب یک نزدیک ترین و بهترین گره‌ای که پاکت می‌تواند به آن برسد را انتخاب کرده و پاکت را تنها به آن ارسال می‌کند البته ممکن است به گره‌هایی که دارای آدرس مقصد یکسانی باشند نیز فرستاده شود؛ این روش مانند آن است که نیاز به یک خودکار با برند مشخص (همان گره‌های یک گروه) داشته باشیم که در قسمت‌ها مختلف یک اتاق پراکنده شده اند و ما نزدیک ترین و در دسترس ترین آن را بر می‌داریم.

Multicast: روش انتقالی است که طی آن پاکت داده از یک مبدا به گروهایی در یک گروه فرستاده می‌شود و هر گره این پاکت را تنها یک بار دریافت می‌کند، مانند آن که پشت بلندگویی ایستاده‌ایم و خطاب به یک گروه خاص، مطلبی را می‌گوییم.

Type of address	Purpose	Prefix	Easily seen Hex Prefix
Global unicast	Like Public Address in IPV4	2000::/3	2 or 3
Unique local	Like Private Address in IPV4	FD00::/8	FD
Link local	Packets Sent in the local Subnet	FE80::/10	FE8
Site local	Not Usable anymore like unique local	FEC0::/10	FEC,FED,FEE,FEF
Unspecified	Appipa Address	::/128	N/A
Loopback	Like 127.0.0.1 in IPV4	::1/128	N/A

آشنایی با Link Local :

Link Local آدرسی است که به صورت اتوماتیک بعد از فعالسازی IPv6 بر روی روتر Generate می شود و موارد مصرف آن برای:

- به عنوان آدرس ارسال کننده RS و RA برای شناسایی روتر استفاده می شود
- مورد استفاده برای پروتکل NDP
- به عنوان آدرس های Next-Hop در پروتکل های روتینگ

- **نکته:** محدوده آدرس دهی برای Link Local به صورت FE80::/10 می باشد که شامل آدرس هایی می شود که با FE8, FE9, FEA, FEB شروع می شوند.

خلاصه سازی IP Address نسخه ۶ در یک نگاه

۰۰۱۰۰۰۰۱۰۰۰۰۱۱۱۱:۰۰۰۰۰۰۰۰۰۰۰۰۰۰۰۰:۰۰۰۰۰۰۰۰۰۰۰۰۰۰۰۰:۱۱۰۰۱۱۰۰۱۱۰۰۱۱۰۰:۰۰۰۰۰۰۰۰۰۰۰۰۰۰۰۰:۰۰۰۰۰۰۰۰۰۰۰۰۱۱۰۰							
Quarter							
۱	۲	۳	۴	۵	۶	۷	۸
۰۰۱۰۰۰۰۱۰۰۰۰۱۱۱۱	۰۰۰۰۰۰۰۰۰۰۰۰۰۰۰۰	۰۰۰۰۰۰۰۰۰۰۰۰۰۰۰۰	۰۰۰۰۰۰۰۰۰۰۰۰۰۰۰۰	۱۱۰۰۱۱۰۰۱۱۰۰۱۱۰۰	۰۰۰۰۰۰۰۰۰۰۰۰۰۰۰۰	۰۰۰۰۰۰۰۰۰۰۰۰۰۰۰۰	۰۰۰۰۰۰۰۰۰۰۰۰۱۱۰۰
210F	0000	0000	0000	CCCC	0000	0000	000D
210F	0	0	0	CCCC	0	0	D
210F	0			CCCC	0	0	D
210F::CCCC:0:0:D							

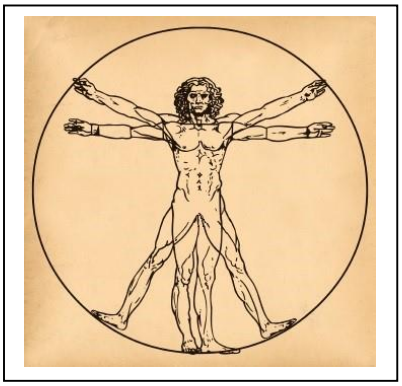
IPV4	32 bit	Net ID	Host ID	CIDR
IPV6	128 bit	Prefix	Interface ID	Prefix Lengh

جهت دریافت اطلاعات بیشتر در خصوص مقایسه دو پروتکل IPv4 و IPv6 به لینک زیر مراجعه نمایید:

https://www.ibm.com/support/knowledgecenter/ssw_i5_54/rzai2/rzai2compipv4ipv6.htm

فصل یازدهم

آشنایی بیشتر با Router



Router یکی از دیوایس های مورد استفاده در شبکه می باشد که در لایه ی سوم OSI (لایه Network) کار می کند. Router بین شبکه های مختلف مسیر یابی می کند و دقیقا به همین دلیل باید حداقل دو عدد اینترفیس داشته باشد که Net ID های آنها حداقل یک بیت با هم فرق داشته باشند. به همین خاطر برای درک ساده تر مطالب آتی interface های یک پورت را همانند دست های یک انسان تصور نمایید (مرد ویترو وین داوینچی). شرکت های زیادی هستند که تجهیزات شبکه مانند Router و دیگر دیوایس های مورد استفاده را تولید می کنند به این سبب Router ها نیز برند ها و مدل های مختلفی دارند اما همانطور که همه می دانید بهترین شرکت تولید کننده تجهیزات شبکه، شرکت Cisco است که نه تنها تجهیزات بلکه صادر کننده علم شبکه به دنیا نیز می باشد.

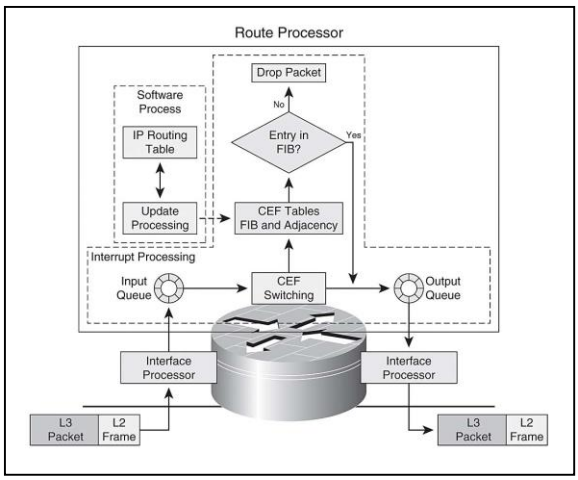
Routing علمی است که Cisco به دنیا معرفی کرد و کاریست که روتر ها برای ما انجام می دهند. به طور کلی Routing به معنی ارسال بسته از مبدا به مقصد بر اساس پروتکل ها ،آدرس لایه سومی (IP) و Routing Table یک روتر می باشد.

تفاوتهای مابین سوییچ و روتر (کلیات)		
Title	**Router**	**Switch**
Technical Specification	Routers Operate at Layer 3 of OSI Model	Routers Operate at Layer 2 , (3) of OSI Model
Table	Store IP Address in Routing Table	Store MAC Address in Lookup Table
Used in	LAN, WAN	LAN
Ports	2 / 4 / 8	Multiport Bridge 24 /48 & more
Data Transmission Form	Packet	Frame (L2 Switch) Frame & Packet (L3 Switch)
Collision	Less	In Full Duplex Switch no Collision Occur
Routing Decision	Take Faster Router Decision	Take more time for complicated routing decision
NAT	Can Perform NAT	Can not Perform NAT
On/Off Button	Yes	No
Ports Situation Default	Shutdown	Ready or UP
Broadcast	Drop	Flood
AUX Connection	Yes, Use by Modem	No
First Interface Number	0	1
Ready to Use	No, Need to Configure & Setting	Basic Yes ,(Advance ,No , Need to Configuration)

هنگامی که یک روتر را خریداری و برای اولین بار روشن می کنید به صورت پیش فرض کاری انجام نمی دهد یعنی نیاز است که همه کار ها و دستورات به آن داده شود.پس ابتدا اینترفیس های روتر را روشن کرده و بر اساس تشخیص مهندس شبکه، IP های مورد نظر به اینترفیس ها داده و Routing Protocol مناسب بروی آن router راه اندازی می شود. حال زمانی را در نظر بگیرید که بسته ای به روتر می رسد، در این حالت ابتدا روتر به Routing Table خود نگاه می کند چنانچه Route و یا مسیری برای آن مقصد مورد نظر داشته باشد، بسته را route می کند و اگر مسیری در Routing table نداشته باشد، default gateway را بررسی میکند. در صورتی که set شده باشد، بسته به آن سمت هدایت می شود در غیر این صورت بسته drop خواهد شد.

نکته : عملیات Routing تنها توسط روتر انجام نمی شود بلکه switch هایی نیز وجود دارند که این کار را انجام می دهند ودر اصطلاح به آنها MLS که مخفف شده عبارت Multi Layer Switch است، گفته می شود. MLS ها قابلیت کارکرد در لایه های دوم و سوم OSI و همچنین دید نسبت به لایه چهارم را دارند.

مروری بر عملکرد Router و چگونگی هدایت و انتقال اطلاعات



روتر Router سخت افزار یا نرم افزاری است که به منظور مدیریت بسته های اطلاعاتی (Data Packet) و هدایت آنها به پیش طراحی و ساخته شده است. روترها با استفاده از جدول مسیریابی در برقراری ارتباط بین کامپیوترها، چه در شبکه های شخصی در منازل و چه در شبکه های بزرگ و پیچیده، نقش حیاتی ایفا می کنند.

ملاحظات درک چگونگی عملکرد اینترنت برای فهم و درک نقش روتر کلیدی است. اینترنت یک شبکه بزرگ و جهانی متشکل از کامپیوتر هاست که از طریق آن می توان به اطلاعاتی که بر روی کامپیوترهای مختلف در اقصی نقاط کره خاکی ذخیره شده است دست یافت. انتقال اطلاعات (دیتا Data) بر روی شبکه اینترنت توسط پروتکل شبکه ای TCP/IP انجام می گیرد. این پروتکل برای نقل و انتقال اطلاعات بر روی اینترنت طراحی و ساخته شده است. برمبنای TCP/IP پیش از آنکه اطلاعات بر روی اینترنت منتقل شوند، ابتدا به تکه های کوچکتر که به آنها بسته packet گفته می شود تقسیم می شوند. این بسته ها در لایه ۳ علاوه بر دارا بودن اطلاعات کاربر، آدرس گیرنده (Source) و فرستنده (Destination) را نیز در پوششی بنام IP-Header حفظ می کند.

روترها در ارتباط با این «بسته» ها (Packets) و هدایت (Route) آنها وارد عمل می شوند. در پوشش IP-Header هر بسته اطلاعاتی، مشخصات ایستگاه گیرنده آن مشخص شده است. روتر پس از خواندن آدرس گیرنده، بر اساس جدول مسیریابی (Routing Table) و الگوریتم های مسیریابی و با توجه به بار ترافیک و سایر پارامترها (Load, Bandwidth, Delay , …) شبکه، بسته را از کوتاهترین و کم ترافیک ترین مسیر به مقصد می رساند و چنانچه در جدول مسیرها، مقصد یا مسیر درخواستی را پیدا نکند برخلاف سوییچ (که آن بسته را به تمامی پورت ها ارسال می کند) آن بسته را Drop می کند. روترها برای تشخیص مسیر مناسب، توسط پروتکل هایی که از قبل تعیین شده و توافق بین المللی در مورد آن وجود دارد، با یکدیگر ارتباط برقرار می کنند. عملکرد روتر ارتباط بین کامپیوتر های داخل هر شبکه با یکدیگر و با کامپیوترهای شبکه های دیگری که متصل به اینترنت باشند را ممکن می سازد. وظیفه روتر هدایت بسته های اطلاعاتی به مقصد است. روتر ها حلقه های رابط بین شبکه های کامپیوتری متصل به اینترنت هستند و مسولیت تعیین کوتاه ترین و یا بهترین مسیر عبور بسته های اطلاعاتی را برعهده دارند. روترها در انواع مختلف و با توانایی های متفاوتی عرضه می شوند. پیشرفته ترین روترها در نقاط کلیدی اینترنت مسوولیت بیشتری برعهده دارند تا روترهای ساده تر که در شبکه های خصوصی در منازل بکار می روند.

انواع مسیردهی در روتر : استاتیک (ایستا) و داینامیک (پویا).

۱. **Static Route**:

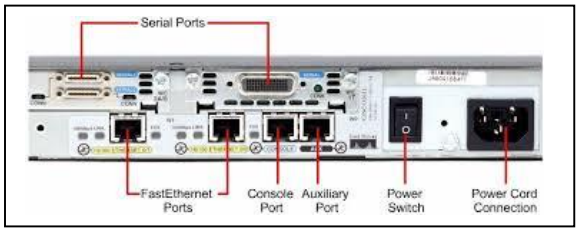
در واقع Route ای است که بصورت دستی توسط مدیر شبکه ایجاد می شود. Static Route ها معمولا در شبکه های کوچک استفاده می شوند. در ساختار Static Routing تمامی Routing Table موجود در Router ها بصورت دستی توسط مدیر شبکه بروز رسانی و ایجاد می شوند. ساختار Dynamic Routing کاملا مخالف ساختار Static Routing است ، در Dynamic Routing تمامی اطلاعات مربوط به Route های موجود در Routing Table ها با استفاده از Routing Protocol ها انجام می شود. تنها مزیتی که در Static Routing وجود دارد این است که به نسبت Dynamic Routing روترهای موجود در مجموعه پردازشی برای روتر ایجاد نمی کنند و ترافیک و Load کاری کمتری بر روی روترهای موجود در مجموعه قرار می گیرد. در این حین بزرگترین عیبی که در Static Routing وجود دارد این است که تغییرات بایستی بصورت دستی به تک تک روتر های موجود در مجموعه توسط مدیر شبکه اعمال شود و این باعث بروز اشتباهات فردی و همچنین بالا رفتن Load کاری مدیر شبکه می شوند ، همچنین در شبکه هایی که دارای ساختار پیچیده هستند یا در اصطلاح Complex Network ها پیاده سازی static routing بسیار دشوار است.

Router1(Config)# ip route NET_ID Subnet_MASK Route

۲. **Dynamic Route**:

مسیریابی داینامیک از طریق بکارگیری Routing Protocols و انجام تنظیمات اولیه که پس از آن نیازی به دخالت یک Admin ندارد و جدول مسیریابی آن بطور خودکار، با استفاده از پروتکل های مسیریابی پویا بروز می شود تا بتواند بسته های اطلاعاتی رسیده را به مقصد بعدی هدایت کند. خاصیت مسیر دهی داینامیک روتر این است که جدول مسیریابی اش را همواره با جدول مسیریابی روترهای نزدیک به خود مبادله می کند و از تغییرات آنها مطلع است. تصور کنید اگر شما به عنوان Admin شبکه سازمانی یا فروشگاهی با ۴۰۰۰ شعبه یا دفاتر فروش بخواهید Routing Table تمامی Router های شبکه را به صورت دستی و Static تنظیم نمایید یا مسیر جدیدی را به/ از مسیرهای قبلی اضافه/ کم نمایید..(God bless you!!!). ویژگی های روترها را می توان با سرویس های ضروری و کارآیی های خاص مورد نیاز هر شبکه ادغام کرد تا مثلاً آن شبکه امن تر شده و بر سرعت انتقال ترافیک آن اضافه شود.

انواع اینترفیس های روتر



اینترفیس ها مسئولیت اتصالات روتر مابین شبکه های داخلی و دنیای خارج را برعهده داشته و می توان آنان را به سه گروه عمده تقسیم نمود:

۱. **اینترفیس های مختص شبکه محلی** : با استفاده از اینترفیس های فوق یک روتر می تواند به محیط انتقال شبکه محلی متصل گردد. اینگونه اینترفیس ها معمولاً نوع خاصی از اترنت (Ethernet, Fast , Gig) می باشند. در برخی موارد ممکن است از سایر تکنولوژی های LAN نظیر Token Ring و یا ATM (برگرفته از Asynchronous Transfer Mode) نیز استفاده گردد. در اکثر محیط های LAN ، روتر با استفاده از یک اینترفیس Ethernet و یا Fast Ethernet به شبکه متصل می گردد. در چنین مواردی روتر همانند یک میزبان است که با شبکه LAN از طریق یک هاب و یا سوئیچ ارتباط برقرار می نماید. به منظور ایجاد اتصال از یک کابل straight-through استفاده می شود. دربرخی موارد، اتصال اترنت روتر مستقیماً به کامپیوتر و یا روتر دیگری متصل می گردد. در چنین مواردی از یک کابل Crossover استفاده خواهد شد.

۲. **اینترفیس های مختص شبکه WAN**: این نوع اینترفیس ها اتصالات مورد نیاز از طریق یک ارائه دهنده سرویس به یک سایت خاص و یا اینترنت را فراهم می نمایند. اتصالات فوق ممکن است از نوع سریال و یا هر تعداد دیگر از اینترفیس های WAN باشند. در زمان استفاده از برخی اینترفیس های WAN ، به یک دستگاه خارجی نظیر CSU به منظور اتصال روتر به اتصال محلی ارائه دهنده سرویس نیاز می باشد. در برخی دیگر از اتصالات WAN، ممکن است روتر مستقیماً به ارائه دهنده سرویس متصل گردد. اتصالات WAN دارای انواع مختلفی بوده و از تکنولوژی های متفاوتی استفاده می نمایند.

سرویس های WAN معمولاً از ارائه دهندگان سرویس اجاره می گردد. خطوط leased و یا packet-switched نمونه هائی از انواع متفاوت اتصالات WAN می باشند. برای هر یک از انواع سرویس های WAN ، دستگاه مشتری (اغلب یک روتر است) به منزله یک DTE (Data Terminal Equipment) رفتار می نماید. پایانه فوق با استفاده از یک دستگاه DCE (برگرفته از Data Circuit-terminating Equipment) که معمولاً یک مودم و یا CSU/DSU (Channel Service Unit/Data Service Unit) می باشد به ارائه دهنده سرویس متصل می گردد. از دستگاه فوق برای تبدیل داده از DTE به یک شکل قابل قبول برای ارائه دهنده سرویس WAN، استفاده می گردد. اینترفیس های سریال ، متداولترین اینترفیس استفاده شده در روتر برای سرویس های WAN می باشند (نهایتاً 1.5 Mb/s). برای انتخاب کابل سریال مناسب، بررسی و شناسایی نوع اینترفیس ضروریست. روترهای سیسکو ممکن است از کانکتورهای متفاوتی برای اینترفیس های سریال استفاده نمایند . مثلاً در برخی روترها از اینترفیس های سریال smart و یا یک اتصال DB-60 استفاده می گردد.

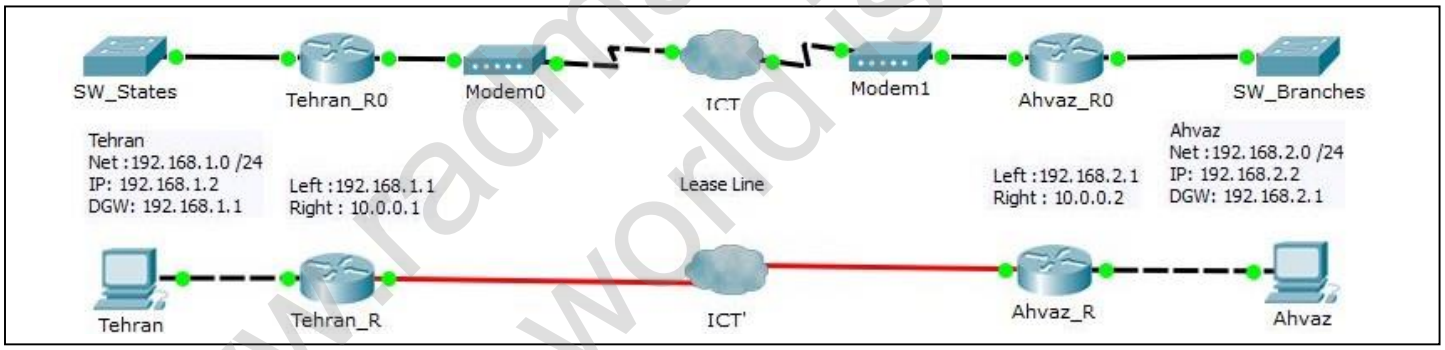
۳. **اینترفیس های کنسول و کمکی :** عملکرد پورت های مدیریتی متفاوت از سایر اتصالات است. اتصالات LAN و WAN ، مسولیت ایجاد اتصالات شبکه ای به منظور ارسال فریم ها را برعهده دارند ولی پورت های مدیریتی یک اتصال مبتنی بر متن به منظور پیکربندی و اشکال زدائی روتر را ارائه می نمایند. پورت های کمکی (Auxilliary) و کنسول (Console) دو نمونه متداول از پورت های مدیریت روتر می باشند. این نوع پورت ها، از نوع پورت های سریال غیرهمزمان EIA-232 می باشند که به یک پورت ارتباطی کامپیوتر متصل می گردند. در چنین مواردی از یک برنامه شبیه ساز ترمینال بر روی کامپیوتر به منظور ایجاد یک ارتباط مبتنی بر متن با روتر استفاده می گردد . مدیران شبکه می توانند با استفاده از ارتباط ایجاد شده مدیریت و پیکربندی دستگاه مورد نظر را انجام دهند.

- **هشدار** : در صورت عدم استفاده صحیح از اینترفیس ها، ممکن است روتر و یا سایر تجهیزات شبکه ای با مشکل مواجه گردند.

همانطور که قبلاً اشاره شد Interface ها یا پورت های یک روتر همانند دست های آن عمل می کنند، این Interface ها دارای تایپ های متفاوتی می باشند که با توجه به مدل روتر، به صورت Modular امکان نصب بر روی دستگاه را خواهند داشت. در زیر با دو تایپ و سه نمونه از این ماجول ها که در مطالب آتی و در نرافزارهای شبیه ساز از آنها استفاده خواهد شد، آشنا می شوید.

WIC (Wan Interface Card) available in Packet Tracer	
WIC-1T	The WIC-1T provides a single port serial connection to remote sites or legacy serial network devices such as Synchronous Data Link Control (SDLC) concentrators, alarm systems, and packet over SONET (POS) devices.
WIC-2T	The dual-serial port WAN interface cards (WICs) feature Cisco`s new, compact, high-density Smart Serial connector to support a wide variety of electrical interfaces when used with the appropriate transition cable. Two cables are required to support the two ports on the WIC. Each port on a WIC is a different physical interface and can support different protocols such as Point-to-Point protocol (PPP) or Frame Relay and Data Terminal Equipment/Data Communications Equipment (DTE/DCE).
WIC-1ENET	This is a single-port 10 Mbps Ethernet interface card, for use with 10BASE-T Ethernet LANs.

برقراری ارتباط مابین دو شهر:



قطعاً منطقی نخواهد بود که جهت برقراری ارتباط دو دفتر یک شرکت، یکی در تهران و دیگری در اهواز، کل مسیر را کابل کشی نمود. به همین خاطر از ارتباطات شبکه زیرساخت و اجاره نمودن یک خط می توان استفاده کرد، چگونگی و نحوه این اتصال را مخابرات مشخص می نماید.

در شبکه های داخلی برای تعیین کردن راه خروجی شبکه Gateway را مشخص می نمودیم و به آن یک IP اختصاص می دادیم و در اینجا نیز با توجه به اینکه هر Interface به عنوان دستی است که در هر شبکه قرار می گیرد و راه خروجی آن شبکه برای ارتباط با سایر شبکه ها می باشد به عنوان یک Gateway محسوب شده و می بایست یک IP در محدوده آدرس های همان شبکه به آن تخصیص داد. نحوه تنظیم و تخصیص IP به Interface (همانند سوییچ) به این شکل می باشد. برقراری ارتباط مابین دو روتر فوق Point-to-Point می باشد.

```
Continue with configuration dialog? [Yes/no]: no          */ First Message in front of you at First Time. (Answer: No)

Tehran_R0(Config) # interface TYPE MOD/NUM                */ Built-in FastEthernet 0/0 | Serial 0/0
Tehran_R0 (Config) # interface TYPE INTERFACE-TYPE/INTERFACE-CARD-SLOT / PORT */ FastEthernet 0/1/0 | Serial 0/2/1
Tehran_R0 (Config-if) # ip address IP NET_MASK            */ Set an IP address on each Interface if uses
Tehran_R0 (Config-if) # no shutdown                       */ Ports must be up on each device for point to point connection
…
Router # show ip route                                    */ Show available routes (Routing Table)
```


heydari.farzad@gmail.com نام مدرس دوره: مهندس فرزاد حیدری
تهیه و گردآوری: دانیال نامورکهن

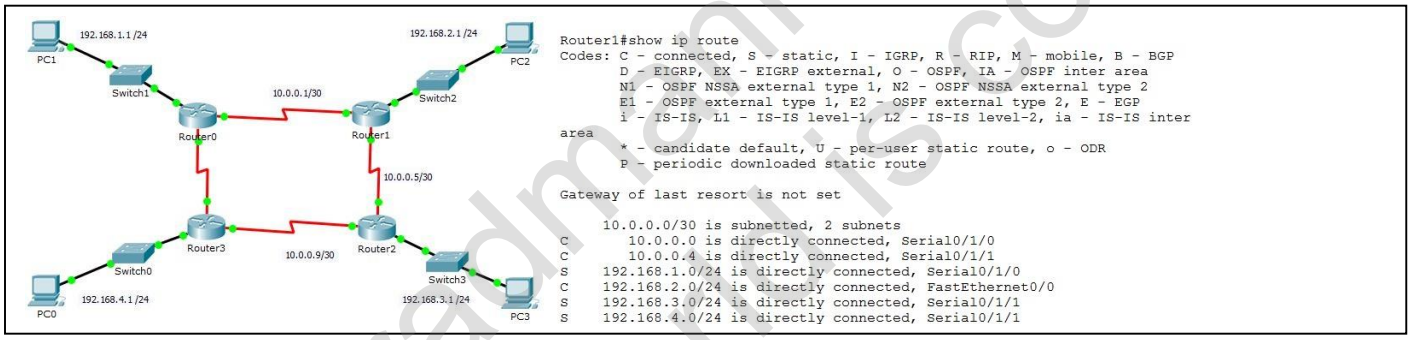
```
Tehran_R0#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     10.0.0.0/30 is subnetted, 1 subnets
C       10.0.0.0 is directly connected, Serial0/1/0
C    192.168.1.0/24 is directly connected, FastEthernet0/0
Tehran_R0#
```

Static Route

همانگونه که در گزارش جدول مسیرها نشان داده شده است در روتر تهران فقط مسیرهای تعریف شده (۲ مسیر) برای Interface ها قابل مشاهده بوده و نشانه ای از آدرس های اهواز نمی باشد و بالعکس. (FastEthrnet 0/0, Serial0/1/0). جهت برقراری ارتباط تهران با اهواز می بایست آدرس روتر اهواز را روی روتر تهران معرفی کرده و یا به اصطلاح Static Route تنظیم گردد(بنویسیم) و بالعکس. انجام این عمل از دو روش امکانپذیر می باشد:

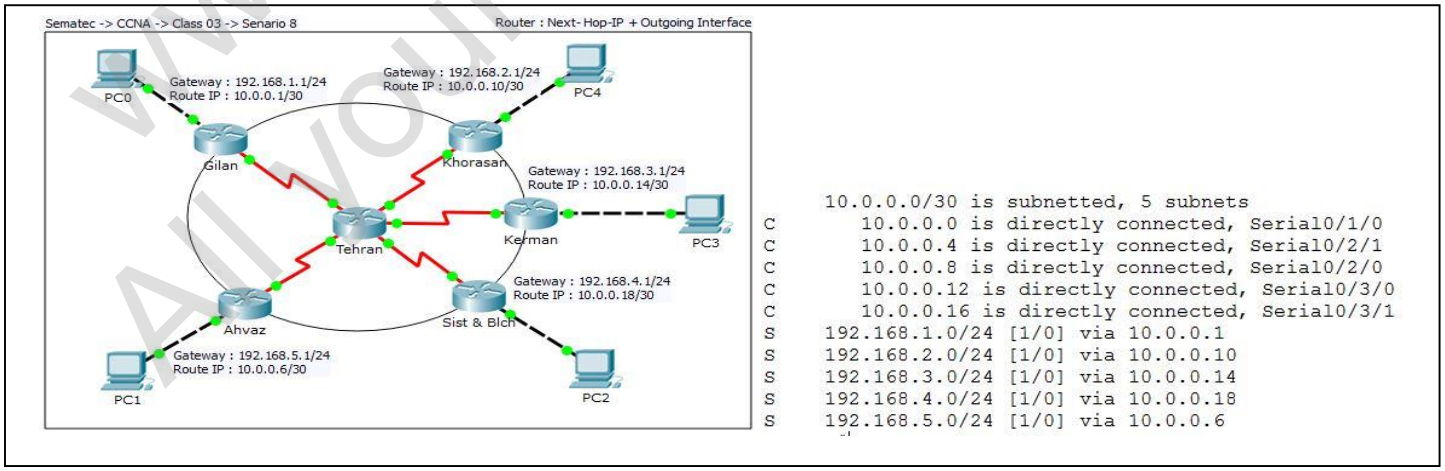
۱- Out-Going: یعنی مسیری که روتر از آن طریق به شبکه دسترسی پیدا می کند.

```
Tehran_R0(Config) # ip route NET_ID  MASK  OUT-GOING          */ A out-going address to access to another network
Tehran_R0(Config) # ip route 192.168.2.0 255.255.255.0 serial0/1/0
```



۲- Next-Hop: یعنی IP مربوط به Interface روتر مجاور داده می شود با این شرط که در یک شبکه باشند.

```
Tehran_R0(Config) # ip route NET_ID  MASK  NEXT-HOP           */ A next-hop address to access to another network
Tehran_R0(Config) # ip route 192.168.2.0 255.255.255.0 10.0.0.2
```



heydari.farzad@gmail.com نام مدرس دوره: مهندس فرزاد حیدری
تهیه و گردآوری: دانیال نامورکهن

Default Route:

با علم به اینکه برای برقراری ارتباط مابین ۲ شبکه مجزا، حتماً باید آدرس (Net_ID) مقصد مشخص شده باشد، اگر بخواهیم امکان استفاده از اینترنت را برای کاربران مهیا کنیم چگونه باید آدرس تمامی سایت ها را برای کاربران شبکه فراهم سازی کنیم؟ آیا بایستی مسیرها را به صورت دستی تنظیم کنیم؟ قطعاً، خیر . اگر هم دستی بر روی روتر تنظیم گردند، به محض اینکه بسته ها به Gateway برسند، چون در Routing Table مسیری برای آن مشخص نگردیده است تمامی بسته ها Drop می شوند. برای رفع این مشکل می بایست یک Default Route برای تمامی مسیرها به روش زیر تعریف می کنیم. جهت برقراری ارتباط اینترنت مهم این است که ترافیک را تحویل ISP دهیم.

```
Tehran_R0(Config) # ip route 0.0.0.0  0.0.0.0 OUT-GOING | NEXT_HOP        */ A default route
```

Routing Protocol	Administrative Distance	
Directly Connected	0	
Static Route	Next-Hop: 1	Outgoing: 0
EIGRP	90	
OSPF	110	
RIP	120	
Unknown	255	

AD: (Administrative Distance)

هنگامی که برای رسیدن به یک مقصد خاص چندین مسیر وجود داشته باشد و راهبری این مسیرها با پروتکل های متفاوتی انجام شده باشد، نیاز به شاخصی است که روترها با مراجعه به آن بتوانند مسیر مناسب را تشخیص، اولویت بندی و انتخاب کنند. این شاخص ها در جدول AD قرار دارند. در این دوره با توجه به پروتکل های مورد بررسی به برخی از رکوردهای این جدول اشاره خواهیم نمود.

Floating Static Route:

در مواقعی که از دو مسیر بیشتر برای رسیدن به یک مقصد وجود داشته باشد و یا یک مسیر پشتیبان در کنار مسیر اصلی برای مواقع ضروری وجود داشته باشد مدیر شبکه باید تمامی مسیرها را به صورت Static بر روی روترهای مبدا و مقصد معرفی کند. این مسیرهای باید به شکلی معرفی و اولویت بندی شوند تا در صورت قطع یا بروز مشکل جایگزین مسیر قبلی گردند. (Redundancy) این کار با تعیین متریک برای هر مسیر امکانپذیر است.

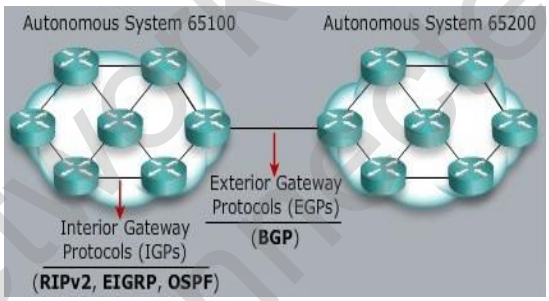
```
Tehran_R0(Config) # ip route NET_ID  NET_MASK  OUT-GOING | NEXT-HOP  DISTANCE_METRIC */1-255
```

فصل دوازدهم

آشنایی با Routing Protocols

شبکه‌های کوچک دارای جداول دستی هستند. شبکه‌های بزرگ توپولوژی پیچیده دارند و به سرعت تغییر می‌کنند. به این طریق ساختار جداول غیرقابل طراحی خواهد شد. بیشتر این شبکه‌های تلفنی کلیدی (PSTN-Public Switch Telephony Network) از این جداول استفاده می‌کنند و نقایص در مسیر این سیستم شناخته و رفع خواهند شد. مسیر یابی دینامیکی تلاشی برای حل مسئله و تشکیل ساختار خودکار جداول است. این براساس اطلاعات پروتکل مسیریابی عملی است. به این طریق شبکه‌ها از هر نقص ایمن خواهند شد. این دینامیک در اینترنت نقش فعال دارد. طراحی پروتکل‌ها به یک تماس ماهرانه نیاز دارد. نباید فرض کرد که شبکه سازی به نقطه اتوماسیون کامل رسیده است.

Dynamic Routing Protocols		
IGP Interior Gateway Protocol	**RIP**	Routing Informaton Protocol (Ver:1,2,3 IPV6)
	OSPF	Open Shortest Path First (Ver: 1,2,3 IPV6)
	IGRP	Interior Gateway Routing Protocol
	EIGRP	Enhance Interior Gateway Routing Protocol
EGP	**EGP**	Exterior Gateway Protocol
	BGP	Border Gateway Protocol
IS-IS	**IS-IS**	Intermediate System to Intermediate System



AS: **A**utonomous **S**ystem, AS Number must be set on Routers.

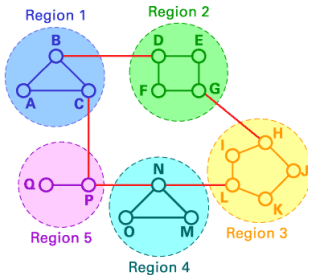
	RIP V1	RIP V2	IGRP	EIGRP	OSPF	IS-IS	BGP
Interior/Exterior	Interior	Interior	Interior	Interior	Interior	Interior	Exterior
Type	Distance Vector	Distance Vector	Distance Vector	HyBrid	Link-State	Link_State	Path Vector
Default Metric	Hopcount	Hopcount	BW / Delay	BW / Delay	Cost	Cost	Multiple Attribute
Administratve Distance	120	120	100	90 (Internal) 170 (External)	110	115	20 (Internal) 200 (External)
Hopcount Limit	15	15	225 (Def 100)	224 (Def 100)	None	None	EBGP Neig :1 IBGP Neig : -
Convergence	Slow	Slow	Slow	Very Fast	Fast	Fast	Average
Update Timers	30 Seconds	30 Seconds	90 Seconds	Only When Change Occurs	Only When Change Occurs [1]	Only When Change Occurs	Only When Change Occurs
Updates	Full Table	Full Table	Full Table	Only Change	Only Change	Only Change	Only Change
Classless	No	Yes	No	Yes	Yes	Yes	Yes
Supports VLSM	No	Yes	No	Yes	Yes	Yes	Yes
Algoritm	Bellman-Ford	Bellman-Ford	Bellman-Ford	Dual	Dijkstra	Dijkstra	Best Path Algorithm
Update Address	Broadcast	224.0.0.9	224.0.0.10	224.0.0.10	224.0.0.5 (All SPF Routers) 224.0.0.6 (DR's & BDR's)	-	Unicast
Protocol & Port	UDP port 520	-	IP Protocol 9	IP Protocol 88	IP Protocol 89	-	TCP port 179
Cisco Proprietary	No	No	No	Yes	No	No	No

[1] (LSA Table is refreshed every 30 Min, however) , LSA: Link State Advertisement, UDP: User Datagram Protocol
Dual: Diffusing Update ALgorithm

AS: یعنی ارتباطات داخلی یک IGP، یعنی تمامی شبکه هایی که در یک AS قرار دارند برای مسیریابی از پروتکل IGP استفاده می کنند و شبکه ایی که AS متفاوتی دارند از EGP استفاده می کنند. به عنوان مثال شعب بانک ملی در ایران یک AS دارد پس مسیر یابی با IGP است ولی برای برقراری ارتباط با شعب بانک تجارت چون AS دیگری دارد از EGP استفاده می گردد. (اینترنت یعنی ارتباط بین AS های مختلف)

- **الگوریتم Distance-Vector**

در این الگوریتم از الگوریتم Bellman – Ford استفاده می‌شود و می‌توان یک رقم و هزینه را برای هر لینک بین گروه‌های شبکه تعیین نمود. گره‌ها می‌توانند اطلاعات را از A به B بفرستند؛ و این از طریق مسیر کم هزینه عملی است. این الگوریتم خیلی ساده عمل می‌کند. ابتدا باید راه‌اندازی انجام شود. بخش‌های همجوار نیز باید شناخته شوند. هر گره به طور منظم می‌تواند هزینه کل را به مقصد بفرستد. گره‌های همجوار به بررسی اطلاعات و مقایسه یافته‌ها می‌پردازند. این عامل پیشرفت در جداول مسیریابی خواهد بود. تمام گره‌ها بهترین حلقه را کشف می‌کنند. وقتی یکی از گره‌ها کاهش یافت آنهایی که در همجوار هستند می‌توانند ورودی را خالی کنند و به مقصد بروند. به این طریق اطلاعات جدول ارائه خواهند شد. آنها می‌توانند اطلاعات را در اختیار گره‌های مجاور قرار دهند. در نهایت اطلاعات ارتقا یافته دریافت می‌شوند و مسیر جدید شناخته خواهد شد.



- **الگوریتم Link-State**

وقتی از این الگوریتم استفاده می‌شود هر گره از داده‌های اصلی در الگوی شبکه‌ای استفاده خواهد نمود. در این شرایط تمام گره‌ها وارد شبکه می‌شوند و اطلاعات با یکدیگر در ارتباط خواهند بود. این گره‌ها می‌توانند اطلاعات را وارد نقشه کنند. به این طریق هر مسیریاب تعیین کننده مسیر کم هزینه به سمت دیگر گره‌ها خواهد بود. در نهایت یک الگوریتم با کوتاهترین مسیر به وجود می‌آید. این درخت می‌تواند ماحصل ترکیب این گره‌ها باشد. در این شرایط بهتر است این درخت در طراحی جدول استفاده شود و حلقه بعدی گره نیز مشخص گردد.

- **پروتکل Path-Vector**

مسیریابی حالت لینک و بردار فاصله پروتکل غالب می‌باشند. آنها از سیستم ناشناخته درونی استفاده می‌نمایند ولی بین سیستم‌های ناشناخته نمی‌باشند. این دو نوع پروتکل می‌توانند در شبکه‌های بزرگ مسیریابی شوند و به این طریق مسیریابی درون حوزه‌ای عملی خواهد شد. مسیریابی حالت لینک می‌تواند اطلاعات زیادی را وارد جدول کند، این عامل تشکیل ترافیک بزرگ می‌باشد. مسیریابی بردار برای درون حوزه‌ها استفاده می‌شود و مانند بردار راه دور است. در این جا یک گره در هر سیستم ناشناخته وجود دارد که به عنوان کل سیستم عمل خواهد کرد. این گره از نوع سخنگو است. این گره جدول مسیریابی را تولید کرده و به گره‌های همجوار می‌فرستد. در این شرایط فقط گره‌های سخنگو در هر سیستم با یکدیگر ارتباط برقرار می‌کنند. این گره می‌تواند در مسیر پیش رود و در سیستم ناشناخته فعال شود. نکته

- **مقایسه الگوریتم مسیریابی**

پروتکلهای مسیریابی Distance-Vector در شبکه‌های کوچک، ساده و کارآمد بوده و به مدیریت اندکی نیازمند هستند. با این وجود آلگوریتم های اولیه Distance-Vector از نظر مقیاس پذیری خوب نیستند و قابلیت های همگرایی آنها ضعیف است که این امر منجر به توسعه الگوریتم های پیچیده تر با مقیاس پذیری بهتر جهت شبکه‌های بزرگ شده‌است. بدین جهت اغلب پروتکل های مسیریابی درونی از پروتکل‌های Link-State مانند ابتدا کوتاه‌ترین مسیر را انتخاب کردن و IS-IS استفاده می‌کنند. یکی از توسعه‌های اخیر در پروتکل‌های Distance-Vector ، قابلیت بدون حلقه یا loop-free می‌باشد که بطور مثال در EIGRP پیاده‌سازی شده‌است. این پروتکل ضمن داشتن تمام قابلیت های پروتکل های Distance-Vector ، مشکل count-to-infinity را حل کرده و از این جهت زمان همگرایی پروتکل را بهبود بخشیده است.

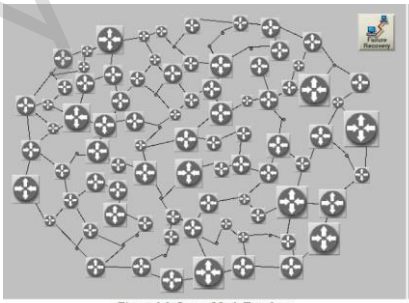


Figure 3.3: Large Mesh Topology

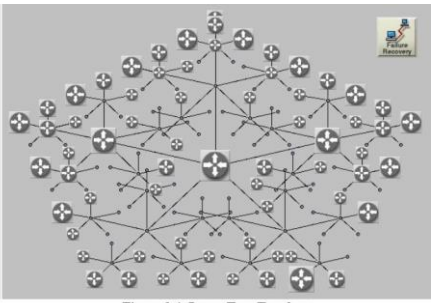
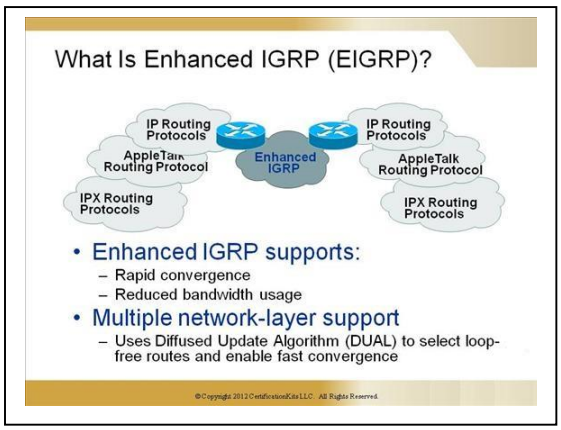


Figure 3.4: Large Tree Topology

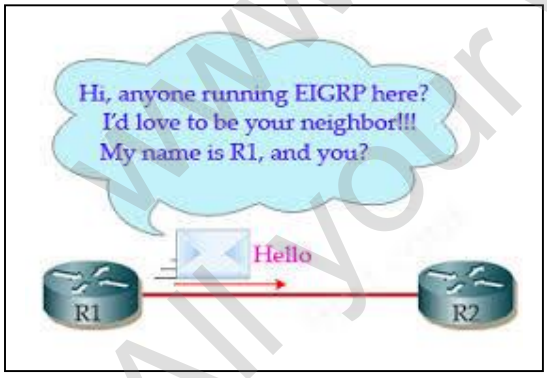
heydari.farzad@gmail.com نام مدرس دوره: مهندس فرزاد حیدری
تهیه و گردآوری: دانیال نامورکهن

پروتکل مسیریابی EIGRP



در اوایل دهه ۹۰ توسط شرکت سیسکو ارائه شد. با اینکه EIGRP نسخه بهبود یافته IGRP است اما از نظر کارائی و عملکرد تفاوت هایی زیر بنائی با کلیه Distance Vector ها دارد و از این لحاظ بیشتر دارای شباهت و خصوصیاتی Link State گونه است بطوریکه به آن Hybrid Routing Protocol گفته میشود و سیسکو آنرا Advance Distance Vector Protocol می نامد. یعنی تلفیقی از خصوصیت پروتکل های Distance Vector مانند RIP و Link State مانند OSPF را دارا می باشد. اما فرق پروتکل های Link State و Distance Vector در چیست؟ پروتکل های Link State دارای یک جدولی هستند که آن جدول یک نقشه از کل شبکه را در اختیار دارد که به آن Topology Table یا جدول توپولوژی می گویند، بر اساس اطلاعات این جدول بهترین مسیر را مشخص می کنند. اما پروتکل های Distance Vector نقشه ای از شبکه ندارند، , بر اساس فاصله (Distance) و جهت (Vector) مسیر مورد نظر خود را انتخاب می کنند. EIGRP برای حل مشکلات رشد شبکه های IGRP و کلاً ضعف های Distance Vector ها بوجود آمد و نهایتاً منجر به کاهش زمان Convergence (همگرایی) در شبکه شد. این بدان معناست که چنانچه روتر یک مسیر را برای مقصدی از دست داد بلافاصله مسیر دوم را جایگزین می کند، که این زمان نسبت دیگر پروتکل های مسیریابی کمتر است . دلیل آن نیز این است که EIGRP در زمان محاسبه بهترین مسیر، بهترین مسیر دوم را نیز مشخص می کند تا بعد از failed شدن مسیر اول بلافاصله مسیر دوم را جایگزین کند. این پروتکل اطلاعات مسیر های را که یاد می گیرد به صورت Route Update به همسایه های خود ارسال می کند. و این update ها را به صورت Classless ارسال می کند، یعنی در زمان ارسال Network به روتر همسایه، Prefix سگمنت مربوطه را نیز ارسال می کند.در این صورت روتر همسایه در زمان دریافت این آپدیت ها دیگر نیازی نیست به صورت Classfull عمل کرده و Prefix آن را بر اساس کلاس IP، حدس بزند. به همین دلیل می گوییم که EIGRP، از VLSM پشتیبانی میکند.

یکی از دیگر مزایای EIGRP تقسیم ترافیک ارسالی در مسیر های با پهنای باند نامساوی است که به آن unequal path load balancing می گویند. در تمام پروتکل های مسیریابی ارسال ترافیک تنها در مسیر هایی قابل تقسیم است که دارای پهنای باند مساوی باشند، , اما در EIGRP می توان ترافیک را بین مسیرهایی نامساوی ، آن هم به نسبت های مختلف ارسال کرد. مثلاً اگر لینکی 2 مگابایت و لینک دیگری ۱ مگابایت پهنای باند داشته باشد، میتوان ترافیک را به نسبت ۲ به ۱ بین این دو مسیر ارسال کرد.



در EIGRP بعد از دریافت Hello packet با هم رابطه همسایگی (adjacency) می کنند، و هر روتر اطلاعات مربوط به روتر همسایه خود را در جدولی به نام Neighbor Table نگهداری می کند. روتر های بعد ایجاد همسایگی شروع به ارسال بسته های با نام Hello Packet می کنند و اگر روتری از همسایه خود در یک بازه زمانی مشخص Hello Packet دریافت نکند، فرض را بر این میگذارد که ارتباطش با همسایه قطع شده و آن همسایگی را Down می کند. این پکت ها در شبکه های پرسرعت مانند Ethernet در بازه های زمانی هر ۵ ثانیه یکبار ارسال می شود و در شبکه های با سرعت کم مانند NBMA به ۶۰ ثانیه می رسد. Hold Time یا زمانی که روتر منتظر دریافت Hello از همسایه می ماند نیز ۳ برابر زمان ارسال Hello می باشد. (در شبکه های پر سرعت ۱۵ ثانیه و در شبکه های کم سرعت ۱۸۰ ثانیه). EIGRP پکت های خود را به آدرس Multicast 224.0.0.10 ارسال می کند، و تمام روتر های همسایه این بسته را دریافت می کند و سپس یک پیغام Acknowledge برای روتر ارسال می کنند، ولی اگر همسایه ای این بسته را نگرید و نتواند پیغام Ack را ارسال کند، روتر این بار بسته را به صورت Unicast برای آن همسایه ارسال می کند.

این پروتکل بر اساس DUAL یا Diffusing Update Algorithm کار میکند و برای ارتباط با همسایگان خود برخلاف RIP_V1 (Broadcast) از Multicast (224.0.0.10) استفاده میکند. همسایه به محض دریافت این Packet به فرستنده Unicast، ACK (رسید) ارسال میکند. برای جلوگیری از Loop در مسیر، روتر مسیر Backup (نام دیگر آن Feasible Successor) را نیز ذخیره میکند. تا در موقع مورد نیاز از آن استفاده کند. همچنین EIGRP برای Summarization برخلاف پروتکلی نظیر OSPF نیازی به تعریف Area ندارد و هرجائی از شبکه این امکان وجود دارد.

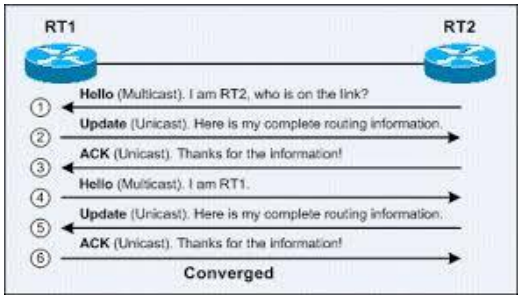
EIGRP بعنوان یک Routing Protocol قابلیت Route پروتکل های IPX،IP و AppleTalk و IPV6 را داراست و برای هریک، Routing Table مجزا میسازد و از آنجا که قابلیت Route کردن پروتکل های مختلف را داراست، به ازای هر پروتکل سه جدول وضع میکند:

- Neighbor Table */ جدول همسایگی پس از برقراری اولین ارتباط
- Topology Table */ تبادل و یادگیری مسیرها از همدیگر و تکمیل جدول توپولوژی
- Routing Table */ آنالیز مسیرها بر اساس اطلاعات دریافتی از جدول توپولوژی

خلاصه مطالب فوق در قالب چهار مزیت EIGRP

Packets	Description
Hello	EIGRP neighbor ship is discovered and maintained by Hello Packets. If the router fails to receive a hello packet within the hold timer, the corresponding router will be declared dead.
Update	At the time of discovering new neighbor, update packets are sent, so tmhat the topology table can be built by the neighbor router. Update packets are unicast and always transmitted reliably.
Query	When the destination goes into Active state, the query packets are sent. Query packets are multicast and replies are always sent in reply to the queries for indicating the originator that it does not need to go into Active state.
Reply	When the destination goes into Active state, the reply packets are sent. Reply packets are unicast to the originator of the query and transmission of reply packets are reliable.
ACK	ACK packets use to know the transmission status. If a Hello packet sent without data is also recognized as acknowledgement. Unicast address with non-zero acknowledgement number is always sent by ACKs.

- **Protocol-Dependent Modules (PDM)**: IPX،IP و AppleTalk و IPV6 را Route میکند و برای هریک Routing Table مجزا میسازد. پروتکل Encapsulate کننده EIGRP برای هر یک از این پروتکل ها از جنس خودش است بطور مثال بسته های EIGRP برای Update های IPX داخل IPX حمل میشوند. EIGRP به صورت خودکارIPX RIP، AppleTalk RTMP و IP IGRP را Redistribute میکند.
- **Reliable Transport Protocol (RTP)**: وظیفه انتقال پیام های EIGRP را بعهده دارد. بوسیله RTP انتقال پیام ها همراه با گارانتی صورت میگیرد. در واقع هر جا RTP همراه با ACK استفاده شود Reliable (مطمئن) است. این بسته ها از IP به شماره Type 88 و آدرس Multicast رزرو شده 224.0.0.10 استفاده می کنند. پیام های Hello نیازی به ACK نداشته و Unreliable رد و بدل میشوند. برای انتقال ACK ها از Unicast استفاده شده و انتقال update، query و reply باید به صورت Reliable باشد و نیاز به دریافت ACK دارند. اگر بسته ای به آدرس Multicast ارسال شود اما ACK از یکی از روتر ها دریافت نشود، بسته بصورت Unicast برای او ارسال میگردد و اگر تا ۱۶ بار Retransmit شد و ACK دریافت نشد آن همسایه بعنوان dead و غیرفعال شناخته میشود. فاصله بین ارسال این Unicast ها را RTO یا Retransmission TimeOut می نامند. برای محاسبه این گونه زمانبندی ها در EIGRP، از فرمول SRTT یا Smooth Round Trip Time استفاده میشود. SRTT میانگین زمان صرف شده از ارسال بسته تا دریافت ACK، بر حسب میلی ثانیه است.
- **Neighbor Discovery Recovery**: از آنجا که EIGRP از Update های نوبتی و دوره ای (Periodic Update) استفاده نمی کند از مکانیزم Hello بین همسایگان خود سود می برد که هر ۵ ثانیه و به صورت Multicast انجام میشود. حال اگر ارتباط به شکل WAN و با پهنای باند کمتر از یک T1 (کمتر از ۲ مگابیت) باشد بصورت Unicast و هر ۶۰ ثانیه رخ میدهد. نباید فراموش کرد که در هر حال Hello نیازی به ACK ندارد. Holddown در



صورت عدم دریافت Hello تا سه برابر زمان Hello محاسبه شده و بعد از آن اگر از همسایه Hello دریافت نشود همسایه Dead شناخته میشود. اطلاعات هر Neighbor یا همسایه داخل Neighbor Table قرار میگیرد. در EIGRP تنها پیام های Hello بصورت Connection-less ارسال شده و بقیه پیام ها Connection-Oriented هستند.

- **DUAL**: Database شبکه توسط DUAL در EIGRP کشف و ایجاد میشود. فلسفه طراحی DUAL بر اساس Diffusing Computation است که اولین بار توسط Dijsktra و Scholten ارائه شد و الگوریتم DUAL توسط Dr. J. J. Garcia-Luna-Aceves پیشنهاد گردید.

مفهوم Wildcard Mask:

اگر از افرادی که در زمینه شبکه مهارت دارند سئوال کنید که Wild Card Mask چیست در جواب معمولا می گویند، برعکس Subnet Mask است ! همین ! اما در این مطلب قصد داریم به شما یاد بدهیم که Wild Card Mask چیست و در کجا استفاده می شود. در بسیاری اوقات ممکن است این تعریف درست باشد و Wild Card Mask تا حدودی و بعضاً دقیقا برعکس Subnet Mask باشد اما همیشه هم اینطور نیست و این عدد می تواند کارهای بسیار بیشتری را برای ما انجام دهد.

یک آدرس ۳۲ بیت می باشد و برای بدست آوردن آن هر Octet را از ۲۵۵ کسر می کنیم. در ساختار Wild Card Mask عدد ۰ به منزله Match بودن و عدد یک به منزله Ignore بودن است.. به مثال زیر دقت کنید که عدد ۱۹۲,۱۶۸,۲۰,۰ را ما بصورت Wild Card Mask در آورده ایم :

IP Address Range (Net_ID)	192.168.20.0
IP Address Range Binary Code	11000000.10101000.00010100.00000000
IP Address Range Subnet Mask	255.255.255.0
IP Address Range Subnet Mask Binary Code	11111111.11111111.11111111.00000000
IP Address Range Wild Card Mask Binary Code	00000000.00000000.00000000.11111111
IP Address Range Wild Card Mask	0.0.0.255

Neghborship Parameters: (پارامترهای احراز همسایگی)

1. **Same AS Number**
2. **Same Subnet**

۱. **AS Number**: در تعریف کلاسیک Autonomos Number تنظیم کردن روترها زیر یک مدیریت تکنیکی واحد هست. بواسطه استفاده کردن از IGP و متریک مشترک مشخص می شوند که تعریف ساده AS یا Autonomous چطور پکت ها در داخل یک AS روت و مسیریابی شوند. در یک System حوزه ای است که روترها همدیگر رو می بینند. مثلا اگر بخواهیم ۱۰ روتر برای همدیگر آپدیت بفرستند باید AS Number هر ده تا را عدد یکسان قرار دهیم. (ساده تر: گروه بندی کردن روترها). همانطور که اشاره شد اولین شرط برای ایجاد همسایگی قرارگیری روترهای در یک حوزه است که با AS Number مشخص می گردد.

۲. **Same Net_ID or Network**: جهت برقراری ارتباط مابین دو روتر باید برای هر یک از پورت ها IP Address مورد نظر را تنظیم نمود که قطعاً این آدرس باید از یک Net_ID تبعیت کنند و در یک شبکه باشند. آدرس مناسب برای دو روتر که بتوانند به صورت Point-to-Point برقراری ارتباط کنند در مثال زیر نشان داده شده است:

10.0.0.0 /30 (Router1: 10.0.0.1, Router2: 10.0.0.2), Net_Mask: 255.255.255.252, WC: 0.0.0.3

```
Router1(Config)# router eigrp ASN
Router1(Config-router)# network NET_ID Wild_Card_mask          */ Define a route in EIGRP
```

- دریافت گزارش از جدول مسیرها

```
Router1(Config)# show ip route                          */ View Routing Table
```

- دریافت گزارش از جدول مسیرها که از طریق پروتکل EIGRP یاد گرفته شده است.

```
Router1(Config)# show ip route eigrp                    */ View Routing Learned by EIGRP
```

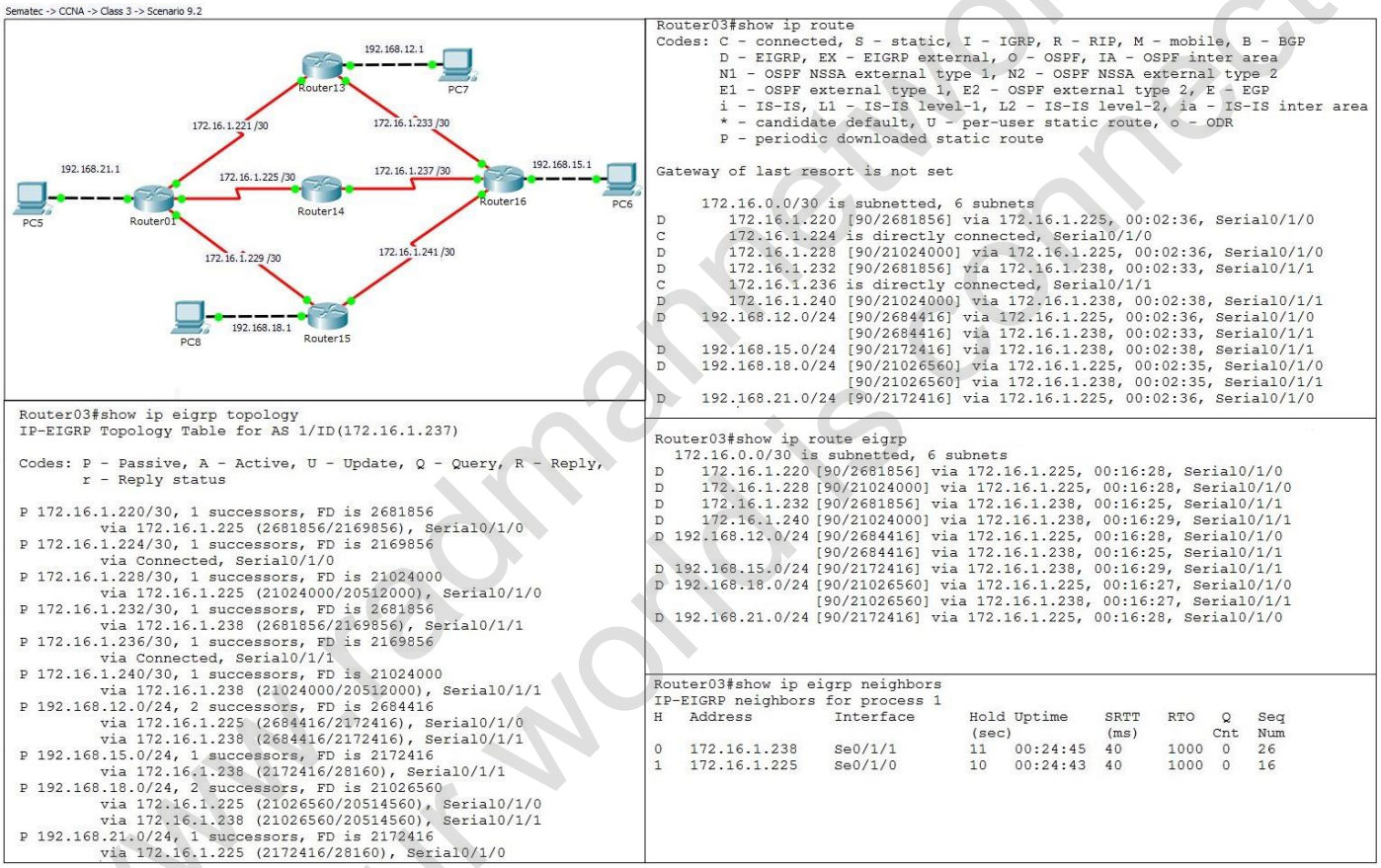
- دریافت گزارش از جدول توپولوژی (مسیرهایی که یادگیری آن از طریق همسایه صورت گرفته است)

```
Router1(Config)# show ip eigrp topology                 */ View Topology Table
```

- دریافت گزارش از همسایه یا همسایه های روتر

```
Router1(Config)# show ip eigrp neighbor                 */ View Neighbors Table
```

پس از برقراری ارتباط پیغام New Adjencency بر روی کنسول مشاهد می شود که به نوعی مشخص کننده صحت تنظیمات انجام شده می باشد.




```
Router03#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     172.16.0.0/30 is subnetted, 6 subnets
D       172.16.1.220 [90/2681856] via 172.16.1.225, 00:02:36, Serial0/1/0
C       172.16.1.224 is directly connected, Serial0/1/0
D       172.16.1.228 [90/21024000] via 172.16.1.225, 00:02:36, Serial0/1/0
D       172.16.1.232 [90/2681856] via 172.16.1.238, 00:02:33, Serial0/1/1
C       172.16.1.236 is directly connected, Serial0/1/1
D       172.16.1.240 [90/21024000] via 172.16.1.238, 00:02:38, Serial0/1/1
D    192.168.12.0/24 [90/2684416] via 172.16.1.225, 00:02:36, Serial0/1/0
                     [90/2684416] via 172.16.1.238, 00:02:33, Serial0/1/1
D    192.168.15.0/24 [90/2172416] via 172.16.1.238, 00:02:38, Serial0/1/1
D    192.168.18.0/24 [90/21026560] via 172.16.1.225, 00:02:35, Serial0/1/0
                     [90/21026560] via 172.16.1.238, 00:02:35, Serial0/1/1
D    192.168.21.0/24 [90/2172416] via 172.16.1.225, 00:02:36, Serial0/1/0
```

```
Router03#show ip eigrp topology
IP-EIGRP Topology Table for AS 1/ID(172.16.1.237)

Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - Reply status

P 172.16.1.220/30, 1 successors, FD is 2681856
         via 172.16.1.225 (2681856/2169856), Serial0/1/0
P 172.16.1.224/30, 1 successors, FD is 2169856
         via Connected, Serial0/1/0
P 172.16.1.228/30, 1 successors, FD is 21024000
         via 172.16.1.225 (21024000/20512000), Serial0/1/0
P 172.16.1.232/30, 1 successors, FD is 2681856
         via 172.16.1.238 (2681856/2169856), Serial0/1/1
P 172.16.1.236/30, 1 successors, FD is 2169856
         via Connected, Serial0/1/1
P 172.16.1.240/30, 1 successors, FD is 21024000
         via 172.16.1.238 (21024000/20512000), Serial0/1/1
P 192.168.12.0/24, 2 successors, FD is 2684416
         via 172.16.1.225 (2684416/2172416), Serial0/1/0
         via 172.16.1.238 (2684416/2172416), Serial0/1/1
P 192.168.15.0/24, 1 successors, FD is 2172416
         via 172.16.1.238 (2172416/28160), Serial0/1/1
P 192.168.18.0/24, 2 successors, FD is 21026560
         via 172.16.1.225 (21026560/20514560), Serial0/1/0
         via 172.16.1.238 (21026560/20514560), Serial0/1/1
P 192.168.21.0/24, 1 successors, FD is 2172416
         via 172.16.1.225 (2172416/28160), Serial0/1/0
```

```
Router03#show ip route eigrp
  172.16.0.0/30 is subnetted, 6 subnets
D    172.16.1.220 [90/2681856] via 172.16.1.225, 00:16:28, Serial0/1/0
D    172.16.1.228 [90/21024000] via 172.16.1.225, 00:16:28, Serial0/1/0
D    172.16.1.232 [90/2681856] via 172.16.1.238, 00:16:25, Serial0/1/1
D    172.16.1.240 [90/21024000] via 172.16.1.238, 00:16:29, Serial0/1/1
D 192.168.12.0/24 [90/2684416] via 172.16.1.225, 00:16:28, Serial0/1/0
                  [90/2684416] via 172.16.1.238, 00:16:25, Serial0/1/1
D 192.168.15.0/24 [90/2172416] via 172.16.1.238, 00:16:29, Serial0/1/1
D 192.168.18.0/24 [90/21026560] via 172.16.1.225, 00:16:27, Serial0/1/0
                  [90/21026560] via 172.16.1.238, 00:16:27, Serial0/1/1
D 192.168.21.0/24 [90/2172416] via 172.16.1.225, 00:16:28, Serial0/1/0
```

```
Router03#show ip eigrp neighbors
IP-EIGRP neighbors for process 1
H   Address         Interface      Hold Uptime    SRTT   RTO   Q   Seq
                                   (sec)          (ms)       Cnt Num
0   172.16.1.238    Se0/1/1        11   00:24:45  40     1000  0   26
1   172.16.1.225    Se0/1/0        10   00:24:43  40     1000  0   16
```

- اگر برای رسیدن به مقصد ۳ مسیر یکسان داشته باشیم از هر ۳ مسیر به صورت Load-balancing استفاده می شود. این تعداد به صورت پیش فرض تا ۴ مسیر می باشد. Maximum Path را بسته به نوع روتر و IOS می توان تغییر داد.
- معیار انتخاب بهترین مسیر بهترین متریک (Metric) است و اگر این متریک یکسان باشد هر ۳ مسیر در Routing Table خواهد آمد.
- حرف **P** مخفف Passive است و مفهوم آن این است که برای این شبکه مسیر دارد.
- حرف **A** مخفف Active است و مفهوم آن این است که برای این شبکه مسیری ندارد.

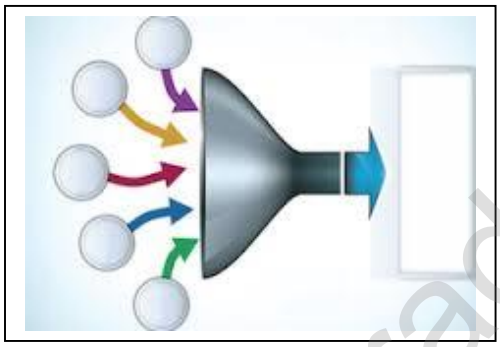
فصل سیزدهم

تغییر زمان Hello Time و Hold Time در EIGRP: به صورت پیش فرض هر ۵ ثانیه یک بار یک بسته HelloTime و هر ۱۵ ثانیه یک بسته HoldTime در پروتکل EIGRP ارسال می شود. همانگونه که مشاهده می شود زمان HoldTime سه برابر بسته HelloTime است پولی چنانچه این نسبت رعایت نشود همسایگب قطع و یا با اختلال مواجه خواهد شد.کار هوشمندانه ای که EIGRP در هنگام تغییر پارامترها انجام می دهد این است که چنانچه Hello Time به ۲ ثانیه و Hold Time به ۶ ثانیه تبدیل شود، EIGRP به همسایه خود اعلام می کند که ۶ ثانیه برای او صبر نماید ولی در OSPF این اطلاع رسانی به همسایه ها صورت نمی گیرد و به همین خاطر این دو پارامتر به عنوان پارامترهایی جهت برقراری شرایط همسایگی در EIGRP در نظر گرفته نشده است ولی در OSPF جزو پارامترهای احراز همسایگی می باشد. این تغییر و تنظیم باید بر روی Interface صورت گیرد. البته تغییر این پارامترها توصیه نمی شود ولی جهت تست دستورات زیر ارائه می شود.

```
Router1(Config-if)# ip hello-interval eigrp ASN Seconed        */ Default 5 Seconed
Router1(Config-if)# ip hold-time eigrp ASN Seconed             */ Default 15 Seconed

Router1(Config)# show ip eigrp interface detail TYPE MOD/NUM   */ To show Hello Time
Router1(Config)# show ip eigrp neighbor                        * To Show Hold Time
```

- نکته: وقتی پهنای باند بالا داریم زمان ارسال بسته Hello را کم می کنیم زیرا ترافیک شبکه زیاد نمی شود.

Summarization



در اینترنت میلیون ها و در شرکتها و موسسات برزگ هزاران خط Route وجود دارد، اگر قرار بود همگی این Route ها روی اینترنت و یا سایت کمپانی ها باقی می ماندند فاتحه اینترنت و سایت ها سال ها پیش خوانده شده بود. نیز همه روزه تعداد Subnet ها و آدرس های شبکه ای رو به افزایش است و همین امر باعث نیاز بیشتر به منابع CPU و RAM و پهنای باند بیشتر برای مدیریت Routing Table های موجود می شود. فرآیند خلاصه سازی Route ها یا Route Summarization که به Supernetting هم معروف است و همچنین تکنیک CIDR می تواند این رشد روز افزون را مدیریت کند. با درک مفاهیمی مثل CIDR و Route Summarization شما می توانید ضمن اینکه یک شبکه قابل اعتماد و توسعه پذیر ایجاد کنید مشکلات ناشی از زیاد شدن تعداد Route ها را نیز نداشته باشید.

برای اینکه بتوانید از قابلیت Route Summarization در شبکه خود استفاده کنید شما نیاز به استفاده از یک پروتکل روتینگ Classless مثل RIPv2 یا EIGRP یا OSPF دارید. همچنین شما بایستی شبکه خود را بصورت سلسله مراتبی و ساختارمند طراحی و پیاده سازی کرده باشید، پیاده سازی Route Summarization نیازمند یک طراحی درست و نقشه اولیه کاملا منظم می باشد. منظور از داشتن طراحی و نظم ساختاری در شبکه این است که شما نمی توانید بصورت تصادفی شبکه هایی با روترهای مختلف را به شبکه های LAN دیگر متصل کنید و وجود یک الگوی منظم در این طراحی الزامی است.

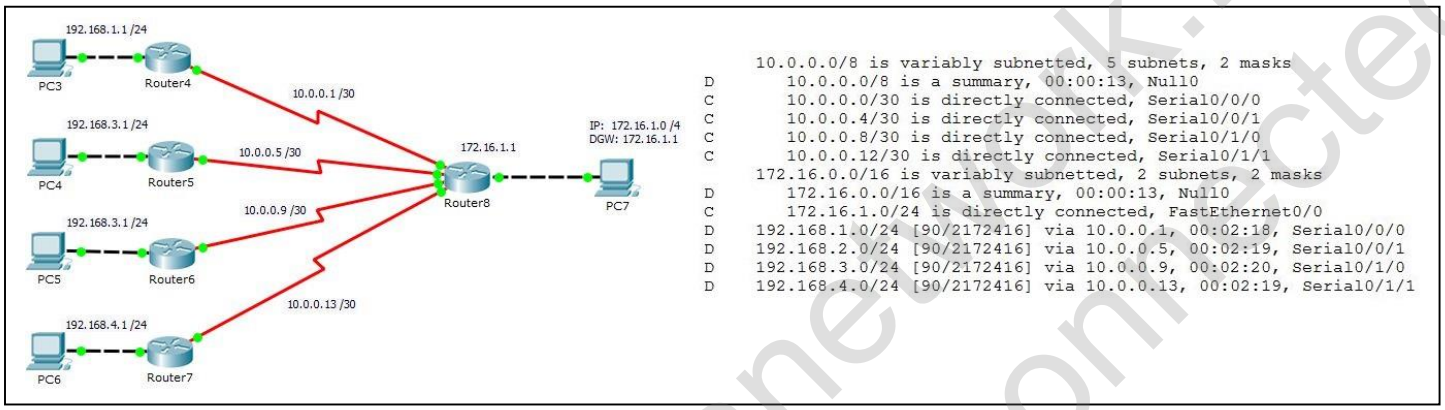
در شبکه های Internetwork بسیار بزرگ ممکن است صدها یا هزاران آدرس شبکه وجود داشته باشد. برای روترهایی که در این شبکه ها وجود دارد نگهداری این تعداد آدرس شبکه در Routing Table کار بسیار مشکل سازی است. فرآیند Route Summarization یا خلاصه سازی Route ها که قبلاً هم اشاره کردیم و شما آن را به اسم Supernetting یا Route Aggregation هم ممکن است بشناسید می تواند تعداد Route هایی که یک روتر به آن نیازمند است را کاهش دهد، روش کاری Route Summarization تقریبا ساده است، در این روش مجموعه ای از شبکه ها در قالب یک آدرس خلاصه شده شبکه در اختیار روترها قرار می گیرد.

Auto Summary در EIGRP

Auto-Summary به صورت پیش فرض فعال است و همانطور که قبلاً عنوان شد به صورت Classless عمل می کند و در صورتی که شبکه ما امکان استفاده از این قابلیت را داشته باشد منجر به کاهش فهرست مسیرها در گزارشات و نیز افزایش کارآیی و بازدهی روتر می گرددر غیر اینصورت می بایست از این قابلیت صرفنظر کرده و آن را غیرفعال نمود.

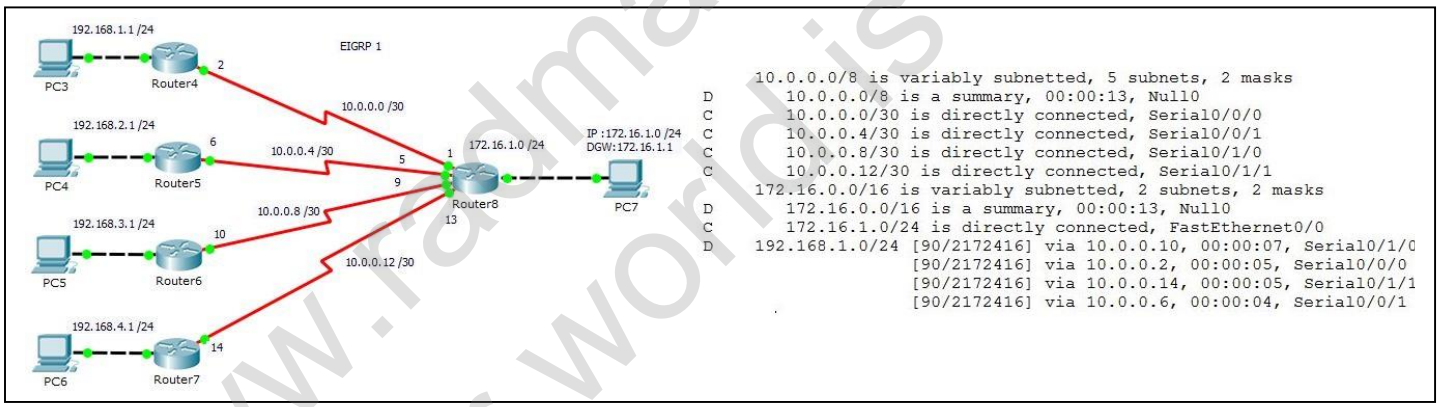
```
Router8(config-router) # auto-summary          */ By Default Auto-Summary is Active
Router8 # show ip route                        */ Routers exist in routing table
```

Summarization is correct. (Test other network with ping command from PCs)




```
Router8 # show ip route                        */ Routers exist in routing table
```

Summarization is incorrect (Test other network with ping command from PCs)




```
Router8(config-router) # no auto-summary       */ Just set this command on routers 4,5,6,7
Router8 # show ip route                        */ Routers exist in routing table
```

Active / Passive

برای کاهش ترافیک شبکه و جلوگیری از ارسال بسته Hello به Interface هایی که مستقیماً به کامپیوتر یا سوییچ متصل شده اند و هیچ شناختی از این بسته ندارند، باید آن پورت را در حالت Passive قرار داد.

```
Router1(Config)# router eigrp ASN                                  */ Set an EIGRP
Router1(Config-router)# passive-interface TYPE MOD/NUM             */ Send Hello Packet to Interface
Router1(Config-router)# no passive-interface TYPE MOD/NUM          */ Don't Send Hello Packet to Interface
Router1(Config-router)# passive-interface default                  */ *Attention* Passive all Interfaces ( 1 of 100 )
Router1(Config-router)# no passive-interface default               */ Active All Interfaces
Router1# Show run                                                  */ Check Active/Passive Ports
Router1# Show ip protocols                                         */ Check Active/Passive Ports
```

روش محاسبه مسیر پروتکل EIGRP

اگر یک روتر در طی فرآیند روتینگ به دو یا بیشتر از دو مسیر برای رسیدن به شبکه مقصد توسط پروتکل های مسیریابی دست پیدا کرد. روتر با استفاده از پارامتر **A**dministrative **D**istance بهترین مسیر را برای رسیدن به مقصد انتخاب می کند. اما برخی اوقات پیش می آید که دو مسیر برای رسیدن به یک شبکه مقصد پیدا می شود که هر دو مسیر دارای یک AD مشابه هستند که از طریق پروتکل های روتینگ محاسبه شده است. در چنین مواقعی است که Routing Protocol ها از پارامتر Route Metric برای انتخاب بهترین مسیر استفاده می کنند. به توپولوژی شبکه ای که در شکل زیر وجود دارد توجه کنید، ما برای رسیدن از شبکه A یا مبدا به شبکه B یا مقصد سه مسیر مختلف را در دسترس داریم، اگر از پروتکل مسیریابی RIP استفاده کنیم بهترین مسیر از نظر این پروتکل مسیری است که کمترین تعداد Hop Count وجود داشته باشد.

Hop Count به معنی تعداد روترهایی است که یک داده بایستی از آنها عبور کند تا به شبکه مقصد برسد، یا به بیانی دیگر Hop Count به تعداد روترهایی گفته می شود که داده ما باید از شبکه مبدا تا شبکه مقصد از آنها عبور کند.

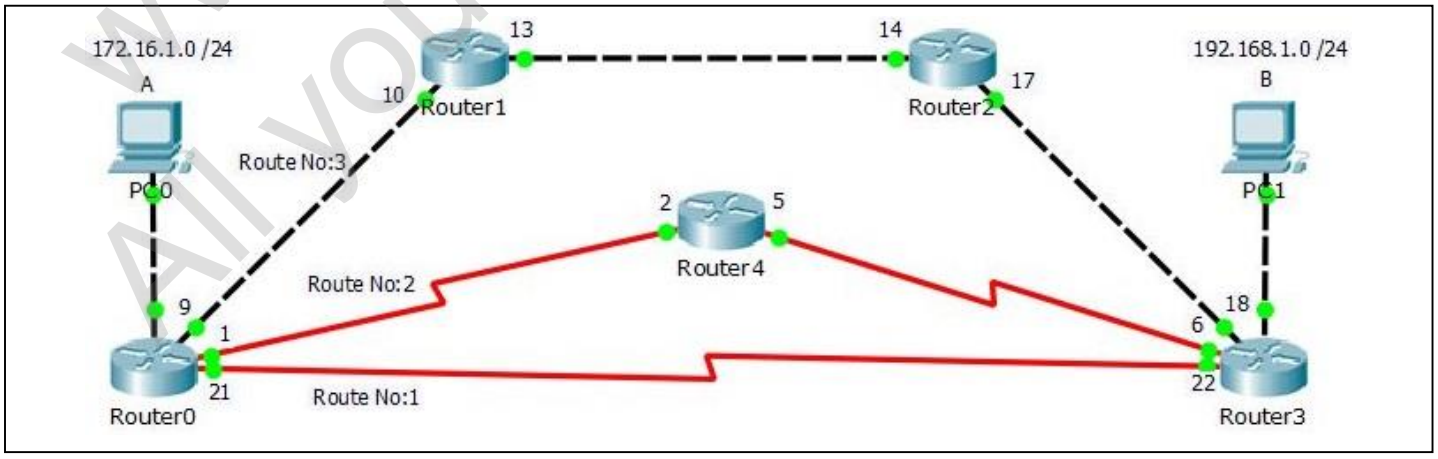
همانطور که در تصویر زیر مشاهده می کنید مسیر اول انتخاب می شود چون تعداد روترهای کمتری در مسیر مبدا تا مقصد وجود دارد. اما کافیست یک نگاه دقیقتر به توپولوژی بیاندازیم، درست است که مسیر اول و دوم تعداد Hop Count کمتری دارد اما سرعت بسیار پایینتری در مقایسه با مسیر دوم دارد ، سرعت مسیر های اول و دوم ۱,۵۴ مگابیت بر ثانیه است و مسیر سوم ۱۰۰ مگابیت بر ثانیه است. با این تفاسیر بهترین مسیر استفاده از مسیر سوم است که بسیار سرعت بیشتری دارد با اینکه دو Hop در مسیرش وجود دارد. توجه کنید که فاکتورهایی از قبیل تاخیر یا Delay و پهنای باند یا Bandwidth توسط RIP برای پیدا کردن بهترین مسیر در نظر گرفته نمی شوند. پروتکل مسیریابی EIGRP از روش نسبتاً پیچیده تری برای محاسبه Metric Value استفاده می کند. EIGRP برای محاسبه Metric از عوامل مختلف مرتبط با کارایی شبکه اعم از موارد زیر برای محاسبه مقدار Metric Value استفاده می کند.

Bandwidth: (پهنای باند) عبارت است از مقدار اطلاعات عبور داده شده از کانال ارتباطی داده شده در واحد زمان. برای اندازه گیری پهنای باند از ضریب های بیت در ثانیه استفاده می شود. مثلا کیلوبیت در ثانیه. برای همین سرعت خطوط معمولی به صورت ۱۴/۴ و ۲۸/۸ و ۳۳/۶ و ۵۶ کیلوبیت در ثانیه نمایش داده می شود.

Delay: (تاخیر) مدت زمانی که طول می کشد بسته از Interface خارج شود. Delay هر Interface را می توان از خروجی Show Interface TYPE/NUM مشاهده و استخراج نمود. شایان ذکر است مقیاس عدد نمایش داده شده در خروجی Interface به کیلوبیت (Kb) می باشد.

MTU: (Maximum Transport Unit) عددی است که معمولاً بر حسب بایت بیان می‌شود و بیشینه اندازه قابل انتقال واحدهای اطلاعاتی را در یک رابط مشخص می‌کند. هریک از واسط‌هایی که توسط TCP/IP استفاده می‌شوند می‌توانند MTU مختص به خود داشته باشند.

$$\left[\frac{10\text{^}7}{\text{Min (Bandwidth)}} + \frac{\Sigma(\text{ Delays })}{10} \right] * 256 = \text{Metric Value}$$



heydari.farzad@gmail.com نام مدرس دوره: مهندس فرزاد حیدری
تهیه و گردآوری: دانیال نامورکهن

```
Router0#show interface fastEthernet 0/0
FastEthernet0/0 is up, line protocol is up (connected)
  Hardware is Lance, address is 000c.852c.8d01 (bia 000c.852c.8d01)
  Internet address is 10.0.0.9/30
  MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  ┊
  ┊
```

```
Router0#show interface serial 0/1/0
Serial0/1/0 is up, line protocol is up (connected)
  Hardware is HD64570
  Internet address is 10.0.0.1/30
  MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  ┊
  ┊
```

```
Router0#show ip eigrp topology
IP-EIGRP Topology Table for AS 1/ID(172.16.1.1)

Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - Reply status

P 10.0.0.0/8, 1 successors, FD is 28160
         via Summary (28160/0), Null0
P 10.0.0.0/30, 1 successors, FD is 2169856
         via Connected, Serial0/1/0
P 10.0.0.4/30, 1 successors, FD is 2177536
         via 10.0.0.10 (2177536/2174976), FastEthernet0/0
         via 10.0.0.2 (2681856/2169856), Serial0/1/0
         via 10.0.0.22 (2681856/2169856), Serial0/1/1
P 10.0.0.8/30, 1 successors, FD is 28160
         via Connected, FastEthernet0/0
P 10.0.0.12/30, 1 successors, FD is 30720
         via 10.0.0.10 (30720/28160), FastEthernet0/0
P 10.0.0.16/30, 1 successors, FD is 33280
         via 10.0.0.10 (33280/30720), FastEthernet0/0
         via 10.0.0.22 (2172416/28160), Serial0/1/1
P 10.0.0.20/30, 1 successors, FD is 2169856
         via Connected, Serial0/1/1
P 172.16.0.0/16, 1 successors, FD is 28160
         via Summary (28160/0), Null0
P 172.16.1.0/24, 1 successors, FD is 28160
         via Connected, FastEthernet0/1
P 192.168.1.0/24, 1 successors, FD is 35840
         via 10.0.0.10 (35840/33280), FastEthernet0/0
         via 10.0.0.22 (2172416/28160), Serial0/1/1
```

```
Router0#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route
Gateway of last resort is not set
     10.0.0.0/8 is variably subnetted, 7 subnets, 2 masks
D       10.0.0.0/8 is a summary, 00:27:37, Null0
C       10.0.0.0/30 is directly connected, Serial0/1/0
D       10.0.0.4/30 [90/2177536] via 10.0.0.10, 00:27:27, FastEthernet0/0
C       10.0.0.8/30 is directly connected, FastEthernet0/0
D       10.0.0.12/30 [90/30720] via 10.0.0.10, 00:27:36, FastEthernet0/0
D       10.0.0.16/30 [90/33280] via 10.0.0.10, 00:27:36, FastEthernet0/0
C       10.0.0.20/30 is directly connected, Serial0/1/1
     172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
D       172.16.0.0/16 is a summary, 00:27:37, Null0
C       172.16.1.0/24 is directly connected, FastEthernet0/1
D    192.168.1.0/24 [90/35840] via 10.0.0.10, 00:27:35, FastEthernet0/0
```

```
Router0#show ip protocols

Routing Protocol is "eigrp  1 "
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Default networks flagged in outgoing updates
  Default networks accepted from incoming updates
  EIGRP metric weight K1=1, K2=0, K3=1, K4=0, K5=0
  EIGRP maximum hopcount 100
  EIGRP maximum metric variance 1
Redistributing: eigrp 1
  Automatic network summarization is in effect
  Automatic address summarization:
    10.0.0.0/8 for FastEthernet0/1
      Summarizing with metric 28160
    172.16.0.0/16 for FastEthernet0/0, Serial0/1/0, Serial0/1/1
      Summarizing with metric 28160
  Maximum path: 4
  Routing for Networks:
     10.0.0.0/30
     10.0.0.8/30
     10.0.0.20/30
     172.16.1.0/24
  Routing Information Sources:
    Gateway         Distance      Last Update
    10.0.0.10       90            0
    10.0.0.2        90            5867
    10.0.0.22       90            185972
  Distance: internal 90 external 170
```

فصل چهاردهم

پروتکل مسیریابی OSPF

به عنوان یک پروتکل استاندارد و Link-State (نقشه کشی جامع مسیرها) از مجموعه پروتکل های Shortest Path First می باشد و یکی از پیچیده ترین Routing Protocol های مورد استفاده در روترهاست. هر روتر سه جدول جداگانه را ایجاد می نماید. یکی از این جداول وضعیت همسایگانی را که مستقیماً به آن متصل شده اند در خود نگهداری می نماید. در جدول دیگر، توپولوژی تمامی شبکه نگهداری می گردد و از جدول سوم برای نگهداری اطلاعات روتینگ استفاده می شود.

پروتکل Link-State نسبت به پروتکل های روتینگ Distance-Vector دارای اطلاعات بیشتری در ارتباط با شبکه و ارتباطات بین شبکه ای می باشند. پروتکل های Link-State اطلاعات بهنگام خود را برای سایر روترهای موجود در شبکه ارسال می نمایند (وضعیت لینک) .

OSPF (برگرفته شده از Open Shortest Path First) یک پروتکل روتینگ IP است که دارای تمامی ویژگی های یک پروتکل Link-State است .پروتکل فوق، یک پروتکل روتینگ استاندارد باز است که توسط مجموعه ای از تولیدکنندگان شبکه از جمله شرکت سیسکو ایجاد شده است. در صورتی که در یک شبکه از روترهائی استفاده می گردد که تمامی آنها متعلق به شرکت سیسکو نمی باشند (تنوع سازنده)، نمی توان از پروتکل EIGRP استفاده کرد. در چنین مواردی می توان از گزینه هائی دیگر نظیر RIP، RIPv2 و یا OSPF استفاده نمود. در صورتی که ابعاد یک شبکه بسیار بزرگ باشد، تنها گزینه موجود پروتکل OSPF و یا استفاده از Route Redistribution است (یک سرویس ترجمه بین پروتکل های روتینگ).

OSPF ، با استفاده از الگوریتم Dijkstra کار می کند. در ابتدا، اولین درخت کوتاهترین مسیر ایجاد می گردد و در ادامه جدول روتینگ از طریق بهترین مسیرها توزیع می گردد. این پروتکل دارای سرعت همگرائی بالائی است (شاید به اندازه سرعت همگرائی EIGRP نباشد) و از چندین مسیر با cost یکسان به مقصد مشابه حمایت می نماید. برخلاف EIGRP ، پروتکل OSPF صرفاً از روتینگ IP حمایت می نماید. به منظور جلوگیری از زیاد شدن پردازش ها در OSPF مدیر شبکه با توجه به ابعاد و شرایط سازمان و آنالیز فاکتورهای کمی و کیفی جمع آوری شده اقدام به ناحیه بندی شبکه یا ایجاد Area های متعدد می نماید.

مهمترین معایبی که در OSPF وجود دارد این است که OSPF برای نگهداری لیست OSPF Neighbor ها ، توپوپولوژی شبکه که شامل یک دیتابیس از تمامی روترها و Route های موجود در آنهاست و همچنین Routing Table خود روتر به حافظه RAM نسبتاً بیشتری در مقایسه با پروتکل های Vector-Distance نیاز دارد ، همچنین OSPF به قدرت پردازشی یا CPU بیشتری برای اجرا کردن الگوریتم SPF نیاز دارد و همین موارد باعث می شود که OSPF در رده بندی پروتکل های مسیریابی پیچیده یا Complex Protocol قرار بگیرد. دو مفهوم بسیار مهم در مواردی که می خواهید از OSPF استفاده کنید وجود دارند که اولین مفهوم **A**utonomous **S**ystem و دومین مفهوم Area می باشد.

Area در OSPF برای ایجاد کردن ساختار مسیریابی سلسله مراتبی یا موروثی (Hierarchical Routing) در یک Autonomous System استفاده می شود. Areaها تعیین کننده این هستند که چگونه و به چه اندازه اطلاعات مربوط به Routing بایستی در شبکه به اشتراک گذاشته شود. OSPF دو لایه وراثت یا Hierarchy دارد، لایه Backbone یا Area 0 و لایه های خارج از Backbone یا Areaهای بین عدد ۱ تا ۶۵۵۳۵ ، ایندو Area دو Area متفاوت هستند که بین آنها اطلاعات مسیریابی رد و بدل می شود.

در توپولوژی OSPF نیز روترها همانند پروتکل EIGRP مسیرها را به هم یاد می دهند با این تفاوت که در EIGRP از روش Topology Exchange و در پروتکل OSPF از Databae Exchange استفاد می شود و پس از آن اجرای الگوریتم SPF انجام می شود. آن مسیری که Cost کمتری دارد در جدول روتینگ و مابقی مسیرها در Database قرار می گیرند.

مراحل معرفی و انجام عملیات مسیریابی با استفاده از پروتکل OSPF

به منظور پیاده سازی صحیح در انجام مسیریابی تحت پروتکل OSPF و اخذ نتیجه مطلوب انجام مراحل (چک لیست) زیر پیشنهاد می گردد ولی قبل از آن لازم است با اصطلاحاتی که در این پروتکل مورد استفاده قرار می گیرد آشنایی پیدا کنیم.

- **AS**: (Autonomous System) یک AS یک گروه از روترهایی میباشد که تحت کنترل یک مدیریت واحد بوده و از یک پروتکل روتینگ مشترک استفاده میکنند بعنوان مثال: یک Corporate Internet و یا یک شبکه ISP میتوانند بعنوان یک AS واحد عمل نمایند.
- **Backbone Area**: Area اصلی و یکتاست که به عنوان Area مرکزی شبکه شناخته شده و با عدد صفر مشخص می گردد.
- **Backbone Router**: به روتری که در Area 0 یا Backbone Area قرار دارد، اطلاق می گردد.
- **Normal Area**: سایر Area ها که با Area 0 در تعامل هستند اطلاق می گردد و عدد Area آنها می تواند ۱ تا ۶۵۵۳۵ باشد.
- **Internal Router**: به روتری که تمامی Interface های (دست ها) آن داخل یک Area باشد گفته می شود.
- **ABR**: (Area Border Router) روتری است که در حاشیه و مرز دو یا چند Area قرار می گیرد و مابین آنها ارتباط برقرار می کند.
- **Loopback Interface**: این نوع از interface در واقع یک virtual interface بر روی روتر است و به صورت پیش فرض روتر فاقد loopback است. کارآیی و نوع برخورد با آن مشابه یک interface فیزیکی است و همچنین می توانید به آنها IP Address نیز اختصاص دهید. Loopback Interface همیشه Active و up است و در گزارش از مسیرها مشاهده می شود، با این وصف نیازی به قرار دادن و تنظیم یک PC روی پورت برای کنترل و تست مسیرها نخواهید داشت و همچنین در هنگام برقراری ارتباط از طریق Telnet نیازی به Interface خاص نخواهد بود. عدد ۰ الی ۲۱۴۷۴۸۳۶۴۷ برای loopback قابل انتخاب می باشد.
- **Router ID**: هر روتر در پروتکل OSPF جهت تهیه نقشه کلی به یک Router ID منحصر به فرد نیاز دارد. OSPF Router ID برای شناسایی یک روتر در توپولوژی OSPF استفاده می شود. معیار و اولویت انتخاب Router_ID به قرار زیر است:

۱- Manually by Direct Command: هر آدرس دستی که به عنوان OSPF Router ID به روتر معرفی شده باشد در فرآیند انتخاب به عنوان OSPF Router ID انتخاب می شود.

۲- Loopback: اگر بر روی روتر OSPF Router ID پیکربندی نشده باشد، بالاترین آدرس IP که بر روی هر یک از Loopback Interface های روتر وجود داشته باشد بصورت خودکار به عنوان OSPF Router ID در فرآیند انتخاب OSPF Router ID انتخاب خواهد شد.

۳- Highest Interface IP Address: اگر هیچ Loopback Interface بر روی روتر تعریف نشده باشد بالاترین آدرس IP از میان Interface های فعال روتر بصورت خودکار به عنوان OSPF Router ID انتخاب خواهد شد.

مراحل پیاده سازی :

۱- تعیین و ترسیم توپولوژی یا ساختار شکلی شبکه و مشخص نمودن Area های مورد نیاز در شبکه با در نظر گرفتن تجهیزات سخت افزاری، نرم افزاری و مخابراتی داخلی و خارجی سازمان، پراکندگی مکانی و منابع انسانی، نرخ رشد و توسعه و ...

۲- تعیین روترهای Internal در هر Area

۳- تعیین روترهای ABR مابین Area ها

۴- نصب و انجام تنظیمات سخت افزاری و برقراری ارتباط کابلی روترها با توجه به نوع Interface های تعبیه شده

۵- معرفی و اختصاص IP Address برای Interface های مورد استفاده بر روی هر روتر (Point-to-Point , Default Gateway for Network ، Loopback) با توجه به چیدمان و ساختار شکلی و ساختار آدرس دهی شبکه ها متناسب با محدوده های تعریف شده.

۶- ایجاد و معرفی OSPF به همراه AS مربوطه بر روی هر روتر

```
Router(config)# router ospf AS_NUM          */ example : router ospf 1
```

۷- اختصاص Router_ID بر روی هر روتر در پروتکل OSPF

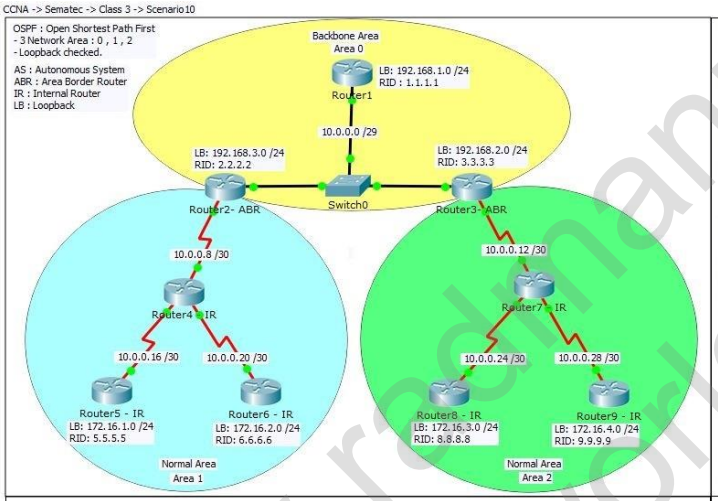
```
Router(config-router)# router-id ROUTER_ID        */ example : router-id 1.1.1.1 , 2.2.2.2 , ….
Router# clear ip ospf process                     */ clear and reset ospf on a router, (regenerate neighborhood)
```

۸- معرفی کلیه Interface های IP دار در پروتکل OSPF (دقت و توجه به شماره ای که به AS اختصاص داده اید و همچنین شماره مربوط به Area و محدوده ای که Interface روتر در آن قرار دارد بسیار حایز اهمیت می باشد.

```
Router(config-router)# network   NETWORK_NUM   WILD_CARD  area   AREA_Num
```

۹- تست و کنترل عملکرد از طریق تهیه گزارش های متعدد در حین انجام مراحل فوق یا پس از پایان مراحل.

```
Router# show ip router connected                  */ display connected interfaces on a router
Router# show ip ospf neighbor                     */ display neighbors connected to a router
Router# show ip ospf interface TYPE/NUM           */ display a router's port information
Router# show ip ospf border-routers                */ display ABR router / s
Router# show ip route ospf                        */ display routes learned by ospf
Router# show ip route                             */ display all routes (routing table)
```




```
Router1#show ip route
Codes:
C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route
Gateway of last resort is not set

     10.0.0.0/8 is variably subnetted, 7 subnets, 2 masks
C       10.0.0.0/29 is directly connected, FastEthernet0/0
O IA    10.0.0.8/30 [110/65] via 10.0.0.3, 00:05:42, FastEthernet0/0
O IA    10.0.0.12/30 [110/65] via 10.0.0.2, 00:05:42, FastEthernet0/0
O IA    10.0.0.16/30 [110/129] via 10.0.0.3, 00:05:42, FastEthernet0/0
O IA    10.0.0.20/30 [110/129] via 10.0.0.3, 00:05:42, FastEthernet0/0
O IA    10.0.0.24/30 [110/129] via 10.0.0.2, 00:05:42, FastEthernet0/0
O IA    10.0.0.28/30 [110/129] via 10.0.0.2, 00:05:42, FastEthernet0/0
     172.16.0.0/32 is subnetted, 4 subnets
O IA    172.16.1.1 [110/130] via 10.0.0.3, 00:05:42, FastEthernet0/0
O IA    172.16.2.1 [110/130] via 10.0.0.3, 00:05:42, FastEthernet0/0
O IA    172.16.3.1 [110/130] via 10.0.0.2, 00:05:42, FastEthernet0/0
O IA    172.16.4.1 [110/130] via 10.0.0.2, 00:05:42, FastEthernet0/0
C    192.168.1.0/24 is directly connected, Loopback0
     192.168.2.0/32 is subnetted, 1 subnets
O       192.168.2.1 [110/2] via 10.0.0.2, 00:05:42, FastEthernet0/0
     192.168.3.0/32 is subnetted, 1 subnets
O       192.168.3.1 [110/2] via 10.0.0.3, 00:05:42, FastEthernet0/0
```

```
Router1#show ip route ospf
     10.0.0.0/8 is variably subnetted, 7 subnets, 2 masks
O IA    10.0.0.8 [110/65] via 10.0.0.3, 01:09:19, FastEthernet0/0
O IA    10.0.0.12 [110/65] via 10.0.0.2, 01:09:19, FastEthernet0/0
O IA    10.0.0.16 [110/129] via 10.0.0.3, 01:09:19, FastEthernet0/0
O IA    10.0.0.20 [110/129] via 10.0.0.3, 01:09:19, FastEthernet0/0
O IA    10.0.0.24 [110/129] via 10.0.0.2, 01:09:19, FastEthernet0/0
O IA    10.0.0.28 [110/129] via 10.0.0.2, 01:09:19, FastEthernet0/0
     172.16.0.0/32 is subnetted, 4 subnets
O IA    172.16.1.1 [110/130] via 10.0.0.3, 01:09:19, FastEthernet0/0
O IA    172.16.2.1 [110/130] via 10.0.0.3, 01:09:19, FastEthernet0/0
O IA    172.16.3.1 [110/130] via 10.0.0.2, 01:09:19, FastEthernet0/0
O IA    172.16.4.1 [110/130] via 10.0.0.2, 01:09:19, FastEthernet0/0
     192.168.2.0/32 is subnetted, 1 subnets
O       192.168.2.1 [110/2] via 10.0.0.2, 01:09:19, FastEthernet0/0
     192.168.3.0/32 is subnetted, 1 subnets
O       192.168.3.1 [110/2] via 10.0.0.3, 01:09:19, FastEthernet0/0
```

```
Router1#show ip ospf interface fastEthernet 0/0

FastEthernet0/0 is up, line protocol is up
  Internet address is 10.0.0.1/29, Area 0
  Process ID 1, Router ID 192.168.1.1, Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State DROTHER, Priority 1
  Designated Router (ID) 192.168.3.1, Interface address 10.0.0.3
  Backup Designated Router (ID) 192.168.2.1, Interface address 10.0.0.2
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:08
  Index 2/2, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 2, Adjacent neighbor count is 2
    Adjacent with neighbor 192.168.3.1  (Designated Router)
    Adjacent with neighbor 192.168.2.1  (Backup Designated Router)
  Suppress hello for 0 neighbor(s)
```

```
Router1#show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
192.168.2.1       1   FULL/BDR        00:00:32    10.0.0.2        FastEthernet0/0
192.168.3.1       1   FULL/DR         00:00:32    10.0.0.3        FastEthernet0/0
```

```
Router1#show ip ospf border-routers
OSPF Process 1 internal Routing Table

Codes: i - Intra-area route, I - Inter-area route

i 192.168.2.1 [1] via 10.0.0.2, FastEthernet0/0, ABR, Area 0, SPF 1
i 192.168.3.1 [1] via 10.0.0.3, FastEthernet0/0, ABR, Area 0, SPF 1
```

- O (OSPF): نشان دهنده این است که آن مسیر داخل همان Area است
- O IA (OSPF Inter Area): به این نکته اشاره می کند که آن مسیر از Area دیگری یاد گرفته شده است.
- C (Connected): مسیر یا مسیرهایی است که روتر گزارش گیرنده به پروتکل OSPF معرفی نموده است.

روش محاسبه مسیر پروتکل OSPF

پروتکل مسیریابیOSPF از معیاری به نام Cost برای محاسبه Metric و از یک پهنای باند مرجع یا Reference Bandwidth به اندازه ۱۰۰ مگابیت بر ثانیه برای محاسبه Cost استفاده می کند. هر چقدر مقدار Cost کمتر باشد به معنای سرعت بیشتر لینک ارتباطی است . برای محاسبه Cost پروتکلOSPF از یک فرمول محاسباتی استفاده می کند که در آن Reference Bandwidth یا پهنای باند مرجع تقسیم بر پهنای باند interface یا Interface Bandwidth می شود و یا به عبارت دیگر از فرمول 10^8 / Bandwidth می توان استفاده نمود.

در نهایت نتیجه بدست آمده نمایانگر Cost لینک ارتباطی خواهد بود. برای مثال اگر شما یک لینک اترنت با سرعت ۱۰۰ Mbps داشته باشید مقدار OSPF Metric شما (100 Mbps / 10 Mbps) برابر ۱۰ خواهد شد.

پهنای باند مرجع یا Reference Bandwidth در OSPF بصورت ۱۰۰ Mbps در نظر گرفته می شود که همانطور که مشاهده کردید مقدار پیش فرض فرمول ما نیز هست، اما در این فرمول تفاوتی بین Interface هایی که بیشتر از ۱۰۰ Mbps سرعت دارند و آنهایی که ۱۰۰ Mbps سرعت دارند وجود ندارد و سرعت های بیش از از ۱۰۰ Mbps به منزله سرعت ۱۰۰ Mbps محاسبه خواهند شد.

Bandwidth	OSPF Cost
100 Gbps	1
40 Gbps	1
10 Gbps	1
1 Gbps	1
100 Mbps	1
10 Mbps	10
1.544 Mbps	64
768 Kbps	133
384 Kbps	266
128 Kbps	781

امروزه زیرساخت های شبکه با سرعت های ۱ Gbps و ۱۰ Gbps نیز بسیار معمول هستند و استفاده می شوند. اگر بخواهیم OSPF Cost را با توجه به فرمول بالا برای یک روتر که دارای دو کارت شبکه Fast Ethernet با سرعت ۱۰۰ Mbps و یک کارت شبکه ۱ Gbps محاسبه کنیم در نهایت هر دو به یک جواب خواهند رسید. اگر می خواهید این رفتار پیش فرض را تغییر دهید، می توانید با استفاده از دستور auto-cost در فرآیند مسیریابیOSPF اینکار را انجام دهید. اگر می خواهید Reference Bandwidth در OSPF را تغییر دهید بایستی مطمئن شوید که اینکار بر روی تمامی روترهایی که در شبکه شما بصورت OSPF پیکربندی شده اند نیز انجام شده باشد. جدول پیش رو لیست Cost های پیش فرض برای پهنای باند های مختلف را نشان می دهد :

```
Router(config-router)# auto cost refrence bandwidth 1000      */ Attention !!!. If need to change, must be set on all router.
```

بسته های Hello و Hold در OSPF

یک بسته با IP Address ۲۲۴,۰,۰,۵ (کلاس D) برای این پروتکل رزرو شده است و هر دریافت کننده ای به محض دریافت این بسته متوجه خواهد شد که این بسته متعلق به پروتکل OSPF است. بر خلاف پروتکل EIGRP چنانچه زمان Hello و Hold با یکدیگر فرق کند، همسایگی در پروتکل OSPF تشکیل نخواهد شد. شایان ذکر است در برخی مستندات از اصطلاح Death Time به جای Hold Time استفاده شده است. تغییر زمان Hello بر روی Interface صورت می گیرد و وقتی زمان مربوط به Hello تغییر داده شود به صورت اتوماتیک چهار برابر آن برای Hold در نظر گرفته خواهد شد.

```
Router(config-if)# ip ospf hello-interval SECONEDS          */ Seconds range 0-65535
```

Active / Passive

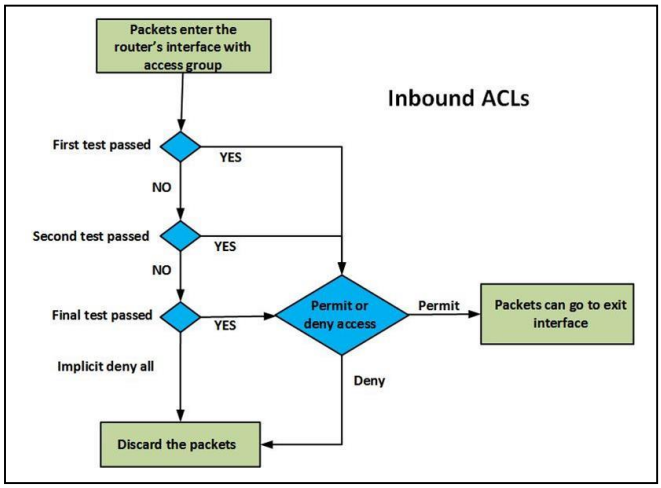
برای کاهش ترافیک شبکه و جلوگیری از ارسال بسته Hello به Interface هایی که مستقیماً به کامپیوتر یا سوییچ متصل شده اند و هیچ شناختی از این بسته ندارند، باید آن پورت را در حالت Passive قرار داد.

```
Router1(Config)# router eigrp ASN                                  */ Set an OSPF
Router1(Config-router)# passive-interface TYPE MOD/NUM             */ Send Hello Packet to Interface
Router1(Config-router)# no passive-interface TYPE MOD/NUM          */ Don't Send Hello Packet to Interface
Router1(Config-router)# passive-interface default                  */ *Attention* Passive all Interfaces ( 1 of 100 )
Router1(Config-router)# no passive-interface default               */ Active All Interfaces
```


heydari.farzad@gmail.com نام مدرس دوره: مهندس فرزاد حیدری
تهیه و گردآوری: دانیال نامورکهن

فصل پانزدهم

Access List



در این سرفصل به طور جامع در خصوص Access List ها، قوانین موجود در تعریف ACL ها، انواع Wildcard Mask می پردازیم. در سرفصل های بعدی در خصوص پیکربندی انواع ACL ها و سناریوهای مختلف پیکربندی ACL بحث خواهد شد. به طور پیش فرض بعد از اینکه روترها شروع به کار می کنند، تمامی پیامها قادر به عبور از یک Interface به Interface های دیگر خواهند بود.

اما شرایطی پیش خواهد آمد که شما برای مقاصد مختلف، چه مباحث امنیتی شبکه و چه سیاست های کلی که در پیش گرفته شده اند، نیاز به اعمال محدودیت در انتقال ترافیک شبکه خواهیم داشت. سیسکو ما را قادر می سازد که در شرایط گفته شده، عبور ترافیک شبکه از یک اینترفیس به اینترفیس های دیگر را کنترل کنیم. ACL ها یکی از خصوصیات قدرتمند IOS می باشند که سیسکو در کنار IP، پروتکل های دیگری را نیز مانند DECnet، XNS، Apple Talk، IPX برای استفاده از ACL پشتیبانی می کند.

Access List یا همان ACL در حقیقت روشی برای فیلتر کردن ترافیک خروجی و ورودی بر روی Interface های روتر می باشد، به صورت پیش فرض همه ترافیک قابلیت ورود و خروج از همه Interface های روتر را خواهند داشت که شما با استفاده از توانمندی ACL ها می توانید ورود و خروج ترافیک را براساس قوانین و پروتکل های خاص فیلتر نمائید. شما می توانید به وسیله ACLها تعیین کنید که چه ترافیکی با چه مشخصاتی از Interface روتر اجازه ورود یا خروج را داشته باشد. از ACL ها در دستوراتی مانند NAT و برخی دستورات دیگر استفاده می شود. شما برای استفاده از ACL ها باید آنها را تعریف نمایید و در مرحله بعد ACL ها را به اینترفیسی که قصد کنترل ترافیک آن را خواهید داشت نسبت دهید که همه ترافیک ها با قوانین موجود در ACL بررسی شوند که براساس این قوانین به ترافیک اجازه ورود یا خروج داده می شود.

آشنایی با ACL در سیسکو

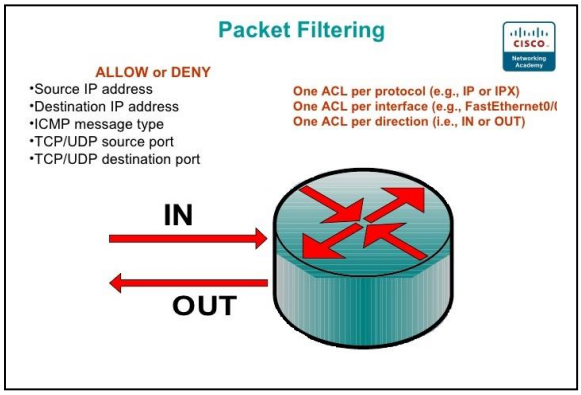
علاوه بر اینکه ACL ها در فیلتر کردن ترافیک های انتقالی در شبکه مورد استفاده قرار می گیرند، برای مقاصد مختلف نیز می توان از آنها بهره برد. برای نمونه چند کاربرد عمده آنها عبارتند از:

- محدود کردن دسترسی از طریق VTY TELNET
- فیلتر کردن اطلاعات routing
- اولویت بندی ترافیک مربوط به WAN
- تغییر پارامتر Administrative distance
- برقراری تماس های تلفنی DDR (Dial-Demand Routing)

ACL ها در Global configuration mode ایجاد شده و سپس آنها را باید فعال نمود. برای کنترل ترافیک انتقالی از راه Interface ها، ACL ها را باید روی Interface مورد نظر فعال نماییم. در هنگام فعال نمودن ACL های 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:

۱- ترافیک ورودی یا Inbound

۲- ترافیک خروجی یا Outbound



در ترافیک ورودی روتر اطلاعات رسیده را ابتدا با ACL های تعیین شده در روی Interface 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 اراسل کرده و سپس اقدام به مقایسه آنها با ACL مربوطه می نماید. یکی از محدودیت هایی که استفاده از ACL داراست این است که نمی توان ترافیکی که خود روتر آنها را ایجاد کرده به وسیله ACL 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 دستگاه های دیگر نماییم، نمی توان این ترافیک ها را به وسیله ACL ها 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.

قوانین موجود در تعریف ACL ها

هر ACL باید با یک شماره یا یک نام منحصر بفرد شناسایی شود.شما قادر خواهید فقط یک ACL را به یک اینترفیس assign کنید.یک ACL بر اساس شرایط و قوانین خاص ترافیک را فیلتر می کند که برخی از این پارامترها که ACL بر اساس آنها می تواند اقدام به بررسی ترافیک نماید، به شرح زیر می باشد:

۱- براساس Source IP Address یا آدرس فرستنده
۲- براساس Destination IP Address یا آدرس مقصد یا گیرنده
۳- براساس شماره پورت خاص
۴- براساس پروتکل های UDP و TCP
۵- براساس یکسری از پروتکلهای شبکه مانند ICMP، OSPF، EIGRP، IGMP و ...

همانطور که اشاره شد، یک ACL لیستی از دستورات می باشد که با یک شماره یا نام شناسایی می شود و این دستورات از بالا به پایین مورد بررسی قرار می گیرند، پس به این نکته توجه داشته باشید که ترتیب نوشتن دستورات داخل ACL بسیار مهم است و در پایان هر ACL یک Deny All وجود دارد که این عبارت Deny All را شما مشاهده نمی کنید ولی توسط خود IOS اضافه خواهد شد. پس در صورتی که ترافیک شما با هیچ کدام از قوانین داخل ACL مطابقت نداشته باشد آن ترافیک Deny خواهد شد. یعنی اجازه عبور از آن Interface را نخواهد داشت. وقتی ترافیک قصد عبور از اینترفیسی را که یک ACL به آن نسبت داده شده است دارد، باید آن ترافیک با دستورات داخل ACL مطابقت شود و خط به خط دستورات ACL بررسی می شوند و در صورتی که، اطلاعات با یکی از خطوط ACL مطابقت داشته باشد، آن قانون اعمال خواهد شد و خطوط بعد از آن قانون دیگر بررسی نخواهند شد و در صورتی که هیچکدام از قوانین داخل ACL با ترافیک مطابقتی نداشته باشند، پیام از بین خواهد رفت. از اینروست که ترتیب مشخص نمودن قانون های موجود در یک ACL بسیار مهم است.

برای مثال اگر دو قانون برای دسترسی به یک دستگاه، که یکی اجازه عبور را داده و یکی نداده در جدول موجود باشند، قانونی را که در اول نوشته شده باشد اجرا شده و از دیگری صرف نظر خواهد شد. برای همین هم در هنگام نوشتن قانون ها موارد اختصاصی تر را باید در اول نوشته و موارد عمومی تر را در آخر لیست قرار دهیم. برای درک بهتر، مثالی را مطرح میکنیم. فرض کنید که یک ACL دارای دو عدد قانون یا به اصطلاح statement در لیست خود می باشد. به ترتیب زیر:

۱- اجازه دسترسی از شبکه ۱۷۲,۱۶,۰,۰ /۱۶
۲- محدودیت دسترسی از دستگاه ۱۷۲,۱۶,۱,۱

با یادآوری این نکته که لیست ACL از بالا به پایین پردازش می شود، فرض می کنیم که روتر یک پیام را با آدرس فرستنده ۱۷۲,۱۶,۱,۱ دریافت کرده است. روتر این آدرس را با اولین مورد موجود در لیست مقایسه می کند: آیا پیام رسیده از طرف شبکه ۱۷۲,۱۶,۰,۰۱۶ می باشد؟ جواب مثبت است و بنابراین اجازه عبور به ترافیک رسیده داده نخواهد شد. اما به دلیل اینکه مورد اول با پیام رسیده مطابقت داشت، مورد دوم هیچ وقت پردازش نخواهد شد. در این مثال همه ترافیک هایی که مربوط به شبکه ۷۲,۱۶,۰,۰۱۶ می باشند، اجازه عبور خواهند یافت، حتی آدرس ۱۶/۱۷۲,۱۶,۱,۱.

بیایید که ترتیب نوشتن دو قانون بالا را تغییر دهیم. بدین صورت:

۱. محدودیت دسترسی از دستگاه ۱۷۲,۱۶,۱,۱
۲. اجازه دسترسی از شبکه ۱۶/ ۱۷۲,۱۶,۰,۰

اگر دستگاه ۱۷۲,۱۶,۱,۱ ترافیکی را به روتر بفرستد، روتر اولین مورد موجود در لیست ACL را با مشخصات پیام مقایسه کرده و از آنجایی که در همان اولین قدم تطابق موردنظر حاصل شد، روتر قانون اول را در مورد پیام رسیده صزفنظر از اینکه چه نوع ترافیکی باشد از بین خواهد رفت. اگر دستگاه دیگری مثل ۱۷۲,۱۶,۱,۲ اقدام به ارسال ترافیک برای روتر نماید، روتر مشخصات پیام را با اولین مورد موجود در لیست ACL مقایسه کرده و به دلیل نیافتن مطابقت مورد نظر، مورد دوم پردازش خواهد شد که تطابق وجود داشته و اجازه دسترسی به ترافیک فوق داده می شود. از همین روست که گفته می شود ترتیب نوشتن هریک از موارد لیست ACL بسیار مهم بوده و انتقال ترافیک شبکه را تحت تاثیر قرار خواهد داد. در تعریف ACLها 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 ACL مورد بررسی قرار بگیرند و به عبارت دیگر مشخص کننده قسمتی از آدرس IP Address می باشد که باید در ACL مورد بررسی قرار بگیرد.Wildcard Mask دقیقاً برعکس Subnet Mask می باشد به جای bit 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 ماسک ۲۵۵,۲۵۵,۰,۰ را در اختیار داریم. اگر این ماسک را در مبنای ۲ بنویسیم خواهیم داشت:

۱۱۱۱۱۱۱۱,۱۱۱۱۱۱۱۱,۰۰۰۰۰۰۰۰,۰۰۰۰۰۰۰۰ = ۲۵۵,۲۵۵,۰,۰

سرانجام اگر این subnet mask را تبدیل به wildcard mask نماییم، نتیجه به صورت زیر خواهد بود:

۰۰۰۰۰۰۰۰,۰۰۰۰۰۰۰۰,۱۱۱۱۱۱۱۱,۱۱۱۱۱۱۱۱

که در این صورت تبدیل این آدرس به حالت دسیمال یا مبنای ۱۰ آدرس ۰,۰,۲۵۵,۲۵۵ به دست خواهد آمد. در این مثال wildcard mask به روتر می گوید که فقط ۱۶ بیت از اول آدرس IP پیا رسیده 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 قانون های بعدی خواهد پرداخت.دو نوع مخصوص از wildcard mask وجود دارد:

1. ۰,۰,۰,۰
2. ۲۵۵,۲۵۵,۲۵۵,۲۵۵

Mask 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 مورد نظر روی آن اجرا شود. برای همین هم اگر wildcard mask برابر با ۰,۰,۰,۰ باشد، به نام host mask نامیده می شود.

یک مثال ساده میزنیم: اگر قانون موجود در ACL را به صورت مقابل داشته باشیم: ۱۹۲,۱۶۸,۱,۱ ۰,۰,۰,۰ به این معنی است که روتر دقیقاً 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 صورت ۱۹۲,۱۶۸,۱,۱ ۰,۰,۰,۰ تنظیم نمودیم، روتر به طور اتوماتیک آن را به حالت host 192.168.1.1 در خواهد آورد.

Mask دوم (۲۵۵,۲۵۵,۲۵۵,۲۵۵) به روتر می فهماند که همه آدرس هایی که وارد روتر می شوند قابل پذیرش بوده و قانون مزبور روی همه پیام های ورودی اجرا خواهند شد. معمولاً 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 ۰,۰,۰,۰ که روتر آن را به صورت any 0.0.0.0 در خواهد آورد. آدرس IP نوشته شده در این فرمول اهمیت چندانی نداشته و می توان هر آدرسی را به دلخواه وارد نمود. مثلاً 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 Mask 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
0.0.0.0	255.255.255.255	تمامی آدرس ها پذیرفته خواهد شد.
172.16.1.1	0.0.0.0	بسته رسیده باید حتماً دارای آدرس ذکر شده باشد تا قانون مورد نظر بر روی آن اجرا شود.
172.16.1.1	0.0.0.255	قانون مذکور بر روی بسته رسیده از شبکه ۱۷۲,۱۶,۱,۰ اعمال می شود.
172.16.2.0	0.0.1.255	قانون مذکور بر روی بسته هایی که دارای آدرس ۱۷۲,۱۶,۲,۰ /۲۳ اعمال می شود.
172.16.0.0	0.0.255.255	قانون مذکور بر روی بسته هایی که دارای آدرس ۱۷۲,۱۶,۰,۰ اعمال می شود.

Access Listها دو نوع به شرح زیر می باشند:

۱. Standard Access List
۲. Extended Access List

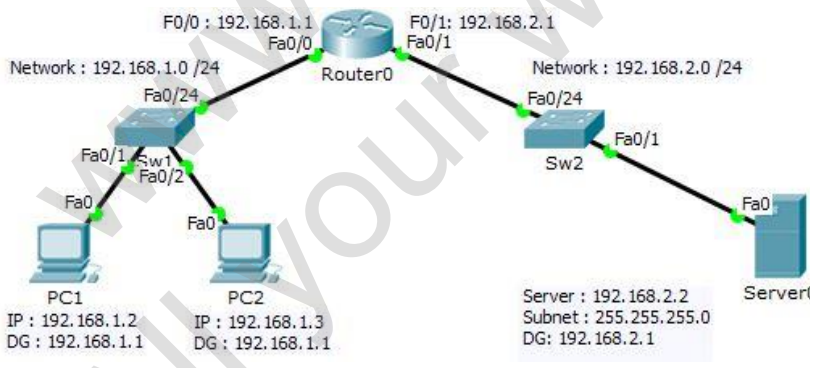
Standard Access List: توسط این ACL ها می توانید اقدام به کنترل ترافیک ورودی و خروجی براساس source ip address یا آدرس فرستنده نمایید و این نوع ACL قادر به کنترل ترافیک ورودی و خروجی براساس پروتکل ها و پورت ها و همچنین براساس آدرس مقصد نمی باشد. این ACL ها از طریق شماره شناسایی می شوند. شماره های ۹۹ – ۱ و ۱۹۹۹ – ۱۳۰۰ مربوط به Standard Access List ها می باشد.

Extended Access List: این ACL ها قادر به کنترل ترافیک ورودی و خروجی براساس پروتکل های لایه ۳ مانند IP و همچنین پروتکل های TCP، UDP و همچنین براساس پورت ها و سایر پروتکل های شبکه مانند ICMP، IGMP، OSPF، EIGRP و ... می باشند. این ACL ها از طریق شماره شناسایی می شوند. شماره های ۱۹۹ – ۱۰۰ و ۲۶۹۹ – ۲۰۰۰ مربوط به Extended Access List ها می باشد.

ACL های استاندارد ساده ترین نوع ACL ها می باشند و عمل فیلتر کردن ترافیک ها را فقط براساس آدرس IP منبع فرستنده پیام انجام می دهند. دستور زیر را می توان برای ایجاد یک ACL استاندارد به کار برد:

Router(config) access-list ACL_NUM <{permit} | {deny} SOURCE_IP_ADDRESS WILDCARD_MASK

برای درک بهتر و آسانتر از طریق یک سناریو پیکربندی Standard Access List بر روی یک روتر را نشان می دهیم:



مرحله اول : پیکربندی IP Address روی Interface های روتر

مرحله دوم : پیکربندی Standard Access List بر روی روتر: در این مرحله ما یک access list نوع standard تعریف خواهیم نمود ، همانطور که در دستور مشاهده می کنید، با این ACL مانع از دسترسی کامپیوتر PC2 به سرور خواهیم شد.

1

```
Router(config)# access-list 1 deny host 192.168.1.3
Router(config)# access-list 1 permit any
```

Router(config)#access-list 1 deny host 192.168.1.3 دستور اول */

در این خط ما با دستور access list 1 یک ACL نوع استاندارد با شماره ۱ تعیین نموده ایم. در ادامه همین دستور عبارت deny ذکر شده است که برای مانع شدن ترافیک استفاده می شود. در ادامه دستور کلمه host ذکر شده است، اشاره به تعریف یک host خاص با IP مشخص را دارد که آدرس این Host در این مثال ۱۹۲,۱۶۸,۱,۳ می باشد.

نتیجه اعمال ACL: این خط از ACL مانع از عبور ترافیکی که مبدا آن PC-2 باشد، خواهد شد.

Router(config)#access-list 1 permit any دستور دوم */

در خط بعد، قانون دوم را به ACL 1 اضافه می کنیم که این بار به جای deny از عبارت permit استفاده شده است یعنی صدور اجازه عبور ترافیک و به جای تعیین شبکه یا host خاص به همه host اجازه داده شده است عبارت Any اشاره به کل آدرس های مبدا دارد.

نتیجه اعمال ACL: این خط از ACL اجازه عبور ترافیک از هر آدرس مبدایی را که باشد خواهد داد.

مرحله سوم: اعمال Access List به Interface

در این مرحله ما می خواهیم این ACL شماره ۱ را که در مرحله ۲ ایجاد نموده ایم، به اینترفیس F0/0 برای Inbound اعمال نماییم. این عمل باعث می شود که هر ترافیکی که می خواهد به این Interface وارد شود با قوانین داخل ACL شماره ۱ بررسی شود که آیا اجازه عبور دارد یا خیر.

Router(config-if) # ip access-group 1 inbound

مرحله ۴: کنترل و تصدیق پیکربندی ACL

در این مرحله از PC-2 که متصل به Switch1 می باشد، کامپیوتر Server، که متصل به Switch2 می باشد را ping میکنیم. همانطور که مشاهده می کنید، ارتباط بین PC2 و Server توسط ACL مسدود (deny) شده است.

```
SERVER>ping 192.168.1.3

Pinging 192.168.1.3 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.1.3:
    Packets: Sent = 4, Received = 0, Lost = 4 (100%
loss),
```

اعمال محدودیت در دسترسی به طریق Telnet:

در کنار قابلیت ACL های استاندارد برای کنترل ترافیک ورودی و خروجی از اینترفیس های روتر، می توان محدودیت هایی را در دسترسی از طریق telnet به روترها نیز اعمال کرد. مثلاً می توان فقط مدیران را قادر ساخت که از طریق telnet با روتر شما اتصال برقرار نمایند.

اولین قدم، ایجاد یک ACL است که در لیست آن آدرس IP تمامی دستگاه هایی که مدیران از طریق آن دستگاه ها به روتر ما ارتباط telnet را برقرار خواهند نمود مشخص کرده و اجازه دسترسی را به وسیله تایپ permit به آنها می دهیم. در مرحله بعدی ACL ایجادی خود را باید فعال سازیم، اما نه بر روی یکی از Interface های روتر. در چنین وضعیتی ACL مربوطه را باید در Vty Line فعال سازیم.

Router(config)# line VTY 0 4
Router(config)#access-class STANDARD_ACL_NUM in|out

یادآوری این نکته ضروری است که به صورت پیش فرض ۵ ارتباط همزمان telnet را می توان به یک روتر برقرار نمود که با مشخص کردن ارتباط اول، یعنی ۰، و ارتباط آخر، یعنی ۴، این ACL در روی تمامی ۵ ارتباط فعال خواهند شد. اگر به خاطر دلایلی مثل فراموشی، ACL ایجاد شده را در روی تعدادی از ارتباطات telnet فعال نساخته باشیم، باعث بروز مشکلات امنیتی در شبکه خواهیم شد. پارامتر in باعث اعمال محدودیت بر روی ارتباطات telnet ورودی به روتر می شود. اما پارامتر out گزینه منحصر به فردی است. با به کار بردن این پارامتر می توان مشخص کرد که این روتر قادر به برقراری ارتباط telnet به وسیله دستورات telnet یا connect با چه دستگاههایی باشد. در ACL های استاندارد این یک استثناء می باشد و روتر را مجبور می کند که آدرس های مشخص شده در قانون های ACL را به عنوان آدرس مقصد در نظر بگیرد. در این شرایط روتر قبل از اینکه اجازه برقراری telnet از طریق روتر خودمان به سوی دستگاه های دیگر را بدهد، ACL را بررسی کرده و در صورت لزوم اجازه را صادر خواهد کرد.

مثال ساده زیر ایجاد و فعال کردن یک ACL را برای یک ارتباط telnet نشان می دهد:

```
Router(config)#access-list 99 permit 192.168.1.0 0.0.0.255
Router(config)# line vty 0 4
Router(config-line)#access-class 99 in
```

در مثال بالا فقط دستگاه های موجود در شبکه ۲۴/۹۲,۱۶۸,۱,۰ اجازه برقراری ارتباط به روتر ما را دارند. نیازی به نوشتن دستورات deny نداریم. زیرا که وجود implicit deny در آخر هریک از قانون های ACL بطور خود به خودی بقیه ترافیک ها به غیر از آنهایی که اجازه عبور دارند را حذف خواهند نمود.

در قسمت بعدی سری مقالات ACL مشاهده خواهید کرد که به وسیله استفاده از ACL های extended نیز می توان در انتقال ترافیک روترها اعمال محدودیت نمود. اما مراحل این کار کمی پیچیده تر می باشد. ACL های گسترده بر روی Interface های روتر تاثیر می گذارند و نمی توان آنها را برای اعمال محدودیت در دسترسی telnet به دستگاه های دیگر مورد استفاده قرار داد. همچنین وقتی که یک ACL را در روی یک Interface فعال می سازیم، کارایی آن Interface کاهش خواهد یافت که بسته به مدل، نسخه نرم افزار IOS و امکانات دستگاه، این کاهش در کارایی و عملکرد دستگاه متفاوت خواهد بود. بنابراین اگر قصد اعمال محدودیت در دسترسی به طریق telnet را دارید، استفاده از ACL های استاندارد و دستور access-list بهترین گزینه می باشد. به مثالی دیگر از ACL های استاندارد توجه کنید:

```
1. Router(config)# access-list 2 deny 192.168.1.0
2. Router(config)# access-list 2 deny 172.16.0.0
3. Router(config)# access-list 2 permit 192.168.1.0
4. Router(config)# access-list 2 permit 0.0.0.0 255.255.255.255
5. Router(config)# interface ethernet 0
6. Router(config-if)# ip access-group 1 out
```

مثال فوق دارای اشکالاتی می باشد. بنابراین به بررسی موارد آن می پردازیم.

قانون اول اجازه عبور به پیام های رسیده از سوی ۱۹۲,۱۶۸,۱,۰ را نخواهد داد. به دلیل اینکه wildcard mask مشخص نشده است، بنابراین Mask فوق به صورت ۰,۰,۰,۰ بوده و نشان دهنده این است که باید مطابقت دقیق وجود داشته باشد. مشکل موجود در این قانون این است که ما اصولاً این آدرس را نمی توانیم در شبکه به کار بگیریم. زیرا که آدرس ۲۴/ ۱۹۲,۱۶۸,۱,۰ یک شماره شبکه می باشد و نه یک آدرس host.

نکته: اولین و آخرین آدرسی که در هر شبکه قرار می گیرد را نمی توان به host ها یا دستگاه های شبکه اختصاص داد. اولین آدرسی که در هر شبکه وجود دارد را به نام شماره شبکه یا Network Broadcast می نامیم.

قانون دوم نیز دچار همین مشکل است اما قانون های سوم و چهارم صحیح نوشته شده اند.

می بینید که تنظیم یک ACL می تواند کار زیرکانه ای باشد. به هر صورت، شکل صحیح تری از مثال بالا به صورت زیر خواهد بود:

```
1. Router(config)# access-list 2 deny 192.168.1.0 0.0.0.255
2. Router(config)# access-list 2 deny 172.16.0.0 0.0.255.255
3. Router(config)# access-list 2 permit 192.168.1.1
4. Router(config)# access-list 2 permit 0.0.0.0 255.255.255.255
5. Router(config)# interface ethernet 0
6. Router(config-if)# ip access-group 1 out
```

همانطوریکه میبینید قانون اول اجازه عبور به ترافیک رسیده از کل شبکه ۲۴/۱۹۲,۱۶۸,۱,۰ را نخواهد داد.

قانون دوم نیز به همین شکل اجازه عبور به ترافیک مربوط به شبکه ۱۶/۱۷۲,۱۶,۰,۰ را نمی دهد.

قانون سوم این اجازه را به دستگاهی با آدرس ۱۹۲,۱۶۸,۱,۱ داده و قانون چهارم نیز همه ترافیک های رسیده را می پذیرد. اما هنوز مشکلی در دستورات فوق به چشم می خورد. به قانون های اول و سوم توجه کنید. آیا روتر قانون سوم را پردازش خواهد کرد یا نه؟ اگر جواب شما "نه" باشد درست حدس

زده اید.گفته شد که در نوشتن قانون های یک ACL باید موارد اختصاصی تر را در اول قرار دهیم. در مثال بالا وقتی روتر قانون اول را می بیند، تمامی ترافیک مربوط به شبکه ۱۹۲,۱۶۸,۱,۰۲۴ را حذف خواهد نمود. در حالیکه در قانون سوم اجازه عبور به ترافیک دستگاه ۱۹۲,۱۶۸,۱,۱ که جزئی از ۱۹۲,۱۶۸,۱,۰۲۴ می باشد داده شده است. روتر با پردازش قانون اول، ترافیک رسیده از ۱۹۲,۱۶۸,۱,۱ را حذف خواهد نمود و دیگر فرصت برای بررسی قانون سوم نخواهد رسید. برای همین باید قانون سوم را در ابتدا و قبل از قانون اول بیاوریم. یعنی به شکل زیر:

1. Router(config)# access-list 2 permit 192.168.1.1
2. Router(config)# access-list 2 deny 192.168.1.0 0.0.0.255
3. Router(config)# access-list 2 deny 172.16.0.0 0.0.255.255
4. Router(config)# access-list 2 permit any
5. Router(config)# interface ethernet 0
6. Router(config-if)# ip access-group 1 out

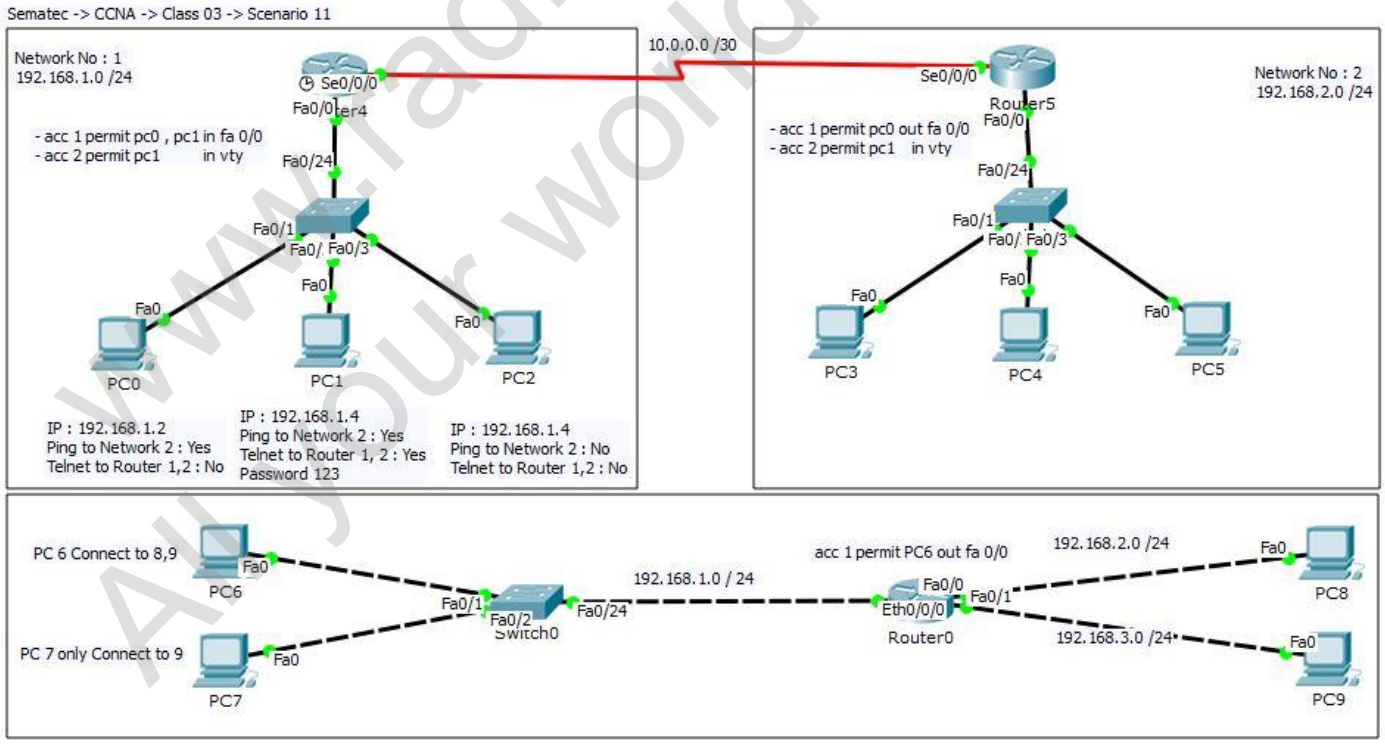
با نگاه دقیق تر به دستورات بالا باز هم مشاهده خواهید کرد که یک مشکل دیگر هنوز باقی مانده و آن هم این است که ما شماره ACL را در موقع فعال کردن در روی Ethernet 0 به اشتباه روی عدد "۲" تنظیم کرده ایم که این عدد باید برابر با "۱" باشد.

بنابراین قسمت آخر دستور نوشته شده را به صورت زیر اصلاح می کنیم:

1. Router(config)# interface ethernet 0
2. Router(config-if)# no ip access-group 1 out
3. Router(config-if)# ip access-group 2 out

البته این نکته را از یاد نبرید که قبل از فعال کردن ACL جدید در ابتدا باید ACL قدیم را حذف کرده و سپس اقدام به آن کار نمایید.

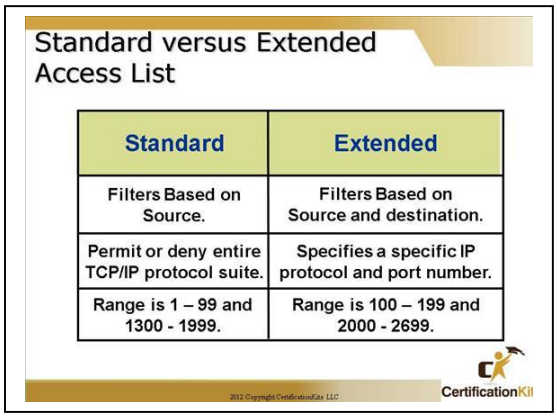
دو نمونه برای کسب مهارت بیشتر بر روی ACL_STD



heydari.farzad@gmail.com نام مدرس دوره: مهندس فرزاد حیدری
تهیه و گردآوری: دانیال نامورکهن

فصل شانزدهم

Access-List های Extended (گسترده)



این ACL ها بسیار قابل انعطاف بوده و دست ما را در فیلتر کردن انواع مختلف ترافیک باز می گذارند. گفتیم که ACL های Extended عمل فیلتراسیون را براساس پارامترهای زیر انجام می دهند:

۱. آدرس IP فرستنده و گیرنده پیام ها
۲. نوع پروتکل IP مورد استفاده مثل IP، ICMP، TCP، UDP و ...
۳. اطلاعات مربوط به پروتکل ها مثل شماره پورت در TCP و UDP و نوع پیام ها یا Message type در پروتکل ICMP

ترکیب دستورات مورد استفاده برای ایجاد این نوع ACL به شکل زیر است:

Router(config)#access-list ACL_NUM {permit} | {deny} Protocol SRC_IP WC_MASK DST_IP WC_MASK DST Por [log]

از این دستور نیز می توان فهمید که دستورات بکار رفته در ایجاد ACL های extended کمی پیچیده تر از قبلی است. شماره ای که برای نام گذاری ACL ها بکار می رود را می توان در رنج ۱۰۰ تا ۱۹۹ و نیز ۱۶۹۹ تا ۲۰۰۰ انتخاب نمود. بعد از مشخص نمودن گزینه های permit / deny نوع پروتکل مورد نظر را نیز باید مشخص نماییم که این نکته اولین تفاوت اساسی بین ACL های استاندارد را با ACL های گسترده نشان می دهد. این پروتکل ها شامل موارد زیر می شوند:

IP, TCP, ICMP, GRE, UDP, IGRP, EIGRP, IGMP, IPINIP, NOS, OSPF

دومین تفاوت بین این دو ACL این است که در ACL های گسترده علاوه بر مشخص نمودن آدرس دستگاه فرستنده، آدرس دستگاه گیرنده را هم باید تعیین نماییم. مشخص کردن Wildcard Mask نیز انتخابی است. بسته به نوع پروتکل موردنظر می توانیم اطلاعات بیشتری را در مورد آن پروتکل ها مشخص کنیم. برای مثال اگر از پروتکل IP استفاده می کنیم، می توان شماره های پورت دستگاه ها را هم تعیین کرد. برای ICMP نیز می توان انواع پیام های ارسالی را مشخص نمود. در آخر نیز با بکار بردن log می توان نتایج را به پورت کنسول و یا یک سرور حاوی اطلاعات log یا sylog منتقل کرده و آنها را به صورت متمرکز در آنجا تحت بررسی قرار داد. بکار بردن log در این دستور نیز انتخابی می باشد.

به کار بردن Extended ACL در TCP/UDP

دستور زیر را برای پیکربندی یک ACL گسترده در پروتکل های TCP و UDP بکار می بریم:

Router(config)# access-list ACL_NUM {Permit}|{Deny} {tcp}|{udp} SRC_IP WC_MASK OPERATOR SRC_PORT_NUM DST_IP WC_MASK OPERATOR DST_PORT_NUM

مشاهده می کنید که ما بعد از مشخص کردن یکی از گزینه های permit یا deny نام پروتکل آورده می شود که در اینجا بحث ما بر سر یکی از پروتکل های TCP یا UDP می باشد. در هنگام به کار بردن این پروتکل ها، آدرس منبع، آدرس مقصد، شماره و یا نام پورت های مورد استفاده را می توان تعیین نمود. همچنین در این پروتکل ها باید یک اپراتور را نیز مشخص کنیم. در جدول زیر لیست اپراتورهای موجود به همراه شرح آنها نیز آمده است. در یاد داشته باشید که این اپراتورها فقط در TCP و UDP کاربرد دارند. همانطوریکه اشاره شد اگر پروتکل مورد استفاده ما TCP یا UDP باشد می توان شماریا

نام پورت ها را هم مشخص نمود. مثلاً اگر منظور ما یک ارتباط telnet باشد، هم می توان عبارت telnet را بکار برد و یا شماره ۲۳ را به عنوان شماره پورت متناظر آن استفاده نمود. جدول زیر نام و شماره برخی از پورت های متداول را لیست کرده است.

Port Name	TCP	UDP	Port Number
FTP Data Transfer	✓	✓	20
FTP Control (command)	✓		21
SSH (Secure Shell)	✓	✓	22
Telnet (unsecure)	✓	✓	23
SMTP (Simple Mail Transfer Protocol)	✓		25
DNS (Domain Name System)	✓	✓	53
DHCP Server (Dynamic Host Control Protocol)		✓	67
DHCP Client		✓	68
HTTP (Hyper Text Transfer Protocol) (www)	✓	✓	80
POP3	✓		110
HTTPS (HTTP+Secure)	✓		443
IPV6 DHCP Client	✓	✓	546
IPV6 DHCP Server	✓	✓	547

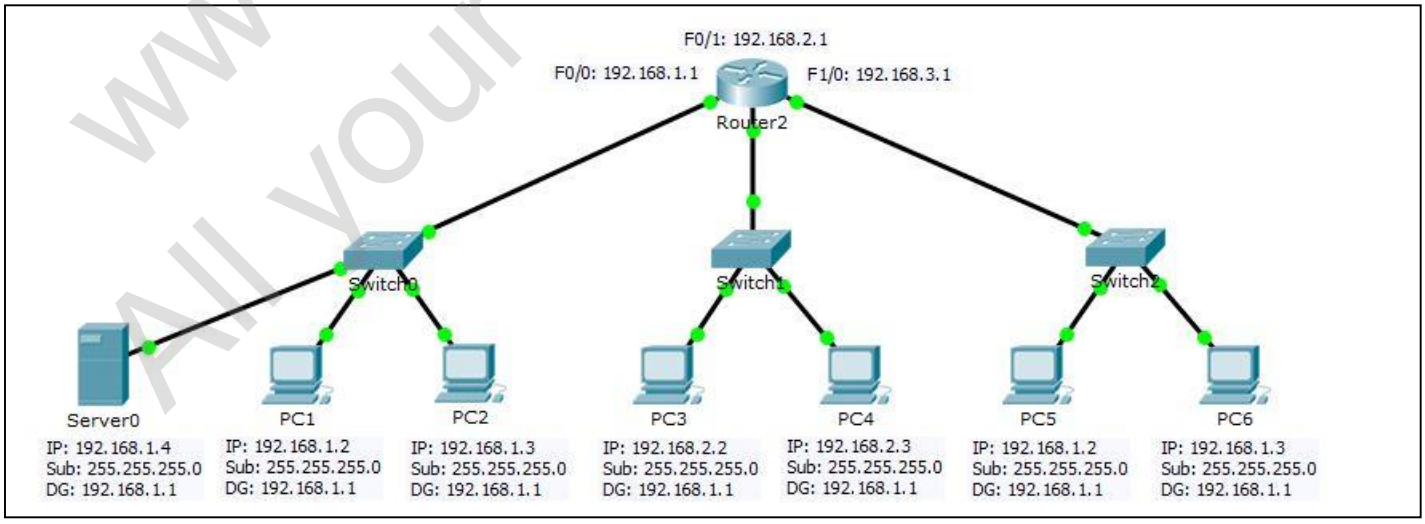
Pop3 معمولا در دسترسی کاربران به سرورهای mail کاربرد دارد. www هم در دسترسی به سرورهای http مورد استفاده قرار می گیرد. اگر نام یک پورت در لیست بالا موجود نبود، می توانید همچنان از شماره آنها استفاده کنید. اگر شماره یا نام پورت موردنظر را مشخص نکنیم، بطور پیش فرض تمامی ارتباطات TCP تحت تاثیر قرار خواهند گرفت.

فعال ساختن یک ACL گسترده

به وسیله دستور زیر می توان بعد از ایجاد یک ACL گسترده آن را در روی یکی از اینترفیس های روتر فعال سازیم:

```
Router(config)# interface TYPE MOD/NUM
Router(config)# ip access-group ACL_# in|out
```

در این سناریو میخواهیم ۶ عدد pc به نام های PC1 تا PC6 و یک سرویس دهنده ی فایل با نام File server وجود خواهد داشت که در سه subnet قرار دارند، با استفاده از Extended Access list ها می خواهیم دسترسی PC5 از subnet3 به File server موجود در subnet1 را مسدود کنیم، ولی دسترسی به سایر کامپیوترهای subnet1 توسط PC5 و سایر PC ها در سایر subnet ها وجود داشته باشد.



مرحله اول : پیکربندی IP Address روی اینترفیس های روتر

پیکربندی IP Address روی اینترفیس های روتر و همچنین تنظیمات IP بر روی PC ها Server

مرحله دوم: پیکربندی Extended Access list بر روی روتر

در این مرحله، یک ACL نوع Extended تعریف و شماره آن را ۱۰۱ انتخاب خواهیم کرد و با استفاده از این ACL مانع از دسترسی کامپیوتر PC5 در Subnet۳ به File Server موجود در Subnet1 خواهیم شد و PC5 این توانایی را خواهد داشت که به سایر کامپیوترهای Subnet1 دسترسی داشته باشد.

```
Router#config t
Router(config)#access-list 101 deny ip host 192.168.3.2 host 192.168.1.4
Router(config)#access-list 101 permit ip any any
```

مرحله سوم: اعمال Access list به Interface

در این مرحله ما می خواهیم ACL شماره ۱۰۱ را که در مرحله ۲ ایجاد نموده ایم، به اینترفیس FastEthernet 1/0 برای Inbound اعمال نماییم. این عمل ما باعث خواهد شد که هر ترافیکی که می خواهد، به اینترفیس FastEthernet 1/0 وارد شود، با قوانین داخل Access list شماره ۱۰۱ بررسی شود که آیا اجازه عبور دارد یا خیر.

```
Router#config t
Router(config)#interface fastethernet 2/0
Router(config)#ip access-group 101 in
```

مرحله چهارم : تصدیق پیکربندی Access List

مرحله بعد، ما از PC5 که عضو Subnet3 می باشد، کامپیوتر سرور را که عضو Subnet1 می باشد، ping می کنیم.

```
PC>ping 192.168.1.4

Pinging 192.168.1.4 with 32 bytes of data:

Reply from 192.168.3.1: Destination host unreachable.
Reply from 192.168.3.1: Destination host unreachable.
Reply from 192.168.3.1: Destination host unreachable.
Reply from 192.168.3.1: Destination host unreachable.
```

همانطور که می بینید، ارتباط بین PC5 که عضو Subnet3 می باشد با سرور که عضو Subnet1 می باشد، توسط ACL مسدود (deny) شده است. مرحله بعد ما از PC5 که عضو Subnet3 می باشد کامپیوتر PC1 را که عضو Subnet1 می باشد، ping می کنیم:

```
PC>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

Reply from 192.168.1.2: bytes=32 time=0ms TTL=127
Reply from 192.168.1.2: bytes=32 time=1ms TTL=127
Reply from 192.168.1.2: bytes=32 time=2ms TTL=127
Reply from 192.168.1.2: bytes=32 time=0ms TTL=127
```

مرحله پنجم : مشاهده همه ACL ها روی روتر و مشاهده تعداد PACKET هایی که با قوانین ACL ها Match بوده اند.

برای مشاهده همه ACL ها روی روتر و مشاهده تعداد PACKET هایی که با قوانین ACL ها Match بوده اند، از دستور show access-list استفاده خواهد شد همانطور که در دستور زیر مشاهده می کنید:

```
Router#show access-lists
Extended IP access list 101
    10 deny ip host 192.168.3.2 host 192.168.1.4 (4 match(es))
    20 permit ip any any (16 match(es))
```

ایجاد ACL با روش اختصاص نام و محیط تنظیمات

در روتر ی توان برای ایجاد ACL از روش دیگری نیز استفاده کرد. البته تمامی مفاهیم و الگوریتم پیاده سازی همانند توضیحات ارائه شده است ولی در اجرا با کمی انعطاف پذیری بیشتر همراه است. در این روش به جای تایپ یک خط دستور طولانی، محیط ACL در اختیار Admin قرار می گیرد و نیز با توجه به دسترسی به Sequence Number ترتیب اجرای ACL نیز قابل ویرایش و مدیریت می باشد.

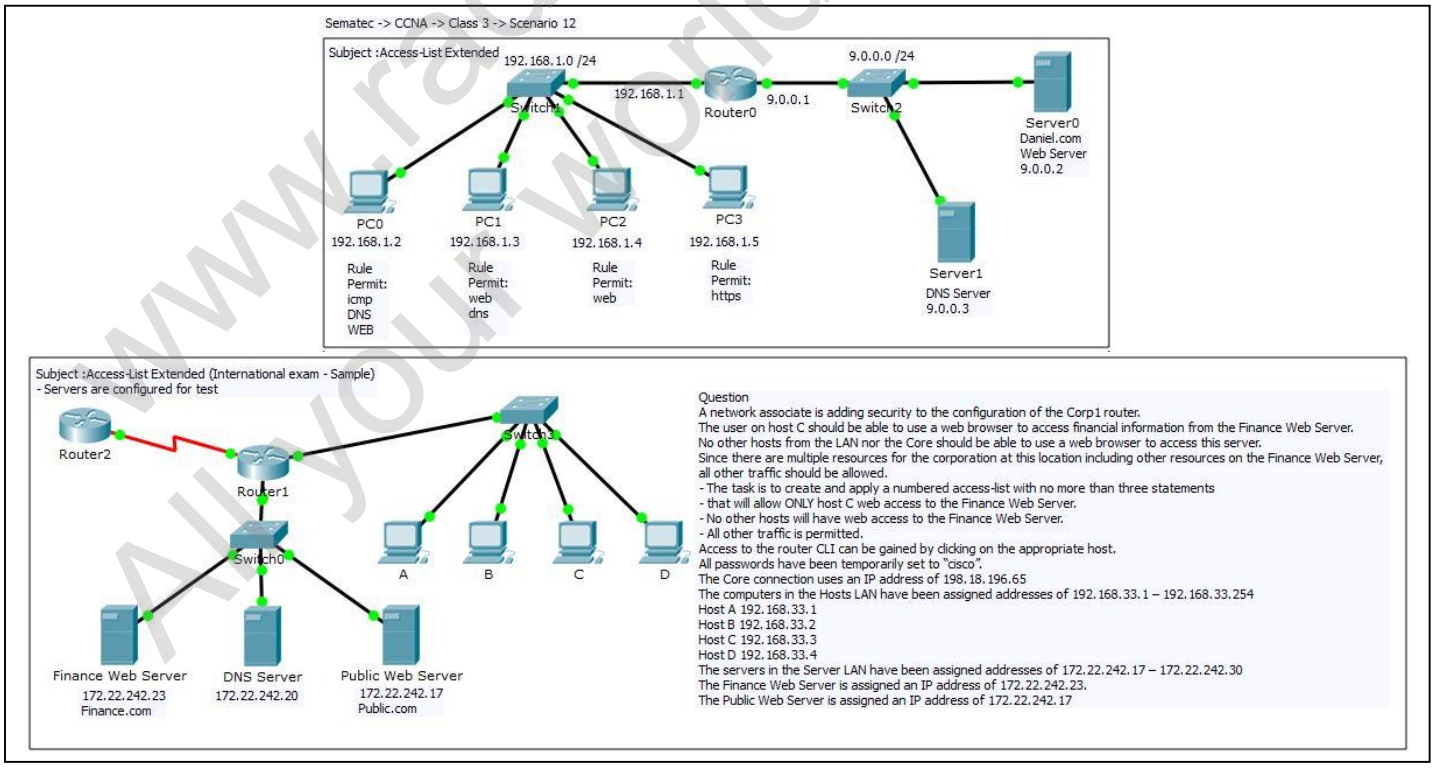
Router(config)# ip access-list {standard | extended} {ACL_NAME | ACL_NUM}
Router(config-std-nacl)# {SEQUENCE_NUM | permit | deny | remark | no }
Router(config-ext-nacl)# {SEQUENCE_NUM | permit | deny | remark | no }
*/ Sample
Router1(config)# ip access-list extended S101
Router1(config-ext-nacl)# deny ip 192.168.3.2 host 192.168.1.4
Router1(config-ext-nacl)# permit tcp any any
*/ apply on interface
Router(config-inf)# ip access-group S101 in

```
Router#show access-lists
Extended IP access list S101
    10 deny ip host 192.168.3.2 host 192.168.1.4
    20 permit ip any any
```

Router1(config-ext-nacl)# 15 deny ip host 192.168.3.3 host 192.168.1.4 */Add one rule between rules

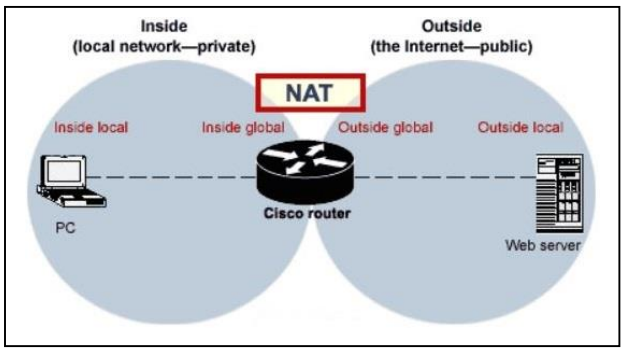
```
Router(config)#show acc
Extended IP access list S101
    10 deny ip host 192.168.3.2 host 192.168.1.4
    15 deny ip host 192.168.3.3 host 192.168.1.4
    20 permit ip any any
```

Router1(config-if) no ip access-group 101 in */ clear ACL with Number Method from interface
Router1(config-if) no ip access-group S101 in */ clear ACL with Name Method from interface
Router1(config) no access-list 101 */ clear ACL Rules with Number fom Router's memory
Router1(config) no ip access-list extended S101 */ clear ACL Rules with Name fom Router's memory



فصل هفدهم

NAT (Network Address Translation)



NAT یکی از ابزارهای قدرتمند دنیای IT است که دقیقا همان کاری را انجام می دهد که از اسم آن بر می آید, به وسیله NAT میتوانیم آدرس های یک شبکه را به یک شبکه دیگر ترجمه کنیم.NAT تقریباً در تمامی سیستم عامل ها و روتر ها قابل انجام است که هر کدام شیوه و روش خود را دارند. برای همه متخصصین واضح است که قوی ترین روتر های دنیا Cisco هستند و تقریبا ۸۰ درصد از بستر اینترنت بر روی دستگاه های Cisco بنا شده اند. در این بخش به توضیح مراحل انجام NAT به صورت عملی بر روی سخت افزارهای سیسکو می پردازیم.

انواع NAT:

- **Static NAT**: ترجمه یک IP به یک IP. یعنی به ازای یک Private IP یک Public IP وجود دارد و برعکس.
- **Dynamic NAT**: ترجمه یک گروه IP به یک گروه IP. یعنی به ازای یک گروه Privae IP یک گروه Public IP وجود دارد و برعکس.
- **Dynamic NAT Overload or PAT**: اختصاص یک IP عمومی برای یک محدوده خصوصی با استفاده از Random Port

از کاربردهای NAT می توان به موارد زیر اشاره کرد:

- ترجمه IP های Private به Public یا بلعکس
- تغییر مرکز سرویس دهنده اینترنت بدون نیاز به تغییر IP ها داخلی
- حفاظت از یک شبکه حساس در مقابل برخی حملات خارجی
- تغییر پورت مقصد پکت ها برای کاربران داخلی به صورت Transparent

تعریف برخی اصطلاحات:

Inside Local: به آدرسی (هایی) اطلاق میشود که بر روی کلاینت های شبکه داخلی تنظیم شده اند.

Inside Global: به آدرسی اطلاق میشود که به Interface داخلی روتر که به شبکه داخلی متصل است داده شده است.

Outside Local: به آدرس هایی که درون اینترنت یا شبکه Public ما قرار دارد گفته می شود.

Outside Global: به آدرسی (هایی) که بر روی Interface خارجی روتر که به شبکه Public متصل است گفته می شود.

استاتیک NAT:

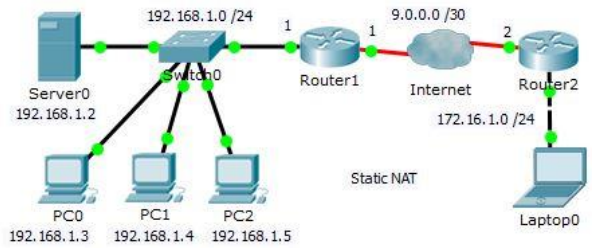
همانطوریکه ذکر شد این نوع NAT به صورت یک به یک عمل میکند. بدین معنی که یک عدد inside-local را به یک outside-global ترجمه می کند. کاربرد این نوع NAT وقتی است که میخواهیم یک private ip را به یک public ip تبدیل کنیم.

در ساختار و شکل دستور پارامترهای Inside و outside مسیری را که باید عمل ترجمه صورت گیرد را نشان می دهد. برای مثال کلمه inside به این معنی است که یک آدرس inside source local به یک آدرس inside global ترجمه می شود. کلمه outside نیز نشان دهنده این است که یک آدرس outside destination global به یک آدرس outside local ترجمه می گردد. بعد از این مرحله نیز باید interface های داخلی یا inside و خارجی یا outside را تعیین نماییم.

```
Router(config)# ip nat inside source static INSIDE_LOCAL_IP   INSIDE_GLOBAL_IP
Router(config)# ip nat outside source static OUTSIDE_LOCAL_IP   OUTSIDE_GLOBAL_IP
*/ set on interfaces
Router(config-if)# ip nat {inside | outside}
```


heydari.farzad@gmail.com نام مدرس دوره: مهندس فرزاد حیدری
تهیه و گردآوری: دانیال نامورکهن

پارامتر inside را در روی interface متصل به LAN و پارامتر outside را در روی interface متصل به اینترنت بکار می بریم. برای آشنایی بیشتر با NAT استاتیک به مثالی که در شکل زیر آورده شده توجه کنید. در این مثال یک آدرس global برابر با ۹,۰,۰,۱ به سرور WEB داخلی با آدرس ۱۹۲,۱۶۸,۱,۱ تخصیص یافته است و مدیر شرکت می خواهد از منزل به منابع اطلاعاتی و اتوماسیون شرکت دسترسی یابد. پیکربندی مربوطه به شکل زیر خواهد بود:




```
Router (config)# interface FastEthernet 0/0
Router (config-if)# ip address 192.168.1.1 255.255.255.0
Router (config-if)# ip nat inside
Router (config-if)# exit
Router (config)# interface serial 0/1/0
Router (config-if)# ip address 9.0.0.1 255.255.255.252
Router (config)# ip nat outside
Router (config)# ip nat inside source static 192.168.1.2  9.0.0.1
```

- نکته: واضح است که Default Route باید روی روترهایی (Edge Router) که در لبه یا مرز داخل و خارج شبکه قرار دارند تنظیم و نوشته شود.

داینامیک NAT:

Dynamic NAT نیز همانند Static NAT است اما با این تفاوت که در NAT به صورت Dynamic میتوانیم یک یا چندین IP با به چندین IP ترجمه کنیم. فرض کنید شما Admin یک ISP هستید و به دلیل کمبود IP نیاز به NAT دارید. بر فرض مثال شما دارای ۱۰ Valid IP و ۱۰۰ Invalid IP که باید به آنها ترجمه کنید. ممکن است تا کنون برای شما پیش آمده باشد که کاربری تماس گرفته و اعلام نارضایتی کند از اینکه مدتهای طولانی برای دانلود یک فایل از سایت Rapidshare.com باید انتظار بکشد. این به دلیل این است که سایت Rapidshare.com تمامی کاربران شما را به چشم یک کاربر می بیند. برای رفع این مشکل میتوانیم ۱۰ آدرس معتبر را به ۱۰۰ آدرس غیر معتبر ترجمه کنیم که تا حدود زیادی مشکل را حل خواهد کرد. در Dynamic NAT معمولاً آدرس های معتبر را به وسیله IP nat pool مشخص و آدرس های غیر معتبر را توسط یک access-list مشخص میکنیم. دلیل استفاده از access-list ایجاد امنیت بیشتر است. برای استفاده از NAT دینامیک باید اقدامات زیر صورت گیرد:

۱. لیست آدرس های داخلی که باید روی آنها عمل ترجمه انجام شود. یک ACL استاندارد از IP های خصوصی شبکه درست می کنیم.

```
Router(config)# access-list ACL_NUM permit IP_ADDRESS WC_MASK          */ Define Private Address Range
```

۲. لیست آدرس های خارجی که آدرس های داخلی باید به آنها ترجمه شوند. ایجاد یک pool و اختصاص نام و نیز تعیین محدوده IP های عمومی.

```
Router(config)# ip nat pool POOL_NAME START_IP  END_IP netmask NET_MASK   */ Define Public Address Range
```

۳. Interface هایی که باید در عمل ترجمه آدرس ها دخالت نمایند.

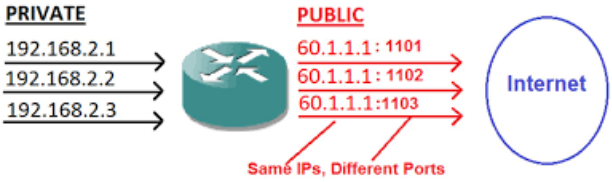
```
Router(config-if)# ip nat { inside | outside }                          */ Determine in & out Interface
```

۴. ایجاد Dynamic NAT با معرفی دو محدوده خصوصی و عمومی جهت تبادل آدرس ها با یکدیگر

```
Router(config)# ip nat inside source list ACL_NUM pool POOL_NAME        */ Introduce two areas together
```


```
*/ Sample ….
Router(config)# access-list 1 permit 10.10.10.0   0.0.0.255
Router(config)# ip nat pool Sematec 20.20.20.25   20.20.20.30 netmask 255.255.255.248
Router(config)# interface FastEthernet0/0
Router(config-if)# ip nat inside
Router(config-if)# exit
Router(config)# interface serial0/1/0
Router(config-if)# ip nat outside
Router(config-if)# exit
Router(config)#ip nat inside source list 1 pool Sematec
```

:Dynamic NAT Overload or PAT (Port Address Translation)



ممکن است ما در شرایطی قرار بگیریم که تنها ۱ عدد آدرس Valid در اختیار داریم و اجبار به NAT کردن آدرس مذکور به چندین آدرس را داریم. در چنین شرایطی باید از قابلیت Overload استفاده کنیم.

در این حالت روتر برای ورود و خروج هر آدرس Invalid یک پورت مجزا در نظر می گیرد که تمامی آنها را در جدولی که درون خود تشکیل می دهد به ثبت می رساند. به این ترتیب هر پکت که از روتر به مقصد اینترنت خارج می شود دقیقاً در هنگام بازگشت به همان آدرس Invalid که صادر کننده آن است باز میگردد. هر یک خط در جدول مذکور یک کانکشن به حساب می آید. اگر دقت کنید بر روی کاتالوگ بعضی سخت افزارها محدودیتی برای تعداد این کانکشن ها قائل می شوند.

مراحل پیکربندی PAT شبیه به NAT دینامیک بوده و همان چهار مرحله را برای انجام کار باید طی نمود. فقط در آخرین مرحله که مشخص کردن و معرفی دو لیست IP هاست که عمل ترجمه روی آنها انجام خواهد شد. دستوری که برای اینکار استفاده می شود شبیه دستوری است که در NAT دینامیک هم مورد استفاده قرار گرفت. اما در آخر دستور کلمه overload را هم باید اضافه نمود که نشان دهنده این است که به جای NAT از PAT استفاده می کنیم.

```
Router(config)# ip nat inside source list ACL_NUM pool POOL_NAME overload        */ Introduce two areas together
```

همانند NAT برای استفاده از PAT باید اقدامات زیر صورت گیرد:

۱. لیست آدرس های داخلی که باید روی آنها عمل ترجمه انجام شود. یک ACL استاندارد از IP های خصوصی شبکه درست می کنیم.

```
Router(config)# access-list ACL_NUM permit IP_ADDRESS WC_MASK                */ Define Private Address Range
```

۲. لیست آدرس خارجی که آدرس های داخلی باید به آنها ترجمه شوند. ایجاد یک pool و اختصاص نام و نیز تعیین IP عمومی.

```
Router(config)# ip nat pool POOL_NAME START_IP  END_IP netmask NET_MASK   */ Define Public Address Range
```

۳. Interface هایی که باید در عمل ترجمه آدرس ها دخالت نمایند.

```
Router(config-if)# ip nat { inside | outside }                              */ Determine in & out Interface
```

۴. ایجاد PAT با معرفی دو محدوده خصوصی و عمومی جهت تبادل آدرس ها با یکدیگر

```
Router(config)# ip nat inside source list ACL_NUM pool POOL_NAME  overload        */ Introduce two areas together
```

***/ Sample** ….

```
Router(config)# access-list 1 permit 192.168.1.0 0.0.0.15                   */ Define Private Address Range
Router(config)# ip nat pool Sematec 9.0.0.1 9.0.0.7 netmask 255.255.255.248 */ Define Public Address Range
Router(config)# interface FastEthernet0/0
Router(config-if)# ip nat inside                                            */ Determine inside Interface
Router(config-if)# exit
Router(config)# interface serial0/1/0
Router(config-if)# ip nat outside                                           */ Determine outside Interface
Router(config-if)# exit
Router(config)#ip nat inside source list 1 pool Sematec overload            */ Apply PAT by Introduce two areas together
```

فصل هجدهم

آشنایی با پروتکل FHRP و زیر مجموعه آن

غالباً یکی از بخش های مهم شبکه که دارای کمترین افزونگی (Redundancy) می باشد, اولین هاپ (Hop) بین میزبان و بقیه شبکه است و دلیل آن این است که این بخش معمولاً با یک آدرس IP Default Gateway پیکربندی شده که این دروازه پیش فرض (Default Gateway) به یک Device مستقل لینک شده است. اگر این Device با مشکل مواجه شود و به اصطلاح Fail شود, تمامی کاربران هایی که در یک سگمنت مشخص از این Default Gateway به عنوان مسیر پیش فرض خود استفاده می کنند, قادر نخواهند بود با هیچ Subnet دیگری از جمله اینترنت ارتباط برقرار کنند و در نتیجه ارتباط آنها با دنیای خارج قطع خواهد شد. چندین راهکار مختلف برای حل این مشکل وجود دارد و تمامی این راه حل ها با یکدیگر هم گروه هستند و اشاره به پروتکل (First Hop Redundancy Protocol) FHRP یعنی پروتکل افزونگی اولین هاپ دارند.

در این مطلب نگاهی اجمالی به پروتکل (Gateway Load Balancing Protocol) GLBP که پروتکل اختصاصیFHRP سیسکو هست خواهیم کرد. پروتکل GLBP نه تنها مثل پروتکل های HSRP و VRRP افزونگی اولین هاپ را فراهم می کند بلکه قابلیت های موازنه بار (Load Balancing) یکپارچه تری را دارد. زیر مجموعه پروتکل FHRP به شرح زیر می باشند:

FHRP	**HSRP**	**H**ost **S**tandby **R**outer **P**rotocol	پروتکل HSRP مخصوص دستگاه های سیسکو می باشد.
	VRRP	**V**irtual **R**outer **R**edundancy **P**rotocol	پروتکل استاندارد می باشد که بسیار شبیه HSRP عمل می کند.
	GLBP	**G**ateway **L**oad **B**alancing **P**rotocol	پروتکل GLBP به دلیل وجود محدودیت در HSRP و VRRP ایجاد شد و مخصوص دستگاه های سیسکو می باشد.

آشنایی و پیاده سازی با HSRP :

اساس کار پروتکل HSRP پیاده سازی High Availability به جهت دسترسی به منابع مهم می باشد. روند کار این پروتکل به این صورت است که ابتدا باید یک گروه ایجاد نمایید. باید توجه داشته باشید که حداکثر تعداد گروه های HSRP روی یک دستگاه ۱۶ گروه می باشد. در بین روترها یا سوییچ های لایه ۳ قرار گرفته در یک گروه می بایست یکی به عنوان Active و یک دستگاه به صورت Standby قرار گیرد که در صورت از مدار خارج شدن دستگاه Active دستگاه Standby جایگزین آن می شود. مابقی دستگاه ها به صورت Listen HSRP State در این گروه قرار می گیرند و زمانی که دستگاه Standby به Active تبدیل می شود، یکی از دستگاه های Listener به Standby تبدیل می شود. روند درک وضعیت دستگاه ها در یک گروه HSRP با ارسال بسته های Hello به یکدیگر می باشند. این بسته ها هر ۳ ثانیه پیکربندی HSRP در لایه اینترفیس روترها و یا در Interface Vlan سوییچ های لایه ۳ انجام می شود. HSRP با ارسال بسته های Hello چک می شود که چه موقع Standby باید جایگزین Active شود که این بسته های Hello به صورت پیش فرض هر ۳ ثانیه یک بار به آدرس Multicast تمام روترها (۲۲۴,۰,۰,۲) بر روی پورت ۱۹۸۵ UDP ارسال می شود. Holde Time در HSRP به صورت پیش فرض ۱۰ ثانیه می باشد که به این معنا است که Standby اگر تا ۱۰ ثانیه بسته Hello در یافت نکند می تواند جایگزین شود.

```
Router(Config-if)# standby GROUP_NUM  timers HELLO_TIME   HOLD_TIME        */ Hello (1-254), Hold (2-255) in Seconds
```

معماری این پروتکل به این صورت است که زمانیکه شما یک Virtual IP برای گروه HSRP ایجاد می کنید، یک Virtual Mac Address برای این IP ایجاد می شود که به صورت c07.acxx۰۰۰۰,۰ می باشد. مقدار c۰۰۰۰,۰ مربوط به تولید کننده سیسکو می باشد، مقدار ac.۰۷ مربوط به پروتکل HSRP و مقدار xx مشخص شده برای شماره گروه HSRP می باشد که از ۰۱ شروع می شود. دستگاهی که به صورت Active در این گروه قرار گرفته است مدام به این MAC Address گوش می دهد و درخواست هایی که توسط کاربران به آن ارسال می شود را پاسخ می دهد.

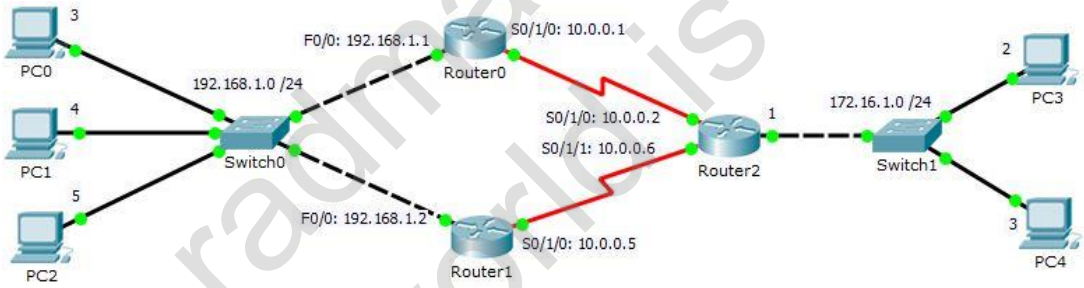
استفاده از HSRP بر روی Router:

به منظور معرفی یک دستگاه به عنوان Active در گروه HSRP می بایست از HSRP Priority استفاده کرد. این Priority مقداری بین ۰ تا ۲۵۵ می باشد و پیش فرض آن ۱۰۰ می باشد. عدد بالاتر معرف اکتیو بودن دستگاه می باشد. در صورتیکه مقدار Priority به صورت پیش فرض تعریف شود ویژگی که باعث اکتیو شدن یک دستگاه می شود بزرگترین آدرس IP بین دستگاه ها می باشد.

دستورات HSRP با کلمه Standby شروع می شوند.

- اختصاص IP به Inerface های مورد استفاده برای مسیرسازی
- معرفی Interface ها درپروتکل EIGRP جهت مسیریابی پویا بین روترها در شبکه و ارتباط بین دو شبکه موجود
- انجام تنظیمات HSRP با استفاده از دستورات زیر و اختصاص یک V_IP_Address از درون شبکه ۱۹۲ مابین روترهای ۰ و ۱
- ذخیره سازی حافظه روترهای ۰ و ۱
- انجام تنظیمات مربوط به کارت شبکه PC های شبکه ۱۷۲ ، ۱۹۲
- تست برقراری ارتباط مابین دو شبکه
- تغییر در تنظیمات مربوط به کارت شبکه PC های شبکه ۱۹۲ و جایگزینی IP Default Gateway با V_IP_Address
- تست برقراری ارتباط مابین دو شبکه (ping –t 172.16.1.2)
- خاموش نمودن روتر ۰

```
Router(Config-if)# standby GROUP_NUM  priority PRIORITY_NUM      */ Group_Num (0-4095) , Priority_Num (0-255)
Router(Config-if)# standby GROUP_NUM  ip Virtual_IP_Address      */ an IP address in same Network Range
```




```
PC>ping -t 192.168.1.3

Pinging 192.168.1.3 with 32 bytes of data:

Reply from 192.168.1.3: bytes=32 time=2ms TTL=126
Reply from 192.168.1.3: bytes=32 time=1ms TTL=126
Reply from 192.168.1.3: bytes=32 time=2ms TTL=126
Request timed out.
Request timed out.
Request timed out.
Reply from 192.168.1.3: bytes=32 time=2ms TTL=126
Reply from 192.168.1.3: bytes=32 time=4ms TTL=126
Reply from 192.168.1.3: bytes=32 time=2ms TTL=126

Ping statistics for 192.168.1.3:
    Packets: Sent = 110, Received = 107, Lost = 3 (3%
loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 16ms, Average = 2ms

Control-C
^C
PC>
```

استفاده از ویژگی Preemption در HSRP: در صورتیکه روتر فعال شما از مدار خارج شود و روتر Standby جایگزین آن شود و پس از مدتی روتر از مدار خارج شده مجدد به مدار بازگردد و Priority بالاتر داشته باشد چه اتفاقی خواهد افتاد؟ ویژگی Preemption به HSRP این قدرت را می دهد تا در صورتیکه روتر اکتیو از مدار خارج شده به مدار بازگردد، مجدد به صورت اکتیو قرار گیرد.

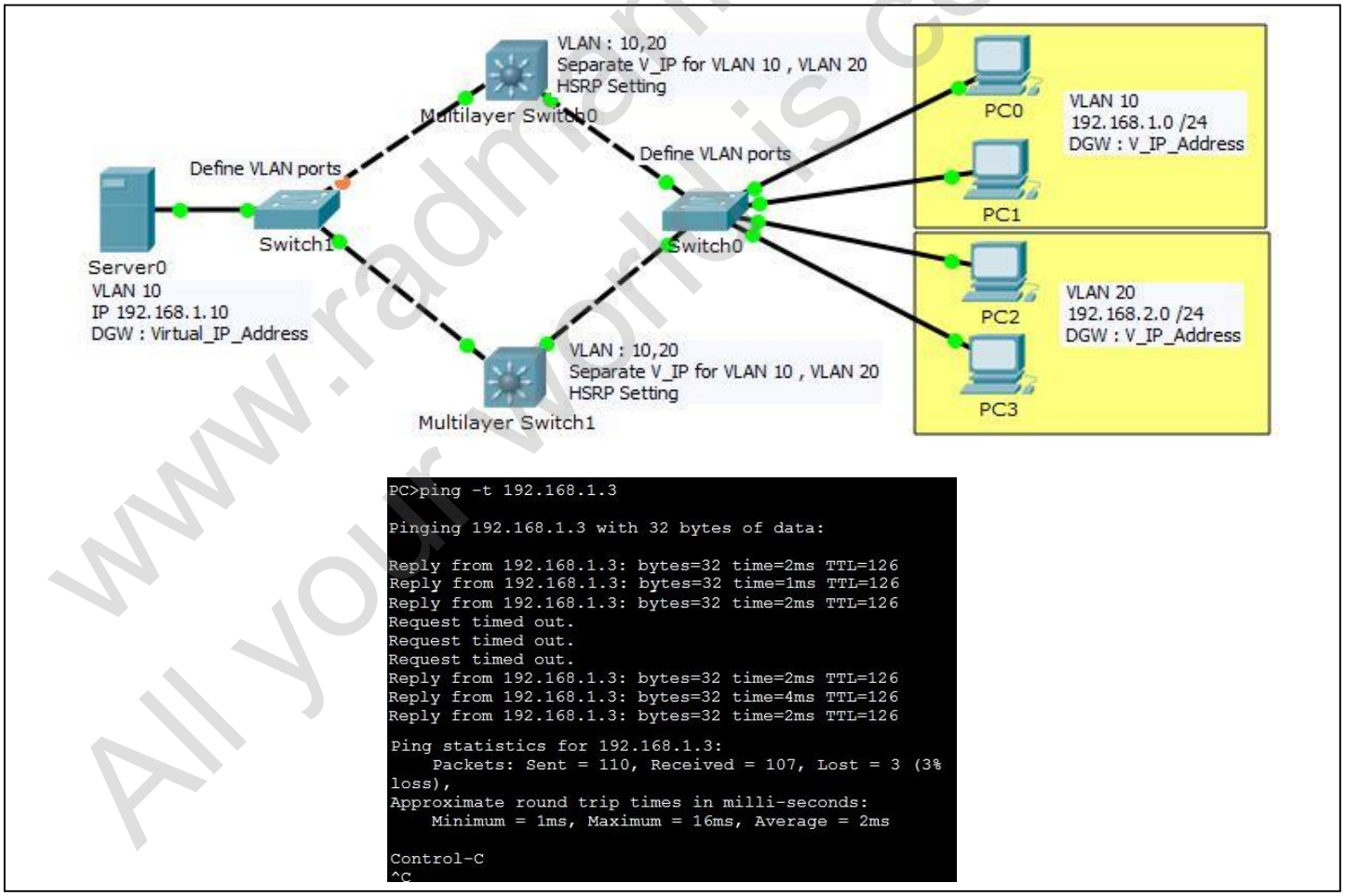
```
Router(Config-if)# standby GROUP_NUM  preempt
```


heydari.farzad@gmail.com نام مدرس دوره: مهندس فرزاد حیدری
تهیه و گردآوری: دانیال نامورکهن

استفاده از پروتکل HSRP بر روی Switch L3:

توجه داشته باشید مکانیزم و الگوریتم پیاده سازی و شکل دستورات پروتکل HSRP بر روی Router و Switch مشابه یکدیگر است با این تفاوت که تنظیمات HSRP بر روی Interface های روتر انجام می گردد ولی در سوییچ این تنظیمات بر روی VLAN ها پیاده سازی و اجرا می شود. چنانچه مفاهیم اختصاص دادن IP و سناریوی ارتباط بین VLAN ها را توسط سوییچ L3 بخاطر داشته باشید ۸۰ درصد کار انجام شده است مابقی دقت در تنظیمات HSRP است که همانطور که ذکر شد مشابه روتر عمل خواهد شد.

۱. ایجاد VLAN ها بر روی سوییچ L3 و طبیعتاً اختصاص IP Unique به هر VLAN معرفی شده در هر سوییچ L3
۲. Trunk نمودن پورت های ارتباطی بین سوییچ ها
۳. اختصاص پورت ها به هر VLAN بر روی سوییچ های L2
۴. تنظیمات کارت شبکه PC ها متناسب با VLAN و پورت های مورد استفاده (IP یکی از سوییچ های L3 به عنوان DGW در نظر گرفته شود)
۵. تست برقراری ارتباط مابین PC ها و VLAN ها
۶. انجام تنظیمات HSRP بر روی هرVLAN بر روی سوییچ های L3
۷. تغییر و جایگزینیIP اختصاص داده شده قبلی درDGW بر روی PC ها با Virtual_IP_Address تعریف شده در HSRP به تفکیک هر VLAN
۸. تست برقراری ارتباط مابین PC ها و VLAN ها با ping –t x.x.x.x
۹. قطع کابل یا Shutdown نمودن پورت مربوط به روتر اصلی




```
PC>ping -t 192.168.1.3

Pinging 192.168.1.3 with 32 bytes of data:

Reply from 192.168.1.3: bytes=32 time=2ms TTL=126
Reply from 192.168.1.3: bytes=32 time=1ms TTL=126
Reply from 192.168.1.3: bytes=32 time=2ms TTL=126
Request timed out.
Request timed out.
Request timed out.
Reply from 192.168.1.3: bytes=32 time=2ms TTL=126
Reply from 192.168.1.3: bytes=32 time=4ms TTL=126
Reply from 192.168.1.3: bytes=32 time=2ms TTL=126

Ping statistics for 192.168.1.3:
    Packets: Sent = 110, Received = 107, Lost = 3 (3%
loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 16ms, Average = 2ms

Control-C
^C
```

Virtual Router Redundancy Protocol یا به اختصار VRRP، یک پروتکل استاندارد است که توسط IEEE ساخته شد. در این پروتکل همانند پروتکل HSRP چندین روتر در یک گروه قرار می گیرد یک روتر Master و سایرین به عنوان Backup قرار میگیرند. فقط روتر Master میتواند ترافیک ارسال کند. در VRRP روتری که بالاترین Priority را دارد به عنوان Master انتخاب می شود و اگر روتر Master پیام Advertisment را ارسال نکند. روتر Backup که بالاترین Priority را دارد جایگزین می شود.

آشنایی با پروتکل GLBP: (Gateway Load Balancing Protocol)

پروتکل GLBP به دلیل وجود محدودیت در HSRP و VRRP ایجاد شد و مخصوص دستگاه های سیسکو می باشد. یکی از دلایل تاثیر گذار در ایجاد این پروتکل شرایط Active بودن تنها یک دستگاه در پروتکل HSRP و VRRP می باشد و مابقی دستگاه ها به صورت Standby قرار می گیرند و به اصطلاح Load Sharing را ایجاد نمی کنند. این پروتکل فقط در سری های ۶۵۰۰ وجود دارد.

همانگونه که ذکر شد هدف توسعه پروتکل GLBP رفع گپ موجود در پروتکل HSRP (Hot Standby Router Protocol) است که پیاده سازی ساده ای از موازنه بار می باشد. با پروتکل HSRP (VRRP که نسخه استاندارد HSRP است) مشکلی که وجود دارد این است که تنها یک Device مستقل در یک گروه, ترافیک را فوروارد و ارسال می کند. وقتی که تنها یک Device ترافیک را Forward کند, پهنای باند غیرفعال زیادی در رابط کاربری Device های آماده به کار باقی می ماند. یک راه برای رفع این مشکل وجود دارد و آن پیکربندی چندین گروه HSRP در Device هاست ولی باز هم این روش نیازمند این است که نیمی از میزبان ها با یک Gateway پیکربندی شوند و نیمی دیگر با Gateway دیگر که این عمل بار کاری مدیریت را بالا می برد و هنوز یک راهکار صحیح و کامل به شمار نمی آید.

پروتکل GLBP کمی با پروتکل های دیگر از این دست متفاوت است. به منظور درک آن دو اصطلاح وجود دارد که باید به توضیح آنها پرداخت .

AVG (Active Virtual Gateway) (دروازه مجازی فعال) و AVF (Active Virtual Forwarder) (فرستنده مجازی فعال)

AVG یا همان دروازه مجازی فعال مسئول مدیریت ترافیک به همه AVF Device است که با پروتکل GLBP پیکربندی شده اند. این کار از طریق کنترل پروسه ARP صورت می پذیرد. یکی از اولین وظایف AVG مسئولیت IP Address های مجازی است و سپس به هر Device با پیکربندی GLBP یک Mac-Address مجازی اختصاص می دهد. وقتی که پیام ARP توسط AVG مشاهده می شود این دروازه پاسخ می دهد و این Mac-Address های مجازی را در به شکل چرخشی (Round-Robin) توزیع می کند.

با این شیوه هر AVF با مقدار محدودی از ترافیک ارسالی از طرف Device های درخواست کننده مواجه می شود.

- *هنگامی که تصمیم می گیرید که از چه نوعی از پروتکل FHRP استفاده کنید , اولین گام این است که می خواهید از چه تولید کننده تجهیزاتی برای Device های خود استفاده کنید. با در نظر گرفتن اینکه HSRP و GLBP هر دو پروتکل های اختصاصی سیسکو هستند و VRRP استاندارد به کار رفته در سایر برندها.*

فصل نوزدهم

IPV6 در سوییچ و روتر:

روش های الصاق آدرس IPv6 به یک Host به روش های زیر است.

Ver	Type	Method	Prefix & Length learned from	Host Learned from	Default Router Learned from	DNS Addresses Learned from
IPV6	Static	Static Conf	Local Config	Lcal Config	Router Using NDP	Stateless DHCP
		Static Conf with EUI-64	Local Config	Derived from MAC	Router Using NDP	Stateless DHCP
	Dynamic	Stateless Auto Conf	Router Using NDP	Derived from MAC	Router Using NDP	Stateless DHCP
		Stateful DHCP	DHCP Server	DHCP Server	Router Using NDP	Stateful DHCP Server

- **نکته:** Stateful به مفهوم بخاطر سپردن یک چیزی می باشد که در اینجا به معنای این است که DHCP می داند که چه آدرسی را به چه سیستمی داده است.
- **نکته:** در IPv6 در تمام روش ها Default Gateway توسط خود روتر و با استفاده از پروتکل NDP یا Network Discovery Protocol به سیستم ها داده می شود.
- **نکته**: در روش دوم کافیست یک روتر در شبکه موجود باشد و روی یک اینترفیس آن IPv6 تنظیم شده باشد. سیستم ها با استفاده از ویژگی Auto Configuration می توانند آدرس IP خود را از آن آدرس بسازند.
- **نکته**: آدرس های Multicast در IPv6 تماما با FF شروع می شوند.

روش دریافت IP توسط سیستم از روتر:

۱. یادگیری Prefix و Length توسط سیستم از روتر از طریق NDP
۲. یادگیری آدرس Gateway خود که همان آدرس روتر می باشد

زمانی که یک سیستم روی Auto Configuration قرار دارد پیغام های RS یا Router Solicitation به آدرس FF02::2 ارسال می نماید که این آدرس مربوط به تمام روترهای موجود در آن لینک می باشد و خواهان معرفی روتر می شود. روتر پیام RA یا Router Advertisement را به آدرس FF02::1 ارسال می کند که این آدرس مربوط به تمام نودهای IPv6 در آن لینک می باشد. در RA موارد زیر موجود است:

۱. آدرس IP خود روتر به عنوان Gateway
۲. اعلام Prefix و Length
۳. اعلام آدرس DNS به صورت Stateless توسط خود روتر

حال بر اساس این اطلاعات سیستم اقدام به ایجاد آدرس IP خود می کند. برای این کار از مکانیزم EUI-64 استفاده می شود و دلیل استفاده از این مکانیزم اطمینان پیدا کردن از Unique بودن آدرس IP می باشد. فرض بر این است که MAC Address یک مقدار Unique می باشد و از این مقدار استفاده می کند، اما طول آدرس MAC تنها ۴۸ بیت می باشد و مقدار مورد نیاز برای ایجاد IP در سیستم ۶۴ بیت می باشد، بنابراین مکانیزم به این صورت عمل می کند:

۱. نصف کردن آدرس MAC از وسط آن
۲. قرار دادن مقدار FFFE در بین این دو نیمه که معادل ۱۶ بیت می باشد
۳. تغییر مقدار بیت ۷ از آدرس MAC از ۰ به ۱ و یا بلعکس

heydari.farzad@gmail.com نام مدرس دوره: مهندس فرزاد حیدری
تهیه و گردآوری: دانیال نامورکهن

نحوه پیکربندی IPv6 در روتر:

IPV6 در روتر و سوییچ به صورت پیش فرض غیرفعال است و می بایست با دستور زیر فعال شود:

```
Router(Config)# ipv6 unicast-routing                    */ Active IPV6 rounting & send RA packets by router's interfcaes
Router(Config-if)# ipv6 address IPV6_ADDRESS / PREFIX LENGTH    */ Set Ip on Interface
Router# show ipv6 interfaces                            */ View interfaces
```

دستور اول به منظور فعالسازی روتینگ IPv6 و ارسال بسته های RA توسط Interface های روتر می باشد و دستور دوم به منظور الصاق آدرس IP به یک]Interface در روتر می باشد.

آدرس های Multicast در IPv6 :

Purpose	IPV6 Address	IPV4 Equivalent
All IPv6 Nodes on the link	FF02::1	Subnet Broadcast Address
All IPv6 Routers on the link	FF02::2	N/A
OSPF Message	FF02::5 , FF02::6	224.0.0.5 , 224.0.0.6
RIP-2 Message	FF02::9	224.0.0.9
EIGRP Message	FF02::A	224.0.0.10
DHCP Relay Agent	FF02:1:2	N/A
DHCP Servers (Site Scope)	FF05::1:3	N/A
All NTP Servers	FF05::101	N/A

تغییرات مورد نیاز جهت راه اندازی پروتکل های مسیریابی روتر تحت IPV6	
RIP	Router(config)# ipv6 router rip NAME Router(config-if)# ipv6 rip NAME enable
Static route	Router(config)# ipv6 route 2000::3:1/64 INTERFACE
Default Route	Router(config)# ipv6 route ::/0 INTERFACE

OSPF	Router(config)# ipv6 router ospf NUM
	Router(config-rtr)# router-id x.x.x.x */ IPV4 Address (32 Bit)
	Router(config-if)# ipv6 ospf OSPF_NUM area AREA_NUM

EIGRP	Router(config)# ipv6 router eigrp NUM
	Router(config-rtr)# eigrp router-id x.x.x.x */ IPV4 Address (32 Bit)
	Router(config-rtr)# no shutdown */ ?!?!?!?!?
	Router(config-if)# ipv6 eigrp NUM

آشنایی با مفهوم Mapping در Layer2 to Layer3 :

در IPv4 با استفاده از ARP که مبتنی بر Broadcast بود می توانستیم از لایه ۲ به لایه ۳ برویم، اما این مفهوم در IPv6 دیگر وجود ندارد. جایگزین این مفهوم چیزی به نام NDP می باشد که با ارسال Neighbor Solicitation که شامل Source IPv6 Address و یک آدرس Multicast می باشد سوال خود را مبنی بر اینکه اطلاعات Datalink Address خود را اعلام کن ارسال می کند و در پاسخ Neighbor Advertisement دریافت می کند که شامل Source IPv6 Address جدید و آدرس مقصد که همان آدرس مبدا ابتدایی به همراه معرفی MAC Address می باشد.

آشنایی با Duplicate Address Detection یا DAD :

به منظور جلوگیری از ایجاد آدرس های تکراری مکانیزمی به نام DAD وجود دارد که قبل از اعمال یک آدرس IP به یک هاست ابتدا اقدام به چک کردن آن کرده و در صورتیکه در شبکه موجود نباشد اجازه اعمال آن را صادر می کند.

- **نکته**: بر روی یک اینترفیس روتر می توان بیش از ۱ آدرس IPv6 تنظیم کرد.

نکته: دستور ipv6 enable باعث ایجاد آدرس Link Local روی روتر می شود.

موفق و پیروز باشید – پایان