
Cisco Systems
CCNA
ترجمه و تالیف : مهدیه توللی
راهنمای اساتید ، کارشناسان و دانشجویان کامپیوتر و مخابرات
ترجمه و تالیف : مهدیه توللی
CCNA
SYSTEMYAR
http://www.systemyar.net
e-mail:info@systemyar.net

فصل اول :

OSI and TCP/IP Model

این فصل مروری بر دلایل طراحی مدل چند لایه ای و مزایای آن و معرفی استانداردهای جهانی خواهد داشت .

درس اول :

OSI Layer
and
TCP/IP Layer

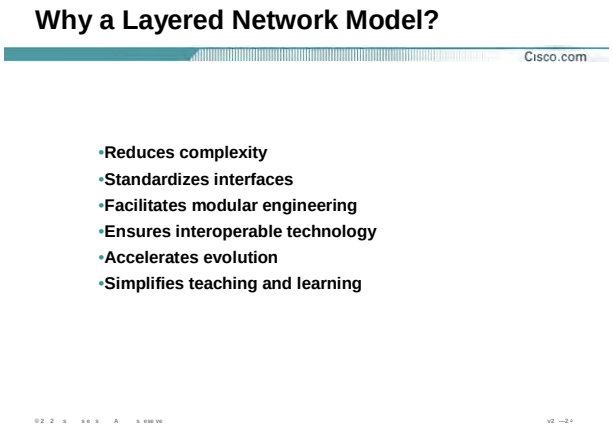
هدف :

۱. بررسی دلایل و ضرورت نیاز به یک مدل چند لایه ای .

۲. شناخت مدل هفت لایه ای OSI .

۳. شناخت مدل چهار لایه ای TCP/IP .

۴. بررسی وظایف تک تک لایه ها و نحوه عملکرد هر کدام از آنها در کنار یکدیگر.

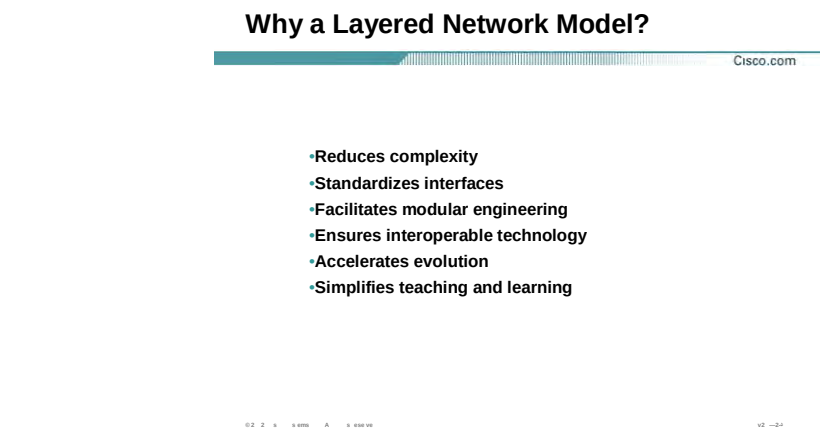


دلایل مدل چند لایه ای :

مقایسه مدل چند لایه ای در مقابل ساختار تک لایه ای ، متناظر با فعالیت یک گروه روی یک فعالیت در مقابل فعالیت تک تک اعضاء گروه به صورت مجزا روی آن فعالیت می باشد .

فعالیت گروهی روی یک موضوع زمانی امکان پذیر می باشد که تقسیم وظایف صورت پذیرفته باشد . بنابراین

- هر شخص در این گروه دارای شرح وظایف مشخصی می باشد .
- عدم حضور و یا عدم فعالیت صحیح یک فرد در این گروه براحتی قابل تشخیص می باشد .
- عدم فعالیت صحیح یک فرد روی عملکرد بقیه افراد گروه تأثیر منفی گذاشته و درنتیجه فعالیت گروهی به نتیجه نخواهد رسید .
- تقسیم وظایف به گونه ای صورت گرفته می گیرد که هر فرد علارقم وابستگی به گروه به تنهایی می تواند وظایف مشخص شده خود را انجام دهد .

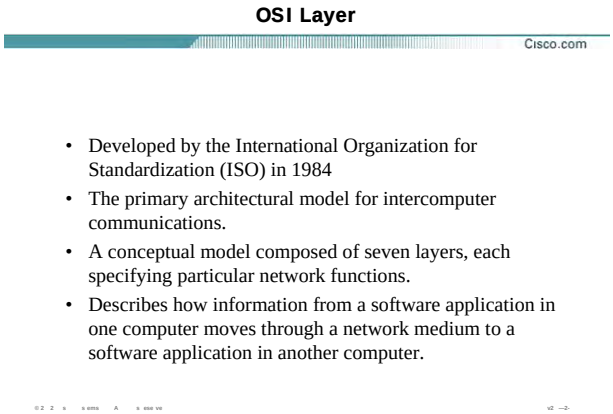


دلایل مدل چند لایه ای(ادامه) :

بنابراین در این معماری چند لایه ای هر لایه مستقل از لایه های دیگر عمل می کند و با وجود مستقل بودن ، می بایست وابستگی بین لایه ها حفظ شود به گونه ای که حذف یک لایه منجر به نتیجه نرسیدن فعالیت های کل لایه ها شود .

با مشخص شدن وظایف هر کدام از لایه ها ، ارتقاء و بهبود عملکرد هر کدام از آنها براحتی امکان پذیر خواهد شد.

این نیاز منجر به طراحی یک مدل هفت لایه تحت عنوان OSI توسط موسسه جهانی استاندارد (ISO) در سال ۱۹۸۴ میلادی شد .

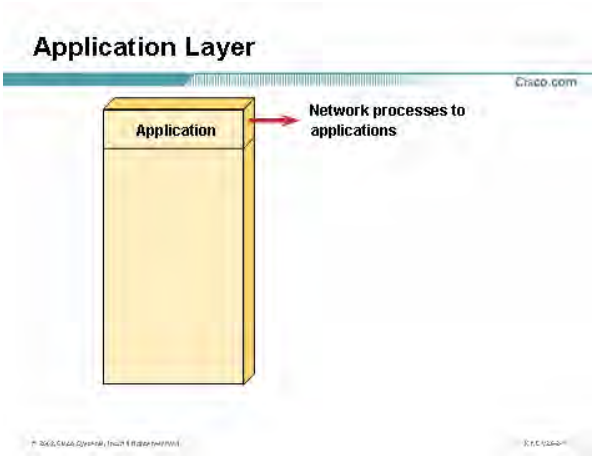


دلایل مدل چند لایه ای :

مدلی که موسسه ISO به عنوان یک استاندارد جهانی در ارتباطات شبکه ای معرفی کرد یک مدل هفت لایه ای است . هر کدام از لایه ها دارای توابع و شرح وظایف خاص خود می باشند و هر کدام از آنها در تعامل با یکدیگر ، می توانند اثر بخش باشند . این هفت لایه عبارتنداز :

- Application
- Presentation
- Session
- Transport
- Network
- Data Link
- Physical

در ادامه با لایه های فوق و شرح عملکرد هر یک ، بیشتر آشنا خواهید شد .



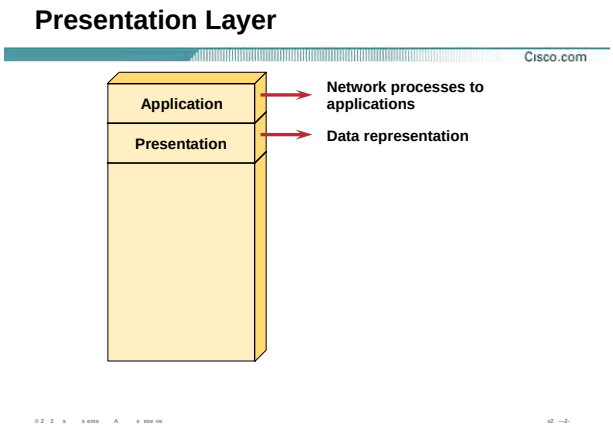
Application Layer:

لایه Application ، لایه هفتم از مدل هفت لایه ای OSI می باشد .

این لایه مجموعه ای از استانداردها و توابع مختلفی می باشد ، به طوریکه وظیفه برقراری ارتباط با کاربر از یک سوی و از سوی دیگر ارتباط با لایه های زیرین را به عهده دارد .

وقتی شما یک مرورگر صفحه web را می گشایید ، این مرورگر به عنوان یک نرم افزار لایه هفتم وظیفه برقراری ارتباط با کاربر را به عهده دارد.

بنابراین سرویس هایی چون سرویس وب و سرویس Email دارای هویت لایه هفتمی هستند که وظیفه برقراری ارتباط با لایه های زیرین و در نتیجه برقراری ارتباط کار با شبکه را به عهده دارند .

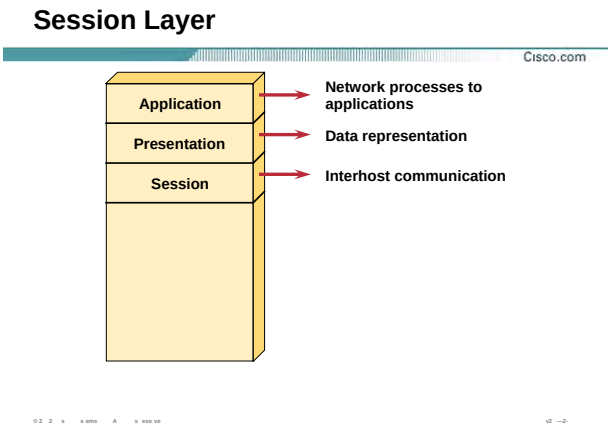


:Presentation Layer

این لایه وظیفه فشرده سازی و رمزنگاری داده ها را به عهده دارد . فشرده سازی اطلاعات به منظور کاهش حجم اطلاعات ارسالی بر روی خطوط انتقال می باشد .

بنابراین در این لایه قبل از اینکه اطلاعات تحویل لایه پایین تر شود می بایست بر اساس استانداردهای موجود فشرده شده و به لایه زیرین تحویل داده شود و در سوی دیگر اطلاعات دریافتی از لایه زیرین در این لایه پس از مشخص شدن قالب فشرده سازی ، از حالت فشرده و کد شده خارج شده و به لایه بالاتر تحویل داده می شود .

سرویس های MP3 و JPEG و GIF را می توان به عنوان نمونه ای از سرویسهای لایه ششم نام برد .

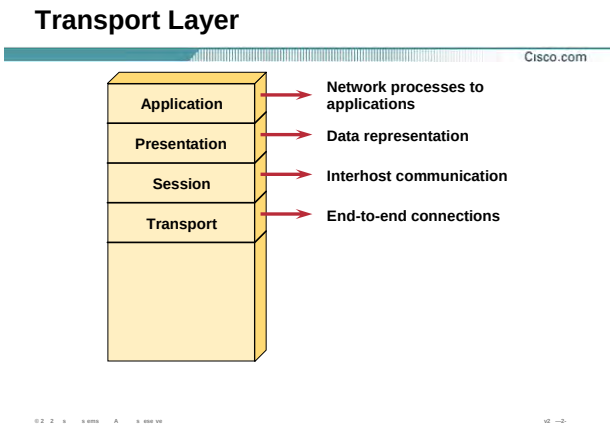


: Session Layer

این لایه وظیفه برقراری شرایط یک Session بین دو Station نهایی را به عهده دارد.

وظیفه تأیید هویت (Authentication) و برقراری یک Session و مدیریت یک Session و درنهایت اتمام session و بررسی حساب (Accounting) را به عهده دارد .

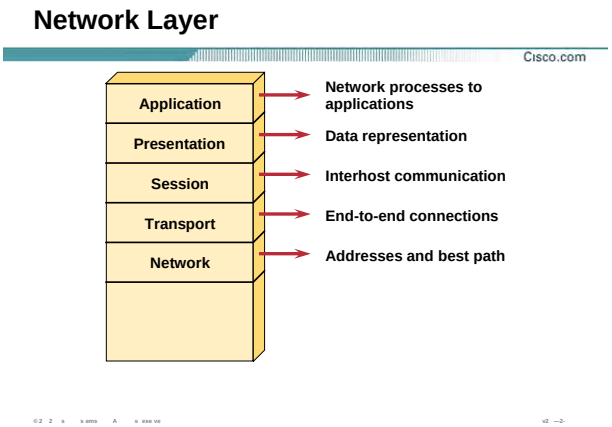
پس از برقراری یک Session ، اطلاعات تحویل لایه چهارم داده می شود . اطلاعاتی که از این سه لایه گذشته و تحویل لایه چهارم داده می شود ، User Data گفته می شود و پس از تحویل به لایه چهارم به قطعات استاندارد شکسته شده و در واقع بسته بندی می شوند .



: Transport Layer

لایه چهارم وظیفه برقراری یک ارتباط end-to-end را به عهده دارد . درواقع این لایه ، وظیفه کنترل ارتباط برقرار شده را به عهده دو Station نهایی می گذارد و آمادگی Station نهایی را برای دریافت ترافیک بررسی می کند و پس از برقراری ارتباط توسط لایه چهارم، ترافیک هدایت خواهد شد .

Data User بعد از تحویل به لایه چهارم در بسته های استانداردی به نام سگمنت بسته بندی (Encapsulate) می شود . ساختار سگمنت و وظایف لایه چهارم به تفسیر در پایان این ماژول شرح داده می شود .

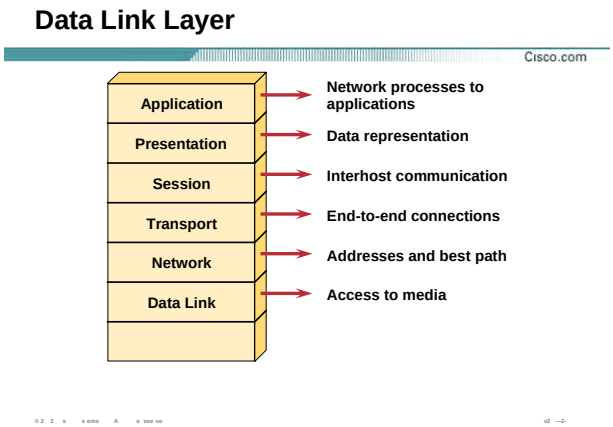


: Network Layer

این لایه وظیفه مسیریابی و هدایت ترافیک را به عهده دارد . درواقع وظیفه انتخاب بهترین مسیر درمیان مسیرهای متفاوت به عهده این لایه می باشد. روتر به عنوان یک Device لایه سوم وظیفه مسیریابی و هدایت ترافیک را به عهده دارد .

هدایت ترافیک در این لایه براساس پروتکل ها و الگوریتم های مسیریابی متفاوتی صورت می گیرد. در این لایه آدرس دهی بسته ها براساس پروتکل IP ، IPX و یا Apple talk صورت می گیرد. دراین لایه هیچگونه پیگیری جهت رسیدن و یا نرسیدن بسته ها صورت نمی گیرد . درواقع وظیفه پیگیری رسیدن بسته ها به مقصد به عهده این لایه نخواهد بود بلکه وظیفه لایه بالاتر (Transport) می باشد .

در فصل آشنایی با روشهای مسیریابی با پروتکل های این لایه و عملکرد هر کدام از آنها به تفسیر آشنا خواهید شد.

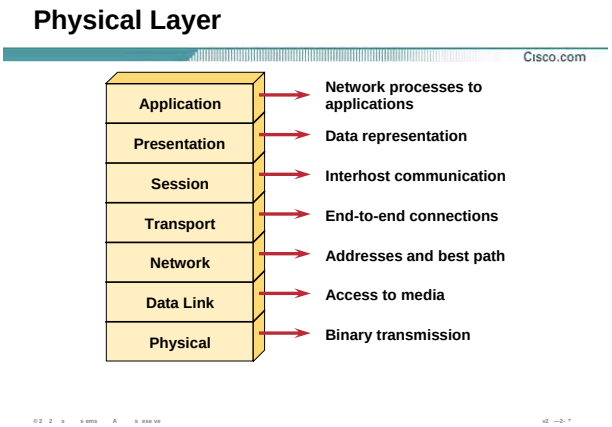


: Data Link Layer

این لایه وظیفه مدیریت منابع سخت افزاری موجود در شبکه های LAN را به عهده دارد. در یک شبکه LAN از آنجایی که منابع سخت افزاری در یک بستر ارتباطی مشترک به تبادل اطلاعات می پردازند ، نیاز به تعریف یکسری استانداردها برای جلوگیری از تصادم و از بین رفتن داده وجود دارد . تعریف این استاندارد ها در لایه دوم از مدل هفت لایه ای OSI صورت می گیرد .

اطلاعات دریافتی از لایه بالاتر در بسته هایی به نام فریم بسته بندی می شود و آدرس دهی هر فریم براساس آدرس سخت افزاری (MAC Address) خواهد بود .

یکی از سخت افزارهایی که وظیفه مدیریت منابع سخت افزاری و ارتباط هر یک از آنها را براساس لایه دوم به عهده دارد سوئیچ می باشد . در ادامه این کتاب با سوئیچ و نحوه عملکرد آن در شبکه به خوبی آشنا می شوید .

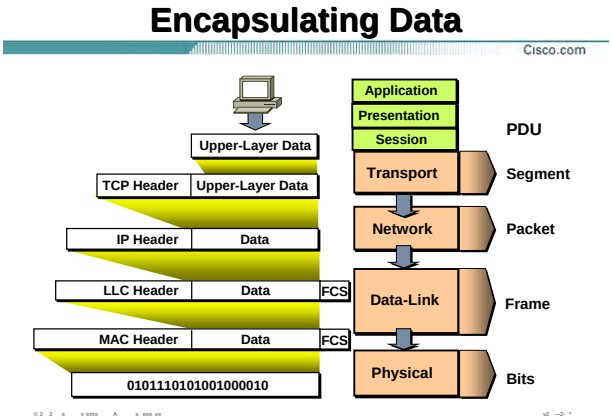


: Physical Layer

در این لایه اطلاعات دریافتی از لایه های بالاتر تبدیل به یک سری بیتهای ۰ و ۱ شده و جهت انتقال برروی بستر ارتباطی ، تبدیل به سیگنال الکتریکی و یا موج نوری خواهند شد .

در این لایه هیچ پردازشی بر اطلاعات ارسالی و یا دریافتی صورت نمی گیرد . نکاتی که در این لایه مورد اهمیت می باشد نوع بستر ارتباطی و پهنای باند مربوط به آن و نرخ ارسال اطلاعات و نوع مدولاسیون مورد اهمیت می باشد .

کارت شبکه به عنوان یک واسط ارتباطی در این لایه ، اطلاعات دریافتی از لایه بالاتر را دریافت و پس از تبدیل به بیتهای صفر و یک ، تحویل بستر ارتباطی می دهد .



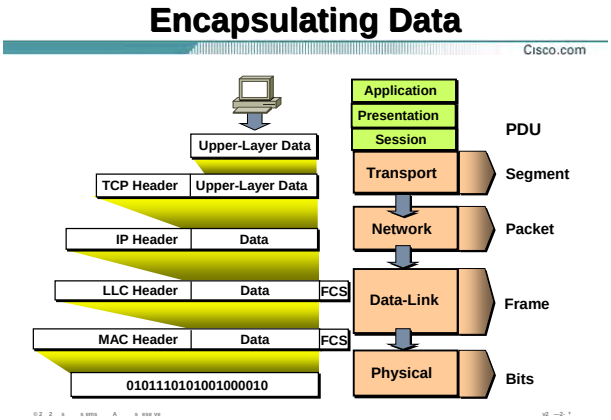
بسته بندی کردن داده ها در هر لایه :

تا به اینجا با لایه ها و عملکرد هر کدام از آنها به اختصار آشنا شدید .

به صورت کلی اطلاعاتی که سه لایه بالاتر را طی می کند با عنوان Data User به لایه چهارم تحویل داده می شود . درلایه چهارم اطلاعات دریافتی درون بسته های استانداردی به نام سگمنت بسته بندی می شود . در این لایه هر کدام از بسته ها یک سری اطلاعات تکمیلی و کنترلی در غالب TCP Header و یا UDP Header خواهند داشت .

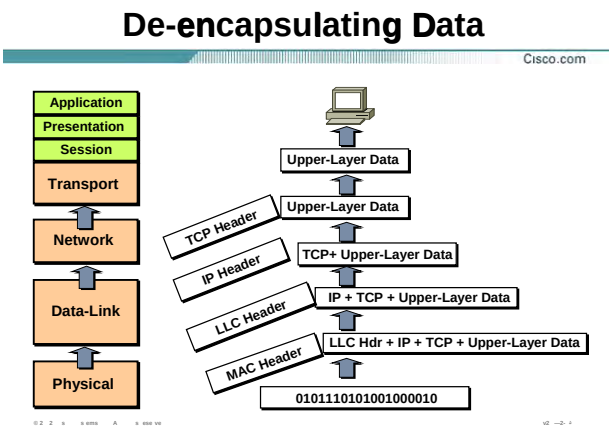
بعد از اینکه بسته های سگمنت تحویل لایه سوم یعنی Network Layer داده شدند بسته بندی جدیدی در مورد آنها صورت می گیرد . فرض کنید آدرس دهی در این لایه براساس پروتکل IP باشد . بنابراین بعد از اضافه شدن IP Header به بسته های دریافتی تحویل لایه پایین تر یعنی لایه Data Link داده می شود . به هر کدام از بسته ها در لایه Network ، Packet گفته می شود .

درلایه دوم یا Data Link Layer با اضافه شدن LLC Header و Mac Header به آن بسته بندی جدیدی به نام Frame خواهیم داشت و در نهایت فریم ها تبدیل به یک سری بیتهای ۰ و ۱ شده و جهت انتقال روی بستر ارتباطی به سیگنالهای الکتریکی و یا موج نوری تبدیل می شوند .



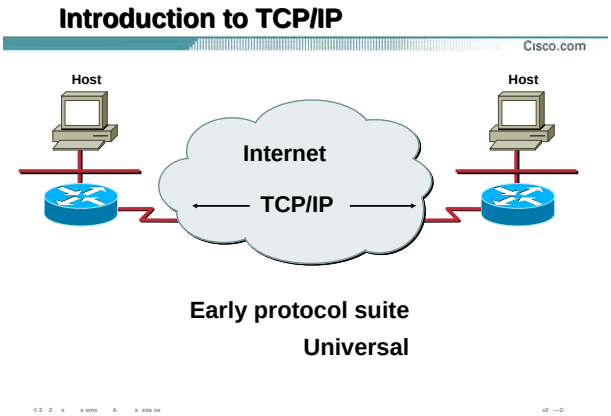
بسته بندی ردن داده ها د هر لایه (ادامه) :

شکل فوق نوع Encapsulation را در هر لایه نشان می دهد . بنابراین روی اطلاعات به ترتیب از لایه هفتم به سمت لایه اول بسته بندی های مختلفی صورت گرفته و در نهایت جهت انتقال در اختیار لایه اول یا Physical Layer قرار می گیرد .



بسته بندی کردن داده ها در هر لایه :

تا به اینجا هفت لایه OSI و پروسه مربوط به آن را از لایه هفتم تا لایه اول بررسی کردیم . از سوی دیگر زمانیکه بیتهای ۰ و ۱ توسط لایه یک (Physical Layer) دریافت شدند در اختیار لایه دوم قرار می گیرند تا با مشخص شدن MAC Header و LLC Header و رفع نیازهای لایه دوم در اختیار لایه سوم قرار گیرد . در لایه سوم هر کدام از پکتها بررسی شده و پس از مشخص شدن آدرس مبدأ و مقصد ، تحویل لایه بالاتر ، Transport Layer داده می شود . در این لایه با توجه به TCP Header و یا UDP Header ، شماره پورت مورد نظر و نحوه دریافت اطلاعات مشخص شده و در نهایت با مشخص شدن فرمت و باز شدن داده های فشرده و کد شده دراختیار لایه هفتم و نرم افزارهایی چون مرورگر Web قرار می گیرد.

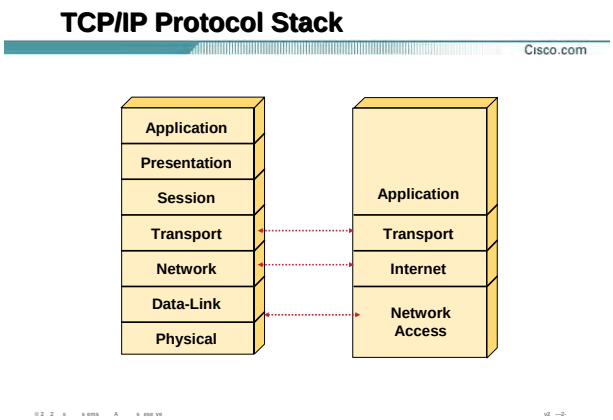


مدل چهار لایه ای TCP / IP :

TCP/IP محصول پروژه تحقیقاتی شبکه ARPANET مربوط به آژانس پروژه های تحقیقاتی دفاعی (DARPA) وابسته به وزارت دفاع امریکا می باشد .

این معماری که امروزه اساس شبکه جهانی اینترنت به حساب می آید یک معماری چهار لایه ای به شرح زیر می باشد :

- Application
- Transport
- Internet
- (Network Access) Network Interface



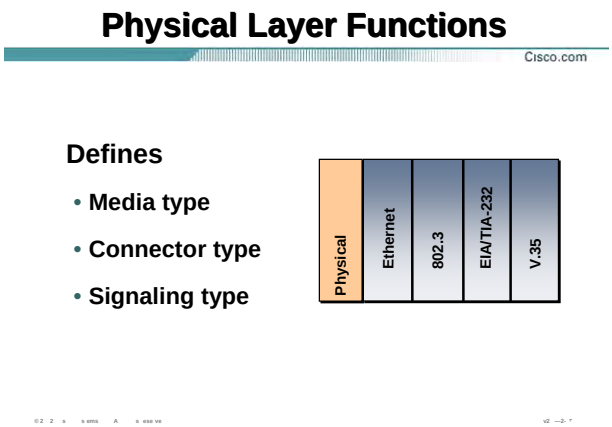
مدل چهار لایه ای TCP/IP :

شکل فوق تناظر بین هفت لایه OIS با چهار لایه TCP/IP را نمایش می دهد .

همانطور که مشاهده می کنید سه لایه بالایی از مدل OSI با لایه Application در مدل TCP/IP و دو لایه پایینی با لایه Network Access در مدل TCP/IP متناظر می باشد .

وظیفه هر کدام از این لایه ها متناظر با عملکرد مدل هفت لایه ای OSI می باشد .

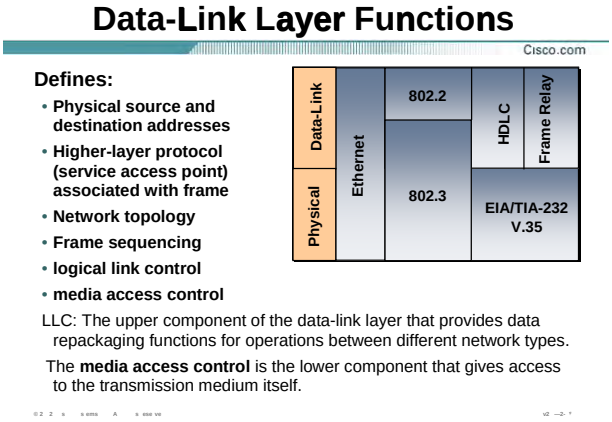
تا به اینجا با هر کدام از لایه ها به اختصار آشنا شدید ، در ادامه چهار لایه از مدل هفت لایه ای OSI به عبارتی لایه های Physical Layer ، Data Link Layer ، Network Layer و Transport Layer را مورد بررسی بیشتری قرار می دهیم .



:Physical Layer

این لایه شامل معرفی انواع بسترهای ارتباطی (کابل ، امواج رادیویی ، ...) و اتصالات مربوط به هر کدام و معرفی انواع سیگنالهایی که وظیفه انتقال بیتهای صفر و یک را به عهده دارند (سیگنالهای الکتریکی ، امواج نوری ، ...) می باشد .

در واقع این لایه شامل یک سری استانداردها مربوط به شبکه LAN (802.3) و شبکه WAN (V.35) می باشد .



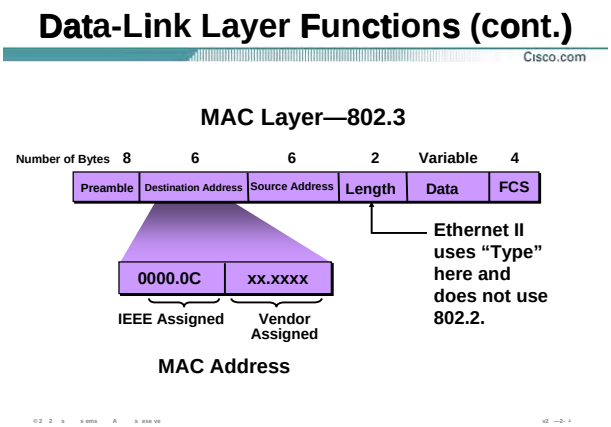
:Data-Link Layer

Data-Link Layer به عنوان لایه دوم از مدل هفت لایه ای OSI وظیفه برقراری یک لینک مورد اطمینان بین دو Station نهایی در یک شبکه LAN را به عهده دارد . آدرس دهی فریم ها در این لایه براساس آدرس فیزیکی (MAC Address) می باشد . بنابراین اطلاعات در این لایه به تعدادی فریم تقسیم شده و در هر فریم بعد از قرار گرفتن آدرس فیزیکی مبدأ و مقصد و اضافه شدن بیتهای خطایابی ، تحویل لایه فیزیکی جهت انتقال داده می شود .

این لایه شامل یکسری استانداردهای مربوط به شبکه LAN (MAC ، LLC)و شبکه WAN (HDLC ، Frame Relay) می باشد.

در شبکه LAN ، این لایه به دو زیر لایه LLC و MAC تقسیم می شود .

زیرلایه LLC (Logical Link Control) وظیفه کنترل مبادله دیتا را برعهده دارد . این لایه بسته به پروتکلهای لایه های بالاتر عمل می کند و می تواند یک سرویس اتصال گرا و یا یک سرویس بدون اتصال باشد . این بدان معنی است که در صورتی که در لایه های بالاتر عملیات تضمین انتقال صورت گیرد نیازی به این تضمین در این لایه نیست بنابراین LLC به صورت یک سرویس بدون اتصال عمل خواهد کرد.

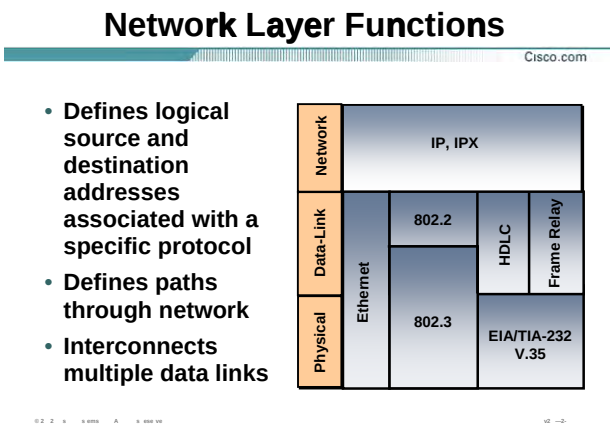


Data-Link Layer (ادامه):

زیرلایه MAC وظیفه خطایابی فریم براساس فیلد FCS و هـدایت فـریم LLC براسـاس فیلـدهای Source MAC Address و Destination MAC Address را به عهده دارد .

MAC Address دارای سـاختار ۴۸ بیتی می باشـد که شـامل دو بخش ۲۴ بیتی می باشـد .

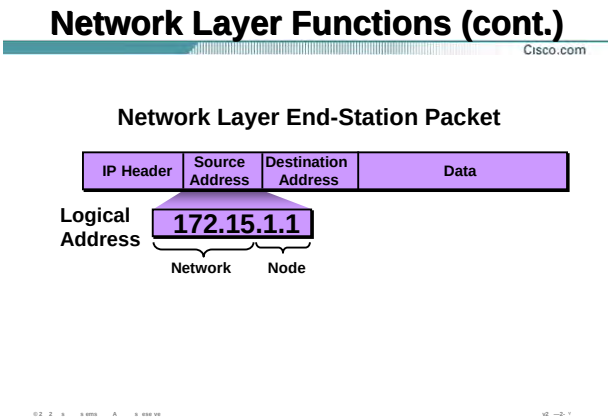
۲۴ بیت اول توسط IEEE به هر کدام از شرکتهای سازنده به صورت منحصر به فرد ارائه می شود و ۲۴ بیـت دوم توسـط هر شرکت به هر سخت افزاری که نیاز به یک آدرس فیزیکی دارد به صورت منحصربه فرد نسبت داده می شود .



:Network Layer

Network Layer به عنوان لایه سوم از مدل هفت لایه ای OSI ، وظیفه تعیین بهترین مسیر از میان مسیرهای متفاوت و هدایت پکتها براساس آدرس منطقی در مبدأ و مقصد را به عهده دارد .

آدرس منطقی در این لایه براساس پروتکل IP ، IPX و Apple talk خواهد بود و مسیریابی به کمک الگوریتم و پروتکلهای مسیریابی همچون RIP و OSPF خواهد بود .



Network Layer (ادامه):

شکل فوق ساختار یک پکت IP را نمایش می دهد . پروتکل IP در دو ورژن متفاوت ارائه شده است ، IPV4 و IPV6 .

IP Address V4 یک آدرس ۳۲ بیتی و IP Address V6 یک آدرس ۱۲۸ بیتی می باشد .

برای شناخت بیشتر با پروتکل IP و ساختار آن و نحوه استفاده از آن در یک شبکه به ماژول دوم و درس سوم مراجعه کنید .

Summary

Cisco.com

Internetworking evolves to support current and future applications

The OSI reference model organizes network functions into seven categories called layers

Data flows from upper-level user applications to lower-level bits transmitted over network media

Peer-to-peer functions use encapsulation and de-encapsulation at layer interfaces

Most network manager tasks configure the lower three layers

خلاصه :

ارتباطات شبکه ای براساس وجود یک ساختار مشخص و یک قاعده کلی می باشد که با رعایت کردن و حرکت کردن براساس این الگو نقل و انتقالات شبکه ای بین دو سخت افزار از دو شرکت سازنده مختلف امکان پذیر باشد .

هفت لایه OSI و یا مدل چهار لایه ای TCP/IP به منظور ارتباطات شبکه ای تعریف شده اند . بنابراین براساس این استانداردها هر لایه دارای تعاریف و مکانیزم کاری مربوط به خود می باشد و هر لایه علاوه بر اینکه دارای وظایف مشخصی می باشد مستقل از لایه های بالا و یا پایین تر نخواهد بود .

اطلاعات بعد از دریافت از لایه های بالاتر و پس از اعمال بسته بندی (Encapsulation) تحویل لایه زیرین شده و درنهایت تحویل آخرین لایه جهت انتقال داده می شود .

فصل دوم :

راه اندازی و پیکربندی
Cisco IOS

ایـن فـصل شـامل معرفـی Device هـای سیـسکو چـون روتـر و سـوئیچ و سیـستم عامـل مخـتص بـه سیـسکو (Cisco IOS) و نحوه ارتباط و پیکربندی اولیه هر کدام از آنها می باشد . در انتهای ایـن فـصل مـی آموزیـد کـه چگونـه بـا Device هایی چون router و switch ارتباط برقرار کرده و آنها را جهت استفاده در یک شبکه پیکربندی کنید .

درس اول :

معرفی و آشنایی با
Cisco IOS

هدف :

۱. معرفی راه های برقراری ارتباط با تجهیزات سیسکو جهت پیکربندی و مدیریت آنها در شبکه .

۲. معرفی IOS و ویژگی های آنها .

۳. معرفی CLI و جایگاه های مختلف (Mode) آن و شرح تک تک آنها .

:IOS

Internetwork operating System (IOS) هسته مرکزی روتر و بیشتر سوئیچ های سیسکو چون سوئیچ 2950 می باشد . در واقع سیستم عامل روترهای سیسکو همانند دیگر سیستم عامل ها وظیفه ذخیره و بازیابی فایل ، مدیریت حافظه و مدیریت سرویس های مختلف را به عهده دارد . این سیستم عامل فاقد محیط گرافیکی بوده و مبتنی بر خط فرمان می باشد لذا دارای یک واسط کاربری UI می باشد که به کمک آن دسترسی به فرامین و پیکربندی تجهیزات سیسکو امکان پذیر می باشد.

IOS در دو mode پیکربندی می شود ، set up mode و دیگری CLI.

:Set UP Mode

هنگامی که روتر و یا بعضی از سوئیچ های سیسکو مثل سوئیچ 2950 را برای بار نخست راه اندازی می کنید وارد set up mode شده و می توانید تنظیمات اولیه چون آدرس دهی و تنظیم پسوردها را انجام دهید . درواقع یک سری سوالات به صورت متوالی از شما پرسیده می شود و می توانید با پاسخ دادن به هر کدام از آنها تنظیمات اولیه را در همین ابتدای کار انجام دهید . البته این تنظیمات کامل نخواهند بود و برای تنظیم بیشتر می بایست به Mode دیگری

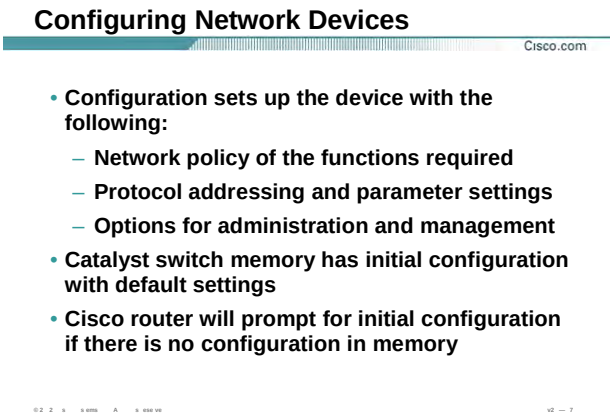
IOS (ادامه):

مراجعه کرد . همچنین می توانید به جای پاسخ دادن به این سوالات مستقیما وارد Setup Mode شوید و در هنگام نیاز این تنظیمات را انجام دهید .

:(Common Line Interface) CLI

Cisco IOS Command-line interface (CLI) جایگاهی است که می توانید تنظیمات بیشتری را روی روتر و سوئیچ انجام دهید. CLI یک محیط text Base می باشد به طوری که user در این محیط فرامین مورد نظرش را type می کند.

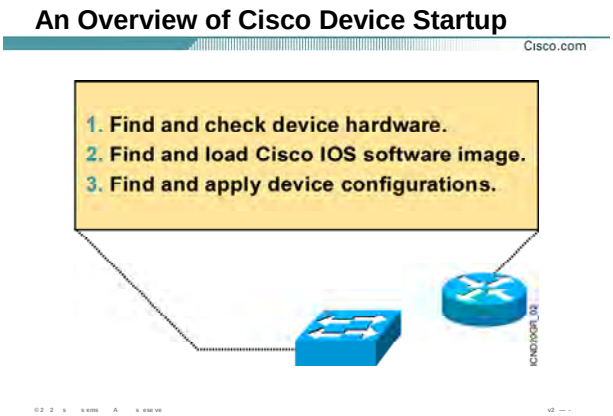
برای دسترسی به این محیط سه روش وجود دارد که در ادامه این درس با این سه روش آشنا می شوید.



تنظیمات تجهیزات شبکه :

تنظیم یک Device جهت کار در شبکه شامل تنظیم یک سری پروتکل ها و توابع خاص می باشد . سوئیچ یکی از تجهیزات شبکه می باشد که به صورت پیش فرض دارای یک سری تنظیمات اولیه بوده و بدون تنظیم اضافی قادر به هدایت ترافیک در یک شبکه LAN می باشد . اما روتر بدون تنظیم نمی تواند در شبکه وظیفه خود را انجام دهد بنابراین می بایست آن را جهت انجام وظیفه مسیریابی تنظیم کرد .

بنابراین در برخورد با روتر و سوئیچی که برای بار نخست تنظیم می شوند ، Setup Mode اولین Mode ایی می باشد که با آن مواجه می شوید .



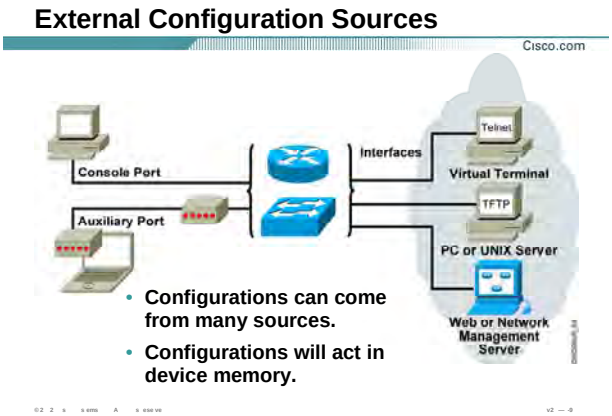
مروری بر نحوه راه اندازی سخت افزارهای سیسکو:

به طور کلی Device های شرکت Cisco از لحظه ای که روشن می شوند تا آمادگی برای شروع کار ۳ گام را پشت سر می گذارند .

در گام اول بعد از زدن کلید power سخت افزارها شناخته شده و سالم بودن آن از نظر سخت افزاری چک می شود.

گام دوم پیدا کردن IOS می باشد . در ادامه این درس می آموزید که IOS به صورت پیش فرض از کجا load شده و چگونه می توان پیش فرض Load شدن آن را تغییر داد .

گام آخر پیدا کردن تنظیمات ذخیره شده و اعمال این تنظیمات روی device .



راههای دسترسی به تجهیزات سیسکو:

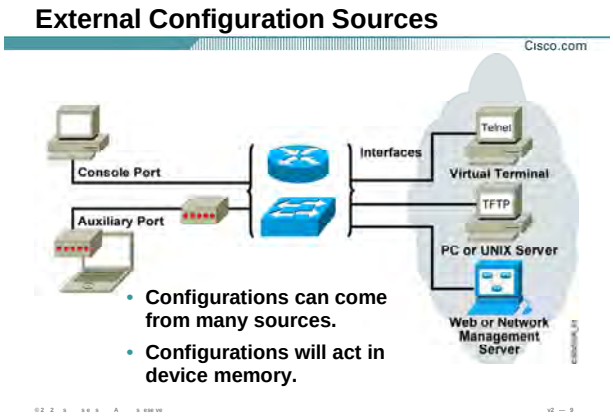
برای دسترسی به روتر یا سوئیچ پنج روش وجود دارد . سه روش جهت دسترسی به CLI و یک روش جهت ارتباط بین TFTP Server و تجیزات سیسکو و روش آخر تنظیم کردن تجهیزات سیسکو به کمک Web Browser می باشد . سه روش برای دسترسی به CLI عبارتنداز :

- console port
- Auxiliary port
- Telnet

:Console port

هنگامی که یک device را برای بار اول خریداری می کنید هیچ تنظیمی روی آن وجود ندارد بنابراین تنها راه دسترسی به IOS و configure کردن آن استفاده از پورت console می باشد.

در این روش شما به کمک کابل Rollover ، روتر یا سوئیچ را به یک PC متصل و به کمک نرم افزار Hyper Terminal با روتر و یا سوئیچ ارتباط برقرار کرده و آن را تنظیم می کنید .



راههای دسترسی به تجهیزات سیسکو (ادامه) :

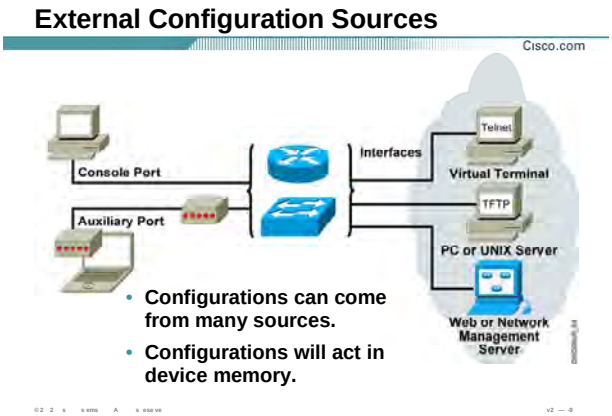
بعد از تنظیم روتر و یا سوئیچ از طریق پورت Console و دادن اجازه دسترسی از طریق روشهای بعدی ، قادر خواهید بود از روشهای دیگر برای برقراری ارتباط بدون ارتباط از طریق پورت Console استفاده کنید .

نکته : کابل Rollover کابلی است که یک سر آن دارای کانکتور Rj 45 جهت اتصال به پورت Console و سر دیگر آن دارای کانکتور 9 pin جهت اتصال به Com Port کامپیوتر می باشد .

Auxiliary port:

در روش دوم یعنی استفاده از پورت AUX ، شما می توانید از راه دور با روتر و یا سوئیچ ارتباط برقرار کرده و آنها را تنظیم کنید . این ارتباط از طریق بستر مخابراتی صورت می پذیرد.

به طور مثال با متصل کردن یک روتر به یک مودم و ارتباط از طریق خطوط Dial up می توان به روتر دسترسی پیدا کرده و آن را تنظیم کنید .



راههای دسترسی به تجهیزات سیسکو (ادامه) :

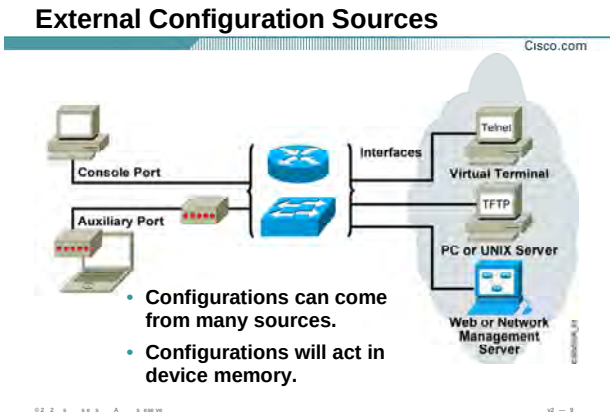
:Telnet

در صورتی که هنگام تنظیم کر ن اولیه روتر و یا سوئیچ آدرسی (IP address) را به آن نسبت داده باشید براحتی می توانید در یک شبکه TCP/IP به روتر یا سوئیچ سترسی پیدا کرده و آن را تنظیم کنید. این ارتباط از طریق سرویس Telnet و استفاده از پروتکل Telnet می ب شد .

بنابراین درصورت داشتن آدرس (IP Address) وتر و سوئیچ و همچنین فعال بودن امکان دسترسی از طریق Telnet ، می توانید با telnet کردن به آنها تنظیمات مورد نظرتان را روی آنها اعمال کنید .

:TFTP

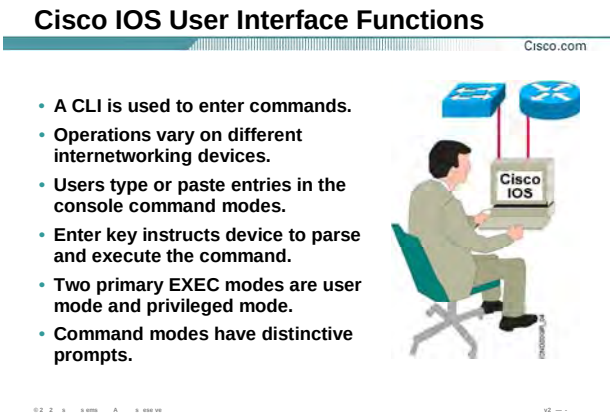
یکی دیگر از راههای ارتباطی ، ارتباط بین تجهیزات سیسکو با TFTP Server می اشد. بنابراین می توان با بهره گرفتن از پروتکل TFTP ، تنظیمات و IOS روتر و یا سوئیچ را در جای دیگری در شبکه و د قع در یک TFTP Server نگهداری کرد .



راههای دسترسی به تجهیزات سیسکو (ادامه) :

Web Browser:

آخرین راه ارتباط از طریق Web Browser می باشد . این ارتباط زمانی امکان پذیر خواهد بود که Device سیسکو جهت کار در شبکه TCP/IP آماده شده باشد . این بدان معنی است که دارای یک IP Address باشد تا به کمک آن بتوان Web Page مربوطه را Browse کنید .



:CLI

همان طور که گفته شد CLI یا همان Common Line Interface یک محیط Text Base می باشد و شما می توانید در این قسمت تنظیمات مختلفی را روی روتر و یا سوئیچ انجام دهید.

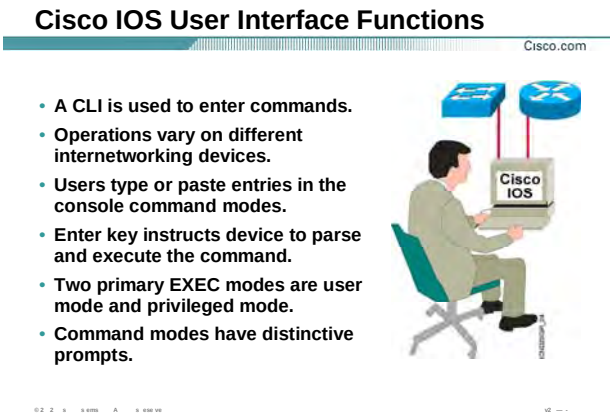
CLI در IOS سیسکو دارای دو mode اجرایی می باشد :

- user mode
- privileged mode

این بدان معنی است که برای وارد کردن تنظیمات روی روتر و یا سوئیچ می بایست وارد mode مربوطه شوید.

:User Mode

در این Mode می توانید عملیات محدودی را انجام دهید . در واقع این Mode پایین ترین سطح دسترسی به روتر یا سوئیچ را نشان می دهد . در این Mode عملیات Monitoring قابل اجرا است .در واقع افراد مختلف می توانند وارد این Mode شده و بدون دسترسی داشتن به تنظیمات ، عملیات محدودی چون چک کردن عملکرد روتر و یا سوئیچ را انجام دهند.



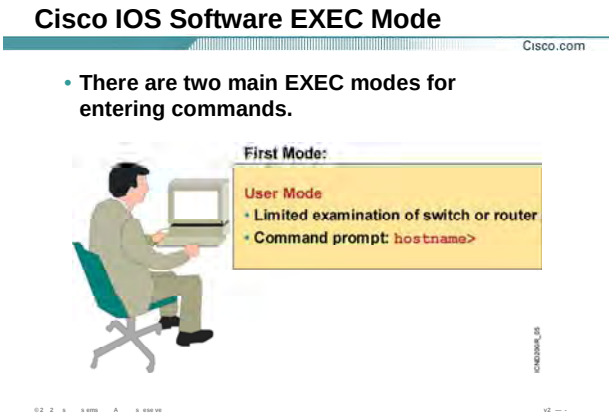
CLI (ادامه):

بنابراین این Mode پایین ترین Mode از نظر سطح دسترسی خواهد بود . لذا فرامین کمتری در این Mode قابل اجرا خواهد بود .

:Privileged Mode

همانطور که از نامش پیداست این Mode ، جایگاهی با سطح دسترسی بالاتر برای انجام تنظیمات روی روتر و یا سوئیچ می باشد . به صورت پیش فرض برای وارد شدن به این Mode نیازی به وارد کردن پسورد نیست ، اما برای برقراری امنیت می بایست قبل از وارد شدن به این Mode پسورد چک شود تا فقط افراد خاصی با داشتن پسورد بتوانند به این Mode دسترسی پیدا کنند.

بنابراین در این Mode ، دسترسی به تنظیمات روتر و یا سوئیچ و مشاهده و تغییر تنظیمات امکان پذیر می باشد .



:User Mode

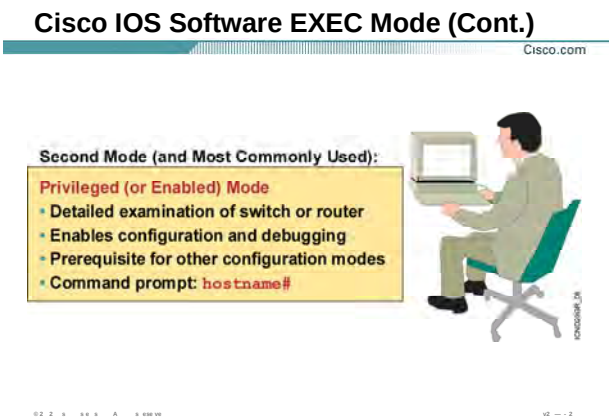
بعد از Boot شدن IOS و Load شدن کامل تنظیمات ، User Mode اولین جایگاهی است که CLI نشان می دهد . در این جایگاه Command prompt به صورت زیر می باشد :

Hostname >

همانطور که گفته شد user mode یک mode با سطح دسترسی های محدود می باشد . بنابراین در این Mode شما قادر به اجرا و به کار بردن برخی فرامین خاص هستید .

به طور مثال برای اجرای بعضی گزارشات همچون وضعیت حافظه و کنترل میزان ترافیک ورودی و یا خروجی به هر اینترفیس روتر و یا سوئیچ از این مد استفاده می شود.

Hostname > show flash



:Privileged Mode

در این mode که به آن enable mode نیز گفته می شود، اجازه دسترسی کامل به تمامی فرامین جهت تنظیمات بیشتر داده می شود . با وارد کردن فرمان زیر در User Mode وارد Privilade Mode خواهید شد :

Hostname > enable

با وارد کردن فرمان بالا ، command prompt به صورت زیر تغییر می کند :

Hostname #

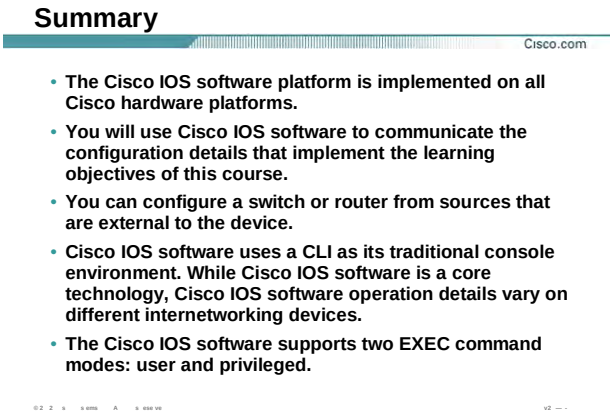
برای خارج شدن از این mode فرمان زیر را وارد می کنید.

Hostname # exit

در privileged mode شما دسترسی به mode های دیگری چون global mode و interface mode را خواهید داشت .

در واقع در این mode هدایت کامل روتر یا سوئیچ به شما واگذار می شود .

در ادامه این فصل می آموزید که چگونه می توان با تعریف کردن password ، امنیت این mode را برقرار کرد.



خلاصه :

در این درس با سیستم عامل روتر (Cisco IOS) و نحوه ارتباط با آن آشنا شدید . IOS سیسکو Text Base بوده و فاقد محیط گرافیکی می باشد . برای دسترسی به روتر یا سوئیچ پنج روش وجود دارد . سه روش جهت دسترسی به CLI و یک روش جهت ارتباط بین TFTP Server و تجیزات سیسکو و روش آخر تنظیم کردن تجیزات سیسکو به کمک Web Browser می باشد .

همچنین CLI یک محیط text-base است به طوری که دارای دو mode اجرایی زیر می باشد:

- user mode
- privileged mode

user mode یک مد اجرایی محدود است و تمامی فرامین در این مد قابل اجرا نمی باشند در حالی که privileged mode ، جایگاهی با حیطه اجرایی بالا ست و کنترل ، مدیریت و تنظیمات به صورت کلی در این Mode قابل اجرا می باشند.

درس دوم :

آشنایی با Router

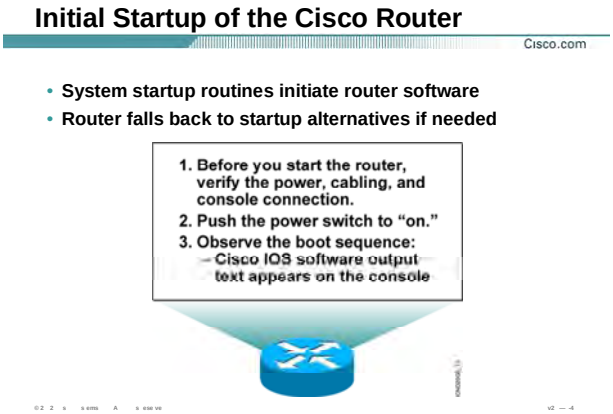
هدف :

۱. مراحل بوت شدن IOS در روترهای سیسکو

۲. CLI و تعامل میان روتر و کاربر به کمک آن .

۳. CLI و استفاده از help در آن .

۴. انواع حافظه ها و محل قرارگیری و نحوه مشاهده محتویات هر کدام از آنها.



راه اندازی اولیه روتر :

برای راه اندازی اولیه روتر ابتدا منبع تغذیه کننده برق را چک کنید و سپس به کمک یک کابل rollover ارتباط کامپیوتر و روتر را برقرار کنید.

یادآوری : همانطور که گفته شد کابل rollover کابلی است که یک سر آن دارای کانکتور RJ-45 می باشد که آن را درون پورت console قرار داده و سر دیگر آن دارای کانکتور 9 pin می باشد که آن را به COM port کامپیوتر متصل می کنید.

بعد از برقراری ارتباط فیزیکی نوبت به یک نرم افزار می رسد که به کمک آن به CLI روتر دسترسی پیدا کنید . به کمک نرم افزار Hyper Terminal ارتباط نرم افزاری با روتر برقرار می شود .

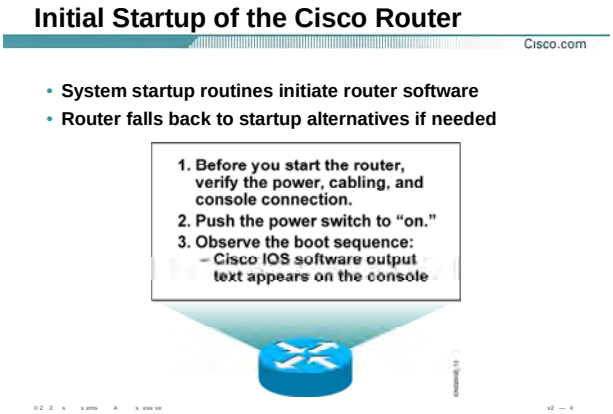
برای این منظور مراحل زیر را به ترتیب انجام دهید:

۱. مسیر زیر را دنبال کنید و سپس Hyper terminal را اجرا کنید:

Start -> all programs -> accessories -> communications -> Hyper Terminal

۲. در پنجره Connection Description نام دلخواهی را وارد کرده و سپس گزینه OK را انتخاب کنید.

۳. در پنجره Connect To و در قسمت Connect Using شماره پورت سریال از کامپیوتر که کابل Rollover را به آن متصل کرده اید را انتخاب کنید .

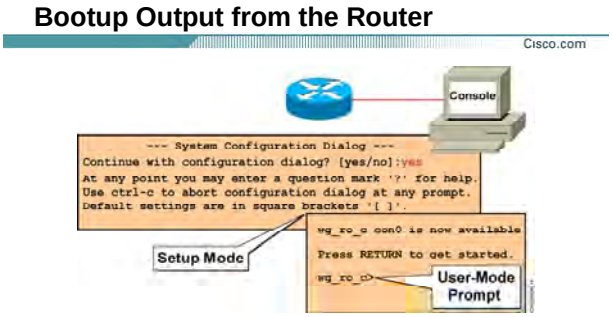


راه اندازی ولیه روتر (ادامه) :

۴. در پنجره Port Setting نرخ ارسال اطلاعات که دارای واحد بیت در ثانیه می باشد را انتخاب کنید. به طور مثال مقدار 9600 ا در این قسمت انتخاب کنید.

بعد از راه اندازی Hyper Terminal ، کلید power روتر را در وضعیت on قرار دهید .

بعد از روشن شدن روتر در پنجره Hyper Terminal یکسری اطلاعات که در مورد سخت افزار و IOS و غیره می باشد نمایش داده شده و سپس وارد User Mode می شو .



Unconfigured Versus Configured Router

Set up Mode و تنظیمات اولیه روتر :

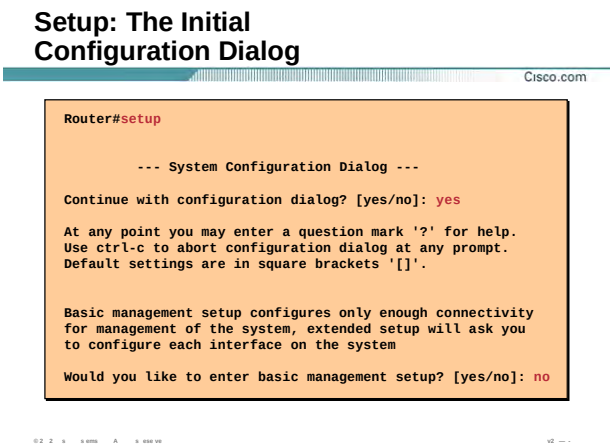
هنگامی که یک روتر را برای بار اول روشن می کنید وارد Set up Mode می شود . همچنین درصورتی که یک روتر تنظیمات خود را از دست داده باشد و یا به هر علتی فراموش کنید تنظیمات را در یک حافظه دائمی ذخیره کنید بعد از Boot مجدد وارد این Mode می شود .

درواقع پس از روشن کردن روتر و بعد از گذراندن مرحله چک سخت افزاری و اطمینان از safe بودن آنها نوبت به خواندن تنظیمات و load آنها می رسد و از آنجایی که روتر فاقد تنظیم است، وارد مرحله Setup Mode می شود .

در این حالت یک سری سوالات به صورت متوالی پرسیده می شود . بنابراین می توانید یک سری تنظیمات اولیه چون نام و آدرس دهی به اینترفیسها را در این مرحله انجام دهید.

اما شما می توانید این کار به موقع دیگری موکول کنید . بنابراین در پاسخ به سوال زیر گزینه No را انتخاب کنید تا وارد User Mode شوید .

Continue with configuration Dialog? [Yes/no]



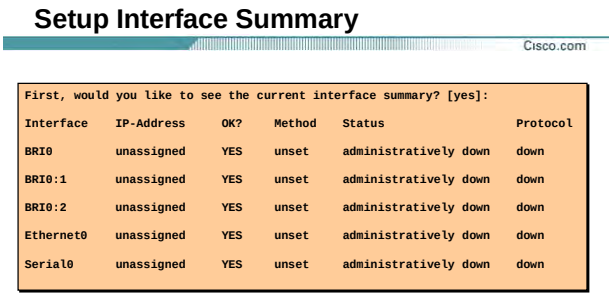
Set up Mode و تنظیمات اولیه روتر :

اگر بخواهید روتر را در گام اول به کمک یک سری سوال و جواب ها تنظیم کنید در پاسخ به اولین سوال که بعد از boot شدن روتر پرسیده می شود پاسخ Yes را انتخاب کنید.

Continue with configuration Dialog? [Yes/no] yes

سوال بعدی در مورد extended setup می باشد . درواقع دراین قسمت می توانید با پاسخ دادن به سوالات متوالی تنظیمات دقیق تری را در مورد اینترفیس های مختلف روی روتر انجام دهید .درغیر این صورت در پاسخ به سوال زیر پاسخ no را انتخاب کنید.

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



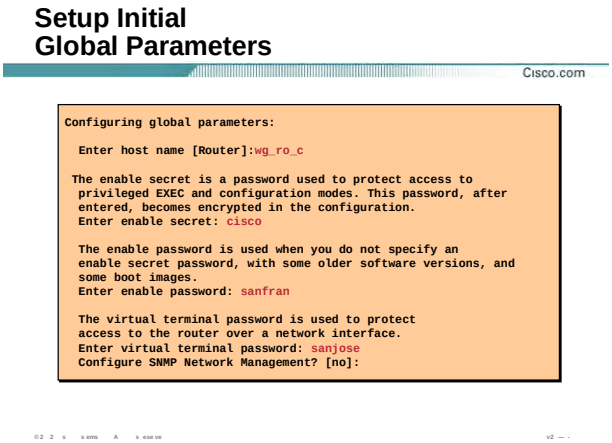
Interfaces Found During Startup

Set up Mode و تنظیمات اولیه روتر :

سوال بعدی از شما می پرسد که آیا مایلید تعداد اینترفیس ها و وضعیت هر کدام از آنها چون up یا down بودن و غیره را مشاهده کنید یا خیر ؟

First, would you like to see the current interface summary? [Yes]:

در صورتی که پاسخ پیش فرض را انتخاب کنید لیست اینترفیس های روتر و state مربوط به هر کدام از آنها به شما نمایش داده می شود .



Set up Mode و تنظیمات اولیه روتر :

سوال بعدی از شما می پرسد چه نامی را می خواهید برای روتر خود انتخاب کنید ؟

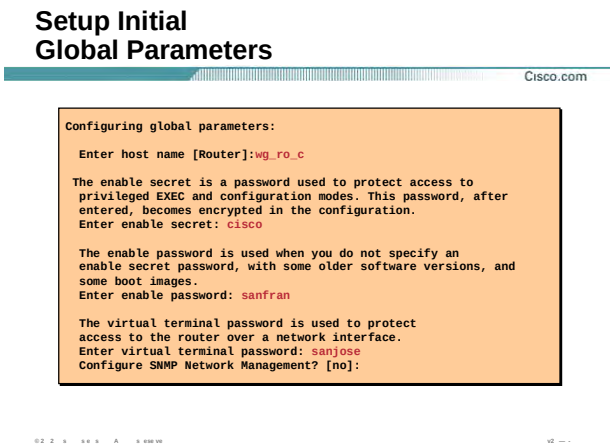
Enter host name [Router] :

در صورتی که متنی را وارد نکنید و کلید ENTER را بفشارید این به معنی آن است که نام پیش فرضی که در داخل کروشه نوشته شده است را به عنوان نام روتر پذیرفته اید .

مرحله بعد و سوالات بعدی به منظور افزایش امنیت دسترسی به روتر است . همانطور که می دانید دسترسی به CLI از طریق سه روش امکان پذیر است . بنابراین باید در مقابل هر کدام از آنها مانعی قرار داشته باشد تا بعد از authentication و تایید اعتبار دسترسی به روتر امکان پذیر باشد.

چهار نوع پسورد موجود می باشد:

- enable password
- secret password
- telnet password
- console password



Set up Mode و تنظیمات اولیه روتر (ادامه) :

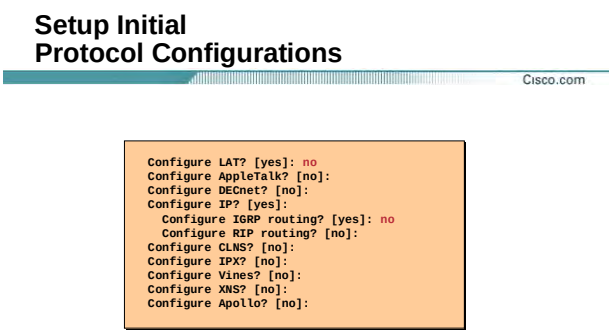
در پایان این فصل می آموزید که هر کدام از اینها در کجا و چگونه عمل می کنند.

اما در setup mode می بایست سه تا از این چهار مورد را تنظیم کنید .

در واقع در اینجا enable password و secret password و telnet password را به ترتیب برای روتر مشخص می کنید .

سوال بعدی در مورد پروتکل SNMP و manage کردن آن می باشد . همانطور که می دانید SNMP پروتکل مدیریت شبکه و دارای option های بسیاری است .

در اینجا مقدار پیش فرض که همان no می باشد را انتخاب کنید تا تنظیم آن را به زمان دیگر موکول کند.

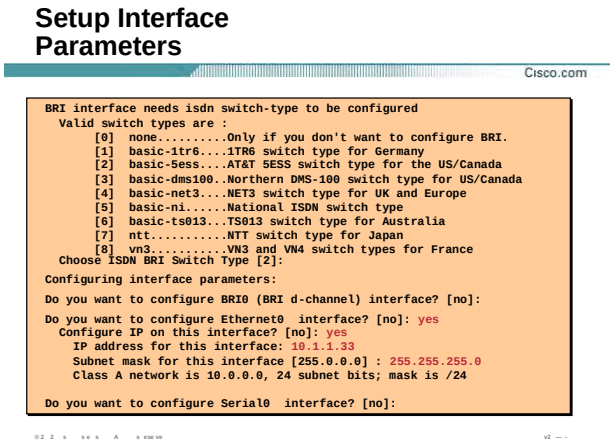


Set up Mode و تنظیمات اولیه روتر :

در ادامه سوالات به این مرحله می رسید که می بایست تنظیمات اولیه پروتکل ها همچون نوع Routing protocol و یا نوع پروتکلی که روی Interface فعال می شود را مشخص کنید .

در این قسمت به جز تنظیم پروتکل IP ، به سوالات دیگر پاسخ no را وارد کنید . درواقع با این کار تنظیم بقیه موارد را به زمان دیگری موکول خواهیم کرد.

Configure IP? [Yes]:



Set up Mode و تنظیمات اولیه روتر :

در این مرحله پارامتر های اولیه مربوط به یک اینترفیس چون IP address تنظیم می شود.

برای هر اینترفیس IP address و subnet mask مربوط به آن پرسیده می شود .

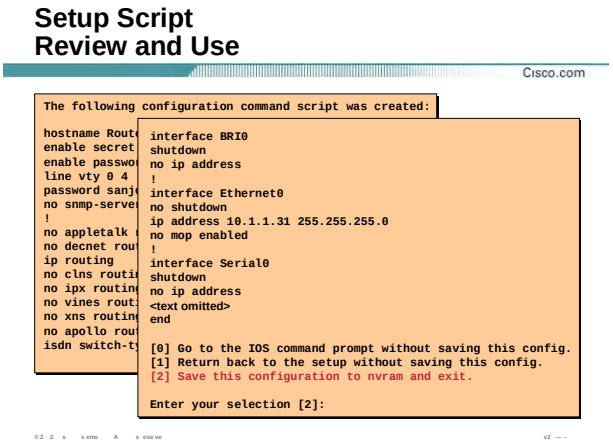
با توجه به کلاس IP address ایی که شما وارد کرده اید ، Subnet mask مربوطه را مشخص می کند که شما می توانید مقدار پیش فرض را نپذیرفته و subnet mask مورد نظرتان را وارد کنید.

Do you want to configure Ethernet0 interface? [No]: yes

Configure IP on this interface? [No]: yes

IP address for this interface: 10.1.1.33

Subnet mask for this interface [255.0.0.0]: 255.255.255.0



Set up Mode و تنظیمات اولیه روتر :

بعد از پایان سوالات نوبت به ذخیره سازی آن می رسد.

شما با سه گزینه روبه رو هستید:

[0] Go to the IOS command prompt without saving this config.

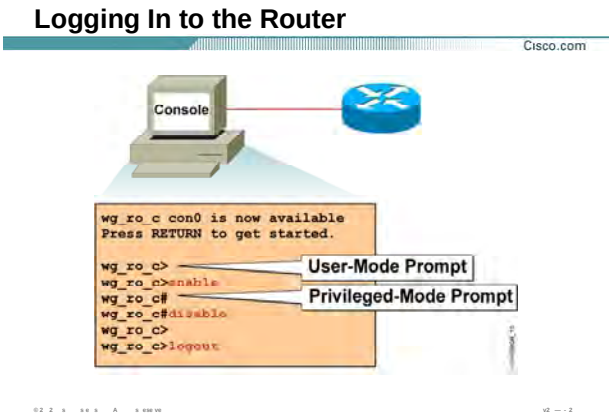
[1] Return back to the setup without saving this config.

[2] Save this configuration to nvram and exit.

اگر اولین گزینه یعنی [0] را انتخاب کنید ، روتر بدون ذخیره کردن تنظیمات فعلی وارد CLI می شود. یعنی بدون ذخیره شدن این تنظیمات وارد user mode شده و انجام تنظیمات به وقت دیگری موکول می شود.

اگر گزینه دوم یعنی [1] را انتخاب کنید ، این بدان معنی است که شما بدون ذخیره کردن تنظیمات فعلی می خواهید دوباره به اولین سوال در set up mode برگشته و مجددا به سوالات پاسخ دهید .

اگر گزینه آخر یعنی [2] را انتخاب کنید ، شما می خواهید تمامی تنظیماتی که تاکنون به صورت سوال و جواب انجام داده اید را در یک حافظه دائم (nvram)ذخیره کنید.



User Mode و Privileged Mode:

بعد از boot کامل و بعد از وارد شدن به CLI ، اولین mode ای که آن را می بینید user-mode می باشد .

wg_ro_c>

همانطور که قبلا به آن اشاره کردیم این mode دارای محدودیت اجرایی است. این بدان معنی است که تعداد کمی از فرامین در این mode قابل اجرا هستند.جایگاه دیگر privileged mode می باشد . در این mode شما می توانید به تمامی فرامین دسترسی داشته باشید . برای وارد شدن به این mode در user mode فرمان enable را به صورت زیر وارد کنید:

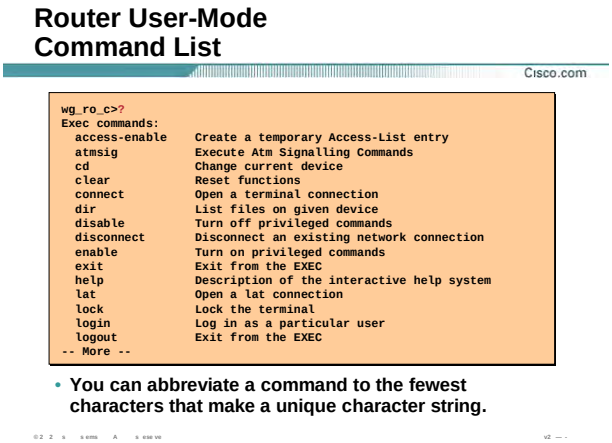
wg_ro_c> enable

شما می توانید به جای نوشتن کل فرمان بخشی از آن را type کنید . به طور مثال به جای نوشتن enable کافیست type کنید en .با وارد شدن به privileged mode ، command prompt به صورت زیر در می آید:

wg_ro_c #

برای خارج شدن از این mode نیز می توانید از فرمان exit یا disable استفاده کنید.

wg_ro_c # exit



فعال شدن Help به کمک علامت ؟ در User Mode:

برای دیدن لیست فرما ها در یک mode می توان از علامت ؟ استفاده کرد . در واقع help روتر یا سوئیچ را با زدن ؟ فعال می کنید و با وارد کردن ؟ ، کل ه فرامین ک د این Mode قابل اجرا می باشد نمایش داده می شود .درصورتی که تعداد فرامین نمایش داده شده از یک صفحه بیشتر باشد ، با زدن کلید space صفحه به صفحه و با زدن کلید enter می توانید خط به خط فرامین را مشاهده کنید .

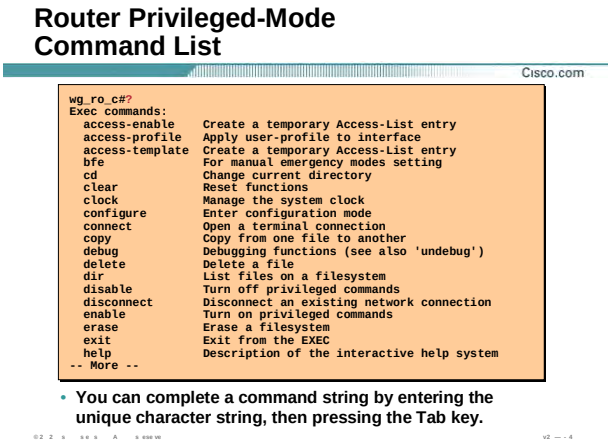
همچنین می توانید چند character اول از یک کلمه ر نوشته و سپس با زدن علامت ؟ فرمانهایی که با این حروف آغاز می شوند را ببینید. به طور مثال بعد از نوشتن حرف e علامت ؟ را تایپ کنید . بنابراین کلماتی که با حرف e نوشته شده اند فیلتر شده و به صورت زیر به شما نمایش داده می شود .

wg_ro_c > e ?

enable, exit

می توانید لیست فرمانهایی را که در user mode قابل استفاده هستند را ا زدن علامت ؟ در مقابل command prompt مشاهده کنید :

wg_ro_c>?

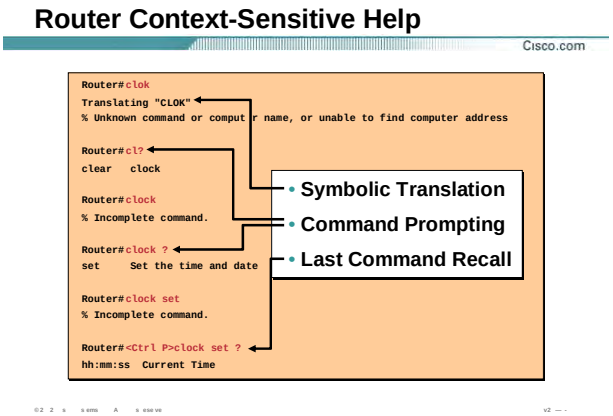


فعال شدن Help به کمک علامت ؟ در Privileged Mode:

برای فعال کردن Help در privileged mode ، ؟ استفاده می شود .

توجه داشته باشید که بعضی از فرمانها هم در User Mode و هم در Privilede Mode قابل اجرا هستند.

به طور مثال فرمان ping قابل اجرا در privileged mode و user mode هستند درحالی که برخی دیگر فقط در Privileged Mode قابل اجرا می باشند و این به خاطر ممتاز بودن این Mode است .



استفاده از Help در یک مثال :

تا به اینجا با Command History و Context-Sensitive Help آشنا شدید . این مثال ترکیبی از این دو ویژگی می باشد . فرض کنید قرار است شما ساعت مربوط به روترتان را تنظیم کنید و این کار را تا به حال انجام نداده اید . در privileged mode فرمان Clok را type می کنید .

همانطور که می بینید پیغامی نمایش داده می شود مبنی بر اینکه یک فرمان ناشناخته می باشد و می بایست این فرمان اصلاح شود . فرض کنید شما نحوه نوشتن آن را فراموش کرده اید ، بنابراین دو حرف اول آن را نوشته و بعد با نوشتن ؟ از help استفاده می کنید .

همانطور که می بینید دو کلمه با فیلتری که گذاشتید منطبق هستند :Clear و clock .

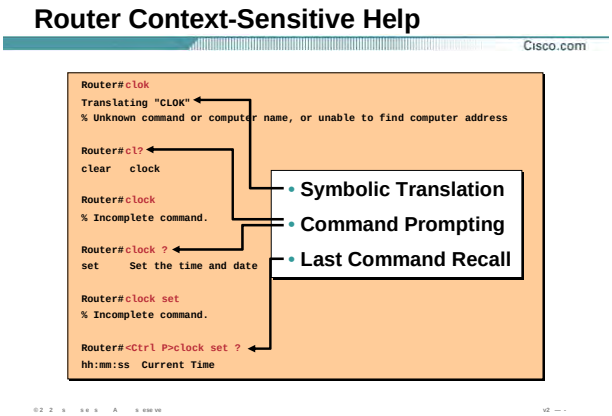
بنابراین شما clock را type می کنید و کلید enter را می زنید .

دوباره به شما پیغام می دهد .

% incomplete command.

فرمان شما کامل نیست . بنابراین باید آن را کامل کنید ولی شما از ادامه فرمان هیچ آگاهیی ندارید پس چه باید کرد؟

این بار هم از help استفاده می کنیم پس با زدن کلید space و زدن علامت ؟ نتیجه help را می بینید:



استفاده از Help در یک مثال (ادامه) :

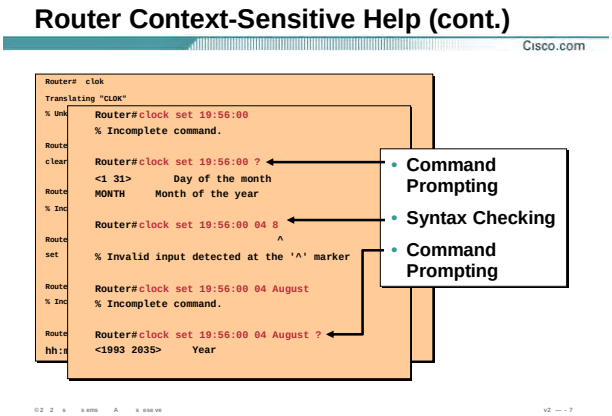
set Set the time and date

بنابراین کلمه بعدی set می باشد که آن را وارد می کنید و کلید enter را می زنید. باز به شما پیغام کامل نبودن فرمان داده شود . آیا راه را دوباره باید بروید و فرمانی را که تا به اینجا نوشته اید را دوباره type کنید؟

خیر ، شما از history کمک می گیرید . History لیستی از آخرین فرمانهایی را که وارد کرده اید را فراخوانی می کند. با زدن **Ctrl-P** می توانید آخرین فرمان را صدا بزنید . اگر آن را چند بار بزنید فرمانهای قبلی نیز به ترتیب به شما نشان داده خواهد شد .

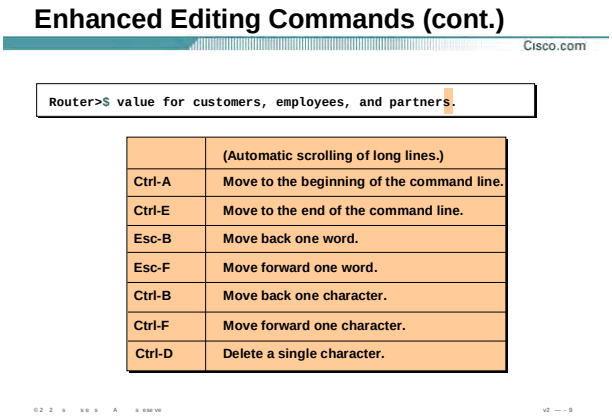
به کمک فرمان زیر می توانید history و محتویات آن را مشاهده کنید .

Router# show history



استفاده از Help در یک مثال(ادامه) :

بنابراین همان طور که مشاهده می کنید به کمک استفاده از Command History و Context-Sensitive Help ، کار تنظیم ساعت و تاریخ روی این روتر به پایان رسید.



استفاده از کلیدهای میانبر در CLI :

استفاده از کلیدهای میانبر در استفاده بهینه از فرمانها به شما کمک بسیاری می کنند . لیست برخی از کلیدهای حرکتی در IOS سیسکو به شرح زیر می باشد:

Ctrl-A: برای رفتن به ابتدای خط فرمان.

Ctrl-E: برای رفتن به انتهای خط فرمان.

Esc-B: برای رفتن به اندازه یک کلمه به عقب.

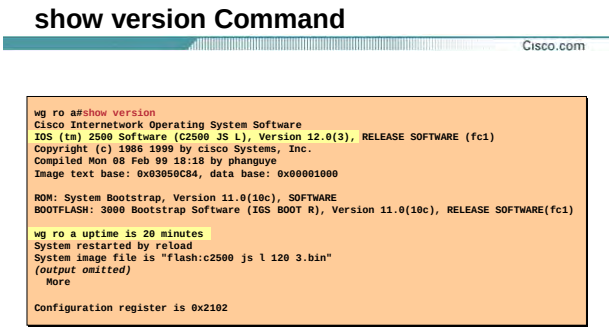
Esc-F: برای رفتن به اندازه یک کلمه به جلو.

Ctrl-B: برای رفتن به اندازه یک کارکتر به عقب.

Ctrl-F: برای رفتن به اندازه یک کارکتر به جلو.

Ctrl-D: برای پاک کردن یک کارکتر استفاده می شود.

Ctrl-P و Ctrl-N: فراخوانی فرامین از حافظه History .



فرمان Show Version و مفاهیم استخراجی از آن :

این فرمان برای دیدن اطلاعات پایه ای کاربرد فراوانی دارد . به کمک این فرمان می توان در مورد سخت افزار و ورژن IOS و میزان حافظه های RAM و NVRAM و FLASH و نام platform و مدت زمان up بودن device ، اطلاعاتی را بدست آورد .

(C2500-JS-L) : IOS به صورت یک فایل اجرایی binary در حافظه flash ذخیره می شود و این فایل دارای نامی می باشد که به صورت پیش فرض سه قسمتی است:

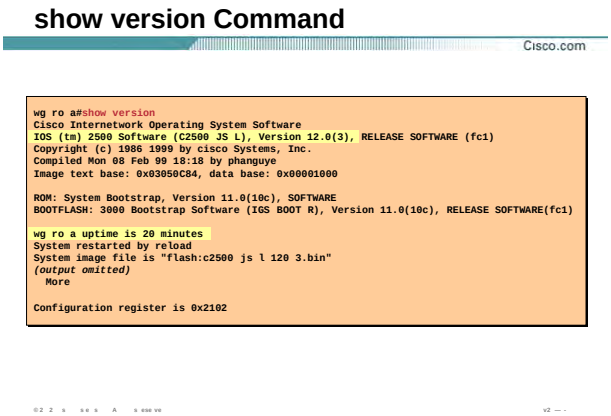
C2500: نام سخت افزاری device است که در این مثال روتری از سری ۲۵۰۰ می باشد.

JS: این نشان می دهد که این ورژن از IOS نسخه enterprise بوده و توانایی توسعه پیدا کردن را دارد.

L: این نشانه بیانگر این است که این فایل توانایی move دادن از حافظه flash را دارد.

Version 12.0(3): ورژن IOS را نمایش می دهد.

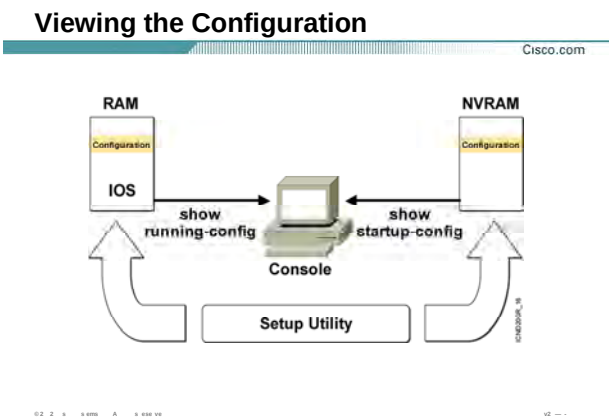
نکته دیگری که میتوان از این فرمان بدست آورد میزان حافظه flash و DRAM میباشد که در هنگام ارتقاء و انتخاب IOS باید به این دو مورد توجه بسیاری کنید .



فرمان Show Version و مفاهیم استخراجی از آن :

به کمک این فرمان میتوان ورژن Registry را دید. در مبحث password recovery برای دیدن ورژن Registry از این فرمـان به خوبی استفاده خواهید کرد .

Configuration register is 0x2102



بررسی حافظه های RAM و NVRAM :

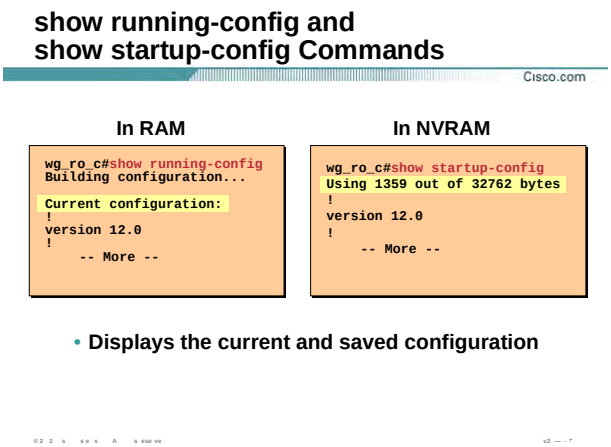
علاوه بر حافظه Flash و ROM روتر دو حافظه دیگری نیز دارد : RAM و NVRAM .

هنگامی که روتر را روشن می کنید روتر بعد از گذراندن مرحله power-on self-test یا همان POST و بعد از load کردن IOS به دنبال تنظیماتی می گردد که قبلا آنها را در حافظه NVRAM ذخیره کرده اید.

در صورتی که آنها را پیدا کند ، آنها را در حافظه فرار و جاری روتر که همان حافظه RAM می باشد قرار می دهد و در صورتی که موجود نباشد وارد set up mode می شود .

تمامی تنظیمات تا زمانی که روتر روشن می باشد در حافظه فرار روتر قرار دارد و این منطقی نیست که با خاموش شدن روتر، تمامی تنظیمات را از دست بدهید . بنابراین باید آنها را در به یک حافظه دائمی منتقل کنید .

NVRAM حافظه دائمی می باشد که محل قرار گیری فایلی به نام startup-config می باشد و RAM محل قرارگیری فایلی به نام running-config .



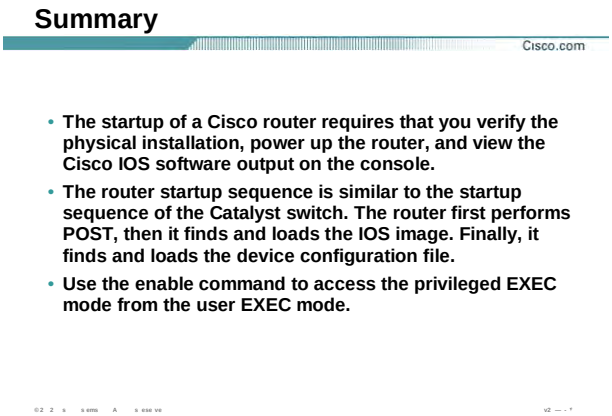
بررسی حافظه های RAM و NVRAM :

برای دیدن محتویات فایل startup-config که در حافظه NVRAM قرار دارد از فرمان زیر استفاده می کنیم :

wg_ro_c#show startup-config

برای دیدن محتویات فایل running-config که در حافظه RAM قرار دارد از فرمان زیر استفاده می کنیم :

wg_ro_c#show running-config



خلاصه :

بعد اینکه روتر را روشن می کنید روتر وارد مرحله Power-on self-test می شود در این مرحله سخت افزار ها از نظر عملکرد تست می شوند . بعد از گذر از این مرحله و بعد از load شدن IOS ، محتویات NVARM بررسی می شود .

تنظیمات تحت نام startup-config در حافظه دائمی NVRAM ذخیره می شود .

در صورتی که روتر را برای بار اول راه اندازی کنید و یا اینکه فراموش کرده باشید تنظیمات قبلی را در NVRAM ذخیره کنید ، روتر وارد setup mode می شود.

در غیر این صورت تنظیمات از NVRAM خوانده شده و در حافظه RAM رگذاری می شود.

برای دیدن اطلاعات پایه چون میزان حافظه DRAM و Flash و همچنین نام فایل IOS که خود شامل اطلاعات بسیاری می باشد از فرمان show version استفاده می کنیم.

درس سوم :

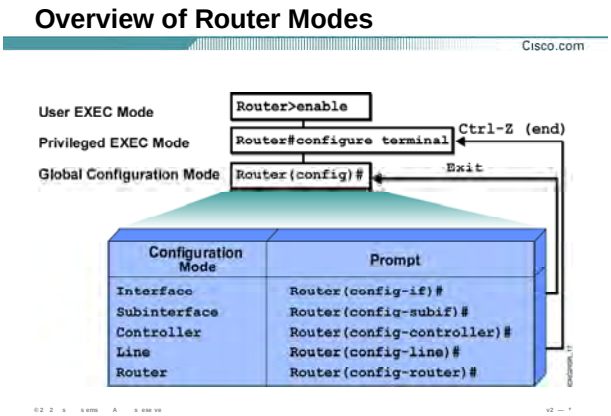
معرفی پروتکل IP و تنظیم آن روی Cisco Router

هدف :

١. تنظیم اولیه یک روتر.

٢. CLI و Mode های مختلف.

٣. انواع پسوردها و نحوه تنظیم آنها .



CLI و Mode های مختلف :

تا به اینجا با دو mode آشنا شدید user mode و privileged mode .

اما mode دیگر ، تحت عنوان global mode موجود می باشد.

در این mode تنظیمات اصلی چون تنظیمات اینترفیس ها و فعال کردن Routing Protocol ها و غیره صورت می گیرد.

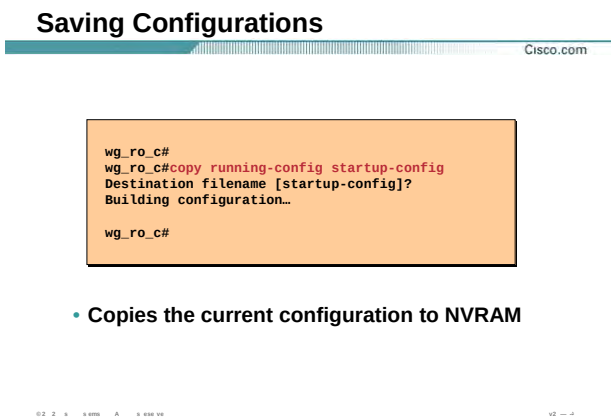
برای وارد شدن به global mode ابتدا باید وارد privileged mode شده و سپس با وارد کردن فرمان Configure terminal وارد این mode شوید.

Router# Configure terminal

با وارد شدن به این mode شکل command prompt به صورت زیر تغییر می کند .

Router(config)#

برای خارج شدن از global mode کافی است فرمان exit را در این mode وارد کنید.



ذخیره کردن تنظیمات :

تا به اینجا با انواع حافظه ها آشنا شدید . همانطور که می دانید تنظیمات در حافظه فرار روتر تحت فایل running-config قرار دارند و با خاموش شدن روتر از بین می رود .

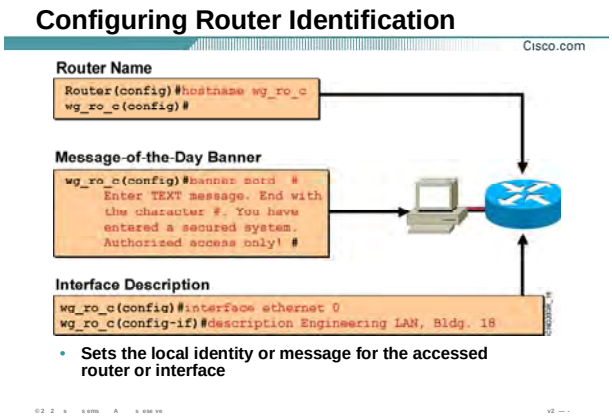
بنابراین باید این تنظیمات را به حافظه پایدار یا همان NVRAM منتقل کنیم . بنابراین با copy کردن فایل running-config در startup-config عملیات انتقال صورت می گیرد.

wg_ro_c# copy running-config startup-config

از طرفی می توان فایل startup-config یا همان محتویات NVRAM را پاک کرد .

برای این منظور فرمان زیر را در privileged mode به صورت زیر وارد کنید:

wg_ro_c# erase startup-config



تنظیم نام و Dscription:

Hostname: برای تغییر نام روتر یا سوئیچ از این فرمان استفاده می شود.

نامی که شما به روتر یا سوئیچ نسبت می دهید فقط یک نام محلی می باشد و روی عملکرد آن تأثیری نمی گذارد.

پیشنهاد می شود نامی که به روتر نسبت می دهید متناسب با محل جغرافیایی و موقعیت مکانی آن باشد.

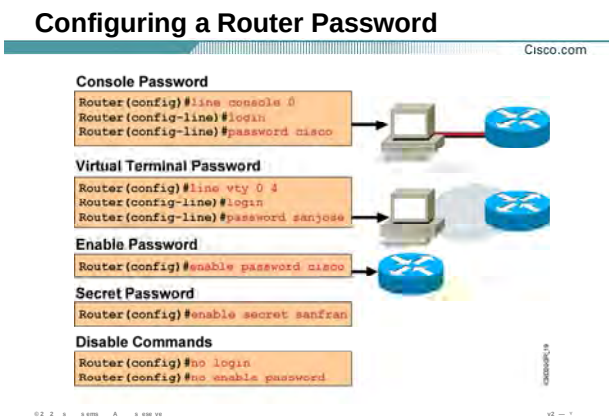
MOTD Banner: MOTDیا همان Message of the day پیغامی می باشد که در هر بار login کردن به روتر برای هر user و برای هر ارتباط نشان داده می شود.

در واقع ارتباط چه از طریق console port و auxiliary port باشد و چه از طریق telnet این پیغام نمایش داده خواهد شد .

این پیام یک اخطار امنیتی می تواند باشد که قبل از login کردن نمایش داده می شود.

Hostname Description: توضیحی می باشد که برای هر اینترفیس می توان نوشت و مانند hostname فقط یک مشخصه محلی می باشد و برای مدیریت بهتر اینترفیس ها از آن استفاده کرد.

برای دیدن description هر اینترفیس می توان از فرمان show running-config کمک گرفت.



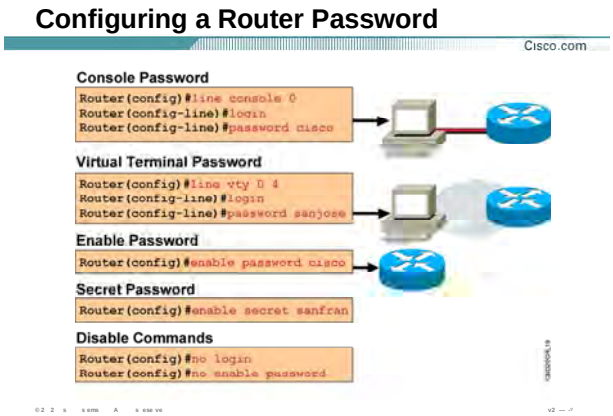
انواع پسورد و نحوه تنظیم کردن آنها :

تابه اینجا با روشهای برقراری ارتباط با روتر یا سوئیچ آشنا شدید . همانطور که می دانید برای افزایش امنیت نیاز به authentication و تأیید هویت می باشد.

در این قسمت انواع پسوردها و محل استفاده از هریک از آنها را مورد بررسی قرار می دهیم :

پنج نوع پسورد وجود دارد:

۱. Enable Password
۲. Secret Password
۳. AUX Password
۴. Telnet Password
۵. Console Password



انواع پسورد و نحوه تنظیم کردن آنها (ادامه) :

Enable password: برای برقراری امنیت هنگام ورود به privileged mode استفاده می شود . هنگامی که در user mode فرمان enable را وارد می کنید و می خواهید وارد privileged mode شوید این password پرسیده می شود.

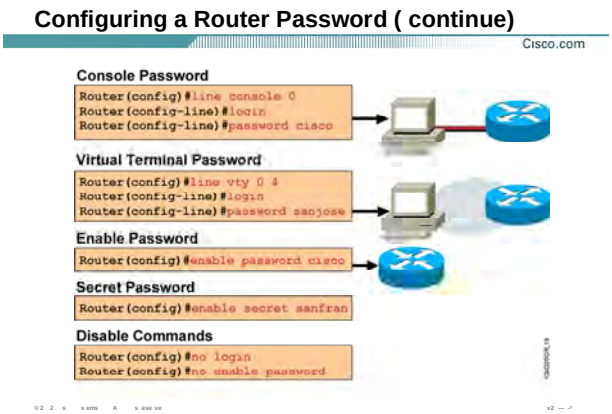
Router(config)#enable password cisco

این پسورد به صورت clear text ذخیره می شود و به کمک فرمان show run می توانید آن را به صورت clear و کد نشده ببینید.

Secret Password: همانند enable password می باشد. با این تفاوت که پسورد به صورت کد شده در فایل Running-config و startup-config ذخیره می شود و به صورت clear-text نمایش داده نمی شود .

Router(config)#enable password cisco

توجه داشته باشید هنگامی که secret password را تنظیم می کنید، تا زمان فعال بودن secret password ، enable Password به صورت غیر فعال در می آید و می بایست هنگام ورود به Priviledeg Mode ، پسورد مربوط به Secret Password را وارد کنید .



انواع پسورد و نحوه تنظیم کردن آنها (ادامه) :

Telnet Password: یکی از راههای دسترسی به روتر Virtual Terminal یا همان Telnet می باشد . بنابراین درصورتیکه به یک روتر Telnet می کنید ، می بایست بعد از بررسی و صحت Authentiction ، ارتباط برقرار شود .

برای تنظیم کردن telnet password وارد global mode شده و فرمان زیر را وارد می کنید:

Router(config)#line vty 0 4

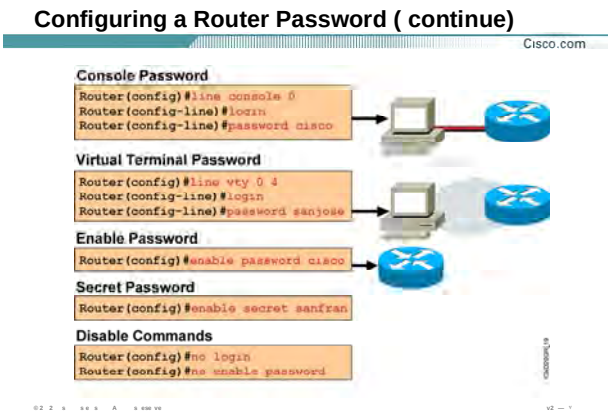
به ازای هر ارتباط Telnet یک Session برقرار می شود بنابراین به اندازه تعداد Line هایی که IOS ساپورت می کند می توانید Telnet Session برقرار کنید.

برای دیدن تعداد Line هایی که IOS ساپورت می کند کافی است از Help کمک بگیرید .

Router(config-line)#line vty 0 ?

<1-4> Last Line Number

<cr>



انواع پسورد و نحوه تنظیم کردن آنها (ادامه) :

فرمان بعدی login می باشد . در واقع با این فرمان می گویید که در صورت telnet شدن به این device ، پسورد پرسیده شود.

Router(config-line)#login

به همین ترتیب می توان با به کار بردن فرمان no login ، بگوییم که در صورت telnet شدن به این device ، پسورد پرسیده نشود.

Router(config-line)#no login

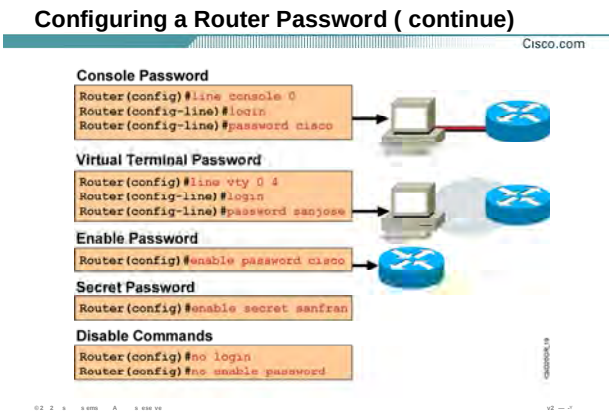
مرحله آخر تعریف پسورد می باشد:

Router(config-line)#password sanjose

توجه داشته باشید telnet password قبل از وارد شدن user به user mode پرسیده می شود.

به کمک فرمان show session می توان تمامی session های برقرارشده و مدت زمان connect بودن هر یک از آنها را مشاهده کرد.

Router# show session



انواع پسورد و نحوه تنظیم کردن آنها (ادامه) :

و می توانید به کمک فرمان disconnect ، ارتباط session خاصی را با روتر قطع کرد . برای این منظور کافی است فرمان زیر را به صورت زیر وارد کنید.

Router# disconnect connection-number

از طرفی با فرمان resume می توانید بین connection ها حرکت کنید بدون اینکه connection ایی را disconnect کنید.

Router# resume connection-number

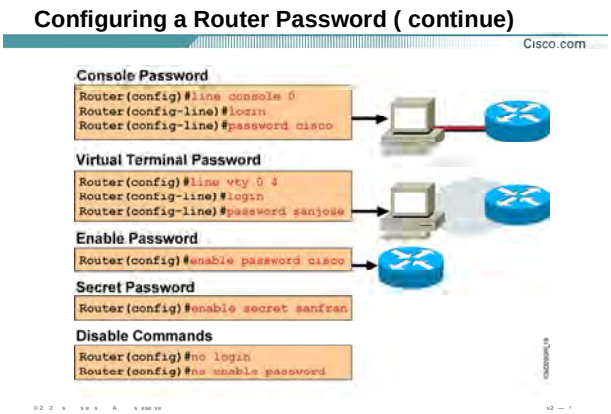
AUX Password:

همانطور که می دانید یکی دیگر از راه های برقراری ارتباط remote ، روش استفاده از پورت AUX می باشد . در این روش روتر را از طریق یک مودم به خط dial-up متصل شده است و دسترسی به صورت remote به آن امکان پذیر می باشد. Aux password ، پسوردی است که قبل از وارد شدن به user mode پرسید می شود .

Router(config)# line aux 0

Router(config-line)# login

Router(config-line)# password cisco



انواع پسورد و نحوه تنظیم کردن آنها (ادامه) :

Console password:

همانطور که گفته شد تنها راه ارتباط با روتر که بدون تنظیم می باشد استفاده از console port است. بنابراین بعد از انجام تنظیمات می توانید روتر را در یک جای ثابت قرار داده و از این به بعد آن را از طریق telnet یا Browser کردن تنظیم کنید.

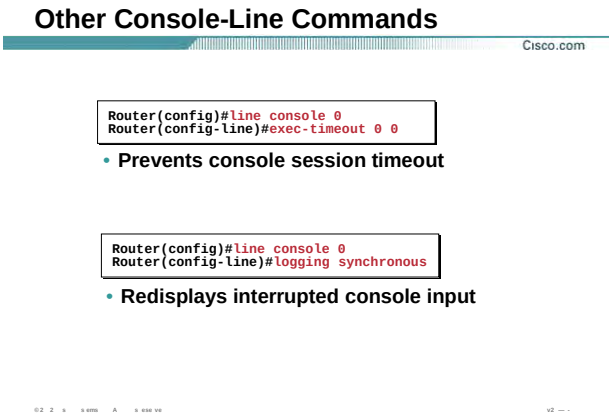
اما توجه داشته باشید که نداشتن پسورد و محدودیت دسترسی افراد برای admin دردسر ساز می شود.

Console Password ، پسوردی است که قبل از وارد شدن به User Mode پرسیده می شود و به صورت زیر تنظیم می شود .

Router(config)# line console 0

Router(config-line)# login

Router(config-line)# password Cisco

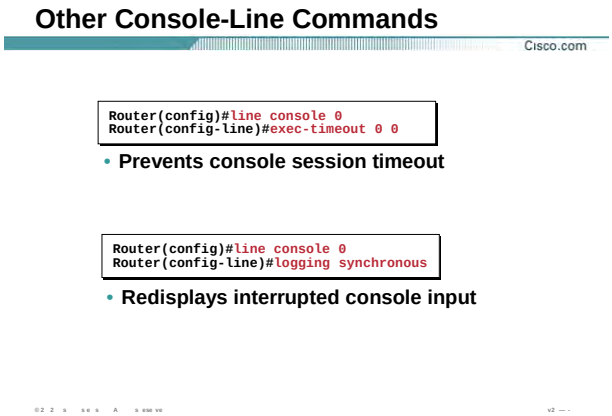


تنظیمات اضافی پورت Console :

تا به اینجا با اینترفیس console آشنا شدید . مدت زمان برقراری ارتباط console با روتر یا سوئیچ بدون قطع شدن این ارتباط به صورت پیش فرض ۱۰ دقیقه می باشد. به کمک دستور زیر می توانید مدت زمانی که این ارتباط برقرار می شود را به صورت نامحدود تعریف کنید. در واقع اگر packet ایی برای مدت زمان طولانی از این اینترفیس رد و بدل نشود این ارتباط قطع نخواهد شد.

Router(config)#line console 0

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

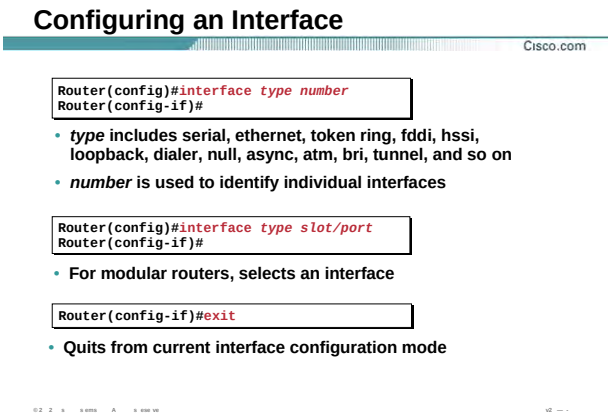


تنظیمات اضافی پورت Console :

یکی دیگر از مشکلاتی که ممکن است با آن مواجه شوید ،این است که شما فرمانی را در command prompt روتر یا سوئیچ وارد می کنید به طور مثال فرمان show run و منتظر نتیجه آن هستید در این لحظه پیام جدیدی مبنی بر اینکه یکی از اینترفیس ها up شده است ظاهر می شود . بنابراین نمی توانید تفاوت بین نتیجه فرمان خودتان و پیامی که ظاهر شده را متوجه شوید. به کمک فرمان زیر می توانید به روتر بگویید پیام جدید را بعد از خروجی فرمان شما نمایش دهد.

Router(config)#line console 0

Router(config-line)#logging synchronous



Interface Mode و تنظیم آن :

تا به اینجا با انواع راه های برقراری ارتباط با روتر آشنا شـدید . در واقـع ایـن ارتبـاط از طریـق اینتـرفیس هـا و پـورت هـای موجود بر روی روتر امکان پذیر می باشد.

به این نکته توجه داشته باشید که یکی از ملاکهای انتخاب روتر نوع و تعداد اینترفیس های آن می باشد.

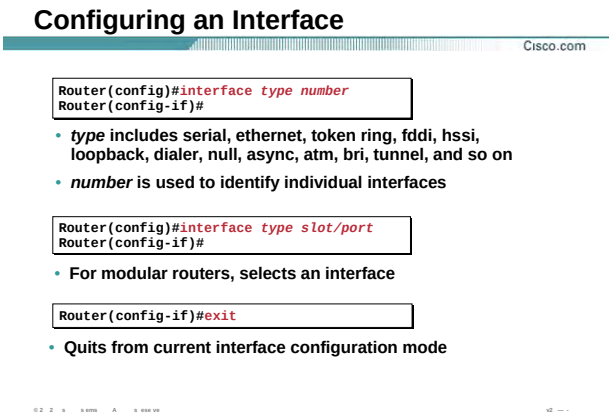
یک اینترفیس ممکن است روی روتر به صورت built-in نباشـد ، امـا از طرفـی روتـر مـی توانـد دارای تعـدادی slat خـالی باشد که می توانید ماژول مربوطه را خریداری کرده و در آن قرار دهید . بنابراین روترها از نظر نوع و تعداد اینترفیس هـای که ساپورت می کنند متفاوت می باشند .

برای اینکه یک اینترفیس را تنظیم کنید به طور مثـال بـه آن IP Address بدهیـد و یـا پهنـای بانـد آن را تغییـر بدهیـد مـی بایست ابتدا تغییر mode داده و وارد interface Mode شده و سپس تظیمات مربوط به آن اینترفیس را انجام دهید.

به کمک فرمان زیر می توان وارد اینترفیس مورد نظر شده و آن را تنظیم کرد .

Router(config)#interface type number

Router(config-if)#



Interface Mode و تنظیم آن (ادامه) :

توجه داشته باشید برای این کار باید نام انیترفیس و شماره آن را بدانید.به طور مثال می خواهید اینتریس serial با شماره ۱ را تنظیم کنید .ابتدا وارد global mode شده و سپس فرمان زیر را وارد کنید.

Router(config)#interface serial ۱

Router(config-if)#

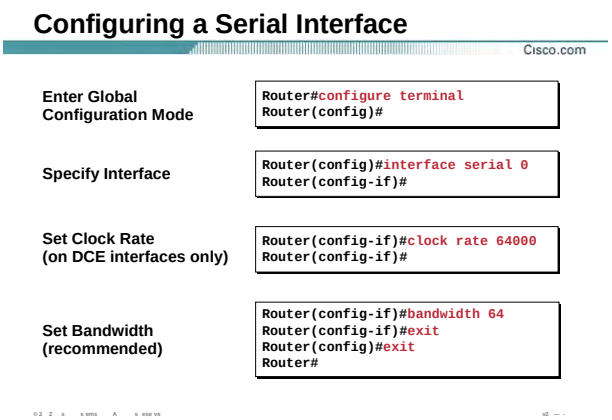
برای ماژول هایی که در slat های خالی قرار می گیرند نام گذاری به این صورت است که ابتدا باید نوع اینترفیس و سپس شماره slat و سپس شماره اینترفیس را وارد کنید.

به طور مثال فرض کنید در slat شماره ۰ دو پورت serial وجود داشته باشد، بنابراین برای صدا زدن آنها می گوییم serial 0/0 و یا serial 0/1.

برای خارج شدن از interface mode از فرمان Exit استفاده می شود .

Router(config-if)#exit

Router(config)#



Serial Interface و تنظیم آن :

به منظور برقراری ارتباط یک روتر با روتر دیگر به صورت Point-to-Point می توان از اینترفیس serial استفاده کرد .

بنابراین اتصال دو روتر به صورت نقطه به نقطه به صورت یکی از دو حالت زیر می باشد:

۱. back-to-back

۲. در دو محل جغرافیایی مختلف بوده و ارتباط آن دو با استفاده از خطوط مخابراتی صورت می گیرد.

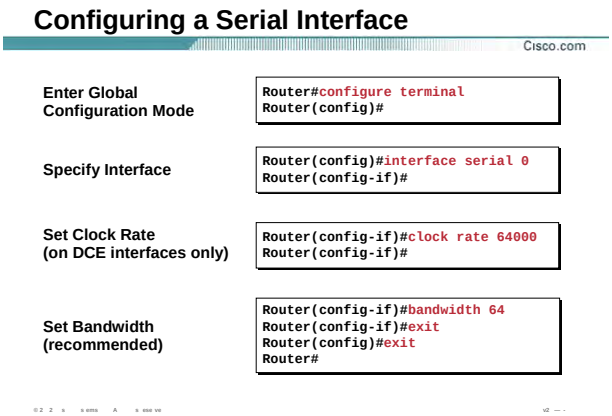
دو روتری که قرار است با هم ارتباط داشته باشند باید با نرخ یکسان ارسال و دریافت اطلاعات کنند.

در روترهایی که خطوط ارتباطی بستر مخابراتی می باشد ، مودم CSU/DSU کار تنظیم این نرخ را به صورت اتوماتیک انجام می دهند.

در صورتی که روترها را به صورت back-to-back به یکدیگر متصل کنید ، کابل های DTE/DCE این ارتباط را برقرار می کنند . در این حالت یک روتر به عنوان DTE و طرف دیگر DCE خواهد بود.

بنابراین لازم است که clock rate را روی اینترفیسی که به کابل DCE متصل شده است ، تنظیم کنید.

اما این سوال اینجا پیش می آید که اینترفیس کدام روتر نقش DTE و کدام یک DCE خواهد بود.



Serial Interface و تنظیم آن (ادامه):

به کمک فرمان زیر می توانید از DTE یا DCE بودن اینترفیس های Serial ،آگاه شوید.

Router> show controller serial 0

برای تنظیم کردن clock rate روی اینترفیس serial به صورت زیر عمل می کنید:

Router(config)#interface serial 0

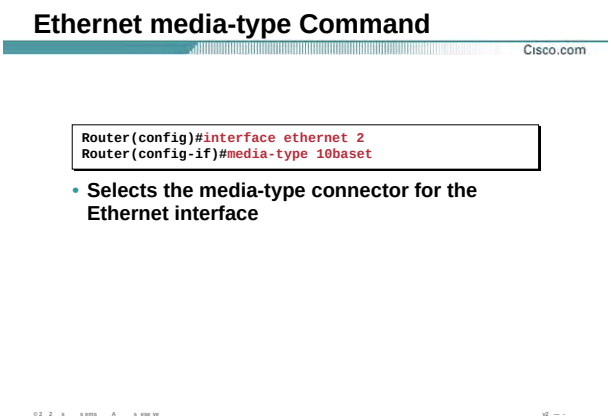
Router(config-if)#Clock rate 64000

Bandwidth یکی دیگر از ویژگیهای اینترفیس serial می باشد که می توانید آن را به کمک فرمان زیر تغییر دهید.

Router(config-if)#bandwidth 64

پهنای باند یکی از ملاکهای می باشد که در مبحث routing protocol ها کاربرد فراوانی دارد و ملاکی می باشد که در انتخاب بهترین مسیر نقش بسزایی را ایفا می کند . در مبحث routing با اهمیت این ملاک به خوبی آشنا خواهید شد.

نکته: اینترفیس serial به صورت پیش فرض دارای پهنای باند 1.544 Mbps می باشد.



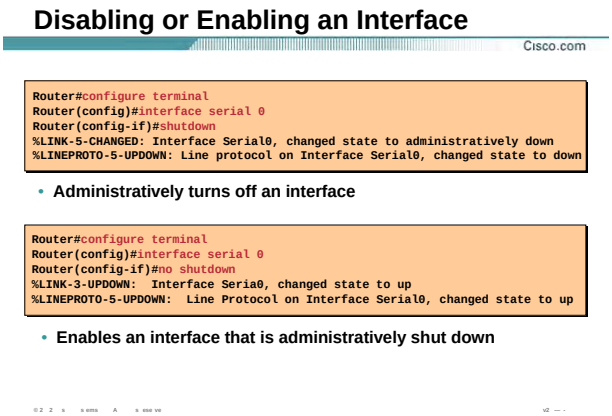
Interface Ethernet و Interface Fast Ethernet و نحوه تنظیمات آن :

یکی دیگر از انواع اینترفیس ها،اینترفیسهای Ethernet و Fast Ethernet هستند که کاربرد آن در اتصال روتر به شبکه LAN می باشد .

اینترفیس Ethernet با سرعت 10/100 Mbps کار می کند در حالی که Fast Ethernet با سرعت 10/100/1000 Mbps کار می کند و از هر دو برای ارتباط روتر به سوئیچ و در نتیجه به شبکه LAN استفاده می شود.

اینترفیس Ethernet با سرعت 10/100 Mbps کار می کند. این بدان معنی است که این اینترفیس می تواند هم با سرعت 10 کار کند و هم با سرعت 100 و اینکه با کدام سرعت کار کند درصورت تنظیم نکردن آن ، خود اینترفیس به صورت اتوماتیک تشخیص می دهد . اما شما می توانید این اینترفیس را طوری تنظیم کنید که فقط با سرعت 10 Mbps کار کند . برای این منظور وارد اینترفیس مربوطه شده و فرمان زیر را وارد می کنید.

Router(config-if)#media-type 10baset



فعال و غیرفعال کردن یک اینترفیس :

تمامی اینترفیس های روتر به صورت default غیرفعال (Shut Down) هستند.

بنابراین زمانی که بخواهید از یک اینترفیس استفاده کنید ابتدا می بایست آن را فعال کنید. برای این منظور وارد اینترفیس مربوطه شده و فرمان زیر را وارد می کنیم.

Router(config)#interface serial 0

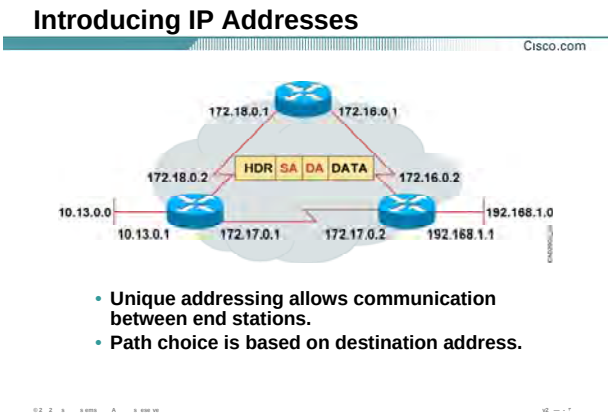
Router(config-if)#no shutdown

بعد از فعال کردن یک اینترفیس ، پیامی مبنی بر اینکه اینترفیس up شده و تغییر state داده است ظاهر می گردد.

بالعکس برای غیر فعال کردن اینترفیس به صورت دستی از فرمان زیر استفاده می کنیم:

Router(config-if)#shutdown

نکته: اینترفیسی که shutdown باشد هیچ گونه پکتی را ارسال و یا دریافت نمی کند.



معرفی IP Address :

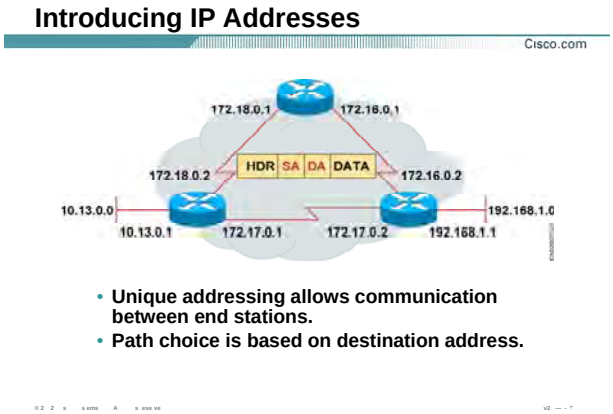
تا به اینجا با انواع اینترفیس ها و ویژگیهای مهم آنها مانند bandwidth و نحوه فعال کردن آنها روی یک اینترفیس آشنا شدید . درواقع تا به اینجا هر کدام از روترهٔ به تنهایی و مستقل از روترهای دیگر بررسی شده اند ، اما سوالی که اینجا مطرح می شود اینست ، چگونه روترها می توانند با هم ارتباط برقرار کنند؟

چگونه می توان به یک روتر از طریق یک شبکه و با استفاده از سرویس Telnet و بدون استفاده از پورت console ، ارتباط برقرار کرده و آن را تنظیم کرد؟

و یا به عبارتی علاوه بر فراهم آوردن بستر ارتباطی مناسب چه پارامترهای دیگری در ارتباط بین روترها نقش خواهد داشت .

یک پاسخ برای تمامی این سوالات وجود دارد و آن هم وجود پارامتری به نام آدرس ، که به کمک آن روترها همدیگر را شناخته و با یکدیگر ارتباط برقرار می کنند . این آدرس منحصربه فرد بوده و امکان دسترسی به تک تک عناصر شبکه را فراهم می کند . این شناسه منحصر به فرد در شبکه های مختلف متفاوت می باشد به طور مثال در شبکه TCP/IP ، این شناسه براساس پروتکل IP و یا پروتکل IPX خواهد بود .

بنابراین در یک شبکه تمامی عناصر شبکه دارای آدرسهای متفاوت ولی منحصر به فرد خو هند بود .



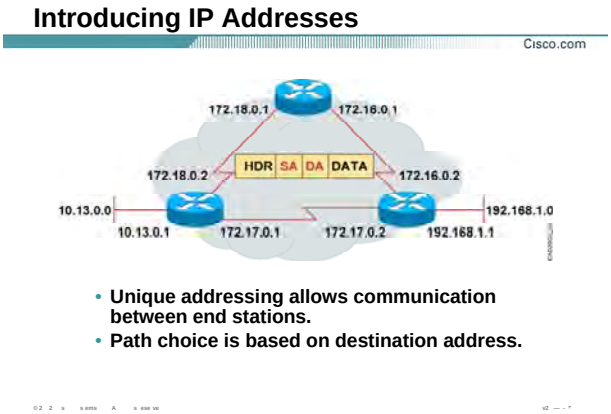
معرفی IP Address (ادامه) :

در واقـع هـر پکـت در شـبکه ماننـد نامـه ای اسـت کـه دارای آدرس فرسـتنده (source address) و آدرس گیرنـده (destination address) می باشد. همانطور که در ساختار شهری تمامی آدرس ها منحصر به فرد بوده و شما نمی توانید پلاک پستی یکسانی را برای دو خانه پیدا کنید ، IP Address ها نیز در شبکه از این ساختار پیروی کرده و منحصر به فرد خواهند بود .

زمانی که صحبت از منحصربه فرد بودن آدرسها پیش می آید ، بلافاصله مسئله نظارت و کنترل اهمیت پیدا می کند . امروزه در دنیا یک مرکز متصدی این امر می باشد.

در واقع **ICANN** (Internet Corporation Assigned Name and Number) وظیفه نظارت و مدیریت روی نام ها ، IP ها و پروتکل ها را به عهده دارد .

ICANN کره زمین را از نظر جغرافیایی به پنج ناحیه (Region) تقسیم بندی می کند و هر کدام از این region ها وظیفه دادن IP و نظارت و مدیریت روی هر کدام از آنها را به عهده خواهد داشت .



معرفی IP Address (ادامه):

این پنج ناحیه به شرح زیر می باشد:

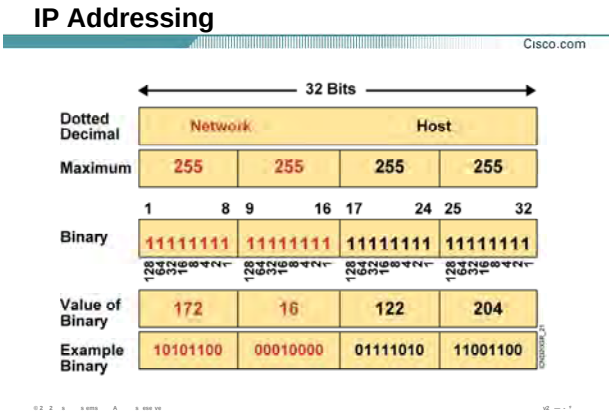
۱. RIP NCC : منطقه اروپا،خاورمیانه و آسیای مرکزی را تحت پوشش دارد.

۲. ARIN : منطقه امریکای شمالی را تحت پوشش دارد.

۳. APNIC : منطقه آسیای شرقی و اقیانوسیه را تحت پوشش دارد.

۴. AfriNIC : منطقه افریقا را تحت پوشش دارد.

۵. LACNIC : منطقه امریکای لاتین و جزایر کاریب را تحت پوشش دارد.



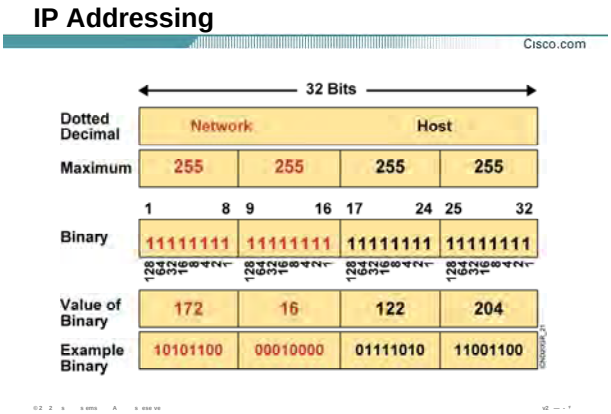
ساختار IP Address :

تا به اینجا با اهمیت آدرس دهی یکتا در شبکه آشنا شدید ، در ادامه با IP Address و ساختار این پروتکل و دسته بندی های متفاوت آن بیشتر آشنا خواهید شد.

IP V4 و یا به عبارتی IP Version 4 ، یک آدرس ۳۲ بیتی می باشد . این آدرس از چهار قسمت (octet) تشکیل شده است و به هر قسمت یک Octet گفته می شود که ۸ بیت می باشد.

درصورتی که در یک octet یک بیت دارای مقدار یک و بقیه بیتها مقدار صفر داشته باشند ، و یا به عبارتی هفت بیت با مقدار ۱ و یک بیت با مقدار صفر موجود باشد ، متناسب با جایگاه آن بیتی که دارای مقدار یک می باشد ، مقدار Octet در مبنای ده می تواند مقادیر ۱۲۸ ، ۶۴ ، ۳۲ ، ۱۶ ، ۸ ، ۴ ، ۲ و ۱ به خود بگیرد .

همانطور که گفته شد IP Address یک آدرس ۳۲ بیتی و دارای چهار قسمت می باشد . هر قسمت می تواند عددی در رنج ۰ تا ۲۵۵ باشد. همانطور که در شکل می بینید IP Address از دو بخش اصلی تشکیل شده است : بخش اول network و بخش دوم host .



ساختار IP Address (ادامه):

سوالی که پیش می آید اینست که هر کدام از آنها چیستند و محدوده آنها چگونه تعیین می شود ؟

Network ID: بخش اول یا همان Network ، مشخصه یک شبکه است. بنابراین این قسمت در تمام station های موجود در یک شبکه یکسان خواهد بود .

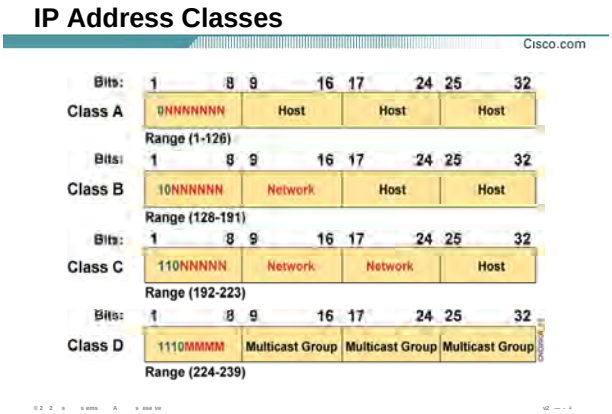
به طور مثال فرض کنید در یک شبکه station ها هر کدام دارای یک IP Address در رنج 172.16.1.1 تا 172.16.255.254 باشد. در این حالت network یا همان مشخصه شبکه ، 172.16.0.0می باشد . زیرا دو قسمت اول در تمامی آدرسها یکسان بوده و تغییر نکرده است.

Host ID: این بخش تمایز بین IP Address را نشان می دهد. بنابراین در یک شبکه با network ID یکسان، تمایز IP Address ها توسط بخش دوم آدرس IP یا همان Host ID صورت می گیرد .

سوالی که اینجا مطرح می شود این است که طول network ID و Host ID چقدر است؟

این اندازه متغیر است و این متغیر بودن ، به کلاس IP Address ها بستگی دارد.

یعنی ممکن است که network ID یک یا دو یا سه octet باشد و host ID نیز متناسب با اندازه Network ID تغییر خواهد کرد.



کلاسهای مختلف IP :

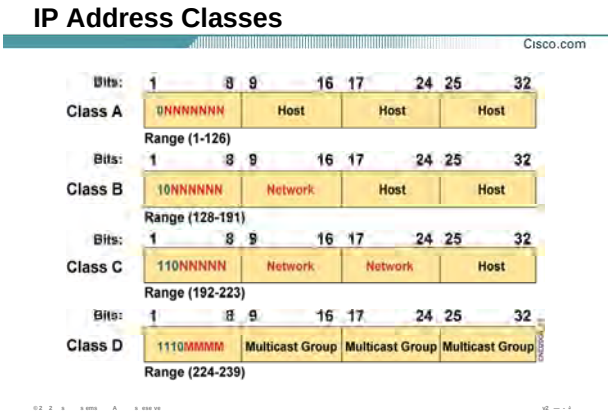
سوالی که مطرح می شود اینست که کلاس IP چیست ؟

در یک IP Address بخش (octet) اول از سمت چپ مهم ترین نقش را در تعیین نوع کلاس بازی می کند و مقادیر مختلفی که این بخش به خود می گیرد می تواند به دسته بندی های مختلفی منجر شود.

به طور استاندارد ۴ دسته IP Address وجود دارد که به صورت فعال از آن استفاده می شود . این دسته بندی به شرح زیر می باشد :

۱. **Class A**
۲. **Class B**
۳. **Class C**
۴. **Class D**

Class A : در این کلاس بیت اول از octet اول دارای مقدار صفر می باشد. بنابراین مقادیری که این octet در مبنای ده می تواند به خود بگیرد عددی در رنج ۱ تا ۱۲۶ خواهد بود.



کلاسهای مختلف IP (ادامه) :

بنابراین در تمامی IP Address هایی که در رنج کلاس A هستند ، octet اول نقش network ID و سه octet آخر نقش Host ID را بازی می کند.

Network ID ، مشخصه یک رنج IP address ایی می باشد که در یک network قرار دارند.

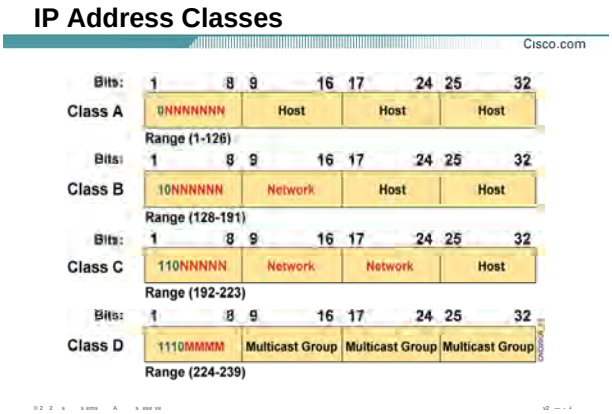
فرض کنید در یک network ، station ها IP Address های خود را از رنج 10.0.0.1 الی 10.255.255.254 انتخاب کرده باشند. بنابراین اگر بخواهیم یک مشخصه برای تمای این IP Address ها معرفی کنیم که نماینده و معرفی کننده تمامی آنها باشد چه کاری باید کرد؟

همانطور که می بینید octet اول در تمامی آنها ثابت بوده و بقیه octet ها متغیر هستند. بنابراین بخش ثابت را آورده و به ازای قسمتهای متغییر مقدار صفر قرار می دهیم.

بنابراین octet ثابت به عنوان network و قسمتهایی که متغییر هستند به عنوان host انتخاب می شوند.

در این مثال network ID ، 10.0.0.0 می باشد .

بنابراین به صورت کلی می توان گفت که در تمامی IP Address هایی که در رنج کلاس A هستند، octet اول نقش network ID و سه تا octet آخر نقش Host ID را بازی می کند.



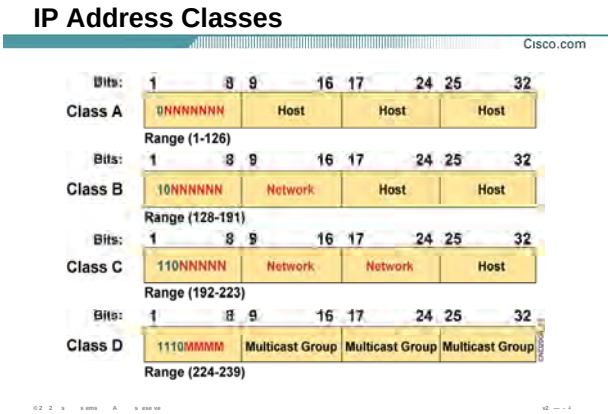
کلاسهای مختلف IP (ادامه) :

Class B : در این کلاس، در octet اول، بیت اول دارای مقدار یک و بیت دوم دارای مقدار صفر می باشد. بنابراین مقادیری که این octet در مبنای ده می تواند به خود بگیرد عددی در رنج ۱۲۸ تا ۱۹۱ می باشد.

از طرفی در تمامی IP Address هایی که در رنج کلاس B هستند ،دو تا octet اول نقش network ID و دو تا octet دوم نقش Host ID را بازی می کند.

Class C : در این کلاس، در octet اول، بیت اول و دوم دارای مقدار یک و بیت سوم دارای مقدار صفر می باشد. بنابراین مقادیری که این octet در مبنای ده می تواند به خود بگیرد عددی در رنج ۱۹۲ تا ۲۲۳ می باشد.

ازطرفی در تمامی IP Address هایی که در رنج کلاس C هستند ، سه تا octet اول نقش network ID و octet آخر نقش Host ID را بازی می کند.



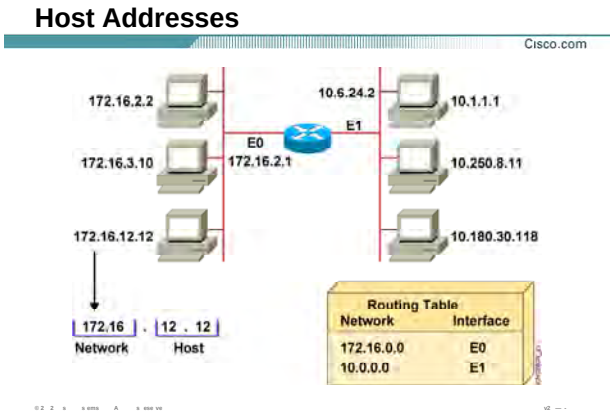
کلاسهای مختلف IP (ادامه):

Class D : در این کلاس، در octet اول، بیت اول و دوم و سوم دارای مقدار یک و بیت چهارم دارای مقدار صفر می باشد. بنابراین مقادیری که این octet در مبنای ده می تواند به خود بگیرد عددی در رنج ۲۲۴ تا ۲۳۹ می باشد.

از این کلاس برای انجام عملیات multicasting در شبکه استفاده می شود. در واقع اگر بخواهید پکت خاصی را در شبکه پخش کنید به طوری که آن دسته از station هایی که مورد نظر شما هستند این پکت را دریافت کنند ، می بایست آدرس مقصد آن را یک آدرس در رنج کلاس D قرار دهید .نگران کاربرد این کلاس نباشید و با آن در مباحث Routing آشنا می شویید . درضمن در این کلاس به سه octet آخر multicast Group نیز گفته می شود.

نکته : یک دسته کلاس به نام class D نیز در دسته بندی ها آورده می شود ولی این کلاس از آنجایی که هنوز به صورت جهانی از آن استفاده نمی شود و کاربرد خاصی نیز ندارد در معرفی کلاس های فعال گفته نخواهد شد .

به کلاس A و کلاس B توجه کنید و به رنج مقایری که octet اول به خود گرفته است دقت کنید. همانطور که مشاهده می کنید عدد ۱۲۷ در هیچ یک از کلاسها گنجانده نشده است. این عدد برای کار خاصی رزرو شده است.آدرس 127.0.0.1 که به آنloopback Address نیز گفته می شود در هیچ یک از دو کلاس A و B گنجانده نمی شود و یک آدرس رزرو شده است که جهت تست کارت شبکه از آن استفاده می شود.



:Host Address

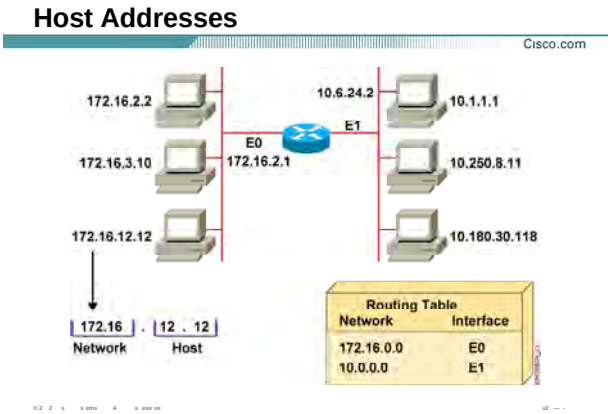
به شکل فوق توجه کنید. دو شبکه با رنج IP Address متفاوت وجود دارد.

در سمت راست یک شبکه با رنج IP کلاس A و در طرف دیگر کلاس B وجود دارد.

و به هر کدام از station ها یک IP Address منحصر به فرد نسبت داده شده است.

همانطور که مشاهده می کنید در شبکه سمت راست octet اول ثابت و بقیه octet ها متغییر هستند ، بنابراین network ID این شبکه 10.0.0.0 خواهد بود.در سمت چپ نیز 172.16.0.0 به عنوان مشخصه تمامی IP address های موجود در شبکه می باشد. از طرفی تمامی station هایی که دارای network ID یکسانی هستند می توانند همدیگر را ببینند . به طور مثال station ایی با آدرس 172.16.2.2 می توانند براحتی با station ایی با آدرس 172.16.12.12 تبادل اطلاعات کند. فرض کنید که station با آدرس 172.16.2.2 بخواهد پکتی را به خارج از شبکه خود و به station ایی با آدرس 10.1.1.1 بفرستد. چگونه این انتقال صورت می گیرد؟در واقع چگونه می توان چندین شبکه ای که هر کدام در رنج های مختلف IP هستند با یکدیگر ارتباط برقرار کنند ؟

پاسخ به این سوال ، عملیات Routing می باشد . یعنی جهت دادن به پکتهایی که مقصد آنها شبکه محلی نیست و می بایست به سمت شبکه دیگری هدایت شود . روتر این وظیفه را به خوبی انجام می دهد. درواقع روتر هم شبکه



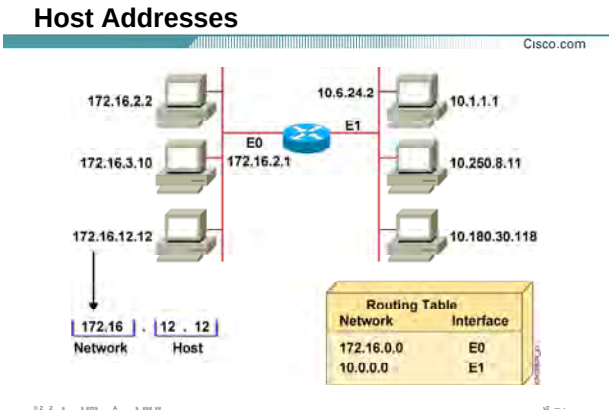
Ho t Address (ادامه):

مبداء و هم شبکه مقصد را به خوبی می شناسد . بنابراین درخواستی که به آن وارد می شود را براحتی به سمت شبکه مقصد هدایت می کند ا ن کار به کمک تعریف یک الگوریتم مسیریابی و فعال کردن آن روی روتر امکان پذیر می باشد . درنهایت روتر به کمک این الگوریتم Table ایی که شامل رکوردهایی براساس شبکه های مختلف و راههای دسترسی به هر کدام از آنها می باشد را ساخته و عملیات مسیریابی را انجام می دهد.

این table شامل اطلاعات زیر می باشد:

۱. Network ID شبکه هایی که به روتر به صورت مستقیم تصل هستند. در این مثال دو شبکه با network ID ، 172.16.0.0 و 10.0.0.0 به روتر متصل هستند.

۲. network ID شبکه هایی که به روتر های دیگر به صورت مستقیم مت ل هستند و این روتر این شبکه ها را از طریق دیگران شناخته است . در مباحث آتی متوجه می شوید که روتر چگونه اطلاعات روتر های دیگر را دریافت کرده و سپس آنها را در routing table خود درج می کند .



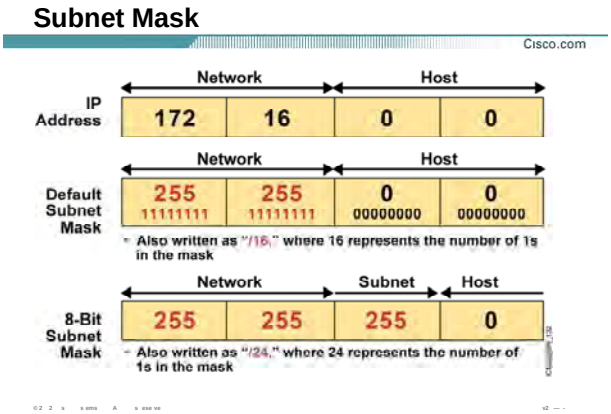
Host Address (ادامه):

۳. اینترفیس هایی که به کمک آنها به شبکه های connect و یا غیر connect دسترسی پیدا می کند. با توجه به شکل، روتر به کمک اینترفیس E0 به شبکه با آدرس 172.16.0.0 و به کمک اینترفیس E1 به شبکه با آدرس 10.0.0.0 دسترسی پیدا می کند.

در مبحث Routing با نحوه پرشدن Routing Table و همچنین نحوه شناخت از شبکه های غیرمحلی بیشتر آشنا می شوید .

تا به اینجا با IP Address و ساختار آن آشنا شدید . در هر کدام از کلاسها ما بخشی را به عنوان Network ID و بخشی را به عنوان Host ID در نظر گرفتیم بدون اینکه بگوییم این تفکیک براساس چه ملاکی صورت گرفته است . سوالی که مطرح می شود اینست که چگونه و با چه ملاکی این کار صورت گرفت .

پاسخ به این سوال Subnet mask می باشد . در واقع به کمک Subnet mask می توان این دو قسمت را از یکدیگر تفکیک کرد .



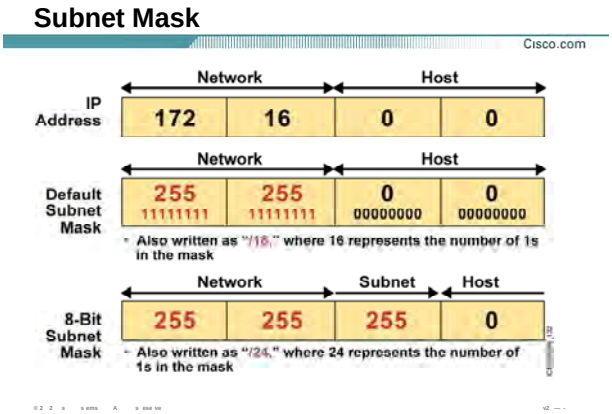
:Subnet mask

Subnet Mask مشخصه ای است که تمایز بین دو بخش Network و host را در IP Address مشخص می کند . یک station به کمک subnet mask می تواند Network ID و Host ID را از یکدیگر تشخیص دهد. در واقع Subnet mask ، یک رشته ۳۲ بیتی می باشد که از چپ به راست شامل دنباله متوالی از بیتهایی با مقدار یک و سپس یک دنباله متوالی از بیتهایی با مقدار صفر می باشد. بنابراین در subnet mask قسمت هایی که دارای مقدار یک هستند بخش network و قسمتهایی که دارای مقدار صفر هستند بخش host را مشخص می کنند.subnet mask به صورت default برای کلاسهای IP به صورت زیر خواهد بود:

Class A: همانطور که با کلاس A آشنا شدید، octet اول مشخص کننده network و سه octet آخر مشخص کننده host می باشد. این بدان معنی است که در subnet mask بیتهای که در Octet اول قرار دارند مقدار یک و بقیه بیتها مقدار صفر خواهند داشت . بنابراین subnet mask در مبنای ۲ و در مبنای ۱۰ به صورت زیر خواهد بود:

Binary: 11111111.00000000.00000000.00000000

Decimal: 255.0.0.0



Subnet mask (ادامه):

Class B: همانطور که می دانید در این کلاس دو octet اول مشخص کننده network و دو octet آخر مشخص کننده host می باشد. بنابراین subnet mask به صورت default برای این کلاس به صورت زیر خواهد بود:

Binary: 11111111.11111111.00000000.00000000

Decimal: 255.255.0.0

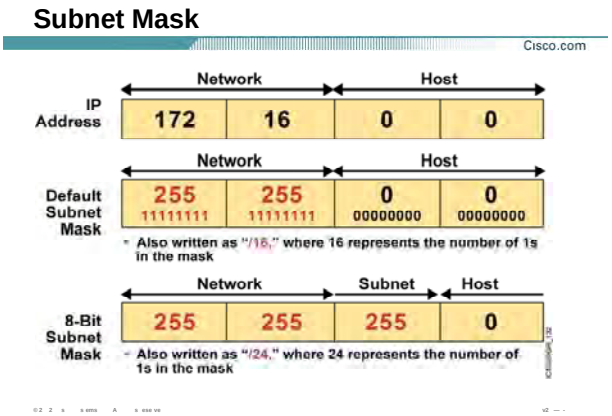
Class C: همانطور که می دانید در این کلاس سه تا octet اول مشخص کننده network و octet آخر مشخص کننده host می باشد. بنابراین subnet mask به صورت default برای این کلاس به صورت زیر خواهد بود :

Binary: 11111111.11111111.11111111.00000000

Decimal: 255.255.255.0

تا به اینجا با ساختار subnet mask به صورت پیش فرض برای هر کدام از کلاس ها آشنا شدید.

فرض کنید IP Address مربوط به یک station را داشته باشید و بخواهید به کمک subnet mask ، network ID آن را تشخیص دهید .



Subnet mask (ادامه):

به طور مثال فرض کنید IP Address مربوط به یک station ، 172.16.12.12 و subnet mask مربوط به آن نیز 255.255.0.0 باشد ، بنابراین به کمک subnet mask می توان تشخیص داد که network ID مربوط به آن 172.16.0.0 می باشد.

:Prefix Notation

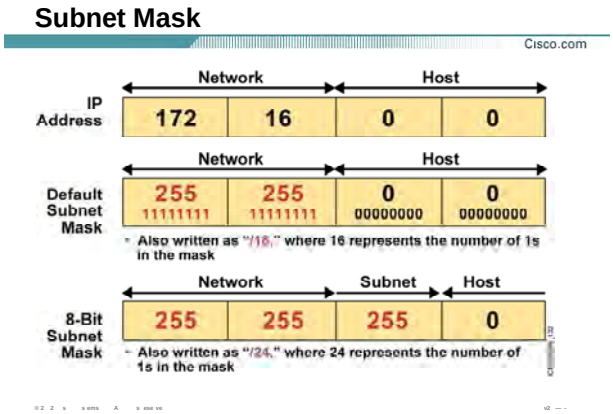
تا به اینجا با فرمتهای نمایش subnet mask آشنا شدید ، نمایش در مبنای دو و نمایش در مبنای ده.

به طور مثال نمایش subnet mask برای IP Address های کلاس A به صورت زیر می باشد :

Binary: 11111111.00000000.00000000.00000000

Decimal: 255.0.0.0

همانطور که متوجه شدید subnet mask جدا کننده دو بخش network و host می باشد. بنابراین به دنبال قرار گرفتن یک دنباله متوالی از بیتهایی با مقدار یک ، یک دنباله بیت با مقدار صفر خواهیم داشت که نشان دهنده قسمت host هستند.



Subnet mask (ادامه):

لذا می توانیم یک نماد دیگر را برای subnet mask ارائه دهیم . در این فرمت تعداد بیتهای یک را شمرده و subnet mask را به کمک آن نمایش دهیم .

به طور مثال نمایش subnet mask برای IP Address های کلاس A به صورت استاندارد ، (/8) خواهد بود. زیرا Octet اول نشان دهنده Network و سه Octet آخر نشان دهنده Host می باشد .بنابراین تعداد هشت بیت نشان دهنده قسمت Network خواهد بود .

به صورت کلی می توان نمایش Subnetmask ، برای کلاس های A ، B و C را به ترتیب /8 ، /16 و /24 معرفی کرد.

Decimal Equivalents of Bit Patterns

Cisco.com

128	64	32	16	8	4	2	1		
0	0	0	0	0	0	0	0	=	0
1	0	0	0	0	0	0	0	=	128
1	1	0	0	0	0	0	0	=	192
1	1	1	0	0	0	0	0	=	224
1	1	1	1	0	0	0	0	=	240
1	1	1	1	1	0	0	0	=	248
1	1	1	1	1	1	0	0	=	252
1	1	1	1	1	1	1	0	=	254
1	1	1	1	1	1	1	1	=	255

اعداد کلیدی و مجموع بیتها از چپ به راست:

این جدول و یادگیری آن به شما در مبحث Subnetting و همچنین تبدیل Binary به Decimal کمک بسیاری می کند .

همانطور که می دانید هر Octet شامل هشت بیت می باشد بطوریکه هر کدام از بیتها می توانند مقدار یک یا صفر به خود بگیرند .

ما برای اینکار دو کلید تعریف می کنیم :

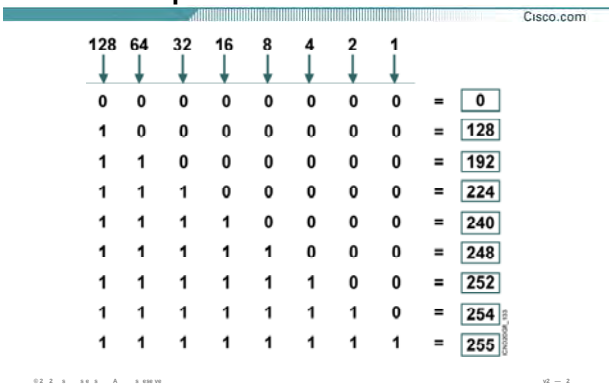
۱. مجموع بیتها از چپ به راست

۲. مجموع بیتها از راست به چپ

مجموع بیتها از چپ به راست :

همانطور که روی شکل مشاهده می کنید ، هشت حالت با قرار گرفتن یک و صفرهای ایجاد کرده ایم که درآن یک و صفرها به صورت متوالی پشت سر هم قرارگرفته اند (این به معنی تمامی حالتهایی که با یک و صفر می توان ایجاد کرد نمی باشد).

Decimal Equivalents of Bit Patterns



اعداد کلیدی و مجموع بیتها از چپ به راست (ادامه):

مقدار صفر : درحالتی که تمامی بیتها یک Octet صفر باشند ، مقداری که به Octet در مبنای ده می توان نسبت داد مقدار صفر می باشد .

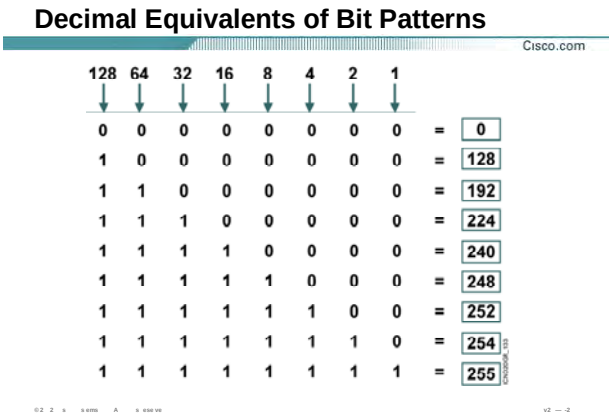
مقدار ۱۲۸ : درحالتی که بیت هشتم از هر Octet مقدار یک و بقیه بیتها مقدار صفر داشته باشند ، مقداری که به Octet در مبنای ده می توان نسبت داد مقدار ۱۲۸ می باشد .

مقدار ۱۹۲ : درحالتی که دو بیت اول (بیت هشتم و هفتم) از هر Octet مقدار یک و بقیه بیتها مقدار صفر داشته باشند ، مقداری که به Octet در مبنای ده می توان نسبت داد مقدار ۱۹۲ می باشد .

مقدار ۲۲۴ : درحالتی که سه بیت اول از هر Octet مقدار یک و بقیه بیتها مقدار صفر داشته باشند ، مقداری که به Octet در مبنای ده می توان نسبت داد مقدار ۲۲۴ می باشد .

مقدار ۲۴۰ : درحالتی که چهار بیت اول از هر Octet مقدار یک و بقیه بیتها مقدار صفر داشته باشند ، مقداری که به Octet در مبنای ده می توان نسبت داد مقدار ۲۴۰ می باشد .

مقدار ۲۴۸ : درحالتی که پنج بیت اول از هر Octet مقدار یک و بقیه بیتها مقدار صفر داشته باشند ، مقداری که به Octet در مبنای ده می توان نسبت داد مقدار ۲۴۸ می باشد .



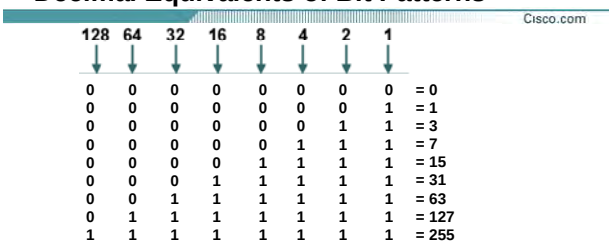
اعداد کلیدی و مجموع بیتها از چپ به راست (ادامه):

مقدار ۲۵۲ : درحالتی که شش بیت اول از هر Octet مقدار یک و بقیه بیتها مقدار صفر داشته باشند ، مقداری که به Octet در مبنای ده می توان نسبت داد مقدار ۲۵۲ می باشد .

مقدار ۲۵۴ : درحالتی که هفت بیت اول از هر Octet مقدار یک و بقیه بیتها مقدار صفر داشته باشند ، مقداری که به Octet در مبنای ده می توان نسبت داد مقدار ۲۵۴ سمی باشد .

مقدار ۲۵۵ : درحالتی که تمامی بیتها از هر Octet مقدار یک داشته باشند ، مقداری که به Octet در مبنای ده می توان نسبت داد مقدار ۲۵۵ می باشد .

Decimal Equivalents of Bit Patterns



اعداد کلیدی و مجموع بیتها از راست به چپ :

در صورتی که محاسبات را از سمت راست به چپ انجام دهیم همانند جدول فوق اعدادی حاصل می شود که در محاسبات Subnetting به شما کمک بسیاری خواهند کرد.

:Subnet

همانطور که متوجه شدید subnet mask جدا کننده دو بخش network و host می باشد. بنابراین به دنبال قرار گرفتن یک دنباله بیت با مقدار یک ، یک دنباله بیت با مقدار صفر خواهیم داشت . بیتهایی که دارای مقدار یک هستند نشان دهنده بخش Network و بیتهایی که دارای مقدار صفر هستند نشان دهنده بخش host خواهند بود.

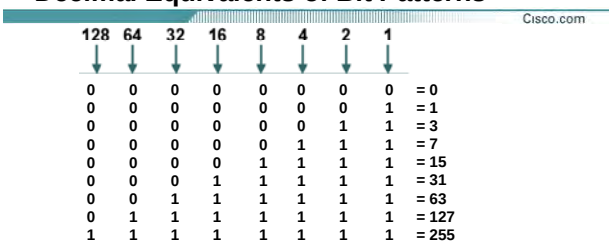
همانطور که می دانید بیتهایی که نشان دهنده Host در IP Address هستند ، می توانند تغییر کنند و با تغییر مقدار آنها آدرسهای جدیدی ایجاد خواهند شد . به عبارتی دیگر ، بیتهایی که دارای مقدار صفر در Subnet mask هستند ، اجازه تغییر مقدار بیتهای متناظر در IP Address را خواهند داد .

به طور مثال به network ID با subnet mask زیر توجه کنید:

Network ID: 192.168.1.0

Subnet mask: 111111111.11111111.11111111.000000000

Decimal Equivalents of Bit Patterns



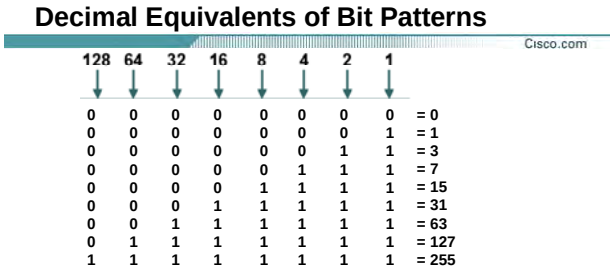
اعداد کلیدی و مجموع بیتها از راست به چپ (ادامه):

چون هشت بیت آخر در subnet mask دارای مقدار صفر می باشد ، بنابراین به ازای هر بیت صفر از subnet mask ، بیت متناظر در IP Address می تواند دارای مقدار یک یا صفر باشد. درنتیجه با تغییر مقدار این بیتها می توان IP Address های متفاوتی را بدست آورد.

به طور مثال اگر بیت اول از octet چهارم از subnet mask مقدار ۱ و بقیه بیت ها از این octet صفر باشد ، در این صورت متناظر با آن آدرس 192.168.1.128 را خواهیم اشت و یا به طـ ر مثال اگر بیت اول از octet چهارم در Subnet mask دارای مقدار صفر و بقیه بیتها از این octet دارای مقدار یک باشند، در ا ن صورت متناظر با آن آدرس 192.168.1.127 را خواهیم داشت.

بنابراین به کمک subnet mask می توان دید کدام بیتها در IP Address می تواند قدار یک و یا صفر به خود بگیرد و منجر به ایجاد IP Address های متفاوتی شوند.

درواقع اگر وارد قسمت بیتهای host در Subnet mask شده و تعدادی از بیتهای آن را تغییر مقدار دهیم ، یعنی مقدار صفر آنها را به مقدار یک تبدیل کنیم ، در این صورت ما اجازه تغییر مقدار بیتهای متناظر در IP Address را خواهیم داشت . درنتیجه بیتهای کمتری به عنوان بیت host معرفی شده و در تعیین IP Address های متفاوت نقش خواهند داشت .



اعداد کلیدی و مجموع بیتها از راست به چپ (ادامه):

بیتهایی که از بخش host در Subnet mask قرض گرفته می شوند به عنوان بیت subnet معرفی شـده و مقـدار آنهـا از صفر به یک تبدیل می شود.

به این نکته توجه کنید در صورتی که ما به صورت استاندارد کار کنیم ، یک network و تعدادی host خواهیم داشت .

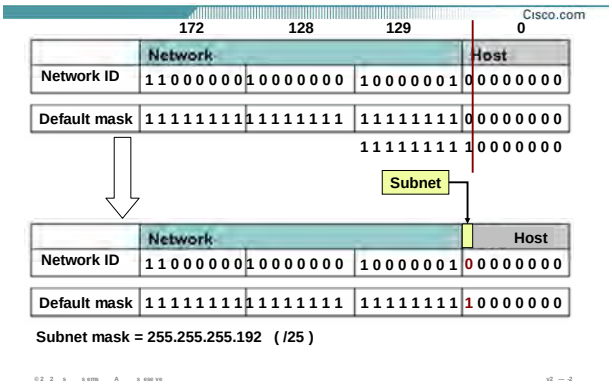
به طور مثال به network ID با subnet mask زیر توجه کنید:

Network ID: 192.168.1.0

Subnet mask: 111111111.11111111.11111111.00000000

در ادامه این درس با نحوه Subnetting در یک شبکه بیشتر آشنا می شوید .

divide network 192.128.129.0 to 2 networks



معرفی Subnetting در یک مثال:

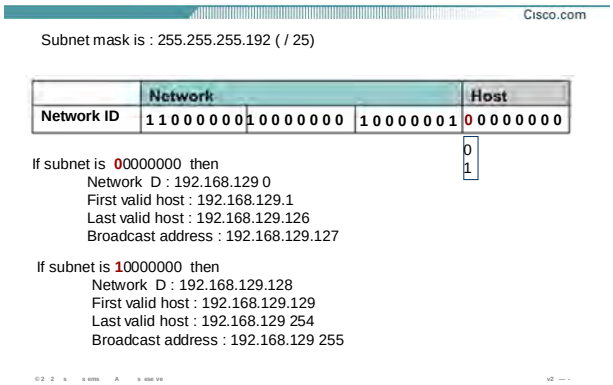
به شکل فوق توجه کنید . در این مثال network Address با subnet mask زیر آورده شده است :

Network ID: 192.168.1.0

Subnet mask: 111111111.11111111.11111111.100000000

همانطور که مشاهده می کنید به اندازه یک بیت به سمت Host پیشروی کرده ایم. درواقع به اندازه یک بیت از بخش host قرض گرفته شده و مقدار آن از صفر به یک تبدیل شده است .بنابراین تعداد بیتهای بخش Host هفت بیت و یک بیت به عنوان بیت subnet انتخاب می شود.

divide network 192.128.129.0 to 2 networks



معرفی Subnetting در یک مثال (ادامه):

تعداد بیتهای بخش subnet به اندازه یک بیت می باشد و تعداد حالتهایی که یک بیت می تواند داشته باشد دو حالت است، یک و صفر .

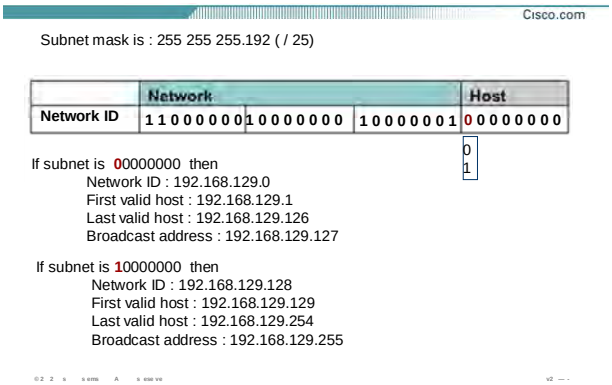
بنابراین به کمک تعداد بیتهای subnet می توان تعداد network های ایجاد شده را تشخیص داد . در این مثال یک network با 256 عدد آدرس به دو network ، هر کدام با تعداد ۱۲۸ عدد آدرس تبدیل شده است.

دراین مثال بیت هشتم از Octet چهارم می تواند هم مقدار یک و هم مقدار صفر بگیرد، بنابراین با توجه به مقادیر یک و صفری که بیت هشتم می تواند به خود گیرد، دو حالت زیر را خواهیم داشت :

صفر:

بیت هشتم صفر و هفت بیت دیگر می توانند مقدار یک و صفر به خود بگیرند ، بنابراین رنج IP address ایی که می توانیم داشته باشیم با احتساب صفر بودن بیت هشتم ، 192.168.1.1 الی 192.168.1.127 خواهد بود. در این حالت network ID تغییر نکرده و همان 192.168.1.0 خواهد بود با این تفاوت که رنج IP Address ها تغییر کرده است.

divide network 192.128.129.0 to 2 networks



معرفی Subnetting در یک مثال (ادامه):

یک :

بیت هشتم یک و هفت بیت دیگر می توانند مقدار یک و صفر به خود بگیرند ، بنابراین رنج IP address ایی که با شرایط جدید می توانیم داشته باشیم با احتساب یک بودن بیت هشتم ، 192.168.1.129 الی 192.168.1.254 خواهد بود.

سوالی که مطرح می شود اینست که network Address در این حالت چه خواهد بود؟

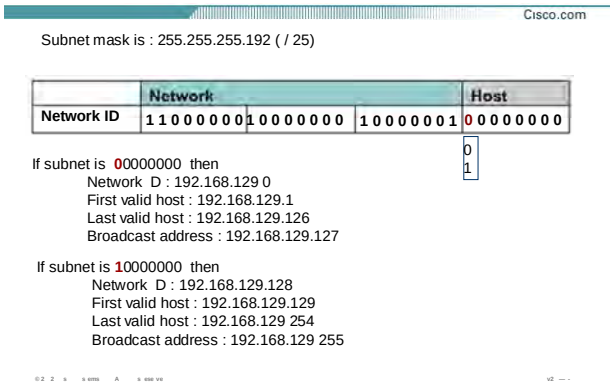
همانطور که می دانید برای تعیین Network Address می بایست در IP Address ، بیتهایی که نشان دهنده Host هستند مقدار صفر بگیرند . لذا network Address با احتساب یک بودن بیت هشتم ، 192.168.1.128 خواهد بود.

و تعداد IP Address هایی که می توان در این شبکه استفاده کرد با حذف کردن حالتهای مربوط به Network Address و Broadcast Address ، 126 آدرس خواهد بود .

بنابراین در این مثال با استفاده از subnetting یک network به دو تا network تبدیل شده و از طرفی با شکسته شدن network ها تعداد host ها نیز تقسیم شده و در هر Network تعداد 126 عدد host وجود خواهد داشت.

تا به اینجا با subnet و نحوه ایجاد آن تا حدودی آشنا شدید.

divide network 192.128.129.0 to 2 networks



معرفی Subnetting در یک مثال (ادامه):

اما سوالی که اینجا مطرح می شود اینست که چه ضرورتی برای انجام این کار وجود دارد و این روش چه مزایایی را به همراه خواهد داشت؟

سه علت عمده زیر این ضرورت را نشان می دهند :

۱. کاهش ترافیک و افزایش کارایی شبکه.

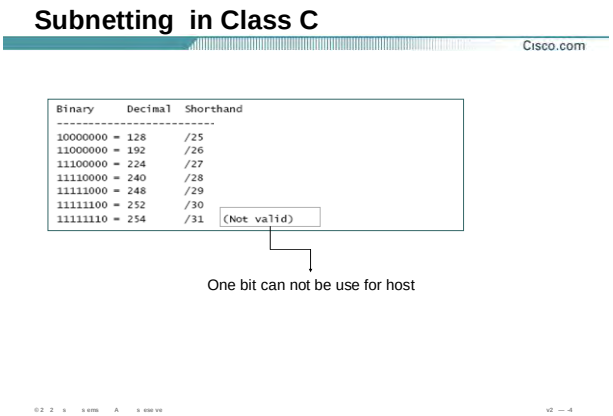
۲. افزایش توان مدیریتی روی شبکه و در نتیجه اشکال زدایی راحتر.

۳. کوچک شدن اندازه Routing table و درنتیجه بالا رفتن سرعت Convergence شبکه .

لازم به ذکراست ، دلایل دیگری نیز موجود می باشد و از آنجایی که آوردن این دلایل نیاز به دانش بیشتری دارد لذا بحث بیشتر در مورد این موضوع به سطوح بالاتر در Cisco واگذار می شود .

بنابراین با شکستن شبکه به چندین زیرشبکه ، تعداد host ها در یک شبکه کم شده و در نتیجه مدیریت و اشکال زدایی روی این شبکه راحتر می شود.

از طرفی ترافیک به صورت محلی در می آید ، درنتیجه broad cast های یک زیرشبکه روی زیرشبکه دیگر تأثیری نخواهد گذاشت .



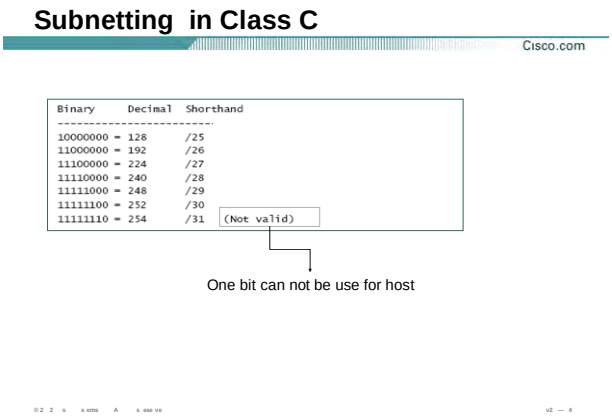
Subnetting در کلاس C:

تا به اینجا با مفهوم Subnetting در یک شبکه آشنا شدید . در Subnetting در هر کلاسی که باشید همیشه از سمت چپ به راست روی بیتها حرکت خواهید کرد. یعنی همیشه تعدادی بیت از سمت راست قرض گرفته می شود و به سمت چپ اضافی می شود .

بنابراین می توان بررسی کرد در هر کلاس به ازای هر بیت قرض گرفته شده چه Subnet mask و چه Network های جدیدی بوجود می آید .

جدول فوق لیست حالتهای ممکنه روی Subnet mask را نشان می دهد . به طور مثال در کلاس C درصورتی که تعداد بیتهای قرض گرفته شده به اندازه یک بیت باشد ، در این حالت Subnet mask جدید 25/ خواهد شد و در تناظر با آن در IP Address فقط هفت بیت به عنوان بیتهای Host انتخاب شده و در تعیین رنج IP Address نقش خواهند داشت .

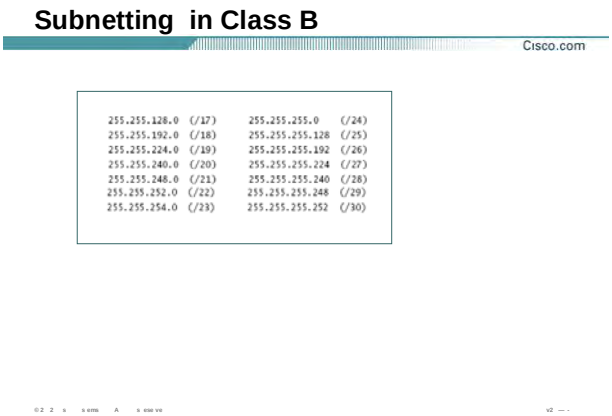
در کلاس c درصورتی کهsubnet mask به صورت 30/ باشد ، لذا دو بیت به عنوان بیتهای host و شش بیت به عنوان بیتهای Subnet شناخته می شوند . در نتیجه تعداد حالتهایی که با دو بیت می توان داشت چهار حالت بوده ، که از



Subnetting در کلاس C (ادامه):

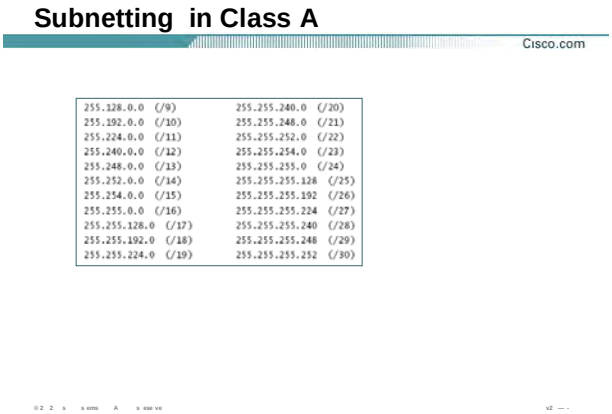
این تعداد فقط دو مورد را می توان به عنوان Valid IP Address به station ها نسبت داد و دو مورد دیگر نشان دهنده Network Address و Broadcast Address خواهند بود .

از طرفی 31/ قابل قبول نمی باشد . زیرا در این حالت یک بیت برای قسمت Host باقی می ماند و دو حالتی که با یک بیت می توان ایجاد کرد را نمی توان به عنوان IP Address به یک Host نسبت داد . زیرا درصورتی که این یک بیت دارای مقدار صفر باشد ما network address را خواهیم داشت و درصورتی که این یک بیت دارای مقدار یک باشد ما broadcast address را خواهیم داشت .



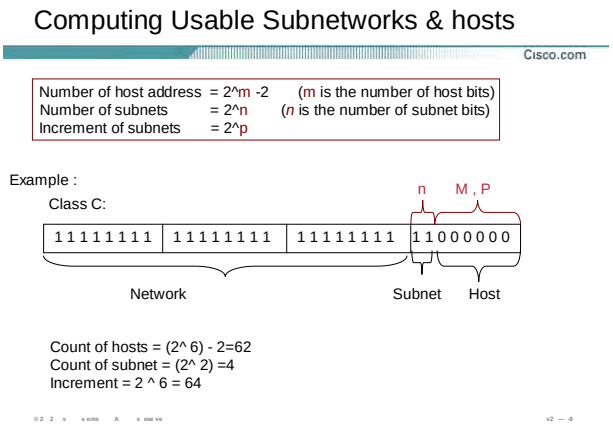
Subnetting در کلاس B:

شکل فوق ، تعداد حالتهای مختلف Subnet mask در کلاس B ، که با قرض گرفتن بیتهایی از قسمت Host شکل گرفته اند را نمایش می دهد .



Subnetting در کلاس A:

این شکل تعداد حالتهای مختلف Subnet mask در کلاس A ، که با قرض گرفتن بیتهایی از قسمت Host شکل گرفته اند را نشان می دهد .



محاسبه تعداد Host و Network:

تـا بـه اینجـا بـا تبـدیل کـردن IP Address از حالـت Decimal بـه Binary و متنـاظر کـردن آن بـا بیتهـای Subnet mask ، توانستیم Subnet work ها و ج آدرس ه ی هر کدام را تعیین کنیم .

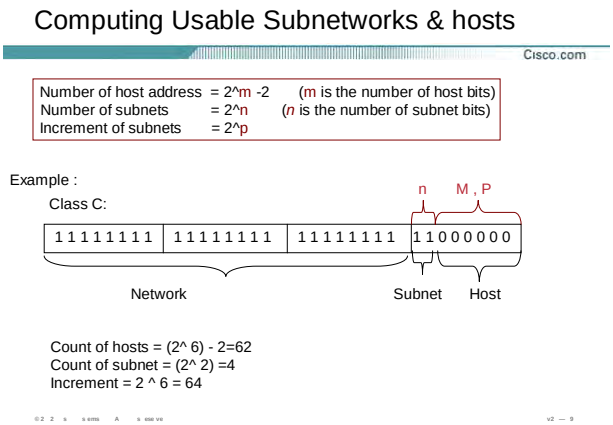
اما این روش زمان بر می باشد . روش سریعتری وجود دارد که می توان به کمک Subnet mask تعداد Subnetwork ها و تعداد IP Address های Valid در هر Subnetwork را مشخص کرد.

به شکل فوق توجـه کنیـد . درحالـت Default کـلاس C دارای subnet m s بـا مقـدار /24 مـی باشـد ، تعـدادی بیـت از قسمت Host قرض گرفته شده و به قسمت Network اضافه می شـود ، بنـابراین قـسمتی تحـت عنـوان subnet ایجـاد خواهد شد که شامل همان بیتهای قرض گرفته شده می ب شد .

محاسبه تعداد Subnet Network :

برای محاسبه این تعداد کافی است تعداد بیتهایی که نشان دهنده قـسمت Subnet مـی باشـد را محاسـبه کـرده و در فرمول زیر قرار دهید .

Number of subnets = 2^n (n is the number of subnet bits)



محاسبه تعداد Host و Network:

محاسبه مرتبه افزایش Subnet work :

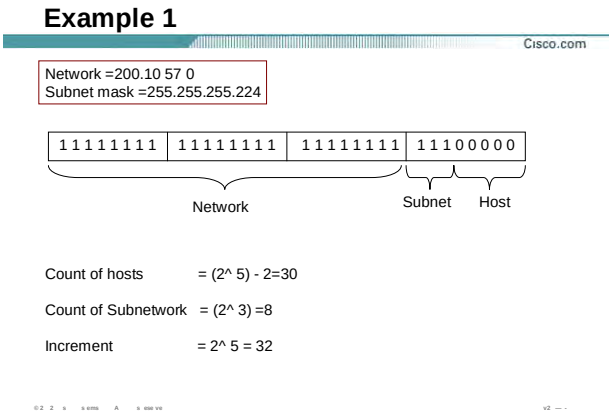
به فاصله بین دو Subnetwork گفته می شود . به طور مثال فاصله بین دو Network با آدرس 192.168.1.0 /24 و 192.168.2.0 /24 به اندازه 256 تا می باشد . اما درحالتی که ما از subnetting در شبکه استفاده کنیم با دانستن فاصله بین دو Subnetwork می توان Subnetwork ID های مختلف را بدست آوریم . برای این منظور تعداد بیتهای قرض گرفته شده در Subnetmask را محاسبه کرده و در فرمول زیر قرار می دهیم ، اما این شمارش در Octet ایی از Subnetmask صورت می گیرد که دارای تعدادی بیت یک و صفر باشد . به طور مثال در کلاس C تعداد بیتهای مورد نظر برای بخش Subnet ،با کل تعداد بیتهای Host یکی می باشد .

Increment of subnets = 2^p

محاسبه تعداد Host ها در هر Subnet Work :

برای محاسبه این تعداد کافی است تعداد بیتهایی از Subnetmask که نشان دهنده قسمت Host و دارای مقدار صفر می باشد را محاسبه کرده و آن را در فرمول زیر قرار دهید .

Number of host address = 2^m -2 (m is the number of host bits)



محاسبه تعداد Host و Network در یک مثال:

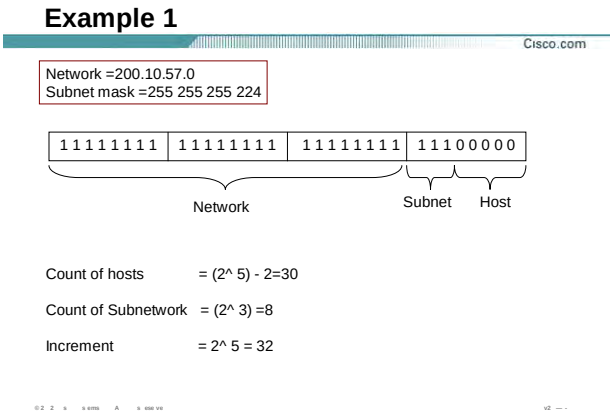
شکل فوق ، یک Network Address در کلاس C را نمایش می دهد که دارای Subnetmask به صورت 255.255.255.0 می باشد.

در صورتی که بخواهید شبکه را به کمک Subnet mask جدید با فرمت 255.255.255.224 ، Subnet کنید تعداد Subnetwork و Host ها و ID هر کدام از آنها را می توان به کمک روش اخیر بدست آورد . همانطور که مشاهده می کنید /27 دارای پنج بیت Host و سه بیت برای Subnet می باشد . به کمک آنچه گفته شد می توان تعداد هر کدام از آنها و مرتبه افزایش را به صورت زیر محاسبه کرد:

تعداد Subnetwork ها : ۸ تا .

مرتبه افزایش : ۳۲ تا .

تعداد Host های موجود در هر Subnetwork : ۳۰ تا .



محاسبه تعداد Host و Network در یک مثال (ادامه):

بنابراین Network با مشخصه 200.20.57.0 به ۸ تا Subnetwork تجزیه شده ، که برای مشخص کردن هر کدام از آنها از مرتبه افزایش کمک می گیریم . مرتبه افزایش برای این مثال ۳۲ می باشد . بنابراین فاصله بین هر دو Subnetwork متوالی به کمک مرتبه افزایش ۳۲ بوده و هر کدام از Network ID های جدید به صورت زیر می باشد :

Subnet 0 : 200.20.57.0

Subnet 1 : 200.20.57.32

Subnet 2 : 200.20.57.64

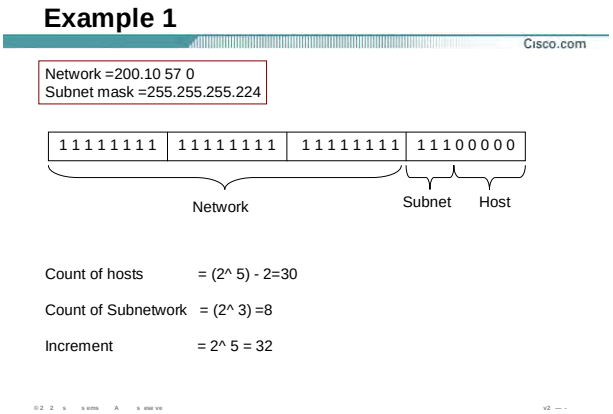
Subnet 3 : 200.20.57.92

Subnet 4 : 200.20.57.128

Subnet 5 : 200.20.57.160

Subnet 6 : 200.20.57.192

Subnet 7 : 200.20.57.224



محاسبه تعداد Host و Network در یک مثال (ادامه):

بنابراین هر یک از این Subnet work به منزله یک Network جدید خواهد بود.

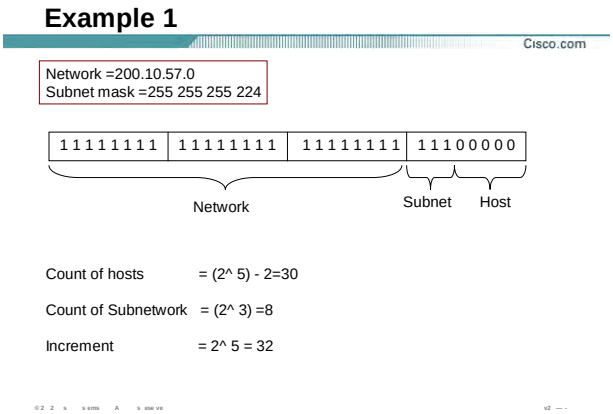
بنابراین بعد از مشخص شدن Subnetwork های جدید نوبت به مشخص کردن رنج IP Address ها مربوطه می رسد .

برای محاسبه رنج IP Address ها ابتدا می بایست دو Subnetwork متوالی مشخص شود . فرض کنید بخواهید رنج آدرس های مشخص شده توسط Network با مشخصه 200.20.57.0/27 را مشخص کنید . بنابراین می بایست دو Subnet work متوالی زیر را محاسبه کنید :

Subnet 0 : 200.20.57.0

Subnet 1 : 200.20.57.32

به کمک Subnet 0 اولین IP Address و به کمک Subnet 1 آخرین IP Address مشخص می شود .



محاسبه تعداد Host و Network در یک مثال (ادامه):

بنابراین با درنظر گرفتن Subnet 0 و اضافه کردن مقدار یک به آن اولین IP Address محاسبه می شود :

First IP Address : 200.20.57.1

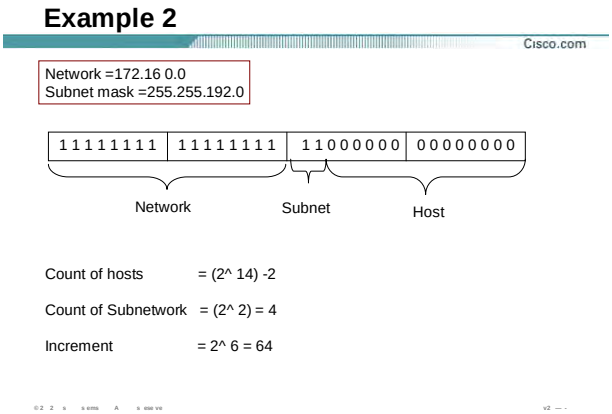
و با درنظر گرفتن Subnet 1 و کم کردن مقدار یک از آن Broad cast Address مشخص می شود :

Broadcast Address : 200.20.57.31

و با کم کردن مقدار ۲ از Subnet 1 مقدار آخرین IP Address مشخص می شود :

Last IP Address : 200.20.57.30

تا به اینجا رنج IP Address و Broadcast Address مربوط به Subnet 0 مشخص شدند . بنابراین برای تک تک Subnet work ها به همین ترتیب عمل کرده و رنج IP Address مربوط به هر کدام مشخص می شود.



محاسبه تعداد Host و Network در یک مثال:

این مثال شامل یک Network Address در کلاس B می باشد بنابراین دارای Subnet mask به صورت 255.255.0.0 خواهد بود . در صورتی که بخواهید شبکه را به کمک Subnet mask جدید با فرمت 255.255.192.0، Subnet کنید تعداد Subnet work و Host ها و ID هر کدام از آنها را می توان به کمک روش اخیر محاسبه و تعیین کرد .

همانطور که در شکل فوق مشاهده می کنید تعداد Subnet work ها ۴ و مرتبه افزایش ۶۴ می باشد .

بنابراین هر کدام از این Subnet work ها عبارتنداز :

Subnet 0 : 172.16.0.0

Subnet 1 : 172.16.64.0

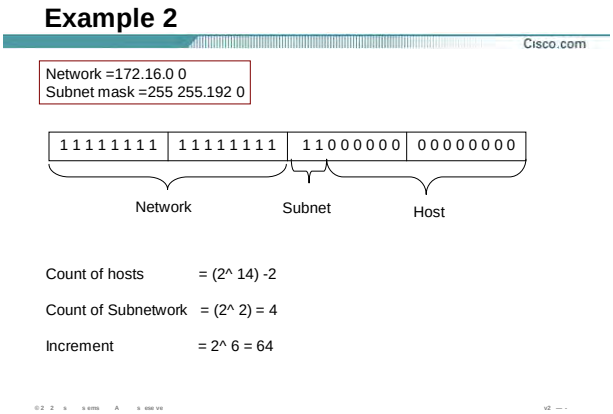
Subnet 2 : 172.16.128.0

Subnet 3 : 172.16.192.0

برای تعیین کردن رنج IP Address های هر کدام از Subnet work ها به صورت زیر عمل می کنیم :

Subnet 0 : 172.16.0.0

Subnet 1 : 172.16.64.0



محاسبه تعداد Host و Network در یک مثال (ادامه):

به کمک Subnet 0 اولین IP Address و به کمک Subnet 1 آخرین IP Address مشخص می شود .

بنابراین با درنظر گرفتن Subnet 0 و اضافه کردن مقدار یک به آخرین Octet ، اولین IP Address محاسبه می شود :

First IP Address : 172.16.0.1

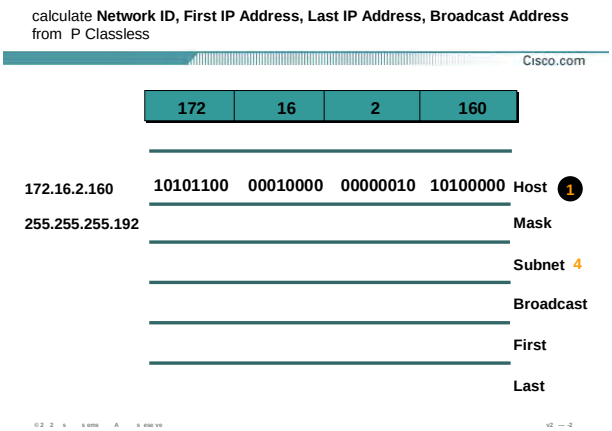
و با درنظر گرفتن Subnet 1 و کم کردن مقدار یک از Octet سوم و در نظر گرفتن مقدار ۲۵۵ برای Octet آخر Broad cast Address مشخص می شود :

Broadcast Address : 172.16.63.255

و با درنظر گرفتن Subnet 1 و کم کردن مقدار یک از Octet سوم و با در نظر گرفتن مقدار ۲۵۴ برای Octet آخر Last IP Address مشخص می شود .

Last IP Address : 172.16.63.254

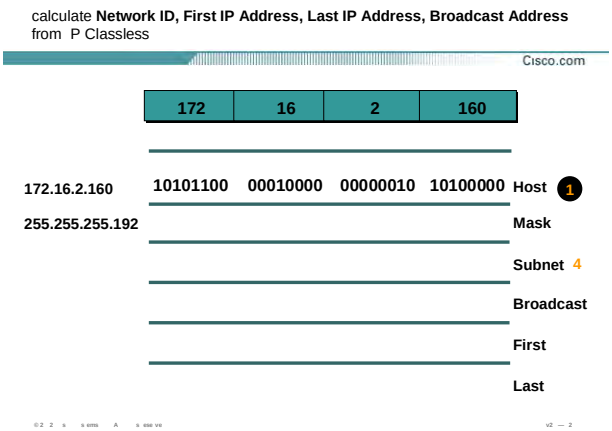
به همین ترتیب رنج IP Address ها در مورد Subnet work های بعدی تعیین می شود.



محاسبه رنج IP Address های یک شبکه به کمک IP Address :

تا به اینجا با روش تجزیه کردن یک Network Address به چند Subnet work و مشخص کردن رنج آدرسهای هر کدام از آنها آشنا شدید . حال اگر بخواهید رودخانه را برعکس شنا کنید و بخواهید از روی یک IP Address ، Subnet work مربوط به آن را تعیین کنید و یا بخواهید رنجی که این آدرس در آن واقع شده است را مشخص کنید چگونه عمل می کنید ؟

درصورتی که به شما یک IP Address به صورت Class Full داده شود ، به کمک Subnet mask می توانید Network Address مربوطه را تعیین کنید . فرض کنید به شما آدرس 192.168.1.1 /24 داده شود و از شما Network Address مربوط به آن خواسته شود .در این حالت چون این IP Address آدرسی در کلاس C بوده و به صورت Class full می باشد ، بنابراین قسمتی که network ID را مشخص می کند در IP Address بدون تغییر باقی مانده و فقط قسمتی که مشخص کننده Host ID در IP Address می باشد دچار تغییر می شود . بنابراین زمانی که به صورت Class Full کار می کنید سه Octet اول بدون تغییر باقی مانده و فقط بیتهای Octet چهارم به صفر تبدیل می شود . بنابراین Network Address مربوطه 192.168.1.0 /24 خواهد بود .



محاسبه رنج IP Address های یک شبکه به کمک IP Address (ادامه):

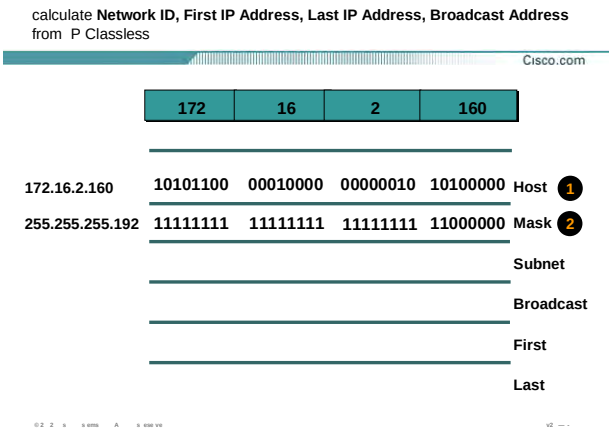
بنابراین به کمک Subnet mask بیتهای Network و Host مشخص شده و با این دانش می توان Subnet work مربوطه را مشخص کرد .

به شکل فوق توجه کنید . در این شکل یک IP Address به صورت classless داده شده است و می بایست برای آن Subnet work و رنج آدرسهایی که این آدرس در آن واقع شده است را مشخص کنید.

برای مشخص کردن آن مراحل زیر را دنبال کنید :

مرحله ۱ :

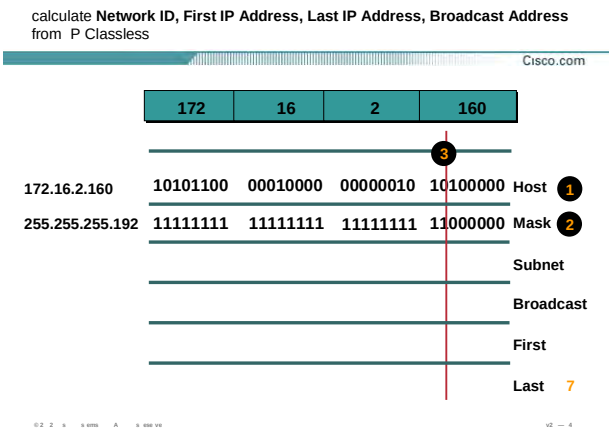
ابتدا IP Address داده شده را به فرمت Binary تبدیل کنید .



مرحله ۲:

Subnet mask مربوط به این آ س را به فرمت binary تبدیل کنید.

به این نکته توجه داشته باشید که Subnet mask رمباحث Subnetting نقش کلیدی دارد .

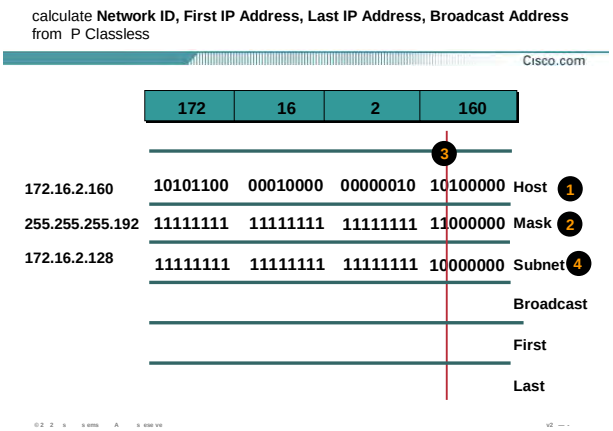


مرحله ۳:

همانطور که می دانید Subnet mask دنباله ای از بیتهای یک و صفر است که جداکننده بخش Network و Host می باشد .

بنابراین در این مرحله از جایی که بیتهای یک و صفر از یکدیگر جدا می شوند خطی کشیده شود .

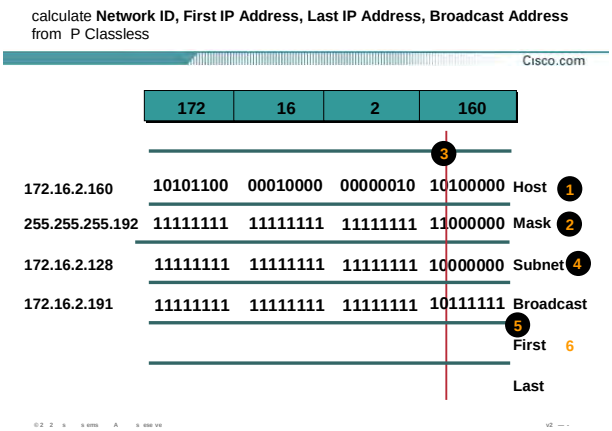
درواقع با این کار مرز بین بیتهای Network و Host در IP Address مشخص می شود .



مرحله ۴:

در این مرحله Subnet Work ID مشخص می شود .

همانطور که می دانید در Network Address ، بیتهایی که در قسمت Host هستند همگی دارای مقدار صفر هستند . بنابراین در این مرحله در IP Address بیتهایی که متناظر با قسمت Host در Subnet Mask هستند به مقدار صفر تبدیل شده و باقیمانده بیتها بدون تغییر باقی می ماند . حال اگر نتیجه کار را به فرمت Decimal تبدیل کنید Network Address مقدار 172.16.2.128 خواهد شد.

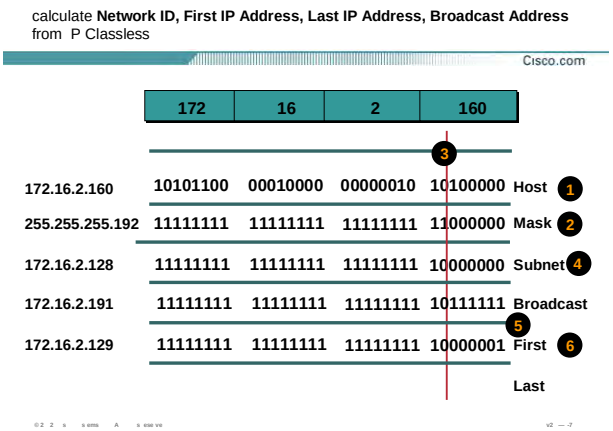


مرحله ۵:

همانطور که می دانید Broadcast Address ، آدرسی است که تمامی بیتهایی قسمت Host در IP Address دارای مقدار یک می باشد . بنابراین در این مثال شش بیت آخر نشان دهنده قسمت Host بوده و درنتیجه برای ایجاد Broadcast Address کافی است شش بیت آخر یک باشد .

بنابراین با تبدیل به فرمت Decimal خواهیم داشت :

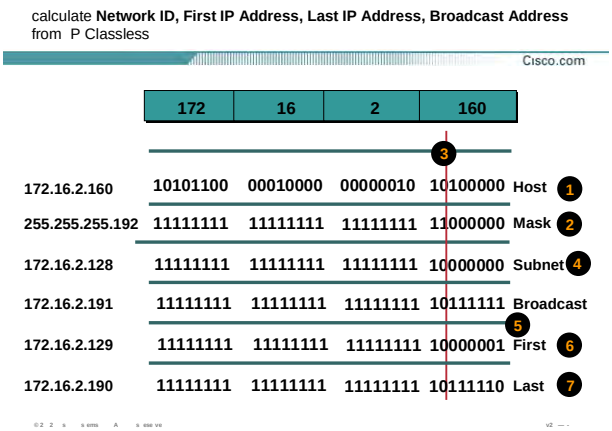
Broadcast Address : 172.16.2.191



مرحله ۶:

همانطور که میدانید برای پیدا کردن رنج IP Address ها در یک Subnet Work کافی است تمامی ترکیباتی که بیتهای Host می توانند داشته باشند را مشخص کرد. در شکل فوق اولین حالت و درنتیجه اولین IP Address مشخص شده است .

بنابراین اولین آدرس در مبنای ده 172.16.2.191 خواهد بود .



مرحله ۷:

در این مرحله آخرین حالتی که بیتهای بخش Host می توانند داشته باشند مشخص می شود . بنابراین آخرین IP Address در این رنج 172.16.2.190 خواهد بود .

درس چهارم :

مدیریت منابع سخت افزاری
Cisco Device

هدف :

۱. معرفی اجزای داخلی یک روتر .

۲. شرح مراحل بوت شدن روتر .

1. **Perform power-on self test (POST).**
2. **Load and run bootstrap code.**
3. **Find the Cisco IOS software.**
4. **Load the Cisco IOS software.**
5. **Find the configuration.**
6. **Load the configuration.**
7. **Run the configured Cisco IOS software.**

مراحل بوت شدن روتر :

تا به اینجا با سیستم عامل روتر (IOS) آشنا شدید . آیا تا به حال از خود پرسیده اید که IOS از کجا و چگونه load می شود؟ و یا اینکه تمامی تنظیماتی را که روی روتر انجام داده اید و در حافظه NVRAMذخیره کرده اید چگونه load شده و در کجا بارگذاری می شود؟

به صورت کلی وقتی شما کلید power روتر را در حالت on قرار می دهید مراحل زیر به ترتیب طی شده تا اینکه شما خط فرمان روتر یا همان command prompt را مشاهده می کنید.

مرحله ۱: در اولین مرحله سخت افزارهای روتر از نظر سالم بودن چک می شوند . این مرحله که به آن POST یا همان power-on self-test گفته می شود هم در سوئیچ و هم در روتر به عنوان گام اول می باشد .

مرحله ۲: در این مرحله فایل bootstrap جستجو و سپس اجرا می شود . نگران نباشید در ادامه با این فایل و نحوه کار آن بیشتر آشنا خواهید شد.

مرحله ۳: در این مرحله فایل IOS جستجو می شود .همانطور که می دانید محل اصلی ذخیره IOS به صورت default ، حافظه Flash می باشد. اما می توان IOS را در جای دیگری به جزء حافظه Flash ذخیره کرده و یا آن را از جای دیگری در شبکه Load کرد .

1. **Perform power-on self test (POST).**
2. **Load and run bootstrap code.**
3. **Find the Cisco IOS software.**
4. **Load the Cisco IOS software.**
5. **Find the configuration.**
6. **Load the configuration.**
7. **Run the configured Cisco IOS software.**

مراحل بوت شدن روتر (ادامه):

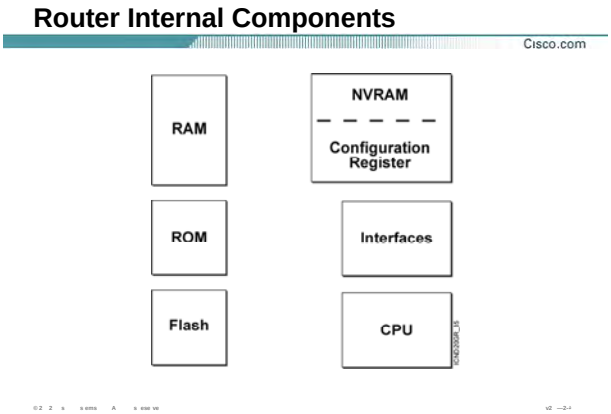
مرحله ۴: در این مرحله و پس از اینکه محل ذخیره شدن IOS مشخص شد، load شده و در حافظه فرار (RAM) بارگذاری می شود.

مرحله ۵: پس از load شدن IOS ، تنظیماتی که قبلا ذخیره شده اند جستجو می شوند. بنابراین در این مرحله محل ذخیره شدن فایل startup-config که حاوی تمامی تنظیمات روتر می باشد مشخص می شود.

Startup-config به صورت پیش فرض در حافظه NVRAM ذخیره می شود ولی شما می توانید محل ذخیره شدن آن را تغییر دهید.

مرحله ۶: پس از مشخص شدن محل ذخیره شدن فایل startup-config ،نوبت به load و بارگذاری آن در حافظه فرار(RAM)می رسد.

مرحله ۷: پس از مشخص شدن محل ذخیره شدن فایل startup-config و پس load شدن آن نوبت به اجرای این فایل می رسد . دراین مرحله این فایل در حافظه RAM بارگذاری می شود . بنابراین تمامی تنظیمات در حافظه RAM اجرا شده و در واقع از این لحظه به بعد روتر وارد مدار می شود.



اجزای داخ ی یک روتر :

تا به اینجا با مراحل boot شدن روتر به صورت کلی آشنا شدید. اما اجزای اصلی که در این سیکل نقش دارند کدام ها هستند و چگونه عمل می کن ؟

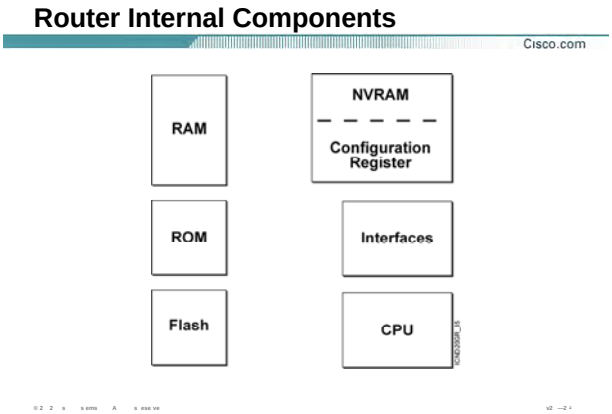
بنابراین قبل از بررسی سیکلstartup router ، ابتد با اجزای اصلی و داخلی روتر آشنا شوید.

RAM: حافظه فرار روتر می باشد .یعنی با خاموش شدن روتر و boot مجدد محتویات این فایل از بین خواهد رفت.

IOS روتر بعد از load شدن از حافظه Flash ، ز حالت فشردگی خارج شده و در حافظه RAM بارگذاری می شود و از طرف دیگر این حافظه محل بارگذاری فایل startup-config نیز ی باشد. بنابراین اولین نکته ای که باید به آن توجه کرد اینست که بعد از انجام تنظیمات و یا تغییرات در روتر ، ن را حتما در یک حافظه غیر فرار و دائمی ذخیره کنید.

از طرفی این حافظه محل نگهداری routing table و محل اجرای الگوریتم های سیریابی مختلف می باشد . نگران نباشید با این مفاهیم در درس های آتی آشنا خواهید شد.

ROM: حافظه فقط خواندنی روتر است . این حافظه شامل توابعی است که وظیفه تست و نگهداری سخت افزارهای روتر را به عهده دارد . در ادامه با ROM و توابع آن و نحوه عملکرد آنها آشنا خواهید شد



اجزای داخلی یک روتر (ادامه):

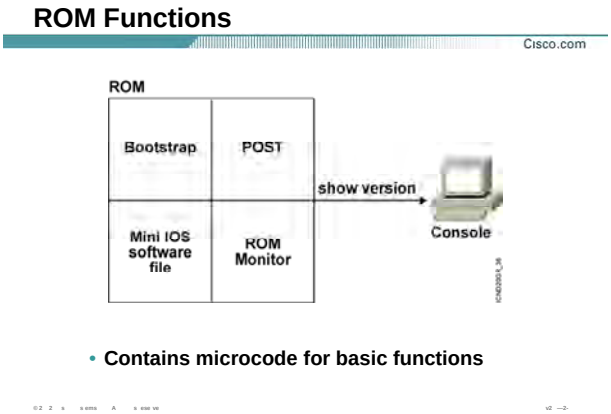
Flash: حافظه دائمی روتر است و محل نگهداری IOS می باشد و توسط شرکت Intel طراحی و برنامه ریزی شده است.

NVRAM: حافظه غیر فرار و دائمی روتر می باشد که با روشن و خاموش شدن روتر ، محتویات آن از بین نخواهد رفت. این حافظه محل نگهداری فایل startup-config می باشد.

Configuration register: مقادیری هستند که روی boot شدن روتر و یا سوئیچ کنترل دارند . به کمک فرمان show version می توانید مقدار آن را مشاهده کنید.

به طور مثال اگر مقدار رجیستری 0x2102 باشد ، روتر IOS را از حافظه flash و تنظیمات را از NVRAM استخراج می کند .

در مبحث password recovery با تغییر رجیستری بیشتر آشنا خواهید شد.



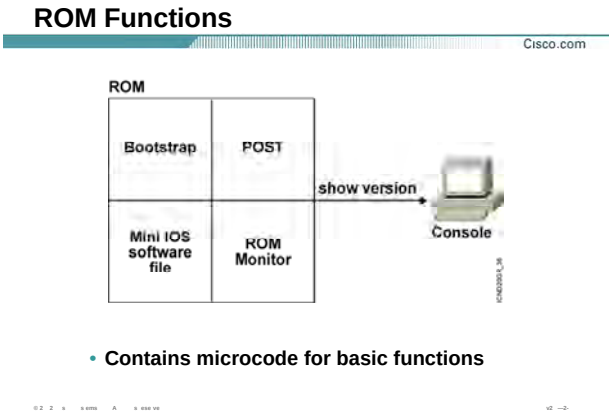
توابع ROM :

همانطور که گفتم ROM حافظه فقط خواندنی روتر می باشد و شامل توابعی است که وظیفه تست و نگهداری سخت افزارها و همچنین آغاز به کار روتر را به عهده دارند . توابع اصلی ROM عبارتند از:

۱. Bootstrap
۲. POST
۳. Mini IOS software file
۴. ROM Monitor

:Bootstrap

یکی از توابع ROM می باشد و وظیفه پیدا کردن محل ذخیره IOS و سپس load کردن آن را به عهده دارد.به کمک فرمان show version می توانید ورژن این تابع را مشاهده کنید.



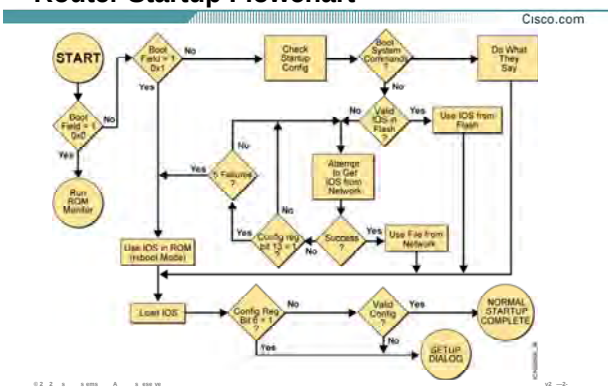
توابع ROM :

POST: یکی از توابع ROM می باشد و وظیفه تست اجزای سخت افزاری روتر را به عهده دارد .درواقع به کمک این تابع تمامی اجزای سخت افزاری درونی و بیرونی از نظر سالم بودن چک و تست می شود .

Mini IOS: یکی از توابع ROM می باشد و در صورتی که IOS از حافظه Flash بوت نشود ، این IOS موقتا Load شده و اجازه می دهد که توابع دیگر نظیر POST اجرا شوند . به طور مثال فرض کنید که حافظه flash مشکل پیدا کند و روتر نتواند IOS را از آن استخراج کند . در این حالت بعد از بوت شدن Mini IOS یکی از اینترفیس ها UP شده و به کمک آن می تواند IOS را از جای دیگر در شبکه load کند.

ROM Monitor: یکی از توابع ROM می باشد و شما می توانید با وارد شدن به این mode عملیاتی چون تغییر رجیستری را انجام دهید.درواقع به مانند مانیتوری برای حافظه ROM عمل می کند و شما فقط می توانید تنظیمات خاصی را از بین تنظیمات موجود انتخاب کنید. برای وارد شدن به این Mode هنگامی که روتر را روشن می کنید قبل از Boot شدن IOS ، کلیدهای ctrl و Break را همزمان بفشارید . در مبحث password recovery با این mode بیشتر آشنا خواهید شد.

Router Startup Flowchart



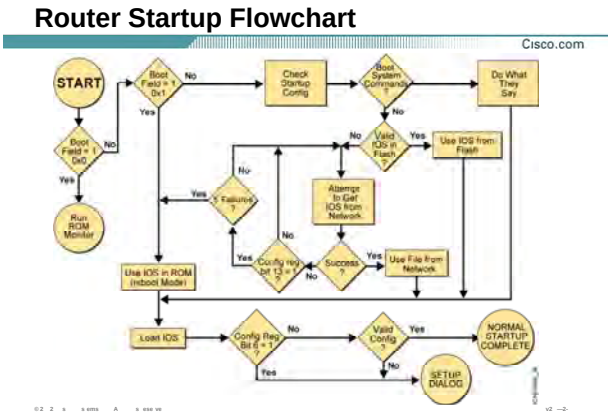
:Router Startup

تا به اینجا با مولفه هایی که در boot شدن نقش دارند به صورت مجزا آشنا شدید . در این لحظه با مراحل بوت شدن روتر به صورت پیوسته و به کمک نموداری از لحظه ای که کلید power روتر را در وضعیت on قرار می دهید تا لحظه ای که وارد CLI می شوید آشنا خواهید شد .

بعد از اینکه کلید power روتر را در وضعیت on قرار می دهید تابع POST که در حافظه ROM قرار دارد اجرا شده و تمامی اجزای سخت افزاری روتر از نظر سالم بودن چک می شود .

بعد از اطمینان از سالم بودن ، تابع bootstrap که جزء توابع حافظه ROM می باشد اجرا می شود.

وظیفه این تابع پیدا کردن محل ذخیره IOS و سپس load کردن آن می باشد . در این مرحله با توجه به مقداری که در Configuration register قرار دارد تصمیم گیری انجام می شود .



Router Startup (ادامه):

سه مقدار برای رجیستری و در نتیجه سه حالت برای تصمیم گیری جهت بوت شدن IOS وجود دارد:

۱. 0X2100

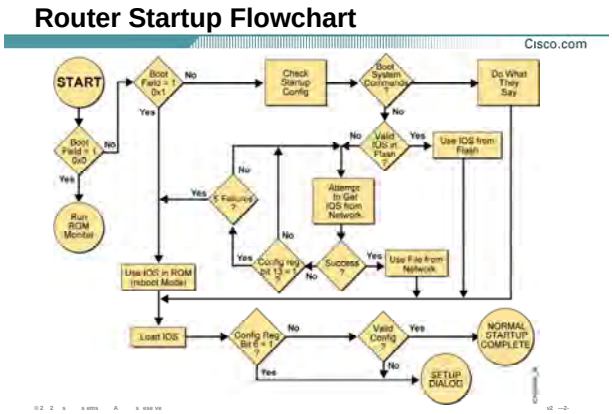
در صورتی که مقدار رجیستری 0x2100 باشد ، IOS ایی که در حافظه flash قرار دارد load نشده و روتر وارد ROM Monitor می شود.

۲. 0X2101

در صورتی که مقدار رجیستری 0x2101 باشد، Mini IOS به جای IOS اجرا می شود. همانطور که می دانید زمانی روتر وارد این مرحله می شود که نخواهد IOS از حافظه flash خوانده شود.

۳. 0X2102-0X210F

در صورتی که مقدار رجیستری 0X2102 تا 0X210F باشد ، IOS ایی که در حافظه flash ذخیره شده load می شود.



Router Startup (ادامه):

0x2102:

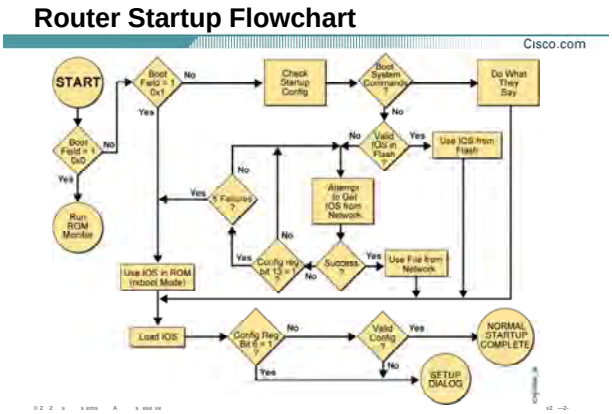
در این حالت ابتدا به حافظه flash نگاهی انداخته می شود و IOS در آنجا جستجو می شود . بنابراین دو حالت ممکن است رخ دهد:

۱. IOS در حافظه flash موجود است

در صورتی که آن را در حافظه flash پیدا کرد وارد مرحله بعد که همان load کردن IOS است می شود.

۲. IOS در حافظه flash موجود نیست

در صورتی که آن را در حافظه Flash پیدا نکند ، آن در شبکه جستجو می کند. اگر IOS ایی را روی TFTP Server پیدا کند آن را load می کند. بعد از طی شدن مراحل فوق و پیدا شدن محل ذخیره شدن IOS ، روتر آن را load می کند. بعد از این مرحله نوبت به تنظیمات روتر می رسد. روتر باید به این نتیجه برسد که آیا تنظیمی از قبل موجود بوده است یا خیر؟



Router Startup (ادامه):

برای این منظور رجیستری بررسی می شود و دو مقدار مختلف برای رجیستری و در نتیجه دو حالت مختلف وجود خواهد داشت:

- **0x2142**

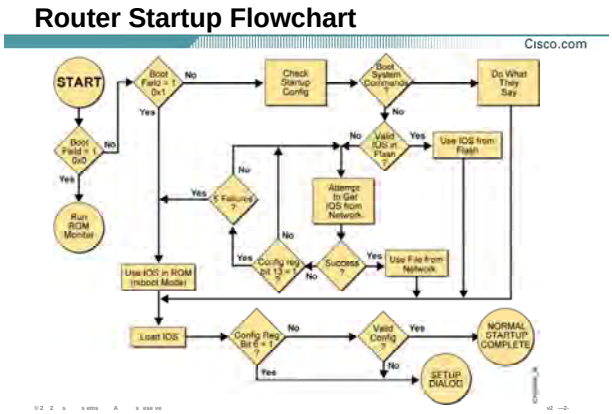
در این حالت روتر بدون نگاه کردن به NVRAM و محتویات آن وارد setup mode می شود .

همانطور که می دانید تنظیمات روتر و سوئیچ در حافظه NVRAM قرار می گیرد.

اگر مقدار رجیستری 0x2142 باشد ، روتر بدون توجه به تنظیمات موجود در حافظه NVRAM ، مستقیما وارد setup mode می شود.

در این mode سوالاتی به صورت متوالی در مورد تنظیمات اولیه روتر از جمله نام و پسورد و غیره پرسیده می شود.

می توانید بدون اینکه وارد setup dialog شوید از این mode خارج شده و مستقیما وارد user mode شده و تنظیمات را به وقتی دیگری موکول کنید.

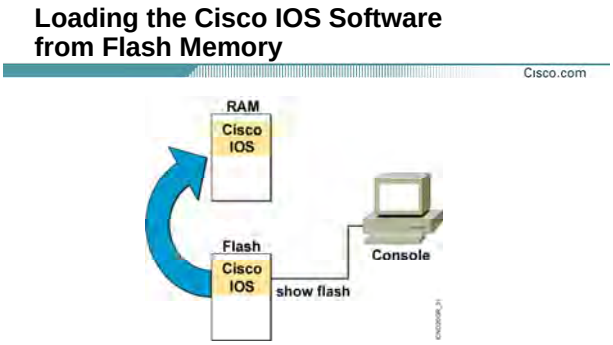


Router Startup (ادامه):

- **0x2102**

در این حالت روتر به حافظه NVRAM نگاهی می اندازد و فایل startup-config را در آن جستجو می کند. در صورتی که آن را در NVRAM پیدا کند ، آن را load کرده و در حافظه RAM بارگذاری می کند. در صورتی که هیچ تنظیمی در NVRAM موجود نباشد وارد setup mode شده تا تنظیمات اولیه روی روتر انجام شود.

بنابراین با طی شدن مراحل فوق روتر به صورت کامل boot می شود.



بارگذاری IOS در حافظه RAM :

در هنگام شدن روتر ، ابتدا روتر از محل ذخیره شده IOS آگاه می شود و سپس آن را load می کند. IOS در حافظه RAM بارگذاری شده و در واقع decompress می شود.

توجه داشته باشید که روتر ، IOS را به صورت یک فایل با پسوند (.bin) و به صورت فشرده ذخیره می کند.

بنابراین هنگام استفاده از آن ، ابتدا آن را decompress کرده و سپس آن را در حافظه RAM بارگذاری می کند.

به کمک فرمان زیر می توانید محتویات حافظه flash را مشاهده کنید.

```
Router>show flash
```

این فرمان هم در user mode و هم در privileged mode قابل اجراست.

show flash Command

Cisco.com

```
wg_ro_a#show flash

System flash directory:
File  Length   Name/status
  1   10084696  c2500-js-l_120-3.bin
[10084760 bytes used, 6692456 available, 16777216 total]
16384K bytes of processor board System flash (Read ONLY)
```


فرمان Show F ash :

همانطور که متوجه شدید برای دیدن محتویات حافظه flash از فرمان show flash استفاده کردیم . اما چه اطلاعاتی را در خروجی ا ن فرمان ی توان مشاهده کرد ؟ همانطور که گفته شد ، روتر فایل IOS را درحافظه flash یا در TFTP Server ذخیره می کند. بنا راین این فایل با نام و پسوند خاص خود ذخیره خواهد شد. روتر برای نام گذاری فایل IOS از قانون خاص و فرمت خاصی پیروی می کند. به خروجی فرمان Show Flash توجه کنید: نام فایل c2500-js-l-12.0-3 و پسوند آن هم bin سوالی که مطرح می شود اینست که هر جزء آن چه معنی و مفهومی دارد ؟

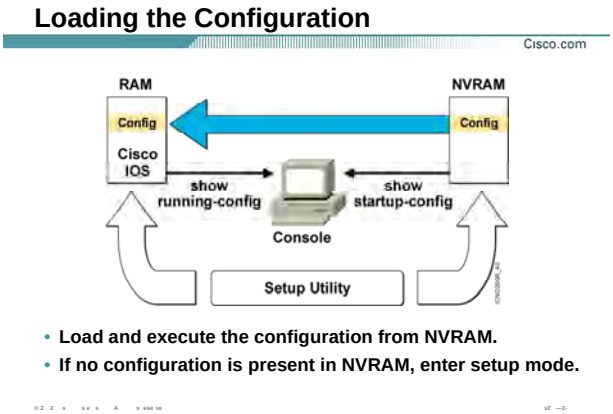
C2500: این نام ، همان نام تجاری device می باشد در این مثال device یک روتر از سری 2500 می باشد.

JS : بیانگر این است که این نسخه از IOS یک نسخه تجاری (enterprise)می باشد.

L: بیانگر این است که IOS به صورت یک فایل غیره فشرده در حافظه flash قرار دارد و آماده برای load شدن و بارگذاری در حافظه RAM می باشد.

12.0-3: در این قسمت می توانید ورژن IOS را مشاهده کنید.

Bin: فایل IOS با پسوند bin و به صورت باینری ذخیره می شود.



Load تنظیمات از NVRAM و بارگذاری آن در RAM:

بعد از مشخص شدن محل دخیره IOS و سپس load آن ، نوبت به پیدا کردن تنظیمات load آن می رسد.

همانطور که گفته شده روتر تنظیمات را درون فایل startup-config و در حافظه NVRAM ذخیره می کند .

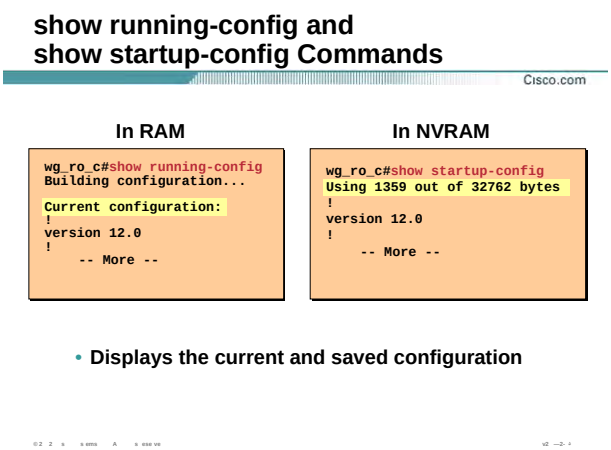
بنابراین بعد از load شدن IOS ، این تنظیمات از حافظه NVRAM خوانده شده و سپس در حافظه RAM بارگذاری می شوند. به کمک فرمان زیر می توانید تنظیمات موجود در NVRAM را مشاهده کنید.

Router# show startup-config

توجه داشته باشید این فرمان فقط در privileged mode قابل استفاده می باشد و به این علت است که این تنظیمات شامل انواع پسورد هایی می باشد که در مباحث قبل آنها را معرفی کردیم و به صورت clear text ، قابل مشاهده هستند.بنابراین فقط کسی باید آنها را ببیند که بتواند وارد این mode شود.

تمامی تنظیماتی که شما روی روتر انجام می دهید در حافظه RAM قرار دارد و با خاموش شدن روتر از بین خواهد رفت. بنابراین باید آنها را در یک حافظه غیر فرار ذخیره کنید . به کمک فرمان زیر می توانید تنظیمات موجود در حافظه RAM را مشاهده کنید.

Router# show running-config



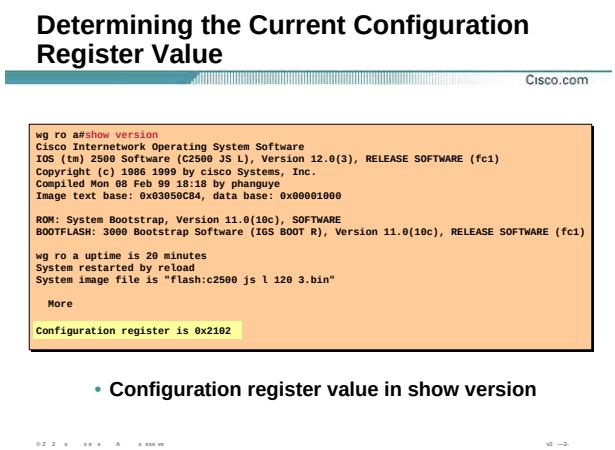
فایل RAM و NVRAM و محتویات هرکدام :

تا به اینجا با حافظه RAM و NVRAM آشنا شدید و آموختید که به کمک فرمان show running-config می توان محتویات حافظه RAM و با استفاده از فرمان show startup-config می توان محتویات حافظه NVRAM را مشاهده کرد.

در مثال فوق مشاهده می کنید که محتویات این دو فایل یکسان نیست. به نظر شما علت این تفاوت در چیست؟

این اختلاف به این علت است که هنوز محتویات حافظه RAM در حافظه NVRAM ذخیره نشده است. بعد از کپی شدن فایل running-config در حافظه NVRAM و در صورت بررسی محتویات هر دو حافظه متوجه یکسان بودن این دو فایل خواهید شد.

نکته : در پایان کار و بعد از تنظیم کردن روتر حتما محتویات RAM را در NVRAM ذخیره کنید تا مجبور نشوید آن را دوباره تنظیم کنید.



بررسی رجیستری :

تا به اینجا با IOS و مراحل بوت شدن آن آشنا شدید. یکی از فاکتورهای مهم در boot شدن روتر رجیستری می باشد و مقادیر مختلف آن در روند بوت شدن روتر تأثیر بسزایی دارند.

به طور مثال در صورتی که مقدار رجیستری 0x2142 باشد روتر به محتویات NVRAM توجهی نکرده و وارد setup mode می شود و یا اگر مقدار رجیستری 0x2101 باشد روتر ابتدا تنظیمات را از NVRAM خوانده و سپس در حافظه RAM بارگذاری می کند.

برای دیدن مقدار رجیستری در privileged mode فرمان زیر را وارد کنید.

Router# show version

Determining the Current Configuration Register Value

Cisco.com

```
wg ro a#show version
Cisco Internetwork Operating System Software
IOS (tm) 2500 Software (C2500 JS L), Version 12.0(3), RELEASE SOFTWARE (fc1)
Copyright (c) 1986 1999 by cisco Systems, Inc.
Compiled Mon 08 Feb 99 18:18 by phanguye
Image text base: 0x03050C84, data base: 0x00001000

ROM: System Bootstrap, Version 11.0(10c), SOFTWARE
BOOTFLASH: 3000 Bootstrap Software (IGS BOOT R), Version 11.0(10c), RELEASE SOFTWARE (fc1)

wg ro a uptime is 20 minutes
System restarted by reload
System image file is "flash:c2500 js l 120 3.bin"

  More

Configuration register is 0x2102
```

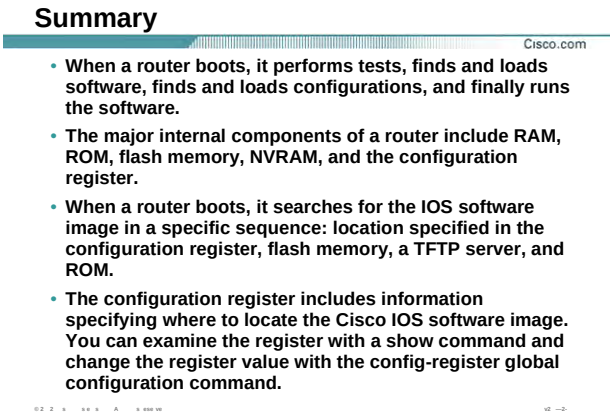
- **Configuration register value in show version**

بررسی رجیستری (ادامه):

درخروجی این فرمان می توانید موارد زیر را مشاهده و بررسی کنید:

۱. configuration register
۲. حجم حافظه RAM
۳. حجم حافظه NVRAM
۴. حجم حافظه Flash
۵. مدت زمان UP بودن روتر
۶. نام فایل IOS و ورژن آن
۷. ورژن فایل Bootstrap

در مبحث password recovery با کاربرد رجیستری بیشتر آشنا خواهید شد.



خلاصه :

بعد از اینکه power روتر را در وضعیت on قرار دادید مراحل بوت آغاز می شود. در اولین مرحله سخت افزارها از نظر safe بودن چک می شوند.

بعد از این مرحله ، روتر به دنبال IOS می گردد و بعد از پیدا کردن، آن را load کرده و در حافظه RAM بارگذاری می کند.

در صورتی که یک روتر دارای تنظیمات ذخیره شده باشد ، این تنظیمات از حافظه NVRAM خوانده می شود و سپس در حافظه RAM بارگذاری می شود . درغیر اینصورت روتر وارد setup mode می شود.

به کمک رجیستری می توانید مراحل بوت شدن روتر را تغییر دهید . به طور مثال با تغییر رجیستری به مقدار 0x2142 ، روتر هنگام بوت شدن با وجود داشتن تنظیمات در حافظه NVRAM وارد setup mode می شود. در واقع تنظیمات موجود در حافظه NVRAM خوانده نمی شود.

بعد از به پایان رسیدن مراحل بوت CLI اولین Mode ایی می باشد که با آن مواجه می شوید .

فصل سوم :

مسیریابی بر اساس
Cisco Routers

تا به اینجا با نحوه تعریف IP و فعال کردن Routed Protocol ایی چون IP روی تک تک اینترفیس ها آشنا شدید.

در واقع Network های متصل به هر کدام از این اینترفیس ها به صورت محلی قابل دسترس می باشد. به طور مثال روتر ، به شبکه LAN متصل به اینترفیس Fast Ethernet براحتی دسترسی دارد و تمامی packet هایی که مقصدشان در این Network باشد را براحتی هدایت می کند ، اما مشکل زمانی پیش می آید که مقصد جای دیگری باشد . در واقع destination مربوط به packet خارج از شبکه محلی باشد.

در این صورت چگونه packet به مقصد می رسد؟

روتر نیاز به شناخت تمامی مسیرهابه شبکه های محلی مختلف را دارد.

درواقع روتر باید بداند که از کدام مسیر باید packet را هدایت کند. و باید بداند که برای رسیدن به مقصد چند مسیر وجود دارد و از بین این مسیرها بهترین مسیر ، کدام یک می باشد.

بنابراین روتر با شناخت کل شبکه و مسیرهای موجود درخواست هایی را که نتواند در شبکه محلی خود پیدا کند به بیرون هدایت می کند و آن را در مسیر مناسب قرار داده و هدایت می کند.

درس اول :

مروری بر مسیریابی

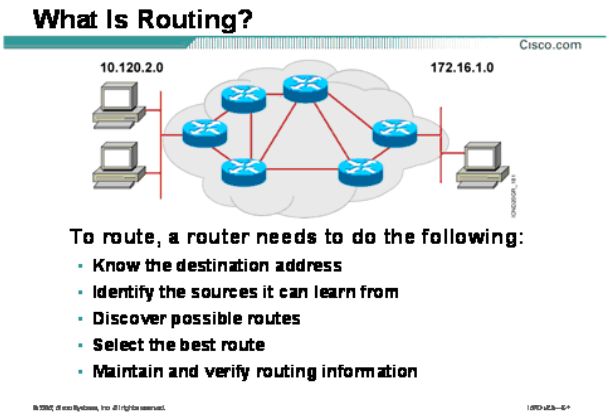
هدف :

۱. آشنایی با مفاهیم اولیه Routing.

۲. آشنایی با الگوریتم های Distance Vector و Link-State و تفاوتهای آن .

۳. آشنایی با الگوریتم مسیریابی Static ، Default.

۴. آشنایی با پروتکل های مسیریابی RIP ، IGRP ، EIGRP و OSPF.



مسیریابی چیست ؟

همانطور که تا به اینجا با مفهوم Routing آشنا شدید ، Routing پروسه انتخاب مسیر برای دسترسی به شبکه های غیر محلی می باشد. بنابراین وتر با شناخت از Network ها و مسیرهای رسیدن به هر کدام و نگهداری این اطلاعات در یک جدول به عنوان یک مسیریاب ایفای نقش می کند.

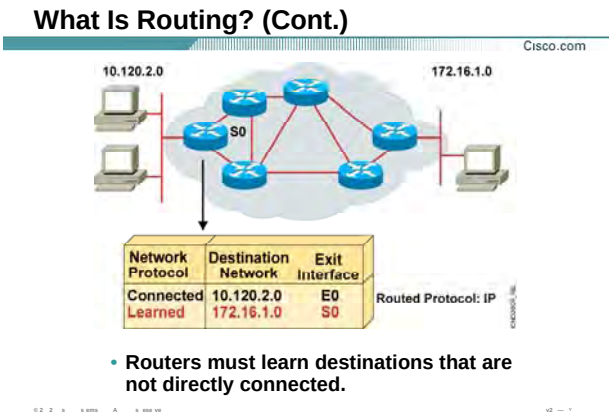
روتر باید بداند که اطلاعات شبکه های غیر محلی را از چه منبع ایی باید تهیه کند.

روتر باید بداند که برای رسیدن به هر کدام از ش که های غیر حلی چندین مسیر موجود است.

روتر باید بداند که از میان تمامی مسیرهای موجود برای رسیدن به یک شبکه غیرمحلی کدام یک بهترین می باشد.

و در نهایت روتر می بایست اطلاعات بدست آورده را در یک Database نگهداری کند تا با ورود یک پکت که آدرس مقصد آن شبکه ای غیرمحلی می باشد ، هدایت در سریعترین زمان ممکن صورت گیرد .

به Databese ایی که اطلاعات مربوط به شبکه های غیرمحلی را نگهداری می کند Routing Table گفته می شود .

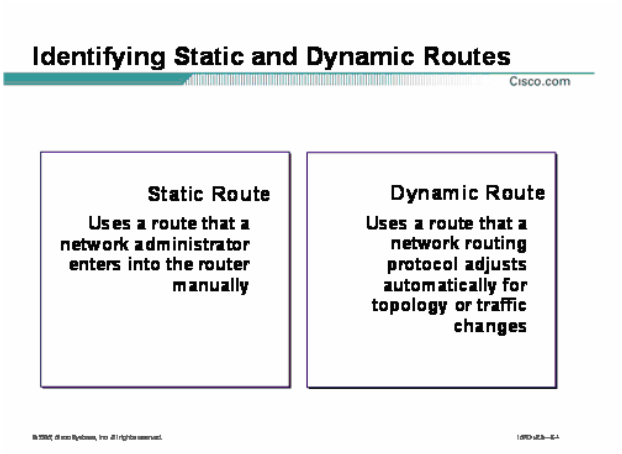


مسیریابی چیست ؟ (ادامه):

سوالی که پیش می آید این است که چه Network هایی در Routing Table نگهداری می شود؟

به شکل توجه کنید. Routing Table مربوط به یکی از روترها را مشاهده می کنید.

این table شامل Network address های شبکه های متصل به خود روتر چون 10.120.2.0 که از طریق اینترفیس E0 به روتر معرفی شده است و همچنین شبکه 172.16.0.0 (غیر Connect) که از طریق اینترفیس S0 به آن دسترسی پیدا می کند ، می باشد.



معرفی Static Routing و Dynamic Routing:

روتر شبکه های connect را به کمک اینترفیس های فعال خود می شناسد . حال سوالی که اینجا پیش می آید اینست که روتر شبکه های غیر محلی را چگونه می تواند بشناسد؟

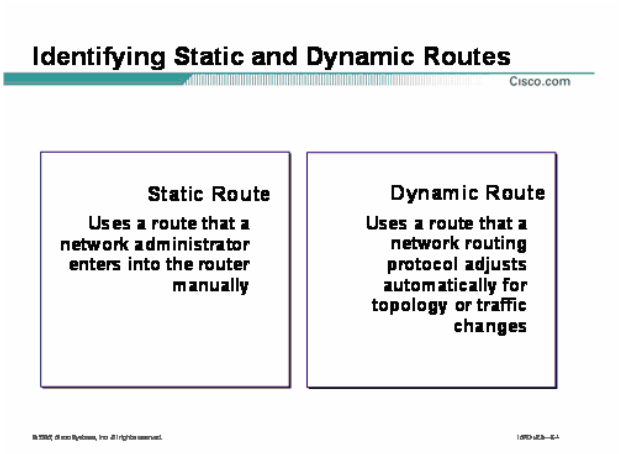
برای معرفی شبکه های غیر محلی به یک روتر در شبکه دو روش وجود دارد:

۱. static routing

۲. dynamic routing

در روش اول Network های غیر محلی و راه دسترسی به هر کدام از آنها به صورت دستی معرفی به روتر گفته می شود . درواقع شما به عنوان admin شبکه با شناخت از تک تک روتر ها و مسیرهای رسیدن به هر کدام و به صورت کلی با شناخت از ساختار کل شبکه ، خودتان عملیات مسیردهی به هر کدام از شبکه های غیر محلی را انجام می دهید.

با معرفی دستی مسیرها ، روتر دیگر نیازی ندارد که خود مسیرها را به صورت اتوماتیک شناسایی کند و یا تغییرات رخ داده شده در شبکه چون حذف یا اضافه شدن یک Network به شبکه را از روتر های دیگر بگیرد. همانطور که می دانید در حالتی که روتر فقط شبکه های متصل به خود را بشناسد ، فقط شبکه های connect در Routing Table نمایش



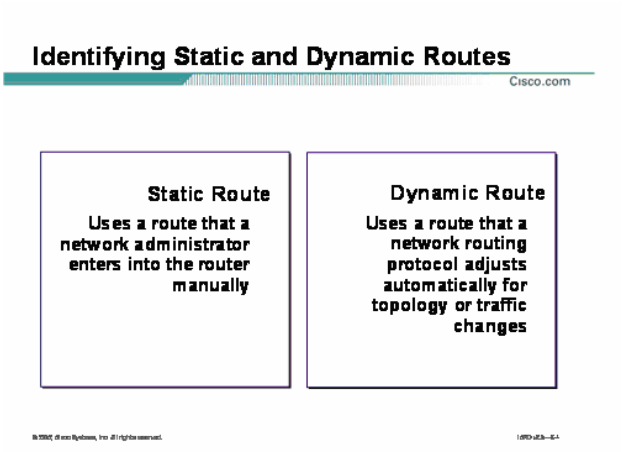
معرفی Static Routing و Dynamic Routing (ادامه):

داده می شوند . برای دسترسی به شبکه های غیر محلی به روش static ، admin شبکه خود می بایست که رکوردهای Routing Table روتر را تکمیل کند . در واقع admin شبکه باید تک تک شبکه ها و مسیر رسیدن به هر کدام از آنها را بداند و خود به صورت دستی این مسیر را به روتر معرفی کند.

بنابراین در صورتی که Network ای اضافه و یا حذف شود ، خود می بایست که روی تک تک روتر ها این تغییرات را اعمال کند. این بدان معنی است که روترها به صورت اتوماتیک از تغییرات رخ داده شده در شبکه مطلع نمی شوند .

بنابراین با توجه به تنظیم دستی تک تک روتر ها، مدیریت در شبکه های بزرگ سخت تر می شود ، درنتیجه استفاده از این روش را در شبکه های کوچکتر که مدیریت آن به صورت دستی امکان پذیر می باشد توصیه می شود.

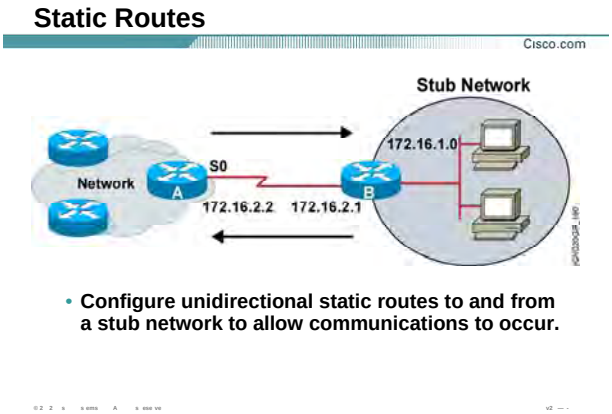
در روش دوم این شناخت به کمک الگورتیم های مسیریابی که در ادامه با آنها آشنا می شویید صورت می پذیرد.در واقع در این روش عملیات مسیریابی به صورت اتوماتیک انجام می گیرد .



معرفی Static Routing و Dynamic Routing (ادامه):

به این ترتیب که روتر اطلاعات شبکه را از روتر های دیگر گرفته و بعد از پردازش لازم و تغییر بعضی از فیلدها ، آن را در Routing Table نگهداری می کند و همچنین در صورتی که تغییری در شبکه رخ دهد این تغییرات منجر به تغییر Routing Table خواهد شد.

در واقع روتر با دریافت update هایی از روتر های مجاورش از تمامی تغییرات موجود در شبکه باخبر می باشد .



معرفی روش مسیریابی Static :

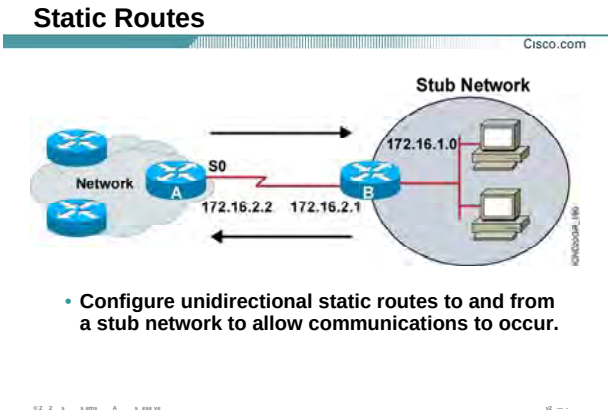
تا به اینجا یاد گرفتید که به کمک static route می توانیم به صورت دستی تمامی شبکه های غیرمحلی را به روتر معرفی کنیم و دانستیم که استفاده از این روش در شبکه های بزرگ چگونه دردسرساز می شود.

درواقع کاربرد اصلی این روش، برقراری ارتباط یک stub Network با شبکه های خارجی چون اینترنت می باشد.

Stub Network شبکه ای است که فقط یک راه خروجی (gateway) برای رسیدن به شبکه های دیگر چون اینترنت دارد. به طور مثال فرض کنید شبکه local یک شرکت قرار است به اینترنت متصل شود. برای این منظور ترافیک موجود در این شبکه می بایست به کمک یک route به خارج از شبکه منتقل شود.

به این مثال توجه کنید . فرض کنید یکی از station های موجود در شبکه درخواستی برای سایت www.yahoo.com داشته باشد ، اما مقصد این در خواست در شبکه محلی 172.16.1.0 موجود نمی باشد.بنابراین این درخواست باید از این شبکه خارج شود.

بنابراین کافی است که تمامی ترافیک موجود در stub Network را به اینترفیس 172.16.2.1 هدایت کنیم و چون این اینترفیس بااینترفیس S0 از روتر A در یک رنج IP می باشند، بنابراین ترافیک به سمت اینترفیس 172.16.2.2 از روتر A هدایت می شود.



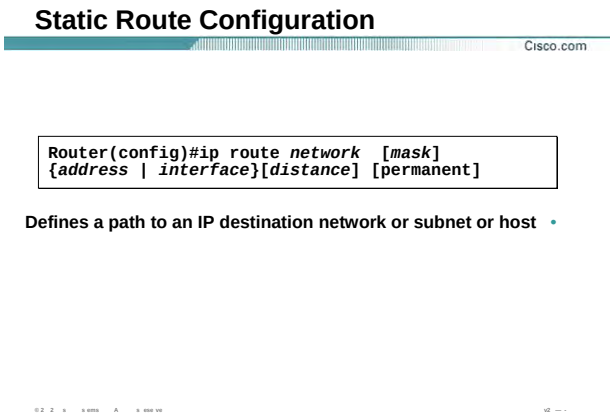
- **Configure unidirectional static routes to and from a stub network to allow communications to occur.**

معرفی روش مسیریابی Static (ادامه):

بنابراین کافی است که روی روتر A ، static route راه اندازی کنیم. درصورتی که روتر A پکتی را دریافت کرد که مقصدش شبکه 172.16.1.0 بود آن را به اینترفیس S0 هدایت می کند . چون یک مسیر به این شبکه از طریق این اینترفیس دارد .

برای تعریف کردن static route کافی است به روتر A به صورت دستی بگوییم که مسیری به شبکه 172.16.1.0 از طریق اینترفیس 172.16.2.1 وجود دارد .

اما روی روتر B چه تنظیمی باید انجام دهیم؟ پاسخ به این سوال default route می باشد که در ادامه با آن آشنا می شوید.



تنظیم Static Route :

برای راه اندازی static route وارد global mode شده و فرمان IP Route را وارد می کنید.

این فرمان شامل اجزای زیر می باشد:

Network: Network addresses مربوط به شبکه غیر محلی می باشد که قرار است ما برای آن یک مسیر تعریف کنیم.

Mask: subnet masks مربوط به شبکه غیرمحلی می باشد که آنها را در قسمت Network معرفی کرده ایم.

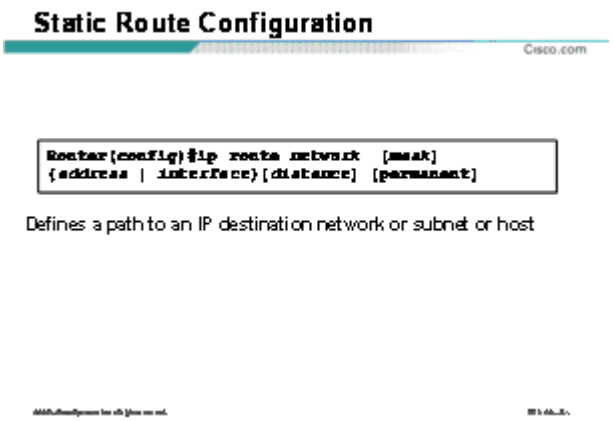
Address | interface: معرفی IP Address مربوط به اینترفیس روتر مجاور که دارای ارتباط Point-to-Point با این روتر می باشد.

تذکر: می توانید به جای IP روتر مجاور ، نام اینترفیس از روتری که روی آن static route راه اندازی کرده اید را وارد کنید.

Distance: static route به صورت پیش فرض دارای administrative distance با مقدار یک می باشد.

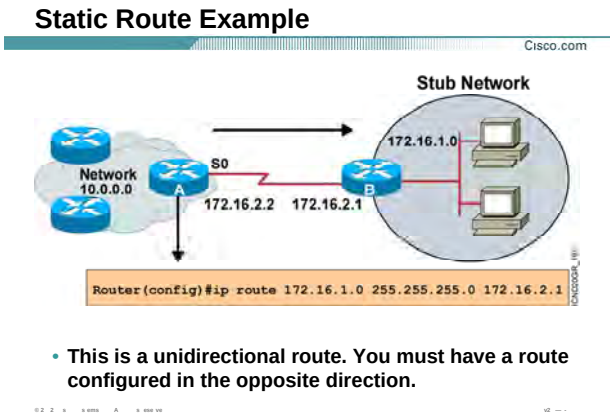
نگران نباشید در ادامه این درس با این مفهوم نیز آشنا خواهید شد.

بنابراین به کمک این فرمان شما می توانید مقدار AD را تغییر دهید .



تنظیم Static Route (ادامه) :

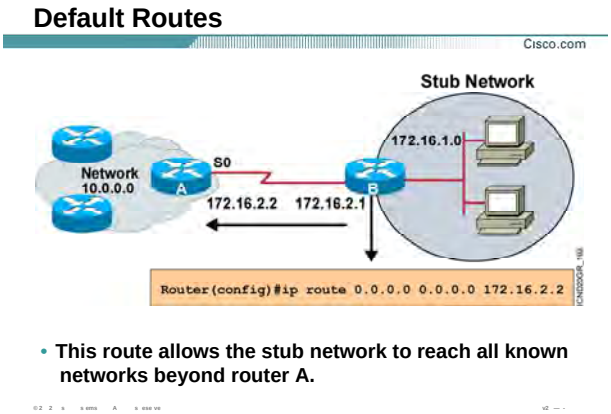
Permanent: با down شدن یک اینترفیس و یا قطع شدن لینک ارتباطی با روتر مجاور یک روتر ، route ایی که توسط static routeتعریف شده باشد در Routing Table نمایش داده نمی شود . اگر بخواهید با وجود down شدن یک اینترفیس و یا قطع شدن لینک ارتباطی با روتر مجاور این مسیر در Routing Table باقی بماند از permanent درهنگام تعریف کردن static route استفاده می کنیم . بنابراین مسیری را که تعریف می کنید همیشه در Routing Table نمایش داده می شود.



Static Route در یک مثال:

به این مثال توجه کنید. برای دسترسی به شبکه stub Network روی روتر A رفته و static route را به صورت بالا تعریف می کنیم.

در واقع کافی است که به روتر A بگوییم که دسترسی به شبکه 172.16.1.0 از طریق اینترفیس S0 می باشد. بنابراین یک مسیر از شبکه 172.16.1.0 به اینترفیس 172.16.2.1 تعریف می کنیم تا روتر A به کمک اینترفیس 172.16.2.2 که با اینترفیس 172.16.2.1 به صورت point-to-point ارتباط دارد ، به شبکه 172.16.1.0 دسترسی پیدا می کند.



: Default Route

تا به اینجا با static route و نحوه کار با آن آشنا شدید. در مثال قبل دیدید که چگونه با تعریف static route روی روتر A ، یک مسیر به شبکه stub تعریف کردیم در واقع روتر A به کمک این مسیر به شبکه 172.16.1.0 دسترسی پیدا می کند.

اما سوالی که اینجا مطرح می شود اینست که روتر B چگونه شبکه های دیگر را بشناسد؟

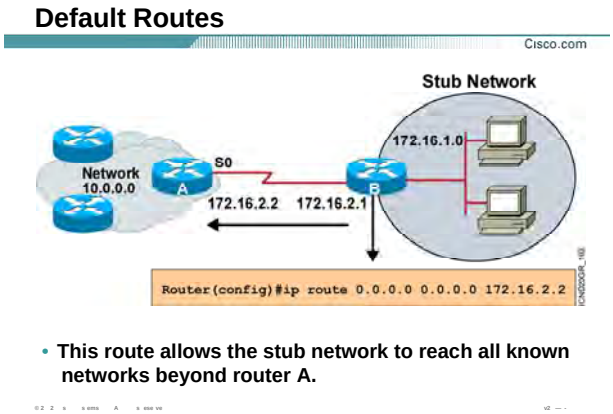
همانطور که مشاهده می کنید شبکه 16.1.0. 17 یک شبکه Stub می باشد و روتر B نقش یک دروازه برای دسترسی به شبکه های دیگر را برای شبکه stub بازی می کند. اما این روتر باید تمامی شبکه های غیر محلی را بشناسد. اما مشکل اینجاست که ما نمی توانیم یکی یکی شبکه های غیر محلی را به این روتر معرفی کنیم.

پس راه حل چیست؟

برای این منظور کافی است پکتی که آدرس مقصدش جای دیگری به غیر از شبکه محلی است ، مسیر دهی شده و از این شبکه خارج شود تا توسط روترهای دیگر مسیردهی شده و به مقصد برسد

درواقع Default route با تعریف یک مسیر به تمامی شبکه های غیر محلی، راه حل این مشکل است

Default route دارای اجزای زیر می باشد:



: Default Route

برای راه اندازی default route وارد global mode شده و فرمان IP Route را وارد می کنید.

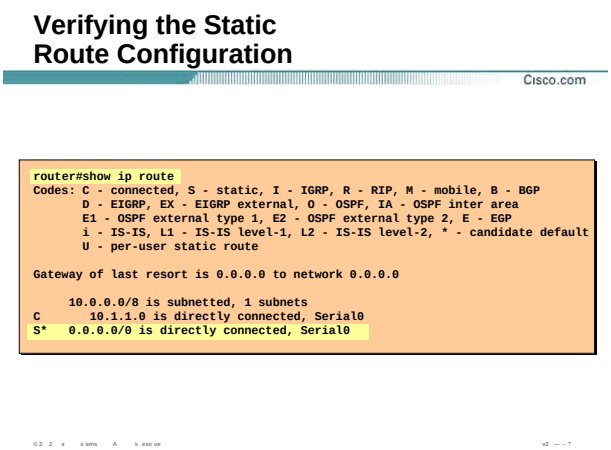
این فرمان شامل اجزای زیر می باشد:

IP route: فعال کردن static routing و یا default routing به کمک این فرمان می باشد.

0.0.0.0: همانطور که می دانید این IP جزء IP های رزرو شده ای می باشد که برای نشان دادن تمامی شبکه می باشد.

0.0.0.0: subnet mask مربوط به IP رزرو شده 0.0.0.0 می باشد.

interface | Address: معرفی IP Address مربوط به اینترفیس روتر مجاور که دارای ارتباط Point-to-Point با این روتر می باشد و یا نام اینترفیس خود روتر که قرار است ترافیک از آن خارج شده و به طرف روترهای دیگر هدایت شود.



بررسی نحوه عملکرد static Route :

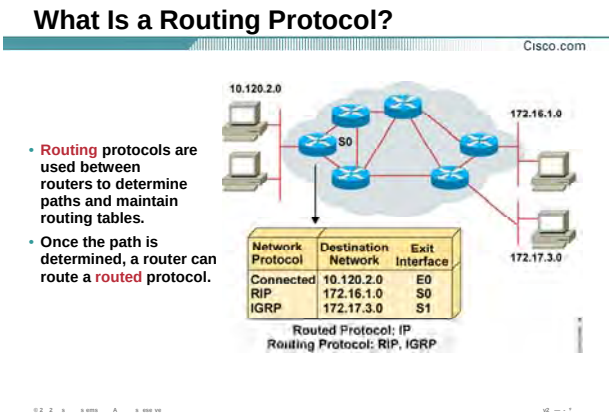
Show IP route: به کمک این فرمان می توانید اطلاعات موجود در Routing Table را مشاهده کنید. این اطلاعات شامل شبکه های متصل به خود روتر و یا شبکه هایی که از طریق Default route به روتر معرفی شده اند می باشد.

به مثال بالا توجه کنید. روتر به شبکه 10.1.1.0 به صورت connected از طریق اینترفیس serial 0 دسترسی دارد.

اما یک رکورد در این table وجود دارد که با علامت S* نشان داده شده است. این رکورد همان default route ایی است که ما تعریف کردیم . در واقع ما با تعریف این مسیر ، ترافیکی را که مقصدشان خارج از شبکه محلی باشد را از طریق اینترفیس serial 0 به بیرون هدایت می کنیم.

در صورتی که شما static route تعریف کرده باشید ، تمامی شبکه هایی را که از طریق static route به روتر معرفی کردید را می توانید در Routing Table با علامت S ببینید.

به ازای هر کدام از routing protocol ها یک کد اختصاری وجود دارد که می توانید لیست آنها را در خروجی فرمان show ip route و در قسمت Codes مشاهده کنید.



What is Routing Protocol?

تا به اینجا با static route و نحوه عملکرد آن آشنا شدید.

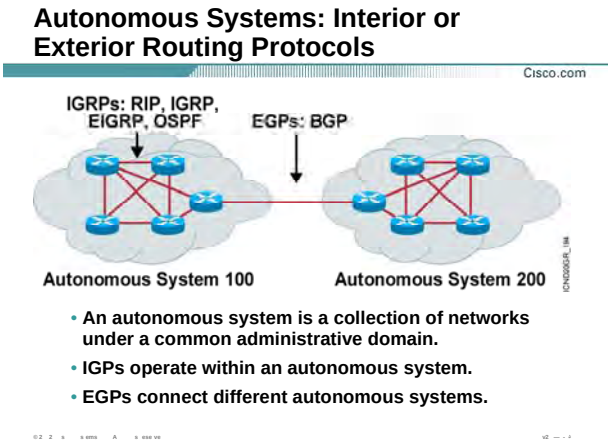
برخلاف Static route ، Dynamic Routing Protocol ها دارای عملکرد غیر دستی می باشند . این بدان معنی است که ما به صورت دستی شبکه های غیر محلی را به روتر معرفی نمی کنیم . این شناخت از طریق روترهای مجاور صورت می گیرد.

هر کدام از این Routing protocol ها دارای الگوریتم مخصوص به خود هستند و به کمک اطلاعات بدست آورده نسبت به انتخاب مسیر تصمیم گیری می کنند.

سوالی که اینجا مطرح می شود این است که چه تفاوتی بین Routing protocol و Routed protocol وجود دارد؟

Routed protocol: به پروتکل های IP ، IPX که در لایه Network عمل می کنند گفته می شود.

Routing protocol: به پروتکل های مسیریابی چون RIP و IGRP گفته می شود که وظیفه مسیریابی به شبکه های غیرمحلی را دارند.



معرفی AS ، IGP و EGP :

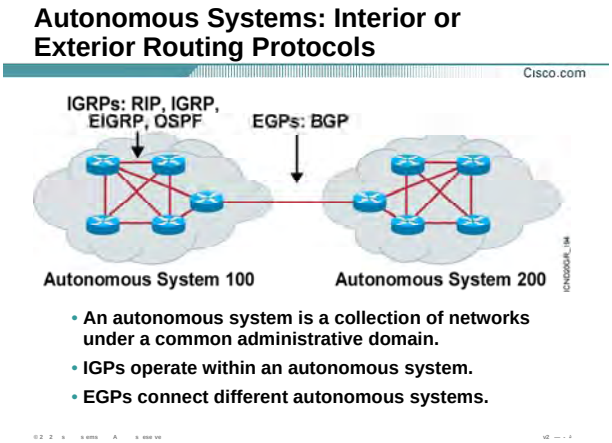
Autonomous system: مجموعه ایی است از روتر هایی که تحت یک مدیریت واحد فعالیت می کنند.

AS می تواند مجموعه ای از روترهایی باشد که یک پروتکل IGP را اجرا می کنند و یا مجموعه ای از روترهایی باشد که پروتکل های مسیریابی مختلف را تحت یک مدیریت واحد اجرا می کنند .

به هر AS عددی نسبت داده می شود و این عدد ، یک عدد شانزده بیتی بین 0 تا 65535 می باشد .

IANA متصددی نظارتی بر تمامی AS ها در دنیا می باشد که مسئولیت رجیستر کردن AS ها را با پنج Region مختلف که هر کدام قسمتی از کره زمین را پوشش می دهند ، انجام می دهد .

دو دسته بندی اصلی با توجه به مفهوم Autonomous system برای Dynamic Routing Protocol ها وجود دارد که به صورت زیر می باشد:



معرفی AS ، IGP و EGP (ادامه) :

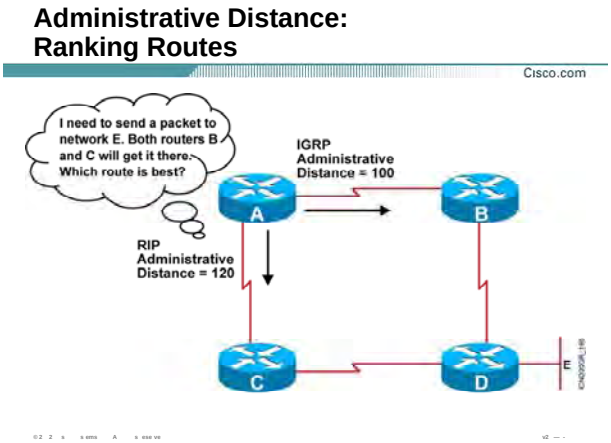
Interior Gateway Protocols (IGPs):

به تمامی Routing Protocol هایی که روتر های درون یک AS را به یکدیگر مرتبط می کند ، گفته می شود و درواقع پروتکل هایی هستند که درون یک AS فعالیت می کنند. روتر های درون یک AS با داشتن یکی از این پروتکل های مسیریابی به تبادل اطلاعات با یکدیگر پرداخته و برای رسیدن به یکدیگر مسیری را پیدا می کنند .

Routing protocol های RIP و IGRP و EIGRP و OSPF همگی جزء پروتکل های مسیریابی هستند که در داخل یک AS فعالیت می کنند .

Exterior Gateway Protocols (EGPs):

به تمامی Routing Protocol هایی که دو AS مختلف را به یکدیگر متصل می کنند گفته می شود . BGP (Border Gateway Protocol) یک نمونه از پروتکل های مسیریابی EGP می باشد .



:Administrative Distance

Administrative Distance یا همان AD معیار و ملاکی برای انتخاب Routing در میان روشهای مختلف مسیریابی می باشد .

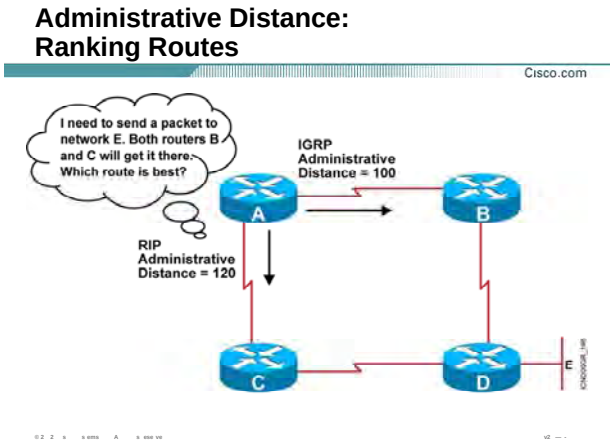
به مثال بالا توجه کنید. روی روتر A دو روش میسریابی RIP و IGRP که در ادامه با آنها آشنا می شویید تنظیم شده است . روتر A برای رسیدن به روتر D دو مسیر را شناسایی می کند. اما سوالی که اینجا مطرح می شود اینست که کدام مسیر به عنوان مسیر اصلی انتخاب می شود؟

بنابراین نیاز به ملاکی داریم که بین دو routing protocol یکی را انتخاب کند.

هر کدام از روش های مسیریابی AD مخصوص به خود را دارند. به طور مثال static route دارای AD با مقدار یک و یا پروتکل مسیریابی RIP دارای AD با مقدار 120 می باشد. AD ، عددی بین 0 تا 255 می باشد .

نکته: در Routing Table مربوط به یک روتر ، هر کدام از شبکه های connect با AD با مقدار صفر نمایش داده می شوند.

سوالی که پیش می آید اینست که در میان چندین روش مسیریابی که AD های مختلفی دارند ، روتر با کدام روش مسیریابی را انجام می دهد؟



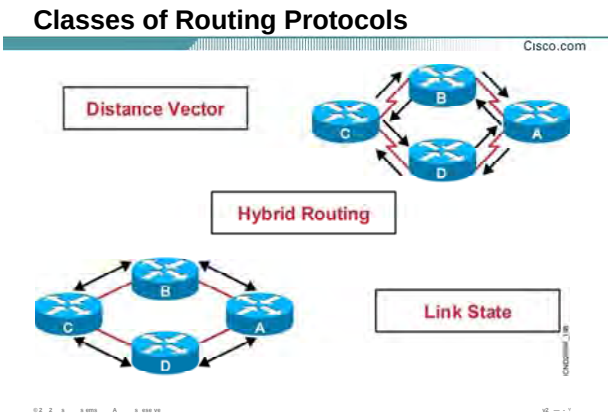
Administrative Distance (ادامه):

در صورتی که چندین روش مسیریابی روی یک روتر تنظیم شـده باشـد ، روشـی کـه دارای کمتـرین مقـدار AD در میـان روش های دیگر باشد انتخاب شده و به عنوان مسیر اصلی تا شبکه مقصد در نظر گرفته می شود و در Routing Table قرار می گیرد.

در مثال بالا دو مسیر برای رسـیدن بـه روتـر D وجـود دارد کـه هـر کـدام از ایـن مـسیرها ، دارای AD مختلفـی هـستند. مسیری که دارای AD کمتری باشد مسیر (ABD) می باشد . بنابراین این مسیر به عنـوان بهتـرین مـسیر انتخـاب مـی شود.

در ادامه با معیار دیگری که وظیفه انتخاب بهترین مسیر در میان روتر هایی کـه دارای یـک routing protocol واحـد مـی باشد ، آشنا می شویید. این ملاک ، متریک می باشد.

بنابراین AD برخلاف متریک ، ملاک انتخاب روش مسیریابی در میان چندین روش مختلف مسیریابی است.



دسته بندی Dynamic Routing Protocol :

روش های مسیریابی به صورت کلی به دو دسته تقسیم می شوند:

۱. Static route

۲. Dynamic route

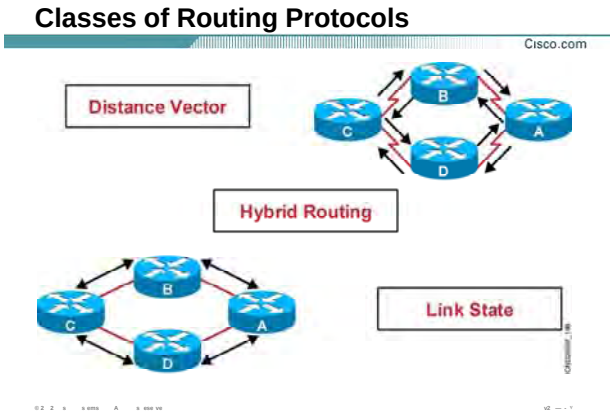
در روش اول که با آن آشنا شدید تمامی مسیرها به صورت دستی و توسط Admin به تک تک روترها معرفی می شود . در این روش روتر نیاز به کسب اطلاع از روترهای دیگر نسبت به Network های غیرمحلی و راه دسترسی به هر کدام از آنها ندارد. در روش دوم وضعیت به سادگی روش اول نیست. در این روش روترها نیاز به اطلاعات روترهای دیگر دارند. این به این معنی است که کوچکترین تغییرات در شبکه مانند up و یا down شدن یک اینترفیس روی عملکرد تک تک روترهای شبکه تأثیر می گذارد و روترها می بایست تغییرات رخ داده شده را به دیگر روترها اطلاع دهند .

Dynamic routing protocol ها به سه دسته کلی تقسیم می شوند:

۱. Distance Vector

۲. Link state

۳. Hybrid Routing



دسته بندی Dynamic Routing Protocol (ادامه):

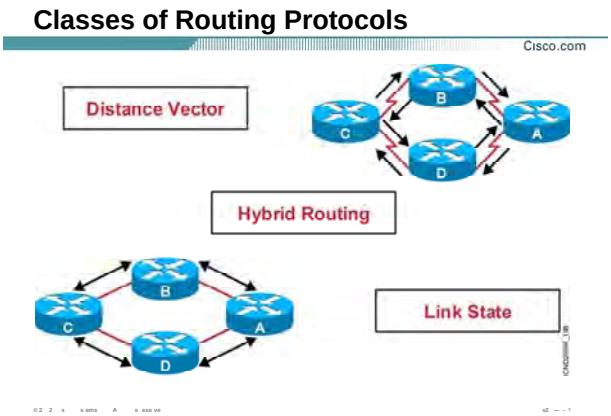
Distance Vector: به Routing Protocol های گفته می شود که هر روتر فقط با روترهای مجاورش به تبادل اطلاعات می پردازد .

بنابراین همانطور که از اسمش پیداست ، روتر برای رسیدن به مقصد یک بردار خطی تعریف می کند به طوری که ابتدای این بردار از خود روتر شروع شده و بعد از گذشتن از یکی از روترهای مجاور و گذشتن از تعدادی روتر به شبکه مقصد می رسد.

به طور مثال در صورتی که یک روتر به دنبال مسیری تا یک شبکه غیر محلی باشد ، کافی است ببیند روتر مجاورش آن شبکه غیر محلی را از چه مسیر و یا مسیرهایی می شناسد . در واقع بهترین مسیری را که روتر مجاورش تا آن شبکه غیرمحلی تشخیص داده کدام مسیر می باشد و از روی این دانسته بهترین مسیر را می تواند انتخاب کند.

بنابراین هر روتر کافی است فقط با روتر مجاورش تبادل اطلاعات داشته باشد .

برای نمونه می توان Routing Protocol های RIP و IGRP را از این دسته معرفی کرد.



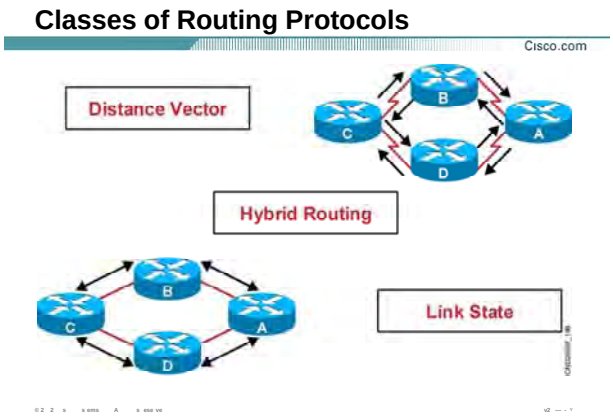
دسته بندی Dynamic Routing Protocol (ادامه):

Link state: به Routing Protocol های گفته می شود که هر روتر ابتدا باید یک تصویر کلی از کل شبکه یا ناحیه ای که روتر در آن واقع شده را داشته و سپس با اشتن این دید کلی عملیات مسیریابی را انجام دهد.

این پروتکل ها ابتدا ساختار غیرمنتظم شبکه را به صورت یک گراف بدون دور در می آورند و سپس از روی این گراف ، بهترین مسیر به هر کدام از شبکه های غیر محلی را شخیص می دهند.

در این پروتکل ها گام اول شناخت روترهای مج ور می باشد و سپس بعد از اینکه هر روتر روتر مجاورش را شناخت و توپولوژی شبکه را از او آموخت ، با کمک گرفتن از این اطلاعات گرافی را طراحی می کند که خود این روتر ، ریشه این گراف است .

برای نمونه می توان پروتکل مسیریابی OSPF را به عنوان یک پروتکل Link state ایی معرفی کرد.



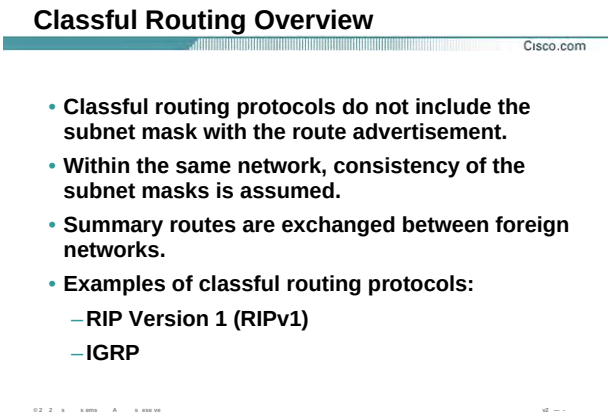
دسته بندی Dynamic Routing Protocol (ادامه):

بنابراین تفاوت عمده پروتکل های Distance Vector و Link State در این است که در پروتکل های Distance Vector لزومی ندارد که روتر تصویری کلی از توپولوژی شبکه را داشته باشد و از روی آن بهترین مسیر به شبکه های غیر محلی را تشخیص دهد. کافی است بداند که روترهای مجاورش شبکه های غیرمحلی را از چه مسیری می شناسند و از روی این دانش خود بهترین مسیر تا مقصد را تعیین کرده و آن را در Routing Table خود درج می کند .

Hybrid Routing: این دسته همانطور که از نامش پیداست ترکیبی است از ویژگیهای Link state و Distance Vector.

مانند Distance Vector عمل می کند چون بین روتر مبدا و روتر مقصد یک بردار در نظر می گیرد و نحوه دسترسی به شبکه های غیرمحلی را از روترهای مجاورش آموخته و نسبت به آن تصمیم گیری می کند.

مانند Link state عمل می کند چون می بایست تصویر کلی از شبکه را داشته باشد و نسبت به این تصویر بهترین مسیرها را به شبکه های غیرمحلی تشخیص می دهد.



:Classful Routing Protocol

Dynamic Routing Protocol ها با توجه به اینکه VLSM را ساپورت کنند یا نه ، به دو دسته کلی تقسیم می شوند:

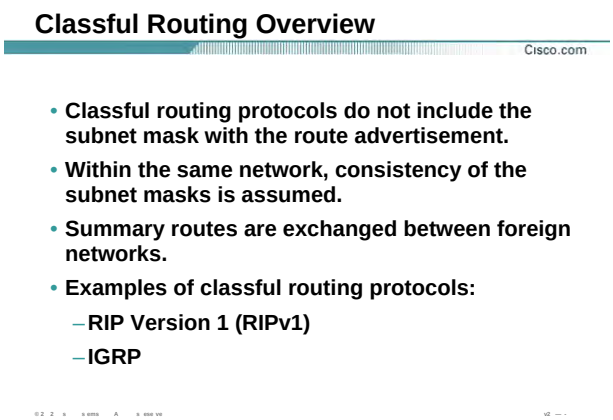
۱. Classful Routing

۲. Classless Routing

Classful Routing:به Routing Protocol هایی گفته می شود که(Variable Length Subnet Mask) VLSM را ساپورت نمی کنند.

این بدان معنی است که، هنگامی که یک روتر Network ایی را به روتر دیگری معرفی می کند همراه با آن Subnet mask مربوط به آن Network را گزارش (Advertise) نمی کند.

بنابراین روتر آدرس شبکه های غیرمحلی را به صورت استاندارد در Routing Table درج می کند حتی اگر CIDR مربوط به آن آدرس به صورت default نباشد. فرض کنید که روی یک روتر ، Classful Routing راه اندازی کرده ایم. در صورتی که این روتر update ایی را از یکی از اینترفیس هایش دریافت کند که شبکه 172.16.128.0/17 را Advertise می کند ، آن را به صورت 172.16.0.0 / 16 در Routing Table درج می کند.



Classful Routing Protocol (ادامه):

توجه:

کلاس A دارای subnet mask ، 255.0.0.0 می باشد.

کلاس B دارای subnet mask ، 255.255.0.0 می باشد.

کلاس C دارای subnet mask ، 255.255.255.0 می باشد.

بنابراین حتی اگر از VLSM در شبکه استفاده کرده باشید ، آدرس ها به صورت اتوماتیک به Boundary استاندارد Summary می شوند.

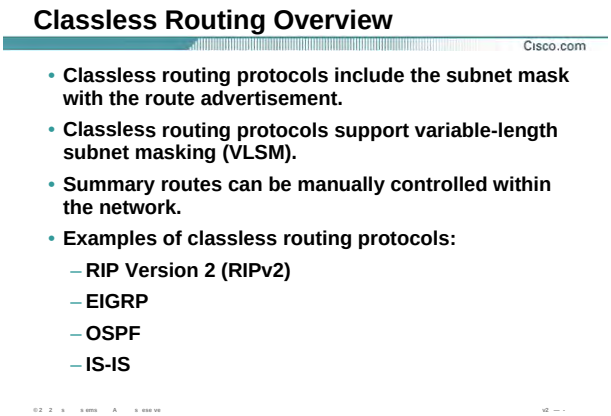
فرض کنید در شبکه دو آدرس زیر موجود باشد .

192.168.1.0/25

192.168.1.128/25

بنابراین این دو شبکه دارای Boundary استاندارد 192.168.1.0/24 می باشد . و به جای دو شبکه یک شبکه Advertise می شود .

برای نمونه می توان پروتکل مسیریابی RIP Version 1 و IGRP را به عنوان Classful Routing Protocol معرفی کرد.



:Classless Routing Protocol

:Classless Routing

برخلاف classful Routing ، این دسته از پروتکل ها VLSM را ساپورت می کنند .

این بدان معنی است که هر روتر علاوه بر Network ، Subnet mask را نیز Advertise می کند.

بنابراین در این حالت آدرس ها به Boundary استاندارد Summary نمی شود.

و در این حالت تعداد شبکه هایی که در Routing Table قرار دارند بیشتر است.

برای نمونه می توان پروتکل مسیریابی RIP Version 2 و EIGRP و OSPF و IS-IS را به عنوان Classless Routing Protocol معرفی کرد.

Routing Protocol Comparison Chart

Cisco.com

Characteristic	RIPv1	IGRP	EIGRP*	IS-IS	OSPF
Distance vector	X	X	X		
Link-state				X	X
Automatic route summarization	X	X	X		
Manual route summarization			X	X	X
VLSM support			X	X	X
Proprietary		X	X		
Convergence time	Slow	Slow	Very Fast	Fast	Fast

* EIGRP is an advanced distance vector protocol with some link features.

جدول مقایسه ای Dynamic Routing Protocols :

تا به اینجا با دسته بندی های مختلف Dynamic Routing Protocol آشنا شدید.

جدول بالا مقایسه بین Dynamic Routing Protocol های مختلف می باشد.

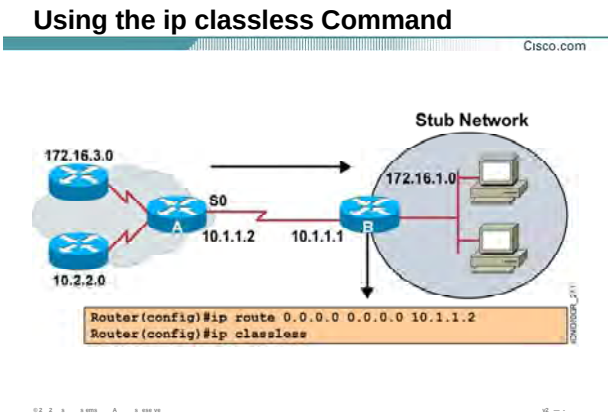
از میان Dynamic Routing Protocol ها RIP و IGRP جزء پروتکل های Distance-Vector و OSPF جزء پروتکل های Link-State به حساب می آید . سوالی که اینجا مطرح می شود اینست که چرا به EIGRP در این جدول پروتکل Distance-Vector پیشرفته گفته شده ، در حالی که پیش از این آن را جزء پروتکل های Hybrid معرفی کردیم ؟

در واقع هر دو گفته درست می باشد . زیرا همانطور که گفته شد EIGRP پروتکلی است که خواص مفید دو دسته دیگر یعنی Link-state و Distance-Vector را دارد. بنابراین به این پروتکل Distance-Vector پیشرفته نیز گفته می شود.

همانطور که مشاهده می کنید IGRP و EIGRP جزء پروتکل های مسیریابی مخصوص به Cisco می باشد.

از میان routing protocol های Dynamic تنها EIGRP و OSPF و IS-IS ، VLSM را ساپورت می کنند.

Convergence Time: به مدت زمانی که پروتکل مسیریابی روی Domain به حالت پایدار می رسد گفته می شود. در این حالت هر روتر بهترین مسیرها به شبکه های غیرمحلی را پیدا کرده و آنها را در یک Database نگهداری می کند.



IP Classless و فعال کردن آن :

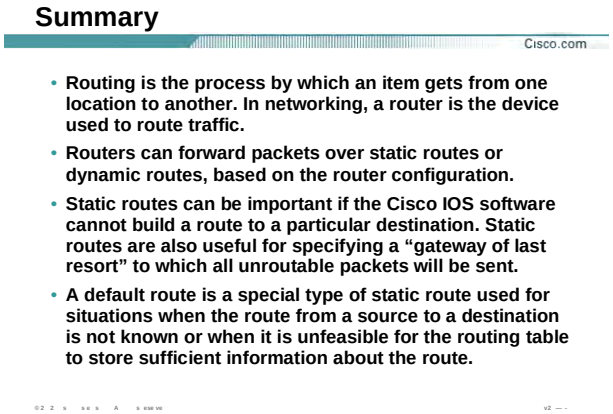
یک روتر شبکه های Connect به خود را براحتی می شناسد . بنابراین درصورتی که پکتی مقصدش یکی از شبکه های Connect باشد آنرا هدایت می کند.

روترهای Classful در صورتی که پکتی را دریافت کنند که مقصد آن به غیر از شبکه های Connect باشد ، پکت را Drop می کنند .

در صورتی که روی روتر یک Default Route نیز تعریف شده باشد باز پکت Drop می شود.

این ویژگی باتنظیم IP Classless تغییر می کند. بنابراین در صورتی که پکتی آدرس مقصدش غیر از شبکه محلی و Connect باشد آن را Drop نمی کند . در این حالت به Routing Table که لیستی از شبکه های محلی و غیرمحلی می باشد نگاهی انداخته می شود و درصورتی که مسیری به آن مقصد در این Table موجود باشد پکت به اینترفیس مربوطه هدایت می شود تا به مقصد هدایت شود.

IP Classless به صورت پیش فرض روی روتر فعال است و در غیر این صورت با فرمان IP Classless در Global Mode می توانید آن را فعال کنید .



خلاصه :

روتر با شناخت کل شبکه و مسیرهای موجود درخواست هایی را که نتواند در شبکه محلی خود پیدا کند به بیرون هدایت می کند و آن را در مسیر مناسب قرار داده و هدایت می کند. بنابراین روتر ،Network های غیرمحلی را شناخته و آنها را در یک Routing Table نگهداری می کند. برای معرفی شبکه های غیر محلی به روترهای موجود در شبکه دو روش وجود دارد: static routing ، dynamic routing .

در روش اول Network های غیر محلی و راه دسترسی به هر کدام از آنها به صورت دستی معرفی می شود . درواقع شما به عنوان admin شبکه با شناخت از تک تک روتر ها و مسیرهای رسیدن به هر کدام و به صورت کلی با شناخت از ساختار کل شبکه ، خودتان عملیات مسیردهی به هر کدام از شبکه های غیر محلی را انجام می دهید.

در روش دوم این شناخت به کمک الگورتیم های مسیریابی که در ادامه با آنها آشنا می شوید صورت می پذیرد.در واقع در این روش عملیات مسیریابی به صورت اتوماتیک انجام می گیرد .

Default route با تعریف یک مسیر به تمامی شبکه های غیر محلی، پکتی که آدرس مقصدش جای دیگری به غیر از شبکه محلی باشد را مسیر دهی کرده و از این شبکه خارج می کند تا توسط روترهای دیگر مسیردهی شده و به مقصد برسد.

درس دوم

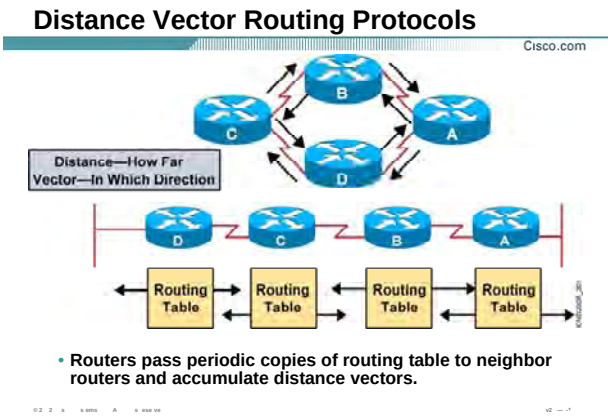
Distance Vector Roruting

هدف:

۱. آشنایی با عملکرد پروتکل های مسیریابی Distance Vector .

۲. آشنایی با نحوه رخ دادن Loop در شبکه هنگام استفاده از پروتکل های Distance Vector .

۳. آشنایی با روش های جلوگیری از Loop .



پروتکل های Distance Vector :

به الگوریتمی که پروتکل های Distance Vector با آن کار می کنند Bellman-Ford گفته می شود . به صورت کلی عملکرد این الگوریتم را می توان به صورت زیر ان کرد.

۱. شناسایی شبکه های connect به رو ر .

۲. ساختن Routing Table .

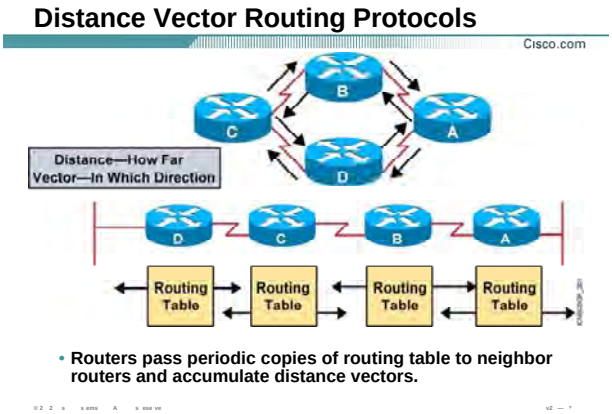
۳. شناسایی روترهای مجاور .

۴. تبادل کل Routing Table با روترهای مجاور بعد از سپری شدن گام سوم.

۵. Periodic Update.

در پروتکل های Distance Vector ، بین روتر مبدا و شبکه غیرمحلی که به روتر Connect نیست یک بردار خطی در نظر گرفته می شود . مبداء این بردار خود روتر و بعد از گذشتن از یکی از روتر های مجا ر به شبکه مقصد می رسد.

بنابراین روتر ابتدا باید بداند که برای رسیدن به شبکه مقصد چند راه وجود دارد و سپس از میان راههای موجود بهترین راه را مشخص کرده و آن را در Routing Table قرار دهد.



پروتکل های Distance Vector (ادامه):

شناسایی شبکه های connect به روتر :

بعد از فعال کردن Routed Protocol ایی چون پروتکل IP روی اینترفیس ها و up شدن اینترفیس ، روتر شبکه هایی را که هر کدام از این اینترفیس های up در آن قرار دارند را به عنوان شبکه connect در نظر می گیرد .

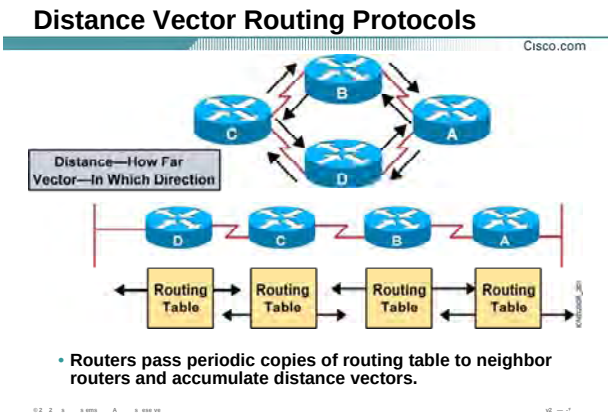
ساختن Routing Table :

مرحله اول شناسایی شبکه های connect به روتر می باشد . بعد از این که شبکه های connect به روتر شناسایی شدند ، در Routing Table به صورت route های Connect نشان داده می شوند .

شناسایی روترهای مجاور :

بعد از این که شبکه های connect به یک روتر شناسایی و در Routing Table قرار گرفتند ، روتر Update ایی را از تمامی اینترفیس هایش به خارج از روتر ارسال می کند. این Update شامل اطلاعات موجود در Routing Table روتر جدید ، یعنی شبکه های connect به روتر می باشد .

Update ها در پروتکل RIP به آدرس 255.255.255.255 و در پروتکل IGRP به آدرس 224.0.0.9 ارسال می شود.

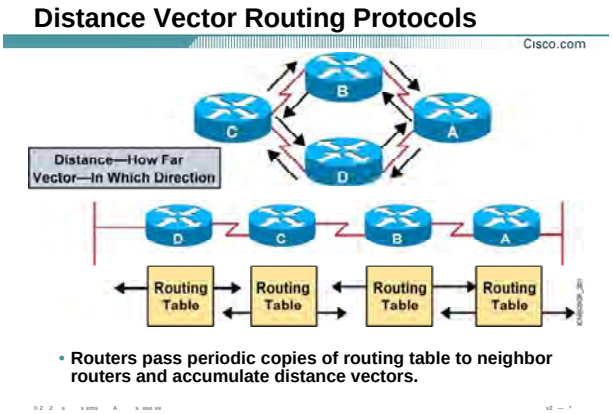


پروتکل های Distance Vector (ادامه):

روترهای مجاور این Update را دریافت می کنند و سپس پروتکل مسیریابی را که این Update آن را معرفی می کند با پروتکل مسیریابی خود مقایسه می کنند .

درصورت یکسان بودن پروتکل ها ، روتر مجاور Update ایی را که شامل کل اطلاعات موجود در Routing Table اش می باشد به روتر درخواست کننده به صورت Unicast ارسال می کند .

بنابراین هر کدام از روترها اطلاعات اولیه را به این روش گرفته و با پردازش مجدد روی این اطلاعات و بعد از اعمال تغییرات لازم در Routing Table درج می کند.

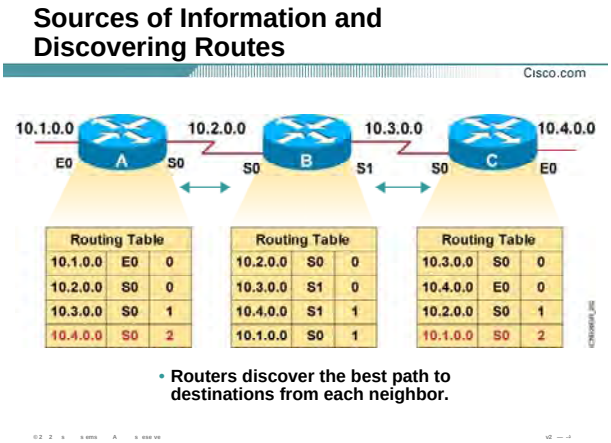


پروتکل های Distance Vector (ادامه):

اما کار به اینجا ختم نمی شود . هر کدام از روترها می بایست که اطلاعات خود و یا به عبارتی Routing Table خود را Update نگه دارند .

برای این منظور Update هایی در فواصل زمانی معین از طریق اینترفیس های Connect بسته به نوع Routing Protocol ، Broadcast یا Multicast می شود . در صورتی Update ایی که روتر دریافت می کند حامل اطلاعات جدیدی بوده و با محتویات Routing Table متفاوت باشد ، این اطلاعات در Routing Table درج می شود .

تغییر در هر روتر روی روترهای مجاورش تأثیر می گذارد . بنابراین یک تغییر روی یک روتر روی روترهای دیگر به صورت زنجیره ای تأثیر می گذارد . در واقع با تغییر کردن Routing Table مربوط به یک روتر تغییرات به صورت دست به دست منتقل می شود .



تکمیل Routing Table در Distance Routing Protocol :

به این شکل توجه کنید . فرض کنید برروی روتر B و روتر C یکی از پروتکل های مسیریابی Distance-Vector تنظیم شده باشد و ما می خواهیم روتر A را نیز وارد شبکه کرده تا با پروتکل مشترک با بقیه روترها شروع به کار کند.

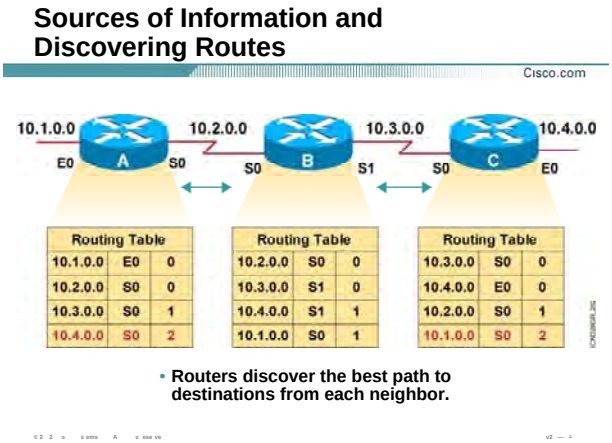
بعد از اینکه پروتکل مسیریابی روی روتر A فعال شد ، همانطور که در مورد الگوریتم پروتکل های مسیریابی distance-Vector گفته شد ، اولین مرحله شناخت شبکه های متصل به خود روتر می باشد .

بنابراین روتر A ابتدا از طریق اینترفیس هایی که up هستند شبکه های connect به خود را شناسایی کرده و آنها را در Routing Table خود به صورت route های connect و با متریک (تعداد گام) صفر نمایش می دهد.

سوالی که اینجا پیش می آید اینست که متریک چیست؟

متریک معیار و یا ملاکی برای انتخاب بهترین مسیر در بین مسیرهایی که توسط یک Routing Protocol شناسایی شده اند ، می باشد. در ادامه با این مفهوم بیشتر آشنا می شویید . فرض کنید در این مثال این معیار ، تعداد گام یا hope count باشد. بنابراین تعداد گام برای رسیدن به شبکه های connect به یک روتر صفر خواهد بود.

همانطور که Routing Table مربوط به روتر A را مشاهده می کنید ، شبکه های connect به روتر A به صورت Route هایی با متریک (تعداد گام) صفر نمایش داده شده است .

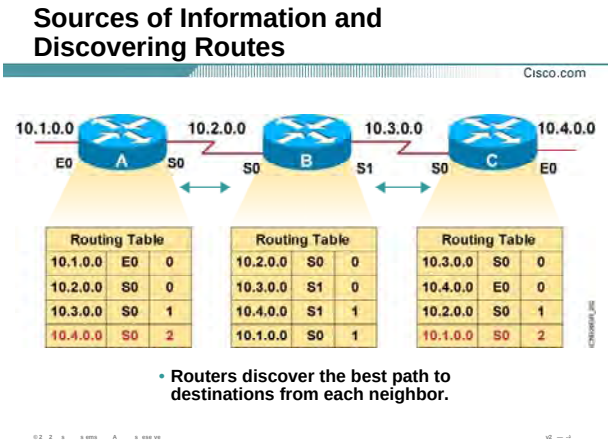


تکمیل Routing Table در Distance Routing Protocol (ادامه):

روتـر بعـد از شناســایی شــبکه هــای Connect و ســاختن Routing Table خــود ، یــک پکــت Update بــه آدرس 255.255.255.255 در پروتکل RIP و به آدرس 224.0.0.9 در پروتکل IGRP و از تمامی اینترفیس های فعال خود بـه خـارج ارسال می کند . در این مثال روتر A ، Broadcast Packet را از اینترفیس هـای E0 و S0 ارسـال مـی کنـد. روتـر B بعـد از دریافت این پکت ، Update ایی را که شامل تمامی رکوردهای Routing Table خود مـی باشـد ،بـه روتـر A ارسـال مـی کند . روتر A این Update را با رکوردهای موجود در Routing Table خود مقایسه می کند . از آنجایی که روتر A به غیـر از شبکه های Connect هیچ شبکه دیگری را نمی شناسد ، بنابراین این اطلاعات را بعد از انجام تغییرات لازم چون متریک در Routing Table خود درج می کند. به طور مثال روتر B شبکه 10.3.0.0 را با متریک (تعداد گـام) صـفر مـی بینـد . در حالی که روتر A هیچ رکوردی در مورد این شبکه ندارد . بنابراین لازم است که در Routing Table خود درج کند.

اما روتر A شبکه 10.3.0.0 را با چه متریکی می تواند ببیند ؟

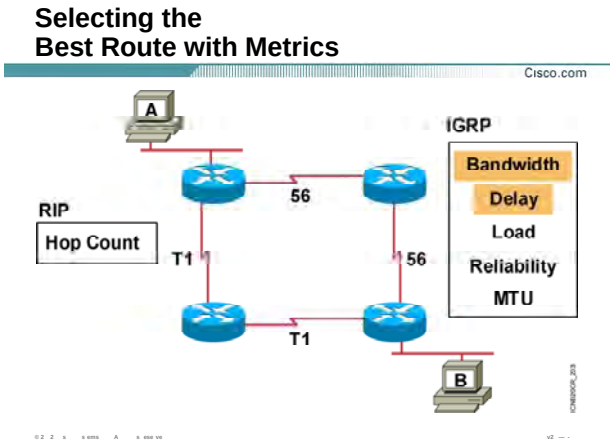
روتر B شبکه 10.3.0.0 را با متریک صفر گزارش داده است . از طرفی فاصله بین روتر B و روتر A ، یـک گـام مـی باشـد . در واقع روتر A با یک گام به جلو رفتن بـه روتـر B مـی رسـد . بنـابراین بـا یـک گـام حرکـت کـردن مـی توانـد بـه شـبکه 10.3.0.0 دسترسی داشته باشد . و روتر A شبکه 10.3.0.0 را با متریک یک در Routing Table خود درج می کند .



تکمیل Routing Table در Distance Routing Protocol (ادامه):

به همین ترتیب در مورد شبکه های دیگری که در Routing Table خود موجود نباشد عمل می کند .

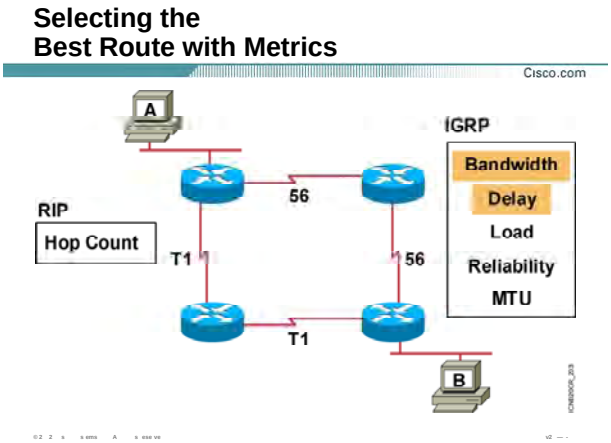
بعد از Convergence شدن شبکه و رسیدن به حالت پایدار ، هر کدام از روترها Update هایی را در فواصل زمانی مشخص ارسال می کنند . در واقع ویژگی اصلی پروتکل های مسیریابی Distance-Vector این است که full Update به تمامی روتر های مجاورش به صورت periodic ارسال می کند. حتی اگر تغییری در شبکه رخ نداده باشد باز این Update به صورت Full ارسال می شوند و این ترافیکی را به شبکه تحمیل می کند.



انتخاب بهترین مسیر به کمک متریک :

متریک : معیار و ملاکی برای انتخاب بهترین مسیر در میان مسیرهایی که با یک پروتکل مسیریابی تعیین شده اند می باشد . در واقع انتخاب بهترین مسیر در میان مسیرهای مختلف به یک شبکه غیر محلی می باشد که متریک یکسان ولی مقادیر هر کدام از مسیرها متفاوت است . در واقع همانطور که متر واحد اندازه گیری مسافت است ، متریک واحد اندازه گیری مسیر می باشد . بنابراین زمانی که واحد اندازه گیری تمامی مسیرها یکسان باشد ، براحتی می توان انتخاب کرده و بهترین مسیر در میان آنها را مشخص کرد . پروتکل های Dynamic هر کدام دارای متریک متفاوتی هستند . متریک در RIP یک متغیره و فقط hop count می باشد ، در حالی که در IGRP متریک مرکب و چند متغیره می باشد . در IGRP ، متریک ترکیبی از پنج فاکتور زیر می باشد:

۱. Bandwidth
۲. Delay
۳. Load
۴. Reliability
۵. MTU



انتخاب بهترین مسیر به کمک متریک :

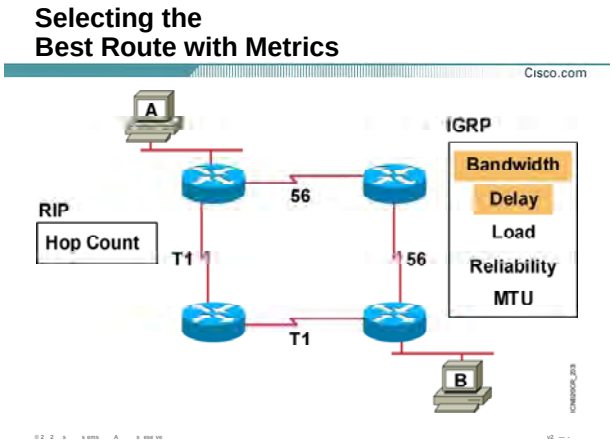
که به صورت پیش فرض فقط دو فاکتور اول ، یعنی Bandwidth و Delay در تعیین متریک در IGRP نقش دارند .

به صورت کلی بهترین مسیر در میان تمامی dynamic Protocol ها ، مسیری است که متریک کمتر داشته باشد.

بنابراین در RIP مسیری بهتر است که تعداد گام کمتری برای رسیدن به شبکه غیرمحلی می پیماید .

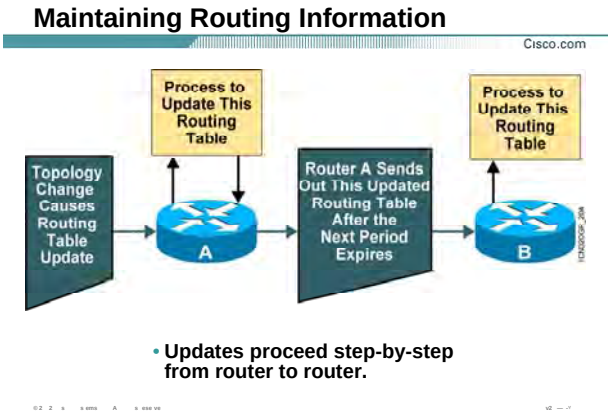
در IGRP متریک رابطه معکوس با bandwidth دارد . یعنی هر چه پهنای باند یک مسیر بیشتر باشد متریک مسیر کمتر می شود . در IGRP با فرض ثابت ماندن فاکتورهای دیگر ، مسیری که در مقایسه با مسیرهای دیگر bandwidth بیشتری داشته باشد ، متریک کمتر خواهد داشت و در نتیجه مسیر بهتری خواهد بود . با متریک IGRP و فاکتورهای آن در مبحث IGRP به خوبی آشنا خواهید شد . بنابراین نگران مبهم بودن این فاکتورها نباشید و برای یادگیری آنها تا پایان این ماژول با من همراه شویید.

در شکل بالا در صورتی که روی تک تک روترها پروتکل RIP فعال باشد، برای رسیدن از نقطه A به نقطه B ، دو مسیر وجود دارد . از آنجایی که متریک در RIP ، hop count می باشد و هر دو مسیر دارای متریک یکسان با مقدار 2 می باشد ، بنابراین هر دو مسیر به عنوان مسیر اصلی انتخاب می شود.



انتخاب بهترین مسیر به کمک متریک :

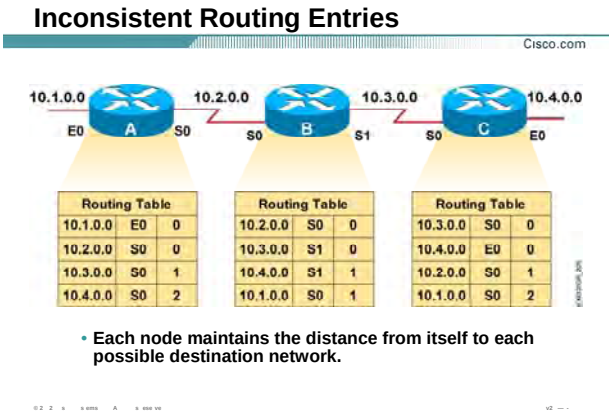
فرض کنید روی تک تک روترها پروتکل مسیریابی IGRP فعال باشد . همانطور که می دانید متریک در IGRP به صورت default به دو فاکتور bandwidth و delay بستگی دارد . با فرض ثابت بودن فاکتور delay در این مثال ، مسیری که پهنای باند بیشتری داشته باشد به عنوان بهترین مسیر انتخاب می شود . بنابراین مسیر با پهنای باند T1 به عنوان بهترین مسیر انتخاب می شود .



Routing Table و وظیفه آن :

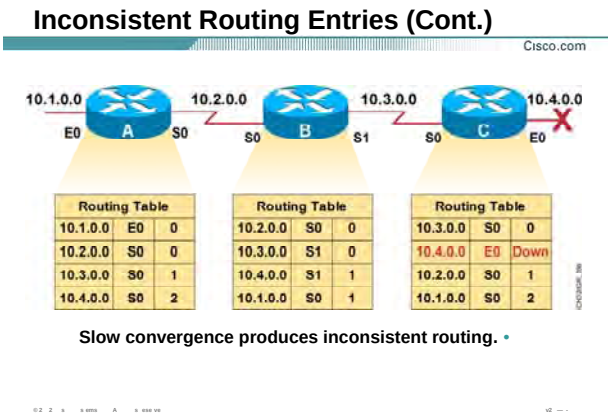
همانطور که تا به اینجا متوجه شدید ،در پروتکل های مسیریابی Distance-Vector هر روتر فقط با روترهای مجاورش به تبادل اطلاعات می پردازد . د واقع بعد از ساخته شدن Routing Table ، روتر در فواصل زمانی مشخص محتویات Routing Table اش را به صورت کامل به روترهای مجاورش گزارش می دهد. هر روتر بعد از گرفتن Update ، اطلاعات جدید را با رکوردهای Routing Table خود مقایسه می کند و در صورتی که تغییری را مشاهده کند ، پس از اعمال تغییرات لازمه چون تغییر متریک در Routing Table خود درج می کند . به این شکل توجه کنید:

روتر A ، Update ایی را دریافت می کند . بنابراین این Update را با محتویات درون Routing Table خود مقایسه می کند. این Update حامل تغییراتی در توپولوژی شبکه می باشد . بنابراین روی Routing Table مربوط به روتر A تأثیر می گذارد . بعد از اینکه روتر A خود را Update کرد ، می بایست این تغییرات را به روتر های مجاورش گزارش دهد . بنابراین بعد از به پایان رسیدن زمان انتظار Periodic Update Time این اطلاعات را به روترهای مجاورش گزارش می دهد.



بررسی رخ دادن Loop در یک مثال :

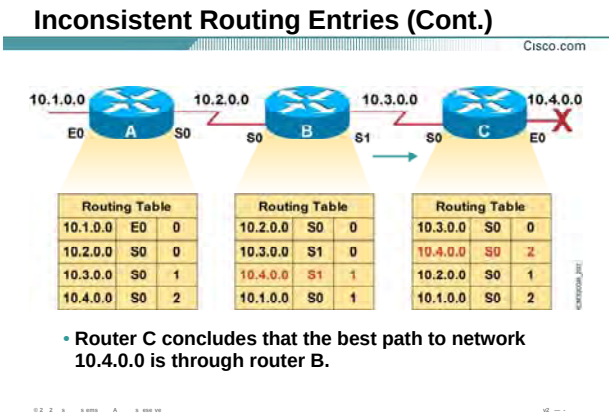
به این شکل و Routing Table های هر کدام از روترها توجه کنید . همانطور که مشاهده می کنید هر روتر علاوه بر شبکه Connect ، شبکه های غیر محلی را شناخته و آن را در Routing Table خود درج کرده است .



بررسی رخ دادن Loop در یک مثال (ادامه):

فرض کنید روتر C یک Full Update به تمامی روترهای مجاورش ارسال کند و بلافاصله بعد از ارسال Full Update ، ما اینترفیس E0 از روتر C را Shut down کنیم . می خواهیم تأثیر down شدن یک network را روی کل شبکه و روی روترهای دیگر بررسی کنیم.

به Routing Table مربوط به روتر C نگاه کنید . این تغییر بلافاصله روی Routing Table روتر C تأثیر گذاشته است . اما روتر های دیگر هنوز دسترسی به شبکه 10.4.0.0 را از طریق روتر C می دانند .

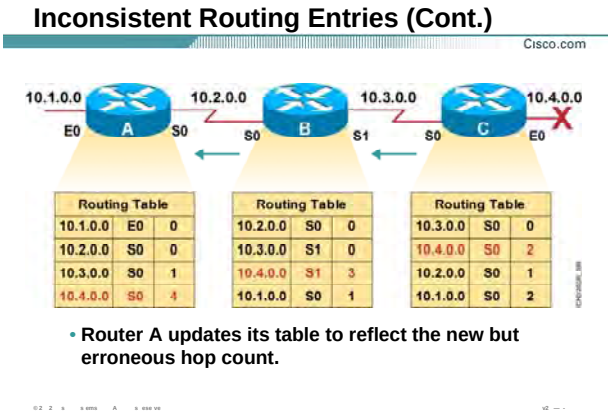


بررسی رخ دادن Loop در یک مثال (ادامه) :

در این لحظه روتر B پکتی را دریافت می کند که آدرس مقصد آن شبکه 10.4.0.0 می باشد . روتر B در Routing Table خود مسیری از طریق اینترفیس s1 با متریک یک به شبکه 10.4.0.0 دارد .

فرض کنید زمان ارسال Periodic Update روتر B فرا رسیده باشد. در این لحظه روتر B یک Full Update به تمامی روترهای مجاورش ارسال می کند . بنابراین روتر C می بایست Routing Table خود را Update کند . زیرا این Update شبکه 10.4.0.0 را به روتر C معرفی می کند . لذا شبکه 10.4.0.0 را که از Routing Table اش حذف کرده بود به آن اضافه می کند . اما روتر B شبکه 10.4.0.0 را با متریک یک به روتر C گزارش داده است ، لذا روتر C این شبکه را با یک گام بیشتر یعنی متریک دو خواهد دید .

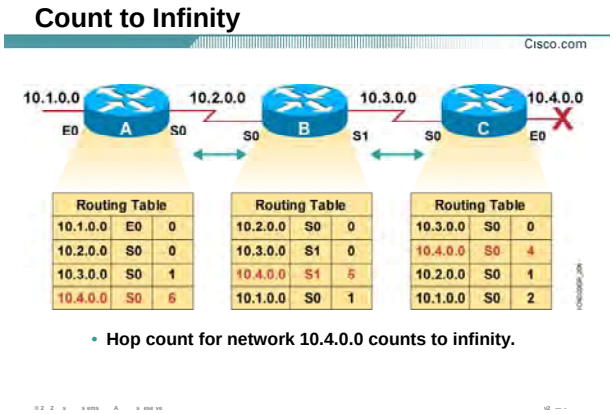
در واقع روتر C دسترسی به شبکه 10.4.0.0 را از طریق روتر B می داند ، این درحالی است که چنین شبکه ایی Down شده و هیچ کدام از روترها به آن دسترسی ندارند.



بررسی رخ دادن Loop در یک مثال (ادامه) :

روتر B به محض Update کردن Routing Table خود ، این تغییرات را به روترهای مجاورش Advertise می کند .روتر B ، Update ایی را که دریافت می کند با Routing Table خود مقایسه می کند . بنابراین روتر C وقتی شبکه 10.4.0.0 را با متریک دو ببیند ، روتر B که روتر مجاور روتر C می باشد باید با یک گام بیشتر به آن دسترسی داشته باشد . بنابراین شبکه 10.4.0.0 را با متریک 3 خواهد دید.

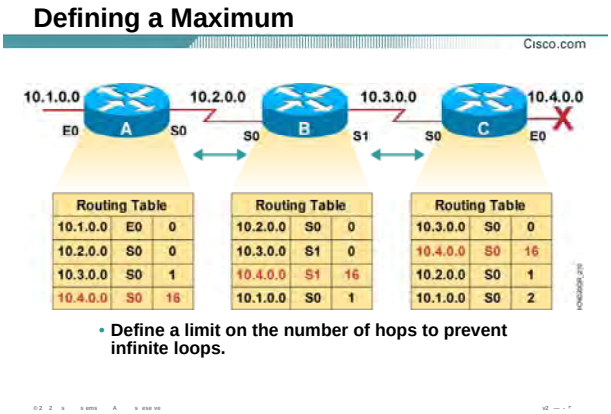
همانطور که متوجه شدید Update شدن Routing Table مربوط به هر کدام از روترها ، منجر به Update شدن روترهای دیگر می شود .



- **Hop count for network 10.4.0.0 counts to infinity.**

بررسی رخ دادن Loop در یک مثال (ادامه) :

درواقع یک اشتباه روی کل شبکه تأثیر گذاشته است و Routing Table هر سه روتر دارای اطلاعات اشتباه می باشد . این روند افزایش متریک روی تک تک روترها تأثیر گذاشته و باعث رشد متریک می شود . به این مشکل پیش آمده Count to Infinity گفته می شود .

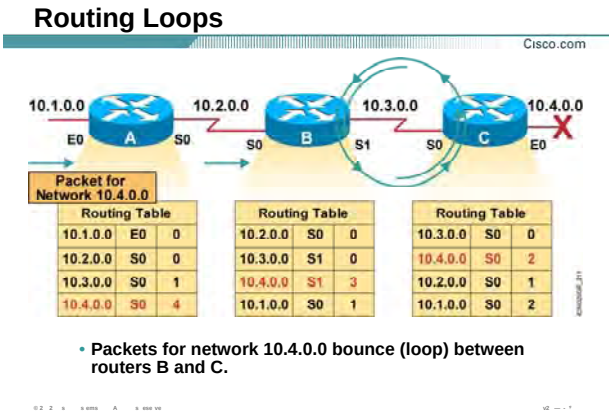


بررسی رخ دادن Loop در یک مثال (ادامه) :

همانطور که متوجه شدید این روند افزایش متریک بدون هیچ محدودیتی در حال افزایش است . بنابراین لازم است که یک maximum مقدار برای رشد متریک در نظر گرفته شود تا در صورتی که متریک روی یک روتر به این مقدار رسید ، روتر متوجه مشکل Count to Infinity شده و به ادامه این روند پایان دهد .

به طور مثال در پروتکل مسیریابی RIP که دارای متریک hop count می باشد maximum مقدار برای متریک مقدار 16 می باشد .

این بدان معنی است که وقتی متریک یک Network برابر با 16 شد ، این شبکه به عنوان یک شبکه غیرقابل دسترس (Unreachable)درنظر گرفته می شود و روند افزایش متریک متوقف می شود .

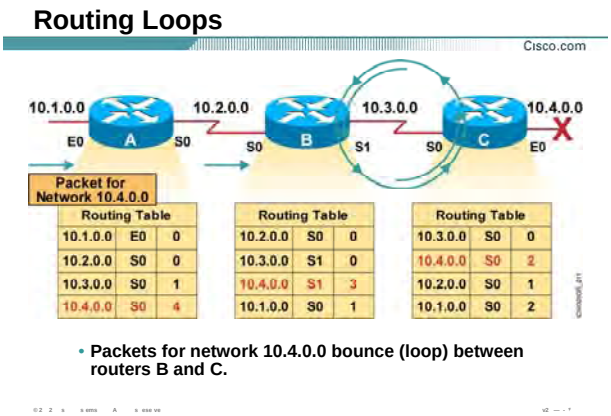


بررسی رخ دادن Loop در یک مثال (ادامه) :

تا به اینجا با مشکل افزایش متریک تا بی نهایت آشنا شدید . اما مشکل دیگری که در شبکه ممکن است رخ دهد Routing loop می باشد .

همانطور که در شکل مشاهده می کنید روتر A یک پکت با مقصد شبکه 10.4.0.0 را دریافت می کند . روتر A با توجه به اطلاعات موجود در Routing Table اش ، آن را به سمت روتر B هدایت می کند . روتر B با نگاه کردن به Routing Table اش ، پکت را از اینترفیس S1 به سمت روتر C هدایت می کند و روتر C نیز با نگاه کردن به Routing Table اش ، پکت را از اینترفیس S0 به سمت روتر B هدایت می کند . این روند ادامه پیدا می کند . درواقع پکت بین روتر B و روتر C درون یک loop قرار می گیرد و درواقع ترافیک بیهوده ای روی لینک ارتباطی این دو روتر و شبکه تحمیل شده است.

رخ دادن loop در شبکه یکی از معایب الگوریتم distance-vector می باشد . اما این بدان معنی نیست که هیچ روشی برای جلوگیری و یا شکستن loop وجود ندارد.

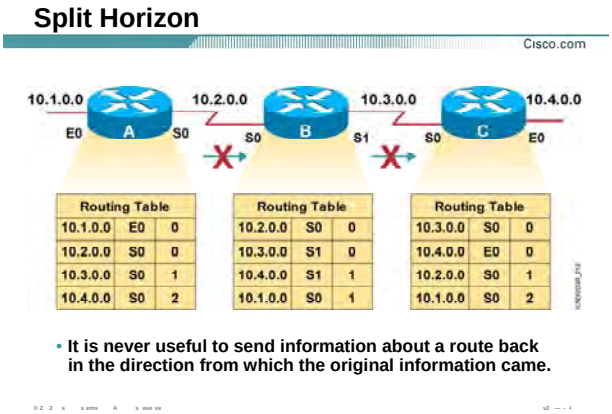


- **Packets for network 10.4.0.0 bounce (loop) between routers B and C.**

بررسی رخ دادن Loop در یک مثال (ادامه) :

الگوریتم distance-vector با بکار بردن پنج روش زیر مانع از بروز loop در شبکه می شود .

۱. Split Horizon
۲. Route Poisoning
۳. Poison Reverse
۴. Holddown Timer
۵. Triggered Update



بررسی روشهای مهار کردن Loop :

تا به اینجا دیدیم که در صورت shut down شدن اینترفیس E0 چگونه بین روتر B و روتر C ، loop رخ می دهد . درواقع مشکل زمانی رخ می دهد که روتر C در مورد شبکه ای که خودش به روتر B خبر داده بود ، خبر می گیرد .

یعنی روتر B اطلاعاتی را که قبلا از روتر C گرفته بود به خودش تحویل می دهد و با این کار این روتر را دچار مشکل می کند . بنابراین راه حل چیست ؟

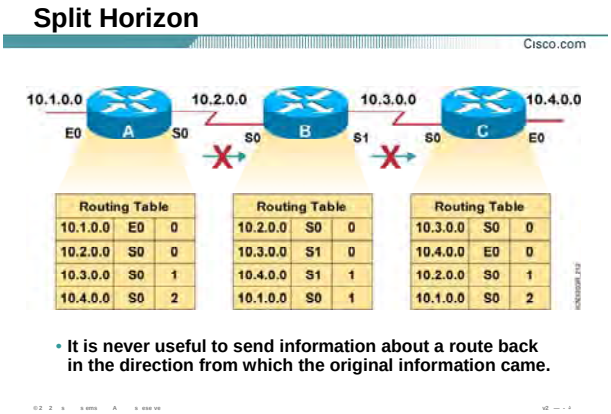
به زبان ساده ، کافی است که یک روتر اطلاعاتی را که از روتر دیگر گرفته به وی تحویل ندهد.

مثلا در این شکل روتر C شبکه 10.4.0.0 را به روتر B گزارش داده است . بنابراین روتر B این اجازه را ندارد که در Full Update ، شبکه 10.4.0.0 را به روتر C گزارش دهد.

فرض کنید که لینک E0 در روتر C قطع شود . روتر C ، Routing Table خود را Update می کند . فرض کنید در روتر C زمان ارسال Full Update فرا نرسیده باشد تا این تغییرات را به روترهای مجاور گزارش دهد .

در این لحظه روتر C ، Update ایی را از روتر B دریافت می کند . این Update حامل اطلاعاتی می باشد که روتر B پیش از این آنها را از روتر C نگرفته است . درواقع روتر B اطلاعاتی را که قبلا از C گرفته را دیگر به خودش تحویل نمی دهد .

بنابراین در مورد شبکه 10.4.0.0 هیچ گزارش نادرستی که قبلا منجر به loop می شد به روتر C داده نمی شود .



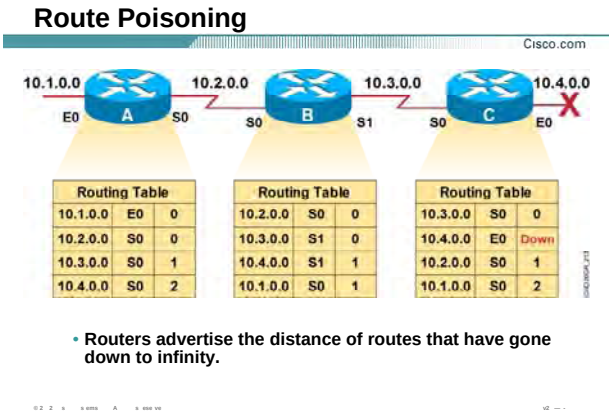
بررسی روشهای مهار کردن Loop :

به این روش که یکی از روشهای جلوگیری از loop بین دو روتر مجاور در شبکه می باشد ، روش Split Horizon گفته می شود .

نکته : روش Split Horizon فقط loop بین دو روتر مجاور را می شکند و loop ایی که در شبکه رخ دهد و بین دو روتر مجاور نباشد را از بین نمی برد.

به طور مثال در صورتی که loop بین روتر C و روتر A رخ دهد این وش نمی تواند loop رخ داده شده را در شبکه از بین ببرد .

در صورتی که یکی از پروتکل های مسیریابی Dist nce-Vector روی روتر فعال شود ، روش Split Horizon به صورت اتوماتیک و بدون نیاز به تنظیم روی روتر فعال می شود. به کمک فرمان no ip split horizon می توانید آن را روی روتر غیرفعال کنید .



بررسی روشهای مهار کردن Loop :

روش split horizon سه نوع می باشد:

۱. simple split horizon

۲. route poisoning

۳. split horizon with poison reverse

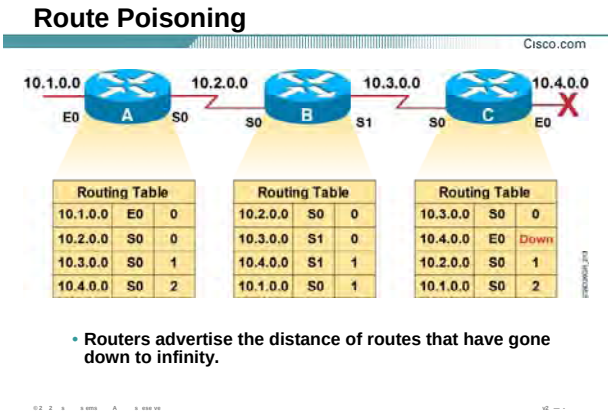
Simple split horizon روشی بود که تا به اینجا با آن آشنا شدید ، درواقع در این روش هر روتر اطلاعاتی را که از یک روتر گرفته بود به وی تحویل نمی دهد.

اما دو روش دیگر چگونه عمل می کند ؟

:Route Poisoning

به شکل بالا توجه کنید . فرض کنید که اینترفیس E0 در روتر C را به صورت دستی shut down کنیم . بنابراین روتر C این تغییر را در Routing Table خود اعمال می کند .

Route Poisoning می گوید بعد از اینکه شبکه ای down شد ، از Routing Table روتر حذف نشود . بلکه این شبکه را با متریک بی نهایت (infinity) در Routing Table خود اصلاح می کند .

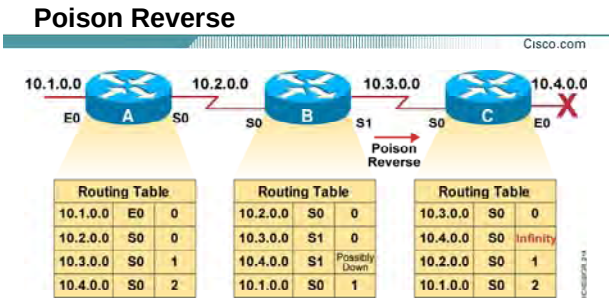


بررسی روشهای مهار کردن Loop (ادامه):

بنابراین با Update شدن Routing Table قبل از فرا رسیدن زمان ارسال full Update ، Unreachable شدن شبکه Down شده را به روترهای مجاورش گزارش می دهد .

روتر های مجاور که این Update را دریافت می کنند ، این Network را از Routing Table شان حذف نمی کنند بلکه تا به پایان رسیدن زمان Holddown timer در Routing Table خود نگهداری می کنند.

توجه داشته باشید که در Routing Table و در کنار شبکه ای که Down شده ، نوشته Possibly Down قرار می گیرد که بیانگر اینست که این شبکه Unreachable بوده ولی هنوز از Routing Table این روتر حذف نشده است .



Poison reverse overrides split horizon. •

بررسی روشهای مهار کردن Loop :

Split horizon with poisoning reverse:

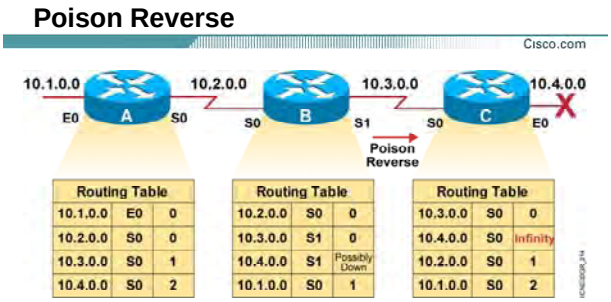
نمونه پیشرفته split horizon می باشد. در این روش برخلاف split horizon ، خبری را که در مورد یک network از یک روتر دریافت کرده به خودش بر می گرداند اما با متریک بی نهایت .

منطق این روش بر این بوده است که شنیدن **خبر بد بهتر از بی خبری** است .

به طور مثال روتر B در Full Update خود شبکه 10.4.0.0 را با متریک بی نهایت به روتر C گزارش می دهد . برخلاف روش split horizon که در مورد شبکه 10.4.0.0 به روتر C هیچ گزارشی نمی دهد .

به این شکل توجه کنید . اینترفیس E0 از روتر C را به صورت دستی shutdown کرده ایم . بنابراین متریک این Route در روتر C به بی نهایت تبدیل می شود . روتر C بی نهایت شدن این Route را به روترهای مجاورش گزارش می دهد . روتر B که این Update را دریافت کرد بلافاصله Update ایی را مبنی بر اینکه روتر B شبکه 10.4.0.0 را با متریک بی نهایت می بیند به روتر C بر می گرداند . درواقع روتر B خبر مسمومی را به روتر C در مورد شبکه 10.4.0.0 می فرستد.

سوالی که پیش می آید اینست که روتر C خود به روتر B بی نهایت شدن شبکه 10.4.0.0 را گزارش داده بود و چه لزومی دارد که روتر B این مورد را به روتر C یادآوری کند؟

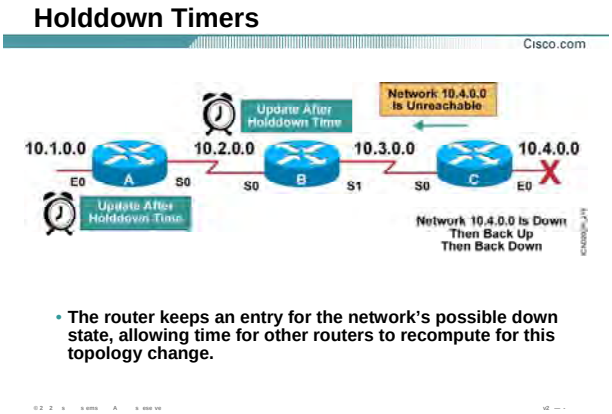


Poison reverse overrides split horizon. •

بررسی روشهای مهار کردن Loop (ادامه):

فرض کنید بلافاصله بعد از اینکه روتر C با یک Update بی نهایت شدن شبکه 10.4.0.0 را به روتر B گزارش داد ، Update ایی از طرف روتر B دریافت کند که شامل یک route به شبکه 10.4.0.0 با متریک بهتر باشد . زیرا روتر B قبل از شنیدن خبر بی نهایت شدن شبکه 10.4.0.0 این Update را به روتر C ارسال کرده است . درنتیجه مشکل loop در این قسمت از شبکه رخ می دهد.

بنابراین برای اطمینان بیشتر ، لازم است روتر B با فرستادن Update ایی به روتر C ، Inaccessible شدن شبکه 10.4.0.0 برای روتر B را به روتر C گزارش دهد .

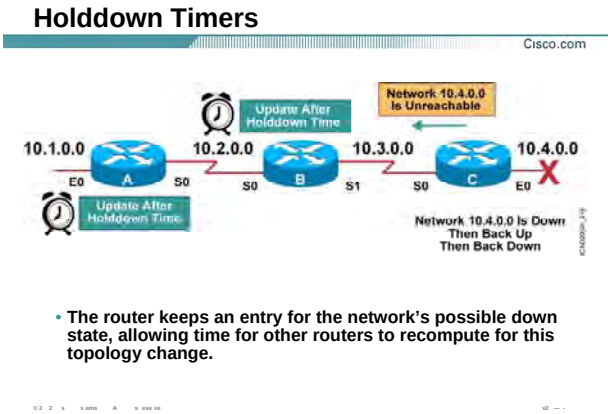


بررسی روشهای مهار کردن Loop :

تا به اینجا با چند روش جلوگیری از رخ دادن Loop در شبکه آشنا شدید ، یکی دیگر از روشهای جلوگیری از بروز Loop در شبکه Holddown Timer می باشد .

Holddown Timer به روتر می گوید در مورد یک network اگر خبر بدی شنیدی به حالت Hold رفته و در طول مدت زمانی که برای holddown timer در نظر گرفته شده هر خبر بد دیگری را در مورد این Network شنیدی به آن توجه نکن . این زمان سه برابر periodic Update می باشد.بنابراین در پروتکل مسیریابی RIP این زمان 180 ثانیه و در IGRP این زمان 270 ثانیه می باشد . اما Holddown timer چگونه عمل می کند:

- اگر روتری از روتر مجاورش Update ایی را دریافت کند که این Update اشاره کند به network ایی در شبکه که هم اکنون غیر قابل دسترس شده ، در این حالت روتر گیرنده Update با به کار بردن واژه possibly down در کنار این network در Routing Table اش به حالت hold رفته و Holddown Timer ، start می شود. بنابراین تا به پایان رسیدن این زمان هر خبر بد دیگری را در مورد این شبکه نشنیده گرفته و آن را ignore می کند .

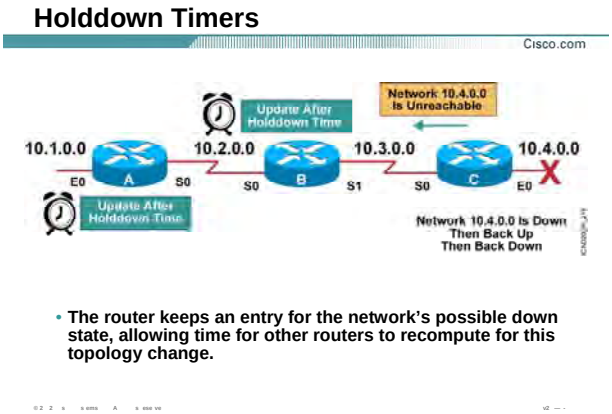


بررسی روشهای مهار کردن Loop (ادامه):

- در صورتی که زمان Holddown timer به پایان نرسیده باشد و در طول این زمان روتر Update ایی را از روتر مجاورش دریافت کند که حاوی مسیری به network علامت زده شده با متریک بهتر باشد ، دراین حالت روتر از حالت hold خارج شده و این Update را در Routing Table خود اعمال می کند .

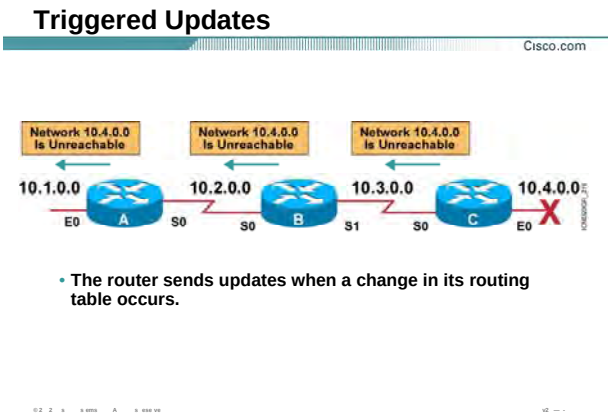
- همانطور که می دانید در صورتی که تغییری در شبکه رخ دهد و این تغییر بخواهد در کل شبکه پخش شود مدت زمانی طول می کشد و همه روترها همزمان از این تغییر آگاه نمی شوند . بنابراین ممکن است که یک روتر از یکی از روترهای مجاورش در دسترس نبودن یک network را بشنود . بنابراین وارد حالت hold شده و در طول این زمان از روتر مجاور دیگرش مسیری با همان متریک قبلی یا بدتر از آن دریافت می کند . این بدان معنی است که این تغییر هنوز در کل شبکه پخش نشده است . بنابراین روتر این Update را Ignore کرده و به آن توجه نمی کند .

نکته : روش Route Poisoning با Holddown Timer عمل می کند . یعنی زمانی که یک Network غیرقابل دسترس شد ، روتر بعد از Update کردن Routing Table خود و تبدیل متریک این Network به Infinity با توجه به روش Route



بررسی روشهای مهار کردن Loop (ادامه):

Poisoning آن را به روتر های مجاورش گزارش می دهد . روتری که این Update را دریافت کند چون این Update حـاوی این Network با متریک بیشتر است ، بنابراین روتر وارد حالت Holddown شده و این Network را در Routing Table اش با واژه Possibly Down علامت می زند .



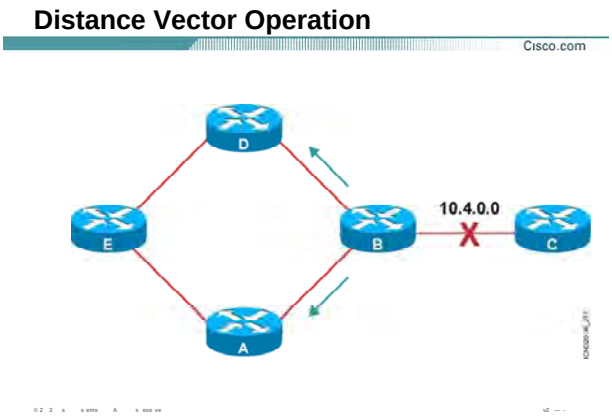
بررسی روشهای مهار کردن Loop :

همانطور که تا به اینجا دیدید مشکل اصلی بروز Loop در شبکه به علت Periodic بودن Update ها در پروتکل های مسیریابی Distance-Vector می باشد . درواقع Down شدن یک Network با تأخیر در شبکه اطلاع داده می شد.

به صورت نرمال در الگوریتم Distance-Vector ، روتر به صورت Periodic جدول مسیریابی خودش را به روترهای همسایه ارسال می کند . اما در روش Triggered Update در صورتی که Routing Table یک روتر تغییر کند ، تغییرات بلافاصله به روترهای همسایه گزارش داده می شود .

این تغییرات دست به دست منتقل می شود . درواقع این تغییرات مانند موجی در قسمتی از شبکه که مسیری به Network قطع شده داشته است منتقل می شود .

از طرفی Triggered Update را زوج مکمل Holddown Timer در نظر می گیرند . زیرا روترها زمانی که به حالت hold می روند و هر Update با متریک بد یا بدتر را قبول نمی کنند ، triggerd Update فرصت این را دارد که down شدن یک Network را در کل شبکه منتشر کند و مانع از وقوع loop در شبکه شود .

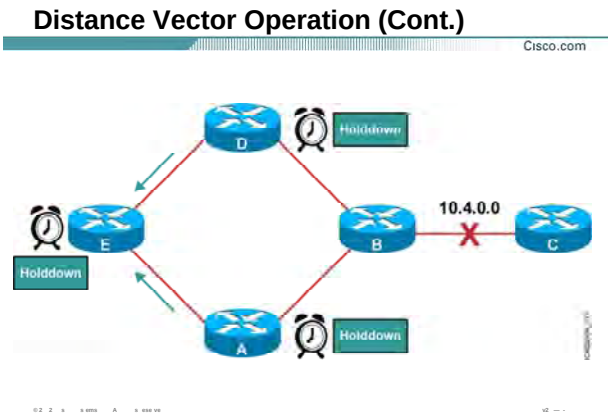


بررسی عملکرد Distance Vector در یک مثال:

تا به اینجا با تک تک روش های جلوگیری از Loop در شبکه آشنا شدید . در این قسمت به کمک یک شبکه نمونه می خواهیم ترکیب این پنج روش را در جلوگیری از Loop بررسی کنیم .

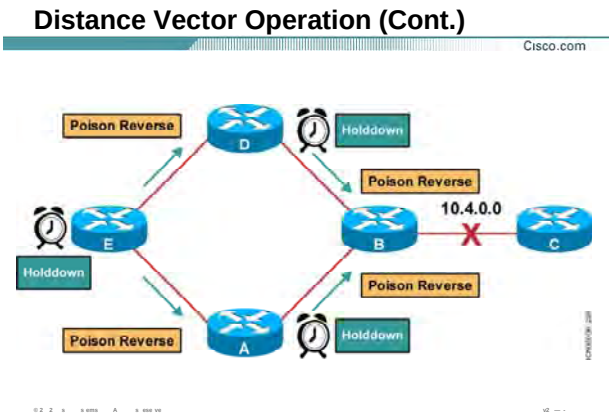
در این قسمت چهار روتر A ، B ، C و D هر کدام دو مسیر برای رسیدن به شبکه 10.4.0.0 دارند . فرض کنید شبکه 10.4.0.0 ای که متصل به روتر B می باشد Down شود . Route Poison می گوید درصورتی که Route ایی که از بین رفت آن را از Routing Table حذف نکن ، بلکه آن را با متریک Infinity در Routing Table اصلاح کن. بنابراین روتر B آن را در Routing Table اصلاح می کند . بعد از اصلاح شدنRouting Table ، Triggered Update این تغییرات را بلافاصله به روتر های مجاور گزارش می دهد .

بنابراین triggered Update به روتر D و روتر A گزارش می دهد که شبکه 10.4.0.0 با متریک بی نهایت دردسترس می باشد.



بررسی عملکرد Distance Vector در یک مثال:

بنابراین هر کدام از روترهای D و A ، متریکی بدتر از متریک سابق به شبکه 10.4.0.0 دریافت کرده اند . بنابه روش Holddown ، روتر A و D به حالت Hold رفته هر Update ایی که حامل متریک بد یا بدتر به این شبکه باشد را نشنیده گرفته و آن را Ignore می کنند . بنابراین در Routing Table شان شبکه 10.4.0.0 را با واژه Possibly Down علامت می زنند . بنابراین Triggered Update تغییرات یجاد شده در روتر A و روتر D را به روتر E می دهد . بنابراین روتر E نیز به حالت Hold رفته و Route به این شبکه را در Rout ng Table اش با واژه Possibly Down علامت می زند .

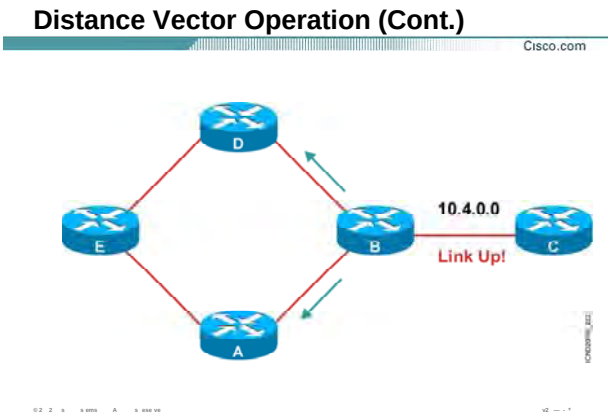


بررسی عملکرد Distance Vector در یک مثال:

همانطور که می دانید روش Split Horizon With Poison Reverse می گوید که بدخبری بهتر است از بی خبری .

بنابراین روتر A و D ، Update ایی را به روتر B می دهند که شبکه 10.4.0.0 غیرقابل دسترس (Inaccessible) می باشد .

روتر E نیز وقتی به حالت Hold رفت ، Update ایی را به روتر های D و A می فرستد و Inaccessible شدن شبکه 10.4.0.0 را به آنها خبر می دهد .

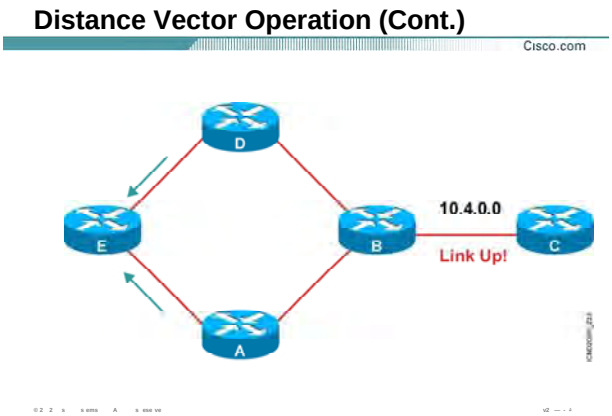


بررسی عملکرد Distance Vector در یک مثال:

همانطور که دید روترها در حالت Hold قرار می گیرند . در صورتی که تا به پایان رسدین زمان Holddown Timer خبر بهتری در مورد شبکه قطع شده نشنیدند، Route به شبکه قطع شده را به صورت کامل از شبکه حذف می کنند . اما در صورتی که قبل از به پایان رسیدن زمان Hold ، شبکه قطع شده up شود در این صورت تک تک روتر ها از حالت hold خارج می شوند.

در شبکه نمونه ای که تا به اینجا بررسی کردیم تمامی روتر ها به حالت hold رفتند.

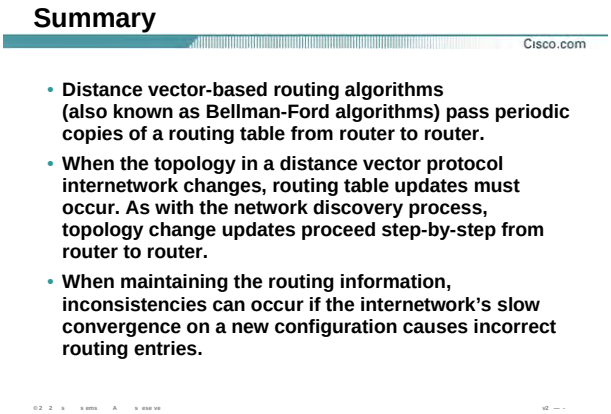
شبکه متصل به 10.4.0.0 به حالت up در می آید بنابراین روتر B خود را اصلاح کرده و Routing Table جدید را به روترهای مجاورش ارسال می کند.



بررسی عملکرد Distance Vector در یک مثال:

هر کدام از روترهایی که به حالت hold رفته بودند با شنیدن این Update ، از حالت hold خارج شده و در Routing Table شان واژه Possibly Down را از جلوی شبکه 10.4.0.0 برمی دارند.

بنابراین بعد از Update کردن Routing Table خود ، این خبر را به روتر های مجاورشان گزارش می دهند . و تمامی روترهایی که به حالت Hold رفته بودند از این حالت خارج می شوند.



خلاصه :

در این درس با الگوریتم Distance-Vector و عملکرد آن آشنا شدید . این الگوریتم همانطور که از نامش پیداست ، بین روتر مبدأ و شبکه مقصد برداری در نظر می گیرد . هر روتر فقط روترهای مجاورش را می شناسد . بنابراین هر روتر فقط با روتر های مجاورش به تبادل اطلاعات می پردازد. در واقع هر روتر با فرستادن Full Update که حاوی کل Routing Table اش می باشد روتر های مجاور را از وضعیت Network های موجود در شبکه آگاه می کند . ویژگی اصلی Update در الگوریتم Distance-Vector این است که حاوی مسیر به شبکه های مختلف می باشد . درواقع هر روتر به روتر مجاورش با فرستادن Update می گوید که من Network های مختلف را با چه متریکی می بینم.

یکی از مشکلات الگوریتم Distance-Vector وقوع Loop در شبکه می باشد.

علت اصلی این مشکل Periodic بودن Update ها در این الگوریتم می باشد. درواقع در صورتی که Network ایی Down شود ، این خبر به کندی در شبکه منتشر می شود و منجر به انتشار خبر نادرست در شبکه می شود . افزایش متریک تا بی نهایت نشانه وقوع loop در شبکه است . البته این بدان معنی نیست که این الگوریتم هیچ روشی برای از بین بردن Loop در شبکه به همراه ندارد بلکه پنج روش برای شناخت و حذف Loop به کار برده می شود .

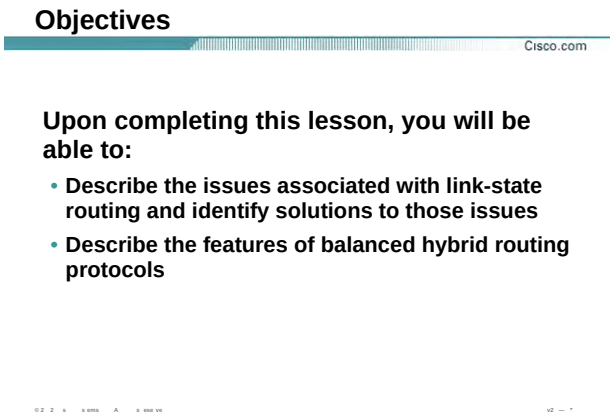
درس سوم :

Link State and Hybrid Routing

هدف :

۱. آشنایی با عملکرد پروتکل های مسیریابی Link state Routing .

۲. آشنایی با عملکرد پروتکل های مسیریابی Hybrid Routing .



مروری بر انواع Routing :

همانطور که تا به اینجا آشنا شدید ، Dynamic Routing Protocol ها به سه دسته عمده تقسیم می شوند:

۱. Distance Vector

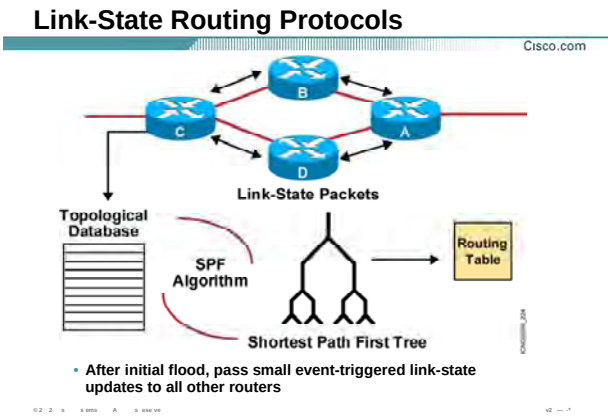
۲. Link State

۳. Hybrid

تا به اینجا با الگوریتم Distance-Vector و عملکرد آن آشنا شدید.

در این درس می آموزید که روتر هایی که با یکی از پروتکل های مسیریابی Link-State کار می کنند ، چگونه با یکدیگر تبادل اطلاعات می کنند و یا اینکه روتر چگونه شبکه های غیرمحلی را شناسایی و بهترین مسیر به هر کدام از آنها را تعیین می کند.

همچنین با دسته دیگری از Dynamic Routing Protocol ها یعنی Hybrid Routing آشنا می شوید.



بررسی پروتکل های Link State :

دسته دیگری از Dynamic Routing Protocol ها ، Link-state Routing Protocol می باشد .

Link-State ها دارای الگوریتمی به نام Dijkstra می باشد و به کمک این الگوریتم روتر می تواند Routing Table اش را تکمیل کند. در این روش کل اطلاعات در سه Table ذخیره می شود :

۱. Routing table

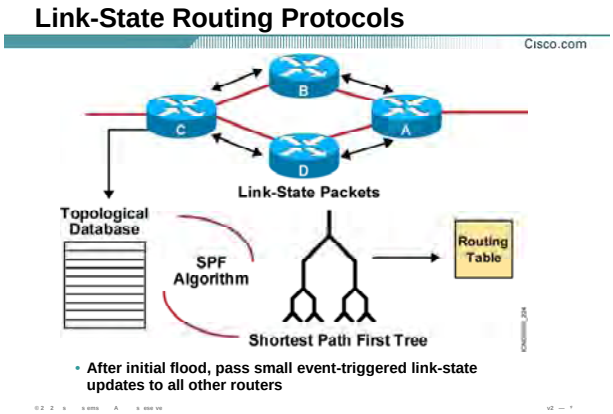
۲. Link-Sate Database

۳. Neighbor table

روتر جدیدی که وارد شبکه می شود ابتدا روترهای مجاورش را شناسایی می کند و با آنها رابطه همسایگی برقرار می کند . بنابراین اطلاعاتی که معرفی کننده روتر مجاورش باشد را در Neighbor table ذخیره می کند .

بعد از این که یک روتر رابطه همسایگی را برقرار کرد شروع به تبادل اطلاعات با روترهای مجاورش می کند .

در واقع بعد از برقراری رابطه همسایگی لازم است که Link-State Database هر دو یکسان شود . در Link-State Database توپولوژی ناحیه ای از شبکه که روتر در آن واقع شده است قرار دارد. بنابراین وقتی روتر جدید توپولوژی



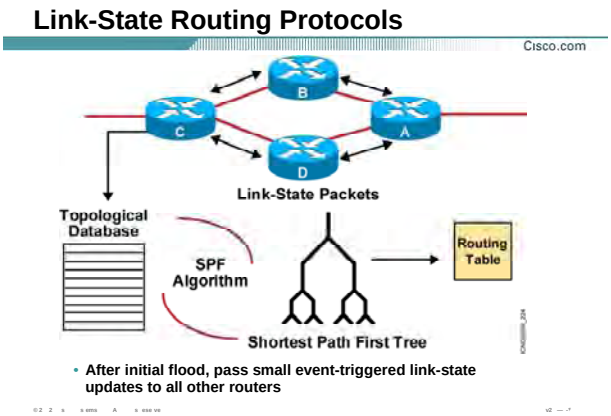
بررسی پروتکل های Link State :

شبکه را از روتر مجاورش آموخت ، الگوریتم SPF روی خود Run می کند و بهترین مسیر به شبکه های غیرمحلی را مشخص کرده و آنها را درون Routing Table قرار می دهد .

همانطور که می دانید ساختار شبکه به صورت یک شکل غیرمنتظم می باشد ، روتر بعد از کامل کردن Link-Sate Database خود از روی اطلاعات بدست آورده الگوریتم SPF را اجرا می کند . این الگوریتم شبکه را به صورت گراف بدون دور (درخت) در می آورد . درختی که ریشه آن خود روتر می باشد .

Link-State Protocol ها طراحی شده اند تا محدودیت های distance vector را بهبود دهند . دراین روش ابتدا شبکه را ناحیه بندی می کنیم . بنابراین مدیریت و اشکال زدایی در شبکه آسان تر می شود .

برخلاف روش Distance-Vector ، Update شامل کل اطلاعات Routing Table نمی باشد . بلکه روتر فقط تغییراتی که درون Link-State Database ایجاد شده را به روترهای دیگر گزارش می دهد . روترهای دیگر هم وقتی این تغییرات را می شنوند آن را در Link-State Database خود اعمال کرده و سپس برای انتخاب بهترین مسیر الگوریتم SPF را اجرا می کند .

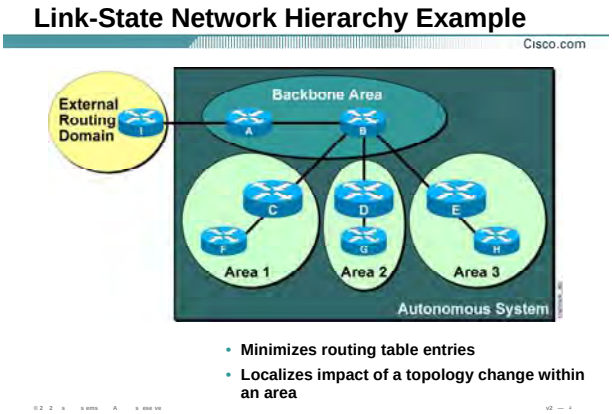


بررسی پروتکل های Link State (ادامه):

در روش Distance-Vector مسیر به یک شبکه در غالب Update به روترهای مجاور گزارش داده می شد . همانطور که دیدید امکان بروز خطا در این شبکه و انتشار مسیر نادرست در شبکه وجود داشت.

اما Update در پروتکل های Link-State حاوی مسیر نیست بلکه حاوی توپولوژی شبکه می باشد . بنابراین روتر خود باید بهترین مسیرها را به شبکه های غیرمحلی با کمک گرفتن از اطلاعات موجود درLink-Stat Database بدست آورد . بنابراین احتمال وقوع Loop در این شبکه تقریبا به صفر می رسد .

پروتکل های OSPF و IS-IS جزء پروتکل های Link-State ایی می باشد.



بررسی ساختاری Link State :

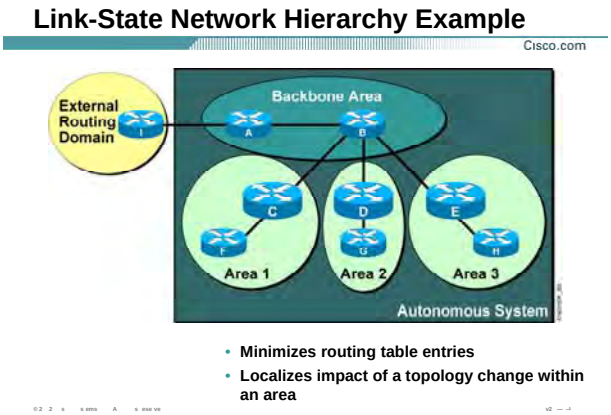
Link-state Protocol از دو دسته بندی شبکه ای استفاده می کند . درواقع از یک ساختار سلسله ای پیروی می کند . این ساختار از یک AS و چندین Area تشکیل شده است.

Autonomous system (AS) : به مجموعه ای از پروتکل های که تحت یک مدیریت واحد اداره می شوند AS گفته می شود . هر AS به چندین ناحیه که به هر کدام از آنها Area گفته می شود تقسیم بندی می شود .

Area : یک مجوعه از شبکه های به هم پیوسته می باشد . روترهای یک Area همگی دارای Link-State Database یکسانی هستند . در واقع روترهای درون یک Area فقط با یکدیگر به تبادل اطلاعات می پردازند و خبری از Link-State Database روترهای دیگر Area ها ندارند . به این نکته توجه داشته باشید که این دسته بندی به صورت منطقی می باشد نه فیزیکی. درواقع به کار بردن چندین Area در یک AS منجر به کاهش حجم Link-State Database و درنتیجه اندازه Routing Table می شود .

به این شکل توجه کنید . روترهای درون این AS دارای یکی از پروتکل های Link-State ایی می باشد .

این AS به چهار دسته منطقی دسته بندی شده است و روترها درون یکی از این چهار دسته قرار گرفته و یا مشترک بین دو دسته می باشند .



بررسی ساختاری Link State (ادامه):

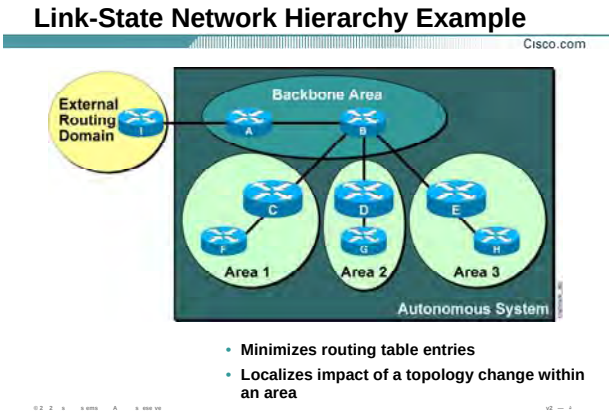
به صورت کلی Area ها به دو دسته کلی تقسیم بندی می شوند :

۱. Backbone Area

۲. non Backbone Area

Backbone Area: این Area که به آن Transit Area نیز گفته می شود ، تمامی Area ها به این Area متصل می شوند و از طریق این Area به یکدیگر مرتبط می شوند. همیشه Backbone Area را با شماره صفر نمایش می دهند . بنابراین Area 0 همان Backbone Area می باشد. همچنین به روترهایی که درون Backbone قرار دارند Backbone Router گفته می شود . بنابراین روترهایی که در این قسمت قرار می گیرند می بایست اطلاعات Area های دیگر را داشته باشند . بنابراین Link-State Database و Routing Table بزرگی دارند . روتری که درون Backbone استفاده می کنند از سری روترهای Core Layer می باشند.

Non Backbone Area : به هر Area غیر از Backbone Area گفته می شود.



بررسی ساختاری Link State (ادامه):

یک Area غیر Backbone یکی از چهار Area زیر می تواند باشد :

۱. Normal Area

۲. Stub Area

۳. Totally Stub Area

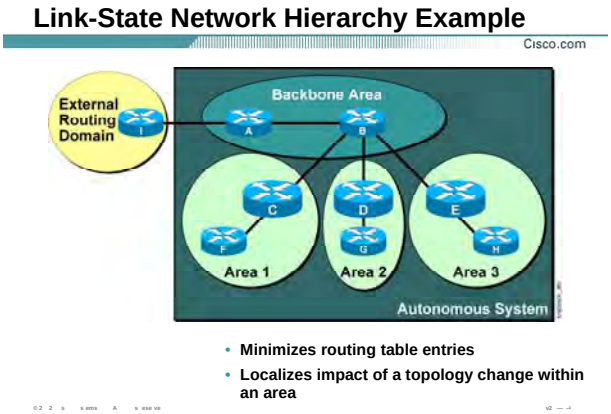
۴. Not-so-Stubby Area (NSSA)

توجه : در دوره CCNA ما فقط با Normal Area آشنا خواهیم شد .

در این شکل ما یک Backbone Area و چهار Area غیر Backbone که Normal هستند را می بینیم .

به روتر هایی که درون این Area قرار می گیرند Interior Router گفته می شود . بنابراین روترهای F ، G و H همگی Interior Router هستند .

Area Border Router (ABR): روترهایی هستند که از یک طرف در Backbone Area قرار بگیرند و از طرف دیگر در یک non Backbone Area. در این شکل روترهای C ، D و E هگی روتر ABR هستند.



بررسی ساختاری Link State (ادامه):

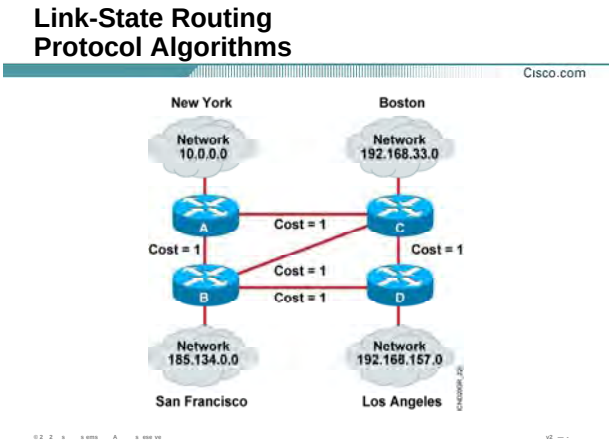
روترهای ABR دارای Link-State Database بزرگتری نسبت به روترهای دیگر هستند زیرا می بایست اطلاعات دو Area را در خود داشته باشد و به عنوان یک دروازه برای روترهای درون Area ایفای نقش می کند .

روترهای درون Area نیازی به دانستن توپولوژی بیرون Area ندارند . بنابراین پکتی که مقصدش درون Area نباشد به روتر ABR تحویل داده می شود تا مسیردهی شود و از Area خارج شود .

Autonomous System Border Router (ASBR):

به روتری که در دو AS مختلف قرار گیرد گفته می شود . درواقع این روتر ارتباطی بین دو AS مختلف را برقرار می کند .

دراین شکل روتر I به عنوان روتر ASBR ارتباط این AS را با External Routing Domain برقرار می کند .



بررسی الگوریتم Link State :

همانطور که متوجه شدید ، Link-state Database شامل توپولوژی شبکه می باشد.

درواقع بسته به اینکه که این روتر چه وظیفه ای را دارد اندازه این Database متفاوت تر می باشد . بنابراین Database ایی که روتر ABR دارد بزرگتر و دارای اطلاعات بیشتری نسبت به یک Interior Router می باشد .

اما یک روتر با فرستادن پکت هایی که به آن (Link State Advertisement) LSA گفته می شود اطلاعات درون Link-State Database اش را به روتر های دیگر ارسال می کند.درواقع در Link State Protocol ها اطلاعات به صورت Full Update ارسال نمی شود . بلکه درصورتی که تغییری در Link-State Database صورت گیرد تغییرات توسط LSA ها به روترهای دیگر گزارش داده می شود.

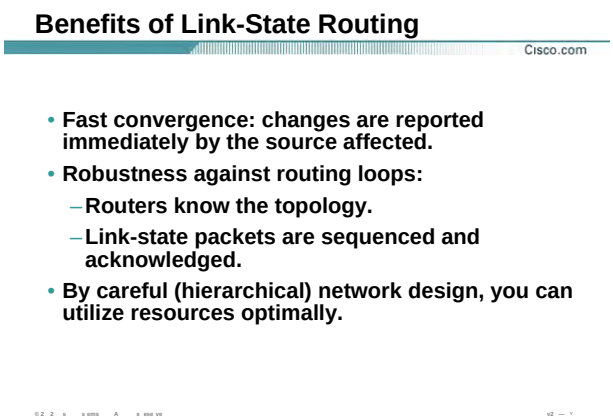
بنابراین روتر منتظر به پایان زمان Periodic Update نمی شود . در این روش سرعت همگرایی شبکه و انتشار تغییرات در شبکه خیلی بیشتر می شود . Link-State Database شامل تمامی شبکه ها و Cost رسیدن به هر کدام از آنها می باشد.

به این شکل توجه کنید . روتر A و روتر D را درنظر بگیرید . روتر A با توجه به LSA های دیگری که از روترهای دیگر گرفته Link-State Database خود را به صورت زیر می سازد.

درواقع جدول پایین Link-State Database مربوط به روتر A می باشد .

Router	Destination	Next Hop	Cost
A	185.134.0.0	B	1
A	192.168.33.0	C	1
A	192.168.157.0	B	2
A	192.168.157.0	C	2
B	10.0.0.0	A	1
B	192.168.33.0	C	1
B	192.168.157.0	D	1
C	10.0.0.0	A	1
C	185.134.0.0	B	1
C	192.168.157.0	D	1
D	10.0.0.0	B	2
D	10.0.0.0	C	2
D	185.34.0.0	B	1
D	192.168.33.0	C	1

هانطور که مشاهده می کنید روتر A برای رسیدن به شبکه 192.168.157.0 دو مسیر با متریک متفاوت و Next Hop متفاوت دارد . بنابراین با به کار بردن الگوریتم SPF کوتاهترین مسیر به شبکه 192.168.157.0 را پیدا کرده و آن را درون Routing Table خود قرار می دهد.



بررسی مزایای استفاده از پروتکل های Link State :

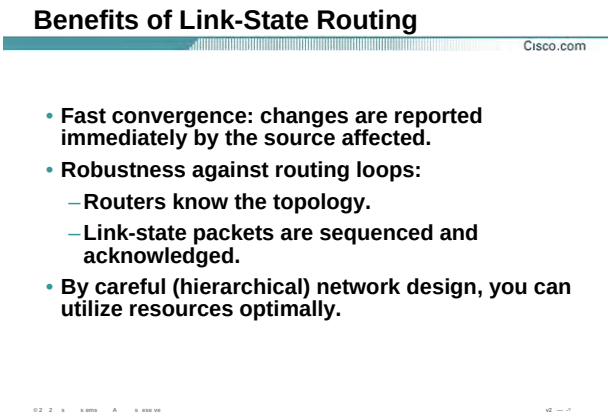
تا به اینجا با Link State Protocol و عملکرد آن آشنا شدید ، در این قسمت مزایا و معایب این روش نسبت به پروتکل های Distance-Vector آشنا خواهید شد .

- متریک در Link- State Protocol ها Cost می باشد .
- تغییرات به صورت Triggered در شبکه منتشر می شود و برخلاف Distance-vector ها فقط تغییرات ارسال می شود . بنابراین سرعت همگرایی در این روش خیلی سریعتر می باشد.
- با یک طراحی دقیق و حساب شده می توان سایز Link-State Database را کوچک کرده و در نتیجه الگوریتم Dijkstra روی اطلاعات کمتری پردازش انجام داده و درنتیجه سریعتر عمل می کند .

سوالی که اینجا مطرح می شود اینست که چه زمانی از Link State Protocol ها استفاده می کنیم و آن به پروتکل های Distance-Vector ایی چون RIP و IGRP ترجیح داده می شود ؟

برخلاف الگوریتم های Distance-Vector که مناسب شبکه های با اندازه کوچک می باشد ، این الگوریتم در هر شبکه با هر اندازه ای مناسب است .

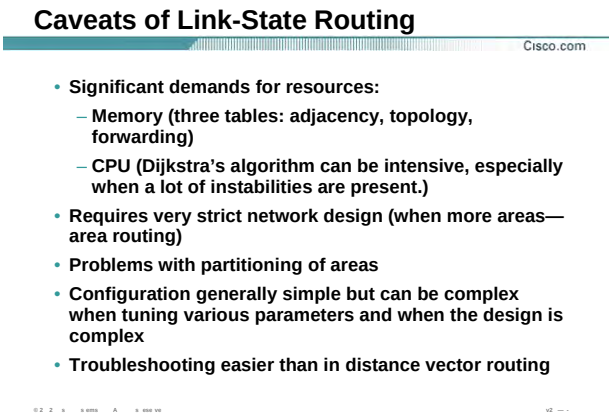
درواقع با یک طراحی مناسب و دقیق این پروتکل دارای بالاترین کارایی در شبکه خواهد بود .



بررسی مزایای استفاده از پروتکل های Link State (ادامه):

زیرا در این حالت تغییرات جزئی در شبکه منجر به تغییرات کل توپولوژی شبکه نمی شود . بلکه فقط روی قسمتی از شبکه که روتر در آن واقع شده است تأثیر می گذارد و این تأثیر به صورت ناحیه ای و در داخل Area می باشد .

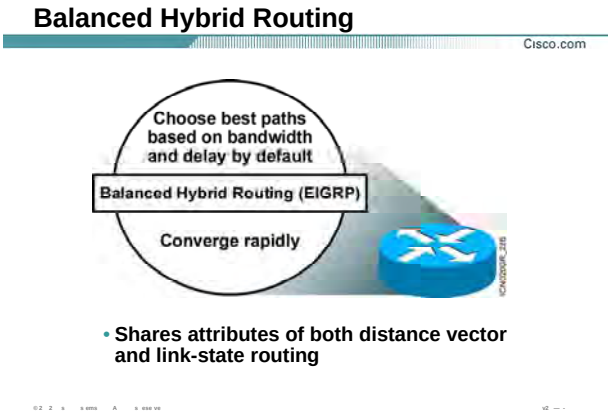
پروتکل های Distance-Vector ، Update هایشان را به صورت Periodic ارسال می کنند . بنابراین پهنای باند زیادی را برای ارسال کل Routing Table اشغال می کنند در صورتی که فقط یک تغییر در یکی از رکوردهای این جدول رخ داده است . پروتکل های Link-State ایی برخلاف پروتکل های Distance-Vector ایی فقط تغییرات را در شبکه منتشر می کند و پهنای باند کمتری را اشغال می کند . بنابراین در صورتی که محدودیت پهنای باند در شبکه را دارید این روش بهترین راه حل است .



بررسی محدودیتهای Link State :

تا به اینجا مزایا استفاده از روش Link-State را بیان کردیم . در این قسمت محدودیت های این روش را بیان می کنیم .

- همانطور که می دانید اطلاعات مختلف در Table های مختلف نگهداری می شود . بنابراین در شبکه های با اندازه بزرگ حجم هر کدام از این Table ها زیاد شده ، و روتر نیاز به Memory بیشتری دارد .
- از طرفی الگوریتم Dijkstra برای انتخاب بهترین مسیر نیاز به CPU قویتری دارد.پس در شبکه هایی که بزرگتر و پیچیده تر هستند و یا شبکه هایی که دارای طراحی خوبی نباشد ، نیاز به یک CPU قویتر برای اجرای الگوریتم Dijkstra لازم و ضروری است.
- طراحی سلسله ای به کاهش حجم Table ها در این الگوریتم کمک می کند . بنابراین با به کار بردن تعداد Area ها در شبکه پیچیدگی الگوریتم Dijkstra را کمتر می کنیم . اما این بدان معنی نیست که با این کار هیچ مشکلی پیش نخواهد آمد . درواقع طراحی سلسله ای هر Area می بایست ارتباطش را با Backbone Area از دست ندهد و همیشه باید یک ارتباط با Backbone Area داشته باشد تا ارتباطش با Area های دیگر قطع نشود .



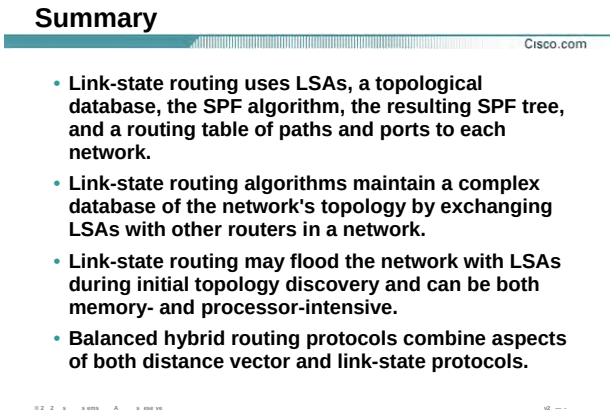
بررسی Hybrid Routing :

این دسته همانطور که از نامش پیداست ترکیبی است از ویژگیهای Link state و Distance Vector.

مانند Distance Vector عمل ی کند چون بین روتر مبدا و روتر مقصد یک بردار در نظر می گیرد و درصورتی که تغییری در شبکه رخ دهد این تغییرات به صورت برداری بین روترهای مجاور منتشر می شود . البته این تغییرات را به صورت Full update ارسال نمی کند بلکه فقط تغییرات جزئی در شبکه به روترهای دیگر ارسال می شود .

مانند Link state عمل می کند چون می بایست تصو رکلی از شبکه را داشته باشد .و اطلاعات مسیرهای شدنی به هر کدام از شبکه های غیرمحلی را در topology table نگهداری می کنند .

نمونه Hybrid routing protocol ، پروتکل EIGRP می باشد



خلاصه :

پروتکل های Link-State برخلاف پروتکل های Distance-Vector دارای سرعت همگرایی بالایی هستند. بنابراین در شبکه هایی با اندازه های بالا با بکار بردن طراحی سلسله ای می توان کارایی Link-State را افزایش داد . در این روش اطلاعات در Table های مختلفی نگهداری می شود . و هر روتر توپولوژی شبکه را با گرفتن اطلاعات از روترهای دیگر کامل کرده و به کمک الگوریتم Dijkstra بهترین مسیرها را به شبکه های غیرمحلی تشخیص داده و آنها را در Routing Table قرار می دهد .

درواقع هر روتر با فرستادن پکتهای LSA اطلاعات موجود در Link-State Database خود را به روترهای دیگر می فرستد . این روش نیاز به Memory بیشتر و CPU قویتری دارد . بنابراین با بزرگ شدن اندازه شبکه ، اندازه Topology Table و Routing Table بزرگتر می شود . این روش با بکار بردن تقسیم بندی در شبکه و به کار بردن چندین Area در شبکه حجم این Table ها را کاهش می دهد .

درس چهارم :

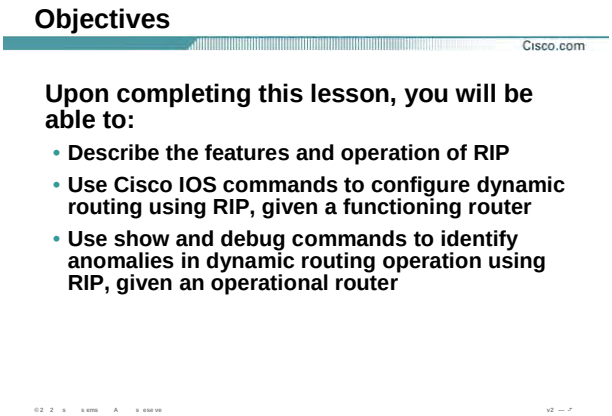
پروتکل مسیریابی
RIP

هدف :

۱. آشنایی با پروتکل مسیریابی RIP و نحوه عملکرد آن .

۲. نحوه تنظیم پروتکل مسیریابی RIP روی یک شبکه .

۳. اشکال زدایی پروتکل مسیریابی RIP .



مروری بر پروتکل RIP :

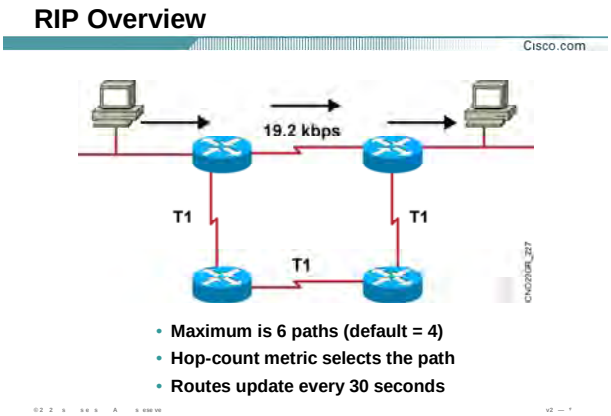
RIP یک پروتکل قدیمی و عمومی می باشد که جزء دسته پروتکل های (IGPs(Interior Gateway Protocol می با شد.

در واقع جزء پروتکل هایی است که در داخل یک AS عمل می کند.

RIP در شبکه های با اندازه کوچک کارایی بالایی دارد و از رده پروتکل های Distance-Vector است .

در این درس با مفاهیم پایه ایی RIP و عملکرد آن در مسیریابی شبکه های غیر محلی و اینکه چگونه می توان RIP را در یک شبکه IP بنا کرد آشنا می شوید.

و می آموزید که چگونه می توان عملکرد لحظه ای این پروتکل را به کمک فرمان Debug بررسی کرد .



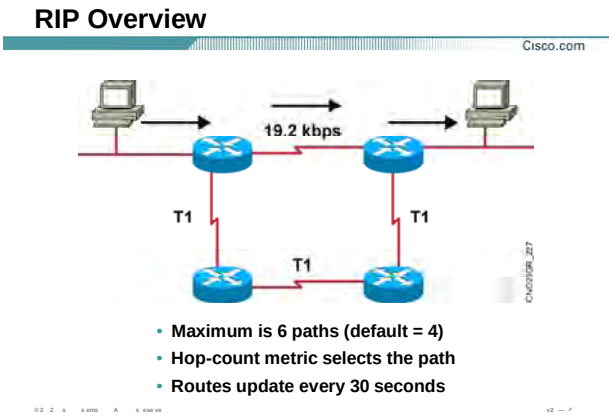
مروری بر پروتکل RIP (ادامه) :

RIP (Routing Information Protocol) ، یک پروتکل مسیریابی Distance-Vector می باشد.

همانطور که می دانید متریک معیار و یا ملاکی برای انتخاب بهترین مسیر در میان مسیرهای مختلف به یک Network با یک پروتکل مسیریابی واحد است. متریک این پروتکل یک متغیره و hop count می باشد. درواقع متریک RIP ، تعداد گام برای رسیدن به یک شبکه غیرمحلی است. همانطور که می دانید یکی از ویژگی های پروتکل های Distance-Vector ، Periodic بودن Update ها می باشد .RIP هر ۳۰ ثانیه یک بار کل اطلاعات Routing table اش را به آدرس 255.255.255.255 (Broadcast) ارسال می کند . پروتکل RIP در شبکه های IP دارای دو نسخه می باشد RIP Version 1(RFC1058) ,RIP Version 2 (RFC 1721 & RFC1722) .

به صورت خلاصه می توان ویژگی های پروتکل RIP را به صورت زیر بیان کرد:

۱. RIP ، یک پروتکل Distance-Vector می باشد.
۲. متریک یا ملاک انتخاب بهترین مسیر در این پروتکل hop cont (تعداد گام) است .
۳. Maximum مقداری که برای متریک در این پروتکل در نظر گرفته شده است ۱۵ می باشد و در صورتی که متریک از این مقدار بیشتر شود مسیر غیر قابل دسترس خواهد بود و در واقع infinity خواهد شد.



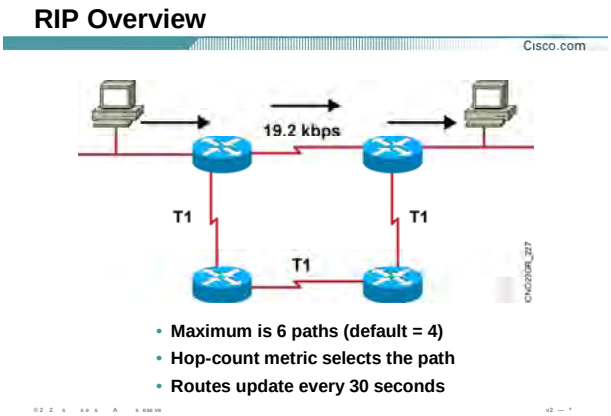
مروری بر پروتکل RIP (ادامه) :

۴. full update در این پروتکل هر ۳۰ ثانیه یک بار در شبکه به صورت Broadcast از اینترفیس های متصل به روتر خارج شده و به روتر های مجاور ارسال می شود.

۵. Load Balancing: در RIP روتر در صورتی که چند مسیر با متریک یکسان به یک شبکه پیدا کند ، ترافیک را بین این مسیر ها تقسیم می کند . بنابراین در این حالت از منابع شبکه و پهنای باند موجود به خوبی استفاده می شود. RIP به صورت پیش فرض توانایی پشتیبانی ۴ مسیر با متریک یکسان جهت load balancing را دارد.

۶. RIP v1 یک Class Full Routing Protocol می باشد ، زیرا VLSM و CIDR را پشتیبانی نمی کند .بنابراین در update هایی که ارسال می کند subnet mask را همراه با Network ID ارسال نمی کند.

۷. RIP V2 یک Classless Routing Protocol می باشد زیرا VLSM و CIDR را پشتیبانی می کند .بنابراین در updateهایی که ارسال می کند subnet mask را همراه با Network ID ارسال می کند.



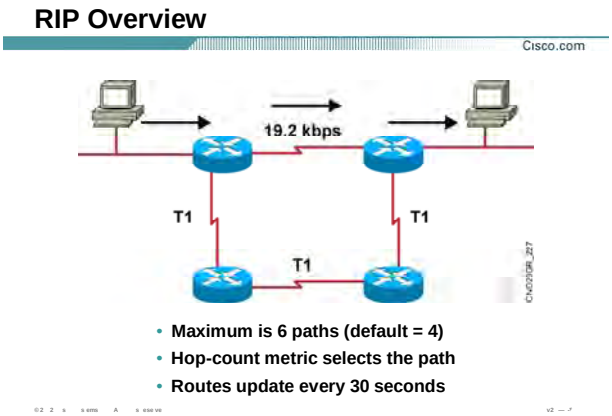
مروری بر پروتکل RIP (ادامه) :

توجه: Load balancing شامل دو دسته بندی کلی می شود :

۱. Equal load balancing

۲. Unequal load balancing

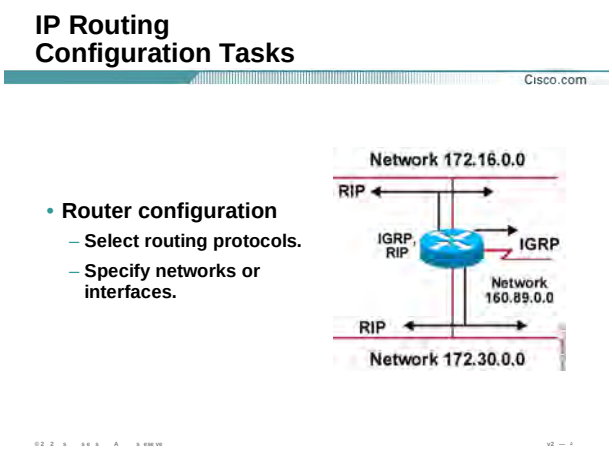
Equal load balancing: در این حالت مسیر هایی که دارای متریک یکسان به یک network باشند Load Balancing انجام می پذیرد. پروتکل مسیریابی RIP این نوع از Load Balancing را پشتیبانی می کند.



مروری بر پروتکل RIP (ادامه) :

Unequal Load Balancing: در این حالت لزومی ندارد که متریک تمامی مسیر ها از نظر عددی یکسان باشند بلکه می بایست در یک رنج قابل قبول قرار بگیرد. برای این منظور فاکتور Variance را تغییر می دهیم . این فاکتور به صورت Default دارای مقدار یک می باشد ، بنابراین مسیری که دارای کمترین متریک باشد به عنوان بهترین مسیر انتخاب می شود . با تغییر Variance می توانید مسیر های بیشتری را داشته و در نتیجه از منابع شبکه به خوبی استفاده کنید .

با مفهوم Variance و Unequal Load Balancing در مبحث EIGRP, IGRP بیشتر آشنا می شوید .



راه اندازی پروتکل RIP :

به صورت کلی برای فعال کردن Dynamic Routing Protocol روی یک روتر در دو مرحله عمل می کنید :

۱. Select Routing Protocol

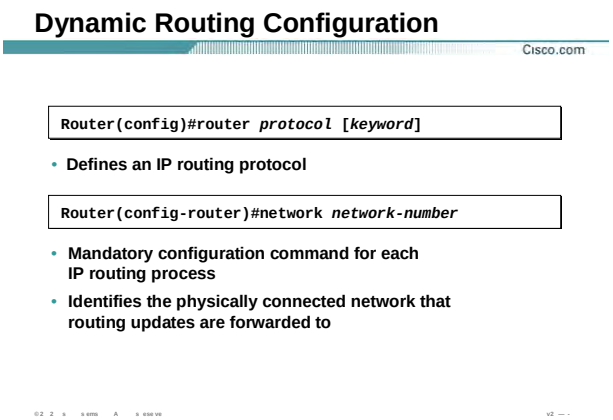
۲. Specify Networks or interface

بنابراین برای فعال کردن Dynamic Routing Protocol می بایست :

۱. Routing Protocol مورد نظر را انتخاب کنید. (RIP ، IGRP ، EIGRP ، OSPF)

۲. معرفی شبکه های IP .

تذکر:در پروتکل OSPF می بایست علاوه بر Network ID ، wildcard mask را معرفی کنید.



راه اندازی پروتکل RIP (ادامه):

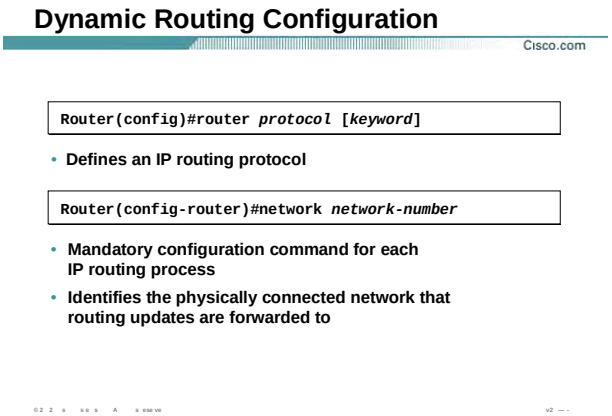
همانطور که گفته شد فعال کردن Dynamic Routing Protocol در دو مرحله انجام می پذیرد .

۱. وارد Global Mode شده و دستور زیر را وارد می کنید :

Router(config)#router protocol [keyword]

Protocol: در این قسمت یکی از Dynamic Routing Protocol هایی را که می خواهید روی روتر فعال شود را معرفی می کنید. به طور مثال : یکی از پروتکل های RIP ، IGRP ، EIGRP و OSPF .

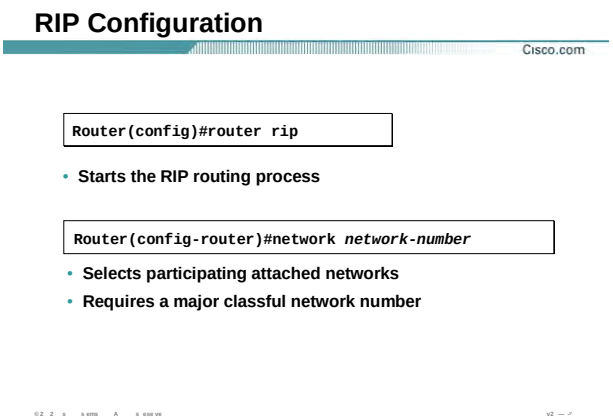
Keyword: بعضی از پروتکل ها چون IGRP, EIGRP نیاز به معرفی AS دارند. بنابراین در این قسمت AS ای که روتر درون آن قرار گرفته را مشخص می کنید. در صورتی که با پروتکل OSPF کار کنید در این قسمت می بایست که Process ID که یک مشخصه Local می باشد را به روتر معرفی کنید. در مبحث معرفی OSPF با این ویژگی آشنا می شوید.



راه اندازی پروتکل RIP (ادامه):

۲. در مرحله دوم می بایست Network های متصل به روتر را معرفی کنید. درواقع مـی بایـست مـشخص کنـیم که کدام اینترفیس های روتر قرار است send و receive پکتهای Update مربوط به این پروتکل را انجام دهنـد .بنابراین در قسمت network-number شبکه های Connect به روتر را معرفی می کنیم.

Router(config-router)#network network-number



راه اندازی پروتکل RIP (ادامه):

تا به اینجا با راه اندازی Dynamic Routing Protocol ها به صورت کلی اشنا شدید.

برای معرفی RIP نیز دقیقا دو مرحله گفته شده را می بایست اجرا کنیم :

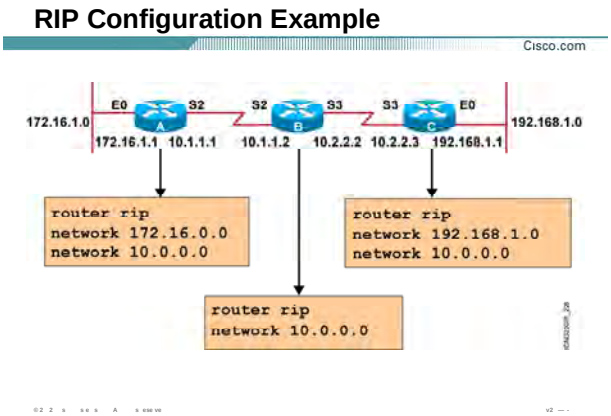
۱. معرفی پروتکل RIP

Router(config)#router rip

۲. معرفی شبکه های Connect

Router(config-router)#network network-number

توجه :شبکه های متصل به اینتر فیس هایی را که می خواهید در پروتکل RIP شرکت کنند معرفی می کنید.



راه اندازی پروتکل RIP در یک مثال:

به این شبکه نمونه توجه کنید : روترهای A ، B و C هرکدام دارای دو شبکه Connect به خود هستند.

در این قسمت راه اندازی RIP را روی روتر A بررسی می کنیم :

Router RIP: فعال کردن Routing Protocol RIP روی روتر A به کمک این فرمان می باشد .

Network 172.16.0.0: معرفی شبکه متصل به روتر از طریق اینترفیس E0.

Network 10.0.0.0: معرفی شبکه متصل به روتر از طریق اینترفیس S2.

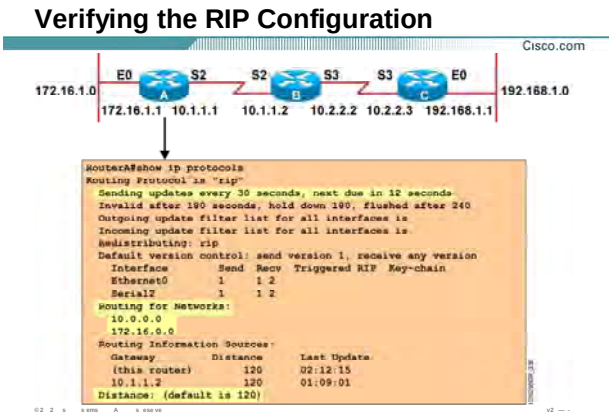
روتر A دارای دو شبکه Connect می باشد .

همانطور که میدانید RIP V1 یک پروتکل Classful میباشد ، بنابراین CIDR را پشتیبانی نمی کند .

به روتر B توجه کنید ، این روتر دارای دو شبکه Connect با Network ID های 10.1.1.0.0/24 و 10.2.2.0/24 می باشد.

در حالی که در هنگام راه اندازی RIP ، می بایست شبکه ها را به صورت classful معرفی کنید .

بنابراین در هنگام معرفی شبکه روی روتر B ، کافی است شبکه 10.0.0.0/8 را به عنوان شبکه connect معرفی کنید.



بررسی تنظیمات :

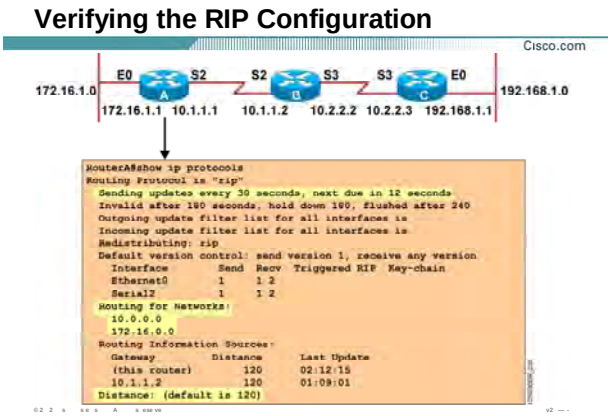
تا به اینجا با راه اندازی و فعال کردن پروتکل RIP آشنا شدید .

همانطور که می دانید اطلاعات شبکه های Connect (محلی) وشبکه های غیر محلی همگی در یک Routing Table نگهداری می شوند . برای مشاهده شبکه های Connect و شبکه های غیر Connect و اینترفیس هایی که از طریق آنها دسترسی امکان پذیر می شود ، فرمان show ip route را به کار می بریم . از طرفی دیگر می توانید اطلاعات مربوط به خود پروتکل مسیریابی و Timer های مختلفی که این پروتکل برروی این روتر دارد را مشاهده کنید .

به خروجی فرمان show ip route در مثال بالا توجه کنید.

روی روتر A پروتکل مسیریابی RIP تنظیم شده است. همانطور که می دانید یکی از ویژگی های پروتکل های Distance-Vector ، Periodic بودن آنها می باشد. این پروتکل ها دارای چهار Time مختلف هستند :

۱. Update Timer
۲. Invalid timer
۳. Holddown Timer
۴. Flush Timer



بررسی تنظیمات (ادامه):

RIP نیز یک پروتکل Distance-Vector می باشد. بنابراین این ۴ زمان در مورد این پروتکل به صورت Default به صورت زیر می باشد:

۱. Update Timer : ۳۰ ثانیه

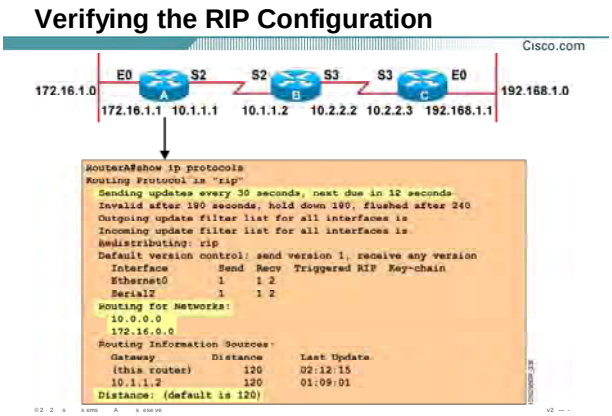
۲. Invalid timer : ۱۸۰ ثانیه

۳. Holddown Timer : ۱۸۰ ثانیه

۴. Flush Timer : ۲۴۰ ثانیه

حال به شرح تک تک انها می پردازیم :

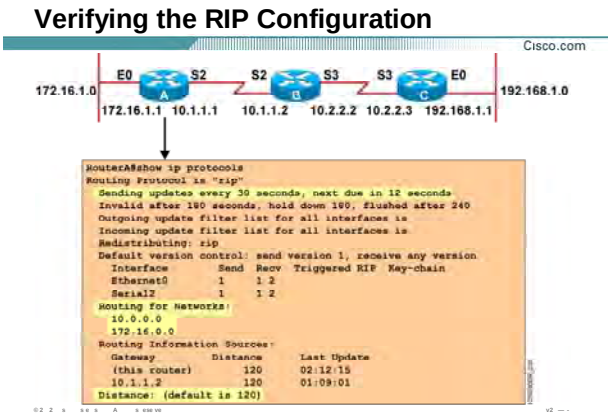
Update Timer: هر روتر به صورت دوره ای هر ۳۰ ثانیه یک بار اطلاعات کل Routing table اش را به آدرس 255.255.255.255(lBroadcast address) ارسال می کند. حتی اگر تغییری در شبکه رخ نداده باشد و یا تغییرات جزئی باشد.



بررسی تنظیمات (ادامه):

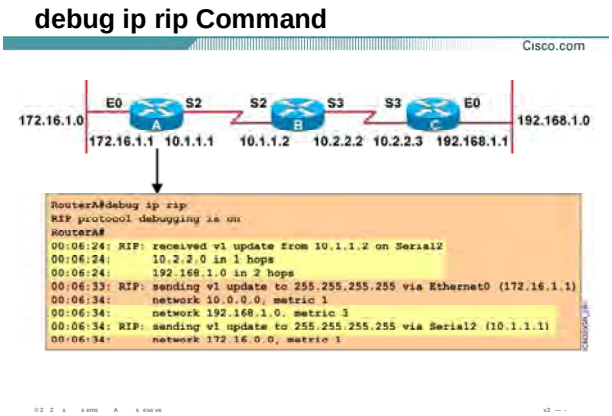
Invalid Timer: در صورتی که یک روتر به اندازه ۱۸۰ ثانیه صبر کرد و هیچ Update ای را در مورد یک شبکه دریافت نکرد ، در این حالت روتر به حالت Hold رفته و در مقابل شبکه ای که هیچ Update ای از آن دریافت نکرده واژه Possibly Downرا در Routing Tableدرج می کند.

Flush Timer: در صورتی که روتر ۶۰ ثانیه دیگر منتظر باقی ماند و باز هیچ Update ایی را از این شبکه دریافت نکرد ، این Network را به صورت کلی از Routing Table اش حذف کرده و این تغییرات را با فرستادن کل Routing Table به روتر های مجاور گزارش می دهد.



بررسی تنظیمات (ادامه):

Holddown Timer: در صورتی که روتر در مورد یک شبکه Update ایی دریافت کند و این Update در مورد یک شبکه افزایش متریک را گزارش دهد ، در این صورت روتر برای جلوگیری از افتادن در حالت Loop این خبر را نشنیده گرفته و به حالت hold می رود. بنابراین این شبکه را از Routing Table اش حذف نمی کند بلکه واژه Possibly Down را در مقابل شبکه مورد نظر قرار می دهد و در طول این ۱۸۰ ثانیه هر گونه خبر دیگری در مورد این شبکه بدست آورد آن را نادیده می گیرد .



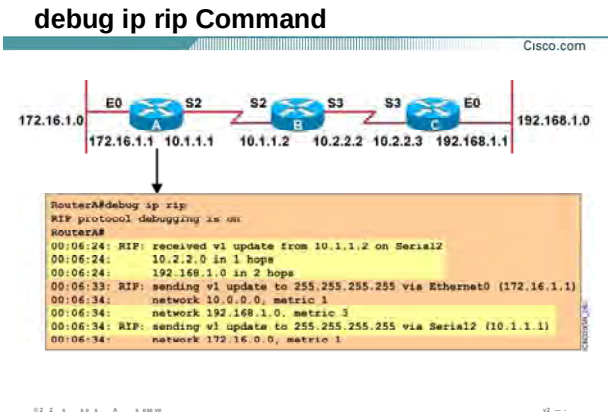
بررسی عملکرد RIP به کمک فرمان Debug :

همانطور که می دانید اطلاعات شبکه های Connect وشبکه های غیر محلی همگی در یک Routing Table نگهداری می شود. به خروجی فرمان Show ip Route که روی روتر A گرفته شده است توجه کنید :

این Table شامل اجزای زیر می باشد :

۱. **R or C:** این نماد نشان دهنده وضعیت محلی یا غیر محلی بودن شبکه موجود در Routing Table می باشد.

در صورتی که این نماد R باشد یعنی شبکه هایی که روتر از طریق دریافت Update از روتر های مجاور می شناسد. درواقع روترهای مجاور با ارسال کل Routing Table شان به این روتر در مورد شبکه های مختلف و متریک های مربوط به هر کدام اطلاع رسانی می کنند و این روتر با درنظر گرفتن کمترین متریک گزارش داده شده بهترین مسیر را به شبکه های غیرمحلی پیدا کرده و در Routing table با علامت R درج می کند.



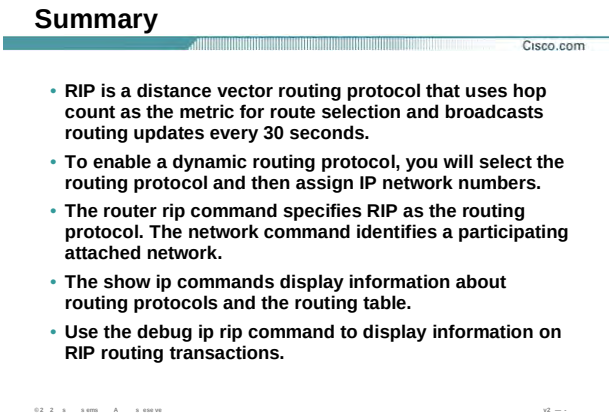
بررسی عملکرد RIP به کمک فرمان Debug :

۲. **120/1 :** عدد اول نمایانگر ADMINISTRA DISTAN وعدد دوم نمایانگر متریک می باشد.

همانطور که در معرفی Dynamic Routing Protocol ها گفته شده ، AD معیار و یا ملاکی برای انتخاب یک Routing Protocol درمیان Routing protocol های مختلف می باشد. دراین حالت چون پروتکل ای که ما به کار برده ایم RIP می باشد بنابراین دارای AD با مقدار ۱۲۰ می باشد .و چون روتر شبکه 10.2.2.0 را با یک گام جلوتر مشاهده می کند بنابر این متریک مربوط به این شبکه را با مقدار ۱ را نمایش می دهد .

۳. **Via 10.1.1.2:** IP Address مربوط به اینترفیس روتر مجاور که با این روتر به صورت point-to-point ارتباط دارد.

۴. **Serial 2:** اینترفیسی از خود روتر می باشد که مسیر از آن تعریف می شود. همانطور که می دانید هنگامی که یک شبکه غیرمحلی شناسایی شود، برداری از خود روتر تا آن شبکه درنظر گرفته می شود. ابتدای این بردار از اینترفیس Connect به خود روتر می باشد پس serial 2 ابتدای این بردار می باشد.



خلاصه :

RIP (Routing Info mation Protocol) یک پروتکل مسیریابی از دسته پروتکل های Distance-Vector می باشد. متریک این پروتکل Hop Count (تعداد گام) می باشد. RIP مانند پروتکل های Distance-Vector ، Update هایش را به صورت Periodic می فرستد و این update شامل کل اطلاعات Routing Table می باشد. بنابراین پروتکلی است که در شبکه های با اندازه کوچک دارای کارایی خوبی می باشد. ز را منابع شبکه چون Bandwidth را صرف ارسال Update های دوره ای می کند حتی اگر تغییری در شبکه رخ نداده باشد. را اندازی این Routing Protocol در دو مرحله صورت می گیرد :

۱. معرفی پروتکل RIP :

Router (config) #router rip

۲. معرفی شبکه های Connect :

Router(config-route)#network network-number

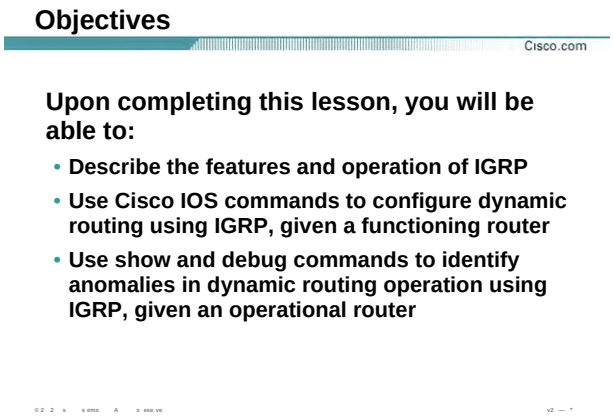
همچنین برای مشاهده Routing Table از فرمان show ip route و برای مانیتور کردن ا ن پروتکل از فرمان debug ip rip استفاده می کنیم.

درس پنجم :

پروتکل مسیریابی
IGRP

هدف :

۱. آشنایی پروتکل مسیریابی IGRP .
۲. پیکربندی و تنظیم پروتکل IGRP .
۳. اشکال زدای در IGRP .



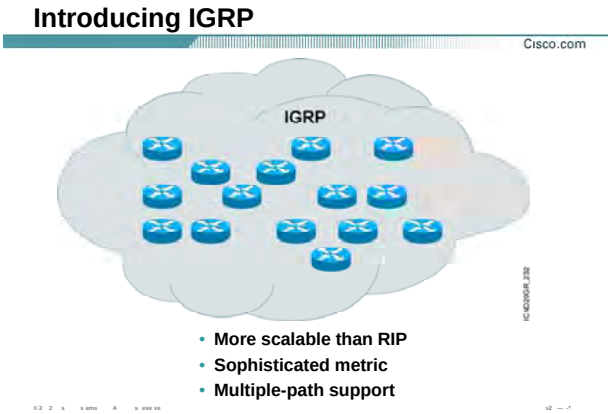
مروری بر پروتکل IGRP :

Interior Gateway Routing Protocol یا IGRP پروتکی است که توسط شرکت Cisco در اواسط دهه 1980 طراحی و ارائه شد .

محبوبیت و قدرت IGRP باعث شد که جایگزین خوبی برای پروتکل مسیریابی RIP شود .

در ادامه این درس با این پروتکل مسیریابی و ویژگیها و نحوه پیاده سازی آن آشنا خواهید شد .

می آموزید که چگونه می توان عملکرد این پروتکل را به کمک فرمان Debug بررسی کرد .

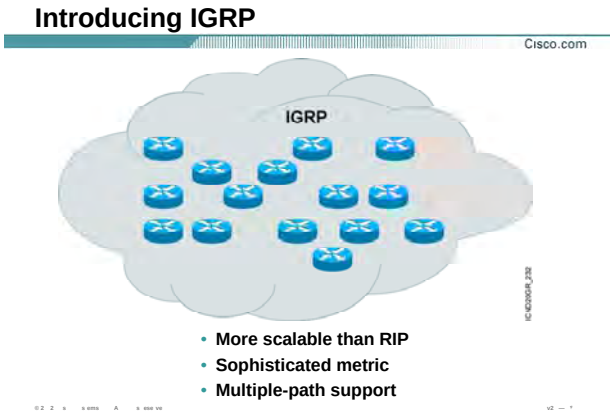


معرفی پروتکل IGRP :

Interior Gateway Routing Protocol یا IGRP پروتکی است که توسط شرکت Cisco در اواسط دهه 1980 طراحی و ارائه شد . این پروتکل دارای یک سری ویژگیهایی می باشد که آن را نسبت به دیگر پروتکل های Distance Vector چون RIP متفاوت می کند. این ویژگیها عبارتند از :

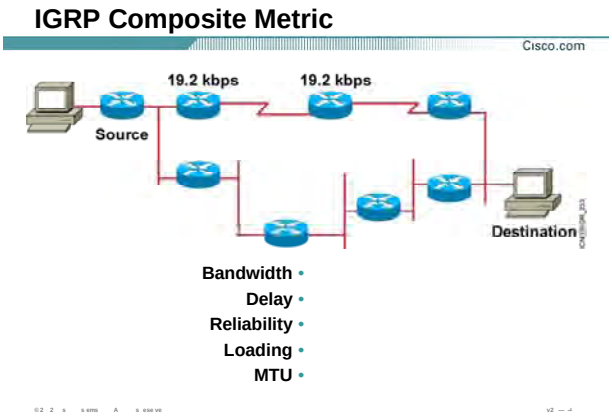
- **افزایش محدوده تحت پوشش :** IGRP برخلاف RIP توانایی انجام عملیات Routing در شبکه هایی بزرگ را دارد .
- **متریک پیچیده :** IGRP برخلاف RIP دارای متریک composite می باشد . متغییرهایی که در تعیین متریک نقش دارند:

۱. bandwidth
۲. Delay
۳. Load
۴. MTU
۵. Reliability



معرفی پروتکل IGRP (ادامه) :

- **Unequal Load Balancing:** پروتکل IGRP مانند RIP می تواند ترافیک را بین چند مسیر balance کند . اما تفاوتی که این پروتکل با RIP دارد در این است که می تواند ترافیک را بین چند مسیر با متریک های مختلف Balance کند . IGRP به صورت Default تا چهار مسیر را برای Unequal Load Balancing انتخاب می کند.



بررسی متریک در IGRP :

- **Composite Metric:**

متریک در IGRP بر خلاف RIP ، ترکیبی از چند متغیر می باشد . این متغیرها عبارتنداز:

۱. Delay

۲. Load

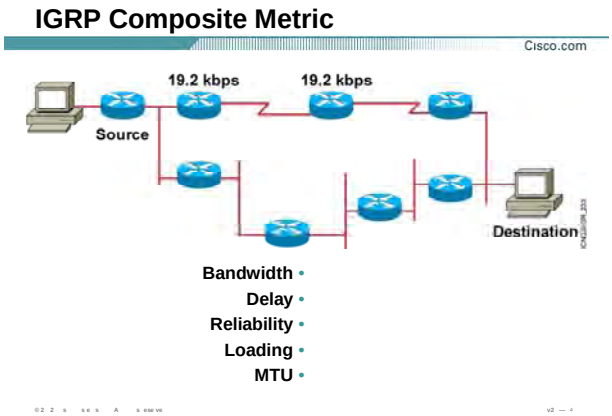
۳. MTU

۴. Bandwidth

۵. Reliability

به صورت پیش فرض دو متغیر Bandwidth و Delay در تعیین متریک نقش دارند. تا پایان این درس با تک تک این متغیرها آشنا خواهید شد ، بنابراین تا پایان این درس با من همراه شوید.

همانطور که می دانید RIP دارای محدودیت 15 گام در متریک می باشد. این بدان معنی است که RIP متریک بیشتر از 15 را بی نهایت در نظر می گیرد. لذا RIP با محدودیت وسعت شبکه مواجه می باشد .

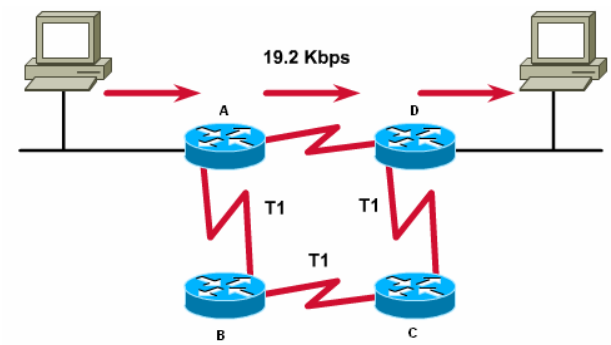


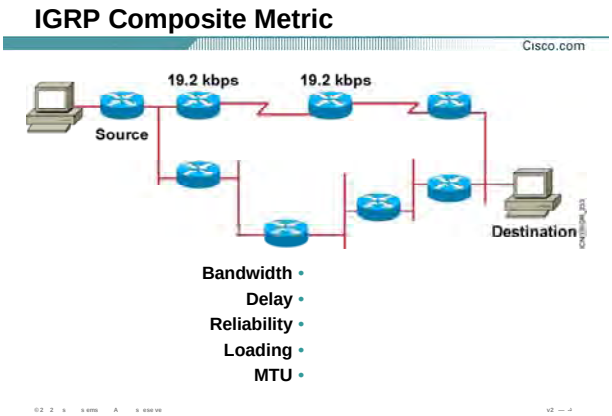
بررسی متریک در IGRP :

اما در IGRP برخلاف RIP این مقدار 255 مـی باشـد . بنـابراین IGRP محـدودیت RIP را در Maximum hop Count بهبـود بخشید.

سوالی که اینجا مطرح می شود اینست که چرا IGRP چندین متغیر را برای تعیین متریک در نظر می گیـرد و مزیـت ایـن انتخاب نسبت به RIP که فقط یک متغیر در تعین متریک شرکت می کند در چیست؟

به شکل زیر توجه کنید :

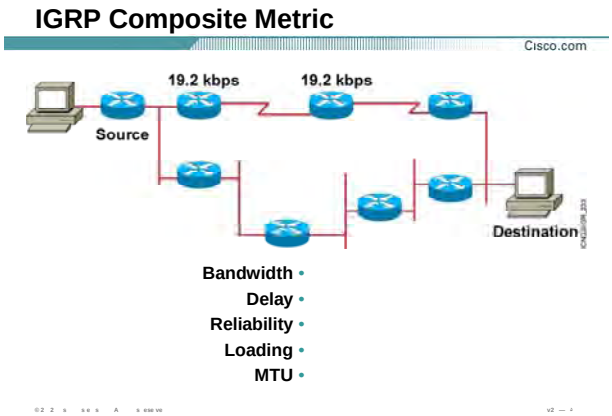




بررسی متریک در IGRP :

فرض کنید پروتکل مسیریابی RIP روی تک تک روترها Run شود ، از آنجایی که متریک در RIP تعداد گام (hop Count) می باشد ، بنابراین مسیر AD به عنوان بهترین مسیر انتخاب می شود.

در واقع مسیری که پهنای باند کمتری دارد به مسیری با پهنای باند T1 ترجیح داده می شود . IGRP با درنظر گرفتن این مشکل متریک را اصلاح می کند . در IGRP پهنای باند یکی از فاکتورهای تعیین متریک می باشد .



بررسی متریک در IGRP (ادامه) :

:Bandwidth

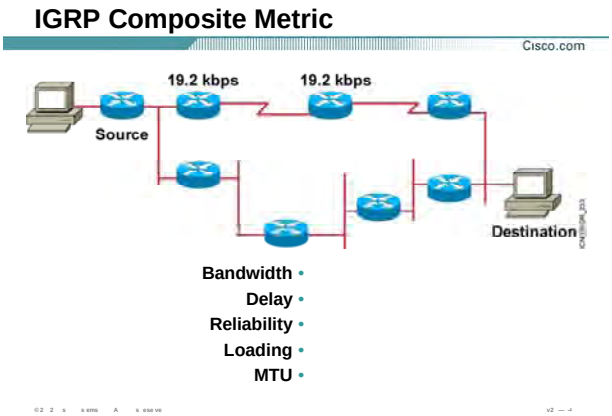
در صورتی که IGRP به عنوان پروتکل مسیریابی انتخاب شود با فرض ثابت بودن متغییرهای دیگر روی تمامی مسیرها ، مسیری که پهنای باند بیشتری دارد به عنوان بهترین مسیر انتخاب می شود . بنابراین در صورتیکه روتر A پکتی را دریافت کرد که مقصد آن PC-2 باشد ، آنرا از مسیر ABCD که پهنای باند بیشتری دارد هدایت می کند.

:Delay

مقیاسی از زمانی است که یک packet در طول مسیر حرکت می کند و مقداری است بین ۰ تا ۲۵۵. بنابراین با فرض ثابت ماندن فاکتورهای دیگر در تعیین متریک ، مسیری که delay کمتری دارد به عنوان بهترین مسیر انتخاب می شود.

:Load

حجم ترافیک براساس بیت در ثانیه که از یک مسیر می تواند منتقل شود. این پارامتر به صورت پیش فرض در تعیین متریک IGRP نقشی ندارد و در غیر این صورت این عدد بین ۰ تا ۲۵۵ می تواند تغییر کند . مسیری که load آن ۲۵۵ باشد مسیری است که load آن ۱۰۰ درصد می باشد. با فرض ثابت ماندن فاکتورهای دیگر در تعیین متریک، مسیری که load کمتری دارد به عنوان بهترین مسیر انتخاب می شود.



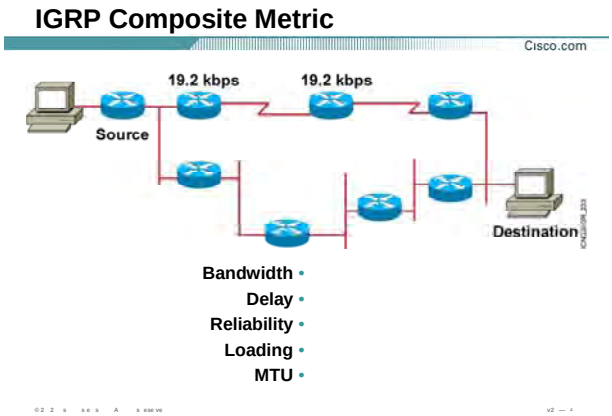
بررسی متریک در IGRP (ادامه) :

Reliability: مقیاسی برای پایداری و مطمئن بودن یک مسیر می باشد. فاکتورهای چون دفعات down شدن یک مسیر و یا packet lost روی این پارامتر تأثیر می گذارد.

این پارامتر به صورت پیش فرض در تعیین متریک IGRP نقشی ندارد و در غیر این صورت این مقدار بین ۰ تا ۲۵۵ می تواند تغییر کند. بنابراین با فرض ثابت ماندن فاکتورهای دیگر در تعیین متریک ، مسیری که Reliability بیشتری داشته باشد به عنوان بهترین مسیر انتخاب می شود.

MTU: Maximum Transmission Unit ، ماکسیمم اندازه ای که برای یک پکت در نظر گرفته می شود بدون اینکه Fragment شود. به صورت پیش فرض این پارامتر در تعیین متریک نقشی ندارد.

تا به اینجا با پارامترهایی که در تعیین متریک نقش داشتند آشنا شدید. به صورت پیش فرض فقط دو پارامتر Bandwidth و Delay در تعیین متریک تأثیرگذار هستند.



بررسی متریک در IGRP (ادامه) :

متریک با bandwidth رابطه معکوس و با Delay رابطه مستقیم دارد . این بدان معنی است که در صورتی که دو مسیر با پهنای باند متفاوت داشته باشیم ، با فرض یکسان بودن پارامتر delay روی هر دو مسیر ، مسیری که پهنای باند بیشتری داشته باشد متریک کمتری خواهد داشت .

سوالی که اینجا مطرح می شود اینست که در صورتی که بین Source و Destination مسیری موجود باشد که تشکیل شده از Type های مختلفی باشد ، به طور مثال قسمتی از آن Ethernet با پهنای باند 1000 Mb/s و قسمتی از آن dial-up با پهنای باند 56 k ، متریک چگونه محاسبه می شود؟

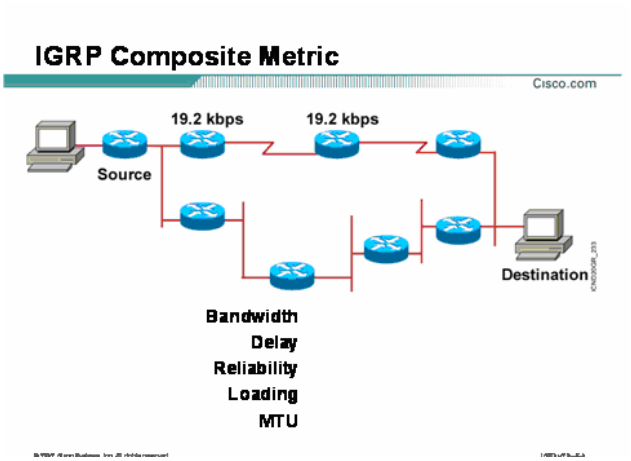
در این حالت IGRP برای تعیین متریک این مسیر ، Minimum Bandwidth و Count of Delay را درنظر می گیرد.

- **Load Balancing:**

Load Balancingدر پروتکل های مسیریابی بر دو نوع می باشد :

۱. Equal Load Balancing

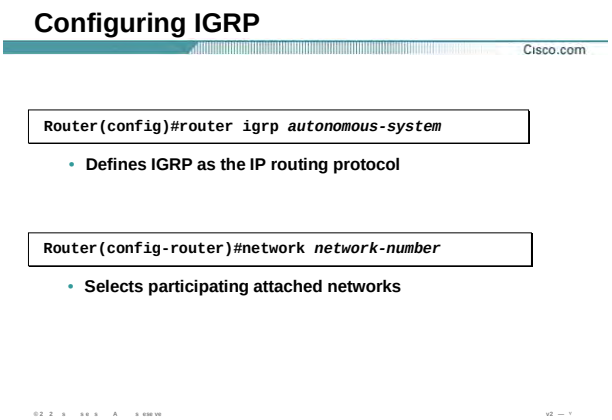
۲. Unequal Load Balancing



بررسی متریک در IGRP (ادامه) :

در Equal Load Balancing ترافیک بین مسیرهایی که متریک یکسان دارند تقسیم می شود . درواقع مسیرهایی که دارای تعداد گام یکسان تا شبکه مقصد باشند در load Balancing شرکت می کنند . RIP به صورت پیش فرض تا 4 مسیر را به صورت default در Load Balancing شرکت می دهد. اما در Unequal Load Balancing همانطور که از نامش پیداست لزومی ندارد که مسیرهای که در این Load Balancing شرکت می کنند از نظر عددی همگی دارای متریک یکسانی باشند. ما در این حالت یک رنج قابل قبول را تعریف می کنیم و مسیرهایی که متریکشان در این رنج قرار گرفت در عملیات Load Balancing شرکت می کنند. این کار را با تغییر Variance روی یک روتر انجام می دهیم .

در ادامه با این واژه و نحوه عملکرد آن آشنا می شوید. بنابراین IGRP ، Unequal Load Balancing را پشتیبانی می کند.



پیکربندی IGRP :

تا به اینجا با مفاهیم اولیه پروتکل مسیریابی IGRP آشنا شدید. در این قسمت با پیکربندی آن آشنا خواهید شد.

پیکربندی این پروتکل همانند دیگر پروتکل های Dynamic در دو مرحله صورت می پذیرد.

۴. فعال کردن پروتکل مسیریابی

۵. معرفی شبکه های Connect به روتر که با این پروتکل مسیریابی کار می کنند.

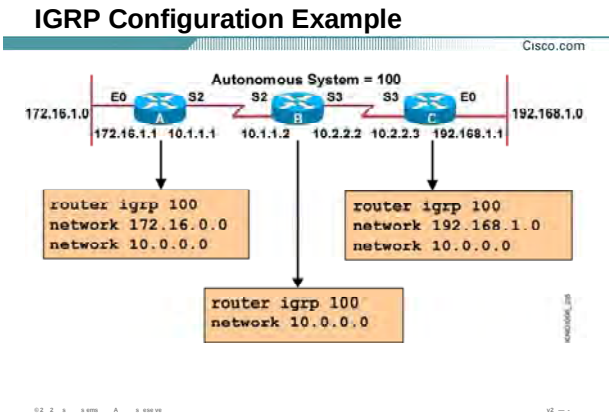
گام اول : معرفی نوع پروتکل مسیریابی می باشد که قرار است آن را روی روتر فعال کنید. برای این منظور فرمان زیر را در Global Mode وارد می کنیم .

Router(config)#router igrp autonomous-system

نکته : تمام روترهایی که قراراست با یکدیگر کار کنند و تبادل information داشته باشند می بایست در یک AS Number یکسان قرار داشته باشند.

گام دوم : می بایست که به هر روتر شبکه های Connect که قرار است در IGRP شرکت کنند را معرفی کنید. برای این منظور فرمان زیر را در Router-mode وارد می کنیم.

Router(config-router)#network network-number



پیکربندی IGRP در یک مثال:

هر سه روتر A ، B و C در یک AS با شماره 100 قرار دارند و می خواهیم پروتکل IGRP را روی روترهای این AS فعال کنیم.

به طور مثال راه اندازی IGRP را روی روتر A بررسی می کنیم.

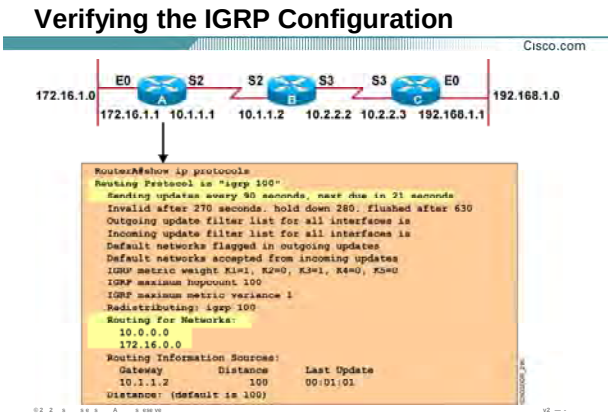
گام اول فعال کردن IGRP روی این روتر می باشد. برای این منظور فرمان زیر را در global mode وارد می کنیم:

Router(config)#router igrp 100

بعد از فعال شدن این پروتکل نوبت به معرفی شبکه های می رسد که این پروتکل می بایست آن را به دیگر روترها advertise کند. روتر A دارای دو شبکه Connect با Network ID های 172.16.0.0 و 10.0.0.0 می باشد.بنابراین به صورت زیر آنها را معرفی می کنیم:

Router(config-router)#network 172.16.0.0

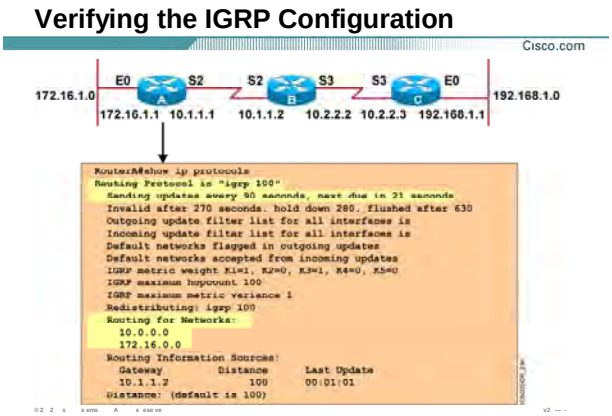
Router(config-router)#network 10.0.0.0



بررسی تنظیمات در IGRP:

تا به اینجا با مفاهیم اولیه پروتکل مسیریابی IGRP و نحوه پیکربندی آن آشنا شدید. همانطور که می دانید IGRP یک پروتکل Distance-Vector می باشد ، بنابراین برخلاف پروتکل های Link-State توپولوژی شبکه را نگهداری نمی کند بلکه فقط بهترین مسیرها به شبکه های محلی و غیرمحلی را مشخص کرده و آنها را در یک Table تحت عنوان Routing Table نگهداری می کند. برای دیدن محتویات این Table فرمان show ip Route به کار می بریم . همانطور که می دانید IGRP پروتکلی است که Update ها را به صورت Periodic و به صورت Full Update ارسال می کند. همچنین IGRP دارای timer های مختلفی می باشد که به کمک فرمان show ip protocol می توانید آنها را مشاهده کنید.

Timer ها در IGRP عبارتنداز Update ، Invalid ، Holddown و Flush که به صورت پیش فرض به ترتیب 90 ، 270 ، 280 و 630 می باشد .



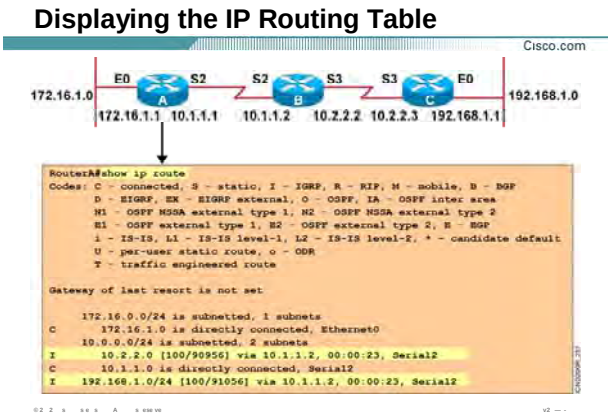
بررسی تنظیمات در IGRP (ادامه):

فرمول متریک در IGRP به صورت زیر می باشد:

Metric = [(k1 * BW) + (K2 * BW) + (K3 * Delay)] + K5 (256 – Load) (Reliability + K4)

همانطور که می دانید به صورت پیش فرض پارامترهای Bandwidth و Delay در تعیین متریک نقش دارند .

بنابراین ضرایب K2=K4=K5=0 و K1=K3=1 می باشد. می توانید این ضرایب را در خروجی فرمان show ip protocol مشاهده کنید.



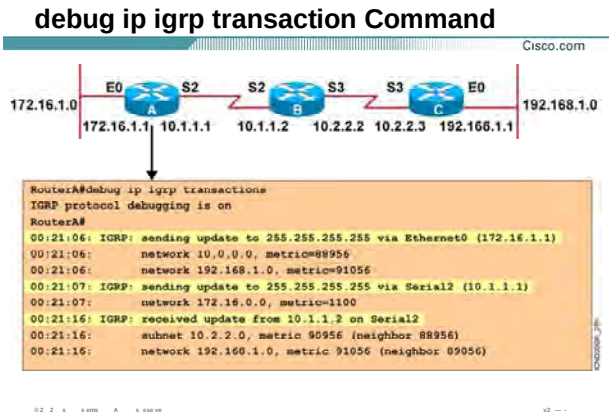
بررسی Routing Table در IGRP :

برای دیدن محتویات Routing Table ، فرمان Show ip Route را در user mode و یا Privileged mode بکار می بریم.

همانطور که می دانید این Table شامل لیست شبکه های Connect و غیر Connect که به کمک پروتکل IGRP بـه روتـر معرفی شده است می باشد.

شبکه های غیرمحلی با علامت (I) مشخص شده و شبکه های Connect با علامت (C) .

درمقابل هر شبکه ای که در Routing Table درج شده است متریک محاسبه شده تا آن شبکه نیـز در مقابـل آن شـبکه درج می شود. به طور مثال در تصویر بالا ، شبکه 10.2.2.0 از طریق اینترفیس Serial 2 با متریـک 90956 قابـل دسـترس می باشد.



بررسی عملکرد IGRP به کمک فرمان Debug :

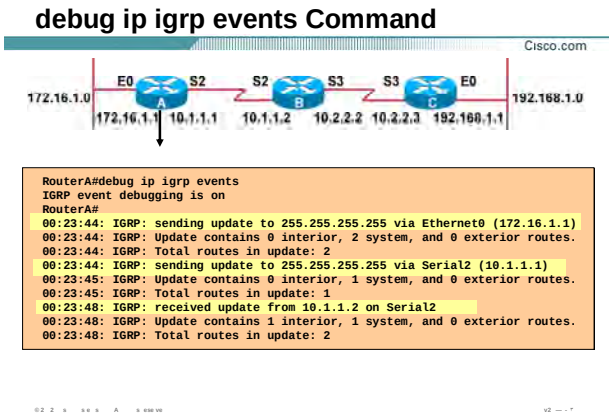
به کمک این فرمان می توانید پکتهایی که از اینترفیس های مختلف روتر خارج و یا وارد این اینترفیس ها می شوند را با جزئیات مشاهده کنید. پارامتر اصلی این فرمان IP-Address می باشد.

درصورتی که روتر پکتی را از یکی از اینترفیس هایش و از طریق روتر مجاور دریافت کند، پیام Receive Update From IP-Address on Interface را دریافت می کند که در این پیام IP-Address ، آدرس اینترفیس روتر مجاور و interface نام اینترفیس از خود روتر که Update را از طریق آن دریافت کرده می باشد. در کنار این پیام زمان دریافت Update از طریق اینترفیس مربوطه نیز مشخص می شود. درصورتی که روتر بخواهد Update را ارسال کند آن را به آدرس 255.255.255.255 (Broadcast Address) در پروتکل IGRP از طریق تمامی اینترفیس هایش ارسال می کند.

بعد از ارسال Update این پیام زیر در Command Prompt نمایش داده می شود :

Sending Update to 255.255.255.255 via Interface

برای غیرفعال کردن Debugging ، از فرمان no debug ip igrp transaction و یا no debug all در Prevailed mode استفاده می کنیم.



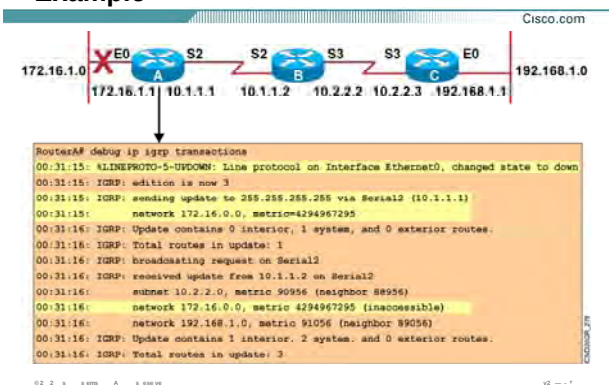
بررسی عملکرد IGRP به کمک فرمان Debug :

زمانی که در AS تعداد زیادی Network موجود باشد بنابراین Update ها شامل اطلاعات بیشتری خواهند بود . بنابراین خروجی Debugging سطرهای بیشتری خواهد داشت . برای خلاصه کردن خروجی Debug ip igrp از کلمه Events در انتهای فرمان استفاده می کنیم.

بنابراین خروجی این فرمان مانند خروجی فرمان Debug ip igrp Transaction می باشد با این تفاوت که به جای معرفی Network ها فقط تعداد آنها را می آورد.

برای غیرفعال کردن این فرمان نیز از کلمه no در ابتدای فرمان و یا Undebug all را به کار می بریم.

Updating Routing Information Example



بررسی تأثیر قطع شدن یک Link در IGRP:

برای آشنایی بیشتر با پروتکل IGRP که یک پروتکل Distance-Vector می باشد به این Scenario توجه کنید.

شبکه ای با سه روتر که هر ک ام دارای دو ش که Connect می باشد در نظر بگیرید.

فرض کنید که پروتکل مسیریابی IGRP را روی تک تک آنها Run کرده و هر کدام از آنها نیز Routing Table خود را کامل کرده اند و شبکه به حالت پایدار رسیده است.

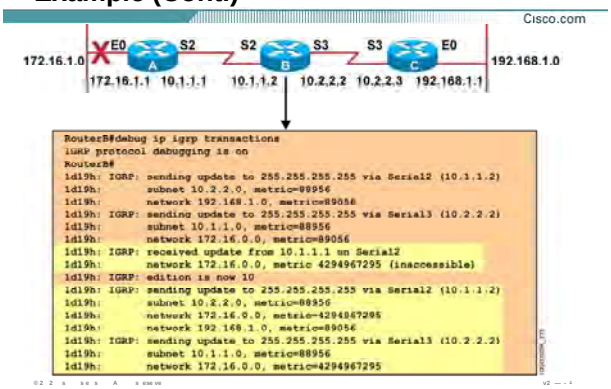
فرض کنید به صورت دستی اینترفیس E0 از روتر A را s ut down کنیم.

بنابراین روتر A با ارسال Update از طریق اینترفیس S2 (Triggered Update) ،بی نهایت شدن متریک شبکه 172.16.1.0 را به روتر مجاور یعنی روتر B اعلام می کند.(زمان 00:31:15)

روتر B این Update را دریافت کرده و در Routing Table اش اصلاحات را انجام می دهد و بلافاصله Update ایی را به روتر A می فرستد و inaccessible شدن شبکه 172.16.1.0 را به روتر a اعلام می کند.

بنابراین روتر در زمان 00:31:16 ، Update را از طریق اینترفیس Serial 2 دریافت می کند که شبکه 172.16.1.0 را با متریک بی نهایت (4294967295)گزارش داده است(Spli Horizon With Poison Reverse)

Updating Routing Information Example (Cont.)

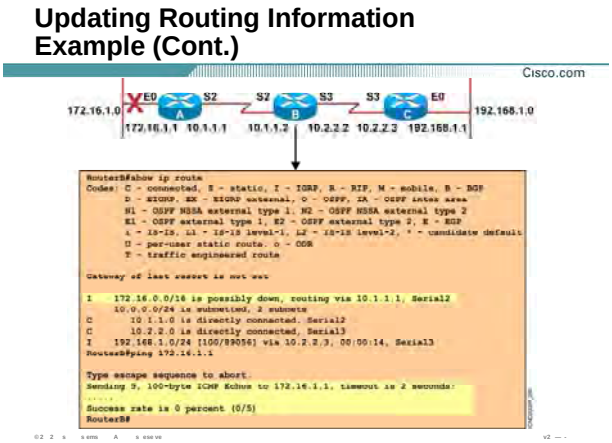


بررسی تأثیر قطع شدن یک Link در IGRP (ادامه):

روتر B به محض دریافت Triggered Update از روتر A ، Routing Table اش را اصلاح می کند. بنابراین می بایست به روترهای مجاورش این تغییرات را اعلام کند.

به روتر A بنابه قانون Poison Reverse که یک قانون جلوگیری از Loop می باشد ، شبکه 172.16.1.0 را با متریک بی نهایت گزارش می دهد و با یک Triggered Update ، Possibly down شدن شبکه 172.16.1.0 را به روتر C گزارش می دهد.

روتر B با گرفتن Triggered Update از روتر A به حالت Hold down می رود بنابراین تا به پایان رسیدن این زمان هر Update دیگری که این شبکه را با متریک بیشتر advertise کند نشنیده گرفته و drop می کند.

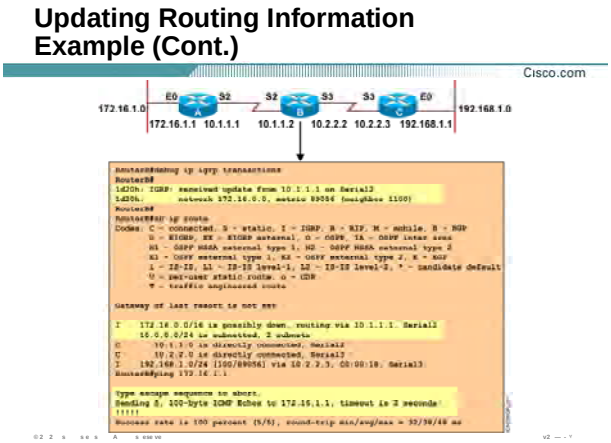


بررسی تأثیر قطع شدن یک Link در IGRP(ادامه):

روتر B با شنیدن خبر Down شدن شبکه 172.16.1.0 به حالت Down می رود .

همانطور که می دانید زمان Holddown در IGRP ، 280 ثانیه می باشد. بنابراین روتر B شبکه 172.16.1.0 را با possibly Down مارک زده و تا پایان زمان 280 ثانیه منتظر مانده و هیچ ترافیکی را به این شبکه هدایت نمی کند.

پس درصورتی که شبکه 172.16.1.0 را Ping کنید پاسخی را دریافت نمی کنید.



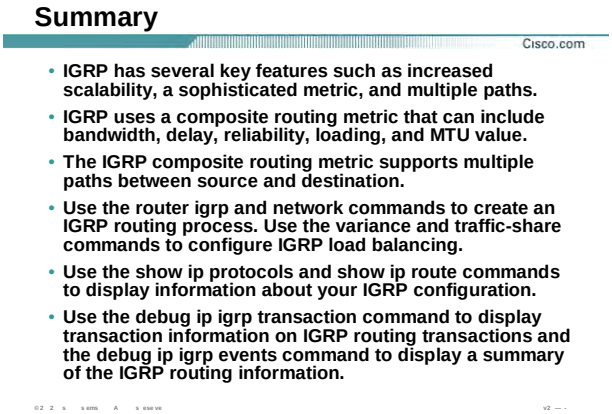
بررسی تأثیر قطع شدن یک Link در IGRP(ادامه):

درصورتی که اینترفیس E0 را که به صورت دستی shut Down کرده بودیم را فعال کنیم ، روتر A بلافاصله Routing Table اش را اصلاح می کند و Update ایی را به روتر B مبنی بر accessible شدن شبکه 172.16.1.0 ارسال می کند(Triggered Update).

بنابراین روتر B با دریافت Update تا پایان زمان Hold down منتظر مانده و سپس Routing Table اش را Update می کند.

بنابراین تا به پایان رسیدن زمان Hold down در مقابل شبکه 172.16.1.0 واژه Possibly Down باقی می ماند.

در صورتی که شبکه 172.16.1.0 را Ping کنید مشاهده می کنید که جواب Ping (echo Reply) مثبت می باشد در حالی که هنوز در Routing Table این شبکه Possibly Down می باشد.



خلاصه :

IGRP (Interior Gateway Routing Protocol) یک پروتکل مسیریابی Distance-Vector می باشد. بنابراین پروتکلی است که اطلاعات شبکه های محلی و غیرمحلی را در یک Routing Table نگهداری می کند. ویژگی عمده این پروتکل Periodic بودن آن می باشد . متریک در این پروتکل برخلاف RIP به چند پارامتر وابسته می باشد. پارامترهایی که در تعیین متریک نقش دارند عبارتنداز Load ، Delay، Bandwidth ، Reliability و MTU که به صورت پیش فرض IGRP در تعیین متریک فقط دو پارامتر Bandwidth و Delay را دخالت می دهد. برای فعال کردن این پروتکل روی یک روتر دو مرحله را می بایست اجرا کنید :

۵. فعال کردن پروتکل مسیریابی
۶. معرفی شبکه های Connect به روتر که با این پروتکل مسیریابی کار می کنند.

به کمک فرمان Debug می توانید پکتهایی که از اینترفیس های مختلف روتر خارج می شود و یا وارد این اینترفیس ها می شوند را با جزئیات مشاهده کنید. پارامتر اصلی این فرمان IP-Address می باشد.

درس ششم :

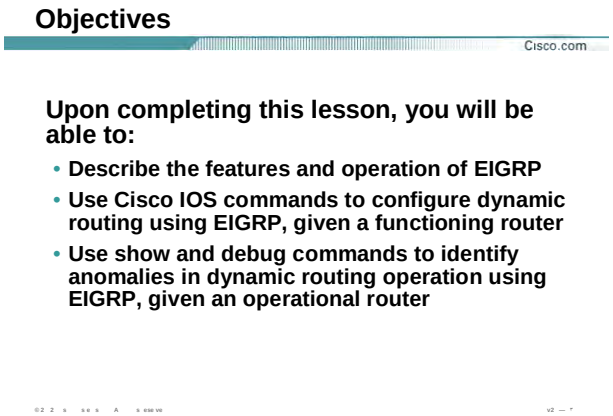
پروتکل مسیریابی
EIGRP

هدف :

۱. آشنایی پروتکل مسیریابی EIGRP .

۲. پیکربندی و تنظیم پروتکل EIGRP .

۳. اشکال زدایی در EIGRP .



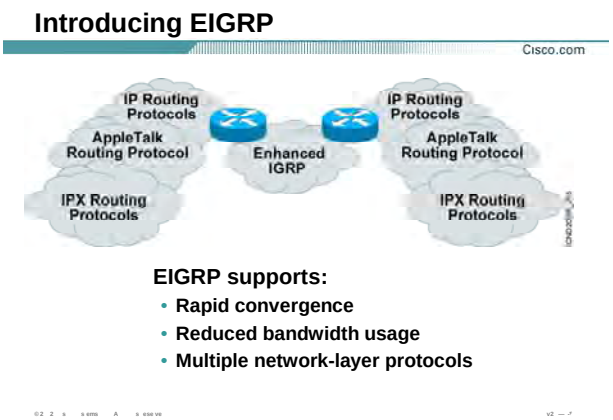
مروری بر پروتکل EIGRP :

EIGRP (Enhanced interior Gateway Routing Protocol) ، نسخه پیشرفته IGRP می باشد که توسط شرکت Cisco طراحی و استاندارد شده است .

EIGRP جزء دسته پروتکل IGPs می باشد که در داخل AS فعالیت می کند .

این پروتکل با هر نوع Topology و Media ایی سازگار می باشد. بنابراین با یک طراحی خوب شبکه ، EIGRP باسرعت Convergence بالا وOverhead کمتری فعالیت می کند .

در این درس با نحوه پیاده سازی و Monitoring آن آشنا خواهید شد.



معرفی پروتکل EIGRP (ادامه):

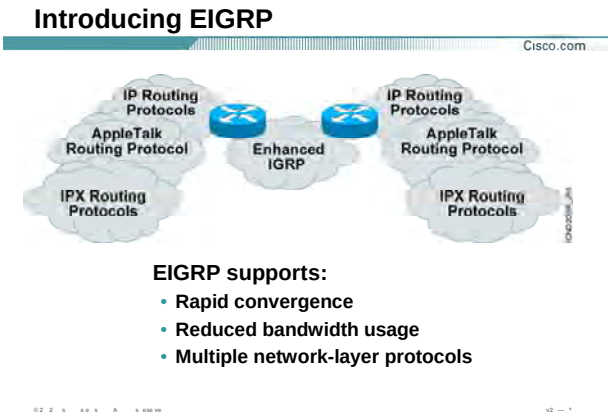
همانطور که می دانید پروتکلهای Dynamic دارای سه دسته بندی به صورت زیر می باشند:

۵. Distance-Vector

۶. Link- state

۷. Hybrid

دسته سوم یعنی Hybrid همانطور که از نامش پیداست از ویژگیهای Link-State و Distance-Vector بهترین ها را انتخاب کرده است. نمونه پروتکل از این دسته EIGRP می باشد.EIGRP در واقع یک پروتکل Hybrid می باشد. مانند Distance-Vector عمل می کند چون بین روتر مبدا و روتر مقصد یک بردار در نظر می گیرد و در صورتی که تغییری درشبکه رخ دهد این تغییر به صورت برداری بین روتر های مجاور منتقل می شود . اما نکته ای که اینجا وجود دارد این است که بر خلاف پروتکل های Distance-Vector این Update به صورت Full Update ارسال نمی شود. بلکه فقط تغییرات به روتر های دیگر اعلام می شود . از طرفی مانند پروتکل های Link-State می باشد زیرا روتر نیاز به دانستن توپولوژی شبکه دارد و با دانستن توپولوژی شبکه بهترین مسیر ها را انتخاب می کند .



معرفی پروتکل EIGRP (ادامه):

بنابراین در EIGRP مانند پروتکل های Link-State ایی Routing Table گزارش داده نمی شود بلکه فقط اطلاعات Topology Table را به دیگر روتر ها گزارش می دهد .

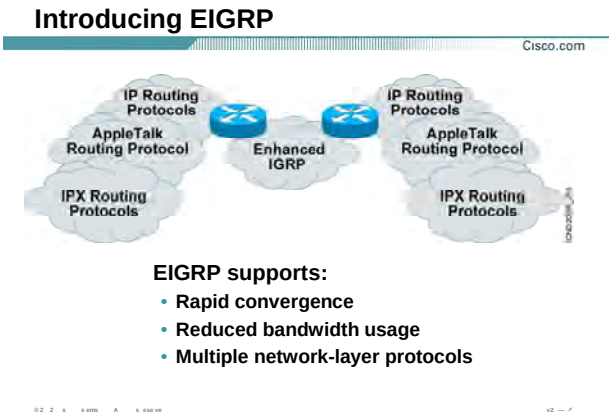
یک طراحی خوب برای شبکه می تواند سرعت همگرایی EIGRP را چندین برابر افزایش داده و ترافیک شبکه را کاهش می دهد . EIGRP دارای اطلاعات مختلفی است که در Table های مختلفی ذخیره و نگهداری می شود .

این Table ها عبارتند از Topology Database که شامل توپولوژی شبکه می باشد و Routing Table که شامل کوتاهترین مسیر ها به Network های مختلف و Neighboring Table که اطلاعات روتر های مجاور به روتر می باشد.

بعضی از ویژگیهای اصلی پروتکل مسیریابی EIGRP به قرار زیر می باشد:

- سرعت بالای همگرایی در صورتی که تغییری در شبکه رخ دهد. EIGRP با به کار بردن الگوریتم Diffusing Update Algorithm (DUAL) سرعت همگرایی شبکه را افزایش می دهد .

نکته قابل توجه ای که EIGRP دارد این است که علاوه بر مسیر اصلی یک یا چند مسیر Back up به هر شبکه در Topology Database نگهداری می کند.



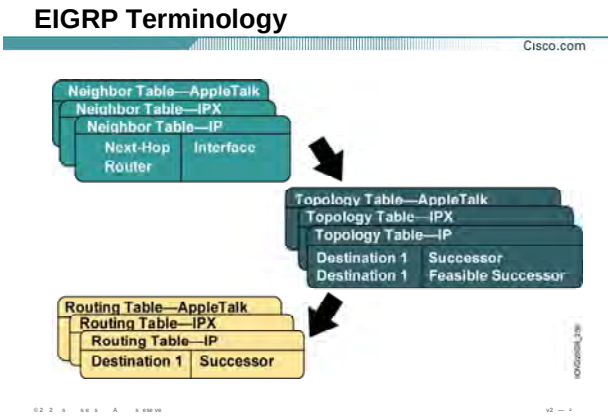
معرفی پروتکل EIGRP (ادامه):

بنابراین با Down شدن مسیر اصلی روتر دیگر الگوریتم Dual را برای پیدا کردن مسیر دیگر به آن شبکه اجرا نمی کند.

پس داشتن مسیر Back up باعث افزایش سرعت همگرایی در شبکه می شود .

زمانی که از EIGRP به عنوان پروتکل مسیر یابی استفاده می کنیم منابع کمتری از شبکه در گیر این پروسه می شوند Hello Packet ها تنها ترافیکی از EIGRP هستند که ر شبکه Stable منتقل می شود .در واقع EIGRP مانند پروتکل های Link-State ایی با به کار بردن Hello Packet رابطه همسایگی ر با روتر مجاور برقرار می کند .هر روتر اطلاعاتی راکه توسط Hello packet ها از روتر هایی که با انها رابطه همسایگی بر قرار کرده (Adjacency) را دریافت می کند و در Neighboring Table نگهداری می کند .

- EIGRP بر خلاف پروتکل های Distance-Vector ایی از Periodic Update ستفاده نمی کند بلکه در صورتیکه تغییری در Routing Table رخ دهد فقط تغییرات را اعلام می کند .بنابر این پهنای با د کمتری را صرف ارسال Update های مربوط به پروتکل می کند.



بررسی مفاهیم اولیه در EIGRP :

EIGRP پروتکل مسیر یابی است که علاوه بر IP Routed Protocol ، پروتکل های IPX وApple Talk رانیز پشتیبانی می کند .روتری که با EIGRP کار می کند اطلاعاتش را درون سه Table نگهداری می کند:

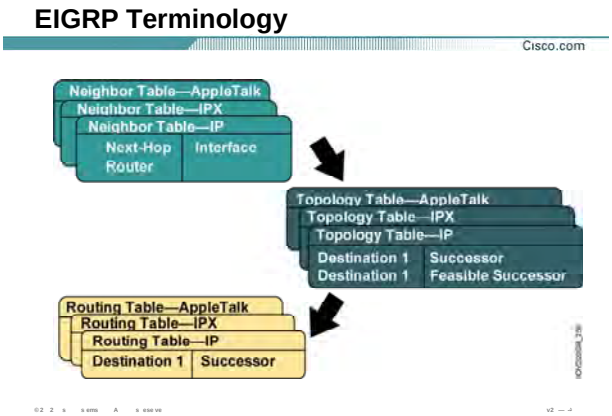
۱. Neighboring table

۲. Topology table

۳. Routing table

Neighboring table: این Table شامل اطلاعاتی از روتر هایی است که با آنها رابطه همسایگی بر قرار کرده است . این اطلاعات شامل IP Address و اینترفیس روتر مجاور می باشد، که با این روتر ارتباط point-to-point دارد .

Topology table : این Table شامل تمامی مسیر های شدنی به مقصد های مختلف می باشد. در واقع توپولوژی شبکه را در این Table نگهداری می کند و روتر با Run کردن الگوریتم DUAL بهترین مسیرها را به شبکه های مختلف انتخاب کرده و انها را Routing table اش قرار می دهد . در واقع دراین مرحله Successor وFeasible Successor ها مشخص می شوند . در ادامه با این مفاهیم آشنا خواهید شد .



بررسی مفاهیم اولیه در EIGRP (ادامه):

Routing table: روتر بعد از اینکه Topology Table خود را کامل کرد الگوریتم DUAL را که مخصوص بـه پروتکـل EIGRP می باشد ،اجرا و بهترین مسیرها را پیدا کرده و در Routing table قرار می دهد .

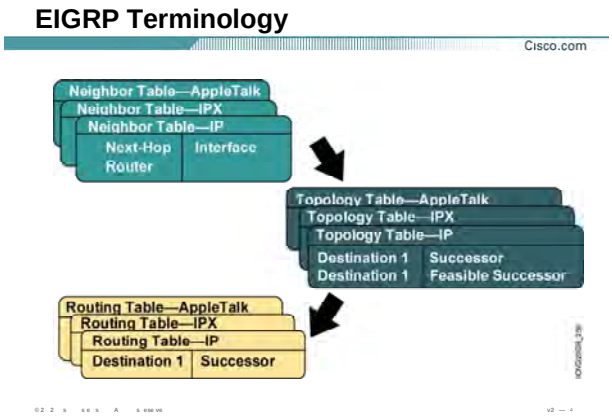
تا بـه اینجـا بـا محتویـات Routing Table و Topology table آشـنا شـدید . پروتکـل EIGRP تنهـا Routing protocol ایـی است که علاوه بر مسیر اصلی یک مسیر Back up به هر Destination در نظر می گیرد و در صـورتی کـه مـسیر اصـلی Down شود مسیر دوم بدون Run شدن الگوریتم DUAL جایگزین مسیر اول می شود و این مطمئن بودن این پروتکـل را نشان می دهد. اما انتخاب این دو مسیر چگونه صورت می گیرد ؟

به مفاهیم زیر توجه کنید تا با نحوه عملکرد آن بیشتر آشنا شوید.

(RD) Reported Distance: متریکی است که توسط روتر مجاور تا مقصد محاسبه شده و گزارش داده می شود.

(FD) Feasible Distance: در میان متریکهای مختلفی که از خود روتر تا مقصد وجود دارد، متریکی که کمتـرین مقـدار را داشته باشد به عنوان FD انتخاب می شود.

Successor: مسیری که متریک FD را داشته باشد به عنوان مسیر Successor انتخاب می شود. درواقـع مـسیری کـه دارای کمترین متریک باشد.



بررسی مفاهیم اولیه در EIGRP (ادامه):

Feasible Condition (FC): درصورتی که در مسیری FD<RD باشد در این حالت شرایط برای انتخاب شدن مسیر به عنوان مسیر Back up فراهم شود. در واقع برای پیدا کردن feasible Successor می بایست این شرایط بر قرار شود و مسیری که در این شرایط صدق کند به عنوان مسیر Back up در نظر گرفته می شود و در Topology table قرار می گیرد .

Feasible Successor: مسیر Backup برای مسیر Successor می باشد و مسیری است که در شرایط FC صدق می کند.

Comparing EIGRP and IGRP

Cisco.com

- **Similar metric**
- **Same load balancing**
- **Improved convergence time**
- **Reduced network overhead**

مقایسه دو پروتکل IGRP و EIGRP :

تا به اینجا با ویژگیهای EIGRP آشنا شدید . در این قسمت می خواهیم به مقایسه بین دو پروتکل مسیر یابی Cisco ای یعنی EIGRP وIGRP بپردازیم.

EIGRP یک پروتکل مسیر یابی Distance-Vector می باشد .عمده ترین ویژگی که پروتکل های Distance-Vector دارا می باشند Periodic بودن آنها است.

ویژگی ای که در شبکه های با اندازه بزرگ چندان خوب نیست و منجر به افزایش ترافیک و کاهش سرعت Convergence در شبکه می شود.

EIGRP یک پروتکل Distance-Vector پیشرفته می باشد . درواقع پروتکلی است که هم Distance-Vector است و هم Link-State .

متریک EIGRP مانند IGRP می باشد و فقط مقدار بدست آمده در عدد 255 ضرب می شود.

در واقع پارامترهایی که در محاسبه متریک نقش دارند عبارتند از bandwidth ، Load ، Delay ، Reliability ، MTU و به صورت Default دو متغیر Bandwidth و Delay درمحاسبه متریک نقش دارند.

- **Similar metric**
- **Same load balancing**
- **Improved convergence time**
- **Reduced network overhead**

مقایسه دو پروتکل IGRP و EIGRP (ادامه):

هردو Unequal load Balancing را پشتیبانی می کنند. بنابراین در صورتی که چند مسیر به یک مقصد با متریک متفاوت وجود داشته EIGRP مانند IGRP به صورت Default تا چهار مسیر را انتخاب کرده و ترافیک را بین آنها Balance می کند.

سرعت همگرایی در EIGRP خیلی بیشتر از IGRP می باشد . زیرا EIGRP یک مسیر Backup در Topology Table نگهداری می کند . بنابراین در صورت Down شدن مسیر اصلی (Successor) ،مسیر Backup (Feasible Successor) بدون اجرای مجدد الگوریتم DUAL جایگزین می شود. لذا سرعت همگرایی(Convergence) پروتکل روی تک تک روترها در شبکه افزایش پیدا می کند. تا به اینجا با مفاهیم اولیه پروتکل مسیریابی EIGRP آشنا شدید. در این قسمت با پیکربندی آن آشنا خواهید شد.

پیکربندی این پروتکل همانند دیگر پروتکل های Dynamic در دو مرحله صورت می پذیرد.

۶. فعال کردن پروتکل مسیریابی

۷. معرفی شبکه های Connect به روتر که با این پروتکل مسیریابی کار می کنند.

- **Similar metric**
- **Same load balancing**
- **Improved convergence time**
- **Reduced network overhead**

مقایسه دو پروتکل IGRP و EIGRP (ادامه):

گام اول : معرفی نوع پروتکل مسیریابی می باشد که قرار است آن را Run کنید .

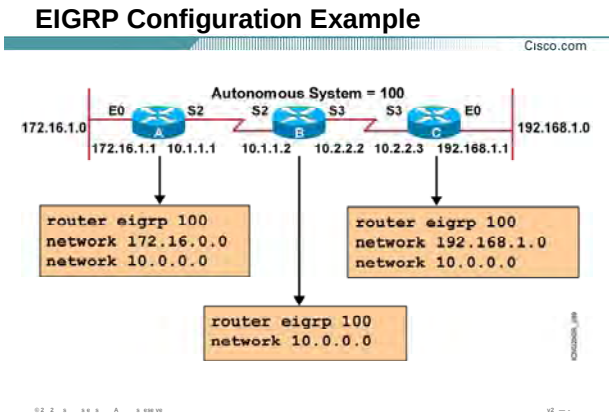
برای این منظور فرمان زیر را در Global Mode وارد می کنیم .

Router(config)#router eigrp autonomous-system

نکته : تمام روترهایی که قراراست با یکدیگر کار کنند و تبادل information داشته باشند می بایست در یک AS Number یکسان قرار بگیرند.

گام دوم : می بایست که به هر روتر شبکه های Connect را معرفی کنید. برای این منظور فرمان زیر را Router Mode وارد می کنید.

Router(config-router)#network network-number



پیکربندی پروتکل EIGRP در یک مثال:

هر سه روتر A ، B و C در یک AS با شماره 100 قرار دارند و می خواهیم پروتکل EIGRP را روی روترهای این AS فعال کنیم.

به طور مثال راه اندازی EIGRP را روی روتر A بررسی می کنیم.

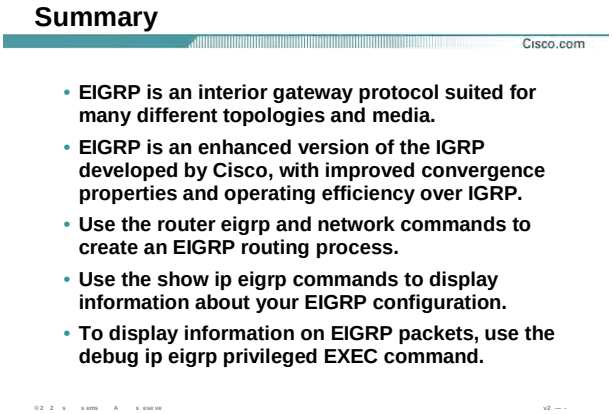
گام اول فعال کردن EIGRP روی این روتر می باشد. برای این منظور فرمان زیر را در global mode وارد می کنیم:

Router(config)#router eigrp 100

بعد از فعال شدن این پروتکل نوبت به معرفی شبکه های می رسد که این پروتکل می بایست آن را به دیگر روترها Advertise کند. روتر A دارای دو شبکه Connect با Network ID های 172.16.0.0 و 10.0.0.0 می باشد.بنابراین به صورت زیر آنها را معرفی می کنیم:

Router(config-router)#network 172.16.0.0

Router(config-router)#network 10.0.0.0



خلاصه :

EIGRP (Enhanced interior Gateway Routing Protocol) ، نسخه پیشرفته IGRP می باشد که توسط شرکت Cisco طراحی و استاندارد شده است .EIGRP جزء دسته پروتکل IGPs می باشد که در داخل AS کار فعالیت می کند .

EIGRP پروتکل مسیر یابی است که علاوه بر IP Routed Protocol ، پروتکل های IPX وApple Talk رانیز پشتیبانی می کند .روتری که با EIGRP کار می کند اطلاعاتش را درون سه Tableنگهداری می کند: Neighboring table ، Topology table ، Routing table.

EIGRP علاوه بر مسیر اصلی یک مسیر Backup در Topology Table نگهداری می کند تا در صورت down شدن مسیر اصلی بدون اجرای مجدد الگوریتم DUAL مسیر دوم جایگزین مسیر اول شود . بنابراین سرعت همگرایی شبکه افزایش پیدا می کند. برای فعال کردن این پروتکل روی یک روتر دو مرحله را می بایست اجرا کنید :

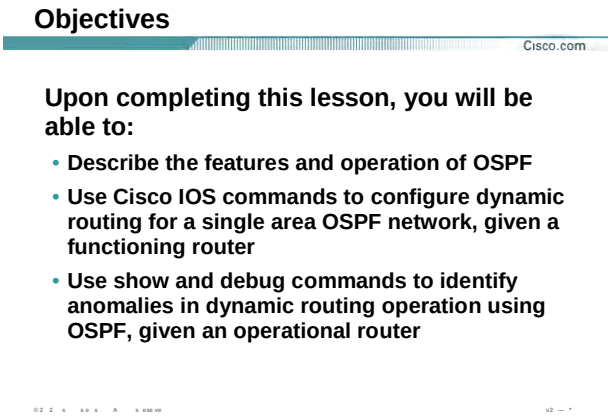
۱. فعال کردن پروتکل مسیریابی
۲. معرفی شبکه های Connect به روتر که با این پروتکل مسیریابی کار می کنند.

درس هفتم :

پروتکل مسیریابی
OSPF

هدف :

۱. آشنایی پروتکل مسیریابی OSPF .
۲. پیکربندی و تنظیم پروتکل OSPF .
۳. اشکال زدایی در OSPF.



مروری بر پروتکل OSPF :

همانطور که می دانید Dynamic Routing Protocol به ۳ دسته تقسیم بندی می شوند :

۱. Distance-Vector

۲. Hybrid

۳. Link-State

بادو دسته اول در درس های گذشته آشنا شدید . در این درس با پروتکل OSPF از دسته سوم یعنی Link-State اشنا خواهید شد .

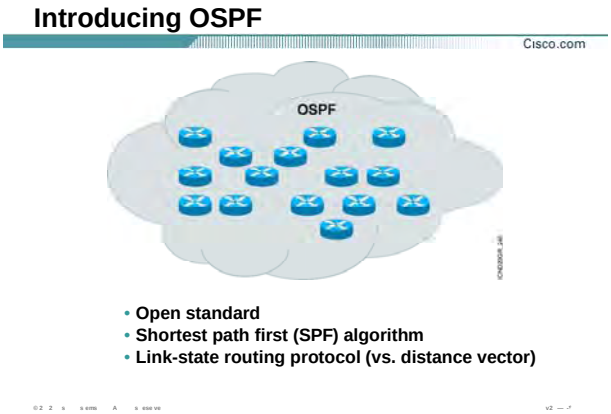
OSPF همانند RIP، IGRP و EIGRP یک پروتکل IGPs می باشد . بنابراین دامنه عملکرد آن در داخل AS می باشد.

در این درس شما با پروتکل OSPF از خانواده پروتکل های Link-State ایی و نحوه راه اندازی آن آشنا خواهید شد.

برای معرفی و راه اندازی OSPF دو دسته بندی کلی درنظر گرفته می شود:

۱. Single Area OSPF

۲. Multiple Area OSPF



معرفی پروتکل OSPF :

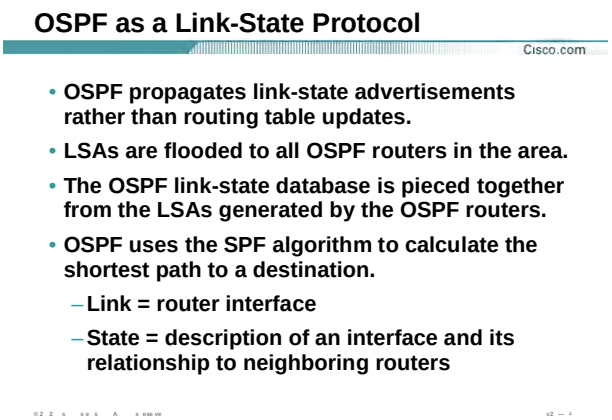
OSPF مانند RIP ، IGRP و EIGRP از دسته پروتکل های igps می باشد . این بدان معنی است این پروتکل در داخل AS عمل می کنند بر خلاف BGP که پروتکلی است بین دو AS عمل کرده و دو AS مختلف را به یکدگر مرتبط می کند .

OSPF بر خلاف IGRP و EIGRP که پروتکل استاندارد شده توسط شرکت Cisco می باشد یک پروتکل Open Source است که توسط IETF در سال ۱۹۸۸ استاندارد شده است .

این پروتکل بر پایه شبکه های IP استاندارد شده است و دارای دو ویژگی زیر است :

۱. یک پروتکل Open Standard است که در سال ۱۹۸۸ استاندارد شده و جدیدترین ورژن آن تحت عنوان OSPF Version 2 در RFC 2328 قابل دسترس می باشد .

۲. OSPF یک پروتکل بر پایه ویژگیهای Link-State ایی می باشد. این بدان معنی است که توپولوژی شبکه را به صورت یک درخت همبند بدون دور درآورده وسپس با استفاده از الگوریتمی تحت عنوان Dijkstra کوتاهترین مسیر را پیدا می کند و در Routing Table قرار می دهد.



معرفی OSPF به عنوان پروتکل Link State :

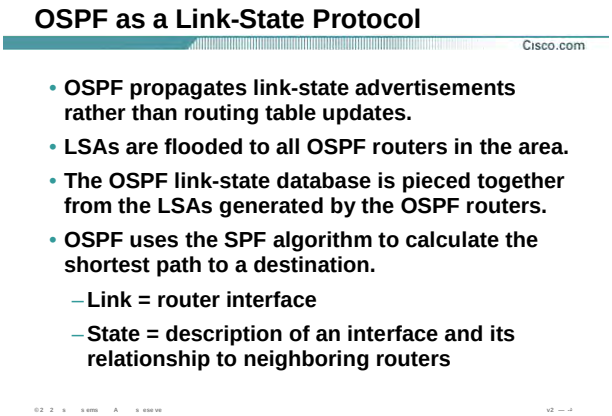
در درس های گذشته با ویژگیهای پروتکل Distance-Vector آشنا شدید. در این قسمت با مقایسه بین OSPF و پروتکل های Distance-Vector ، با این پروتکل بیشتر آشنا خواهید شد .

OSPF یک پروتکل Link-State ایی می باشد و اطلاعات شامل link ها و State هر کدام از این Link ها را در یک Link-State Database نگهداری می کند.

در واقع State مربوط به یک Link در مورد Interface و نحوه ارتباط همسایگی آن روتر با روترهای مجاور را توضیح می دهد .

توضیح در مورد یک اینترفیس شامل موارد زیر می باشد:

۱. IP Address اینترفیس
۲. Subnet Mask
۳. Type شبکه ای که اینترفیس در آن واقع شده است .به طور مثال Point-to-point یا Multipoint و یا هر Type دیگر .
۴. و غیره ...

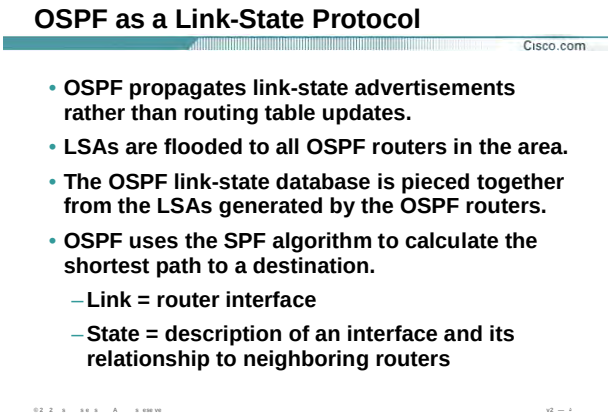


معرفی OSPF به عنوان پروتکل Link State (ادامه):

بنابراین تا به اینجا اولین اختلاف بین پرونکل OSPF و پروتکل های Distance-Vector مشخص شد. در پروتکل های Distance-Vector به جز یک Table که شامل اطلاعات بهترین مسیر ها می باشد ، اطلاعات دیگری در عملیات مسیریابی نقشی ندارد. روتر ها در OSPF به کمک ارسال پکتهایی به نام Link-State Advertisement (LSA) اطلاعات Link-State Database خود را به روترهای دیگری که در یک ناحیه مشخص قرار دارند ارسال می کند.

در صورتی که یک تغییری در Topology این ناحیه رخ دهد همچون Down شدن Network ، روتر این تغییرات را با ارسال LSA به روتر های دیگر در آن ناحیه گزارش می دهد . بنابراین OSPF بر خلاف پروتکلهای Distance-Vector ، Periodic-Update ندارد. همانطور که می دانید در پروتکلهای Distance-Vector حتی اگر تغییری در Topology شبکه رخ ندهد باز در زمانهای مشخص هر روتر کل Routing Table اش را به روتر های مجاور تحت یک Update ارسال می کند.

اما در OSPF وضعیت این گونه نیست. این بدان معنی است که در این پروتکل Periodic-Update مربوط به Routing Table وجود ندارد.



معرفی OSPF به عنوان پروتکل Link State (ادامه):

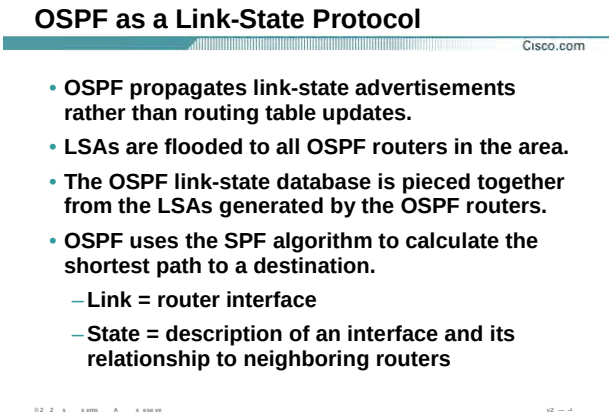
نکته: OSPF هر ۳۰ دقیقه یک بار کل اطلاعات Link-State Database اش را در ناحیه مشخص Advertise می کند.

LSA پکتها شامل اطلاعات اینترفیس های متصل و متریکی که روی هر کدام از اینترفیس ها تنظیم شده و غیره می باشد .

هر روتر در OSPF بعد از تکمیل Link-State Database خود , به کمک Run کردن الگوریتم OSPF (Dijkstra) کوتاهترین مسیر ها را پیدا کرده و آنها را در Routing Table قرار می دهد.

OSPF بر خلاف RIP ، IGRP و EIGRP می تواند در یک شبکه hierarchical عمل کند.این بدان معنی است که می توان شبکه را به ناحیه های کوچکتری تقسیم بندی کرده و سپس OSPF را روی این قسمت ها Run کنیم.

سوالی که پیش می آید این است که چه الزامی به تقسیم بندی شبکه وجود دارد؟

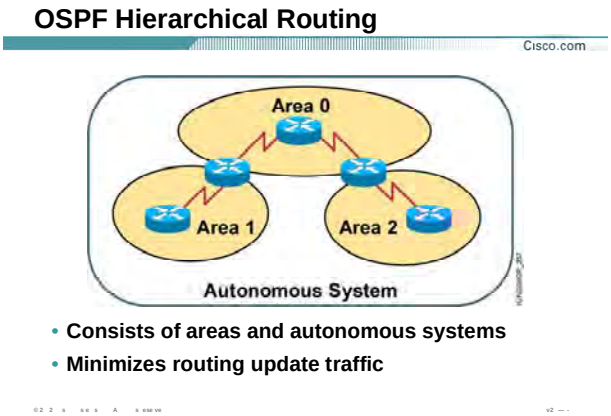


معرفی OSPF به عنوان پروتکل Link State :

همانطور که می دانید Link-State Database شامل اطلاعات توپولوژی شبکه می باشد و الگوریتم OSPF به کمک این اطلاعات کوتاهترین مسیر ها را پیدا کرده و در Routing Table اش قرار می دهد . حال اگر این Link-State Database بزرگ باشد پردازش بیشتری باید صورت گیرد.

در صورتی که با تقسیم بندی شبکه به ناحیه های کوچکتر هر روتر کافی است که توپولوژی آن ناحیه ای(Area) که در آن واقع شده را بداند. بنابراین هرچه اندازه Link-State Database کوچکتر باشد ، الگوریتم Dijkstra سریعتر عمل کرده و سرعت همگرایی شبکه بیشتر می شود .در واقع در OSPF یک AS به چندین ناحیه تحت عنوان Area تقسیم می شود که هر کدام از این Area ها شامل Network های مختلفی می باشد.

بنابراین Link-State Database یک روتر شامل تمامی اطلاعاتی است که توسط LSA ها از روترهای دیگر درون Area دریافت می شود .بنابراین روترهایی که درون یک Area قرار دارند Link-State Database خود را با یکدیگر مبادله می کنند و در نتیجه دارای Link-State Database یکسانی می شوند .



بررسی مدل لایه ای OSPF :

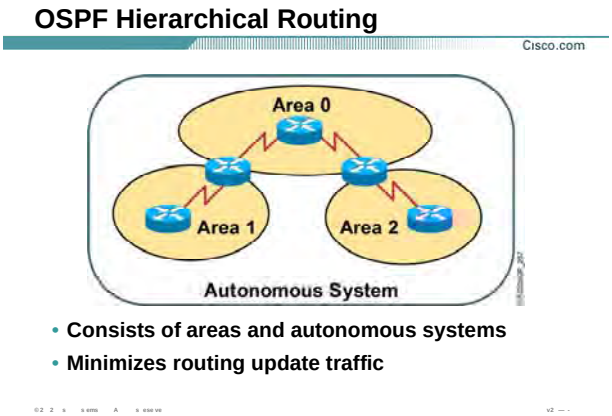
همانطور که تا اینجا متوجه شدید OSPF قادر است یک AS را به چندین ناحیه که به هر کدام از آنها یک Area گفته می شود تقسیم می کند. Area به دو دسته کلی تقسیم می شوند:

۱. Backbone Area

۲. non Backbone Area

Backbone Area: Backbone Area ، ناحیه ای است که Area های دیگر به آن متصل شده و با یکدیگر ارتباط بر قرار می کنند این Area را با Area 0 نمایش داده می شود. به روتر هایی که درون Area 0 قرار می گیرند Backbone Router گفته می شود .

Non Backbone Router: بنابراین با داشتن یک طراحی Hierarchical و داشتن چندین Area تغییر در یک Area روی کل AS تاثیر نمی گذارد بلکه فقط به صورت ناحیه ای تاثیر می گذارد .



بررسی مدل لایه ای OSPF (ادامه):

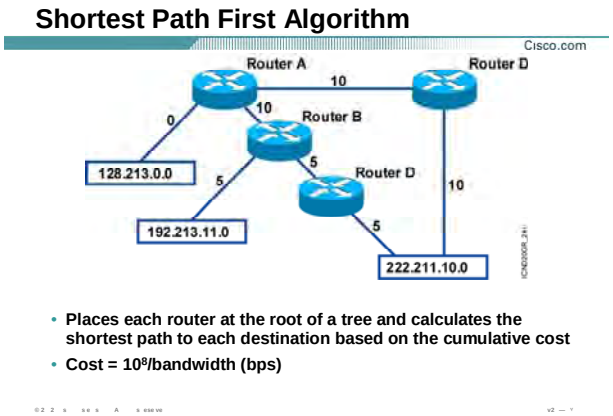
بنابراین فقط Link-State Database و Routing Table روتر های این Area دچار تغییر می شوند .

بنابراین می توان مزایای کلی طراحی Hierarchical یک AS را به صورت زیر بیان کرد:

۱. افزایش سرعت محاسبه الگوریتم SPF .

۲. کوچک شدن Routing Table .

۳. کاهش Overhead و اندازه Link-State Database و درنتیجه کاهش ترافیک در شبکه.



بررسی الگوریتم SPF :

همانطور که می دانید الگوریتم SPF ، هر روتر را به عنوان ریشه یک درخت و سپس روترهای دیگر را به صورت شاخه های درخت در نظر می گیرد . بنابراین کوتاهترین مسیر به هر کدام از Node ها را براساس متریک Cost محاسبه کرده و آن را در Routing Table خود قرار می دهد .

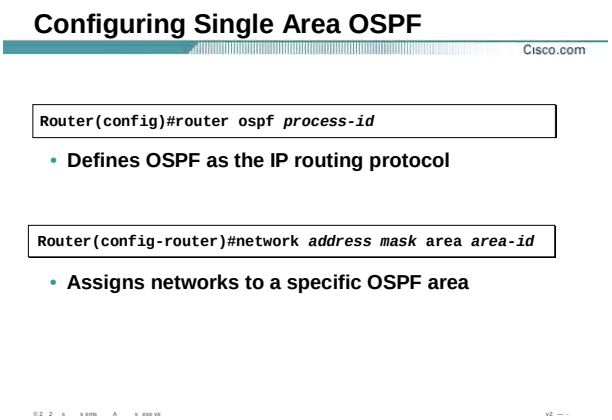
Cost مربوط به یک اینتر فیس رابطه معکوس با Bandwidth دارد .

به طور مثال یک لینک با پهنای باند 56 K دارای Overhead و Delay بیشتری نسبت به یک لینک با پهنای باند 10 Mb/s می باشد . در نتیجه بدیهی است که در انتخاب بین این دو ، لینکی که پهنای باند آن 10 Mb/s می باشد به عنوان مسیر بهتر انتخاب شود.

OSPF به صورت پیش فرض فرمولی را برای محاسبه Cost برای هر اینترفیس به صورت زیر در نظر می گیرد :

Cost=100000000/Bandwdth (in bps)

بنابراین خط T1 با پهنای باند 1.544Mbps دارای Cost با مقدار 64=100000000/1544000 می باشد.



پیکربندی OSPF در حالت Single Area :

تا به اینجا با مفاهیم او یه پروتکل مسیریابی OSPF آشنا شدید. در این قسمت با پیکربندی آن آشنا خواهید شد.

پیکربندی این پروتکل همانند گر Dynamic Routi g Protocol ها در دو مرحله صورت می پذیرد.

۱. فعال کردن پروتکل مسیریابی

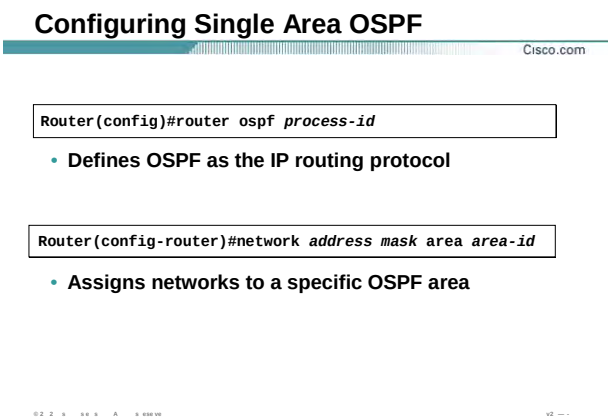
۲. معرفی شبکه های Connect به روتری که د Area مربوطه قرار گرفته اند.

گام اول : فعال کردن پروتکل مسیریابی OSPF همراه با Process-id محلی .

برای این منظور فرمان زیر را در Global Mode وارد می کنیم .

Router(config)#router ospf process-id

Process-id : عددی است که به پروسه OSPF نسبت داده می شود . روی یک وتر چندین پروسه OSPF می تواند Run شود. بنابراین نیاز به یک عدد واحدی می باشد که این پروسه ها را از یکدیگر تفکیک کند. لذا این عدد Local بوده و روی عملکرد روتر های دیگر تاثیر نمی گذارد . بنابراین روتر هایی که با OSPF کار می کنند نی زی ندارند که Process-id یکسانی داشته باشند.



پیکربندی OSPF در حالت Single Area (ادامه):

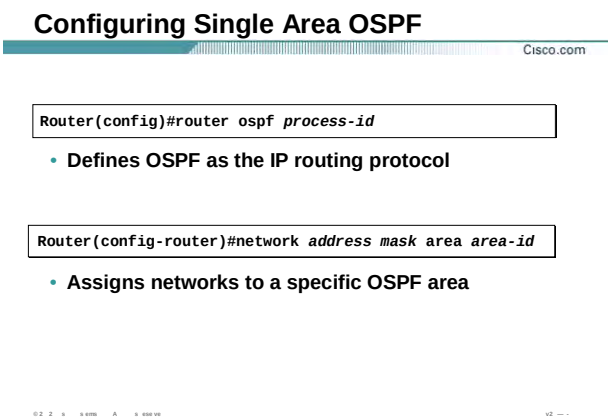
گام دوم : در این قسمت می بایست مشخص کنیم که چه شبکه هایی درپروسه OSPF شرکت می کنند .بنابراین در این قسمت شبکه های Connect ایی را که می خواهیم در OSPF شرکت کنند را معرفی می کنیم .

Router(config-router)#network address mask area area-id

اما می بایست بعد از مشخص کردن Network ، مشخص کنیم که به چه IP Address هایی از این Network و از طریق این روتر دسترسی پیدا خواهیم کرد. بنابراین به کمک Wild Card Mask این تعریف را انجام می دهیم . برای محاسبه Wild Card Mask ، کافی است در Subnet Mask مربوطه به جای بیت های ۱ بیت صفر و به جای بیت های صفر بیت ۱ قرار دهیم . به مثال زیر توجه کنید :

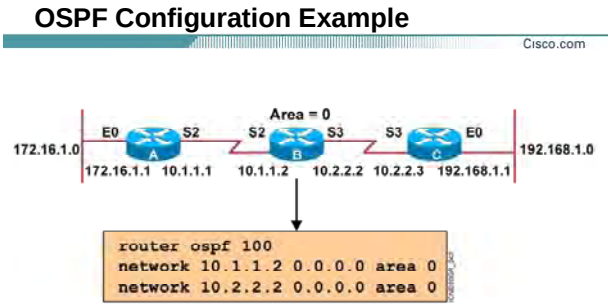
Subent mask: 255.255.0.0

Wild Card Mask: 0.0.255.255



پیکربندی OSPF در حالت Single Area (ادامه):

از طرفی حالتی پیش می آید که یک روتر از طریق دو اینترفیس مختلف در دو Area مختلف واقع می شود . بنابراین لازم است که وقتی شبکه ای را در OSPF معرفی می کنیم بگوییم که این شبکه در چه Area ای واقع شده است . بنابراین در قسمت Area-id شماره Area ایی که اینترفیس و شبکه متصله در آن واقع شده است را وارد می کنید.



پیکربندی OSPF در یک مثال:

به این شکل نمونه توجه کنید . می خواهیم پروتکل OSPF را روی این سه روتر فعال کنیم.

هر سه روتر در Area 0 واقع شده اند. به طور مثال راه اندازی OSPF را روی روتر B بررسی می کنیم .

برای راه اندازی OSPF دو گام را باید پشت سر بگذاریم .

گام اول : Run کردن OSPF روی روتر.

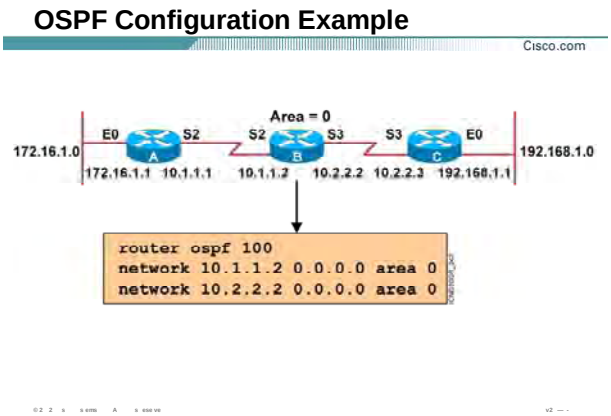
روی این روتر OSPF را با Process-id با مقدار 100 را به صورت زیر فعال می کنیم :

Router(config)#router ospf 100

گام دوم : معرفی شبکه های Connect.

رروی این روتر هم می توان شبکه های Connect را به صورت Network ID معرفی کرد و هم می توانیم Host Address (IP Address اینترفیس) را معرفی کنیم .

همانطور که می دانید Host Address دارای Subnet mask به صورت 255.255.255.255 می باشد . بنابراین Wild Card Mask آن به صورت 0.0.0.0 می باشد .

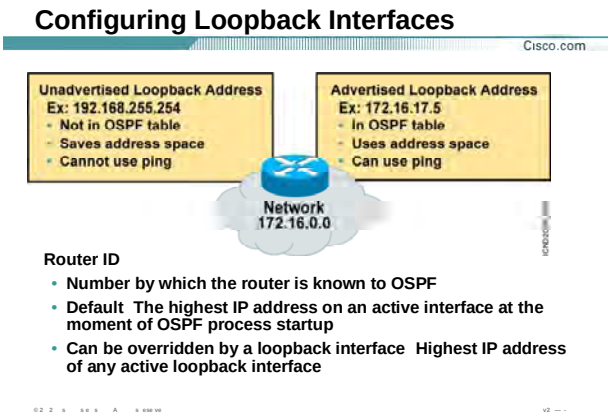


پیکربندی OSPF در یک مثال (ادامه):

Router(config-router)#network 10.1.1.2 0.0.0.0 area 0

Router(config-router)#network 10.2.2.2 0.0.0.0 area 0

این دو اینترفیس در AREA 0 واقع شده اند . بنابراین هنگام تعریف باید مشخص کنیم که در چه Area ایی واقع شده اند.



تنظیم RID در OSPF :

Router ID: مشخصه ای است که به کمک آن هر روتر در شبکه OSPF شناخته می شود. در شبکه ای که پروتکل مسیریابی OSPF اجراست هر روتر جدید خود را با RID به دیگر روترها معرفی می کند و بقیه روترها را نیز با RID هایشان می شناسد.

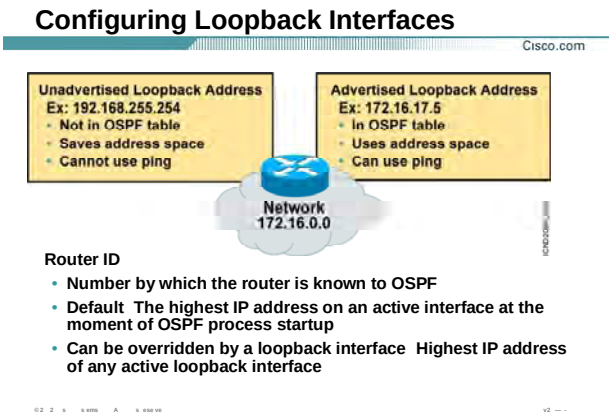
سوالی که پیش می آید این است که این عدد را چگونه می توان مشاهده کرد ؟

به صورت پیش فرض بالاترین IP Address در میان اینتر فیس های فعال یک روتر به عنوان RID یک روتر مشخص می شود .

این تعریف درست است ولی RID یک روتر پایدار نخواهد ماند. زیرا انتخاب RID را به پارامتر اینترفیس که یک پارامتر ناپایدار می باشد نسبت داده ایم . اینتر فیس در صورتی که Down شود روی عملکرد OSPF و در نتیجه انتخاب RID تاثیر خواهد داشت.

توصیه شده که برای پایدار کردن عملکرد OSPF آن را به یک پارامتر ثابت و بدون تغییر مرتبط کنید .

Loop Back Interface ، اینتر فیسی مجازی است که همیشه UP می باشد .



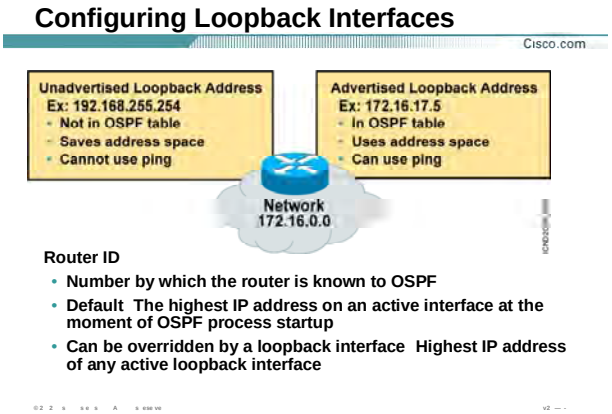
تنظیم RID در OSPF :

در واقع Loop Back Interface یک اینترفیس فیزیکی نیست . می توانید روی یک روتر تعداد زیادی اینترفیس مجازی تعریف کنید . نحوه تعریف این اینتر فیس مجازی به صورت زیر می باشد .

Router(Config)#interface loopback number

number: می تواند عددی بین 0 تا 65535 باشد . این بدان معنی است که می توانید به تعداد 65536 اینتر فیس مجازی روی یک روتر تعریف کنید . به محض تعریف آن , این اینتر فیس UP شده و تا حذف نکردن ان UP باقی می ماند. بنابراین هنگام انتخاب RID , درصورتی که روی روتر اینتر فیس Loop back تعریف کرده باشید ، اولویت اول در انتخاب RID با Loop Back Interface می باشد و از میان اینترفیس های Loop Back ، بالاترین IP Address به عنوان RID انتخاب می شود .

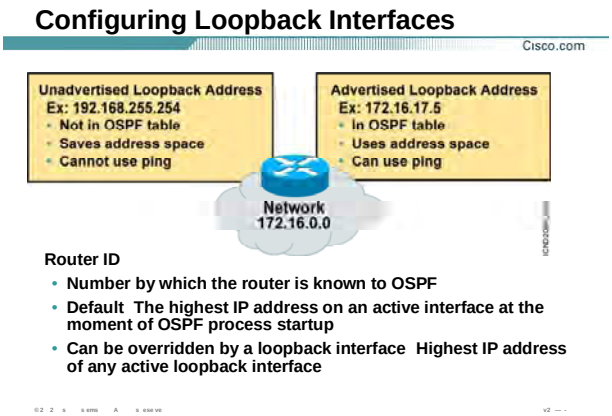
در صورتی که روی یک روتر اینترفیس Loop Back تعریف نکرده باشید RID از میان اینترفیس های فعال انتخاب خواهد شد .تا به اینجا با انتخاب RID روی هر روتر آشنا شدید . بنابراین از این به بعد در شبکه OSPF ، هر روتر با RID شناخته خواهد شد.



تنظیم RID در OSPF (ادامه):

DR/BDR:

در یک شبکه Multi-access مانند Ethernet در صورتی که چندین روتر روی این شبکه موجود باشند همگی باهم رابطه Neighboring دارند .یعنی هر روتر با روترهای دیگر همسایه (Neighbor) می باشد .در صورتی که در یک روتر تغییر رخ دهد و بخواهد این تغییر را گزارش دهد می بایست هر روتر به تمامی روتر هایی که روی شبکه Ethernet واقع شده اند ارسال می کند. بنابراین در این حالت در صورتی که n تا روتر روی شبکه Multi-access موجود باشد به اندازه n(n-1)/2 رابطه بین روترها خواهیم داشت و این نشان از ترافیک بالا در یک شبکه Multi-access خواهد بود . راه حل این مشکل چیست ؟

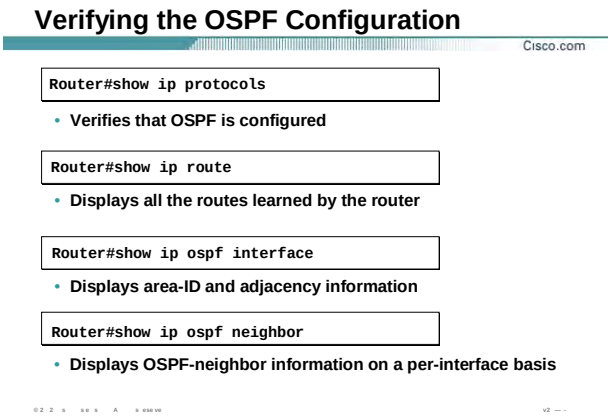


تنظیم RID در OSPF :

درصورتی که یک روتر به عنوان نماینده انتخاب شود ، تمامی روترها می توانند Link-State Database خود را با این روتر یکسان کنند و روتر نماینده در صورتی که تغییری را از روترهای دیگر دریافت کند ، این تغییرات را به روترهای دیگر اطلاع بدهد.

درمیان روترهایی که در یک محیط Multi-access قراردارند روتر نماینده با چه معیاری انتخاب می شود؟

پاسخ به این سوال RID می باشد . در میان روترهایی که در یک محیط Multi-access قرار گرفته اند روتری که بالاترین RID را داشته باشد به عنوان Designated Router و یا همان روتر پاسخگو انتخاب می شود. در صورتی که تغییری در شبکه رخ دهد روتر این تغییرات در قالب LSU (Link-State Update) به روتر DR و BDR اطلاع می دهد . بنابراین هر دو روتر Link-State Database خود را اصلاح می کنند ولی فقط روتر DR این تغییرات را به بقیه روترهای دیگر در محیط Multi-access اعلام می کند و BDR این کار را تا زمانی که DR فعال می باشد انجام نمی دهد و به محض Down شدن روتر DR ، روتر BDR به عنوان DR انتخاب می شود.



بررسی تنظیمات OSPF :

تا به اینجا با راه اندازی پروتکل مسیریابی OSPF روی یک Single Area آشنا شدید .

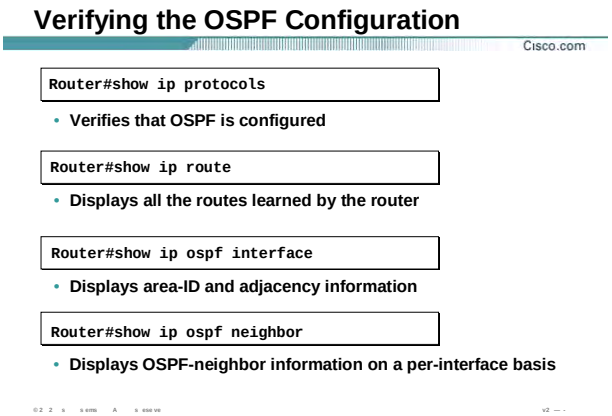
همانطور که تا به اینجا با پروتکل های Link-State ایی خصوصا OSPF آشنا شدید ،می دانید اطلاعات را در چندین Table مختلف نگهداری می کنند . برای مشاهده محتویات این Table ها از فرمان Show کمک می گیریم .

Show IP protocol: به کمک این فرمان پارامترهایی چون زمان ها و فیلترها و متریک های اینترفیس ها و Network ها و اطلاعات دیگری که در مورد یک روتر وجود دارد می توانید مشاهده کنید.

Show IP Route: همانطور که می دانید بعد از اینکه اگوریتم Dijkstra روی روتر اجرا شد ، بهترین مسیرها به مقصدهای مختلف در Routing Table نگهداری خواهد شد.

Show IP OSPF Interface: این فرمان اینترفیس هایی از روتر را که در پروسه OSPF شرکت می کنند را نشان می دهد. در خروجی این فرمان می توانید Timer Interval ها (Hello Interval و Dead Interval) و همچنین Network Type ایی که این اینترفیس در آن واقع شده است را مشاهده کنید.

به کمک این فرمان می توانید مشاهده کنید که این روتر با چه روتری ارتباط Adjacency برقرار کرده و روتر Adjacent دارای چه Router ID ایی می باشد.



بررسی تنظیمات OSPF (ادامه):

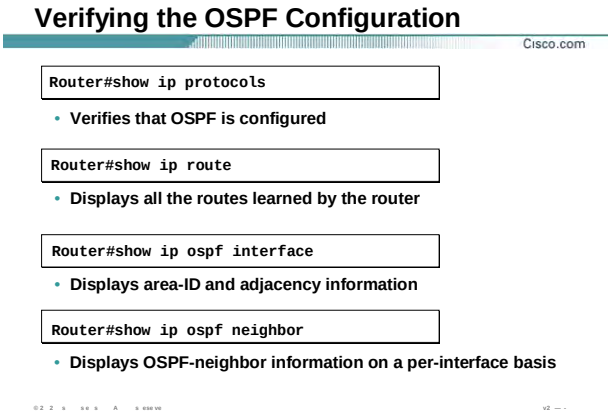
Adjacent With Neighbor 131.108.1.2 (Designated Router)

سوالی که اینجا مطرح می شد اینست که چه تفاوتی بین Neighboring و Adjacency در پروتکل مسیریابی OSPF وجود دارد؟

یک محیط Multi-access مانند شبکه Ethe net رادرنظر بگیرید. چندین روتر در یک Broadcast Domain وجود دارند که دو به دو با یکدیگر مجاور و همسایه هستند.

اما زمانی که که انتخابات DR و BDR صورت بگیرد ، تمامی روترها با DR و BDR یک رابطه دیگری را ایجاد می کنند که به این رابطه Adjacency گفته می شود.

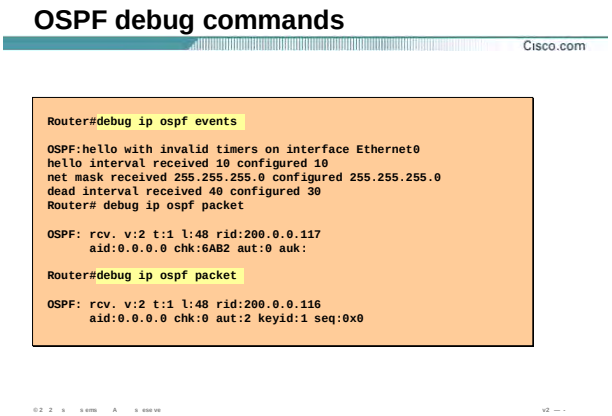
بنابراین درصورتی که یکی از روترهایی که نه DR و نه BDR می باشد تغییری را Link-State Database خود اعمال کند آن را فقط به DR و BDR اعلام می کنند . بنابراین DR و BDR علاوه بر رابطه هم سایگی رابطه دیگری با بقیه روترهای برقرار کرده اند که منجر به یکسان شدن Link-State Database در کل روترهـ ی محیط Multi-access می شود. بنابراین همه روترها تغییراتشان را به جای اینکه به تک تک روترها در این محیط بدهند این تغییرات را به



بررسی تنظیمات OSPF (ادامه):

روترهای DR و BDR اعلام می کند و سپس DR ، Link-State Database خود را update کرده و سپس این DR است که این تغییرات را به روترهای دیگر اعلام می کند .

Show IP OSPF Neighbor: این فرمان اطلاعات روترهای مجاور به یک روتر چون Router ID و state مربوط به این ارتباط را مشخص می کند . اینکه روتر مجاور به این روتر ، DR و یا BDR و یا اینکه هیچ کدام از آنها (DOTHER) باشد را نمایش می دهد.



بررسی عملکرد OSPF به کمک فرمان Debug:

یکی از فرمانهای اشکال زدایی پروسه OSPF ، Debug می باشد . Debug فرمانی است که رخدادهای لحظه ای را بررسی کرده و نمایش می دهد. در این قسمت دو تا از فرمانهای Troubleshooting مربوط به OSPF را بررسی می کنیم.

Debug IP OSPF Events:

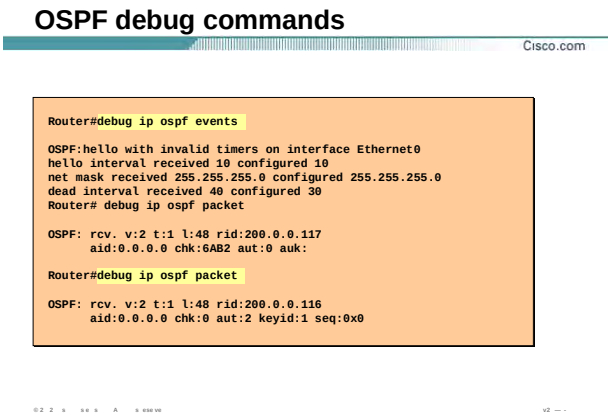
این فرمان زمانی یکسری اطلاعات را نمایش می دهد که یکی از تغییرات زیر رخ دهد:

۱. متفاوت بودن Subnet Mask روترهایی که در یک Broadcast Domain قرار دارند.

۲. متفاوت بودن Hello Interval در دو روتر مجاور.

۳. متفاوت بودن Dead Interval در دو روتر مجاور.

بنابراین درصورتی که دو روتر مجاوری که با پروتکل مسیریابی OSPF کار می کنند با یکدیگر رابطه همسایگی برقرار نکردند موارد زیر را بررسی کنید:



بررسی عملکرد OSPF به کمک فرمان Debug (ادامه):

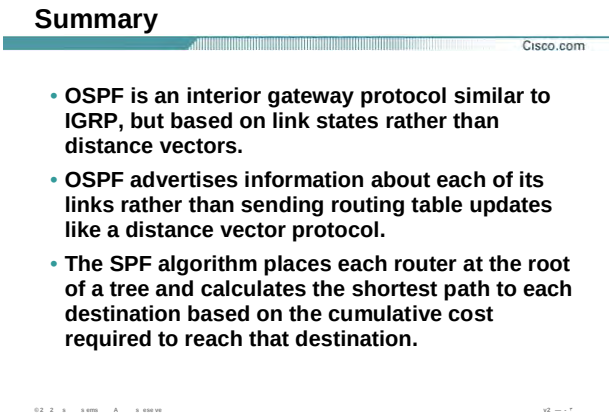
۱. Subnet Mask ، Hello Interval و dead Interval را روی آن دو بررسی کرده و از یکسان بودن آنها در دو روتر مطمئن شویید.

۲. مطمئن شویید که هر دو اینترفیس از دو روتر که قرار است رابطه Neighboring را برقرار کنند در یک Area واقع شده باشند.

:Debug IP OSPF Packet

برای مشاهده اطلاعات پکتهای دریافتی و ارسالی از این فرمان استفاده می کنیم.

به کمک این فرمان می توانید روند SPF الگوریتم و انتخاب DR و BDR و روند برقراری Adjacency را مشاهده کنید.



خلاصه :

OSPF (Open Short Path First) یک پروتکل از دسته پروتکل های IGPs می باشد . بنابراین پروتکلی است که در داخل AS معتبر بوده و مسیریابی را انجام می دهد.

از طرفی OSPF جزء پروتکل های Link-State ایی می باشد. و توپولوژی شبکه را به صورت درختی درآورده که خود رأس و ریشه این درخت می باشد .سپس این توپولوژی بدست آورده را در یک Link-State Database نگهداری می کند.

پس از تکمیل Link-State Database به کمک الگوریتمی تحت عنوان Dijkstra یا همان SPF Algorithms کوتاهترین مسیرها را تعیین و در Routing Table خود نگهداری می کند.

OSPF برخلاف پروتکل های Distance-Vector ، Periodic نمی باشد . این بدان معنی است که روتر کل اطلاعات Routing Table اش را به صورت Periodic Update به روترهای مجاورش ارسال نمی کند ، بلکه فقط تغییراتی که در Link-Sate Database رخ دهد به روترهای دیگر اطلاع داده می شود بنابراین هر کدام از روترها با اصلاح کردن Link-State Database خود الگوریتم SPF را اجرا کرده و Routing Table خود را می سازند.

فصل چهارم :

معرفی و پیکربندی
سوئیچهای سیسکو

این فصل شامل معرفی سوئیچهای سیسکو و نحوه پیکربندی آن و پروتکل های مختلف آن می باشد .

درس اول :

معرفی و آشنایی با
Cisco Switch

هدف :

۴. راه اندازی اولیه یک سوئیچ .

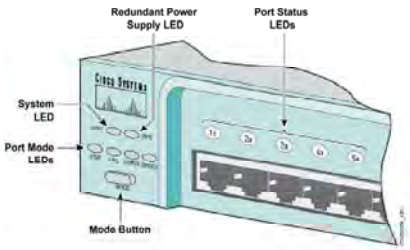
۵. نحوه کارکرد سوئیچ .

۶. Loop و نحوه رخ دادن آن و نحوه عملکرد STP در جلوگیری از LOOP .

۷. معرفی Virtual LAN (VLAN) .

۸. معرفی TRUNK .

Catalyst 2950
Switch LED Indicators



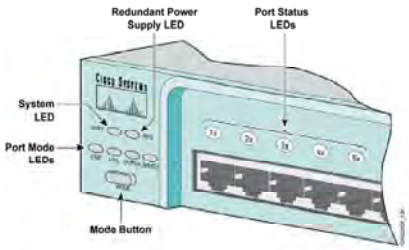
بررسی ظاهری سوئیچ سری 2950 :

سوئیچ سخت افزاری است که وظیفه اصلی آن هدایت فریم ها براساس MAC Address در شبکه می باشد. برخلاف روتر ، سوئیچ می تواند بدون تنظیم کردن در داخل شبکه استفاده شود و عملیات سوئیچینگ را انجام دهد .

در این کتاب از میان سوئیچ های سیسکو و سوئیچهای لایه دوم ، سوئیچ ۲۹۵۰ بررسی می شود . سوئیچهای سری ۲۹۵۰ دارای پورتهای اترنت (۱۰۰ Mbps) و برخی از مدلهای این سری دارای پورتهای اترنت گیگابیت (1000 Mbps) نیز می باشند . همانند روتر ، سیستم عامل سوئیچ تحت عنوان IOS نقش واسط نرم افزاری بین سخت افزارها و کاربر را بازی می کند. نمای ظاهری یک سوئیچ ۲۹۵۰ در شکل بالا نمایش داده شده است .به صورت کلی می توان نمای ظاهری سوئیچ های سری ۲۹۵۰ را به سه دسته تقسیم کرد :

۱. پورتها
۲. LED
۳. Mode Button

Catalyst 2950
Switch LED Indicators



بررسی ظاهری سوئیچ سری 2950 (ادامه) :

پورتها :

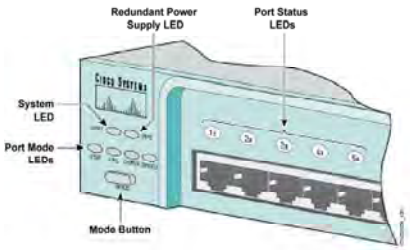
بسته به اینکه سوئیچ ۲۹۵۰ ه مدلی باشد نوع پورتها و تعداد آنها متفاوت می باشد به طور مثال سوئیچ 2550G-12 دارای دو پورت اترنت گیگا بیت مبتنی بر فیبرنوری و ۱۲ پورت اترنت می باشد .

:LED

شامل چهار دسته می شود :

- Port Status LED
- Port Mode LED
- System LED
- Power Supply LED

Catalyst 2950
Switch LED Indicators



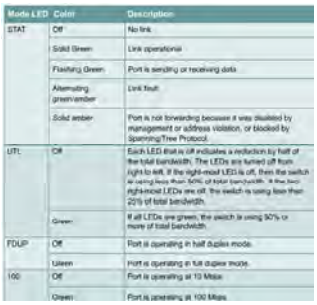
بررسی ظاهری سوئیچ سری 2950 (ادامه) :

Port Status LED : به ازای هر کدام از پورتها سوئیچ ،یک LED وجود دارد که نمایانگر وضعیت و کارکرد پورت می باشد .

پنج رنگ و به ازای آن پنج نتیجه متفاوت درمورد Prot LED حاصل می شود :

۱. Off : به پورت هیچ Link ایی متصل نمی باشد .
۲. سبز : به پورت Link ایی متصل است ولی پورت Active نیست .
۳. سبز چشمک زن : Active بودن Link و هدایت ترافیک را نشان می دهد.
۴. کهربایی و سبز : درصورتی که رنگ LED متناوبا به رنگ کهربایی و سبز درآید ، این بدان معنی است که خطایی در Link چون Collision رخ داده شده است .
۵. کهربایی : در این حالت پورت به صورت دستی Disable شده است .

Switch LED Indicators



Mode LED	Color	Description
STAT	Off	No link
	Solid Green	Link operational
	Flashing Green	Port is sending or receiving data
	Alternating green/amber	Link fault
	Solid amber	Port is not forwarding because it was disabled by management or address violation, or blocked by Spanning Tree Protocol
UTL	Off	Each LED that is off indicates a reduction by half of the total bandwidth. The LEDs are turned off from right to left. If the right-most LED is off, then the switch is using less than 50% of total bandwidth. If the two right-most LEDs are off, the switch is using less than 25% of total bandwidth.
	Green	If all LEDs are green, the switch is using 50% or more of total bandwidth.
FDUP	Off	Port is operating in half duplex mode.
	Green	Port is operating in full duplex mode.
100	Off	Port is operating at 10 Mbps
	Green	Port is operating at 100 Mbps

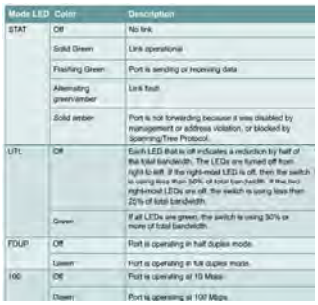
:Port Mode LED

این کلید چهار وضعیت را نشان می دهد :

۱. **STST LED :** به صورت پیش فرض وقتی سوئیچ را روشن می کنید این چراغ روشن می شود . هنگامی که STST LED روشن باشد ، هرکدام از LED هایی که در بالای هر پورتهای قرار گرفته است و رنگهای مختلف آن می تواند در تعیین سالم یا خراب بودن پورت کمک کند.

۲. **UTL LED :** زمانی که کلید Mode را در این وضعیت قرار می دهید LED های بالای هر پورت به منزله نموداری عمل می کنند که میزان bandwidth مورد استفاده را نشان می دهند . در صورتی که تمامی LED ها روشن باشند این بدان معنی است که از پنجاه درصد از Bandwidth استفاده شده است و در صورتی که کلیدهای که به سمت راست نزدیک هستند روشن شوند این بدان معنی است که کمتر از پنجاه درصد از پهنای باند استفاده شده است .

Switch LED Indicators



Mode LED	Color	Description
STAT	Off	No link
	Solid Green	Link operational
	Flashing Green	Port is sending or receiving data
	Alternating green/amber	Link fault
	Solid amber	Port is not forwarding because it was disabled by management or address violation, or blocked by Spanning Tree Protocol.
UTIL	Off	Each LED that is off indicates a reduction by half of the total bandwidth. The LEDs are turned off from right to left. If the right-most LED is off, then the switch is using less than 30% of total bandwidth. If the two right-most LEDs are off, the switch is using less than 20% of total bandwidth.
	Green	If all LEDs are green, the switch is using 30% or more of total bandwidth.
FDUP	Off	Port is operating in half duplex mode.
	Green	Port is operating in full duplex mode.
100	Off	Port is operating at 10 Mbps.
	Green	Port is operating at 100 Mbps.

Port Mode LED (ادامه) :

۳. **FDUP LED :** این Mode کارکرد هر کدام از پورتها را به صورت Halfduplex و Full Duplex نشان می دهد . بنابراین PORT LED ها در دو رنگ نمایش داده می شود :

Off : در این حالت پورت به صورت Half Duplex کار می کند .

سبز : در این حالت پورت به صورت Full Duplex کار می کند .

۴. SPEED LED :

این Mode سرعت مبادله اطلاعات را در مورد هر کدام از پورتها نشان می دهد . بنابراین PORT LED ها در دو رنگ نمایش داده می شود :

Off : در این حالت پورت به صورت Auto تنظیم شده است .

سبز : در این حالت پورت برای کار با سرعت 100 تنظیم شده است .

Port LEDs During Switch POST

1. **At the start, all port LEDs are green.**
2. **Each LED turns off after its test completes.**
3. **If a test fails, its LED turns amber.**
4. **System LED turns amber if any test fails.**
5. **If no test fails, POST completes.**
6. **On POST completion, LEDs blink, then turn off.**

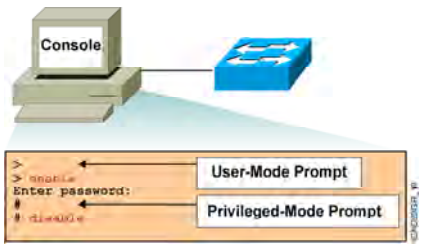
بررسی عملکرد سوئیچ در مرحله POST :

بعد از اینکه کلید Power را در وضعیت ON قرار می دهید ، تمامی PORT LED ها به رنگ سبز در می آید . این مرحله که همان مرحله POST یا به عبارتی چک سخت افزاری می باشد تمامی پورتها مورد بررسی قرار می گیرد درصورتی که دراین مرحله پورتی از نظر سخت افزاری دارای مشکل باشد به رنگ کهربایی درمی آید .و درصورتی که سوئیچ و سخت افزارهای مختلف آن از نظر Safe بودن مورد بررسی قرار گرفته و مشکلی نداشته باشند System LED به رنگ کهربایی در می آید .

درصورتی که مرحله POST به پایان برسد و هیچ اشکال سخت افزاری مشخص نشود، تمامی LED ها یک بار چشمک زده و خاموش می شوند .

بنابراین بعد از طی شدن مرحله POST و Load شدن IOS و تنظیمات ، سوئیچ وارد CLI می شود .

Logging In to the Switch and Entering the Enable Password



CLI و Mode های مختلف:

همان طور که گفته شد CLI یا همان Common Line Interface یک محیط Text Base می باشد و شما می توانید در این قسمت تنظیمات مختلفی را روی روتر و یا سوئیچ انجام دهید.

CLI در IOS سیسکو دارای دو mode اجرایی می باشد :

۱. user mode

۲. privileged mode

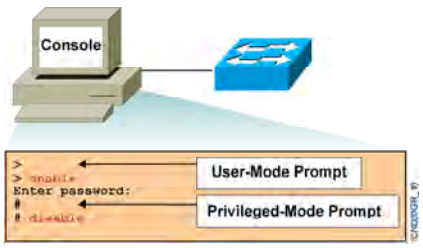
این بدان معنی است که برای انجام تنظیمات برروی سوئیچ می بایست وارد mode مربوط شوید.

User Mode:

در این Mode می توانید عملیات محدودی را انجام دهید . درواقع این Mode پایینترین سطح دسترسی به سوئیچ را نشان می دهد . در این Mode عملیات Monitoring قابل اجرا است.درواقع افراد مختلف می توانند وارد این Mode شده و بدون دسترسی داشتن به تنظیمات ، عملیات محدودی چون چک کردن عملکرد سوئیچ را انجام دهند.

بنابراین این Mode پایین ترین Mode از نظر سطح دسترسی خواهد بود . لذا فرامین کمتری در این Mode قابل اجرا خواهند بود .

Logging In to the Switch and Entering the Enable Password



CLI و Mode های مختلف (ادامه) :

Privileged Mode:

همانطور که از نامش پیداست این Mode ، دارای جایگاه برتری می باشد . به صورت پیش فرض و بدون تنظیم کردن سوئیچ ، هنگام وارد شدن به این Mode پسوردی پرسیده نمی شود ، همانطور که گفته شد این Mode محلی برای انجام و تغییر تنظیمات می باشد بنابراین می بایست از امنیت بالایی برخوردار باشد ، لذا می بایست برای وارد شدن به این mode پسوردی تعریف کرد، تا فقط افراد خاصی با داشتن پسورد بتوانند به این Mode دسترسی پیدا کنند.

Configuring the Switch

Configuration Modes:

- Global configuration mode
  - `wg_sw_a#configure terminal`
  - `wg_sw_a(config)#`
- Interface configuration mode
  - `wg_sw_a(config)#interface e0/1`
  - `wg_sw_a(config-if)#`

پیکربندی سوئیچ 2950 :

برای تنظیم کردن تک تک پورتهای سوئیچ ، فرمان ذیل را به همراه نام پورت مربوطه وارد می کنید .

wg_sw_a(config)#interface e0/1

بعد از وارد کردن فرمان فوق Command Prompt به صورت زیر تغییر می کند :

wg_sw_a(config-if)#

Configuring the Catalyst Switch

پیکربندی سوئیچ 2950 :

برای تنظیم کردن IP Address روی سوئیچ ، وارد Global Mode شده و فرمان زیر را وارد کنید :

Switch(config)# interface VLAN1

بعد از وارد شدن به Mode اینترفیس ، فرمان ذیل را وارد کنید.

Switch(config-if)# ip address 192.168.1.2 255.255.255.0

علاوه بر دادن IP Address ، می بایست Gate Way شبکه LAN را برای سوئیچ مشخص کنید . در ادامه این فصل با کاربرد Gateway بیشتر آشنا می شویید.

برای این منظور آدرس اینترفیسی از روتر که در شبکه LAN قرار دارد را با کمک فرمان ذیل به عنوان Gateway شبکه LAN مشخص می کنید .

Switch(config)#ip default-gateway 192.168.1.1

Switch show interfaces Command

```
wg_sw_a#show interfaces ethernet 0/1

Ethernet 0/1 is Enabled
Hardware is Built-in 10Base-T
Address is 0050.BD73.E2C1
MTU 1500 bytes, BW 10000 Kbits
802.1d STP State:  Forwarding     Forward Transitions:  1
Port monitoring: Disabled
Unknown unicast flooding: Enabled
Unregistered multicast flooding: Enabled
Description:
Duplex setting: Half duplex
Back pressure: Disabled
--More--
```

بررسی وضعیت پورتهای یک سوئیچ :

به کمک فرمان show interface می توان موارد ذیل را روی یک سوئیچ بررسی کرد :

۱. Enable یا Disable بودن یک پورت
۲. آدرس سخت افزاری پورت
۳. STP State
۴. Bandwidth
۵. Half duplex یا Full duplex بودن پورت

Summary

- **The startup of a Catalyst switch requires that you verify the physical installation, power up the switch, and view the Cisco IOS software output on the console.**
- **The Catalyst switches have several status LEDs that are generally lit in green when the switch is functioning normally but turn amber when there is a malfunction.**
- **The Catalyst POST is executed only when the switch is powered up. The POST uses the switch port LEDs to indicate test progress and status.**
- **During initial startup, if POST test failures are detected, they are reported to the console. If POST completes successfully, you can configure the switch.**

خلاصه :

سوئیچ برخلاف روتر می تواند بدون هیچ گونه تنظیمی در شبکه قرار داده شود و هدایت ترافیک را انجام دهد ، اما جهت مدیریت و بهبود کارایی آن در یک شـ که می بایست با آن ارتباط برقرار کرده و آن را تنظیم کرد .

بعد از اینکه کلید Power سوئیچ را در وضع ت ON قرار دهید ، IOS جستجو شده و بعد از Load شدن در حافظه RAM بارگذاری می شود .

در مراحل بوت شدن و در مرحله POST ابتدا تمامی PORT LED ها به رنگ سبز درمی آید. درصورتی که در این مرحله پورتی به رنگ کهربایی درآید معیوب بودن آن مشخص می شود .

بعد از اینکه مرحله POST طی شود و معیوب بودن سخت افزاری در این مرحله مشخص شود ، System LED به رنگ کهربایی درمی آید .در صورتی که مرحله POST بدون مشخص شدن مشکلی به پایان برسد وارد CLI شده و می توان آن را تنظیم و یا تنظیمات آن را تغییر داد .

درس دوم :

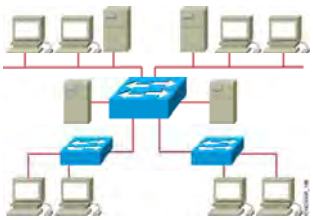
بررسی عملکرد
سوئیچ های لایه ۲

هدف :

۱. بررسی عملکرد سوئیچ های لایه ۲.

۲. یادگیری MAC Address توسط سوئیچ و مقایسه آن با Hub .

Ethernet Switches and Bridges

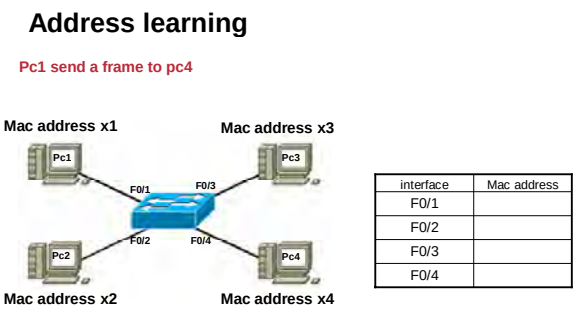


- **Address learning**
- **Forward/filter decision**
- **Loop avoidance**

وظایف سوئیچ های لایه ۲ :

سوئیچ های لایه ۲ و همچنین Bridge ، سخت افزارهایی هستند که به صورت هوشمند در لایه دوم از مدل OSI کار می کنند . این سخت افزارها براساس آدرس سخت افزاری (MAC Address) در شبکه هدایت ترافیک را به عهده دارند . هر سوئیچ به کمک پورتهایی که روی آن قرار دارد به Device دیگر در شبکه چون کامپیوتر ، روتر و غیره متصل شده و هر فریمی را که از پورتهایش دریافت کند می بایست تصمیم گیری کرده و آن را به سوی مقصد هدایت کند . سوالی که پیش می آید اینست که سوئیچ چگونه می تواند از آدرس مقصد شناخت پیدا کند ؟ همانطور که در فصل اول گفته شد ، آدرس دهی در لایه دوم براساس آدرس سخت افزاری یا همان MAC address می باشد . بنابراین در هر فریم آدرس source و آدرس Destination قرار گرفته و سوئیچ با بررسی کردن آدرس مقصد آن را هدایت می کند . سوال دیگری که پیش می آید اینست که سوئیچ چگونه می تواند با شناخت آدرس مقصد در مورد انتخاب اینترفیس تصمیم گیری کند و فریم را بدرستی هدایت کند ؟

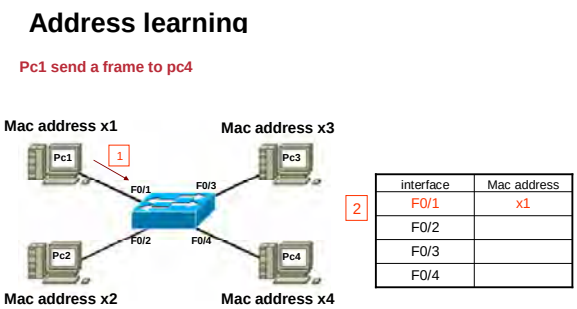
سوئیچ نیاز به یک Database دارد تا بتواند اطلاعات مربوط به آدرسهای مختلف را در آن نگهداری کند تا بتواند براساس آن هدایت فریم را انجام دهد . این database تحت عنوان MAC Table محل قرار گیری MAC Address و Interface های متناظر با هر کدام از آنها می باشد که در ادامه این درس با آن بیشتر آشنا خواهید شد .



یک مثال :

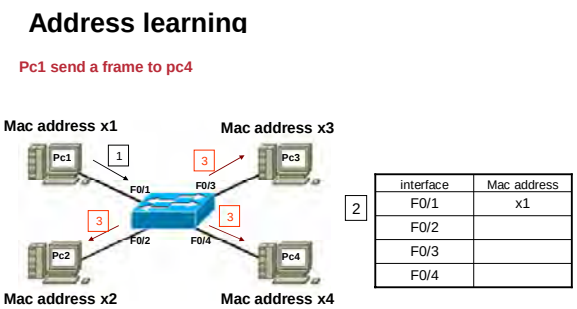
به مثال فوق توجه کنید .

یک سوئیچ و چهار PC که به پورتهای یک سوئیچ متصل شده اند . MAC Table خالی بوده وفاقد هرگونه سطری می باشد . زیرا فرض شده است که سوئیچ هیچ فریمی را دریافت نکرده است .



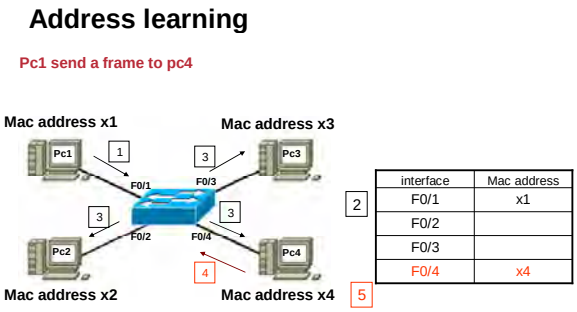
یک مثال :

فرض کنید PC1 قصد ارتباط با PC2 را داشته باشد . بنابراین فریمی را به سوئیچ ارسال می کند . سوئیچ وقتی فریمی را دریافت می کند به آدرس مبداء و مقصد آن نگاه می اندازد . از آنجا که سوئیچ برای بار اول از PC1 فریمی را دریافت کرده است ، بنابراین آدرس PC1 را در MAC Table خود ندارد . لذا MAC Address مربوط به PC1 و شماره پورتی از سوئیچ که به PC1 متصل شده است را در MAC Table خود درج می کند.



یک مثال (ادامه) :

اما PC1 قصد ارتباط با PC4 را دارد و سوئیچ با نگاه کردن به MAC Table خود هیچ آگاهی در مورد PC4 و اینکه از طریق کدام پورت می تواند به آن دسترسی پیدا کند ندارد . بنابراین سوئیچ در این لحظه فریم را به تمامی پورتهایش به جزء پورتی که متصل به PC1 می باشد ارسال می کند . درواقع با Broadcast کردن ،از Device هایی که به پورتهایش متصل هستند می پرسد که آدرس X4 مربوط به کیست ؟



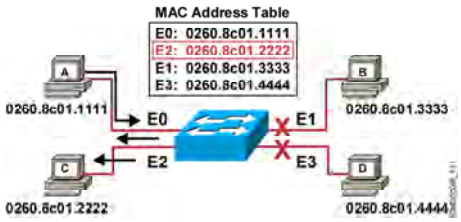
یک مثال (ادامه) :

PC4 که دارای آدرس سخت افزاری X4 می باشد به سوئیچ پاسخ داده و سوئیچ این آدرس و شماره پورتی که متصل به PC4 می باشد را در MAC Table خود قرار می دهد .

بنابراین بعد از گذشتن زمان اندکی این Table تکمیل می شود .

درنتیجه سوئیچ برای تکمیل کردن MAC table خود از مکانیزم Broadcast در شبکه استفاده می کند و بعد از تکمیل آن به صورت Unicast ترافیک را در شبکه منتقل می کند .

Filtering Frames



- **Station A sends a frame to station C.**
- **Destination is known frame is not flooded.**

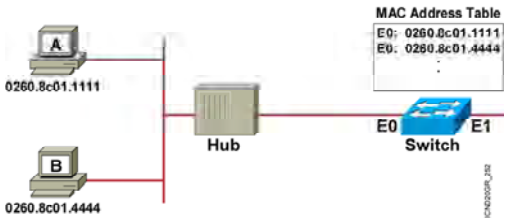
فیلتر شدن فریمها :

یکی دیگر از کارهای مهم دیگری که سوئیچ انجام می دهد Frame Filtering می باشد . این بدان معنی است که وقتی Station ایی فریمی را به سوئیچ ارسال می کند فریم فقط به پورت مشخصی که به Station مقصد متصل است ارسال می شود و به پورتهای دیگر ارسال نمی شود .

سوئیچ زمانی قادر به فیلتر کردن فریمها و ارسال آن به مقصد می باشد که MAC Table خود را تکمیل کرده باشد.

به این مثال توجه کنید . PC A فریمی را به PC C ارسال می کند. سوئیچ فریم را بررسی کرده و آدرس مقصد آن را می خواند و سپس به MAC Table خود نگاهی می اندازد . دسترسی به آدرس **0260.8c01.2222** از طریق پورت E2 امکان پذیر می باشد. بنابراین فریم فقط به سمت پورت E2 هدایت می شود و به پورتهای دیگر ارسال نمی شود . و سوئیچ به کمک MAC Table خود عملیات فیلترینگ فریم ها را انجام میدهد . بنابراین ، این Table می بایست دائما به روز شود تا بتواند هدایت فریم ها را بدرستی انجام دهد .

Filtering Frames (Cont.)

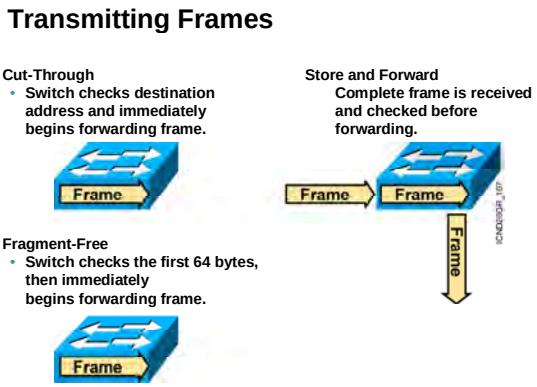


- **Station A sends a frame to station B.**
- **The switch has the address for station B in the MAC address table.**

فیلتر شدن فریمها :

این شکل دو Station را نشان می دهد که از طریق یک Hub به یک پورت سوئیچ متصل شده اند . MAC Table سوئیچ شامل آدرس Station B و Station A می باشد .

بنابراین درصورتی که Station A فریمی را برای Station B بفرستد سوئیچ آن را از تمامی پورتهایش خارج نمی کند بلکه فقط از طریق پورت E0 به سمت Station B ارسال می کند . بنابراین فریم ارسالی از Station A به هیچ پورتی ارسال نخواهد شد.



نحوه انتقال فریم ها توسط سوئیچ :

سوئیچ یکی از سه حا ت زیر را برای انتقال فریم در شبکه LAN استفاده می کند :

۱. Cut-Through

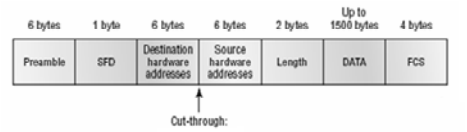
۲. Fragment-Free

۳. Store and Forward

سوئیچ های سری 1900 از روش Fragment-Free و سوئیچ های سری 2950 از روش Store and Forward برای انتقال فریم در شبکه LAN استفاده می کنند .

در ادامه با تک تک این روشها آشنا می شوید.

Cut – through



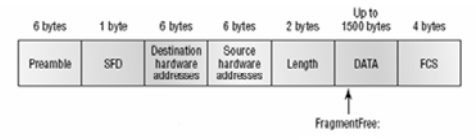
•reads only the destination address
•No error checking

:Cut-Through

در این روش به محض اینکه فیلد Destination از فریمی که توسط سوئیچ در حال دریافت شدن است خوانده شد ، فریم بدون هیچ اتلاف وقتی به سمت Destination ارسال می شود . درواقع در این روش با مشخص شدن Destination سوئیچ به کمک MAC Table پورت خروجی را مشخص کرده و فریم را به سمت مقصد هدایت می کند . در این روش لزومی وجود ندارد کل فریم توسط سوئیچ دریافت شود و سپس عملیات هدایت صورت گیرد . به محض اینکه سوئیچ از بیتهای دریافتی بتواند Destination Address را تشخیص دهد آن را به سمت مقصد هدایت می کند .

بنابراین در این روش تشخیص Error (Error checking) صورت نمی گیرد . لذا سرعت هدایت فریمها در این روش نسبت به دو روش دیگر خیلی بیشتر خواهد بود .

Fragment-Free



•check for the collision on first 64 bytes of frame before forwarding
•provides better error checking than the cut-through

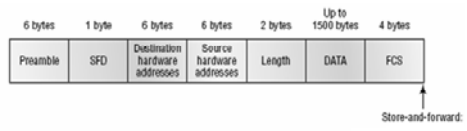
:Fragment-Free

این روش که به آن Cut-Through اصلاح شده نیز می گویند 64 بایت اول از فریم دریافتی خوانده می شود و از نظر نداشتن error چک می شود و سپس سوئیچ فریم را به سمت مقصد هدایت می کند .

سوالی که اینجا مطرح می شود اینست که چرا ۶۴ بایت اول خوانده می شود ؟

درصورتی که بخواهد Collison ایی رخ دهد معمولا در 64 بایت اول رخ می دهد . بنابراین در این روش فریم های Fragment شده شناسایی شده و از ارسال آنها جلوگیری می شود . این روش نسبت به روش Cut-Through تأخیر زمانی بالاتری دارد ولی مطمئن تر عمل می کند .

Store-and-Forward



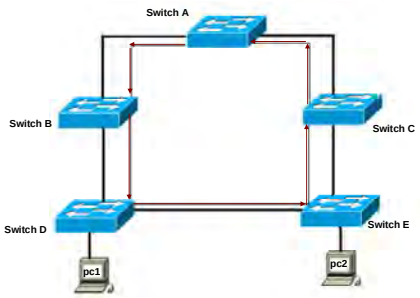
•Use CRC algorithm to error checking
•copies the entire frame in to buffers then error checking

:Store-and-Forward

دراین روش فریم به صورت کامل دریافت شده و سپس به سمت Destination هدایت می شود . ابتدا فریم به صورت کامل Buffer می شود و سپس درصورتی که بیتهای این فریم به صورت کامل دریافت شود و فیلدها Destination و FCS بررسی شود و همچنین درصورتی که الگوریتم CRC خطایی را مشخص نکند ، فریم به سمت مقصد هدایت می شود .

در صورتی که الگوریتم CRC خطایی را مشخص کند فریم Discard می شود . بنابراین این روش نسبت به دو روش دیگر دارای تأخیر زمانی بالاتری می باشد .

Loop in switch



Loop و نحوه رخ دادن و مهار آن :

تا به اینجا با نحوه کارکرد یک سوئیچ در یک شبکه LAN آشنا شدید . فرض کنید در یک شبکه LAN بیش از یک سوئیچ وجود داشته باشید . بنابراین می بایست ارتباط فیزیکی بین این دو برقرار شود . فرض کنید ارتباط فیزیکی به گونه ای باشد که بین هر دو سوئیچ حداقل دو مسیر وجود داشته باشد . این درواقع به معنی وجود Loop در شبکه می باشد . اما باید دید که این ارتباط چه مشکلاتی را به همراه خواهد داشت .

Witch problem can occur when there is loop?

- **Broadcast storm**
- **A device can receive multiple copies of the same frame**

Loop و نحوه رخ دادن و مهار آن :

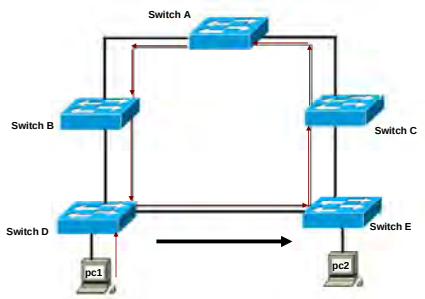
سوالی که مطرح شد اینست که درصورت وقوع Loop در شبکه چه مشکلاتی ممکن است رخ دهد ؟

۱. Broadcast Storm

۲. دریافت همزمان یک فریم از دو مسیر مختلف و افزایش ترافیک در شبکه

موارد فوق پاسخ به سوال مطرح شده می باشد . اما برای رفع مشکلات ذکر شده یک راه حل وجود دارد و آن STP می باشد که در ادامه این فصل مورد بررسی قرار می گیرد .

Broadcast storm

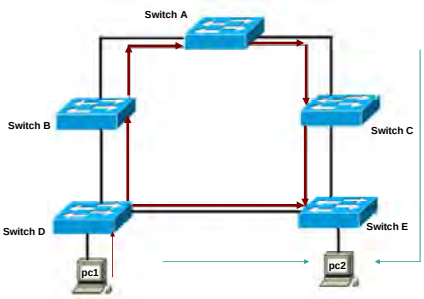


Loop و نحوه رخ دادن و مهار آن :

یکی از مشکلاتی که در صورت وجود Loop در شبکه سوئیچینگ رخ می دهد Broadcast storm یا طوفان Broadcast می باشد .به این شکل توجه کنید . PC1 فریمی را با آدرس مقصد FF.FF.FF.FF.FF.FF که آدرس Broadcast می باشد از تمامی پورتهایش به بیرون ارسال می کند .

یکی از ویژگی های سوئیچ اینست ، درصورتی که فریمی را دریافت کند که آدرس مقصد آن FF.FF.FF.FF.FF.FF باشد آن را فیلتر نکرده و به سمت تمامی پورتهای خروجی ارسال می کند . بنابراین هر کدام از سوئیچ های شکل فوق درصورتی که فریم با آدرس Broadcast را دریافت کنند آن را هدایت می کنند . بنابراین این فریم در هیچ جای این شبکه متوقف نخواهد شد و ترافیکی را به شبکه تحمیل می کند که می تواند مشکل ساز باشد .

Receive multiple copies of the same frame



Pc1 Send a frame **Pc 2 receive two same frame**

Loop و نحوه رخ دادن و مهار آن :

یکی دیگر از مشکلاتی که در صورت وجود Loop در شبکه ممکن است رخ دهد دریافت همزمان دو نسخه یکسان از یک فریم است .

به این شکل توجه کنید PC1 فریمی را به آدرس مقصد PC2 به سوئیچ D تحویل می دهد . سوئیچ D برای MAC Address مربوط به PC2 دو رکورد در MAC table خودش دارد . بنابراین این فریم را از دو جهت مختلف به سمت PC2 ارسال می کند . بنابراین PC2 همزمان دو نسخه یکسان از یک فریم را دریافت می کند . این مشکل منجر به ترافیک اضافی در شبکه می شود و هیچ کاربرد دیگری ندارد .

تا به اینجا با مشکلاتی که در صورت وقوع Loop در شبکه رخ می دهد آشنا شدید . اما سوئیچ به صورت پیش فرض به گونه ای کار می کند که مانع از وقوع Loop در شبکه می شود . درواقع سوئیچ اینکار را با فعال کردن پروتکلی تحت عنوان STP انجام می دهد . درادامه این فصل با این پروتکل و نحوه عملکرد آن در مهار Loop در شبکه بیشتر آشنا خواهید شد.

Summary

- **Ethernet switches and bridges increase the available bandwidth of a network by creating dedicated network segments and interconnecting the segments.**
- **Switches and bridges use one of three operating modes to transmit frames: store and forward, cut-through, and fragment-free.**
- **Switches and bridges maintain a MAC address table to store address-to-port mappings so it can determine the locations of connected devices.**
- **When a frame arrives with a known destination address, it is forwarded only on the specific port connected to the destination station.**

خلاصه :

سوئیچ یک سخت افزار لایه ۲ می باشد . بنابراین هدایت ترافیک در شبکه LAN براساس MAC address صورت می گیرد .

انتقال فریم ها در شبکه براساس یکی از سه متد زیر می باشد :

۱. Cut-Through
۲. Fragment-Free
۳. Store and Forward

روش اول سریعترین روش می باشد زیرا در این روش هیچ گونه error checking صورت نمی گیرد . روش دوم فقط 64 بایت اول از نظر نداشتن error چک می شود و در نهایت در روش آخر کل فریم توسط الگوریتم CRC چک می شود . بنابراین روش آخر نسبت به دو روش دیگر دارای تأخیر زمانی بیشتری می باشد .

درس سوم :

معرفی پروتکل STP
و نقش آن در جلوگیری از Loop

هدف :

۱. STP چیست و چگونه مانع از وقوع Loop در شبکه Switching می شود .

۲. فعال و غیر فعال کردن این پروتکل .

Spanning-Tree Protocol

- **Provides a loop-free redundant network topology by placing certain ports in the blocking state.**

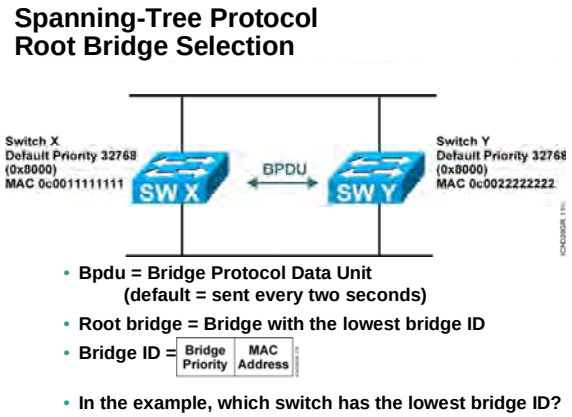
بررسی پروتکل STP :

Spanning-tree Protocol یا همان STP پروتکلی است که ابتدا توسط شرکت DEC و سپس توسط IEEE تحت عنوان 802.1Dاستاندارد شد.

تمام سوئیچ های سیسکو با ورژن 802.1D کار می کنند.

وظیفه اصلی STP جلوگیری از رخ دادن Loop و متوقف کردن Loop رخ داده شده در لایه ۲ می باشد . در واقع این کار را با shutdown کردن link های اضافه انجام می دهد.

STP با به کار بردن Spanning-tree Algorithm یا همان STA،توپولوژی شبکه را به صورت درخت درآورده و سپس با غیرفعال کردن مسیرهای اضافی که منجر به رخ دادن Loop در شبکه شده اند ،Loop رخ داده شده را مهار می کند .



بررسی پروتکل STP (ادامه) :

برای آشنایی با عملکرد STA ابتدا با مفاهیم اولیه آن آشنا شوید:

Bridge ID(BID): ملاک شناسایی یک سوئیچ در STP می باشد.

در واقع مشخصه ایی است که یک سوئیچ به کمک آن در میان سوئیچ های دیگر شناخته و تمییز داده می شود.

دو فاکتور در ساختن این مشخصه نقش دارد :

۱. Priority

۲. MAC Address

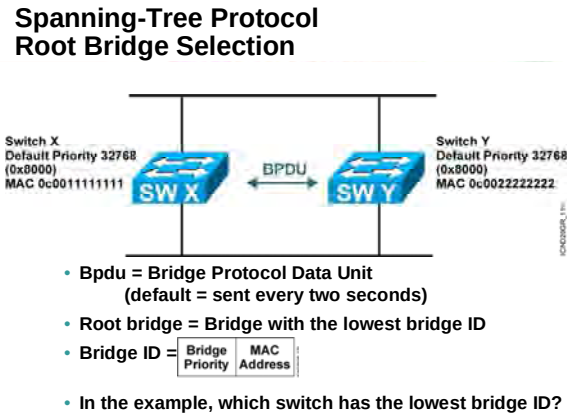
(Priority عددی است که روی سوئیچ های سیسکو به صورت default ، ۳۲۷۶۸ می باشد و قابل تغییر نیز است.)

ترکیب این دو فاکتور به صورت زیر می باشد:

BID = Bridge ID = Bridge Priority + MAC Address

Root Bridge: بعد از اینکه BID به صورت محلی در هر سوئیچ محاسبه شد ،BID ها با هم مقایسه شده و سوئیچی که دارای پایین ترین BID باشد به عنوان Root Bridge انتخاب می شود.

اما این مقایسه براساس چه معیاری صورت می گیرد؟



بررسی پروتکل STP (ادامه) :

اولین معیار برای مقایسه ، priority می باشد . سوئیچی که پایین ترین priority را داشته باشد به عنوان Root Bridge انتخاب می شود.

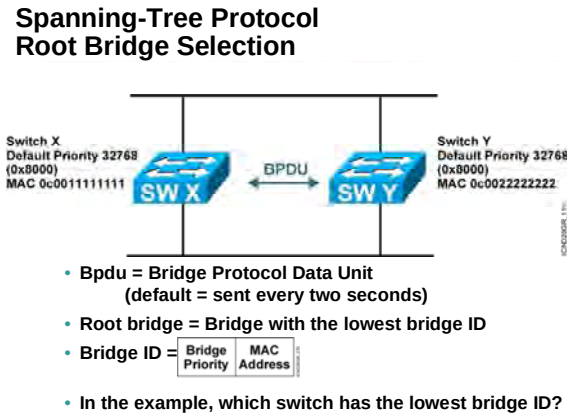
اگر priority در همه سوئیچ ها یکسان بود ، معیار بعدی که همان Mac address می باشد در این انتخاب نقش دارد .

در این حالت سوئچی که دارای پایین ترین Mac address باشد به عنوان Root Bridge انتخاب می گردد.

به نظر شما در مثال بالا کدام سوئیچ به عنوان Root Bridge انتخاب می شود ؟

همانطور که مشاهده می کنید ، هر دو سوئیچ دارای priority یکسان هستند، بنابراین معیار دوم در انتخاب تعیین کننده است .Mac address در سوئیچ SW Y پایین تر از سوئیچ SW X می باشد. بنابراین SW Y به عنوان Root Bridge انتخاب می شود.

توجه داشته باشید که در هر شبکه فقط یک Root Bridge می تواند وجود داشته باشد . در واقع اگر به مثال درخت توجه کنیم یک درخت فقط می تواند یک ریشه داشته باشد نه چند ریشه.



بررسی پروتکل STP (ادامه) :

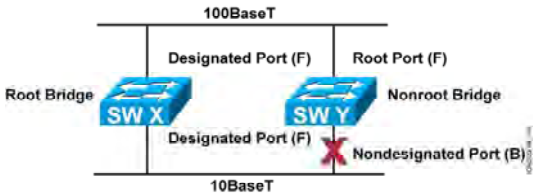
BPDU: Bridge Protocol Data Unit یا همان BPDU فریمی است که سوئیچ ها به کمک آن با هم تبادل اطلاعات می کنند و به کمک این فریم با یکدیگر صحبت می کنند و خود را به دیگران معرفی کنند تا در نهایت بتوانند در شبکه root bridge را انتخاب کنند. همچنین هر گونه تغییری که بابت تغییر توپولوژی رخ داده شود به کمک BPDU به دیگر سوئیچ ها اطلاع داده می شود.

Root Port: پورتی از سوئیچ که دارای کمترین Cost تا Root bridge باشد.

Designated Port: پورتی از سوئیچ که به عنوان پورت forwarding انتخاب می شود.در این حالت پورت قابلیت ارسال و دریافت اطلاعات را خواهد داشت .

Spanning-Tree Operation

- **One root bridge per network**
- **One root port per nonroot bridge**
- **One designated port per segment**
- **Nondesignated ports are unused**



بررسی پروتکل STP در یک مثال (ادامه) :

تا به اینجا با اصطلاحات فنی در الگوریتم STA آشنا شدید . در این مرحله با عملکرد این الگوریتم بیشتر آشنا خواهید شد.

مهمترین وظیفه الگوریتم STA شکستن loop در شبکه و تبدیل شبکه به یک ساختار درختی می باشد.

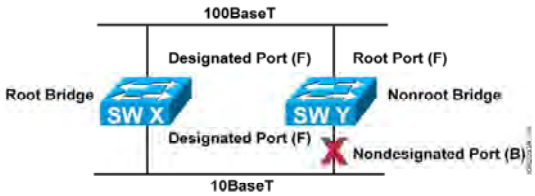
الگوریتم STA با انتخاب یک سوئیچ به عنوان سوئیچ سخنگو و گره اصلی درخت ، بقیه سوئیچ ها را از بالا به پایین نسبت به این گره چیدمان می کند . در الگوریتم STA ،ابتدا هر کدام از سوئیچ ها Bridge ID خود را به صورت محلی محاسبه می کنند. سپس هر کدام از آنها با فرستادن BPDU به سوئیچ های مجاور، خود را معرفی و تبلیغ می کنند.

در این معرفی سوئیچ Bridge ID خود را به سوئیچ مجاور می گوید و سوئیچ مجاور آن را با Bridge ID خود مقایسه می کند . در صورتی که Bridge ID سوئیچ مجاور از Bridge ID خودش کمتر باشد آن را در نظر نگرفته و Bridge ID خود را به دیگران تبلیغ می کند ، در غیر این صورت می گوید که من سوئیچی با Bridge ID کمتر پیدا کردم و می بایست وی را به سوئیچ های مجاورش در غالب BPDU اعلام می کند.

به همین ترتیب هر سوئیچ با مقایسه Bridge ID خود با Bridge ID ایی که به او تبلیغ شده ، می تواند سوئیچی که کمترین Bridge ID را دارد شناسایی کند.

Spanning-Tree Operation

- **One root bridge per network**
- **One root port per nonroot bridge**
- **One designated port per segment**
- **Nondesignated ports are unused**



بررسی پروتکل STP در یک مثال (ادامه) :

بنابراین سوئیچ با کمترین Bridge ID به عنوان Root Bridge انتخاب میگردد.

بعد از انتخاب Root Bridge ، نوبت به تعیین وضعیت پورتها در تک تک سوئیچ های شبکه میرسد.

ابتدا از سویئچ Root Bridge که در ریشه درخت می باشد شروع و سپس تعیین وضعیت پورتهای هر سوئیچ را از بالا به پایین این درخت بررسی می کنیم.

برای درک عملکرد الگوریتم STA ، دو scenario مختلف را مورد بررسی قرار می دهیم .

به scenario اول توجه کنید . در این scenario دو سوئیچ وجود دارد که ارتباط آنها از طریق دو link برقرار شده است . همانطور که تا به اینجا آموختید وقوع loop در این ارتباط بدیهی می باشد.حال ببینم که STA چگونه مانع از وقوع Loop می شود.

STA در پنج مرحله عمل می کند:

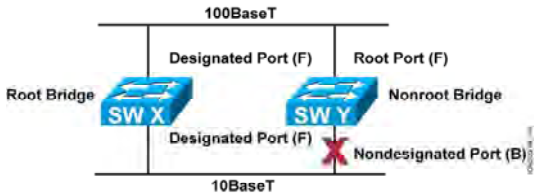
مرحله اول:

هرکدام از سوئیچ ها به صورت محلی Bridge ID خود را محاسبه می کنند.

مرحله دوم:

Spanning-Tree Operation

- One root bridge per network
- One root port per nonroot bridge
- One designated port per segment
- Nondesignated ports are unused



بررسی پروتکل STP در یک مثال (ادامه) :

بعد از اینکه هر کدام از آنها Bridge ID خود را محاسبه کردند، آن را به کمک BPDU به دیگری تبلیغ کنند تا پایین ترین Bridge ID به عنوان Root Bridge انتخاب گردد. بنابر این سوئیچ SW X به عنوان Root bridge انتخاب می گردد.

مرحله سوم:

بعد از انتخاب Root Bridge نوبت به تعیین پورت برگزیده یا همان Designated Port می رسد.

تمامی پورتهای متصل به Root Bridge به عنوان پورت Designated Port انتخاب می شوند و در این حالت،سوئیچ قادر به ارسال و دریافت اطلاعات از طریق این پورت می باشد.

مرحله چهارم:

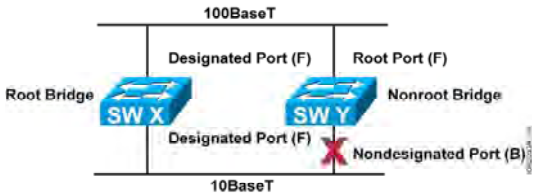
در این مرحله نوبت به انتخاب Root Port می رسد.

در سوئیچ های غیر Root bridge ایی ، Root Port پورتی می باشد که دارای کمترین Cost تا Root Bridge باشد.

به شکل نگاه کنید . در این شکل بین سوئیچ SW X و سوئیچ SW Y دو لینک ارتباطی وجود دارد ، یکی با پهنای باند ۱۰۰ مگابیت در ثانیه و دیگری ۱۰ مگابیت در ثانیه .

Spanning-Tree Operation

- One root bridge per network
- One root port per nonroot bridge
- One designated port per segment
- Nondesignated ports are unused



بررسی پروتکل STP در یک مثال (ادامه) :

فکر می کنید چه ارتباطی بین Cost و Bandwidth وجود دارد؟

Cost نسبت عکس با bandwidth دارد. این بیان گر اینست که با افزایش پهنای باند ،cost کم می شود.

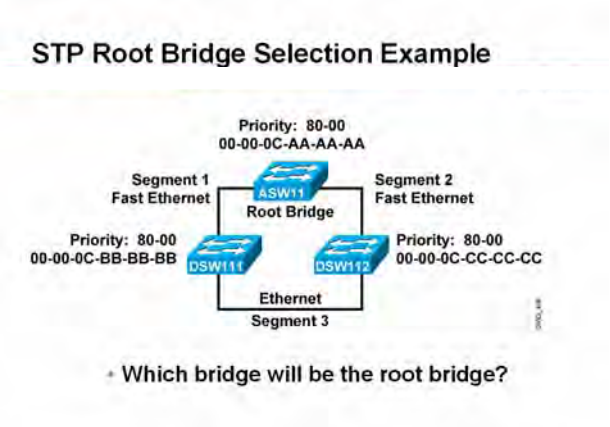
Link با پهنای باند ۱۰۰مگا بیت در ثانیه دارای cost کمتری می باشد ، بنابراین پورت متصل به SW Y که link ارتباطیش دارای کمترین Cost می باشد به عنوان Root Port انتخاب می گردد.

مرحله پنجم:

در آخرین مرحله پورتی که دارای Cost بیشتری در مقایسه با Root Port باشد block شده تا مانع از وقوع loop شود.

نکته: توجه داشته باشید که در هر network ما فقط یک Root Bridge می توانیم داشته باشیم .

زمانی که یک ارتباط چند تایی بین دو سوئیچ وجود دارد برای جلوگیری از loop فقط یک link می تواند فعال باشد بنابراین به همان نسبت در مورد وضعیت دو سر این link ، یکی به عنوان Designated Port و دیگری به عنوان Root Port انتخاب می شود.



بررسی پروتکل STP در یک مثال (ادامه):

تا به اینجا با عملکرد الگویتم STA تا حدودی آشنا شدید . به کمک Scenario دوم درک بیشتری از آن پیدا خواهید کرد.

در این scenario ، ۳ تا سوئیچ موجود است که دو به دو به یکدیگر متصلند. همانطور که می دانید وقوع loop بین این سه غیر قابل انکار می باشد.

حال ببینم الگوریتم STA چگونه link های اضافه را تشخیص داده و ساختار این شبکه را به صورت درختی در می آورد.

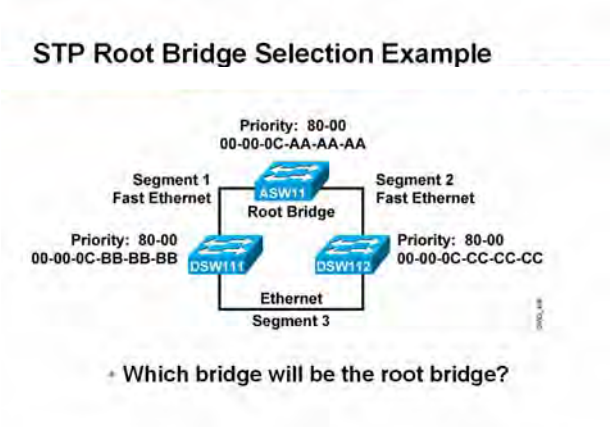
الگورتیم STA در پنج مرحله عمل می کند.

مرحله اول :

همانطور که تا به اینجا آموختید هر کدام از سوئیچ ها به صورت local شناسه خودشان را که همان Bridge ID می باشد ، تعیین می کنند ، توجه داشته باشید که این مشخصه منحصر به فرد می باشد.در واقع دو سوئیچ را نمی توانید پیدا کنید که Bridge ID یکسانی داشته باشند.

مرحله دوم:

نوبت به تبلیغ به دیگران می رسد . در این مرحله هر سوئیچ خود را به کمک BPDU به دیگران تبلیغ می کند تا پایین ترین Bridge ID به عنوان Root Bridge انتخاب گردد.

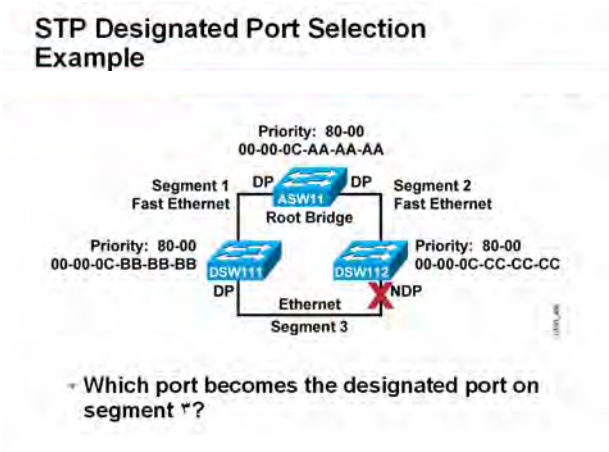


بررسی پروتکل STP در یک مثال (ادامه):

حال یک سوال مطرح می شود ، با توجه به این scenario کدام سوئیچ به عنوان Root Bridge انتخاب می گردد؟

پاسخ :سوئیچ ASW11 به عنوان Root Bridge انتخاب می گردد .

هر سه سوئیچ دارای Priority یکسانی هستند بنا راین زمانی که معیار اول یکسان باشد معیار دوم در انتخاب تعیین کننده است. سوئیچ ASW11 کمترین Mac Add ess را در بین این سه سوئیچ دارا می باشد ، بنابراین به عنوان Root Bridge انتخاب می شود.



بررسی پروتکل STP در یک مثال (ادامه):

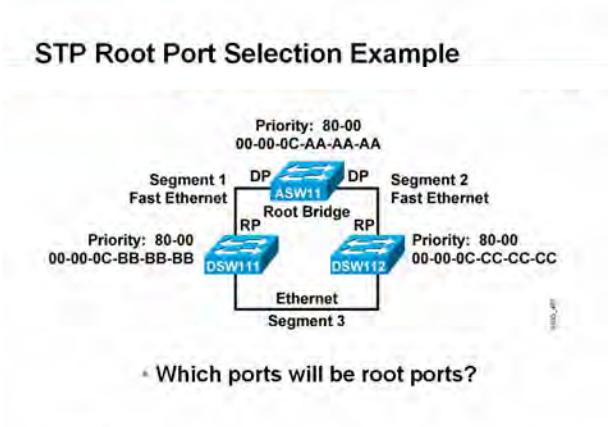
مرحه سوم:

بعد از انتخاب Root Bridge نوبت به تعیین Designated Port می رسد.

همانطور که گفتم تمامی پورتهای متصل به Root Bridge به عنوان DP انتخاب می شوند.

از طرفی در link بین دو سوئیچ غیر Root Bridge ایی ، فقط یک پورت به عنوان DP انتخاب و دیگری به عنوان Root Port یا Blocking port انتخاب می شود.

بعد از اینکه Root Bridge انتخاب شد الگویتم STA شروع به پیمایش درخت از بالا به پایین می کند و پورتهای متصل به Root Bridge را به عنوان DP انتخاب می کند.



بررسی پروتکل STP در یک مثال (ادامه):

مرحله چهارم:

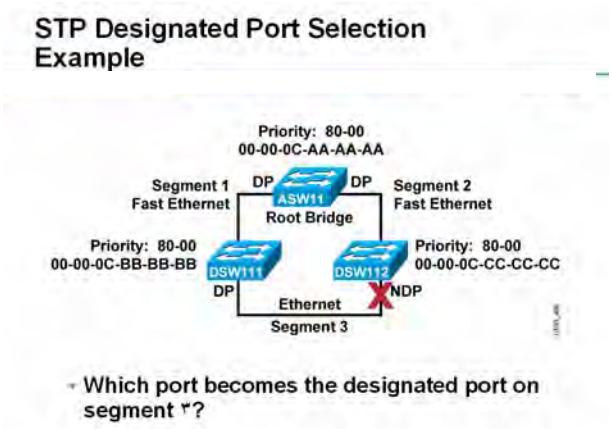
از آنجایی که در هر link فقط یک پورت می تواند DP باشد و دیگری می تواند Root Port یا پورت Block شده باشد ، بنابراین در این Scenario در لینکهای متصل به Root Bridge ، پورت متصل به Root Bridge به عنوان DP انتخاب می شود و طرف دیگر link به عنوان RP انتخاب می گردد.

مرحله پنجم:

تا به اینجا وضعیت پورت ها در Segment1 و Segment2 مشخص شدند.

به segment 3 نگاه کنید . در سوئیچ های DSW11 و DSW12 چون DP انتخاب نشده و از طرفی در هر سوئیچ فقط یک پورت می تواند DP باشد بنابراین پورتهایی که در Segment3 هستند کاندید برای انتخاب DP می باشند.

حال به نظر شما الگوریتم STA کدام پورت را به عنوان DP انتخاب می کند؟



بررسی پروتکل STP در یک مثال (ادامه):

برای انتخاب DP در segment 3 ، تصمیم گیری بر اساس دو معیار صورت می گیرد:

۱. cost

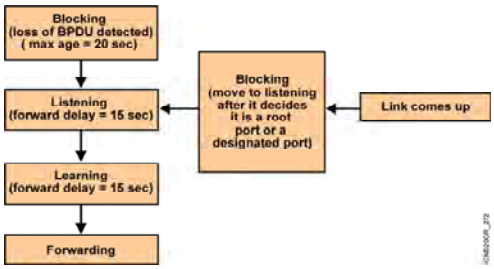
۲. Bridge ID

اولین معیار مقایسه بین دو پورت Cost می باشد. در این حالت پورتی که دارای bandwidth بیشتری باشد ، cost کمتری داشته و به عنوان DP انتخاب می گردد و پورت با cost بیشتر به عنوان پورت Block شده انتخاب می گردد.

اما در صورتی که هر دو پورت دارای cost یکسانی باشند ، پورت مربوط به سوئیچی که دارای Bridge ID کمتری باشد به عنوان DP انتخاب می گردد .

Spanning-Tree Port States

- **Spanning-tree transits each port through several different states:**



وضعیت پورتها در پروتکل STP :

هر پورت در سوئیچی که الگوریتم STA روی آن فعال است می تواند در یکی از پنج state زیر قرار داشته باشد .

پنج state ایی که برای هر پورت در الگویتم STA در نظر گرفته شده است به قرار زیر می باشد:

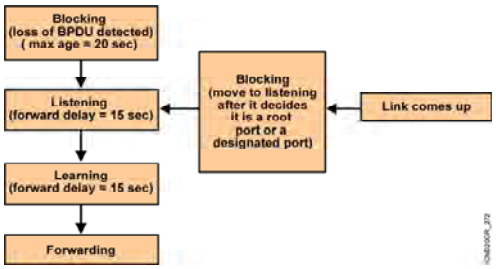
۱. disable
۲. blocking
۳. listening
۴. learning
۵. forwarding

Blocking:

وقتی سوئیچی را روشن می کنید تمامی پورتها در حالت blocking قرار دارند و هیچ فریمی را ارسال و یا دریافت نمی کنند . در این حالت پورت فقط به BPDU ها گوش می دهد تا بتواند در مورد وضعیت بعدی خود تصمیم گیری کند.

Spanning-Tree Port States

- **Spanning-tree transits each port through several different states:**



وضعیت پورتها در پروتکل STP (ادامه) :

Listening:

در این State هر سوئیچ با توجه به BPDU هایی که می شنود Root Bridge را انتخاب کند . بنابراین اگر به این پورت فریمی وارد شود که حاوی Mac address جدیدی باشد ، در Mac table قرار نمی گیرد.

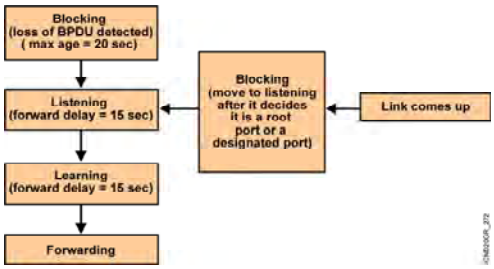
Learning:

بعد از سپری شدن مدت زمان listening ، پورت تغییر state داده و وارد learning state می شود. در این حالت سوئیچ تمامی مسیرهای موجود در شبکه و مسیرهایی که فاقد loop هستند را شناسایی می کند.

در این حالت اگر به این پورت از سوئیچ فریمی وارد شود که حاوی Mac address جدیدی در شبکه باشد ، آن را در Mac Address table قرار می دهد، اما هدایت فریم در این State صورت نمی گیرد .این وضعیت برای پورت دائمی و پایدار نبوده و می بایست به State بعدی برود.

Spanning-Tree Port States

- **Spanning-tree transits each port through several different states:**



وضعیت پورتها در پروتکل STP (ادامه) :

Forwarding:

بعد از اینکه root Port وDesignated Port بودن یک پورت در مرحله learning مشخص شد ، در مرحله Forwarding پورت قادر به ارسال و دریافت فریم می باشد .

Blocking:

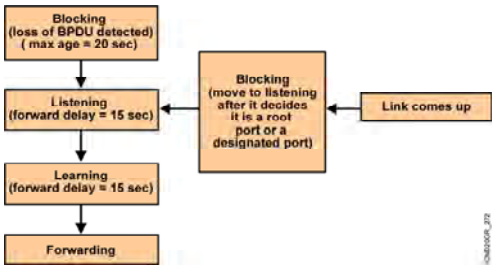
در صورتی که در مرحله learning ، مشخص شد که یک پورت برای جلوگیری از loop باید block شود .در این مرحله پورت در blocking state قرار می گیرد . این پورت فریمی را ارسال یا دریافت نمی کند بلکه فقط به BPDU ها گوش می دهد تا در صورت رخ دادن تغییری در شبکه مثل down شدن یک سوئیچ و یا تغییر cost بتواند از تغییرات حاصله آگاهی پیدا کند و در صورت لزوم خود تغییر state بدهد.

Disable:

در این حالت پورت نه فریمی را دریافت و نه ارسال می کند. پورت به صورت دستی غیر فعال شده بنابراین با تغییر در شبکه پورت تغییر State نمی دهد .

Spanning-Tree Port States

- **Spanning-tree transits each port through several different states:**



وضعیت پورتها در پروتکل STP (ادامه) :

در پایان الگوریتم STA و زمانی که شبکه به صورت کامل همگرا شده باشد، تمامی پورتها در یکی از دو state زیر قرار می گیرند:

۱. forwarding state

۲. Blocking State

توجه داشته باشید که هرگونه تغییردر شبکه که منجر به تغییر توپولوژی شود الگوریتم STA دوباره اجرا شده و پورتها از حالت forwarding و blocking خارج می شوند.

Summary

- **STP is a bridge-to-bridge protocol used to maintain a loop-free network.**
- **STP establishes a root bridge, a root port, and designated ports.**
- **With STP, the root bridge has the lowest bridge ID, which is made up of the bridge's priority and MAC address.**
- **With STP, ports transition through four states: blocking, listening, learning, and forwarding.**
- **If a change occurs to the network topology, STP maintains connectivity by transitioning some blocked ports to the forwarding state.**
- **RSTP significantly speeds the recalculation of the spanning tree when the network topology changes.**

خلاصه :

یکی از مشکلات شبکه از دیدگاه لایه دوم یا همان Data Link مشکل وقوع loop می باشد. STP پروتکلیست که با به کار بردن الگویتم STA توپولوژی شبکه را به صورت درختی و بدون loop در می آورد.

در این حالت یک سوئیچ نقش گره اصلی درخت را بازی می کند وبقیه سوئیچ ها با توجه به گره از بالا به پایین چیدمان می شوند.

الگورتم STA در مورد وضعیت پورتها و اینکه کدام پورت ارسال و دریافت فریم را به عهده داشته باشد و یا کدام پورت غیر فعال باشد تصمیم گیری می کند.

بعد ازاینکه کار الگوریتم STA به پایان رسد تمامی پورتها در دو State پایدار قرار می گیرند ، Forwarding یا Blocking.

در صورتی که تغییری در شبکه رخ دهد و توپولوژی شبکه تغییر کند الگوریتم STA دوباره روی تمامی سوئیچ ها اجرا می شود .

درس چهارم :

Virtual Link
و نقش آن در مدیریت ترافیک

هدف :

۱. Virual Link و نقش آن در مدیریت ترافیک .

۲. معرفی VLAN و ویژگی های آن .

۳. نحوه تنظیم VLAN روی یک سوئیچ.

۴. اشکال زدایی .

VLANs

مفهوم VLAN :

تا به اینجا با عملکرد سوئیچ در یک شبکه آشنا شدید . تمامی پورتهای یک سوئیچ در یک محیط Broadcast Domain قرار دارد .این بدان معنی است که تمامی Device هایی که به این سوئیچ متصل هستند همگی در یک LAN قرار دارند ، بنابراین می توانند براحتی به یکدیگر دسترسی داشته باشند .

قرارگیری تمامی منابع شبکه مانند Server ها ، کاربران ، اینترنت در یک LAN واحد مشکلاتی را بدنبال دارد . نتیجه آن

۱. ترافیک بالا
۲. امنیت پایین

به عبارتی در چنین شبکه ای نمی توان مدیریت روی ترافیک و امنیت داشت . درحالی که اگر یک Broadcast Domain را به چندین Broadcast Domain تفکیک کنیم ، ترافیک کاهش و محلی شده و دسترسی ها محدود می شود .

درواقع با تبدیل کردن یک LAN به چندین LAN یا همان VLAN نتایج زیر حاصل می شود:

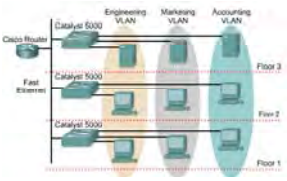
۱. کوچک شدن Broadcast Domain
۲. کاهش و محلی شدن ترافیک
۳. محدود کردن سطح دسترسی

VLANs

مفهوم VLAN (ادامه) :

فرض کنید تعدادی کامپیوتر در یک LAN قرارداشته باشند . بنابراین همه این کامپیوترها براحتی با یکدیگر ارتباط دارند . اما درصورتی که یک LAN را به چندین VLAN تبدیل کنید ، کامپیوترهایی که در یک VLAN قرار دارند نمی توانند با VLAN های دیگر ارتباط برقرار کنند .

VLANs



VLANs logically segment switched networks based on an organization's functions, project teams, or applications as opposed to a physical or geographical basis.

بررسی VLAN در یک مثال نمونه :

به شکل فوق توجه کنید . این شکل نشان دهنده یک ساختمان و سه طبقه مختلف می باشد . در طبقات اول و دوم تعدادی کامپیوتر و در طبقه سوم تعدادی Server قراردارد .

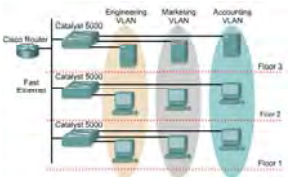
در هر طبقه یک سوئیچ قراردارد . هر سه سوئیچ به صورت پشته به یکدیگر مرتبط شده اند و درواقع به مانند یک سوئیچ واحد عمل خواهند کرد . درنتیجه تمامی کامپیوترها و Server ها از دیدگاه لایه دوم در یک Broadcast Domain و از دید لایه سوم دارای Network ID یکسانی هستند . بنابراین علاوه بر اینکه ترافیک در این شبکه بالا می باشد کنترل دسترسی در این شبکه از دید لایه سوم امکان پذیر نخواهد بود .

فرض کنید بخواهید به هر کدام از Server ها Node های خاصی دسترسی داشته باشند و امکان جابجایی فیزیکی هر کدام از آنها وجود ندارد . پس راه حل چیست ؟

چگونه می توان دسترسی را بدون تغییر در ساختار فیزیکی و محل قرارگیری کامپیوتر ها انجام داد ؟

Virtual LAN یا همان LAN مجازی راه حل این مشکل خواهد بود . با شکستن یک شبکه LAN به چند شبکه LAN کوچکتر ، هم کنترل ترافیک و هم محدود کردن سطح دسترسی در لایه دوم امکان پذیر خواهد شد .

VLANs



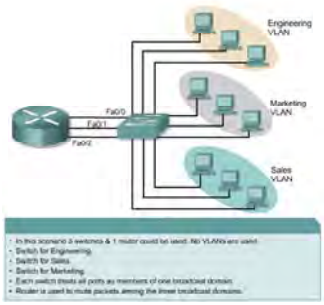
VLANs logically segment switched networks based on an organization's functions, project teams, or applications as opposed to a physical or geographical basis.

بررسی VLAN در یک مثال نمونه (ادامه) :

تعریف و ساخت VLAN در لایه دوم از مدل OSI امکان پذیر می باشد . با توجه به شکل فوق سه VLAN با نام های Engineering VLAN ، Marketing VLAN ، Accounting VLAN روی هر سه سوئیچ تعریف می کنیم . سپس پورتها را در VLAN های مربوطه قرار می دهیم تا کامپیوترهای متصل به هر کدام از پورتها در VLAN مربوطه قرار گیرند .

همانطور که مشاهده می کنید این دسته بندی به صورت منطقی بوده و فیزیکی صورت نمی گیرد .سه رنگ متفاوت در این شکل مشخص کننده محدوده تعریف هر کدام از VLAN های ساخته شده می باشد و عناصر موجود در هر VLAN با یکدیگر ارتباط نخواهند داشت . بنابراین به کمک VLAN توانستیم محدود کردن دسترسی و محلی کردن ترافیک را در لایه دوم و به کمک سوئیچ انجام دهیم .

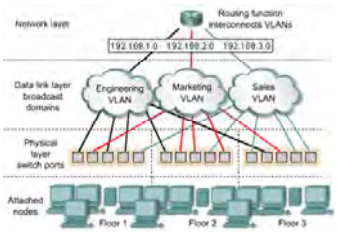
Broadcast Domains with VLANs and Routers



نقش VLAN و Router در شکستن یک Broadcast Domain :

تمامی پورتهای یک سوئیچ به صورت Default در یک Broadcast Domain قرار دارند . با تعریف کردن VLAN ، Broadcast Domain به نواحی منطقی کوچکتری تقسیم می شود . لذا هر کدام از VLAN ها یک Broadcast Domain جدید خواهند بود . Node های موجود در هر کدام از VLAN ها براحتی با یکدیگر تبادل اطلاعات خواهند داشت. مشکل زمانی پیش می آید که شما بخواهید دسترسی به یک VLAN را برای بعضی از VLAN ها برقرار کنید . درواقع می خواهید ارتباط بین یک یا چند VLAN را برقرار کنید. برای این منظور کافی است که از یک Router که یک Device لایه سوم می باشد استفاده کنید به طوری که ترافیک را از یک VLAN به سمت VLAN دیگر هدایت کند .

VLAN and OSI



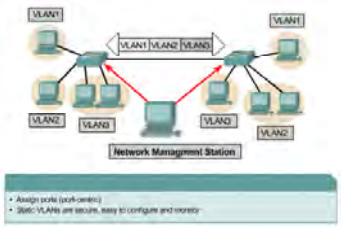
مکانیزم کاری یک VLAN در مقایسه با مدل OSI :

به شکل فوق توجه کنید . این شکل نمایشگر سه لایه انتهایی مدل OSI می باشد . در لایه فیزیکی پورتهای سوئیچ نمایش داده شده اند . هر کدام از این پورتها به node های مربوطه در هر Floor متصل شده اند . لایه دوم از مدل OSI محل تعریف و ساخت VLAN ها می باشد . سه VLAN ساخته شده متناسب به نیاز دارای تعدادی پورت از هر سه سوئیچ می باشد . سه رنگ مشکی ، آبی و قرمز به ترتیب پورتهایی را نشان می دهد که در این سه VLAN قرار گرفته اند .

از طرفی به منظور ارتباط این سه VLAN با یکدیگر نیاز به یک Device لایه سوم می باشد . بنابراین به کمک روتر می توان ارتباط هر کدام از این VLAN ها را که دارای Network ID های متفاوتی می باشند برقرار کرد.

سوالی که مطرح می شود اینست که چگونه می توان پورتهای یک سوئیچ را درون VLAN هایی که به صورت منطقی تعریف شده اند قرار دهیم ؟ در ادامه این درس با روشهای مختلف جهت انجام اینکار آشنا خواهید شد .

Static VLANs



عضویت در VLAN به روش Static VLAN :

تابه اینجا با مفهوم VLAN و دلیل استفاده از آن در یک شبکه آشنا LAN شدید .

بعد از ساخت هر کدام از VLAN ها نوبت به عضویت در هر کدام از VLAN ها می رسد.

نحوه عضویت در VLAN ها به دو صورت می باشد :

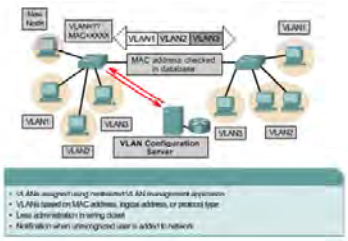
- Static VLAN
- Dynamic VLAN

:Static VLAN

به صورت پیش فرض روی تمامی روترهای یک VLAN به نام VLAN 1 وجود دارد به طوریکه تمامی پورتهای یک سوئیچ در آن قرار دارد . بنابراین برای رسیدن به هدف داشتن VLAN روی یک سوئیچ می بایست ابتدا VLAN های دیگری تعریف شده و سپس پورت به صورت تنظیمی از VLAN 1 خارج شده و درون VLAN مربوطه انداخته شوند . برای انجام دستی این کار از روش Static استفاده می کنیم . در روش Static VLAN بعد از تعریف کردن VLAN ها می بایست پورتهای مورد نظر را به داخل VLAN های تعریف شده انتقال داد و مابقی پورتها را در داخل VLAN 1 باقی گذاشت .

این روش بسیار ساده و دارای امنیت بالایی می باشد .

Dynamic VLANs



عضویت در VLAN به روش Dynamic VLAN :

در این روش VALN ها براساس شماره پورت دسته بندی نمی شوند . هر کدام می توانند مجموعه ای از آدرسهای فیزیکی (MAC Address) و یا آدرس منطقی (IP Address) و یا پروتکل باشند .

در این روش مدیریت هر کدام از VLAN ها به عهده یک Server مرکزی(VMPS)VLAN Membership Policy Server خواهد بود . این روش نسبت به روش Static دارای انعطاف پذیری بیشتر و Overhead بالاتری می باشد .

با این روش هر کدام از Node ها به هر کدام از سوئیچ ها که متصل شوند با مدیریتی که از سوی VMPS صورت می گیرد هر کدام Policy های مربوط به خود را خواهند داشت . در حالی که در روش Static هر کدام از پورتها مختص و متعلق به VLAN خاصی خواهند بود .

Adding a VLAN

Catalyst 2950

```
wg_sw_2950#vlan database
wg_sw_2950(vlan)# vlan vlan#  [name vlan-name]
```

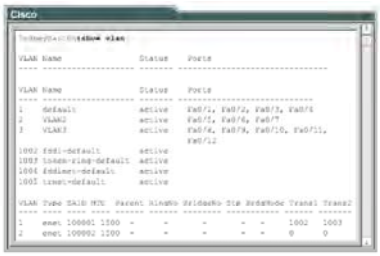
```
wg_sw_2950#vlan database
wg_sw_ 2950(vlan)#vlan 9 name switchlab2
wg_sw_ 2950(vlan)#exit
```

اضافه کردن VLAN :

شکل فوق نحوه تعریف یک VLAN جدید را روی Switch Catalyst 2950 نمایش می دهد . بعد از وارد شدن به VLAN Mode می توانید هر تعداد VLAN ایی را که می خواهید تعریف کنید .

شماره VLAN ها می توانند یکی از اعداد رنج 1 تا 4094 باشند .

Verifying VLAN Configuration



بررسی VLAN ها :

به کمک فرمان show VLAN می توان تعداد و نام VLAN ها و وضعیت هر کدام از آنها و پورتهایی را که در هر یک از آنها قرار دارد را مشاهده کرد .

Assigning Switch Ports to a VLAN

Catalyst 2950

```
wg_sw_2950(config-if)#switchport access vlan vlan-Name
```

قراردادن منطقی پورتها در VLAN مورد نظر :

بعد از تعریف کردن یک VLAN می بایست اعضاء آن را مشخص کرد . در صورتیکه بخواهید از روش Static VLAN برای نسبت دادن پورتها به VLAN استفاده کنید کافی است وارد اینترفیس مورد نظر شده و به کمک فرمان زیر آن را به صورت منطقی به داخل VLAN مورد نظر Move دهید .

درواقع به کمک فرمان زیر مشخص می کنید که Mode این پورت Access بوده و با آوردن نام VLAN ، VLAN ایی را که این پورت در آن قرار دارد مشخص می کنید . در ادامه این فصل با واژه Access و علت استفاده از آن بیشتر آشنا می شوید .

wg_sw_2950(config-if)#switchport access vlan *vlan-Name*

Deleting VLANs

حذف یک VLAN :

در تمامی سوئیچها VLAN 1 به صورت پیش فرض تعریف شده است و تمامی پورتها در داخل آن قرار دارد . بنابراین امکان حذف آن وجود ندارد.

درحالی که هر کدام از VLAN هایی را که تعریف می کنید می توانید حذف کنید . برای این منظور ابتدا می بایست تمامی پورتهایی را که در آن قرار دارند را حذف کرده و سپس VLAN مورد نظر را حذف کنید .

برای خارج کردن یک پورت از یک VLAN کافی است وارد اینترفیس مربوطه شده و فرمان زیر را وارد کنید :

Switch(config-if)# no switchport access vlan 300

Summary

- **After creating a VLAN, you can statically assign a port or a number of ports to that VLAN. A port can belong to only one VLAN at a time.**
- **You can verify the VLAN configuration using the show commands.**
- **As network topologies, business requirements, and individual assignments change, VLAN requirements also change.**

خلاصه :

به منظور کنترل و مدیریت ترافیک و افزایش security در یک شبکه LAN می بایست آن را به تعدادی Broadcast Domain تقسیم کرد به طوری که هر کدام از این Broadcast Domain های جدید یک Virtual LAN و یا VLAN خواهند بود .

هر کدام از VLAN ها شامل تعدادی پورت خواهند بود که این پورتهای می توانند همگی از یک سوئیچ و یا از تعدادی سوئیچ انتخاب شده باشند .

نحوه عضویت در هر کدام از VLAN ها به دو صورت امکان پذیر می باشد :

- Static VLAN
- Dynamic VLAN

درصورتیکه پورتها را به صورت Static عضو VLAN ها کنید در صورت تغییر در شبکه می بایست هر کدام از آنها را به صورت دستی تغییر دهید .

در روش Dynamic ، node های یک شبکه بر اساس آدرسهای فیزیکی و یا منطقی و یا پروتکل های مختلف دسته بندی می شوند و مدیریت آنها توسط یک Server انجام می شود .

درس پنجم :

Trunk
و نقش آن در هدایت
ترافیک تفکیک شده شبکه

هدف :

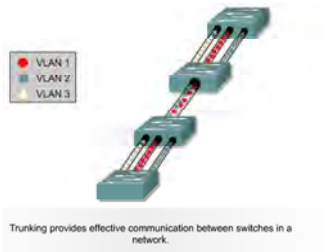
۱. معرفی Trunk و نحوه عملکرد آن در انتقال اطلاعات مربوط به VLAN ها .

۲. معرفی پروتکل های ISL و 802.1 Q و نحوه عملکرد آنها .

۳. نحوه تنظیم پروتکل های ISL و 802.1Q بر روی روتر و سوئیچ.

۴. معرفی native VLAN و تأثیری که برروی ترافیک Trunk می گذارد.

VLANs and Trunking



Trunking provides effective communication between switches in a network.

Trunk و نقش آن در انتقال ترافیک VLAN ها :

در درس گذشته با مفهوم VLAN و با ضرورت استفاده از آن در یک شبکه آشنا شدید . همانطور که می دانید VLAN ها به دو صورت روی سوئیچ تعریف می شوند :

۱. همگی روی یک سوئیچ تعریف می شوند (Local VLAN) .

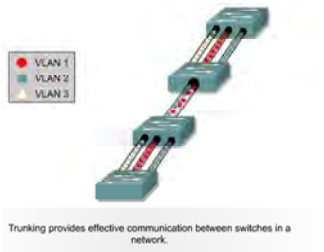
۲. روی سوئیچ های مختلف تعریف می شوند (End-to-End VLAN).

زمانی که تمامی VLAN ها روی یک سوئیچ تعریف شوند ارتباطی بین VLAN ها وجود نخواهد داشت . در صورتی که بخواهید این ارتباط را بین برخی از آنها برقرار کنید نیاز به یک Device لایه سوم (روتر) خواهید داشت تا ارتباط بین Broadcast Domain های متفاوت (VLAN) را برقرار کند .

بنابراین اینترفیسی که قرار است با روتر ارتباط داشته باشد را پورت Trunk و به این ارتباط Trunk گفته می شود .

در صورتی که حالت دوم رخ دهد و VLAN ها روی سوئیچ های متفاوتی قرار داشته باشند چگونه می توان ترافیک مربوط به هر کدام از VLAN ها را بین سوئیچ ها انتقال داد ؟

VLANs and Trunking



Trunking provides effective communication between switches in a network.

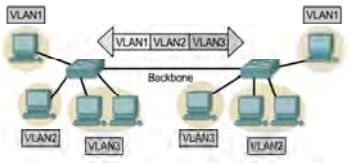
Trunk و نقش آن در انتقال ترافیک VLAN ها :

به شکل فوق توجه کنید . سه VLAN با نام های VLAN 1 ، VLAN 2 و VLAN 3 و ترافیک مربوط به هر کدام با رنگهای قرمز ، سبز و زرد روی هر سه سوئیچ نمایش داده شده است . در صورتیکه بخواهید بین VLAN ها ارتباط برقرار کنید دو راه پیش روی دارید :

یا VLAN های همنام را دو به دو با یک کابل ارتباطی متصل کنید که در این صورت تعدادی از پورتها را می بایست برای این کار کنار بگذارید و یا ترافیک تمامی VLAN ها را از یک کانال مشترک (Trunk) هدایت کنید . راه دوم منطقی تر و به صرفه تر می باشد اما یک مشکل وجود خواهد داشت .

چگونه ترافیکی که از این کانال مشترک هدایت می شود و شامل فریم هایی از VLAN های مختلف می باشد توسط سوئیچ دریافت کننده قابل تشخیص باشد !

Frame Tagging



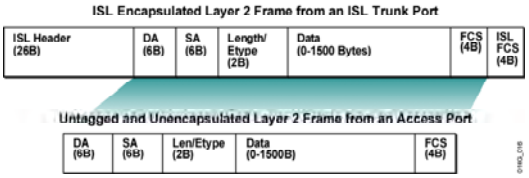
Tag زدن به هر فریم جهت انتقال در Trunk:

در صورتیکه هر کدام از فریمهای ارسالی از یک سوئیچ دارای برچسب باشد بنابراین براحتی می توان تشخیص داد که فریم از چه VLAN ایی آمده است و سوئیچ دریافت کننده آن را تحویل VLAN مربوطه می دهد .

بنابراین Trunk وظیفه انتقال فریم هایی را که دارای Tag مربوطه هستند به عهده دارد . به منظور Tag زدن به یک فریم در یک شبکه Ethernet دو استاندارد زیر تعریف شده است .

۱. **802.1Q**
۲. **Inter-Switch Link Protocol (ISL)**

ISL and Layer 2 Encapsulation

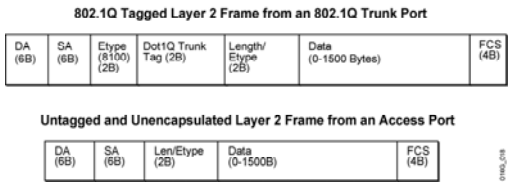


ISl به عنوان یک استاندارد لایه دوم :

ISL به عنوان یک استاندارد لایه دوم به منظور بسته بندی کردن یک فریم جهت انتقال در یک کانال ارتباطی مشترک (Trunk) می باشد . این پروتکل مختص به شرکت سیسکو بوده و روی device های لایه دوم به صورت پیش فرض فعال می باشد .

در این استاندارد ساختار فریم اولیه Ethernet تغییری نمی کند بلکه فقط فیلدهای ISL Header و ISL FCS به آن اضافه می شود .

802.1Q and Layer 2 Encapsulation



802.1Q به عنوان یک استاندارد لایه دوم:

802.1 Q به عنوان یک استاندارد Open در لایه دوم جهت برچسب زدن به فریم هایی که می بایست در داخل Trunk منتقل شوند به کار می رود نابراین سوئیچهایی از شرکتهای مختلف این پروتکل را ساپورت می کنند . بنابراین درصورتیکه که در یک شبکه تمامی سوئیچها سیسکویی نیستند ، می بایست از این پروتکل جهت Tag زدن به فریم ها استفاده کرد .

براساس این پروتکل ساختار فریم Ethernet تغیر می کند و منجر به ایجاد یک فریم جدید می شود .

Configuring ISL Trunking

```
Switch(config)#interface fastethernet 2/1
```

- **Enters interface configuration mode**

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

- **Configures the interface as a Layer 2 trunk**

```
Switch(config-if)#switchport trunk encapsulation isl
```

- **Selects the encapsulation**

نحوه تنظیم پروتکل ISL برروی Switch catalyst 2950 :

برای تنظیم کردن پروتکل ISL ابتدا به اینترفیسی که قرار است وظیفه ترانزیت ترافیک VLAN ها را به عهده گیرد وارد شده و سپس Mode مربوط به این اینترفیس را در وضعیت Trunk قرار می دهید .

نکته : یک پورت از سوئیچ می تواند در دو Mode مختلف قرار گیرد و نسبت به هر کدام از آن عکس العمل متفاوتی را نشان می دهد :

Access Mode و Trunk Mode .

یک پورت به صورت پیش فرض در حالت Access می باشد و هنگام تعریف VLAN و انتقال پورتهای به داخل VLAN ایجاد شده ، می بایست بگوییم که این پورت در حالت Access می باشد و یا اینکه می بایست ترافیک چند VLAN را منتقل کند . بنابراین درصورتی که قرار باشد ترافیک چند VLAN را منتقل کند ، میبایست آن را به صورت Trunk تعریف کرد تا قادر به تفکیک و شناسه گذاری جهت تفکیک VLAN ها باشد .

نکته : به صورت پیش فرض پروتکل ISL به منظور frame Tagging روی سوئیچ های سیسکو فعال می باشد .

Configuring 802.1Q Trunking

```
Switch(config)#interface fastethernet 2/1
```

- **Enters interface configuration mode**

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

- **Configures the interface as a Layer 2 trunk**

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

- **Selects the encapsulation**

802.1 Q به عنوان یک استاندارد لایه دوم :

درصورتی که بخواهید در یک شبکه از استاندارد 802.1 Q جهت برچسب گذاری فریم های VLANهای مختلف جهت انتقال برروی کانال مشترک (Trunk) استفاده کنید ، به کمک فرمان زیر ابتدا مشخص می کنید که این پورت به منظور انتقال ترافیک VLAN ها به عنوان پورت trunk انتخاب شده است .

Switch(config-if)#switchport mode trunk

سپس فرمان زیر پروتکل 802.1 Q را به عنوان پروتکل برچسب گذاری فریم ها تعیین می کند .

Switch(config-if)#switchport trunk encapsulation dot1q

Configuring 802.1Q Trunking

```
Switch(config)#interface fastethernet 2/1
```

- **Enters interface configuration mode**

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

- **Configures the interface as a Layer 2 trunk**

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

- **Selects the encapsulation**

802.1 Q به عنوان یک استاندارد لایه دوم (ادامه) :

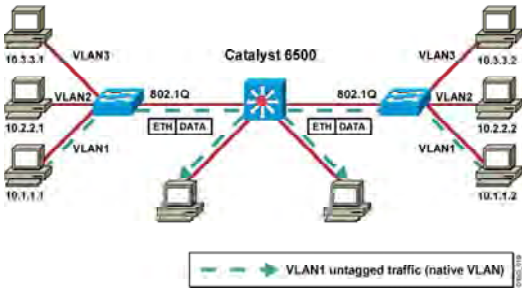
نکته : زمانی که Mode یک پورت Trunk تعریف شود این پورت وظیفه انتقال و Tag زدن به فریمهای تمام VLAN ها را بـه عهده دارد .می توانید به کمک فرمان زیر مشخص کنید که این پورت ترافیک کدام VLAN ها را جهت خـروج توسـط پـورت Trunk برچسـب زند :

Switch(config)#interface fastethernet 5/8

Switch(config-if)#switchport trunk allowed vlan 1,15

در این مثال این پورت وظیفه انتقال ترافیک مربوط به VLAN های 1 و 15 را به عـهده داشـته و فریم های مربوط به ایـن دو VLAN را جهت انتقال برچسـب خواهد زد .

Importance of Native VLANs



:Native VLAN

پورت Trunk تمامی فریمهای خروجی را Tag می زند . به شکل فوق توجه کنید . در این شکل روی Switch Catalyst 6500 فقط یک VLAN وجود دارد و آن هم VLAN 1 می باشد . در حالی که روی دو سوئیچ دیگر سه VLAN تعریف شده است .

همانطور که مشاهده می کنید VLAN 1 روی هر سه مشترک می باشد درحالی که فریم های که از VLAN 1 تولید می شوند توسط پورت Trunk برچسب زده می شوند و این منجر به افزایش Overhead روی پورت Trunk می شود .

در این مثال Native VLAN می گوید که فریم هایی که مربوط به VLAN 1 می باشند توسط پورت trunk برچسب زده نشوند .

پروتکل 802.1Q ، Native VLAN را پشتیبانی می کند و به کمک فرمان زیر نیز روی پورت Trunk فعال می شود :

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

Summary

- **A trunk is a Layer 2 point-to-point link between networking devices capable of Layer 2 operations. Trunks carry the traffic of multiple VLANs or multiple networks over a single physical link.**
- **ISL is a Cisco proprietary protocol for interconnecting Layer 2-capable devices. The 802.1Q protocol is an open standard protocol used to interconnect multiple Layer 2-capable devices.**
- **802.1Q trunks define a native VLAN for frames that are not tagged by default.**
- **ISL VLAN numbers are in the range 1 to 1001, while 802.1Q VLAN numbers are in the range 0 to 4094.**

خلاصه :

Trunk عبارت است از یک کانال ارتباطی مشترک که حامل ترافیک VLAN ها می باشد و پورتی از سوئیچ که وظیفه انتقال ترافیک VLANها را به عهده دارد پورت Trunk خواهد بود .

این پورت به منظور تفکیک فریم ها در سوئیچ مقصد ، شماره VLAN ایی را که هر کدام از فریم ها از آنجا نشأت گرفته شده اند را با زدن برچسب مشخص می کند .

دو استاندارد جهت برچسب گذاری به VLAN تعریف شده است :

- ISL
- 802.1 Q

ISL پروتکل مخصوص به سیسکو بوده و روی تجهیزات سیسکو به صورت پیش فرض فعال می باشد درحالی که 802.1 Q یک استاندارد عمومی می باشد که مختص به شرکت خاصی نمی باشد و درصورتی که در یک شبکه سوئیچ هایی از شرکت های متفاوتی داشته باشید میبایست از این استاندارد به منظور Frame Tagging استفاده کنید .

براساس استاندارد ISL شماره VLAN ها در رنج 1 تا 1001 شماره گذاری می شوند درحالی که براساس استاندارد 802.1 Q شماره VLAN ها عددی از رنج 0 تا 4094 خواهند بود .

درس ششم :

VTP
و نقش آن در مدیریت
شبکه Switching

هدف :

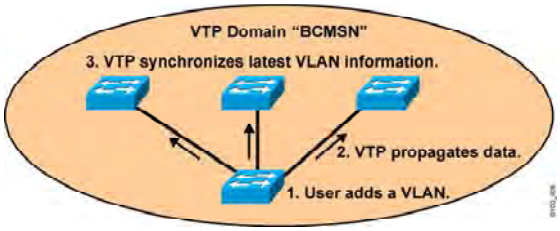
۱. تعریف VTP .

۲. عملکرد VTP دریک شبکه و Mode های مختلف آن .

۳. بررسی و خطایابی در عملکرد VTP .

VTP Protocol Features

- Advertises VLAN configuration information
- Maintains VLAN configuration consistency throughout a common administrative domain
- Sends advertisements on trunk ports only



ویژگی های پروتکل VTP :

در درسهای گذشته با مفهوم VLAN و Trunk در یک شبکه Ethernet آشنا شدید . با بزرگ شدن یک شبکه و افزایش تعداد سوئیچها ، تغییرات جزئی در هر کدام از VLAN ها و یا ساختن یک VLAN جدید منجر به ایجاد تغییر در بقیه سوئیچها می شود ، بنابراین مدیریت منابع در این شبکه با مشکلات بسیار زیادی همراه خواهد بود .

سیسکو برای رفع این مشکل VTP را ارائه کرده است .

VTP ، طرح مدیریت گروهی سوئیچ ها را معرفی می کند . بنابراین VTP با تعریف کردن یک ناحیه که شامل تعدادی سوئیچ می باشد و تعریف Client و Server در این شبکه ، تغییرات روی را Server اعمال کرده و سپس به اطلاع دیگر سوئیچها می رساند . بنابراین اطلاع رسانی درمورد VLAN ها و تغییرات آنها در این شبکه خیلی راحتر و سریعتر خواهد شد.

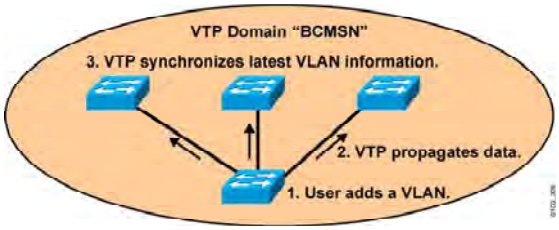
برای روشن شدن مطلب ابتدا با اصطلاحات مربوط به VTP شوید .

VTP Domain:

ناحیه ای که شامل تعدادی سوئیچ بوده به طوریکه هر سوئیچ اطلاعات مربوط به VLAN خود را با بقیه سوئیچ ها به اشتراک می گذارد .

VTP Protocol Features

- Advertises VLAN configuration information
- Maintains VLAN configuration consistency throughout a common administrative domain
- Sends advertisements on trunk ports only



ویژگی های پروتکل VTP (ادامه) :

هر سوئیچ تنها می تواند عضو یک VTP Domain باشد و سوئیچ هایی که در VTP Domain های متفاوتی هستند نمی توانند اطلاعات مربوط به VLAN هایشان را با یکدیگر به اشتراک بگذارند .

به شکل فوق توجه کنید . این شکل نشان دهنده یک VTP Domain به نام BCMSN می باشد .

همانطور که مشاهده می کنید خبر ساخته شدن یک VLAN روی یک سوئیچ به دیگر سوئیچ های این VTP Domain گزارش داده می شود .

:VTP advertisement

هر کدام از سوئیچ های سیسکو در VTP Domain اطلاعات مربوط به VLAN ها را به کمک VTP Advertisement از سوئیچ های مجاورش که از طریق پورت Trunk به آنها متصل است دریافت می کند .

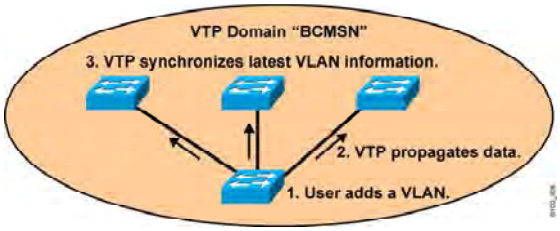
VTP Advertisement ها به صورت فریم های Multicast در VTP Domain ارسال می شود .

نکته : لینک بین دو سوئیچ می بایست به صورت Trunk تعریف شود تا VTP Advertisement ها قادر به انتقال باشند .

VTP Advertisement به سه فرم در یک VTP Domain منتشر می شوند :

VTP Protocol Features

- Advertises VLAN configuration information
- Maintains VLAN configuration consistency throughout a common administrative domain
- Sends advertisements on trunk ports only



ویژگی های پروتکل VTP (ادامه) :

- **Summary Adve tisement :**

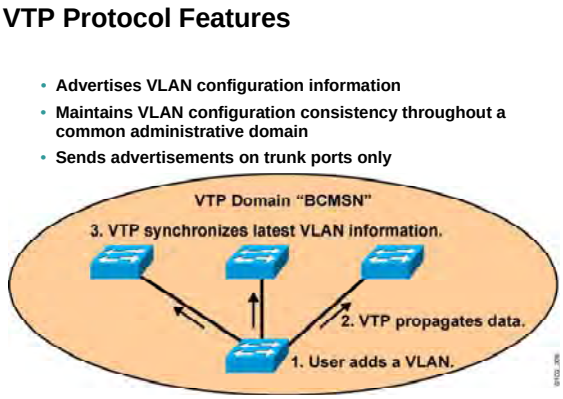
اطلاعاتی هستند که هر 300 ثانیه توسط VTP Server به بقیه سوئیچ ها در VTP Domain ارسال می شود و شامل اطلاعات مربوط به VLAN Database می باشد .

- **Subset Advertisement :**

اطلاعاتی هستند که توسط VTP Server هنگام رخ دادن تغییر در تنظیمات VLAN ها ارسال می شود و شامل اطلاعات VLAN Database و وضعیت هر کدام از VLAN ها می باشد .

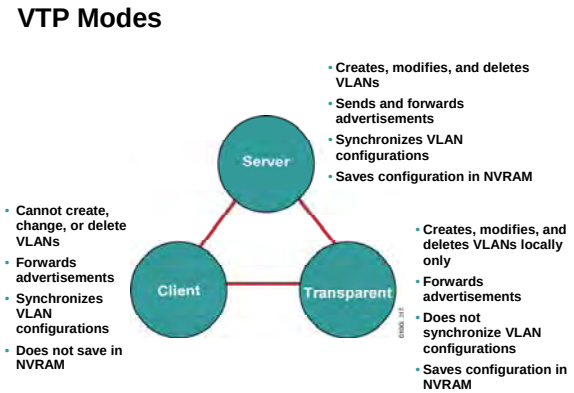
- **Advertisement requests from Clients :**

اطلاعاتی هستند که توسط VTP Client از VTP Server درخواست می شوند .



ویژگی های پروتکل VTP (ادامه):

به طور مثال زمانی که یک VTP Client را خاموش و سپس روشن کنید اطلاعات مربوط به VTP را که در حافظه فرار RAM نگهداری کرده بود از دست می دهد . بنابراین می بایست این اطلاعات را دوباره از VTP Server دریافت کند . پس درخواستی را به VTP Server ارسال می کند و VTP Server در پاسخ VLAN Database خود را در به VTP Client ارسال می کند .



Mode های مختلف پروتکل VTP :

در یک VTP Domain هر کدام از سوئیچ ها می بایست در یکی از Mode های زیر ایفای نقش کنند :

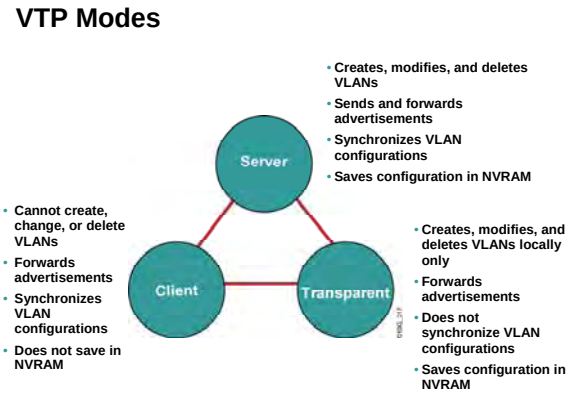
- Server Mode
- Client Mode
- Transparent Mode

در واقع VTP Mode مشخص می کند که هر کدام از سوئیچ ها چگونه در اطلاع رسانی در مورد VLAN ها و عملکرد VTP نقش خواهند داشت .

:Server Mode

سوئیچی که در این Mode قرار گیرد دارای توانایی کامل در ایجاد ، حذف و تغییر VLAN و مدیریت Domain خواهد بود.تمامی سوئیچ ها به صورت پیش فرض در این Mode قرار دارند .

نکته : در یک VTP Domain دست کم یک سوئیچ می بایست نقش VTP Server را به عهده داشته باشد .



Mode های مختلف پروتکل VTP :

Client Mode:

سوئیچی که در این Mode قرار می گیرد قادر به حذف و یا اضافه و یا تغییر VLAN نخواهد بود .

سوئیچی که در این Mode قرار می گیرد به تغییراتی که توسط سوئیچ های دیگر گزارش می شود گوش می دهد و این تغییرات را روی خود اعمال می کند.

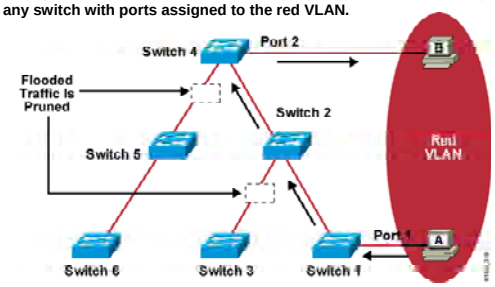
Transparent Mode:

سوئیچی که در این Mode قرار می گیرد به عنوان یک عضو خنثی عمل می کند . اطلاعاتی که در مورد VTP از سوئیچ های مجاور دریافت می کند را بدون اینکه روی خود اعمال کند از طریق پورت Trunk به سوئیچهای مجاورش ارسال می کند . در این Mode سوئیچ قادر به حذف و اضافه کردن VLAN می باشد اما این تغییرات را به دیگر سوئیچ ها ارسال نمی کند .

درواقع تفاوت اصلی Transparent Mode با Server Mode در این است که VTP Server تغییرات روی VLAN های خود را به تمامی سوئیچ های موجود در VTP Domain اطلاع می دهد درحالی که VTP Transparent تغییرات روی VLAN های خود را به دیگران اطلاع نمی دهد .

VTP Pruning

- Increases available bandwidth by reducing unnecessary flooded traffic
- Example Station A sends broadcast, and broadcast is flooded only toward any switch with ports assigned to the red VLAN.



:VTP Pruning

همانطور که می دانید Broadcast ای که یک سوئیچ دریافت می کند از تمامی پورتهایش به بیرون ارسال می کند .

اگر پورتی که در یک VALN قرار دارد فریم Broadcast را به سوئیچ ارسال کند ، تمامی پورتهایی که در این VLAN قرار دارند فریم Broadcast را دریافت می کنند و همچنین سوئیچ های دیگری که دارای VLAN همنام با این VLAN هستند نیز فریم Broadcast را دریافت می کنند .

به شکل فوق توجه کنید تمامی سوئیچ ها دارای VLAN ایی به نام Red VLAN هستند اما فقط Switch1 و Switch 4 در VLAN1 تعدادی پورت دارند . سوئیچ های دیگر علیرغم داشتن VLAN 1 هیچ پورتی در این VLAN ندارند . با این وجود هر کدام از سوئیچ ها ، Broadcast هایی را که مربوط به VLAN 1 می باشد را به سمت پورت Trunk و درنتیجه کانال ارتباطی trunk هدایت کرده و این منجر به افزایش ترافیک بیهوده بر این کانال می شود .

VTP Prunning می گوید که فریم های Broadcast در یک VLAN به سوئیچ هایی تحویل داده شوند که پورتی در آن VLAN داشته باشند . به طور مثال در این شکل Switch 1 و Switch 4 هر دو دارای پورتهایی در Red VLAN هستند درحالی که سوئیچ های دیگر علیرغم داشتن این VLAN فاقد پورتی در این VLAN هستند . درنتیجه ترافیک بیهوده روی کانال ارتباطی Trunk تحمیل نخواهد شد.

VTP Configuration Guidelines

- **Configure the following:**
  - **VTP domain name**
  - **VTP mode (server mode is the default)**
  - **VTP pruning**
  - **VTP password**

تنظیم پروتکل VTP روی یک سوئیچ :

تنظیم کردن VTP شامل مراحل زیر می باشد :

به منظور تنظیم کردن VTP روی یک سوئیچ می بایست مراحل زیر را انجام دهید :

- تعیین نام VTP Domain
- تعیین VTP Mode
- تعیین VTP Password
- فعال کردن VTP Pruning

Configuring a VTP Server

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

- **Configures VTP server mode**

```
Switch(config)#vtp domain domain-name
```

- **Specifies a domain name**

```
Switch(config)#vtp password password
```

- **Sets a VTP password**

```
Switch(config)#vtp pruning
```

- **Enables VTP pruning in the domain**

تنظیم VTP Server :

تعیین نام VTP Domain :

به کمک فرمان زیر نام Domain را برای سوئیچ مشخص می کنید . سوئیچ های که دارای نام VTP Domain یکسان باشند می توانند اطلاعات مربوط به VLAN ها را با یکدیگر به اشتراک بگذارند .

Switch(config)#vtp domain *domain-name*

تعیین VTP Mode :

سوئیچ ها به صورت پیش فرض Server Mode هستند . به کمک فرمان زیر می توانید VTP Mode را روی سوئیچ 2950 در حالت Server قرار دهید .

Switch(config)#vtp server

تعیین VTP Password :

در یک VTP Domain با مشخص شدن VTP Server هر سوئیچ دیگری که Client Mode باشد اطلاعات مربوط به VLAN ها را از VTP Server می گیرد . حال در صورتی که نخواهید هر کسی براحتی بتواند سوئیچ خود را وارد شبکه کرده و

Configuring a VTP Server

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

- **Configures VTP server mode**

```
Switch(config)#vtp domain domain-name
```

- **Specifies a domain name**

```
Switch(config)#vtp password password
```

- **Sets a VTP password**

```
Switch(config)#vtp pruning
```

- **Enables VTP pruning in the domain**

تنظیم VTP Server (ادامه) :

اطلاعات مربوط Vlan ها را دریافت کند می بایست پس از انجام Authentication و یکسان بودن پسورد اطلاعات مربوط به VLAN را دریافت کند.

Switch(config)#vtp password *password*

فعال کردن VTP Pruning :

با به کار بردن فرمان زیر ویژگی pruning روی سوئیچ فعال می شود .

Switch(config)#vtp pruning

Configuring a VTP Client

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

- **Configures VTP server mode**

```
Switch(config)#vtp domain domain-name
```

- **Specifies a domain name**

```
Switch(config)#vtp password password
```

- **Sets a VTP password**

تنظیم VTP Client :

درصورتی که بخواهید یک سوئیچ را به عنوان VTP Client معرفی کنید ، می بایست نام VTP Domain و سپس VTP Mode و VTP Password را روی سوئیچ تنظیم کنید تا این سوئیچ بتواند اطلاعات مربوط به VLAN های دیگر را از VTP Server دریافت کند .

بنابراین درصورتیکه که یک سوئیچ را به صورت Client Mode تعریف کنید توانایی ایجاد و یا حذف VLAN را نخواهد داشت . بنابراین می بایست این تغییرات روی VTP Server اعمال شود و سپس به کمک VTP Advertisement هایی که توسط VTP Server ارسال می شود روی VTP Client اعمال شود .

Verifying the VTP Configuration

```
Switch#show vtp status
```

```
Switch#show vtp status

VTP Version                     : 2
Configuration Revision          : 247
Maximum VLANs supported locally : 1005
Number of existing VLANs        : 33
VTP Operating Mode              : Client
VTP Domain Name                 : Lab_Network
VTP Pruning Mode                : Enabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0x45 0x52 0xB6 0xFD 0x63 0xC8 0x49 0x80
Configuration last modified by 0.0.0.0 at 8-12-99 15:04:49
Switch#
```

بررسی عملکرد VTP روی یک سوئیچ :

شکل فوق وضعیت VTP را روی یک سوئیچ نمایش می دهد . به کمک فرمان زیر می توانید وضعیت VTP را روی یک سوئیچ بررسی کنید .

Switch#show vtp status

این سوئیچ در VTP Domain ایی با نام Lab_Network و به صورت VTP Client می باشد . روی این سوئیچ VTP Pruning فعال شده است .

Verifying the VTP Configuration (Cont.)

```
Switch#show vtp counters
```

```
Switch#show vtp counters

VTP statistics:
Summary advertisements received    : 7
Subset advertisements received     : 5
Request advertisements received    : 0
Summary advertisements transmitted : 997
Subset advertisements transmitted  : 13
Request advertisements transmitted : 3
Number of config revision errors   : 0
Number of config digest errors     : 0
Number of V1 summary errors        : 0

VTP pruning statistics:
Trunk            Join Transmitted Join Received    Summary advts received from
                                                   non-pruning-capable device
---------------- ---------------- ---------------- ---------------------------
Fa5/8              43071            42766            5
```

بررسی عملکرد VTP روی یک سوئیچ (ادامه) :

به کمک فرمان زیر می توانید پورتی را که به عنوان Trunk ، ترافیک VLAN ها را منتقل مـی کنـد و همچنـین انـواع VTP Advertisement ها و تعداد ه کدام از آنها را مشاهده و بررسی کنید .

Switch#show vtp counters

Problem: VTP Not Updating Configuration on Other Switches

- **Make sure switches are connected through trunk links.**
- **Make sure the VTP domain name is the same on the appropriate switches.**
- **Check that the switch is not in VTP transparent mode.**
- **Verify the same password used on all switches in the VTP domain.**

طرح یک مشکل :

چه مشکلاتی ممکن است رخ دهد تا یک سوئیچ نتواند تنظیمات مربوط به VLAN ها را از VTP Server دریافت کند ؟

در صورتیکه سوئیچ اطلاعات مربوط به VLAN های دیگر را دریافت نکند می بایست موارد زیر را بررسی شود :

۱. از برقراری ارتباط فیزیکی پورت Trunk با سوئیچ مجاورش مطمئن شوید .

۲. از یکسان بودن نام VTP Domain در این سوئیچ با VTP Server مطمئن شوید.

۳. بررسی کنید که Mode سوئیچ Transparent نباشد .

۴. و در آخر از یکسان بودن پسورد این سوئیچ با دیگر سوئیچ ها اطمینان حاصل کنید .

Summary

- **VTP is used to distribute and synchronize information about VLANs configured throughout a switched network.**
- **When a network device is in VTP server mode, you can change the VLAN configuration and have it propagate throughout the network.**
- **Use show commands to verify the VTP configuration.**
- **Problems with VTP configuration can frequently be traced to improperly configured trunk links, domain names, VTP modes, or passwords.**

خلاصه :

بزرگ شدن یک شبکه و افزایش تعداد سوئیچها نیاز به مدیریت روان تر را ایجاب می کند زیرا در یک شبکه با اندازه بزرگ ، تغییرات جزئی مانند تغییر هر کدام VLAN ها و یا ساختن یک VLAN جدید نیاز به تغییر در بقیه سوئیچها دارد و این کار می بایست به صورت دستی توسط admin شبکه صورت گیرد ، بنابراین مدیریت منابع در این شبکه با مشکلات بسیار زیادی همراه خواهد بود . VTP راه حل سیسکویی این مشکل خواهد بود .

VTP ، طرح مدیریت گروهی سوئیچ ها را معرفی می کند . بنابراین VTP با تعریف کردن یک ناحیه که شامل تعدادی سوئیچ می باشد و تعریف Client و Server در این شبکه ، تغییرات را روی Server اعمال کرده و سپس به اطلاع دیگر سوئیچها می رساند .

فصل پنجم :

NAT

NAT (Network Address Translation):

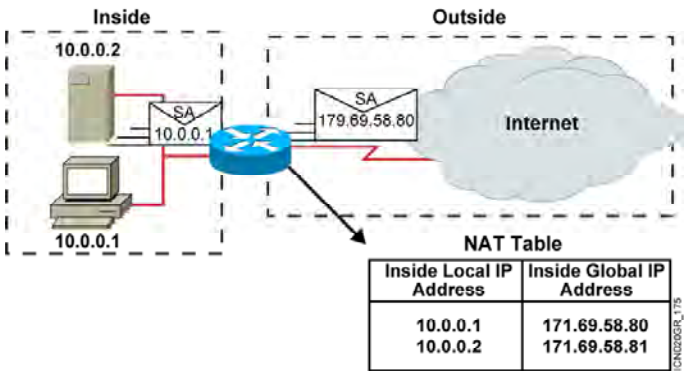
NAT (Network Address Translation) مکانیزم ترجمه آدرس های Invalid به آدرسهای Valid می باشد.

همانطور که می دانید آدرس های Valid آدرس های هستند که توسط Region های مختلف IANNA رجیستر شده و منحصر به فرد می باشند .
از آنجایی که تعداد IP V4 محدود می باشد بنابراین نمی توان به هر Station در دنیا یک IP رجیستر شده نسبت داد . پس راه حل مشکل کمبود تعداد IP رجیستر شده چه می تواند باشد؟ IP V6 راه حل تعداد محدود IP V4 می باشد .
اما مسئله اینجاست که استفاده از آن و گسترده شدنش زمان بر است بنابراین نمی تواند یک راه حل کوتاه مدت باشد . راه حل دیگر استفاده از ترجمه آدرسها یا همان NAT می باشد.
درواقع NAT با ترجمه کردن تعدادی از آدرسهای Invalid به آدرس و یا آدرسهای رجیستر شده این مشکل را حل کرده است. اما این تنها کاربرد NAT نیست ، بلکه یکی دیگر از کاربردهای NAT برقراری امنیت در شبکه می باشد .
درواقع یکی از راههای دور نگه داشتن شبکه محلی از دسترس هکرها ، پنهان کردن دستگاه ها به کمک آدرس غیر واقعی است. بنابراین با ترجمه کردن آدرس واقعی یک Station به آدرس دیگر می توان امنیت این دستگاه را برقرار کرد.

بنابراین به طور کلی می توان گفت NAT مکانیزم ترجمه آدرسهای Invalid یک شبکه به آدرس های رجیستر شده می باشد.
در این درس با نحوه عملکرد NAT و انواع آن آشنا خواهید شد . بنابراین تا پایان این درس با من همراه شویید.

Network Address Translation

Cisco.com



- An IP address is either local or global.
- Local IP addresses are seen in the inside network.

معرفی مفاهیم اولیه NAT و انواع آن :

همانطور که می دانید آدرسهای Valid آدرسهای هستند که توسط Region های مختلف IANNA در نقاط مختلف جهان رجیستر می شوند . درواقع آدرسهای IP V4 و IP V6 توسط این Region ها رجیستر می شوند . درصورتی که از IP V6 استفاده شود بنا به ساختار آن احتمال تمام شدن این آدرس تقریبا غیر ممکن می باشد ، اما مشکل زمانی پیش می آید که از IP V4 استفاده کنیم . درواقع نمی توان به ازای هر Station در شبکه یک آدرس Valid دریافت کرد . پس تا به اینجا با مشکل و صورت مسئله آشنا شدید اما سوالی که مطرح می شود اینست که راه حل چیست ؟

NAT (Network Address Translation) مکانیزم ترجمه آدرسهای Invalid به آدرسهای Valid می باشد. درواقع پکتی که از شبکه خارج می شود دیگر با نام و مشخصه داخلی خود به شبکه های بیرون معرفی نمی شود ، بلکه آدرس ایی که از آنجا نشأت گرفته شده است را با آدرس رجیستر شده جابه جا کرده و با این آدرس جدید ارسال و دریافت پکت را انجام می دهد .
می توان گفت NAT راه برقراری ارتباط شبکه داخلی به شبکه اینترنت و تبدیل آدرسهای invalid به آدرسهای معتبر و منحصر به فرد می باشد .
برای شناخت بیشتر آن گام اول شناخت مفاهیم اولیه می باشد.
از دیدگاه NAT شبکه به دو دسته کلی زیر تقسیم می شود :

١. Inside Network
٢. Outside Network

Inside Network: به شبکه یا شبکه های گفته می شود که دارای آدرسهای Invalid باشند . درواقع شبکه داخلی که آدرس Station های مختلف آن توسط IANNA رجیستر نشده است در مفهوم NAT همان Inside Network است.

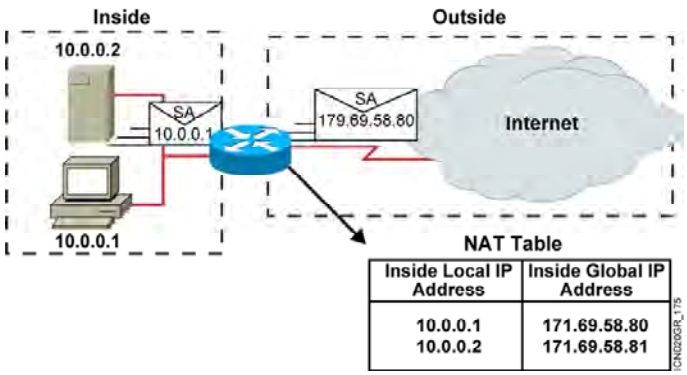
Outside Network: به شبکه های گفته می شوند که دارای آدرسهای رجیستر شده باشند. اینترنت مجموعه ای از شبکه هایی با آدرسهای رجیستر شده می باشد که در مفهوم NAT همان Outside Network تلقی می شود.

Inside Interface : به اینترفیسی از روتر NAT که در داخل ناحیه Inside Network قرار گرفته است گفته می شود . درواقع اینترفیسی که در رنج آدرس شبکه داخلی قرار دارد .

Outside Interface : به اینترفیسی از روتر NAT که در داخل ناحیه Outside Network قرار گرفته است گفته می شود . آدرسی که به این اینترفیس نسبت داده می شود لزوما آدرس رجیستر شده نیست و حتی می تواند از آدرس Unnumbered استفاده کرد .

Network Address Translation

Cisco.com



- **An IP address is either local or global.**
- **Local IP addresses are seen in the inside network.**

معرفی مفاهیم اولیه NAT و انواع آن :

IP Address ها در مفهوم NAT به چهار دسته زیر تقسیم می شوند:

١. Inside Local
٢. Inside Global
٣. Outside Local
٤. Outside Global

Inside Local :
به آدرسهایی گفته می شود که به Station های مختلف در یک شبکه محلی داده می شود . ازطرفی این آدرسها ، آدرسهایی نیستند که توسط Region های مختلف رجیستر شده باشند . درواقع این آدرسها برای ارتباط با اینترنت قابل استفاده نبوده و نیاز به ترجمه به آدرسهای رجیستر شده دارند.
مانند آدرسی که به یک کامپیوتر یا یک سوئیچ و ... داده می شود .

Inside Global :
به آدرسهایی گفته می شود که توسط Region های مختلف IANNA رجیستر شده اند و آدرسهای محلی جهت نمایش در اینترنت به این آدرسها ترجمه می شوند. درواقع دسته ای از آدرسهای هستند که در عملیات NAT از آنها استفاده خواهد شد.

Outside Local :
به آدرسی گفته می شود که در رنج آدرس Inside Network قرارداشته و نمایش دهنده راه ارتباط NAT Router با شبکه Inside است .
به عبارتی باید به روتر بگوییم که از چه طریق به شبکه Inside دسترسی پیدا می کند درنتیجه در رنج آدرس شبکه Inside نیز می بایست باشد.

Outside Global :
به آدرسهای رجیستر شده ای گفته می شود که در Outside Network قرار داشته و قابل Route شدن نیز هستند. درواقع Destination Address مربوط به پکتهایی است که از شبکه Inside نشأت گرفته شده است و NAT Router آن را قابل هدایت به سمت شبکه هایOutside می کند .

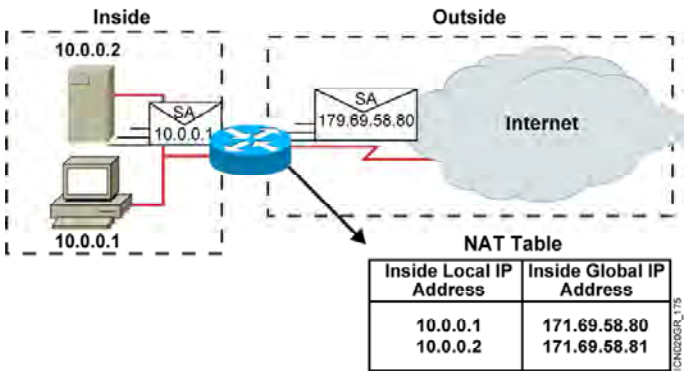
انواع NAT :

همانطور که می دانید NAT وظیفه ترجمه آدرسهای invalid به آدرسهای Valid را به عهده دارد . بنابراین با توجه به اینکه این ترجمه چگونه انجام می شود ، NAT را می توان به سه دسته کلی زیر دسته بندی کرد :

١. Static NAT
٢. Dynamic NAT
٣. Dynamic NAT With Overload

Network Address Translation

Cisco.com



- **An IP address is either local or global.**
- **Local IP addresses are seen in the inside network.**

معرفی مفاهیم اولیه NAT و انواع آن :

Static NAT :

همانطور که از نامش مشخص می باشد ، عملیات ترجمه به صورت دستی صورت می گیرد . درواقع به صورت دستی به NAT Router گفته می شود که کدام آدرس Invalid را به چه آدرس Valid و رجستر شده ای ترجمه کند.

بنابراین به صورت دستی یک تناظر یک به یک بین آدرسهای Invalid و آدرسهای Valid شکل می گیرد .

درنتیجه درصورتی که یک Station نیاز به ارتباط با شبکه Outside داشته باشد NAT Router یک آدرس Valid به این آدرس متناظر کرده و از این به بعد این آدرس Valid در تناظر یک به یک با آدرس invalid خواهد بود و روتر NAT هر درخواستی که با این آدرس دریافت کند آن را ترجمه کرده و با آدرس Valid مربوطه به Outside Network هدایت می کند .

اما این روش دارای یک مشکل می باشد . درصورتی که تعداد station هایی که دارای آدرس Invalid هستند بیشتر از آدرسهای Valid باشد تناظر یک به یک امکان پذیر نخواهد بود.

Dynamic NAT :

در این حالت عملیات ترجمه به صورت اتوماتیک توسط NAT Router انجام می شود . در این روش لیستی از آدرسهای invalid که نیاز به ارتباط با شبکه های Outside دارند و یک لیست از آدرسهای Valid که رجیستر شده اند تهیه شده و در نهایت NAT Router ارتباط این دو لیست را برقرار می کند.

بنابراین در صورتی که تعداد آدرسهای Invalid بیشتر از آدرسهای Valid باشد و درخواستی برای ترجمه به NAT Router وارد شود و روتر تمامی آدرسهای Valid خود را استفاده کرده باشد ، درخواست برگشت می خورد و تا زمانی که یک آدرس Valid آزاد نشود درخواست های جدید drop خواهند شد.

Dynamic NAT With Overload:

این روش همانند روش Dynamic NAT می باشد ، با این تفاوت که ترجمه بین آدرسهای Invalid با فقط یک آدرس Valid صورت می گیرد.

بنابراین برای تفکیک کردن آدرسهای Invalid از یکدیگ نیاز به مشخصه دیگری هم هست.

PAT یا همان Port Address Translation مکانیزمی است که در آن تفکیک آدرسها به کمک پورتهای مختلف صورت می گیرد.

بنابراین دراین حالت آدرسهای Invalid به یک آدرس Valid ترجمه می شوند اما Nat Router برای هر کدام از آنها یک پورت جداگانه باز می کند . بنابراین تمایز بین آدرسها به کمک شماره پورت ها صورت می گیرد.

NAT Table:

تا به اینجا با انواع NAT آشنا شدید . سوالی که پیش می آید اینست که NAT Router اطلاعات بدست آورده را در کجا نگهداری می کند ؟

NAT Table شامل اطلاعاتی می باشد که توسط NAT Router بدست آمده است . درواقع شامل آدرسهای Inside Local ، Inside Global ، Outside Local و Outside Global می باشد .

بنابراین به کمک این جدول می توان دید که کدام آدرس Invalid به کدامیک از آدرسهای Valid ترجمه شده است .

نحوه ترجمه آدرس مبداء در NAT :

تا به اینجا با مفاهیم اولیه NAT و انواع آن آشنا شدید. سوالی که پیش می آید اینست که NAT Router چگونه عملیات Translation را انجام می دهد ؟
برای پاسخ به این سوال به این شکل توجه کنید.
در این مثال کامپیوتر با آدرس Invalid از ناحیه Inside قصد ارتباط با یک کامپیوتر با آدرس Valid در ناحیه Outside را دارد .
این کامپیوتر پکتی را با آدرس مبداء 1.1.1.1 و آدرس مقصد 9.6.7.3 به سمت روتر NAT ارسال می کند .
آدرس 1.1.1.1 همان Inside Local Address و آدرس 9.6.7.3 همان Outside Global Address می باشد.

NAT Router به کمک NAT Table خود عملیات ترجمه را انجام می دهد . اینکه این Table چگونه تکمیل شده است کاملا بستگی به نوع NAT ایی می باشد که ما انتخاب و تنظیم کرده ایم .
بنابراین NAT Router به کمک اطلاعات جدول خود ، جای Source Address را در پکت دریافتی عوض کرده و آن را با Source Address جدید به سمت مقصد هدایت می کند. اما NAT Router بدون تغییر دادن آدرس مقصد پکت آن را به سمت مقصد هدایت می کند .

همانطور که گفته شد Inside Global Address مجموعه ایست از آدرسهایی که توسط Region های مختلف در دنیا رجیستر شده است . بنابراین به مانند استخری از آدرس هایی می باشند که در دل NAT Router قرار داشته و نسبت به نوع NAT ایی که روی روتر تنظیم شده است از آن استفاده می شود .

Configuring Static Translation

Cisco.com

```
Router(config)#ip nat inside source static local-ip global-ip
```

- Establishes static translation between an inside local address and an inside global address

```
Router(config-if)#ip nat inside
```

- Marks the interface as connected to the inside

```
Router(config-if)#ip nat outside
```

- Marks the interface as connected to the outside

Static NAT و نحوه پیکربندی آن :

در این حالت عملیات ترجمه آدرس مبداء به صورت دستی انجام می گیرد . درواقع به NAT Router می گوییم که کدام آدرس Invalid را به کدام آدرس Valid ترجمه کند .
این تنظیم شامل سه مرحله می باشد :

۱. فعال کردن Static NAT
۲. تعیین Inside Interface
۳. تعیین Outside Interface

فعال کردن Static NAT :
این مرحله شامل فعال کردن Static NAT بین Inside Local و Inside Global می باشد.
برای این منظور وارد Global Mode شده و فرمان زیر را وارد می کنید .

Router(config)#ip nat inside source static local-ip global-ip

Local-ip همان Inside Local Address و Global-address همان آدرس Inside Global می باشد.

تعیین Inside Interface :

در این مرحله اینترفیسی از NAT Router که در ناحیه Inside قرار دارد را انتخاب کرده و به کمک فرمان زیر آن را به عنوان Inside Interface انتخاب می کنیم .

Router(config-if)#ip nat inside

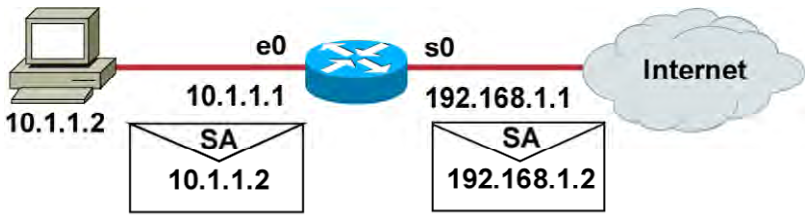
تعیین Outside Interface :

در این مرحله اینترفیسی از NAT Router که در ناحیه Outside قراردارد را انتخاب کرده و به کمک فرمان زیر آن را به عنوان Outside Interface انتخاب می کنیم .

Router(config-if)#ip nat outside

Enabling Static NAT Address Mapping Example

Cisco.com




```
interface s0
ip address 192.168.1.1 255.255.255.0
ip nat outside
!
interface e0
ip address 10.1.1.1 255.255.255.0
ip nat inside
!
ip nat inside source static 10.1.1.2 192.168.1.2
```

ICND2OGR_282

راه اندازی Static NAT در یک مثال :

مثال زیر نمونه ای از راه اندازی Static NAT روی NAT Router می باشد . در این مثال آدرس 10.1.1.2 به عنوان Inside Local Address و آدرس 192.168.1.1 به عنوان Inside Global Address انتخاب شده است . بنابراین Static NAT ارتباط یک به یک بین آدرس Inside Local با یک آدرس Inside Global می باشد.

بنابراین پکتی که آدرس مبداء آن 10.1.1.2 باشد به وسیله NAT Router با آدرس 192.168.1.2 جابه جا شده و سپس به سمت اینترنت هدایت می شود.
بنابراین در مکانیزم NAT فقط جای source Address عوض می شود و Destination Address بدون تغییر باقی می ماند.

Configuring Dynamic Translation

Cisco.com

```
Router(config)#ip nat pool name start-ip end-ip
{netmask netmask | prefix-length prefix-length}
```

- **Defines a pool of global addresses to be allocated as needed**

```
Router(config)#access-list access-list-number permit
source [source-wildcard]
```

- **Defines a standard IP access list permitting those inside local addresses that are to be translated**

```
Router(config)#ip nat inside source list
access-list-number pool name
```

- **Establishes dynamic source translation, specifying the access list defined in the prior step**

Dynamic NAT و نحوه پیکربندی آن :

در این حالت عملیات ترجمه آدرس مبداء به صورت دستی صورت نمی پذیرد . در این روش لیستی از آدرسهای invalid که نیاز به ارتباط با شبکه های Outside دارند و لیستی از آدرسهای Valid رجیستر شده تهیه می شود و سپس ارتباط بین این دو لیست توسط NAT Router برقرار می شود .

این تنظیم شامل پنج مرحله زیر می باشد :

۱. معرفی لیستی از آدرسهای Valid یا همان Inside Global Address
۲. معرفی لیستی از آدرسهای Invalid یا همان Inside Local Address
۳. فعال کردن Dynamic NAT
۴. تعیین Inside Interface
۵. تعیین Outside Interface

معرفی لیستی از آدرسهای Valid یا همان Inside Global Address :

در این مرحله لیستی از آدرسهای رجیستر شده ای را که می خواهید در عملیات Translation شرکت کنند را انتخاب کرده و در یک Pool قرار می دهید .
برای این منظور وارد Global Mode شده و به کمک فرمان زیر این Pool را معرفی می کنید.

Router(config)#ip nat pool name start-ip
end-ip {netmask netmask | prefix-length prefix-length}

Name : نام اختیاری است که به Pool نسبت داده می شود و در هنگام تعریف NAT از آن استفاده می کنیم.
Start-ip : اولین آدرس از رنج آدرس های رجیستر شده .
End-ip : آخرین آدرس از رنج آدرس های رجیستر شده .
Netmask : Subnet mask مربوطه که نمایش دهنده تعداد IP های رجیستر شده می باشد .

معرفی لیستی از آدرسهای Invalid یا همان Inside Local Address :

در این مرحله لیستی از آدرسهای Invalid را که می خواهید در عملیات ترجمه شرکت کرده و قادر به ارسال پکت به شبکه اینترنت باشند را به کمک Access List معرفی می کنید .

فعال کردن Dynamic NAT :

این مرحله شامل فعال کردن Dynamic NAT و برقراری ارتباط بین Access List که لیستی از آدرس های Invalid است و Pool که لیستی از آدرسهای رجیستر شده است ، می باشد.
برای این منظور وارد Global Mode شده و فرمان زیر را وارد می کنید .

Configuring Dynamic Translation

Cisco.com

```
Router(config)#ip nat pool name start-ip end-ip
{netmask netmask | prefix-length prefix-length}
```

- **Defines a pool of global addresses to be allocated as needed**

```
Router(config)#access-list access-list-number permit
source [source-wildcard]
```

- **Defines a standard IP access list permitting those inside local addresses that are to be translated**

```
Router(config)#ip nat inside source list
access-list-number pool name
```

- **Establishes dynamic source translation, specifying the access list defined in the prior step**

Dynamic NAT و نحوه پیکربندی آن :

Router(config)#ip nat inside source
list access-list-number pool name

بنابراین این جمله ارتباط بین Access List که با شماره مشخص شده است و Pool که با نام معرفی شده است را برقرار می کند.

تعیین Inside Interface :

در این مرحله اینترفیسی از NAT Router که در ناحیه Inside قراردارد را انتخاب کرده و به کمک فرمان زیر آن را به عنوان Inside Interface انتخاب می کنیم .

Router(config-if)#ip nat inside

تعیین Outside Interface :

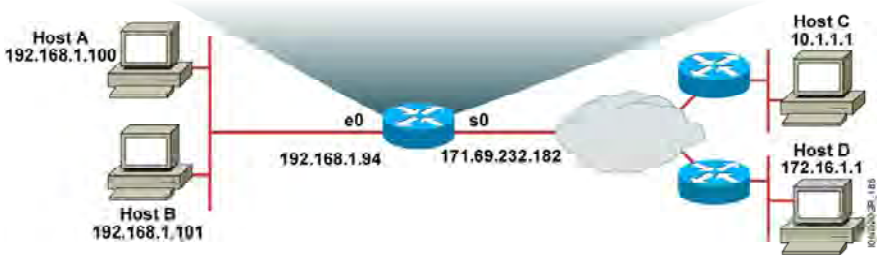
در این مرحله اینترفیسی از NAT Router که در ناحیه Outside قراردارد را انتخاب کرده و به کمک فرمان زیر آن را به عنوان Outside Interface انتخاب می کنیم .

Router(config-if)#ip nat outside

Dynamic Address Translation Example

Cisco.com

```
ip nat pool net-208 171.69.233.209 171.69.233.222 netmask
255.255.255.240
ip nat inside source list 1 pool net-208
!
interface serial 0
 ip address 171.69.232.182 255.255.255.240
 ip nat outside
!
interface ethernet 0
 ip address 192.168.1.94 255.255.255.0
 ip nat inside
!
access-list 1 permit 192.168.1.0 0.0.0.255
```

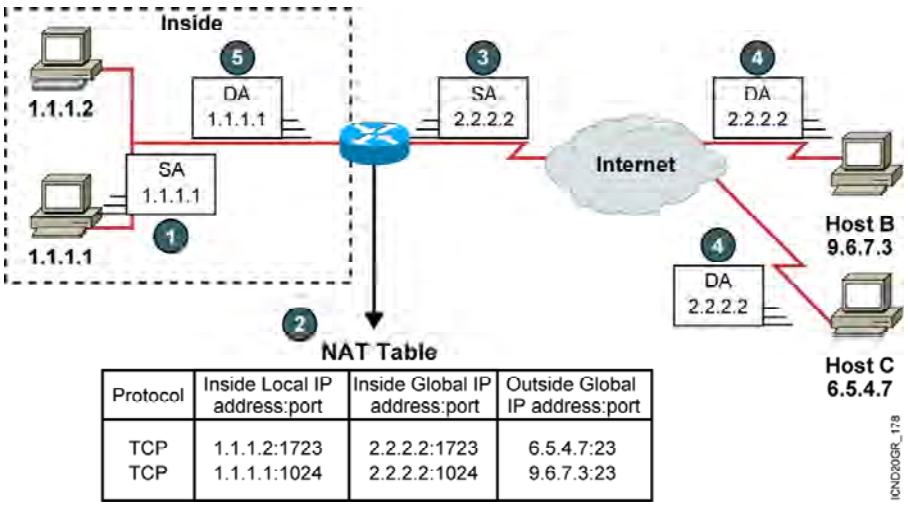


راه اندازی Dynamic NAT در یک مثال :

این مثال نمونه ای از راه اندازی Dynamic NAT روی NAT Router می باشد .
در این مثال آدرسهایی که در رنج 192.168.1.0 /24 قرار دارند همگی Invalid باشند. بنابراین لیستی از آدرسهای Invalid ایی که می خواهیم قادر به ارتباط با اینترنت باشند را به کمک Access List مشخص می کنیم .
از طرفی در این مثال ما رنجی از آدرسهای رجیستر شده ای را داریم که آنها را با یک Pool معرفی می کنیم .
بعد از ساختن Access List و Pool نوبت به برقراری ارتباط بین این دو دسته می رسد .
بنابراین از این به بعد آدرسهایی که در Access List قرارداشته باشند به آدرسهای درون Pool ترجمه شده و قادر به ارتباط با شبکه های Outside خواهند شد.

Overloading an Inside Global Address

Cisco.com



Protocol	Inside Local IP address:port	Inside Global IP address:port	Outside Global IP address:port
TCP	1.1.1.2:1723	2.2.2.2:1723	6.5.4.7:23
TCP	1.1.1.1:1024	2.2.2.2:1024	9.6.7.3:23

Dynamic NAT With Overload :

این روش همانند روش Dynamic NAT است ، با این تفاوت که ترجمه بین آدرسهای Invalid فقط با یک آدرس Valid صورت می گیرد.بنابراین مشخصه دیگری وجود دارد که منجر به منحصر به فرد شدن آدرسهای ترجمه شده می شود.
این مشخصه همان Port می باشد. بنابراینPAT یا همان Port Address Translation مکانیزمی است که در آن تفکیک آدرسها به کمک پورتهای مختلف صورت می گیرد.

بنابراین دراین حالت آدرسهای Invalid به یک آدرس Valid ترجمه می شوند اما Nat Router برای هر کدام از آدرسهای Invalid یک پورت جداگانه باز می کند . درنتیجه تمایز بین آدرسها به کمک شماره پورت ها صورت می گیرد.
NAT Table علاوه به IP Address شامل شماره پورت نیز می باشد . بنابراین پکتی که توسط روتر NAT دریافت می شود ، پروتکل و IP Address آن بررسی شده و درصورتی که رکوردی متناظر با این آدرس و پروتکل مربوطه موجود باشد از آن استفاده می کند و عملیات ترجمه صورت می گیرد . اما درصورتی که چنین نباشد یعنی درصورتی که آدرس مبداء پکت دریافت شده متناظر با آدرسهای Inside Local موجود در NAT Table نباشد و یا حتی در صورت موجود بودن ، پروتکل آنها یکسان نباشد ، در این صورت رکورد جدید تلقی شده و در NAT Table درج خواهد شد .

Configuring Overloading

Cisco.com

```
Router(config)#access-list access-list-number permit
source source-wildcard
```

- **Defines a standard IP access list permitting those inside local addresses that are to be translated**

```
Router(config)#ip nat inside source list
access-list-number interface interface overload
```

- **Establishes dynamic source translation, specifying the access list defined in the prior step**

پیکربندی Dynamic NAT With Overload :

این تنظیم شامل چهار مرحله می باشد :

۱. معرفی لیستی از آدرسهای Invalid یا همان Inside Local Address
۲. فعال کردن Dynamic NAT With Overload
۳. تعیین Inside Interface
۴. تعیین Outside Interface

معرفی لیستی از آدرسهای Invalid یا همان Inside Local Address :

در این مرحله لیستی از آدرسهای Invalid را که می خواهید در عملیات ترجمه شرکت کرده و قادر به ارسال پکت به شبکه اینترنت باشند را به کمک Access List معرفی می کنید .

فعال کردن Dynamic NAT With Overload :

این مرحله شامل فعال کردن Dynamic NAT و برقراری ارتباط بین Access List با تک آدرس رجیستر شده می باشد.
برای این منظور وارد Global Mode شده و فرمان زیر را وارد می کنید .

Router(config)#ip nat inside source
List access-list-number interface interface overload

این فرمان ارتباط بین Access List با اینترفیسی از روتر که روی آن آدرس رجیستر شده تنظیم شده است را برقرار می کند. درواقع در این حالت Inside Global Address همان Inside Interface می باشد .

تعیین Inside Interface :

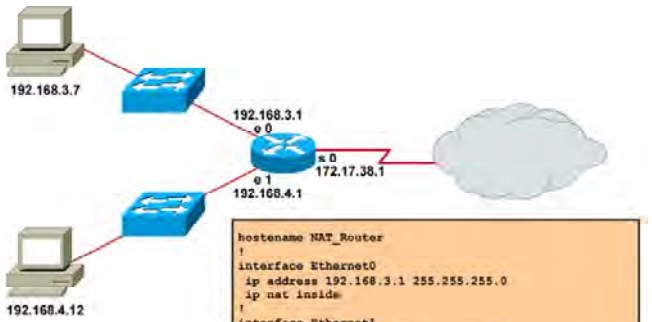
در این مرحله اینترفیسی از NAT Router که در ناحیه Inside قراردارد را انتخاب کرده و به کمک فرمان زیر آن را به عنوان Inside Interface انتخاب می کنیم .

Router(config-if)#ip nat inside

تعیین Outside Interface :

در این مرحله اینترفیسی از NAT Router که در ناحیه Outside قراردارد را انتخاب کرده و به کمک فرمان زیر آن را به عنوان Outside Interface انتخاب می کنیم .
Router(config-if)#ip nat outside

Overloading an Inside Global Address Example




```
hostname NAT_Router
!
interface Ethernet0
 ip address 192.168.3.1 255.255.255.0
 ip nat inside
!
interface Ethernet1
 ip address 192.168.4.1 255.255.255.0
 ip nat inside
!
interface Serial0
 description To ISP
 ip address 172.17.38.1 255.255.255.0
 ip nat outside
!
ip nat inside source list 1 interface Serial0 overload
!
ip route 0.0.0.0 0.0.0.0 Serial0
!
access-list 1 permit 192.168.3.0 0.0.0.255
access-list 1 permit 192.168.4.0 0.0.0.255
!
```

راه اندازی Dynamic NAT with Overload در یک مثال :

این مثال نمونه ای از راه اندازی Dynamic NAT with Overload روی NAT Router می باشد .
دسته ای از آدرسهای Invalid ایی که نیاز به ارتباط با اینترنت را دارند به کمک Access List مشخص کرده و به کمک فرمان IP Nat Inside به آدرس Valid منسوب می شوند.
بنابراین تمایز بین آدرس های Invalid به کمک شماره پورت های مختلف صورت می گیرد .
فرض کنید شما با کامپیوتری با آدرس 192.168.4.12 در Inside Network و روتری با آدرس 10.10.10.1 در Outside Network قرار داشته باشد و شما به ترتیب به این آدرس ping و Telnet می کنید .
برای شروع آدرس 10.10.10.1 را ping می کنید ، بنابراین ICMP Request ها به سمت روتر NAT هدایت می شود و روتر NAT آنها را دریافت کرده و می بایست با یک عملیات ترجمه آن را به سمت Outside Network هدایت کند . بنابراین NAT Router رکوردی را در NAT Table درج می کند اما در این رکورد اطلاعات پروتکل مربوطه نیز درج می شود . از آنجایی که ping براساس پروتکل ICMP می باشد بنابراین آدرس های Inside و Outside به همراه فیلد پروتکل در NAT Table درج می شود.
حال به آن روتر Telnet می کنیم . در این حالت آدرس مبداء و مقصد تغییری نکرده بلکه فقط پروتکل تغییر کرده است .بنابراین این اطلاعات به همراه پروتکل مربوطه در NAT Table درج خواهد شد . درنتیجه دو رکورد از نظر آدرسهای مبداء و مقصد یکسان هستند و تفاوت آنها در پروتکلی است که کامپیوتر براساس آن اطلاعات را ارسال کرده است . بنابراین به ازای تغییر پروتکل رکورد جدیدی در NAT Table درج خواهد شد.

Clearing the NAT Translation Table

Cisco.com

```
Router#clear ip nat translation *
```

- Clears all dynamic address translation entries

```
Router#clear ip nat translation inside global-ip
local-ip [outside local-ip global-ip]
```

- Clears a simple dynamic translation entry containing an inside translation, or both inside and outside translation

```
Router#clear ip nat translation outside
local-ip global-ip
```

- Clears a simple dynamic translation entry containing an outside translation

```
Router#clear ip nat translation protocol inside global-ip
global-port local-ip local-port [outside local-ip
local-port global-ip global-port]
```

- Clears an extended dynamic translation entry

نحوه پاک کردن رکوردهای موجود در NAT Table :

تا به اینجا با نحوه راه اندازی NAT روی روترهای سیسکو آشنا شدید . بعد از راه اندازی NAT ، NAT Table یا به صورت Static و یا به صورت Dynamic تکمیل می شود.
اما رکوردهای این Table را می توان به صورت دستی پاک کرد . برای این منظور فرمان Clear ip nat را در User Mode به صورتهای زیر به کار می بریم :

Router#clear ip nat translation *

با به کار بردن این فرمان تمامی رکوردهای موجود در NAT Table بدون غیر فعال شدن عملکردNAT پاک می شود .

**Router#clear ip nat translation inside global-ip
local-ip [outside local-ip global-ip]**

با به کار بردن این فرمان می توان یک رکورد از NAT Table را حذف کرد . بنابراین به ترتیب آدرسهای Inside Global و Inside Local را وارد می کنیم.

**Router#clear ip nat translation protocol inside global-ip
global-port local-ip local-port [outside local-ip
local-port global-ip global-port]**

به منظور پاک کردن یک رکورد که به وسیله Dynamic NAT with Overload درون NAT Table درج شده است از این فرمان استفاده می کنیم .

Displaying Information with show Commands

Cisco.com

```
Router#show ip nat translations
```

- **Displays active translations**

```
Router#show ip nat translation
     Pro Inside global      Inside local       Outside local      Outside global
     --- 172.16.131.1        10.10.10.1         ---                ---
```

```
Router#show ip nat statistics
```

- **Displays translation statistics**

```
Router#show ip nat statistics
      Total active translations: 1 (1 static, 0 dynamic; 0 ext nded)
      Outside interfaces:
      Ethernet0, Serial2.7
      Inside interfaces:
      Ethernet1
      Hits: 5  Misses: 0
      …
```

نحوه نمایش اطلاعات مربوط به NAT به کمک فرمان Show :

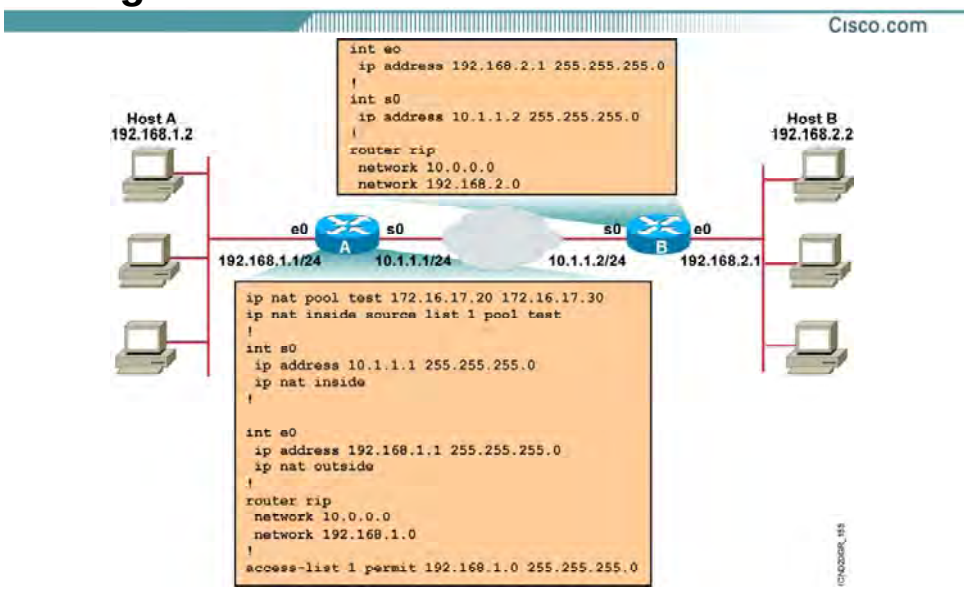
Router#show ip nat translations

به کمک این فرمان می توان رکوردهای موجود در NAT Table و در واقع نحوه ترجمه آدرس ها به یکدیگر را مشاهده کرد.
خروجی این فرمان شامل آدرسهای Inside Local ، Inside Global ، Outside local و Outside Global می باشد.

Router#show ip nat statistics

به کمک این فرمان می توان تعداد رکوردهای موجود در NAT Table و اطلاعات مربوط به اینترفیس های Inside و Outside و همچنین Pool را مشاهده کرد.

Sample Problem: Cannot Ping Remote Host

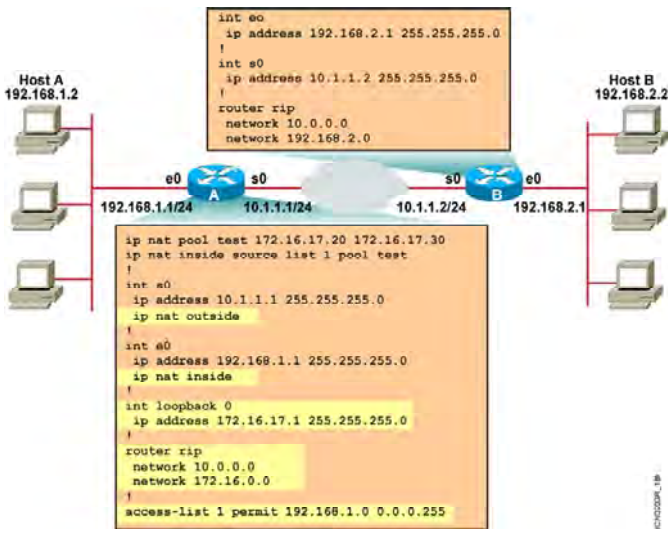


یک مشکل نمونه :

در این مثال روتر A به عنوان NAT Router می باشد ، بنابراین شبکه 192.168.1.0 /24 به عنوان Inside Network و روتر B و شبکه های متصل به آن به عنوان Outside Network درنظر گرفته می شوند .
با توجه به تعریف NAT روی روتر A ، Dynamic NAT به کمک تعریف pool و Access-list می بایست کار ترجمه کردن آدرسها را انجام دهد. اما در عمل اینگونه نیست .Host A واقع در ناحیه Inside قادر به ping کردن Host B واقع در ناحیه outside نمی باشد .
سوالی که پیش می آید اینست که مشکل چیست و چگونه می توان آن را رفع کرد ؟

Solution: New Configuration

Cisco.com



راه حل مشکل :

به تنظیمات موجود روی روتر A که نقش NAT Router را دارا می باشد توجه کنید .
برای رفع مشکل پیش آمده می بایست تنظیم این روتر را به صورت زیر تغییر داد :

۱. تنظیم اینترفیس e0 به عنوان Inside Interface .
۲. تنظیم اینترفیس s0 به عنوان Outside Interface .
۳. Network 172.16.0.0 به عنوان آدرسهای Inside Global توسط pool معرفی شده است در حالی که وجود خارجی نداشته است . بنابراین به وسیله Loop Back این شبکه را معرفی می کنیم .
۴. روتر B در مورد شبکه 172.16.0.0 اطلاعاتی ندارد . درواقع روتر A شبکه 192.168.1.0 را که یک شبکه محلی می باشد را به جای آدرسهای رجیستر شده 172.16.0.0 که می بایست توسط روتر B شناخته شوند Advertise می کند . بنابراین با اصلاح کردن تنظیم پروتکل RIP روی روتر A مشکل حل می شود.

Translation Not Installed in the Translation Table?

Cisco.com

- Verify that:
  - The configuration is correct.
  - There are not any inbound access lists denying the packets from entering the NAT router.
  - The access list referenced by the NAT command is permitting all necessary networks.
  - There are enough addresses in the NAT pool.
  - The router interfaces are appropriately defined as NAT inside or NAT outside.

دلایل عدم رکورد در NAT Table :

درصورتی که با وجود راه اندازی NAT روی یک روتر ، در خروجی فرمان show ip nat translation رکوردی را مشاهده نکردید موارد زیر را بررسی کنید تا به دلیل مشکل پیش آمده پی ببرید:

۱. بررسی کنید که آیا پیکربندی NAT با توجه به نوع آن درست می باشد یا خیر .
۲. درصورت راه اندازی Dynamic NAT و Dynamic Nat with Overload ، بررسی کنید که آیا Access List به درستی ساخته شده است یا خیر .
۳. بررسی صحت درستی آدرسهایی که در pool تعریف شده اند.
۴. بررسی اینکه آیا اینترفیس های Inside و Outside به درستی معرفی شده است یا خیر .

Summary

Cisco.com

- Cisco IOS NAT allows an organization with unregistered private addresses to connect to the Internet by translating those addresses into globally registered IP addresses.
- You can translate your own IP addresses into globally unique IP addresses when communicating outside of your network.
- Overloading is a form of dynamic NAT that maps multiple unregistered IP addresses to a single registered IP address (many-to-one) by using different ports, known also as PAT.
- Once you have configured NAT, verify that it is operating as expected using the clear and show commands.
- Sometimes NAT is blamed for IP connectivity problems when there is actually a routing problem.

خلاصه :

NAT یا همان Network Address Translation مکانیزم ترجمه آدرس می باشد جهت برقراری ارتباط با اینترنت و یا جهت Secure کردن شبکه .
NAT با ترجمه کردن آدرسهای Private به آدرسهای رجیستر شده کار ترجمه را انجام می دهد . این ترجمه می تواند یک به یک و یک به چند باشد . بنابراین می توان با توجه به نحوه ترجمه NAT را به سه دسته کلی تقسیم کرد :

۱. Static NAT
۲. Dynamic NAT
۳. Dynamic NAT With Overload

Static NAT ترجمه یک به یک و دوتای آخر ترجمه یک به چند می باشد . روتر اطلاعات لازم برای Translation را در یک Table نگهداری می کند و ترجمه براساس آن صورت می گیرد . در حالتی که Static NAT استفاده کنیم این Table بدون تغییر باقی می ماند در حالی که اگر از Dynamic NAT و یا Dynamic NAT with Overload استفاده شود این Table تغییر می کند .

فصل ششم :

WAN Connection

این فصل مروری بر مفاهیم اولیه شبکه های گسترده ، ساختارهای ارتباطی و پروتکل های ارتباطی مورد نیاز در آن می باشد .

درس اول :

برقراری یک ارتباط
Point-to-Point
ازطریق اینترفیس Serial

هدف :

این درس شامل :

۱. معرفی شبکه های Leased-Line ، Circuit-switch و Packet-switch .
۲. معرفی پنج استاندارد برای اینترفیس سریال که توسط تجهیزات سیسکو ساپورت می شود .

WAN Overview

Cisco.com

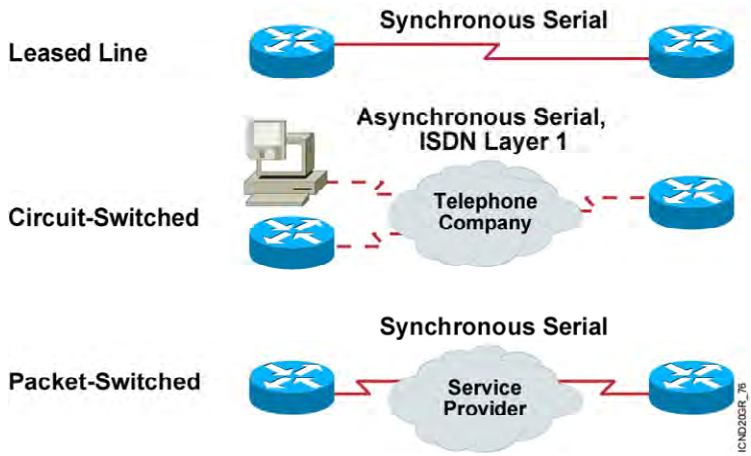
- **WANs connect remote sites.**
- **Connection requirements vary depending on user requirements, cost, and availability.**

بررسی شبکه WAN :

شبکه WAN مجموعه ای از شبکه های محلی گسسته ای است که توسط یک بستر ارتباطی به یکدیگر مرتبط می شوند .
فرض کنید یک شرکت دارای دو ساختمان در منطقه جغرافیایی متفاوت به طور مثال در دو شهر مختلف باشند ، برای برقراری ارتباط این دو ساختمان و یا به عبارتی دو شبکه LAN می بایست ازسرویسهای استفاده کرد که این کار را برای ما انجام دهد .
با این تفکر نیاز به یک service Provide خواهد بود که این بستر ارتباطی بین دو شبکه LAN را فراهم کند .
بنابراین قسمتی از این شبکه تحت مدیریت شما نخواهد بود و شما فقط دریافت کننده سرویس ارائه شده توسط Service Provider خواهید بود .
دربعضی از مواقع شما به عنوان یک Customer نیاز به یک ارتباط امن دارید . بنابراینService Provider به عنوان فراهم کننده یک ارتباط VPN همچون یک خط Leased Line می تواند برقرار کننده یک ارتباط امن بین نقاط مورد نظرتان باشد.

WAN Connection Types: Layer 1

Cisco.com



انواع ارتباطات :

سرویسهایی که توسط Service Provider ارائه می شود را می توان به سه دسته کلی زیر تقسیم بندی کرد :

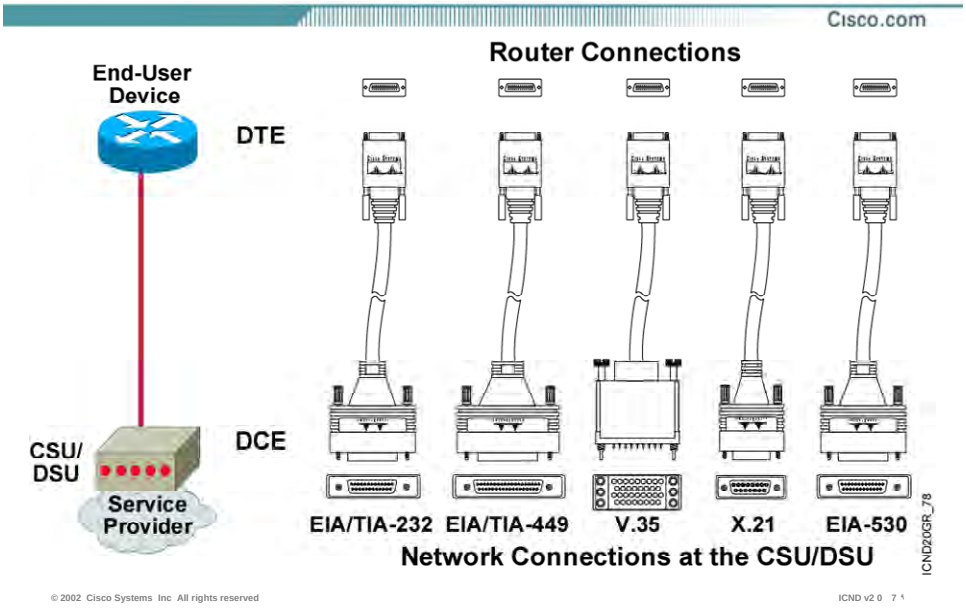
۱. Leased Line
۲. Circuit-Switched
۳. Packet-Switched

Leased Line :
عبارتنداز یک ارتباط نقطه به نقطه و مستقیم که توسط Service Provider ارائه می شود . Leased Line ارتباطی است که همواره برقرار می باشد و با مشخص بودن دو سر آن به عنوان یک ارتباط اختصاصی به عنوان یک ارتباط Secure توسط Service Provider ارائه می شود .
پهنای باند این ارتباط می تواند تا 45 Mbps باشد .

Circuit-Switched :
در این روش همانطور که از نامش پیداست یک مدار مجازی بین دو Station نهایی تعریف می شود .
در سوئیچینگ مداری ابتدا ارتباط بین دو Station نهایی برقرار شده و سپس اطلاعات منتقل می شود .
نمونه شبکه سوئیچینگ مداری ، شبکه تلفن می باشد . در این شبکه بعد از برقراری ارتباط بین دو نقطه نهایی ، یک ارتباطی فیزیکی برقرار شده و طرفین می توانند به مکالمه و یا حتی انتقال دیتا بپردازند و تا زمانی که طرفین به صورت کامل این ارتباط را قطع نکنند این مدار آزاد نخواهد شد .
بنابراین می توان گفت که یکی از نقاط ضعف سوئیچینگ مداری ، اشغال کانال های فیزیکی حتی در زمانی که هیچ گونه اطلاعاتی ردوبدل نمی شود، است .
این بدان معنی است که با محدود بودن ظرفیت سوئیچینگ و با اشغال شدن یک کانال، حتی اگر طرفین برای مدتی انتقال سیگنال نداشته باشند کانال اشغال خواهد ماند . شبکه تلفن معمولی و شبکه ISDN نمونه ای از سوئیچینگ مداری هستند .

Packet-Switched:
در این روش برخلاف سوئیچینگ مداری ، مداری بین دو Station نهایی برقرار نمی شود ، بلکه در این روش اطلاعات به بسته های کوچکی تقسیم شده و به همراه یکسری اطلاعات کنترلی به شبکه سوئیچینگ پکتی تحویل داده می شود . بنابراین سوئیچ های مختلف با در نظر گرفتن بهترین مسیر پکت را هدایت کرده و به مقصد می رسانند . لذا در این روش منابع شبکه درگیر برقراری یک مدار دائمی بین دو Station نهایی نخواهند شد.
برای نمونه می توان شبکه های Frame-relay و X.25 را به عنوان شبکه سوئیچینگ پکتی معرفی کرد.

Serial Point-to-Point Connections



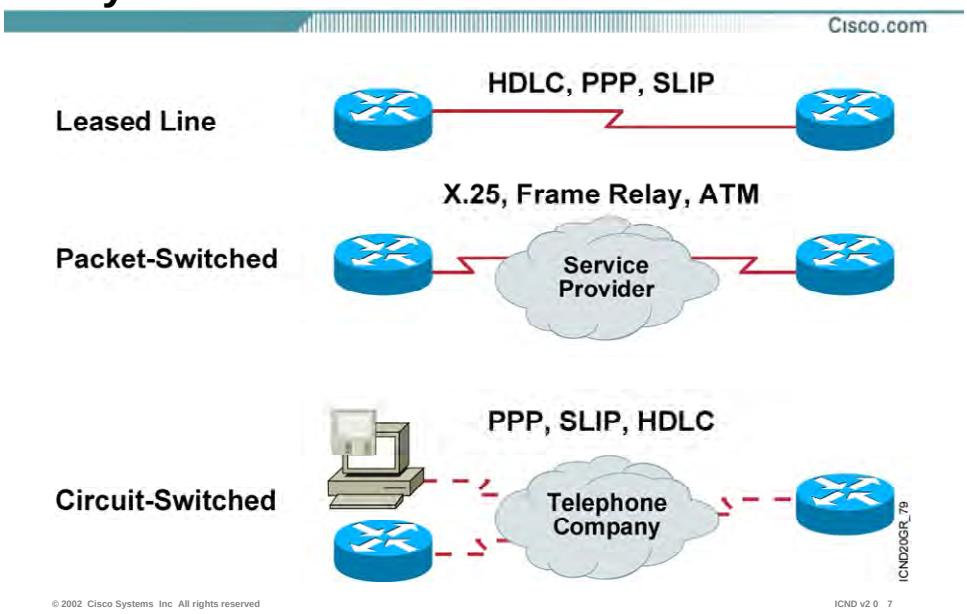
اینترفیس Serial :

اینترفیس Serial ، اینترفیسی است که در آن انتقال دیتا به صورت متوالی (Serial) صورت می گیرد . این بدان معنی است که در هر زمان یک المان سیگنال روی کانال ارتباطی ارسال می شود ، بنابراین بیتهای دیتا پشت سر هم روی خط حرکت خواهند کرد .
روترهای سیسکو استانداردهای زیر را برای اینترفیس Serial ساپورت می کنند :

- EIA/TIA-232
- EIA/TIA-449
- V.35
- X.21
- EIA-530

اینترفیس Serial که به آن اینترفیس WAN نیز گفته می شود یک پورت 60 Pin می باشد (DB-60) و به آن یک کانکتور DB-60 متصل می شود .
درصورت ارتباط روتر با شبکه WAN می بایست از کابلی استفاده شود که از یک سو دارای کانکتور DB-60 باشد که به اینترفیس Serial روتر متصل شود و از سوی دیگر می توان با توجه به سرویسی که استفاده می شود کانکتور مشخصی داده باشد .
همانطور که در شکل مشاهده می کنید CSU/DSU و یا مودم به عنوان سخت افزاری است که دیتای دریافتی از روتر را قابل ارسال به شبکه WAN می کند .
در انتقال سریال دیتا می بایست سرعت انتقال دیتا در اینترفیس سریال گیرنده و فرستند یکسان باشد. درواقع می بایست Clock Rate یا همان نرخ ارسال دیتا در اینترفیس سریال فرستنده و گیرنده یکسان باشد .
DTE یا همان Data terminal equipment ، که در این شکل روتر درنظر گرفته شده است ، نیاز به تعیین Clock Rate از سوی مودم و یا CSU/DSU دارد تا سرعت ارسال دیتا براساس نرخ مشخص شده باشد .
DCE یا همان Data Circuit terminating که معمولا یک مودم و یا یک CSU/DSU می باشد وظیفه تبدیل اطلاعات دریافتی از یک DTE به فرمت قابل قبول شبکه WAN را به عهده دارد و از طرفی DCE وظیفه تعیین Clock Rate را به عهده دارد .
بنابراین اینترفیس های Serial می توانند نقش DTE و یا DCE را داشته باشند ، به طور مثال در استاندارد EIA/TIA-530 روتر فقط می تواند DTE باشد .

Typical WAN Encapsulation Protocols: Layer 2



بررسی پروتکلهای WAN در لایه دوم :

همانطور که می دانید در شبکه Ethernet دیتا به صورت فریم های Ethernet بسته بندی شده و سپس در اختیار لایه فیزیکی قرار داده می شود . در شبکه WAN نیز قبل از اینکه اطلاعات تحویل بستر ارتباطی WAN شود ،در فریم های مشخصی بسته بندی می شود .
پروتکلهای لایه دوم در شبکه WAN نحوه این بسته بندی را مشخص می کنند . با توجه به سرویس و استانداردی که استفاده می شود پروتکلهای لایه دوم خاصی می بایست استفاده کرد .
همانطور که در شکل مشاهده می کنید متناسب به انواع شبکه های WAN ، پروتکل های متفاوتی به منظور بسته بندی اطلاعات استفاده می شود .
در ادامه این فصل با پروتکلهای PPP ، HDLC آشنا خواهید شد .

Summary

Cisco.com

- A WAN makes data connections across a broad geographic area so that information can be exchanged between distant sites.
- Some of the WAN connection types available are leased line, circuit-switched, and packet-switched.
- Cisco routers support the EIA/TIA-232, EIA/TIA-449, V.35, X.21, and EIA/TIA-530 standards for serial connections.
- To encapsulate data for crossing a WAN link, you can choose from a variety of Layer 2 protocols, including HDLC, PPP, SLIP, X.25/LAPB, Frame Relay, and ATM.

خلاصه :

WAN و سرویس های مختص به شبکه WAN به منظور انتقال دیتا و تبادل اطلاعات شبکه های مختلف در ناحیه های مختلف جغرافیایی ، استاندارد و طراحی شده اند .
ارتباطات WAN دارای انواع مختلفی می باشند به طوریکه در یکی از دسته های زیر قرار می گیرند :

- Leased-Line
- Circuit-Switched
- Packet-Switched

براساس دسته بندی فوق ، پروتکل های WAN در لایه دوم نیز طبقه بندی می شوند. به طور مثال پروتکل PPP و HDLC پروتکلهایی هستند که به منظور فریم بندی اطلاعات قبل از تحویل به لایه فیزیکی استفاده می شوند و هر دو جزء پروتکل های دو دسته Leased-Line و Circuit-Switched هستند .

از دید لایه فیزیکی به منظور برقراری ارتباط یک روتر با شبکه WAN ، اینترفیس Serial روتر و یک کابل نیاز می باشد . بنابراین این کابل از یک طرف دارای کانکتور DB-60 به منظور اتصال به روتر و از سوی دیگر با توجه به سرویس WAN ، نوع کانکتور متفاوتی خواهد داشت . روترهای سیسکو پنج استاندارد متفاوت را به منظور ارتباط با شبکه WAN ساپورت می کنند . این پنج استاندارد عبارتنداز :

- EIA/TIA-232
- EIA/TIA-449
- V.35
- X.21
- EIA-530

از آنجایی که اینترفیس Serial دیتا را به صورت متوالی ارسال و دریافت می کنند ، بنابراین می بایست نرخ ارسال و دریافت دیتا بین گیرنده و فرستنده یکسان باشد . لذا Clock Rate با همان نرخ ارسال اطلاعات در واحد زمان توسط یکی از طرفین تعیین می شود . در ارتباطات سریال Clock Rate توسط DCE تعیین می شود ، و این DTE می باشد که Clock Rate مشخص شده را پذیرفته و با آن دیتا را ارسال و دریافت می کند .

درس دوم :

PPP و HDLC

هدف :

این درس شامل :

۹. معرفی پورتکل های PPP و HDLC به عنوان پروتکل های مربوط به ارتباط Leased-Line .
۱۰. تنظیم پروتکلهای PPP و HDLC روی روترهای سیسکو و استفاده از فرمان show و Debug جهت بررسی نحوه کارکرد آنها .

HDLC Frame Format

Cisco.com

Cisco HDLC

- **Uses a proprietary data field to support multiprotocol environments**

Standard HDLC

ICND2_GR_283

- **Supports only single-protocol environments**

پروتکل HDLC و بررسی فریم آن :

High-Level Data Link Control یا همان HDLC پروتکل لایه دوم برای بسته بندی دیتا جهت ارسال توسط اینترفیس Serial می باشد .
این پروتکل توسط مرکز استاندارد جهانی (ISO) به عنوان یک پروتکل لایه دوم و بسته بندی دیتا روی اینترفیس Serial استاندارد شده است .
HDLC دارای دو فرمت زیر می باشد :

- Cisco HDLC
- Standard HDLC

Standard HDLC :
این نسخه فقط توانایی هدایت و کپسوله کردن یک پروتکل از لایه سوم را به عهده دارد و این به دلیل اینست که فیلدی که بتواند پروتکل های مختلف را تفکیک کند ،ندارد .
Cisco HDLC:
نسخه اختصاصی Cisco به طوری که توانایی کپسوله کردن چندین پروتکل لایه Network را توسط اینترفیس سریال به عهده دارد .
فیلد Proprietary امکان کپسوله کردن و تفکیک چندین پروتکل لایه Network توسط فریم HDLC را فراهم می کند .

Configuring HDLC Encapsulation

Cisco.com

```
Router(config-if)#encapsulation hdlc
```

- **Enables HDLC encapsulation**
- **Uses the default encapsulation on synchronous serial interfaces**

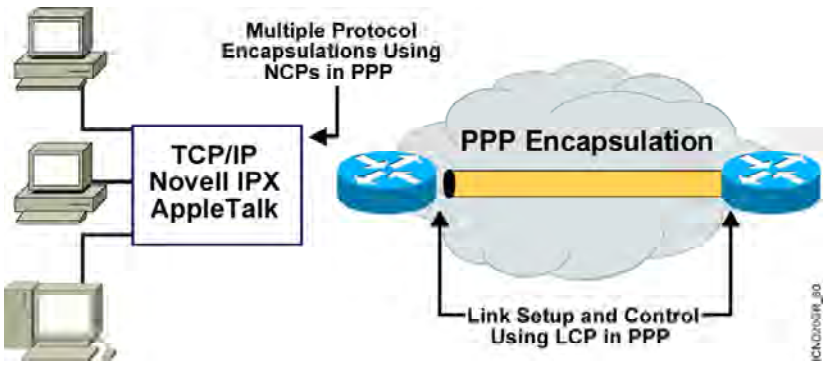
پیکربندی پروتکل HDLC :

پروتکل HDLC به صورت پیش فرض روی اینترفیس های Serial در تجهیزات سیسکو فعال می باشد .
همانطور که می دانید پروتکل HDLC به عنوان پروتکل لایه دوم برروی خطوط Leased-Line به کار گرفته می شود . بنابراین درصورتی که در دو سر این کانال ارتباطی تجهیزات سیسکو مورد استفاده قرار گیرد ، این پروتکل به منظور کپسوله کردن دیتا استفاده خواهد شد . درحالی که اگر هر دو سوی این کانال تجهیزات سیسکو استفاده نشود می بایست از پروتکل PPP به عنوان پروتکل لایه دوم استفاده کرد .
برای تعریف پروتکل HDLC روی اینترفیس Serial ، ابتدا وارد Mode مربوط به اینترفیس Serial شده و سپس فرمان زیر را وارد می کنید :

Router(config-if)#encapsulation hdlc

An Overview of PPP

Cisco.com



- **PPP can carry packets from several protocol suites using NCP.**
- **PPP controls the setup of several link options using LCP.**

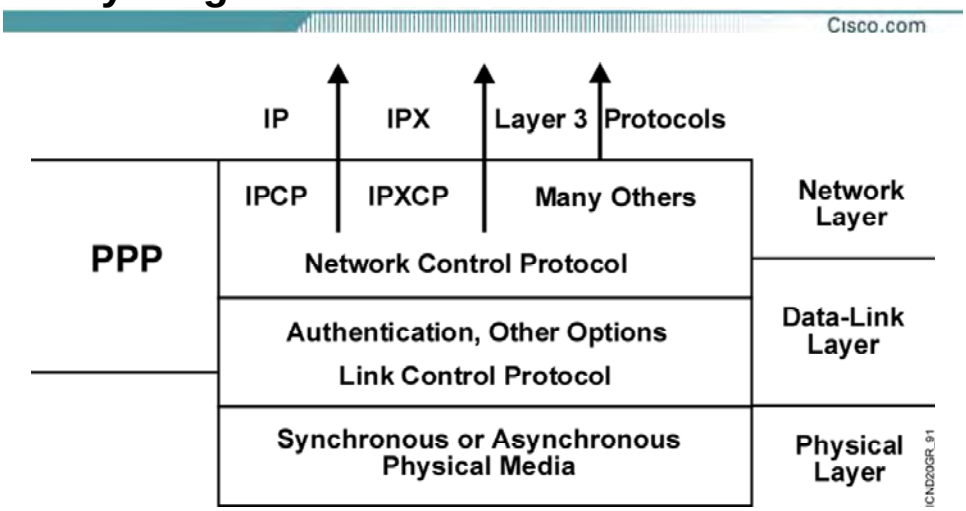
مروری بر پروتکل PPP :

PPP به منظور کپسوله کردن اطلاعات لایه Network به منظور انتقال روی یک ارتباط نقطه به نقطه استاندارد شده است .
پروتکل PPP از یک معماری چند لایه ای تبعیت می کند . این پروتکل دارای زیر لایه های NCP و LCP می باشد .

NCP (Network Control Protocol):
این زیرلایه وظیفه کپسوله کردن پروتکلهای مختلف لایه Network و سپس تفکیک هر کدام از آنها را به عهده دارد . به طور مثال کپسوله کردن پروتکلهای IPX ، IP ، AppleTalk .

LCP (Link Control Protocol):
وظیفه کنترلی ، شامل برقراری و حفظ ارتباط روی یک لینک Point-to-point را به عهده دارد . در ادامه با ویژگی های مختلف این زیر لایه بیشتر آشنا خواهید شد .

Layering PPP Elements



PPP: A data link with network layer services •

اجزای پروتکل لایه ای PPP :

همانطور که گفته شد پروتکل PPP ، پروتکل لایه دوم ایی می باشد که در لایه Network نیز فعالیت می کند .
PPP دارای سرویسهایی برای کنترل Data Link می باشد که جزء Option های زیرلایه LCP است .
از طرفی پروتکل PPP توانایی کپسوله کردن پکتهایی از پروتکل های متفاوت به کمک زیر لایه NCP را دارا است.

PPP LCP Configuration Options

Cisco.com

Feature	How It Operates	Protocol
Authentication	Requires a password Performs challenge handshake	PAP CHAP
Compression	Compresses data at source; reproduces data at destination	Stacker or Predictor
Error Detection	Monitors data dropped on link Avoids frame looping	Quality Magic Number
Multilink	Load-balances across multiple links	Multilink Protocol (MP)

ICND2GR_90

گزینه های زیرلایه LCP از پروتکل PPP :

همانطور که تا به اینجا گفته شد ، زیر لایه LCP دارای ویژگی کنترلی می باشد و این کار توسط گزینه های زیر امکان پذیر می باشد :

Authentication :
بررسی مجوز برقراری ارتباط لایه دوم در دو سر لینک . به طور مثال در یک ارتباط نقطه به نقطه مانند Leased-Line که دو روتر در دو سر آن واقع شده است ارتباط لایه دوم زمانی برقرار می شود که طرفین مجوز برقراری ارتباط را بررسی کرده باشند .
تآیید اعتبار توسط پروتکل PPP به دو فرمت امکان پذیر است :

- PAP (Password Authentication Protocol)
- CHAP (Challenge Handshake Authentication Protocol)

در زیرلایه LCP مشخص می شود که طرفین با چه متدی عملیات Authentication را انجام می دهند .

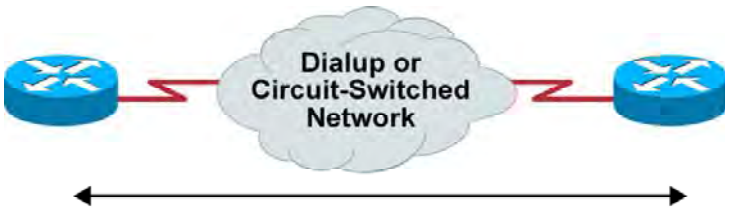
Compression:
این گزینه وظیفه فشرده کردن دیتا در مبداء و خارج کردن از حالت فشردگی در مقصد را به عهده دارد . این ویژگی به منظور افزایش ظرفیت یک لینک PPP به کار برده می شود .

Error Detection:
مکانیسمی به منظور کشف خطا و جلوگیری از وقوع Loop می باشد که توسط پروتکل های Magic Number و Quality صورت می پذیرد .

Multilink:
به کمک این ویژگی اینترفیسهایی از روتر که PPP روی آنها فعال باشد می توانند در Balance کردن پکتها روی Link های متفاوت نقش داشته باشند .

PPP Session Establishment

Cisco.com



PPP Session Establishment

1. Link Establishment Phase
2. Authentication Phase (Optional)
3. Network Layer Protocol Phase

ICND20GR_81

- **Two PPP authentication protocols: PAP and CHAP**

برقراری یک PPP Session بین دو نقطه :

برقراری نشست PPP در سه مرحله صورت می پذیرد :

۱. Link Establishment
۲. Authentication
۳. Network Layer Protocol

Link Establishment:

در این مرحله اینترفیسی که پروتکل PPP روی آن تنظیم شده و درخواست برای برقراری ارتباط دارد ، درخواستی را برای تنظیم و تست Link به طرف دیگر ارسال می کند
این درخواست شامل اطلاعاتی درمورد مکانیزم Authentication و فشرده سازی و ماکزیمم سایز فریم ها است .

Authentication:

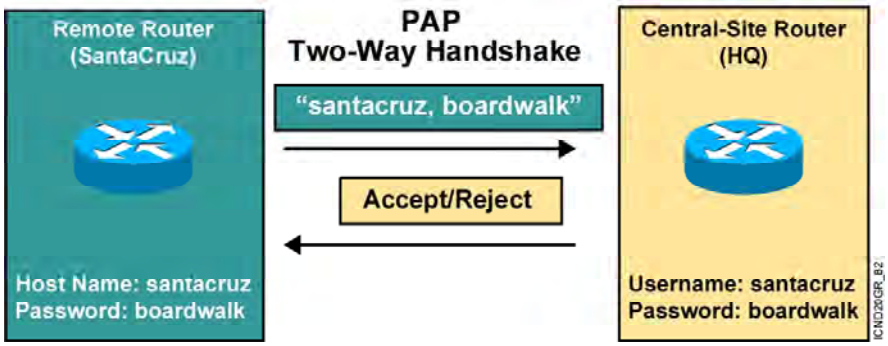
بعد از برقراری Link و مشخص شدن نوع پروتکل Authentication توسط زیرلایه LCP نوبت به تأیید اعتبار می رسد .
PPP دو متد برای تأیید اعتبار معرفی می کند : PAP و CHAP .
در ادامه با این دو متد بیشتر آشنا خواهید شد .

Network Layer Protocol:

بعد از اینکه تأیید اعتبار صورت گرفت در این مرحله پکتهای NCP ارسال شده تا مشخص شود یک یا چند پروتکل لایه Network و کدام ها می بایست به انتقال پکتهایشان بپردازند . به طور مثال بعد از اینکه پروتکل IP به عنوان پروتکل لایه Network مشخص شد ، طرفین می توانند پکتهای IP خود را روی Link برقرار شده ارسال کنند .

PPP Authentication Protocols

Cisco.com



- **Passwords sent in clear text**
- **Peer in control of attempts**

پروتکلهای تأیید اعتبار در PPP :

همانطور که گفته شد دو متد و درواقع دو پروتکل وظیفه تأیید اعتبار در PPP را به عهده دارند .
تآیید اعتبار توسط پروتکل PPP به دو فرمت امکان پذیر می باشد :

- PAP (Password Authentication Protocol)
- CHAP (Challenge Handshake Authentication Protocol)

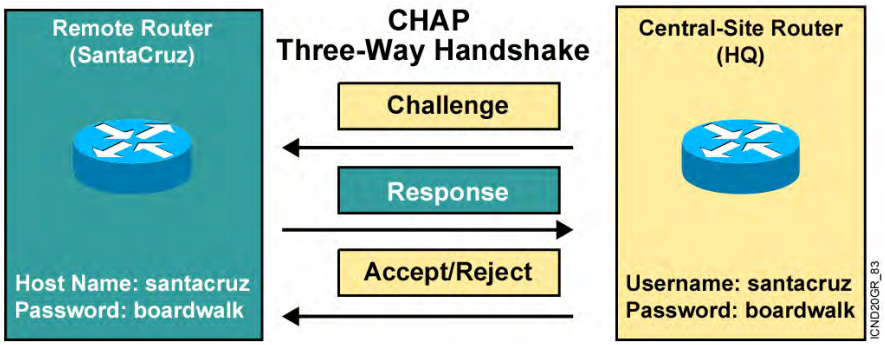
بنابراین زمانی که شما پروتکل PPP را انتخاب می کنید ، می بایست مشخص کنید از چه متدی برای تأیید اعتبار استفاده خواهید کرد .
در ادامه با هر دو متد و نحوه تنظیم آنها روی اینترفیس های Serial یک روتر آشنا خواهید شد .

PAP:

بعد از اینکه فاز اول PPP ، یعنی برقراری ارتباط براساس لایه دوم صورت پذیرفت می بایست Authentication صورت گیرد . PAP متدی است که عملیات تأیید اعتبار را در دو مرحله انجام می دهد . به علت سادگی این پروتکل پسورد به صورت Clear Text برروی Link ارسال می شود . بنابراین از نظر امنیتی در سطح پایینی عمل می کند . درصورتی که تأیید اعتبار بخواهد به صورت کمی پیچیده تر انجام گیرد نیاز به پردازش بیشتری می باشد و این از سرعت برقراری یک ارتباط می کاهد ، درنتیجه زمانی که در تأیید اعتبار نیازی به دقت بالا نباشد از این متد استفاده می شود .

Challenge Handshake Authentication Protocol

Cisco.com



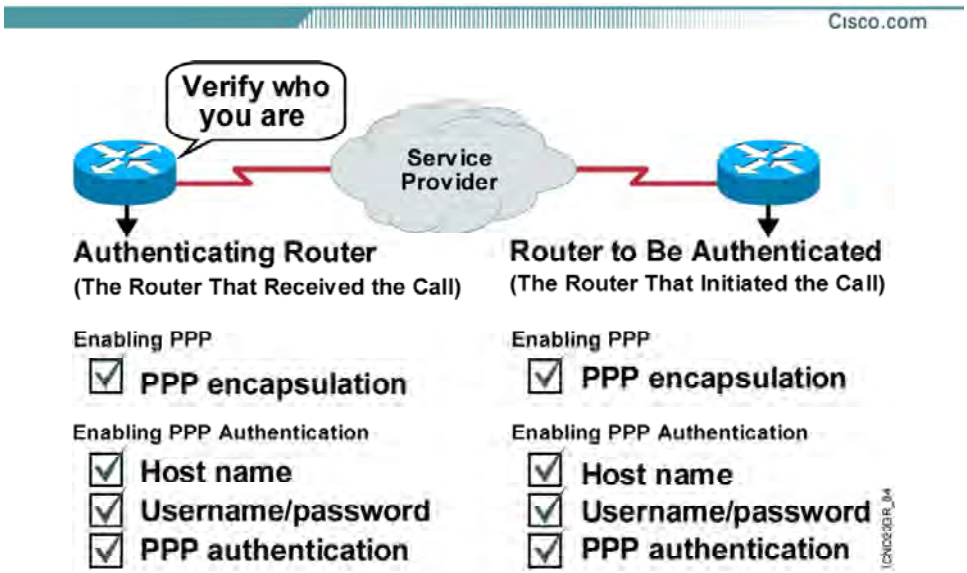
- **Hash values, not actual passwords, are sent across link.**
- **The local router or external server is in control of attempts.**

پروتکلهای تأیید اعتبار در PPP :

CHAP:

پروتکل CHAP از یک مکانیزم سه مرحله ای برای شناخت و تأیید اعتبار استفاده می کند .
گام اول : بعد از مبادله پکتهای LCP و برقراری لینک PPP ، Challenge Message توسط درخواست کننده ارتباط Local Router به Remote Router ارسال می شود .
گام دوم : Remote Router پس از دریافت Message و بعد از به کار بردن الگوریتم MD5 روی پسورد ، مقدار جدید که حاصل الگوریتم MD5 می باشد را با یک Response Message به Local Router ارسال می کند .
گام سوم : Local Router پسوردی که نزد خود داشته است را به کمک الگوریتم MD5 تبدیل به مقداری می کند و سپس مقدار حاصله را با مقدار دریافت شده توسط Response Message مقایسه کرده و درصورت یکسان بودن دو مقدار ، تأیید اعتبار در این ارتباط به Remote Router اطلاع داده می شود.

Configuring PPP and Authentication Overview



مروری بر مراحل تنظیم کردن PPP روی یک لینک نقطه به نقطه :

بعد از اینکه پروتکل PPP به عنوان پروتکل لینک Point-to-Point انتخاب شد ، می بایست آن را روی اینترفیس مربوطه فعال کرد . به کمک فرمان encapsulation PPP روی اینترفیس Serial پروتکل PPP فعال می شود .
بعد از فعال کردن پروتکل PPP می بایست Authentication و متد مورد نظر انتخاب و سپس تنظیم شود .

Configuring PPP

Cisco.com

```
Router(config-if)#encapsulation ppp
```

- **Enables PPP encapsulation**

نحوه تنظیم پروتکل PPP :

وارد مد اینترفیس شده و فرمان زیر را وارد می کنید :

```
Router(config-if)#encapsulation ppp
```

Configuring PPP Authentication

Cisco.com

```
Router(config)#hostname name
```

- Assigns a host name to your router

```
Router(config)#username name password password
```

- Identifies the username and password of remote router

```
Router(config-if)#ppp authentication
{chap | chap pap | pap chap | pap}
```

- Enables PAP and/or CHAP authentication

نحوه تنظیم Authentication در پروتکل PPP :

پس از فعال شدن پروتکل PPP روی اینترفیس Serial می بایست Authentication و متد مورد نظر را روی اینترفیس serial فعال کرد .

- مشخص کردن یک نام برای روتر .

Router(config)#hostname *name*

- مشخص کردن Username و Password .

نکته :در تنظیم Authenticatin روی یک لینک نقطه به نقطه ، می بایست Username نام روتر طرف مقابل و پسورد روی هر دو روتر یکسان باشد .

Router(config)#username *name* password *password*

- تعیین نوع پروتکل Authentication ، به عبارتی مشخص کردن PAP یا CHAP .

Router(config-if)#ppp authentication{chap | chap pap | pap chap | pap}

CHAP Configuration Example

Cisco.com


```
hostname left
username right password sameone
!
int serial 0
 ip address 10.0.1.1 255.255.255.0
 encapsulation ppp
 ppp authentication CHAP
```

```
hostname right
username left password sameone
!
int serial 0
 ip address 10.0.1.2 255.255.255.0
 encapsulation ppp
 ppp authentication CHAP
```

ICND20GR_85

مثالی از تنظیم CHAP :

شکل فوق نحوه تنظیم پروتکل PPP با متد تأیید اعتبار CHAP را نشان می دهد .
در هر دو روتر پس از مشخص شدن Hostname مـی بایـست Username و Password را روی هـر کـدام از روترها مشخص کرد .
Username نام روتر مقابل و پسورد روی هر دو روتر یکسان می باشد .

Verifying the HDLC and PPP Encapsulation Configuration

Cisco.com

```
Router#show interface s0
Serial0 is up, line protocol is up
  Hardware is HD64570
  Internet address is 10.140.1.2/24
  MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec, rely 255/255, load 1/255
  Encapsulation PPP, loopback not set, keepalive set (10 sec)
  LCP Open
  Open: IPCP, CDPCP
  Last input 00:00:05, output 00:00:05, output hang never
  Last clearing of "show interface" counters never
  Queueing strategy: fifo
  Output queue 0/40, 0 drops; input queue 0/75, 0 drops
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     38021 packets input, 5656110 bytes, 0 no buffer
     Received 23488 broadcasts, 0 runts, 0 giants, 0 throttle
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     38097 packets output, 2135697 bytes, 0 underruns
     0 output errors, 0 collisions, 6045 interface resets
     0 output buffer failures, 0 output buffers swapped out
     482 carrier transitions
     DCD=up  DSR=up  DTR=up  RTS=up  CTS=up
```

بررسی عملکرد پروتکل PPP و یا HDLC :

به کمک فرمان show interface می توان نوع پروتکل لایه دوم و متد Authentication که روی آن اینترفیس تنظیم شده است را مشاهده کرد . به کمک این فرمان می توانید State هر کدام از زیرلایه های پروتکل PPP را مشاهده کنید .

Verifying PPP Authentication

Cisco.com


```
Router#debug ppp authentication
4d20h: %LINK-3-UPDOWN: Interface Serial0, changed state to up
4d20h: Se0 PPP: Treating connection as a dedicated line
4d20h: Se0 PPP: Phase is AUTHENTICATING, by both
4d20h: Se0 CHAP: O CHALLENGE id 2 len 28 from "left"
4d20h: Se0 CHAP: I CHALLENGE id 3 len 28 from "right"
4d20h: Se0 CHAP: O RESPONSE id 3 len 28 from "left"
4d20h: Se0 CHAP: I RESPONSE id 2 len 28 from "right"
4d20h: Se0 CHAP: O SUCCESS id 2 len 4
4d20h: Se0 CHAP: I SUCCESS id 3 len 4
4d20h: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0, changed state to up
```

ICND20GR_86

- **debug ppp authentication shows successful CHAP output.**

بررسی عملکرد پروتکل PPP و یا HDLC :

به کمک فرمان debug PPP authentication می توانید فازهای مختلف در برقراری یک نشست PPP را بررسی کنید .

Summary

Cisco.com

- HDLC is the Cisco default data-link layer protocol for encapsulating data on synchronous serial data links.
- PPP encapsulates network layer protocol information over point-to-point links.
- Configurable aspects of PPP include methods of authentication, compression, and error detection, as well as whether or not multilink is supported.
- PPP session establishment progresses through three phases: link establishment, authentication, and network layer protocol.

پروتکل PPP و HDLC به عنوان پروتکل های لایه دوم روی بسترهای ارتباطی WAN استفاده می شوند .
پروتکل Cisco HDLC مخصوص به شرکت سیسکو بوده و روی تجهیزات سیسکو به صورت پیش فرض فعال می باشد .
پروتکل PPP به منظور کپسوله کردن دیتا قبل از تحویل به لایه فیزیکی به کار برده می شود . پروتکل PPP دارای دو زیر لایه LCP و NCP می باشد . LCP دارای وظیفه برقراری و کنترل لینک ارتباطی و NCP وظیفه تعیین پروتکل های لایه Network را دارا می باشد .
پروتکل PPP دارای یک مکانیزم سه مرحله ای می باشد :

- Link Establishment
- Authentication
- Network Layer Protocol

بعد از اینکه نوع پروتکل در زیر لایه NCP مشخص شد ، پکتهای لایه Network روی لینک ارتباطی برقرار شده منتقل خواهند شد .

درس سوم :

Frame Relay

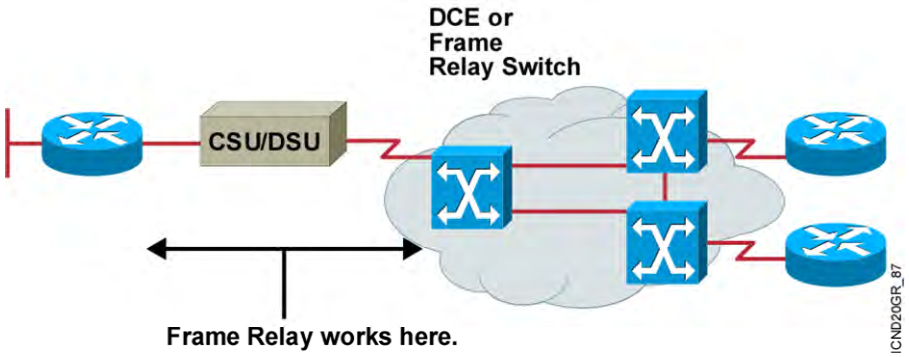
هدف :

این درس شامل :

۳. معرفی ویژگی ها و نحوه عملکرد یک شبکه Frame Relay .
۴. معرفی پارامترهای اصلی Frame Relay .

Frame Relay Overview

Cisco.com

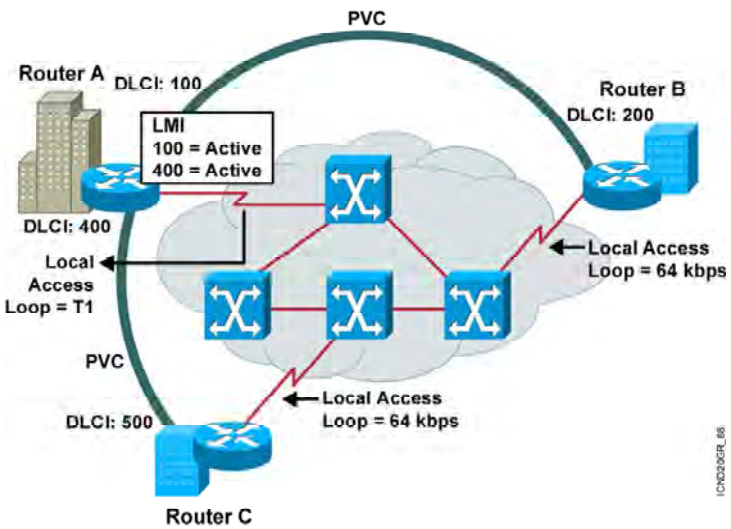


- Connections made by virtual circuits
- Connection-oriented service

مروری بر Frame Relay :

Frame Relay پروتکل لایه Data Link و یک سرویس Connection Oriented (اتصال گرا) می باشد . Frame Relay با تعریف کردن مدار ، ارتباطات منطقی بین نقاط انتهایی برقرار می کنند . بنابراین با این تکنیک از یک کانال فیزیکی می تواند چندین مدار مجازی (VC) عبور داد . هر کدام از این مدارهای مجازی مشخص کننده دو نقطه انتهایی می باشند .
در شبکه Frame Relay هر کدام از نقاط انتهایی به عنوان DTE و سوئیچهای شبکه Frame Relay به عنوان DCE انتخاب می شوند .
بنابراین اینترفیس های Serial به عنوان DTE عمل کرده و با نرخ ارسال اطلاعات که توسط سوئیچ های شبکه Frame Relay تعیین می شود به ارسال دیتا می پردازد.
در شبکه Frame Relay ما با دو دسته مدار بین نقاط انتهایی روبه رو هستیم ، PVC و SVC .
PVC مداری است که همواره برقرار می باشد ، بنابراین می بایست برای برقراری این ارتباط هزینه بیشتری پرداخت کرد ، این درحالی است که مدار SVC ، مداری است که هنگامی که نیاز به برقراری ارتباط باشد فعال می شود .بنابراین از مدارات PVC جهت برقراری ارتباطات سوئیچها در Service Provider و از مدارات SVC جهت ارتباط Customer ها با Service Provider استفاده می شود.

Frame Relay Terminology

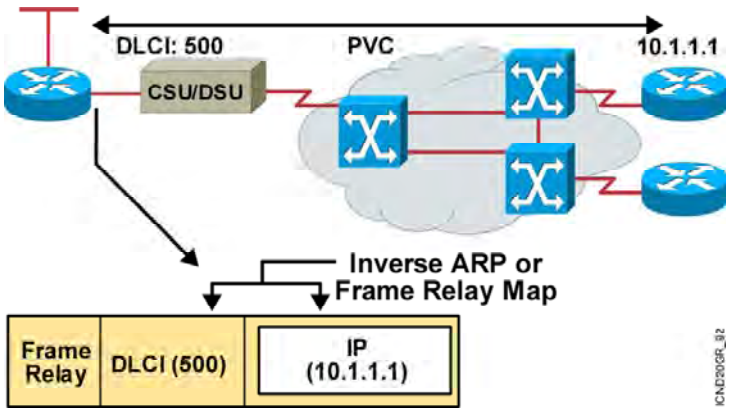


اصطلاحات شبکه Frame Relay :

Local Loop : ارتباط فیزکی بین Customer که می تواند یک تلفن باشد با Service Provider گفته می شود.
VC: در شبکه Frame Relay به مدار مجازی برقرار شده در شبکه Frame Relay گفته می شود.
PVC (Permanent Virtual Circuit): مدار مجازی تعریف شده در شبکه Frame Relay که به طور ثابت و دائمی برقرار است . این مدار بین سوئیچهای شبکه Frame Relay برقرار می شود. درواقع ارتباط بین دو DCE مدار مجازی ثابت خواهد بود.

SVC (Switched Virtual Circuit): مدار مجازی موقت که با برقراری ارتباط ، برقرار و با قطع ارتباط ، قطع می شود . ارتباط بین یک DTE با یک DCE از نوع مدار مجازی موقت می باشد .
DLCI : یک عدد 10 بیتی است که در Header هر فریم Frame Relay قرار گرفته و مشخص کننده مدار مجازی (VC) می باشد.
به طور مثال در شکل فوق روتر A دارای دو مقدار برای DLCI و در نتیجه فراهم کننده دو مدار مجازی (VC) خواهد بود . DLCI با مقدار 400 ، یک مدار مجازی برای ارتباط با روتر C و DLCI با مقدار 100 ، یک مدار مجازی برای ارتباط با روتر B را برقرار می کنند.
LMI (Local Management Interface) : استاندارد سیگنالینگ بین روتر DTE و سوئیچ Frame Relay (DCE) ، به طوریکه روی برقراری و نگهداری یک ارتباط بین روتر و سوئیچ Frame Relay نظارت و مدیریت دارد .

Frame Relay Address Mapping



- **Use LMI to get locally significant DLCI from the Frame Relay switch.**
- **Use Inverse ARP to map the local DLCI to the remote router's network layer address.**

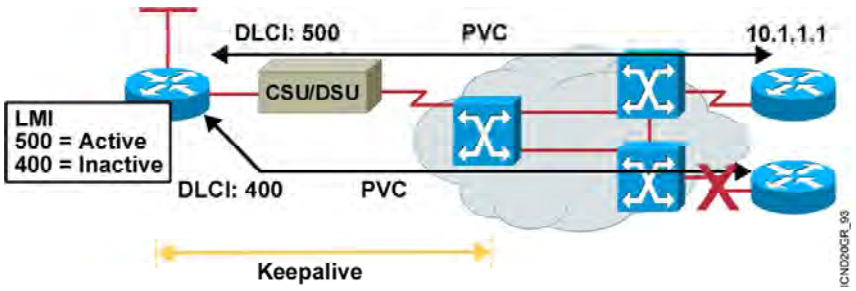
اصطلاحات شبکه Frame Relay :

بعد از مشخص شدن Destination در لایه Network ، اطلاعات تحویل لایه Data Link می شود . از آنجایی که قرار است از سرویس Frame Relay به عنوان پروتکل لایه دوم استفاده شود ، بنابراین می بایست Frame Relay Header به اطلاعات دریافت شده اضافه گردد.
همانطور که می دانید در شبکه Frame Relay بین هر دو DTE یک مدار مجازی تعریف شده است . بنابراین در چنین شبکه ای دانستن فقط آدرس منطقی (IP Address) کافی نیست و نیاز به مشخصه ای داریم که هرکدام از این مدارها را مشخص کند. DLCI عددی است که به هر کدام از VC ها نسبت داده می شود . به شکل فوق توجه کنید . روتر سمت چپ به دو روتر دیگر در سمت راست با تعریف دو مدار مجزا ارتباط برقرار می کند . DLCI با مقدار 500 فقط یکی از این مدارها را مشخص می کند و برای مدار دیگر می بایست DLCI دیگری را برای آن معرفی کنیم .
بنابراین درصورتیکه روتر سمت چپ درخواستی به آدرس 10.1.1.1 داشته باشد ، کافی است آن را تحویل مداری با DLCI(500) قرار دهد ، درواقع مقدار 500 را درون فیلد DLCI قرار دهد .
نکته : DLCI مقداری است که توسط شرکت ارائه دهند سرویس Frame Relay گفته شده و به ازای هر ارتباط Point – to – Point یک شماره DLCI خواهید داشت .

Inverse ARP : عبارتند از عملیات تناظر بین IP Address و شماره DLCI . در شکل فوق آدرس 10.1.1.1 متناظر با DLCI با مقدار 500 می باشد . بنابراین درصورتیکه روتر درخواستی برای آدرس 10.1.1.1 داشته باشد به صورت اتوماتیک عدد 500 در فیلد DLCI در فریم Frame Relay قرار می گیرد.
در Inverse ARP عملیات تناظر به صورت اتوماتیک انجام می گیرد ، می توانید به صورت دستی این تناظر را با تعریف Static Frame Relay map ، درون MAP Table قرار دهید .

Frame Relay Signaling

Cisco.com



- Cisco supports three LMI standards:
  - Cisco
  - ANSI T1.617 Annex D
  - ITU-T Q.933 Annex A

سیگنالهای مورد استفاده از Frame Relay :

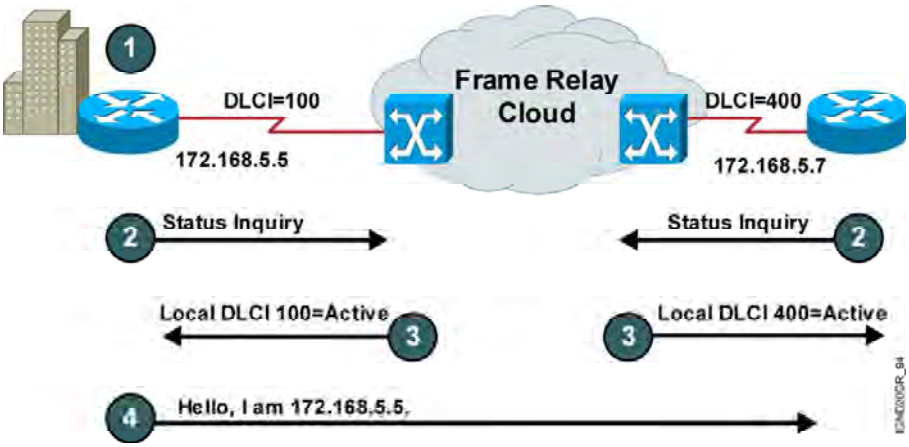
LMI (Local Management Interface) ، سیگنالینگ بین روتر و سوئیچ Frame Relay می باشد به طوریکه هرکدام با ردوبدل کردن LMI Request و LMI Response ، ارتباط را برقرار و آن را مدیریت کرده و به تبادل اطلاعات می پردازند .
سیسکو سه استاندارد زیر را به منظور سیگنالینگ بین روتر و سوئیچ Frame Relay پشتیبانی می کند .

- Cisco
- ANSI
- Q.933

نکته : استاندارد سیگنالینگ بین روتر و سوئیچ Frame Relay می بایست یکسان باشد .

به صورت پیش فرض استاندارد Cisco روی روترهای سیسکو فعال است . درصورتی که از IOS با ورژن 11.1 و به قبل استفاده کنید می بایست LMI Type را برای روتر و اینترفیس مربوطه مشخص کنید ، درحالی که در IOS های ورژن 11.2 به بعد خود روتر، به تنهایی Type مربوط به LMI را به صورت اتوماتیک و با توجه به LMI Type مربوط به سوئیچ Frame Relay که به آن متصل است ، مشخص می کند و نیاز به تنظیم اضافی نمی باشد.

Frame Relay Inverse ARP and LMI Signaling



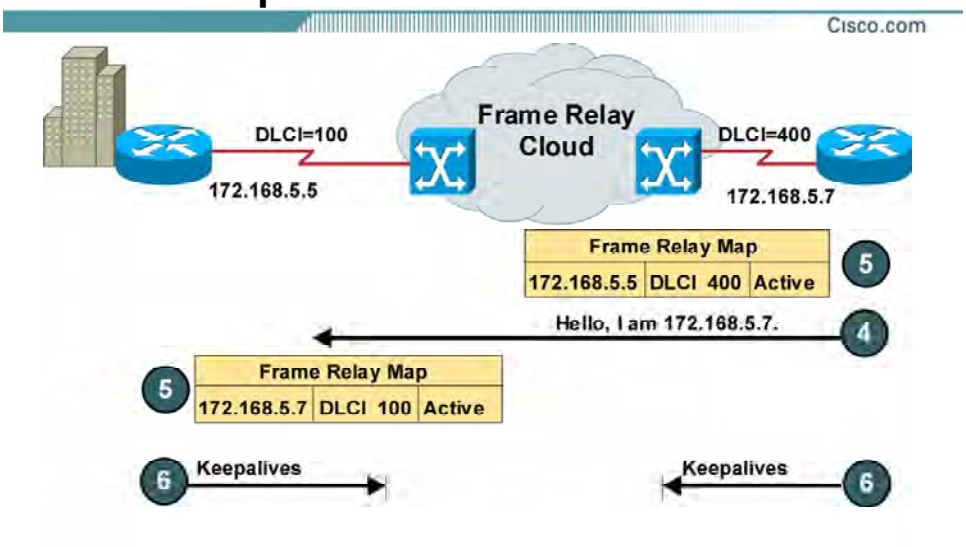
نحوه برقراری یک ارتباط لایه دوم توسط Frame Relay :

شکل فوق مراحل برقراری یک مدار مجازی (VC) بین دو DTE را نشان می دهد .
مرحله ۱ : هر کدام از روتر ها به صورت فیزیکی به یک CSU/DSU به شبکه Frame Relay و درواقع به سوئیچ های Frame Relay متصل شده اند .

مرحله ۲ : هر کدام از روتر ها با فرستادن یک LMI Status Inquiry درخواستی را به سوئیچ Frame Relay ارسال می کنند مبنی بر برقراری یک مدار مجازی .

مرحله ۳ :
سوئیچ Frame Relay پس از دریافت درخواست از DTE ، یک LMI Message از طرف سوئیچ به روتر ارسال می شود که این Message شامل شماره DLCI مربوط به مدارهای مجازی که این روتر با روتر های DTE دیگر برقرار کند می باشد .
به طور مثال در شکل فوق هر کدام از سوئیچ ها Local DLCI مربوط به هر کدام از روترها را در پاسخ به روتر ها اعلام می کنند . بنابراین روتر سمت چپ از این به بعد روتر سمت راست را با DLCI 500 می شناسد ، این شماره Local بوده و مربوط به روتر سمت دیگر نیست ، بلکه مشخص کننده مدار مجازی بین این روتر محلی و روتر سمت دیگر می باشد .
مرحله ۴ :
بعد از اینکه روتر یک LMI Message شامل شماره DLCI خود را از سوئیچ Frame Relay دریافت کرد ، با فرستادن یک پکت Inverse ARP خود را به روتر طرف مقابل معرفی می کند.

Stages of Inverse ARP and LMI Operation



نحوه برقراری یک ارتباط لایه دوم توسط Frame Relay :

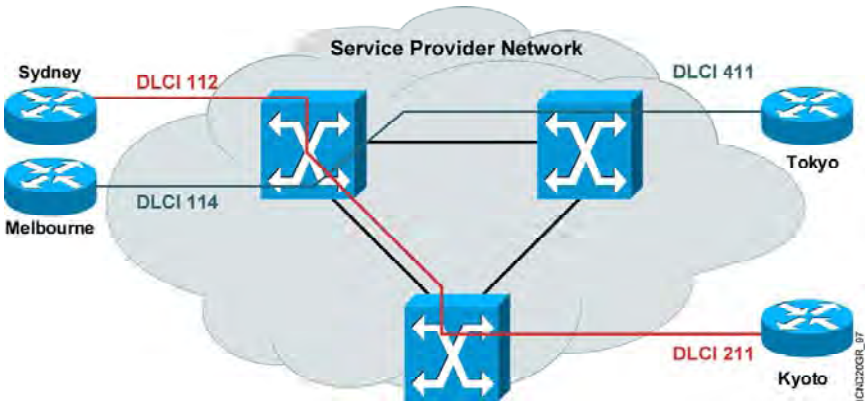
مرحله ۵ :
بعد از اینکه روترها پکتهای Inverse ARP را دریافت کردند ، آن را درون جدول Frame Relay MAP خود وارد می کنند . این جدول شامل ستونهای IP Address و DLCI Number می باشد که در تناظر یک به یک با یکدیگر هستند .
در شکل فوق درصورتی که آدرس مقصد برای پکتی 172.168.5.7 باشد ، در فریم Frame Relay و در فیلد DLCI مقدار 100 قرار می گیرد . DLCI 100 مشخص کننده یک مدار مجازی بین این دو روتر خاص برای روتر سمت چپ می باشد .

مرحله ۶ :
بعد از تکمیل شدن جدول Frame Relay MAP روی هر دو روتر ، یک مدار مجازی بین دو روتر که در دو سر این مدار قرار دارد برقرار می شود .

هر کدام از روتر ها هر ۶۰ ثانیه یک بار پکت Inverse ARP را به تمامی DLCI های فعال ارسال می کنند و از طرفی هر ۱۰ ثانیه یکبار LMI Message بین روتر و سوئیچ Frame Relay ردوبدل می شود .
نکته : در صورتی که Frame Relay MAP به صورت دستی و با Static Frame Relay تعریف شده باشد ، لزوی به ارسال متوالی پکتهای Inverse ARP نخواهد بود و ترافیک اضافی بر لینک ارتباطی تحمیل نخواهد شد .

How Service Providers Map Frame Relay DLCIs: Enterprise View

Cisco.com



هدایت فریم ها در شبکه Frame Relay به کمک DLCI:

همانطور که می دانید در شبکه Frame Relay ، DLCI مشخه ای است که نشان دهنده هر کدام از VC ها است . بنابراین یک روتر می تواند یک یا چند DLCI و متناسب با هر کدام از آنها یک مدار ارتباطی مجازی با روترهای دیگر داشته باشد . بنابراین در دو سر این مدار مجازی و برای هر کدام از روترها یک DLCI به صورت محلی تعریف می شود ، به طوری که هر کدام از آنها به کمک DLCI محلی خود می تواند با طرف مقابل از یک مدار ارتباط برقرار کند .
سوالی که پیش می آید این است که سوئیچ شبکه Frame Relay خود چگونه این مدار را برقرار می کند و انتقال اطلاعات را انجام می دهد؟
این کار در چهار مرحله صورت می گیرد :

- سوئیچ شماره DLCI مربوط به فریم دریافتی را چک می کند .
- سوئیچ شماره DLCI را بررسی می کند به طوری که این شماره متناسب با کدام یک از نقاط انتهایی می باشد .
- با افزودن شماره DLCI مربوطه به این فریم آن را به سمت سوئیچ مورد نظر هدایت می کند . سوئیچ انتهایی با دریافت فریم مربوطه و با توجه به فیلد DLCI ،فریم را تحویل نقطه انتهایی مورد نظر می دهد . بنابراین تبادل اطلاعات در شبکه Frame Relay براساس IP Address نخواهد بود ، بلکه هدایت فریم ها براساس شماره DLCI صورت می گیرد.

نکته : یک پورت سوئیچ Frame Relay و همچنین اینترفیس یک روتر می تواند چند DLCI داشته باشد . به عبارتی با تعریف کردن تعدادی Subinterface روی یک اینترفیس و نسبت دادن هر DLCI به هر کدام از این Subinterface ها می توانید چندین مدار مجازی را روی یک اینترفیس فیزیکی و همچنین روی یک خط ارتباطی داشته باشید .
یکی از توانایی های Frame Realy در این است که می تواند چندین مدار مجازی (VC) را همزمان روی یک کانال ارتباطی هدایت کند (Multiplexing) .

Summary

- Frame Relay is an ITU-T and ANSI standard that defines the process for sending data over a public data network.
- The core aspects of Frame Relay function at the lower two layers of the OSI reference model.
- A Frame Relay connection requires that, on a VC, the local DLCI be mapped to a destination network layer address such as an IP address.
- LMI is a signaling standard between the router and the Frame Relay switch that is responsible for managing the connection and maintaining status between the devices.

خلاصه :

- Frame Realy پروتکل لایه دومی می باشد که دارای مکانیزم سوئیچینگ پکتی است. این پروتکل به کمک تعریف یک سری مدارهای مجازی (VC) و با به کار بردن مشخصه ای به نام DLCI اطلاعات لایه Network را دریافت و آنها را در فریم های Frame Relay کپسوله کرده و تحویل لایه فیزیکی می دهد .
- DLCI مشخصه محلی می باشد که مشخص می کند که سر دیگر مدار مجازی چه روتری قرار دارد .

درس چهارم :

پیکربندی و مانیتورینگ
Frame Relay

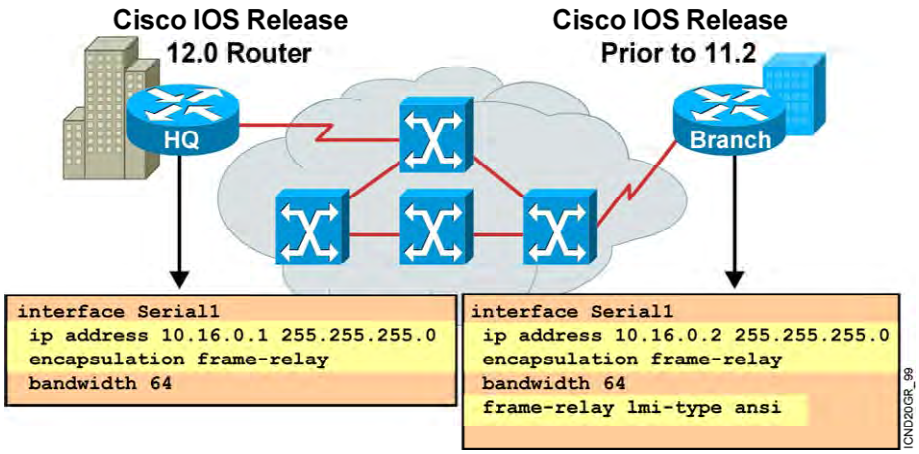
هدف :

این ماژول شامل :

۱. نحوه پیکربندی Frame Relay و پارامترهای آن روی روترهای سیسکو .
۲. بررسی تنظیمات و نحوه عملکرد Frame Relay به کمک فرمان های show و debug .

Configuring Basic Frame Relay

Cisco.com



تنظیمات اولیه پروتکل Frame Relay :

برای تنظیم کردن پروتکل Frame Relay روی یک روتر ، ابتدا می بایست مشخص شود که می خواهیم ارتباط این روتر با روتر و یا روترهای دیگر به چه صورتی باشد، یک به یک (Point-to-Point) و یا یک به چند (point-to-multipoint) .
بعد از مشخص شدن نوع ارتباط می بایست اینترفیس را برای ارتباط با شبکه Frame Relay تنظیم کنیم.

- فعال کردن پروتکل Frame Relay :
با فعال شدن این پروتکل ، فیلد DLCI به هر کدام از بسته ها IP اضافی و تحویل شبکه Frame Relay داده می شود .
- تعیین LMI Type :
به کمک LMI Type ، سیگنالینگ بین روتر و سوئیچ شبکه Frame Relay تعیین می شود.
- تعیین DLCI :
DLCI شماره ای است که در شبکه Frame Relay مشخص کننده یک مدار مجازی مشخص می باشد . بنابراین فریم های ارسالی از این اینترفیس با این شماره DLCI برچسب زده شده و تحویل شبکه Frame Relay داده می شود .
- تعیین IP Address

Configuring Subinterfaces

Cisco.com

- **Point-to-point**
  - **Subinterfaces act like leased lines.**
  - **Each point-to-point subinterface requires its own subnet.**
  - **Point-to-point is applicable to hub and spoke topologies.**
- **Multipoint**
  - **Subinterfaces act like NBMA networks, so they do not resolve the split-horizon issues.**
  - **Multipoint can save address space because it uses a single subnet.**
  - **Multipoint is applicable to partial mesh and full mesh topologies.**

تنظیم اینترفیس منطقی (Subinterface) :

همانطور که گفته شد اولین گام در تنظیم Frame Relay روی یک روتر ، مشخص و تنظیم کردن اینترفیسی است که به سوئیچ شبکه frame Relay متصل است . این انتخاب به نوع توپولوژی شبکه Frame Relay برمی گردد . شبکه Frame Relay از نقطه نظر Topology به سه دسته زیر تقسیم می شود:

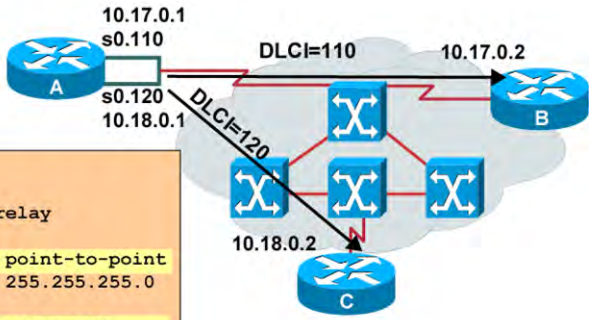
- توپولوژی hub and spoke
- توپولوژی Full Mesh
- توپولوژی Partial Mesh

در توپولوژی Hub and Spoke یک روتر به عنوان روتر مرکزی و سایر روترها به مانند بازوهای این روتر مرکزی عمل می کنند . درواقع دراین توپولوژی یک ارتباط یک به چند بین یک روتر مرکزی و سایر روترها وجود دارد .
در توپولوژی Full Mesh ، هر روتر دارای یک مدار مجازی با سایر روترها می باشد .
در توپولوژی Partial Mesh ، برخی از روترها به کمک مدارهای مجازی به تمامی روترها متصل هستند .
در شبکه Frame Relay رایجترین توپولوژی ، توپولوژی Hub and Spoke می باشد . براساس این توپولوژی یک روتر به عنوان روتر مرکزی با تعدادی مدار مجازی به سایر روترهای دیگر متصل می باشد . یکی از ویژگی های شبکه Frame Relay ، قدرت ادغام (Multiplexing) چند مدار مجازی روی یک بستر ارتباطی و یا به عبارتی روی یک اینترفیس فیزیکی می باشد . Frame Relay با به کار بردن مفهوم اینترفیس منطقی (Subinterface) عملیات تفکیک مدارهای مجازی را انجام می دهد . حال هر کدام از مدارهای مجازی (VC) به یک Subinterface متصل بوده و می بایست تنظیمات Frame Relay چون تعریف IP Address و شماره DLCI را درمورد این اینترفیس به کار برد .
Subinterface به دو صورت (Mode) قابل تنظیم می باشد :

- Point-to-Point:
این Mode زمانی روی یک Subinterface استفاده می شود که بخواهید یک مدار مجازی با اینترفیس فیزیکی و یا منطقی دیگری داشته باشید . بنابراین هر جفت از روترهایی که به صورت point-to-point به یکدیگر متصل هستند دارای Subnet متفاوت با جفت روتر های دیگر می باشند . بنابراین هر کدام از مدارهای مجازی دارای Subnet و یا درواقع رنج IP جداگانه ای می باشند .
- Multipoint:
این Mode زمانی روی یک Subinterface استفاده می شود که بخواهید چند مدار مجازی با چند اینترفیس فیزیکی و یا منطقی دیگر داشته باشید . دراین حالت تمامی اینترفیس هایی که به یکدیگر به کمک مدارهای مجازی متصل هستند می بایست دارای Subnet یکسان باشند .

Configuring Point-to-Point Subinterfaces

Cisco.com




```
interface Serial0
 no ip address
 encapsulation frame-relay
!
interface Serial0.110 point-to-point
 ip address 10.17.0.1 255.255.255.0
 bandwidth 64
 frame-relay interface-dlci 110
!
interface Serial0.120 point-to-point
 ip address 10.18.0.1 255.255.255.0
 bandwidth 64
 frame-relay interface-dlci 120
!
```

ICND20GR_104

پیکربندی اینترفیس منطقی در حالت Point-to-point :

درصورتی که یک Subinterface به صورت Point-to-point به یک روتر دیگر متصل باشد ، مدار مجازی به این اینترفیس متصل شده و می بایست IP Address و شماره DLCI که مشخص کننده این مدار مجازی می باشد را روی این Subinterface تنظیم کرد . برای مرتبط کردن این روتر به شبکه frame Relay می بایست مراحل زیر دنبال کنید :

گام اول : فعال کردن پروتکل Frame Relay :

وارد اینترفیس فیزیکی شده و پروتکل Frame Relay را روی آن فعال کنید.
به کمک فرمان زیر پروتکل Frame Relay ، روی یک اینترفیس فیزیکی فعال می شود .

Router(config-if)# Encapsulation Frame-relay

گام دوم : تنظیم اینترفیس منطقی :

۱. مشخص کردن Subinterface مربوطه و تعیین Point-to-point Mode :

شماره گذاری اینترفیس های منطقی (Subinterface) به این صورت است که ابتدا شماره اینترفیس فیزیکی را آورده و سپس شماره اینترفیس منطقی را.
به طور مثال برای تعریف اینترفیسهای منطقی (Subinterface) مربوط به اینترفیس فیزیکی Serial 0 ، ابتدا شماره اینترفیس فیزیکی و سپس شماره اینترفیس منطقی آورده می شود . درنتیجه Subinterface ها به صورت اینترفیس Serial 0.1 و یا اینترفیس Serial 0.2 نام گذاری می شوند .

Router(config-subif)# Interface <u>subinterface-number</u> point-to-point

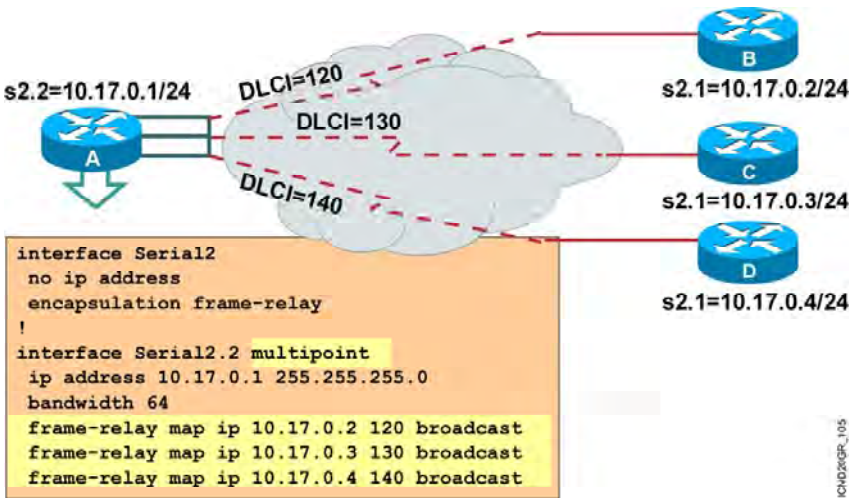
۲. شماره DLCI و IP Address را روی این اینترفیس منطقی تنظیم کنید :

Router(config-subif)# Frame-relay interface-dlci <u>dlci-number</u>

به شکل فوق توجه کنید .روتر A به کمک دو مدار مجازی به روترهای B و C متصل شده است .
اینترفیس فیزیکی Serial 0 نقطه اتصال به این دو روتر می باشد . بنابراین می بایست به دو مدار مجازی متصل شود . در این مثال از ارتباط Point-to-point استفاده شده است ، یعنی هر کدام از مدارهای مجازی در Subnet های جداگانه ای قراردارند . مدار مجازی بین روتر A و C دارای رنج آدرس 10.17.0.0 و مدار دیگر ، دارای رنج آدرس 10.18.0.0 می باشد .

تنظیم هر کدام از Subinterface ها ، شامل تنظیمات فوق با درنظر گرفتن متفاوت بودن Subnet ها در هر کدام از جفت روترهای می باشد . بنابراین هر کدام از این Subinterface ها در یک رنج IP Address قرار دارد . این روش زمانی مفید می باشد که با محدودیت تعداد IP مواجه نباشید ، درغیراین صورت روش دوم یعنی Multimode پاسخگوی محدودیت IP خواهد بود .

Multipoint Subinterfaces Configuration Example



پیکربندی اینترفیس منطقی در حالت Multipoint :

در این روش subinterface به مانند یک اینترفیس فیزیکی عمل می کند ، با این تفاوت که می بایست به جای یک ارتباط ، ارتباط چندگانه با اینترفیس های دیگر و دارای Subnet یکسانی با آنها باشد.
برای مرتبط کردن این روتر به شبکه frame Relay می بایست مراحل زیر دنبال کنید :

گام اول : فعال کردن پروتکل Frame Relay :
وارد اینترفیس فیزیکی شده و پروتکل Frame Relay را روی آن فعال کنید.
به کمک فرمان زیر پروتکل Frame Relay ، روی یک اینترفیس فیزیکی فعال می شود .

Router(config-if)# Encapsulation Frame-relay

گام دوم : تنظیم اینترفیس منطقی :

۱. مشخص کردن Subinterface مربوطه و تعیین Multipoint Mode:

Router(config-subif)# Interface subinterface-number multipoint

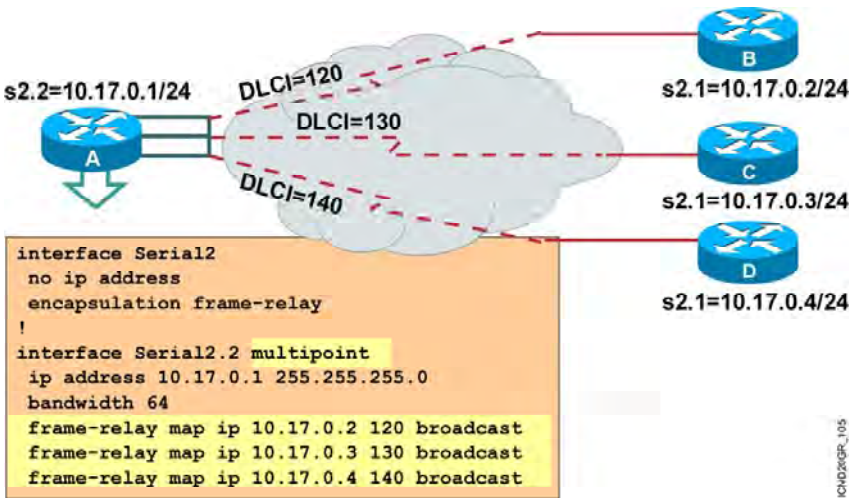
۲. مشخص کردن هر کدام از مدارهای مجازی به کمک map کردن IP Address مشخص به شماره DLCI مشخص:
در Multipoint Mode ، اینترفیسی که به چندین مدار مجازی متصل باشد ، می بایست فریم های هر کدام از این مدارها را تفکیک کرده و با شماره DLCI مشخص تحویل شبکه frame Relay دهد .
به طور مثال این اینترفیس باید بداند پکتهایی که دارای آدرس مقصد 10.17.0.2 می باشند می بایست در مداری قرار گیرند که با 120 DLCI مشخص شده اند . درواقع می بایست در فریم Frame Relay و در فیلد DLCI مقدار 120 قرار گیرد به طوری که توسط سوئیچ frame Relay قابل تفکیک باشد .
به کمک فرمان زیر می توان تناظر بین یک IP Address مشخص با یک شماره DLCI مشخص را انجام داد .

Router(config-subif)#Frame-relay map ip ip address dlci-number broadcast

در شکل فوق روتر A به کمک سه مدار مجازی به روترهای B ، C و D به صورت Multipoint متصل شده است . بنابراین روتر با بررسی Map Table ، به راحتی می تواند تناظر بین IP Address ها و شماره DLCI را مشخص و به کمک آن فریم های Frame Relay را تحویل شبکه Frame Relay دهد .

تا به اینجا با مفهوم Subinterface و هر کدام از Mode های آن آشنا شدید ، سوالی که پیش می آید اینست که تفاوت این دو Mode در چیست ؟
به صورت کلی می توان گفت تفاوت عمده این دو Mode در مواجه با پکتهای Broadcast می باشد.

Multipoint Subinterfaces Configuration Example



پیکربندی اینترفیس منطقی در حالت Multipoint :

فرض کنید پروتکل RIP به عنوان پروتکل مسیریابی روی روترهای شبکه Frame Relay فعال شود ، همانطور که می دانید این پروتکل به صورت پیش فرض هر 30 ثانیه یکبار Update هایی به آدرس Broadcast به تمامی روترهای مجاور ارسال می کند .
هر روتر با دریافت Update جدید و اعمال آن روی Routing table خود ، اطلاعات جدید و تغییرات را به تمامی روتر های مجاور به جز روتری که این اطلاعات را از او گرفته بود ارسال می کند . و این نتیجه الگوریتم Split Horizon می باشد . درواقع الگوریتم Split Horizon می گوید "فرض کنید یک روتر Update ایی را از یک اینترفیس دریافت کند که منجر به تغییر Routing Table شود ، بنابراین پس از اعمال روی Routing Table اش ، می بایست اطلاعات کل Routing Table اش را به تمامی اینترفیس ها جز اینترفیسی که Update را از آن دریافت کرده بود ارسال کند " ، با این تعریف در شبکه Frame Relay در صورتی که اینترفیس Multipoint ، Update ایی را از طریق یکی از مدارهای خود دریافت کند می بایست بعد از اعمال تغییرات لازمه آن را دراختیار روترهای دیگر قرار دهد .
سوالی که مطرح می شود اینست که آیا روتر می تواند Update را از طریق همین subinterface دراختیار روترهای متصل دیگر قرار دهد ؟
همانطور که گفته شد در حالتی که از Multipoint استفاده شود تمامی اینترفیسهای متصله در این محیط ، دارای Subnet یکسانی هستند و Update ایی که از یک اینترفیس دریافت شود با وجود فعال بودن الگوریتم Split Horizon نمی تواند دوباره از این اینترفیس خارج شود .
درصورتی که در Point-to-point mode ، هر کدام از مدارهای مجازی به یک Subinterface مستقل و دارای Subnet متفاوت با بقیه ، متصل هستند.
بنابراین Update ایی که توسط یک Subinterface دریافت شود براحتی توسط Subinterface های دیگر منتشر می شود .

نکته : درصورتی که بخواهید از Multipoint mode استفاده کنید ، اما بخواهید Update ها براحتی در شبکه منتشر شوند دو راه پیش رو خواهید داشت :

- غیر فعال کردن Split Horizon که می بایست عواقب بروز Loop در شبکه را در نظر بگیرید.
- استفاده از دستور Broadcast درانتهای فرمان Frame Relay map ، بنابراین Broadcast و Multicast های مربوط به Update پروتکل های مسیریابی توسط اینترفیس Multipoint روی مدارهای مجازی منتقل خواهد شد .

show interfaces Example

Cisco.com

```
Router#show interfaces s0
Serial0 is up, line protocol is up
  Hardware is HD64570
  Internet address is 10.140.1.2/24
  MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec, rely 255/255, load 1/255
  Encapsulation FRAME-RELAY, loopback not set, keepalive set (10 sec)
  LMI enq sent  19, LMI stat recvd 20, LMI upd recvd 0, DTE LMI up
  LMI enq recvd 0, LMI stat sent  0, LMI upd sent  0
  LMI DLCI 1023  LMI type is CISCO  frame relay DTE
  FR SVC disabled, LAPF state down
  Broadcast queue 0/64, broadcasts sent/dropped 8/0, interface broadcasts 5
  Last input 00:00:02, output 00:00:02, output hang never
  Last clearing of "show interface" counters never
  Queueing strategy: fifo
  Output queue 0/40, 0 drops; input queue 0/75, 0 drops
  <Output omitted>
```

- **Displays line, protocol, DLCI, and LMI information**

بررسی فرمان Show interface:

بعد از اینکه اینترفیسی را جهت اتصال به شبکه Frame Relay تنظیم کردید ،به کمک فرمان زیر می توانید وضعیت آن و صحت تنظیمات را بررسی کنید :

Router# show interface s0

همانطور که در شکل فوق مشاهده می کنید ، با فعال شدن پروتکل Frame Relay ، نوع Encapsulation روی این اینترفیس Frame Relay خواهد شد .
در خروجی این فرمان می توانید DLCI Number و LMI Type ایی را که روی این اینترفیس تنظیم شده است را مشاهده کنید .

show frame-relay pvc Example

Cisco.com

```
Router#show frame-relay pvc 100

PVC Statistics for interface Serial0 (Frame Relay DTE)

DLCI = 100, DLCI USAGE = LOCAL, PVC STATUS = ACTIVE, INTERFACE = Serial0

  input pkts 28             output pkts 10           in bytes 8398
  out bytes 1198            dropped pkts 0           in FECN pkts 0
  in BECN pkts 0            out FECN pkts 0          out BECN pkts 0
  in DE pkts 0              out DE pkts 0
  out bcast pkts 10          out bcast bytes 1198
  pvc create time 00:03:46, last time pvc status changed 00:03:47
```

- **Displays PVC traffic statistics**

بررسی فرمان Show frame-relay pvc:

به کمک فرمان فوق می توان تک تک مدارهای مجازی و State هر کدام و شماره DLCI مربوط به آن را مشاهد کرد .
شکل فوق خروجی این فرمان را روی یک روتر نمایش می دهد . این روتر به کمک یک مدار مجازی از طریق اینترفیس فیزیکی serial 0 به شبکه Frae Relay متصل شده است . وضعیت این مدار مجازی در حالت active و با شماره DLCI 100 مشخص می شود .

show frame-relay map Example

Cisco.com

```
Router#show frame-relay map
Serial0 (up): ip 10.140.1.1 dlci 100(0x64,0x1840), dynamic,
              broadcast,, status defined, active
```

- Displays the route maps, either static or dynamic

بررسی فرمان Show frame-relay map:

به کمک فرمان فوق می توانید Map Table مربوط به Frame Relay را بررسی کنید .
شکل فوق Map Table مربوط به یک روتر را نشان می دهد . این جدول دارای یک رکورد می باشد که دارای فیلدهای IP Address و DLCI Number می باشد .
بنابراین آدرس 10.140.1.1 در تناظر با DLCI 100 می باشد که به صورت Dynamic و توسط LMI Message ها بدست آمده است .

Summary

Cisco.com

- A basic Frame Relay configuration assumes one or more physical interfaces, and LMI and Inverse ARP are running on the remote routers. In this type of environment, the LMI notifies the router about the available DLCIs.
- When the remote router does not support Inverse ARP, or when you want to control routed broadcast traffic, you must define the address-to-DLCI table statically.
- You can configure Frame Relay subinterfaces in either point-to-point or multipoint mode.
- After you configure Frame Relay, you can verify that the connections are active using the available show commands.
- Use the debug frame-relay lmi command to verify and troubleshoot a Frame Relay connection.

خلاصه :

برای تنظیم کردن پروتکل Frame Relay روی یک روتر ، ابتدا می بایست مشخص شود که می خواهیم ارتباط این روتر با روتر و یا روترهای دیگر به چه صورتی باشد، یک به یک (Point-to-Point) و یا یک به چند (point-to-multipoint) .
بعد از مشخص شدن نوع ارتباط می بایست اینترفیس را برای ارتباط با شبکه Frame Relay تنظیم کنیم.

- فعال کردن پروتکل Frame Relay
- تعیین LMI Type
- تعیین DLCI
- تعیین IP Address

پیکربندی اینترفیس منطقی در حالت Point-to-point و multipoint :
گام اول : فعال کردن پروتکل Frame Relay
گام دوم : تنظیم اینترفیس منطقی