CCNA :

Cisco Certified Network Associate

Study Guide

Engineer SHOWAN KOLIJI

مهندس شوان کلیجی

Email : WWW.Kolijis@yahoo.com

WWW.Koliji_Cisco@yahoo.com

OSI and TCP/IP Model

مدل چند لایه ای :

مقایسه مدل چند لایه ای در مقابل ساختار چند لایه ای , متناظر با فعالیت یک گروه روی یک فعالیت در مقابل 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 یا عدم فعالیت صحیح یک فرد در این گروه به راحتی قابل تشخیص می باشد.
- عدم فعالیت صحیح یک فرد روی عملکرد بقیه افراد گروه تاثیر منفی گذاشته و درنتیجه فعالیت گروهی به نتیجه نخواهد رسید .
- تقسیم وظایف به گونه ای صورت گرفته میگیرد که هر فرد علارغم وابستگی به گروه به تنهایی میتواند وظایف مشخص شده خود را انجام دهد .

بنابراین در این معماری چند لایه ای هر لایه مستقل از لایه های دیگر عمل میکند 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 .

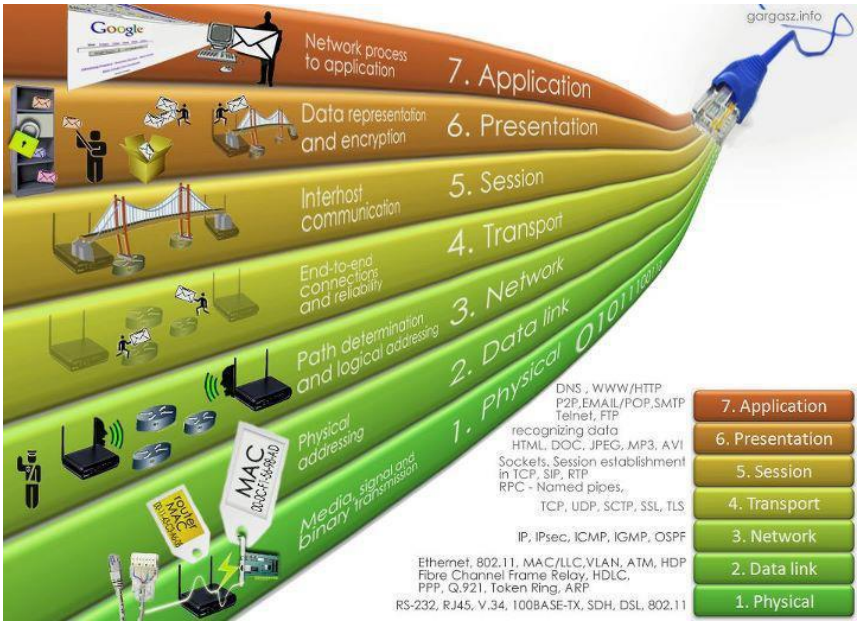
امروزه عملا غیر ممکن است که کامپیوتری بدونه پشتیبانی از مجموعه پروتکل های TCP/IP وجود داشته باشد . سیستم عامل های مایکروسافت و لینوکس و یونیکس و تلفن های همراه از TCP/IP حمایت میکنند . محصولات سیسکو نیز حمایت گسترده ای از TCP/IP دارند , زیرا محصولات سیسکو زیر ساختی فراهم می کنند که به کامپیوترها اجازه میدهد با یکدیگر بر اساس TCP/IP ارتباط برقرار کنند . زمانی پروتکل های شبکه و از جمله TCP/IP , OSI وجود نداشت و کامپیوترها نمیتوانستند با هم ارتباط داشته باشند.

این نیاز منجر به طراحی یک مدل هفت لایه تحت عنوان OSI (اتصال سیستم های باز) توسط موسسه جهانی استاندارد (ISO) در سال 1984 میلادی شد . ISO هدف بزرگی از OSI داشت : استاندارد سازی پروتکل های شبکه داده , که ارتباط بین تمام کامپیوترهای دنیا را میسر ساخت .

البته تلاش های دیگری ولی با رسمیت کمتر از سوی وزارت دفاع ایالات متحده و برای ایجاد یک مدل شبکه عمومی و استاندارد شده صورت گرفت . محققان دانشگاه های مختلف علاوه بر کار اصلی , جهت کمک به پیشرفت پروتکل ها داوطلب شدند. این تلاش ها منجر به مدل شبکه رقیبی به نام TCP/IP شد که پرکاربردترین مجموعه پروتکل شبکه ای شده است .

مدل هفت لایه ای OSI :

OSI : Open System Interconnection



: Application Layer

لایه Application , لایه هفتم از مدل هفت لایه ای OSI میباشد .

این لایه مجموعه ای از استانداردها و توابع مختلفی می باشد . بطوریکه 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 وب را می گشایید این مرورگر به عنوان یک نرم افزار لایه هفتم وظیفه برقراری ارتباط با کاربر را به عهده دارد .

در واقع همان برنامه های نرم افزاری است که شما در صفحه نمایش مانیتور از آن استفاده می کنید .

: 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 .
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 .

: Session Layer

این لایه وظیفه برقراری شرایط یک session بین دو Station نهایی را بر عهده دارد.
وظیفه تأید هویت (Authentication) و برقراری یک Session و در نهایت اتمام Session و بررسی حساب (Accounting) را به عهده دارد.
پس از برقراری یک Session , اطلاعات تحویل لایه چهارم داده میشود . به 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 شود.

: Transport Layer

لایه چهارم وظیفه برقراری یک ارتباط End-to-End را به عهده دارد . وظیفه کنترل ارتباط برقرار شده را به عهده دو Station نهایی میگذارد و آمادگی station نهایی را برای دریافت ترافیک بررسی می کند و پس از برقراری ارتباط توسط لایه چهارم , ترافیک هدایت خواهد شد.
User Data بعد از تحویل در بسته های استاندارد به نام سگمنت بسته بندی (Encapsulate) می شود .
وظیفه پیگیری رسیدن یا نرسیدن بسته ها به مقصد به عهده این لایه می باشد .

Network Layer :

این لایه وظیفه مسیریابی و هدایت ترافیک را به عهده دارد . در واقع انتخاب بهترین مسیر در میان مسیرهای متفاوت را به عهده دارد . Router به عنوان یک Device لایه سوم وظیفه مسیریابی و هدایت ترافیک را به عهده دارد .

هدایت ترافیک در این لایه بر اساس پروتکل ها و الگوریتم ها ی مسیریابی متفاوتی صورت میگیرد. در این لایه آدرس دهی بسته ها بر اساس پروتکل IP , IPX , Apple Talk صورت میگیرد.

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 یک سری استانداردها برای جلوگیری از تصادم و از بین رفتن داده وجود دارد , تعریف این استاندارد ها در لایه دوم صورت می گیرد .

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

یکی از سخت افزارهایی که وظیفه مدیریت منابع سخت افزاری و ارتباط هر یک از آنها را بر اساس لایه دوم به عهده دارد Switch می باشد .

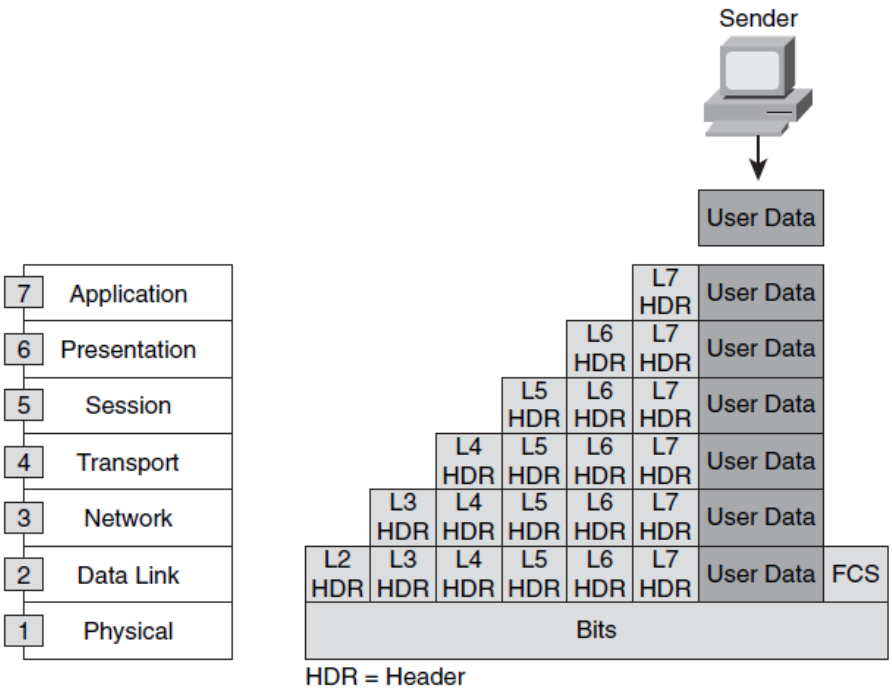
Physical Layer :

در این لایه اطلاعات دریافتی از لایه های بالاتر تبدیل به یک سری بیت های 0 و 1 شده و جهت انتقال بر روی بستر ارتباطی , تبدیل به سیگنال الکتریکی و یا موج نوری خواهد شد .

در این لایه هیچ پردازشی بر روی 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 بیت های 0 و 1 تحویل بستر ارتباطی می دهد .

به فرایند اضافه شدن Header ها در هر لایه Encapsulation و به فرایند کندن آنها در هر لایه Dencapsulation می گویند .



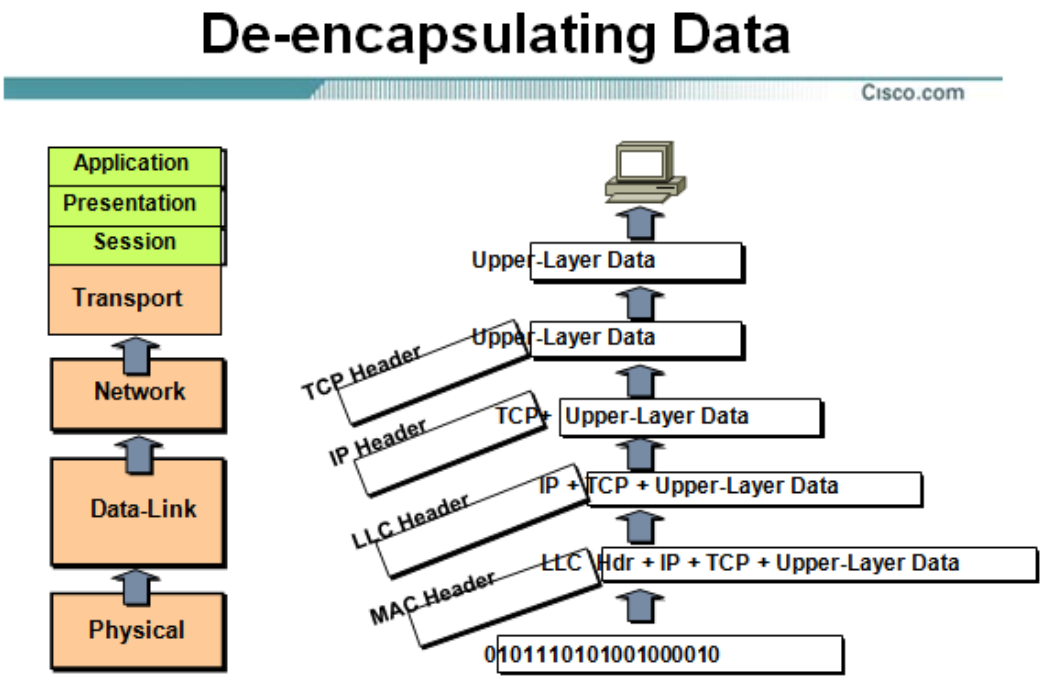
بسته بندی کردن داده ها در هر لایه :

به صورت کلی اطلاعاتی که سه لایه بالاتر را طی میکند با عنوان Data User به لایه چهارم تحویل داده می شود .در لایه چهارم اطلاعات دریافتی درون بسته های استانداردی به نام سگمنت بسته بندی می شوند . در این لایه هر کدام از بسته ها یک سری اطلاعات تکمیلی و کنترلی در غالب TCP Header و یا UDP Header خواهد 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 بر اساس پروتکل IP باشد . بنابراین بعد از اضافه شدن IP Header به بسته های دریافتی تحویل لایه پایین تر یعنی لایه Data Link داده میشود . به هر کدام از بسته ها در لایه Network , Packet گفته می شود .

در لایه دوم یا Data Link Layer با اضافه شدن LLC Header , Mac Header به آن بسته بندی جدیدی به نام Frame خواهیم داشت و در نهایت فریم ها تبدیل به یک سری بیت های 0 و 1 شده و جهت انتقال روی بستر ارتباطی به سیگنالهای الکتریکی و یا موج نوری تبدیل می شود.

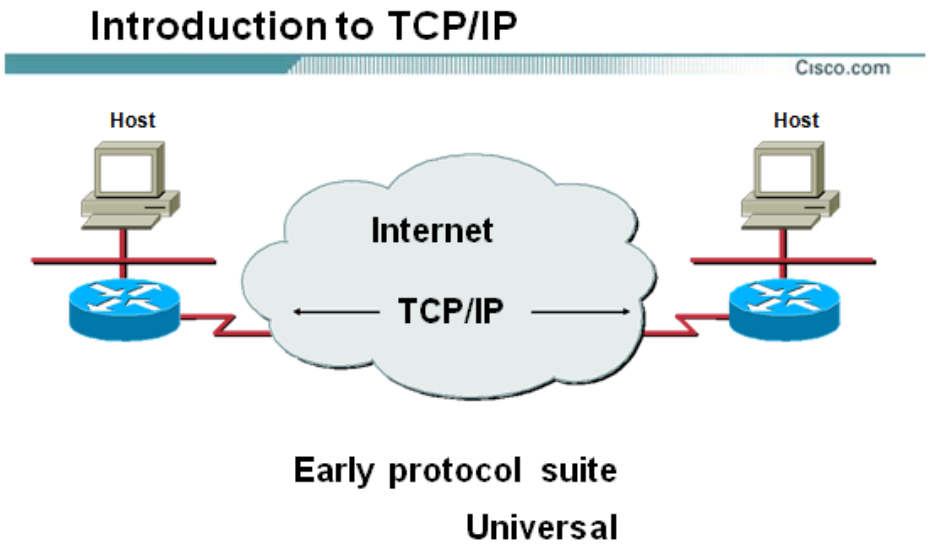
شکل صفحه قبل نوع Encapsulation را در هر لایه نشان می دهد . بنابراین روی اطلاعات به ترتیب از لایه هفتم به سمت لایه اول بسته بندی های مختلفی صورت گرفته و در نهایت جهت انتقال در اختیار لایه اول قرار می گیرد .



بسته بندی کردن داده ها در هر لایه :

از سوی دیگر زمانیکه بیت های 0 و 1 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 می گیرد . در لایه سوم هر کدام از پکت ها بررسی شده و پس از مشخص شدن آدرس مبدا و مقصد , تحویل لایه بالاتر , Transport Layer داده می شود . در این لایه با توجه به TCP Header 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 در اختیار لایه هفتم و نرم افزارهایی چون مرورگر Web قرار می گیرد .

شکل فوق نوع De-encapsulation را در هر لایه نشان میدهد . بنابراین اطلاعات به ترتیب از لایه اول به سمت لایه هفتم با کندن Header ها در هر لایه صورت گرفته و جهت نمایش به لایه هفتم 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 آمریکا می باشد.

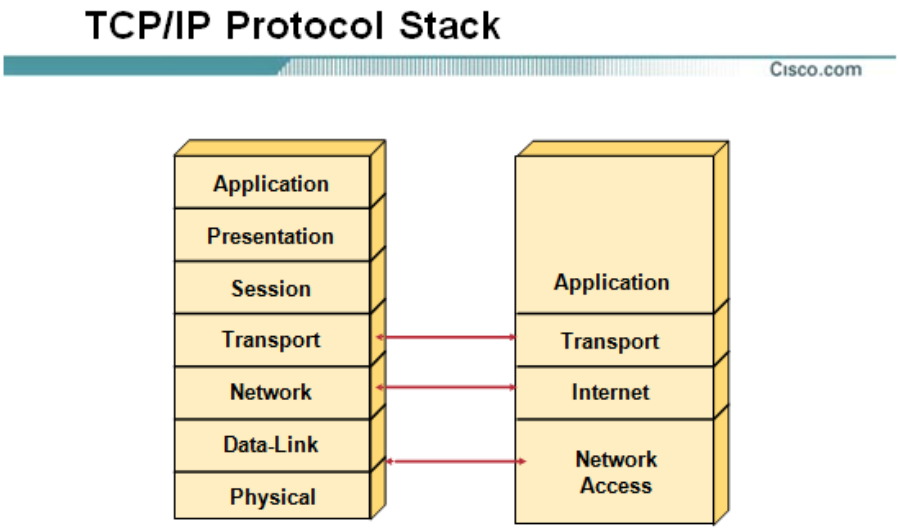
این معماری که امروزه اساس شبکه جهانی اینترنت به حساب می آید یک معماری چهار لایه ای به شرح زیر می باشد :

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

TCP/IP مجموعه بزرگی از پروتکل ها را تعریف می کند که ارتباط بین کامپیوترها را میسر میسازد . TCP/IP جزئیات هر یک از پروتکل ها را در اسنادی به نام RFC ها (درخواست توضیحات) تعریف می کند .کامپیوتری که پروتکل های شبکه استاندارد شده توسط TCP/IP را پیاده سازی می کند , می تواند با کامپیوترهای دیگری که استاندارد TCP/IP را به کار می برند , ارتباط برقرار کند .

مدل معماری TCP/IP و نمونه پروتکل های آن

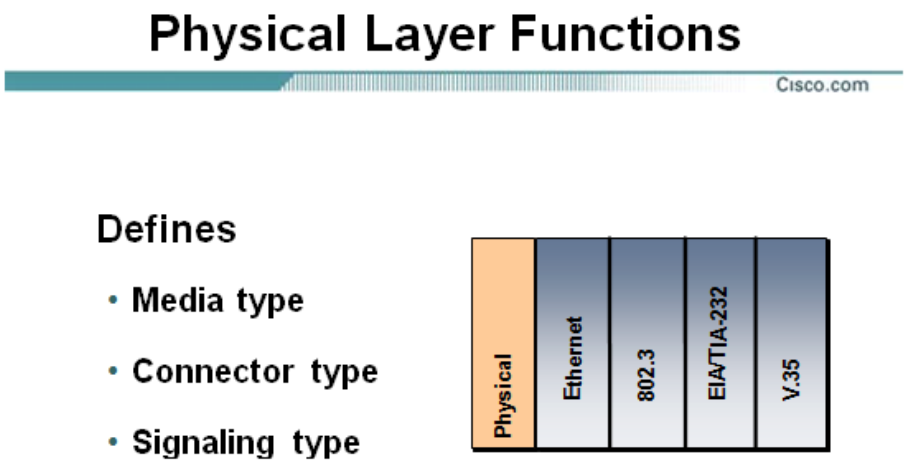
لایه معماری TCP/IP	نمونه پروتکل ها
کاربرد	SMTP ,POP3 ,HTTP
انتقال	UDP ,TCP
میان شبکه	IP
واسط شبکه	Frame Relay ,Ethernet



شکل فوق تناظر بین هفت لایه OSI با چهار لایه ای 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 هرکدام از این لایه ها متناظر با عملکرد مدل هفت لایه ای OSI می باشد.



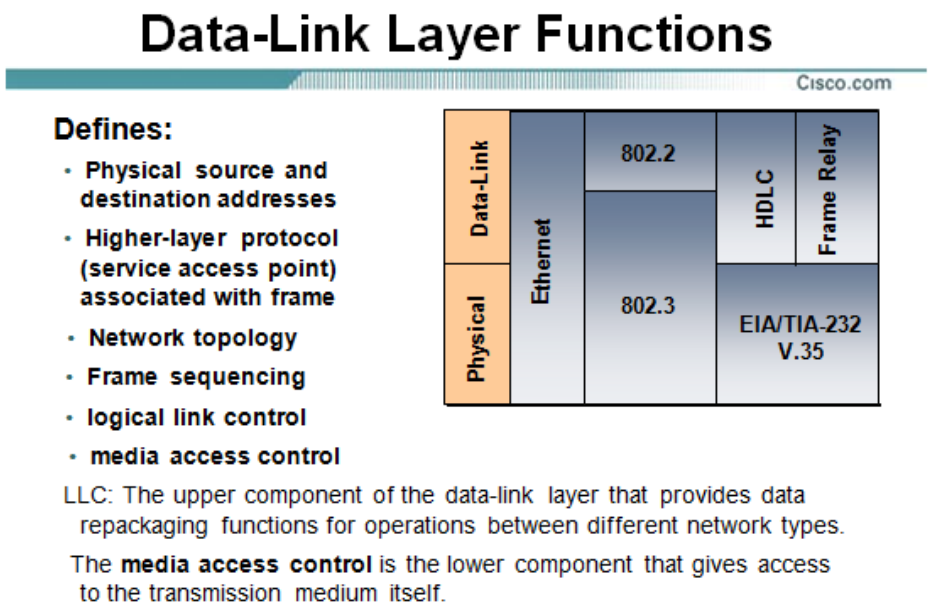
: Physical Layer

این لایه شامل معرفی انواع بسترهای ارتباطی (کابل , امواج رادیویی , ...) و اتصالات مربوط به هر کدام و معرفی انواع سیگنال هایی که وظیفه انتقال بیت های 0 و 1 را به عهده دارند

(سیگنال های الکتریکی , امواج رادیویی , ...) می باشد .

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

این لایه پروتکل ها و سخت افزار لازم برای تحویل داده از طریق شبکه فیزیکی را تعریف می کند . این لایه بین شبکه و کامپیوتر است . برای نمونه , اترنت مثالی از پروتکل های لایه واسط شبکه TCP/IP می باشد . اترنت نحوه کابل بندی , آدرس دهی و پروتکل های مورد نیاز برای ایجاد یک LAN اترنت را تعریف می کند . علاوه بر این , کانکتورها , کابل ها , سطوح ولتاژ و پروتکل های لازم برای تحویل داده از طریق لینک های WAN , در پروتکل های متنوعی که در این لایه قرار می گیرند , تعریف شده اند .



: Data Link Layer

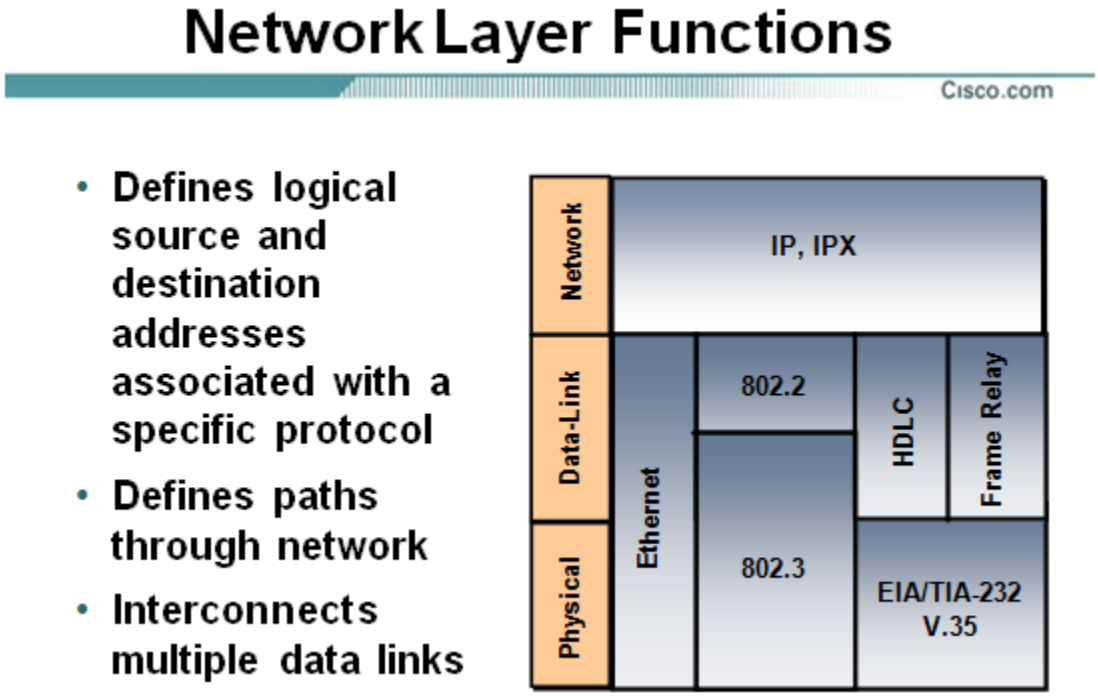
Data Link Layerبه عنوان لایه دوم از مدل هفت لایه ای OSI وظیفه برقراری یک لینک مورد اطمینان بین دو Station نهایی در یک شبکه LAN را به عهده دارد . آدرس دهی فریم ها در این لایه بر اساس آدرس فیزیکی (MAC Address) می باشد . بنابراین اطلاعات در این لایه به تعدادی فریم تقسیم شده و در هر فریم بعد از قرار گرفتن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

این لایه شامل یک سری 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 , MAC تقسیم می شود .

زیر لایه LLC (Logical Link Control) وظیفه کنترل مبادله Data را بر عهده دارد .

زیر لایه MAC وظیفه خطایابی فریم بر اساس فیلد FCS و هدایت فریم LLC بر اساس فیلدهای Source MAC Address و Destination MAC Address را به عهده دارد.



: Network Layer

Network Layer به عنوان لایه سوم از مدل هفت لایه ای OSI , وظیفه تعیین بهترین مسیر از میان مسیرهای متفاوت و هدایت پکت ها بر اساس آدرس منطقی در مبداء و مقصد را به عهده دارد.

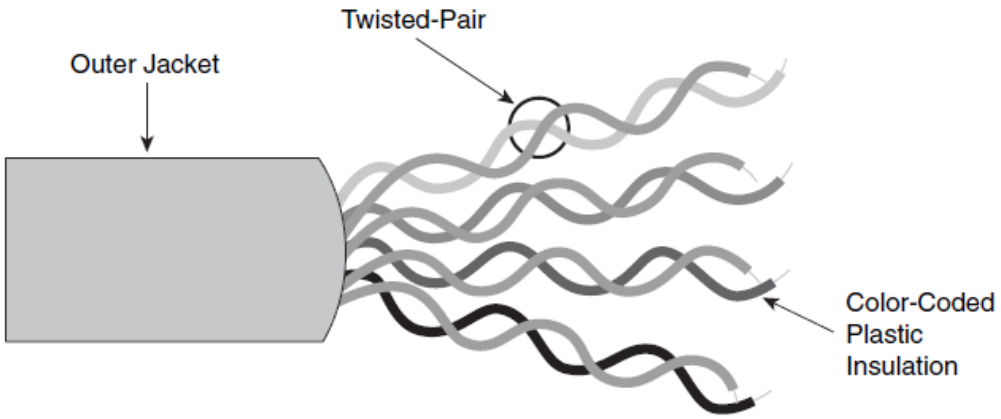
آدرس منطقی در این لایه بر اساس پروتکل IP , IPX , Apple Talk خواهد بود و مسیریابی به کمک الگوریتم و پروتکل های مسیریابی همچون RIP , OSPF خواهد بود .

TCP/IP : Transmission Control Protocol / Internet Protocol

پروتکلی است که بسته (محموله) را در اینترنت حمل می کند .

تعدادی از اعضای مجموعه TCP/IP و عملکرد آنها

نام	عملکرد
TCP (پروتکل کنترل انتقال)	اطمینان میدهد که اتصال بین کامپیوترها برقرار است
IP (پروتکل اینترنت)	آدرس کامپیوتری را کنترل می کند
ARP (پروتکل آدرس یابی)	آدرس های IP را با آدرس های MAC مرتبط می کند
OSPF (اول کوتاهترین مسیر باز)	نوعی RIP که سرعت و قابلیت اطمینان بیشتری دارد
ICMP (پروتکل کنترل پیام اینترنتی)	خطاها را کنترل و پیام های خطا برای TCP/IP می فرستد
BGP/EGP (پروتکل ورود و خروج)	چگونگی عبور داده ها از شبکه ای به شبکه دیگر را کنترل میکند
SNMP (پروتکل مدیریت شبکه)	به مدیران شبکه اجازه می دهد که با وسایل شبکه ارتباط برقرار و آنها را مدیریت کنند
PPP (پروتکل نقطه به نقطه)	ارتباط از طریق شماره گیری را برای شبکه ها فراهم می سازد
SMTP (پروتکل حمل و نقل پست)	پست الکترونیکی چگونه در یک شبکه TCP/IP بین سرورها ردوبدل می شود
IMAP4 (پروتکل پیامهای آگهی اینترنتی V4)	پروتکل شیوه هایی را برای تماس مشتری ها با سرورها و جمع آوری ایمیل ها اعمال میکنند
POP3 (پروتکل اداره پست v3)	



: Cable

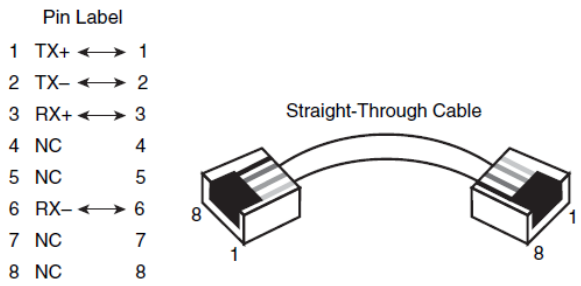
کابل های Twisted-Pair متشکل از 8 سیم پیچیده به هم است . دلیل پیچیده شدن آنها در هم آن است که هر سیم , Noise سیم دیگر را خنثی میکند . با پیچیده شدن آنها به هم جریان القایی هر سیم تقریبا صفر است . سیم ها 2 به 2 در هم پیچیده شده اند.

Copper Cables :

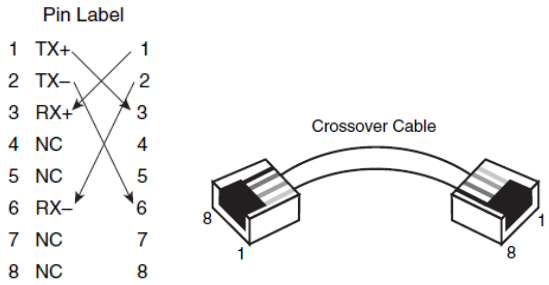
Category	Wi	Pair	Bit-Rate	Bond-Rate	Usage
Cat 1	4	2			Voice
Cat 2	8	4	4 Mbps		Data
Cat 3	8	4	10 Mbps	16 MHz	Data
Cat 4	8	4	16 Mbps	20 MHz	Data
Cat 5	8	4	100 Mbps	80 MHz	Data
Cat 5e	8	4	1000 Mbps	100 MHz	Data
Cat 6	8	4	1 Gbps	250 MHz	Data
Cat 6A	8	4	10 Gbps	500 MHz	Data
Cat 7	8	4		600 MHz	Data
Cat 8	8	4		1.2 GHz	Data

Bit-Rate = نرخ انتقال داده bps

Bond-Rate = پهنای باند – فرکانس Hz



کابل Straight-Through



کابل Crossover

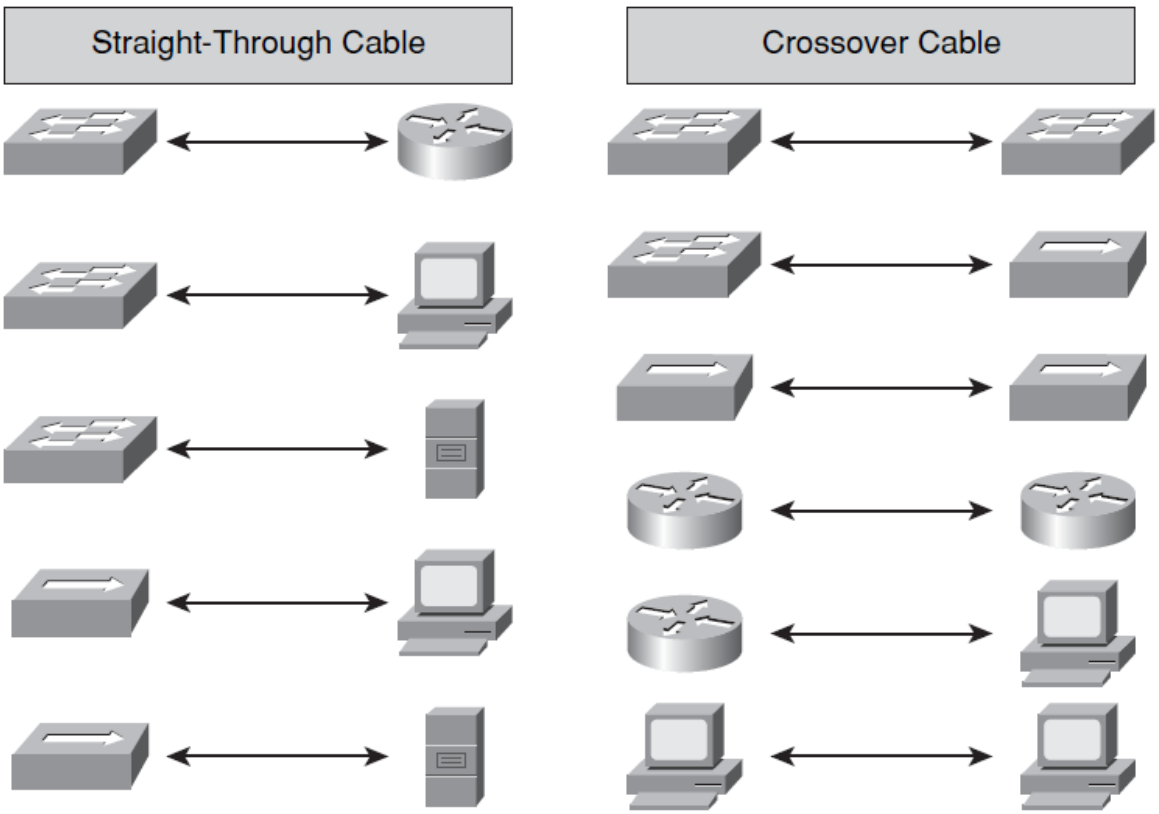
استانداردهای رنگ سیم ها :

EIA / TIA 568A	EIA / TIA 568B
سفید / سبز	سفید / نارنجی
سبز	نارنجی
سفید / نارنجی	سفید / سبز
آبی	آبی
سفید / آبی	سفید /آبی
نارنجی	سبز
سفید / قهوه ای	سفید / قهوه ای
قهوه ای	قهوه ای

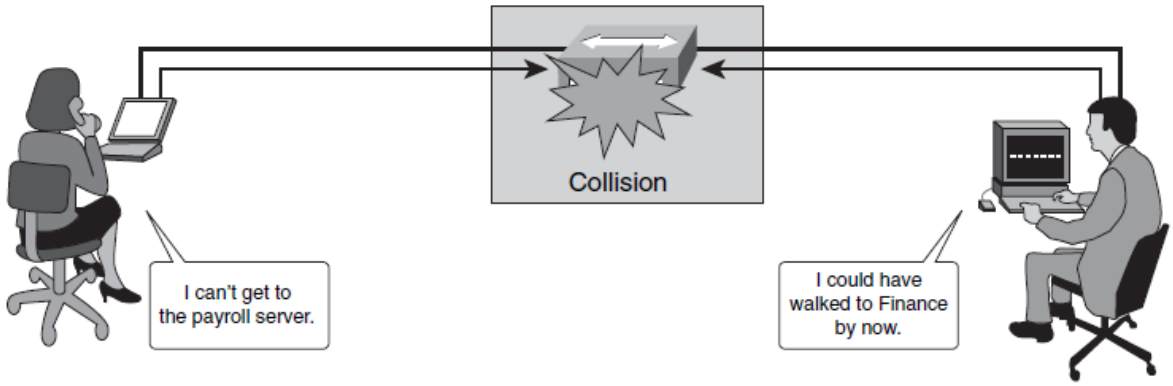
اتصال Device ها با کابل ها :

برای اتصال دستگاه های همنام از کابل Crossover استفاده می کنیم و برای دستگاه های غیر همنام از کابل Straight Through استفاده می کنیم . (Switch و Hub یک دستگاه هستند یعنی Pin-Out آنها یکی است) . اتصال PC و Router استثنا است .

نوع کابل برای اتصال دستگاه های مختلف :



Collision



برخورد یا تصادم (collision) در اصطلاح شبکه بندی به حالتی گفته می شود که دو PC همزمان سعی در انتقال داده در یک سیم شبکه بکنند اطلاعات به هم برخورد می کنند و collision به وجود می آید و هر دو اطلاعات از بین می رود .

ناحیه تصادم (Collision Domain) :

ناحیه ای که مجموعه کامپیوترهایی که امکان بروز تصادم بین آنها وجود دارد را ناحیه تصادم میگویند .

راه جلوگیری از عمل تصادم :

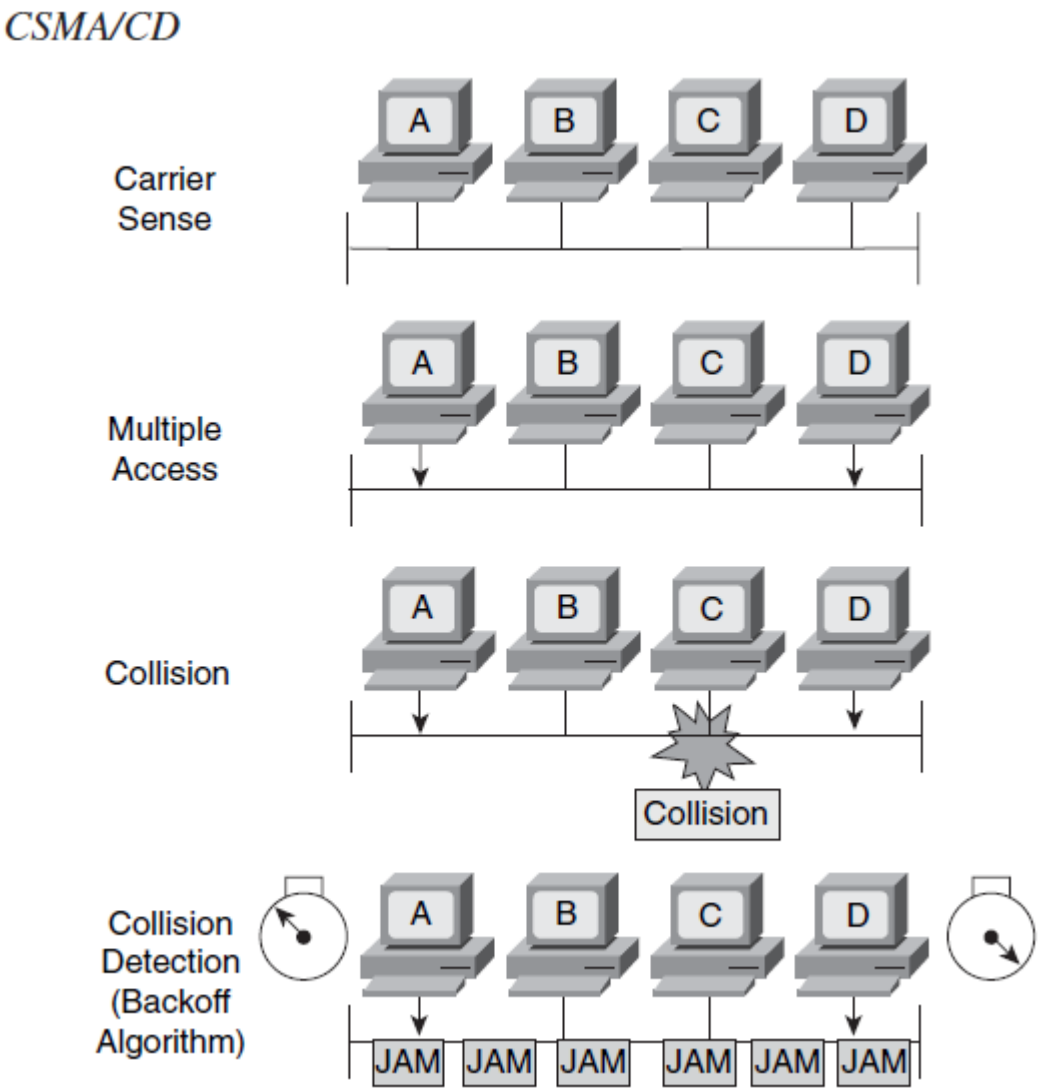
استفاده از CSMA / CD

Carrier Sense Multiple Access / Collision Detection : CSMA / CD

در این حالت PCها اول به خط گوش می کنند اگر سطح ولتاژی وجود داشته باشد صبر می کنند تا زمانی که تمام شود و آنگاه می توانند سیگنال بفرستند یعنی تنها وقتی تبادل داده ای میکنند که PC های دیگر در حال انتقال داده نباشند .

نکته :

هرگاه دو PC با همدیگر تبادل اطلاعات می کنند و collision رخ دهد باید حتما بعداز تصادم Jam Signal به تمام PC های دیگر ارسال کنند تا همه مطلع شوند و بعد دوباره تلاش کنند برای ارسال اطلاعات.



CRC

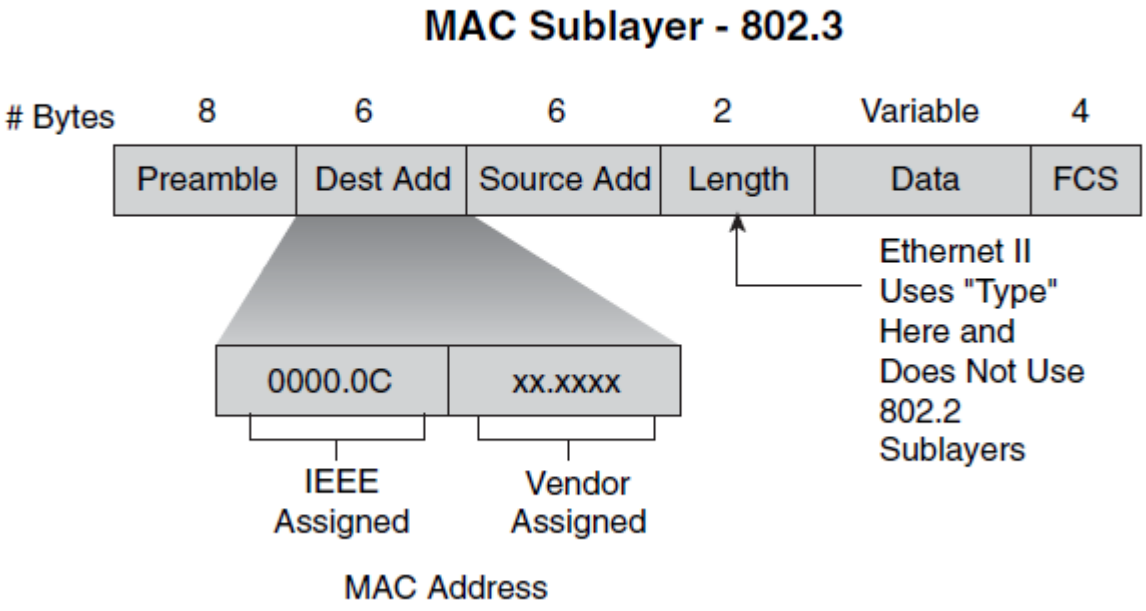
Cyclic Redundancy Check : رویه ای که در خطایابی حین انتقال داده استفاده می شود .

MAC :

Media Access Control :دارای ساختار 48 بیتی می باشد که شامل دو بخش 24 بیتی میباشد.

24 بیت اول توسط IEEE به هر کدام از شرکت های سازنده به صورت منحصر به فرد ارائه می شود و 24 بیت دوم توسط هر شرکت به سخت افزاری که نیاز به یک آدرس فیزیکی دارد به صورت منحصر به فرد داده می شود .

Ethernet MAC Address



OUI : Organizationally Uniqe Identifier

قسمت ثابت MAC که توسط IEEE ارائه شده است.

VAA : Vendor Assigned Address

قسمت منحصر به فردی که توسط کارخانه سازنده دستگاه حک می شود.

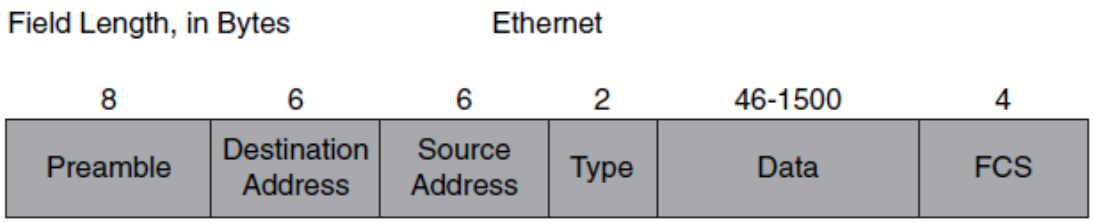
نمایش آدرس MAC به دو صورت زیر است :

DD:51:FD:EE:F7:EA

DD51.FDEE.F7EA : که در سیسکو اینگونه نمایش داده می شود

: Ethernet

استاندارد IEEE 802.3 برای اتصال شبکه ها . اترنت از یک توپولوژی گذرگاهی یا ستاره ای استفاده میکند و به روش دستیابی CSMA/CD متکی است تا ترافیک خط ارتباطات را منظم کند اولین بار توسط سه شرکت Digital, Intel , Xerox تولید شد با نام Ethernet OIX و بعد از چند سال به Ethernet II تغییر نام داد و بعد یک اترنت توسط IEEE طراحی شد با نام IEEE 802.3 .



Preamble : شروع فریم را نمایش میدهد .

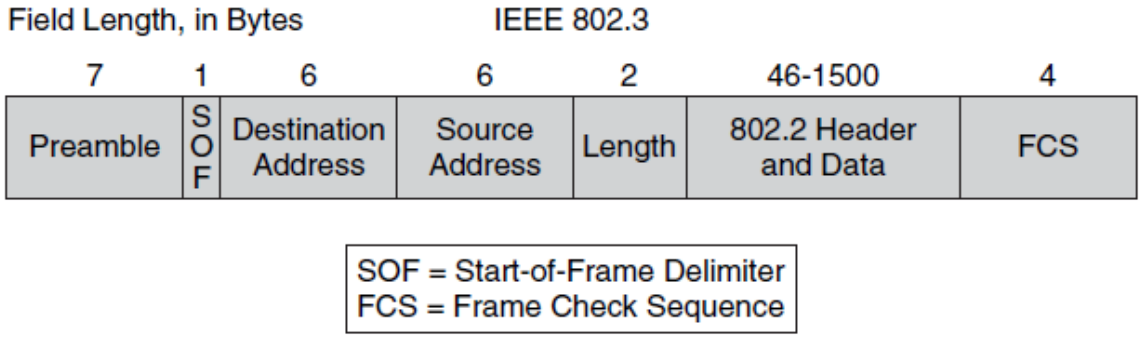
Destination Address : آدرس مبداء در آن نوشته می شود.

Source Address : آدرس مقصد در آن نوشته می شود.

Type : پروتکل لایه 3 در آن نوشته می شود .

FCS : نتیجه CRC در آن نوشته می شود .

فریم IEEE 802.3 :



Length : فقط طول Data در آن نوشته می شود .

نکته :

Ethernet II در لایه Data Link قرار دارد .

در اترنت IEEE 802.3 لایه Data Link به دو قسمت زیر تقسیم می شود :

LLC : Logical Link Control ====== IEEE 802.2

MAC : Media Access Control ====== IEEE 802.3

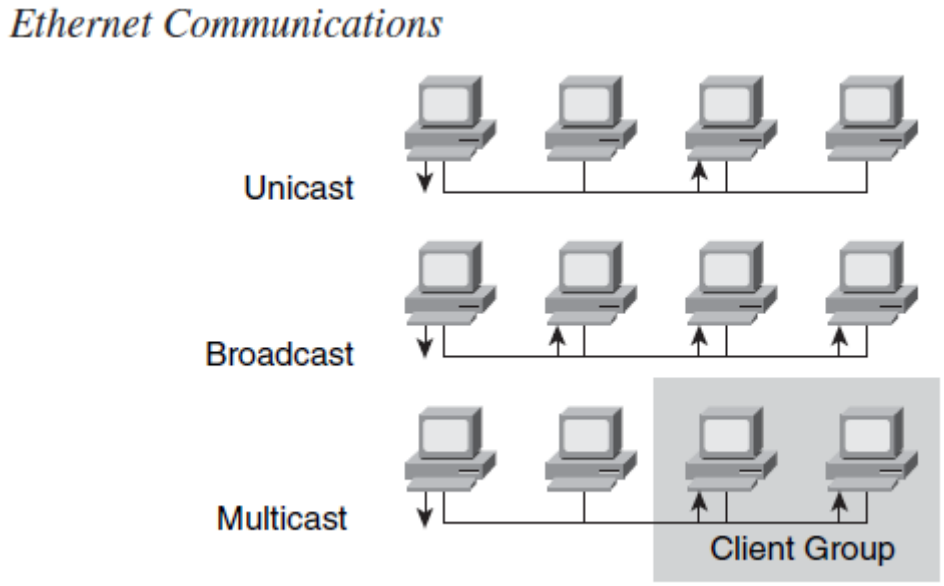
کارهایی که در لایه 2 انجام می شود :

- Framing
- Error-Detection
- Aribittration
- Addressing

انواع ارتباطات :

1. Simplex : یک طرفه = مانند = TV
2. Half Duplex : دو طرفه = مانند = بی سیم
3. Full Duplex : دو طرفه = مانند = تلفن

انواع ارتباطات از نظر نوع مخاطب :



نکته : Broadcast از یک شبکه به شبکه دیگر نمی رود .

IP Broadcast : FFFFFFFFFFFF Subnet mask : 255.255.255.255

لایه 3 :

مهمترین وظیفه لایه 3 آدرس دهی و مسیر یابی است .

IP : Internet Protocol

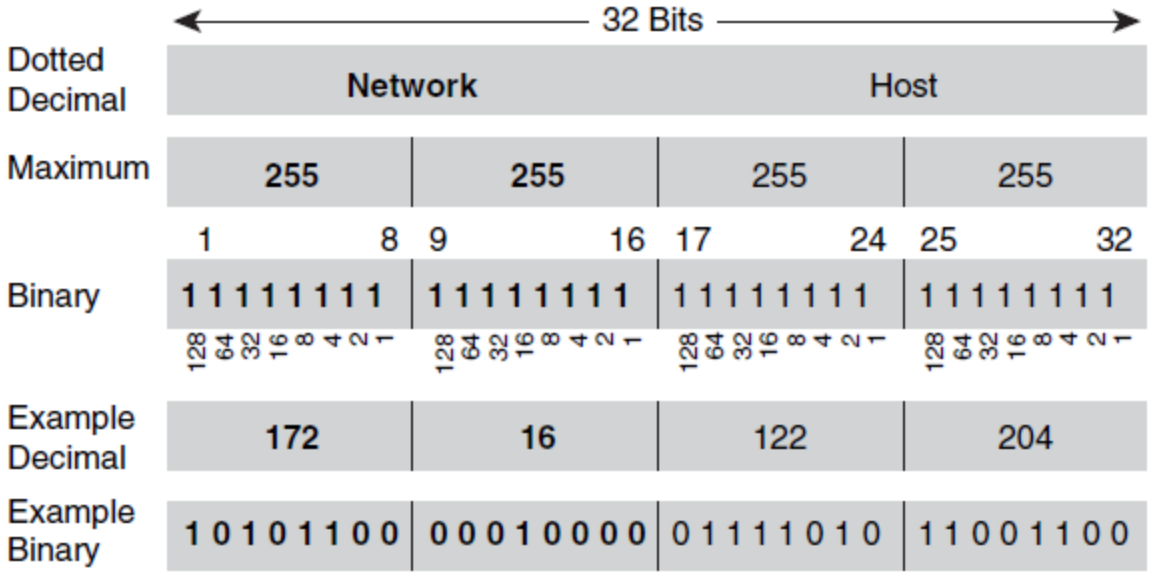
هر IP دارای ساختار 32 بیتی است . شامل دو بخش زیر است :

IP = Network ID + Hast ID

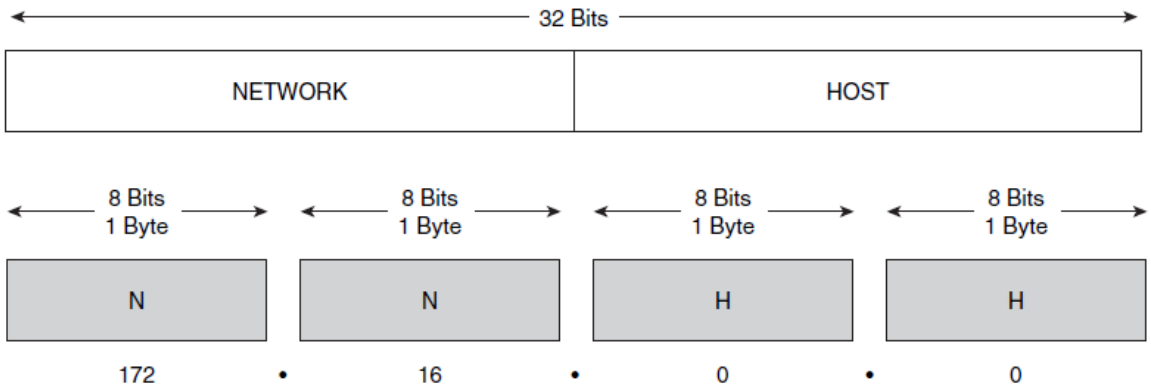
ID : Identifier ===== شناسه

همه آدرس های IP بصورت ترکیبی از اعداد دهدهی 1 بایتی (8 بیتی) و نقطه ای مابین آنها , مثلا به صورت 192.168.100.25 نوشته می شود و به علت آنکه هر عدد با 1 بایت (8 بیت) توصیف می شود , این عددها می توانند بین 0 تا 255 باشند .

IP Address Format



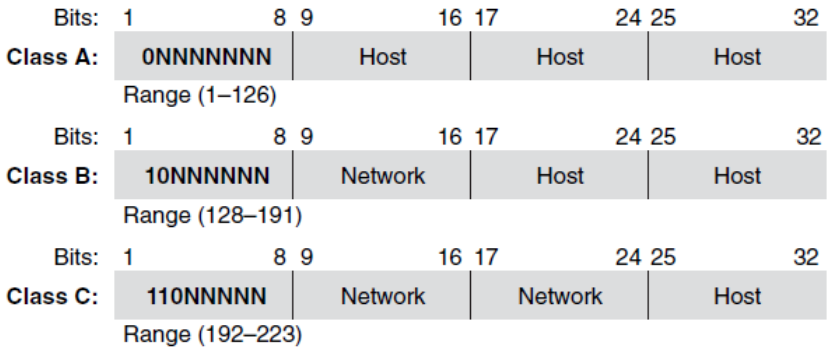
هر IP از چهار بخش 8 بیتی که به هر بخش یک Octet گفته می شود تشکیل شده است . برای اینکه تشخیص بدهیم که IP موجود در کدام کلاس است فقط به Octet اول توجه می کنیم .



کلاس های IP :

اگر octet اول اعداد زیر باشد کلاس های زیر تشکیل می شود :

Address Classification



Class D : Range (224 – 239)

Class E : Range (240 – 255)

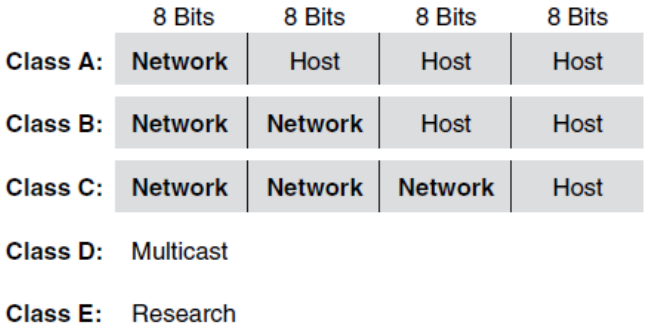
در کلاس A از 0 و 127 نمی توانیم استفاده کنیم . از همه IPهای کلاس های B , C می توانیم استفاده کنیم . از کلاس D برای آدرس دهی Multicastها استفاده میشود و کلاس E رزرو شده است و اصلا نمی توانیم استفاده کنیم .

IPهای رزرو شده :

0 مانند 0.1.2.3

127 مانند 127.0.0.1

Address Classes



نکته :

برای همه کلاس ها دو حالت 0 و 1 در تعداد Hostها کم می شود .

10.0.0.0 = 0 10.255.255.255 = 1

Subnet Mask :

مشخصه ای است که تمایز بین دو قسمت Host و Network را در IP مشخص می کند یا به عبارت دیگر قسمت Host را از قسمت Network جدا می کند . در Subnet Mask قسمت Host با عدد صفر و قسمت Network با عدد 1 نشان داده می شود .

مثال :

IP ==== 192.168.1.5

Subnet Mask ==== 255.255.255.0

حالت هایی که می توانیم Subnet Mask را بنویسیم :

128	64	32	16	8	4	2	1		
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

شیوه نمایش :

A.B.C.D/X X : نشان دهنده تعداد بیت های Network در آن کلاس است

مثال : 10.0.0.1/8 === A

192.168.1.5/24 === C 172.16.1.5/16 === B

Single Length Subnet Mask :

شبکه هایی که فقط از یک Subnet Mask استفاده می کنند SLSM گفته می شود .

Variable Length Subnet Mask :

شبکه هایی که از چندین Subnet Mask استفاده می کنند VLSM گفته می شود .

IP Addressing and Subnetting

Network and Host Boundaries

Address Class	Network Bytes	Host Bytes	Beginning Bit Values	Addresses (First Octet)
A	1 (8 bits)	3 (24 bits)	0	1–126; 0 and 127 are reserved
B	2 (16 bits)	2 (16 bits)	10	128–191
C	3 (24 bits)	1 (8 bits)	110	192–223
D	N/A	N/A	1110	224–239
E	N/A	N/A	11110	240–254; 255 is reserved

اگر یک IP را به ما بدهند و از ما بخواهند که این IP را به چندین شبکه تقسیم کنیم بسته به کلاس IP و قسمت Network و قسمت Host آن میتوانیم به چندین شبکه تقسیم کنیم . در هر کلاس با تغییر قسمت Host آن IP میتوانیم به شبکه های متعددی تقسیم کنیم . همانطور که می دانید هر actet از 8 بیت تشکیل شده است و با تغییر این بیت ها Subnetهای زیر به دست می آید :

Valid Subnet Mask Values in an Octet

00000000 = 0	11100000 = 224	11111100 = 252
10000000 = 128	11110000 = 240	11111110 = 254
11000000 = 192	11111000 = 248	11111111 = 255

برای مثال با این IP : 192.168.1.0 /24 میخواهیم 4 شبکه بسازیم و در هر شبکه 60 کامپیوتر قرار دهیم و آدرسدهی کنیم .

- Dotted-decimal 192.168.1.0 255.255.255.0
- Number of networking bits 192.168.1.0/24
- Hexadecimal 192.168.1.0 0xFFFFFF00
- Binary 192.168.1.0 11111111111111111111111100000000

همانطور که در حالت Binary مشاهده میکنید در actet چهارم از هشت بیت که همه 0 هستند تشکیل شده است و اگر به Number of networking نگاه کنیم 24/ است . یعنی ما میتوانیم از 192.168.1.0 تا 192.168.1.255 زیرشبکه داشته باشیم . چون ما میخواهیم 4 شبکه بسازیم پس 2 بیت از Host را لازم داریم که که چهار حالت Binary به صورت زیر به وجود بیاید :

192.168.1.0 / 24 : . /24 _ _ _ _ _ _ _ _

192.168.1.0 / 26 : ._ _ / 26 _ _ _ _ _ _

00 : 192.168.1.0 / 26

01 : 192.168.1.64 / 26

10 : 192.168.1.128 / 26

11 : 192.168.1.192 / 26

Host	Network Address	Host Address	Broadcast Address
62 Host	192.168.1.0	1 – 62	192.168.1.63
62 Host	192.168.1.64	65 – 126	192.168.1.127
62 Host	192.168.1.128	129 – 190	192.168.1.191
62 Host	192.168.1.192	193 – 254	192.168.1.255

همانطور که مشاهده میکنید 4 شبکه که هر کدام با Host = 64 ساخته شد دقت کنید که در هر شبکه یک IP برای Network Address و یک IP برای Broadcast Address مورد استفاده قرار میگیرد پس از Host = 62 میتوانیم استفاده کنیم برای آدرسدهی کامپیوترها .

برای IP Addressing و Subnetting از فرمول های زیر نیز میتوانید استفاده کنید :

- 2^S >= number of networks you need (*S* represents subnet bits)
- $2^H - 2$ >= number of hosts on your largest segment (*H* represents host bits)
- *S* + *H* <= total number of host bits you have for a class of address

مثال : با IP = 192.168.1.0 / 24 شبکه زیر را آدرسدهی کنید :

7 شبکه با Host = 30 و 7 شبکه با Host = 2

Network = 7 , Host = 30 : 7 * 30

2^H-2 ≥ Host : 2^H -2 ≥ 30 : H = 5

2^S ≥ Network : 2^S ≥ 7 : S = 3

S + H ≤ Bit Number : 3 + 5 ≤ 8

از 8 بیت ، actet چهارم 3 بیت را جدا میکنیم تا 7 شبکه با 30 کامپیوتر را IP بدهیم .

Network = 7 , Host = 2 : 7 * 2

2^H - 2 ≥ Host : 2^H - 2 ≥ 2 : H = 2

2^S ≥ Network : 2^S ≥ 7 : S = 3

S + H ≤ Bit Number : 3 + 2 ≤ 5

از 5 بیت باقیمانده actet چهارم 3 بیت دیگر را جدا میکنیم تا 7 شبکه با 2 کامپیوتر را IP بدهیم.

192.168.1.0 / 24 ⟶ 192.168.1./24 _ _ _ /27 _ _ _ _ _

Net 1 ⟶ 000 : 192.168.1.0 / 27

Net 2 ⟶ 001 : 192.168.1.32 / 27

Net 3 ⟶ 010 : 192.168.1.64 / 27

Net 4 ⟶ 011 : 192.168.1.96 / 27

Net 5 ⟶ 100 : 192.168.1.128 / 27

Net 6 ⟶ 101 : 192.168.1.160 / 27

Net 7 ⟶ 110 : 192.168.1.192 / 27

⟶ 111 : 192.168.1.224 / 27 ⟶ 192.168.1.111 / 27 _ _ _ / 30 _ _

Net 8 ⟶ 000 : 192.168.1.224 / 30

Net 9 ⟶ 001 : 192.168.1.228 / 30

Net 10 ⟶ 010 : 192.168.1.232 / 30

Net 11 ⟶ 011 : 192.168.1.236 / 30

Net 12 ⟶ 100 : 192.168.1.240 / 30

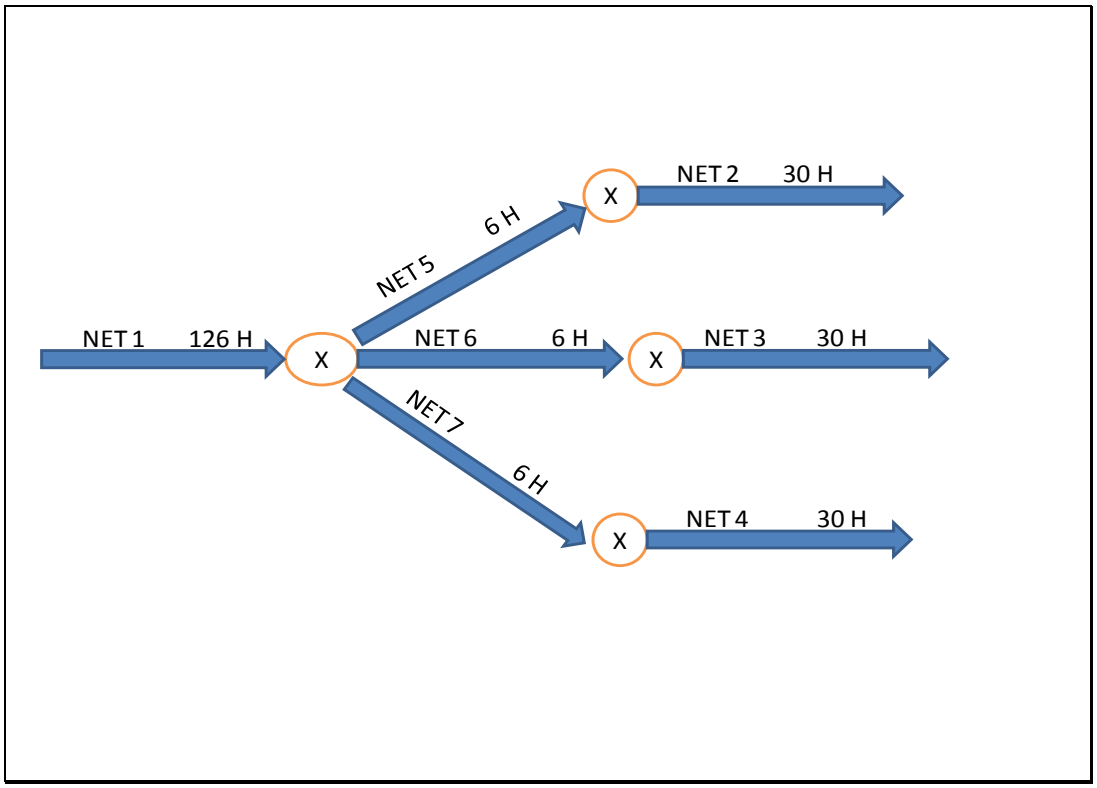
Net 13 ⟶ 101 : 192.168.1.244 / 30

Net 14 ⟶ 110 : 192.168.1.248 / 30

⟶ 111 : 192.168.1.252 / 30

از Net 1 تا Net 7 هر Net دارای 32 عدد IP و از Net 8 تا Net 14 هر Net دارای 4 عدد IP است که در هر Net یکی از IPها برای Network Address و یکی دیگر از IPها برای broadcast استفاده میشود .

مثال : شبکه زیر را آدرس دهی کنید .



یک شبکه با Host = 126 و 3 شبکه با Host = 30 و 3 شبکه با Host = 6 را آدرسدهی کنید :

1 Network * 126 Host

3 Network * 30 Host

3 Network * 6 Host

IP : 192.168.2.0 / 24

192.168.2.0 / 24 ⟶ 192.168.2.-/25-------

Net 1 : 0 ⟶ 192.168.2.0 / 25

1 ⟶ 192.168.2.128 / 25 ⟶ 192.168.2.1/--/27-----

Net 2 : 00 ⟶ 192.168.2.128 / 27

Net 3 : 01 ⟶ 192.168.2.160 / 27

Net 4 : 10 ⟶ 192.168.2.192 / 27

11 ⟶ 192.168.2.224 / 27 ⟶ 192.168.2.11/--/29----

Net 5 : 00 ⟶ 192.168.2.224 / 29

Net 6 : 01 ⟶ 192.168.2.230 / 29

Net 7 : 10 ⟶ 192.168.2.236 / 29

11 ⟶ 192.168.2.242 / 29

جدول Subnet Mask های کلاس A :

در این جدول Subnet Mask و Networking Bits و تعداد Host هایی که میتوانیم در کلاس A استفاده کنیم را نشان میدهد .

Valid Subnet Masks for Class A Networks

Subnet Mask	Networking Bits	Number of Subnets	Number of Hosts per Subnet
255.255.255.252	/30	4,194,304	2
255.255.255.248	/29	2,097,152	6
255.255.255.240	/28	1,048,576	14
255.255.255.224	/27	524,288	30
255.255.255.192	/26	262,144	62
255.255.255.128	/25	131,072	126
255.255.255.0	/24	65,536	254
255.255.254.0	/23	32,768	510
255.255.252.0	/22	16,384	1022
255.255.248.0	/21	8192	2046
255.255.240.0	/20	4096	4094
255.255.224.0	/19	2048	8190
255.255.192.0	/18	1024	16,382
255.255.128.0	/17	512	32,766
255.255.0.0	/16	256	65,534
255.254.0.0	/15	128	131,070
255.252.0.0	/14	64	262,142
255.248.0.0	/13	32	524,286
255.240.0.0	/12	16	1,048,574
255.224.0.0	/11	8	2,097,150
255.192.0.0	/10	4	4,194,302
255.128.0.0	/9	2	8,388,606
255.0.0.0	/8	1	16,777,216

جدول Subnet Mask های کلاس B و C :

در این جدول Subnet Mask و Networking Bits و تعداد Host هایی که میتوانیم در کلاس B و C استفاده کنیم را نشان میدهد .

Valid Subnet Masks for Class B Networks

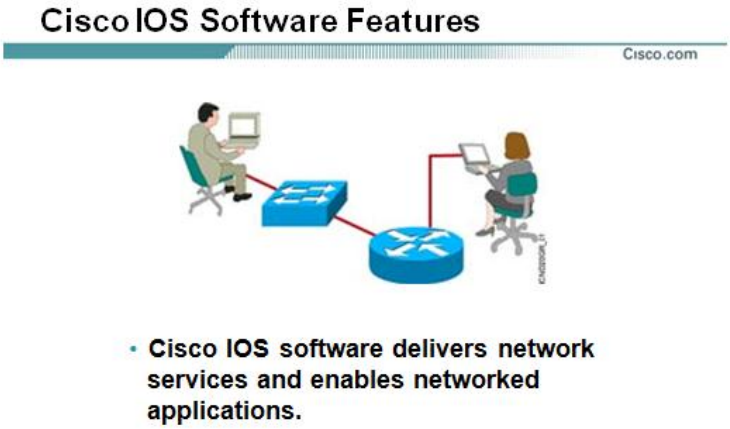
Subnet Mask	Networking Bits	Number of Subnets	Number of Hosts per Subnet
255.255.255.252	/30	32,768	2
255.255.255.248	/29	8192	6
255.255.255.240	/28	4096	14
255.255.255.224	/27	2048	30
255.255.255.192	/26	1024	62
255.255.255.128	/25	512	126
255.255.255.0	/24	256	254
255.255.254.0	/23	128	510
255.255.252.0	/22	64	1022
255.255.248.0	/21	32	2046
255.255.240.0	/20	16	4094
255.255.224.0	/19	8	8190
255.255.192.0	/18	4	16,382
255.255.128.0	/17	2	32,764
255.255.0.0	/16	1	65,534

Valid Subnet Masks for Class C Networks

Subnet Mask	Networking Bits	Number of Subnets	Number of Hosts per Subnet
255.255.255.252	/30	64	2
255.255.255.248	/29	32	6
255.255.255.240	/28	16	14
255.255.255.224	/27	8	30
255.255.255.192	/26	4	62
255.255.255.128	/25	2	126
255.255.255.0	/24	1	254

Cisco IOS

Internetwork Operating System (IOS)



IOS :

Internetwork Operating System (IOS) هسته مرکزی روتر و بیشتر سوئیچ های سیسکو می باشد . در واقع سیستم عامل روترها و سوئیچ های 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

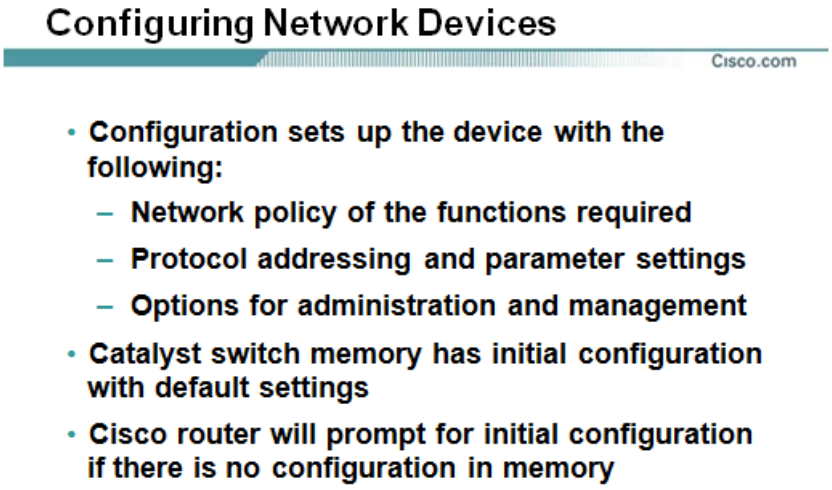
Set UP Mode :

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 . در واقع 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 نخواهد بود و برای تنظیم بیشتر می بایست به Mode دیگری مراجعه کرد . همچنین می توانید به جای پاسخ دادن به این سوالات مستقیما وارد Set up Mode شوید و در هنگام نیاز این تنظیمات را انجام دهید .

(Common-Line Interface) :

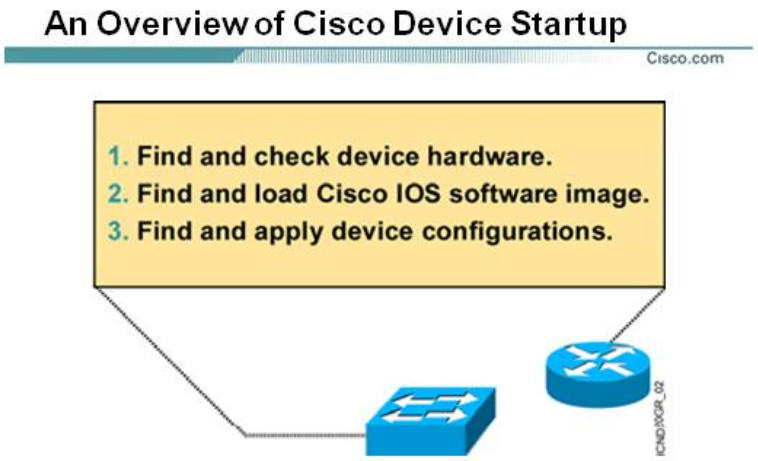
CLI جایگاهی است که می توانید تنظیمات بیشتری را روی روتر و سوئیچ انجام دهید . CLI یک محیط Text Base می باشد به طوری که User در این محیط فرامین مورد نظرش را Type می کند .



تنظیمات تجهیزات شبکه :

تنظیم یک Device جهت کار در شبکه 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 شود , Setup Mode اولین Mode ایی می باشد که با آن مواجه می شوید .



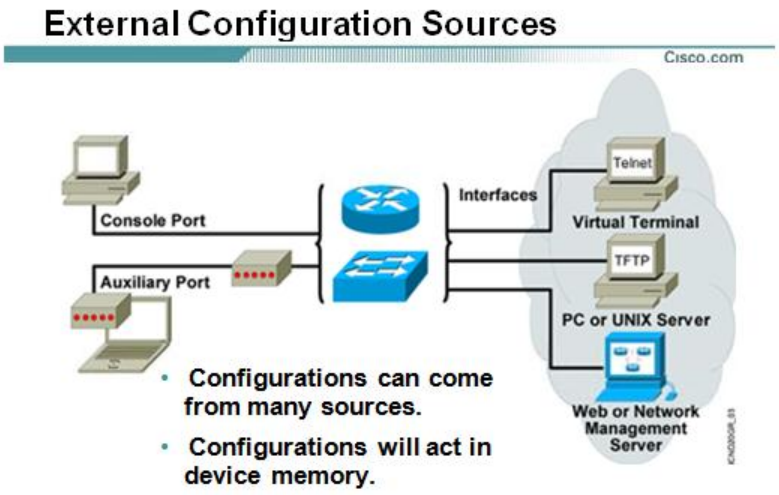
مروری بر نحوه راه اندازی سخت افزارهای سیسکو :

به طور کلی Deviceهای شرکت Cisco از لحظه ای که روشن می شوند تا آمادگی برای شروع کار 3 گام را پشت سر می گذارد .

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

در گام دوم پیدا کردن IOS می باشد .

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



راه های دسترسی به تجهیزات سیسکو :

برای دسترسی به روتر و سوئیچ پنج روش وجود دارد . سه روش جهت دسترسی به CLI و یک روش جهت ارتباط بین TFTP Server و تجهیزات 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

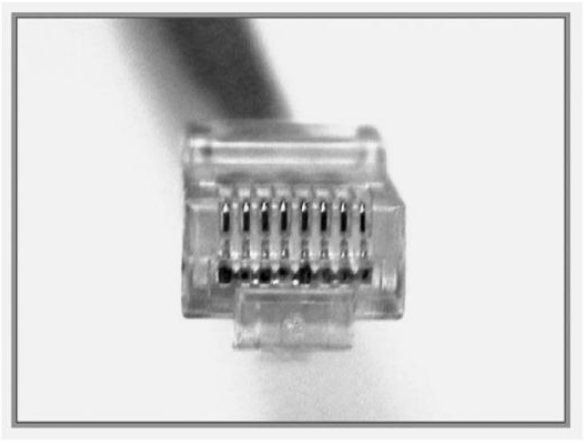
Concole Port :

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 و سوئیچ را به یک PC متصل و به کمک نرم افزار Hyper Terminal با روتر و سوئیچ ارتباط برقرار کرده و آن را تنظیم می کنید. بعد از تنظیم روتر و 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.

RJ-45 Connector



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 .

Telnet:

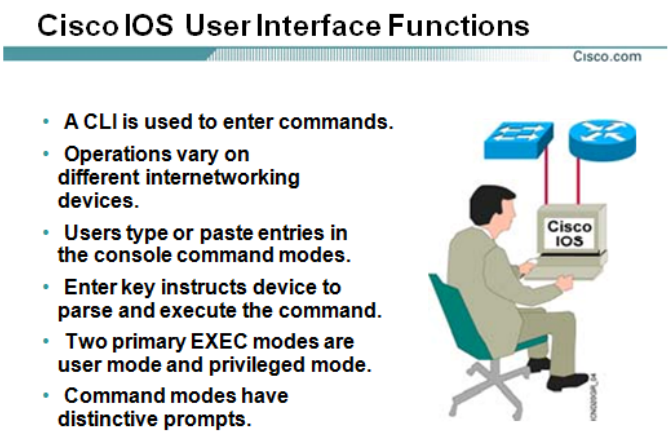
در صورتی که هنگام تنظیم کردن اولیه روتر و سوئیچ آدرسی (IP Address) را به آن نسبت داده باشید براحتی می توانید در یک شبکه TCP /IP به روتر یا سوئیچ دسترسی پیدا کرده و آن را تنظیم کنید . این ارتباط از طریق سرویس Telnet و استفاده از پروتکل Telnet می باشد . بنابراین در صورت داشتن آدرس (IP Address) روتر یا سوئیچ و همچنین فعال بودن امکان دسترسی از طریق Telnet , میتوانید با telnet کردن به آنها تنظیمات مورد نظرتان را روی آنها اعمال کرد .

TFTP :

یکی دیگر از راه های ارتباطی , ارتباط بین تجهیزات سیسکو با TFTP Server می باشد . بنابراین می توان با بهره گرفتن از پروتکل TFTP , تنظیمات و IOS روتر و یا سوئیچ را در جای دیگری در شبکه و در واقع در یک TFTP Server نگهداری کرد .

Web Browser :

آخرین راه ارتباط از طریق Web Browser می باشد .این ارتباط زمانی امکان پذیر است که Device سیسکو جهت کار در شبکه TCP / IP آماده شده باشد . این به دان 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 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 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.

بعد از Boot شدن IOS و Lode 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 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 یا سوئیچ از این مد استفاده می کنیم :

Hostname > Show Flash

Privileged Mode :

این Mode جایگاهی با 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 خاص با داشتن پسورد به این Mode دسترسی پیدا کنند . در این Mode دسترسی به تنظیمات و مشاهده و تغییر تنظیمات امکان پذیر می باشد .

در این مد 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 Privileged Mode خواهید شد :

Hostname > enable

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

Hostname #

برای خارج شدن از این مد فرمان زیر را وارد می کنید :

Hostname # exit

Switch

سوئیچ سخت افزاری است در لایه دوم از مدل OSI که وظیفه اصلی آن هدایت فریم ها بر اساس MAC Address در شبکه می باشد . سوئیچ می تواند بدون تنظیم کردن در داخل شبکه استفاده شود و عملیات سوئیچینگ را انجام دهد.سوئیچ های سری 2950 دارای پورت های اترنت (100 Mbps) و برخی از مدل های این سری دارای پورت های اترنت گیگا بیت (1000 Mbps) نیز می باشد . سیستم عامل سوئیچ تحت عنوان IOS نقش واسط نرم افزاری بین سخت افزارها و کاربر را بازی می کند . می توان نمای ظاهری سوئیچ های 2950 را به سه دسته تقسیم کرد :

1. پورت ها

بسته به اینکه سوئیچ 2950 چه مدلی باشد نوع پورت ها و تعداد آنها متفاوت می باشد به طور مثال سوئیچ 2550G-12 دارای دو پورت گیگا بیت مبتنی بر فیبر نوری و 12 پورت اترنت میباشد .

2. LED

شامل چهار دسته می شوند :

- Port Status LED
- Port Mode LED
- System LED
- Power Supply LED

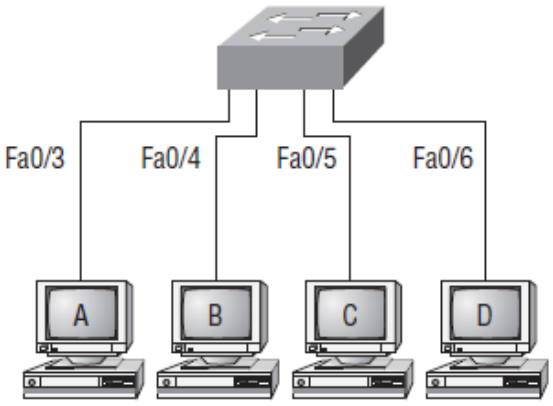
3. Mode Button

ویژگی سوئیچ :

ویژگی سوئیچ این است که مثلا اگر PC1 اطلاعاتی برای PC 4 ارسال کند سوئیچ دقیقا به آدرس مقصد PC4 اطلاعات PC1 را می فرستد . در شبکه ای که از سوئیچ استفاده می شود Collision رخ نمیدهد چون یک سیم برای ارسال و یک سیم برای دریافت اطلاعات هر PC دارد . سوئیچ برای هر پورت یک بافر (حافظه) دارد که اگر همزمان دو PC برای یک PC دیگر اطلاعات ارسال کنند سوئیچ اطلاعات یکی از PCها را در بافر پورتی که به PC مقصد متصل است ذخیره می کند و اطلاعات PC دیگر را از طریق همان پورت به PC مقصد می رساند و بعد از ارسال کامل اطلاعات PC اول , اطلاعات PC دوم را ارسال میکند . در سوئیچ , CSMA / CD در پورتها خاموش است چون تصادم رخ نمی دهد ولی در Hub , CSMA / CD در پورت ها و Hub روشن است .

Port Table :

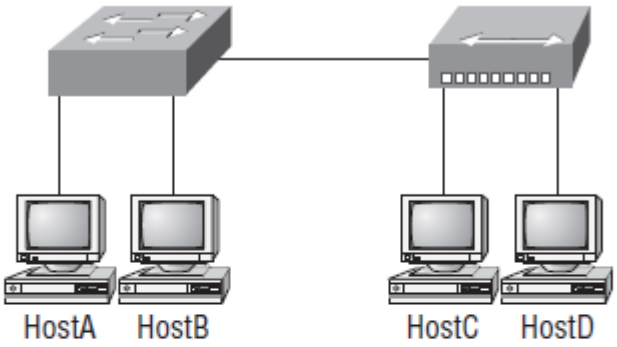
در حافظه سوئیچ یک جدول قرار دارد که برای ذخیره کردن MAC دستگاهی که به پورتی از سوئیچ متصل است مورد استفاده قرار میگیرد که به دو صورت Static یا Dynamic این جدول پر می شود . نام جدول MAC-Address Table یا Port Address Table است .




```
Switch#sh mac address-table
Vlan    Mac Address       Ports
----    -----------       -----
   1    0005.dccb.d74b    Fa0/4
   1    000a.f467.9e80    Fa0/5
   1    000a.f467.9e8b    Fa0/6
```

سوئیچ برای بار اول که روشن می شود جدول حافظه سوئیچ خالی است در حالت Static باید یکی یکی Portها را برای هر MAC مشخص کنیم ولی در حالت Dynamic این مراحل انجام می پزیرد :

اول از PC A که به یکی از پورت های سوئیچ متصل است فریمی برای PC D فرستاده می شود فریم که به سوئیچ برسد , سوئیچ میداند که در آن پورت PC A قرار دارد و MAC آن را در جدول خود ذخیره می کند بعد طبق آدرس مقصد که در فریم ارسالی از PC A گرفته و چون این آدرس را در جدول خود ندارد پس بر روی همه پورت های خود که به PCهای دیگری وصل هستند به غیر از پورتی که PC A به آن متصل است ارسال می کند , PCها به قسمت آدرس مقصد فریم نگاه می کنند اگر آدرس مقصد با PC یکی نباشد PC فریم را Break میکند ولی اگر آدرس یکی باشد فریم را دریافت کرده و یک پاسخ به PC A ارسال می کند پس سوئیچ میداند که PC D نیز بر روی کدام پورت قرار دارد و در جدول ذخیره می کند . این کار را برای PCهای دیگر نیز تکرار میکند تا جدول پورت خود را تکمیل کند .



MAC Address	Type	Ports
0005.dccb.d74b	DYNAMIC	Fa0/1
000a.f467.9e80	DYNAMIC	Fa0/1
000a.f467.9e8b	DYNAMIC	Fa0/4
000a.f467.9e8c	DYNAMIC	Fa0/3

نکته : سوئیچ دو مرحله دارد :

1. Learning
2. Forwarding

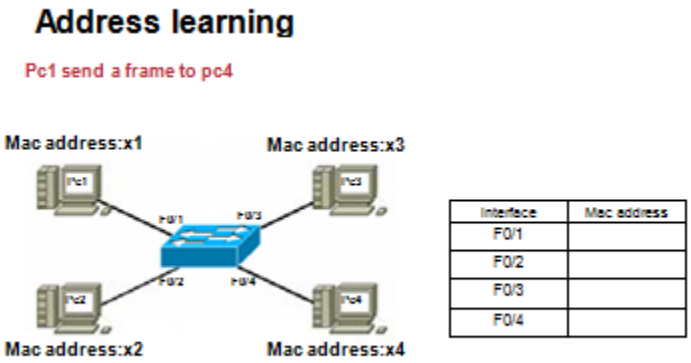
سوئیچ برای هر پورت می تواند تا حدود 8000 MAC Address, را Learn کند .

کل مکانیزم به این صورت است که ابتدا یک Frame از PC به Switch ارسال می شود , سوئیچ آن پورت را Learn می کند اگر در MAC Table وجود داشته باشد بعد از 300 ثانیه Update می شود , اگر نداشت برای اولین بار آن را Learn می کند سپس اگر مقصد را در جدول داشت به آن Forward میکند و اگر نداشت به تمام پورتهایی که به PC وصل هستند Broadcast (منتشر) میکند .

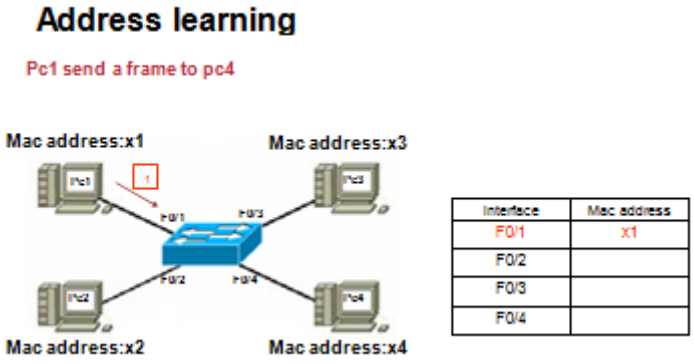
اگر ارتباطی قطع شود سوئیچ بعد از مدت معینی MAC Address آن پورت را از جدول پاک می کند .

مراحل Address Learning :

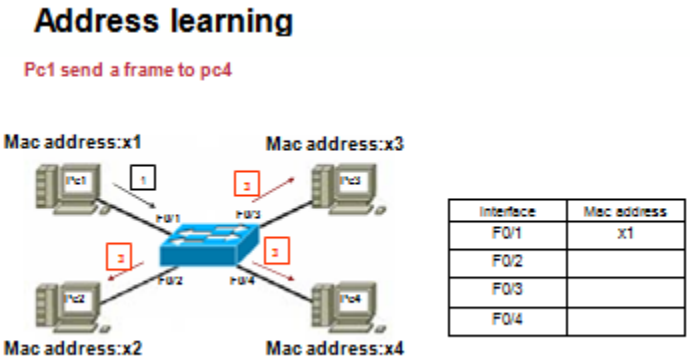
1 : در شکل زیر MAC Table خالی بوده زیرا فرض شده است که سوئیچ هیچ فریمی را دریافت نکرده است :



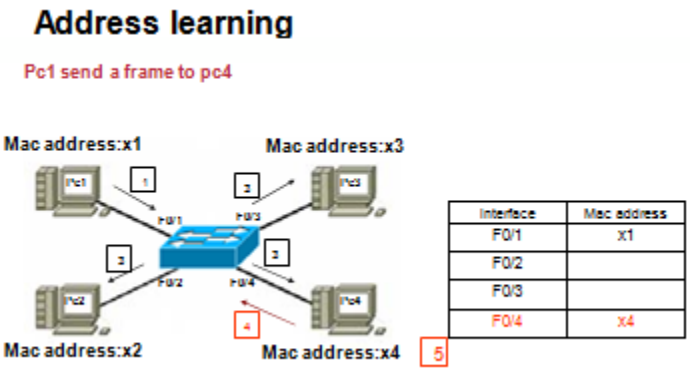
2 : فرض کنید PC 1 قصد ارتباط با PC 4 را داشته باشد . بنابراین فریمی را به سوئیچ ارسال می کند . از آنجا که سوئیچ برای بار اول از PC 1 فریمی دریافت می کند بنابراین آدرس PC 1 و شماره پورتی از سوئیچ که به PC 1 متصل است را در MAC Table خود ذخیره می کند .



3 : چون سوئیچ در جدول خود آدرس PC 4 را ندارد و نمی داند باید از طریق کدام پورت به آن دسترسی پیدا کند بنابراین سوئیچ فریم را به تمام پورت هایش به جز پورتی که به PC 1 متصل است ارسال می کند . در واقع با Broadcast کردن از Deviceهایی که به پورت هایش متصل هستند می پرسد که آدرس X4 مربوط به کیست ؟



4 : PC 4 که دارای آدرس سخت افزاری X4 می باشد به سوئیچ پاسخ می دهد و سوئیچ این آدرس و شماره پورتی که متصل به PC 4 می باشد را در MAC Table خود قرار میدهد.

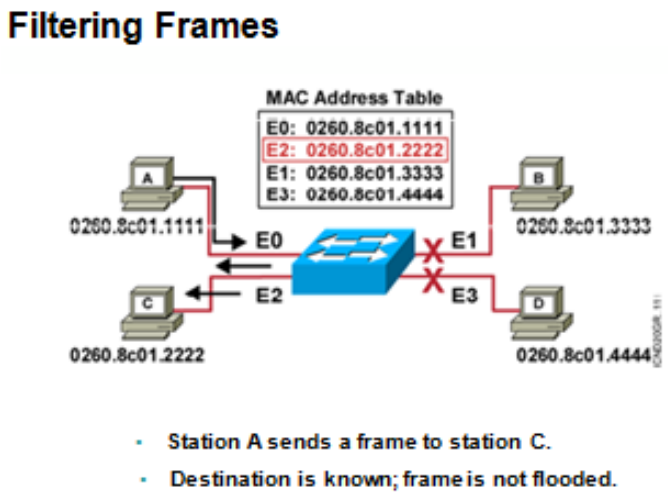


بنابراین بعد از گذشتن زمان اندکی این Table تکمیل می شود .

نکته :

سوئیچ برای تکمیل کردن MAC Table خود از مکانیزم Broadcast در شبکه ها استفاده می کند و بعد از تکمیل آن به صورت Unicast ترافیک را در شبکه منتقل می کند .

فیلتر شدن فریم ها :



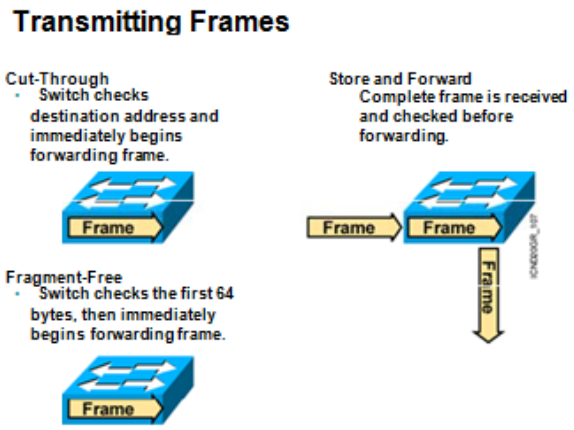
یکی از کارهای مهم دیگری که سوئیچ انجام می دهد Frame Filtering می باشد . این بدان معنی است که وقتی PC A فریمی را به سوئیچ ارسال کند که فریم فقط به پورت مشخصی که به PC مقصد متصل است ارسال می شود و به پورت های دیگر ارسال نمی شود .

سوئیچ زمانی قادر به فیلتر کردن فریم ها و ارسال آن به مقصد می باشد که MAC Table خود را تکمیل کرده باشد .

در مثال صفحه قبل : PC A فریمی را به PC C ارسال میکند . 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 پورت های دیگر ارسال نمی شود .

سوئیچ به کمک MAC Table خود عملیات فیلترینگ فریم ها را انجام می دهد . بنابراین , این Table می بایست دائما به روز شود تا بتواند فریم ها را بدرستی هدایت کند .

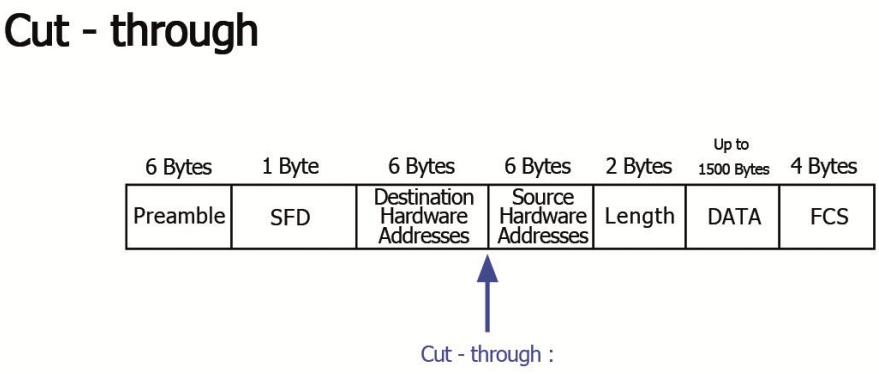
نحوه انتقال فریم ها توسط سوئیچ :



سوئیچ یکی از سه حالت را برای انتقال فریم در شبکه LAN استفاده می کند :

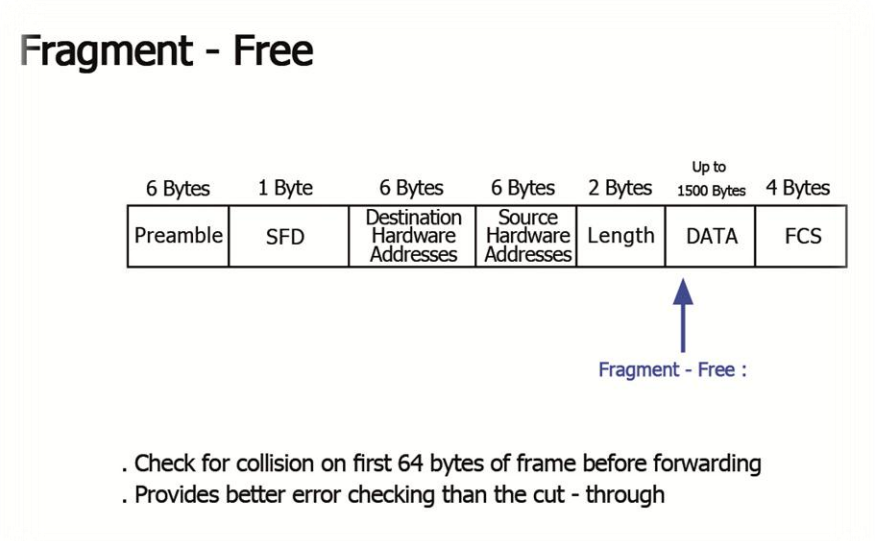
Cut-Through

در این روش به محض اینکه فیلد Destination از فریمی که توسط سوئیچ در حال دریافت است خوانده شد , فریم بدون هیچ اتلاف وقتی به سمت Destination ارسال می شود در این روش لزومی ندارد کل فریم توسط سوئیچ دریافت شود و سپس عملیات هدایت صورت گیرد . به محض اینکه سوئیچ از بیت های دریافتی بتواند Destination Address را تشخیص دهد به کمک MAC Table خود آن را به سمت مقصد هدایت می کند .



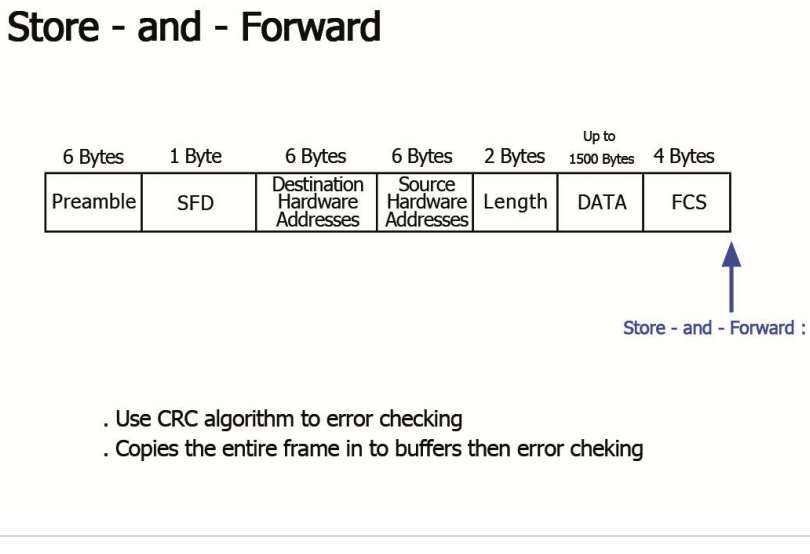
Fragment-Free

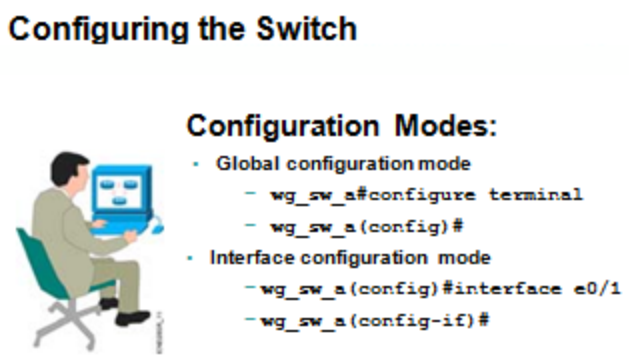
در این روش 64 بایت اول از فریم دریافتی خوانده می شود و از نظر نداشتن error چک می شود و سپس سوئیچ فریم را به سمت مقصد هدایت می کند . در صورتی که بخواهد Collisionایی رخ دهد معمولا در 64 بایت اول رخ میدهد بنابراین فریم های Fragment شده شناسایی شده و از ارسال آنها جلوگیری می شود .



Store and Forward

در این روش فریم به صورت کامل دریافت شده و سپس به سمت Destination هدایت میشود. ابتدا فریم به صورت کامل Buffer میشود و سپس در صورتی که بیت های این فریم به صورت کامل دریافت شد و فیلدهای Destination و FCS بررسی شود و همچنین در صورتی که الگوریتم CRC خطایی را مشخص نکند , فریم به سمت مقصد هدایت میشود . در صورتی که الگوریتم CRC خطایی را مشخص کند فریم Discard میشود .





پیکربندی سوئیچ 2950 :

با وارد کردن فرمان زیر در Enable Mode وارد Configuration Mode می شوید :

Switch # configure Terminal

بعد از وارد کردن فرمان فوق Command Prompt به صورت زیر تغییر میکند :

Switch (config) #

در مد config امکان تنظیمات کلی سوئیچ وجود دارد . با فرمان Exit از مد config خارج می شوید .

برای اینکه مستقیم از مد config به مد enable بروید یا دستور End را وارد می کنیم یا کلیدهای ctrl + z را میزنیم .

کلیدهای میانبر :

Ctrl + A : مکان نما به اول خط برمی گردد	Ctrl + R :خط فرمان را Refresh می کند
Ctrl + E : مکان نما به آخر خط می رود	Esc + B : مکان نما یک کلمه عقب می رود
Ctrl + F : مکان نما یک کارکتر به جلو میرود	Esc + F :مکان نما یک کلمه جلو می رود
Ctrl + B :مکان نما یک کارکتر به عقب میرود	$: یعنی قبل از این کارکتر نیز نوشته هست
Ctrl + D : یک کارکتر را پاک می کند	Up & Down OR Ctrl + P & Ctrl + N : فراخوانی فرامین از حافظه History
Ctrl + U :از جای مکان نما تا اول مد را پاک میکند	

فعال شدن Help به کمک علامت سوال (؟) :

برای دیدن لیست فرمان ها در یک Mode می توان از علامت سوال (؟) استفاده کرد . با وارد کردن (؟) , کلیه فرامین قابل اجرا در هر Mode که هستیم را نمایش می دهد .

در صورتی 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 کارکتر اول از یک فرمان را نوشته و سپس با زدن علامت ؟ فرمان هایی 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 :

```
Switch > e ?

Enable , exit
```

نکته : وقتی چند حرف از یک command را تایپ کنیم بعد با زدن کلید Tab همه فرمان نوشته میشود .

استفاده از Help در یک مثال :

تنظیم clock در enable mode :

```
Switch # clock  ?
   Set       set the time and date
Switch # clock   set   ?
    hh:mm:ss     Current  Time
Switch # clock   set   18 : 52 : 23     ?
    < 1 – 31 >       Day   of   the   month
      MONTH          Month  of  the  year
Switch # clock    set   18 : 52 : 23    11    jan    ?
    < 1993 – 2011 >   Year
Switch # clock    set   18 : 52 : 23    11    jan    2011   ?
     < CR >
```

با زدن دستور زیر می توانیم ساعت تنظیم شده را مشاهده کنیم :

Switch # show clock

: < CR >

Carriage Return : یعنی به آخر دستور رسیدیم یا دستور کامل است .

فرمان History :

History لیستی از آخرین فرامینی را که وارد کرده اید را فراخوانی می کند . به کمک فرمان زیر می توانید History و محتویات آن را مشاهده کنید .

Switch # show history

با این فرمان 10 دستور قبل را که اجرا کرده ایم را نمایش می دهد .

با فرمان زیر می توانیم از 0 تا 256 دستور را در History ذخیره کنیم :

Switch # Terminal history size 0 – 256

فرمان Version :

این فرمان برای 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 .

Switch # Show version

پیغام های خطا :

% Ambiguous Command : " e "

یعنی با کلمه e آپشن های متفاوتی داریم , فقط یک آپشن نیست .

% Unknown Command

یعنی همچین آپشنی وجود ندارد .

% Invalid input detected at ' ^ ' marker

یعنی با این علامت ' ^ ' نشان می دهد کجای کلمه آپشن مورد نظر را اشتباه تایپ کرده ایم.

% Incomplete Command

یعنی فرمان کامل نیست .

% Unrecognized Command

یعنی این فرمان را در این Mode نمی شناسد .

تغییر نام Switch :

Switch (config) # Hostname Cisco

Cisco (config) #

پیام روزانه :

Message of the day

پیغامی می باشد که در هر بار Login کردن به سوئیچ برای هر کاربر و برای هر ارتباط نشان داده می شود .

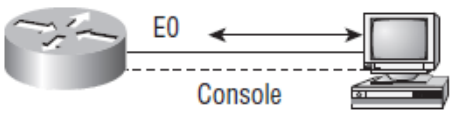
Switch (config) # Banner motd " Message "

پیام طولانی :

Switch (config) # Banner login " Message "

Switch (config) # Banner exec " Message "

Console Port



تنها راه ارتباط با سوئیچ یا روتر که بدون تنظیم می باشد استفاده از Console port است .

از دستور زیر برای وارد شدن به Console port استفاده می کنیم تا بتوانیم تنظیماتی روی console port انجام دهیم :

Switch (config) # line console 0

Switch (config – Line) #

مدت زمان برقراری ارتباط console با سوئیچ یا روتر بدون قطع شدن این ارتباط به صورت پیش فرض 10 دقیقه می باشد . به کمک دستور زیر می توانید مدت زمانی که این ارتباط برقرار می شود را به صورت نا محدود تعریف کنیم . در واقع اگر Packetیی برای مدت زمان طولانی از این اینترفیس ردوبدل نشود این ارتباط قطع نخواهد شد . اگر فقط عدد 0 را بنویسیم هیچ وقت ارتباط قطع نخواهد شد .

Switch (config – Line) # exec – timeout 0 0

یکی دیگر از مشکلاتی که ممکن است با آن مواجه شوید , این است که شما فرمانی را در Command prompt سوئیچ یا روتر 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 است را متوجه شوید. به کمک فرمان زیر می توانید به سوئیچ یا روتر بگویید پیام جدید را بعد از خروجی فرمان شما نمایش دهد :

Switch (config – Line) # logging synchronous

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 . دو روش برای دادن پسورد وجود دارد که به صورت زیر تنظیم می شود :

روش اول :

```
Switch ( config – Line ) # Password Cisco
Switch ( config – Line ) # login
```

روش دوم :

```
Switch ( config ) # Username Cisco Password Cisco
Switch ( config ) #line console 0
Switch ( config – Line ) #login local
```

با این روش در User Mode می توانیم افرادی را که با Usernameهای مختلف وارد شده اند و کار کرده اند را مشاهده و کنترل کنیم .

رمز دادن به Enable Mode :

برای برقراری امنیت هنگام وارد شدن به Privileged Mode استفاده می شود . هنگامی که در User Mode فرمان Enable را وارد کنیم این پسورد پرسیده می شود .

```
Switch ( 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 . برای اینکه کسی نتواند رمزهای ما را در show run ببیند میتوانیم از دستور زیر استفاده کنیم :

```
Switch ( config ) # enable Secret Cisco
```

یا

Switch (config) # Username Cisco Secret Cisco

Password و Secret همانند هم هستند با این تفاوت که در Secret , پسورد به صورت کد شده در حافظه های سوئیچ یا روتر ذخیره می شود و به صورت clear text نمایش داده نمی شود . دستور Secret بر دستور Password اولویت دارد .

از دستور زیر برای پنهان کردن کارکترهای Password استفاده می کنیم . پسوردها را به یک سری اعداد تبدیل می کند :

Switch (config) # Service Password – encryption

Interface ها و تنظیمات آنها :

به کمک فرمان زیر می توانیم وارد اینترفیس مورد نظر شده و آن را تنظیم کنیم :

Switch (config) # Interface type mod/num

Switch (config – if) #

Type :

در قسمت type نوع اینترفیس را مشخص می کنیم مثلا : Ethernet یا Fastethernet یا Gigabitethernet یا ...

Number :

در قسمت num شماره port یا اینترفیس مورد نظر نوشته می شود .

شماره اینترفیس در سوئیچ از 0/1 شروع می شود .

روشن یا خاموش کردن یک اینترفیس :

Switch (config) # Interface Fastehernet 0/1

روشن یا فعال می شود

Switch (config – if) # Shutdown

خاموش یا غیر فعال می شود

Switch (config – if) # No Shutdown

فرمان نمایش دادن وضعیت یک Port یا اینترفیس :

Switch # show Interface fastethernet 0/1

فرمان نمایش دادن وضعیت تمام Portها :

Switch # show Interface status

فرمان تغییر نام برای هر Pore :

توضیحی می باشد که برای هر اینترفیس می توان نوشت و برای مدیریت بهتر اینترفیس ها از آن استفاده می شود .

Switch (config) # Interface Fastehernet 0/1

Switch (config – if) # Description name

دستور انتخاب چند پورت :

دو روش وجود دارد :

روش اول برای انتخاب اینترفیس های غیر متوالی :

Switch (config) # Inteface range type num type num …

مثال :

Switch (config) # Inteface range Fastethernet 0/1 Fastethernet 0/3 Fastethernet 0/6 …

Switch (config – Range – if) #

روش دوم برای انتخاب اینترفیس های متوالی :

Switch (config) # Inteface range type num – num

مثال :

Switch (config) # Inteface range Fastethernet 0/1 – 5

Switch (config – Range – if) #

اینترفیس مجازی سوئیچ :

VLAN برگرفته از عبارت Virtual LAN یا LANهای مجازی می باشد که یکی از توانمندی های مربوط به سوئیچ است که به شما این امکان را می دهد که کامپیوترهای متصل به یک سوئیچ یا چندین سوئیچ را به صورت منطقی در گروه های خاص قرار دهید,به طوری که ترافیک این گروه ها از یکدیگر جدا شوند و در این حالت هر گروه یا هر VLAN تبدیل به یک حوزه Broadcast مجزا خواهد شد .

وارد VLAN 1 می شویم :

Switch (config) # Interface VLAN 1

VLAN را فعال می کنیم :

Switch (config – If) # no shutdown

VLAN 1 را آدرس دهی میکنیم :

Switch (config – If) # IP Address ip subnet mask

مثال آدرس دهی به VLAN 1 :

Switch (config – If) # IP Address 192.168.1.1 255.255.255.0

Telnet :

یکی از راه های دسترسی به سوئیچ یا روتر Virtual Terminal یا همان Telnet می باشد . 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 تنظیم Telnet باید 3 مرحله زیر را طی کنید :

1. Setting IP Address
2. User mode Security
3. Enable mode Security

مرحله اول به صورت بالا VLAN 1 را آدرس دهی می کنیم یعنی به سوئیچ یا روتر یک IP اختصاص می دهیم .

مرحله سوم را در صفحات قبلی توضیح داده ایم . باید به Enable mode پسورد بدهیم .

مرحله دوم به یکی از دو روش زیر صورت می گیرد :

روش اول :

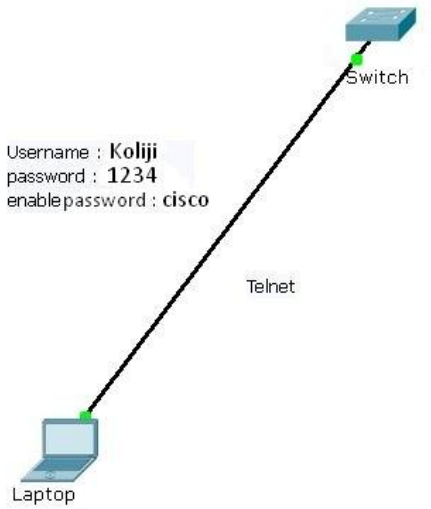
```
Switch ( config ) # Line Vty  0  15
Switch ( config – Line ) # Password  Cisco
Switch ( config – Line ) # Login
```

روش دوم :

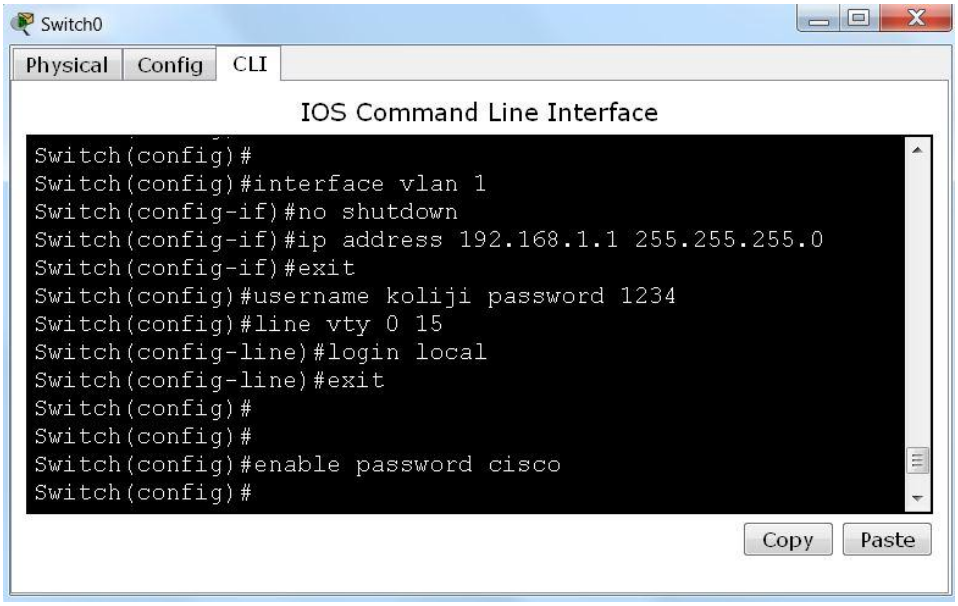
```
Switch ( config ) # Username  name  Password  password
Switch ( config ) # Line Vty  0  15
Switch ( config – Line ) # Login local
```

Vty: شماره Vty از 0 تا 4 یا 0 تا 15 است. یعنی تعداد Vty به منزله این است که به آن تعداد User میتوانند همزمان با اتصال Telnet به سوئیچ وصل شوند .

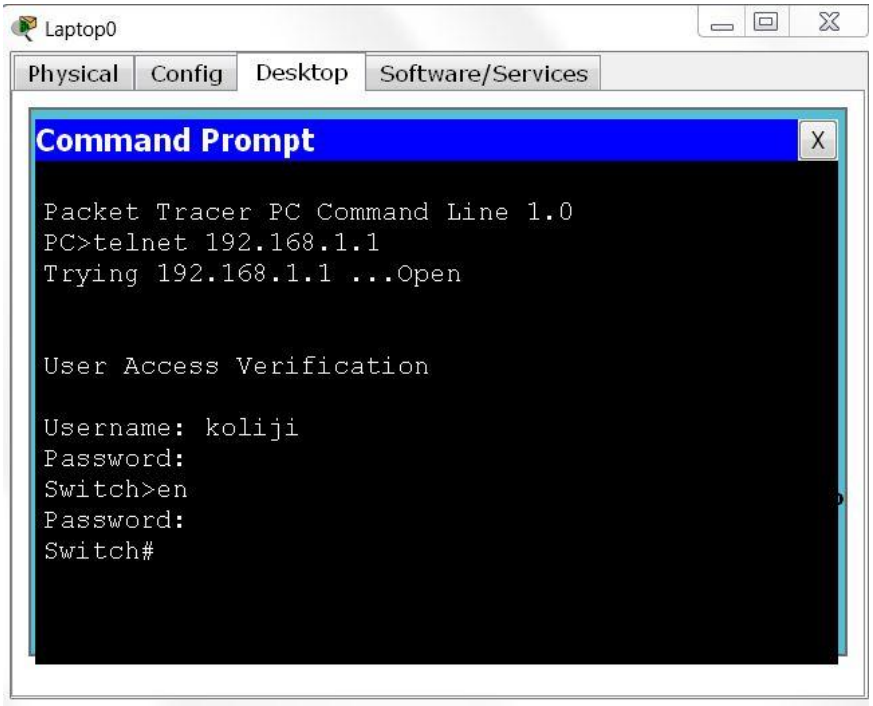
مثال : به شکل زیر نگاه کنید ، دستوراتی را که برای Telnet زدن لازم داریم را مطابق دستورات زیر وارد می کنیم :



دستوراتی که بر روی سوئیچ اعمال می کنیم :



دستور Telnet ip address را در command prompt کامپیوتر وارد می کنیم تا به سوئیچ telnet بزنیم :



IP address :

در دستور بالا ip address یی را می نویسیم که برای Vlan 1 تعریف کرده ایم .

نکته :

Protocol Telnet به صورت Text اطلاعات را میفرستد و امنیت ندارد ولی SSH (Secur Shell) اطلاعات را رمزگزاری میکند و امنیت بیشتری دارد .این پروتکل ورژن های مختلفی دارد ولی مشهورترین و پرکاربردترین آنها ورژن های 1 و 1.5 و 2 هستند .

SSH :

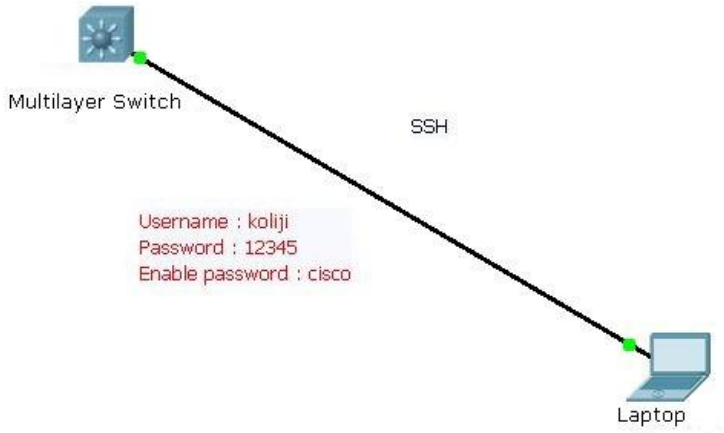
مراحل تنظیم SSH :

1. IP Mode Assignment
2. User Mode Security
3. Enable Mode Security
4. IP Domain-name Cisco.com
5. Crypto Key Generate Rsa
6. IP SSH Version 2

1. IP سوئیچ را Set می کنیم
2. User Mode را با دستور Username و Password , پسورددهی میکنیم .
3. به Enable Mode پسورد اختصاص می دهیم .
4. دستور IP domain-name را اجرا میکنیم که حتما باید نام کلید پسوند .com داشته باشد .
5. با دستور Crypto key generate rsa کلید را می سازیم
6. با دستور show crypto key mypubkey rsa نگاه میکنیم ببینیم کلید ساخته شده است یا نه .
7. ورژن SSH را تعیین می کنیم .
8. یک بار Ping می کنیم بعد با نرم افزار Putty یا Secure CRT از طریق SSH به سوئیچ وصل می شویم .
9. در محیط command prompt در PC دستور IP Username –L SSH را می نویسم و Enter می زنیم .

با انجام مراحل بالا از کامپیوتر می توانیم به سوئیچ وصل شویم از طریق پروتکل SSH و تنظیمات خود را بر روی سوئیچ انجام دهیم .

مثال :
به شکل زیر نگاه کنید ، دستوراتی را که برای SSH زدن لازم داریم را مطابق دستورات زیر وارد می کنیم :



دستورات زیر را بر روی سوئیچ اعمال می کنیم :

Multilayer Switch0

Physical | Config | CLI

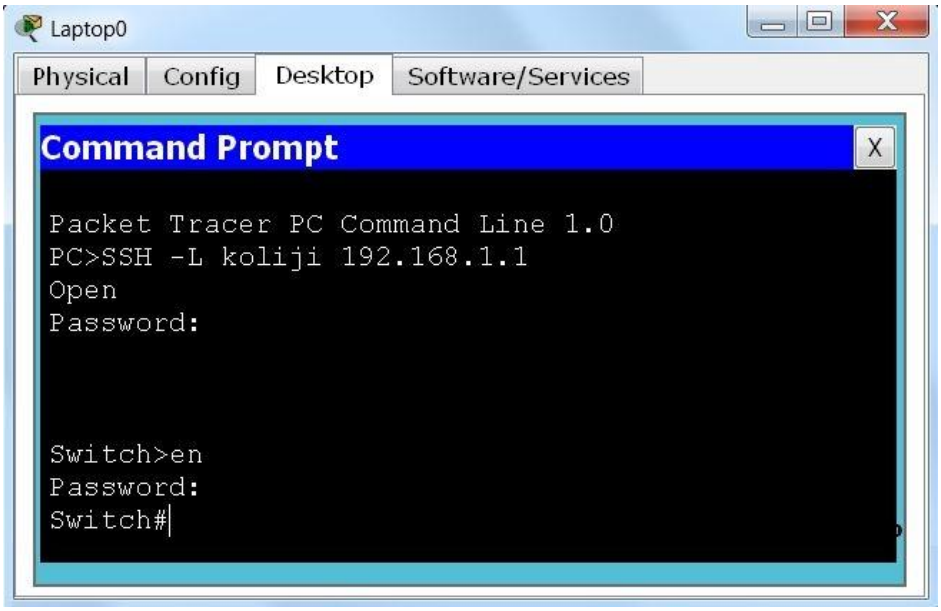
IOS Command Line Interface

```
Switch(config)#
Switch(config)#interface vlan 1
Switch(config-if)#no shutdown
Switch(config-if)#ip address 192.168.1.1 255.255.255.0
Switch(config-if)#exit
Switch(config)#username koliji password 12345
Switch(config)#line vty 0 15
Switch(config-line)#login local
Switch(config-line)#exit
Switch(config)#enable password cisco
Switch(config)#ip domain-name cisco.com
Switch(config)#crypto key generate rsa
Choose the size of the key modulus in the range of 360 to 2048 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

*???? 1 0:11:40.402:  %SSH-5-ENABLED: SSH 2 has been enabled
Switch(config)#ip ssh version 2
Switch(config)#
```

دستور SSH –L Username ip address را در command prompt کامپیوتر وارد می کنیم تا از طریق SSH به سوئیچ وصل شویم :



انواع اتصال :

1. Console
2. Telnet
3. SSH
4. Web Browser
5. Aux

نکته :

IP برای مسیریابی استفاده می شود در لایه 3 کار می کند .

MAC برای تحویل اطلاعات استفاده می شود در لایه 2 کار می کند .

در طول مسیر IP ثابت است و هیچ وقت تغییر نمی کند ولی MAC در طول مسیر تغییر می کند .

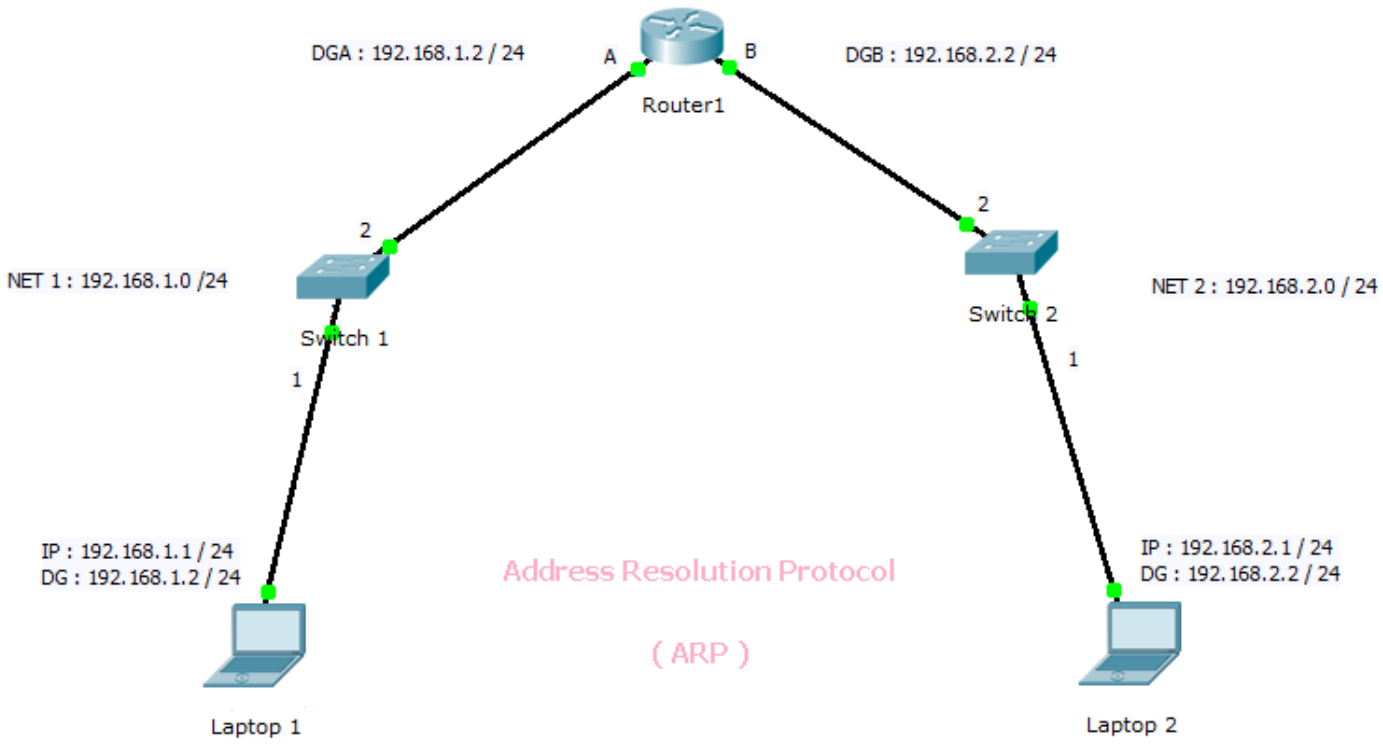
تعیین Defualt – Gateway سوئیچ :

Switch (config) # IP Defualt-Gateway ip address

Address Resolution Protocol

پروتکل تعیین آدرس:

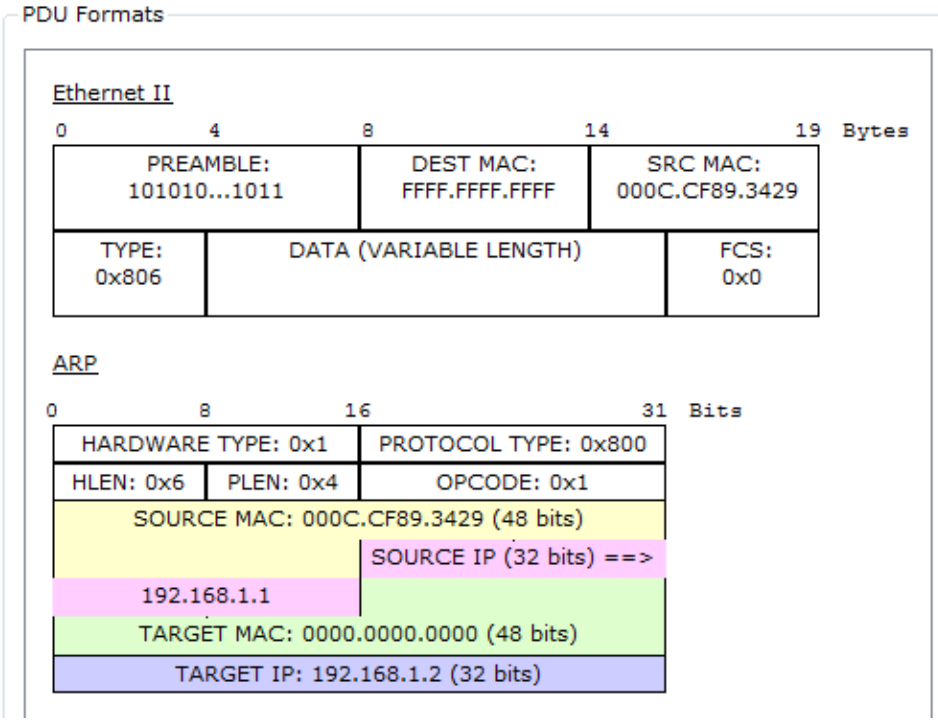
پروتکل TCP / IP برای تعیین آدرس سخت افزاری (یا آدرس فیزیکی) گره ای بر روی شبکه محلی مرتبط با اینترنت . زمانی که فقط آدرس IP (یا آدرس منطقی) شناخته شده باشد , درخواستی از ARP به شبکه ارسال می شود و گره ای که آن آدرس را داشته باشد , به آدرس سخت افزاری خود پاسخ می دهد . ARP به یافتن آدرس سخت افزاری اشاره می کند.



با توجه به شکل بالا مراحل ARP به این صورت است :

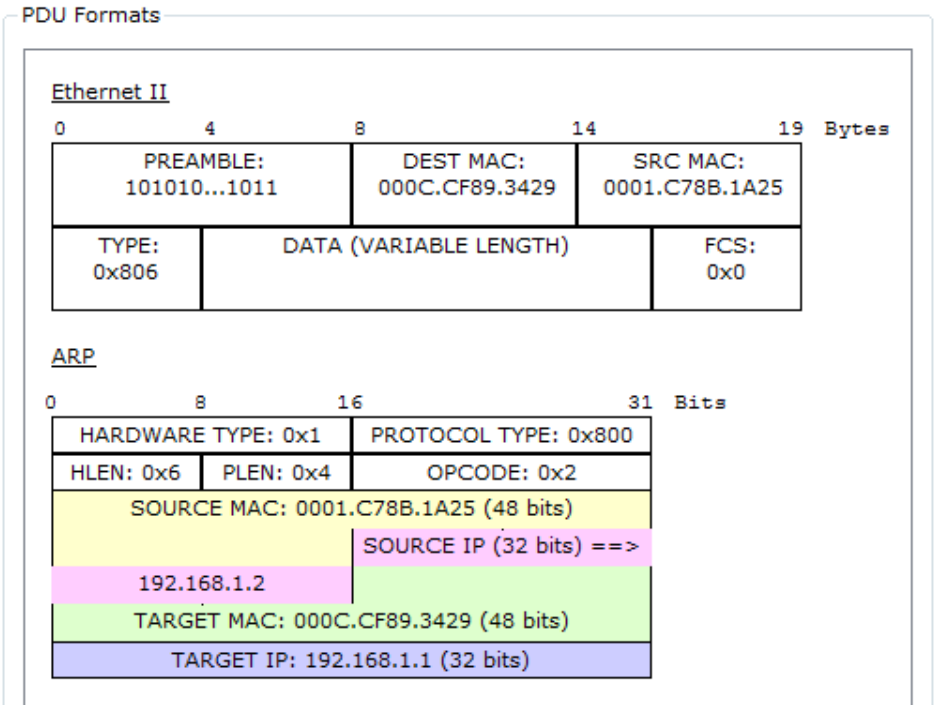
1. از PC 1 با دستور PC > Ping 192.168.2.1 , PC 2 را Ping می کنیم

2. از PC 1 یک بسته PDU حاوی Ethernet II و ARP Request مثل شکل زیر به PC 2 فرستاده می شود :



در ARP Request نوشته شده است که ای کسی که IP : 192.168.1.2 است لطفا MACات را به من بگو .

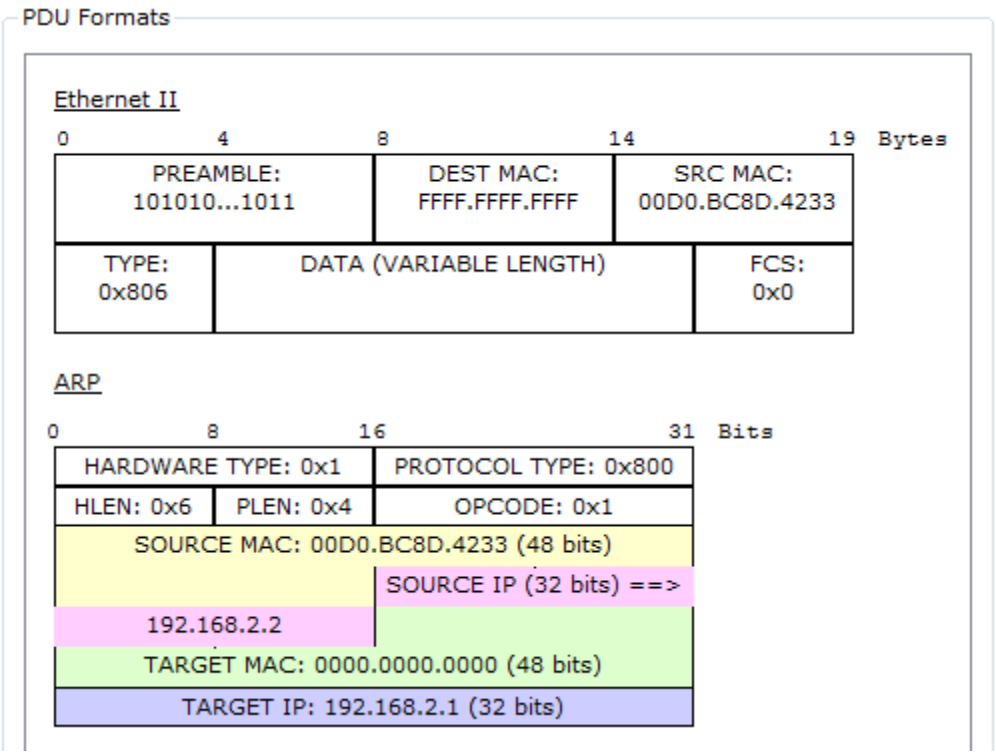
3. در این مرحله Switch 1 در port table خود MAC کامپیوتر 1 را Learn می کند و میفهمد که بر روی پورت 1 خود PC 1 قرار دارد .
4. سوئیچ به قسمت DEST MAC فریم Ethernet II نگاه می کند و می بیند که دوازده F نوشته شده (یعنی آدرس Broadcast) است پس به همه پورت های خود که به یک Device متصل هستند Forward می کند .
5. چون فقط پورت 2 سوئیچ به روتر متصل است پس سوئیچ از پورت 2 خود عمل Forwarding را انجام می دهد .
6. روتر بسته فریم را دریافت می کند و چون می بیند که IP درخواستی مال خودش است پس با یک بسته فریم به شکلی که در صفحه بعد نمایش داده شده است جواب PC 1 را می دهد (ARP Replay) .



ARP Replay : نوشته شده که MAC من این است و برای PC 1 می فرستد .

7. روتر به قسمت IP فریم نگاه میکند و بر اساس Routing Table خود می فهمد که باید به اینترفیس B بفرستد .
8. روتر از طریق اینترفیس B خود یک فریم حاوی ARP Request و Ethernet II می فرستد مانند شکلی که در صفحه بعد نمایش داده شده است :

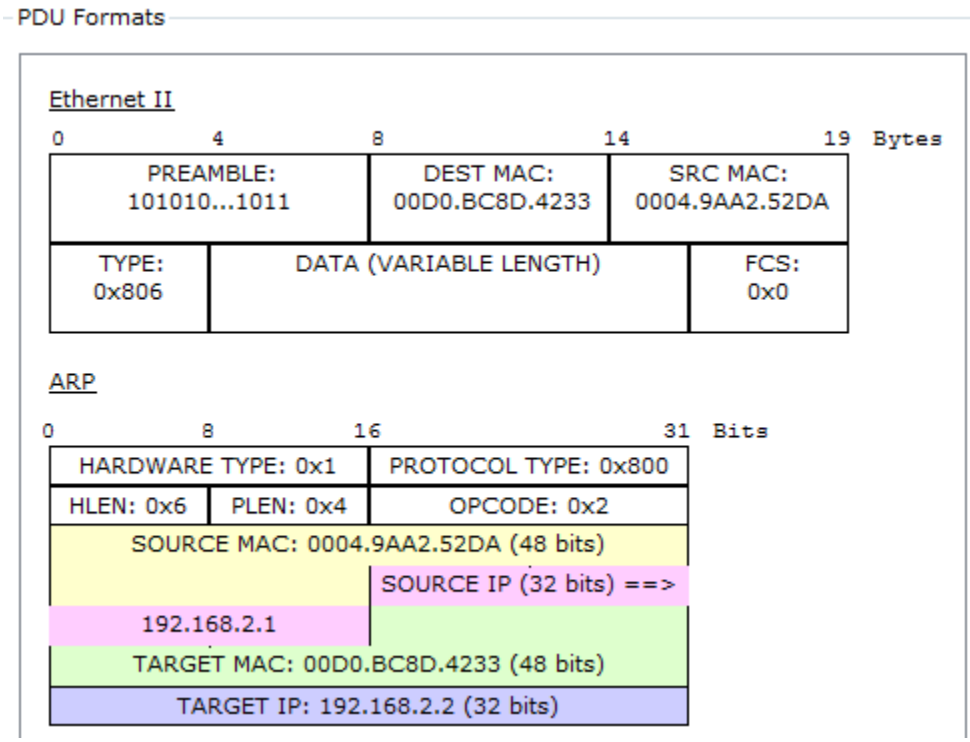
ARP Request : نوشته شده است که ای کسی که IP : 192.168.2.1 است MACات چند است . چون MAC مقصد آن IP را ندارد در قسمت DEST MAC : FFFF.FFFF.FFFF می نویسد (آدرس Broadcast) و به طرف سوئیچ 2 می فرستد.



9. سوئیچ 2 آدرس MAC B روتر را در Port Table خود ذخیره می کند و سوئیچ چون می بیند که در قسمت DEST MAC فریم آدرس Broadcast نوشته شده به همه پورت هایی که به Device وصل هستند می فرستد .

10. سوئیچ 2 از پورت 1 خود ARP را Forward می کند .

11. PC 2 بسته ARP را گرفته و یک بسته ARP Replay را در جواب می فرستد . مانند شکلی که در صفحه بعد نمایش داده شده است :



12. روتر ARP Replay را به PC 1 می فرستد و PC 1 وقتی که MAC کامپیوتر 2 را دریافت می کند .
13. در آخر فریم به PC 2 می رسد.

نکته : در Command Prompt دستور زیر را می زنیم تا آدرس MAC کامپیوتر را ببینیم

PC > ipconfig / ALL

نکته :

روشن و خاموش کردن سوئیچ با دستور نرم افزاری :

Switch # Reload

نکته :

پسوند فایل های IOS یا .bin یا .tar است .

حافظه های سوئیچ و روتر :

ROM : Read – Only Memory

ROM یک حافظه فقط خواندنی است که وظایفی را به شرح زیر انجام می دهد :

- راه اندازی اولیه روتر و سوئیچ
- نگهداری از برنامه bootstrap و همچنین در نگهداری از یک نسخه اولیه با امکانات محدود از IOS با نام Mini - IOS که در صورتی که IOS اصلی در دسترس نباشد یا دچار مشکل شود جهت Boot روتر یا سوئیچ از Mini – IOS استفاده می کند .

Flash

Flash یک حافظه قابل خواندن و نوشتن و پایدار می باشد که وظایفی را به شرح زیر در سوئیچ و روتر انجام می دهد :

- نگهداری از سیستم عامل سوئیچ و روتر که به IOS مشهور است
- با خاموش شدن سوئیچ یا روتر محتویات Flash پاک نمی شود
- امکان نگهداری از چندین نسخه IOS متفاوت درون Flash امکانپذیر است

RAM : Random Access Memory

RAM حافظه دسترسی تصادفی و ناپایدار است که وظایفی را به شرح زیر در سوئیچ و روتر انجام می دهد :

- نگهداری از جدول ها مانند Routing Table , MAC Table و ...
- نگهداری از ARP Cache
- نگهداری از Packet Buffering
- نگهداری از Running – Config یا فایل پیکربندی فعال
- محتویات RAM در زمان روشن بودن سوئیچ یا روتر نگهداری می شود . در صورتی که سوئیچ یا روتر خاموش شوند همه محتویات RAM پاک می شود

NVRAM : Nonvolatile Random Access Memory

NVRAM یک حافظه قابل خواندن و نوشتن و پایدار است که وظایفی را به شرح زیر در روتر و سوئیچ انجام می دهد :

- نگهداری از فایل های Startup – Config که شامل تنظیمات و پیکربندی های دائمی سوئیچ یا روتر است .
- NVRAM یک حافظه پایدار می باشد که با خاموش شدن سوئیچ یا روتر محتویات آن پاک نمی شود .

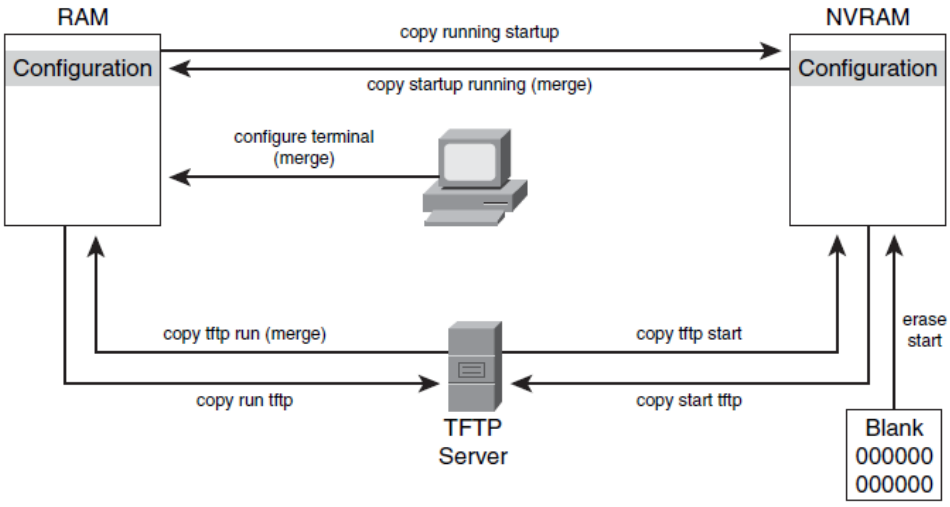
دستور نمایش محتویات حافظه ها :

Switch # Show Running – Config

Switch # Show Startup – Config

Switch # Show Flash

Copy کردن حافظه ها در همدیگر :



Switch # Copy Source – Memory Destination – Memory

RAM ⟶ NVRAM : Switch # Copy Running – Config Startup – Config

NVRAM ⟶ RAM : Switch # Copy Startup – Config Running – Config

RAM ⟶ Flash : Switch # Copy Running – Config Flash :

Flash ⟶ RAM : Switch # Copy Flash Running – Config

NVRAM ⟶ Flash: Switch # Copy Startup – Config Flash :

Flash ⟶ NVRAM : Switch # Copy Flash Startup – Config

Replace : در این حالت تمام اطلاعات قبلی پاک می شود و اطلاعات جدید جایگزین می شود.

Merge : در این حالت اطلاعات قبلی و جدید با هم ادغام می شوند و فقط دستورات که مثل هم هستند تغییر می کند و اطلاعات جدید جای قبلی را می گیرد .

کپی کردن حافظه Running – config در Flash و startup – config و کپی کردن Startup – config در Flash و برعکس حالت Replace اتفاق می افتد .

اما در کپی کردن حافظه های Flash و Startup – config در حافظه Running – config حالت Merge اتفاق می افتد .

پاک کردن حافظه ها :

در حافظه RAM (running – config) هر دستوری را که بخواهیم پاک کنیم باید کلمه NO را در جلوی همان دستور تایپ کرده و Enter بزنیم :

Switch (config) # no دستور مورد نظر

Switch (config) # no shutdown

Flash :

Switch # delete Flash : File name

Startup – config (NVRAM)

Switch # Erase startup – config

کپی کردن در TFTP :

Switch # copy startup – config TFTP

Switch # copy TFTP Flash :

Port Security

تجهیزات سیسکو توانمندی پیشرفته ای را به نام Port security پشتیبانی می کنند که قابلیت افزایش امنیت را روی پورتهای سوئیچ به شما خواهد داد که این افزایش امنیت مخصوصا بر روی سوئیچ های لایه Access که کامپیوترهای کاربران به آن متصل میباشند , اهمیت بیشتری دارد .

Port security به شما این امکان را می دهد که قادر باشید کنترل کاملی روی دستگاه هایی که به سوئیچ متصل می شود داشته باشید .

مثلا شما می توانید توانمندی Port security را روی پورت FastEthernet 0/1 سوئیچ فعال کنید و اجازه بدهید فقط PC 1 قادر به برقراری ارتباط با این پورت باشد و سایر کامپیوترها قادر به برقراری ارتباط با پورت FastEthernet 0/1 را نداشته باشند . در صورتی که کامپیوتر یا هر Device دیگری غیر از PC 1 قصد استفاده از پورت FastEthernet 0/1 را داشته باشند , قادر به برقراری ارتباط با این پورت نباشند . در پیکربندی Port security می توانید تعیین کنید در صورتی که دستگاهی غیر از PC 1 قصد ارتباط با پورت FastEthernet 0/1 را داشته باشد این پورت Shutdown و غیر فعال شود .

Port security برای شناسایی کامپیوترها و تعیین مجاز بودن یا غیر مجاز بودن آن کامپیوتر برای استفاده از پورت از MAC Addresss آن کامپیوتر یا Device استفاده می کنند .

روی پورت هایی می توانیم امنیت برقرار کنیم که پورت ها Access باشند .

مثال برای پورت 0/1 :

Switch (config) # interface fastethernet 0/1

Switch (config – if) # Switchport Mode Access

Switch (config – if) # Switchport Port – Security

Switch (config – if) # Switchport Port – Security Maximum 1

Switch (config – if) # Switchport Port – Security MAC – Address mac-address

Switch (config – if) # Switchport Port – Security Violation Mode

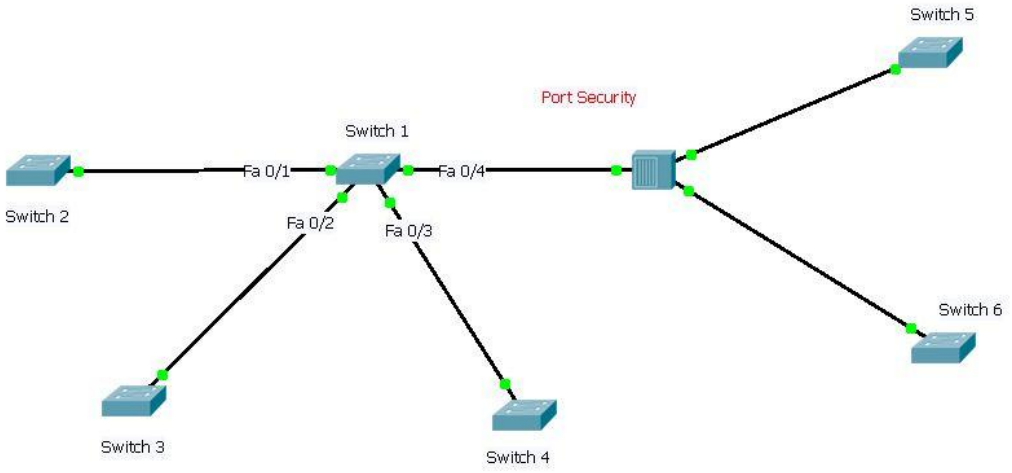
با فرمان زیر در Port security خود سوئیچ به صورت دینامیک پورت ها را Learn می کند یعنی با توجه به مقدار Maximum که تعریف کرده ایم MAC کامپیوترهایی را که برای اولین بار به پورت وصل می شوند ذخیره می کند :

Switch (config – if) # Switchport Port – Security MAC – Address sticky

mode در قسمت Violation سه حالت زیر را دارد :

- Shutdown : در این حالت اگر تخلف در شبکه بر روی پورت انجام شود پورت خاموش یا غیر فعال می شود .
- Restrict : در این حالت پورت در همان وضعیت فعال باقی می ماند اما پاکت های ارسالی از آدرس های MAC غیر مجاز را بلوکه می کند . در این بین تعداد پاکت های ارسالی از آدرس های MAC غیر مجاز شمارش شده و یک SNMP Trap و همچنین یک Log Message نیز ایجاد و فرستاده می شود .
- Protect : در این حالت پورت در همان وضعیت فعال باقی می ماند اما پاکت های ارسالی از آدرس های MAC غیر مجاز را بلوکه می کند . در این بین هیچ اطلاعاتی ثبت نشده و پیام خطایی نیز نمایش داده نمی شود .

مثال :



دستوراتی که در Switch 1 وارد می کنیم :

```
Switch(config)#interface fastethernet 0/1
Switch(config-if)#switchport mode access
Switch(config-if)#switchport port-security
Switch(config-if)#switchport port-security maximum 1
Switch(config-if)#switchport port-security mac-address sticky
Switch(config-if)#switchport port-security violation restrict
Switch(config-if)#exit
Switch(config)#interface fastethernet 0/2
Switch(config-if)#switchport mode access
Switch(config-if)#switchport port-security
Switch(config-if)#switchport port-security maximum 1
Switch(config-if)#switchport port-security mac-address sticky
Switch(config-if)#switchport port-security violation protect
Switch(config-if)#exit
Switch(config)#interface fastethernet 0/3
Switch(config-if)#switchport mode access
Switch(config-if)#switchport port-security
Switch(config-if)#switchport port-security maximum 1
Switch(config-if)#switchport port-security mac-address sticky
Switch(config-if)#switchport port-security violation protect
Switch(config-if)#exit
Switch(config)#interface fastethernet 0/4
Switch(config-if)#switchport mode access
Switch(config-if)#switchport port-security
Switch(config-if)#switchport port-security maximum 1
Switch(config-if)#switchport port-security mac-address sticky
Switch(config-if)#switchport port-security violation shutdown
Switch(config-if)#exit
Switch(config)#
```

Showهای Port – security :

Switch # Show Port – security

Switch # Show Port – Security – Address

Switch # Show Port – security interface type mod/num

Switch # Show Port – security

```
Switch#
Switch#show port-security
Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security Action
               (Count)       (Count)        (Count)
---------------------------------------------------------------------
        Fa0/1        1          1                0         Restrict
        Fa0/2        1          1                0          Protect
        Fa0/3        1          1                0          Protect
        Fa0/4        1          1                1         Shutdown
---------------------------------------------------------------------
Switch#
```

Switch # Show Port – Security – Address

```
Switch#show port-security address
                        Secure Mac Address Table
------------------------------------------------------------------------------
Vlan    Mac Address     Type                    Ports           Remaining Age
                                                                (mins)
----    -----------     ----                    -----           -------------
1       0001.C9E4.6501  DynamicConfigured       FastEthernet0/1         -
1       0001.6362.8D01  DynamicConfigured       FastEthernet0/2         -
1       0030.F226.A002  DynamicConfigured       FastEthernet0/3         -
1       0000.0C67.4201  SecureSticky            FastEthernet0/4         -
------------------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 0
Max Addresses limit in System (excluding one mac per port) : 1024
Switch#
```

Switch # Show Port – security interface Fastethernet 0/4

```
Switch#
Switch#show port-security interface fastEthernet 0/4
Port Security              : Disabled
Port Status                : Secure-down
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 1
Total MAC Addresses        : 0
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 0000.0000.0000:0
Security Violation Count   : 0
Switch#
```

این دستور قبل از اعمال Port-Security بر روی پورت 4/0 اجرا شده

```
Switch#
Switch#show port-security interface fastEthernet 0/4
Port Security              : Enabled
Port Status                : Secure-shutdown
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 1
Total MAC Addresses        : 1
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 1
Last Source Address:Vlan   : 0004.9A38.4301:1
Security Violation Count   : 1

Switch#
```

این دستور بعد از اعمال Port-Security بر روی پورت 4/0 اجرا شده

زمانی در شبکه تخلف ایجاد شود پورت Shutdown می شود و پیغام Error – Disable را می دهد .

برای برطرف کردن این پیام اول باید ارتباط PC که تخلف کرده را قطع کنیم , بعد PC اصلی را وصل می کنیم و بعد دوباره پورت را روشن می کنیم با دستورات زیر :

Switch (config)# Interface type mod/num

Switch (config – if)# shutdown

Switch (config – if)# No shutdown

نکته :

وقتی در یک شبکه یک Hub به یک سوئیچ وصل باشد و یک PC به همان Hub وصل شده باشد و در تنظیمات Port – security همان پورتی که Hub به سوئیچ وصل شده تعداد Maximum را 2 تعریف کنیم اولین PC که به Hub وصل شود MAC آن در جای خالی MAC – Address – Table سوئیچ ذخیره می شود و تا زمانی که سوئیچ خاموش و روشن نشود این MAC از حافظه پاک نمی شود .

MAC – Addressهایی را که به صورت Dynamic , Learn کرده ایم با دستور زیر پاک می شوند :

Switch # Clear Port – security Dynamic

MAC - Addressهایی را که به صورت Static , Learn کرده ایم با دستور زیر پاک می شوند :

Switch # Clear Port – security Static

Speed :

سرعت انتقال یک بیت در زمان

سرعت اینترفیس ها در انتقال یک بیت :

Ethernet 10 mbps → IEEE 802.3

FastEthernet 100 mbps → IEEE 802.3u

GigabitEthernet 1000 mbps → IEEE 802.3z , IEEE 802.3ab

TenGigabitEthernet 10000 mbps → IEEE 802.3ae

فرمان تغییرسرعت یک اینترفیس :

Switch (config – if) # Speed { 10 | 100 | 1000 | Auto }

نکته :

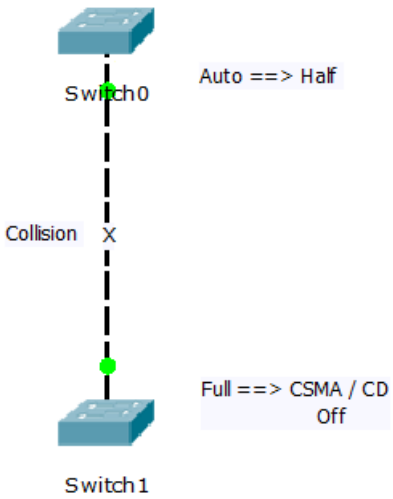
اگر دو سوئیچ را به یکدیگر وصل کنیم باید سرعت هر دو طرف پورت (اینترفیس های هر دو سوئیچ) برابر باشند , بهتر است از Auto استفاده کنیم و دو سوئیچ با توافق هم از بالاترین سرعت ممکن برای انتقال داده استفاده میکنند .

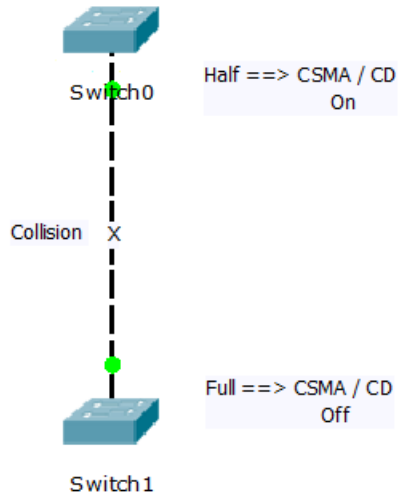
تنظیم Duplex اینترفیس :

Switch (config – if) # Duplex { Half | Full | Auto }

نکته :

در شبکه بسته های کوچکتر از 64 byte یعنی error. وقتی Runt Error که باید بین (64 – 1518 byte) باشد کمتر از 64 byte باشد یعنی احتمالا مشکل Duplex در شبکه وجود دارد و شبکه سرعت پایینی دارد . همیشه باید Duplex را در حالت Full تنظیم کنیم مگر در حالتی خاص مثلا سوئیچ را به یک Hub وصل کنیم .





در هر دو حالت Collision رخ میدهد . در حالتی که یکی از سوئیچ ها در حالت Full و دیگری در حالت Auto باشد چون سوئیچ 1 جواب سوئیچ 0 را نمی دهد که Duplex را در حالت auto است یا نه , پس سوئیچ 0 خود را در حالت کمتر قرار می دهد یعنی حالت Half و چون یک طرف پورت Half و طرف دیگر حالت Full است collision رخ می دهد .

پیش فرض حالت Duplex در سوئیچ Auto است .

نکته :

بهتر است تنظیمات جاهای حساس شبکه را همیشه به صورت Static وارد کنیم یعنی در حالت پیش فرض ها قرار ندهیم .

دستور نمایش MAC – Address :

Switch # Show MAC – Address – Table

```
Switch#show mac-address-table
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

   1    0001.6362.8d01    STATIC      Fa0/2
   1    0001.c9e4.6501    STATIC      Fa0/1
   1    0030.f226.a002    STATIC      Fa0/3
Switch#
```

اگر بعد از Table در دستور بالا کلمه Dynamic یا static را بنویسیم فقط MAC – Address هایی را که به صورت Dynamic یا Static ذخیره شده اند را نمایش میدهد :

Switch # Show MAC – Address – Table Dynamic

Switch # Show MAC – Address – Table Static

با دستور زیر فقط MAC – Address یک اینترفیس را نمایش می دهد :

Switch # Show MAC – Address – Table type mod/num

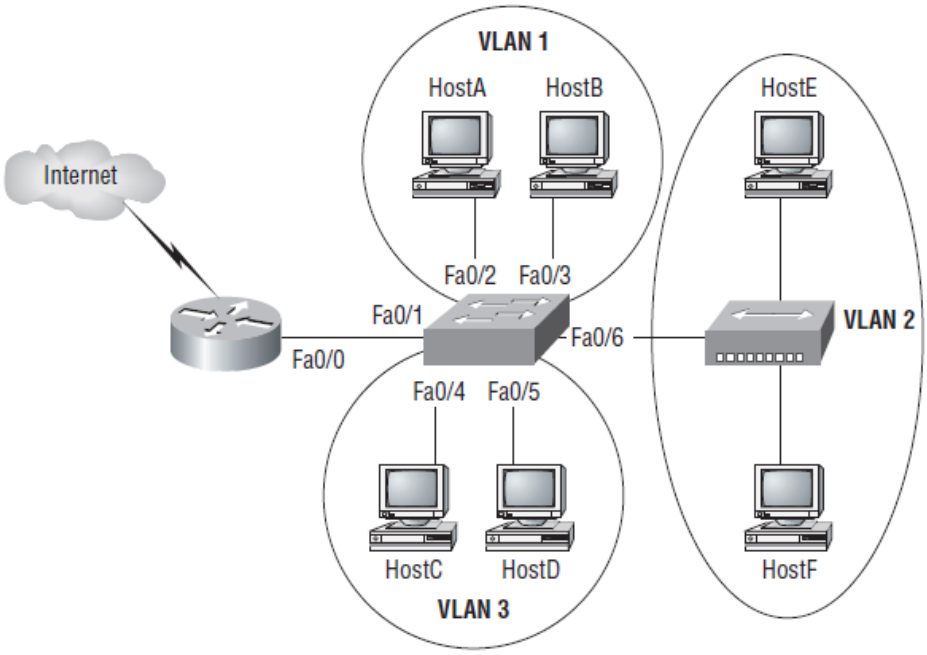
نکته :

وقتی که یک Device مثلا Server را داشته باشیم که 2 کارت شبکه داشته باشد یکی برای Send و دیگری برای Receiv . باید برای کارت شبکه ای که Receiv است به صورت Static , MAC – Address را وارد کنیم . چون فقط دریافت می کند و نمی تواند ارسال کند پس سوئیچ نمی تواند MAC آن را Learn کند .

با دستور زیر :

Switch (config)# MAC – Address – Table static mac VLAN vlan Interface type mod / num

Virtual LAN



: VLAN

تمامی پورت های یک سوئیچ در یک محیط Broadcast Domain قرار دارد . این بدان معنی است که تمامی Deviceهایی 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 Serverها , کاربران , اینترنت در یک LAN واحد مشکلاتی را به دنبال دارد نتیجه آن :

1. ترافیک بالا
2. امنیت پایین

به عبارتی در چنین شبکه ای نمی توان مدیریت روی ترافیک و امنیت داشت . در حالی که اگر یک Broadcast Domain را به چندین Broadcast Domain تفکیک کنیم , ترافیک کاهش و محلی شده و دسترسی ها محدود می شود .

در واقع با تبدیل کردن یک LAN به چندین LAN یا همان VLAN نتایج زیر حاصل می شود :

- کوچک شدن Broadcast Domain
- کاهش و محلی شدن ترافیک
- محدود کردن سطح دسترسی

فرض کنید تعدادی کامپیوتر در یک LAN قرار داشته باشند . بنابراین همه این کامپیوترها به راحتی با یکدیگر ارتباط دارند . اما در صورتی که یک LAN را به چندین VLAN تبدیل کنیم , کامپیوترهایی که در یک VLAN هستند نمی توانند با VLANهای دیگر ارتباط برقرار کنند . تعریف و ساخت VLAN در لایه دوم از مدل OSI امکان پذیر می باشد . تعریف نام برای VLAN اختیاری است .

در یک سوئیچ بین 0 تا 4095 عدد VLAN می توان درست کرد . VLANهای 0 و 4095 رزرو شده هستند و نمی توان از این دو استفاده کرد . تعداد و شماره VLANهایی را که می توانیم از آنها استفاده کنیم بین 1 تا 1005 است که به آنها استاندارد می گویند . از 1006 تا 4094 را Extand می گویند . از 1002 تا 1005 را نمیتوانیم استفاده کنیم به آنها VLANهای Token Ring و FDDI می گویند .

دستور ساخت VLAN :

Switch (config)# VLAN vlan – number

Switch (config - Vlan)# Name name

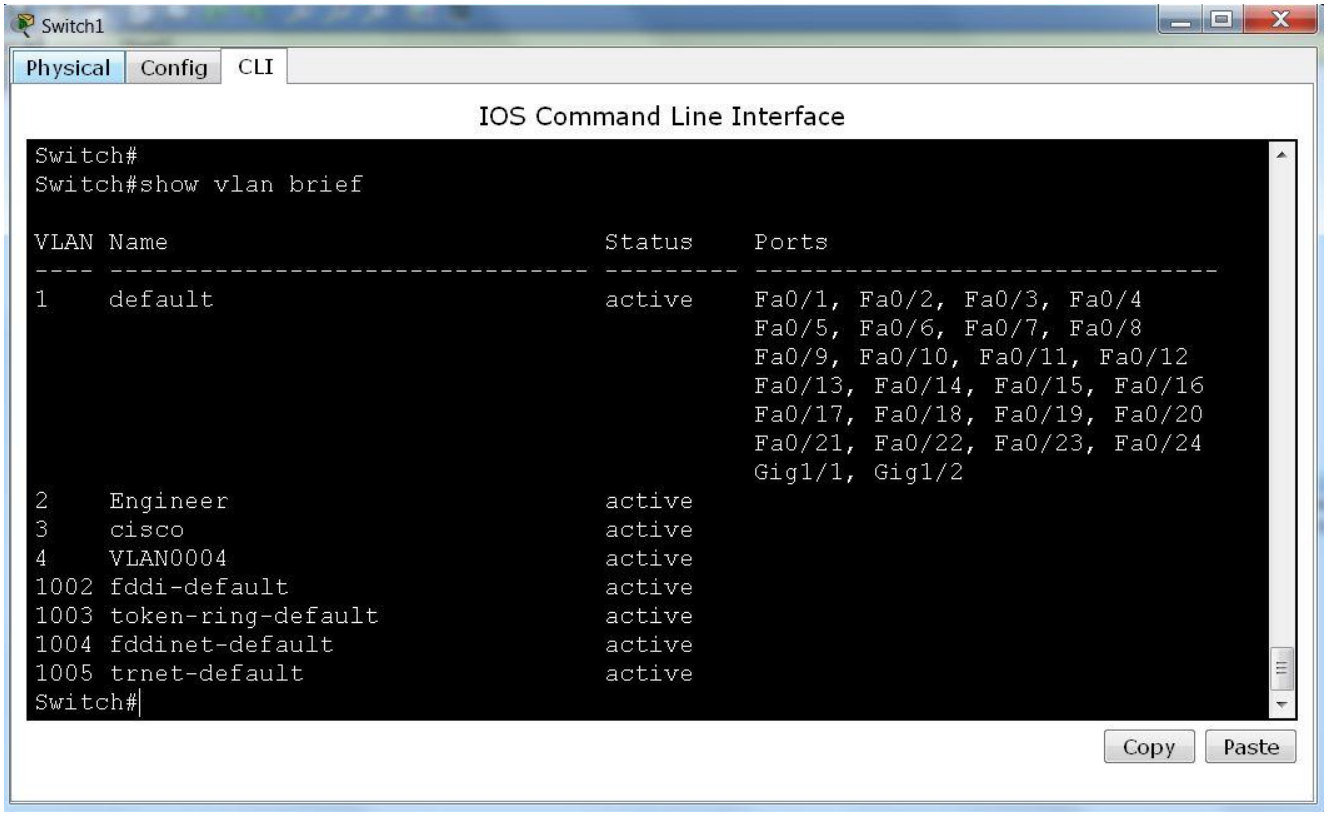
مثال :

دستور نمایش VLANها :

Switch # Show VLAN

Switch # Show VLAN Brief

مثال دستور Show VLAN Brief :



همانگونه که در خروجی دستور Show VLAN Brief مشاهده می کنید Vlan 2 با نام Engineer و Vlan 3 با نام cisco و Vlan 4 که با نام VLAN0004 ساخته شده اند .

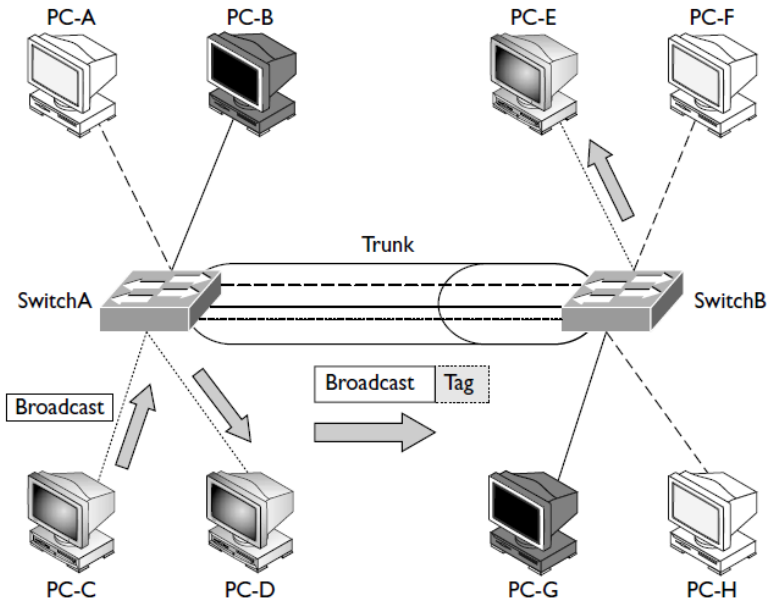
خروجی Show VLAN Brief خلاصه شده دستور Show VLAN است و بهتر است که از این دستور استفاده کنیم .

نکته :

VLAN 1 غیر قابل تغییر نام است و حذف نمی شود و به صورت پیش فرض تعریف شده است و در حالت اول همه اینترفیس ها در VLAN 1 قرار دارند .

انواع Port از نظر ترافیک VLANها :

1. **Access** : پورت هایی که فقط ترافیک یک VLAN را از خود عبور می دهند.
2. **Trunk** : پورت هایی که محدود به ترافیک یک VLAN نیستند و ترافیک همه VLANها را از خود عبور می دهند .



در شکل بالا PCهای همرنگ در یک VLAN قرار دارند .

وقتی که PC – C که با PC – D و PC – E در یک VLAN قرار دارند می خواهد برای PC – E بسته Data بفرستد اول به سوئیچ A میرسد و سوئیچ بسته را گرفته و به آن Tag میچسباند که این بسته متعلق به VLAN خاکستری است و ارسال میکند به سوئیچ B از طریق پورتی که در حالت Trunk قرار دارد . سوئیچ B بسته را دریافت میکند و به قسمت Tag آن نگاه می کند و میبیند که متعلق به VLAN خاکستری است پس در VLAN خاکستری آن را منتشر میکند (این در حالتی است که MAC کامپیوتر E هنوز Learn نشده باشد) پس به PC – E می رسد . قبل از ارسال به VLAN خاکستری باید سوئیچ B بسته را که دریافت کرد Tag آن را بعد از خواندن از بسته جدا کند و بعد ارسال کند .

نکته :

پورت هایی که PC به سوئیچ متصل می شود را access تعریف میکنیم و پورت بین سوئیچ ها را باید حتما Trunk تعریف کنیم .

دستور قرار دادن پورت در VLAN :

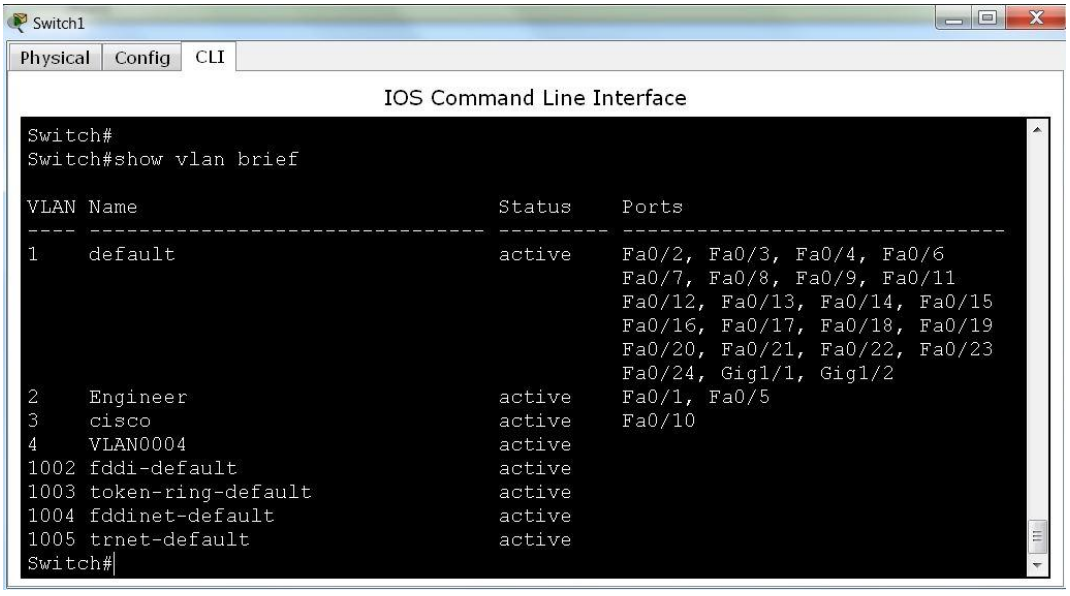
Switch (config) # Interface FastEthernet type mod/num

Switch (config – if) # Switchport mode access

Switch (config – if) # Switchport Access VLAN vlan-number

مثال :

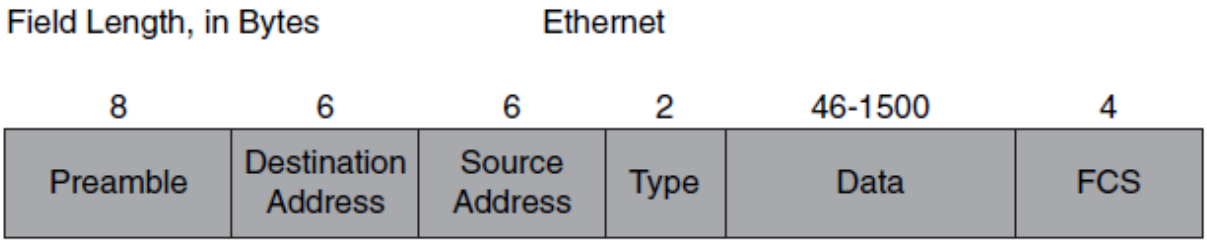
همانگونه که در زیر مشاهده میکنید با این دستور پورت 0/1 و 0/5 در VLAN 2 و پورت 0/10 در VLAN 3 قرار می گیرند .



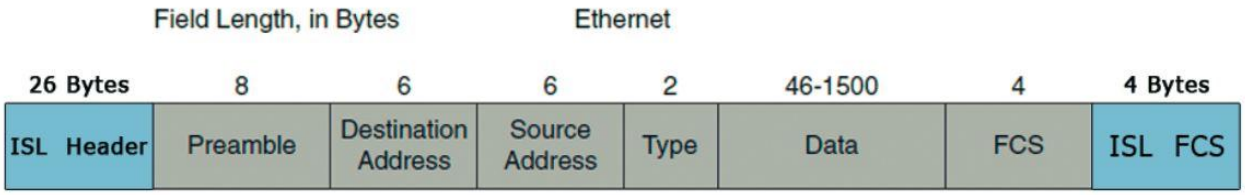
پروتکل های VLAN در اتصالات Trunk :

1. **ISL (Inter Switch Link)** یک روش Encapsulation مخصوص Deviceهای سیسکو است . Framing مخصوص به خود دارد . Native VLAN ندارد .

شکل الف :

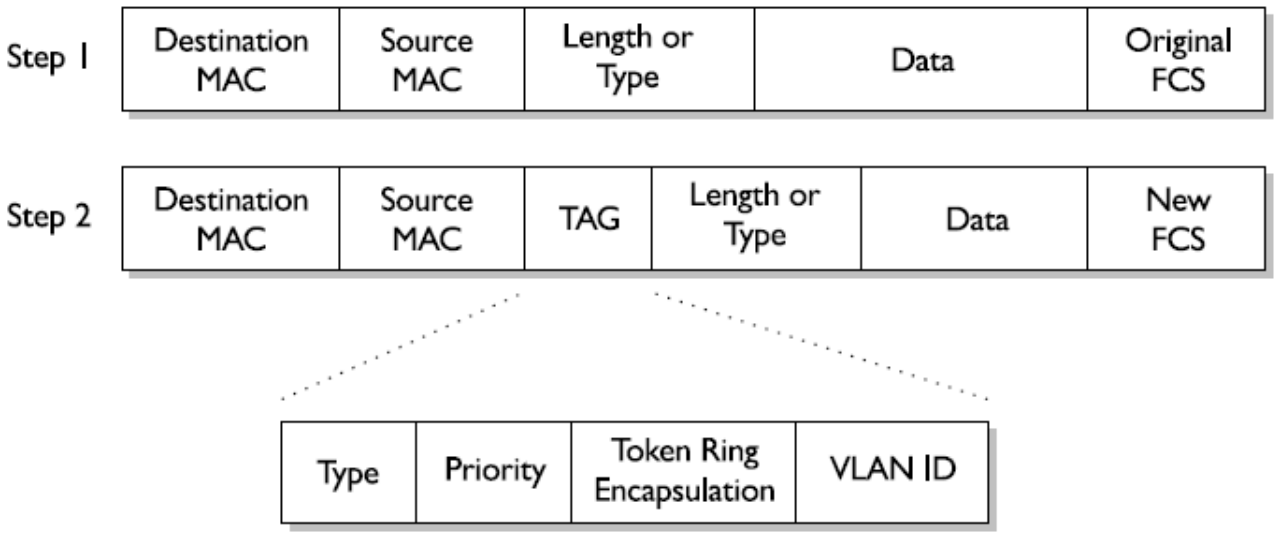


شکل ب :



پروتکل ISL فریم ارسالی که به صورت شکل الف است را بعد از Tag به صورت شکل ب تغییر می دهد یعنی به اول فریم ISL Header به اندازه 26 بایت و به آخر فریم ISL FCS به اندازه 4 بایت را اضافه می کند و بعد ارسال می کند .

2. **پروتکل IEEE 802.1Q** یک پروتکل بین المللی است و همه شرکت ها از آن استفاده می کنند . Framing مخصوص به خود دارد و Native VLAN را دارد .



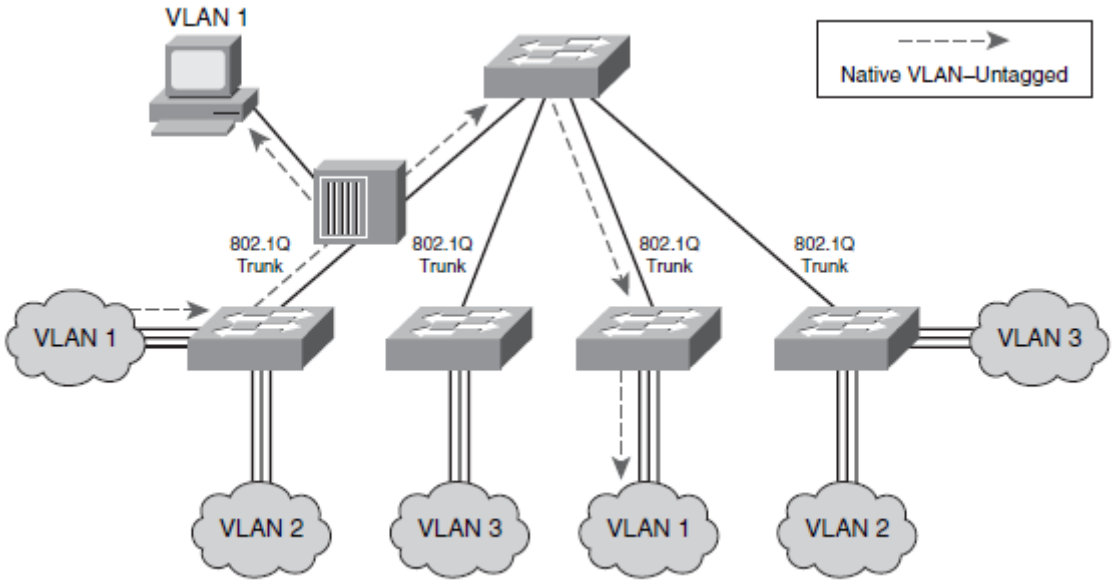
این پروتکل فریم اصلی که در شکل با Step 1 مشخص شده می گیرد و با Tag زدن به آن مثل فریم Step 2 که 4 byet است و حاوی شماره VLAN است را تغییر می دهد و ارسال می کند.

نکته :

ISL بر 802.1Q اولویت دارد .

: Native VLAN

برای کنترل ارسال و دریافت ترافیک سوئیچ ها مورد استفاده قرار میگیرد. اگر بخواهیم فریم های یک VLAN را Tag نزنیم از Native VLAN استفاده می کنیم . چون اگر این کار را نکنیم منجر به افزایش Overhead روی پورت Trunk می شود .



در شکل بالا VLAN 1 را Native VLAN تنظیم کرده ایم تا فریم های ارسالی در این VLAN را Tag نزند . حتما باید دو طرف پورت یک پروتکل داشته باشد و باید تعیین کنیم چه پروتکلی باشد .

پروتکل 802.1Q از Native VLAN پشتیبانی می کند و به کمک فرمان زیر روی پورت Trunk فعال می شود :

Switch (config – if) # Switchport trunk native VLAN vlan – number

دستورات تنظیم VLAN :

Switch (config) # Interface type mod/num

Switch (config – if) # Switchport trunk encapsulation { ISL | Dot1Q }

Switch (config – if) # Switchport mode trunk

دستوری که ترافیک یک یا چند VLAN را از یک پورت در حالت Trunk مجاز می کند و برچسب (Tag) می زند :

Switch (config – if) # Switchport trunk Allowed VLAN vlan – range

در VLAN – Range می توانیم از 3 حالت زیر استفاده کنیم :

1. 2 , 4 , 5
2. 2 – 5
3. 2 – 5 , 10 – 15

دستور حذف یک VLAN از بقیه VLAN های یک پورت :

Switch(config – if)#Switchport trunk Allowed VLAN Remove vlan-num

دستور اضافه کردن یک VLAN به بقیه VLAN های یک پورت :

Switch (config – if)# Switchport trunk Allowed VLAN add vlan-num

دستوری که همه VLAN ها را مجاز میکند :

Switch (config – if) # Switchport trunk Allowed VLAN ALL

دستوری که همه VLAN ها را مجاز میکند بغییر از چند Vlan :

Switch (config – if)#Switchport trunk Allowed VLAN except vlan-num

دستوری که هیچکدام از VLAN ها را مجاز نمیکند :

Switch (config – if) # Switchport trunk Allowed VLAN none

Dynamic Trunking Protocol

DTP :

این پروتکل بررسی می کند آیا اینترفیس های سوئیچ باید Trunk شوند یا نه و اگر بشود با چه پروتکلی Trunk شوند . فقط Device های شرکت سیسکو این پروتکل را دارند .

Mode های DTP :

1. **Access** : اگر یک طرف پورت در حالت Access باشد به طرف دیگر پورت پیشنهاد نمی دهد .
2. **Trunk** : در این حالت پورت می گوید من Trunk هستم و پیشنهاد Trunk بودن را به طرف دیگر پورت می دهد .
3. **Dynamic Auto** : در این حالت پورت پیشنهاد نمی دهد ولی اولین پورتی که پیشنهاد دهد را قبول می کند .
4. **Dynamic Desirable** : در این حالت پورت هم پیشنهاد می دهد هم اولین پیشنهادی که طرف دیگر پورت بدهد را قبول می کند .

switch A / switch B	**Access**	**Trunk**	**Dynamic Auto**	**Dynamic Desirable**
Access	Access	**X**	Access	Access
Trunk	**X**	Trunk	Trunk	Trunk
Dynamic Auto	Access	Trunk	Access	Trunk
Dynamic Desirable	Access	Trunk	Trunk	Trunk

پیش فرض پورت ها Dynamic Auto یا Dynamic Desirable است .

: Administrativ Mode

به چهار حالتی که کاربر وارد می کند یعنی (Dynamic Desirable Access , Dynamic Auto , Trunk ,) که در بالای جدول نوشته شده می گویند .

: Operational Mode

به دو حالت داخل جدول یعنی (Trunk , Access) که DTP تعیین می کند یعنی Modeهایی که DTP برای پورت ها تعیین می کند می گویند .

نکته :

وقتی در یک mode باشیم که یک طرف پورت در حالت Access باشد و طرف دیگر در حالت Trunk باشد , این حالت بدترین حالت است چون هیچ کدام از طرفین پورت حالت خود را تغییر نمی دهند تا هر دو طرف در یک حالت access یا Trunk قرار گیرند .

نکته :پروتکل DTP مرتبا در بین سوئیچ های شبکه در حال رفت و آمد است و این کار باعث ارسال بسته های اضافی DTP در مدار و کاهش سرعت شبکه می شود .

دستور خاموش کردن DTP :

Switch (config – if) # Switchport Nonegotiate

این دستور را در حالتی می توانیم وارد کنیم که Switchport Mode دو طرف یک پورت به حالت دستی (Static) وارد کرده باشیم.

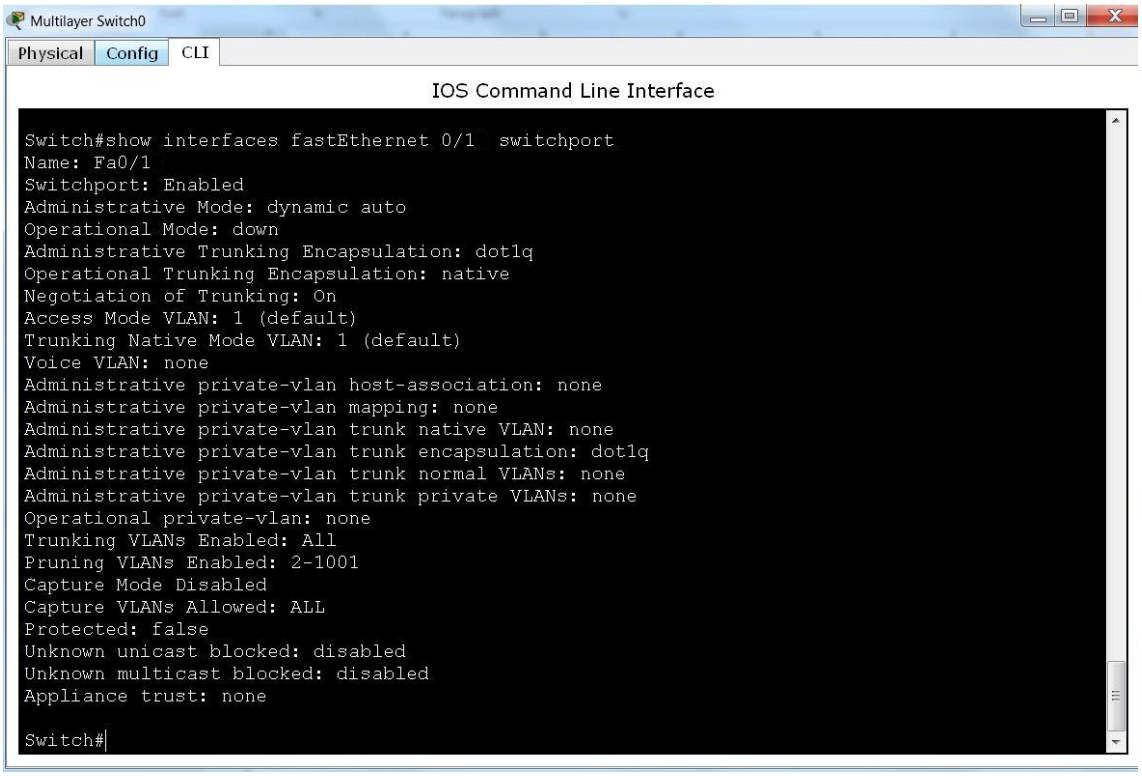
بهتر است در شبکه دستور switchport Mode را برای سوئیچ های اصلی به صورت دستی وارد کنیم و دستور Nonegotiate را در آن سوئیچ ها وارد کنیم . برای سوئیچ های معمولی در شبکه زیاد لازم نیست این کار را بکنیم .

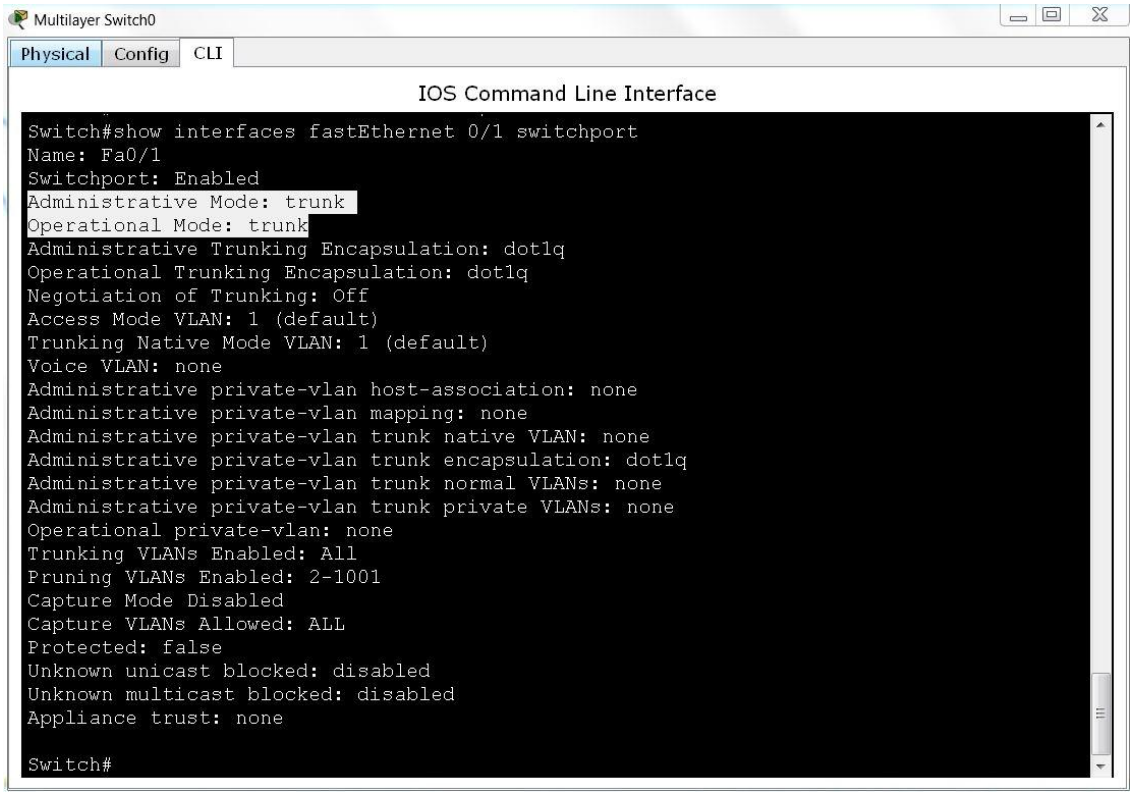
دستور Show های DTP :

Switch # Show interface type mod/num switchport

Switch # Show DTP

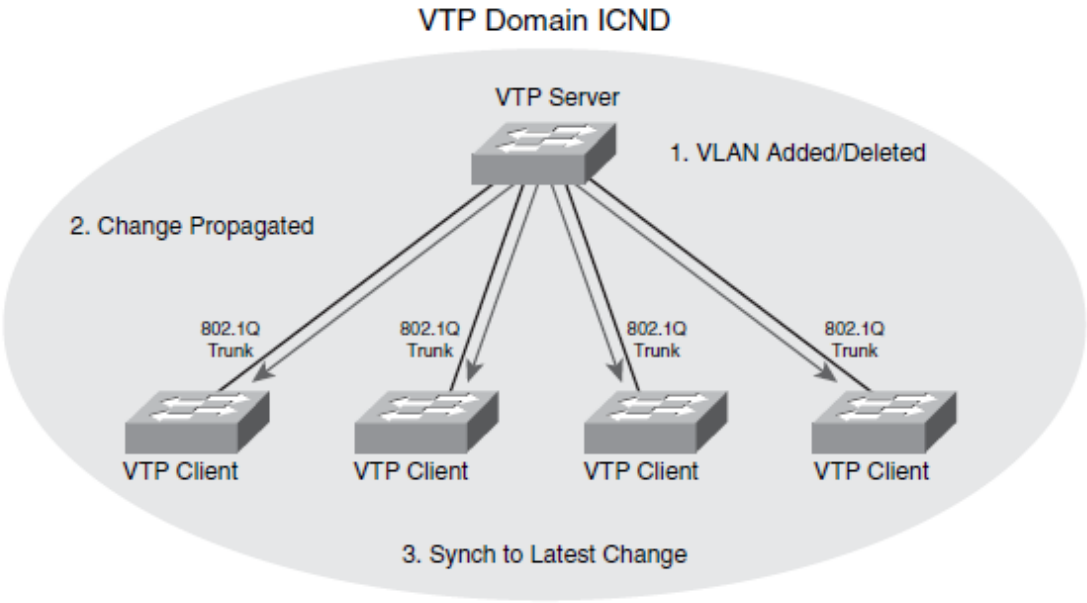
مثال دستور switchport interface fastethernet 0/1 Show interface قبل و بعد از اجرای DTP را در صفحه بعد مشاهده می کنید :





همانگونه که در خروجی دستور بالا مشاهده می کنید هم Administrative Mode و هم Operational Mode پورت 1/0 به حالت Trank تبدیل شده است و از Encapsulation dot1q استفاده کرده است .

VLAN Trunking Protocol



: 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 می کند و سپس به اطلاع سوئیچ های دیگر می رساند . مخصوص دستگاه های سیسکو است .

: VTP Domain

ناحیه ای که شامل تعدادی سوئیچ بوده به طوری که هر سوئیچ اطلاعات مربوط به VLAN خود را با بقیه سوئیچ ها به اشتراک می گذارد .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 VLANهایشان را با یکدیگر به اشتراک بگذارند.

: 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 Advertisementها به صورت فریم های Multicast در VTP Domain ارسال می شوند. لینک بین دو سوئیچ باید به صورت Trunk تعریف شود تا VTP Advertisementها قادر به انتقال باشند.

VTP Messages

If you use a client/server configuration for VTP, these switches can generate three types of VTP messages:

- Advertisement request
- Subset advertisement
- Summary advertisement

VTP Advertisementها به 3 فرم در یک VTP Domain منتشر می شوند :

Summary Advertisement :

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 .

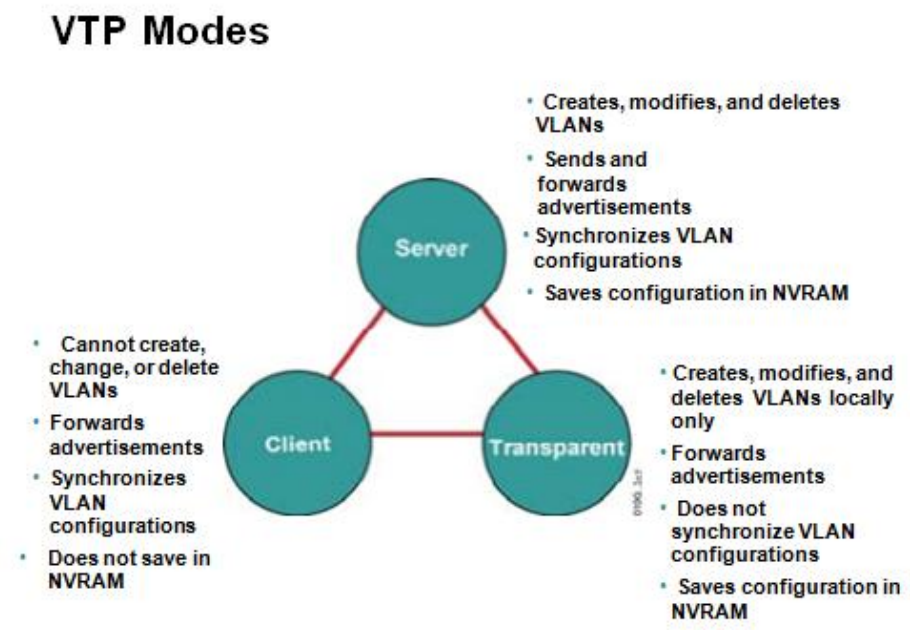
Subset Advertisement :

اطلاعاتی هستند که توسط Server هنگام رخ دادن تغییر در تنظیمات VLANها ارسال می شود و شامل اطلاعات VLAN Database و وضعیت هر کدام از VLANها می باشد.

Advertisement Request :

اطلاعاتی هستند که توسط VTP Clientها از VTP Server درخواست می شوند.

Modeهای 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 VLANها و عملکرد VTP نقش خواهد داشت .

Server Mode :

سوئیچی که در این Mode قرار میگیرد دارای توانایی کامل در ایجاد , حذف و تغییر VLAN و مدیریت Domain خواهد بود . تمام سوئیچ ها به صورت پیش فرض در این Mode قرار دارند.

Client Mode :

سوئیچی که در این Mode قرار می گیرد قادر به حذف یا اضافه یا تغییر VLAN نخواهد بود . سوئیچی که در این Mode قرار میگیرد به تغییراتی که توسط سوئیچ های دیگر گزارش می شود گوش می دهد و این تغییرات را روی خود اعمال می کند .

Transparent Mode :

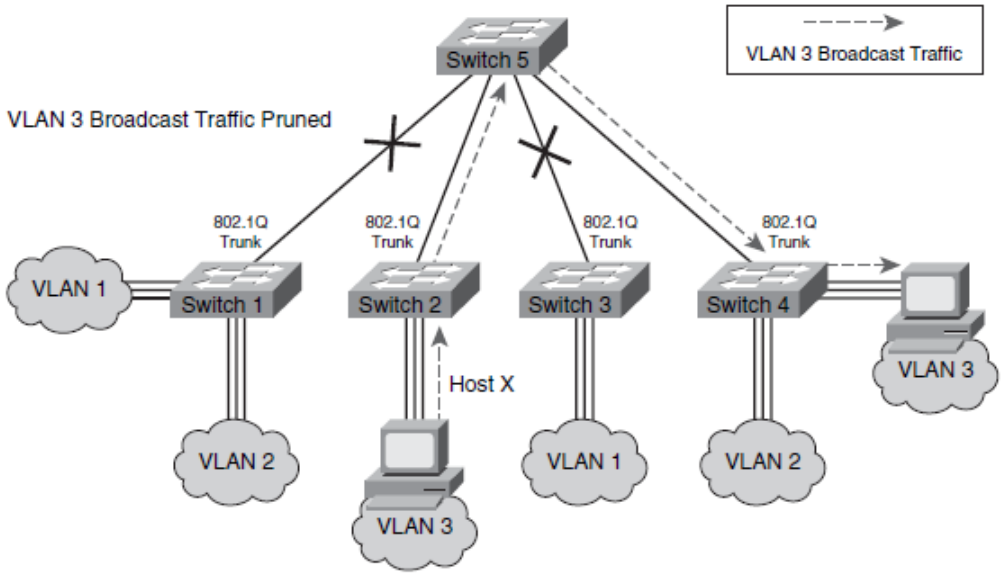
سوئیچی که در این Mode قرار می گیرد به عنوان یک عضو خنثی عمل میکند . اطلاعاتی که در مورد VTP از سوئیچ های مجاور دریافت می کند را بدون اینکه روی خود اعمال کند از طریق پورت Trunk به سوئیچ های مجاورش ارسال می کند . قادر به حذف و اضافه کردن VLAN می باشد اما این تغییرات را به دیگر سوئیچ ها ارسال نمی کند .

نکته :

در یک شبکه حتما باید اول لینک بین سوئیچ ها را در حالت Trunk قرار داد بعد VTP را اجرا کرد. یعنی اول DTP اجرا شود بعد VTP .

VTP PRUNING :

همانطور که می دانید Broadcastای که یک سوئیچ دریافت می کند از تمام پورتهایش به بیرون ارسال می کند . این باعث افزایش ترافیک بیهوده بر این کانال می شود . VTP Pruning می گوید که فریم های Broadcast در یک VLAN به سوئیچ هایی تحویل داده شود که پورتی در آن VLAN داشته باشند . در نتیجه ترافیک بیهوده روی کانال ارتباطی Trunk تحمیل نخواهد شد .



تنظیم پروتکل VTP بر روی سوئیچ :

تنظیم کردن VTP روی یک سوئیچ می بایست مراحل زیر را انجام دهید :

- تعیین نام **VTP Domain**

نام Domain را برای سوئیچ تعریف می کنیم . سوئیچ هایی که VTP Domain یکسان داشته باشند میتوانند اطلاعات مربوط به VLANها را با یکدیگر به اشتراک بگذارند . برای بار اول اگر Domain name را از Server تعیین کنیم رو همه سوئیچ های دیگر اعمال می شود چون domain همه Null است . ولی برای بار دوم یا بیشتر باید تک تک domain همه را وارد کنیم :

```
Switch ( config ) # Vtp  Domain  domain – name
```

- تعیین **VTP Mode**

سوئیچ ها به صورت پیش فرض Server Mode هستند . به کمک فرمان زیر می توان Mode vtp را تغییر دهیم :

```
Switch ( config ) # Vtp  Mode { Server | Client | Transparent }
```

- تعیین **VTP Version**

VTP دارای 3 ورژن 1 و 2 و 3 است . که ورژن 3 را ساپورت نمی کند و ورژن 2 , Takenring را ساپورت می کند ولی ورژن 1 ساپورت نمی کند .در ورژن 1 باید برای سوئیچ های Transparent حتما Domain name را تعریف کنیم ولی در ورژن 2 لازم نیست :

```
Switch ( config ) # Vtp  Version { 1 | 2 }
```

- تعیین **VTP Password**

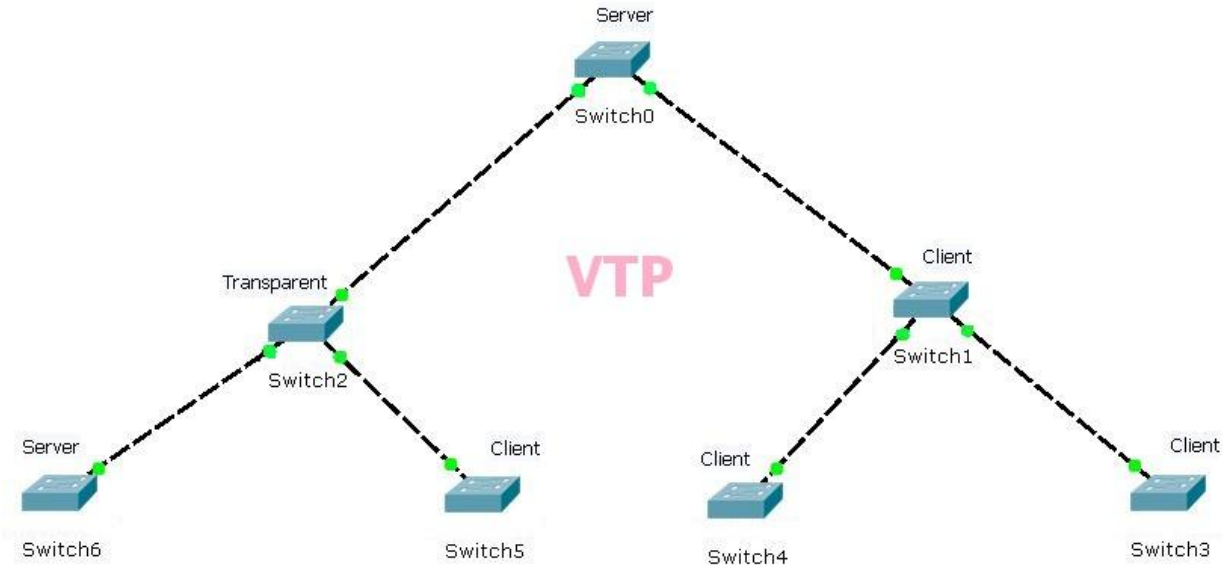
در یک VTP Domain با مشخص شدن VTP Server هر سوئیچ دیگری که Client Mode باشد اطلاعات مربوط به VLAN ها را از VTP server می گیرند . حال در صورتی که نخواهید هر کسی به راحتی بتواند سوئیچ خود را وارد شبکه کند و اطلاعات مربوط به VLANها را دریافت کند یا خرابکاری کند می بایست پس از انجام Authentication و یکسان بودن پسورد اطلاعات مربوط به VLAN را دریافت کند . با فرمان زیر پسورد را Set می کنیم :

```
Switch ( config ) # Vtp  Password  password
```

فعال کردن **VTP Pruning**

Switch (config) # Vtp Pruning

مثال :



دستوراتی که بر روی سوئیچ 1 اعمال می شود :

بررسی عملکرد VTP روی سوئیچ :

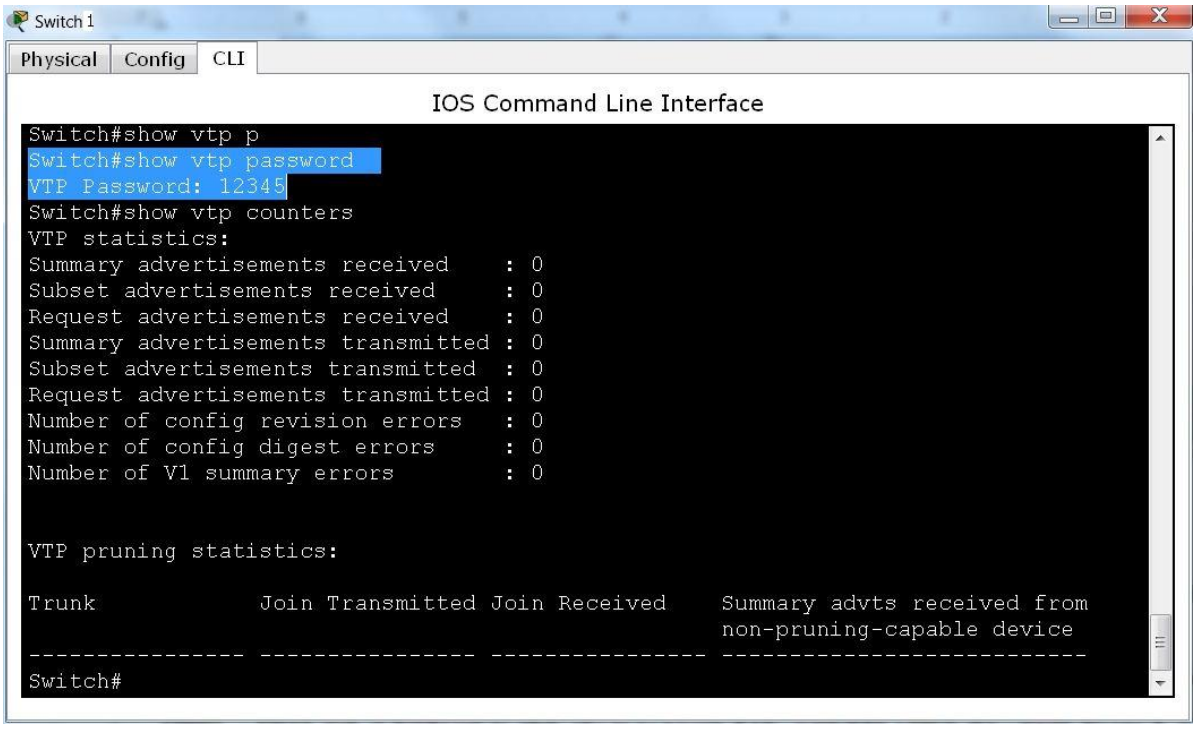
Switch #Show Vtp Password

Switch #Show Vtp Status

Switch #Show Vtp Counters

مثال : دستور Show Vtp Status در مثال بالا :

مثال : دستور Show Vtp Password و دستور Show Vtp Counters در مثال بالا :



Check کردن بسته های VTP توسط سوئیچ ها :

وقتی سوئیچ سرور بسته VTP را می فرستد همراه این بسته یک بسته VTP دیگری را که با رمز خود Hash شده می فرستد (این کار را با متد Massag Digest 5) انجام می دهد . سوئیچ Client هر دو بسته را دریافت می کند و بسته اصلی که حاوی اطلاعات VTP است را با رمز خود با استفاده از متد MD5 , Hash میکند و اگر نتیجه Hash خود با Hash فرستاده شده از سوئیچ Server برابر باشد بسته اصلی VTP را روی خود اعمال می کند و اگر برابر نباشد بسته را دور می اندازد .

Revision Number :

هر وقت در شبکه یک بسته VTP از طریق سرور ارسال شود و clientها آن را دریافت کنند و بر روی خود اعمال کنند یک واحد به Revision Number همه اضافه می شود .

Revision Numberها به دو صورت اضافه می شوند :

1. Topology Change : تغییر در ساختار VLAN شبکه به وسیله سرور .
2. هر 300 ثانیه یک بار بسته VTP در شبکه توسط سرور ارسال می شود .

سوئیچ ها وقتی بسته ای را دریافت می کنند قسمت Revision Number بسته را با قسمت Revision Number خود مقایسه می کنند اگر مساوی بود تغییرات را روی خود اعمال نمی کنند یعنی قبلا اعمال کرده اند ولی اگر بیشتر باشد آن وقت تغییرات را انجام می دهند . و یک واحد به Revision Number خود می افزایند .

نکته مهم :

اگر یک شبکه داشته باشیم و بعدا بخواهیم یک سوئیچ دیگری به این شبکه اضافه کنیم باید حتما Revision Number آن را صفر کنیم چون اگر Revision Number سوئیچ بیشتر از مقدار Revision number شبکه باشد دستورات خود را به کل شبکه ارسال می کند و سوئیچ های دیگر وقتی Revision Number بسته ارسالی را با Revision Number خود مقایسه می کنند و می بینند که بیشتر است , دستورات را روی خود اعمال می کنند و شبکه بهم ریخته می شود و خراب می شود .

چگونه Revision Number را در سوئیچ صفر کنیم :

1. VTP domain name را یک بار تغییر می دهیم
2. VTP Mode را یک بار عوض می کنیم

با این دو روش در هر دو حالت Revision Number صفر می شود و میتوانیم به شبکه وصل کنیم.

فایل Vlan.dat :

در حافظه Flash همه تنظیمات و اطلاعات مربوط به VLANهای شبکه را در خود ذخیره می کند. در سوئیچ های Server و Client در حافظه Flash ذخیره می شوند ولی در سوئیچ های Transparent در حافظه Running – config ذخیره می شود . برای دیدن محتویات فایل Vlan.dat در سوئیچ هایی که Server و Client هستند باید اول Mode آنها را تغییر دهیم به Transparent و بعد در حافظه Running – config می توانیم محتویات فایل را ببینیم.

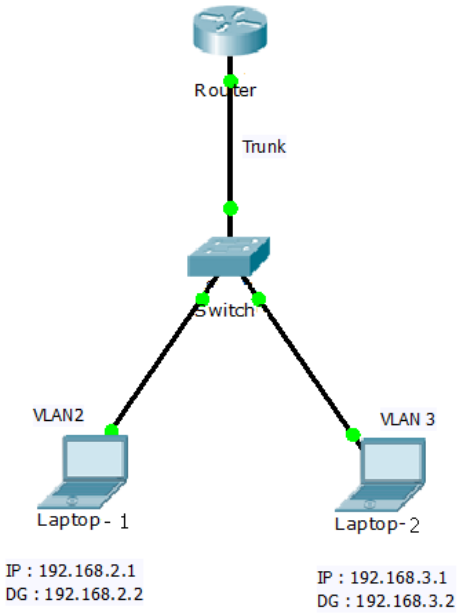
نکته :

برای خام کردن سوئیچ ها باید 3 مرحله زیر را انجام دهیم :

1. Erase Startup – config
2. Delete Flash : Vlan.dat
3. Reload

Inter Vlan Routing

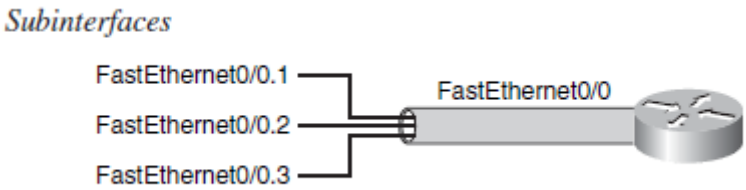
برای برقراری ارتباط PCهایی که در VLANهای مختلف عضویت دارند از INTER VLAN استفاده می کنیم .



روش اول :

از یک روتر استفاده کنیم . لینک سوئیچ و روتر باید به صورت Static در حالت Trunk قرار دهیم . در روتر بر روی اینترفیس 0/0 نباید IP تعریف کنیم آدرس IP بر روی SubInterface ست خواهد شد . تنها کار روتر TAG زدن و TAG برداشتن است .

: SubInterface



با این روش یک اینترفیس را به هر چند اینترفیس که لازم داشته باشیم می توانیم تقسیم کنیم ولی نباید برای اینترفیس اصلی IP تعیین کنیم .

دستورات اصلی :

Router (config) # Interface type Mod/Num

Router (config – if) # No shotdown

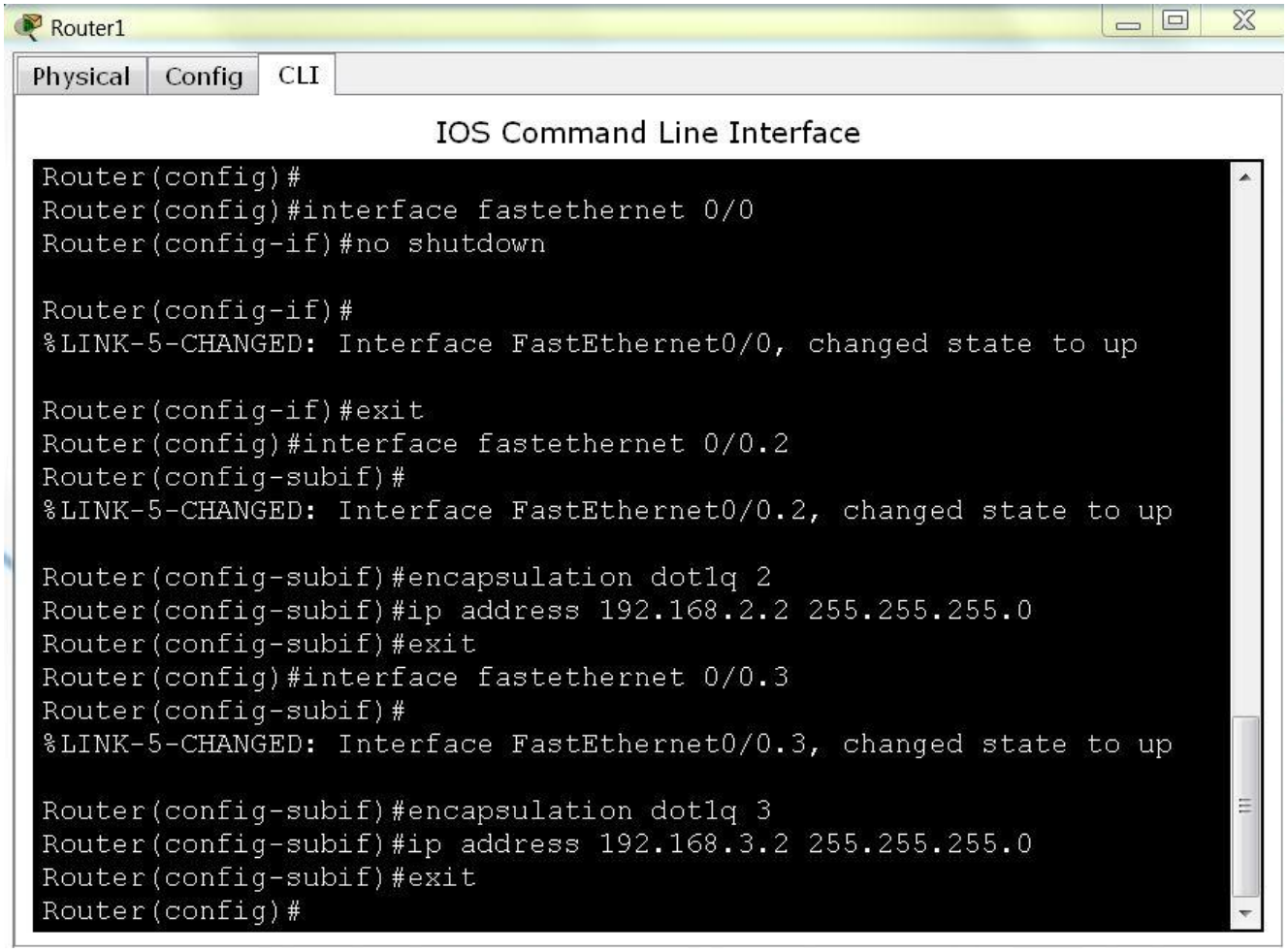
Router (config – if) # Exit

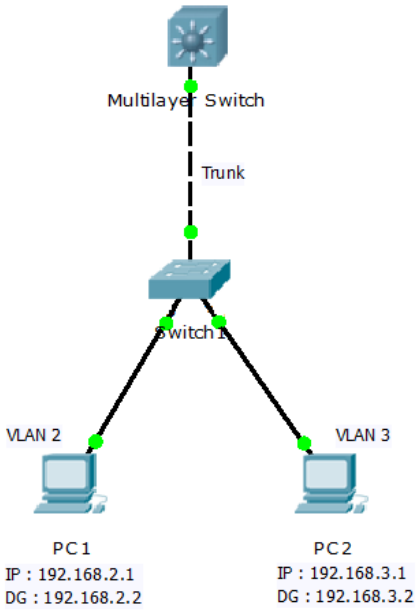
Router (config) # Interface FastEthernet Subinterface – number

Router (config – subif) # Encapsulation Dot1q vlan – number

Router (config – subif) # IP Address Default Gateway Subnet Mask

دستورات مثال شکل بالا :





روش دوم :

وقتی از یک سوئیچ لایه 3 یعنی مدل 3560 به جای روتر استفاده کنیم دستورات زیر را می زنیم . ولی اول باید DTP بعد VTP اجرا شود بعد مراحل پایین اجرا شود .

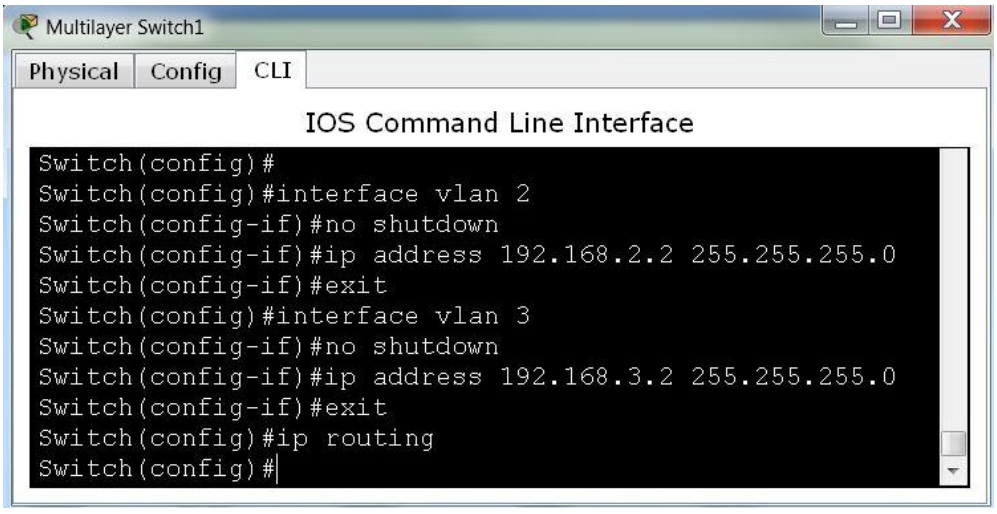
دستورات اصلی :

Switch (config) # Interface Vlan vlan - id

Switch (config – if) # IP Address Default Gateway Subnet Mask

Switch (config) # IP Routing

دستورات مثال بالا :



Spanning – Tree Protocol

: STP

وظیفه اصلی STP جلوگیری از رخ دادن Loop و متوقف کردن Loop رخ داده شده در لایه 2 می باشد . در واقع این کار را با Shutdown کردن لینک های اضافی انجام میدهد .

تمام سوئیچ های سیسکو با ورژن IEEE 802.1D کار می کنند .

STP با بکار بردن Spanning – Tree Algorithm یا همان STA , توپولوژی شبکه را به صورت درخت درآورده و سپس با غیر فعال کردن مسیرهای اضافی که منجر به رخ دادن Loop در شبکه شده اند , Loop رخ داده شده را مهار می کند . در شبکه انتخاب Root (ریشه) خیلی مهم است .

این پروتکل در 3 مرحله کار خود انجام می دهد :

1. Elect Root Bridge Per Network
2. Select Root Port Per Switch
3. Select designated Port Per Link (segment)

: Bridge ID

BID ملاک شناسایی یک سوئیچ در STP می باشد . در واقع مشخصه ای است که یک سوئیچ به کمک آن در میان سوئیچ های دیگر شناخته می شود .

BID : Bridge Priority + MAC Address

: Priority

عددی است که روی سوئیچ سیسکو به صورت Default : 32768 ست شده است و قابل تغییر نیز است , عددی بین 0 تا 65535 را می توانیم انتخاب کنیم . در سوئیچ اینطوری نمایش داده می شود :

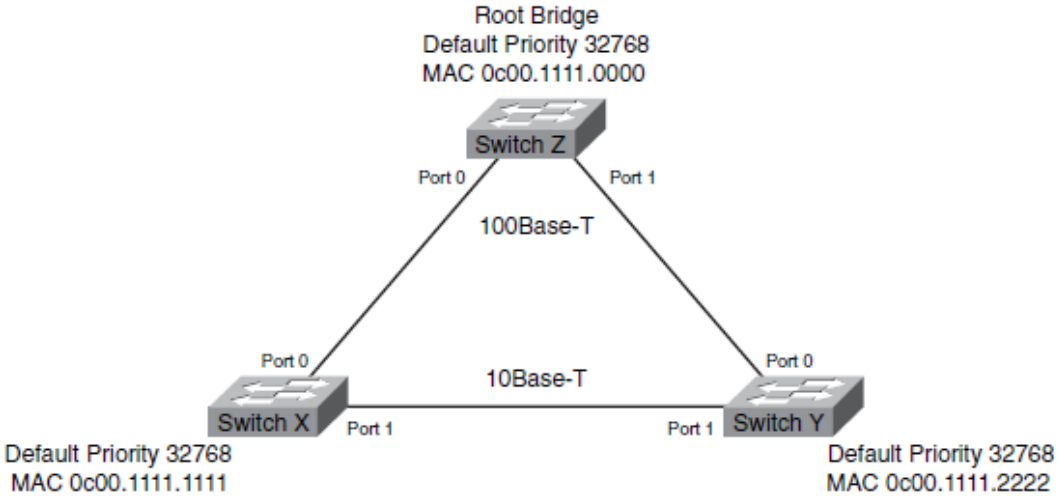
Bridge ID : 32768 : MAC Address

Root Bridge :

BID های سوئیچ های شبکه با هم مقایسه می شوند و سوئیچی که دارای پایین ترین BIDباشد به عنوان Root Bridge انتخاب می شود .

نکته : اولین معیار برای مقایسه , Priority می باشد . سوئیچی که پایینترین Priority را داشته باشد Root Bridge انتخاب می شود .

اگر Priority همه سوئیچ ها با هم برابر باشد در این حالت سوئیچی که دارای پایین ترین MAC Address باشد به عنوان Root Bridge انتخاب می شود .



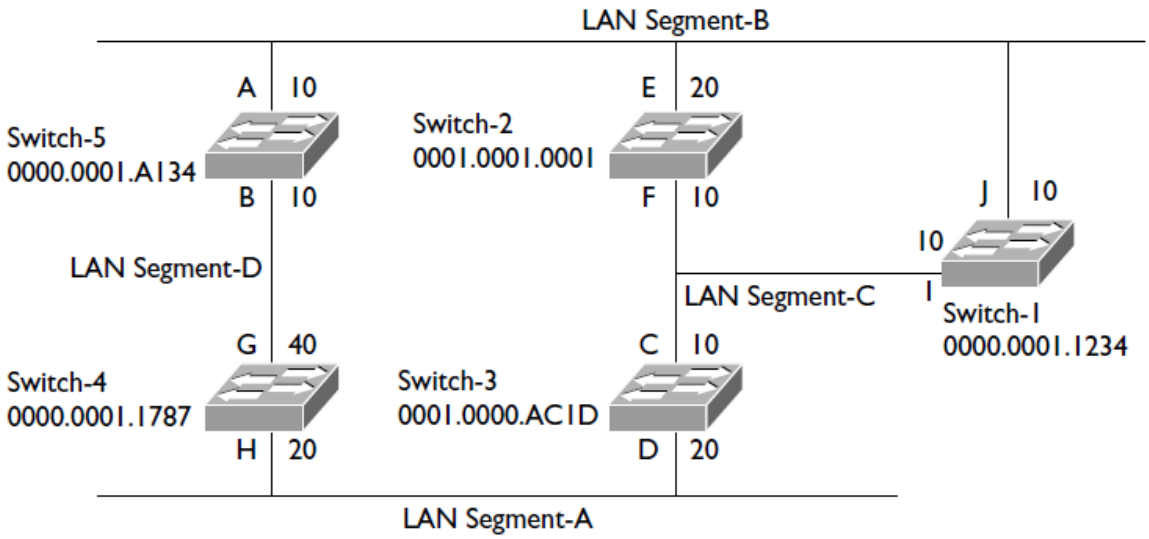
در شکل بالا چون priority همه سوئیچ ها برابر است و MAC سوئیچ Z از همه پایین تر است پس به عنوان Root Bridge انتخاب می شود .

BPDU : Bridge Protocol Data Unit

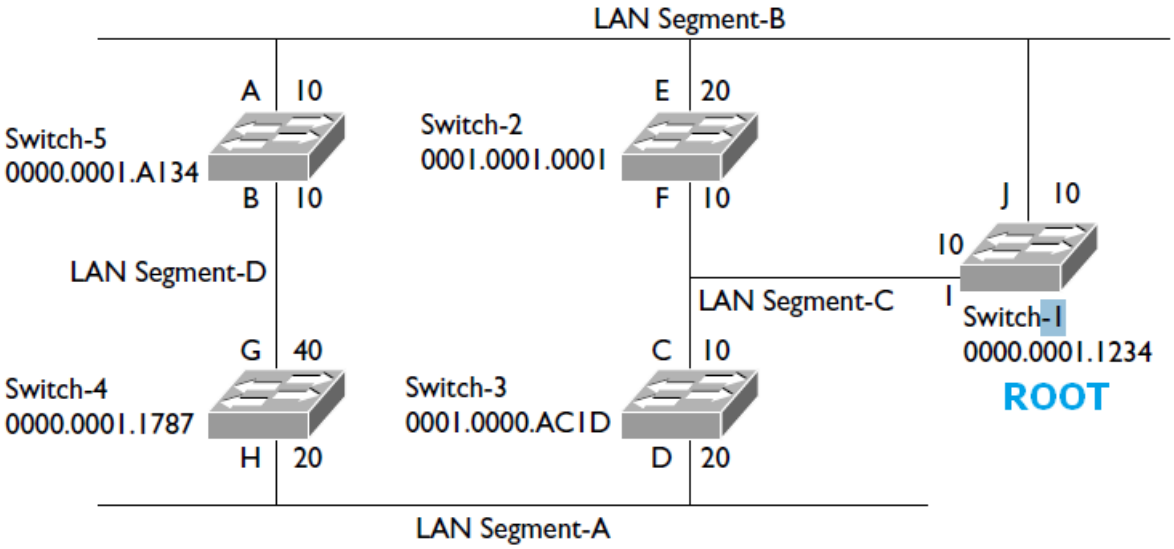
فریمی است که سوئیچ ها به کمک آن با هم تبادل اطلاعات می کنند , به کمک این فریم با یکدیگر صحبت می کنند و خود را به دیگران معرفی می کنند تا در نهایت بتوانند در شبکه Root Bridge را انتخاب کنند . همچنین هر گونه تغیراتی که بابت تغییر توپولوژی رخ دهد با این فریم ها به هم اطلاع می دهند .

مراحل STP :

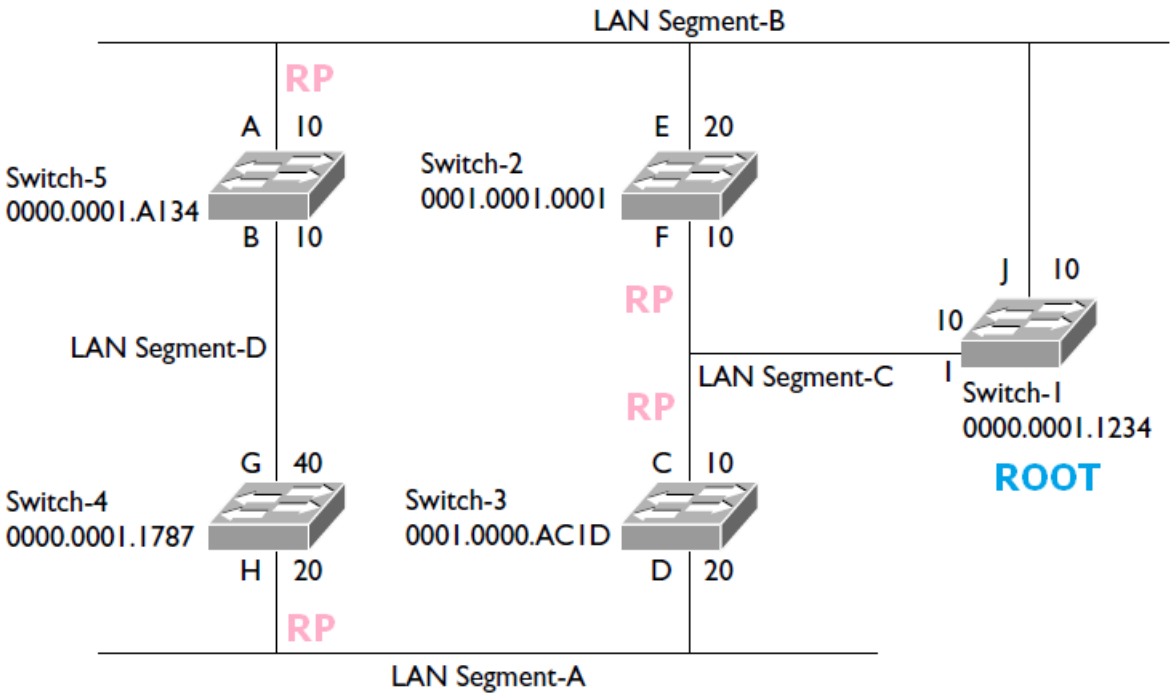
به شکل زیر توجه کنید :



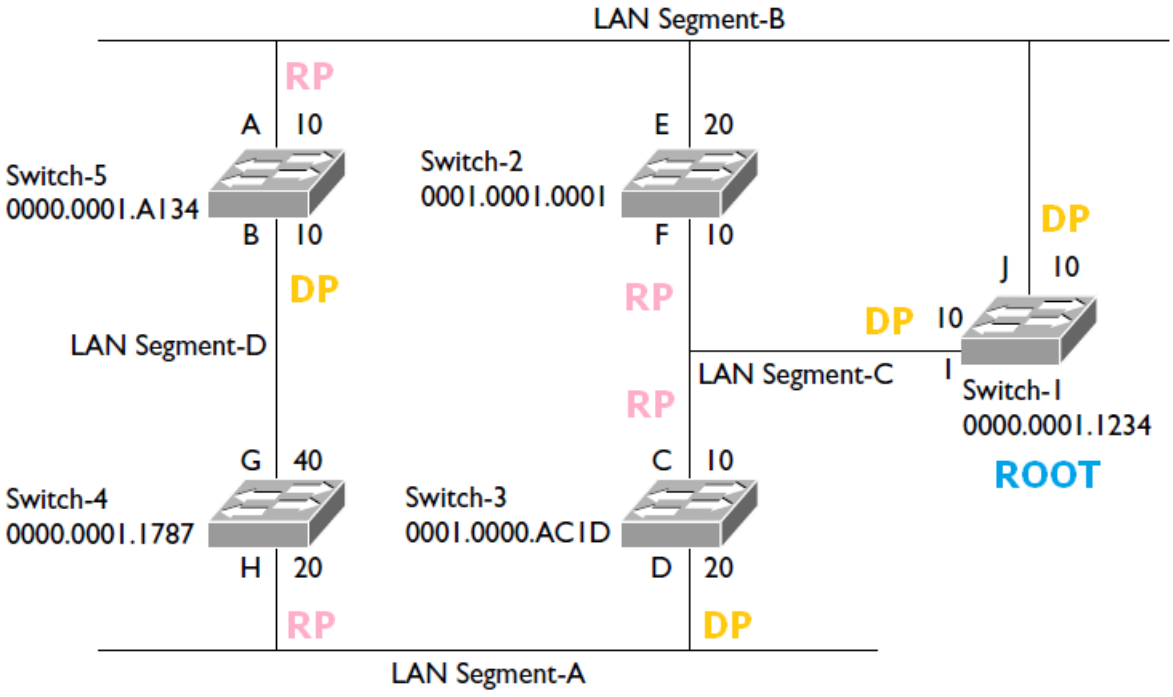
مرحله اول : **Root Bridge** انتخاب می شود



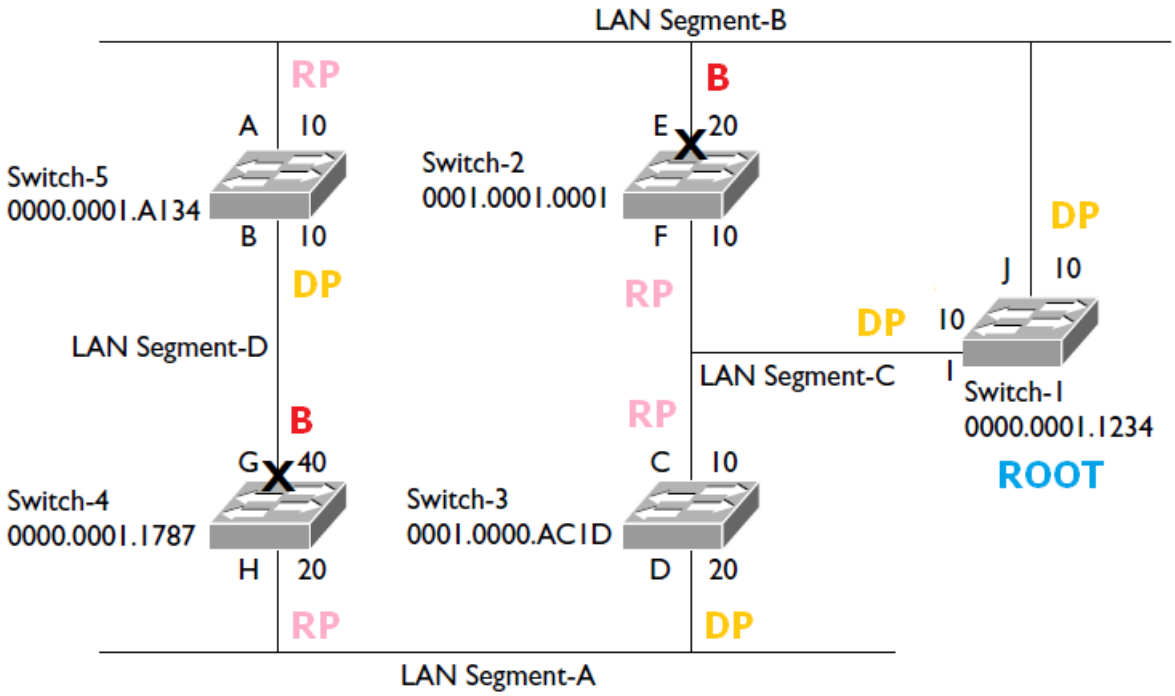
مرحله دوم : Root Port انتخاب می شود



مرحله سوم : Designated Port مشخص می شود



مرحله چهارم : لینک های **Block** تعیین و Shutdown می شوند



: Root Port

پورتی از سوئیچ که دارای کمترین Cost تا Root Bridge است .

: 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 .

: Block

لینک هایی که نه RP و نه DP باشد یا پورتی که دارای Cost بیشتری در مقایسه با RP باشد Block شده و مانع از رخ دادن Loop می شود . زمانی که یکی از پورت ها قطع شود این پورت وصل می شود .

نکته :

تمامی پورت هایی که به Root Bridge متصل هستند به عنوان DP انتخاب می شوند.

Cost نسبت عکس با Bandwidth دارد . این بیانگر آن است که با افزایش پهنای باند , Cost کم می شود .

در شروع شبکه هر سوئیچ یک فریم BPDU به شرح زیر تهیه و ارسال می کند:

1. Root Bridge " Bridge ID "
2. Sender Bridge " Bridge ID "
3. Root Path Cost
4. Sender Port ID

وقتی که Root Bridge یک شبکه مشخص شد از آن به بعد فقط او فریم های BPDU را می فرستد .

جدول هزینه (Cost) :

Spanning-Tree Path Costs

Link Speed	Cost (Revised IEEE Specification)	Cost (Previous IEEE Specification)
10 Gbps	2	1
1 Gbps	4	1
100 Mbps	19	10
10 Mbps	100	100

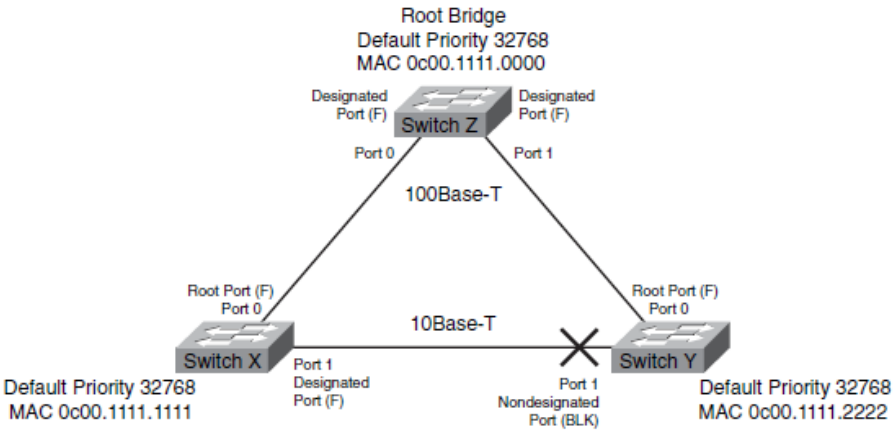
STP Port ID : Port priority . Port #

Priority عددی است بین 0 تا 255 که پیش فرض 128 است .

نکته :

Cost زمانی افزایش پیدا می کند که وارد اینترفیس سوئیچ شود نه خارج .

مثال :



فریم های BPDU که سوئیچ های شبکه شکل صفحه قبل به هم می فرستند :

BPDU Switch Z → Switch X

- Switch Z
- Switch Z
- 0
- 128 . 0

BPDU Switch Z → Switch Y

- Switch Z
- Switch Z
- 0
- 128 . 1

BPDU Switch X

- Switch Z
- Switch X
- 19
- 128 . 1

BPDU Switch Y

- Switch Z
- Switch Y
- 19
- 128 . 1

RP : پورتی است که BPDU با کاست کمتری دریافت بشود .

DP : پورتی است که BPDU با کاست کمتری روی آن ارسال می شود .

اگر COST برابر باشد به Sender Bridge ID نگاه می کند که کدام بهتر است یعنی کدام کمتر باشد آن را RP تعیین می کند .

اگر هم Cost هم Sender Bridge ID برابر باشند به Sender Port ID نگاه می کند هر کدام کمتر باشد آن را RP تعیین می کند .

تغییر Root Bridge :

روش اول : کم کردن Priority یک سوئیچ :

Switch (config) # Spanning – tree VLAN vlan – num Priority 0 – 65535

مثال :

Switch (config) # Spanning – tree VLAN 1 Priority 4096

روش دوم : روی سوئیچی که می خواهیم Root Bridge باشد این دستور را وارد می کنیم :

Switch (config) # Spanning – tree VLAN vlan – num Root Primary

این دستور را در سوئیچ دوم می زنیم تا اگر Root Bridge اول قطع شد این Root Bridge شود :

Switch (config) # Spanning – tree VLAN vlan – num Root Secondary

نکته :

پورتی که Block است قطع نیست ولی از Loop جلوگیری می کند یعنی خاموش است ولی فریم های BPDU را دریافت می کند .

STP Timer :

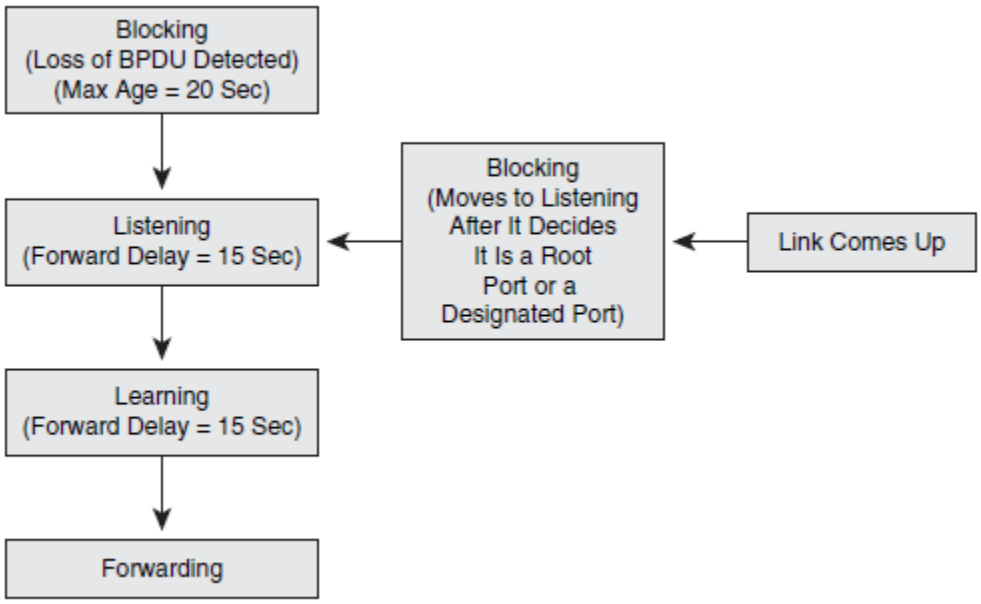
Hello – time : 2 sec

Max – age : 20 sec

Forward – Delay time : 15 sec

وضعیت پورت ها در STP :

1. **Disable** : در این حالت پورت نه فریمی را دریافت میکند نه ارسال . پورت به صورت دستی غیرفعال شده .
2. **Blocking** : وقتی سوئیچ را روشن می کنیم پورت ها در حالت blocking قرار دارند و هیچ فریمی را ارسال یا دریافت نمی کنند . در این حالت پورت ها فقط به BPDU ها گوش می دهند تا بتوانند در مورد وضعیت بعدی خود تصمیم بگیرند .
3. **Listening** : در این حالت هر سوئیچ با توجه به BPDUهایی که می شنود Root bridge را انتخاب می کند . بنابراین اگر به این پورت فریمی وارد شود که حاوی MAC Address جدیدی باشد در MAC Table خود ذخیره نمی کند .
4. **Learning** بعد از سپری شدن مدت زمان Listening پورت تغییر وضعیت داده و وارد حالت Learning می شود . در این حالت سوئیچ تمامی مسیرهای موجود در شبکه و مسیرهای فاقد Loop را شناسایی می کند .
5. **Forwarding** : بعداز اینکه Root Port و Designated Port بودن یک پورت مشخص شد در مرحله Forwarding پورت قادر به ارسال و دریافت فریم می باشد .



نکته :

مراحلی که یک پورت از حالت Block به حالت Forwarding تغییر وضعیت می دهد :

Blocking Port ⟶ Listening (15 sec) ⟶ Learning (15 sec) ⟶ Forwarding

	BPDU Send	BPDU Listening	MAC_Address Learning	Data Forwarding
Block	NO	YES	NO	NO
Listening	YES	YES	NO	YES
Learning	YES	YES	NO	NO
Forwarding	YES	YES	YES	YES

با دستور زیر BPDU guard را بر روی اینترفیس فعال می کنیم :

Switch (config - if) # Spanning – tree BPDU guard enable

: Port – Fast

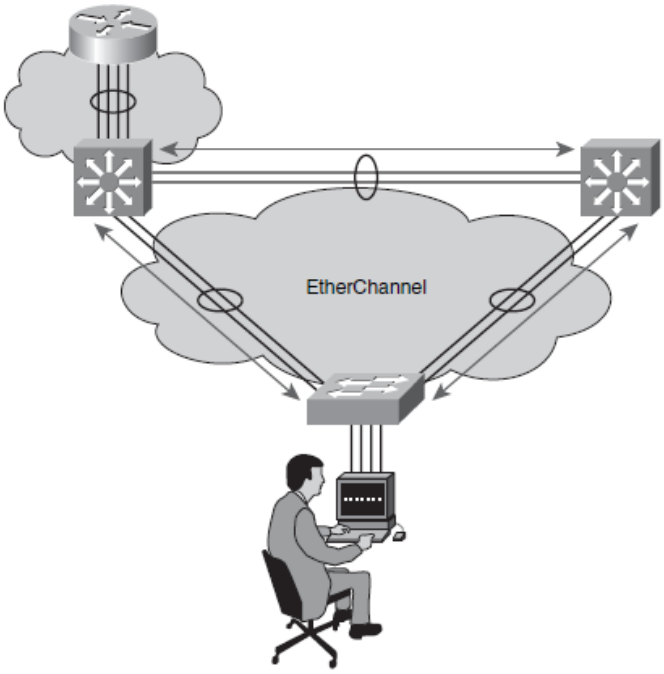
مختص دستگاه های سیسکو است که باعث می شود مراحل Listening و Learning روی اینترفیس های Access صورت نگیرد و زودتر فعال شود .

Switch (config) # Spanning – tree Pore – Fast default

Switch (config – if) # Spanning – tree Pore – Fast

نکته : حتما Port – Fast روشن شود .

EtherChannel



Etherchannel توانمندی می باشد که اجازه می دهد چندین پورت فیزیکی سوئیچ در یک گروه منطقی قرار گیرند که به منظور دسترسی به پهنای باند بالاتر و ایجاد تحمل خطا در اتصالات بین سوئیچ ها استفاده می شود که به شما اجازه خواهد داد از مجموعه پهنای باند اتصالات فیزیکی که در گروه منطقی قرار دارند استفاده کنید .

در گروه Etherchannel می توانیم از پورت های FastEthernet و GigabitEthernet استفاده کنید که میزان پهنای باند بین سوئیچ ها افزایش یابد . می توانیم دو یا چهار یا هشت پورت فیزیکی را داخل یک گروه قرار دهیم .

مهم نیست که پورت ها به ترتیب و پشت سر هم انتخاب شوند . همه پورت های شرکت کننده باید دارای سرعت و Duplex مساوی و Enable و فعال باشد .

Etherchannel دارای 2 پروتکل PAgP و LACP است که با یکدیگر سازگار نمی باشند .

باید پورت ها همه یا در حالت Access یا در حالت Trunk باشند .

پروتکل های مدیریت اتصالات Etherchannel :

PAgP : Port Aggregation Protocol

یک پروتکل انحصاری مربوط به شرکت سیسکو می باشد . در صورتی می توان از این پروتکل استفاده نماییم که تجهیزات دو طرف اتصال شما سیسکو باشد .

LACP : Link Aggregation Control Protocol

این پروتکل توسط همه شرکتها پشتیبانی می شود و اگر تجهیزات شما از شرکت های متفاوتی باشند می توان از این پروتکل استفاده کرد . در این پروتکل می توان تا 16 پورت را در یک باندر جای داد ولی 8 تای آن Active است اگر یکی از پورت ها قطع شود به صورت اتوماتیک یکی دیگر از پورت ها فعال می شود .

Mode های پروتکل های PAgP و LACP :

EtherChannel Modes

Mode	Protocol	Description
auto	PAgP	Passively listens for PAgP queries from a Cisco device configured with either *desirable* or *on*. By default the interface is not part of a channel.
desirable	PAgP	Generates PAgP queries to form a channel, but by default is not part of a channel.
on	PAgP & LACP	Generates PAgP queries and assumes the port is part of a channel.
active	LACP	Enables a channel if the other side responds to its LACP messages.
passive	LACP	Passively listens for LACP messages to form a channel from an active port.

Auto : در این مد هیچ پیام PAgP از طرف اینترفیس ارسال نمی شود ولی آماده پاسخ گویی به پیام های PAgP از سوئیچ مقابل می باشد و قادر به آغاز PAgP Negotiation نیست.

Desirable : در این مد اینترفیس پیام های PAgP را ایجاد و به طرف سوئیچ مقابل ارسال می کند و قادر به آغاز PAgP Negotiation می باشد .

On : این مد باعث فعال شدن Etherchannel بر روی اینترفیس ها می شود بدون ارسال هیچ پیام LACP و PAgP .

Active : در این مد اینترفیس پیام های LACP را ایجاد و به طرف سوئیچ مقابل ارسال می کند و قادر به آغاز LACP Negotiation می باشد .

Passive : در این مد هیچ پیام LACP از طرف اینترفیس ارسال نمی شود ولی آماده پاسخگویی به پیام های LACP از سوئیچ مقابل است و قادر به آغاز LACP Negotiation نمی باشد .

PAgP →

Switch A \ Switch B	Auto	Desirable	On
Auto	NO	YES	NO
Desirable	YES	YES	NO
On	NO	NO	YES

LACP →

Switch A \ Switch B	Passive	Active	On
Passive	NO	YES	NO
Active	YES	YES	NO
On	NO	NO	YES

دستورات زیر را در دو طرف لینک وارد می کنیم :

Switch (config) # Interface type mod/num

Switch (config – if) # Channel – Protocol { PAgP | LACP }

Switch (config – if) # Channel – group number Mode mode

دستورات نمایش وضعیت Etherchannel :

Switch # Show Etherchannel

Switch # Show Etherchannel Load – balance

Switch # Show Etherchannel Port – channel

Switch # Show Etherchannel Summary

ترافیک بین لینک ها :

Load Balancing metod

- Src – MAC
- Dst – MAC
- Src , Dst – MAC
- Src – IP
- Dst – IP
- Src , Dst – IP

Switch : 2960 & 2950 & 3750 & 3760 & 3550

- Src – Port
- Dst – Port
- Src , Dst – Port

switch : 6500 & 4500

دستور Load Balancing :

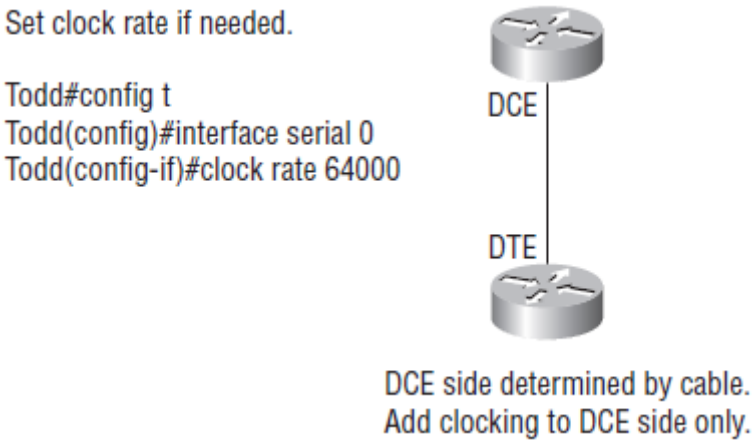
Switch (config) # Port Channel load – balance metod

Router

Cisco 28000 Series Routers

روتر (مسیریاب) وسیله ای است که جریان بسته های داده ای را که در داخل شبکه محلی آدرس دهی نشده اند , اداره می کند . روتر نیاز به شناخت تمامی مسیرها به شبکه های محلی مختلف را دارد . در واقع روتر باید بداند از کدام مسیر 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 است . بنابراین روتر با شناخت کل شبکه و مسیرهای موجود درخواست هایی را که نتواند در شبکه محلی پیدا کند به بیرون هدایت می کند و آن را در مسیر مناسب قرار داده و هدایت می کند . روتر می بایست اطلاعات مربوط به شبکه های غیر محلی را در یک Database به نام جدول Routing Table نگهداری کند تا با ورود یک Packet که آدرس مقصد آن شبکه ای غیر محلی می باشد , در سریعترین زمان ممکن هدایت کند . اینترفیس های روتر آدرس IP می گیرند . بر خلاف سوئیچ ها اینترفیس کمی دارند ولی تنوع زیادی دارد . اینترفیس های روتر را حتما باید روشن یا فعال کرد .

روترها با کابل Serial به هم وصل می شوند . یک سر کابل Serial به نام DTE و سر دیگر کابل DCE نام دارد . باید فقط در طرف DCE کابل سریال Clock Rate را تنظیم کنیم .



نکته :

باید اول روتر را خاموش کنیم بعد ماژول های اینترفیس های متفاوت را نصب کنیم و بعد روشن کنیم . روتر بر خلاف سوئیچ به وسیله دکمه Power روشن و خاموش می شود .

نمایش وضعیت روتر :

Router # Show IP Interface

Router # Show Controllers Serial number

Routig Table :

تفاوت جدول مسیریابی روتر با سوئیچ :

Switching	Routing
MAC – Address – Table	Routing – Table
MAC – Address	IP – Address
Unknown MAC – Address → Flood	Unknown MAC – Address → Drop
Broadcast → Flood	Broadcast → Drop
Automatic & Static Learning	Dynamic & Static Learning

IP دهی به اینترفیس های روتر به دو صورت Static و Dynamic امکانپذیر است :

Static IP :

Router(config)#IP Route Dst – IP Dst – subnet { Interface |Next – Hop }

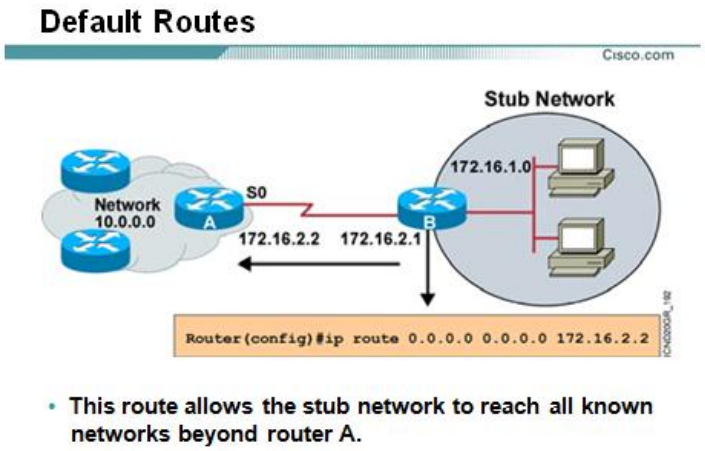
مثال :

Router (config) # IP Route 192.168.1.0 255.255.255.0 Se 0/0

Router (config) # IP Route 192.168.1.0 255.255.255.0 11.0.0.2

نکته :

در شبکه های Point to Point فرقی نمی کند از این دو حالت استفاده کنیم ولی در شبکه های دیگر باید حتما از حالت Next – Hop استفاده کرد.



مسیر پیش فرض (Default Route) :

به شبکه شکل بالا نگاه کنید . شبکه 172.16.1.0 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 تمام 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 . برای این منظور کافی است Packet که آدرس مقصدش جای دیگری به غیر از شبکه محلی است , مسیردهی شده و از این شبکه خارج شود تا توسط روترهای دیگر مسیردهی شود و به مقصد برسد .

دستور Default Route :

Router (config) # IP Route 0.0.0.0 0.0.0.0 { Interface | Next – Hop }

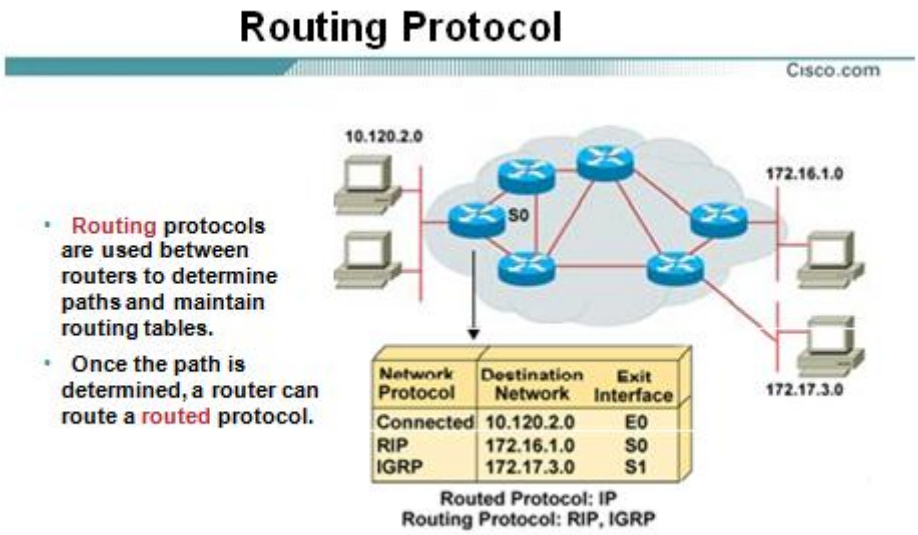
Default Route دارای اجزای زیر می باشد :

0.0.0.0 : این IP جزء IP های رزرو شده ای میباشد 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 | Next – Hop : معرفی IP آدرس 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 .

Dynamic Routing Protocol



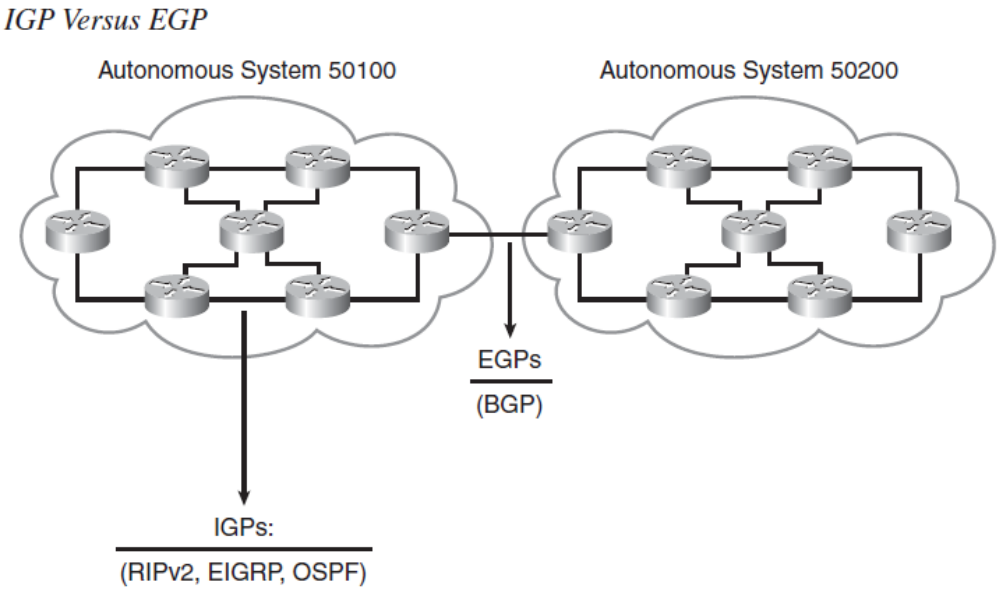
Dynamic Routing Protocolها دارای عملکرد غیر دستی می باشد . یعنی ما به صورت دستی شبکه های غیر محلی را به روتر معرفی نمی کنیم . این شناخت از طریق روترهای مجاور صورت می گیرد . هر کدام از این Routing Protocolها دارای الگوریتم مخصوص به خود هستند و به کمک اطلاعات به دست آورده نسبت به انتخاب مسیر تصمیم گیری می کنند .

Routed Protocol :

به پروتکل های IP و IPX که در لایه Network عمل می کنند گفته می شود .

Routing Protocol :

به پروتکل های مسیریابی چون RIP و OSPF و EIGRP گفته می شود که وظیفه مسیریابی به شبکه های غیر محلی را دارند .



: Autonomous System

مجموعه ایی است از روترهایی که تحت یک مدیریت واحد فعالیت میکنند.AS میتواند 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 .

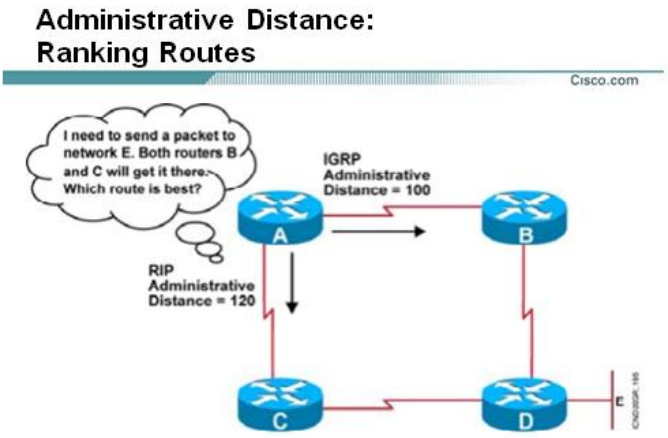
IGP : Interior Gateway Protocol

به تمامی Routing Protocolهایی که روترهای درون یک AS را به یکدیگر مرتبط می کند , گفته می شود و در واقع پروتکل هایی هستند که در یک AS فعالیت می کنند . RIP و IGRP و OSPF و EIGRP همگی جزء پروتکل های مسیریابی هستند که در داخل یک AS فعالیت می کنند .

EGP : Exterior Gateway Protocol

به تمامی پروتکل 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

AD معیار و ملاکی برای انتخاب Routing در میان روش های مختلف مسیریابی می باشد. سیسکو به هر کدام از این پروتکل های مسیریابی یک عدد نسبت داده است که هر کدام کمتر باشد روتر حرف آن را قبول میکند.به این عدد AD می گویند که عددی است بین 0 تا 255 .

نکته :

مسیرهایی Connected عدد AD آنها 0 است و اهمیت بیشتری دارند از همه مهمتر است . اگر مسیری را Static معرفی کنیم اولویتش از پروتکلهای مسیریابی بیشتر است ولی از Connected کمتر است .

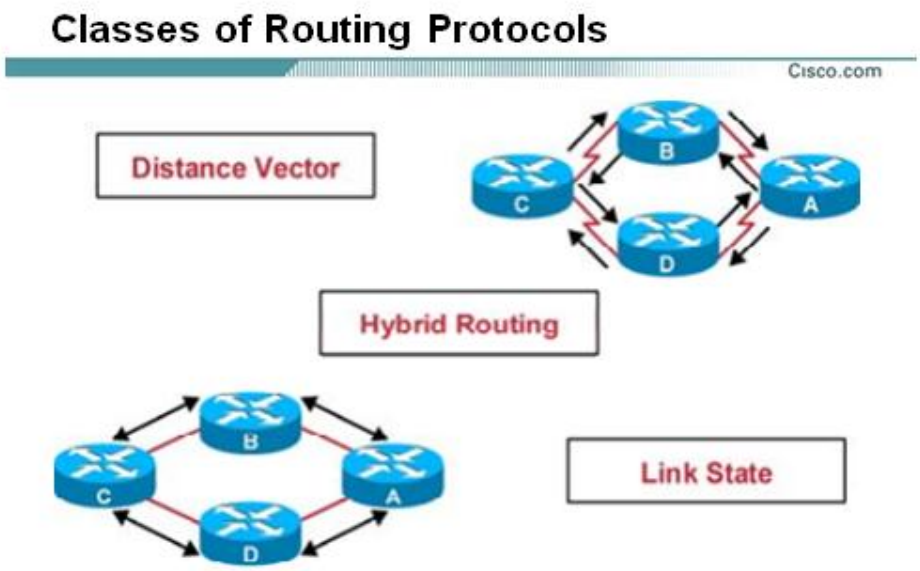
جدول AD :

Default Administrative Distance Values

Route Source	Default Distance
Connected network	0
Static route	1
EIGRP	90
OSPF	110
RIP	120
External EIGRP	170
Unknown or unbelievable	255 (will not be added to the routing table to pass traffic)

نکته:

اگر IP Route را با نام اینترفیس (Se 0/0) وارد کنیم به صورت Connect تعریف میشود ولی اگر به صورت Next – Hop تعریف کنیم به صورت Static تعریف میشود و AD آن برابر با 1 است .



Dynamic Routing Protocol ها به سه دسته کلی تقسیم می شوند :

Distance Vector

به Roting Protocolهایی گفته می شود که هر روتر فقط با روتر مجاورش به تبادل اطلاعات می پردازد . RIP در این دسته قرار دارد .

Link State

به Roting Protocolهایی گفته می شود که هر روتر ابتدا باید یک تصویر کلی از کل شبکه یا ناحیه ای که روتر در آن واقع شده است را داشته و سپس با داشتن این دید کلی عملیات مسیریابی را انجام دهد . OSPF و IS – IS در این دسته قرار دارند .

Hybrid Routing

این دسته ترکیبی است از ویژگیهای Link State و Distance Vector . چون بین روتر مبدا و روتر مقصد یک بردار در نظر می گیرد و می بایست یک تصویر کلی از شبکه را داشته باشد . EIGRP در این دسته قرار دارد .

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

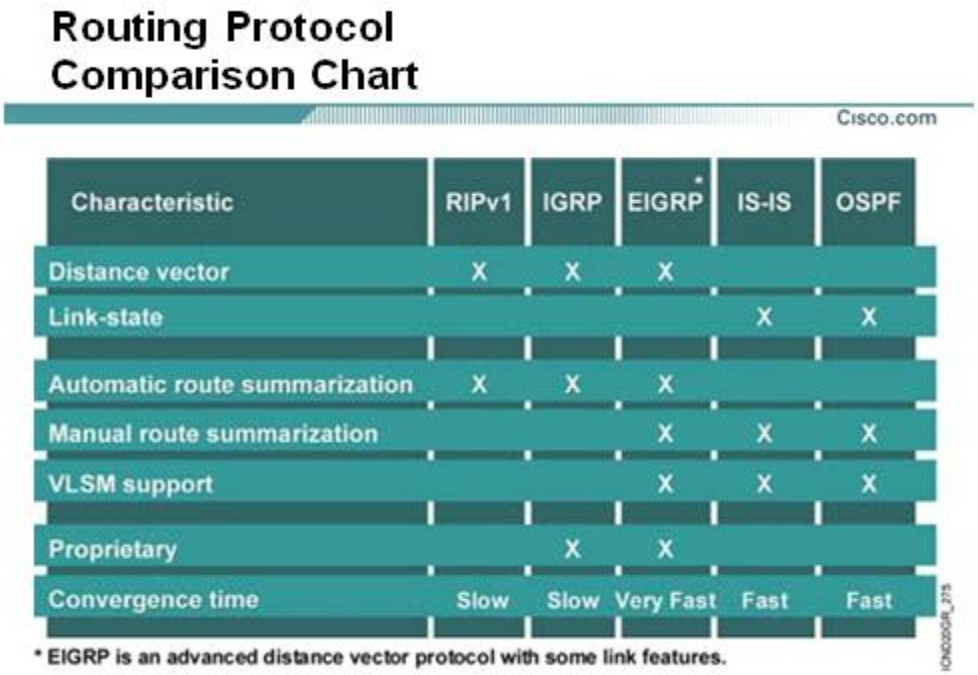
1. Classful Routing

به Routing Protocolهایی گفته می شود که VLSM را ساپورت نمی کند . این بدان معنی است که یک روتر شبکه ای را به روتر دیگری معرفی می کند همراه با آن Subnet Mask مربوط به آن شبکه را گزارش (Advertise) نمی کند . RIP Version 1 و IGRP در این دسته قرار دارند .

2. Classless 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 گزارش (Advertise) می کند . RIP Version 2 و EIGRP و OSPF و IS – IS در این دسته قرار دارند .

جدول مقایسه بین Dynamic Routing Protocol های مختلف :



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

: (RIP v1) Routing Information Protocol

این پروتکل بر اساس جهت کار می کند . هر روتر به روتر مجاورش مسیرهایی را که دارد معرفی می کند و همه مال هم را در Routing Table خود ذخیره می کنند و روترها با بررسی جهت , خوبی و بدی مسیر را تعیین می کنند و مسیر بد را پاک می کنند. تنها معیار متریک پروتکل RIP تعداد روتر (Hop Count) آن مسیر است .

این پروتکل جهت Update جدول مسیریابی بین روترهای شبکه از پیام های Broadcast استفاده می کند که هر 30 ثانیه یک بار کل جدول مسیریابی را از طریق اینترفیس های فعال منتشر می کند. محدودیت Hop Count 15 (تعداد روتر) را دارد . این پروتکل Classful است و در صورتی که چندین مسیر Hop Count یکسان داشته باشند Load balancing بین مسیرها به وجود خواهد آمد . حداکثر بر روی 6 مسیر با متریک یکسان می توان Load balancing را ایجاد کرد .

بسته های ارسالی RIP هر 30 ثانیه یک بار فرستاده میشود و بدون تغییر هستند که به این بسته ها Hello Time می گویند (Interval Update). اگر یک روتر 6 عدد Hello Time که 180 ثانیه میشود را دریافت نکند که Dead Time نام دارد مسیر را پاک می کند .

: Metric

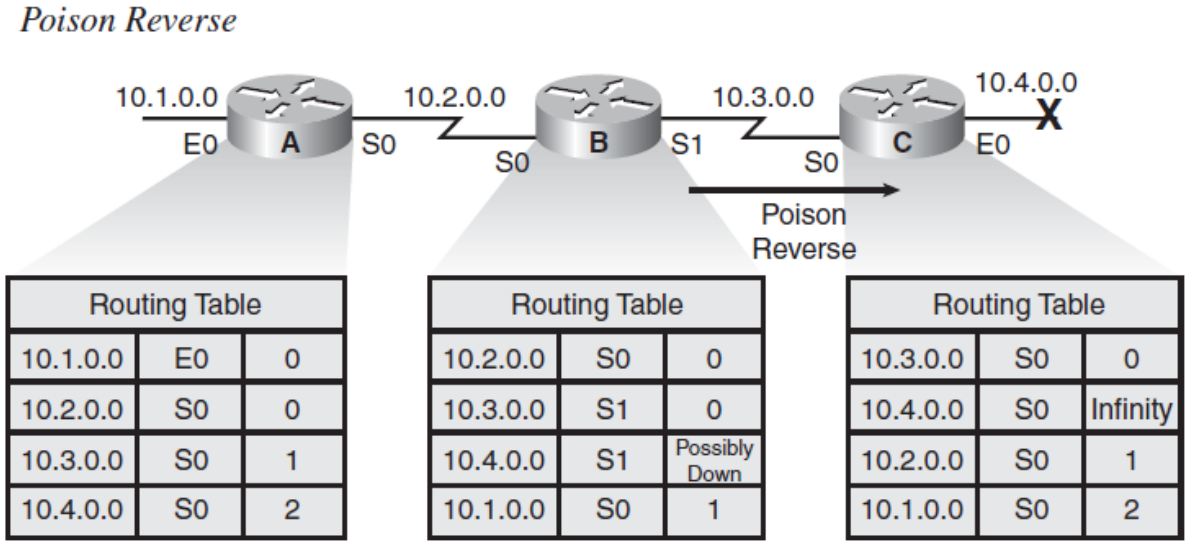
ممکن است در شبکه Internetwork شما , برای رسیدن به یک شبکه چندین مسیر یا لینک وجود داشته باشد در این وضعیت از واحدی به نام متریک برای انتخاب بهترین مسیر استفاده می شود . هر پروتکل مسیریابی به یک شکل و فرم متریک را محاسبه می کنند .

: Triggered update

با این مکانیزم اگر هر وقت مسیری قطع یا وصل شود همان لحظه بسته ای می فرستد و به همه اطلاع می دهد در RIP ورژن 2 قرار دارد ولی در ورژن 1 این مکانیزم وجود ندارد .

Loop لایه سوم :

اگر 2 روتر با هم بسته ای را ردوبدل کنند در یک زمان به صورت اتفاقی Loop به وجود می آید .



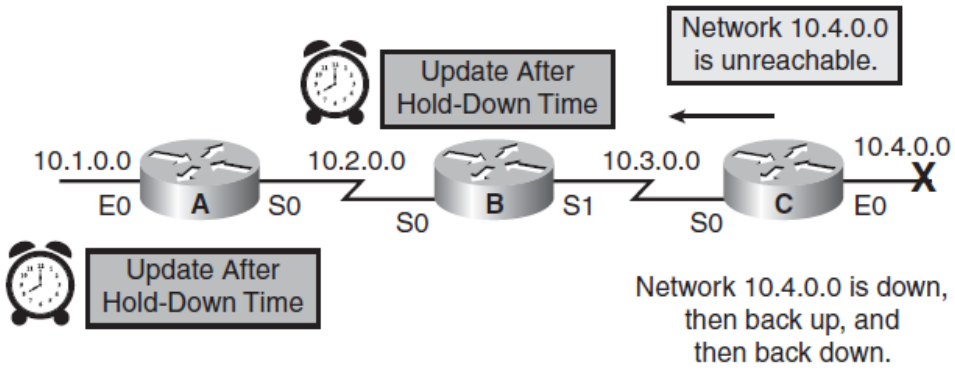
مکانیزم Root Poisoning :

با این مکانیزم اگر یک مسیر قطع شود پروتکل RIP در بسته های Broadcast مقدار Hop Count را عدد 16 می گذارد و به روتر بعدی می فرستد تا بفهمد آن شبکه مسیرش قطع است .

مکانیزم Split – Horizon :

یعنی وقتی مسیری را از کسی یاد گرفتی به خودش یاد نده .

Hold-Down Timers



: Flash timer & Hold – Down timer

اگر روتر 1 به روتر 2 بگوید مسیری قطع شده است و عدد 16 را بفرستد , روتر 2 مسیری که قطع است را پاک نمی کند در حالت Stene نگه می دارد تا همه بفهمند قطع است چون اگر زودتر مسیر را پاک کند امکان دارد دوباره مسیری را بهش پیشنهاد دهند و آن را قبول کند و Loop رخ دهد. مدت Stene , 180 ثانیه است که Hold Down timer می گویند . بعد از این مدت نیز 60 ثانیه دیگر اضافه نگه می دارد که به آن Flash timer می گویند و بعد از این مدت اگر خبری نیامد مسیر را پاک می کند . اگر قبل از این مدت مسیر وصل شود و بسته ای را دریافت کند از حالت Stene درمی آورد .

دستورات RIP ورژن 1 :

Router (config) # Router RIP

Router (config – router) # Network IP Address

Router (config) # Version 1

دستور نمایش وضعیت RIP :

Router # Show IP Protocol

در جدول RIP در جلوی IPهایی که به صورت RIP وارد شده اند حرف R نوشته میشود.

(1 / 120) عدد 1 متریک است و عدد 120 , AD پروتکل است .

تفاوت RIP ورژن 1 با ورژن 2 :

RIPv2	RIPv1
Multicast : 224.0.0.9	Broadcast : 255.255.255.255
Max Hop Count of 15	Max Hop Count of 15
Classless	Classful
Sending Subnet Mask	Not Sending Subnet Mask
Support VLSM Network	No Support VLSM Network
Authentication	No Authentication

برای فعال سازی ورژن 2 کافی است که دستورات RIP ورژن 1 را وارد کنیم و فقط دستور Version 2 را وارد کنیم .

نکته :

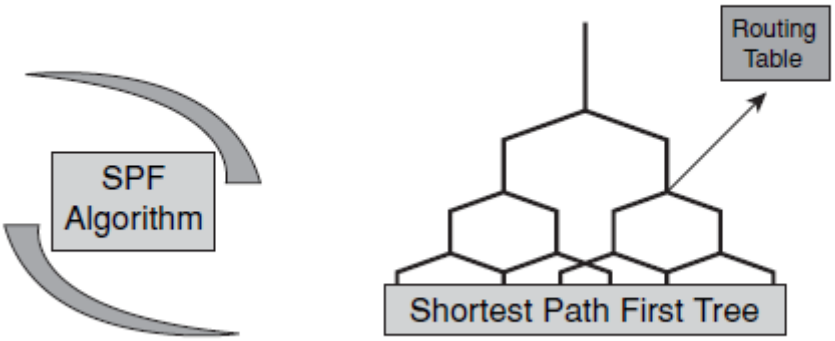
در سوئیچ ها IGMP خاموش است . اگر روشن باشد و در بین دو روتر قرار بگیرد 224.0.0.9 را مستقیم به اینترفیس روتر می فرستد ولی اگر خاموش باشد روی همه اینترفیس ها می فرستد ولی Userها (PC) آن را آنالیز نمی کنند .

نکته :

در RIP v2 حتما IP و Subnet Mask را با هم می فرستد تا روترها در تشخیص شبکه اشتباه نکنند . پیش فرض RIP v2 : Classful است باید با دستور پایین به Classless تبدیل کنیم :

```
Router ( config – Router ) # No auto Summary
```

OSPF : Open Shortest Path First



OSPF : این پروتکل داخل AS عمل می کند . یک پروتکل بر پایه ویژگی های Link – State می باشد . توپولوژی شبکه را به صورت یک درخت همبند بدون دور درآورده سپس با استفاده از الگوریتمی تحت عنوان Dijkstra کوتاهترین مسیر را پیدا می کند و در Routing Table خود قرار می دهد.

دو ورژن دارد :

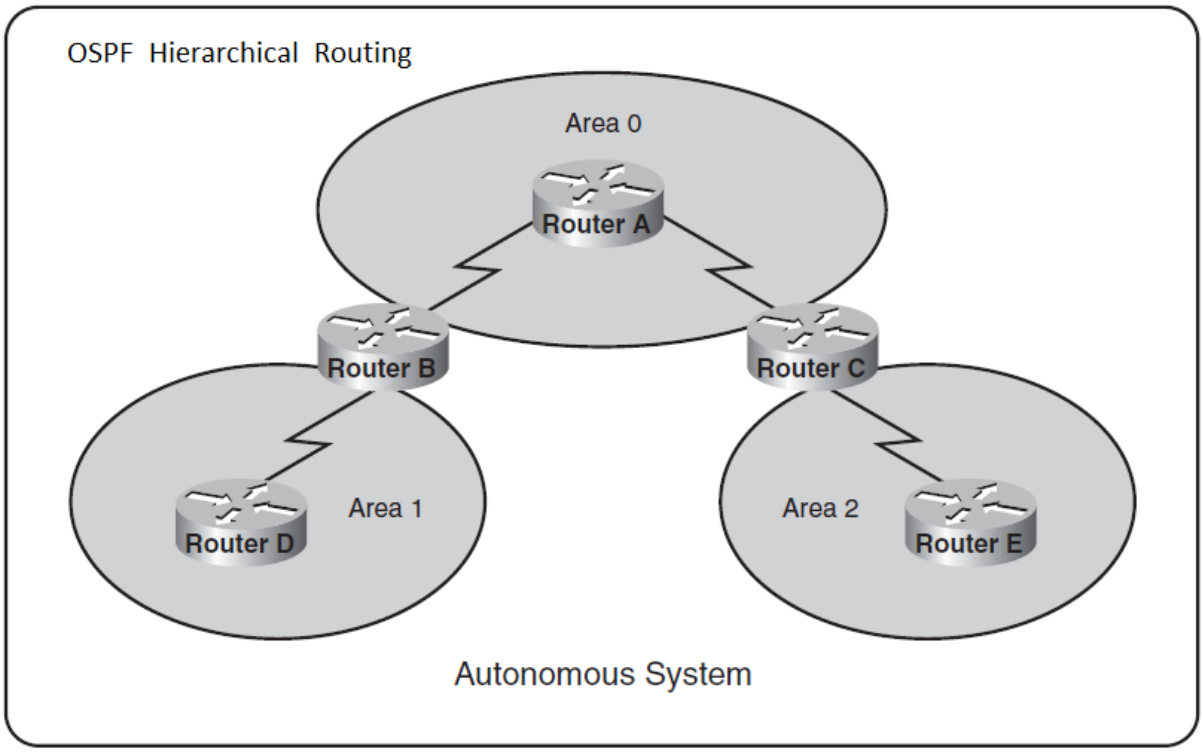
OSPF v2 ⟶ IP v4

OSPF v3 ⟶ IP v6

در OSPF یک AS به چندین ناحیه تحت عنوان Area تقسیم می شود که هر کدام از این Areaها شامل Networkهای مختلفی می باشد .

مزایای طراحی Hierarchical یک AS :

1. افزایش سرعت محاسبه الگوریتم SPF
2. کوچک شدن Routing Table
3. کاهش Overhead و اندازه Database و در نتیجه کاهش ترافیک در شبکه



Area : اگر تعداد روترها در شبکه بیشتر شود پروتکل OSPF زمان بیشتری طول می کشد که جداول خود را تکمیل کند و سرعت شبکه پایین می آید برای رفع این مشکل شبکه را به Areaهای متعددی تقسیم می کند . پیش فرض صفر است .

الگوریتم OSPF هر روتر را به عنوان ریشه درخت و سپس روترهای دیگر را به صورت شاخه های درخت در نظر می گیرد . بنابراین کوتاهترین مسیر به هر کدام از Nodeها را بر اساس متریک Cost محاسبه کرده و در Routing table خود قرار می دهد .

Cost مربوط به یک اینترفیس رابطه معکوس با Bandwidth دارد .

فرمول محاسبه Cost در پروتکل OSPF :

Cost = 100000000/ Bandwidth

جداول OSPF :

- Topology – Table
- Routing – Table
- Neighbor – Table

شرایط لازم برای تشکیل جدول بین دو یا چند Router :

Subnet Number	باید در هر دو روتر برابر باشد
Subnet Mask	
Hello Time → 10 s	
Dead Time → 40 s	
Password	باید برابر باشند

نکته :

در دو روتر که از پروتکل OSPF استفاده می کنند زمانی با هم ارتباط برقرار می کنند که اول بین آنها همسایگی (Neighbor) تشکیل شود بعد مرحله Topology Change و بعد OSPF اجرا شود و Routing Table درست شود .

هدف از همسایگی (Neighbor Ship) :

1. اطمینان از پارامترهای همسایگی
2. اطمینان از زنده بودن روتر همسایه (alive)

مراحل تشکیل همسایگی :

1. در مرحله اول Down هستند .
2. بسته ای که در آن پارامترهای همسایگی نوشته شده با آدرس Multicast : 224.0.0.5 ارسال می شود . (مرحله Init)
3. بعد یک پیام تایید به مقصد IP یکدیگر می فرستند و همسایگی به وجود می آید به این مرحله 2- way می گویند .

روترها تا به مرحله 2 – way نرسند نمی توانند با هم تبادل اطلاعات بکنند و نمی توانند جدول روتر خود را تشکیل دهند.

همسایگی همیشه در بین روترهایی که با هم Connect هستند تشکیل می شود .

بعد از مرحله 2 – way مراحل زیر اتفاق می افتد :

4. Exstart :

در این مرحله می گوید من Master هستم (هرکس Router – ID بزرگتری داشته باشد شروع می کند به حرف زدن)

5. Exchang :

بسته های DBD را ارسال می کند . شرح مختصری از خود می فرستد و می گوید کدامشان را می خواهی ؟

روتر دیگر در جواب بسته LSR را می فرستد یعنی اینها را می خواهم .

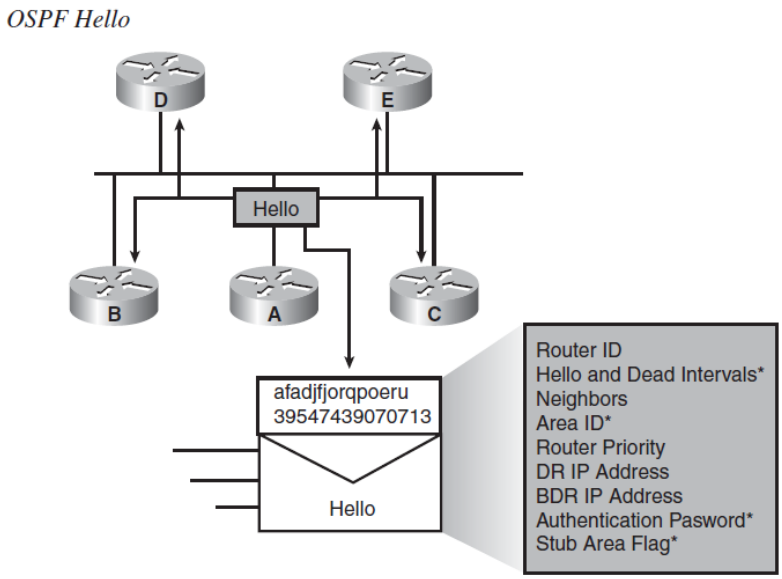
6. بسته های LSU که حاوی چند LSA است را می فرستد و در مقابل روتر که بسته را می گیرد LSAck را می فرستد یعنی بسته را گرفته ام .(مرحله Loading)
7. وارد مرحله Full می شوند یعنی جدول آنها تکمیل شده است .

DBD : Data Base Description

LSR : Link State Request

Router ID :

در فرایند OSPF یک شناسه برای هر روتر اختصاص داده می شود که یکدیگر را با این شناسه می شناسند . این شناسه (RID) یک عدد 32 بیتی است.



دستورات Router ID :

Router (config – Router) # Router – ID A.B.C.D

Interface Loopback ⟶ Highset IP – Address

Highset IP – Address of Another Interface

از این 3 حالت بالا یکی را اجرا می کنیم

نکته :

دو روتر که با هم همسایگی تشکیل می دهند یکی از روترها Master نام دارد و روتر دیگر Slave نام دارد .

نکته :

Loopback Interfaceها مجازی هستند و همیشه Up هستند . می توان بر روی روتر تعداد زیادی Loopback تعریف کرد . می توانیم Router – ID را روی این اینترفیس فعال کنیم چون تا وقتی که حذف نکرده ایم Up خواهد ماند .

نحوه تعریف این اینترفیس و آدرس دهی به آن :

Router (config) # Interface Loopback number

Router (config – if) # IP Address IP – address

Number : می تواند عددی بین 0 تا 65535 باشد . یعنی به این تعداد می توانید Loopback روی یک روتر تعریف کنیم .

نکته :

در جدول IP Route در جلوی IPهایی که از طریق پروتکل OSPF به جدول اضافه شده اند با حرف O بزرگ نمایش داده می شود .

Wild – card mask ⟵ Inverse Subnet Mask :

هدف آن است که مشخص می کند کدام بخش از بخش های IP مهم است و کدام مهم نیست یعنی هر بیتی که 0 باشد مهم است و هر بیتی که 1 باشد بی اهمیت است :

Subnet Mask Versus Wildcard Mask

Bit Value	Subnet Mask	Wildcard Mask
0	Host component	Must match
1	Network component	Ignore

مثال :

192.168.1.1

0.0.0.255

این Wild – card mask که در مثال بالا است یعنی قسمتی که 0 گذاشته شده (192.168.1) فقط مهم است قسمت آخر که 255 گذاشته شده مهم نیست می تواند از 1 تا 255 هر عددی باشد .

Wild – card mask به 5 حالت نوشته می شود :

Wildcard Mask Examples

IP Address	Wildcard Mask	Matches
0.0.0.0	255.255.255.255	Match on any address (keyword `any` in an ACL statement).
172.16.1.1	0.0.0.0	Match only if the address is 172.16.1.1 (preceded by the keyword `host`).
172.16.1.0	0.0.0.255	Match only on packets that are in 172.16.1.0/24 (172.16.1.0–172.16.1.255).
172.16.2.0	0.0.1.255	Match only on packets that are in 172.16.2.0/23 (172.16.2.0–172.16.3.255).
172.16.0.0	0.0.255.255	Match only on packets that are in 172.16.0.0/16 (172.16.0.0–172.16.255.255).

فرمان تعریف پروتکل OSPF :

Router (config) # Router OSPF number

Router (config – router)# Network IP – address wild – card mask Area number

دستور نمایش وضعیت OSPF :

Router # Show IP OSPF neighbor

Router # Show IP OSPF Database

Router # Show IP Route OSPF

Router # Show IP OSPF Interface

نکته :

با زدن دستور Clear IP OSPF Process جدول پاک می شود و بعد دوباره تشکیل می شود .

دستور بدست آوردن مقدار دقیق Bandwidth :

Router (config – Router) # Auto – Cast Refrence – Bandwidth number

DR : Designated Router

BDR : Backup Designated Router

در میان روترهایی که در یک Multi – access قرار گرفته اند روتری که بالاترین RID را داشته باشد به عنوان DR انتخاب می شود و روتر دومی که بالاترین RID را بعد از روتر DR داشته باشد به عنوان روتر BDR انتخاب می شوند . در صورتی که تغییری در شبکه رخ دهد روترها این تغییرات را در قالب LSU (Link – State Update) به روتر DR و BDR اطلاع می دهند. بنابراین هر دو روتر 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 یا خراب شدن روتر DR , روتر BDR به عنوان DR انتخاب می شود .

دستور دادن اولویت به یک اینترفیس :

Router (config - if) # IP OSPF Priority 0 – 255

پیش فرض 1 است .

نکته :

آدرس Multicast : 224.0.0.6 مخصوص DR و BDR است . یعنی روترهای دیگر با این IP بسته های خود را به DR و BDR ارسال می کنند و روتر DR با آدرس 224.0.0.5 اطلاعات را به همه روترها می فرستد .

معیار تعیین DR :

1. Highset Priority
2. Highset RID

نکته :

اگر Priority یک اینترفیس روتر را 0 بگذاریم هیچ وقت DR نمی شود در آن شبکه ای که به این اینترفیس وصل است ولی شاید اینترفیس دیگری از همان روتر به یک شبکه دیگری وصل باشد و در آنجا DR باشد.

نکته :

اگر همه روترها Priority مساوی داشته باشند از روی Router ID تعیین می کنند کدام روتر DR باشد .

بهتر است در یک شبکه اول IP گذاری کنیم بعد DR را تعیین کنیم.

نکته :

به روترهایی که نه DR و نه BDR هستند DROTHER گفته می شود . همه DROTHERها با DR و BDR به وضعیت Full میرسند ولی با هم به وضعیت 2 – way میرسند یعنی همسایگی دارند .

مراحل OSPF :

Down ⟶ Init ⟶ 2 – Way ⟶ Exstart ⟶ Exchang ⟶ Loading ⟶ Full

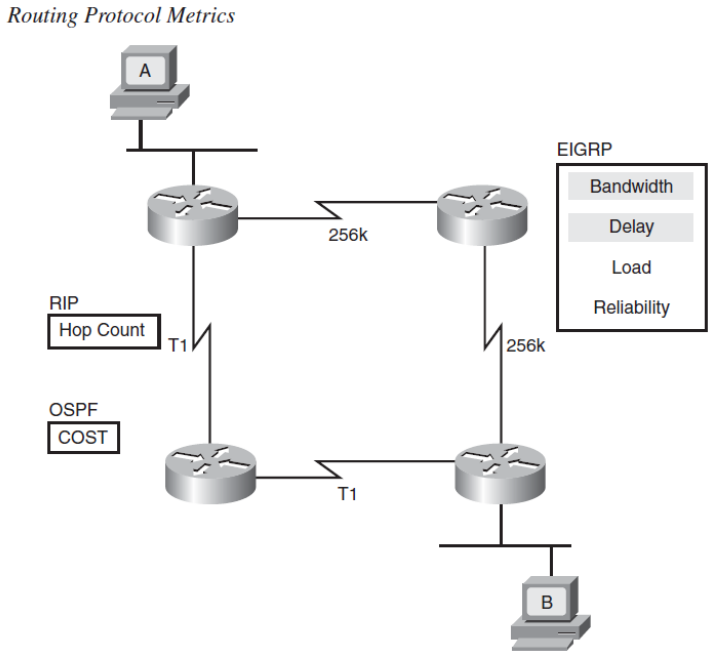
نکته :

وارد کردن دستور Router # wr برابر است با دستور زیر :

Router # Copy Running – config Startup – config

Wr ⟶ write Memory

EIGRP : Enhanced Interior Gateway Routing Protocol



: EIGRP

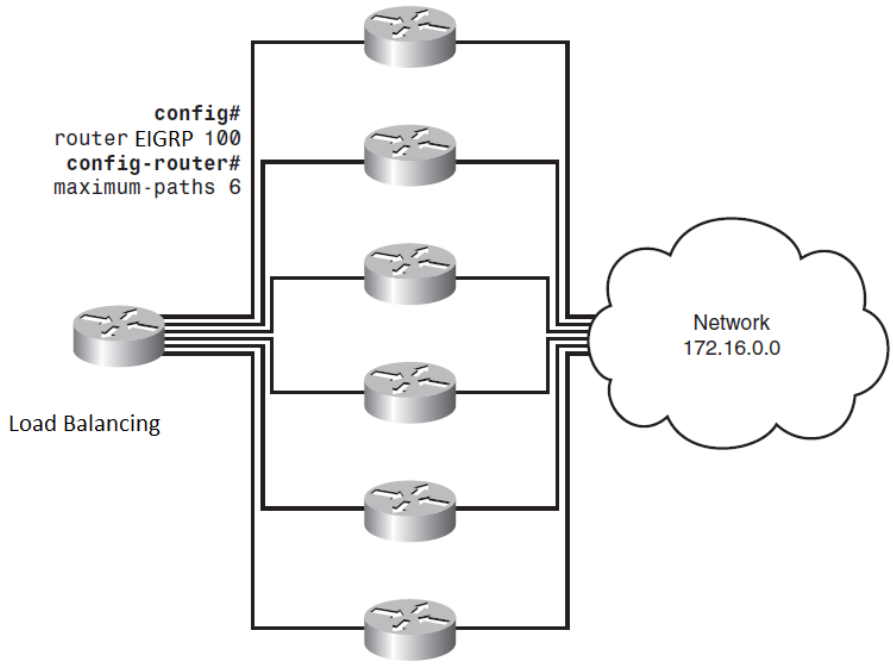
پروتکل EIGRP نسخه پیشرفته IGRP می باشد که توسط شرکت سیسکو طراحی و استاندارد شده است . شرکت سیسکو بهترین توانمندی پروتکل های Link – State و Distance – Vector را در این پروتکل قرار داده است .

EIGRP با به کار بردن الگوریتم (DUAL) Diffusing Update Algorithm سرعت همگرایی شبکه را افزایش می دهد . یک پروتکل Classless است و قادر به پشتیبانی از توانمندی VLSM است و از پیام های Multicast برای Update جدول مسیریابی استفاده می کند .

برای محاسبه متریک و انتخاب بهترین مسیر از پارامترهای Bandwidth و Delay و Load و MTU و Reliabilityاستفاده می کند ولی به صورت پیش فرض از Bandwidth و Delay استفاده میکند .

در پیکربندی EIGRP نیاز به تعریف یک شماره به نام AS یا Autonomous System می باشد که این شماره باید در بین کل روترهای یک شبکه یکسان باشد . روتر ها توانایی ارسال جدول های مسیریابی و Update آنها را فقط به روترهایی دارد که دارای AS مشترک باشند . AS به صورت اختیاری تعیین می شود و عددی بین 1 تا 65535 می باشد.

این پروتکل امکان Load balancing برای 6 مسیر با ارزش مساوی Equal Cost Path و 6 مسیر با ارزش نامساوی Unequal Cost Path را دارا می باشد .



مراحل EIGRP :

Neighbor Ship ⟶ Topology Exchang ⟶ Routing table

پارامترهای تشکیل همسایگی در پروتکل EIGRP :

1. AS Number
2. K Values
3. Authentication
4. Subnet Number

انواع K Values :

1. Min Bandwidth ⟶ K_1 پیش فرض
2. Load ⟶ K_2
3. Delay ⟶ K_3 پیش فرض
4. Reliability ⟶ K_4 , K_5

روترها با آدرس Multicast : 224.0.0.10 به یکدیگر بسته های Hello می فرستند و با فرستادن Ack همسایگی را تایید می کنند .

محاسبه متریک در EIGRP :

Metric : [10000000 / Bandwidth + Σ Delay] × 256

Bandwidth ⟶ Kbps

Delay ⟶ 10 Ms

ویژگی های EIGRP :

1. Very Fast Convergency
2. Hop Count ⟶ 100
3. Classless
4. Metric ⟶ Compsite
5. Multicast ⟶ 224.0.0.10
6. VLSM
7. Incremental Update

نکته :

EIGRP وقتی مسیرها را بررسی می کند و بهترین مسیر را که انتخاب می کند در جدول خود مسیرهای دیگر را نیز نگه می دارد و دور نمی ریزد یعنی پاک نمی کند . زمانی که مسیر اصلی به هر دلیلی قطع شود فورا مسیر بعدی را جایگزین میکند که از مسیر اصلی مستقل باشد .

مسیرها و متریک های موجود در Routing Table :

Reported Distance (RD) : متریکی است که توسط روتر مجاور تا مقصد محاسبه شده و گزارش داده می شود .

Feasible Distance (FD) : در میان متریک های مختلفی که از خود روتر تا مقصد وجود دارد , متریکی که کمترین مقدار را داشته باشد به عنوان FD انتخاب می شود .

Successor : مسیری که متریک FD را داشته باشد به عنوان مسیر Seccessor انتخاب می شود . در واقع مسیری که دارای کمترین متریک باشد.

Feasible Condition (FC) : در صورتی که در مسیری FD < RD باشد در این حالت شرایط برای انتخاب شدن مسیر به عنوان مسیر Back up فراهم می شود . در واقع برای پیدا کردن FS می بایست این شرایط برقرار باشد 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 (FS) : مسیر Back up برای مسیر Successor می باشد و مسیری است که در شرایط FC صدق می کند .

Advertised Distance (AD) : متریکی که همسایه به روتر می دهد که به روتر دیگر بدهد.

نکته:

Hello Time → 5 Sec

Hold Time → 15 Sec

دستورات EIGRP :

Router (config) # Router EIGRP AS – Number

Router (config – Router) # Network Ip – Address [Wild – Card – mask]

Router (config – Router) # No Auto – Summary

دستور نمایش وضعیت EIGRP :

Router # Show IP EIGRP Neighbor

Router # Show IP EIGRP Topology

Router # Show IP Route EIGRP

دستور حداکثر پورت هایی که در Load balancing استفاده کنیم :

Router (config – Router) # Maximum – Paths 4 – 32

Router (config – Router) # Variance 1 – 128

دستور خاموش کردن بالانسینگ اینترفیس :

Router (config – Router) # Traffic – Shere min aeross Interface

دستور روشن کردن دوباره بالانسینگ :

Router (config – Router) # Traffic – Shere Balanced

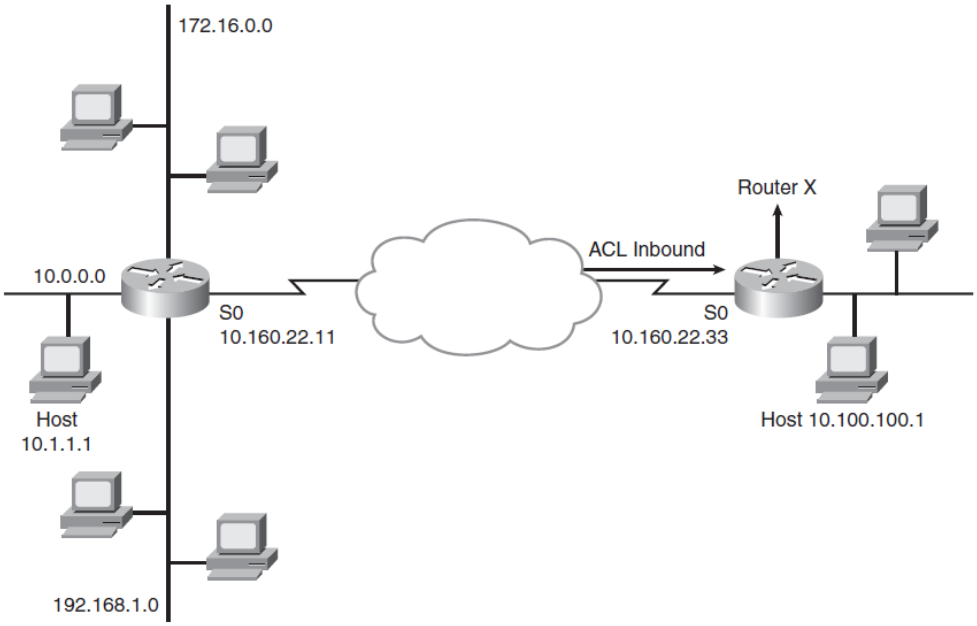
جدول مقایسه پروتکل ها :

Prorotol	Convergance Speed	Cpu & Memory Usage	Metric
RIP	Slow	Low	Bad
OSPF	Fast	High	Good
EIGRP	Very Fast	Medium	Very Good

جدول Routing Protocols در مقابل Routed Protocols :

Routed Protocols	Routing Protocols
IP	RIP . IGRP . OSPF . EIGRP . BGP . IS – IS
IPX	RIP . NLSP . EIGRP
Apple Talk	RMTP . AURP . EIGRP

Access Control List



Access List یا همان ACL روشی برای Filter کردن ترافیک خروجی و ورودی بر روی اینترفیس های روتر می باشد . شما می توانید به وسیله ACL تعیین کنید که چه ترافیکی با چه مشخصاتی از اینترفیس روتر اجازه ورود یا خروج را داشته باشد . شما باید برای استفاده از ACL ابتدا آن را تعریف کنید و بعد ACLها را به اینترفیسی که قصد کنترل ترافیک آن را خواهید داشت نسبت دهید . هر ACL باید با یک شماره یا یک نام منحصر به فرد شناسایی شود.

دستورات ACL از بالا به پایین مورد بررسی قرار می گیرند . پس ترتیب نوشتن دستورات اهمیت خاصی دارد و در پایان هر ACL یک Deny All وجود دارد که شما مشاهده نمی کنید ولی توسط خود IOS اضافه خواهد شد . پس در صورتی که ترافیک شما با هیچ کدام از قوانین داخل ACL مطابقت نداشته باشد آن ترافیک Deny خواهد شد یعنی اجازه عبور از آن اینترفیس را نخواهد داشت .

ترافیک با داخل دستورات ACL خط به خط بررسی می شود و در صورتی که اطلاعات با یکی از خطوط ACL مطابقت داشته باشد آن قانون اعمال میشود و خطوط بعد از آن قانون دیگر بررسی نمی شوند و در صورتی که هیچ کدام از قوانین با ترافیک مطابقت نداشته باشد در نهایت ترافیک به خاطر وجود Deny All در پایان ACL فیلتر خواهد شد و اجازه عبور نخواهد داشت . در تعریف ACLها به جای استفاده از Subnet Mask از Wild card mask استفاده میشود که بیان کننده تعداد بیت ها از آدرس می باشد که باید در ACL مورد بررسی قرار گیرد .

پارمترهایی که ACL می تواند بر اساس آنها اقدام به فیلتر کردن ترافیک ها نماید :

1. بر اساس آدرس فرستنده (Source IP Address)
2. بر اساس آدرس مقصد یا گیرنده (Destination IP Address)
3. بر اساس شماره پورت خاص
4. بر اساس پروتکل های UDP و TCP
5. بر اساس یک سری از پروتکل های شبکه مانند : ICMP و OSPF و EIGRP ...

ACL ها دو نوع هستند :

- **Standard Access List**
- **Extended Access List**

Standard Access List

توسط این ACLها می توان اقدام به کنترل ترافیک ورودی و خروجی بر اساس آدرس فرستنده (Source IP Address) نمایید . این ACL از طریق شماره شناسایی می شود شماره های 1 – 99 و 1300 – 1999 مربوط به ACLهای استاندارد هستند .

دستور ساخت ACL :

Router (config) # Access – List number { Permit | Deny } IP – Address

[wild card mask]

Permit : به معنای صدور مجوز عبور

Deny : مانع عبور ترافیک خواهد شد

دستور اعمال کردن ACL ها بر روی اینترفیس ها :

Router (config) # Interface type mod/num

Router (config – if) # IP Access – group number { in | out }

In : ACL ترافیک را قبل از اینکه وارد اینترفیس روتر شود فیلتر می کند .

Out : ACL ترافیک را بعد از اینکه داخل روتر شد و در هنگام خروج از اینترفیس فیلتر می کند.

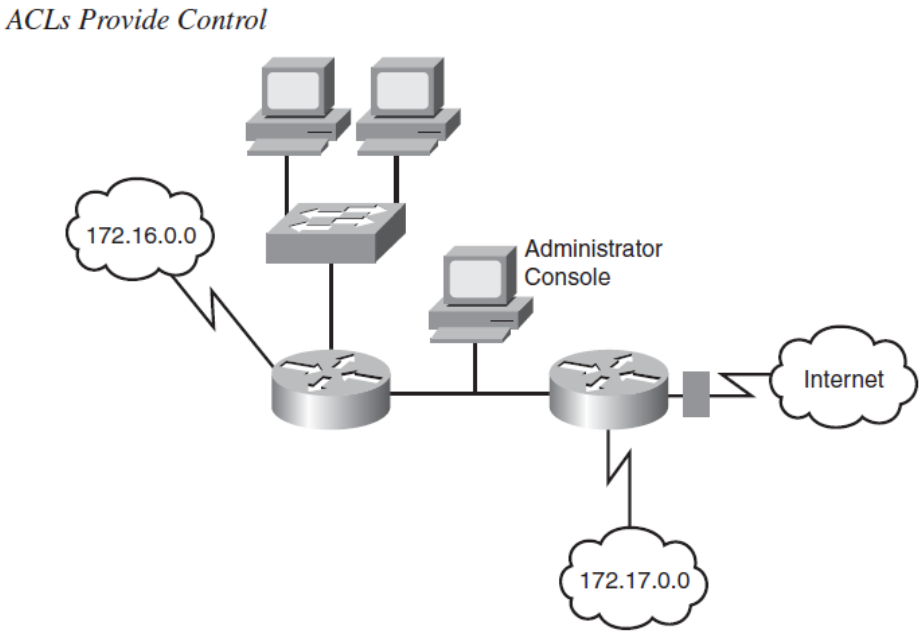
دستور نمایش همه Denyها در دستور Show :

Router (config – Route) # Access – List number Deny Any

دستور نمایش Access List :

Router # Show Access List

Extended Access List



این ACLها قادر به کنترل ترافیک ورودی و خروجی بر اساس پروتکل های لایه 3 مانند IP و همچنین پروتکل های TCP , UDP و همچنین بر اساس پورت ها و سایر پروتکل های شبکه مانند ICMP , OSPF , EIGRP ... می باشد . این ACLها نیز از طریق شماره شناسایی می شوند. از شماره های 100 – 199 و 2000 – 2699 می توانیم استفاده کنیم .

دستور تعریف ACL :

Router(config)#Access – List number { Permit | Deny | remark } Protocol source-IP wild-card-mask source–port destination–IP wild-card-mask destination-port

Router (config) # Interface type mod/num

Router (config – if) # IP Access – group number { in | out }

دستور ACL با نام :

Router (config) # Access – List { Srandard | Extended } name

Router (config – {std | ext } - nacl) # Std Access – List { Permit | Deny | remark } source-IP wild-card-mask

Router (config – {std | ext } – nacl) # Ext Access – List { Permit | Deny | remark } Protocol source-IP wild-card-mask [source–port] destination–IP wild-card-mask [operator destination-port]

جدول تفاوت ACL ها با هم :

Standard and Extended ACL Comparison

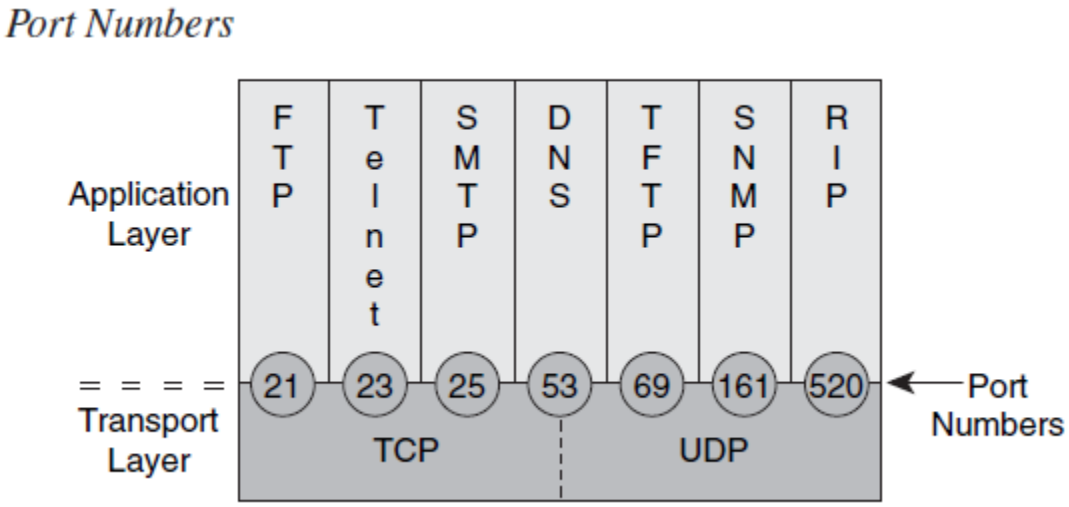
Filtered Information	Standard IP ACL	Extended IP ACL
Source address	Yes	Yes
Destination address	No	Yes
IP protocol (i.e., TCP or UDP)	No	Yes
Protocol information (i.e., port number)	No	Yes

جدول شمارههای ACL :

ACL Types and Numbers

ACL Type	ACL Numbers
IP Standard	1–99, 1300–1999
IP Extended	100–199, 2000–2699

جدول شماره پورت UDP و TCP :



مثال ACL برای Telnet و SSH :

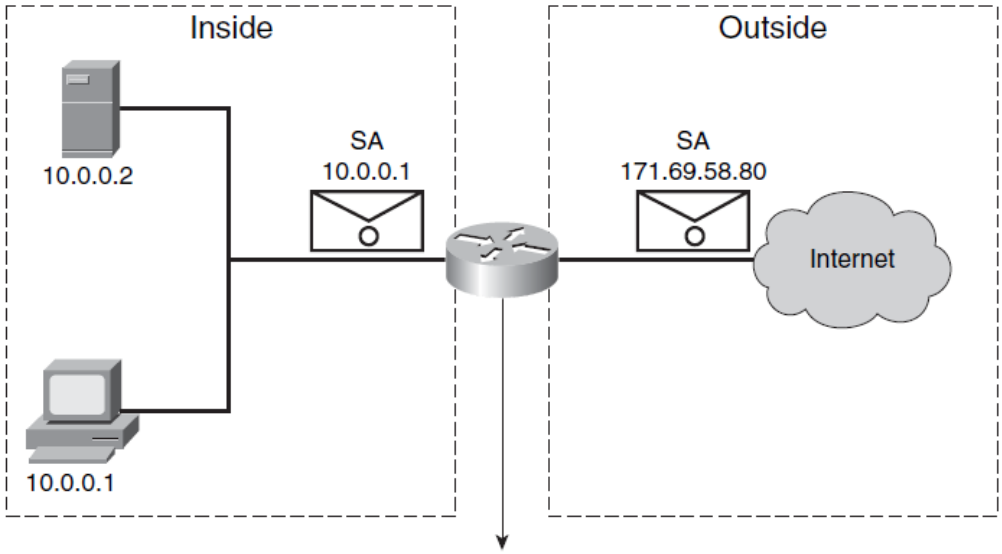
اول ACL را می نویسیم بعد دستور زیر را وارد می کنیم :

Router (config) # line vty 0 15

Routr (config – line) # Access – class number in

هر کس بخواهد با Telnet یا SSH وصل شود در Line vty پردازش می شود و شبکه کند نمی شود .

Network Address Translation



NAT Table

Inside Local IPv4 Address	Inside Global IPv4 Address
10.0.0.1	171.69.58.80
10.0.0.2	171.69.58.81

NAT :

برگرفته از عبارت Network Address Translation یا ترجمه آدرسهای IP Addressها میباشد. توانمندی NAT علاوه بر اینکه مشکل کمبود IP Addressها را برطرف کرده به شما اجازه می دهد که با استفاده از Private IP Addressها که همان IP Addressهای ثبت نشده و خصوصی میباشند به شبکه اینترنت متصل شوید. بدون استفاده از توانمندی NAT هر کامپیوتر یا Device که نیاز به دسترسی به اینترنت را داشته باشد باید از آدرس های ثبت شده یا همان Public IP Addressها استفاده کند که برای استفاده از این آدرس ها باید با هزینه زیادی خریداری نمود و این کار باعث کاهش امنیت شبکه سازمان شما می شود و مشکل دیگر آن است که با کمبود آدرس های Public مواجه هستیم . توانمندی NAT به ما اجازه خواهد داد تعداد زیادی آدرس Private IP Address ثبت نشده را از طریق یک یا تعداد کمی آدرس Public ترجمه شوند و به اینترنت وصل شوند .

برای استفاده از توانمندی NAT شما باید از رنج آدرس های Private که در جدول پایین مشاهده می کنید برای Hostهای داخلی شبکه استفاده کنید :

RFC 1918 Private Addresses

Class	Range of Addresses
A	10.0.0.0–10.255.255.255
B	172.16.0.0–172.31.255.255
C	192.168.0.0–192.168.255.255

مزایای استفاده از NAT :

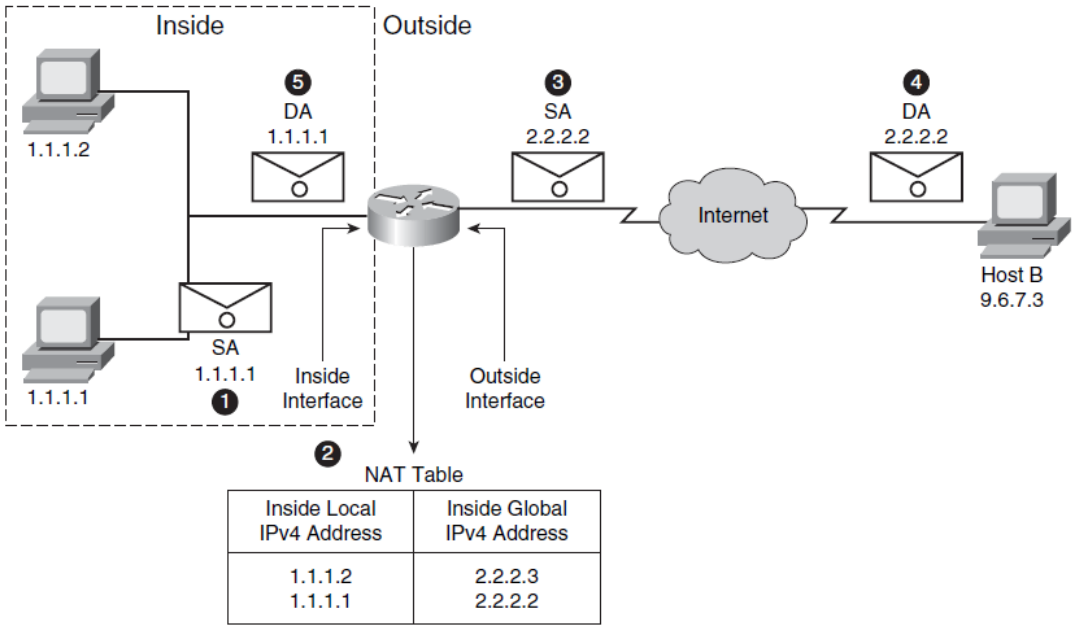
- حل مشکل کمبود آدرس های Public IP Address
- افزایش امنیت
- دسترسی به اینترنت با استفاده از یک IP Address ثبت شده اینترنتی Public
- کاهش هزینه دسترسی به اینترنت
- مدیریت ساده و متمرکز بر روی دسترسی به اینترنت

معایب استفاده از NAT :

- ایجاد یک Delay یا وقفه برای عمل ترجمه .
- به علت مخفی شدن شبکه داخلی امکان Trace و تست کردن ارتباطات End-to-Endوجود ندارد .
- برخی از برنامه ها و سرویس ها با NAT پشتیبانی نمی شود .

برای پیکربندی NAT نیاز به دستگاهی دارید که توانمندی NAT روی آن فعال شود و توانایی ترجمه آدرس های خصوصی Private را به آدرس های Public داشته باشد که این دستگاه می تواند یک Server یا Router یا Switch لایه 3 یا حتی یک Firewall باشد که در هر کدام از این تجهیزات برای پیکربندی NAT نیاز به حداقل دو اینترفیس خواهیم داشت که یکی از اینترفیس ها به شبکه داخلی متصل می شود و به

اینترفیس Inside و اینترفیس بعدی که به شبکه خارجی (اینترنت) متصل است به نام اینترفیس Outside معروف می باشد.



: NAT Static

در این روش تبدیل آدرس Private IP Address به آدرس Public IP Address به صورت دستی می باشد . در این نوع NAT تعداد آدرس های Private با تعداد آدرس های Public باید با هم مساوی باشند .

تعریف NAT بر روی روتر :

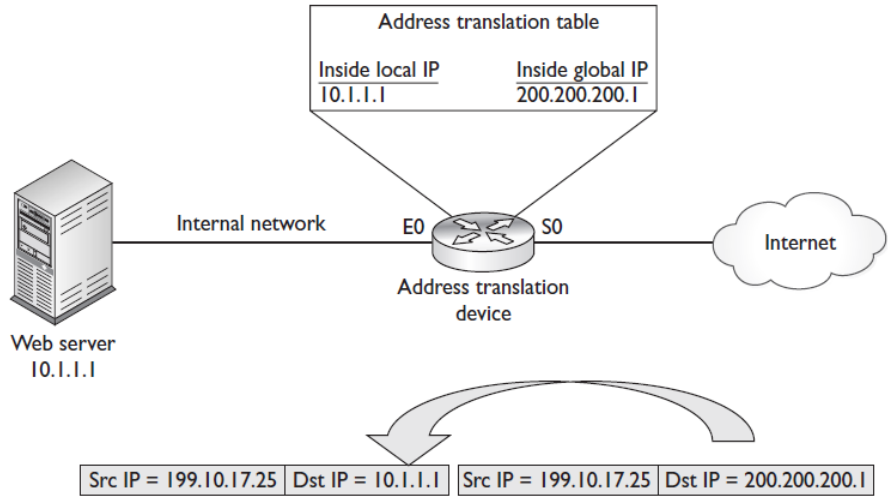
Router (config) # IP NAT Source Static IP-Private IP-Public

دستور وارد کردن NAT به اینترفیس :

Router (config – if) # IP nat { inside | outside }

دستور نمایش وضعیت NAT :

Router # Show IP NAT Translastion



NAT Dynamic :

در این روش شما آدرس های Public را در داخل یک گروه Pool (مخزن) قرار می دهید و از این مجموعه آدرس ها می توانید به صورت Dynamic برای ترجمه گروهی از آدرس های Private استفاده کنید . در این روش آدرس های Public در یک گروه Pool می باشد و آدرس های Private شبکه که باید ترجمه شوند با یک Access list مشخص می شوند .

در این روش برای هر کامپیوتر داخلی شبکه که نیاز به دسترسی به اینترنت دارد در آن مقطع زمانی باید یک آدرس Public در داخل آن گروه Pool وجود داشته باشد که پروسه NAT انجام شود . در صورتی که در آن مقطع زمانی آدرس Public آزاد در Address Pool وجود نداشته باشد آن کامپیوتر قادر به دسترسی به اینترنت نیست .

تعریف NAT روی روتر :

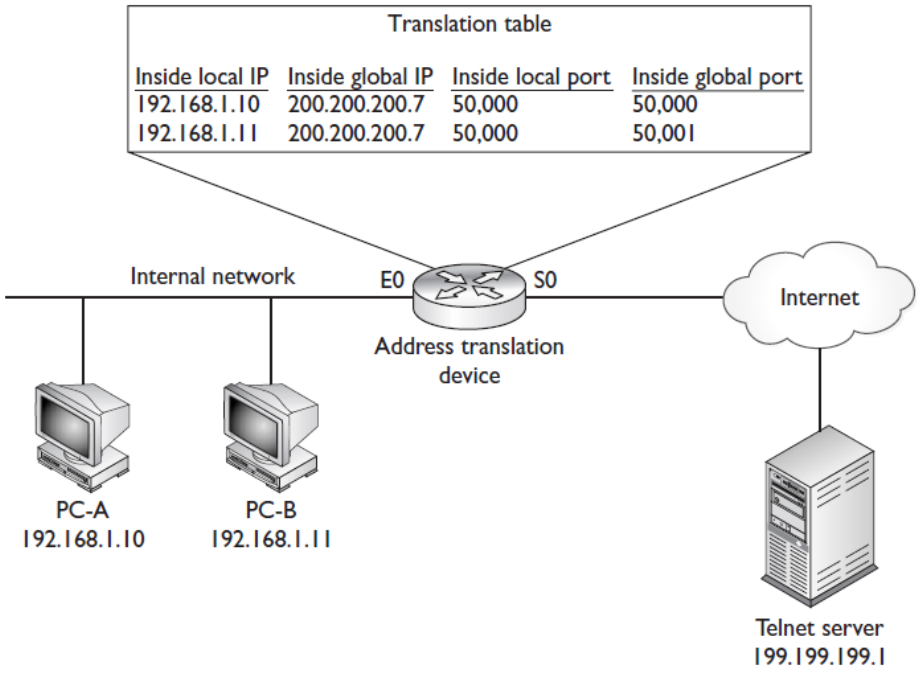
Router (config) # IP NAT Pool pool-name start-IP end-IP netmask subnet-ask

Router (config) # Access – List number { Permit | Deny } IP – Address [wild card mask]

Router (config) # IP NAT inside source List list-number Pool pool-name

: PAT

در این روش همه آدرس های Private IP Address از طریق یک Public IP Address تبدیل می شوند و این از نظر اقتصادی بسیار مناسب تر است . در این روش NAT Router برای ترجمه هر آدرس Private IP Address از یک شماره پورت خاص و متفاوت استفاده می کند و به دلیل اینکه برای همه آدرس های Pirvate از یک IP Public استفاده خواهد شد و از شماره پورت های متفاوت استفاده می شود . امنیت بالاتری نسبت به سایر روش های NAT دارد این روش به Overload هم معروف است .



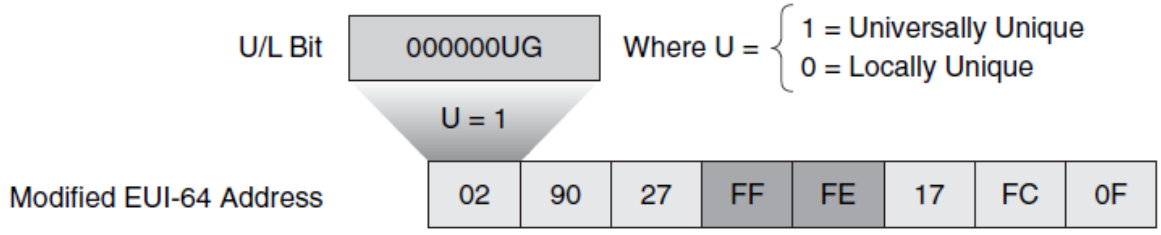
پیکربندی PAT بر روی روتر :

Router (config) # IP NAT Pool pool-name start-IP end-IP netmask subnet-ask

Router (config) # Access – List number { Permit | Deny } IP – Address [wild card mask]

Router (config) # IP NAT inside source List list-number Pool pool-name Overload

IPv6



مزایا :

1. Very Large Address Space → 128 bit
2. Security
3. Mobility
4. Stream Lined Encapsulation
5. Transition Cupabilities

قوانین ساده سازی :

1. حروف بزرگ و کوچک فرقی ندارد
2. اگر به چهار صفر برخوردیم می توانیم 2 تا علامت کالون (::) بگذاریم البته فقط یک بار می توانیم این کار را بکنیم
3. در یک Field اگر بیت سمت چپ صفر باشد می توانیم آن را حذف کنیم

0111 → 111

IP Loopback :

127.x.x.x ⟶ 0:0:0:0:0:0:0:1 ⟶ ::1

تفاوت در نوع نوشتن و مقدار IP ها :

Version	IPv4	IPv6
Notation of address	192.168.201.113	A524:72D3:2C80:DD02:0029:EC7A :002B:EA73
Total number of addresses available	4,294,467,295 IP addresses	3.4 x 10^{38} IP addresses

انواع IP v6 :

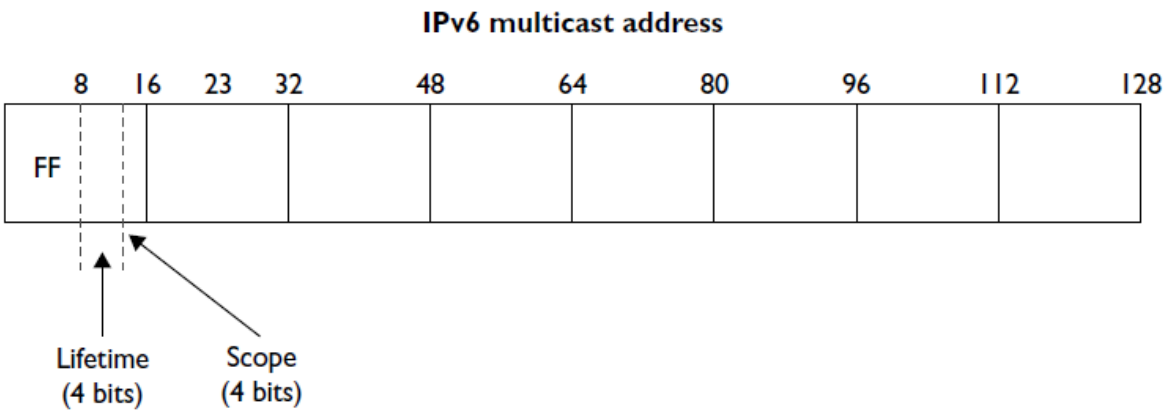
1. **Anycast** : چند دستگاه یک IP دارند ولی وقتی اطلاعات بفرستیم به نزدیکترین دستگاه می رسد و اگر ارتباط آن قطع شود به دومی می فرستد بهتر است در مقصد از این IP استفاده کنیم .
2. **Multicast** : به آدرس هایی که 8 بیت اول آنها با FF شروع می شود .

Multicast دو نوع دارد :

Temporary : موقتی هستند و با FF1 شروع می شود

Permanent : دائمی هستند و با FF0 شروع می شود

4 بیت بعدی نشان دهنده (Lifetime) ناحیه انتشار Multicast است :



اگر Lifetime مقدار های زیر باشد در این نواحی انتشار می یابد :

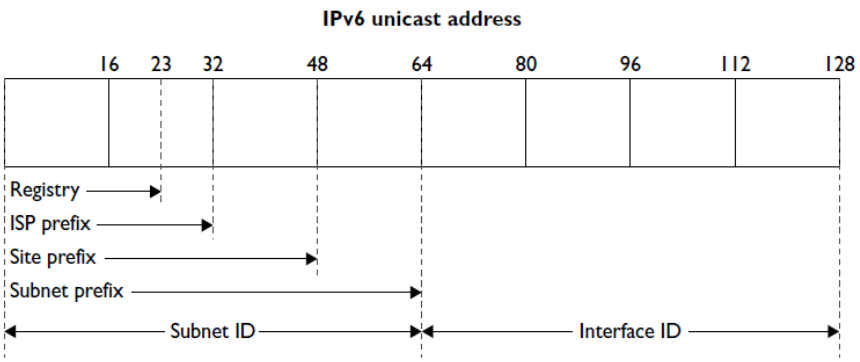
Node = 1 , Link = 2 , Site = 5 , Organization = 8 , Global = E

3. **Unicast** : به دو دسته زیر تقسیم می شود :

F E C :: ⟶ F E F : Site – Local
F E 8 :: ⟶ F E B : Link – local
} : Private

Link – Local : آدرسی است که دستگاه ها خودشان برای ارتباط این آدرس را می سازند .

Public : بغییر از IPهای گفته شده بقیه IP های دیگر Public هستند .



قسمت Subnet ID :

Registry ⟶ 2000:: /23 ⟶ 23 bit

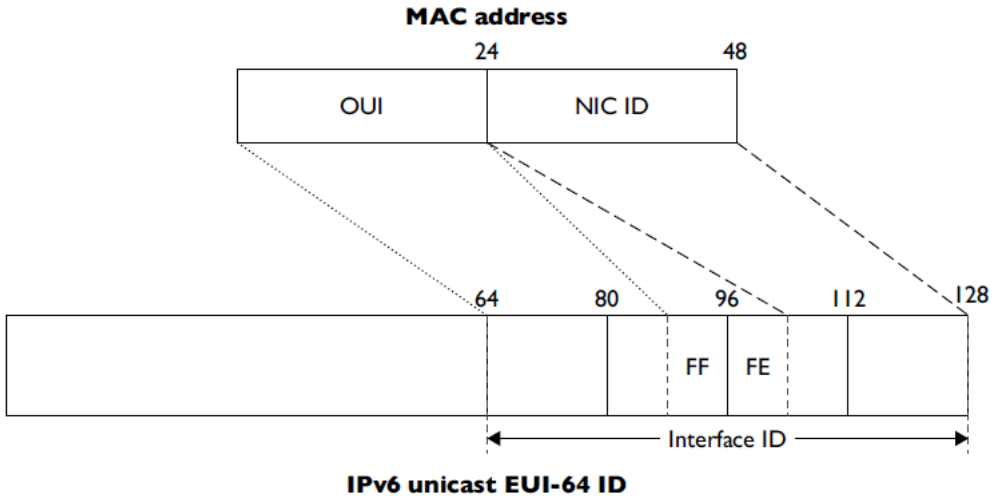
ISP ⟶ 2000:5:: /32 ⟶ 32 bit

Site ⟶ 2000:5:1:: /48 ⟶ 48 bit

Subnet ⟶ 2000:5:1:1:: /64 ⟶ 64 bit

قسمت Interface ID :

از آنجایی که بخش Host , 64 بیت است و می خواهیم Unic باشد از روی MAC – Address که Unic است تعیین میشود .



IPv6 unicast EUI-64 ID

EUI-64 ID : Extended Unic Indentifier

یک مکانیزم است که بخش Host را به صورت Unic می سازد

MAC Addres s ⟶ 48 bit ⟶ 24 bit OUI + 24 bit VAA

تبدیل میشود به :

EUI ⟶ 24 bit OUI + 16 bit FFFE + 24 bit VAA

این مکانیزم بیت هفتم را به 1 تبدیل می کند مانند مثال پایین :

مثال 1 :

ABCD : 12FF : FE34 : 3567

بیت هفتم که در قسمت اول در B قرار دارد و به صورت زیر است :

1011 == B چون بیت هفتم یک است یک می ماند

مثال 2 :

A025 : 23FF : FE45 : 6789

بیت هفتم که در قسمت اول 0 قرار دارد و به صورت زیر است :

0000 == 0 چون بیت هفتم 0 است به 1 تغییر می یابد و این می شود :

0010 == 2 است IP بالا به صورت IP پایین در می آید :

A225 : 23FF : FE45 : 6789

تخصیص IP :

1. Menval
2. Automatic مانند Link – Local
3. Dynamic

- **Stateful**
- **Stateless**

در مدل Stateless دستگاه هایی مانند روتر و غیره قسمت Net شبکه را به PC ها می فرستند. PC به روتر یک پیام Router Solicitation می فرستد و روتر یک IP منحصر به فرد (Unic) به PC می فرستد .

دستور :

Router(config – if)#IPv6 Address IPv6–address / Profix leghth [eui–64]

Router # Show IP v6 Interface type mod/num

مثال :

```
Router(config)# ipv6 unicast-routing
Router(config)# interface fastethernet0/0
Router(config-if)# ipv6 address 2001:1cc1:dddd:2::/64 eui-64
Router(config-if)# end
```

RIP در IP v6 :

- Distance Vector
- 15 Hop count
- RIP v2
- FF02 : : 9
- UDP 521

دستورات RIP با IP v6 :

IP v6 را فعال می کنیم : Router (config) # IP v6 Unicast-routing

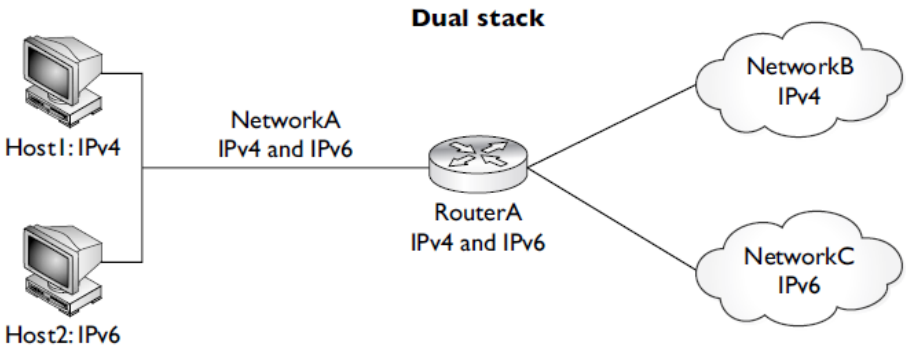
IP را تعریف می کنیم : Router (config) # IP v6 Router RIP name

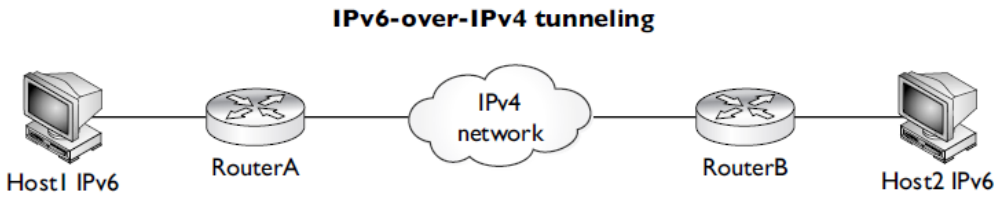
روی اینترفیس اعمال می کنیم : Router (config - if) # IP v6 RIP name Enable

دستور نمایش وضعیت IP v6 :

Router # Show IP v6 Route

Router # Show IP v6 RIP





IEEE Ethernet Components

Address	Value	Description
Global	2000::/3	These are assigned by the IANA and used on public networks. They are equivalent to IPv4 global (sometimes called public) addresses. ISPs summarize these to provide scalability in the Internet.
Reserved	(range)	Reserved addresses are used for specific types of anycast as well as for future use. Currently about 1/256th of the IPv6 address space is reserved.
Private	FE80::/10	Like IPv4, IPv6 supports private addressing, which is used by devices that don't need to access a public network. The first two digits are FE, and the third digit can range from 8 to F.
Loopback	::1	Like the 127.0.0.1 address in IPv4, 0:0:0:0:0:0:0:1, or ::1, is used for local testing functions; unlike IPv4, which dedicates a complete A class block of addresses for local testing, only one is used in IPv6.
Unspecified	::	0.0.0.0 in IPv4 means "unknown" address. In IPv6, this is represented by 0:0:0:0:0:0:0:0, or ::, and is typically used in the source address field of the packet when an interface doesn't have an address and is trying to acquire one dynamically.

Network Engineer
IRAN : +989127687757
ERBIL : +964 750 530 8221
Kolijis@Yahoo.com
Showan.Koliji

Showan koliji