آموزش

CCNA ++

نویسنده:

فرشید باباجانی

CCNA++

به جویبارها سوگند دریاد من می‌مانی، به برگ‌های نارنجی پاییزی، به سبد میوه‌های کال و نارس در دل پشت بام های دلتنگی، به طعم بی هوایی زرد آلو در جاده های سکوت و غمناکی، به پرنده، به پرواز، به شیرینی لبخند رؤیایی، به آسمان، به حیرانه های تنهایی، به تبسم، به خیال، به زیبایی، به عشق، به برگ‌های نارنجی پاییزی. . . دریاد من می-مانی. . . (آزاده تیشه بر سر)

مقدمه:

این کتاب دربرگبرنده دوره‌ی CCNA شرکت سیسکو است و سرفصل‌های آن دقیقاً برابر این دوره است و حتی از این سرفصل‌ها فراتر رفته و به دوره‌ی CCNP رسیده که امیدوارم برای شما عزیزان مفید واقع شود.

دوستان توجه داشته باشید که تلاش و پشتکار شما باعث پیشرفت جدی در کار شما خواهد شد، پس در خواندن این کتاب تمام سعی و تلاش خود را انجام دهید و کتاب را از به نام خدا تا پایان به دقت بخوانید و مطمئن باشید در پایان کار، کاملاً بر موضوعات دوره‌ی CCNA و کمی از دوره‌ی CCNP مسلط خواهید شد.

این کتاب را تقدیم می‌کنم به خانواده‌ی عزیز و همسر فداکارم که در نوشتن این کتاب این‌جانب را همراهی کردند.

در پایان برای شما عزیزان آرزوی موفقیت می‌کنم، پاینده باشید.

فرشید باباجانی / زمستان 1392

ویراستار: آزاده تیشه بر سر

ویرایش شده در پائیز 1393

تاریخچه:

(لن بزاک و سندی لرنر) دارای مدرک لیسانس از دانشگاه ایالتی کالیفرنیا، فوق‌لیسانس اقتصادسنجی از دانشگاه کلرمونت و فوق‌لیسانس علوم کامپیوتر از دانشگاه استنفورد)، زوجی که در بخش کامپیوتر دانشگاه استنفورد کار می‌کردند، شرکت Cisco را در سال ۱۹۸٤ تأسیس کردند. بزاک نرم‌افزار روترهای چند پروتکل را که توسط ویلیام یاگر(یک کارمند دیگر که کار خود را سال‌ها قبل از بزاک شروع کرده بود) نوشته‌شده بود، تکمیل کرد.

باوجوداینکه Cisco اولین شرکتی نبود که Router طراحی و تولید می‌کرد، اولین شرکتی بود که یک Router چند پروتکل موفق تولید می‌کرد که اجازه‌ی ارتباط بین پروتکل‌های مختلف شبکه را می‌دهد. از زمانی که پروتکل اینترنت (IP) به یک استاندارد تبدیل شد، اهمیت Router های چند پروتکل کاهش یافت. امروزه بزرگ‌ترین روترهای Cisco طراحی‌شده‌اند تا بسته‌های IP و فریم‌های MPLS را هدایت کنند. در سال۱۹۹۰، شرکت سیسکو به سهامی عام تبدیل شد و سهام آن در بازار بورس عرضه شد. بزاک و لرنر با ۱۷۰ میلیون دلار از شرکت خارج شدند و بعد از مدتی جدا شدند. زمان انفجار اینترنت در ۱۹۹۹، Cisco شرکت Cerent واقع در کالیفرنیا را با قیمت ۷ میلیارد دلار خریداری کرد. این شرکت گران‌ترین خرید Cisco در آن زمان بود. تنها خرید گران‌تر، مربوط به ساینتیفیک آتلانتا است.

در اواخر مارس ۲۰۰۰، در اوج رشد دات کام، Cisco با ارزش مالی بالغ بر ۵۰۰ میلیارد دلار ارزشمندترین شرکت دنیا بود. در سال ۲۰۰۷ نیز با ارزشی بالغ بر ١٦٥ میلیارد دلار همچنان یکی از ارزشمندترین شرکت‌ها بود.

با خرید شرکت‌های دیگر، توسعه داخلی و همکاری با دیگر شرکت‌ها، Cisco به بازار بسیاری از قطعات دیگر شبکه (غیر از Router) راه پیدا کرده است، مانند Ethernet Switching، دسترسی از راه دور، Routerهای شعبه‌ای، شبکه‌ی خودپردازهای بانک‌ها، امنیت، fire wall، تلفن اینترنتی و غیره. در ۲۰۰۳، Cisco شرکت محبوب LinkSys تولیدکننده‌ی سخت‌افزار شبکه‌ی کامپیوتر را خریداری کرد و آن را در صدر تولید کننده‌های قطعات مربوط به کاربران عادی گذاشت.

ریشه‌ی نام سیسکو:

اسم «سیسکو» مخفف سانفرانسیسکو است. با توجه به اظهارات جان مرگریج، کارمند ۳٤ ساله و مدیر پیشین شرکت، مؤسسان شرکت زمانی که داشتند به سمت ساکرامنتو رانندگی می‌کردند تا شرکت را به ثبت برسانند، با تصویر پل گلدن گیت در نور آفتاب مواجه می‌شوند و اسم و نماد شرکت را بر این اساس انتخاب می‌کنند. نماد شرکت منعکس‌کننده‌ی اصلیت سان‌فرانسیسکویی آن است که نشان‌دهنده‌ی پل گلدن گیت است که به سبک خاصی طراحی شده است. در اکتبر ۲۰۰٦، سیسکو نماد جدید خود را که از نماد قبلی ساده‌تر و ساخت‌یافته‌تر بود، به نمایش گذاشت.

مدارک سیسکو:

سیسکو در 156 کشور دنیا، به‌منظور تعلیم افراد برای طراحی نگهداری شبکه‌های کامپیوتری، مرکزهای آموزشی تأسیس کرده است. سیسکو مدارکی را برای متخصصین در زمینه‌های مختلف شبکه ارائه می‌کند که شامل این مدارک می‌شود:

دسته‌ی اول (دستیار یا کارشناس شبکه)

Associate یا دستیار، یعنی قرار گرفتن در ابتدای مسیر.گرایش شما هرچه که باشد می‌بایست پیش از اخذ هر مدرک و یا گذراندن هر دوره‌ای، CCNA با گرایش Routing&Switching را بگذرانید! بعدازآن چنانچه خواستارتغییرگرایش از Routing&Switching به سایرگرایش‌ها باشید، می‌بایست مدرکAssociate آن گرایش را نیز اخذ کنید، مثلاً چنانچه بهSecurity علاقه‌مند هستید، باید مدرک CCNA با گرایش Security را کسب کرده و سپس به سطح بالاتر یعنی Professional صعود نمود.

Associate Certifications

- CCNA Routing and Switching
- CCDA
- CCNA Data Center
- CCNA Security

- CCNA Service Provider
- CCNA Service Provider Operations
- CCNA Video
- CCNA Voice
- CCNA Wireless

دسته‌ی دوم (کارشناس ارشد شبکه)

Professional Certifications

- CCDP
- CCNP
- CCNP Data Center
- CCNP Security
- CCNP Service Provider
- CCNP Service Provider Operations
- CCNP Voice
- CCNP Wireless

دسته‌ی سوم (متخصص شبکه یا همان دکترای شبکه)

Expert Certifications

- CCDE
- CCIE Collaboration
- CCIE Data Center
- CCIE Routing & Switching
- CCIE Security
- CCIE Service Provider
- CCIE Service Provider Operations
- CCIE Voice (Retiring February 13, 2014)
- CCIE Wireless

دسته‌ی چهارم (معمار شبکه و همه‌کاره شبکه)

سطح Architect که در سال‌ها اخیر توسط سیسکو ارائه‌شده است، بالاترین سطح مدرک مهندسی شبکه در بین کلیه‌ی مدارک بین‌المللی شبکه است. ظاهراً شرکت سیسکو با ارائه‌ی این سطح خواسته تا برترین متخصصان

بین‌المللی شبکه را گلچین نماید، شاید بتوان رتبه‌ی Cisco Certified Architect معادل فوق دکترای شبکه در گرایش Design دانست!

Architect Certification

توپولوژی‌های شبکه:

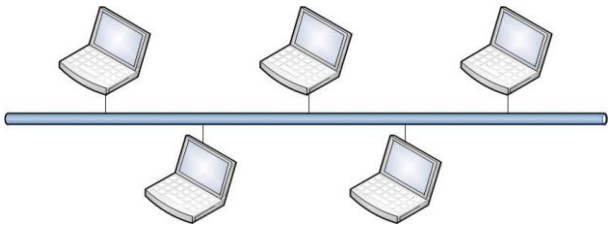
اصولاً به شکل هندسی اتصالات ادوات شبکه به هم را توپولوژی می‌گویند که به انواع مختلف زیر تقسیم‌بندی می‌شوند:

- Bus
- Ring
- Star
- Mesh
- Hybrid
- Point to Point
- Point to Multi Point

که هرکدام از این شبکه‌ها در جاهای مختلف به کار می‌روند.

توپولوژی BUS(خطی):

در توپولوژی Bus، همه‌ی کامپیوترهای شبکه از طریق یک کابل به هم متصل می‌شوند. در این شبکه، هر کامپیوتر سیگنال‌ها را دریافت کرده و آن را به کامپیوتر بعدی می‌فرستد. این شبکه یکی از آسان‌ترین شبکه‌های موجود است که در حال حاضر هم از آن استفاده می‌شود. مشکل این شبکه زمانی اتفاق می‌افتد که 2 کامپیوتر بخواهند در یک‌زمان اطلاعات را بر روی یک خط بفرستند که در این صورت collision رخ می‌دهد.



مزایا:

1- پیاده‌سازی آن بسیار آسان است.

2- صرفه‌جویی در هزینه، چون احتیاج به یک کابل دارد.

3- به‌راحتی می‌توان قطع شدن کابل را مشخص کرد و عیب‌یابی آن آسان است.

معایب:

1- اگر برای یکی از کامپیوترها مشکلی ایجاد شود، کل شبکه از کار می‌افتد.

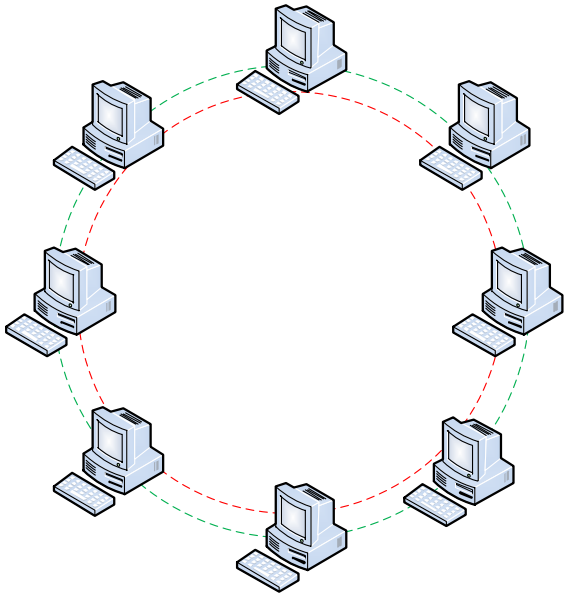
2- با افزودن کامپیوترهای جدید و ارسال حجم زیاد اطلاعات بر روی یک خط، کارایی شبکه کم می‌شود.

3- نرخ انتقال اطلاعات به نسبت توپولوژی‌های دیگر پایین است.

4- در کل برای شبکه‌های با تعداد کامپیوترهای کم به کار می‌آید.

توپولوژی Ring (حلقوی):

در این توپولوژی، کامپیوترها با استفاده از یک کابل به‌صورت دایره‌وار به هم متصل می‌شوند و این کابل انتها ندارد. کامپیوترها با دریافت سیگنال از کامپیوتر قبلی، آن را تقویت کرده و به کامپیوتر بعدی می‌فرستند. در این شبکه، اگر در یکی از کامپیوترها مشکلی ایجاد شود، کل شبکه از کار خواهد افتاد که برای حل این مشکل از 2 خط با جهت‌های متفاوت استفاده می‌کنند تا وقتی‌که یکی از کابل‌ها قطع شد، دیگری بتواند به کار خود ادامه دهد.



مزایا:

1- استفاده از طول کابل کمتر نسبت به روش قبلی.

2- نیاز به فضای زیاد برای راه‌اندازی شبکه ندارد.

معایب:

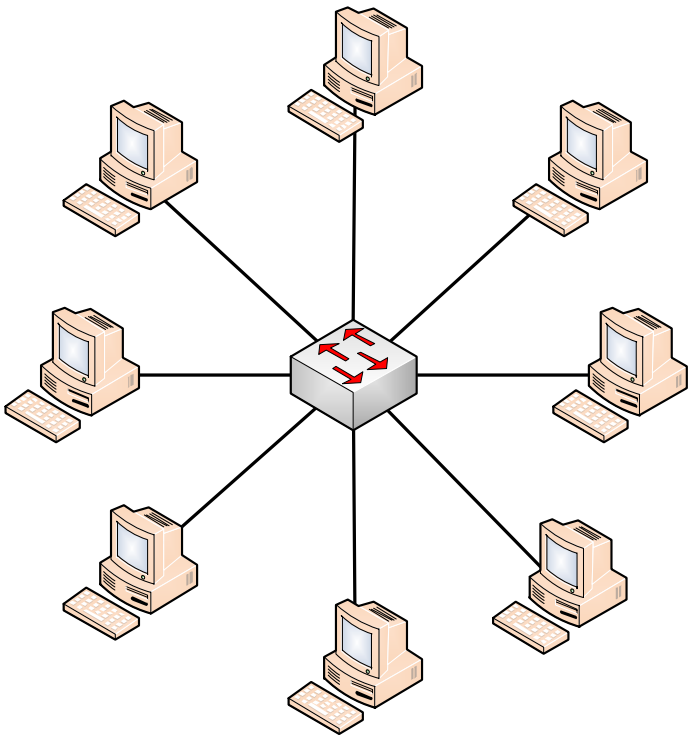
1- اگر یکی از کامپیوترها از کار بیفتد کل شبکه از کار خواهد افتاد.

2- اشکال‌زدایی مشکل است، چون باید تک‌تک کامپیوترها بررسی شوند.

3- تغییر در ساختار شبکه در آینده مشکل است.

توپولوژی Star (ستاره‌ای):

در این نوع از شبکه، کامپیوترها و یا ادوات دیگر شبکه به‌وسیله‌ی یک دستگاه مرکزی مانند Hub یا Switch به همدیگر متصل می‌شوند که امروزه هم در اکثر جاها از این شبکه استفاده می‌کنند.



مزایا:

1- سادگی دسترسی به شبکه.

2- با ایجاد مشکل در یک کامپیوتر، آن کامپیوتر از مسیر خارج می‌شود و بقیه‌ی شبکه به کار خود ادامه می‌دهد.

3- می‌تواند در آینده برای شبکه‌های جدیدتر توسعه پیدا کند.

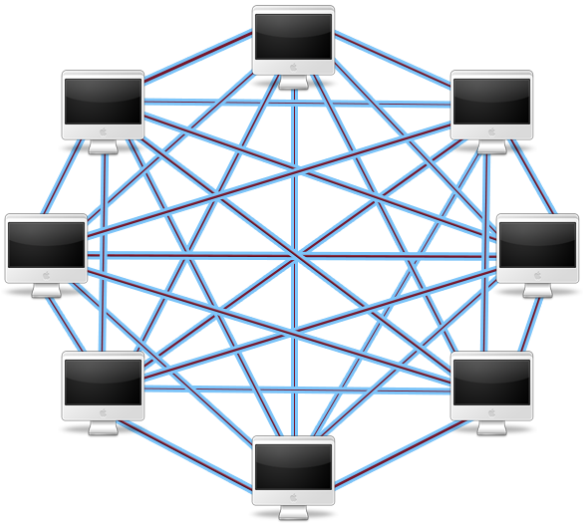
معایب:

1- درصورتی‌که نقطه‌ی مرکزی شبکه، یعنی Hub یا Switch از کار بیفتد کل شبکه مختل می‌شود.

2- اندازه‌ی کابل به علت دستیابی مستقیم هر کامپیوتر به آن بسیار زیاد است و هزینه را افزایش می‌دهد.

توپولوژی mesh (تو در تو):

در این توپولوژی هر گره به‌طور مستقیم، بدون هیچ واسطه‌ای با کلیه‌ی گره‌های دیگر در ارتباط است؛ بنابراین با فرض N گره در توپولوژی، هر گره باید دارای N-1 پورت باشد. اگر یک گره به کلیه‌ی گره‌ها متصل باشد به آن Full Mesh هم می‌گویند و بیشتر در مکان‌های نظامی کاربرد دارد.



مزایا:

1- سرعت بسیار بالا.

2- امنیت بالا.

3- اگر مشکلی در یک لینک ایجاد شود، تأثیری بر روی شبکه نخواهد داشت.

4- سادگی در عیب‌یابی.

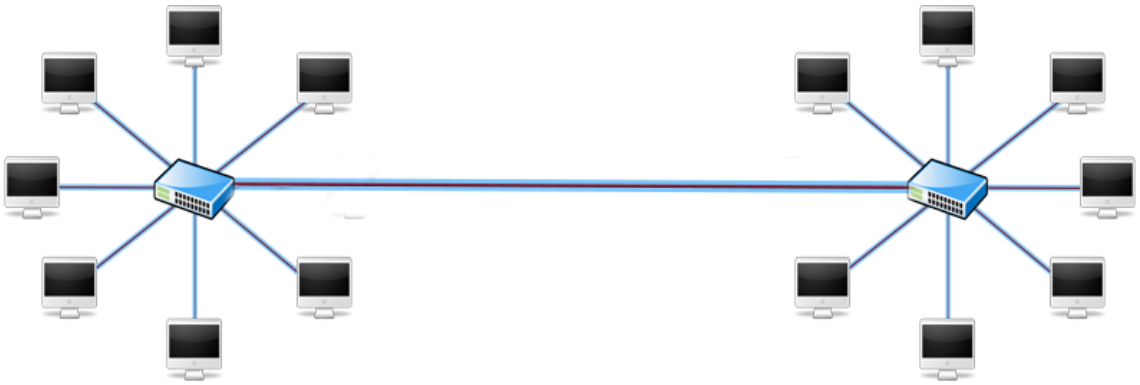
معایب:

1- هزینه‌ی بالا به علت استفاده‌ی زیاد از کابل.

2- هر گره برای اتصال به شبکه، نیاز به چندین interface دارد.

توپولوژی Hybrid (دو رگه):

این شبکه به این علت به نام Hybrid است که در ساختار خود از دو شبکه‌ی Bus و Star استفاده می‌کند.

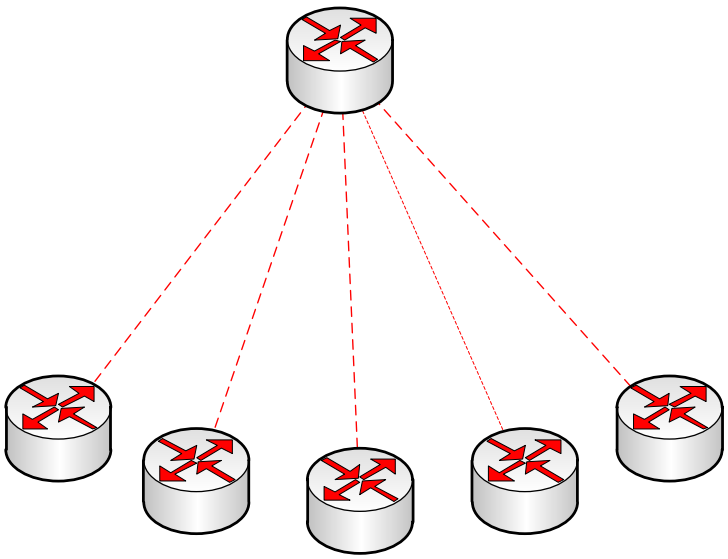


توپولوژی point to Point (نظیر به نظیر):

در این نوع شبکه، 2 دستگاه به‌صورت مستقیم توسط یک کابل به هم متصل می‌شوند و باهم ارتباط برقرار می‌کنند.

توپولوژی Point to Multi Point: (یک به چند):

در این شبکه، چندین Node به یک سیستم ارتباطی متصل می‌شوند، این حالت را می‌توان در سیستم‌های wireless مشاهده کرد.



لایه‌بندی شبکه:

در ساختار شبکه از دو مدل لایه‌بندی استفاده می‌شود.

- ✓ مدل OSI
- ✓ مدل TCP/IP

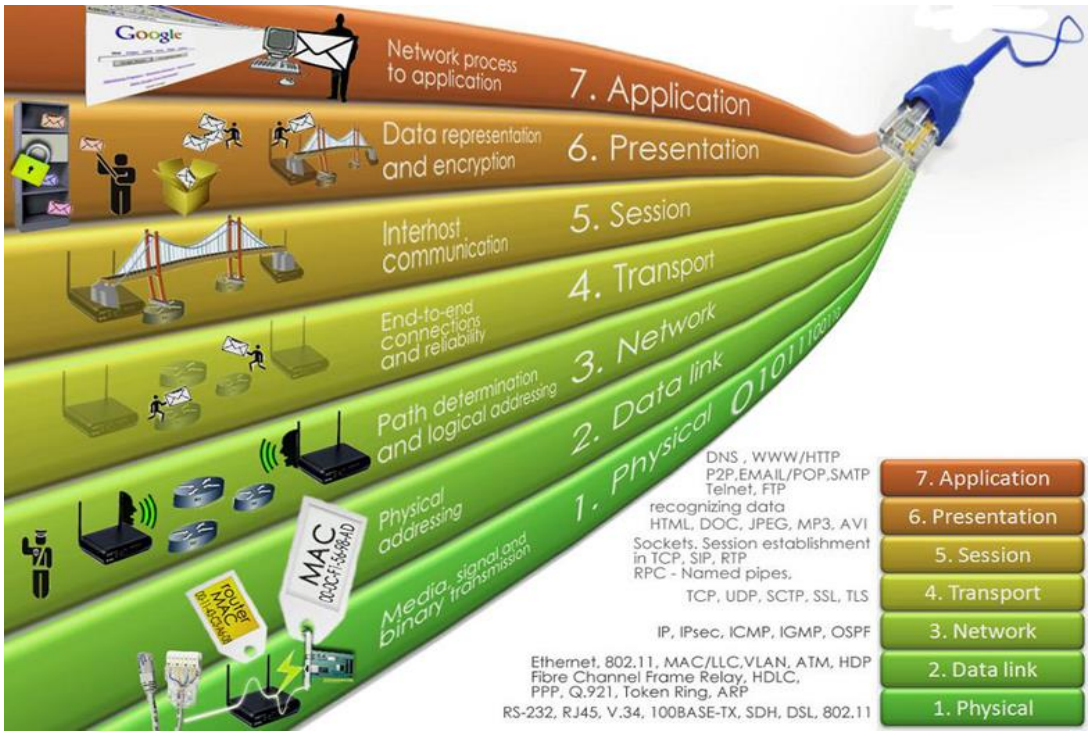
مدل OSI:

این مدل برگرفته از کلمه‌ی Open System Interconnection است و برای ارتباط بین دو کامپیوتر مبدأ و مقصد به کار می‌رود. این مدل در سال 1980 توسط سازمان ISO طراحی و پیاده‌سازی شده است و طبق سالیان متوالی تغییراتی روی آن صورت گرفته است، هرچند که همان ساختار اصلی خود را حفظ کرده است.

این مدل بر اساس یکی سری قراردادها با لایه‌ی مقابل خود در کامپیوتر دیگر ارتباط برقرار می‌کند و این کار باعث افزایش سرعت و امنیت در شبکه خواهد شد.

تمام کمپانی‌های نرم‌افزاری و سخت‌افزاری طبق این قرارداد محصولات خود را پیاده‌سازی می‌کنند. اگر توجه کرده باشید، بعضی از شرکت‌ها دارای گواهینامه ISO 9001,9002 و غیره می‌باشند، یعنی اینکه طبق استاندارد این سازمان باید کار کنند.

این مدل به صورت قراردادی از هفت لایه‌ی زیر تشکیل‌شده است که هر لایه را برای شما توضیح می‌دهیم:



اگر به شکل صفحه‌ی قبل توجه کنید، لایه‌های بالاتر به‌صورت نرم‌افزاری می‌باشند و هر چه به طرف لایه‌های پایین‌تر می‌آییم با سخت‌افزار کار داریم.

7– لایه‌ی Application (کاربردی):

این لایه با برنامه‌های کاربردی روی سیستم عامل که در شبکه کار می‌کنند ارتباط دارد، مانند نرم‌افزارهای مرورگر و انواع سرویس‌های مربوط به شبکه مانند (Telnet – pop3 – mail – ftp - tftp,...)، این لایه اطلاعات دریافتی را قطعه‌قطعه کرده به صورتی که لایه‌ی پایینی بتواند این اطلاعات را درک کند. نظارت بر Error Recovery و Flow control در هنگام ارسال و دریافت اطلاعات بر عهده‌ی این لایه است.

6–لایه‌ی presentation (نمایش):

این لایه اطلاعات دریافتی را از لایه‌ی بالایی خود دریافت می‌کند و آن‌ها را فشرده‌سازی(Compression) و رمزنگاری(encryption) می‌کند و به لایه‌ی پایینی ارسال می‌کند، البته این لایه هم می‌تواند اطلاعات فشرده‌سازی شده را از حالت فشرده خارج کند (DeCompression) و هم می‌تواند قفل‌گشایی کند(decryption).

5– لایه‌ی Session (جلسه):

در این لایه، 2 کامپیوتر ارسال و دریافت‌کننده اطلاعات، دور یک میز می‌نشینند و جلسه‌ای باهم برقرار می‌کنند. در این جلسه بر نوع فایل ارسالی بحث و گفتگو می‌شود که این فایل از چه نوعی است، وقتی به نتیجه رسیدند باهم ارتباط برقرار می‌کنند، به این موضوع هم توجه داشته باشید که آغاز و اتمام یک ارتباط از طریق این لایه انجام می‌گیرد.

4–لایه‌ی Transport (انتقال):

برای توضیح این لایه، باید 2 نوع ارتباط را برای شما تشریح کنم:

1- Connection Less

2- Connection Oriented

1- در ارتباط connection Less کامپیوتر مبدأ برای کامپیوتر مقصد اطلاعات ارسال می‌کنند، اما کامپیوتر مقصد هیچ‌گونه پیامی (Acknowledge) مبنی بر دریافت اطلاعات به کامپیوتر مبدأ نمی‌دهد. این مدل را

می‌توانید در نرم‌افزارهای چت که به‌صورت صوتی با طرف خود صحبت می‌کنید، مشاهده کنید که با این کار سرعت انتقال اطلاعات به علت عدم دریافت Acknowledge افزایش می‌یابد.

2- در ارتباط Connection oriented که ارتباط بسیار مهمی است، کامپیوتر مبدأ اطلاعات خود را به کامپیوتر مقصد ارسال می‌کند و منتظر می‌ماند تا کامپیوتر مقصد، پیام Acknowledge را به مبدأ ارسال کند تا متوجه‌ی دریافت اطلاعات در مقصد شود. اگر این کار انجام نشود در طی زمان مشخص، دوباره اطلاعات را برای مقصد ارسال می‌کند، تا زمانی این کار انجام می‌شود که کامپیوتر مقصد Acknowledge را ارسال کند. این روش برای ارتباطات بسیار مهم، کاربرد دارد.

Acknowledge یک تأییدی بر دریافت اطلاعات به صورت صحیح است.

در این لایه، این 2 ارتباط که در بالا توضیح دادم مشخص می‌شود، یعنی طبق فایلی که ارسال می‌شود ارتباط آن هم مشخص می‌شود.

پروتکل‌هایی که در این لایه کار می‌کنند:

- ✓ ADSP, AppleTalk Data Stream Protocol
- ✓ ASP, AppleTalk Session Protocol
- ✓ H.245, Call Control Protocol for Multimedia Communication
- ✓ ISO-SP, OSI session-layer protocol (X.225, ISO 8327)
- ✓ iSNS, Internet Storage Name Service
- ✓ L2F, Layer 2 Forwarding Protocol
- ✓ L2TP, Layer 2 Tunneling Protocol
- ✓ NetBIOS, Network Basic Input Output System
- ✓ PAP, Password Authentication Protocol
- ✓ PPTP, Point-to-Point Tunneling Protocol
- ✓ RPC, Remote Procedure Call Protocol
- ✓ RTCP, Real-time Transport Control Protocol
- ✓ SMPP, Short Message Peer-to-Peer
- ✓ SCP, Session Control Protocol
- ✓ SOCKS, the SOCKS internet protocol, see Internet socket
- ✓ ZIP, Zone Information Protocol
- ✓ SDP, Sockets Direct Protocol

3– لایه‌ی Network (شبکه):

این لایه با ip ها سروکار دارد و ip مقصد و مبدأ را به بسته‌ی ارسالی ما اضافه می‌کند و به لایه پایین‌تر می‌فرستد.

پروتکل‌هایی که در این لایه کار می‌کنند:

- ✓ IPv4/IPv6, Internet Protocol
- ✓ DVMRP, Distance Vector Multicast Routing Protocol
- ✓ ICMP, Internet Control Message Protocol
- ✓ IGMP, Internet Group Management Protocol
- ✓ PIM-SM, Protocol Independent Multicast Sparse Mode
- ✓ PIM-DM, Protocol Independent Multicast Dense Mode
- ✓ IPsec, Internet Protocol Security
- ✓ IPX, Internetwork Packet Exchange
- ✓ RIP, Routing Information Protocol
- ✓ DDP, Datagram Delivery Protocol
- ✓ RSMLT Routed-SMLT
- ✓ ARP, Address Resolution Protocol

2–لایه‌ی Data Link (داده):

آدرس Mac کارت‌های شبکه که یک شماره اختصاصی است به بسته‌ها اضافه می‌شود. اگر به شکل لایه‌ها تصویر قبلی توجه کنید متوجه‌ی این موضوع خواهید شد.

پروتکل‌هایی که در این لایه کار می‌کنند:

- ✓ Address Resolution Protocol (ARP)
- ✓ ARCnet
- ✓ ATM
- ✓ Cisco Discovery Protocol (CDP)
- ✓ Controller Area Network (CAN)
- ✓ Econet
- ✓ Ethernet
- ✓ Ethernet Automatic Protection Switching (EAPS)
- ✓ Fiber Distributed Data Interface (FDDI)
- ✓ Frame Relay
- ✓ High-Level Data Link Control (HDLC)
- ✓ IEEE 802.2 (provides LLC functions to IEEE 802 MAC layers)
- ✓ IEEE 802.11 wireless LAN
- ✓ LattisNet
- ✓ Link Access Procedures, D channel (LAPD)

- ✓ LocalTalk
- ✓ Multiprotocol Label Switching (MPLS)
- ✓ Nortel Discovery Protocol (NDP)
- ✓ OpenFlow (SDN)
- ✓ Split multi-link trunking (SMLT)
- ✓ Point-to-Point Protocol (PPP)
- ✓ Serial Line Internet Protocol (SLIP) (obsolete)
- ✓ Spanning Tree Protocol
- ✓ StarLan
- ✓ Token ring
- ✓ Unidirectional Link Detection (UDLD)
- ✓ and most forms of serial communication.

1–لایه‌ی Physical (لایه‌ی فیزیکی):

این لایه که آخرین لایه در مدل OSI است، با سیگنال‌ها و کابل‌ها در ارتباط است و سیگنال را از طریق کابل به کامپیوتر مورد نظر ارسال می‌کنند.

پروتکل‌هایی که در این لایه کار می‌کنند:

- ✓ Telephone network modems- V.92
- ✓ IRDA physical layer
- ✓ USB physical layer
- ✓ EIA RS-232, EIA-422, EIA-423, RS-449, RS-485
- ✓ Ethernet physical layer Including 10BASE-T, 10BASE2, 10BASE5, 100BASE-TX, 100BASE-FX, 100BASE-T, 1000BASE-T, 1000BASE-SX and other varieties
- ✓ Varieties of 802.11 Wi-Fi physical layers
- ✓ DSL
- ✓ ISDN
- ✓ T1 and other T-carrier links, and E1 and other E-carrier links
- ✓ SONET/SDH
- ✓ Optical Transport Network (OTN)
- ✓ GSM Um air interface physical layer
- ✓ Bluetooth physical layer
- ✓ ITU Recommendations: see ITU-T
- ✓ IEEE 1394 interface
- ✓ TransferJet physical layer
- ✓ Etherloop
- ✓ ARINC 818 Avionics Digital Video Bus
- ✓ G.hn/G.9960 physical layer
- ✓ CAN bus (controller area network) physical layer
- ✓ Mobile Industry Processor Interface physical layer

مدل TCP / IP:

IP، پروتکلی استاندارد برای ارتباط کامپیوترهای موجود در یک شبکه‌ی مبتنی بر ویندوز ۲۰۰۰ است. از پروتکل فوق، به منظور ارتباط در شبکه‌های بزرگ استفاده می‌گردد. برقراری ارتباط از طریق پروتکل‌های متعددی که در چهار لایه مجزا سازمان‌دهی شده‌اند، میسر می‌گردد. هر یک از پروتکل‌های موجود در پشته‌ی TCP/IP، دارای وظیفه‌ای خاص در این زمینه (برقراری ارتباط) می‌باشند. در زمان ایجاد یک ارتباط، ممکن است در یک لحظه تعداد زیادی از برنامه‌ها، با یکدیگر ارتباط برقرار نمایند. TCP/IP، دارای قابلیت تفکیک و تمایز یک برنامه‌ی موجود بر روی یک کامپیوتر با سایر برنامه‌ها بوده و پس از دریافت داده‌ها از یک برنامه، آن‌ها را برای برنامه‌ی متناظر موجود بر روی کامپیوتر دیگر ارسال می‌نماید. نحوه‌ی ارسال داده توسط پروتکل TCP/IP از محلی به محل دیگر با فرآیند ارسال یک نامه از شهری به شهر دیگر، قابل‌مقایسه است.

برقراری ارتباط مبتنی بر TCP/IP با فعال شدن یک برنامه بر روی کامپیوتر مبدأ آغاز می‌گردد. برنامه‌ی فوق، داده‌های موردنظر جهت ارسال را به‌گونه‌ای آماده و فرمت می‌نماید که برای کامپیوتر مقصد، قابل خواندن و استفاده باشند. (مشابه‌ی نوشتن نامه با زبانی که دریافت‌کننده، قادر به مطالعه‌ی آن باشد). در ادامه، آدرس کامپیوتر مقصد به داده‌های مربوطه اضافه می‌گردد (مشابه‌ی آدرس گیرنده که بر روی یک نامه مشخص می‌گردد). پس از انجام عملیات فوق، داده به همراه اطلاعات اضافی (درخواستی برای تأیید دریافت در مقصد) در طول شبکه به حرکت درآمده تا به مقصد مورد نظر برسد. عملیات فوق، ارتباطی به محیط انتقال شبکه به منظور انتقال اطلاعات نداشته و تحقق عملیات فوق با رویکردی مستقل نسبت به محیط انتقال، انجام خواهد شد.

لایه‌های پروتکلTCP/IP:

TCP/IP ، فرآیندهای لازم به منظور برقراری ارتباط را سازمان‌دهی می‌کند و در این راستا از پروتکل‌های متعددی در پشته‌ی TCP/IP استفاده می‌گردد. به منظور افزایش کارایی در تحقق فرآیندهای موردنظر، پروتکل‌ها در لایه‌های متفاوتی، سازمان‌دهی شده‌اند. اطلاعات مربوط به آدرس‌دهی در انتها، قرارگرفته و بدین ترتیب کامپیوترهای موجود در شبکه قادر به بررسی آن با سرعت مطلوب خواهند بود. در این راستا، صرفاً کامپیوتری که به عنوان کامپیوتر مقصد معرفی شده است، امکان بازنمودن بسته‌ی اطلاعاتی و انجام پردازش‌های لازم بر روی آن را دارا خواهد بود. TCP/IP از یک مدل ارتباطی چهار لایه به منظور ارسال اطلاعات از محلی به محل دیگر استفاده می‌نماید. Application ,Transport ,Internet و Network Interface، لایه‌های موجود در پروتکل TCP/IP می‌باشند. هر یک از پروتکل‌های وابسته به پشته‌ی TCP/IP با توجه به رسالت خود، در یکی از لایه‌های فوق، قرار می‌گیرند.

لایه‌ی Application:

لایه‌ی Application، بالاترین لایه در پشته‌ی TCP/IP است. تمامی برنامه‌ها و ابزارهای کاربردی در این لایه، با استفاده از لایه‌ی فوق، قادر به دست‌یابی به شبکه خواهند بود. پروتکل‌های موجود در این لایه، به منظور فرمت-دهی و مبادله‌ی اطلاعات کاربران استفاده می‌گردند. HTTP و FTP دو نمونه از پروتکل‌های موجود در این لایه می‌باشند.

پروتکل HTTP (Hypertext Transfer Protocol) از پروتکل فوق، به منظور ارسال فایل‌های صفحات وب، استفاده می‌گردد.

پروتکل FTP (File Transfer Protocol) از پروتکل فوق، برای ارسال و دریافت فایل استفاده می‌گردد.

لایه‌ی Transport:

لایه‌ی حمل، قابلیت ایجاد نظم و ترتیب و تضمین ارتباط بین کامپیوترها و ارسال داده به لایه‌ی Application (لایه‌ی بالای خود) و یا لایه اینترنت (لایه‌ی پایین خود) را بر عهده دارد. لایه‌ی فوق، همچنین مشخصه‌ی منحصر به فردی از برنامه‌ای که داده را عرضه نموده است، مشخص می‌نماید. این لایه، دارای دو پروتکل اساسی است که نحوه‌ی توزیع داده را کنترل می‌نمایند.

TCP(Transmission Control Protocol) پروتکل فوق، مسئول تضمین صحت توزیع اطلاعات است.

UDP(User Datagram Protocol) پروتکل فوق، امکان عرضه‌ی سریع اطلاعات بدون پذیرفتن مسئولیتی در رابطه با تضمین صحت توزیع اطلاعات را بر عهده دارد.

لایه‌ی Internet:

لایه‌ی اینترنت، مسئول آدرس‌دهی، بسته‌بندی و روتینگ داده‌ها است. لایه‌ی فوق، شامل چهار پروتکل اساسی است:

IP(Internet Protocol) پروتکل فوق، مسئول آدرسی داده‌ها به‌منظور ارسال به مقصد مورد نظر است.

ARP(Address Resoulation Protocol) پروتکل فوق، مسئول مشخص نمودن آدرس MAC (Media Access Control) آداپتور شبکه بر روی کامپیوتر مقصد است.

ICMP(Internet Control Message Protocol) پروتکل فوق، مسئول ارائه‌ی توابع عیب‌یابی و گزارش خطا در صورت عدم توزیع صحیح اطلاعات است.

IGMP(Internet Group Managemant Protocol) مسئولیت مدیریت Multicasting در TCP/IP را بر عهده دارد.

لایه‌ی Network:

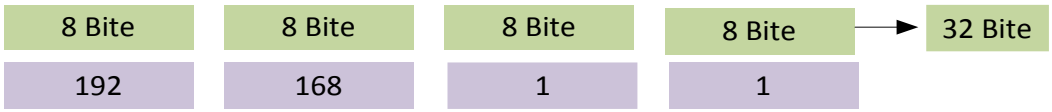
لایه‌ی شبکه، مسئول استقرار داده بر روی محیط انتقال شبکه و دریافت داده از محیط انتقال شبکه است. لایه‌ی فوق، شامل دستگاه‌های فیزیکی نظیر کابل شبکه و آداپتورهای شبکه است. کارت شبکه (آداپتور) دارای یک عدد دوازده رقمی مبنای شانزده (نظیر B : ٥-٥٠-٠٤-D٢٢-٤-٦٦) بوده که آدرس MAC، نامیده می‌شود. لایه‌ی اینترفیس شبکه، شامل پروتکل‌های مبتنی بر نرم‌افزار مشابه‌ی لایه‌های قبل نیست. پروتکل‌های Ethernet و ATM (Asynchronous Transfer Mode)، نمونه‌هایی از پروتکل‌های موجود در این لایه می‌باشند. پروتکل‌های فوق، نحوه‌ی ارسال داده در شبکه را مشخص می‌نمایند.

بررسی IPV4:

در این بخش، گذری به دنیای زیبای IP ها داریم و نحوه‌ی آدرس‌دهی در شبکه را می‌آموزیم. اگر با IP ها مشکل دارید، حتماً این بخش را به دقت مطالعه کنید .

شروع کار:

همان‌طور که مشاهده می‌کنید، IPv4 از چهار قسمت تشکیل شده است که هر بخش، 8 بیت است و اگر 8 ضربدر 4 کنیم، می‌شود 32 بیت.



به هر یک از این قسمت‌ها، یک هشت‌تایی یا همان octet می‌گویند. مثلاً 192.168.1.1 که به هر قسمت برفرض 192یک octet می‌گویند.

IP ها به 5 کلاس تقسیم می‌شوند که هرکدام را باهم مرور می‌کنیم.

Class A: 1 – 127

Class B: 128-191

Class C: 192- 223

Class D: 224 – 239

Class E: 240 – 255

مثال:

192.168.1.1 که IP اول عدد آن 192 است، این IP در رنج کلاس c قرار دارد. به همین صورت اگر Octed اول در یکی از رنج‌های مشخص‌شده‌ی بالا قرار داشته باشد، می‌گوییم که در این کلاس قرار دارد. مثلاً، 10.10.10.1 یک IP در کلاس A است، چون 10 عدد قسمت اول آن است و بین شماره 1-127 قرار دارد.

- تذکر: رنج IP کلاس A از 1 - 126 است و شماره‌ی 127 برای تست کارت شبکه به کار می‌رود که همان 127.0.0.1 است و به آدرس loopback معروف است، پس برای استفاده از کلاس A می‌توان از شماره‌ی 1 – 126 استفاده کرد.

توجه داشته باشید که کلاس D برای Multicasting به کار می‌رود که این بحث در درس‌های بعدی باهم مرور می‌کنیم، این IP ها روی هاست یا همان سیستم تنظیم نمی‌شوند و IP های کلاس E برای تحقیقات به کار می‌رود و قابل‌استفاده نیست، پس فقط از IP های کلاس‌های A,B,C برای شبکه خود استفاده می‌کنیم.

IP ها بر دو نوع می‌باشند:

1- Private address: این دسته از IP، فقط و فقط در شبکه‌های داخلی به کار می‌روند و در دنیای اینترنت اعتباری ندارند. این نوع از IP ها در هر کلاس وجود دارند که به ترتیب زیر است:

Class A:	**10.0.0.0**
Class B:	**172.16.0.0 - 172.31.255.255**
Class C:	**192.168.0.0**

IP هایی که با این اعداد شروع می‌شوند، مربوط به شبکه‌ی داخلی می‌باشند و اعتباری در اینترنت ندارند.

2- Public Address: این دسته از IP ها توسط سازمانی به نام IANA رجیستر می‌شوند و بعد از این کار در اینترنت اعتبار دارند. این دسته شامل تمام IP های کلاس‌های A,B,C است، به غیر از آدرس‌های Private Address که در قسمت قبل باهم بررسی کردیم.

یک IP از دو بخش تشکیل شده است:

- Network address
- Host address

Network Address، به تعداد شبکه‌های موجود و Host address، به تعداد میزبان موجود اشاره دارد.

برای اینکه بتوانیم این دو موضوع را درک کنیم، باید subnet mask را بررسی کنیم.

Subnet Mask:

این آدرس، نشان‌دهنده‌ی این است که چه مقدار بیت متعلق به آدرس شبکه و چه مقدار آن، متعلق به میزبان شبکه است.

Class	IP	Subnet Mask
A	**11.1.5.1**	255.0.0.0
B	**175.1.1.1**	255.255.0.0
C	**192.168.1.1**	255.255.255.0

همان‌طور که مشاهده می‌کنید برای هر IP در کلاس مشخص، یک subnet mask تعریف شده است که نشان‌دهنده‌ی تعداد شبکه و هاست است.

اگر به جدول توجه کنید در قسمت Subnet Mask اعداد 255 مربوط به Network Address و اعداد 0 مربوط به Host address می‌باشند.

مثلاً اگر IP به شماره 195.1.1.1 به شما بدهند و بگویند subnet Mask آن را مشخص کنید، سریع با نگاه کردن به کلاس‌های IP متوجه می‌شوید که عدد اول این IP در رنج کلاس c قرار دارد وSubnet Mask آن به‌صورت 255.255.255.0 است.

همیشه روال به این صورت نیست که IP ها به همین صورت استاندارد در شبکه‌ها نشان داده شوند به این کلاس‌بندی‌ها اصولاً یک الگوی استاندارد می‌گویند، امّا همیشه این‌چنین نیست و الگوی غیراستاندارد هم وجود دارد.

الگوی غیراستاندارد:

هر قسمت IP (octet) از هشت عدد تشکیل شده است که می‌تواند صفر یا یک باشد.

11000111 . 11101011 . 11111110 . 11110111

هرکدام از این شماره‌ها در هر بخش دارای یک شماره اختصاصی می‌باشند که به‌صورت زیر است.

1 2 4 8 16 32 64 128 این شماره‌ها، روی هرکدام از چهار بخش بالا به‌صورت جداگانه قرار می‌گیرند.

اولین قسمت از سمت چپ را در زیر مشاهده می‌کنید، به نحوه‌ی قرار گرفتن اعداد توجه کنید.

128	64	32	16	8	4	2	1
1	**1**	**1**	**1**	**0**	**1**	**1**	**1**

برای درک بهتر موضوع، یک مثال را باهم بررسی می‌کنیم:

192.168.1.1، برای به دست آوردن Binary این IP، طبق شماره‌هایی که در هر قسمت به شما گفتیم، عمل کنید. مثلاً اگر بخواهیم شماره‌ی 192 را از بین شماره‌های 1 2 4 8 16 32 64 128 به دست بیاوریم، همیشه از سمت چپ شروع می‌کنیم، می‌گوییم 128 از 192 کوچک‌تر است، پس زیر 128 را 1 قرار می‌دهیم ، در ادامه اگر 64 را با 128 که قبلاً به دست آوردیم جمع کنیم می‌شود 192 !!! چه جالب 192 شد پس زیر 64 هم 1 قرار می‌دهیم؛ با این حساب، توانستیم شماره‌ی 192 را پیدا کنیم، وقتی به شماره‌ی مورد نظر رسیدیم، زیر بقیه‌ی شماره‌ها صفر قرار می‌دهیم. طبق جدول:

128	64	32	16	8	4	2	1
1	1	0	0	0	0	0	0

پس شماره‌ی باینری به‌دست‌آمده، 11000000 است. بقیه‌ی اعداد هم به‌صورت زیر است.

192	168	1	1
11000000	10101000	00000001	00000001

در یک رنج IP، دو نوع IP قابل‌استفاده نیستند، به مثال زیر توجه کنید (مهم):

IP : 192.168.1.1
Sbnet Mask :255.255.255.0

همان‌طور که آموختیم، 255 به این نکته اشاره می‌کند که IP های 192.168.1 ثابت است و فقط octet آخر قابل‌تغییر از 0 تا 255 است. هر یک از قسمت‌های IP از 0 تا 255 قابل‌تغییر است.

این IP، فقط در قسمت آخر قابل‌تغییر است، بین 0 تا 255، همان‌طور که گفتیم دو IP در هر رنج مانند این IP قابل‌استفاده نیستند. به جدول زیر توجه کنید:

192.168.1.0	Network address
192.168.1.1	IP قابل‌استفاده
192.168.1.2	IP قابل‌استفاده
192.168.1.3	IP قابل‌استفاده
⋮	
192.168.1.255	Broadcast

اولین IP به‌عنوان Network address و آخرین IP به‌عنوان Broadcast IP انتخاب می‌شود و نمی‌توانیم در شبکه از آن‌ها استفاده کنیم.

تذکر: نام دیگر Network address، Net ID است.

مثالی دیگر: در IP زیر، Net ID و Broadcast ID را به دست می‌آوریم:

IP: 172.16.1.1
Subnetmask: 255.255.0.0

در این مثال،IP از رنج B است. همان‌طور که مشاهده می‌کنید، subnet mask از دو تا 255 تشکیل شده است پس 2 قسمت اول IP، ثابت(172.16) و دو قسمت بعد قابل‌تغییرند، به این صورت نتیجه می‌دهد که:

Net ID: 172.16.0.0
Broadcast ID: 172.16.255.255

اختصاص دادن رنج IP به شبکه:

زمانی پیش می‌آید که شما مدیر شبکه‌ی یک شرکت یا یک کارخانه می‌شوید، رئیس شما یک رنج IP خاصی را به شما می‌دهد و می‌گوید که این رنج IP را به اتاق‌های مختلف این شرکت بدهید، به‌طوری‌که IP ها هدر نرود و کم نیاید.

برای این کار یک مثال می‌زنیم و باهم حل می‌کنیم:

شما در یک شرکت کار می‌کنید که از 3 اتاق حسابداری، کامپیوتر و طراحی تشکیل شده است؛ در این اتاق‌ها، چندین کامپیوتر به قرار زیر وجود دارد.

اتاق حسابداری: 50 کامپیوتر

اتاق کامپیوتر: 60 کامپیوتر

اتاق طراحی: 14 کامپیوتر

IP در رنج زیر می‌باشد.

192.168.1.0
255.255.255.0

سریع این IP را در ذهن خود تحلیل کنید، حداکثر IP قابل‌استفاده، 255 عدد است. امیدوارم بحث‌های قبلی را خوب خوانده باشید. اگر متوجه شده باشید که حتماً هم همین‌طور است، Subnet mask از سه قسمت ثابت تشکیل شده است که فقط گزینه‌ی آخر قابل‌تغییر از 0 تا 255 است.

برای اختصاص دادن IP به این اتاق‌ها، اول از همه، اتاقی را انتخاب می‌کنیم که بیشترین کامپیوتر را دارد که در این مثال، اتاق کامپیوتر از 60 کلاینت برخوردار است.

همان‌طور که قبلاً گفتیم در هر قسمت از IP، اعدادی استاندارد و ثابتی وجود دارد.

128 64 32 16 8 4 2 1

همیشه این اعداد را در ذهن خود نگه داشته باشید، کل IP به همین اعداد خلاصه می‌شود و در ادامه، خیلی به آن نیاز داریم.

شما اول باید ببینید 60 بین کدام‌یک از اعداد بالا قرار دارد. با کمی دقت متوجه می‌شوید که بین 32 و 64 قرار دارد، چون ما احتیاج به 60 تا IP داریم، پس عدد 64 انتخاب می‌شود.

آدرس IP می‌شود 192.168.1.0~63 در این IP، از علامت ~ استفاده کردیم که نشان‌دهنده‌ی تعداد IP است.

همان‌طور که گفتیم، دو آدرس از این رنج برای Net ID و Broadcast ID است، یعنی رنج زیر:

Net ID: 192.168.1.0
Broadcast ID: 192.168.1.63

پس با کسر این دوIP، 62 آدرس برای ما می‌ماند که 60تا آدرس آن به کامپیوترها تخصیص داده می‌شود و 2، IP هم برای زمانی که اگر خواستیم کامپیوتر جدید در اتاق اضافه کنیم، به کار می‌رود.

رنج IP را به دست آوردیم؛ ولی subnet mask مربوط به این IP را به دست نیاوردیم؛ برای این کار همان عدد 64 را که درون شماره‌ها به دست آوردیم منهای 256 می‌کنیم (256 عددی است که از اعداد 0 تا 255 به دست می‌آید).

256 - 64 = 192

پس subnet mask برای این IP می‌شود: 255.255.255.192 که 192 نشان‌دهنده‌ی 64، IP برای این شبکه است.

اتاق بعدی‌ای که انتخاب می‌شود، اتاق حسابداری است که شامل 50 کامپیوتر است. برای به دست آوردن رنج IP برای این اتاق، از IP هایی که استفاده نشده است، استفاده می‌کنیم.

IP هایی که در اختیارداریم به‌صورت زیر است:

192.168.1.64

به این خاطر، از عدد 64 در آخر این IP استفاده کردم که 64 تا آدرس به اتاق قبلی داده شده است و قابل‌استفاده نیست.

مانند اتاق قبلی، شما به 64، IP نیاز دارید، چون 50 بین 32 و 64 قرار دارد، پس 64 انتخاب می‌شود.

IP و subnet mask برای این اتاق، به‌صورت زیر است:

192.168.1.64~128
255.255.255.192

برای اتاق سوم (طراحی)، احتیاج به 14، IP داریم، باید از بین 8 و 16 عدد 16 را انتخاب کنیم، پس IP و subnet mask به صورت زیر می‌شود:

192.168.1.129~145
255.255.255.240

باید متوجه شده باشید که ما احتیاج به 16، IP داریم، پس برای به دست آوردن subnet mask باید 16 را از 256 کم کنیم تا عدد آخر که 240 است به دست بیاید.

با این حساب، جدول نهایی IP ها به‌صورت زیر است:

طراحی	حسابداری	کامپیوتر
192.168.1.129~145	192.168.1.64~128	192.168.1.0~63
255.255.255.240	255.255.255.192	255.255.255.192
16	64	64

در این رنج‌ها، حداقل هدر رفت IP را داشتیم.

در این قسمت اگر مشکلی داشتید، می‌توانید از طریق ایمیل با من در تماس باشید.

IP ها به دو نوع Class Full و Class Less تقسیم می‌شوند که کلاس‌های A,B,C از نوع Class Full می‌باشند، به این دلیل به آن‌ها Class Full می‌گویند که subnet mask آن‌ها ثابت است و تغییری نمی‌کند، مثلاً 255.255.0.0 که این subnet مربوط به Class b است.

CIDR (Class Less Inter-Domain Routing)

این قسمت را با کمال دقت بخوانید.

این دسته از IP ها برای شرکت‌هایی که ارائه‌دهنده‌ی خدمات اینترنتی هستند(ISP) به کار می‌رود. برای این شبکه‌ها، مهم است که چه مقدار IP را به چه کسی می‌دهند.

IP هایی که به‌عنوان Class Less شناخته می‌شوند، به‌صورت زیر می‌باشند:

172.16.1.1/16

یک‌چیز جدید در این IP مشاهده می‌کنید و آن هم، یک slash به همراه یک شماره 16 است که نشان‌دهنده‌ی تعداد شبکه یا همان Net ID است که در این رابطه باهم به‌صورت کامل بحث می‌کنیم.

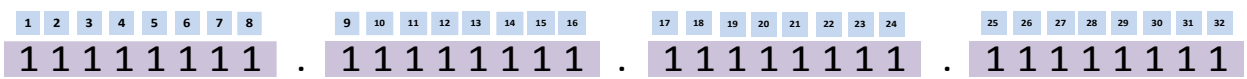
بعد از Slash، عددی بین 1 تا 32 قرار می‌گیرد. این همان عددی است که در ابتدای کار اشاره کردیم، یعنی هر IP از چهار قسمت هشت‌تایی تشکیل‌شده که می‌شود 32 تا، توجه داشته باشید که حداکثر عددی که پشت slash قرار می‌گیرد 30 است، چون 2 بیت برای host Bite است.

مثال: تعداد Host و subnet mask رنج IP زیر را به دست می‌آوریم:

192.168.1.1/24

سریع‌ترین روش برای به دست آوردن جواب به‌صورت زیر است:

هر قسمت از IP از هشت بیت تشکیل شده است که به صورت زیر است:



در مثالی که زدیم 24/ است که اگر به شکل نگاه کنید 3 تا octet اول را باهم جمع کنیم 24 می‌شود، پس می‌توان IP و Subnet mask را به این صورت نوشت:

192.168.1.0
255.255.255.0

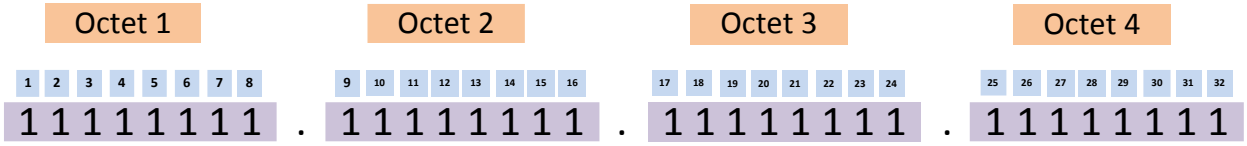
24/ می‌گوید که 3 تا octet اول ثابت باشد و octet آخر تغییر کند.

مثال بعدی:

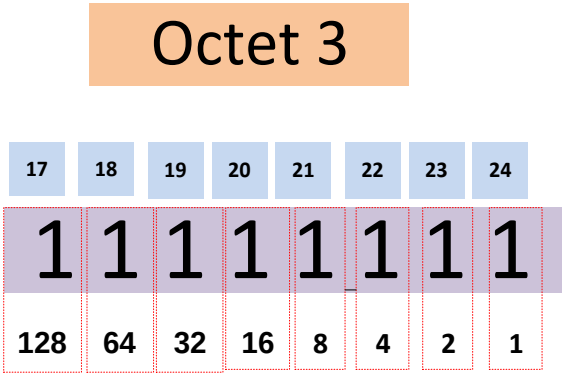
172.16.1.1/17

اگر به شکل زیر درست نگاه کنید 16 عدد اول را داریم، پس 2تا عدد اول IP ثابت است که در یک‌گوشه می‌نویسیم 172.16 بعد عدد 17 در octet سوم قرار دارد؛ پس، فقط با octet سوم کار می‌کنیم.

سریع اعداد 1 2 4 8 16 32 64 128 یادداشت می‌کنیم و بعد از آن، این اعداد را بالای عدد 17 تا 24 از سمت چپ به راست قرار می‌دهیم تا عدد 17 را پیدا کنیم. به شکل زیر توجه کنید:



در این شکل، به راحتی می‌توانید درک کنید که 17/ یعنی چه، ببینید سؤال از ما 17/ را می‌خواهد، پس طبق شکل، ما با octed3 کار داریم و دو octet اول را به‌صورت ثابت می‌نویسیم، چون تمام اعداد آن 1 است، پس برای به دست آوردن عدد 17، باید اعداد 1 2 4 8 16 32 64 128 را یادداشت کرده و از سمت چپ، اعداد 17 تا 24 را به آن‌ها اختصاص دهیم، یعنی عدد اولی که 128 باشد، به عنوان عدد 17 است و عدد دوم که عدد 64 باشد، به عنوان عدد 18 است. به شکل زیر توجه کنید:

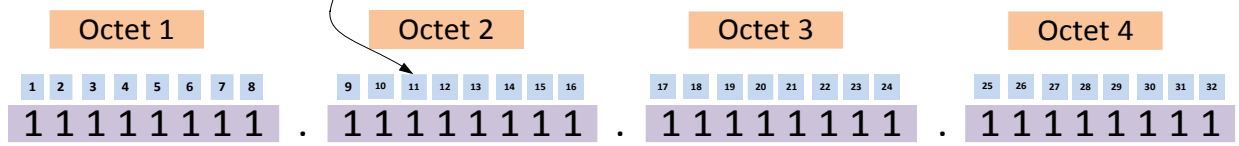


پس 17 همان عدد 128 است. این عدد را از 256 کم می‌کنیم و subnet mask ما به دست می‌آید.

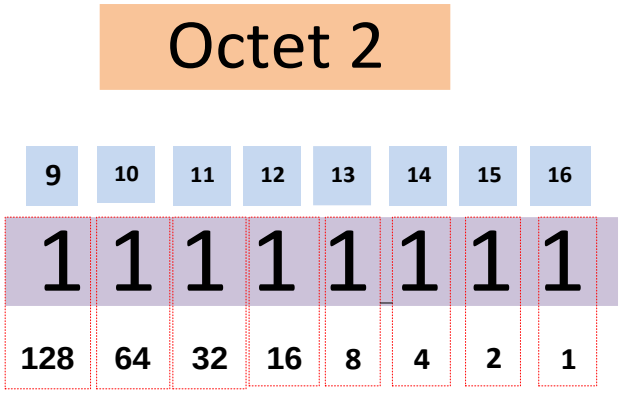
172.16.0~127.0
255.255.128.0

مثال پایانی این بحث:

10.10.10.1/11



همان‌طور که مشاهده می‌کنید 11/ از octed اول رد شده است، پس با octed دوم کار داریم این قسمت از عدد 9 شروع شده و به 16 ختم می‌شود. عددی که در مثال گفته 11/ است، پس از 9 و 10 باید بگذریم تا به عدد 11 برسیم. برای این منظور اعداد 1 2 4 8 16 32 64 128 و از سمت چپ اعداد را با شماره 9 و بعد 10 و بعد 11 شماره‌گذاری می‌کنیم، مانند شکل بالا عدد زیر 11 که عدد 32 است را از 256 کم می‌کنیم که 224 به دست می‌آید.



10.0~32.0.0

255.224.0.0

اگر در این بخش مشکلی داشتید، می‌توانید با من در تماس باشید.

Farshid_babajani2yahoo.com
Samancd2009@gmail.com

نگاهی به کابل‌ها در شبکه:

در این بخش، کابل‌های مختلف را بررسی می‌کنیم و با انواع آن کار می‌کنیم.

کل شبکه‌های امروزی از یکی از گروه‌های کابلی زیر استفاده می‌کند.

- کابل هم‌محور(coaxial)
- زوج تابیده‌شده(twisted-pair)
- فیبر نوری(fiber-optic)
- کابل سریال
- کابل Console

کابل هم‌محور coaxial:

این نوع کابل معمولاً در بیشتر شبکه‌های امروزی استفاده می‌شود، اما فقط در استفاده‌های خاص در ساده‌ترین شکل آن، کابل coaxial تشکیل‌شده است از یک هسته‌ی ساخته‌شده از مس خالص که توسط روکشی پوشیده شده است. یک روکش فلزی توری مانند و یک روکش بیرونی. هسته‌ی کابل coaxial حامل سیگنال‌های الکتریکی است که در واقع همان اطلاعات ما را تشکیل می‌دهد. این نوع کابل‌ها از یک روکش توری استفاده می‌کنند که کابل را در برابر امواج مزاحم یا همان Noise دور می‌کند. کلاً این نوع کابل برای ارتباط راه دور استفاده می‌شود، چون در ارتباط راه دور، افت سیگنال ندارد و نسبت به کابل Twisted Pair بهتر است.

انواع کابل coaxial:

- نازک(Thinnet)
- ضخیم (Thicknet)

کابل نوع Thinnet:

Thinnet یک کابل coaxial انعطاف‌پذیر به ضخامت ۰/۲۵ اینچ است.

به خاطر انعطاف و سادگی استفاده، تقریباً در نصب هر نوع شبکه‌ای می‌توان از آن استفاده کرد. این نوع کابل می‌تواند سیگنال را تقریباً ۱۸۵ متر بدون افت سیگنال حمل نماید. کابل thninnet در خانواده‌ای از کابل‌ها به نام RG– ۵۸ قراردارد و امپدانس معادل ۵۰ اهم دارد. امپدانس، مقاومت سیم است که برحسب اهم، اندازه‌گیری شده

است. اختلاف اصلی در کابل‌های خانواده‌ی ۵۸– RG، هسته‌ی کابل است که ممکن است به شکل تک رشته یا چند رشته باشد.

کابل نوع Thicknet:

Thicknet یک کابل coaxial ضخیم به قطر ۰/۵ اینچ است. هرچه هسته‌ی مس ضخیم‌تر باشد، به همان اندازه کابل می‌تواند سیگنال را به فاصله‌ی طولانی‌تر حمل کند. این بدین معناست که کابل‌های Thicknet سیگنال را بیشتر از کابل‌های Thinnet می‌توانند حمل کنند. کابل Thinnet می‌تواند سیگنال را تا ۵۰۰ متر حمل کند. توجه داشته باشید که به این کابل Ethernet هم می‌گویند، چون برای اولین بار در این شبکه استفاده شده است. به دلیل اینکه این کابل می‌تواند در فاصله‌ی دورتر سیگنال را انتقال دهند. معمولاً از آن به عنوان ارتباط‌دهنده‌ی چندین شبکه محلی استفاده می‌کنند. به این موضوع هم توجه داشته باشید که این کابل برای انتقال تصاویر متحرک و صوت در فواصل دور استفاده می‌شود.

انواع connector های که در کابل Coaxial استفاده می‌شوند به صورت زیر می‌باشند.

کارت شبکه‌ای که برای این کابل استفاده می‌شود، مخصوص همین کابل است. به شکل زیر توجه کنید.

برای ارتباط کابل Thinnet به کابل Ticknet از وسیله‌ای به نام Tranciver استفاده می‌شود که شکل آن را مشاهده می‌کنید.

همان‌طور که گفتیم حداکثر طول انتقال سیگنال‌ها توسط این دو نوع کابل coaxial، 185 و 500 متر است و بعد از آن بر روی آن noise تأثیرگذار می‌شود و عملاً کابل از مسیر خارج می‌شود. برای حل این مشکل از وسیله‌ای به نام Repeater استفاده می‌کنند که سیگنال‌ها را تقویت می‌کند و به کابل بعدی می‌فرستد که در زیر، شکل این دستگاه را مشاهده می‌کنید.

کابل Twisted-pair یا زوج به هم تابیده:

در ساده‌ترین شکل، کابل Twisted-pair دارای یک زوج سیم به هم تابیده از مس که دارای روکش است. دو نوع کابل Twisted-pair وجود دارد:

- روکش‌دار یا STP (Shielded Twisted-pair)
- بدون روکش یا UTP(Unshielded Twisted-pair)

این کابل از noise های مزاحم با استفاده از پیچیدگی‌هایی که دارد جلوگیری می‌کند، البته استاندارد ساخت این کابل‌ها برای کارخانه‌ها مهم است. اگر این کابل‌ها به‌درستی تابیده نشوند، به مشکل برمی‌خورند.

کابل روکش‌دار یا (STP)

این نوع کابل به هم تابیده شده، معمولاً توسط غلافی پوشیده می‌شوند تا در برابر امواج الکترومغناطیسی محافظت شوند. از آنجا که این غلاف‌ها فلزی هستند، می‌توانند نقش سیم ارت را نیز ایفا کنند، اما معمولاً این نوع کابل‌ها دارای رشته سیمی به همین منظور هستند که به آن، سیم تخلیه (drain wire) نیز می‌گویند.

کابل کاملاً روکش‌دار یا (Screened Fully shielded Twisted Pair) SSTP:

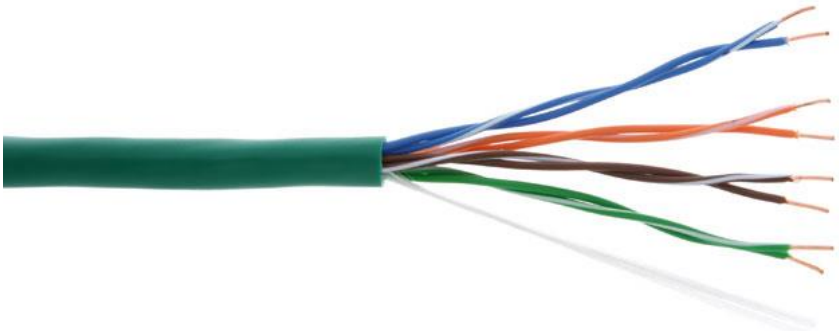
این کابل مانند کابل STP است، به‌طوری‌که به غیر از روکش‌های فلزی روی آن یک روکش فلزی دیگر، کل این روکش‌ها را دربرمی‌گیرد که این کابل را به نسبت قوی‌تر و محکم‌تر در برابر ضربه و امواج الکترومغناطیسی کرده است.

کابل‌های بدون روکش یا (Unshielded Twisted-pair) UTP

معمول‌ترین نوع کابل Twisted-pair نوع بدون روکش آن با مشخصه‌ی 10 Base T است که به‌عنوان یکی از محبوب‌ترین نوع کابل‌کشی برای شبکه‌ی LAN شناخته شد. این کابل‌ها در شبکه‌های امروزی استفاده می‌شود، مثلاً مودم ADSL شما از طریق همین کابل به کارت شبکه‌ی کامپیوتر شما متصل می‌شود.

شما می‌توانید این کابل‌ها را در سیستم‌های تلفن خانگی و اداره‌ی مخابرات مشاهده کنید که تمامی از این نوع کابل‌ها استفاده می‌کنند.

این نوع کابل‌ها، بسیار نازک و انعطاف‌پذیر است و به خاطر کوچک بودنشان برای سیم‌کشی به‌صرفه است، اما در برابر ضربه زیاد دوام ندارد.



کابل‌های UTP از انواع مختلف تشکیل‌شده‌اند، جدول زیر انواع کابل‌های UTP را نشان می‌دهد:

طبقه‌بندی کابل	نوع	پهنای باند	موارد استفاده	توضیحات
Level 1		0.4 MHz	Telephone and modem lines	Not described in EIA/TIA recommendations. Unsuitable for modern systems.
Level 2		4 MHz	Older terminal systems, e.g. IBM 3270	Not described in EIA/TIA recommendations. Unsuitable for modern systems.
Cat3	UTP	16 MHz	10BASE-T and 100BASE-T4 Ethernet	Described in EIA/TIA-568. Unsuitable for speeds above 16 Mbit/s. Now mainly for telephone cables
Cat4	UTP	20 MHz	16 Mbit/sToken Ring	Not commonly used
Cat5	UTP	100 MH	100BASE-TX & 1000BASE-T Ethernet	Common in most current LANs
Cat5e	UTP	100 MHz	100BASE-TX & 1000BASE-T Ethernet	Enhanced Cat5. Same construction as Cat5, but with better testing standards.
Cat6	UTP	250 MHz	10GBASE-T Ethernet	Most commonly installed cable in Finland according to the 2002 standard. SFS-EN 50173-1
Cat6a		500 MHz	10GBASE-T Ethernet	ISO/IEC 11801:2002 Amendment 2.
Class F	S/FTP	600 MHz	Telephone, CCTV, 1000BASE-TX in the same cable. 10GBASE-T Ethernet.	Four pairs, S/FTP (shielded pairs, braid-screened cable). Development complete - ISO/IEC 11801 2nd Ed. Unofficially, Category 7 cable.
Class Fa		1000 MHz	Telephone, CATV, 1000BASE-TX in the same cable. 10GBASE-T Ethernet.	Four pairs, S/FTP (shielded pairs, braid-screened cable). Development complete - ISO/IEC 11801 2nd Ed. Am. 2. Unofficially, Category 7a cable.

کانکتورهای استاندارد برای کابل‌های UTP در شبکه‌های LAN به نام RG45 است که شکل آن را در زیر مشاهده می‌کنید.

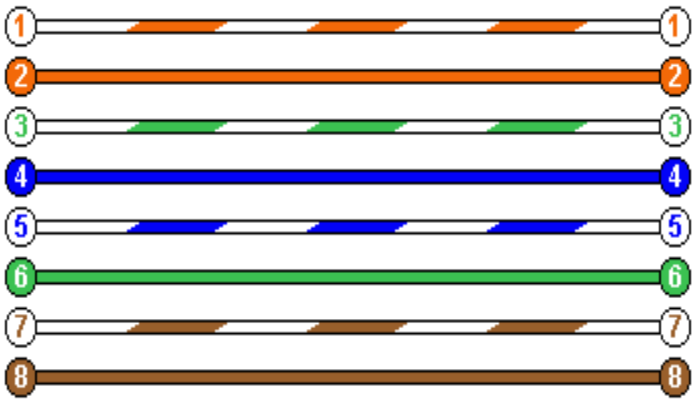
این کابل‌ها از رنگ‌بندی خاصی استفاده می‌کند، این رنگ‌بندی بی‌دلیل نیست. در ادامه به این موضوع پی خواهیم برد.

نحوه‌ی به هم بستن کابل‌ها بر دو نوع است:

- Straight (به صورت مستقیم – برای دستگاه‌های غیرمشابه)
- Cross (برای به هم بستن دستگاه‌های شبیه به هم)

کابل Straight :

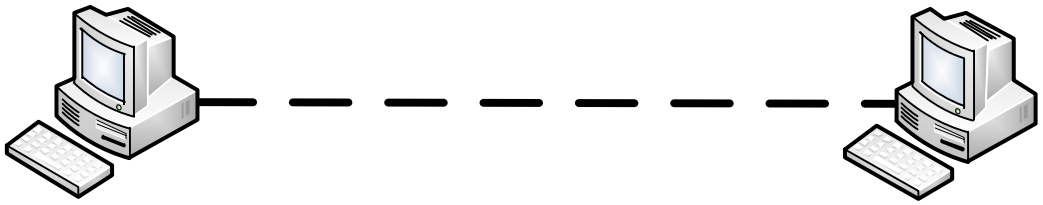
این نوع کابل برای ارتباط دو وسیله‌ی غیرمشابه مانند سوئیچ و کامپیوتر استفاده می‌شود. باید دو سرکابل را به یک صورت ببندیم، یعنی رنگ‌بندی را تغییر ندهیم.

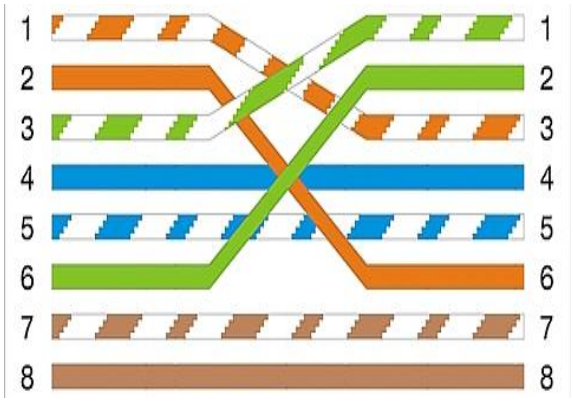
کابل طرف سوئیچ		رنگ‌بندی	کابل طرف کامپیوتر	
سفید نارنجی	(+TD)		(+TD)	سفید نارنجی
نارنجی	(–TD)		(–TD)	نارنجی
سفید سبز	(+RD)		(+RD)	سفید سبز
آبی	(NC)		(NC)	آبی
سفید آبی	(NC)		(NC)	سفید آبی
سبز	(–RD)		(–RD)	سبز
سفید قهوه‌ای	(NC)		(NC)	سفید قهوه‌ای

قهوه‌ای	(NC)		(NC)	قهوه‌ای

کابل Cross:

برای ارتباط 2 دستگاه شبیه به هم مثلاً، ارتباط 2 کامپیوتر باهم قضیه کمی فرق می‌کند. برای این کار باید یک سری تغییرات در یک طرف کابل انجام دهید. به جدول زیر توجه کنید.



کابل طرف کامپیوتر 1		رنگ‌بندی	کابل طرف کامپیوتر 2	
سفید نارنجی	(+TD)		(+TD)	سفید سبز
نارنجی	(–TD)		(–TD)	سبز
سفید سبز	(+RD)		(+RD)	سفید نارنجی
آبی	(NC)		(NC)	آبی
سفید آبی	(NC)		(NC)	سفید آبی
سبز	(–RD)		(–RD)	نارنجی
سفید قهوه‌ای	(NC)		(NC)	سفید قهوه‌ای
قهوه‌ای	(NC)		(NC)	قهوه‌ای

این رنگ‌ها در همه‌ی کابل‌ها ثابت است و یک استاندارد است که همه‌ی کارخانه‌های تولیدی، آن را پیروی می‌کنند.

در جدول زیر نحوه‌ی ارتباط دو دستگاه را از طریق کابل مربوطه مشاهده می‌کنید:

	Hub	Switch	Router	Workstation

Hub	Crossover	Crossover	Straight	Straight
Switch	Crossover	Crossover	Straight	Straight
Router	Straight	Straight	Crossover	Crossover
Workstation	Straight	Straight	Crossover	Crossover

نکته: کامپیوترهایی که از یک برند کارت شبکه استفاده می‌کنند می‌توانند با کابل Straight هم به هم متصل شوند.

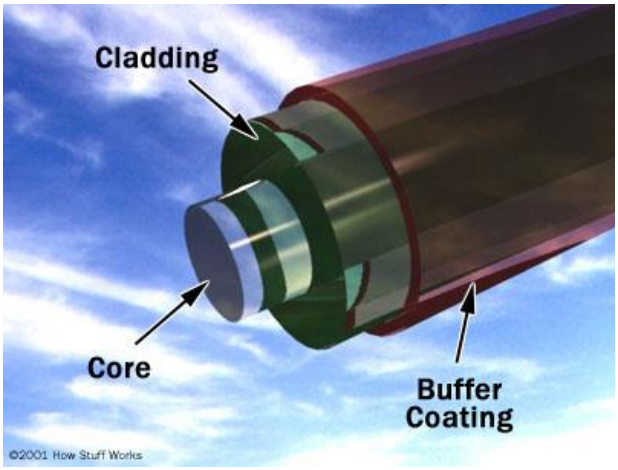
فیبر نوری:

ساختمان فیبر نوری:

فیبرهای نوری تشکیل شده‌اند از یک استوانه‌ی شیشه‌ای بسیار نازک به نام هسته که توسط لایه‌ی ضخیم‌تر از شیشه پوشیده شده است که به این لایه، Cladding می‌گویند.

سرعت انتقال اطلاعات بر روی فیبر نوری، به خاطر استفاده از نور به‌جای سیگنال، خیلی سریع است. فیبرهای نوری فقط یک‌طرفه هستند و امواج را از یک‌طرف ارسال می‌کنند، به همین دلیل در داخل آن از دو مسیر برای انتقال و دریافت استفاده می‌کنند.

یک فیبر نوری از سه بخش متفاوت تشکیل شده است:



هسته (Core): هسته‌ی نازک شیشه‌ای در مرکز فیبر که سیگنال‌های نوری در آن حرکت می‌نمایند.

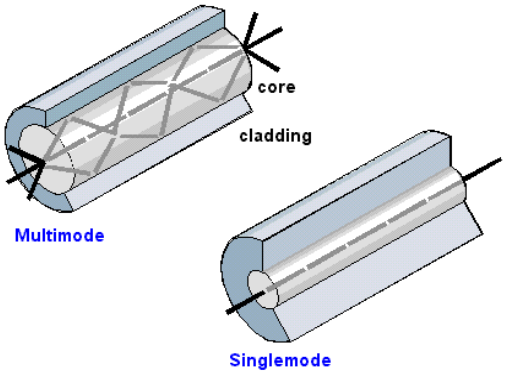
روکش (Cladding): بخش خارجی فیبر بوده که دور تا دور هسته را دربرمی‌گیرد و باعث برگشت نور منعکس‌شده به هسته می‌گردد.

بافر رویه (Buffer Coating): روکش پلاستیکی که باعث حفاظت فیبر در مقابل رطوبت و سایر موارد آسیب‌پذیر است.

فیبرهای نوری در دو گروه عمده ارائه می‌گردند:

1- فیبرهای تک‌حالته (Single-Mode)

2- فیبرهای چندحالته (Multi-Mode)

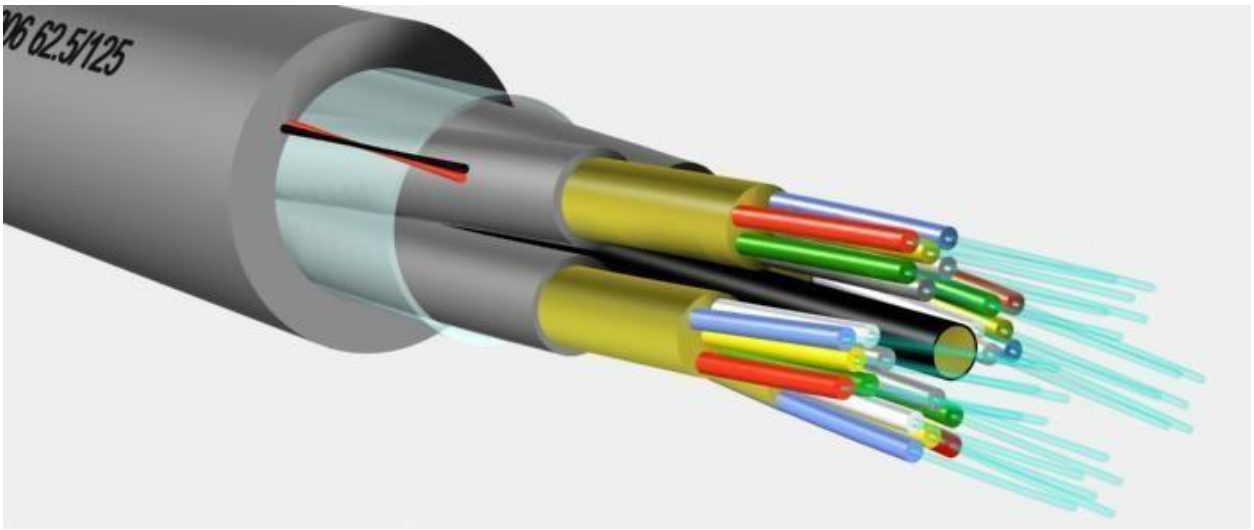


فیبر نوری به سه دسته کلی تقسیم می-شود:

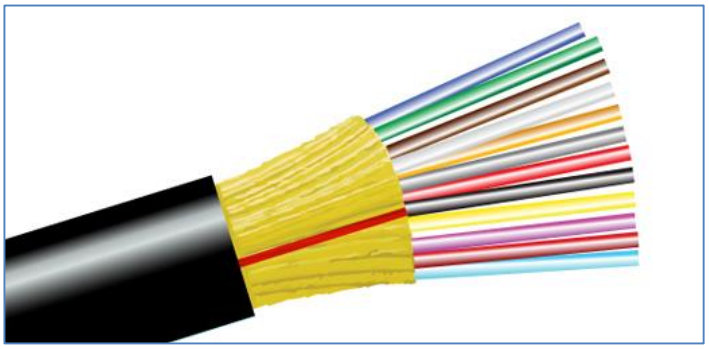
- Breakout
- Distribution
- Interconnect

فیبرهای نوری Breakout:

این کابل امکان خم کردن ندارد و چون از تعداد زیاد فیبر تشکیل شده است، این کابل را برای ارتباط Datacenter ها مناسب کرده است. از این کابل‌ها برای زیر دریاها و زیر خاک استفاده می‌شود، چون مقاومت آن به علت لایه‌های متعدد محافظتی بسیار زیاد است. در زیر، شکل این کابل را مشاهده می‌کنید.



فیبرهای نوری Distribution:



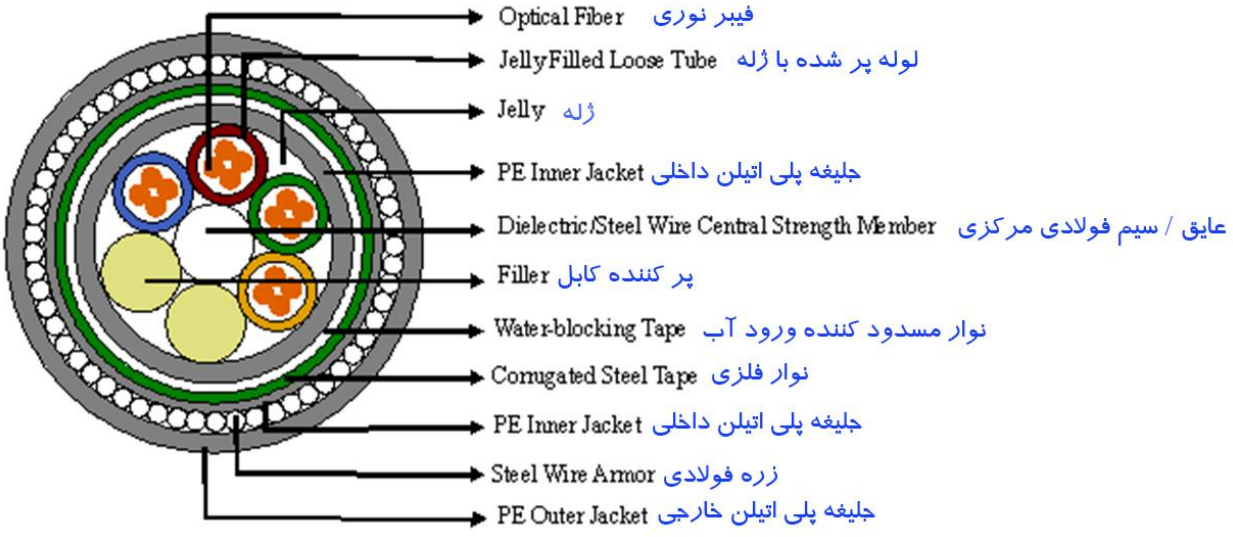
این نوع کابل‌ها به نسبت کابل قبلی کمی خم می-شوند و تعداد رشته‌ها در آن زیاد است و برای ارتباط کابل‌های Backbone با یک rack به کار می‌رود که شکل آن را می‌توانید در زیر مشاهده کنید.

فیبرهای نوری Interconnect:

این نوع کابل که از یک پوشش پلاستیکی استفاده می‌کند، امکان خمش بالایی دارند و عموماً در داخل Rack استفاده می‌شود (Rack تجهیزاتی است که در داخل آن روتر، سوئیچ، فایروال و.... قرار می‌گیرد).

انواع لایه‌ها در فیبر نوری:

فیبرهای نوری در درون خود از چندین لایه تشکیل شده‌اند که هرکدام از آن‌ها، کار خاصی را انجام می‌دهند.



همان‌طور که در شکل صفحه‌ی قبل مشاهده می‌کنید، انواع لایه‌های محافظ در این کابل وجود دارد که البته این کابل برای زیر دریاها و زیر خاک بسیار کاربرد دارد. ماده‌ی ژله‌ای که در این کابل وجود دارد، باعث می‌شود فیبر نوری داخل آن کمی متحرک باشد که اگر کمی خمیده شد، مشکلی برای آن پیش نیاید.

در شکل‌های زیر انواع کانکتورهای فیبر نوری را مشاهده می‌کنید.

کابل Serial:

این کابل‌ها برای ارتباط یک دستگاه، مانند روتر با روتر دیگر به کار می‌رود، که مدل آن RS232 است که فقط برای اتصالات کوتاه که حداکثر 14 یا 15 متر باشد کاربرد دارد، البته برای فواصل طولانی می‌توان از مدل RS485 استفاده کرد.

دو مفهوم کلی برای کابل‌های RS232 وجود دارد.

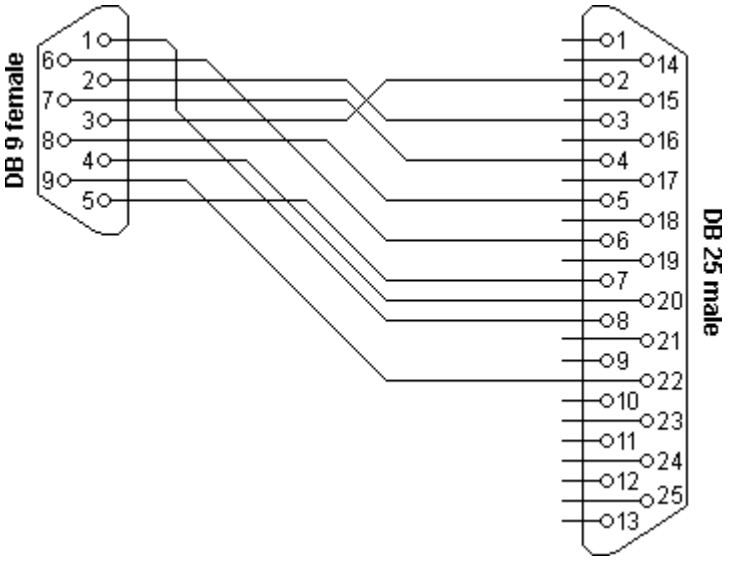
- DTE (Data Terminal Equipment)
- DCE (Data Communications Equipment)

DTE ها از یک کانکتور 9 پین یا 25 پین که به این کانکتور مادگی می‌گویند تشکیل می‌شوند و طرف دیگر DTE هم به همین صورت است که از یک کانکتور 9 پین یا 25 پین استفاده می‌کند که به آن نرگی می‌گویندکه در شکل زیر هر دو پین 9 و 25 را مشاهده می‌کنید.

تفاوت DCE با DTE:

تفاوت این دو در این است که طرف کابلی که DTE است، مربوط به شبکه‌ی خودمان است و طرف دیگر که DCE است مربوط به مخابرات و یا همان Service Provider است که آن‌طرفی که DCE است، باید روی آن سرعت یا همان Clock Rate را تنظیم کند.

در شکل زیر نحوه‌ی بستن کابل‌های 9 پین و 25 پین را مشاهده می‌کنید.



کابل‌های سریال به انواع مختلفی تقسیم می‌شوند که در زیر انواع آن‌ها را مشاهده می‌کنید:

کابل DTE Smart Serial Cables :

این نوع کابل برای ارتباط روترهای DTE استفاده می‌شود.

کابل DCE Smart Serial Cables:

این نوع کابل برای ارتباط روترهای DCE استفاده می‌شود.

کابل E1:

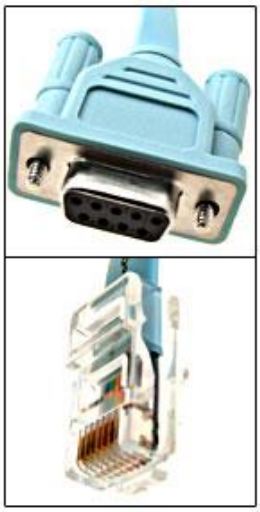
این کابل در شبکه‌های Wan بیشترین کاربرد را دارند.

کابل Stacking Cables:

این نوع کابل‌ها برای ارتباط سوئیچ‌ها با هم مورد استفاده قرار می‌گیرند.

کابل کنسول Console:

این نوع کابل که یک‌طرف آن از کانکتور RG-45 و در طرف دیگر از پورت COM استفاده می‌کند و همیشه هم به رنگ آبی است برای اتصال روتر یا سوئیچ به یک کامپیوتر برای تنظیم کردن روتر است. در درس‌های آینده، نحوه‌ی اتصال کامپیوتر به روتر از طریق این کابل بررسی می‌شود.



کابل Octal:

این کابل که برای اتصال مدارهای چندگانه استفاده می‌شود، از کیفیت بالایی برای انتقال اطلاعات برخوردار است.

دستگاه‌های شبکه

Router:

روترها، دستگاه‌هایی هستند که کار تفکیک شبکه‌ها را انجام می‌دهند و به عنوان یک پل ارتباطی بین دو شبکه مختلف انجام وظیفه می‌کنند. روترها در لایه‌ی 3 مدل osi کار می‌کنند و با IP ها سر و کار دارند و بسته‌های اطلاعاتی را از یک شبکه به شبکه‌ی دیگر حمل می‌کنند، البته این عمل را از طریق پروتکل‌های مسیریابی انجام می‌دهند که در درس‌های آینده به آن‌ها می‌پردازیم.

یکی از مهم‌ترین کاربردهای روترها جلوگیری از Broadcast است. مسیریاب‌ها با استفاده از پروتکل‌های مسیریابی، بهترین مسیر را در شبکه پیدا کرده و از آن مسیر، برای ارتباط با شبکه‌ی دیگر استفاده می‌کنند.

در صحفه‌ی قبل، یک روتر از شرکت سیسکو را مشاهده می‌کنید.

یک مسیریاب شبکه از دو بخش عمده سخت‌افزار و نرم‌افزار تشکیل می‌شود. نرم‌افزار مسیریاب شامل سیستم عامل و رابط کاربری آن است. یک سیستم عامل معروف که شرکت سیسکو در مسیریاب‌های خود استفاده می‌کند، IOS نام دارد.

اجزای زیر را برای یک مسیریاب مرسوم می‌توان نام برد:

- ✓ بدنه (شامل کانکتورها و...)
- ✓ سخت‌افزار مسیریابی
- ✓ رابط‌های شبکه
- ✓ سیستم‌عامل
- ✓ رابط کاربری

تولیدکنندگان معروف روترها و دستگاه‌های شبکه:

- Juniper Networks
- Cisco Systems, Inc
- Lucent Technologies (Alcatel-Lucent）
- MRV Communications
- Mikrotik RouterOS

:Switch

سوئیچ برای اتصال دستگاه‌های مختلف از قبیل رایانه، مسیریاب، چاپگرهای تحت شبکه، دوربین‌های مداربسته و ... در شبکه‌های کابلی مورد استفاده قرار می‌گیرد.

از نظرظاهری، سوئیچ همانند جعبه‌ای است متشکل از چندین درگاه اترنت که از این لحاظ شبیه به هاب (Hub) است، با وجود این‌که هر دوی این‌ها وظیفه‌ی برقراری ارتباط بین دستگاه‌های مختلف را بر عهده دارند، تفاوت از آنجا آغاز می‌شود که هاب، بسته‌های ارسالی از طرف یک دستگاه را به همه‌ی درگاه‌های خود ارسال می‌کند و کلیه‌ی دستگاه‌های دیگر، علاوه بر دستگاه مقصد، این بسته‌ها را دریافت می‌کنند، درحالی‌که در سوئیچ، ارتباطی مستقیم بین درگاه دستگاه مبدأ با درگاه دستگاه مقصد، برقرار شده و بسته‌ها به‌طور مستقیم فقط برای آن ارسال می‌شوند.

این خصوصیت از آنجا می‌آید که سوئیچ می‌تواند بسته‌ها را پردازش کند، در سوئیچ‌های معمولی که به سوئیچ لایه‌ی دوم معروف‌اند، این پردازش تا لایه‌ی دوم مدل OSI پیش می‌رود و نتیجه‌ی این پردازش، جدولی است که در سوئیچ، با خواندن آدرس سخت‌افزاری (MAC) فرستنده‌ی بسته و ثبت درگاه ورودی تشکیل می‌شود.

سوئیچ با رجوع به این جدول، عملیات آدرس‌دهی بسته‌ها در لایه‌ی دوم را انجام می‌دهد، بدین معنا که این جدول مشخص می‌کند بسته‌ی ورودی می‌بایست فقط برای کدام درگاه ارسال شود.

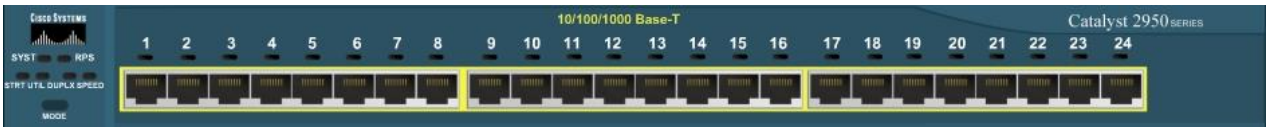
در شبکه‌های بزرگ Switch ها جدول‌های خود را به اشتراک می‌گذارند تا هرکدام بدانند چه دستگاهی به کدام سوئیچ متصل است و با این کار ترافیک کمتری در شبکه ایجاد کنند.

سوئیچ به طور معمول در لایه‌ی دوم مدل OSI کار می‌کند، ولی سوئیچ‌هایی با قابلیت کارکرد در لایه‌های مختلف حتی لایه هفتم هم وجود دارد. پرکاربردترین سوئیچ در بین لایه‌های مختلف به‌جز لایه‌ی دوم می‌توان به سوئیچ لایه‌ی سه اشاره کرد که در بسیاری موارد جایگزین مناسبی برای روتر می‌باشند. از سوئیچ می‌توان در یک شبکه‌ی خانگی کوچک تا شبکه‌های بزرگ با Backbone های چند گیگابایتی استفاده کرد.

برخی مزیت‌های و قابلیت‌های سوئیچ:

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

سوئیچ‌ها در انواع مختلف 8 ، 16 ،24 ،48 پورت وجود دارد. در زیر یک سوئیچ 2950 مشاهده می‌کنید که دارای 24 پورت است.



سوئیچ‌ها در دو نوع لایه‌ی 2 و 3 قرار دارند، سوئیچ‌های لایه‌ی 2 سوئیچ‌های معمولی هستند که در بالا باهم بررسی کردیم، اما سوئیچ‌های لایه‌ی 3 توانایی کار روتر را هم دارند و عملیات روتینگ که در آینده باهم بررسی می‌کنیم را می‌توانند انجام دهند و می‌توان تمام پروتکل‌های Routing را روی این سوئیچ‌ها اجرا کرد. در زیر، سوئیچ 3560 شرکت سیسکو را مشاهده می‌کنید، این سوئیچ یک سوئیچ لایه‌ی 3 است:

Hub:

هاب ازجمله تجهیزات سخت‌افزاری است که از آن به منظور برپاسازی شبکه‌های کامپیوتری استفاده می‌شود. گرچه در اکثر شبکه‌هایی که امروزه ایجاد می‌گردد از سوئیچ در مقابل هاب استفاده می‌گردد، اما ما همچنان شاهد استفاده از این نوع تجهیزات سخت‌افزاری در شبکه‌های متعددی هستیم. در این مطلب، قصد داریم به بررسی هاب و نحوه‌ی عملکرد آن اشاره نماییم. قبل از پرداختن به اصل موضوع لازم است در ابتدا با برخی تعاریف مهم که در ادامه به دفعات به آنان مراجعه خواهیم کرد، بیشتر آشنا شویم.

Domain: تمامی کامپیوترهای عضو یک domain (دامنه)، هر اتفاق و یا رویدادی را که در دامنه اتفاق می‌افتد، مشاهده کرده و یا خواهند شنید.

Collision Domain: در صورت بروز یک تصادف (Collision) بین دو کامپیوتر، سایر کامپیوترهای موجود در domain آن را شنیده و آگاهی‌های لازم در خصوص آن چیزی که اتفاق افتاده است را پیدا خواهند کرد. کامپیوترهای فوق، عضو یک Collision Domain یکسان هستند. تمامی کامپیوترهایی که با استفاده از هاب به یکدیگر متصل می‌شوند، عضو یک Collision Domain یکسان خواهند بود (برخلاف سوئیچ).

Broadcast Domain: در این نوع domain، یک پیام broadcast (یک فریم و یا داده که برای تمامی کامپیوترها ارسال می‌گردد) برای هر یک از کامپیوترهای موجود در domain ارسال می‌گردد. هاب و سوئیچ با موضوع broadcast domain برخورد مناسبی نداشته (ایجاد حوزه‌های مجزا) و در این رابطه، به یک روتر نیاز خواهد بود.

انواع هاب عبارت‌اند از:

هاب کنترل‌پذیر(manageable):

این نوع هاب هوشمند و انعطاف‌پذیر است. بدین معنی که هر یک از درگاه‌های (ports) آن توسط مدیر شبکه از طریق نرم‌افزار می‌توانند فعال یا غیرفعال شوند.

هاب مستقل (stand-alone):

این نوع هاب برای یک گروه از کامپیوترهایی که به طور مجزا از کل شبکه کار می‌کنند، به کار می‌رود.

هاب پیمانه‌ای(modular):

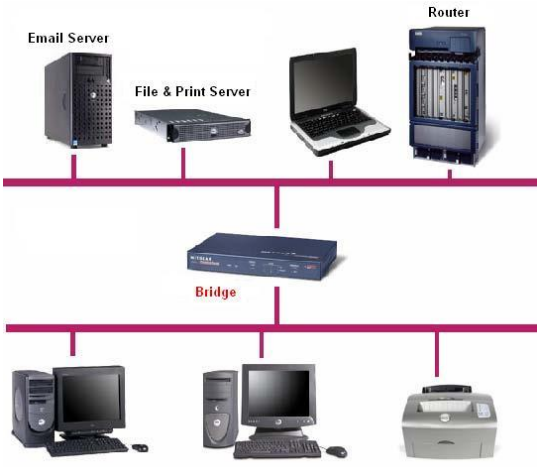
این نوع هاب با یک کارت همراه است و توسط این کارت می‌توان تعداد درگاه‌های آن را افزایش داد.

هاب پشته‌ای (stackable):

این نوع هاب، شبیه هاب مستقل (stand-alone) است. با این تفاوت که تعدادی از آن‌ها را می‌توان مثل یک پشته به یکدیگر متصل کرد تا تعداد پورت‌های کل هاب آن افزایش یابد.

Bridge:

شبیه به سوئیچ است، با این تفاوت که از 2 یا 4 پورت تشکیل شده است و با آدرس Mac مربوط به دستگاه‌ها کار می‌کند و مانند سوئیچ، دارای جدول برای نگهداری Mac address های شبکه است و برای ارتباط با شبکه‌های Bus استفاده می‌شود.



Firewall:

دیوار آتش (برابر فرهنگستان زبان: بارو) تاربارو یا فایروال، نام عمومی برنامه‌هایی است که از دستیابی غیرمجاز به یک سیستم رایانه جلوگیری می‌کند. در برخی از این نرم‌افزارها، برنامه‌ها بدون اخذ مجوز قادر نخواهند بود از یک رایانه برای سایر رایانه‌ها، داده ارسال کنند. به این‌گونه نرم‌افزارها، تاربارو‌ی دوطرفه گویند، زیرا علاوه بر درگاه ورودی (Incoming)، درگاه‌های خروجی (Outing) هم کنترل می‌شوند. بسته‌های اطلاعاتی که حاوی اطلاعات بدون مجوز هستند، به وسیله‌ی تاربارو متوقف می‌شوند. نوع دیگری از فایروال نیز وجود دارد که به آن فایروال معکوس می‌گویند. فایروال معکوس ترافیک خروجی شبکه را فیلتر می‌کند، برخلاف فایروال معمولی که ترافیک ورودی را فیلتر می‌کند. در عمل، فیلتر کردن برای هر دوی این مسیرهای ورودی و خروجی، احتمالاً توسط دستگاه یا نرم‌افزار یکسانی انجام می‌شود.

امکانات:

یکی از کاربردهای معمول فایروال، واگذاری اختیار ویژه به گروهی خاص از کاربران جهت استفاده از یک منبع بوده و همچنین بازداشتن کسانی که از خارج از گروه، خواهان دسترسی به منبع هستند، است. استفاده‌ی دیگر فایروال، جلوگیری از ارتباط مستقیم یک سری از رایانه‌ها با دنیای خارج است. هرچند فایروال بخش مهمی از سیستم امنیتی را تشکیل می‌دهد، ولی طراحان به این نکته نیز توجه می‌کنند که اکثر حملات از درون شبکه می‌آیند و نه از بیرون آن.

نحوه‌ی عملکرد بسیاری از سیستم‌های فایروال این‌گونه است، تمامی ارتباطات از طریق یک سرویس‌دهنده‌ی پروکسی به سمت فایروال، هدایت شده و همین سرویس‌دهنده درباره‌ی امن بودن یا نبودن عبور یک پیام یا یک فایل از طریق شبکه تصمیم‌گیری می‌کند.

این سیستم امنیتی معمولاً ترکیبی از سخت‌افزار و نرم‌افزار است. با توجه به ضرورت‌های استاندارد (ISMS ISO&۲۷۰۰۱) فایروال‌ها جز لاینفک شبکه‌های کامپیوتری قرارگرفته‌اند و یکی از دغدغه‌های اصلی مسئولین شبکه شده‌اند. در این میان، با توجه به حساسیت هر سازمان، لایه‌بندی و قدرت فایروال‌ها در نظر گرفته می‌شود. مثلاً در بانک‌ها به لحاظ اهمیت و ارزش اطلاعات، فایروال‌ها جایگاه حساسی دارند و مسئولین شبکه‌ی بانک‌ها، همواره دقت بسیاری را به خرج می‌دهند. برخی از شرکت‌های بزرگی که در این ارتباط با مهم‌ترین بانک‌های بین‌المللی همکاری دارند، عبارت‌اند از Cisco، Juniper، Securepoint و....

انواع فایروال ها:

سیستم‌های فایروال، معمولاً به سه دسته عمومی تقسیم‌بندی می‌شوند، البته یک سیستم ممکن است ترکیبی از گونه‌های مختلف فایروال را هم‌زمان استفاده کند.

تصفیه کننده‌ی بسته‌های اطلاعاتی (Packets):

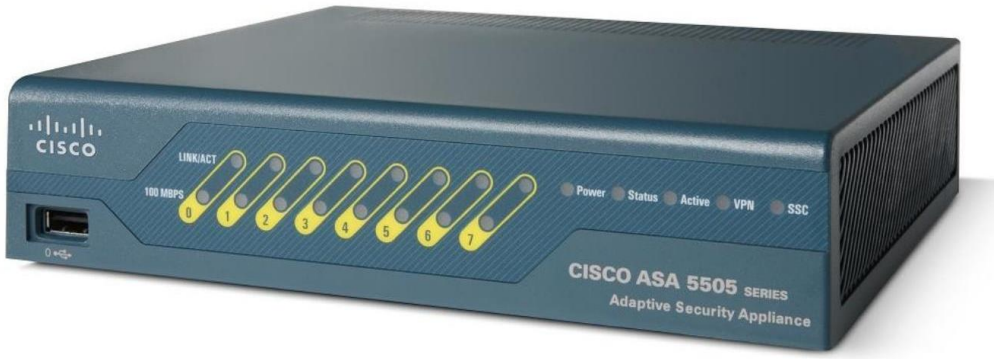
در این‌گونه سیستم‌ها، بسته‌ها بر اساس قانون خاصی متوقف می‌شوند. این قانون می‌تواند بستگی به جهت حرکت بسته، پروتکل خاص استفاده شده، آدرس فرستنده، شماره‌ی پورت پروتکل (مثلاً در TCP/IP)، واسطه‌ی فیزیکی و غیره طراحی شده باشد. این‌گونه فایروال، معمولاً در روتر (Router) انجام می‌شود. به‌عنوان مثال، از Configurable access control lists یا ACLs در روترهای Cisco می‌توان نام برد.

بازرسی کننده‌ی سطوح بالاتر شبکه:

این‌گونه سیستم‌ها، مانند تصفیه‌کننده‌ی بسته‌های اطلاعاتی بوده، با این تفاوت که به دلیل آگاهی از تمامی لایه‌ها و سطوح مختلف در stack پروتکل، هوشمندتر عمل می‌کنند. این‌گونه سیستم‌ها معمولاً حافظه‌دار بوده، اجازه آن را می‌دهند که یک بسته‌ی اطلاعاتی نه به‌صورت مجزا، بلکه به‌عنوان بخشی از جریان داده‌ها نگاه کند.

سرویس‌دهنده‌ی پروکسی:

یک یا چند سیستم که به نظر می‌آید که خدماتی را به خارج می‌دهند، ولی عملاً به عنوان پروکسی برای سیستم اصلی عمل می‌کنند. بنابراین سیستم خارجی مستقیماً به سیستم درونی وصل نشده و پروکسی بین آن‌ها قرار می‌گیرد. پیاده‌سازی آن‌ها می‌توانند در سطح مدار(سخت‌افزار) یا در سطح برنامه‌ی رایانه‌ای (نرم‌افزار) باشد.
در زیر، تصویری از فایروال شرکت سیسکو با نام ASA 5505 را مشاهده می‌کنید.



Wireless Access Point (AP):

نقطه‌ی دسترسی بی‌سیم یا اکسس پوینت بی‌سیم، وسیله‌ای است در یک شبکه رایانه‌ای بی‌سیم که به دستگاه‌های مجهز به ارتباط بی‌سیم نظیر وای- فای، بلوتوث، یا سایر پروتکل‌های مرتبط اجازه می‌دهد تا به عضویت شبکه‌های بی‌سیم درآمده و با سایر دستگاه‌ها و شبکه‌های دیگر ارتباط برقرار کنند. این وسیله را غالباً به یک رهیاب (روتر) متصل می‌کنند و با این کار، ارتباط بین شبکه‌های بی‌سیم و سیمی برقرار می‌شود. این نوع دستگاه‌ها، امروزه از فرکانس‌های رادیویی استانداردی برای دریافت و ارسال داده‌ها پشتیبانی می‌کنند. این استانداردها توسط سازمان IEEE تعیین شده‌اند و غالب نقاط دسترسی بی‌سیم از استاندارد ۸۰۲,۱۱ استفاده می‌کنند.

معرفی سیستم عامل دستگاه‌های شرکت سیسکو با عنوان IOS:

IOS مخفف کلمه‌ی Internetwork operation cisco است که سیستم عامل دستگاه‌هایی مانند روتر و سوئیچ است و کنترل آن از طریق خط فرمان یا همان CLI امکان‌پذیر است. ios هم در این دستگاه‌ها اطلاعات را ذخیره، بازیابی، آدرس‌دهی و ... می‌کند که مانند یک سیستم عامل ویندوز کار می‌کند اما گرافیکی نیست. Ios در انواع مختلفی وجود دارد که در حال حاضر، آخرین ورژن آن IOS 15 است.

راه‌اندازی سخت‌افزار:

روتر از زمانی که روشن می‌شود تا زمانی که آماده به کار می‌شود، از 7 مرحله عبور می‌کند:

1- روشن شدن و چک کردن سخت‌افزارهای خود که به آن مرحله‌ی post هم می‌گویند.

2- بارگذاری فایل boot starp.

3- پیدا کردن مسیر ios که به‌طور پیش‌فرض روی Flash است.

4- فایل ios روی Ram اجرا می‌شود.

5- پیدا کردن تنظیمات ذخیره‌شده.

6- انتقال تنظیمات Startup config از Nvram به Ram.

7- اجرا کردن تنظیمات از روی Ram.

اصولاً روترها از حافظه‌های Rom , Ram , Nvram , Flash تشکیل‌شده‌اند که هرکدام از مراحل بالا با این حافظه‌ها کار می‌کنند.

حافظه‌ی Rom: حافظه‌ای در دل روتر که فقط خواندنی است و قسمت‌های زیر در آن وجود دارد.

- ✓ Boot starp
- ✓ Post
- ✓ Rom Monitor
- ✓ Mini Ios

Boot starp:

این قسمت زمانی که اجرا شود، محل قرارگیری ios را پیدا می‌کند که همان‌طور در مراحل 7 گانه مشاهده می‌کنید، در مرحله‌ی دوم این فایل اجرا می‌شود و محل IOS را پیدا می‌کند.

POST: این مرحله همان مرحله تست سخت‌افزار است که در مرحله 1 برای شما معرفی کردیم.

Rom Monitor:

بیشترین کاربرد این قسمت در Password Recovery است که با تغییر در رجیستری می‌توانیم Password قرار داده‌شده روی روتر را پاک کنیم. این قسمت را در درس‌های بعدی توضیح خواهیم داد.

Mini IOS: این قسمت زمانی اجرا می‌شود که روتر نتواند ios اصلی را پیدا کند.

- **حافظه‌ی Ram:**

یک حافظه‌ی فرّار که با قطع شدن برق، اطلاعات ایجادشده روی آن پاک‌شده و ذخیره نمی‌شوند، از بین مراحل هفت‌گانه همان‌طور که اشاره کردیم در مرحله‌ی 4، IOS بر روی Ram اجرا می‌شود، یعنی اینکه فایل IOS به‌صورت فشرده است که از حالت فشرده، خارج شده و روی Ram قرار می‌گیرد و اجرا می‌شود. کلاً به این حافظه، زیاد اعتماد نداشته باشید و سعی کنید اطلاعات را در یک حافظه‌ی دیگر که در ادامه، راجع به آن بحث خواهیم کرد، کپی کنید.

- **حافظه Flash:**

این حافظه، مانند یک هارد دیسک روی روتر است که یک حافظه‌ی دائمی است و محل قرار گرفتن ios در آن است.

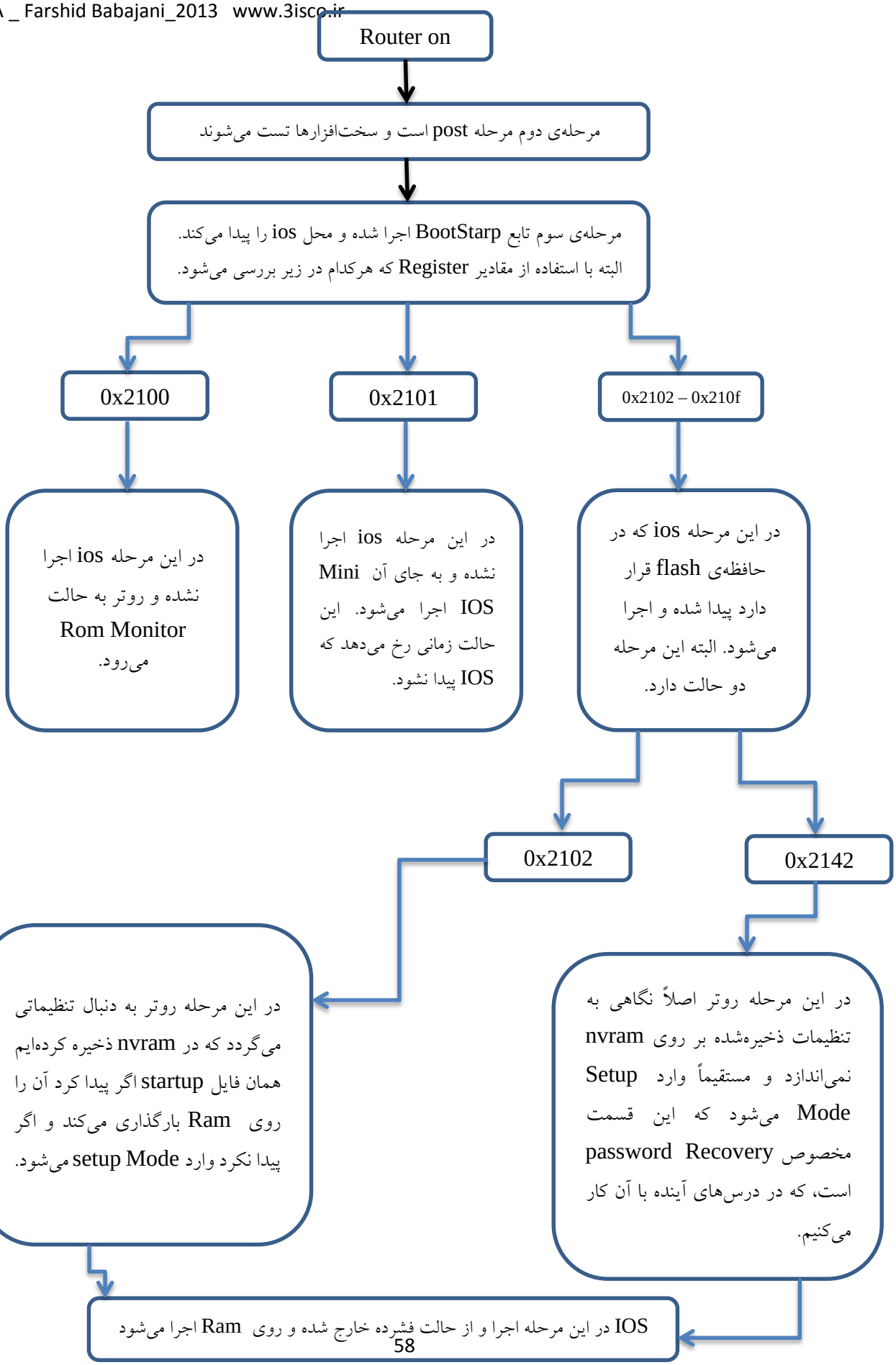
- **حافظه‌ی Nvram:**

حافظه‌ی دائمی روتر برای ذخیره‌سازی تنظیمات روتر در آن است که زمانی که کاری روی روتر انجام دادیم برای ذخیره باید اطلاعات Ram را به Nvram با دستور خاصی کپی کنیم تا با خاموش شدن روتر و یا سوئیچ، تنظیمات از دست نرود که این تنظیمات می‌تواند آدرس یک اینترفیس یا یک پروتکل برای روتر باشد.

تا به اینجا با روشن شدن یک روتر چندین کار انجام شد که باهم بررسی کردیم. روترها در موقع بوت شدن از چندین کد رجیستری استفاده می‌کنند که هرکدام به مفهوم یک مسیر خاص است که باهم این موضوع را بررسی می‌کنیم.

Configuration register: یک سری اعداد که مسیر اجراشدن روتر را تعیین می‌کنند که برای به دست آوردن این اعداد باید در روتر و خط فرمان از دستور Show Version استفاده کنند.

در شکل بعد کاملاً با این مبحث آشنا خواهید شد.



قبل از کار با روترو سوئیچ‌ها و اتصالات آن‌ها ، نرم‌افزار شبیه‌ساز این ادوات را معرفی می‌کنیم و کار با آن را می‌آموزیم .

نصب نرم‌افزار مجازی‌سازی شبکه Packet Tracer 6.0.1 **:**

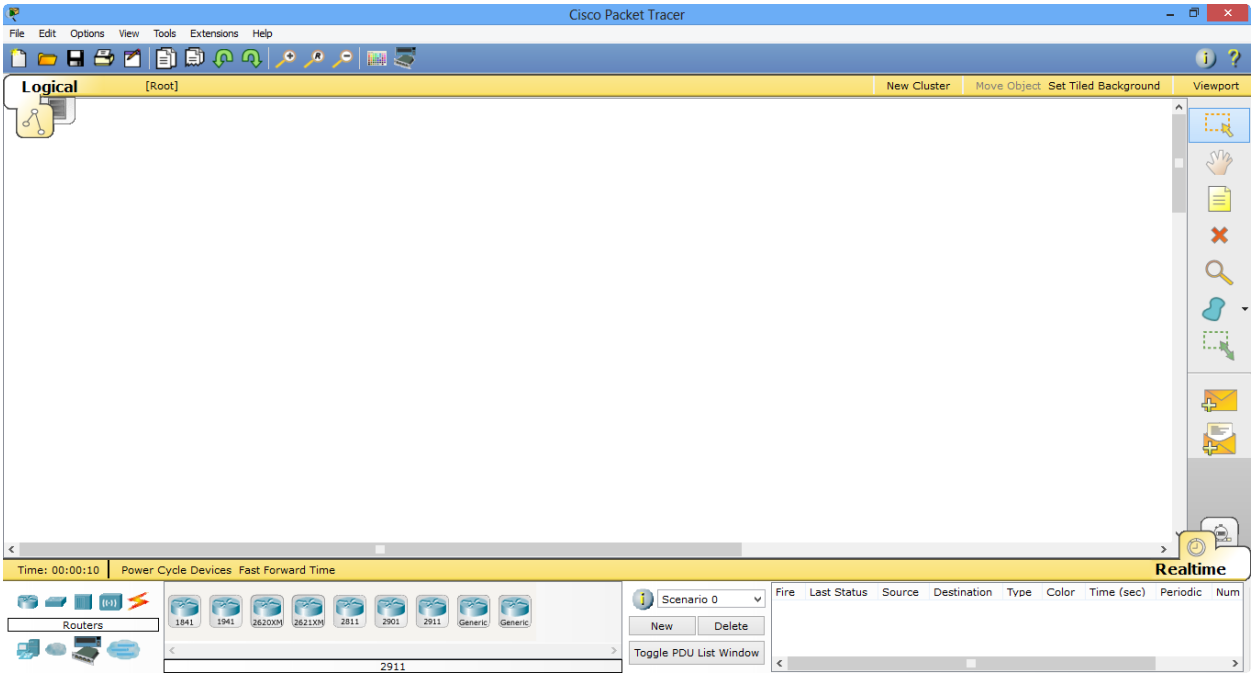
این نرم‌افزار را از لینک زیر دانلود کنید:

http://3isco.ir/post-2792.aspx

این نرم‌افزار یکی از بهترین نرم‌افزارهای مجازی‌سازی برای دوره‌ی CCNA بوده و توسط شرکت سیسکو برای دوره‌های درسی که اجرا می‌کند طراحی و پیاده‌سازی شده است.

نصب این نرم‌افزار به‌راحتی انجام می‌شود، چنانچه در موقع نصب مشکلی برای شما پیش آمد با من در تماس باشید.

بعد از نصب Packet Tracer 6.0.1 آن را اجرا کنید. محیط این نرم‌افزار را در زیر مشاهده می‌کنید.

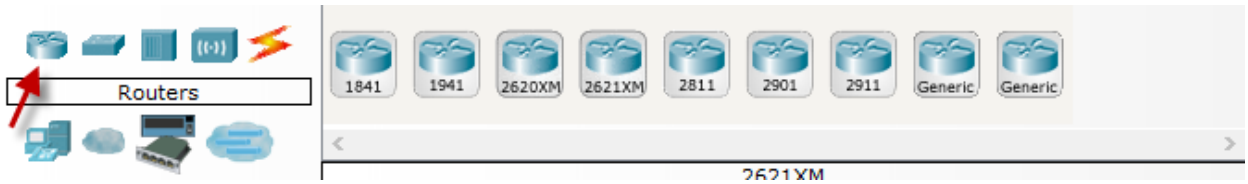


این نرم‌افزار از انواع روترها، سوئیچ‌ها، کابل‌ها، دستگاه‌های بی‌سیم و ... تشکیل شده است که یک دنیای مجازی را برای ما ایجاد می‌کند، البته تمام کارهای این نرم‌افزار در واقعیت هم، به همین صورت است.

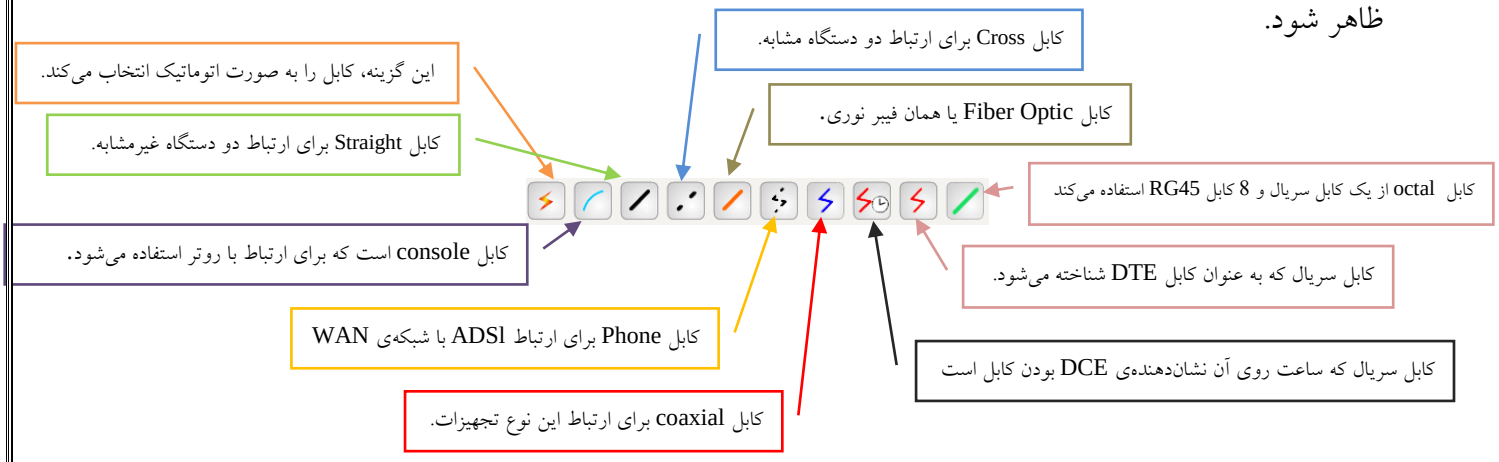
خوب با ابزارهای این نرم‌افزار آشنا می‌شویم.

اگر در سمت چپ، قسمت پایین نرم‌افزار مشاهده فرمایید، تمام ادوات مورد نظر به ترتیب در کنار هم قرارگرفته‌اند که در شکل زیر مشاهده می‌کنید.

برای مشاهده‌ی لیست روترها در سمت چپ مطابق شکل زیر بر روی روتر کلیک کنید تا لیست روترهای این نرم‌افزار را به شما نشان دهد.



همین‌طور می‌توانید بر روی Switch , Hub , Wireless Device , End Device , WAN کلیک کنید و لیست همه‌ی آن‌ها را مشاهده کنید. برای مشاهده لیست کابل‌ها بر روی کلیک کنید تا لیست کابل‌ها مطابق شکل زیر ظاهر شود.

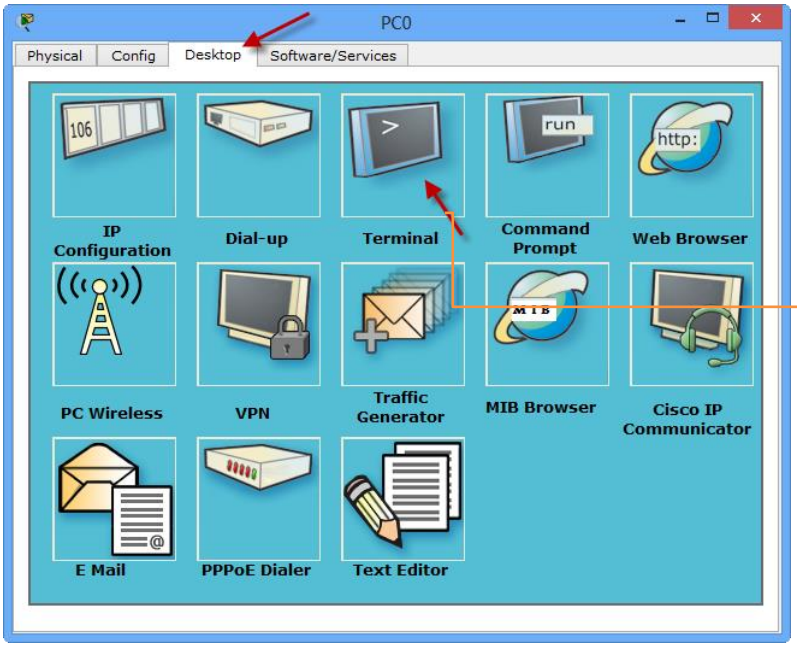


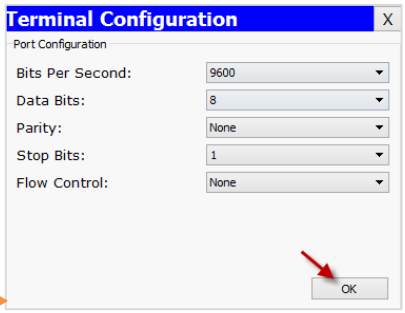
همان‌طور که مشاهده می‌کنید، انواع کابل در این قسمت وجود دارد، البته این کابل‌ها را در درس‌های قبلی توضیح دادیم.

شما وقتی یک روتر را خریداری می‌کنید، هیچ‌گونه تنظیماتی روی آن انجام نشده است. برای تنظیم کردن روتر باید از طریق یک کامپیوتر و یک کابل console به پورت روتر متصل شوید و از طریق نرم‌افزار Terminal برای متصل شدن به روتر اقدام کنیم.

از قسمت پایین نرم‌افزار Packet Tracer ، سمت چپ بر روی روتر کلیک کنید و یک روتر 1841 را انتخاب کنید و به صفحه کار اضافه کنید بعدازاین کار یک کامپیوتر را از قسمت End Device انتخاب و به صفحه اضافه کنید، بعدازآن در قسمت کابل‌ها ، کابل console که آبی‌رنگ است را انتخاب کنید و بعد بر روی کامپیوتر کلیک کنید؛بعد از کلیک دو گزینه به‌صورت منو ظاهر می‌شود که گزینه‌ی اول یعنی، پورت RS232 که یک پورت Com است را انتخاب کنید و بعد بر روی روتر کلیک کنید و پورت console را انتخاب کنید. مانند شکل زیر باید ایجاد شود.

برای وارد شدن به تنظیمات روتر باید از طریق نرم‌افزار Terminal کامپیوتر، این کار را انجام داد، برای این کار بر روی کامپیوتر کلیک کنید تا شکل زیر ظاهر شود و از تب Desktop گزینه Terminal را انتخاب کنید.





در شکل بازشده‌ی بالا، گزینه‌های مورد نظر را که مربوط به سرعت و ... است، دست نزنید و بر روی ok کلیک کنید.

با کلیک بر روی ok وارد ios روتر شده و می‌توانیم تنظیماتی گوناگونی را روی آن انجام دهیم که همه آن‌ها را در درس‌های آینده فرامی‌گیریم.

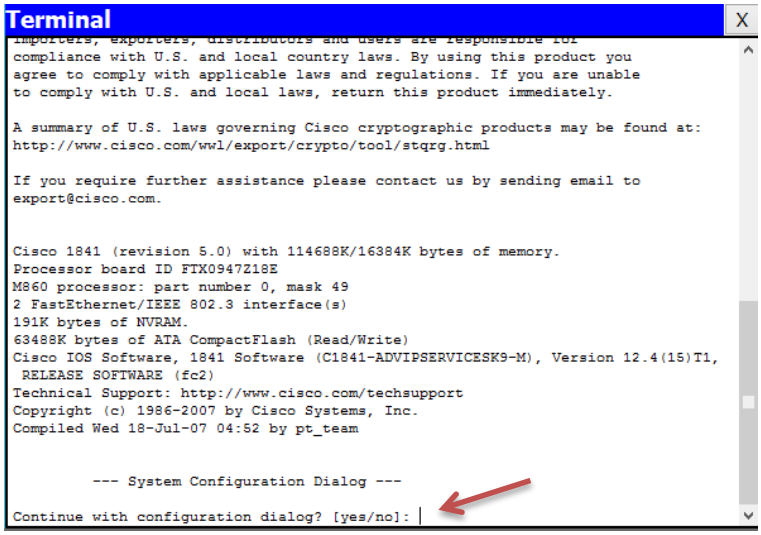
پیکربندی IOS:

برگردیم به درس قبلی که در مورد پیکربندی IOS بود ، در روتر دو نوع پیکربندی وجود دارد:

1- Setup Mode
2- Command Line Interface

:Setup Mode

این قسمت اکثراً زمانی به شما نمایش داده می‌شود که هیچ‌گونه تنظیماتی روی روتر در Nvram ذخیره نشده باشد، مثلاً در قسمت قبل که روتر را از طریق کابل console اجرا کردیم، وارد قسمت Setup Mode شده است .



این مد، به صورت پیش‌فرض سؤالاتی از شما می‌پرسد مثلاً ip address یک پورت را از شما دریافت می‌کند، نام دستگاه را از شما سؤال می‌کند و می‌توانید رمز عبور برای دستگاه خود تعریف کنیدو... که این کارها برای کسانی است که علم کار با روترها را به صورت کامل ندارند و این سؤالات برای راحتی کار آن‌ها است ولی من و شما علم این کار را فرامی‌گیریم پس احتیاجی به Setup Mode نداریم، ولی در ادامه کار آموزش داده می‌شود.

:Command Line Interface

اگر no را وارد کنید و Enter کنید وارد مدCli یا Command Line Interface می‌شوید که این مد، همان مدی است که ما با آن کار می‌کنیم، در این مد امکانات فوق‌العاده‌ای می‌توانیم داشته باشیم و اگر حرفه‌ای شویم که همین‌طور هم می‌شود کارهای زیادی می‌توانید روی روتر خود انجام دهیم که در ادامه به همه‌ی این مسائل پی خواهیم برد.

کار با مدهای CLI در روتر:

Cli از دو مد برای ورود تنظیمات خود استفاده می‌کند.

- ✓ User Mode
- ✓ Privileged Mode

در IOS این مدها برای این تعریف شده‌اند که مثلاً اگر کاربری وارد مد User شود، چقدر توانایی برای کنترل روتر یا سوئیچ دارد و یا اگر وارد مد Privileged شود، چقدر توانایی دارد، که هرکدام را در اینجا مورد بررسی قرار می‌دهیم.

User Mode:

این مد، یکی از پایین‌ترین مدها ازنظر سطح دسترسی کاربران به تنظیمات روتر است، حداکثر کاری که یک کاربر می‌تواند در این مد انجام دهد، انجام Monitoring است و به دلیل دستورات کمی که در این مد اجرا می‌شود، سطح دسترسی آن در پایین‌ترین سطح قرار دارد.

Privileged Mode: این مد به نسبت مد قبلی از دسترسی بالاتری برخوردار است و رتبه‌ی آن کمی بالاتر است، چون در این مد، تنظیمات روتر می‌تواند چک شود.

حالا می‌خواهیم به صورت واقعی این مدها را در روتر تست کنیم. روتر را اجرا کنید و در قسمتی که از شما سؤال می‌کند، No را تایپ و بعد، Enter کنید، اولین خطی که بعدازآن می‌بینید، خط زیر است:

```
Router>
```

این همان قسمت است که به آن User mode میگوییم که سطح دسترسی آن پایین است.

برای رفتن به مد بالاتر، یعنی Privileged Mode از دستور enable استفاده می‌کنیم:

```
Router>enable
Router#
```

همان‌طور که مشاهده می‌کنید با واردکردن دستور enable وارد Privileged Mode شده‌ایم که می‌توانیم در این مد، کارهای مختلفی انجام دهیم، برای خروج از این مد و یا هر مدی از دستور Exit استفاده می‌کنیم:

```
Router#exit
Router>
```

البته در این مد، می‌توانید با دستورات Disable و Logout هم از این مد خارج شویم.

مد Privileged، مد بسیار مهمی است که تنظیمات کامل روتر از طریق این مد و مدهای بعدازآن انجام می‌شود که باید بر روی این مد رمز قرار دهیم تا زمانی که کسی وارد این مد می‌شود از وی رمز درخواست شود.
پس باهم رمزگذاری روی انواع پورت‌های روتر را انجام می‌دهیم.
توجه داشته باشید، راه‌های دسترسی به یک روتر از راه‌های مختلفی امکان‌پذیر است که می‌توانیم بر روی همه این راه‌ها رمز عبور قرار دهیم.
قبل از اینکه وارد رمزگذاری روی روترها شویم ، یک سری مسائل باید بررسی شوند.
در **ios** دو مد دیگر به‌جز مدهای گفته‌شده، وجود دارد و آن‌هم، مدهای Global و Interface است، با وارد شدن به مد Global تمام تنظیمات روتر، مانند رمزگذاری روی پورت‌ها، وارد شدن به مد Interface برای آدرس‌دهی به پورت‌ها، راه‌اندازی انواع پروتکل‌ها و هزاران کار دیگر که در این مد انجام می‌شود را می‌توانیم انجام دهیم.
برای ورود به این مد، اول وارد مد privileged و بعد، با دستور configure terminal وارد این مد می‌شویم:

```
Router>enable
Router#configure terminal
Router(config)#
```

سیسکو از علامت سؤال برای کمک کردن به ما استفاده کرده، مثلاً اگر علامت سؤال را در مد Global وارد کنید، تعداد زیادی دستورات را به ما نشان می‌دهد.

```
Router(config)# ?
Configure commands:
aaa             Authentication, Authorization and Accounting.
access-list     Add an access list entry
banner          Define a login banner
boot            Modify system boot parameters
cdp             Global CDP configuration subcommands
class-map       Configure Class Map
clock           Configure time-of-day clock
config-register Define the configuration register
crypto          Encryption module
do              To run exec commands in config mode
dot11           IEEE 802.11 config commands
enable          Modify enable password parameters
end             Exit from configure mode
exit            Exit from configure mode
hostname        Set system's network name
interface       Select an interface to configure
ip              Global IP configuration subcommands
ipv6            Global IPv6 configuration commands
line            Configure a terminal line
logging         Modify message logging facilities
```

```
login           Enable secure login checking
-- More—
```

در آخر، کلمه‌ی More را مشاهده می‌کنید که به ما می‌گوید، تعداد دستورات در این بخش بیشتر است و اگر بر روی کلید Space روی صفحه‌کلید فشار دهیم، بقیه‌ی دستورات را به ما نشان می‌دهد.

حالا کلمه‌یconf را وارد و بعدازآن، علامت سؤال (؟)وارد کنید:

```
Router#conf?
configure  connect
Router#con
```

همان‌طور که مشاهده می‌کنید با واردکردن علامت سؤال، دو دستور که با حروف conf شروع شده‌اند را به ما نشان می‌دهد، این کار زمانی به کار می‌آید که یک کلمه را به صورت کامل در ذهن ندارید که با این کار، به کلمه‌ی موردنظر خود می‌رسید. در ضمن، شما می‌توانید کلمات را به صورت کوتاه شده هم بنویسید، مثلاً برای نوشتن دستور configuration Terminal می‌توانید از دستور کوتاه شده Conf t استفاده کنید.

```
Router#conf t
Router(config)#
```

زمانی که مقداری کمی از دستور را تایپ کردید و حوصله‌ی نوشتن بقیه‌ی دستورات را ندارید، می‌توانید با زدن کلید TAB روی صفحه‌کلید، بقیه‌ی دستور را کامل کنید، خودتان امتحان کنید.

نحوه‌ی کار با Interface:

ادوات شرکت سیسکو از interface های مختلفی برای ارتباط با دیگر ادوات شبکه استفاده می‌کنند، بستگی به مدل روتر یا سوئیچ از چندین پورت و یا همان Interface تشکیل‌شده‌اند، یک روتر از چندین جای خالی یا همان Slat برای اضافه کردن پورت‌های متفاوت به آن استفاده می‌کند، یعنی اینکه شما می‌توانید پورت‌ها را جداگانه خریداری کرده و به آن اضافه کنید، در ضمن هر Slat روی روتر، یک شماره‌ی اختصاصی دارد. اولین Slat شماره‌ی صفر است؛ وقتی شما یک پورت خریداری می‌کنید و وارد Slat یک می‌کنید شماره‌ی آن در روتر مثلاً می‌شودFastEhternet 1/1 که یک اولی برای شماره Slat و یک دومی برای شماره پورت است.

پورت‌ها انواع مختلفی دارند:

- Ethernet
- FastEthernet
- GigaEthernet
- Serial

پورت‌های Ethernet از سرعت‌های 10 و 100 مگابایت پشتیبانی می‌کنند – پورت‌های Fast Ethernet از سرعت‌های 10 ،100 ، 1000 مگابایت پشتیبانی می‌کنند و پورت Giga Ethernet که پورت جدید با سرعت بسیار زیاد است از سرعت‌های بالاتری پشتیبانی می‌کند.

همان‌طور که در درس‌های قبل در مورد کابل سریال توضیح دادیم، می‌توانیم در ارتباط دو روتر باهم استفاده کنیم که به‌اصطلاح به آن ارتباط Point to Point می‌گویند، می‌توانیم در ارتباط با یک Service Provider هم استفاده کنیم، کابل سریال ویژگی خاصی دارد؛ زمانی که دو روتر می‌خواهند باهم ارتباط برقرار کنند باید از سرعت یکسانی برخوردار باشند، در کابل سریال می‌توانید پهنای باند یا همان BandWidth را تنظیم کنید. کابل‌های سریال از دو ویژگی DTE و DCE برای ارتباط باهم استفاده می‌کنند، یعنی یک سر کابل DCE و سر دیگر DTE است، در طرفی که DCE است باید clock Rate تنظیم شود(Clock Rate سرعت ارتباطی بین دو روتر با استفاده از کابل سریال). حالا چگونه بفهمیم که کدام سر کابل DCE است تا بتوانیم clocke Rate را برای آن تنظیم کنیم، باید از دستور زیر استفاده کنیم:

Router(config)# **show controllers Serial 0/1**

با اجرای این دستور، DCE بودن کابل را به ما نشان می‌دهد (در ادامه به صورت کامل به این موضوع خواهیم پرداخت) و بعد از مشخص شدن DCE بودن کابل، باید Clock Rate را بر روی پورت سریال وارد کنیم، که برای این کار، وارد پورت موردنظر شده و دستور زیر را وارد می‌کنیم:

Router(config)# Clock Rate 64000

در این قسمت، عدد موردنظر را 64000 وارد کردیم که شما می‌توانید اعداد دیگری را هم وارد کنید. برای مشخص کردن این اعداد بعد از clock Rate، یک علامت سؤال قرار دهید تا اعداد مشخص شود.

همان‌طور که گفتیم، یکی دیگر از ویژگی‌های کابل سریال، BandWidth و یا پهنای باند آن است که در انتخاب مسیر برای Routing Protocol ها استفاده می‌شود که این مبحث را در درس‌های بعدی می‌آموزید، برای تغییر BandWidth باید وارد پورت سریال شده و از دستور زیر استفاده کرد:

Router(Config)#Bandwidth 128

:SubInterface

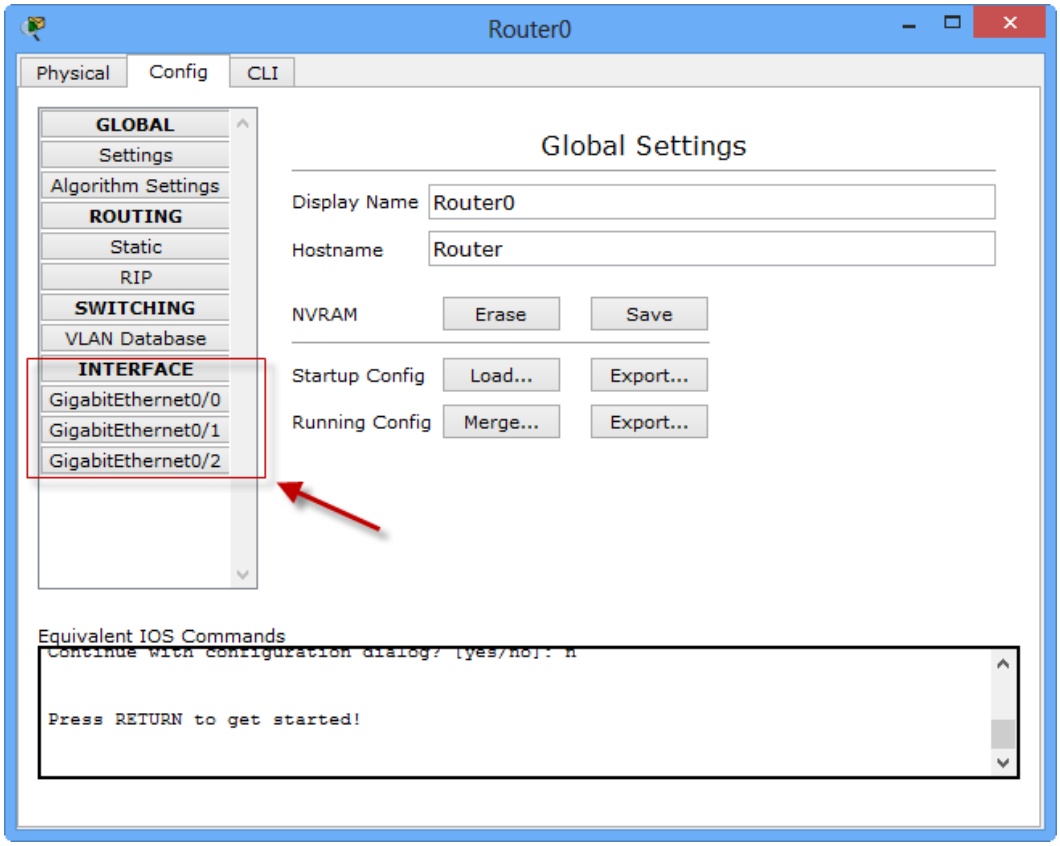
این پورت‌ها، پورت‌های مجازی می‌باشند که روی هر پورت فیزیکی قرار دارند و به صورت 0/0.? هستند.

Router(config)#**interface gigabitEthernet 0/0.?**
<0-4294967295> GigabitEthernet interface number

همان‌طور که مشاهده می‌کنید بعد از شماره پورت یک نقطه قرار دادم و بعدازآن یک علامت سؤال قرارگرفته که تعداد پورت‌های مجازی را 4294967295 نشان می‌دهد که واقعاً زیاد است. مانند زیر عمل کنید:

Router(config)#interface gigabitEthernet 0/0.125

در packet tracer یک روتر 2911 را به صفحه اضافه کنید. بعد بر روی آن کلیک کنید، طبق شکل با رفتن به تب Config می‌توانید interface های مختلف آن را مشاهده کنید:



روی هرکدام که کلیک کنید، می‌توانید آن را خاموش یا روشن و یا آدرس‌دهی کنید که در ادامه با آن کار می‌کنیم.

برای کار با Interface ها به CLI رفته و در مد Privileged دستور زیر را وارد می‌کنیم تا لیست Interface های روی روتر را مشاهده کنید.

Router#**show ip interface brief**

همان‌طور که مشاهده می‌کنید، لیست Interfaceهای مختلف را به ما نشان می‌دهد.

خوب حالا می‌خواهیم یکی از این Interface ها را آدرس‌دهی کنیم، برای این کار باید وارد این Interface ها شویم، کارهای زیر را انجام می‌دهیم:

```
Router#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol

GigabitEthernet0/0     unassigned      YES unset  administratively down down
GigabitEthernet0/1     unassigned      YES unset  administratively down down
GigabitEthernet0/2     unassigned      YES unset  administratively down down
Vlan1                  unassigned      YES unset  administratively down
```

همان‌طور که مشاهده می‌کنید با واردکردن دستور show ip interface brief لیست interface ها را برای شما نمایش داده است، بعد با دستور زیر وارد interface موردنظر می‌شویم:

Router(config)#**Interface ?**

بعد از نوشتن دستور Interface، یک علامت سؤال قرار دهید تا انواع interface ها را به شما نشان دهد. اگر در قسمت قبل، متوجه شده باشید اینترفیس‌های ما از نوع GigaEthernet است، پس ادامه‌ی دستور به این صورت می‌شود:

Router(config)#**interface gigabitEthernet 0/0**

با این دستور وارد GigaEthernet 0/0 می‌شویم و می‌توانید کارهای مختلف روی پورت انجام دهیم، می‌خواهیم به این پورت IP address بدهیم برای این کار از دستور زیر استفاده می‌کنیم:

Router(config-if)#**ip address 192.168.1.1 255.255.255.0**

بعد از IP address باید ip مربوط به این interface را وارد کنیم که در اینجا 192.168.1.1 وارد می‌کنیم بعد، باید Subnet Mask را وارد کنیم که 255.255.255.0 را وارد می‌کنیم، این آدرس، به این Interface داده شد و بعدازاین کار، باید Interface مورد نظر را روشن کنیم. توجه داشته باشد که همه‌ی Interface های روی روتر به صورت پیش‌فرض، خاموش (ShutDown) می‌باشند و باید به صورت دستی روشن شوند، برای این کار از دستور زیر استفاده می‌کنیم:

Router(config-if)#**no shutdown**

با این دستور، پورت موردنظر روشن می‌شود و برای خاموش کردن آن از دستور shutdown استفاده می‌کنیم.

با دستور Show Protocols لیست interface های روتر و فعال و غیرفعال بودن آن‌ها را به ما نشان می‌دهد.

Router#**show protocols**
Global values:
  Internet Protocol routing is enabled
GigabitEthernet0/0 is administratively down, line protocol is down
GigabitEthernet0/1 is administratively down, line protocol is down
GigabitEthernet0/2 is administratively down, line protocol is down
Vlan1 is administratively down, line protocol is down

روش‌های دسترسی و رمزگذاری:

برای دسترسی به روتر چندین روش وجود دارد که هرکدام را مورد بررسی قرار می‌دهیم:

1– پورت console:

این همان پورتی است که از طریق کابل Console به روتر متصل شدیم و برای متصل شدن به یک روتر خام است که هیچ‌گونه تنظیماتی روی آن انجام نشده است، برای رمزنگاری این پورت، باید کارهای زیر را انجام دهیم.

وارد مد global شوید و با دستور Line console 0، وارد پورت کنسول شوید. مانند زیر عمل کنید:

```
Router(config)#line consol 0
Router(config-line)#
```

اصولاً روی روترها، یک پورت کنسول وجود دارد که شماره‌ی آن صفر است.

در این قسمت می‌خواهیم روی این پورت رمز قرار دهیم، باید کارهای زیر را انجام دهیم:

```
Router(config-line)# password 123
```

برای این کار، از دستور Password و بعدازآن، از یک کلمه‌ی عبور، مانند 123 استفاده می‌کنیم که شما می‌توانید به جای این کلمه‌ی عبور (123)، کلمه‌ی عبور دلخواهی را وارد کنید.

بعدازاین که رمز را وارد و enter کردیم باید از دستور login استفاده کنیم تا زمانی که می‌خواهیم وارد تنظیمات روتر شویم از ما رمز عبور پرسیده شود، پس به این صورت این دستور را وارد می‌کنیم:

```
Router(config-line)# Login
```

اگر شما دستور Login را وارد نکنید، هر رمزی را هم روی روتر فعال کنید، باز برای ورود از شما رمز عبور درخواست نمی‌شود، پس به این نکته توجه کنید.

در حال حاضر با واردکردن این دستورات، روی روتر رمز قرار دادیم و زمانی‌که می‌خواهیم از طریق کابل Console وارد User Mode شویم، از شما رمز درخواست می‌شود که در ادامه، نحوه‌ی رمزنگاری پیشرفته‌تر را باهم فرامی‌گیریم، به دلیل اینکه این نوع رمزها، TEXT Base بوده و قابل‌شناسایی و هک شدن می‌باشند.

دستورات دیگری در این پورت وجود دارد که باهم مورد بررسی قرار می‌دهیم:

دستور exec-timeout:

زمانی‌که وارد یک مد می‌شوید، اگر مدت‌زمانی با روتر کار نکنید، در هر مدی که هستید، خارج شده و به مد اول، یعنی UserMode برگشت می‌کند، برای جلوگیری از این کار، باید از دستور زیر در پورت consol استفاده کنید:

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

همان‌طور که مشاهده می‌کنید، در این دستور از دو صفر استفاده شده است که اولی برای دقیقه و دومی برای ثانیه است، با صفر کردن هر دو اگر در هر مدی باشید در همان مد ثابت خواهد ماند و خارج نمی‌شود، البته می‌توانید هر زمان که خودتان دوست دارید وارد کنید.

دستور logging synchronous:

زمانی در حال تایپ کردن دستورات هستید، روتر به صورت خودکار یک سری اطلاعات را به شما نمایش می‌دهد، مانند فعال شدن یک پورت و یا اجرا شدن یک پروتکل و... که این کار باعث می‌شود دستوراتی که در حال نوشتن هستیم برای آن‌ها مشکلی ایجاد شود و جا به جا شوند. برای جلوگیری از این کار در پورت Console از دستور زیر استفاده کنید:

Router(config-line)#**logging synchronous**

2- Enable Password:

این رمز برای Privileged Mode است. اگر کاربری بخواهد وارد این مد شود از وی پسورد درخواست می‌شود. برای فعال کردن آن، وارد مد Global می‌شویم و دستور زیر را تایپ و بعد enter می‌کنیم.

Router(config)#**enable password 123**

با این دستور، رمز عبور بر روی مد Privileged فعال می‌شود و زمانی که بخواهیم وارد این مد شویم از شما رمز عبور درخواست می‌شود که در زیر مشاهده می‌کنید.

User Access Verification

password:

Router>enable
Password:
Router#

توجه داشته باشید در موقع واردکردن رمز عبور، رمز عبور به شما نمایش داده نمی‌شود.

رمزهای عبوری که با دستور Enable Password فعال می‌شوند، زیاد نمی‌توانند امن باشند، چون این رمزها به صورت Text Base بوده و با یک فرمان می‌توانید رمز عبور را به دست آورید. برای دیدن رمز عبور از دستور Show Runing-config استفاده کنید، دستور show برای نمایش اطلاعات به کار برده می‌شود، که با این دستور در درس‌های آینده زیاد کار خواهیم کرد، این دستور در مدهای UserMode و Priviliged Mode کار می‌کند، البته در مد Global هم کار می‌کند که در درس‌های بعدی به آن می‌پردازیم، دستور بعدی که بعد از دستور show

به کار بردیم Running-Config است. این دستور اطلاعات حاضر در Ram را به ما نشان می‌دهد، یعنی اینکه هر تنظیماتی که روی روتر انجام شده، در این قسمت قرار دارد. می‌خواهیم با این دستور به شما نشان دهیم که دستور Enable Password زیاد هم امن نیست، این دستور را در مد Privileged وارد کنید.

```
Router#show running-config
Building configuration...

Current configuration : 648 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Router
!
!
!
enable password 123
!
!
!
!
!
!
!
!
!
 --More--
```

همان‌طور که مشاهده می‌کنید با واردکردن دستور Show Running-config، رمز عبور واردشده، نمایش داده شد، پس باید کاری کرد که این رمز به صورت Hashing یا کد شده در این قسمت نمایش داده شود تا کسی نتواند این رمز را مشاهده کند، مانند قبل وارد مد global شوید و کارهای زیر را انجام دهید:

اول از همه، رمز قبلی را که وارد کردیم، حذف می‌کنیم. برای حذف هر دستوری که وارد کردیم، باید قبل از آن دستور، از کلمه‌ی No استفاده کنیم تا دستور مورد نظر حذف شود، برای این کار از دستور No enable password استفاده می‌کنیم، بعد از این کار، از دستور enable Secret 123 استفاده می‌کنیم که رمز عبور را به صورت کد شده درمی‌آورد و برای شما نمایش می‌دهد، بعد از این کار در مد Privileged دستور show Running-config را اجرا کنید، متوجه می‌شوید که رمز عبور 123 به صورت کد شده درآمده، مانند رمز زیر:

```
enable secret 5 $1$mERr$3HhIgMGBA/9qNmgzccuxv0
```

زمانی‌که Enable Secret فعال است، Enabel Password روی روتر کاربردی ندارد و اگر هر دو دستور را در یک‌زمان فعال کنید، فقط رمز عبوری که با دستور Enable Secret فعال کردیم، جواب می‌دهد .

3- پورت AUX:

این پورت برای ارتباط از راه دور از طریق خط تلفن با روتر استفاده می‌شود که می‌توانیم به روش زیر فعال کنیم:

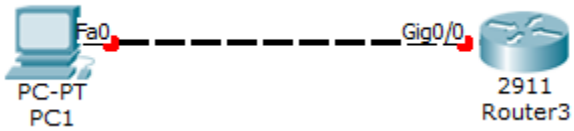
```
Router(config)#Line aux 0
Router(config-line)#password 123
Router(config-line)#login
```

این رمز عبور قبل از وارد شدن به User Mode پرسیده می‌شود.

4 –Telnet:

Telnet یکی از راه‌های محبوب برای ورود به روتر از راه دور است، که برای فعال کردن آن باید کارهای مختلفی انجام بگیرد، این کار را با مثالی کامل انجام می‌دهیم تا متوجه کار آن شویم.

یک روتر 2911 و یک pc به صفحه اضافه کنید و بعد با کابل Cross پورت Fast Ethernet 0 کامپیوتر را به پورت GigaEthernet0/0 متصل کنید، مانند شکل زیر:



خوب، بعد از این کار بر روی روتر کلیک کنید تا صفحه‌ی موردنظر باز شود وارد مد Global شوید و بعدازآن با دستور زیر پورت GigaEthernet را آدرس‌دهی می‌کنیم.

```
Router(config)#interface gigabitEthernet 0/0
Router(config-if)#ip address 192.168.1.1 255.255.255.0
Router(config-if)#no shutdown
```

با دستور interface gigabitEthernet 0/0 وارد interface مورد نظر شده‌ایم، بعد یک ip آدرس به این پورت نسبت داده‌ایم و بعد از این کار پورت موردنظر را با دستور **no shutdown** روشن کرده‌ایم.

پورت موردنظر را آدرس‌دهی و روشن کرده‌ایم، بعد از این کار باید Telnet را فعال کنیم تا بتوانیم از راه دور با استفاده از آدرسی که دادیم به روتر متصل شویم.

برای فعال کردن Telnet باید پورت‌های مجازی Vty را فعال کنیم. Vty مخفف Virtual terminal که از چندین پورت مجازی برای ورود به روتر استفاده می‌کند، مثلاً در روتر 2911 که ما در حال کار با آن هستیم از 15 پورت تشکیل شده است. برای مشاهده این پورت‌ها در مد Global دستور زیر را وارد کنید:

```
Router(config)#line vty ?
<0-15>  First Line number
```

با واردکردن دستور Line Vty و بعدازآن، علامت سؤال به ما تعداد پورت‌های مجازی برای این روتر را نشان می‌دهد که 15 عدد است. شما می‌توانید تمام این 15 پورت را فعال کنید که با این کار 15 نفر در یک‌زمان می‌توانند وارد روتر یا سوئیچ شوند.

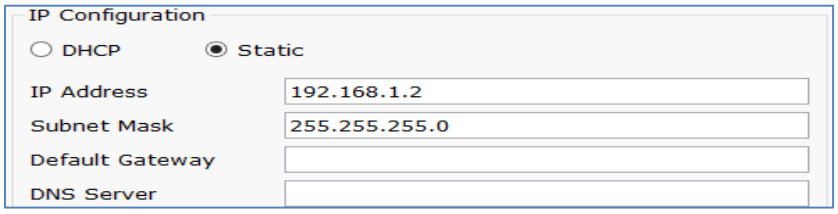
در اینجا تمام این 15 پورت را انتخاب و همه‌ی آن‌ها را فعال می‌کنیم، و روی همه آن‌ها رمز قرار می‌دهیم:

```
Router(config)#line vty 0  15
Router(config-line)#pass 123
Router(config-line)#login
Router(config-line)#
```

تعجب نکنید که به جای نوشتن Password از pass استفاده کردیم، چون همان‌طور که گفتیم در IOS می‌توانیم فرمان‌ها را به صورت کوتاه شده بنویسیم.

در قسمت سوم از دستور Login استفاده کردیم که با این دستور به روتر اعلام می‌کنیم که در زمان Telnet رمز عبور را درخواست کن. اگر به جای Login از دستور No Login استفاده کنید، روتر هیچ‌گونه رمزی درخواست نخواهد کرد، پس مواظب این دستور باشید. شما می‌توانید به چند پورت اجازه دسترسی بدهید و به بقیه‌ی پورت‌ها اجازه دسترسی ندهید.

همه‌چیز آماده است برای Telnet کردن، بر روی Pc کلیک کنید و وارد Ip configuration شوید و یک IP در رنج ip که در روتر وارد کردیم را وارد کنید که 192.168.1.2 را وارد می‌کنیم، مانند شکل زیر:



خوب، بعد بر روی Command Promt کلیک کنید و دستور زیر را وارد کنید.

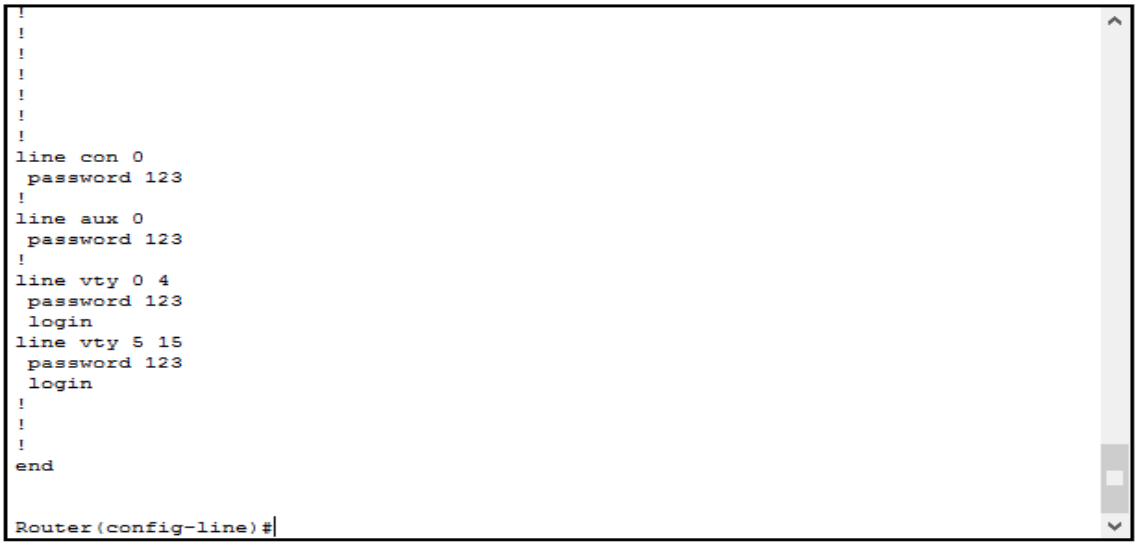
```
Telnet 192.168.1.1
```

Telnet که نام دستور است و این IP هم، آدرس روتری است که ما می‌خواهیم به آن متصل شویم.

بعد از enter، به روتر موردنظر متصل شده و از شما درخواست رمز عبور می‌شود.

می‌توانیم در روتر با دستور show Session، تمام ارتباطات انجام‌گرفته و در حال انجام را مشاهده کنید.

شما اگر یک بار دیگر دستور show Running-config را اجرا کنید، متوجه می‌شوید که تمام رمزهایی را که برای پورت‌های console، AUX و VTY وارد کرده‌ایم در این دستور قابل مشاهده است. به شکل زیر توجه کنید:



برای این‌که این رمزها یا هر رمزی که داخل IOS وارد می‌کنید، به صورت کد شده (Hash) تبدیل شود از دستور زیر در مد Global استفاده می‌کنیم.

Router(config)# **service password-encryption**

بعد از واردکردن این دستورف تمام رمزها به صورت Hash شده یا کد شده درمی‌آید. به شکل زیر توجه کنید:

همان‌طور که در شکل مشاهده می‌کنید، تمام رمزها به صورت Hash شده درآمده، البته این روش به صورت کامل، روتر را در برابر نفوذ امن نگه نمی‌دارد، اما از قدیم گفته‌اند: «لنگه‌کفشی در بیابان نعمت است».

نکته: شما شاید دیده باشید که زمانی در روتر یک دستور را اشتباه وارد می‌کنید روتر به جستجوی آن دستور می‌پردازد، در زیر جمله rn را که کاربردی در روتر ندارد وارد کردیم، اما روتر چنین دستوری ندارد و برای پیدا کردن آن به جستجو می‌پردازد و همین باعث اتلاف وقت می‌شود.

Router>**rn**

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

% Unknown command or computer name, or unable to find computer address

برای جلوگیری از این موضوع وارد مد Global شده و دستور زیر را وارد کنید:

Router(config)#**no ip domain-lookup**

با این دستور، روتر دیگر به جستجوی دستورات نمی‌پردازد.

تا اینجا رمز عبور را برای پورت‌ها و مسیرهای مختلف فعال کردیم و نحوه‌ی کد (Hash)کردن آن‌ها را هم یاد گرفتیم، حالا اگر روتر را خاموش کنیم، آیا این تنظیمات روی روتر باقی خواهد ماند؟

به‌هیچ‌وجه این تنظیمات روی روتر باقی نمی‌ماند، چون تمام این اطلاعات در فایلی به نام Running-Config روی Ram قرار دارد و چون Ram حافظه‌ای فرار است، این اطلاعات بعد از خاموش کردن از بین می‌رود، برای حل این مشکل باید این اطلاعات را به یک حافظه غیرموقت ارسال کنیم تا اطلاعات از بین نرود.

برای ذخیره کردن اطلاعات دو راه وجود دارد:

- Nvram
- TFTP Server

1- برای ذخیره اطلاعات به حافظه‌ی Nvram، از دستور زیر در مد Privileged استفاده می‌کنیم.

```
Router#copy running-config startup-config
Destination filename [startup-config]?
Building configuration…
[OK]
Router#
```

همان‌طور که گفتیم running-config، فایلی است که روی Ram قرار دارد و Startup-config فایل است که بر روی nvram قرار دارد و با این دستور اطلاعاتی که درون فایل running-config است وارد startup-config می‌شود.

در قسمت بعدی از شما نام فایل مقصد را می‌پرسد که چیزی وارد نکنید و بعد Enter را زده تا اطلاعات ذخیره شود و حالا اگر روتر را خاموش و بعد روشن کنید اطلاعات آن از بین نمی‌رود.

حذف کردن اطلاعات Nvram:

برای حذف اطلاعات موجود در حافظه‌ی Nvram، باید دستور زیر را در مد Privileged وارد کنید:

```
Router# erase startup-config
```

بعد از Enter کردن به شما اخطار می‌دهد که آیا مطمئن به پاک کردن اطلاعات موجود در Nvram هستید؟

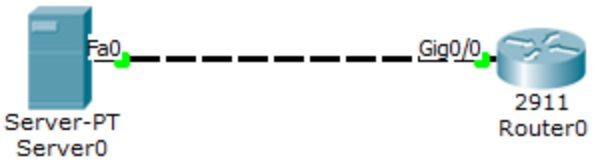
```
Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]
```

اگر enter کنید، کل اطلاعات موجود در Nvram از بین خواهد رفت. فایل startup-config مربوط به حافظه‌ی Nvram است.

2- TFTP Server:

در روش دوم اطلاعات از روتر به یک سرور خارجی منتقل می‌شود و دوباره می‌توان این اطلاعات را از سرور وارد روتر کرد، این کار را باهم انجام می‌دهیم، یک روتر و یک سرور 

را به لیست اضافه کنید و بعد با کابل Cross این دو را به هم متصل کنید، مانند شکل زیر:



بعد مانند روش‌های قبلی به Interface های روتر و سرور آدرس 192.168.1.1 برای روتر و آدرس 192.168.1.2 برای سرور نسبت دهید، بعد وارد روتر شوید و در مد Privileged دستور زیر را وارد کنید:

Router#**copy running-config tftp:**

بعد از واردکردن این دستور از شما آدرس سرور درخواست می‌شود که شما باید آدرس سرور که 192.168.1.2 است را وارد کنید و بعد از Enter، باید نام فایل مقصد را وارد کنید، مانند دستور زیر:

Address or name of remote host []? 192.168.1.2
Destination filename [Router-confg]? Babajani_Router

با انجام این دستورات اطلاعات از روتر به یک سرور خارجی انتقال داده می‌شود.

کار با Setup Mode:

همان‌طور که قبلاً گفتیم وقتی روتر را برای اولین بار روشن می‌کنیم، هیچ‌گونه تنظیماتی روی آن قرار ندارد، وارد Setup Mode می‌شویم که با واردکردن YES وارد این مد می‌شویم و از شما سؤالاتی می‌پرسد. خوب می‌خواهیم سؤالات این بخش را باهم مورد بررسی قرار دهیم.

برای ورود به این مد، می‌توانید در مد Privileged از دستور Setup استفاده کنیدکه بعد از وارد شدن به این مد از شما سؤالاتی پرسیده می‌شود که باهم مورد بررسی قرار می‌دهیم:

Router# **setup**
Continue with configuration Dialog? [Yes/No] Yes

در این قسمت از شما پرسیده می‌شود، آیا می‌خواهید تنظیمات روتر را با استفاده از سؤالات مختلف انجام دهید، که Yes را وارد می‌کنیم.

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

در این سؤال از شما پرسیده می‌شود، آیا می‌خواهید وارد تنظیمات جزئی‌تر شوید مانند تنظیم اینترفیس‌ها و .... که با YES وارد آن می‌شویم.

Enter host name [Router]: R1

در سؤال اول از شما نام دستگاه پرسیده می‌شود که شما می‌توانید یک اسم دلخواه وارد کنید.

Enter enable secret: cisco

در سؤال بعدی از شما رمز عبور درخواست می‌شود، این رمز به صورت Secret است و قابل‌شناسایی برای هرکسی نیست و Hash شده است.

Enter enable password: ciscoR1

در این قسمت رمز عبور دیگری از شما پرسیده می‌شود که برتری آن کمتر از رمز عبور قبلی است و تا زمانی که رمز عبور قبلی فعال است این رمز کاربردی ندارد.

Enter virtual terminal password: FR122

در این قسمت از شما رمز عبور مربوط به پورت ترمینال پرسیده می‌شود که آن را وارد کنید.

Configure SNMP Network Management? [no]:

این قسمت مربوط به تنظیمات SNMP است که فقط بر روی enter کلیک کنید تا از این قسمت خارج شویم، بعدازآن لیست Interface های روتر را به شما نشان می‌دهد.

Current interface summary

Interface IP-Address OK? Method Status Protocol

GigabitEthernet0/0 unassigned YES manual administratively down down

GigabitEthernet0/1 unassigned YES manual administratively down down

GigabitEthernet0/2 unassigned YES manual administratively down down

Vlan1 unassigned YES manual administratively down down

Enter interface name used to connect to the

*management network from the above interface summary:***GigabitEthernet0/2**

در این قسمت نام یکی از اینترفیس‌ها را نوشته و بر روی enter کلیک کنید.

Configure IP on this interface? [yes]: yes

اگر می‌خواهید این Interface را آدرس‌دهی کنید yes را وارد و enter کنید.

IP address for this interface: 192.168.1.1

در این قسمت ip address را وارد و Enter کنید.

Subnet mask for this interface [255.255.255.0] : 255.255.255.0

در این قسمت از شما subnet Mask مربوط به IP بالا درخواست می‌شود، وارد کنید و بعد enter.

The following configuration command script was created:

!

```
hostname r1
enable secret 5 $1$mERr$Wmdu8FSDG1wNa1xa4SQGi.
enable password 21
line vty 0 4
password 2
!
interface Vlan1
shutdown
no ip address
!
interface GigabitEthernet0/0
no shutdown
ip address 192.168.1.1 255.255.255.0
!
interface GigabitEthernet0/1
shutdown
no ip address
!
interface GigabitEthernet0/2
shutdown
no ip address
!
end

[0] Go to the IOS command prompt without saving this config.
[1] Return back to the setup without saving this config.
[2] Save this configuration to nvram and exit.

Enter your selection [2]:
```

در آخر کار به شما تمام تنظیمات را که انجام داده‌اید، نمایش می‌دهد. به شما اعلام می‌کند که آیا می‌خواهید تنظیمات را در Nvram ذخیره کنید که با انتخاب گزینه‌ی 2 این اطلاعات در Nvram ذخیره می‌شود و بعد از خاموش و روشن شدن روتر اطلاعات در حافظه باقی می‌ماند.

کلیدهای ترکیبی:

کلید ترکیبی Ctrl_A باعث می‌شود مکان‌نما به خط آغازین انتقال پیدا کند.

کلید ترکیبی Ctrl_E باعث می‌شود مکان‌نما به انتهای خط برود.

کلید ترکیبی Ctrl_B به اندازه‌ی یک حروف به عقب برگشت می‌کند.

کلید ترکیبی Ctrl_F به اندازه‌ی یک حروف به جلو انتقال داده می‌شود.

کلید ترکیبی Ctrl_D کاراکترهای جلوی مکان‌نما را حذف می‌کند.

کلید ترکیبی Ctrl_U کل خط موردنظر را پاک می‌کند.

کلید ترکیبی Ctrl_W یک کلمه را پاک می‌کند.

کلید ترکیبی Ctrl_Z باعث می‌شود که مکان‌نما در هر مدی که قرار داشته باشد به مد Privileged انتقال پیدا کند.

- ✓ اگر بر روی کلیدهای جهت بالا و پایین فشار دهید ، آخرین دستوراتی را که وارد کرده اید را می‌توانید مشاهده کنید.
- ✓ با استفاده از دستورshow history می‌توانید 10 دستور آخر واردشده را مشاهده کنید.

```
Router#show history
 en
 conf t
 show history
```

تغییر نام روتر (HostName):

می‌توانید نام روتر را تغییر دهید تا استفاده از آن برای شما آسان‌تر شود. سعی کنید نام روتر را طبق محلی که قرار دارید تغییر دهید، مثلاً اگر روتر در شهر بابل قرار دارد، نام آن را به بابل تغییر دهید. برای انجام این کار در مد Global، دستور زیر را وارد کنید:

```
Router(config)#hostname babol
babol(config)#
```

همان‌طور که مشاهده می‌کنید، نام روتر به babol تغییر کرده است.

نمایش پیام در زمان ورود به روتر (Banner):

این دستور زمانی به کار می‌رود که بخواهیم برای کسی که وارد روتر می‌شود پیام نمایش بدهیم که برای انجام این کار وارد مد Global می‌شویم و از دستور زیر استفاده می‌کنیم.

```
Router1(config)#banner ?
loginSet login banner
motdSet Message of the Day banner
```

با واردکردن دستور Banner و بعد آن علامت سؤال دو حالت را نمایش می‌دهد که Login برای کاربرانی است که از طریق Telnet وارد روتر می‌شوند و Motd برای کاربرانی است که به صورت مستقیم وارد روتر می‌شوند. در این قسمت از Motdاستفاده می‌کنیم:

```
Router1(config)#banner motd@
```

در دستور بالا از کلمه‌ی @ استفاده کردیم که به جای آن هر کلمه‌ای می‌توانید قرار دهید. این کلمه، به این معنا است که پیامی که می‌نویسیم، بعد از اتمام پیام اگر این کلمه را در انتهای آن قرار دهید، یعنی اتمام کار و enter کنید، پیام ثبت می‌شود.

```
Router1(config)#banner motd @
Enter TEXT message.  End with the character '@'.
in the name of god @
Router1(config)#
```

banner motd را باهم انجام دادیم، وارد UserMode شوید و قبل از اینکه بخواهیم کاری انجام دهیم این پیام نمایش داده می‌شود.

```
in the name of god

Router1>
```

نوع دیگری از banner وجود دارد که به آن Banner Login می‌گویند. این روش در موقع ورود از طریق Telnet کاربرد دارد. برای فعال کردن آن دستور زیر را وارد کنید.

```
Router1(config)#banner login @
Enter TEXT message.  End with the character '@'.
Welcom @
```

مانند روش قبلی است، فقط به جای Motd، Login قرار می‌دهیم و پیام موردنظر را وارد می‌کنیم.

در زمان Telnet کردن این پیام نمایش داده خواهد شد.

نوشتن توضیحات برای یک Interface:

در IOS این امکان وجود دارد که بر روی interface می‌توانید توضیحاتی قرار دهید، برای این کار وارد interface موردنظر می‌شویم و دستور زیر را وارد می‌کنیم:

```
Router(config-if)#description connection iran to usa
```

بعد از دستور description پیام خود را وارد کنید، مانند مثال بالا.

بعد از انجام این کار برای نمایش این پیام دستور **show Running-config** را در مد privileged وارد کرده و این توضیحات زیر Interface موردنظر نمایش داده می‌شود، مانند دستور زیر:

```
interface GigabitEthernet0/0
description connection iran to usa
```

تنظیم ساعت و تاریخ روتر:

برای اینکه ساعت روتر خود را تنظیم کنید از دستور زیر استفاده کنید:

Router# Clock Set 10:05:05 19 Nov 2013

با دستور Clock Set این کار انجام می‌شود و بعد از این دستور ساعت، دقیقه و ثانیه را وارد کنید مانند 10:05:05 و بعدازآن، روز، ماه، سال را وارد کنید مانند 19 Nov 2013، بدین‌ترتیب ساعت و تاریخ روتر تنظیم می‌شود.

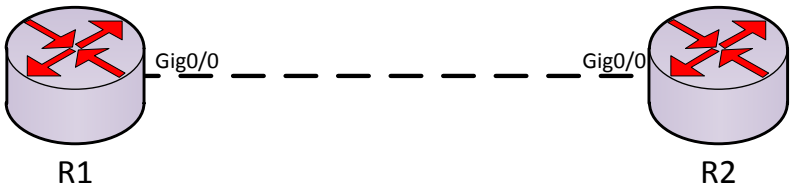
مسیریابی (IP Routin)

:Routing

Routing یا مسیریابی، روشی است برای انتخاب مسیرهای شبکه‌های غیر محلی و انتقال اطلاعات به شبکه‌ای دیگر که این کار توسط پروتکل‌های مسیریابی انجام می‌شود.

در مسیریابی، بهترین و کوتاه‌ترین مسیر برای رسیدن اطلاعات مشخص می‌شود که این کار توسط جدول Routing مشخص و مسیر انتخاب می‌شود، درباره‌ی این موضوعات به‌طور مفصل در ادامه‌ی کتاب باهم بحث خواهیم کرد.

Routing Table: این جدول تشکیل شده است از آدرس‌های متصل به روتر و آدرس‌های شبکه‌های غیر محلی، یعنی از شبکه دیگر.



Router#**show ip route**

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

Gateway of last resort is not set

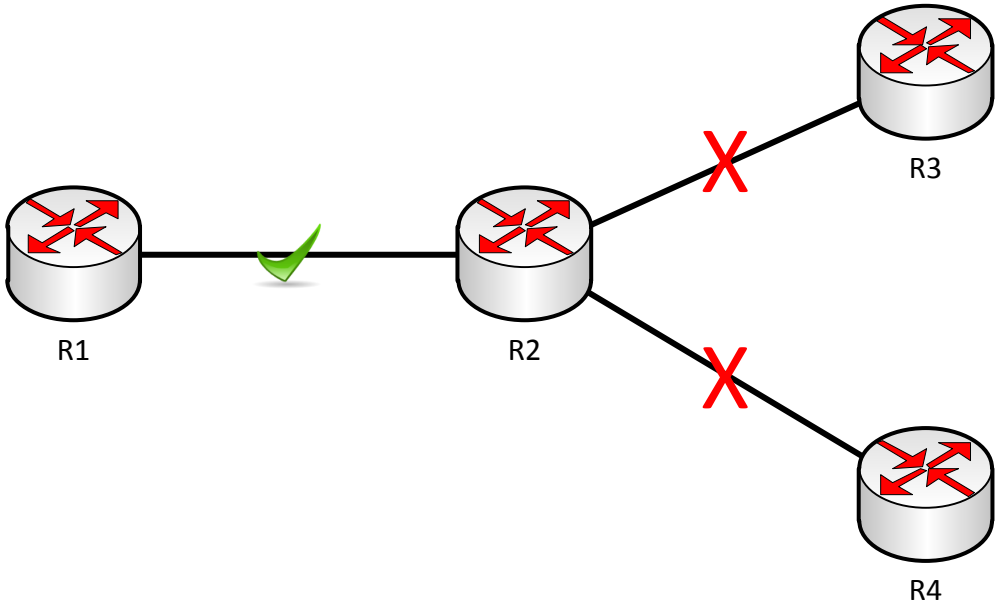
192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C 192.168.1.0/24 is directly connected, GigabitEthernet0/0
L 192.168.1.1/32 is directly connected, GigabitEthernet0/0

در این شکل دو روتر به هم متصل شده‌اند. ip هایی که به آن‌ها داده شده در رنج 192.168.1.0 است که همان‌طور مشاهده می‌کنید، این ip به عنوان شبکه‌ی محلی روتر(رنگ قرمز) ثبت شده است. یک کلمه‌ی C اول ip مشاهده

می‌کنید که نشان‌دهنده‌ی connected بودن آن است، البته هر حرفی که اینجا نوشته می‌شود در بالای آن کلمه‌ی مربوط به آن نوشته شده است.

این جدول همان جدول **Iprouting** است که در بالا باهم درباره آن صحبت کردیم.

لازم است اینجا یک نکته را به شما دوستان بگویم که یک روتر فقط و فقط از شبکه‌های داخل خود که شبکه‌ی محلی است، خبر دارد و از شبکه‌های خارج از آن خبری ندارد. به شکل زیر توجه کنید.



همان‌طور که در شکل می‌بینید، R1 از اطلاعات شبکه‌ای که به وی متصل است خبر دارد، اما از اطلاعات شبکه‌های دیگر در روترهای دیگر خبری ندارد. برای حل این مشکل دو راه‌کار وجود دارد؛ برای معرفی شبکه‌های غیر محلی به روترها:

- **Static Route** ✓
- **Dynamic Routing** ✓

روش Static Route:

معرفی شبکه‌های غیر محلی در static Route به دو روش انجام می‌گیرد:

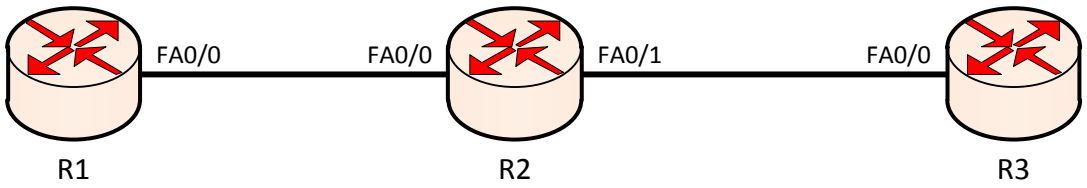
- **IP Route**
- **Defualt Route**

روش اول IP Route:

در این روش شبکه‌های غیر محلی را به صورت دستی به روتر معرفی می‌کنیم و می‌گوییم برای رفتن به این شبکه از کجا عبور کنید، این روش به علت اینکه معرفی و حذف مسیرهای شبکه به صورت دستی انجام می‌گیرد در شبکه‌های بزرگ بسیار کار وقت‌گیر و خسته‌کننده‌ای است و کمتر در این نوع شبکه‌ها استفاده می‌شود.

مثال1: سه روتر وارد صفحه کنید و آن‌ها را با کابل Cross به هم متصل کنید، مانند شکل زیر ip های روترها به صورت جدول زیر وارد شود.

R1	F 0/0	192.168.1.1
R2	F0/0	192.168.1.2
	F0/1	192.168.2.1
R3	F0/0	192.168.2.2



برای اینکه متوجه شویم به روترها درست ip داده‌ایم از دستور ping استفاده می‌کنیم. برای این منظور وارد روتر R1 شوید و در مد Privileged دستور زیر را وارد کنید.

Router# **Ping 192.168.1.2**

با این دستور این تست انجام می‌شود و نتیجه‌ی کار باید به صورت زیر باشد:

Router#ping 192.168.1.2

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.2, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/0/0 ms
```

علامت ! پشت سر هم به این معنا است که به روتر روبرو متصل هستیم.
شما می‌توانید بعدازاینکه Ip address را در اینترفیس وارد کردید، یک اسم را به ip ارتباط دهید و به جای ip، اسم آن را Ping کنید.

```
Router(config)# ip  host  cisco  192.168.1.2
```

همان‌طور که مشاهده می‌کنید نام cisco را به ip ، 192.168.1.2 ارتباط داده‌ایم که برای Ping کردن فقط اسم cisco را Ping می‌کنیم:

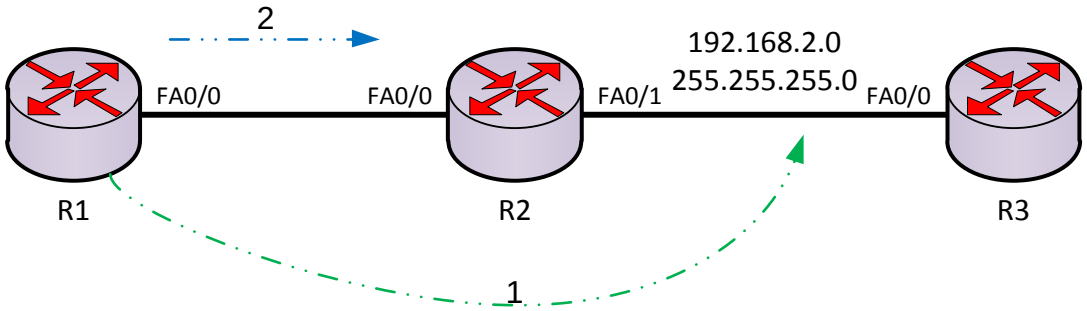
```
Router # ping cisco
```

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.2, timeout is 2 seconds:
.!!!!
Success rate is 0 percent (4/5)
```

به این موضوع توجه کنید که R1 فقط به شبکه‌های متصل به خودش دسترسی دارد و این شبکه‌ها را به صورت شبکه‌ی connected در جدول روتینگ خود ثبت می‌کند. حالا موقع این است که شبکه‌های غیر محلی را به روتر معرفی کنیم.
برای معرفی شبکه غیر محلی به روتر باید از دستور Ip Route استفاده کنیم. چطوری این کار را انجام بدهیم؟
در روتر R1 وارد مد Global شده و دستور زیر را وارد می‌کنیم:

```
Router(config)#  ip route 192.168.2.0  255.255.255.0  192.168.1.2
```

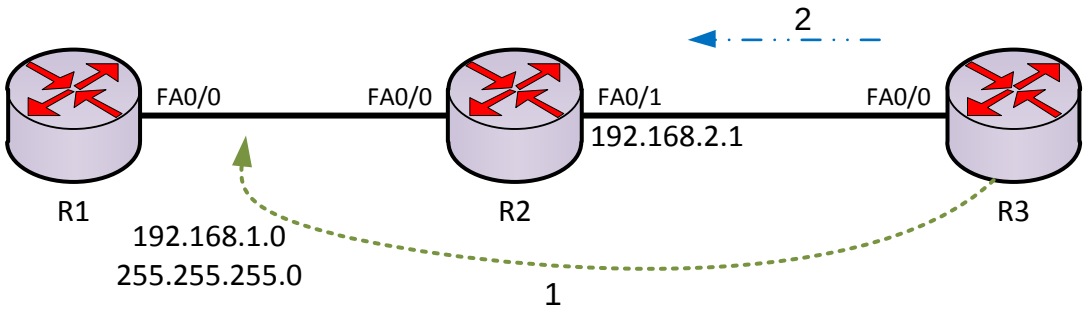
این دستور را به این صورت بخوانید (همراه با شکل بخوانید)، بگویید: برو به شبکه 192.168.2.0 با SubnetMask، 255.255.255.0 از 192.168.1.2 عبور کن. در شکل زیر می‌توانید این موضوع را مشاهده کنید.



نکته‌ی مهم: این عمل باید از هر دو طرف انجام بگیرد، یعنی اینکه مثلاً در این مثال در R3 هم باید این کار را انجام دهید، اما برعکس قبل که به صورت زیر باید دستور را در روتر R3 وارد کنید.

Router(config)# **ip route 192.168.1.0 255.255.255.0 192.168.2.1**

این دستور را به این صورت بخوانید؛ بگویید (شماره‌ی 1) برو به شبکه‌ی 192.168.1.0 با SubnetMask، 255.255.255.0 از 192.168.2.1 (شماره‌ی 2) عبور کن. در شکل زیر هم می‌توانید این موضوع را مشاهده کنید.



خوب، حالا اگر شما از R1 بخواهید، R3 را Ping کنید، این کار به خاطر فعال کردن IP Route انجام می‌شود.

Router# **ping 192.168.2.2**

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/2/13 ms

به راحتی توانستیم این کار را انجام دهیم، حالا وقت آن است که سری به جدول روتینگ بزنیم. برای نمایش جدول روتینگ از دستور Show IP Route در مد Privileged استفاده می‌کنیم، مانند زیر:

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

Gateway of last resort is not set

C    192.168.1.0/24 is directly connected, FastEthernet0/0
S    192.168.2.0/24 [1/0] via 192.168.1.2
```

همان‌طور که مشاهده می‌کنید، لیست شبکه‌های متصل به روتر را با حروف C مشخص کرده است. اگر توجه کنید، شبکه‌ای با حروف S وجود دارد که S در اینجا به معنای static است و این همان شبکه‌ای است که به صورت دستی تعریف کرده‌ایم.

نکته: اگر interface مورد نظر به هر دلیلی Down (خاموش) شود، ip Route که برای این مسیر ایجاد کرده‌ایم، حذف می‌شود. برای اینکه بعد از Down شدن اینترفیس، IP Route از بین نرود، آخر این دستور از دستور permanent استفاده می‌کنیم، یعنی:

Router(config)#**ip route 192.168.1.0 255.255.255.0 192.168.2.1 Permanent**

روش Defualt Route:

شبکه‌ها را در قسمت قبل توانستیم به صورت دستی تعریف کنیم. اگر تعداد شبکه زیاد شود، این کار وقت‌گیر است. متخصصان یک روش دیگر با عنوان Defualt Route معرفی کردند که دیگر لازم نیست تک‌تک شبکه‌های روترها را معرفی کنیم، فقط به روتر می‌گوییم، هر چیزی را که نمی‌دانی، بفرست به روتر کناری، به همین راحتی. برای انجام این کار در مثال قبلی دستور Ip route را با گذاشتن no در اول آن حذف کنید، مانند زیر:

Router(config)#**no ip route 192.168.2.0 255.255.255.0 192.168.1.2**
Router(config)#**no ip route 192.168.1.0 255.255.255.0 192.168.2.1**

بعد از پاک کردن ip route های قبلی به این صورت دستورات را در روترهای R1 و R3 وارد می‌کنید.

در روتر R1:

Router(config)# **Ip Route 0.0.0.0 0.0.0.0 192.168.1.2**

در روترR3:

Router(config)# **Ip Route 0.0.0.0 0.0.0.0 192.168.2.1**

این دستورات به این صورت است که می‌گوید هر Ip (0.0.0.0) با هر SubnetMask (0.0.0.0) که نمی‌شناسی را بفرست به روتر کناری خودت که به شما متصل است. به این صورت عمل می‌کند که وقتی روتر R1 بخواهد با روتر R3 ارتباط برقرار کند، به R2 می‌گوید که من ip، 192.168.2.2 را می‌خواهم، چون روتر R2 متصل است به روتر R3، همین امر باعث می‌شود که کار به نتیجه برسد. در حال حاضر اگر Ping از R1 به طرف R3 بزنید، جواب خواهد داد.

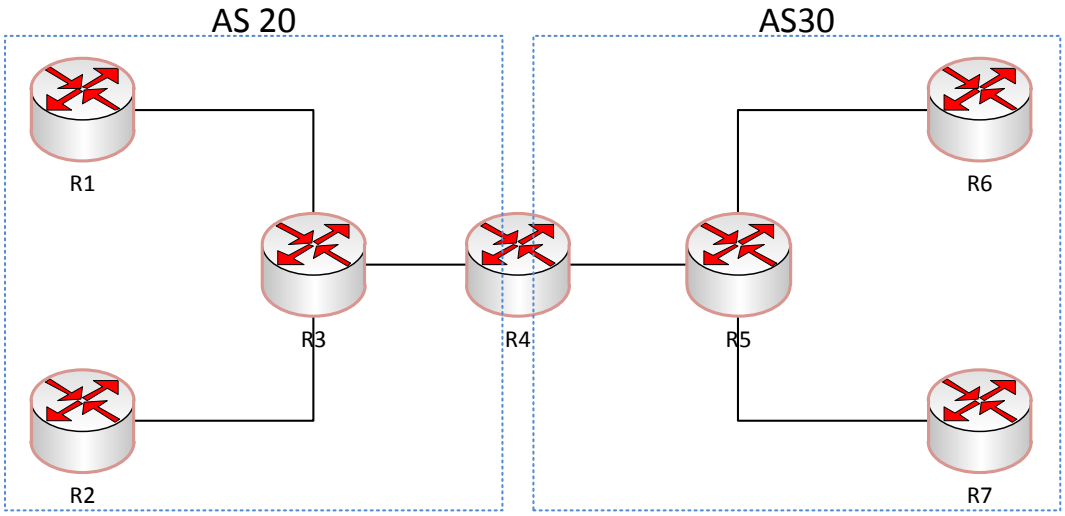
2–Dynamic Routing:

این دسته از روش‌های دسترسی به شبکه‌های غیر محلی دیگر به صورت دستی انجام نمی‌شود، بلکه به صورت خودکار از طریق Routing Protocols ها انجام می‌شود.

Routing Protocols ها در انواع مختلف و با سرعت‌های متفاوتی وجود دارند که در ادامه‌ی کتاب درباره آن‌ها بحث می‌کنیم. این پروتکل‌ها از طریق الگوریتمی که در خود دارند شبکه‌های خود را به دیگر روترها معرفی می‌کنند و در جدول روتینگ خود این شبکه‌ها را درج می‌کنند.

تعریف Autonomuos System:

به مجموعه‌ای از روترها که در یک منطقه قرار دارند، گفته می‌شود که روترها فقط در همان منطقه باهم در ارتباط هستند. اگر به شکل زیر نگاه کنید، متوجه‌ی این موضوع می‌شوید.



عدد AS یا همان Autonomous System می‌تواند عددی بین 0 تا 65535 باشد. در ادامه با اجرای یک پروتکل مانند IGP با AS آشنا می‌شوید.

پروتکل‌های مسیریابی بر دو نوع هستند:

- ✓ IGPs(Interior Gateway Protocol)
- ✓ EGPs(Exterior Gateway Protocol)

پروتکل‌های IGPs:

به روتینگ پروتکل‌هایی که داخل یک AS کار می‌کنند و باهم در ارتباط هستند، مانند پروتکل‌های IGRP و RIP و EIGRP و OSPF، پروتکل‌های IGPs گفته می‌شود.

پروتکل‌های EGPs:

روتینگ پروتکل‌هایی که می‌توانند AS های مختلف را به هم ارتباط دهند، مانند پروتکل BGP پروتکل‌های EGPs گفته می‌شود که به آن‌ها روترهای مرزی هم گفته می‌شود.

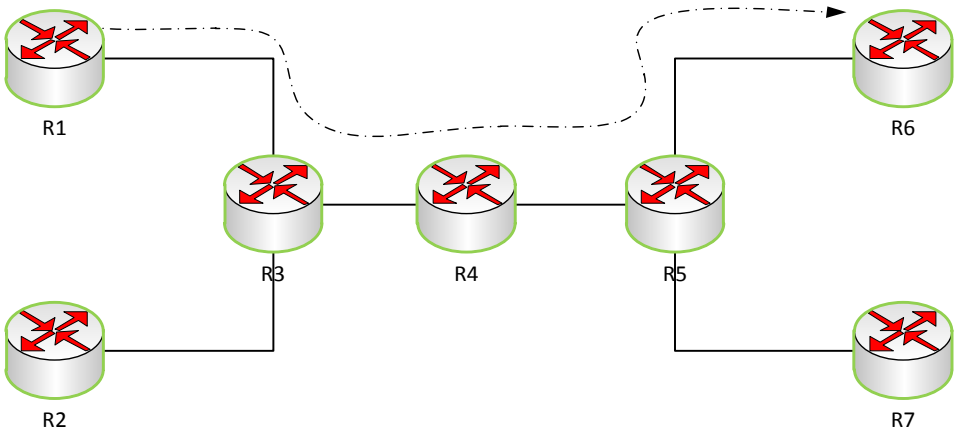
Dynamic Routing به سه دسته‌ی کلی تقسیم می‌شوند که هر 3 را باهم مورد بررسی قرار می‌دهیم:

- ✓ **Distance Vector**
- ✓ **Link State**
- ✓ **Hybrid**

پروتکل‌های Distance Vector یا بردار فاصله:

به پروتکل‌هایی گفته می‌شود که فقط و فقط با روتر کناری خود در ارتباط هستند و تمام اطلاعات خود را به روتر کناری خود منتقل و دریافت می‌کنند.

برای رسیدن به یک شبکه‌ی خاص از یک بردار خطی استفاده می‌کند، مانند شکل زیر:

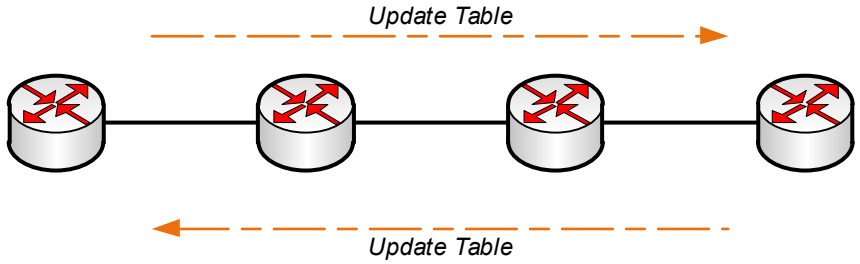


در این پروتکل‌ها اگر روتری، روتر کناری خود را بشناسد، می‌تواند بهترین مسیر را از روتر کناری خود دریافت کند. روتینگ پروتکل‌های RIP و IGRP از این نوع می‌باشند.

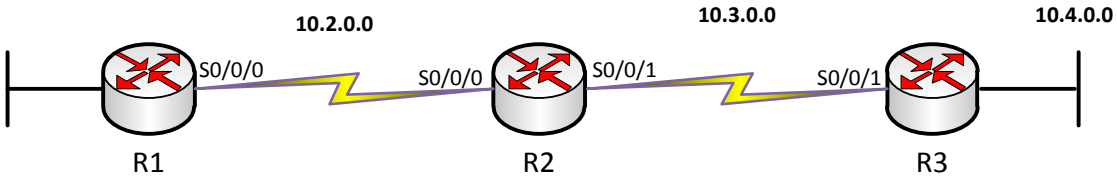
الگوریتمی که این نوع پروتکل‌ها با آن کار می‌کنند، Bellman_Ford است که ویژگی‌های آن به صورت زیر است:

- ساخت جدول Routing برای آدرس‌های شبکه.
- شناسایی شبکه‌های متصل به آن و ثبت در جدول.
- انتقال اطلاعات این جداول به صورت کلی در زمان مشخص که به آن Priodic Update می‌گویند.

این نوع پروتکل‌ها در جدول روتینگ خود ابتدا، شبکه‌های connect به خود را در جدول درج می‌کنند و بعد از ارتباط با روترهای دیگر بهترین مسیر را انتخاب و در جدول خود درج می‌کنند. روترها جداول خود را به صورت Broadcast به روترهای مجاور خود می‌فرستند که در پروتکل Rip به ip، 255.255.255 و در پروتکل IGRP به‌ip، 224.0.0.9 فرستاده می‌شود و بعد روتر در پاسخ به روتری که Update فرستاده، اطلاعات جدول خود را به صورت Unicast به این روتر می‌دهد و به همین صورت همه‌ی روترها از کل شبکه‌ی موجود باخبر می‌شوند.



Metric: در جدول روتینگ معیاری وجود دارد به نام متریک که تعداد روترهای سر راه برای رسیدن به شبکه موردنظر را مشخص می‌کند. در یک پروتکل مشخص برای رسیدن به یک شبکه اگر تعداد روترهای سر راه 3 تا باشد، متریک می‌شود 3 و به این هم توجه داشته باشید که هر چه متریک کمتر، مسیر بهتر و سریع‌تر است و همان مسیر انتخاب می‌شود.



Network	Interface	Hop
10.1.0.0	Fa0/0	0
10.2.0.0	S0/0/0	0
10.3.0.0	S0/0/0	1

Network	Interface	Hop
10.2.0.0	S0/0/0	0
10.3.0.0	S0/0/1	0
10.1.0.0	S0/0/0	1
10.4.0.0	S0/0/1	1

Network	Interface	Hop
10.3.0.0	S0/0/1	0
10.4.0.0	Fa0/0	0
10.2.0.0	S0/0/1	1

به شکل بالا توجه کنید، در جدول روتر R1 دو تا از مسیرها، متریک آن صفر در نظر گرفته شده، آن‌هم به خاطر این است که متریک شبکه‌های متصل به روتر، صفر است. توجه داشته باشید به متریک، Hop Count هم می‌گویند. اگر با دقت بیشتر به جدول نگاه کنید، R1 شبکه 10.3.0.0 را با متریک 1 در جدول خود قرار داده است، آن‌هم به این خاطر است که فقط یک روتر برای رسیدن به این شبکه در سر راه قرار دارد. اگر R1 بخواهد به شبکه‌ی 10.4.0.0 برسد، متریک سر راه را 2 در نظر می‌گیرد، چون 2 تا روتر در سر راه تا رسیدن به آن شبکه قرار دارد.

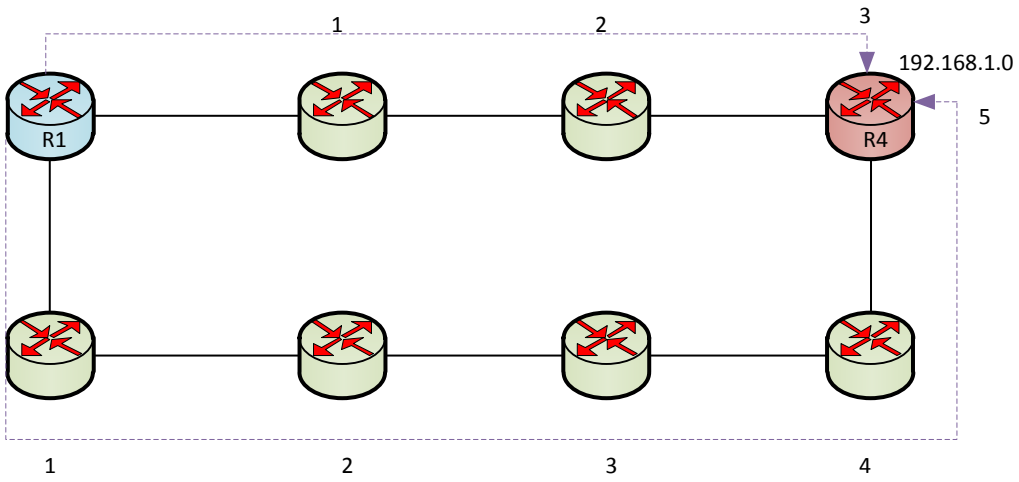
Convergence Time:

به مدت‌زمانی گفته می‌شود که یک روتر به حالت پایدار می‌رسد و تمام شبکه‌های خود و اطراف خود را می‌شناسد و در جدول خود ثبت می‌کند.

بعد از این‌که روتر یک به حالت پایدار رسیده و جدول روتینگ خود را کامل کرده، در طی زمان‌های مشخص تمام جدول روتینگ خود را به صورت Full Update به روترهای دیگر ارسال می‌کند. چه تغییری در جدول این روتر صورت بگیرد، چه نگیرد این Update ارسال می‌شود. به این روش ارسال اطلاعات که در طی زمانی مشخص صورت می‌گیرد، Priodic Update می‌گویند که این موضوع یکی از مهم‌ترین ویژگی‌های پروتکل‌های Distance Vectore است.

روش‌های انتخاب بهترین مسیر:

در شبکه‌هایی که با پروتکل Rip راه‌اندازی می‌شوند، انتخاب بهترین مسیر از روی Hop Count یا تعداد روترهای سر راه است. برای درک بهتر این موضوع به این شکل توجه کنید.

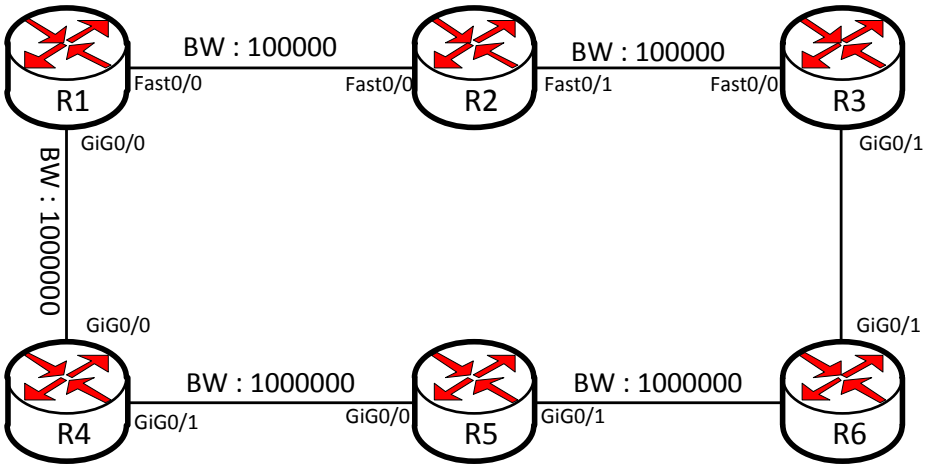


به دقت به شکل توجه کنید، R1 برای رسیدن به شبکه‌ی 192.168.1.0 دو مسیر سر راه خود می‌بیند. در مسیر بالایی برای رسیدن به شبکه‌ی 192.168.1.0، سه روتر در سر راه قرار دارد، اما در مسیر پایینی پنج روتر در سر راه قرار دارد، پس به این نتیجه می‌رسیم که مسیر بالایی نسبت به مسیر پایینی سریع‌تر و کوتاه‌تر است. در پروتکل Rip که در ادامه با آن آشنا می‌شویم، انتخاب بهترین مسیر از روی متریک و یا همان روترهای سر راه است.

در شبکه‌هایی که با پروتکل IGRP راه‌اندازی می‌شوند، قضیه کمی فرق می‌کند. در پروتکل IGRP برای انتخاب بهترین متریک، چند روش وجود دارد که هر کدام را باهم دیگر بررسی می‌کنیم.

- Bandwidth
- Delay
- Reliability
- Loading
- MTU

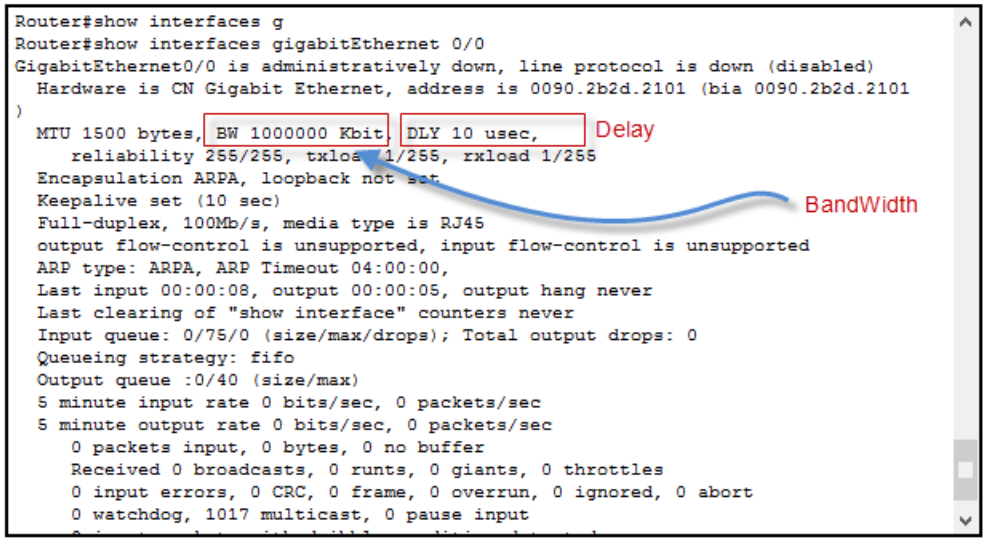
در این پروتکل، انتخاب بهترین مسیر از روی متریک صورت نمی‌گیرد، بلکه از روی دو گزینه‌ی اول، یعنی Bandwidth و Delay صورت می‌گیرد که این دو گزینه به نسبت بقیه‌ی گزینه‌ها مهم‌تر هستند. اگر پهنای باند یک مسیر بیشتر باشد، همان مسیر به عنوان بهترین مسیر انتخاب می‌شود.



به شکل بالا توجه کنید، مسیر یک از پورت‌های FastEthernet استفاده می‌کند و مسیر دوم از پورت‌های GigabitEthernet استفاده می‌کند که پهنای باند FastEthernet، 100000 است و پهنای باند GigabitEthernet، 1000000 است و Delay اولی 100 میلی‌ثانیه و دومی 10 میلی‌ثانیه است و به خاطر بیشتر بودن پهنای باند و کمتر بودن زمان تأخیر، مسیر دوم، یعنی روترهای R4، R5، R6، R3 انتخاب می‌شود، به همین راحتی.

برای اینکه بتوانید پهنای باند مورد نظر یک پورت را مشاهده کنید، در مد Privileged از دستور زیر استفاده کنید، مثلاً برای پورت GigabitEthernet به این صورت استفاده کنید:

Router# **Show interface GigabitEthernet0/0**

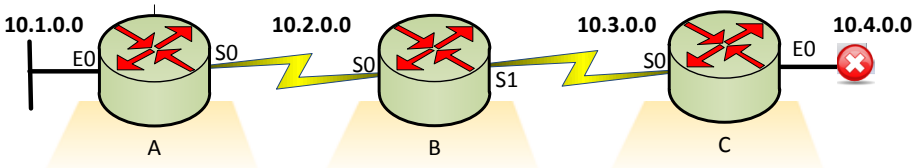


با این دستور، اطلاعات روبرو را به ما نشان می‌دهد.

همان‌طور که مشاهده می‌کنید، پهنای باند برای پورت GigaEthernet، 1000000 و Delay، 10 است.

بررسی loop در پروتکل‌های Distance Vectore:

رویداد loop یا دور در شبکه، یکی از ویژگی‌های پروتکل‌های Distance Vectore است و باعث مشکلات عمده‌ای در شبکه می‌شود، البته این‌گونه مشکلات با ارائه‌ی روش‌های خاص حل شده است، اما باهم این مشکلات را بررسی می‌کنیم.

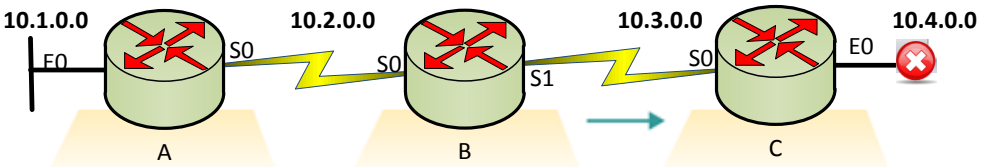


Routing Table		
10.1.0.0	E0	0
10.2.0.0	S0	0
10.3.0.0	S0	1
10.4.0.0	S0	2

Routing Table		
10.2.0.0	S0	0
10.3.0.0	S1	0
10.4.0.0	S1	1
10.1.0.0	S0	1

Routing Table		
10.3.0.0	S0	0
10.4.0.0	E0	Down
10.2.0.0	S0	1
10.1.0.0	S0	2

همان‌طور که در شکل بالا مشاهده می‌کنید، قبل از اینکه مشکلی برای پورت E0 روتر C پیش بیاید روتر C اطلاعات جدول روتینگ خود را به روترهای مجاور فرستاده است، یعنی در زمان مشخص‌شدهPriodic Update خود را برای بقیه‌ی روترها فرستاده است و روتر B شبکه‌ی 10.4.0.0 را با متریک 1 و روتر A این شبکه را با متریک 2 در شبکه‌ی خود ثبت کرده است، بعد برای پورت E0 مربوط به روتر C مشکلی ایجاد شده است وshutdown شده است و down شدن این پورت در جدول روتر C ثبت می‌شود، اما بقیه‌ی روترها از این موضوع خبر ندارند، چون زمان Full Update یا همان Priodic Update روتر C فرا نرسیده است، قبل از اینکه روتر C این عمل را انجام دهد، روتر B، Priodic Update خود را به روترهای مجاور خود قرار دارند ارسال می‌کند، چون در جدول روتر B شبکه‌ی 10.4.0.0 قرار دارد و نمی‌داند که Down شده است به شبکه‌های دیگر می‌فرستد و روتر C جدول روتینگ خود را update می‌کند و این شبکه را در جدول خود جای می‌دهد. با این کار متریک‌ها به صورت زیر تغییر می‌کنند.

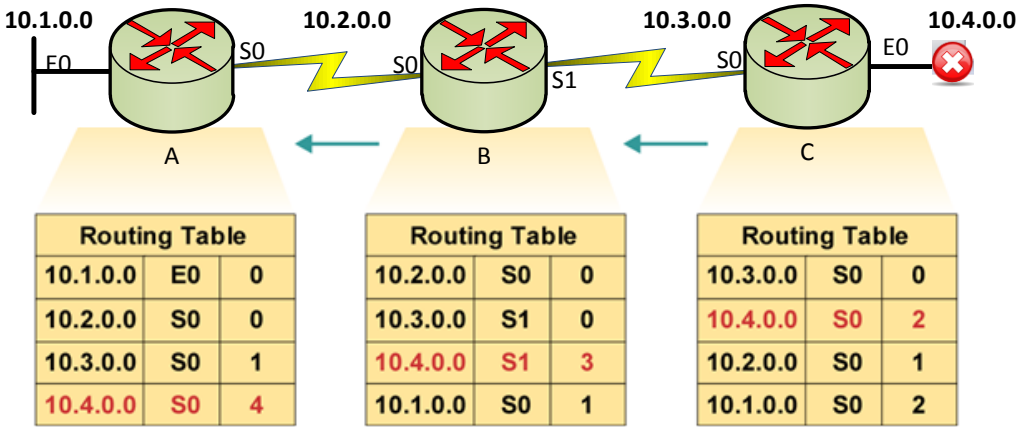


Routing Table		
10.1.0.0	E0	0
10.2.0.0	S0	0
10.3.0.0	S0	1
10.4.0.0	S0	2

Routing Table		
10.2.0.0	S0	0
10.3.0.0	S1	0
10.4.0.0	S1	1
10.1.0.0	S0	1

Routing Table		
10.3.0.0	S0	0
10.4.0.0	S0	2
10.2.0.0	S0	1
10.1.0.0	S0	2

اگر متوجه شده باشید، روتر B اولین بار شبکه‌ی 10.4.0.0 را با متریک 1 از روتر c یاد گرفته بود، بعدازاینکه آپدیت خود را به روترهای دیگر می‌فرستد، روتر C این شبکه را که در جدول خود ندارد، با متریک 2 قبول می‌کند، چون با متریک 1 از روتر B دریافت می‌کند و وقتی وارد روتر C می‌شود، 2 می‌شود؛ همین‌طور این کار ادامه داده می‌شود و متریک‌ها به اشتباه در تمام روترها افزایش پیدا می‌کند، مانند شکل زیر:



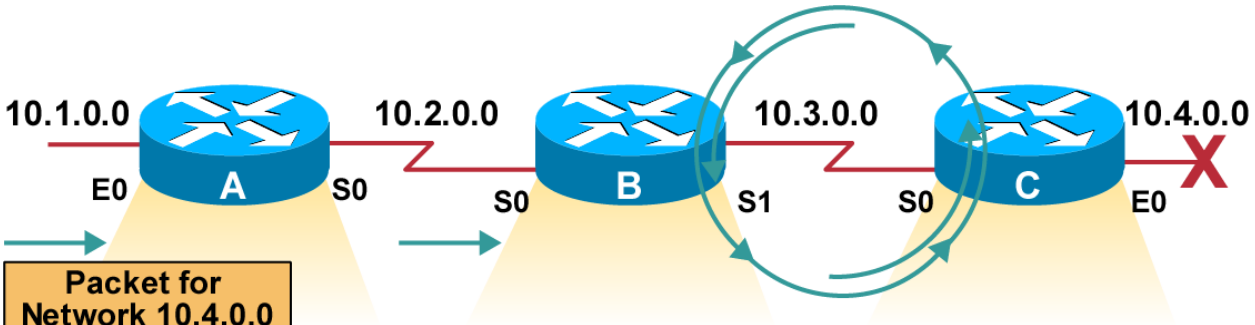
Routing Table		
10.1.0.0	E0	0
10.2.0.0	S0	0
10.3.0.0	S0	1
10.4.0.0	S0	4

Routing Table		
10.2.0.0	S0	0
10.3.0.0	S1	0
10.4.0.0	S1	3
10.1.0.0	S0	1

Routing Table		
10.3.0.0	S0	0
10.4.0.0	S0	2
10.2.0.0	S0	1
10.1.0.0	S0	2

دوباره روتر c جدول آپدیت خود را به روترهای مجاور خود می‌دهد و دوباره این متریک افزایش پیدا می‌کند، به این افزایش متریک بی‌رویه و اشتباه در اصطلاح، countingtoinfinity گفته می‌شود. برای حل این مشکل باید حداکثر مقدار Metric را در پروتکل Rip تعریف کنیم که در بحث Rip این کار را انجام می‌دهیم.

مشکل بعدی این است که دو روتر B و C در یک loop قرار می‌گیرند، وقتی روتر A، 10.4.0.0 را درخواست می‌کند، آن را به روتر B می‌دهد و روتر B هم به روتر C می‌دهد و روتر C برای رفتن به شبکه‌ی 10.4.0.0 اطلاعات را دوباره به طرف روتر B می‌فرستد و بعد، روتر B هم آن را دوباره به روتر c می‌فرستد که این امر باعث افتادن دو روتر در یک دایره‌ی تکرار می‌شود، مانند شکل زیر:



Routing Table		
10.1.0.0	E0	0
10.2.0.0	S0	0
10.3.0.0	S0	1
10.4.0.0	S0	4

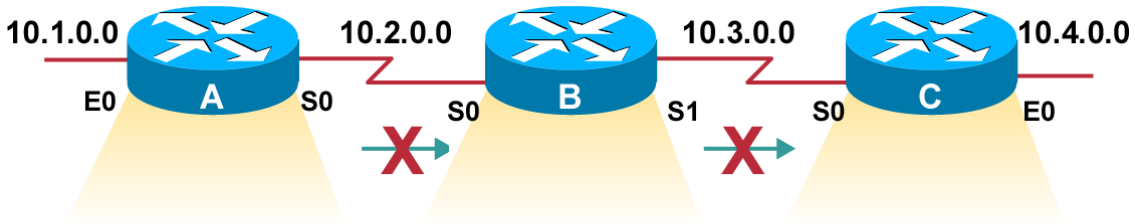
Routing Table		
10.2.0.0	S0	0
10.3.0.0	S1	0
10.4.0.0	S1	3
10.1.0.0	S0	1

Routing Table		
10.3.0.0	S0	0
10.4.0.0	S0	2
10.2.0.0	S0	1
10.1.0.0	S0	2

روش‌های مختلفی برای جلوگیری از loop در پروتکل‌های Distance Vector وجود دارد که باهم مورد بررسی قرار می‌دهیم.

روش اول Split Horizon:

در این روش اگر روتر C شبکه‌ی 10.4.0.0 را به روتر B داده است، روتر B دیگر این شبکه را به روتر C نمی‌فرستد، یعنی هر چیز گرفت، دیگر همان شبکه را پس نمی‌دهد.



Routing Table		
10.1.0.0	E0	0
10.2.0.0	S0	0
10.3.0.0	S0	1
10.4.0.0	S0	2

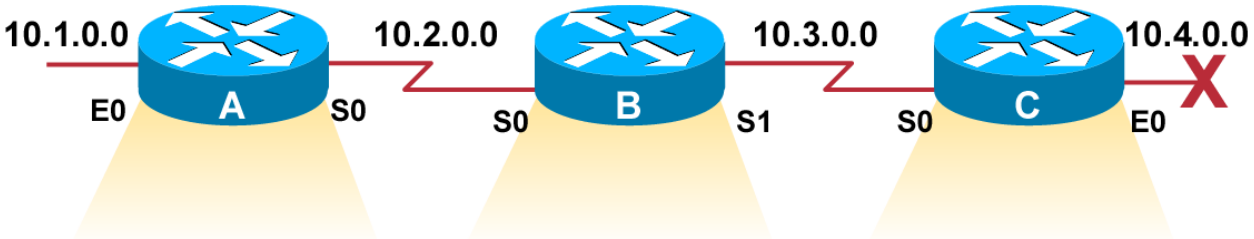
Routing Table		
10.2.0.0	S0	0
10.3.0.0	S1	0
10.4.0.0	S1	1
10.1.0.0	S0	1

Routing Table		
10.3.0.0	S0	0
10.4.0.0	E0	0
10.2.0.0	S0	1
10.1.0.0	S0	2

ICND20GR_212

همان‌طور در شکل بالا مشاهده می‌کنید، شبکه‌هایی که از طریق روتر A به B و B به C می‌رسد، دوباره به خودشان برگشت داده نمی‌شود.

روش دوم Route Poisoning:



Routing Table		
10.1.0.0	E0	0
10.2.0.0	S0	0
10.3.0.0	S0	1
10.4.0.0	S0	2

Routing Table		
10.2.0.0	S0	0
10.3.0.0	S1	0
10.4.0.0	S1	1
10.1.0.0	S0	1

Routing Table		
10.3.0.0	S0	0
10.4.0.0	E0	Down
10.2.0.0	S0	1
10.1.0.0	S0	2

ICND20GR_213

در این روش وقتی شبکه‌ای از مسیر خارج و down می‌شود، این شبکه از جدول حذف نمی‌شود، بلکه متریک آن به بی‌نهایت تغییر کرده و همین امر باعث می‌شود که به دیگر روترها این update ارسال شود و بقیه‌ی روترها این شبکه را با متریک بی‌نهایت در جدول روتینگ خود ثبت می‌کنند و وقتی روترها این شبکه را درخواست کنند، Unriachable بودن آن و از دست رفتن آن مشخص می‌شود. این شبکه در جدول روترها تا زمان به پایان رسیدن Holddown Timer در جدول باقی می‌ماند و حذف نمی‌شود.

این روش هم‌زمان با روش زیر کار می‌کند.

روش سوم Split Horizon With Poisoning Revers:

زمانی که از یک روتر بی‌نهایت شدن متریک را دریافت می‌کند، دوباره همان شبکه را با متریک بی‌نهایت به شبکه‌ای که این خبر را ارسال کرده، می‌فرستد این موضوع زمانی به کار می‌آید که اگر در زمان Down شدن شبکه، روتر C، روتر مجاور آن، یعنی روتر B یک update ارسال کند که این شبکه با متریکی پایین‌تر از متریک قبلی به روتر C داده شود، دوباره روتر C این شبکه را که از روتر B با متریک بهتر یاد گرفته، در جدول روتینگ خود قرار می‌دهد و همین کار باعث در Loop قرار گرفتن شبکه می‌شود، پس این روش، بهبودیافته‌ی روش Split Horizon است.

روش چهارم Holddown Timer:

یک زمان‌سنج است که برای پروتکل Rip، 180 ثانیه و برای پروتکل IGRP، 270 ثانیه است. این زمان‌سنج، زمانی اجرا می‌شود که یک روتر بفهمد که یک شبکه Down شده است. تا زمانی که این شبکه Down است تا مدت‌زمان مشخص به‌هیچ‌وجه به هیچ سؤالی که از این شبکه بیاید، جواب نمی‌دهد. اگر بعد از پایان زمان مورد نظر، این شبکه up نشود، روتر، این شبکه را از لیست خود حذف می‌کند، اما اگر در این مدت‌زمان شبکه‌ای با متریک کمتر به روتر برسد، آن شبکه را جایگزین شبکه‌ی قبلی می‌کند و از حالت Holddown خارج می‌شود.

حالتی به نام Triggered Update وجود دارد و هم‌زمان با Holddown Timer کار می‌کند و زمانی‌که یک شبکه Down شد و شبکه‌ی مورد نظر به حالت Hold رفت، در مدت‌زمان مشخص‌شده، Triggered Update به کل روترها خبر Down شدن این شبکه را می‌دهد و باعث جلوگیری از Loop می‌شود.

کار با پروتکل Routing Information Protocol**(Rip):**

این پروتکل یکی از محبوب‌ترین پروتکل‌های روتینگ و یکی از قدیمی‌ترین آن‌ها هم است. این پروتکل زیرمجموعه‌ی پروتکل‌های Distance Vector است و یک پروتکل IGPs است و در داخل یک AS(Autonomous System) کار می‌کند.

این پروتکل، مخصوص شبکه‌های کوچک است و در شبکه‌های بزرگ بالای 15روتر کاربرد ندارد.

یکی دیگر از ویژگی‌های این پروتکل، این است که جدول روتینگ را به صورت کامل در فواصل زمانی 30 ثانیه به دیگر روترها ارسال می‌کند که به آن Priodic Update می‌گویند که قبلاً روی این موضوع صحبت کردیم.

پروتکل Rip بر دو نوع است:

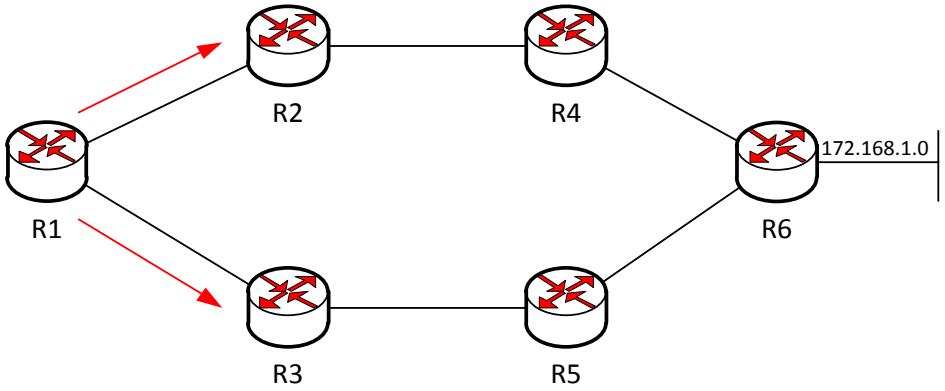
- **Rip Version 1**
- **Rip Version 2**

همان‌طور که در مطالب قبلی خواندید، ملاک انتخاب بهترین مسیر در این پروتکل، Hop Count یا روترهای سر راه است. توجه داشته باشید، حداکثر متریک در این پروتکل، 15 است و شما حداکثر روتری که در این پروتکل در یک AS می‌توانید استفاده کنید، 15 عدد است. اگر متریک بیشتر از 15 شود، شبکه غیرقابل‌دسترس خواهد بود.

ویژگی‌های پروتکل Rip در یک نگاه:

- این پروتکل از زیرمجموعه‌ی پروتکل‌های Distance Vector است.
- در فواصل زمانی مشخص (30 ثانیه) کل جدول روتیگ را به صورت Broadcast به روترهای مجاورش ارسال می‌کند (Priodic Update).
- جزو پروتکل‌های IGPs است.
- حداکثر متریک 15 است.

یکی دیگر از ویژگی‌های پروتکل Rip، استفاده بهینه از شبکه یا Load Balancing است. اگر دو مسیر با متریک یکسان داشته باشد، اطلاعات را بر روی هر دو مسیر انتقال می‌دهد و این امر باعث افزایش کارایی شبکه می‌شود.



در این شکل، R1 برای رسیدن به R6 می‌تواند از دو مسیر حرکت کند، چون برای رسیدن به روتر مورد نظر Hop Count سر راه یا روترهای سر راه در هر دو مسیر برابر است، پس از هر دو مسیر به صورتLoad Balancing استفاده می‌کند.

حالا سؤال پیش می‌آید که Rip Version 1 و Rip Version 2 چه تفاوتی باهم دارند؟ برای دریافت جواب به جدول زیر توجه کنید:

RIPv1	RIPv2
Distance vector	Distance vector
Maximum hop count of 15	Maximum hop count of 15
Classful	Classless
Broadcast based	Uses Multicast 224.0.0.9
No support for VLSM	Supports VLSM networks
No authentication	Allows for MD5 authentication
No support for discontiguous networks	Supports discontiguous networks

Rip Version 1 از CIDR و VLSM پشتیبانی نمی‌کند و SubnetMask را به همراه Net ID نمی‌فرستد. امیدوارم که متوجه شده باشید، اگر هم نشدید در ادامه، متوجه خواهید شد.

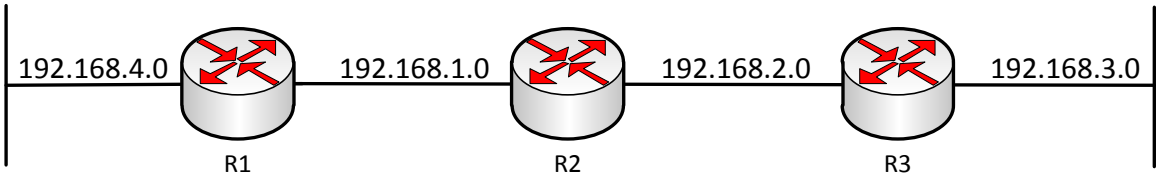
راه‌اندازی پروتکل Rip:

برای راه‌اندازی پروتکل Rip به صورت زیر عمل می‌کنیم:

Router(Config)# **Router Rip**
Router(config-router)# **Netwok** ***Network number***

در قسمت اول وارد مد Global می‌شویم و با دستور Router Rip پروتکل Rip بر روی روتر راه‌اندازی می‌شود و بعدازآن باید شبکه‌های متصل به روتر را به آن معرفی کنیم. با یک مثال به این موضوع پی خواهیم برد.

مثال 2: Packet Tracer را اجرا کرده و 3 روتر مانند شکل زیر به صفحه اضافه کنید و آن‌ها را از طریق کابل به هم متصل کنید و طبق شکل آدرس‌دهی کنید.



می‌خواهیم در این شبکه، پروتکل Rip راه‌اندازی کنیم؛ بر روی R1 کلیک می‌کنیم و دستورات زیر را در آن وارد می‌کنیم:

```
Router(config)#router Rip
Router(config-router)#network 192.168.1.0
Router(config-router)#network 192.168.4.0
```

همان‌طور که مشاهده می‌کنید، با دستور Router Rip، وارد پروتکل Rip شده‌ایم. بعدازآن باید آدرس NET ID شبکه‌های متصل به روتر را معرفی کنیم، شبکه‌هایی که به روتر R1 متصل می‌باشند، 192.168.1.0 و 192.168.4.0 هستند. همین کار را روی روترهای دیگر انجام می‌دهید.

تنظیمات روتر R2:

```
Router(config)#router Rip
Router(config-router)#network 192.168.1.0
Router(config-router)#network 192.168.2.0
```

تنظیمات روتر R3:

```
Router(config)#router Rip
Router(config-router)#network 192.168.2.0
Router(config-router)#network 192.168.3.0
```

به همین راحتی توانستیم این پروتکل را روی تک‌تک روترها راه‌اندازی کنیم. حالا باید ببینیم جدول روتینگ در چه وضعیتی است. همان‌طور که قبلاً گفتیم این جدول اطلاعات مسیرهای مختلف شبکه‌ها را در خود ذخیره می‌کند. برای نمایش جدول Routing باید از دستور زیر در یکی از روترها استفاده کنیم، وارد مد Privileged می‌شویم و دستور Show IP Route را وارد می‌کنیم، این کار را در روتر R1 انجام می‌دهیم:

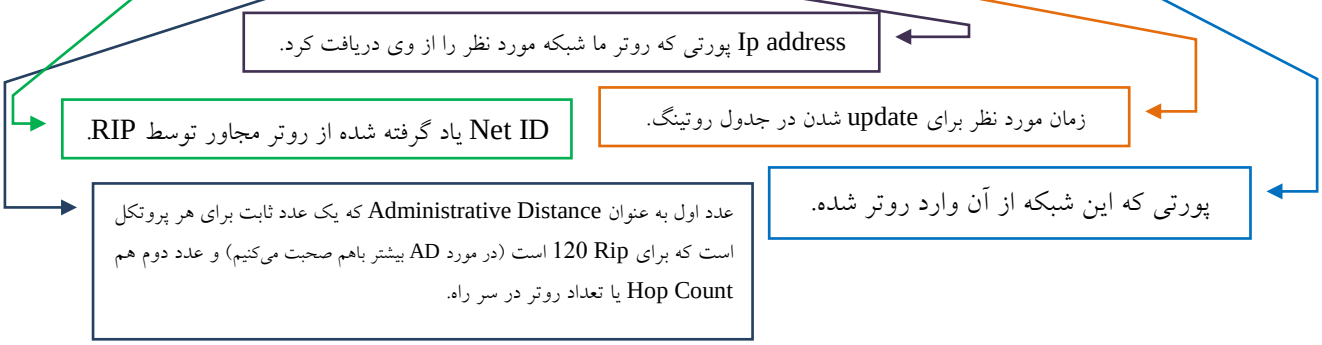
```
Router#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E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

Gateway of last resort is not set

     192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.1.0/24 is directly connected, GigabitEthernet0/0
L       192.168.1.1/32 is directly connected, GigabitEthernet0/0
R    192.168.2.0/24 [120/1] via 192.168.1.2, 00:00:01, GigabitEthernet0/0
R    192.168.3.0/24 [120/2] via 192.168.1.2, 00:00:01, GigabitEthernet0/0
     192.168.4.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.4.0/24 is directly connected, GigabitEthernet0/1
L       192.168.4.1/32 is directly connected, GigabitEthernet0/1
```

همان‌طور که مشاهده می‌کنید، جدول روتیگ با ip address های مختلفی را به ما نشان می‌دهد. شبکه‌هایی که با C شروع می‌شوند، شبکه‌های connected و متصل به روتر و شبکه‌ای که با L شروع می‌شود، IP address متصل به روتر است، اما R شبکه‌هایی هستند که از طریق پروتکل Rip وارد جدول شده‌اند و اگر به شکل توجه کنید این شبکه‌ها را از روترهای R2 و R3 یاد گرفته است، مثلاً یکی از این خط‌ها به صورت زیر است:

R 192.168.2.0/24 [120/1] via 192.168.1.2, 00:00:06, GigabitEthernet0/0



همان‌طور که مشاهده می‌کنید IP ها به صورت ClassFull در جدول روتینگ قرار دارند و این موضوع را بیان می‌کند که پروتکل Rip Version 1 از ClassLess پشتیبانی نمی‌کند. امیدوارم درباره‌ی ClassLess در قسمت IP ها مطالعه کرده باشید.

به خاطر ClassFull بودن این پروتکل(مثلاً اگر شما ip هایی در رنج کلاس b داشته باشید، مانند این ip های 172.16.1.0، 172.16.2.0، 172.16.3.0) در این صورت در معرفی Network در پروتکل Rip از این روش استفاده می‌کنید.

Network 172.16.0.0

به خاطر اینکه همه‌ی IP ها در رنج کلاس b بودند، فقط لازم است در موقع تعریف شبکه از Net ID آن استفاده کنید. این Net ID همه‌ی این IP ها را دربرمی‌گیرد. به جدول زیر توجه کنید.

172.16.0.0/16	172.16.1.0
	172.16.2.0
	172.16.3.0

تایمرها در پروتکل Rip:

- ✓ Update Timer
- ✓ Invalid Timer
- ✓ Holddown Timer
- ✓ Flush Timer

Update Timer:

این زمان، همان زمان Priodic Update است و هر 30 ثانیه یک‌بار، کل جدول روتینگ را به صورت Broadcast به ip، 255.255.255.255 می‌فرستد، البته در پروتکل Rip ver2 به صورت Multicast و به IP، 224.0.0.9 می‌فرستد.

Invalid Timer:

این تایمر زمانی اجرا می‌شود که در مورد یک شبکه، هیچ‌گونه اطلاعاتی در زمان 90 ثانیه دریافت نکند، به حالت Hold رفته و در جدول روتینگ مقابل این شبکه، جمله‌ی Posibly Down را درج می‌کند.

Holddown Timer:

این تایمر با تایمر invalid Timer باهم کار می‌کنند، هر موقع در مورد یک شبکه متریک بی‌نهایت را دریافت کند، به حالت Hold رفته و جمله‌ی Posibly Down را در کنار آن شبکه در جدول روتینگ درج می‌کند و زمان آن 180 ثانیه است.

Flush Timer:

این تایمر بعد از 270 ثانیه که تمام تایمرهای بالا به کار خود پایان دادندآن را از جدول حذف خواهد کرد. اگر update برای شبکه‌ی مورد نظر نرسد، آن را از لیست یا همان Routing Table حذف می‌کند.

این سؤال شاید برای شما پیش آید که آیا می‌شود این تایمرها را تغییر داد؟

بله این کار شدنی است و باید وارد پروتکل Rip شده و دستور زیر را وارد کنید:

```
Router(config-router)# timers basic ?
<0-4294967295>  Interval between updates
Router(config-router)#timers basic 10 ?
<1-4294967295>  Invalid
Router(config-router)#timers basic 10 50 ?
<0-4294967295>  Holddown
Router(config-router)#timers basic 10 50 90 ?
<1-4294967295>  Flush
Router(config-router)#timers basic 10 50 90 30
```

همان‌طور که مشاهده می‌کنید با دستور Timer basic می‌توان این کار را انجام داد. اولین تایمر همان Priodic Update است که به صورت پیش‌فرض 30 است و شما می‌توانید آن را تغییر دهید. در قسمت دوم، Invalid است که به‌طور پیش‌فرض 90 است و می‌توانید آن را تغییر دهید. در قسمت بعد، Holddown تایمر است که زمان آن 180 است و می‌توانید تغییر دهید و قسمت آخر، تایمر Flush است که زمان آن 270 ثانیه است و می‌توانید آن را تغییر دهید.

فرمان Debug:

این فرمان برای کنترل و عیب‌یابی به کار می‌رود و برای فعال کردن آن برای پروتکل RIP دستور زیر را در مد Privileged وارد می‌کنیم:

Router# **Debug IP Rip**

این دستور را در مثال بالا در R1 اجرا می‌کنیم:

```
Router#
Router#
Router#
Router#
Router#
Router#debug ip rip
RIP protocol debugging is on
Router#RIP: ignored v1 packet from 192.168.1.2 (illegal version)
RIP: sending  v2 update to 224.0.0.9 via GigabitEthernet0/0 (192.168.1.1)
RIP: build update entries
      192.168.4.0/24 via 0.0.0.0, metric 1, tag 0
RIP: sending  v2 update to 224.0.0.9 via GigabitEthernet0/1 (192.168.4.1)
RIP: build update entries
      192.168.1.0/24 via 0.0.0.0, metric 1, tag 0
RIP: ignored v1 packet from 192.168.1.2 (illegal version)
RIP: sending  v2 update to 224.0.0.9 via GigabitEthernet0/0 (192.168.1.1)
RIP: build update entries
      192.168.4.0/24 via 0.0.0.0, metric 1, tag 0
RIP: sending  v2 update to 224.0.0.9 via GigabitEthernet0/1 (192.168.4.1)
RIP: build update entries
      192.168.1.0/24 via 0.0.0.0, metric 1, tag 0
```

همان‌طور که مشاهده می‌کنید، این دستور اجرا شده است و تمام حرکات پروتکل Rip را در نظر دارد. این پروتکل بعد از زمان‌های مشخص نسبت به ارسال و دریافت اطلاعات اقدام می‌کند. اگر دقیق نگاه کنید، یک

ip به شماره‌ی 224.0.0.9 وجود دارد که این ip همان Multicast است که در Rip Version2 کاربرد دارد. این حالت نشان‌دهنده‌ی ارسال جدول روتینگ به این آدرس است، برای اطلاع به روترهای دیگر در شبکه RIP است.
برای اینکه این دستور را غیرفعال کنید از دستور زیر استفاده کنید:

Router#**no debug all**

راه‌اندازی پروتکل Rip Version2:

یکی از ویژگی‌های مهم Rip V2 این است که ClassLess و VLSM را پشتیبانی می‌کند و بهره‌دهی شبکه را افزایش می‌دهد.
برای اینکه در پروتکل rip از این Version استفاده کنید، در داخل Rip دستور Version 2 را وارد کنید، مانند زیر عمل کنید:

Router(config)#**router rip**
Router(config-router)#**version 2**

به همین راحتی پروتکل V1 تبدیل به V2 شد و توانایی پشتیبانی از CIDR و VLSM را دارد.

پروتکل IGRP:

قبل از اینکه این بحث را شروع کنیم، در مورد Administrative Distance کمی صحبت می‌کنیم؛ یک عدد مختص پروتکل‌های شبکه و شبکه‌های **connected** است. به جدول زیر نگاه کنید:

Route Source	Default AD
Connected interface	0
Static route	1
EIGRP	90
IGRP	100
OSPF	110
RIP	120
External EIGRP	170
Unknown	255 (this route will never be used)

Administrative Distance، معیار و ملاکی است برای انتخاب یک پروتکل از بین پروتکل‌های مختلف در یک شبکه، مثلاً اگر به یک روتر از دو طرف اطلاعات برسد و یکی از این طرف‌ها Rip با120 AD و طرف دیگر با IGRP با 100 AD است. برای انتخاب یکی از این مسیرها، مسیری که AD پایین‌تر دارد، انتخاب می‌شود (AD مخفف کلمه‌ی Administrative Distance است) و اطلاعات را از همان مسیر دریافت می‌کند. AD مربوط بهstatic route که به صورت دستی وارد می‌کردیم 1 است. در ادامه AD در شبکه را دست‌کاری می‌کنیم و کارهای مختلفی روی آن انجام می‌دهیم.

پروتکل (Interior Gateway Routing Protocol) IGRP:

این پروتکل از دسته پروتکل‌های IGPs است و سازنده‌ی آن شرکت سیسکو است. از نظر قدرت نسبت به پروتکل Rip خیلی کارآمدتر است. این پروتکل از دسته پروتکل‌هایDistance Vector است. اگر یادتان باشد در پروتکل Rip، حداکثر تعداد روترها یا همان Hop Count، 15 تا بود، اما در IGRP این عدد به 255 تغییر می‌کند و همین امر یکی از ویژگی‌های خوب این پروتکل محسوب می‌شود، اما به طور پیش‌فرض این عدد در این پروتکل 100 است.

برای محاسبه‌ی متریک این پروتکل باید کمی بیشتر کار کرد، یعنی مانند پروتکل Rip نیست که متریک از طریق تعداد روترهای سر راه تشخیص داده شود. در این پروتکل از پنج فاکتور برای محاسبه‌ی متریک استفاده می‌کنند که به شرح زیر می‌باشند.

1- Bandwidth
2- Delay
3- Load
4- MTU
5- Relibility

پروتکل IGRP به‌طور پیش‌فرض از فاکتورهای Bandwidth و Delay برای به دست آوردن بهترین مسیر استفاده می‌کند.

در مورد Bandwidth قبلاً باهم صحبت کردیم و گفتیم هر خط که Bandwidth بالاتری داشته باشد به‌عنوان بهترین مسیر انتخاب می‌شود که بالاتر بودن این فاکتور بستگی دارد به کابل و ادوات مختلف استفاده‌شده در شبکه.

در مورد Delay هم باهم صحبت کردیم که گفتیم بستگی به پورت استفاده‌شده دارد که پورت‌های GigabiteEthernet، نسبت به پورت‌های FastEthernet از زمان پاسخ‌گویی کمتری برخوردار بودند که اگر در یک شبکه، BandWidth یکی باشد به زمان Delay نگاه می‌کنند که هر چه این زمان پایین‌تر باشد، بهتر است.

این دو فاکتور را در قسمت‌های قبل کتاب و با عنوان **روش‌های انتخاب بهترین مسیر** به صورت کامل توضیح دادیم.

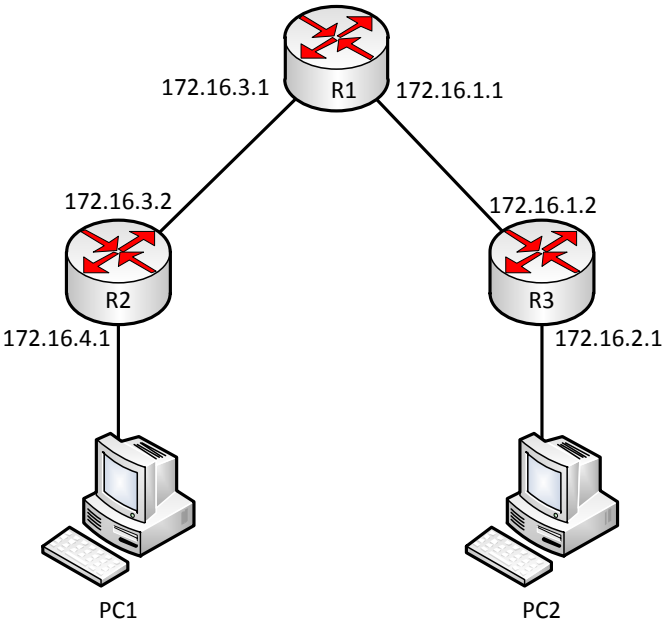
Load، عددی بین 0 تا 255 است و اگر در انتخاب یک مسیر همه‌ی فاکتورها ثابت باشند، مسیری انتخاب می‌شود که، عددی که load کمتری دارد و ترافیک کمی روی آن قرار دارد انتخاب می‌شود. همان‌طور که قبلاً گفتیم، پروتکل Rip روی حداکثر 4 خط با متریک مساوی اطلاعات را تقسیم می‌کند و روی 4 خط انتقال می‌دهد که این کار هم توسط IGRP انجام می‌شود، اما لازم نیست دارای متریک یکسانی باشند، فقط با تعریف یک رنج که به آن **variance** می‌گویند، مسیرهای متفاوت با متریک‌های متفاوت می‌توانند در این **load** شرکت کنند و حداکثر 6 خط می‌توانید استفاده کنیم.

Relibility یا اطمینان‌پذیری که بدین معنا است اگر یک خط همیشه UP باشد و مشکلی نداشته باشد، این خط از Relibility بالاتری برخوردار است و از این خط به عنوان بهترین مسیر استفاده می‌شود، به شرطی که بقیه‌ی فاکتورها ثابت باشد. این را هم اضافه کنیم که اگر یک خط Down شود و بعد Up شود، Relibility آن به نسبت خط‌های دیگر کاهش می‌یابد.

MTU به حداکثر اندازه‌ی یک پکت بر روی یک خط است که هر چه آن خط بتواند پکت با اندازه‌ی بیشتر را انتقال دهد، آن خط به‌عنوان بهترین مسیر استفاده می‌شود، اما در کل به‌ندرت استفاده می‌شود.

راه‌اندازی پروتکل IGRP:

این کار را با یک مثال انجام می‌دهیم:



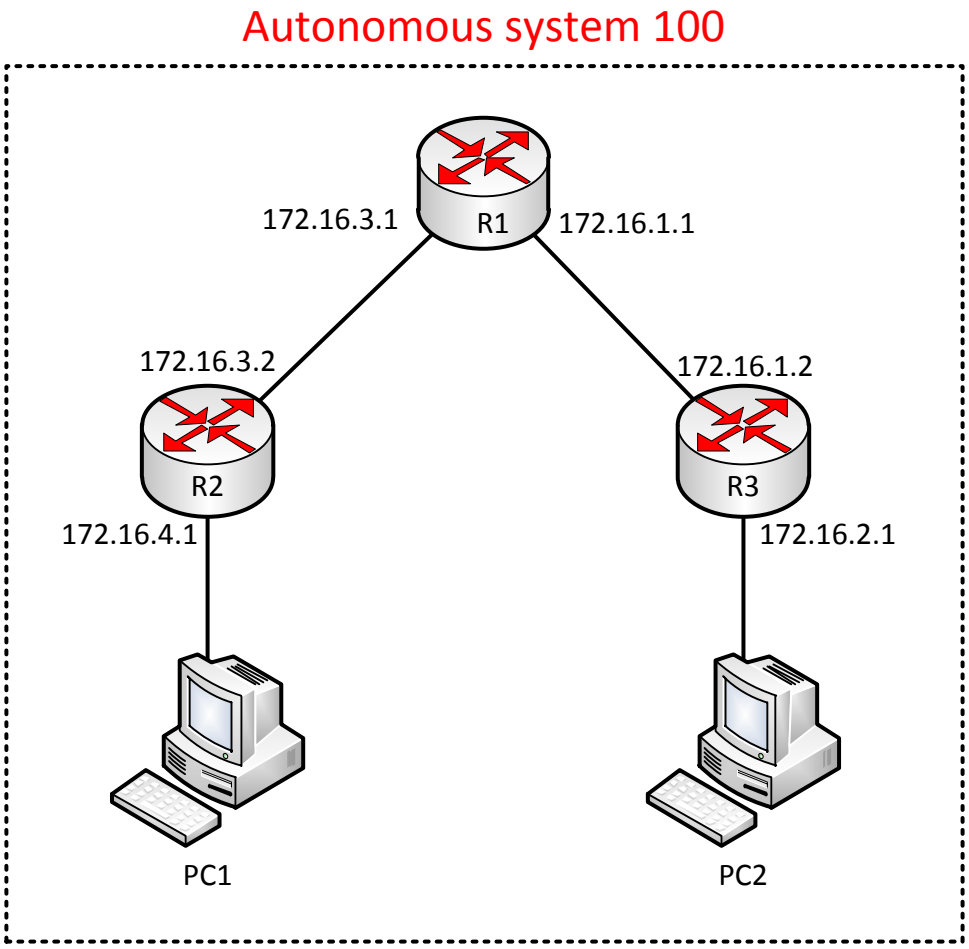
در این مثال 3 تا روتر به همراه دو PC را به هم متصل کردیم و به پورت‌های آن‌ها، طبق شکل IP داده‌ایم. حالا می‌خواهیم پروتکل IGRP را روی هر یک از روترها راه‌اندازی کنیم.

وارد روتر R1 شده و در مد Global دستور زیر را وارد کنید:

Router(config)# **Router IGRP 100**

دستور Router در تمام روتینگ پروتکل‌ها ثابت است. بعدازآن، نام پروتکل که IGRP است و بعد، شماره‌ی AS را وارد می‌کنیم. شماره‌ی 100 چیست؟

این شماره مربوط به شماره‌ی Autonomous System است و روترهایی که دارای این شماره هستند، باهم داخل یک اتاق هستند و باهم ارتباط برقرار می‌کنند. به شکل زیر توجه کنید:



همان‌طور که در شکل می‌بینید همه‌ی این روترها در AS 100 قرار دارند و باهم در ارتباط هستند. توجه داشته باشید که این شماره می‌تواند بین 1 تا 65535 باشد:

Router(config)# **router igrp ?**
<1-65535> Autonomous system number

به هر یک از روترها وارد شوید و Network های آن را تعریف کنید:

Router0(config)# **Router igrp 100**
Router0(config-Router)# network 172.16.1.0
Router0(config-Router)# network 172.16.3.0

در روترهای بعدی همین کار را انجام دهید و فقط Network های Connected مربوط به هر روتر را وارد کنید.

برای اینکه بفهمیم که روترهایی که پروتکل IGRP روی آن‌ها اجرا شده است، چه آپدیت‌هایی به هم می‌فرستند از دستور زیر در مد privileged استفاده می‌کنیم:

Router# **debug ip igrp events**

با این دستور، کل اطلاعات پروتکل IGRP پشت سر هم به صورت اتوماتیک نمایش داده می‌شود.

Router#**debug ip igrp transactions**

این دستور آپدیت‌های بین دو روتر که پروتکل IGRP روی آن‌ها اجرا شده است را نمایش می‌دهد.

برای غیرفعال کردن هر دو دستور از فرمان No Debug All استفاده کنید، البته با اجرای این دستور تمام دستوراتی که با debug نوشته شده‌اند، غیرفعال می‌شوند.

برای محاسبه‌ی Bandwith باید از فرمول زیر استفاده کنید:

$$\left[\left(K_1 \cdot \text{Bandwidth}_E + \frac{K_2 \cdot \text{Bandwidth}_E}{256 - \text{Load}} + K_3 \cdot \text{Delay}_E\right) \cdot \frac{K_5}{K_4 + \text{Reliability}}\right] \cdot 256$$

در فرمول بالا، حرف K را مشاهده می‌کنید که برای اینکه آن‌ها را پیدا کنیم باید از دستور Show ip protocol استفاده کنیم.

Router#**show ip protocol**

Routing Protocol is "Eigrp 100 "
Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
Default networks flagged in outgoing updates
Default networks accepted from incoming updates
EIGRP metric weight K1=1, K2=0, K3=1, K4=0, K5=0
EIGRP maximum hopcount 100
EIGRP maximum metric variance 1
Redistributing: eigrp 100

```
  Automatic network summarization is in effect
  Automatic address summarization:
  Maximum path: 4
  Routing for Networks:
    192.168.1.0
    192.168.2.0
  Routing Information Sources:
    Gateway         Distance      Last Update
Distance: internal 90 external 170
Router#
```

نکته‌ی بسیار مهم: این پروتکل توسط سیسکو از نسخه‌ی IOS 12.3 به بعد، جای خود را به پروتکل Eigrp داده و از دنیای پروتکل‌ها خداحافظی کرده است.

تایمرها در پروتکل IGRP:

Update Timer:

در این پروتکل زمان ارسال کل جدول روتینگ برای روترهای مجاور 90 ثانیه است که به این آپدیت، Priodic Update می‌گفتیم.

Invalid timers:

این تایمر به صورت پیش‌فرض، سه برابر **Update Timer** است که سه برابر **Update Timer** می‌شود، 270 ثانیه.

Holddown timers:

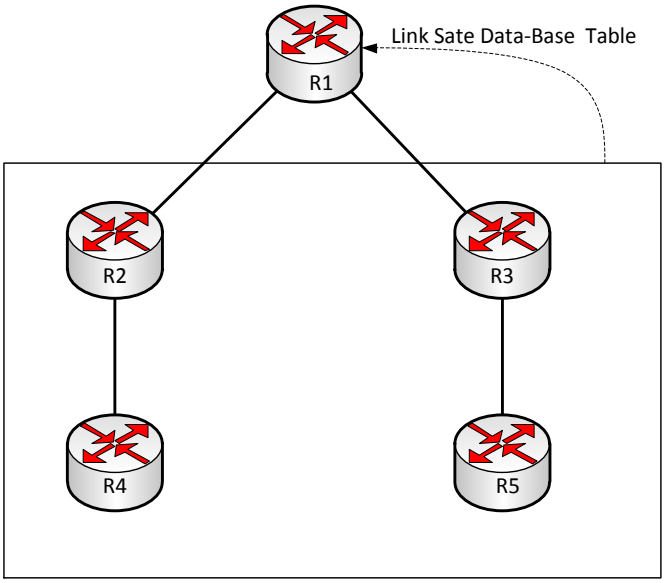
این تایمر هم، سه برابر تایمر **Update Timer** است و به علاوه 10 ثانیه بیشتر از آن، یعنی در کل 280 ثانیه.

Flush timers:

این تایمر که برای حذف یک شبکه از جدول روتینگ استفاده می‌شود، 7 برابر تایمر **Update Timer** است که در کل می‌شود، 630 ثانیه است.

پروتکل‌های Link State:

این نوع پروتکل، یک ویژگی عمده دارند و آن‌هم این است که تصویر کلی از شبکه یا همان گراف کامل از شبکه را دارند، یعنی هر روتر دارای پروتکل‌های Link State خود را به عنوان ریشه‌ی درخت و بقیه را به عنوان شاخه و برگ حساب می‌کند، اما بدون دور است و به‌این‌ترتیب یک تصویر کلی از شبکه را دارد و از روی همین گراف، بهترین و کوتاه‌ترین مسیر تا شبکه‌ی دیگر را محاسبه و انتخاب می‌کند. به شکل زیر توجه کنید:



در این شکل، روتر R1 با استفاده از گراف از نقشه‌ی کل شبکه خبر دارد و بر طبق همین نقشه به بهترین مسیر دست پیدا می‌کند، شاید کمی گیج‌کننده باشد، اما در ادامه، کاملاً با این پروتکل‌ها آشنا می‌شویم، پروتکلی که در این دسته قرار دارند، OSPF(Open Shortest Path First) است که به صورت مفصل روی این پروتکل بحث خواهیم کرد.

پروتکل‌ها از نوع Link State از سه جدول تشکیل شده‌اند:

- Routing Table
- Link state Data-base
- Neighbor Table

در روترهایی که این نوع پروتکل‌ها اجرا می‌شوند، 3 جدول داخل آن‌ها تشکیل می‌شود که در جدول اول که Neighbor است، اطلاعات شبکه‌های روترهای مجاور در آن ثبت می‌شود و بعد از آن این جدول به صورت آپدیت به روترهای دیگر فرستاده می‌شود و تشکل جدول Link Sate Data-Base می‌دهند. بعد از آن الگوریتم

بهترین مسیر با عنوان SPF که مخفف Shortest Path First است، اجرا می‌شود و شبکه را به صورت یک درخت بدون دور درمی‌آورد و بهترین مسیر را به صورت روش‌های خاصی پیدا می‌کند.
پروتکل‌های OSPF و ISIS از دسته پروتکل Link state هستند.

پروتکل‌های Hybrid:

این دسته از پروتکل‌ها از دو ویژگی پروتکل‌های بالا استفاده می‌کند، یکی اینکه از کل اطلاعات شبکه به صورت درخت بدون دور خبر دارد، مانند پروتکل Link state و از روتر مجاورش، اطلاعات شبکه‌ی غیر محلی را دریافت می‌کند و از روتر مورد نظر تا شبکه‌ی مورد نظر از یک بردار خطی استفاده می‌کند، مانند پروتکل‌های Distance Vector. از جمله‌ی این پروتکل‌ها که در این گروه قرار دارد، پروتکل Eigrp است که با هم آن را بررسی می‌کنیم.

پروتکل (Enhanced Interior Gateway Routing Protocol) EIGRP:

یکی از محبوب‌ترین پروتکل‌ها در دنیای امروز است و فقط روی دستگاه‌های سیسکو کاربرد دارد، یعنی اینکه این پروتکل ساخت سیسکو است و فقط روی ادوات سیسکو کار می‌کند، یکی از پرسرعت‌ترین پروتکل‌ها است که سرعت convergence یا هماهنگی بسیار بالایی دارد.

ویژگی‌های پروتکل EIGRP:

- از خانواده‌ی Distance Vector است، چون از یک بردار خطی برای رسیدن به شبکه‌ی مورد نظر استفاده می‌کند.
- از خانواده‌ی Link state هم است، چون نقشه‌ی کامل شبکه را برای پیدا کردن بهترین مسیر در دست دارد.
- این پروتکل برگرفته از پروتکل **IGRP** است که سیسکو آن را بازسازی کرده و سرعت آن را افزایش داده است و ویژگی‌های دیگری نیز به آن اضافه کرده است.
- پشتیبانی از VLSM / CIDR.
- پشتیبانی از پروتکل‌های IP , IPx , Apple Talk.
- انتخاب بهترین مسیر از طریق الگوریتم انتشار مسیر **Dual(**Diffusing Update Algorithm**)**.
- از دسته پروتکل‌های IGPs که داخل یک AS کار می‌کند.

پروتکل Eigrp از چندین جدول تشکیل شده است:

جدول Topology Database Table:

کل نقشه‌ی شبکه در این جدول ثبت می‌شود و یکی دیگر از ویژگی‌های آن، استفاده از مسیرهای BackBone در این جدول است، یعنی اگر مسیر اصلی Down شود از مسیرهای دیگری که در این جدول ذخیره شده است، استفاده می‌کند.

جدول Routing Table:

در این جدول، بعد از محاسبات الگوریتم Dual، کوتاه‌ترین مسیر به شبکه به دست می‌آید و در این جدول قرار می‌گیرد.

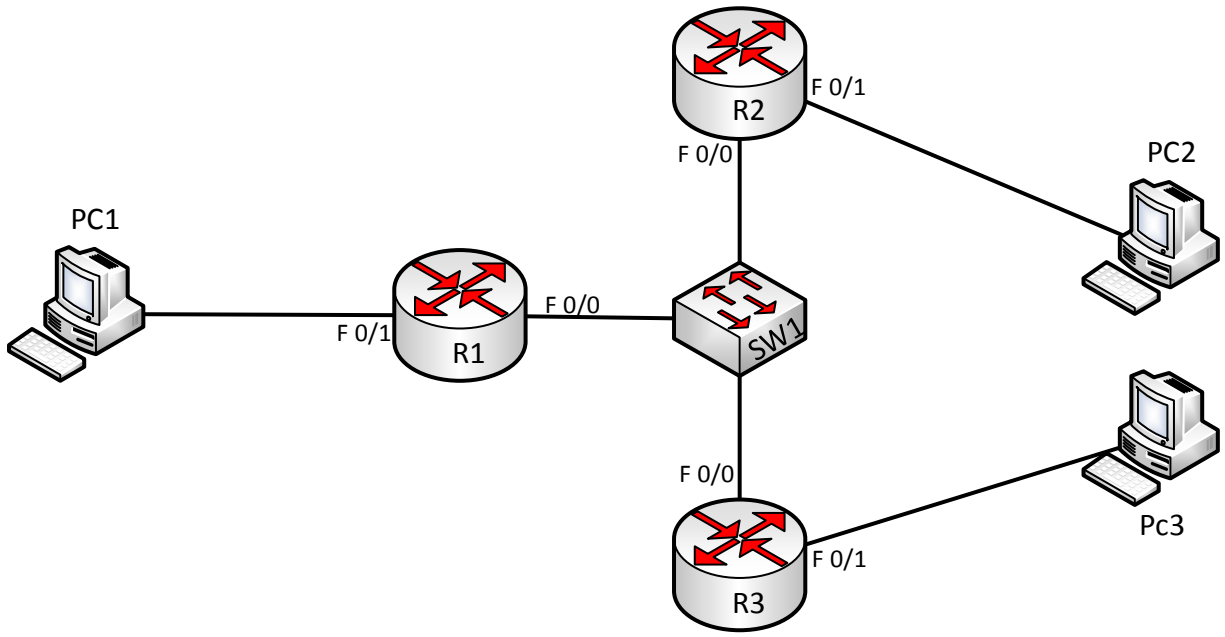
جدول Neighbors Table:

در این جدول، اطلاعات روترهای همسایه که به صورت Connected به روتر اصلی متصل هستند، قرار می‌گیرد.
زمانی که از الگوریتم EIGRP استفاده می‌کنیم، این الگوریتم فقط برای اطلاع دادن از update جدید از بسته‌های Hello Packet استفاده می‌کند و به خاطر همین از پهنای باند کمتری استفاده می‌کنند، یعنی برخلاف الگوریتم‌های Distance Vector، وقتی در جدول روتینگ تغییری ایجاد شود، کل جدول روتینگ را برای روترهای همسایه ارسال نمی‌کند، یعنی Priodic Update ارسال نمی‌کند و فقط همان تغییر را بلافاصله به دیگر روترها در شبکه اطلاع می‌دهد.
به این پروتکل، پروتکل Distance Vectore پیشرفته هم می‌گویند، به دلیل داشتن ویژگی‌هایDistance Vectore و Link State.
برای محاسبه‌ی متریک باید به متریک IGRP مراجعه کنید که دقیقاً همان متریک است و فقط باید عددی که به دست می‌آید در 255 ضرب شود.
فاکتورهای انتخاب مسیر هم، مانند IGRP است، اما به صورت پیش‌فرض از Bandwidth و Delay برای انتخاب بهترین مسیر استفاده می‌شود.
سرعت Convergence (هماهنگی با روترهای دیگر) به نسب الگوریتم IGRP خیلی بیشتر است، به خاطر اینکه وقتی الگوریتم Dual به دنبال بهترین مسیر می‌گردد و مسیرهای دیگر را هم به همراه مسیر اصلی در جدول Routing ثبت می‌کند و اگر مسیر اصلی Down شود، مسیر دیگر که به عنوان مسیر Backup است، به جای آن مسیر شروع به کار می‌کند و این در صورتی است که الگوریتم Dual برای به دست آوردن بهترین مسیر، دوباره اجرا نمی‌شود، چون قبل از آن، مسیر را پیدا کرده بود و این یکی از ویژگی‌های مهم این پروتکل است.
نکته: به مسیر اصلی در Eigrp، successor می‌گویند و به مسیر فرعی یا Backup، Feasible Successor می‌گویند.

کار با پروتکل Eigrp:

این پروتکل برای شبکه‌های بزرگ، بسیار کاربرد دارد و بسیار خوب عمل می‌کند. برای فعال کردن این پروتکل، یک مثال را باهم انجام می‌دهیم.

مثال: سه روتر 2811، یک سوئیچ 2960 و سه PC را به صورت زیر به هم متصل کنید.



IP ها را به صورت جدول زیر وارد کنید:

	F 0/0	F0/1
R1	192.168.1.1/24	192.168.2.1/24
R2	192.168.2.2/24	192.168.3.1/24
R3	192.168.2.3/24	192.168.4.1/24
PC1	192.168.1.2/24	
PC2	192.168.3.2/24	
PC3	192.168.4.2/24	

بعد از واردکردن IP ها در interface مورد نظر و روشن کردن interface با دستور ،Ping شبکه را تست کنید تا متصل بودن به شبکه‌ی روبرو انجام شده باشد.

حالا باید بین روترها، پروتکل Eigrp را راه‌اندازی کنیم. برای این کار وارد R1 می‌شویم و دستور زیر را وارد می‌کنیم:

Router(config)#**router Eigrp ?**
<1-65535> Autonomous system number

Router Eigrp را وارد کردیم و بعدازآن از علامت سؤال استفاده کردیم که به ما تعداد AS های موجود را نشان می‌دهد. AS یا همان **Administrative Distance**، عددی برای ایجاد یک منطقه برای ارتباط روترها باهم است، یعنی هر پروتکل Eigrp در هر روتر از یک عدد مشابه استفاده کند با روترهای دیگر در یک منطقه قرار می‌گیرند و باهم ارتباط دارند.

Router(config)#**router eigrp 200**

با دستور بالا، Eigrp 200 را ایجاد و وارد آن می‌شویم و بعد..

Router(config-router)#**no auto-summary**

همان‌طور که در اوایل این درس بیان کردیم، Eigrp یک پروتکل Class Less است و برای همین از این دستور برای جلوگیری از ثبت IP ها به صورت Class Full جلوگیری می‌کنیم.

Router(config-router)# **network 192.168.1.1 ?**
A.B.C.D EIGRP wild card bits

این قسمت، برای واردکردن اینترفیس‌های Connected به روتر است که کمی با پروتکل‌های قبلی تفاوت دارد. اول، دستور Network، بعد ip مورد نظر را به صورت کامل وارد می‌کنیم، در قدم بعدی، باید Mask Wild Card را وارد کنیم. این عدد برعکس Subnet Mask است که باید به صورت 0.0.0.255 وارد شود، یعنی قسمت آخر ip که تغییر می‌کند را وارد کنیم که به صورت زیر می‌شود:

Router(config-router)#network 192.168.1.1 0.0.0.255

شما می‌توانید به جای نوشتن ،Wild Card Mask فقط چهارتا صفر قرار دهید، به خاطر اینکه IP ها ثابت است و تغییری ندارد و می‌خواهیم به صورت Class Less به شبکه تزریق شود:

Router(config-router)#network 192.168.1.1 0.0.0.0
Router(config-router)#network 192.168.2.1 0.0.0.0

تا اینجا بر روی روتر R1، پروتکل EIGRP را با شماره‌ی AS 200 راه‌اندازی کردیم و Network های مربوط به خودش را هم وارد کردیم.

نکته: وقتی Network را در یک پروتکل تعریف می‌کنیم، به معنای این نیست که Network را به پروتکل دادیم، به معنای این است که پروتکل را روی این Network راه‌اندازی کردیم، پس به این نکته توجه کنید.

تنظیمات را در روترهای دیگر هم انجام می‌دهیم.

تنظیمات روی روتر R2:

```
Router(config)#Router Eigrp 200
Router(config-router)#no auto-summary
Router(config-router)#network 192.168.2.2 0.0.0.0
%DUAL-5-NBRCHANGE: IP-EIGRP 200: Neighbor 192.168.2.1 (FastEthernet0/0) is up: new
adjacency
Router(config-router)#network 192.168.3.1 0.0.0.0
```

همان‌طور که مشاهده می‌کنید در این روتر هم Eigrp 200 تعریف کردیم، چون همان‌طور که گفتیم روترها باید در یک eigrp و یا در یک AS قرار گیرند تا باهم در ارتباط باشند.

همان‌طور که مشاهده می‌کنید، بعد از واردکردن Network 192.168.2.2، سریع پیغامی نمایش داده است که می‌گوید، الگوریتم Dual یک مسیر به شماره‌ی 192.168.2.1 پیدا کرده که این پروتکل روی آن اجرا شده است.

در روتر R3 هم تنظیمات مربوط به آن را وارد کنید:

```
Router(config)#router eigrp 200
Router(config-router)#no auto-summary
Router(config-router)#network 192.168.2.3 0.0.0.0
%DUAL-5-NBRCHANGE: IP-EIGRP 200: Neighbor 192.168.2.1 (FastEthernet0/0) is up: new
adjacency

%DUAL-5-NBRCHANGE: IP-EIGRP 200: Neighbor 192.168.2.2 (FastEthernet0/0) is up: new
adjacency
Router(config-router)#network 192.168.4.1 0.0.0.0
```

در این قسمت، به ما دو پیام نمایش داده شده که می‌گوید 2 تا پروتکل روی این اینترفیس‌ها فعال شده است.

تا اینجا روی همه روترها، پروتکل EIGRP را اجرا کرده‌ایم، در این قسمت با اجرای دستور زیر جدول روتینگ را بررسی می‌کنیم

دستور show ip Route**:**

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

```
Gateway of last resort is not set
D   192.168.1.0/24 [90/30720] via 192.168.2.1, 00:04:48, FastEthernet0/0
C   192.168.2.0/24 is directly connected, FastEthernet0/0
D   192.168.3.0/24 [90/30720] via 192.168.2.2, 00:04:47, FastEthernet0/0
C   192.168.4.0/24 is directly connected, FastEthernet0/1
```

با دستور **show ip Route**، جدول روتینگ نمایش داده شده است که اگر به جدول توجه کنید، دو شبکه را دریافت کرده که با حرف D شروع می‌شوند. حرف D به معنای Eigrp است و نشان‌دهنده‌ی این است که از روترهای دیگر این شبکه‌ها را یاد گرفته، شبکه‌های پشت روترهای R2 و R3 را یاد گرفته است. در روترهای دیگر هم به همین صورت است.

دستور show ip eigrp neighbors:

برای نمایش همسایگی (Neighbors)، باید از دستور زیر در مد Privileged استفاده کنید:

```
Router# show ip eigrp neighbors
IP-EIGRP neighbors for process 200
H  Address         Interface    Hold Uptime    SRTT  RTO  Q  Seq
                                (sec)          (ms)       Cnt Num
0  192.168.2.1     Fa0/0        13  00:44:14  40    1000 0  6
1  192.168.2.3     Fa0/0        11  00:39:02  40    1000 0  7
```

این دستور در روتر R2 وارد شده است و نتیجه‌ی آن را مشاهده می‌کنید؛ لیست Ip هایی که با آن‌ها ارتباط همسایگی دارد را نمایش داده است.

دستور Show Ip Eigrp Interface:

این دستور برای نمایش اطلاعات interface هایی است که پروتکل EIGRP روی آن فعال شده است. این دستور را در R2 وارد می‌کنیم:

```
Router#show ip eigrp interface
IP-EIGRP interfaces for process 200

                Xmit Queue   Mean   Pacing Time   Multicast    Pending
Interface       Peers  Un/Reliable  SRTT  Un/Reliable  Flow Timer  Routes
Fa0/0           2          0/0      1236  0/10         0       0
Fa0/1           0          0/0      1236  0/10         0       0
```

به نتیجه‌ی کار دقت کنید، اگر به Fa0/0 دقت کنید، نوشته است، PEER 2، یعنی اینکه از طریق اینترفیس Fa0/0 توانسته دو تا Neghibors را یاد بگیرد، Neighbors همان اینترفیس‌های روترهای همسایه هستند که روی آن‌ها Eigrp راه‌اندازی شده است.

دستور Show ip eigrp Topology:

این دستور کل اطلاعات جدول توپولوژی را به شما نمایش می‌دهد و می‌گوید که شبکه را از کدام مسیر دریافت کرده و...

Router# **show ip eigrp topology**
IP-EIGRP Topology Table for AS 200
Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,r - Reply status

P 192.168.2.0/24, 1 successors, FD is 28160
via Connected, FastEthernet0/0
P 192.168.3.0/24, 1 successors, FD is 28160
via Connected, FastEthernet0/1
P 192.168.4.0/24, 1 successors, FD is 30720
via 192.168.2.3 (30720/28160), FastEthernet0/0
P 192.168.1.0/24, 1 successors, FD is 30720
via 192.168.2.1 (30720/28160), FastEthernet0/0

اگر به گزینه‌ی اول نگاه کنید، می‌گوید شبکه‌ی 192.168.2.0 یک مسیر successor است، یعنی یک مسیر اصلی است و از طریق اینترفیس FastEthernet 0/0 وارد همین روتر که داخل آن هستیم، شده است. بقیه هم به همین صورت است، پس نتیجه می‌گیریم که این جدول، کل اینترفیس‌هایی را به ما نشان می‌دهد که Eigrp روی آن‌ها Run شده است.

دستور Show ip eigrp Traffic:

این دستور نشان‌دهنده‌ی پکت‌های دریافتی و ارسالی است، مانند زیر:

Router#**show ip eigrp traffic**
IP-EIGRP Traffic Statistics for process 100
Hellos sent/received: 0/0
Updates sent/received: 0/0
Queries sent/received: 0/0
Replies sent/received: 0/0
Acks sent/received: 0/0
Input queue high water mark 1, 0 drops
SIA-Queries sent/received: 0/0
SIA-Replies sent/received: 0/0

پروتکل OSPF:

پروتکل OSPF(Open Shortest Patch First) یک پروتکل آزاد است و مختص شرکت خاصی نیست و توسط سازمان IETF در سال 1988 نوشته شده است، مانند Eigrp نیست که فقط در روترهای سیسکو قابل اجرا باشد، بلکه در تمام روترهای شرکت‌های مختلف کاربرد دارد.

پس اگر شما در شبکه‌های خود از روترهای مختلف با برندهای مختلف استفاده کنید، نمی‌توانید روی آن‌ها Eigrp اجرا کنید، بلکه فقط باید پروتکل OSPF یا RIP روی آن‌ها run کنید تا بتوانند باهم دیگر ارتباط برقرار کنند.

این پروتکل از مجموعه پروتکل‌های Link state است و زیرمجموعه‌ی پروتکل‌های IGPs است، یعنی داخل یک AS کار می‌کنند.

الگوریتمی که در این پروتکل استفاده می‌شود، Dijkstra است که شبکه را به صورت یک درخت بدون دور در نظر می‌گیرد.

Ospf که در این قسمت بررسی می‌کنیم، Ospf Version 2 است که با IPV4 کار می‌کند و در آخر کتاب، در قسمت IPV6 از OSPF Version 3 استفاده می‌شود.

Ospf از جدولی به نام Link-satate Dtabase استفاده می‌کند که کل اطلاعات شبکه یا نقشه‌ی شبکه را برای انتخاب کوتاه‌ترین مسیر در خود ذخیره می‌کند و برای به دست آوردن کوتاه‌ترین مسیر از الگوریتمی به نام SPF استفاده می‌کند و بعد از پیدا شدن مسیر، آن را در جدول دیگری به نام Routing Table ذخیره می‌کند.

OSPF برای ارسال آپدیت از بسته‌هایی به نام LSA (Link-state Advertisement) استفاده می‌کند که اطلاعات جدول خود را به نام Link-state Database به روترهای دیگر ارسال می‌کند.

اگر کتاب را تا اینجا کامل خوانده باشید، گفتیم که پروتکل‌های Distance Vectore برای ارسال Update کل جدول را به روترهای همسایه ارسال می‌کردند که به عنوان Priodic Update بود، اما در OSPF این‌چنین نیست.

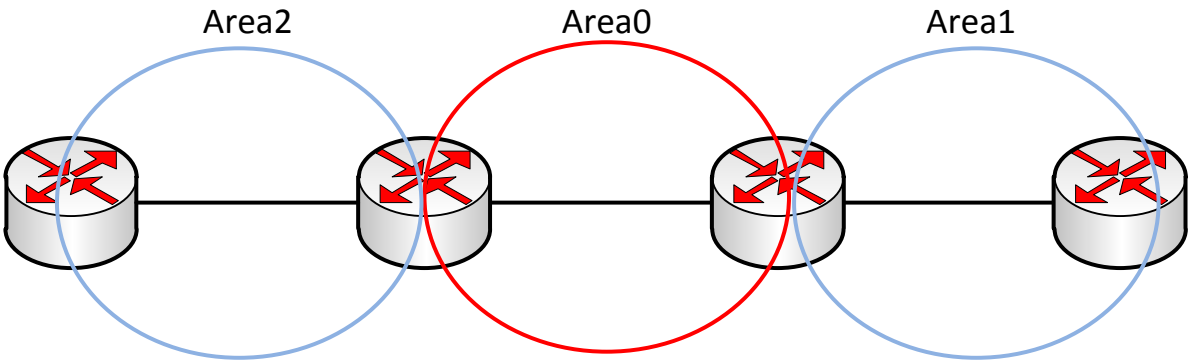
اگر تغییری در جدول ایجاد شود، این تغییر بلافاصله از طریق LSA که بالا توضیح دادیم به بقیه‌ی روترها خبر داده می‌شود و خیلی کم از پهنای باند شبکه استفاده می‌کند، به این آپدیت، Triggered Update می‌گویند که تغییرات را بسیار سریع اعلام می‌کند.

باید گفت: این‌گونه هم نیست که ospf نخواهد کل جدول را هرگز ارسال نکند، این کار را هر 30 دقیقه یک‌بار انجام می‌دهد که کل جدول Database را به شبکه‌ی مورد نظر ارسال می‌کند.

این پروتکل برای شبکه‌های بزرگ بسیار کارآمد است و در حال حاضر در حال استفاده در شبکه‌های بزرگ است.

OSPF شبکه‌های بزرگ را به ناحیه‌های(Area) مختلف تقسیم می‌کند که دلایل خاص خودش را دارد:

- با ایجاد ناحیه، سرعت کار این الگوریتم بسیار افزایش پیدا می‌کند.
- کم حجم شدن جدول Routing به خاطر ایجاد ناحیه.
- مدیریت بر چند روتر بهتر از مدیریت بر چندین روتر است.
- با ایجاد ناحیه، اگر یکی از روترها دستکاری یا مشکلی برای آن پیش بیاید، بقیه‌ی روترها در ناحیه‌ی دیگر بدون مشکل به کار خود ادامه می‌دهند.



BackBone Area یا Area0 ناحیه‌ای است که area های دیگر به وی متصل می‌شوند و تمام اطلاعات area های دیگر باید از این area رد شود، پس این area به‌عنوان BackBone یا ستون فقرات شبکهOSPF شناخته می‌شود. به طور خلاصه می‌توان گفت این area پادشاه همه‌ی area هاست.

نکته: اگر دسته بندی یا ناحیه در OSPF وجود نداشت، الگوریتم SPF که کار پیدا کردن کوتاه‌ترین مسیر را انجام می‌دهد با مشکل مواجه می‌شود، چون جدول Database که گراف شبکه در آن قرار دارد، بسیار بزرگ می‌شود. توجه داشته باشید با ایجاد یک area، الگوریتم SPF فقط در همان Area پردازش خود را انجام می‌دهد و بر کل شبکه تأثیر ندارد، پس الگوریتم SPF(Shortest Path First)، فقط در یک Area پردازش خود را انجام می‌دهد و زمانی که به نتیجه برسد، این نتیجه را با area های دیگر در میان می‌گذارد.

انتخاب بهترین مسیر در OSPF:

در ospf انتخاب بهترین مسیر از طریق متریکی به نام Cost انجام می‌شود که از طریق الگوریتم SPF کوتاه‌ترین مسیر به دست می‌آید.

این نکته را توجه داشته باشید که هر چه پهنای باند یک خط بیشتر باشد، cost آن کمتر است، پس پهنای باند رابطه‌ی معکوس با cost دارد.

برای به دست آوردن Cost باید 1000000000 را تقسیم‌بر مقدار پهنای باند کنیم تا عدد مورد نظر به دست آید.

راه‌اندازی پروتکل ospf:

برای فعال کردن پروتکل ospf باید از دستور زیر به همراه یک Proccess ID استفاده کنیم:

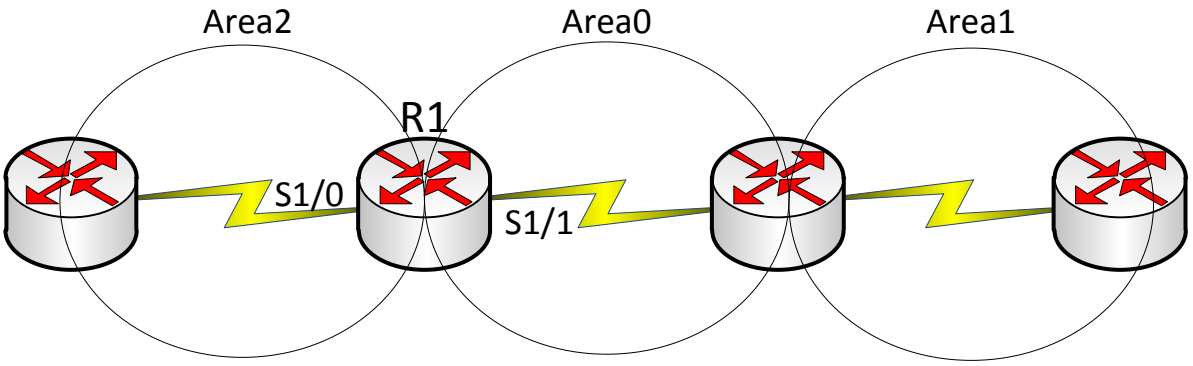
```
Router(Config)# router ospf ?
<1-65535>  Process ID
```

در پروتکل EIGRP، شماره‌ای که اختصاص می‌دهیم، باید در همه‌ی روترها یکی باشد، اما شماره‌ای که به این پروتکل داده می‌شود، لازم نیست که در همه‌ی روترها یکی باشد؛ از شماره 1 تا 65535 می‌توانید اختصاص دهید، پس مانند AS ها نیستند که باید در همه‌ی روترها یکی باشد. این عدد فقط برای متمایز کردن OSPF ها باهم است.

برای تعریف کردن NETWORK، باید از روش زیر استفاده کنید.

```
Router(config-router)#Network 192.168.1.1 0.0.0.0  area0
```

برای تعریف شبکه، IP Address را وارد می‌کنیم، بعد Wild Card Mask را و بعدازآن مشخص می‌کنیم که این شبکه در کدام Area یا ناحیه قرار دارد. به شکل نگاه کنید، اگر توجه داشته باشید Se 1/1 مربوط به R1 در area 0 قرار دارد، پس اگر وارد این روتر شدیم در موقع تعریف شبکه در پروتکل OSPF باید آن را داخل Area0 قرار دهیم، مثلاً در سمت دیگر، روتر R1 پورت سریال Se1/0 در area2 قرار دارد که باید در تعریف شبکه‌ی این پورت در area2 قرار دهیم.



در مورد Wild Card Mask که باهم در پروتکل Eigrp صحبت کردیم، گفتیم که این عدد برعکس Subnet Mask است و بعدازآن گفتیم که لازم نیست که Wild Card Mask بنویسید، فقط به جای Wild Card Mask از چهار تا صفر استفاده کنید.

Router ID:

نشان‌دهنده‌ی یک روتر در شبکه‌ی OSPF است که برای ارتباط روترها باهم در پروتکل OSPF از این شناسه استفاده می‌کنند. از این به بعد Router ID را خلاصه می‌کنیم و از RID استفاده می‌کنیم.

این ip از بین ip های یک روتر انتخاب می‌شوند که بزرگ‌ترین ip آدرس باشد. همان‌طور که می‌دانید این اینترفیس‌ها که ip روی آن‌ها Set شده است به صورت فیزیکی می‌باشند و زمانی که Down شوند، بر روی کارکرد پروتکل OSPF تأثیرگذار است و باعث مشکل در شبکه می‌شود. برای حل این مشکل باید از یک اینترفیس مجازی استفاده کرد که هیچ وقت Down نمی‌شود، این اینترفیس، loopback است که در قسمت‌های قبل کتاب با این اینترفیس کار کردیم.

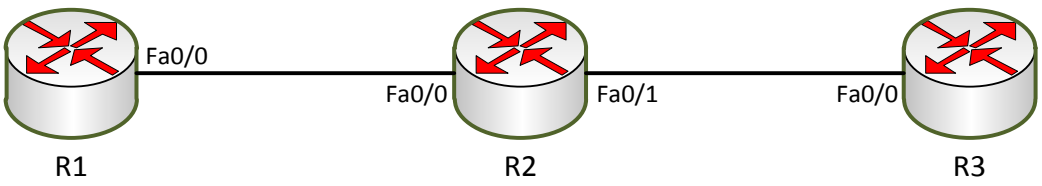
نکته: اگر شما از چندین Loopback استفاده کنید، RID از بین آن‌هایی انتخاب می‌شود که بالاترین IP Address را دارند.

روترهای DR و BDR:

در شبکه‌های تحت OSPF، روتری تحت عنوان **DR (Designated Router)** وجود دارد که همه‌ی روترهای داخل یک Area، تمام اطلاعات و تغییرات را به این روتر می‌فرستند و این روتر به دیگر روترها اعلام می‌کند، یعنی اینکه هر روتر هر تغییری را به همه‌ی روترها ارسال نمی‌کند که باعث ایجاد بار سنگین در شبکه شود، فقط اطلاعات خود را به روتر اصلی در شبکه، یعنی DR می‌فرستد و DR پخش می‌کند، اما اگر این روتر از کار بیفتد، چه باید کرد؟ اگر این روتر down شود، روتری که BDR(**BackBone Designated Router**) است به جای این روتر کار می‌کند و تمام اطلاعات به این روتر ارسال می‌شود.

نکته: درصورتی‌که تغییری در شبکه ospf رخ دهد، این تغییر از طریق LSU به روترهای DR و BDR فرستاده می‌شود، پس توجه داشته باشید که هر چه در روتر DR وجود دارد در روتر BDR هم وجود دارد.

نکته بسیار مهم: روتر DR و BDR در هر Area وجود دارند، اما بین هر Subnet قرار دارند. به شکل زیر توجه کنید.

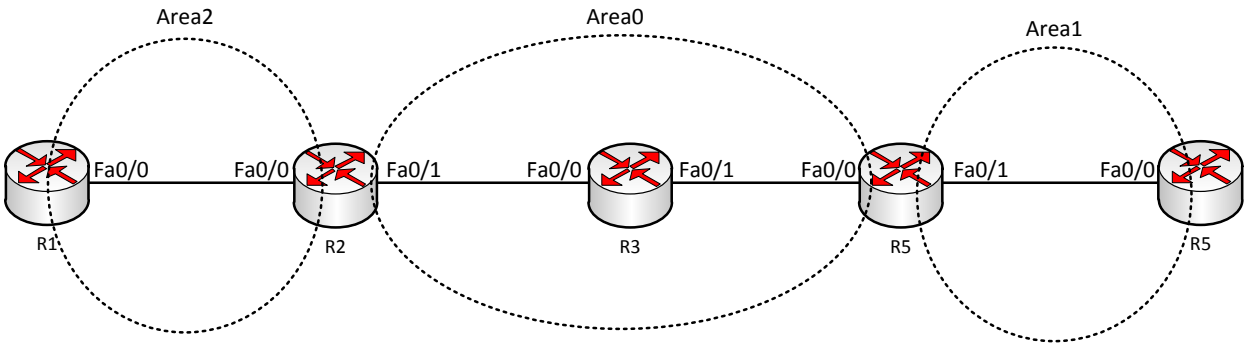


روترهای DR و BDR بین دو Subnet انتخاب می‌شود، یعنی اینکه در شکل بالا بین روترهای R1 و R2 یک آدرس 172.16.1.0 وجود دارد که بین این دو روتر، روتری به عنوان DR انتخاب می‌شود که ip address بزرگ‌تری داشته باشد، البته یک فاکتور دیگر در انتخاب روترهای DR و BDR وجود دارد که خیلی مهم‌تر از بقیه‌ی فاکتورها است و آن هم، Priority است که اگر Priority یک روتر از روتر دیگر بزرگ‌تر باشد، همان روتر به‌عنوان DR انتخاب می‌شود، اما به صورت پیش‌فرض Priority=1 است و به خاطر همین از ip address برای انتخاب روترهای DR و BDR استفاده می‌کند.

مثال 3:

در این مثال، نحوه‌ی راه‌اندازی پروتکل OSPF را باهم کار می‌کنیم.

چهار روتر را به لیست اضافه کنید و به صورت زیر به هم متصل کنید.



	Fa0/0	Fa0/1	LoopBack
R1	172.16.1.1/16		150.1.1.1/24
R2	172.16.1.2/16	172.16.2.1/16	150.1.2.2/24
R3	172.16.2.2/16	172.16.3.1/16	150.1.3.3/24
R4	172.16.3.2/16	172.16.4.1/16	150.1.4.4/24
R5	172.16.4.2/16		150.1.5.5/24

بعد از تخصیص IP ها به صورت جدول بالا در روتر باید پروتکل OSPF را راه‌اندازی کنیم:

روتر R1 :

Router(config)#**router ospf 20**

تعریف Router OSPF 20 که 20 یک شماره‌ی شناسایی برای این پروتکل است که تأثیری در روند کار ندارد، اما باید تعریف شود.

Router(config-router)#**router-id 150.1.1.1**

در این قسمت باید RID روتر را تعریف کنید که این IP مربوط به اینترفیس LoopBack است، پس بعد از ورود به پروتکل OSPF در درجه‌ی اول RID را تعریف کنید.

Router(config-router)#**network 172.16.1.1 0.0.0.0 area 2**

در این قسمت Network های مربوط به روتر را تعریف می‌کنیم و می‌گوییم که در کدام area قرار دارد، مثلاً در این قسمت، اینترفیس Fa0/0 روتر R1 در Area2 قرار دارد. در تعریف Network، اول خود Ip و بعد، Wild Card MASk مربوط به آن را وارد می‌کنیم که همان‌طور که در مطالب قبلی کتاب گفتیم، سعی کنید به جای Wild Card Mask از چهار صفر استفاده کنید (0.0.0.0).

در بقیه‌ی روترها هم همین کار را انجام دهید:

روتر R2:

```
Router(config)#router ospf 10
Router(config-router)#router-id 150.1.2.2
Router(config-router)#network 172.16.1.2 0.0.0.0 area 2
Router(config-router)#network 172.16.2.1 0.0.0.0 area 0
```

روتر R3:

```
Router(config)#router ospf 10
Router(config-router)#router-id 150.1.3.3
Router(config-router)#net 172.16.2.2 0.0.0.0 area 0
Router(config-router)#net 172.16.3.1 0.0.0.0 area 0
```

روتر R4:

```
Router(config)#router ospf 30
Router(config-router)#router-id 150.1.4.4
Router(config-router)#net 172.16.3.2 0.0.0.0 area 0
Router(config-router)#net 172.16.4.1 0.0.0.0 area 1
```

روتر R5:

```
Router(config)#router ospf 30
Router(config-router)#router-id 150.1.5.5
Router(config-router)#net 172.16.4.2 0.0.0.0 area 1
```

در این قسمت، از طریق فرمان Show Ip Route، نگاهی به جدول روتینگ روتر R1 می‌کنیم و این دستور را در مد Privileged وارد می‌کنیم:

Router#**show Ip route**

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

```
      P - periodic downloaded static route

Gateway of last resort is not set

    150.1.0.0/24 is subnetted, 1 subnets
C      150.1.1.0 is directly connected, Loopback0
    172.16.0.0/24 is subnetted, 4 subnets
C      172.16.1.0 is directly connected, FastEthernet0/0
O IA   172.16.2.0 [110/2] via 172.16.1.2, 00:14:31, FastEthernet0/0
O IA   172.16.3.0 [110/3] via 172.16.1.2, 00:11:56, FastEthernet0/0
O IA   172.16.4.0 [110/4] via 172.16.1.2, 00:08:42, FastEthernet0/0
Router(config)#
```

همان‌طور که مشاهده می‌کنید، Network هایی که از طریق OSPF یاد گرفته است به صورت O IA نمایش داده است که O IA، بیانگر OSPF inter area است و نشان‌دهنده‌ی این است که این شبکه‌ها را از Area دیگری غیر از area خود یاد گرفته است و اگر یک روتر در area خود چیزی یاد بگیرد، آن را با حرف O ثبت می‌کند.

نکته: تمام دستوراتی که در مد Privileged اجرا می‌شوند، در مد Global هم اجرا می‌شوند، اما این کار باید از طریق اضافه کردن کلمه‌ی do به اول دستور انجام شود. به مثال زیر توجه کنید.

```
Router(config)#do sh ip int b
Interface              IP-Address      OK? Method Status                Protocol
FastEthernet0/0        172.16.2.2      YES manual up                    up
FastEthernet0/1        172.16.3.1      YES manual up                    up
Loopback0              150.1.3.3       YES manual up                    up
Vlan1                  unassigned      YES unset  administratively down down
```

همان‌طور که مشاهده می‌کنید، دستور **Show Ip Inerface Brife** را هم به صورت کوتاه شده و هم در مد Global با اضافه کردن کلمه‌ی do اجرا کردیم، به همین سادگی، پس همیشه کلمه‌ی do یادتان باشد و سعی کنید از این کلمه استفاده کنید تا سرعت کار بالا رود.

کلمه‌ی do را زمانی استفاده می‌کنیم که بخواهیم دستوراتی که در مد Privileged اجرا می‌شوند را در مد بالاتر، یعنی Global استفاده کنیم، مانند دستور Ping که در مد Global اجرا نمی‌شود، اما اگر در اول این دستور، کلمه‌ی do قرار گیرد، اجرا می‌شود.

دستور Show IP OSPF Database:

این دستور را در روتر R3 و در مد Global با اضافه کردن کلمه‌ی do اجرا کنید:

```
Router(config)#do sh ip ospf database
            OSPF Router with ID (150.1.3.3) (Process ID 10)

                Router Link States (Area 0)

Link ID         ADV Router      Age         Seq#       Checksum Link count
150.1.4.4       150.1.4.4       409         0x80000003 0x00355a 1
150.1.3.3       150.1.3.3       409         0x80000005 0x00946d 2
150.1.2.2       150.1.2.2       409         0x80000002 0x005744 1

                Net Link States (Area 0)
Link ID         ADV Router      Age         Seq#       Checksum
172.16.3.2      150.1.4.4       409         0x80000001 0x005a26
172.16.2.2      150.1.3.3       409         0x80000001 0x00f586

                Summary Net Link States (Area 0)
Link ID         ADV Router      Age         Seq#       Checksum
172.16.1.0      150.1.2.2       404         0x80000001 0x00956f
172.16.4.0      150.1.4.4       399         0x80000001 0x005ba2
```

در این قسمت RID هایی که داخل یک area شرکت دارند، نمایش داده می‌شود.

شبکه‌های روترهای مجاور که به صورت مستقیم به روتر R3 متصل هستند.

شبکه‌هایی که از Area های دیگر وارد این area شده‌اند.

دستور show ip ospf interface:

این دستور، interface های فعال در پروتکل OSPF را نمایش می‌دهد. در روتر R3 این دستور را اجرا می‌کنیم:

```
Router#show ip ospf interface
FastEthernet0/0 is up, line protocol is up
  Internet address is 172.16.2.2/24, Area 0
  Process ID 10, Router ID 150.1.3.3, Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 150.1.3.3, Interface address 172.16.2.2
  Backup Designated Router (ID) 150.1.2.2, Interface address 172.16.2.1
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:02
  Index 1/1, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
```

```
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 150.1.2.2  (Backup Designated Router)
  Suppress hello for 0 neighbor(s)
FastEthernet0/1 is up, line protocol is up
  Internet address is 172.16.3.1/24, Area 0
  Process ID 10, Router ID 150.1.3.3, Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State BDR, Priority 1
Designated Router (ID) 150.1.4.4, Interface address 172.16.3.2
Backup Designated Router (ID) 150.1.3.3, Interface address 172.16.3.1
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:02
  Index 2/2, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 150.1.4.4  (Designated Router)
  Suppress hello for 0 neighbor(s)
```

همان‌طور که در بالا مشاهده می‌کنید، روترهای DR و BDR را مشخص کردیم. در بین روترهای R2 و R3، روتر R3 به خاطر داشتن IP Adderss بزرگ‌تر به عنوان روتر DR انتخاب شده است و روتر R2 به عنوان BDR انتخاب شده است و در بین روترهای R3 و R4 روتر R4 به عنوان DR و روتر R3 به عنوان BDR انتخاب شده است.

دستور Show ip ospf neighbor:

Router# **show ip ospf neighbor**

Neighbor ID	Pri	State	Dead Time	Address	Interface
150.1.2.2	1	FULL/BDR	00:00:31	172.16.2.1	FastEthernet0/0
150.1.4.4	1	FULL/DR	00:00:31	172.16.3.2	FastEthernet0/1

با این دستور می‌توانید، DR یا BDR بودن روترهای همسایه را مشخص کنید. همان‌طور که مشاهده می‌کنید این دستور در روتر R3 اجرا شده و در نتیجه‌ی آن به ما RID روترهای همسایه را نشان داده است و مشخص کرده است که روتر R4 به عنوان DR و روتر R2 به عنوان BDR انتخاب شده است.

دستور show ip ospf border-routers:

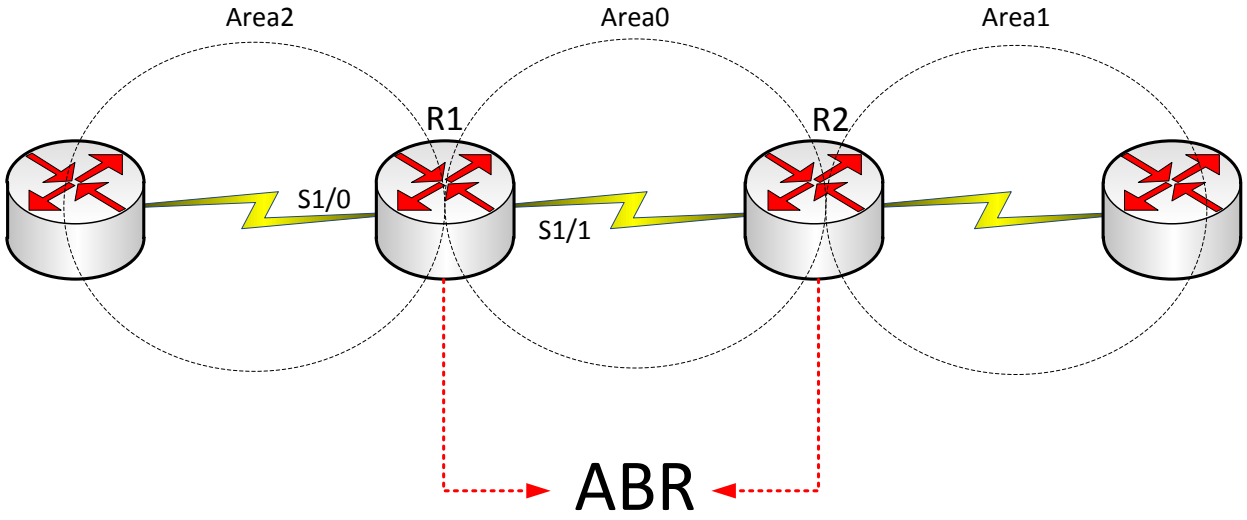
```
Router#show ip ospf border-routers
OSPF Process 10 internal Routing Table
Codes: i - Intra-area route, I - Inter-area route
i 150.1.2.2 [1] via 172.16.2.1, FastEthernet0/0, ABR, Area 0, SPF 1
i 150.1.4.4 [1] via 172.16.3.2, FastEthernet0/1, ABR, Area 0, SPF 1
```

این دستور، روترهای همسایه را به ما نشان می‌دهد و Ip address آن‌ها را مشخص می‌کند.

روتر ABR (Area Border Router):

به روتری می‌گویند که بین دو Area قرار دارد و کار انتقال اطلاعات از یک area به area دیگر را بر عهده دارد.

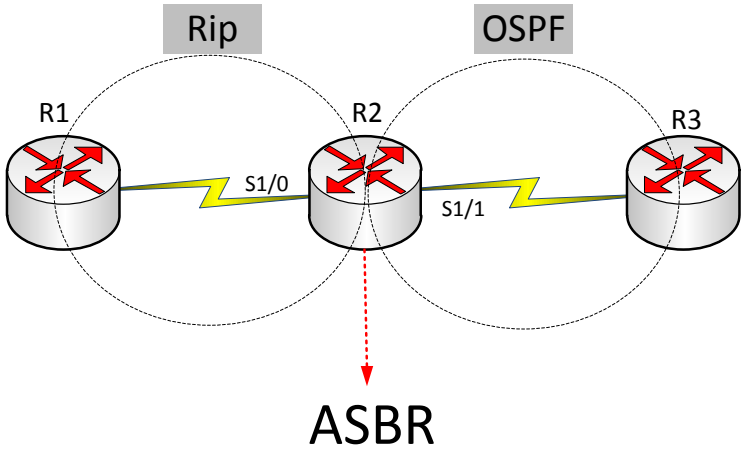
به شکل زیر توجه کنید.



همان‌طور که در شکل بالا مشاهده می‌کنید، روترهای R1 و R2 روترهایی هستند که بین دو area قرار دارند و کار انتقال را انجام می‌دهند که به این روترها، روترهای ABR گفته می‌شود.

روتر ASB (Autonomous System Border Router):

این روتر کار انتقال اطلاعات از یک پروتکل یا یک دومین دیگر به داخل OSPF را انجام می‌دهد. به شکل زیر توجه کنید.

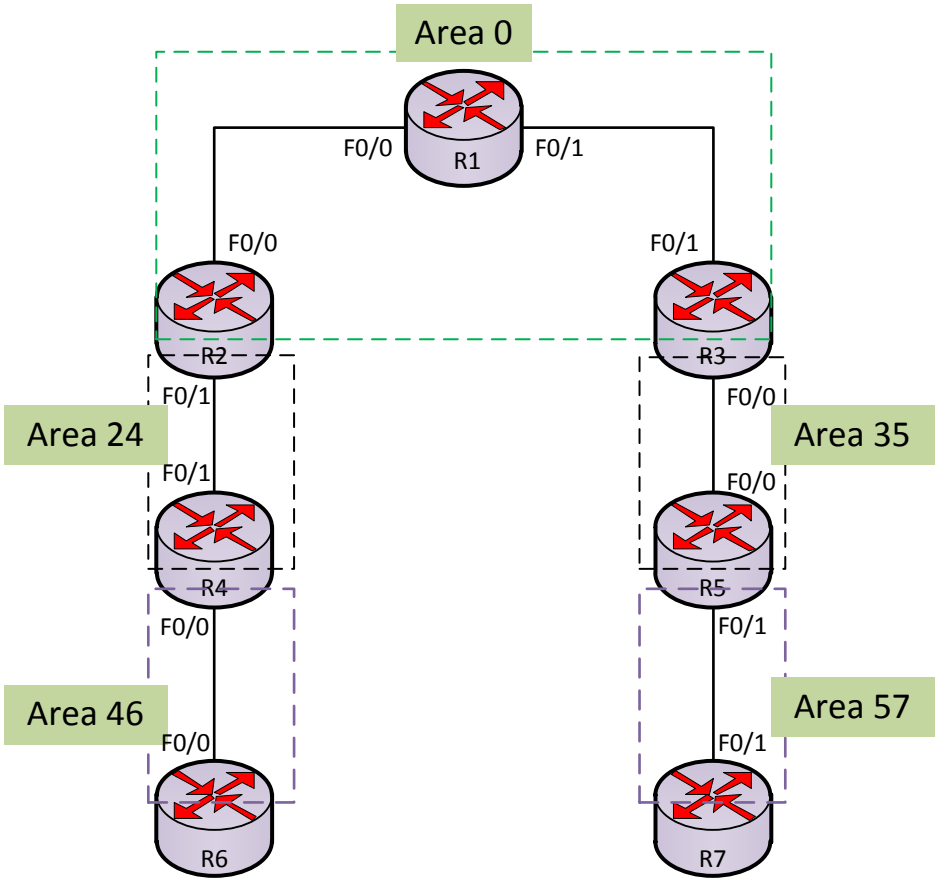


در این شکل روتر R2 بین دو پروتکل قرار دارد و کار ترجمه یا Redistribute را انجام می‌دهد به عنوان روتر ASBR شناخته می‌شود.

درباره‌ی Redistribute در بحث‌های پایانی کتاب صحبت خواهیم کردیم.

کار با Virtual Link در OSPF:

همان‌طور که قبلاً بیان کردیم، تمام Area ها باید به Area 0 متصل باشند تا بتوانند اطلاعات خود را انتقال دهند. اگر این Area ها به صورت مستقیم، مانند شکل زیر به Area 0 متصل نباشند، نمی‌توانند داده‌ها را انتقال دهند. برای درک این موضوع یک مثال را باهم بررسی می‌کنیم.



در این مثال، Area های 46 و 57 نمی‌توانند اطلاعات خود را در شبکه ارسال کنند، به این علت که به Area 0 متصل نیستند. برای حل این مشکل از Area 24,35 که بین این دو Area قرار دارد، کمک می‌گیریم و یک لینک مجازی بین Area ها ایجاد می‌کنیم. برای این کار باید وارد روترهای مرزی شویم که در این مثال برای متصل

شدن Area46 به Area0 از روترهای R4 و R2 کمک می‌گیریم و Virtual Link را روی این دو فعال می‌کنیم تا یک پل از Area46 به Area0 زده باشیم.

جدول ip address به صورت زیر است:

Router	F0/0	F0/1	LoopBack
R1	1.1.12.1/24	1.1.13.1/24	100.1.1.1/24
R2	1.1.12.2/24	1.1.24.2/24	100.2.2.2/24
R3	1.1.35.3/24	1.1.13.3/24	100.3.3.3/24
R4	1.1.46.4/24	1.1.24.4/24	100.4.4.4/24
R5	1.1.35.5/24	1.1.57.5/24	100.5.5.5/24
R6	1.1.46.6/24	…	100.6.6.6/24
R7	…	1.1.57.7/24	100.7.7.7/24

بعد از واردکردن IP address در روترها باید پروتکل OSPF را روی تک‌تک روترها فعال کنیم؛

وارد روتر R1 شوید و دستورات زیر را وارد کنید:

```
Router(config)#router ospf 1
Router(config-router)#router-id 100.1.1.1
Router(config-router)#network 1.1.12.1 0.0.0.0 area 0
Router(config-router)#network 1.1.13.1 0.0.0.0 area 0
```

همان‌طور که مشاهده می‌کنید، پروتکل OSPF را روی این روتر فعال و شبکه‌های مربوط به آن را معرفی کردیم در بقیه‌ی روترها هم به صورت زیر عمل می‌کنیم:

وارد روتر R2 شوید و دستورات زیر را وارد کنید:

```
Router(config)#router ospf 1
Router(config-router)#router-id 100.2.2.2
Router(config-router)#network 1.1.12.2 0.0.0.0 area 0
Router(config-router)#network 1.1.24.2 0.0.0.0 area 24
```

وارد روتر R3 شوید و دستورات زیر را وارد کنید:

```
Router(config)#router ospf 1
Router(config-router)#router-id 100.3.3.3
Router(config-router)#network 1.1.13.3 0.0.0.0 area 0
Router(config-router)#network 1.1.35.3 0.0.0.0 area 35
```

وارد روتر R4 شوید و دستورات زیر را وارد کنید:

```
Router(config)#router ospf 1
Router(config-router)#router-id 100.4.4.4
Router(config-router)#network 1.1.24.4 0.0.0.0 area 24
Router(config-router)#network 1.1.46.4 0.0.0.0 area 46
```

وارد روتر R5 شوید و دستورات زیر را وارد کنید:

```
Router(config)#router ospf 1
Router(config-router)#router-id 100.5.5.5
Router(config-router)#network 1.1.35.5 0.0.0.0 area 35
Router(config-router)#network 1.1.57.5 0.0.0.0 area 57
```

وارد روتر R6 شوید و دستورات زیر را وارد کنید:

```
Router(config)#router ospf 1
Router(config-router)#router-id 100.6.6.6
Router(config-router)#network 1.1.46.6 0.0.0.0 area 46
```

وارد روتر R7 شوید و دستورات زیر را وارد کنید:

```
Router(config)#router ospf 1
Router(config-router)#router-id 100.7.7.7
Router(config-router)#network 1.1.57.7 0.0.0.0 area 57
```

بعد از اتمام کار، اگر وارد روتر R6 و R7 شوید و دستور **Show Ip Route** را وارد کنید، متوجه می‌شوید هیچ شبکه‌ای را از طریق OSPF یاد نگرفته است.

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

Gateway of last resort is not set

    1.0.0.0/24 is subnetted, 1 subnets
C       1.1.46.0 is directly connected, FastEthernet0/0
```

همان‌طور که مشاهده می‌کنید، هیچ شبکه‌ای را از طریق پروتکل OSPF یاد نگرفته است، به خاطر این‌که Area 46 و Area 57 به Area 0 متصل نیستند. برای حل این مشکل، یک پل به Area0 می‌زنیم.

ایجاد Virtual Link:

برای ایجاد این لینک، باید وارد روترهای R2 و R4 و روترهای R3 و R5 شوید و دستور ساخت Virtual Link را وارد کنید:

وارد روتر R2 شوید و دستور زیر را وارد کنید:

```
Router(config)#router ospf 1
Router(config-router)#area 24 virtual-link 100.4.4.4
```

همان‌طور که مشاهده می‌کنید، اول وارد OSPF 1 شدیم که قبلاً ایجاد کردیم و بعد با دستور area 0 virtual-link 100.4.4.4 به روتر گفتیم که یک Virtual Link ایجاد کند. برای ارتباط با روتر روبرو که مرز بین Aera دیگر است، این کار را باید در طرف روبرو هم انجام دهیم، یعنی روتر R4.

وارد روتر R4 شوید و دستور زیر را وارد کنید:

```
Router(config)#router ospf 1
Router(config-router)# area 24 virtual-link 100.2.2.2
```

بعد از این‌که در روتر R4 هم این دستور را وارد کردید، ارتباط بین Area 46 و Area0 توسط این لینک برقرار می‌شود. برای درک این موضوع وارد روتر R6 شوید و دستور Show IP Route را وارد کنید:

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

Gateway of last resort is not set

     1.0.0.0/24 is subnetted, 5 subnets
O IA    1.1.12.0 [110/3] via 1.1.46.4, 00:00:56, FastEthernet0/0
O IA    1.1.13.0 [110/4] via 1.1.46.4, 00:00:56, FastEthernet0/0
O IA    1.1.35.0 [110/5] via 1.1.46.4, 00:00:56, FastEthernet0/0
C       1.1.46.0 is directly connected, FastEthernet0/0
O IA    1.1.57.0 [110/6] via 1.1.46.4, 00:00:56, FastEthernet0/0
```

روترR6 تمام آدرس‌های شبکه را از طریق OSPF یاد گرفته است. در ادامه باید همین کار را در طرف دیگر وارد کنید، یعنی بین روترهای R3 و R5:

وارد روتر R3 شوید و دستور زیر را وارد کنید:

```
Router(config)#router ospf 1
Router(config-router)#area 35 virtual-link 100.5.5.5
```

وارد روتر R5 شوید و دستور زیر را وارد کنید:

```
Router(config)#router ospf 1
Router(config-router)#area 35 virtual-link 100.3.3.3
```

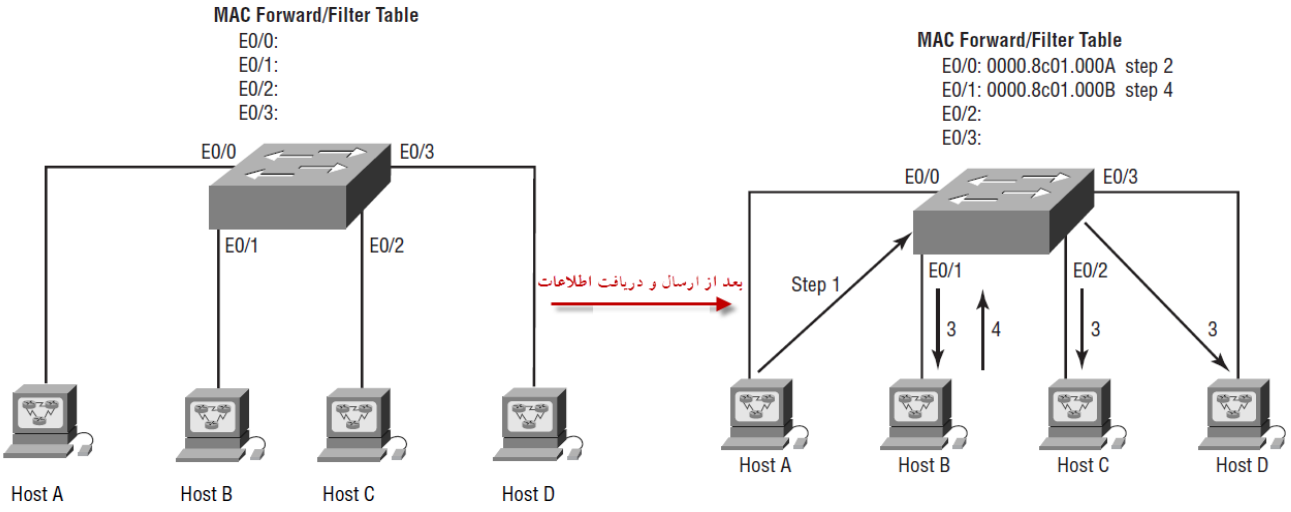
بعد از اتمام کار، تمام روترها در شبکه قابل شناسایی هستند و می‌توانند همدیگر را ببینند.

سوئیچ لایه‌ی 2:

سوئیچ‌ها در لایه‌ی دوم مدل OSI کار می‌کنند. سوئیچ‌ها در انواع مختلف 8، 16، 24، 48 پورت وجود دارد که با استفاده از آدرس Mac ترافیک را در شبکه انتقال می‌دهند که همین امر این دستگاه را با Hub متمایز کرده است، البته Bridge هم نوعی سوئیچ است، اما با پورت‌های کمتر.

سوئیچ‌ها از یک جدول استفاده می‌کنند که تمام mac address دستگاه‌های متصل به خود را در آن جای می‌دهند و از طریق آن کار آدرس‌دهی را انجام می‌دهند.

در زیر یک سوئیچ لایه‌ی دو قرار دارد و چهار Pc به آن متصل هستند. در لحظه‌ی اول جدول MAC forward/filter خالی است، تا زمانی که Pc ها اقدام به ارسال اطلاعات کنند؛ با این کار سوئیچ به جدول خود نگاهی می‌کند و وقتی مشاهده کرد که mac address این pc ها در داخل جدول قرار ندارد آن را در جدول ثبت می‌کند. همان‌طور که در شکل زیر مشاهده می‌کنید، Host A بعد از ارسال اطلاعات Mac آدرس آن در جدول سوئیچ ثبت شد و بعدی Host B است که به محض دریافت اطلاعات، Mac address آن‌هم در جدول سوئیچ ثبت شد و به همین ترتیب این کار ادامه می‌یابد.



نکته: سوئیچ برای اینکه برای اولین بار جدول خود را تکمیل کند از Broadcast برای آگاهی از تمام Mac Address شبکه استفاده می‌کند و بعد، تکمیل جدول ارتباط دستگاه‌ها به صورت Unicast انجام می‌شود که این یک ویژگی سوئیچ است و آن را از Hub متمایز می‌کند، مثلاً اگر در شکل بالا Host A بخواهد اطلاعات را به Host D بفرستد، چون سوئیچ از آدرس Mac، Host D خبری ندارد، این پیام را به صورت Broadcast به همه‌ی pc های متصل به سوئیچ ارسال می‌کند و وقتی این کار را انجام داد، تک‌تک آدرس‌های Mac مربوط به pcها در جدول سوئیچ ثبت می‌شوند.

توجه داشته باشید که وقتی Host A بخواهد به Host B اطلاعات ارسال کند، سوئیچ فقط به پورتی که Host B به آن متصل است اطلاعات را ارسال می‌کند و به پورت‌های دیگر کاری ندارد که به این روش، فیلتر کردن فریم‌ها هم گفته می‌شود.

روش‌های انتقال فریم (LAN Switch Types):

سوئیچ از سه روش برای انتقال فریم (اطلاعات) در شبکه استفاده می‌کنند که هرکدام را باهم مورد بررسی قرار می‌دهیم.

روش اول (FastForward) Cut-through:

در این روش زمانی که سوئیچ فریمی را دریافت کند که مربوط به یک pc باشد، سریع آن را از طریق جدول Mac خود به طرف پورت مورد (**destination**) نظر ارسال می‌کند، این روش بسیار سریع است، چون آدرس مقصد (**destination**) را در سوئیچ به صورت کامل مورد بررسی قرار نمی‌دهد، یعنی وقتی‌که یک آدرس وارد سوئیچ شد چند عدد اول مورد بررسی قرار می‌گیرد و آدرس مقصد مشخص می‌شود.

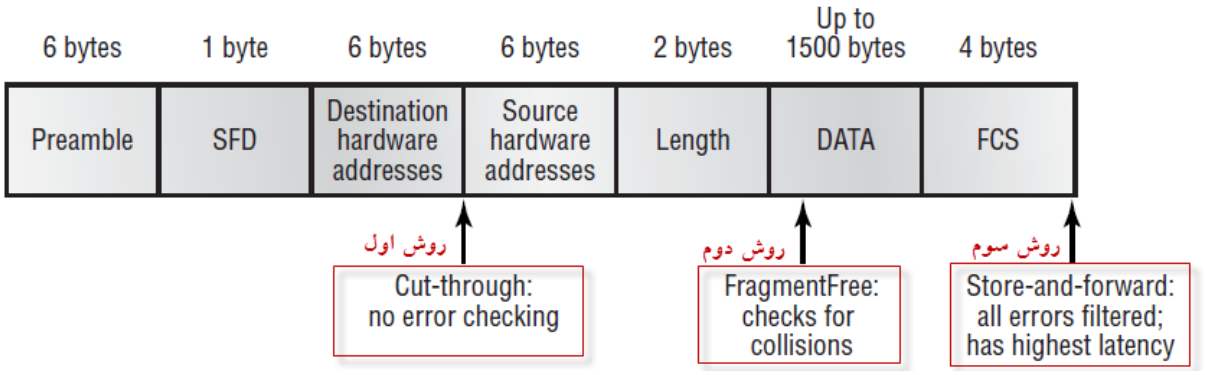
روش دوم (modified cut-through) FragmentFree:

در این روش که کمی سرعت آن به نسبت روش قبلی کمتر است و اصلاح‌شده‌ی روش قبلی است، 64 بیت اول MAC آدرس مقصد (Destination) در سوئیچ مورد بررسی قرار می‌گیرد و از نظر Error چک می‌شود و اگر مشکلی نداشت به طرف آدرس مقصد ارسال می‌شود.

روش سوم Store-and-forward:

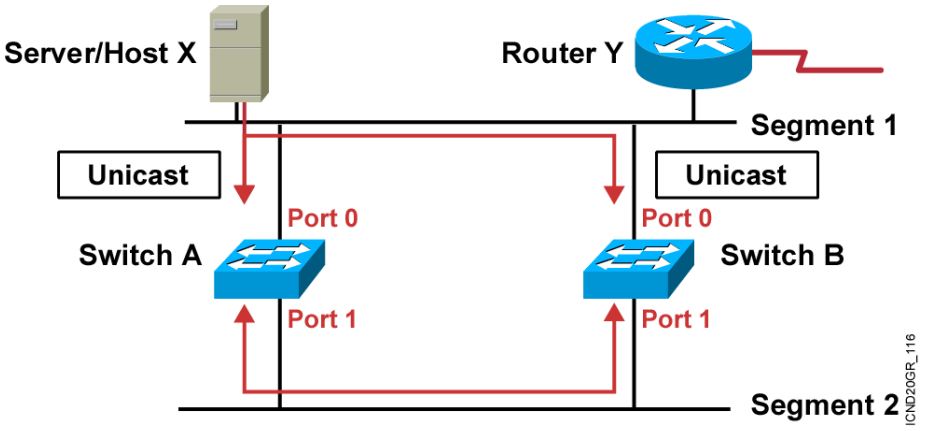
در این روش فریم مورد نظر به صورت کامل دریافت می‌شوند و Buffer می‌شوند و در صورتی که الگوریتم CRC خطایی را تشخیص ندهد به آدرس مقصد مورد نظر ارسال می‌شود که البته اگر خطایی داشته باشد، این فریم پس زده می‌شود.

به شکل زیر توجه کنید، این شکل (Frame) هر سه حالت را برای شما نمایش می‌دهد.



بررسی Loop در سوئیچ:

به این شکل توجه کنید.



در شکل بالا، Server X در حال ارسال Frame به Router Y است که یک مشکل در سر راه وجود دارد و آن‌هم این است که سوئیچ A و B از دو مسیر مختلف، آدرس MAC سرور X را در جدول خود ثبت کردند و زمانی که بخواهد یک فریم را به روتر مورد نظر ارسال کنند، به علت یکسان بودن فریم دچار بار اضافه در شبکه می‌شوند و در اصطلاح Loop ایجاد می‌شود.

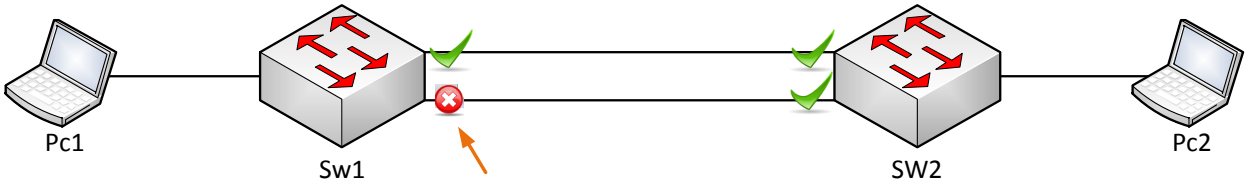
روش‌های جلوگیری از loop:

STP(Spanning Tree Protocol):

پروتکل STP توسط سازمان IEEE با شماره‌ی 802.1D استاندارد شده است و شرکت سازنده‌ی آن DCE است.

کار این پروتکل این است که وقتی شبکه در Loop قرار می‌گیرد، بعضی از interface های اضافه را ShutDown می‌کند و فقط به یک طرف اجازه‌ی ارسال و دریافت اطلاعات می‌دهد.

این پروتکل از طریق الگوریتمی به نام STA (Spanning Tree Algorithm) برای این کار استفاده می‌کند که کار این الگوریتم به این صورت است که کل ساختار شبکه را به صورت یک درخت درآورده و جاهایی را که Loop در آن ایجاد شده، مهار می‌کند. در شکل زیر، 2 سوئیچ با دو لینک به هم متصل شده‌اند و پروتکل STP برای جلوگیری از Loop، یکی از لینک‌ها را از رده خارج کرده است.



نحوه‌ی کارکرد الگوریتم STA:

قبل از این کار به چند موضوع می‌پردازیم:

Bridge ID:

شناسه‌ای است برای تمایز دادن سوئیچ‌ها در پروتکل STP، پس می‌توان گفت با کمک این شناسه، سوئیچ‌ها در یک شبکه قابل تشخیص هستند و اجزای تشکیل‌دهنده‌ی Bridgr Id دو چیز است:

- **Priority**: عددی است روی سوئیچ‌های شرکت سیسکو که به صورت پیش‌فرض 32769 است.
- **Mac Address**: آدرس Mac پورت مورد نظر در سوئیچ.

پس Bridge ID، جمع این دو گزینه می‌شود. به شکل صفحه‌ی قبل توجه کنید؛ در سوئیچی که پروتکل STP روی آن اجرا شده است (که با جهت‌نما آن را مشخص کردیم) در مد Privileged دستور زیر را وارد کنید:

```
Switch# show spanning-tree
VLAN0001
Spanning tree enabled protocol ieee
Root ID    Priority    32769
Address     0001.C9A6.90A3
Cost        19
(Port       1(FastEthernet0/1

Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

(Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1

Address     0090.0C6C.EE69
Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
Aging Time  20

Interface       Role Sts Cost      Prio.Nbr Type
---------------------------- -------- --------- --- ---- ----------------

Fa0/1           Root FWD 19        128.1    P2p
Fa0/2           Altn BLK 19        128.2    P2p
Fa0/3           Desg FWD 19        128.3    P2p
```

این اعداد به رنگ قرمز در نتیجه مشخص شده‌اند.

Root Bridge:

برای انتخاب یک سوئیچ به عنوان root Bridge تمام Bridge ID های مختلف سوئیچ‌ها باهم مقایسه می‌شوند و هرکدام که کوچک‌تر بود، همان سوئیچ به عنوان Root Bridge انتخاب می‌شود.

:BPDU

فریمی در سوئیچ است که برای انتقال اطلاعات بین سوئیچ‌ها کاربرد دارد و یکی دیگر از ویژگی‌های آن این است که تغییر ساختار شبکه را خیلی سریع به دیگر سوئیچ‌ها در شبکه اطلاع می‌دهد.

:Root Port

پورتی است که ارتباط مستقیم با Root Bridge دارد و از طریق آن انتخاب می‌شود.

:Designated port

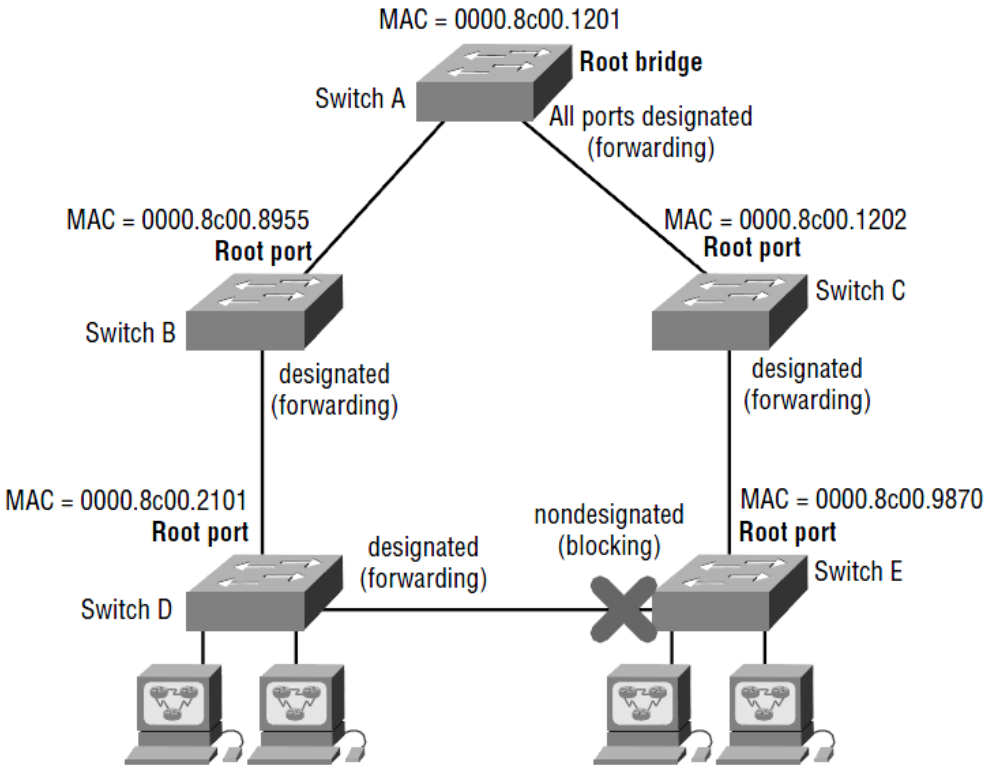
پورتی از سوئیچ است که به عنوان Forwarding انتخاب می‌شود و کار ارسال و دریافت اطلاعات را انجام می‌دهد.

:NonDesignated port

برای جلوگیری از loop این پورت shutdown می‌شود.

پس در کل در الگوریتم STA هر سوئیچ Bridge ID خود را محاسبه می‌کند و بعد، از طریق BPDU آن را در شبکه تبلیغ می‌کند، بعد Bridge ID خود را با دیگر سوئیچ‌ها مقایسه می‌کند، اگر Bridge ID خودش کمتر از دیگران باشد، Bridge ID خود را در شبکه تبلیغ می‌کند، اما اگر یکی کمتر از خود را پیدا کند آن را در قالب فریم BPDU به دیگر سوئیچ‌ها اعلام می‌کند تا در آخر کار بعد از مقایسه، Bridge ID کمترین Bridge ID به دست آید که آخرین سوئیچ با کمترین Bridge Id به عنوان Root Bridge انتخاب می‌شود. بعد از این کار، نوبت به انتخاب وضعیت پورت‌ها است که چه پورتی در چه وضعیتی قرار دارد.

در شکل صفحه‌ی بعد، تمام مراحل بالا وجود دارد. اگر به شکل توجه کنید، Switch A به علت کوچک‌تر بودنMac Address نسبت به بقیه‌ی سوئیچ‌ها، به عنوان Root bridge انتخاب شده است و هر دو پورت آن به حالت Forwarding رفته است. پورت‌های سوئیچ‌های B و C که به سوئیچ A متصل هستند به عنوان Root Port انتخاب شده‌اند. پورت بعدی سوئیچ‌های B و C به عنوان پورت Forwarding انتخاب شده‌اند و به همین ترتیب بقیه‌ی پورت‌ها انتخاب می‌شوند. برای جلوگیری از loop یکی از پورت‌های سوئیچ E به حالت Nondesignated رفته و Block شده است که البته این پورت به نسبت پورت دیگر دارای cost بیشتر و پهنای باند کمتری بوده است.



پس اگر مراحل کار الگوریتم STA را طبق مراحل زیر در نظر بگیریم، متوجه‌ی کار این الگوریتم خواهیم شد.

1- سوئیچ‌ها، Bridge ID خود را مشخص می‌کنند.

2- در این مرحله، هر سوئیچ Bridge ID خود را تحت فریم BPDU به دیگر سوئیچ‌ها تبلیغ می‌کند تا پایین‌ترین Bridgr ID مشخص شود و بعدازآن، Root Bridge مشخص می‌شود.

3- باید Designated Port انتخاب شود که پورت‌های متصل به سوئیچ Root Bridge به عنوان Designated Port انتخاب می‌شوند و کار ارسال و دریافت اطلاعات را انجام می‌دهند. در بین دو سوئیچ هم پورتی که کمترین cost را داشته باشد، به عنوان Designated Port انتخاب می‌شود.

4- در این مرحله که مرحله‌ی مهمی است در آن قسمت که loop ایجاد می‌شود، یکی از پورت‌ها که پهنای باند کمتر و Cost بیشتر داشته باشد، به عنوان پورت NonDesignated Port انتخاب و Block می‌شود. اگر چنانچه هر دو فاکتور پهنای باند و cost یکی باشد، معیار انتخاب Bridge ID بزرگ‌تر است.

هر پورت سوئیچ دارای 5 وضعیت است:

Blocking: وقتی سوئیچ روشن می‌شود، همه‌ی پورت‌های آن در حالت Block قرار دارند و منتظر هستند تا فریم BPDU به آن‌ها برسد تا وضعیت خود را تغییر دهند.

Listening:

در این وضعیت سوئیچ بر طبق فریم‌های BPDU، سوئیچ Root Bridge را انتخاب می‌کند.

Learning:

این وضعیت بعد از وضعیت listening اجرا می‌شود و تمامی مسیرهای موجود در شبکه که در loop قرار ندارد را شناسایی می‌کند. به این موضوع توجه کنید که در وضعیت Listening اگر Mac address جدید به سوئیچ برسد، سوئیچ در جدول آن را ثبت نمی‌کند، اما اگر به وضعیت Learning برسد در جدول خود ثبت می‌کند. در این مرحله، پورت‌های Root Port و Designated Port مشخص می‌شوند.

Forwarding:

یک پورت زمانی به این حالت می‌رود که وضعیت قبل را طی کرده باشد، در این حالت، پورت قادر به دریافت و ارسال اطلاعات می‌کند.

Blocking:

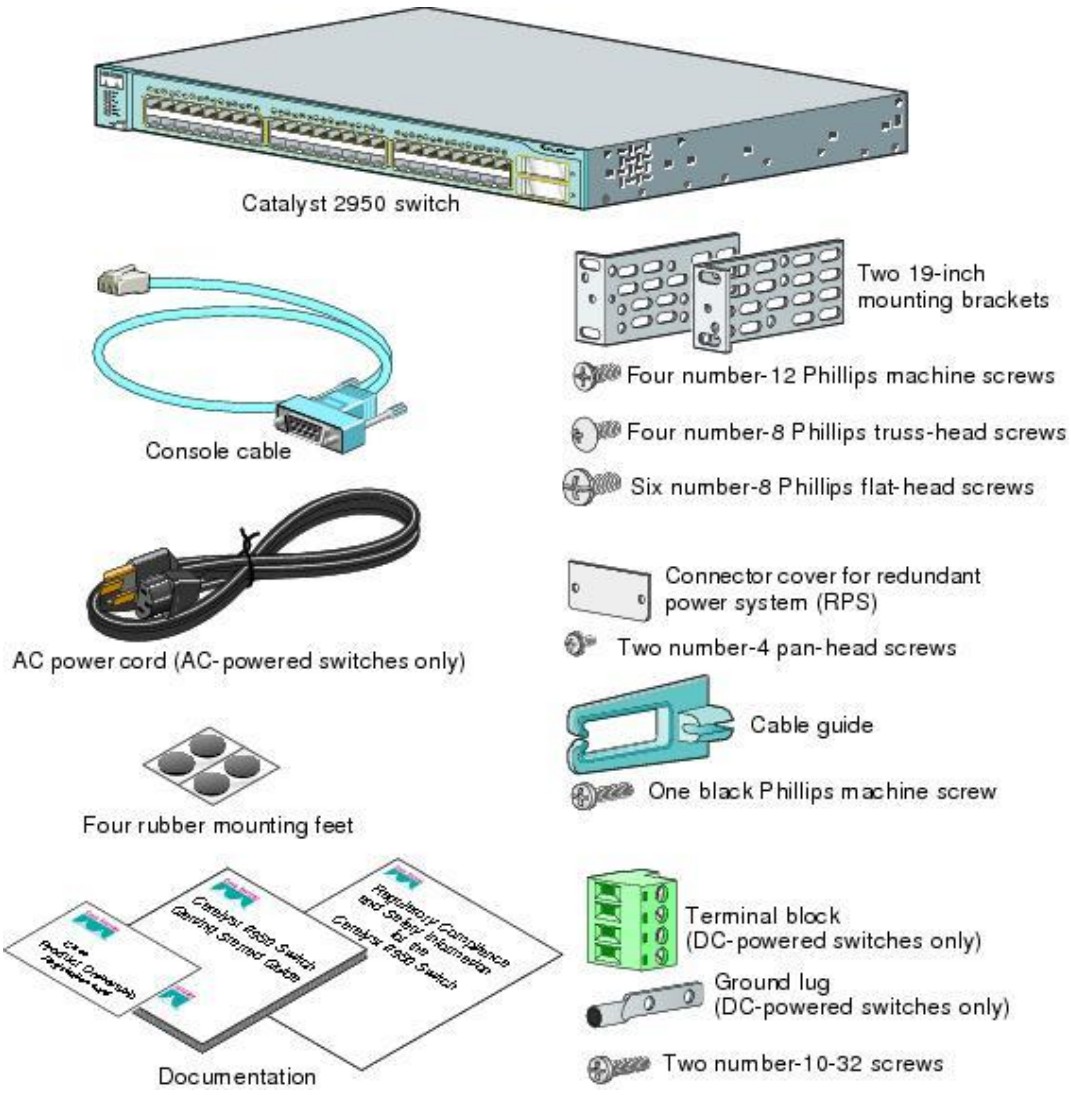
این حالت زمانی رخ می‌دهد که یک پورت برای جلوگیری از Loop در شبکه باید به حالت Blocking برود، البته در این حالت، پورت Shutdown نمی‌شود، بلکه منتظر فریم‌های BPDU می‌نشیند که اگر تغییری در شبکه رخ داد، دوباره به حالت دیگر تغییر وضعیت دهد.

Disable:

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

نگاهی به سوئیچ 2950:

زمانی که یک سوئیچ 2950 را خریداری می‌کنید، شامل اجزای زیر است:



سوئیچ‌ها در انواع مختلف 8، 16، 24، 26، 48 پورت و ... وجود دارند که بنا به نیاز خود، یکی از این مدل‌ها را تهیه می‌کنیم. سوئیچ‌ها دستگاه‌های هوشمندی هستند و از طریق Mac address کارهای خود را انجام می‌دهند. سوئیچ‌ها در انواع سرعت‌های 10، 100، 1000، 10000 مگابایت وجود دارند و سیستم عامل‌های آن‌ها، مانند روترها ios است که اولین ios آن مدل 12،1 بوده است.

زمانی که یک سوئیچ روشن می‌شود به حالت post می‌رود و در این مرحله، تمام سخت‌افزار آن تست می‌شود و اگر یکی از پورت‌ها مشکلی داشت به رنگ کهربایی درمی‌آید و اگر هیچ‌کدام مشکلی نداشت، همه‌ی آن‌ها

یک‌بار چشمک زده و اعلام آمادگی می‌کنند. بعد از این کار، سوئیچ به دنبال فایل ios می‌گردد و وقتی فایل مورد نظر را پیدا کرد، وارد مد Cli می‌شود.

سوئیچ‌ها از چراغ‌هایی تشکیل شده‌اند و این چراغ‌ها به 4 نوع تقسیم می‌شوند:

Port status Led:

روی سوئیچ‌ها به ازای هر پورتی که وجود دارد، یک چراغ چشمک‌زن هم وجود دارد که این چراغ به رنگ‌های مختلف نمایانگر می‌شود که هر رنگ آن را باهم مورد بررسی قرار می‌دهیم:

سبز	به این پورت کابلی متصل شده است، اما فعال نشده است.
سبز چشمک‌زن	این پورت فعال و در حال ارسال و دریافت اطلاعات است.
سبز و کهربایی	در این حالت یک collision در سوئیچ رخ داده است.
کهربایی	در این حالت پورت Disable شده، اما به صورت دستی.
off	به پورت کابلی متصل نشده است.

Port Mode Led:

در این حالت دو نوع چراغ وجود دارد:

UTL LED: این چراغ‌ها نشان‌دهنده‌ی پهنای باند مصرفی در سوئیچ می‌باشند.

STST LED: زمانی که سوئیچ روشن شود، این چراغ هم روشن می‌شود.

FDUP LED: در این حالت پورت‌ها در دو حالت Half-duplex و Full-duplex قرار دارند و اگر چراغ پورت خاموش باشد، یعنی در حالت Half-duplex قرار دارد و اگر روشن باشد و سبز در حالت Full-duplex قرار دارد.

100 یا Speed Led: این چراغ نشان‌دهنده‌ی سرعت یک پورت است که اگر خاموش باشد، یعنی از 10 مگابایت استفاده می‌کند و اگر روشن و سبز باشد، یعنی از حداکثر سرعت استفاده می‌کند.

انواع مدها در سوئیچ:

سوئیچ از انواع مد در ios استفاده می‌کند که دقیقاً شبیه به روتر است و هیچ فرقی با روتر ندارد.

User Mode:

این مد اولین مدی است که وارد روتر می‌شویم و سطح دسترسی آن بسیار محدود است و بیشتر برای Monitoring استفاده می‌شود. وقتی وارد سوئیچ می‌شوید، خط فرمان به صورت زیر مشاهده می‌شود:

Switch>

Privileged Mode:

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

```
Switch>Enable
Switch#
```

Global Mode:

این مد دارای مجوز دسترسی بالایی است. وقتی وارد این مد می‌شوید، می‌توانید تمام تنظیمات سوئیچ را در دست بگیرید و آن‌ها را تغییر دهید. برای ورود به آن، باید از طریق مد Privileged اقدام کنید:

```
Switch# Conf terminal
Switch(Config)#
```

بررسی VLAN (Virtual Link):

وقتی چندین کامپیوتر را به یک سوئیچ متصل می‌کنیم، آن‌ها به راحتی می‌توانند باهم ارتباط داشته باشند و از منابع شبکه استفاده کنند، اما تعداد زیاد کامپیوترها می‌تواند حجم کاری سوئیچ را افزایش دهند، یعنی این‌که تمام سوئیچ‌ها در یک منطقه‌ی کاری باهم در ارتباط هستند و امنیت در این نوع شبکه‌ها بسیار پایین می‌آید، اما می‌توان با تقسیم یک منطقه به چندین منطقه امنیت را افزایش داد و ترافیک شبکه را به راحتی کنترل کرد.

مثالی بزنیم، شما مدیر شبکه‌ی یک شرکت هستید و این شرکت از 3 بخش حسابداری، فروش و اداری تشکیل شده است و می‌خواهید این چند اتاق را توسط سوئیچ به هم شبکه کنید که با متصل کردن همه‌ی کامپیوترهای این اتاق‌ها، آن‌ها به هم متصل می‌شوند و می‌توانند به منابع شبکه دسترسی داشته باشند. با این کار ترافیک روی سوئیچ افزایش پیدا می‌کند، چون همه‌ی این کامپیوترها در یک Broadcast Domain قرار دارند و امنیت در این شبکه به خاطر دسترسی همگان به همه‌ی اطلاعات پایین می‌آید. شما که مدیر شبکه هستید، باید کاری انجام دهید که این اتاق‌ها از هم جدا شوند، مثلاً کامپیوتر اتاق حسابداری نتواند با اتاق اداری ارتباط برقرار کند. خوب این کار توسط Vlan انجام می‌شود که همه‌ی کامپیوترهای اتاق حسابداری را می‌توان در یک منطقه قرار داد و باهم در ارتباط باشند و با اتاق‌های دیگر نتوانند در ارتباط باشند.

ایجادVLAN:

برای ایجاد یک VLAN در سوئیچ وارد مد Global می‌شوید و دستور زیر را وارد می‌کنید:

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

همان‌طور که مشاهده می‌کنید، بعد از تعریف Vlan علامت سؤال قرار دادیم که به ما تعداد Vlan های قابل ایجاد را نمایش می‌دهد، یعنی می‌توانیم از 1 تا 1005 عدد VLan در یک سوئیچ تعریف کنیم. توجه داشته باشید که VLan 1 را نمی‌توانید ایجاد کنید، چون به صورت پیش‌فرض تمام پورت‌های سوئیچ در این Vlan قرار دارد و به خاطر همین است که تمام پورت‌ها باهم در ارتباط هستند.

Switch(config)#**vlan 20**
Switch(config-vlan)#**Name Tehran**

در این دستور Vlan شماره‌ی 20 تعریف شده است و بعد از آن، یک اسم از طریق دستور Name به آن نسبت دادیم. برای مشاهده‌ی Vlan که تعریف کردیم و نام این Vlan از دستور زیر استفاده می‌کنیم:

Switch#**show vlan brief**

VLAN	Name	Status	Ports
1	default	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4 Fa0/5, Fa0/6, Fa0/7, Fa0/8 Fa0/9, Fa0/10, Fa0/11, Fa0/12 Fa0/13, Fa0/14, Fa0/15, Fa0/16 Fa0/17, Fa0/18, Fa0/19, Fa0/20 Fa0/21, Fa0/22, Fa0/23, Fa0/24
10	**babol**	**active**	
20	**Tehran**	active	
1002	fddi-default	active	
1003	token-ring-default	active	
1004	fddinet-default	active	
1005	trnet-default	active	

همان‌طور که مشاهده می‌کنید، Vlan 20 با نام Tehran تعریف شده است و وضعیت آن فعال است. اگر به Vlan 1 نگاهی کنید، متوجه می‌شوید که تمام پورت‌های سوئیچ در این Vlan قرار دارد.

قرار دادن پورت‌ها داخل Vlan مورد نظر:

این کار به دو صورت انجام می‌پذیرد:

1- Static:

این روش به صورت دستی است و می‌توانیم هر پورتی را در Vlan مورد نظر خود قرار دهیم، این روش یکی از امن‌ترین روش‌ها است.

2- Dynamic:

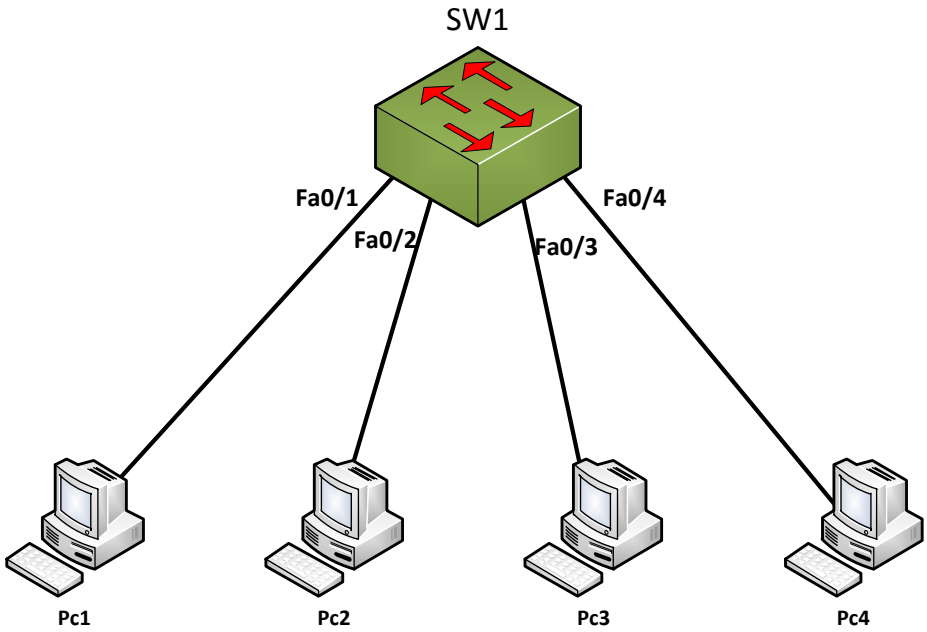
در این روش نسبت دادن پورت به یک Vlan از طریق دستی صورت نمی‌گیرد، بلکه از طریق یک سرور مرکزی با نام VMPS (Vlan Membership Policy Server) ایجاد و مدیریت می‌شوند.

در این قسمت، نحوه‌ی قرار دادن پورت‌های یک سوئیچ را در یک Vlan باهم بررسی می‌کنیم.

هر پورت سوئیچ از دو Mode تشکیل شده است:

- Mode Access
- Mode Trunk

تمام پورت‌های یک سوئیچ به صورت پیش‌فرض در مد access قرار دارد. برای اینکه یک پورت را به یک Vlan نسبت دهید، باید از این مد استفاده کنید. با یک مثال، کاملاً به این موضوع پی می‌برید.



یک سوئیچ و 4 PC را به صفحه اضافه و آن‌ها را به هم متصل کنید و طبق جدول صفحه بعد به کامپیوترها آدرس دهید:

Station	IP Address	Subnet Mask
PC1	192.168.1.1	255.255.255.0
PC2	192.168.1.2	255.255.255.0
PC3	192.168.1.3	255.255.255.0
Pc4	192.168.1.4	255.255.255.0

بعد از این‌که آدرس‌دهی کردید، اگر ارتباط بین PC ها را تست کنید، متوجه می‌شوید که همه‌ی آن‌ها باهم در ارتباط می‌باشند. حالا می‌خواهیم از طریق Vlan ارتباط 2 کامپیوتر Pc1 و Pc2 را با Pc3 و Pc4 جدا کنیم. برای این کار در داخل سوئیچ دو Vlan تعریف می‌کنیم:

Switch(config)#**vlan 10**
Switch(config-vlan)#ex
Switch(config)#**vlan 20**
Switch(config-vlan)#

Vlan های 10 و 20 در داخل سوئیچ ایجاد شده است و حالا باید پورت‌های سوئیچ که Pc ها به آن متصل هستند را داخل این Vlan ها قرار دهیم. به شکل توجه کنید، ارتباط پورت‌ها با pc ها به صورت جدول زیر است.

Station	Port	Vlan
PC1	Fa0/1	10
PC2	Fa0/2	10
PC3	Fa0/3	20
PC4	Fa0/4	20

بر طبق جدول، Pcها را درون Vlan های مورد نظر قرار می‌دهیم؛ برای این کار وارد پورت‌هایی می‌شویم که کامپیوتر مورد نظر به آن متصل است، مثلاً در بالا Pc1 به پورت Fa0/1 متصل است که این پورت باید در Vlan 10 قرار بگیرد:

Switch(config)#**interface fastEthernet 0/1**
Switch(config-if)#**switchport mode access**
Switch(config-if)#**switchport access vlan 10**

همان‌طور که مشاهده می‌کنید، در قسمت اول وارد پورت Fa0/1 شده‌ایم و بعدازآن از دستور switchport mode access استفاده کردیم تا مد بر روی Access تنظیم شود و بعدازآن از دستور switchport access vlan 10 استفاده کردیم تا این پورت را وارد Vlan 10 کنیم. بقیه‌ی پورت‌ها هم به صورت زیر انجام می‌شود.

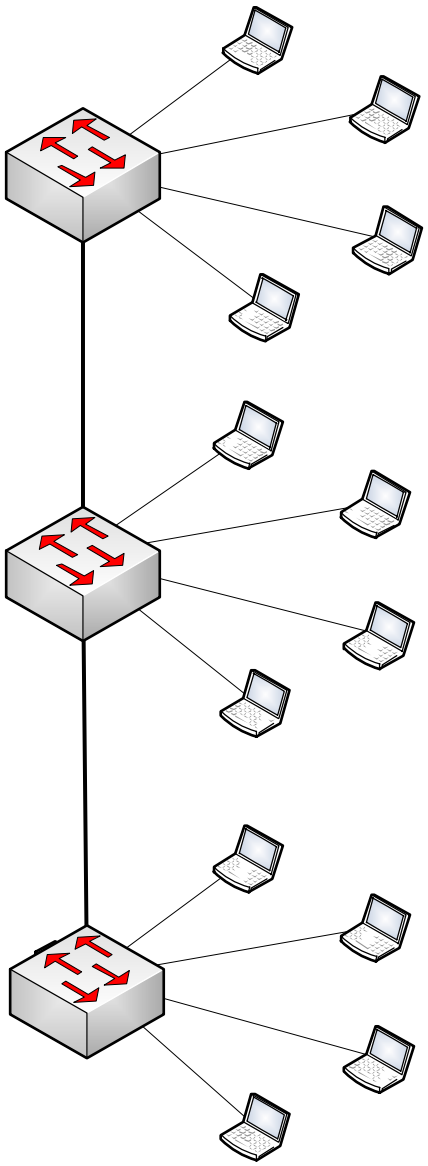
Switch(config)#**int f0/2**
Switch(config-if)# **switchport mode access**
Switch(config-if)# **switchport access vlan 10**

```
Switch(config-if)#int f0/3
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 20
Switch(config-if)#int f0/4
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 20
```

بعد از اتمام کار از طریق PC1، PC4 را Ping کنید که متوجه می‌شوید این کار امکان‌پذیر نیست و آن‌هم به خاطر جدا کردن آن‌ها و قرار دادن داخل دو vlan جدا است و فقط PC1 و PC2 می‌توانند همدیگر را ببینند و باهم در ارتباط باشند، چون در یک Vlan قرار دارند.

Trunk Mode:

قبل تعریف این مد، یک مثال برای درک بهتر این موضوع تعریف می‌کنیم؛ شما مدیر شبکه‌ی یک ساختمان هستید و این ساختمان از سه طبقه تشکیل شده است و در هر طبقه از یک سوئیچ برای شبکه کردن کامپیوترها استفاده شده است و تمام سوئیچ‌ها به هم متصل شده‌اند. نکته‌ی مهم در این قسمت این است که در هر طبقه بخش حسابداری، اداری و فروش وجود دارد و می‌خواهیم تمام بخش‌های هر ساختمان باهم در ارتباط باشند؛ برای این کار شما در هر طبقه، مانند مثال قبل برای هر بخش یک Vlan تعریف می‌کنید و پورت‌ها را داخل Vlan مورد نظر قرار می‌دهید، اما یک مشکل وجود دارد این‌که سوئیچ باید با vlan های دیگر در طبقات مختلف در ارتباط باشند. برای حل این مشکل باید از Trunk استفاده کرد، Trunk روشی برای انتقال Vlan ها در سوئیچ‌های مختلف است و با استفاده از آن این مشکل به راحتی حل می‌شود.



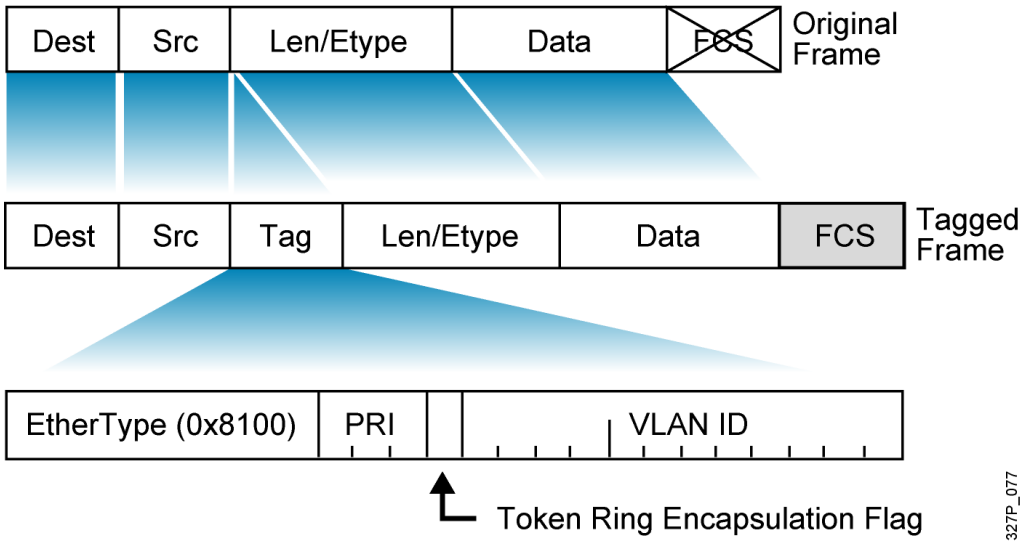
Tag زدن روی فریم‌ها:

برای انتقال Vlan ها در مد Trunk دو روش وجود دارد که از طریق آن یک Vlan شناسایی می‌شود:

- **802.1Q**
- **ISL(Inter-Switch Link Protocol)**

ISL: یک استاندارد برای بسته‌بندی فریم‌ها برای انتقال در یک مسیر یا همان Trunk که این استاندارد مختص شرکت سیسکو بوده و به صورت پیش‌فرض در دستگاه‌های لایه‌ی دوم این شرکت فعال است.

802.1Q: یک استاندارد Open Source است و مختص شرکت خاصی نیست و اگر در شبکه‌ی خود از سوئیچ‌های شرکت‌های متفاوت استفاده می‌کنید، برای برچسب زدن روی فریم‌ها باید از این استاندارد استفاده کنید. این پروتکل ساختار فریم‌ها را به کل تغییر می‌دهد.



فعال کردن پروتکل ISL:

این پروتکل به صورت پیش‌فرض روی سوئیچ‌های شرکت سیسکو فعال است.

فعال کردن پروتکل 802.1Q:

برای فعال کردن این پروتکل باید وارد interface مورد نظر شوید و دستور زیر را وارد کنید:

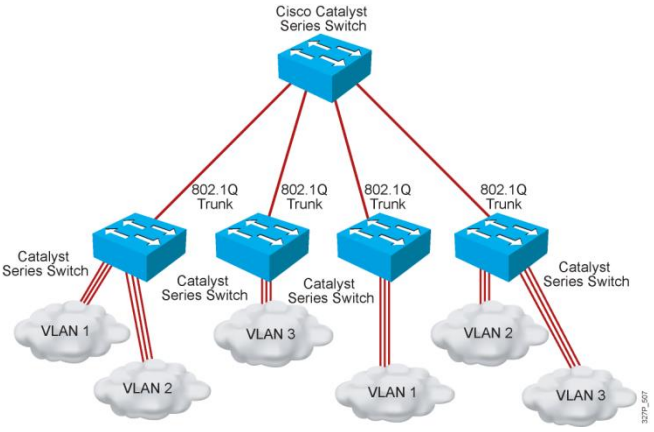
Switch(config-if)#**switchport mode trunk**
Switch(config-if)#**switchport trunk encapsulation dot1q**

با اجرای این دستورات، یک سوئیچ تمام Vlan ها را برچسب‌گذاری می‌کند و از خود عبور می‌دهد. شاید شما بخواهید به سوئیچ بگوئید که فقط Vlan های خاصی از وی عبور کنند؛ برای این منظور از دستور زیر استفاده می‌کنیم:

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

با این دستور فقط Vlan 10 حق عبور دارد و بقیه Vlanها از این سوئیچ عبور نمی‌کنند.

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



در این شکل، سوئیچ‌ها به هم متصل شده‌اند و سوئیچ‌هایی که در زیر قرار دارند از Vlan های مختلفی تشکیل شده‌اند. برای ارتباط Vlan1 به Vlan1 در سوئیچ دیگر، باید پروتکل Trunk را روی پورت‌های سوئیچ که به سوئیچ اصلی متصل است، اجرا کنیم و بعد 802.1Q را راه‌اندازی کنیم تا عملیات برچسب‌گذاری روی Vlan ها را انجام دهد.

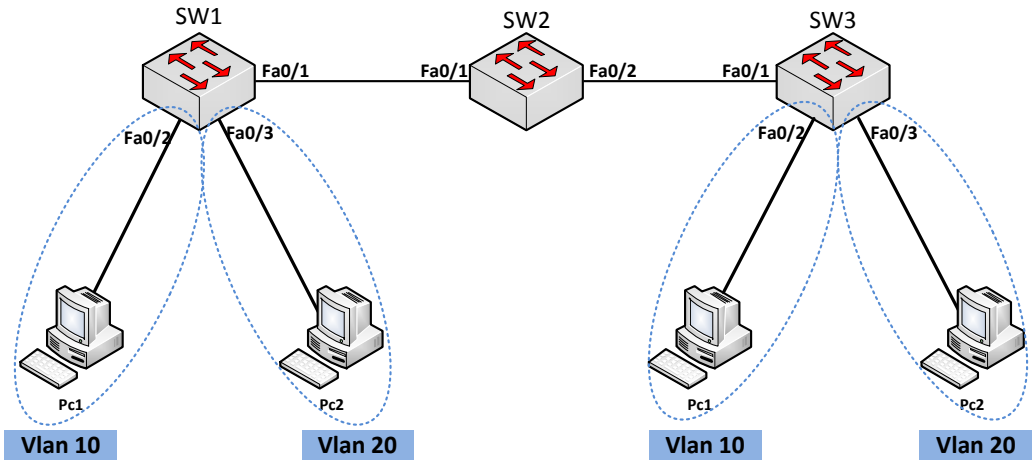
Native Vlan:

همان‌طور که قبلاً گفتیم در تمام سوئیچ‌ها Vlan1 وجود دارد و قادر به ایجاد و یا حذف آن نیستیم، اما وقتی چندین سوئیچ را با پروتکل 802.1Q، Trunk می‌کنید در زمان انتقال Vlan 1 بین سوئیچ‌ها روی آن‌ها هم برچسب‌گذاری می‌شود و همین کار باعث استفاده‌ی بیش از حد از پهنای باند شبکه می‌شود و برای جلوگیری از این کار باید روی پورتی که Trunk شده است، دستور زیر را وارد کنیم:

Switch(config-if)# **switchport trunk native vlan 1**

با این کار، Vlan1 در پروتکل Trunk انتقال داده نمی‌شود.

مثال4:



Station	Ip address	SubnetMask
Pc1	192.168.1.1	255.255.255.0
Pc2	192.168.1.2	255.255.255.0
Pc3	192.168.1.3	255.255.255.0
Pc4	192.168.1.4	255.255.255.0

بعد از این‌که Ip address ها را در pc ها وارد کردیم، نوبت به تعریف Vlan در سوئیچ است. در داخل هر یک از سوئیچ‌ها، Vlan های 10و20 را به صورت زیر تعریف می‌کنیم:

Switch(config)#**vlan 10**
Switch(config)# **vlan 20**

بعد از تعریف Vlan باید پورت‌های متصل به Pc را داخل Vlan های مشخص‌شده قرار دهیم، مثلاً pc1 باید در Vlan 10 قرار بگیرید؛ برای این کار وارد سوئیچ و بعد، وارد interface fa0/2 که به pc1 متصل است، می‌شویم و آن را طبق دستور زیر داخل Vlan 10 قرار می‌دهیم:

Switch(config)#**int f0/2**
Switch(config-if)#**switchport mode access**
Switch(config-if)#**switchport access vlan 10**

بقیه‌ی پورت‌های سوئیچ که به pc متصل است را درون Vlan قرار می‌دهیم.

Switch(config)#**int f0/3**
Switch(config-if)#**switchport mode access**
Switch(config-if)#**switchport access vlan 20**

پورت‌های سوئیچ 3 را به صورتی که در بالا انجام دادیم، درون Vlan قرار می‌دهیم.

بعد از این‌که این کار را انجام دادید، یک Ping از Pc1 به Pc3 بگیرید و مطمئن باشید جواب نمی‌گیرید، به خاطر این‌که پروتکل Trunk روی پورت‌های سوئیچ فعال نشده و به خاطر این ارتباط برقرار نمی‌شود.

وارد SW1 شوید و پورتی که به طرف SW2 می‌رود را Trunk کنید:

Switch(config)#**Interface Fa0/1**
Switch(config-if)#**switchport mode trunk**

بعد از این کار، مدل برچسب‌گذاری روی فریم‌ها را باید مشخص کنید که ISL باشد یا 802.1Q که در برنامه‌ی Packet Tracer به صورت پیش‌فرض dot1q است و ISL وجود ندارد که این کار از شرکت سیسکو بعید است، چون در سوئیچ 2950 استاندارد ISL وجود ندارد، استانداردی که مختص سیسکو است.

بقیه‌ی پورت‌های متصل به سوئیچ‌های دیگر را Trunk کنید:

:SW2

Switch(config)#**Interface Fa0/1**
Switch(config-if)#**switchport mode trunk**
Switch(config)#**Interface Fa0/2**
Switch(config-if)#**switchport mode trunk**

:SW3

Switch(config)#**Interface Fa0/1**
Switch(config-if)#**switchport mode trunk**

بعد از این کار، ارتباط بین Vlan ها برقرار می‌شود و pc1 با pc3 باهم ارتباط برقرار می‌کنند.

بعد از این مثال، سؤالی برای شما ایجاد می‌شود که اگر تعداد سوئیچ‌ها زیاد باشد و ما بخواهیم داخل هرکدام از سوئیچ‌ها vlan تعریف کنیم، کار بسیار وقت‌گیری است. آیا روش دیگری هم وجود دارد؟

بله، روش دیگری هم وجود دارد که می‌توانیم در یک سوئیچ یا هر سوئیچی در شبکه‌ی Vlan تعریف کنید و این Vlan ها به صورت خودکار وارد سوئیچ دیگر می‌شوند که به این روش VLAN Trunking Protocol (VTP) می‌گویند.

کار با (VLAN Trunking Protocol)VTP

این پروتکل توسط شرکت سیسکو ارائه شده است، اما انحصاری نیست و شرکت‌های دیگر می‌توانند از این پروتکل استفاده کنند. این پروتکل برای مدیریت Vlan ها و ایجاد امنیت به کار برده می‌شود. VTP به مدیر شبکه، اجازه‌ی ایجاد، حذف، تغییر نام و ... را می‌دهد. چند ویژگی این پروتکل:

- پیکربندی Vlan ها به صورت سریع در همه‌ی سوئیچ‌ها.
- نظارت کامل بر کار Vlan ها در یک زمان.
- ایجاد Vlan به صورت Plug-and-Play.

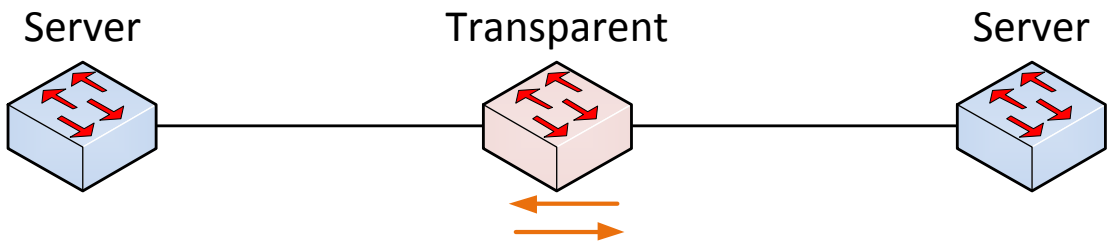
VTP دارای سه حالت است.

1- Server Mode: در این حالت یک سوئیچ می‌تواند Vlan ها را ایجاد، حذف و به طور کامل مدیریت کند که به صورت پیش‌فرض همه‌ی سوئیچ‌ها در مد Server قرار دارند.

2- Client Mode: در این حالت سوئیچ به سرور گوش می‌دهد و نمی‌تواند یک Vlan را ایجاد، حذف و مدیریت کند و همه چیز از طریق Server به وی اعمال می‌شود.

3- Transparent Mode: این سوئیچ فقط Vlan هایی که به وی می‌رسد را از خود عبور می‌دهد و کاری روی آن‌ها انجام نمی‌دهد، اما این سوئیچ می‌تواند Vlan را تعریف و یا حذف کند، اما به کسی اعلام نمی‌کند که این Vlan های من است؛ کلاً سوئیچ خودمختاری است و همه‌ی کارها را خودش انجام می‌دهد. به شکل صفحه‌ی بعد توجه کنید.

در بین دو سوئیچ Server یک سوئیچ transparent قرار گرفته است. این سوئیچ فقط Vlan هایی را که از دو سرور برای وی ارسال می‌شود به سوئیچ دیگر انتقال می‌دهد و کاری روی این Vlan ها انجام نمی‌دهد، اما خودش می‌تواند vlan ایجاد کند و روی آن‌ها کار کند، ولی VLan های مربوط به خودش را به کسی نمی‌دهد.

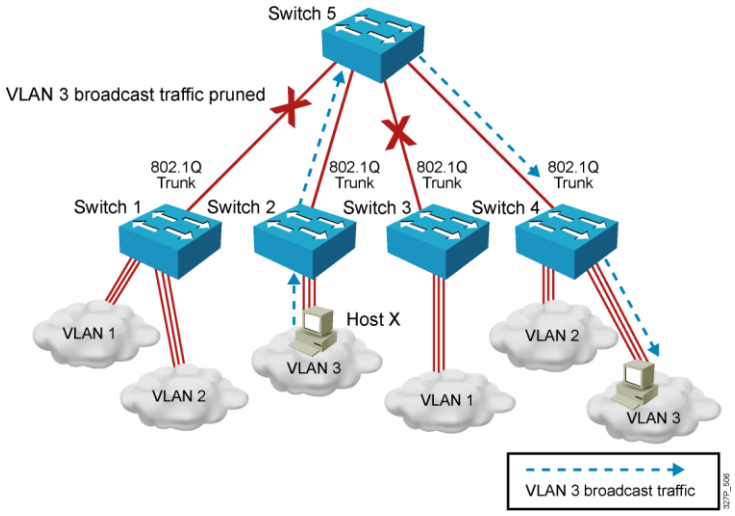


:VTP domain

به ناحیه‌ای گفته می‌شود که سوئیچ‌هایی داخل آن عضو هستند و Vlan های خود را با همدیگر به اشتراک می‌گذارند و سوئیچ‌ها تنها می‌توانند در یک VTP Doamin عضو شوند و نمی‌توانند Vlan های خود را با VTP domain دیگری به اشتراک بگذارند.

:VTP Pruning

در شکل زیر به سوئیچ 2 یک pc متصل است و در Vlan 3 قرار دارد و می‌خواهد با pc دیگر در سوئیچ 4 ارتباط برقرار کند. همان‌طور که می‌دانید سوئیچ، بعد از رسیدن درخواست به پورت، خود آن را به صورت Broadcast برای دیگر سوئیچ‌ها که به آن‌ها Trunk شده است، ارسال می‌کند، اما با فعال کردن VTP Pruning این کار انجام نمی‌شود و فقط پیام Broadcast به سوئیچ‌هایی ارسال می‌شود که یکی از پورت‌های آن‌ها در Vlan مورد نظر قرار داشته باشد.

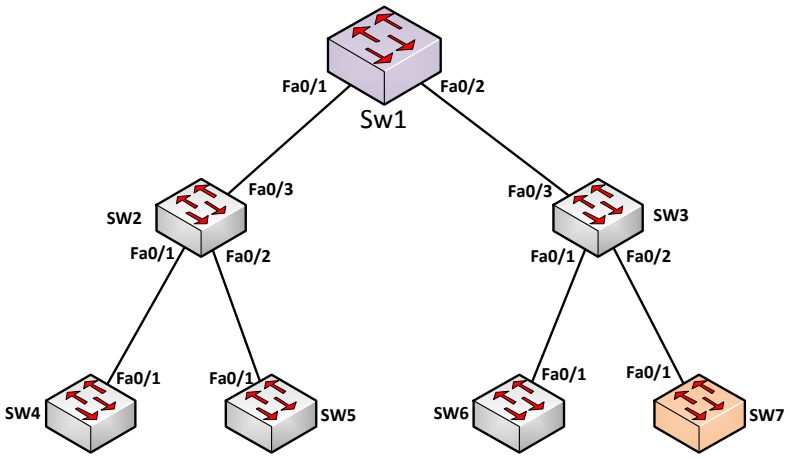


فعال کردن VTP:

برای فعال کردن Vtp باید از دستورات زیر در سوئیچ استفاده کنیم:

Switch# configure terminal
Switch(config)# vtp mode [server | client | transparent]
Switch(config)# vtp domain *domain-name*
Switch(config)# vtp password *password*
Switch(config)# vtp pruning
Switch(config)# end

با یک مثال این دستورات را داخل آن به کار می‌بریم:



در این مثال، سوئیچ 1 به عنوان سرور و سوئیچ 7 به عنوان Transparent و بقیه، به عنوان Client هستند.

همیشه به یاد داشته باشید که قبل از ایجاد VTP، حتماً تمام بورت‌های سوئیچ‌ها که به هم متصل هستند را در وضعیت Trunk قرار دهیم تا Vlan ها بتوانند بین سوئیچ‌ها حرکت کنند، پس در پورت‌های سوئیچ‌ها که به سوئیچ دیگری متصل است دستور زیر را وارد می‌کنیم، مثلاً در سوئیچ یک پورت Fa0/1 آن با پورت Fa0/3 سوئیچ دو در ارتباط است و باید این پورت‌ها در وضعیت Trunk قرار بگیرند:

Switch(config)#**int f0/1**
Switch(config-if)#**switchport mode trunk**

بعد از این‌که در تمام سوئیچ‌ها، پورت‌ها را در وضعیت Trunk قرار دادیم، نوبت به ایجاد VTP است. برای این کار وارد سوئیچ 1 می‌شویم و دستورات زیر را وارد می‌کنیم:

Switch(config)# **vtp mode server**

Device mode already VTP SERVER.

با دستور بالا این سوئیچ به عنوان سرور انتخاب می‌شود، البته این وضعیت به صورت پیش‌فرض فعال است.

```
Switch(config)#vtp domain cisco.com
Changing VTP domain name from NULL to cisco.com
```

در این قسمت هم، نام دومین را به cisco تغییر می‌دهیم، توجه داشته باشید تمام سوئیچ‌ها برای ارتباط باهم باید در یک domain قرار داشته باشند.

```
Switch(config)#vtp password 123
Setting device VLAN database password to 123
```

رمز عبور را برای این VTP فعال می‌کنیم که گزینه‌ی مهمی در ارتباط با سوئیچ‌های دیگر است. با قرار دادن رمز عبور، کسی دیگر نمی‌تواند بدون اجازه، خودش را عضو این Domain کند. سعی کنید رمز عبور را به صورت پیچیده وارد کنید.

با دستورات بالا VTP را روی سوئیچ 1 فعال کردیم و این سوئیچ به عنوان سوئیچ سرور نقش اصلی را در این شبکه بازی می‌کند. بقیه‌ی سوئیچ‌ها به جز سوئیچ 7 باید در مد VTP Client قرار بگیرند و اطلاعات را از VTP Server دریافت کنند:

سوئیچ 2:

```
Switch(config)#vtp mode client
Setting device to VTP CLIENT mode.
Switch(config)#vtp password 123
Setting device VLAN database password to 123
Switch(config)#vtp domain cisco.com
Domain name already set to cisco.com.
```

سوئیچ 3:

```
Switch(config)#vtp m c
Setting device to VTP CLIENT mode.
Switch(config)#vtp pass 123
Setting device VLAN database password to 123
Switch(config)#vtp d cisco.com
Domain name already set to cisco.com.
```

سوئیچ 4:

```
Switch(config)#vtp m c
Setting device to VTP CLIENT mode.
Switch(config)#vtp pass 123
Setting device VLAN database password to 123
Switch(config)#vtp d cisco.com
Domain name already set to cisco.com
```

سوئیچ 5:

```
Switch(config)#vtp m c
Setting device to VTP CLIENT mode.
Switch(config)#vtp pass 123
Setting device VLAN database password to 123
Switch(config)#vtp d cisco.com
Domain name already set to cisco.com.
```

سوئیچ 6:

```
Switch(config)#vtp m c
Setting device to VTP CLIENT mode.
Switch(config)#vtp pass 123
Setting device VLAN database password to 123
Switch(config)#vtp d cisco.com
Domain name already set to cisco.com.
```

سوئیچ 7 را باید در مد Transparent قرار دهیم:

```
Switch(config)#vtp mode transparent
Setting device to VTP TRANSPARENT mode.
Switch(config)#vtp d cisco.com
Domain name already set to cisco.com.
Switch(config)#vtp pass 123
Setting device VLAN database password to 123
```

بعد از اتمام کار، نوبت به تعریف Vlan در سوئیچ 1 می‌رسد که سوئیچ سرور است. در این سوئیچ، Vlan های 100، 200، 300 را تعریف می‌کنیم. با اجرای دستور Show vlan brief، می‌توانید لیست Vlan های ساخته‌شده را مشاهده کنید.

```
Switch#show vlan brief

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/3, Fa0/4, Fa0/5, Fa0/6
                                                 Fa0/7, Fa0/8, Fa0/9, Fa0/10
                                                 Fa0/11, Fa0/12, Fa0/13, Fa0/14
                                                 Fa0/15, Fa0/16, Fa0/17, Fa0/18
                                                 Fa0/19, Fa0/20, Fa0/21, Fa0/22
                                                 Fa0/23, Fa0/24, Gig1/1, Gig1/2
100  VLAN0100                          active
200  VLAN0200                          active
300  VLAN0300                          active
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
```

1005 trnet-default active

تا اینجا در سوئیچ یک، Vlan ها را تعریف کردیم، چون این سوئیچ سرور است. بقیه‌ی سوئیچ‌ها به علت VTP Client بودن Vlan ها را از سوئیچ سرور دریافت می‌کنند. اگر شما در سوئیچ 6 دستور Show vlan brief را اجرا کنید، تمام vlan هایی را که در سوئیچ یک ساختیم را در این سوئیچ هم نمایش می‌دهد:

```
Switch#show vlan brief

VLAN Name                       Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                    active    Fa0/2, Fa0/3, Fa0/4, Fa0/5
                                          Fa0/6, Fa0/7, Fa0/8, Fa0/9
                                          Fa0/10, Fa0/11, Fa0/12, Fa0/13
                                          Fa0/14, Fa0/15, Fa0/16, Fa0/17
                                          Fa0/18, Fa0/19, Fa0/20, Fa0/21
                                          Fa0/22, Fa0/23, Fa0/24, Gig1/1
                                          Gig1/2
100  VLAN0100                   active
200  VLAN0200                   active
300  VLAN0300                   active
1002 fddi-default               active
1003 token-ring-default         active
1004 fddinet-default            active
1005 trnet-default              active
```

اگر در سوئیچ 7 این دستور را وارد کنید، چیزی مشاهده نمی‌کنید، چون این سوئیچ در مد Transparent قرار گرفته است که آن را توضیح دادیم.

دستور Show Vtp Status:

با این دستور اطلاعاتی را درباره‌ی VTP و اجزای آن که روی سوئیچ برقرار شده است، نمایش می‌دهد:

```
Switch#show vtp status
VTP Version                     : 2
Configuration Revision          : 3
Maximum VLANs supported locally : 255
Number of existing VLANs        : 8
VTP Operating Mode              : Server
VTP Domain Name                 : cisco.com
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
```

MD5 digest : 0x5C 0xF1 0xFA 0x4C 0xCB 0x3F 0xB8 0xD3
Configuration last modified by 0.0.0.0 at 3-1-93 00:40:23
Local updater ID is 0.0.0.0 (no valid interface found)

دستور Show vtp counters:

این دستور تعداد بسته‌های ارسالی و دریافتی پروتکل VTP را به ما نشان می‌دهد.

Summary advertisements: اطلاعاتی است که هر 300 ثانیه توسط Server به بقیه‌ی سوئیچ‌ها در شبکه ارسال می‌شود.

Subset advertisements: شامل تغییرات در یک vlan است و توسط VTP server ارسال می‌شود.

```
Switch#show vtp counters
VTP statistics:
Summary advertisements received    : 45
Subset advertisements received     : 14
Request advertisements received    : 9
Summary advertisements transmitted : 24
Subset advertisements transmitted  : 14
Request advertisements transmitted : 0
Number of config revision errors   : 3
Number of config digest errors     : 0
Number of V1 summary errors        : 0


VTP pruning statistics:

Trunk          Join Transmitted Join Received   Summary advts received from
                                                 non-pruning-capable device
---------------- ---------------- ---------------- --------------------------
```

دستور Show vtp Password:

رمز عبور قرار داده‌شده روی Vtp Password را نمایش می‌دهد.

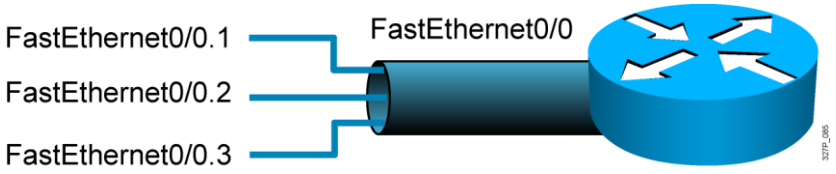
Inter Vlan Routing:

آیا این موضوع به ذهن شما رسیده که وقتی دو کامپیوتر در دو Vlan متفاوت قرار دارند، راهی وجود دارد که این دو بتوانند باهم در ارتباط باشند؟، بله این راه از طریق Inter vlan Routing امکان‌پذیر است، یعنی از طریق یک روتر ارتباط Vlan های تعریف‌شده در سوئیچ را باهم برقرار می‌کنیم.

همان‌طور که می‌دانید سوئیچ‌های لایه‌ی 2، مانند 2950 قادر به انجام عملیات روتینگ نمی‌باشند و برای همین از روتر برای انجام عملیات روتینگ بین Vlan ها استفاده می‌شود.

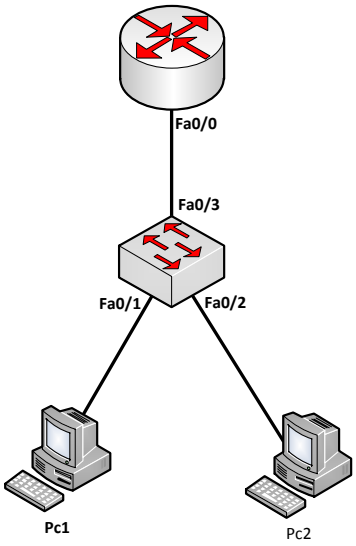
ارتباط Vlan های مختلف هم می‌تواند از طریق روتر انجام گیرد و هم از طریق سوئیچ‌هایی که در لایه‌ی 3 کار می‌کنند.

به شکل زیر توجه کنید، برای انجام عملیات روتینگ روی روتر فقط از یک interface فیزیکی استفاده می‌شود و برای ارتباط با vlan ها از پورت‌های مجازی استفاده می‌کنند که قابلیت Encapsulation را دارند. روتر برای انجام عملیات روتینگ باید یک اینترفیس داخل Vlan داشته باشد، یعنی اگر 4 تا vlan داریم، باید 4 تا پورت روتر را به سوئیچ اتصال دهیم که باعث به هدر رفتن پورت‌های روتر و افزایش هزینه می‌شود و به خاطر همین از یک اینترفیس فیزیکی به همراه اینترفیس مجازی داخل آن استفاده می‌کنند.



مثالی از Inter Vlan Routing:

مانند شکل یک روتر، سوئیچ و دو PC را به صفحه اضافه کنید و به صورت زیر به هم متصل کنید:



وارد سوئیچ شوید و پورت متصل به روتر را در Trunk قرار دهید، چون مسئول انتقال Vlan ها است:

```
Switch(config)#interface fastEthernet 0/3
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport trunk encapsulation dot1q
```

همان‌طور که می‌دانید dot1q روی سوئیچ‌های سری 2500 به صورت پیش‌فرض فعال است و لازم به واردکردن دستور switchport trunk encapsulation dot1q نیست.

بعد از این کار، دو vlan با شماره‌های 100 و 200 تعریف کنید.

```
Switch(config)#vlan 100
Switch(config-vlan)#ex
Switch(config)#vlan 200
```

پورت‌های متصل به pc را داخل Vlan قرار دهید، pc1 داخل Vlan 100 و pc2 داخل Vlan 200.

```
Switch(config)#int f0/1
Switch(config-if)#sw m ac
Switch(config-if)#sw ac vlan 100

Switch(config-if)#int f0/2
Switch(config-if)#sw m ac
Switch(config-if)#sw ac vlan 200
```

حالا وارد روتر شوید و کارهای زیر را انجام دهید:

در این سناریو، ما احتیاج به دو اینترفیس مجازی داریم. پورت سوئیچ به پورت Fa0/0 متصل است، پس اینترفیس مجازی به صورت زیر تعریف می‌شود:

```
Router(config)#int f0/0.100
Router(config-subif)#encapsulation dot1Q 100
Router(config-subif)#ip add 192.168.1.1 255.255.255.0
Router(config-subif)#int f0/0.200
Router(config-subif)#encapsulation dot1Q 200
Router(config-subif)#ip add 192.168.2.1 255.255.255.0
Router(config-subif)#int f0/0
Router(config-if)#no shutdown
```

به دقت به دستورات توجه کنید؛ در قدم اول int f0/0.100 را نوشتیم که با این دستور، وارد اینترفیس مجازی با شماره‌ی 100 که روی interface f0/0 قرار دارد، شدیم. بعد از آن، روش برچسب‌زنی را مشخص کردیم، چون در مرحله‌ی Trunk روی سوئیچ، dot1Q را انتخاب کردیم. در این قسمت هم، بعد از encapsulation باید dot1Q قرار داشته باشد. بعد از آن، عدد 100 که نمایانگر Vlan 100 است و ارتباط مستقیم با Vlan 100 دارد و

در ادامه، ip address مورد نظر را وارد کردیم و همین کار را در پورت مجازی int f0/0.200 هم انجام دادیم، اما با تغییر شماره‌ی Vlan و شماره‌ی ip، بعد از اتمام کار وارد اینترفیس فیزیکی می‌شویم و آن را فعال می‌کنیم.
نکته: دستور No Shutdown را در اینترفیس مجازی وارد نکنید، چون پورت اصلی نیست و برای ارتباط باید پورت فیزیکی یا اصلی روشن شود.
در این قسمت وارد pc ها می‌شویم و Ip address و Defualt Gateway را برای آن‌ها تعریف می‌کنیم:
برای pc1 به این صورت تعریف می‌کنیم:

IP Address	192.168.1.2
Subnet Mask	255.255.255.0
Default Gateway	192.168.1.1

برای pc2 به این صورت تعریف می‌کنیم:

IP Address	192.168.2.2
Subnet Mask	255.255.255.0
Default Gateway	192.168.2.1

بعد از اتمام کار، دو pc که در Vlan های مختلف قرار دارند، می‌توانند همدیگر را ببینند. اگر از pc2، pc1 را Pnig کنیم، به صورت زیر جواب می‌دهد:

PC>**ping 192.168.1.2**

Pinging 192.168.1.2 with 32 bytes of data:

Request timed out.
Reply from 192.168.1.2: bytes=32 time=0ms TTL=127
Reply from 192.168.1.2: bytes=32 time=10ms TTL=127
Reply from 192.168.1.2: bytes=32 time=0ms TTL=127

Ping statistics for 192.168.1.2:
  Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
  Minimum = 0ms, Maximum = 10ms, Average = 3ms

امنیت در سوئیچ:

امنیت یکی از مهم‌ترین موضوعات در سوئیچ‌ها است که باهم به این موضوع می‌پردازیم.

امنیت از طریق قرار دادن رمز عبور روی پورت consol که قبلاً در روتر این کار را انجام دادیم.

Console Password

```
SwitchX(config)#line console 0
SwitchX(config-line)#login
SwitchX(config-line)#password cisco
```

امنیت در VTY یا همان خط مجازی که از طریق این روش به سوئیچ یا روتر Telnet می‌کنیم:

Virtual Terminal Password

```
SwitchX(config)#line vty 0 4
SwitchX(config-line)#login
SwitchX(config-line)#password sanjose
```

ایجاد رمز عبور از طریق تعریف Enable Password:

Enable Password

```
SwitchX(config)#enable password cisco
```

ایجاد رمز عبور از طریق تعریف Secret Password:

Secret Password

```
SwitchX(config)#enable secret sanfran
```

Hash کردن تمام Password های بکار برده شده در سوئیچ از طریق فرمان زیر و حذف کردن این دستور:

Service Password-Encryption Commands

```
SwitchX(config)#service password-encryption
SwitchX(config)#no service password-encryption
```

3031P 256

Port Security:

شما وقتی یک سوئیچ را در یک اتاق قرار می‌دهید و کابل‌های Pc را به سوئیچ متصل می‌کنید و این pc ها از خدمات شبکه بهره می‌برند، شاید یک نفر بدون اجازه بخواهد از طریق لپ‌تاپ خود وارد شبکه‌ی شما شود و

یکی از کابل‌های pc های متصل به سوئیچ را درآورد و کابل لپ‌تاپ خود را به سوئیچ متصل می‌کند و همه‌ی اطلاعات را به دست می‌آورد. برای جلوگیری از این کار، باید روی پورت‌های سوئیچ امنیت ایجاد کنید که این کار به صورت زیر قابل انجام است.

باید در یک پورت سوئیچ، دستورات زیر را وارد کنید:

```
SwitchX(config)#interface fa0/5
SwitchX(config-if)#switchport mode access
SwitchX(config-if)#switchport port-security
SwitchX(config-if)#switchport port-security maximum 1
SwitchX(config-if)#switchport port-security mac-address sticky
SwitchX(config-if)#switchport port-security violation shutdown
```

اول وارد اینترفیس مورد نظر می‌شویم، بعد با دستور switchport mode access پورت مورد نظر را در حالت Access قرار می‌دهیم. با دستور switchport port-security این دستور اجرا می‌شود و دستور switchport port-security maximum 1، یعنی حداکثر کامپیوتر یا دستگاهی که می‌تواند به این پورت متصل شود، 1 دستگاه است و دستور switchport port-security mac-address sticky می‌گوید که Mac address کامپیوتر یا دستگاهی که به این پورت متصل شده را دریافت کن و در جدول Mac Table قرار بده. بعد از آن، هیچ Mac address دیگری را از این پورت قبول نکن و در آخر دستور switchport port-security violation shutdown را وارد می‌کنیم که می‌گوید اگر کسی خواست دستگاه دیگری را به جای دستگاه قبلی جا بزند، این پورت را shutdown کن.

توجه داشته باشید که این پورت زمانی که shutdown شد، باید از طریق مدیر شبکه no shutdown شود.

با دستور زیر، port-security فعال‌شده روی پورت مورد نظر نمایش داده می‌شود.

```
Switch#show port-security interface f0/1
Port Security              : Enabled
Port Status                : Secure-up
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
```

با دستور زیر، Mac address ذخیره‌شده در جدول نمایش داده می‌شود.

```
Switch#show port-security address
                          Secure Mac Address Table
------------------------------------------------------------------------------
Vlan    Mac Address       Type                  Ports             Remaining Age
                                                                    (mins)
----    -----------       ----                  -----             -------------
100     0060.70C9.CD3C    SecureSticky          FastEthernet0/1             -
------------------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 0
Max Addresses limit in System (excluding one mac per port) : 1024
```

Access List

از Access List برای مدیریت ترافیک در شبکه استفاده می‌شود، مثلاً شما می‌توانید به یک یا چند کامپیوتر اجازه دسترسی به منابع خاصی از شبکه را ندهید که یکی از مهم‌ترین بخش‌های کار در شبکه است.

در کل دو نوع Access List در شبکه داریم که با شماره‌های مختلف مشخص شده‌اند.

- Access List استاندارد با شماره‌های 1 تا 99 و 1300 تا 1999.
- Access List پیشرفته با شماره‌های 100 تا 199 و 2000 تا 2699.

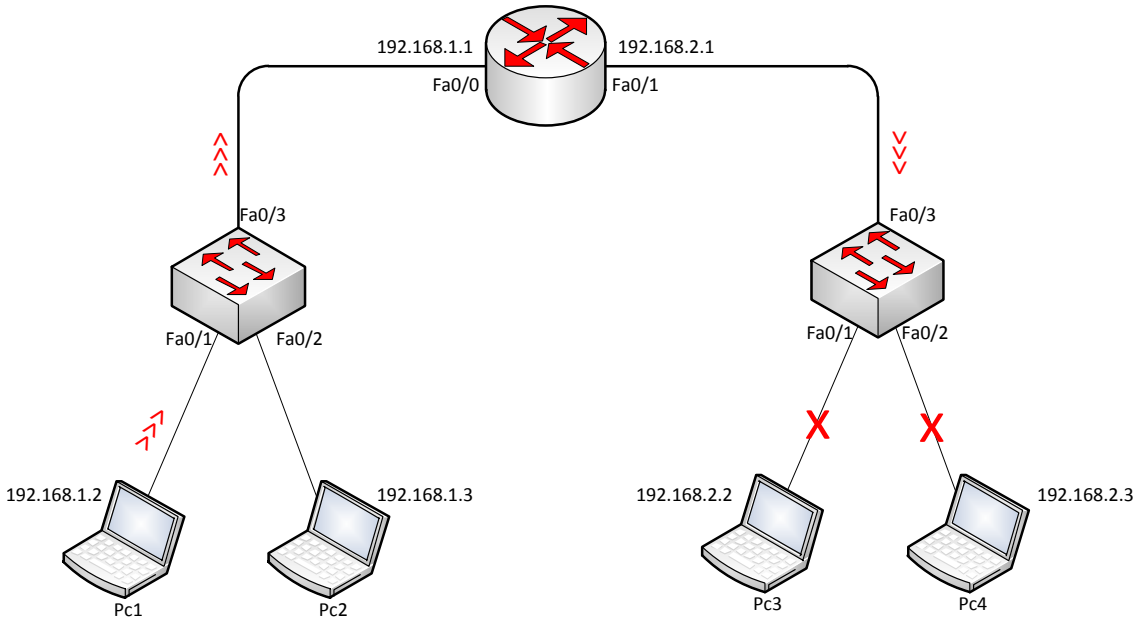
Access List استاندارد:

این نوع از Access List ها از شماره‌های ذکرشده در بالا استفاده می‌کنند و فقط ترافیک‌های مربوط به مبدأ را مورد بررسی قرار می‌دهند. با نحوه‌ی کار این Access List آشنا می‌شویم.

Deny: این دستور در access List برای جلوگیری از دسترسی یک Node خاص به یک شبکه‌ی دیگر است که بسیار پرکاربرد و خطرناک است، به دلیل اینکه با یک اشتباه، نصف یا کل شبکه از کار می‌افتد.

Permit: این دستور ضد دستور Deny است و برای دسترسی به شبکه کاربرد دارد.

در این مثال می‌خواهیم از دسترسی pc1 به Pc3 و Pc4 جلوگیری کنیم.



وارد روتر می‌شویم و دستورات زیر را به ترتیب وارد می‌کنیم:

Router(config)#**ip access-list standard dpc1**

در قسمت اول باید access List را تعریف کنیم؛ هم می‌توانیم با نام و هم می‌توانیم با شماره تعریف کنیم که در این قسمت از نام dpc1 استفاده کردیم. شما می‌توانید هر اسم دیگری در این قسمت قرار دهید و یا از شماره استفاده کنید، اما همیشه سعی کنید از نام استفاده کنید که مدیریت آن آسان باشد.

Router(config-std-nacl)#**deny 192.168.1.2 0.0.0.0**

با این دستور، ip address مربوط به pc1 را Deny می‌کنیم. اگر توجه کنید در قسمت اول، دستور Deny و بعد، ip address مربوط به pc1 و بعد از آن که مهم است از Wildcard Mask تأکیدی استفاده کردیم، یعنی استفاده از 4 تا صفر که تأکید بر Deny کردن همین ip را دارد. اگر wild Card Mask را به صورت 0.0.0.255 وارد کنیم، یعنی تمام ip address ها در رنج 192.168.1.0 فیلتر شود، پس سعی کنید از Wild card Mask تأکیدی استفاده کنید.

Router(config-std-nacl)#**permit any**

بعد از Deny حتماً از Permit استفاده کنید، چون هر زمان که از Deny استفاده می‌کنید، بقیه‌ی شبکه هم deny می‌شود و به خاطر همین از Permit Any استفاده می‌کنیم تا بقیه‌ی شبکه اجازه‌ی دسترسی داشته باشند.

بعد از تعریف کامل access List باید به روتر بگوییم که این فیلترینگ را روی کدام پورت انجام بدهد، پس وارد روتر می‌شویم. اگر توجه کنید می‌خواهیم دسترسی pc1 به pc3 و pc4 جلوگیری کنیم، پس باید در پورت Fa0/1 روتر دستور زیر را وارد کنیم:

```
Router(config)# int f0/1
Router(config-if)#ip access-group dpc1 out
```

به دستور توجه کنید، ip Access-group را تعریف و بعد از آن، نام Access List که ایجاد کرده‌ایم را وارد می‌کنیم. گفتیم ترافیک این access List در زمان خروج از اینترفیس فیلتر شود. اگر به جای out، گزینه‌ی in را انتخاب می‌کردید، این بدان معنا بود که شما access List را برای شبکه‌ی 192.168.2.0 نوشتید که این امر اشتباه است و این access list عمل نمی‌کند.

و حالا اگر از pc1 به pc3 و pc4، Ping کنید، با پیام زیر مواجه می‌شوید:

```
PC>ping 192.168.2.3

Pinging 192.168.2.3 with 32 bytes of data:

Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.
```

و حالا اگر از طریق pc2 بخواهید pc3 و pc4 را Ping کنید، جواب خواهید گرفت.

```
PC>ping 192.168.2.3

Pinging 192.168.2.3 with 32 bytes of data:

Reply from 192.168.2.3: bytes=32 time=1ms TTL=127
Reply from 192.168.2.3: bytes=32 time=0ms TTL=127
Reply from 192.168.2.3: bytes=32 time=0ms TTL=127
Reply from 192.168.2.3: bytes=32 time=0ms TTL=127

Ping statistics for 192.168.2.3:
   Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
   Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

برای قرار دادن توضیحات روی یک Access List، باید از دستور Remark استفاده کرد:

```
Router(config-std-nacl)# remark Access List Deny Pc1
```

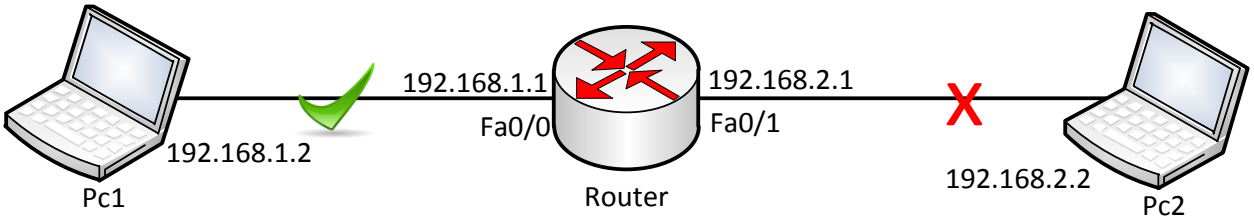
برای مشاهده‌ی این دستور باید وارد Running-config شوید تا این پیام را مشاهده کنید.

Router# **show Running-Config**
access-list 20 remark Access List Deny Pc1

Access List پیشرفته:

این نوع Access List از شماره‌های 100 تا 199 و 2000 تا 2699 تشکیل شده است و می‌تواند ترافیک مربوط به مبدأ و مقصد را مورد بررسی قرار دهد، حتی می‌توانید پروتکل‌ها یا برنامه‌های خاص را Deny یا Permit کنید.

مثال5: در این مثال می‌خواهیم Telnet را روی روتر راه‌اندازی کنیم و accessList بنویسیم که از دسترسی Pc2 به Telnet جلوگیری کند.



وارد روتر می‌شویم و به صورت زیر عمل می‌کنیم:

Router(config)#**ip access-list extended Dpc2tel**

یک access List extended با نام Dpc2tel را ایجاد کردیم که شما می‌توانید به جای این نام از نام دلخواه یا از شماره‌های ذکرشده در قسمت قبل استفاده کنید.

Router(config-ext-nacl)# **deny tcp 192.168.2.0 0.0.0.255 any eq 23**

در این قسمت برای Deny کردن pc2 برای جلوگیری از Telnet، باید از پروتکل Tcp و پورت 23 که مربوط به Telnetاست را Deny کنید. در زیر جدول مربوط به پروتکل‌ها و شماره‌ی پورت‌ها مشخص شده است.

Decimal	Keyword	Description	Protocol
0		Reserved	
1-4		Unassigned	
20	FTP-DATA	FTP (data)	TCP
21	FTP	FTP	TCP
23	TELNET	Terminal connection	TCP
25	SMTP	SMTP	TCP
42	NAMESERVER	Host name server	UDP
53	DOMAIN	DNS	TCP/UDP
69	TFTP	TFTP	UDP
70		Gopher	TCP/IP
80	HTTP	WWW	TCP
133-159		Unassigned	
160-223		Reserved	
162		FNP	UDP
224-241		Unassigned	
242-251		Unassigned	

Router(config-ext-nacl)# **deny tcp 192.168.2.0 0.0.0.255 any eq 23**

چون در اینجا قرار است که Telnet را برای pc2 ببندیم، از پروتکل TCP طبق جدول و از پورت 23 که مربوط به Telnet است، استفاده می‌کنیم، پس به این صورت بخوانیم که Deny کن، پروتکل TCP را برای شبکه‌ی 192.168.2.0 با Wild Card mask، 0.0.0.255 و با پورت 23 که مربوط به Telnet است.

نکته: بعد از این کار، تمام ترافیک مربوط به شبکه‌ی 192.168.2.0 فیلتر می‌شود، به خاطر این باید از دستور زیر در آخر کار برای Permit دادن به بقیه‌ی شبکه استفاده کرد.

Router(config-ext-nacl)#**permit ip any any**

با این کار، pc2 می‌تواند با روتر ارتباط داشته باشد و فقط پروتکل Telnet بسته شده است. اگر یادتان باشد در access List standard همه‌ی ترافیک مربوط به یک دستگاه فیلتر می‌شد و حق دسترسی به هیچ عنوان نداشت، اما در accesslist Extended این چنین نیست و فقط pc2 نمی‌تواند Telnet کند، اما می‌تواند روتر را ping کند.

در ادامه باید این access List را روی پورت روتر فعال کنیم:

Router(config-if)#**ip access-group Dpc2tel in**

پس این دستور به این صورت خوانده می‌شود که Ip access-group Dpc2tel را بر روی این پورت به صورت ورودی فعال کن، ورودی یعنی این‌که Pc2 در حال ورود به روتر است. اگر از Pc2 به روتر Telnet کنیم، جواب نمی‌دهد.

PC>**telnet 192.168.2.1**
Trying 192.168.2.1 ...
% Connection timed out; remote host not responding

اما اگر به روتر ping کنیم، جواب می‌گیریم:

PC>**ping 192.168.2.1**

Pinging 192.168.2.1 with 32 bytes of data:

Reply from 192.168.2.1: bytes=32 time=1ms TTL=255
Reply from 192.168.2.1: bytes=32 time=0ms TTL=255
Reply from 192.168.2.1: bytes=32 time=0ms TTL=255
Reply from 192.168.2.1: bytes=32 time=0ms TTL=255

Ping statistics for 192.168.2.1:
  Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
  Minimum = 0ms, Maximum = 1ms, Average = 0ms

دستور Show access-lists:

این دستور، تعداد Access List های موجود در روتر را با جزئیات نمایش می‌دهد:

```
Router(config)#do sh ip access-list
Extended IP access list Dpc2tel
```

دوستان توجه داشته باشید که دستورات به صورت خلاصه‌شده وارد شده است و چون در مد Global هستیم، در اول دستور از do استفاده کردیم.

دستورshow access-list:

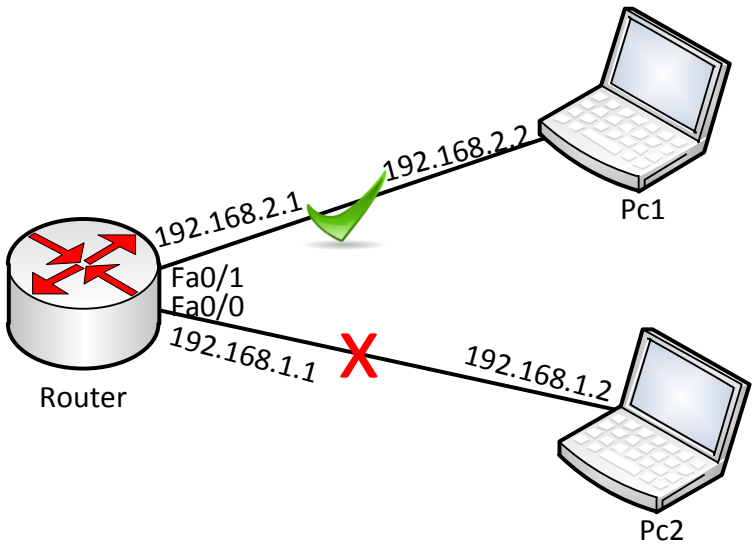
با این دستور می‌توانیم جزئیات یک access-list را مشاهده کنیم:

```
Router#show access-lists Dpc2tel
Extended IP access list Dpc2tel
   deny tcp 192.168.2.0 0.0.0.255 any eq telnet (24 match(es))
   permit ip any any (8 match(es))
```

در ادامه از access-List بسیار استفاده می‌کنیم و این دستور یک دستوراساسی در سیسکو است.

استفاده از Access-List در پورت مجازی VTY:

شما می‌توانید با تعریف یک ACCESS List و فعال کردن آن در پورت Vty به یک ip اجازه‌ی Telnet بدهید یا ندهید. برای انجام این کار به مثال زیر توجه کنید:



مانند شکل بالا، یک روتر و دو pc به صفحه اضافه و به هم متصل کنید و به پورت‌های مورد نظر ip دهید.

وارد روتر شوید و access-List زیر را وارد کنید:

```
Router(config)#ip access-list standard 10
Router(config-std-nacl)#permit 192.168.1.0 0.0.0.255
```

در دستورات بالا، یک access-list استاندارد با شماره‌ی 10 تعریف کردیم و بعد از آن به شبکه‌ی 192.168.1.0 اجازه دسترسی دادیم و زمانی که یک Permit برای یک شبکه تعریف می‌کنیم، بقیه‌ی شبکه‌ها Deny می‌شوند.
بعد از ایجاد Access-list، وارد پورت Line Vty می‌شویم و telnet را روی پورت‌ها فعال می‌کنیم:

```
Router(config)#line vty 0 15
Router(config-line)#password 123
Router(config-line)#login
Router(config-line)#access-class 10 in
```

در دستور اول وارد پورت15 0 VTY می‌شویم و بعد، رمز عبور را بر روی پورت‌ها قرار می‌دهیم، سپس با دستور login می‌گوییم که در زمان telnet شدن، رمز عبور را درخواست کند و بعد از آن، با دستور access-class به این پورت می‌گوییم که در زمان telnet شدن، فقط ip address هایی را قبول کن که 10 access-list می‌گوید.
بعد از اتمام کار، اگر از طریق pc1 به روتر telnet کنید، جواب می‌گیرید، اما از طریق pc2 این امکان وجود ندارد.

Nat & Pat

همان‌طور که می‌دانید ip هایی که درون شبکه خود استفاده می‌کنیم، invalid می‌باشند و برای ارتباط با دنیای اینترنت باید تبدیل به یک ip valid شوند، ip valid توسط سازمان IANNA رجیستر و تعریف می‌شود و در دنیای اینترنت اعتبار دارد.
NAT(Network Address Translation) روشی برای ترجمه‌ی ip Invalid یا درون شبکه به ip valid یا اینترنت است. Nat شبکه را به دو صورت در نظر می‌گیرد.

- Inside Network : به شبکه‌هایی گفته می‌شود که از ip invalid استفاده می‌کنند، مانند شبکه‌ی داخلی یک اتاق. Inside Interface هم وجود دارد که به اینترفیسی گفته می‌شود که در شبکه‌ی Inside Network قرار داشته باشد.
- Outside Network : منظور آدرس‌های valid است که می‌توان به اینترنت اشاره کرد. Outside interface هم وجود دارد که اینترفیسی است که پورت آن داخل شبکه‌ی Outside قرار داشته باشد.

انواع Nat:

- Static Nat

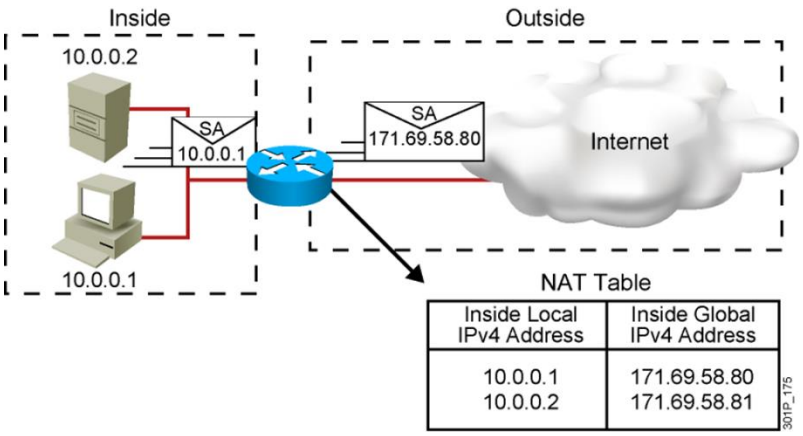
- Dynamic Nat
- Dynamic Nat With Overload

:Static Nat

این روش به صورت دستی انجام می‌شود، یعنی به صورت دستی به روتر می‌گوییم که ip invalid داخل شبکه را به ip Valid تبدیل کن.

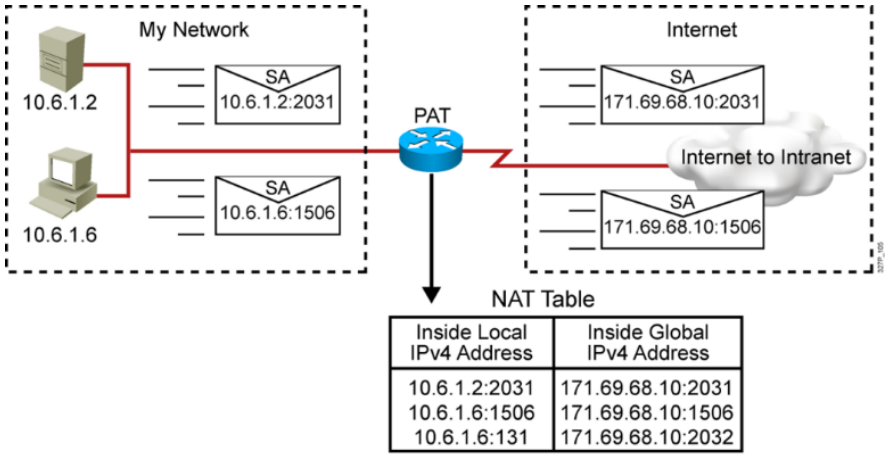
:Dynamic Nat

در این حالت، لیستی از ip invalid آماده و لیست دیگر از ip Valid آماده می‌شود و روتر به صورت خودکار این دو لیست را در موقع ترجمه در کنار هم قرار می‌دهد و تبدیل می‌کند.



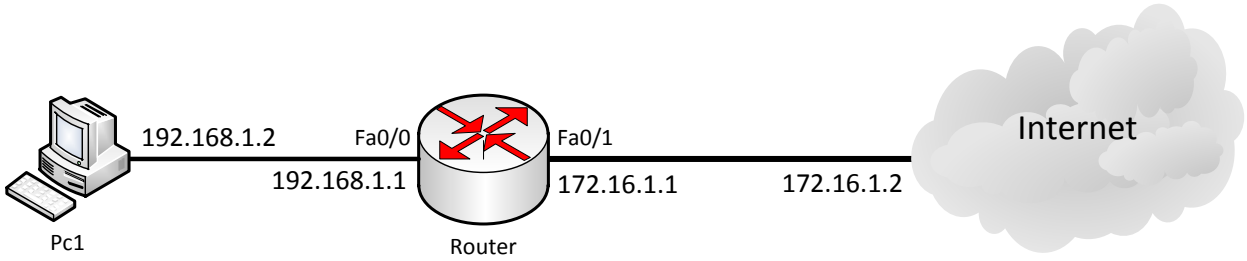
:Dynamic Nat With Overload(PAT)

این روش یکی از بهترین روش‌ها در حال حاضر است، به دلیل اینکه شما احتیاج به یک ip valid دارید و تمام ip invalid داخل شبکه‌ی شما از طریق یک ip valid ترجمه می‌شود، اما با استفاده از پورت، یعنی این‌که وقتی ip



invalid می‌خواهد به اینترنت راه پیدا کند از طریق همان ip valid و به همراه یک پورت به اینترنت راه پیدا می‌کند. در ادامه به صورت کامل با این موضوعات کار می‌کنیم.

مثالی از Static Nat:



در این مثال Pc1 می‌خواهد به اینترنت متصل شود و به خاطر invalid بودن ip آن باید ترجمه آدرس به ip valid انجام شود. وارد روتر شوید و دستورات زیر را وارد کنید:

Router(config)# **ip nat inside source static 192.168.1.2 172.16.1.2**

این دستور می‌گوید که Ip Nat را روی شبکه داخلی و روی مبدأ فعال کن و به صورت دستی (Static) ip به شماره 192.168.1.2 را به ip valid ، 172.16.1.2تبدیل کن.

بعد وارد اینترفیس Fa0/0 که به سمت شبکه داخلی است می‌شویم و دستور زیر را وارد می‌کنیم:

Router(config-if)#**ip nat inside**

با این دستور Nat روی این اینترفیس فعال می‌شود، در اینترفیس دیگرFa0/1 که به سمت شبکه Outside است دستور زیر را وارد می‌کنیم:

Router(config-if)#**ip nat Outside**

بعد از اتمام کار ip مربوط به pc1 برای رفتن به شبکه اینترنت تبدیل می‌شود، می‌توانید با دستور زیر Nat فعال‌شده روی این روتر را مشاهده کنید:

Router#**show ip nat translations**

Pro	Inside global	Inside local	Outside local	Outside global
---	172.16.1.2	192.168.1.2	---	---

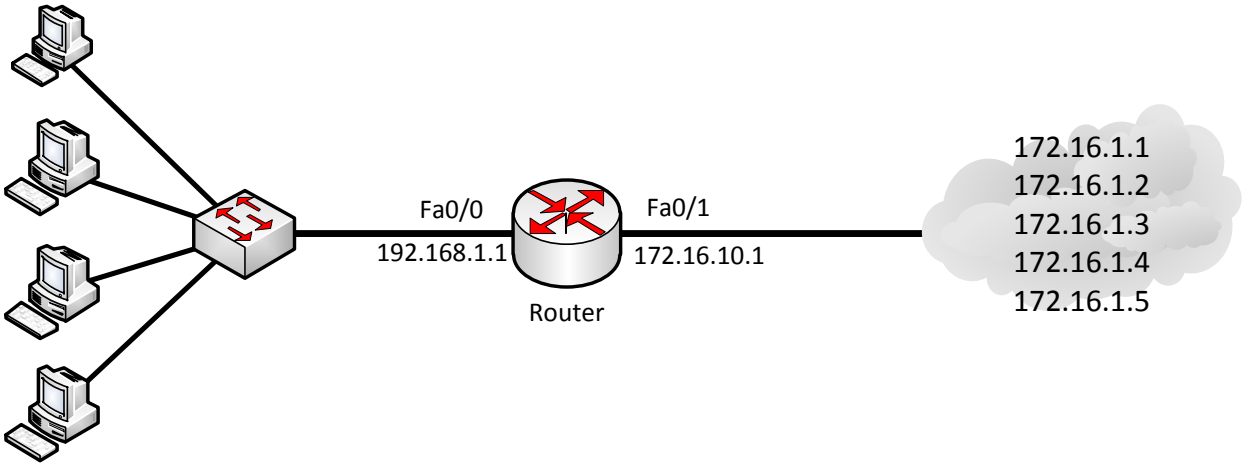
با دستور زیر اطلاعات کامل از Nat روی روتر به دست خواهید آورد:

Router# **show ip nat statistics**

Total translations: 1 (1 static, 0 dynamic, 0 extended)
Outside Interfaces: FastEthernet0/1
Inside Interfaces: FastEthernet0/0
Hits: 0 Misses: 14
Expired translations: 0
Dynamic mappings:

مثالی از dynamic Nat:

به‌دقت به این مثال توجه کنید تا به خوبی به مطالب آن واقف شوید.



برای استفاده از Dynamic Nat، اول از همه دو چیز تعریف می‌کنیم، یکی ip pool که مجموعه ip های Valid که در این مثال 5 تا است را در خود نگه می‌دارد و بعد باید یک access List برای ip های invalid داخل شبکه خود تعریف کنیم و در آخر این دو را باهم ترکیب کنیم.

وارد روتر شوید و دستور زیر را وارد کنید:

Start IP End IP

Router(config)#**ip nat pool oip 172.16.1.1 172.16.1.5 netmask 0.0.0.248**

این دستور را به این صورت بخوانید: ip nat pool ایجاد کن با نام OIP که می‌توانید هر نام دیگری هم قرار دهید و بعد از آن باید ip های Vlaid را وارد کنید که در قسمت اول، شروع ip و در قسمت بعدی، پایان ip را مشخص کنید، مانند دستور بالا و در قسمت آخر هم Netmask آن را وارد کنید که همان Wild Card mask است. تا این قسمت، ip nat pool را تعریف کردیم و برای ادامه باید access-list را برای شبکه‌ی داخلی تعریف کنیم:

Router(config)#**access-list 10 permit 192.168.1.0 0.0.0.255**

Ip های داخلی شبکه را در یک access-list قرار می‌دهیم و اجازه‌ی دسترسی به شبکه را به آن‌ها داده‌ایم.

حالا نوبت این است که این دو را به هم ارتباط دهیم:

Router(config)#**ip nat inside source list 10 pool oip**

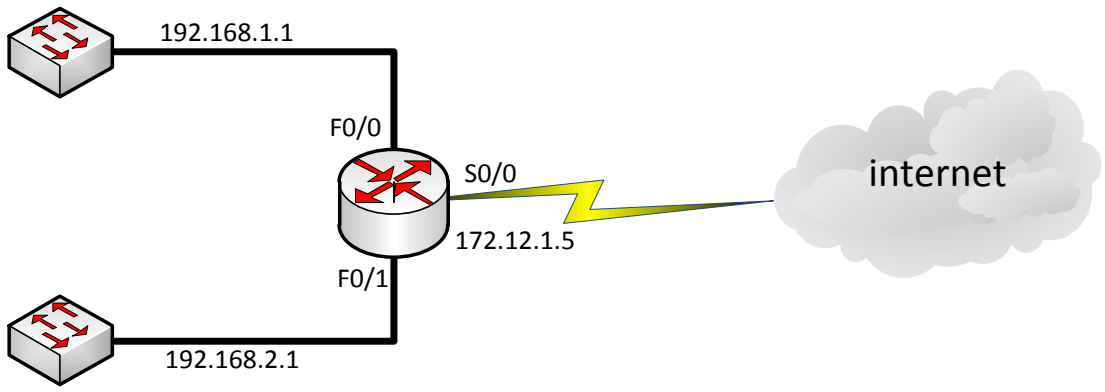
با این دستور accss-list 10 با pool oip ارتباط برقرار می‌کند و در زمان خروج ip های تعریف‌شده در access-list به ip تعریف‌شده در pool oip تبدیل می‌شوند.

بعد از این کار وارد اینترفیس می‌شویم و دستورات زیر را وارد می‌کنیم:

Router(config)**#int f0/0**
Router(config-if)**#ip nat inside**
Router(config-if)**#int f0/1**
Router(config-if)**#ip nat outside**

مثالی از PAT(Port Address Translation):

در این قسمت نیاز به یک IP Valid است و از طریق پورت، IP ها را از هم جدا می‌کند. به شکل زیر توجه کنید:



در این شکل، دو شبکه‌ی داخلی داریم که باید برای هرکدام یک access-list بنویسیم.

access-list 1 permit 192.168.1.0 0.0.0.255
access-list 1 permit 192.168.2.0 0.0.0.255

با دستور بالا، access-list شماره‌ی یک ایجاد شده است که ip های invalid شبکه‌های داخلی را در خود قرار داده است.

وارد روتر می‌شویم و دستور زیر را وارد می‌کنیم:

ip nat inside source list 1 interface Serial0 overload

با تعریف دستور بالا، access-list با شماره‌ی 1 که ایجاد کرده‌ایم، انتخاب و روی اینترفیس Serial0 که به طرف شبکه‌ی خارجی است، فعال می‌کنیم و در آخر دستور از overload استفاده می‌کنیم که در زمان خروج، ip را به همراه یک پورت به بیرون ارسال می‌کند.

بعد از آن وارد اینترفیس‌های روتر می‌شویم و nat را فعال می‌کنیم:

ip nat inside

نحوه‌ی پاک کردن آدرس‌های موجود در جدول Nat:

Router#**clear ip nat translation ***

با این دستور، کل آدرس‌های موجود در جدول Nat حذف خواهد شد.

Router#**clear ip nat translations inside a.b.c.d outside e.f.g.h**

با این دستور یکی از رکوردهای ایجادشده از جدول Nat حذف خواهد شد.

سرویس DHCP:

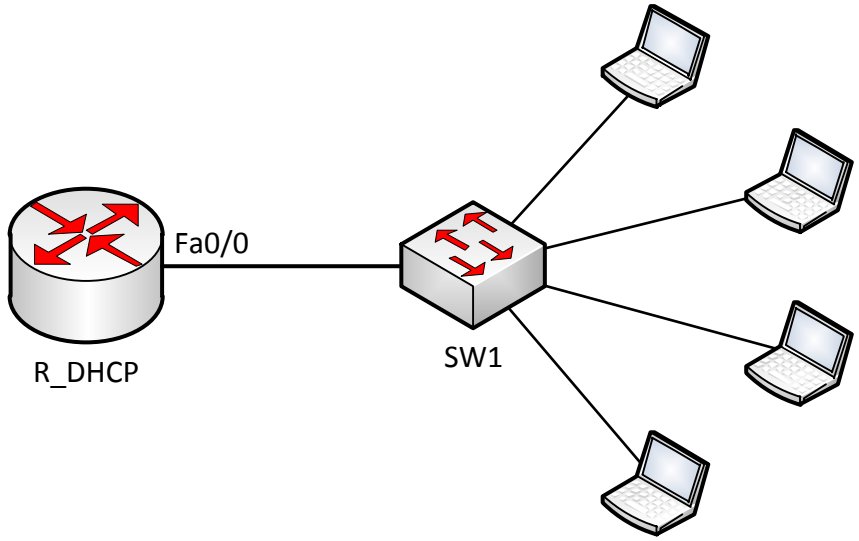
سرویس Dynamic Host Configuration Protocol یا DHCP به شما اجازه می‌دهد تا به صورت خودکار به کلاینت‌های خود ip دهید. سرویس بسیار پرکاربرد که با نحوه‌ی راه‌اندازی آن آشنا خواهیم شد.

یک سرور که نقش DHCP را بازی می‌کند از اجزای زیر تشکیل شده است:

- IP address
- Subnet mask
- Domain name
- Default gateway (routers)
- DNS
- WINS information

همه‌ی آن‌ها را می‌توانید بر روی یک DHCP Server فعال کنید تا به کلاینت‌ها داده شود، البته گزینه‌های دیگری هم وجود دارد که در دوره‌ی ccna بررسی نمی‌شود.

مثال 7:



در این مثال می‌خواهیم روی روتر R_DHCP، سرویس DHCP را راه‌اندازی کنیم، بعد از راه‌اندازی این سرویس، کلاینت‌ها اگر درخواست آدرس دهند، IP ها و اطلاعات را از سرور دریافت می‌کنند.

وارد پورت Fa0/0 شوید و آدرس زیر را در آن وارد کنید:

R_DHCP(config-if)**#ip address 192.168.1.1 255.255.255.0**

بعد، سرویس Dhcp را راه‌اندازی می‌کنیم.

R_DHCP(config)**#ip dhcp pool r_dhcp**

با این دستور، DHCP Pool با نام r_dhcp ساخته می‌شود و وارد آن می‌شویم.

R_DHCP (dhcp-config)**#network 192.168.1.0 255.255.255.0**

تعریف رنج ip برای اختصاص دادن به کلاینت‌ها.

R_DHCP(dhcp-config)**#default-router 192.168.1.1**

به کلاینت‌ها می‌گوییم که Default gateway مورد نظر، این روتر است.

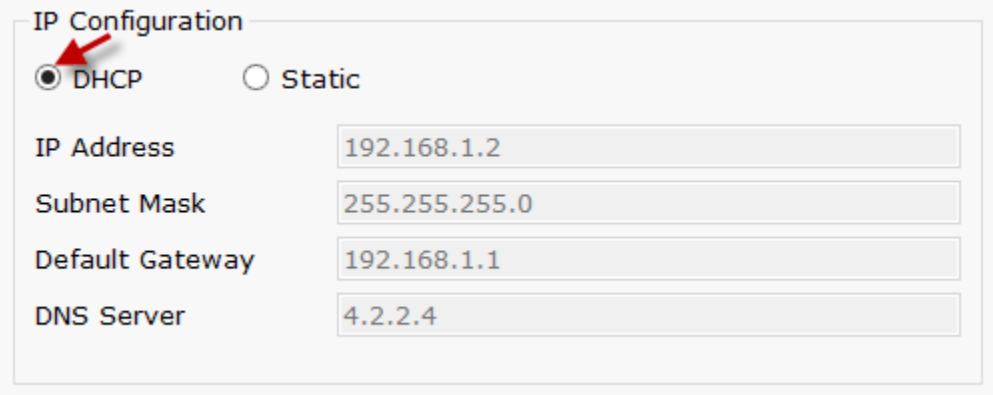
R_DHCP(dhcp-config)**#dns-server 4.2.2.4**

با این دستور، DNS Server را برای کلاینت‌ها تعریف می‌کنیم.

R_DHCP(dhcp-config)**#lease 0 1 05**

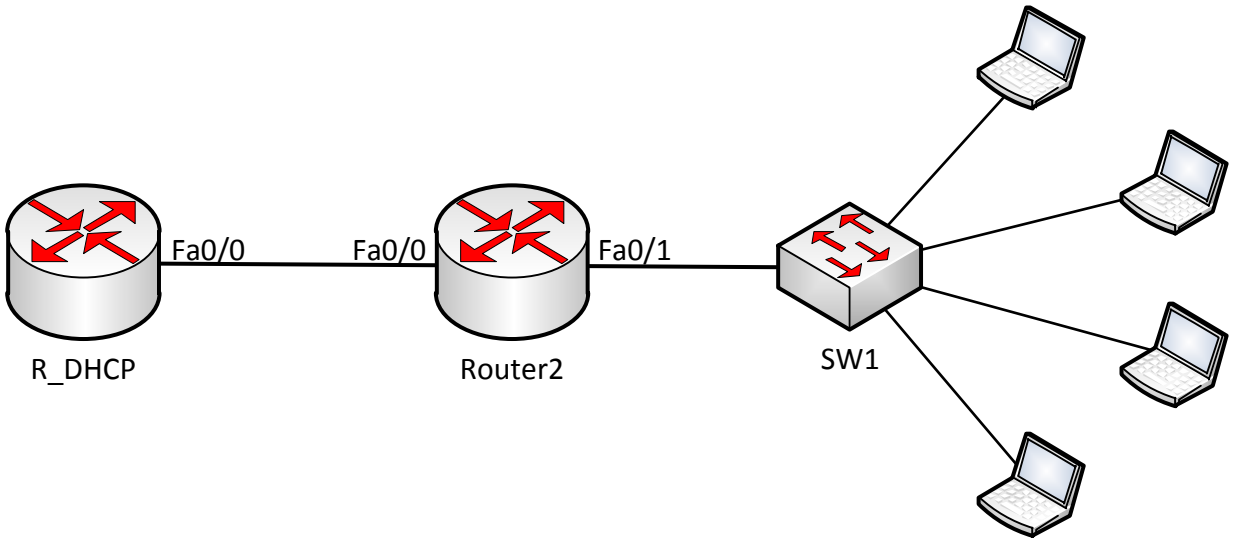
این دستور، مقدار زمانی است که به یک کلاینت داده می‌شود و این کلاینت باید در این زمان مشخص با ارسال پکت‌هایی حضور خود را اعلام کند. اگر بعد از پایان این زمان، موجودیت خود را اعلام نکرد، IP اختصاص داده به این کلاینت پس گرفته خواهد شد.

بعد از راه‌اندازی سرویس DHCP باید به کلاینت‌ها بگوییم که ip address را از طریق DHCP به دست بیاورند. در برنامه‌ی packet tracer، وارد pc مورد نظر می‌شویم و از تب Desktop، گزینه‌ی ip Configuration را انتخاب می‌کنیم.



همان‌طور که مشاهده می‌کنید، بعد از انتخاب گزینه‌ی DHCP، به صورت خودکار اطلاعات از dhcp سرور دریافت کرد.

نکته: شاید شما شبکه‌ای داشته باشید که از دو روتر تشکیل شده است و می‌خواهید روی یکی از آن‌ها سرویس DHCP را راه‌اندازی کنید، مانند شکل زیر، اگر روی روتر R_DHCP، این سرویس را راه‌اندازی کنید کلاینت‌ها نمی‌توانند اطلاعات را از این سرور بگیرند، به خاطر این‌که Router 2 در سر راه قرار دارد و سرویس DHCP برای انجام کار خود از طریق Broadcast، اطلاعات خود را ارسال می‌کند. Router2 جلوی Broadcast را خواهد گرفت و این سرویس کارایی خود را از دست می‌دهد، برای حل این مشکل باید دستوری را در Router 2 اجرا کنید:



وارد روتر Router2 شوید و در مد Global دستور زیر را وارد کنید:

R_DHCP(config-if)#**ip helper-address 192.168.1.1**

با این دستور، سرویس dhcp به کار خود ادامه می‌دهد و کلاینت‌ها می‌توانند از این سرور اطلاعات را دریافت کنند.

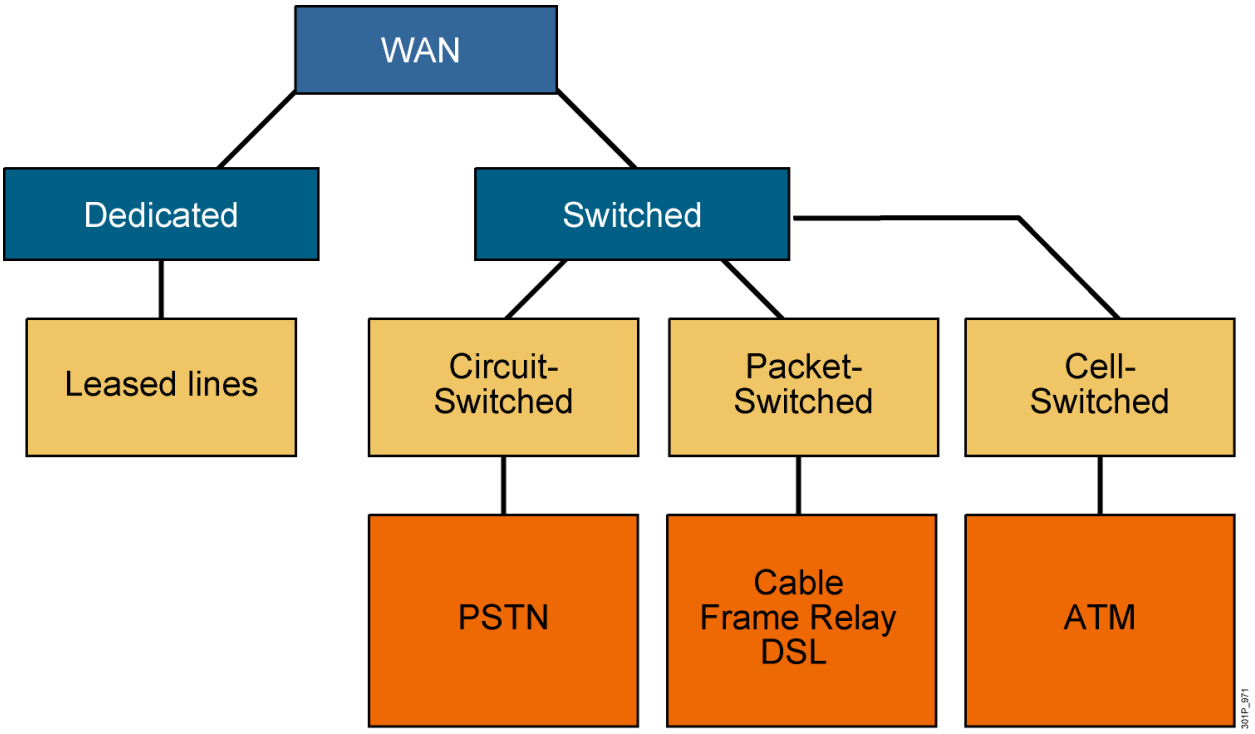
Wan Connection

شبکه‌ی گسترده (WAN) یک شبکه‌ی رایانه‌ای است که ناحیه‌ی جغرافیایی نسبتاً وسیعی را پوشش می‌دهد (برای نمونه از یک کشور به کشوری دیگر یا از یک قاره به قاره‌ای دیگر). این شبکه‌ها معمولاً از امکانات انتقال خدمات دهندگان عمومی، مانند شرکت‌های مخابرات استفاده می‌کند. به عبارت کمتر رسمی، این شبکه‌ها از مسیریاب‌ها و لینک‌های ارتباطی عمومی استفاده می‌کنند. شبکه‌های گسترده از نظر محدوده‌ی تحت پوشش با شبکه‌های شخصی (به انگلیسی: PAN)، شبکه‌های محلی (به انگلیسی: LAN)، شبکه‌های دانشگاهی (به انگلیسی: CAN) (شبکه‌هایی که چند ساختمان یک سازمان را پوشش می‌دهند) یا شبکه‌های کلان‌شهری (به انگلیسی: MAN) که

معمولاً محدود به یک اتاق، یک ساختمان، فضای چند دانشکده یا یک شهر می‌باشند قابل مقایسه هستند. بزرگ‌ترین و شناخته‌شده‌ترین مثال از یک شبکه‌ی گسترده، شبکه‌ی اینترنت است.

سرویس‌هایی که با آن‌ها می‌توانیم شبکه‌های خود را در نقاط مختلف به هم متصل کنیم و توسط مخابرات ارائه می‌شود، به شرح زیر است:

- خطوط استیجاری (Leased Line)
- راه گزینی مداری (Circuit Switching)
- راه گزینی بسته (Packet Switching)
- راه گزینی سلول (Cell Switching)
- راه گزینی برچسب (Label Switching)



خطوط استیجاری (Leased Line):

این خطوط که توسط مخابرات اجاره داده می‌شود، یک خطوط امن (Secure) محسوب می‌شود و مانند خط تلفن پایدار و ثابت است و پهنای باند آن حدود 45 مگابایت است. برای استفاده از این خطوط باید شرایط زیر برقرار باشد:

•باید بدانید که مخابرات قابلیت اتصال خطوط استیجاری را در منطقه‌ی شما دارد.

•باید امکانات سخت‌افزاری و نرم‌افزاری فراهم شود.

•امنیت شبکه باید بالا باشد، به دلیل نفوذپذیری زیاد به شبکه.

راه گزینی مداری (Circuit Switching):

در این روش که ازخطوط تلفن و یا ISDN استفاده می‌کنند و دو مدار منطقی در هر دو طرف ایجاد و ارتباط برقرار می‌شود، اما مشکلی که این روش دارد، این است که در صورتی‌که هیچ‌گونه اطلاعاتی رد و بدل نشود باز هم خطوط اشغال است تا زمانی که هر دو طرف ارتباط را قطع کنند، مانند تلفن‌های خانگی.

راه گزینی بسته (Packet Switching):

این سرویس، مانند سرویس راه گزینی مداری نیست که در هر دو طرف از مدار منطقی استفاده کنند، بلکه این سرویس اطلاعات دریافتی را به بسته‌های کوچک‌تر تقسیم می‌کند و به همراه اطلاعات دیگر به شبکه‌ی مورد نظر ارسال می‌کند، شبکه‌های Frame-relay و X.25 از این نوع می‌باشند.

راه گزینی سلول (Cell Switching):

سلولی است شامل مسیر مورد نظر در شبکه که توسط سوئیچ این مسیر انتخاب می‌شود. این شبکه اغلب برای شبکه‌های با سرعت بالا، مانند ستون فقرات استفاده می‌شود؛ پهنای باند آن می‌تواند بین 56 کیلوبایت تا چند گیگابایت باشد. این شبکه بیشتر برای صوت و تصویر استفاده می‌شود.

راه گزینی برچسب (Label Switching):

در این روش که سریع‌ترین روش موجود است بر روی بسته‌ها برچسب‌گذاری و انتقال داده می‌شود. این روش در لایه‌ی 2، یعنی لایه‌ی پیوند داده‌ها کار می‌کند. استفاده از برچسب‌گذاری و Multiport فن‌آوری‌های جدید در این زمینه هستند.

بررسی پروتکل‌های مربوط به Leased Line یا خطوط استیجاری:

پروتکل‌های مربوط به خطوط Leased به دو دسته تقسیم می‌شوند:

- **PPP**
- **HDLC**

بررسی پروتکل PPP:

این پروتکل که در یک ارتباط Point To Point کاربرد دارد دارای دو زیر لایه است:

Network Control Protocol یا NCP:

این پروتکل وظیفه‌ی بسته‌بندی یا کپسوله کردن پروتکل‌های لایه‌ی Network، مانند IP و IPX را دارد.

Link Control Protocol یا LCP:

وظیفه‌ی این پروتکل، کنترل برقراری ارتباط بین دو نقطه است. این زیر لایه دارای ویژگی‌های زیر است.

Authentication:

در این قسمت، مجوز برقراری ارتباط بین دو نقطه در ارتباط Point to Point بررسی می‌شود. برای تأیید اعتبار از دو روش استفاده می‌کند:

- PAP
- CHAP

MultiLink:

با این ویژگی، اینترفیسی که پروتکل PPP روی آن اجرا شده است، می‌تواند پکت‌ها را روی خط‌های مختلف Balance کند.

Error Detection :

روشی برای کشف خطا و جلوگیری از Loop است.

Comperession:

این روش که برای افزایش ظرفیت پروتکل ppp استفاده می‌شود، برای فشرده‌سازی و خارج کردن از حالت فشرده اطلاعات است.

برای این‌که یک ppp با خط دیگر ppp اتصال برقرار کند، نیازمند 3 مرحله است:

Link Establishment:

زمانی که بر روی یک اینترفیس، پروتکل PPP اجرا شده باشد، این پروتکل برای برقراری با اینترفیس مقابل خود یک درخواست ارسال می‌کند که این درخواست دربرگیرنده‌ی **Authentication**، **Comperession** و ... است.

Authentication:

در این مرحله، دو متد برای برقراری ارتباط امنیتی استفاده می‌شوند:

PAP (Password Autentication Protocol**)**:

این متد از نظر امنیتی، زیاد در سطح بالایی قرار ندارد، آن‌هم به خاطر Clear Text بودن آن است. این متد زمانی استفاده می‌شود که نیاز به امنیت بین دو خط PPP داشته باشیم.

CHAP(Challenge Handshake Authentication Protocol**)**:

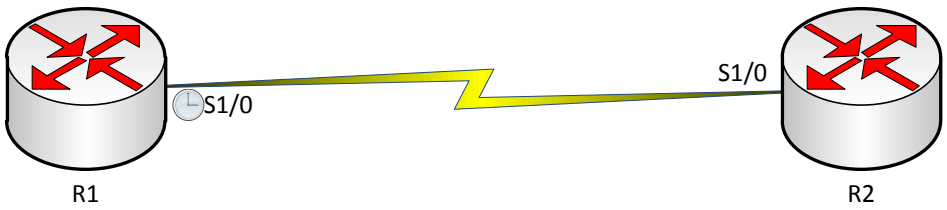
این متد بسیار پیچیده و با امنیت بسیار بالا نسبت به رفیق قبلی خود، یعنی PAP عمل می‌کند. این متد در سه مرحله کار خود را انجام می‌دهد:

در مرحله‌ی اول، روتری درخواست‌کننده‌ی ارتباط یک Challenge Message به روتر مقابل خود ارسال می‌کند، روتر مقابل هم با دریافت پیام روی آن عملیات MD5 را انجام می‌دهد و با یک Response Message به روتر مقابل ارسال می‌کند. در این مرحله، روتر ارسال‌کننده، اطلاعات اولیه‌ی پسورد خود را توسط MD5 تبدیل به مقدار مورد نظر می‌کند و این مقدار را با مقدار دریافتی از روتر روبرو مقایسه می‌کند، در صورت تأیید آن، ارتباط برقرار خواهد شد.

Network Layer Protocol:

این مرحله، بعد از Authentication اجرا شده و پروتکل‌های لایه‌ی Network برای ارتباط مشخص می‌شوند.

در مثال زیر می‌خواهیم روش راه‌اندازی پروتکل ppp را باهم بررسی کنیم، مانند شکل زیر، دو روتر به صفحه اضافه کنید و از طریق کابل سریال آن‌ها را به هم متصل کنید:



وارد روتر 1 شوید و دستورات زیر را وارد کنید:

```
Router(config)# hostname R1
R1(config)# Interface S1/0
R1(config-if)#  clock rate  64000
R1(config-if)#  ip add 192.168.1.1 255.255.255.0
R1(config-if)#  Encapsulation ppp
```

همان‌طور که مشاهده می‌کنید از **clock rate** استفاده کردیم، به دلیل اینکه این سر کابل سریال DCE است و بعدازآن Ip address را وارد و در آخر از پروتکل ppp برای ارتباط استفاده کردیم.

وارد روتر 2 شوید و دستورات زیر را وارد کنید:

```
Router(config)# hostname R2
R2(config)# Interface S1/0
R2(config-if)#  ip add 192.168.1.2 255.255.255.0
```

R2(config-if)# **Encapsulation ppp**

در این روتر ip address را وارد می‌کنیم و بعدازآن پروتکل PPP را فعال می‌کنیم.

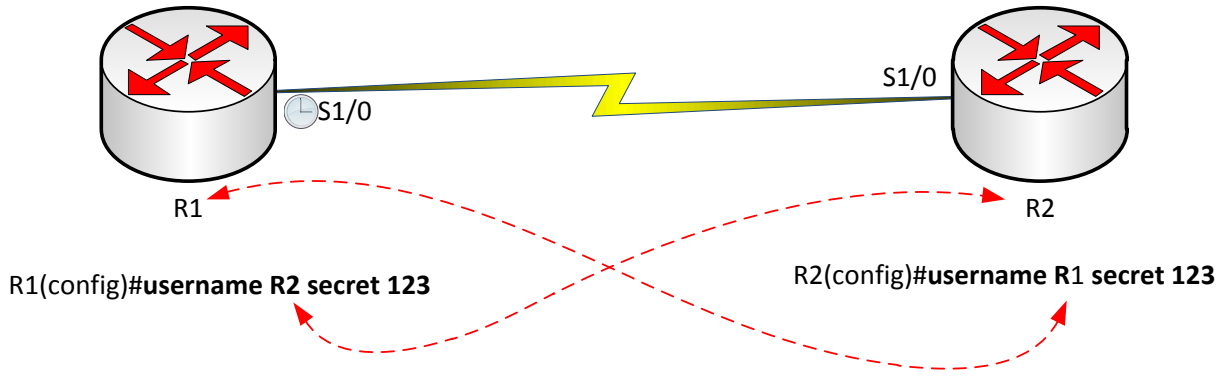
بعد از اتمام این کار دو روتر می‌توانند باهم ارتباط برقرار کنند، اما این ارتباط امن نیست؛ برای امن کردن این ارتباط باید کارهای زیر را انجام دهید.

وارد مد Global شوید و دستور زیر را وارد کنید:

R1(config)# **username R2 secret 123**

با این دستور، Username و Password را برای هر روتر وارد می‌کنیم. به شکل زیر توجه کنید در موقع واردکردن username حتماً نام روتر مقابل را وارد کنید، مثلاً برای روتر R1 باید username آن را R2 وارد و برای روتر R2 هم R1 وارد کنید و در انتها، Password هم باید برای هر دو روتر یکی باشد.

R2(config)#username R1 secret 123



بعدازآن باید Usrname و Password را روی پروتکل PPP فعال کنیم که وارد اینترفیس سریال در هر روتر می‌شویم و دستور زیر را وارد می‌کنیم:

R1(config-if)#ppp authentication chap
R2(config-if)#ppp authentication chap

با دستور debug ppp packet در مد privileged می‌توانید بسته‌های ارسالی بین دو روتر را مشاهده کنید.

با دستور debug ppp authentication می‌توانید نحوه‌ی برقراری و ایجاد نشست بین دو پروتکل را مشاهده کنید.

بررسی پروتکل HDLC:

High-Level Data Link Control یک پروتکل لایه‌ی دومی است که برای بسته‌بندی اطلاعات و انتقال آن توسط کابل سریال استفاده می‌شود. این پروتکل دارای دو نوع است:

Standard HDLC:

این نوع، توانایی بسته‌بندی کردن یک پروتکل لایه‌ی سوم را دارد و در همه‌ی روترها می‌توان از آن استفاده کرد.

Cisco HDLC:

این فرمت که مختص سیسکو است، فقط در روترهای سیسکو کار می‌کند و نمی‌تواند در یک روتر با برند دیگر استفاده کرد. این پروتکل توانایی بسته‌بندی کردن چندین پروتکل لایه‌ی سومی را برای انتقال روی یک خط سریال را دارد.

برای فعال کردن این پروتکل، وارد اینترفیس سریال مورد نظر می‌شویم و از دستور زیر استفاده می‌کنیم:

R1(config-if)#**encapsulation hdlc**

این نکته را همیشه به یاد داشته باشید که این پروتکل فقط روی تجهیزات سیسکو کارایی دارد و اگر در یک ارتباط دو سر روتر از روترهای شرکت سیسکو نباشند، نمی‌توان از آن استفاده کرد.

همه‌چیز درباره‌ی Frame Relay:

این پروتکل از دسته پروتکل‌های Packet Switching است و پهنای باند آن عموماً 56 کیلوبایت تا 45 مگابایت است. هر مسیر که در fram relay ایجاد می‌شود، به عنوان یک VC (Virtual Circuit) در نظر گرفته می‌شود، اگر این مسیر دائمی باشد به عنوان PVC (Permanent Virtual Circuit) گفته می‌شود و اگر موقتی باشد به آن SVC (Switched Virtual Circuit) است که اصولاً از PVC برای ارتباط بین دو مسیر استفاده می‌کنند.

در شبکه‌ی Frame Relay دستگاه‌های شبکه به دو دسته تقسیم می‌شوند:

1- DCE که در سمت سرویس‌دهنده و یا مخابرات است که کار سوئیچینگ و Clocking را انجام می‌دهند.

2- DTE که در سمت سرویس‌گیرنده یا مشتری وجود دارد و ارتباط با شبکه WAN را برقرار می‌کند.

مفهوم DLCI:

هر VC توسط یک عدد که به آن عدد DLCI(Data-Link Connection Indentifier) از دیگر VC ها متمایز می‌شود. از طریق این عدد، ip address ها را هدایت و کنترل می‌کنیم، توجه داشته باشید این عدد 10 بیتی است.

Frame Relay یک شبکه‌ی Broadcast نیست، بلکه یک شبکه‌ی NBMA (Non-broadcast Multi-access) است و همه‌ی اعضای شرکت‌کننده در یک ارتباط Frame Relay، باید یک ip در یک رنج داشته باشند.

LMI(Local management Interface):

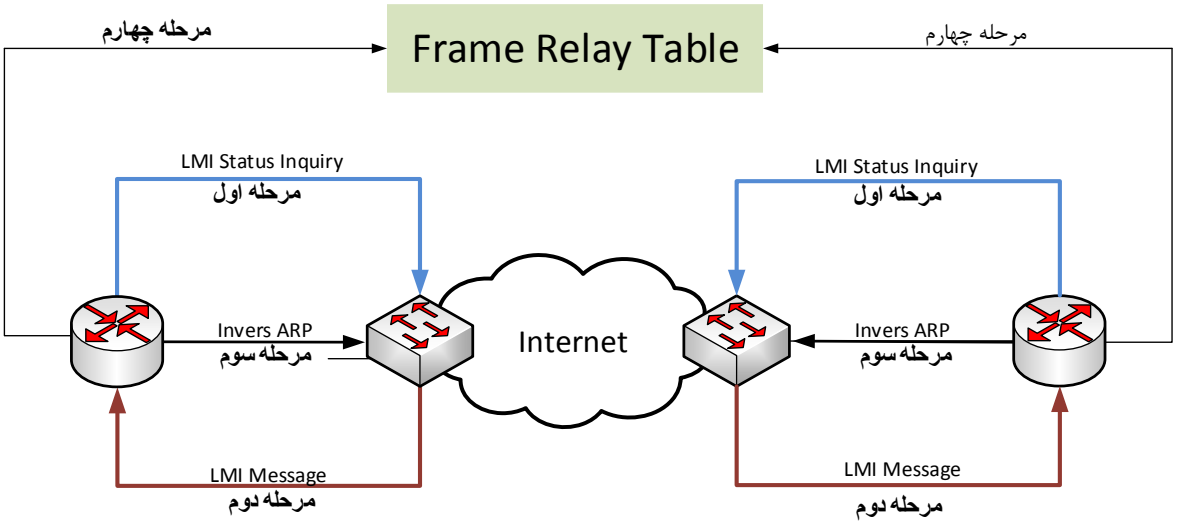
استانداردی است که بر روی ارتباط بین DCE و DTE نظارت و کنترل می‌کند که بر سه نوع است.

- Cisco
- Ansi
- Q.933

در ارتباط Fram Relay باید استاندارد به‌کاربرده شده یکی باشد.

Inverse Arp: این عبارت عدد DLCI مربوط به یک Interface را در به صورت خودکار در فریم Frame Relay قرار می‌دهد.

چگونه ارتباط از طریق Fram relay انجام می‌شود؟، به شکل زیر دقت کنید؛ هر مرحله از آن را باهم بررسی می‌کنیم:



برای ایجاد ارتباط Frame Relay باید روتر به یک سوئیچ Frame Relay متصل شود. به این سوئیچ‌ها CSU/DSU می‌گویند. بعد از ارتباط، مرحله‌های بالا را باهم مورد بررسی قرار می‌دهیم.

مرحله‌ی اول:

روتر یک پیام LMI Status Inauriy به سوئیچ FR (FR مخفف Frame Relay است) می‌فرستد و درخواست ایجاد یک مدار مجازی VC را می‌کند.

مرحله‌ی دوم:

در این مرحله سوئیچ FR یک LMI Message را برای روتر ارسال می‌کند که در این پیام، شماره‌ی DLCI مربوط به همان شبکه‌ای که روتر در آن قرار دارد، به روتر داده می‌شود که از طریق این شماره، می‌توان در مدار مجازی VC با روتر شبکه‌ی دیگر ارتباط برقرار کرد.

نکته: LMI Message هر 10 ثانیه یک‌بار بین سوئیچ و روتر انجام می‌شود.

مرحله‌ی سوم:

در این مرحله روتر بعد از دریافت DLCI در مرحله‌ی قبل، یکInvers ARP را به روترهای مقابل خود ارسال می‌کند و خود را به آن‌ها معرفی می‌کند.

نکته: روتر هر 60 ثانیه یک‌بار پیام Invers ARP را برای همه‌ی DLCI های خود ارسال می‌کند.

مرحله‌ی چهارم:

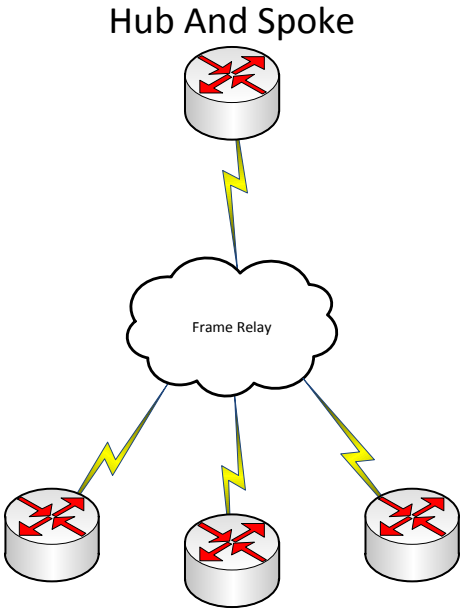
روترها بعد از دریافت پیام Invers ARP که حاوی اطلاعات DLCI و IP Address است، آن‌ها را در جدولی به نام Frame Relay Map قرار می‌دهند.

کار با Frame Relay:

شبکه‌ی Fram Relay از نظر هندسی. توپولوژی به سه دسته تقسیم می‌شوند:

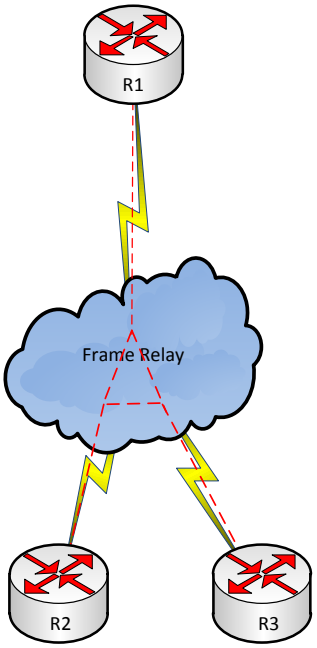
Hub And Spoke:

در این توپولوژی، یک روتر می‌تواند از طریق پورت‌های Subinterface خود به روترهای دیگر متصل شود، مانند شکل زیر:



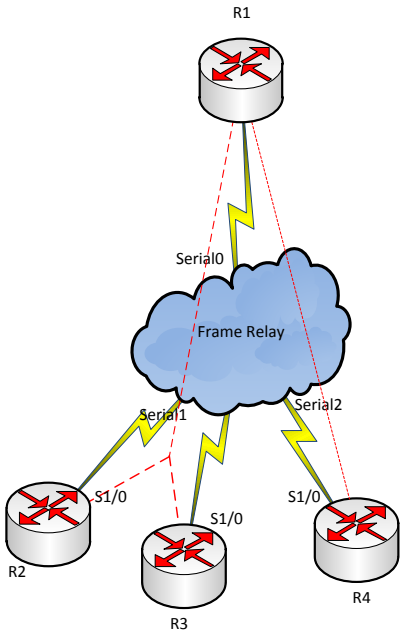
توپولوژی Full Mesh:

در این توپولوژی هر روتر دارای یک ارتباط با روترهای دیگر است یا دارای یک مدار مجازی VC با روترهای دیگر است.



توپولوژی MeshPartial:

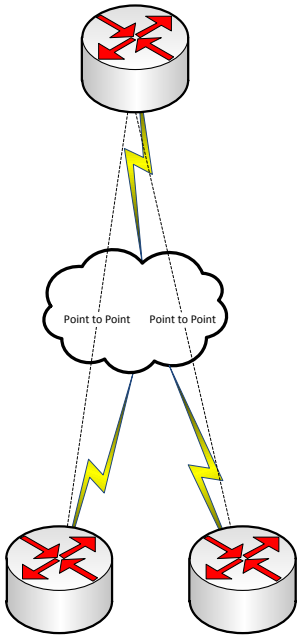
در این توپولوژی یک روتر به همه‌ی روترهای دیگر در شبکه Frame Relay متصل است.



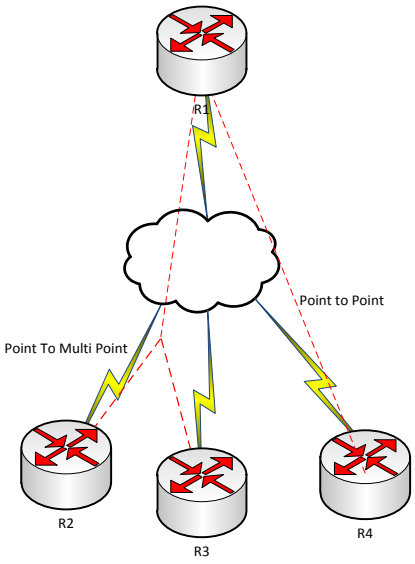
پیکربندی اینترفیس مجازی یا SubInterface به دو صورت انجام می‌گیرد:

- Point To Point
- Point To Multi Point

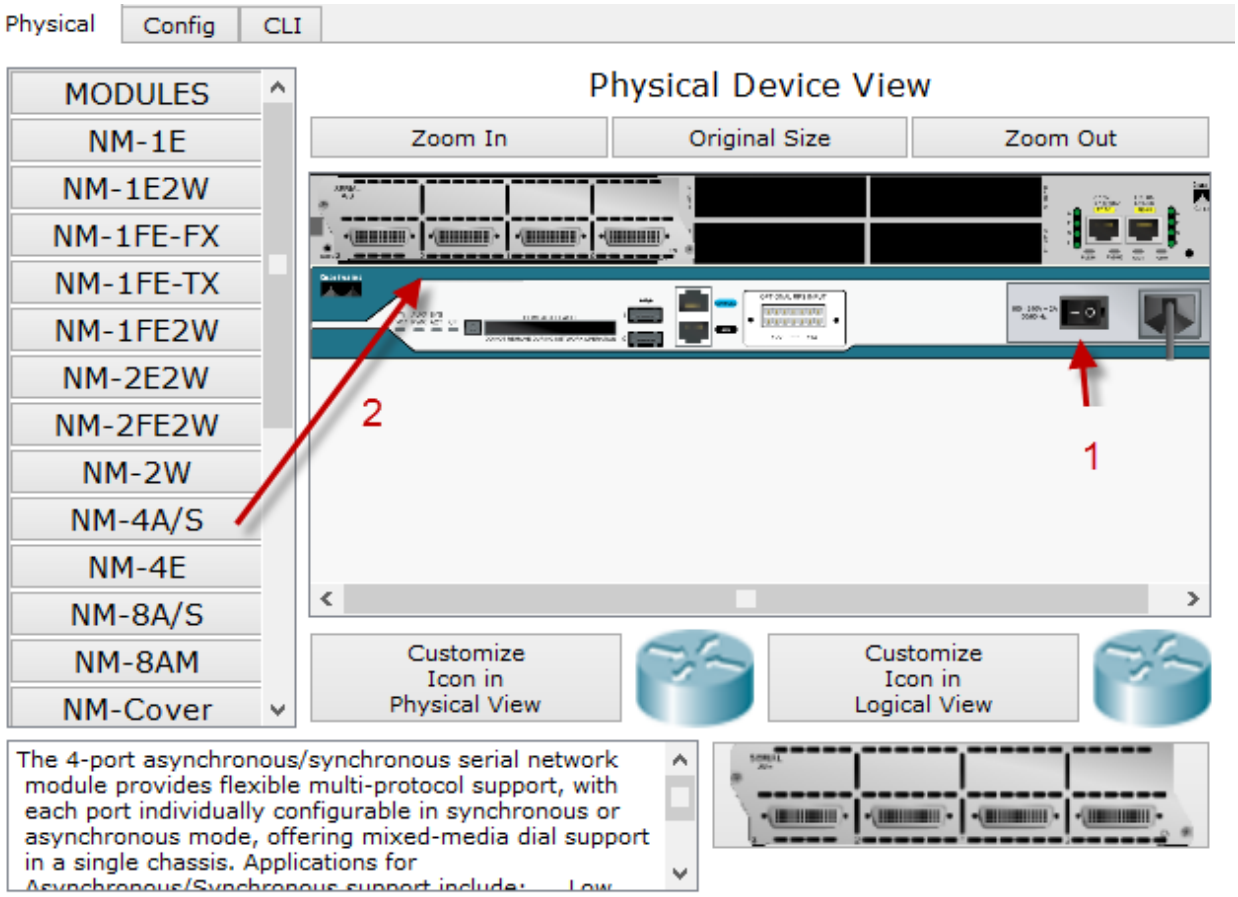
در مد Point To Point، یک روتر با روتر دیگر به صورت مستقیم در ارتباط است. هر روتر با روتر مقابل خود در یک رنج یا Subnet قرار دارند.



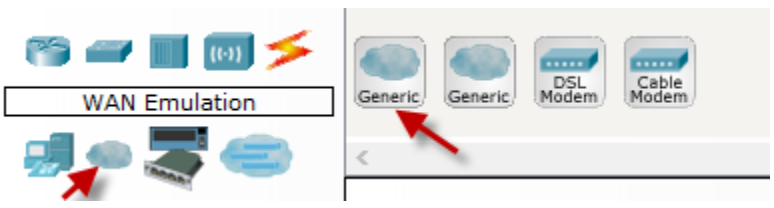
در مد Point To Multipoint، یک روتر می‌تواند با چند روتر دیگر در یک رنج قرار داشته باشد و باهم در ارتباط باشند. در شکل زیر R1 با روترهای 2 و 3 در یک رنج قرار دارند و به صورت **Point To Multi Point** در ارتباط هستند و روتر 1 با روتر 4 به صورت point to point می‌باشند.



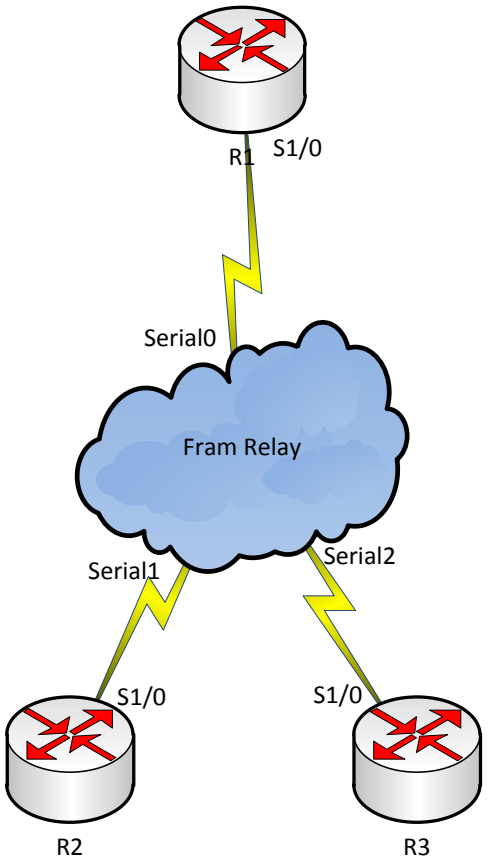
در این مثال می‌خواهیم کار با Fram relay را به صورت عملی بررسی کنیم. برنامه‌ی packet tracer را باز می‌کنیم و سه روتر 2811 به لیست اضافه و به هرکدام از آن‌ها یک ماژول سریال اضافه می‌کنیم، به صورت زیر:



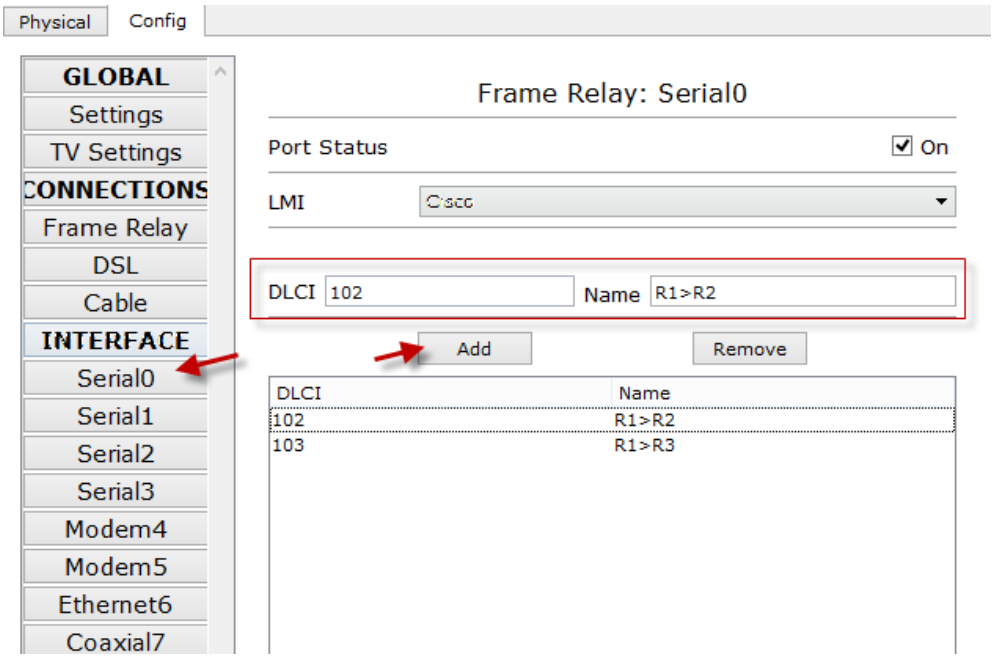
مانند شکل بر روی روتر کلیک و در تب Physical اول روتر را طبق شماره‌ی یک خاموش می‌کنیم و بعد از لیست سمت چپ ماژول NM-4A/S را می‌کشیم و در جای مشخص‌شده در شماره‌ی 2 قرار می‌دهیم و بعد، روتر را روشن می‌کنیم. در بقیه‌ی روترها هم این کار را انجام می‌دهیم، بعد باید سوئیچ Frame Relay را به لیست اضافه کنیم، برای این کار، طبق شکل زیر بر روی Wan Emulation کلیک و گزینه‌ی Generic را به صفحه اضافه می‌کنیم.



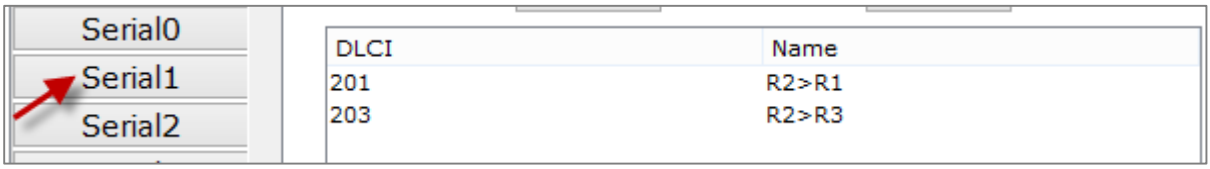
مانند شکل زیر آن‌ها را از طریق کابل سریال به هم متصل کنید:



بعد از این کار وارد Generic می‌شویم و بر روی پورت‌های سریال که در شکل به روترها متصل کردیم، کلیک می‌کنیم:

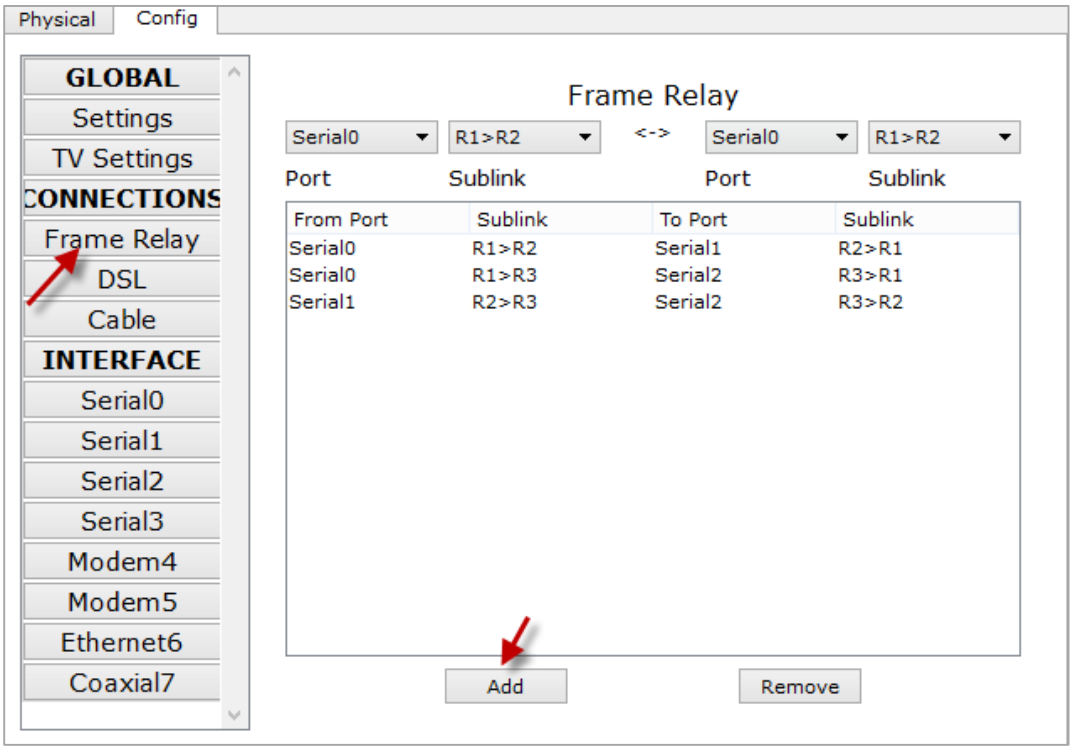


مانند شکل صفحه‌ی قبل بر روی سریال شماره‌ی صفر کلیک کردیم، اگر در شکل توجه کنیم سریال صفر به روتر R1 متصل است و باید DLCI یا مدار منطقی بین روترها را ایجاد کنیم. در DLCI شماره‌ی 102 را وارد می‌کنیم که عدد ارتباطی بین روتر 1 و 2 است و در قسمت Name می‌توانیم مشخص کنیم این عدد ارتباط بین کدام روتر است، مثلاً R1>R2 برای روترهای R1 و R3 هم DlCI را مشخص می‌کنیم، می‌نویسیم 103 که عددی بین روتر 1 و 3 است. در شماره‌ی سریال 1 که به روتر 2 متصل است، اعداد زیر را وارد می‌کنیم:



در پورت سریال شماره‌ی 3 اطلاعات زیر را وارد می‌کنیم:

بعد از این کار بر روی قسمت FRam Relay کلیک می‌کنیم و عملیات زیر را انجام می‌دهیم:



مانند شکل بر روی Fram Relay کلیک می‌کنیم، شما باید ارتباط بین روترها را مشخص کنید، مثلاً کابل سریال صفر با نام R1> R2 به کابل سریال 1 با نام R1 < R2 متصل می‌شود، در کل مانند شکل عمل کنید.

بعد از آماده شدن کار باید Frame Relay را روی روترها فعال کنیم، روش‌های متفاوتی برای این کار وجود دارد که باهم این روش‌ها را بررسی می‌کنیم.

در روش اول به صورت اتوماتیک انجام می‌گیرد و با فعال کردن Frame Reley به صورت خودکار، روترهای مجاور شناسایی می‌شوند.

وارد روتر R1 شوید و دستورات زیر را وارد کنید:

```
R1(config)#int s1/0
R1(config-if)#encapsulation frame-relay
R1(config-if)#ip add 1.1.123.1 255.255.255.0
```

در دستورات بالا وارد اینترفیس سریال 1/0 شدیم و **encapsulation frame-relay** این دستور را فعال کردیم و بعدازآن ip address مربوط به این اینترفیس را وارد کردیم.

وارد روتر R2 شوید و دستورات زیر را وارد کنید:

```
R2(config)#int s1/0
R2(config-if)#encapsulation frame-relay
R2(config-if)#ip add 1.1.123.2 255.255.255.0
```

وارد روتر R3 شوید و دستورات زیر را وارد کنید:

```
R3(config)#int s1/0
R3(config-if)#encapsulation frame-relay
R3(config-if)#ip add 1.1.123.3 255.255.255.0
```

بعد از این کار و با فعال کردن Frame Relay به صورت خودکار توسط متدی به نام invers ARP، بقیه‌ی روتر ها متصل به این Fram Relay را شناسایی می‌کند و برای مشاهده‌ی جدول FR از دستور زیر استفاده کنید:

```
R1#show frame-relay map
Serial1/0 (up): ip 1.1.123.2 dlci 102, dynamic, broadcast, CISCO, status defined, active
Serial1/0 (up): ip 1.1.123.3 dlci 103, dynamic, broadcast, CISCO, status defined, active
```

همان‌طور که مشاهده می‌کنید با دستور **show frame-relay map**، لیست روترهای متصل از طریق FR به ما نمایش داده شد، اگر به پایان هر دستور نگاه کنید، گزینه‌ی Active را مشاهده می‌کنید که نشان‌دهنده‌ی فعال بودن خط است و می‌توانید به ip address های مورد نظر Ping کنید. در غیر این صورت اگر گزینه‌ی دیگری باشد، یعنی ارتباط با روتر دیگر برقرار نشده است.

نکته: همان‌طور که گفتیم، متد Invers ARP هر 60 ثانیه یک‌بار بین روتر و سوئیچ FR فعال می‌شود تا فعال بودن خط و شماره‌ی DLCI را چک کند و همین امر باعث ایجاد ترافیک بیهوده در آن می‌شود، برای حل این مشکل باید از Static Frame Relay استفاده و Invers ARP را خاموش کنید، به صورت زیر:

فعال کردن Static Frame Relay:

نکته: نرم‌افزار Packet Tracer این روش را پشتیبانی نمی‌کند، اما این روش را باهم بررسی می‌کنیم که روی بقیه‌ی نرم‌افزارها مانند GNS3 که در ادامه‌ی کتاب درباره‌ی آن بحث خواهیم کردیم، اجرا می‌شوند:

وارد روتر R1 شوید و دستورات زیر را وارد کنید:

```
R1(config)#int s1/0
R1(config-if)# Encapsulation Frame-relay
R1(config-if)#no frame-relay inverse-arp
R1(config-if)#frame-relay map ip 1.1.123.2 102 broadcast
R1(config-if)#frame-relay map ip 1.1.123.3 103 broadcast
```

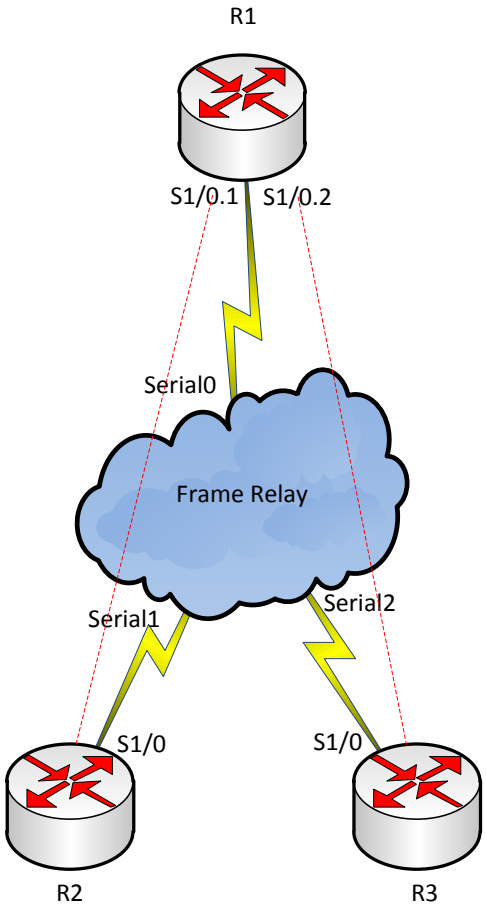
به دستورات بالا توجه کنید، وارد اینترفیس سریال 1/0 شدیم و Frame Relay را فعال کردیم و بعدازآن با دستور no frame-relay inverse-arp این متد را غیرفعال کردیم که به صورت خودکار عمل نکند در ادامه با دستور frame-relay map ip 1.1.123.2 102 broadcast یکی‌یکی، Ip address های روترهای دیگر را Map می‌کنیم شماره‌ی 102 هم به عنوان DLCI مربوط به روتر 2 است و در آخر می‌بایستی از عبارت "broadcast" استفاده کنیم، به خاطر اینکه به صورت پیش‌فرض split-horizon که در بحث‌های قبلی روی آن کار کردیم از آپدیت کردن Routing جلوگیری می‌کند (به این صورت که از طریق اینترفیسی که آن Route را دریافت کرده، دوباره به همان اینترفیس برنمی‌گرداند). برای مثال، اگر روتر R1 یک آپدیت به سمت R2 می‌فرستد R2 نمی‌تواند یک آپدیت به R1 ارسال کند، به خاطر اینکه هر دوی آن‌ها از طریق یک اینترفیس آپدیت‌ها را ارسال و دریافت می‌کنند. با استفاده از عبارت "broadcast" ما به R2 می‌گوییم که یک کپی از هر broadcast یا multicasti که از طریق اینترفیس خودت دریافت می‌کنی را به مدار مجازی (virtual circuit) که با مقدار DLCI اختصاص داده شده، در دستور "frame-relay map" ارسال کن. در واقع یک پکت کپی شده به صورت unicast (نه broadcast) ارسال می‌شود که بعضی اوقات نیز با نام "pseudo-broadcast" نیز شناخته می‌شود.

برای روتر بعدی هم می‌نویسیم frame-relay map ip 1.1.123.3 103 broadcast و در بقیه‌ی روترها هم همین کار را انجام می‌دهیم و به این صورت، روترها به صورت دستی همدیگر را شناسایی می‌کنند.

Hub And Spoke:

این روش به این صورت است که یک روتر به عنوان روتر اصلی انتخاب می‌شود و بقیه‌ی روترها فقط به این روتر متصل می‌شوند و از طریق این روتر به بقیه‌ی روترها دسترسی پیدا می‌کنند. موضوعی که در این روش به چشم می‌خورد SubInterface است که برای هر یک از روترها به صورت Point To Point یا Point To Multi Point تعریف می‌شود.

به شکل زیر توجه کنید:



در این شکل روتر R1 از دو Subinterface برای ارتباط با روترهای R2 و R3 استفاده می‌کند که روش تنظیم کردن آن به صورت زیر است:

وارد روتر R1 شوید و دستورات زیر را وارد کنید:

```
Router(config)#int s1/0
Router(config-if)#encapsulation frame-relay
Router(config-if)#exit
Router(config)#int s1/0.1 point-to-point
Router(config-subif)#frame-relay interface-dlci 102
Router(config-subif)#ip add 1.1.123.1 255.255.255.0
```

اول وارد اینترفیس s1/0 می‌شویم و Frame Relay را فعال می‌کنیم و بعدازآن با دستور Exit خارج شده و با دستور int s1/0.1 point-to-point وارد اینترفیس مجازی می‌شویم؛ Point to Point نشان‌دهنده‌ی ارتباط مستقیم

با روتر روبرو است، یعنی اینکه دو روتر در یک Subnet کار می‌کنند، بعد از وارد شدن باید ip address را وارد کنیم که به صورت ip add 1.1.123.1 255.255.255.0 وارد می‌کنیم.

همان‌طور که مشاهده کردید، این ارتباط با روتر R2 بوده و برای R3 هم به صورت زیر عمل می‌کنیم:

```
Router(config)#int s1/0.2 point-to-point
Router(config-subif)#frame-relay interface-dlci 103
Router(config-subif)#ip add 1.1.124.1 255.255.255.0
```

بعد از واردکردن دستورات در روتر R1 باید در روترهای دیگر هم دستورات را وارد کنیم:

وارد روتر R2 شوید و دستورات زیر را وارد کنید:

```
Router(config)#int s1/0
Router(config-if)#encapsulation frame-relay
Router(config-if)#exit
Router(config)#int s1/0.1 point-to-point
Router(config-subif)#frame-relay interface-dlci 201
Router(config-subif)#ip add 1.1.123.2 255.255.255.0
Router(config-subif)#int s1/0
Router(config-if)#no shut
```

وارد interface S1/0 شدیم و بعدازآن Frame Relay را با دستور encapsulation Frame Relay فعال کردیم بعد با دستور Exit از اینترفیس اصلی خارج شده و با دستور int s1/0.1 point-to-point وارد اینترفیس مجازی s1/0.1 شدیم که همین اینترفیس را در روتر 1 ایجاد کردیم. بعدازآن از دستورframe-relay interface-dlci 201 استفاده می‌کنیم که ارتباط با روتر R1 از طریق DLCI 201 برقرار شود و بعدازآن از دستور ip add 1.1.123.2 255.255.255.0 استفاده می‌کنیم که ip address است که در رنج روتر R1 قرار دارد، توجه داشته باشید بعد از واردکردن دستورات، حتماً وارد پورت S1/0 شوید و آن را فعال کنید؛ به هیچ وجه در پورت مجازی این کار را انجام ندهید.

وارد روتر R3 شوید و دستورات زیر را وارد کنید:

```
Router(config)#int s1/0
Router(config-if)#encapsulation frame-relay
Router(config-if)#exit
Router(config)#int s1/0.2 point-to-point
Router(config-subif)#frame-relay interface-dlci 301
Router(config-subif)#ip add 1.1.124.2 255.255.255.0
Router(config-subif)#int s1/0
Router(config-if)#no shut
```

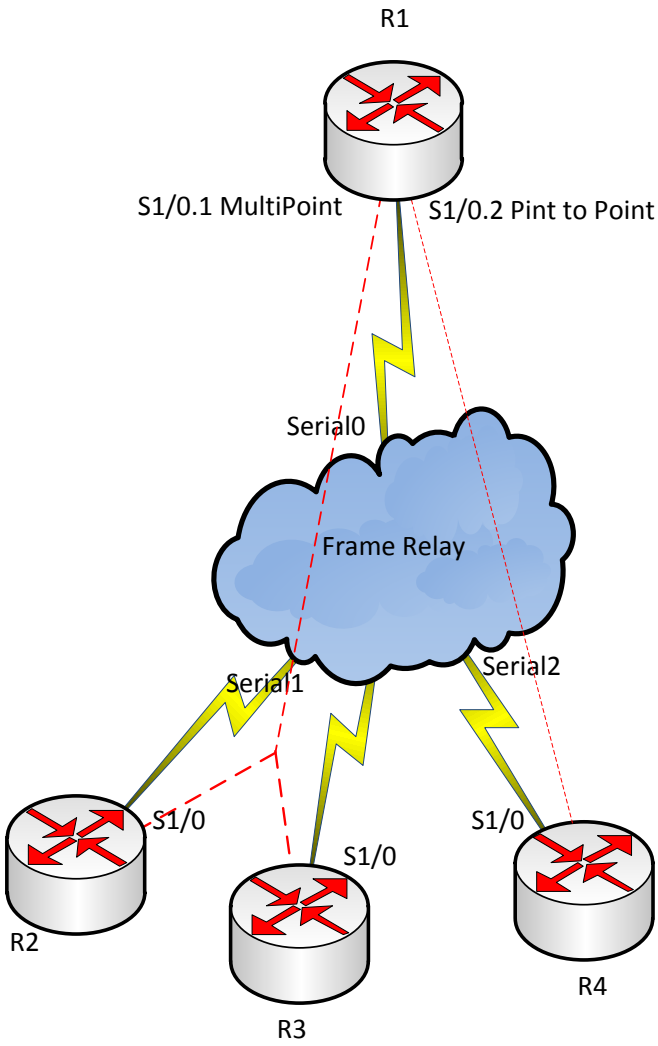
بعد از پایان کار، وارد روتر یک شوید و دستور زیر را وارد کنید:

Router#**show frame-relay map**
Serial1/0.1 (up): point-to-point dlci, dlci 102, broadcast, status defined, active
Serial1/0.2 (up): point-to-point dlci, dlci 103, broadcast, status defined, active

همان‌طور که مشاهده می‌کنید دو مسیر به لیست اضافه شده است. از روتر R1 می‌توانید به روترهای R2 و R3 ارتباط داشته باشید، اما روتر R2 نمی‌تواند به روتر R3 ارتباط داشته باشد! این موضوع به خاطر این است که هیچ روتینگ پروتکلی بین آن‌ها راه‌اندازی نشده است، برای این کار روی هر روتر، پروتکل EIGRP اجرا می‌کنیم وNetwork ها را به این پروتکل معرفی می‌کنیم.

ایجاد Hybrid Topology:

به شکل زیر توجه کنید:



در شکل صفحه قبل، روترهای R1 و R2 و R3 به صورت MultiPoint به هم متصل هستند و در یک شبکه قرار دارند و روترهای R1 و R4 هم به صورت Point To Point به هم متصل هستند و در یک شبکه قرار دارند.
وارد روتر R1 شوید و دستورات زیر را وارد کنید:

```
R1(config)#int s1/0
R1(config-if)#encapsulation frame-relay
R1(config-if)#no shutdown
R1(config)#int s1/0.123 multipoint
R1(config-subif)#frame-relay interface-dlci 102
R1(config-subif)#frame-relay interface-dlci 103
R1(config-subif)#ip add 1.1.123.1 255.255.255.0
```

در مرحله‌ی اول، وارد اینترفیس فیزیکی می‌شویم و Frame Relay را راه‌اندازی و پورت را روشن می‌کنیم. بعدازآن از پورت خارج می‌شویم و با دستور int s1/0.123 multipoint وارد اینترفیس مجازی با عملکرد MultiPoint می‌شویم و DLCI های مربوط به روترهای دیگر را که در این شبکه می‌خواهند قرار بگیرند را وارد می‌کنیم، بعد Ip address را برای این پورت مجازی وارد می‌کنیم.
برای پورت مجازی دیگر که به روتر R4 متصل و اتصال آن به صورت Point To Point است، دستورات زیر را وارد می‌کنیم:

```
R1(config)#int s1/0.124 point-to-point
R1(config-subif)#frame-relay interface-dlci 104
R1(config-subif)#ip add 1.1.124.1 255.255.255.0
```

وارد روتر R2 شوید و دستور زیر را وارد کنید:

```
R2(config-if)# encapsulation frame-relay
R2(config-if)#no sh
R2(config)#int s1/0.123 multipoint
R2(config-subif)#frame-relay interface-dlci 201
R2(config-subif)#frame-relay interface-dlci 203
R2(config-subif)#ip add 1.1.123.2 255.255.255.0
```

در این روتر همان‌طور که مشاهده می‌کنید، DLCI های مربوط به روترهای R1 و R3 را وارد کردیم و IP Address را وارد کردیم که دو روتر دیگر هم در این رنج قرار دارند.
یک نکته بسیار مهم این است که حتماً از MultiPoint استفاده کنید تا ارتباط بین روترها باهم برقرار شود.
وارد روتر R3 شوید و دستورات زیر را وارد کنید.

```
R2(config-if)# encapsulation frame-relay
R2(config-if)#no sh
R2(config)#int s1/0.123 multipoint
```

```
R2(config-subif)#frame-relay interface-dlci 301
R2(config-subif)#frame-relay interface-dlci 302
R2(config-subif)#ip add 1.1.123.3 255.255.255.0
```

در این روتر، DLCI مربوط به روترهای R1 و R2 را وارد کردیم و یک ip address در رنج روترهای دیگر وارد کردیم.

وارد روتر R4 شوید و دستورات زیر را وارد کنید:

```
Router>
Router>en
Router#conf t
Router(config)#int s1/0
Router(config-if)#encapsulation frame-relay
Router(config-if)#exit
Router(config)#int s1/0.124 point-to-point
Router(config-subif)#frame-relay interface-dlci 401
Router(config-subif)#ip address 1.1.124.2 255.255.255.0
Router(config-subif)#int s1/0
Router(config-if)#no sh
```

تا اینجا تنظیمات روی تمام روترها انجام شده است. برای مشاهده‌ی جدول Frame Relay از دستور زیر استفاده کنید:

```
R1(config-if)#do sh fram map
Serial1/0.123 (up): ip 1.1.123.2 dlci 102, dynamic, broadcast, CISCO, status defined, active
Serial1/0.123 (up): ip 1.1.123.3 dlci 103, dynamic, broadcast, CISCO, status defined, active
Serial1/0.124 (up): point-to-point dlci, dlci 104, broadcast, status defined, active
```

همان‌طور که مشاهده می‌کنید، خط‌های دوم و سوم مربوط به روترهای R2 و R3 است و خط چهارم مربوط به روتر R4 است که به صورت point-to-point به آن متصل شده‌ایم. در این قسمت اگر سؤالی برای شما پیش آمده است، با من در تماس باشید.

IPv6

شبکه‌هایی که با آن‌ها در حال حاضر کار می‌کنیم، بیشتر آن‌ها از IPV4 استفاده می‌کنند، به دلیل تولید بسیار زیاد ادوات الکترونیکی و استفاده‌ی آن‌ها از اینترنت این آدرس‌ها در حال اتمام می‌باشند که همین امر باعث شد که محققان سازمان Internet Engineering Task Force (IETF) مدل جدید آن را با عنوان IPv6 معرفی کردند که بسیار بیشتر از ipv4 آدرس در اختیار جامعه قرار داده است، البته IPV5 هم وجود داشت که به خاطر مشکلاتی که در سر راه قرار داشت، گسترش نیافت و به فراموشی سپرده شد.

ویژگی‌های ipv6:

- ✓ **فضای آدرس‌دهی بسیار بزرگ:**

همان‌طور که می‌دانید و در درس‌های قبلی هم بیان کردیم، ipv4 از 32 بیت تشکیل شده است، اما ipv6 از 128 بیت تشکیل شده است که به صورت زیر بیان می‌شود:

2^128 = 340,282,366,920,938,463,374,607,431,770,000,000

این تعداد ip address هایی است که این پروتکل پشتیبانی می‌کند که واقعاً زیاد است، یعنی در هر مترمربع کره‌ی زمین، چندین هزار آدرس IP اختصاص داده می‌شود.

- ✓ **حذف NAT:**

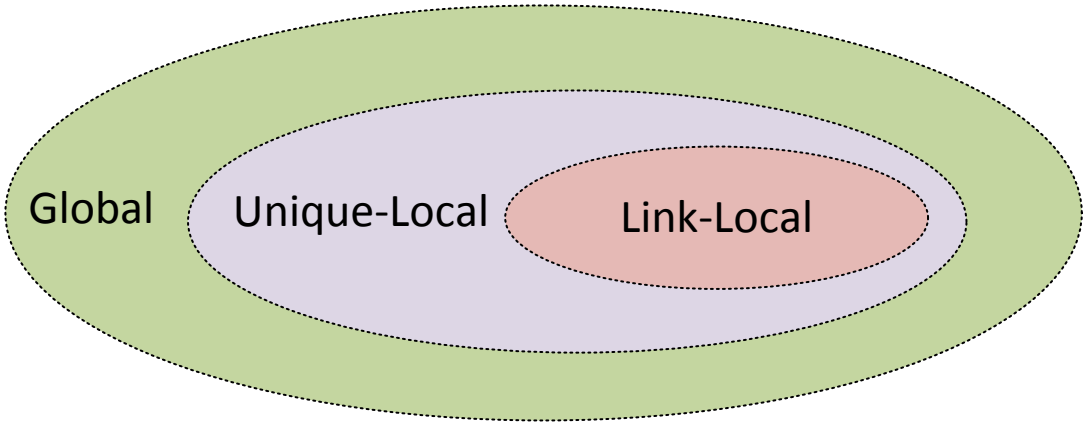
همان‌طور که قبلاً باهم بررسی کردیم، IPV4 برای خارج شدن از شبکه‌ی داخلی و ورود به اینترنت باید تبدیل به IP های VALID می‌شد که این کار را با ترجمه‌ی آدرس‌های Invalid به Valid انجام می‌دادیم که به آن NAT می‌گفتند، اما در مورد IPV6 این چنین نیست و دیگر NAT در این پروتکل استفاده نمی‌شود.

✓ **حذف شدن آدرس‌های Broadcast:**

در این پروتکل، به علت افزایش تعداد آدرس‌های Multi cast دیگر خبری از Broadcast نیست و آدرس‌ها به صورت Unicast و Multicast و Anycast می‌باشند.

Unicast:

به آدرس‌هایی گفته می‌شود که برای ارتباط بین یک مبدأ و مقصد استفاده می‌شوند.



- **Global unicast address**: به مفهوم آدرس‌های unicast قابل انتقال در اینترنت است (قابلیت آدرس‌دهی در اینترنت را دارد) و شبیه به نوع متناظر آن در IPv4 می‌باشد، به این نوع آدرس‌ها Aggregatable Address نیز می‌گویند. این ساختار از قسمت‌های زیر تشکیل شده است.
- **Unique local address**: این آدرس‌ها را با نام Site-Local unicast هم می‌شناسند که قابلیت انتقال در اینترنت را نداشته، اما در هر جا که مورد استفاده قرار گیرند ، در بین تمامی دیگر آدرس‌های اینترنت منحصربه‌فرد می‌باشند. عملکرد این نوع آدرس‌ها دقیقاً شبیه به آدرس‌های private در IPv4 بوده و امکان برقراری ارتباط بین دستگاه‌های یک سازمان محلی را با واسطه روترها ممکن می‌سازند. این آدرس‌ها با 16 بیت ثابت (feco) شروع می‌شوند و به دنبال آن 32 بیت صفر و سپس 16 بیت مربوط به Subnet ID است که معمولاً آن را هم صفر در نظر می‌گیرند.64 بیت پایانی هم که Interface ID است که برای هر کامپیوتر منحصربه‌فرد است*
- **Link local address**: شبیه به آدرس‌های Private یا خصوصی در IPv4 بوده و قابل انتقال در اینترنت نیستند. این آدرس‌ها را می‌توان به اعضای یک شبکه LAN و یا چند LAN مختلف که قصد برقراری ارتباط

با یکدیگر دارند را تخصیص داد. این آدرس‌ها که در غیاب DHCP Server ایجاد می‌شوند، در IPv6 معادل Fe80::/64هستند. به بیانی دیگر اگر در هنگام تنظیم IP آدرس، در کادر محاوره‌ای Properties کارت شبکه گزینه‌ی obtain IPv6 address automatically را انتخاب کنیم، سیستم عامل به طور خودکار بر اساس تلفیقی از MAC Address مربوط به کارت شبکه با آدرس Link-Local یک آدرس IPv6 به کارت شبکه اختصاص می‌دهد.

- **Special unicast address**: مانند Loopback ::1

Multicast:

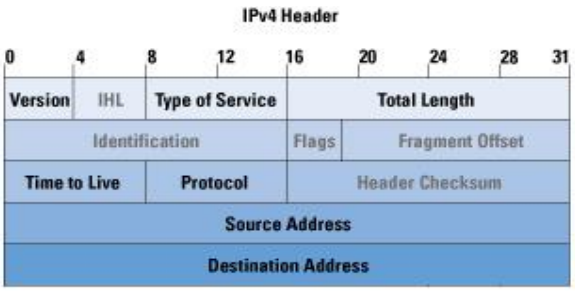
برای ارتباط یک مبدأ با چند مقصد مشخص‌شده استفاده می‌شود که این مقصد در یک گروه قرار دارند؛ این آدرس جایگزین Broadcast در ipv4 شده است. در ادامه، جدول کامل این آدرس‌ها قرار گرفته شده است.

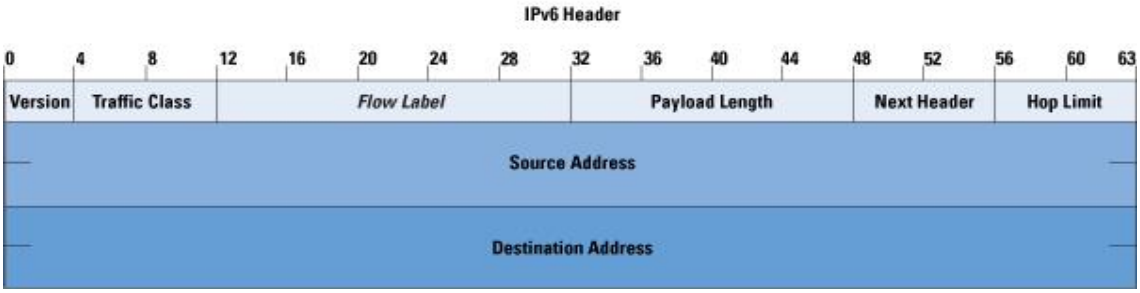
Anycast:

در این آدرس‌دهی برای مثال روتر شما برای رسیدن به یک سرور چند مسیر را در پیش رو دارد، روتر مسیری را انتخاب می‌کند که کمترین Cost را داشته باشد، پس آدرس Anycast آدرسی است برای انتخاب بهترین مسیر تا رسیدن به یک سرور و یا انتخاب یک سرور بین چند سرور یکسان که هزینه‌ی کمتری دارد.

تفاوت Header های ipv4 و ipv6:

اگر به IPV4 دقیق نگاه کنید، متوجه‌ی پیچیده‌تر بودن آن نسبت به IPV6 می‌شوید، در واقع ipv6 خیلی ساده‌تر از رفیق قبلی خود، یعنی IPV4 است.





هر یک از گزینه‌های موجود در این Header ها را باهم مورد بررسی قرار می‌دهیم:

Version: این فیلد 4 بیتی بوده و نشان‌دهنده‌ی نسخه‌ی IP موجود است.

Traffic Class: برای مشخص کردن کلاس‌های مختلف و مشخص کردن اولویت پکت‌ها IPV6 استفاده می‌شود و طول آن 8 بیت است.

Flow Label: طول این فیلد 20 بیت است. یکی از ویژگی‌های آن پشتیبانی از QOS است که یکی از ویژگی‌های جدید در IPV6 است و توانایی مسیریابی ترافیک مشخص را در شبکه می‌دهد.

Payload Length: طول این بخش 20 بیت است که شامل طول بخش بسته‌ی IPV6 است.

NextHeader: طول این فیلد 8 بیت است که نشان‌دهنده‌ی نوع Header در IPV6 است.

Hop Limit: طول این فیلد 8 بیت است که برای مشخص کردن تعداد روترهایی است که بسته‌ی اطلاعاتی از آن رد می‌شود، یعنی زمانی‌که این بسته از یک روتر در سر راه رد می‌شود یک شماره از این زمان کم می‌شود و تا زمانی که این شماره به پایان برسد و بسته مورد نظر حذف شود.

Source Address: نشان‌دهنده‌ی آدرس مبدأ است.

DestinationAddress: نشان‌دهنده‌ی آدرس مقصد است.

روش آدرس‌دهی در IPV6:

IPV6 از 128 بیت تشکیل شده است یعنی از 8 قسمت 16 بایتی تشکیل شده است که هر قسمت آن به صورت hexadecimal است یعنی از 0 تا F و توسط (:) هر قسمت از قسمت دیگر جدا می‌شود:

2001:0DA8:E800:0000:0260:3EFF:FE47:0001

فکر می‌کنم بعد از دیدن این آدرس سردرگم شده‌اید، اما نگران نباشید می‌توانیم با روش‌هایی این آدرس را بررسی کنیم:

- ✓ **روش اول – حذف صفرهای ابتدایی:**

در این روش هر چه صفر قبل از یک عدد وجود دارد را حذف می‌کنیم:

2001:0DA8:E800:0000:0260:3EFF:FE47:0001

2001: DA8:E800:0: 260:3EFF:FE47: 1

✓ **روش دوم – حذف صفرهای پشت سر هم:**

در این روش اگر بین یک کلون " : " چندین صفر وجود داشت، می‌توانید صفرها را حذف کرده و فقط کلون را قرار دهیم. به روش زیر توجه کنید:

2001:0000:0000:2260:3EFF:FE47:0001

2001:: 2260:3EFF:FE47:1

همان‌طور که مشاهده می‌کنید به جای صفرهایی که در قسمت 2 و 3 قرار داشتند، فقط :: قرار دادیم که همین کار باعث کوتاه شدن این IP شده است.

تذکر مهم: دو بار استفاده از کلون یا :: در یک IP امکان‌پذیر نیست و مشکل ایجاد می‌شود.

در آدرس‌دهی IPV4 اگر یادتان باشد ما از IP address به همراه SubnetMask استفاده می‌کردیم که چنین موضوعی در IPv6 وجود ندارد و به جای آن از subnet Prefix استفاده می‌کند.

در IPV6 چیزی به نام NETMASK وجود ندارد و جایگزین آن Prefix است، در واقع Prefix جداکننده‌ی NET ID از HOST ID است.

Net ID Host ID

2014:2015:0000:0000:BC02:0000:0001:0002/64

در مثال بالا 64/ به این معناست که از سمت چپ 64 بیت به جلو برویم و بعد از 64 بیت قسمت HOST ID شروع می‌شود و قبل از آن مربوط به NET ID می‌شود. هر عدد در اینجا معادل 4 بیت است.

انواع آدرس‌های ipv6:

روش‌های آدرس‌دهی به صورت Unicast:

فرم کلی Global Unicast:

از چپ به راست

FP	TLA-ID	RES	NLA-ID	SLA-ID	INTERFACEID
3 بیت	13 بیت	8 بیت	16 بیت	24 بیت	64 بیت

FP: نشان‌دهنده‌ی نوع IPV6 است (Format Prefix) ipهای PUBLIC ورژن 6 در حالت باینری با 001 شروع می‌شود.

TLA-ID: مخفف (TopLevel Aggregator Identifire) دسته‌بندی IP هایی هستند که به جاهای بزرگ، مانند قاره‌ها اختصاص پیدا می‌کنند.

RES: یعنی رزرو شده است.

NLA-ID: مخفف(Next Aggregator Identifire) IP های منحصربه‌فردی هستند که به جاهای بزرگ، مانند کشورها اختصاص پیدا می‌کنند.

SLA-ID: مخفف (Site Level) ip های منحصربه‌فردی هستند که به جاهای بزرگ، مانند شهرها و سازمان‌های بزرگ اختصاص پیدا می‌کنند (ایران خودرو).

Ip های خاصی در IPV6 وجود دارند که به شرح زیر می‌باشند:

::/128 یک آدرس نامشخص ابتدای یک بایت است که می‌خواهد آدرس Link-Local را مشخص کند.

::/0 این آدرس معادل 0.0.0.0 در IPV4 است و برای مسیریابی به صورت دستی از این آدرس استفاده می‌کنند.

::1/128 این آدرس معادل آدرس LoopBack است که در ipv4 به صورت 127.0.0.1 بوده است و برای تست کارت شبکه و پروتکل TCP/IP استفاده می‌شود.

FE80::/10 آدرس Link Local Unicast است که شبیه به آدرس 169.254.x.x است.

FF00::/8 آدرس‌های مربوط به Multicast است.

آدرس‌های Multicast:

این آدرس‌ها جایگزین Broadcast در IPV4 شده‌اند و برای کارهای زیر استفاده می‌شوند:

- برای استفاده در سرویس DHCP.
- اعلام مسیرها در روترiا که قبلاً به صورت Broadcast در IPV4 آموختیم.
- برای تقاضاهای روتر.
- و...
- این آدرس‌ها از 8 بیت پسوند Prefix استفاده می‌کنند که به صورت FF00::/8 است، default Gateway برای کلاینت‌ها وجود ندارد.

در جدول زیر، انواع ip های multicast برای پروتکل‌ها و سرورها و ... را مشاهده می‌کنید:

Address	توضیحات
ff02::1	همه‌ی گره‌ها در بخش شبکه‌های محلی
ff02::2	تمام روترها در بخش شبکه‌های محلی
ff02::5	برای الگوریتم spf مربوط به OSPFV3
ff02::6	مربوط به همه‌ی روترهای DR در پروتکل OSPF
ff02::8	مربوط به پروتکل IS-IS
ff02::9	مربوط به پروتکل RIP
ff02::a	مربوط به پروتکلEIGRP
ff02::d	مربوط به روترهای Protocol Independent Multicast (PIM)
ff02::16	گزارش مربوط به MLDv2 تعریف‌شده در RFC 3810
ff02::1:2	همه‌ی سرورهای DHCP و Real Agent ها در شبکه‌ی محلی
ff02::1:3	تمام میزبان‌های (Link Local Multicast Name Resolution) LLMNR در شبکه‌ی محلی
ff05::1:3	همه‌ی سرورهای DHCP در سایت شبکه‌ی محلی
ff0x::c	مربوط به Service Discovery Protocol
ff0x::fb	مربوط به(DNS) Multicast Domain Name System
ff0x::101	Network Time Protocolمربوط به

IPV6 می‌تواند به صورت خودکار توسط روش‌های زیر تنظیم شود:

stateful Auto configuration
stateless Auto configuration
EUI – 64

stateful Auto configuration:

در این روش که سرویس DHCP از آن استفاده می‌کند یک آدرس با طول 128 بیت واگذار می‌شود.

stateless Auto configuration:

در این روش یک IPV6 که 128 بیت است را نصف می‌کند و 64 بین از آن را استفاده و 64 بیت دوم را بعداً استفاده می‌کند، یعنی اینکه 64 بین از یک آدرس واگذار می‌شود و 64 بیت در یک زمان دیگر استفاده می‌شود.

EUI – 64:

در این روش روتر برای اختصاص دادن IP به کلاینت مورد نظر از آدرس Mac آن در IPv6 استفاده می‌کند به این صورت که 64 بین اول به صورت دستی وارد می‌شود و 64 بیت دوم از طریق Mac address دستگاه مورد نظر استخراج می‌شود، اما آدرس Mac، 48 بیتی است. برای حل این مشکل از مقدار FFFE در وسط آدرس Mac استفاده می‌کنند و به‌این‌ترتیب آدرس مورد نظر به دستگاه مورد نظر داده می‌شود.

مثلاً برای واردکردن آدرس به این روش، وارد اینترفیس می‌شویم و از آدرس زیر استفاده می‌کنیم:

Router(config-if)# ipv6 address 2011:1111:11::1/64 eui-64

بعد از اینکه آدرس را وارد کردیم با دستور **Show IPV6 Interface Berife** می‌توانیم آدرس اصلی را مشاهده کنیم که به صورت زیر است:

Static Address	Mac Address
2011:1111:11:0:	2D0:97FF:FE51:6A02

همان‌طور که مشاهده می‌کنید در قسمت دوم از آدرس FFFE برای کامل کردن آدرس Mac دستگاه مورد نظر استفاده کرده است.

استفاده از ipv6 در پروتکل RIP :

پروتکل RIP را با عنوان RIP NG برای IPV6 می‌شناسند، برای فعال کردن RIP برای استفاده از IPV6 باید قبل از هر کاری ipv6 unicast-routing را فعال کنید. اگر این قسمت را فعال نکنید به شما پیغام خطا می‌دهد و می‌گوید که ipv6 Routing فعال نشده، پس قبل از هر چیز این دستور را اجرا کنید، بعد با دستور زیر پروتکل RIP برای IPV6 فعال می‌شود:

ipv6 router rip RIPNG

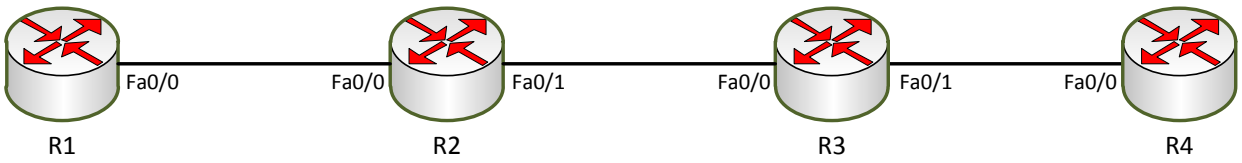
این دستور با دستورات گذشته که برای RIP تعریف می‌کردیم، متفاوت است و یک اسم باید برای این RIP وارد کنیم که در این دستور از اسم RIPNG استفاده کردیم و شما می‌توانید هر اسم دیگری را وارد کنید، بعد از فعال شدن RIP دیگر لازم نیست که شبکه‌های متصل به روتر را در RIP تعریف کنیم، باید وارد اینترفیس مربوطه شویم و RIP را روی این اینترفیس فعال کنیم، به صورت زیر:

R1(config-rtr)**#int s0/1**
R1(config-if)**#ipv6 rip RIPNG enable**

همان‌طور که مشاهده می‌کنید وارد اینترفیس S0/1 شدیم و پروتکل RIP با نام RIPNG که قبلاً ایجاد کرده‌ایم را فعال کردیم.

شماره‌ی پورت برای پروتکل RIP Ng ، 520 با پروتکل UDP است.

مثال برای RIP NG:



در این مثال می‌خواهیم به اینترفیس‌ها، آدرسی از نوع IPV6 بدهیم و بعدازآن RIP را فعال کنیم:

این شکل را در نرم‌افزار خود ایجاد کنید.

وارد روتر R1 می‌شویم و دستور زیر را وارد می‌کنیم:

```
R1#conf t
R1(config)# ipv6 unicast-routing
R1(config)# ipv6 router rip rip1
R1(config)# int f0/0
R1(config-if)# ipv6 address 2011:111:12::1/64
R1(config-if)#ipv6 rip rip1 enable
```

همان‌طور که مشاهده می‌کنید در مرحله‌ی اول با دستور ipv6 unicast-routing باعث فعال شدن IPV6 Routing شدیم. بعدازآن RIP را با نام RIP1 تعریف کردیم، وارد اینترفیس شدیم و آدرس IPV6 مربوطه را وارد کردیم. این آدرس به این صورت است که 12 را به عنوان شماره‌ی روترها که بین روتر 1 و 2 است وارد کردیم و 1:: هم شماره‌ی مختص این اینترفیس است. در آخر هم پروتکل Rip را که با نام RIP1 ایجاد کردیم، بر روی این اینترفیس فعال می‌کنیم.

وارد روتر R2 می‌شویم و دستور زیر را وارد می‌کنیم:

```
R2#conf t
R2(config)# ipv6 unicast-routing
R2(config)# ipv6 router rip rip1
R2(config)# int f0/0
R2(config-if)# ipv6 address 2011:111:12::2/64
R2(config-if)#ipv6 rip rip1 enable
R2(config)# int f0/1
R2(config-if)# ipv6 address 2011:111:23::1/64
```

R2(config-if)#ipv6 rip rip1 enable

در R2 در هر دو اینترفیس پروتکل RIP را فعال کردیم و آدرس متفاوت وارد کردیم.

وارد روتر R3 می‌شویم و دستور زیر را وارد می‌کنیم:

R3(config)#ipv6 unicast-routing
R3(config)#ipv6 router rip rip1

R3(config-rtr)**#int f0/0**
R3(config-if)**#ipv6 address 2011:1111:23::2/64**
R3(config-if)**#ipv6 rip rip1 en**
R3(config-if)**#ipv6 rip rip1 enable**
R3(config-if)**#no shutdown**

R3(config-if)**#int f0/1**
R3(config-if)**#ipv6 address 2011:1111:34::1/64**
R3(config-if)**#ipv6 rip rip1 enable**
Router(config-if)**#no shutdown**

وارد روتر R4 می‌شویم و دستور زیر را وارد می‌کنیم:

Router(config)**#ipv6 unicast-routing**
Router(config)**#ipv6 router rip rip1**
Router(config-rtr)**#int f0/0**
Router(config-if)**#ipv6 address 2011:1111:34::2/64**
Router(config-if)**#ipv6 rip rip1 enable**
Router(config-if)**#no shutdown**

بعد از اتمام کار وارد روتر R1 شوید و روتر R4 را Ping کنید:

R1(config-if)**#do ping 2011:1111:34::2**

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2011:1111:34::2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1

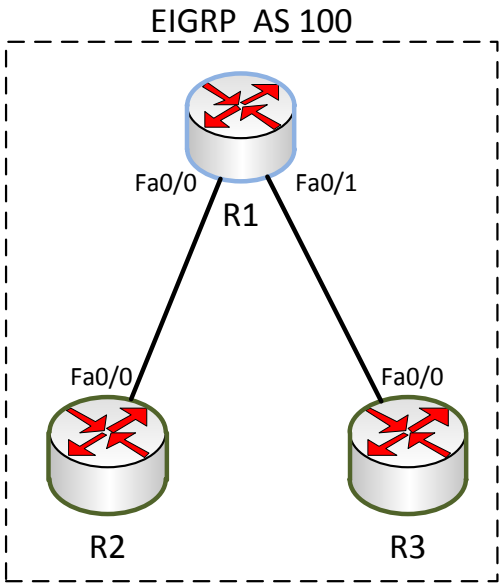
برای نمایش جدول روتینگ در ipv6 از دستور زیر استفاده می‌کنیم:

R1**#show ipv6 route**
IPv6 Routing Table - 5 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
U - Per-user Static route, M - MIPv6
I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
D - EIGRP, EX - EIGRP external
C 2011:1111:12::/64 [0/0]
via ::, FastEthernet0/0
L 2011:1111:12::1/128 [0/0]

```
    via ::, FastEthernet0/0
R   2011:1111:23::/64 [120/2]
    via FE80::290:CFF:FEA4:8B01, FastEthernet0/0
R   2011:1111:34::/64 [120/3]
    via FE80::290:CFF:FEA4:8B01, FastEthernet0/0
L   FF00::/8 [0/0]
via ::, Null0
```

فعال کردن IPV6در پروتکل EIGRP:

با یک مثال این موضوع را بررسی می‌کنیم، شبکه‌ی زیر را ایجاد کنید:



ایجاد پروتکل EIGRP برای استفاده از IPV6 بسیار شبیه به پروتکل RIP است، اما یک نکته در درون آن نهفته است که با هم بررسی می‌کنیم.

وارد روتر R1 شوید و دستورات زیر را وارد کنید:

```
R1(config)#ipv6 unicast-routing
R1(config)#ipv6 router eigrp 100
R1(config-rtr)#no shutdown
R1(config-rtr)#int f0/0
R1(config-if)#ipv6 address 2011:1111:12::1/64
R1(config-if)#ipv6 eigrp 100
R1(config-if)#no shutdown
R1(config)#int f0/1
R1(config-if)#ipv6 add
R1(config-if)#ipv6 address 2011:1111:13::1/64
R1(config-if)#ipv6 eigrp 100
R1(config-if)#no shutdown
```

با دستور ipv6 unicast-routing پروتکل IPV6 را روی این روتر فعال کردیم، بعدازآن EIGRP 100 را ایجاد کردیم و بعدازآن دستور No Shutdown را وارد کردیم که نکته‌ای که به شما گفته بودم، همین موضوع است که باید دستور no shutdown بعد از وارد شدن درون Eigrp اجرا کنیم تا فعال شود به طور پیش‌فرض این پروتکل غیرفعال است. بقیه‌ی کار مانند قبل است، وقتی وارد اینترفیس شدیم، آدرس مورد نظر را وارد و بعدازآن EIGRP ساخته‌شده را روی این اینترفیس فعال می‌کنیم.

وارد روتر R2 شوید و دستورات زیر را وارد کنید:

```
R2(config)#ipv6 unicast-routing
R2(config)#ipv6 router eigrp 100
R2(config-rtr)#no shutdown
R2(config-rtr)#int f0/0
R2(config-if)#ipv6 address 2011:1111:12::2/64
R2(config-if)#ipv6 eigrp 100
R2(config-if)#no shutdown
```

وارد روتر R3 شوید و دستورات زیر را وارد کنید:

```
R3(config)#ipv6 unicast-routing
R3(config)#ipv6 router eigrp 100
R3(config-rtr)#no shutdown
R3(config-rtr)#int f0/0
R3(config-if)#ipv6 address 2011:1111:13::2/64
R3(config-if)#ipv6 eigrp 100
R3(config-if)#no shutdown
```

وارد روتر R2 شوید و روتر R3 را ping کنید:

```
R2(config-if)#do ping 2011:1111:13::2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2011:1111:13::2, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
```

به هیچ عنوان جواب نمی‌دهد، به این دلیل که وقتی EIGRP را با IPV6 فعال می‌کنیم، حتماً باید برای هر یک از روترها Router-id تعریف کنیم تا بتوانند همدیگر را ببینند. برای این کار، وارد هر یک از روترها می‌شویم و در اینترفیس LoopBack 0، یک آدرس وارد می‌کنیم، مانند دستور زیر:

```
R2(config-if)# int LoopBack 0
R2(config-if)# ip add  100.1.2.2 255.255.255.0
```

فقط کافی است، شما Router-Id را تعریف کنید، خود پروتکل Eigrp به صورت خودکار روتر روبرو را شناسایی می‌کند.

بعد از فعال کردن Router-id، می‌توانید روترها را به هم ping کنید:

R2(config-if)#**do ping 2011:1111:13::2**

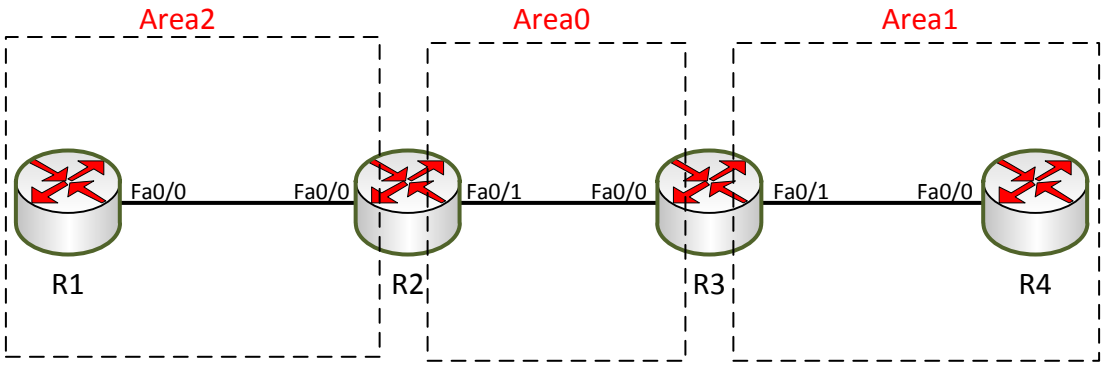
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2011:1111:13::2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms

با دستور **show ipv6 route**، نگاهی به جدول روتینگ می‌اندازیم:

R2#**show ipv6 route**
IPv6 Routing Table - 4 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
U - Per-user Static route, M - MIPv6
I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
D - EIGRP, EX - EIGRP external
C 2011:1111:12::/64 [0/0]
via ::, FastEthernet0/0
L 2011:1111:12::2/128 [0/0]
via ::, FastEthernet0/0
D 2011:1111:13::/64 [90/30720]
via FE80::290:21FF:FEB9:2101, FastEthernet0/0
L FF00::/8 [0/0]
via ::, Null0

همان‌طور که مشاهده می‌کنید، شبکه‌ی 2011:1111:13::/64 را از طریق Eigrp یاد گرفته است.

فعال کردن IPV6 روی پروتکل OSPF V3:



در این مثال، می‌خواهیم با نحوه‌ی کار IPV6 در پروتکل OSPF آشنا شویم. به پروتکل OSPF که IPV6 روی آن فعال می‌شود، OSPF V3 می‌گویند که ورژن 3 این پروتکل است.

وارد روتر R1 می‌شویم و دستورات زیر را وارد می‌کنیم:

```
R1(config)#ipv6 unicast-routing
R1(config)#ipv6 router ospf 100
R1(config-rtr)#router-id 150.1.1.1
R1(config-rtr)#int f0/0
R1(config-if)#ipv6 address 2011:1111:12::1/64
R1(config-if)#ipv6 ospf 100 area 2
R1(config-if)#no shutdown
```

دستورات، مانند گذشته است، فقط زمانی که با دستور ipv6 router ospf 100، پروتکل OSPF را تعریف کردیم و وارد آن شدیم، باید Router-ID را تعریف کنیم. بعدازآن وارد اینترفیس می‌شویم، آدرس را تعریف می‌کنیم و در آخر با دستور ipv6 ospf 100 area 2، پروتکل OSPF را روی این اینترفیس فعال می‌کنیم و در area 2 (طبق شکل) قرار می‌دهیم و بعد با دستور no shutdown، اینترفیس مورد نظر را روشن می‌کنیم.

در بقیه‌ی روترها به صورت زیر، دستورات را وارد کنید:

وارد روتر R2 شوید و دستورات زیر را وارد کنید:

```
R2(config)#ipv6 unicast-routing
R2(config)#ipv6 router ospf 100
R2(config-rtr)#router-id 150.1.2.2
R2(config-rtr)#int f0/0
```

R2(config-if)**#ipv6 address 2011:1111:12::2/64**
R2(config-if)**#ipv6 ospf 100 area 2**
R2(config-if)**#no sh**
R2(config-if)**#int f0/1**
R2(config-if)**#ipv6 address 2011:1111:23::1/64**
R2(config-if)**#ipv6 ospf 100 area**
R2(config-if)**#ipv6 ospf 100 area 0**
R2(config-if)**#no sh**

وارد روتر R3 شوید و دستورات زیر را وارد کنید:

R3(config)**#ipv6 unicast-routing**
R3(config)**#ipv6 router ospf 100**
R3(config-rtr)**#router-id 150.1.3.3**
R3(config-rtr)**#int f0/0**
R3(config-if)**#ipv6 address 2011:1111:23::2/64**
R3(config-if)**#ipv6 ospf 100 area 0**
R3(config-if)**#no sh**
R3(config-if)**#int f0/1**
R3(config-if)**#ipv6 address 2011:1111:34::1/64**
R3(config-if)**#ipv6 ospf 100 area 1**
R3(config-if)**#no sh**

وارد روتر R4 شوید و دستورات زیر را وارد کنید:

R4(config)**#ipv6 unicast-routing**
R4(config)**#ipv6 router ospf 100**
R4(config-rtr)**#router-id 150.1.4.4**
R4(config-rtr)**#int f0/0**
R4(config-if)**#ipv6 address 2011:1111:34::2/64**
R4(config-if)**#ipv6 ospf 100 area 1**
R4(config-if)**#no sh**

کار به اتمام رسیده است. برای مشخص شدن درستی انجام کار، در یکی از روترها، دستور زیر را وارد کنید:

R4(config-if)**#do sh ipv6 route**
IPv6 Routing Table - 5 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
U - Per-user Static route, M - MIPv6
I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2

```
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
       D - EIGRP, EX - EIGRP external
OI  2011:1111:12::/64 [110/3]
     via FE80::20A:F3FF:FEBA:E802, FastEthernet0/0
OI  2011:1111:23::/64 [110/2]
     via FE80::20A:F3FF:FEBA:E802, FastEthernet0/0
C   2011:1111:34::/64 [0/0]
     via ::, FastEthernet0/0
L   2011:1111:34::2/128 [0/0]
     via ::, FastEthernet0/0
L   FF00::/8 [0/0]
     via ::, Null0
```

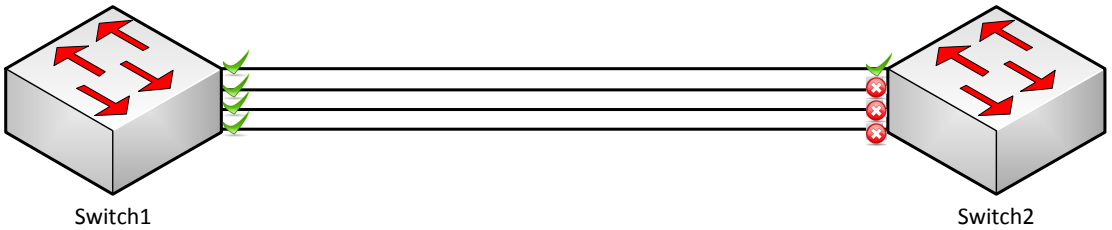
همان‌طور که مشاهده می‌کنید، آدرس‌های شبکه‌های دیگر را از طریق OSPF یاد گرفته است.

امیدوارم متوجه باشید که دستور show ipv6 route، باید در مد Privileged استفاده شود، به خاطر اینکه در مد Global بودیم و برای اینکه از آن مد خارج نشویم، در اول دستور، **do** قرار دادیم، البته این موضوع را قبلاً گوشزد کرده بودیم.

کار با EtherChannel:

شما مدیر یک شبکه‌ی بسیار بزرگ هستید و از کار افتادن شبکه، حتی برای چند لحظه هم برای شما مشکل‌ساز خواهد بود، برای همین شما باید از روش‌هایی استفاده کنید تا در زمانی که یک مشکل برای یک کابل ایجاد شود، کل شبکه از رده خارج نشود.

برای اتصال 2 سوئیچ به هم از چند خط استفاده کنید که اگر یکی یا دو تا از این خط‌ها از کار افتاد، سوئیچ به کار خود روی خط‌های دیگر ادامه دهد؛ برای این کار از EtherChannel استفاده کنید، برای انجام این کار دو سوئیچ به لیست اضافه کنید و 4 کابل را به این سوئیچ‌ها، مانند شکل زیر متصل کنید:



همان‌طور که در شکل مشاهده می‌کنید، 4 کابل به هر دو سوئیچ متصل شده است، اما به خاطر ایجاد Loop، الگوریتم STP فعال‌شده و فقط از یک کابل برای ارتباط با سوئیچ روبرو استفاده کرده است. برای حل چنین مشکلی باید به الگوریتم STP بگوییم که این 4 کابل را به صورت یک کابل مشاهده کند، لذا از EtherChannel استفاده می‌کنیم.

Etherchannel با ایجاد گروه از پورت‌های مورد نظر باعث می‌شود که چند پورت به صورت یک پورت نمایش داده شود. با این کار باعث ایجاد Redundancy در سوئیچ شده و با قطع شدن یکی از کابل‌ها سوئیچ به کار خود ادامه می‌دهد. این نکته را هم توجه داشته باشید که Etherchannel روی روترها و سرورها هم کارایی دارد.

برای ایجاد EtherChannel چه کاری باید انجام دهیم؟

- پورت‌ها باید یا به صورت Full Duplex و یا به صورت Half Duplex باشند.
- پورت‌ها باید یک نوع داشته باشند، یعنی همگی Fast Ethernet باشند.
- پورت‌ها از سرعت یکسانی برخوردار باشند.
- همگی عضو یک VlAN باشند.
- همگی Trunk باشند که در صورت Trunk بودن، باید در یک Native VLAN قرار داشته باشند.

پروتکل‌های EtherChannel:

برای ارتباط دو سوئیچ به روش EtherChannel، باید پروتکل‌های مربوط به آن را معرفی کنیم تا دو سوئیچ بتوانند باهم صحبت کنند.

PAgP *(Port Aggregation Protocol)*:

پروتکل PAgP که از ساخته‌های سیسکو است، برای ارتباط دو سوئیچ که EtherChannel روی آن‌ها اجرا شده است، به کار می‌رود. این پروتکل به دو صورت تنظیم می‌شود؛ اگر به صورت Desirable روی سوئیچ اجرا شود به سوئیچ‌های مقابل خود، تقاضای ایجاد Etherchannel می‌دهد، البته به صورت پیش‌فرض بر روی Auto قرار دارد.

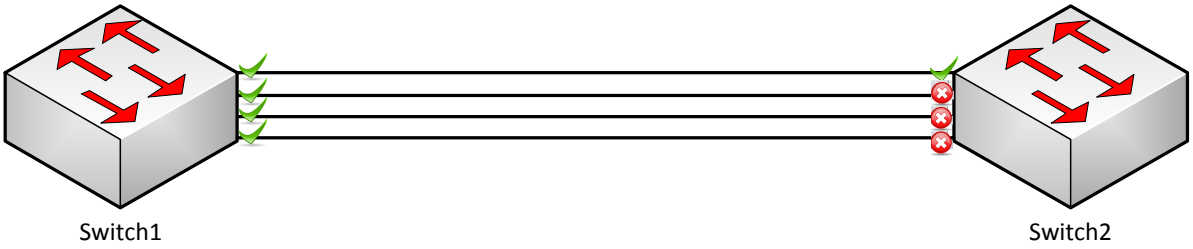
LACP (Link Aggregation Control Protocol):

پروتکل LACP می‌تواند 16 پورت را در یک Etherchannel قرار دهد که در یک زمان از 8 عدد آن استفاده می‌کند و 8 پورت دیگر به حالت Standby می‌رود و هنگامی‌که یکی از آن‌ها با مشکل مواجه شد، این پورت‌ها جایگزین آن‌ها می‌شوند.

این پروتکل به دو صورت تنظیم می‌شود؛ اگر Active باشد به سوئیچ مقابل خود، تقاضای ایجاد Etherchannel را می‌فرستد و اگر Passive باشد، منتظر می‌ماند و فقط گوش می‌کند.

ایجاد EtherChannel با یک مثال:

دو سوئیچ به صفحه اضافه کنید و به صورت زیر به هم متصل کنید:



در مرحله‌ی اول، باید وارد هر 4 پورت به طور هم‌زمان شویم؛ برای این کار وارد سوئیچ 1 می‌شویم و دستور زیر را وارد می‌کنیم:

```
Switch(config)# int range fastEthernet 0/1 - 4
Switch(config-if-range)#
```

با دستور int range fastethernet 0/1 - 4 در یک زمان، وارد 4 پورت شدیم و می‌توانیم این 4 پورت را به صورت هم‌زمان کنترل کنیم. بعد از این کار، نوبت به تعریف Etherchannel می‌رسد. برای تعریف EhterChannel، باید از دستور Channel-Group استفاده کنیم.

```
Switch(config-if-range)#channel-group ?
  <1-48>  Channel group number
```

با واردکردن دستور Channel-group و قرار دادن علامت سؤال به شما تعداد Channel-group که می‌توانید ایجاد کنید را نمایش می‌دهد که در این قسمت، شماره‌ی یک را انتخاب می‌کنیم و در ادامه، دستور Mode را قرار می‌دهیم و بعد، علامت سؤال که به شما انواع روش‌های ایجاد Channel-Group را نمایش می‌دهد.

```
Switch(config-if-range)#channel-group 1 mode ?
  active      Enable LACP unconditionally
  auto        Enable PAgP only if a PAgP device is detected
  desirable   Enable PAgP unconditionally
  on          Enable Etherchannel only
  passive     Enable LACP only if a LACP device is detected
```

در قسمت بالا، انواع مدهای ایجاد channel-Group را مشاهده می‌کنید که مدهای Active و Passive باهم کار می‌کنند و مدهای Auto و Desirable باهم کار می‌کنند و مد On به صورت جدا کار می‌کند.

کار با مدهای Active و passive:

نکته‌ی مهم: قبل از ایجاد مد Active، این نکته را در نظر داشته باشید که زمانی‌که Active فعال شود، شروع به Negotiation یا مذاکره می‌کند که اگر کسی به وی جواب ندهد، Shutdown می‌شود و از کار می‌افتد، پس

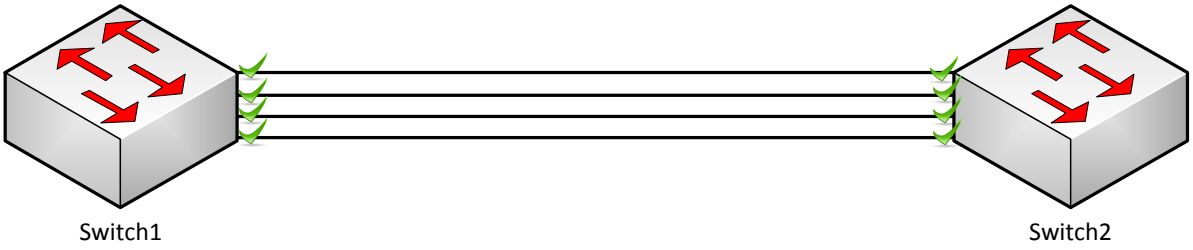
سعی کنید اول از Passive استفاده کنید، چون بچه‌ی ساکتی است و کاری انجام نمی‌دهد و بعدازآن از Active استفاده کنید.

```
SW1(config)# int  rang  f0/1 - 4
SW1(config-if-range)# channel-group 1 mode passive
```

وارد سوئیچ 2 می‌شویم و دستور زیر را وارد می‌کنیم:

```
SW2(config)# int rang fa 0/1 - 4
SW2(config-if-range)# channel-group 1 mode active
```

بعد از این کار، دو سوئیچ بر روی 4 خط کار می‌کنند که در شکل زیر این موضوع را مشاهده می‌کنید.



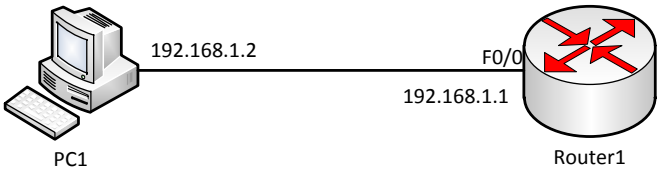
کار با مدهای Auto و desirable:

مانند روش قبلی است که در یکی از سوئیچ‌ها از Auto و در طرف دیگر از desirable استفاده کنید.

کار با SSH:

SSH یک پروتکل رمزنگاری برای ارتباط بین کاربر با سرور است که این ارتباط از نوع راه دور است و ضریب امنیتی آن بسیار بالا است.

باهم یک مثال از این پروتکل را بررسی می‌کنیم. یک روتر 2811 و یک pc را به لیست اضافه کنید و آن‌ها را به مانند شکل زیر متصل کنید.



در مرحله‌ی اول، ip مورد نظر را برای روتر و pc وارد و پورت‌ها را روشن کنید.

وارد روتر شوید و دستورات زیر را وارد کنید.

```
Router(config)# hostname Router1
Router1(config)# username  babajani  secret 123
```

```
Router1(config)# ip domain-name babajani.tk
Router1(config)# crypto key generate rsa
How many bits in the modulus [512]: 1024
Router1(config)#ip ssh version 2
Router1(config)#line vty 0 15
Router1(config-line)#transport input ssh
Router1(config-line)#login local
```

خط به خط دستورات را باهم بررسی می‌کنیم:

در خط اول، نام روتر را با دستور Hostname تغییر دهید.

در خط دوم برای استفاده از SSH، حتماً باید نام کاربری و رمز عبور را تعریف کنیم.

در خط سوم، نام دومین را تعریف می‌کنیم که کاربری که در خط قبل تعریف کردیم، زیرمجموعه‌ی آن می‌شود.

در خط چهارم با یک دستور جدید با نام Crypto key آشنا می‌شویم که به‌عنوان دسته‌کلید شناخته می‌شود. با فعال کردن آن، الگوریتم رمزنگاری rsa فعال می‌شود که رمز عبور را به صورت Hash شده و با امنیت بالا درمی‌آورد.

در خط پنجم، بعد از این‌که دستور crypto key generate rsa را وارد و enter کردید، از شما یک عدد بین 360 تا 2048 سؤال می‌شود که اگر شما یک عدد در رنج بالاتر تعریف کنید، الگوریتم rsa رمز را به صورت پیچیده‌تر درمی‌آورد که در این قسمت از عدد 1024 استفاده کردیم.

در خط ششم، ورژن دوم SSH را فعال کنید، چون این ورژن از نظر پیچیدگی امنیتی در سطح بالاتری قرار دارد و طول کلید آن بسیار بیشتر است و نفوذ به آن را هرکسی نمی‌داند.

بعد از اتمام کار، لازم است وارد پورت VTY شویم و SSH را داخل آن فعال کنیم.

در خط هفتم، وارد Line Vty 0 15 می‌شویم و دستور transport input ssh را وارد می‌کنیم تا SSH فعال شود.

در آخر، فرمان login local را وارد می‌کنیم و تمام.

نحوه‌ی اتصال به روتر از طریق SSH:

برای اتصال از طریق SSH به روتر از دستور زیر استفاده می‌کنیم.

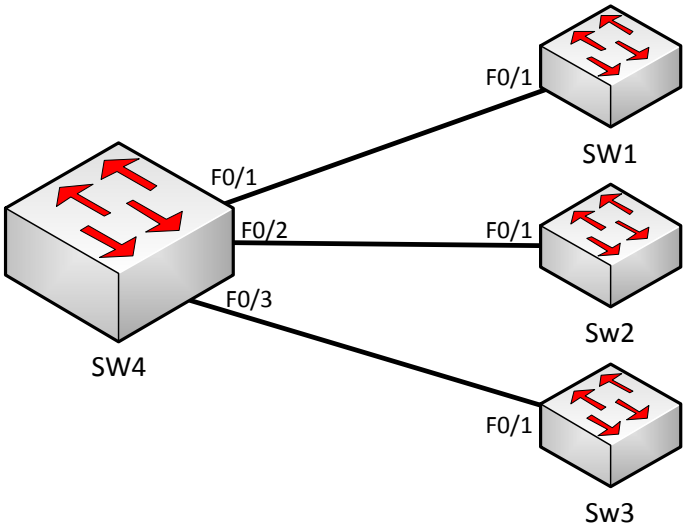
```
ssh - L babajani 192.168.1.1
```

این دستور را در Pc وارد کنید. در این دستور، babajani نام کاربری است که قبلاً در خط دوم تعریف کردیم و آدرس 192.168.1.1 مربوط به روتر مورد نظر است. بعد از تأیید از شما، رمز عبور درخواست می‌شود و بعد از واردکردن رمز، وارد مد User روتر می‌شوید.

دستور CDP (Cisco discovery Protocol):

این دستور که از سری دستورات شرکت سیکو است، دستگاه‌های متصل به یک روتر یا سوئیچ و ... را نمایش می‌دهد، مثلاً شما وارد شبکه‌ای شده‌اید که از ساختار آن خبر ندارید، می‌توانید با استفاده از این دستور دستگاه‌های متصل به دستگاه مورد نظر را بیابید.

با این مثال کاملاً این موضوع را درک می‌کنید.



در این مثال از 4 سوئیچ استفاده می‌کنیم که سوئیچ‌های 1، 2 و 3 به سوئیچ 4 متصل هستند. زمانی برای شما اتفاق می‌افتد که وارد تنظیمات سوئیچ می‌شوید و می‌خواهید بدانید چه دستگاه‌هایی از چه مدلی به این سوئیچ متصل است، برای این کار از دستور زیر استفاده می‌کنیم:

وارد سوئیچ 4 شوید و در مد Privileged، دستور زیر را وارد کنید:

```
SW4# show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone
Device ID    Local Intrfce   Holdtme   Capability   Platform   Port ID
SW1          Fas 0/1         151       S            2950       Fas 0/1
SW3          Fas 0/3         155       S            2950       Fas 0/1
SW2          Fas 0/2         153       S            2950       Fas 0/1
```

همان‌طور که مشاهده می‌کنید با اجرای دستور show cdp neighbors، لیست سوئیچ‌های متصل به این سوئیچ را با ویژگی‌های سوئیچ‌های مربوطه نمایش داد.

در این دستور به ما شماره‌ی پورت، شماره‌ی دستگاه، نوع دستگاه، پورت ورودی به سوئیچ و مقدار زمانی که طول کشید سوئیچ دستگاه‌های متصل به خودش را شناسایی کند را نمایش می‌دهد.

برای اینکه به جزئیات بیشتر در مورد دستگاه‌های متصل شده دست پیدا کنیم از دستور زیر استفاده می‌کنیم:

SW4# **show cdp neighbors detail**

پروتکل CDP هر 60 ثانیه یک‌بار، اطلاعات مربوط را به دستگاه‌های متصل به خود ارسال می‌کند و دستگاه‌هایی که این پیام را دریافت می‌کنند در جدولی که معرفی کردیم، ذخیره می‌کنند.

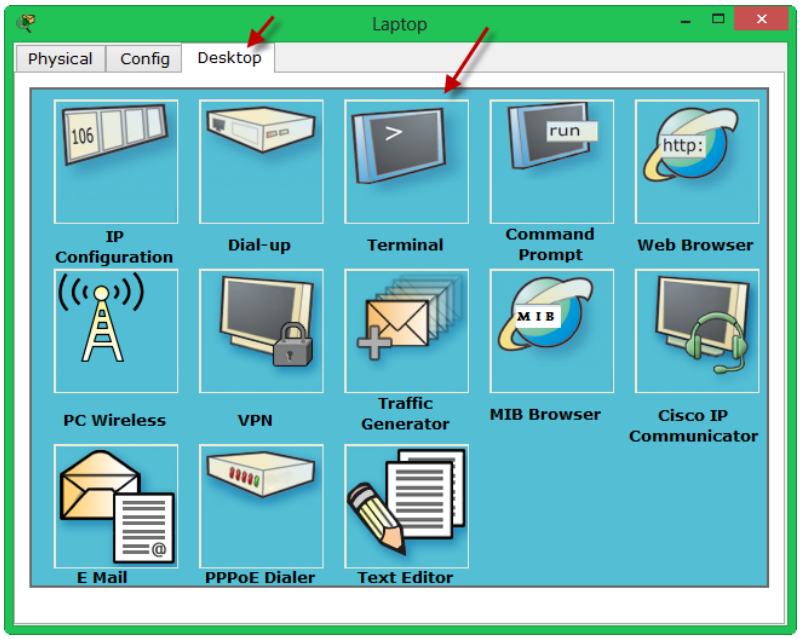
Password Recovery، ریکاوری و یا تغییر رمز عبور:

شما مدیر یک شبکه هستید و روی روتر خود، رمز عبور قرار می‌دهید تا کسی بدون اجازه وارد روتر نشود، اما زمانی پیش می‌آید که شما این رمز را فراموش کردید و در آن موقع است که درگیر این رمز می‌شوید تا رمز مورد نظر روتر را به یاد بیاورید، اما نمی‌شود. برای اینکه این مشکل را حل کنیم، باید تغییراتی را درون تنظیمات روتر انجام دهیم و بتوانیم رمز دیگری را جایگزین رمز جدید کنیم.

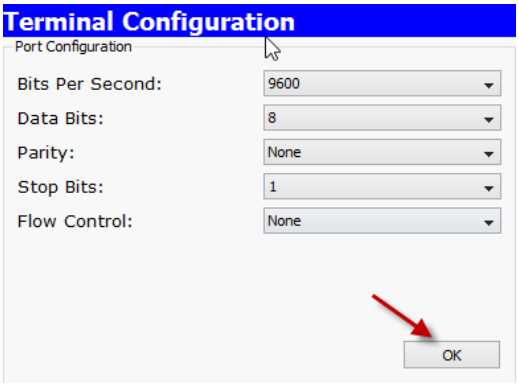
وقتی روتر را روشن می‌کنیم به مرحله‌ی Post رفته و سخت‌افزارهای آن چک می‌شوند. در صورت سالم بودن آن‌ها به مرحله‌ی BootStarp رفته و محل ios را پیدا و اجرا می‌کند که این کار توسط مقادیر Register انجام می‌شود. اگر مقدار رجیستر برابر 0x2102 باشد، اطلاعات ذخیره‌شده روی Nvram را به Ram انتقال می‌دهد و وارد CLI می‌شود، یعنی وقتی شما رمز عبور برای روتر خود قرار می‌دهید، این اطلاعات بر روی nvram ذخیره می‌شود و در زمان اجرای دوباره‌ی روتر از nvram خوانده می‌شود، اما اگر مقدار رجیستر به 0x2142 تغییر کند، دیگر روتر به حافظه‌ی nvram نگاهی نمی‌اندازد و مستقیم وارد Setup Mode می‌شود، پس باید کاری کنیم که روتر در موقع اجرا شدن، شماره‌ی رجیستر 0x2142 را اجرا کند، یعنی باید روتر را گمراه کنیم.

با یک مثال به این موضوع پی می‌برید:

یک روتر 2811 به همراه یک لپ تاپ به صفحه اضافه کنید و از طریق کابل Consol، این دو را به هم متصل کنید.

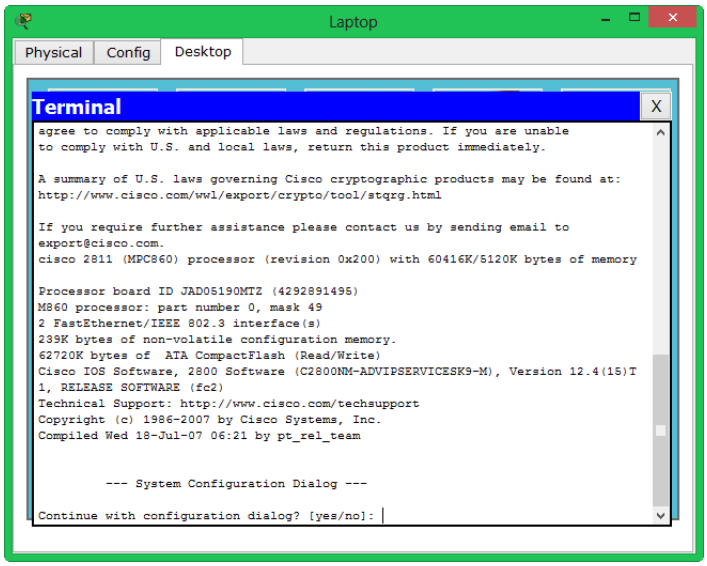


بعد از اتصال این دو به هم، وارد Laptop شده و از تب Desktop، گزینه‌ی Terminal را انتخاب کنید.



در این قسمت، شما باید سرعت انتقال اطلاعات که Bits per Second است را مشخص کنید. در کل به چیزی دست نزنید و بر روی ok کلیک کنید.

همان‌طور که می‌دانید، شما می‌توانید از طریق نرم‌افزارهایی، مانند hyper Terminal و از طریق کابل console به روتر متصل شوید، البته این موضوعات را در فصل‌های اول توضیح دادیم.

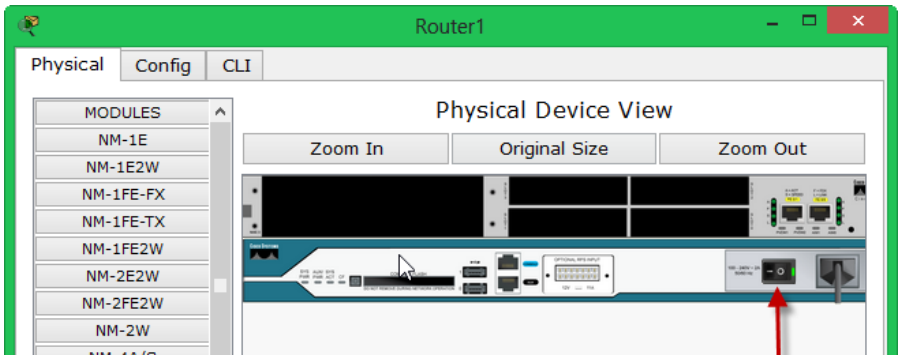


همان‌طور که مشاهده می‌کنید، وارد مد CLI روتر شدیم. برای انجام Password Recovery روی روتر یک رمز عبور قرار می‌دهیم و تنظیمات را ذخیره می‌کنیم و بعد، آن را ریکاوری می‌کنیم.

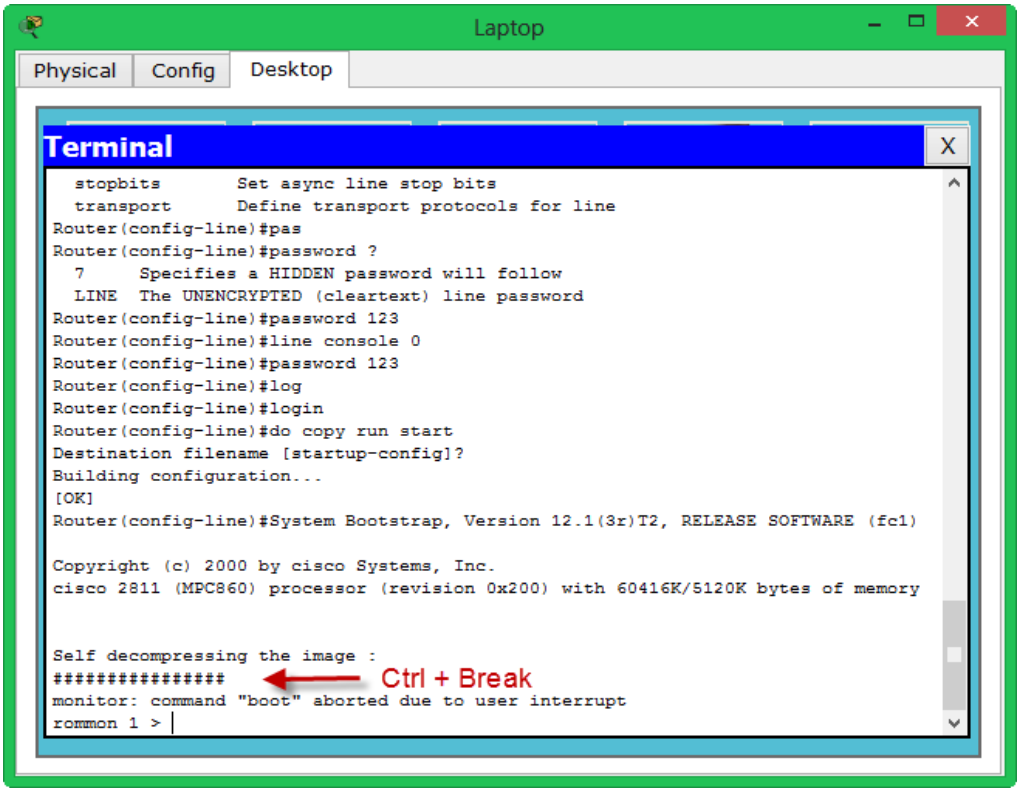
```
Router(config-line)#line console 0
Router(config-line)#password 123
Router(config-line)#login
Router(config-line)#do copy run start
```

همان‌طور که مشاهده می‌کنید، رمز عبور 123 را تعریف و بعدازآن اطلاعات را از Ram به Nvram انتقال دادیم.

در این لحظه باید روتر را خاموش و دوباره روشن کنید و در زمان بالا آمدن روتر باید در laptop، کلید ترکیبی Ctrl + Break را فشار دهید تا بتوانید وارد مد مانیتورینگ شوید.



در شکل بالا، کلید Power روتر 2811 را مشاهده می‌کنید که در واقعیت هم به همین صورت است. این کلید را بر روی off قرار دهید و دوباره روشن کنید. در زمان روشن شدن، وارد laptop شوید و کلید ترکیبی Ctrl+Break را فشار دهید، مانند شکل زیر:



همان‌طور که مشاهده می‌کنید با فشار دادن همزمان کلید ترکیبی Ctrl + Break، وارد مد Rommon 1 > شدیم. در این قسمت از دستورات زیر استفاده می‌کنیم:

rommon 1 > **confreg 0x2142**
rommon 3 > **reset**

در دستور اول، شماره‌ی رجیستر که 0x2102 بود را به شماره‌ی 0x2142 تغییر دادیم و بعدازآن روتر را Reset کردیم تا دوباره اجرا شود.

بعد از این‌که روتر راه‌اندازی می‌شود و وارد Setup mode می‌شود، باید کارهای زیر را برای تغییر رمز انجام دهید.

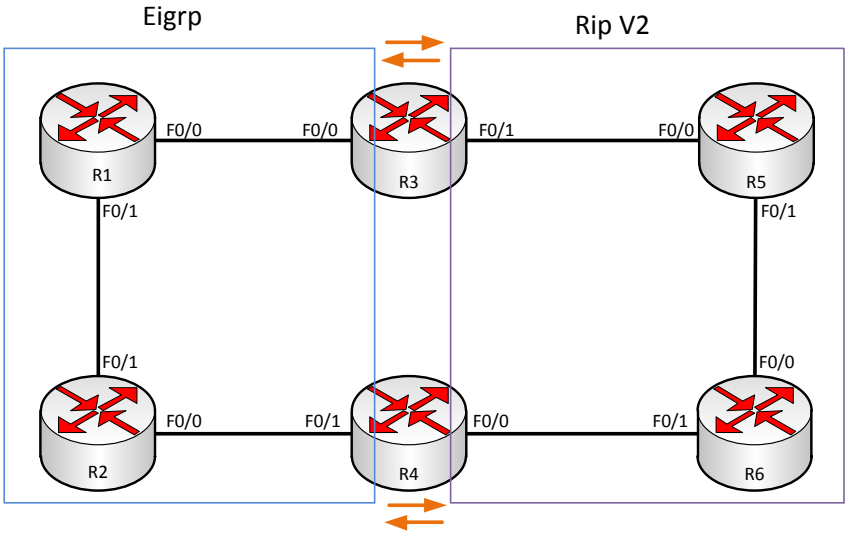
```
Router#copy startup-config running-config
Router#conf t
Router(config)#enable secret 1234
Router(config)#config-register 0x2102
Router(config)#exit
Router#copy run start
```

در مرحله‌ی اول با دستور **copy startup-config running-config**، اطلاعات موجود بر روی Nvram را روی ram کپی می‌کنیم. بعدازآن، وارد مد Global می‌شویم و رمز جدید را جایگزین رمز قبلی می‌کنیم. بعدازآن، شماره‌ی رجیستری را که قبلاً تغییر دادیم با دستور **config-register 0x2102** به حالت اول برمی‌گردانیم و در آخر کار همه‌ی اطلاعات را دوباره در Nvram کپی می‌کنیم و حالا می‌توانید از رمز جدید خود لذت ببرید.

دستور Redistribute:

پروتکل‌های مختلف را باهم کار کردیم و نحوه‌ی راه‌اندازی آن را باهم یاد گرفتیم. زمانی پیش می‌آید که شما در شبکه‌ی خود از دو پروتکل مختلف، مانند Rip و Eigrp استفاده می‌کنید که این دو پروتکل اگر تنظیماتی روی آن‌ها انجام نشود، نمی‌توانند با همدیگر ارتباط برقرار کنند، به این علت از دستور Redistribute برای ترجمه‌ی دو پروتکل و انتقال اطلاعات به همدیگر استفاده شده است.

با یک مثال نحوه‌ی کارکرد این پروتکل را باهم بررسی می‌کنیم.



مثال 1: ارتباط RIP با EIGRP:

در این مثال، در یک طرف از پروتکل Rip Ver 2 استفاده می‌کنیم و در طرف دیگر از EIGRP. بعد از این کار باید کاری روی روترهای مرزی بین این دو پروتکل انجام دهیم که پروتکل‌ها همدیگر را بشناسند.
جدول ip address روترها به صورت زیر است:

Router name	Fa0/0	Fa0/1
R1	1.1.13.1/24	1.1.12.1/24
R2	1.1.12.2/24	1.1.24.2/24
R3	1.1.13.3/24	1.1.25.3/24
R4	1.1.46.4/24	1.1.24.4/24
R5	1.1.35.5/24	1.1.56.5/24
R6	1.1.56.6/24	1.1.46.6/24

همان‌طور که می‌دانید منظور از 24/ یعنی 255.255.255.0 که به صورت CIDR نوشته شده است. بعد از واردکردن IP address ها باید پروتکل‌های مورد نظر را روی روترها راه‌اندازی کنید:
وارد روتر R1 شوید و پروتکل EIGRP را فعال کنید:

```
Router(config)#router eigrp 100
Router(config-router)#no auto-summary
Router(config-router)#network 1.1.13.1 0.0.0.0
Router(config-router)#network 1.1.12.1 0.0.0.0
```

وارد روتر R2 شوید و پروتکل EIGRP را فعال کنید:

```
Router(config)#router eigrp 100
Router(config-router)#no auto-summary
Router(config-router)#network 1.1.12.2 0.0.0.0
Router(config-router)#network 1.1.24.2 0.0.0.0
```

در روترهای R3 و R4 هم باید EIGRP را تعریف کنیم و هم RIP V2:
وارد روتر R3 شوید و دستورات زیر را وارد کنید:

```
Router(config)#router rip
Router(config-router)#version 2
Router(config-router)#no auto-summary
Router(config-router)#network 1.1.35.0
Router(config-router)#passive-interface f0/0
Router(config-router)#exit
Router(config)#router eigrp 100
Router(config-router)#no auto-summary
```

Router(config-router)#**network 1.1.13.3 0.0.0.0**
Router(config-router)#**passive-interface f0/1**

همان‌طور که مشاهده می‌کنید، هر دو پروتکل را روی روتر R3 فعال کردیم. امیدوارم که دستور passive-interface یادتان باشد. این دستور را زمانی استفاده می‌کردیم که یک پروتکل با یک اینترفیس در روتر کاری نداشته و ما نمی‌خواستیم که آپدیت‌ها را روی این اینترفیس ارسال کند.

وارد روتر R4 شوید و دستورات زیر را وارد کنید:

Router(config)#**router rip**
Router(config-router)#**version 2**
Router(config-router)#**no auto-summary**
Router(config-router)#**network 1.1.46.0**
Router(config-router)#**passive-interface f0/1**
Router(config-router)#exit
Router(config)#**router eigrp 100**
Router(config-router)#**no auto-summary**
Router(config-router)#**network 1.1.24.4 0.0.0.0**
Router(config-router)#**passive-interface f0/0**

وارد روتر R5 شوید و پروتکل RIP V2را فعال کنید:

Router(config)#**router rip**
Router(config-router)#**ver 2**
Router(config-router)#**no auto-summary**
Router(config-router)#**network 1.1.35.0**
Router(config-router)#**network 1.1.56.0**

وارد روتر R6 شوید و پروتکل RIP V2 را فعال کنید:

Router(config)#**router rip**
Router(config-router)#**version 2**
Router(config-router)#**no auto-summary**
Router(config-router)#**network 1.1.46.0**
Router(config-router)#**network 1.1.56.0**

بعد از اتمام کار، وارد روتر R1 شوید و دستور زیر را وارد کنید:

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

Gateway of last resort is not set

1.0.0.0/24 is subnetted, 3 subnets
C 1.1.12.0 is directly connected, FastEthernet0/1

C 1.1.13.0 is directly connected, FastEthernet0/0
D 1.1.24.0 [90/30720] via 1.1.12.2, 00:22:04, FastEthernet0/1

همان‌طور که مشاهده می‌کنید، روتر R1 فقط شبکه‌ی 1.1.24.0 را از طریق پروتکل Eigrp شناسایی کرده و از بقیه‌ی شبکه‌ها خبر ندارد. برای حل این مشکل باید عملیات Redistribute را روی روترهای مرزی بین دو پروتکل انجام دهیم تا اطلاعات پروتکل‌ها به داخل هم انتقال داده شود. در واقع این ابزار، کار ترجمه را انجام می‌دهد.

وارد روتر R3 شوید و دستورات زیر را وارد کنید:

Router(config-router)#**router rip**
Router(config-router)# **redistribute eigrp 100 metric 1**

در اول کار، وارد پروتکل مورد نظر می‌شویم و بعد با دستور Redistribute به این پروتکل می‌گوییم که پروتکل Eigrp با شماره‌ی 100 را به صورت Metric 1 وارد شبکه کند. شماره‌ی متریک را می‌توانید بین 0 تا 16 وارد کنید، بستگی به خودتان دارد؛ هر چه کمتر، بهتر.

بعد از وارد شدن به پروتکل rip و فعال کردن redistribute باید وارد پروتکل 100 eigrp شویم و داخل آن بگوییم که این redistribute را برای پروتکل rip فعال کند.

Router(config)#**router eigrp 100**
Router(config-router)#**redistribute rip metric 1 1 1 1 1**

همان‌طور که مشاهده می‌کنید، وارد 100 eigrp شدیم و با دستور redistribute rip metric 1 1 1 1 1، پروتکل rip را وارد پروتکل eigrp کردیم. اگر به دستور توجه کنید از 5 عدد یک پشت سر هم استفاده کردیم که شما هم می‌توانید از اعداد دیگری استفاده کنید، البته رنج اعداد را با وارد کردن علامت سؤال مشاهده خواهید کرد. هر عددی را وارد کنید، زیاد تأثیری در کار این پروتکل ندارد، پس سعی کنید همیشه از این 5 عدد یک استفاده کنید. در زیر، جدول مربوط به هر یک از عددها را مشاهده می‌کنید که مشخص می‌شود مربوط به چه چیزی است.

گزینه‌ی اول	Bandwidth	<1-4294967295>
گزینه‌ی دوم	EIGRP delay metric	<0-4294967295>
گزینه‌ی سوم	EIGRP reliability metric	<0-255>
گزینه‌ی چهارم	EIGRP Effective bandwidth metric	<1-255>
گزینه‌ی پنجم	EIGRP MTU of the path	<1-65535>

وارد روتر R4 شوید و این دستورات را تکرار کنید:

Router(config)#**router rip**

Router(config-router)#**redistribute eigrp 100 metric 1**
Router(config-router)#**router eigrp 100**
Router(config-router)#**redistribute rip metric 1 1 1 1 1**

در این لحظه و بعد از اتمام کار، همه‌ی روترها همدیگر را شناسایی کردند. برای مشاهده‌ی این موضوع در روتر R6، دستور زیر را وارد کنید:

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

Gateway of last resort is not set

1.0.0.0/24 is subnetted, 6 subnets
R 1.1.12.0 [120/1] via 1.1.46.4, 00:00:13, FastEthernet0/1
R 1.1.13.0 [120/1] via 1.1.46.4, 00:00:13, FastEthernet0/1
R 1.1.24.0 [120/1] via 1.1.46.4, 00:00:13, FastEthernet0/1
R 1.1.35.0 [120/1] via 1.1.56.5, 00:00:22, FastEthernet0/0
C 1.1.46.0 is directly connected, FastEthernet0/1
C 1.1.56.0 is directly connected, FastEthernet0/0

همان‌طور که مشاهده می‌کنید با واردکردن دستور show ip route، تمام آدرس‌هایی که مربوط به روترها است را شناسایی کرده است و می‌تواند با همه‌ی آدرس‌ها ارتباط داشته باشد. این موضوع را در روتر R2 هم تست می‌کنیم:

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

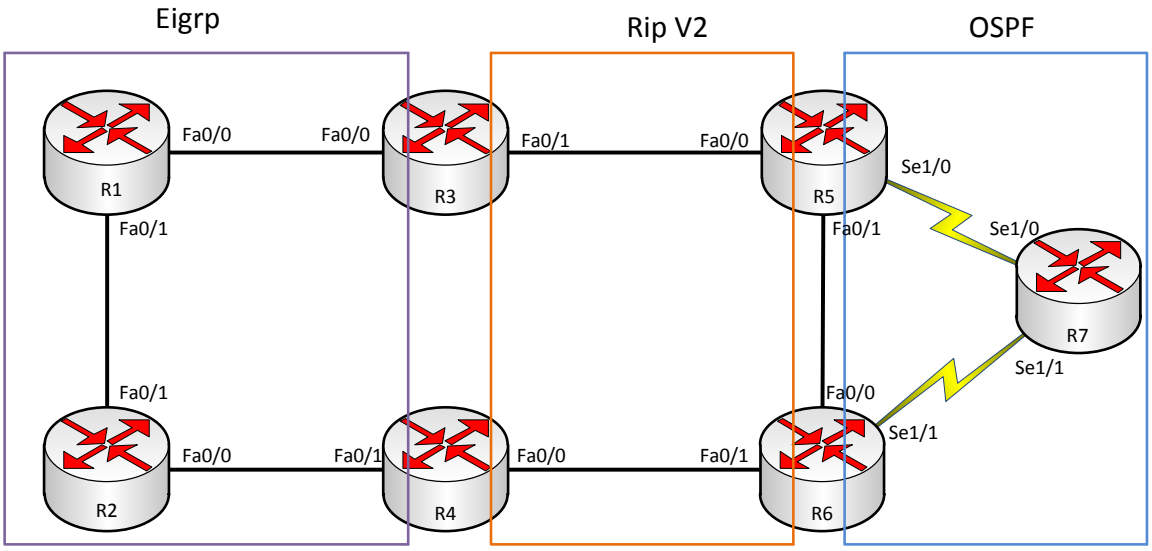
Gateway of last resort is not set

1.0.0.0/24 is subnetted, 6 subnets
C 1.1.12.0 is directly connected, FastEthernet0/1
D 1.1.13.0 [90/30720] via 1.1.12.1, 00:47:07, FastEthernet0/1
C 1.1.24.0 is directly connected, FastEthernet0/0
D EX 1.1.35.0 [170/2560002816] via 1.1.24.4, 00:05:02, FastEthernet0/0
D EX 1.1.46.0 [170/2560002816] via 1.1.24.4, 00:05:02, FastEthernet0/0
D EX 1.1.56.0 [170/2560002816] via 1.1.24.4, 00:05:02, FastEthern

همان‌طور که در صفحه قبل مشاهده کردید، پروتکل Eigrp در جدول روتینگ خود، آدرس‌هایی را که از پروتکل Rip دریافت کرده به صورت DEX نمایش داده است که Ex، مخفف کلمه‌ی EIGRP external است، یعنی - روتینگ‌هایی که از بیرون، از این پروتکل وارد شده است.

ترکیب پروتکل‌های OSPF و EIGRP و RIP V2 با همدیگر:

به شکل قبلی یک قسمت دیگر اضافه می‌کنیم و پروتکل OSPF را روی آن راه‌اندازی می‌کنیم.



جدول آدرس‌های ip به صورت زیر تغییر می‌کند:

Router name	Fa0/0	Fa0/1	Se1/0	Se1/1	Loopback 0
R1	1.1.13.1/24	1.1.12.1/24	-----	-----	
R2	1.1.12.2/24	1.1.24.2/24	-----	-----	
R3	1.1.13.3/24	1.1.35.3/24	-----	-----	
R4	1.1.46.4/24	1.1.24.4/24	-----	-----	
R5	1.1.35.5/24	1.1.56.5/24	1.1.57.5/24	-----	150.1.5.5/24
R6	1.1.56.6/24	1.1.46.6/24	-----	1.1.67.6/24	150.1.6.6/24
R7	-----	-----	1.1.57.7/24	1.1.67.7/24	150.1.7.7/24

بعد از واردکردن ip address، وارد روتر می‌شویم و پروتکل ospf را راه‌اندازی می‌کنیم.

وارد روتر R5 می‌شویم و دستور زیر را وارد می‌کنیم:

Router(config)#**router ospf 1**

```
Router(config-router)# router-id  150.1.5.5
Router(config-router)#network 1.1.57.5 0.0.0.0 area 0
```

وارد روتر R6 می‌شویم و دستور زیر را وارد می‌کنیم:

```
Router(config)# router ospf 1
Router(config-router)# router-id  150.1.6.6
Router(config-router)# network  1.1.67.6 0.0.0.0  area 0
```

وارد روتر R6 می‌شویم و دستور زیر را وارد می‌کنیم:

```
Router(config)#router ospf 1
Router(config-router)#router-id 150.1.7.7
Router(config-router)#network 1.1.57.7 0.0.0.0 area 0
Router(config-router)#network 1.1.67.7 0.0.0.0 area 0
```

بعد از تعریف پروتکل مورد نظر، وارد روترهای R5 و R6 می‌شویم و دستور Redisribut را در هر دو پروتکل مانند قبل فعال می‌کنیم:

وارد روتر R5 می‌شویم و دستور زیر را وارد می‌کنیم:

```
Router(config)#router ospf 1
Router(config-router)#redistribute rip subnets
```

با دستور **redistribute rip subnets**، شبکه‌های پروتکل rip وارد پروتکل ospf می‌شوند. اگر به دستور توجه کنید در آخر آن از Subnet استفاده کردیم و این به خاطر این است که وقتی شبکه‌های rip وارد ospf می‌شوند به صورت ClassFull وارد نشوند و اگر این گزینه را بردارید به صورت ClassFull وارد OSPF می‌شوند.

وارد پروتکل OSPF 1 می‌شویم و RIP را وارد می‌کنیم:

```
Router(config-router)#router rip
Router(config-router)#redistribute ospf 1 metric 1
```

وارد روتر R6 می‌شویم و دستور زیر را وارد می‌کنیم:

```
Router(config)#router ospf 1
Router(config-router)#redistribute rip subnets
Router(config-router)#router rip
Router(config-router)#redistribute ospf 1 metric 1
```

برای اینکه متوجه شویم روتر اطلاعات روترهای دیگر را دریافت کردند، وارد روتر R2 می‌شویم و از دستور زیر استفاده می‌کنیم:

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

Gateway of last resort is not set

     1.0.0.0/24 is subnetted, 8 subnets
C       1.1.12.0 is directly connected, FastEthernet0/1
D       1.1.13.0 [90/30720] via 1.1.12.1, 02:31:48, FastEthernet0/1
C       1.1.24.0 is directly connected, FastEthernet0/0
D EX    1.1.35.0 [170/2560005376] via 1.1.12.1, 00:00:38, FastEthernet0/1
D EX    1.1.46.0 [170/2560002816] via 1.1.24.4, 01:49:43, FastEthernet0/0
D EX    1.1.56.0 [170/2560002816] via 1.1.24.4, 01:01:56, FastEthernet0/0
D EX    1.1.57.0 [170/2560005376] via 1.1.12.1, 00:00:38, FastEthernet0/1
D EX    1.1.67.0 [170/2560002816] via 1.1.24.4, 01:01:56, FastEthernet0/0
```

همان‌طور که مشاهده می‌کنید، روتری که eigrp روی آن فعال بود، توانسته است از طریق RIP به اطلاعات ospf دست پیدا کند و برعکس.

نکته: اگر در یک شبکه از چند eigrp با as های مختلف استفاده کنید، باید از طریق Redistribute آن‌ها را به هم معرفی کنید، مثلاً اگر در یک شبکه، EIGRP 100 و EIGRP 200 داشته باشید، این دو شبکه به هیچ عنوان همدیگر را شناسایی نمی‌کنند، چون از دو منطقه‌ی جدا تشکیل شده‌اند. برای حل این مشکل باید از دستور Redistribute استفاده کنید.

HSRP (Hot Standby Router Protcol):

اگر شما مدیر شبکه هستید، همیشه سعی کنید Redundancy یا اطمینان کار را در شبکه‌ی خود حفظ کنید. این پروتکل که از ساخته‌های شرکت سیسکو است، با عنوان HSRP به شما این قابلیت را می‌دهد که چند روتر را در یک مجموعه قرار دهید و یکی از این روترها را که روتر اصلی است Active Router، یکی دیگر از روترها به عنوان Standby Router و بقیه‌ی روترها را به عنوان آماده به کار در نظر می‌گیریم. این روترها به عنوان Defualt Gateway کلاینت‌ها در نظر گرفته می‌شوند. اگر زمانی روتری از کار بیفتد، روتر دیگر جایگزین آن می‌شود و باعث ادامه‌ی کار شبکه می‌شود. پورت مربوط به این پروتکل، UDP 1985 است و از آدرس MultiCast، 224.0.0.2 برای انتقال اطلاعات استفاده می‌کند. شماره‌ی گروه آن از 0 تا 255 قابل تخصیص است.

برای انتخاب روتر اصلی در HSRP از Priority استفاده می‌کنند که عددی بین 255-0 است که البته روی همه‌ی روترها و سوئیچ‌های لایه‌ی 3، 100 است که در صورت برابر بودن Priority، انتخاب روتر Active از روی شماره‌ی ip بزرگ‌تر است.

روترهای Standby، روترهایی هستند که فقط به پیغام‌های روترهای Active که هر 3 ثانیه ارسال می‌شود، گوش دهند و اگر در مدت 10 ثانیه Hello Packet از طرف روتر Active به روتر Standby نرسد، این روتر فرض می‌کند که روتر Active از کار افتاده و خود را به عنوان روتر Active، فعال می‌کند.

زمان Hold برابر 10 ثانیه است.

می‌توانیم با دستور زیر، زمان‌های Hello و Hold را تغییر دهیم:

SW1 (confing – if)#standby 1 timers 10 15

در این دستور Hello برابر 10 و Hold برابر 15 است.

زمانی که روی یک روتر پروتکل HSRP را فعال می‌کنیم در چند حالت قرار می‌گیرد:

1- Disable
2- Init
3- Listen
4- Speak
5- Standby
6- Active

هرگاه در یک شبکه، یک روتر به‌عنوان روتر Active شناخته شود و شما روتر دیگری به شبکه با تنظیمات و Priority بهتر متصل کنید، این روتر به‌عنوان Active انتخاب نمی‌شود، اما با دستور زیر می‌توان روتر جدید را به عنوان Active روتر انتخاب کرد.

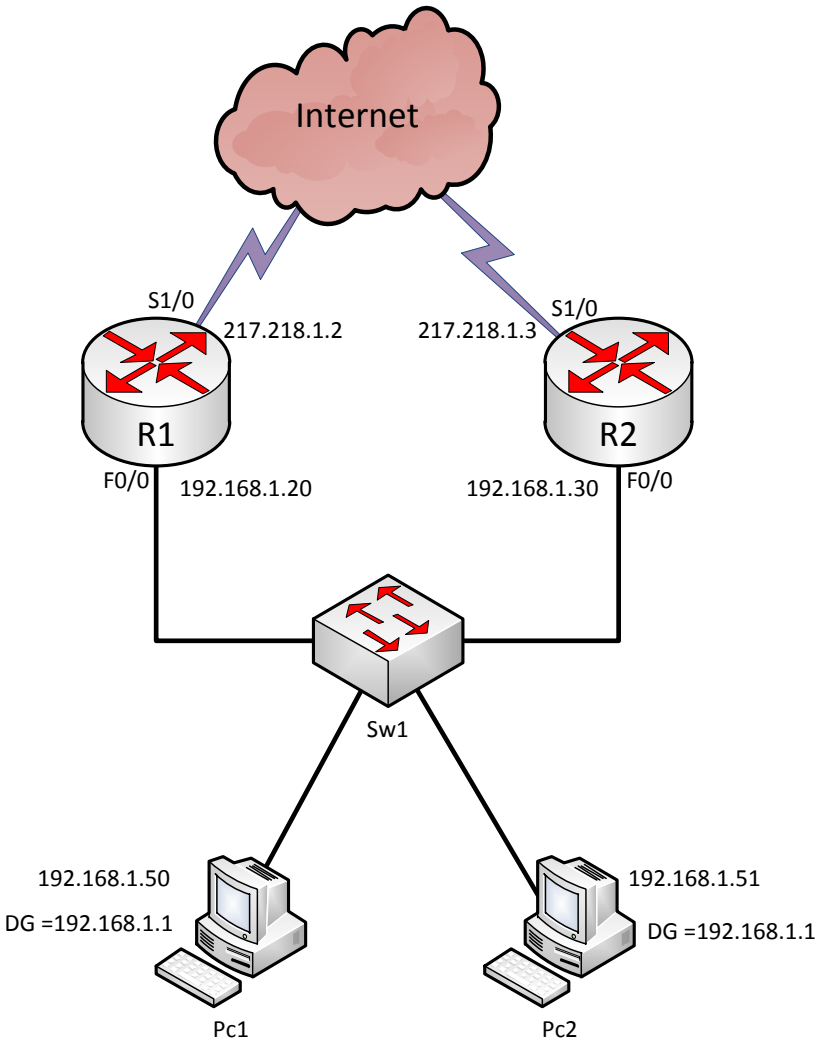
```
R1(config-if)# Standby 1 Preempt
```

این دستور، Active بودن یک روتر را از آن پس می‌گیرد و به روتر دیگر می‌دهد که Priority بهتری دارد.

مثال HSRP:

در این مثال، کلاینت‌ها از طریق یک سوئیچ و بعدازآن از طریق روتر وارد اینترنت می‌شوند. در این سناریو دو روتر که به سوئیچ متصل هستند، نقش HSRP را بازی می‌کنند و یکی از روترها به عنوان Active و روتر دیگر به عنوان standby در نظر گرفته می‌شود و Defualt Gateway را برای کلاینت‌ها مشخص می‌کنند که اگر زمانی یک روتر از کار افتاد روتر دیگر جایگزین می‌شود.

در packet Tracer، شکل زیر را ایجاد کنید و کابل‌های مورد نظر را به هم متصل کنید.



وارد روتر R1 می‌شویم و تنظیمات مربوط به HDLC را انجام می‌دهیم:

```
R1(config)#int f0/0
R1(config-if)#ip add 192.168.1.20 255.255.255.0
R1(config-if)#standby 1 ip 192.168.1.1
R1(config-if)#standby 1 priority 150
R1(config-if)#standby 1 preempt
R1(config-if)#standby 1 track fastEthernet 0/0
```

در دستور اول وارد اینترفیس F0/0 می‌شویم. یک آدرس برای این اینترفیس در نظر می‌گیریم. بعدازآن باید HDLC را با دستور Standby فعال کنیم. برای این کار، دستور standby 1 ip 192.168.1.1 را وارد می‌کنیم شماره‌ی 1 نام گروه مورد نظر است و آدرس 192.168.1.1 هم آدرس DG(Defualt Gateway) است، یعنی روتر روی این

آدرس، نقش Defult Gateway را بازی می‌کند. برای این‌که این روتر به‌عنوان روتر اصلی در نظر گرفته شود، باید مقدار priority آن که به صورت پیش‌فرض 100 است را به 150 تغییر دهیم. بعد از تغییر priority به روتر با دستور Standby 1 preempt می‌گوییم که سریع‌تر به حالت Active سوئیچ کند، مثلاً اگر شما دو روتر داشته باشید، اولی Active باشد و روتر دیگر، standby. اگر Priority روتری که standby است را به 150 تغییر دهیم، در حالت کلی باید به روتر Active تغییر کند، اما این کار انجام نمی‌شود. برای حل این مشکل از دستور preempt استفاده می‌کنیم تا حالت Active را از روتر اولی بگیرد و به روتر دومی دهد.

در دستور standby 1 track fastEthernet 0/0 در یک فاصله‌ی زمانی مشخص، پورت fastEthernet 0/0 توسط Track، Ping می‌شود تا از فعال بودن آن با خبر شود. به محض این‌که لینک مورد نظر down شد. روتر Active تغییر می‌کند و به روتر دیگر داده می‌شود.

در روتر R2 هم، مانند روتر قبلی همین کار را انجام می‌دهیم:

```
Router(config)#int f0/0
Router(config-if)#ip add 192.168.1.30 255.255.255.0
Router(config-if)#no sh
Router(config-if)#standby 1 ip 192.168.1.1
Router(config-if)#standby 1 preempt
Router(config-if)#standby 1 track fastEthernet 0/0
```

در این روتر هم، مانند روتر R1 دستورات را وارد کردیم. در این روتر نیز از DG، 192.168.1.1 استفاده کردیم و از دستور Preempt هم برای تغییر وضعیت سریع استفاده کردیم. در حال حاضر روتر R1 به عنوان Active روتر و روتر R2 به‌عنوان standby روتر است. زمانی که روتر R1 از شبکه خارج شود، روتر R2 جایگزین می‌شود. به این حالت، Redundancy می‌گویند که اطمینان کارایی شبکه را بالا می‌برد.

در HSRP می‌توانیم روش‌های امنیتی را به کار ببریم که کسی بدون اجازه وارد این شبکه نشود و خودش را به عنوان یک روتر HSRP معرفی نکند.

دو مدل Authentication در HSRP وجود دارد.

1- Plain Text:

در این روش، امنیت از طریق یک کلمه که می‌تواند حداکثر 8 کاراکتر باشد، صورت گیرد:

Sw1 (Config-if)# Standby **1** Authentication **babajani**

در هر دو روتر باید این دستور را وارد کنید که در اینجا، کلمه‌ی babajani به‌عنوان رمز عبور برای هر دو روتر است و اگر در هر روتر رمز برقرار باشد، ارتباط برقرار می‌شود.

2- MD5:

در این روش که از طریق Hash کردن اطلاعات صورت می‌گیرد، خیلی قوی‌تر و بهتر از روش قبلی است.

Sw1 (Config-if)# Standby **1** Authentication md5 key-string **saman**

این نکته را هم در نظر داشته باشید که دستورات رمزنگاری روی نرم‌افزار Packet Tracer، تعریف نشده و شما باید در نرم‌افزارهای دیگر، مانند GNS3 و یا IOU که در زیر آن‌ها را بررسی خواهیم کردیم، اجرا کنید.

از HSRP می‌توانیم برای Load balancing هم استفاده کنیم تا بار کاری بین روترها تقسیم شود، یعنی برای یک روتر، یک DG مشخص و برای روتر دیگر، DG دیگر و هرکدام از این روترها به‌عنوان Active روتر در نظر گرفته می‌شوند؛ مثلاً اگر در شبکه‌ی خود 6 کلاینت دارید، می‌توانید 3 کلاینت را به R1 متصل کنید و 3 کلاینت دیگر را به R2 متصل کنید تا بار شبکه، بین روترها تقسیم شود.

نکته: اصولاً HSRP روی سوئیچ‌های لایه‌ی 3 اجرا می‌شود و در بعضی از روترها تعریف نشده است.

با دستور show standby می‌توانید اطلاعات مربوط به HSRP روی روتر مورد نظر را مشاهده کنید:

```
R1# show standby
FastEthernet0/0 - Group 1 (version 2)
  State is Active
    4 state changes, last state change 00:18:45
  Virtual IP address is 192.168.1.1
  Active virtual MAC address is 0000.0C9F.F001
    Local virtual MAC address is 0000.0C9F.F001 (v2 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 1.066 secs
  Preemption enabled
  Active router is local
  Standby router is 192.168.1.30, priority 150 (expires in 0 sec)
  Priority 150 (configured 150)
  Group name is hsrp-Fa0/0-1 (default)
```

با دستور show Standby Brife، می‌توانید اطلاعات سریع در مورد Active و Standby بودن روتر را به دست بیاورید:

```
R1#show standby brief
                     P indicates configured to preempt.
                     |
Interface   Grp   Pri P   State   Active          Standby         Virtual IP
Fa0/0       1     150 P   Active  local       192.168.1.30    192.168.1.1
```

GLBP (Gateway Load Balancing Protocol):

این پروتکل، نسخه‌ی بهبودیافته‌ی پروتکل HSRP است که توسط شرکت سیسکو ارائه شده است و برای Load balancing استفاده می‌شود. کار اصلی این پروتکل به این صورت است که چند روتر در یک Subnet قرار دارند و باید مانند قبل، روی یک IP نقش Defualt Gateway را بازی کنند. روتری که Priority آن بالاتر باشد، می‌شود Active Forwarder، کار این روتر این است که اگر کلاینتی درخواستی به سمت این روتر ارسال کند، این روتر Mac address یکی از روترهایی که در همان گروه قرار دارد را برای کلاینت ارسال می‌کند و در دفعه‌ی بعد، Mac روتر دیگر را می‌فرستد که این کار توسط الگوریتم‌های زیر انجام می‌پذیرد:

الگوریتم Round Robin:

به صورت گردشی عمل می‌کند و به صورت پیش‌فرض فعال است.

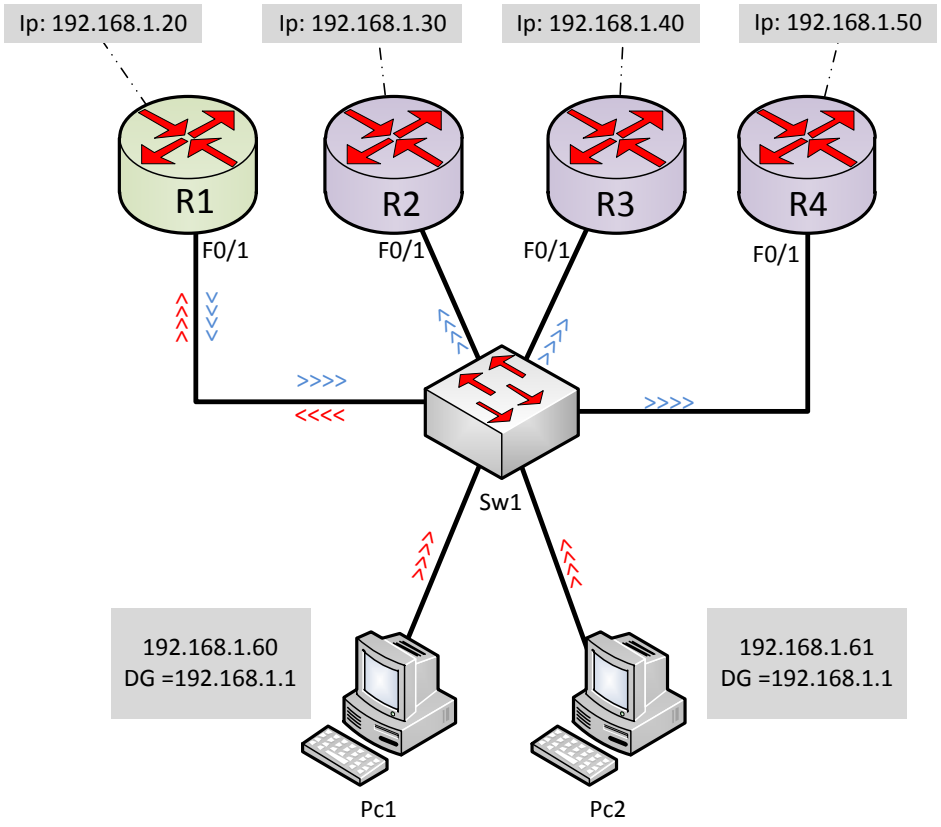
الگوریتم Weighted:

این الگوریتم بار کاری را به صورت مساوی بین روترها تقسیم می‌کند.

الگوریتم Host-Dependent:

در این الگوریتم از طریق access List به روتر می‌گوییم که این کلاینت‌ها از روتر خاصی استفاده کنند.

مثالی از این پروتکل:



در این مثال، روتر R1 به عنوان روتر Active انتخاب می‌شود و بقیه، به عنوان روتر Standby می‌باشند.
وقتی کلاینت درخواستی را می‌فرستند، در مرحله‌ی اول به روتر R1 می‌رسد و بعد، این روتر Mac address یکی از روترهای گروه خود را به کلاینت مورد نظر می‌دهد و به کلاینت بعدی Mac address روتر دیگر را می‌دهد و همین‌طور ادامه خواهد داشت. در صورت غیرفعال شدن روتر اصلی، روتر دیگر در گروه مورد نظر به جای آن قرار می‌گیرد.
وارد روتر R1 شوید و دستورات زیر را وارد کنید:

```
R1(config)#int f0/1
R1(config-if)#ip add 192.168.1.20 255.255.255.0
R1(config-if)#no sh
R1(config-if)#glbp 1 ip 192.168.1.1
R1(config-if)#glbp 1 priority 150
R1(config-if)#glbp 1 preempt
R1(config-if)#glbp 1 authentication text babajani
```

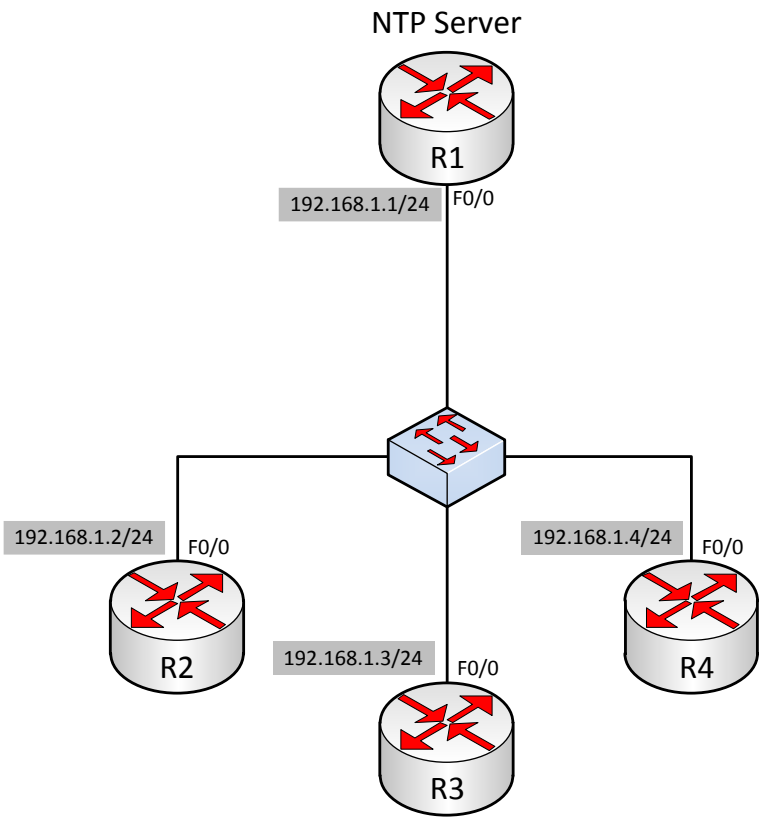
همان‌طور که مشاهده می‌کنید، وارد اینترفیس مورد نظر شدیم و IP address را وارد کردیم و بعدازآن اینترفیس را روشن کردیم. ادامه‌ی کار، مانند HDLC است. در روترهای دیگر هم به همین صورت دستورات را وارد کنید، اما دستور glbp 1 priority 150 را فقط برای همین روتر، یعنی روتر R1 وارد کنید.

VRRP (Virtual Router Redundancy Protocol):

این پروتکل کاملاً شبیه به HSRP است. شماره‌ی گروه در این پروتکل از 0 تا 255 و شماره‌ی Priority از 0 تا 254 است. روتر اصلی به‌عنوان روتر Master در نظر گرفته می‌شود و روترهای فرعی به‌عنوان Backup در نظر گرفته می‌شود. این پروتکل مربوط به سازمان IETF است.
این پروتکل از آدرس 224.0.0.18 استفاده می‌کند و پروتکلی که با آن کار می‌کند، IP Protocol با شماره‌ی پورت 112 است. این پروتکل در هر 1 ثانیه، پیام‌های خود را ارسال می‌کند و دستور Preempt هم به صورت پیش‌فرض بر روی این پروتکل فعال است.
شاید در شبکه‌ی خود از دستگاه‌هایی غیر از دستگاه‌های شرکت سیسکو استفاده کنید که برای Redundancy حتماً باید از این پروتکل استفاده کنید.
دستورات، کاملاً شبیه به HSRP است. فقط به جای قرار دادن کلمه‌ی HSRP، کلمه‌ی VRRP را جایگزین کنید.

:**NTP** (Network Time Protocol)

این پروتکل برای تنظیم تاریخ و ساعت استفاده می‌شود که یکی از کارهای مدیریتی در شبکه است. با یک مثال این پروتکل را بررسی می‌کنیم:



در این مثال، R1 به عنوان سرور NTP در نظر می‌گیریم و به بقیه‌ی روترها می‌گوییم که از روتر R1، تنظیمات ساعت و تاریخ را دریافت کنند.

وارد روتر R1 شوید و دستورات زیر را وارد کنید:

R1#**clock set 10:15:00 22 nov 2013**

R1#configure t
R1#configure terminal
R1(config)#ntp master 1
R1(config)#ntp authentication-key 1 md5 saman 123

در قسمت اول، ساعت و تاریخ روتر را تنظیم کردیم و بعد وارد مد Global شدیم و دستور Ntp Master 1 را وارد کردیم که با این دستور، این روتر را به عنوان روتر سرور برای پروتکل NTP در نظر می‌گیریم. عدد 1 که

در انتهای دستور مشاهده می‌کنید، می‌تواند از 1 تا 15 و برای مشخص کردن Master مورد نظر باشد و بعدازآن، یک کلید امنیتی تعریف می‌کنیم تا کسی بدون اجازه، زیرمجموعه این سرور نشود.

بعد از مشخص کردن سرور NTP، باید وارد روترهای دیگر شویم و روتر R1 را به عنوان روتر NTP به روترهای دیگر معرفی کنیم:

در روترهای R2,R3,R4 دستورات زیر را وارد کنید:

R5(config)#ntp server 192.168.1.1
R5(config)#ntp authentication-key 1 md5 saman 123

با این دستور، روترها تنظیمات ساعت و تاریخ خود را از سرور، یعنی R1 دریافت می‌کنند. برای مشاهده‌ی این موضوع از دستور زیر استفاده می‌کنیم:

R2#show ntp status
Clock is synchronized, stratum 2, reference is 192.168.1.1
nominal freq is 250.0000 Hz, actual freq is 250.0003 Hz, precision is 2**18
reference time is D639AF96.2C66330A (10:25:26.173 UTC Fri Nov 22 2013)
clock offset is 12.7890 msec, root delay is 43.90 msec
root dispersion is 902.04 msec, peer dispersion is 889.22 msec

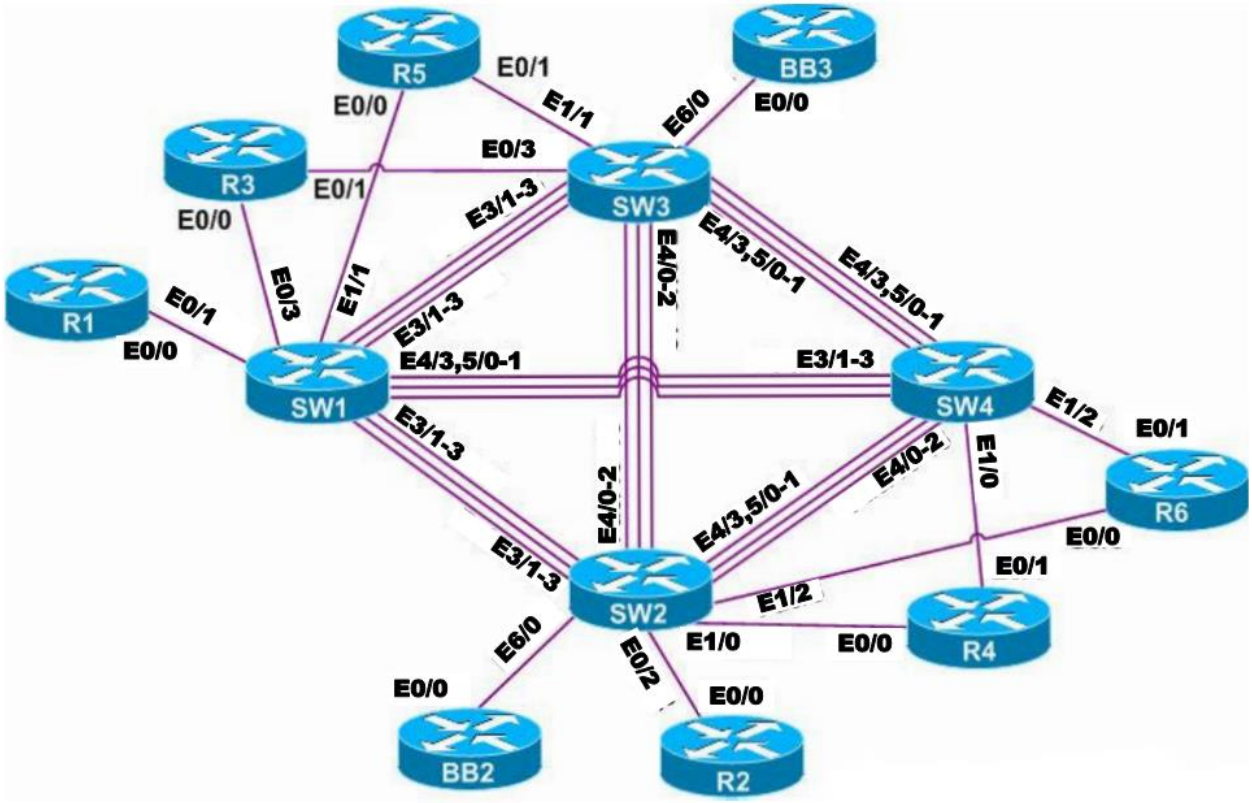
همان‌طور که مشاهده می‌کنید، وارد روتر R2 شدیم و از دستور **show ntp status** استفاده کردیم که به ما تاریخ و ساعت مورد نظر را نمایش داد.

.

آموزش نرم‌افزار IOU:

این نرم‌افزار یکی از نرم‌افزارهای مرکز امتحانات سیسکو است که برای مدرک CCIE و در قسمت اول آن به کار می‌رود. همان‌طور که می‌دانید امتحان CCIE در دو مرحله انجام می‌گیرد که مرحله‌ی اول، بر روی همین نرم‌افزار است و مرحله‌ی دوم روی Rack واقعی انجام می‌گیرد.

این نرم‌افزار دقیقاً بر طبق CCIE Rack ایجاد شده است و از 6 روتر اصلی، 3 روتر BackBone، 4 سوئیچ لایه‌ی 3 تشکیل شده است که شکل آن را در زیر مشاهده می‌کنید:

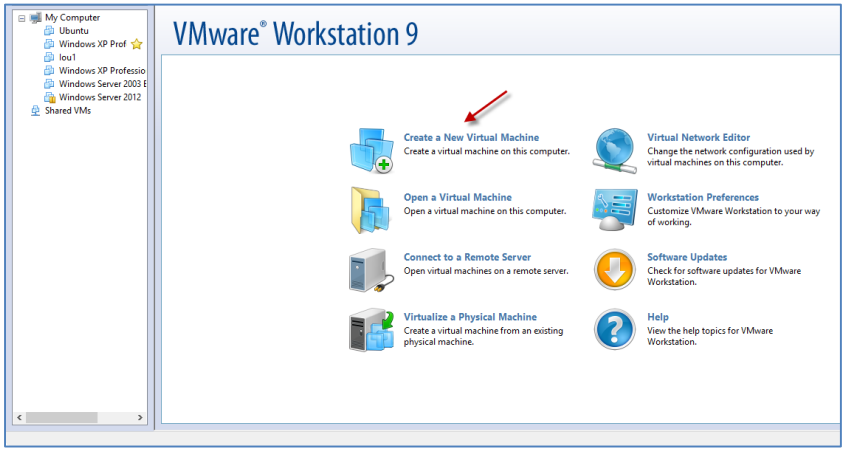


برای راه‌اندازی این نرم‌افزار احتیاج به یک نرم‌افزار مجازی‌سازی داریم تا بتوانیم در ویندوز خود آن را اجرا کنیم. نرم‌افزار IOU از هسته‌ی لینوکس پیروی می‌کند و باید به صورت مجازی روی ویندوز اجرا شود، پس قبل از شروع به کار، نرم‌افزار Vmware 9 یا هر ورژن دیگری که در دسترس دارید را نصب کنید. همان‌طور که می‌دانید این نرم‌افزار برای راه‌اندازی چندین سیستم عامل در کنار هم است و مخصوص کاربران شبکه است.

برای دانلود این نرم‌افزار می‌توانید از لینک زیر استفاده کنید و بعد از دانلود، آن را نصب کنید:

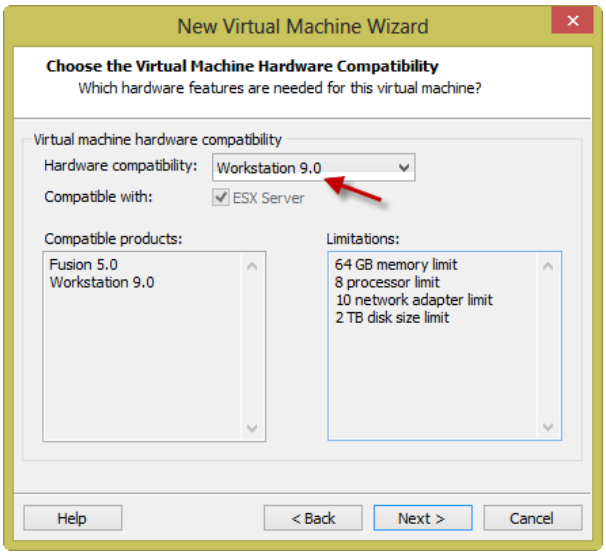
http://dl1.sarzamindownload.com/sdlftpuser/91/06/18/VMware_Workstation_9.exe

نرم‌افزار را اجرا و به شکل زیر توجه کنید.

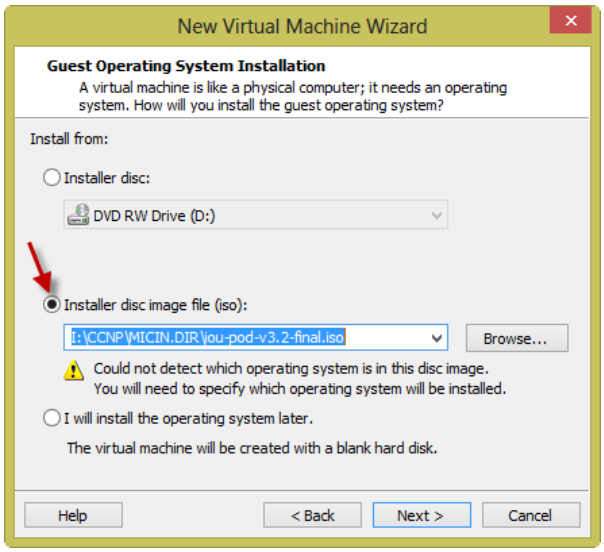


بر روی گزینه‌ی Create New Virtual Machine کلیک کنید تا شکل زیر ظاهر شود:

در این شکل، گزینه‌ی Custom را انتخاب و بر روی Next کلیک کنید.



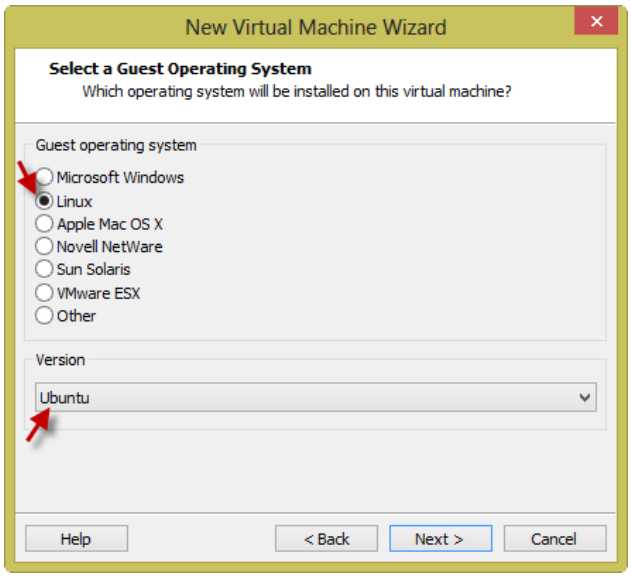
در این شکل، Workstation 9 را انتخاب و بر روی Next کلیک کنید.



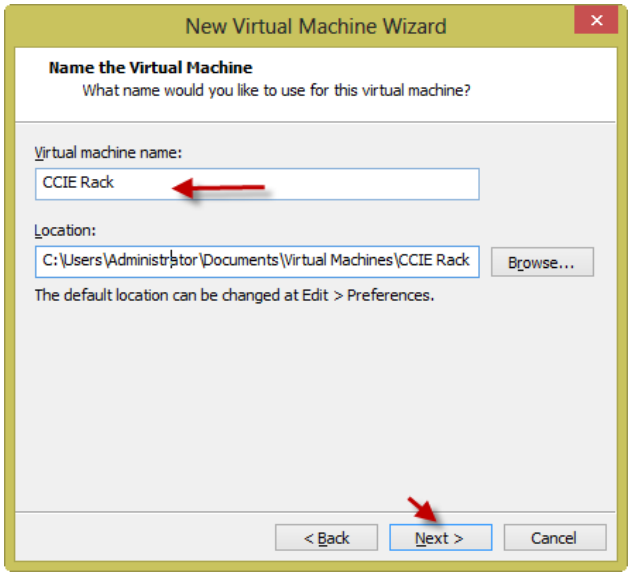
در این قسمت باید IOU را به این نرم‌افزار معرفی کنیم که IOU به صورت فایل فشرده ISO است و از آدرس زیر می‌توانید آن را دانلود کنید:

http://www.4shared.com/file/5CR_MwvA/iou-pod-v32-final.htm

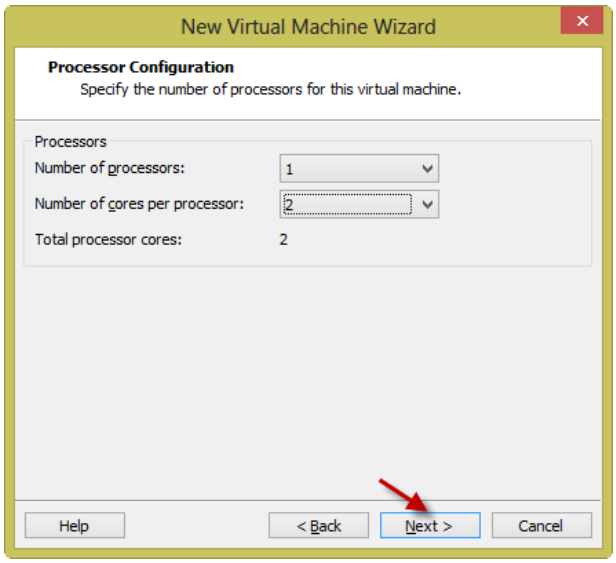
بعد از دانلود، مانند شکل روبرو به نرم‌افزار معرفی کنید و بر روی Next کلیک کنید.



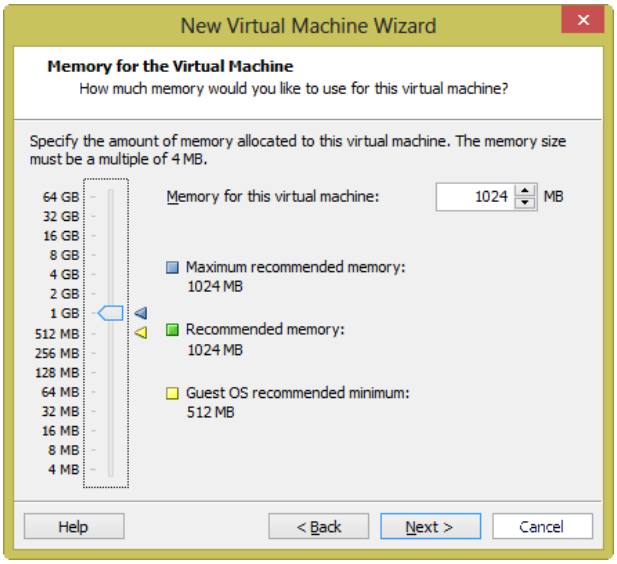
در این قسمت، گزینه‌ی Linux را انتخاب و بر روی Next کلیک کنید.



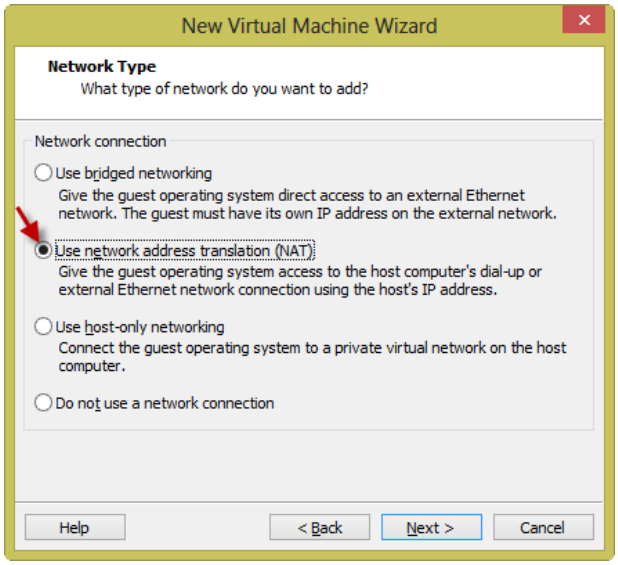
در این قسمت، نام پروژه را وارد کنید. از قسمت Location می‌توانید محل ذخیره‌سازی آن را تعیین کنید. بر روی Next کلیک کنید.



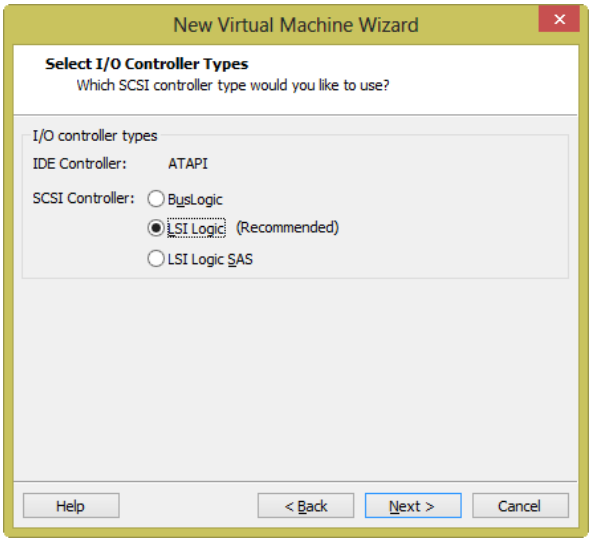
در این شکل، تعداد پردازنده و هسته‌ی آن را مشخص و بر روی Next کلیک کنید.



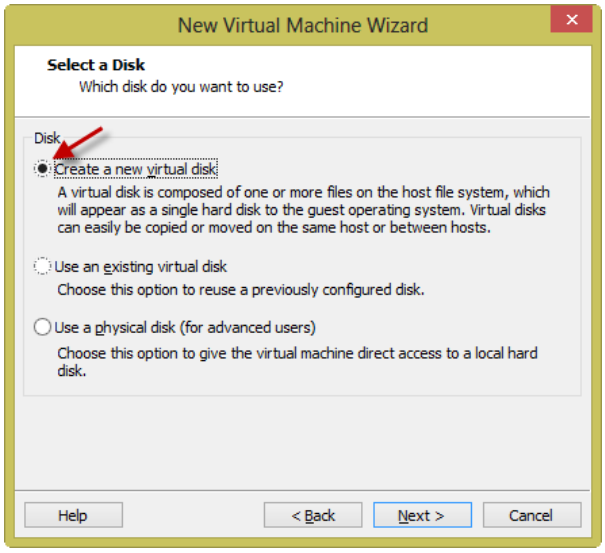
در این قسمت باید حافظه‌ی Ram مورد نظر برای این ماشین مجازی را تعیین کنید. توجه داشته باشید که IOU، احتیاج زیادی به Ram دارد تا بتواند به صورت صحیح کار کند. برای همین سعی کنید از RAM 2GB استفاده کنید. بر روی Next کلیک کنید.



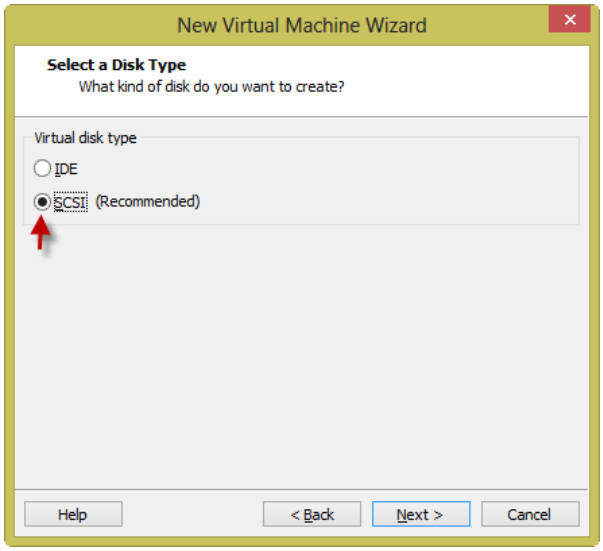
در این قسمت که مربوط به تنظیمات کارت شبکه‌ی سیستم مجازی است، گزینه‌ی مورد نظر را انتخاب کنید تا بتوانید از ویندوز اصلی خود به این ماشین مجازی ارتباط داشته باشید. بر روی Next کلیک کنید.



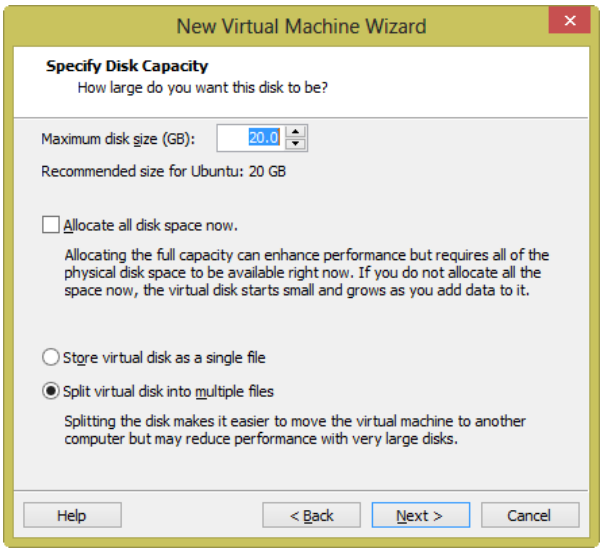
در این قسمت، نوع ارتباط هارد دیسک را مشخص می‌کند. بر روی گزینه‌ی پیش‌فرض کلیک و Next کنید.



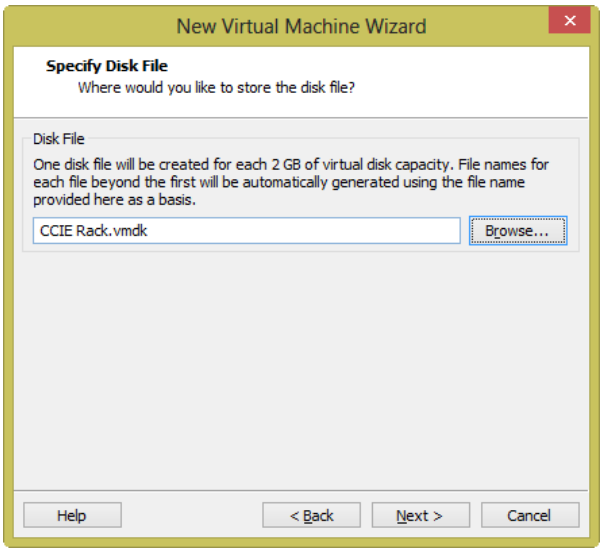
در این قسمت بر روی گزینه‌ی اول کلیک کنید تا یک هارد دیسک مجازی برای شما ایجاد شود، البته می‌توانید از هارد دیسک اصلی خود هم استفاده کنید که بهتر است این کار را انجام ندهید و بر روی Next کلیک کنید.



در این قسمت، گزینه‌ی مورد نظر را انتخاب کنید و بر روی Next کلیک کنید.

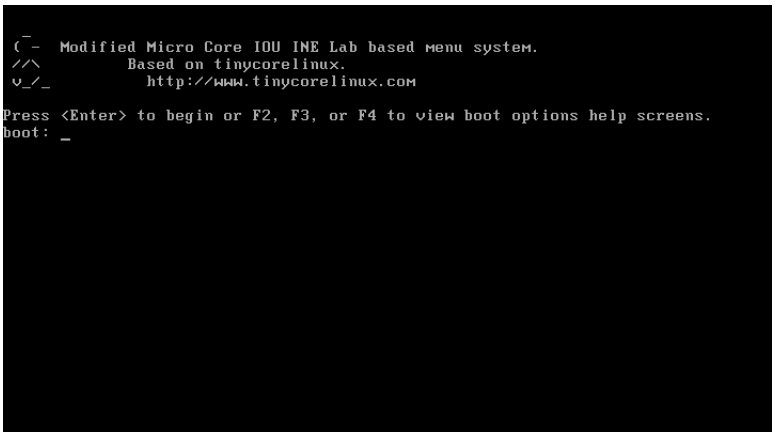


در این قسمت می‌توانید مقدار فضای هارد دیسک مجازی خود را مشخص کنید. اگر تیک گزینه‌ی Allocate All Disk Space Now را بزنید، باعث می‌شود که کل این فضا اشغال شود، پس این کار را انجام ندهید و تنها بر روی Next کلیک کنید.

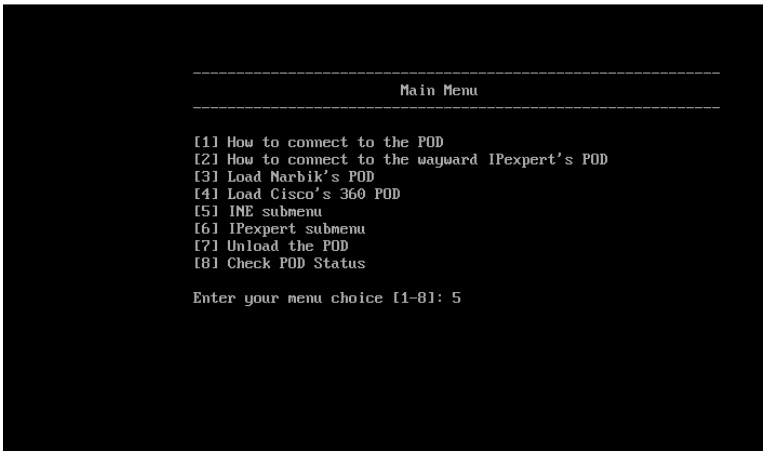


در این قسمت می‌توانید هارد دیسک ایجادشده را در جای دلخواه خود ذخیره کنید. بعد از این کار، بر روی Next کلیک کنید و در قسمت بعد هم بر روی Finish کلیک کنید.

بعد از ایجاد این ماشین مجازی، شکل زیر ظاهر می‌شود که برای روشن کردن این سیستم باید بر روی گزینه‌ی Power On...کلیک کنید.

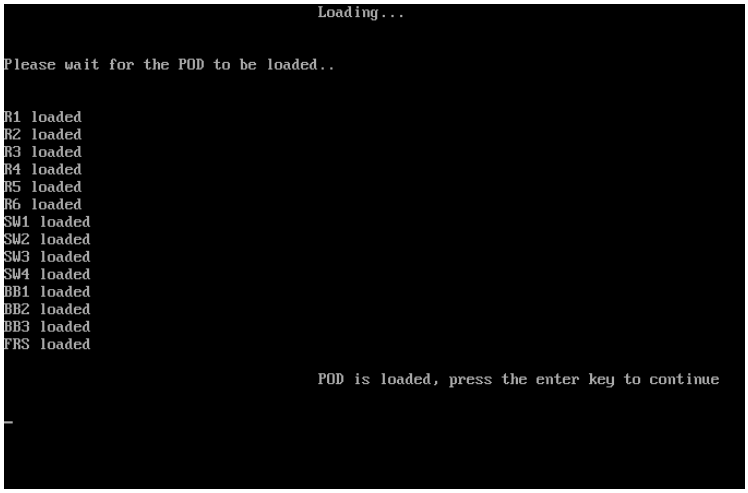


بعد از اجرا کردن نرم‌افزار IOU، شکل مقابل ظاهر می‌شود. بر روی Enter کلیک کنید تا نرم‌افزار اجرا شود.

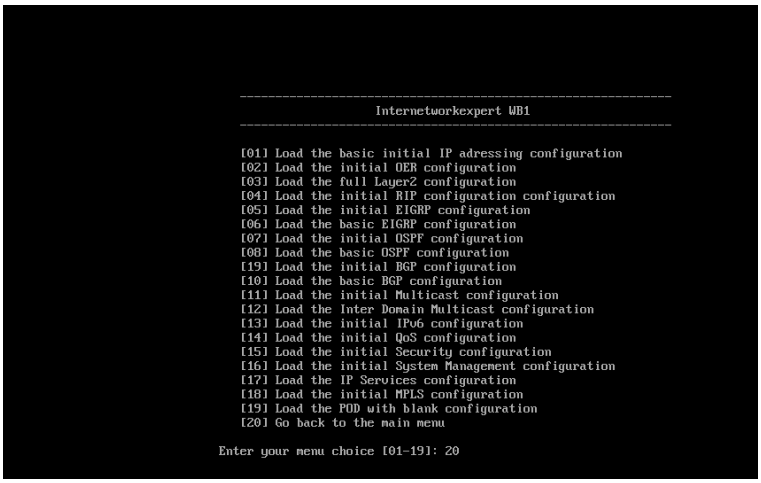


در این قسمت، شماره 5 را وارد کنید و بر روی Enter کلیک کنید.

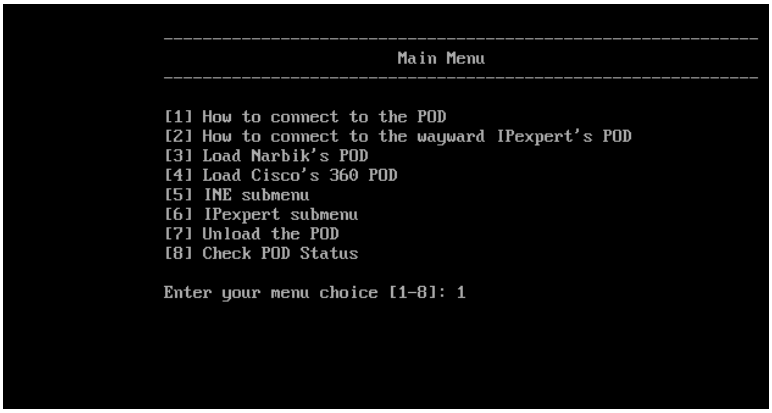
در این قسمت، عدد 19 را وارد کنید و بر روی Enter کلیک کنید.



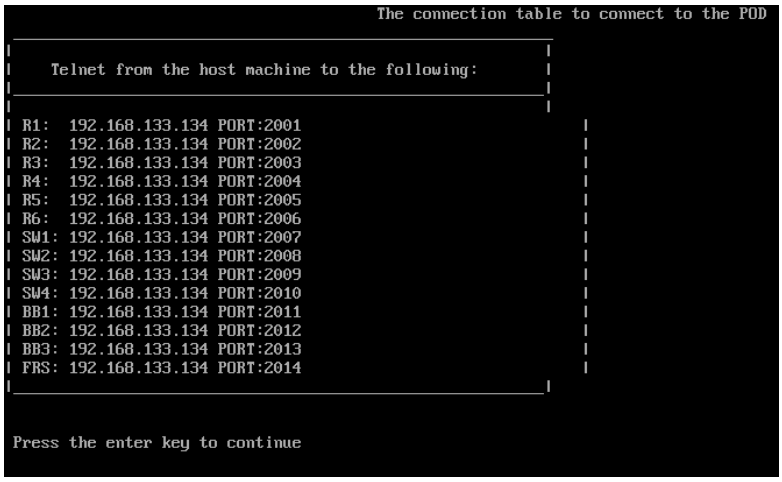
همان‌طور که مشاهده می‌کنید، تمام روترها و سوئیچ‌ها اجرا شده‌اند و نرم‌افزار آماده به کار است. بر روی enter کلیک کنید تا به قسمت قبل برگردیم.



در این قسمت، گزینه‌ی 20 را وارد کنید و بر روی Enter کلیک کنید تا به مرحله‌ی قبل برگردیم.



در این قسمت، گزینه‌ی 1 را وارد کنید تا لیست IP ها و پورت‌های سوئیچ‌ها و روترها را نمایش دهد.



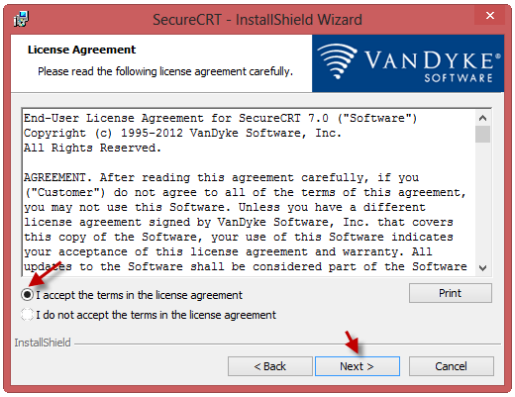
در این قسمت، IP ها و پورت‌های مربوط به روترها و سوئیچ‌ها نمایش داده می‌شود که شما باید از طریق نرم‌افزار خاصی به این روترها و سوئیچ‌ها متصل شوید و تنظیمات مربوط به آن‌ها را انجام دهید. خوب برای این کار از چه نرم‌افزاری استفاده کنیم؟

پیشنهاد من این است که از نرم‌افزار Secure CRT استفاده کنید که واقعاً از همه لحاظ کامل بوده و کار با نرم‌افزار IOU را برای شما آسان می‌کند.

برای دانلود این نرم‌افزار از لینک زیر استفاده کنید.

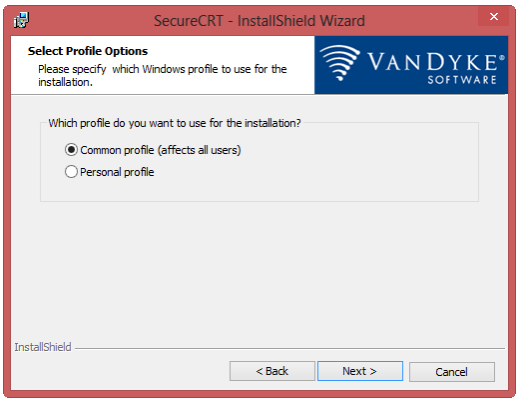
http://soft98.ir/internet/network/15209-vandyke-securecrt.html

نصب این نرم‌افزار شاید برای بعضی‌ها مشکل باشد که باهم این نرم‌افزار را نصب می‌کنیم و نحوه‌ی ارتباط با نرم‌افزار IOU را باهم می‌آموزیم.

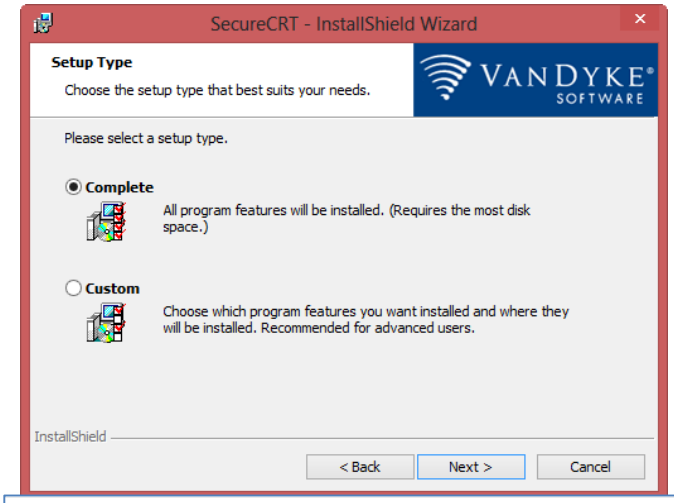


بر روی Setup.exe کلیک کنید و در پنجره‌ی بازشده بر روی Next کلیک کنید تا شکل روبرو ظاهر شود.

در این قسمت، قرارداد استفاده از نرم‌افزار را قبول کنید و بر روی Next کلیک کنید.

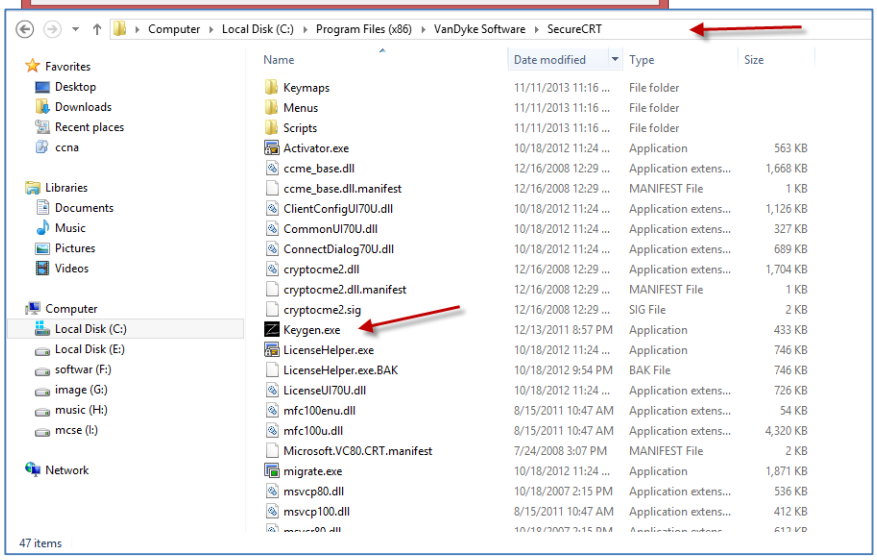


در این قسمت می‌توانید مشخص کنید که آیا فقط خودتان می‌خواهید از این نرم‌افزار استفاده کنید یا همه‌ی کاربران سیستم شما. بعد از انتخاب یکی از گزینه‌ها بر روی Next کلیک کنید.



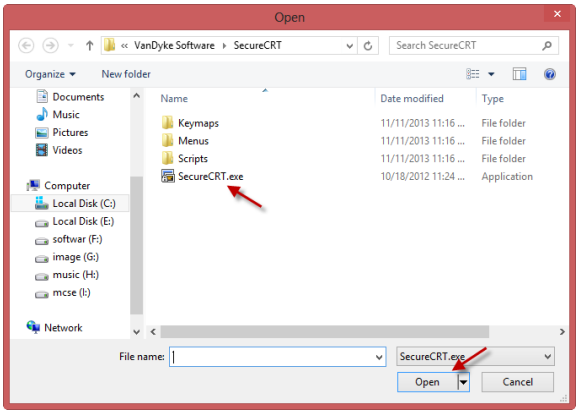
در این قسمت، گزینه‌ی اول را انتخاب و بر روی Next کلیک کنید. در صفحه‌ی بعد هم بر روی Next کلیک کنید و در قسمت آخر بر روی Install کلیک کنید تا نرم‌افزار نصب شود.

بعد از نصب شدن نرم‌افزار آن را اجرا نکنید. به پوشه‌ی Keygen بروید و فایل داخل آن را کپی و در پوشه‌ای که نرم‌افزار Secure CRT نصب شده است، Past کنید.

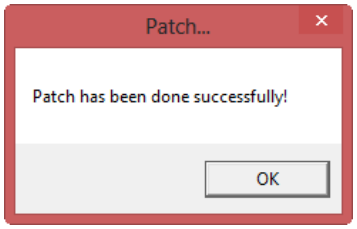


همان‌طور که مشاهده می‌کنید در پوشه‌ی مورد نظر قرار گرفته است؛ آن را با اولویت کاربر Administrator اجرا کنید.

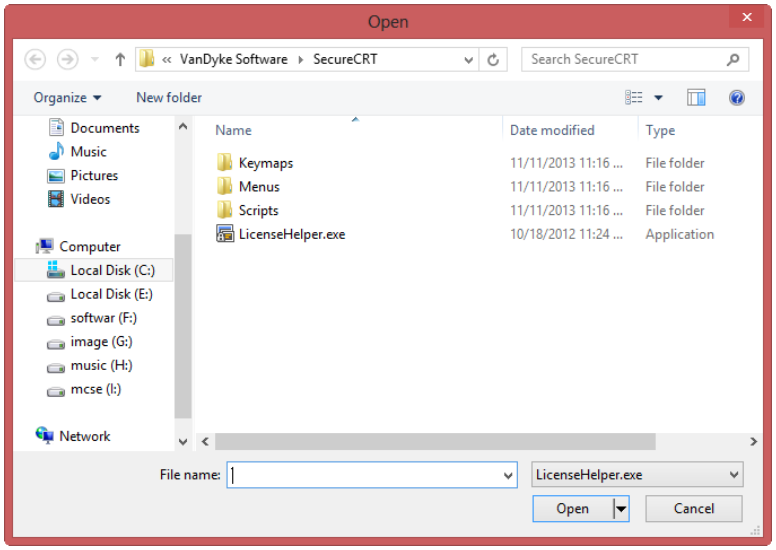
در این قسمت به هیچ گزینه‌ای دست نزنید و فقط بر روی Patch کلیک کنید و بعدازآن نرم‌افزار مورد نظر را به آن معرفی کنید.



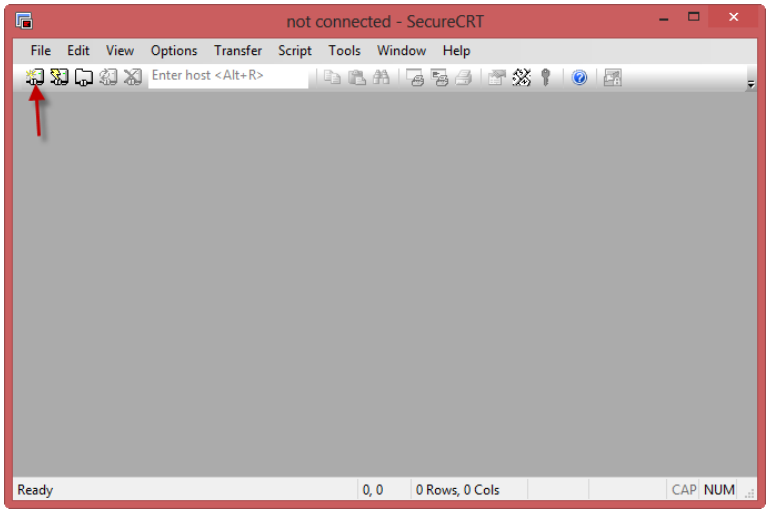
نرم‌افزار SecureCRT را انتخاب و بر روی Open کلیک کنید تا پیغام زیر ظاهر شود:



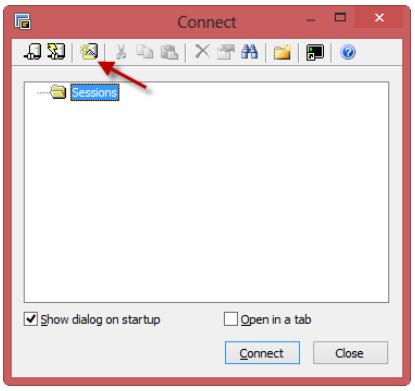
یک نکته بسیار مهم این است که در هنگام اجرا کردن Keygen حتماً از کاربر Admin استفاده کنید یا با کلیک راست کردن بر روی فایل مورد نظر و انتخاب گزینه‌ی Run As Administrators مجوزهای لازم به آن داده شود.



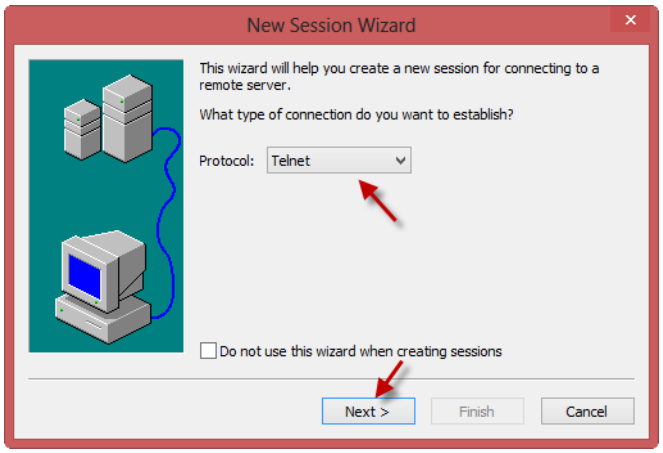
بعد از این‌که بر روی ok کلیک کردیم، شکل زیر ظاهر می‌شود که باید گزینه‌ی LicenseHelper.exe را انتخاب و بر روی Open کلیک کنیم و بعدازآن بر روی OK کلیک می‌کنیم که نرم‌افزار به صورت کامل نصب شود. بعد از نصب این نرم‌افزار آن را اجرا کنید تا باهم نحوه‌ی ارتباط با iou را کار کنیم.



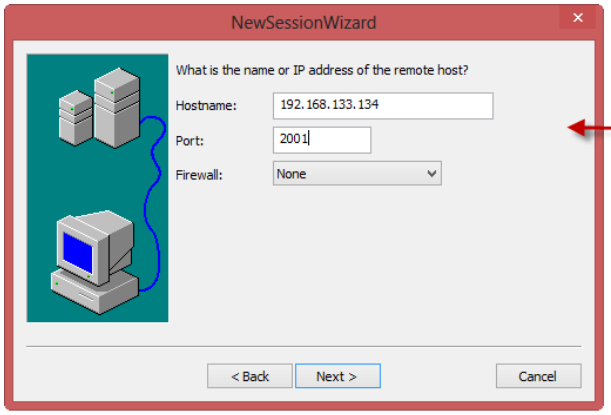
بعد از اجرای نرم‌افزار بر روی گزینه‌ی مورد نظر کلیک کنید یا از کلید ترکیبی Alt + C استفاده کنید تا شکل روبرو ظاهر شود.

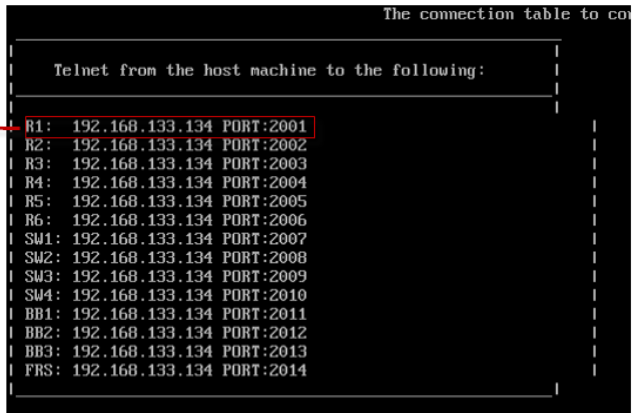


توجه داشته باشید در این قسمت می‌خواهیم تمام روترها و سوئیچ‌های مورد نظر را در یک بسته قرار دهیم تا برای استفاده از نرم‌افزار IOU، دیگر نیاز به واردکردن این اطلاعات نباشد و بتوان به صورت همزمان از همه‌ی آن‌ها استفاده کرد. بر روی گزینه‌ی مورد نظر کلیک کنید تا شکل زیر ظاهر شود:

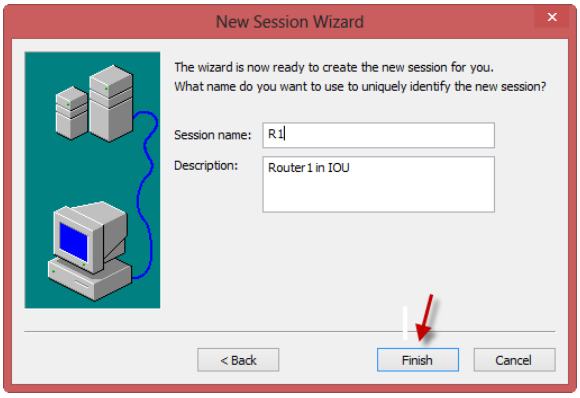


در این قسمت باید گزینه‌ی Telnet را انتخاب کنید و بر روی Next کلیک کنید.

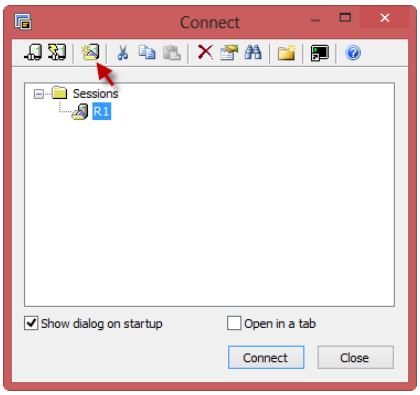




در شکل بالا آدرس ip و پورت مورد نظر مربوط به روتر 1 را در قسمت مورد نظر وارد کنید. همان‌طور که در شکل سمت راست مشاهده می‌کنید، آدرس‌های مشخص‌شده در IOU را وارد این نرم‌افزار کردیم. بر روی next کلیک می‌کنیم.

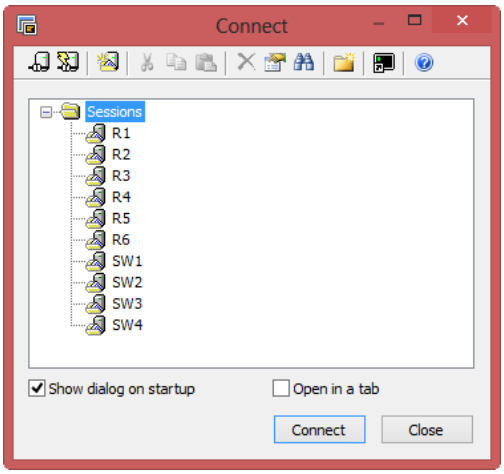


در این قسمت، نام روتر را وارد می‌کنیم که روتر 1 است و در قسمت Description هم توضیحاتی درباره‌ی روتر مورد نظر وارد می‌کنیم؛ بعد از اتمام کار، بر روی Finish کلیک می‌کنیم.

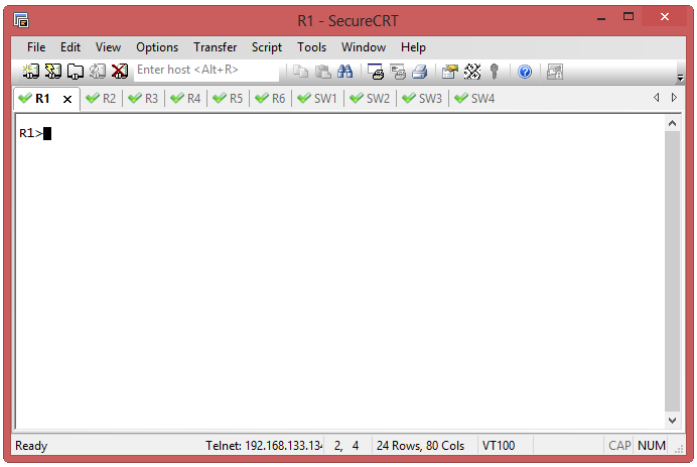


بعد از اتمام کار روتر R1، باید بقیه‌ی روترها و سوئیچ‌ها را به همین صورت انجام دهیم تا به لیست اضافه شوند که در قسمت بعدی این موضوع را مشاهده می‌کنیم.

همان‌طور که مشاهده می‌کنید، تمام روترها و سوئیچ‌ها به لیست اضافه شده است. امیدوارم که شما هم این کار را انجام داده باشید.



بعد از اتمام کار، Sessions را انتخاب و بر روی connect کلیک کنید تا به همه‌ی دستگاه‌ها در یک زمان متصل شوید. این کار را در شکل بعد مشاهده می‌کنید



همان‌طور که مشاهده می‌کنید به صورت صحیح و بدون خطا به روترها و سوئیچ‌های IOU متصل شده‌ایم و می‌توانیم تنظیمات را روی روترها و سوئیچ‌ها انجام دهید.

اگر در این بخش نتوانستید با iou ارتباط ایجاد کنید از طریق email با من در تماس باشید.

کار با نرم‌افزار GNS3:

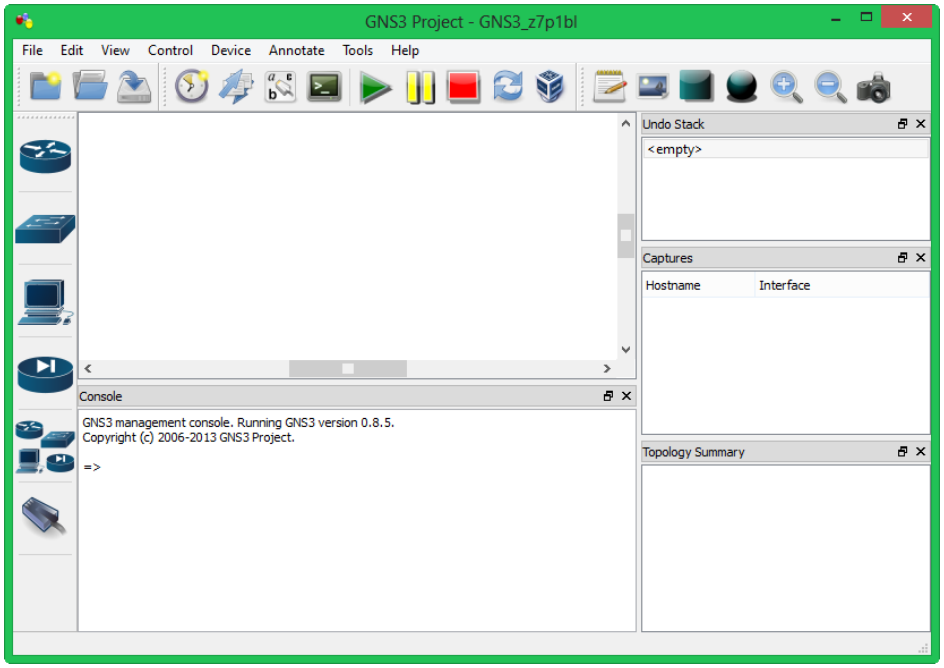
این نرم‌افزار که قوی‌ترین نرم‌افزار موجود است با بهره‌گیری ازIOS واقعی روترها از امکانات کاملی برخوردار است. در گذشته به خاطر استفاده‌ی بیش از حد روترها از CPU و مختل کردن کار سیستم، طرفدارهای زیادی نداشت، البته با استفاده از گزینه‌ی IDLE PC توانسته کمی از بار سیستم بکاهد، اما باز هم مشکل‌ساز بود. این مشکلات تا ز مانی وجود داشت که GNS ver 8.6 معرفی نشده بود. در این ورژن ابتدا با ایجاد تغییرات در ios های مورد نظر، مشکل تحمیل بار زیاد روی سیستم‌ها را حل کرده است، پس باهم این نرم‌افزار را نصب می‌کنیم و با جزئیات آن آشنا می‌شویم.

برای دانلود این نرم‌افزار به آدرس زیر مراجعه کنید:

http://www.gns3.net/download/

بعد از وارد شدن در سایت بر روی GNS3 v0.8.6 all-in-one و یا ورژن بالاتر از آن کلیک کنید.

بعد از دانلود، نرم افزار مورد نظر را نصب و اجرا کنید تا شکل زیر ظاهر شود.



در شکل بالا محیط این نرم‌افزار را مشاهده می‌کنید. در سمت چپ، روترها و سوئیچ‌ها و ... را مشاهده می‌کنید.

برای استفاده از روترها باید ios های مربوط به هر روتر را به برنامه اضافه کنیم.

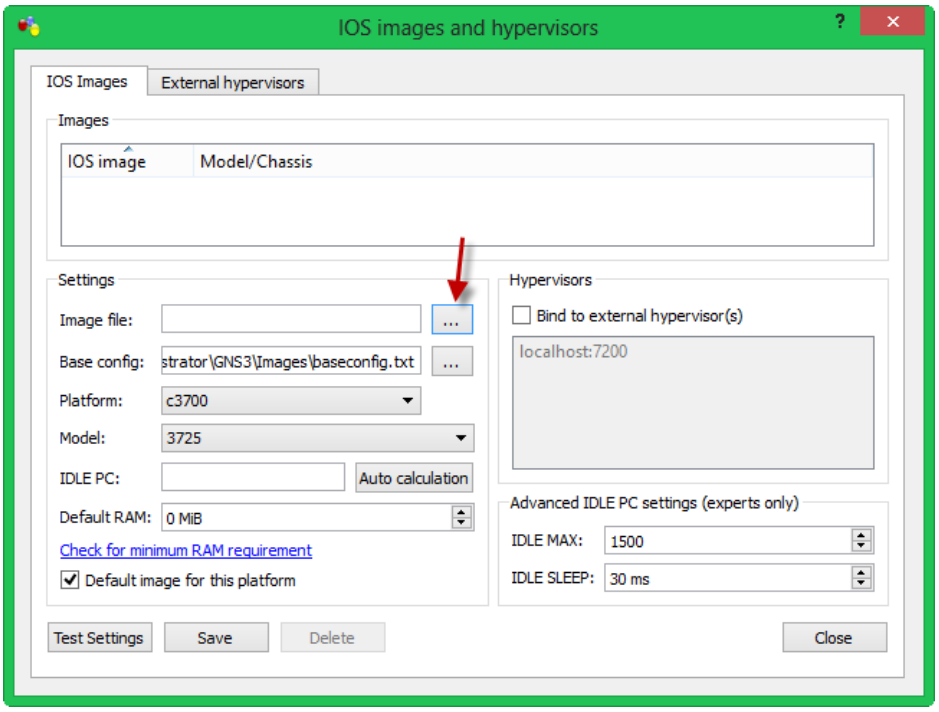
چگونه ios ها را به دست بیاوریم؟

شما می‌توانید از طریق وبلاگ شخصی من به این ios ها دست پیدا کنید:

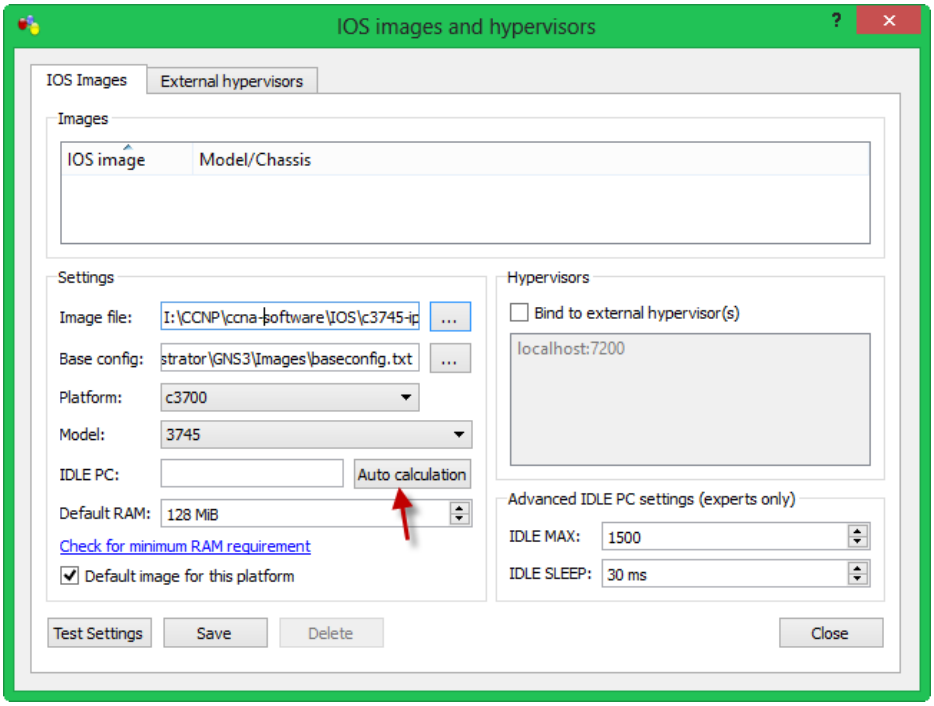
http://samancd.blogfa.com

چگونه iosها را در برنامه قرار دهیم؟

برای این کار از منوی Edit گزینه‌ی IOS image.... را انتخاب کنید یا از کلید ترکیبی Ctrl + shift + I استفاده کنید.

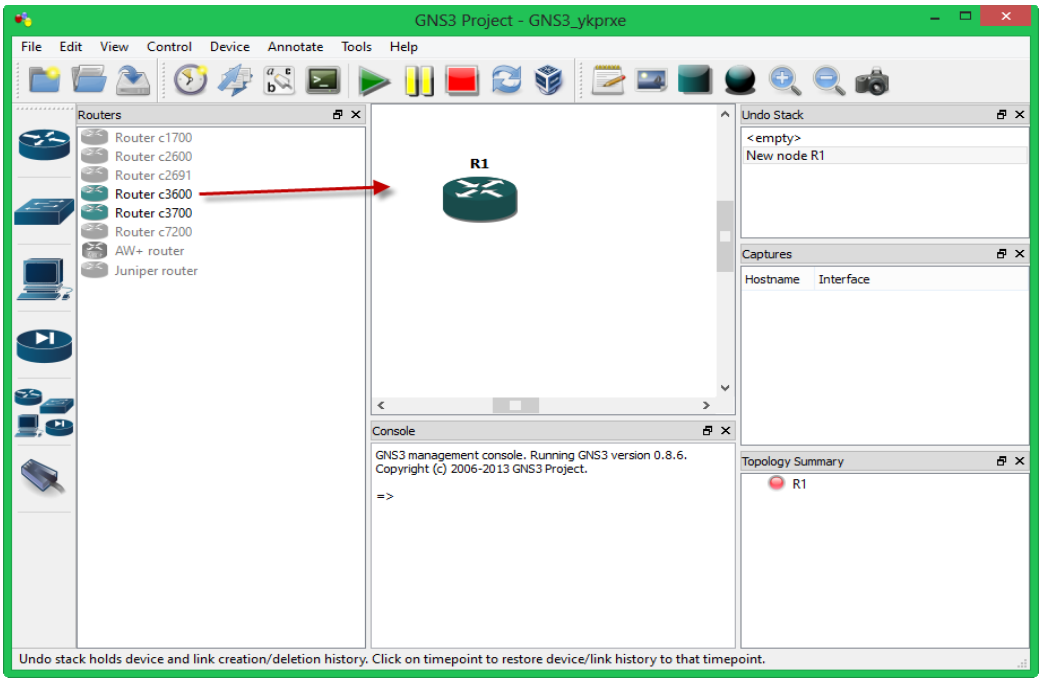


در شکل مقابل بر روی گزینه‌ی مورد نظر کلیک کنید و IOS مورد نظر را به لیست اضافه کنید. به شکل بعد توجه کنید.

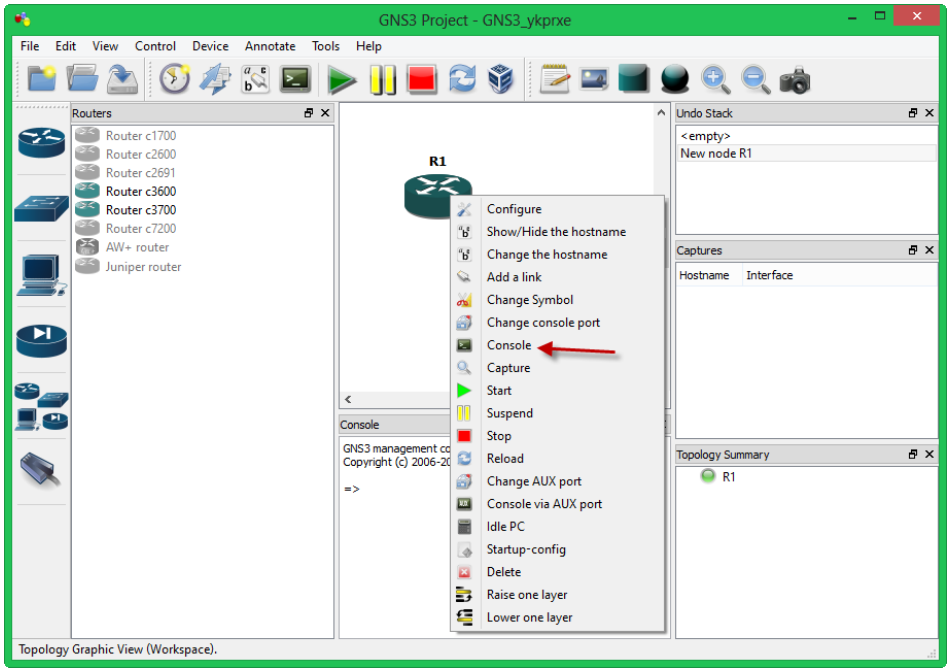


بعد از اضافه کردن IOS مورد نظر بر روی گزینه‌ی Auto Calculation کلیک کنید تا IDLE Pc برای این IOS انجام شود و بعد از اتمام این کار بر روی گزینه‌ی Save کلیک کنید تا اطلاعات ذخیره شوند.

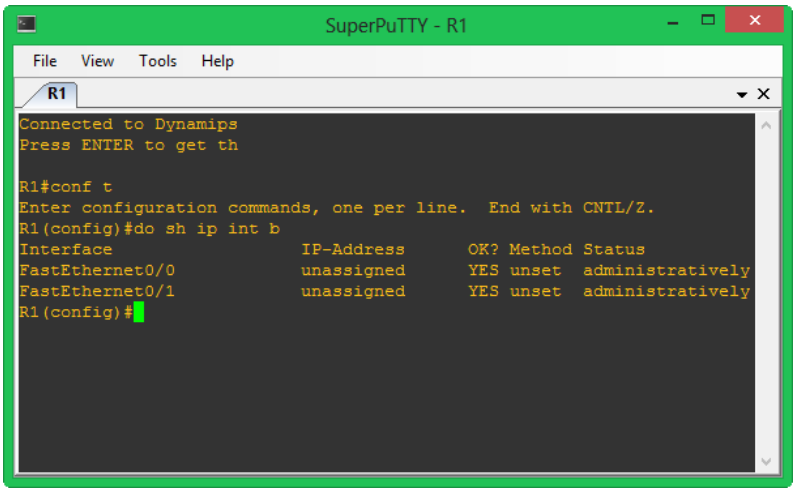
بعد از اضافه کردن IOS می‌توانید با روترها کار کنید.



در این قسمت، روتر را وارد صفحه می‌کنیم و برای روشن کردن روتر می‌توانیم از نوار ابزار بر روی دکمه‌ی START کلیک کنیم.



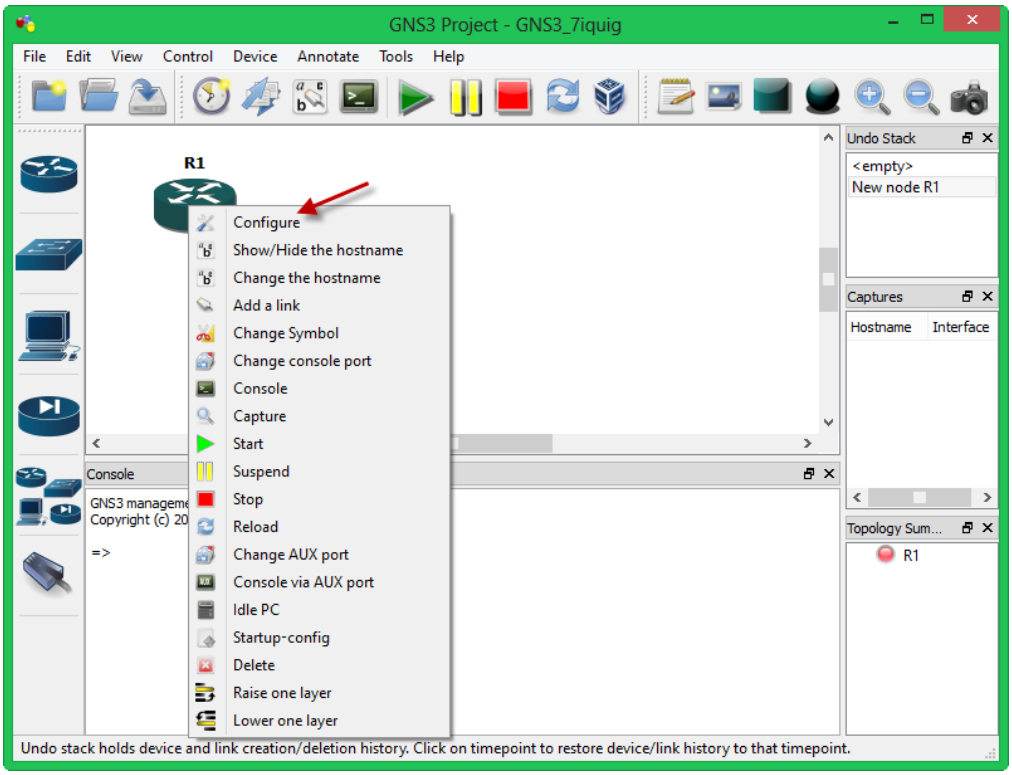
برای وارد شدن به ios روتر، روی روتر مورد نظر کلیک راست کرده و گزینه‌ی Console را انتخاب کنید یا بر روی روتر دو بار کلیک کنید تا شکل زیر ظاهر شود:

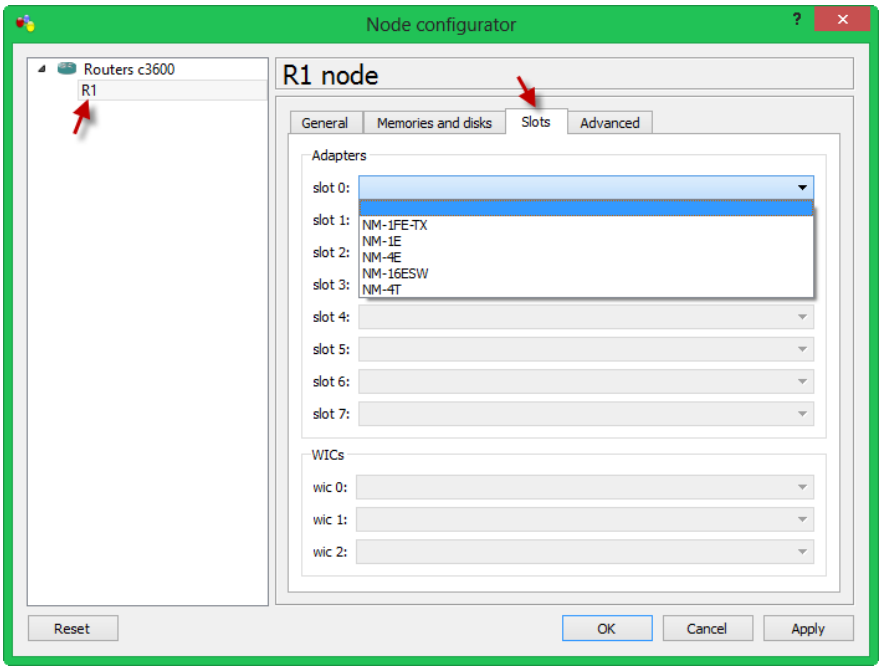


در شکل مقابل وارد روتر R1 شده‌ایم و می‌توانیم تنظیمات مربوط به این روتر را انجام دهیم.

برای متصل کردن دو روتر به هم از کابل‌های مربوط به اینترفیس‌های مورد نظر استفاده می‌کنیم. برای این کار دو روتر به صفحه اضافه می‌کنیم و از طریق گزینه‌ی  کابل مورد نظر را انتخاب و بر روی هر یک از روترها کلیک و گزینه‌ی مورد نظر را انتخاب می‌کنیم.

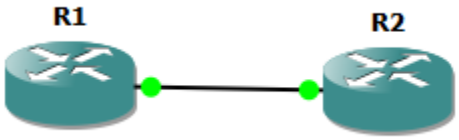
برای اتصال روتر به هم می‌توانید از اینترفیس‌های مختلف استفاده کنید. شاید روتری که به صفحه اضافه می‌کنید، هیچ‌گونه اینترفیسی نداشته باشد؛ برای حل این مشکل، بر روی روتر کلیک راست کرده و گزینه‌ی Configure را انتخاب کنید.

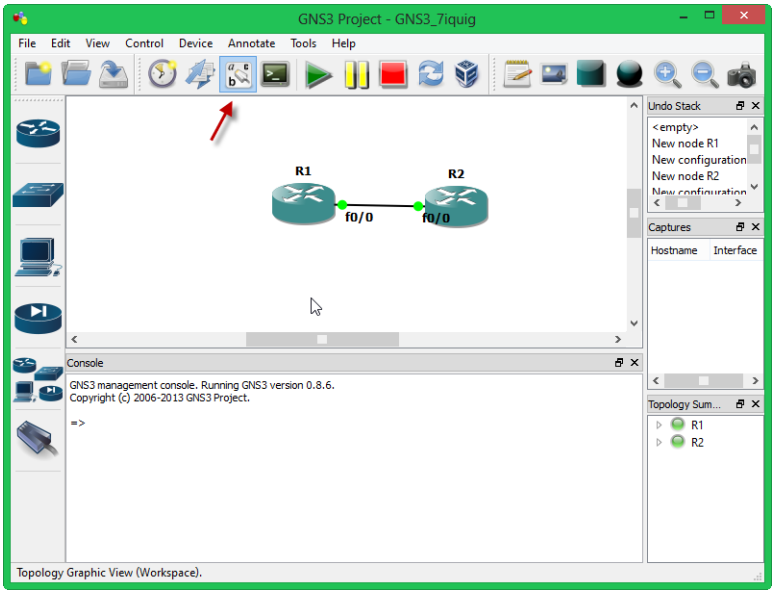




بعد از انتخاب این گزینه، شکل روبرو ظاهر می‌شود و شما با انتخاب تب Slots می‌توانید در هر Slots یک ماژول اضافه کنید که در این روتر 4 ماژول وجود دارد و می‌توانید از هر یک از آن‌ها استفاده کنید؛ بعد از انتخاب، بر روی Ok کلیک کنید.

حالا می‌توانید دو روتر را توسط کابل که به صورت خودکار انتخاب می‌شود را به هم متصل کنید، مانند شکل زیر:





برای نمایش شماره‌ی پورت‌ها روی صفحه، باید گزینه‌ی Show / Hide Interface Lable را انتخاب کنید که در شکل زیر این موضوع را مشاهده می‌کنید.

کل دستورات دوره‌ی CCNA به صورت سریع

نگاه کلی به دستورات و نحوه‌ی نوشتن و کار کردن با آن‌ها:

Router>enable Router>enab Router>en	می‌توانید دستورات را به صورت کامل و یا به صورت چند کلمه بنویسید.
Router#configure terminal Router#config t	به جای نوشتن یک کلمه به صورت کامل آن را خلاصه کنید.
Router#sh Tab= Router#show	بعد از نوشتن چند کلمه از یک دستور، بعدازآن بر روی کلید TAB کلیک کنید تا دستور کامل نوشته شود.
Router#?	با نوشتن علامت سؤال، لیست همه‌ی دستورات در مد مورد نظر نمایش داده می‌شود.
Router#c? clear clock	با نوشتن یک کلمه و بعدازآن نوشتن علامت سؤال، لیست دستوراتی که با این کلمه وجود دارد، نمایش داده می‌شود.
Router#cl? clear clock	نمایش دستوراتی که با حروف cl شروع می‌شوند.
Router#clock	
% Incomplete Command	این پیام زمانی نمایش داده می‌شود که یک دستور را به صورت کامل وارد نکرده باشیم.
Router#clock ? set	با گذاشتن علامت سؤال بعد از Clock دستورات بعدازآن نمایش داده می‌شود.
Router>enable Router#	با دستور enable در مد User وارد مد بعدی، یعنی مد Privileged می‌شویم.
Router#exit or Router>exit	با دستور Exit در دو مد اول از همه‌ی مدها خارج می‌شوید، در واقع، Sign Out می‌کنید.
Router(config-if)#exit	با نوشتن دستور exit از مد interface خارج شده و به مد قبلی برمی‌گردیم.

Router (config)#	
Router#disable Router>	با این دستور در مد Privileged از آن خارج و به مد User می‌رویم.
Router#logout	با این دستور اگر در مد userو Privileged باشیم از آن‌ها به طور کامل خارج می‌شود.
Router#setup	با این دستور وارد Setup Mode می‌شوید.
Router#show version	نمایش اطلاعات درباره‌ی IOS روتر.
Router#show flash	نمایش اطلاعات حافظه‌ی Flash روتر.
Router#show history	لیست 10 دستور آخر که وارد کرده‌ایم را به ما نشان می‌دهد.

انواع مد روتر:

Router>	User mode
Router#	Privileged mode
Router(config)#	Global configuration mode
Router(config-if)#	Interface mode
Router(config-subif)#	Subinterface mode
Router(config-line)#	Line mode
Router(config-router)#	Router configuration mode

Router(config)#hostname Cisco	با این دستور می‌توانید نام روتر یا سوئیچ را تغییر دهید.
Cisco(config)#	نام تغییر کرده.
Router(config)#enable password cisco	فعال کردن Password.
Router(config)#enable secret class	فعال کردن secret password.
Router(config)#line con 0	وارد شدن به پورت console.

Router(config-line)#password console	رمزگذاری در این پورت.
Router(config-line)#login	فعال کردن رمز گذاشته‌شده بر روی پورت با این دستور.
Router(config)#line vty 0 4	وارد شدن به پورت Vty که 5 پورت است.
Router(config-line)#password telnet	رمزگذاری در پورت Vty.
Router(config-line)#login	فعال کردن رمز گذاشته‌شده بر روی پورت با این دستور.
Router(config)#line aux 0	وارد شدن به پورت auxiliary.
Router(config-line)#password backdoor	رمزگذاری در این پورت.
Router(config-line)#login	فعال کردن رمز گذاشته‌شده بر روی پورت با این دستور.
Router(config)#service password-encryption	فعال کردن سرویس کد کردن رمز عبور تا امنیت روتر افزایش پیدا کند.
Router(config)#no service password-encryption	غیرفعال کردن این امکان.
Router#show ?	تمام دستورات که با دستور show اجرا می‌شود را نمایش می‌دهد.
Router#show interfaces	نمایش اطلاعات تمام Interface های روتر یا سوئیچ.
Router#show interface serial 0	نمایش اطلاعات یک اینترفیس سریال.
Router#show ip interface brief	نمایش همه‌ی اینترفیس‌ها به همراه اطلاعاتی از قبیل ip address و روشن یا خاموش بودن پورت.
Router#show controllers serial 0	با این دستور متوجه می‌شویم که کدام طرف از کابل سریال DTE است یا DCE.
Router#show clock	نمایش ساعت دستگاه.
Router#show hosts	نمایش اطلاعات کش روتر در مورد Ipaddress ها و...
Router#show users	نمایش همه کاربرانی که به روتر متصل هستند.

Router#show arp	نمایش جدول پروتکل ARP.
Router#show protocols	نمایش اینترفیس‌های روتر که در لایه‌ی 3 کار می‌کنند.
Router#show startup-config	نمایش تنظیمات ذخیره‌شده در حافظه‌ی NVram.
Router#show running-config	نمایش اطلاعات ذخیره‌شده در Ram.
Router(config)#int s0	وارد شدن به interface با شماره‌ی صفر.
Router(config-if)#exit	خارج شدن از اینترفیس.
Router(config)#int e0	وارد شدن interface مورد نظر.
Router(config)#int s0/0	وارد شدن به اینترفیس Serial 0/0.
Router(config-if)#description Link to ISP	برچسب‌گذاری روی اینترفیس Serial 0/0.
Router(config-if)#ip address 192.168.10.1 255.255.255.0	آدرس‌دهی به اینترفیس.
Router(config-if)#clock rate 56000	تعیین نرخ انتقال.
Router(config-if)#no shut	روشن کردن اینترفیس.
Router(config)#banner motd # This is a securesystem. Authorized Personnel Only! # Router(config)#	Banner یک پیغام ایجاد می‌کنیم تا کسانی که قصد ورود به روتر یعنی قبل از مد UserMode برای آن‌ها نمایش داده شود. # این علامت برای قطع کردن دستور است.
Router(config)#clock timezone EST 5	مشخص کردن منطقه‌ی جهانی. 5 در اینجا به معنای تعداد ساعت عقب یا جلو بودن ساعت شما با ساعت جهانی.
Router(config)#ip host london 172.16.1.3	نسبت دادن یک نام به یک ip address و ارتباط با آن.
Router#ping london	Ping کردن آدرس London.
Router(config)#no ip domain-lookup	زمانی که یک دستور را به اشتباه وارد کردید، روتر دنبالش می‌گردد و وقت‌گیر است. با این دستور از این کار جلوگیری می‌کنیم.

Router(config)#line con 0	وارد پورت console شوید.
Router(config-line)#logging synchronous	با فعال شدن این دستور از نمایش پیام‌های خودکار در هنگام تایپ دستورات جلوگیری می‌کند.
Router(config-line)#exec-timeout 0 0	این دستور مدت‌زمان قرار گرفتن در یک مد را به بی‌نهایت تبدیل می‌کند.
Router#copy run start	ذخیره کردن تنظیمات از Ram به Nvram.
Router#copy run tftp	ذخیره کردن تنظیمات از Ram به یک سرور.
Router#erase start	حذف تنظیمات ذخیره‌شده در Nvram.
Router(config)#ip route 172.16.20.0 255.255.255.0 172.16.10.2	با این دستور یک شبکه‌ی غیرمحلی را به روتر معرفی می‌کنیم.

شماره‌ی Administrative Distance برای پروتکل‌های مختلف:

Route Type	**Administrative Distance**
Connected	0
Static	1
EIGRP Summary Route	5
EBGP	20
EIGRP (Internal)	90
IGRP	100
OSPF	110
IS-IS	115
RIP	120
EGP	140
On-Demand Routing	160
EIGRP (External)	170
iBGP (External)	200
Unknown	255

Router#show ip route	این دستور برای نمایش جدول روتینگ استفاده می‌شود.
Router(config)#router rip	فعال کردن پروتکل Rip.
Router(config-router)#network w.x.y.z	معرفی شبکه‌ها متصل به روتر برای پروتکل Rip.
Router(config)#no router rip	حذف پروتکل Rip.
Router(config-router)#no network w.x.y.z	حذف شبکه مورد نظر از پروتکل Rip.
Router(config-router)#passive-interface s0/0	Passive-interface با این دستور Update ها را به یک اینترفیس مشخص ارسال نمی‌کند.
Router(config-router)#neighbor a.b.c.d	تعریف همسایه‌ی خاص برای تبادل اطلاعات.
Router(config-router)#no ip split-horizon	می‌توانید split horizon که روشی برای جلوگیری از loop بود را غیرفعال کنید.
Router(config-router)#ip split-horizon	می‌توانید split horizon را فعال کنید.
Router(config-router)# timers basic 30 90 180 270 360	می‌توانید تایمرهای مختلف در پروتکل Rip را تغییر دهید. 30 = Update timer (in seconds) 90 = Invalid timer (in seconds) 180 = Hold-down timer (in seconds) 270 = Flush timer (in seconds) 360 = Sleep time (in milliseconds)
Router(config-router)#maximum-paths x	با این دستور می‌توانید مسیرهای load balancing را تغییر دهید که به طور پیش‌فرض 4 است.
Router(config-router)#default-information originate	با این دستور default route وارد Rip می‌شود.
Router(config-router)#version 2	تبدیل پروتکل Rip به Version2.
Router(config-if)#ip rip send version 1	ارسال پکت‌های Rip V1 از طریق اینترفیس.

Router(config-if)#ip rip send version 2	ارسال پکت‌های Rip V2 از طریق اینترفیس.
Router(config-if)#ip rip send version 1 2	ارسال پکت‌های Rip Version 1 و Version2 از طریق اینترفیس.
Router(config-if)#ip rip receive version 1	دریافت اطلاعات Rip Version 1 از طریق اینترفیس.
Router(config-if)#ip rip receive version 2	دریافت اطلاعات Rip Version2 از طریق اینترفیس.
Router(config-if)#ip rip receive version 1 2	دریافت پکت‌های Rip Version 1 , Version2 از طریق اینترفیس.
Router#debug ip rip	عیب‌یابی پروتکل Rip.
Router#show ip rip database	نمایش جدول روتینگ و نحوه‌ی ارتباط آن‌ها.
Router(config-router)#no version 2	تغییر حالت به Vrsion 1.
Router(config-router)#version 1	تغییر به Version1.
Router(config-router)#no auto-summary	جلوگیری از summarizes در پروتکل.
Router(config-router)#auto-summary	فعال کردن summarizes در پروتکل.
Router(config)#router igrpas-number	راه‌اندازی پروتکل IGRP است که as-number شماره‌ای است که روترها باهم در ارتباط هستند.
Router(config-router)#network w.x.y.z	تعریف شبکه‌ی روتر مورد نظر در پروتکل IGRP.
Router(config)#no router igrp as-number	حذف کردن پروتکل IGRP.
Router(config-router)#no network w.x.y.z	حذف شبکه‌ی موجود در پروتکل IGRP.
Router(config-if)#bandwidth x	تغییر پهنای باند برای انتخاب مسر بهتر.
Router(config-router)#variance x	مجوز استفاده از چندین متریک مختلف برای IGRP.
Router#debug ip igrp events	نمایش همه‌ی رویدادهای مربوط به IGRP.

Router#debug ip igrp transactions	نمایش آپدیت‌های بین دو. روتر در IGRP.
Router(config)#router eigrp 100	راه‌اندازی پروتکل eigrp.
Router(config-router)#network 10.0.0.0	تعریف NETWork در شبکه EIGRP.
Router(config-router)#eigrp log-neighbor-changes	نمایش پیغام برای زمانی که تنظیمات روتینگ تغییر کند که بیشتر برای عیب‌یابی استفاده می‌شود.
Router(config-router)#no network 10.0.0.0	حذف Network در پروتکل EIGRP.
Router(config)#no eigrp 100	غیرفعال کردن پروتکل EIGRP 100.
Router(config-if)#bandwidth x	تغییر پهنای باند اینترفیس مورد نظر.
Router#show ip eigrp neighbors	نمایش شبکه‌های که با آن‌ها در ارتباط است.
Router#show ip eigrp neighbors detail	Displays a detailed neighbor table.
Router#show ip eigrp interfaces	نمایش interface هایی که پروتکل Eigrp روی آن فعال شده است.
Router#show ip eigrp int s 0/0	نمایش اطلاعات مربوط به یک interface خاص درباره‌ی eigrp.
Router#show ip eigrp topology	نمایش کل جدول توپولوژی که کل نقشه‌ی شبکه در آن ذخیره می‌شود.
Router#show ip eigrp traffic	نمایش ارسال و دریافت پکت‌ها و آپدیت‌ها.
Router#debug eigrp fsm	نمایش رویدادهای الگوریتم Dual.
Router#debug eigrp packet	نمایش رویدادهای انجام‌گرفته در ارسال پکت‌ها
Router#debug eigrp neighbor	نمایش پیام‌های شبکه‌ای که اتصال همسایگی دارند.

پروتکل OSPF:

فعال کردن پروتکل OSPF با شماره‌ی 123.	`Router(config)#router ospf 123` `Router(config-router)#`
تعریف شبکه‌ی مربوط به روتر و قرار دادن آن داخل Area0.	`Router(config-router)#network 172.16.10.0 0.0.0.255 area 0`
وارد شدن به اینترفیس loopback.	`Router(config)#interface loopback 0`
تعریف ip address در loopback.	`Router(config-if)#ip address 192.168.100.1 255.255.255.255`
وارد شدن در interface Serial 0/0.	`Router(config)#int S0/0`
تغییر priority به 50 برای خارج شدن روتر از حالت DR یا BDR.	`Router(config-if)#ip ospf priority 50`
وارد شدن در interface Serial 0/0.	`Router(config)#int s 0/0`
تغییر پهنای باند اینترفیس مورد نظر.	`Router(config-if)#bandwidth 128`
تغییر cost مربوط به یک interface برای استفاده در OSPF.	`Router(config-if)#ip ospf cost 1564`
	`Router(config)#router ospf 456`
فعال کردن Authentication بر روی یک area که رمز عبور در آن به صورت clear Text است.	`Router(config-router)#area 0 authentication`
قرار دادن رمز برای پروتکل ospf.	`Router(config-if)#ip ospf authentication-key fred`
	`Router(config)#router ospf 456`
فعال کردن MD5 برای hash کردن password.	`Router(config-router)#area 0 authentication message-digest`
تعریف رمز عبور به همراه MD5.	`Router(config-if)#ip ospf message-digest-key 1 md5 fred`
تغییر تایمر Hello به 20 ثانیه.	`Router(config-if)#ip ospf hello-interval timer 20`
تغییر تایمر Dead به 80 ثانیه.	`Router(config-if)#ip ospf dead-interval 80`
تعریف ip Route.	`Router(config)#ip route 0.0.0.0 0.0.0.0 s0/0`

Router(config-router)#default-information-originate	تزریق Default Route به پروتکل Ospf.
switch#show version	نمایش اطلاعاتی از نرم‌افزار و سخت‌افزار سوئیچ.
switch#show flash:	جزئیان ios سوئیچ.
switch#show mac-address-table	نمایش جدول MAC address سوئیچ.
switch#show running-config	نمایش اطلاعات ذخیره‌شده در حافظه‌ی ram.
switch#show start	نمایش اطلاعات ذخیره شده در حافظه‌ی NVRAM.
switch#show post	نمایش حالت Post سوئیچ.
switch#show vlan	نمایش تنظیمات Vlan.
switch#show interfaces	نمایش اطلاعات interface های سوئیچ.
switch#show interface vlan1	نمایش اطلاعات Vlan1.
switch#delete flash:vlan.dat	حذف VLAN database از روی حافظه‌ی Flash.
Switch#erase startup-config	حذف اطلاعات حافظه‌ی Nvram.
Switch#reload	ریسیت کردن سوئیچ.
Switch(config)#hostname 2900Switch	تغییر نام سوئیچ.
2900Switch(config)#enable password cisco	فعال کردن رمز عبور.
2900Switch(config)#enable secret class	فعال کردن secret password روی سوئیچ.
2900Switch(config)#line con 0	وارد شدن به console mode.
2900Switch(config-line)#login	درخواست دریافت رمز عبور صادر شود.
2900Switch(config-line)#password cisco	گذاشتن رمز عبور بر روی console.
2900Switch(config-line)#exit	خروج از console mode.
2900Switch(config-line)#line aux 0	ورود به auxiliary mode.
2900Switch(config-line)#login	درخواست دریافت رمز عبور صادر شود.
2900Switch(config-line)#password cisco	فعال کردن رمز عبور روی پورت auxiliary.

2900Switch(config-line)#exit	خروج از auxiliary mode.
2900Switch(config-line)#line vty 0 4	ورود به پورت مجازی VTY.
2900Switch(config-line)#login	درخواست دریافت رمز عبور صادر شود.
2900Switch(config-line)#password cisco	فعال کردن رمز عبور روی پورت VTY.
2900Switch(config-line)#exit	خروج از VTY mode.
2900Switch(config)#int vlan1	وارد شدن در Vlan1.
2900Switch(config-if)#ip address 172.16.10.2 255.255.255.0	ثبت ip address در این Vlan.
2900Switch(config-if)#exit	
2900Switch(config)#ip default-gateway 172.16.10.1	ثبت default-gateway برای این سوئیچ.
2900Switch(config-if)#description Finance VLAN	قرار دادن توضیحات در یک interface خاص.
2900Switch(config-if)#speed 10	تعیین سرعت 10 مگابایت.
2900Switch(config-if)#speed 100	تعیین سرعت 100 مگابایت.
2900Switch(config-if)#speed auto	تعیین سرعت به صورت اتوماتیک.
X900Switch(config)#ip http server	فعال کردن سرویس http روی سوئیچ.
X900Switch(config)#ip http port 80	اختصاص دادن پورت به سرویس http.
2900Switch(config)#mac-address-table static aaaa.aaaa.aaaa fa0/1 vlan 1	قرار دادن پارامتر در Mc Address.
2900Switch(config)#no mac-address-table static aaaa.aaaa.aaaa fa0/1 vlan 1	حذف کردن پارامتر در Mc Address.
2950Switch(config-if)#switchport port-security	فعال کردن port-security.
2950Switch(config-if)#switchport port-security mac-address sticky	دریافت اطلاعات آدرس mac از دستگاه متصل به پورت.
2950Switch(config-if)#switchport port-security maximum 1	مشخص کردن حداکثر تعداد دستگاه‌های متصل به پورت.
2950Switch(config-if)#switchport port-security violation shutdown	دسترسی غیر مجاز باعث shutdown شدن پورت می‌شود.

2900Switch#show port security	نمایش اطلاعات مربوط به port security.
2900#show spanning-tree brief	نمایش اطلاعات پروتکل STP.
Switch(config)#int fa 0/11	
Switch(config-if)#channel-group x mode on	ایجاد Channel-Group با مد on.
2950Switch(config)#vlan 10	ایجاد Vlanبا شماره‌ی 10.
2950Switch(config-vlan)#name Accounting	نام‌گذاری Vlan.
2950Switch(config-vlan)#exit	خروج از vlan.
2900Switch(config-if)#switchport mode access	تبدیل پورت به حالت access.
2900Switch(config-if)#switchport access vlan 2	قرار دادن پورت در vlan 2.
2900Switch(config-if)#int fa0/3	وارد شدن به پورت Fa0/3.
2950Switch(config)#int range fa 0/1 - 4	وارد شدن به چند پورت هم‌زمان و ایجاد تغییرات روی آن.
2900Switch#delete flash:vlan.dat	حذف فایل Vlan.dat از روی حافظه‌ی Falsh.
2900Switch(config-if)#no switchport access vlan 3	خروج پورت از vlan 3 و انتقال آن به Vlan1.
2900Switch#vlan database	حذف Vlan Database.
2900(vlan)#no vlan 3	حذف Vlan با شماره 3.
2900Switch#show vlan	نمایش جزئیات یک Vlan.
2900Switch#show vlan brief	نمایش جزئیات سریع از vlan.
2900Switch#show interfaces	نمایش اطلاعات interface مورد نظر.
2900Switch#debug sw-vlan packets	عیب‌یابی vlan.
2900Switch(config-if)#switchport mode trunk	فعال کردن وضعیت Trunk روی پورت مورد نظر.
2900Switch(config-if)#switchport trunk encapsulation isl	نحوه‌ی برچسب‌گذاری روی فریم‌ها.
2950Switch(config-if)#switchport mode trunk	فعال کردن وضعیت Trunk روی پورت مورد نظر.

29x0Switch#show int fa 0/1 switchport	نمایش اطلاعات witchport روی یک پورت.
2950Switch(config)#vtp mode client	تبدیل سوئیچ به VTP Client.
2950Switch(config)#vtp mode server	تبدیل سوئیچ به VTP Server.
2950Switch(config)#vtp mode transparent	تبدیل سوئیچ به .VTP Transparent
2950Switch(config)#vtp domain academy	تعیین دومین برای سوئیچ.
2950Switch(config)#vtp password catalyst	فرار دارد رمز عبور برای VTP.
2950Switch(config)#vtp v2-mode	تعیین ورژن VTp.
2950Switch(config)#vtp pruning	فعال کردن قابلیت Pruning.
29x0Switch#show vtp status	نمایش اطلاعات دومین.
29x0Switch#show vtp counters	نمایش اطاعات بسته‌های ارسالی و دریافتی در VTP.
Router(config-if)#int fa 0/0.1	ساختن interface مجازی.
Router(config-subif)#encapsulation dot1q 10	نسبت دادن این پورت به Vlan 10 با برچسب‌گذاری dot1q.
Router(config-subif)#ip address 192.168.10.1 255.255.255.0	واردکردن IP address در اینترفیس مجازی.
Router(config)#boot system flashimage-name	اجرای ios از روی ایمیج مورد نظر.
Router(config)#boot system tftpimage-name172.16.10.3	اجرای ios از روی سرور TFTP.
Router(config)#boot system rom	اجرای IOS از روی Rom.
copy tftp running-config	انتقال اطلاعات از سرور TFTP به Ram.
copy tftp startup-config	انتقال اطلاعات از سرور TFTP به Nvram.
show startup-config	نمایش اطلاعات ذخیره‌شده روی Nvram.
erase startup-config	پاک کردن Nvram.
copy run start	انتقال اطلاعات از Ram به Nvram.
copy run tftp	انتقال اطلاعات از Nvram به Ram.

show run	نمایش اطلاعات ذخیره‌شده روی ram.
router#show version	نمایش ورژن ios روتر یا سوئیچ.
router(config)#config-register 0x2142	تغییر شماره‌ی رجیستر با دستور confreg.
Router#show cdp	نمایش دستگاه‌های متصل.
Router#show cdp neighbors	نمایش دستگاه‌های متصل .
Router#show cdp neighbors detail	نمایش دستگاه‌های متصل با جزئیات کامل.
Router#show cdp entry word	نمایش دستگاه‌های متصل با استفاده از نام دستگاه.
Router#show cdp entry *	نمایش همه دستگاه‌های متصل
Router#show cdp interface	نمایش اینترفیسی که CDP روی آن فعال شده است
Router#show cdp interface x	نمایش اینترفیسی که CDP روی آن فعال شده است
Router#show cdp traffic	نمایش ترافیک مربوط به CDP
Router(config)#cdp holdtime x	تغییر ساعت holdtime در CDP
Router(config)#cdp timer x	تغییر ساعت ارسال آپدیت در CDP
Router(config)#cdp run	فعال کردن CDP.
Router(config)#no cdp run	غیرفعال کردن فرمان CDP.
Router(config-if)#cdp enable	فعال کردن CDP روی یک اینترفیس خاص.
Router(config-if)#no cdp enable	غیرفعال کردن CDP روی یک اینترفیس خاص.
Router#clear cdp counters	ریسیت کردن شماره‌ی counters در CDP.
Router#clear cdp table	حذف جدول CDP.
Router#debug cdp adjacency	مانیتور کردن اطلاعات CDP مربوط به همسایه.

Router#debug cdp events	مانیتور کردن تمام رویدادهای CDP.
Router#debug cdp ip	نمایش اطلاعات CDP مربوط به یک ip خاص.
Router#debug cdp packets	مانیتور کردن پکت‌های مربوط به CDP.
Router#traceroute 172.168.20.1	نمایش روترهای سر راه تا رسیدن به ip مورد نظر.
Router#TRace paris	نمایش روترهای سر راه تا رسیدن به Host مورد نظر.
Router#show ip route	نمایش جدول Route.
Router#show ip route protocol	نمایش اطلاعات جدول روتینگ بر طبق یک پروتکل خاص مانند Rip و Eigrp.
Router#show ip route w.x.y.z	نمایش اطلاعات route در مورد یک آدرس خاص.
Router#show ip route connected	نمایش اطلاعات روترهای متصل به این روتر.
Router#show ip route static	نمایش static Route.
Router#show ip route summary	نمایش اطلاعات کامل از جدول route.
Router(config)#ip route 0.0.0.0 0.0.0.0 172.16.20.1	فعال کردن Ip Route برای روتر که هر چه نمی‌داند را بفرستد به ip 172.16.20.1.
Router#show ip route	نمایش جدول روتینگ.
Router#debug telnet	نمایش اطلاعات رد و بدل شده دستور Telnet.
Router#show interface serial 0/0	نمایش وضعیت پورت سریال 0/0
Router#clear counters	پاک کردن همه‌ی شمارنده‌ها.
Router#clear counters interface type/slot	پاک کردن شمارنده‌ی مربوط به یک اینترفیس خاص.
Corp(config)#ip nat pool scott 64.64.64.70 64.64.64.126 netmask 255.255.255.128	فعال کردن Pool برای یک رنج ip خاص که مربوط به ip Valid است.

Corp(config)#access-list 1 permit 172.16.10.0 0.0.0.255	ساخت access-list و مجوز دادن به ip های در رنج مورد نظر.
Corp(config)#ip nat inside source list 1 pool scott	متصل کردن pool و Access-list مورد نظر در کنار هم.
Router(config)#int fa 0/0	وارد شدن به interface مورد نظر برای فعال کردن nat.
Router(config-if)#ip nat inside	فعال کردن nat بر روی اینترفیس داخلی شبکه.
Router(config-if)#ip nat Outside	فعال کردن nat بر روی اینترفیس خارجی شبکه.
Corp(config)#ip nat inside source list 1 interface serial 0/0 overload	فعال کردن access-list بر روی یک اینترفیس مورد نظر به صورت Overload (Pat).
Corp(config)#ip nat inside source static 172.16.10.5 64.64.64.65	فعال کردن Static Nat.
Router#show ip nat translations	نمایش اطلاعات مربوط به آدرس‌های مربوط به NAT.
Router#show ip nat statistics	نمایش کامل اطلاعات NAT.
Router#clear ip nat translations inside a.b.c.d outside e.f.g.h	حذف اطلاعات nat مربوط به آدرس خاص.
Router#clear ip nat translations *	پاک کردن کامل اطلاعات مربوط به جدول translations.
Router#debug ip nat	فعال کردن Debug برای Nat.
Router#debug ip nat detailed	نمایش اطلاعات پکت‌های مربوط به Nat به صورت کامل.
Router(config)#ip dhcp pool academy	تعریف کردن Dhcp Pool و فعال شدن آن.
Router(dhcp-config)#network 172.16.10.0 255.255.255.0	تعریف کردن رنج Ip برای DHCP .
Router(dhcp-config)#default-router 172.16.10.1	تعریف کردن Default-Route برای کلاینت‌ها.

Router(dhcp-config)#dns-server 172.16.10.10	تعریف کردن Dns Server برای کلاینت‌ها.
Router(dhcp-config)#netbios-name-server 172.16.10.10	تعریف کردن Netbios برای کلاینت‌ها.
Router(dhcp-config)#domain-name empson.ca	تعریف کردن Domain برای کلاینت‌ها.
Router(dhcp-config)#lease 14 12 23	حداکثر زمان در اختیار قرار گذاشتن ip address به یک کلاینت.
Router(dhcp-config)#lease infinite	زمان نامحدود برای پس گرفتن ip address از کلاینت.
Router(config)#ip dhcp excluded-address 172.16.10.1 172.16.10.9	اختصاص ندادن رنج ip مورد نظر به کلاینت‌ها.
Router(config)#no service dhcp	غیرفعال کردن سرویس DHCP.
Router(config)#service dhcp	فعال کردن سرویس DHCP.
Router#show ip dhcp binding	نمایش اطلاعات سرویس DHCP.
Router#show ip dhcp server statistics	نمایش اطلاعات مربوط به ارسال و دریافت اطلاعات از طریق DHCP.
Router#debug ip dhcp server events	نمایش رویدادهای مربوط به DHCP.
Router(config-if)#ip helper-address 172.16.20.2	انتقال اطلاعات مربوط به یک DHCP سرور به یک اینترفیس خاص.
Router#config t	وارد شدن به مد Global.
Router(config)#int s 0/0	وارد شدن به اینترفیس سریال 0/0
Router(config-if)#encapsulation hdlc	فعال کردن برچسب‌گذاری به روش HDLC.
Router(config-if)#encapsulation ppp	فعال کردن برچسب‌گذاری به صورت PPP.
Router(config)#username routerb password cisco	تعریف UserName و Password.
Router(config)#int s 0/0	ورود به پورت سریال s0/0

Router(config-if)#ppp authentication pap	فعال کردن الگوریتم رمزنگاری PAP.
Router(config-if)#ppp authentication chap	فعال کردن الگوریتم رمزنگاری CHAP.
Router(config-if)#ppp authentication pap chap	فعال کردن الگوریتم‌های رمزنگاریPAP و CHAP.
Router(config-if)#ppp authentication chap pap	فعال کردن الگوریتم‌های رمزنگاریCHAP و PAP.
Router(config-if)#ppp pap sent-username routerb password cisco	تعریف نام کاربری و رمز عبور روتر روبرو.
Router#show interfaces serial x	نمایش اطلاعات اینترفیس سریال.
Router#show controllers serial x	نمایش اطلاعات مربوط به اینترفیس سریال برای مشخص کردن DCE و DTE بودن کابل مورد نظر.
Router#debug serial interface	نمایش رویدادهای مربوط به اینترفیس سریال.
Router#debug ppp	نمایش رویدادهای مربوط به پروتکل PPP.
Router#debug ppp packet	نمایش رویدادهای مربوط به پکت‌های پروتکل PPP.
Router#debug ppp negotiation	نمایش رویدادهای مربوط به پروتکل PPP.
Router#debug ppp error	نمایش پکت‌های مشکل دار در پروتکل PPP.
Router#debug ppp authentication	نمایش رویدادهای مربوط به پکت‌هایی که دارای احراز هویت هستند.
Router(config)#int s 0/0	وارد شدن به اینترفیس سریال 0/0
Router(config-if)#encapsulation frame-relay	فعال کردن Frame Relay روی اینترفیس سریال مورد نظر.
Router(config-if)#frame-relay lmi-type {ansi | cisco | q933a}	مشخص کردن نوع پروتکل Frame Relay برای ارتباط در روترهای شرکت‌های مختلف.
Router(config-if)#frame-relay interface-dlci 110	تعریف شماره‌ی DLCI 110 بر روی اینترفیس مورد نظر.
Router(config-if)#frame-relay map ip 192.168.100.1 110 broadcast	تعریف آدرس با شماره‌ی DLCI روتر دیگر در یک ارتباط Frame Relay.

Router(config-if)#no frame-relay inverse arp	غیرفعال کردن حالت خودکار Invers Arp.
Router(config-subif)#int s 0/0.103 point-to-point	ساخت اینترفیس مجازی با حالت Point To Point
Router(config-subif)#ip address 192.168.20.1 255.255.255.0	تخصیص دادن IP address به اینترفیس مجازی.
Router(config-subif)#frame-relay interface-dlci 103	تعریف DLCI برای این اینترفیس.
Router(config)#access-list 10 permit 172.16.0.0 0.0.255.255	فعال کردن AL 10 و اجازه‌ی عبور دادن IP Address 172.16.0.0.
access-list	دستور Access List.
Router(config)#access-list 10 permit any	این Access List با شماره‌ی 10 به همه‌ی آدرس‌ها اجازه عبور می‌دهد (Any یعنی همه).
Router(config)#int fa0/0	وارد شدن به اینترفیس مورد نظر.
Router(config-if)#ip access-group 10 in	فعال کردن Access List شماره‌ی 10 روی اینترفیس مورد نظر به صورت in.
Router#show access-lists	نمایش Access List های تعریف‌شده روی روتر.
Router#show access-list access-list-number	نمایش Access List با شماره‌ی مورد نظر.
Router#show access-list name	نمایش Access List با اسم مورد نظر.
Router(config)#access-list 110 permit tcp 172.16.0.0 0.0.0.255 192.168.100.0 0.0.0.255 eq 80	اجازه‌ی عبور به شبکه مورد نظر برای دسترسی به پروتکل HTTP که پورت آن 80 است.
Router(config)#access-list 110 deny tcp any 192.168.100.7 0.0.0.0 eq 23	فعال کردن access List Estended برای جلوگیری از IP adderss 192.168.100.7 برای دسترسی به Telnet.

منابع:

- CCNA Self-Study: CCNA Portable Command Guide

  By Scott Empson

- CCNA™:Cisco®Certified Network AssociateStudy Guide 5th Edition

  By Todd Lammle

- CCNP - Routing Study Guide

  By Todd Lammle – Sean Odom – with kevin wallac

- http//cisco .com

- http://forum.ciscoinpersian.com

- http://fa.wikipedia.org/wiki/

- http://network.itpro.ir

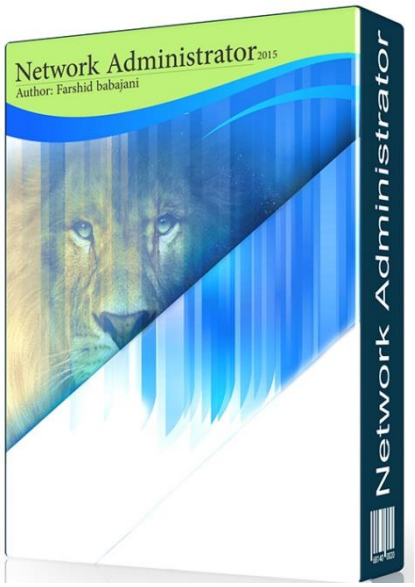
دوستان عزیز و گرامی در این کتاب تمام تلاش خود را کرده‌ام تا بتوانم موضوعات این دوره را به صورت ساده برای شما عزیزان بیان کنم، امیدوارم که توانسته باشم.

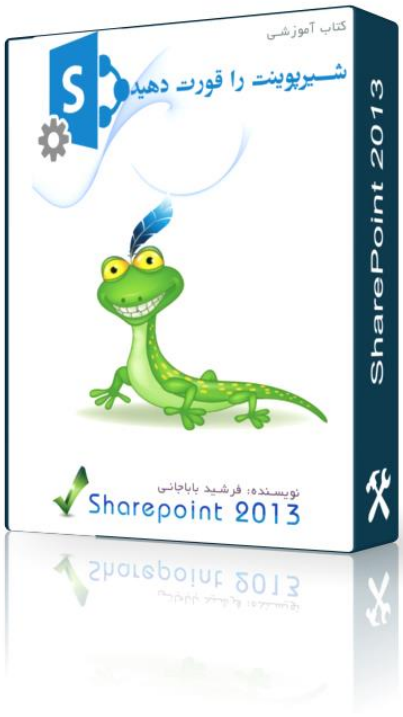
اگر درباره‌ی قسمت‌های مختلف این کتاب سؤالی دارید، می‌توانید با من در تماس باشید.:

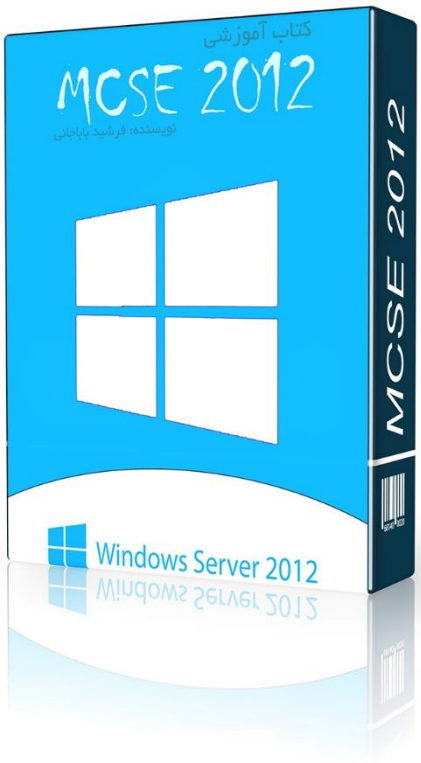
- Farshid_babajani@yahoo.com
- Farshid_babajani@live.com
- http://3isco.ir

برای کمک مالی به بنده برای پیشبرد اهداف بلند مدت، برای نوشتن آموزش های بهترمی‌توانید از شماره کارت های زیر استفاده کنند.

بانک سامان	6219	8610	0688	3549
بانک ملی	6037	9918	7468	0410







برای دسترسی به این کتاب‌ها به سایت 3isco.ir مراجعه کنید