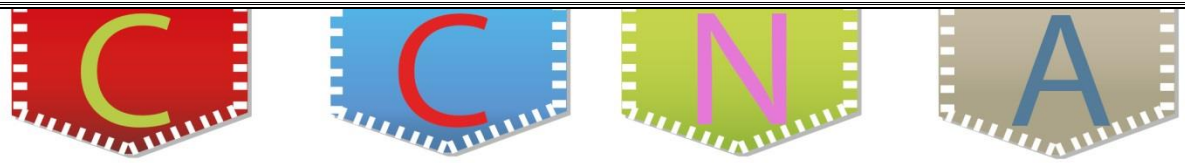


آموزش CCNA ++

نویسنده:

فرشید باباجانی

CCNA++

به جویبارها سوگند دریاد من می‌مانی، به برگ‌های نارنجی پاییزی، به سبد میوه‌های کال و نارس در دل پشت بام‌های دلتنگی، به طعم بی‌هوایی زرد آلو در جاده‌های سکوت و غمناکی، به پرنده، به پرواز، به شیرینی لبخند رؤیایی، به آسمان، به حیرانه‌های تنهایی، به تبسم، به خیال، به زیبایی، به عشق، به برگ‌های نارنجی پاییزی... دریاد من می‌مانی... (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:

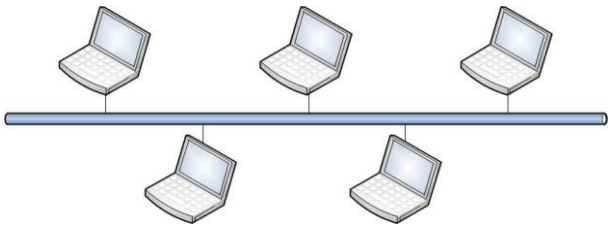
اصولاً به شکل هندسی اتصالات ادوات شبکه به هم را توپولوژی می‌گویند که به انواع مختلف زیر تقسیم‌بندی می‌شوند:

- 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.

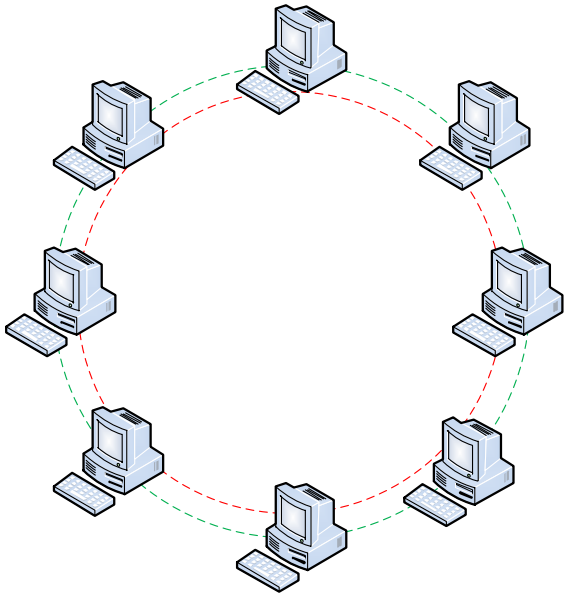
2- با افزودن کامپیوترهای جدید و ارسال حجم زیاد اطلاعات بر روی یک خط، کارایی شبکه کم می‌شود.

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:

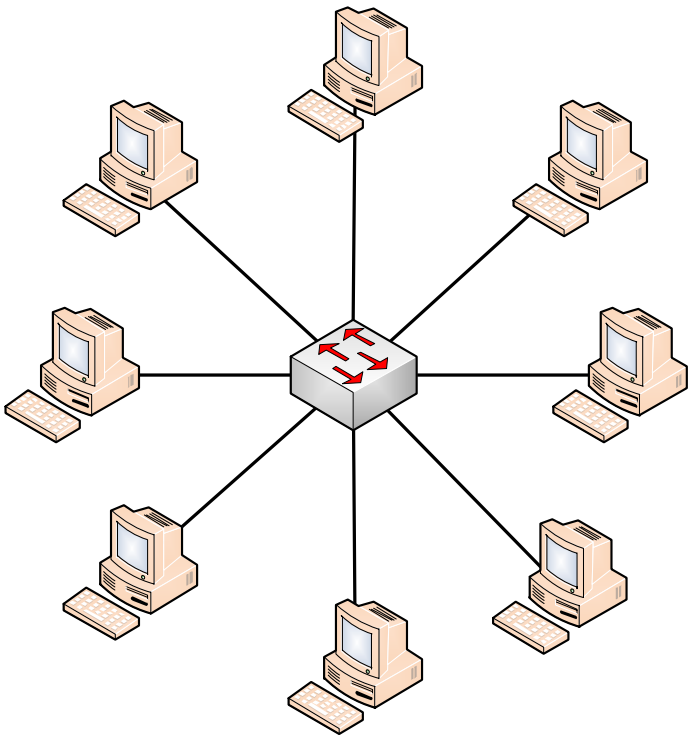
1- اگر یکی از کامپیوترها از کار بیفتد کل شبکه از کار خواهد افتاد.

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.

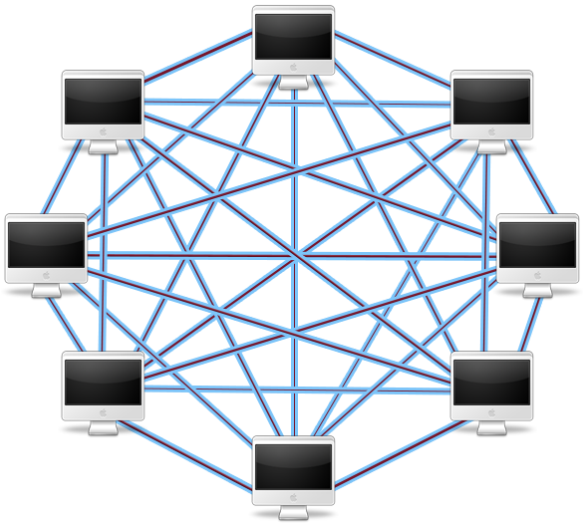
معایب:

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.

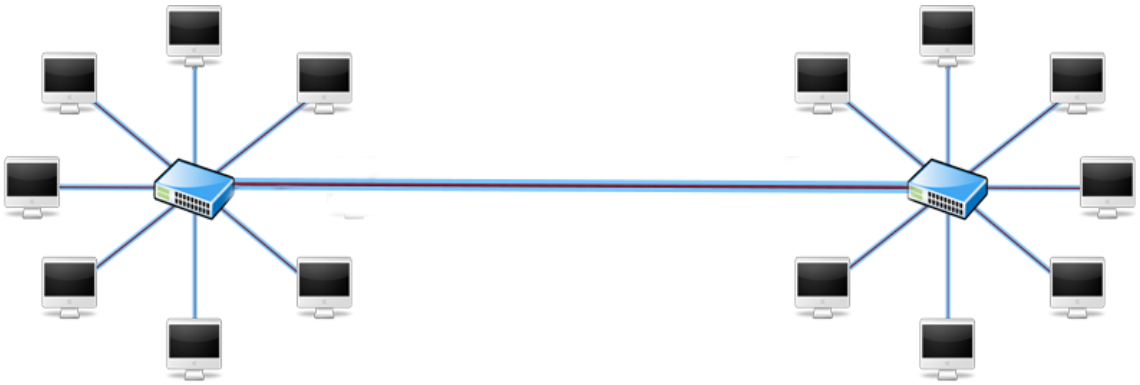
معایب:

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.

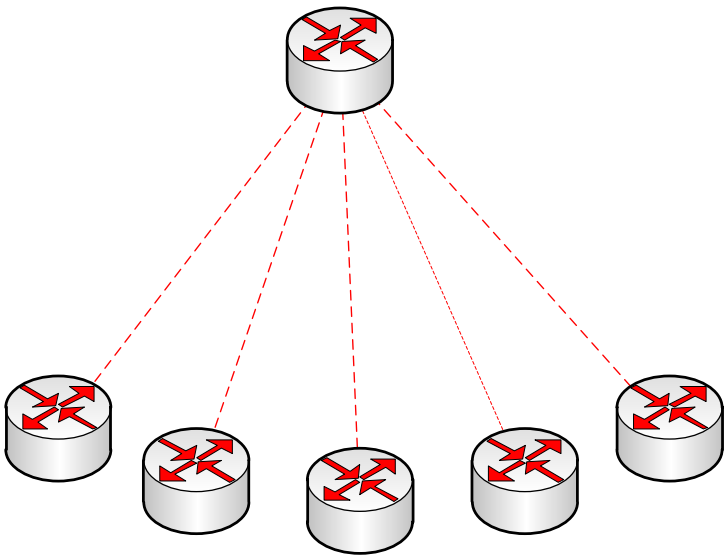


توپولوژی point to Point (نظیر به نظیر):

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

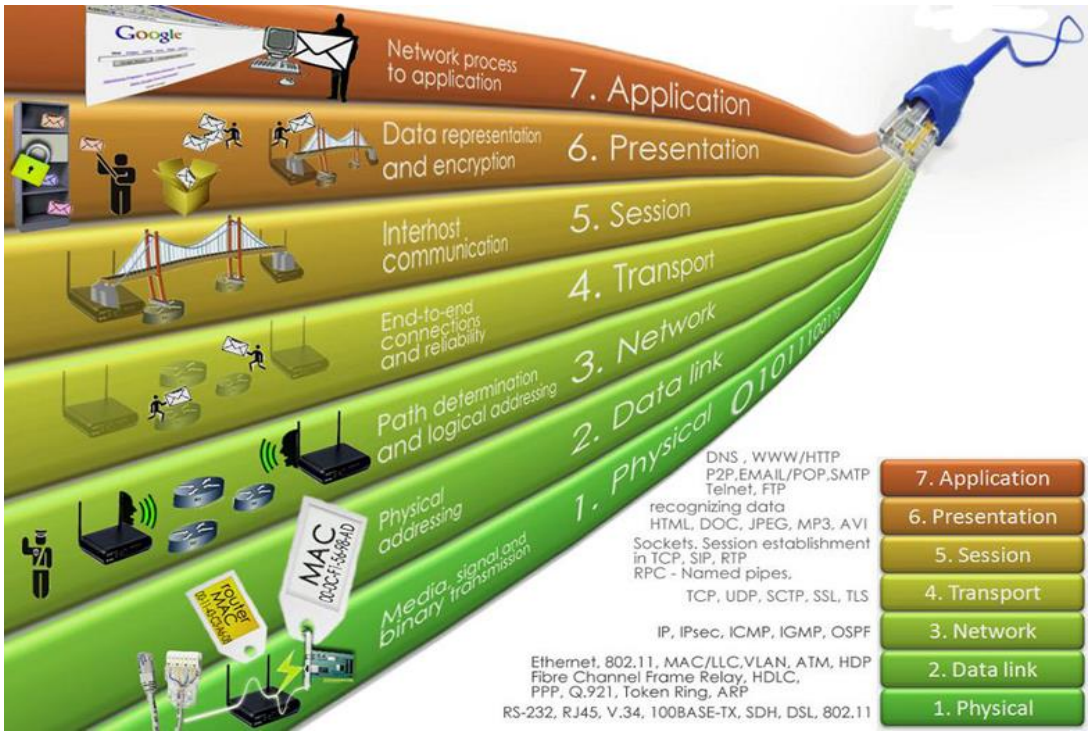
مدل OSI:

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:

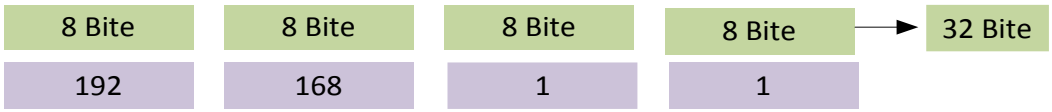
لایه‌ی شبکه، مسئول استقرار داده بر روی محیط انتقال شبکه و دریافت داده از محیط انتقال شبکه است. لایه‌ی فوق، شامل دستگاه‌های فیزیکی نظیر کابل شبکه و آداپتورهای شبکه است. کارت شبکه (آداپتور) دارای یک عدد دوازده رقمی مبنای شانزده (نظیر B : ٥-٥٠-٠٤-D٢٢-٤-٦٦) بوده که آدرس MAC، نامیده می‌شود. لایه‌ی اینترفیس 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:

1	2	3	4	5	6	7	8		9	10	11	12	13	14	15	16		17	18	19	20	21	22	23	24		25	26	27	28	29	30	31	32
1	1	1	1	1	1	1	1	.	1	1	1	1	1	1	1	1	.	1	1	1	1	1	1	1	1	.	1	1	1	1	1	1	1	1

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

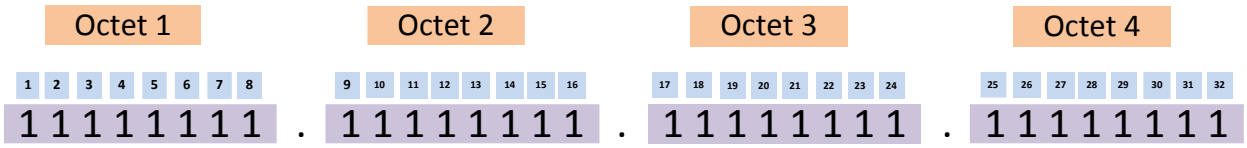
24/ می‌گوید که 3 تا octet اول ثابت باشد و octet آخر تغییر کند.

مثال بعدی:

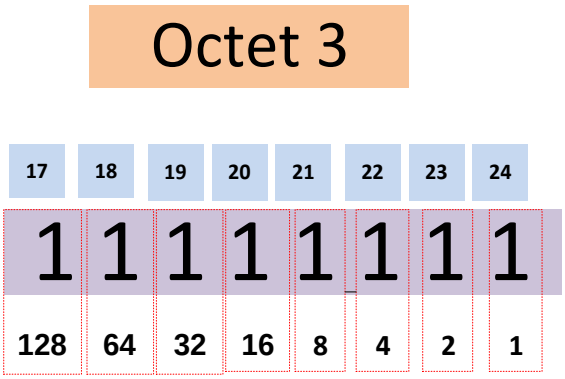
172.16.1.1/17

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:

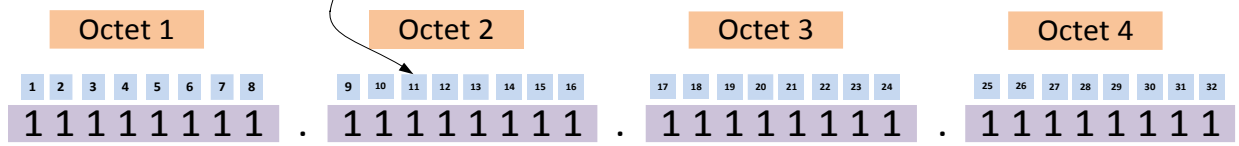


پس 17 همان عدد 128 است. این عدد را از 256 کم می‌کنیم و subnet mask ما به دست می‌آید.

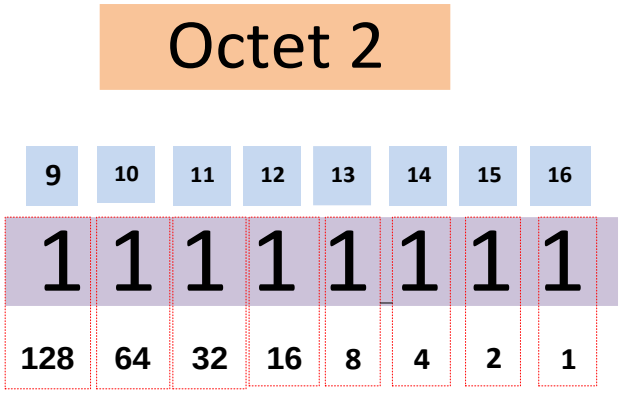
172.16.0~127.0
255.255.128.0

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:

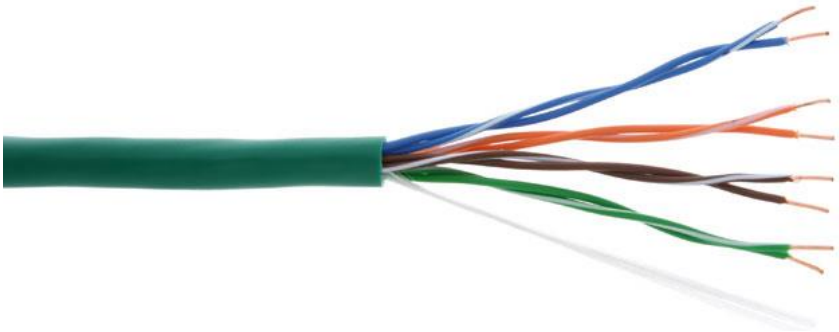
این کابل مانند کابل STP است، به‌طوری‌که به غیر از روکش‌های فلزی روی آن یک روکش فلزی دیگر، کل این روکش‌ها را دربرمی‌گیرد که این کابل را به نسبت قوی‌تر و محکم‌تر در برابر ضربه و امواج الکترومغناطیسی کرده است.

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.

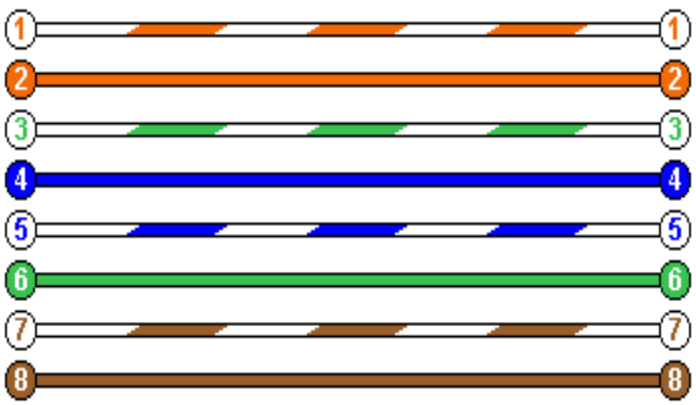
این کابل‌ها از رنگ‌بندی خاصی استفاده می‌کند، این رنگ‌بندی بی‌دلیل نیست. در ادامه به این موضوع پی خواهیم برد.

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 :

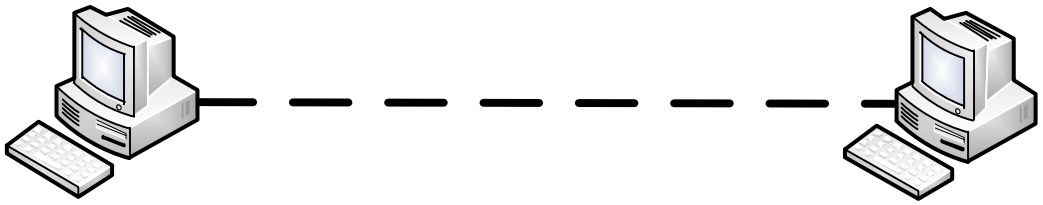
این نوع کابل برای ارتباط دو وسیله‌ی غیرمشابه مانند سوئیچ و کامپیوتر استفاده می‌شود. باید دو سرکابل را به یک صورت ببندیم، یعنی رنگ‌بندی را تغییر ندهیم.

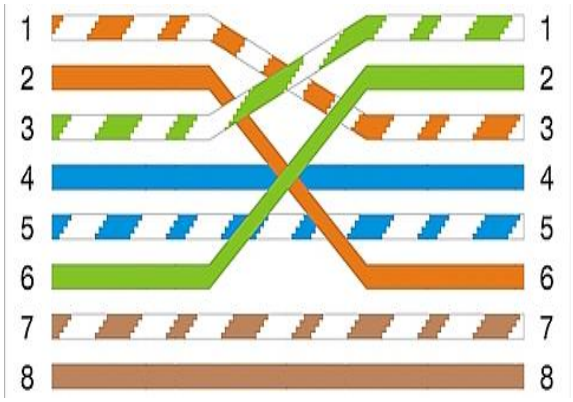
کابل طرف سوئیچ		رنگ‌بندی	کابل طرف کامپیوتر	
سفید نارنجی	(+TD)		(+TD)	سفید نارنجی
نارنجی	(–TD)		(–TD)	نارنجی
سفید سبز	(+RD)		(+RD)	سفید سبز
آبی	(NC)		(NC)	آبی
سفید آبی	(NC)		(NC)	سفید آبی
سبز	(–RD)		(–RD)	سبز
سفید قهوه‌ای	(NC)		(NC)	سفید قهوه‌ای

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.

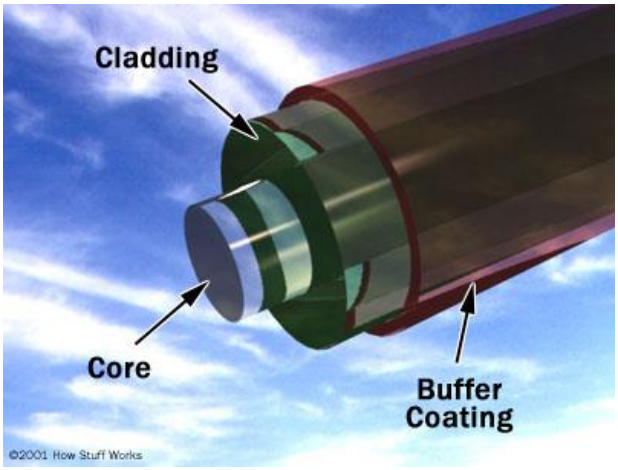
فیبر نوری:

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.

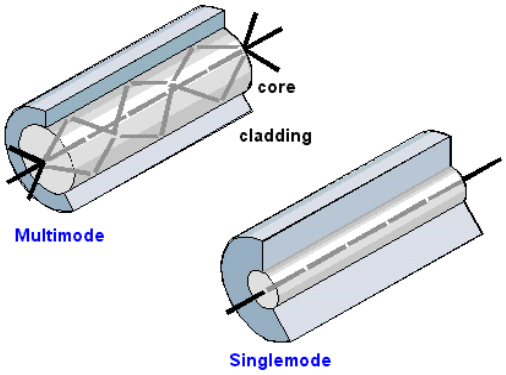
روکش (Cladding): بخش خارجی فیبر بوده که دور تا دور هسته را دربرمی‌گیرد و باعث برگشت نور منعکس‌شده به هسته می‌گردد.

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)

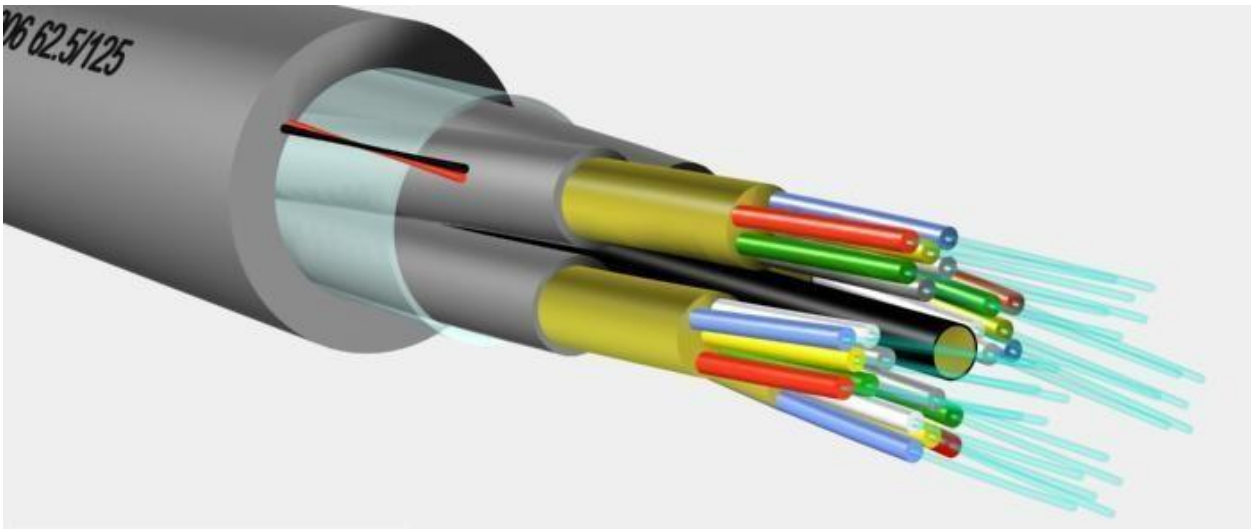


فیبر نوری به سه دسته کلی تقسیم می‌شود:

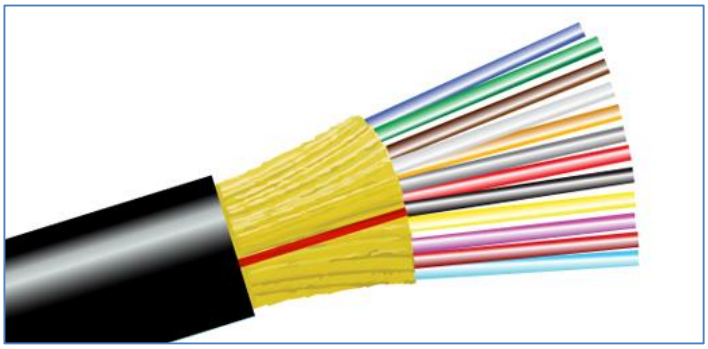
- Breakout
- Distribution
- Interconnect

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:



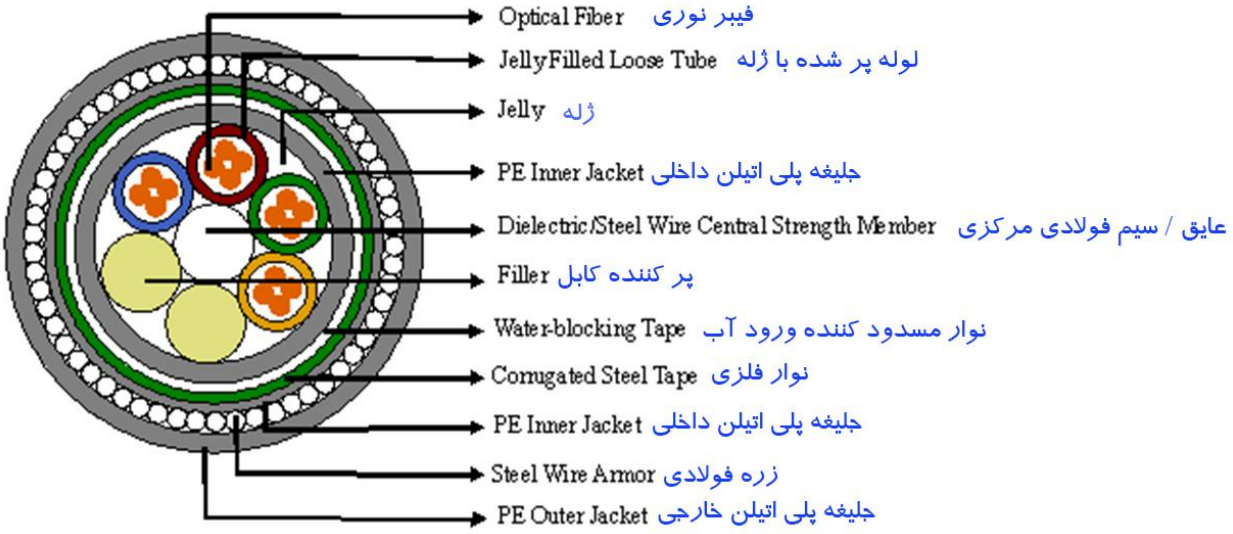
این نوع کابل‌ها به نسبت کابل قبلی کمی خم می-شوند و تعداد رشته‌ها در آن زیاد است و برای ارتباط کابل‌های Backbone با یک rack به کار می‌رود که شکل آن را می‌توانید در زیر مشاهده کنید.

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.

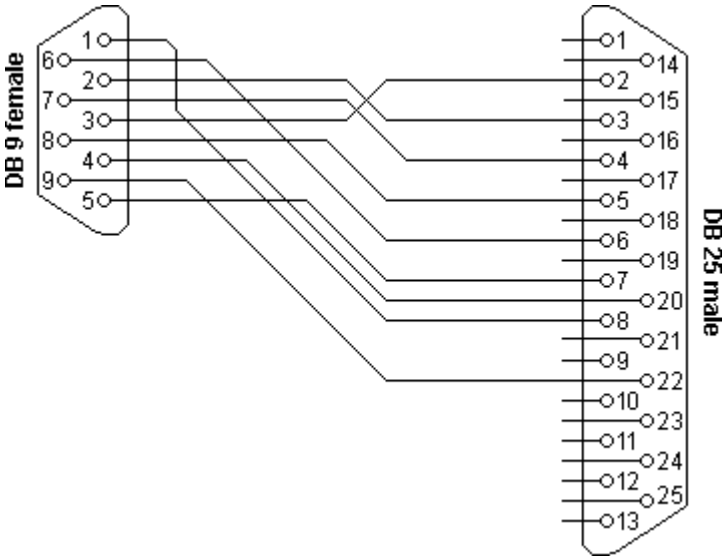
- DTE (Data Terminal Equipment)
- DCE (Data Communications Equipment)

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:

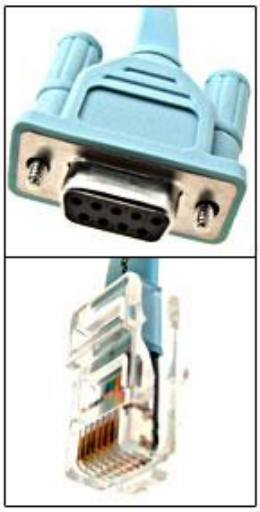
این کابل در شبکه‌های Wan بیشترین کاربرد را دارند.

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.

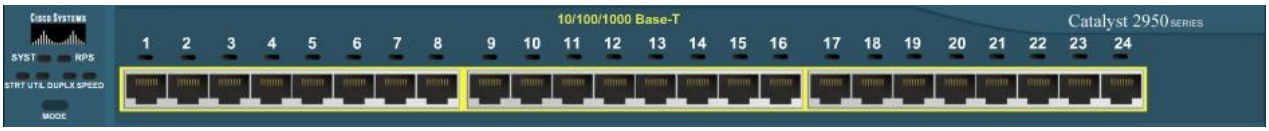
در شبکه‌های بزرگ Switch ها جدول‌های خود را به اشتراک می‌گذارند تا هرکدام بدانند چه دستگاهی به کدام سوئیچ متصل است و با این کار ترافیک کمتری در شبکه ایجاد کنند.

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):

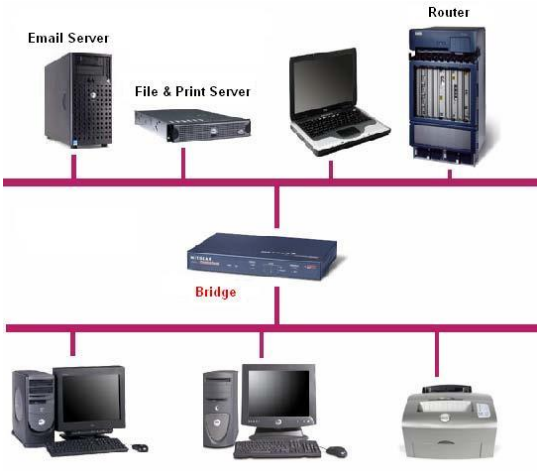
این نوع هاب با یک کارت همراه است و توسط این کارت می‌توان تعداد درگاه‌های آن را افزایش داد.

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):

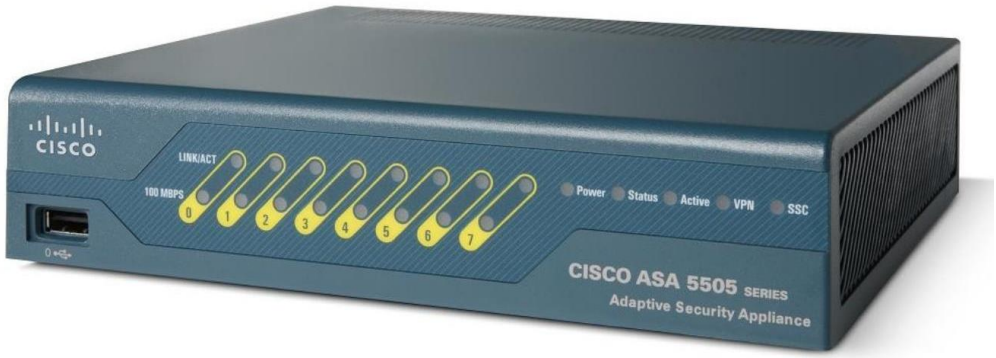
در این‌گونه سیستم‌ها، بسته‌ها بر اساس قانون خاصی متوقف می‌شوند. این قانون می‌تواند بستگی به جهت حرکت بسته، پروتکل خاص استفاده شده، آدرس فرستنده، شماره‌ی پورت پروتکل (مثلاً در TCP/IP)، واسطه‌ی فیزیکی و غیره طراحی شده باشد. این‌گونه فایروال، معمولاً در روتر (Router) انجام می‌شود. به‌عنوان مثال، از Configurable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

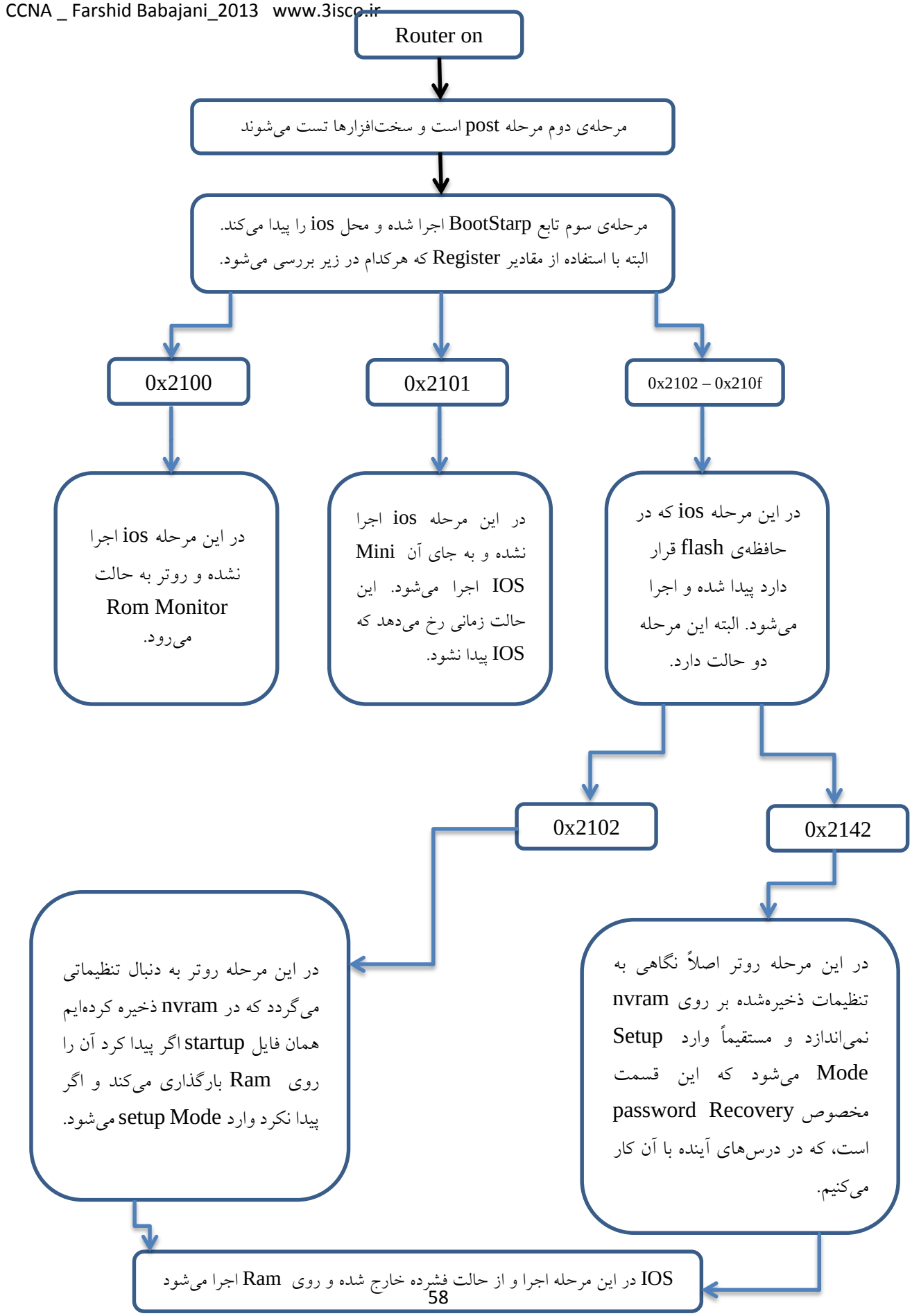
- **حافظه‌ی Nvram:**

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 **:**

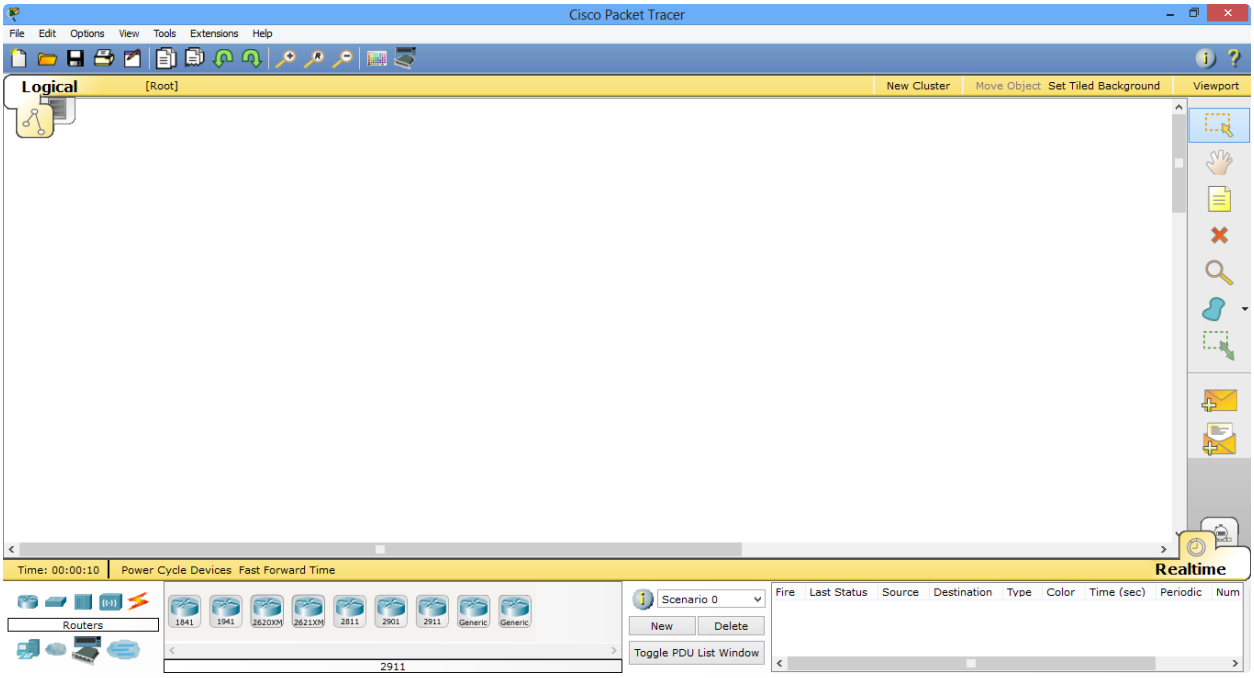
این نرم‌افزار را از لینک زیر دانلود کنید:

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.

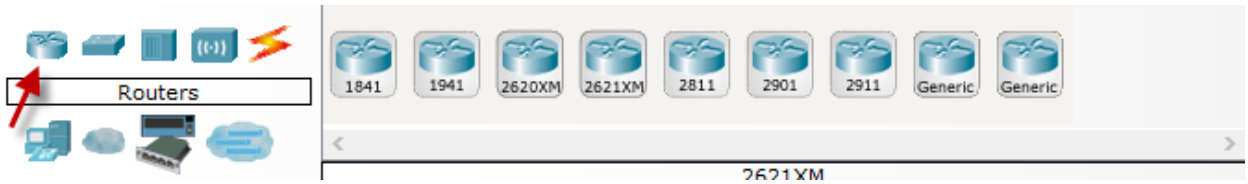


این نرم‌افزار از انواع روترها، سوئیچ‌ها، کابل‌ها، دستگاه‌های بی‌سیم و ... تشکیل شده است که یک دنیای مجازی را برای ما ایجاد می‌کند، البته تمام کارهای این نرم‌افزار در واقعیت هم، به همین صورت است.

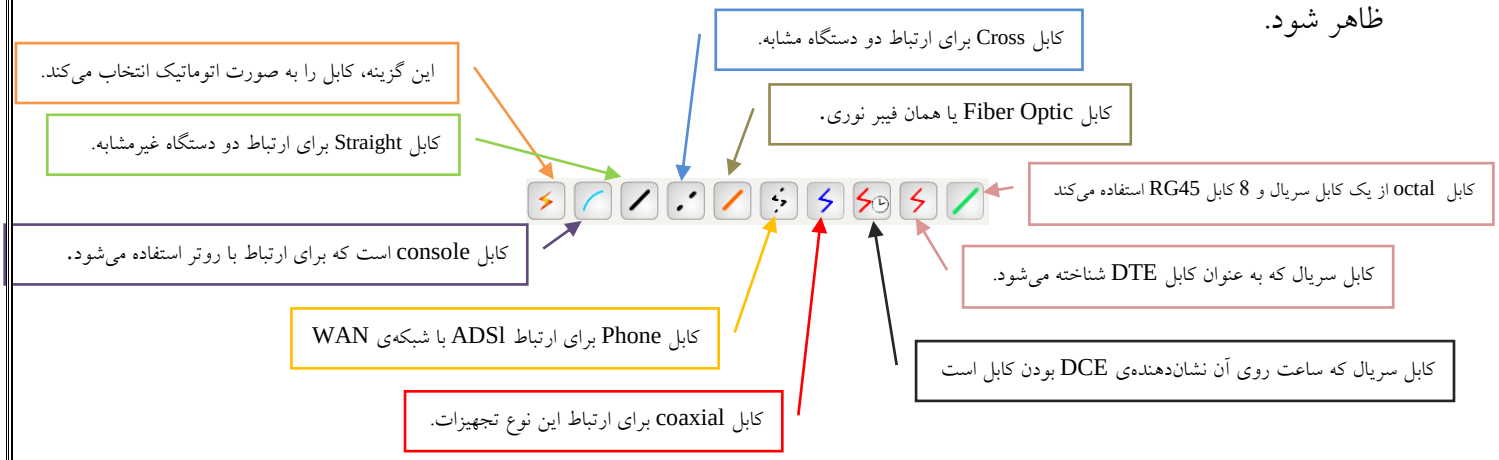
خوب با ابزارهای این نرم‌افزار آشنا می‌شویم.

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.

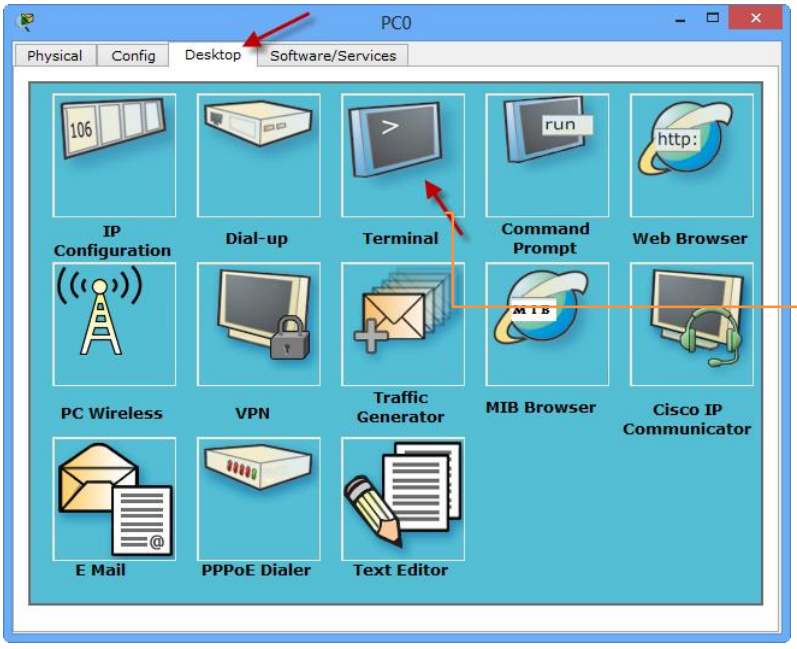


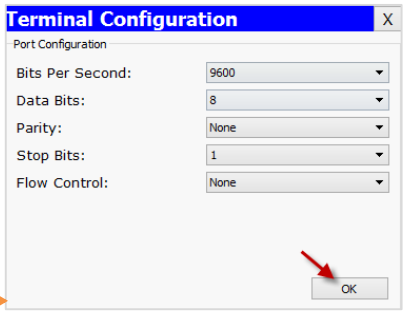
همان‌طور که مشاهده می‌کنید، انواع کابل در این قسمت وجود دارد، البته این کابل‌ها را در درس‌های قبلی توضیح دادیم.

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.

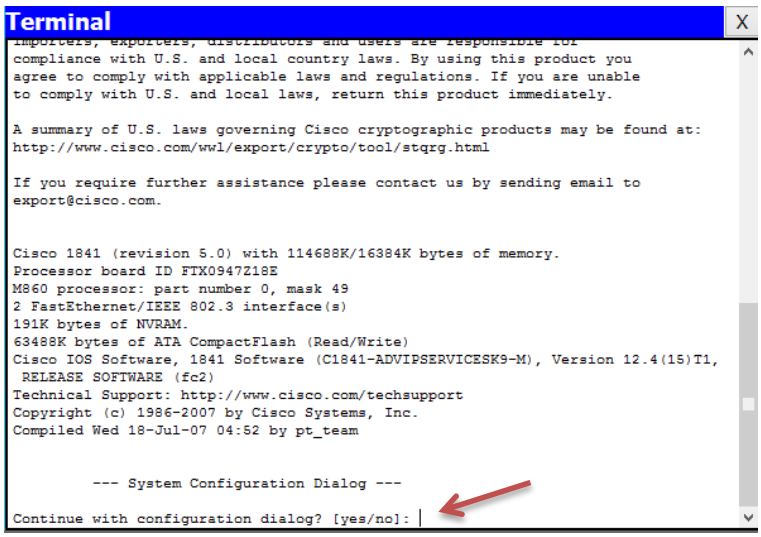
پیکربندی IOS:

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

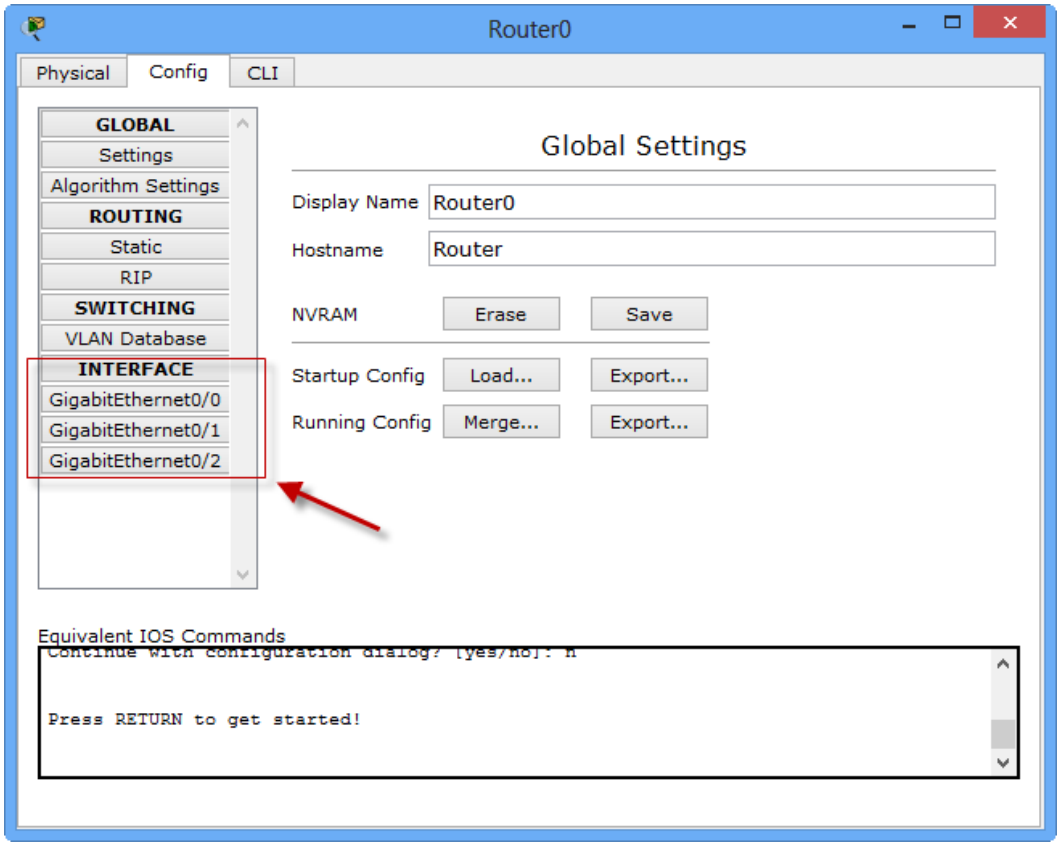
این پورت‌ها، پورت‌های مجازی می‌باشند که روی هر پورت فیزیکی قرار دارند و به صورت 0/0.? هستند.

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:

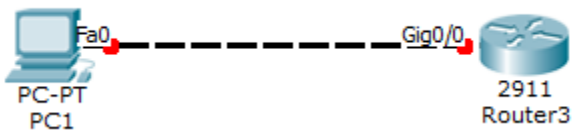
```
Router(config)#Line aux 0
Router(config-line)#password 123
Router(config-line)#login
```

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.

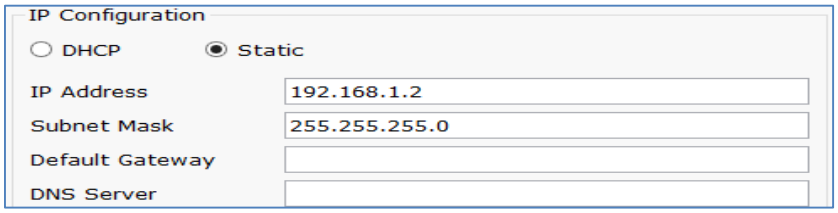
در اینجا تمام این 15 پورت را انتخاب و همه‌ی آن‌ها را فعال می‌کنیم، و روی همه آن‌ها رمز قرار می‌دهیم:

```
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.

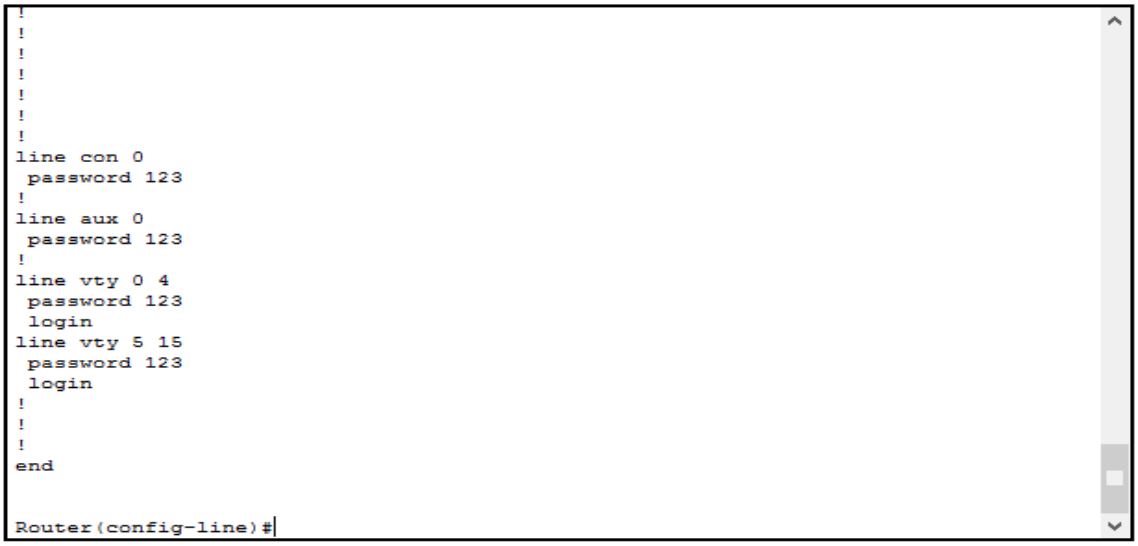
```
Telnet 192.168.1.1
```

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؟

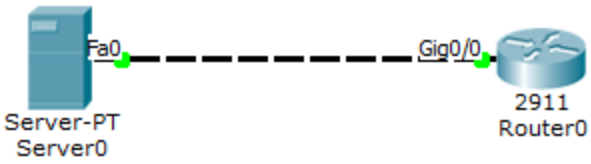
```
Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]
```

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.

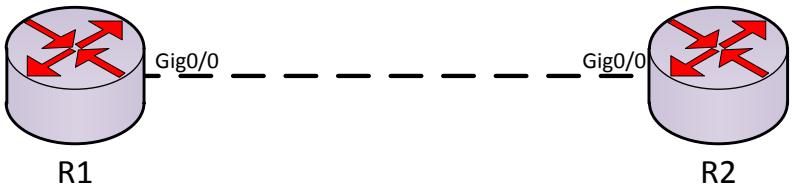
مسیریابی (IP Routin)

: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

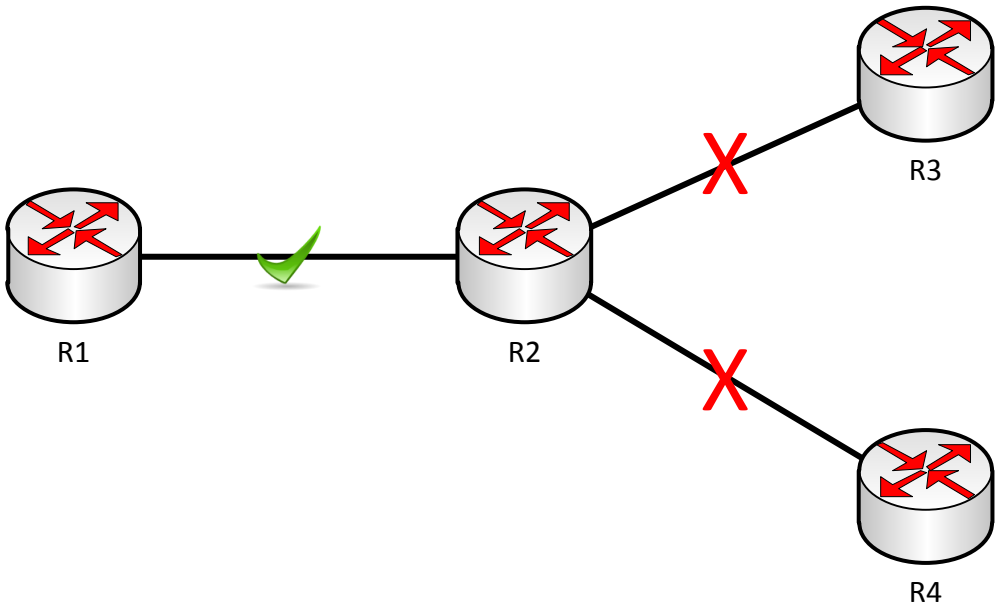
192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C 192.168.1.0/24 is directly connected, GigabitEthernet0/0
L 192.168.1.1/32 is directly connected, GigabitEthernet0/0

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:

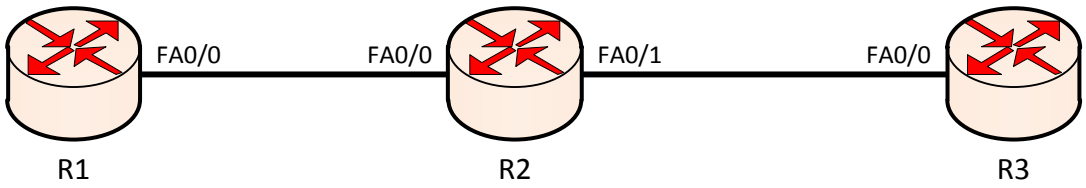
- **IP Route**
- **Defualt Route**

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)
```

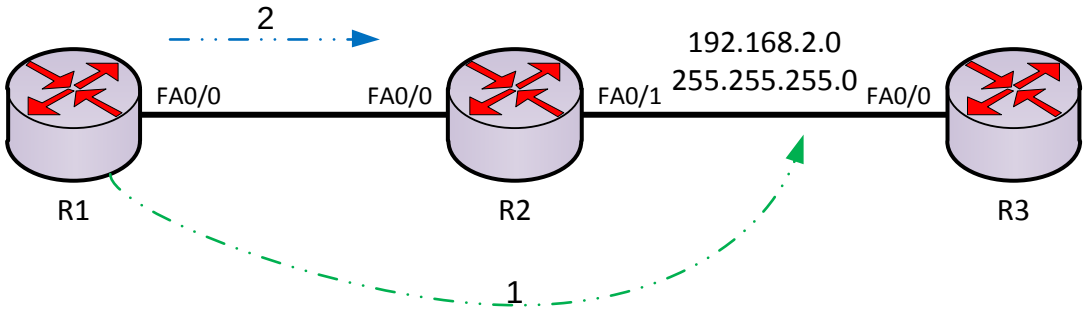
به این موضوع توجه کنید که R1 فقط به شبکه‌های متصل به خودش دسترسی دارد و این شبکه‌ها را به صورت شبکه‌ی connected در جدول روتینگ خود ثبت می‌کند. حالا موقع این است که شبکه‌های غیر محلی را به روتر معرفی کنیم.

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
```

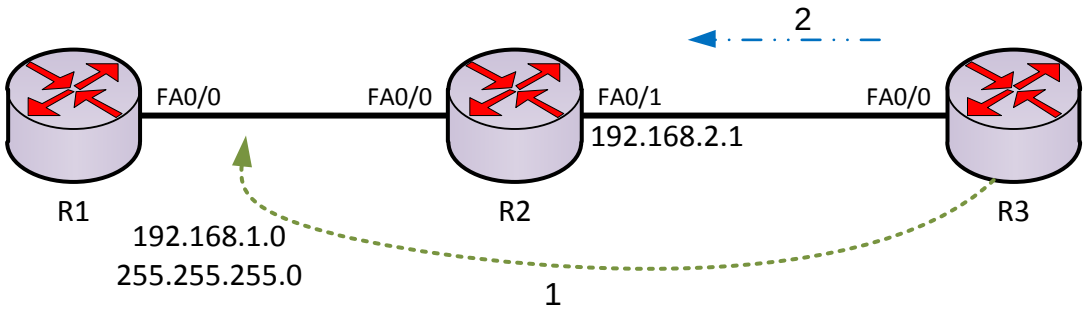
این دستور را به این صورت بخوانید (همراه با شکل بخوانید)، بگویید: برو به شبکه 192.168.2.0 با SubnetMask، 255.255.255.0 از 192.168.1.2 عبور کن. در شکل زیر می‌توانید این موضوع را مشاهده کنید.



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.

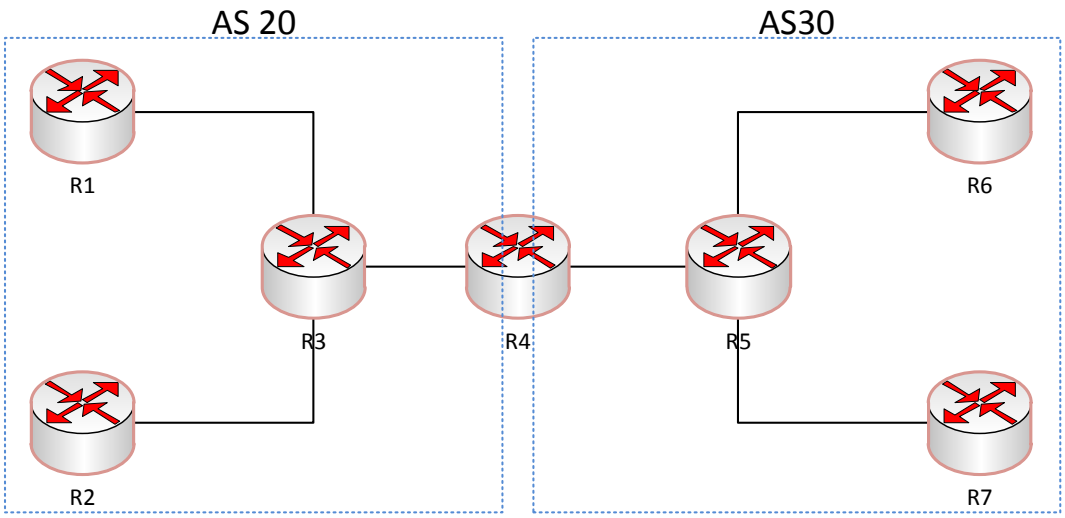
2–Dynamic Routing:

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.

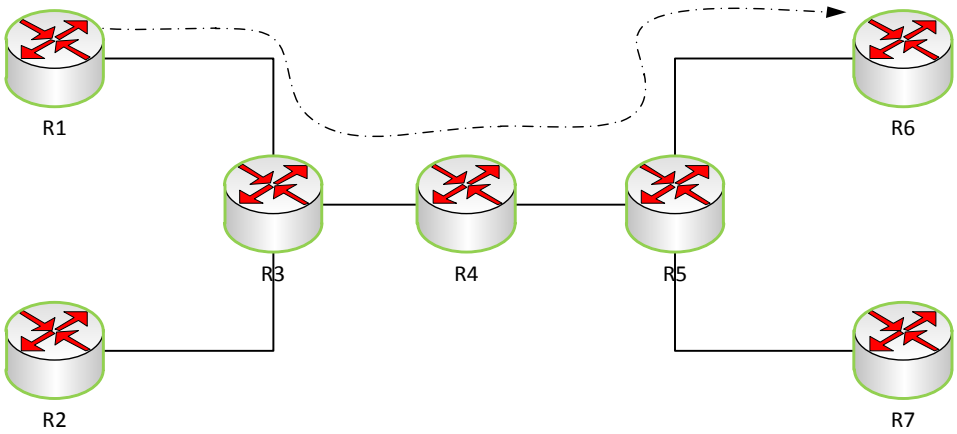
Dynamic Routing به سه دسته‌ی کلی تقسیم می‌شوند که هر 3 را باهم مورد بررسی قرار می‌دهیم:

- ✓ **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:

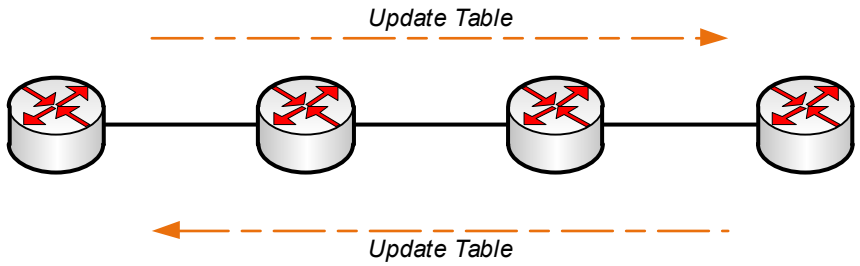


در این پروتکل‌ها اگر روتری، روتر کناری خود را بشناسد، می‌تواند بهترین مسیر را از روتر کناری خود دریافت کند. روتینگ پروتکل‌های RIP و IGRP از این نوع می‌باشند.

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.