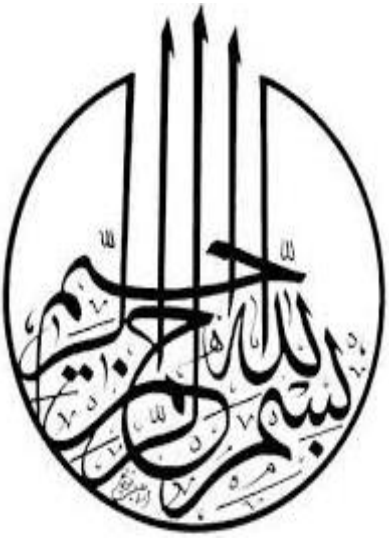

بسم الله الرحمن الرحيم

آزمایشگاه شبکه های کامپیوتری

(آموزش کاربردی نرم افزار شبیه ساز شبکه)

Cisco Packet Tracer

فاطمه صالح احمدی

شکر خدا که هر چه طلب کردم از خدا بر منتهای همت خود کامران شدم

تقدیم به همه پدران ، مادران و به محضر ارزشمند پدر و مادر عزیزم به خاطر همه ی تلاشهای محبت آمیز ی که در دوران مختلف زندگی ام انجام داده اند و بامهربانی چگونه زیستن را به من آموخته اند.

فهرست مطالب

فصل اول ۱۵

آشنایی با مفاهیم اولیه شبکه ۱۵

تاریخچه شبکه ۱۷

شبکه کامپیوتری و انواع آن..... ۱۹

تعریف شبکه ۱۹

تقسیم بندی شبکه ها ۱۹

تقسیم بندی بر اساس نوع وظایف..... ۱۹

تقسیم بندی بر اساس توپولوژی ۲۱

توپولوژی خطی یا اتوبوسی ۲۲

مزایای توپولوژی خطی ۲۲

معایب توپولوژی خطی ۲۳

توپولوژی ستاره ای ۲٤

مزایای توپولوژی ستاره ای..... ۲٤

معایب توپولوژی ستاره ای..... ۲۵

توپولوژی حلقوی ۲۵

مزایای توپولوژی حلقوی..... ۲٦

معایب توپولوژی حلقوی ۲۷

تقسیم بندی بر اساس حوزه جغرافی تحت پوشش ۲۸

رسانه های انتقال در شبکه ۲۹
کابل زوج سیم بهم تابیده ۲۹
مزایای کابل های بهم تابیده..... ۳۱
معایب کابل های بهم تابیده..... ۳۱
رنگ بندی در کابل ها و نوع استاندارد استفاده آن ها..... ۳۲
کابل کواکسیال..... ۳۳
مزایای کابل های کواکسیال..... ۳٤
معایب کابل های کواکسیال..... ۳٤
فیبر نوری ۳٥
مزایای فیبر نوری ۳٦
معایب فیبر نوری ۳٦
کابل های استفاده شده در شبکه های اترنت..... ۳۷
مدلOSI ۳۷
پروتکل های پشته ای ۳۹
لایهNetwork Interface ٤۱
اترنت چیست؟..... ٤٤
واسطهای شبکه هاب..... ٤۷
سوییچ ٤۸
نحوه کار سوییچ..... ٤۹
روتر(مسیریاب) ٥۱
انواع روتر ٥۳

پورت های کنسول و AUX روتر ٥٤
نحوه کار کرد یک روتر ٥٤
آدرس فیزیکی یا مک آدرس ٥٥
آدرس منطقی یا آدرس IP..... ٥٦
IP نسخه ۴ ..... ٥٧
IPنسخه۶..... ٥٨
کلاسهای آدرس IP..... ٥٩
Loop Back..... ٦٠
Multicasting..... ٦٢
IDهای شبکه ٦٣
Subnetmaskچیست؟..... ٦٥
CIDRچیست؟..... ٦٥
Wild Card Maskچیست؟ ٦٧
Default gateway..... ٦٨
معرفی پروتکل های مسیریابی یا روتینگ ٦٨
بردار– فاصله ٦٨
پروتوکلهای های حالت پیوند ٦٩
پروتوکل های مسیریابی ترکیبی ٧٠
Classless routing و Classful ٧٢
VLSM..... ٧٢
خصوصیاتVLSM ٧٣
مسیر دهی ایستا و پویا ٧٨
پروتوکلهای کاربردی در شبکه و کارآیی آن ها ٧٩

دستورات پر کاربرد در شبکه ۸۱
دستورPing ۸۲
دستور Tracert ۸۲
دستور ipconfig ۸۲
دستورGETMAC ۸۲
دستورroute ۸۳
دستورARP ۸۳
فصل دوم: آموزش کار با نرم افزار Packet tracer ۸٤
معرفی نرم افزار ۸۵
نصب نرم افزار در ویندوز و لینوکس ۸٦
نمایی از محیط نرم افزار ۸۷
برنامه جادوگر(Wizard) فعالیت ۸۸
ویژگی های Packet Tracer ۸۹
پروتوکلهای مورد حمایتPacket Tracer ۸۹
تشریح بخش های نرم افزار Packet Tracer ۹۰
نمونه ابزارهای در دسترس ۹۲

شروع کار ۹۳
اضافه کردن دستگاه به صفحه نرم افزار ۹۳
برگه Physical ۹۵
برگهConfig..... ۹۶
برگهCLI ۹۷
برگهDesktop ۱۰۰
معرفی تعدادی از تنظیمات برگهِ Desktop..... ۱۰۱
تنظیمIp Configuration..... ۱۰۱
بخش Terminal ۱۰۲
بخشCMD یا Command Prompt..... ۱۰۲
بخشSimulation ۱۰۳
تنظیم علاقمندیها ۱۰۶
ایجاد اتصالات ۱۰۷
وضعیت اتصال ۱۰۹
تجهیزات و دستگاه های نرم افزار Packet Tracer ۱۱۰
روتر ها ۱۱۰
سوئیچ ها ۱۱۱
سایر دستگاه ها..... ۱۱۲
شخصی یا سفارشی سازی دستگاه ها با ماژول وافزودن ماژولها..... ۱۱۳
قرار داد نام گذاری..... ۱۱۴
ساخت یک دستگاه شخصی..... ۱۱۷

پیکر بندی سوئیچ ۱۲۲
Vlan ۱۲۵
انواع پورت در سوئیچ ۱۲۶
VLAN trunks ۱۲۶
اتصال کامپیوتر به سوئیچ ۱۳۰
پیکربندی روتر ۱۳۴
ROM ۱۴۵
Nonvolatile RAM (NVRAM) ۱۴۵
فصل سوم ۱۴۷
سناریوهای مهم Packet Tracer ۱۴۷
سناریویStatic routing یا مسیریابی دستی ۱۴۸
معرفی پروتکل مسیریابیOpen Shortest Path First ۱۵۳
راه اندازی کامل سناریوی پیاده سازی OSPF ۱۵۸
انجام تنظیمات مربوط به پروتکل OSPF روی روتر R۱ ..... ۱۵۸
انجام تنظیمات مربوط به پروتکل OSPF روی روتر R۳ ..... ۱۶۰
مشاهده Routing Table های موجود روی R۱ ..... ۱۶۱
اطمینان از عملکرد درست و تست ارتباط بین شبکه ها با استفاده از دستورPing .. ۱۶۲
راه اندازی کامل سناریو پیاده سازی پروتکلRIPv۲ ..... ۱۶۳
انجام تنظیمات RIPv۲برای R۱ ..... ۱۶۵
انجام تنظیمات RIPv۲برای R۲ ..... ۱۶۶

اطمینان از عملکرد درست و تست ارتباط بین شبکه ها با استفاده از دستور Ping .. ۱۶۸
تفاوت RIPv۱ و RIPv۲ در چیست ؟ ۱۶۹
ویژگی های ۱ Routing Information Protocol Version ۱۶۹
ویژگی های ۲ Routing Information Protocol Version ۱۷۰
راه اندازی Mailserver در Packet Tracer ۱۷۲
راه اندازی DNS Server & WEB ۱۸۰
منظور از Routing Loop چیست ؟ ۱۸۶
راه اندازی پروتوکل EIGRP ۱۹۰
راه اندازی کامل پروتکل Interior Gateway Routing Protocol یا IGRP . ۱۹۳
انجام تنظیمات IGRP بر روی R۱ ..... ۱۹۵
انجام تنظیمات IGRP بر روی R۳ ..... ۱۹۷
مشاهده Routing Table های موجود در R۱ ..... ۱۹۸
اطمینان از عملکرد درست و تست ارتباط بین شبکه ها با استفاده از دستور Ping ۱۹۹
ترجمه آدرس ها یا Address Translation ۲۰۰
انواع سیستم ترجمه آدرس ها یا Address Translation ۲۰۱
NAT یا Network Address Translation ۲۰۱
NAT دینامیک یا Dynamic NAT ۲۰۳
PAT یا Port Address Translation ۲۰۴

راه اندازی NAT وPAT ۲۰۵
کاربردTelnet یا همان دسترسی از راه دور ۲۱۰
راه اندازیSSH ۲۱۳
نحو ه ی فعال سازیSSH ۲۱٤
تغییر نسخه مورد استفاده..... ۲۱٤
راه اندازیDHCP ۲۱٥
راه اندازیVOIP ۲۱۷
راه اندازی TFTP سرور..... ۲۲۷
منابع ۲۲۹

مقدمه مؤلف

در آستانه تحول بنیادین علمی و اقتصادی برای رسیدن به خود باوری و شکوفا شدن استعدادهای رهپویان علم، دانشجویان، مهندسین و کاربران IT، براین باور شدم که در عرصه تکنولوژی و کاربرد فنآوری نیاز است، به همت دست اندرکاران علم روز و رایانه، مقوله ای را به شرح زیر به منظور استفاده متقاضیان ارائه دهم.با توجه به کمبودهای موجود در دانشگاهها و مراکز آموزشی از نظر وجود محتوای علمی و عملی در رشته رایانه و نیازهای موجود، این کتاب براساس اطلاعات روز در زمینه شبکه های رایانه ای و آموزش نرم افزار شبیه سازی شبکه(PacketTracer) با زبانی ساده و ارائه مطالب بصورت عملی و کاربردی برای کاربران IT، دانشجویان رشته کامپیوتر و همچنین دانش آموزان علاقمند حاضر در مراکز فنی و حرفه ای تهیه و تنظیم شده است و با بهره گیری از مثال ها و تمرینات تصویری، امید است بتواند نیاز این عزیزان را برطرف نماید.این کتاب به همت تلاش یک ساله و به قلم این حقیر که سابقه کار بعنوان مربی شبکه و کامپیوتر در دانشگاه آزاد اسلامی واحد دشتستان- بوشهر و مسوول اتوماسیون و هوشمند سازی و متخصص رایانه در سازمان آموزش و پرورش استان بوشهر- برازجان را دارم و فارغ التحصیل کارشناسی ارشد فنآوری اطلاعات می باشم، تهیه و تنظیم شده است.امید است به منظر ارائه بهتر کتاب در چاپ های بعد از نظر کاربران عزیز هم استفاده شود.

فاطمه صالح احمدی

Certificates: CCNA,CEH,
NETWORK+,MIKROTIK,LINUX,MCITP
fatemehsalehahmadi۲٤@gmail.com

فصل اول

آشنایی با مفاهیم اولیه شبکه

تاریخچه شبکه

پس از پرتاب نخستین ماهواره اتحاد جماهیر شوروی به فضا و هنگامی که رقابت سختی از نظر تسلیحاتی بین دو ابرقدرت آن زمان جریان داشت و دنیا در دوران جنگ سرد به سر می برد، وزارت دفاع آمریکا در واکنش به این اقدام رقیب نظامی خود، آژانس پروژه های تحقیقاتی پیشرفته یا آرپا[۱] را تاسیس کرد. یکی از پروژه های مهم این آژانس تامین ارتباطات در زمان جنگ جهانی احتمالی تعریف شده بود. در همین سال ها در مراکز تحقیقاتی غیرنظامی که در امتداد دانشگاه ها بودند، تلاش برای اتصال کامپیوترها به یکدیگر در جریان بود. در آن زمان کامپیوتر های مین فریم[۲] از طریق ترمینال ها به کاربران سرویس می دادند. در اثر اهمیت یافتن این موضوع آژانس آرپا منابع مالی پروژه اتصال دو کامپیوتر از راه دور به یکدیگر را در دانشگاه ام. آی.تی بر عهده گرفت. در اواخر سال ۱۹۶۰ اولین شبکه کامپیوتری بین چهار کامپیوتر که دو تای آن ها در ام.آی.تی، یکی در دانشگاه کالیفرنیا و دیگری در مرکز تحقیقاتی استنفورد قرار داشتند، راه اندازی شد. این شبکه آرپانت نامگذاری شد. در سال ۱۹۶۵ نخستین ارتباط راه دور بین انشگاه ام.آی.تی و یک مرکز دیگر نیز برقرار شد.

تا این سال ها شبکه آرپانت به امور نظامی اختصاص داشت، اما در سال ۱۹۲۷ به عموم معرفی شد. در این سال شبکه آرپانت مراکز کامپیوتری بسیاری از دانشگاه ها و مراکز تحقیقاتی را به هم متصل کرده بود. در سال ۱۹۲۷ نخستین نامه الکترونیکی از طریق شبکه منتقل شد. در این سال ها حرکتی غیرانتفاعی به نام مریت[۳] که چندین دانشگاه بنیانگذار آن بوده اند، مشغول توسعه روش های اتصال کاربران ترمینال ها به کامپیوتر

---

۱ ARPA
۲ Mainframe
۳ MERIT

مرکزی یا میزبان بود. مهندسان پروژه "مریت" در تلاش برای ایجاد ارتباط بین کامپیوترها، مجبور شدند تجهیزات لازم را خود طراحی کنند. آنان با طراحی تجهیزات واسطه برای مینی کامپیوتر DECPDP-۱۱ نخستین بستر اصلی[۴] شبکه کامپیوتری را ساختند. تا سال ها نمونه های اصلاح شده این کامپیوتر با نام پی.سی.پی[۵] نقش میزبان را در شبکه ها ایفا می کرد. نخستین شبکه از این نوع که چندین ایالت را به هم متصل می کرد "میچنت[۶]" نام داشت. روش اتصال کاربران به کامپیوتر میزبان در آن زمان به این صورت بود که یک نرم افزار خاص روی کامپیوتر مرکزی اجرا می شد و ارتباط کاربران را برقرار می کرد اما در سال ۱۹۷۶ نرم افزار جدیدی به نام هرمس[۷] عرضه شد که برای نخستین بار به کاربران اجازه می داد از طریق یک ترمینال به صورت تعاملی مستقیماً به سیستم "مریت" متصل شوند. از وقایع مهم تاریخچه شبکه های کامپیوتری، ابداع روش سوئیچینگ بسته ای است. قبل از معرفی شدن این روش ازسوئیچینگ مداری برای تعیین مسیر ارتباطی استفاده می شد اما در سال ۱۹۷۴ با پیدایش پروتکل ارتباطی TCP/IP این پروتکل جایگزین پروتکل NCP شد و به پروتکل استاندارد برای آرپانت تبدیل شد. با این تغییر و تحول، شبکه های زیادی به بخش تحقیقاتی این شبکه متصل شدند و آرپانت به اینترنت تبدیل شد.

[۴] Backdone
[۵] PCP
[۶] MICHNET
[۷] HERMES

شکل ۱-۱

شبکه کامپیوتری و انواع آن

تعریف شبکه

یک شبکه شامل مجموعه ای از دستگاهها (کامپیوتر ، چاپگر و ...) بوده که با استفاده از یک روش ارتباطی (کابل ، امواج رادیوئی ، ماهواره) و به منظور اشتراک منابع فیزیکی مانند چاپگر و منابع منطقی (فایل) به یکدیگر متصل می گردند. شبکه ها می توانند با یکدیگر نیز مرتبط شده و شامل زیر شبکه هائی باشند.

تقسیم بندی شبکه ها

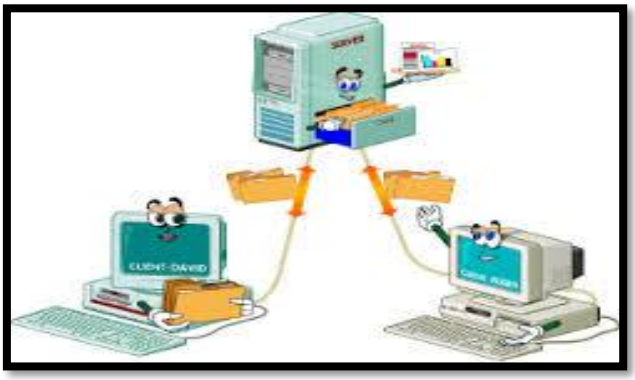
شبکه های کامپیوتری را بر اساس مولفه های متفاوتی تقسیم بندی می نمایند. در ادامه به برخی از متداولترین تقسیم بندی های موجود اشاره می گردد .

تقسیم بندی بر اساس نوع وظایف

کامپیوترهای موجود در شبکه را با توجه به نوع وظایف مربوطه به دو گروه عمده سرویس دهندگان یا سرورها[۸] و یا سرویس گیرندگان [۹] یا کلاینت ها تق سیم می نمایند. کامپیوترهائی در شبکه که برای سایر کامپیوترها سرویس ها و خدماتی را ارائه می نمایند ، سرویس دهنده نامیده می گردند. کامپیوترهائی که از خدمات و سرویس های ارائه شده توسط سرویس دهندگان استفاده می کنند ، سرویس گیرنده نامیده می شوند . در شبکه های کلاینت/سرور ، یک کامپیوتر در شبکه

[۸] Servers
[۹] Clients

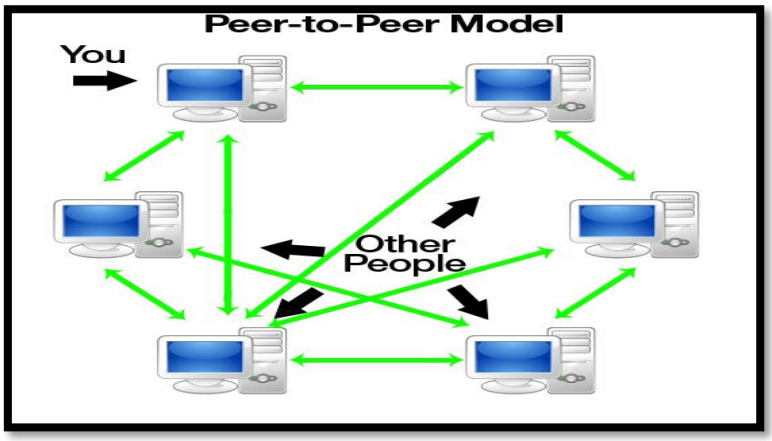
نمی تواند هم به عنوان ســـرویس دهنده و هم به عنوان ســـرویس گیرنده ، ایفای وظیفه نماید.



شکل۲-۱

در شبکه های نظیر به نظیر [۱۰]، یک کامپیوتر می تواند هم بصورت سرویس دهنده و هم بصورت سرویس گیرنده ایفای وظیفه نماید.

[۱۰] Peer-To-Peer



شکل۳-۱

تقسیم بندی بر اساس توپولوژی

الگوی هندسی استفاده شده جهت اتصال کامپیوترها ، توپولوژی نامیده می شود. توپولوژی انتخاب شده برای پیاده سازی شبکه ها، عاملی مهم در جهت کشف و برطرف نمودن خطاء در شبکه خواهد بود. انتخاب یک توپولوژی خاص نمی تواند بدون ارتباط با محیط انتقال و روش های استفاده از خط مطرح گردد. نوع توپولوژی انتخابی جهت اتصال کامپیوترها به یکدیگر ، مستقیما" بر نوع محیط انتقال و روش های استفاده از خط تاثیر می گذارد. با توجه به تاثیر مستقیم توپولوژی انتخابی در نوع کابل کشی و هزینه های مربوط به آن ، می بایست با دقت و تامل به انتخاب توپولوژی یک شبکه همت گماشت . سه نوع توپولوژی رایج در شبکه های محلی استفاده می گردد :

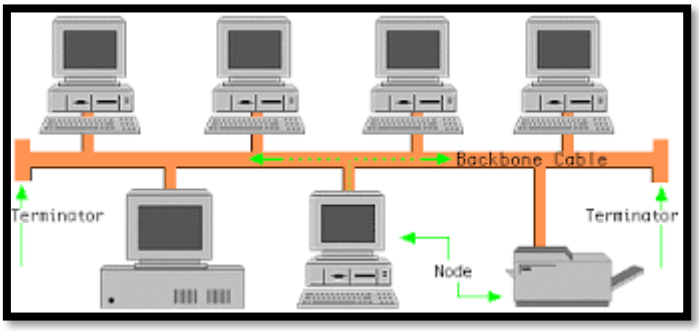
- خطی[۱۱]

[۱۱] BUS

- ستاره ای[۱۲]
- حلقوی[۱۳]

توپولوژی خطی یا اتوبوسی

یکی از رایجترین توپولوژی ها برای پیاده سازی شبکه های محلی[۱۴] است . در مدل فوق از یک کابل به عنوان ستون فقرات اصلی در شبکه استفاده شده و تمام کامپیوترهای موجود در شبکه (سرویس دهنده ، سرویس گیرنده) به آن متصل می گردند.



شکل۴-۱

مزایای توپولوژی خطی

- کم بودن طول کابل: بدلیل استفاده از یک خط انتقال جهت اتصال تمام کامپیوترها ، در توپولوژی فوق از کابل کمی استفاده می شود.موضوع فوق

[۱۲] STAR
[۱۳] RING
[۱۴] LAN

باعث پایین آمدن هزینه نصب و ایجاد تسهیلات لازم در جهت پشتیبانی شبکه خواهد بود.

- ساختار ساده : توپولوژی خطی دارای یک ساختار ساده است . در مدل فوق صرفا" از یک کابل برای انتقال اطلاعات استفاده می شود.
- توسعه آسان : یک کامپیوتر جدید را می توان براحتی در نقطه ای از شبکه اضافه کرد. در صورت اضافه شدن ایستگاههای بیشتر در یک سگمنت ، می توان از تقویت کننده هائی به نام تکرارکننده[۱۵] استفاده کرد.

معایب توپولوژی خطی

- مشکل بودن عیب یابی : با اینکه سادگی موجود در تویولوژی خطی امکان بروز اشتباه را کاهش می دهند، ولی در صورت بروز خطاء کشف آن ساده نخواهد بود. در شبکه هائی که از توپولوژی فوق استفاده می نمایند ، کنترل شبکه در هر گره دارای مرکزیت نبوده و در صورت بروز خطاء می بایست نقاط زیادی به منظور تشخیص خطاء بازدید و بررسی گردند.
- ایزوله کردن خطاء مشکل است : در صورتی که یک کامپیوتر در توپولوژی فوق دچار مشکل گردد ، می بایست کامپیوتر را در محلی که به شبکه متصل است رفع عیب نمود. در موارد خاص می توان یک گره را از شبکه جدا کرد. در حالتیکه اشکال در محیط انتقال باشد ، تمام یک سگمنت می بایست از شبکه خارج گردد.
- ماهیت تکرارکننده ها : در مواردیکه برای توسعه شبکه از تکرارکننده ها استفاده می گردد، ممکن است در ساختار شبکه تغییراتی نیز داده شود.

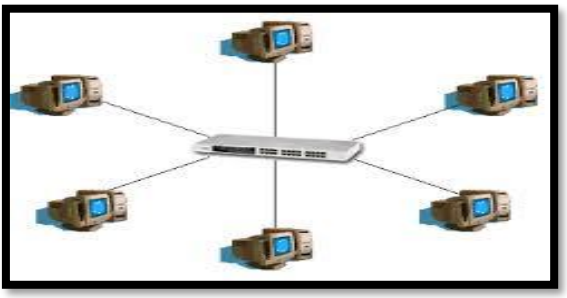
---

[۱۵] Repeater

موضوع فوق مستلزم بکارگیری کابل بیشتر و اضافه نمودن اتصالات مخصوص شبکه است .

توپولوژی ستاره ای

در این نوع توپولوژی همانگونه که از نام آن مشخص است ، از مدلی شبیه "ستاره" استفاده می گردد. در این مدل تمام کامپیوترهای موجود در شبکه معمولا" به یک دستگاه خاص با نام " هاب " متصل خواهند شد.



شکل۵-۱

مزایای توپولوژی ستاره ای

- سادگی سرویس شبکه: توپولوژی ستاره ای شامل تعدادی از نقاط اتصالی در یک نقطه مرکزی است . ویژگی فوق تغییر در ساختار و سرویس شبکه را آسان می نماید.
- در هر اتصال یک دستگاه: نقاط اتصالی در شبکه ذاتا" مستعد اشکال هستند. در توپولوژی ستاره ای اشکال در یک اتصال ، باعث خروج آن خط از شبکه و سرویس و اشکال زدائی خط مزبور است . عملیات فوق تاثیری در عملکرد سایر کامپیوترهای موجود در شبکه نخواهد گذاشت .

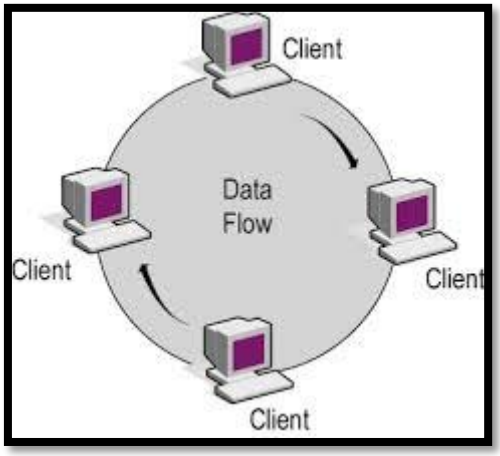
- **کنترل مرکزی و عیب یابی: با توجه به این مسئله که نقطه مرکزی مستقیما" به هر ایستگاه موجود در شبکه متصل است ، اشکالات و ایرادات در شبکه بسادگی تشخیص و مهار خواهند گردید.**
- **روش های ساده دستیابی : هر اتصال در شبکه شامل یک نقطه مرکزی و یک گره جانبی است . در چنین حالتی دستیابی به محیط انتقال جهت ارسال و دریافت اطلاعات دارای الگوریتمی ساده خواهد بود.**

معایب توپولوژی ستاره ای

- **زیاد بودن طول کابل : بدلیل اتصال مستقیم هر گره به نقطه مرکزی ، مقدار زیادی کابل مصرف می شود. با توجه به اینکه هزینه کابل نسبت به تمام شبکه ، کم است ، تراکم در کانال کشی جهت کابل ها و مسائل مربوط به نصب و پشتیبانی آن ها بطور قابل توجهی هزینه ها را افزایش خواهد داد.**
- **مشکل بودن توسعه : اضافه نمودن یک گره جدید به شبکه مستلزم یک اتصال از نقطه مرکزی به گره جدید است . با اینکه در زمان کابل کشی پیش بینی های لازم جهت توسعه در نظر گرفته می شود ، ولی در برخی حالات نظیر زمانیکه طول زیادی از کابل مورد نیاز بوده و یا اتصال مجموعه ای از گره های غیر قابل پیش بینی اولیه ، توسعه شبکه را با مشکل مواجه خواهد کرد.**
- **وابستگی به نقطه مرکزی : در صورتی که نقطه مرکزی (هاب) در شبکه با مشکل مواجه شود ، تمام شبکه غیرقابل استفاده خواهد بود.**

توپولوژی حلقوی

در این نوع توپولوژی تمام کامپیوترها بصورت یک حلقه به یکدیگر مرتبط می گردند. تمام کامپیوترهای موجود در شبکه (سرویس دهنده ، سرویس گیرنده) به یک کابل که بصورت یک دایره بسته است ، متصل می گردند. در مدل فوق هر گره به دو و فقط دو همسایه مجاور خود متصل است . اطلاعات از گره مجاور دریافت و به گره بعدی ارسال می شوند. بنابراین داده ها فقط در یک جهت حرکت کرده و از ایستگاهی به ایستگاه دیگر انتقال پیدا می کنند.



شکل۶-۱

مزایای توپولوژی حلقوی

- کم بودن طول کابل : طول کابلی که در این مدل بکار گرفته می شود ، قابل مقایسه به توپولوژی خطی نبوده و طول کمی را در بردارد. ویژگی فوق باعث

کاهش تعداد اتصالات (کانکتور) در شبکه شده و ضریب اعتماد به شبکه را افزایش خواهد داد.

- نیاز به فضائی خاص جهت انشعابات در کابل کشی نخواهد بود: بدلیل استفاده از یک کابل جهت اتصال هر گره به گره همسایه اش ، اختصاص محل هائی خاص به منظور کابل کشی ضرورتی نخواهد داشت .
- مناسب جهت فیبر نوری : استفاده از فیبر نوری باعث بالا رفتن نرخ سرعت انتقال اطلاعات در شبکه است. چون در توپولوژی فوق ترافیک داده ها در یک جهت است ، می توان از فیبر نوری به منظور محیط انتقال استفاده کرد.در صورت تمایل می توان در هر بخش ازشبکه از یک نوع کابل به عنوان محیط انتقال استفاده کرد . مثلا" در محیط های ادرای از مدل های مسی و در محیط کارخانه از فیبر نوری استفاده کرد.

معایب توپولوژی حلقوی

- اشکال در یک گره باعث اشکال در تمام شبکه می گردد: در صورت بروز اشکال در یک گره ، تمام شبکه با اشکال مواجه خواهد شد. و تا زمانی‌که گره معیوب از شبکه خارج نگردد ، هیچگونه ترافیک اطلاعاتی را روی شبکه نمی توان داشت .
- اشکال زدائی مشکل است : بروز اشکال در یک گره می تواند روی تمام گرههای دیگر تاثیر گذار باشد. به منظور عیب یابی می بایست چندین گره بررسی تا گره مورد نظر پیدا گردد.
- تغییر در ساختار شبکه مشکل است : در زمان گسترش و یا اصلاح حوزه جغرافیائی تحت پوشش شبکه ، بدلیل ماهیت حلقوی شبکه مسائلی بوجود خواهد آمد .

- **توپولوژی بر روی نوع دستیابی تاثیر می گذارد: هر گره در شبکه دارای مسئولیت عبور دادن داده ای است که از گره مجاور دریافت داشته است . قبل از اینکه یک گره بتواند داده خود را ارسال نماید ، می بایست به این اطمینان برسد که محیط انتقال برای استفاده قابل دستیابی است .**

تقسیم بندی بر اساس حوزه جغرافی تحت پوشش

شبکه های کامپیوتری با توجه به حوزه جغرافیائی تحت پوشش به سه گروه تقسیم می گردند :

- **شبکه های محلی (کوچک)یا LAN**
- **شبکه های متوسط یا شهری یا MAN**
- **شبکه های گسترده یا WAN**

شبکه های محلی: حوزه جغرافیائی که توسط این نوع از شبکه ها پوشش داده می شود ، یک محیط کوچک نظیر یک ساختمان اداری است . این نوع از شبکه ها دارای ویژگی های زیر می باشند :

- **توانائی ارسال اطلاعات با سرعت بالا**
- **محدودیت فاصله**
- **قابلیت استفاده از محیط مخابراتی ارزان نظیر خطوط تلفن به منظور ارسال اطلاعات**
- **نرخ پایین خطاء در ارسال اطلاعات با توجه به محدود بودن فاصله**

شبکه های شهری حوزه جغرافیائی که توسط این نوع شبکه ها پوشش داده می شود ، در حد و اندازه یک شهر و یا شهرستان است . ویژگی های این نوع از شبکه ها بشرح زیر است :

- پیچیدگی بیشتر نسبت به شبکه های محلی
- قابلیت ارسال تصاویر و صدا
- قابلیت ایجاد ارتباط بین چندین شبکه

شبکه های گسترده : حوزه جغرافیائی که توسط این نوع شبکه ها پوشش داده می شود ، در حد و اندازه کشور و قاره است . ویژگی این نوع شبکه ها بشرح زیر است :

- قابلیت ارسال اطلاعات بین کشورها و قاره ها
- قابلیت ایجاد ارتباط بین شبکه های محلی
- سرعت پایین ارسال اطلاعات نسبت به شبکه های محلی
- نرخ خطای بالا با توجه به گستردگی محدوده تحت پوشش

رسانه های انتقال در شبکه

در شبکه های محلی از چندین نوع کابل به عنوان محیط انتقال و به منظور ارسال اطلاعات استفاده می گردد. در برخی موارد ممکن است در یک شبکه صرفا" از یک نوع کابل استفاده و یا با توجه به شرایط موجود از چندین نوع کابل استفاده گردد. نوع کابل انتخاب شده برای یک شبکه به عوامل متفاوتی نظیر : توپولوژی شبکه، پروتکل و اندازه شبکه بستگی خواهد داشت . آگاهی از خصایص و ویژگی های متفاوت هر یک از کابل ها و تاثیر هر یک از آن‌ها بر سایر ویژگی های شبکه، به منظور طراحی و پیاده سازی یک شبکه موفق بسیار لازم است .

کابل زوج سیم بهم تابیده[۱۶]

[۱۶] Twisted pair

متداولترین نوع کابلی که در انتقال اطلاعات استفاده می گردد ، کابل های بهم تابیده می باشند. این نوع کابل ها دارای دو رشته سیم به هم پیچیده بوده که هر دو نسبت زمین دارای یک امپدانش یکسان می باشند. بدین ترتیب امکان تاثیر پذیری این نوع کابل ها از کابل های مجاور و یا سایر منابع خارجی کاهش خواهد یافت . کابل های بهم تابیده دارای دو مدل متفاوت : روکش دار و بدون روکش می باشند. کابل UTP[۱۷] نسبت به کابل STP[۱۸] بمراتب متداول تر بوده و در اکثر شبکه های محلی استفاده می گردد.کیفیت کابل های UTP متغیر بوده و از کابل های معمولی استفاده شده برای تلفن تا کابل های با سرعت بالا را شامل می گردد. کابل دارای چهار زوج سیم بوده و درون یک روکش قرار می گیرند. هر زوج با تعداد مشخصی پیچ تابانده شده تا تاثیر پذیری آن از سایر زوج ها و یاسایر دستگاههای الکتریکی کاهش یابد.

کاربرد	Type
فقط صوت (کابل های تلفن)	Cat ۱
داده با سرعت ۴ مگابیت در ثانیه	Cat ۲
داده با سرعت ۱۰ مگابیت در ثانیه	Cat ۳
داده با سرعت ۲۰ مگابیت در ثانیه	Cat ٤
داده با سرعت ۱۰۰ مگابیت در ثانیه	Cat ٥

جدول ۱-۱

[۱۷] UNSHEULEDE Twisted Pair
[۱۸] Sheilded Twisted Pair

کابل های UTP دارای استانداردهای متعددی بوده که در گروههای (Categories) متفاوت زیر تقسیم شده اند:

مزایای کابل های بهم تابیده :

- **سادگی و نصب آسان**
- **انعطاف پذیری مناسب**
- **دارای وزن کم بوده و براحتی بهم تابیده می گردند.**

معایب کابل های بهم تابیده :

- **تضعیف فرکانس**
- **بدون استفاده از تکرارکننده ها ، قادر به حمل سیگنال در مسافت های طولانی نمی باشند.**
- **پایین بودن پهنای باند**
- **بدلیل پذیرش پارازیت در محیط های الکتریکی سنگین بخدمت گرفته نمی شوند.**

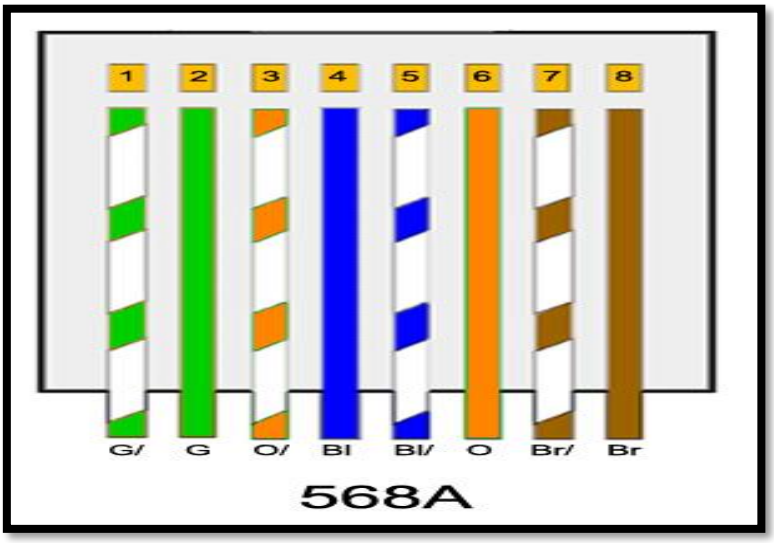
کانکتور استاندارد برای کابل های UTP ، از نوع RJ- ۴۵ می باشدکه شباهت زیادی به کانکتورهای تلفن (RJ-۱۱) دارد. هر یک از پین های کانکتور فوق می بایست بدرستی پیکربندی گردند.

شکل۷-۱

رنگ بندی در کابل ها و نوع استاندارد استفاده آن ها

کابل های بهم تابیده ۴ زوج از ۸ رنگ بصورت ۴ زوج دو بدو بهم تابیده تشکیل شده است

شامل: {سفید نارنجی/نارنجی} # {سفید سبز/سبز} # {سفید آبی/آبی} # {سفید قهوه ای/قهوه ای}



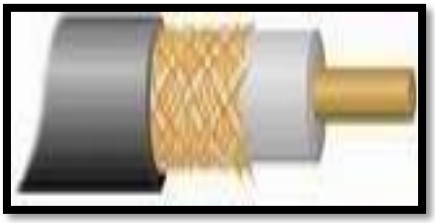
شکل۸-۱

شکل ۹-۱

کابل کواکسیال

یکی از مهمترین محیط های انتقال در مخابرات کابل کواکسیال و یا هم محور می باشد . این نوع کابل ها از سال ۱۹۳۶ برای انتقال اخبار و اطلاعات در دنیار به کار گرفته شده اند. در این نوع کابل ها، دو سیم تشکیل دهنده یک زوج ، از حالت متقارن خارج شده و هر زوج از یک سیم در مغز و یک لایه مسی بافته شده در اطراف آن تشکیل می گردد. در نوع دیگر کابل های کواکسیال ، به حای لایه مسی بافته شده ، از تیوپ مسی استوانه ای استفاده می شود. ماده ای پلاستیکی این دو هادی را از یکدیگر جدا می کند. ماده پلاستیکی ممکن است بصورت دیسکهای پلاستیکی یا

شیشه ای در فواصل مختلف استفاده و مانع از تماس دو هادی با یکدیگر شود و یا ممکن است دو هادی در تمام طول کابل بوسیله مواد پلاستیکی از یکدیگر جدا گردند.



شکل ۱۰-۱

مزایای کابل های کواکسیال :

- قابلیت اعتماد بالا
- ظرفیت بالای انتقال ، حداکثر پهنای باند ۳۰۰ مگاهرتز
- دوام و پایداری خوب
- پایین بودن مخارج نگهداری
- قابل استفاده در سیستم های آنالوگ و دیجیتال
- هزینه پائین در زمان توسعه
- پهنای باند نسبتا" وسیع که مورد استفاده اکثر سرویس های مخابراتی از جمله تله کنفرانس صوتی و تصویری است .

معایب کابل های کواکسیال :

- مخارج بالای نصب

- نصب مشکل تر نسبت به کابل های بهم تابیده
- محدودیت فاصله
- نیاز به استفاده از عناصر خاص برای انشعابات

از کانکتورهای BNC[۱۹] بهمراه کابل های کواکسیال استفاده می گردد. اغلب کارت های شبکه دارای کانکتورهای لازم در این خصوص می باشند.

فیبر نوری

یکی از جدیدترین محیط های انتقال در شبکه های کامپیوتری ، فیبر نوری است . فیبر نوری از یک میله استوانه ای که هسته نامیده می شود و جنس آن از سیلیکات است تشکیل می گردد. شعاع استوانه بین دو تا سه میکرون است . روی هسته ، استوانه دیگری (از همان جنس هسته) که غلاف نامیده می شود ، استقرار می یابد. در این نوع فیبرها ، نور در اثر انعکاسات کلی در فصل مشترک هسته و غلاف ، انتشار پیدا خواهد کرد. منابع نوری در این نوع کابل ها ، دیود لیزری و یا دیودهای ساطع کننده نور می باشند.منابع فوق ، سیگنال های الکتریکی را به نور تبدیل می نمایند.

شکل ۱۱-۱

[۱۹] (Bayone -Neill - Concelman)

مزایای فیبر نوری :

- حجم و وزن کم
- پهنای باند بالا
- تلفات سیگنال کم و در نتیجه فاصله تقویت کننده ها زیاد می گردد.
- فراوانی مواد تشکیل دهنده آن ها
- مصون بودن از اثرات القاهای الکترو معناطیسی مدارات دیگر
- آتش زا نبودن آن ها بدلیل عدم وجود پالس الکتریکی در آن ها
- مصون بودن در مقابل عوامل جوی و رطوبت
- سهولت در امر کابل کشی و نصب
- استفاده در شبکه های مخابراتی آنالوگ و دیجیتال
- مصونیت در مقابل پارازیت

معایب فیبر نوری :

- براحتی شکسته شده و می بایست دارای یک پوشش مناسب باشند. مسئله فوق با ظهور فیبر های تمام پلاستیکی و پلاستیکی / شیشه ای کاهش پیدا کرده است .
- اتصال دو بخش از فیبر یا اتصال یک منبع نور به فیبر ، فرآیند دشواری است . در چنین حالتی می توان از فیبرهای ضخیم تر استفاده کرد اما این مسئله باعث تلفات زیاد و کم شدن پهنای باند می گردد.
- از اتصالات T شکل در فیبر نوری نمی توان جهت گرفتن انشهاب استفاده نمود. در چنین حالتی فیبر می بایست بریده شده و یک Detector اضافه گردد. دستگاه فوفق می بایست قادر به دریافت و تکرار سیگنال را داشته باشد.

- تقویت سیگنال نوری یکی از مشکلات اساسی در زمینه فیبر نوری است . برای تقویت سیگنال می بایست سیگنال های توری به سیگنال های الکتریکی تبدیل ، تقویت و مجددا" به علائم نوری تبدیل شوند.

کابل های استفاده شده در شبکه های اترنت

مشخصه	نوع کابل	حداکثر طول
۱۰BaseT	Unshielded Twisted Pair	۱۰۰ meters
۱۰Base۲	Thin Coaxial	۱۸۵ meters
۱۰Base۵	Thick Coaxial	۵۰۰ meters
۱۰BaseF	Fiber Optic	۲۰۰۰ meters
۱۰۰BaseT	Unshielded Twisted Pair	۱۰۰ meters
۱۰۰BaseTX	Unshielded Twisted Pair	۲۲۰ meters

جدول۲-۱

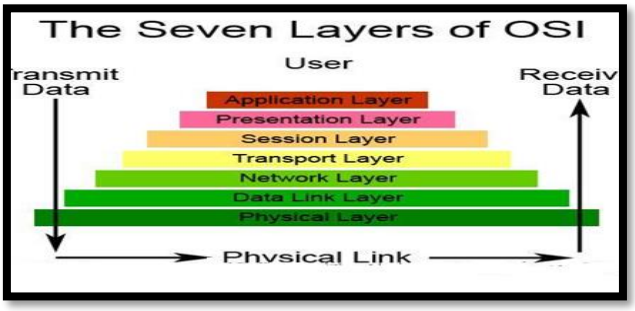
مدلOSI[۲۰]

همانطور که برای ساخت یک ساختمان شما نیاز به یک نقشه دارید تا بدانید جای هرچیز کجاست مثلا مسیر برق ساختمان از کجا می گذرد ، درها کجا هستند ، راه ورود و خروج کجاست و هر واحد در کدام طبقه ساختمان قرار دارد در شبکه نیز لازم است بدانید ارتباط شبکه شما چه مسیری را طی می کند و در هر مسیری چه اتفاقی برای داده های شما می افتد . این کار به دو صورت به شما کمک می کند :

۱. درک خوبی از شبکه و تبادلهای شبکه ای بدست می آورید.
۲. در صورت بروز مشکل میدانید باید در کجا دنبال مشکل بگردید.

[۲۰] Open Systems Interconnection

امروزه دو مدل شبکه وجود دارد. مدلOSI که به عنوان استاندارد پذیرفته شده و مدل TCP/IP که توسط وزارت دفاع آمریکا طراحی شده است.در عمل بیشتر مدل TCP/IPمورد استفاده قرار می‌گیرد و OSI بیشتر مدل آموزشی محسوب می‌شود.



شکل۱۲-۱

لایه هفت (**Application**) یا کاربرد : این لایه با سیستم عامل و یا برنامه های کاربردی ارتباط دارد. کاربران با استفاده از نرم افزارهای کاربردی متفاوت قادر به انجام عملیات مرتبط با شبکه خواهند بود. مثلا" کاربران می توانند اقدام به ارسال فایل خواندن پیام ارسال پیام و ... نمایند.

لایه شش (**Presentation**) یا نمایش: لایه فوق داده های مورد نظر خود را از لایه Application اخذ و آن ها را بگونه ای تبدیل خواهد کرد که توسط سایر لایه ها قابل استفاده باشد.

لایه پنج (**Session**) یا جلسه: لایه فوق مسئول ایجاد ، پشتیبانی و ارتباطات مربوطه با دستگاه دریافت کننده اطلاعات است .

لایه چهار (Transport) یا انتقال: .لایه فوق مسئول پشتیبانی کنترل جریان داده ها و و بررسی خطاء و بازیابی اطلاعات بین دستگاه های متفاوت است . کنترل جریان داده ها ، بدین معنی است که لایه فوق در صورتی که اطلاعاتی از چندین برنامه ارسال شده باشد ، داده های مربوطه به هر برنامه را به یک Stream آماده تبدیل تا در اختیار شبکه فیزیکی قرار داده شوند.

لایه سه (Network) یا شبکه: در لایه فوق روش ارسال داده ها برای دستگاه گیرنده تعیین خواهد شد. پروتکل های منطقی ، روتینگ و آدرس دهی در این لایه انجام خواهد شد.

لایه دو (Data Link) یا پیوند داده ها: در لایه فوق ، پروتکل های فیزیکی به داده اضافه خواهند شد. در این لایه نوع شبکه و وضعیت بسته های اطلاعاتی (Packet) نیز تعیین می گردند.

لایه یک (Physical) یا فیزیکی: لایه فوق در ارتباط مستقیم با سخت افزار بوده و خصایص فیزیکی شبکه نظیر : اتصالات ، ولتاژ و زمان را مشخص می نماید.مدل OSI بصورت یک مرجع بوده و پروتکل های پشته ای یک و یا چندین لایه از مدل فوق را ترکیب و در یک لایه پیاده سازی می نمایند.

پروتکل های پشته ای [۲۱]

یک پروتکل پشته ای ، شامل مجموعه ای از پروتکل ها است که با یکدیگر فعالیت نموده تا امکان انجام یک عملیات خاص را برای سخت افزار و یا نرم افزار فراهم نمایند. پروتکل TCP/IP نمونه ای از پروتکل های پشته ای است . پروتکل فوق

[۲۱] Stack Protocols

از چهار لایه استفاده می نماید. پروتکل های TCP/IP در چهار لایه مفهومی جای گرفته اند که به آن مدل دارپا (DARPA) گویند؛ این نام پس از توسعه TCP/IP توسط دولت امریکا بر آن نهاده شده است.

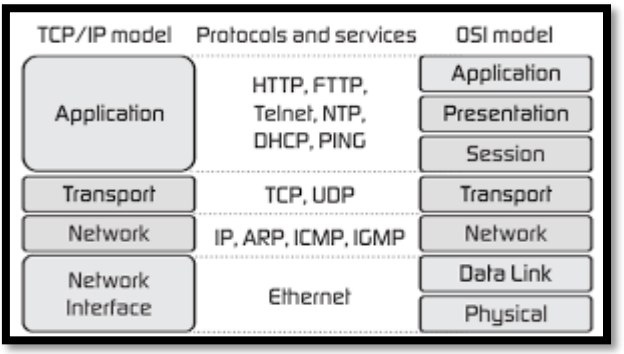
لایه یک (Interface Network) یا لایه واسط شبکه: لایه فوق ، لایه های Physical و Data را ترکیب و داده های مربوط به دستگاه های موجود در یک شبکه را روت خواهد کرد.

لایه دو (Internet) یا لایه اینترنت: لایه فوق متناظر لایه Network در مدل OSI است . پروتکل اینترنت (IP) ، با استفاده از آدرس IP (شامل یک مشخصه شبکه و یک مشخصه میزبان) ، آدرس دستگاه مورد نظر برای ارتباط را مشخص می نماید.

لایه سه (Transport) یا لایه انتقال: لایه فوق متناظر با لایه Transport در مدل OSI است .

لایه چهار (Application) . لایه فوق متناظر با لایه های Session,Presentation و Application در مدل OSI است. پروتکل هائی نظیر FTP و SMTP در لایه فوق ایفای وظیفه می نمایند.

این پروتکل با سرویس های نام دهی در ویندوز مانند DNS و تکنولوژی های امنیتی مثل IPSec تعامل خوبی دارد و ارتباط بین دو سیستم را در اینترنت تسهیل میکند. اگر بخواهیم بصورت ایده‌آل صحبت کنیم باید بگوییم که هر زمان کامپیوترها (با سیستم عامل ویندوز) در شبکه با یکدیگر ارتباط برقرار میکنند، از مجموعه پروتکل TCP/IPاستفاده شده است. در زیر معماری پروتکل TCP/IP را شاهد هستیم:



شکل۱۳-۱

لایه Network Interface

این لایه که به لایه Network Access **هم شناخته میشود، وظیفه قرار دادن بسته های** TCP/IP **را بر روی شبکه (رسانه انتقال) دارند و در مقابل، بسته های** TCP/IP **را از شبکه (رسانه انتقال) تحویل می گیرند . قابلیت بالای** TCP/IP **در همخوانی با هر رسانه خاص شبکه باعث شده است تا با رسانه جدیدی مثل** ATM **نیز سازگاری داشته باشد. این لایه با لایه های** Data Link **و** Physical **در مدل** OSI **همخوانی دارد. این نکته را نیز باید خاطر نشان کرد که لایه** Internet **اگر از وجود سرویس های** Sequencing **و** Acknowledgment **بهره نبرد، ممکن است به همراه لایه** Network Interface **بیان شود .**

لایه Internet

لایه اینترنت وظایف آدرس دهی، بسته بندی و مسیر یابی را بر عهده دارد .پروتکل های اصلی در این لایه عبارتند از IP ، ARP ، ICMP **و** IGMP.

- Internet Protocolیا IPیک پروتکل مسیر یابی است که آدرس دهیIP ، مسیریابی و قطعه قطعه کردن (Fragmentation) و سر هم کردن (Reassembly)بسته ها را کنترل می کند.
- Address Resolution Protocol)یا ، ARP ، تناظر و تبدیل آدرس لایه اینترنت را با آدرس لایه Network Interface مثل آدرس سخت افزاری کنترل می کند.
- Internet Control Message Protocol یا ICMP ، وظایف رفع خطا و گزارش خطا به هنگام عدم تحویل موفق یک بسته IP را دارد.
- Internet Group Management Protocolیا IGMPمدیریت اعضای گروه IP Multicast را بر عهده دارد.

لایه اینترنت مشابه لایه network در OSI است .

لایهTransport

این لایه که به لایه Host-to-Host Transport نیز معروف است، سرویس های ارتباطی دیتاگرام و session را برای لایه Application آماده می کند. پروتکل های اصلی در این لایه عبارتند از Transmission Control protocolیا TCPو User Datagram Protocol یا UDP.

- TCPیک سرویس یک به یک، Connection-Oriented، با ارتباطات قابل اعتماد را ایجاد می کند .TCP قبل از ارسال اطلاعات از وجود یک خط ارتباطی بین دو طرف را اطمینان حاصل می کند (مفهوم-Connection Oriented، ترتیب و تائیدیه های بسته های ارسالی را کنترل و بسته هایی که به هر دلیل در حین انتقال دچار مشکل میشوند را بازیابی می کند).

- UDP یک ســرویس یک به یک یا یک به چند، Connectionless ، با ارتباطات غیرقابل اطمینان را ایجاد می کند .UDP زمانی مورد استفاده قرار می گیرد که مقدار کمی از اطلاعات را می خواهیم منتقل کنیم (مانند داده ای که در یک بسته سیگنال جا گرفته است) و یا آن که اطلاعات ارسالی ارزش چندانی ندارند و به مقصـد نرسـیدن آن ها اهمیت خاصـی ندارد (مثل پخش آنلاین فیلم). همچنین زمانی از UDP استفاده می کنیم که اپلیکیشن ها و یا پروتکل های موجود در لایه بالا دستی، سرویس تحویل قابل اعتمادی دارند. لایه Transport در TCP/IP مشــابه لایه Transport در OSI اســت .

لایه Application

این لایه به برنامه ها این اجازه را می دهد تا به سرویس های موجود در لایه های دیگر دسترسی داشته باشند و بتوانند پروتکل هایی که برای تبادل دیتا استفاده می کنند، تعریف نمایند. پروتکل های زیادی در لایه Application وجود دارند و پروتکل های جدید نیر مرتبا در حال توسعه هستند. اکثر پروتکل های معروف موجود در این لایه آن هایی هستند که در تبادل اطلاعات کاربر نقش دارند :

- Hyper Text Transfer Protocol (HTTP) : برای تبادل فایل های سازنده صفحات وب در اینترنت استفاده میشود.
- File Transfer Protocol (FTP): برای انتقال متقابل فایل استفاده میشود.
- Simple Mail Transfer Protocol (SMTP):برای انتقال پیام های ایمیل و فایل های ضمیمه به آن ها استفاده می شود.

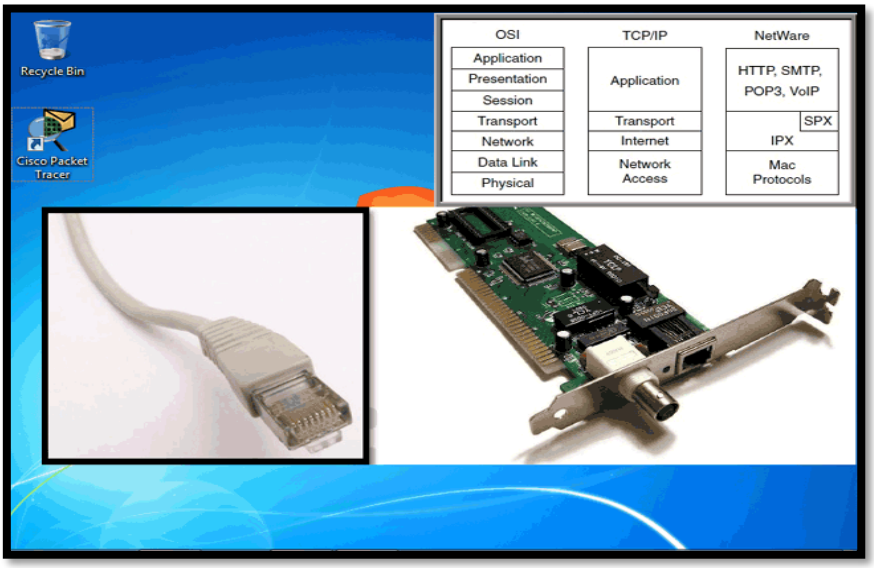
- Telnet که یک پروتکل شبیه ساز ترمینال است، برای لاگین به یک سیستم در شبکه از طریق ریموت استفاده می‌شود.علاوه بر پروتکل های یاد شده، پر که در تبدیل آدرس IP به نام هاست و بلعکس مورد استفاده قرار می‌گیرد .
- Routing Information Protocol (RIP):یک پروتکل مسیریابی است که روترها از آن برای تبادل اطلاعات مسیریابی در یک شبکه داخلی استفاده می‌کنند.
- Simple Network Management Protocol (SNMP):بین یک کنسول مدیریتی شبکه و یک دیوایس مانند روترها، Bridgeها و هاب های هوشمند برای جمع آوری و تبادل اطلاعات مدیریتی شبکه مورد استفاده قرار می‌گیرد.اگر بخواهیم از رابط های کاربری موجود در این لایه که برای اپلیکیشن ها بکار می‌روند هم نام ببریم می‌توانیم Windows Sockets و NetBIOSرا معرفی کنیم Windows Sockets .استانداردی را برای API[۲۲]ایجاد می‌کند؛ یک API رابط پیاده سازی توسط نرم افزار است که به دیگر برنامه ها اجازه می دهد با آن ارتباط داشته باشند .NetBIOS هم یک رابط کاربری استاندارد و صنعتی برای دسترسی به خدمات پروتکل مثل sessionها، دیتاگرام ها و تطابق نام ها و آدرس ها است.

اترنت[۲۳] چیست؟

یکی از فناوریهای مبتنی بر Frame در شبکه‌های رایانه برای شبکه‌های محلی می‌باشد. این نام از مفهوم فیزیکی ether گرفته شده‌است. شبکه‌های محلی اترنت را با استاندارد IEEE ۸۰۲,۳ می‌شناسیم. اترنت برای شبکه‌های داخلی LAN ساخته شده و شامل، استانداردهای فیزیکی و لایه پیوند داده ها بوده وخود برای ساخت

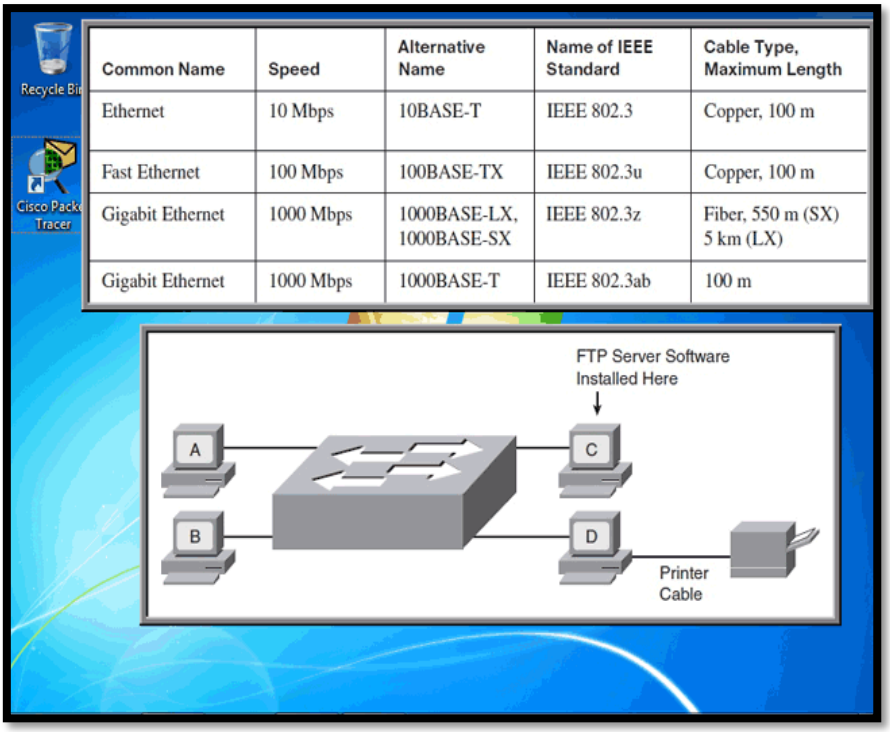
[۲۲] Application Programming Interface
[۲۳] Ethernet

فریمی از داده ها است. معمولاً در آن از کانکتور RJ-٤٥ و کابل زوج سیم بهم تابیده،استفاده می‌شود. در تصویر زیر کابل و کارت شبکه اترنت را مشاهده می‌کنید.



شکل۱۴-۱

شبکه اترنت با سرعت‌های ۱۰ مگا بایت، ۱۰۰ مگابایت، ۱ گیگا بایت تا ۴۰ و ۱۰۰ گیگا بایت در ثانیه پیاده‌سازی شده است. در شکل زیر یک شبکه LAN معمولی مشاهده می‌کنید که در آن چهار کامپیوتر A ، B، Cو D به یکدیگر متصل شده‌اند. به کامپیوتر D یک پرینتر نیز متصل گردیده است .در جدول زیر انواع پرکاربرد اترنت را مشاهده می‌کنید.



شکل ۱۵-۱

اترنت در ابتدا به صورت شبکه‌های خطی یا باس پدید آمد. در این نوع پیکربندی از مجموعه کابل به عنوان ستون فقرات اصلی در شبکه استفاده شده و تمام کامپیوترهای موجود در شبکه (سرویس‌دهنده‌ها، سرویس‌گیرنده‌ها) با استفاده از کارت‌های شبکه به صورت اشتراکی[۲۴] به آن متصل می‌شدند و کامپیوترها برای انتقال پیام به یک کامپیوتر دیگر یک سیگنال الکتریکی را به همه کامپیوترها ارسال می‌کردند، اما شبکه باس دارای معایب زیادی است. از جمله آنکه بستن آن کار دشواری است و شبکه به

[۲۴] shared

صورت اشتراکی می‌باشد و چون هنگام ارسال سیگنال یک کامپیوتر بقیه قادر به ارسال نیستند، زمان اشغال شبکه بالا می‌رود. اگر در حین ارسال سیگنال از جانب یک کامپیوتر، کامپیوتر دیگری سیگنال ارسال کند، باعث بوجود آمدن تصادف[۲۵] یا خواهد شد. راه حل این موضوع استفاده از الگوریتمی به نام CSMA/CD[۲۶] است. که طبق آن در زمان واحد فقط یک کامپیوتر قادر به ارسال سیگنال می‌باشد. اگر در این حین تصادم به وجود آمد، همه کامپیوترها برای خود یک زمان تصادفی[۲۷]، تنظیم می‌کنند و زمان هر یک از کامپیوترها که زودتر صفر شد، شروع به ارسال سیگنال می کند. در واقع CSMA/CD مانند پلیس عمل می‌کند، یعنی با وضع قوانین باعث کاهش تصادفات می‌شود.

واسطهای شبکه

هاب[۲۸]

هاب به جای باس استفاده می شود. در اولین لایه مدل مرجع OSI فعالیت می‌کند . هابها فریم‌های داده را نمی‌خوانند (کاری که سوئیچ و یا روتر انجام می‌دهند) و صرفاً این اطمینان را ایجاد می‌کنند، که فریم‌های داده بر روی هر یک از پورت‌ها، تکرار خواهد شد. سیگنال از یک پورت وارد می‌شود و از سایر پورت‌ها خارج می‌شود. گره[۲۹]هایی که در یک اترنت با استفاده از قوانین CSMA/CD به اشتراک گذاشته می‌باشند، عضو یک دامنه تصادم [۳۰]مشابه می‌باشند و زمانیکه یک تصادم یا تصادف اتفاق می‌افتد، سایر گرههای موجود در دامنه نیز آن را می‌شنوند و زمان تصادفی را Setمی‌کنند .

---

[۲۵] Collision
[۲۶] Carrier Sense Multiple Access with Collision Detection
[۲۷] Random Timer
[۲۸] HUB
[۲۹] Node
[۳۰] Collision Domain

شکل۱۶-۱

سوییچ[۳۱] **یا راهگزین: شکل ظاهری سوئیچ همانند جعبه‌ای است که متشکل از چندین درگاه است که از این لحاظ شبیه هاب می‌باشدو با وجود آنکه هم هاب و هم سوئیچ وظیفه برقراری ارتباط بین دستگاه‌های مختلف را بر عهده دارند, تفاوت آن ها از آنجا آغاز می‌شود که هاب بسته‌های ارسالی از طرف یک دستگاه را به همه درگاه‌های خود ارسال می‌کند و کلیه دستگاه‌های دیگر علاوه بر دستگاه‌های مقصد این بسته را دریافت می‌کند. در حالیکه سوئیچ ، بسته‌های دریافتی را بدون درگیر کردن سایر درگاه‌ها فقط به درگاه مقصد ارسال می‌کند.**

[۳۱] switch

شکل ۱۷-۱

سوئیچ می‌تواند بسته‌های داده را پردازش کند, از این رو توانایی شناسایی پورت مقصد را دارد. در سوئیچ های معمولی که به سوئیچ لایه دو معروفند این پردازش تا لایه دوم مدل OSI پیش می‌رود و نتیجه این پردازش جدولی است که در سوئیچ با خواندن آدرس سخت افزاری[۳۲] فرستنده بسته و ثبت درگاه ورودی تشکیل می‌شود . سوئیچ با رجوع به این جدول عملیات آدرس‌دهی بسته‌ها در لایه دوم را انجام می‌دهد, از این رو این جدول مشخص می‌کند بسته ورودی می‌بایست فقط برای کدام پورت ارسال شود .

نحوه کار سوییچ

در ابتدا باید به تفاوت بین سوئیچ و هاب پی ببرید ، در یک هاب در حقیقت هیچگونه عملی بر روی فریم ها که نام بسته های اطلاعاتی در لایه دوم از مدل OSI هستند انجام نمی شود ، این وسیله صرفا از یک پورت خود اطلاعات را دریافت می کند و آن ها را تقویت و به تمامی پورت های خود ارسال می کند ، این وسیله هیچگونه درکی از وجود فریم در خود نداشته و صرفا در لایه فیزیکی مدل OSI فعالیت می کند ، در

[۳۲] MAC

هنگام ارسال یک فریم از خود آن را به تمامی پورت های خود ارسال می کند که همین امر موجب می شود که پهنای باند موجود در هاب به نسبت تعداد پورت های آن تقسیم شده و طبیعتا سرعت نیز به نسبت پایین خواهد آمد . و اما در سوئیچ هر پورت برای خود پهنای باند مستقلی دارد و در هنگام ارسال فریم ، فریم صرفا برای مقصد مورد نظر ارسال خواهد شد و از پخش شدن در کلیه پورت ها جلوگیری خواهد شد . این شیوه کاری به این شکل است که در فریم ارسالی از سوی کامپیوتر مبدا آدرس کامپیوتر مقصد قرار گرفته است ، سوئیچ با خواندن آدرس مقصد فریم مورد نظر را صرفا به آدرس مقصد ارسال کرده و مسیر منحصر به فردی برای این دو کامپیوتر برای برقراری ارتباط ایجاد خواهد کرد . در این روش پهنای باند بصورت اختصاصی برای کامپیوتر ها خواهد بود زیرا فریم در کل پورت های سوئیچ ، پخش نخواهد شد .

اما سوئیچ چگونه می فهمد که آدرس مبدا و مقصد چیست و آن فریم را می بایست به کدام پورت انتقال دهد ؟ در جواب این سئوال باید گفت که سوئیچ، از ساختاری به نام یا جدول آدرس سخت افزاری[۳۳] استفاده میکند که در این جدول لیست کلیه آدس های سخت افزاری که بر روی هر پروت قرار دارند نوشته شده و مشخص شده است که هر یک از آدرس ها در کدام یک از پورت های سوئیچ اتصال یافته اند. حال این سئوال پیش می آید که سوئیچ چگونه این جدول را تشکیل می دهد؟ هنگامی که یک کامپیوتر قصد برقراری ارتباط با کامپیوتر دیگری در شبکه را داشته باشد فریم خود را به پورت مورد نظر بر روی سوئیچ ارسال خواهد کرد ، این فریم شامل آدرس سخت افزاری مبدا و مقصد خواهد بود ، به محض اینکه سوئیچ فریم مورد نظر را دریافت می کند ابتدا به آدرس مبدا توجه می کند ، اگر آدرس مبدا را در جدول خود موجود نداشته باشد آدرس سخت افزاری مبدا را در جدول MAC خود یادداشت می کند و سپس به سراغ آدرس مقصد می رود ، اگر آدرس مقصد نیز در جدول وجود نداشته

[۳۳] MAC Table

باشد فریم ارسالی را برای هر یک از پورت های موجود ارسال می کند و قاعدتا ، صرفا یک آدرس سخت افزاری متناسب با مقصد در پورت های سوئیچ به آن فریم پاسخ خواهد داد ، سپس سوئیچ آدرس مقصد را نیز با شماره پورت مورد نظر در جدول آدرس سخت افزاری خود قرار خواهد داد . این روش همچنان ادامه خواهد داشت تا جدول بصورت کامل تشکیل شود . در مراحل بعدی و بعد از تشکیل شدن جدول MACدر صورت ارسال فریم ، سوئیچ بلافاصله با استفاده از جدول ، فریم ارسالی را به مقصد مورد نظ هدایت خواهد کرد .توجه داشته باشید که سوئیچ هیچگاه فریم ارسالی از یک پورت را به خود آن پورت ارسال نخواهد کرد . سوئیچ به محض دریافت یک فریم سه عمل بر روی آن انجام خواهد داد :

۱.ارسال کردن[۳۴] فریم: در صورتیکه آدرس مقصد در جدول آدرس موجود باشد سوئیچ فریم را به مقصد مورد نظر ارسال یا Forward خواهد کرد .

۲.فیلترکردن[۳۵]: در صورتیکه آدرس مقصد ارسالی در جدول آدرس به همان پورتی اشاره کند که از آن وارد سوئیچ شده است بسته Drop شده و به سوئیچ وارد نخواهد شد . این بدین معناست که آدرس درخواستی از کامپیوتر یا سوئیچ در همان پورتی قرار دارد که از آن ارسال شده ، پس سوئیچ نمی تواند کار خاصی را بر روی آن انجام دهد و صرفا آنرا بلوکه میکند تا ترافیک اضافی در شبکه تولید نشود.

۳.ارسال همگانی[۳۶]: در صورتیکه آدرس مقصد در جدول MAC سوئیچ موجود نباشد ، سوئیچ بصورت خودکار فریم را به تمامی پورت های خود به غیر از پورت مبدا ارسال کرده و منتظر جواب از کامپیوتر مقصد خواهد شد.

روتر یا مسیریاب[۳۷]

---

[۳٤] . Forward
[۳٥] Drop
[۳٦] Flood
[۳۷] Router

روتر یکی از دستگاه های شبکه ای مهم و حیاتی است که از آن در شبکه های محلی و گسترده استفاده می گردد . روترها تاکنون در مدل های متفاوت و با معماری مختلف طراحی ، تولید و عرضه شده اند. استفاده از روترها در شبکه به امری متداول تبدیل شده است . یکی از دلایل مهم گسترش استفاده از روتر ، ضرورت اتصال یک شبکه به چندین شبکه دیگر (اینترنت و یا سایر سایت ها ی از راه دور) در عصر حاضر است . نام در نظر گرفته شده برای روترها ، متناسب با کاری است که آنان انجام می دهند : " ارسال داده از یک شبکه به شبکه ای دیگر " . مثلا" در صورتی که یک شرکت دارای شعبه ای در تهران و یک دفتر دیگر دربوشهر باشد ، به منظور اتصال آنان به یکدیگر می توان از یک خط اختصاصی که به هر یک از روترهای موجود در دفاتر متصل می گردد ، استفاده نمود . بدین ترتیب ، هر گونه ترافیکی که لازم است از یک سایت به سایت دیگر انجام شود از طریق روتر محقق شده و تمامی ترافیک های غیرضروری دیگر فیلتر و در پهنای باند و هزینه های مربوطه ، صرفه جوئی می گردد. روتر یکی از دیوایس‌های مورد استفاده در شبکه می باشد که در لایه ی سوم OSI (لایه شبکه) کار می کند. روتر بین شبکه های مختلف مسیر یابی می کند و دقیقا به همین دلیل باید حداقل دو عدد اینترفیس داشته باشد که Net ID های آن ها حداقل یک بیت با هم فرق داشته باشند. شرکت های زیادی هستند که تجهیزات شبکه مانند روتر و دیگر دیوایس های مورد استفاده را تولید می کنند به این سبب روتر ها نیز برند ها و مدل های مختلفی دارند اما همانطور که همه می دانیم بهترین شرکت تولید کننده تجهیزات شبکه، شرکت سیسکواست که نه تنها تجهیزات بلکه صادر کننده علم شبکه به دنیا نیز می باشد. مسیریابی[۳۸] علمی است که سیسکو به دنیا معرفی کرد و به معنی ارسال بسته از مبدا به مقصد بر اساس پرتکل ها ،آدرس لایه سومی (IP) و جدول مسیر یابی یک روتر می باشد.

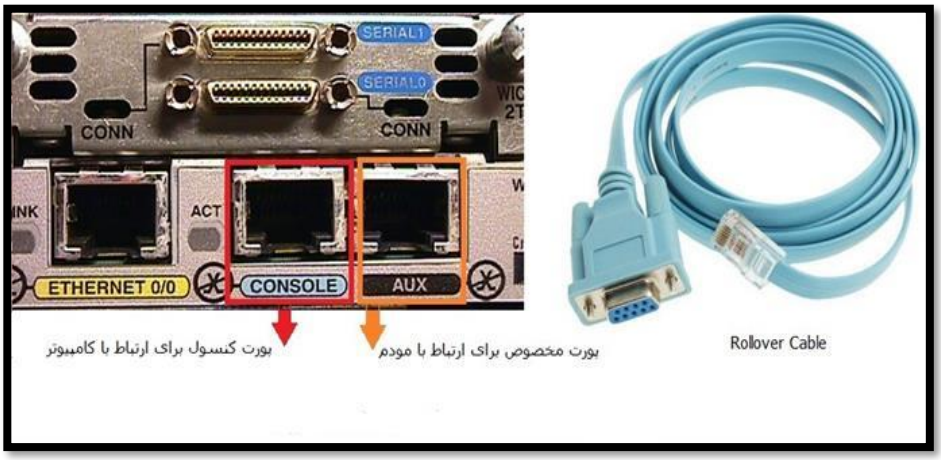
[۳۸] Routing

شکل ۱۸-۱

انواع روترها

روترها را می توان به دو گروه عمده سخت افزاری و نرم افزاری تقسیم نمود:
روترهای سخت افزاری : روترهای فوق ، سخت افزارهائی می باشند که نرم افزارهای خاص تولید شده توسط تولید کنندگان را اجراء می نمایند .
روترهای نرم افزاری : روترهای نرم افزاری دارای عملکردی مشابه با روترهای سخت افزاری بوده و مسئولیت اصلی آنان نیز ارسال داده از یک شبکه به شبکه دیگر است. یک روتر نرم افزاری می تواند یک سرویس دهنده NT ، یک سرویس دهنده Netware و یا یک سرویس دهنده لینوکس باشد . تمامی سیستم های عامل شبکه ای مطرح ،دارای قابلیت های روتینگ از قبل تعبیه شده می باشند. در اکثر موارد از روترها به عنوان فایروال و یا gateway اینترنت ، استفاده می گردد .

پورت های کنسول و AUX روتر : این پورت ها از مولفه هایی است که در پشت روتر های سیسکو قرار دارند. پورت کنسول اولین راه برقراری ارتباط با روتر سیسکو محسوب می شود. از طریق وصل یک کابل مخصوص به نام Rollover Cable به این پورت می توانید روتر را به یک PC متصل کرده و از طریق آن کامپیوتر اقدام به پیکربندی روتر نمایید. پورت کنسول از لحاظ ظاهری شبیه به پورت RG-٤٥ می باشد اما تفاوت هایی از لحاظ کارکرد با آن دارد، به همین دلیل برای اتصال کامپیوتر به پورت کنسول کابل مخصوصی وجود دارد که به همراه روتر به شما فروخته می شود. همچنین با استفاده از پورت Auxiliary یا به اختصار AUX شما می توانید یک مودم را به روترتان وصل کرده و کاربر نیز با اتصال به این مودم از طریق اتصال از راه دور اقدام به پیکربندی روتر نماید.



شکل ۱۹-۱

نحوه کار کرد یک روتر

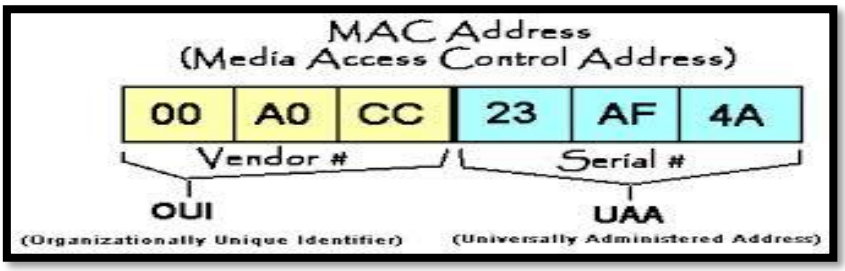
هنگامی که یک روتر را خریداری و برای اولین بار روشن می کنید به صورت پیش فرض کاری انجام نمی دهد یعنی نیاز است که همه کار ها و دستورات به آن داده شود.پس ابتدا اینترفیس های روتر را روشن کرده و بر اساس تشخیص مهندس شبکه، IPهای مورد نظر به اینترفیس ها داده و پروتوکل مسیریابی[۳۹] مناسب بروی آن روتر راه اندازی می شود. حال زمانی را در نظر بگیرید که بسته ای به روتر می رسد ، در این حالت ابتدا روتر به جدول مسیریابی خود نگاه می کند چنانچه روت یا مسیری برای آن مقصد مورد نظر داشته باشد ، بسته را روت می کند و اگر مسیری در جدول مسیریابی نداشته باشد ، default gatewayرا بررسی میکند. در صورتی که Set شده باشد ، بسته به آن سمت هدایت می شود در غیر این صورت بسته drop خواهد شد .

نکته : عملیات Routing تنها توسط روتر انجام نمی شود بلکه سوئیچ هایی نیز وجود دارند که این کار را انجام می دهند ودر اصطلاح به آن ها MLS [۴۰] گفته می شود. MLS ها قابلیت کار کرد در لایه های دوم و سوم OSI و همچنین دید نسبت به لایه چهارم را دارند.

آدرس فیزیکی[۴۱] یا مک آدرس

مک آدرس یک آدرس فیزیکی است که محل نگهداری آن بر روی حافظه ROM داخل کارت شبکه می باشد. مک آدرس در تمامی کارت شبکه ها دارای طول یکسان می باشد که طول آن برابر ۶ بایت یا ۴۸ بیت است. به تصویر زیر دقت کنید.

[۳۹] Routing Protocol
[۴۰] Multi Layer Switch
[۴۱] Mac Address, Media Access Control Address



شکل ۲۰-۱

همانطور که در شکل بالا می بینید فرمت آدرس دهی به صورت هگزا دسیمال است.۲۴بیت اول را سازمان استاندارد سازی[۴۲] به شرکت های تولیدکننده کارت شبکه یاOUI[۴۳] می‌دهد. ۲۴بیت دوم ، توسط شرکت های تولید کننده بر روی کارت های شبکه[۴۴] قرار می گیرد .

آدرس منطقی[۴۵] یا آدرس IP

آدرس IP[۴۶] که به صورت مختصر، IP نیز نامیده می‌شود، یک برچسب شناسایی عددی است که برای هر چیزی که به شبکه از طریق پروتکل اینترنت (IP)یا به خود بستر اینترنت متصل شود، اغلب توسط سرویس دهنده اینترنتی اختصاص داده می‌شود. این نشانی برای شناسایی مجزای هر دستگاه (کامپیوتر، موبایل یا به طور کل، هر چیزی که از پروتکل اینترنت استفاده کند) نسبت به دیگری به کار می‌رود. به عبارت ساده تر، IP آدرس شماره شناسایی هر یک از این کامپیوترها یا دستگاه‌ها است.کامپیوترها و کاربران بسیار زیادی به اینترنت (یا به طور کل شبکه‌ای که از

---

[۴۲] IEEE
[۴۳] Organization Unit Identifier
[۴۴] UAA
[۴۵] Logical Address
[۴۶] Internet Protocol Address

پروتکل اینترنت استفاده می‌کند) متصل می‌شوند. هر یک از این کامپیوترها درصورتی که دارای یک آدرس مشخص نباشند عملاً غیرقابل استفاده خواهند بود. برای درک بهتر، فرض کنید که هر کامپیوتر یک شخصی عادی بوده و آدرس IP همان کامپیوتر نیز آدرس ایمیل فرد باشد. حال شما با داشتن آدرس ایمیل فرد می‌توانید به راحتی به وی نامه ارسال یا دریافت کنید. اما درصورتی که آدرس ایمیل فرد را نداشته باشید به هیچ وجه امکان ارسال ایمیل برای وی وجود نخواهد داشت.بنابراین با استفاده از آدرس IP، پروتکل اینترنت می‌تواند کاربران را تشخیص داده و امکان ارسال و دریافت داده‌ها را فراهم کند. به این ترتیب برای این که کامپیوترها بتوانند بر روی یک شبکه یا بستر اینترنت از یکدیگر به صورت مجزا شناخته شوند، حداقل باید دارای یک آدرس IP باشند. در این صورت بدون این که هیچ اختلالی در مسیر انتقال داده بین مبداء و مقصد بوجود بیاید، هر کامپیوتر داده‌هایی را دریافت یا ارسال می‌کند که فقط مختص به همان کامپیوتر باشد.

IP نسخه ۴

آی پی نسخه ۴ یا IPv٤ همان چیزی است که معمولاً زمانی که از آدرس IP حرف می‌زنیم، به کار می‌بریم. در واقع تاکنون رایج ترین نسخه آی پی بوده و حدود ۹۶ درصد ترافیک کل اینترنت جهان از این نسخه از آی پی استفاده می‌کنند (طبق آمار ویکی‌پدیا). هر دستگاهی که از پروتکل اینترنت استفاده کند به طور حتم باید دارای یک آدرس IP باشد. البته IPv٤ اشاره به پروتکل نسخه چهارم اینترنت دارد ولی از آن جایی که ما در این پست آدرس IP را مورد بررسی قرار می‌دهیم از پرداختن به خود پروتکل خودداری می‌کنیم.در این نسخه، IP آدرس ها یک عبارت عددی ۳۲ بیتی (شامل ۴ بخش ۸ بیتی) هستند که با استفاده از سه نقطه (.) از هم جدا شده اند. ساختار عددی این ورژن مانند عبارت زیر است:

YYY.YYY.YYY.YYY

در این عبارت Y ها متغیرهای عددی هستند که آی پی نهایی را مشخص می‌کنند .این آدرس می‌تواند چیزی شبیه به ۱۴۴،۷۶،۱۶۸،۱۸۷ باشد. هر بخش جدا شده به وسیله نقطه می‌تواند یک عدد ۰ تا ۳ رقمی، از عدد ۰ تا ۲۵۵ را در خود نگه دارد. به عبارت بهتر، دامنه آدرسIP هایی که در اختیار داریم از ۰،۰،۰،۰ تا ۲۵۵،۲۵۵،۲۵۵،۲۵۵ است.از آن جایی که این نوع اعداد برای کامپیوتر هیچ مفهموی ندارند، معمولاً در این گونه موارد از بیت‌ها برای بیان مطلب استفاده می‌شود. برای کامپیوتر تبدیل شده این آدرس به بیت کاربرد دارد. تبدیل شده آی پی آدرس ۱۴۴،۷۶،۱۶۸،۱۸۷ به باینری عبارت زیر است:

۱۰۰۱۰۰۰۰،۰۱۰۰۱۱۰۰،۱۰۱۰۱۰۰۰،۱۰۱۱۱۰۱۱

نکته: چون IPv٤ دارای ۳۲ بیت است و خود آی پی نیز از چهار قسمت تشکیل شده است، یعنی هر قسمت یک بایت یا ۸ بیت یا یک Octet است، بنابراین آخرین حدی که می‌توان در آن بایت ذخیره کرد ۲۵۶ است. با توجه به این که ما از رقم صفر نیز می‌توانیم استفاده کنیم پس ۲۵۵ آخرین عددی است که می‌توانیم در هر بخش از آن استفاده کنیم.همان طور که می‌بینید عبارت ۱۰۰۱۰۰۰۰ تبدیل شده قسمت اول آی پی یعنی عدد ۱۴۴، ۰۱۰۰۱۱۰۰ تبدیل شده قسمت دوم آی پی یعنی عدد ۷۶ و ... است.

IPنسخه۶

باتوجه به افزایش دستگاه‌هایی که از پروتکل اینترنت استفاده می‌کنند، در آینده نزدیک هیچ آی پی آدرس نسخه ۴ ای آزاد باقی نخواهد ماند. بنابراین برای افزایش تعداد آی پی های آزاد، نسخه ۶ آن با نام IPv٦ طراحی شد. به دلیل تازه بودن این نسخه، استفاده از آن گسترده نیست و نسخه ۴ تقریباً به صورت کامل نیازهای آی پی

آدرس را تامین می‌کند. به عبارت دیگر تقریباً ۹۶ درصد کل ترافیک اینترنت از آی پی آدرس های نسخه ۴ استفاده می‌کنند. اما در آینده نزدیک حتماً به این نسخه از آی پی ها نیاز خواهیم داشت.در نسخه ۶، آی پی آدرس ها یک عبارت ۱۲۸ بیتی (شامل ۸ بخش ۱۶ بیتی) بوده و هر بخش به وسیله کاراکتر دو نقطه (:) از هم جدا می‌شوند. ساختار این آی پی نسبت به نسخه ۴ پیچیده تر بوده و یک IP آدرس نسخه ۶ مانند عبارت زیر است:

D۹۱:C۰۵۱:۰۰۰۰:۰۰۰۰:۰۰۰۰:E۰:۹۰۰۲A۰:F۲۶۰۱

همان طور که می‌بینید این نسخه دارای ۷ کاراکتر دو نقطه است که بخش‌های ۱۶ بیتی که شامل اعداد و حروف استاندارد هگزادسیمال ، حروف (A, B, C, D, E, Fهستند را از یکدیگر جدا کرده است. برای راحتی در خواندن این عبارت، قسمت‌هایی که دارای چهار رقم صفر هستند می‌توانند حذف شوند. بنابراین ساده شده آی پی آدرس بالا، عبارت زیر است: D۹۱::C۰۵۱:E۰:۹۰۰۲A۰F:۲۶۰۱

کلاسهای آدرس IP

متخصصان شبکه با توجه به نیاز شبکه تصمیم به استاندارد سازی و ایجاد کلاسهای مختلف شبکه نموده اند که با توجه به نیاز هر شبکه باید از آن استفاده نمود. ای پی آدرس ها در ۵ کلاس رده بندی میشوند و عدد اول هر آدرس نشان دهنده کلاس آن آدرس است.هرچند تقسیم بندی نامناسب فضای آدرس ، باعث هدر رفتن میلیون ها آدرسIP شده است. این مشکل در فرهنگ رایج اینترنت به مشکل سه خرس مشهور است.(برگرفته از داستان موطلایی و سه خرس).

Class A	۱-۱۲۶
Class B	۱۲۸-۱۹۱
Class C	۱۹۲-۲۲۳
Class D	۲۲۴-۲۳۹
Class E	۲۴۰-۲۵۴

شکل ۲۱-۱

مثلا ip ۱۰,۱۰,۱۰,۱ با توجه به اینکه رقم اول آن ۱۰ است نشان دهنده این است که در کلاس A می باشد. ip ۱۹۲,۱۶۸,۱۰,۲۰ با توجه به اینکه رقم اول آن ۱۹۲ است نشان دهنده این است که در کلاس C می باشد.

Loop Back

اگر دقت کرده باشید عدد ۱۲۷ در کلاسهای فوق نبود. به این دلیل است که این عدد برای کنترل کردن کارت شبکه مورد استفاده قرار می‌گیرد و اگر بخواهیم از صحت سالم بودن کارت شبکه اطمینان حاصل کنید، میتوانید از این آدرس استفاده کنید.

ping۱۲۷,۰,۰,۱

کلاس A

شبکه های کلاس A برای شبکه هایی که تعداد شبکه هایشان کم ,ولیکن تعداد میزبآن هایشان زیاد است و معمولا برای استفاده توسط انستیتوهای دولتی و آموزشی انتخاب می‌شوند مناسب هستند .در یک آدرس شبکه کلاس A , بخش نخست آن نشان

دهنده آدرس شبکه (network address) **و سه بخش دیگر نیز نشان‌دهنده آدرس میزبان** (host address) **در شبکه است. بطور مثال** IP ۱۰,۲۰,۲۰,۲۰ **عدد ۱۰ به آدرس شبکه و عدد ۲۰,۲۰,۲۰ به آدرس میزبان تعلق دارد .در آدرس دهی کلاس** A **اولین بیت صفر می‌باشد.**

۰۱۱۱۱۱۱۱ = ۰ + ۶۴ + ۳۲+ ۱۶+ ۸+ ۴+ ۲+ ۱ = ۱۲۷

کلاس B

شبکه های کلاس B **برای شبکه هایی که تعداد شبکه هایشان بین شبکه های بسیار بزرگ و بسیار کوچک است در نظر گرفته شده است .در یک آدرس شبکه کلاس** B **دو بخش نخست آن نشان دهنده آدرس شبکه و دو بخش دیگر نشاندهنده آدرس میزبان است .بطور مثال** IP ۱۷۲,۱۶,۱۰,۱۰ **عدد ۱۷۲,۱۶ به آدرس شبکه تعلق دارد و عدد ۱۰,۱۰ به آدرس میزبان تعلق دارد .در آدرس دهی کلاس** B **دومین بیت صفر می‌باشد.**

۱۰۱۱۱۱۱۱ = ۱۲۸+ ۰+ ۳۲+ ۱۶+ ۸+ ۴+ ۲+ ۱ = ۱۹۱

کلاس C

شبکه های کلاس C **برای شبکه هایی که تعداد شبکه های زیادی دارند اما میزبان کمتری دارند تدارک داده شده است .در یک آدرس شبکه کلاس** C**، سه بخش نخست آن نشان دهنده آدرس شبکه و بخش آخر به آدرس میزبان تعلق دارد .بطور مثال**

IP ۱۹۲,۱۶۸,۱۰,۲۰ عدد ۱۹۲,۱۶۸,۱۰ به آدرس شبکه و ۲۰ به آدرس میزبان تعلق دارد . در ای پی آدرس دهی کلاس C ، سومین بیت صفر میباشد.

۱۱۰۱۱۱۱۱ = ۱۲۸ + ۶۴+ ۰ +۱۶+ ۸+ ۴ + ۲+ ۱ = ۲۲۳

کلاس D

آدرس کلاس D برای Multicasting استفاده میشود.بدلیل اینکه این آدرس رزو شده است بهمین دلیل از بحث درباره آن خوداری می‌کنیم.در کلاس D چهارمین بیت صفر می‌باشد.

۱۱۱۰۱۱۱۱= ۱۲۸+۶۴+۳۲+۰+۸+۴+۲+۱=۲۳۹

Multicasting

فرایند ارسال یک پیام همزمان به بیش از یک مقصد در شبکه را گویند.

کلاس E

آدرس های کلاس E برای research and Development استفاده می‌شود.

در هر کلاس دو نوع IP Address(آدرس ای پی) موجود می‌باشد:آدرس ای پی خصوصی یا **Private address** وآدرس ای پی عمومی یا **public address**

Private address آدرس خصوصی

برای تعیین شبکه های محلی استفاده میشود و برای استفاده از آن ها احتیاج به هیچ

مجوزی نیست. آی پی خصوصی برای استفاده در شبکه خصوصی (مانند شبکه داخلی ادارات و شرکت‌ها) یا شبکه محلی بوده ، یعنی این آی پی در شبکه خصوصی یا شبکه محلی دارای اعتبار و قابل استفاده است . در واقع برای جلوگیری ازهدردهی آی‌پی در هر کلاس، یک محدوده آی‌پی برای شبکه خصوصی در نظر گرفته شده است. در ضمن برای اتصال یک شبکه خصوصی به اینترنت از پروتکل NAT[۴۷] استفاده می‌شود به این ترتیب که نشانی خصوصی به یک یا چند نشانی منحصربه‌فرد عمومی ترجمه می‌شود .

public address یا آدرس عمومی

برای تعیین شبکه های عمومی استفاده میشود و باید از سازمان IANA[۴۸] مجوز داشت. چگونه می‌توان تشخیص داد ای پی عمومی است یا خصوصی ؟ برای IP های خصوصی یک Range یا دامنه موجود میباشد اگر IP در آن Range بود خصوصی است در غیر اینصورت IP عمومی است.

PRIVATE IP ADDRESS		
Class A	۱۰.۰.۰.۰	۱۰.۲۵۵.۲۵۵.۲۵۵
Class B	۱۷۲.۱۶.۰.۰	۱۷۲.۳۱.۲۵۵.۲۵۵
Class C	۱۹۲.۱۶۸.۰.۰	۱۹۲.۱۶۸.۲۵۵.۲۵۵

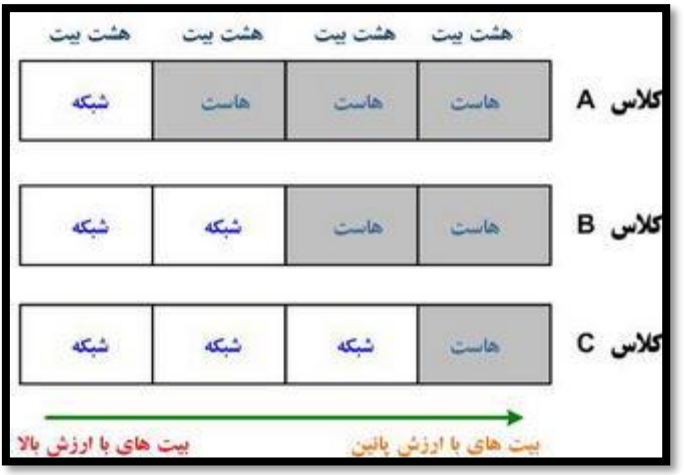
شکل ۲۲-۱

ID های شبکه

مشخصه شبکه (network ID) و یا آدرس شبکه ، گره هائی را که بر روی شبکه منطقی یکسانی قرار دارند ، مشخص می نماید . در اکثر موارد، یک شبکه منطقی

[۴۷] Network Address translation
[۴۸] **Internet Assigned Numbers Authority**

مشابه یک سگمنت فیزیکی شبکه بوده که محدوده های مرزی آن توسط آدرس IP روترها تعریف می گردد . در برخی موارد ، چندین شبکه منطقی بر روی شبکه فیزیکی یکسانی وجود داشته که از روشی با نام Multinetting استفاده می نمایند. تمامی گره ها در یک شبکه منطقی یکسان ، مشخصه شبکه (Network ID) یکسانی را به اشتراک می گذارند. در صورتیکه تمامی گره ها بر روی یک شبکه منطقی یکسان ، بدرستی پیکربندی نگردند (عدم لحاظ نمودن مشخصه شبکه یکسان) ، عملیات روتینگ و عرضه بسته های اطلاعاتی با مشکل مواجه خواهد شد . مشخصه شبکه ، می بایست منحصر بفرد در نظر گرفته شود. مشخصه میزبان (host ID) و یا آدرس میزبان ، یک گره موجود در شبکه را مشخص می نماید . یک گره می تواند یک روتر و یا یک میزبان (یک ایستگاه کاری ، سرویس دهنده و یا سایر سیستم های مبتنی بر TCP/IP) باشد . مشخصه میزبان ، می بایست در هر سگمنت شبکه منحصر بفرد باشد .



شکل ۲۳-۱

Subnetmaskچیست؟

این آدرس نشان می‌دهد چه مقدار بیت متعلق به آدرس شبکه و چه مقداربیت متعلق به آدرس میزبان(هاست) است.

Class	A	B	C
IP	۱۰.۱۰.۱۰.۱	۱۷۲.۱۶۸.۸۸.۹۸	۱۹۲.۱۶۸.۱۰۰.۳
Subnet Mask	۲۵۵.۰.۰.۰	۲۵۵.۲۵۵.۰.۰	۲۵۵.۲۵۵.۲۵۵.۰

شکل ۲۴-۱

قسمتی که ۲۵۵ است متعلق به network **و قسمتی که ۰ است متعلق به** host **می باشد.**

CIDR[۴۹]چیست؟

اصطلاح دیگری که شما باید با آن آشنا بشوید CIDR **است این بطور اساسی یک روش است که ISP[۵۰]ها برای تخصیص دادن یک مقدار از آدرس به یک کمپانی و یا مشتری استفاده می‌کنند. زمانی که شما یک دسته آدرس را از یک** ISP **دریافت می-کنید چیزی شبیه به این۱۹۲,۱۶۸,۱۰,۳۲ /۲۸ است.این به شما** subnet mask **شما را می‌گوید .نشان** slash **به معنای این است که چه مقدار ازبیت ها روشن است. بدیهی است که بیشترین۳۲/ است،زیرا یک** byte **است،یعنی ۸** bit**، پس ۴*۸=۳۲ اما بخاطر داشته باشید که بیشترین** subnet mask **میتواند ۳۰/ باشد، زیرا شما باید حداقل دو بیت برای** host bits **نگه دارید. بطور مثال در کلاس**A defult subnet, mask**۲۵۵,۰,۰,۰ است ،این بدین معنی است که اولین** byte **از** subnet mask

[۴۹] **C**lassless **I**nter**—D**omain **R**outing

[۵۰] Providers Internet Service

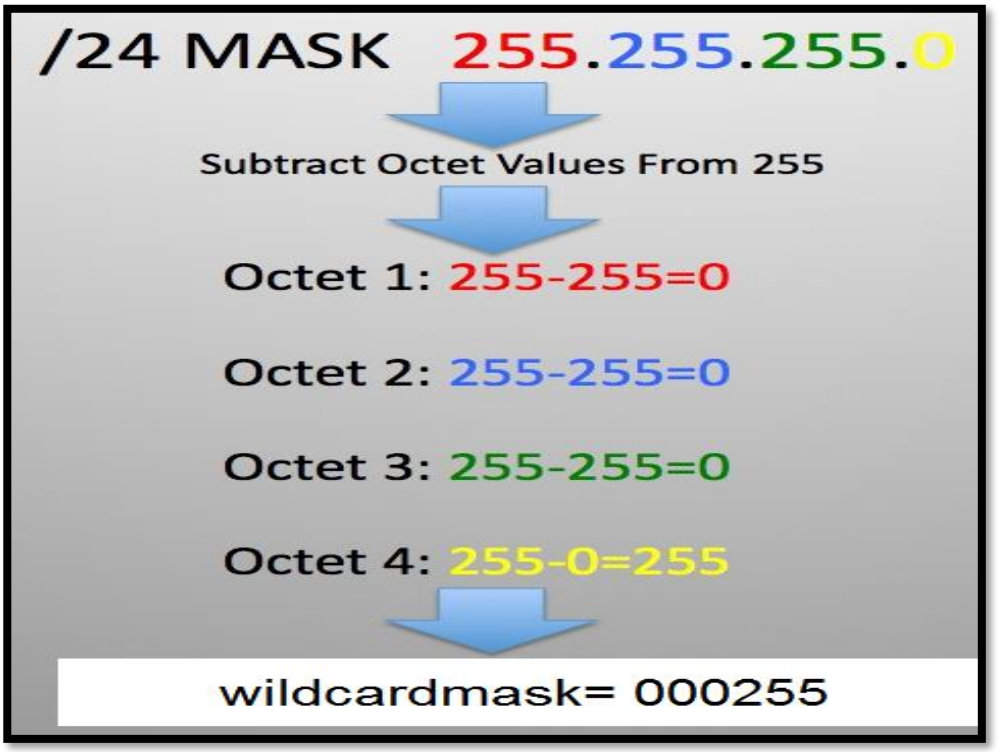
همگی یک است (۱۱۱۱۱۱۱۱) وقتی استناد به علامت slash کنیم بطور مسلم چیزی معادل ۸/ ۲۵۵,۰,۰,۰ است، زیرا هشت بیت دارد .همچنین subnetmask برای کلاس B ۲۵۵,۲۵۵,۰,۰یا۱۱۱۱۱۱۱,۱۱۱۱۱۱۱,۰,۰ است و همچنین میتوانیم تعریف کنیم ۱۶/ .

Subnet Mask	CIDR value
۲۵۵.۰.۰.۰	/۸
۲۵۵.۱۲۸.۰.۰	/۹
۲۵۵.۱۹۲.۰.۰	/۱۰
۲۵۵.۲۲۴.۰.۰	/۱۱
۲۵۵.۲۴۰.۰.۰	/۱۲
۲۵۵.۲۴۸.۰.۰	/۱۳
۲۵۵.۲۵۲.۰.۰	/۱۴
۲۵۵.۲۵۴.۰.۰	/۱۵
۲۵۵.۲۵۵.۰.۰	/۱۶
۲۵۵.۲۵۵.۱۲۸.۰	/۱۷
۲۵۵.۲۵۵.۱۹۲.۰	/۱۸
۲۵۵.۲۵۵.۲۲۴.۰	/۱۹
۲۵۵.۲۵۵.۲۴۰.۰	/۲۰
۲۵۵.۲۵۵.۲۴۸.۰	/۲۱
۲۵۵.۲۵۵.۲۵۲.۰	/۲۲
۲۵۵.۲۵۵.۲۵۴.۰	/۲۳
۲۵۵.۲۵۵.۲۵۵.۰	/۲۴
۲۵۵.۲۵۵.۲۵۵.۱۲۸	/۲۵
۲۵۵.۲۵۵.۲۵۵.۱۹۲	/۲۶
۲۵۵.۲۵۵.۲۵۵.۲۲۴	/۲۷

شکل ۲۵-۱

Wild Card Mask چیست؟

در جواب معمولا می گویند ، برعکس Subnet Mask است وبرای بدست آوردن آن مقدار هر octet را از۲۵۵ کم می کنیم. حاصل برابر با Wild Card Mask است.



شکل ۲۶-۱

Default gateway

برای اینکه کامپیوتر هایی که روی شبکه های متفاوت هستند یعنی بخش Network ID آن ها متفاوت است با هم ارتباط داشته باشند نیاز به یک دروازه یا default gateway می باشد.در واقع default gateway، IP Address نزدیکترین و اولین اینترفیس یک روتر است که با شبکه ای که با آن در ارتباط است در یک رنج IP قرار دارد.

معرفی پروتکل های مسیریابی یا روتینگ

بصورت کلی ما پروتکل های مسیریابی را به سه دسته کلی تقسیم بندی می کنیم :

بردار– فاصله یا[۵۱] : پروتکل های بردار- فاصله از معیار Hop Count یا تعداد روترهای مسیر برای متریک[۵۲] در جدول مسیریابی خود استفاده می کنند. الگوریتم مورد استفاده در اینگونه از پروتکل ها بسیار ساده است و جدول مسیریابی با محاسبات ساده ریاضی ایجاد می شود. پروتکل های بردار- فاصله معمولا برای شبکه های کوچکی که کمتر از ۱۶ عدد روتر در آن ها وجود دارد مورد استفاده قرار می گیرند در واقع این نوع پروتکل ها با کم کردن تعداد روترهای مسیر از به وجود آمدن حلقه[۵۳] در شبکه یا بهتر بگوییم Routing Loop در شبکه جلوگیری می کنند. این پروتکل ها در وهله های زمانی معین جداول مسیریابی خود را با یکدیگر یکسان سازی می کنند ، یکی از مشکلات الگوریتم های بردار- فاصله در این است که کلیه اطلاعات موجود در جداول مسیریابی را حتی با کوچکترین تغییر برای سایر روترهای

[۵۱] Distance-Vector
[۵۲] Metric
[۵۳] Loop

مجموعه ارسال می کنند و[۵۴] به روزرسانی افزایشی را در واقع پشتیبانی نمی کردند که در نسخه های جدید الگوریتم های بردار- فاصله این مشکل حل شد. الگوریتم های مسیریابی مثل RIPv۱ و IGRP از این نوع پروتوکل‌های مسیریابی هستند.

پروتوکلهای های حالت پیوند یا Link-State: در پروتکل های مسیریابی که بصورت Link State کار می کنند تفاوت محسوسی با حالت بردار- فاصله وجود دارد.الگوریتم های مورد استفاده در این نوع پروتکل ها نسبت به بردار- فاصله ها کاملا متفاوت عمل می کند و دارای پیچیدگی های خاص خود می باشد ، در این الگوریتم ها از فاکتورهایی مثل Hop Count ، فاصله ، سرعت لینک و ترافیک بصورت همزمان برای تعیین بهترین مسیر و بهترین cost برای انجام عملیات مسیریابی استفاده می شود. در این پروتوکل ها که نام دیگر آن ها Shortest Path First است،هر روتر سه جدول جداگانه را ایجاد می کند. یکی از این جداول وضعیت همسایگانی را که مستقیما به آن متصل است در خود نگه داری می کند. در جدول دیگر، توپولوژی تمامی شبکه ها نگه داری کرده و از جدول سوم برای نگه داری اطلاعات روتینگ استفاده می کند. این پروتوکل ها نسبت به پروتوکل های بردار – فاصله، دارای اطلاعات بیشتری در رابطه با شبکه و ارتباطات بین شبکه ای می باشند. پروتوکل‌های Link-State از الگوریتمی به نام دایجسترا[۵۵]برای تعیین پایینترین هزینه برای روت‌ها استفاده می کنند. روترهایی که از پروتکل های Link State استفاده می کنند ، فقط زمانی جداول مسیریابی همدیگر را یکسان سازی می کنند(وضعیت لینک را برای سایر روترها ارسال می کنند)، که چیز جدیدی به جداول مسیریابی یکی از روتر ها اضافه شده باشد. به همین دلیل هم کمترین ترافیک را در

[۵۴] Incremental Update
[۵۵] Dijkstra

هنگام یکسان سازی جداول مسیریابی با همدیگر ایجاد می کنند. الگوریتم های مسیریابی مثل OSPF و IS-IS از این نوع پروتکل های Link State هستند.

پروتوکل های مسیریابی ترکیبی یا Hybrid : همانطور که از نام این نوع پروتکل مسیریابی نیز پیداست این نوع پروتکل ترکیبی از پروتکل های بردار- فاصله و وضعیت است و در واقع مزایای هر یک از این نوع پروتکل ها را در خود جای داده است.زمانیکه صحبت از قدرت پردازشی روترها می شود از قابلیت های بردار- فاصله ها و زمانیکه صحبت از تبادل جداول مسیریابی در شبکه می باشد از قابلیت های Link State ها استفاده می کند. امروزه تقریبا همه شبکه های بزرگ در دنیا از پروتکل های Hybrid استفاده می کنند ، الگوریتم مسیریابی مثل EIGRP از انواع پروتکل های Hybrid Routing هستند. پروتکل های مسیریابی را می توان از لحاظ پارامترهای مختلف در گروه های جداگانه قرار داد.یکی از تفاوت ها در ماسک مربوط به آدرس ها در داخل پیام های ارسالی می باشد.بدین صورت که برخی از آن ها ماسک مربوطه را نیز در داخل پیام ارسالی گنجانده ولی برخی دیگر این کار را نمی کنند.به ترتیب پروتکل های دسته اول را Classless وپروتکل های دسته دوم را Classful گویند.

Classful routing

مشخصات کلی مربوط به این گروهIP آدرس ها:

۱)عمل Summarization در مرز بین شبکه ها بصورت خود به خود انجام می گیرد.

۲)عملیات Summarization در مورد route هایی که بین شبکه های ناشناخته منتقل می شوند انجام شده و به صورت آدرس های با کلاس استاندارد در خواهند آمد.

۳)پیام هایی که بین Subnet **های یک شبکه کلاس استاندارد منتقل می شوند،دارای ماسک(سابنت ماسک) مربوط به آدرس ها نیستند.**

۴)پروتکل های Classful **فرض را بر این می گیرند که**Interface **های مربوط به تمامی روترها به شبکه هایی با ماسک یکسان متصل گشته اند ودلیل نگنجاندن ماسک مربوطه در داخل پیام های ارسالی نیز همین مسئله است.**

۵)شامل پروتکل های RIPv۱ **و** IGRP **می باشد.**

طرز هدایت پیام ها توسط پروتکل های Classful **، وابسته به قانون های مربوط به آن هاست.بدین صورت که اگر مورد متناظری در داخل جدول** routing **وجود داشته باشد،پیام دریافت شده به طرف همان مقصد هدایت خواهد شد. اگر هیچ مورد متناظری در داخل جدول وجود نداشته باشد،پیام از بین خواهد رفت.حتی اگر از یک** Default Route**نیز استفاده شود، تنها در صورتی استفاده از آن مجاز خواهد بود که هیچ نوع مورد متناظری در داخل جدول وجود نداشته باشد.بدین معنی حتی در صورت وجود شبکه اصلی در داخل جدول** route **پیام ها از بین رفته و به سمت** Default Route**نیز ارسال نخواهند شد.**

محدودیت های مربوط به این دسته پروتکل ها:

۱-پروتکل های Classful **باعث از دست رفتن آدرس های بیشتری می شوند.**

۲-استفاده از ویژگی VLSM **در داخل شبکه مجاز نیست.**

۳-بدون استفاده از VLSM **اندازه جدول روتینگ بیش از حد نرمال افزایش یافته و بنابراین پیام های** Update **انتقالی بین روتر ها نیز دارای سایزی بزرگتر خواهند بود.**

Classless routing

پروتکل های فوق برای حل محدودیت های موجود در پروتکل های Classful **مورد استفاده قرار می گیرند.**

مشخصات کلی این دسته از آدرس Ip **ها:**

۱.Interface**های متصل به یک شبکه لایه سوم می توانند از ماسک های متفاوتی استفاده نمایند.**

۲.شامل پروتکل هایBGP ،RIPV۲،IS-IS،EIGRP، OSPF**می شوند.**

۳.استفاده از ویژگی CIDR **در داخل شبکه مجاز می باشد.**

۴.استفاده از هر نوع Stigmatization **دستی و اتوماتیک در مورد**Route **های موجود در جدول** Routing **مجاز می باشد.**

برای اینکه پروتکل های Classful **نیز از برخی مزایای موجود در پروتکل های** Classless **برخوردار گردند، دستور** IP CLASSLESS **را می توان اجرا نمود.البته بصورت** Default**،دستور مزبور در نسخه های اخیر** IOS **فعال گشته است.**

VLSM[۵۶]

VLSM در استاندارد RFC ۱۸۱۲ **تعریف شده و اجازه استفاده از** Subnet Mask**های با اندازه مختلف در خلال یک آدرس با کلاس استاندارد را به ما می دهد. به بیان ساده : استفاده بهینه از فضای آدرسی که در اختیارمان قرار داده شده است .فرض کنید که دو سگمنت را در شبکه ایجاد کرده ایم که یکی شامل ۲**

[۵۶] Variable Length Subnet Masking

دستگاه بوده و دیگری یک شبکه LAN با دستگاههای زیاد می باشد. در این-صورت یک Subnet Mask مناسب برای یک ارتباط نظیر به نظیر یا Point-to-Point می تواند به صورت ۲۵۵,۲۵۵,۲۵۵,۲۵۲ باشد که تعداد ۲ آدرس را برای دو دستگاه موجود در اختیار ما قرار می دهد. همچنین یک Subnet Mask مناسب برای آن شبکه LAN می تواند به صورت ۲۵۵,۲۵۵,۲۵۵,۱۹۲ باشد که تعداد ۶۲ آدرس را برای هر شبکه در اختیار ما قرار می دهد. به کار بردن ۲۵۵,۲۵۵,۲۵۵,۲۵۲ به علت تعداد آدرس کمی که ارائه میدهد برای یک شبکه LAN مناسب نبوده و به همین شکل بکار بردن ۲۵۵,۲۵۵,۲۵۵,۱۹۲ در یک ارتباط نظیر به نظیر، جایی که ما فقط نیاز به دو آدرس داریم، باعث هدر رفتن مقدار زیادی از آدرس ها خواهد شد. یک راه حل برای این مشکل این است که Subnet Mask را در حد وسط قرار دهیم و از هدر رفتن بیشتر آدرس ها جلوگیری کنیم. اما این کار نیز دارای اشکال است زیرا که از طرف دیگر باعث کم شدن مقدار آدرس های موجود برای شبکه LAN خواهد شد .VLSM .راه حل مناسب تری را برای حل این مشکل ارائه می‌دهد. با استفاده از این خاصیت می توان MASK های با اندازه مختلف را در شبکه ای که از یک آدرس IP با کلاس استاندارد استفاده می کند بکار برد.

خصوصیات VLSM

VLSM ما را قادر به بکارگیری MASK های با اندازه مختلف برای یک کلاس استاندارد آدرس IP می نماید. پروتکل هایی که در زمره پروتکل های Classful قرار میگیرند یعنی پروتکل های RIP ۱ و IGRP ، از ایده VLSM پشتیبانی نمی کنند. برای همین هم برای استفاده از مزیت هایی که VLSM ارائه می دهد نیاز

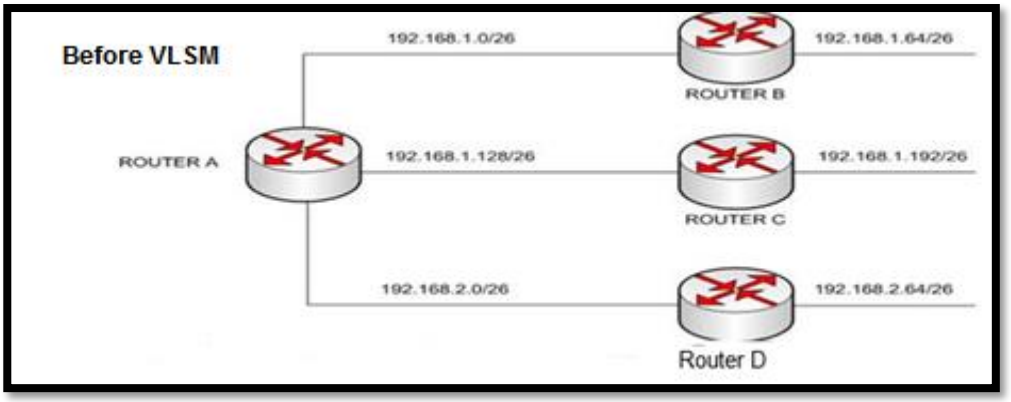
به بکارگیری پروتکل های Classless **مانند**BGP ، EIGRP، IS-IS، OSPF، RIP ۲ **داریم .**

مزیت های VLSM شامل دو مورد مهم زیر است :

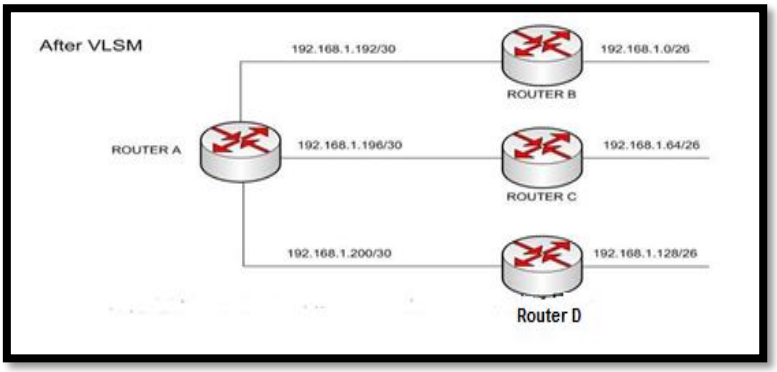
۱.استفاده هر چه بهتر از فضای آدرسی که در اختیار ما قرار گرفته است .

۲.استفاده از خصوصیت Route Summarization

همانطوریکه مورد اول اشاره کرد، با استفاده از VLSM **می توان از فضای آدرسی که در اختیار ما قرار داده می شود به بهترین شکل استفاده کرد. این شکل مثال ساده ای را قبل و بعد از** VLSM **نشان می دهد .**



شکل ۲۷-۱



شکل ۲۸-۱

در این مثال یک روتر در داخل شبکه خودی وجود دارد (روتر A) که توسط اتصالات WANبه روترهای دیگر (B,C,D) در جاهای دیگر وصل شده است. در هر یک از این سایت ها حداکثر تعداد ۵۰ عدد دستگاه وجود دارد و بنابراین subnet mask را برابر با ۲۶/ انتخاب نمودیم . در قسمت بالای شکل که از VLSM استفاده نشده است. فقط می توان یک MASK که برابر با ۲۵۵,۲۵۵,۲۵۵,۱۹۲ بوده و حداکثر ۶۲ آدرس برای هریک از شبکه ها ارائه می دهد را در کل شبکه بکار برد. بخاطر تعداد شبکه ها یاSubnet های مورد استفاده باید از دو آدرس در کلاس C استفاده نمائیم که در این صورت آدرس های زیادی در شبکه WAN به هدر خواهند رفت . در قسمت بعدی آدرس دهی شبکه را با استفاده از VLSM انجام داده ایم. در این مثال شبکه های دور (Remote) از ۲۶و شبکه خودی از ۳۰به عنوان ماسک استفاده می کنند و بدین صورت فقط یک آدرس در کلاس C برای آدرس دهی کل دستگاههای شبکه مورد نیاز خواهد بود و در نتیجه از به هدر رفتن آدرس های زیادی در اتصالات WAN جلوگیری به عمل خواهد آمد .

برای آدرس دهی با روش VLSM مراحل زیر را به ترتیب باید طی نمود:

۱.آن شبکه یا سگمنتی را که دارای بیشترین تعداد دستگاه خواهد بود مشخص می کنیم .
۲. بهترین ماسک ممکن را برای بزرگترین شبکه تعیین می نماییم .
۳.سپس شروع به نوشتن شبکه های ایجادی به وسیله ماسک تعیین شده می کنیم .
۴.برای شبکه های که دارای تعداد دستگاه کمتری هستند، یکی از شبکه های ایجادی را تخصیص داده و متناسب با مقدار دستگاه موجود در آن شبکه، ماسک مناسب را تعیین می کنیم .
۵. دوباره اقدام به نوشتن شبکه های ایجادی با استفاده از ماسک نعیین شده جدید می کنیم .
۶. برای هر یک از شبکه های کوچکتر بعدی، مراحل ۴ به بعد را تکرار می نمائیم .
عملیات انجام گرفته، در واقع تقسیم کردن شبکه ای که خود تقسیم شده است، به شبکه های کوچکتر و در صورت لزوم تقسیم بندی مجدد آن ها می باشد و بدین صورت است که از فضای آدرسی که در اختیار ما گذاشته شده است می توان به مناسب‌ترین حالت بهره لازم را برد. برای مثال فرض کنید که آدرسی در کلاس C و به صورت ۱۹۲,۱۶۸,۱,۰ تحویل گرفته ایم و سه شبکه LAN که به ترتیب دارای تعداد ۱۲۰ دستگاه، ۶۰ دستگاه و ۳۰عدد دستگاه هستند نیز در اختیار داریم. بر طبق مراحل گفته شده ۱ و ۲ بزرگترین شبکه ما دارای ۱۲۰ عدد دستگاه بوده که با توجه به آدرس داده شده، ماسک مناسب به صورت ۲۵/۱۹۲,۱۶۸,۱,۰ خواهد بود که ۱۲۸ عدد آدرس را ارئه می دهد. در مرحله ۳ شروع به نوشتن شبکه های ایجادی با استفاده از ماسک جدید می کنیم:

۱۹۲,۱۶۸,۱,۰/۲۵ - ۱۱۹۲,۱۶۸,۱,۱۲۸/۲۵

فرض کنید که آدرس ۱۹۲,۱۶۸,۱,۰ ۲۵را به این شبکه که دارای ۱۲۸ عدد دستگاه است تخصیص داده ایم. حالا ما دارای دو شبکه باقیمانده هستیم که یکی دارای ۶۰ عدد و دیگری دارای ۳۰ عدد دستگاه می باشد. در مرحله بعدی دوباره اقدام به انتخاب بزرگترین شبکه موجود خواهیم کرد. بنابراین شبکه ای که درای ۶۰ دستگاه می باشد را برگزیده و سپس مراحل ۴ به بعد را بار دیگر در مورد این شبکه نیز تکرار می کنیم. فکر می کنید کدام ماسک بهترین انتخاب برای شبکه ای با ۶۰ عدد دستگاه باشد ؟ اگر حدس شما ۲۶می باشد، بهترین گزینه را انتخاب نموده اید که در این صورت تعداد ۶۲ آدرس در اختیار خواهید داشت. سپس شبکه های ایجادی را با استفاده از ماسک جدید دوباره می نویسیم

۱۹۲,۱۶۸,۱,۱۹۲/۲۶ - ۱۱۹۲,۱۶۸,۱,۱۲۸/۲۶

در این شرایط نیز ما ۱۹۲,۱۶۸,۱,۱۲۸ ۲۶ را به این شبکه که دارای ۶۰ دستگاه می باشد تخصیص داده و سراغ شبکه ای که دارای ۳۰ دستاه می باشد می رویم . همانطوریکه می بینید ما دارای یک فضای آدرس دهی اضافی با ۶۲ آدرس هستیم که می توان آن را به شبکه دارای ۳۰ دستگاه تخصیص داد. اما باز هم می توان از به هدر رفتن آدرس های بیشتر در این مرحله نیز جلوگیری به عمل آورد .بنابراین به مرحله ۴ رفته و بار دیگر ماسک مناسب برای ۳۰ عدد دستگاه را به صورت ۲۷ خواهد بود تعیین می کنیم. اگر شبکه های ایجادی جدید را به وسیله این ماسک جدید بنویسیم، دو شبکه جدید خواهیم داشت

۱۹۲,۱۶۸,۱,۲۲۴/۲۷ - ۱۱۹۲,۱۶۸,۱,۱۹۲/۲۷

اگر مورد اولی را به شبکه مزبور اختصاص دهیم، باز هم مورد دوم باقی می ماند که می توان برای رشد بیشتر شرکت در آینده از آن استفاده نمود .همان‌طوریکه مشاهده

کردید به وسیله استفاده از VLSM می توانید بهترین شرایط را در هنگام بکارگیری آدرس های IP خلق نمائید .

توصیه می گردد که در هر شبکه، تعدادی آدرس را نیز برای دستگاههای دیگری که ممکن است در آینده در آن شبکه تعبیه شوند به صورت رزرو شده نگه دارید .برای نمونه در مثالی که زده شد، به وسیله بکار بردن ماسک ۲۷/ دو شبکه جدید که هرکدام ۳۰ عدد آدرس را ارائه می دهند در اختیار خواهیم داشت.

مسیر دهی ایستا و پویا[۵۷]

مسیر دهی ایستا این قابلیت را به مدیریت شبکه می دهد که بتواند بصورت دستی یک سری روت های خاص را در جدول مسیریابی روتر ایجاد کند .مسیریابی پویا از پروتکل های مسیریابی[۵۸] یا برای شناسایی شبکه ها و مقصدها و همچنین پیدا کردن بهترین مسیر برای رساندن بسته اطلاعاتی به مقصد استفاده می کنند.مسیریابی پویا این قابلیت را به جدول مسیریابی می دهد که بتواند زمانیکه یک روتر خاموش است یا در دسترس نیست یا اینکه یک شبکه جدید به مجموعه اضافه می شود این تغییرات را در جداول مسیریابی اضافه کند . مسیریابی پویا ،با استفاده از پروتکل های مسیریابی این قابلیت را دارند که بصورت مستمر با شبکه تبادل اطلاعات داشته باشند و وضعیت هر یک از روتر های شبکه را بررسی کنند و با استفاده از انتقال همگانی[۵۹] و یا انتقال یک به چند [۶۰]با هم ارتباط برقرار کنند و اطلاعات جداول مسیریابی را بروز کنند. با این روش همیشه توپولوژی شبکه بروز باقی می ماند و همگی دستگاه

[۵۷] Static routing , Dynamic routing
[۵۸] Routing Protocol
[۵۹] Broadcast
[۶۰] Multicast

های روتر شبکه از آخرین جداول مسیریابی بروز استفاده می کنند. از پروتکل های مسیریابی پویا می توان به RIP[۶۱] ، EIGRP[۶۲] وOSPF[۶۳] اشاره کرد.

پروتوکلهای کاربردی در شبکه و کارآیی آن ها

FTAM : (مدیریت و دسترسی انتقال فایل) که پروتکل دسترسی به فایل است

FTP : (پروتکل انتقال فایل) پروتکل انتقال فایل در اینترنت

SMTP : (پروتکل انتقال پستی ساده) پروتکل اینترنت برای انتقالات پست الکترونیکی

SNMP : (پروتکل مدیریت شبکه ای ساده) پروتکل اینترنت برای نظارت بر شبکه ها و اجزای شبکه

Telnet : پروتکل اینترنت برای برقراری ارتباط با میزبآن های راه دور و پردازش محلی داده ها

Gopher : پروتکلی برای در اختیار قرار گذاشتن اطلاعات با استفاده از سیستمی از منوها، صفحات یا اتصالاتی به Telnet است

NCP : پروتکل هسته مرکزی

UDP : پروتکل انتقال داده نا مطمئن

DNS : پروتکلی است که یک نام دامنه را به یک آدرس تبدیل می کند.

TCP : (پروتکل کنترل انتقال) از پروتکل TCP/IP برای ضمانت تحویل داده های متوالی

STP : قسمتی از پشته پروتکل IPX/SPX مربوط به شرکت Novell

NwLink : نسخه مایکروسافت IPX/SPX است

---

[۶۱] Routing Information Protocol
[۶۲] Enhanced Interior Gateway Routing
[۶۳] Open Shortest Path First

NetBEUI : پروتکل گسترش یافته کاربر NetBIOS (NetBIOS) ، اعمال سطح پایین شبکه مثل با اشتراک گذاشتن فایلها و چاپگرها را انجام می دهد)

ATP : پروتکل مبادلات Apple Talk

RIP : پروتکل مسیریابی مبتنی بر بردار–فاصله RFC اساس یک الگوریتم می باشد.

SLIP : پروتکلی که برای تبادل یک TCP/IP روی یک اتصال سریال می باشد مثل مودم.

PPP : پروتکلی بسیار پیشرفته تر از SLIP که برای اتصال سریال می باشد.

HTTP : پروتکلی که برای انتقال ابرمتن و صفحات وب در شبکه بکار می رود

NEWS : پروتکلی برای انتقال

BGP : یک پروتکل دروازه خارجی مبتنی بر RFC

ARP : پروتکلی که برای شناسائی آدرس یک ایستگاه براساس آدرس IP بکار می رود.

DHCP : پروتکلی جهت تخصیص آدرس های IP بصورت پویا است

CIDR : پروتکل مخصوص تعریف شده برای هر IP است

IP : (پروتکل اینترنت) از پروتکل TCP/IP برای تعیین مسیر و ارسال بسته

IPX : (تبادل بین شبکه ای پشته ها) از رشته پروتکل IPX/SPX شرکت Novell برای تعیین مسیر و ارسال بسته

DDP : پروتکل حمل داده های Apple Talk

ICMP : پروتکلی برای گزارش خطاها بر روی اینترنت است

CSMA/CD : هنگامی که در شبکه تصادم داده ها بوجود آید، یک دوره تناوبی انتظار، جهت کاهش تصادم ها تحمیل می شود.

نکته: مفهوم Load Balancing بدین شکل است که از ۲ یا چند سرویس دهنده مختلف برای انجام یک کار واحد بطور همزمان و متوازن استفاده کرد . سرویس دهنده ها می توانند DNS، Internet، Database و یا Computing باشند.

CHAP وPAP: پروتکل های تصدیق هویت (authentication) هستند که هر کدام امکانات و مزایایی را فراهم می‌کنند. pap یا Password Authentication Protocolیک پروتکل بسیار ساده و سریع و البته نا امن است که پسورد ها را بدون رمز نگاری دریافت و مورد بررسی قرار می‌دهد.

chapیا Challenge Handshake Authentication Protocol : این پروتکل پیچیده تر از pap است و امنیت بیشتری را تامین می‌کند . نکته قابل توجه در این پروتکل این است که username به صورت خام و clear textمنتقل شده ولی پسورد در شبکه عینا منتقل نمی‌شوند ، بلکه یک challange message که از سه فاکتور secret, session IDو password که با یک الگوریتم رمز نگاری (MD۵) به صورت hashدر آمده ،به جای پسورد به شکل خام و رمز نشده مورد مقایسه قرار میگیرد ، و اگر یکسان بود ارتباط برقرار میشود. پس در نتیجه علاوه بر اینکه پسورد ها به صورت رمز نگاری در شبکه منتقل میشوند ، هر دو طرف می بایست علاوه بر دانستن یوزرنیم – پسورد ، secret خاص را هم بدانند تا بتوانند ارتباط برقرار کنند و تصدیق هویت شوند . در غیر این صورت تلاش برای login شکست می‌خورد.

دستورات پر کاربرد در شبکه

برای وارد شدن به محیط CMD از دو روش متداول می توان استفاده کرد:

روش اول: به منوی Start/All Programs/Accessories رفته و سپس Command Prompt را اجرا کنید.

روش دوم: کلیدهای Win+R را زده تا وارد Run شوید سپس در کادر متنی cmd را تایپ کرده و با زدن OK برنامه خط فرمان اجرا خواهد شد.

دستورPing

دستور Ping یا Packet Internet Group از ساده ترین و کاربردی ترین ابزارهای خطایابی قابل دسترس TCP/IP است.این دستور برای تست اتصال یک دستگاه یا سیستم به سیستم های دیگر و تایید فعال بودن سیستم مقصد استفاده می شود.همچنین برای بررسی برقراری ارتباط با یک host در شبکه نیز از این دستور استفاده می شود.

دستور Tracert

این دستور، تنها برای انجام یک وظیفه ی اساسی طراحی شده است و آن نیز تعیین مسیری است که بسته های داده برای رسیدن به مقصد طی می کنند. این دستور با دستور ping متفاوت است. درواقع ping به شما می گوید که آدرسی که آن را ping کرده اید فعال یا runاست یا خیر و برقراری ارتباط را بررسی می کند اما tracert تک تک روترهایی را که بسته های داده در مسیر با آن برخورد خواهند داشت را برای کاربر نشان می دهد.در واقع زمانی که بسته های داده به مقصد نمی رسند و یا زمان پاسخ دستور ping زمانی نامعقول و طولانی باشد از این دستور استفاده می کنیم.

دستور ipconfig : نمایش سریع IP آدرس سیستم.

دستورGETMAC : با دستور GETMAC /V بی توان ، آدرس فیزیکی کارت شبکه های یک سیستم لوکال را بدست آورد.با دستور GETMAC /S [COMPUTER NAME /V]می توان آدرس فیزیکی کارت شبکه های یک سیستم راه دور را بدست آورد.

دستور route: تمامی routing table های موجود بر روی سرور را نشان می دهد

دستورARP: تبدیل آدرس ۳۲ بیتی IP به آدرس ۴۸ بیتی MAC

دستورRARP : تبدیل آدرس ۴۷ بیتی MAC به آدرس ۳۲ بیتی IP

فصل دوم: آموزش کار با نرم افزار Packet tracer

معرفی نرم افزار

نرم افزار Packet Tracer **یک محیط شبیه سازی برای کسانی است که قصد طراحی شبکه، توپولوژی، پیکر بندی، بررسی مشکلات و ... را دارند. کاربران می‌توانند به راحتی ابزارهای مورد نظر خود را در محیط شبیه سازی وارد نموده و توپولوژی مورد نظر خود را ایجاد کنند. پس از پیکر بندی شبکه ایجاد شده می توانند به بررسی ، تحلیل ورفع مشکلات آن بپردازند .انواع تکنولوژی ها و توپولوژی هایی که توسط این نرم افزار پشتیبانی می شود به این شرح هستند:**

اتصالات , stright ,cross ,consol: **فیبر نوری , سریال ، بی سیم و مودم.**

روترها، مشتمل برpat,dhcp ,NAT, VLSM , ACLs.

مسیر یابی، مشتعل بر RIP **، مسیرهای پیش فرض و استا تیک و** LOAD BALANCING.

ابرها، پل ها، هاب ها، access point**ها، تکرار کننده ها ، رایانه های شخصی، سرور ها چاپگرها.**

ابرها ، پل ها ، هاب ها ، access point**ها، تکرار کننده ها ، رایانه های شخصی، سرور ها و چاپگرها.**

مشاهده جداول مسیریابی و سوئیچینگ و ایجاد پل ، داده های OSI **و وضعیت لینک** Ping ، Ping**توسعه یافته و قابلیت**traceroute.

مدل سازی لایه های ۱ ، ۲ ، ۳ و ۴.

حالت Challenge **برای هدایت بسته ها توسط دانشجویان بر اساس الگوریتم های ابزارها.**

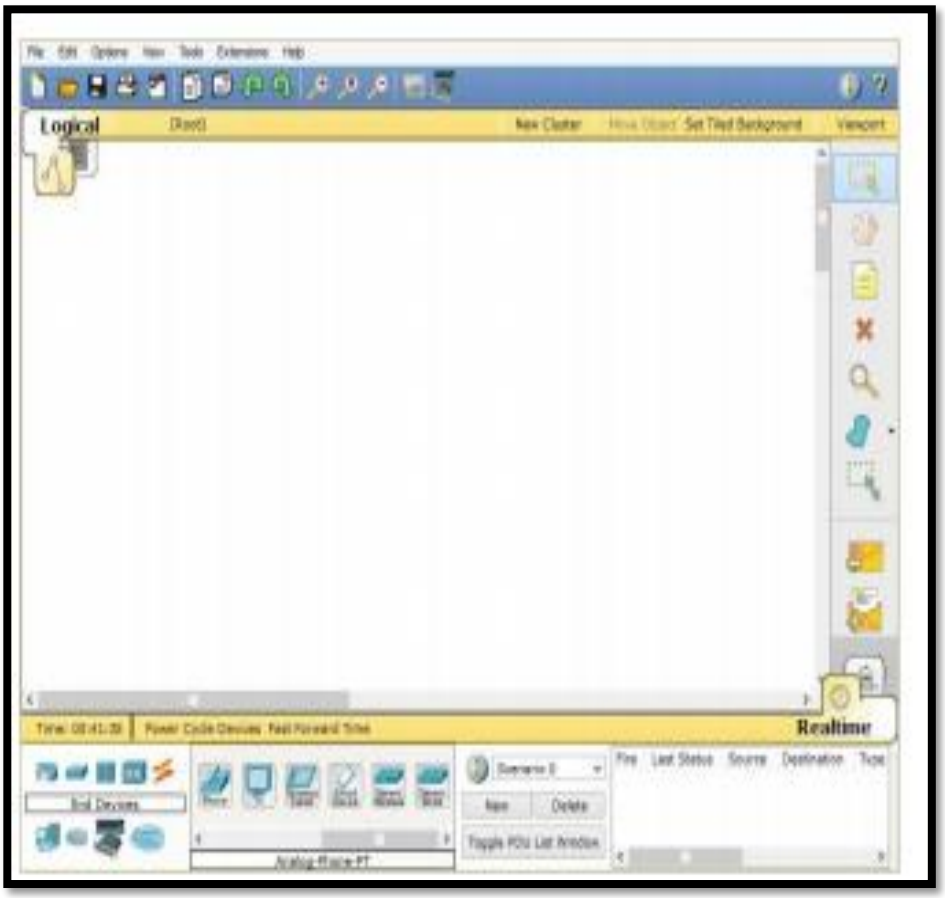
Activity Wizard ، برای تمرین طراحی، پیکربندی و رفع مشکلات در فعالیت ها.

نرم افزار Packet Tracer شامل دو فضای کاری منطقی و فیزیکی و دو حا Realtime و شبیه سازی است. هرشبکه را می‌توان در نمای منطقی ایجاد کرده و در حالت Realtime، اجرای آن را مشاهده نمود.

نصب نرم افزار در ویندوز و لینوکس

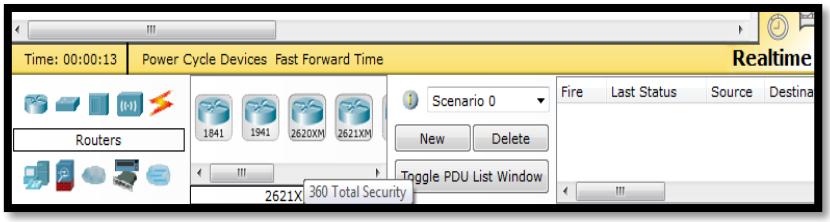
برای دانلود packet Tracer به وبسایتwww.netacad.com بروید و برروی گرافیک آن کلیک نمایید و پکیج مناسب برای سیستم خود را دانلود کنید. نصب این نرم افزار در ویندوز بسیار ساده است. برای راه اندازی، فایلی بنام Packet Tracer_Setup.exe را باز کنید، گواهینامه توافق را بپذیریدتا نصب شروع شود.کاربران لینوکس اوبونتو باید فایل متناسب با اوبونتو و کاربران لینوکس فدورا و... می‌بایست فایل مربوط به نسخه های نامبرده لینوکس را دانلود نمایند.

نمایی از محیط نرم افزار



شکل ۱-۲

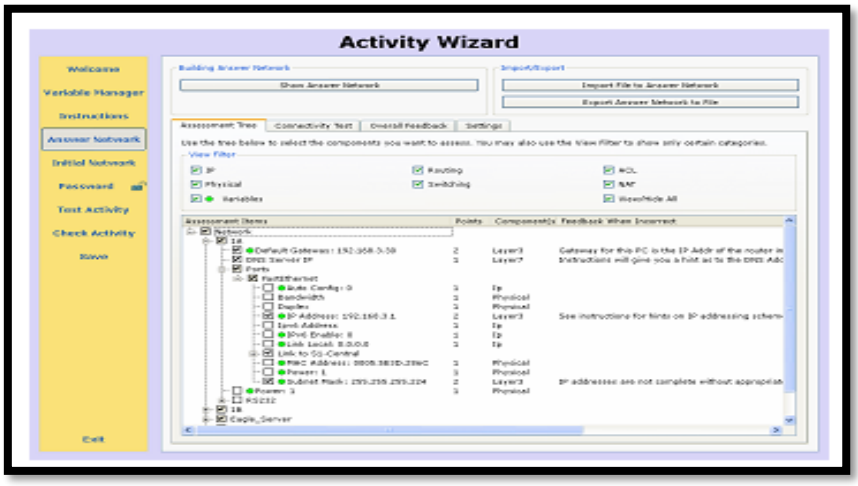
در این قسمت می توان مدل دستگاه مورد نظر را انتخاب کرد. انتخاب هر دستگاه به نوع شبکه ی شما مربوط می شود که آیا نیاز به روتر یا سوییچ دارید یا هاب، کاملا متفاوت می باشد. با کلیک بر روی دستگاه مورد نظر زیر مجموعه دستگاه مربوطه نمایش داده می شود و با کشیدن آن دستگاه به مرکز صفحه می توان آن را اضافه کرد.



شکل ۲-۲

برنامه جادوگر(Wizard) فعالیت

این برنامه به کاربران کمک می کند تا سناریوهای جدید را به راحتی خلق نموده وفعالیت‌های خود را انجام دهند.



شکل ۳-۲

ویژگی های Packet Tracer

- فضای کاری فیزیکی و منطقی
- مودهای بلادرنگ و شبیه سازی
- واسط خط فرمان یا CLI[۶۴]کاربرپسند
- لیست رویدادهای سراسری(Packet Sniffer)
- پشتیبانی از پروتکلهای LAN، سوئیچینگ،TCP/IP،مسیریابی و WAN
- جادوگر فعالیت و آزمایش های طبقه بندی شده
- پشتیبانی از سیستم عامل های مختلف
- پشتیبانی از زبان های مختلف
- ضمیمه شدن مستندات و راهنماهای خوب و قوی

پروتوکلهای مورد حمایتPacket Tracer

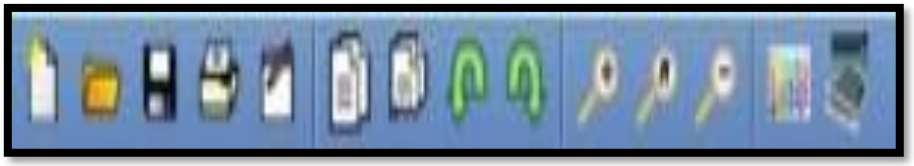
DHCP-DNS-SSH-Telnet-TFTP-HTTP-TCP-UDP-IPV٤-ICMP-ARP-IPV٦-EIGRP-OSPF-HDLC-Ethernet-PPP-ICMPV٦-Multi-Area-RIPV١/٢/ng-STP-RSTP-VTP-DTP-CDP-٨٠٢,١١-٨٠٢,١q Frame Relay–باز توزیع مسیر و سوئیچینگ چند لایه.

[۶۴] Command Line Interface

تشریح بخش های نرم افزار Packet Tracer

شکل ۴-۲

در این منو شما امکان استفاده از گزینه های Open, New, Save, Print, Copy, Paste, Undo, Redo, Drawing Palette **را دارید. در میان این گزینه ها تنها گزینه ناشناس** Drawing Palette **است. این گزینه به شما امکان کشیدن یک سری اشکال هندسی خاص مانند دایره و چهار را به شما می دهد که البته در آخرین نسخه از این نرم افزار امکان کشیدن چند ضلعی نا منظم را نیز به آن افزوده است.**

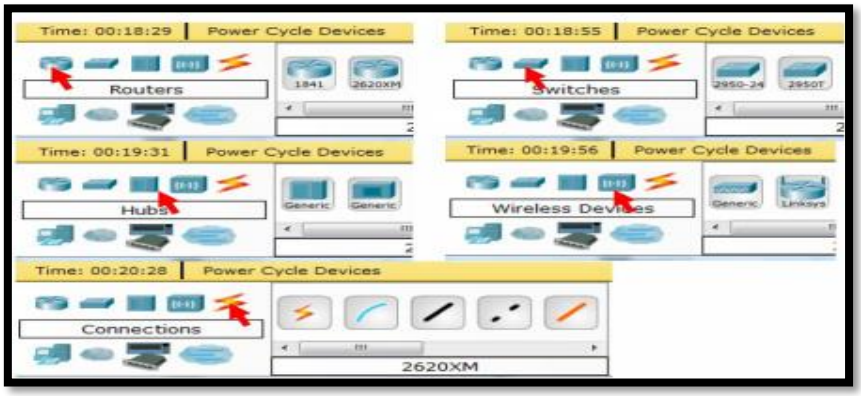


شکل ۵-۲

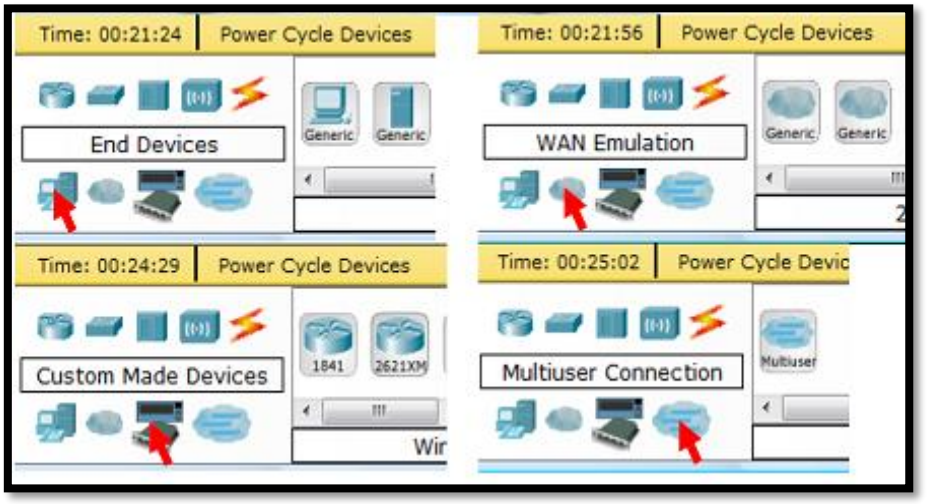
شکل ۶-۲

شکل ۷-۲

نمونه ابزارهای در دسترس



شکل ۸-۲

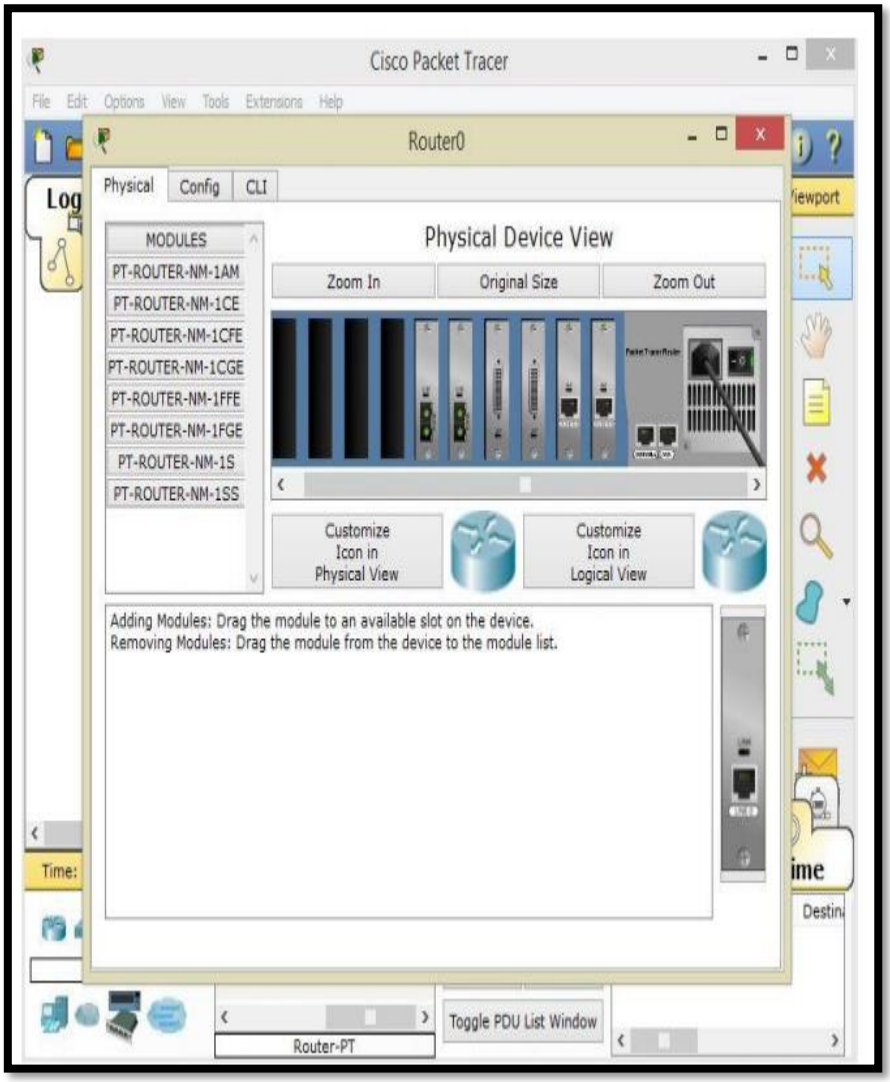


شکل ۹-۲

شروع کار

اضافه کردن دستگاه به صفحه نرم افزار

اول در قسمت Deviceمربوطه کلیک می کنیم. زیر مجموعه دستگاه در سمت راست نمایش داده می شود. بر روی مدل مورد نظر کلیک کرده و آن را به صفحه بکشید.(Drag& Drop). برای شروع کار با این نرم افزار باید نقشه شبکه خود را ترسیم کنید و به صورت منظم و شکیل برروی صفحه جاگذاری نمایید. برای شروع یک روتر را به صفحه اضافه کنید و برروی آن کلیک کنید:

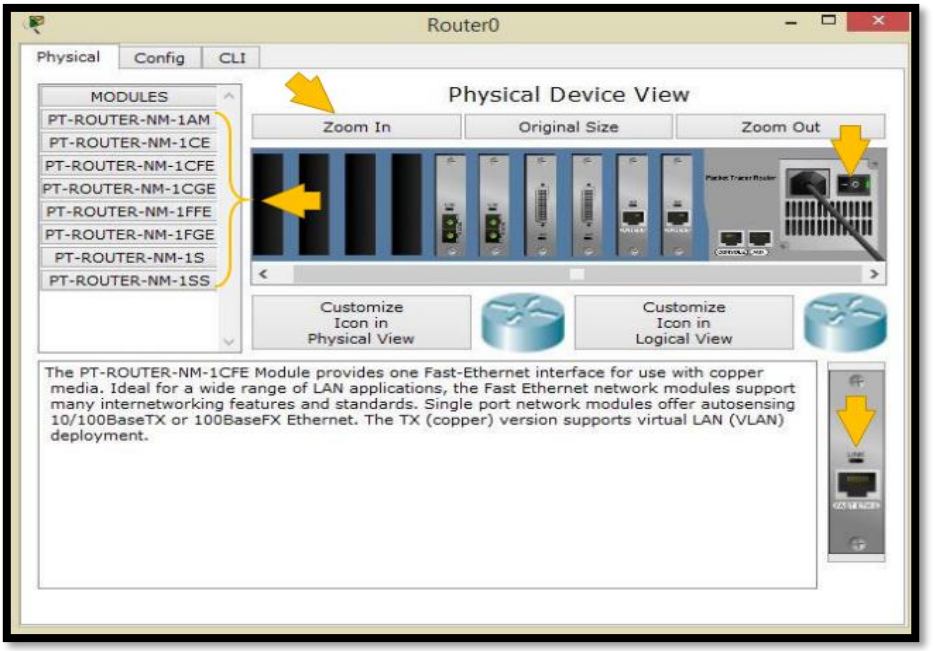


شکل ۱۰-۲

همانطور که در تصویر مشاهده می کنید، پنجره باز شده دارای سه برگه است که به اختصار به توضیح آن ها می پردازیم.

برگه Physical

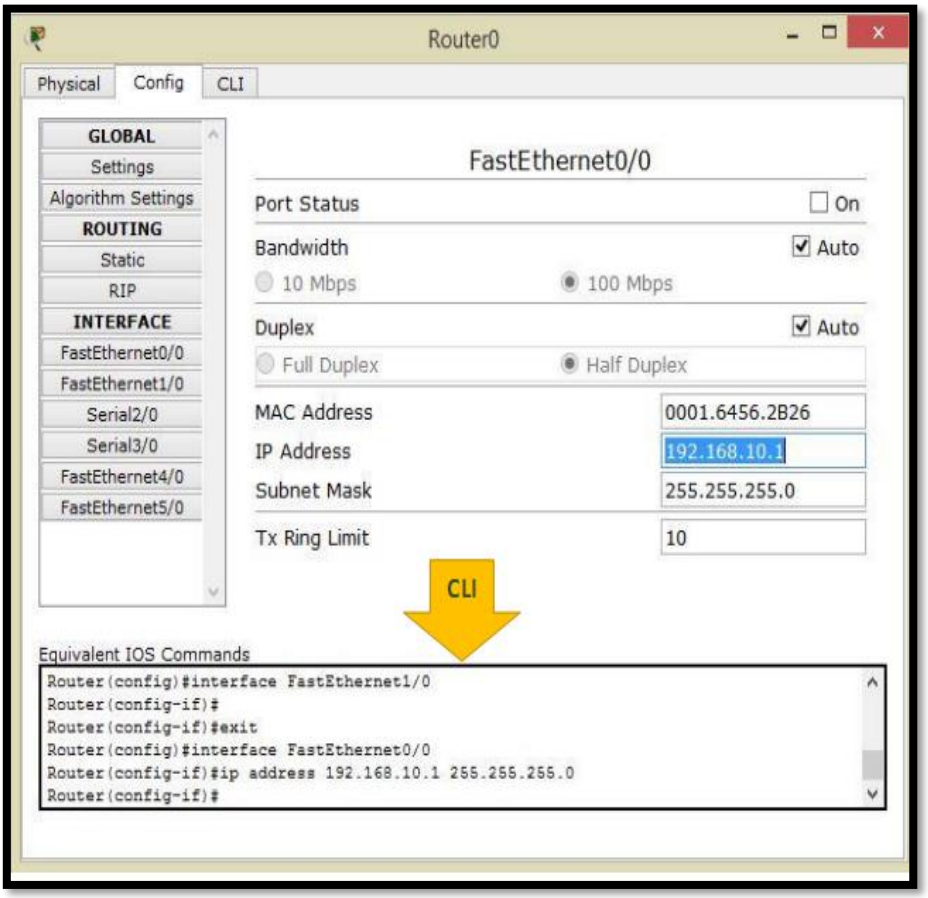
در این برگه به صورت فیزیکی می توانید اجزای دستگاه خود را مشاهده کنید و حتی به دستگاه خود ماژولهایی مانند کارت های شبکه با ورودیهای مختلف(فیبر نوری- کابل های شبکه – کابل سریال و ...) متصل نمایید.(طریقه اضافه کردن بصورت Drag & Drop**) می باشد.در این نرم افزار می توانید همانند دستگاه واقعی آنرا با استفاده از کلید خاموش یا روشن نمایید و دستگاه در حالت روشن اجازه نصب ماژول را به شما نمی دهد.**



شکل ۱۱-۲

برگهConfig

این قسمت یکی از مهمترین قسمت ها در پیکربندی دستگاه می باشد. همانطور که در تصویر مشاهده می کنید ، پورتهای مختلف این دستگاه نیازمند IP می باشند تا با روتر و سوئیچ های مربوطه کار کنند. معمولا برای ارتباط روتر با روتر از پورتSerialاستفاده می شود و برای اتصال روتر به سوییچ از پورت FastEthernet استفاده می گردد.بعد از Setکردن Ipحتما پورت مربوطه را روشن کنید.

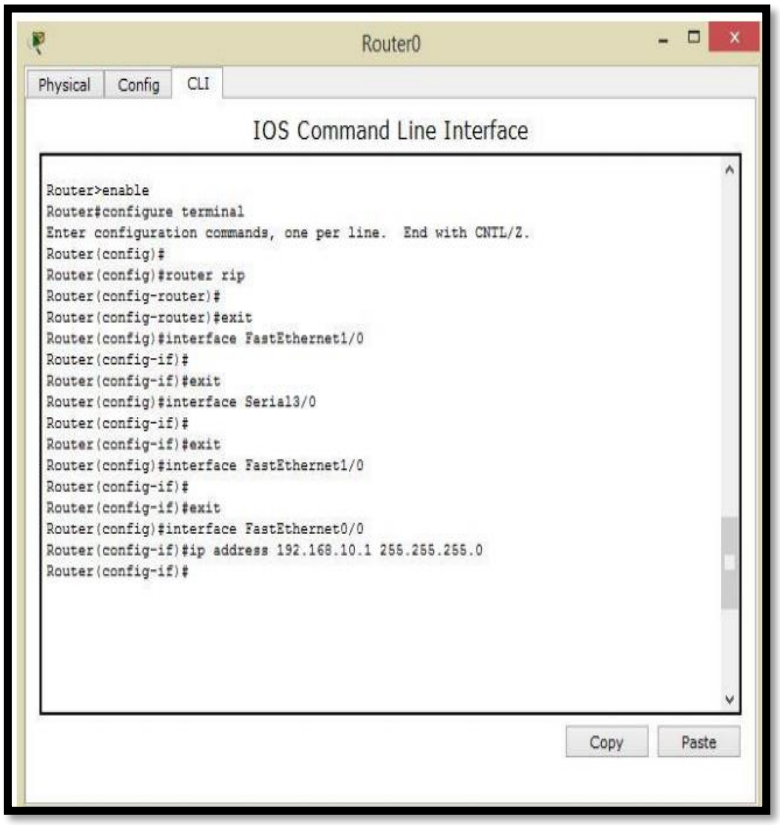


شکل ۲-۱۲

نکته: Fast Ethernet Interface **پورت اترنت با سرعت** Mbps ۱۰۰ **است.**

برگهCLI

این قسمت بخش اصلی دستگاه بوده و محل کدنویسیIOS **می باشد. تمامی تنظیمات و پیکربندی دستگاه در این قسمت انجام می شود.**



شکل ۱۳-۲

این ساده ترین راه دسترسی به رابط کاربری دستوردهی یک دستگاه است. بر روی یک دستگاه کلیک کنید و به تب CLI رفته و پردازش Boot را خواهید دید.

محیط CLI

برای تنظیم سیسکو دو سطح دسترسی وجود دارد:

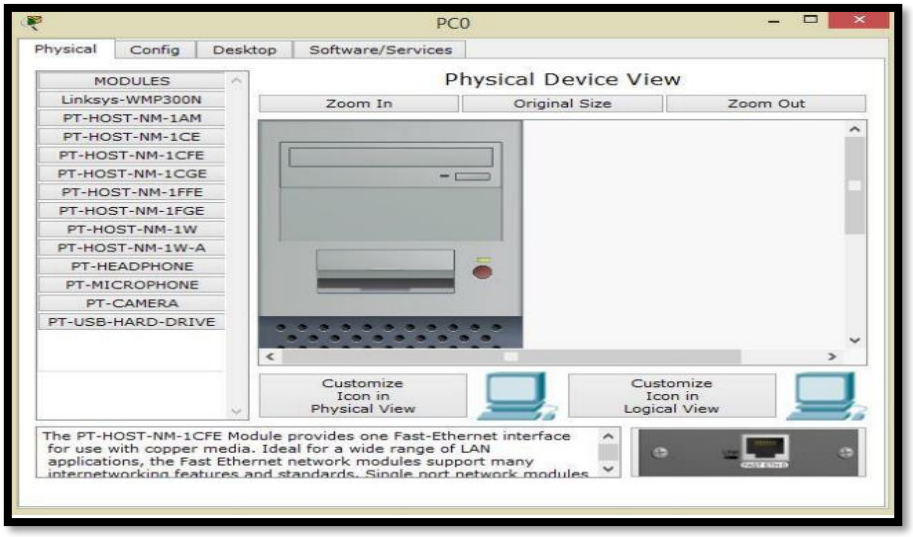
دسترسی کاربر (User-Mode)

دسترسی Admin (Privileged-Mode)

دسترسی کاربر یا Privilege=۱ **برای اپراتورهایی که به دسترسی محدودی نیاز دارند استفاده می‌شود. بطور مثال توانایی این را داشته باشند که یک** IP **را از روتر** Ping **کنند. این محیط** User=mode **نام دارد.**

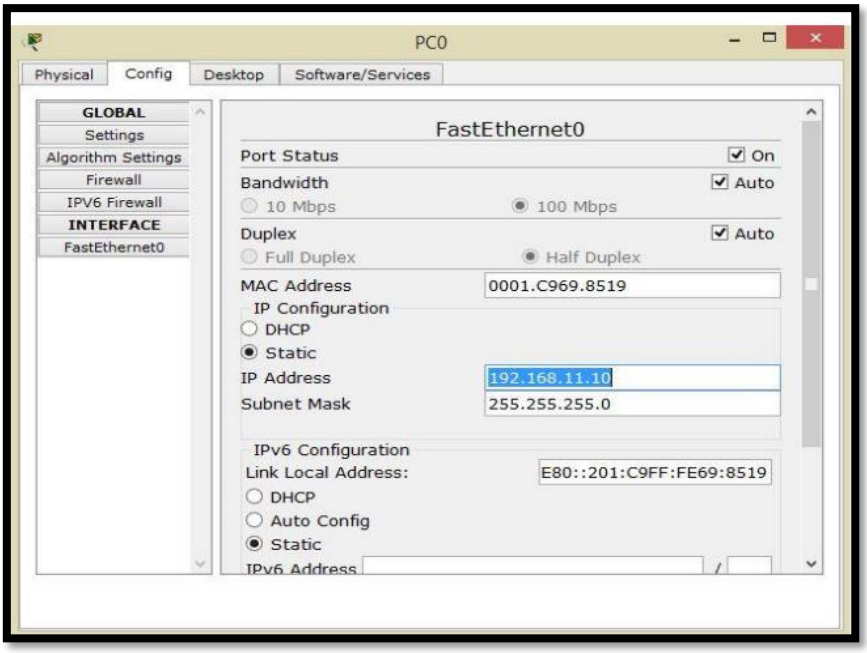
معرفی و تنظیمات End Devices

در این قسمت می توان تنظیمات مربوط به کارت شبکه را انجام داد و بصورت مجازی، IP **و** DNS **و...را پیکربندی کنیم. با اضافه کردن یک کامپیوتر وبعد از کلیک بر روی آن تصویر زیر را مشاهده می کنیم:**



شکل ۲-۱۴

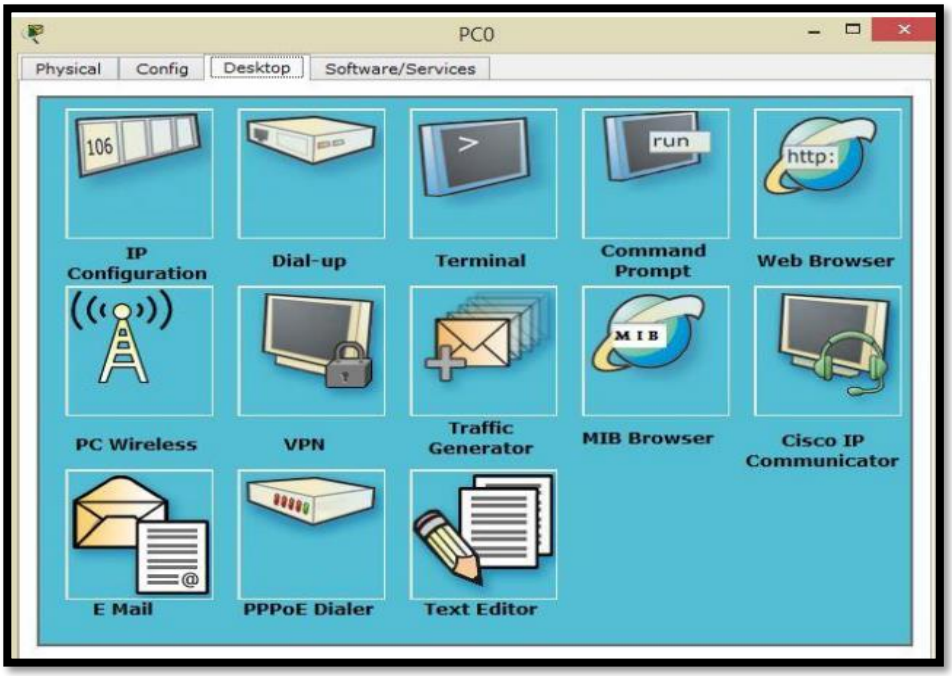
در سربرگPhysical می توان کارت شبکه را بصورت کابلی یا مجهز به فیبرنوری و وایرلس و یا سخت افزارهای جانبی دیگر مانند وب کم- میکروفون و... را اضافه کرد. برگه Config محل SetکردنIP-DNS- Gateway-Firewallو... است.در این قسمت میتوان تنظیمات کامپیوتر را بصورت DHCPیاSTATIC و در قسمت IPV٦ پروتکلهای مختلف نظیر TCP-UDP-ICMPرا تنظیم کرد.



شکل ۱۵-۲

برگهDesktop

این قسمت یک محیط تقریبا آشنا شبیه به ویندوز را نمایش می دهد. ابزارهای کاربردی و متنوعی در این بخش نشان داده شده اند مانندCMD-Terminal- مرورگر- برنامه ارسال ایمیل و ...را مشاهده کرد.

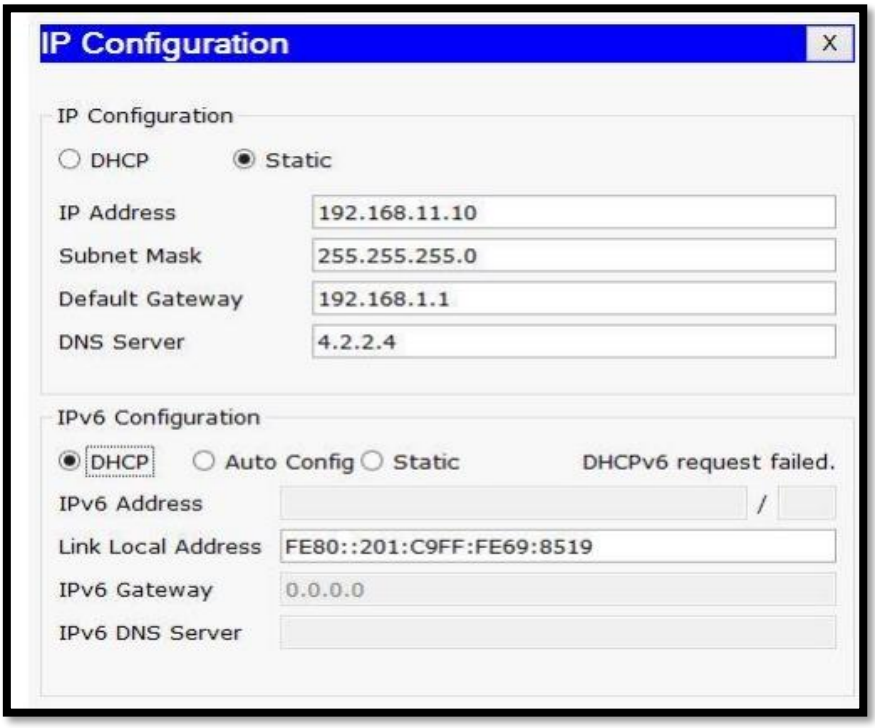


شکل ۱۶-۲

معرفی تعدادی از تنظیمات برگهِ Desktop

تنظیمIp Configuration

با کلیک بر روی این گزینه در برگه Desktopپنجره مربوطه باز می شود و می توانید مشخص کنید کارت شبکه به صورت DHCPیا Static باشد و در گزینه های زیر می توانیدDNS Sever-Default Gateway-Subnet Mask-Ip Addressرا Setنمایید.



شکل ۱۷-۲

بخش Terminal

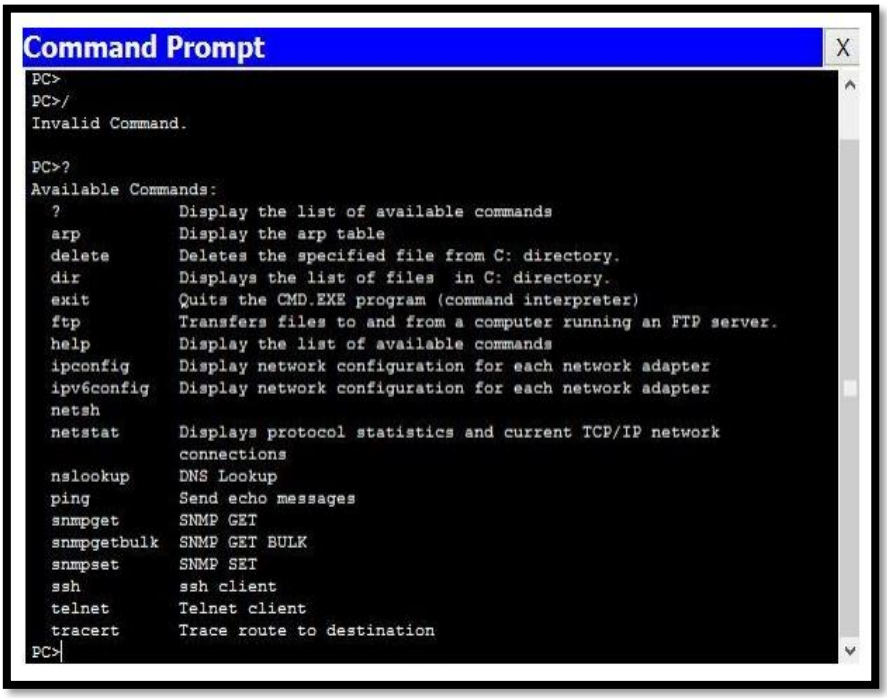
در این بخش می توانید میزان ارسال داده را برحسبBit برثانیه تعریف کنید و تعیین کنید که چه تعداد از بیت ها بر روی Terminalارسال و دریافت شوند.

شکل ۱۸-۲

بخشCMD یا Command Prompt

در برگه Desktop **و با کلیک بر روی گزینه** Command Prompt **پنجره مربوطه باز می شود. این پنجره همانند پنجرهCMD در ویندوز تمامی دستورات مربوط به**

تست شبکه و پیکر بندی را پشتیبانی می کند. بعد از ساخت شبکه مربوطه می توانید کامپیوترها را با دستور pingو ...تست کرده تا از صحت عملکرد شبکه آگاه گردید.



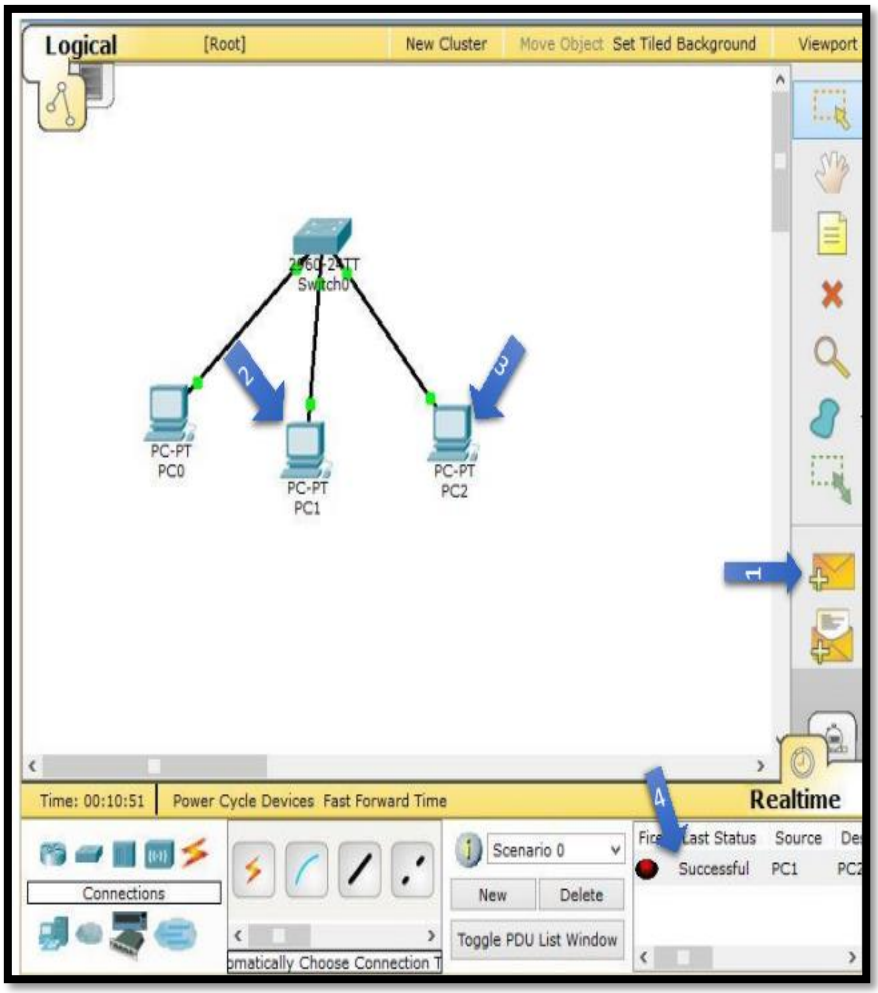
شکل ۱۹-۲

بخش Simulation

همانطور که در شکل مشاهده می کنید به دو صورت می توانید شبکه خود را تست نمایید و از صحت کارکرد آن مطمئن گردید.

۱. استفاده از PDU نوار ابزار کنار نرم افزار که به شکل پاکت می باشد.و در صورت به مقصد رسیدن اطلاعات از یک کامپیوتر به کامپیوتر دیگر پیغامsuccessful را نمایش می دهد. یعنی ارسال بسته ازpc1 به pc2 با موفقیت به انجام رسیده است.

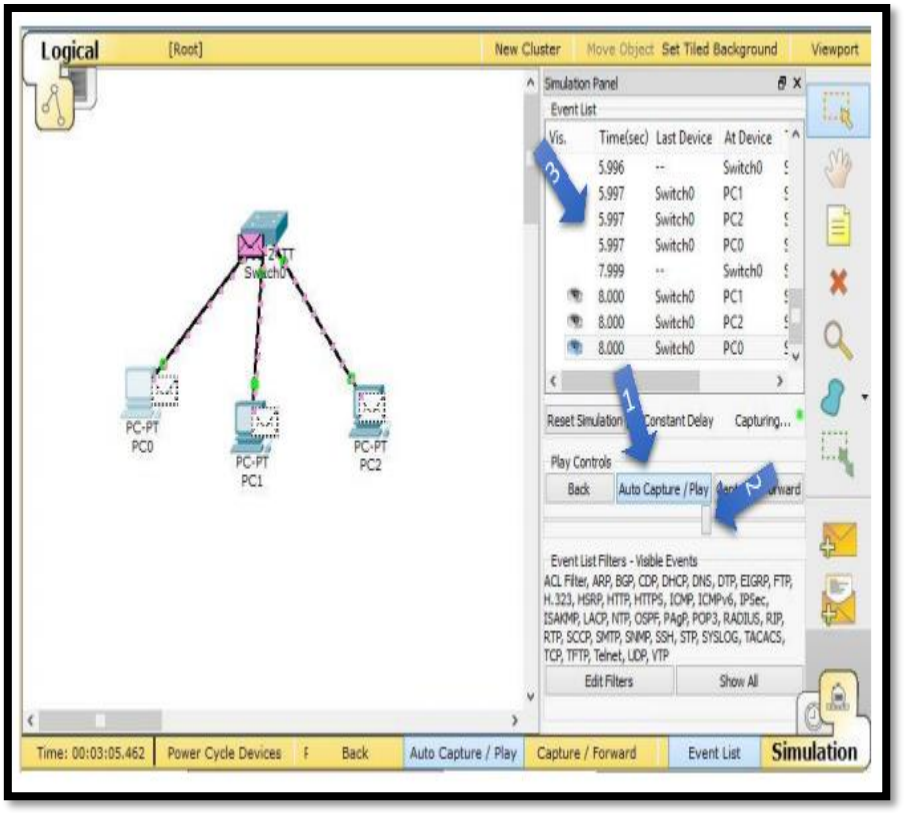
حالت اول



شکل ۲۰-۲

حالت دوم

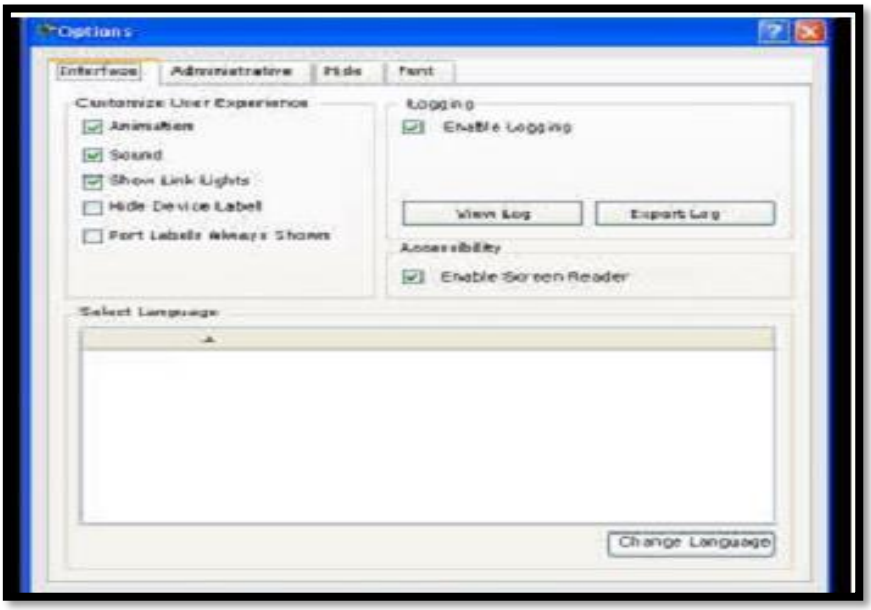
این حالت قسمت Simulation **نرم افزار می باشد که به صورت زنده و مجازی حرکت بسته ها را می توانید مشاهده کنید.دراین قسمت چنانچه بر روی گزینه** Auto Capture **کلیک کنید حرکت پاکتهارا بین کامپیوترها بصورت مجازی مشاهده می کنید و با نوار ابزار کشویی زیر آن می توانید سرعت ارسال را کمتر یا بیشتر نمایید.**



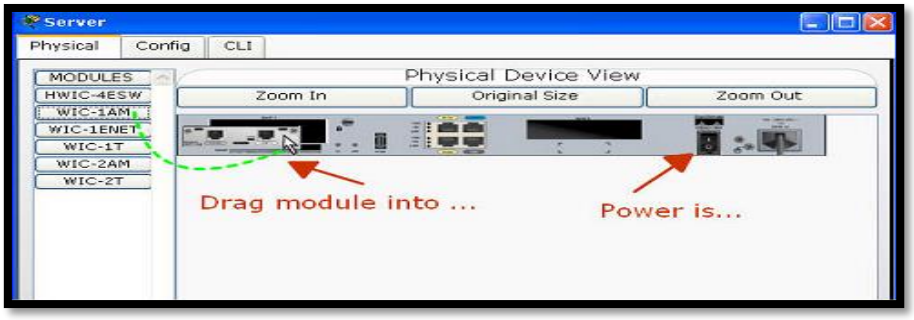
شکل ۲۱-۲

تنظیم علاقمندیها

نرم افزار Packet Tracer **را می توان به دلخواه تنظیم کرد. برای این کار از منوی** Option **دستور** Preferences **را اجرا کنید تا تنظیمات برنامه مانند تنظیم صدا، انیمیشن، مخفی کردن ابزارها یا پورت‌ها و تغییر فونت وزبان را مشاهده کنید.**



شکل ۲-۲۲



شکل ۲-۲۳

ایجاد اتصالات

برای ایجاد یک اتصال بین دو دستگاه، ابتدا روی آیکنConnections در کادر انتخاب نوع وسیله کلیک نمایید تا لیستی از انواع اتصالات موجود نمایش داده شود. سپس روی نوع کابل مورد نظر کلیک کنید. نشانگر ماوس به شکل اتصال تغییر خواهد کردو روی اولین وسیله کلیک کرده و واسط مناسب با کابل را انتخاب کنید.روی دومین وسیله نیز کلیک کرده و به همین ترتیب عمل کنید.یک کابل بین دو دستگاه ایجاد خواهد شد و در انتهای آن چراغ‌هایی وجود دارد که وضعیت اتصال را ددر دو طرف نمایش می دهد.

نوع کابل	شرح
 Console	اتصال کنسول بین رایانه ها مسیریاب ها یا سوئیچ ها برقرار می شود. برای ورود به بخش کنسول می بایست تنظیمات یکسانی در دو دستگاه برقرار شود. (parity ، stop bit و...)
 Copper Straight-through	کابل استاندارد اترنت برای اتصال بین دستگاه هایی که در لایه های مختلف قرار دارند. (مانند هاب به روتر، سوئیچ به رایانه، روتر به هاب و ...) و می تواند به پورت های زیر متصل شود. 10 Mbps Copper (Ethernet), 100 Mbps Copper (Fast Ethernet), 1000 Mbps Copper (Gigabit Ethernet)
 Copper Cross-over	کابل اترنت برای اتصال بین دستگاه هایی که در لایه های یکسان قرار دارند. (مانند هاب به هاب، رایانه به رایانه، رایانه به چاپگر و ...) و می تواند به پورت های زیر متصل شود. 10 Mbps Copper (Ethernet), 100 Mbps Copper (Fast Ethernet), 1000 Mbps Copper (Gigabit Ethernet).
 Fiber	برای اتصال بین پورت های فیبر نوری(100 Mbps or 1000 Mbps)
 Phone	اتصال خط تلفن می تواند بین دستگاه هایی که پورت مودم دارند برقرار شود. کاربرد استاندارد آن بین رایانه و ابر است.
 Coaxial	برای اتصال بین پورت های coaxial (نظیر مودم کابلی و ابر)
 Serial DCE and DTE	اتصال سریال معمولا یک اتصال WAN است و فقط می تواند بین پورت های سریال برقرار شود. برای استفاده از این اتصال باید clocking را در سمت DCE فعال کنید. سمت DCE با یک علامت ساعت در کنار پورت آن مشخص می شود.

شکل ۲۴-۲

وضعیت اتصال

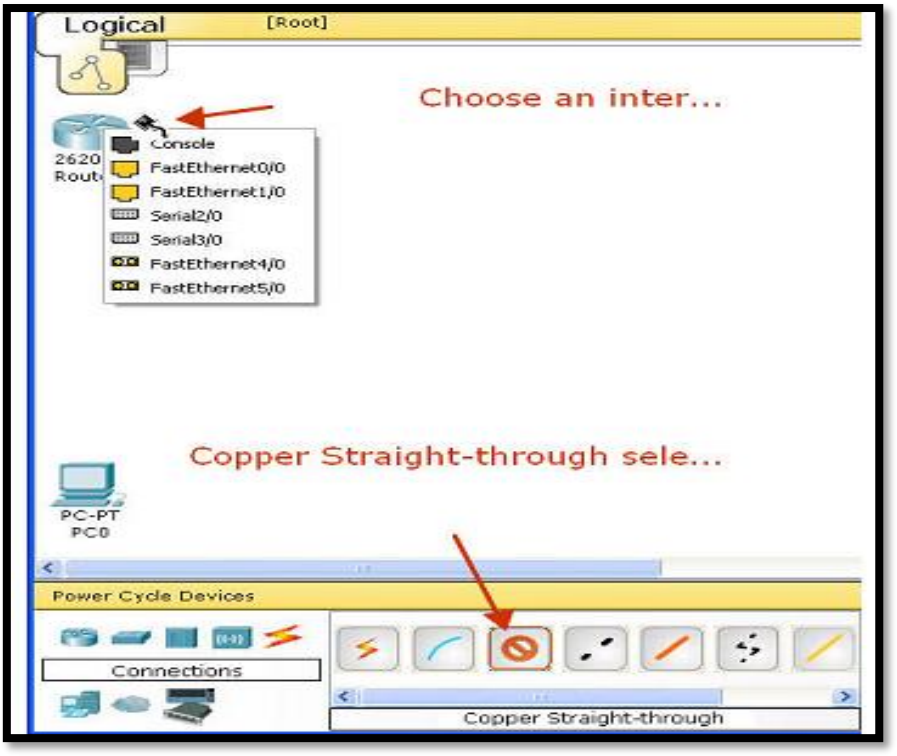
وقتی که دو وسیله به هم متصل می شوند، معمولا چراغهایی را در دو سمت اتصال مشاهده می کنید.

سبز روشن: اتصال فیزیکی up **است.**

سبز چشمک زن: اتصال فعال است.

قرمز: اتصالdown **است و سیگنالی پیدا نمی شود.**

کهربایی: پورت در وضعیت بلاک است.



شکل ۲۵-۲

تجهیزات و دستگاه های نرم افزار Packet Tracer

در کادر انتخاب نوع دستگاه Device Type در نرم افزار ؛ Switch یا Router را که با برچسب Generic هستند را انتخاب کنید. این ها دستگاه های معروف اجرایی در سیستم عامل سیسکو هستند اما درگاه هایی که ماژول ها را نگه داری میکنند متفاوت است.

روتر ها

یک روتر ، برقرای ارتباط بین دو شبکه ی منطقی را برقرار می سازد. هر روتر نرم افزار Packet Tracer می تواند با استفاده از دکمه ی خاموش/روشن Power کنترل شود. این خاصیت برای جلوه ی واقعی بخشیدن به شبیه سازی دستگاه ضروری است. ماژول ها فقط در صورت خاموش بودن کلید دستگاه می توانند حذف یا اضافه شوند. اگر پیکربندی درحال اجرا ذخیره نشده باشد، با خاموش شدن کلید Power آن پیکربندی از بین خواهد رفت. روترهای ذیل در نرم افزار Packet Tracer موجود اند:

(Cisco ۱۸٤۱) یک روتر سرویس مجتمع(ISR) است که دو پورت سریع Ethernet ، دو پورت پرسرعت رابط کاربری WAN(HWIC) و یک درگاه ماژول مجتمع پیشرفته AIM دارد.

(Cisco ۱۹٤۱) مشابه مدل قبلی است اما در سیستم عامل سیسکو ورژن ۱۵ اجرا می شود که دارای دو پورت پرسرعت Gigabit Ethernet است.

(Cisco ۲٦۲۰XM) یک روتر چندکاره با یک پورت پرسرعت Ethernet و دو درگاه کاردهای WAN و یک درگاه AIM است.

(Cisco ۲۶۲۱XM) مشابه مدل قبل است با این تفاوت که دارای دو پورت پر سرعت Ethernet است.

(Cisco ۲۸۱۱) این روتر سرویس مجتمع ISR دارای دو پورت Ethernet و چهار درگاه WIC و دو درگاه AIM است.

(Cisco ۲۹۰۱) دارای دو پورت Gigabit Ethernet ، ۴ پورت WIC و دو درگاه پردازنده ی دیجیتالی سیگنالDSP است. این روتر از IOS۱۵ استفاده می کند.

(Cisco ۲۹۱۱) دارای سه پورت Gigabit Ethernet و تمام قابلیت های مدل فوق است و در نسخه ی ۱۵ سیسکو اجرا می شود.

(Cisco-PT عمومی) یک روتر شخصی قابل ویرایش و اجرا روی سیستم عامل سیسکو است که دارای ۱۰ درگاه و ماژول های جداگانه است که نام هرکدام با PT شروع می شود.

سوئیچ ها

یک سوئیچ (که پل بریج چند پورته هم نامیده می شود) دو دستگاه یا تعدا بیشتر از دستگاه های مقصد را بهم دیگر متصل می سازد. هر پورت سوئیچ دارای یک دامنه ی قابل تداخل است. سوئیچ های زیر در نرم افزار امکان پذیر است :

(Cisco ۲۹۵۰-۲۴) این سوئیچ مدیریت شده دارای ۲۴ پورت سریع Ethernet است.

(Cisco ۲۹۵۰T-۲۴) یک عضو از خانواده ی سوئیچ های هوشمند سری Catalyst ۲۵۹۰ است و دو پورت Gigabit Ethernet به اضافه ی ۲۴ پروت سریع Ethernet است.

(Cisco ۲۹۶۰-۲۴TT) یک سوئیچ دیگر ۲۴ پورته است. سوئیچ قبل دارای یک مبدل رابط کاربری GBIC برای پورت گیگابیت است در حالی که این سوئیچ برای پورت گیگابیت یک ماژول قابل اتصال کوچک SFP دارد. این نکته را درنظر داشته

باشید که تفاوت ذکر شده درمورد سوئیچ های واقعی است و در نرم افزار شبیه سازی Packet Tracer تاثیری ندارد.

(Cisco ٣٥٦٠-٢٤PS) این سوئیچ از بقیه موارد فوق از این جهت متفاوت است که یک سوئیچ لایه ۳ است، یعنی در کنار عملیات سوئیچینگ می تواند کار روتر را هم انجام دهد. پسوند PS این سوئیچ نشانگر استفاده از منبع تغذیه ی خود Ethernet است که برای کار با IP دستگاه های قابل حمل مثل موبایل ها نیاز به آداپتور تغذیه ی جدا ندارد.

(Cisco Bridge-PT) یک دستگاه برای بخش بندی و سلول بندی کردن یک شبکه است و تنها دو پورت دارد و به همین دلیل پل نامیده شده است نه سوئیچ .

(Cisco PT سوئیچ عمومی) یک سوئیچ عمومی قابل اجرا روی IOS سیسکو و قابل شخصی سازی تا ۱۰ درگاه و شماری ماژول است. همانند روترها، سوئیچ ها نیز یک نوع عمومی ۱۰ پورته دارند که قابل ویرایش و شخصی سازی با ماژول های مورد نیاز است. بجز این نوع سوئیچ، بقیه سوئیچ ها قابل شخصی سازی نیستند و دارای کلید Power نمی باشند؛ چون که طبق سوئیچ واقعی آن مدل طراحی شده اند.

سایر دستگاه ها

نرم افزار Packet Tracer علاوه بر روتر و سوئیچ ها چند دستگاه دیگر به شرح ذیل را هم ارائه می کند که قابل شخصی سازی نیستند:

(HUB-PT) یک هاب شبکه، قدیمیترین روش برای اتصال چند دستگاه مقصد به همدیگر است و برای یادگیری و استفاده در نرم افزار مسیریاب بسته ای موجود است که دارای ۱۰ درگاه هم می باشد.

(Repeater-PT) این دستگاه که رله یا ترانسدیوسر هم نامیده می شود برای تقویت سیگنال در شبکه ی سیمی وقتی که فاصله ی دونقطه از هم زیاد باشند، مورد استفاده قرار میگیرد. همچنین دارای ۲ درگاه است.

جداکننده Spliter-PT) برای تفکیک یک رابط هم محور حاوی سیگنال تنها به دو شاخه ی مجزا است که دارای ۳ درگاه فیزیکی بوده و به هیچ وجه قابل شخصی سازی نیست.

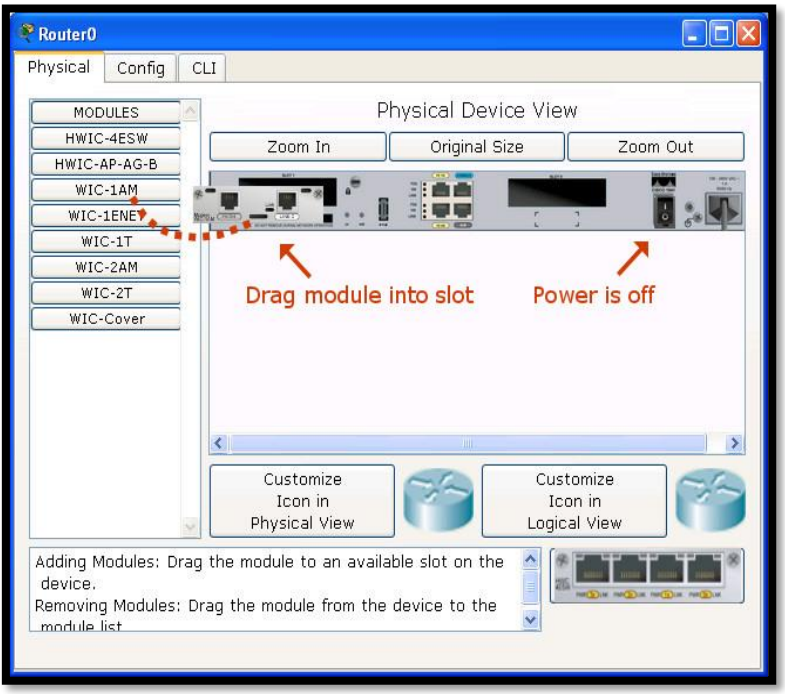
شخصی یا سفارشی سازی دستگاه ها با ماژول وافزودن ماژول‌ها

اکثر دستگاههای Packet Tracer محفظه های ماژولار دارند که شما می توانید ماژولها را در آن ها قرار دهید. در فضای کار، روی یک دستگاه کلیک کنید تا پنجره پیکربندی های آن نمایش داده شود. به طور پیش فرض شما در برگه Physical خواهید بود. یک تصویر محاوره ای از وسیله نیز در سمت راست و لیستی از ماژول های سازگار با آن در سمت چپ قرار دارد. شما می توانید تصویر را با دکمه های zoom in، Original Size وZoom out تغییر اندازه دهید.

یک ماژول دستگاه، بخشی از سخت افزار است که شامل چندین رابط کاربری است. برای مثال یک ماژول HWIC-٤ESW محتوی ۴ پورت پرسرعت(١٠MB/S) Ethernet است. مشابه یک روتر/سوئیچ واقعی باید دستگاه را به منظور حذف یا اضافه کردن ماژول خاموش کرد. دکمه ی Power در سمت راست هر دستگاه قرار داشته و با یک LED سبز رنگ برای حالت روشن دستگاه نمایش داده می شود. روی کلید کلیک کرده تا دستگاه خاموش شود.

برای اضافه کردن یک ماژول، یکی را از لیست ماژول ها به داخل درگاه خالی با ماوس کشیده و رها کنید. اگر ماژول با آن درگاه هم خوانی نداشته باشد به صورت خودکار به جای خود در لیست باز می گردد. برای حذف و جداسازی ماژول، ابتدا دستگاه را

خاموش کرده سپس آن را با ماوس از درگاه کشیده و به درون لیست برده و رها کنید.



شکل ۲-۲۶

قرار داد نام گذاری

هر روتر بیش از ۱۲ ماژول دارد اما رابط کاربری که ارائه می دهد توسط نام آن ها، شناخته می شود. بنابراین ما آن ها را برحسب شباهت های عملکردی‌اشان دسته بندی می کنیم:

- رابط کاربری کابل مسیEthernet LAN : یک رابط کاربری معمولی است که از یک سوکت RJ-٤٥ متصل به کابل مسی استفاده می کند. براساس سرعت آن ها نامگذاری های مختلفی دارند؛ Ethernet ١٠MB/s , Fast Ethernet ١٠٠MB/S ,

Gigabit Ethernet ۱۰۰۰MB/S . **ماژول هایی که رابط کاربری** Ethernet **دارند را می توان با یک عدد بهمراه پسوند** E , FE , CE , CFE , CGE **شناسایی کرد. ماژول هایی با پسوند** SW **وقتی روی روتر استفاده می شوند ، ویژگی های سوئیچینگ را ارائه می دهند.**

(HWIC-٤ESW) **دارای چهار پورت سوئیچینگ** Ethernet

(WIC-١ENET) **دارای یک پورت** Ethernet

(NM-١E) **دارای یک پورت** Ethernet

(NM-١FE-TX) **دارای یک پورت** Fast Ethernet

(NM-٤E) **دارای چهار پورت** Ethernet

(NM-ESW-١٦١) **دارای ۱۶ پورت سوئیچینگ** Ethernet

با قابلیت ویرایش) ماژول هایی-PT-ROUTER-NM-١CE, PT-ROUTER-NM-١CFE, PT-ROUTER-NM-١CGE

- **رابط کاربری رشته ای Fiber Ethernet : مشابه رابط کاربری قبلی است بجز آنکه از یک کابل رشته ای استفاده می کند و براساس پسوند** F **شناسایی می شوند.**
- (NM-1FE-FX) **یک رشـــته ی رســـانه ای**(Fiber Media) **با رابط** Fast Ethernet

(PT-ROUTER-NM-١FFE, PT-ROUTER-NM-١FGE) **ماژول های قابل ویرایش.**

- **رابط کاربری سریال : ماژول هایی دارای رابط کاربری سریال با حرف** T **یا رشته ی** A/S **نشان داده می شوند. تفاوت این دو در آنست که نوع** T **بصورت همگام سازی شده لند ولی** A/S **این‌طور نیست. این تفاوت در محیط واقعی موثر است و در یک نرم افزار شبیه سازی شبکه تفاوتی باهم ندارند.**

(WIC-١T , WIC-٢T) **یک یا دو پورت همگام سازی شده ی سریال دارد.**

(NM-٤A/S , NM-٨A/s چهار پورت یا هشت پورت همگام سازی شده یا نشده ی سریال دارد.

(PT-ROUTER-NM-١S, PT-ROUTER-NM-١SS) نوع قابل ویرایش

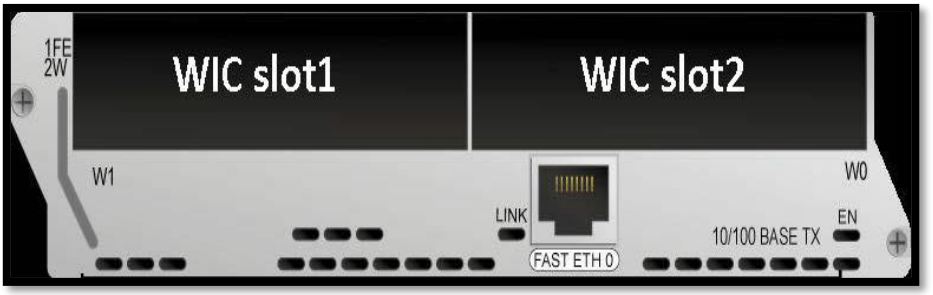
- **رابط کاربری مودم : شامل ماژول هایی دارای پورت RJ١١ برای کابل های آنالوگ تلفن است. آن ها با حرف AM که بعد از یک عدد میاید، شناسایی می شوند.**

(WIC-١AM) دو پورت RJ١١ برای مودم و تلفن دارد.

(WIC-٢AM , WIC-٨AM) دو یا هشت پورت RJ١١ دارد.

(PT-ROUTER-NM-١AM) نوع قابل ویرایش و شخصی سازی

- **ماژول WIC بهمراه NM : برخی ماژول های شبکه(NM) تمام فضای درگاه را اشغال نمی کنند، بنابراین درگاه های WIC همراه آن ها ارائه می شوند تا با کارت های کوچکتر وفق داده شود. این ماژول ها را می توان با حرف W در آخر نام آن ها شناسایی کرد.**



شکل ٢٧-٢

(NM-١E٢W, NM-١FE٢W) یک پورت Ethernet یا Fast Ethernet و دو درگاه WIC دارد.

(NM-٢E٢W, NM-٢FE٢W) دو پورت Ethernet یا Fast Ethernet و دو درگاه WIC دارد.

(NM-٢W) بدون رابط کاربری است و تنها دارای دو درگاه WIC است .

- **درپوش های درگاه: نرم افزار Packet Tracer برای درگاه های خالی، درپوش هایی فرآهم آورده است. اگرچه در شبیه سازی تفاوتی ایجاد نمی شود ولی یک دید شفاف و بهتر از لحاظ فیزیکی خواهد داشت.**

(NM-Cover) درپوش یک درگاه شبکه است.

(WIC-Cover) درپوش یک دستگاه WIC است.

- **HWIC-۸A : این ماژول در نرم افزار ٦ Packet Tracer یک ماژول جدید است. این ماژول هشت سوکت همگام سازی نشده EIA-۲۳۲ را برای پورت کنسول ارائه می دهد. اگر این ماژول نصب و فعال شود ، یک روتر می تواند بعنوان یک سرور دسترسی شبکه مورد استفاده قرار گیرد.**

ساخت یک دستگاه شخصی

اگر شما نیاز به یک روتر یا دسته ی مشخصی از ماژول ها دارید می توانید هربار آن را با کشیدن و رها کردن ماژول قبل از ایجاد یک توپولوژی انجام دهید. بنابراین نرم افزار Packet Tracer یک ویژگی برای ذخیره ی دستگاه شخصی سازی شده ی شما را ارائه می دهد. برای انجام چنین کاری کافیست گام های زیر را دنبال کنید:

۱) **یک دستگاه شبکه را با ماوس کشیده و در محیط کاری رها کنید. برای این مثال از سوئیچ عمومی PT-empty استفاده کنید.**

۲) **بر روی سوئیچ کلیک کنید تا کادر پیکربندی باز شود و دستگاه را خاموش کنید.**

۳) **ماژول های پرکاربرد خود را به سوئیچ اضافه کنید.**

۴) **با استفاده از کلید ترکیبی Ctrl+E یا به مسیر Tools→custom device dialog بروید.**

۵) بر روی دکمه ی Select کلیک کنید و سپس بر روی سوئیچی که بتازگی ویرایش شده کلیک کنید.

۶) یک نام و توضیح برای دستگاه درنظر بگیرید و بر روی Add و سپس Save کلیک کنید.

این دستگاه شخصی با پسوند Ptd. و در مسیر ٪USERPROFILE%\Cisco Packet Tracer \templates\ذخیره می شود. برای آنکه دستگاه ایجاد شده برای همه ی کاربران قابل دسترسی باشد آن را در مسیر /%PT٥HOME%/Templates% کپی کنید.

شبیه سازی WAN

برای هرچه واقعی تر کردن محیط، نرم افزار Packet Tracer دستگاه هایی دارد که یک شبکه ی WAN را شبیه سازی و تقلید می کنند. از کادر Device Type روی گزینه ی WAN Emulation کلیک کرده تا لیستی شامل موارد زیر را مشاهده کنید:

- **Cloud- PT** : این دستگاه شبیه یک گزینه در نوار ابزار است اما در زیر پنجره ی پیکربندی بیشتر شبیه یک روتر با چند درگاه است. ماژول های زیر برای دستگاه توده ای Cloud امکان پذیر است:

(NM-١AM) این ماژول یک سوکت RJ١١ برای اتصال مودم با استفاده از کابل تلفن است و حرف اختصاری این ماژول N است.

(NM-١CE, NM-١CFE, NM-١CGE): این سه ماژول بترتیب یک رابط کاربری Fast Ethernet , Gigabit Ethernet و Ethernet دارند و بوسیله ی مودم و کابل متصل شده به دستگاه قابل دسترسی اند. به جز تفاوت در سرعت، هر سه دارای کاربرد مشابهی هستند.

(NM-۱FE , NM-۱FGE) این دوماژول یک پورت Fast Ethernet یا Gigabit Ethernet برای انتقال به رشته ی رسانه ای (Media Fiber) دارند. آن ها همان کاربرد ماژول قبل را دارند.

(NM-۱CX) دارای یک سوکت هم محور برای اتصال به کابل مودم است.

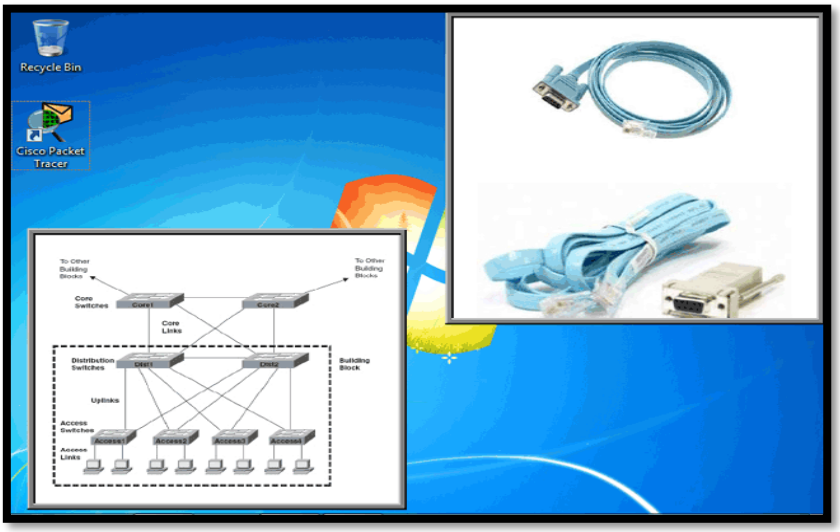
(NM-۱S) یک پورت سریال دارد که برای پیکربندی چارچوب تقویتی دستگاه(Frame Relay Mapping) است. تب Config برای این رابط کاربری گزینه هایی را برای ایجاد یک چارچوب تقویتی ارائه می دهد.

- **DSL-Modem-PT** : یک مودم با رابط کاربری Ethernet و RJ۱۱ است. رابط کاربری Ethernet می تواند از بین سه مدل Ethernet , Fast Ethernet , Gigabit Ethernet انتخاب شود . این دستگاه هیچگونه گزینه ی پیکربندی ندارد.
- **Cable-Modem-PT** : این مودم شبیه حالت قبلی است با این تفاوت که از پورت هم محور پشتیبانی می کند.

آشنایی با IOS

IOSیا Internet work Operating System سیستم عامل سیسکو است که روی انواع مختلف روتر پیاده و اجرا می‌شود. مثل هر سیستم عامل دیگری رابط ماشین با انسان و تنظیمات صورت گرفته است. بدین ترتیب اگر زبان IOS را بدانیم تنظیم انواع مختلف روتر حتی سوئیچ و محصولات بیسیم سیسکو به سادگی امکان‌پذیر است. روتر با هر بار بوت شدن IOS را از فلش خوانده و داخل RAMآن را باز و Decompress می‌کند. همانند یک PC می‌توان چندین سیستم‌عامل را روی یک روتر نگه داشت اما سیستم در آن واحد با یکی از آن ها بالا می‌آید. این IOS را می‌توانیم داخل فایل تنظیمات برای روتر مشخص کنیم در غیر این صورت روتر خود یکی را به ترتیب انتخاب کرده و بوت

می‌شود.ساده‌ترین راه دسترسی به کنسول استفاده از درگاه Console است. برای اتصال به کنسول به یک پورت سریال روی PC و یک کابل سریال نیاز داریم. در شکل
زیر دو نوع کابل Console را مشاهده می‌کنید.



شکل ۲-۲۸

- کابل کنسول یک کابل Roll-Over است. یعنی پین اول در یک سمت به پین هشتم متصل شده و پین دو به پین هفتم و به همین ترتیب به صورت معکوس پین‌های RJ٤٥ به یکدیگر وصل شده‌اند. این کابل را می‌توان به راحتی ساخت.
راه دیگر اتصال به روتر SNMP, Telnet, AUX و HTTP است. روش‌های اتصال و مدیریت روتر بوسیله Console و AUX را In-Bound Managementمی‌گوییم که در همه زمان دسترسی به آن محیا است .

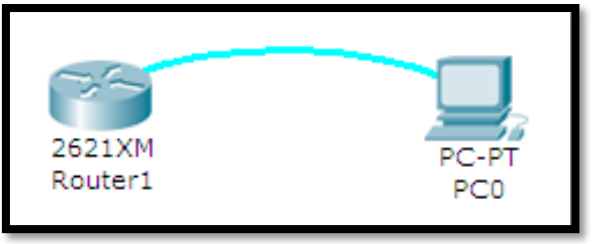
پورت کنسول [۶۵]

تفاوتی در آنچه مشاهده و کنترل می شود در این روش با روش قبل وجود ندارد، اما پورت کنسول می تواند برای ساخت و پیرایش یک توپولوژی مشابه با دنیای واقعی مورد استفاده قرار بگیرد. گام های زیر را برای پیکربندی آن دنبال کنید:

۱) یک محیط کاری کامپیوتر یا لپ تاب را اضافه کنید.

۲) اتصالات را انتخاب کرده سپس روی کابل کنسول کلیک کنید.

۳) کابل کنسول دستگاه شبکه را به پورت RS-۲۳۲ لپ تاب یا کامپیوتر وصل کنید.



شکل ۲۹-۲

۴) کامپیوتر یا لپ تاب را باز کرده و به تب Desktop رفته و تب Terminal را باز کنید. شپس با همان تنظیمات پیش فرض OK را بزنید تا کنسول را مشاهده نمایید. تصویر زیر یک نما از کنسول روتر در ترمینال مربوط به آن را نشان می دهد.

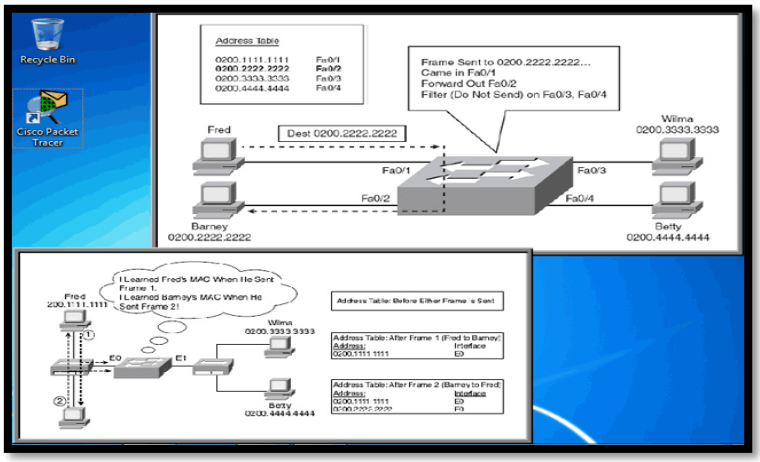
نکته: مهم‌ترین کار سوئیچ دریافت فریم Ethernet است و تصمیم گیری در مورد Forward کردن آن فریم از سایر پورت‌ها یا Ignore کردن آن می‌باشد. این کارها در سه مرحله توسط سوئیچ انجام می‌شود:

[۶۵] Console

۱.تصمیم‌گیری در مورد Forward کردن یا Filter کردن فریم براساس Mac Address مقصد.

۲. Learnکردن (یاد گیریMac Address های مبداء با بررسی هر فریم ورودی).

۳. ایجاد محیط بدون Loop لایه ۲ با سایر سوئیچ‌ها به وسیله پروتکل Spanning Tree.در شکل زیر مراحل یادگیری Mac Address به وسیله سوئیچ را مشاهده می‌کنید.



شکل ۳۰-۲

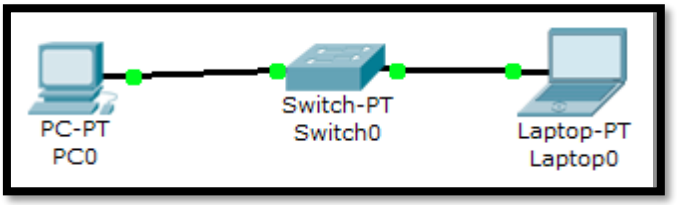
پیکر بندی سوئیچ

با افزودن یک سوئیچ Ethernet و بادرنظر گرفتن گام های زیر می توان ۲ دستگاه را بهم متصل نمود :

۱) از کادر Device Type Selection بر روی Switch کلیک کنید و تمام سوئیچ ها (بغیر از PT-empty) را به فضای کاری وارد کنید.

۲) از نوار ابزار معمولی و با ابزار Delete اتصال بین کامپیوتر و لپ تاب را قطع کنید.

۳) یک کابل Copper Straight-Through را انتخاب کرده و با استفاده از سوئیچ، کامپیوتر و لپ تاب را به همدیگر وصل کنید،دراین لحظه نشانگر LED سوئیچ به رنگ نارنجی است زیرا پورت سوئیچ در وضعیت دریافت و پردازش اطلاعات از طریق پروتکل فراگیر درختی STP است.



شکل ۳۱-۲

۴) وقتی یکبار نشانگر به رنگ سبز درآمد (مثل شکل فوق) دوباره برای اطمینان از اتصال از Ping استفاده کنید. برای ذخیره ی این توپولوژی از منوی File گزینه ی Save as را کلیک کرده و محل مورد نظر برای ذخیره را انتخاب کنید. پسوند فایل توپولوژی ذخیره شده Pkt. است. سپس مراحل زیر را به ترتیب انجام می دهیم:

۱. ساخت username و password و ایجاد سطح دسترسی برای سوئیچ

switch>enable (privilage ورود به محیط)

switch#conf t (وارد شدن به محیط کانفیگ)

switch(config)#username **sahel** password • **cisco**

switch(config)#enable secret **sahel**

۲ . اختصاص دادن یک IP **و** default gateway **به سوئیچ برای دسترسی**

switch(config)#int vlan **۱** (**۱**[۶۶] **کانفیگ وی لن**)

switch(config-if)#ip add **۱۹۲,۱۶۸,۱,۱ ۲۵۵,۲۵۵,۲۵۵,۰** (**اختصاص آدرس**)

switch(config-if)#no sh
switch(config-if)#exit
switch#vlan database
switch(vlan)#vlan **۱** name shabake (**۱ ساخت وی لن**)

switch(vlan)#exit
switch#conf t
switch(config)#ip default-gateway **۱۹۲,۱۶۸,۱,۲** (**آدرس روتر**)

با این روش که ملاحظه کردید به راحتی میتوانید یک vlan **بسازید و به آن** IP **اختصاص دهید ، توجه کنید که** vlan۱ **به شکل پیشفرض ساخته شده و تمامی پورت ها عضو** vlan ۱ **هستند.**

۳. اختصاص هر پورت به vlan **خاص:**

براس مثال میخواهید چند پورت عضو Vlan **خاصی باشند ، ابتدا با روش بالا** vlan **ها را بسازید (، نیازی هم به اختصاص** IP **به هر** vlan **نیست)، سپس ، با روش زیر هر پورت را عضو** vlan **مورد نظر کنید:**

switch(config)#int fas **۱/۰**
switch(config-if)#description “connected to cisco router”
switch(config-if)#switchport access vlan **۱۰**
switch(config-if)#exit

[۶۶] VLAN

switch(config)#int fas ۲/۰

switch(config-if)#description “web Server”

switch(config-if)#switchport access vlan ۲۰

switch(config-if)#exit

توجه داشته باشید در هر لحظه می توانید با دستور زیر تغییرات را ذخیره کنید ، در غیر این صورت بعد از خاموش روشن کردن سوئیچ ، کانفیگی وجود نخواهد داشت.

switch#write mem

Vlan[۶۷]چیست؟ یک LAN شامل تمام دستگاه‌هایی است که در یک Broadcast Domain باشند. Broadcast Domain (پیامهای فراگیر) است. به Domain هایی که این پیام‌ها تا آنجا می‌توانند ارسال شوند و پیش بروند Broadcast Domain (دامنه Broadcast) گفته می شود. به عنوان یک تعریف دیگر تمام ایستگاه‌ها و وسایلی که به‌LAN متصل‌اند عضو یک Broadcast Domain اند و در این صورت اگر یکی از ایستگاه‌ها پیامی را به صورت Broadcast ارسال کند،تمام ایستگاههای عضو آن Domain Broadcast یک کپی از آن پیام را دریافت می‌کنند. حالتی را در نظر بگیرید که VLAN نداریم؛ در حالت معمول در یک LAN تمام پورت‌های یک سوییچ عضو Broadcast Domain مشابه‌اند. به این ترتیب اگر یک ایستگاه پیامی را به صورت Broadcast ارسال کند، تمام دستگاه‌هایی که در آن Broadcast Domain هستند. مثلا در شکل زیر کامپیوترشماره ۱ پیامی را به صورت Broadcast ارسال می‌کند و همان طور که در شکل مشخص است این پیام به تمام هاست‌هایی که در آن Broadcast Domain هستند می‌رسد.

[۶۷] Virtual Local Area Network

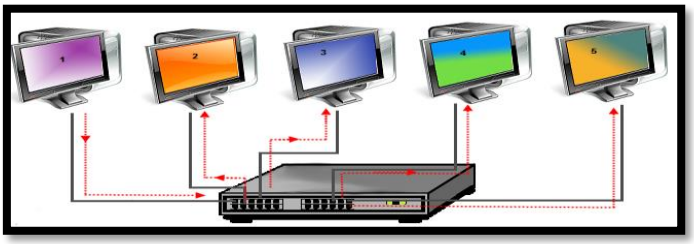
انواع پورت در سوئیچ

Access port: متصل به کاربر

Trunk port:اتصال دوسوئیچ به یکدیگر و اتصال یک سویچ به روتر یا ارتباط سوئیچ با یک کارت شبکه سازگار با trunk

VLAN trunks

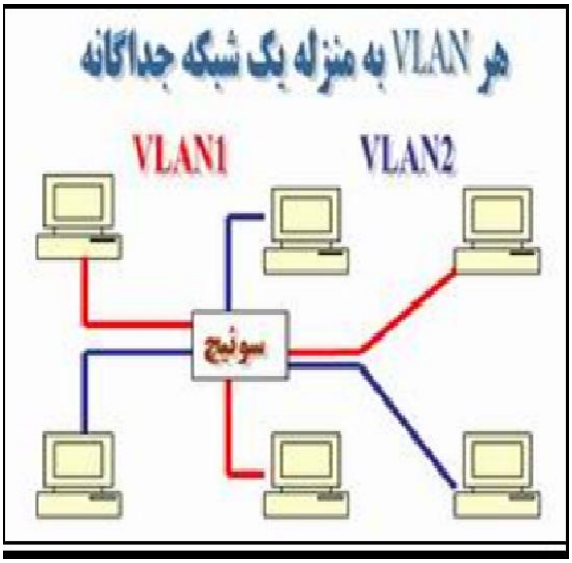
مسیری برای فرستادن ترافیک بیشتر از یک vlan از میان یک لینک را VLAN trunks گویند. ه عبارت ساده تر وقتی روی سوئیچ-ها VLAN تعریف می کنیم، سوئیچ-ها را از طریق ترانک به هم وصل می کنیم. بنابراین در مورد مثال دانشکده IT و فیزیک نیز بایستی که بین سوئیچ ها از VLAN Trunking استفاده کنیم. تا سوئیچ دانشکده فیزیک بتواند با VLAN خود در سوئیچ دانشکده IT در ارتباط باشد.



شکل ۳۲-۲

در حالت کلی خوب نیست! زیرا ممکن است که کامپیوتر ۱ بخواهد که این پیام را تنها به کامپیوتر ۲ برساند، اما از این طریق سایر کامپیوترها نیز این پیام را دریافت می کنند، شاید به نظرتان برسد ، که برای این کار به جای ارسال Broadcast می‌تواند از

ارسال مستقیم به کامپیوتر۲ استفاده کند؛ این فکر درست است ، اما اگر فرض کنید که هر کدام از این کامپیوترها نماد ۱۰۰۰ کامپیوتر هستند، دیگر ارسال Broadcast **کاملاً مفید به نظر نمی رسد. اما همان طور که گفتیم هنوز این مشکل وجود دارد، که علاوه بر کامپیوتر ۱(یا کامپیوترهای ۱) سایر کامپیوترها هم این پیام را دریافت می کنندو این کار پهنای باند زیادی را به هدر می‌دهد. علاوه بربحث پهنای باند ، از نظر امنیتی به مشکل برمی‌خوریم. برای رفع این مشکل، می‌توان کامپیوترهای ۱ و ۲ را عضو یک** LAN **قرار داد و سایر کامپیوترها را را عضو یک** LAN **دیگر، طوری که هر کدام از این** LAN **ها** Broadcast Domain **خودرا داشته باشند . اما برای این راه حل نیازاست، که یک سوییچ دیگر بخریم و این یعنی هزینه زیادی ! اما اگر از** VLAN **استفاده کنیم می توانیم همین دو شبکه مجزا را روی یک سوییچ پیاده سازی کنیم و دو** VLAN **مجزا داشته باشیم. به این ترتیب که برخی از پورت‌های سوییچ را مثلا به** VLAN **شماره ۲ و برخی دیگر را به** VLAN **شماره ۳ نسبت می‌دهیم و هر کدام از** VLAN**ها** Broadcast Domain **خاص خود را خواهند داشت که از دسترس سایر ایستگاه‌های** VLAN**دیگر دور خواهد ماند.**



شکل ۳۳-۲

در شکل فوق، با استفاده از پتانسیل VLANسوئیچ ، دو VLAN ایجاد شده است که به هر یک سه ایستگاه متصل شده است (VLAN۱) و (VLAN۲). زمانی که ایستگاه شماره یک متعلق به VLAN۱، یک پیام Braodcast را ارسال می نماید (نظیر FF:FF:FF:FF:FF:FF :)، سوئیچ موجود، آن را صرفا" برای ایستگاه‌های شماره دو وسه Forward می نماید . در چنین مواردی سایر ایستگاههای متعلق به VLAN۲، آگاهی لازم در خصوص پیام های broadcastارسالی بر روی VLAN۱ را پیدا نکرده و درگیر این موضوع نخواهند شد.

۴. کانفیگ پورت سوئیچ سیسکو برای مود ترانک:[۶۸]

ترانک نوعی ارتباط است که حامل vlan هاست ! این ساده ترین نوع توضیح است ! برای مثال شما ۲ سوئیچ سیسکو دارید و روی هر سوئیچ ۳ عدد vlan به شماره های

[۶۸] TRUNK

۱۰،۲۰،۳۰ ، حال می‌خواهید nod هایی از هر سوئیچ امکان دسترسی به nod های سوئیچ دیگر که در همان vlan هستند داشته باشند.

```
switch-a(config)#int gi ۱/۰
switch-a(config-if)#description “Trunk to switch B”
switch-a(config-if)#switchport mode trunk
```

مشابه همین تنظیمات را در سمت دیگر نیز انجام داده و سوئیچ ها را توسط این پورت به هم متصل کنید.

نکته: کار VTP انتقال جدول VLAN ها به سوئیچ های سیسکو همجوار که در یک VTP Domainقرار دارند میباشد VTP. بر روی لایه ۲ توسط ارتباطات ترانک ، اسم و شماره و MTU تمامی VLAN های تعریف شده در سوئیچی که نقش VTP سرور را دارد ، ارسال می‌نماید.

۵ . استفاده از امکان POE : یکی از قابلیت های سوئیچ های سیسکو ، امکان پشتیبانی از POE یا همان استاندارد ۸۰۲,۳ که برق را با ولتاژ ۴۸ولت، به نود ارسال کرده و امکان روشن کردن دیوایس هایی که از POE پشتیبانی میکنند مثل – IP Phone IP Cam – Wireless radioو … را دارد.

```
switch(config)#int fas ۱/۰
switch(config-if)#power inline auto
```

دستور فوق باعث می‌شود ، در صورتی که دیوایس متصل شده به سوئیچ سیسکو قابلیت POE را دارا بود ، ولتاژ به آن ارسال شود.

اتصال کامپیوتر به سوئیچ

سوئیچ مورد استفاده در packet tracer **در این جا، سوئیچ ۲۹۶۰ می باشد. از لیست سوئیچ ها آن را انتخاب کنید.**

شکل ۲-۳۴

از لیست End Devices **هم می توانید یک کلاینت انتخاب کنید.**

شکل ۲-۳۵

یک کامپیوتر و سوییچ ۲۹۶۰ انتخاب می کنید.

شکل ۲-۳۶

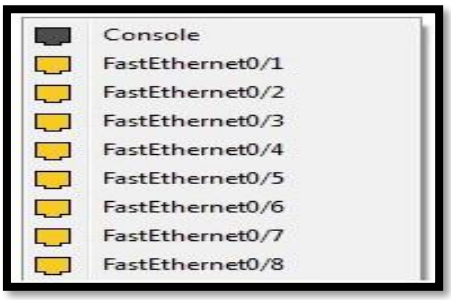
کابل کنسول را انتخاب کنید.

شکل ۲-۳۷

روی کامپیوتر کلیک کنید. گزینه RS۲۳۲ را انتخاب کنید.

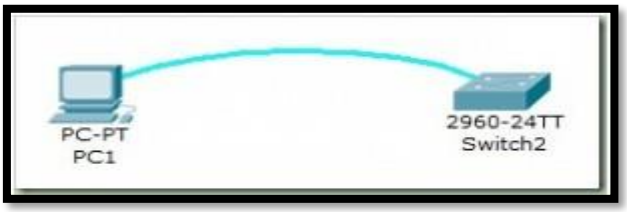
شکل ۲-۳۸

سوئیچ ۲۹۶۰ کلیک کنید. گزینه Console را انتخاب کنید.



شکل ۲-۳۹

شکلی شبیه به شکل زیر ایجاد می شود. در اینجا کامپیوتر با کابل کنسول به سوییچ متصل است.



شکل ۲-۴۰

برای رفتن به CLI یا Command Line Interface یعنی محیط Command در سوئیچ دو راه وجود دارد.

از طریق PC و برنامه Hyper Terminal مجازی آن

از طریق خود سوئیچ

- **از طریق PC و برنامه Hyper Terminal مجازی آن‌روی کامپیوتر کلیک کنید. دنبال Terminal بگردید. کلیک کنید.**

شکل ۴۱-۲

- **از طریق سوئیچ**

روی سوئیچ کلیک کنید. CLI را پیدا کنید.

شکل ۴۲-۲

در هر دو حالت می توانید وارد محیط Command شوید یا به خط فرمان CLI دسترسی پیدا کنید.

پیکربندی روتر

وقتی به روتر متصل می‌شویم بر روی آن کلیک کرده و در محیطCLI اولین خط برای وارد کردن Command به صورت زیر است:

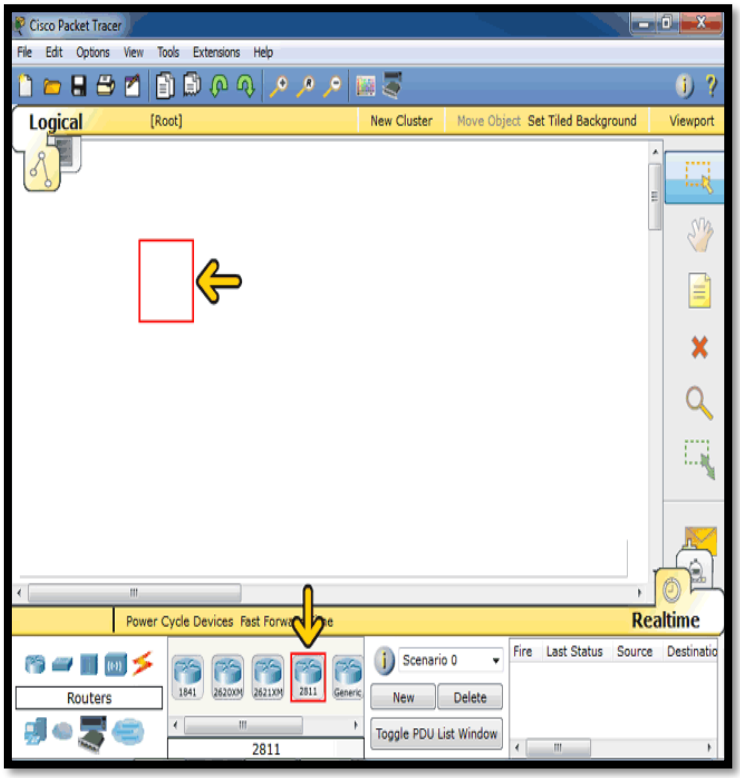
```
Router >
```

برای اینکه به دسترسی بالاتر برسیم باید به Privileged-mode برویم، این کار توسط دستور Enable بصورت زیر انجام می‌شود:

```
Router>
Router>enable
Router#
```

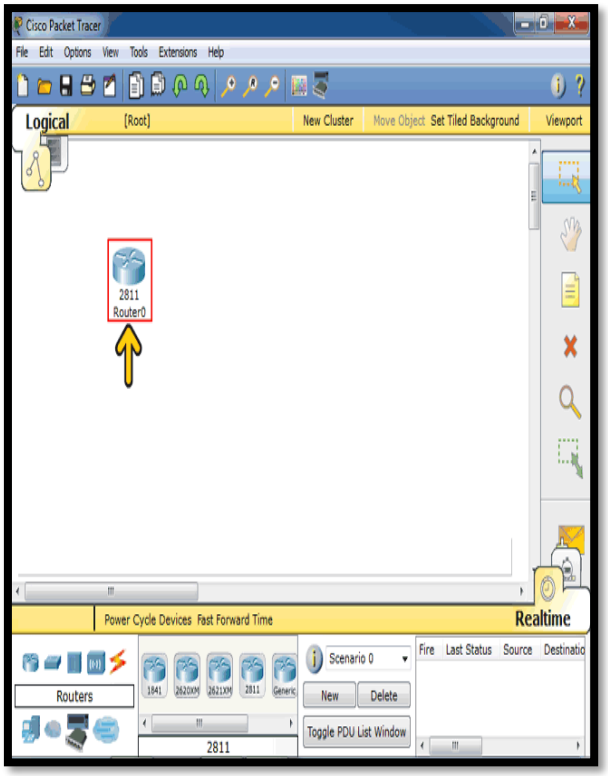
تخصیص رمز عبور به یک روتر را بررسی می‌کنیم.

روی روتر ۲۸۱۱ که با فلش مشخص شده است کلیک کنید .در محل مشخص شده با کادر قرمز کلیک کنید تا روتر در این قسمت قرار بگیرد.



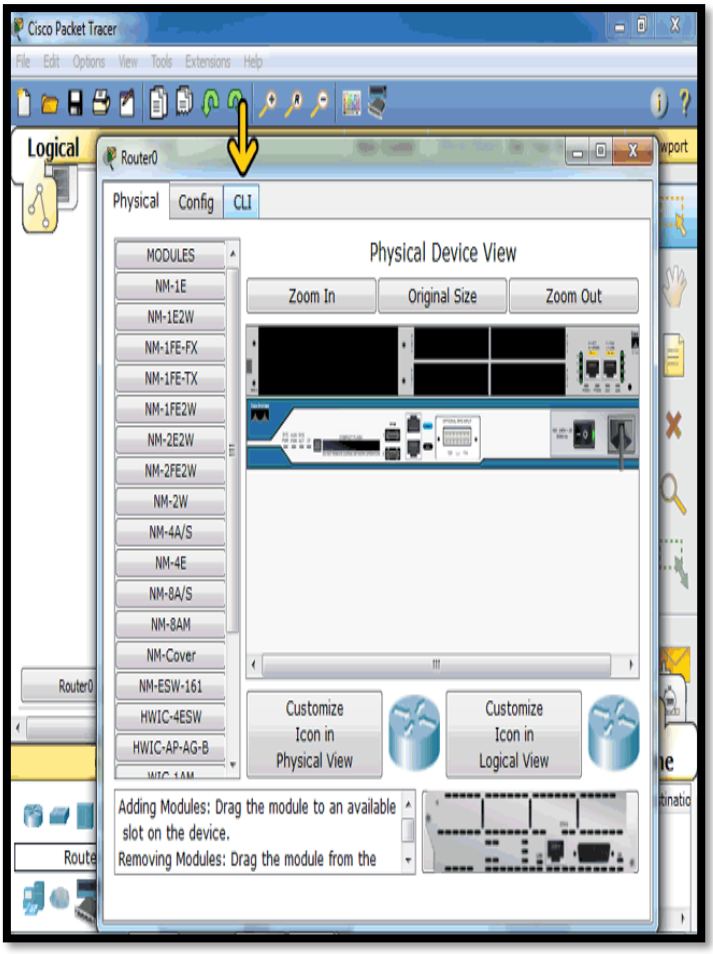
شکل ۲-۴۳

روی روتر ۲۸۱۱ که در صفحه قرار دادیم، کلیک کنید تا انتخاب شود.



شکل ۴۴-۲

انجامConfig ها و کنترل IOS سوئیچ و روتر در CLI انجام می‌شود. روی سربرگ CLI کلیک کنید.



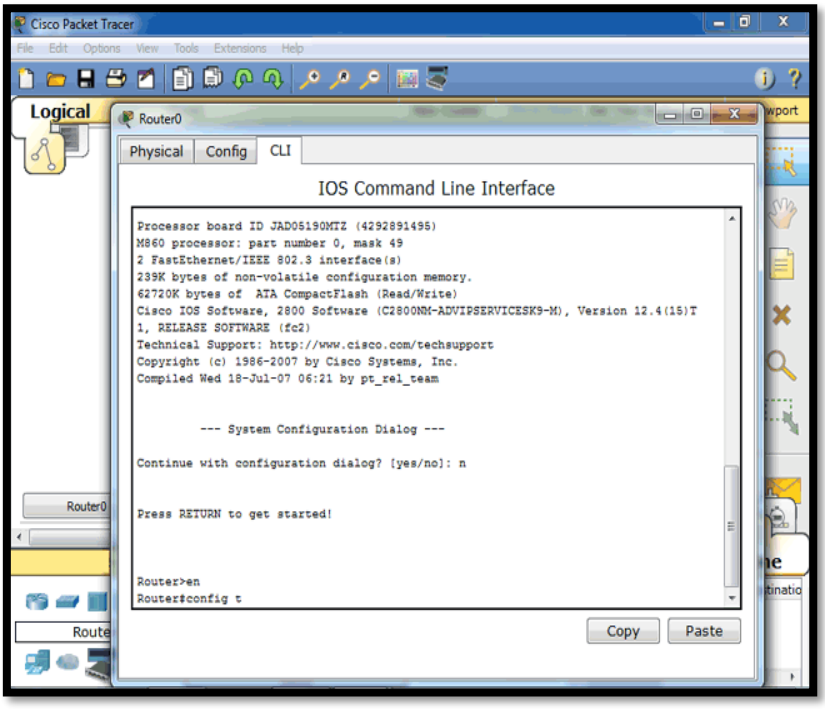
شکل ۴۵-۲

اگر روتر تاکنون تنظیم نشده باشد و روتر فایل تنظیمات را درون NVRAM **پیدا نکند، برنامه** Setup **اجرا می‌شود که با پرسیدن سوال‌های ساده بصورت اتوماتیک روتر را تنظیم می‌کند. با تایپ حرف** N **و فشردن کلید** Enter **تنظیمات** Setup **کنار گذاشته می‌شود. دکمه** N **صفحه کلید را فشار دهید .**

برای اجرای هر command **یا دستور باید بعد از تایپ آن دکمه** Enter **را فشار**

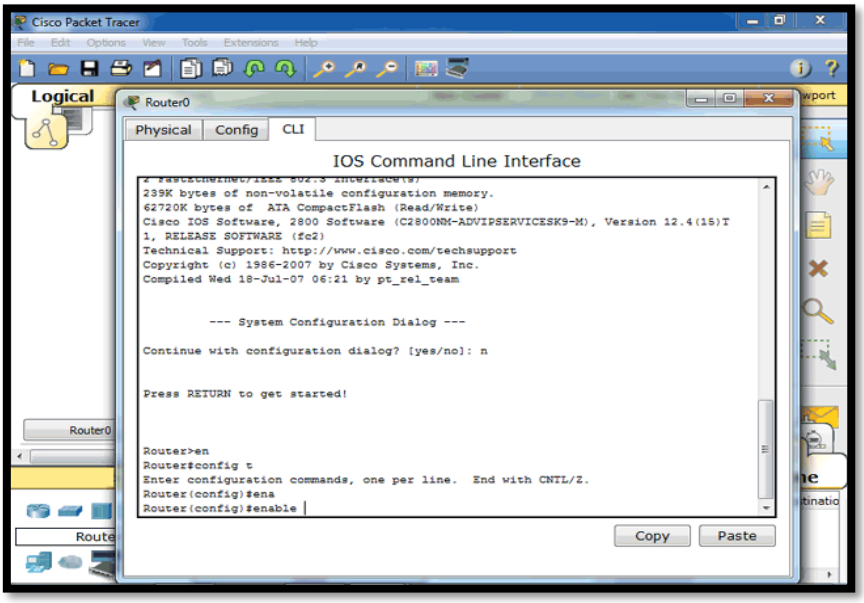
دهید تا command بر روی روتر اعمال شود. دکمه Enter صفحه کلید را فشار دهید .

دوباره دکمه Enter صفحه کلید را فشار دهید. تا عبارت Router> ظاهر شود. همانطور که دیدید، با فشار دادن دکمه Enter به محیط Privileged که قبلاً شرح داده شد رسیدیم. عبارت en که مخفف دستور enable است را تایپ کنید . دکمه Enter صفحه کلید را فشار دهید .برای انجام تنظیمات باید در محیط Configuration Modeقرار داشته باشیم. بدین منظور باید دستور Config T یا Configuration Terminalرا وارد کنیم. در ادامه دستور config t را خودمان وارد می‌کنیم .



شکل ۴۶-۲

دکمه Enter صفحه کلید را فشار دهید.در ادامه به Set کردن یا تنظیم کردن رمز عبور می‌پردازیم. برای این کار دو دستور وجود دارد، یکی enable password که به صورت Clear Text می‌باشد و دیگری enable secret که در آن رمزعبور به صورت Hash نمایش داده می‌شود، که امن‌تر است. در اینجا ما از enable secret استفاده می‌کنیم. یکی از نکات مثبت استفاده از CLI این است که بعد از تایپ کردن قسمتی از کلمه با فشردن دکمه TAB درصورت منحصر بفرد بودن command بقیه کلمه حدس زده می‌شود. مثلاً در این مورد با تایپ سه حرف ena و فشردن کلید TAB عبارت enable ظاهر می‌شود. سه حرف ena را وارد کنید.دکمه TAB صفحه کلید را فشار دهید.همانطور که مشاهده می‌کنید دستور enable وارد شده است. در ادامه عبارت se را وارد می‌کنیم.



شکل ۲-۴۷

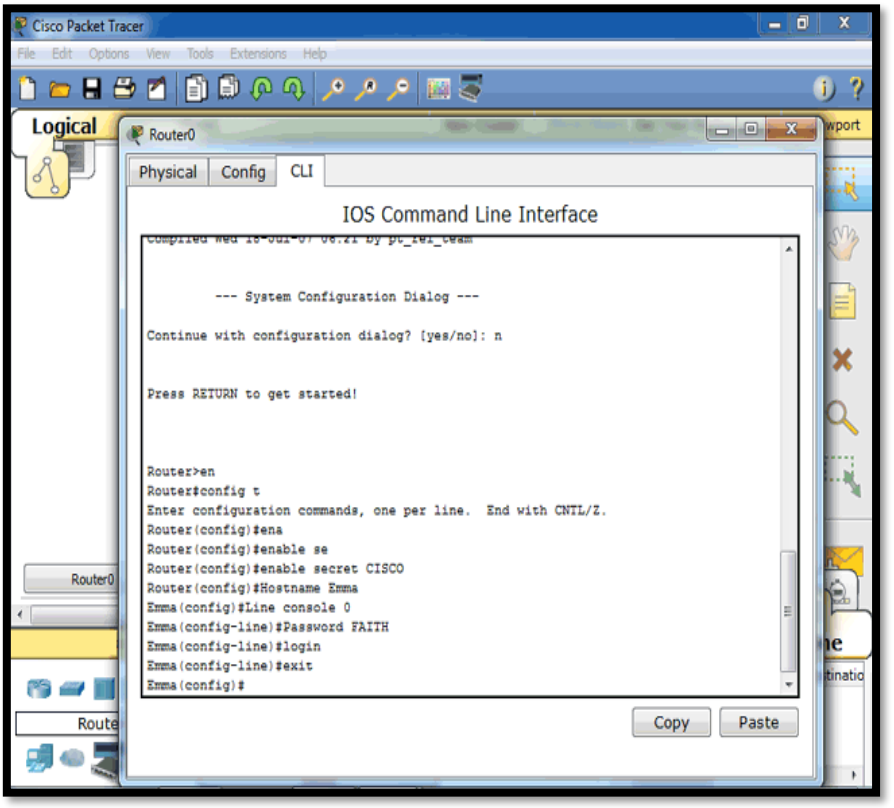
دکمه TAB صفحه کلید را فشار دهید.همانطور که مشاهده می‌کنید دستور secretوارد شده است .در ادامه عبارت CISCO را به عنوان رمز عبور وارد می‌کنیم .

دکمه Enter صفحه کلید را فشار دهید .حال قصد تغییر Hostname را داریم. برای این کار در ادامه دستور Hostname را وارد می‌کنیم و کلید Spaceرا فشار می‌دهیم .در ادامه عبارت Emma را به عنوان نام جدید روتر وارد می‌کنیم. دکمه Enter صفحه کلید را فشار دهید. می‌خواهیم دسترسی به کنسول را مشروط به وارد کردن رمزعبور نماییم. برای این کار ابتدا باید وارد محیط Line console شویم. در ادامه برای وارد شدن به این محیط دستور ۰ Line console را وارد می‌کنیم. ۰ در این دستور به صورت Default است .دکمه Enter صفحه کلید را فشار دهید .همانطور که می‌بینید وارد محیط کنسول شدیم. اینک باید رمزعبور را تعیین کنیم. در ادامه برای این کار دستور Password به همراه رمز عبورFAITH را وارد می‌کنیم .

دکمه Enter صفحه کلید را فشار دهید.در ادامه عبارت login را تایپ می‌کنیم. این دستور به منظور تخصیص دادن Password CISCO به کنسول است.دکمه Enter صفحه کلید را فشار دهید.برای خروج از این حالت و بازگشت به حالت قبل از دستور exit استفاده می‌کنیم. عبارت exit را تایپ کنید.دکمه Enter صفحه کلید را فشار دهید.در حالتDefault ، سوئیچ و روتر Cisco این اجازه را به کاربر می‌دهند که بدون آنکه نیاز به وارد کردن Password داشته باشد به حالت User Modeدسترسی پیدا کند. اما به کاربران Telnet و SSH این اجازه داده نخواهد شد. با Set کردن رمز عبور برای vty کاربر با وارد کردن رمزعبور می‌تواند به

Telnetدسترسی داشته باشد، این command به Device می‌گوید که تمام commandهایی را که در ادامه آن ذکر خواهد شد به صورت هم‌زمان روی هر ۱۶ ترمینال مجازی اعمال کند. که در ادامه برای اجرای آن دستور را وارد می‌کنیم .

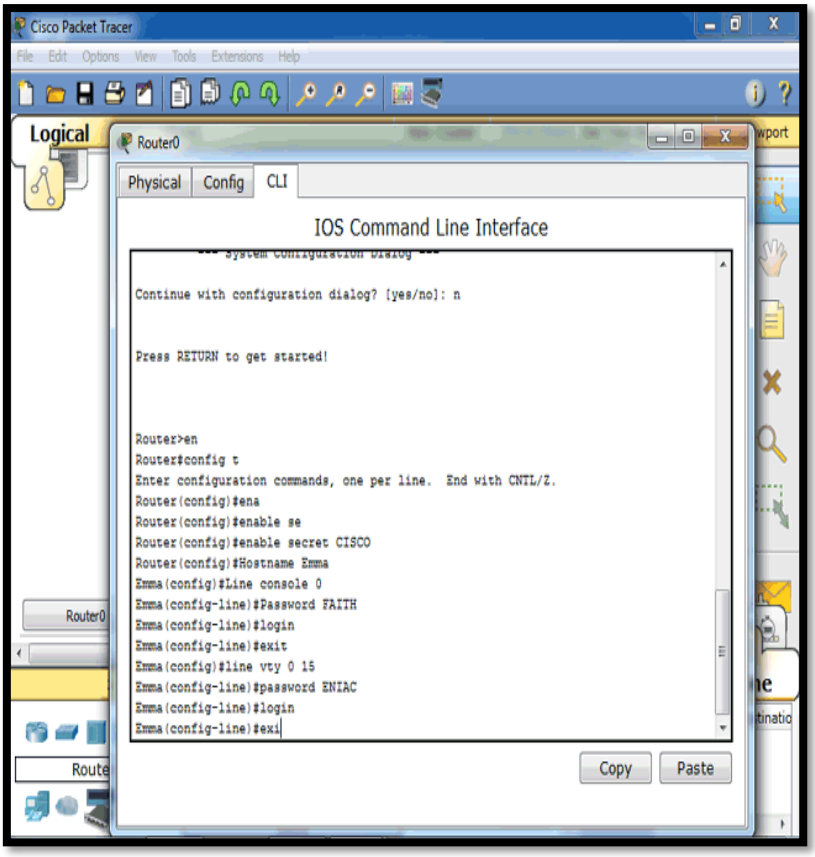
line vty ۰ ۱۵



شکل ۴۸-۲

دکمه Enter صفحه کلید را فشار دهید.اینک نوبت Set کردن رمز عبور است. برای این کار دستور password را تایپ می‌کنیم و کلمه ENIAC را به عنوان رمزعبور قرار می‌دهیم.دکمه Enter صفحه کلید را فشار دهید.برای آنکه از کاربر فقط

رمزعبور خواسته شود از عبارت Login استفاده می‌کنیم. کلمه login را تایپ کنید.دکمه Enter صفحه کلید را فشار دهید.برای خروج عبارت exi را تایپ کنید.

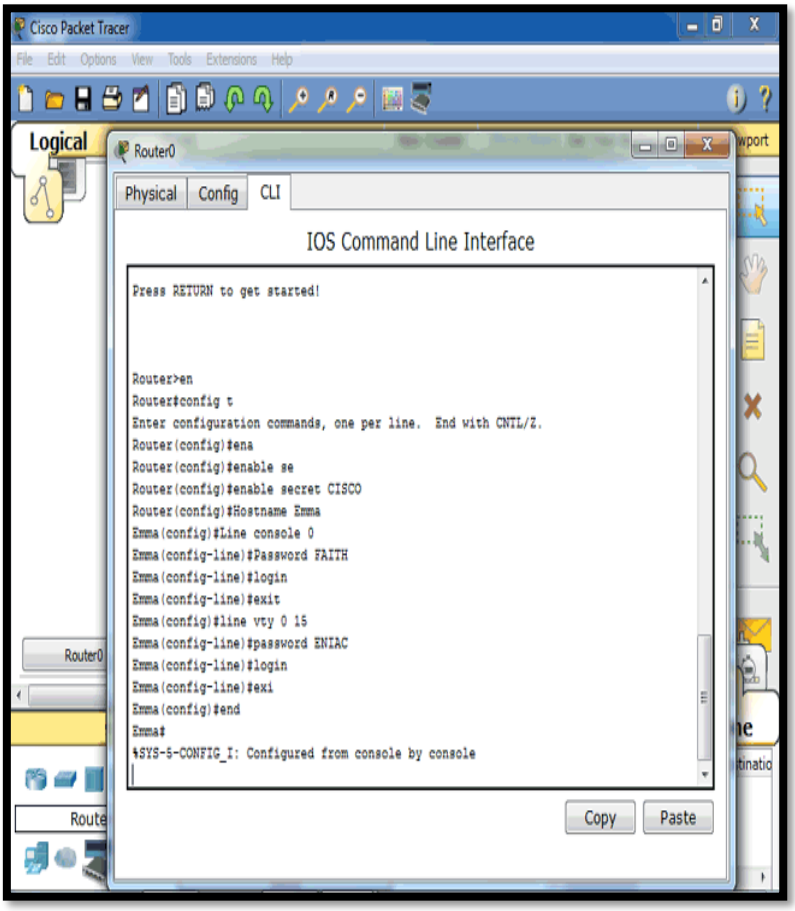


شکل ۲-۴۹

دکمه Enter صفحه کلید را فشار دهید. با تایپ End به محیط اولیه Privileged می‌رویم. کلمه end را تایپ کنید.دکمه Enter صفحه کلید را فشار دهید.

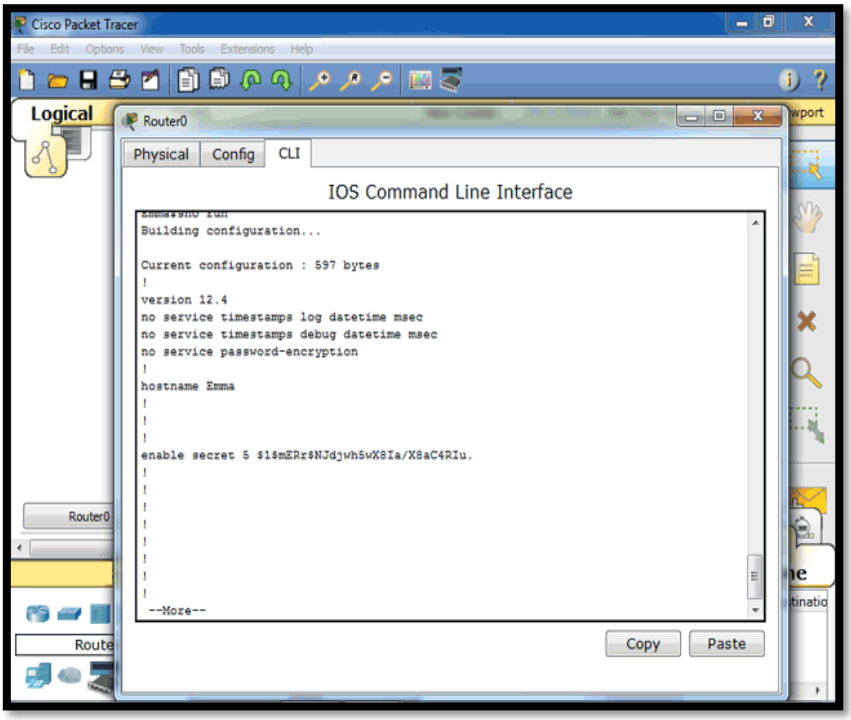
برای مشاهدهcommand هایی که در هر قسمت وارد کرده‌اید از دستور show

running- config می‌توان استفاده کرد. این دستور کلیه تنظیماتی که در روتر وجود دارد را نمایش خواهد داد. Show گرفتن در مراحل بالاتر یکی از کارهایی است که جهت Trouble Shooting باید انجام داد. دستور sho run را وارد می‌کنیم. توجه کنید که ما در نوشتن command از مخفف‌ها استفاده کرده‌ایم .



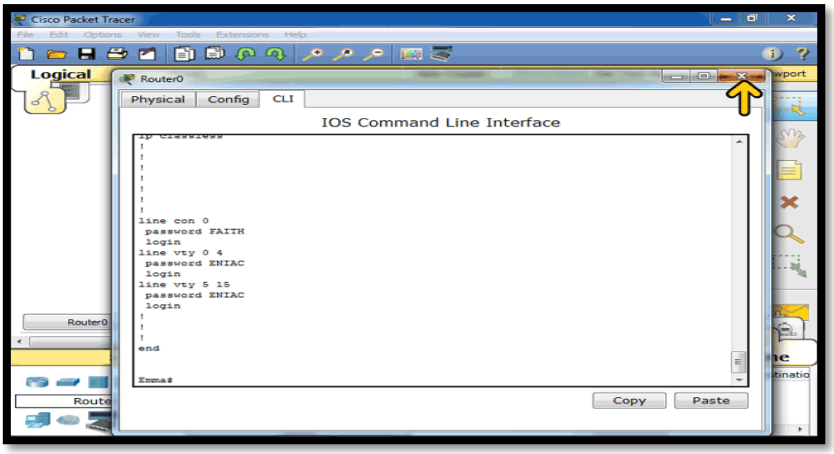
شکل ۵۰-۲

اکنون شماConfig های Default را مشاهده می‌کنید. برای دیدنConfig هایی که انجام دادیم لازم است به قسمت ۰ line console برسیم، برای این کار دکمه Enterصفحه کلید را فشار دهید.



شکل ۵۱-۲

برای رد کردن صفحه به صفحه سه بار دکمه Space صفحه کلید را فشار دهید.با اینکارConfig های صورت گرفته را مشاهده کردید. می‌توان در مورد درستی commandهای وارد شده اطمینان حاصل نمود. برای بستن پنجره مربوط به روتر Emmaروی دکمه Close کلیلک کنید .



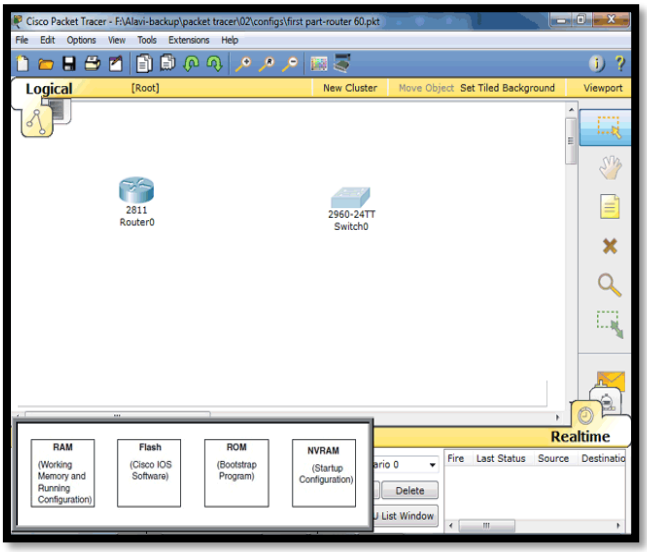
شکل ۵۲-۲

ROM

Read-Only Memory برنامه‌های Bootstrap یا Boot helper را در خود ذخیره می‌کند و هنگامی که سوئیچ برای اولین بار بالا می‌آید Load می‌شوند. سیستم عامل های سیسکو، عکس یا Image را به صورت کامل می‌یابد و روند Load شدن آن را در RAM مدیریت می‌کند. Flash Memory چه به صورت Chip در داخل دستگاه باشد و چه به صورتRemovable Memory Card ، وظیفه ذخیره‌سازی IOS Imageرا دارد علاوه بر آن قابلیت ذخیره فایل‌های دیگر از جمله کپی Backup‌از فایل‌های Configuration را دارد .

Nonvolatile RAM (NVRAM)

Configهای ابتدایی یا Start Up Configuration را در خود نگه‌داری می‌کند. که هنگام Reload شدن یا اولین بار بالا آمد، سوئیچ استفاده می‌شود.

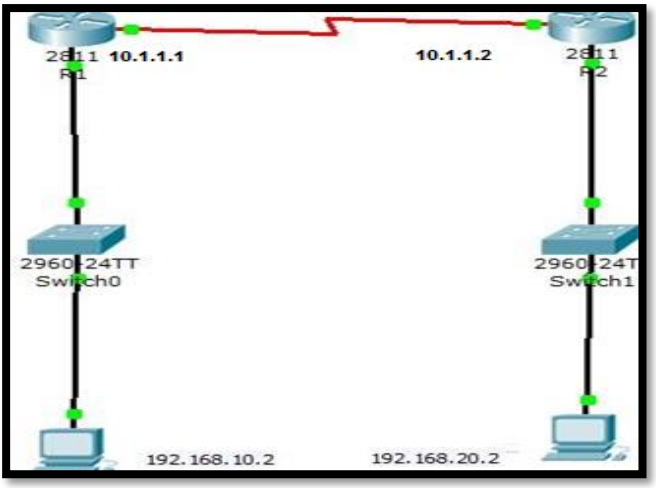

Cisco Packet Tracer - F:\Alavi-backup\packet tracer\02\configs\first part-router 60.pkt
File Edit Options View Tools Extensions Help
Logical
[Root]
New Cluster
Move Object
Set Tiled Background
Viewport
2811
Router0
2960-24TT
Switch0
RAM
(Working Memory and Running Configuration)
Flash
(Cisco IOS Software)
ROM
(Bootstrap Program)
NVRAM
(Startup Configuration)
Realtime
Fire
Last Status
Source
Destinatio
Delete
List Window

شکل ۵۳-۲

فصل سوم

سناریوهای مهم Packet Tracer

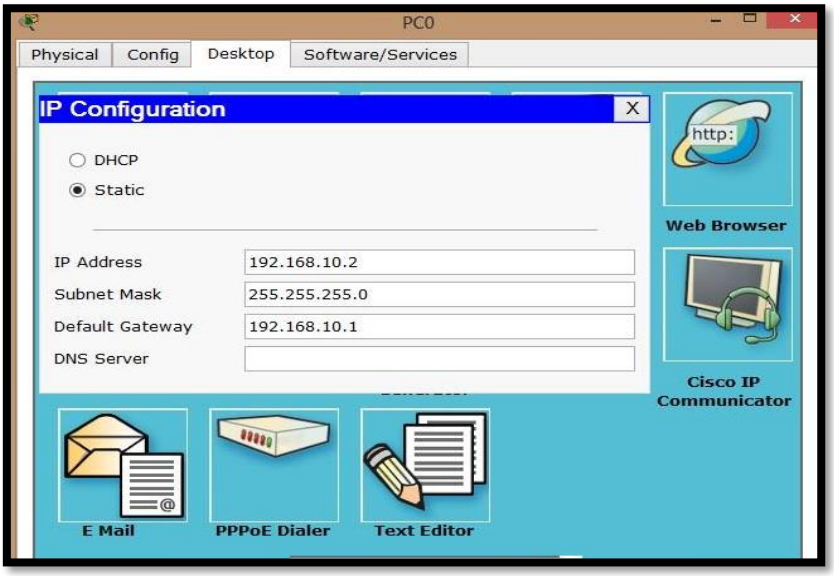
سناریویStatic routing یا مسیریابی دستی



شکل ۱-۳

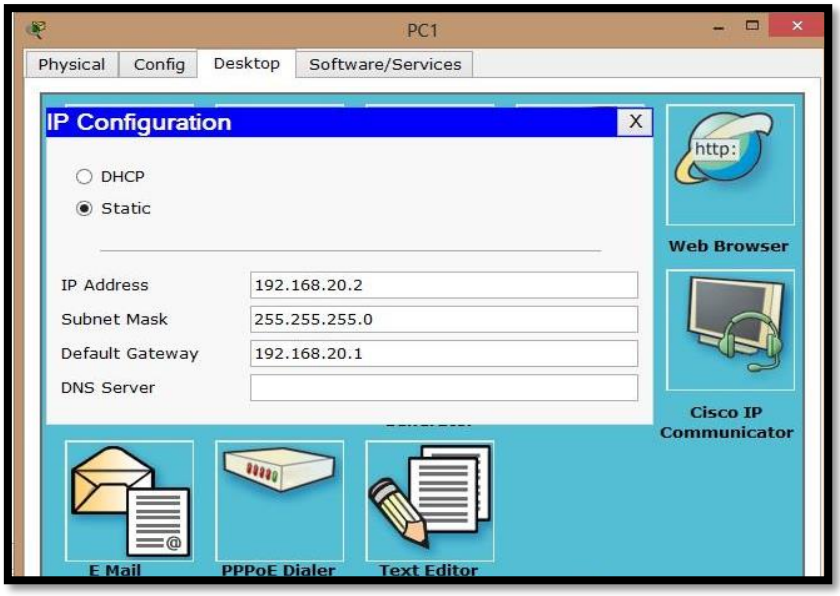
ابتدا طبق شکل بالا device **های لازم را گذاشته و ارتباطات لازم را برقرار می کنیم.**

سپس برای pc۰ **بصورت دستی** ip **تنظیم می کنیم مانند تصویر زیر:**



شکل ۲-۳

و هم چنین برای pc۱



شکل ۳-۳

به قسمت CLI روتر R۱رفته و دستورات زیر را می نویسیم :

Router>enable

Router#conf terminal

Router(config)#hostname R۱

R۱(config)#interface FastEthernet۰/۰

R۱(config-if)#ip address ۱۹۲,۱٦۸,۱۰,۱ ۲۵۵,۲۵۵,۲۵۵,۰

R۱(config-if)#no shutdown

اینتر فیس سریال ۰/ ۰

R۱(config)#interface Serial ۰/۰

R۱(config-if)#ip address ۱,۱,۱,۱ ۲۵۵,۲۵۵,۲۵۵,۰

R۱(config-if)#no shutdown

R۱(config-if)#clock rate ٦٤۰۰۰

از دستور clock rate **برای سمت** (DCE**سرویس دهنده**) **استفاده می کنیم. طریقه تشخیص آن هم در نرم افزار** Packet tracer **به این صورت است که هنگامی که روی اتصال** DCE **با ماوس برویم یک علامت ساعت در آن سمت ظاهر می شود**

. و برای اســتفاده از این اتصــالSERIAL DCE در نرم افزار، ابتدا باید روتر را خاموش کرده و ماژول WIC-۱T را به آن اضـافه نمود و دوباره روتر را روشــن می کنیم .

شکل ۴-۳

حالا به سراغ روتر R۲ می رویم و تنظیمات اینترفیس ها را مانند روتر R۱ انجام می دهیم.

Router>enable

Router#conf terminal

Router(config)#hostname R۲

R۲(config)#interface FastEthernet۰/۰

R۲(config-if)#ip address ۱۹۲,۱۶۸,۲۰,۱ ۲۵۵,۲۵۵,۲۵۵,۰

R۲(config-if)#no shutdown

اینترفیس سریال ۳/۰

R۲(config)#interface Serial۳/۰

R۲(config-if)#ip address ۱,۱,۱,۲ ۲۵۵,۲۵۵,۲۵۵,۰

R۲(config-if)#no shutdown

تا اینجا فقط تنظیمات اولیه را انجام دادیم و هنوز بین pc **رتباط برقرار نیست.برای استفاده از** static routing **از دستور زیر استفاده می کنیم:**

روتر R۱

R۱(config)#ip route ۱۹۲,۱۶۸,۲۰,۰ ۲۵۵,۲۵۵,۲۵۵,۰ serial ۰/۰

البته به جای استفاده از اینترفیس سریال در آخر دستور می شود ip **را که برای روتر** R۲ **تنظیم شده نیز استفاده کرد:**

R۱(config)#ip route ۱۹۲,۱۶۸,۲۰,۰ ۲۵۵,۲۵۵,۲۵۵,۰ ۱,۱,۱,۲

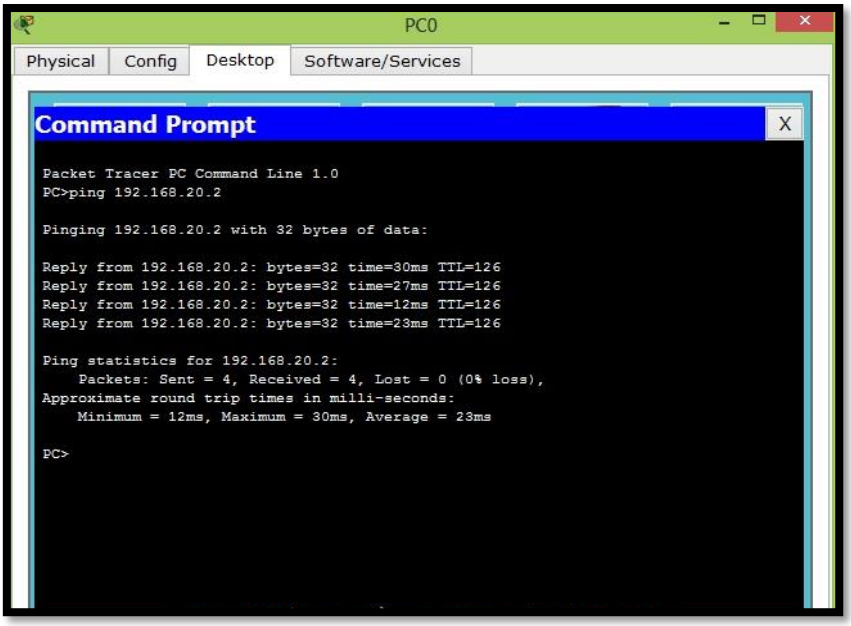
وبرای روتر R۲

R۲(config)#ip route ۱۹۲,۱۶۸,۱۰,۰ ۲۵۵,۲۵۵,۲۵۵,۰ serial ۳/۰

البته به جای استفاده از اینترفیس سریال در آخر دستور می شود ip **را که برای روتر** R۱ **تنظیم شده نیز استفاده کرد.**

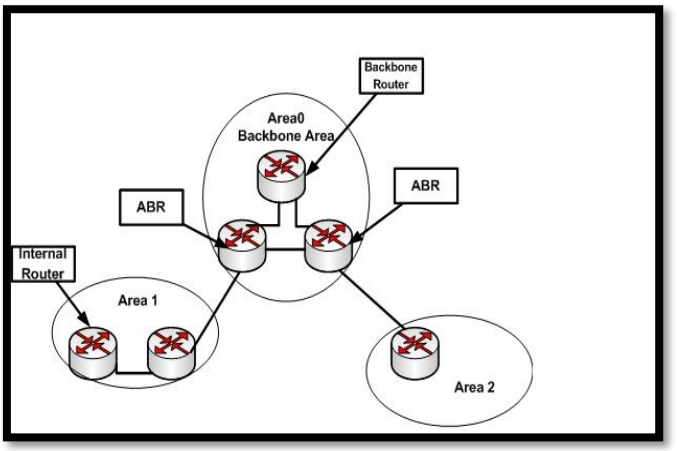
R۲(config)#ip route ۱۹۲,۱۶۸,۱۰,۰ ۲۵۵,۲۵۵,۲۵۵,۰ ۱,۱,۱,۱

حالا ارتباط را تست می کنیم . همانطور که مشاهده می کنید، ارتباط برقرار است.



شکل ۵-۳

معرفی پروتکل مسیریابیOpen Shortest Path First



شکل ۶-۳

پروتکل مسیریابی Open Shortest Path First یا OSPF، **یک پروتکل مسیریابی Link state است که می تواند ترافیک های مربوط به پروتکل** IP **را مدیریت کند** . OSPF**بر خلاف برخی پروتکل ها که بصورت انحصاری توسط شرکت ها ارائه می شوند یک پروتکل کاملا جامع و بدون وابستگی به هیچ برند خاصی است . تقریبا همه روترهایی که در دنیا وجود دارند از پروتکل** OSPF **پشتیبانی می کنند** .OSPF **از الگوریتم** Shortest Path First یا SPF **که توسط** Dijkstra **طراحی شده است برای جلوگیری از بوجود آمدن Routing Loop در توپولوژی شبکه ها استفاده می کند و به نوع یک شبکه** Loop Free **ایجاد می کند** .OSPF **فرآیند Convergence سریعی دارد و از طرفی قابلیت** Incremental Update **را نیز با استفاده از Link State Advertisement یا LSA فراهم می کند.** OSPF **یک پروتکل** Classless **است و به شما این اجازه را می دهد که برای طراحی یک ساختار سلسله مراتبی شبکه از** VLSM **و** ROUTE Summarization **براحتی استفاده کنید.**

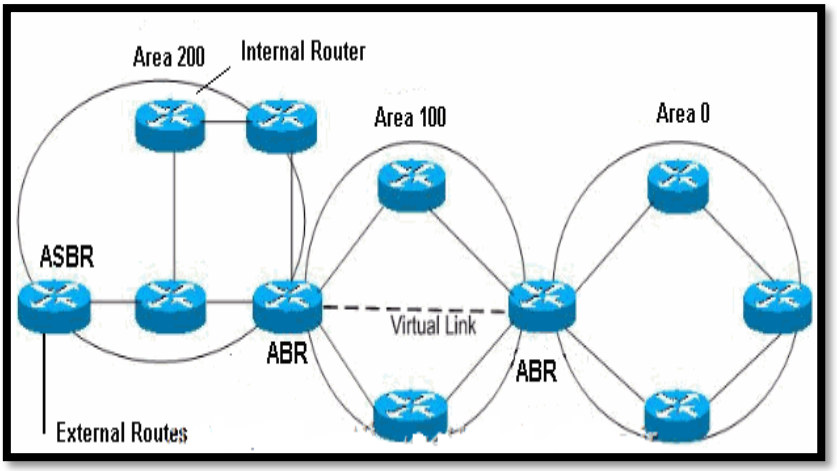
مهمترین معایبی که در OSPF **وجود دارد این است که** OSPF **برای نگهداری**

لیست OSPF Neighborها ، توپوپولوژی شبکه که شامل یک دیتابیس از تمامی روترها و Routeهای موجود در آن هاست و همچنین Routing Table خود روتر، به حافظه RAM نسبتا بیشتری در مقایسه با پروتکل های **Distance Vector** نیاز دارد ، همچنین OSPF به قدرت پردازشی یا CPU بیشتری برای اجرا کردن الگوریتم SPF نیاز دارد و همین موارد باعث می شود که OSPF در رده بندی پروتکل های مسیر یابی پیچیده یا Complex Protocol قرار بگیرد. دو مفهوم بسیار مهم در مواردی که می خواهید از OSPF استفاده کنید وجود دارند که اولین مفهوم **Autonomous System**و دومین مفهوم **Area** می باشد .**Area**در OSPF برای ایجاد کردن ساختار مسیریابی سلسله مراتبی یا موروثی (Hierarchical Routing)در یک **Autonomous System**استفاده می شود. **Area** ها تعیین کننده این هستند، که چگونه و به چه اندازه اطلاعات مربوط به Routing بایستی در شبکه به اشتراک گذاشته شود. OSPF دو لایه وراثت یا Hierarchyدارد ، لایه Backbone یا ۰ **Area**و لایه های خارج از Backbone یا **Area**های بین عدد ۱ تا ۶۵۵۳۵ . این‌دو ، دو **Area**ای متفاوت هستند که می توان در بین آن ها اطلاعات مسیریابی را **Summarize**کرد **Route** . **Summarization** به ما کمک می کند که بتوانیم Routing Table های خود را فشرده سازی و کوچکتر کنیم. تمامی **Area**ها بایستی به ۰ **Area**متصل شوند و تمامی روترها در این **Area**از یک توپولوژی یکسان استفاده می‌کنند .

واژه های مرتبط باOSPF

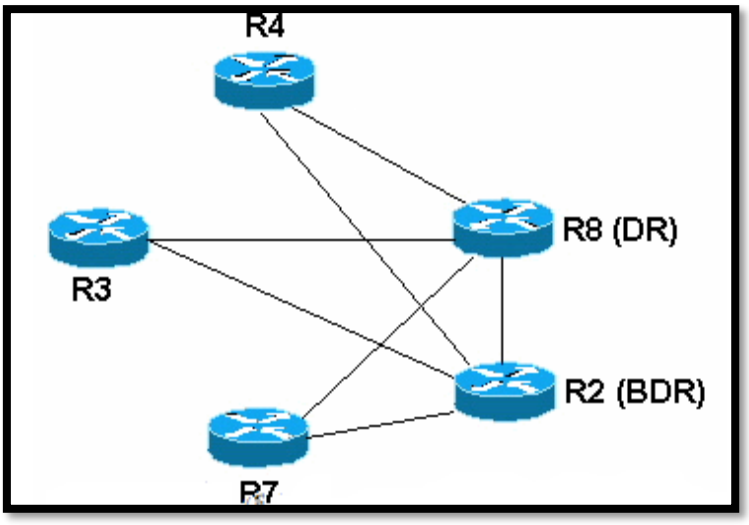
- **Router ID**در **OSPF** : هر روتر در پروتکل OSPF به یک **Router ID**منحصر به فرد نیاز داردکه برای شناسایی یک روتر در توپولوژی OSPFاستفاده می شود.

- **Loopback Interface**: این interface در واقع یک virtual interfaceبر روی روتر است ، بصورت پیشفرض روتر **loopback interface** ندارد ولی می توان به راحتی آن را ایجاد کرد ، این interface ها برای روتر به منزله یک interface فیزیکی واقعی در نظر گرفته می شوند و می توانید به آن ها نیز آدرس IP اختصاص بدهید.



شکل ۷-۳

- **Area Border Router**یا **ABR**: به روتری که یک یا چندین **OSPF Area**را به شبکه Backbone متصل می کند گفته می شود . این Router به عنوان یک عضو در نظر گرفته می شود که در توپولوژی OSPF به تمامی **Area**ها متصل شده است.
- **Internal Router**: به روتری که رابطه OSPF ای با سایر روترهای موجود در همان **Area**را دارد، گفته می شود.
- **Backbone Router**: قسمت مهمی از OSPF Backbone می باشد که شامل تمامی ABR ها و همچنین روترهایی که به **Area**های مختلف متصل شده اند می شود.



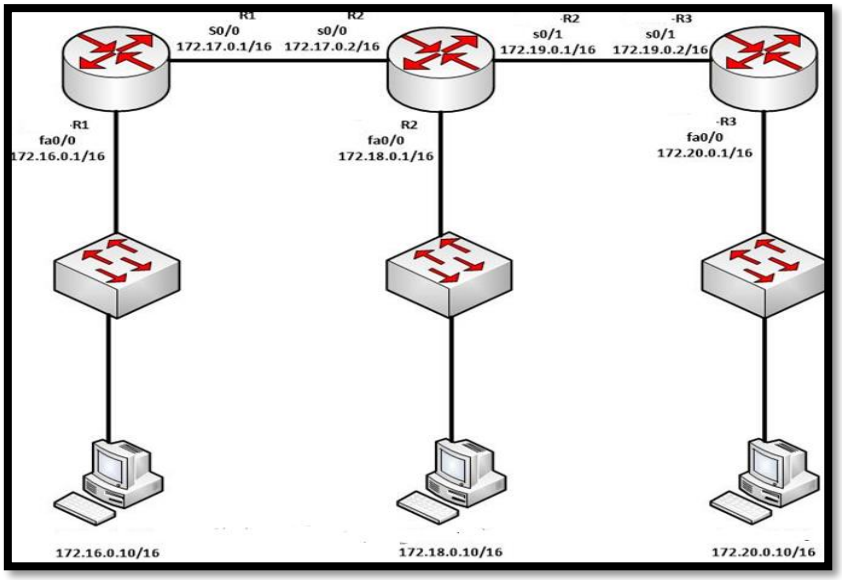
شکل ۸-۳

- **Designated Routerیا DR و Backup Designated Router یا BDR**

وروتر DR یا Designated Router **: در واقع یک** router interface **است که توسط همه روترهای موجود در یک سگمنت شبکه به عنوان روتر منتخب انتخاب شده است و** BDR **یا** Backup Designated Router **روتر جانشین یا** Backup**همین** DR **است** .DR **ها با تعریف مسیرهای ویژه برای رد و بدل شدن** Routing Update**ها باعث کاهش ترافیک شبکه می شوند** .DR **ها وظیفه نگهداری** Topology Table**یا توپولوژی کامل شبکه به همراه تمامی** Update **های شبکه ها را بر عهده دارد .** DR**این اطلاعات را که مربوط به** Update **شدن اطلاعات است در قالب** **Multicast** **برای سایر روترهای شبکه ارسال می کند. تمامی روترهای موجود در یک** **Area** **با استفاده از** Designated Router **یا** DR**ها می توانند یک رابطه** Slave/Master **را با همدیگر ایجاد کنند.**

راه اندازی کامل سناریوی پیاده سازی OSPF

سه عدد روتر ، سه عدد سوئیچ و سه عدد Host داریم که با سه محدوده آدرسی دهی متفاوت به هم متصل شده اند :



شکل ۹-۳

انجام تنظیمات مربوط به پروتکل OSPF روی روتر R۱

با استفاده از دستور زیر به پورت کنسول R۱متصل شوید و تنظیمات OSPF را روی آن انجام دهید. با استفاده از دستور network همانطور که در تصویر پایین مشاهده می کنید ما فقط لینک هایی که بصورت مستقیم به روتر متصل شده اند را به آن معرفی می کنیم ، دستورات زیر را می توانید بدون کمی و کاستی در روتر خود وارد کنید :

```
١

٢
R١>enable
٣R١#configure terminal
٤Enter configuration commands, one per line.  End with CNTL/Z.
R١ (config)#router ospf ١
٥R١ (config-router)#network ١٧٢,١٦,٠,٠ ٠,٠,٢٥٥,٢٥٥ area ٠
٦R١ (config-router)#network ١٧٢,١٧,٠,٠ ٠,٠,٢٥٥,٢٥٥ area ٠
R١ (config-router)#exit
٧R١ (config)#exit
٨R١#

٩
```

فراموش نکنید که بعد از وارد کردن دستورات بالا در انتها دستور

copy running-config startup-config

را در enable modeبزنید تا تنظیمات شما روی روتر بصورت دائمی ذخیره شود و بعد از restart **شدن روتر تنظیمات از بین نرود.**

انجام تنظیمات مربوط به پروتکلOSPF روی روتر R۲

با استفاده از دستور زیر به پورت کنسول R۲ متصل شوید و تنظیمات OSPFرا روی آن انجام دهید. با استفاده از دستور networkهمانطور که در تصویر پایین مشاهده می کنید ما فقط لینک هایی که بصورت مستقیم به روتر متصل شده اند را به آن معرفی می کنیم ، دستورات زیر را می توانید بدون کمی و کاستی در روتر خود وارد کنید. فراموش نکنید که بعد از وارد کردن دستورات زیر در انتها، دستور

copy running-config startup-config

را در **enable mode** بزنید تا تنظیمات شما روی روتر بصورت دائمی ذخیره شود و بعد از restart شدن روتر تنظیمات از بین نرود.

:

۱

۲

۳ R۲>
R۲>enable

۴ R۲#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.

۵ R۲(config)#router ospf ۱

۶ R۲(config-router)#network ۱۷۲,۱۷,۰,۰ ۰,۰,۲۵۵,۲۵۵ area ۰
R۲(config-router)#network ۱۷۲,۱۸,۰,۰ ۰,۰,۲۵۵,۲۵۵ area ۰

۷ R۲(config-router)#network ۱۷۲,۱۹,۰,۰ ۰,۰,۲۵۵,۲۵۵ area ۰

۸ R۲(config-router)#exit
R۲(config)#exit

۹

۱۰

انجام تنظیمات مربوط به پروتکل OSPF روی روتر R۳

با استفاده از دستور زیر به پورت کنسول **ITPRO-R۳**متصل شوید و تنظیمات **OSPF**را روی آن انجام دهید. با استفاده از دستور **network** همانطور که در تصویر پایین مشاهده می کنید ما فقط لینک هایی که بصورت مستقیم به روتر متصل شده اند را به آن معرفی می کنیم ، دستورات زیر را می توانید بدون کمی و کاستی در روتر خود وارد کنید:

```
۱
۲ R۳>enable
۳R۳#configure terminal
۴Enter configuration commands, one per line.  End with CNTL/Z.
  R۳(config)#router ospf ۱
۵R۳(config-router)#network ۱۷۲,۱۹,۰,۰ ۰,۰,۲۵۵,۲۵۵ area ۰
۶R۳(config-router)#network ۱۷۲,۲۰,۰,۰ ۰,۰,۲۵۵,۲۵۵ area ۰
  R۳(config-router)#exit
۷R۳(config)#exit
۸R۳#
۹
```

فراموش نکنید که بعد از وارد کردن دستورات بالا در انتها دستور copy running-config startup-configرا در enable modeبزنید تا تنظیمات شما روی روتر بصورت دائمی ذخیره شود و بعد از restart شدن روتر تنظیمات از بین نرود .

مشاهده Routing Table های موجود روی R۱

بعد از وارد کردن دستورات بالا برای پیاده سازی پروتکل OSPFدر روتر R۱با استفاده از دستور show ip routeدر این روتر شما می توانید خروجی routing table**موجود در این روتر را به شکل زیر مشاهده کنید:**

```
  R۱>enable
۱ R۱#show ip route
۲  Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile,
   B - BGP
```

```
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N١ - OSPF NSSA external type ١, N٢ - OSPF NSSA external type ٢
E١ - OSPF external type ١, E٢ - OSPF external type ٢, E - EGP
i - IS-IS, L١ - IS-IS level-١, L٢ - IS-IS level-٢, 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   ١٧٢,١٦,٠,٠/١٦ is directly connected, FastEthernet٠/٠
     C   ١٧٢,١٧,٠,٠/١٦ is directly connected, Serial٠/٠
     O   ١٧٢,١٨,٠,٠/١٦ [١١٠/٦٥] via ١٧٢,١٧,٠,٢, ٠٠:٢٦:٣١, Serial٠/٠
     O   ١٧٢,١٩,٠,٠/١٦ [١١٠/١٢٨] via ١٧٢,١٧,٠,٢, ٠٠:٢٦:٢١, Serial٠/٠
     O   ١٧٢,٢٠,٠,٠/١٦ [١١٠/١٢٩] via ١٧٢,١٧,٠,٢, ٠٠:٢٤:٥٤, Serial٠/٠
```

در خروجی دستورات بالا کاراکتر O **در ابتدای خط مربوط به** routing table **ها به معنی این است که مسیری که پیدا شده است از طریق پروتکل مسیریابی OSPF شناسایی شده است و کاراکتر** C **به معنی اتصال مستقیم یا** directly connected **می باشد .**

اطمینان از عملکرد درست و تست ارتباط بین شبکه ها با استفاده از دستور Ping

برای اینکه مطمئن شویم که پروتکل مسیریابی OSPF ، به درستی کار می کند از طریق دستور ping **از** Host٠١ **که دارای آدرس** IP **به شکل١٦/١٠,٠,١٦٧٢,١٦ است،** Host٠٣ **که دارای آدرس** IP **به شکل ١٦/١٠,٠,٢٠,١٧٢است را** ping **می**

کنیم در صورتی‌که عملیات با موفقیت مانند خروجی زیر انجام شد کار به درستی انجام شده است و OSPF پیاده سازی شده است :

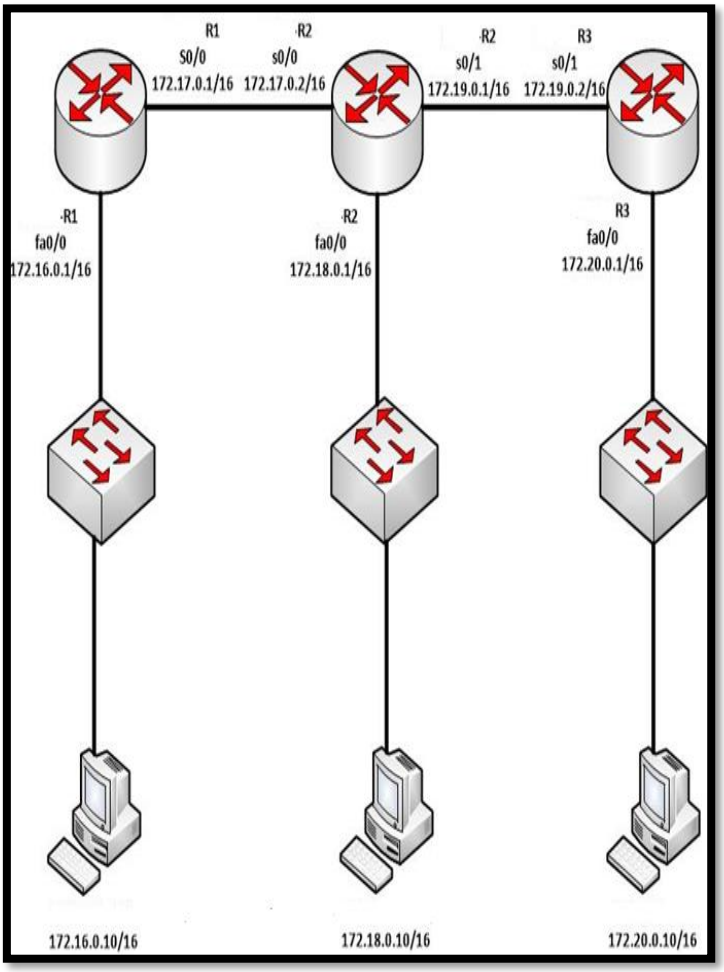
```
۱
۲
C:\>ping ۱۷۲,۲۰,۰,۱۰
۳ Pinging ۱۷۲,۲۰,۰,۱۰ with ۳۲ bytes of data:
۴ Reply from ۱۷۲,۲۰,۰,۱۰: bytes=۳۲ time=۱۷۲ms TTL=۱۲۵
Reply from ۱۷۲,۲۰,۰,۱۰: bytes=۳۲ time=۱۸۸ms TTL=۱۲۵
۵ Reply from ۱۷۲,۲۰,۰,۱۰: bytes=۳۲ time=۱۵۷ms TTL=۱۲۵
۶ Reply from ۱۷۲,۲۰,۰,۱۰: bytes=۳۲ time=۱۸۸ms TTL=۱۲۵
Ping statistics for ۱۷۲,۲۰,۰,۱۰:
۷ Packets: Sent = ٤, Received = ٤, Lost = ۰ (۰٪ loss),
۸ Approximate round trip times in milli-seconds:
Minimum = ۱۵۷ms, Maximum = ۱۸۸ms, Average = ۱۷٦ms
۹
۱۰
```

همان‌طور که در خروجی دستور ping بالا مشاهده می کنید خروجی reply from به درستی انجام می شود و این یعنی OSPFبه درستی پیکربندی شده است.

راه اندازی کامل سناریو پیاده سازی پروتکل RIPv۲

توپولوژی شبکه هایی که قرار است در آن ها RIPv۲را پیاده سازی کنیم به شکل زیر می باشد. همانطور که در پایین مشاهده می کنید ما ۳ عدد سوئیچ ، ۳ عدد روتر و سه عدد کامپیوتر داریم که به شبکه های مختلف متصل شده اند. نام روترها یا

Hostnameها و آدرس های IP آن ها را نیز در تصویر به خوبی می توانید مشاهده کنید:



شکل ۱۰-۳

انجام تنظیمات RIPv۲ برای R۱

برای پیکربندی RIPv۲ با استفاده از دستورات زیر به پورت کنسول R۱ متصل شوید. با استفاده از دستور network همانطور که در تنظیمات پایین مشاهده می کنید ما فقط شبکه هایی که مستقیما به روتر متصل شده اند را به آن معرفی می کنیم .

```
۱
۲
   R۱>enable
۳  R۱#configure terminal
۴  Enter configuration commands, one per line.  End with CNTL/Z.
   R۱(config)#router rip
۵  R۱(config-router)#version ۲
۶  R۱(config-router)#network ۱۷۲,۱٦,۰,۰
   R۱(config-router)#network ۱۷۲,۱۷,۰,۰
۷  R۱(config-router)#exit
۸  R۱(config)#exit
   R۱#
۹
۱۰
```

فراموش نکنید که بعد از وارد کردن دستورات بالا در انتها دستور

copy running-config startup-config

را در enable mode بزنید تا تنظیمات شما روی روتر بصورت دائمی ذخیره شود و بعد از restart شدن روتر تنظیمات از بین نرود .

انجام تنظیمات RIPv۲ برای R۲

برای پیکربندی RIPv۲ با استفاده از دستورات زیر به پورت کنسول R۲ متصل شوید. با استفاده از دستور network همانطور که در تنظیمات پایین مشاهده می کنید ما فقط شبکه هایی که مستقیما به روتر متصل شده اند را به آن معرفی می کنیم .

```
۱
۲
۳  R۲>enable
   R۲#configure terminal
۴  Enter configuration commands, one per line.  End with CNTL/Z.
۵  R۲(config)#router rip
   R۲(config-router)#version ۲
۶  R۲(config-router)#network ۱۷۲,۱۷,۰,۰
۷  R۲(config-router)#network ۱۷۲,۱۸,۰,۰
   R۲(config-router)#network ۱۷۲,۱۹,۰,۰
۸  R۲(config-router)#exit
۹  R۲(config)#exit
   R۲#
۱۰
۱۱
```

فراموش نکنید که بعد از وارد کردن دستورات بالا در انتها دستور

copy running-config startup-config

را در **enable mode** بزنید تا تنظیمات شما روی روتر بصورت دائمی ذخیره شود و بعد از restart شدن روتر تنظیمات از بین نرود .

انجام تنظیمات RIPv۲ برای R۳

برای پیکربندی RIPv۲ با استفاده از دستورات زیر به پورت کنسول R۳ متصل شوید. با استفاده از دستور network همانطور که در تنظیمات پایین مشاهده می کنید ما فقط شبکه هایی که مستقیما به روتر متصل شده اند را به آن معرفی می کنیم .

```
۱
۲
   R۳>enable
۳  R۳#configure terminal
۴  Enter configuration commands, one per line.  End with CNTL/Z.
   R۳(config)#router rip
۵  R۳(config-router)#version ۲
۶  R۳(config-router)#network ۱۷۲,۱۹,۰,۰
   R۳(config-router)#network ۱۷۲,۲۰,۰,۰
۷  R۳(config-router)#exit
۸  R۳(config)#exit
   R۳#
۹
۱۰
```

فراموش نکنید که بعد از وارد کردن دستورات بالا در انتها دستور،

copy running-config startup-config

را در **enable mode** بزنید تا تنظیمات شما روی روتر بصورت دائمی ذخیره شود و بعد از restart شدن روتر تنظیمات از بین نرود.

مشاهده Routing Table موجود روی R۱

بعد از اینکه شبکه ها به خوبی **Converged** شدند و تنظیمات اولیه **Routing Information Protocol Version ۲** به درستی انجام شد ، ما می توانیم با استفاده از دستور show ip route در روتر R۱ محتویات Routing Table این روتر را مشاهده کنیم ، همانطور که در نتیجه دستور زیر مشاهده می کنید :

```
R١>enable
R١#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
N١ - OSPF NSSA external type ١, N٢ - OSPF NSSA external type
٢
E١ - OSPF external type ١, E٢ - OSPF external type ٢, E - EGP
i - IS-IS, L١ - IS-IS level-١, L٢ - IS-IS level-٢, 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   ١٧٢,١٦,٠,٠/١٦ is directly connected, FastEthernet٠/٠
C   ١٧٢,١٧,٠,٠/١٦ is directly connected, Serial٠/٠
R   ١٧٢,١٨,٠,٠/١٦ [١٢٠/١] via ١٧٢,١٧,٠,٢, ٠٠:٠٠:٢٢, Serial٠/٠
R   ١٧٢,١٩,٠,٠/١٦ [١٢٠/١] via ١٧٢,١٧,٠,٢, ٠٠:٠٠:٢٢, Serial٠/٠
R   ١٧٢,٢٠,٠,٠/١٦ [١٢٠/٢] via ١٧٢,١٧,٠,٢, ٠٠:٠٠:٢٢, Serial٠/٠
```

حرف R به معنای این است که Route ای که در این خط مشاهده می کنید، با استفاده از RIPv٢شناسایی شده است، حرف C نیز به معنای این است که Routeای که در این خط مشاهده می کنید بصورت مستقیم یا Directly Connectedبه روتر متصل شده است.

اطمینان از عملکرد درست و تست ارتباط بین شبکه ها با استفاده از دستور Ping

برای تست کردن Route های ایجاد شده توسط RIPv٢ و تست ارتباط بین شبکه کافیست با استفاده از دستور ping از Host٠١ به آدرس IP به

شـــماره ۱۷۲,۱۶,۰,۱۰/۱۶به Host۰۳ بـــه آدرس IP بـــه شـــماره ۱۶/۱۷۲,۲۰,۰,۱۰ تســت ارتبــاط و صــحت عملکــرد RIPv۲را مطــابق نتیجــه دستور پایین انجام دهیم:

```
۱
۲
   C:\>ping ۱۷۲,۲۰,۰,۱۰
۳  Pinging ۱۷۲,۲۰,۰,۱۰ with ۳۲ bytes of data:
۴  Reply from ۱۷۲,۲۰,۰,۱۰: bytes=۳۲ time=۱۷۲ms TTL=۱۲۵
   Reply from ۱۷۲,۲۰,۰,۱۰: bytes=۳۲ time=۱۸۸ms TTL=۱۲۵
۵  Reply from ۱۷۲,۲۰,۰,۱۰: bytes=۳۲ time=۱۵۷ms TTL=۱۲۵
۶  Reply from ۱۷۲,۲۰,۰,۱۰: bytes=۳۲ time=۱۸۸ms TTL=۱۲۵
   Ping statistics for ۱۷۲,۲۰,۰,۱۰:
۷  Packets: Sent = ٤, Received = ٤, Lost = ۰ (۰٪ loss),
۸  Approximate round trip times in milli-seconds:
   Minimum = ۱۵۷ms, Maximum = ۱۸۸ms, Average = ۱۷٦ms
۹
۱۰
```

نتیجه دستور نشان می دهد که ارتباط برقرار است.

تفاوت RIPv۱ و RIPv۲ در چیست ؟

ویژگی های Routing Information Protocol Version ۱

۱. RIPv۱یک پروتکل مسیریابی **Distance-Vector** است.
۲. RIPv۱یک پروتکل مسیریابی Classful است. پروتکل های مسیریابی Classful ، فقط از شبکه هایی پشتیبانی می‌کنند که Subnet نشده اند. پروتکل های مسیریابی Classful اطلاعات مربوط به Subnet Maskرا در

Routing Updateهای خود ارسال نمی کنند. به زبان دیگر اگر شما شبکه ای دارید که در RIPv۱ Routing Domain قرار دارد، RIPv۱ این شبکه را به عنوان شبکهSubnet ، نشده به سایر شبکه های موجود در Routing Domainمعرفی می کند.

۳. RIPv۱ از **Variable Length Subnet Masking** یا **VLSM** پشتیبانی نمی‌کند.

۴. RIPv۱ حداکثر از **Metric Value**ی ۱۵ پشتیبانی می کند یا به عبارتی فقط ۱۵ عدد **Hop Count**را پشتیبانی می‌کند. اگر تعداد **Hop Count** ها بیشتر از عدد ۱۵ شود RIPv۱ این شبکه را به عنوان شبکه غیر قابل دسترس یا Unreachable در نظر می‌گیرد.

۵. RIPv۱ توسط مکانیزم **Broadcast**، بسته های بروزرسانی یا Routing Updateرا هر ۳۰ ثانیه یکبار بصورت متناوب برای روترهای همسایه ارسال می کند. با توجه به اینکه بسته های بروز رسانی با استفاده از آدرس IP مقصد به شکل ۲۵۵,۲۵۵,۲۵۵,۲۵۵ یا همان **Broadcast IP**ارسال می شوند، هر روتری که در مسیر اس، نیازمند پردازش پیام های دریافتی از این فرآیند و انجام Process های لازم برای تعیین اینکه روتر ارسال کننده از پروتکل RIPv۱استفاده کرده است یا خیر می‌باشد.

۶. RIPv۱ برای ارسال پیام های بروز رسانی یا update message ها دارای مکانیزم احراز هویت نمی باشد.

ویژگی های Routing Information Protocol Version ۲

۱. RIPv۲یک پروتکل مسیریابی از نوعِ Distance Vector است.

۲. RIPv۲یک پروتکل مسیریابی Classless است که به شما اجازه می دهد که بتوانید از شبکه هایی که Subnet شده اند نیز در فرآیند مسیریابی استفاده کنید. همچنین RIPv۲ اجازه ارسال شدن Network Mask شبکه را در بین شبکه ها می دهد تا فرآیند Classless Routing به درستی انجام شود.

۳. RIPv۲از **Variable Length Subnet Masking** یا **VLSM** پشتیبانی می کند.

۴. RIPv۲حداکثر از Metric Valueی ۱۵ پشتیبانی می کند یا به عبارتی فقط ۱۵ عدد Hop Countرا پشتیبانی می کند. اگر تعداد Hop Count ها بیشتر از عدد ۱۵ شود RIPv۲ این شبکه را به عنوان شبکه غیر قابل دسترس یا Unreachableدر نظر می گیرد.

۵. RIPv۲از Triggered Update پشتیبانی می کند یا به نوعی می توانیم بگوییم Incremental Updateرا پشتیبانی می کند.

۶. RIPv۲توسط مکانیزم Multicastبه آدرس Multicastبه شماره ۲۲۴.۰.۰.۹ بسته های Routing Update را به سایر روترهای موجود در مسیر منتقل می کند. بروز رسانی با استفاده از Multicast باعث کاهش ترافیک شبکه می شود. همچنین استفاده از این مکانیزم باعث کاهش Overhead روی روترهایی می شود که در Routing Domain قرار دارند. نکته قابل توجه در RIPv۲ این است که فقط روترهایی که از RIPv۲ پشتیبانی می کنند می توانند به Multicast Group ۲۲٤.۰.۰.۹عضو شوند و سایر روترهایی که RIPv۲ را ندارند تنها می توانند Routing Update ها را در لایه دوم فیلتر کنند.

۷. RIPv۲ برای ارسال پیام های بروز رسانی یا update message ها دارای مکانیزم احراز هویت می باشد. مکانیزم احراز هویتی باعث می شود که روتر مطمئن باشد ترافیک Update های ورودی از منابعl معتبری ارسال می شوند.

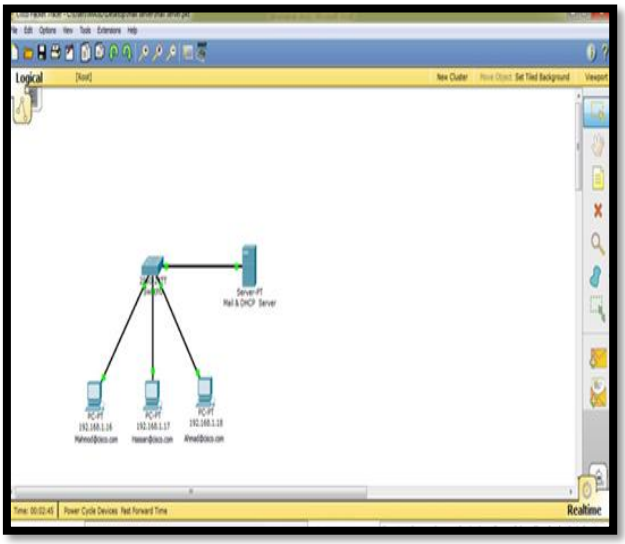
راه اندازی Mailserverدر Packet Tracer

برای این سناریو به تجهزات زیر نیازمندیم :

۱ . سرور

۲. سوییچ ۲۹۶۰

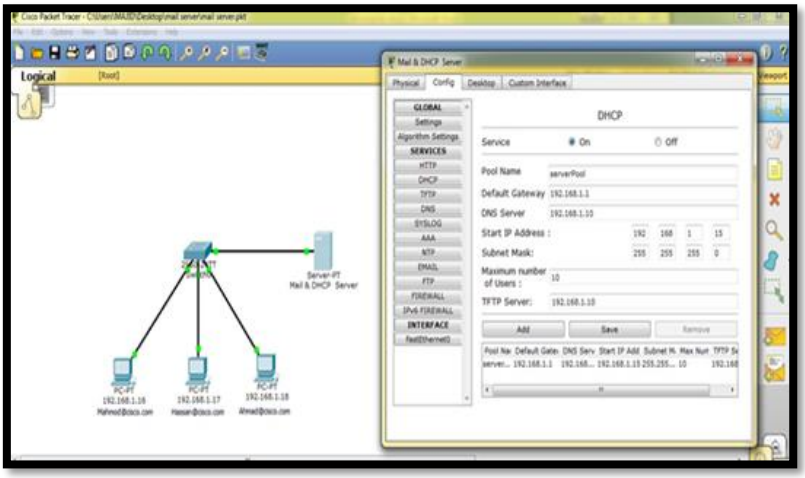
۳. کامپیوتر



شکل ۱۰-۳

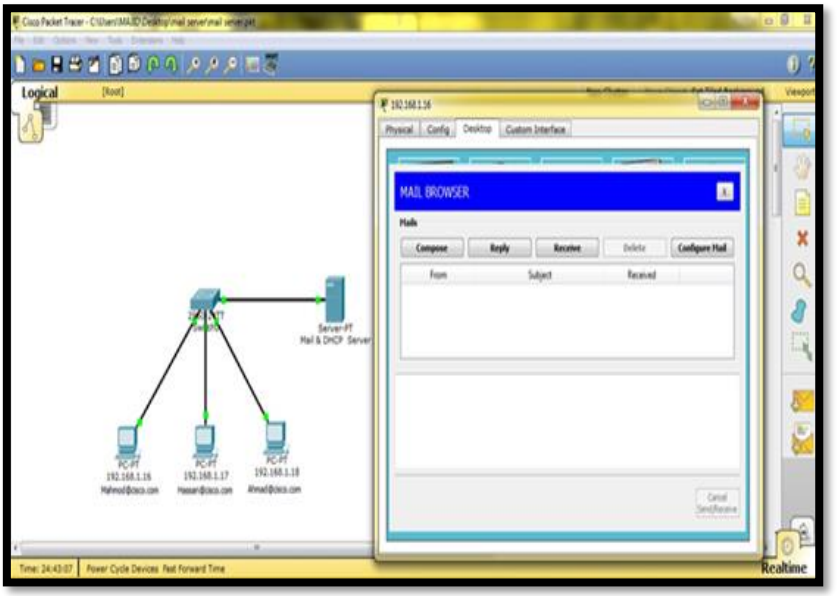
ارتباطات را با کابل Straight **برقرار نموده و به سرور** ip **۱۹۲,۱۶۸,۱,۱۰ می دهیم و برای باقی سیستم ها در این سناریو جهت سهولت در کار از** DHCP **استفاده می نماییم، که برای این کار ابتدا بر روی سرور کلیک کرده به قسمت** Config **رفته و سرویس** DHCP **را به حالت** ON **قرار بدهید و در قسمت** Pool Name **نام** DHCP **سرور را وارد کنید، که بطور پیش فرض** ServerPool **است و در این سناریو از همین نام استفاده می کنیم و در قسمت بعد** Default Gateway **آدرس** Gateway،IP

شبکه را وارد می کنیم که بصورت اتوماتیک به کلیه سیستم ها نیز اعمال می شود و درقسمت بعدDNS server شبکه را وارد می کنیم که در این سناریو DNS server استفاده نشده و در قسمت بعد Start IP Address ، اولین آدرس IP که به سیستم اعمال می شود تعریف می کنیم، که در این سناریو از شبکه ۱۹۲,۱۶۸,۱۰,۰/۲۴ که اولین آدرس IP در این شبکه از ۱۵ شروع شده است و در قسمت بعد subnet mask شبکه را وارد می کنیم ۲۵۵,۲۵۵,۲۵۵,۰ . در قسمت بعد بیشترین تعداد user ها تعیین می گردد که در این سناریو ۱۰ عدد استفاده شده است .



شکل ۱۱-۳

کلیه تنظیمات برای DHCP Server اعمال شده است و با زدن کلید Save سرویس مورد نظر فعال می شود و می توانید به کامپیوتر ها مراجعه کنید و در انجا به تنظیمات IP Configuration بروید و از DHCP استفاده کنید، که بطور اتوماتیک آدرس IP وسایر آدرس ها ارایه می شود.



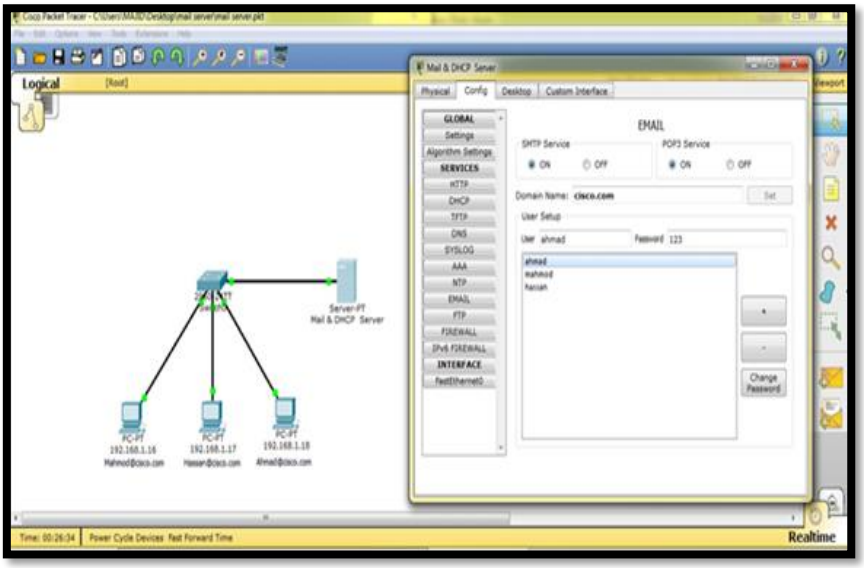
شکل ۱۲-۳

برای سیستم های دیگر نیز این کار را انجام بدهید تا آدرس IP آن ها اعمال شود . حال برای راه اندازی Mail Server بر روی سرور کلیک می کنید و قسمت Email رفته و سرویس های STPو۳Pop را در حالت ON قرار دهید و در قسمت Domain Name نام دامینی که قرار است، سرویس ایمیل ارایه کند را وارد می کنیم که دراین سناریو از Cisco.com استفاده شده است و در قسمت بعد یعنی در USER Setup ، نوبت به تعریف نام کاربری و رمز عبور برای ایمیل های کاربران می رسد که در این سناریو کاربران زیر با رمز عبور تعریف شده اند :

۱ Ahmad۱۲۳

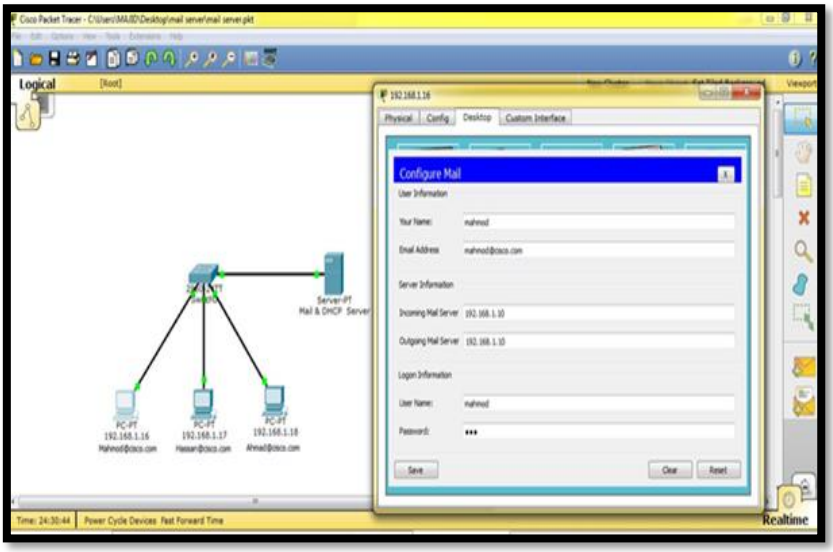
۲ Mahmod۴۵۶

۳ Hassan۷۸۹



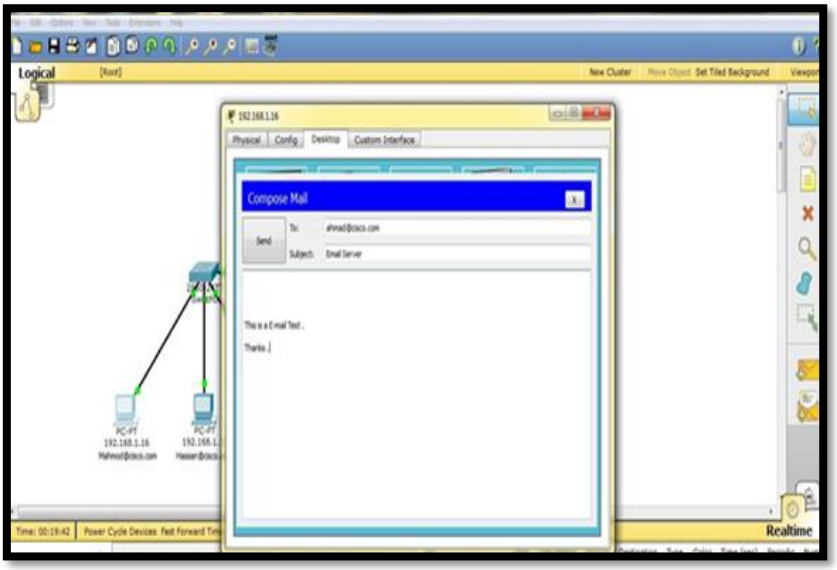
شکل ۱۳-۳

سرویس ایمیل به صورت کامل فعال و نوبت به اعمال تنظیمات در کامپیوترهای کاربران شده است . برای این کار ابتدا بر روی کامپیوتر کلیک کرده و به قسمت Desktop **رفته و بعد بر روی** email **کلیک می کنیم و سرویس ایمیل را بصورت زیر تنظیم کنید :**

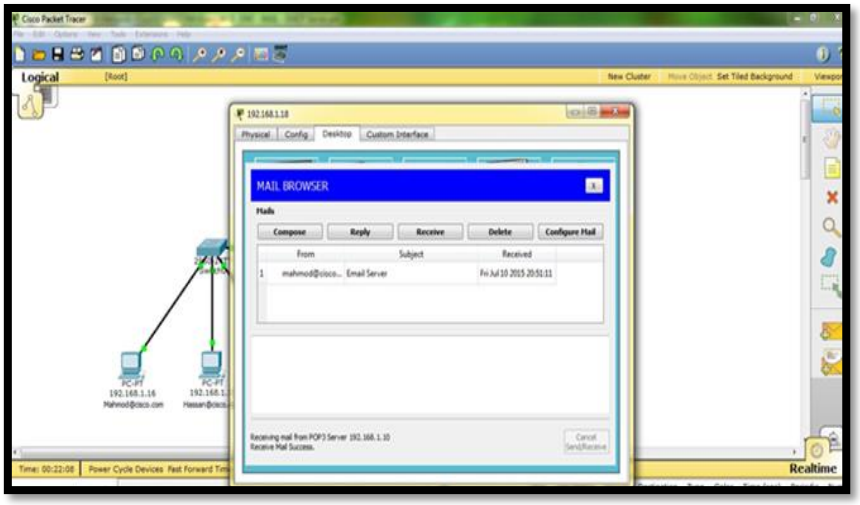


شکل ۱۴-۳

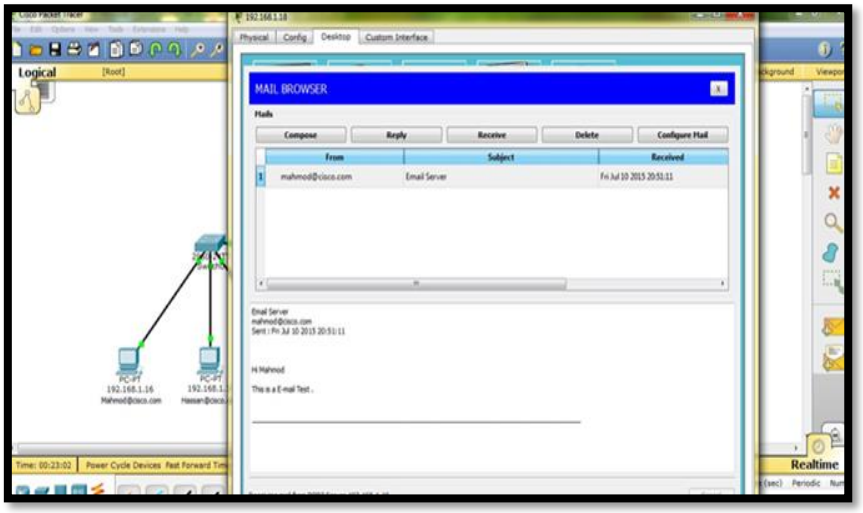
آدرس ایمیل و نام در قسمت User Information **وارد می‌شود و آدرس ۱۹۲,۱۶۸,۱,۱۰ جهت ارسال و دریافت ایمیل در قسمت** Server Information **وارد شود و در انتها** Pass & User **وارد می شود، هم چنین برای سایر سیستم ها نیز این کار را انجام دهید . سرویس ایمیل فعال شده است و کافی است در** Mail Browser **با زدن دکمه** Compose **ایمیلی را آماده کنید و زدن دکمه** Send **آن را برای کاربر مورد نظر ارسال کنید که ما از کاربر** Mahmod **به کاربر** Ahmad **ایمیل می زنیم و پاسخ آن را از** Ahmad **دریافت می کنیم برای بررسی عملکرد صحیح در این سناریو تصاویر زیر را دنبال کنید:**



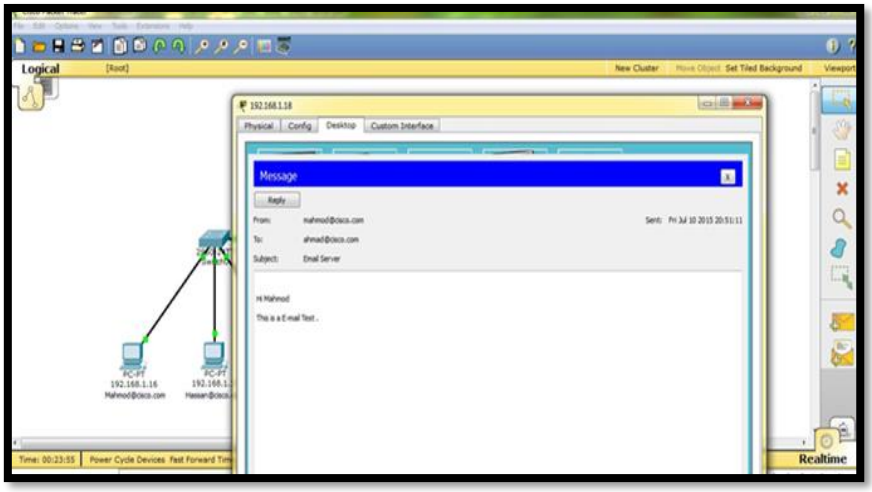
شکل ۱۵-۳



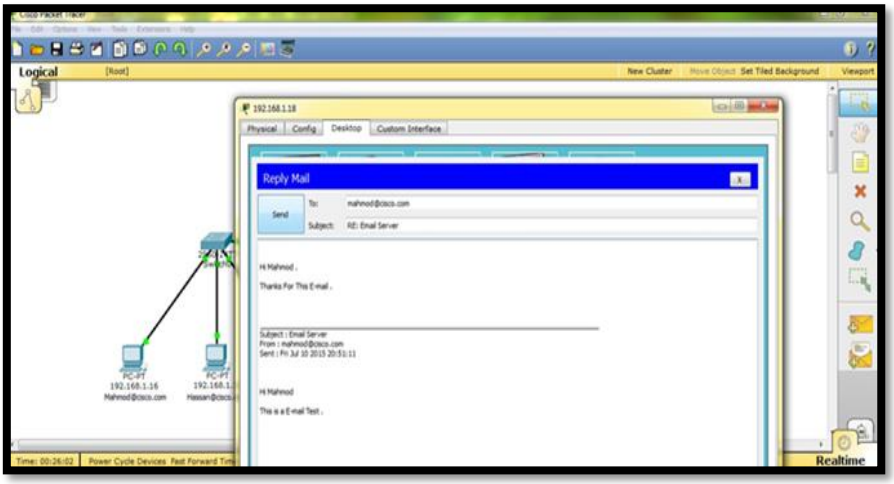
شکل ۱۶-۳



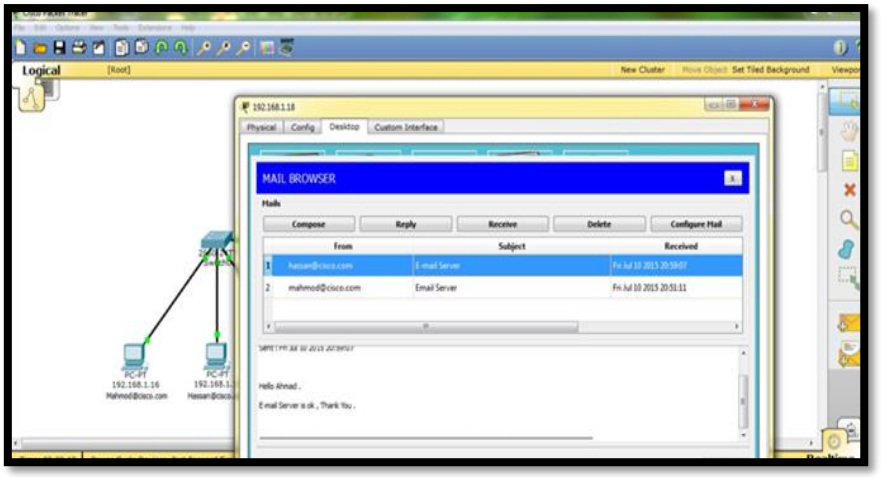
شکل ۱۷-۳



شکل ۱۸-۳



شکل۱۹-۳



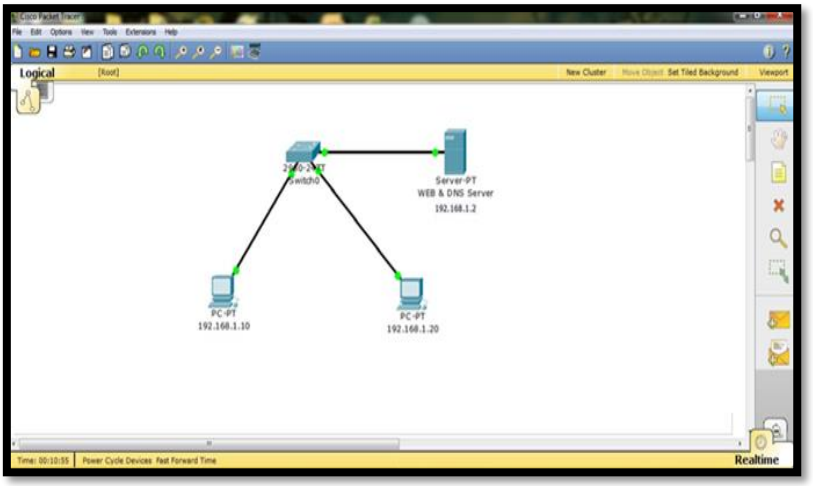
شکل ۲۰-۳

راه اندازی DNS Server & WEB

برای راه اندازی این سناریو از Device های زیر استفاده می کنیم :

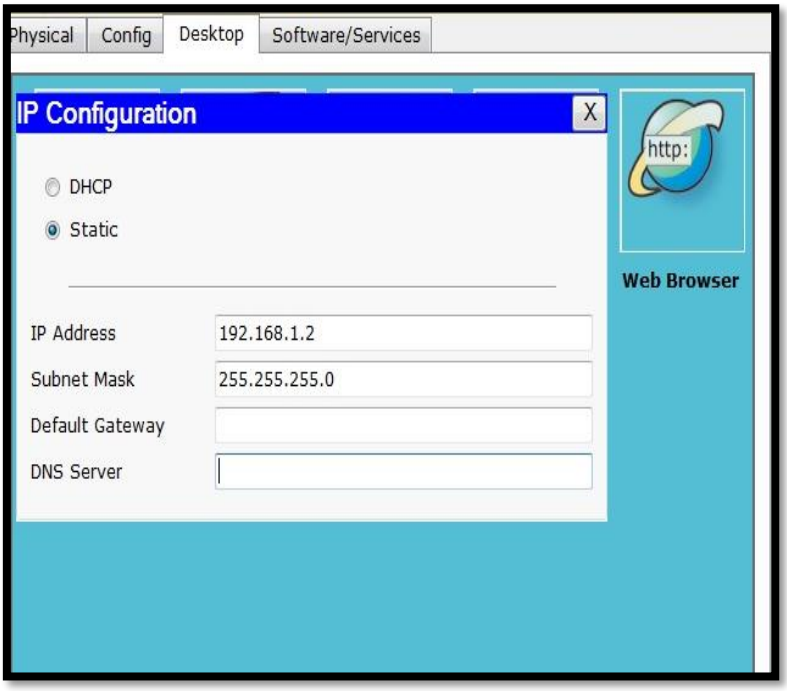
۱. سوییچ ۲۹۶۰ سیسکو
۲. PC
۳. سرور DNS & WEB

در گام نخست ارتباط بین سوییچ و سایر Device ها را با کابل Straight برقرار می کنیم .



شکل ۲۱-۳

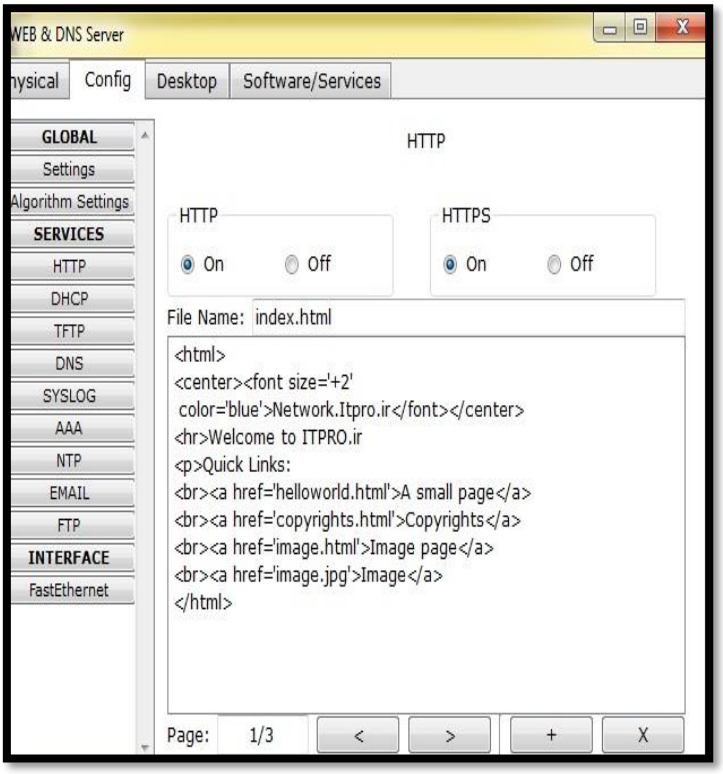
در ادامه به SERVER یک IP بصورت دستی اختصاص می دهیم که در این سناریو از Range ۲۴/۱۹۲,۱۶۸,۱,۰ استفاده می شود که به سرور ۱۹۲,۱۶۸,۱,۲ اختصاص داده شده است .



شکل ۲۲-۳

برای این کار کافی است روی سرور کلیک کرده و از قسمت DESKTOP **گزینه** IP Configuration **را انتخاب کرده و مانند تصویر فوق** IP **و** Subnet Mask **مورد نظر را وارد می کنیم .حال باید** WEB **و** DNS **رو روی سرور فعال کنیم برای این کار مراحل زیر را دنبال کنید :**

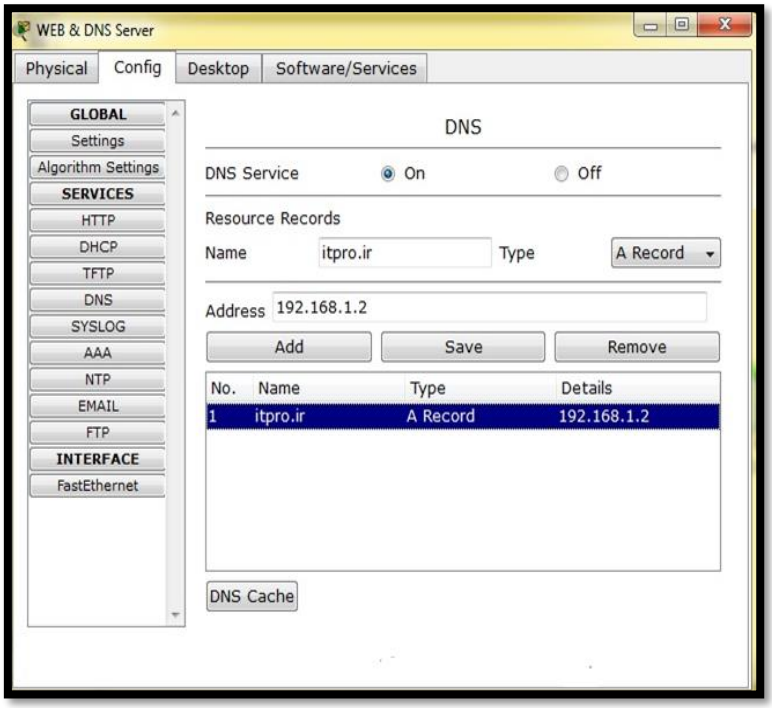
- **برای فعال کردن** WEB Server **روی سرور کلیک کرده و از قسمت** Config **گزینه** HTTP **را انتخاب می کنیم ، حال دو گزینه** HTTP **و** HTTPS **را روی** On **قرار می دهیم تا** WEB Server **بر روی سرور مورد نظر فعال شود .**



شکل ۲۳-۳

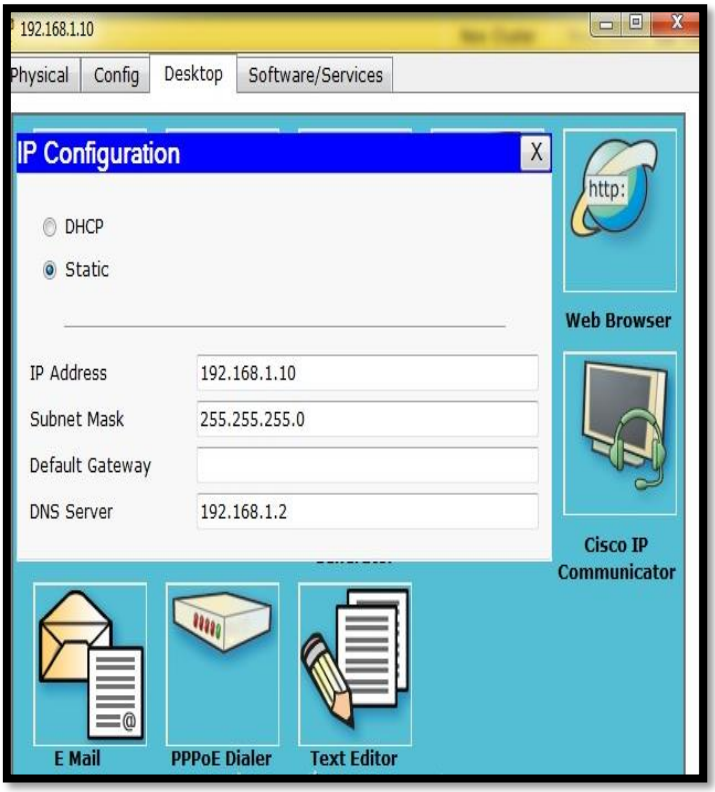
- **در ادامه برای فعال کردن** DNS Server **از قسمت** Config **گزینه** DNS **را انتخاب می کنیم و برای فعال کردن** DNS Service **گزینه** On **را انتخاب می کنیم و در قسمت** Name **نام مورد نظر وب سایت را وارد کرده و در قسمت** Address **آدرس آن را وارد کرده و گزینه** ADD **را انتخاب می کنیم**

.



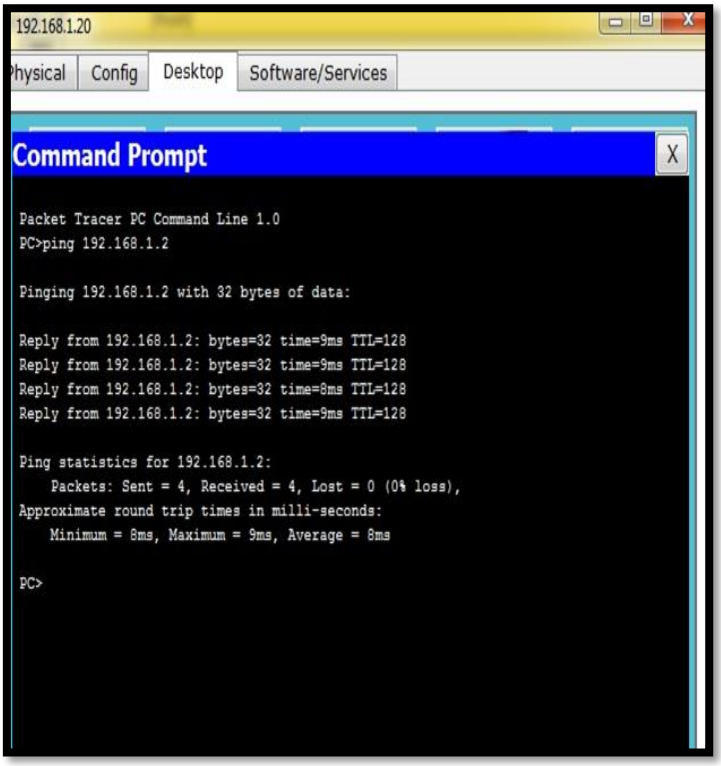
شکل ۳-۲۴

اکنون باید به PC ها آدرس IP بصورت دستی اختصاص دهیم ،که برای این کار کافی است روی PC مورد نظر کلیک کرده و از قسمت Desktop گزینه IP Configuration را انتخاب نموده و مطابق شکل زیر IP اختصاص دهیم (در قسمت DNS Server آدرس IP سرور DNS را وارد می نماییم) .



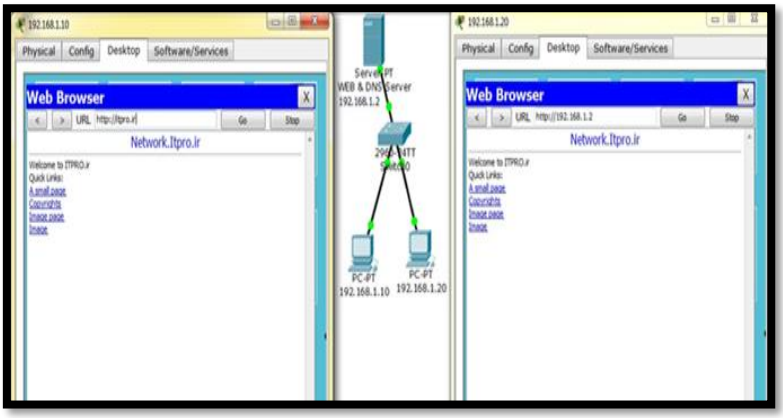
شکل ۲۵-۳

برای PC بعدی هم به همین شکل و IP ۱۹۲,۱۶۸,۱,۲۰ را وارد می کنیم .حال باید ارتباط بین PC ها و Server را تست کنیم که برای این کار می توان از دستور Ping استفاده نمود ، بر روی یکی از PC ها کلیک کرده و به قسمت Desktop رفته و گزینه Command Prompt را انتخاب کرده و با دستور Ping ۱۹۲,۱۶۸,۱,۲ ارتباط را چک می کنیم مطابق شکل زیر:



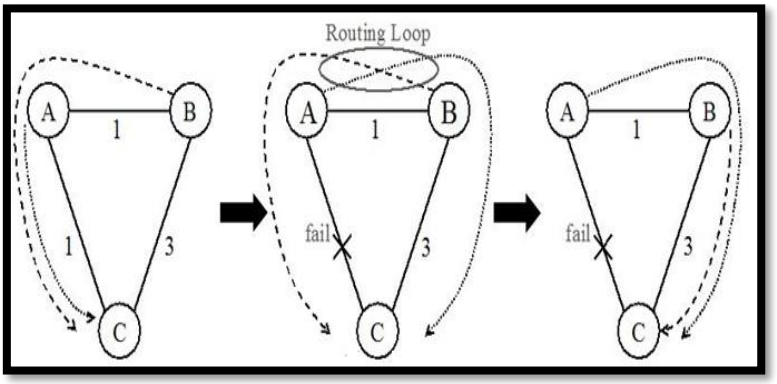
شکل ۲۶-۳

در انتها روی یکی از PC ها کلیک کرده و وارد Browser آن می شویم و آدرس ۱۹۲,۱۶۸,۱,۲ را وارد می کنیم و یک وب سایت با نام Network.itpro.ir نمایش داده می شود .



شکل ۲۷-۳

منظور از Routing Loop چیست ؟



شکل ۲۸-۳

Routing Loopیک مشکل جدی در فرآیند های مسیریابی شبکه محسوب می شود ، در این حالت یک Packet داده بصورت متناوب از همان روتری که آمده است ، مجددا و مجددا مسیریابی و عبور می کند و باز هم به همان روتر برمی گردد و مسیریابی می شود. این تناوب اینقدر ادامه دار می شود که تقریبا می توان گفت هیچوقت تمام نمی شود و در یک چرخه بی نهایت مسیریابی این بسته اطلاعاتی انجام

می شود . Routing Loop ها می توانند مشکل بسیار جدی برای شبکه های ما ایجاد کنند و در برخی اوقات توان این را دارند که شبکه را بصورت کلی از مدار خارج کنند و غیرفعال کنند. معمولا مشکلات مربوط به Routing Loop **در پروتکل های مسیریابی Distance Vector مشاهده می شود .مهمترین مشکلی که Routing Loop ها برای شبکه های ما ایجاد می کنند، گرفتن پهنای باند مفید شبکه است . با به وجود آمدن Routing Loopها ،پهنای باند مفید شبکه دچار اختلال می شود و پهنای باند غیر مفیدی که توسط** Packet **های** Loop **ایجاد شده اند جایگزین آن ها می شوند و این یعنی پایین آمدن کارایی شبکه . اما دومین مشکلی که Routing Loopها ایجاد می کنند و باعث کاهش کارایی شبکه ما می شوند این است که قدرت پردازشی که در روترهای شبکه ما وجود دارد در چنین حالتی مجبور است به** Packet **های ایجاد شده توسط** Loop **بی مصرف هم جوابگو باشد و به همین دلیل قدرت پردازشی روترهای ما برای** Packet **های سالم شبکه دچار مشکل خواهد شد و به طبع کارایی روتر نیز پایین خواهد آمد. Routing Loop ها معمولا در شبکه های بزرگی اتفاق می افتند، که در آن ها یک تغییر، قبلا در توپولوژی شبکه انجام شده است اما هنوز به روترهای دیگر Converge نشده است و در همین حین تغییر دومی در توپولوژی شبکه ایجاد می شود و قبل از رسیدن تغییرات اول در شبکه پخش می شود و باعث بروز مشکل در Converge شدن شبکه می شود. Convergence یا Convergeشدن به فرآیندی گفته می شود که در آن تمامی روترهای موجود در یک شبکه بر روی یک توپولوژی مشترک شبکه به توافق می رسند. پروتکل های Link Stateسرعت Convergenceبسیار بالایی دارند و این در حالی است که پروتکل های Distance Vector از سرعت پایینی در Convergeکردن شبکه ها برخوردارند .**

راهکارهای جلوگیری از بوجود آمدن Routing Loop در شبکه

۱. تعیین Maximum Hop Count یا حداکثر تعداد Hop Count

مکانیزم تعیین حداکثر تعداد Hop Count می تواند از به وجود آمدن Routing Loopجلوگیری کند. پروتکل های مسیریابی Distance Vector از مقدار TTLیا Time To Liveدر IP Datagram Headerخود برای جلوگیری از به وجود آمدن Routing Loop استفاده می کنند. زمانیکه یک IP Datagram از یک روتر به روتر دیگری منتقل می شود، روتر وضعیت تعداد Hopهای رد شده توسط IP Datagram را در فیلد TTL در Header آن نگهداری می کند. با عبور کردن از هر Hopیک عدد از این عدد TTL کاسته می شود و زمانیکه این عدد به صفر برسد به این معناست که بسته اطلاعاتی دیگر به مقصد نخواهد رسید و روترهای دیگر به محض دریافت آن بسته، آن را Drop می کنند که این یعنی دیگر Loop ای ایجاد نخواهد شد .کافیست برای درک بهتر دستور Ping را اجرا کنید و به قسمت TTL توجه کنید. اگر این قسمت در پروتکل های مسیریابی در اینترنت وجود نداشت اینترنت پر از بسته های اطلاعاتی می شد که بدون هدف در اینترنت سرگردان می‌شدند.

۲.قابلیت Split Horizon

قابلیتی است که شما می توانید در روترهای خود پیکربندی کنید و مکانیزم کاری آن به ترافیک یا بسته اطلاعاتی که یکبار مسیریابی شده است اجازه بازگشت به همان مسیری که از ان آمده است را نمی دهد . به زبان ساده ،اگر Route ای از شبکه شما خارج شده باشد و مجددا به شبکه شما وارد شود ایجاد Loop می کند این مکانیزم اجازه ورود مجدد بسته اطلاعاتی به درون شبکه شما را نخواهد داد. به زبان فنی اگر یک Neighbor Router یا روتر همسایه یک Route به سمت روتر دیگری ارسال

کند ، روتر دریافت کننده دیگر این Route را به سمت Router ای که از آن دریافت کرده است بازگشت یا Advertiseنمی کند .

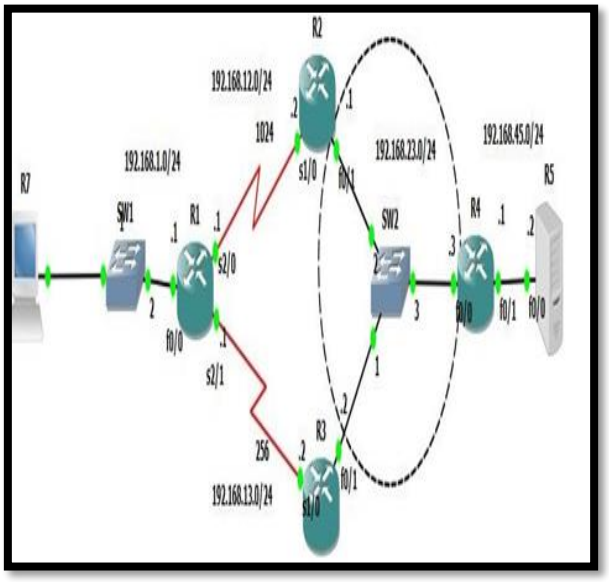
۳. فرآیند Route Poisoning

روشی است که در آن از ارسال شدن Route های Invalid در شبکه جلوگیری می شود. زمانیکه پروتکل مسیریابی به هر دلیلی اعم از قطع شدن لینک یا کابل شبکه تشخیص بدهد که یک route نامعتبر یا Invalid است، به تمامی روترهای شبکه اطلاع رسانی می شود که Route ای که Invalid است دارای **Hop Count**عدد ۱۶ است و این بدین معناست که این Route در شبکه تا ابد باقی خواهند ماند و به محض اینکه روترهای دیگر شبکه در فرآیند **Convergence**این Route را تشخیص دهند، دیگر به این Route چیزی ارسال نمی کنند و از به وجود آمدن Loop جلوگیری می کنند .

۴. مکانیزم Hold-Down Timer

یکی دیگر از مکانیزم هایی است که برای جلوگیری از به وجود آمدن Bad Route ها در شبکه استفاده می شود. زمانیکه یک Route در وضعیت Hold-Down قرار می گیرد روترهای دیگر موجود در شبکه نه به این Route چیزی ارسال می کنند و نه چیزی از آن دریافت می کنند ، این فرآیند تا مدت زمانی طول می کشد که Route به حالت Valid در بیاید یا دوباره وارد مدار شود ، در این حالت به مدت زمانی که Routeدر این وضعیت باقی می ماند Hold-Down گفته می شود که می تواند از به وجود آمدن Loop در شبکه های **Distance Vector**جلوگیری کند.

راه اندازی پروتوکل EIGRP



شکل ۲۹-۳

تنظیمات روتر ۱ :

```
interface Serial۲/۰
 bandwidth ۱۰۲٤
 ip address ۱۹۲,۱٦۸,۱۲,۱ ۲٥٥,۲٥٥,۲٥٥,۰

interface Serial۲/۱
 bandwidth ۲٥٦
 ip address ۱۹۲,۱٦۸,۱۳,۱ ۲٥٥,۲٥٥,۲٥٥,۰

router eigrp ۱
 network ۱۹۲,۱٦۸,۱,۰
 network ۱۹۲,۱٦۸,۱۲,۰
 network ۱۹۲,۱٦۸,۱۳,۰
 no auto-summary
```

```
interface FastEthernet٠/٠
 ip address ١٩٢,١٦٨,١,٢٥٠ ٢٥٥,٢٥٥,٢٥٥,٠
```

```
R١(config)#route-map ccnp permit ١٠

R١(config-route-map)#match ip address ١٠١

R١(config-route-map)#set interface serial ٢/١
```

```
access-list ١٠١ permit ip ١٩٢,١٦٨,١,٠ ٠,٠,٠,٢٥٥ ١٩٢,١٦٨,٤٥,٠ ٠,٠.
٠,٢٥٥

R١(config)#access-list ١٠١ permit ip any any
```

```
R١(config)#int fa ٠/٠

R١(config-if)#ip policy route-map ccnp
```

ip policy **روی اینترفیس ورودی روتر** set **می‌شود**.

تنظیمات روتر ۲

```
interface FastEthernet٠/١
 ip address ١٩٢,١٦٨,٢٣,١ ٢٥٥,٢٥٥,٢٥٥,٠

interface Serial١/٠
 bandwidth ١٠٢٤
 ip address ١٩٢,١٦٨,١٢,٢ ٢٥٥,٢٥٥,٢٥٥,٠
```

```
router eigrp ١
 network ١٩٢,١٦٨,١٢,٠
```

```
 network ۱۹۲,۱٦۸,۲۳,۰
 no auto-summary
```

تنظیمات روتر ۳

```
interface FastEthernet۰/۱
 ip address ۱۹۲,۱٦۸,۲۳,۲ ۲٥٥,۲٥٥,۲٥٥,۰

interface Serial۱/۰
 bandwidth ۲٥٦
 ip address ۱۹۲,۱٦۸,۱۳,۲ ۲٥٥,۲٥٥,۲٥٥,۰

router eigrp ۱
 network ۱۹۲,۱٦۸,۱۳,۰
 network ۱۹۲,۱٦۸,۲۳,۰
 no auto-summary
```

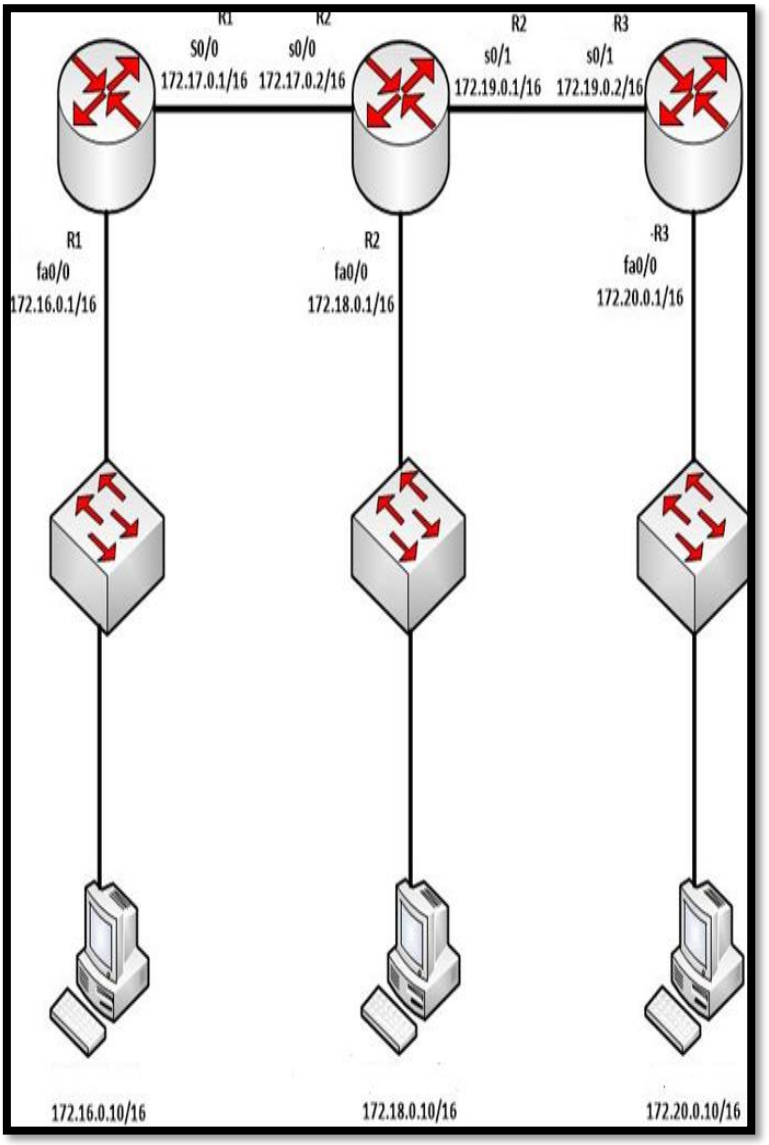
تنظیمات روتر ۴

```
interface FastEthernet۰/۰
 ip address ۱۹۲,۱٦۸,۲۳,۳ ۲٥٥,۲٥٥,۲٥٥,۰


interface FastEthernet۰/۱
 ip address ۱۹۲,۱٦۸,٤٥,۱ ۲٥٥,۲٥٥,۲٥٥,۰

router eigrp ۱
 network ۱۹۲,۱٦۸,۲۳,۰
 network ۱۹۲,۱٦۸,٤٥,۰
 no auto-summary
```

در این سناریو ترافیک network ۱۹۲,۱۶۸,۱,۰ به سمت ۱۹۲,۱۶۸,۴۵,۰ از روتر R۳ R۱ عبور می‌کند.

راه اندازی کامل پروتکل Interior Gateway Routing Protocol یا IGRP

در تصویر زیر شما سه عدد روتر ، سه عدد سوئیچ و سه عدد سیستم Host را مشاهده می کنیم ، آدرس های IP و اسم روترهای استفاده شده در سناریو را به شرح زیر مشاهده می کنید:


R1
S0/0
172.17.0.1/16
R2
s0/0
172.17.0.2/16
R2
s0/1
172.19.0.1/16
R3
s0/1
172.19.0.2/16
R1
fa0/0
172.16.0.1/16
R2
fa0/0
172.18.0.1/16
R3
fa0/0
172.20.0.1/16
172.16.0.10/16
172.18.0.10/16
172.20.0.10/16

شكل ٣٠-٣

انجام تنظیمات IGRP بر روی R۱

به پورت کنسول روتر R۱متصل شوید . برای پیکربندی IGRPبر روی R۱ کلیک کنید. همانطور که در دستورات مشاهده می کنید ما شبکه هایی که بصورت مستقیم یا directly به روتر متصل شده اند را به روتر معرفی می کنیم و ASN مربوطه را نیز در کنار آن قرار می دهیم :

```
۱
۲.R۱>enable
۳.R۱#configure terminal
۴.Enter configuration commands, one per line. End with CNTL/Z.
  R۱(config)# router igrp ۱
۵.R۱(config-router)# network ۱۷۲,۱۶,۰,۰
۶.R۱(config-router)# network ۱۷۲,۱۷,۰,۰
  R۱(config-router)#exit
۷.R۱(config)#exit
۸.R۱#
۹.
```

فراموش نکنید که بعد از وارد کردن دستورات بالا در انتها دستور

copy running-config startup-config

را در enable mode بزنید تا تنظیمات شما روی روتر بصورت دائمی ذخیره شود و بعد از restart شدن روتر تنظیمات از بین نرود .

انجام تنظیمات IGRP بر روی R۲

به پورت کنسول روتر R۲ متصل شوید . برای پیکربندی IGRPبر روی R۲وارد کنید. همانطور که در دستورات مشاهده می کنید ما شبکه هایی که بصورت مستقیم

یا directly به روتر متصل شده اند را به روتر معرفی می کنیم و ASNمربوطه را نیز در کنار آن قرار می دهیم :

```
۱
۲
   R۲>enable
۳  R۲#configure terminal
۴  Enter configuration commands, one per line. End with CNTL/Z.
   R۲(config)# router igrp ۱
۵  R۲(config-router)# network ۱۷۲,۱۷,۰,۰
۶  R۲(config-router)# network ۱۷۲,۱۸,۰,۰
   R۲(config-router)# network ۱۷۲,۱۹,۰,۰
۷  R۲(config-router)#exit
۸  R۲(config)#exit
    R۲#
۹
۱۰
```

فراموش نکنید که بعد از وارد کردن دستورات بالا

در انتها دستور **copy running-config startup-config**

را در **enable mode**بزنید تا تنظیمات شما روی روتر بصورت دائمی ذخیره شود

و بعد از restart شدن روتر تنظیمات از بین نرود .

انجام تنظیمات IGRP بر روی R۳

به پورت کنسول روتر R۳متصل . برای پیکربندی IGRPبر روی R۳وارد کنید. همانطور که در دستورات مشاهده می کنید ما شبکه هایی که بصورت مستقیم به روتر متصل شده اند را به روتر معرفی می کنیم و ASN مربوطه را نیز در کنار آن قرار می‌دهیم :

۱

۲ .R۳>enable

۳.R۳#configure terminal

۴.Enter configuration commands, one per line. End with CNTL/Z.
R۳(config)# router igrp ۱

۵.R۳(config-router)# network ۱۷۲,۱۹,۰,۰

۶.R۳(config-router)# network ۱۷۲,۲۰,۰,۰
R۳(config-router)#exit

۷.R۳(config)#exit

۸.R۳#

۹.

فراموش نکنید که بعد از وارد کردن دستورات بالا در انتها

دستور copy running-config startup-config

را در enable mode بزنید تا تنظیمات شما روی روتر بصورت دائمی ذخیره شود و بعد از restart **شدن روتر تنظیمات از بین نرود .**

مشاهده Routing Table های موجود در R۱

بعد از اینکه شبکه ها به خوبی Converged شدند و تنظیمات Interior Gateway Routing Protocol یا IGRP به درستی انجام شد شما می توانید با استفاده از دستور show ip route در روتر R۱ محتویات Routing Table این روتر را به شکل زیر مشاهده کنید :

```
۱
۲
۳  R۱>enable
   R۱#show ip route
۴  Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B
۵  - BGP
   D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
۶  N۱ - OSPF NSSA external type ۱, N۲ - OSPF NSSA external type
۷  ۲
   E۱ - OSPF external type ۱, E۲ - OSPF external type ۲, E - EGP
۸  i - IS-IS, L۱ - IS-IS level-۱, L۲ - IS-IS level-۲, ia - IS-IS inter area
۹  * - candidate default, U - per-user static route, o - ODR
   P - periodic downloaded static route
۱۰ Gateway of last resort is not set
۱۱ C   ۱۷۲,۱۶,۰,۰/۱۶ is directly connected, FastEthernet۰/۰
   C   ۱۷۲,۱۷,۰,۰/۱۶ is directly connected, Serial۰/۰
۱۲ I   ۱۷۲,۱۸,۰,۰/۱۶ [۱۲۰/۱] via ۱۷۲,۱۷,۰,۲, ۰۰:۰۰:۲۲, Serial۰/۰
۱۳ I   ۱۷۲,۱۹,۰,۰/۱۶ [۱۲۰/۱] via ۱۷۲,۱۷,۰,۲, ۰۰:۰۰:۲۲, Serial۰/۰
   I   ۱۷۲,۲۰,۰,۰/۱۶ [۱۲۰/۲] via ۱۷۲,۱۷,۰,۲, ۰۰:۰۰:۲۲, Serial۰/۰
۱۴
۱۵
```

در خروجی دستور بالا کاراکتر I در خطوطی که Routing Table را نمایش می دهند به معنی این است، که این شبکه با استفاده از پروتکل مسیریابی Interior Gateway Routing Protocol یا IGRP شناسایی شده است و در Routing

Tableقرار گرفته است ، کاراکتر C هم مانند سناریوهای قبلی که انجام دادیم به معنای Connectedیا Directly Connectedبه معنی ارتباط مستقیم با این شبکه می‌باشد .

اطمینان از عملکرد درست و تست ارتباط بین شبکه ها با استفاده از دستور Ping

برای اینکه مطمئن شویم که IGRP ما به درستی کار می کند و ارتباطات بین شبکه ها به درستی برقرار شده است، دستور Ping از Host۰۱ به آدرس شبکه ۱۷۲,۱۶,۰,۱۰/۱۶در شبکه R۱، کامپیوتر Host۰۳ به آدرس ۱۷۲,۲۰,۰,۱۰/۱۶در شبکه R۳را مشابه زیر انجام می دهیم که نتیجه را مشاهده می کنید ، این بدین معناست که IGRPبه درستی پیکربندی شده است:

```
۱
۲
   C:\>ping ۱۷۲,۲۰,۰,۱۰
۳  Pinging ۱۷۲,۲۰,۰,۱۰ with ۳۲ bytes of data:
۴  Reply from ۱۷۲,۲۰,۰,۱۰: bytes=۳۲ time=۱۷۲ms TTL=۱۲۵
   Reply from ۱۷۲,۲۰,۰,۱۰: bytes=۳۲ time=۱۸۸ms TTL=۱۲۵
۵  Reply from ۱۷۲,۲۰,۰,۱۰: bytes=۳۲ time=۱۵۷ms TTL=۱۲۵
۶  Reply from ۱۷۲,۲۰,۰,۱۰: bytes=۳۲ time=۱۸۸ms TTL=۱۲۵
   Ping statistics for ۱۷۲,۲۰,۰,۱۰:
۷  Packets: Sent = ٤, Received = ٤, Lost = ۰ (۰٪ loss),
۸  Approximate round trip times in milli-seconds:
   Minimum = ۱۵۷ms, Maximum = ۱۸۸ms, Average = ۱۷٦ms
۹
۱۰
```

همانطور که مشاهده کردید پیاده سازی پروتکل مسیریابی IGRPچندان هم دشوار نبود و براحتی پیاده سازی شد ، تست Ping هم نشان داد که شبکه به درستی پیکربندی شده است و ارتباط بین همه این شبکه ها برقرار شده است ،

ترجمه آدرس ها یا Address Translation

ترجمه آدرس ها یا Address Translation در ابتدا به دو منظور مورد استفاده قرار می گرفت. یکی جبران کمبود آدرس های IP و دیگری مخفی سازی پیکربندی کلی شبکه یا Scheme.

به دلیل رشد فزاینده اینترنت در اوایل دهه ۹۰، قابل پیش بینی بود که سیستم آدرس دهی موجود برای تخصیص آدرس های عمومی یا public کافی به تمامی دستگاههای متصل به شبکه اینترنت با مشکل مواجه خواهد شد. سرانجام راه حل جامعی برای این مشکل پیشنهاد و تائید گردید که به نام IPV6 خوانده می شود، که در فصول قبل به شرح آن پرداختم. اما مشکلی که در این بین وجود دارد این است که هنوز برای تبدیل شدن IPv6 به عنوان یک استاندارد عمومی در محیط اینترنت زمان باقی است و حتی ISPها به عنوان یکی از اجزای ستون فقرات شبکه و بسیاری از شرکت های بزرگ هنوز از IPv4 استفاده می نمایند. یکی از دلایل مهمی که باعث ماندگاری IPv4 شده است، دو خصوصیت عمده آن می باشد: استفاده از آدرس های خصوصی در شبکه های LAN یا Private address و دیگری قابلیت تبدیل این آدرس ها به آدرس های عمومی یا public در محیط اینترنت.

انواع سیستم ترجمه آدرس ها

برای سیستم ترجمه آدرس انواع مختلفی جود دارد که شامل موارد زیر است :

- NAT
- PAT
- ترجمه آدرس ها به صورت دینامیک
- ترجمه آدرس-ها به صورت استاتیک

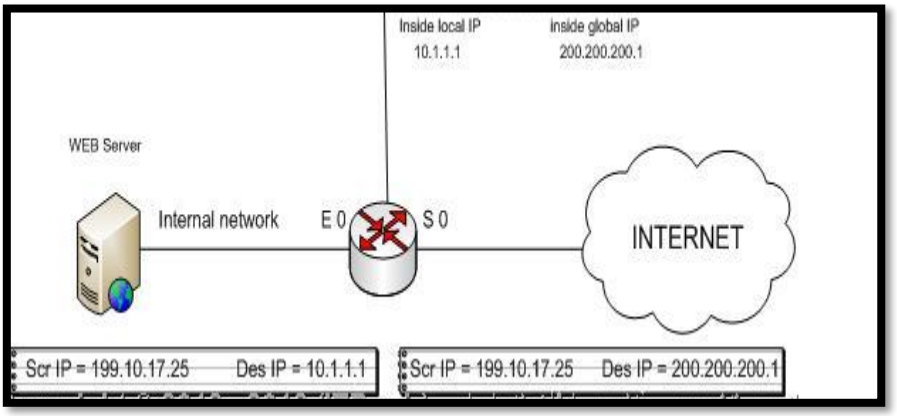
NATیاNetwork Address Translation

NAT عمل ترجمه یک آدرس IP به آدرسی دیگر را انجام می دهد. آدرس مربوطه می تواند هم آدرس گیرنده و هم آدرس فرستنده باشد. همچنین NAT نیز به دو نوع می تواند انجام گیرد :استاتیک و دینامیک

NATاستاتیک یاStatic NAT

در این نوع، عمل ترجمه آدرس از یک آدرس به دیگری به صورت دستی در روی دستگاه مربوطه تنظیم می شود. عموما NAT استاتیک عمل ترجمه آدرس های گیرنده موجود در داخل بسته هایی که وارد شبکه می شوند را انجام خواهد داد.اما می توان آدرس های فرستنده را نیز به وسیله آن ترجمه نمود.شکل زیر مثال ساده ای را نشان می دهد که کاربران خارجی می خواهند به یک سرور داخلی شبکه دسترسی داشته باشند. اما این سرور دارای یک آدرس از نوع آدرس های خصوصی یا Private به صورت ۱۰,۰,۰,۱ است. این مسئله کاربران خارجی را دچار مشکل می نماید. زیرا که اگر آدرس ۱۰,۰,۰,۱ را به عنوان آدرس گیرنده پیام در داخل بسته های ارسالی قرار دهند، روترهای میانی، پیام فوق را فیلتر خواهند نمود. بنابراین کاربران بیرونی قادر به برقراری تماس با سرور داخلی شبکه نخواهند بود. بنابراین باید آدرس دهی

سرور را طوری انجام دهیم که از دید کاربران خارجی، این سرور دارای یک آدرس publicیا عمومی باشد. این وظیفه فوق را دستگاه مسئول که در اینجا یک دستگاه روتر سیسکو می باشد انجام خواهد داد .



شکل ۳۱-۳

سرور داخلی موجود در شبکه دارای آدرس ۲۰۰,۲۰۰,۲۰۰,۱ می باشد که یک آدرس **Inside Global** آدرس عمومی یا public اختصاص یافته به یک دستگاه موجود در شبکه داخلی بوده و همین آدرس توسط سرور DNSبه کاربران خارجی نمایش داده می شود. وقتی کاربران خارجی اطلاعاتی را با آدرس گیرنده ۲۰۰,۲۰۰,۲۰,۱ به شبکه داخلی می فرستند، روتر با دریافت این پیام آدرس گیرنده پیام را بررسی کرده و در داخل جدولی که حاوی آدرس های ترجمه شده می باشد دنبال یک آدرس متناظر با آن می گردد. در این مثال معادل آدرس ۲۰۰,۲۰۰,۲۰۰,۱ را آدرس ۱۰,۱,۱,۱ تشکیل می دهد. در مرحله بعدی، روتر آدرس گیرنده پیام را از ۲۰۰,۲۰۰,۲۰۰,۱به آدرس ۱۰,۱,۱,۱تغیر داده و سپس پیام را به سوی

سرور ارسال می کند. اما در صورتیکه هیچ متناظری برای آدرس در داخل جدول یافت نشود، روتر مقصد پیام را تشخیص نخواهد داد. همچنین اگر سرور داخلی قصد ارسال اطلاعاتی را به اینترنت داشته باشد، آدرس فرستنده پیام که یک آدرس خصوصی یا Private می باشد توسط روتر به یک آدرس عمومی یا Public ترجمه شده و سپس به محیط اینترنت فرستاده می شود .

NATدینامیک یاDynamic NAT

اگر در شبکه ای از NAT استاتیک استفاده می کنیم، باید به صورت دستی جدول حاوی آدرس های دستگاه‌ها و نیز آدرس-های متناظر آن ها را نیز ایجاد نمائیم.اگر برای مثال شبکه ما دارای ۱۰۰۰ عدد دستگاه باشد برای هر یک از این دستگاه‌ها باید به طور جداگانه آدرس های متناظر را در داخل جدول ایجاد نموده که کار زیادی را می طلبد. معمولا این نوع NAT هنگامیکه که کاربران خارجی می خواهند به دستگاههای داخلی اتصال داشته باشند به کار می رود. اما عموما وقتی که کاربران داخلی اقدام به دسترسی به محیط اینترنت می کنند، از نوع دینامیک بهره می بریم.در این شرایط آدرس IP کاربران داخلی برای کاربران خارجی اهمیت خاصی ندارد. زیرا آن ها مستقیما با دستگاههای داخلی در تماس نبوده و فقط ترافیکی را به شبکه داخلی ارسال می کنند که کاربران داخلی آن را درخواست کرده باشند. در NATدینامیک، دو دسته از آدرس ها را باید به صورت دستی مشخص نمائیم. یک دسته را برای مشخص کردن دستگاههایی که از NAT استفاده خواهند کرد و دیگری تعیین کردن آدرس هایی است که آدرس های داخلی به آن آدرس ها ترجمه خواهند شد. هنگامیکه یک دستگاه داخلی ترافیکی را به محیط بیرونی از طریق یک دستگاه روتر ارسال می کند، روتر آدرس فرستنده پیام را با لیست آدرس های

Inside Local آدرس private تخصیص یافته به دستگاه موجود در شبکه داخلی خود مقایسه کرده و در صورتی‌که مشابه آن را یافت، آدرس متناظری را از بین آدرس های Inside Globalخود که به دستگاههای دیگر اختصاص نداده، انتخاب کرده و سپس پیام را به کاربران خارجی ارسال خواهد کرد. اما در صورتیکه آدرس مشابه آدرس فرستنده در داخل جدول **Inside global** وجود نداشت، این پیام ترجمه نشده و به صورت دست نخورده به محیط اینترنت ارسال خواهد شد. به همین ترتیب هنگامیکه ترافیکی از بیرون وارد شبکه داخلی می شود، روتر آدرس گیرنده را بررسی کرده و دوباره به دنبال یافتن آدرس متناظری برای آن می گردد تا آدرس گیرنده موجود در داخل پیام رسیده را که یک آدرس عمومی یا Public می باشد، به یک آدرس خصوصی یا Private ترجمه نماید. در واقع در این شرایط عمل ترجمه آدرس Inside globalبه آدرس Inside Local انجام می‌شود .

Port Address TranslationیاPAT

یکی از محدودیت‌های موجود در NAT این است که در این سیستم عمل تبدیل یک آدرس به یک آدرس دیگر انجام می‌شود. بنابراین اگر در شبکه ای تعداد ۵۰۰۰ دستگاه داشته باشیم که هرکدام دارای یک آدرس خصوصی یا Private مخصوص به خود باشند، باید ۵۰۰۰ عدد آدرس عمومی یا Public نیز در اختیار داشته باشیم تا همه دستگاه‌های داخلی در صورتیکه بخواهند هم‌زمان به اینترنت متصل گردند، آدرس کافی برای ترجمه آدرس های آن ها وجود داشته باشد.اما اگر فقط ۱۰۰۰ عدد آدرس عمومی در اختیار داشته باشیم، فقط ۱۰۰۰ دستگاه اول قادر به دسترسی به اینترنت بوده و ۴۰۰۰ دستگاه باقی مانده توانایی اینکار را نخواهند داشت. در این مواقع از پروسه ای به نام **Address Overloading**برای حل این مشکل استفاده می گردد که شامل مباحث **PAT**و **NPAT**می شوند. در

صورت کمبود آدرس های عمومی یا Public که در اختیار ما قرار گرفته است، می توان با استفاده از PAT همین آدرس را به دستگاههای مختلف شبکه بطور همزمان اختصاص داد. بدین صورت که یک آدرس عمومی یا Publicرا در جدول Network Translation معادل تمامی دستگاههای شبکه (که دارای آدرس های خصوصی مخصوص به خود هستند) قرار می دهیم؛ با این تفاوت که هر یک از آن ها از شماره پورت جداگانه ای استفاده خواهند کرد.اگر دو دستگاه دارای شماره پورت فرستنده یکسانی باشند، روتر شماره یکی از آن ها را بطور اتوماتیک تغییر خواهد داد .

به طور کلی جدول **Translation** حاوی موارد زیر می باشد:

- آدرس **inside local** آدرس خصوصی یا private مربوط به دستگاه داخلی
- شماره پورت **inside local** شماره پورت مربوط به دستگاه داخلیآدرس **inside global**یک آدرس عمومی یا public که آدرس خصوصی دستگاه داخلی به آن ترجمه می شود
- شماره پورت **inside global** شماره پورت آدرس جدید
- آدرس **outside global** آدرس عمومی مربوط به گیرنده پیام
- شماره پورت **outside global** شماره پورت مربوط به گیرنده پیام

راه اندازی NAT وPAT

دو نوع مختلف از NAT وجود دارد : استاتیک و دینامیک.مراحلی که برای ایجاد این دو نوع بکار می روند، شبیه هم می باشند. شاید یکی از سخت ترین مراحل پیکربندی NATدرک دو کلمه Inside و outside می باشد. این دو کلمه به محل قرار گرفتن دستگاه‌ها اشاره می کند. جایی که دستگاههای داخلی شما قرار دارند به مفهوم inside

و جایی که دستگاه‌های خارجی یا اینترنت قرار دارند، outsideمی نامیم. در هنگام پیکربندی NAT به دو چیز باید توجه کنیم :

- **مشخص نمودن نوع سیستم ترجمه آدرس ها**
- **مشخص نمودن محل قرارگیری دستگاهها**

در مواقعی که کاربران خارجی به دستگاههای داخلی مثل سرورهایDNS ، WEBو یا کاربران داخلی متصل می شوند، از NAT استاتیک استفاده می کنیم.دستورات بکار رفته به شکل زیر است:

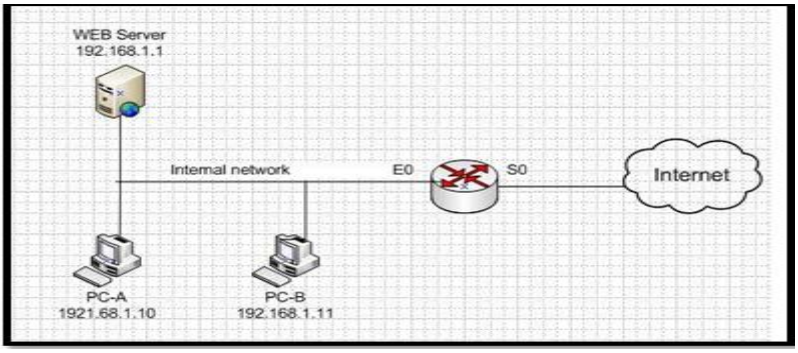
پارامترهای Inside و outside مسیری را که باید عمل ترجمه صورت گیرد را نشان می دهد. برای مثال کلمه inside به این معنی است که یک آدرس inside source localبه یک آدرس inside global ترجمه می شود. کلمه outside نیز نشان دهنده این است که یک آدرس outside destination global به یک آدرس outside localترجمه می گردد. بعد از این مرحله نیز بایدinterface های داخلی یا inside و خارجی یا outside را تعیین نماییم. به صورت زیر :

```
۱Router (config)#Interface type [slot_# / ] port_#
۲Router (config-if)#ip nat inside | outside
```

پارامتر inside را در روی interface متصل به LAN و پارامتر outside را در روی interfaceمتصل به اینترنت بکار می بریم. برای آشنایی بیشتر با NAT استاتیک به مثالی که در شکل زیر آورده شده توجه کنید. در این مثال یک آدرس globalبرابر با ۲۰۰,۲۰۰,۲۰۰,۱ به سرور WEB داخلی با آدرس ۱۰,۱,۱,۱ تخصیص یافته است. پیکربندی مربوطه به شکل زیر خواهد بود :

```
Router (config)#ip nat inside source static ١٩٢,١٦٨,١,١ ٢٠٠,٢٠٠,٢٠٠,١
Router (config)#interface ethernet ٠
Router (config-if)#ip nat inside
Router (config-if)#exit
Router (config)#interface serial ٠
Router (config)#ip nat outside
```

دستور ip nat inside source static عمل ترجمه آدرس را فعال می کند .عبارات ip nat inside **و** ip nat outside **نیز مشخص می کنند که کدام** interface **به اینترنت (S٠) و کدام** interface **به** LAN **داخلی (S١) متصل می باشد. به یاد داشته باشید که هر ترافیکی که با قانونهای تعیین شده مطابقت نداشته باشد، بین این دو اینترفیس منتقل گردند، باید از** ACL **برای اینکار استفاده نماییم .**



شکل ٣٢-٣

برای استفاده از NAT **دینامیک باید اقدام به مشخص نمودن سه چیز بکنیم :**

- **لیست آدرس های داخلی که باید روی آن ها عمل ترجمه صورت بگیرد.**
- **لیست آدرس های خارجی که آدرس های داخلی باید به آن ها ترجمه شوند.**

- **اینترفیس هایی که باید در عمل ترجمه آدرس ها دخالت نمایند.**

برای رسیدن به هدف اول، یعنی تعیین کردن دستگاههایی که آدرس آن ها باید ترجمه شود.دستورات زیر را باید نوشت:

```
۱Router(config)#ip nat inside source list standard_IP_ACL_# pool
NAT_pool_name
```

بعد از دستور ip nat inside source list **باید شماره** ACL **حاوی لیست دستگاه‌های مجاز را بیاوریم. در مورد آدرس‌هایی که در لیست** ACL **دارای پارامتر** permit**می باشند، عمل ترجمه یا** address translation **صورت گرفته ولی در مورد آدرس هایی که با پارامتر** deny **مشخص شده اند و یا بوسیله** implicit deny **حذف می شوند، عمل ترجمه صورت نمی گیرد. سپس بعد از پارامتر** pool **باید اسمی را به این** Range **آدرس تخصیص دهیم. هدف دومی که در بالا نیز گفته شد، تعیین کردن** Range **آدرس‌های عمومی یا** public **است که آدرس های داخلی به آن ها ترجمه می شوند . دستورات زیر را برای تعیین کردن** Range **آدرس های عمومی بکار می‌بریم:**

```
۱Router(config)#ip nat pool NAT_pool_name
۲begining_inside_global_IP_address
۳ending_inside_global_IP_address
٤netmask subnet_mask_of_address
```

بعد از دستور ip nat pool **اسمی را که در دستور اول به** pool **تخصیص داده بودیم نوشته و سپس آدرس شروع و پایانی، به همراه ساب نت ماسک مربوطه را نیز باید مشخص نمود.آخرین هدف ما تعیین کردن اینترفیس های دخیل در عمل ترجمه می باشد. یعنی باید مشخص کنید که کدام اینترفیس به اینترنت و کدام اینترفیس به** LAN**متصل است.برای مثال می توان به مورد اشاره شده در مثال قبل اشاره کرد .**

در این مثال در مورد دو کامپیوتر A و B عمل NAT دینامیک صورت گرفته است. پیکربندی مربوطه چنین خواهد بود :

```
Router(config)#ip nat inside source list ۱ pool ITPro
Router(config)#access-list ۱ permit ۱۹۲,۱۶۸,۱,۱۰ ۰,۰,۰,۰
Router(config)#access list ۱ permit ۱۹۲,۱۶۸,۱,۱۱ ۰,۰,۰,۰
Router(config)#ip nat pool ITPro ۲۰۰,۲۰۰,۲۰۰,۰ ۲۰۰,۲۰۰,۲۰۰,۳
netmask ۲۵۵,۲۵۵,۲۵۵,۰
Router(config)#interface ethernet۰
Router(config-if)#ip nat inside
Router(config-if)#exit
Router(config)#interface serial۰
Router(config-if)#ip nat outside
```

مراحل پیکربندی PAT شبیه به NAT دینامیک بوده و سه مرحله را برای انجام کار باید طی نمود. اولین مرحله مشخص کردن لیست دستگاه‌هایی است که عمل ترجمه روی آن ها انجام خواهد شد. دستوری که برای اینکار استفاده می شود شبیه دستوری است که در NAT دینامیک هم مورد استفاده قرار گرفت. اما در آخر دستور کلمه Overload را هم باید اضافه نمود که نشان دهنده این است که به جای NAT از PATاستفاده می کنیم :

```
Router(config)# ip nat source list standard_IP_ACL_#
pool NAT_pool_name Overload
```

در مرحله دوم لیست آدرس‌های global مورد نیاز را باید مشخص نمود. دستور بکار برده شده در اینجا نیز مثل دستوری است که در NAT دینامیک نیز استفاده شد :

```
Router(config)#ip nat pool NAT_pool_name
begining_inside_global_IP_address
ending_inside_global_IP_address
netmask subnet_mask_of_address
```

مرحله آخر تعیین کردنinterface هایی است که در عمل ترجمه شرکت خواهند نمود .دستورات مورد استفاده نیز به صورت ip nat inside و ip nat outside است که به ترتیب نشان دهند interface داخلی و خارجی می باشند. برای درک مسئله (در مثال قبل) فقط یک آدرس در داخل گروه آدرس های global به صورت ۲۰۰,۲۰۰,۲۰۰,۰ قرار دارد :

```
۱ Router(config)# ip nat inside source list ۱ pool ITPro overload
۲ Router(config)#access-list ۱ permit ۱۹۲,۱۶۸,۱,۱۰ ۰,۰,۰,۰
۳ Router(config)#access-list ۱ permit ۱۹۲,۱۶۸,۱,۱۱ ۰,۰,۰,۰
٤ Router(config)#ip nat pool ITPro ۲۰۰,۲۰۰,۲۰۰,۲۰
٥ ۲۰۰,۲۰۰,۲۰۰,۲ net mask ۲٥٥,۲٥٥,۲٥٥,۰
٦ Router(config)#interface ethernet۰
۷ Router(config)#ip nat inside
۸ Router(config)#exit
۹ Router(config)#interface serial ۰
  Router(config)#ip nat outside
```

کاربردTelnet یا دسترسی از راه دور

وقتی برای اولین بار می‌خواهیم دستگاهی را پیکربندی کنیم (روتر یا سوئیچ) ابتدا از طریق کابل کنسول به دستگاه متصل شده و اقدام به پیکربندی دستگاه می نمائیم. اما برای دفعات بعد دیگر نیازی به حضور فیزیکی در کنار دستگاه نداریم و می‌توانیم از راه دور به وسیله telnet به دستگاه متصل شده و کارهای مورد نظر را انجام دهیم.(مثلا تغییرات در پیکربندی). تنهادر یک مورد است که نیاز به حضور فیزیکی در هر شرایطی و همراه داشتن کابل کنسول است و آن برای مواقعی است که پسورد دستگاه تحت هر شرایطی (فراموشی یا ...) نیاز به بازگردانی (recovery) دارد. سوئیچ ۲۹۵۰ تعداد ۱۶ ارتباط همزمان telnet را پشتیبانی می کند که هر یک از این ارتباطات را با شماره ۰ تا ۱۶ نام گذاری می‌کنیم (Vty ۰ ۱۵) .

سه روش برای برقراری telnet به سمت دستگاه‌های دیگر وجود دارد که می توان از هریک از آن ها برای برقراری ارتباط telnet استفاده نمود. این دستورات به شرح زیراست:

```
Router# name_of_the_destination | destination_IP_address
Router# telnet name_of_the_destination | destination_IP_address
Router#connect name_of_the_destination | destination_IP_address
```

در این سه روش، هم می توان نام و آدرس دستگاه مقابل را به تنهایی تایپ کرد و یا اینکه این اطلاعات را بعد از دستورات telnet و یا connect آورد. در هر حال همه دستورات فوق یک عمل را انجام می دهند : برقراری ارتباط **telnet** با یک دستگاه دیگر .

معوق کردن ارتباطات Telnet

در مواقعی که دستگاه را به قصد کاری موقتا ترک می کنیم، ارتباط telnet برقرار شده را باید قطع نماییم. این کار را می توان به دو صورت انجام داد : یکی قطع کامل ارتباط و برقراری دوباره آن در صورت لزوم و دیگری قطع موقت ارتباط . اگر برای مدت کوتاهی دستگاه را ترک می کنیم، استفاده از روش دوم که به اصطلاح **suspend**نامیده می شود بهتر از روش اول می باشد. زیرا که مجددا مجبور به استفاده از logon شدن از طریق telnet نخواهیم بود. برای این منظور، ترکیب کلیدهای **Ctrl+Shift+**٦و یا بسته به نوع صفحه کلیدی که استفاده می کنیم، **Ctrl+**٨را بکار خواهیم برد. در روی دستگاه منبع، می توان به وسیله دستور **Show Session**ارتباط‌هایی را که به حالت suspend قرار گرفته اند، مشاهده نمود:

```
Router# show session
Conn Host Address  Byte  Idle  Conn Name
 1 10.1.1.1 10.1.1.1    0     1     10.1.1.1
* 2 10.1.1.2 10.1.1.2    0     2     10.1.1.2
```

در این مثال، دو ارتباط telnet **در روی دستگاه مشاهده می‌شود و ارتباطی که با " * " مشخص شده است، ارتباط آخر را نشان می‌دهد. برای فعال کردن آخرین ارتباط معوق شده، باید در خط فرمان کلید** Enter **را فشار دهیم. اما برای فعال کردن یک ارتباط بخصوص، دستور زیر را بکار خواهیم گرفت :**

```
Router# resume connection_
```

شماره ارتباط، همان شماره ای است که در ستون Conn **خروجی دستور** Show session **نشان داده می شود. در روی دستگاه مبدا می توان بدون فعال کردن یک ارتباط** telnet**، اقدام به قطع آن نمود. دستور زیر را به همین منظور بکار می بریم :**

```
Router# disconnect connection_#
```

در تمامی روترها و نیز سوئیچ ۲۹۵۰ می توان با استفاده از دستور زیر لیست کاربرانی که در این دستگاه login **شده اند را مشاهده نمود .**

```
1
Router# show users
  Line User Host(s) Idle Location
 0 con 0 idle
 2 vty 0 idle 0 10.1.1.1
* 3 vty 1 idle 0 10.1.1.2
5
```

ارتباط آخر و یا ارتباط فعال، آن ارتباطی است که در خروجی دستور با علامت * "

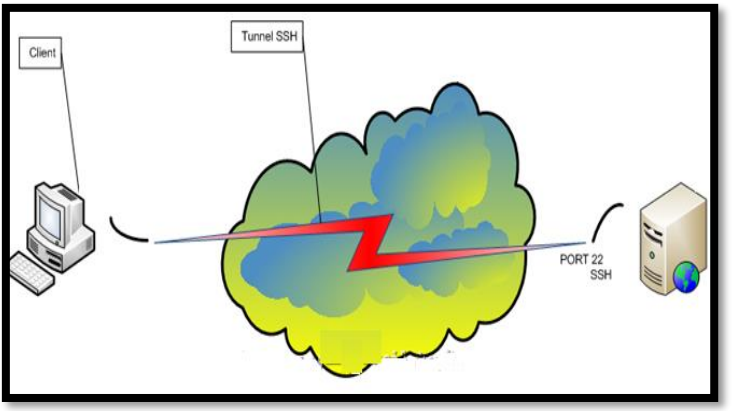
"مشخص گردیده است.اگر مایل به قطع ارتباط یک کاربر می‌باشید در mode Privilege دستور زیر را تایپ نمایید :

۱ Router# clear line line_#

شماره Line همان شماره ای است که در ستون Line دستور show user نشان داده شده است.

راه اندازی SSH

telnetکه برای ارتباط با تجهیزات از راه دور به صورت خط فرمان است استفاده می شود، یک مشکل امنیتی بزرگ دارد و ان ارسال اطلاعات بین کاربر و دستگاه به صورت رمز نشده یا همان Clear Text است در صورتیکه یک نفر بسته های ارسالی بین کاربر و دستگاه را Sniffکند به راحتی می تواند محتوای بسته را ببیند و به اطلاعات آن دسترسی پیدا کند برای جلوگیری از این مشکل باید از پروتکل SSH استفاده شود .



شکل ۳۳-۳

SSH یک پروتکل برای ایجاد دسترسی به تجهیزات از راه دور به صورت امن می باشد در تمام نسخه های SSH اطلاعات به صورت رمز شده ارسال می شوند SSH. دارای دو نسخه ۱ و ۲ می باشد که نسخه دوم از الگوریتم رمزنگاری بهینه تری استفاده می کند.

- نکته: برای استفاده از SSH روی روتر ها و سوئیچ ها باید نسخه سیستم عامل دستگاه از این قابلیت پشتیبانی کند که در صورت وجود عبارت K۹ در نام سیستم عامل (IOS) دستگاه این قابلیت را می‌توان استفاده کرد به طور مثال c۳۷۵۰e-universalk۹-tar.۱۲۲-۳۵.SE۵.tar یک نسخه با قابلیت استفاده از SSHمی‌باشد.

نحو ه ی فعال سازی

در ابتدا یک نام غیر از نام پیش فرض باید برای روتر یا سوئیچ در نظر بگیریم با استفاده از دستور زیر :

```
۱Router(config)#host-name R۱
```

سپس باید یک نام دامین برای دستگاه در نظر بگیریم به صورت زیر :

```
۱R۱(config)#ip domain-name itpro.ir
```

حالا باید یک کلید برای SSH ایجاد کنیم به صورت زیر :

```
۱R۱(config)#crypto key generate rsa
```

حالا باید در line vty انرا فعال کنیم:

```
۱R۱(config)#line vty ۰ ٤
۲R۱(config-line)#transport input ssh
```

تغییر نسخه مورد استفاده SSH

- نکته : برای تغییر به نسخه ۲ باید کلید تولید شده حداقل ۷۶۸ بیت باشد.

```
۱R۱(config)#ip ssh version ۲
```

برای مشاهده اتصالات و تظیمات مربوط به SSH از دستورات زیر استفاده می کنیم :

```
۱  R۱#show ssh
۲R۱#show ip ssh
```

راه اندازی DHCP

به روتر یا سوئیچ متصل می شویم ومراحل زیر را دنبال می کنیم:

روی یکی از interface های روتر یک IP استاتیک تعریف می‌کنیم و بعد interfaceرا up می‌کنیم :

```
۱Router(config)# interface ethernet۰/۰
۲Router(config-if)#ip address ۱,۱,۱,۱ ۲۵۵,۰,۰,۰
۳Router(config-if)# no shutdown
```

اکنون یک address pool تعریف می‌کنیم :

```
۱Router(config)# ip dhcp pool mypool
```

subnet mask مربوط به Range IP مورد نظر را در ادامه وارد می‌کنیم ، روتر این Range رو به درخواست هایی که به روتر می‌رسد اختصاص می‌دهد:

```
۱Router(dhcp-config)# network ۱,۱,۱,۰ /۸
```

نام دامنه یا دامین را به DHCP سرور معرفی می‌کنیم :

```
۱Router(dhcp-config)#domain-name Modir.ir
```

آدرس Primary و Secondary مربوط به DNS سرور را هم به روتر معرفی می-کنیم :

```
۱Router(dhcp-config)#dns-server ۱,۱,۱,۱۰ ۱,۱,۱,۱۱
```

آدرس روتر یا Default Gateway **را در مرحله بعد اضافه می‌کنیم :**

```
Router(dhcp-config)#default-router ۱,۱,۱,۱
```

زمان Lease **یا** Lease Duration **را هم اضافه می‌کنیم :**

```
Router(dhcp-config)#lease ۷
```

از حالت configuration mode **خارج می‌شویم :**

```
Router(dhcp-config)#exit
```

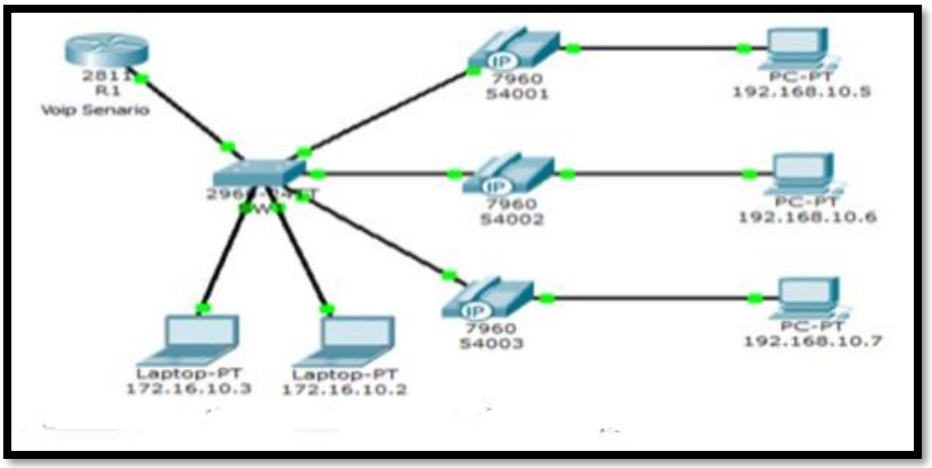
با این دستور مجددا به حالت global configuration **وارد شده و می‌توان آدرس هایی را که مد نظر است،** exclude **نمود .در این حالت وقتی** DHCP **سرور می خواهد آدرس دهی کند، از این** Range **، برای** classnet **ها استفاده نمی کند و ما می توانیم به عنوان استاتیک** IP **برای سرور ها ی خود از این** Range **استفاده نماییم.**

با دستور زیر ۱۰۰ تا آدرس اول رنج IP **رو** exclude **میکنیم .**

```
Router(config)#ip dhcp excluded-address ۱,۱,۱,۰ ۱,۱,۱,۱۰۰
```

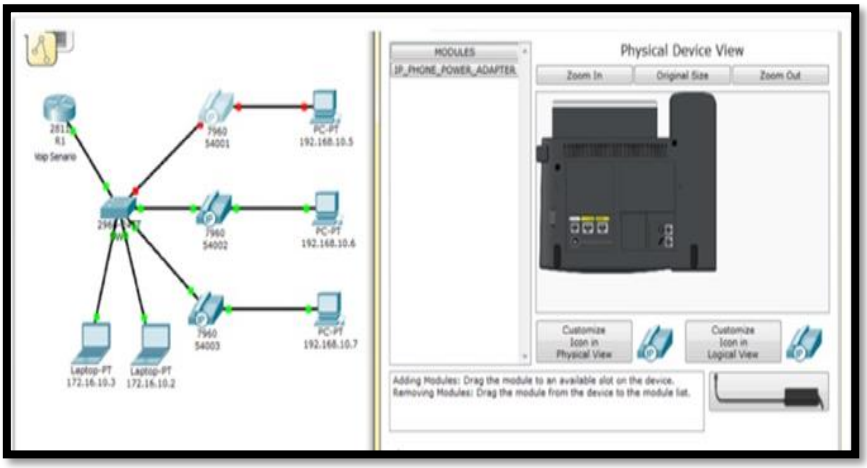
اکنون، تنظیمات کامل شده است و می‌توان به راحتی با استفاده از دستور ipconfig /renew**آدرس** IP **کلاینت رو مجددا از** DHCP **درخواست کنید .**

راه اندازی VOIP

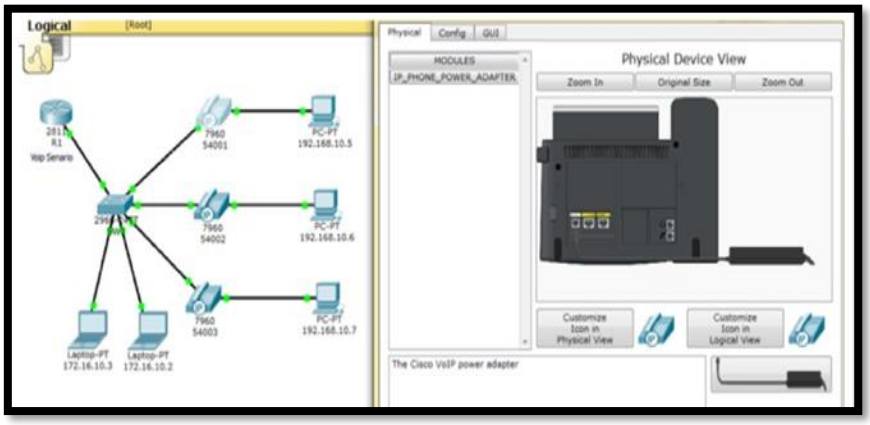


شکل ۳۴-۳

در این سناریو راه اندازی Voip در Packet Tracer را انجام می‌دهیم . برای راه اندازی این سناریو از یک عدد روتر ۲۸۱۱ و یک سوییچ ۲۹۶۰ و سه عدد IP Phoneو ۵ عدد کامپیوتر استفاده می‌کنیم .در این سناریو از دو Range ipاستفاده شده که نمایانگر دو شبکه مجزا در سوییچ است که همزمان به درستی عمل می‌کند و از DHCP استفاده شده است. ابتدا ارتباطات بین سوییچ و تلفن ها و ...برقرار کرده به صورت شکل بالا و سپس بر روی تلفن‌ها کلیک می‌کنیم.



شکل ۳۵-۳



شکل ۳۶-۳

پس از آن به پیکربندی سوییچ می‌پردازیم . ابتدا پورتی که متصل به روتر است را به حالت Trunk **تغییر می‌دهیم تا ترافیک بین** vlan **ها را انتقال بدهد مانند دستور زیر :**

```
SW۱(config)#interface fastEthernet ۰/۱
SW۱(config-if)#switchport mode trunk
```

سپس باید پورت‌هایی که به تلفن متصل است به یک vlan **و لپ تاپ‌ها را به** vlan **دیگری اختصاص بدهیم که در این سناریو برای** Voip **از** vlan ۱ **استفاده شده است و برای شبکه ۱۷۲,۱۶,۱۰,۰ که برای لپ تاپ ها است از** vlan ۱۰ **استفاده شده است . برای ساخت** vlan **مطابق دستور زیر عمل می‌کنیم :**

```
SW۱(config)#vlan ۱۰
SW۱(config-vlan)#name DATA
```

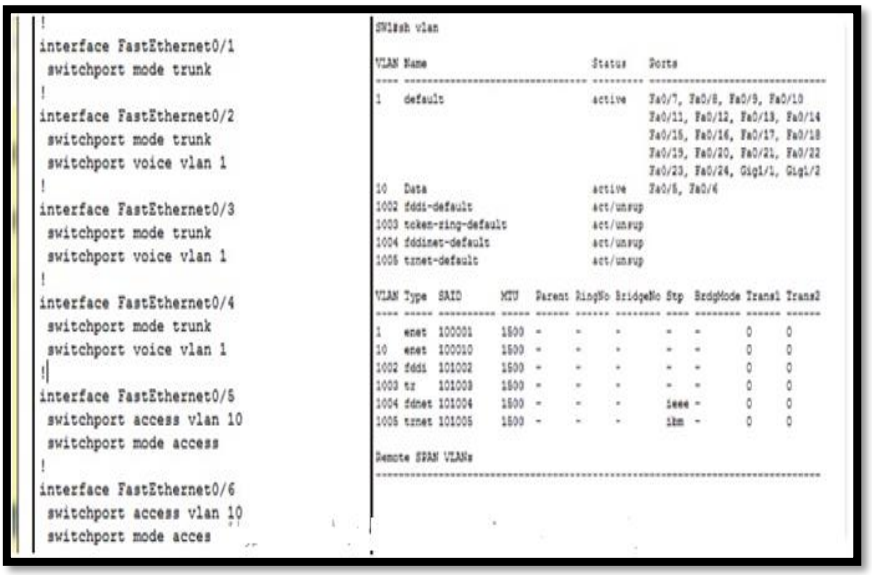
پورت ۵ و ۶ سوییچ متصل به لپ تاپ‌ها است و با دستور زیر این پورت ها را به vlan ۱۰ **اختصاص می‌دهیم:**

```
SW۱(config)#in ra fa ۰/۵-٦
SW۱(config-if-range)#switchport mode access
SW۱(config-if-range)#switchport access vlan ۱۰
```

پس از این کار باید پورت‌هایی که به تلفن ها متصل است را به حالت Trunk **تغییر داده و سپس دسترسی** voice **رو در** Vlan ۱ **فعال کنیم مانند دستور زیر :**

```
SW۱(config)#in ra fa ۰/۲-٤
SW۱(config-if-range)#switchport mode trunk
SW۱(config-if-range)#switchport voice vlan ۱
```

با این کار ما توانستیم ترافیک بین تلفن و کامپیوتر های موجود در شبکه ۱۹۲,۱۶۸,۱۰,۰را جدا کنیم و در پایان کلیه تنظیمات اعمال شده را بررسی می‌کنیم.



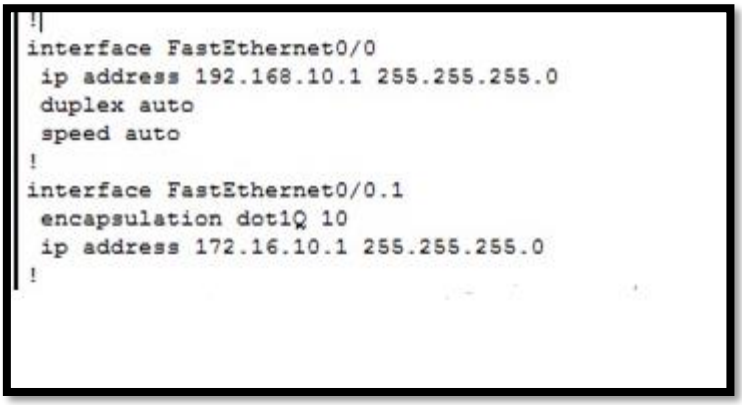
شکل ۳-۳۷

حال به پیکر بندی روتر می‌پردازیم ابتدا باید اینترفیس متصل به سوییچ را IP بدهیم که در این سناریو از ۱۹۲,۱۶۸,۱۰,۱ استفاده شده است که برای شبکه ۱۹۲,۱۶۸,۱۰,۰نقش gateway را ایفا می‌کند مانند دستورات زیر:

R۱#conf t
R۱(config)#interface fastEthernet ۰/۰
R۱(config-if)#ip address ۱۹۲,۱۶۸,۱۰,۱ ۲۵۵,۲۵۵,۲۵۵,۰
R۱(config-if)#no Shutdown

سپس باید یک gateway دیگر برای شبکه ۱۷۲,۱۶,۱۰,۰ ایجاد کنیم که در این سناریو از اینترفیس مجازی استفاده کرده ایم مانند دستورات زیر :

R۱(config)#interface fastEthernet ۰/۰,۱
R۱(config-subif)#encapsulation dot۱Q ۱۰
R۱(config-subif)#ip address ۱۷۲,۱۶,۱۰,۱ ۲۵۵,۲۵۵,۲۵۵,۰
R۱(config-subif)#no shutdown



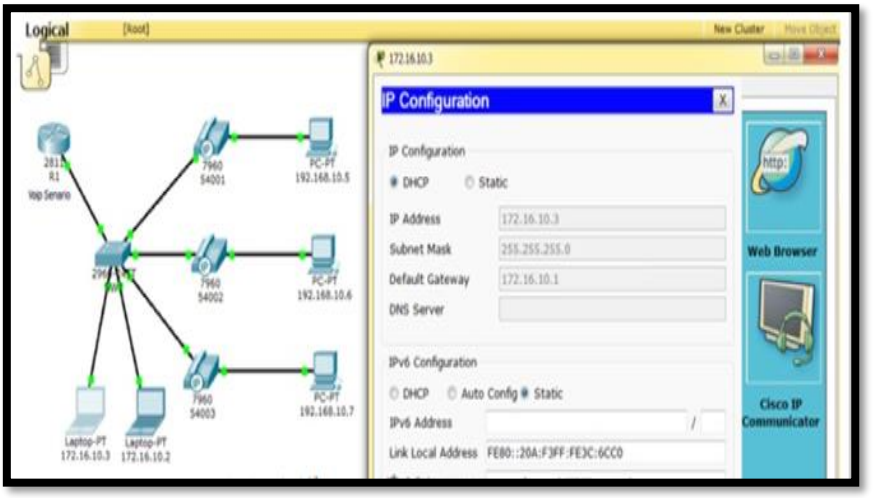
شکل ۳۸-۳

برای این سناریو دو DHCP Pool **در نظر گرفته ایم اولی با عنوان** Voice **جهت تلفن‌ها و کامپیوتر های متصل به شبکه ۱۹۲,۱۶۸,۱۰,۰ و دیگری با عنوان** Data **برای لپ تاپ‌های متصل به شبکه ۱۷۲,۱۶,۱۰,۰ مانند شکل زیر:**

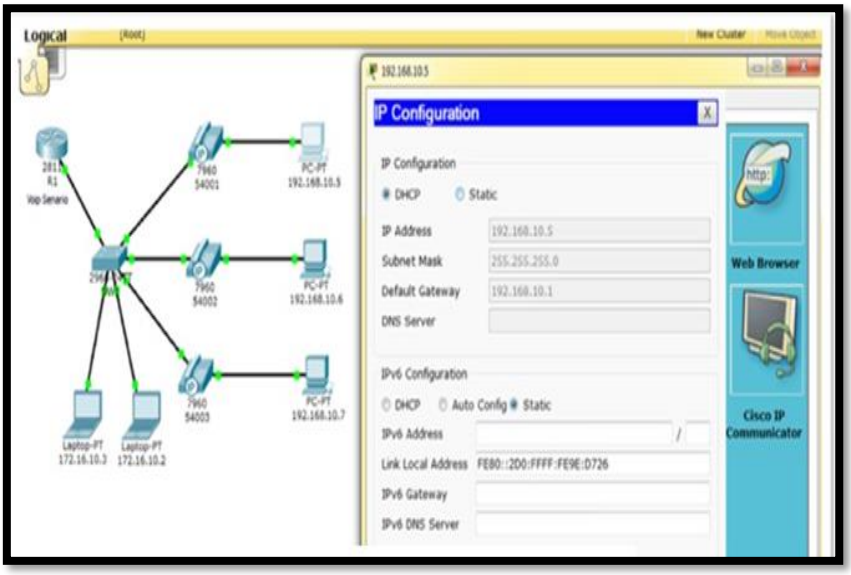
```
hostname R1
!
!
!
!
!
ip dhcp pool Voice
 network 192.168.10.0 255.255.255.0
 default-router 192.168.10.1
 option 150 ip 192.168.10.1
ip dhcp pool Data
 network 172.16.10.0 255.255.255.0
 default-router 172.16.10.1
 option 150 ip 172.16.10.1
!
!
```

شکل ۳۹-۳

پس از این کار به سراغ سیستم‌ها می‌رویم و بررسی می‌کنیم که از DHCP می توانند IP بگیرند یا خیر مانند تصویر زیر:



شکل ۴۰-۳



شکل ۴۱-۳

همانطور که در تصاویر مشخص است کلیه ارتباط برقرار است و هم چنین DHCP هم به درستی عمل می‌کند حال نوبت به تنظیمات تلفن ها است که برای این کار مراحل زیر را دنبال کنید:

ابتدا باید سرویس تلفن را در روتر فعال کنیم که با دستور زیر انجام می‌شود:

```
R۱(config)#telephony-service
R۱(config-telephony)#max-Ephones ٥
R۱(config-telephony)#max-dn ٥
R۱(config-telephony)#ip source-address ۱۹۲,۱٦۸,۱۰,۱ port ۲۰۰۰
R۱(config-telephony)#auto assign ٤ to ٦
R۱(config-telephony)#auto assign ۱ to ٥
R۱(config-telephony)#exi
```

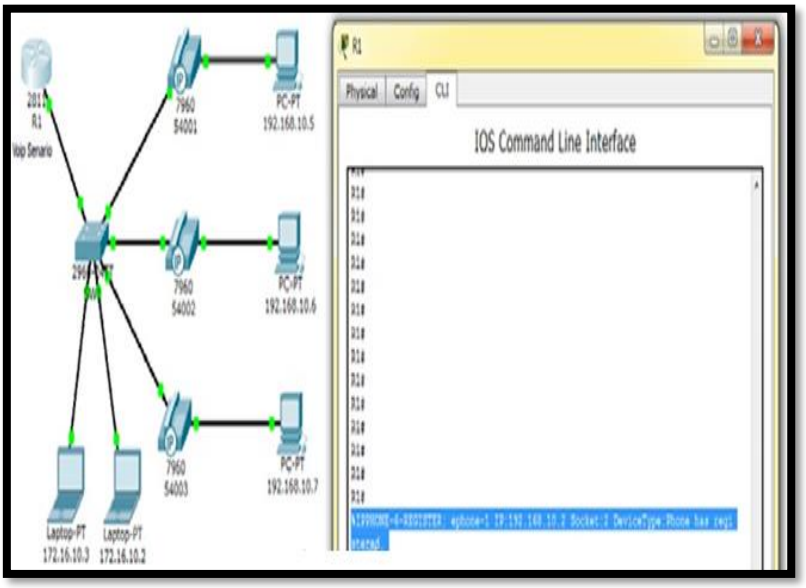
سرویس تلفن را برای ۵ عدد تلفن فعال کردیم و حالا نوبت به شماره دادن به تلفن ها است که طبق دستورات زیر انجام می‌دهیم :

R١(config)#ephone-dn ١
R١(config-ephone-dn)#number ٥٤٠٠١
R١(config-ephone-dn)#exit

شماره تلفن ۵۴۰۰۱ به اولین تلفن که در شبکه Register **شده اختصاص یافت حال باید برای دو تلفن دیگر نیز شماره اختصاص بدهیم :**

R١(config)#ephone-dn ٢
R١(config-ephone-dn)#number ٥٤٠٠٢
R١(config-ephone-dn)#exit
R١(config)#ephone-dn ٣
R١(config-ephone-dn)#number ٥٤٠٠٣
R١(config-ephone-dn)#exit

کلیه تنظیمات تلفن‌ها و سرویس تلفنی هم انجام شد و پس از گذشت چند ثانیه باید تلفن‌ها در روتر رجیستر شوند مانند تصویر زیر :



شکل ۴۲-۳

حال برای تلفن زدن کافی است که روی یک تلفن کلیک کرده و به Gui رفته و روی گوشی کلیک کنید و سپس شروع به شماره گیری نمایید بطور مثال ۵۴۰۰۲ را از تلفن ۵۴۰۰۱ شماره گیری نماییم مانند تصویر زیر:

شکل ۳-۴۳

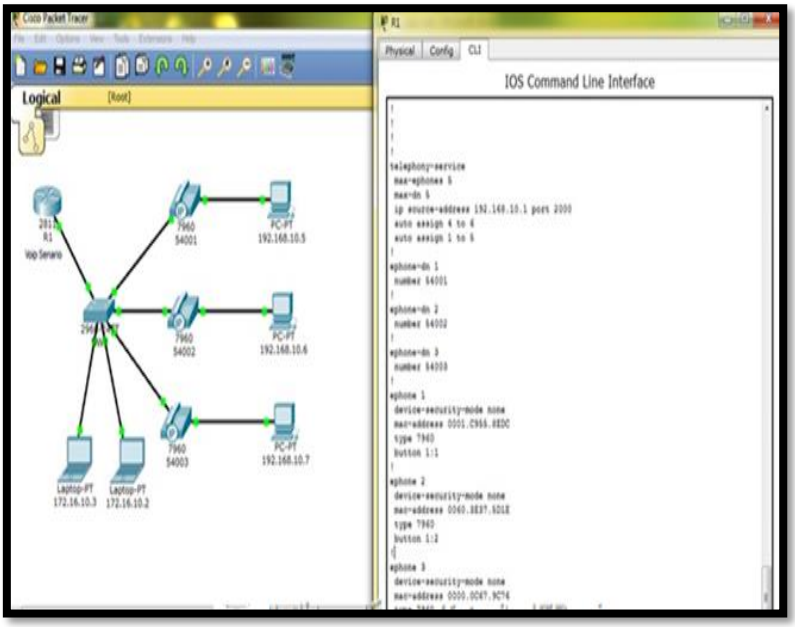
در اینجا مشاهده می کنید که تلفن ۵۴۰۰۲ یک تماس دریافتی از ۵۴۰۰۱ دارد که با کلیک بر روی گوشی ارتباط برقرار می شود و روی مانیتور نمایش داده می شود مانند تصویر زیر:

شکل ۴۴-۳

و پس از قطع کردن ارتباط تلفنی بصورت شکل زیر نشان داده می شود:

شکل ۴۵-۳

پس از رجیستر شدن تلفن ها Macaddress **آن ها بر روی روتر ذخیره می گردد مانند تصویر زیر:**

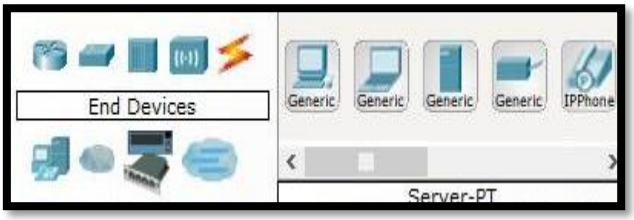


شکل ۴۶-۳

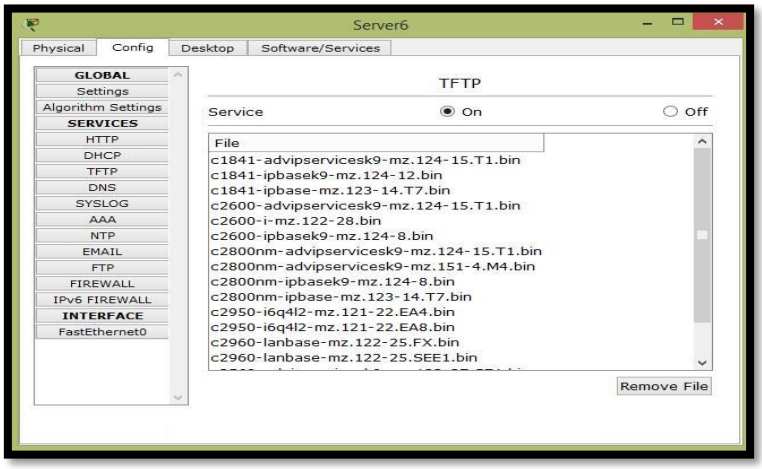
راه اندازی TFTP سرور

برای انجام اینکار لازم است، مراحل زیر را دنبال کنید :

۱. **از قسمت پایین** Packet Tracer **گزینه** End Devices **را انتخاب کنید**
۲. **از قسمت** Generic **گزینه** Server-PT **را انتخاب کنید و آنرا به داخل** Packet Tracer**بکشید.**
۳. **بر روی آن** Double Click **کنید و تنظیمات آدرس** IP **آنرا انجام دهید.**
۴. **به قسمت** Config **بروید و مطمئن شوید که قسمت** TFTP **روی** On **قرار دارد**
۵. **اکنون** TFTP **سرور شما آماده کار در** Packet Tracer **شما است و لیست یک سری از** IOS **ها نیز در** TFTP **قرار دارد.**



شکل ۳-۴۷



شکل ۳-۴۸

منابع

مردانی،علی(۱۳۹۳)، اصول و مفاهیم اولیه ی شبکه های کامپیوتری ، تهران، نشر نیبگ

http://network.itpro.ir.

http://ciscopersian.blogsky.com/۱۳۹۲/۰٦/۲۰/post-۲٤/Policy-routing#ixzz۳wolkjkea.

http://www.irstu.com.

Todd Lammle. CCNA Cisco Certified Network Associate Study Guide, ۷th EditionISBN: ۹۷۸-۰-٤۷۰-۹۰۱۰۷-٦, April ۲۰۱۱.

Jesin A.Packet tracer Network Simulator. BIxMINGHAM – MUMBAI.January,۲۰۱٤

www.aprarat.com.

http://reza.ramezani.student.um.ac.ir

Help نرم افزار Packet Tracer