مولف

دکتر رضا حسین‌زاده

فهرست مطالب

عنوان
صفحه

فصل 12: مباحث تکميلی

فصل 13: سناريوهای تکميلی

فصل 1

مبانی پایه شبکه

شبکه

- اتصال داخلی[1] دو یا چندین دستگاه را شبکه می‌نامند.
- ارتباط بین دو یا چندین دستگاه بهم پیوسته را networking می‌گویند.
- اتصال دو یا چندین شبکه را internework می‌نامند.
- Internetworking به معنی ارتباط بین شبکه‌های مختلف می‌باشد.

توپولوژی شبکه

نحوه‌ی قرارگیری کامپیوترها در شبکه را توپولوژی می‌نامند.

انواع مختلف توپولوژی‌های شبکه عبارتند از:

1. **توپولوژی گذرگاه**[2]
2. **توپولوژی حلقه ای**[3]
3. **توپولوژی ستاره ای**[4]
4. **توپولوژی مش**[5]
5. **توپولوژی ترکیبی**[6]

توپولوژی گذرگاه

نوعی توپولوژی است که هر دستگاه به یک کابل منفرد و یا backbone متصل می‌شود.

[1] interconnection
[2] Bus Topology
[3] Ring Topology
[4] Star Topology
[5] Mesh Topology
[6] Hybrid Topology

شکل 1- 1 نمایی از
توپولوژی گذرگاه

ویژگی‌ها

- داده را فقط در یک مسیر انتقال می‌دهد.
- ارتباط نیمه دوطرفه[1] را پشتیبانی می‌کند.
- هر دستگاه به یک کابل منفرد متصل می‌شود.

مزایا

- مقرون به صرفه است.
- در مقایسه با توپولوژی های دیگر، حداقل کابل مورد نیاز است.
- در شبکه‌های کوچک استفاده می‌شود.
- یادگیری آن آسان است.
- گسترش الحاق دو کابل به یکدیگر آسان است.

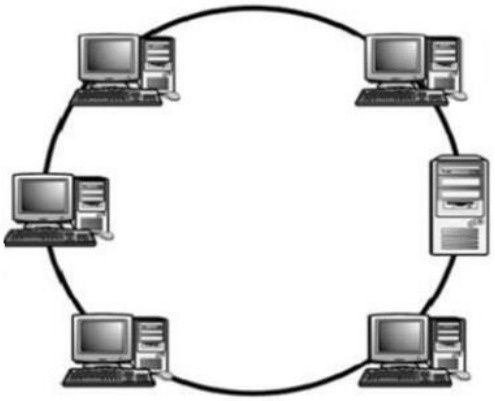
معایب

- در صورت خرابی کابل، کل شبکه خراب می‌شود.
- اگر ترافیک شبکه سنگین باشد یا گره‌های بیشتری وجود داشته باشد، کارایی شبکه کاهش پیدا می‌کند.
- کابل طول محدودی دارد.
- نسبت به توپولوژی حلقه ای کند می‌باشد.

توپولوژی حلقه‌ای

به این دلیل توپولوژی حلقه‌ای نامیده شده است که با اتصال هر کامپیوتر به کامپیوتر دیگر یک حلقه ایجاد می‌شود. در این توپولوژی هر دستگاه دقیقا دو همسایه دارد.

[1] Half Duplex



شکل 1-2 نمایی از توپولوژی حلقه‌ای

ویژگی‌ها

- از تعدادی تکرار کننده با تعداد زیادی گره در این توپولوژی استفاده می‌شود، زیرا وقتی داده‌ای بخواهد به آخرین گره با تعداد 100 گره ارسال شود باید داده از 99 گره عبور کند تا به 100 امین گره برسد. از این‌رو برای جلوگیری از گم شدن داده باید تکرار کننده در شبکه استفاده شود.
- انتقال یک‌سویه است اما با ایجاد 2 اتصال بین هر گره شبکه می توان انتقال دوسویه را به‌وجود آورد که در این حالت توپولوژی حلقه‌ای دوتایی[1] می‌نامند.
- داده به شیوه‌ای ترتیبی به صورت بیت به بیت انتقال داده می‌شوند.
- ارسال داده به‌صورت broadcast می‌باشد.

مزایا

- انتقال دهی در شبکه با ترافیک شبکه یا افزودن گره‌های زیاد تحت تاثیر قرار نمی‌گیرد، فقط گره‌های دارای توکن می‌توانند داده را انتقال دهند.
- برای نصب و گسترش آسان است.

معایب

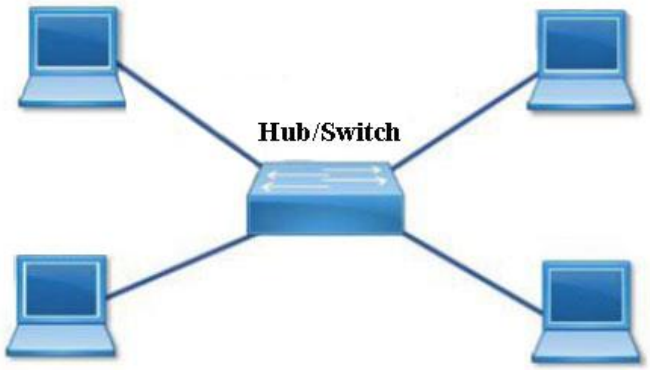
- عیب‌یابی در توپولوژی حلقه‌ای مشکل است.
- اضافه یا حذف کامپیوتر موجب اختلال در فعالیت شبکه می‌شود.

[1] Dual Ring Topology

- خرابی یک دستگاه یا یک شکست در نقطه‌ای از کابل منجر به متوقف شدن ارتباط در کل شبکه می‌شود.

توپولوژی ستاره‌ای

این توپولوژی شامل یک دستگاه متمرکز (مرکزی) همانند سوئیچ یا هاب می‌باشد که همه‌ی دستگاه‌ها به پورت‌های مختلف روی این دستگاه مرکزی متصل می‌شوند.



شکل 1-3 نمایی از توپولوژی ستاره‌ای

ویژگی‌ها

- رایج‌ترین توپولوژی مورد استفاده است.
- دستگاه مرکزی به عنوان تکرارکننده برای جریان داده عمل می‌کند.
- می‌تواند با کابل زوج بهم تابیده، کواکسیال یا فیبر نوری استفاده شود.
- ارسال داده به صورت unicast می باشد.

مزایا

- کارایی بالا با تعداد گره کمتر و ترافیک پایین شبکه
- دستگاه مرکزی به راحتی می‌تواند آپدیت شود.
- عیب‌یابی این توپولوژی آسان است.
- تنظیم و اصلاح این توپولوژی آسان است.
- فقط گرهی تحت تاثیر قرار می‌گیرد که خراب شده است، بقیه‌ی گره‌ها به راحتی می‌توانند به کار خود ادامه دهند.

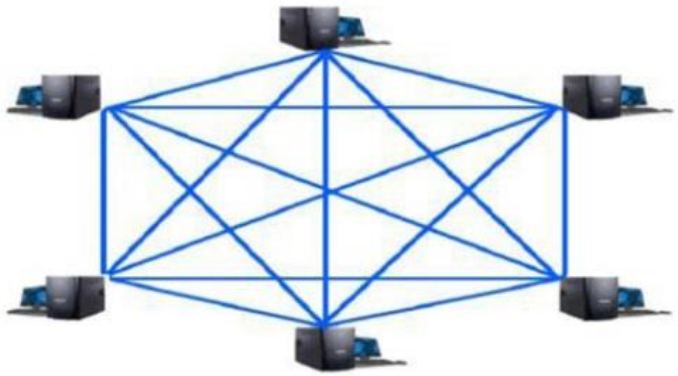
معایب

- هزینه‌ی نصب بالاست.
- برای استفاده گران است.

- اگر دستگاه مرکزی خراب شود، کل شبکه متوقف می‌شود زیرا همه‌ی گره‌ها وابسته به دستگاه مرکزی می‌باشند.

توپولوژی مش

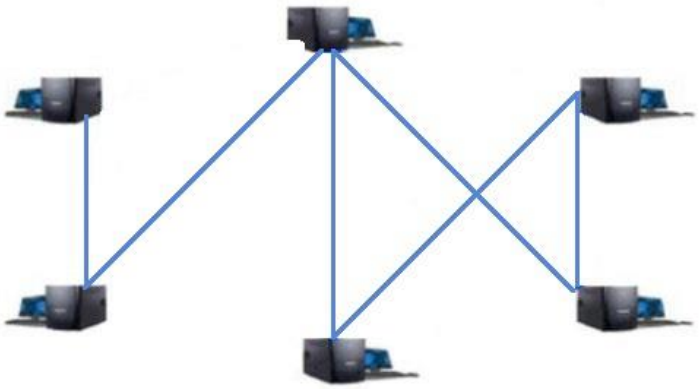
این نوع توپولوژی یک اتصال point-to-point به گره‌ها یا دستگاه‌های دیگر می‌باشد. همه ی گره‌های شبکه به همدیگر به‌صورت مستقیم متصل می‌شوند.



شکل 1-4 نمایی از توپولوژی مش

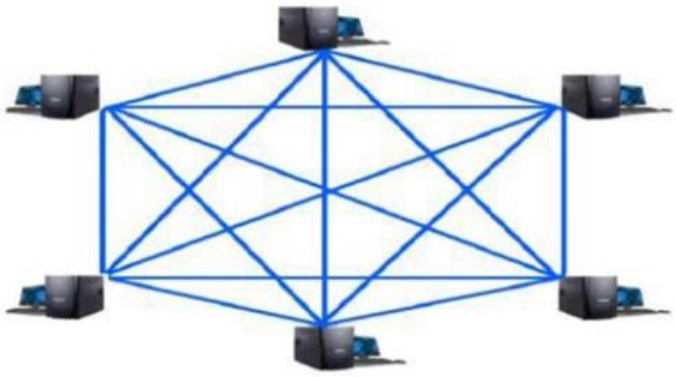
انواع توپولوژی مش

1. **Partial Mesh:** در این توپولوژی ساختار مش رعایت می‌شود اما همه‌ی دستگاه‌ها به همدیگر متصل نمی‌شوند.



شکل 1-5 نمایی از توپولوژی Partial Mesh

2. **Full Mesh:** در این توپولوژی همه‌ی دستگاه‌ها یا گره‌ها به همدیگر متصل می‌شوند.



شکل 1-6 نمایی از توپولوژی
Full Mesh

ویژگی توپولوژی مش

- اتصال کامل
- مقاوم
- غیرقابل انعطاف‌پذیر

مزایا

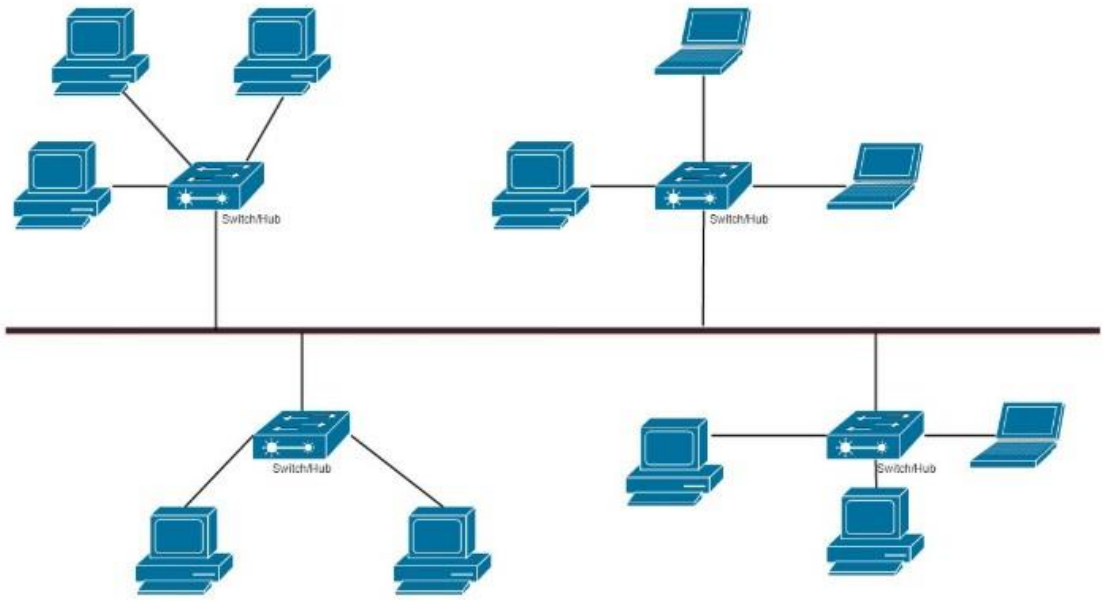
- مقاوم است.
- خطا به راحتی تشخیص داده می‌شود.
- امنیت را فراهم می‌کند.
- هر اتصالی می‌تواند بار داده‌های خود را حمل کند.

معایب

- نصب و پیکربندی در این توپولوژی سخت است.
- هزینه‌ی کابل بندی زیاد است.

توپولوژی ترکیبی

این توپولوژی، ترکیبی از دو یا چند توپولوژی می‌باشد. برای مثال اگر یک اداره در یک ساختمان از توپولوژی گذرگاه و دیگری از توپولوژی ستاره‌ای استفاده کند، اتصال این توپولوژی‌ها منجر به توپولوژی ترکیبی خواهد شد.



شکل 1-7 نمایی از

ویژگی‌ها

- ترکیبی از دو یا چند توپولوژی می‌باشد.
- مزایا و معایب توپولوژی‌های مشمول را به ارث می‌برد.

مزایا

- کارا
- انعطاف‌پذیر
- مقیاس پذیر
- قابل اعتماد

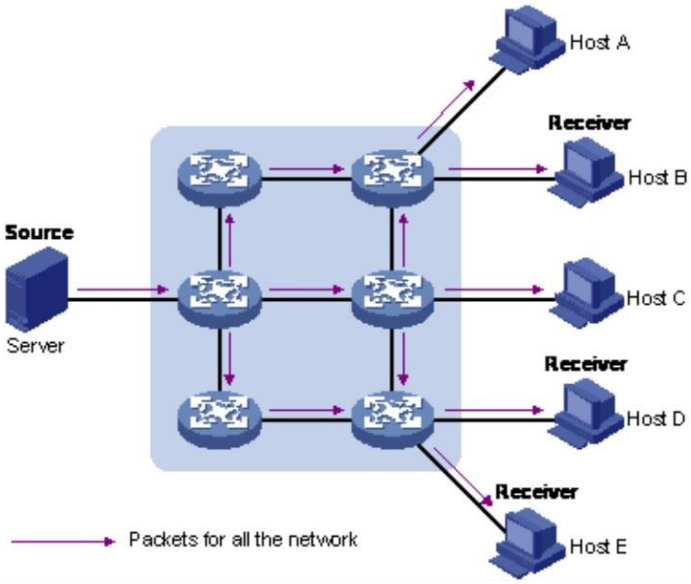
معایب

- پیچیدگی طراحی
- پرهزینه

انواع ارسال داده در شبکه

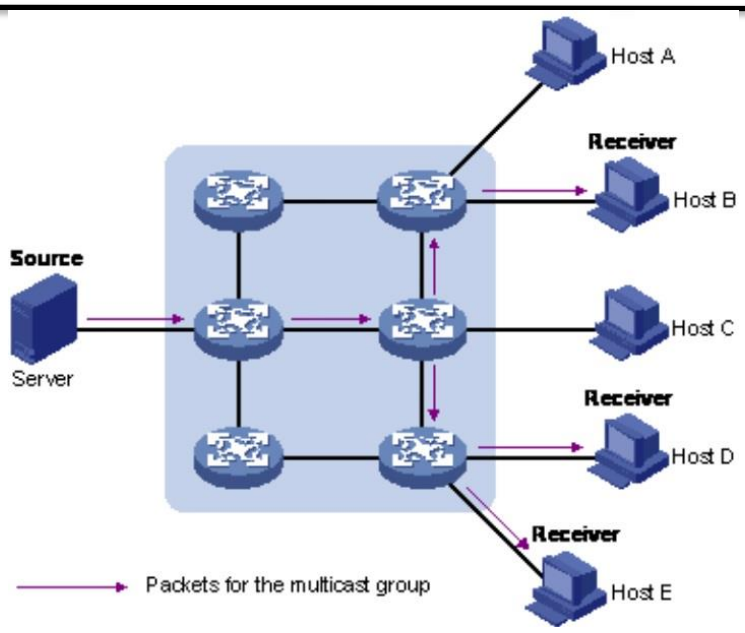
روش‌های ارسال داده در شبکه‌ها به 3 صورت زیر می‌باشد:

- **Broadcast:** ارسال داده‌ها به‌صورت همزمان،به‌طوریکه تمام اجزای شبکه بتوانند داده را دریافت بکنند.



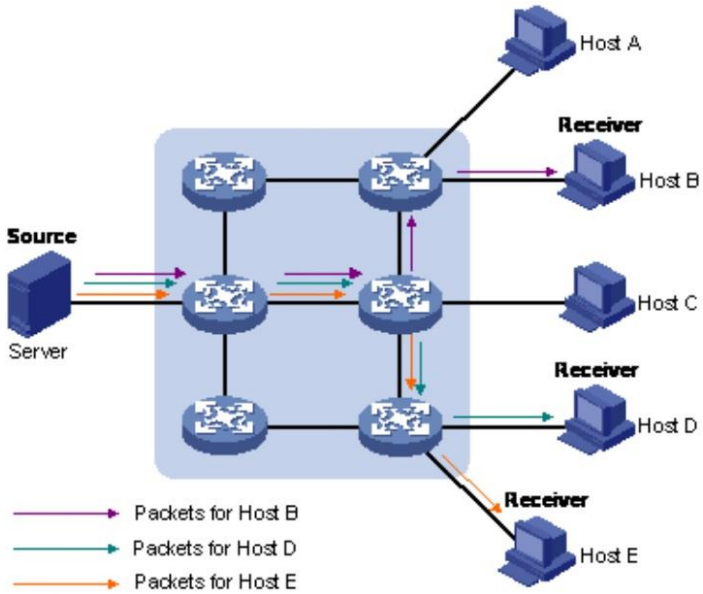
شکل 1-8 ارسال داده به صورت Broadcast

- **Multicast:** ارسال داده‌ها به یک گروه خاص از بین تمام اجزای شبکه



شکل 1-9 ارسال داده به‌صورت Multicast

- **Unicast:** ارسال داده‌ها به یک سیستم خاص از بین تمامی اجزای شبکه



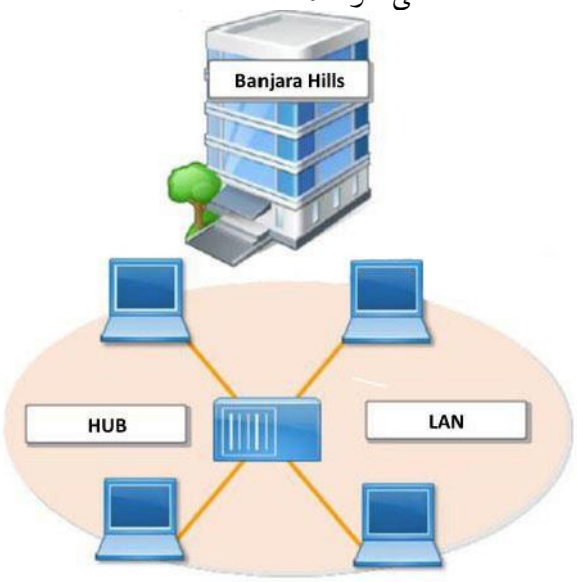
شکل 1-10 ارسال داده به‌صورت Unicast

هر چقدر از Broadcast به سمت Unicast حرکت کنیم، ترافیک شبکه کمتر و کیفیت سرویس دهی در شبکه افزایش پیدا می‌کند.

انواع شبکه از جهت ابعاد

شبکه‌ها از لحاظ موقعیت جغرافیایی به 3 دسته زیر تقسیم می‌گردند:

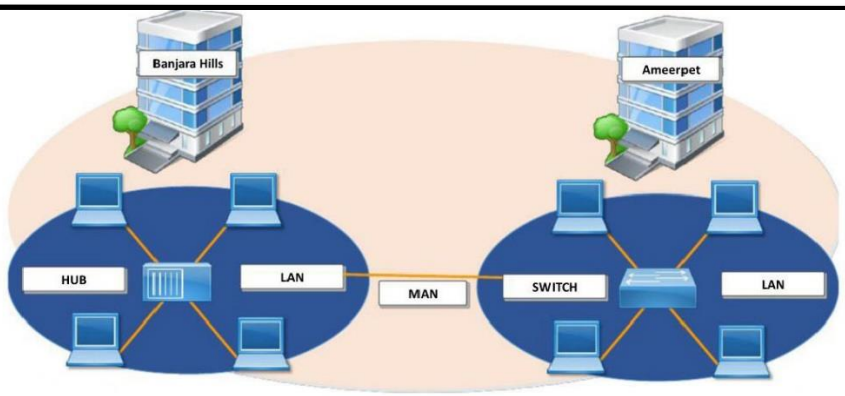
- **LAN**[1]: نوعی شبکه کامپیوتری است که دو یا چندین دستگاه درون یک اتاق، یک طبقه از یک ساختمان یا نهایتا یک ساختمان به صورت کامل را بهم متصل می‌کند. در این شبکه‌ها، سوئیچ یا هاب حتما وجود دارد ولی لزوما همیشه روتر وجود ندارد، در مواقعی که نیاز به اتصال به شبکه‌های دیگر باشد یا درگاه جدیدی ایجاد شود از روتر استفاده می‌شود.



شکل 1-11 شبکه LAN

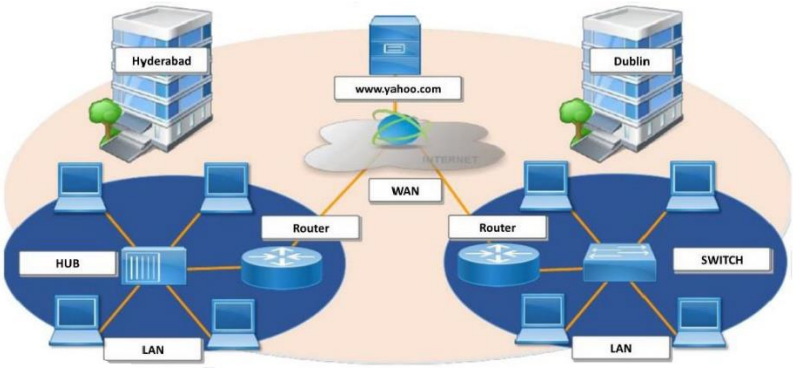
- **MAN**[2]: یک نوع شبکه‌ی کامپیوتری است که کاربران با منابع شبکه را در یک موقعیت جغرافیایی بزگتر نسبت به LAN بهم متصل می‌کند (در حد شهر، استان، کشور). این نوع شبکه دارای موقعیت جغرافیایی کوچکتری نسبت به WAN می باشد.

[1] Local Area Network
[2] Metropolitan Area Network



شکل 1-12 شبکه MAN

- **WAN**[1]**:** دو یا چندین LAN موجود در موقعیت‌های جغرافیایی مختلف را بهم متصل می‌کند، در واقع از بهم پیوستن تمامی شبکه‌های مخابراتی در تمام دنیا به‌وجود آمده است. مثل: اینترنت



شکل 1-13 شبکه WAN

مدل‌های شبکه

انواع مدل‌های شبکه عبارتند از:

- **مدل نظیر به نظیر**[2]

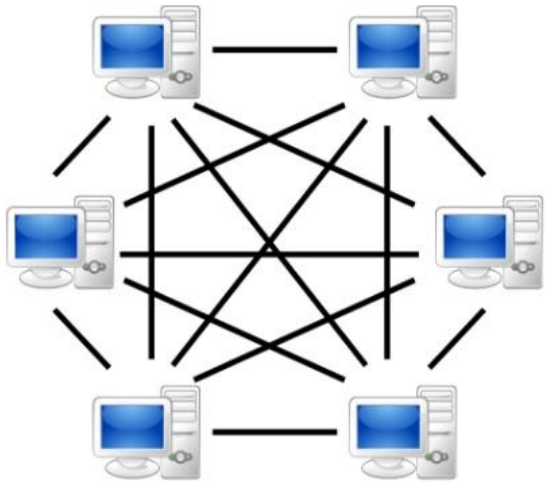
[1] Wide Area Network
[2] Peer-to-Peer

- **مدل کلاینت/سرور**

مدل نظیر به نظیر

شبکه نظیر به نظیر زمانی ایجاد می‌شود که دو یا چندین کامپیوتر بدون اینکه از یک سرور کامپیوتری جداگانه استفاده کنند، بهم متصل شوند و یا منابع خود را به اشتراک بگذارند. از این شبکه‌ها به‌عنوان شبکه‌های Workgroup هم یاد می شود. ویژگی‌های این مدل عبارتند از:

- نصب و پیکربندی کامپیوتر در این شبکه آسان است.
- قابل اعتمادتر است، وابستگی مرکزی از میان رفته‌است.
- شکست یک نظیر نمی‌تواند بر عملکرد نظیرهای دیگر اثر بگذارد.
- نیاز به مدیر سیستم به‌صورت تمام وقت نیست. هر کاربر مدیر ماشین خود است.کاربر می‌تواند منابع به اشتراکی را کنترل کند.
- فقط برای استفاده در شبکه‌های کوچک یا خانگی مناسب می‌باشند.
- هزینه‌ی ایجاد و نگهداری این نوع شبکه به نسبت خیلی پایین است.
- چون کل سیستم به‌صورت غیرمتمرکز است، اداره کردن این نوع شبکه خیلی سخت است.
- امنیت این نوع شبکه خیلی پایین است.
- بازیابی اطلاعات یا نسخه‌ی پشتیبان[1] خیلی سخت است.



شکل 1-14 مدل شبکه به صورت نظیر به نظیر

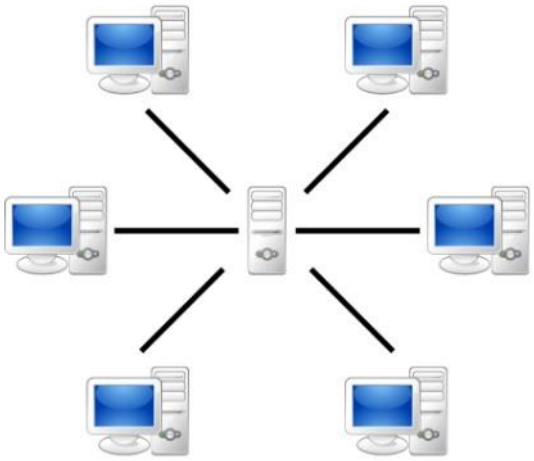
مدل کلاینت/سرور

یک ساختار توزیع‌شده‌ی برنامه‌ی کامپیوتری است که وظایف و یا بارکاری بین فراهم کنندگان منابع یا خدمات، با نام سرور، درخواست‌کننده سرویس، کلاینت‌ها تقسیم می‌شوند. اغلب کلاینت‌ها و یا سرورها بر روی یک شبکه‌ی کامپیوتری روی سخت‌افزار جداگانه ارتباط برقرار می‌کنند، اما کلاینت‌ها و سرورها ممکن است بر روی سیستم مشابه قرار بگیرند.

[1] Backup

سرور می‌تواند یک یا چندین برنامه سرور را اجرا کند که منابع خود را با کلاینت‌ها به اشتراک بگذارند. کلاینت‌ها نمی‌توانند منابع خود را به اشتراک بگذارند. هم‌چنین به‌عنوان Domain یاد می‌شوند. ویژگی های این مدل عبارتند از:

- کنترل مرکزی وجود دارد.
- همه‌ی فایل‌ها در مکان مشابه ذخیره می‌شوند، بنابراین مدیریت فایل‌ها راحت است و به راحتی می‌توان فایل‌ها را پیدا کرد.
- بازیابی اطلاعات و تهیه‌ی نسخه‌ی پشتیبان به راحتی انجام می شود.
- تغییرات با بروزرسانی سرور به راحتی انجام می‌شود.
- از پلتفرم های مختلف در شبکه، سرور از راه دور قابل دسترسی است.
- امنیت بالاتری دارد.
- موجب ازدحام در شبکه می‌شود.
- هزینه‌ی نصب و مدیریت این نوع شبکه خیلی بالا است.



شکل 1-15 مدل شبکه به‌صورت کلاینت/سرور

سیگنال

سیگنال به انتقال اطلاعات از نقطه‌ای به نقطه‌ی دیگر و یک سری پالس در کامپیوتر اشاره می‌کند. نمونه‌ای از سیگنال: امواج رادیویی و تصویری می‌باشد.

انواع سیگنال در شبکه

- **آنالوگ:** این نوع سیگنال‌ها به‌صورت پیوسته بوده و بی نهایت حالت دارند، همانند موج سینوسی می‌مانند. مثل: امواج رادیویی
- **دیجیتال:** این نوع سیگنال‌ها گسسته بوده و دارای دو حالت 0 و 1 می‌باشند. کامپیوترها دارای ساختار دیجیتال هستند.

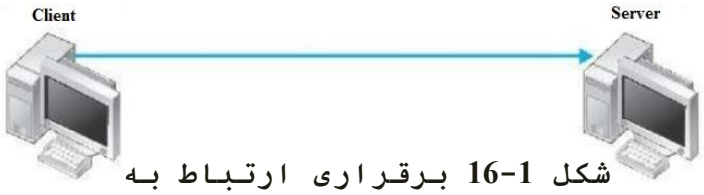
آشنایی با برخی اصطلاحات

- **Bandwidth:** میزان ظرفیت لینک ارتباطی برای ارسال داده است و بر حسب Kbps، Mbps، Gbps و... می‌باشد.
- **Baseband:** لینک ارتباطی دارای یک سیگنال می‌باشد، مثل خطوط تلفن
- **Broadband:** اگر لینک ارتباطی کانال بندی شود و از هر کانال یک سیگنال ارسال شود به مفهوم Broadband می‌باشد. مثل DSL که هم از خطوط تلفن استفاده می‌کند و هم از اینترنت.
- **Mac Address:** آدرسی 48 بیتی در مبنای هگزا است و از دو قسمت تشکیل شده است:
  - کد استاندارد اخذ شده توسط شرکت سازنده
  - شماره سریال کارخانه‌ای که این قطعه را تولید کرده است.
- **Intranet Network:** شبکه‌ای با ساختار WAN به‌صورت خصوصی
- **Extranet Network:** اتصال شبکه‌های Intranet با بستر WAN در نقاط مختلف جهان
- **IP Address(Network Address):** مشخصه‌ای است که هر سیستم توسط آن در شبکه شروع به برقراری ارتباط می‌کند.
- **Network Name:** اتصال سیستم‌ها با استفاده از نام سیستم
- **DNS[1]:** برای اینکه IP معادل با Name قرار گیرد از سرور DNS استفاده می‌شود.
- **Packet:** بسته‌های داده که در شبکه منتقل می‌شوند و از 3 قسمت تشکیل شده است:
  - Header: مسیر دسترسی از فرستنده به گیرنده در هدر نوشته می‌شود.
  - Data: داده‌ی مورد نظر در این قسمت قرار می‌گیرد.
  - Footer (یا Trailer): کنترل مسیر از دیدگاه سخت‌افزاری را انجام می‌دهد.

تکنیک‌های برقراری ارتباط دو طرفه

[1] Domain Name System

- **Simplex :** ارتباط و ارسال داده به‌صورت یکطرفه می‌باشد، مثل: تلویزیون



شکل 1-16 برقراری ارتباط به صورت Simplex

- **Half Duplex:** ارتباط به‌صورت دو طرفه‌ی غیر متقابل می‌باشد، مثل: هاب

شکل 1-17 برقراری ارتباط به صورت Half Duplex

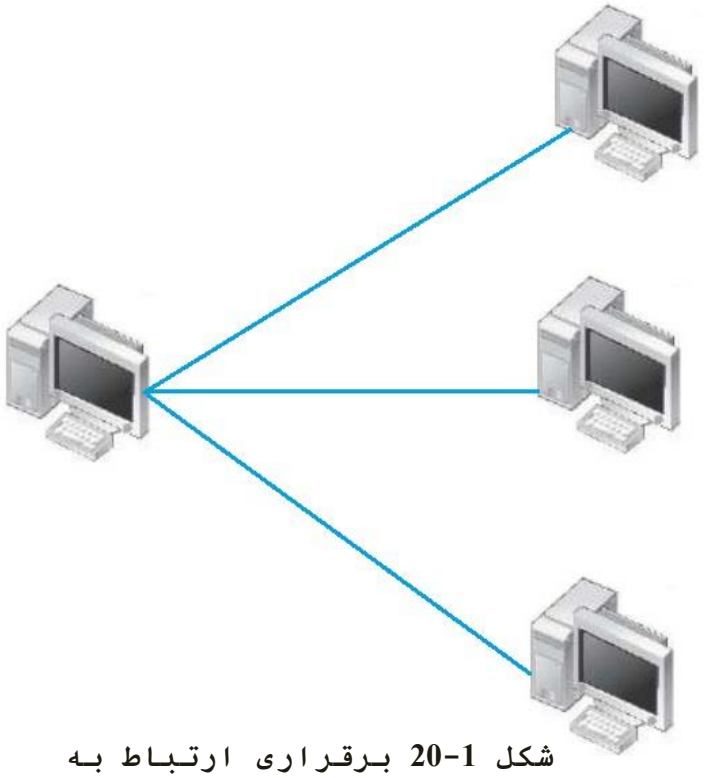
- **Full Duplex:** ارتباط به‌صورت دو طرفه‌ی متقابل است، مثل سوئیچ

شکل 1-18 برقراری ارتباط به صورت Full Duplex

- **Point-to-Point :** ارتباط بین دو سیستم به‌صورت مستقیم بدون هیچ واسط ارتباطی

شکل 1-19 برقراری ارتباط به‌صورت point-to-point

- **Multipoint:** ارتباط بیش از چندین Point بدون هیچ واسط ارتباطی



شکل 1-20 برقراری ارتباط به صورت Multipoint

نکات

- امکان تبدیل Full Duplex به Half Duplex وجود دارد ولی برعکس امکان‌پذیر نیست.
- Multipoint به‌صورت فیزیکی راه اندازی نمی‌شود بلکه با پروتکل‌ها راه اندازی می‌شود.

کابل‌های شبکه

کابل رسانه‌ای است که برای انتقال اطلاعات از یک دستگاه به دستگاه دیگری استفاده می‌شود. انواع مختلفی کابل وجود دارد که به‌طور گسترده‌ای در شبکه‌های LAN استفاده می‌شود. در برخی موارد یک شبکه تنها از یک کابل و شبکه‌های دیگر از کابل‌های متعدد استفاده خواهند کرد. انتخاب نوع کابل به موارد متعددی نظیر: توپولوژی، پروتکل و اندازه بستگی دارد. انواع مختلف کابل‌های شبکه عبارتند از:

- کابل‌های مسی[1]
- کابل‌های زوج بهم تابیده[2]
- کابل‌های فیبر نوری[3]

کابل‌های مسی

نمونه‌ای از این کابل‌ها، کابل کواکسیال می‌باشد. کابل‌های کواکسیال نوع اصلی کابل‌های استفاده شده برای انتقال ویدئو، ارتباطات و صدا می‌باشند. این کابل دارای پهنای باند بالا و ظرفیت انتقال بیشتر می‌باشد. بیشتر کاربران کابل کواکسیال، از این نوع کابل برای اتصال تلویزیون‌های خود به یک سرویس تلویزیون کابلی استفاده می‌کنند، هم‌چنین از کابل‌های کواکسیال برای شبکه‌های کامپیوتری هم چون اترنت نیز استفاده می‌شود. این نوع کابل شامل لایه‌های متحدالمرکز از رساناهای الکتریکی و مواد عایق می‌باشد. این نوع ساخت در کابل‌های کواکسیال تضمین می‌کند که سیگنال‌ها درون کابل محصور شده و مانع از نویز الکتریکی از تداخل با سیگنال می‌شود.

شکل 1-21 نمونه‌ای از یک کابل مسی

کابل‌های زوج بهم تابیده

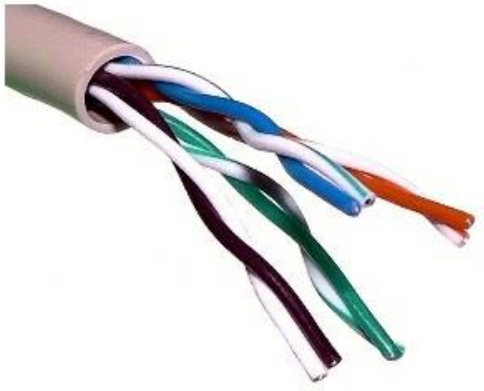
این نوع کابل‌ها شامل زوج سیم‌های عایق بندی شده می‌باشند که با همدیگر پیچ خورده‌اند. این کابل‌ها در مخابرات برای انتقال صدا و ارتباطات تلفنی به مدت زمان طولانی استفاده می‌شوند. امروزه به طور گسترده در شبکه ها مورد استفاده واقع
می‌شوند. کابل‌های زوج بهم تابیده به کاهش نویز از منابع خارجی و تداخل بر روی کابل‌های چند جفتی کمک می‌کنند. کابل‌های زوج بهم تابیده به دو روش ساخته می‌شوند:

- **UTP**[4]

[1] Copper Cables
[2] Twisted Pair Cables
[3] Fiber Optic Cables
[4] Unshielded twisted pair

- **STP** [1]

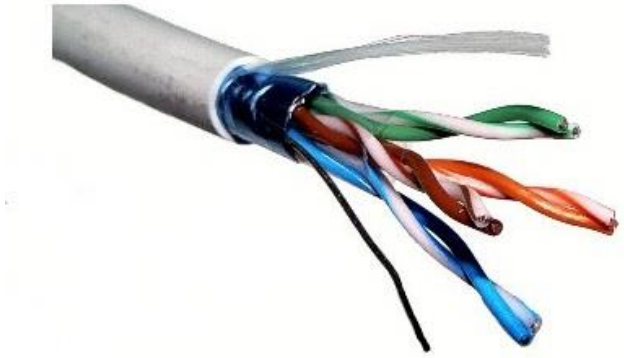
UTP: این نوع کابل از زوج سیم‌ها تشکیل شده است و در شبکه‌های گوناگون استفاده می‌شود. در یک کابل UTP هر هشت سیم مسی جداگانه توسط مواد عایق پوشیده شده‌اند. علاوه بر این، سیم‌ها در هر جفت دور یکدیگر پیچ خورده‌اند.



شکل 1-22 نمونه کابل UDP

STP

کابل STP ترکیبی از تکنیک‌های محافظت، خنثی‌سازی، و سیم‌های به هم تابیده است. هر زوج از سیم‌ها در فویل فلزی پیچیده شده است. سپس چهار زوج سیم به‌طور کلی با فویل یا فلز به‌هم تابیده پوشانده می‌شوند.



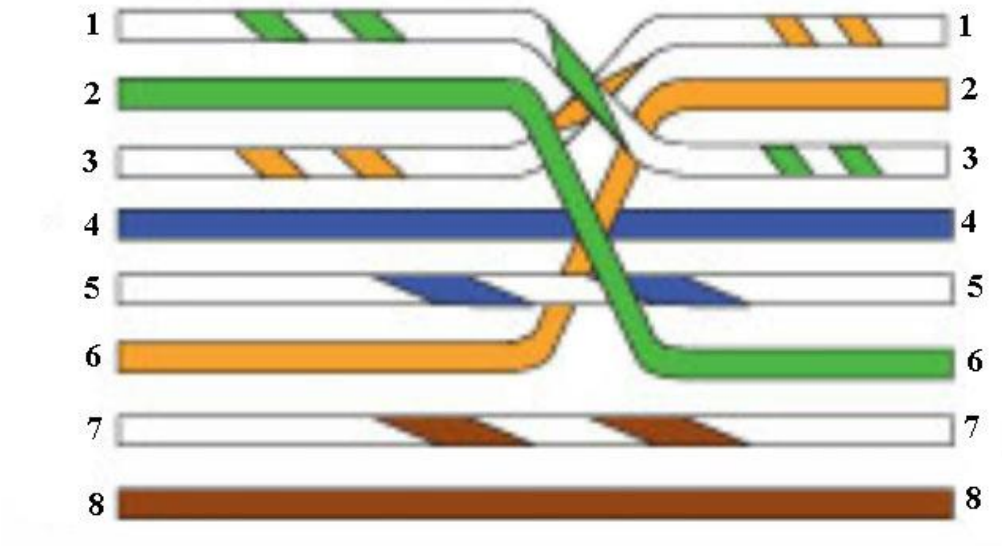
شکل 1-23 نمونه کابل STP

کابل‌های زوج بهم تابیده براساس کاربرد

[1] shielded twisted pair

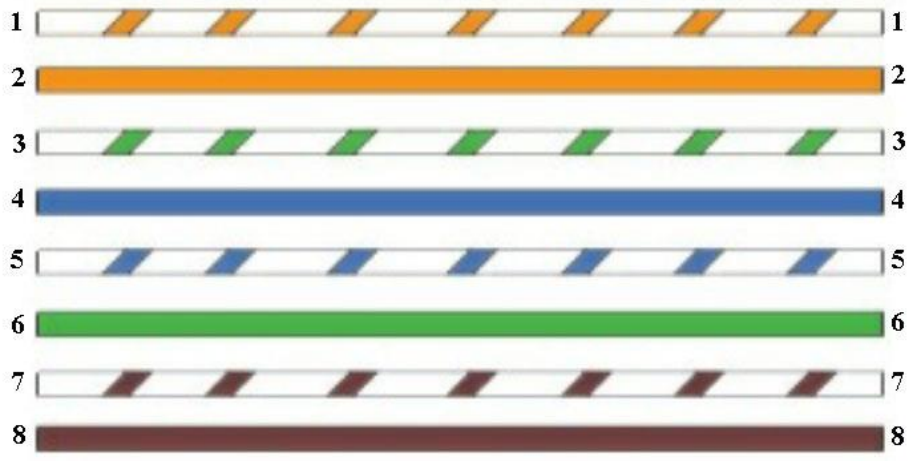
کابل‌های زوج بهم تابیده براساس کاربرد عبارتند از:

- **Cross over :** برای اتصال دو سیستم یکسان(هم جنس) از این کابل استفاده خواهد شد.



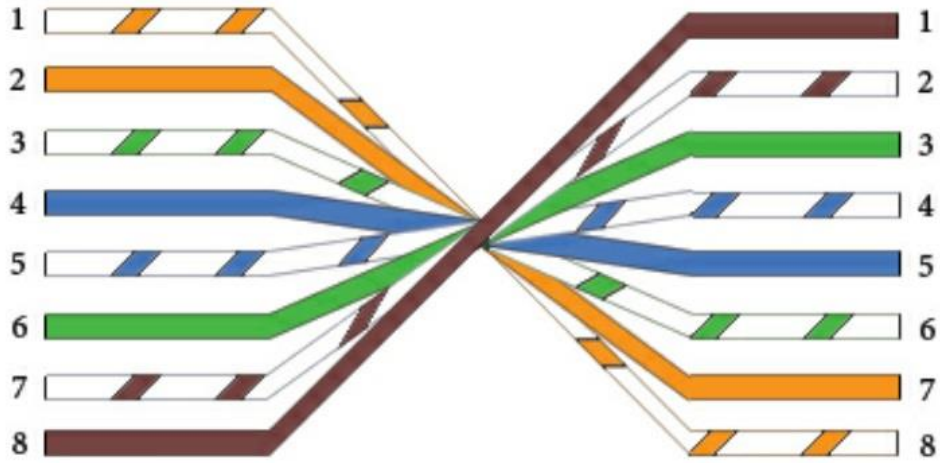
شکل 1-24 ترکیب رنگبندی سیم‌ها در

- **Straight through :** برای اتصال دو سیستم متفاوت از این کابل استفاده می‌شود.

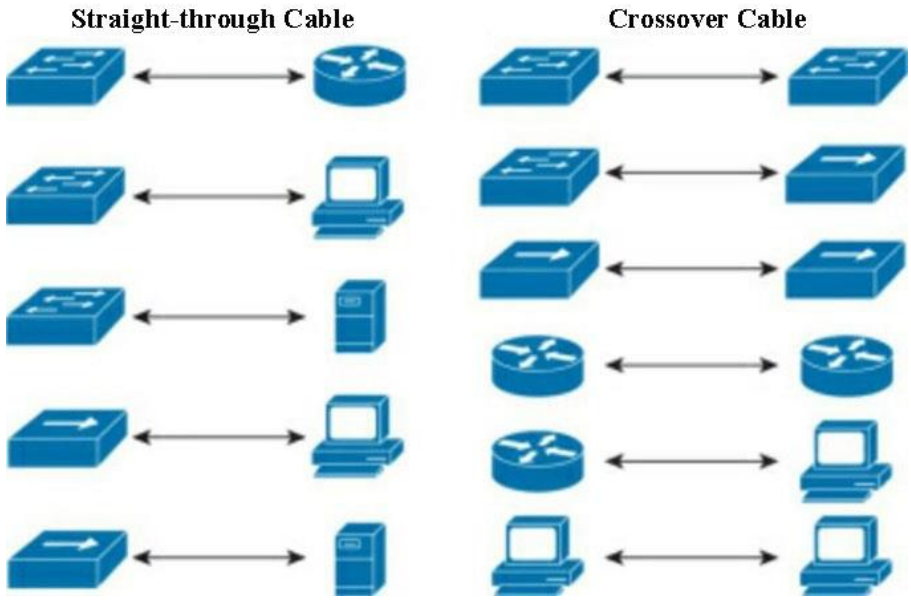


شکل 1-25 ترکیب رنگبندی سیم‌ها در
Straight through

- **Roll Over (Console):** وقتی برای اولین بار یک سوئیچ یا روتر کانفیگ می‌شود از این کابل استفاده می‌شود.



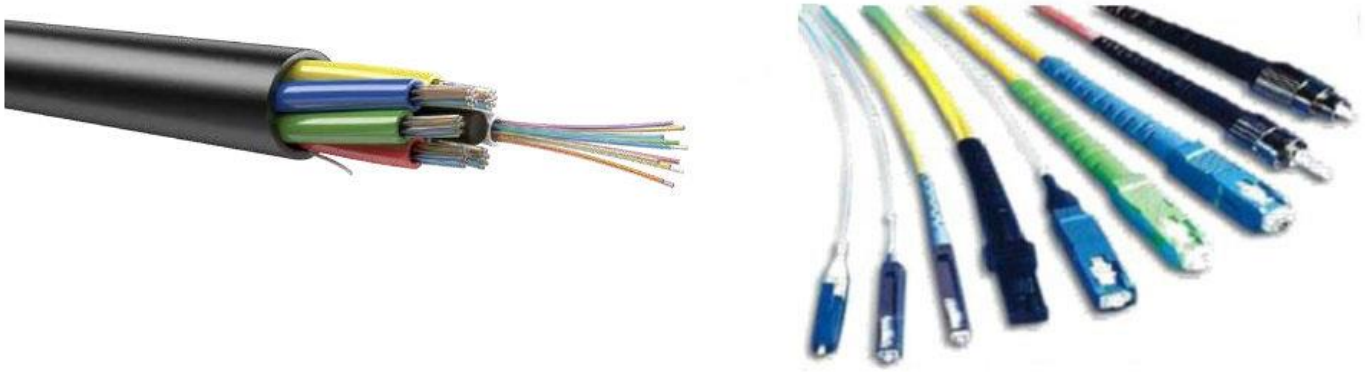
شکل 1-26 ترکیب رنگبندی سیم‌ها



شکل 1-27 اتصال دستگاه‌ها براساس نوع کابل

کابل‌های فیبرنوری

این کابل‌ها از امواج نور برای انتقال داده‌ها استفاده می‌کنند. در کابل‌های فیبر نوری سرعت افزایش چشمگیری پیدا می‌کند و حجم قابل توجهی از داده‌ها انتقال داده می‌شود، هم‌چنین قابلیت شنود فیبرنوری بسیار پایین است.



شکل 1-28 نمونه‌ای از کابل‌های فیبرنوری

تجهیزات ارتباطی شبکه

- **NIC**[1]
  - وسیله‌ی ارتباطی کلاینت‌ها با شبکه می‌باشد.
  - IP بر روی کارت شبکه قرار می‌گیرد.
  - با کابل زوج بهم تابیده به شبکه متصل می‌شوند، یعنی حداقل یک عدد کانکتور Rj-45 دارند.
  - هر کارت شبکه لزوما دارای MAC Address مخصوص به خود می باشد.

- **Tranceiver:** ارسال و دریافت داده توسط این وسیله انجام می‌شود.

- **Repeater (تکرارکننده):** برای قوی کردن سیگنال در جاهایی که سیگنال تضعیف شده است مورد استفاده قرار می‌گیرد، معمولا در توپولوژی گذرگاه استفاده می‌شوند تا بتوانند در مسیرهای طولانی‌تر استفاده کنند.

- **Hub**
  - برای اتصال بخش‌های یک شبکه LAN استفاده می شود.
  - شامل پورت‌های متعددی می‌باشد.
  - Broadcast انجام می‌دهد.
  - اساس عملکردش براساس Mac Address می‌باشد.

[1] Network Interface Card

- **Switch**

  - برای اتصال دستگاه‌های مختلف در شبکه استفاده می‌شود.
  - Multicast و Unicast انجام می دهد.
  - اساس عملکردش براساس Mac Address است.
  - کیفیت ترافیک را نسبت به هاب به صورت بهتر انجام می‌دهد.
  - جایگزین هاب شده است.

- **Bridge (پل) :** برای اتصال یک LAN به LAN دیگر که از پروتکل مشابه استفاده می‌کنند، مورد استفاده واقع می‌شود.

سوئیچ قابل تبدیل شدن به bridge می باشد.

- **Router :** عمل مسیریابی در شبکه را انجام می‌دهند و براساس IP کار می‌کنند.

- **Wireless Access Point**

  - جایگزین سوئیچ در وایرلس می‌باشد.
  - با Mac Address کار می‌کنند.

- **Gateway(دروازه) :**توسط Gateway از یک توپولوژی می‌توان به توپولوژی دیگری وصل شد، برای مثال برای اتصال شبکه‌ی LAN به WAN از این دستگاه استفاده می‌شود.

لایه های مدل OSI[1]

مدل OSI توسط سازمان استانداردسازی در سال 1984 طراحی شده است. این مدل یک چارچوب شبکه برای اجرای پروتکل ها در 7 لایه تعریف می کند. هر لایه شامل مجموعه ای از عملکردها در طول ارتباطات داده می باشد. لایه های مدل OSI عبارتند از:

- لایه فیزیکی[2]
- لایه انتقال داده[3]
- لایه شبکه[4]
- لایه انتقال[5]
- لایه جلسه[6]
- لایه نمایش[7]
- لایه کاربرد[8]

شکل 1-29 مدل 7 لایه ای OSI

لایه فیزیکی

- در این لایه داده ها با فرمت باینری قرار دارند که توسط کامپیوترها قابل شناسایی می‌باشند.
- انتقال داده ها به‌صورت بیت‌های 0 و 1 توسط کابل‌های شبکه انجام می‌شوند.
- کابل‌های شبکه، هاب و تکرار کننده در این لایه قرار دارند.

لایه پیوند داده

- لایه‌ای است که از دو زیر مجموعه پروتکلی تشکیل شده است:
  - **MAC**[9]: باعث ارتباط برقرار کردن سیستم ها در شبکه با استفاده از Mac Address می‌شود.

[1] Open Systems Interconnection
[2] Physical Layer
[3] Data Link Layer
[4] Network Layer
[5] Transport Layer
[6] Session
[7] Presentation Layer
[8] Application Layer
[9] Media Access Control

- **LLC**[1]: کنترل سخت‌افزاری ارتباط از فرستنده به گیرنده
  - کشف خطا در برقراری ارتباط ما بین سیستم‌های شبکه توسط LLC انجام می‌شود.

- در این لایه، اطلاعات هم در Header و هم در Footer نوشته می‌شود ولی در بقیه لایه‌ها فقط در Header نوشته می‌شود.
- اطلاعات Mac Address در header و اطلاعات LLC در Footer نوشته می‌شود.
- سوئیچ به‌صورت پایه‌ای در این لایه قرار دارد.

لایه شبکه

- اصلی‌ترین لایه‌ی ارتباطی در شبکه‌ها می‌باشد.
- این لایه مسیر رسیدن به مقصد را تعیین می‌کند.
- مشخصه‌ی اصلی این لایه، پروتکل IP می‌باشد.
- روتر در این لایه قرار دارد.

لایه انتقال

- مکانیزم انتقال داده بین برنامه‌های کاربردی در شبکه را فراهم می‌کند.
- شامل دو پروتکل مهم زیر می‌باشد:
  - **TCP**[2]
    - اتصال گرا است.
    - .Ack را پشتیبانی می‌کند.
    - قابل اعتماد می‌باشد.
    - انتقال داده‌ها به کندی انجام می‌شود.
    - شماره پروتکل برابر 6 است.
  - **UDP**[3]
    - غیراتصال گرا است.
    - .Ack را پشتیبانی نمی‌کند.
    - غیرقابل اعتماد می‌باشد.
    - انتقال داده ها به سرعت انجام می‌شود.
    - شماره پروتکل برابر 17 است.

[1] Logical Link Control
[2] Transmission Control Protocol
[3] User Datagram Protocol

- عمده‌ترین وظایف لایه انتقال عبارتست از:
  - شناسایی سرویس
  - قطعه‌بندی
  - ترتیب‌گذاری
  - بازیابی خطا
  - کنترل جریان

لایه جلسه

- مدیریت، ایجاد و بستن sessionهای ارتباطی وظیفه‌ی این لایه می باشد.

نکات

- ارسال درخواست برای برقراری ارتباط را Session می‌نامند.
- Session ارتباطی از فرستنده با آدرسی بنام Socket Address انجام می‌شود.
- Socket Address=ip:port

لایه نمایش

- فرمت داده‌ها برای انتقال در شبکه در این لایه انجام می‌شود.
- عمده‌ترین وظایف لایه انتقال عبارتست از:
  - رمزگذاری و رمزگشایی داده
  - فشرده‌سازی و از حالت فشرده خارج ساختن داده

لایه کاربرد

- سرویس‌های متداول شبکه در این لایه انجام می‌شود، مثل: وب سرور
- احراز هویت در این لایه انجام می شود.

هر ارتباطی در شبکه باید دارای قابلیت تشریح با مدل OSI باشد.

پورت

- پورت یک کانال ارتباط منطقی است.
- از شماره پورت‌ها برای شناسایی سرویس‌ها استفاده می‌شود.
- مجموع شماره های پورت: 0- 65535

- پورت‌های رزرو شده: 1-49151، پورت‌های باز: 49152-65535

پروتکل

پروتکل‌ها، سیاست‌ها و استانداردهای متشکل از قوانین، رویه‌ها و فرمت‌ها می‌باشند که ارتباط دو یا چندین دستگاه بر روی یک شبکه را تعریف می‌کنند.

جدول 1-1 انواع

پروتکل	توضیح
ARP	تبدیل IP به Mac Address
RARP	تبدیل Mac Address به IP
ICMP	تست ارتباط ما بین دو سیستم، دستور ping از ICMP استفاده می‌کند.
IGMP	راه اندازی Multicast
DHCP	اختصاص اتوماتیک IP به ازای کامپیوترها
APIPA	اختصاص IP توسط سیستم عامل موقعی که DHCP از کار می‌افتد
FQDN	مشخص کردن اسم Domain برای کامپیوتر یا هاست بر روی اینترنت

نکات

- محدوده آدرس‌های APIPA: 169.254.0.0 تا 169.254.255.255
- Host file: یک فایل کامپیوتری می‌باشد که توسط سیستم عامل برای نگاشت hostname به IP استفاده می‌شود.

سرویس TCP/IP

سرویس در واقع همان پروتکل می‌باشد، وظیفه‌ش انجام دادن کاری در شبکه می‌باشد. انواع سرویس‌های TCP/IP عبارتند از:

- **FTP**[1]
  - برای آپلود و دانلود فایل در شبکه استفاده می‌شود.

[1] File Transfer Protocol

- شماره پورت: 20 و 21
- TCP است.

- **Telnet**
  - پروتکل اتصال از راه دور نسبت به شبکه است.
  - شماره پورت: 23
  - TCP است.
- **NTP[1]**
  - پروتکل تنظیم ساعت در کل شبکه می‌باشد.
  - شماره پورت: 123
  - UDP است.
  - از لایه‌های مختلف منابع ساعت استفاده می‌کند.
  - به‌عنوان مدل کلاینت/سرور کار می‌کند.
- **SMTP[2]**
  - پروتکل ارسال ایمیل در شبکه است.
  - شماره پورت: 25
  - TCP است.

- **POP3[3]**
  - پروتکل دریافت ایمیل در شبکه است.
  - شماره پورت :110
  - TCP است.

- **IMAP4[4]**
  - پروتکلی است که برای ارسال و دریافت ایمیل استفاده می‌شود.
  - شماره پورت: 143
  - TCP است.
- **NNTP [5]**
  - پروتکل پوشش‌دهی شبکه‌های خبری است.
  - شماره پورت: 119
  - TCP می باشد.
- **HTTP[6]**
  - پروتکل راه‌اندازی سرویس وب است.
  - شماره پورت : 80

[1] Network Time Protocol
[2] Simple Mail Transfer Protocol
[3] Post Office Protocol 3
[4] Internet Message Access Protocol 4
[5] Network News Transfer Protocol
[6] Hypertext Transfer Protocol

- TCP است.

- **HTTPs**[1]
  - پروتکل راه‌اندازی سرویس وب به‌طور امن می‌باشد.
  - شماره پورت: 443
  - هم TCP و هم UDP است.
- **LPR/LPD**[2]
  - این دو پروتکل با هم همکاری می‌کنند.
  - LPR پروتکل ارسال درخواست پرینت در شبکه می‌باشد.
  - LPD پروتکل انجام پرینت تحت شبکه می‌باشد.
  - شماره پورت: 515
  - TCP است.

- **NFS** [3]
  - پروتکلی است که اجازه‌ی دسترسی به منابع اشتراکی شبکه را می‌دهد.
  - شماره پورت: 2049
  - هم TCP و هم UDP است.
- **SSH** [4]
  - پروتکل اتصال امن از راه دور است.
  - شمار پورت: 22
  - TCP است.
- **SCP** [5]
  - برای عبور داده‌ها در تونل امن به صورت کد شده از این پروتکل استفاده می‌شود.
  - زمانی استفاده می‌شود که SSH وجود داشته باشد.
  - شماره پورت: 22
  - TCP است.
- **SMB** [6]
  - پروتکل به اشتراکگذاری منابع شبکه می‌باشد.

[1] HTTP Secure
[2] Line Printer Remote/ Line Printer Daemon
[3] Network File System
[4] Secure Shell
[5] Secure Copy Protocol
[6] Server Message Block

- SMB در سرور انجام می‌شود ولی اگر شبکه workgroup باشد در کلاینت هم انجام می‌شود.
- SMB می‌تواند بالای لایه‌ی جلسه (و پایین‌تر) به روش‌های مختلفی اجرا شود:
  - به صورت مستقیم بر روی TCP ، پورت: 445
  - از طریق NetBIOS API، که در حقیقت می‌تواند بر روی لایه‌های انتقال روی پورت‌های UDP: 137 و 138 و پورت‌های TCP: 137 و 139 اجرا شود.

- **LDAP** [1]
  - پروتکل اتصال به سرویس دایرکتوری می‌باشد.
  - توسط تمامی سیستم عامل‌ها پشتیبانی می‌شود.
  - شماره پورت: 389
  - TCP است.

- **SNMP** [2]
  - پروتکل مدیریت شبکه‌ها است.
  - شماره پورت: 161
  - UDP است.
  - توسط همه‌ی دستگاه‌ها پشتیبانی می‌شود.
  - مدیران شبکه از SNMP برای مانیتور و نگاشت قابلیت‌ها، کارایی و خطاهای شبکه استفاده می‌کنند.

[1] Lightweight Directory Access Protocol
[2] Simple Network Management Protocol

فصل2

IP Addressing & Subneting

IP Address

IP Address یک شناسه برای کامپیوترها یا دستگاه‌هایی است که در یک شبکه برای برقراری ارتباط استفاده می‌کنند. در واقع IP Address:

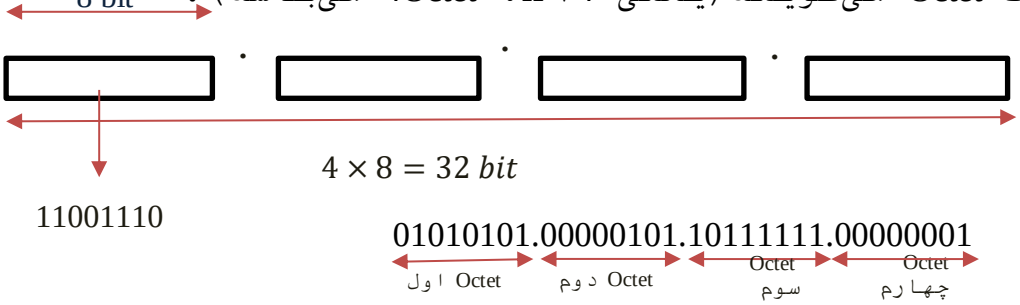
- یک آدرس منطقی[1] می‌باشد.
- یک آدرس لایه‌ی شبکه (لایه 3) می‌باشد.
- به‌طور کلی در حال حاضر در دو نسخه وجود دارند:

  - IPV4: 32 بیت می‌باشد.
  - IPV6: 128 بیت می‌باشد.

تا چندین سال قبل همه‌ی آدرس‌هایی که استفاده می‌شد IPV4 بود ولی اخیرا به‌خاطر اتمام IPV4 ها از IPV6 برای تخصیص ip استفاده می‌شود. در این فصل بحث ما روی IPV4 می‌باشد.

IPV4

شامل یکسری بیت‌های 0 و1 می‌باشند، به‌طور کلی این بیت‌ها در 4 بلوک 8 بیتی در کنار هم قرار گرفته‌اند. به هر 8بیتی که در یک بلوک قرار گرفته‌اند یک Octet می‌گویند (یعنی IPV4، 4Octet می‌باشد).



IP Address در فرم دسیمال:

85.5.191.1

محدوده IPV4

با یک مثال برای octet اول توضیح می‌دهیم:

مجموع 8 بیت درoctet قرار دارد که مقادیر 0 و 1 در octet قرار خواهد گرفت، به این ترتیب $2^8 = 256$ حالت وجود دارد.

2^7 2^6 2^5 2^4 2^3 2^2 2^1 2^0
0 0 0 0 0 0 0 0 = 0

مجموع محدوده IP Address

0.0.0.0
To
255.255.255.255

[1] Logical Address

0 0 0 0 0 0 0 1 = 1

0 0 0 0 0 0 1 0 = 2

0 0 0 0 0 0 1 1 = 3

0 0 0 0 0 1 0 0 = 4

1 1 1 1 1 1 1 1= 255

جدول 2-1 مثالی از تبدیل اعداد

128	64	32	16	8	4	2	1	جواب
1	1	0	0	0	0	0	0	192
0	0	0	0	1	0	1	0	10
1	0	1	0	1	0	0	0	168
1	0	1	0	1	1	0	0	172
0	0	0	1	0	0	0	0	16

جدول 2-2 مثالی از تبدیل اعداد
دسیمال به باینری

دسیمال	جواب							
	128	64	32	16	8	4	2	1
18	0	0	0	1	0	0	1	0
152	1	0	0	1	1	0	0	0
200	1	1	0	0	1	0	0	0
15	0	0	0	0	1	1	1	1
240	1	1	1	1	0	0	0	0

IPV4 از دو قسمت اصلی تشکیل شده است:

- **Network ID** :مشخصه ای از IP است که نشان‌دهنده‌ی یک شبکه‌ی مستقل می‌باشد.
- **Host ID** : نشان‌دهنده‌ی یک کامپیوتر در یک شبکه‌ی مستقل می‌باشد.

دو سیستم در یک شبکه، هیچ وقت دارای Host ID یکسان نخواهند شد ولی Net ID هایشان لزوما یکسان خواهد شد.

IP Address= Net ID + Host ID

Mask

برای شناسایی بیت‌های Net ID و Host ID در IPV4 از مفهومی به‌نام Mask استفاده می‌شود.در واقع Mask بیان کننده‌ی تعدادبیت‌های Host ID و Net ID می‌باشد.

IP همواره باید با Mask نوشته شود.

اگر IP ی یک شبکه مدنظر باشد آن IP، Subnet می‌باشد.

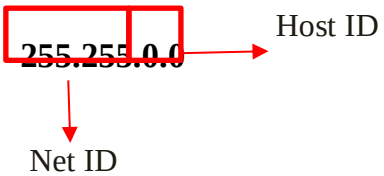
Sunbet Mask : Mask به ازای یک شبکه مستقل می‌باشد.

انواع Mask

- استاندارد
- متغیر

Mask از نوع استاندارد

طبق این نوع استاندارد اگر در IP ی مورد نظر عدد 255 مشاهده شود، نشان‌دهنده‌ی Net ID و اگر عدد 0 مشاهده شود، نشان‌دهنده‌ی Host ID می‌باشد(به‌طور پیش فرض، Mask دو عدد 255 و 0 را می‌شناسد).



برای مدیریت بهتر IP ها از کلاس‌های IP استفاده می‌شود.

کلاس های استاندارد IPV4

کلاس‌های IP، بلوک‌های طبقه‌بندی شده ای هستند که براساس Net ID و Host ID مشخص شده اند (در واقع تعریف Mask از نوع استاندارد می‌باشد). این کلاس‌ها شامل کلاس‌های: A، B، C، D و E می‌باشند (A، B و C کلاس‌های اصلی هستند و غالبا از این کلاس‌ها استفاده می‌شود).

نکات

- معیار تفکیک کردن IP Address ها، ظرفیت IP ها در شبکه می‌باشد. هرچقدر ظرفیت IP بیشتر باشد، آن IP گران‌تر است (IP کلاس A گران‌تر از کلاس C می‌باشد).
- کلاس‌های A، B، C در شبکه های LAN و WAN استفاده می‌شود.
- کلاس D برای Multicasting رزرو شده است.
- کلاس‌هاي E جهت انجام کارهاي آزمايشي و تحقيقاتي استفاده مي‌شوند.

شناسایی کلاس‌های IP

- برای طبقه‌بندی IP Address ها از بیت‌های اولویت[1] استفاده می شود.
- پر اهمیت‌ترین بیت(بیت‌ها) از Octet اول برای بیت(بیت‌های) اولویت انتخاب شده اند.
- بیت اولویت کلاس A ، 0 می‌باشد.
- بیت‌های اولویت کلاس B، 10 می‌باشد.
- بیت‌های اولویت کلاس C ، 110 می‌باشد.
- بیت‌های اولویت کلاس D ، 1110 می‌باشد.
- بیت‌های اولویت کلاس E ، 1111 می‌باشد.

محدوده کلاس A

- در کلاس A، اولین بیت از Octet اول به عنوان بیت اولویت انتخاب شده و مقدار این بیت 0 می‌باشد.
- **0xxxxxxx. xxxxxxxx. xxxxxxxx. xxxxxxxx**

2^7 2^6 2^5 2^4 2^3 2^2 2^1 2^0

0 0 0 0 0 0 0 0 = 0

0 0 0 0 0 0 0 1 = 1

0 0 0 0 0 0 1 0 = 2

0 0 0 0 0 0 1 1 = 3

0 0 0 0 0 1 0 0 = 4

0 1 1 1 1 1 1 1 = 127

محدوده کلاس A
0. 0. 0. 0
To
127. 255. 255. 255

[1] Priority

محدوده کلاس B

- در کلاس B، دو بیت اول از Octet اول برای بیت‌های اولویت انتخاب شده و مقدار بیت 10 می‌باشد.
- 10xxxxxx. xxxxxxxx. xxxxxxxx. xxxxxxxx

2^7 2^6 2^5 2^4 2^3 2^2 2^1 2^0

1 0 0 0 0 0 0 0 = 128

1 0 0 0 0 0 0 1 = 129

1 0 0 0 0 0 1 0 = 130

1 0 0 0 0 0 1 1 = 131

1 0 0 0 0 1 0 0 = 132

1 0 1 1 1 1 1 1 = 191

محدوده کلاس B
128. 0. 0. 0
To
191. 255. 255. 255

محدوده کلاس C

- در کلاس C، 3 بیت اول از Octet اول به عنوان بیت‌های اولویت انتخاب شده و این بیت‌ها مقادیر 110 می‌باشند.
- 110xxxxx. xxxxxxxx. xxxxxxxx. xxxxxxxx

2^7 2^6 2^5 2^4 2^3 2^2 2^1 2^0

1 1 0 0 0 0 0 0 = 192

1 1 0 0 0 0 0 1 = 193

1 1 0 0 0 0 1 0 = 194

1 1 0 0 0 0 1 1 = 195

1 1 0 0 0 1 0 0 = 196

1 1 0 1 1 1 1 1 = 223

محدوده کلاس C
192. 0. 0. 0
To
223. 255. 255. 255

محدوده کلاس D

- در این کلاس، 4 بیت اول از Octet اول به‌عنوان بیت اولویت در نظر گرفته شده‌اند و دارای مقادیر 1110 می‌باشند.
- 1110xxxx. xxxxxxxx. xxxxxxxx. xxxxxxxx

2^7 2^6 2^5 2^4 2^3 2^2 2^1 2^0

1	1	1	0	0	0	0	0	= 224
1	1	1	0	0	0	0	1	= 225
1	1	1	0	0	0	1	0	= 226
1	1	1	0	0	0	1	1	= 227
1	1	1	0	0	1	0	0	= 228
1	1	1	0	1	1	1	1	= 239

محدوده کلاس D
224 .0. 0. 0
To
239. 255. 255. 255

محدوده کلاس E

- در این کلاس، 4 بیت از Octet اول به عنوان بیت اولویت در نظر گرفته شده است و دارای مقادیر 1111 می‌باشد.
- 1111xxxx. xxxxxxxx. xxxxxxxx. xxxxxxxx

2^7 2^6 2^5 2^4 2^3 2^2 2^1 2^0

1	1	1	1	0	0	0	0	= 240
1	1	1	1	0	0	0	1	= 241
1	1	1	1	0	0	1	0	= 242
1	1	1	1	0	0	1	1	= 243
1	1	1	1	0	1	0	0	= 244
1	1	1	1	1	1	1	1	= 255

محدوده کلاس E
240. 0. 0. 0
To
255. 255. 255. 255

جدول 2-3 مثالی از

IP Address	Class
10.1.100.1	A
150.17.2.200	B
192.1.1.1	C
224.0.0.10	D
120.200.1.1	A

تعداد شبکه و هاست در کلاس‌ها

تعداد شبکه و هاست کلاس A

- فرمت Octet کلاس A به‌صورت: N.H.H.H می‌باشد.
  - 8 بیت شبکه
  - 24 بیت هاست
- تعداد شبکه
  - = بیت اولویت–تعداد بیت شبکه 2
  - = 2^{8-1} (1- به‌خاطر بیت اولویت کلاس A است)
  - = 128-2 (2- برای شبکه‌ی 0 و 127 است)
  - = 126
- تعداد هاست
  - = 2 - تعداد بیت های هاست
  - = 2^{24} - 2 (2- برای Net ID و Broadcast ID است)
  - 16777216 – 2
  - 16777214

تعداد شبکه و هاست کلاس B

- فرمت Octet کلاس B به‌صورت N.N.H.H می‌باشد.
  - 16 بیت شبکه
  - 16 بیت هاست

- تعداد شبکه
  - $2^{\text{تعداد بیت شبکه}}$ = بیت اولویت–تعداد بیت شبکه
  - 2^{16-2} = (2- به‌خاطر بیت‌های اولویت است)
  - 2^{14} =
  - 16384 =
- بیت‌های هاست

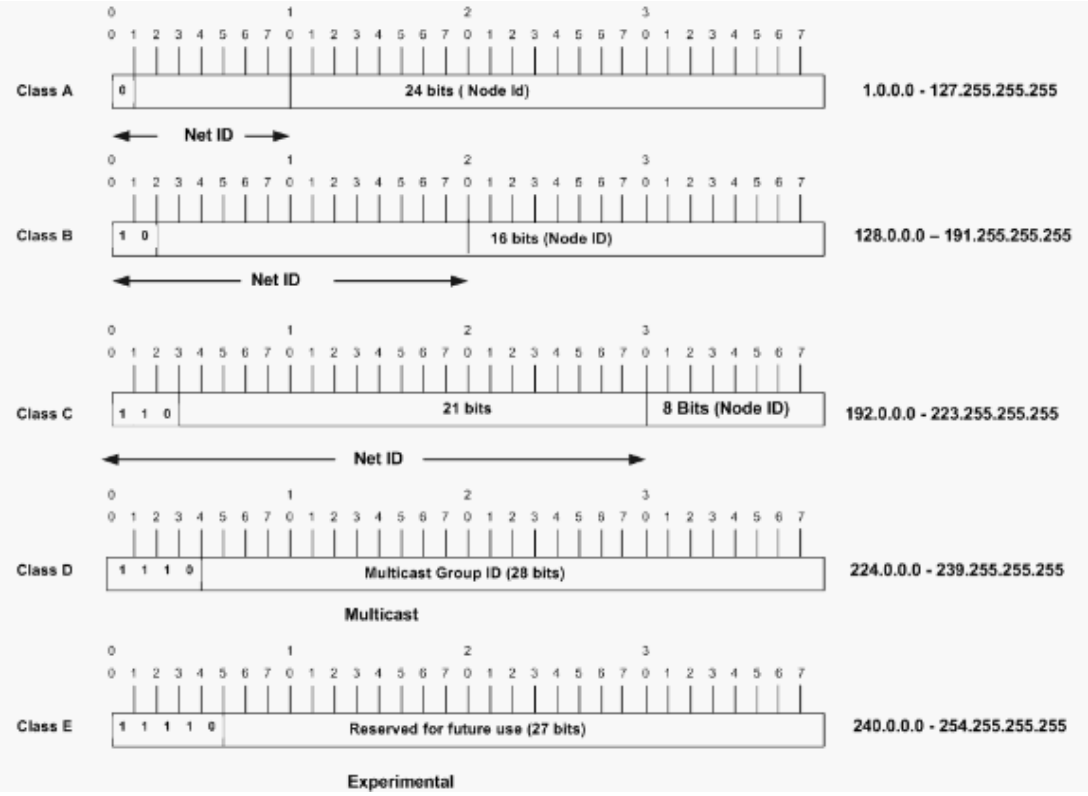
  - $2^{\text{تعداد بیت های هاست}}$ -2 =
  - 2^{16} - 2= (2- برای Net ID و Broadcast ID است)
  - 65536 – 2 =
  - 65534 =

تعداد شبکه و هاست کلاس C

- فرمت Octet کلاس C به‌صورت N.N.N.H می‌باشد.
  - 24 بیت شبکه
  - 8 بیت هاست
- تعداد شبکه
  - $2^{\text{تعداد بیت های شبکه}}$ = بیت اولویت–تعداد بیت های شبکه
  - 2^{24-3} = (3- برای بیت اولویت می‌باشد)
  - 2^{21} =
  - 2097152 =
- تعداد هاست
  - $2^{\text{تعداد بیت های هاست}}$ - 2 =
  - 2^{8} - 2= (2- برای Net ID و Broadcast ID است)
  - 256-2 =
  - 254 =

خلاصه کلاس‌های IP Address

N/W	Host	Host	Host	Class A
N/W	N/W	Host	Host	Class B
N/W	N/W	N/W	Host	Class C



Class	1st Octet Decimal Range	1st Octet High Order Bits	Network/Host ID (N=Network, H=Host)	Default Subnet Mask	Number of Networks	Hosts per Network (Usable Addresses)
A	1 – 126*	0	N.H.H.H	255.0.0.0	126 (2^7 – 2)	16,777,214 (2^{24} – 2)
B	128 – 191	10	N.N.H.H	255.255.0.0	16,382 (2^{14} – 2)	65,534 (2^{16} – 2)
C	192 – 223	110	N.N.N.H	255.255.255.0	2,097,150 (2^{21} – 2)	254 (2^8 – 2)
D	224 – 239	1110	Reserved for Multicasting			
E	240 – 254	1111	Experimental; used for research			

هر IP Address در شبکه اگر دارای 4 مشخصه‌ی زیر باشد، از جهت ارتباطی کامل می‌باشد:

- **Net ID**
- **Valid IP**
  - **First IP**
  - **Last IP**
- **Broadcast IP**

Net ID: IP Address با تمام بیت‌های0 در قسمت Host (با تبدیل کردن تمام بیت‌های Host به 0 ، Net ID به‌دست می‌آید)

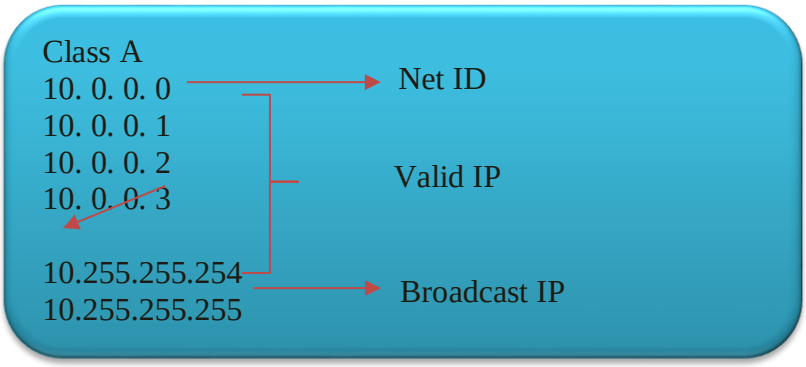
Broadcast IP: IP Address با همه‌ی بیت‌های 1 در موقعیت Host (اگر بیت‌های Host ID را که 0 هستند کلا به 1 تبدیل کنیم، broadcast ip به‌دست می‌آید).

Valid IP: بین Net ID و Broadcast IP واقع شده اند.

اگر در آخرین Octet (Octet چهارم) عدد 255 دیده شود یعنی broadcast. 255 را نمی‌توان روی یک کامپیوتر تنظیم کرد، مثلا IP:192.168.10.255 را نمی‌توان به کامپیوتر اختصاص داد چون این یک IPی broadcast بوده و برای ارسال ترافیک در کل شبکه استفاده می‌شود.

مثال برای کلاس A

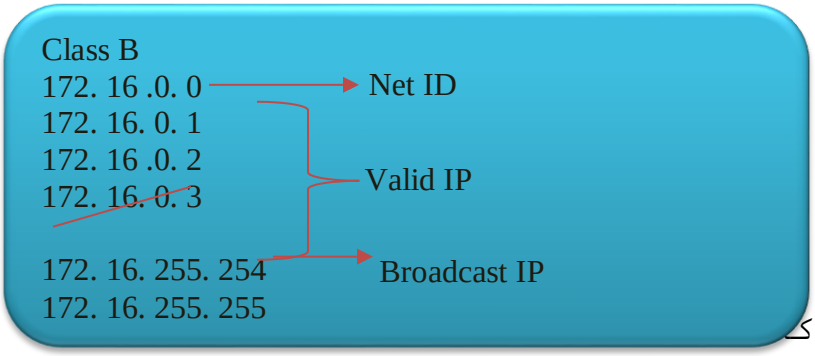
- کلاس A: N.H.H.H
  - Net ID:
    - 0xxxxxxxx. 00000000. 00000000. 00000000
  - Broadcast IP:
    - 0xxxxxxxx. 11111111. 11111111. 11111111



مثال برای کلاس B

- کلاس B: N.N.H.H
  - Net ID:
    - 10xxxxxx. xxxxxxxx. 00000000. 00000000

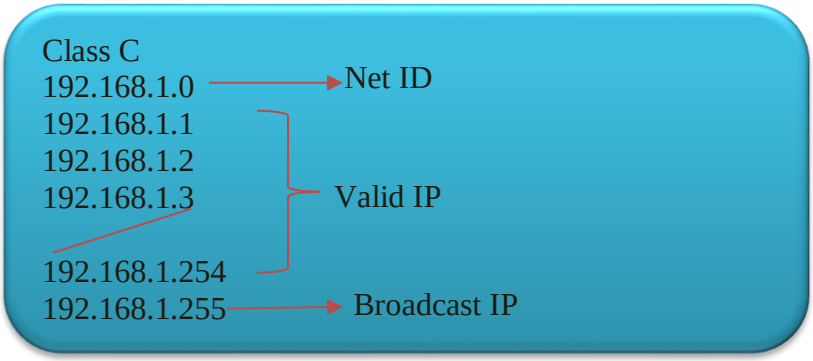
➢ Broadcast IP:
- 10xxxxxx. xxxxxxxx. 11111111. 11111111



مثال برای کلاس C:
- کلاس C: N.N.N.H

➢ Net ID:
- 110xxxxx. xxxxxxxx. xxxxxxxx. 00000000

➢ Broadcast ID:
- 110xxxxx. xxxxxxxx. xxxxxxxx. 11111111



مثال:

IP:192.168.20.10
Mask: 255.255.255.0

Network_ID: 192.168.20.0
First IP: Net_ID + 1 = 192.168.20.1
Last IP: Broadcast -1 = 192.168.20.254
Broadcast IP: Next Network – 1= 192.168.20.255

جدول 2-4 مثالی از شناسایی NetID و Broadcast IP از روی

IP Address	Net ID & Broadcast IP

120.1.1.1	120.0.0.0 & 120.255.255.255
172.16.1.1	172.16.0.0 & 172.16.255.255
10.100.1.10	10.0.0.0 & 10.255.255.255
192.168.1.10	192.168.1.0 & 192.168.1.255
150.10.1.1	150.10.0.0 & 150.10.255.255

Mask از نوع متغیر

Mask های از نوع استاندارد در دنیای واقعی زیاد کاربرد ندارند، برای مثال وقتی یک سازمانی 50 کامپیوتر دارد اگر بخواهد IPهایی از نوع Mask های استاندارد را خریداری کند، فقط از 50 عدد IP استفاده خواهد کرد و بقیه هدر خواهند رفت، بنابراین برای جلوگیری از اتلاف IP ها از Mask های متغیر استفاده می‌شود. در Mask های متغیر (یا Subneting) از یک شبکه‌ی مستقل، شبکه های جدیدی ایجاد می‌شود.
Subnet : شبکه‌ی مستقل با مشخصه‌ی IP
Subnetting : ایجاد شبکه های جدید از یک شبکه‌ی مستقل. یعنی در یک شبکه، Net ID را تغییر داد تا Net ID جدیدی استخراج شود که لزوما هرکدامیک از آن‌ها، Host ID های جدیدی دارند.

Net ID	+ Host ID
عدد 1 است و ثابت است.	متغیر است

برای انجام Subnetting از بیت‌های Host ID استفاده می‌شود. در واقع به تعداد بیتی که از Host ID استفاده می‌شود، عدد 0 تبدیل به 1 می‌شود و به Net ID افزوده می‌شود و Subnet جدید به‌دست می‌آید.

برای حل Mask های متغیر از سوالات زیر استفاده میکنیم:

1- به ازای IP و Mask داده شده، چه تعداد شبکه جدید قابل تعریف است:

$2^{Subnet\ Bits}$

Subnet Bits تعداد بیت‌های متغیر mask می‌باشد (بیت‌های متغیر همان بیت های 0 هستند که تبدیل به 1 شده اند)

2- به ازای هر شبکه جدید چه تعداد Host وجود دارد؟

$2^{Host\ Bits} - 2$

3- Net ID شبکه‌های جدید چه می‌باشد؟

$256 - Subnet\ Mask$

4- آدرس Broadcast برای هر شبکه چیست؟

$Next\ Subnet - 1$

5- اولين IP مورد استفاده براي هر شبكه چه مي باشد؟

$Net\ ID + 1$

6- آخرين IP مورد استفاده براي هر شبكه چيست؟

$Broadcast - 1$

- **Example : IP:192.168.10.0 , Mask:255.255.255.192.**

S:

255.	255.	255.	192
			11000000

1. $2^2 = 4\ Subnets$
2. $2^6 - 2 = 64 - 2 = 62$ يعني 4 شبكه داريم كه در هر كدام 62 آي پي جاي مي‌گيرد.
3. $256 - 192 = 64$
4. .

	A	B	C	D	...
Net_ID	0	64	128	192	...
First	1	65	129	193	...
Last	62	126	190	254	...
Broadcast	63	127	191	255	...

- **Example. IP:192.168.10.0, Mask: 255.255.255.224**

S:

255.	255.	255.	224
			11100000

1. $2^3 = 8\ Subnets$
2. $2^5 - 2 = 30\ Host$
3. 256-224=32
4. .

	A	B	C	D	E	F
Net_ID	32	64	96	128	160	192
First	33	65	97	129	161	193
Last	62	94	126	158	190	222
Broadcast	63	95	127	159	191	223

- **Example. IP:192.168.10.0 , Mask: 255.255.255.240**

S:

255.	255.	255.	240
			11110000

5. $2^4 = 16\ Subnets$
6. $2^4 - 2 = 14\ Host$
7. 256-240=16
8. .

	A	B	C	D	E	F
Net_ID	16	32	48			
First	17	33				
Last	30	45				
Broadcast	31	47				

- **Example. IP:192.168.10.0 , Mask: 255.255.255.252**

S:

255.	255.	255.	252
			11111100

9. $2^6 = 64\ Subnets$
10. $2^2 - 2 = 2\ Host$
11. 256-252=4
12. .

	A	B	C	D	E	F
Net_ID	4	8	12	16		
First	5	9	13			
Last	6	10	14			
Broadcast	7	11	15			

- مثال: اگر يك IP بصورت 192.168.10.64 موجود باشد، Mask تعريف شده براي آن بصورت 255.255.255.192 است. آيا Mask داده شده با توجه به IP موجود صحيح است؟ و آيا IP:192.168.10.68 مي‌تواند Net_ID باشد؟
  - آدرس Broadcast براي اين شبكه چيست؟
  - رنج قابل استفاده براي كاربران شبكه چه مي‌باشد؟

255.	255.	255.	192	
			11000000	⇨ /26

1. $2^2 = 4\ Subnets$

2. $2^6 - 2 = 62\ Host$
3. 256-192=64
4. .

	A	B	C	D	E	F
Net_ID	**64**	**128**	**192**			
First IP	**65**	**129**				
Last IP	**126**	**190**				
Broadcast	**127**	**191**				

192.168.10.64غلط است. زيرا 192.168.10.64، به عنوان Net ID مي‌باشد و نمي‌تواند آدرس IP سيستمي در شبكه باشد.
IP:192.168.10.68نمي‌تواند Net_ID باشد اما مي‌تواند IP يك سيستم باشد.

- **Example . <u>IP: 192.168.10.38</u> و <u>Mask:255.255.255.240</u>**

S:

255.	255.	255.	192	
			11110000	⇨ **<u>/28</u>**

1. $2^4 = 16$ تعداد شبكه هايي كه مي‌توانيم داشته باشيم.
2. $2^4 - 2 = 14$ تعداد تجهيزاتي كه مي‌توانيم در هر شبكه داشته باشيم.
3. **256-240=16** طول گام ها

	1th Subnet	2th Subnet	3th Subnet	4th Subnet	…	16th ...Subnet
Net_ID:	**0**	**16**	**32**	**48**	…	…
First IP:	**1**	**17**	**33**		…	
Last IP:	**14**	**30**	**46**		…	
Broadcast	**15**	**31**	**47**	**48-1=47**	…	

- **Example. <u>IP: 192.168.10.13</u> و <u>Mask:255.255.255.252</u>**

حل:

1. **255-252=3** ⇨2^2 ⇨00 ⇨ **<u>11111111. 11111111. 11111111.11111100</u>**⇨ **<u>/30</u>**
2. **8-6=2**

3. $2^6 = 64$ تعداد شبکه‌هایی که می‌توانیم داشته باشیم.
4. $2^2 - 2 = 2$ تعداد تجهیزاتی که می‌توانیم در هر شبکه داشته باشیم.
5. 256-252=4 طول گام‌ها

	1th S.	2th S.	3th S.	4th S.	16th S.
Net_ID:	**0**	**4**	**8**	**12**	**…**
First IP:			**9**		
Last IP:			**10**		
Broadcast			**11**		

- مثال: اگر یک IP در کلاس C موجود باشد، از چه Mask ی استفاده کنیم تا به ازای هر شبکه تعداد 35، Host موجود باشد؟

32<	35	<64
2^5		2^6

Host<$2^n - 2$

35<$2^6 - 2$ ⇨ 11111111. 11111111. 11111111.11**000000**

تعداد هاست‌ها از راست به چپ شمرده می‌شود.

به تعداد 6 بیت باید از سمت راست به چپ شمرده شود و جدا گردد (صفر می‌گذاریم).

11111111.	11111111.	11111111.	11000000
255.	255.	255.	192

- **Example. IP: 192.168.20.18, Mask: 255.255.255.224**

S:

1. 255-224=31 ⇨2^5 ⇨00000 ⇨ 11111111. 11111111. 11111111.11100000 ⇨/27
2. $2^3 = 8$
3. $2^5 - 2 = 30$
4. 256-224=32

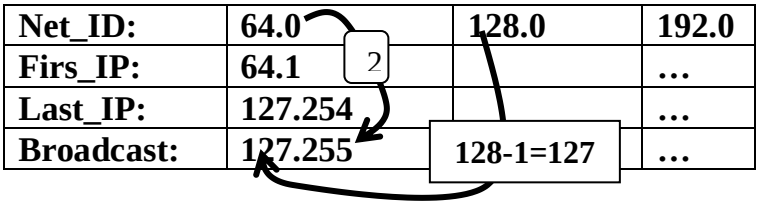
- **Example. IP:172.16.0.0, Mask:255.255.192.0**

S:

255.	255.	192.	0
		11000000	00000000

1. $2^2 = 4$
2. $2^{14} - 2 = 16,382$
3. 256-192=64.0

Net_ID:	0.0	64.0	128.0	192.0	
Firs_IP:	0.1	64.1	128.1	…	
Last_IP:	63.254	127.254	192.254	…	
Broadcast:	63.255	127.255	191.255	…	



2 ⇨ صفرها تبدیل به یك مي شوند.

Net_ID: 64.0 ⇨Broadcast: 127.255

جدول 2-5 تـعداد هاستهای موجود و دسیمال Subnet mask از Prefix فرمت

Prefix Format	Decimal	Available Host Addresses
/8	255.0.0.0	16777214
/9	255.128.0.0	8388606
/10	255.192.0.0	4194302
/11	255.224.0.0	2097150
/12	255.240.0.0	1048574
/13	255.248.0.0	524286
/14	255.252.0.0	262142
/15	255.254.0.0	131070
/16	255.255.0.0	65534
/17	255.255.128.0	32766
/18	255.255.192.0	16382
/19	255.255.224.0	8190
/20	255.255.240.0	4094
/21	255.255.248.0	2046
/22	255.255.252.0	1022
/23	255.255.254.0	510
/24	255.255.255.0	254
/25	255.255.255.128	126
/26	255.255.255.192	62
/27	255.255.255.224	30
/28	255.255.255.240	14
/29	255.255.255.248	6
/30	255.255.255.252	2

جدول 2-6 شناسایی Subnet mask و wildcard

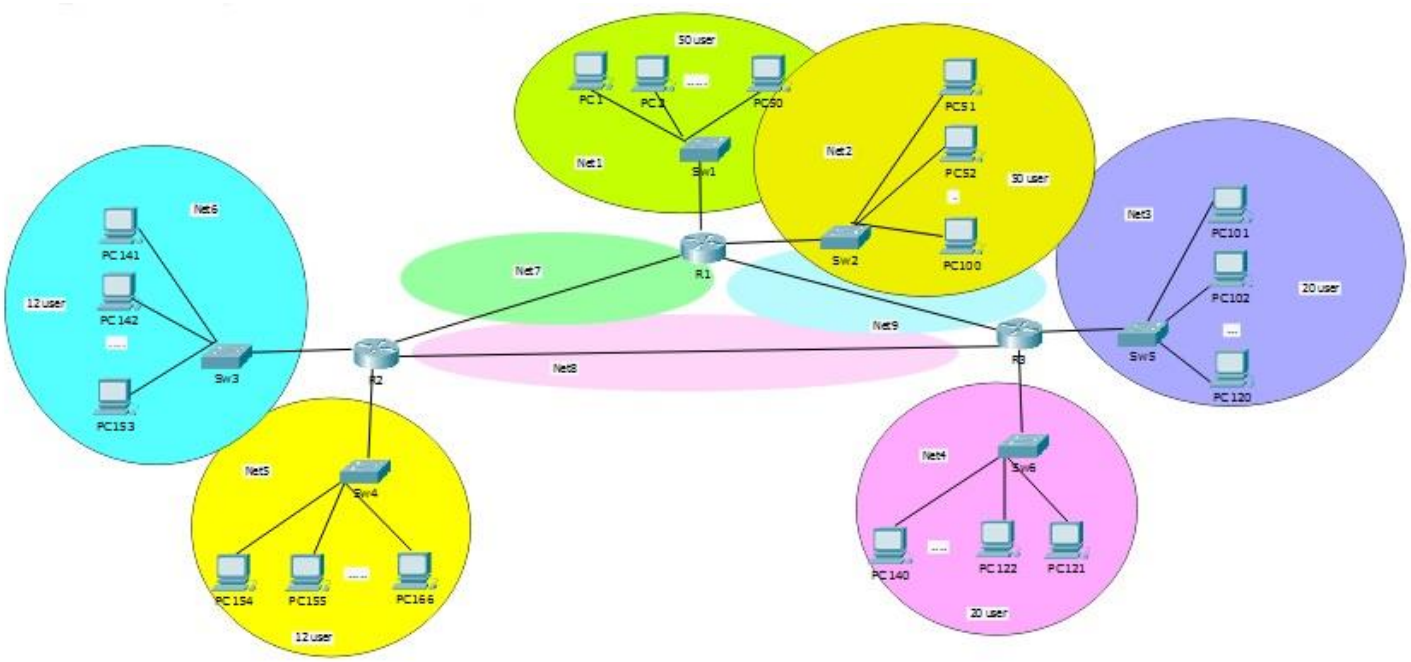
	Net Mask	Net Mask	Wildcard
.10000000	/25	128	127
.11000000	/26	192	63
.11100000	/27	224	31
.11110000	/28	240	15
.11111000	/29	248	7
.11111100	/30	252	3
.11111110	/31	254	1

VLSM[1]

- ایجاد زیر شبکه‌های جدید از یک زیر شبکه با اندازه‌های مختلف ، VLSM نامیده می‌شود.
- VLSM قابلیت ارائه‌ی بیش از یک Subnet mask درون یک شبکه‌ی بزرگ را دارد.

مثال: در یک دانشگاهی 3 دانشکده وجود دارد که هرکدام دارای ساختمان جداگانه‌ای بوده و هر ساختمان دو طبقه می‌باشد. در هر طبقه تعدادی کاربر وجود دارد. برای ارتباط کاربران یک دانشکده با دانشکده‌ی دیگر در هر ساختمان یک روتر و در هر طبقه‌ای یک سوئیچ قرار داده شده است(2 سوئیچ در هر ساختمان). با توجه به IP:192.168.1.0/24 و تعداد کاربران موجود در هر طبقه در شکل زیر، subnetting را انجام دهید.

دو سوئیچ: 50 کاربر، دو سوئیچ: 20 کاربر، دو سوئیچ: 12 کاربر



حل:

برای حل این نوع سوالات بهتر است از IP با تعداد user بیشتری شروع کنیم، بنابراین با 50 کاربر شروع می‌کنیم. ابتدا باید n را در

[1] Variable Length Subnet Mask

فرمول تعداد هاست به دست بیاوریم. تا تعداد بیت‌های هاست معلوم شود.

$$Host \leq 2^n - 2$$

$$1.\ 50 \leq 2^n - 2 \rightarrow n = 6$$

پس به تعداد 6 بیت 0 و به تعداد 2 بیت 1 وجود دارد. بنابراین :

Subnet mask

255.	255.	255.	192	
			11000000	⇨/26

$$2.\ 2^2 = 4$$ تعداد

3. 256-192=64 تعداد

	A	B	C	D
Net_ID	0	64	128	192
First_IP	1	65	129	193
Last_IP	62	126	190	254
Broadcast	63	127	191	255

چون به دو شبکه نیاز داریم نه 4 شبکه، پس دو شبکه‌ی موجود A و B را به اختیار از بین 4 شبکه‌ی موجود انتخاب می‌کنیم، بنابراین:

شبکه اول	192.168.1.0/26
شبکه دوم	192.168.1.64/26

هر دو شبکه 50 کاربر را پشتیبانی می‌کنند.

شبکه های موجود براساس 20 کاربر

$$1.\ 20 \leq 2^n - 2 \rightarrow n = 5$$

Subnet mask

255.	255.	255.	224	
			11100000	⇨ /27

2. $2^3 = 8$ تعداد

3.256-224=32 تعداد گام ها

برای به‌دست‌آوردن شبکه برای 20 کاربر می‌توان از شبکه‌ی C یا D استفاده کرد. ما از شبکه‌ی C به‌طور اختیاری استفاده کردیم.

چون به تعداد 2 شبکه نیازمندیم بنابراین از 8 شبکه2 شبکه را انتخاب می‌کنیم.

	C_1	C_2	C_3	....
Net_ID	128	160	192	
First_IP	129	161	193	
Last_IP	158	190	222	
Broadcast	159	191	223	

بنابراین شبکه‌های مورد نظر برای 20 کاربر عبارتند از:

شبکه اول	192.168.1.128/27
شبکه دوم	192.168.1.160/27

شبکه‌های موجود براساس 12 کاربر

برای به‌دست‌آوردن شبکه‌های 12 کاربر هم همانند مراحل قبل استفاده می‌کنیم.

1. $12 \leq 2^n - 2 \rightarrow n = 4$

تعداد

Subnet mask

255.	255.	255.	240	
			11110000	⇨ /28

2. $2^4 = 16$

تعداد

3.256-240=16

برای به‌دست‌آوردن شبکه‌های 20 کاربر از شبکه‌های C_3 استفاده می‌کنیم.
بنابراین:

	C_{31}	C_{32}	C_{33}	C_{34}
Net_ID	**192**	**208**	**224**	**240**
First_IP	**193**	**209**	**225**	…
Last_IP	**206**	**222**	**238**	
Broadcast	**207**	**223**	**239**	

چون به دو شبکه نیازمندیم، دو شبکه را فقط انتخاب می‌کنیم.
بنابراین شبکه‌ها عبارتند از:

شبکه اول	**192.168.1.192/28**
شبکه دوم	**192.168.1.208/28**

شبکه‌های موجود بین روترها

حال برای به دست‌آوردن شبکه های بین دو روتر باز همان مراحل قبلی را تکرار می‌کنیم. در این قسمت 3 شبکه می‌خواهیم که هرکدام نیازمند 2 آدرس می‌باشد، بنابراین باید n را برای 2 هاست به دست بیاوریم.

1. $2 \leq 2^n - 2 \rightarrow n = 2$

Subnet mask

255.	255.	255.	252	
			11111100	⇨ /30

2. $2^6 = 64$ تعداد
3. 256-252=4 تعداد

برای به دست آوردن شبکه‌های بین روترها از شبکه های C_{33} استفاده کردیم.

	C_{331}	C_{332}	C_{333}	C_{334}
Net_ID	224	228	232	236
First_IP	225	229	233	...
Last_IP	226	230	234	
Broadcast	227	231	235	

بنابراین شبکه‌های مورد نظر عبارتند از:

شبکه اول	192.168.1.224/30
شبکه دوم	192.168.1.228/30
شبکه سوم	192.168.1.232/30

در حالت کلی تمام شبکه‌های به‌دست آمده به‌صورت زیر می‌باشد:

192.168.1.0/26	192.168.1.160/27	192.168.1.224/30
192.168.1.64/26	192.168.1.192/28	192.168.1.228/30
192.168.1.128/27	192.168.1.208/28	192.168.1.232/30

فصل3
مفاهیم اولیه روتر و سوئیچ

روتر[1]

روترها دستگاه‌هایی با نام مسیریاب می‌باشند که وظیفه‌ی اتصال شبکه‌های مختلف یا مسیریابی بین شبکه‌های مختلف را بر عهده دارند.

- روتر یک دستگاه لایه شبکه (لایه 3) می‌باشد.
- روتر دستگاهی است که بهترین مسیر برای رسیدن به شبکه‌ها را پیدا می‌کند.
- IP ی روتر به عنوان Gateway پیش فرض برای همه‌ی دستگاه‌های واقع در شبکه LAN می‌باشد.

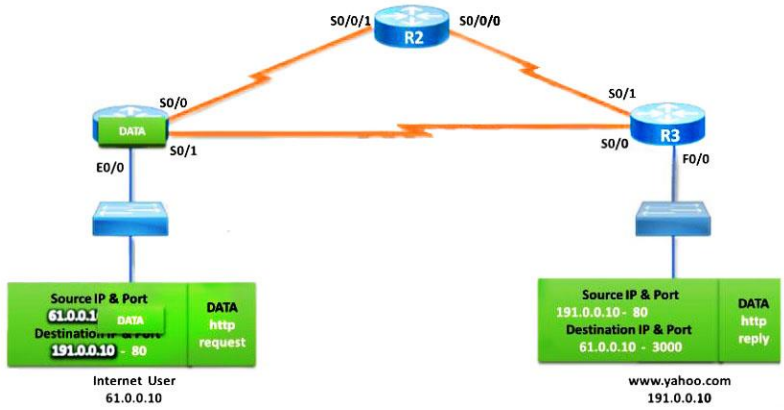
انواع روتر

دو نوع روتر وجود دارد:

- **روترهای سخت‌افزاری**
  - مثل: Cisco، HP، Dlink، juniper و ...
- **روترهای نرم‌افزاری**
  - مثل: سرور مایکروسافت، سرور لینوکس

عملکرد روتر

- ارتباط بین شبکه ای[2]
- انتخاب بهترین مسیر
- سوئیچینگ بسته
- ارسال بسته[3]



شکل 3-1 نحوه‌ی عملکرد روتر به

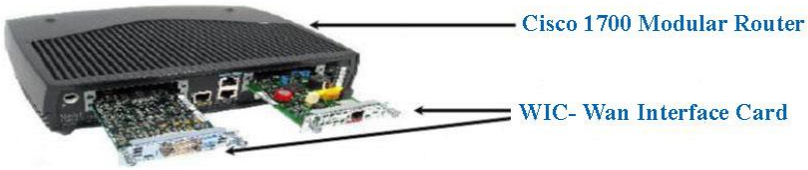
روترهای سخت افزاری

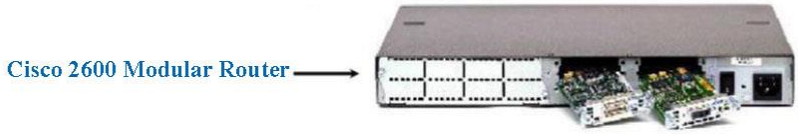
- **روتر ثابت**

[1] router
[2] Inter–network communication
[3] Packet Forwarding

شکل 3-2 یک نمونه از

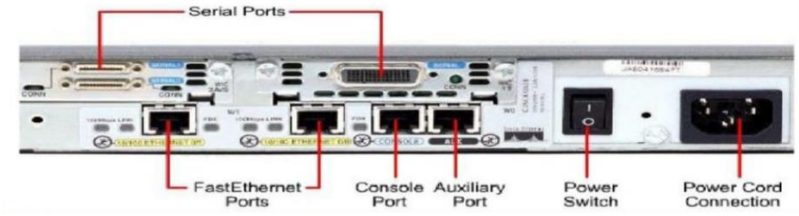
- روتر ماژولار





شکل 3-3 نمونه‌هایی از روترهای ماژولار سیسکو

اجزای خارجی روتر



شکل 3-4 اجزای خارجی

اجزای خارجی روتر به شرح زیر می‌باشد:

- **AUI**[1]

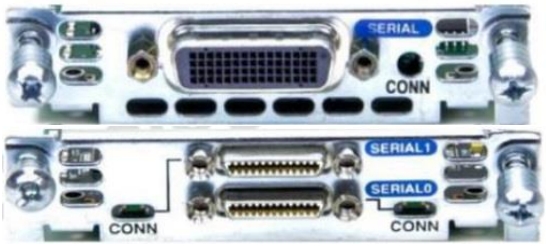
- برای اتصال روتر به LAN استفاده می‌شود.
- به عنوان اینترفیس اترنت نیز نامگذاری شده است.
- Transceiver برای اتصال پورت AUI به هاب/سوئیچ LAN استفاده می‌شود.

Transceiver

[1] Attachment Unit Interface

- Transceiver، سیگنال DB-15 را به RJ-45 تبدیل می‌کند.

- **پورت‌های RJ-45**
  - روترها پورت‌های RJ-45 را برای کانکت شدن به LAN دارند.
  - سرعت پورت‌های RJ-45 می‌تواند:
    - 10 Mbps :Ethernet
    - 10/100 Mbps :Fast Ethernet
    - 10/100/1000 Mbps :Gigabit Ethernet



- **پورت سریال**
  - پورت سریال برای اتصال WAN استفاده می‌شود.
  - کابل V.35 برای کانکت پورت سریال روتر به leased line مودم (CSU/DSU) استفاده می‌شود.

شکل 3-5 نمونه هایی از

- **HWIC**[1]
  - HWIC، اتصال به WAN را فراهم می کند.

- **پورت کنسول**
  - یک پورت اجرایی می‌باشد.
  - یک پورت RJ-45 است.
  - برای کانفیگ اولیه و عیب‌یابی پیشرفته استفاده می‌شود.
  - این پورت، مهم‌ترین و حساس‌ترین پورت روی روتر است.

تبدیل کننده DB-9
[1] High-speed WAN Interface Card

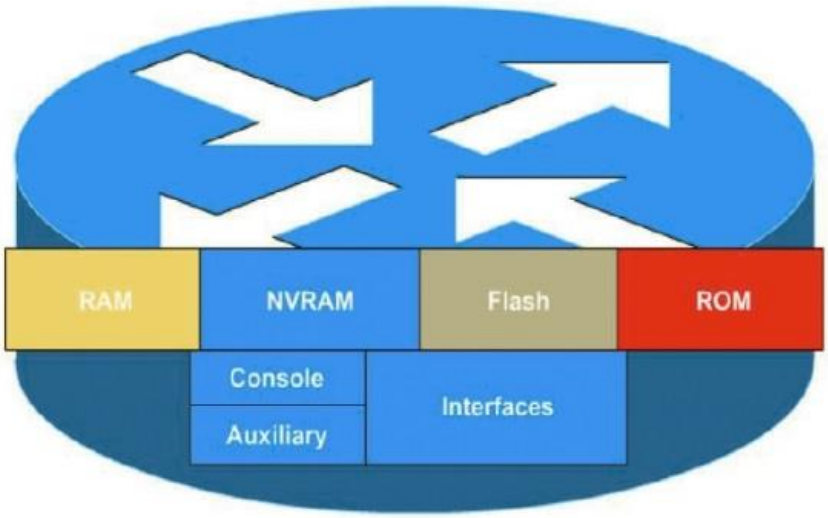
کابل کنسول

- **پورت Auxiliary**

- یک پورت اجرایی از راه دور می‌باشد.
- برای کانفیگ/ اجرا از راه دور استفاده می‌شود.
- یک پورت RJ-45 است.
- یک کابل console/ rollover برای کانکت پورت Auxiliary به مودم Dial-up استفاده می‌شود.

اجزای داخلی روتر

اجزای داخلی روتر عبارتست از:



- **RAM**: وظیفه‌ی ایجاد حافظه‌ی موقت برای اجرا کردن دستورات روی سیستم را بر عهده دارد. RAM در روتر به حافظه‌ی کوتاه مدت اطلاق می‌شود و با نامی به نام running-config (حافظه ی در حال اجرا) شناخته می‌شود.

- **NVRAM**[1]: حافظه‌ی بلند مدت بوده و با نام startup-config شناخته می‌شود. NVRAM مانند سیستم عامل یک کامپیوتر می‌باشد، یعنی زمانی که دستگاه start شود تمامی دستوراتی که بر روی سیستم اجرا شده است را می‌توان با startup-config مشاهده نمود. اگر NVRAM در روتر نباشد، روتر بوت نخواهد شد.

نکات

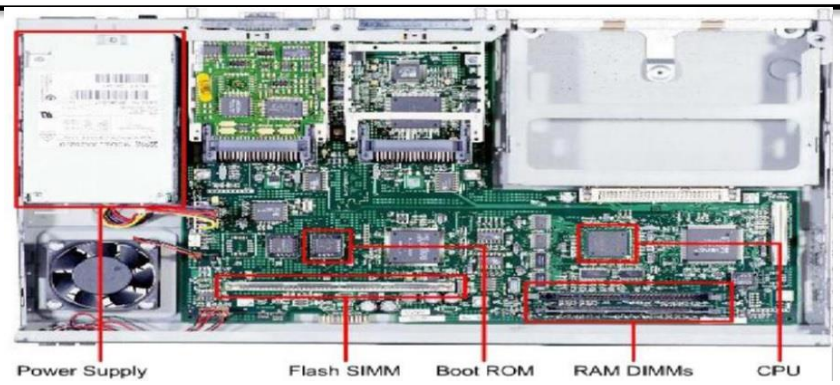
- حافظه‌ی بلند مدت و کوتاه مدت دو حافظه‌ی مجزا می‌باشند.
- در حافظه‌ی بلند مدت اطلاعات به صورت دائمی ذخیره و نگهداری می‌شود، بنابراین اگر دستوری در یک دستگاهی اجرا شود باید از حافظه‌ی کوتاه مدت به حافظه‌ی بلندمدت منتقل شود تا به صورت دائمی باقی بماند در غیر این صورت اگر سیستم خاموش شود، اطلاعات حافظه‌ی کوتاه مدت از بین خواهد رفت.

- **ROM**: تقریبا شبیه به ROM کامپیوتر بوده و وظیفه‌ی کنترل اجزای سخت افزاری سیستم مثل Bios و بوت سیستم را برعهده دارد. شامل یک ROMMON برای عیبیابی پیشرفته است.

- **Flash**: وظیفه‌ی نگهداری سیستم عامل روتر[2] و فایل‌های بوت logical سیستم را بر عهده دارد.

IOS فایلی با پسوند .bin می‌باشد در واقع یک Image ای است که شامل دستورات قابل اجرایی می باشد .

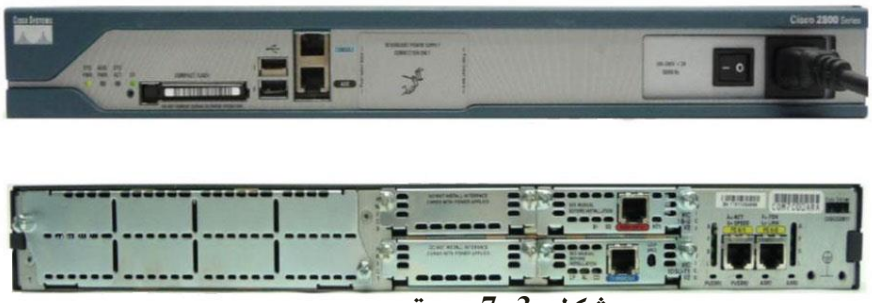
[1] Non Volatile Random Access Memory
[2] IOS



شکل 3-6 نمایی از شمای داخلی یک

نکات

- روترهای سیسکو از سری 800 تا 12000 می باشند.
- روتر سری 800 در یک Office کوچک استفاده می‌شود.
- روتر سری 12000 در backbonke اینترنت استفاده می شود.
- روتر 2851 یعنی: روتر از سری 2800، مدل 51
- روتر 2811یعنی: روتر از سری 2800، مدل 11



شکل 3-7 روتر سری 2800

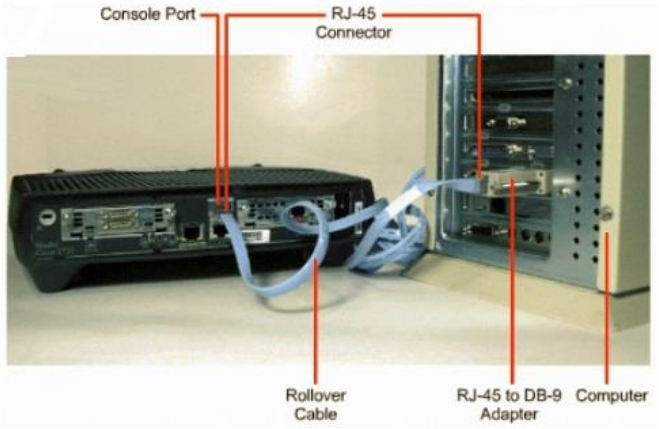
روشهای اتصال به روتر

روشهای اتصال به روتر به 3 دسته تقسیم می‌شود:

1) **Console:** اولین روش اتصال به روتر استفاده از کابل کنسول می‌باشد. در شکل زیر نمونه‌ای از این کابل نشان داده شده است.

شکل 3-8 کابل

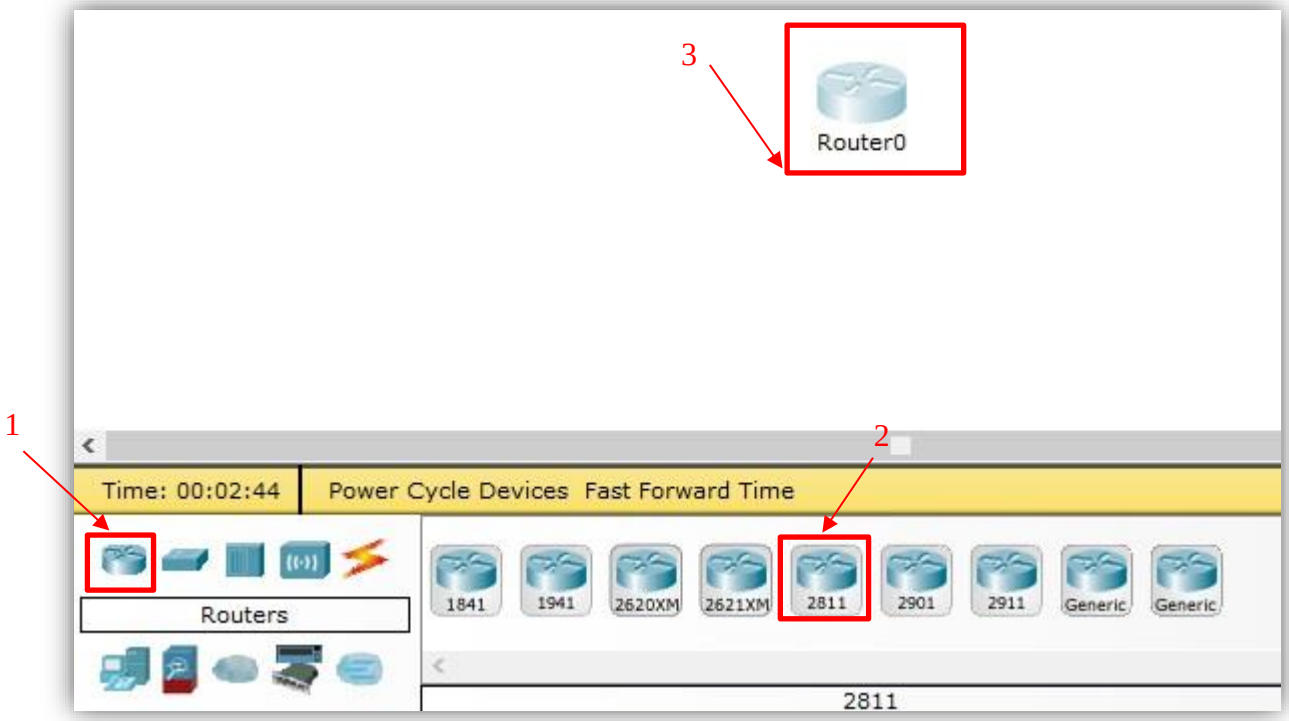
همان‌طور که در شکل(3-8) می‌بینیم، این کابل از یک سمت با نام DB-9 به پورت COM کامپیوتر و از سمت دیگر با نام RJ-45 به پورت Console روتر وصل می‌شود و اجازه‌ی ارتباط با سیستم را می‌دهد.



شکل 3-9 روش اتصال

روش اتصال کنسول در Packet tracer

1. ابتدا نرم افزار packet tracer را باز کرده سپس بر روی Router کلیک کرده و از روترهای نشان داده شده ، روتر 2811 را انتخاب کرده و بر روی صفحه drag می‌کنیم.

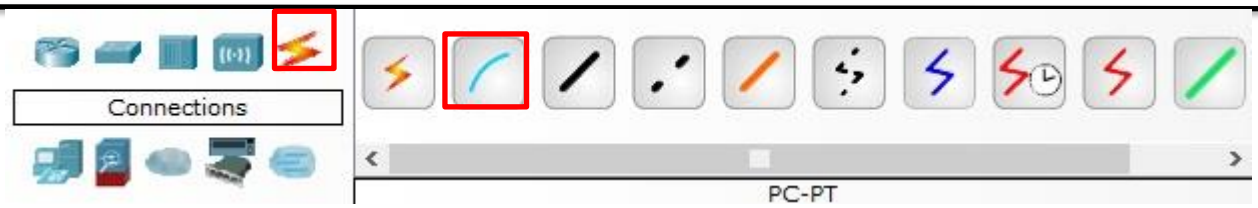


شکل 3-10 طریقه‌ی انتخاب روتر در Packet Tracer

2.بعد از قرار دادن روتر، روتر باید از طریق یک کامپیوتر ترمینال کند. بنابراین از طریق End Device، کامپیوتر را انتخاب کرده و بر روی صفحه قرار می‌دهیم.

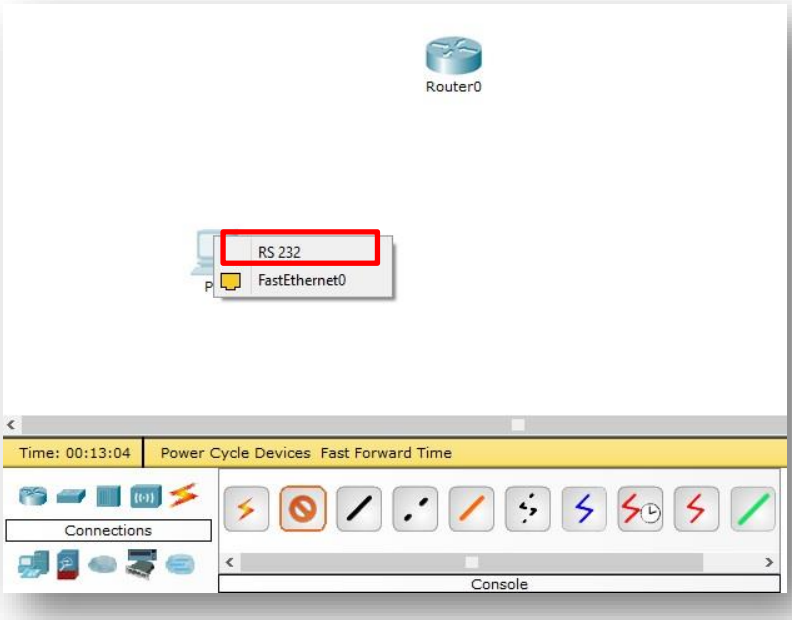
شکل 3-11 طریقه‌ی انتخاب PC در Packet Tracer

3.برای ارتباط بین کامپیوتر و روتر باید کابل کنسول را انتخاب کنیم. برای انتخاب کابل کنسول از قسمت Connection، کابل Console را انتخاب می‌کنیم.



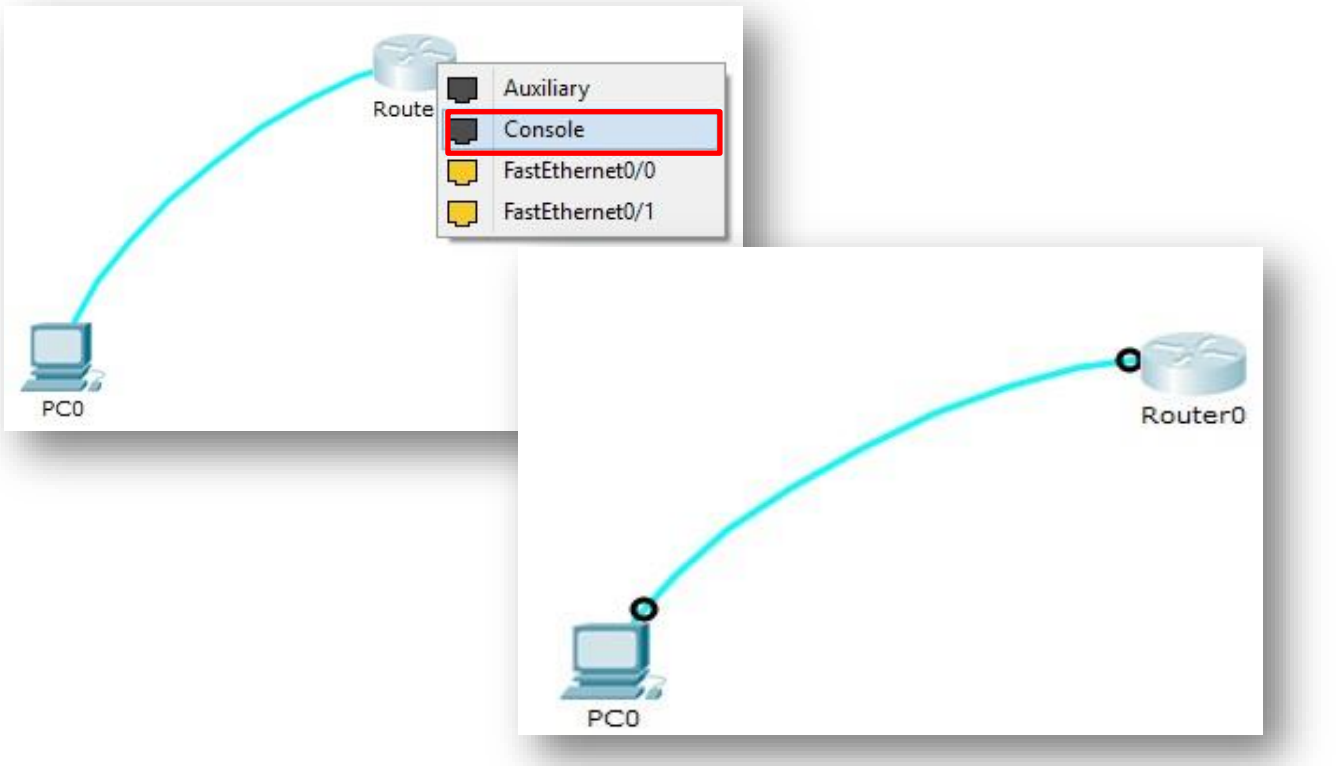
شکل 3-12 طریقه‌ی انتخاب کابل کنسول در

4. سپس بر روی کامپیوتر کلیک کرده و گزینه‌ی RS232 (منظور همان پورتCOM می‌باشد) را انتخاب می‌کنیم.



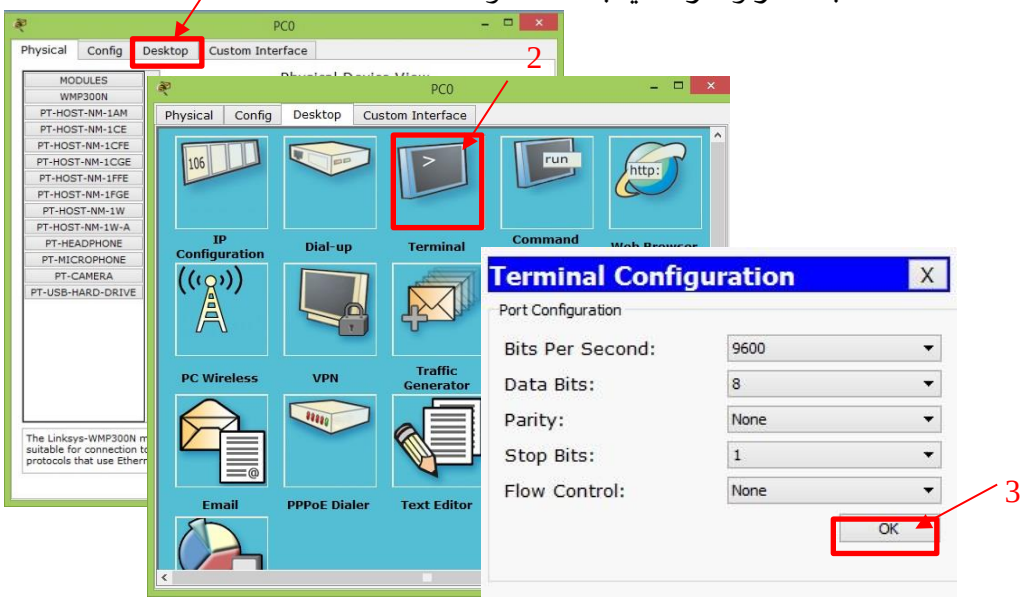
شکل 3-13 نحوه‌ی اتصال پورتCOM به روتر در Packet

5. سپس بر روی روتر کلیک کرده و گزینه‌ی Console را انتخاب می‌کنیم. وقتی گزینه‌ی Console را می‌زنیم، کابل اتصال پیدا می‌کند.

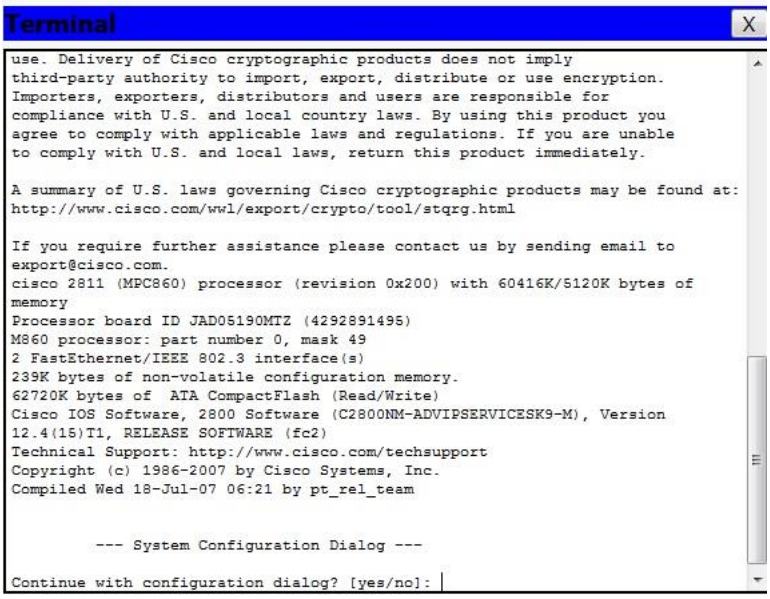


شکل 3-14 نحوه‌ی انتخاب کابل کنسول در Packet Tracer

6.سپس بر روی PC دابل کلیک کرده، صفحه‌ای همانند شکل زیر باز می‌شود، وارد تب Desktop شده و گزینه‌ی Terminal را انتخاب می‌کنیم. بعد از انتخاب گزینه‌ی Terminal و باز شدن صفحه‌ی Terminal Configuration، گزینه‌ی OK زده می‌شود تا اتصال به روتر ایجاد شود.

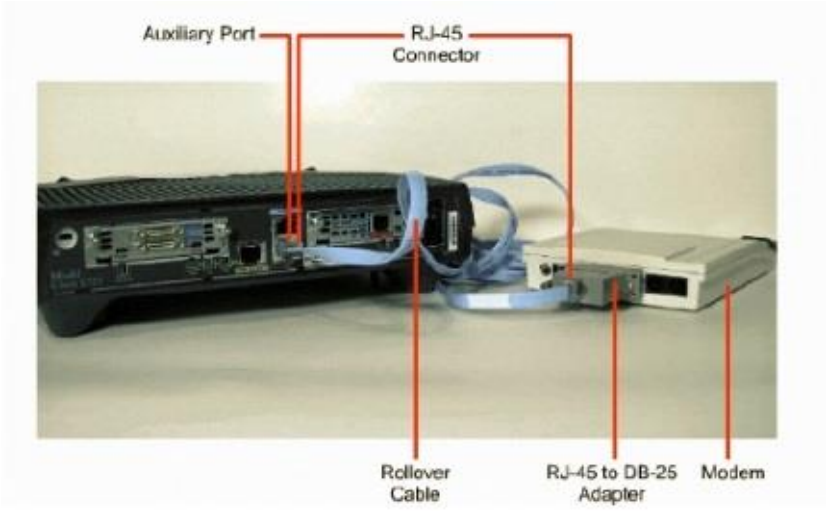


4



شکل 3-15 اتصال PC به روتر

2) **Auxiliary:** دومین روش اتصال به روتر به‌صورت Auxiliary می‌باشد. در این ساختار از خطوط تلفنی استفاده می‌شود. در روتر پورتی به نام AUX یا Auxiliary قرار گرفته است که به پورت DB-25 مودم وصل می‌شود، سپس مودم با پورت Rj-11 به خط تلفنی وصل می‌شود.



شکل 3-16 اتصال به روتر با استفاده از پورت Auxiliary

در واقع در این روش وقتی کاربری خواست به یک روتر وصل شود، یک کانکشن Dialup ایجاد می‌کند، سپس شماره تلفن مودم را وارد می‌کند و از طریق خط تلفنی متصل می‌شود. پس اگر زمانی هیچ خط ارتباطی نباشد از این طریق می‌توان به روتر وصل شد.

3) Interface: سومین روش اتصال به روتر ، اینترفیس می‌باشد.

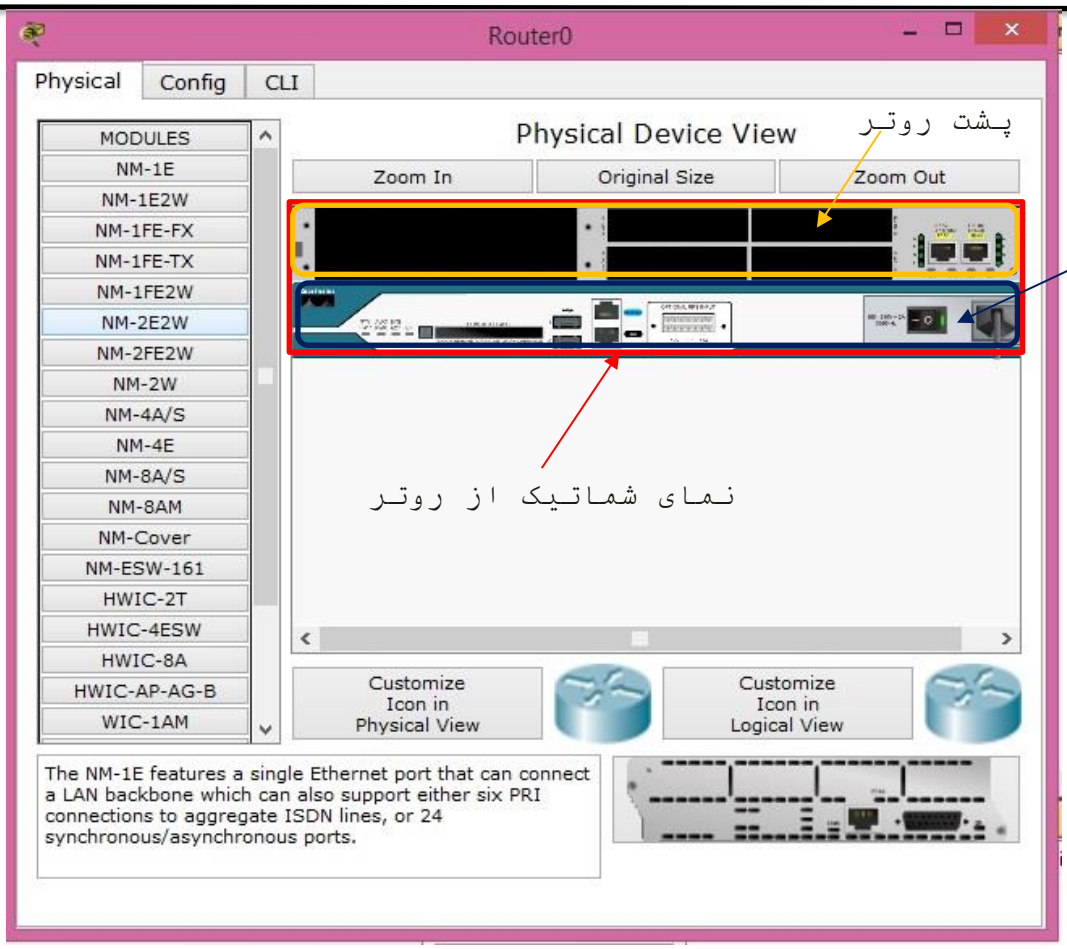
اینترفیس: درگاه های اتصال روتر می‌باشد. اینترفیس‌ها به 3 دسته تقسیم می‌شوند:

- اینترفیس LAN
  - AUI 10Mbps
  - RJ 45 Ethernet/ FastEthernet/ Gigabit Ethernet
- اینترفیس WAN
  - اینترفیس سریال نرمال
  - اینترفیس سریال کوچک
- اینترفیس اجرایی
  - Console
  - Auxiliary

اینترفیس‌های اترنت

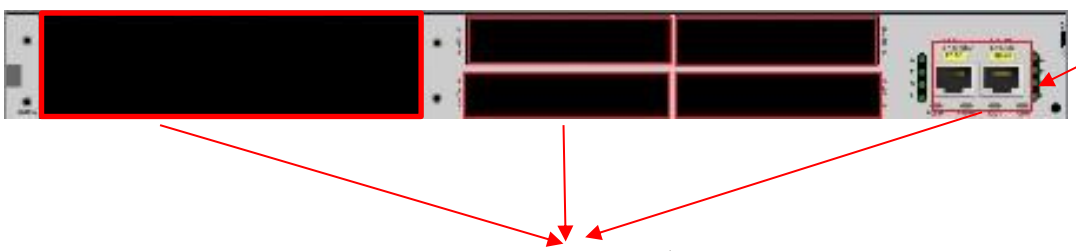
اترنت در شبکه های LAN وجود دارد. درگاه اترنت برای اتصال روتر به سوئیچ استفاده می‌شود (در شبکه هایLAN از درگاه اترنت برای اتصال به سوئیچ استفاده می‌شود، سوئیچ اترنت را می‌شناسد).

برای مشاهده‌ی طرح شماتیک از روتر، اگر در نرم افزار Packet tracer بر روی روتر کلیک کنیم، صفحه ای همانند شکل(3-17) باز می‌شود.



شکل 3-17 نمایی شماتیک از روتر

جایگاه اینترفیس‌ها در شکل (3-18) مشخص شده است.



شکل 3-18 جایگاه اینترفیس‌ها

اینترفیس‌های اترنت به دو صورت FastEthernet و GigaEthernet می‌باشد. تفاوت این دو در سرعت می‌باشد. در FastEthernet نرخ داده برابر 100Mbps و در GigaEthernet برابر 1000 Mbps می‌باشد.

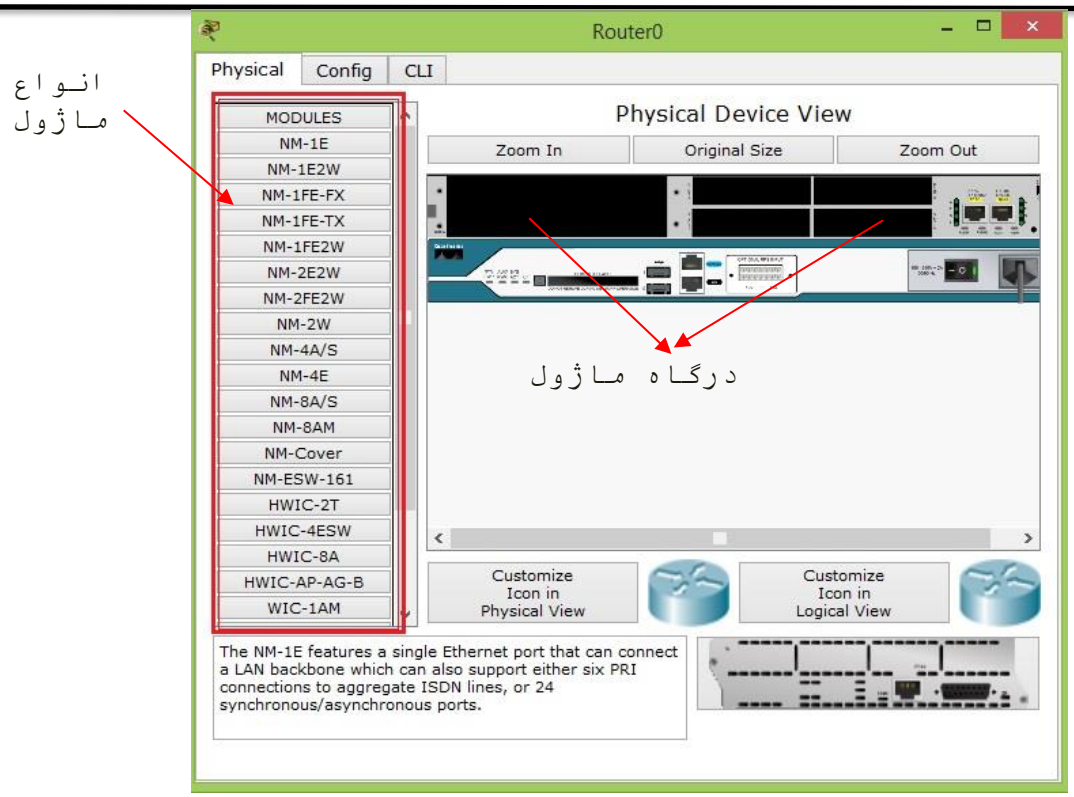
کابل‌های FastEthernet را باید به پورت FastEthernet و کابل‌های GigaEthernet را باید به پورت GigaEthernet وصل کرد، در غیر این‌صورت هیچ اتفاقی نمی‌افتد چون از نظر سرعت ساپورت نمی‌شود.

اینترفیس‌های سریال

کابل‌های سریال روی روترها برای اتصال درگاه‌های سریال نسبت بهم استفاده می‌شود(برای اتصال روترها استفاده می‌شود)

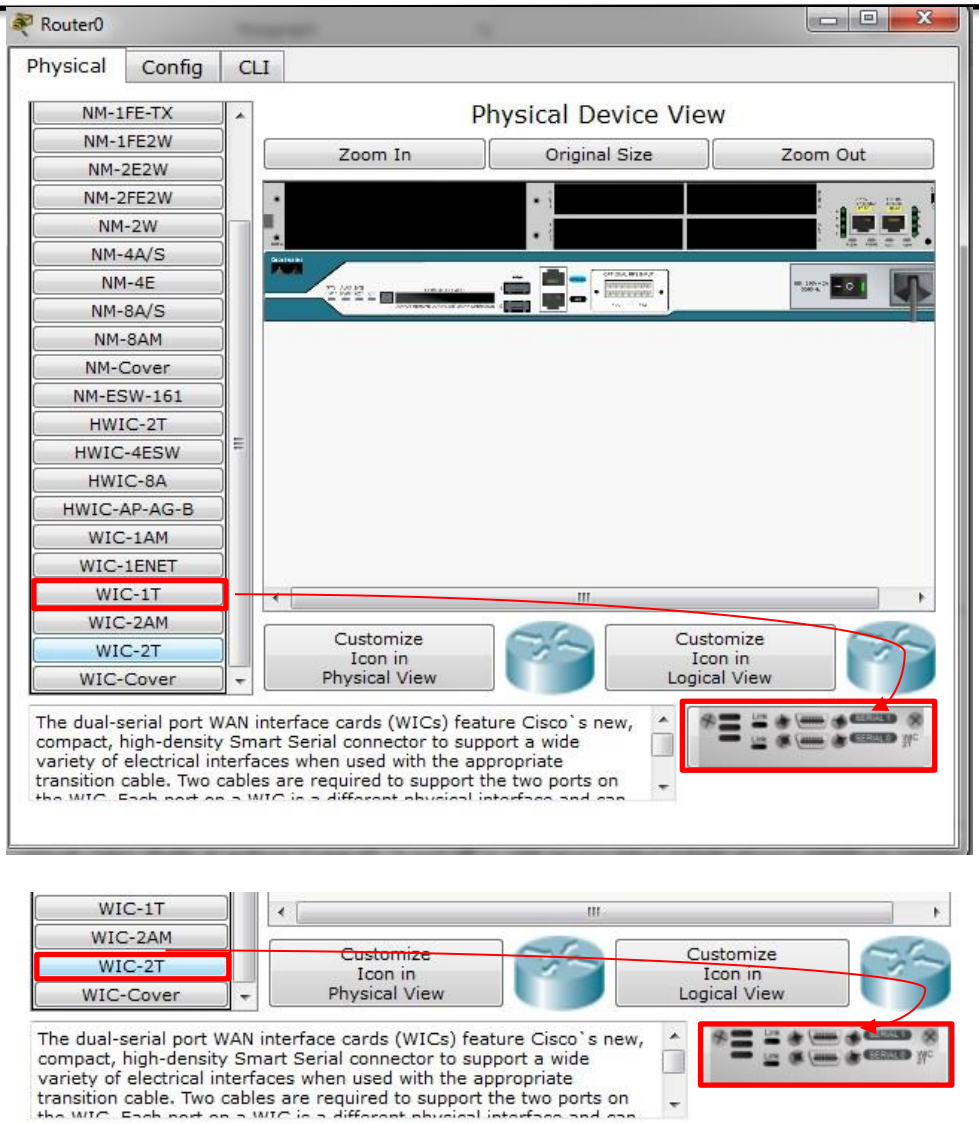
نحوه ی استفاده از اینترفیس‌های سریال

در شکل (3-19)، درگاه‌های مشکی رنگ وجود دارند که درگاه قرار دادن ماژول می‌گویند. به روتری که درگاه ماژول داشته باشد، روتر ماژولار می‌گویند. در سمت چپ شکل، لیست انواع ماژول‌ها قرار داده شده است.



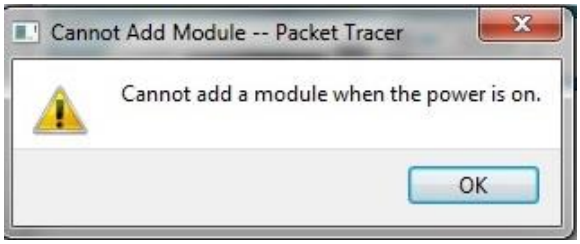
شکل 3-19 درگاه و انواع ماژول در

ماژول‌هایی به‌نام WIC-1T (با یک پورت سریال) و WIC-2T (با دو پورت سریال) وجود دارند که با کلیک بر روی منوی هرکدامیک از آن‌ها می‌توان تصویرش را مشاهده نمود.



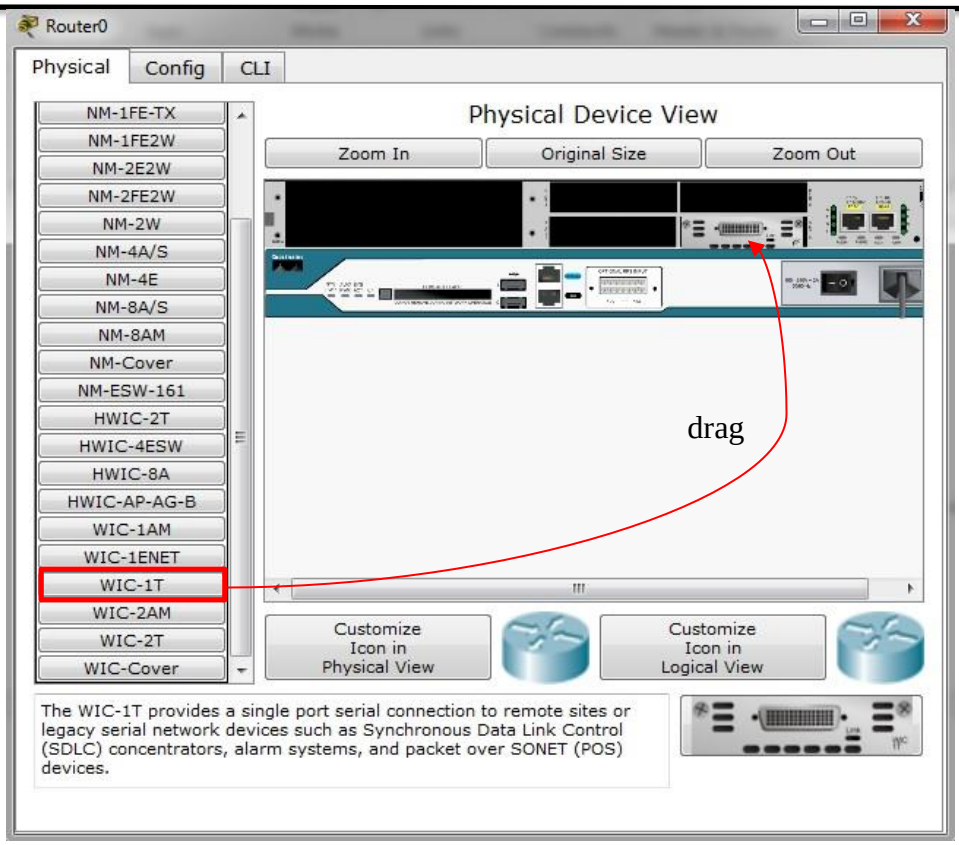
شکل 3-20 مشاهده ی ماژول در Packet

برای استفاده کردن از هرکدامیک از ماژولها ابتدا باید دکمه‌ی خاموش دستگاه  را بزنیم وگرنه هنگام drag ماژول در درگاه پیغام خطای شکل (3-21) مشاهده خواهد شد.



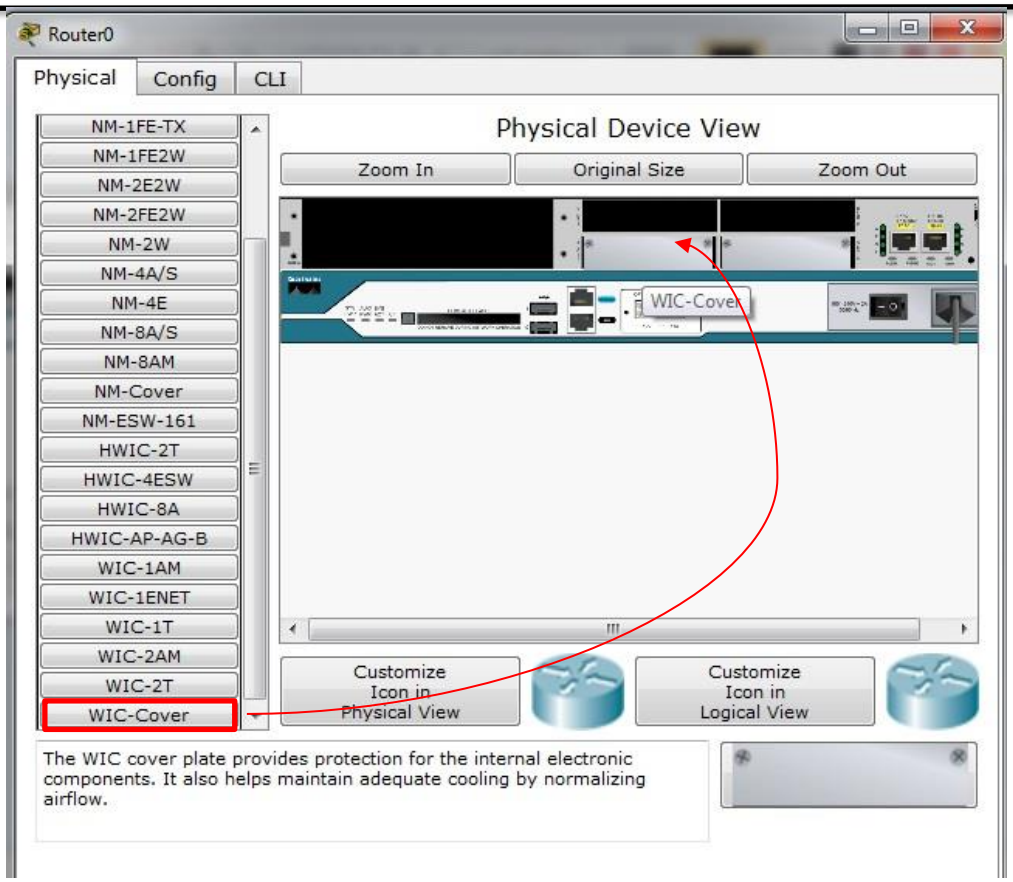
شکل 3-21 پیغام خطا در صورت عدم

بعد از خاموش کردن دستگاه، می‌توان ماژول را در درگاه ماژول دلخواه drag کرد.



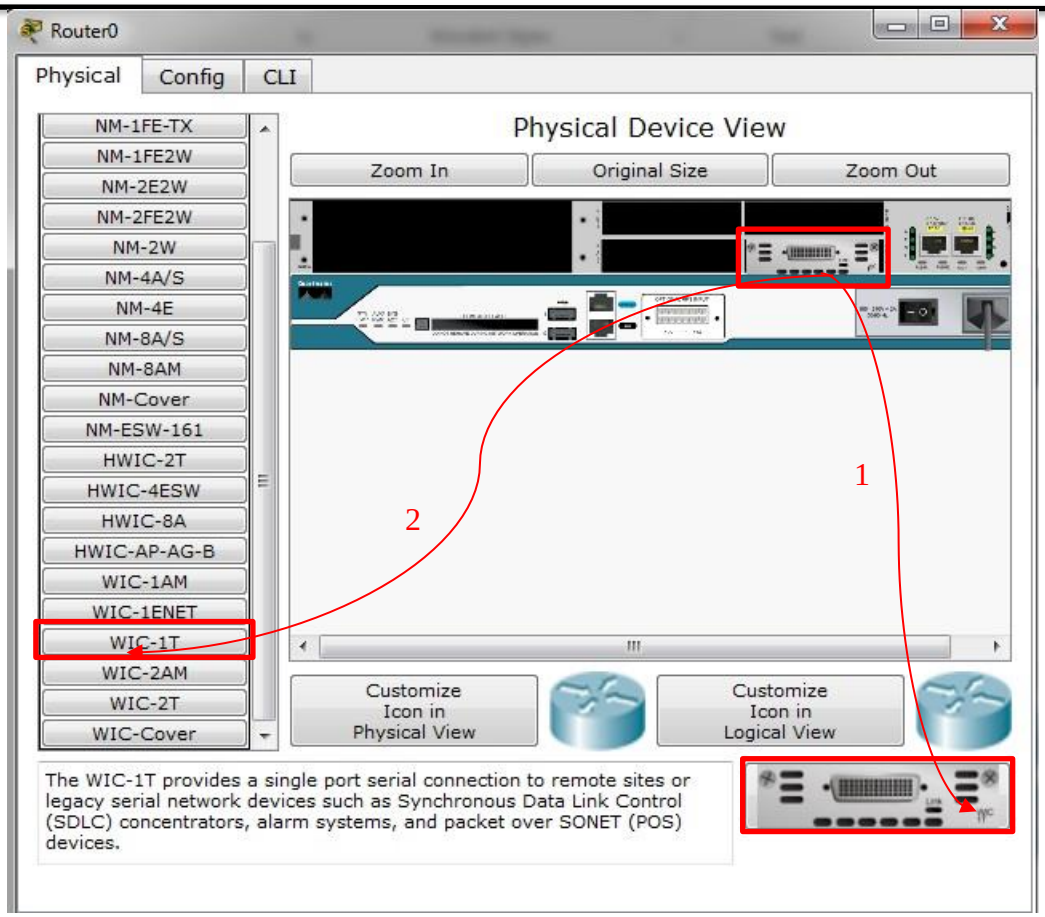
شکل 3-22 نحوه ی drag ماژول در

از ماژول WIC-Cover برای پوشاندن درگاه استفاده می‌شود.



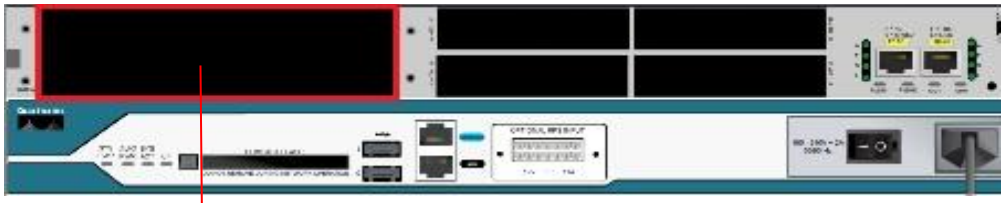
شکل 3-23 استفاده از ماژول

برای حذف ماژول هم می‌توان ماژول را به قسمت مشخص شده (1) در شکل (3-24) یا بر روی منوی خود ماژول (2) drag کرد.



شکل 3-24 حذف ماژول

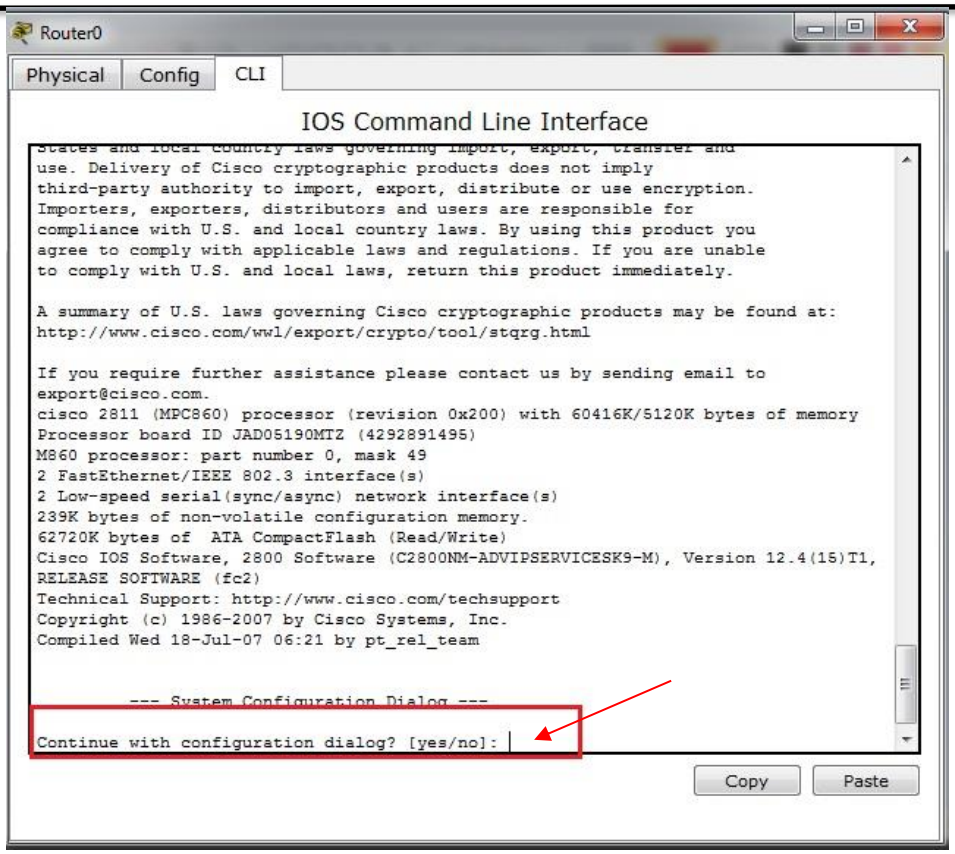
درگاه NM هم به‌صورت شکل (3-25) می‌باشد.



شکل 3-25 درگاه NM

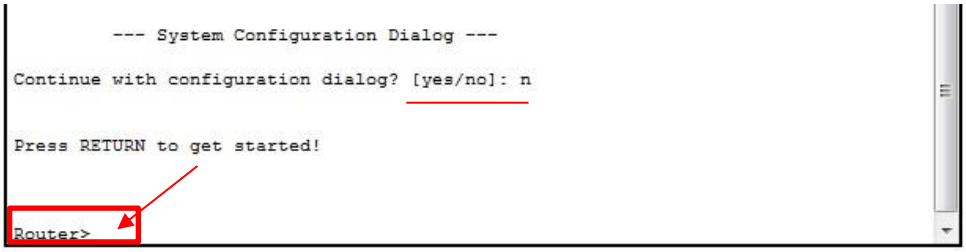
بعد از انجام تنظیمات با  درگاه NM را روشن کرد .

وقتی برای اولین بار به روتر وصل می‌شویم (روتر خام باشد) ، در CLI این سوال پرسیده می‌شود که آیا می‌خواهید به صورت پرسش و پاسخ کانفیگ کنید یا نه؟ چون به صورت دستی می‌خواهیم کانفیگ کنیم در جواب NO زده می‌شود.



شکل 3-26 محیط CLI روتر در Packet

بعد از تایپ NO (یا N) می توان به Command line اولیه‌ی روتر دسترسی پیدا کرد.



شکل 3-27 دسترسی اولیه به line Command روتر

مدهای دسترسی به روتر

به‌طور کلی یک روتر، 3 مد دسترسی به شرح زیر دارد:

1. **User EXEC Mode**: دستورات اجرایی در این مد قابل مشاهده است.

```
Router>
```

2. **Privileged EXEC Mode (enable mode)**: این مد دستورات بیشتری نسبت به user mode دارد. برای قرار گرفتن در این مد باید در user mode دستور enable را تایپ کرد و Enter را زد.

```
Router>enable
Router#
```

تفاوت اصلی user mode و privilege mode: در privilege mode هر دستوری در روتر اجرا شود، قابل مشاهده است، در واقع تصدیق دستورات یا Verify کردن دستورات در این مد انجام می‌شود.

3. **Global Configuration Mode**: اصلی‌ترین دستورات روتر در این مد قرار گرفته است. برای کانفیگ کردن روتر باید در این مد قرار گرفت. با تایپ Configure Terminal در privilege mode می‌توان در این مد قرار گرفت.

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

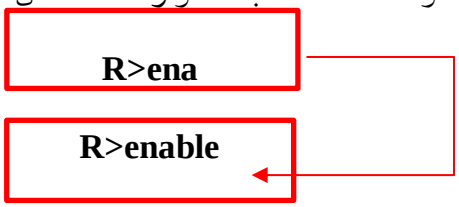
هر مدی در روتر شامل یکسری دستورات خاص می‌باشد که قابل اجرا در مدهای دیگر نیست.

با تایپ exit و زدن Enter در هر مد، می‌توان یک مد به عقب برگشت.

```
Router(config)#exit
```

Router#configure terminal

ساده‌ترین روش تایپ کردن کلمات استفاده از کلید Tab در صفحه کلید می‌باشد. برای مثال اگر در CLI، دستور Router>ena را تایپ کنیم و کلید Tab را فشار دهیم خود کلمه به‌صورت کامل در می‌آید.



برای help دستورات از ? استفاده می‌شود. برای مثال:

```
Router#conf?
configure
Router#configure ?
terminal    Configure from the terminal

<cr>
```

برای دیدن دستورات یک مد، در آن مد می‌توان ? را تایپ کرد.

```
Router#?
Exec commands:
<1-99>          Session number to resume
Auto            Exec level Automation
clear           Reset functions
clock           Manage the system clock
configure       Enter configuration mode
connect         Open a terminal connection
copy            Copy from one file to another
debug           Debugging functions (see also 'undebug')
delete          Delete a file
dir             List files on a filesystem
disable         Turn off privileged commands
disconnect      Disconnect an existing network connection
enable          Turn on privileged commands
erase           Erase a filesystem
exit            Exit from the EXEC
logout          Exit from the EXEC
mkdir           Create new directory
more            Display the contents of a file
no              Disable debugging informations
```

ping	Send echo messages
reload	Halt and perform a cold restart
resume	Resume an active network connection
rmdir	Remove existing directory
send	Send a message to other tty lines
setup	Run the SETUP command facility
show	Show running system information
ssh	Open a secure shell client connection
telnet	Open a telnet connection
terminal	Set terminal line parameters
traceroute	Trace route to destination
undebug	Disable debugging functions (see also 'debug')
vlan	Configure VLAN parameters
write	Write running configuration to memory, network, or terminal

دستورات اولیه

دستوراتی مثل show که در privilege mode استفاده می‌شوند، جزء دستورات اصلی می‌باشند که برای verify کردن دستورات استفاده می‌شوند. عمده‌ترین دستورات show در زیر آورده شده است.

1	Router#**show startup-config**
2	Router#**show running-config**
3	Router#**show flash:**
4	Router#**show version**

- خط1: مشاهده‌ی NVRAM
- خط2: مشاهده ی محتویات RAM روتر
- خط3: دیدن IOS

- خط4: اطلاعات سخت افزاری کل سیستم و مطالب مربوط به Copyright سیستم را نشان می دهد.

Router#**show startup-config**

startup-config is not present

اگر هیچ اطلاعاتی در NVRAM ذخیره نشود، پیغام مشخص شده در قسمت بالا را خواهد داد.

```
Router#show running-config

Building configuration...

Current configuration : 547 bytes
!
version 12.4
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Router
!
!
!
!
!
!
ip cef
no ipv6 cef
!
!
!
!

--More--
```

More یعنی خروجی بیش از یک صفحه است. با زدن دکمه‌ی space از روی صفحه کلید می‌توان خروجی صفحات بعدی را هم مشاهده کرد (اگر Enter زده شود خروجی به‌صورت خط به خط نشان داده می‌شود).

```
Router#show flash:

System flash directory:
File  Length    Name/status
  3   50938004  c2800nm-advipservicesk9-mz.124-15.T1.bin
```

روتر IOS

```
 2       28282       sigdef-category.xml
 1       227537      sigdef-default.xml
[51193823 bytes used, 12822561 available, 64016384 total]

63488K bytes of processor board System flash (Read/Write)
```

C2800nm: یعنی یک IOS سری 2800 می باشد.

advipservice: یعنی می‌توان کامنت‌های پیشرفته را اجرا کرد.

K9: دستورات بحث‌های امنیتی را می‌توان بر روی روتر اجرا کرد.

mz.124-15: یعنی IOS از نوع 12.4-15 را پشتیبانی می‌کند.

T1: مربوط به بحث‌های VOIP می‌باشد.

```
Router#copy running-config  startup-config
```

اطلاعات از RAM به NVRAM منتقل می شود.

دستورات پیکربندی

تغییر نام در روتر

```
Router#configure terminal

Router(config)#hostname name
```

غیرفعال کردن دستور

برای غیرفعال کردن یک دستور از کلمه‌ی no در ابتدای هر دستور استفاده می‌شود. برای مثال:

```
Router(config)#no hostname
```

Lookup mode: وقتی در CLI یک روتر دستور ناشناخته‌ای تایپ شود، روتر دستور را جستجو می‌کند تا اجرا کند، در واقع در این موقع روتر در حالت lookup mode قرار می‌گیرد. مثل زیر:

```
Router>enw

Translating "enw"...domain server (255.255.255.255)
```

برای خارج شدن از Lookup mode، دکمه‌ی Ctrl+shift+6 را فشار می‌دهیم.

دستور غیرفعال کردن Lookup mode:

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

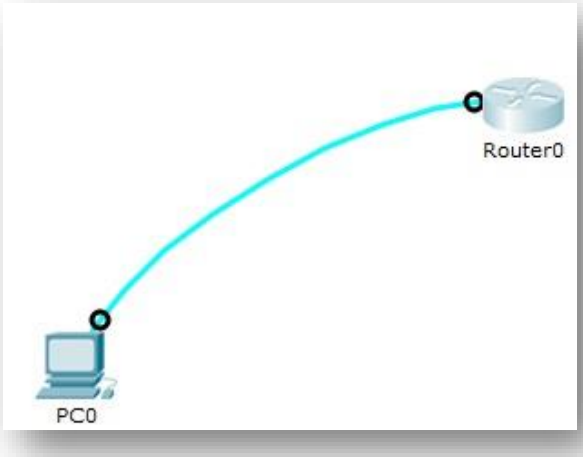
دستورات مربوط به اینترفیس‌های روتر

1	Router#**show ip interface brief**
2	Router(config)#**interface *interface***
3	Router(config-if)#**ip address *ip* *mask***
4	Router(config-if)#**no shutdown**

- خط1: خلاصه‌ای از اینترفیس‌هایی که با IP عمل می‌کنند را نمایش می‌دهد.
- خط2: قرار گرفتن در اینترفیس مورد نظر
- خط3: به اینترفیس مورد نظر IP اختصاص داده می‌شود.
- خط4: برای اینکه اینترفیس به وضعیت up در بیاید از این دستور استفاده می‌شود.

```
Router#show ip interface brief

Interface              IP-Address      OK? Method  Status                Protocol
FastEthernet0/0        unassigned      YES unset   administratively down down
FastEthernet0/1        unassigned      YES unset   administratively down down
Serial0/0/0            unassigned      YES unset   administratively down down

Vlan1                  unassigned      YES unset   administratively down down
```

همان‌طور که نشان داده شده است، خروجی شامل دو اینترفیس FastEthernet، یک اینترفیس Serial و یک اینترفیس مجازی به‌نام Vlan1 می‌باشد. در خروجی این دستور IP ای که برای اینترفیس تنظیم می‌شود، نمایش داده می‌شود، اگر IP تنظیم نشود با unassigned نمایش داده می‌شود. همچنین وضعیت up و down بودن اینترفیس و پروتکل هم نمایش داده می‌شود.



1	Router(config)#**interface FastEthernet 0/0**
2	Router(config-if)#**ip address 192.168.10.1 255.255.255.0**
3	Router(config-if)#**no shutdown**
4	%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

- خط4: یعنی اینترفیس به حالت up درآمده است.

Router#**sh ip int br**

Interface	IP-Address	OK? Method	Status	Protocol
FastEthernet0/0	192.168.12.1	YES manual	up	down
FastEthernet0/1	unassigned	YES unset administratively	down	down
Serial0/0/0	unassigned	YES unset administratively	down	down
Vlan1	unassigned	YES unset administratively	down	down

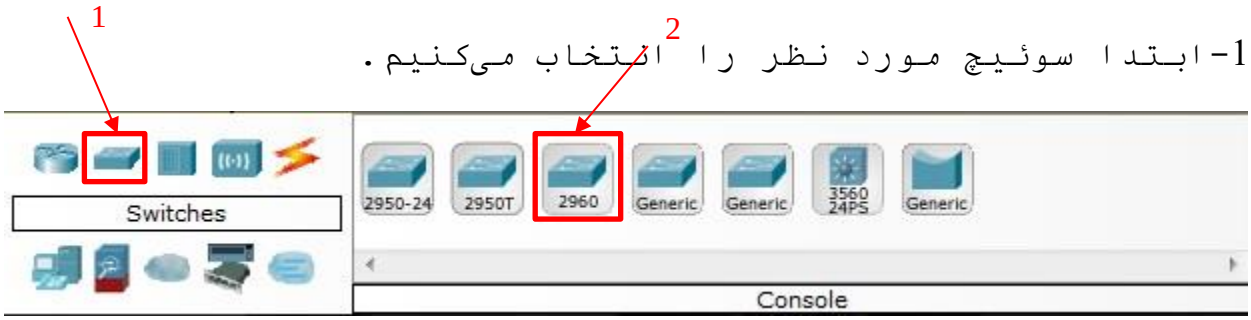
همان‌طور که مشاهده می‌شود، اینترفیس FastEthernet با IP: 192.168.12.1 قرار دارد، status در وضعیت up و protocol در وضعیت down می‌باشد. پروتکل زمانی up می‌شود که از نظر سخت افزاری پورت را روی دستگاهی نصب کرد.

نکات

- یک اینترفیس برای اینکه به شبکه متصل شود و با شبکه ارتباط برقرار کند باید IP داشته باشد و در وضعیت up&up قرار بگیرد (یعنی status و protocol در وضعیت up باشند).
- در روتر، اینترفیس‌ها همیشه shutdown می‌باشد.

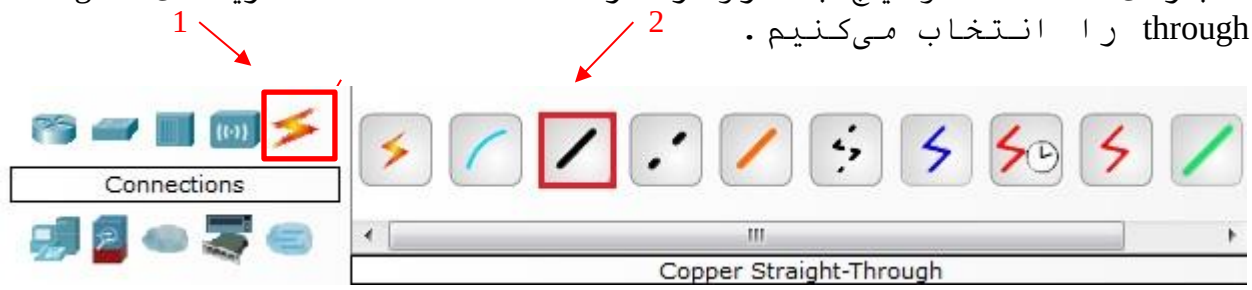
طریقه‌ی اتصال سوئیچ به روتر و PC

1- ابتدا سوئیچ مورد نظر را انتخاب می‌کنیم.



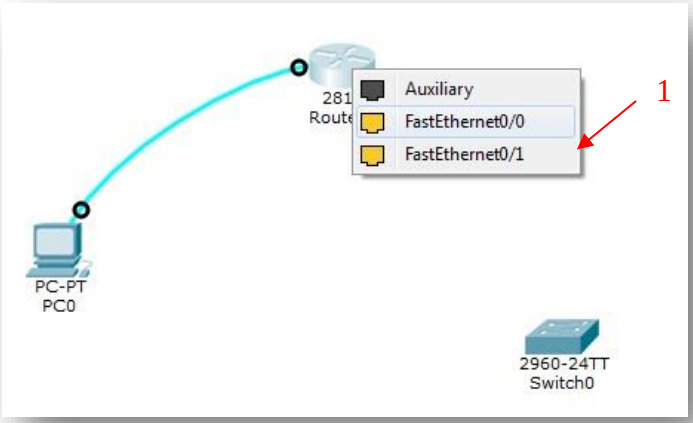
شکل 3-28 نحوه انتخاب سوئیچ در

2- برای اتصال سوئیچ به روتر از قسمت Connection گزینه‌ی Copper straight-through را انتخاب می‌کنیم.

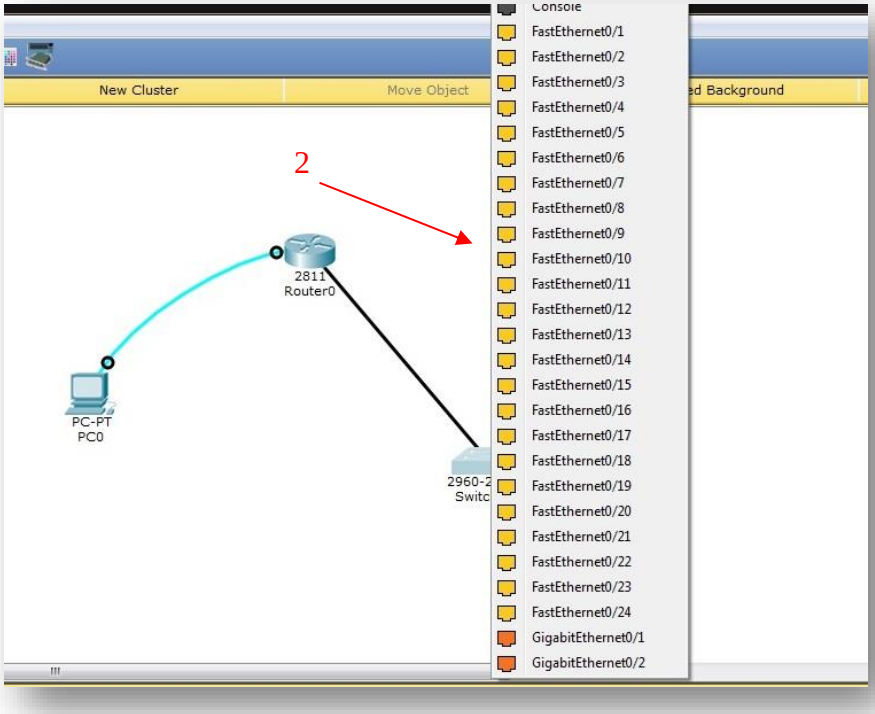


شکل 3-29 نحوه انتخاب کابل برای اتصال سوئیچ

3- بعد از انتخاب کابل، بر روی روتر قرار گرفته و گزینه‌ی FastEthernet 0/0 (یا FastEthernet 0/1) را انتخاب کرده، سپس بر روی سوئیچ کلیک کرده و یکی از 24 پورت موجود را انتخاب می‌کنیم.

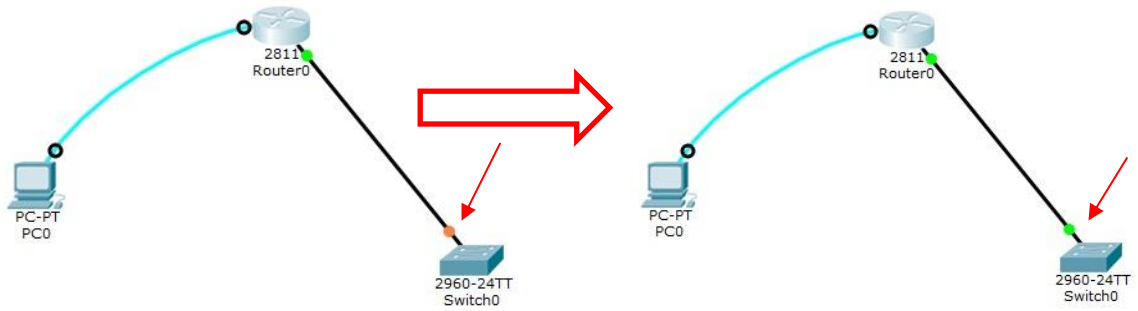


شکل 3-30 انتخاب پورت مورد نظر
برای روتر



شکل 3-31 انتخاب پورت مورد

بعد از انتخاب پورت، به طور اتوماتیک سوئیچ شروع به روشن شدن می‌کند (چون پورت‌های سوئیچ همیشه در وضعیت up هستند).



شکل 3-32 وضعیت پورت های سوئیچ بعد

وقتی پورت سوئیچ از رنگ نارنجی به رنگ سبز تبدیل شود یعنی پورت در وضعیت آماده است.

لینک‌های سریال

شکل (3-33) لینک‌های سریال را نشان می‌دهد، اگر بر روی لینک‌ها قرار بگیریم یکی از لینک‌ها Serial DCE و دیگری Serial DTE می‌باشد.

شکل 3-33 وضعیت لینک های سریال در

فرق لینک‌های سریال DCE و DTE

DCE: همیشه مخابرات است.

DTE: اتصال به مخابرات(یا service provider) با استفاده از این کابل انجام می‌شود.

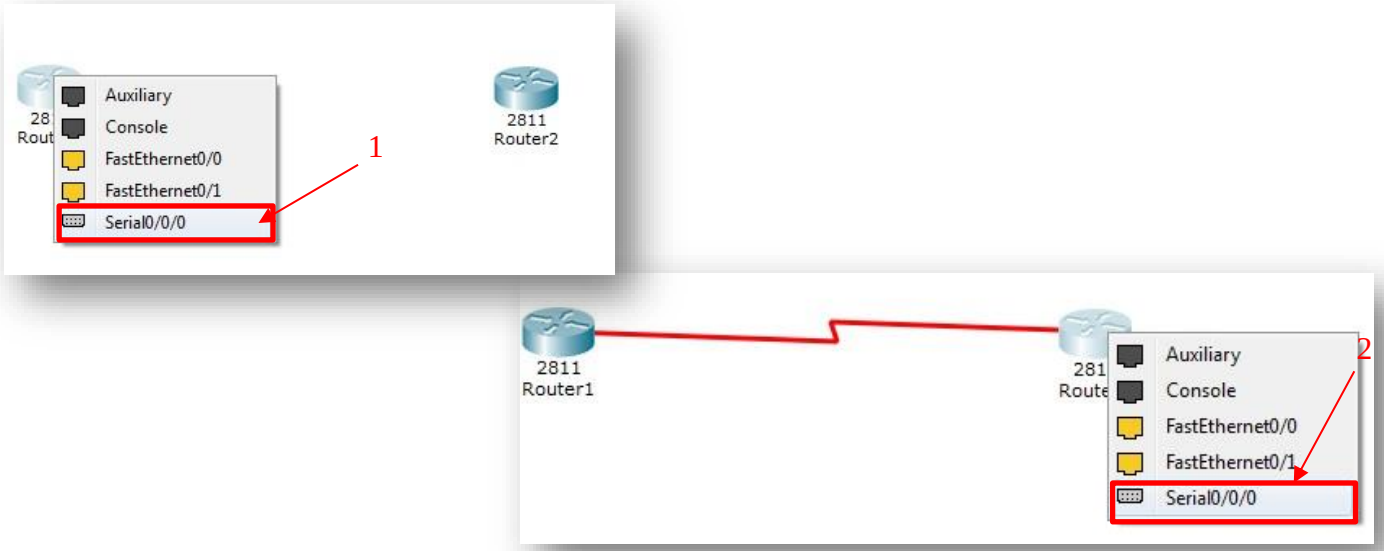
اطلاعات همیشه از سمت DCE ارسال می‌شود و DTE پاسخ می‌دهد.

در ارتباطات سریال یک سمت حتما باید DCE و سمت دیگر باید DTE باشد.

کانکت روترها نسبت بهم با استفاده از اینترفیس‌های سریال

1-برای کانکت روترها نسبت بهم ابتدا ماژول‌های مورد نظر را بر روی روترها قرار داده.

2-سپس لینک‌های ارتباطی بین روترها را انتخاب می‌کنیم.



شکل 3-34 انتخاب لینک‌های

3-سپس به اینترفیس‌ها در هر دو روتر IP داده و در وضعیت up قرار

می‌دهیم.

192.168.12.0/24

شکل 3-35 اتصال لینک های ارتباطی
به روترها

Router1

1	Router(config)#**int s0/0/0**
2	Router(config-if)#**ip address 192.168.12.1 255.255.255.0**
3	Router(config-if)#**clock rate 64000**
4	Router(config-if)#**no shutdown**
5	%LINK-5-CHANGED: Interface Serial0/0/0, changed state to down

- خط3: سمتی که DCE باشد این دستور باید زده شود. این دستور نرخ تبادل داده را مشخص می‌کند و یک عددی برحسب bps انتخاب می‌شود. پیش فرض 64000 می‌باشد. لینک‌های سریال از 64000 bps تا 2Mbps می‌باشند.
- خط5: اگر سمت مقابل کانفیگ نشود، status در وضعیت down قرار می‌گیرد.

Router2

1	Router(config)#**int s0/0/0**
2	Router(config-if)#**ip address 192.168.12.2 255.255.255.0**
3	Router(config-if)#**no shutdown**
4	Router(config-if)#
5	%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up
6	%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up

- خط5: اینترفیس up شده است.
- خط6: پروتکل up شده است.

```
Router#show ip interface brief
Interface          IP-Address   OK? Method  Status    Protocol
FastEthernet0/0    unassigned   YES unset   administratively  down  down
FastEthernet0/1    unassigned   YES unset   administratively  down  down
Serial0/0/0        192.168.12.2 YES manual  up        up

Vlan1              unassigned   YES unset administratively  down  down
```

دستور ping: برای تست connectivity بین سیستم ها استفاده می‌شود.

```
Router#ping ip سمت مقابل
```

Router1

```
Router#ping 192.168.12.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.12.2, timeout is 2 seconds:
!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/15/65 ms
```

بازه زمانی ارسال و دریافت بسته

خروجی این دستور بیان می‌کند که درصد موفقیت 100 درصد بوده و هر 5 بسته را دریافت کرده است.

Ping پروتکل ICMP می‌باشد.

CDP[1]

CDP یک پروتکل شبکه لایه دو (Data Link) مخصوص سیسکو می‌باشد که این پروتکل جهت به اشتراک‌گذاری اطلاعات دستگاه های سیسکو (همانند نسخه سیستم عامل و IP آدرس) که بصورت مستقیم به یکدیگر متصل هستند، توسط شرکت سیسکو توسعه یافته است و این پروتکل در تجهیزات ساخته شده زیر توسط شرکت سیسکو اجرا می‌شود:

- **Router**
- **Bridge**
- **Access Server**
- **Switch**

پیام های CDP از طریق یک دستگاه سیسکو همسایه دریافت می‌شود و بصورت پیش فرض به هیچ دستگاه دیگری ارسال نمی‌شود . این بدان معنی است که CDP فقط از دستگاه های سیسکو که به صورت مستقیم متصل می‌باشد عبور می‌کند .هر دستگاه سیسکو (که CDP را پشتیبانی می‌کند) اطلاعات دریافت شده از دستگاه های همسایه را در یک جدول ذخیره می‌کند که با استفاده از دستور show cdp neighbors می‌توانیم آن را مشاهده کنیم.

دستگاه های سیسکو پیغام های CDP را به آدرس مقصد مالتی کاست 01:00:0C:CC:CC:CC ارسال می‌کنند. پیغام های CDP در هر 60 ثانیه روی اینترفیس‌هایی که پروتکل دسترسی به زیر شبکه ها (SNAP[2]) را پشتیبانی می‌کند، ارسال می‌شود. پشتیبانی از SNAP در هر نوع رسانه لایه دو (data link layer) موجود نمی‌باشد . مدل های رسانه ای که CDP را پشتیبانی می‌کنند عبارتند از:

Ethernet, Token Ring, FDDI, PPP, HDLC, ATM و Frame Relay

پیغام CDP شامل اطلاعات زیر می‌باشد:

1- نام دستگاه (که با دستور hostname تنظیم شده است)
2- نسخه نرم افزار IOS
3- امکانات سخت افزار (routing/switching)
4- پلت فرم سخت افزار
5- آدرس IP دستگاه

[1] Cisco Device Protocol
[2] Subnetwork Access Protocol

6- اینترفیسی که پیام CDP را ایجاد کرده است.

جدول 3-1 مزایا و معایب CDP

مزایا	معایب
هنگامی که لایه 1 فعال است، CDP اطلاعات را به همسایه های فعال خود ارسال می‌کند.	فقط در دستگاه های سیسکو می‌تواند استفاده شود.
می‌تواند برای عیبیابی لایه های 1، 2 و 3 استفاده شود.	فقط اطلاعات همسایه هایی که به طور مستقیم وصل شده اند، می‌تواند شناخته شود.

دستورات مهم CDP قابل استفاده در IOS

فعال یا غیر فعال کردن CDP در IOS سیسکو:
CDP به‌صورت پیش‌فرض در روترهای سیسکو فعال می‌باشد. اگر شما ترجیح می‌دهید که این قابلیت را غیر فعال کنید، می‌توانید از دستور no cdp run برای غیر فعال کردن آن و مجددا برای فعال کردن CDP می‌بایستی از دستور cdp run در وضعیت global configuration استفاده نمایید.

- **RouterX# show cdp neighbors :**

برای دیدن خلاصه ای از دستگاه های سیسکو همسایه می‌توانیم در privilege mode از این دستور استفاده کنیم.

1	Router01#**show cdp neighbors** Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone Device ID Local Intrfce Holdtme Capability Platform Port ID networkinpersian.com.router02 Ser 0/0 156 R C2600 Ser 0/0 networkinpersian.com.switch01 Fas 0/0 149 S 2950 Fas 0/1 networkinpersian.com.router01#

دستور #show cdp neighbors اطلاعات زیر را نمایش می‌دهد.

- نوع دستگاه پیدا شده
- نام دستگاه
- تعداد و نوع پورت‌ها یا اینترفیس‌های local
- شماره محصول دستگاه
- شناسه پورت

- **RouterX# show cdp neighbor detail:**

برای دیدن اطلاعات جزئی از دستگاه‌های سیسکو همسایه می‌توانیم در privilege mode از این دستور استفاده کنیم.

1	Router#**show cdp neighbor detail** Device ID: networkinpersian.com.router02 Entry address(es): ...

- **RouterX#show cdp interface:**

برای دیدن تنظیمات CDP روی اینترفیس در privilege mode از این دستور استفاده می‌کنیم.

	Router#**show cdp interface** FastEthernet0/0 is up, line protocol is up ...

- **RouterX#show cdp:**

برای دیدن وضعیت CDP در دستگاه سیسکو در privilege mode می‌توانیم از این دستور استفاده کنیم.

1	Router#**show cdp** Global CDP information: Sending CDP packets every 60 seconds Sending a holdtime value of 180 seconds Sending CDPv2 advertisements is enabled

انواع پسورد در روتر

1- Enable Password : برای برقراری امنیت هنگام ورود به privileged mode استفاده می‌شود. هنگامی که در user mode فرمان enable را وارد می‌کنید و می‌خواهید وارد privileged mode شوید این password پرسیده می‌شود.

1	**Router (config) # enable password پسورد مورد نظر**

حال زمانی که می‌خواهیم وارد مد enable شویم از ما پسورد می‌خواهد:

```
Router>en
Password:
```

این پسورد از امنیت بالایی برخوردار نیست چون در Show Run کاملا نمایش داده می‌شود و برای بالا بردن امنیت پسورد مد Enable باید آن‌را رمز نگاری کرد که از Secret Password باید استفاده شود.

2- Secret Password : همانند enable password می‌باشد، با این تفاوت که با MD5 کدگذاری می‌شود.

1	Router (config) # **enable secret پسورد مورد نظر**

توجه داشته باشید هنگامی که secret password را تنظیم می‌کنید، تا زمان فعال بودن secret password ، Enable password به صورت غیر فعال در می‌آید و می‌بایست هنگام ورود به Privileged Mode پسورد مربوط به Secret Password را وارد کنید.

3- Telnet Password : یکی از راه‌های دسترسی به روتر Virtual Terminal یا همان Telnet می‌باشد. بنابراین در صورتی‌که به یک روتر Telnet

می‌کنید، می‌بایست بعد از بررسی و صحت Authentication ارتباط برقرار شود.

```
1  Router (config) # line vty 0 4
2
3  Router (config-line) # line vty 0 ?
4  <1-4> last line number
5  <cr>
6
7  Router (config-line) # login
8  Router (config-line) # password یسورد مورد نظر
9  Router # show session
10
11 Router # disconnect connection-number
```

- خط 1: برای تنظیم کردن telnet password وارد global mode شده ودستور زیر را وارد می‌کنیم:

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

- خط 3: برای دیدن تعداد Line هایی که IOS را ساپورت می کنند، کافی است از Help کمک بگیرید.
- خط7: فرمان بعدی login می‌باشد. در واقع با این فرمان می‌گویید که در صورت telnet شدن به این device ، پسورد پرسیده شود.
- خط 8: مرحله آخر تعریف پسورد می‌باشد:

Router (config-line) # **password یسورد مورد نظر**


توجه داشته باشید که telnet password قبل از وارد شدن user به user mode پرسیده می‌شود.

- خط 9: به کمک فرمان show session می‌توان تمامی session های برقرار شده و مدت زمان connect بودن هر یک از آن‌ها را مشاهده کرد.

- خط 11: می توان به کمک فرمان disconnect ، ارتباط session خاصی را با روتر قطع کرد.

4- AUX Password: همان‌طور که می‌دانید یکی دیگر از راه‌های برقراری ارتباط remote ، روش استفاده از پورت AUX می باشد. در این روش، روتر از طریق یک مودم به خط dial-up متصل شده است و دسترسی به صورت remote به آن امکان‌پذیر می‌باشد.AUX Password پسوردی است که قبل از وارد شدن به user mode پرسیده می‌شود.

1	Router (config) # **line aux o**
2	Router (config-line) # **login**
3	Router (config-line) # **password** **پسورد مورد نظر**

5- Console password: تنها راه ارتباط با روتر که بدون تنظیم می‌باشد، استفاده از console port است. بنابراین بعد از انجام تنظیمات می‌توانید روتر را در یک جای ثابت قرار داده و از این به بعد آن را از طریق telnet یا Browser کردن تنظیم کنید.
اما توجه داشته باشید که نداشتن پسورد و محدودیت دسترسی افراد برای admin دردسر ساز می‌شود.

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

1	Router (config) # **line console0**
2	
3	Router (config-line) # **login**
4	
5	Router (config-line) # **password** **پسورد مورد نظر**

تنظیمات اضافی پورت Console :

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

```
1  Router (config) # line console o
2  Router (config-line) # exec-timeout o o
```

حال اگر بخواهیم براي برقراري امنيت بيشتر، اين زمان را كمتر كنيم تا زمانيكه اگر شخص از پشت سيستم خود بلند شد و براي اينكه شخص ديگري از فرصت استفاده نكند و نتواند Config ها را دستكاري كند، زمان را كم مي‌كنيم كه با اين كار به‌طور خودكار در زمان تعيين شده روتر از مد Config خارج مي‌گردد.

```
1  Router (config) # line console 0
2  Router (config-line) # exec-timeout    دقيقه    ثانيه
```

يكی ديگر از مشكلاتی كه ممكن است با آن مواجه شويد، اين است كه شما فرمانی را در command prompt روتر يا سوئيچ وارد می‌كنيد، به‌طور مثال دستور show run و منتظر نتيجه آن هستيد در اين لحظه پيام جديدی مبنی بر اينكه يكی از اينترفيس‌ها up شده است، ظاهر می‌شود. بنابراين نمی‌توانيد تفاوت بين نتيجه فرمان خودتان و پيامی كه ظاهر شده را متوجه شويد. به كمک فرمان زير می‌توانيد به روتر بگوييد پيام جديد را جدا از خروجی فرمان شما نمايش دهد.

```
1  Router (config) # line console 0
2  Router (config-line) # logging synchronous
```

6- براي اينكه باقي پسوردهاي موجود در سيستم را نيز رمز نگاري كنيم از دستور زير استفاده مي‌كنيم.

```
1  Router (config) #service password-encryption
```

مكانيزم Password Recovery

قبل از انجام password recovery ابتدا باید با دستور R#wr دستورات مورد نظر را در startup config ذخیره کرد. برای انجام password recovery باید دسترسی فیزیکی به دستگاه را داشت در غیر اینصورت امکان‌پذیر نخواهد شد.

1-برای این کار بعد وارد کردن 3 بار پسورد اشتباه در user mode، برای reset کردن دستگاه یکبار دکمه‌ی روشن/خاموش زده می‌شود 

2-سپس وارد CLI شده و زمانی که روتر بوت می‌شود دکمه ی Ctrl+Break را از روی صفحه کلید فشار داده، وارد یک محیطی به نام runmonitor (یا rommon) می‌شویم.

```
Press RETURN to get started!

System Bootstrap, Version 12.1 (3r) T2, RELEASE SOFTWARE (fc1)
Copyright (c) 2000 by Cisco systems, INC
Cisco 2811 (MPC860) processor (revision 0x200) with 60416k/5120k bytes of memory


Self decompressing the image :
##########
monitor: command "boot" aborted due to user interrupt
rommon 1 >
```

3-سپس دستور زیر را وارد کرده، در واقع دستور زیر در هنگام بوت شدن روتر، NVRAM را نادیده می‌گیرد.

```
rommon 1>confreg 0X2142
```

4-با اجرای دستور قبلی وارد مد rommon 2 شده و دستور زیر را اجرا می‌کنیم.

```
rommon 2>reset
```

وقتی این دستور اجرا می‌شود، روتر بوت شده و به جای اینکه NVRAM را بخواند مستقیم وارد RAM می‌شود (در واقع وارد روتری می‌شود که هیچ دستوری بر روی آن اجرا نشده است). با اجرا شدن این دستور پیغام زیر مشاهده می‌شود:

```
rommon 2 > reset
System Bootstrap, Version 12.1 (3r) T2, RELEASE SOFTWARE (fc1)
Copyright (c) 2000 by Cisco systems, INC
Cisco 2811 (MPC860) processor (revision 0x200) with 60416k/5120k bytes of memory


Self decompressing the image :
##################################################
```

5-سپس وارد user mode شده و به راحتی بدون پسورد می‌توان وارد privilege mode شد. اگر دستور R#sh running-config اجرا شود، مشاهده می‌شود که روتر خام می‌باشد.

```
--- System Configuration Dialog ---

Continue with configuration dialog? [yes/no]: n


Press RETURN to get started!



Router>en        بدون پسورد
Router#
```

6-اطلاعات چون در NVRAM باقی مانده برای فراخوانی اطلاعات در NVRAM از دستور زیر استفاده می‌شود.

```
Router#copy startup-config running-config
```

حال اگر دستور R#sh running-config را اجرا شود می‌توان تمامی کانفیگ‌های انجام شده را مشاهده نمود.

7-سپس دستورات زیر را اجرا می‌کنیم تا پسوردهایی که بر روی روتر قرار داشت را حذف کنیم.

```
Router(config)#no enable secret
Router(config)#line console 0
Router(config-line)#no password
Router(config-line)#no login
```

8-برای اینکه روتر به حالت عادی برگردد، دستور زیر به کار برده می شود.

```
Router(config)#config-register 0X2102
```

9-در انتها باید اطلاعات ذخیره شود.

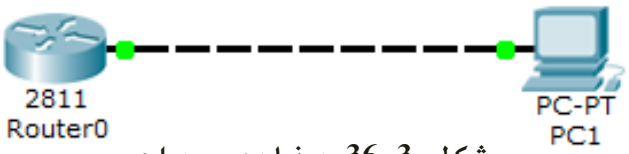
```
Router#wr
```

10-برای اینکه روتر را به‌صورت نرم افزاری بوت کنیم، دستور زیر به کار برده می‌شود.

```
Router#reload
```

راه اندازي مكانيزم Telnet

- Telnet برای پیکربندی دستگاه‌های شبکه از راه دور استفاده می‌شود.
- Telnet داده‌ها را به‌صورت متن ساده ارسال می‌کند، بنابراین امن نیست.

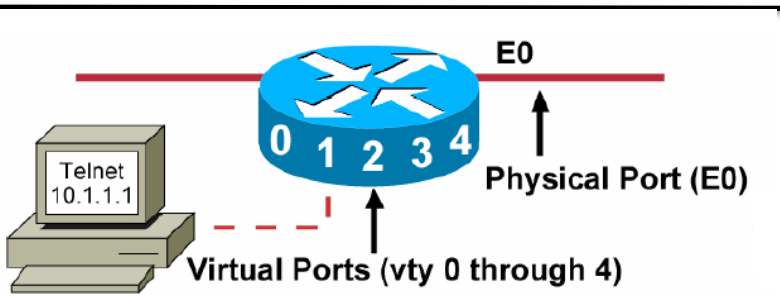


شکل 3-36 سناریو راه

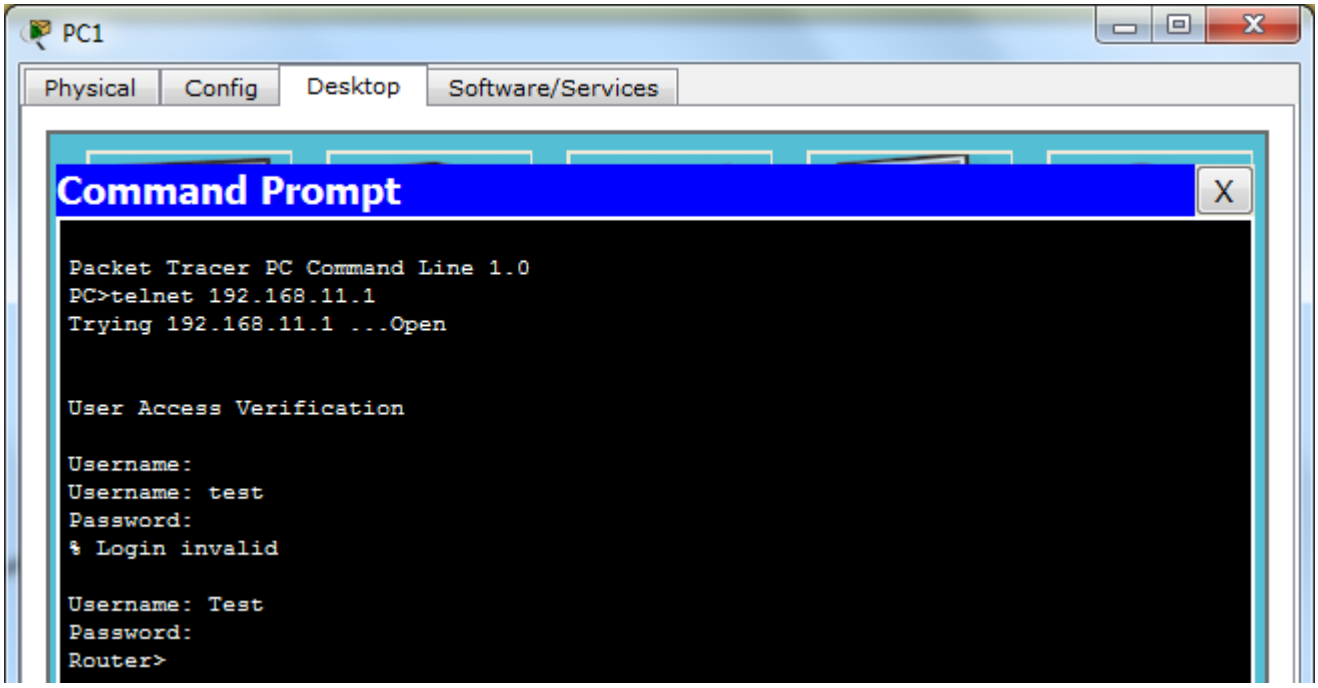
```
1  Router>en
2  Router#conf t
3
4  Router(config)#interface fastEthernet 0/1
5  Router(config-if)#ip address 192.168.11.1 255.255.255.0
6  Router(config-if)#no sh
7
8  Router(config)#username Test password 123
9  Router(config)#line vty 0 4
10 Router(config-line)#login local
11 Router(config-line)#transport input telnet
```

حال می‌خواهیم از کامپیوتر مورد نظر از طریق Telnet به روتری که در آن Telnet را فعال نمودیم، وصل شویم.

- صفحه Command prompt را باز می‌کنیم.
- IP روتر مورد نظر را به همراه کامند Telnet در خط فرمان می‌نویسیم.
- باید توجه داشته باشیم که به حروف بزرگ و کوچك حساس می‌باشد. مثلا در اینجا ما Username را با Test انتخاب نمودیم که حرف T آن بزرگ می‌باشد و همان‌گونه که در شکل زیر مشاهده می‌نمایید، زمانی‌که ما test را با حرف کوچك وارد نمودیم پیغام خطا صادر نمود. (Login Invalid).
- زمانی‌که پسورد خواست باید همان پسورد 123 را که در خط username Test password 123 نوشتیم را وارد کنیم.



شکل 3-37 نمایی شماتیک از پورت های



شکل 3-37 اتصال به روتر از
طریق Telnet

راه اندازي مکانیزم SSH

- SSH برای امن کردن دسترسی از راه دور استفاده می‌شود.
- SSH داده‌ها را به‌صورت رمزنگاری بین هاست‌ها و دستگاه شبکه فراهم می‌کند.

- IOS سیسکو باید رمزگذاری را برای اجرای SSH پشتیبانی کند.

ابتدا SSH را روي روتر مورد نظر فعال مي‌كنيم:

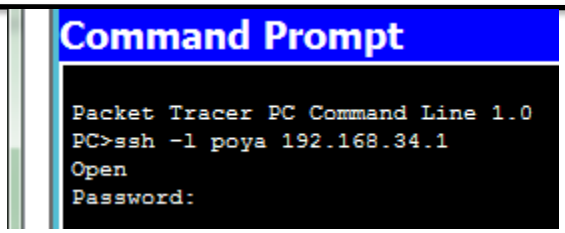
```
1  R3(config)# hostname TEST
2  TEST(config)# ip domain-name CISCO.com
3  TEST(config)# crypto key generate rsa
4  % You already have RSA keys defined named TEST.CISCO.com .
5  % Do you really want to replace them? [yes/no]:1024
6  TEST(config)# ip ssh version 2
7  TEST(config)# username poya password 123
8
9  TEST(config)# enable secret 12345
10 TEST(config-line)# line vty 0 4
11 TEST(config-line)# login local
12  TEST(config-line)# transport input ssh
```

توضیح کد:

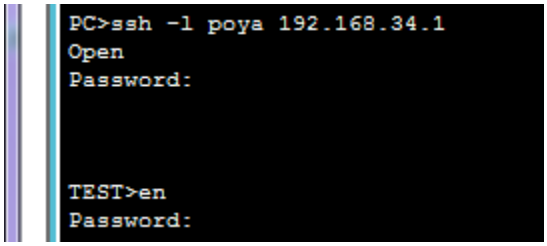
- خط 1: عوض کردن hostname (برای راه اندازی ssh ابتدا باید hostname را عوض کرد)
- خط 2: تعریف یک domain برای IP
- خط 3: کلید امنیتي با الگوریتم رمز نگاري RSA
- خط 5: 1024 را وارد مي‌كنيم (براي اينكه طول كليد امنيتي بالا برود و رمز نگاري آن مشكل‌تر شود)
- خط 6: براي ساپورت طول كليد بزرگتر، بايد وارد Ver2 شويم.
- خط 7: انتخاب نام براي SSH و پسورد.
- خط 9: انتخاب پسورد مناسب براي مد enable روتر
- خط 10 الي 12: تنظيمات مربوط به ssh (براي زماني‌كه كه كسي مي‌خواهد از طريق ssh به روتر شماره 3 وصل شود و وارد مد enable شود)

PC>ssh –L poya 192.168.34.1(آي پي روتري را كه مي خواهيم به آن وصل شويم)

اگر از سیستم‌هاي ديگر بخواهيم از طريق SSHمتصل شويم، مي‌توانيم اين كار را انجام بدهيم.



حال باید پسورد اول را وارد کنیم: 123



سپس پسورد enable را وارد میکنیم: 12345

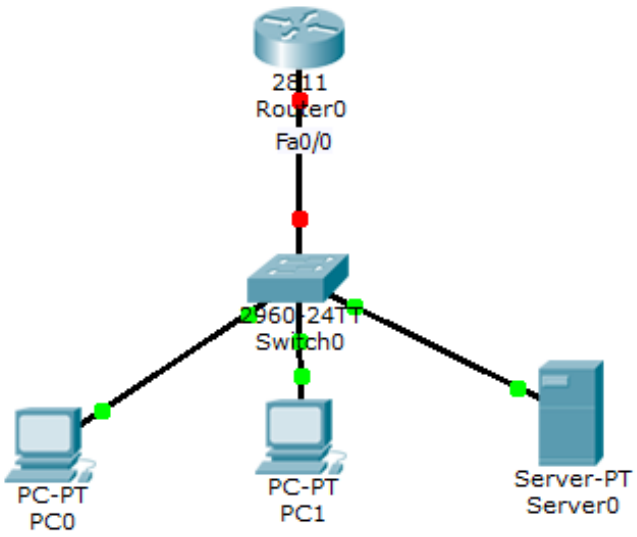
شکل 3-38 اتصال به روتر از طریق SSH

و وارد مد enable روتر میشویم.

در راه اندازی telnet و ssh باید enable password یا enable secret را تنظیم کرد وگرنه اجازه‌ی دسترسی به privilege mode داده نمی‌شود.

راه اندازي سرويس DHCP

- اختصاص اتوماتيك IP به اجزاي شبكه
- سرور DHCP: IP، Subnet mask، gateway پیشفرض، IP ی سرور DNS را برای کلاینت‌های DHCP فراهم میکند.



شکل 3-39 سناریو راه اندازی

1- براي شروع كار ابتدا به Interface FastEthernet 0/0 روتر IP اختصاص مي‌دهيم.

```
1  Router(config)#interface fastEthernet 0/0
2  Router(config-if)#ip address 192.168.10.1 255.255.255.0
3  Router(config-if)#no sh
```

2- راه اندازي DHCP در روتر:

```
1  Router(config)#ip dhcp pool Test
2  Router(dhcp-config)#network 192.168.10.2  255.255.255.0
3  Router(dhcp-config)#default-router 192.168.10.1
4  Router(dhcp-config)#dns-server 192.168.10.2
5
6  Router(config)#ip dhcp excluded-address 192.168.10.4 192.168.10.10
```

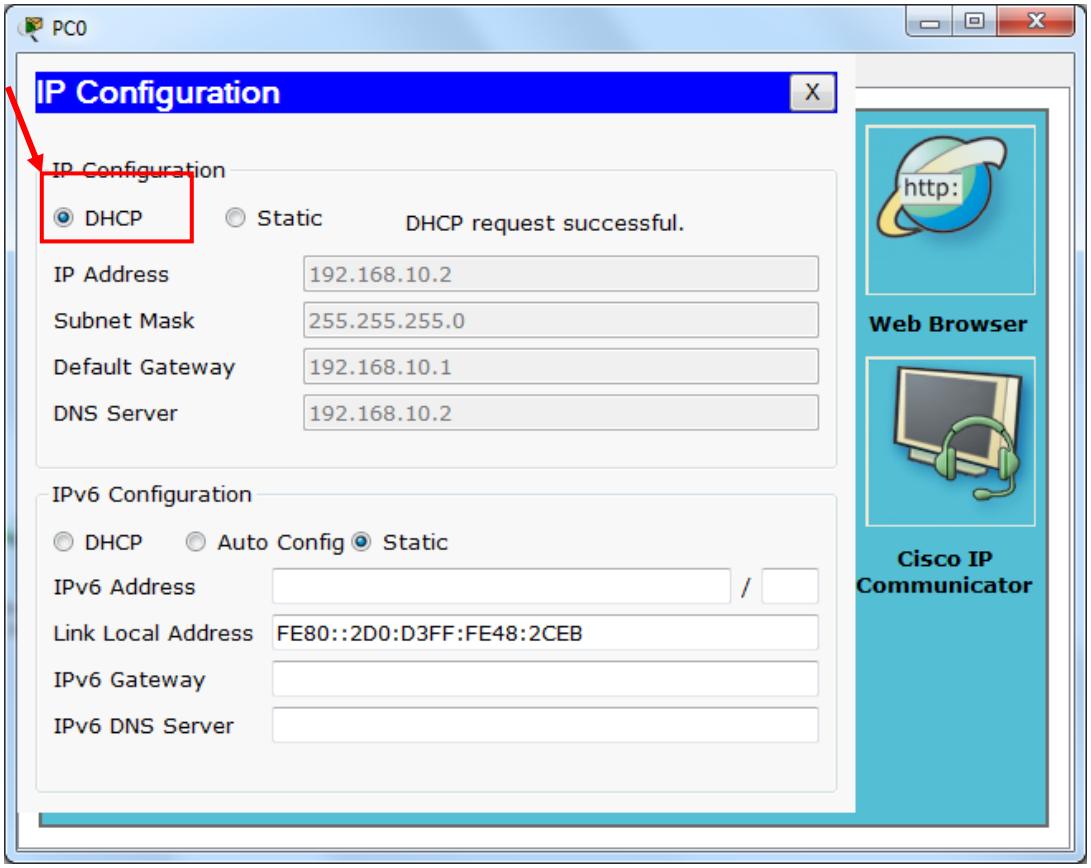
- خط 1: بايد مخزني را تعريف كنيم كه كلاينت‌ها بتوانند از آنجا IP دريافت كنند (Pool درياچه‌اي از IP ها است).

Router(config)#ip dhcp pool نام دلخواه

- خط 2: رنج IP ها را تعريف مي‌كنيم.
- خط 3: تعريف Default Gateway. در اينجا Interface FastEthernet 0/0 در نقش Gateway است و IP اي كه به آن اختصاص داده ايم را بايد در اين قسمت به عنوان Gateway تعريف نماييم.
- خط 4: تعريف Domain Name server (ضروري نيست).
- خط 6: در صورتي كه بخواهيم يك‌سري از IP ها را از ليست خارج نماييم (مثلا بعضي از IP ها را به صورت دستي به سيستم‌ها و

اجزاي شبكه اختصاص داده ايم) از اين دستور استفاده مي‌كنيم و در اينجا رنج بين 4 الي 10 از طريق DHCP به كسي اختصاص داده نمي‌شود.

و در نهايت بر روي تنظيمات سيستم ها و تجهيزات شبكه IP Configuration را بر روي DHCP قرار مي‌دهيم تا از DHCP، آي پي دريافت كند.

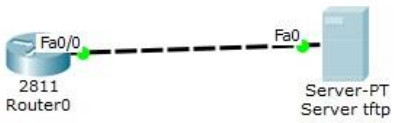


شكل 3-40 نحوه‌ی دريافت IP از DHCP

سرور TFTP

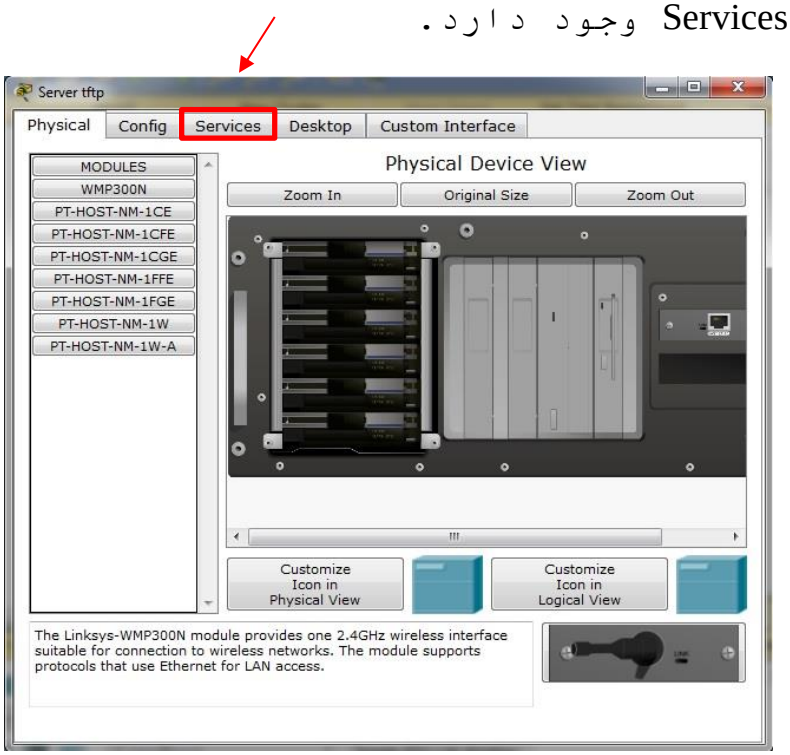
براي آپلود و تعويض سيستم عامل روترها به‌صورت پيش‌فرض از اين سرور در شبكه استفاده مي‌شود. در حقيقت هدف حذف IOS يک روتر و انتقال IOS جديد از سرور TFTP به روتر مي‌باشد.

براي مشاهده‌ی IOS های يک سرور TFTP در نرم افزار Packet tracer به صورت زير عمل مي‌كنيم:



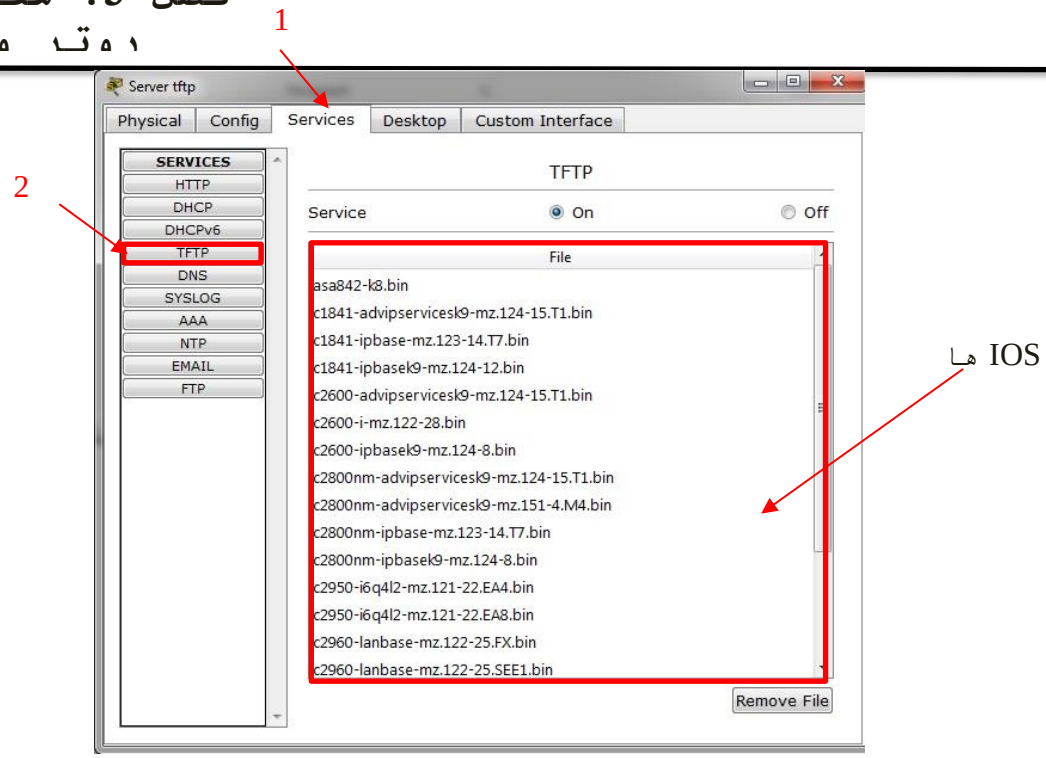
شکل 3-41 سناریو راه اندازی

1- ابتدا بر روی سرور کلیک کرده، در صفحه ای که باز می‌شود یک Tab ای با نام Services وجود دارد.



شکل 3-42 انتخاب گزینه‌ی

2- اگر بر روی services کلیک کنیم، گزینه ای به‌نام TFTP وجود دارد، با کلیک بر روی TFTP تمامی IOS های موجود بر روی دستگاه های مختلف به نمایش در می‌آید.



شکل 3-43 نمایش IOS های

دستورات TFTP

1	Router#**show flash:**
2	Router#**delete flash**
3	Delete filename[]:**c2800nm-advipservicesk9-mz.124-15.T1.bin**
4	Router#**copy tftp:flash:**
5	Address or name of remote host[]? ***آدرس سرور TFTP***
6	Source filename []?**c2800nm-advipservicesk9-mz.124-15.T1.bin**

- خط1: نمایش IOS ها
- خط2: برای پاک کردن IOS از این دستور استفاده می‌شود.
- خط3: بعد از زدن دستور خط 2 ، باید در خط 3، IOS ای که حذف شود را نوشت.
- خط5: با اجرای خط 4، سوال خط 5 پرسیده می‌شود، باید در خط 5 آدرس سرورTFTP را وارد کرد.
- خط6: نام فایلی که باید کپی شود باید وارد شود.

بعد از زدن دستور خط 6، خروجی‌ای به صورت زیر مشاهده می‌شود که این بدان معنی است پروسه‌ی کپی شروع شده است.

```
Router#copy tftp: flash:
Address or name of remote host []? 192.168.50.2
Source filename []? c2800nm-advipservicesk9-mz.124-15.T1.bin
Destination filename [c2800nm-advipservicesk9-mz.124-15.T1.bin]?

Accessing tftp://192.168.50.2/c2800nm-advipservicesk9-mz.124-15.T1.bin....
Loading c2800nm-advipservicesk9-mz.124-15.T1.bin from 192.168.50.2:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 50938004 bytes]


50938004 bytes copied in 3.946 secs (935976 bytes/sec)
```

فصل 4

Switching

مفاهیم سوئیچ[1]

سوئیچ نوع دیگری از ابزارهایی است که برای اتصال چند شبکه محلی به یکدیگر مورد استفاده قرار می‌گیرد که باعث افزایش توان عملیاتی شبکه می‌شود. سوئیچ وسیله ای است که دارای درگاه های متعدد است که

[1] Switch

بسته‌ها را از یک درگاه می‌پذیرد، آدرس مقصد را بررسی می‌کند وسپس بسته‌ها را به درگاه مورد نظر " که متعلق به ایستگاه میزبان با همان آدرس مقصد می‌باشد" ارسال می‌کند. اغلب سوئیچ‌های شبکه محلی در لایه پیوند داده های مدل OSI عمل می‌کنند.

در وجه ظاهری، سوئیچ همانند جعبه‌ایست متشکل از چندین درگاه اترنت که از این لحاظ شبیه هاب‌می‌باشد، با وجود آن‌که هر دو این‌ها وظیفه برقراری ارتباط بین دستگاه‌های مختلف را بر عهده دارند، تفاوت از آنجا آغاز می‌شود که هاب‌بسته‌های ارسالی از طرف یک دستگاه را به همه‌ی درگاه‌های خود ارسال می‌کند و کلیه‌ی دستگاه‌های دیگر علاوه بر دستگاه مقصد این بسته‌ها را دریافت می‌کنند، در حالیکه درسوئیچ ارتباطی مستقیم بین درگاه دستگاه مبدا با درگاه دستگاه مقصد برقرار شده و بسته‌ها مستقیما فقط برای آن ارسال می‌شود.

این خصوصیت از آنجا ناشی می‌شود که سوئیچ می‌تواند بسته‌ها را پردازش کند، در سوئیچ‌های معمولی که به سوئیچ لایه‌ی 2 معروفند این پردازش تا لایه دوم مدل OSI پیش می‌رود و نتیجه این پردازش جدولی است که در سوئیچ با خواندن آدرس سخت افزاری (MAC) فرستنده بسته و ثبت درگاه ورودی تشکیل می‌شود.

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

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

سوئیچ بطور معمول در لایه دوم مدل OSI کار می‌کند ولی سوئیچ‌هایی با قابلیت کارکرد در لایه‌های مختلف حتی لایه هفتم هم وجود دارد. از پرکاربردترین سوئیچ در بین لایه‌های مختلف به جز لایه دوم می‌توان به سوئیچ لایه 3 اشاره کرد که در بسیاری موارد جایگزین مناسبی برای روتر می‌باشد.

مزیت‌ها و قابلیت‌های سوئیچ:

- از سوئیچ می‌توان در یک شبکه خانگی کوچک تا در شبکه های بزرگ با Backbone های چند گیگابایتی استفاده کرد.
- سوئیچ امکان برقراری ارتباط بین ده ها و گاها صدها دستگاه را به طور مستقیم و هوشمند به ما می‌دهد.
- سوئیچ امکان برقرای ارتباط با سرعت بسیار بالا را فراهم می‌کند.
- سوئیچ امکان نظارت و مدیریت بر عملکرد کاربران را فراهم می‌کند.
- سوئیچ امکان کنترل پهنای باند مصرفی کاربران را فراهم می‌کند.
- سوئیچ امکان تفکیک شبکه به بخش‌های کوچکتر و مشخص کردن نحوه دسترسی افراد به قسمت‌های مختلف را فراهم می‌کند.
- و ده ها مزیت دیگر

انواع سوئیچ‌ها

طبقه‌بندی اول

- **سوئیچ‌های قابل مدیریت**[1]

بر روی این سوئیچ‌ها می‌توان IP Address تخصیص داد و پیکربندی را ایجاد کرد. این سوئیچ دارای پورت کنسول می‌باشد.

- **سوئیچ‌های غیرقابل مدیریت**[2]

بر روی این سوئیچ‌ها نمی‌توان IP Address تخصیص داد و پیکربندی انجام داد، هم‌چنین پورت کنسول وجود ندارد.

طبقه بندی دوم

سوئیچ ها بر اساس کاربردشان به دو دسته زیر تقسیم می‌شوند:

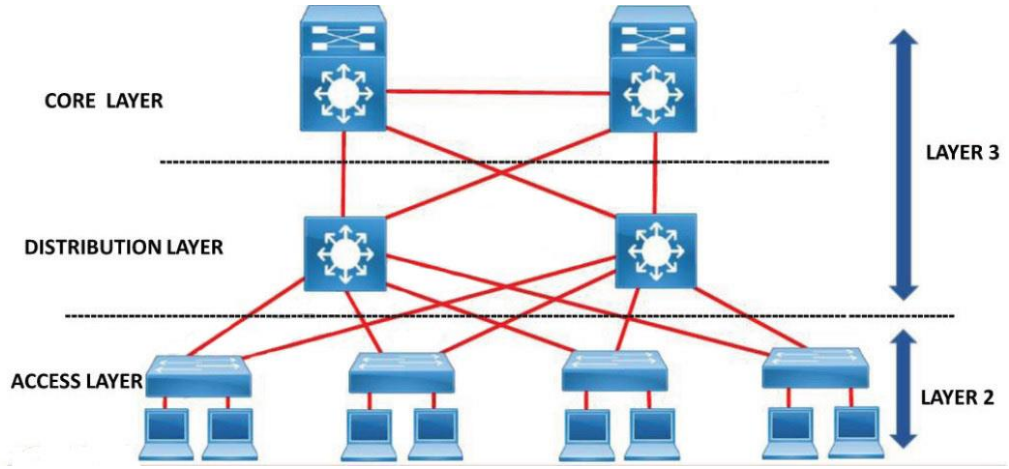
[1] Manageable Switches
[2] Unmanageable Switches

- **متقارن** [1]
در نوع متقارن، عمل سوئیچینگ بین سگمنت‌هایی که دارای پهنای باند یکسان می‌باشند، انجام می‌شود یعنی 10 mbps به 10 mbps و... .
- **نامتقارن**[2]
در نوع نامتقارن عملکرد سوئیچینگ بین سگمنت‌هایی با پهنای باند متفاوت انجام می‌شود.

شبکه Campus

- Campus یک شبکه LAN است که ساختمان‌های بزرگ یا چندین ساختمان نزدیک به یک area خاص را پشتیبانی می‌کند.
- سیسکو از 3 واژه برای توصیف نقش هر سوئیچ در طراحی Campus استفاده می‌کند:

  - Access
  - Distribution
  - Core



شکل 4-1 لایه های مختلف در یک شبکه Campus

طراحی سلسله مراتبی سیسکو برای سوئیچ‌ها

سوئیچ‌های سیسکو می‌توانند به 3 لایه طبقه‌بندی شوند:

- سوئیچ‌های لایه‌ی Access

[1] Symmetric
[2] Asymmetric

سوئیچ‌های سری: 1900، 2950، 2960

- سوئیچ‌های لایه‌ی Distribution

سوئیچ‌های سری:

- ثابت: 3550، 3560، 3750
- ماژولار: 4500، 5500

- سوئیچ‌های لایه‌ی Core

سوئیچ‌های سری: 6500

وضعیت پورت‌های سوئیچ

پورت‌هاي سوئیچ داراي چهار وضعیت هستند:

1- **Block:** پیش فرض در این حالت قرار دارد.
2- **Listen:** شناسایي پورت‌ها و... تشکیل Mac Table.
3- **Learn:** Mac address ها را یاد مي‌گیرد
4- **Send/Receive Forward**: بعد از نوشتن Mac address ها در جدول خودش شروع به forward شدن می کند.

- در سوئیچ جدولي به نام Mac Table قرار دارد که آدرس IP ها به همراه Mac Address ها در آن نگهداري مي شوند. Mac table مشخصه ای 48 بیتی در لایه‌ی Data Link دارای ساختار هگز است.

مزیت وجود Mac Table:

- افزایش سرعت و ارتباطات
- جلوگیري از Broadcast هاي اضافي.

- Mac Table زماني پر مي‌شود که همه‌ي پورت‌هاي آن مشغول باشند.
- ترتیب وضعیت پورت‌هاي سوئیچ:

Block → Listen → Learn → Forward

چگونه اطلاعاتي از Mac Table حذف مي‌شود؟
در صورتي‌كه پورت به صورت فيزيكي خارج شود (قطع شود) يا پورتي را Shut Down كنيم (بصورت منطقي Logical)

- به‌طوركلي سوئيچ ها در دو حالت Broadcast مي‌كنند:

  - زماني‌كه مي‌خواهد اطلاعات از سيستم ها ياد بگيرد.
  - زماني‌كه سوئيچ مي‌خواهد اطلاعاتي را به يك Mac خاص ارسال كند و آدرس سيستم را نداشته باشد ← در سوئيچ‌هاي ديگر Broadcast انجام مي‌دهد تا سيستم مورد نظر خود را پيدا كند.

مدهای سوئیچ

مدهاي سوئيچ نيز شبيه روتر به 3 دسته زير تقسيم مي‌گردد:

1- **User exe mode**
2- **Privilege exe mode**
3- **Global Config mode**

مفاهیم VLAN[1]

VLAN همان‌طور كه از نام آن پيداست شبكه LAN مجازي است كه Broadcast Domain اصلي سوئيچ را كه به‌صورت يك VLAN وجود دارد (VLAN1) به چندين Broadcast Domain ديگر مي‌شكند، به دليل اينكه سوئيچ ها قادر به برقراري ارتباط و Learn كردن از هم هستند لذا چندين پورت از سوئيچ ديگر مي‌توانند عضو VLAN سوئيچ ما باشد بدون اينكه Broadcast را به سوئيچ‌ها يا VLAN هاي ديگر منتقل كند. معمولا VLAN براي شبكه‌هاي بزرگ با ترافيك بالا كاربرد دارد. قبل از اينكه به نحوه تنظيم VLAN بپردازم نكاتي را كه بايد قبل از اين تنظيمات بدانيد را بيان مي‌كنيم.

- VLAN در واقع يك Broadcast Domain مي‌باشد كه توسط سوئيچ ايجاد مي‌شود.
- VLAN امنيت لايه 2 را فراهم مي‌كند.

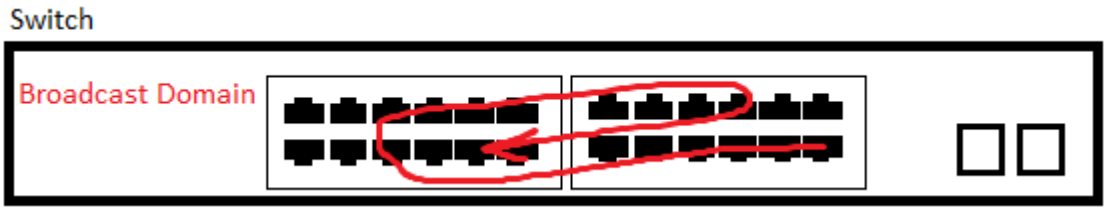
[1] Virtual LAN

- براي تنظيم VLAN مدير شبكه ابتدا بايد VLAN را ايجاد كند و سپس پورت‌هاي سوئيچ را به آن مرتبط سازد.
- همه سوئيچ‌هاي سيسكو داراي يك VLAN (VLAN 1) به‌صورت پيش فرض هستند.
- VLAN مي‌تواند از 2-1001 ايجاد شود.
- در هر VLAN پورتي به نام Trunk تعريف مي‌شود كه قادر است ترافيك‌هاي VLAN را به خارج يا داخل هدايت كند. اين پورت از پروتكل ISL يا 802.1q براي اين كار استفاده مي‌كند. با كلامي ديگر اين پورت بين چندين VLAN مشترك است و كليه‌ی ترافيک آن‌ها را به سوئيچ يا روتر انتقال مي‌دهد
- براي ارتباط چندين VLAN از سوئيچ لايه 3 يا روتر استفاده مي‌شود.

مزاياي VLAN:

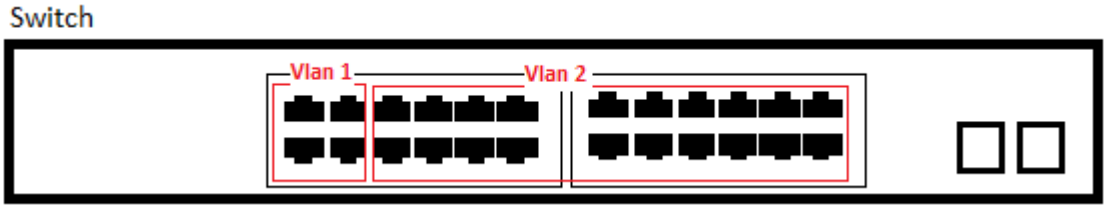
1- Segmentation

به ازاي تمامي پورت‌ها يك Segment در لايه‌ي 2 و يك Broadcast Domain وجود دارد.
به ازاي هر VLAN يك Broadcast Domain وجود دارد.



شكل 4-2 نمايشي از Broadcast Domain كلي

- به‌صورت پيش‌فرض به ازاي تمامي پورت‌هاي سوئيچ يك Vlan با شماره‌ي 1 وجود دارد.
- حال اگر بخواهيم مثلا دو Segment مختلف ايجاد كنيم بايد دو Vlan بسازيم كه Vlan آنها جدا مي‌شود و در نتيجه Broadcast Domain آن‌ها نيز از هم جدا مي‌گردد.



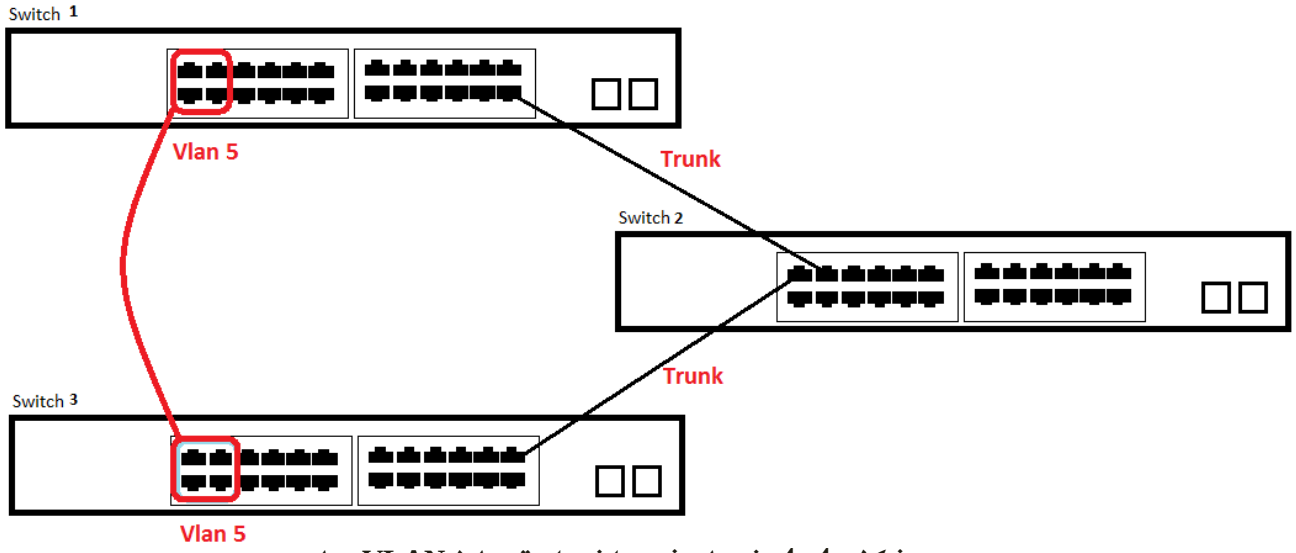
شكل 4-3 نمايشي از ايجاد VLAN هاي مختلف بر

دلیل ایجاد سگمنت در شبکه‌ها افزایش بازدهی و کارایی شبکه می‌باشد.

2- Flexibility:

قابلیت انعطاف پذیری در شبکه به‌وجود می‌آید.

- مثلا می‌خواهیم دو پورت از یک سوئیچ را به پورت سوئیچ دیگر در یک Vlan قرار دهیم و آنهایی که در یک Vlan قرار دارند دارای یک Broadcast هستند.



شکل 4-4 نمایشی از ارتباط VLAN های

3- Security: ایجاد امنیت

- Mode های پورت‌های سوئیچ (Switch Interface Mode):
  - **Access:** در حالتی است که سوئیچ به PC متصل می‌گردد که در حالت پیش‌فرض در این حالت قرار دارد.
  - **Trunk:** حالتی است که سوئیچ به سوئیچ متصل شده است.

نکات:

- شرط مد trunk در هر سوئیچی داشتن Vlanهایی غیر از Vlan 1 می باشد.
- اگر Vlan ای به غیر از Vlan 1 وجود نداشته باشد، سوئیچ‌ها را در مد access هم می‌شود بهم کانکت کرد.
- Trunk عضو هیچ Vlan ای نمی‌باشد، فقط برای انتقال ترافیک چندین Vlan استفاده می‌شود.
- پروتکل‌های trunk دو نوع می‌باشند:

- ISL[1]
- 802.1q

ISL	802.1q
مخصوص سیسکو	استاندارد باز
30 بایت	4 بایت

انواع VLAN

- **Static VLAN**

- این VLAN ها براساس پورت هستند، از این‌رو VLAN های براساس پورت نامیده‌شده اند.
- پورت‌ها به‌صورت دستی به یک VLAN اختصاص داده می‌شود.
- یک پورت می‌تواند عضوی از یک VLAN واحد باشد.

- **Dynamic VLAN**

- براساس MAC Address یک دستگاه می‌باشند.
- سوئیچ به‌صورت اتوماتیک، پورت را به یک VLAN اختصاص می‌دهد.
- هر پورت می‌تواند عضوی از چندین VLAN باشد.
- برای پیکربندی این نوع VLAN، یک نرم‌افزار با نام VMPS[2] مورد نیاز است.

پیکربندی VLAN

[1] Inter Switch Link
[2] VLAN Management Policy Server

جهت مشاهده‌ي Vlan هاي موجود در سوئيچ از دستور زير استفاده مي‌كنيم:

```
1  Switch#show vlan brief
   VLAN Name                             Status    Ports
   ---- -------------------------------- --------- -------------------------------
   1    default                          active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                   Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                   Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                   Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                   Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                   Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                                   Gig0/1, Gig0/2
   1002 fddi-default                     active
   1003 token-ring-default               active
   1004 fddinet-default                  active
   1005 trnet-default                    active
```

ساخت Vlan

```
1  Switch(config)#vlan 20
2  Switch(config-vlan)#name Test
3
4  Switch(config-vlan)#vlan 30
5  Switch(config-vlan)#name CCNA
6
7  Switch#show vlan brief
```

```
Switch#show vlan brief
VLAN  Name                             Status    Ports
----  -------------------------------- --------- -------------------------------
1     default                          active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                 Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                 Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                 Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                 Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                 Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                                 Gig0/1, Gig0/2
20    Test
30    CCNA
1002  fddi-default                     active
1003  token-ring-default               active
1004  fddinet-default                  active
1005  trnet-default                    active
```

- خط 1: ساخت Vlan به شماره 20
- خط 2: اختصاص نام به Vlan شماره 20
- خط 4: ساخت Vlan با شماره 30
- خط 5: اختصاص نام به Vlan شماره 30

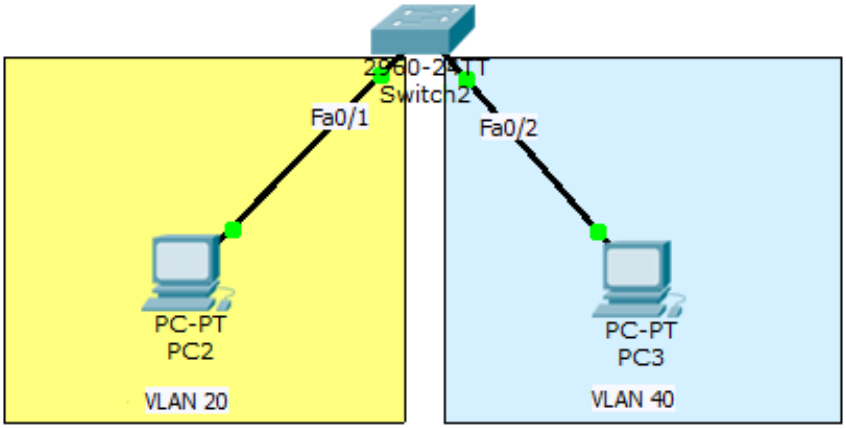
قبل از اينكه پورت‌هاي سوئيچ را به Vlan خاصي اختصاص دهيم ابتدا بايد Vlan را در سوئيچ مورد نظر بسازيم (در غير اينصورت با پيغام خطا مواجه مي شويم .% Access VLAN does not exist (Creating vlan ... سپس پورت‌ها را در Vlanهاي ساخته شده قرار دهيم.

دستور حذف Vlan:

1	Switch(config)#**no vlan 20**

سناريو: اتصال سوئيچ به كامپيوتر

مثال: سناريوي شكل(4-5) را اجرا كنيد:



شکل 4-5 سناریو اتصال سوئیچ

1- ابتدا باید VLAN ها را تعریف کنیم:

```
Switch(config)#vlan 20
Switch(config-vlan)#vlan 40
```

2- حال وضعیت پورت‌ها را تعریف می‌کنیم، چون پورت‌های سوئیچ به کامپیوتر وصل شده اند ← از نوع Access باید تعریف گردند.

```
1 Switch(config)#interface fastEthernet 0/1
2 Switch(config-if)#switchport mode access
3 Switch(config-if)#switchport access vlan 20
4 Switch(config-if)#do show vlan brief
```

- خط 1: وارد Interface مربوطه می‌شویم.
- خط 2: مد پورت را مشخص می‌کنیم. در اینجا چون پورت سوئیچ به کامپیوتر متصل شده است درنتیجه از نوع Access باید تعریف گردد.
- خط 3: حال باید Interface مورد نظر را در Vlan مربوطه (مطابق شکل) قرار دهیم.
- خط 4: خلاصه دستور : SW#Show vlan brief می‌باشد.

```
Switch#show vlan brief
VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/2, Fa0/3, Fa0/4, Fa0/5
                                                Fa0/6, Fa0/7, Fa0/8, Fa0/9
                                                Fa0/10, Fa0/11, Fa0/12, Fa0/13
```

			Fa0/14, Fa0/15, Fa0/16, Fa0/17 Fa0/18, Fa0/19, Fa0/20, Fa0/21 Fa0/22, Fa0/23, Fa0/24, Gig0/1 Gig0/2
20	VLAN0020	active	Fa0/1
40	VLAN0040	active	
1002	fddi-default	active	
1003	token-ring-default	active	
1004	fddinet-default	active	
1005	trnet-default	active	

همانگونه که در شکل مي‌بينيم، Interface Fa 0/1 در Vlan 20 قرار گرفت.
براي Interface fa 0/2 نيز دقيقا کارهاي بالا را مطابق با سناريو انجام مي‌دهيم.

```
1  Switch(config)#int f0/2
2  Switch(config-if)#switchport mode access
3  Switch(config-if)#switchport access vlan 40
4  Switch(config-if)#do show vlan brief
```

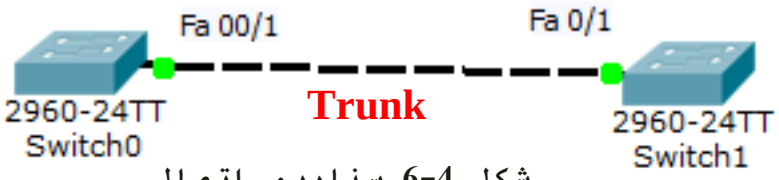
```
Switch#show vl br
VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/2, Fa0/3, Fa0/4, Fa0/5
                                                Fa0/6, Fa0/7, Fa0/8, Fa0/9
                                                Fa0/10, Fa0/11, Fa0/12, Fa0/13
                                                Fa0/14, Fa0/15, Fa0/16, Fa0/17
                                                Fa0/18, Fa0/19, Fa0/20, Fa0/21
                                                Fa0/22, Fa0/23, Fa0/24, Gig0/1
                                                Gig0/2
20   VLAN0020                         active    Fa0/1
40   VLAN0040                         active    Fa0/2
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
```

سناريو: اتصال سوئيچ ها با يکديگر

سوئيچ‌ها را بايد با کابل Cross به يکديگر متصل کنيم.

می‌خواهیم Vlanning را بر روی بیشتر از یک سوئیچ داشته باشیم درنتیجه باید ارتباطات بین سوئیچ‌ها را Trunk تعریف کنیم.

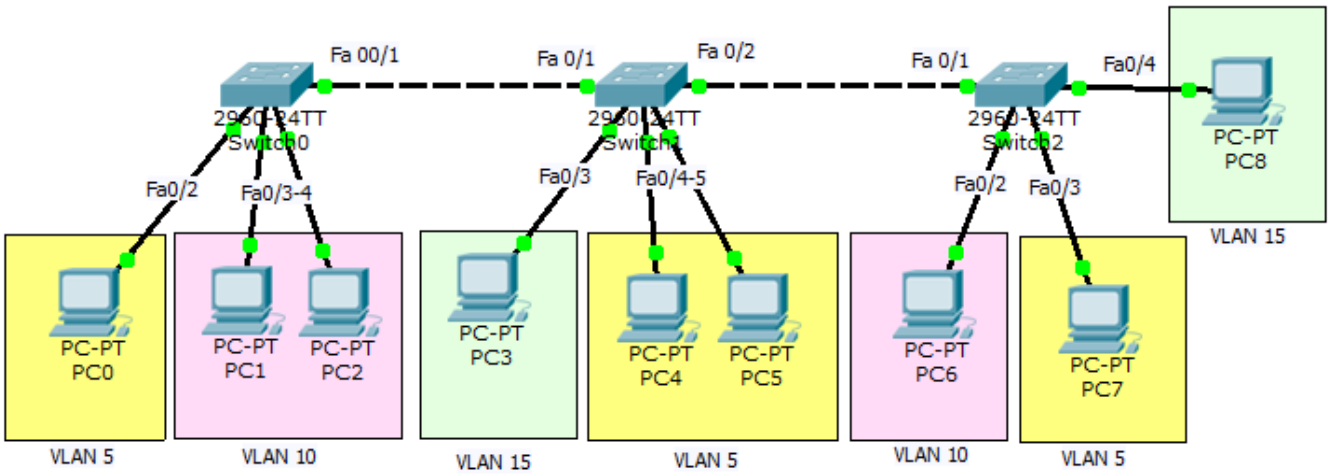
```
1  Switch(config)#interface fastEthernet 0/1
2  Switch(config-if)#switchport mode trunk
3
4  Switch#show interfaces trunk
```



شکل 4-6 سناریو اتصال

```
Switch#show interfaces trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/1       on           802.1q         trunking      1

Port        Vlans allowed on trunk
Fa0/1       1-1005

Port        Vlans allowed and active in management domain
Fa0/1       1

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/1       none
```

سناریو: سوئیچ و VLAN:



شکل 4-7 سناریو سوئیچ و VLAN

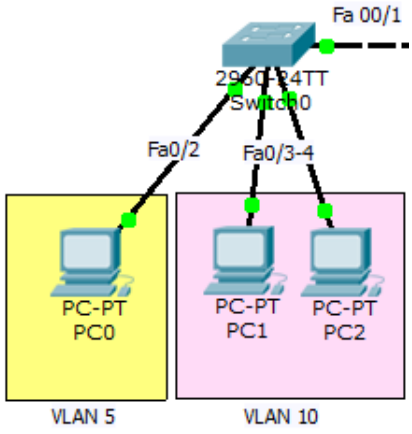
VLAN 5: 192.168.5.0/24
VLAN 10: 192.168.10.0/24
VLAN 15: 192.168.15.0/24

ترتیب اجرای سناریو:

1- ایجاد Vlanها مطابق با سوئیچهای مورد نظر
2- اختصاص پورتهای Access به ازای کامپیوترها و راه اندازی لینکهای trunk
3- اختصاص IP به کامپیوترها و تست ارتباط مابین Vlan های همنام

Sw0

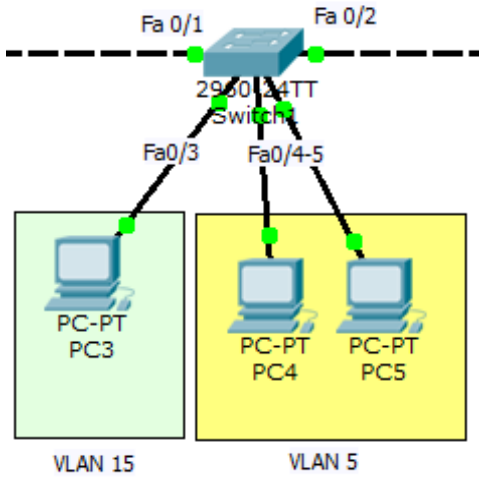
1	Switch(config)#**vlan 5**
2	Switch(config-vlan)#**vlan 10**
3	
4	Switch(config)#**interface fastEthernet 0/1**
5	Switch(config-if)#**switchport mode trunk**
6	
7	Switch(config)#**interface fastEthernet 0/2**
8	Switch(config-if)#**switchport mode access**
9	Switch(config-if)#**switchport access vlan 5**
10	
11	Switch(config)#**interface range fastEthernet 0/3-4**
12	Switch(config-if-range)#**switchport mode access**
13	Switch(config-if-range)#**switchport access vlan 10**



```
Switch#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                                Gig0/1, Gig0/2
5    VLAN0005                         active    Fa0/2
10   VLAN0010                         active    Fa0/3, Fa0/4
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
```

SW1

```
1  Switch(config)#interface range fastEthernet 0/1-2
2  Switch(config-if-range)#switchport mode trunk
3
4  Switch(config)#interface fastEthernet 0/3
5  Switch(config-if)#switchport mode access
6  Switch(config-if)#switchport access vlan 15
7
8  Switch(config)#interface range fa 0/4-5
9  Switch(config-if-range)#switchport mode access
10 Switch(config-if-range)#switchport access vlan 5
```

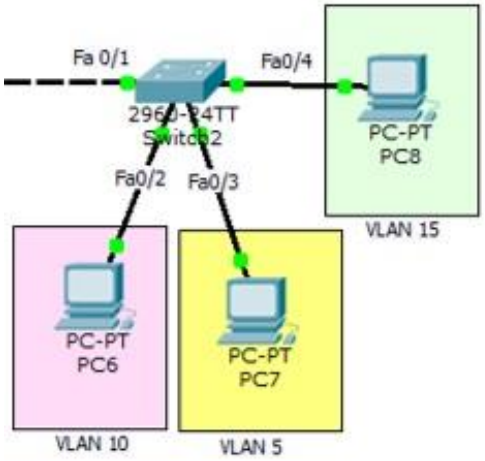



```
Switch#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/6, Fa0/7, Fa0/8, Fa0/9
                                                Fa0/10, Fa0/11, Fa0/12, Fa0/13
                                                Fa0/14, Fa0/15, Fa0/16, Fa0/17
                                                Fa0/18, Fa0/19, Fa0/20, Fa0/21
                                                Fa0/22, Fa0/23, Fa0/24, Gig0/1
                                                Gig0/2
5    VLAN0005                         active    Fa0/4, Fa0/5
10   VLAN0015                         active    Fa0/3
```

1002	fddi-default	active
1003	token-ring-default	active
1004	fddinet-default	active
1005	trnet-default	active

Sw2

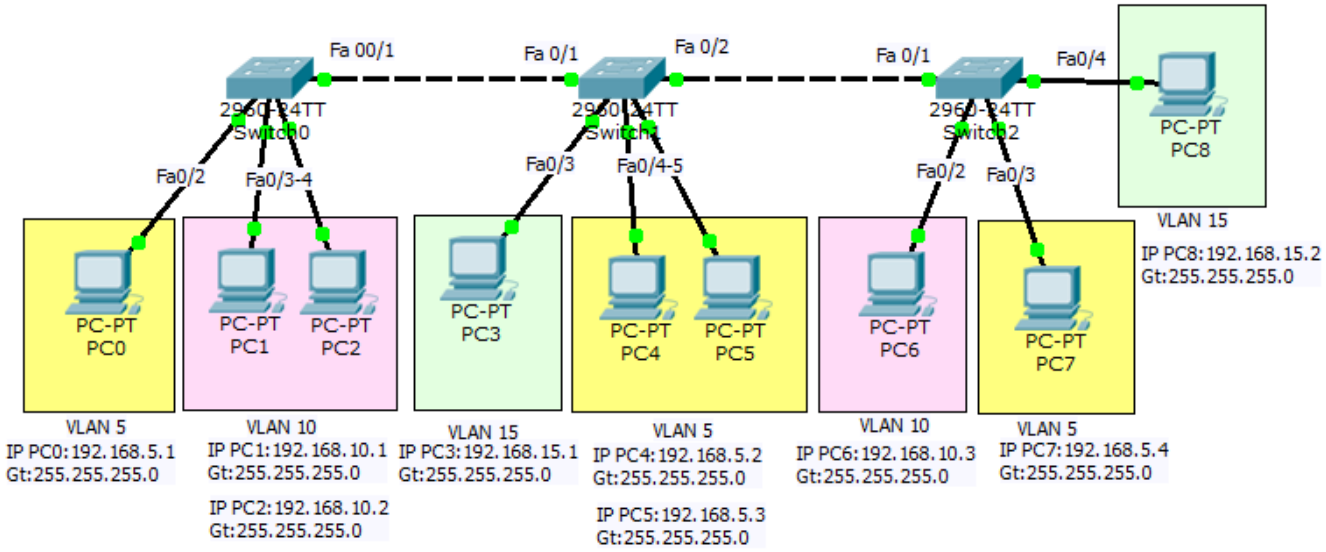
```
1   Switch(config)#vlan 10
2   Switch(config-vlan)#vlan 5
3   Switch(config-vlan)#vlan 15
4
5   Switch(config)#int f0/2
6   Switch(config-if)#switchport mode access
7   Switch(config-if)#switchport access vlan 10
8
9   Switch(config-if)#int f0/3
10  Switch(config-if)#switchport mode access
11  Switch(config-if)#switchport access vlan 5
12
13  Switch(config-if)#int fa 0/4
14  Switch(config-if)#switchport mode access
15  Switch(config-if)#switchport access vlan 15
```




```
Switch#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                                Gig0/1, Gig0/2
5    VLAN0005                         active    Fa0/3
10   VLAN0010                         active    Fa0/2
15   VLAN0015                         active    Fa0/4
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
```

حال باید به کامپیوترها IP اختصاص دهیم:

در IP دادن به کامپیوترها نیاز به تعریف Gateway نداریم چون همه Switch هستند.



پروتکل VTP[1]

قرارداد VTP برای ساده کردن کار مدیریت VLAN ها توسط شرکت سیسکو ارائه شده است. با استفاده از VTP می‌توان اقدام به ایجاد و حذف اتوماتیک Vlan ها بر روی سوئیچ‌های موجود در شبکه نمود، بدون آنکه عملیات ایجاد و یا حذف نمودن VLANها را بر روی تک تک سوئیچ‌ها انجام داد. این پروتکل براي زماني‌که تعداد سوئیچ‌ها در شبکه افزایش یابد جهت مدیریت Vlanها بسیار مفید مي‌باشد. VTP یک پروتکل مخصوص سیسکو می‌باشد.

مزیت‌های پروتکل VTP:

- از یک نقطه‌ی مرکزی، روی شبکه می‌توان مدیریت داشت.
- می‌توان شبکه‌ی سوئیچ‌ها را که به صورت client/server ایجاد شده است را داخل یک domain قرار داد و از مکانیزم‌های پسوردگذاری ما بین ارتباط سوئیچ‌ها استفاده کرد.

مدهاي VTP:

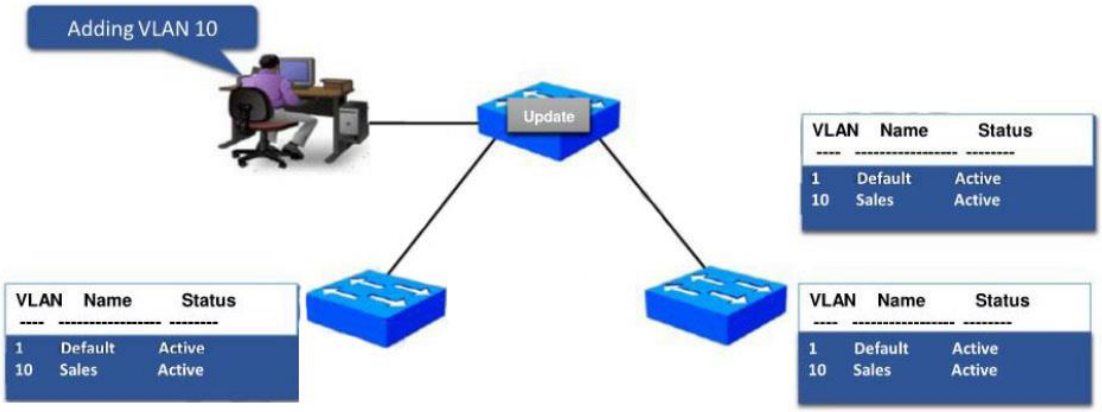
به‌طور کلی مدهای VTP به 3 دسته تقسیم می‌شوند:

- **Server:** مدیریت، ایجاد و بهره‌برداری اصلی از VLAN ها را در شبکه تعریف می‌کند. پیش فرض تمامي سوئیچ‌ها است.
- **Client:** دخل و تصرفی در محتوای VLAN ها ندارد، اطلاعات VLAN ها را از سرور دریافت می‌کند و از اطلاعات استفاده می‌کند.
- **Transparent:** سوئیچی است مجزا که هیچ ارتباطی به کلاینت و سرور به صورت مستقیم ندارد، خودش به‌صورت مستقل می‌تواند VLAN ایجاد می‌کند و از آن‌ها استفاده می‌کند.

به عنوان مثال فرض کنید که شما 3 سوئیچ در اختیار دارید و می‌خواهید روی همه‌ی آنها VlAN 10 یکسان ایجاد نمایید. در این صورت بایستی یک به یک به سوئیچ‌ها متصل شده و VLAN های مورد نظر خود را بر روی آن‌ها ایجاد نمایید. اما هنگامی که شما از قرارداد VTP استفاده کرده و تنظیمات مورد نیاز را اعمال نمایید، هنگامی که بر روی یک سوئیچ VLAN

[1] VLAN Trunking Protocol

ای را ایجاد نمایید، به صورت خودکار این VLAN بر روی تمامی سوئیچ های دیگر نیز ایجاد خواهد شد. لازم به ذکر است که این فرآیند در مورد حذف کردن VLAN ها نیز صادق می‌باشد.



شکل 4-8 نحوه‌ی کارکرد VTP

برای اجرای VTP روی سوئیچ‌ها ابتدا باید یک سوئیچ به عنوان سرور و مابقی سوئیچ ها به عنوان کلاینت انتخاب شوند.

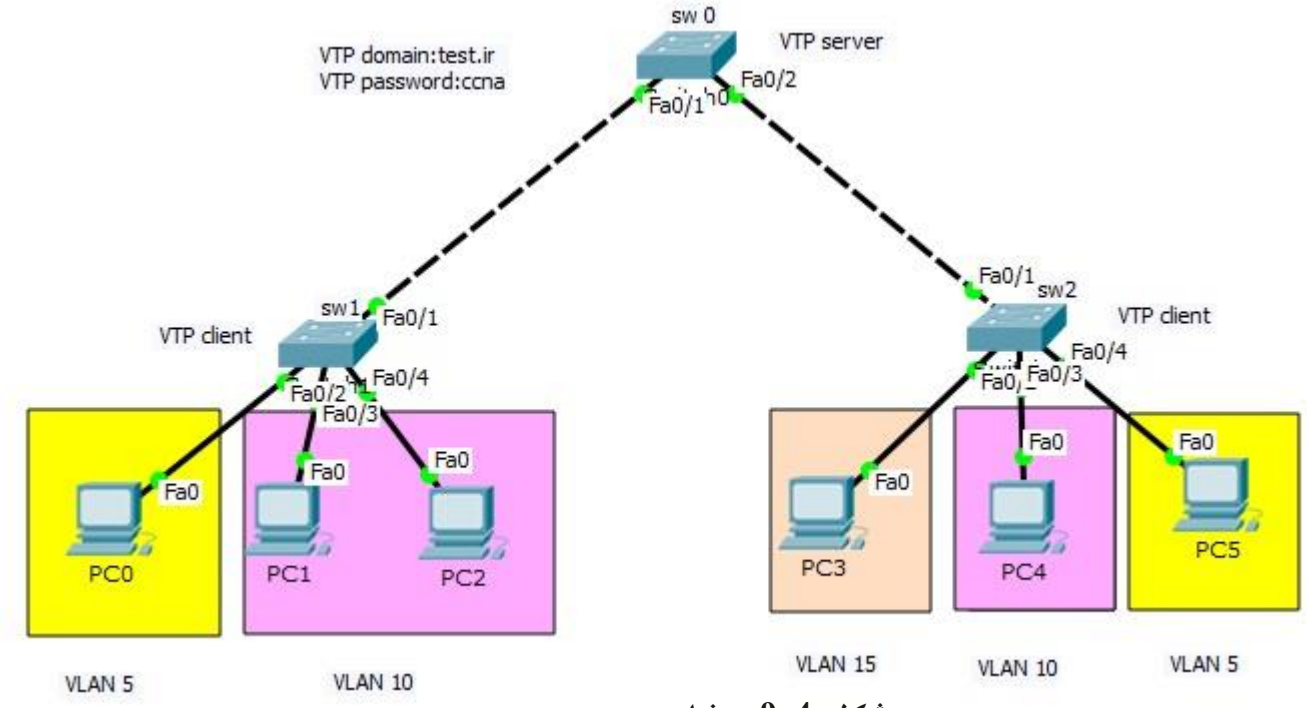
دستورات VTP

1	Switch(config)#**vtp mode [client | server | transparent]**
2	Switch(config)#**vtp domain** نام دامنه ی مورد نظر
3	Switch(config)#**vtp password** پسورد مورد نظر
4	Switch#**show vtp status**
5	Switch#**show interface trunk**

- خط1: تعیین اینکه سوئیچ در چه مدی از VTP قرار گرفته است.
- خط2: ایجاد یک Domain Name. این Domain Name یک مورد حساسی بوده و باید در همه‌ی سوئیچ‌ها با یک نام مشابه تنظیم شود. این خط اجباری می‌باشد.
- خط3: قرار دادن یک پسورد
- خط4: نمایش تغییرات
- خط5: اینترفیس‌های از نوع Trunk را نمایش می‌دهد.

ساختار ارتباطی سوئیچ‌ها در VTP باید به صورت Trunk باشد. چون از طریق سوئیچ سرور، Vlanها و اطلاعات آن‌ها برای کلاینت‌ها ارسال خواهد شد و در حقیقت کلاینت‌ها از طریق سرور آپدیت می‌شوند، به همین خاطر مسلما Vlan هایی غیر از Vlan1 وجود دارد.

سناریو VTP

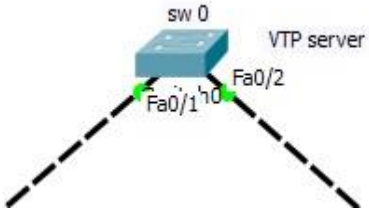


شکل 4-9 سناریو VTP

مراحل اجراي سناريو VTP:

1. اتصال سوئیچ‌ها به یکدیگر و تعریف لینک‌هاي Trunk .
2. مشخص نمودن اطلاعات پروتکل VTP مطابق با شکل و ایجاد Vlan ها در سوئیچ سرور
3. مشاهده‌ي Vlanها در سوئیچ‌هاي کلاینت و اختصاص پورت‌ها به ازاي آن‌ها
4. اختصاص IP Add. مطابق با Vlan و تست ارتباط مابین Vlanهاي هم نام.

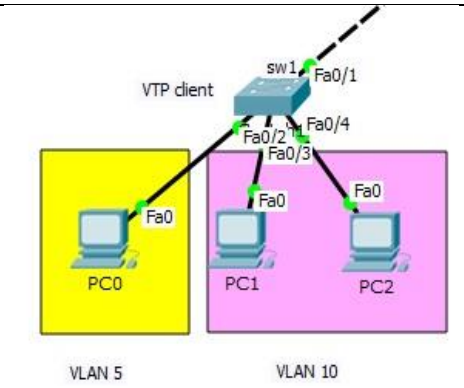
Sw0

1	Switch(config)#**int range fastEthernet 0/1-2**	
2	Switch(config-if-range)#**switchport mode trunk**	
3		
4	Switch(config)#**vtp mode server**	
5	Device mode already VTP SERVER.	
6		
7	Switch(config)#**vtp domain test.ir**	
8	Changing VTP domain name from NULL to test.ir	
9		
10	Switch(config)#**vtp password ccna**	
11	Setting device VLAN database password to ccna	
12		
13	Switch(config)#**vlan 5**	
14	Switch(config)#**vlan 10**	
15	Switch(config)#**vlan 15**	

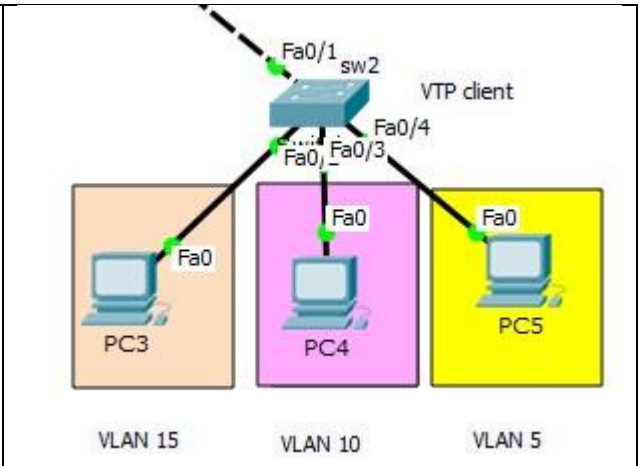
- خط 1 تا 2: مد لینك بین سوئیچ‌ها را مشخص می‌کنیم که از نوع Trunk است.
- خط 4: Switch 0 را از نوع Server انتخاب می‌کنیم.
- خط 7: دامنه را تعریف می‌کنیم.
- خط 10: پسورد دامنه را تعریف می‌کنیم.
- خط 13 الی 15: Vlan ها را تعریف می‌کنیم.

حال باید تنظیمات سوئیچ‌هاي کلاینت را انجام دهیم:

Sw1

1 2 3 4 5 6 7 8	Switch(config)#**interface fastEthernet <u>0/1</u>** Switch(config-if)#**switchport mode <u>trunk</u>** Switch(config)#**vtp mode <u>client</u>** Setting device to VTP CLIENT mode. Switch(config)#**vtp password <u>ccna</u>** Setting device VLAN database password to ccna	

Sw2

1 2 3 4 5 6 7 8	Switch(config)#**interface fastEthernet <u>0/1</u>** Switch(config-if)#**switchport mode <u>trunk</u>** Switch(config)#**vtp mode <u>client</u>** Setting device to VTP CLIENT mode. Switch(config)#**vtp password <u>ccna</u>** Setting device VLAN database password to ccna	

حال مي‌بينيم كه Vlan هاي تعريف شده در سرور به كلاينت‌ها نيز منتقل شده است.

Sw1, Sw2

Switch#**show vlan brief**

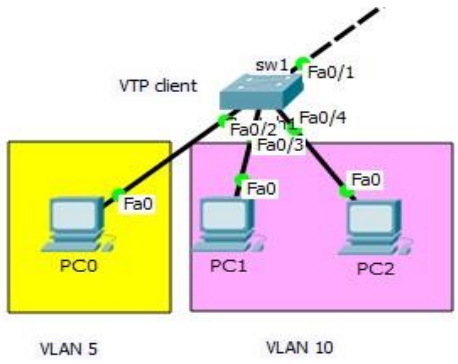
VLAN	Name	Status	Ports
1	default	active	Fa0/2, Fa0/3, Fa0/4, Fa0/5 Fa0/6, Fa0/7, Fa0/8, Fa0/9 Fa0/10, Fa0/11, Fa0/12, Fa0/13 Fa0/14, Fa0/15, Fa0/16, Fa0/17 Fa0/18, Fa0/19, Fa0/20, Fa0/21 Fa0/22, Fa0/23, Fa0/24, Gig0/1 Gig0/2

5	VLAN0005	active
10	VLAN0010	active
15	VLAN0015	active
1002	fddi-default	active
1003	token-ring-default	active
1004	fddinet-default	active
1005	trnet-default	active

حال مي‌توانيم به راحتي Interface هاي سوئيچ‌هاي كلاينت را در Vlan هاي مربوطه قرار دهيم.

Sw1

```
1  Switch(config)#interface fastEthernet 0/2
2  Switch(config-if)#switchport mode access
3  Switch(config-if)#switchport access vlan 5
4
5  Switch(config-if)#int range fa 0/3-4
6  Switch(config-if-range)#switchport mode access
7  Switch(config-if-range)#switchport access vlan
8  10
9  Switch#show vlan brief
10
```

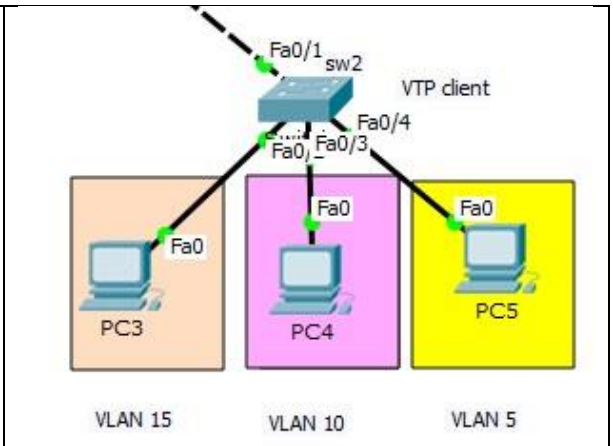


Switch#**show vlan brief**

VLAN	Name	Status	Ports
1	default	active	Fa0/5, Fa0/6, Fa0/7, Fa0/8 Fa0/9, Fa0/10, Fa0/11, Fa0/12 Fa0/13, Fa0/14, Fa0/15, Fa0/16 Fa0/17, Fa0/18, Fa0/19, Fa0/20 Fa0/21, Fa0/22, Fa0/23, Fa0/24 Gig0/1, Gig0/2
5	VLAN0005	active	Fa0/2
10	VLAN0010	active	Fa0/3, Fa0/4
15	VLAN0015	active	
1002	fddi-default	active	
1003	token-ring-default	active	
1004	fddinet-default	active	
1005	trnet-default	active	

Sw2

```
1  Switch(config)#int f0/2
2  Switch(config-if)#switchport mode access
3  Switch(config-if)#switchport access vlan 15
4
5  Switch(config-if)#int f0/3
6  Switch(config-if)#switchport mode access
7  Switch(config-if)#switchport access vlan 10
8
9  Switch(config-if)#int f0/4
10 Switch(config-if)#switchport mode access
11 Switch(config-if)#switchport access vlan 5
12
   Switch#show vlan brief
```




```
Switch#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                                Gig0/1, Gig0/2
5    VLAN0005                         active    Fa0/4
10   VLAN0010                         active    Fa0/3
15   VLAN0015                         active    Fa0/2
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
```

كانفيگ كلي سوئيچ 1 :

Sw1

```
1  Switch(config)#interface fastEthernet 0/1
2  Switch(config-if)#switchport mode trunk
3
4  Switch(config)#vtp mode client
5  Setting device to VTP CLIENT mode.
6
```

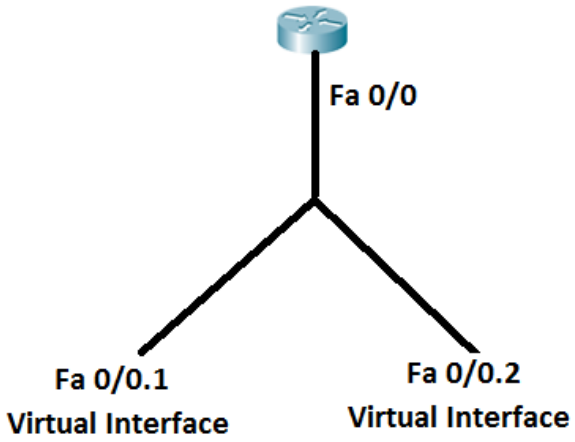
```
7  Switch(config)#vtp password ccna
8  Setting device VLAN database password to ccna
9
10 Switch(config)#interface fastEthernet 0/2
11 Switch(config-if)#switchport mode access
12 Switch(config-if)#switchport access vlan 5
13
14 Switch(config-if)#int range fa0/3-4
15 Switch(config-if-range)#switchport mode access
16 Switch(config-if-range)#switchport access vlan 10
17
18 Switch#show vlan brief
```

کانفیگ کلی سوئیچ 2:

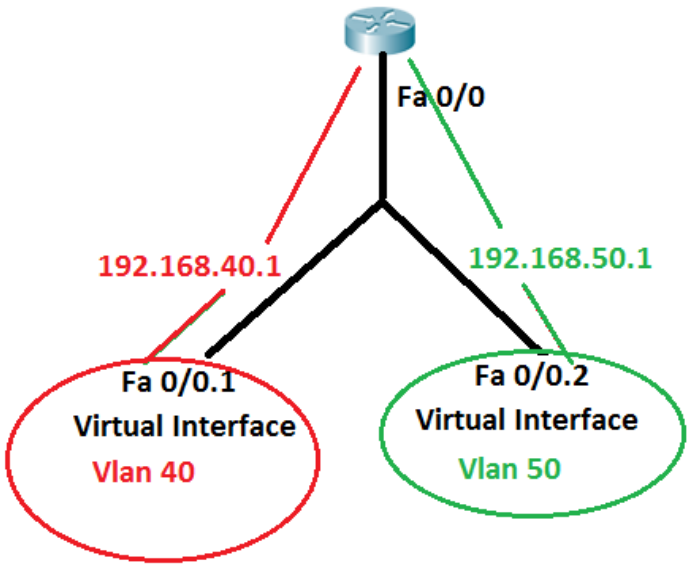
```
1  Switch(config)#int f0/1
2  Switch(config-if)#switchport mode trunk
3
4  Switch(config)#vtp mode client
5  Setting device to VTP CLIENT mode.
6
7  Switch(config)#vtp password ccna
8  Setting device VLAN database password to ccna
9
10 Switch(config)#int f0/2
11 Switch(config-if)#switchport mode access
12 Switch(config-if)#switchport access vlan 15
13
14 Switch(config-if)#int f0/3
15 Switch(config-if)#switchport mode access
16 Switch(config-if)#switchport access vlan 10
17
18 Switch(config-if)#int f0/4
19 Switch(config-if)#switchport mode access
20 Switch(config-if)#switchport access vlan 5

21 Switch#show vlan brief
```

Inter-Vlan Routing

- پروسه‌ی ارسال ترافیک شبکه از یک Vlan به Vlan دیگری می‌باشد (برای اتصال دو Vlan غیر هم نام به یکدیگر استفاده می‌شود).
- برای انجام Inter-Vlan Routing باید از یک دستگاه لایه3 (مثلا روتر) استفاده شود.
- روتر را باید به سوئیچ سرور وصل کرد.
- از تکنیك Sub interface استفاده مي‌كنيم. يك Interface حقيقي به دو Subinterface تقسيم مي‌شود (مثل سه راهي).
- هر Sub interface باید به یک Vlan اختصاص داده شود.
- پورت سوئیچ اختصاص داده شده به روتر باید در مد Trunk باشد.



شکل 4-10 شمایی از



شکل 4-11 شمایی از قراردادن اینترفیس های

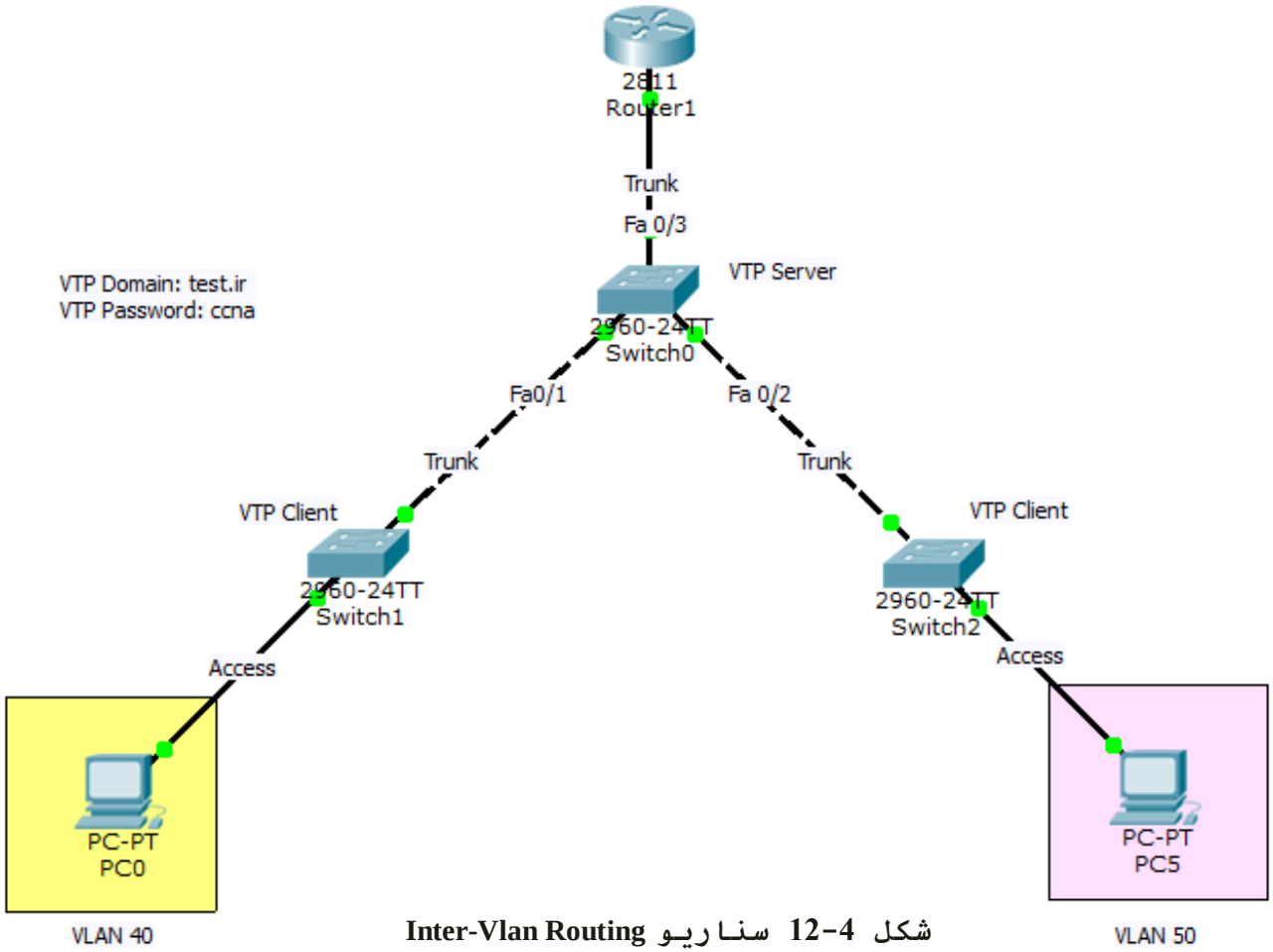
Fa0/0 اینترفیس حقیقی و Fa0/0.1 و Fa0/0.2 اینترفیس مجازی است که رنج IP هایشان با هم متفاوت می‌باشد.

انجام Inter-Vlan Routing شامل مراحل زیر می‌باشد:

1) Trunk کردن لینک بین سوئیچ‌های موجود
2) تعریف دستورات VTP در صورتی که سوئیچ سرور و کلاینت وجود داشته باشد
3) تعریف Vlaning
4) تخصیص پورت ها در سوئیچ‌ها
5) Trunk کردن لینک بین سوئیچ و روتر
6) اتصال VLAN های غیرهمنام (ایجاد Sub- interface)

سناریو : Inter-vlan Routing

سناریوي شکل(4-12) را اجرا کنید و کاري کنید که کامپیوترها همدیگر را پینگ کنند.



شکل 4-12 سناریو Inter-Vlan Routing

Sw0

```
1  Switch(config)#int range fastEthernet 0/1-2
2  Switch(config-if-range)#switchport mode trunk
3
4  Switch(config)#interface fastEthernet 0/3
5  Switch(config-if)#switchport mode trunk
6
7  Switch(config)#vtp mode server
8  Device mode already VTP SERVER.
9
10 Switch(config)#vtp domain test.ir
11 Changing VTP domain name from NULL to test.ir
```

```
12
13  Switch(config)#vtp password ccna
14  Setting device VLAN database password to ccna
15
16  Switch(config)#vlan 50
17  Switch(config)#vlan 40
```

- خط 1 و 2: مانند سناريوهاي قبل، پورت‌هاي بين سوئيچ‌ها را از نوع trunk تعريف مي‌كنيم.
- خط 4 و 5: پورت بين سوئيچ و روتر را بايد از نوع Trunk تعريف كنيم.
- باقي تعريف‌ها همانند سناريوي قبل.

Sw1:

```
1   Switch(config)#interface fastEthernet 0/1
2   Switch(config-if)#switchport mode trunk
3
4   Switch(config)#vtp mode client
5   Setting device to VTP CLIENT mode.
6
7   Switch(config)#vtp password ccna
8   Setting device VLAN database password to ccna
9
10  Switch(config)#interface fastEthernet 0/2
11  Switch(config-if)#switchport mode access
12  Switch(config-if)#switchport access vlan 40
13
14  Switch#show vlan brief
15
```

Sw2:

```
1   Switch(config)#interface fastEthernet 0/1
2   Switch(config-if)#switchport mode trunk
3
4   Switch(config)#vtp mode client
5   Setting device to VTP CLIENT mode.
6
7   Switch(config)#vtp password ccna
8   Setting device VLAN database password to ccna
9
10  Switch(config)#interface fastEthernet 0/2
11  Switch(config-if)#switchport mode access
12  Switch(config-if)#switchport access vlan 50
```

```
13
14  Switch#show vlan brief
```

Router

```
1   Router(config-if)#interface fastEthernet 0/0.1
2   Router(config-subif)#encapsulation dot1Q 40
3   Router(config-subif)#ip address 192.168.40.1 255.255.255.0
4
5   Router(config)#interface fastEthernet 0/0.2
6   Router(config-subif)#encapsulation dot1Q 50
7   Router(config-subif)#ip address 192.168.50.1 255.255.255.0
8
9   Router(config)#interface fastEthernet 0/0
10  Router(config-if)#no sh
11
12  Router(config-if)#
13  %LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up
14
15  %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to
16  up
17
18  %LINK-5-CHANGED: Interface FastEthernet0/0.1, changed state to up
19
20  %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0.1, changed state
21  to up
22
23  %LINK-5-CHANGED: Interface FastEthernet0/0.2, changed state to up

    %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0.2, changed state
    to up
```

مي‌خواهيم پورت‌هاي مجازي را تعريف نماييم.

- خط 1 و 5: وارد پورت‌هاي مجازي مي‌شويم.
- خط 2و 6: حتما در جلوي هر كدام بايد شماره Vlan اي كه پورت مجازي به آن اتصال دارد را بنويسيم. مثلا پورت مجازي Fa 0/0.1 در Vlan 40 قرار دارد.
- خط 3و 7: IP هر رنج از Vlan ها را به پورت‌هاي مجازي اختصاص مي‌دهيم.
- خط 9: وارد پورت حقيقي روتر مي‌شويم.
- خط 10: No shutdown مي‌كنيم.

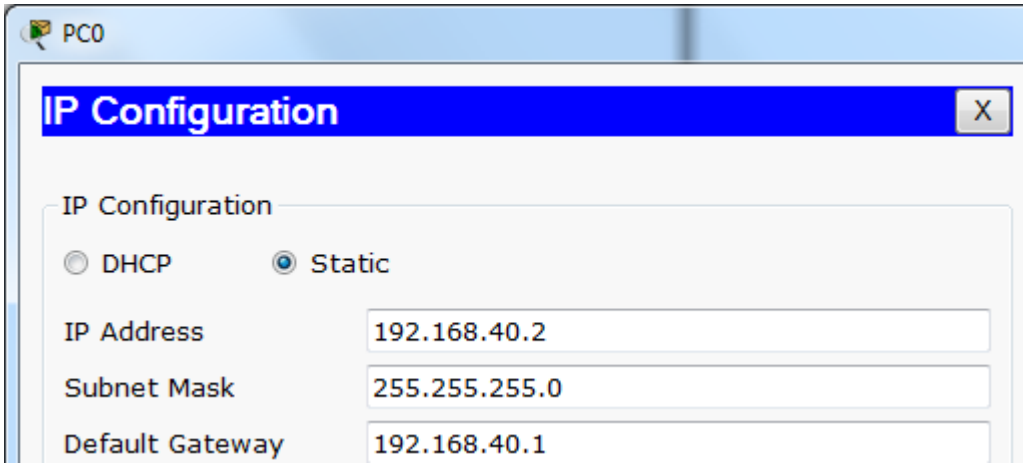
اگر پورت حقیقي را Up نكنيم، پورت‌هاي مجازي Up نمي‌شوند

- همان‌طوري كه در خطوط 13 به بعد مشاهده مي‌فرماييد، 3 پورت را Up مي‌كند كه شامل يك پورت حقيقي و دو پورت مجازي است.

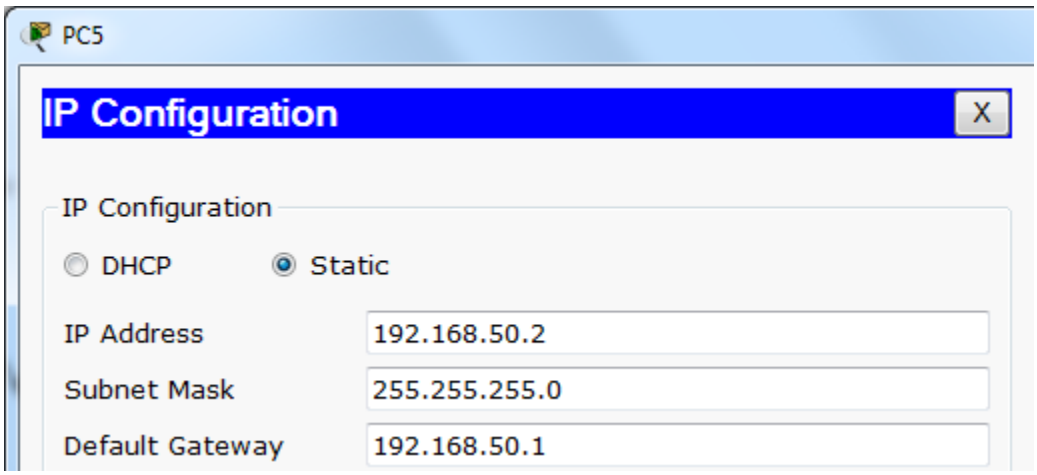
اختصاص IP به كامپيوترها:

Gateway هر كدام از كامپيوترها، IP اي است كه به پورت‌هاي مجازي روتر اختصاص داده ايم.

PC0:

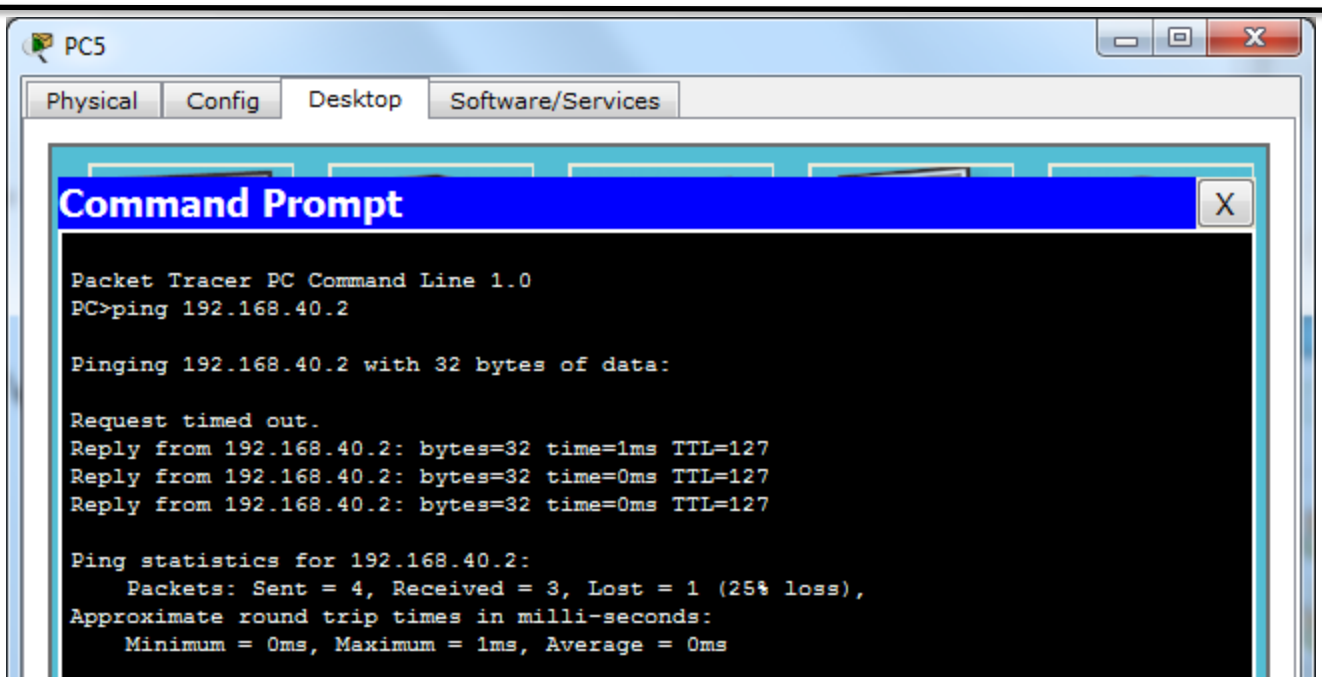


PC1:



شكل 4-13 نحوه‌ی اختصاص IP به

حال مي‌توانيم كامپيوترهاي موجود در دو Vlan مختلف را Ping كنيم:



شکل 4-12 ping
کامپیوترها

Port Security

در این قسمت با مفهوم Port Security و اینکه چگونه از این قابلیت سوئیچ‌های سیسکو در جهت ایمن‌سازی سوئیچ‌ها و محدودسازی دسترسی به پورت‌های سوئیچ شبکه خود استفاده کنیم، آشنا خواهیم شد.

یکی از مشکلاتی که مدیران شبکه بسیار با آن درگیر هستند این است که چگونه می‌توانند دسترسی‌های غیر مجاز به شبکه را کنترل کنند، در واقع مشکل اصلی اینجاست که نمی‌دانیم چگونه می‌توان برای تجهیزات شبکه تعریف کرد که چه کسی بتواند به آن‌ها متصل شود و چه کسی نتواند متصل شود. برای مثال شما نمی‌خواهید که هر کسی که وارد سازمان شما شد به راحتی با استفاده از لپ تاپ خود و متصل کردن آن به یکی از پورت‌های سوئیچ شبکه به شبکه شما متصل شده و به منابع شبکه شما دسترسی پیدا کند. شاید با خود بگویید که تمامی پورت‌های شبکه ما که بر روی دیوار قرار گرفته‌اند و کامپیوتری به آن‌ها متصل نیست به‌صورت فیزیکی به سوئیچ و شبکه متصل نیستند و دیگر جای نگرانی در این خصوص وجود ندارد، اما اگر شخص کابل کامپیوتر فعالی که مشغول سرویس دهی در شبکه است را از جای خود در آورده و از آن برای اتصال به سوئیچ و شبکه استفاده کند چطور؟ این کامپیوتر در ساده‌ترین حالت ممکن می‌تواند ویروس‌ها و کرم‌های خطرناکی را وارد شبکه ما بکند.

شناخت مبانی Port Security

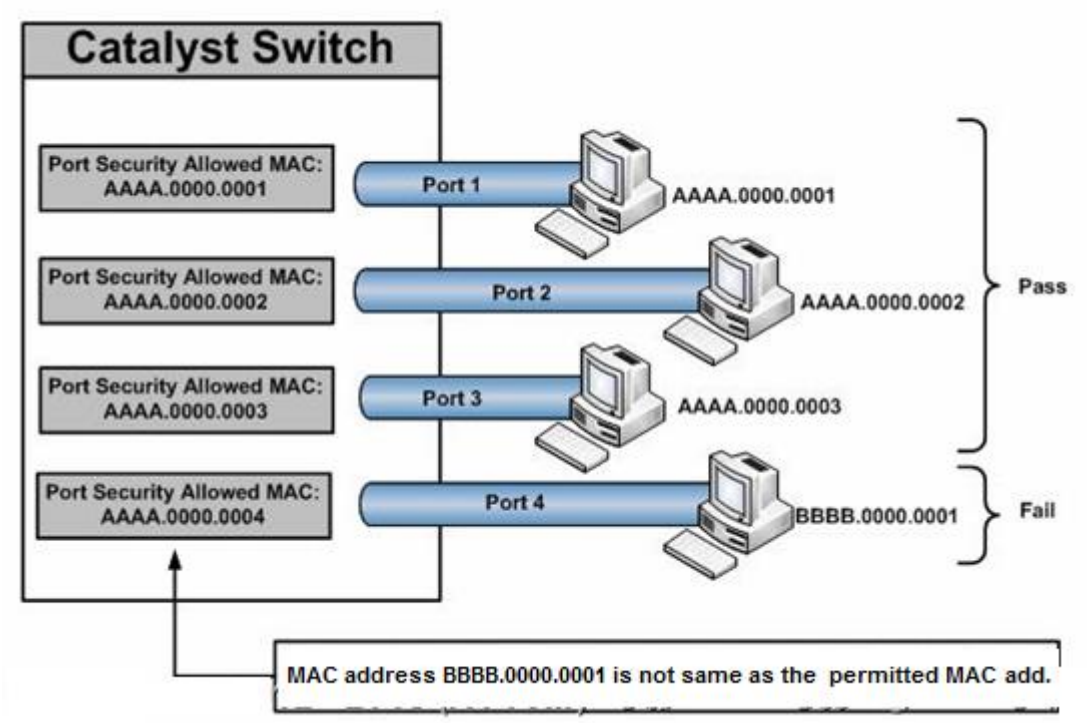
در ساده‌ترین حالت ممکن این قابلیت، آدرس سخت افزاری کارت شبکه شما یا همان MAC شما را در حافظه‌ای مربوط به آن پورت ذخیره می‌کند و فقط به همین آدرس سخت افزاری اجازه ورود به پورت شبکه را می‌دهد. اگر آدرس سخت افزاری دیگری بخواهد از طریق همان پورت سوئیچ به شبکه متصل شود، سوئیچ آن را بلوکه کرده و اجازه ورود به سیستم را به آن پورت نخواهد داد، این می‌تواند غیرفعال کردن پورت سوئیچ نیز باشد. در شبکه‌هایی که سیستم‌های مانیتورینگ یا پایش شبکه راه اندازی شده‌اند با استفاده از پروتکل SNMP تنظیماتی انجام شده است که بلافاصله بعد از غیرفعال شدن پورت سوئیچ به سیستم مانیتورینگ اطلاع رسانی می‌شود و در لاگ این سیستم ثبت می‌شود.

همیشه انجام تنظیمات امنیتی بر روی شبکه نیاز به سبک سنگین کردن و بررسی درست پیامدهای آن دارد. برخی اوقات پیاده‌سازی امنیت باعث پایین آمدن سهولت کاربری و سخت کردن فعالیت کاری می‌شود. وقتی شما از قابلیت Port Security استفاده می‌کنید، در حقیقت اتصال هر دستگاهی به شبکه را محدود کرده‌اید و بر حسب آن امنیت خود و شبکه را بالا برده‌اید، اما همیشه حالت برعکسی هم وجود دارد، در این حالت از Port Security فقط مدیر شبکه می‌تواند پورت غیرفعال شده را فعال یا به اصطلاح unlock کند و این خود باعث به‌وجود آمدن دردسرهای مدیریتی زیادی برای مدیر شبکه خواهد شد.

Port Security برای کنترل دسترسی شبکه براساس:

- Mac Address
- تعداد Mac Address ها در هر پورت

استفاده می‌شود.



شکل 4-14 نحوه ی عملکرد Port Security

1	Switch# **config t**
2	Switch(config)# **int fa0/5**
3	Switch(config-if)# **switchport port-security[mac-address *mac-address* |mac-address**
4	**sticky[macaddress] | maximum *value* | violation{restrict|shutdown}]**
5	Switch(config-if)# **switchport mode access**
6	Switch(config-if)# **switchport port-security**
7	Switch(config-if)# **switchport port-security maximum 1**
8	Switch(config-if)# **switchport port-security mac-address sticky**
9	Switch(config-if)# **switchport port-security violation [shutdown| restrict|protect]**
10	
11	Switch# **show port-security interface FastEthernet 0/5**

به ازای هر پورت می‌توان این دستورات را اجرا کرد.

- خط 5: پورتی که می‌خواهیم در وضعیت Security قرار دهیم باید در مد access باشد.
- خط 6: حال باید Port Security را روی آن فعال کنیم.
- حال که فعال شد باید دو نوع دستور مجاز و غیر مجاز را تعریف کنیم.
- خط 7: یعنی ماکزیمم فقط یک سیستم را بتوانیم وصل کنیم.
- خط 8: اولین سیستم، سیستمی باشد که اولین بار به آن وصل شده است. به جای Sticky می‌توانیم Mac Address سیستم مورد نظرمان را وارد کنیم که اگر سیستم دیگری به آن پورت وصل شد نتواند وارد شبکه شود.
- خط 9: در غیر این‌صورت پورت را protect/ restrict / Shutdown کن (در حالت Shutdown، پورت مسدود می‌شود و log را به Admin ارسال می‌نماید، در حالت Restrict پورت مسدود می‌شود و log آن به Admin ارسال نمی شود).
- خط 11: دستور Verify، اطلاعات پورت Fastethernet 0/5 را نمایش می‌دهد.

جهت پاک کردن کلیه تنظیمات Port Security از دستور زیر استفاده می‌کنیم.

1	Switch#**clear port-security all**
2	Switch#**reload**

دسترسی به سوئیچ از راه دور

- **Telnet**
- **SSH**

Interface Vlan های مجازی در سوئیچ وجود دارد:

جهت اتصال از طریق Telnet و SSH ابتدا باید به سوئیچ IP اختصاص دهیم.

- در سوئیچ‌ها Interface مجازی با عنوان Vlan1 وجود دارد.

```
1  Switch#show ip interface brief
2  Interface              IP-Address      OK? Method Status                Protocol
3
4  FastEthernet0/1        unassigned      YES manual down                  down
…    …
54 Vlan1                  unassigned      YES manual administratively down down
```

- Vlan1 همان Interface مجازی است. زمانی قابل استفاده است که وجود داشته باشد، جهت اتصال از راه دور به این Interface، IP اختصاص می‌دهیم.

```
1  Switch(config)#interface vlan 1
2  Switch(config-if)#ip address 192.168.10.1 255.255.255.0
3  Switch(config-if)#no shutdown
4
5  Switch(config-if)#
6  %LINK-5-CHANGED: Interface Vlan1, changed state to up
7
8  %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up
```

- خط 1: وارد Interface مجازی می‌شویم.
- خط 2: به آن IP اختصاص می‌دهیم.
- خط 3: Up می‌کنیم.

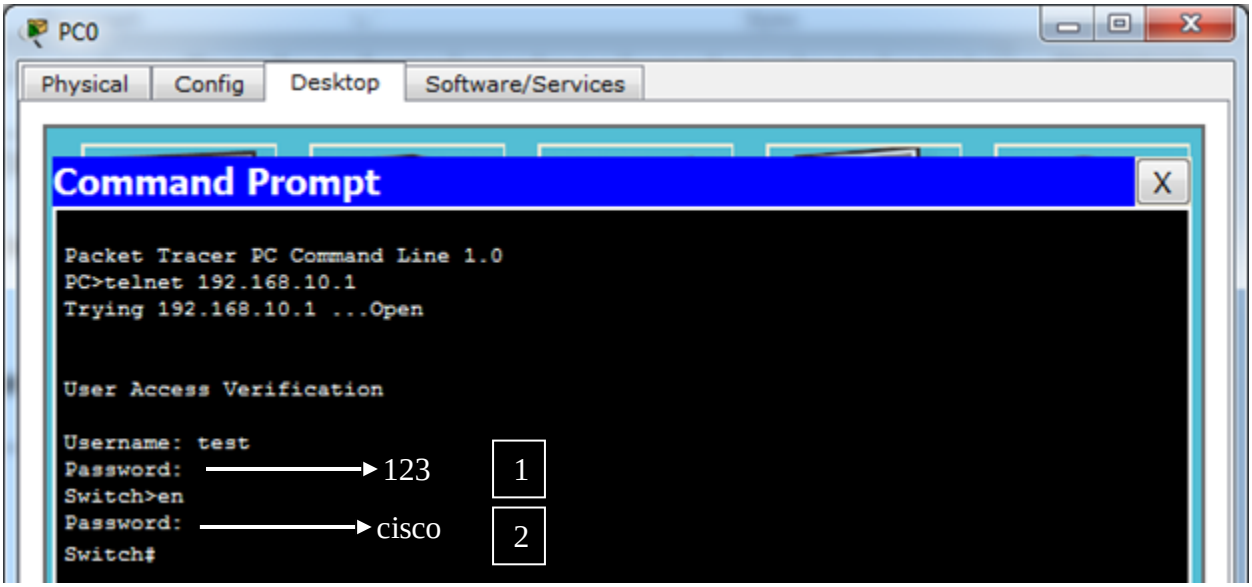
```
1  Switch#show ip interface b
2  Interface              IP-Address      OK? Method Status                Protocol
3
4  FastEthernet0/1        unassigned      YES manual down                  down
…    …
```

54	Vlan1	192.168.10.1	YES manual up	up

حال Interface مورد نظر up شده و سوئیچ مورد نظر قابل دسترسی از راه دور می‌باشد.

```
1  Switch(config)#username test password 123
2  Switch(config)#line vty 0 4
3  Switch(config-line)#transport input telnet
4  Switch(config-line)#exit
5
6  Switch(config)#enable password cisco
```

- خط 1: تعریف Username و Password جهت اتصال به سوئیچ (پسورد شماره 1 مطابق شکل زیر)
- خط 3: نحوه‌ی اتصال
- خط 6: تعریف پسورد برای مد Enable سوئیچ (پسورد شماره 2 مطابق شکل زیر)



STP [1]

پروتکل STP یک پروتکل است که از به‌وجود آمدن Loop در سوئیچ جلوگیری می‌کند. منظور از Loop هم این است که یک بسته از نقطه وارد شبکه شود و در یک حلقه بیفتد و مدام بین سوئیچ‌های شبکه بچرخد. در این حالت بسته مورد نظر هرگز از بین نخواهد رفت. اگر تعداد این بسته‌ها زیاد شود مسلما به زودی شبکه پر از این بسته‌های مزاحم خواهد شد و شبکه را مختل خواهد کرد.

نکات

- ایجاد Loop سبب کندي و پايين آمدن كارايي شبكه مي‌شود و شبكه را Down مي‌كند.
- STP یک پروتکل استاندارد باز می‌باشد (IEEE 802.1D).

اگرLoop ای به‌وجود نیاید هرگز مشکل فوق اتفاق نخواهد افتاد، چرا؟ چون بسته که از مبدا ارسال می‌شود به سمت مقصد حرکت کرده و به آن که می‌رسد یعنی اینکه بسته از بستر فیزیکی شبکه خارج می‌شود.

- پورت‌هاي سوئيچ چهار مرحله را طي مي‌كنند تا به حالت Fwd برسند: Block ،Listen ،Learn و Fwd. -
- در دو حالت سوئيچ در شبكه Broadcast انجام مي‌دهد: 1- موقعي كه روشن مي‌شود. 2- زماني‌كه آدرس مقصد را نمي‌شناسد.

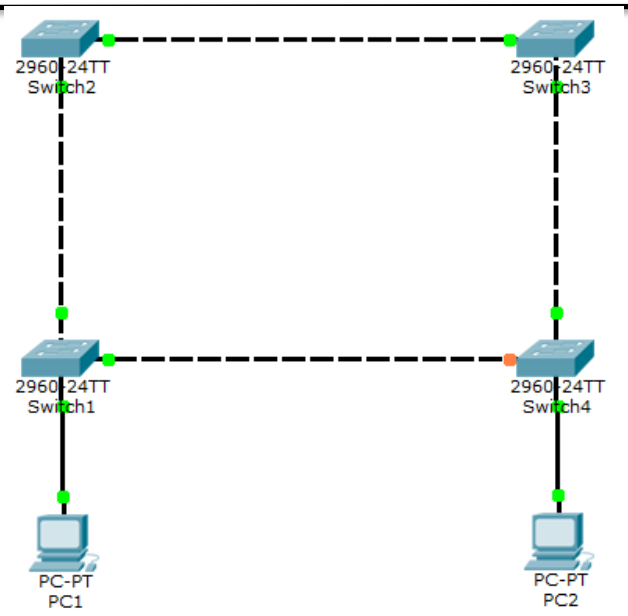
پروتکل STP همیشه به صورت پیش فرض بر روی همه سوئیچ‌ها فعال است و نیاز نیست ما آن‌را فعال کنیم.

[1] Spanning Tree Protocol

در شکل (4-16) PC1 میخواهد با PC2 ارتباط برقرار کند.
Mac را ارسال می کند.
یک پکت Broadcast میکند.
همانطور که در شکل میبینید دو مسیر بین PC1 و PC2 وجود دارد.

- مستقیم از Sw1→Sw4
- از طریقSw1→Sw2→Sw4

یکی از مسیرهای موجود برای جلوگیری از بوجود آمدن Loop باید بسته شود (به این حالت حلقه بسته میگویند که حلقه بسته سبب بوجود آمدن Loop میشود.)



شکل 4-16 نمایشی از ایجاد Loop

برای فراگیری روش کار این پروتکل، در بسیاری از مواقع میتوانید با تنظیم و تغییر شبکه باعث عملکرد بهتر این پروتکل شوید.

برای ادامه بحث باید با برخی مفاهیم آشنا شویم:

- **BPDU**[1]:

- سوئیچهای شبکه که بر روی آنها پروتکل STP اجرا شده، برای تبادل اطلاعات از بستههای BPDU استفاده میکنند.
- BPDU شامل اطلاعاتی میباشد که به سوئیچ در تعیین توپولوژی کمک میکند.
- BPDU هر 2 ثانیه ارسال میشود.
- دو نوع بسته BPDU در پروتکل STP وجود دارد:

- **BPDU Configuration:** سوئیچها از این بستهها برای محاسباتشان استفاده میکنند.

- **TCN BPDU:** وقتی تغییری بر روی سوئیچی در شبکه رخ دهد برای اعلام تغییرات، این مدل بسته را به سوئیچهای دیگه ارسال می کند تا بروز تغییرات رو اعلام کند.

[1] Bridge Protocol Data Unit

- **Root Bridge:** یکی از سوئیچ‌ها در شبکه به عنوان سوئیچ Root Bridge انتخاب می‌شود. این سوئیچ تعیین کننده‌ی مسیر انتقال بسته‌ها در شبکه است. مبنای انتخاب Root Bridge در شبکه Bridge ID است. هر سوئیچ در شبکه یک Bridge ID منحصر به فرد دارد. سوئیچی که Bridge ID آن از همه کمتر باشد به عنوان Root Bridge انتخاب خواهد شد.

- **Bridge ID.** یک مقدار 8 بایتی است که از دو قسمت تشکیل شده:

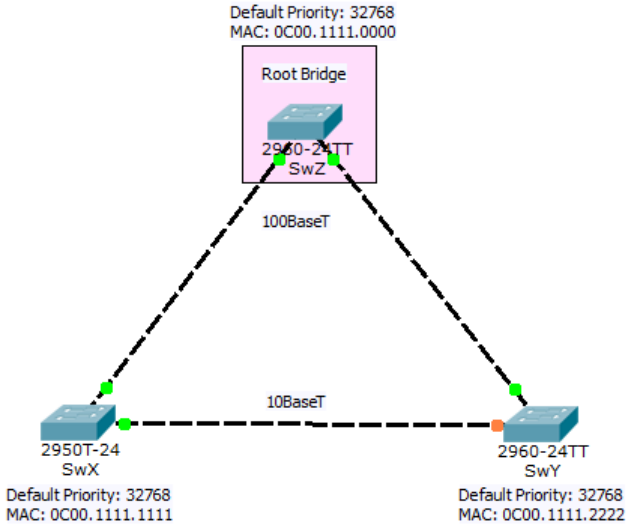
B.ID= Bridge Priority (2 byte) + Mac Add. (8 byte)

لحظه‌ای که سوئیچ‌ها به یکدیگر متصل می‌شوند، B.ID هایشان را با هم تبادل می‌کنند.

دستور مربوط به مشاهده‌ی Spanning Tree:

1	Switch#**Show spanning tree**

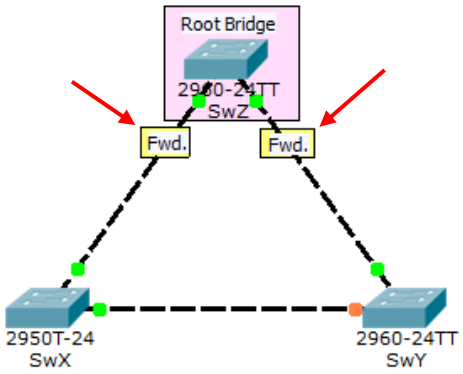
- **قانون اول:** Bridge Priority (اولویت Bridge) عددی بین 0 تا 65535 است. سوئیچی که Bridge Priority آن از سوئیچ‌های دیگر کمتر باشد به عنوان Root Bridge انتخاب خواهد شد. در صورتی که Bridge Priority همه سوئیچ‌ها یکسان باشد، از آدرس Mac سوئیچ‌ها به عنوان الگوی انتخاب استفاده می‌شود. در این حالت سوئیچی که آدرس Mac آن از سوئیچ‌های دیگر کمتر باشد به عنوان Root Bridge انتخاب خواهد شد.



شکل 4-17 انتخاب Root

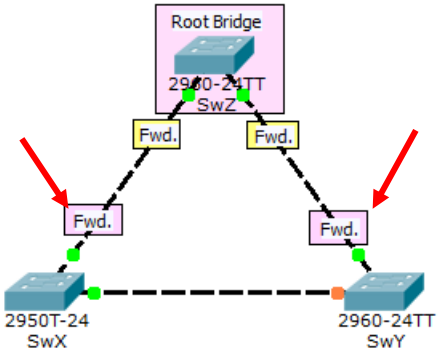
SwZ: { SwZ: 32768 + 0C00.1111.0000 ; SwX: 32768 + 0C00.1111.1111 ; SwY: 32768 + 0c00.1111.2222 } از همه کوچکتر است و به عنوان Root Bridge انتخاب می‌شود .

Root Bridge: باید با همه‌ي سیستم ها در ارتباط باشد ← پورت‌هایش باید در وضعیت .Fwd باشند.



شکل 4-18 وضعیت پورت‌های Root

- **قانون دوم:** بین سوئیچ‌هاي باقي مانده، آنهائیکه بطور مستقیم به R.Bridge متصل هستند، پورت‌هایشان باید در وضعیت Fwd باشد (چون R.Bridge باید با همه در ارتباط باشد).

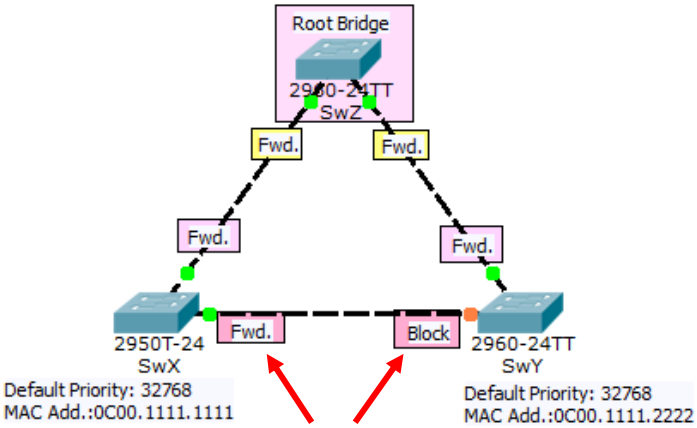


شکل 4-19 وضعیت پورت های متصل به Root Bridge

- **قانون سوم :** بین سوئیچ‌های باقی مانده دوباره باید B.ID محاسبه شود.

سوئیچی که از همه دارای B.ID کوچکتری است پورتش در حالت Fwd. قرار می‌گیرد .
سوئیچی که از همه دارای B.ID بزرگتر است پورتش در حالت Block قرار می‌گیرد.

SwX: 32768 + 0C00.1111.1111 *Fwd.*
SwY: 32768 + 0c00.1111.2222 Block



شکل 4-20 وضعیت پورت های غیرمتصل به Root Bridge

1- پورت‌های R.B ← Desinated Port (پورت‌های برگزیده) گویند.
2- آن‌هایی که از جهت فیزیکی به R.B نزدیکترند ← Root Port
3- سوئیچی که دارای کمترین BID ما بین سوئیچ‌های منتهی به RB باشد پورتش بلاک شده و به آن non Desinated port می‌گویند.

دستور عوض کردن priority به‌صورت دستی

1	Switch(config)#**spanning-tree vlan <*vlan number*> priority <*priority*>**

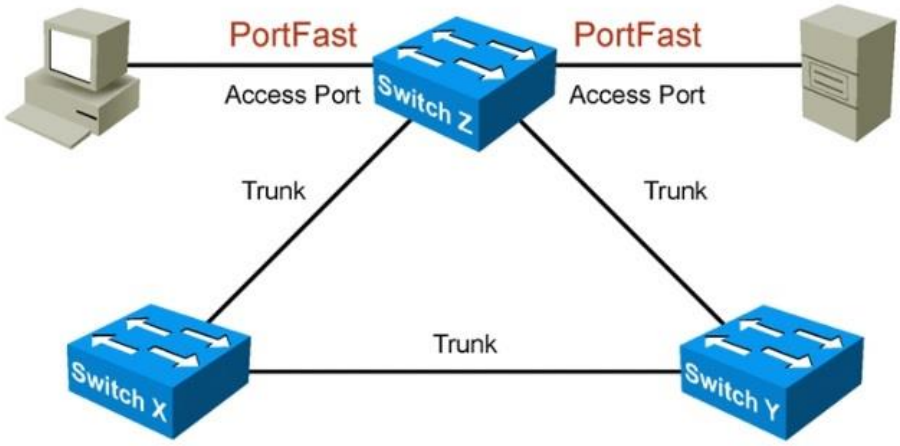
مقدار priority باید ضریبی از 4096 باشد.

Portfast

وقتی پورتی از PC به سوئیچ وصل می‌شود یک بازه‌ی زمانی طول می‌کشد تا پورت UP شود(از رنگ نارنجی به سبز در بیاید)، این بازه‌ی زمانی برابر 4 مرحله‌ی Block، Listen، Learn و Forward می‌باشد که برابر 50 ثانیه است.
قابلیت Portfast بیان می‌کند که در شبکه برای end system ها به‌منظور عملکرد بهتر، Listen و Learn را حذف کنید(با حذف این دو مرحله بازه‌ی زمانی UP شدن پورت برابر 20 ثانیه می‌شود)، چون mac address را قبلا در سوئیچ یاد گرفته و نوشته است پس نیازی نیست که همیشه 4 مرحله را طی کند.

نکات

- Portfast باعث می‌شود که کاربر با سرعت بالایی به شبکه متصل شود.
- Portfast باید بر روی پورتی که دستگاه‌های کاربر وصل است(پورت Access)، فعال شود.
- Portfast نباید بر روی پورتی که spanning-tree اعمال شده است، فعال گردد.



شکل 4-21 شمایی از عملکرد Portfast

دستورات Portfast

1	Switch(config-if)#**spanning-tree portfast**
2	Switch(config)#**spanning-tree portfast default**

	Switch#**show running-config interface *interface***

- خط1: فعال‌سازی Portfast بر روی یک اینترفیس
- خط2: فعال‌سازی portfast برروی تمام پورت‌ها
- خط3: تائید اینکه Portfast بر روی اینترفیس فعال شده است.

BPDU Guard

- اگر نیاز به دریافت BPDU بر روی پورتی نباشد، قابلیت BPDU Guard آن پورت را غیرفعال می‌کند.
- توصیه می‌شود که این ویژگی بر روی پورتی که قابلیت PortFast تنظیم شده است، فعال گردد. زیرا بر روی این پورت Listen و Learn حذف شده و اگر فرد مزاحمی سوئیچ را به Portfast بزند هیچ اتفاقی نمی‌افتد.

دستورات BPDU Guard

1	Switch(config-if)#**switchport mode access**
2	Switch(config-if)#**spanning-tree portfast**
3	Switch(config-if)#**spanning-tree bpduguard enable**

- خط1: قرار دادن پورت در مد Access
- خط2: فعال‌سازی Portfast بر روی اینترفیس
- خط3: فعال‌سازی BPDU Guard بر روی اینترفیس

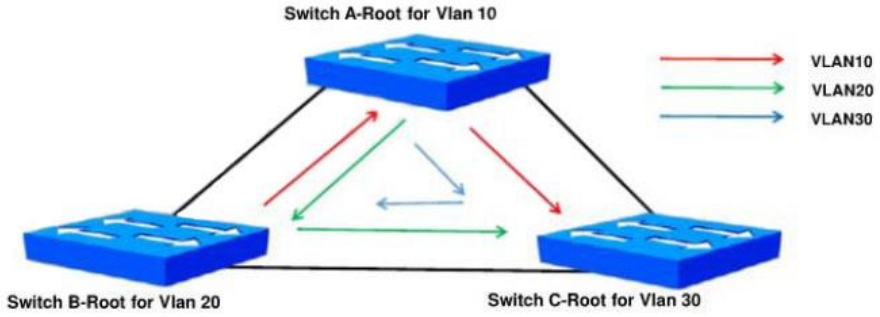
RSTP[1]

- بهبود یافته‌ی نسخه‌ی STP می‌باشد (802.1w).
- همگرایی STP را بهبود داده.
- برای انتخاب RSTP کارهای زیر را باید انجام داد:
  - انتخاب Root Bridge
  - انتخاب Root Port
  - انتخاب پورت جایگزین[2] (پشتیبان Root Port)
  - انتخاب Designated Port
  - انتخاب Backup port (پشتیبان Designated Port)

[1] Rapid Spanning Tree Protocol
[2] Alternate Port

PVST[1]

- یک پروتکل مخصوص شرکت سیسکو است.
- با استفاده از این پروتکل، هر سوئیچ برای Vlan خاصی root bridge می‌باشد.
- برای هر Vlan به‌صورت جداگانه، Root Port، Designated Port و Undesignated Port وجود دارد.
- ترافیک بار می‌تواند در سراسر لینک‌های موجود تقسیم شود.



شکل 4-22 شمایی از عملکرد PVST

نکات

- با استفاده از قابلیت PVST پورت نارنجی رنگ در سوئیچ ها وجود نخواهد داشت، فقط سوئیچی که برای Vlan 1، root bridge شده یک نقطه ای را بلاک خواهد کرد.
- عدم وجود پورت نارنجی رنگ دلیل بر نبود Spannig Tree نیست (لزوما Spanning Tree وجود دارد و با تکنیک دیگری کار می‌کند).

دستورات PVST

1	Switch(config)#**spanning-tree vlan <*vlan number*> root primary**
2	Switch(config)#**spanning-tree vlan <*vlan number*> root secondary**

[1] Per-Vlan Spanning tree

- خط1: با استفاده از این دستور می‌توان root bridge را عوض کرد. برای عوض کردن root bridge باید priority را تغییر داد چون نمی‌توان mac addressرا تغییر داد. در واقع با این دستور priority سوئیچ پایین آورده می‌شود تا به سوئیچ به عنوان root bridge نگاه شود.

- خط2: این دستور به‌عنوان backup به کار برده می‌شود.

فصل 5

Routing

مبانی مسیریابی

روترها برای اینکه شبکه های مختلف را شناسایی بکنند، هرکدام برای خود جدولی با نام routing table دارد. جدول مسیریابی در یک روتر با دستور R#sh ip route نشان داده می‌شود. به‌طور پیش فرض روترها، شبکه هایی را بلد هستند که به‌طور مستقیم به خودشان وصل است و شبکه های دیگر را نمی‌شناسند (هر روتر، روتر مجاور را ping می‌کند). اگر شبکه ای در routing table وجود نداشته باشد، روتر به آن شبکه دسترسی نخواهد داشت که در آن موقع بحث routing مطرح می‌شود.

Routing

- Routing پروسه‌ی انتقال بسته‌های IP از یک شبکه به شبکه‌ی دیگر می‌باشد.
- Routing شامل دو فعالیت اساسی زیر می‌باشد:
  - تعیین بهترین مسیر
  - ارسال بسته‌ها از طریق این مسیرها

انواع مسیریابی

- **Dynamic (اتوماتیک)**
- **Static (دستي)**
- **Default (پیش‌فرض)**

مسیریابی دستي (Static route)

- مسیریابی دستی به‌صورت دستی توسط مدیر شبکه آپدیت، کانفیگ و نگهداری می‌شود.
- مدیر شبکه باید IP مقصد شبکه را برای پیکربندی در اختیار داشته باشد.
- از طریق Command باید شبکه‌ها معرفي شود.

دستور مسیریابی دستی

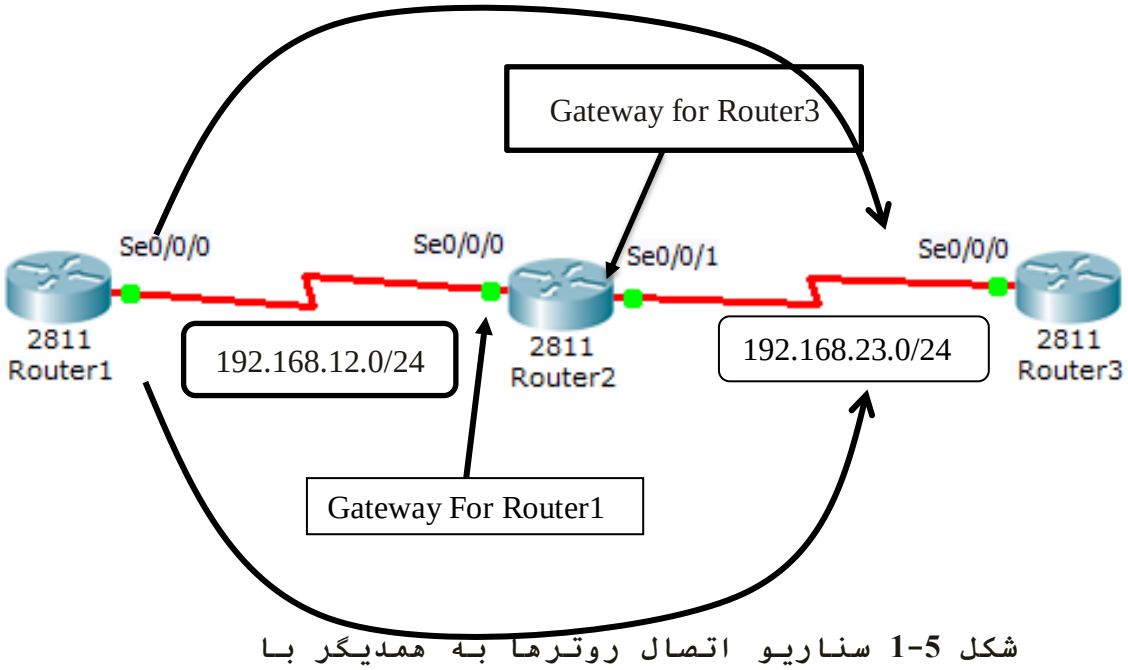
1	Router(config)#**ip route** شبکه طرف مقابل شبکه طرف مقابل **Mask Gateway**

جدول 5-1 مزایا و معایب

معایب	مزایا
به‌صورت اتوماتیک آپدیت نمی‌شوند	امن
نیاز به IP شبکه مقصد برای پیکربندی دارند	قابل اعتماد
نیاز به مدیریت بیشتری توسط مدیر شبکه دارد	سریعتر هستند
در شبکه های کوچک استفاده می‌شود	اتلاف پهنای باند وجود ندارد

در شکل(5-1) می‌خواهیم Router 1 و Router 3 بتوانند بهم متصل شوند. بنابراین ابتدا در Router 1 اگر show ip route بگیریم فقط شبکه ای که به صورت مستقیم به روتر وصل است را می‌شناسد.

```
C       192.168.12.0/24 is directly connected, Serial0/0/0
```



شکل 5-1 سناریو اتصال روترها به همدیگر با استفاده از مسیریابی دستی

حال برای اینکه روترها بتوانند به همدیگر متصل شوند در Router1 و Router3 دستورات زیر را به کار می‌بریم:

Router1

```
1  Router(config)#ip route 192.168.23.0 255.255.255.0 192.168.12.2
2  Router#show ip route
```

برای این شبکه Gateway ما پورت Serial 0/0/0 ، Router2 می‌باشد.

```
Router#show ip route
```

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

Gateway of last resort is not set

C   192.168.12.0/24 is directly connected, Serial0/0/0
S   192.168.23.0/24 [1/0] via 192.168.12.2
```

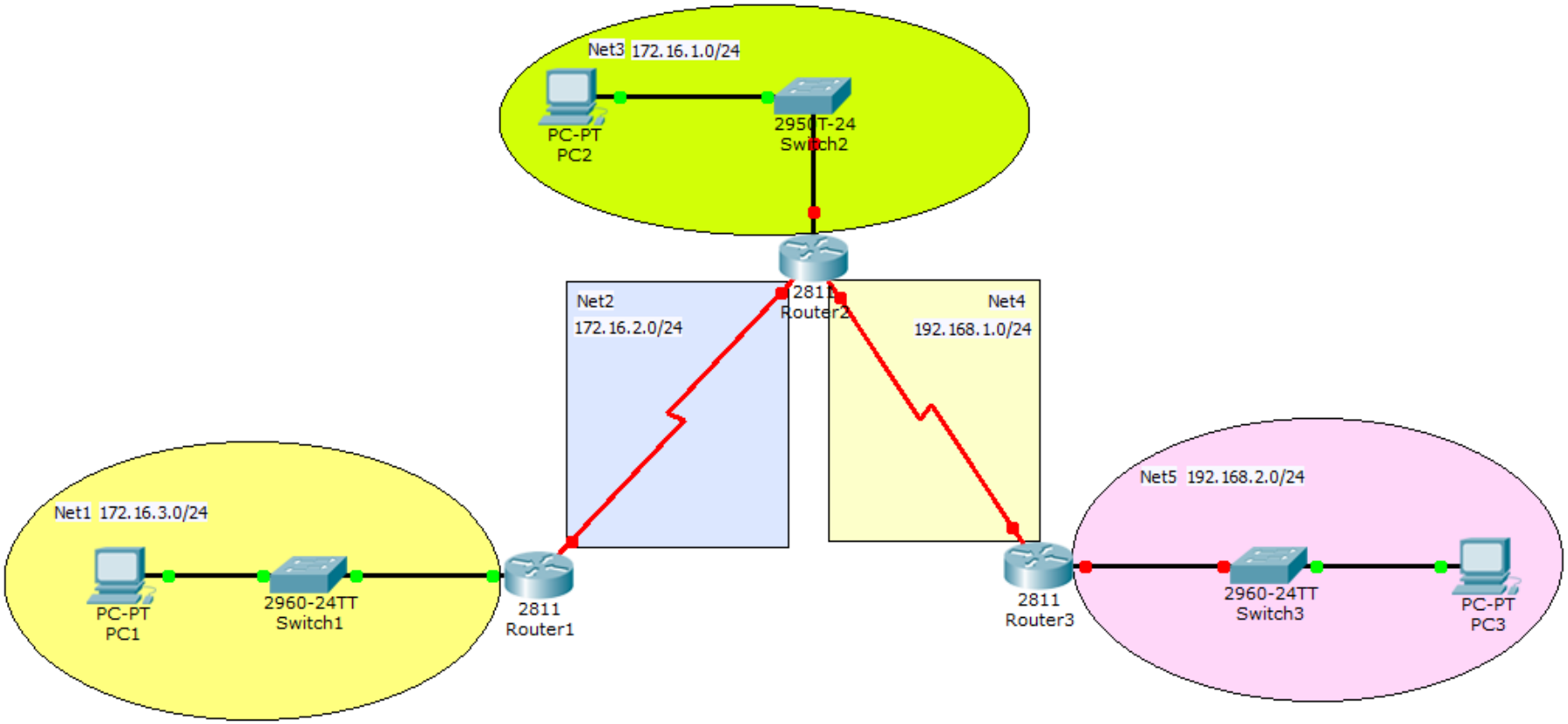
حال مي‌بينم كه شبكه طرف مقابل را نيز مي‌شناسد و حرف S به معناي Static مي‌باشد.
و اين كار را نيز در مورد Router 3 تكرار مي‌كنيم.

Router3:

1	Router(config)#**ip route 192.168.12.0 255.255.255.0 192.168.23.2**
2	Router#**show ip route**

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

Gateway of last resort is not set

S   192.168.12.0/24 [1/0] via 192.168.23.2
C 192.168.23.0/24 is directly connected, Serial0/0/0
```

سناریو : Static Route



شکل 5-2 سناریو Static Route

به طور کلي ما 5 شبکه داريم که به ترتيب شماره‌گذاري شده است.
Net1: 172.16.3.0/24 Net2:172.16.2.0/24 Net3:192.16.1.0/24
Net4:192.168.1.0/24 Net5:192.168.2.0/24

1- ابتدا به اينترفيس‌ها IP اختصاص مي‌دهيم و سپس عمل Routing را انجام مي‌دهيم.

Router1:

```
1  Router(config)#int f0/0
2  Router(config-if)#ip address 172.16.3.1 255.255.255.0
3  Router(config-if)#no shutdown
4
5  Router(config-if)#int s0/0/0
6  Router(config-if)#ip address 172.16.2.2 255.255.255.0
7  Router(config-if)#no shutdown
```

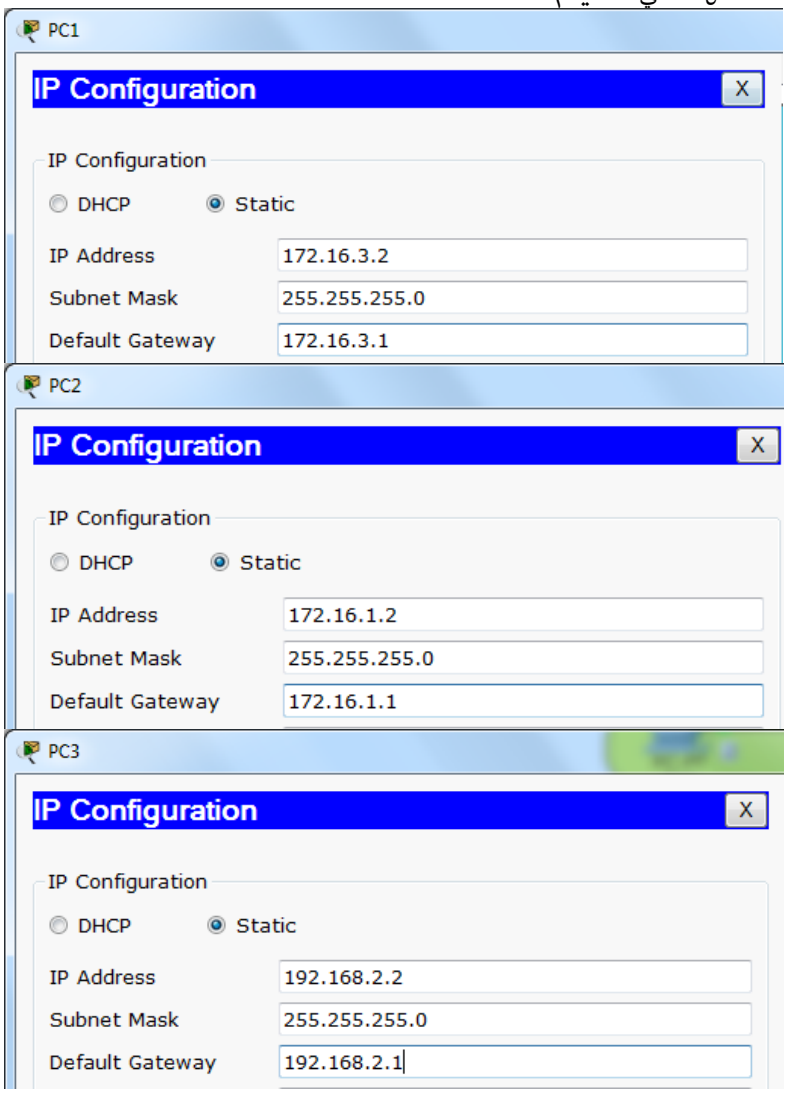
Router2:

```
1  Router(config)#interface serial 0/0/0
2  Router(config-if)#ip address 172.16.2.1 255.255.255.0
3  Router(config-if)#clock rate 64000
4  Router(config-if)#no shutdown
5
6  Router(config-if)#int s0/0/1
7  Router(config-if)#ip address 192.168.1.1 255.255.255.0
8  Router(config-if)#clock rate 64000
9  Router(config-if)#no shutdown
10
11 Router(config-if)#int fa 0/0
12 Router(config-if)#ip address 172.16.1.1 255.255.255.0
13 Router(config-if)#no shutdown
```

Router3:

```
1  Router(config)#interface s0/0/0
2  Router(config-if)#ip address 192.168.1.2 255.255.255.0
3  Router(config-if)#no shutdown
4
5  outer(config-if)#int fa0/0
6  Router(config-if)#ip address 192.168.2.1 255.255.255.0
7  Router(config-if)#no shutdown
```

2-به کامپیوترها نیز IP اختصاص می‌دهیم.



شکل 5-3 اختصاص IP به کامپیوترها

2- حال باید Routing را انجام دهیم.

Router 1: به دو شبکه (Net1 و Net2) به صورت مستقیم متصل می‌باشد و سه شبکه دیگر (Net3, Net4, Net5) را باید به آن معرفی کنیم. براي همه‌ي اين شبکه ها Gateway یکسان می‌باشد (Gateway : 172.16.2.1)

Router1:

1	Router(config)#**ip route 172.16.1.0 255.255.255.0 172.16.2.1**
2	Router(config)#**ip route 192.168.1.0 255.255.255.0 172.16.2.1**
3	Router(config)#**ip route 192.168.2.0 255.255.255.0 172.16.2.1**

Router 2: به سه شبکه (Net2 و Net3 و Net4) به صورت مستقیم متصل می‌باشد و دو شبکه دیگر (Net1, Net5) را باید به آن معرفی کنیم.

براي ارتباط با شبكه‌ي Net1، Gateway، 172.16.2.2 مي باشد.

براي ارتباط با شبكه‌ي Net5، Gateway، 192.168.1.2 مي‌باشد.

Router2:

1	Router(config)#**ip route 172.16.3.0 255.255.255.0 172.16.2.2**
2	Router(config)#**ip route 192.168.2.0 255.255.255.0 192.168.1.2**

Router 3: به دو شبكه (Net4و Net5) به صورت مستقيم متصل مي‌باشد و سه شبكه ديگر (Net3, Net2, Net1) را بايد به آن معرفي كنيم. براي همه‌ي اين شبكه‌ها Gateway يكسان مي‌باشد (Gateway: 192.168.1.1).

Router3:

1	Router(config)#**ip route 172.16.1.0 255.255.255.0 192.168.1.1**
2	Router(config)#**ip route 172.16.2.0 255.255.255.0 192.168.1.1**
3	Router(config)#**ip route 172.16.3.0 255.255.255.0 192.168.1.1**

3- تست ارتباطات

Router1

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

Gateway of last resort is not set

     172.16.0.0/24 is subnetted, 3 subnets
S       172.16.1.0 [1/0] via 172.16.2.1
C       172.16.2.0 is directly connected, Serial0/0/0
C       172.16.3.0 is directly connected, FastEthernet0/0
S    192.168.1.0/24 [1/0] via 172.16.2.1
S    192.168.2.0/24 [1/0] via 172.16.2.1
```

Router2

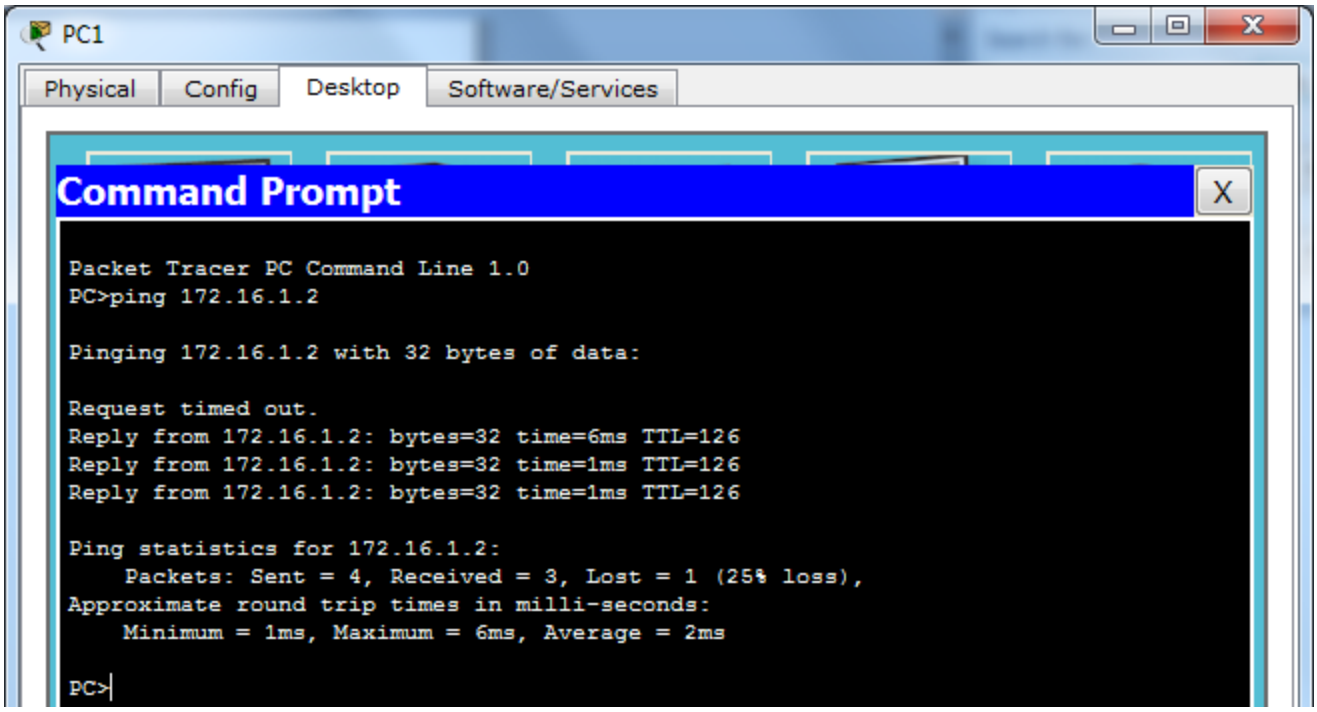
```
Router#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E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

```
        * - candidate default, U - per-user static route, o - ODR
        P - periodic downloaded static route

Gateway of last resort is not set

     172.16.0.0/24 is subnetted, 3 subnets
C       172.16.1.0 is directly connected, FastEthernet0/0
C       172.16.2.0 is directly connected, Serial0/0/0
S       172.16.3.0 [1/0] via 172.16.2.2
C    192.168.1.0/24 is directly connected, Serial0/0/1
S    192.168.2.0/24 [1/0] via 192.168.1.2
```

Router3

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

Gateway of last resort is not set

     172.16.0.0/24 is subnetted, 3 subnets
S       172.16.1.0 [1/0] via 192.168.1.1
S       172.16.2.0 [1/0] via 192.168.1.1
S       172.16.3.0 [1/0] via 192.168.1.1
C    192.168.1.0/24 is directly connected, Serial0/0/0
C    192.168.2.0/24 is directly connected, FastEthernet0/0
```

و یا اینکه میتوانیم کامپیوترهای هر مجموعه را Ping کنیم: از کامپیوتر PC1 موجود در شبکه Net1، کامپیوتر PC2 موجود در شبکه Net3 را Ping میکنیم. همانگونه که مشاهده میفرمایید کامپیوترها همدیگر را میبینند.



شکل 5-4 Ping از PC1 به PC2

جمع‌بندي : كانفيگ‌هاي انجام شده در روترها

Router1

1	Router(config)#**interface fa0/0**
2	Router(config-if)#**ip address 172.16.3.1 255.255.255.0**
3	Router(config-if)#**no shutdown**
4	
5	Router(config-if)#**int s0/0/0**
6	Router(config-if)#**ip address 172.16.2.2 255.255.255.0**
7	Router(config-if)#**no shutdown**
8	
9	Router(config)#**ip route 172.16.1.0 255.255.255.0 172.16.2.1**
10	Router(config)#**ip route 192.168.1.0 255.255.255.0 172.16.2.1**
11	Router(config)#**ip route 192.168.2.0 255.255.255.0 172.16.2.1**
12	
13	Router#**show ip route**

Router2

1	Router(config)#**interface serial 0/0/0**
2	Router(config-if)#**ip address 172.16.2.1 255.255.255.0**

```
3  Router(config-if)#clock rate 64000
4  Router(config-if)#no shutdown
5
6  Router(config-if)#int s0/0/1
7  Router(config-if)#ip address 192.168.1.1 255.255.255.0
8  Router(config-if)#clock rate 64000
9  Router(config-if)#no shutdown
10
11 Router(config-if)#int fa 0/0
12 Router(config-if)#ip add 172.16.1.1 255.255.255.0
13 Router(config-if)#no shutdown
14
15 Router(config)#ip route 172.16.3.0 255.255.255.0 172.16.2.2
16 Router(config)#ip route 192.168.2.0 255.255.255.0 192.168.1.2
17
18 Router#show ip route
```

Router3

```
1  Router(config)#interface s0/0/0
2  Router(config-if)#ip address 192.168.1.2 255.255.255.0
3  Router(config-if)#no shutdown
4
5  outer(config-if)#int f0/0
6  Router(config-if)#ip address 192.168.2.1 255.255.255.0
7  Router(config-if)#no shutdown
8
9  Router(config)#ip route 172.16.1.0 255.255.255.0 192.168.1.1
10 Router(config)#ip route 172.16.2.0 255.255.255.0 192.168.1.1
11 Router(config)#ip route 172.16.3.0 255.255.255.0 192.168.1.1
12
13 Router#show ip route
```

2-مسیریابی اتوماتیک (Dynamic route)

در بحث Dynamic Route باید با ساختار و مفهوم پروتکل‌های مسیریابی آشنا شویم. پروتکل‌های مسیریابی، پروتکل هایی هستند که به روترها اجازه می‌دهند که به حالت Discovery در شبکه، اطلاعات routing و اطلاعات شبکه‌هایی که در اختیار دارند را به‌صورت Dynamic با هم رد و بدل

کنند. یعنی روترها جداول مسیریابی را با هم مقایسه می‌کنند و هرشبکه ای که در جداول مسیریابی ندارند را با پرسش از روترهای مجاور به دست می‌آورند.

مزایای مسیریابی اتوماتیک

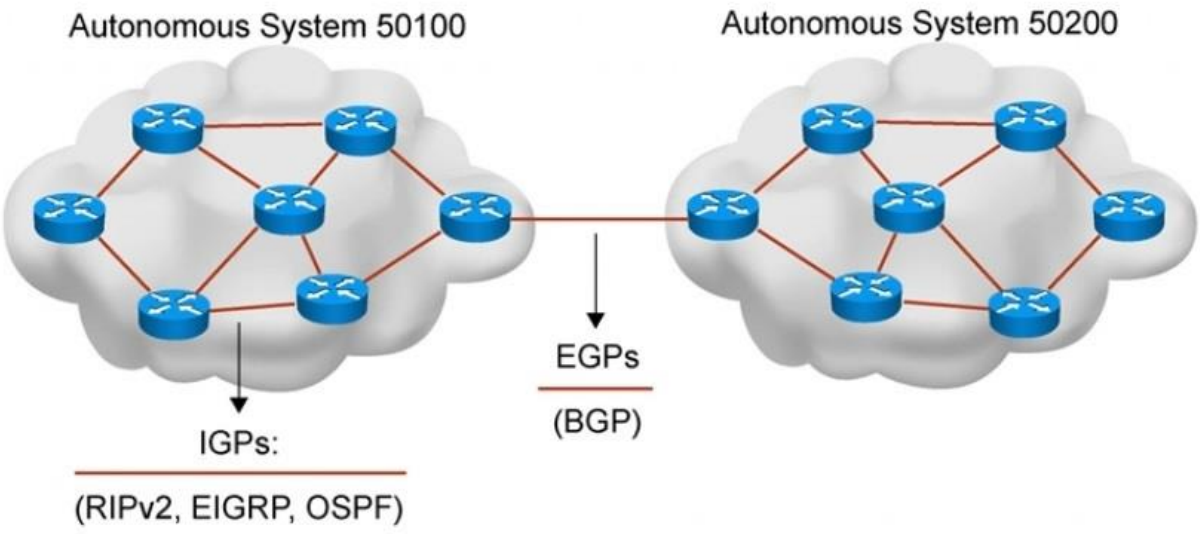
- تغییرات در توپولوژی شبکه به‌صورت اتوماتیک آپدیت می‌شوند.
- فقط اطلاعات شبکه‌هایی که به‌صورت مستقیم متصل هستند برای پیکربندی لازم می‌باشند.
- مدیریت شبکه توسط مدیر شبکه کاهش پیدا کرده است.
- برای شبکه‌های متوسط و بزرگ استفاده می‌شود.

طبقه بندی پروتکل‌های مسیریابی

طبقه اول

- **IGP[1]:** این نوع پروتکل برای تبادل اطلاعات مسیریابی روترهایی که درون مرز مشخصی بنام AS یا area قرار دارند، استفاده می‌شود. پروتکل‌های مسیریابی OSPF[2]، EIGRP[3] و RIP V2[4] شامل این دسته می‌باشند.
- **EGP[5]:** وظیفه‌ی این نوع پروتکل اتصال دو IGP نسبت بهم است. پروتکلی که به عنوان EGP استفاده می‌شود، BGP نام دارد (برای تبادل اطلاعات بین AS ها استفاده می‌شود)

[1] Interior Gateway Protocol
[2] Open Shortest Path First
[3] Enhanced Interior Gateway Routing Protocol
[4] Routing Information Protocol
[5] Exterior Gateway Protocol



شکل 5-5 نمایی شماتیک از

طبقه دوم

- **Distance Vector**

اگر یک سری روتر در راستای یک خط داشته باشیم، ساختار Distance Vector به وجود می‌آید. در این حالت برای برقراری ارتباط ما بین روترها، هر روتر با روترهای مجاورش شروع به برقراری ارتباط می کند، در صورتیکه تعداد زیادی روتر وجود داشته باشد، بازه‌ی زمانی نسبتا طولانی برای برقراری ارتباط ما بین تمامی تجهیزات وجود دارد که از دیدگاه شبکه‌های امروزی مناسب نیست، بدین جهت از این پروتکل در شبکه‌های کوچک با تعداد Device پایین استفاده می‌شود. پروتکل RIP جزء این دسته می‌باشد.

عیب Distance Vector : کند بودن و محدود بودن Device ها

- **Link-state**

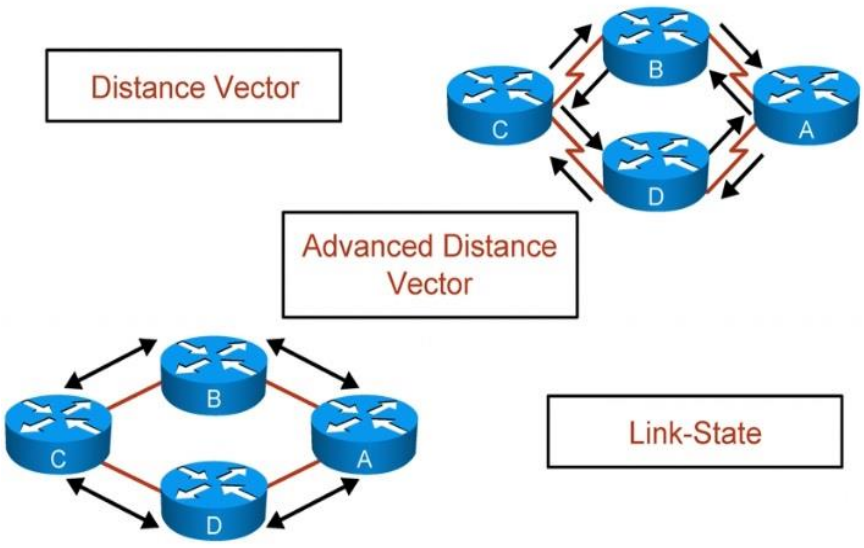
به خاطر محدودیت‌هایی که Distance Vector داشت، Linkstate به وجود آمد. Linkstate یک پروتکل به صورت ساختار سلسله مراتبی می‌باشد که این ساختار سلسله مراتبی باعث افزایش سرعت دستیابی به نقاط مختلف شبکه شد. در link- state هر گره یک نگاشت کامل از توپولوژی را دارد، در صورتی که یک گره خراب شود هر گره می‌تواند مسیر جدیدی را محاسبه کند. پروتکل OSPF در این دسته قرار دارد.

نکات

- ساختار Link-state اگر در یک پهنای باند متناسب پیاده‌سازی شود، شبکه‌ی مقبولی به وجود خواهد آمد.
- عیب Link-state این است که همه‌ی گره‌ها نیازمند یک دید راسخ از شبکه هستند.

- **Advanced Distance Vector**

این پروتکل مسیریابی یک پروتکل Hybrid یا دو رگه می‌باشد. ترکیبی از دو نوع Distance Vector و Link-state می‌باشد. بهترین نقاط از هرکدام در کنار هم قرار گرفتند و این ساختار تشکیل شد. پروتکل EIGRP در این دسته قرار دارد که از جهت سرعت عملکرد، بهترین پروتکل مسیریابی می‌باشد، اما فقط در دستگاه‌های سیسکو کاربرد دارد.



شکل 5-6 عملکرد پروتکل های مسیریابی Distance Vector، Link-state و Advanced Distance Vector

Route advertisement

Route advertisement به معنی exchange کردن جداول مسیریابی می‌باشد یعنی یک شبکه جدول مسیریابی خود را به یک شبکه دیگر یاد می‌دهد و جدول مسیریابی آن شبکه را هم یاد می‌گیرد. در واقع advertisement کردن برای سینک شدن جداول مسیریابی است.

طبقه سوم

پروتکل‌های مسیریابی classless و classful

پروتکل‌های مسیریابی در ابتدا با شبکه‌های پیش فرضی که داشتند شروع به کار کردن می‌کردند. شبکه های پیش فرض در ابتدا کوچک و تعداد محدودی بودند. در شبکه‌های کوچک مفاهیم VLSM، Subneting و Mask های متغیر خیلی مطرح نبود چون آدرس‌ها به تعداد کافی وجود داشت.
advertisement در پروتکل‌های اولیه به صورت classful انجام می‌شد، یعنی فقط در کلاس‌های با mask ،A،B و C استاندارد انجام می‌شد. پس پروتکل مسیریابی classful دارای ویژگی‌های زیر می‌باشد:

- کاملا وابسته به کلاس‌های استاندارد می‌باشند و شامل subnet mask نمی شوند.
- RIPV1 و IGRP مثال‌هایی از این نوع پروتکل مسیریابی می‌باشند.

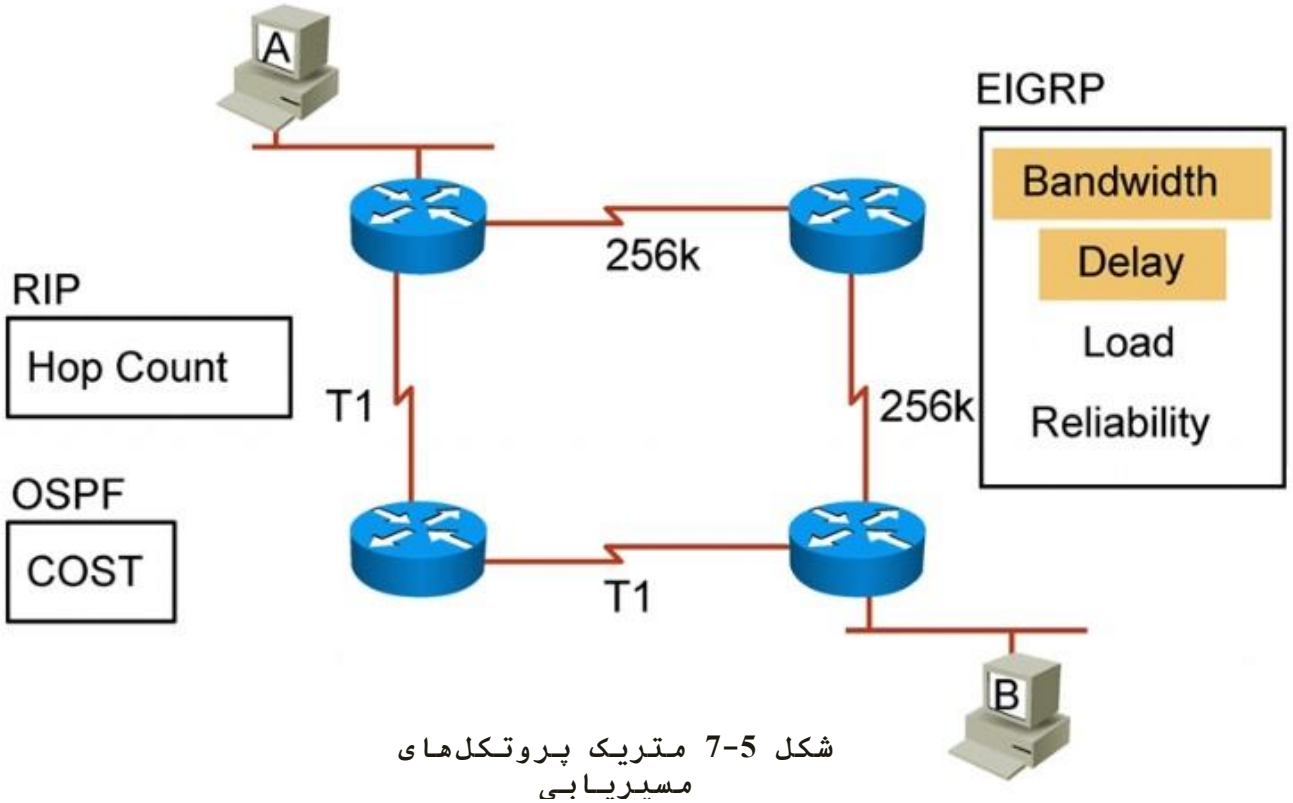
به دلیل گستردگی شبکه‌ها محدودیت آدرس به وجود آمد که باعث شد نیاز به Mask های متغیر پیدا شود. برای استفاده از mask های متغیر پروتکل مسیریابی Classless به وجود آمد. ویژگی های پروتکل مسیریابی Classless به شرح زیر می باشد:

- وابسته به کلاس نمی‌باشند و شامل subnet mask می‌باشند.
- Subnet mask با طول متغیر (VLSM) را پشتیبانی می‌کنند.
- Summary routes به صورت دستی می‌تواند در شبکه کنترل شود.
- پروتکل‌های RIPV2 ، EIGRP، OSPF و IS-IS مثال هایی از این نوع می‌باشند.

متریک

اگر یک نقطه به نقطه‌ی دیگری بخواهد دسترسی پیدا کند ممکن است توپولوژی شبکه به این صورت باشد که از مسیرهای مختلفی امکان

دسترسی از فرستنده به گیرنده وجود داشته باشد. برای همین منظور از مفهومی بنام متریک استفاده می‌کنند.
متریک مشخصه ای است که باعث می‌شود بین مسیرهای مختلف بهترین مسیر از جهت دسترسی را پیدا کرد. بهترین مسیر از جهت دسترسی یعنی معیاری که برای برقراری ارتباط بین فرستنده و گیرنده باید در نظر گرفت. مثلا در شکل زیر اگر PCA بخواهد با PCB ارتباط برقرار کند و از پروتکل RIP استفاده کند چه معیاری را باید در نظر گرفت.



شکل 5-7 متریک پروتکل‌های مسیریابی

پروتکل RIP از معیاری بنام Hop Count استفاده می‌کند.
Hop Count : یعنی شمارش تعداد روترها. مسیری که دارای Hop Count کمتری باشد به عنوان بهترین مسیر انتخاب می‌شود (کوتاهترین مسیر).
با رشد شبکه ها دیگر کوتاهترین مسیر به عنوان بهترین مسیر نمی‌توانست انتخاب شود، چون در لینک‌های ارتباطی بین نقاط شبکه ها پهنای باند وجود داشت.

پهنای باند[1]: ظرفیت قابل تبادل برای انتقال داده

[1] bandwidth

همان‌طور که در شکل(5-7) مشاهده می‌شود، ممکن است یک لینکی دارای سرعت 256K و لینک دیگر معادل T1 (T1 دارای پهنای باند 1.54Mbps می باشد) باشد، بنابراین اگر بسته ای بخواهد از لینک بالایی عبور کند، مدت زمان زیادی طول می‌کشد تا به مقصد برسد. به خاطر همین امر باید پهنای باند را در محاسبات قرار داد، بنابراین در پروتکل OSPF از متریکی بنام Cost استفاده کردند.

$$\text{Cost}=\frac{10^8}{refrence\ bandwidth}$$

هرچقدر که مقدار Cost کوچکتر باشد، بهتر می‌باشد.

Reference bandwidth: ظرفیت کابل مورد نظر می‌باشد، مثلا: FastEthernet دارای ظرفیت 100Mbps و Serial دارای 2Mbps می‌باشد.

محاسبه‌ی Cost برای FastEthernet و Serial:

FastEthernet برای $\text{Cost}=\frac{10^8}{100M}=1$

Serial برای $\text{Cost}=\frac{10^8}{2M}=50$

متریک‌های EIGRP:

$$\left.\begin{matrix} bandwidth \\ delay \\ load \\ reliability \\ MTU \end{matrix}\right\}$$

Bandwidth: پهنای باند(Mbps)
Delay: تاخیر در دریافت اطلاعات به ازای مقصد، برحسب میکروثانیه می باشد(مدت زمانی که داده به مقصد می‌رسد).
Load: میزان باری که برخط به ازای یک بازه‌ی زمانی مشخص قرار می‌گیرد. هرچی load خط بالاتر باشد، سرعت دسترسی به شبکه پایین می‌آید.

1<load<255
هرچه load به 1 نزدیک تر باشد، بهتر است.

Reliability: قابلیت در دسترس بودن خط

1<reliability<255

هرچه reliability به 255 نزدیکتر باشد، بهتر است.

MTU: حجم مجاز برای تبادل داده می‌باشد.

ضریب bandwidth و delay در فرمول 1 است یعنی در فرمول به صورت مستقیم محاسبه می‌شوند ولی 3 متریک دیگر برای حالاتی است که در شبکه می خواهند محاسبات دقیق انجام دهند، ضریب‌شان صفر است و باید با command از ضریب صفر درآورد که در محاسبه بتوان استفاده کرد.

نکات:

- هرچقدر bandwidth بالاتر برود، delay پایین می‌آید.
- هرچقدر bandwidth بهتر باشد از جهت بحث مسیریابی ظرفیت بهتری را برای شبکه می‌توان تامین کرد.

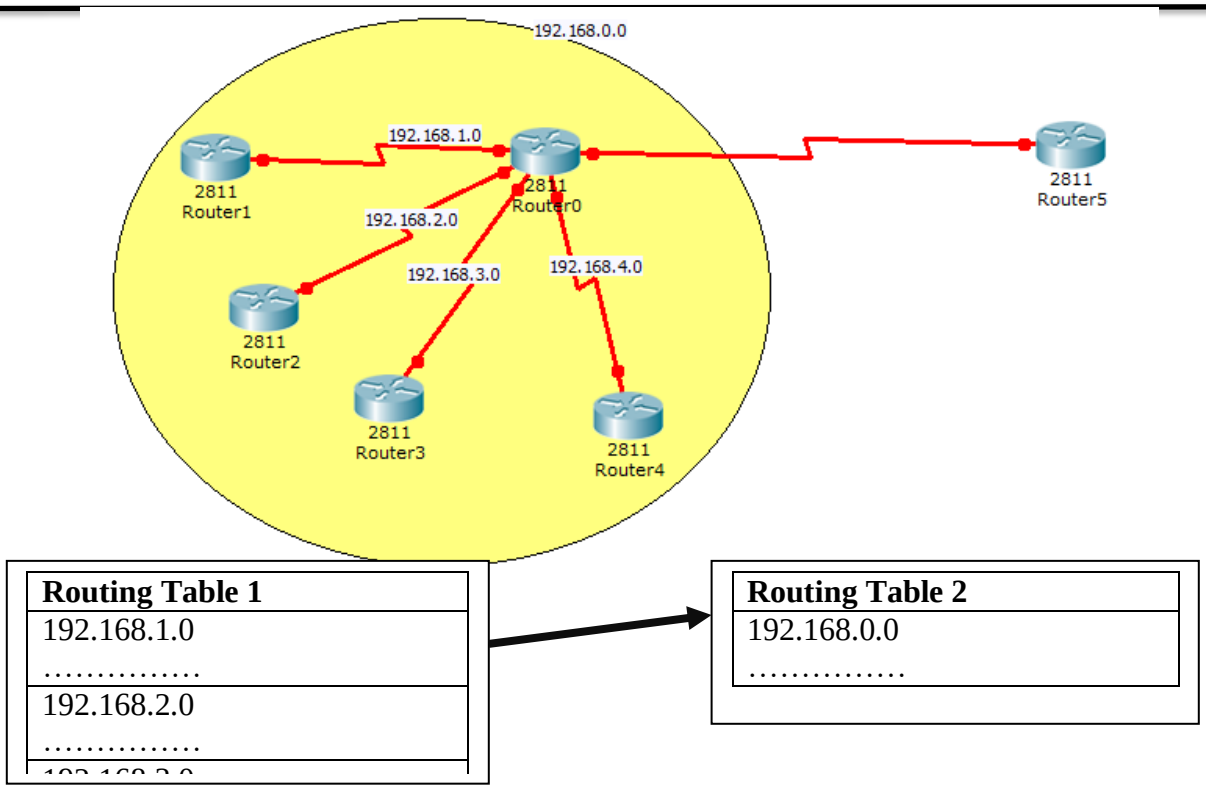
Summary: به معناي خلاصه‌سازي شبکه‌ها که دو نوع استاتيك (Static) و اتوماتيك (Automatic) مي‌باشد، که نوع اتوماتيک فقط در پروتکل‌هاي مسيريابي RIP و EIGRP وجود دارد.
زماني‌که چند IP داريم ← به يك IP واحد تبديل مي‌کنيم. Supernetting کمتر مي‌شود (شبکه‌ها را خلاصه مي‌کنيم).

مزیت Summary:

- کمتر حرف مي‌زنند و در نتيجه ترافيك شبکه کمتر مي‌شود.
- حجم کمتري ديتا در لينك قرار مي‌گيرد.
- حجم جدول مسيريابي کم مي‌شود که باعث افزايش کيفيت مسيريابي مي‌شود.

$\begin{cases} IP1 \\ IP2 \\ IP3 \end{cases} \rightarrow IP$ تبديل به يك آي پي مي‌شوند.

همان‌گونه که مي‌بينيد Routing Table 1, 2 از لحاظ اندازه بسيار متفاوتند.



شکل 5-8 نحوه ی عملکرد Summary

RIP

ویژگی‌های RIP:

- دارای ساختار Distance Vector می باشد.
- در شبکه‌های کوچک استفاده می‌شود.
- یک پروتکل استاندارد باز است.
- از الگوریتم Bellman-ford استفاده می‌کند.
- کل جدول مسیریابی را به‌عنوان آپدیت ارسال می‌کند.
- هر آپدیت حداکثر می‌تواند شامل 25 مسیر باشد.
- متریکش hop count می‌باشد.
- ماکزیمم hop count هایی که پشتیبانی می‌کند برابر 15 می‌باشد.
- Load balancing به‌صورت پیش فرض بر روی 4 مسیر با ارزش یکسان انجام می‌شود (ماکزیمم 16 مسیر یکسان)
- دارای Administrative Distance برابر 120 می‌باشد.
- دارای قابلیت Split horization و route poisoning می‌باشد. از این قابلیت‌ها برای جلوگیری از Loop در لایه 3 استفاده می‌شود.

RIP در حالت پایه در version1 قرار داشته است ولی الان در version2 استفاده می‌شود.

جدول 5-2 تفاوت

پروتکل مسیریابی	RIP V1	RIP V2
پشتیبانی از VLSM ؟	Classful	Classless
ارسال Subnet mask از طریق آپدیت مسیریابی؟	No	Yes
نوع ارسال داده	Broadcast	Multicast
تعریف شده در...	RFC 1058	RFCs 1721,1722 and 2453
پشتیبانی از خلاصه‌سازی به صورت دستی؟	No	Yes
پشتیبانی از احرازهویت؟	No	Yes

جدول 5-3 تایمرهای RIP

تایمر	توضیح
Update Timer	▪ 30 ثانیه

	▪ زمان بین دو آپدیت متوالی
Invalid Timer	▪ 180 ثانیه ▪ زمانی که یک روتر منتظر دریافت آپدیت از همسایه است. ▪ اگر هیچ آپدیتی برای این دوره‌ی زمانی وجود نداشته باشد، مسیر به عنوان غیرقابل دسترس علامت گذاری می‌شود.
Flush Timer	▪ 240 ثانیه ▪ زمان نهایی برای خارج شدن route از جدول

معایب RIP

- پهنای باند بیشتری برای ارسال آپدیت‌ها مورد استفاده قرار می‌گیرد.
- در محاسبه‌ی متریک پهنای باند را در نظر نمی‌گیرد، فقط از Hop Count استفاده می‌کند.
- همگرایی کند[1]
- تشکیل حلقه‌های مسیریابی
- محدودیت تعداد device (ماکزیمم 15 عدد device)

حلقه‌های مسیریابی

- حلقه‌های مسیریابی به علت رفتار پیش فرض RIP تشکیل می‌شوند.
- به‌طور کامل جداول مسیریابی را مبادله می‌کنند.
- همگرایی کند
- آپدیت‌های دریافتی را تائید نمی‌کنند.

:Rip Configuration

1	Router(config)#**router rip**
2	Router(config-router)#**version 2**
3	Router(config-router)#**no auto-summary**
4	Router(config-router)#**network *net-id***

- خط 1: فعال کردن پروتکل مسیریابي
- خط 2: پیش فرض Ver2 فعال مي باشد.
- خط 3: شبکه‌ها را به صورت اتوماتیك خلاصه نكن.
- خط 4: معرفي شبکه‌هايي كه به روتر متصل مي‌باشند.

دستورات Verify RIP:

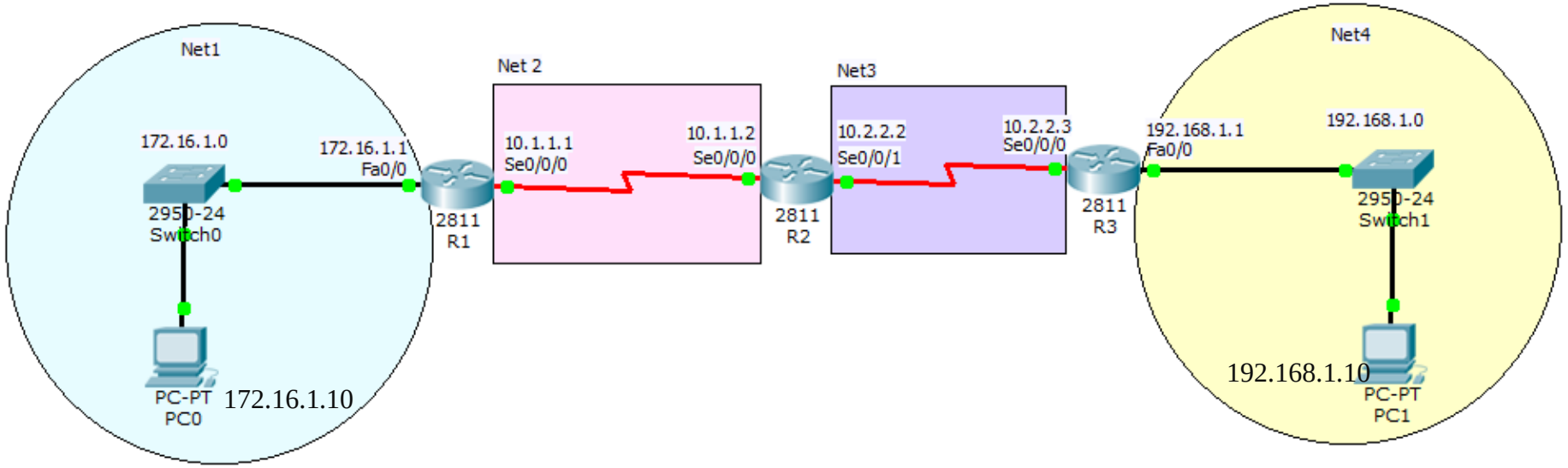
1	Router#**show ip protocols**
2	Router#**show ip route**
3	Router#**debug ip rip**

[1] Slow Convergence

4	Router#**undebug all**

- خط 1: اطلاعات مربوط به پروتکل مسیریابی که روی روتر اجرا شده است را نشان می‌دهد.
- خط 2: مشاهده‌ي جدول مسيريابي
- خط 3: جهت عیب‌یابي اطلاعات تبادل شده ما بین روترها استفاده مي‌شود، زماني به كار مي‌رود كه چند شبكه را به هم وصل كرده‌ايم و ممكن است اشتباه پيش بيايد و بخواهيم چك كنيم كه آيا ارتباط درست برقرار شده‌است يا خير. در اين حالت Log ها را نمايش مي‌دهد.
- خط 4: جهت غيرفعال كردن debug.

سناریو Dynamic Routing with RIP



شکل 5-9 سناریو Dynamic Routing with RIP

1- اختصاص IP به اینترفیس روترها

Router1:

```
1  Router(config)#int f0/0
2  Router(config-if)#ip address 172.16.1.1 255.255.255.0
3  Router(config-if)#no shutdown
4
5  Router(config-if)#int s0/0/0
6  Router(config-if)#ip address 10.1.1.1 255.255.255.0
7  Router(config-if)#clock rate 64000
8  Router(config-if)#no shutdown
```

Router2:

```
1  Router(config)#int s0/0/0
2  Router(config-if)#ip address 10.1.1.2 255.255.255.0
3  Router(config-if)#no shutdown
4
5  Router(config-if)#int s0/0/1
6  Router(config-if)#ip address 10.2.2.2 255.255.255.0
7  Router(config-if)#clock rate 64000
8  Router(config-if)#no shutdown
```

Router3:

```
1  Router(config)#int f0/0
2  Router(config-if)#ip address 192.168.1.1 255.255.255.0
3  Router(config-if)#no shutdown
4
5  Router(config-if)#int s0/0/0
6  Router(config-if)#ip address 10.2.2.3 255.255.255.0
7  Router(config-if)#no shutdown
```

2- اجرای RIP

Router1:

```
1  Router(config)#router rip
2  Router(config-router)#version 2
3  Router(config-router)#network 172.16.0.0
4  Router(config-router)#network 10.0.0.0
```

Router2:

```
1  Router(config)#router rip
2  Router(config-router)#version 2
3  Router(config-router)#network 10.0.0.0
```

Router3:

```
1  Router(config)#router rip
2  Router(config-router)#version 2
3  Router(config-router)#network 192.168.1.0
4  Router(config-router)#network 10.0.0.0
```

3-خروجی

Router1:

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

Gateway of last resort is not set

     10.0.0.0/24 is subnetted, 2 subnets
C       10.1.1.0 is directly connected, Serial0/0/0
R       10.2.2.0 [120/1]  via 10.1.1.2, 00:00:06, Serial0/0/0
     172.16.0.0/24 is subnetted, 1 subnets
C       172.16.1.0 is directly connected, FastEthernet0/0
R    192.168.1.0/24 [120/2] via 10.1.1.2, 00:00:06, Serial0/0/0
```

همانطور که مشاهده می‌کنیم این دستور، route های شبکه‌ی rip را نمایش می‌دهد. route های شبکه rip با R نمایش داده می‌شود. در این خروجی پروتکل rip شبکه‌ی 10.2.2.0 را از اینترفیس Seial0/0/0 با IP:10.1.1.2 و شبکه‌ی 192.168.1.0 را از اینترفیس Serial0/0/0 با IP:10.1.1.2 یاد گرفته است.

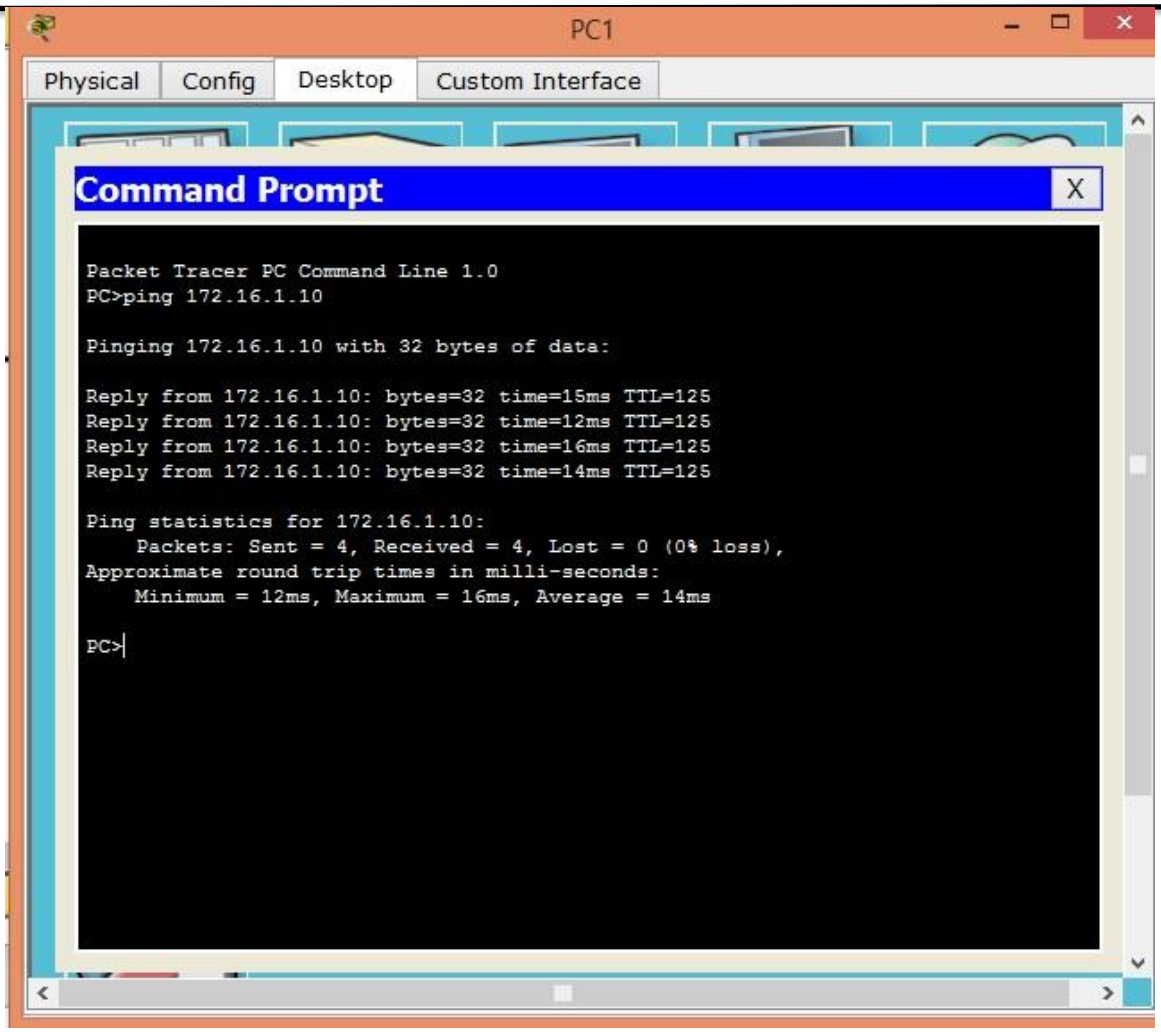
```
Router#show ip protocols
Routing Protocol is "rip"
Sending updates every 30 seconds, next due in 16 seconds
Invalid after 180 seconds, hold down 180, flushed after 240
Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
Redistributing: rip
```

```
Default version control: send version 2, receive 2
  Interface              Send  Recv  Triggered RIP  Key-chain
  FastEthernet0/0        2     2
  Serial0/0/0            2     2
Automatic network summarization is in effect
Maximum path: 4
Routing for Networks:
  10.0.0.0
  172.16.0.0
Passive Interface(s):
Routing Information Sources:
  Gateway         Distance      Last Update
  10.1.1.2        120           00:00:00
Distance: (default is 120)
```

در خروجی این دستور مشاهده می‌کنیم که :

- ✓ پروتکل مسیریابی rip می‌باشد.
- ✓ Update ها هر 30 ثانیه ارسال می‌شوند.
- ✓ مدت زمان ارسال آپدیت بعدی، 16 ثانیه می‌باشد.
- ✓ از اینترفیس های fa0/0 و S0/0/0 برای انجام advertise استفاده می‌کند.
- ✓ شبکه هایی که advertise می‌کند، شبکه های 10.0.0.0 و 172.16.0.0 می‌باشند.
- ✓ Gateway برای دسترسی 10.1.1.2 می‌باشد.

```
Router#debug ip rip
RIP protocol debugging is on
RIP: received v2 update from 10.1.1.2 on Serial0/0/0
     10.2.2.0/24 via 0.0.0.0 in 1 hops
     192.168.1.0/24 via 0.0.0.0 in 2 hops
RIP: sending v2 update to 224.0.0.9 via FastEthernet0/0 (172.16.1.1)
RIP: build update entries
     10.0.0.0/8 via 0.0.0.0, metric 1, tag 0
     192.168.1.0/24 via 0.0.0.0, metric 3, tag 0
RIP: sending v2 update to 224.0.0.9 via Serial0/0/0 (10.1.1.1)
RIP: build update entries
     172.16.0.0/16 via 0.0.0.0, metric 1, tag 0
```



شکل 5-10 Ping از PC1

OSPF

ویژگی‌های OSPF:

- پروتکلی با ساختار Link state می‌باشد.
- پروتکل استاندارد باز است.
- از مفهوم COST استفاده می‌کند.

$$Cost = \frac{10^8}{R.B}$$

- از الگوریتم درختی[1] برای مسیریابی استفاده می‌کند.
- ساختار درختی را در یک D.B[2] قرار می‌دهد و بهترین مسیر را از D.B استخراج می‌کند.
- روترهایی که در یک Area قرار دارند، پکت‌هایی که به یکدیگر می‌فرستند LSA Packet[3] نام دارند.
- ساختار فیزیکی اتصال روترها درختی است.
- سرعت عملکرد بالایی دارد.
- برای شبکه‌هایی با ساختار بزرگ به‌کار برده می‌شوند.
- الگوریتمی که برای مسیریابی استفاده می کند، الگوریتم SPF[4] می‌باشد.
- دارای Administrative Distance برابر 110 می‌باشد.
- آپدیت‌ها را از طریق IP های 224.0.0.6 و 224.0.0.5 (IPی Multicast) ارسال می‌کند.

انواع روترها در OSPF

روترها در OSPF به دو دسته تقسیم می‌شوند:

- **Single Area:** در این حالت یک محدوده وجود دارد که روترها داخل آن محدوده قرار دارند و فعالیت می‌کنند. این محدوده با نام area مشخص می‌شود و area همیشه با یک شماره باید تعریف شود. در این حالت شماره‌ی area خیلی مهم نیست و هرعددی می‌تواند باشد.

- **Multi Area:** در این حالت چندین areaی مختلف بهم وصل وصل شده اند. ساختار به صورت درختی است روترها جایگاه خاصی دارند (بعضی‌ها بالا، بعضی ها پایین و بعضی‌ها ما بین areaها) و چون areaهای مختلفی وجود دارد، شماره‌ی area ها طبق قواعدی که جلوتر بحث خواهد شد باید انتخاب شوند.

[1] Hierchical
[2] Data Base
[3] Link State Advertisement
[4] Shortest Path First

نقش‌های روترها در یک Area

بطور کلی روترهایی که در یک Area قرار می‌گیرند 3 نقش اصلی دارند.

1- **DR[1]:** روتری است که اگر تغییری برای یکی از روترها اتفاق بیفتد، آن تغییرات را به بقیه‌ی روترها می‌رساند(کنترل و مدیریت محدوده‌ی داخلی Area)

2- **BDR[2]:**

- پشتیبان DR است، فقط آپدیت‌ها را دریافت خواهد کرد اما بقیه‌ی روترها را آپدیت نخواهد کرد.
- به محض خارج شدن DR از شبکه وظیفه‌ی DR را ادامه می‌دهد.

3- **DROTHER:** روترهای معمولی هستند که به صورت پیش فرض، روترها در این گروه هستند(روتری که DR و BDR نباشد) .

نکات

- انتخاب DR و BDR با استفاده از پکت‌های Hello انجام می‌شود.
- روتر با اولویت بالا در OSPF به‌عنوان DR و روتر با دومین اولویت به‌عنوان BDR انتخاب خواهد شد.
- به‌صورت پیش فرض، اولویت همه‌ی روترها برابر 1 می‌باشد.
- در حقیقت روتر با بالاترین اولویت Router-id به عنوان DR و روتر با دومین اولویت به عنوان BDR انتخاب خواهد شد.
- آدرس‌های Multicast برای آپدیت استفاده می‌شود:
  - روترهای دیگر به DR : 224.0.0.6
  - DR به روترهای دیگر: 224.0.0.5

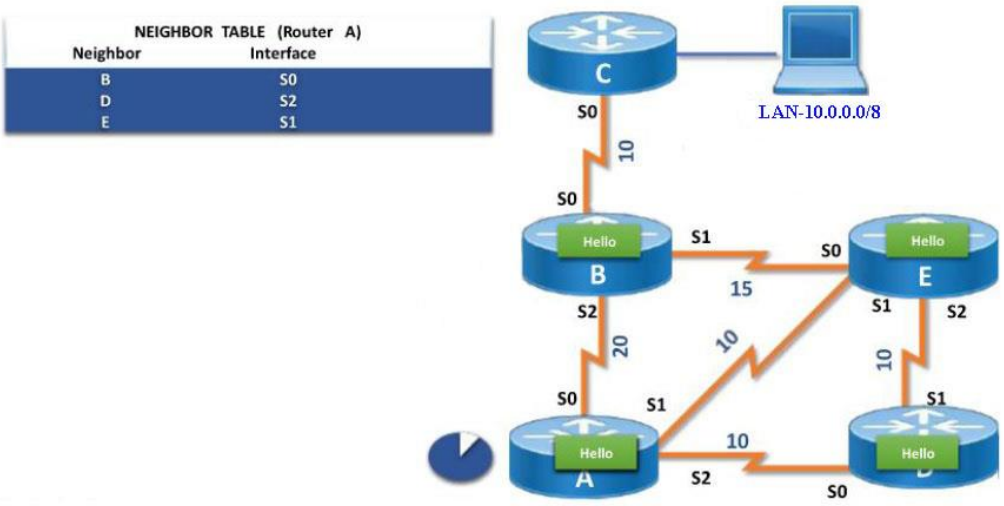
جداول OSPF

OSPF دارای 3 جدول زیر می‌باشد:

- **Neighbor Table**

حاوی اطلاعاتی در مورد همسایگان OSPF می‌باشد.

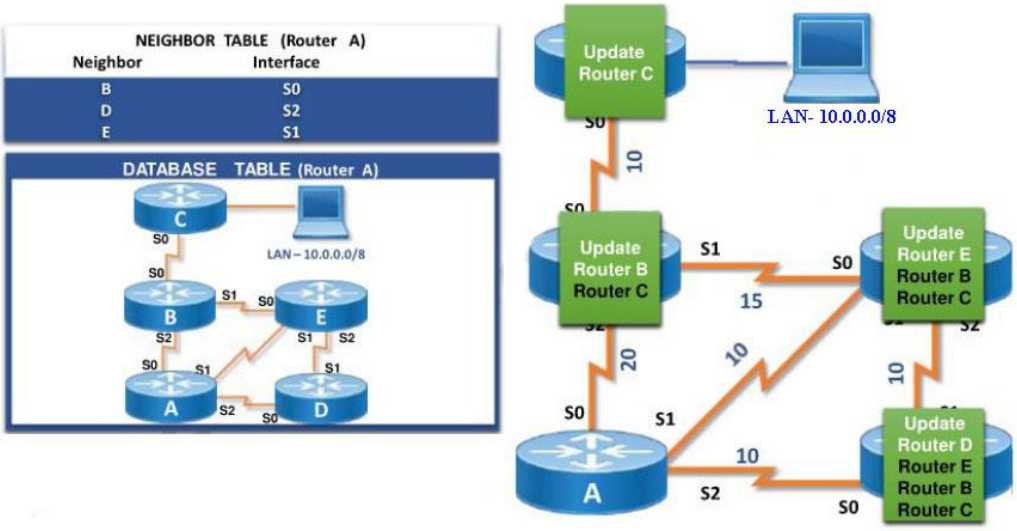
[1] Desinated Router
[2] Backup DR



شکل 5-10 Neighbor Table در OSPF

- **Database Table**

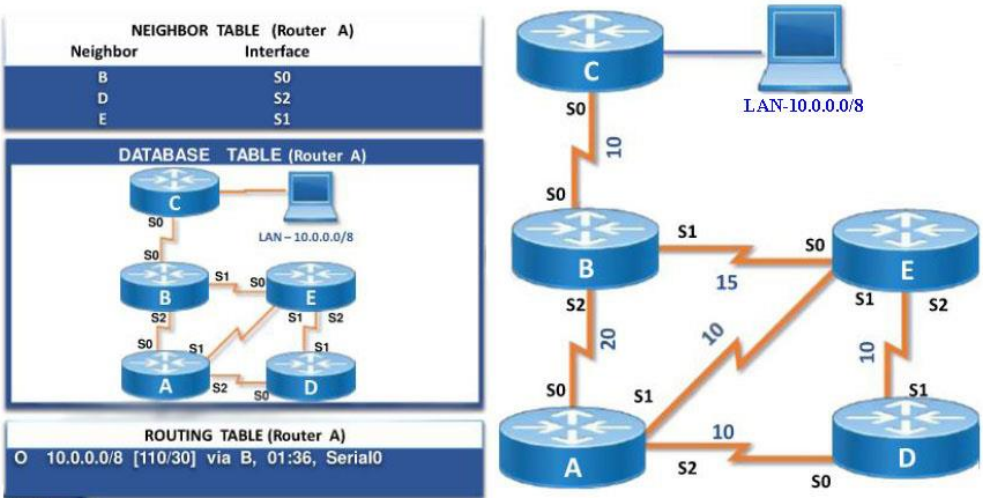
شامل اطلاعاتی در مورد نمایش کلی توپولوژی با توجه به هر روتر می‌باشد.



شکل 5-11 Database Table در OSPF

- **Routing Table**

حاوی اطلاعاتی در مورد بهترین مسیر محاسبه شده با استفاده از الگوریتم SPF در Database Table می باشد.



شکل 12-5 Routing Table در

انواع روترها در Multi areaها

1- **Backbone Router**: روترهایی هستند که با همه‌ی اینترفیس‌هایشان در backbone area قرار گرفته‌اند. مثل: روترهای A و B

Backbone router ها باید همیشه دارای شماره صفر باشند.

به دلیل وجود ساختار درختی Area های غیر از صفر باید به Areaهای صفر متصل باشند ← حتما یک Backbone Area داریم.

2- **Internal Router**: روترهایی که با تمامی Interface هایشان در Area های غیر صفر قرار گرفته‌اند، یعنی باقی روترها در Area های 1و 2و3 مثل روتر H,G,F.

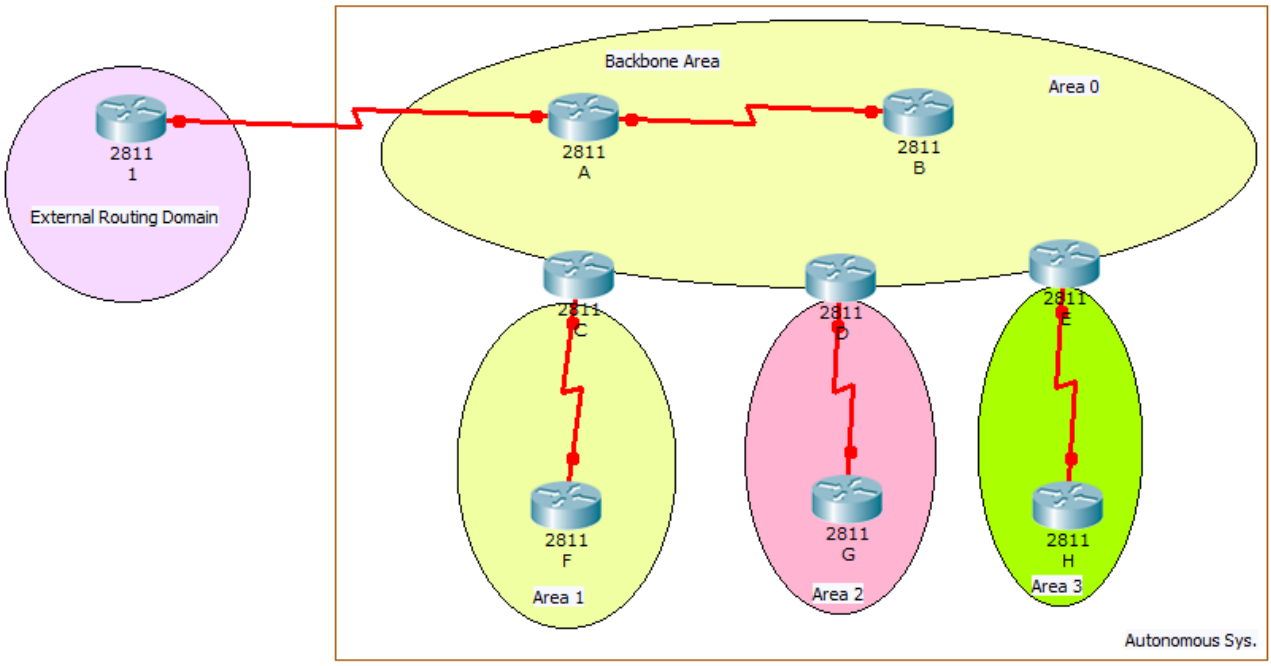
3- **ABR**[1]: روترهایی که در مرز Areaها قرار گرفته‌اند. مثل روترهای E,D,C.

وظیفه‌ی اتصال Area های مختلف نسبت به هم را بر عهده دارند.

4- **ASBR**[2]: روتری است که در مرز AS قرار گرفته است. مثل روتر I

AS: مجموعه همه‌ی Area ها با هم می‌شود.

[1] Area Border Router
[2] Autonomous System Border Router



شکل 5-13 انواع روترها

- **Router-ID:** یک IP به‌صورت 4octet می‌باشد. تفاوتش با IPهای معمولی این است که به عنوان مشخصه یا برچسب روی روتر مورد نظر در شبکه قرار می‌گیرد و دسترسی به آن روتر و اطلاعات آن روتر را ساده‌تر می‌کند. پس مشخصه‌ای Unique است که از طریق آن به راحتی می توان روترها را شناسایی کرد.
- **Process-ID:** OSPF قابلیت چند پروسس بودن را دارد، یعنی روی یک روتر می‌شود چند تا OSPF اجرا کرد، به همین خاطر از process-id استفاده می‌شود. process-id مشخصه‌ای است که توسط آن یک پروسس مستقل برای پروتکل OSPF تعریف می‌شود. عددی دلخواه است که توسط خودمان تعیین می‌شود.

- **Wildcard:** مربوط به بحث IP-Address ها است. اگر Mask متغیر باشد از 255 کم می‌کنیم و Wildcard بدست می‌آید.

محاسبه Wildcard

Global Subnet Mask – Subnet Mask = Wildcard Mask

مثال:

Net ID: 192.168.18.0
Mask: 255.255.255.0
Wide Card=255.255.255.255 – 255.255.255.0 = 0.0.0.255

زمانی که IP اینترفیس نوشته شود، wildcard برابر 0.0.0.0 می‌باشد ولی اگر NET ID نوشته شود، wildcard از دستور بالا به دست می آید.

- **Area-ID:** شماره‌ی Area است که در سناریو گفته می‌شود (دلخواه نیست).

OSPF Configuration:

1	Router(config)# **router ospf *process-id***
2	Router(config-router)#**router-id *router_id***
3	Router(config-router)#**network *net_id* *wildcard* area *area_id***
4	**OR**
5	Router(config-router)#**network *interface_ip* *wildcard* area *area_id***

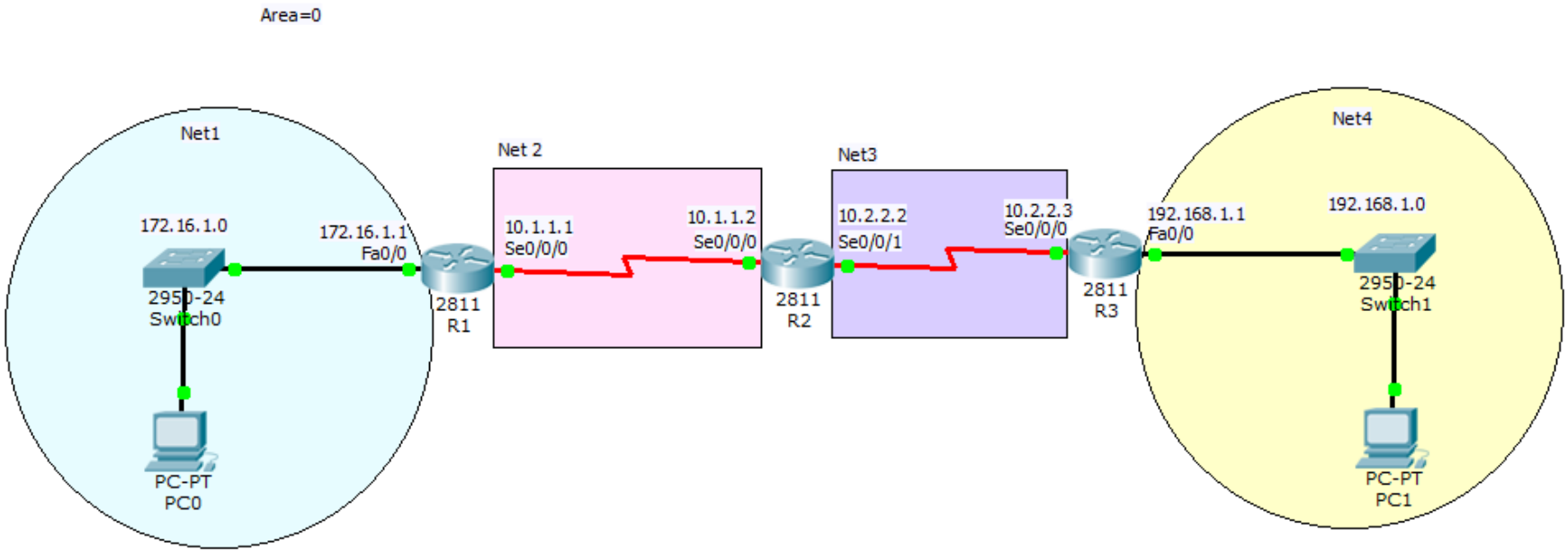
- خط1: تعریف OSPF به عنوان پروتکل مسیریابی.
- خط2: یک شماره‌ی دلخواه اما یونیک برای router-id مشخص می‌شود (این خط اجباری نیست).
- خط3: شبکه‌هایی که به اینترفیس‌های روتر در یک areaی مشخص متصل هستند، معرفی می‌شود. چون OSPF یک پروتکل Classless می‌باشد بنابراین فرقی ندارد که interface-ip یا net-id نوشته شود. بنابراین برای معرفی شبکه‌ها از دستور خط3 یا خط 5 استفاده می‌شود.

دستورات Verify OSPF

1	Router#**show ip protocols**
2	Router#**show ip route**
3	Router#**show ip ospf**
4	Router#**show ip ospf neighbor**
5	Router#**debug ip ospf events**
6	Router#**debug ip ospf packet**
7	Router#**undebug all**
8	Router#**clear ip ospf process**

- خط 2 : دیدن جدول مسیریابی روترهای مربوطه، routeهای OSPF با مشخصه‌ی "O" نمایش داده می‌شود.
- خط3: این دستور: router-id ، process-id و تعداد دفعاتی که الگوریتم SPF محاسبه شده است را نمایش می‌دهد.
- خط4: شناسایی روترهای مجاور که شامل پروتکل مسیریابی OSPF می‌باشند و بررسی وضعیت DR/BDR
- خط5و 6: دستور عیب یابی
- خط7: غیرفعال کردن عیب یابی
- خط8: انتخاب پروسه

سناریو : Dynamic Routing with OSPF



شکل 5-14 سناریو : Dynamic Routing

1-اختصاص IP به روترها

اختصاص IP در سناریوی شکل (5-9) آورده شده است.

2-اجرای OSPF

Router1:

```
1  Router(config)#router ospf 100
2  Router(config-router)# router-id 1.1.1.1
3  Router(config-router)#network 10.1.1.1 0.0.0.0 area 0
4  Router(config-router)#network 172.16.1.1 0.0.0.0 area 0
```

Router 2:

```
1  Router(config)#router ospf 100
2  Router(config-router)# router-id 2.2.2.2
3  Router(config-router)#network 10.1.1.2 0.0.0.0 area 0
4  Router(config-router)#network 10.2.2.2 0.0.0.0 area 0
```

Router3:

```
1  Router(config)#router ospf 100
2  Router(config-router)# router-id 3.3.3.3
3  Router(config-router)#network 10.2.2.3 0.0.0.0 area 0
4  Router(config-router)#network 192.168.1.1 0.0.0.0 area 0
```

3-خروجی

Router1:

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

Gateway of last resort is not set

     10.0.0.0/24  is  subnetted, 2  subnets
C       10.1.1.0   is directly connected, Serial0/0/0
O       10.2.2.0 [110/128]  via 10.1.1.2,  00:14:14, Serial0/0/0
     172.16.0.0/24  is subnetted, 1  subnets
C       172.16.1.0   is directly connected,  FastEthernet0/0
O    192.168.1.0/24 [110/129]  via 10.1.1.2,  00:13:24, Serial0/0/0
```

Router1

Router#show ip protocols

Routing Protocol is "ospf 100"
Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
Router ID 1.1.1.1
Number of areas in this router is 1. 1 normal 0 stub 0 nssa
Maximum path: 4
Routing for Networks:
10.1.1.1 0.0.0.0 area 0
172.16.1.1 0.0.0.0 area 0
Routing Information Sources:

Gateway	Distance	Last Update
1.1.1.1	110	00:20:02
2.2.2.2	110	00:19:22
3.3.3.3	110	00:19:09

Distance: (default is 110)

Router1

Router#show ip ospf
Routing Process "ospf 100" with ID 1.1.1.1
Supports only single TOS(TOS0) routes
Supports opaque LSA
SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
Number of external LSA 0. Checksum Sum 0x000000
Number of opaque AS LSA 0. Checksum Sum 0x000000
Number of DCbitless external and opaque AS LSA 0
Number of DoNotAge external and opaque AS LSA 0
Number of areas in this router is 1. 1 normal 0 stub 0 nssa
External flood list length 0
Area BACKBONE(0)
Number of interfaces in this area is 2
Area has no authentication
SPF algorithm executed 6 times
Area ranges are
Number of LSA 3. Checksum Sum 0x01dbc6
Number of opaque link LSA 0. Checksum Sum 0x000000
Number of DCbitless LSA 0
Number of indication LSA 0
Number of DoNotAge LSA 0
Flood list length 0

همان‌طور که می‌بینیم، process-idی این روتر برابر 100 و router-id برابر 1.1.1.1 می‌باشد و الگوریتم SPF، 6بار محاسبه شده است.

Router1

```
Router#show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
2.2.2.2           0   FULL/ -         00:00:33    10.1.1.2        Serial0/0/0
```

این روتر به روتر همسایه ای با مشخصات زیر متصل شده است:

Router-idی روتر همسایه :2.2.2.2

ip ی اینترفیس همسایه : 10.1.1.2

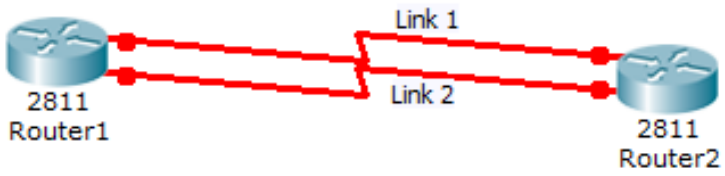
اینترفیس روتر همسایه : Serial0/0/0

Router1

```
Router#debug ip ospf events
OSPF events debugging is on
Router#
06:46:20: OSPF: Rcv hello from 2.2.2.2 area 0 from Serial0/0/0 10.1.1.2

06:46:20: OSPF: End of hello processing
```

Load Balancing with OSPF

Load balancing یعنی load را به ازای لینک‌های ارتباطی موجود تقسیم کرد. یعنی اگر از یک نقطه‌ای مثل A به نقطه‌ی B بیش از یک لینک ارتباطی وجود داشت، به‌جای اینکه از یک لینک برای تبادل اطلاعات استفاده شود از همه‌ی لینک‌های ارتباطی موجود به‌صورت همسان و همزمان استفاده شود.
Load balancing باعث می‌شود، باری که از یک نقطه به نقطه‌ی دیگری منتقل می‌شود بر تمام لینک‌ها تقسیم شود و ترافیک کمتری از لینک‌ها عبور کند و باعث افزایش سرعت عمل در شبکه شود. پروتکل‌های مسیریابی به‌صورت پیش فرض، load balancing را به‌طور اتوماتیک بین 4 لینک با ارزش گذاری یکسان را انجام می‌دهند (ارزش گذاری یکسان یعنی یکسان بودن متریک).



شکل 5-15 Loadbalancing بین دو

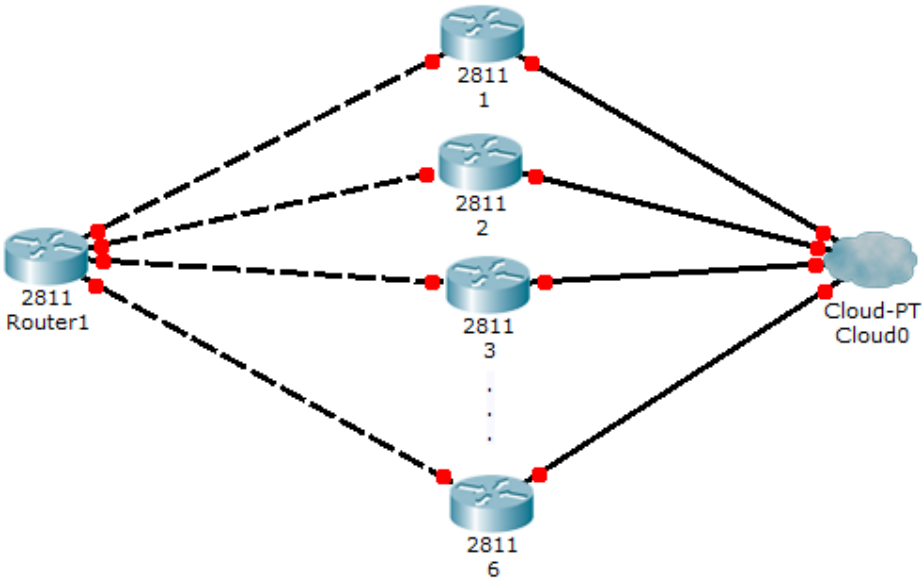
پروتکل OSPF، load balancing به ازای لینک های با ارزش یکسان را انجام می‌دهد. چون OSPF از متریکی بنام Cost استفاده می‌کند بنابراین باید برای ارزش‌گذاری یکسان بین لینک ها از دستور زیر استفاده کرد:

1	Router(config-if)#**ip ospf cost <value>**

در واقع با استفاده از این دستور Costها را برای لینک‌های موجود یکسان می‌کنیم.
برای تعریف لینک‌هایی بیش از 4 عدد، دستور زیر بکار برده می‌شود:

1	Router(config-router)#**maximum-paths <value>**

Maximum-path: تعداد مسیرها به‌طور پیش فرض 4 و حداکثر 16 مسیر می‌تواند باشد.
برای مثال در شکل (5-16)، یک روتر به 6 روتر مقابل متصل شده است. برای تقسیم بار بین این 6 لینک باید به‌صورت زیر عمل کرد.



شکل 5-16 Loadbalancing بین 6 لینک

```
1  Router(config)#interface range fastEthernet 0/1-6
2  Router(config-if)#ip ospf cost 5
3  Router(config)#router ospf 100
4  Router(config-router)#maximum–paths 6
```

- خط 2: عدد 5 به این معناست که ارزش همه‌ی لینک‌ها 5 می‌باشد.
- خط 4: تعداد لینک ارتباطی به منظور تقسیم بار برابر 6 می باشد.

OSPF Authentication

در لایه‌ی سوم بین پروتکل‌های مسیریابی پسوردگذاری می‌تواند انجام شود یعنی مثلا وقتی دو روتر می‌خواهند تبادل اطلاعات بکنند، سیستم احراز هویت اجرا شود. در واقع احراز هویت به این منظور انجام می‌شود که اگر از بیرون یک روتری خواست به شبکه وصل شود، نتواند داخل areaای شود که پروتکل OSPF در آن run شده است.
پروتکل OSPF دو نوع Authentication را پشتیبانی کند:

- **PlainText(Simple):** بدین معناست که در مورد یک رمز شفاف صحبت شود (پسورد بین روترها رمز نمی‌شود).

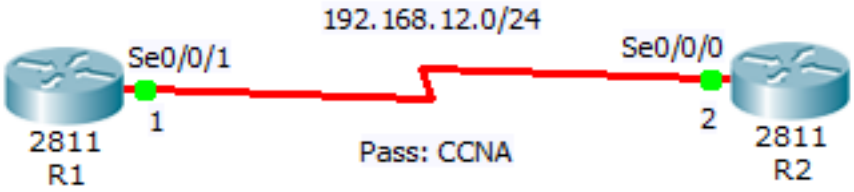
امنیت PlainText پایین است و دیگر کاربرد ندارد. رمزها به راحتی برای یکدیگر بصورت واضح ارسال می‌شوند.

- **MD5[1]:** ، این پروتکل برای رمز نمودن اطلاعات می‌باشد.

```
1  R1(Config)#interface Serial0/0/0
2  R1(Config-if)# ip ospf authentication-key یسورد مورد نظر
3  R1(Config-if)#ip ospf authentication [message-digest| Null]
4  R1(config-router)#area area-id authentication [message-digest]
```

- خط 1: وارد Interface ای می‌شویم که قرار است بین دو روتر، مکانیزم احراز هویت راه اندازی نماییم.
- خط 2: در این خط رمز تعریف می‌کنیم که باید بین دو روتر مشترک باشد.
- خط3: پسوردی که در خط 2 تعریف شده است را با الگوریتم MD5، احراز هویت می‌کند. گزینه‌ی Null حالت authentication از نوع plainText می‌باشد (در واقع نوع authentication برای یک اینترفیس خاص را مشخص می‌کند).
- خط 4: Authentication به ازای کل Area است که در Multi Area استفاده می‌شود.

مثال:



شکل 5-17 سناریو

R1

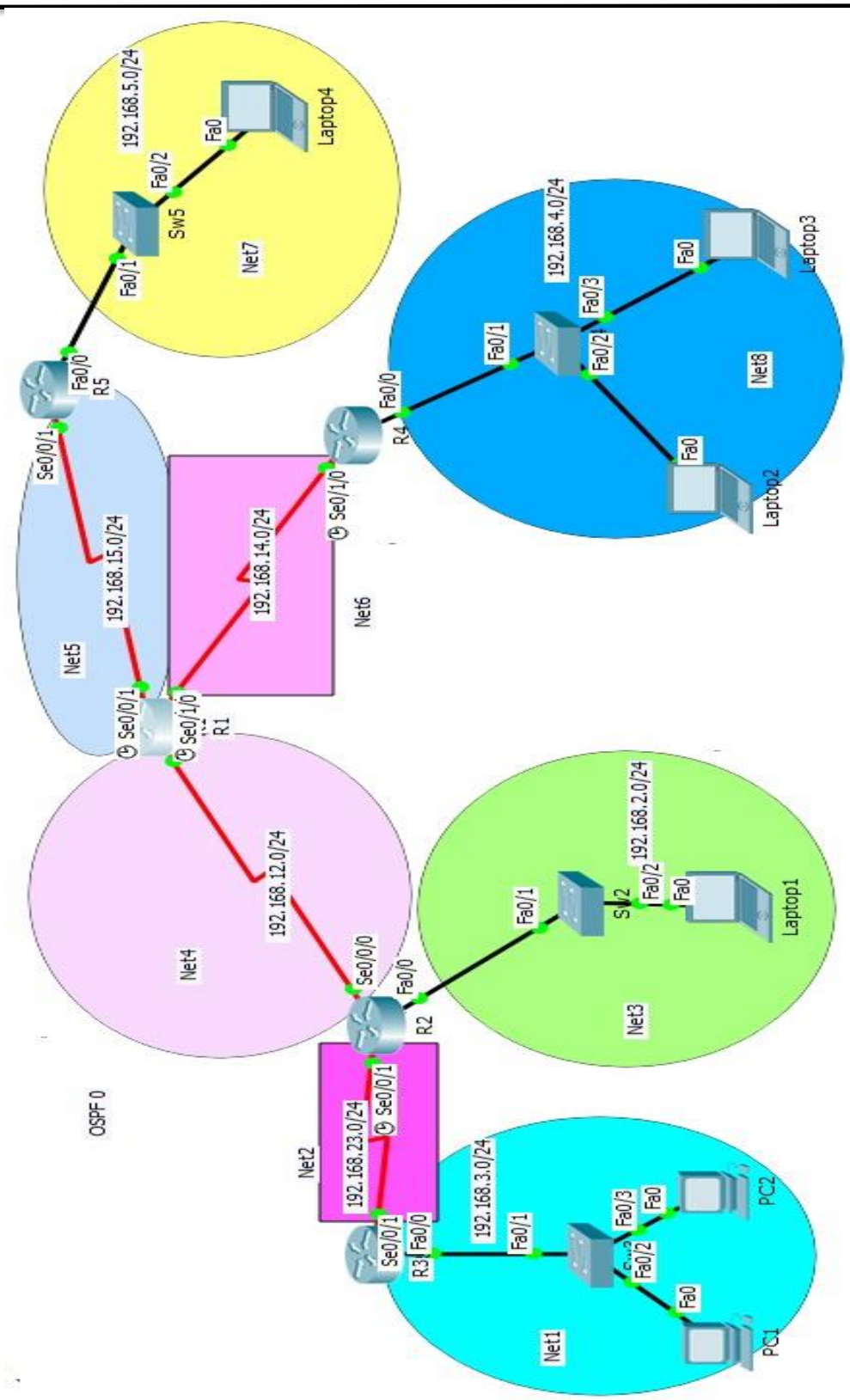
```
1  R1(Config)#interface Serial0/0/1
2  R1(Config-if)#clock rate 64000
3  R1(Config-if)#ip address 192.168.12.1 255.255.255.0
4  R1(Config-if)#no shutdown
5  R1(Config-if)#ip ospf authentication message-digest
6  R1(Config-if)#ip ospf authentication-key CCNA
```

R2

[1] Message Digest 5

1	R2(Config)#**interface Serial0/0/0**
2	R2(Config-if)#**ip address 192.168.12.2 255.255.255.0**
3	R1(Config-if)#**no shutdown**
4	R2(Config-if)#**ip ospf authentication message-digest**
5	R2(Config-if)#**ip ospf authentication-key CCNA**

سنـاريـو : OSPF-authentication



شکل 5-18 سناریو : -OSPF

با توجه به دیاگرام شکل(5-18) پروتکل مسیریابی OSPF را در area 0 راه اندازی کرده و ارتباط R3 با R2 و R1 با R4 را با استفاده از مکانیزم احراز هویت پیاده‌سازی نمایید.

1- اختصاص IP به اینترفیس‌های روتر

R1

```
1  Router(config)#interface serial 0/0/0
2  Router(config-if)#ip address 192.168.12.1 255.255.255.0
3  Router(config-if)#clock rate 64000
4  Router(config-if)#no shutdown
5
6  Router(config-if)#int s0/0/1
7  Router(config-if)#ip address 192.168.15.1 255.255.255.0
8  Router(config-if)#clock rate 64000
9  Router(config-if)#no shutdown
10
11 Router(config-if)#int s0/1/0
12 Router(config-if)#ip address 192.168.14.1 255.255.255.0
13 Router(config-if)#no shutdown
```

R2

```
1  Router(config)#int s0/0/0
2  Router(config-if)#ip address 192.168.12.2 255.255.255.0
3  Router(config-if)#no shutdown
4
5  Router(config-if)#int s0/0/1
6  Router(config-if)#ip address 192.168.23.2 255.255.255.0
7  Router(config-if)#clock rate 64000
8  Router(config-if)#no shutdown
9
10 Router(config-if)#int f0/0
11 Router(config-if)#ip address 192.168.2.2 255.255.255.0
12 Router(config-if)#no shutdown
```

R3

```
1  Router(config)#int f0/0
2  Router(config-if)#ip address 192.168.3.3 255.255.255.0
3  Router(config-if)#no shutdown
4
5  Router(config-if)#int s0/0/1
6  Router(config-if)#ip address 192.168.23.3.255.255.255.0
7  Router(config-if)#no shutdown
```

R4

```
1  Router(config)#int f0/0
2  Router(config-if)#ip address 192.168.4.4 255.255.255.0
3  Router(config-if)#no shutdown
4
5  Router(config)#int s0/1/0
6  Router(config-if)#ip address 192.168.14.4 255.255.255.0
7  Router(config-if)#clock rate 64000
8  Router(config-if)#no shutdown
```

R5

```
1  Router(config)#int f0/0
2  Router(config-if)#ip address 192.168.5.5 255.255.255.0
3  Router(config-if)#no shutdown
4
5  Router(config-if)#int s0/0/1
6  Router(config-if)#ip address 192.168.15.5 255.255.255.0
7  Router(config-if)#no shutdown
```

2- اجرای OSPF

R1

```
1  Router(config)#router ospf 1
2  Router(config-router)#router-id 1.1.1.1
3  Router(config-router)#network 192.168.12.1 0.0.0.0 area 0
4  Router(config-router)#network 192.168.15.1 0.0.0.0 area 0
5  Router(config-router)#network 192.168.14.1 0.0.0.0 area 0
6  Router(config-router)#
7  00:10:51: %OSPF-5-ADJCHG: Process 1, Nbr 2.2.2.2 on Serial0/0/0 from LOADING to
   FULL, Loading Done

   00:17:13: %OSPF-5-ADJCHG: Process 1, Nbr 4.4.4.4 on Serial0/1/0 from LOADING to
   FULL, Loading Done

   00:20:10: %OSPF-5-ADJCHG: Process 1, Nbr 5.5.5.5 on Serial0/0/1 from LOADING to
   FULL, Loading Done
```

R2

```
1  Router(config)#router ospf 1
2  Router(config-router)#router-id 2.2.2.2
3  Router(config-router)#network 192.168.2.2 0.0.0.0 area 0
4  Router(config-router)#network 192.168.12.2 0.0.0.0 area 0
5  Router(config-router)#network 192.168.23.2 0.0.0.0 area 0
```

```
6  Router(config-router)#
7  00:10:51: %OSPF-5-ADJCHG: Process 1, Nbr 1.1.1.1 on Serial0/0/0 from LOADING to
   FULL, Loading Done

   00:12:27: %OSPF-5-ADJCHG: Process 1, Nbr 3.3.3.3 on Serial0/0/1 from LOADING to
   FULL, Loading Done
```

R3

```
1  Router(config)#router ospf 1
2  Router(config-router)#router-id 3.3.3.3
3  Router(config-router)#network 192.168.23.3 0.0.0.0 area 0
4  Router(config-router)#network 192.168.3.3 0.0.0.0 area 0
5  Router(config-router)#
6  00:12:27: %OSPF-5-ADJCHG: Process 1, Nbr 2.2.2.2 on Serial0/0/1 from LOADING to
   FULL, Loading Done
```

R4

```
1  Router(config)#router ospf 1
2  Router(config-router)#router-id 4.4.4.4
3  Router(config-router)#network 192.168.14.4 0.0.0.0 area 0
4  Router(config-router)#network 192.168.4.4 0.0.0.0 area 0
5  Router(config-router)#
6  00:17:13: %OSPF-5-ADJCHG: Process 1, Nbr 1.1.1.1 on Serial0/1/0 from LOADING to
   FULL, Loading Done
```

R5

```
1  Router(config)#router ospf 1
2  Router(config-router)#router-id 5.5.5.5
3  Router(config-router)#network 192.168.5.5 0.0.0.0 area 0
4  Router(config-router)#network 192.168.15.5 0.0.0.0 area 0
5  Router(config-router)#
6  00:20:10: %OSPF-5-ADJCHG: Process 1, Nbr 1.1.1.1 on Serial0/0/1 from LOADING to
   FULL, Loading Done
```

خروجی تا این مرحله

R1

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

```
Gateway of last resort is not set

O       192.168.2.0/24 [110/65]   via   192.168.12.2,  00:19:16,  Serial0/0/0
O       192.168.3.0/24 [110/129]  via   192.168.12.2,  00:17:30,  Serial0/0/0
O       192.168.4.0/24 [110/65]   via   192.168.14.4,  00:12:54,  Serial0/1/0
O       192.168.5.0/24 [110/65]   via   192.168.15.5,  00:09:57,  Serial0/0/1
C       192.168.12.0/24   is directly  connected,  Serial0/0/0
C       192.168.14.0/24   is directly  connected,  Serial0/1/0
C       192.168.15.0/24   is directly  connected,  Serial0/0/1
O       192.168.23.0/24 [110/128]  via  192.168.12.2,  00:19:16,  Serial0/0/0
```

R1

Router#show ip protocols

```
Routing Protocol is "ospf 1"
    Outgoing update filter list for all interfaces is not set
    Incoming update filter list for all interfaces is not set
    Router  ID  1.1.1.1
    Number of areas in this router is 1. 1 normal 0 stub 0 nssa
    Maximum path: 4
    Routing for Networks:
      192.168.12.1   0.0.0.0   area 0
      192.168.15.1   0.0.0.0   area 0
      192.168.14.1   0.0.0.0   area 0
   Routing Information Sources:
      Gateway         Distance      Last Update
      1.1.1.1              110          00:09:57
      2.2.2.2              110          00:17:34
      3.3.3.3              110          00:17:33
      4.4.4.4              110          00:12:52
      5.5.5.5              110          00:09:57
Distance: (default is 110)
```

R1

Router#show ip ospf neighbor

Neighbor ID	Pri	State	Dead Time	Address	Interface
2.2.2.2	0	FULL/ -	00:00:35	192.168.12.2	Serial0/0/0
5.5.5.5	0	FULL/ -	00:00:36	192.168.15.5	Serial0/0/1
4.4.4.4	0	FULL/ -	00:00:37	192.168.14.4	Serial0/1/0

R1

```
Router#show ip ospf
 Routing Process "ospf 1" with ID 1.1.1.1
 Supports only single TOS(TOS0) routes
 Supports opaque LSA
 SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
 Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
 Number of external LSA 0. Checksum Sum 0x000000
 Number of opaque AS LSA 0. Checksum Sum 0x000000
 Number of DCbitless external and opaque AS LSA 0
 Number of DoNotAge external and opaque AS LSA 0
 Number of areas in this router is 1. 1 normal 0 stub 0 nssa
 External flood list length 0
    Area BACKBONE(0)
       Number of interfaces in this area is 3
       Area has no authentication
       SPF algorithm executed 7 times
       Area ranges are
       Number of LSA 5. Checksum Sum 0x021578
       Number of opaque link LSA 0. Checksum Sum 0x000000
       Number of DCbitless LSA 0
       Number of indication LSA 0
       Number of DoNotAge LSA 0
       Flood list length 0
```

3-اجرای احرازهویت بین R3 با R2 و R1 با R4

R2,R3

```
Router(config)#int s0/0/1
Router(config-if)#ip ospf authentication-key ccna
Router(config-if)#ip ospf authentication message-digest
```

R1,R4

```
Router(config)#int s0/1/0
Router(config-if)#ip ospf authentication-key ccna
Router(config-if)#ip ospf authentication message-digest
```

مشاهده‌ی دستورات احرازهویت با command زیر:

R1

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

Current configuration : 1036 bytes
!
version 12.4
```

```
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Router
!
!
!
!
!
!
interface Serial0/1/0
ip address 192.168.14.1 255.255.255.0
ip ospf authentication message-digest
ip ospf authentication-key ccna
```

EIGRP

ویژگی‌های پروتکل EIGRP:

- مهمترین مشخصه اش، پروتکل اختصاصي شرکت سیسکو است و اگر تجهیزات سیسکو باشد، بهترین عملکرد را دارد.
- پروتکلی با ساختار advanced distance vector می‌باشد.

- VertyFast و Hybrid است.
- پیدایش آن IGRP است که بهبود یافته است (Enhanced IGRP).
- Classless است.
- پیاده‌سازی پروتکل eigrp خیلی ساده است.
- Update:
  - **Full:** اگر تغییري هم نیافته کل جدول مسیریابي را براي اطرافیان ارسال مي‌کند← پهناي باند شبکه را اشغال مي‌کند (در Rip بدین صورت مي‌باشد).
  - **Incremental:** ارسال گزارش تغییرات در زماني اتفاق مي‌افتد که واقعا تغییري بوجود بیاید و فقط تغییرات را ارسال مي‌کند ← پهناي باند کمي را اشغال مي‌کند (در OSPF بدین صورت مي‌باشد).
  - آپدیت‌ها را از طریق IP: 224.0.0.10 (IPی Multicast) ارسال می‌کنند.

- Load Balancing: ساختار Load به ازاي مسیرهاي با ارزشگذاري یکسان و غیریکسان قابل اجراست. مسیرهاي غیر یکسان فقط توسط EIGRP ساپورت مي‌شوند.
- استفاده از Multicast و Unicast به جاي ← Broadcast
- VLSM را ساپورت مي‌کند.
- Summarization را به‌صورت دستی و اتوماتیک انجام مي‌دهد.
- از الگوریتم DUAL[1] استفاده می‌کند.
- متریک:
  - شامل متریک‌های bandwidth، delay، load، reliability و MTU می‌باشد.
  - به صورت پیش فرض از bandwidth و delay استفاده می‌شود.
- دارای Administrative distance برابر 90 می‌باشد.

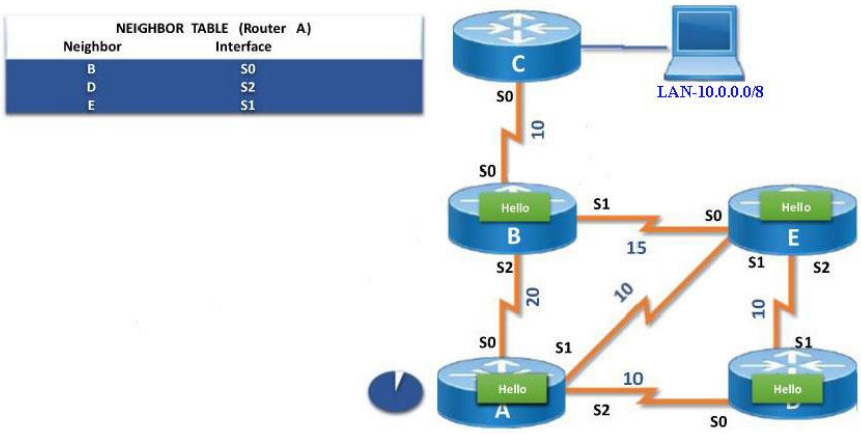
جداول مسیریابي در پروتکل EIGRP

مسیریابی در eigrp ساختار درختی را طی می‌کند. برای اینکه شبکه‌ای در eigrp براساس ساختار درختی مسیریابی بکند باید 3 جدول مسیریابی وجود داشته باشد تا یک routing table به صورت کلی وجود داشته باشد، این 3 جدول عبارتند از:

- **Neighbor Table**

[1] Diffusion Update Algorithm

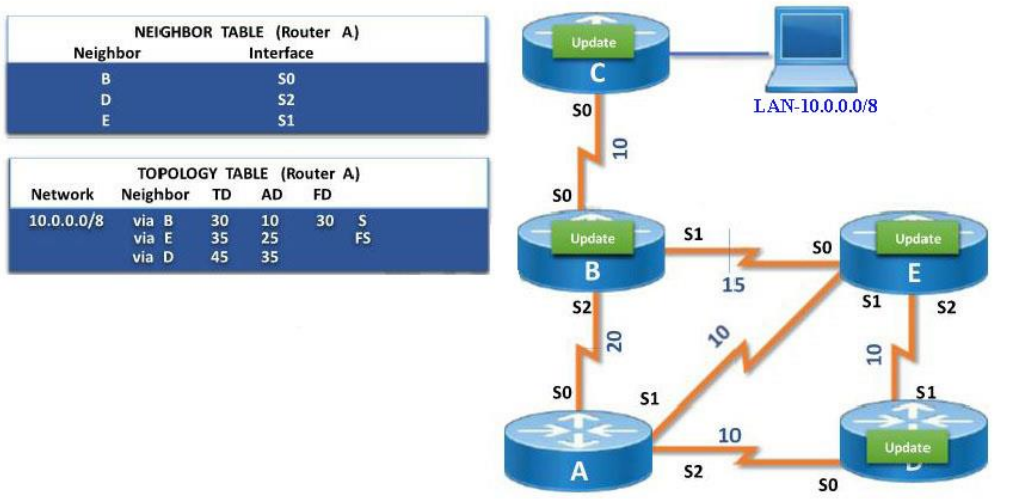
یک روتر برای اینکه در حالت درختی کار کند باید یک جدول همسایگی با نام neighbor table داشته باشد. این جدول شامل لیستی از روترهای همسایه‌ای می‌باشد که پروتکل eigrp را اجرا می‌کنند.



شکل 5-19 Neighbor Table در EIGRP

- **Topology Table**

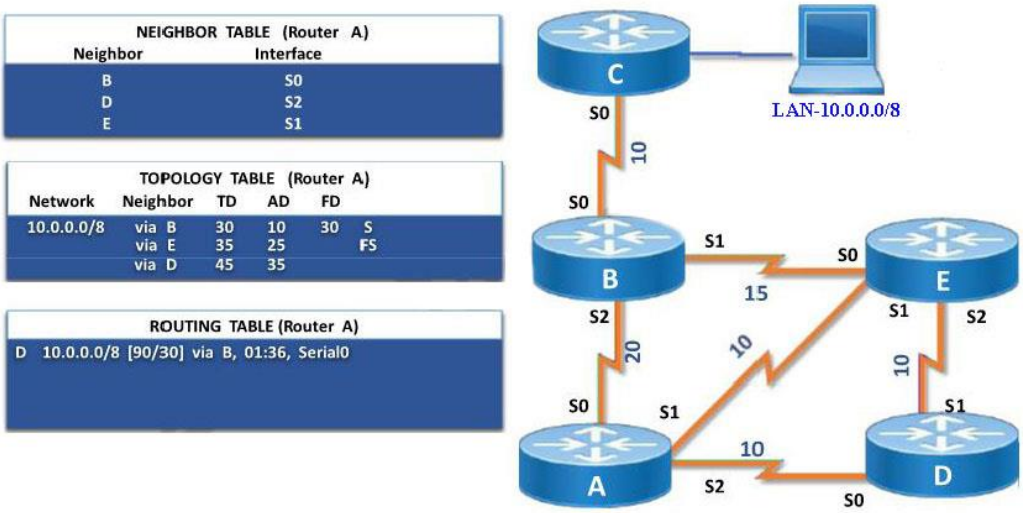
این جدول بعد از به وجود آمدن neighbor table ایجاد می‌شود و شامل تمامی networkهایی در شبکه می‌باشد که یک روتر با ارتباط برقرار کردن از روترهای مجاور به دست‌آورده است. در این جدول بین مسیرهای مختلفی که وجود دارد، مسیری که به عنوان بهترین مسیر انتخاب شود با نام Successor شناخته می‌شود، در واقع این مسیر دارای بهترین متریک می‌باشد. در این جدول علاوه بر مسیرهای Successor ، مسیرهایی با نام Feasible Successor هم وجود دارد، این مسیر backup ای از مسیر Successor می‌باشد تا اگر اتفاقی برای مسیر Successor اتفاق افتاد یا شبکه down شد، جایگزینی برای مسیر Successor باشد، در واقع با این کار اجازه نمی‌دهد شبکه دچار Delay Time بالایی شود.



شکل 5-20 Topology Table در EIGRP

- **Routing Table**

مسیرهای Successor ای که در topology table وجود داشتند در این جدول قرار می‌گیرند.

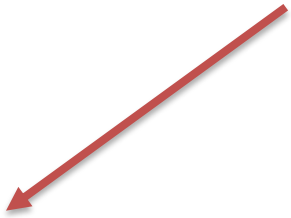


شکل 5-21 Routing Table در EIGRP

IP EIGRP neighbor table	
Next-Hop Router	**Interface**

IP EIGRP topology table	
Destination1	

The IP routing table	
Destination1	



شکل 5-22 ترتیب اجرای جداول در EIGRP

ساختار سلسله مراتبی به‌صورت Step-by-Step توسط 3جدول معرفی شده، به‌وجود می‌آید. همه‌ی کارها به‌صورت اتوماتیک توسط الگوریتم پروتکل EIGRP با نام Dual انجام می‌شود.

:EIGRP Configuration

1	Router(config)# **router eigrp <u>A.S(Autonomous-system)</u>**
2	Router(config-router)#**network <u>net-number</u>/<u>interface-ip wildcard –Mask</u>**

نکات

- در eigrp از مفهوم AS (autonomous-system) استفاده می‌شود. AS ها مجموعه‌ها یا محیط‌هایی هستند که از area ظرفیت پردازش بزرگتری دارند.

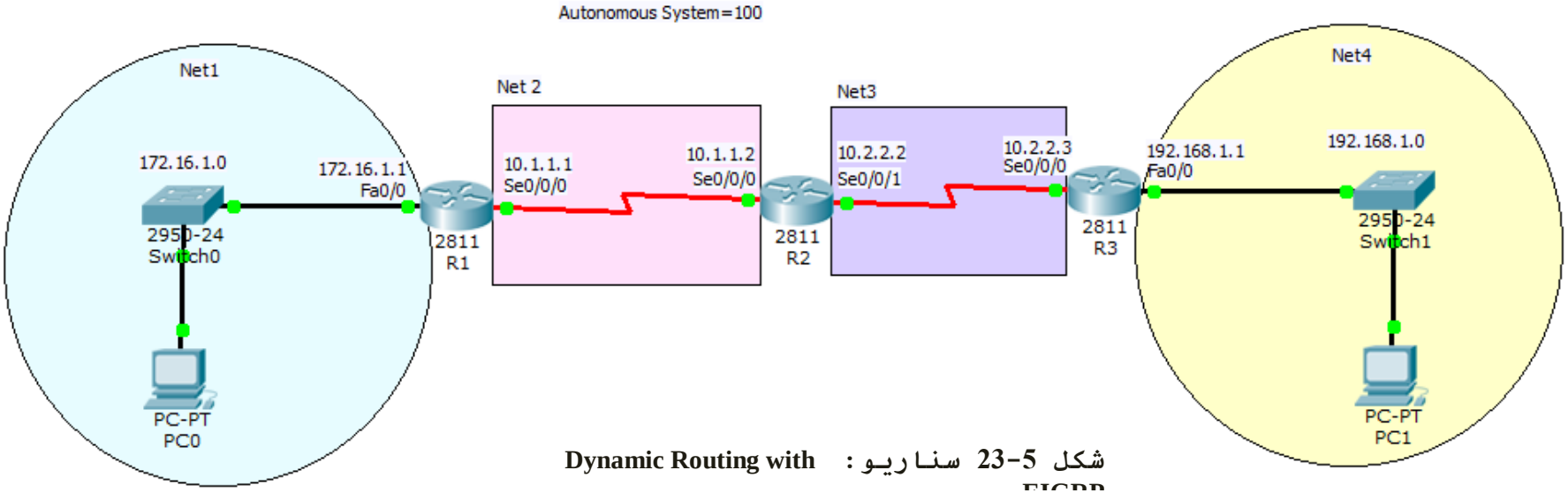
- AS ها با شماره شناسایی می‌شوند.
- محدوده شماره AS ها از 65535-0 می باشد.
  - Public: 1-64511
  - Private: 64512- 65535

دستورات Verify EIGRP

1	Router#**show ip route eigrp**
2	Router#**show ip protocols**
3	Router#**show ip eigrp interfaces**
4	Router#**show ip eigrp neighbors**
5	Router#**show ip eigrp topology**
6	Router#**show ip eigrp traffic**
7	Router#**debug ip eigrp**

- خط1: جدول مسیریابی eigrp را نشان می‌دهد. route های eigrp با "D" نمایش داده می شوند.
- خط2: پروتکل استفاده شده یا enable بودن پروتکل روی روتر را نشان می‌دهد.
- خط3: اینترفیس‌هایی که برای advertise استفاده می‌شود را نشان می‌دهد.
- خط4: این دستور neighbor table را نشان می‌دهد.
- خط5: تمام شبکه‌های موجود را نشان می‌دهد. مسیر Successor با کلمه‌ی "passive" یا "P" نشان داده می‌شود.
- خط6: تعداد و نوع packet هایی که توسط پروتکل رد و بدل می‌شود را نشان می‌دهد.

سناریو : Dynamic Routing with EIGRP



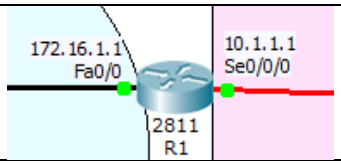
شکل 5-23 سناریو : Dynamic Routing with EIGRP

1-اختصاص IP به اینترفیس‌های روتر

اختصاص IP در سناریوی شکل (5-9) انجام شده است.

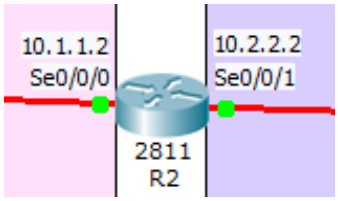
2-اجرای EIGRP

Router 1:

1 2 3	Router(config)#**router eigrp 100** Router(config-router)#**network 172.16.1.1** Router(config-router)#**network 10.1.1.1**	

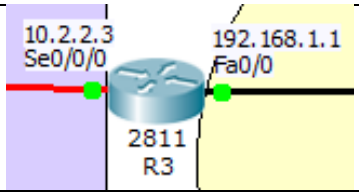
- خط 1: در جلوي EIGRP شماره‌ي A.S را مي‌نويسيم.
- خط 2و 3: IPی، Interfaceهايي كه مستقيما به روتر متصل شده اند را مي‌نويسيم.

Router 2:

1 2 3 4 5 6 7	Router(config)#**router eigrp 100** Router(config-router)#**network 10.1.1.2** Router(config-router)# %DUAL-5-NBRCHANGE: IP-EIGRP 100: Neighbor 10.1.1.1 (Serial0/0/0) is up: new adjacency Router(config-router)#**network 10.2.2.2**	

- خط 4: در صورتي كه پروتكل مسيريابي در دو سر لينك برقرار شود، اين پيغام را مي‌بينيم.

Router 3:

1 2 3	Router(config)#**router eigrp 100** Router(config-router)#**network 10.2.2.3** Router(config-router)#**network 192.168.1.1**	

3-خروجی

R1

```
Router#show ip route eigrp
      10.0.0.0/24 is subnetted, 2 subnets
D        10.2.2.0 [90/2681856] via 10.1.1.2, 00:03:19, Serial0/0/0
      172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
D        172.16.0.0/16 [90/2684416] via 10.1.1.2, 00:03:19, Serial0/0/0
D     192.168.1.0/24 [90/2684416] via 10.1.1.2, 00:03:04, Serial0/0/0
```

R1

```
Router#show ip protocols

Routing Protocol is "eigrp 100 "
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Default networks flagged in outgoing updates
  Default networks accepted from incoming updates
  EIGRP metric weight K1=1, K2=0, K3=1, K4=0, K5=0
  EIGRP maximum hopcount 100
  EIGRP maximum metric variance 1
Redistributing: eigrp 100
  Automatic network summarization is not in effect
  Maximum path: 4
  Routing for Networks:
    172.16.0.0
    10.0.0.0
  Routing Information Sources:
    Gateway         Distance      Last Update
    10.1.1.2              90      755756
  Distance: internal 90 external 170
```

R1

```
Router#show ip eigrp interfaces
IP-EIGRP interfaces for process 100

                   Xmit Queue   Mean   Pacing Time   Multicast    Pending
Interface   Peers  Un/Reliable  SRTT   Un/Reliable   Flow Timer   Routes
Fa0/0         0        0/0     1236       0/10          0           0
Se0/0/0       1        0/0     1236       0/10          0           0
```

R1

```
Router#show ip eigrp neighbors
IP-EIGRP neighbors for process 100
H   Address         Interface       Hold Uptime   SRTT   RTO  Q  Seq
                                    (sec)         (ms)       Cnt Num
0   10.1.1.2        Se0/0/0           13 01:38:02   40   1000  0   8
```

R1

```
Router#show ip eigrp topology
IP-EIGRP Topology Table for AS 100

Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
```

```
r - Reply status

P    10.1.1.0/24, 1 successors, FD is 2169856
          via Connected, S erial0/0/0
P    10.2.2.0/24, 1 successors, FD is 2681856
          via 10.1.1.2 (2681856/2169856), Serial0/0/0
P    172.16.0.0/16, 1 successors, FD is 2684416
          via 10.1.1.2 (2684416/2172416), Serial0/0/0
P    172.16.1.0/24, 1 successors, FD is 28160
          via Connected, FastEthernet0/0
P    192.168.1.0/24, 1 successors, FD is 2684416
          via 10.1.1.2 (2684416/2172416), Serial0/0/0
```

R1

```
Router#show ip eigrp traffic
IP-EIGRP Traffic Statistics for process 100
  Hellos sent/received: 3013/1496
  Updates sent/received: 4/5
  Queries sent/received: 0/0
  Replies sent/received: 0/0
  Acks sent/received: 5/4
  Input queue high water mark 1, 0 drops
  SIA-Queries sent/received: 0/0
  SIA-Replies sent/received: 0/0
```

R1

```
Router#ping 192.168.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 2/2/3 ms
```

Interface-loopback

اینترفیس‌هایی بصورت مجازي هستند و به تعداد نامحدود قابل تعریف‌اند و همواره Up می‌باشند. می‌توانیم به آنها IP اختصاص دهیم.

```
1  Router(config)#interface loopback 1
2  Router(config-if)#ip address  IP  Mask
```

- خط 1: Interface Loopback شماره‌ي 1 را انتخاب کرده‌ایم.
- خط 2: به آن IP اختصاص می‌دهیم.

انواع Packet ها در EIGRP

1- **Hello Packet / Dead time:** يك بازهي زماني 30 ثانيه‌اي است كه روتر اطلاعات را هر 30 ثانيه ارسال مي‌كند. يكي از پكت‌هاي ارسال شده توسط روتر، Hello packet است و روتر انتظار دارد كه روتر مجاور به اين Hello Packet پاسخ دهد، اگر بعد از 4 بار ارسال، روترهاي مجاور پاسخ ندهند، روتر اصلي (كه پكت را ارسال كرده) روتر مقابل را از جدول مسيريابي خودش حذف مي‌كند.

2- **Update Packet:** پكت‌هايي كه در جهت آپديت كردن شبكه است. هر تغييری افتاد روتر بايد شبكه را نسبت به تغييراتی كه پيش آمده، آپديت كند.

3- **Query:** دريافت اطلاعات جديد توسط روتر به نسبت روترهای بعدی توسط اين نوع packet انجام می‌شود.

4- **Reply:** جواب پكت Query است.

5- **Ack:** تصديق دريافت اطلاعات در مقصد داده توسط اين packet انجام می‌شود (در پروتكل های TCP اتفاق می‌افتد).

تمامی پروتكل‌های اصلی شبكه به دليل حفظ reliability و اطمينان از سالم رسيدن Data به مقصد دارای ساختار TCP base هستند ولی چون ACK در شبكه وجود دارد، سرعت تبادل اطلاعات كاهش پيدا خواهد كرد، به اين دليل كه هر ارسال و دريافتی منتظر يک ACK جديد خواهد بود به همين خاطر تا ACK دريافت نشود، بقيه‌ی داده‌ها ارسال نخواهد شد. EIGRP و OSPF از زير ساخت TCP برای ارتباطات استفاده می‌كنند.

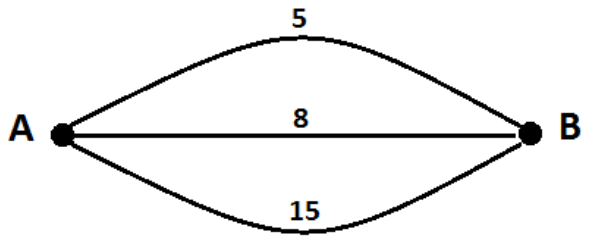
EIGRP Load Balancing

Loadbalancing در EIGRP به دو صورت انجام می‌شود:

1- مسیرهای با متریک یکسان (ارزشگذاری یکسان): تا چهار مسیر را می‌تواند بصورت اتوماتیک Load Balance کند و خودمان می‌توانیم تا 16 مسیر را Load Balance کنیم. از طریق دستور Maximum-Paths می‌توانیم مقدار مورد نظرمان را وارد کنیم.

```
Router(config-router)# maximum-paths 16
```

2- مسیرهای با متریک غیریکسان (ارزشگذاری غیریکسان):
Loadbalancing در مسیرهای غیریکسان فقط در پروتکل EIGRP انجام می‌شود و Command آن فقط در این پروتکل وجود دارد. Loadbalancing در مسیرهای غیریکسان می‌تواند با استفاده از "variance" کانفیگ شود (مقدار variance به‌صورت پیش فرض برابر 1 می‌باشد).
مثلا: اگر بیش از یک مسیر با اعداد متریک 5و8و15 وجود داشته باشد، به صورت پیش فرض بهترین مسیر براي رسیدن از A به B، مسیر با متریک کوچکتر است یعني 5.
در صورتي‌که ترافیک زیاد شود، تنها مسیر 5 از عهده‌ي عبور اطلاعات بر نمي‌آید، بنابراین باید با انجام محاسبات از مسیرهاي دیگر نیز استفاده شود.



اگر بخواهیم بین دو یا چند مسیر Loadbalancing با متریک‌های غیریکسان انجام دهیم، بین مسیرها بین بدترین و بهترین متریک یک نسبت تناسب می‌گیریم، سپس عدد را به یک عدد تقریبی گرد می‌کنیم. عدد تقریبی به‌دست‌آمده را به عنوانvariance وارد می‌کنیم.

$$Multipier = \frac{\text{بزرگترین متریک}}{\text{کوچکترین متریک}}$$

کانفیگ variance

```
1  R(config)#router eigrp AS
2  R(config-router)#variance <Multipier>
```

EIGRP Authentication

دو Step اصلي وجود دارد و لزوماً از MD5 استفاده مي‌كند (حتما رمزنگاري مي‌كند).

1- تعريف كردن پسورد با Key Chain

Key chain دسته كليدي است كه يك كليد Select مي‌شود و به آن كليد يك پسورد اختصاص مي‌دهيم.

```
1  Router(Config)#key chain name-of-chain
2  Router(Config-keyChain)#key key-ID
3  Router(Config-keyChain-key)#key-string text
4  Router(Config-keychain-key)#accept-lifetime  start-time{infinit|end-time|duration-
5  second}
6  Router(Config-keychain-key)#send-lifetime  start-time{infinit|end-time|duration-
7  second}
```

- خط 1: تعريف يک نام براى Key chain
- خط 2: انتخاب يک كليد از بين دسته كليد
- خط3: تعريف پسورد براى كليد انتخاب شده
- خط 4: يعني بازه زماني كه در آن كليد از روتر مجاور دريافت شود. (اين خط الزامي نيست)
- خط 6: بازه زماني است كه در آن كليد براي روتر مجاور ارسال مي‌شود. (اين خط الزامي نيست)
  - **Infinit** ← زمان نامعلوم است
  - **End-time** ←راس ساعتي كه تمام مي‌شود.
  - **Duration** ← بازه‌ي زماني تعريف مي‌شود.

2- مكانيزم ارسال كليد:

استفاده از كليدهاي دريافت شده براي ارسال در شبكه.

```
1  Router(Config-if)#ip authentication mode eigrp autonomous-system md5
2  Router(Config-if)# ip authentication key-chain eigrp autonomous-system name-of-chain
```

```
Keychain test
    Key-id 1
        Key-string 123
            Accept-lifetime 04:00:00 Jan 12006 infinites
```

جهت پياده‌سازي EIGRP Authentication بايد از نرم افزار Gns3.net استفاده شود.

EIGRP Summarization

دستور Summary در EIGRP

1	R(config-if)#**ip summary-address eigrp *AS#* *summary-ip* *summary-mask***

Redistribution

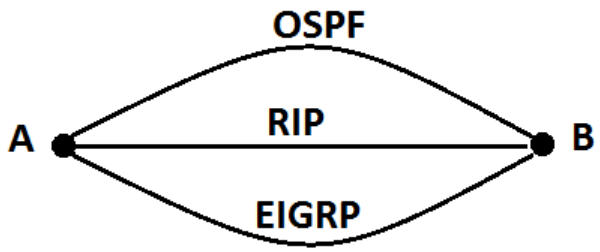
اگر شبکه هایی وجود داشتند که ترکیبی از پروتکل‌های مختلف بودند از مفهوم Redistribution استفاده می‌شود. قبل از اینکه به مفهوم Redistribution بپردازیم باید با Administrative Distance آشنا شویم.

Administrative Distance

Administrative Distance به 2 صورت زیر تعریف می گردد:

1- Internal
2- External

همان طوری که قبلا ذکر شد، پروتکل rip، ospf و eigrp جزء پروتکل‌های Internal و پروتکل bgp جزء پروتکل‌های External می‌باشد. اگر یک پروتکل کلا به‌صورت Internal کار کند از نظر Administrative دارای مقدار 120 (rip)، 110 (ospf) و 90 (eigrp) می‌باشد و برای Internal bgp دارای مقدار 200 است. به این دلیل برای Internal bgp عدد بزرگتری می‌باشد چون bgp یک پروتکل External است. برای rip و ospf ، External تعریف نشده است ولی برای External eigrp برابر 170 می‌باشد. در حالت External، ترافیک از یک محدوده‌ی دیگری وارد محدوده‌ی مورد نظر می‌شود. برای مثال اگر شبکه‌ای وجود داشته باشد که با پروتکل ospf راه اندازی شود و خارج از شبکه ترافیک دیگری وارد این شبکه شود (مثلا پروتکل eigrp)، External محسوب می‌شود (پروتکل eigrp، External حساب می‌شود).
اگر بخواهیم از این پروتکل‌ها در شبکه‌ای استفاده کنیم، اولویت‌دهی پروتکل‌ها را با این اعداد مشخص می‌کنیم. Administrative هرکدام‌یک از پروتکل‌ها کمتر باشد، اولویت دهی بیشتری برای مسیریابی دارد. برای مثال در شکل زیر اگر از نقطه‌ی A به B مسیرهای مختلفی با پروتکل های مختلف وجود داشته باشد، به جای اینکه از همه‌ی مسیرها استفاده شود بین مسیرها مقایسه انجام می شود و پروتکلی که دارای Administrative کمتری باشد، آن مسیر را انتخاب می‌کند. در این شکل چون Administrative پروتکل eigrp از بقیه کمتر بوده آن مسیر را انتخاب می‌کند.



Rip 120
OSPF 110
EIGRP 90

هر چقدر عدد کوچکتر باشد↓، اولویت بیشتر است↑.

جدول 5-4 مقادیر AD برای پروتکل‌های مسیریابی

Routing Protocol	Administrative Distance Value
Connected interface	**0**
Static route out an interface	**1**
Static route to a next-hop address	**1**
EIGRP Summary route	**5**
External BGP	**20**
Internal EIGRP	**90**
IGRP	**100**
OSPF	**110**
IS-IS	**115**
Ripv1, Ripv2	**120**
EGP	**140**
On-Demand Routing(ODR)	**160**
External EIGRP	**170**
Internal BGP	**200**
Unknown	**255**

همیشه در یک شبکه، route هایی‌که داخل آن شبکه هستند، اولویت بیشتری نسبت به آن route هایی که از خارج از شبکه می‌آیند، دارند.

حال برای تشریح redistribution فرض کنید که یک روتری وجود دارد که یک سمتش یک پروتکل(مثلا ospf) و سمت دیگرش پروتکل دیگری(مثلا eigrp) باشد، در این‌صورت سیستم هایی که در هر دو طرف وجود دارند، نمی توانند همدیگر را ping کنند چون پروتکل مسیریابی آن‌ها متفاوت

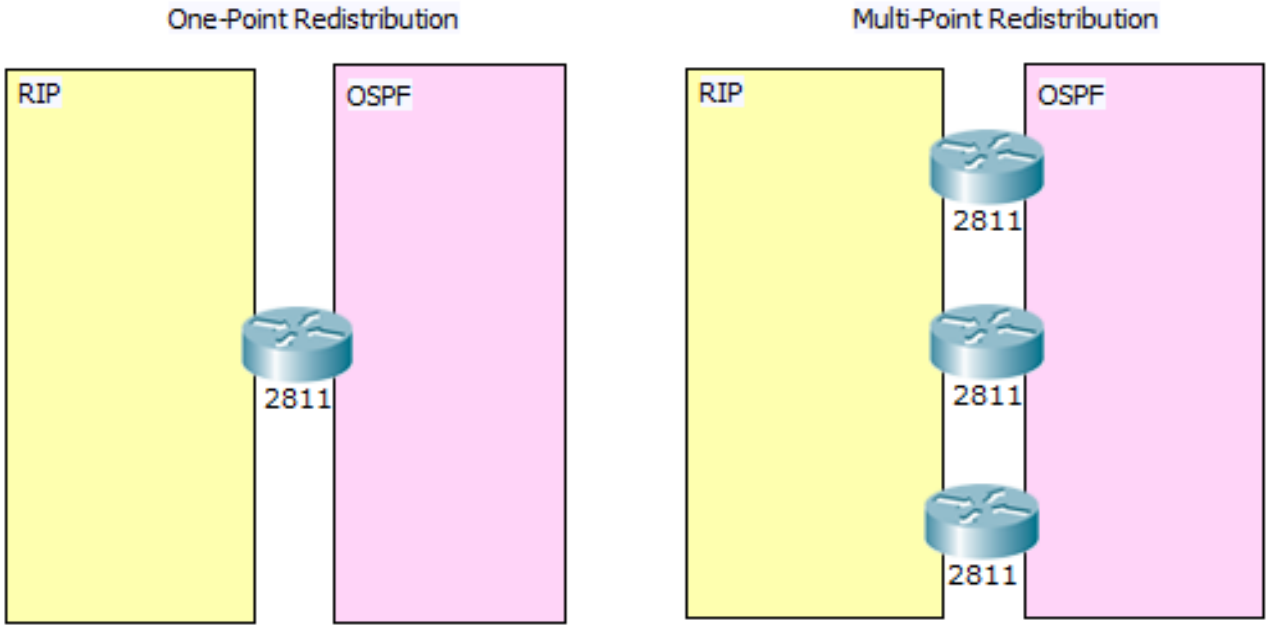
می‌باشد، اما اگر در روتر مرزی عمل redistribution انجام شود، آن موقع سیستم ها همدیگر را ping خواهند کرد.

Redistribution در حالت کلی به 2 دسته تقسیم می‌شود:

1- **One-point redistribution:** یک روتر وجود دارد.

2- **Multi-point redistribution:** چندین روتر وجود دارد که عمل redistribution در نقاط مختلف بر روی آن ها انجام می‌شود.

در اینجا one-point redistribution مد نظر است.

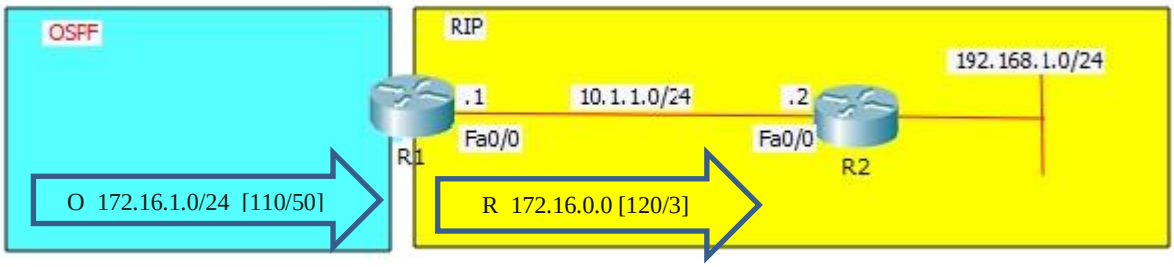


شکل 5-24 حالات مختلف Redistribution

انجام redistribution در پروتکل rip

یعنی یک پروتکلی همانند eigrp و ospf وجود دارد که می‌خواهد ترافیکش را به داخل شبکه‌ای که دارای پروتکل rip می‌باشد، بفرستد.

1	Router(Config-router)# **redistribiution Protocol [process-id] [Metric metric-value]**

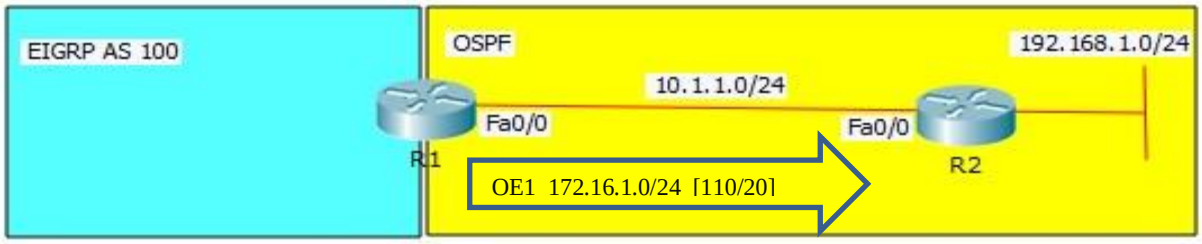


شکل 5-25 Redistribution در RIP

1	Router(config)#**router rip**
2	Router(config-router)#**redistribute ospf 1 metric 3**

انجام redistribution در پروتکل OSPF

1	Router(Config-router)# **redistribiution <u>Protocol</u> [process-id] [Metric <u>metric-value</u>] [subnets]**



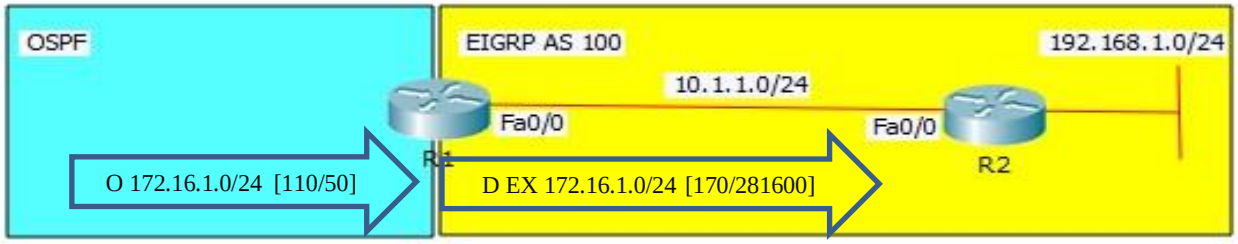
شکل 5-26 Redistribution در OSPF

1	Router(config)#**router ospf 1**
2	Router(config-router)#**redistribute eigrp 100 metric 10 subnets**

نوشتن subnets در دستور بالا الزامی است چون پروتکل ospf به‌صورت classless کار می‌کند در صورتی که subnets به کار برده نشود فقط classful را advertise می‌کند.

انجام redistribution در پروتکل EIGRP

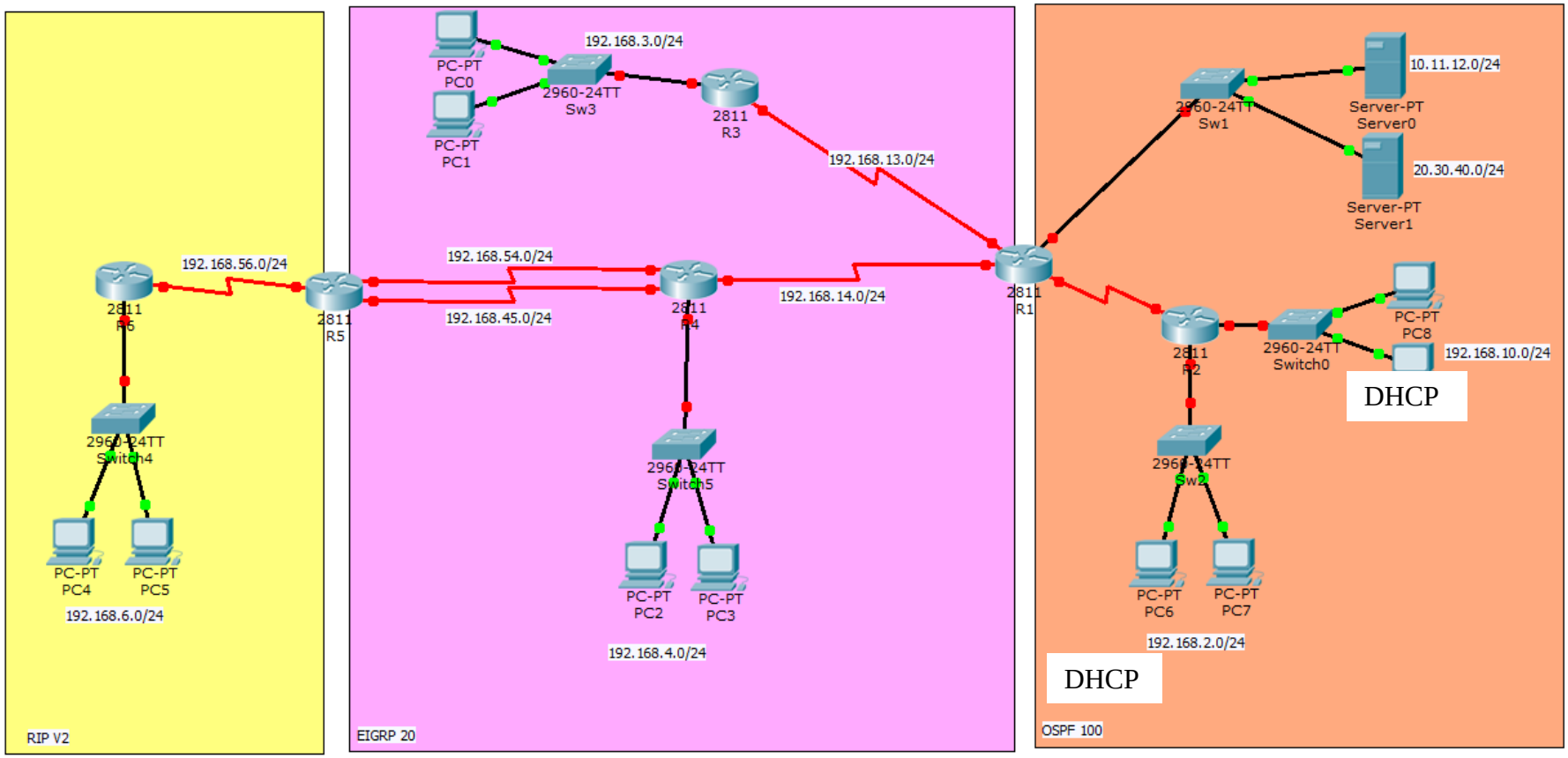
1	Router(Config-router)# **redistribiution Protocol [process-id] [Metric metric-value]**



شکل 5-27 Redistribution در EIGRP

1	Router(config)#**router eigrp 100**
2	Router(config-router)#**redistribute ospf 1 metric 10000 100 255 1 1500**

سنـاريـو (IP-DHCP-RIP-EIGRP-OSPF-Redistribution)

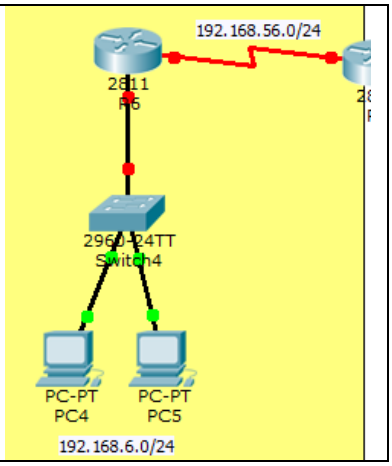


شكل5-28 سنـاريـو IP-DHCP-RIP-EIGRP-OSPF-Redistribution

1- اختصاص IP به Interface هاي روترها

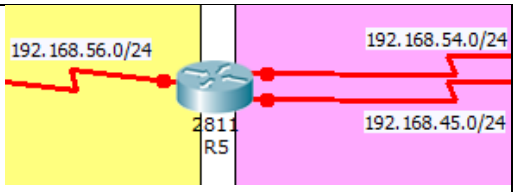
R6

```
1  Router>en
2  Router#conf t
3  Router(config)#interface fastEthernet 0/0
4  Router(config-if)#ip address 192.168.6.1 255.255.255.0
5  Router(config-if)#no shutdown
6
7  Router(config)#interface serial 0/0/0
8  Router(config-if)#ip address 192.168.56.2 255.255.255.0
9  Router(config-if)#no shutdown
10
```



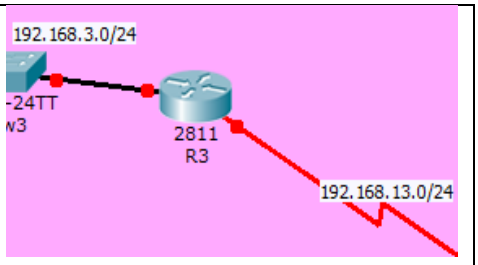
R5

```
1  Router(config)#interface serial 0/2/0
2  Router(config-if)#ip address 192.168.56.1 255.255.255.0
3  Router(config-if)#clock rate 64000
4  Router(config-if)#no shutdown
5
6  Router(config)#interface serial 0/0/0
7  Router(config-if)#ip address 192.168.54.1 255.255.255.0
8  Router(config-if)#clock rate 64000
9  Router(config-if)#no shutdown
10
11 Router(config)#interface serial 0/0/1
12 Router(config-if)#ip address 192.168.45.1 255.255.255.0
13 Router(config-if)#clock rate 64000
14 Router(config-if)#no shutdown
```



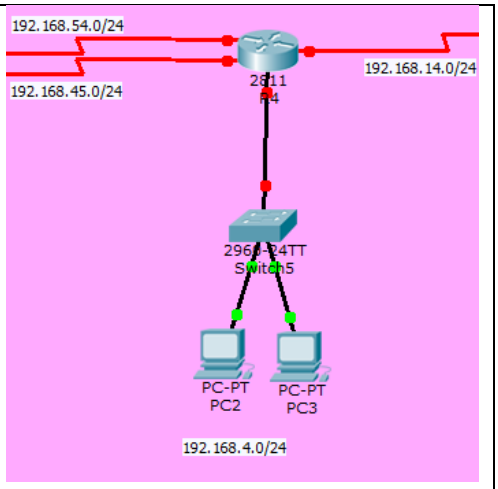
R3

```
1  Router(config)#interface fastEthernet 0/0
2  Router(config-if)#ip address 192.168.3.1 255.255.255.0
3  Router(config-if)#no shutdown
4
5  Router(config)#interface serial 0/0/0
6  Router(config-if)#ip address 192.168.13.1
7  255.255.255.0
8  Router(config-if)#clock rate 64000
   Router(config-if)#no shutdown
```



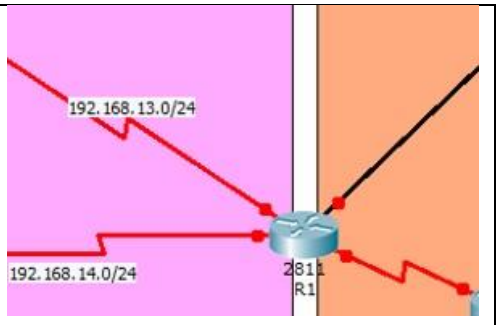
R4

1	Router(config)#**interface serial 0/0/0**
2	Router(config-if)#**ip address 192.168.54.2 255.255.255.0**
3	Router(config-if)#**no shutdown**
4	
5	Router(config)#**interface serial 0/0/1**
6	Router(config-if)#**ip address 192.168.45.2 255.255.255.0**
7	Router(config-if)#**no shutdown**
8	
9	Router(config)#**interface serial 0/2/0**
10	Router(config-if)#**ip address 192.168.14.1 255.255.255.0**
11	Router(config-if)#**clock rate 64000**
12	Router(config-if)#**no shutdown**
13	
14	Router(config)#**interface fastEthernet 0/0**
15	Router(config-if)#**ip address 192.168.4.1 255.255.255.0**
16	Router(config-if)#**no shutdown**



R1:

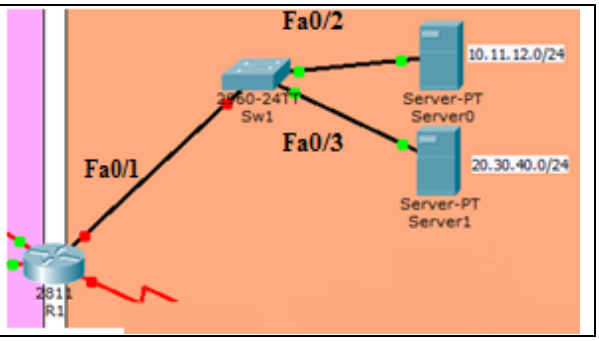
1	Router(config)#**interface serial 0/0/0**
2	Router(config-if)#**ip address 192.168.14.2 255.255.255.0**
3	Router(config-if)#**no shutdown**
4	
5	Router(config)#**interface serial 0/2/0**
6	Router(config-if)#**ip address 192.168.13.2 255.255.255.0**
7	Router(config-if)#**no shutdown**
8	
9	Router(config)#**interface serial 0/0/1**
10	Router(config-if)#**ip address 192.168.12.1 255.255.255.0**
11	Router(config-if)#**clock rate 64000**
12	Router(config-if)#**no shutdown**
13	



2- حال براي ادامه‌ي كار و تعريف دو رنج IP مختلف روي سوئيچ بايد روي سوئيچ دو Vlan بسازيم :

Sw1

1	Switch>**en**
2	Switch#**conf t**
3	Switch(config)#**vlan 10**
4	Switch(config-vlan)#**vlan 20**
5	
6	Switch(config)# **interface fastEthernet 0/2**
7	Switch(config-if)#**switchport mode access**
8	Switch(config-if)#**switchport access vlan 10**

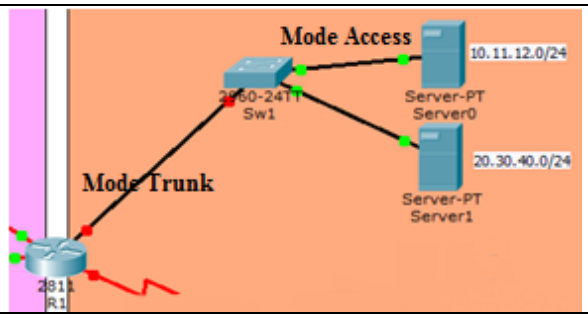


- خط 3و 4 : تعريف Vlan

- خط 6: قرار دادن interface fastEthernet 0/2 در VLAN10

Sw1

```
1  Switch(config)#interface fastEthernet 0/3
2  Switch(config-if)#switchport mode access
3  Switch(config-if)#switchport access vlan 20
4
5  Switch(config)#interface fastEthernet 0/1
6  Switch(config-if)#switchport mode trunk
```



- خط 1-3: قرار دادن interface fastEthernet 0/3 در VLAN20
- خط 5-6: حال باید در سوئیچ، پورتي که به روتر متصل شده است را Trunk تعریف کنیم:

سپس باید به پورت‌هاي مورد نظر IP اختصاص دهیم:

R1:

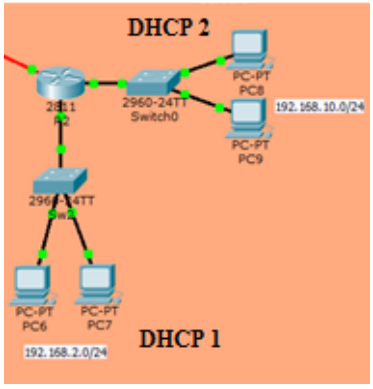
```
1  Router(config)#interface fastEthernet 0/0.1
2  Router(config-subif)#encapsulation dot1Q 10
3  Router(config-subif)#ip address 10.11.12.1 255.255.255.0
4
5  Router(config)#interface fastEthernet 0/0.2
6  Router(config-subif)#encapsulation dot1Q 20
7  Router(config-subif)#ip address 20.30.40.1 255.255.255.0
8
9  Router(config)#interface fastEthernet 0/0
10 Router(config-if)#no shutdown
11 Router(config-if)#
12 %LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up
13 %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to
14 up
15 %LINK-5-CHANGED: Interface FastEthernet0/0.1, changed state to up
16 %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0.1, changed state
17 to up
18 %LINK-5-CHANGED: Interface FastEthernet0/0.2, changed state to up
   %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0.2, changed state
   to up
```

- خط 1-3: اختصاص IP به پورت مجازي که به سرور اولي متصل شده است.
- خط 5-7: اختصاص IP به پورت مجازي که به سرور دوم متصل شده است.

- خط 10: توجه: براي فعال کردن پورت حتما باید کامند no sh را بر روي پورت اصلي بزنيم.

R2

1	Router(config)#**interface serial 0/0/0**
2	Router(config-if)#**ip address 192.168.12.2 255.255.255.0**
3	Router(config-if)#**no shutdown**
4	
5	Router(config-if)#**int fa0/1**
6	Router(config-if)#**ip address 192.168.10.1 255.255.255.0**
7	Router(config-if)#**no shutdown**
8	
9	Router(config)#**ip dhcp pool test**
10	Router(dhcp-config)#**network 192.168.2.2 255.255.255.0**
11	Router(dhcp-config)#**default-router 192.168.2.1**
12	
13	Router(config)#**interface fastEthernet 0/1**
14	Router(config-if)#**ip address 192.168.10.1 255.255.255.0**
15	Router(config-if)#**no sh**
16	
17	Router(config)#**ip dhcp pool test2**
18	Router(dhcp-config)#**network 192.168.10.2**
19	**255.255.255.0**
20	Router(dhcp-config)#**default-router 192.168.10.1**



- خط 9: راه اندازي DHCP 1.
- خط 17: راه اندازي DHCP 2

3- راه اندازي پروتكل‌هاي مسيريابي بر روي روترها

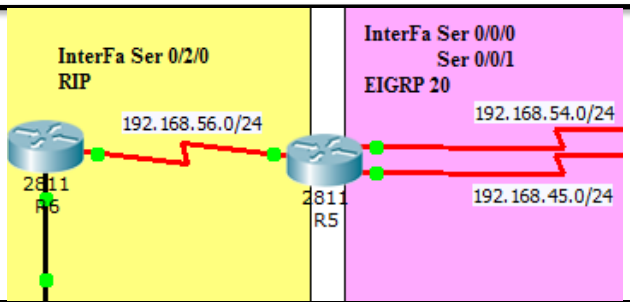
R6:

1	Router(config)#**router rip**
2	Router(config-router)#**version 2**
3	Router(config-router)#**network 192.168.6.0**
4	Router(config-router)#**network 192.168.56.0**

روتر R5 يك پورت آن در بخش پروتكل RIP قرار دارد و دو پورت ديگر آن در پروتكل EIGRP كه بايد به صورت زير تعريف شود:

R5:

```
1  Router(config)#router rip
2  Router(config-router)#version 2
3  Router(config-router)#network 192.168.56.0
4
5  Router(config)#router eigrp 20
6  Router(config-router)#network 192.168.54.0
7  Router(config-router)#network 192.168.45.0
```



- خط 1و2و3: یك Interface روتر R5 داخل RIP است.
- خط 5و6و7: دو Interface دیگر آن در EIGRP است.

R4:

```
1  Router(config)#router eigrp 20
2  Router(config-router)#network 192.168.54.0
3  Router(config-router)#network 192.168.45.0
4  Router(config-router)#network 192.168.4.0
5  Router(config-router)#network 192.168.14.0
```

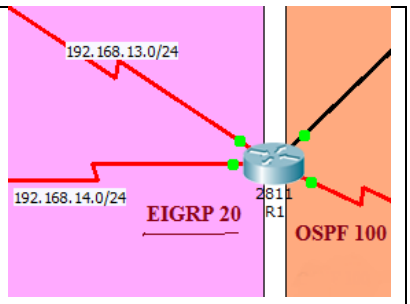
R3

```
1  Router(config)#router eigrp 20
2  Router(config-router)#network 192.168.13.0
3  Router(config-router)#network 192.168.3.0
```

روتر 1 نیز مانند روتر 5، در مرز دو پروتکل مسیریابي قرار دارد که بصورت زیر config مي‌گردد:

R3:

```
1  Router(config)#router eigrp 20
2  Router(config-router)#network 192.168.13.0
3  Router(config-router)#network 192.168.14.0
4
5  Router(config)#router ospf 1
6  Router(config-router)#network 192.168.12.1 0.0.0.0 area
7  100
8  Router(config-router)#network 10.11.12.0 0.0.0.255 area
   100
   Router(config-router)#network 20.30.40.0 0.0.0.255 area
   100
```



R2:

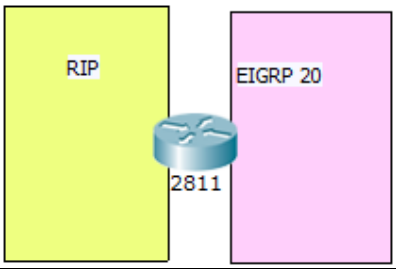
```
1  Router(config)#router ospf 1
2  Router(config-router)#network 192.168.12.2 0.0.0.0 area 100
3  Router(config-router)#network 192.168.2.1 0.0.0.0 area 100
4  Router(config-router)#network 192.168.10.1 0.0.0.0 area 100
```

4- کانفیگ روترهای مرزی که بین دو پروتکل مسیریابی مختلف قرار دارند: **Redistribution**

حالت اول: Redistribution روتر بین پروتکل‌های مسیریابی RIP و EIGRP:

R5:

```
1  Router(config)#router rip
2  Router(config-router)#redistribute eigrp 20 metric 1
3
4  Router(config)#router eigrp 20
5  Router(config-router)#redistribute rip metric 1 1 1
   1 1
```

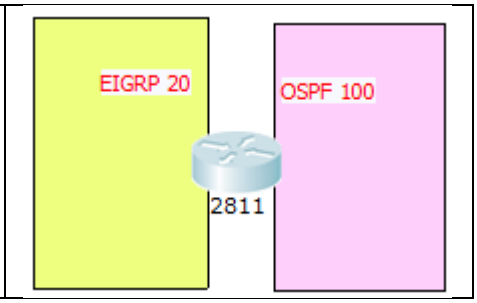


- خط 1و 2: راه اندازي پروتكل‌هاي redistribute داخل پروتكل RIP
- خط 4و5: راه اندازي پروتكل‌هاي redistribute داخل پروتكل EIGRP

حالت دوم: Redistribution روتر بین پروتکل‌های مسیریابی OSPF و EIGRP

R1:

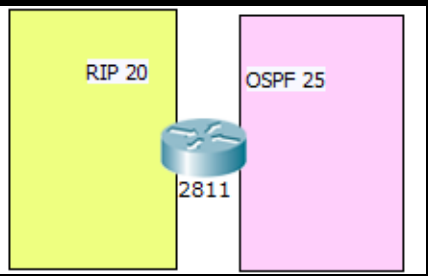
```
1  Router(config)#router eigrp 20
2  Router(config-router)#redistribute ospf 1 metric 1 1 1 1 1
3
4  Router(config)#router ospf 1
5  Router(config-router)#redistribute eigrp 20 metric 1
   subnets
```



- خط 1و2: راه اندازي پروتكل redistribute داخل پروتكل EIGRP.
- خط 4و5: راه اندازي پروتكل redistribute داخل پروتكل OSPF.

حالت سوم: Redistribution روتر بین پروتکل‌های مسیریابی RIP و OSPF:

```
1  Router(config)#router rip
2  Router(config-router)#redistribute ospf 1 metric 1
3
4  Router(config)#router ospf 1
5  Router(config-router)#redistribute rip metric 1 subnets
```



Defualt Route-3

- Default Route اجازه‌ی ارسال ترافیک بدون نیاز به یک مسیر خاص برای یک شبکه خاص را می‌دهد.
- در جدول مسیریابی به‌صورت ***S**** نمایش داده می‌شود.

دستور Default Route

1	R(config)#**ip route 0.0.0.0 0.0.0.0**

فصل 6

ACL

ACL[1]:

- ACL امنیت شبکه را فراهم می‌کند.
- امنیت لایه 3 و لایه 4 را فراهم می‌کند.
- جریان ترافیک از یک شبکه به شبکه‌ی دیگر را کنترل می‌کند.
- پکت‌های IP را فیلتر می‌کند.

هدف از انجام ACL

1- Classification: طبقه‌بندی پروتکل‌ها و ارتباطات از نوع‌ها و دسته‌های مختلف، یعنی ارتباطاتی که مبنا بر TCP، UDP، ICMP و... دارند (طبقه‌بندی ترافیک‌های مختلف شبکه است).
2- Filtering: بعد از اینکه یک ترافیک شناخته می‌شود از این پس می‌توان فیلتر را پیاده‌سازی کرد (چه فیلتر خوب چه فیلتر بد) با کنترل سطح دسترسی سروکار داریم.
یک سری ترافیک Select می‌کنیم بر حسب نیاز فیلتر می‌کنیم.

انواع ACL

1- Standard ACL
فیلترینگ را به ازای مبداء[2] شبکه انجام می‌دهند. از همان مبداء ترافیک را فیلتر می‌کند. یعنی اگر از یک مبدا در شبکه ترافیک خواست عبور کند در همان مبدا فیلتر می‌شود و اجازه نمی‌دهد داده وارد شبکه شود.

2- Extended ACL
با گسترش شبکه‌ها، دیگر فیلترینگ فقط به ازای مبداء مفهومی نداشت چون ممکن بود داده‌ای که از مبداء شبکه می‌آید نیاز به دسترسی به یک سیستم خاص نداشته باشد ولی سیستم‌های دیگر نیاز به اطلاعات آن مبداء داشته باشند، به همین خاطر اگر در نقطه‌ی ابتدایی از بین برده می‌شد باعث به وجود آمدن مشکل می‌شد، بنابراین استفاده از Extended ACL به وجود آمد. در این حالت فیلترینگ یا کنترل دسترسی به ازای یک مبداء به یک مقصد[3] خاص انجام می شود (فیلتر بر مبنای مبدا و مقصد را گویند).

[1] Access Control List
[2] source
[3] Destination

طریقه ی نگارش ACL:

1- شماره ی ACL (ACL Number)

$ACL\ Number: \begin{cases} 1-99 \\ 1300-1999 \end{cases}$ → Standard

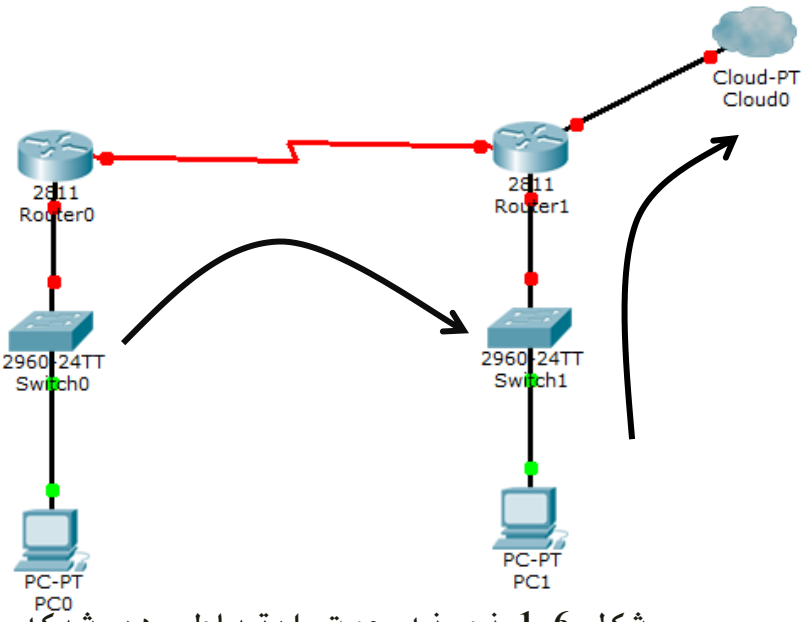
$\begin{cases} 100-199 \\ 200-2699 \end{cases}$ → Extended

2- اسم ACL (ACL Name)

$ACL\ Name$: نام مورد نظر

نکات مهم پیاده سازی ACL

1- به ازای هر Interface ، هر پروتکل و هر جهت ارتباطی در شبکه فقط یک ACL قابلیت پیاده‌سازی دارد.



شکل 6-1 نمونه جهت ارتباطی در شبکه

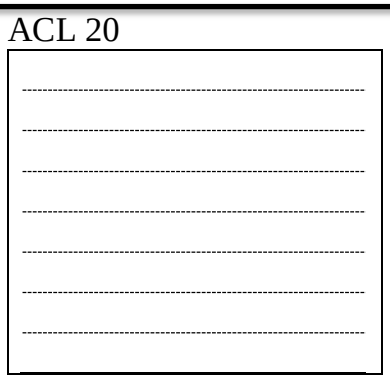
a. PC0 به PC1 دسترسی نداشته باشد.
b. PC1 به اینترنت دسترسی نداشته باشد.

منظور از جهت ← Source به Destination است.
چون مبدا به مقصد این دو تفاوت دارند، باید دو ACL بنویسیم.

	Source		Destination
1.	PC0	↛	PC1
2.	PC1	↛	Internet

3- در نوشتن ACL ها اولویت‌بندی حائز اهمیت می‌باشد، بدین جهت ACL هائیکه در ابتدا نوشته شوند، در ابتدا نیز اجرا می‌گردد.

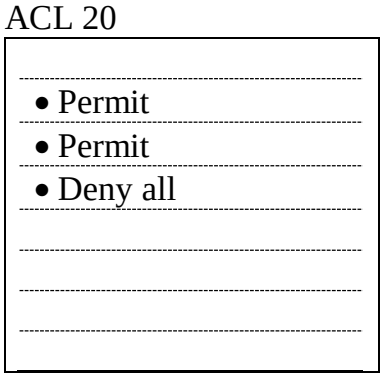
اگر چند خط دستور باشد ← ابتدا خطهای اول را اجرا می‌کند.
اولویت خط 1 بالاتر از خطوط پایین‌تر است.



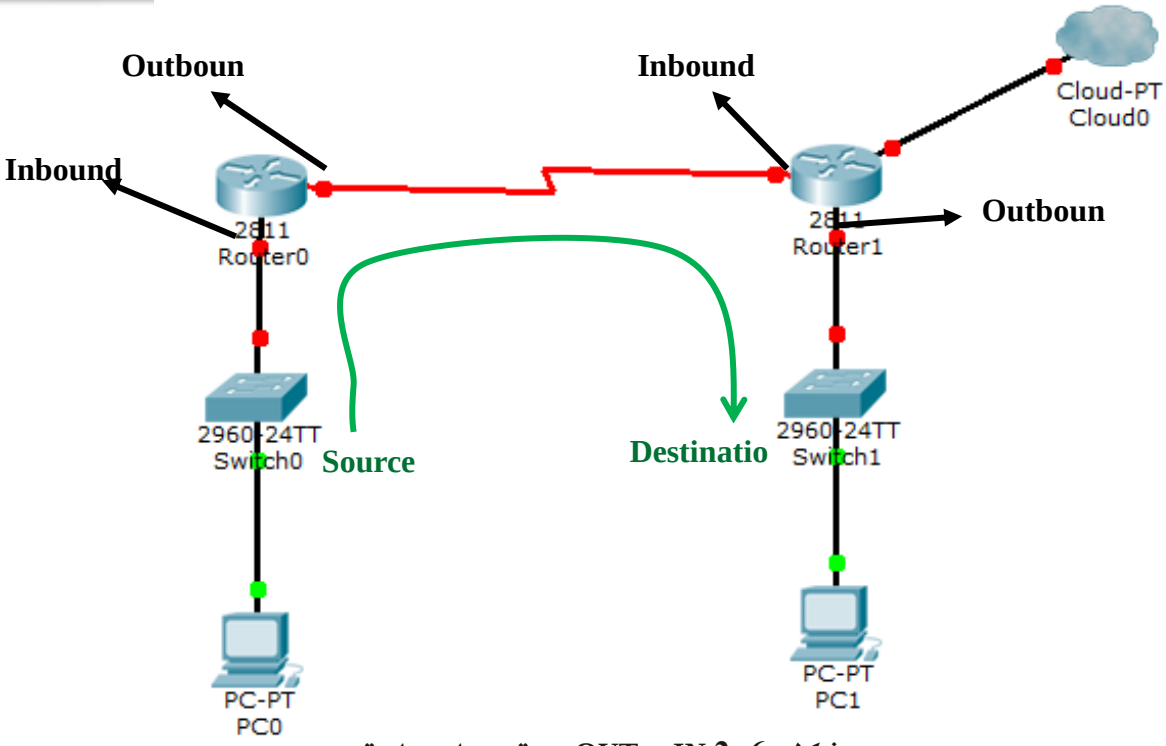
4- مکانیزم عملکرد ACL ها بصورت Implicit Deny All می‌باشد. بدین جهت دسترسی‌های مورد نیاز باید در ابتدا معرفی شود.

که دو حالت دارد:
- Permit
- Deny

- مبنا را بر اساس deny قرار می‌دهیم.
- سپس آنهائیکه می‌خواهیم باز باشد را، باز می‌کنیم. (هر چیزی که نیاز داریم را باز می‌کنیم).



5- نوشتن ACL ها در مد Config انجام می‌شود، اما اعمال آن‌ها به Interface های روتر در حالت Inbound و یا Outbound قابل اجراست.



شکل 6-2 IN و OUT روترها با توجه

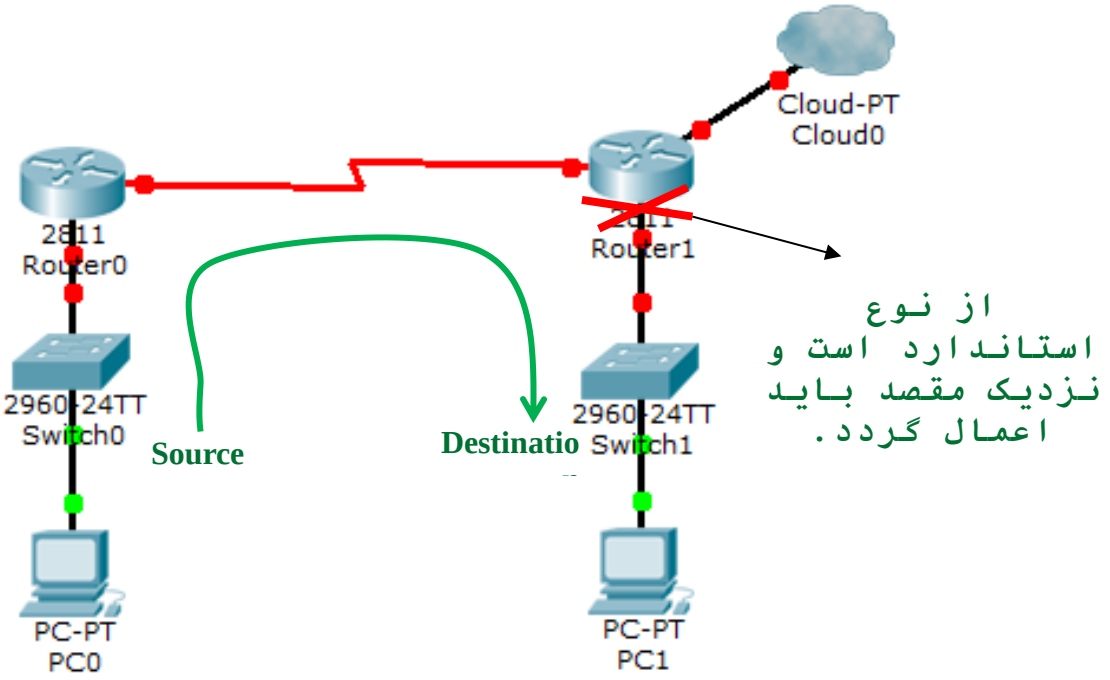
از مبدا به مقصد حرکت می‌کنیم و هر Interface ای که در جهت حرکت ما به روتر وارد شود Inbound است و هر کدام که از روتر خارج گردد Outbound می‌شود.

ACL زمانی فعال می شود که به یک اینترفیس در inbound و outbound یک روتر اعمال شود، در صورتی‌که اعمال نشود آن ACL عملکرد نخواهد داشت.

5- برای اِعمال ACL ها در صورتی‌که از نوع Extended باشند، آن‌ها را نزدیک به مبدا و در صورتی‌که از نوع Standard باشند نزدیک به مقصد اعمال می‌کنیم.

- اگر Standard باشد ← نزدیک به مقصد چون مبدا را نمی توانیم تعیین کنیم.
- اگر Extended باشد ← نزدیک مبدا باید تعریف شود.

چون در استاندارد می‌دانیم که packet نباید به کجا برسد ← نزدیک مقصد فیلتر می‌شود از آن مبداء ای که آمد نباید به مقصد برسد. زمانی‌که چیزی از مبدا مورد نظر ما رسید نباید رد شود .



شکل 6-3 نمایی از اعمال ACL از نوع استاندارد در روتر مقصد

دستورات پیاده سازی ACL

1- Numbered Standard

تعریف ACL هائیکه با شماره نوشته می‌شوند:

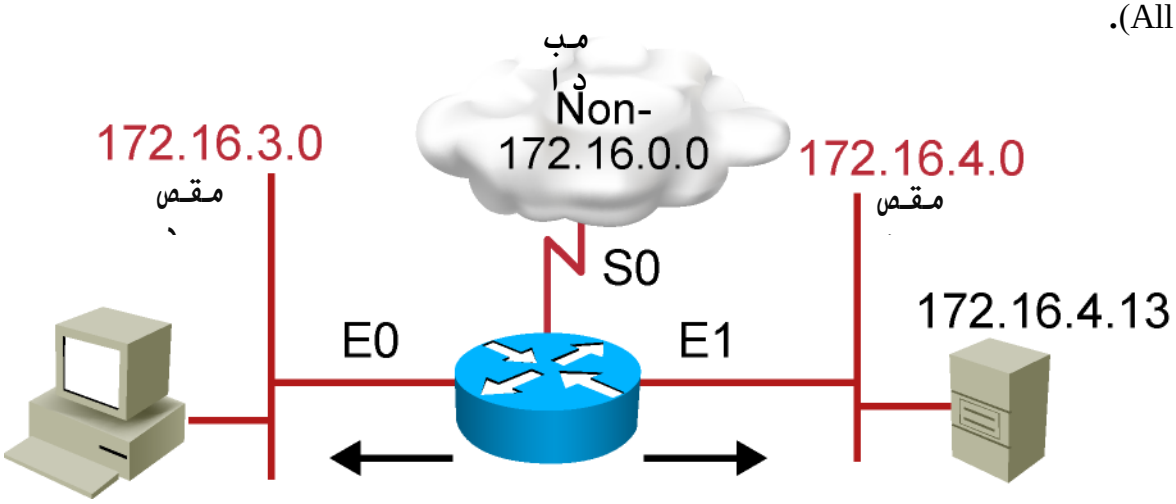
```
1  RouterX(config)# access-list access-list-number {permit | deny | remark} source [mask]
2  RouterX(config-if)# ip access-group access-list-number {in | out}
```

- خط1: نوشتن دستور ACL
- خط2: اعمال ACL به اینترفیس

منظور از In همان Inbound و Out همان Outbound می‌باشد.

مثال1: در شکل (6-4) ، امکان دسترسی کاربران از رنج IP:172.16.0.0/24 نسبت به شبکه مقدور گردیده است.

- اولویت بندی: کسانی‌که IP: 172.16.0.0 دارند ← Permit (با Wildcard کار می‌کند)
- بر اساس منطق Firewall ← چیزی برای کسی دیده نشود. ابتدا Permit را اجرا می‌کند سپس همه را به‌صورت خودکار می‌بندد (Implicit Deny All).



شکل 6-4 سناریو

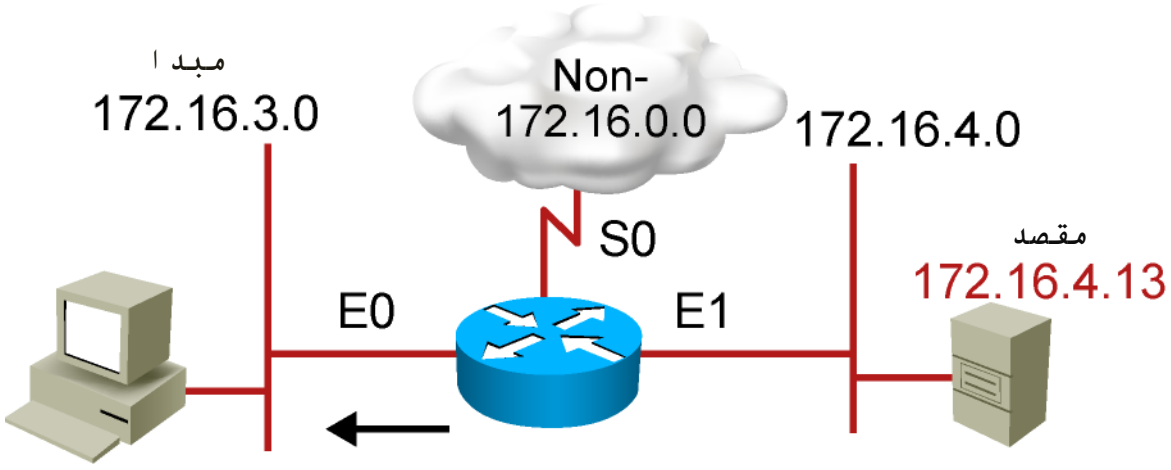
جهت حرکت از سمت ابر (172.16.0.0) به سمت شبکه های 172.16.4.0 و 172.16.3.0 میباشد.

```
1  RouterX(config)# access-list 1 permit 172.16.0.0  0.0.0.255
2  (implicit deny all - not visible in the list)
3  (access-list 1 deny 0.0.0.0   255.255.255.255)
4
5  RouterX(config)# interface ethernet 0
6  RouterX(config-if)# ip access-group 1 out
```

```
7
8  RouterX(config)# interface ethernet 1
9  RouterX(config-if)# ip access-group 1 out
```

خط 2و 3 نوشته نمی‌شود اما به صورت خودکار اجرا می‌شود، یعنی زمانی‌که ما به 172.16.0.0 دسترسی داریم به صورت خودکار این دسترسی برای بقیه بسته می‌شود و به غیر از 172.16.0.0 به بقیه اجازه‌ی عبور نمی‌دهد (Deny All).

مثال 2: کاربران شبکه به سرور 172.16.4.13 دسترسی نداشته باشند.

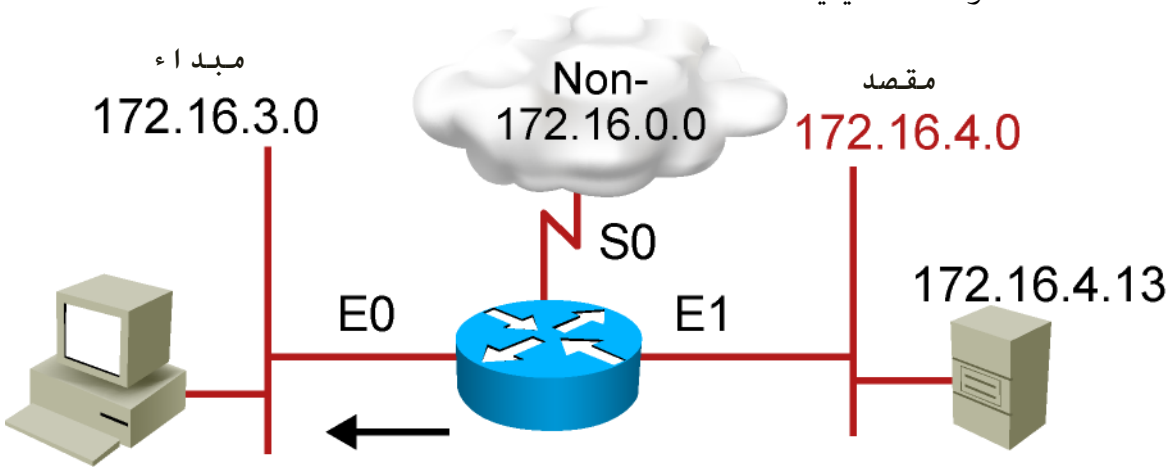


شکل 6-5 سناریو
مثال 2

```
1  RouterX(config)# access-list 1 deny 172.16.4.13 0.0.0.0
2  RouterX(config)# access-list 1 permit 0.0.0.0  255.255.255.255
3  (implicit deny all)
4  (access-list 1 deny 0.0.0.0   255.255.255.255)
5
6  RouterX(config)# interface ethernet 0
7  RouterX(config-if)# ip access-group 1 out
```

- خط 1: ابتدا دسترسی را می بندیم.
- خط 2: سپس دسترسی را برای بقیه باز می‌کنیم.

مثال 3: درشکل (6-6) دسترسی کاربران شبکه به سروربا رنج 172.16.4.0/24 مسدود نمایید.



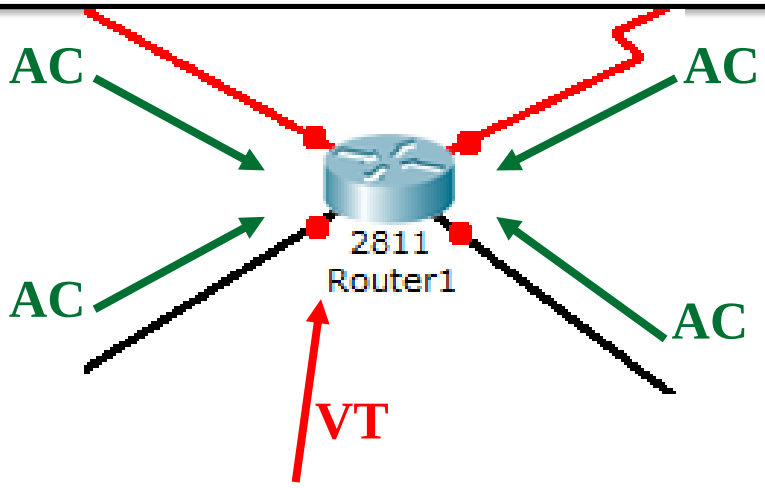
شکل 6-6 سناریو

```
1  RouterX(config)# access-list 1 deny 172.16.4.0  0.0.0.255
2  RouterX(config)# access-list 1 permit any
3  (implicit deny all)
4  (access-list 1 deny 0.0.0.0   255.255.255.255)
5
6  RouterX(config)# interface ethernet 0
7  RouterX(config-if)# ip access-group 1 out
```

- خط2: کلمه‌ی any برابر همان 0.0.0.0 255.255.255.255 می‌باشد

دسترسی به روتر از طریق Telnetو SSH

در Standard ACL اگر یک روتری به عنوان درگاه شبکه باشد که به این روتر تعداد زیادی اینترفیس وصل باشد، نوشتن ACL به ازای هر اینترفیس کار دشواری است، بنابراین اگر ارتباط به‌صورت telnet و ssh باشد موقعی که ACL نوشته می شود به جای اعمال ACL به اینترفیس به line vty اعمال شود کار راحت می‌شود.



شکل 6-7 نمایی از به کاربردن ACL در دسترسی به روتر از

1	RouterX(config-line)# **access-class *access-list-number* {in | out}**

- **Example:**

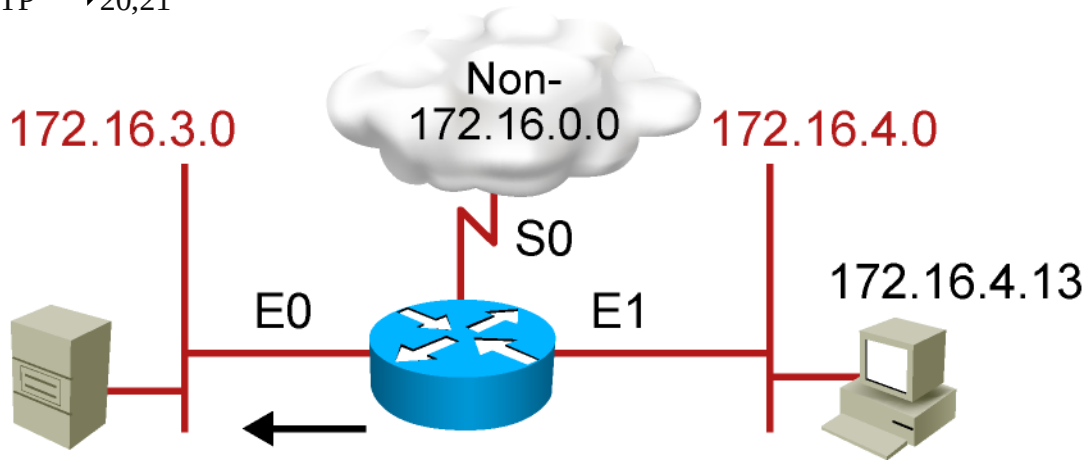
1	R(config)#**access-list 12 permit 192.168.1.0 0.0.0.255**
2	**(implicit deny any)**
3	
4	R(config)#**line vty 0 4**
5	R(config-line)#**access-class 12 in**

Numbered Extended -2

```
1  RouterX(config)# access-list access-list-number {permit | deny}
2  protocol source  source-wildcard [operator port]
3  destination destination-wildcard [operator port]
4  [established] [log]
5
6  RouterX(config-if)# ip access-group access-list-number  {in | out}
```

مثال4: در مثال شکل(6-8) دسترسی کاربران شبکه 172.16.4.0/24 به سرور FTP در رنج 172.16.3.0/24 مسدود گردیده است.

Port FTP ➡20,21



شکل 6-8 سناریو
مثال 4

```
1  RouterX(config)# access-list 101 deny tcp 172.16.4.0 0.0.0.255 172.16.3.0 0.0.0.255 eq 21
2  RouterX(config)# access-list 101 deny tcp 172.16.4.0 0.0.0.255 172.16.3.0 0.0.0.255 eq 20
3  RouterX(config)# access-list 101 permit ip any any
4  (implicit deny all)
5  (access-list 101 deny ip 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255)
6
7  RouterX(config)# interface ethernet 0
8  RouterX(config-if)# ip access-group 101 out
```

- خط 1و2: دسترسی کاربران با IP:172.16.4.0 (مبدا) ← به سرور FTP با آدرس E0 IP:172.16.3.0 مسدود شود.
- خط3: دسترسی را برای بقیه باز میکند.

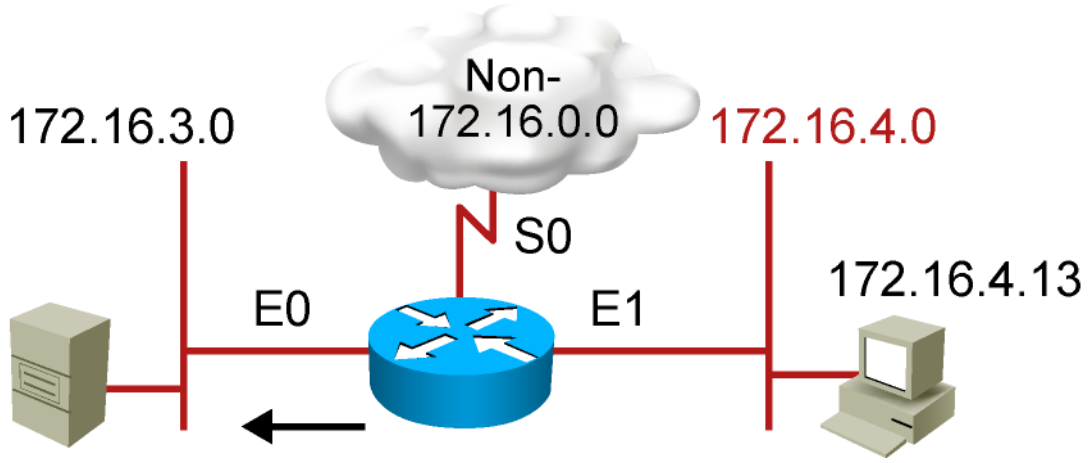
- خط5: دسترسی از طریق int e0 مسدود شود.

Ports:

$Web \longrightarrow TCP\ 80$ $DNS \longrightarrow TCP/UDP\ 53$ $Smtp \longrightarrow TCP\ 25$ ارسال ایمیل $Pops \longrightarrow TCP\ 110$ دریافت ایمیل	$Telnet \longrightarrow TCP\ 23$ $SSH \longrightarrow TCP\ 22$ $FTP \longrightarrow \begin{cases} TCP\ 20 \\ TCP\ 21 \end{cases}$

مثال 5: در شکل(6-9)، دسترسی کاربران شبکه به سرور از طریق Telnet مسدود گردیده است.

$Telnet \longrightarrow TCP\ 23$



شکل6-9 سناریو

```
1  RouterX(config)# access-list 101 deny tcp 172.16.4.0  0.0.0.255  any eq 23
2  RouterX(config)# access-list 101 permit ip any any
3  (implicit deny all)
4
5  RouterX(config)# interface ethernet 0
6  RouterX(config-if)# ip access-group 101 out
```

- خط1: به جای نوشتن IP سرور شبکه می‌توان any را به‌کار برد.
- خط 2: به غیر از 172.16.4.0 باقی دسترسی‌ها به بقیه‌ی شبکه باز باشد.

Name Standard & Extended -3

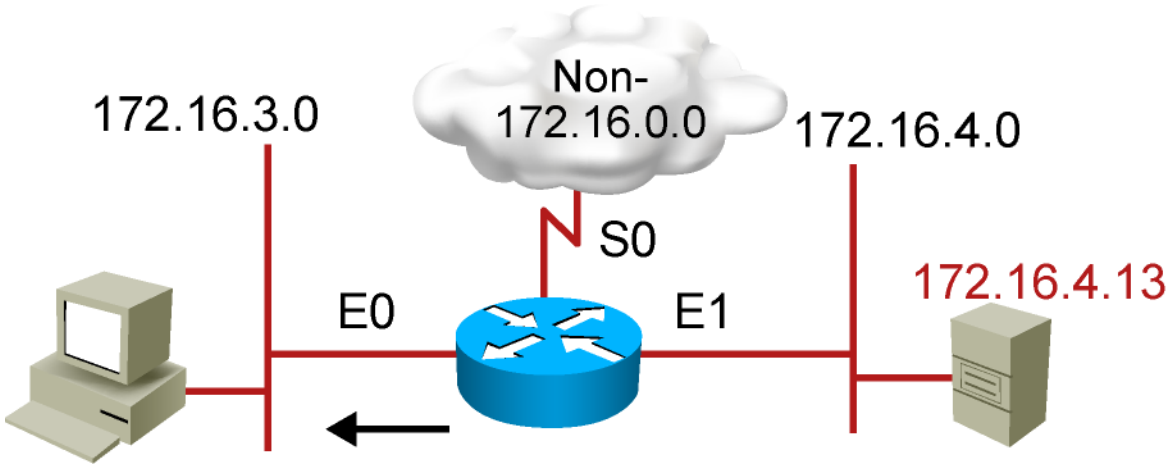
```
1  Router(config)#ip access-list {standard|extended} name
```

```
2  Router(config{std-| ext-}nacl)#
3  {sequence-number}{permit | deny}{ip access-list test conditions}
4  {permit | deny}{ip access-list test conditions}
5
6  Router(config-if)#ip access-group name {in |out}
```

- خط1: نوع ACL را مشخص کرده و یک نام برای ACL نوشته می‌شود.
- خط2: نوع دسترسی براساس ACL انتخابی در خط 1 مشخص می‌شود.

ip access-list test conditions: نوشتن ACL براساس وضعیت. وضعیت در خط 1 مشخص می‌شود یعنی اگر ACL از نوع standard انتخاب شود در این خط source و اگر Extended انتخاب شود باید source و destination نوشته شود.

مثال6: دسترسی کاربران شبکه به سرور 172.16.4.13 مسدود باشد.

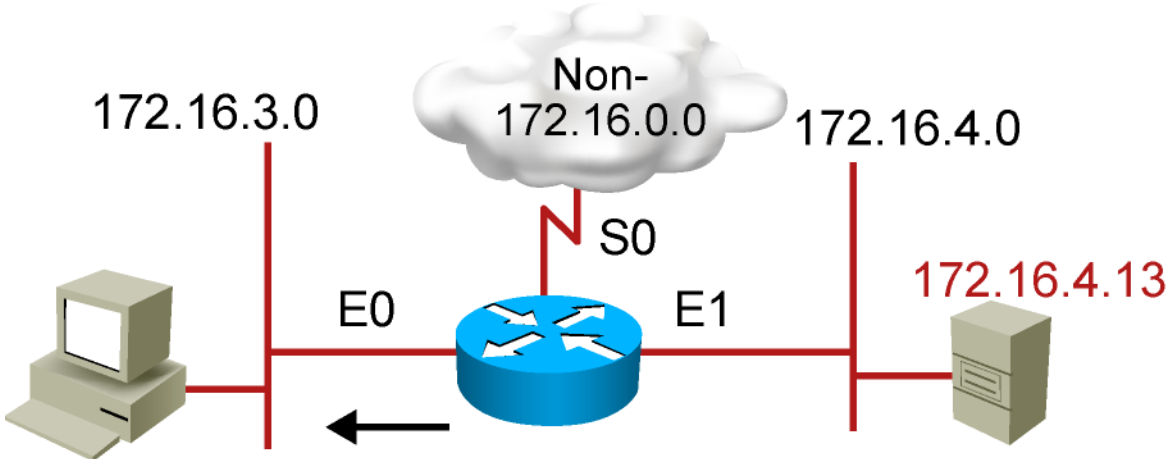


شکل 6-10 سناریو مثال 6

```
1  R(config)#ip access-list standard troublemarker
2  R(config-std-nacl)#deny host 172.16.4.13
3  R(config-std-nacl)#permit 172.16.4.0 0.0.0.255
4
5  R(config-std-nacl)#interface Ethernet 0
6  R(config-if)#ip access-group troublemarker out
```

- خط1: ACL از نوع standard بوده.
- خط2: دسترسی به سرور 172.16.4.13 مسدود گردیده.به جای نوشتن IP با wildcard می‌توان قبل نوشتن IP کلمه‌ی host را به کار برد و wildcard را ننوشت.
- خط3: دسترسی برای بقیه باز باشد. می توان به جای نوشتن ip با wildcard کلمه‌ی any را به‌کار برد.
- خط4: اعمال ACL به اینترفیس

مثال7: در شکل(6-11) دسترسی کاربران شبکه از طریق telnet مسدود باشد.



شکل 6-11 سناریو

1	R(config)#**ip access-list extended badgroup**
2	R(config-ext-nacl)#**deny tcp 172.16.4.0 0.0.0.255 any eq 23**
3	R(config-ext-nacl)#**permit ip any any**
4	
5	R(config-ext-nacl)#**interface e0**
6	R(config-if)#**ip access-group badgroup out**

دستور remark برای نوشتن توضیحات به ازای ACL

1	R(config)#**ip access-list {standard | extended}** ***name***
2	R(config{std- |ext-}nacl)#**remark** ***remark***
3	
4	R(config)#**access-list** ***access-list-number*** **remark** ***remark***

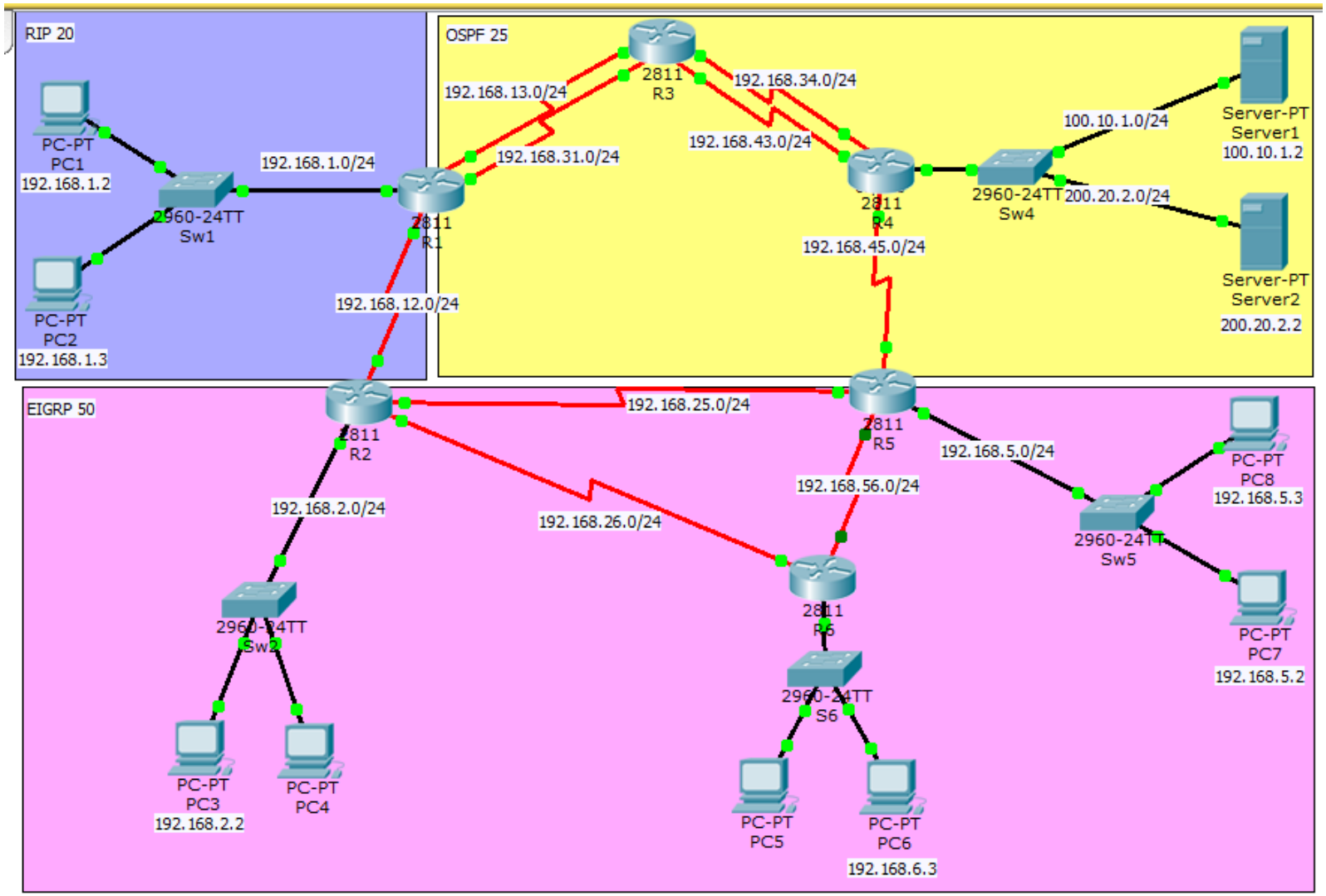
- خط1و2: اگر ACL از نوع نام باشد این دو دستور به‌کار برده می‌شود.
- خط4: اگر ACL از نوع عدد باشد این دستور به‌کار برده می‌شود.

دستور verify

Router#**show access-list**

ACLهای نوشته شده را نمایش می‌دهد.

سناریو ACL



شکل 6-12 سناریو ACL

سوال 1: دسترسي PC1 نسبت به سرور 1 فقط از طريق وب و نسبت به سرور 2 فقط از طريق پروتكل ICMP مقدور باشد.

پاسخ

- **بخش اول:** پروتكل‌ها را، فقط از طريق ACL Extended مي‌توان نوشت ⇐ ACL را بايد در روتر Source (روتر R1) بنويسيم.

دسترسي PC1 نسبت به سرور 1 فقط از طريق وب(tcp و پورت 80)

Source	نحوه ي ارتباط	Destination
PC1→	Web Browser	→ Server 1
192.168.1.2	80	100.10.1.2

- خط 1: ابتدا فقط دسترسي را براي **مبدا: PC1 (با IP:192.168.1.2)** به **مقصد: Server1 (با IP:100.10.1.2)** از طريق **TCP**، باز مي‌كنيم، كه پورت آن 80 (WWW) است:
- خط 2: سپس بقيه‌ي دسترسي‌هاي PC1 به Server1 را مي‌بنديم.

بخش دوم: دسترسي PC1 نسبت به سرور 2 فقط از طريق پروتكل ICMP (Command Prompt) مقدور باشد (فقط بتواند Ping بكند و مثلا از طريق Web browser نتواند باز كند)

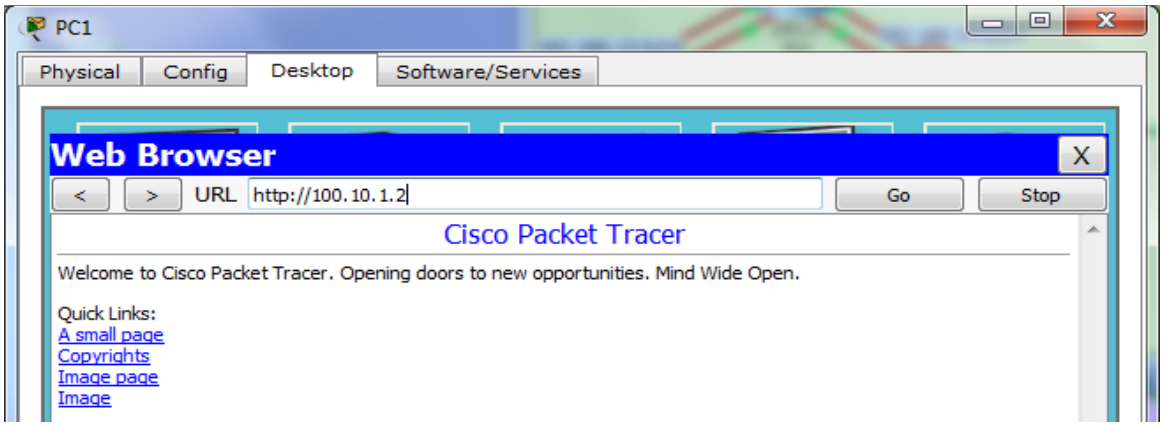
Source	نحوه ي ارتباط	Destination
PC1→	Command Prompt	→ Server 2
192.168.1.2	Permit ICMP	200.20.2.2

- خط 4: ابتدا دسترسي **ICMP**، را براي **مبدا: PC1 (با IP:192.168.1.2)**، به **مقصد: Server2 (با IP:200.20.2.2)** باز مي‌كنيم:
- خط 5: سپس بقيه‌ي دسترسي‌هاي PC1 به Server2 را مي‌بنديم.
- خط7 : حال دسترسي‌ها را براي بقيه باز مي‌كنيم.
- خط 9: سپس اين ACL را در جهت جريان (يعني از سمت مبدا PC1 كه از طريق interface fastEthernet 0/0 روتر R1، به سمت مقصد مي‌رود) اعمال مي‌كنيم.
- خط 10: براي اعمال ACL نوشته شده بايد آن‌را به Inbound، interface fastEthernet 0/0 روتر R1 اعمال كنيم.

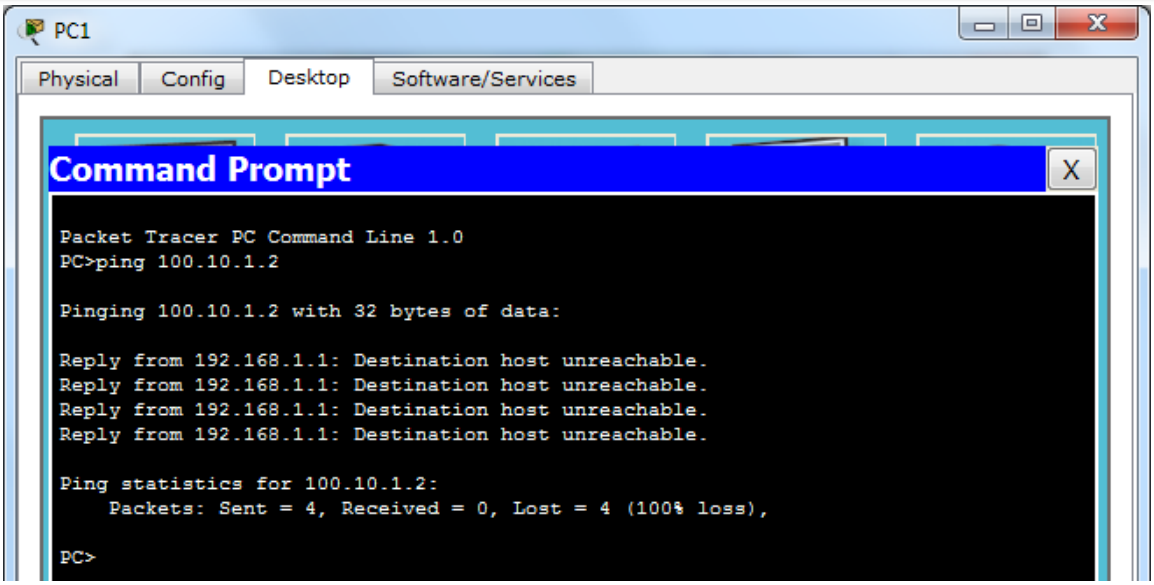
- کد نوشته شده در روتر R1:

```
1   R1(config)# access-list 120 permit tcp host 192.168.1.2 host 100.10.1.2 eq 80
2   R1(config)# access-list 120 deny ip host 192.168.1.2 host 100.10.1.2
3
4   R1(config)# access-list 120 permit icmp host 192.168.1.2 host 200.20.2.2
5   R1(config)# access-list 120 deny ip host 192.168.1.2 host 200.20.2.2
6
7   R1(config)# access-list 120 permit ip any any
8
9   R1(config)# interface fastEthernet 0/0
10  R1(config-if)# ip access-group 120 in
```

تست بخش اول:
باید از PC1 به Server1 از طریق Browser دسترسي داشته باشيم، براي اين كار Browser را باز مي‌كنيم و IPServer1: 100.10.1.2 را وارد مي‌كنيم:



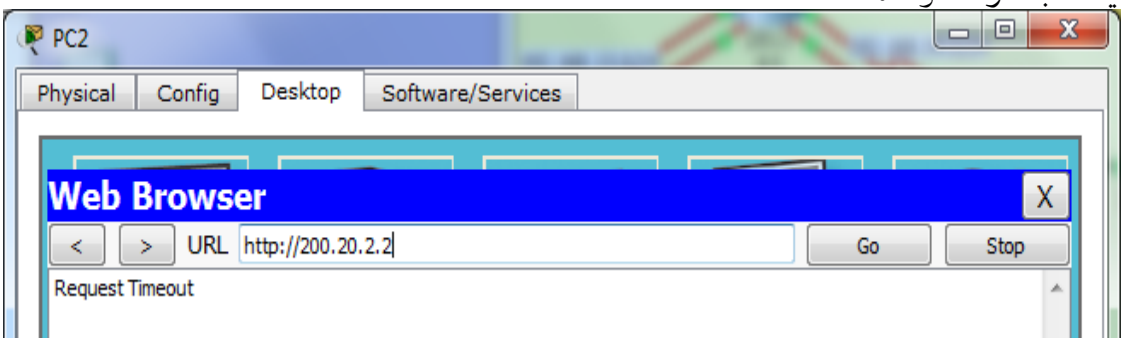
شکل 6-13 طریقه‌ی اتصال PC1 به Server 1 از طریق Web



شکل 6-14 عدم ping از PC1 به

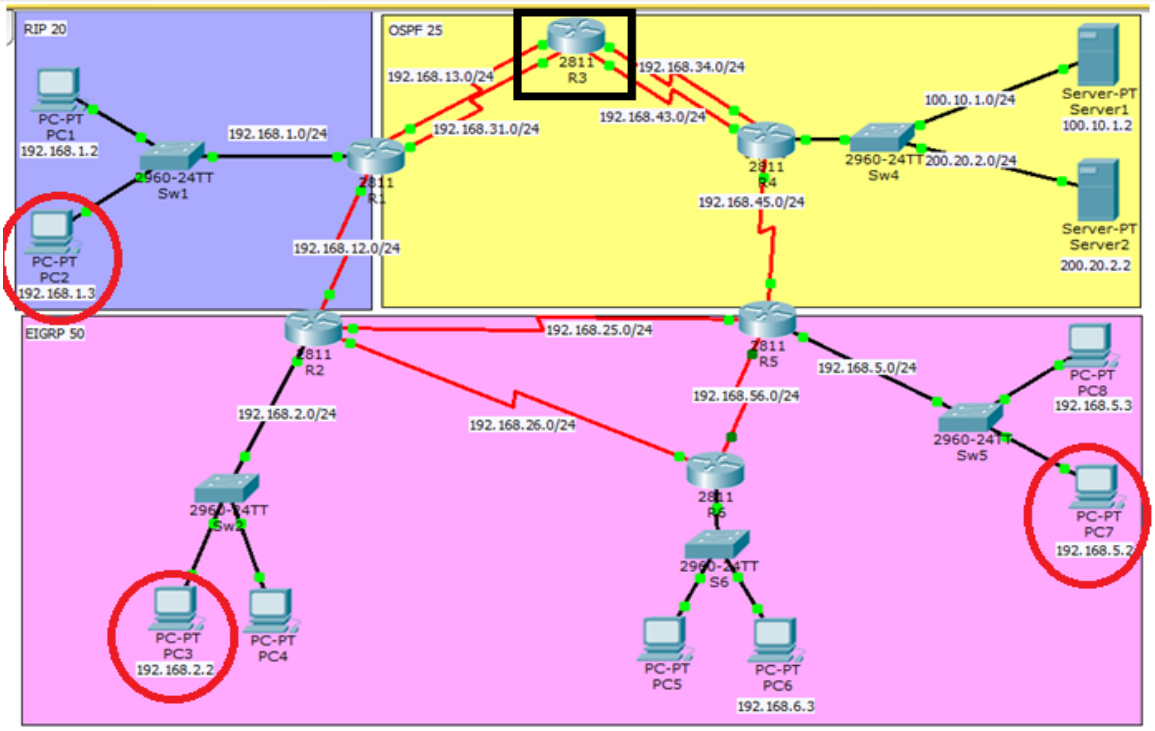
تست بخش دوم:

حال اگر از PC1 بخواهیم Server2 را از طریق Browser باز کنیم. نباید باز شود:



شکل 6-15 عدم اتصال PC1 به Server2 از طریق Web

سوال 2: قابلیت SSH نسبت به روتر 3 برای PC2، PC3 و PC7 مسدود باشد.



پاسخ

ابتدا SSH را روي روتر 3 فعال مي‌كنيم:

```
1  R3(config)# hostname TEST
2  TEST(config)# ip domain-name CISCO.com
3  TEST(config)# crypto key generate rsa
4  % You already have RSA keys defined named TEST.CISCO.com .
5  % Do you really want to replace them? [yes/no]:1024
6  TEST(config)# ip ssh version 2
7  TEST(config)# username poya password 123
8  TEST(config)# enable secret 12345
9  TEST(config-line)# line vty 0 4
10 TEST(config-line)# login local
11  TEST(config-line)# transport input ssh
```

توضيح كد:

- خط 3: كليد امنيتي با الگوريتم رمز نگاري RSA
- خط 5 : 1024 را وارد مي‌كنيم براي اينكه طول كليد امنيتي بالا رود و رمزنگاري آن مشكل‌تر شود.
- خط 6: براي ساپورت طول كليد بزرگتر، بايد وارد Ver2 شويم.

- خط 7: انتخاب نام براي SSH و پسوورد

PC>**ssh –l poya 192.168.13.2(ip router 3)**

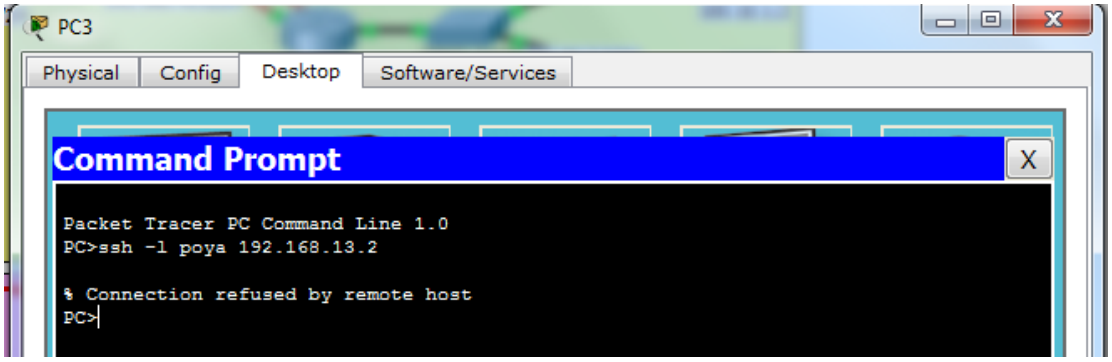
- خط 8: پسورد ورود به مد enable روتر را در اينجا تعريف مي‌كنيم (براي زماني‌كه كه كسي مي‌خواهد از طريق ssh به روتر شماره 3 وصل شود و وارد مد enable شود)

حال ACL مورد نظر را مي‌نويسيم، اين ACL از نوع استاندارد است و بايد آن‌را در مقصد (R3) اعمال كنيم:

1	R3(config)#**access-list 20 deny host 192.168.1.3**
2	R3(config)#**access-list 20 deny host 192.168.2.2**
3	R3(config)#**access-list 20 deny host 192.168.5.2**
4	R3(config)#**access-list 20 permit any**
5	R3(config)#**line vty 0 4**
6	R3 (config-line)# **access-class 20 in**

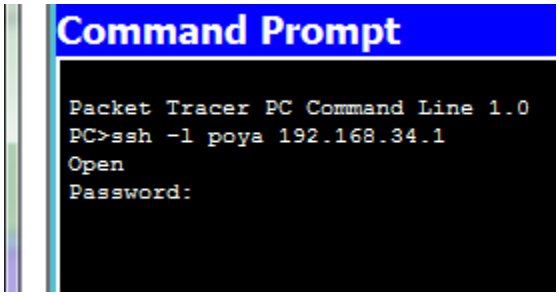
- خط 1و2و3: حال دسترسي‌ها را براي(192.168.1.3 :IP(PC2 و PC3(IP:192.168.2.2) و PC7(IP:192.168.5.2) مي‌بنديم.
- خط 4: دسترسي را براي بقيه باز مي‌كنيم.
- خط 5:
- خط 6: اعمال ACL20 بر روي inbound روتر R3. اجراي دسترسي به دستور Telnet، **access-class** مي باشد.

تست: حال اگر از سيستم‌هاي PC3,PC2,PC7 بخواهيم از طريق ssh به روتر R3 وصل شويم با پيغام شكل (6-16) مواجه مي‌شويم:

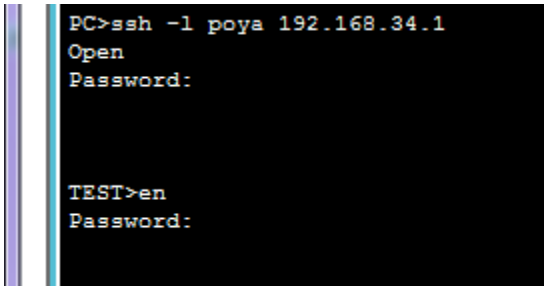


شكل 6-16 نمايش پيغام مبني برعدم اتصال PC2.PC3,PC7 به

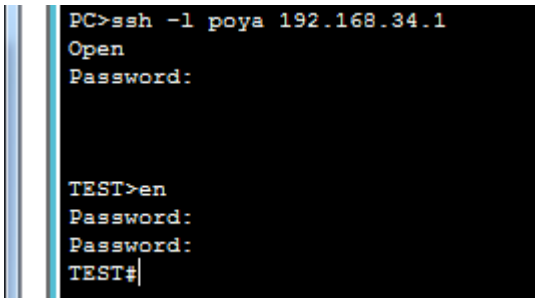
و اگر از سیستم‌هاي دیگر بخواهیم از طریق SSH متصل شویم، می‌توانیم این کار را انجام بدهیم.



حال باید پسورد اول را وارد کنیم: 123

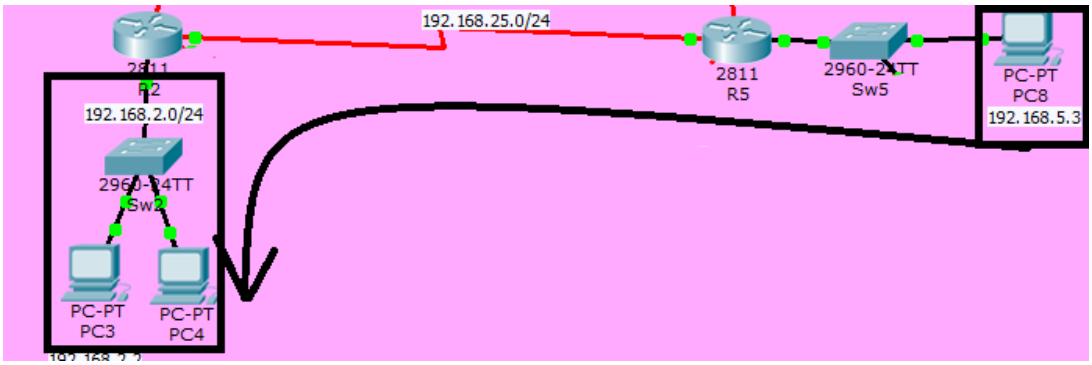


سپس پسورد enable را وارد می‌کنیم: 12345
و وارد مد enable روتر می‌شویم.



شکل 6-17 اتصال به روتر3 از طریق ssh

سوال 3: دسترسي PC8 نسبت به كاربران سوئيچ 2 كلا مسدود باشد.



Source	نحوه ي ارتباط	Destination
PC8→	كلا مسدود شود	→ Switch 2
192.168.5.3	×	192.168.2.0

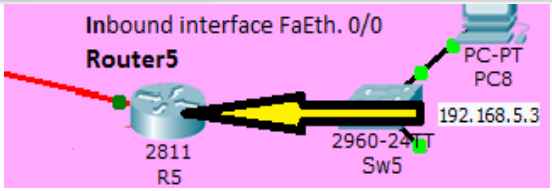
پاسخ

اين ACL را بصورت Extended مينويسيم. همانگونه كه در شكل بالا مشاهده ميفرماييد، **مبدا PC8 IP:192.168.5.3** ميباشد و **مقصد شبكه با NET ID:192.168.2.0** و **WildCard:0.0.0.255** (چون مقصد Net ID است بايد حتما WildCard را وارد كنيم، اگر مقصد host باشد WildCard ندارد) ميباشد.

- خط 1: ابتدا دسترسي را براي **مبدا: PC8:IP:192.168.5.3** را به **مقصد: شبكه NET ID :192.168.2.0** ميبنديم.
- خط 2: باقي دسترسيها را باز ميكنيم.
- خط 3و 4: چون مبدا PC8 ميباشد و ACL نوشته شده از نوع Extended است، آنرا بايد در جهت جريان و به ورودي Inbound در اينترفيس fastEthernet 0/0 روتر R5 اعمال كنيم.

R5:

```
1  R5(config)#access-list 150 deny ip host 192.168.5.3 192.168.2.0 0.0.0.255
2  R5(config)#access-list 150 permit ip any any
3  R5(config)#interface fastEthernet 0/0
4  R5(config-if)#ip access-group 150 in
```



سوال 4: قابلیت ping از PC6، نسبت به PC2 امکان‌پذیر نباشد.

Source	نحوه ي ارتباط	Destination
PC6→	Command Prompt×	→ PC2
192.168.6.3	Deny ICMP	192.168.1.3

پاسخ

این ACL را نیز از نوع Extended می‌نویسیم.
مبدا PC6 IP:192.168.6.3 و **مقصد PC2 IP:192.168.1.3** می‌باشد و این ACL چون از نوع Extended است باید **در روتر مبدا R6** و ورودي Inbound آن اعمال گردد.

R6:

1	R6(config)#**access-list 180 deny icmp host 192.168.6.3 host 192.168.1.3**
2	R6(config)#**access-list 180 permit ip any any**
3	R6(config)#**interface fastEthernet 0/0**
4	R6(config-if)#**ip access-group 180 in**

تست ACL نوشته شده:

```
PC>ping 192.168.1.3

Pinging 192.168.1.3 with 32 bytes of data:

Reply from 192.168.6.1: Destination host unreachable.
Reply from 192.168.6.1: Destination host unreachable.
Reply from 192.168.6.1: Destination host unreachable.
Reply from 192.168.6.1: Destination host unreachable.

Ping statistics for 192.168.1.3:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

شکل 6-18 عدم ping از PC6 به PC2

فصل 7

NAT

آدرس های ipv4 به دو دسته ی اصلی تقسیم می شوند:

- **آدرس‌های public:** آدرس‌هایی هستند که اکثر محدوده موجود در کلاس‌های A، B و C را اشغال کرده اند و برای مسیریابی در شبکه های WAN استفاده می‌شوند.

جدول7-1 محدوده IP های Public

Class	Public IP Range
A	1.0.0.0 to 9.255.255.255 11.0.0.0 to 126.255.255.255
B	128.0.0.0 to 172.15.255.255 172.32.0.0 to 191.255.255.255
C	192.0.0.0 to 192.167.255.255 192.169.0.0 to 223.255.255.255

- **آدرس‌های private:** آدرسی است که فقط داخل شبکه LAN استفاده می شود، یعنی متعلق به شبکه داخلی بوده و با دنیای بیرون ارتباطی ندارد.

جدول 7-2 محدوده IP های

Class	Private IP Range
A	10.0.0.0 to 10.255.255.255
B	172.16.0.0 to 172.31.255.255
C	192.168.0.0 to 192.168.255.255

NAT[1]

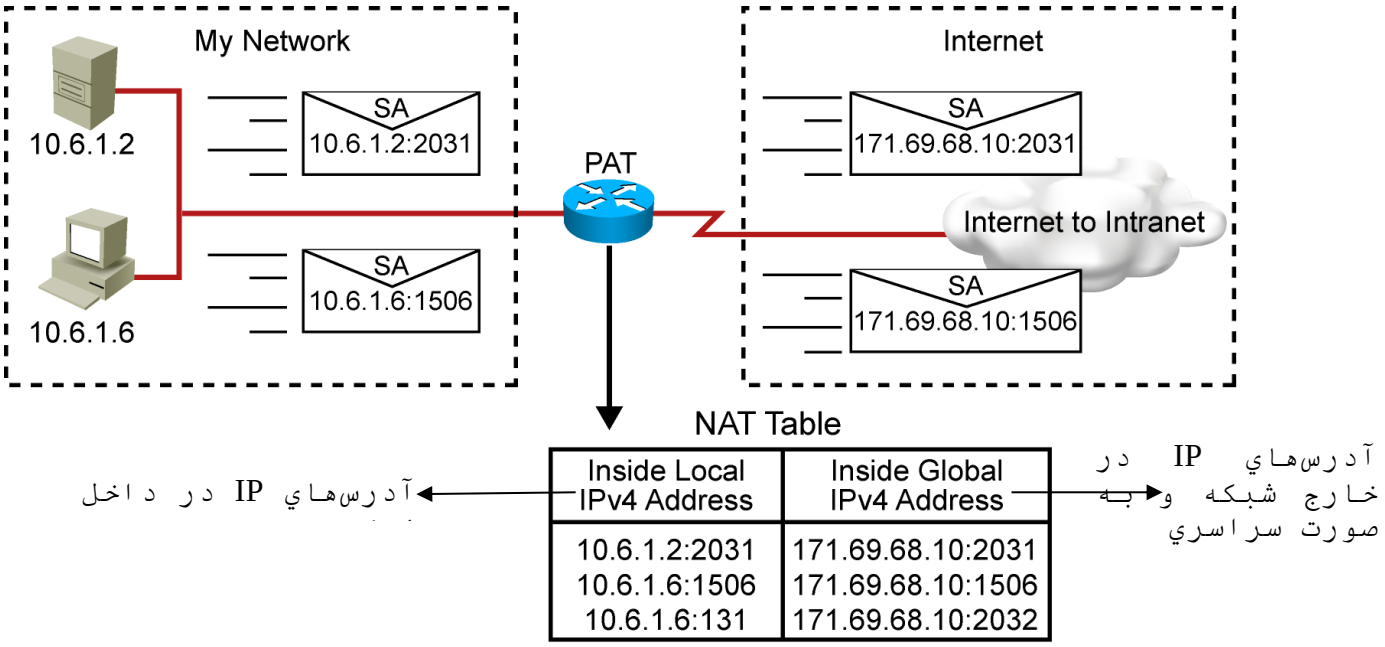
NAT را به طور کلی در دستگاه‌های مختلفی در شبکه پیاده سازی می‌کنند. در بحث سیسکو معمولا NAT را روی روتر اجرا می‌کنند. مفهوم NAT به این صورت است که یک آدرس private به آدرس public ترجمه می شود. روتر باید حداقل 2 اینترفیس داشته باشد که یک اینترفیس به LAN و یک اینترفیس به WAN کانکت شود. محدوده ای که اینترفیس روتر به LAN کانکت می‌شود با نام inside و محدوده‌ی خارجی با نام outside شناخته می‌شود.

ترجمه‌ی آدرس‌ها از سمت inside به سمت outside اتفاق می‌افتد.

پس هدف از انجام NAT عبارتست از:

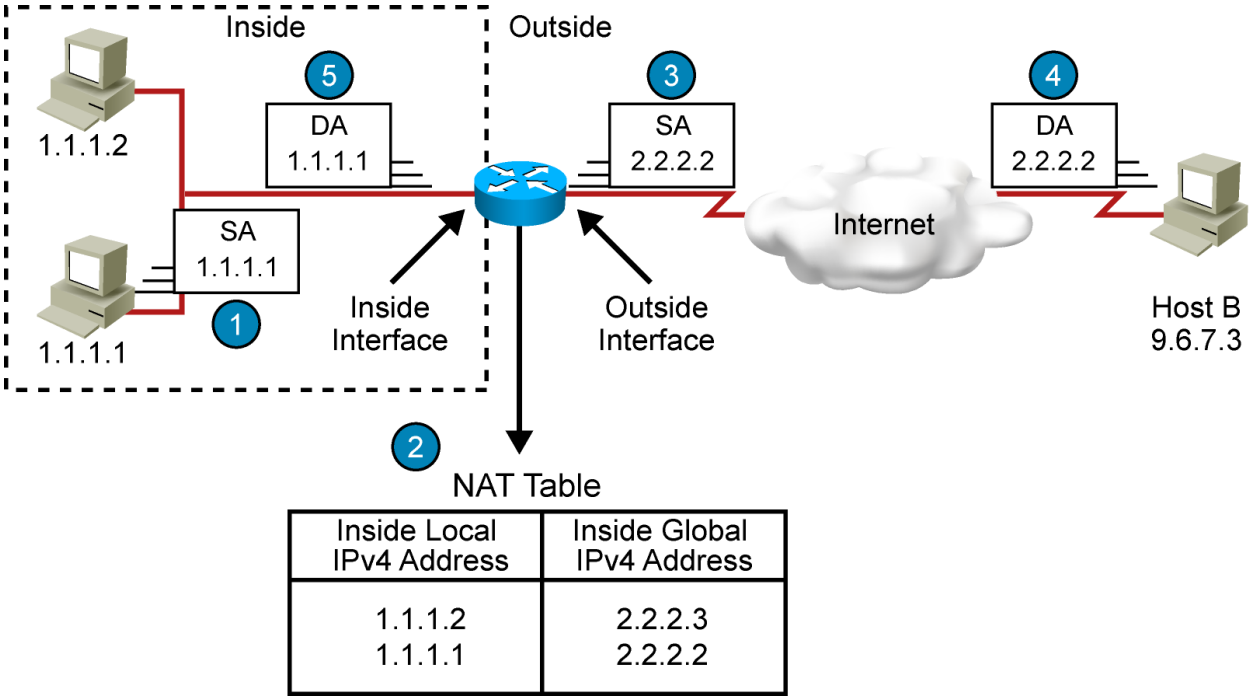
- پنهان‌سازي رنج IP هاي داخلي شبكه
- تبديل IP هاي Private به Public
- هميشه يك كامپيوتر داخل شبكه مي‌خواهد به شبكه External از طريق درگاه خروجي شبكه وصل شود.
- فراهم كردن امنيت

[1] Network Access Translation



شکل 7-1 نمونه ای از یک Nat Table بر

- انجام عمل NAT روي روترها توسط عملي به نام Natting مي‌باشد.
- در روترها يك Nat Table وجود دارد كه مشخص مي‌كند هر IP به چه چيزي تبديل شده است.



شکل 7-2 یک نمونه از تبدیل IP ها به همدیگر

انواع روشهاي NAT

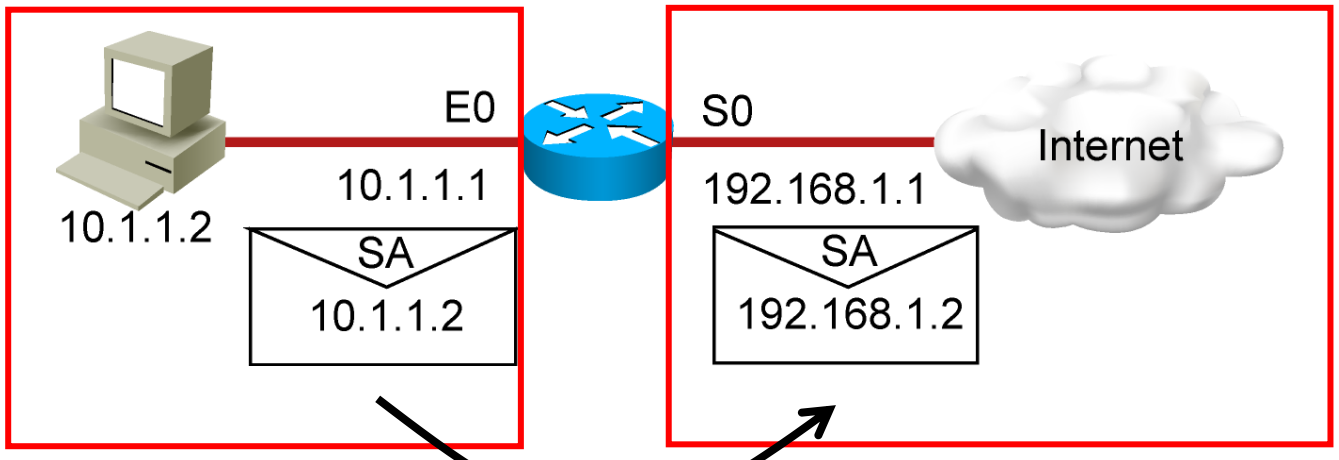
1- Static NAT

- یک IP Address خصوصی به یک IP Address عمومی نگاشت می‌شود.
- معمولا برای اینترنت به سرور استفاده می‌شود.
- معمولا برای ترافیک ورودی پیکربندی می‌شود.

دستورات Static NAT

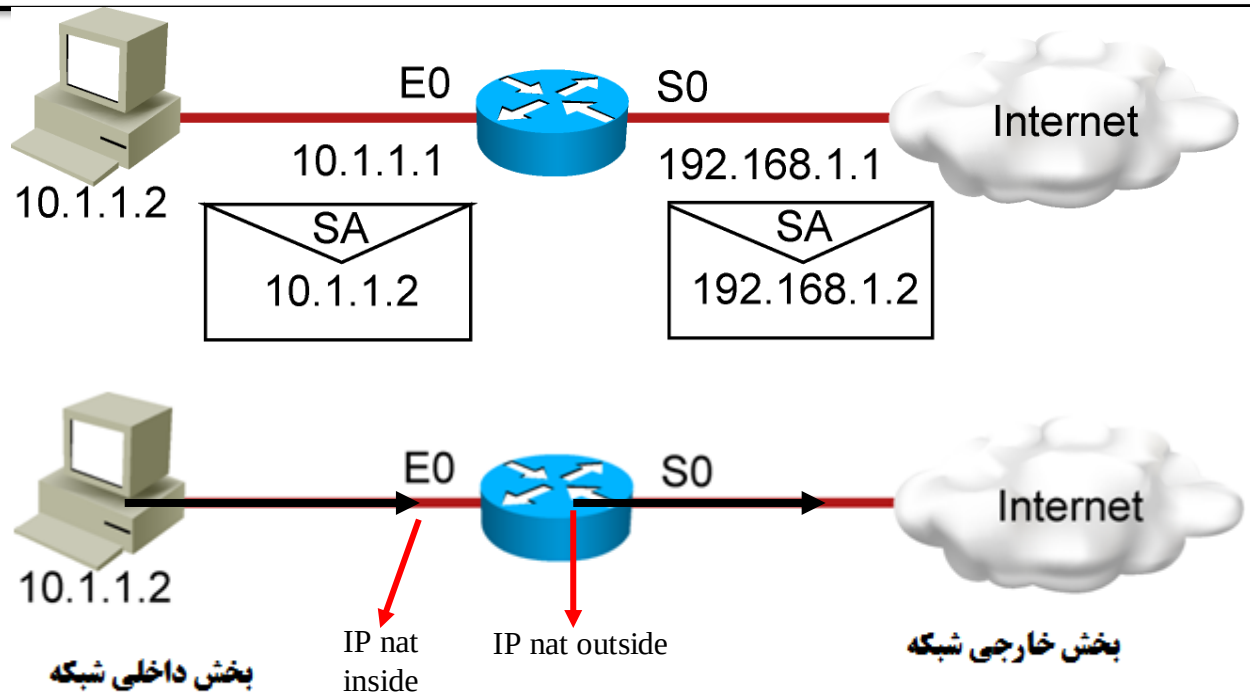
```
1  RouterX(config)# ip nat inside source static local-ip global-ip
2
3  RouterX(config-if)# ip nat inside
4  RouterX(config-if)# ip nat outside
5
6  RouterX# show ip nat translations
```

- خط 1: ترجمه‌ی آدرس‌های private شبکه LAN برای استفاده در WAN
- خط 3و 4: وارد Interface می‌شویم و نوع Interface را انتخاب می‌کنیم (Inside /Outside)
- خط 6: مشاهده Nat Table (مشاهده‌ي اینکه آیا Natting انجام می‌دهد یا خیر)



تبدیل به یک IP حقیقي
براي خارج شبکه شود.

شکل 7-3 نمونه‌ای از تبدیل آدرس‌های



شکل 7-4 سناریو مثال 1

مثال 1: با توجه به سناریوی شکل (7-4)، Static NAT را انجام دهید.

```
1  RouterX(config)#interface s0
2  RouterX(config-if)# ip address 192.168.1.1 255.255.255.0
3  RouterX(config-if)# ip nat outside
4
5  RouterX(config)#interface e0
6  RouterX(config-if)# ip address 10.1.1.1 255.255.255.0
7  RouterX(config-if)# ip nat inside
8
9  RouterX(config)# ip nat inside source static 10.1.1.2 192.168.1.2

   RouterX# show ip nat translations

      Pro  Inside global   Inside local   Outside local  Outside global
      ---  192.168.1.2     10.1.1.2       ---            ---
```

- خط 9: IP شبکه داخلي 10.1.1.2 ← IP در خارج از شبکه‌ي داخلي (در شبکه‌ي سراسري) 192.168.1.2.
- يعني IP:10.1.1.2 در هنگامي که از شبکه داخلي خارج مي‌شود به ← IP:192.168.1.2 تبديل شود.
- در اين روش بايد به تعداد کلاينت‌ها IP خريداري/ اجاره شود. در حال حاضر اين روش استفاده نمي‌شود چون گران است.

Dynamic NAT -2

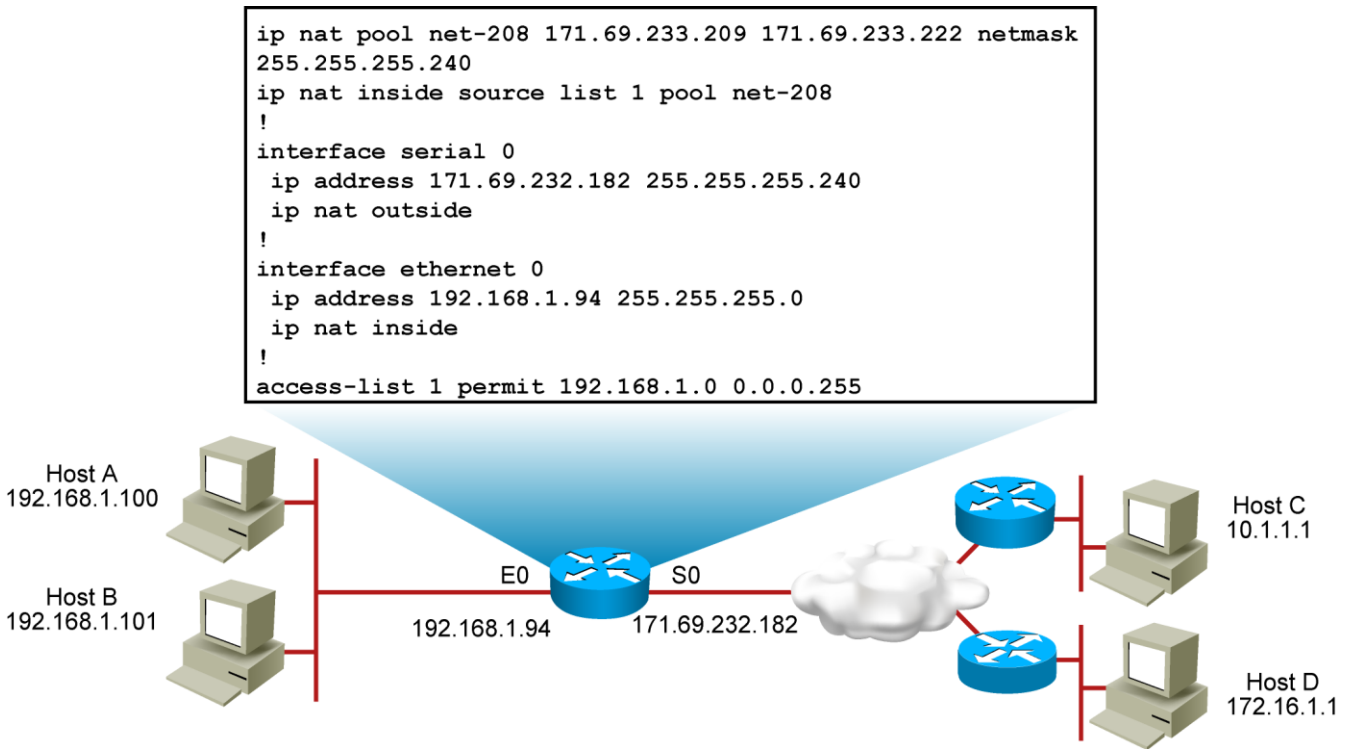
- چندین IP Address خصوصی به چندین IP Address عمومی نگاشت می شود.
- برای ترافیک خروجی پیکربندی شده است(LAN به اینترنت).
- تعداد کاربرانی که به اینترنت کانکت می شوند برابر تعداد IP Address های عمومی است.

دستورات Dynamic NAT

```
1  RouterX(config)# ip nat pool name start-ip end-ip {netmask netmask | prefix-length
2  prefix-length}
3  RouterX(config)# access-list access-list-number permit source [source-wildcard]
4
5  RouterX(config)# ip nat inside source list access-list-number pool name
6
7  RouterX# show ip nat translations
```

- خط 1: معرفي منبعي از آدرس‌هاي IP جهت اختصاص در زمان مورد نياز.
- خط 3: تعريف ACL استاندارد IP كه اجازه مي‌دهد IP هاي محلي به آدرس‌هاي جديد تبديل شوند.
- خط 5: ايجاد Dynamic Nat و اختصاص ACLي كه در مرحله‌ي قبل تعريف كرديم.
- خط 7: مشاهده‌ي Nat Table.

اگر نتوان به ازاي هر كلاينت IP خريداري نمود، مثلا اگر 100 كلاينت داريم و ما فقط 50، IP خريداري كرده باشيم، به تعداد همان 50 نفر مي‌توانند به بيرون از شبكه متصل شوند از نفر 51 ام بايد منتظر شود كه يك IP خالي شود تا به او IP اختصاص داده شود.



شکل 7-5 نمونه یک مثال از کارکرد
Dynamic NAT

ACL ای که در این بخش استفاده میشود فقط برای Select کردن ترافیك است.

```
RouterX# show ip nat translations
  Pro  Inside global     Inside local       Outside local      Outside global
  ---  171.69.233.209    192.168.1.100      ---                ---
  ---  171.69.233.210    192.168.1.101      ---                ---
```

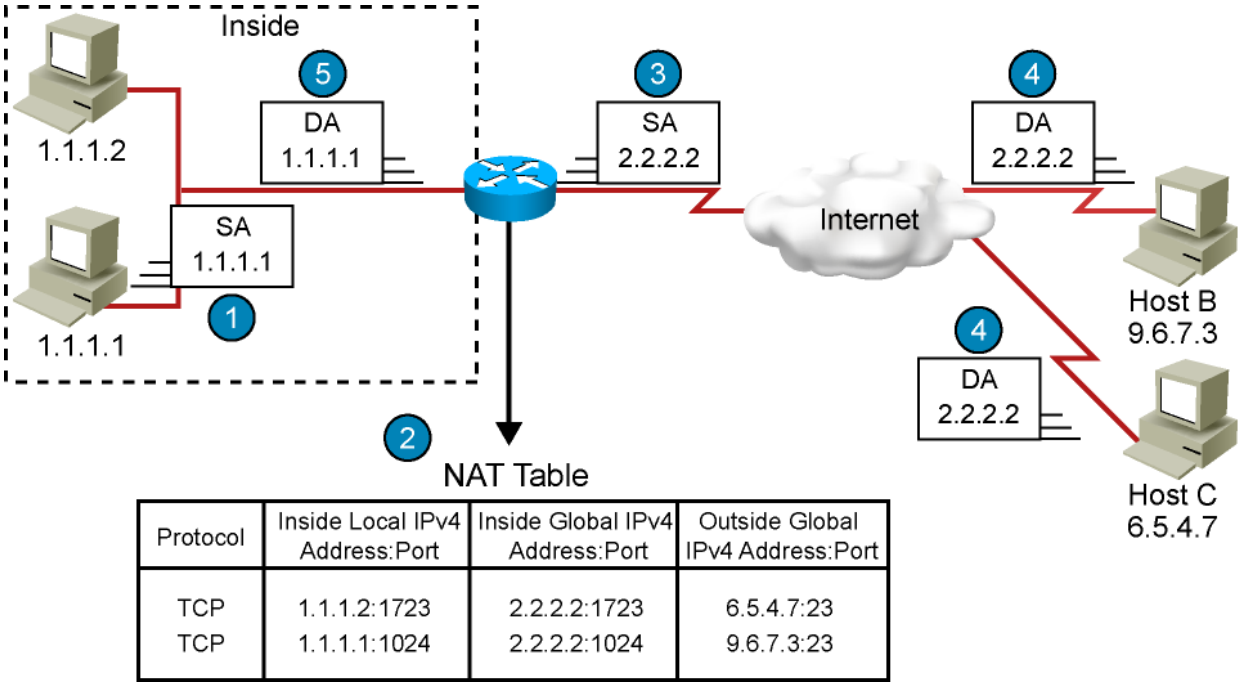
این روش بهتر از روش اول است اما با این حال باز هم IP ها تمام میشود و باید از روش دیگر استفاده گردد.

3- PAT[1]

در این روش به جای اینکه IP را به IP، Point کنیم ← IP را به پورت‌های روتر Point می‌کنیم، روتر 65535 پورت دارد.
اگر ما یک روتر داشته باشیم که به عنوان Gateway باشد هر کامپیوتر را به یکی از پورت‌های روتر Point می‌کنیم و شماره پورت را به انتهای IP سراسری اضافه می‌کنیم و در این حالت از یک IP Global می‌توانیم چند هزار IP جدید ایجاد کنیم.

نکات

- در روش PAT، همه‌ی کاربران می‌توانند در زمان یکسان به اینترنت دسترسی داشته باشند.
- روش PAT، برای ترافیک خروجی پیکربندی شده است (LAN به اینترنت).



Protocol	Inside Local IPv4 Address:Port	Inside Global IPv4 Address:Port	Outside Global IPv4 Address:Port
TCP	1.1.1.2:1723	2.2.2.2:1723	6.5.4.7:23
TCP	1.1.1.1:1024	2.2.2.2:1024	9.6.7.3:23

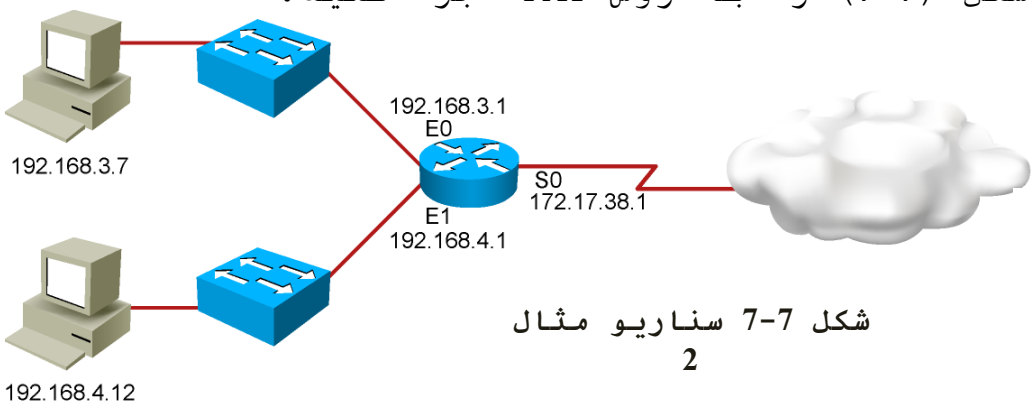
شکل 7-6 نمونه یک مثال از کارکرد PAT

[1] Overloading Port Address Translation

دستورات PAT

1	RouterX(config)# **access-list *access-list-number* permit *source* *source-wildcard***
2	RouterX(config)# **ip nat inside source list *access-list-number* interface *interface* overload**
3	RouterX# **show ip nat translations**

مثال2: سناریوی شکل (7-7) را به روش PAT اجرا کنید.



شکل 7-7 سناریو مثال 2

1	RouterX(config)#**hostname RouterX**
2	
3	RouterX(config)#**interface Ethernet0**
4	RouterX(config-if)#**ip address 192.168.3.1 255.255.255.0**
5	RouterX(config-if)#**ip nat inside**
6	
7	RouterX(config)#**interface Ethernet1**
8	RouterX(config-if)#**ip address 192.168.4.1 255.255.255.0**
9	RouterX(config-if)#**ip nat inside**
10	
11	RouterX(config)#**interface Serial0**
12	RouterX(config-if)#**ip address 172.17.38.1 255.255.255.0**
13	RouterX(config-if)#**ip nat outside**
14	
15	RouterX(config)#**ip nat inside source list 1 interface Serial0 overload**
16	
17	RouterX(config)#**ip route 0.0.0.0 0.0.0.0 Serial0**
18	
19	RouterX(config)#**access-list 1 permit 192.168.3.0 0.0.0.255**
20	RouterX(config)#**access-list 1 permit 192.168.4.0 0.0.0.255**
21	
22	RouterX# **show ip nat translations**
23	Pro Inside global Inside local Outside local Outside global
24	TCP 172.17.38.1:1050 192.168.3.7:1050 10.1.1.1:23 10.1.1.1:23
25	TCP 172.17.38.1:1776 192.168.4.12:1776 10.2.2.2:25 10.2.2.2:25

26	

خط 22 : Nat هـاي Active را نـمـايـش مـي دهـد و Nat table را Refresh مـيكـنـد .

پـاك كـردن Nat Table :

1	RouterX# **clear ip nat translation**
2	
3	RouterX# **clear ip nat translation inside *global-ip* *local-ip* [outside *local-ip* *global-ip*]**
4	
5	RouterX# **clear ip nat translation outside *local-ip* *global-ip***
6	
7	RouterX# **clear ip nat translation protocol inside *global-ip* *global-port local-ip* *local-***
8	***port* [outside *local-ip* *local-port* *global-ip* *global-port*]**
9	
10	RouterX# **debug ip nat**
11	
12	RouterX# **show ip nat statistics**

- Line1: Clears all dynamic address translation entries
- Line3: Clears a simple dynamic translation entry that contains an inside translation or both an inside and outside translation.
- Line5: Clears a simple dynamic translation entry that contains an outside translation
- Line7: Clears an extended dynamic translation entry (PAT entry)
- Line10: Displaying Information with show and debug Commands
-

- خط 12 : تـعـداد NATهـای مـتـنـوع كـه روی سـيـسـتـم اجـرا مـیشـود را نـشـان مـیدهـد .

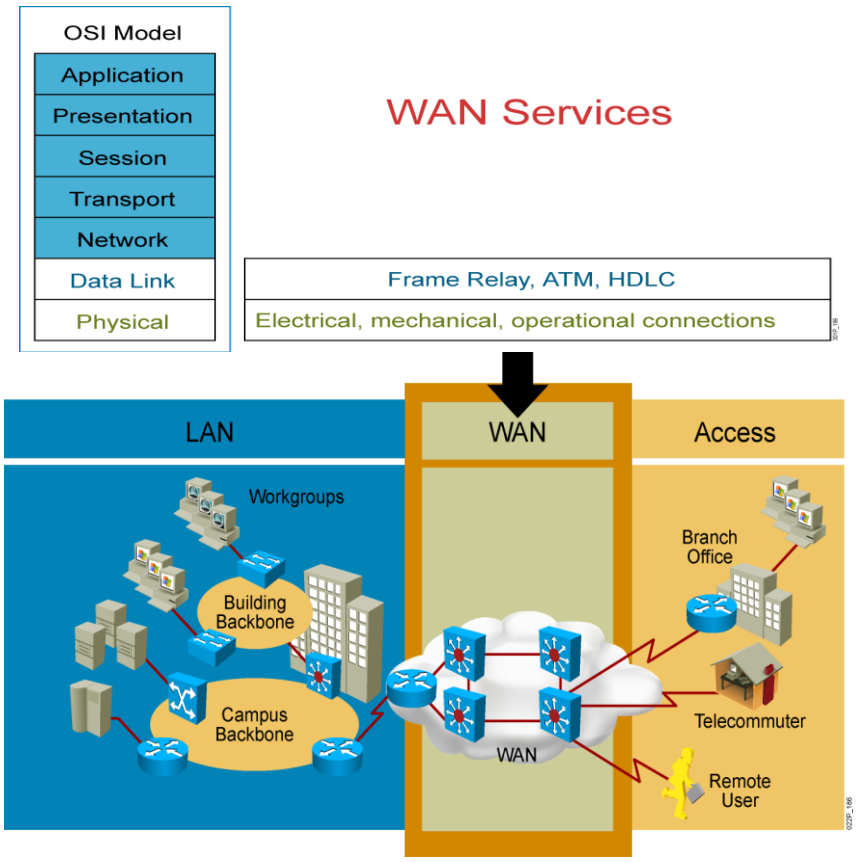
فـصل 8

WAN Connection

WAN[1]

در WAN همیشه با یک سری پروتکل سر و کار داریم که در scale کلان استفاده می‌شوند. این پروتکل‌ها به‌صورت پایه‌ای پروتکل‌هایی هستند که با بستر مخابراتی ارتباط برقرار می‌کنند و امکان دسترسی شبکه‌ها را در چارچوب WAN نسبت بهم فراهم می‌کنند. پروتکل‌های اصلی ساختار WAN ، پروتکل‌هايي هستند که در لايه‌ي Data Link قرار گرفته‌اند که بستر اوليه‌ي دسترسي به شبکه جهاني اينترنت را فراهم مي‌کنند.
نمونه پروتکل‌هایی که در لایه‌ی 2 در بحث WAN وجود دارد، عبارتند از:

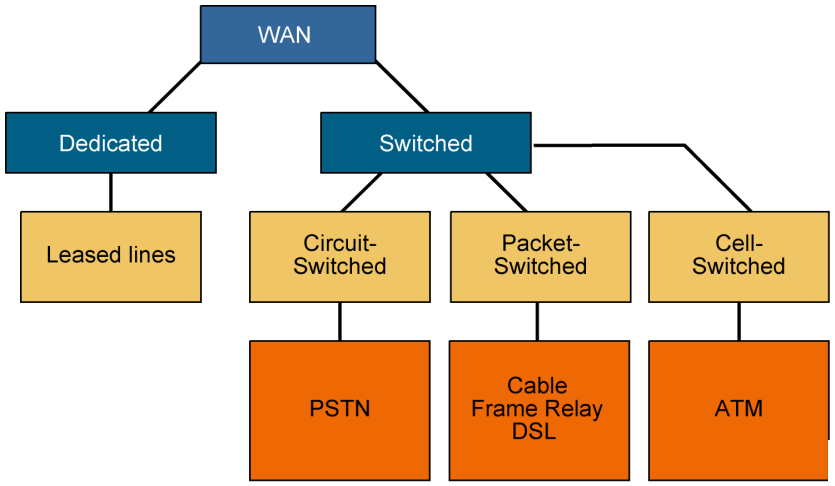
- **HDLC**
- **PPP**
- **Framerelay**
- **ATM**



شکل 8-1 ساختار یک شبکه WAN

[1] Wide Area Network

تکنولوژی‌های WAN



شکل 8-2 تکنولوژی مورد WAN استفاده

Dedicated: یعنی به‌صورت اختصاصی فقط یک کاربر استفاده می‌کند. خطوط Leased line در این دسته قرار دارند. این خطوط از جهت اقتصادی پرهزینه هستند. پهنای باندی که در Leased line اختصاص داده می‌شود مختص یک کاربر بوده و اگر از این پهنای باند استفاده‌ی کامل شود یا نه، باید هزینه کامل پرداخت شود.

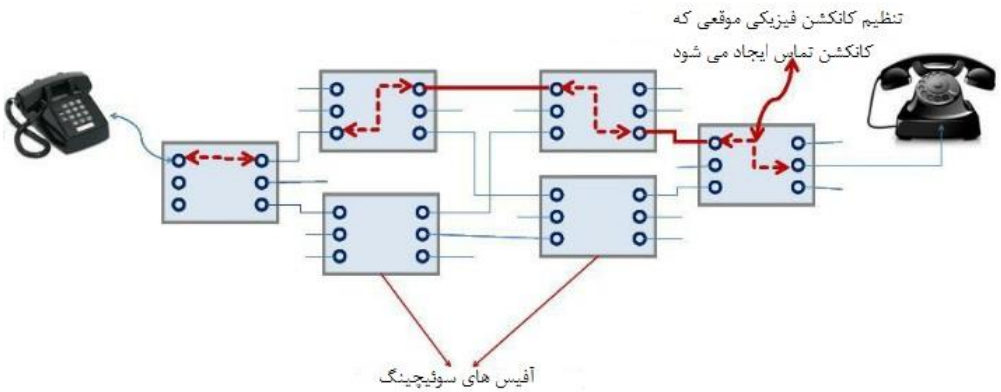
Switched: در این حالت استفاده از پهنای باند به‌صورت اشتراکی می‌باشد و به 3 دسته‌ی زیر تقسیم می‌شود:

- **Circuit-Switched**
  - تکنیک استفاده شده برای ایجاد یک ارتباط شبکه‌ای است.
  - برای تماس‌های تلفنی عادی استفاده می‌شود.
  - اجازه می‌دهد تا تجهیزات ارتباطی و مدارات بین کاربران به اشتراک گذاشته شود.
  - قبل از ارتباط اولیه یک مسیر (کانال اختصاصی) با استفاده از پروتکل سیگنالینگ به‌طور جداگانه رزرو می‌شود.
  - برای ارتباطات Half Duplex یک کانال و برای ارتباطات Full Duplex دو کانال اختصاص داده می‌شود.
  - انتقال داده فقط بعد از فاز ایجاد مسیر انجام می‌شود.
  - همه‌ی داده‌ی یک Session از طریق مسیر یکسان عبور می‌کند.
  - بقیه‌ی کاربران تا زمانی که Session کامل شود، نمی‌توانند از مسیر استفاده کنند.
  - اطلاعات سیگنالینگ همراه با داده ارسال نمی‌شود.
  - مسیر بعد از انتقال داده با استفاده از پروتکل سیگنالینگ آزاد می‌شود.
  - برای ارتباطات صوتی استفاده می‌شود.

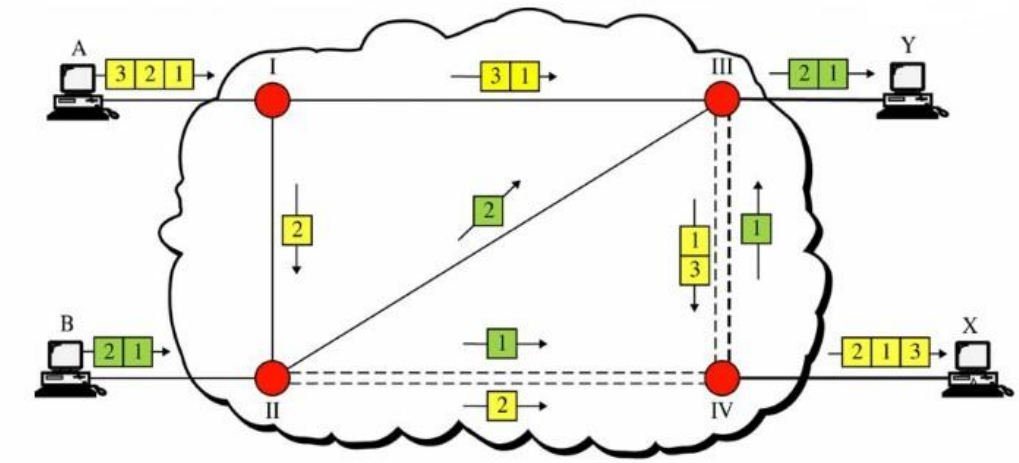
- اتلاف پهنای باند وجود دارد (پهنای باند ثابت است).
- تاخیر تنظیم تماس وجود دارد.

- **Packet-Switched**
  - پروسه‌ی انتقال داده در واحدهای کوچکتری به‌نام Packet انجام می‌شود.
  - داده‌ی انتقالی به واحدهای کوچکتری شکسته می‌شود.
  - از Packet های با طول متغیر استفاده می‌کند.
  - Packet ها در یک زمان از مسیرهای مختلف ارسال می‌شوند.
  - بعد از اینکه Packet ها به مقصد رسیدند، مجددا در ترتیب مناسبی برای ایجاد پیام بهم وصل می‌شوند.
  - هر Packet شامل هدر و داده است.
  - هر Packet اطلاعات سیگنالینگ در تشکیل آدرس مبدا و مقصد در هدر بسته را دارد.
  - اطلاعات سیگنالینگ دستگاه‌های تبادل داده برای مسیر Packet ها استفاده می‌شود.
  - دستگاه‌های تبادل همانند روترها و سوئیچ ها یک رویکرد ذخیره و ارسال برای انتقال بسته‌ها از یک پورت ورودی به یک پورت خروجی استفاده می‌کنند.
  - قبل از ارتباط اولیه هیچ مسیر اختصاصی بین فرستنده و گیرنده ایجاد نمی‌شود.
  - اتلاف پهنای باند وجود ندارد (پهنای باند پویا است).
  - تاخیر انتقال بسته وجود دارد.
  - شامل دو نوع مختلف زیر می‌باشد:
    - **Virtual Circuit:** اصولا در لایه‌ی پیوند داده (لایه 2) استفاده می‌شود.
    - **Datagram:** در لایه‌ی شبکه و پیوند داده مورد استفاده واقع می‌شود.

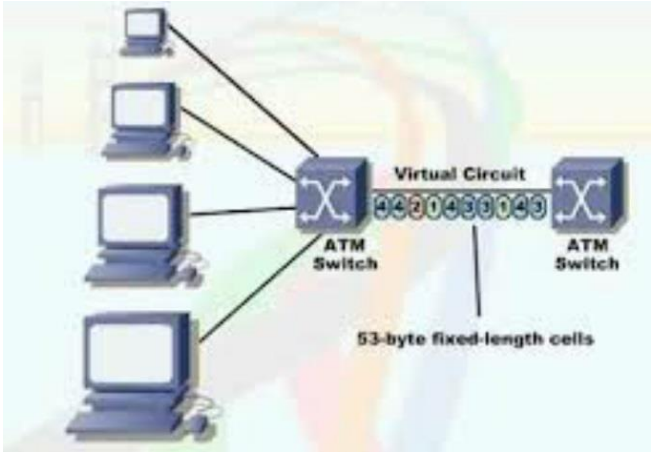
- **Cell-Switched**
  - شبیه به Packet-switching عمل می‌کند.
  - از Packet های با طول ثابت 53 بایتی برای انتقال داده استفاده می‌کند که 5 بایت برای هدر رزرو شده است.
  - این نوع تکنولوژی درون شبکه‌های یکپارچه مبتنی بر سلول همانند شبکه‌های ATM یافت می‌شود.
  - انواع مختلف داده همانند: صوت، ویدئو و داده به‌کار برده می‌شود.
  - یک نوع تکنولوژی با پهنای باند و سرعت بالا است.
  - کارایی این نوع تکنولوژی بالا است.
  - پهنای باند به‌صورت پویا بوده، مقیاس‌پذیر می‌باشند.



شکل 8-3 شبکه های Circuit Switching



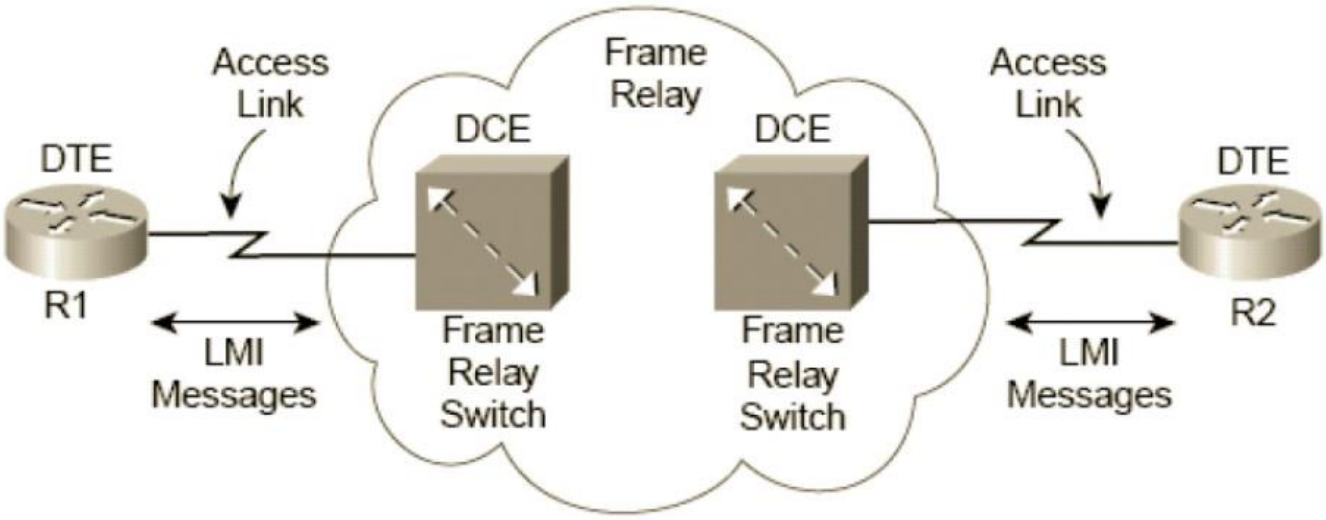
شکل 8-4 شبکه های Packet Switching



شکل 8-5 شبکه های Cell Switching

Frame Relay

Frame-relay در provider برای سرویس WAN استفاده می شود. درحقیقت یک سری سوئیچ‌هایی هستند که در مرکز مخابراتی قرار گرفته‌اند و روترها را در نقاط مختلف بهم کانکت می‌کنند. این سوئیچ‌ها باید در مراکز مختلف مخابراتی قرار بگیرند تا دسترسی ارتباطی به شبکه فراهم شود.



شکل 8-6 نمونه‌ای از سوئیچ‌های Frame Relay و ارتباط با روترها

نکات

- مخابرات همیشه DCE و روترها DTE خواهند بود.

- سوئیچ های مخابراتی برای ارتباط روترها باید داخل سوئیچ هایشان یک map بنویسند.
- به map ای که نوشته می‌شود VC (virtual circuit) می‌گویند.
- VC در مخابرات تعریف می‌شود.
- فقط یک اینترفیس سریال روتر برای اتصال با سایت‌های متعدد با استفاده از VC ها استفاده می‌شود.
- VC ها ارتباط Full Duplex را فراهم می‌کنند.
- بعد تعریف VC، مخابرات از VC مشخصه ای با نام DLCI استخراج می‌کند.
- DLCI[1] :
  - کدی است که به مشتری داده می شود تا روی روتر تنظیم کند که به سوئیچ مخابراتی وصل شود.
  - برای شناسایی هر VC روی یک اینترفیس فیزیکی استفاده می‌شوند.
  - هر VC یک شماره DLCI واحد دارد.
  - سوئیچ‌های Framerelay از شماره DLCI برای ارسال داده به شبکه‌ی راه دور استفاده می‌کنند.
  - محدوده DLCI از 16 تا 1007 است.
- LMI Message[2] :
  - پروتکلی است که ترافیک بین DTE و DCE را مدیریت می کند.
  - استانداردهای LMI: Cisco، ANSI، Q933a
  - LMI باید بین روتر و سوئیچ Framerelay یکسان باشد.

توپولوژي‌هاي پياده سازي Frame Relay

Star(Hub-and-Spoke)-1

- این نوع توپولوژی دارای یک هاب یا روتر مرکزی است که سایت‌های از راه دور به این سایت مرکزی متصل می‌شوند.
- کمترین تعداد VC در این توپولوژی مورد نیاز است.

[1] Data Link Connection Identifier
[2] Local Management Interface

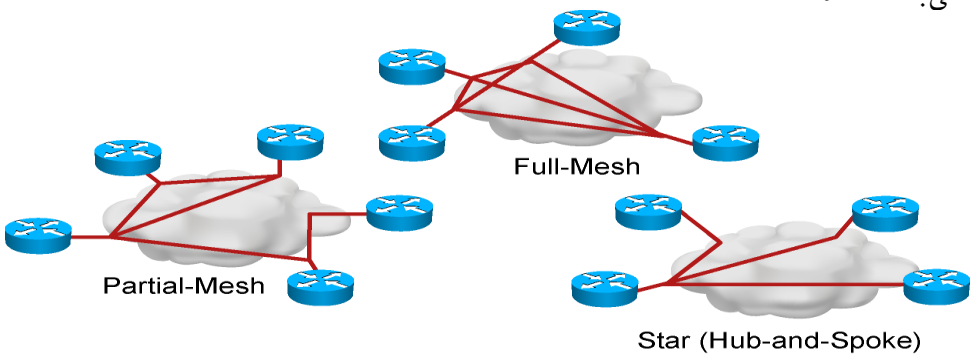
- روتر مرکزی با نام Hub و بقیه‌ی روترها با نام Spoke شناخته شده اند.
- مدیریت این نوع توپولوژی آسان است.
- اگر روتر مرکزی خراب شود و یا down شود هیچ کدامیک از روترها نمی‌توانند با یکدیگر ارتباط برقرار کنند.
- توپولوژی مقیاس‌پذیری نمی‌باشد.

Full-Mesh -2

- در این نوع توپولوژی همه‌ی سایت‌ها به یکدیگر متصل می‌شوند.
- این مدل توپولوژی گران است.
- چون همه‌ی سایت‌ها به همدیگر متصل شده اند، دارای افزونگی می‌باشد.
- تعداد VCهای مورد نیاز از رابطه‌ی $\frac{n\times(n-1)}{2}$ به‌دست می‌آید که n تعداد گره‌ها است.

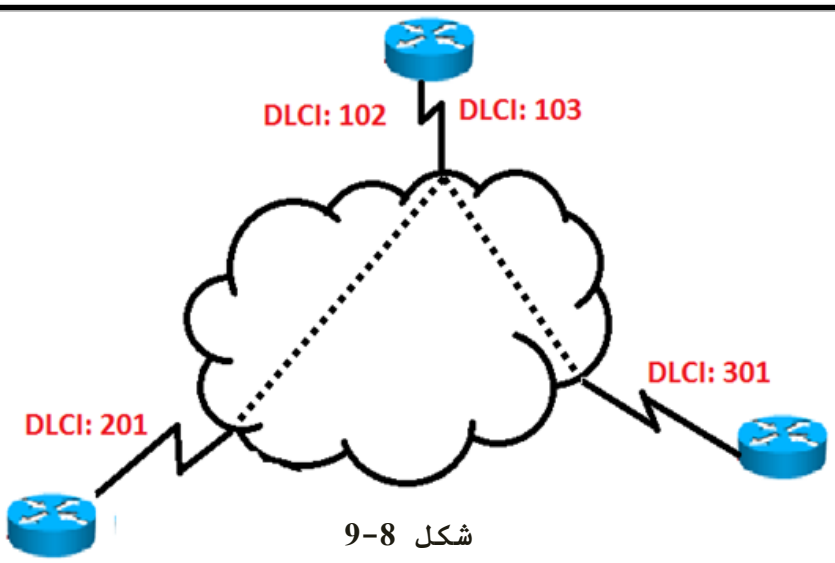
Partial-Mesh-3

- همه‌ی سایت‌ها دارای دسترسی مستقیم به یکدیگر نیستند.
- اتصال معمولا وابسته به الگوهای ترافیک درون شبکه است.
- تعداد VCهای مورد نیاز از رابطه‌ی $(n-1) \le x \le \frac{n\times(n-1)}{2}$ به‌دست می‌آید که x تعداد VC مورد نیاز است و n تعداد endpoint ها در شبکه می‌باشد.



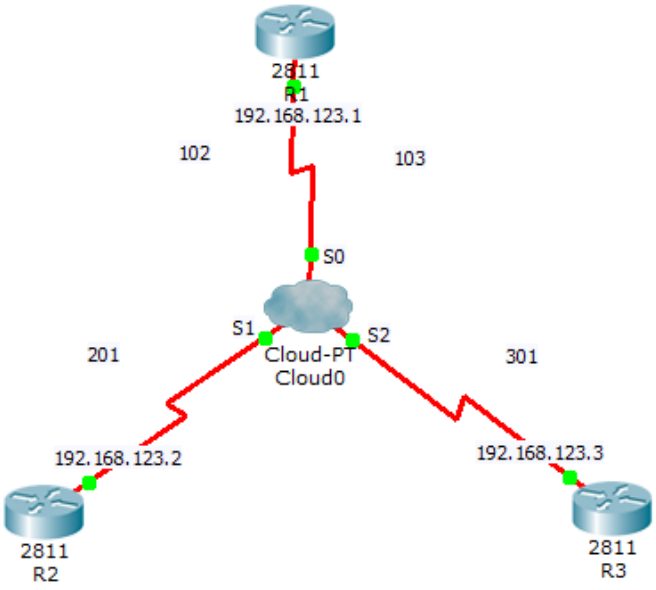
شکل 8-7 انواع توپولوژی‌های Frame-relay

نحوه‌ی کارکرد با frame-relay در Packet Tracer



شکل 8-9

در این حالت پورت ابر DCE میشود و با کابل Serial DTE باید روتر را به ابر وصل کنیم.



شکل 8-10 سناریوی

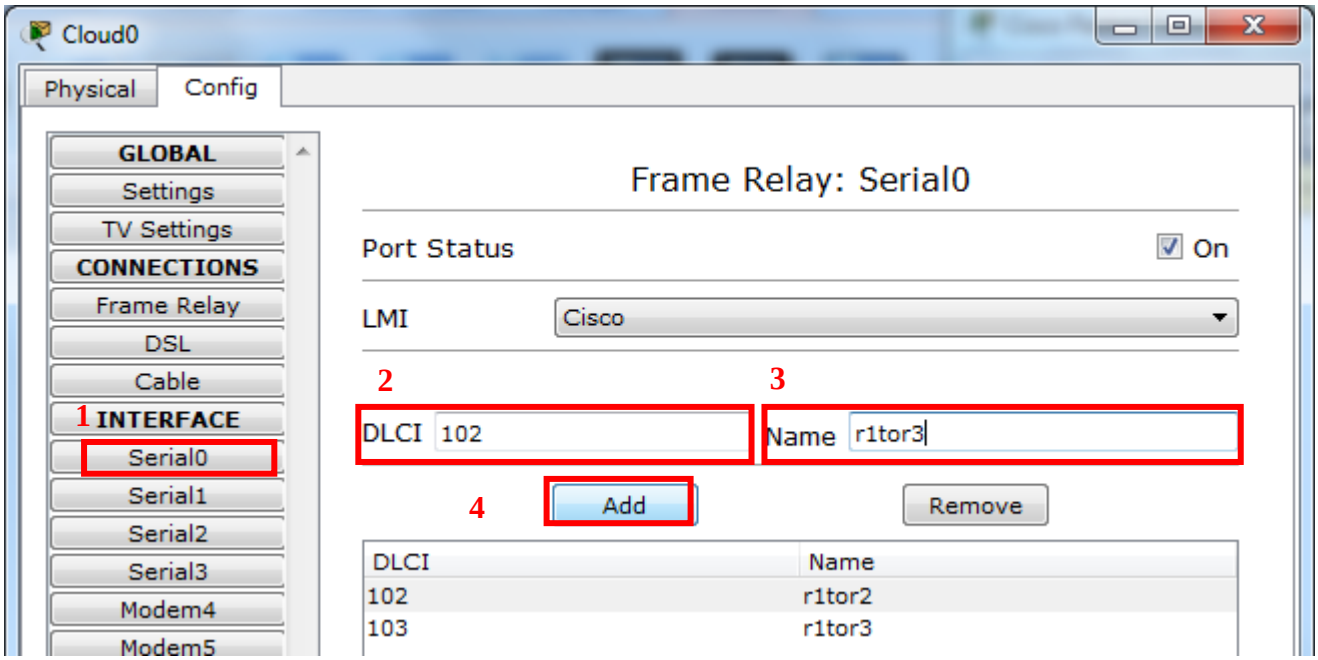
1	Router(Config)#**Show frame-relay map**

1-بر روي ابر کلید کرده و DLCI را از قسمت Config و Interface تعریف میکنیم.

a. Serial 0 را کلیک میکنیم.

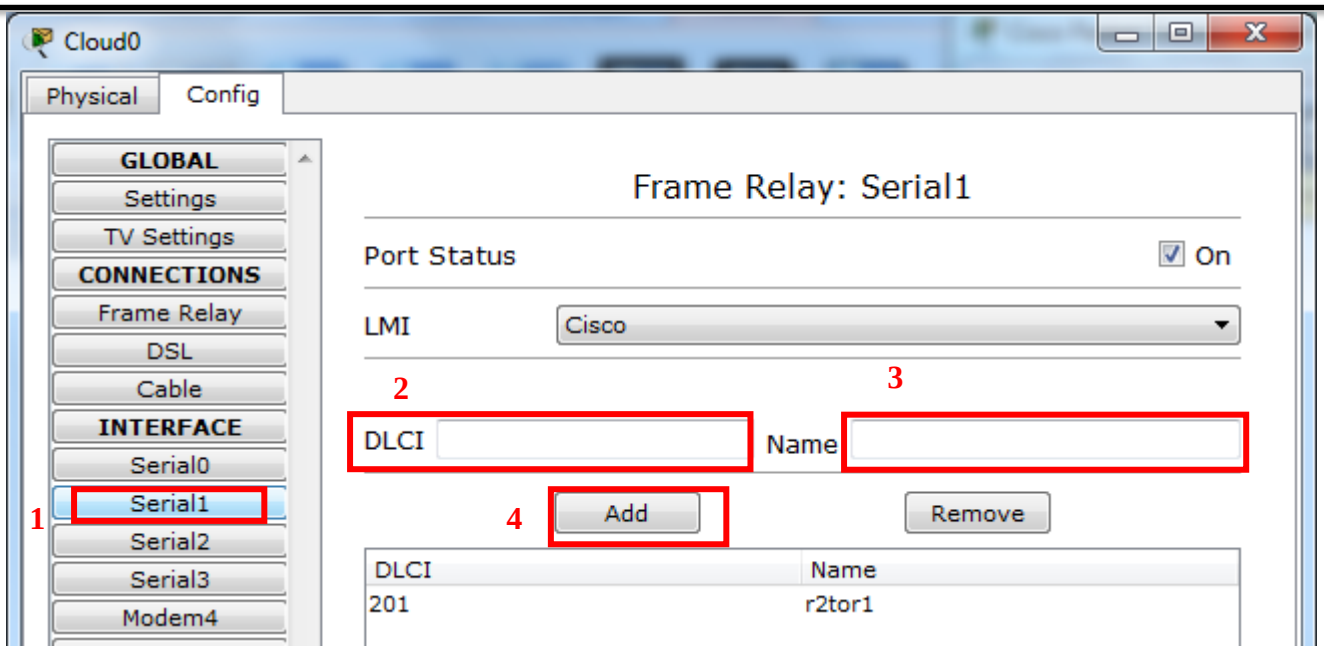
b. DLCI هائیکه به پورت سریال ابر متصل هستند را وارد میکنیم و براي آنها نام انتخاب کرده.

c. سپس در هر مرحله کلید ADD را میزنیم.



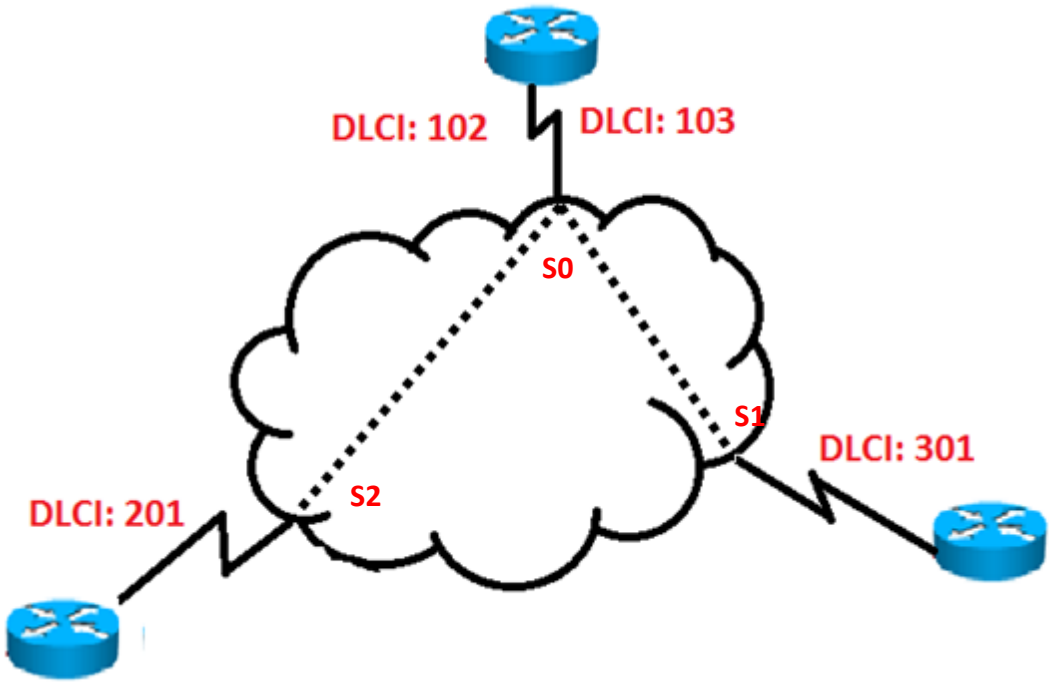
شکل 8-11 نحوه‌ی تعریف DLCI برای

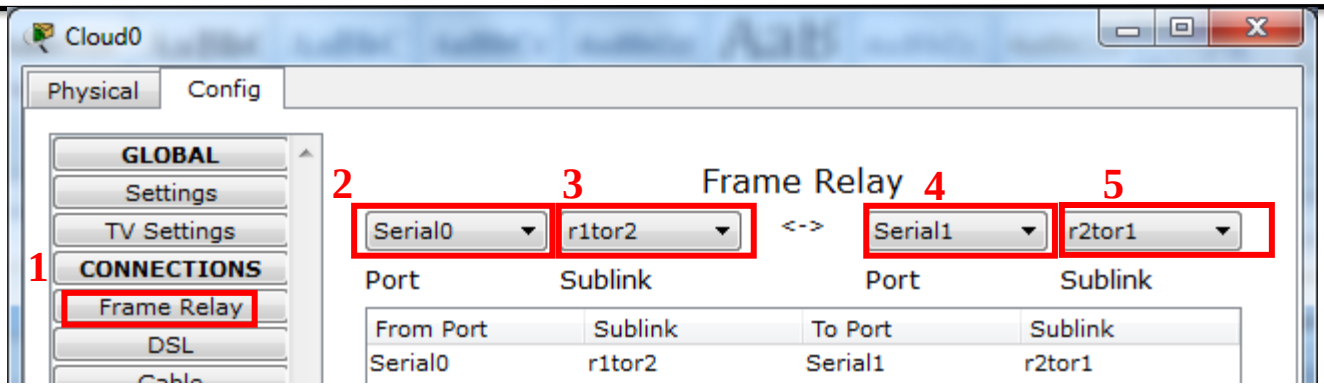
d. پورت Serial 1 را کلیک کرده و مانند بالا DLCI مرتبط به این پورت را Add میکنیم.



e. هچنین برای پورت serial2 نیز مراحل بالا را تکرار میکنیم.

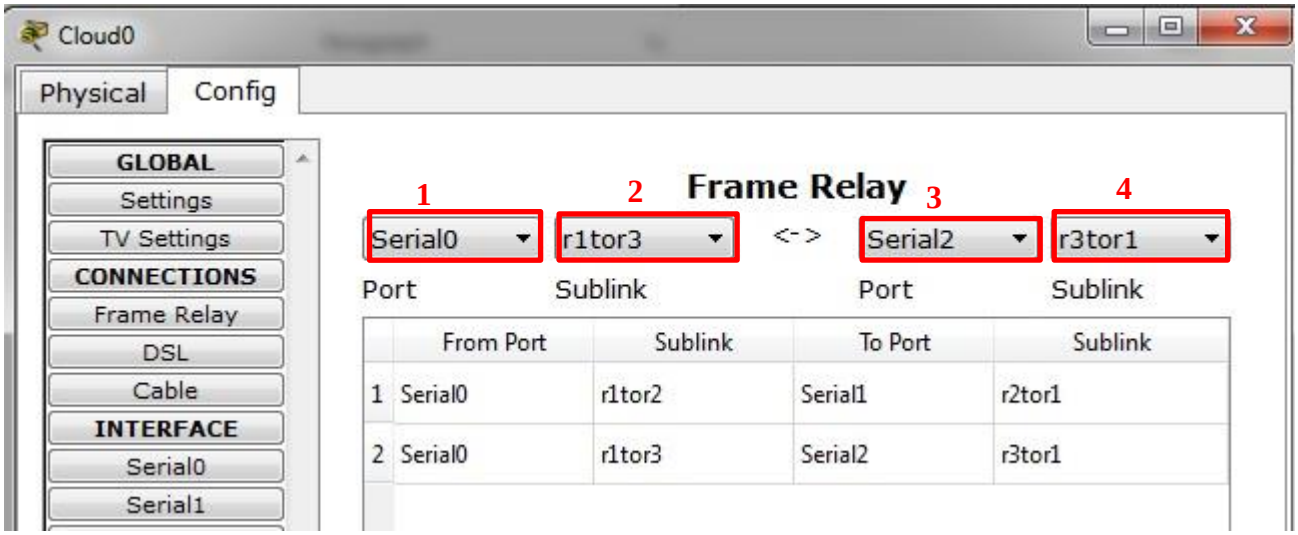
2- مجددا بر روي ابر كليك كرده و Frame Relay ها را دقیقا مطابق به شکل زیر تعریف میکنیم.





شکل 8-13 نحوه تعریف frame-relay بین S0 و S1

در سمت اول از پورت سریال Se0 ابر با نام r1tor2 و در سمت دیگر ابر از طریق پورت سریال Se1 با نام r2tor1 به روتر R2 متصل‌می شویم.



شکل 8-14 نحوه تعریف frame-relay بین S0 و S2

در سمت اول از پورت سریال Se0 ابر با نام r1tor3 و در سمت دیگر ابر از طریق پورت سریال Se2 با نام r1tor3 به روتر R3 متصل می شویم.

3- حال باید روترها را کانفیگ کنیم و به پورت‌های روتر IP بدهیم.

کانفیگ روترها:

R1

1	Router(Config)#**interface Serial0/0/0**
2	Router(Config-if)#**ip address 192.168.123.1 255.255.255.0**
3	

4	Router(Config-if)#**encapsulation frame-relay**
5	Router(Config-if)#**frame-relay map ip 192.168.123.2 102 broadcast**
6	Router(Config-if)#**frame-relay map ip 192.168.123.3 103 broadcast**
7	Router(Config-if)# **no shutdown**

R2

1	Router(Config)#**interface Serial0/0/0**
2	Router(Config-if)#**ip address 192.168.123.2 255.255.255.0**
3	
4	Router(Config-if)#**encapsulation frame-relay**
5	Router(Config-if)#**frame-relay map ip 192.168.123.1 201 broadcast**
6	Router(Config-if)#**frame-relay map ip 192.168.123.3 201 broadcast**
7	Router(Config-if)#**no shutdown**

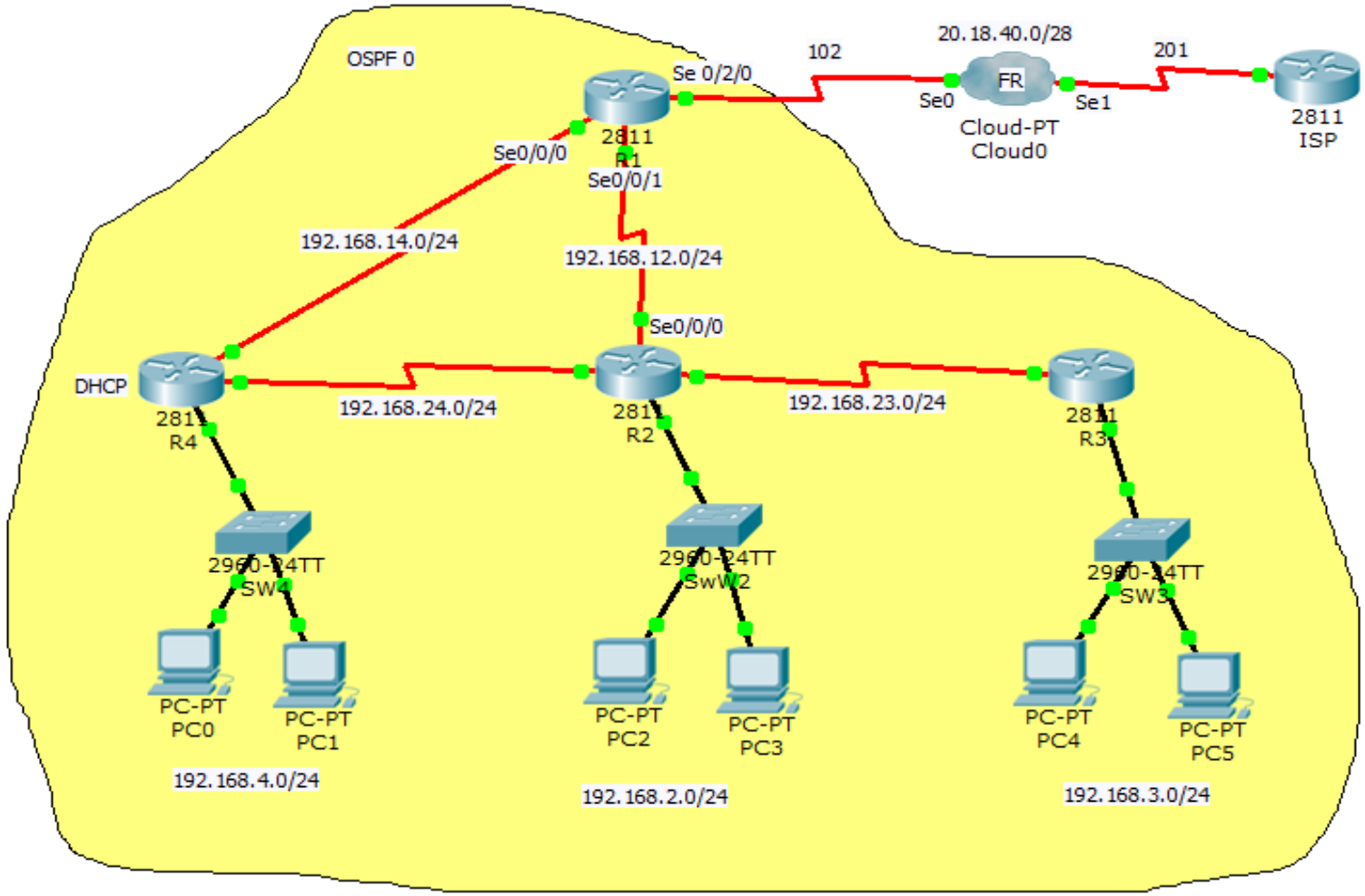
R3:

1	Router(Config)#**interface Serial0/0/0**
2	Router(Config-if)#**ip address 192.168.123.3 255.255.255.0**
3	
4	Router(Config-if)#**encapsulation frame-relay**
5	Router(Config-if)#**frame-relay map ip 192.168.123.1 301 broadcast**
6	Router(Config-if)#**frame-relay map ip 192.168.123.2 301 broadcast**
7	Router(config-if)#**no shutdown**

نكته: روتر همه را به غير از خودش Ping مي‌كند، براي اينكه خودش را هم Ping كند بايد يك Map ديگر هم بنويسيم:

1	Router(Config)#**interfce serial 0/0/0**
2	Router(Config-if)# **frame-relay map ip 192.168.123.1 102**
3	
4	Router#**ping 192.168.123.1**

سناریو NAT & PAT & Frame Relay



شکل 8-15 سناریو NAT & PAT & Frame Relay

- با توجه به دیاگرام شکل (8-11) به سوالات زیر پاسخ دهید:

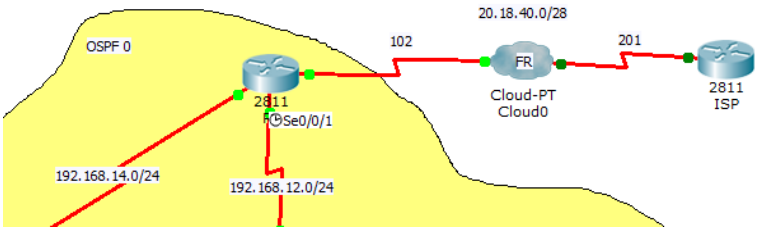
1. با استفاده از IPهاي داده شده به اختصاص IP پرداخته و در روتر R4 از سرویس DHCP استفاده نمایید.
2. با استفاده از پروتکل‌هاي Frame-Relay ارتباط روتر R1 با ISP را برقرار نموده و از DLCI هاي داده شده استفاده نمایید (102 و 201).
3. پروتکل مسیریابي OSPF در Area 0 را پیاده‌سازي کرده و ارتباط R1 با R2 را به وسیله‌ي مکانیزم احراز هویت MD5 راه اندازي شود.
4. با استفاده از مکانیزم PAT دسترسي کاربران سوئیچ SW3 را نسبت به ISP فراهم نمایید.

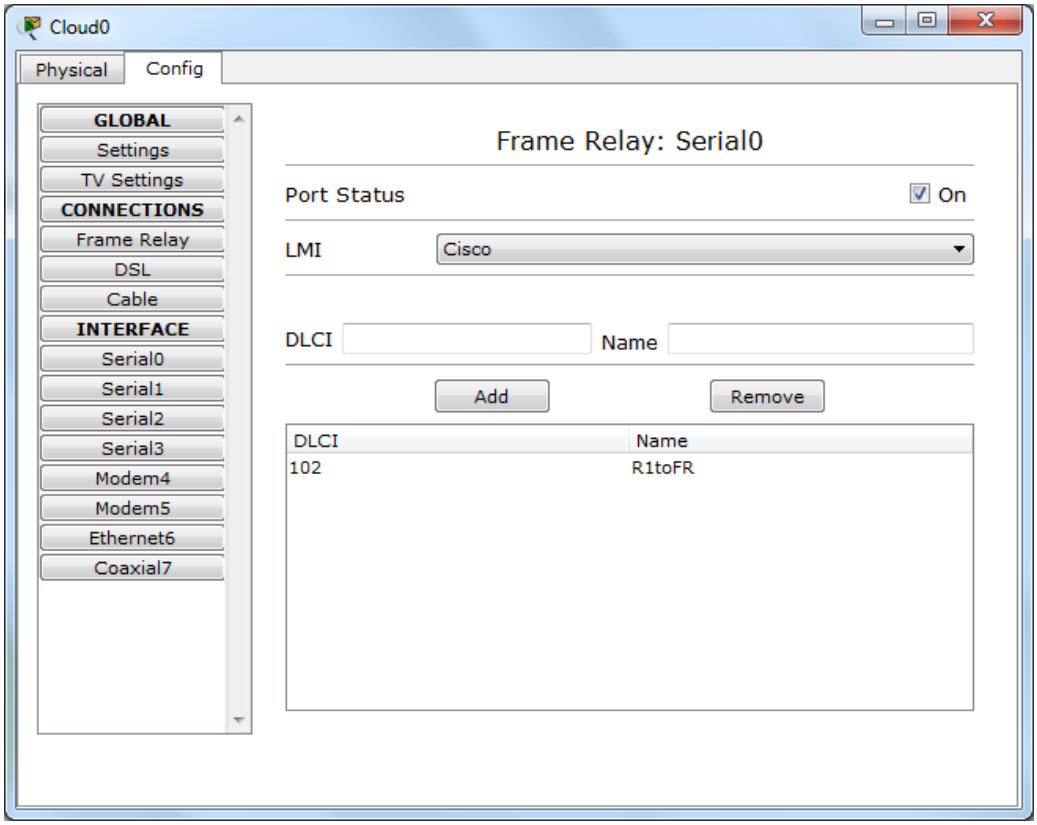
جواب سوال 1: با استفاده از IPهاي داده شده به اختصاص IP پرداخته و در روتر R4 از سرویس DHCP استفاده نمایید.

R4:

```
1  R4(config)#ip dhcp pool TEST
2  R4(dhcp-config)#network 192.168.4.0 255.255.255.0
3  R4(dhcp-config)# default-router 192.168.4.1
5
6  R4(config)#router ospf 1
7  R4(config-router)# network 192.168.14.1 0.0.0.0 area 0
8  R4(config-router)# network 192.168.24.1 0.0.0.0 area 0
9  R4(config-router)# network 192.168.4.1 0.0.0.0 area 0
```

جواب سوال 2: با استفاده از پروتکل‌هاي Frame-Relay ارتباط روتر R1 با ISP را برقرار نموده و از DLCI هاي داده شده استفاده نمایید (102و 201).





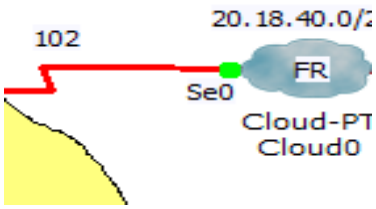
شکل 8-16 تنظیم

بر روي ابر Cloud 0 كليك كرده و وارد بخش Config آن مي شويم.
LMI را چون از تجهيزات Cisco استفاده مي‌كنيم ==> Cisco انتخاب مي‌كنيم.

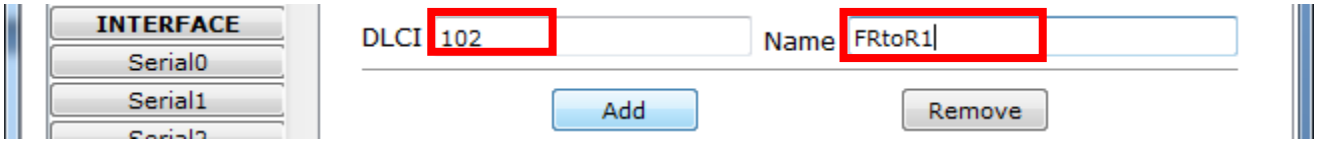
شکل 8-17 انتخاب

سپس DLCI ها را طبق شكل وارد مي‌كنيم:
از قسمت زير:

<u>تنظيمات پورت سريال صفر (Se0) ابر:</u>

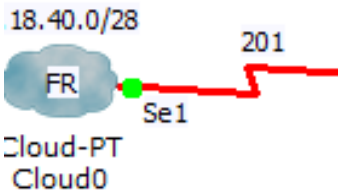


1- Cloud 0> Config> INTERFACE> Serial0
2- DLCI: 102, Name: FrtoR1 مربوطه و را وارد مي‌كنيم
   نام دلخواه DLCI
3- Add
4-

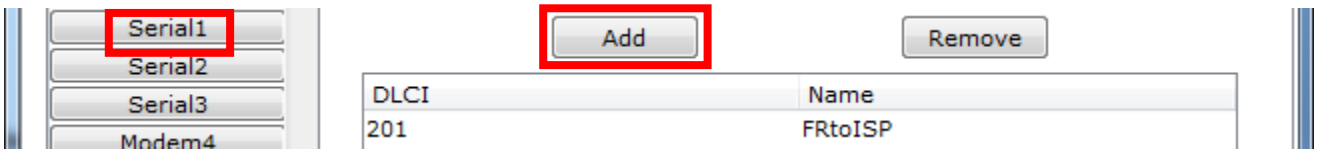


شکل 8-18 تنظیم

تنظیمات پورت سریال صفر (Se1) ابر:



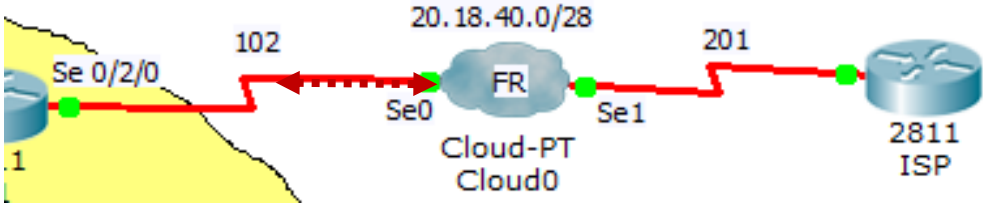
1. Cloud 0> Config> INTERFACE> Serial1
2. DLCI: 201,Name:FRtoISP مربوطه و نام دلخواه را انتخاب کنیم DLCIمی
3. Add

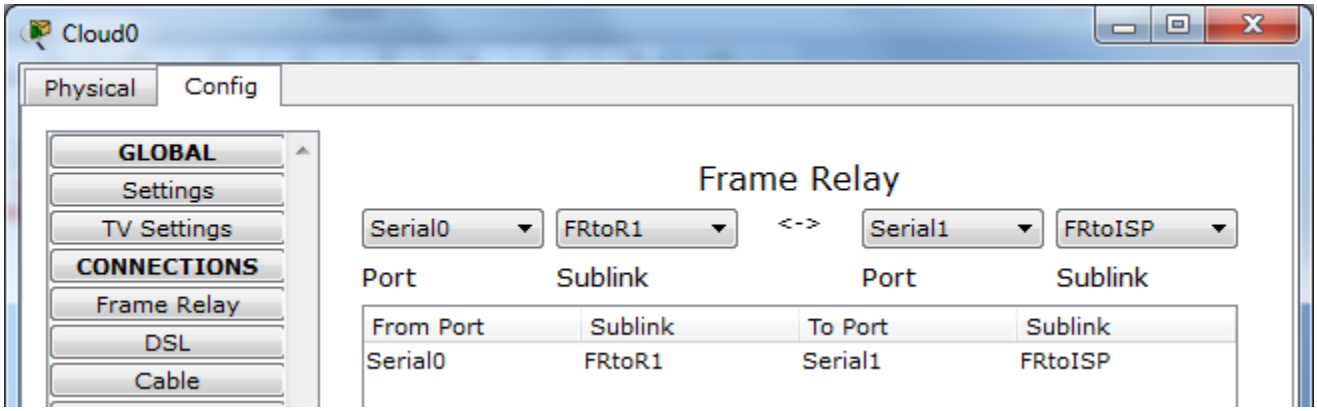


شکل 8-19 تنظیم DLCI:201

تنظیمات ارتباط Frame Relay

5- Cloud 0> Config>Frame Relay
6- ارتباطات را تعریف میکنیم.
7- از پورت سریال صفر ابر با مشخصات 102 به پورت سریال 1 ابر با نام 201 متصل شده ایم
8- Add





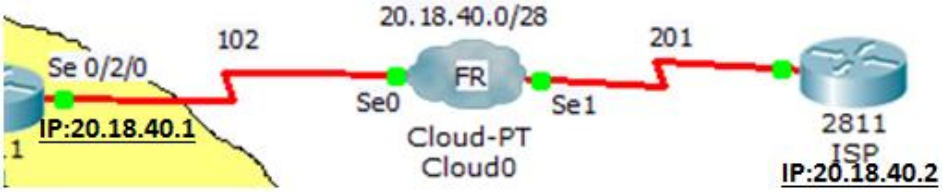
شکل 8-20 تنظیمات Frame-relay بین

R1:

```
1  R1(config)#interface Serial0/2/0
2  R1(config-if)#encapsulation frame-relay
3  R1(config-if)# ip address 20.18.40.1 255.255.255.240
4  R1(config-if)#frame-relay map ip 20.18.40.2 102 broadcast
5  R1(config-if)#no sh
6
7  R1(config)#interface Serial0/0/1
8  R1(config-if)#ip address 192.168.12.1 255.255.255.0
9  R1(config-if)#clock rate 64000
10 R1(config-if)#no sh
11 R1(config)#interface Serial0/0/0
12 R1(config-if)#ip address 192.168.14.2 255.255.255.0
13 R1(config-if)#clock rate 64000
14 R1(config-if)#no sh
```

که از طریق آن به سمت مقابل IP طرف مقابل R1(config-if)#**frame-relay map ip** **DLCI اتصال می یابیم broadcast**

- خط 4: بدین معناست که روتر R1 از طریق DLCI: 102 به ISP با IP:20.18.40.2 متصل شده است.
- ما از روتر 1، با استفاده از DLCI:102 به ISP:20.18.40.2 ارتباط داریم.



ISP:

```
1  ISP(config)#interface Serial0/0/0
2  ISP (config-if)#ip address 20.18.40.2 255.255.255.240
3  ISP (config-if)#encapsulation frame-relay
4  ISP (config-if)#frame-relay map ip 20.18.40.1 201 broadcast
```

جواب سوال 3: پروتکل مسیریابي OSPF در Area 0 را پیاده‌سازي کرده و ارتباط R1 با R2 بوسیله‌ي مکانیزم احراز هویت MD5 راه اندازي شود.

تنظیمات روتر 1:

R1:

```
1  R1(Config)#router ospf 1
2  R1(config-router)#network 192.168.14.2 0.0.0.0 area 0
3  R1(config-router)#network 192.168.12.1 0.0.0.0 area 0
4  R1(config-router)# network 20.18.40.0 0.0.0.15 area 0
5
6  R1(Config)#interface Serial0/0/1
7  R1(Config-if)# ip ospf authentication-key CCNA
8  R1(Config-if)#ip ospf authentication message-digest
```

تنظیمات روتر 2 نیز همانند بالاست:

R2

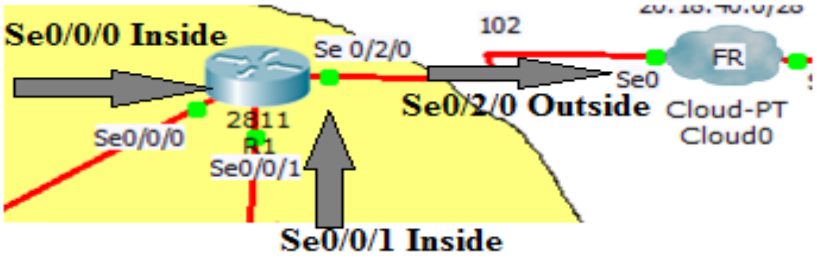
```
1  R2(Config)#router ospf 1
2  R2(config-router)#network 192.168.23.1 0.0.0.0 area 0
3  R2(config-router)#network 192.168.12.2 0.0.0.0 area 0
4  R2(config-router)#network 192.168.24.2 0.0.0.0 area 0
5  R2(config-router)#network 192.168.2.1 0.0.0.0 area 0
6
7  R1(Config)#interface Serial0/0/0
8  R1(Config-if)# ip ospf authentication-key CCNA
9  R1(Config-if)#ip ospf authentication message-digest
```

جواب سوال 4: با استفاده از مکانیزم PAT دسترسي کاربران سوئیچ SW3 را نسبت به ISP فراهم نمایید.به ترتیب:

1. نوشتن ACL

1	R1(config)#**access-list 1 permit 192.168.3.0 0.0.0.255**

2. تعریف inside و Outeside ها در روتر 1



3. نوشتن دستور PAT:

1	R1(config)#**interface Serial0/2/0**
2	R1(config-if)#**ip nat outside**
3	R1(config)#**interface Serial0/0/1**
4	R1(config-if)#**ip nat inside**
5	R1(config)#**interface Serial0/0/0**
6	R1(config-if)#**ip nat inside**
7	
8	R1(config)#**access-list 1 permit 192.168.3.0 0.0.0.255**
9	R1(config)#**ip nat inside source list 1 interface Serial0/2/0 overload**

اینترفیس‌های سریال در WAN

$$\textbf{\textit{Serial Interface}}: \begin{cases} HDLC \\ PPP \begin{cases} Chap \\ PAP \end{cases} \end{cases}$$

- **HDLC:** به صورت پیش فرض روي پورت‌هاي سریال Run مي‌باشد.
- **Chap:** امنیت بالایي دارد. تمامي رمزها، Encrypt شده هستند.
- **PAP:** امنیت پایيني دارد و چون پسوردهایي که بین روترها تبادل مي‌گردد بدون رمزنگاری است و به علت امنیت پایینش از آن استفاده نمي‌شود.
- مزیت PPP، Feature هاي بیشتري را نسبت به HDLC ساپورت مي‌کند. مثل Authentication.

- **Configuration HDLC Encapsulation:**

	RouterX(config-if)# **encapsulation hdlc**

- **Configuration PPP Encapsulation:**

	RouterX(config-if)# **encapsulation ppp**

- **Configuration PPP and Authentication:**

1	RouterX(config-if)# **encapsulation ppp**
2	
3	RouterX(config)# **hostname *name***
4	RouterX(config)# **username *name* password *password***
5	RouterX(config-if)# **ppp authentication {chap | chap pap | pap chap | pap}**

- خط 1: فعال کردن PPP
- خط 2: انتخاب نام براي روتر
- خط 3: انتخاب یوزر و پسورد براي روتر (که Username همان Hostname روتر مقابل است) و پسورد بین دو روتري که مي‌خواهیم PPP راه اندازي نماییم مشترک مي‌باشد.

PPP and CHAP Configuration

شکل 8-21 مثالی از پیکربندی CHAP

```
1  RouterX(config)# hostname RouterX
2  RouterX(config)# username RouterY
3  password 1234
4
5  RouterX(config)# int serial 0
6  RouterX(config-if)# ip address 10.0.1.1
7  255.255.255.0
8  RouterX(config-if)# encapsulation ppp
9  RouterX(config-if)# ppp authentication
   chap
```

```
1  RouterY(config)# hostname RouterY
2  RouterY(config)# username RouterX
3  password 1234
4
5  RouterY(config)# int serial 0
6  RouterY(config-if)# ip address 10.0.1.1
7  255.255.255.0
8  RouterY(config-if)# encapsulation ppp
9  RouterY(config-if)# ppp authentication
   chap
```

- خط 1: نام روتر را تعریف میکنیم.
- خط 2: در قسمت username، نام روتر مقابل را مینویسم و در قسمت password، پسورد مشترك بين دو روتر را انتخاب مي كنيم.
- خط 6: به پورتهاي طرفين IP اختصاص ميدهيم.

خطایابی PPP

```
1  RouterX# show interface s0
2  Serial0 is up, line protocol is up
3    Hardware is HD64570
.    Internet address is 10.140.1.2/24
.    MTU
24   LCP Open
     Open: IPCP, CDPCP
     …

30   RouterX# debug ppp authentication
     4d20h: %LINK-3-UPDOWN: Interface Serial0, changed state to up
     4d20h: Se0 PPP: Treating connection as a dedicated line
     4d20h: Se0 PPP: Phase is AUTHENTICATING, by both
     4d20h: Se0 CHAP: O CHALLENGE id 2 len 28 from ”left"

     RouterX# debug ppp negotiation
```

- خط 24 : چك كـردن مـكـانـيـزم Authentication PPP .
- خط 30 : بـراي Debug كـل پـروتـكـل PPP.

فصل 9

Wireless

وایرلس

همان‌طوری که قبلا ذکر شده، شبکه‌های سیمی[1] از دیدگاه سیسکو دارای 4 جزء زیر می‌باشند:

- **End system**
- **Inter connect**
- **Switch**
- **Router**

شبکه‌های بی‌سیم[2] هم دارای 4 جزء زیر می‌باشند:

- **End system**
- **Wireless inter connect**
- **Access point[3]:** دستگاه‌هایی هستند که ساختار سوئیچ ها را دارند یعنی با mac address ها کار می‌کنند.
- **Router:** ماژول‌های وایرلس بر روی روترها قرار می‌گیرد.

اصلی‌ترین بحث در شبکه‌های وایرلس بحث امواج می‌باشد. در شبکه‌های وایرلس از محدوده امواج رادیویی[4] استفاده می‌شود. امواج رادیویی دو range مجاز 2.4 و 5 گیگاهرتز را برای این شبکه‌ها مشخص کرده‌اند.

IEEE استاندارد 802.11 را برای شبکه‌های وایرلس تخصیص داده است که حاوی زیر مجموعه های زیر می‌باشد:

- **802.11a**
- **802.11b**
- **802.11g**
- **802.11n**
- **802.11ac**

[1] wired
[2] wireless
[3] AP
[4] Radio frequency

نکات

- در شبکه‌های وایرلس زمانی که از مرکز انتشار امواج فاصله گرفته شود به ازای فاصله‌ای که گرفته می‌شود، محدوده که افزایش می‌یابد، rate سرعت کاهش می‌یابد.
- در 802.11n که wifi و wimax وجود دارد، وقتی از سمت wifi به سمت wimax حرکت می‌کنیم، علاوه بر کاهش سرعت قابلیت mobility هم وجود دارد (اصلی‌ترین قابلیت wifi به wimax همین mobility می‌باشد).

توپولوژی‌های وایرلس

دو دسته توپولوژی اصلی در وایرلس وجود دارد:

- **Ad-hoc**

Ad-hoc معادل با workgroup می‌باشد. در workgroup یک کامپیوتر به کامپیوتر دیگر به‌صورت مستقیم می‌شود.
در ad-hoc هیچ واسط ارتباطی برای کانکشن وجود ندارد.

شکل 9-1 توپولوژی Ad-hoc

- **Infrastructure mode**

اگر workgroup تبدیل به domain شود، Infrastructure به‌وجود می‌آید.
Infrastructure به دو دسته تقسیم می‌شود:

- **BSS**[1]

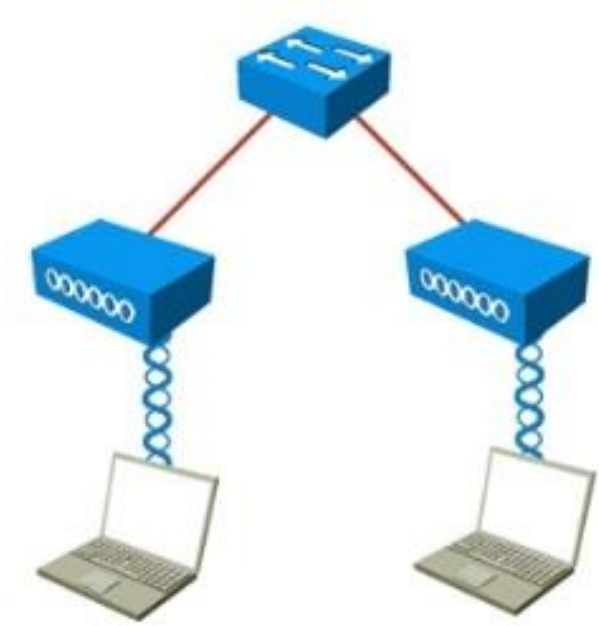
یک AP برای اتصال به یکدیگر کلاینت‌های سیار[2] از یا به منابع شبکه‌های سیمی استفاده می‌کنند (یک AP وجود دارد).

[1] Basic Service Set
[2] Mobile clients

شکل 9-2

- **ESS**[1]

حداقل دو AP وجود دارد.



شکل 9-3

در حالت ESS قابلیت اتصال AP ها به سوئیچ وجود دارد یعنی این ویژگی وجود دارد که شبکه ی سیمی در کنار شبکه‌ی وایرلس استفاده شود.

[1] Extended Service Set

پروتکل‌های امنیتی وایرلس

به دلیل media بودن امواج شبکه‌های وایرلس خیلی راحت می‌توان به این شبکه‌ها نفوذ کرد. به همین خاطر از سال 1997 میلادی پروتکل‌هایی برای امن کردن ارتباطات در شبکه‌های وایرلس به‌وجود آمد. در ابتدا که پروتکل‌های امنیتی طراحی شدند این پروتکل‌ها روی ساختار ارتباطی مکانیزم رمزنگاری[1] را به‌صورت پایه‌ای اجرا کردند.

در پروتکل‌های امنیتی بحث طول کلید[2] و basic و enterprise بودن سیستم‌های امنیتی اهمیت زیادی دارد. اگر سیستم‌های امنیتی به‌صورت basic در نظر گرفته شوند، معمولا از خود دستگاه برای بحث امنیت استفاده می‌شود اما اگر به صورت enterprise مطرح شود باید در کنار دستگاهی که وجود دارد از یک سرور مجزا برای افزایش کارایی[3] کار استفاده کرد. این سرورها، سرورهایی هستند که معمولا برای سیستم‌های احراز هویت به‌صورت مستقل عمل می‌کنند.

سیستم های احراز هویت دو پروتکل شناخته شده دارند:

- **RADIUS**
- **Tacacs+**

+Tacacs سروری است که اطلاعات احرازهویت کاربران را در خود نگه‌داری می‌کند (AP خودش را درگیر نمی‌کند). موقعی که یک کاربر قصد کانکت شدن را دارد، ابتدا اطلاعاتش به AP انتقال داده می‌شود، سپس AP اطلاعات را به سرور +tacacs می‌فرستد، سرور چک می‌کند اگر اطلاعات Ok بود به AP اعلام می‌کند که به اطلاعات اجازه دهد تا وارد شبکه شوند. در سیستم‌های enterprise این سرورها در کنار دستگاه‌های ارتباطی شبکه مثل AP ها استفاده می‌شوند.

اولین پروتکل امنیتی WEP بود که در سال 1997 به‌وجود آمد. این پروتکل از رمزنگاری پایه[4] استفاده می‌کرد. بعد از راه‌اندازی رمزنگاری پایه، چون شبکه‌ها بزرگتر می‌شدند باید چارچوب ساختار امنیتی را افزایش می‌داد بنابراین enterprise تعریف شد. بعد از تعریف enterprise یکسری از سرورها به‌وجود آمدند که برای مدیریت این سرورها

[1] Encryption
[2] Key length
[3] Performance
[4] Basic encryption

باید پروتکل‌های قوی‌تری معرفی می‌شدند، بنابراین پروتکل‌هایی همچون: 802.1X EAP، WPA و WPA2 معرفی شدند. فرق این پروتکل‌ها در طول کلید، الگوریتم‌های قوی‌تر، ساختارهای enterprise یا پشتیبانی از enterprise و basic در کنار هم و پشتیبانی از پروتکل‌های امنیتی بیشتری بود.

جدول 9-1 ارزیابی امنیت

WEP	802.1x EAP
▪ استفاده از رمزنگاری پایه ▪ ضعیف بودن احراز هویت ▪ کلیدها به صورت استاتیک و قابل شکستن هستند ▪ قابل گسترش نمی باشند	▪ کلیدها به صورت اتوماتیک بوده ▪ رمزنگاری در این پروتکل بهبود یافته است ▪ احراز هویت کاربران ▪ استفاده از سرور RADIUS
WPA	**802.11i/WPA2**
▪ Standardized ▪ رمزنگاری در این پروتکل بهبود یافته است ▪ احراز هویت کاربران قوی بوده	▪ استفاده از الگوریتم رمزنگاری قوی بنام AES ▪ احراز هویت ▪ مدیریت اتوماتیک کلیدها

فصل10

IPV6

IPV6

IPV6، نسل جدیدی از IP ها می‌باشد که بعد از IPV4 تعریف شده اند. دلیل تعریف کردن این آدرس‌ها اتمام آدرس‌های IPV4 بود. تفاوت‌های عمده از لحاظ ساختاری بین IPV4 و IPV6 عبارتند از:

- در IPV4، 4 Octet باینری وجود دارد (32 بیت آدرس) که ظرفیت آدرس‌ها 4294467295 بود.

IPV4	4Octet
11000000.10101000.11001001.01110001	
192.168.201.113	

معادل

- IPV6 در ابتدا به‌صورت 16 Octet باینری بود ولی به دلیل اینکه نوشتن 16 Octet باینری سخت بود به 8 Octet هگزا تبدیل شدند. ظرفیت IPV6: 3.4×10^{38} برآورد شده است.

IPV6	16Octet
11010001.11011100.11001001.01110001.11010001.11011100 11001100.01110001.11010001.11011100.11001001.01110001 11010001.11011100.11001001.01110001	
A524:72D3:2C80:DD02:0029:EC7A:002B:EA73	

معادل

ویژگی‌های متمایز IPV6 از IPV4

- **Autoconfiguration**
آدرس‌هایی که به‌صورت اتوماتیک تولید می‌شوند و نیاز به استفاده از DHCP و بحث‌های آدرس‌دهی ندارند.

- **End to End without Nat**
آدرس‌هایی که برای دسترسی به WAN نیاز به NAT ندارند.

- **No broadcast**
عدم استفاده از ساختارهای broadcast

- **Routing efficiency**
افزایش بازدهی در مسیریابی به این دلیل است که در ساختار مسیریابی IPV6 از unicast به‌صورت پیش فرض استفاده می‌شود (کمترین میزان پهنای باند اشغال می‌شود).

- **Dual stack**

استفاده‌ی همزمان بیش از یک IP بر روی اینترفیس(از هر دو IPV4 و IPV6 می‌توان استفاده کرد).

- **6 to 4 and manual tunnels**

اگر بستر ارتباطی IPV4 و IP هایی که استفاده می‌شود IPV6 باشد در این حالت از تونل 6 to 4 استفاده می‌شود که از طریق تونل، IP های V6 رد می‌شوند.

ساختار IPV6

فرمت IPV6 به‌صورت X:X:X:X:X:X:X:X می‌باشد که X یک فیلد هگزا دسیمال است(8Octet هگز). آدرس‌های هگز از 0-9 و A-F تعریف می‌شوند که A معادل عدد 10 و F معادل عدد 15 می‌باشد
مثال:

2031:0000:130F:0000:0000:09C0:876A:130B

اگر در IPV6 چندین Octet به‌صورت متوالی صفر بودند، می‌توان صفرها را حذف کرد و از "::" استفاده کرد(تعداد Octet های صفر باید بیشتر از یک باشد در غیر این صورت امکان‌پذیر نیست).

2031:0000:130F:0000:0000:09C0:876A:130B

درست

2031:0:130F::9C0:876A:130B

2031:0000:130F:0000:0000:09C0:876A:130B

اشتباه

2031::130F::9C0:876A:130B

FF01:0:0:0:0:0:0:1 → FF01::1
0:0:0:0:0:0:0:1 → ::1
0:0:0:0:0:0:0:0 → ::

انواع آدرس‌ها در IPV6

8 octet در مبنای 16 می‌باشد. $2^{\times}$

- **Unspecified**

آدرس‌هایی که به صورت 128/:: می‌باشند.
این نوع آدرس برای حالتی است که سیستم IP ندارد.

نکات:

- در IPV6، آدرس‌ها با mask: 255 نوشته نمی‌شوند بلکه با "/" نوشته می‌شوند.
- ماکزیمم آدرس در IPV6، "/128" می‌باشد

- **Loopback**

این آدرس‌ها به‌صورت 1/128:: می‌باشند (معادل 127.0.0.1 در IPV4).

- **Multicast**

ادرس‌هایی که به‌صورت FF00::/8 می‌باشند.
معادل ip های 224.0.0.0 تا 239.255.255.255 در IPV4 می‌باشد.

- **Link-local unicast**

این آدرس‌ها به فرمت FE80::/10 می‌باشند.
معادل IPی 169.254.0.0 در IPV4 می‌باشد. زمانی که کامپیوتر بخواهد از DHCP، IP بگیرد که DHCP خراب باشد در این حالت سیستم عامل IP از رنج 169.254.0.0 را اختصاص می‌دهد. سیستم عامل‌ها وقتی از این رنج IP می‌دهند، ارتباط شبکه داخلی وجود دارد اما ارتباط بیرونی وجود ندارد چون DHCP از کار افتاده است.

- **Site-local unicast**

آدرس‌هایی با فرمت FEC0::/10 می‌باشند.
معادل آدرس‌های private در IPV4 می‌باشند.

- **Global unicast**

هر آدرسی غیر از آدرس‌های ذکر شده در بالا در این دسته قرار می‌گیرند.
رنجی که فعلا در همه‌جا استفاده می‌شود 2000::/3 می‌باشد.

راه اندازی IPV6

```
1  R(config)#ipv6 unicast-routing
2
3  R(config-if)#ipv6 address ip address
```

- خط1: برای فعال کردن IPV6 حتما باید این دستور زده شود.

- خط3: با استفاده از این دستور به اینترفیس روتر IP داده می شود.

مثال1:

شکل 10-1 سناریو مثال 1

R1

1	R(config)#**ipv6 unicast-routing**
2	R(config)#**interface fa0/0**
3	R(config-if)#**ipv6 address 2001:db8:D1A5:C900::1/64**
4	R(config-if)#**no shutdown**

R2

1	R(config)#**ipv6 unicast-routing**
2	R(config)#**interface fa0/0**
3	R(config-if)#**ipv6 address 2001:db8:D1A5:C900::2/64**
4	R(config-if)#**no shutdown**

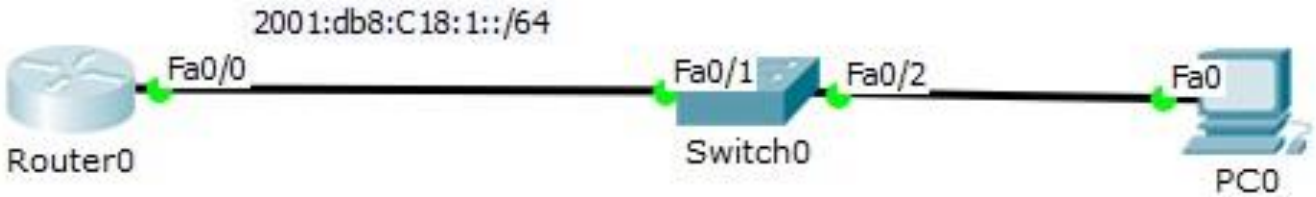
آدرس‌های eui-64

این آدرس‌ها در IPV6 به‌صورت اتوماتیک تولید می‌شوند. در این آدرس‌ها، آدرس‌های 128 بیتی به دو دسته‌ی 64 بیتی تقسیم می‌شود. 64 بیت آدرس global به‌صورت دستی وارد می‌شود سپس به‌صورت اتوماتیک 48 بیت mac address و FFFE (16بیت) در کنار هم قرار می‌گیرند و یک آدرس 128 بیتی تولید می‌شود.

دستور eui-64

	Router(config-if)#**ipv6 *address ipv6prefix/prefix-length* eui-64**

مثال2:



شکل 10-2 سناریو مثال 2

Router

```
1  Router(config)#ipv6 unicast-routing
2  Router(config)#int f0/0
3  Router(config-if)#ipv6 address 2001:db8:C18:1::/64 eui-64
4  Router(config-if)#no shutdown

   Router(config-if)#
   %LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

   %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to
   up
```

```
Router#sh ipv6 interface fastEthernet 0/0
FastEthernet0/0 is up, line protocol is up
    IPv6 is enabled, link-local address is FE80::200:CFF:FECD:1701
    No Virtual link-local address(es):
    Global unicast address(es):
      2001:DB8:C18:1:200:CFF:FECD:1701, subnet is 2001:DB8:C18:1::/64 [EUI]
    Joined group address(es):
      FF02::1
      FF02::2
      FF02::1:FFCD:1701
    MTU is 1500 bytes
    ICMP error messages limited to one every 100 milliseconds
    ICMP redirects are enabled
    ICMP unreachables are sent
    ND DAD is enabled, number of DAD attempts: 1
    ND reachable time is 30000 milliseconds
    ND advertised reachable time is 0 (unspecified)
    ND advertised retransmit interval is 0 (unspecified)
    ND router advertisements are sent every 200 seconds
    ND router advertisements live for 1800 seconds
    ND advertised default router preference is Medium
        Hosts use stateless autoconfig for addresses.
```

FFFE

Mac address

مسیریابی در IPV6

انواع مسیریابی در IPV6 عبارتند از:

- **Static**
- **RIPng**
- **OSPFV3**
- **IS-IS**
- **MP-BGP4**
- **EIGRPV6**

Static Routing

- مسیر بین دو دستگاه IPV6 را فراهم می‌کند.
- شبیه به Static Route در IPV4 است.
- آپدیت ها را تولید نمی‌کند.
- زمان پردازش را برای یک روتر IPV6 کاهش می‌دهد.
- در صورت تغییر توپولوژی شبکه یا از بین رفتن مسیر، نیاز به کانفیگ مجدد به‌صورت دستی دارد.

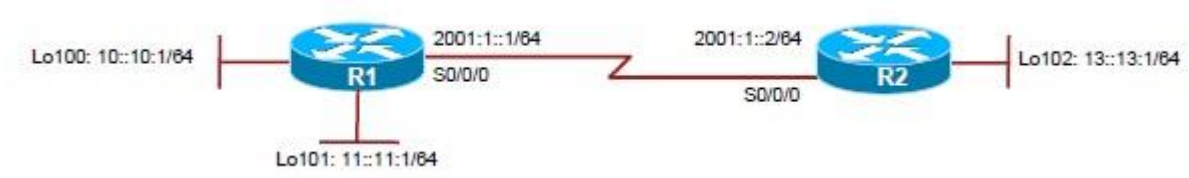
انواع Static Route در IPV6

- **Directly Attached**
- **Fully Specified**
- **Floating**
- **Default**

Directly Attached

1	Router(config)# **ipv6 route ipv6-prefix/prefix-length {ipv6- address | interface-type interface- number [ipv6- address] } [administrative- distance]**

- این نوع Static Route هنگامی که فقط اینترفیس خروجی مشخص باشد، ایجاد می‌شود.
- پارامتر ipv6- prefix/ prefix- length ، شبکه‌ی مقصد IPV6 و طول پیشوند آن را مشخص می‌کند.
- پارامتر interface-type interface- number، اینترفیسی که از طریق آن می توان به شبکه‌ی مقصد رسید را تعیین می‌کند.



شکل 10-3 سناریوی Directly Attached

```
1  R1(config)#ipv6 route 13::/64  S0/0/0
2  R1(config)#exit
```

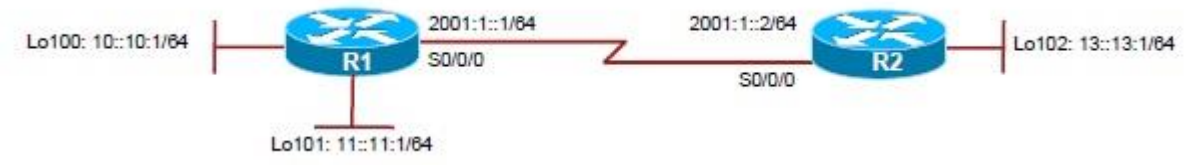
```
R1#show ipv6 route static
IPV6 Routing Table – 9 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route, M - MIPv6
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
       D - EIGRP, EX - EIGRP external

S      13::/64  [1/0]
       via :: , Serial0/0/0
```

یک Directly Attached برای شبکه‌ی 13::13:1/64 بر روی روتر R1 کانفیگ شده است.

Fully Specified

```
1  Router(config)#
   ipv6 route  ipv6-prefix/prefix-length  {ipv6- address | interface-type interface- number
   [ipv6- address] } [administrative- distance]
```

- این نوع Static Route هنگامی ایجاد می‌شود که :
  - اینترفیس خروجی
  - و IP ی همسایه مشخص باشد.



شکل 10-4 سناریو Fully Specified

1	R1(config)#**ipv6 route 13::/64 S0/0/0 2001:1::2**

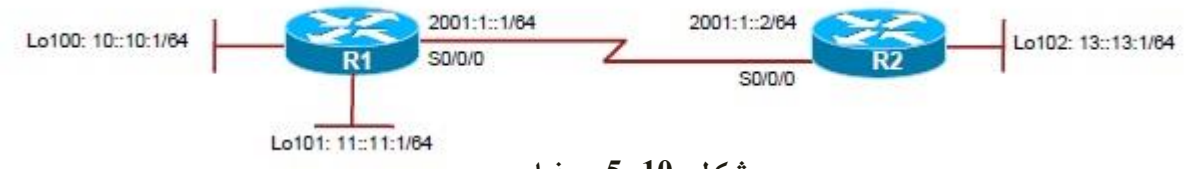
```
R1#show ipv6 route static
IPV6 Routing Table – Default- 8 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route, M - MIPv6
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
       D - EIGRP, EX - EIGRP external

S      13::/64  [1/0]
        via 2001:1::2 , Serial0/0/0
```

یک fully Specified برای شبکه‌ی 13::13:1/64 بر روی روتر R1 کانفیگ شده است.

Floating

1	Router(config)# **ipv6 route ipv6-prefix/prefix-length {ipv6- address | interface-type interface- number [ipv6- address] } [administrative- distance]**

- این نوع Static route معمولا هنگامی کانفیگ می‌شود که مسیرهای متعدد برای شبکه‌ی مقصد وجود داشته باشد و یک مسیر نسخه‌ی پشتیبان فعال برای پشتیبانی از مسیرهای کشف شده IGP مورد نیاز است.
- پارامتر administrative-distance، ارزش مسیر را مشخص می‌کند که باید نسبت به IGP در جدول مسیریابی بالاتر باشد.



شکل 10-5 سناریوی Floating

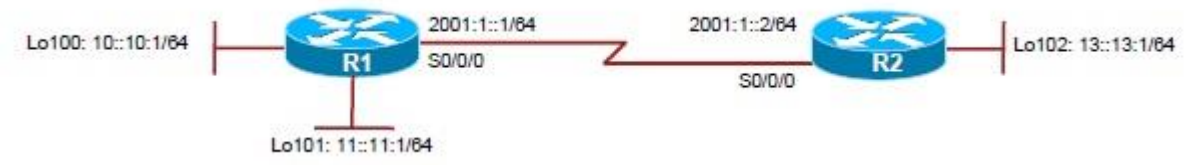
1	R1(config)#**ipv6 route 13::/64 130**

R1 کانفیگ شده با Floating، یک Administrative Distance برابر 130 بر روی شبکه‌ی LAN ، R2 مشخص می‌کند.

Default

1	Router(config)#**ipv6 route ::/0 {ipv6- address | interface-type interface- number [ipv6- address]} [administrative-Distance]**

- Static Route به‌صورت Default در IPV6 شبیه به Static Route به‌صورت پیش‌فرض در IPV4 (0.0.0.0) است.
- در عوض دستور IPV6 از ::/0 برای مشخص کردن همه‌ی شبکه‌ها استفاده می‌کند.

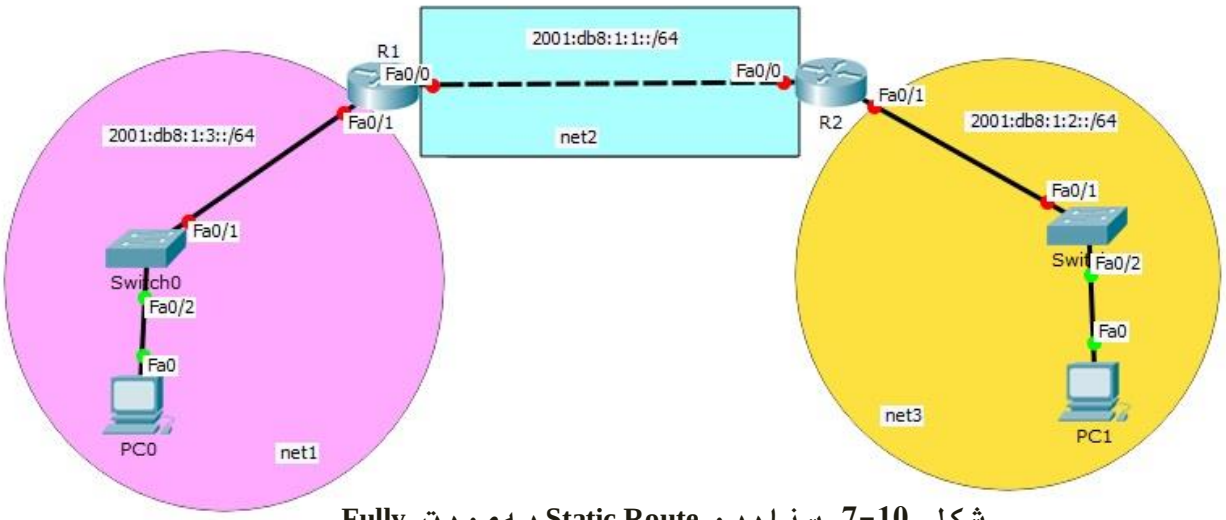


شکل 10-6 سناریوی Default

1	R2(config)#**ipv6 route ::/0 S0/0/0**

```
R1#show ipv6 route static
IPV6 Routing Table – Default- 8 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route, M - MIPv6
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
       D - EIGRP, EX - EIGRP external
S      ::/0  [1/0]
       Via  ::, Serial0/0/0
```

سناریو : Static Route



شکل 10-7 سناریو Static Route به‌صورت Fully

1	Router(config)#**ipv6 unicast-routing**
2	Router(config)#**int f0/0**
3	Router(config-if)#**ipv6 address 2001:db8:1:1::/64 eui-64**
4	Router(config-if)#**no shutdown**
5	
6	Router(config-if)#**int f0/1**
7	Router(config-if)#**ipv6 address 2001:db8:1:3::/64 eui-64**
8	Router(config-if)#**no shutdown**
9	IPی اینترفیس
10	Router(config)#**ipv6 route 2001:db8:1:2::/64 fastEthernet 0/0** **2001:DB8:1:2:209:7CFF:FE32:1302**

R2

```
1   Router(config)#ipv6 unicast-routing
2   Router(config)#int f0/0
3   Router(config-if)#ipv6 address 2001:db8:1:1::/64 eui-64
4   Router(config-if)#no shutdown
5
6   Router(config-if)#int f0/1
7   Router(config-if)#ipv6 address 2001:db8:1:2::/64 eui-64
8   Router(config-if)#no shutdown
9
10  Router(config)#ipv6 route 2001:db8:1:3::/64 fastEthernet 0/0
    2001:DB8:1:1:2D0:D3FF:FE6E:9601
```

خروجي

```
Router#sh ipv6 route
IPv6 Routing Table - 6 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route, M - MIPv6
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
       D - EIGRP, EX - EIGRP external
 C    2001:DB8:1:1::/64 [0/0]
       via ::, FastEthernet0/0
L     2001:DB8:1:1:2D0:D3FF:FE6E:9601/128 [0/0]
       via ::, FastEthernet0/0
S     2001:DB8:1:2::/64 [1/0]
       via 2001:DB8:1:2:209:7CFF:FE32:1302, FastEthernet0/0
C     2001:DB8:1:3::/64 [0/0]
       via ::, FastEthernet0/1
L     2001:DB8:1:3:2D0:D3FF:FE6E:9602/128 [0/0]
       via ::, FastEthernet0/1
L     FF00::/8 [0/0]
       via ::, Null0
```

RIPng

- Distance Vector است.
- از IPV6 برای انتقال استفاده می‌کند.
- از الگوریتم Bellman برای تعیین بهترین مسیر به مقصد استفاده می‌کند.
- از Hop count به عنوان متریک استفاده می‌کند.
- از Authentication پشتیبانی نمی‌کند.

- از شماره پورت 521 استفاده می‌کند.
- UDP است.
- آدرس Multicast مقصد استفاده شده FF02::9 است.
- مبتنی بر RIPV2 است.

دستورات پیاده‌سازی RIPng

1	R(config)#**ipv6 router rip *tag***
2	
3	R(config-if)#**ipv6 rip tag enable**

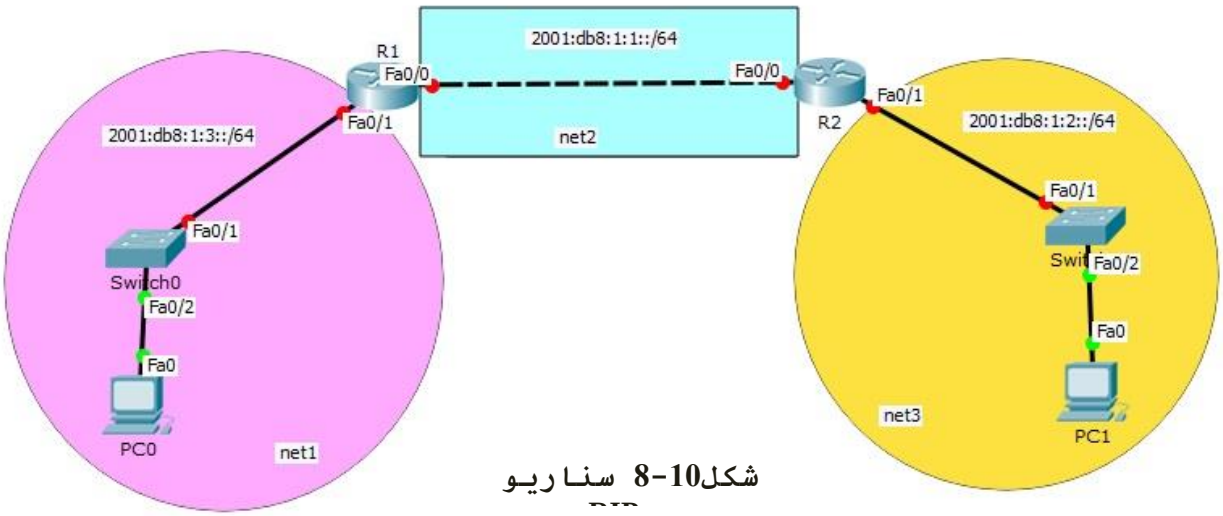
- خط1: فعال‌سازی پروتکل مسیریابی rip
tag: یک اسم دلخواه است که توسط آن مشخصه‌ی پروتکل وجود خواهد داشت.
- خط3: اعمال پروتکل مسیریابی rip روی اینترفیس مورد نظر
برای اینکه معلوم شود که کدام اینترفیس‌ها می‌خواهند advertise کنند باید روی اینترفیس مورد نظر tag را فعال کرد. از زمان فعال شدن شروع به advertise می‌کند.

در RIPng دستور network وجود ندارد، هر اینترفیسی که ip داشته باشد می‌توان با فعال کردن پروتکل مسیریابی روی آن اینترفیس اجازه مسیریابی داد. در واقع در IPV6 ، multicast وجود خارجی ندارد فقط با unicasting پیاده سازی انجام می شود، به خاطر همین دستور tag را روی اینترفیس خاصی که unicasting انجام می دهد، می زنند.

دستور Verify RIPng

1	Router#**show ipv6 rip**
2	Router#**show ipv6 route rip**

سنـاريـو : RIPng



شكل10-8 سنـاريـو RIP

R1

```
1  Router(config)#ipv6 unicast-routing
2  Router(config)#ipv6 router rip RTO
3
4  Router(config)#interface f0/1
5  Router(config-if)#ipv6 address 2001:db8:1:3::/64 eui-64
6  Router(config-if)#ipv6 rip RTO enable
7  Router(config-if)#no shutdown
8
9  Router(config-if)#int f0/0
10 Router(config-if)#ipv6 address 2001:db8:1:1::/64 eui-64
11 Router(config-if)#ipv6 rip RTO enable
12 Router(config-if)#no shutdown
```

R2

```
1  Router(config)#ipv6 unicast-routing
2  Router(config)#ipv6 router rip RTO
3
4  Router(config)#interface f0/0
5  Router(config-if)#ipv6 address 2001:db8:1:1::/64 eui-64
6  Router(config-if)#ipv6 rip RTO enable
```

```
7   Router(config-if)#no shutdown
8
9   Router(config-if)#int f0/1
10  Router(config-if)#ipv6 address 2001:db8:1:2::/64 eui-64
11  Router(config-if)#ipv6 rip RTO enable
12  Router(config-if)#no shutdown
```

خروجی

R1

```
Router#sh ipv6 route
IPv6 Routing Table - 6 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route, M - MIPv6
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
       D - EIGRP, EX - EIGRP external
C    2001:DB8:1:1::/64  [0/0]
       via ::, FastEthernet0/0
L    2001:DB8:1:1:2D0:BAFF:FE78:E101/128  [0/0]
       via ::, FastEthernet0/0
R    2001:DB8:1:2::/64  [120/2]
       via FE80::2D0:FFFF:FECD:1801, FastEthernet0/0
C    2001:DB8:1:3::/64  [0/0]
       via ::,  FastEthernet0/1
L    2001:DB8:1:3:2D0:BAFF:FE78:E102/128  [0/0]
       via ::, FastEthernet0/1
L    FF00::/8 [0/0]
       via ::, Null0
```

R1

```
Router#sh ipv6 interface
FastEthernet0/0 is up, line protocol is up
IPv6 is enabled, link-local address is FE80::2D0:BAFF:FE78:E101
    No Virtual link-local address(es):
    Global unicast address(es):
      2001:DB8:1:1:2D0:BAFF:FE78:E101, subnet is 2001:DB8:1:1::/64 [EUI]
    Joined group address(es):
      FF02::1
      FF02::2
      FF02::9
      FF02::1:FF78:E101
    MTU is 1500 bytes
    .
```

ip ی

```
.
.
FastEthernet0/1 is up, line protocol is up
IPv6 is enabled, link-local address is FE80::2D0:BAFF:FE78:E102
    No Virtual link-local address(es):
    Global unicast address(es):
      2001:DB8:1:3:2D0:BAFF:FE78:E102, subnet is 2001:DB8:1:3::/64 [EUI]
    Joined group address(es):
      FF02::1
      FF02::2
      FF02::9
      FF02::1:FF78:E102
   MTU is 1500 byte
.
.
.
```

R2

```
Router#ping 2001:DB8:1:3:2D0:BAFF:FE78:E102

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8:1:3:2D0:BAFF:FE78:E102, timeout is 2
seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms
```

OSPFV3

- شبیه به ویژگی OSPF در IPV4 است.
- از IPV4 برای router-id استفاده می‌کند.
- پروتکل Link State می‌باشد.
- برای انتقال LSA از IPV6 استفاده می‌شود.
- OSPFV3 به ازای هر لینک فعال می‌شود نه به ازای هر شبکه.
- شناسایی همسایه‌ها و Adjecency با ابتدا توسط آدرس link-local انجام می‌شود.

دستور اجرای OSPFV3

1	R(config)#**ipv6 router ospf *process-id***
2	R(config-rtr)#**router-id *router-id***
3	
4	R(config-if)#**ipv6 ospf *process-id* area *area-id***

- خط1: فعال‌سازی پروتکل مسیریابی OSPFv3
- خط2: router-id باید به فرمت IPV4 نوشته شود(این دستور اختیاری است).
- خط4: به ازای اینترفیسی که IP دارد، پروتکل مسیریابی اجرا می‌شود.

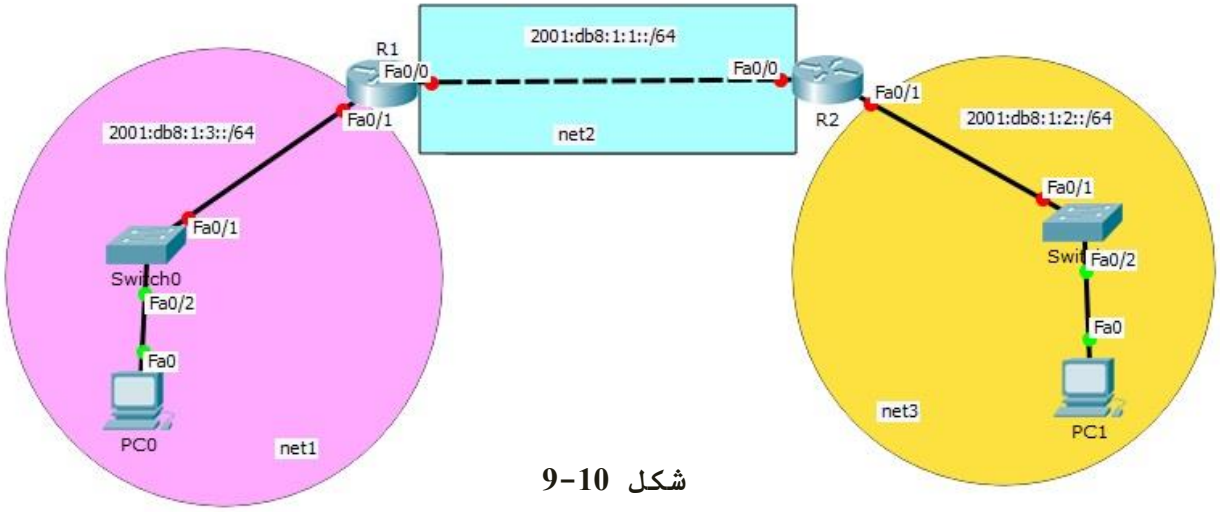
دستورات Verify OSPFv3

1	Router#**show ipv6 route ospf**
2	Router#**show ipv6 ospf neighbor**
3	Router#**show ipv6 ospf**

- خط1: route های ospf را نشان می‌دهد.
- خط2: دیدن neighbor table
- خط3: این دستور router-id، process-id و تعداد دفعاتی که الگوریتم SPF محاسبه شده است را نمایش می‌دهد.

سناریو: OSPFv3

Area 0



شكل 10-9

R1

```
1  Router(config)#ipv6 unicast-routing
2  Router(config)#ipv6 router ospf 1
3  %OSPFv3-4-NORTRID: OSPFv3 process 1 could not pick a router-id,please configure
4  manually
5  Router(config-rtr)#router-id 1.1.1.1
6  Router(config-rtr)#exi
7  Router(config)#int f0/0
8  Router(config-if)#ipv6 address 2001:db8:1:1::/64 eui-64
9  Router(config-if)#ipv6 ospf 1 area 0
10 Router(config-if)#no shutdown
11
12 Router(config-if)#int f0/1
13 Router(config-if)#ipv6 address 2001:db8:1:3::/64 eui-64
14 Router(config-if)#ipv6 ospf 1 area 0
   Router(config-if)#no shu
```

R2

```
1  Router(config)#ipv6 unicast-routing
2  Router(config)#ipv6 router ospf 1
3  %OSPFv3-4-NORTRID: OSPFv3 process 1 could not pick a router-id,please configure
4  manually
5  Router(config-rtr)#router-id 2.2.2.2
6  Router(config-rtr)#exi
7  Router(config)#interface f0/0
8  Router(config-if)#ipv6 address 2001:db8:1:1::/64 eui-64
9  Router(config-if)#ipv6 ospf 1 area 0
10 Router(config-if)#no shu
```

```
11
12  Router(config-if)#int f0/1
13  Router(config-if)#ipv6 address 2001:db8:1:2::/64 eui-64
14  Router(config-if)#ipv6 ospf 1 area 0
    Router(config-if)#no shu
```

خروجی

R1

```
Router#sh ipv6 route
IPv6 Routing Table - 6 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route, M - MIPv6
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
       D - EIGRP, EX - EIGRP external
C      2001:DB8:1:1::/64 [0/0]
         via ::, FastEthernet0/0
L      2001:DB8:1:1:2D0:BAFF:FE78:E101/128 [0/0]
         via ::, FastEthernet0/0
O      2001:DB8:1:2::/64 [110/2]
         via FE80::2D0:FFFF:FECD:1801, FastEthernet0/0
C      2001:DB8:1:3::/64 [0/0]
         via ::, FastEthernet0/1
L      2001:DB8:1:3:2D0:BAFF:FE78:E102/128 [0/0]
         via ::, FastEthernet0/1
L      FF00::/8 [0/0]
         via ::, Null0
```

R1

```
Router#sh ipv6 ospf neighbor

Neighbor ID     Pri   State           Dead Time   Interface ID    Interface
2.2.2.2           1   FULL/DR         00:00:38    1               FastEthernet0/0
```

R1

Process-id

Router-id

```
Router#sh ipv6 ospf
 Routing Process "ospfv3 1" with ID 1.1.1.1
 SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
 Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
 LSA group pacing timer 240 secs
 Interface flood pacing timer 33 msecs
```

```
Retransmission pacing timer 66 msecs
Number of external LSA 0. Checksum Sum 0x000000
Number of areas in this router is 1. 1 normal 0 stub 0 nssa
Reference bandwidth unit is 100 mbps
   Area BACKBONE(0)
      Number of interfaces in this area is 2
      SPF algorithm executed 4 times
      Number of LSA 6. Checksum Sum 0x0309e2
      Number of DCbitless LSA 0
      Number of indication LSA 0
      Number of DoNotAge LSA 0
      Flood list length 0
```

تعداد دفعاتی که الگوریتم SPF

ip ی اینترفیس R2

R1

```
Router#ping 2001:DB8:1:2:2D0:FFFF:FECD:1802

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8:1:2:2D0:FFFF:FECD:1802, timeout is 2
seconds:
!!!!!
```

EIGRPV6

- شبیه به ویژگی EIGRP در IPV4 است.
- به ازای هر لینک فعال می شود.

1	R(config)#**ipv6 router eigrp *AS***
2	R(config-if)#**ipv6 eigrp *AS***

- خط1: فعال‌سازی پروتکل مسیریابی eigrp در IPV6
- خط2: اجرای پروتکل مسیریابی به ازای اینترفیس خاص

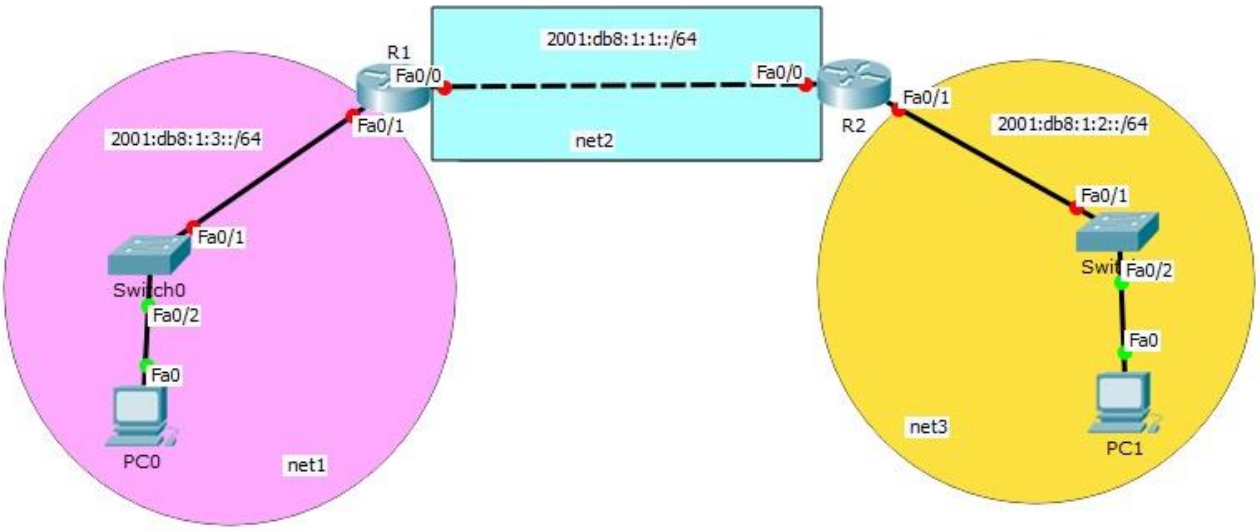
دستور Verify EIGRP

1	Router#**show ipv6 eigrp topology**
2	Router#**show ipv6 route eigrp**

- خط1: مشاهده‌ی topology table
- خط2: مشاهده‌ی جدول مسیریابی eigrp

سناریو : EIGRPV6

Eigrp 100



شکل 10-10سناریو EIGRPV6

R1

1	Router(config)#**ipv6 unicast-routing**

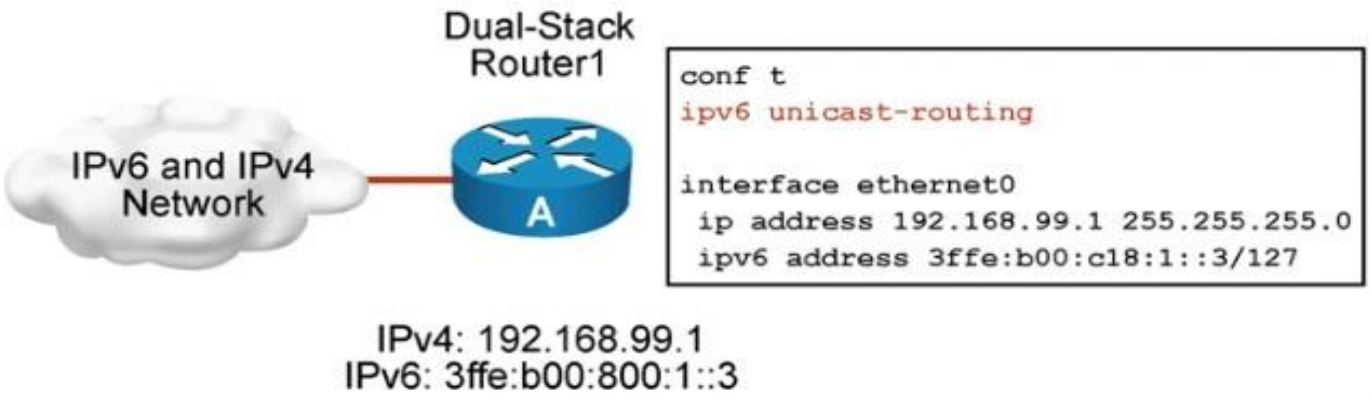
```
2  Router(config)#ipv6 router eigrp 100
3
4  Router(config)#int f0/0
5  Router(config-if)#ipv6 address 2001:db8:1:1::/64 eui-64
6  Router(config-if)#ipv6 eigrp 100
7  Router(config-if)#no shutdown
8
9  Router(config-if)#int f0/1
10 Router(config-if)#ipv6 address 2001:db8:1:3::/64 eui-64
11 Router(config-if)#ipv6 eigrp 100
12 Router(config-if)#no shutdown
```

R2

```
1  Router(config)#ipv6 unicast-routing
2  Router(config)#ipv6 router eigrp 100
3
4  Router(config)#int f0/0
5  Router(config-if)#ipv6 address 2001:db8:1:1::/64 eui-64
6  Router(config-if)#ipv6 eigrp 100
7  Router(config-if)#no shutdown
8
9  Router(config-if)#int f0/1
10 Router(config-if)#ipv6 address 2001:db8:1:2::/64 eui-64
11 Router(config-if)#ipv6 eigrp 100
12 Router(config-if)#no shutdown
```

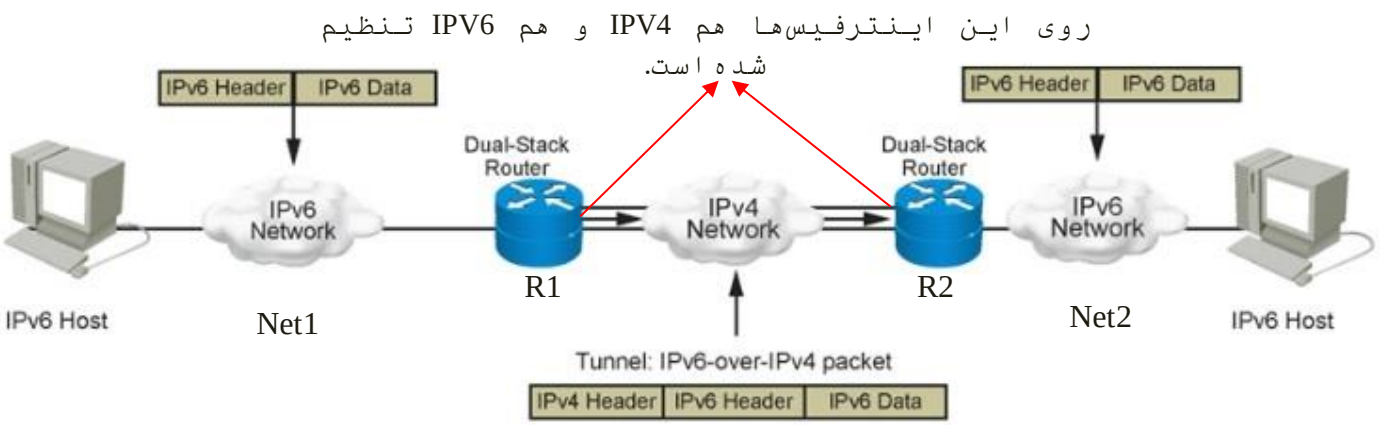
قابلیت Dual stack

قابلیت Dual stack به این صورت است که در یک روتر یا دستگاه بر روی اینترفیس می‌توان همزمان هم IPV4 و هم IPV6 به‌کار گرفت. مزیت این عمل این است که اگر بستر زیر ساخت ارتباط IPV4 باشد، می‌توان نقاط مختلف شبکه را با آدرس‌های IPV6 بهم وصل کرد. استفاده‌ی اصلی از Dual stack در تونل IPV6 می‌باشد.



شکل 10-11 قابلیت Dual Stack

تونل در IPV6



شکل 10-12 تونل 4 to 6

همان‌طوری که در شکل (10-8) مشاهده می‌کنیم، 2 شبکه با IPV6 در نقاط مختلف قرار گرفته اند (مانند دو سازمان مختلف). برای اینکه این دو شبکه بهم وصل شود باید از مخابرات استفاده کرد (مخابرات IPV4 می باشد). برای این‌که مخابرات یک کانکت ارتباطی بین سازمان‌ها برقرار کند ابتدا روترهایی که در IPV6 هستند را با IPV4 بهم کانکت

می‌کند (شبکه IPV4 اجرا می‌شود)، سپس روی روترهایی که در IPV6 هستند یک تونل ایجاد می‌کند (tunnel 6 to 4). در واقع با این‌کار IPV6 بر روی IPV4 ، over می‌شود. (یعنی بستر ارتباطی IPV4 می‌باشد و ترافیک IPV6 از IPV4 رد می‌شود). روترها یک IPV6 تنظیم می‌کنند که یکی ابتدای تونل و دیگری انتهای تونل می‌شود. داده‌ی انتقالی از Net1 ابتدا به R1 می‌رسد در R1 پکت، هدر IPV6 و هدر IPV4 را دارد. در تونل پکت با هدر IPV4 به انتهای تونل هدایت می‌شود در انتهای تونل هدر IPV4 برداشته می‌شود و با هدر IPV6 تحویل Net2 داده می‌شود.

نکات

- تونل‌های 4 to 6 به‌صورت point-to-multipoint هستند.
- IPV6 ای که در ابتدا و انتهای تونل تنظیم می‌شود، IPای تونل می‌باشد.
- محدودیت‌های تونل 4 to 6:
  - فقط static route یا BGP پشتیبانی می‌کند.
  - عدم پشتیبانی از NAT

فصل 11

VPN

VPN[1]

- ایجاد یک کانکشن امن در یک بستر نا امن (مثل WAN) را گویند.
- اتصال point-to-point فراهم می‌کند.
- مقیاس‌پذیر[2] می‌باشد.
- پیاده سازی VPN با دو مدل Device قابل انجام شدن است:

[1] Virtual Private Network
[2] Scalable

- **VPN**: $\begin{cases} Firewall \begin{bmatrix} Hard(ASA, SSG) \\ Soft(ISA, TMG) \end{bmatrix} \\ Router \rightarrow K9 \end{cases}$

مزيت هاي استفاده از VPN:

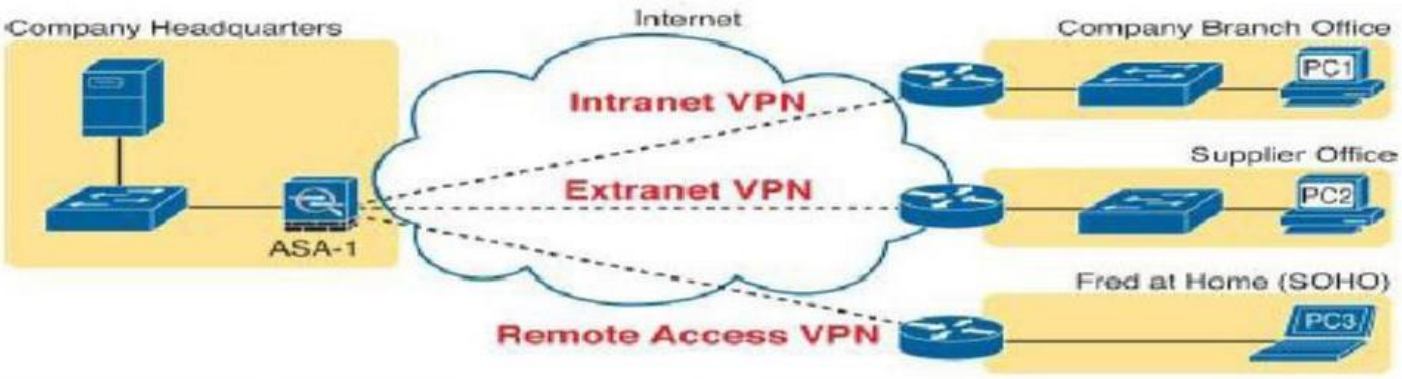
- كاهش هزينه ها
- قابليت رشد و گسترش شبكه
- ايجاد امنيت

انواع روشهاي پياده سازي VPN

1- **Site to Site VPN:** دو نوع مي‌باشد:

- **Intranet:** همه‌ی كامپيوترهای موجود در دو site از سازمان مشابه را بهم كانكت می‌كند، معمولا از يک دستگاه VPN در هر site استفاده می‌كند.
- **Extranet:** همه‌ی كامپيوترهای موجود در دو site مختلف را بهم كانكت می‌كند اما سازمان‌ها باهم همكاری می‌كنند. معمولا از يک دستگاه VPN در هر site استفاده می‌كند.

2- **Remote Access VPN:** استفاده از يك نرم افزار جانبي جهت اتصال به سرور (مثل VPN هايي كه در ايران براي عبور از فيلترينگ استفاده مي‌شود و يا Cisco Easy VPN: نرم افزار رايگاني است كه شركت سيسكو ارائه داده است).



شكل 11-1
انواع VPN

ویژگی‌های VPN

1- Confidentiality: محرمانگي داده ها
2- Data Integrity: يكپارچگي و تضمين سلامت داده ها در رسيدن به مقصد
3- Authentication: احراز هويت
4- Antireplay Protection: تصديق فرستنده‌ي واقعي

پروتکل های امن‌سازی VPN

- **IPSec**
  - چگونگی اتصال دو دستگاه به اینترنت را مشخص می‌کند.
  - در لایه 3 کار می‌کند.
  - مجموعه عملکرد یکسری پروتکل امنیتی است.
  - می‌تواند به تمام ویژگی‌های VPN (احرازهویت، رمزنگاری و ...) دست یابد.
  - از رمزنگاری استفاده می‌کند، یک بسته IP را درون یک بسته IPSec کپسوله می‌کند.
  - هنگامی که بسته‌ی اورجینال IP رمزگشایی شود و به مقصد مورد نظر برسد، در انتهای تونل بسته‌ای که کپسوله شده بود از حالت کپسوله خارج می‌شود.
  - یک تونل IPSec همه‌ی ارتباطات بین دستگاه‌ها را صرف نظر از نوع ترافیک امن می‌کند.

- **SSL**[1]
  - یک فرمی از VPN است که می‌تواند با یک استاندارد مرورگر وب استفاده شود.
  - به‌عنوان Web VPN هم شناخته شده است.
  - در لایه 7 کار می‌کند.
  - برای پشتیبانی دسترسی کاربران از راه دور برای شبکه‌های سازمانی از هر نقطه‌ای بر روی اینترنت فراهم شده است.
  - دسترسی از راه دور از طریق یک دروازه SSL VPN فراهم شده است.
  - دروازه‌ی SSL VPN اجازه می‌دهد تا کاربران یک تونل امن VPN با استفاده از یک مرورگر وب فراهم کنند.

[1] Secure Socket Layer

- SSL VPN دسترسی آنلاین به‌صورت امن برای تراکنش‌های مالی را پشتیبانی می‌کند.
- از رمزنگاری و احرازهویت برای حفظ ارتباطات خصوصی بین دو دستگاه، وب سرور و کاربر ماشین استفاده می‌کند.
- انعطاف‌پذیری را با فراهم کردن سطوح امنیتی فراهم می‌کند.
- همه‌ی برنامه‌های کاربردی مرورگر وب همانند: IE، Mozila به‌صورت پیش‌فرض از SSL پشتیبانی می‌کنند.

الگوریتم‌های رمزنگاری[1]

جهت محرمانگی (محرمانه نگه داشتن داده‌ها) از الگوریتم‌های رمزنگاری استفاده می‌شود.

- معروف‌ترین الگوریتم‌های رمزنگاری عبارتند از:
  - DES
  - 3DES
  - AES
  - RSA

تفاوت الگوریتم‌های رمزنگاری در طول کلید آنهاست

$$\begin{cases} 1.\ DES & 56\ bit \\ 2.\ 3DES & 3 \times 56\ bit \\ 3.\ RSA & 512\ bit \\ 4.\ AES & 128\ bit \end{cases}$$

- بعد ازتعریف الگوریتم‌های رمزنگاری، الگوریتم‌های Key Exchange بوجود آمد که عمل رد و بدل کردن کلیدها بین مبدا و مقصد (دو نقطه) را انجام می‌دهد. یکی از این الگوریتم‌ها که عمل تبادل را انجام می‌دهد، Diffie-Hellman می‌باشد.

$$\begin{cases} 1.\ DH1 \\ 2.\ DH2 \\ 3.\ DH5 \\ 4.\ DH7 \end{cases}$$

تضمین سلامت داده‌ها

زمانی‌که داده بین مبدا و مقصد رد و بدل می‌گردد باید مطمئن شویم که داده‌ی ارسال شده به صورت درست و بدون دستکاری به مقصد می‌رسد.

[1] Encryption Algorithm

باید کاري کنیم که اگر بخواهیم داده‌اي را از نقطه‌ي A به نقطه‌ي B انتقال دهیم در صورتي که داده تغییر کند ← گیرنده بفهمد که این داده تغییر کرده است. در این حالت ما از الگوریتم‌هاي Hashing استفاده مي‌کنیم.

Hashing Algorithms: $\begin{cases} 1. HMAC - MD5 \\ 2. HMAC - SH1 - 1 \end{cases}$

احراز هویت

- دو معیار و بحث کلي در دنیا در این بخش موجود است. PSK و CA.

1. $\boldsymbol{PSK \rightarrow Password} \begin{cases} \boldsymbol{Private\ Key} \\ \boldsymbol{Public\ Key} \end{cases}$ **انواع کلیدهاي رد و بدل شده بین مبدا و مقصد.**

- یك پسورد (رمز ارتباطي) تعریف مي‌کنیم (جهت ورود به نقطه‌ي مورد نظر)
- الگوریتم‌هایي که از این دو دسته (Public Key و Private Key) استفاده مي‌کنند به دو دسته تقسیم مي‌شوند:
- $\begin{cases} \boldsymbol{Symetric} \\ \boldsymbol{A - Symetric} \end{cases} \rightarrow$ مبدا $\xrightarrow{\boxtimes}$ مقصد

  Private Key ***Public Key***

- A-Semetric دو کلیدي است. در مبدا با Public key قفل مي‌شود.
- کلید همراه بسته ارسال مي‌گردد که این روش خطرناك است و گیرنده با کلید شخصي‌اش بسته را باز مي‌کند.

2. $\boldsymbol{CA \rightarrow \boxed{CA}\ Server}$

- Certification : تاریخ Expire در آن قرار دارد. درخواست کننده نیز وجود دارد.

پیاده سازي IPSec

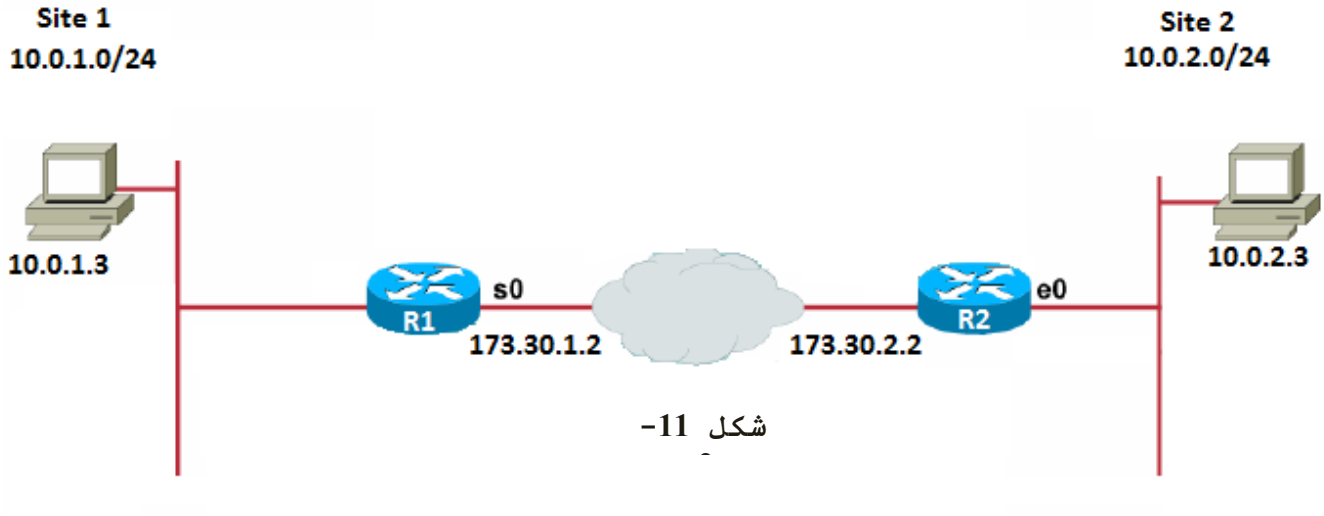
6 مرحله دارد.

1- نوشتن ACL متناسب براي سایت‌هایي که امکان اتصال VPN براي آن‌ها فراهم مي‌گردد.

Site 1
10.0.1.0/24

←■→

Site 2
10.0.2.0/24



شکل 11-

R1:

1	Router(Config)#**Access-list 110 permit ip 10.0.1.0 0.0.0.255 10.0.2.0 0.0.0.255**

R2:

1	Router(Config)#**Access-list 120 permit ip 10.0.2.0 0.0.0.255 10.0.1.0 0.0.0.255**

این ACL صرفا جهت کنترل ترافیك است.
شماره‌ي ACL ها در روتر نیاز نیست شبیه به هم باشد.

2- نوشتن Policy امنیتي براي مشخص نمودن پروتکل‌هائیکه در IPSec میخواهیم از آن‌ها استفاده کنیم.

1	Router(Config)#**Crypto isakmp policy *priority***

Priority: شماره‌ي اولویت است. در زمانیکه چند Policy وجود داشته باشد اولویت اجراي Policy ها را براساس این شماره تعیین میکند.

Router 1, 3:

1	Router(Config)#**Crypto isakmp policy *110***
2	Router(Config-isakmp)#**authentication pre-share**
3	Router (config-isakmp)#**encryption aes 256**
4	Router (config-isakmp)#**group 1**
5	Router (config-isakmp)#**hash md5**
6	Router (config-isakmp)#**lifetime 86400**

در هر دو روتر باید عینا Policy یکسان بنویسیم.

3-تعریف رمز متناسب مابین روترها

1	Router(config)#**crypto isakmp key رمز مناسب address IPمقابل**

R1

1	R1(config)#**crypto isakmp key cisco123 address 172.30.2.2**

بعد از address باید IP اینترفیس روتر مقابل(173.30.2.2) را بنویسیم.

R2

1	R2(config)# **crypto isakmp key cisco123 address 173.30.1.2**

4- تعریف Transform Set: مکانیزمي است که Header داده را مشخص مي‌کنیم.

R1:

1	RouterX(config)#**crypto ipsec transform-set *MYSET(ccna)* esp-aes 128**

R2:

1	RouterY(config)#**crypto ipsec transform-set *OtherSET* esp-aes 128**

- نام طرفین مي‌تواند همسان باشد.
- طول کلید طرفین (عددي که در جلوي esp-aes نوشته شده است) باید یکسان باشد.

R1,R2:

1	RouterX(config)#**crypto ipsec transform-set cisco123 esp-aes 128**

5- تعریف Crypto Map:

R1, R2:

1	R1(config)#**crypto map MYMAP 10 ipsec-isakmp**
2	R1(config-crypto-map)#**match address 110**
3	R1(config-crypto-map)#**set peer 172.30.2.2 ~~default~~**
4	R1(config-crypto-map)#**set pfs group1**
5	R1(config-crypto-map)#**set transform-set (MYSET) ccna**
6	R1(config-crypto-map)#**set security-association lifetime seconds 86400**

- خط 1: اسم دلخواه انتخاب مي‌کنیم که در جلوي آن برایش اولویت تعریف مي‌کنیم که در صورتي که از چند Crypto استفاده کردیم سیستم بداند که اولویت اجرا به چه ترتیبي است.
- خط 2: باید شماره‌ي ACL نوشته شده را در جلوي آن بنویسیم.
- خط 3: در قسمت Set peer، IP سمت مقابل را مي‌نویسیم. نوشتن Defualt نیاز نیست. در جایي که Slave /Master داشته باشیم نیاز است.

6- اعمال Crypto Map نوشته شده به پورت مورد نظر.

R1, R2:

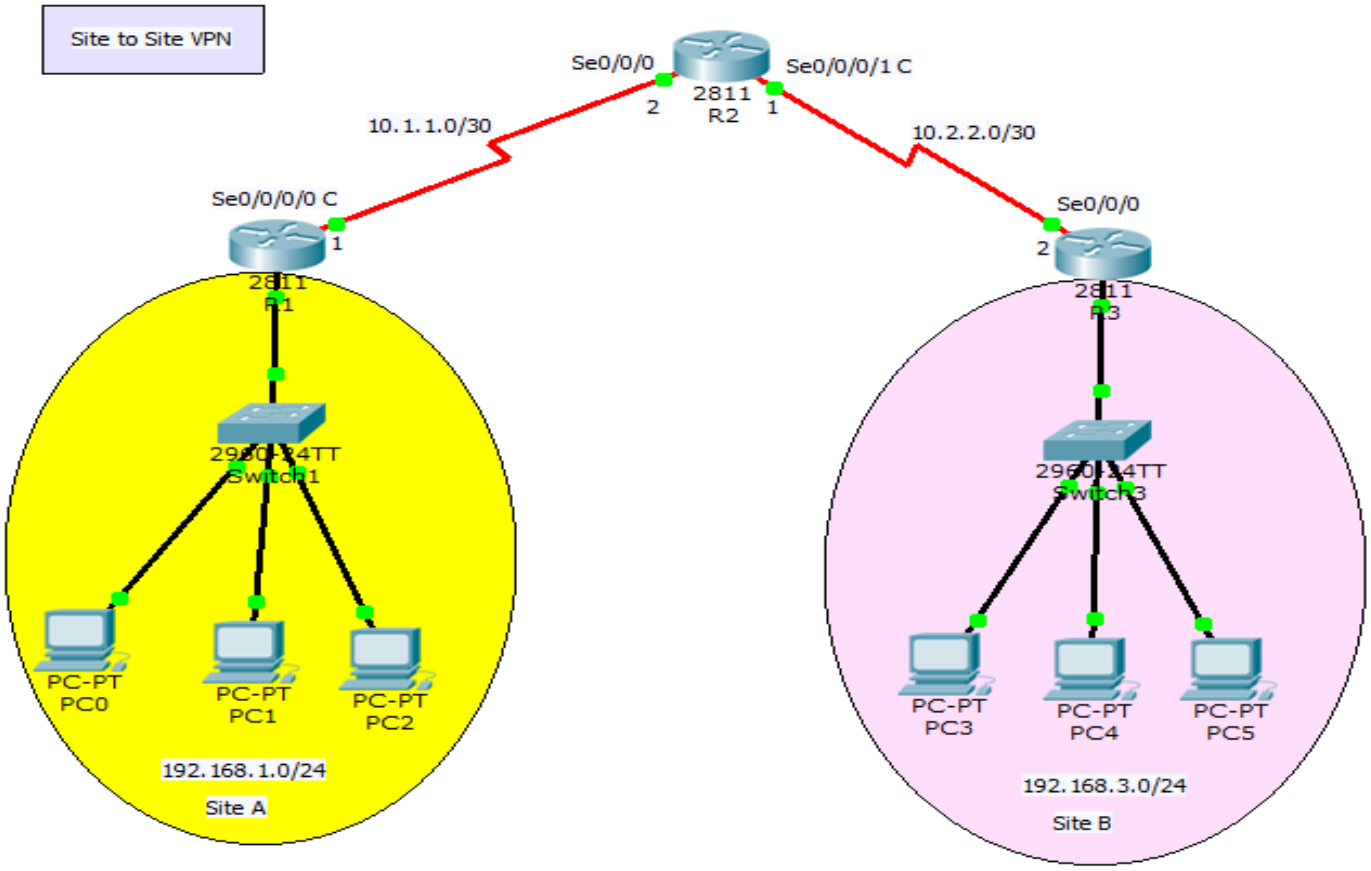
1	R1, R3(config)#**interface Interface**
2	Router(config-if)#**crypto map MYMAP**
3	*Jan 3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON

دستور verify :

1	**R#show crypto ipsec sa**

این دستور کل اطلاعات تونل IPsec را نشان می‌دهد.

سناریو VPN Site to Site



شکل 3-11 سناریو VPN Site to Site

با توجه به دیاگرام شکل(11-3) ارتباط روتر 1 با روتر 3 را با استفاده از VPN Site to Site راه اندازي كنيد(پروتكل مسيريابي به صورت دلخواه)

پروتكل مسيريابي را در اينجا RIP انتخاب نموده ايم.

R1

```
1 R1(config)#router rip
2 R1(config-router)#version 2
3 R1(config-router)#network 192.168.1.0
4 R1(config-router)#network 10.1.1.0
```

R2

```
1 R2(config)#router rip
2 R2(config-router)#version 2
3 R2(config-router)#network 10.1.1.0
4 R2(config-router)#network 10.2.2.0
```

R3

```
1 Router(config)#router rip
2 Router(config-router)#version 2
3 Router(config-router)#network 10.2.2.0
4 Router(config-router)#network 192.168.3.0
```

---

1. ابتدا ACL(Access List) مناسب را جهت ارتباط سايت‌ها نسبت به هم مي‌نويسيم.

R1

```
1 R1(config)#access-list 101 permit ip 192.168.1.0 0.0.0.255 192.168.3.0 0.0.0.255
```

IP Source: 192.168.1.0 0.0.0.255 و سپس IP Des:192.168.3.0 0.0.0.255 به همراه Widcard مناسب را مي‌نويسيم.

- در روتر مقابل نيز ACL مورد نظر را مي‌نويسيم:

R3

```
1 R3(config)#access-list 101 permit ip 192.168.3.0 0.0.0.255 192.168.1.0 0.0.0.255
```

- اين ACL جهت كنترل ترافيك است.

2. نوشتن Policy امنيتي براي مشخص نمودن پروتكل‌هائيكه در IPsec مي‌خواهيم از آن‌ها استفاده كنيم. در هر دو روتر R1 و R3 كد زير را مي‌نويسيم:

R1, R3

```
1  R1,R3 (config)#crypto isakmp policy 10
2  R1,R3 (config-isakmp)#authentication pre-share
3  R1,R3 (config-isakmp)#encryption aes 256
4  R1,R3 (config-isakmp)#group 1
5  R1,R3 (config-isakmp)#hash md5
6  R1,R3 (config-isakmp)#lifetime 86400
```

3. تعريف رمز مناسب مابين روترهاي R1, R3.

Router(config)#**crypto isakmp key رمز مناسب address آی پی مقابل**

R1

```
1  R1(config)#crypto isakmp key minush address 10.2.2.2
```

بعد از address بايد ip اينترفيس روتر مقابل (10.2.2.2) را بنويسيم.

R3

```
1  R3(config)#crypto isakmp key minush address 10.1.1.1
```

4. تعريف Transform Set مناسب.

R1

```
1  R1(config)#crypto ipsec transform-set ccna esp-aes 128
```

R3

```
1  R3(config)#crypto ipsec transform-set ccna esp-aes 128
```

5. تعريف Crypto Map

R1

```
1  R1(config)#crypto map VPN 10 ipsec-isakmp
2  % NOTE: This new crypto map will remain disabled until a peer  and a valid access
3  list have been configured.
4  R1(config-crypto-map)#match address 101
5  R1(config-crypto-map)#set peer 10.2.2.2
6  R1(config-crypto-map)#set pfs group?
7  group1  group2  group5
8  R1(config-crypto-map)#set pfs group1
9  R1(config-crypto-map)#set transform-set ccna
10 R1(config-crypto-map)#set security-association lifetime seconds 86400
```

R3

```
1  R3(config)#crypto map VPN 10 ipsec-isakmp
2  % NOTE: This new crypto map will remain disabled until a peer  and a valid access
3  list have been configured.
4  R3(config-crypto-map)#match address 101
5  R3(config-crypto-map)#set peer 10.1.1.1
6  R3(config-crypto-map)#set pfs group1
7  R3(config-crypto-map)#set transform-set ccna
8  R3(config-crypto-map)#set security-association lifetime seconds 86400
```

---

6. اعمال Crypto Map نوشته شده به پورت سريال خروجي روتر مورد نظر (در پورت سريال Se0/0/0 روترهاي R1, R3)

R1, R3:

```
1  R1, R3(config)#interface serial 0/0/0
2  Router(config-if)#crypto map vpn
3  ERROR: Crypto Map with tag vpn does not exist.
4
5  R1,R3(config-if)#crypto map VPN
6  *Jan  3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
```

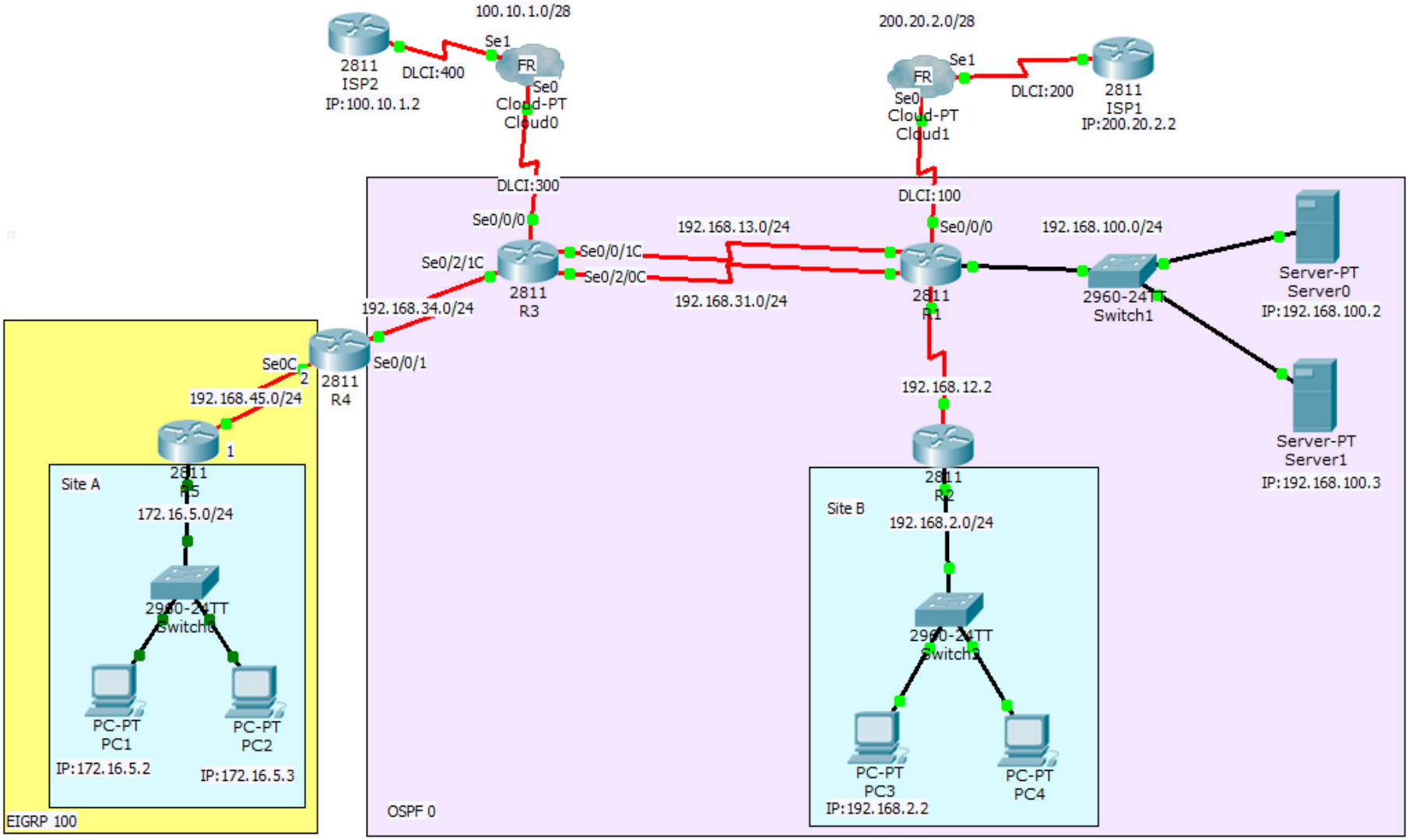
7.تست تانل ايجاد شده: ابتدا از كامپيوترهاي سايت A، كامپيوترهاي سايت B را Ping مي‌كنيم و بالعكس.

سپس با استفاده از دستور زیر چك مي كنيم كه ارتباط بين دو سايت برقرار مي باشد يا نه؟

```
R1#show crypto ipsec sa
…
interface: Serial0/0/0
   Crypto map tag: VPN, local addr 10.1.1.1

  protected vrf: (none)
  local  ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)
  remote  ident (addr/mask/prot/port): (192.168.3.0/255.255.255.0/0/0)
  current_peer 10.2.2.2 port 500
   PERMIT, flags={origin_is_acl,}
  #pkts encaps: 11, #pkts encrypt: 11, #pkts digest: 0
  #pkts decaps: 10, #pkts decrypt: 10, #pkts verify: 0
…
```

در صورتي كه تانل برقرار شده باشد و پكتها بعد از ping بين دو سايت رد و بدل شده باشند بايد مقادير
pkts encaps, pkts encrypt, pkts decaps, pkts decrypt صفر نباشد.

PPP, Frame Relay, Redistribution, Pat, ACL, VPN - سناريو

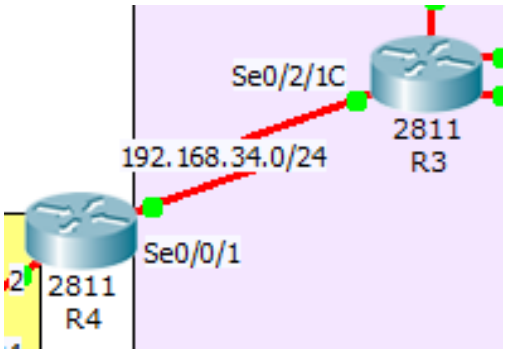


شكل 11-3 سناريو - PPP, Frame Relay, Redistribution, Pat, ACL, VPN

با توجه به سناريوي شكل(11-3) به سوالات پاسخ دهيد.

1- با IPهاي داده شده به اختصاص IP پرداخته و از پروتكل PPP براي ارتباط Router 3 با Router 4 به همراه مكانيزم Chap استفاده كنيد:
2- از پروتكل Frame Relay استفاده نموده و ارتباط Router 1 و Router 3 را با ISP هاي 1 و 2 با استفاده از اطلاعات داده شده راه اندازي نماييد.
3- با استفاده از پروتكل‌هاي مسير يابي داده شده، مطابق با دياگرام به پياده سازي مسيريابي پرداخته و در روتر R4، Redistribution استفاده نماييد.
4- دسترسي PC1 نسبت به ISP1 و دسترسي PC3 نسبت به ISP2 را از طريق PAT مقدور نماييد.
5- دسترسي PC2 را نسبت به Server0 كلا مسدود و از طريق Server 1 به طريق Web مقدور نماييد.
6- از مكانيزم VPN Site to site به روش IPsec ارتباط سايت A و B را برقرار كنيد.

جواب سوال 1: با IP هاي داده شده به اختصاص IP پرداخته و از پروتكل PPP براي ارتباط Router 3 با Router 4 به همراه مكانيزم Chap استفاده كنيد:



R3:

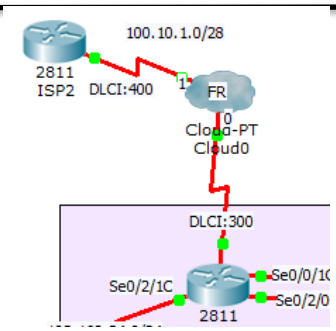
```
1  Router(config)#hostname R3
2  R3(config)#username R4 password 1234
3  R3(config)#interface serial 0/2/1
4  R3(config-if)#encapsulation ppp
5  R3(config-if)#ppp authentication chap
6  R3(config-if)#no sh
```

R4:

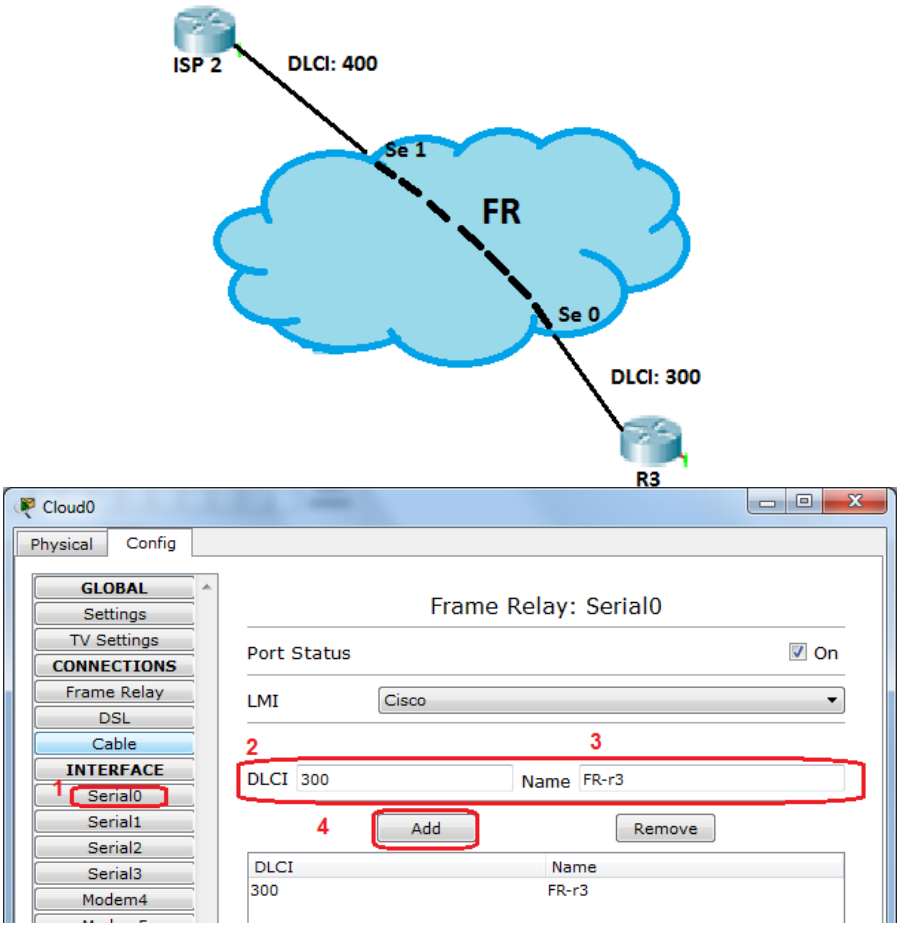
```
1  Router(config)#hostname R4
2  R4(config)#username R3 password 1234
3  R4(config)#interface serial 0/0/1
4  R4(config-if)#encapsulation ppp
5  R4(config-if)#ppp authentication chap
6  R4(config-if)#no sh
```

Router(config)#**username** نام روتر مقابل **password** در دوسمت يسورد مشترك وارد مي كنيم

جواب سوال 2: از پروتكل Frame Relay استفاده نموده و ارتباط Router 1 و Router 3 را با ISP هاي 1 و 2 با استفاده از اطلاعات داده شده راه اندازي نماييد.

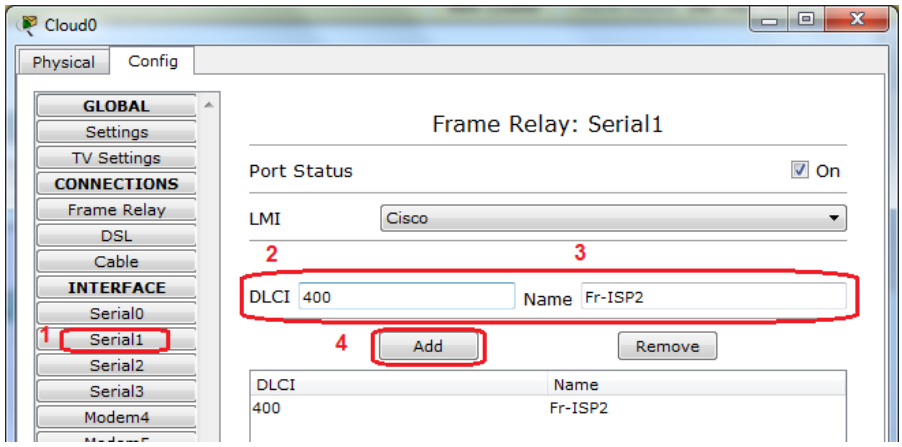


- با توجه به شکل می‌بینیم که DLCI 300، از طریق Interface Serial 0 ابر، به ابر متصل شده است و تنظیمات مربوطه را مطابق شکل زیر وارد می‌کنیم.



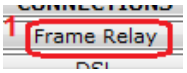
شکل 11-4 تنظیم DLCI برای Serial0 در

- با توجه به شکل می بینیم که DLCI 400، از طریق Interface Serial 1 ابر، به ابر متصل شده است.



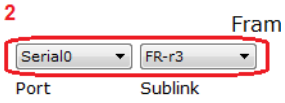
شکل 11-5 تنظیم DLCI برای Serial1 در Cloud 0

- حال باید ارتباط را برقرار کنیم، همانگونه که در شکل می‌بینیم:



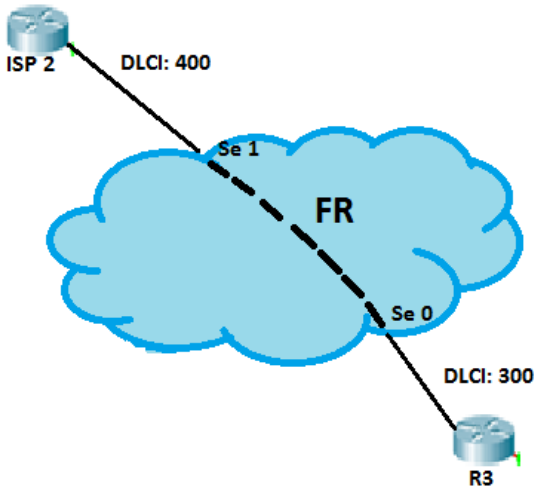
1- وارد قسمت Frame Relay می شویم.

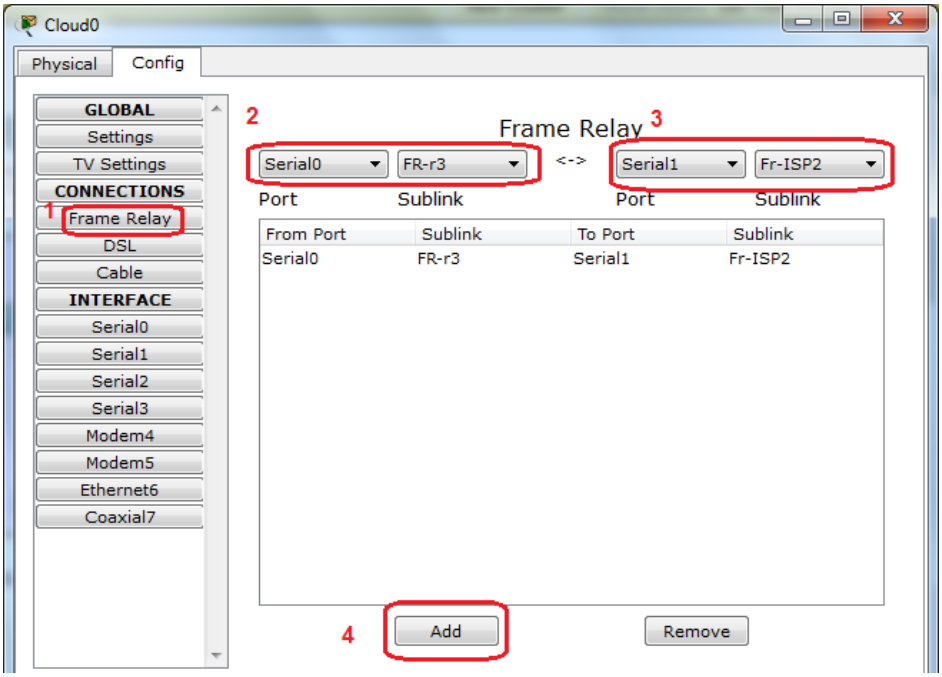
2- روتر R3 از طریق Interface serial 0 به Fr (ابر) متصل شده ایم.



3- و از طریق Interface serial 1 از FR (ابر) به ISP 2 متصل شده ایم.

4- در قسمت پایین پنجره کلید Add را می‌زنیم.





شکل 6-11 تنظیمات Frame-relay بین

R3:

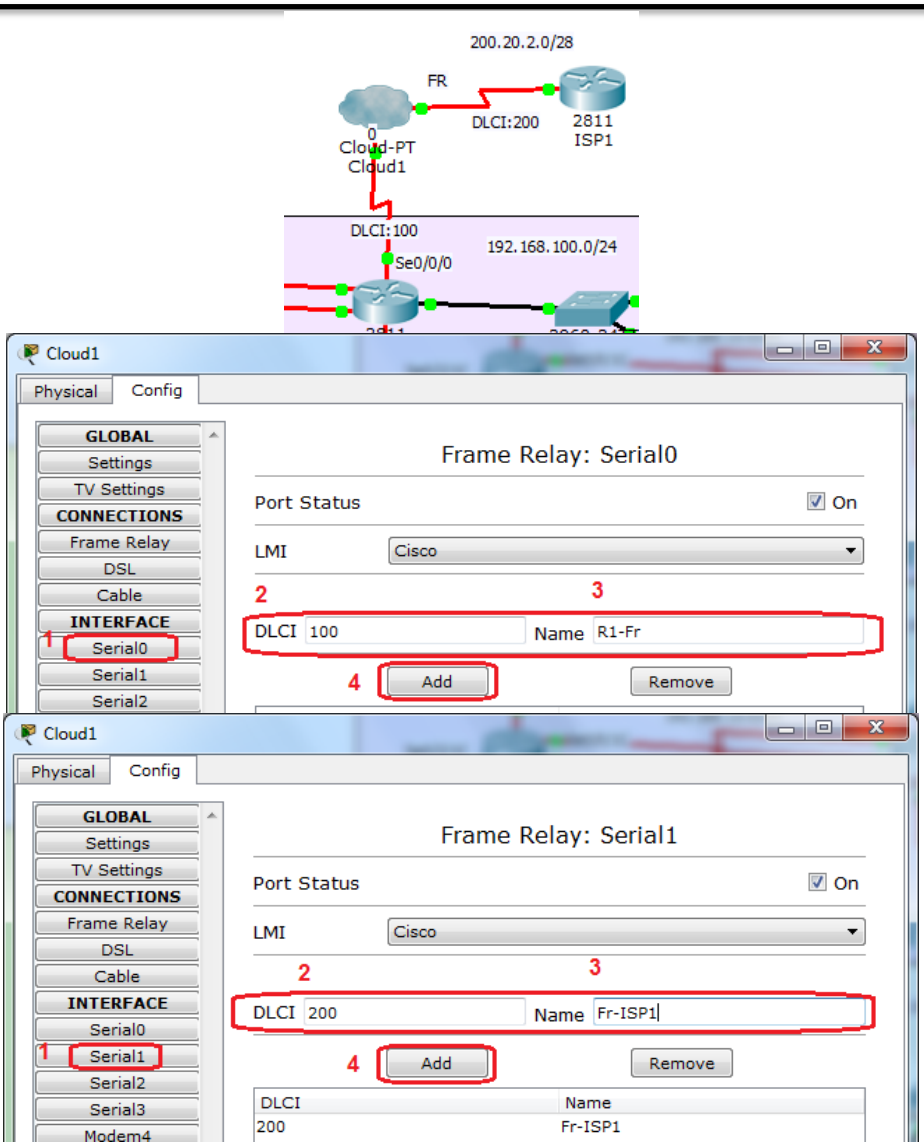
1	Router(config)#**interface serial 0/0/0**
2	Router(config-if)#**encapsulation frame-relay**
3	Router(config-if)#**ip address 100.10.1.3 255.255.255.240**
4	Router(config-if)#**frame-relay map ip 100.10.1.2 300 broadcast**
5	Router(config-if)#**no sh**

ISP2:

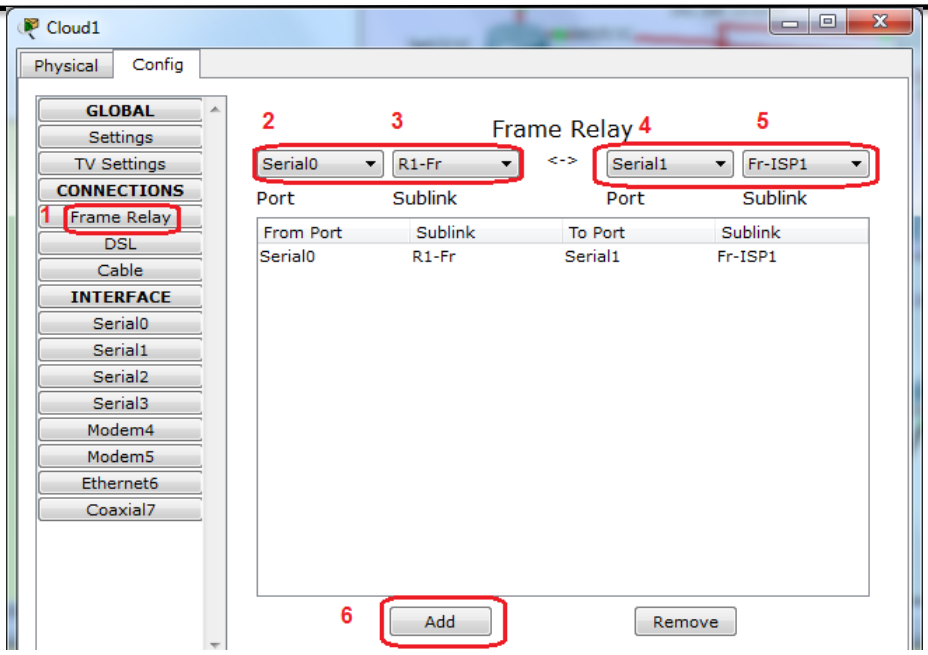
1	Router(config)#**interface serial 0/0/0**
2	Router(config-if)#**encapsulation frame-relay**
3	Router(config-if)#**ip address 100.10.1.2 255.255.255.240**
4	Router(config-if)#**frame-relay map ip 100.10.1.3 400 broadcast**
5	Router(config-if)#**no sh**

Router(config-if)#**frame-relay map ip** آی پی سمت مقابل **DLCI** مبدا **broadcast**

براي قسمت دوم، عينا مشابه بالا عمل مي‌كنيم:



شكل 11-7 تنظيمات DLCI براى



شکل 11-8 تنظیمات Frame-relay بین

R1:

```
1  Router(config)#interface serial 0/0/0
2  Router(config-if)#encapsulation frame-relay
3  Router(config-if)#ip address 200.20.2.1 255.255.255.240
4  Router(config-if)#frame-relay map ip 200.20.2.2 100 broadcast
5  Router(config-if)#no sh
```

ISP1:

```
1  Router(config)#interface serial 0/0/0
2  Router(config-if)#encapsulation frame-relay
3  Router(config-if)#ip address 200.20.2.2 255.255.255.240
4  Router(config-if)#frame-relay map ip 200.20.2.1 200 broadcast
5  Router(config-if)#no sh
```

جواب سوال 3: با استفاده از پروتکل‌هاي مسير يابي داده شده، مطابق با ديا‌گرام به پياده سازي مسيريابي پرداخته و در روتر 4، Redistribution استفاده نماييد.

راه اندازي پروتکل هاي مسير يابي:

R1:

```
1  Router(config)#router ospf 1
2  Router(config-router)#router-id 1.1.1.1
3  Router(config-router)#network 192.168.13.1 0.0.0.0 area 0
4  Router(config-router)#network 192.168.31.1 0.0.0.0 area 0
5  Router(config-router)#network 200.20.2.0 0.0.0.15 area 0
6  Router(config-router)#network 192.168.12.1 0.0.0.0 area 0
```

7	Router(config-router)#**network 192.168.100.1 0.0.0.0 area 0**

R2:

1	Router(config)#**router ospf 1**
2	Router(config-router)#**router-id 2.2.2.2**
3	Router(config-router)#**network 192.168.12.2 0.0.0.0 area 0**
4	Router(config-router)#**network 192.168.2.1 0.0.0.0 area 0**

R3:

1	Router(config)#**router ospf 1**
2	Router(config-router)#**router-id 3.3.3.3**
3	Router(config-router)#**network 192.168.34.2 0.0.0.0 area 0**
4	Router(config-router)#**network 192.168.13.1 0.0.0.0 area 0**
5	Router(config-router)#**network 192.168.31.1 0.0.0.0 area 0**
6	Router(config-router)# **network 100.10.1.0 0.0.0.15 area 0**

R4:

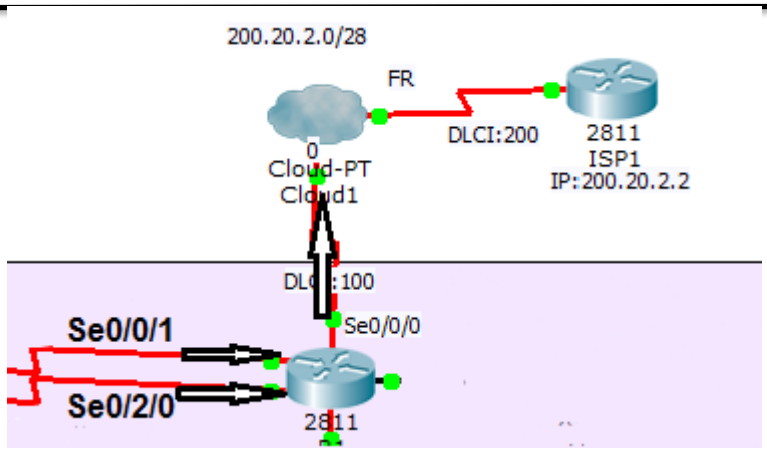
1	Router(config)#**router eigrp 100**
2	Router(config-router)#**network 192.168.45.0**
3	Router(config-router)# **redistribute ospf 1 metric 1 1 1 1 1**
4	
5	Router(config)#**router ospf 1**
6	Router(config-router)#**router-id 4.4.4.4**
7	Router(config-router)#**network 192.168.34.4 0.0.0.0 area 0**
8	Router(config-router)# **redistribute eigrp 100 metric 1 subnets**

R5:

1	Router(config)#**router eigrp 100**
2	Router(config-router)#**network 192.168.45.0**
3	Router(config-router)#**network 172.16.5.0**

جواب 4: دسترسی PC1 نسبت به ISP1 و دسترسی PC3 نسبت به ISP2 را از طریق PAT مقدور نمایید.

PC1: 172.16.5.2 ISP1:200.20.2.1

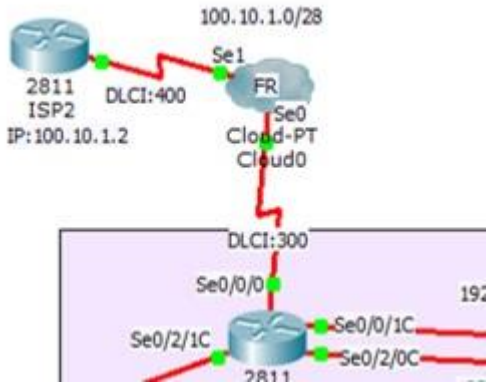


دسترسی PC1 نسبت به ISP1

R1:

1	R1(config)#**interface serial 0/0/0**
2	R1(config-if)#**ip nat outside**
3	
4	R1(config-if)#**int ser 0/0/1**
5	R1(config-if)#**ip nat inside**
6	
7	R1(config-if)#**int ser 0/2/0**
8	R1(config-if)#**ip nat inside**
9	
10	R1(config)#**access-list 1 permit 172.16.5.2 0.0.0.0**
11	R1(config)#**ip nat inside source list 1 interface serial 0/0/0 overload**

دسترسی PC3 نسبت به ISP2



R3:

1	R3(config)#**access-list 1 permit 192.168.2.2 0.0.0.0**
2	R3(config)#**interface serial 0/2/0**
3	R3(config-if)#**ip nat inside**
4	
5	R3(config-if)#**interface serial 0/0/1**
6	R3(config-if)#**ip nat inside**

7	
8	R3(config-if)#**interface serial 0/0/0**
9	R3(config-if)#**ip nat outside**
10	
11	R1(config)#**ip nat inside source list 1 interface serial 0/0/0 overload**

جواب سوال 5: دسترسي PC2 را نسبت به Server0 كلا مسدود و از طريق Server 1 به طريق Web مقدور نماييد.

Source	Access	Destination
PC2: **172.16.5.3**	**Block**	Server0: **192.168.100.2**
PC2: **172.16.5.3**	**Web**	Server1: **192.168.100.3**

Access List را از نوع Extended مي نويسيم ← بايد در روتر نزديك به Source (مبدا) يعني روتر R5 نوشته شود.
ابتدا دسترسي‌هايي كه جزئي هستند را مي‌نويسيم.

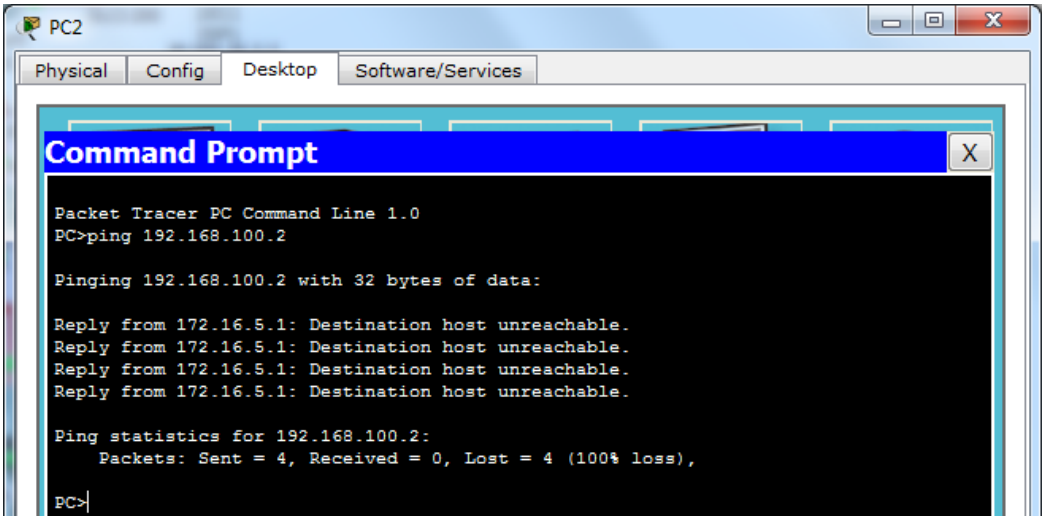
R5

```
1  Router(config)#access-list 100 permit tcp host 172.16.5.3 host 192.168.100.3 eq 80
2  Router(config)#access-list 100 deny ip host 172.16.5.3 host 192.168.100.3
3
4  Router(config)#access-list 100 deny ip host 172.16.5.3 192.168.100.2 0.0.0.0
5  Router(config)#access-list 100 permit ip any any
6
7  Router(config)#interface fastEthernet 0/0
8  Router(config-if)#ip access-group 100 in
```

- خط 1: ابتدا دسترسي PC2 را به Server1 از طريق وب باز مي‌كنيم.
- خط 2: باقي دسترسي‌هاي PC2 به Server1 را مي‌بنديم.
- خط 4: كليه‌ي دسترسي‌هاي PC2 به Server0 را مي‌بنديم.
- خط 5: دسترسي را براي باقي سيستم‌ها باز مي‌كنيم.
- خط 7: وارد Interface روتر مبدا مي‌شويم.
- خط 8: ACL نوشته شده را به ورودي Interface روتر نزديك به مبدا (يعني روتر R5) اعمال مي‌كنيم.

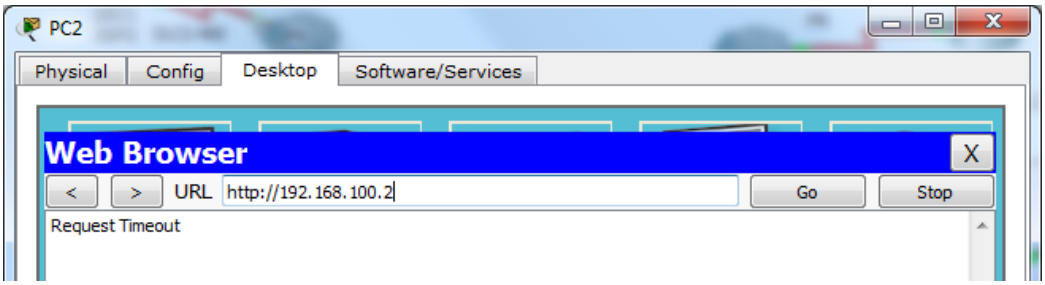
تست ارتباطات

- دسترسي از PC2 به Server0 بايد از طريق Command بسته باشد. ✓



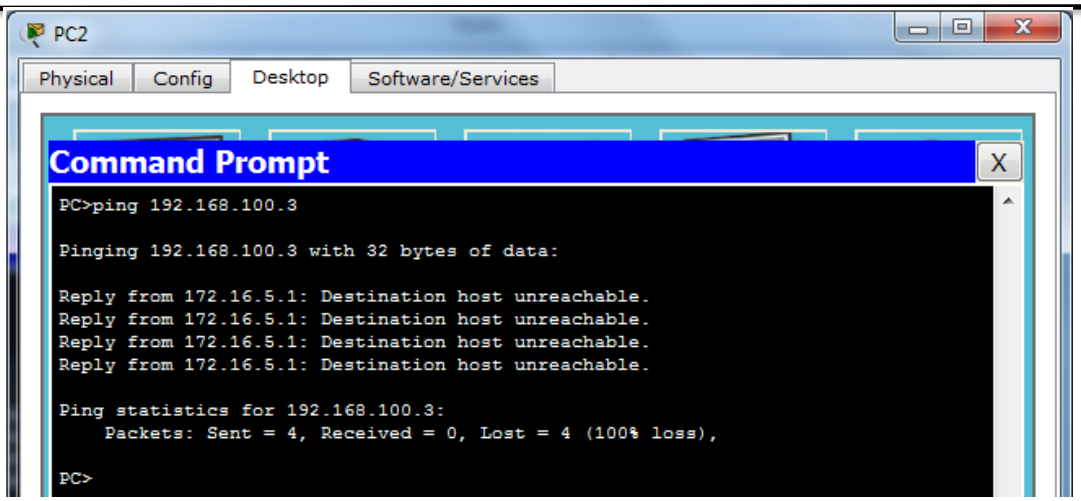
شكل 11-9 نمايش عدم Ping از PC2

- دسترسي از PC2 به Server0 بايد از طريق Web بسته باشد. ✓



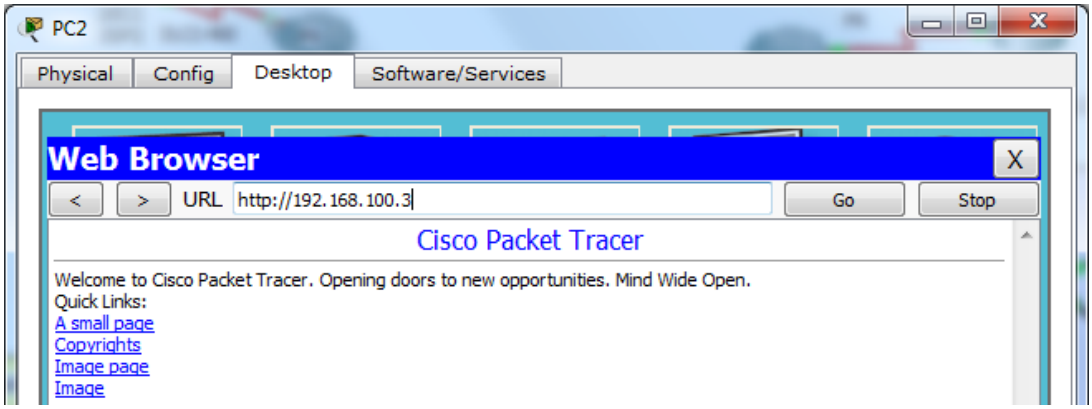
شكل 11-10 نمايش عدم دسترسي از PC2 به Server0 از طريق Web

- دسترسي از PC2 به Server1 بايد از طريق Command بسته باشد. ✓



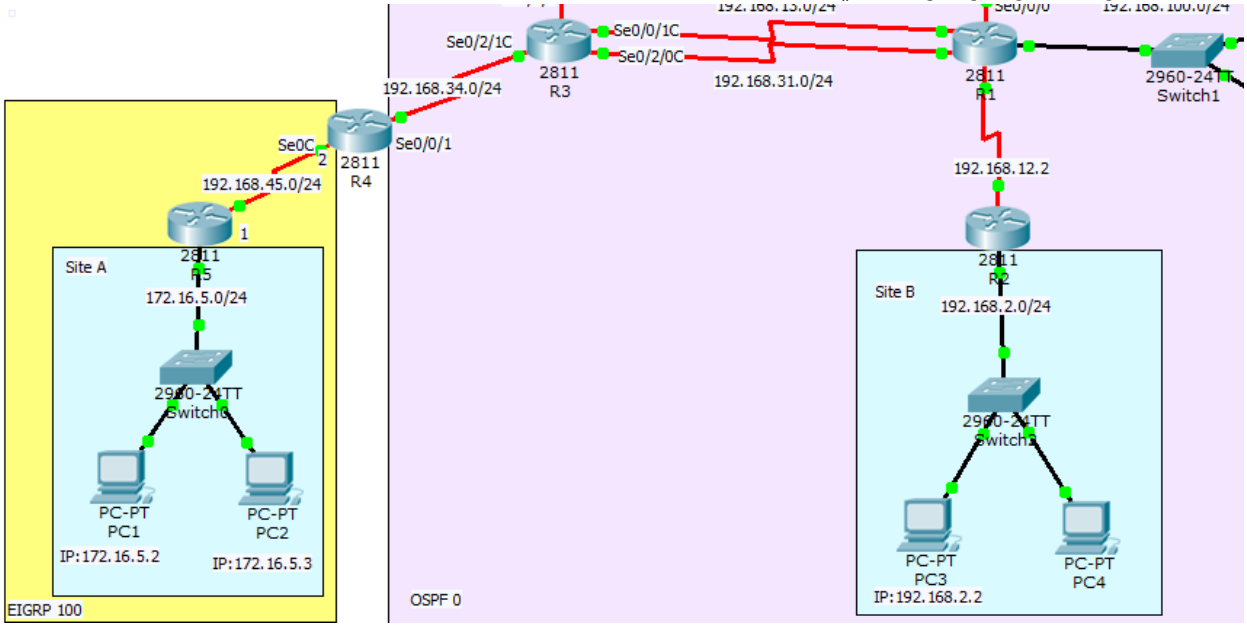
شکل 11-11 نمایش عدم Ping از PC2 به Server1

- دسترسي از PC2 به Server1 بايد از طريق Web باز باشد. ✓



شکل 11-12 نمایش دسترسی از PC2 به Server1 از طریق Web

جواب سوال 6: از مکانیزم VPN Site to site به روش IPsec ارتباط سایت A و B را برقرار کنید.



1- راه اندازي پروتكل‌هاي مسيريابي كه در بخش 1 راه اندازي شده است.

2- نوشتن ACL مناسب در روترهاي متصل به سايت‌ها (روتر R5 متصل به سايت A و روتر R2 متصل به سايت B)

R5:

1	Router(config)#**access-list 102 permit ip 172.16.5.0 0.0.0.255 192.168.2.0 0.0.0.255**

R2:

1	Router(config)#**access-list 102 permit ip 192.168.2.0 0.0.0.255 172.16.5.0 0.0.0.255**

3- نوشتن Policy امنيتي براي مشخص نمودن پروتكل‌هايي كه در IPsec مي‌خواهيم از آن‌ها استفاده كنيم. در هر دو روتر R5 و R2 كد زير را مي‌نويسيم:

R2, R5:

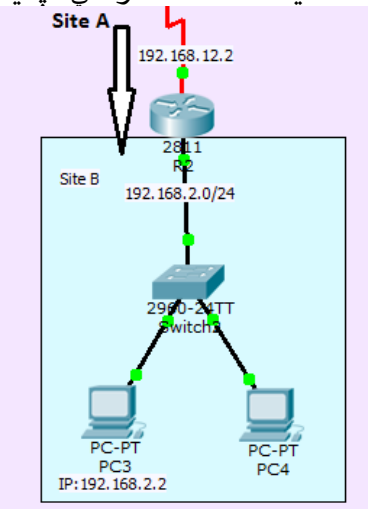
1	Router(config)#**crypto isakmp policy 10**
2	Router(config-isakmp)#**authentication pre-share**
3	Router(config-isakmp)#**encryption aes 256**
4	Router(config-isakmp)#**group 1**
5	Router(config-isakmp)#**hash md5**
6	Router(config-isakmp)#**lifetime 86400**

4- تعریف رمز مناسب و مشترك بین روترهاي R5 و R2 (روترهاي متصل به سایتهاي مورد نظر)

R5:

```
Router(config)#crypto isakmp key pari address 192.168.12.2
```

آي پي Interface روتر مقابل (Inbound) که از طریق آن سایت A وارد روتر سمت مقابل مي شود و به سایت B دسترسي پیدا مي‌کند.



در سمت دیگر هم عینا به روش بالا کانفیگ مي‌کنیم:

R2

```
Router(config)#crypto isakmp key pari address 192.168.45.5
```

5- تعریف Transform Set مناسب:

R2, R5:

```
Router(config)#crypto ipsec transform-set ccna esp-aes 128
```

6- تعریف Crypto Map:

R5:

```
1  Router(config)#crypto map VPN 10 ipsec-isakmp
2  % NOTE: This new crypto map will remain disabled until a peer
3    and a valid access list have been configured.
4  Router(config-crypto-map)#match address 102
5  Router(config-crypto-map)#set peer 192.168.12.2
6  Router(config-crypto-map)#set pfs group1
7  Router(config-crypto-map)#set transform-set ccna
8  Router(config-crypto-map)#set security-association lifetime seconds 86400
```

R2:

```
1  Router(config)#crypto map VPN 10 ipsec-isakmp
2  % NOTE: This new crypto map will remain disabled until a peer
3    and a valid access list have been configured.
4  Router(config-crypto-map)#match address 102
5  Router(config-crypto-map)#set peer 192.168.45.1
6  Router(config-crypto-map)#set pfs group1
7  Router(config-crypto-map)#set transform-set ccna
8  Router(config-crypto-map)#set security-association lifetime seconds 86400
```

7- اعمال Crypto Map نوشته شده به پورت سريال خروجي روترهاي مورد نظر:

```
1  Router(config)#interface serial 0/0/0
2  Router(config-if)#crypto map vpn
3  ERROR: Crypto Map with tag vpn does not exist.
4
5  Router(config-if)#crypto map VPN
6  *Jan  3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
```

نكته: حتما بايد به نام Map نوشته شده دقت كنيم. ما در بالا نام Map را VPN (كليه حروف بزرگ هستند) گذاشته‌ايم و همانگونه كه در خط 3 مشاهده مي‌نماييد زمانيكه نام مورد نظر را به حروف كوچك نوشتيم پيغام خطا صادر كرد.

8- تست تانل ايجاد شده: براي اينكه اطلاع پيدا كردن از اينكه تانل ايجاد شده درست كار مي‌كند و پكت‌ها بين اين دو سايت ارسال مي‌شوند يا نه ابتدا از هر سايت كامپيوترهاي سايت مقابل را ping مي‌كنيم. سپس با استفاده از Command زير تانل را چك مي‌كنيم.

```
1  Router#show crypto ipsec sa
.
.  …
10   #pkts encaps: 23, #pkts encrypt: 23, #pkts digest: 0
11   #pkts decaps: 21, #pkts decrypt: 21, #pkts verify: 0
.  …
.
```

در صورتیکه تانل برقرار باشد و پکت‌ها بعد از ping کردن، بین دو سایت رد و بدل شده باشد این مقادیر **pkts encaps** ، **pkts encrypt** ، **pkts decaps**و **pkts decrypt** نباید صفر باشد، در صورتیکه که صفر باشد نشان دهنده‌ي این است که تانل ایجاد نشده است.

فصل 12

مباحث تکمیلی

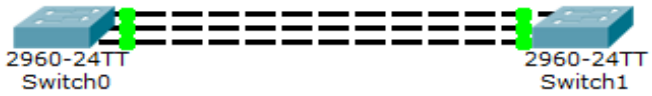
تکنولوژی EtherChannel

➢ **ساختار EtherChannel در پورت سوئیچ:**

- در سوئیچ‌هاي لايه 2 و لايه 3 به‌منظور يكپارچه‌سازي تمامي لينك‌هاي سوئيچ، براي استفاده از حداكثر ظرفيت ارتباطي مورد استفاده قرار مي‌گيرد.
- به‌صورت پيش‌فرض اگر بين دو سوئيچ چند مسير وجود داشته باشد (يعني Loop داشته باشيم)، سيستم بصورت اتوماتيك يك مسير را باز مي‌گذارد و بقيه مسيرها را بلاك مي‌كند، براي اينكه جلوي بلاك شدن را بگيريم، بايد باقي مسيرهاي موجود را ادغام (Bundle) كنيم.

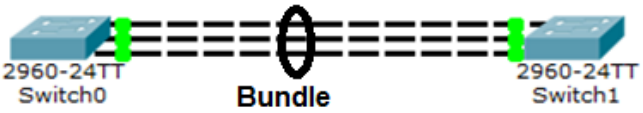
شکل 12-1 لینک های ارتباطی بین

- همانگونه كه در شكل (12-1) مي‌بينم فقط يكي از مسيرها باز است (دو سمت ارتباط به رنگ سبز است) و دو لينك ديگر تنها يك سر لينك سبز است و سر ديگر ارتباط بلاك (به رنگ نارنجي در آمده) شده است.
- حال اگر اين لينك‌ها را با هم ادغام كنيم ارتباط كليه‌ي مسيرهاي ادغام شده برقرار مي‌گردد.



شکل 12-2 ادغام لینک‌های

- لينك‌هاي ادغام شده (Bundle) به‌صورت شكل (12-3) نمايش داده مي‌شود.



شکل 12-3 نحوه نمایش

- ادغام چندين پورت سوئيچ بعنوان يك لينك منطقي را Etherchannel يا Aggregation يا Bundling مي‌نامند.
- حداقل 2 و حداكثر 8 لينك مي‌تواند در هر Etherchannel قرار بگيرد.
- پورت‌هايي كه مي‌خواهند ادغام شوند بايد عضو يك Vlan باشند اگر بعنوان Trunk بخواهند استفاده شوند بايد پورت ها در حالات trunk باشند و حتي Speed و از نظر Duplex آن‌ها بايد يكسان باشند.

- هر EtherChannel می‌تواند از سوئیچ به سرور، سوئیچ به روتر، سوئیچ به فایروال و سوئیچ به سوئیچ استفاده شود.
- فقط پورت‌های فیزیکی (اترنت یا فیبر) مشابه می‌توانند ادغام شوند.

- Loadbalancing براساس Mac Address است.
- ترافیک به‌طور مساوی روی لینک‌ها فرستاده نمی‌شود بر اساس الگوریتم از یک لینک خاص فرستاده می‌شوند.
- EtherChannel، دارای 3 پروتکل است: **LACP -1** **PAGP -2** **Without -3**

mode	SW1	SW2
LACP	Active	Passive
PAGP	Auto	Desirable
Without	On	On

PAGP: این پروتکل توسط شرکت سیسکو ارائه شده است و دارای 2 مد است:

- Auto: در این حالت سوئیچ به پیغام‌های PAGP جواب می‌دهد یعنی صبر می‌کند تا از او خواسته شود اما ارتباط برقرار نمی‌شود.
- Desirable: در این حالت سوئیچ یک پیغام جهت برقراری ارتباط می‌فرستد.

اگر هر دو سمت سوئیچ در حالت Auto باشند Etherchannel برقرار نمی‌شود.

LACP: توسط IEEE ارائه شده و در انحصار سیسکو نیست لذا بقیه تولیدکنندگان از LACP به‌صورت استاندارد 802.3ad استفاده می‌کنند. تا 16 پورت را می‌توان در یک Etherchannel گنجاند اما 8 پورت Active و 8 پورت دیگر بقیه بصورت Standby در می‌آیند و دارای 2 مد است:

- Passive: سوئیچ صبر می‌کند تا از او جهت برقراری Etherchannel خواسته شود
- Active: سوئیچ یک پیغام جهت برقراری Etherchanne می‌فرستد

شکل 12-

Switch 0:

```
1  Switch0(config)#interface port-channel 2
2  Switch0(config-if)#no shutdown
3
4  Switch0(config)#interface range fastEthernet 0/1-3
5  Switch0(config-if-range)#channel-group 2 mode active
```

Switch 1:

```
1  Switch1(config)#interface port-channel 2
2  Switch1(config-if)#no shutdown
3
4  Switch1(config)#interface range fastEthernet 0/1-3
5  Switch1(config-if-range)#channel-group 2 mode passive
```

Switch0 :

- خط 1:

interface port-channel شماره ي دلخواه (در اينجا شماره 2)
Switch0(config)#

- خط 4: وارد Interface هايي مي‌شويم كه مي‌خواهيم در يك گروه قرار دهيم.

- خط 5:

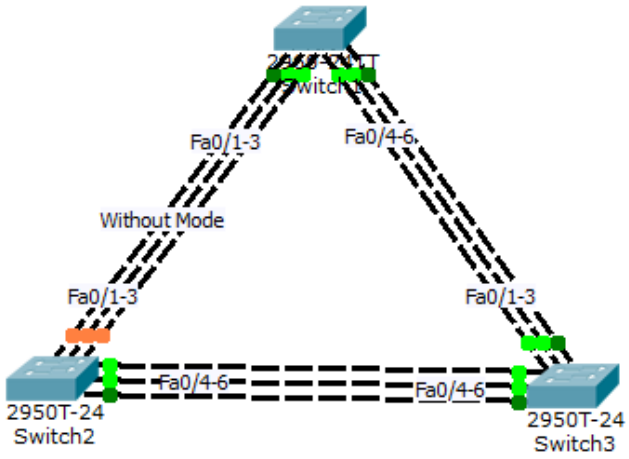
مد مورد نظر (در اينجا Active) mode شماره اي كه در خط 1 انتخاب كرده بوديم
Switch0(config-if-range)# channel-group

Switch1 :

- خط 1: دقيقا همان شماره‌اي كه در سوئيچ مقابل انتخاب كرده‌ايم را بايد وارد كنيم (كه در اينجا شماره 2 را انتخاب كرده ايم).
- خط 5:

مد مورد نظر (در اينجا desirable) mode شماره اي كه در خط 1 سوئيچ اول انتخاب كرده بوديم
Switch1(config-if-range)# channel-group

سناریو: راه اندازي ساختار EtherChannel

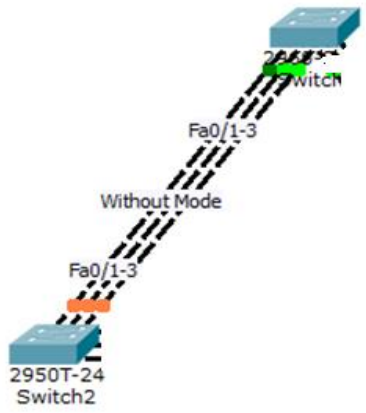


شکل 12-5 سناریو راه اندازی

1- Without Mode:

Switch 1 , Port Fa0/1-3

Switch 2 , Port Fa0/1-3

1 2 3 4 5	Switch1(config)#**interface port-channel 1** Switch1(config-if)#**no shutdown** Switch1(config)#**interface range fastEthernet 0/1-3** Switch1(config-if-range)#**channel-group 1 mode on**	
	sw2-port 0/1-3	
1 2 3 4 5	Switch2(config)#**interface port-channel 1** Switch2(config-if)#**no shutdown** Switch2(config)#**interface range fastEthernet 0/1-3** Switch2(config-if -range)#**channel-group 1 mode on**	

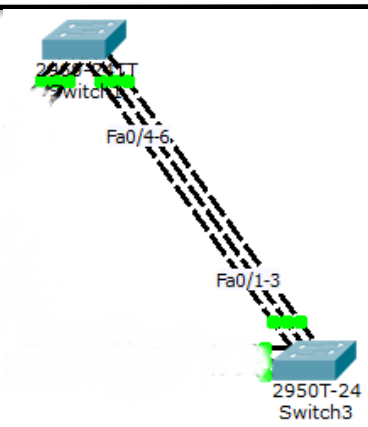
2- PAGP Mode:

Switch 1 - Port Fa0/4-6

Switch 3 - Port Fa0/1-3

	Sw1- port0/4-6	
1 2 3	Switch1(config)#**interface port-channel 2** Switch1(config-if)#**no shutdown**	

4 5	Switch1(config)#**interface range fastEthernet 0/4-6** Switch1(config-if-range)#**channel-group 2 mode auto**
	Sw3- port 0/1-3
1 2 3 4 5	Switch(config)#**interface port-channel 2** Switch(config-if)#**no shutdown** Switch(config)#**interface range fastEthernet 0/1-3** Switch(config-if-range)#**channel-group 2 mode desirable**

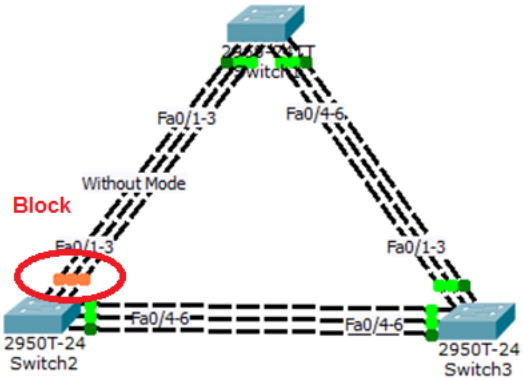


3- LACP

Switch 2 - Port Fa0/4-6
Switch 3 - Port Fa0/4-6

	Sw2-port-0/4-6
1 2 3 4 5	Switch2(config)#**interface port-channel 3** Switch2(config-if)#**no shutdown** Switch2(config)#**interface range fastEthernet 0/4-6** Switch2(config-if-range)#**channel-group 3 mode passive**
	Sw 3-port0/4-6
1 2 3 4 5	Switch3(config)#**interface port-channel 3** Switch3(config-if)#**no shutdown** Switch3(config)#**interface range fastEthernet 0/4-6** Switch3(config-if-range)#**channel-group 3 mode active**

همان‌طوري‌كه در شكل اول مي‌بينيد به علت به وجود آمدن حلقه (Loop)، خود سيستم يكي از مسيرها را مسدود مي‌كند(كه در اينجا لينك ارتباطي بين Sw1 و Sw2 را مسدود كرده است.



mode	SW1	SW2

LACP	Active	Passive
PAGP	Auto	Desirable
Without	On	On

FHRP[1]

- FHRP گروهی از پروتکل‌ها است که اگر بیش از یک مسیر به مقصد یکسان وجود داشته باشد، افزونگی Gateway پیش فرض را فراهم می‌کنند.
- انواع FHRP عبارتند از:
  - **HSRP**[2]
  - **VRRP**[3]
  - **GLBP**[4]
- FHRP، دو یا چندین دستگاه (روترها) را قادر می‌سازد تا با همدیگر در یک گروه کار کنند. آن ها یک IP Address مشترک با نام IP Address مجازی[5] را به اشتراک می‌گذارند. این IP Address مجازی به عنوان آدرس Gateway پیش فرض برای هاست‌های LAN است.

HSRP

- با یک مدل active/standby عمل می‌کند.
- پروتکل اختصاصی شرکت سیسکو است.
- از IP Address مجازی استفاده می‌کند.
- پروتکل لایه‌ی 3 است.
- از ipv6 پشتیبانی می‌کند.
- شماره پورت: UDP 1985
- HSRP اجازه می‌دهد تا دو روتر با یکدیگر همکاری کنند، هر دو مایل هستند که به عنوان روتر پیش فرض عمل کنند.
- فقط یک روتر به‌طور فعال (active)ترافیک کاربر نهایی را پشتیبانی می‌کند، روتر دیگری در حالت انتظار(standby) می‌باشد.

- قابلیت tracking وجود دارد یعنی می‌توان دو گروه ایجاد کرد و در صورتی که یک گروه شکست خورد و گروه دیگری up شد، به‌صورت ضربدری بین گروه‌ها حرکت کرد.
- روتری که دارای اولویت بالاتری باشد به عنوان روتر فعال می‌باشد.

[1] First Hop Redundancy Protocol
[2] Hot Standby Router Protocol
[3] Virtual Router Redundancy Protocol
[4] Gateway Load Balancing Protocol
[5] Virtual IP Address

- اولویت همه‌ی روترها به‌صورت پیش‌فرض برابر 100 است.
- اگر اولویت همه‌ی روترها برابر باشد، روتر با IP Address بالاتر به عنوان روتر فعال انتخاب خواهد شد.
- همه‌ی روترهای مجازی از Mac Address: 0000.0c07.acxx استفاده می‌کنند (x شماره‌ی گروه است).

VRRP

- با یک مدل active/standby عمل می‌کند.
- پروتکل استاندارد IETF است.
- پروتکل لایه 3 است.
- از IP Address های واقعی استفاده می‌کند.
- از ipv6 پشتیبانی نمی‌کند.
- شماره پورت: UDP 112
- یک روتر به عنوان رئیس(Master) و بقیه به عنوان نسخه‌ی پشتیبان (backup) هستند.
- قابلیت tracking وجود ندارد.
- همه‌ی روترها از طریق IP Multicast: 224.0.0.18 برای ارتباط استفاده می‌کنند.
- همه‌ی روترهای مجازی از 0000-5E00-01xx به عنوان Mac Address خود استفاده می‌کنند.

GLBP

- با یک مدل active/listner عمل می‌کند.
- پروتکل اختصاصی سیسکو است.
- پروتکل لایه 2 است.
- از ipv6 پشتیبانی می‌کند.
- شماره پورت: UDP 3222
- یک gateway به عنوان gateway مجازی فعال(AVG[1]) برای گروه وجود دارد.
- انتخاب AVG براساس اولویت هر gateway (بالاترین اولویت) است.
- در صورتی که اولویت همه‌ی gateway ها برابر باشد، AVG براساس IP Address های واقعی انتخاب می‌شود.

- قابلیت tracking وجود ندارد.
- قابلیت loadbalancing وجود دارد.
- از IP Multicast: 224.0.0.102 برای ارتباط استفاده می‌کنند.
- از 0007.b4xx.xxxx به عنوان Mac Address خود استفاده می‌کنند.

[1] Gateway Virtual Gateway

Syslog

- Syslog یک برنامه‌ی کاربردی است که اطلاعات log از دستگاه های شبکه را ذخیره می‌کند.
- Syslog با یک مدل کلاینت/سرور کار می‌کند.
- Syslog با مدل کلاینت: یک دستگاه شبکه که پیام log را تولید می کند و به سرور Syslog ارسال می‌کند.
- Syslog با مدل سرور: یک کامپیوتر/سرور که نرم‌افزار نصب شده‌ی Syslog را دارد و پیام‌های Syslog را ذخیره و قبول می‌کند.

دستورات Syslog

1	Router(config)#**logging enable**
2	Router(config)#**logging on**
3	Router(config)#**logging buffered**
4	Router(config)#**logging <syslog server ip>**
5	Router#**show logging**

- خط1: دستور فعال‌سازی logging
- خط2: دستور نمایش شروع ارسال پیام‌های log به تمام موقعیت‌های خروجی
- خط3: دستور ارسال پیام‌های syslog به بافر داخلی log
- خط4: دستور ارسال پیام‌های Syslog به سرور
- خط5: نمایش پیکربندی اجرای logging

Netflow

- Netflow، ترتیب بسته‌های ارسالی از دستگاه مبدا به دستگاه مقصد است.
- در یک جریان، بسته‌ها شامل: IPی مبدا، IPی مقصد، اطلاعات پورت و ... است.

- Netflow یک سرویس است که در روتر و سوئیچ پیکربندی شده است.
- Netflow به مدیر اجازه می‌دهد تا جریان انواع مختلف ترافیک شبکه را مانیتور کند.
- همه‌ی سوئیچ‌ها و روترها، Netflow را پشتیبانی می‌کنند، با این حال یک IOS مناسب لازم است.

مزایای کلیدی Netflow

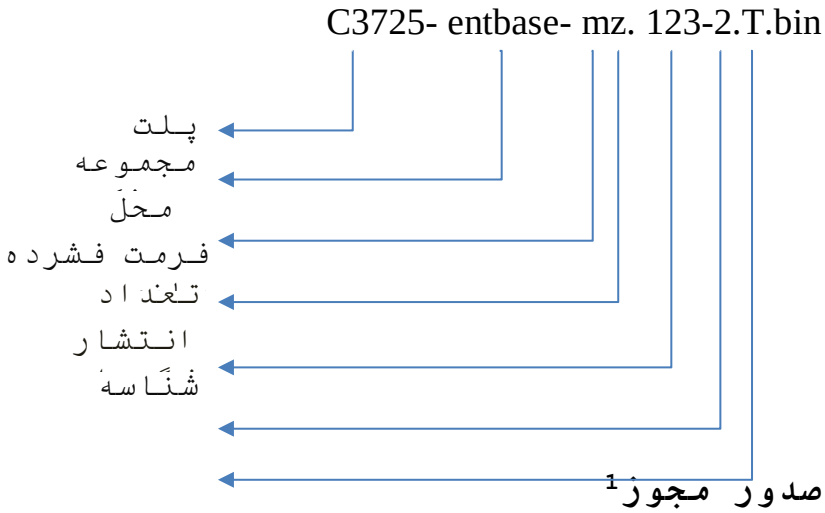
- بازدهی شبکه و استفاده از منابع شبکه
- آنامولی شبکه و آسیب‌پذیری‌های امنیتی
- مانیتورینگ استفاده از شبکه و برنامه‌های کاربردی

IOS-Licensing

- سیسکو برای هر سری روتر و سوئیچ به‌طور جداگانه IOS image را فراهم می‌کند. IOS image در نسخه‌های متعددی وجود دارد
- سیسکو بازبینی‌های مجدد برای نرم‌افزار IOS سیسکو با استفاده از اصطلاح نسخه فراهم می‌کند.

قرارداد نامگذاری IOS image سیسکو

- یک IOS image سیسکو، یک فایل اجرایی باینری از یک مجموعه ویژگی برای پلت فرم خاص است.
- نام IOS image سیسکو، اطلاعاتی شامل: پلت فرم، مجموعه ویژگی، فرمت و دیگر اطلاعات فایل image را نمایش می‌دهد.



صدور مجوز[1]

- مجوز نرم افزار توسط سیسکو با تعیین شماره محصول، شماره سریال و کلید فعال‌سازی محصول ارائه می‌شود.
- مجوز از طریق ایمیل یا CD پس از سفارش IOS با مجموعه ویژگی مورد نیاز دریافت خواهد شد.
- توجه داشته باشید: به صورت پیش فرض، ما مجوز را با دستگاهی که با ویژگی‌های مورد نیاز سفارش می‌دهیم، به‌دست خواهیم آورد.
- برای نصب مجوز، باید مجوز را با دستور زیر در سرور tftp کپی کرد.

1	Router#**license install tftp://<ip address of tftp>/license.lic**

- بعد از نصب موفقیت‌آمیز مجوز، روتر مجددا لود می‌شود.

CEF[2]

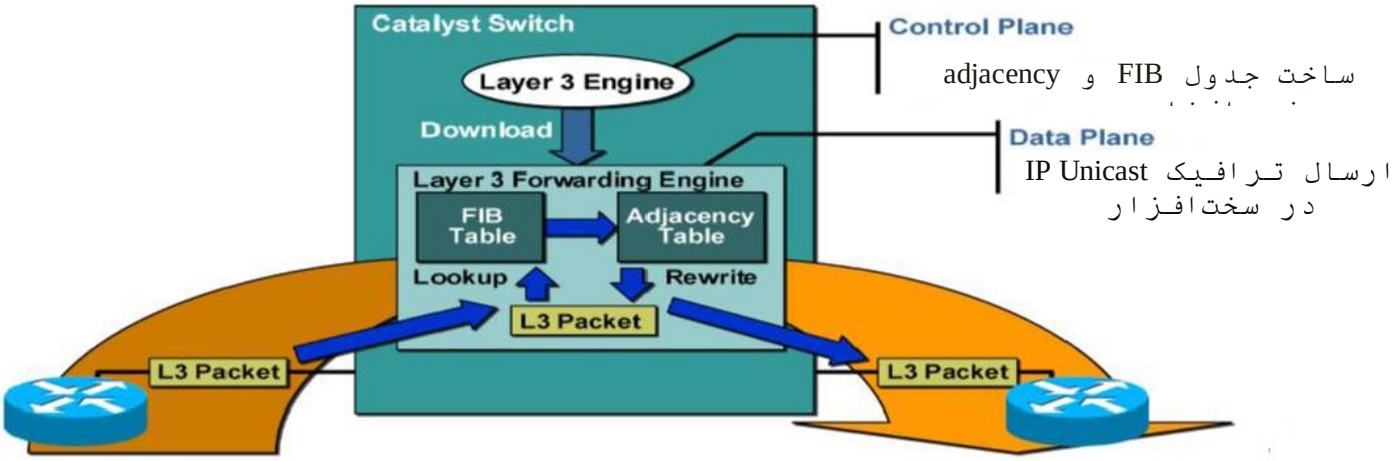
- یک تکنولوژی سوئیچینگ لایه 3 به‌صورت پیشرفته است.
- اساسا در هسته‌ی شبکه‌های بزرگ یا اینترنت برای بهبود کارایی کلی شبکه استفاده می‌شود.
- پروتکل اختصاصی شرکت سیسکو است.
- برای افزایش سرعت سوئیچینگ بسته با کاهش سربار و تاخیر توسط دیگر تکنیک‌های مسیریابی استفاده می‌شود.
- شامل دو مولفه‌ی کلیدی زیر می‌باشد:
  - FIB[3]

[1] licensing
[2] Cisco Express Forwarding
[3] Forwarding Information Base

- FIB شبیه به جدول مسیریابی است.
- FIB، مقصد را با IPای هاب بعدی نگاشت می‌کند.
- جدول FIB همراه با جدول مسیریابی آپدیت می‌شود.
- FIB در فرآیندهای سوئیچینگ سخت‌افزار استفاده می‌شود.

➢ Adjacencies

- جدول Adjancency اطلاعات لایه 2 یا سوئیچینگ مرتبط با ورودی خاص FIB را نگهداری می‌کند و از نیاز به درخواست ARP برای هر جدول lookup جلوگیری می‌کند.



شکل 12-6 چگونگی کارکرد CEF

دستور نمایش ورودی‌های CEF در FIB

	Switch#**show ip cef**

فصل 13

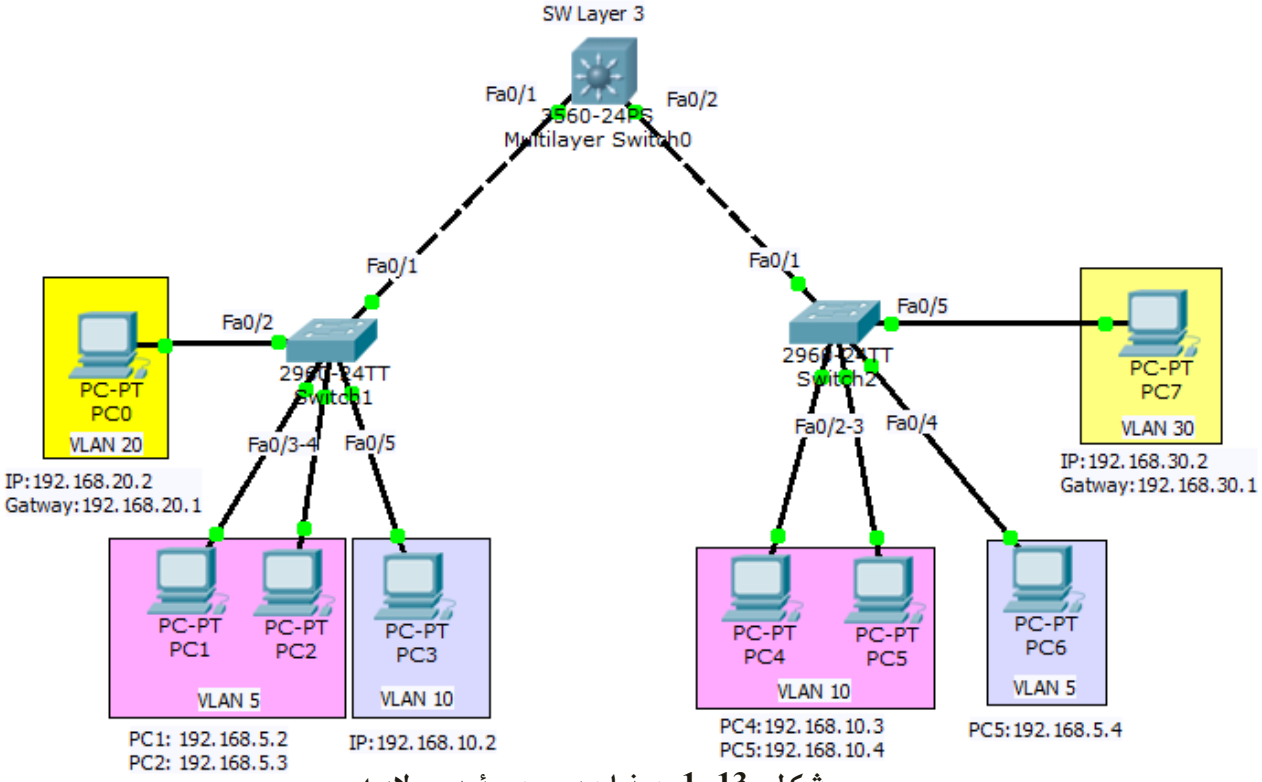
سناریوهای تکمیلی

سناریو : سوئیچ لایه 3- VLAN-VTP

- ساختار زیر را به گونه اي تنظیم نمایید که Vlan 20 بتواند Vlan 30 را Ping کند.
- سوئیچ بالا از نوع سوئچ لایه 3 باشد.
- VTP را راه اندازي نمایید. Domain: **cisco.com** و Pass: **ccna**
- رنج IP هاي زیر:

Vlan 5: 192.168.5.0/24
Vlan 10: 192.168.10.0/24
Vlan 20: 192.168.20.0/24

Vlan 30: 192.168.30.0/24



شکل 13-1 سناریو سوئیچ لایه 3

مراحل کار:

1. برقراري لينكهاي Trunk بين سوئيچها: ارتباط بين دو سوئيچ بايد از نوع Trunk تعريف كنيم.

براي اينكه در سوئيچ لايه 3 بخواهيم پورتي را از نوع Trunk تعريف كنيم بايد دستورهای زير را بنويسيم:

1	Sw(config)#**interface fastEthernet** **شماره‌ی اینترفیس مورد نظر**
2	Sw(config-if)#**switchport trunk encapsulation dot1q**
3	Sw(config-if)#**switchport mode trunk**

SW Layer3

1	Switch(config)#**interface fastEthernet 0/1**
2	Switch(config-if)#**switchport trunk encapsulation dot1q**
3	Switch(config-if)#**switchport mode trunk**
4	
5	Switch(config)#**interface fastEthernet 0/2**
6	Switch(config-if)#**switchport trunk encapsulation dot1q**
7	Switch(config-if)#**switchport mode trunk**

Sw1 , Sw2:

```
1 Switch(config)#interface fastEthernet 0/1
2 Switch(config-if)#switchport mode trunk
```

2. تعریف VTP (سوئیچ سرور و سوئیچ کلاینت) :

سوئیچ لایه‌ي 3 در اینجا به‌عنوان سرور است:

Sw Layer3:

```
1 Switch(config)#vtp mode server
2 Switch(config)#vtp domain cisco.com
3 Switch(config)#vtp password ccna
```

دو سوئیچ دیگر به‌عنوان کلاینت هستند(در این حالت دیگر نیاز نیست VLAN ها را در هر یك از سوئیچ‌ها تعریف کنیم و VLAN ها را فقط در سوئیچ سرور تعریف مي‌کنیم) :

Sw 1, Sw2:

```
1 Switch(config)#vtp mode client
2 Switch(config)#vtp password ccna
```

3. تعریف VLAN ها در سوئیچ سرور:

```
1 Switch(config)#vlan 5
2 Switch(config-vlan)#vlan 10
3 Switch(config-vlan)#vlan 20
4 Switch(config-vlan)#vlan 30
```

مشاهده‌ي VLAN ها در سوئیچ‌هاي کلاینت:

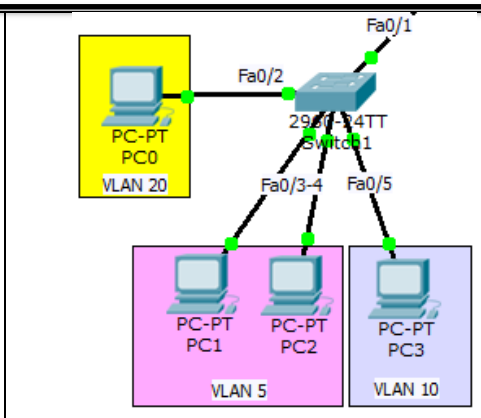
Sw1, Sw2:

```
1 Switch#show vlan brief
```

قرار دادن کامپیوترها در VLANهاي مورد نظر:

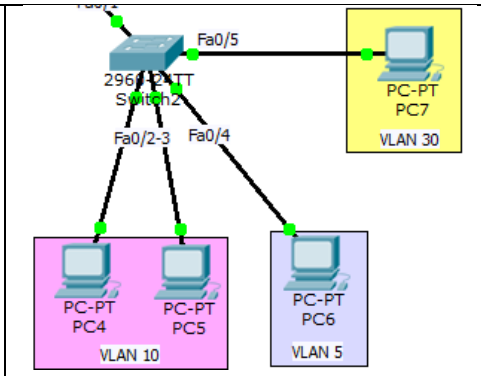
Sw1:

```
1  Switch(config)#interface fastEthernet 0/2
2  Switch(config-if)#switchport mode access
3  Switch(config-if)#switchport access vlan 20
4
5  Switch(config)#interface range fastEthernet 0/3-4
6  Switch(config-if-range)#switchport mode access
7  Switch(config-if-range)#switchport access vlan 5
8
9  Switch(config)#interface fastEthernet 0/5
10 Switch(config-if)#switchport mode access
11 Switch(config-if)#switchport access vlan 10
```

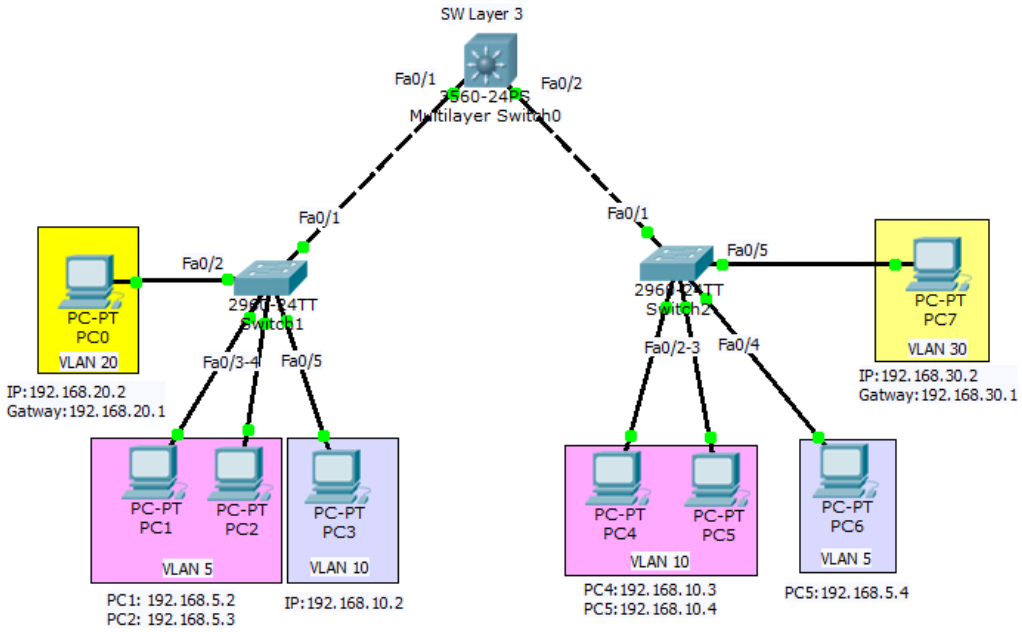


Sw 3:

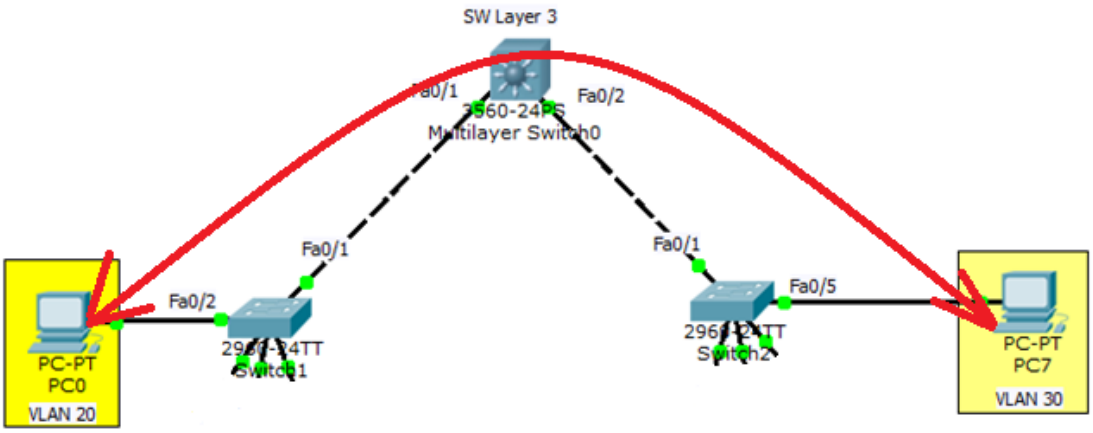
```
1  Switch(config)#interface fastEthernet 0/5
2  Switch(config-if)#switchport mode access
3  Switch(config-if)#switchport access vlan 30
4
5  Switch(config)#interface fastEthernet 0/4
6  Switch(config-if)#switchport mode access
7  Switch(config-if)#switchport access vlan 5
8
9  Switch(config)#interface range fastEthernet 0/2-3
10 Switch(config-if-range)#switchport mode access
11 Switch(config-if-range)#switchport access vlan 10
```



حال به کامپیوترها IP می‌دهیم:



4. ایجاد Interface VLAN :



Sw Layer3:

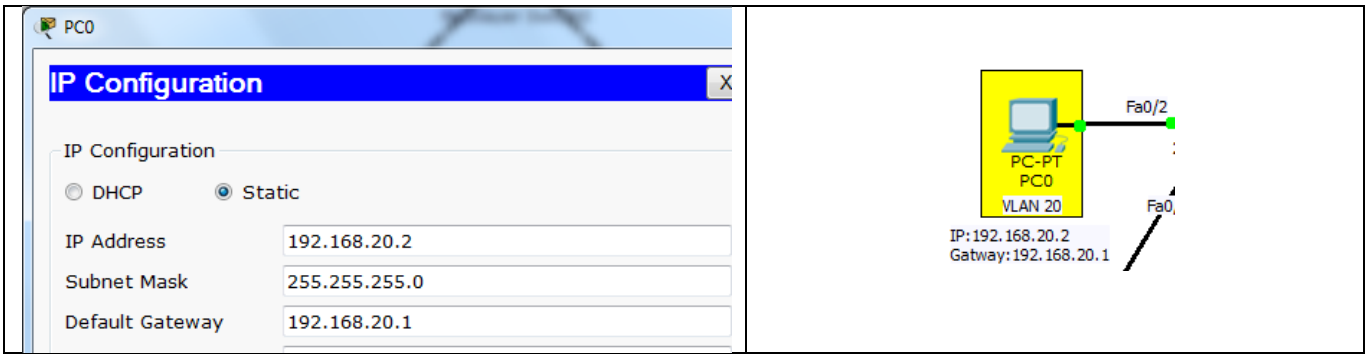
```
1  Switch(config)#interface vlan 20
2  Switch(config-if)#ip address 192.168.20.1 255.255.255.0
3
4  Switch(config)#interface vlan 30
5  Switch(config-if)#ip address 192.168.30.1 255.255.255.0
6
7  Switch(config)#ip routing
```

خط 1: براي اينكه دو VLAN با رنج IP هاي متفاوت را با هم اتصال دهيم بايد ابتدا يك Interface مجازي بسازيم .

خط 2: سپس به این Interface ساخته شده IP اختصاص میدهیم.که این IP را باید به‌عنوان Gateway کامپیوترهای موجود در VLAN های مربوطه تعریف کنیم:

تعریف Interface Vlan مجازی برای Vlan 20:

Switch(config)#**interface vlan 20**
Switch(config-if)#**ip address 192.168.20.1 255.255.255.0**



خط 7: سپس با دستور ip routing ارتباط بین این دو VLAN غیرهمنام برقرار میگردد.

کانفیگ کلی:

Sw Layer 3:

```
1  Switch(config)#interface fastEthernet 0/1
2  Switch(config-if)#switchport trunk encapsulation dot1q
3  Switch(config-if)#switchport mode trunk
4
5  Switch(config)#interface fastEthernet 0/2
6  Switch(config-if)#switchport trunk encapsulation dot1q
7  Switch(config-if)#switchport mode trunk
8
9  Switch(config)#vtp mode server
10 Switch(config)#vtp domain cisco.com
11 Switch(config)#vtp password ccna
12
13 Create VLAN:
14 Switch(config)#vlan 5
15 Switch(config-vlan)#vlan 10
16 Switch(config-vlan)#vlan 20
17 Switch(config-vlan)#vlan 30
18
19 Creat Interface VLAN:
20 Switch(config)#interface vlan 20
21 Switch(config-if)#ip address 192.168.20.1 255.255.255.0
22 Switch(config)#interface vlan 30
```

23	Switch(config-if)#**ip address 192.168.30.1 255.255.255.0**
24	Switch(config)#**ip routing**

Sw1:

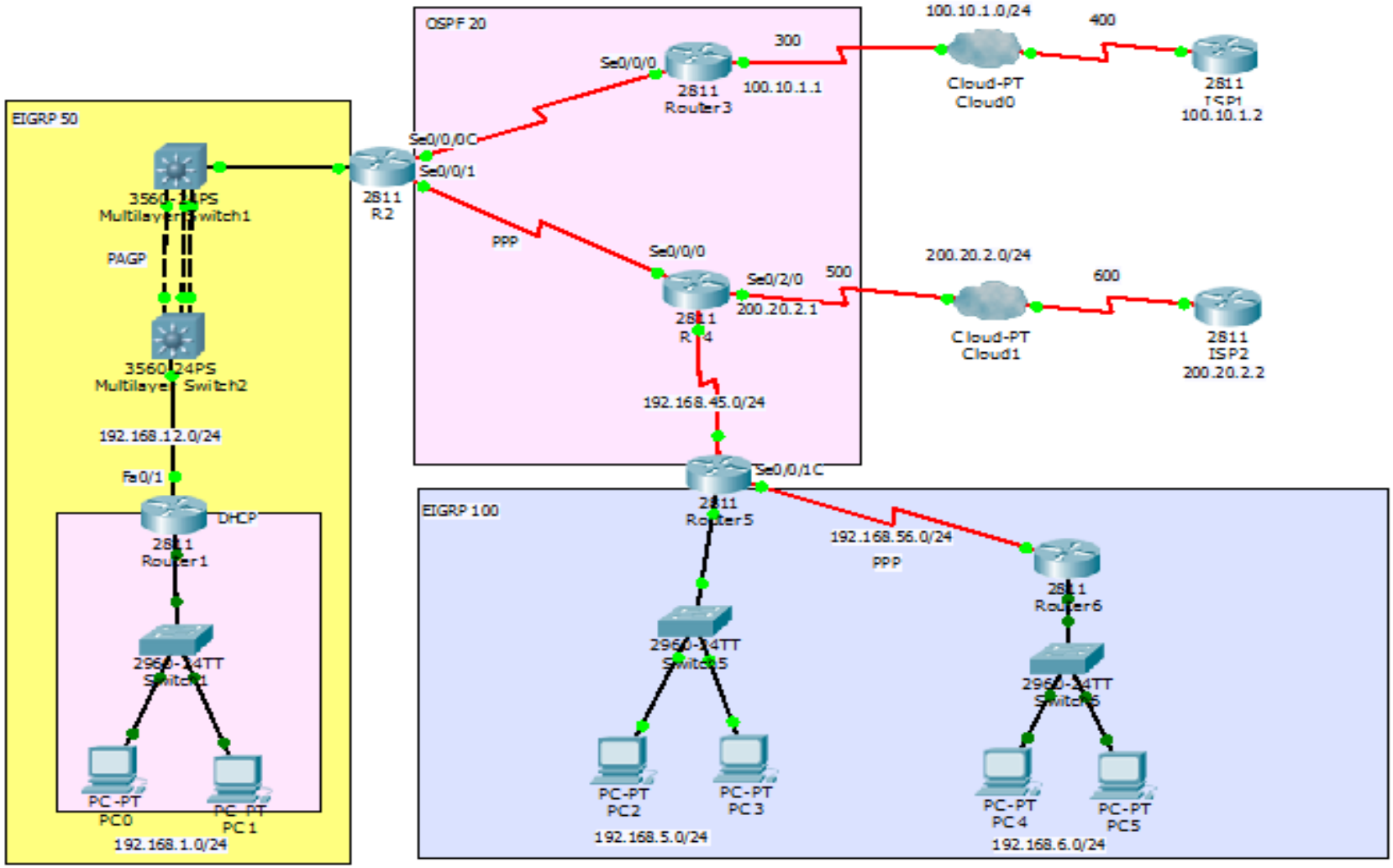
1	Switch(config)#**interface fastEthernet 0/1**
2	Switch(config-if)#**switchport mode trunk**
3	
4	Define VTP:
5	Switch(config)#**vtp mode client**
6	Switch(config)#**vtp password ccna**
7	
8	View VLAM:
9	Switch#**show vlan b**
10	
11	Assign Vlan to interfases:
12	Switch(config)#**interface fastEthernet 0/2**
13	Switch(config-if)#**switchport mode access**
14	Switch(config-if)#**switchport access vlan 20**
15	
16	Switch(config)#**interface range fastEthernet 0/3-4**
17	Switch(config-if-range)#**switchport mode access**
18	Switch(config-if-range)#**switchport access vlan 5**
19	
20	Switch(config)#**interface fastEthernet 0/5**
21	Switch(config-if)#**switchport mode access**
22	Switch(config-if)#**switchport access vlan 10**

SW2

1	Switch(config)#**interface fastEthernet 0/1**
2	Switch(config-if)#**switchport mode trunk**
3	
4	Define VTP:
5	Switch(config)#**vtp mode client**
6	Switch(config)#**vtp password ccna**
7	
8	Assign Vlan to interfases:
9	Switch(config)#**interface fastEthernet 0/5**
10	Switch(config-if)#**switchport mode access**
11	Switch(config-if)#**switchport access vlan 30**
12	
13	Switch(config)#**interface fastEthernet 0/4**
14	Switch(config-if)#**switchport mode access**
15	Switch(config-if)#**switchport access vlan 5**

```
16
17 Switch(config)#interface range fastEthernet 0/2-3
18 Switch(config-if-range)#switchport mode access
19 Switch(config-if-range)#switchport access vlan 10
```

سناریو : Frame relay -PPP - PAGP-DHCP



شکل 13-2 سناریو : Frame relay -PPP - PAGP-DHCP

با توجه به دیاگرام شکل(13-2) به سوالات پاسخ دهید:

سوال 1: با IP های داده شده به اختصاص آدرس‌ها پرداخته و سرویس DHCP در روتر R1 پیاده سازی گردد.

سوال 2: ارتباط سوئیچ‌های 1 با 2 را با استفاده از پروتکل PAGP پیاده سازی نمایید.

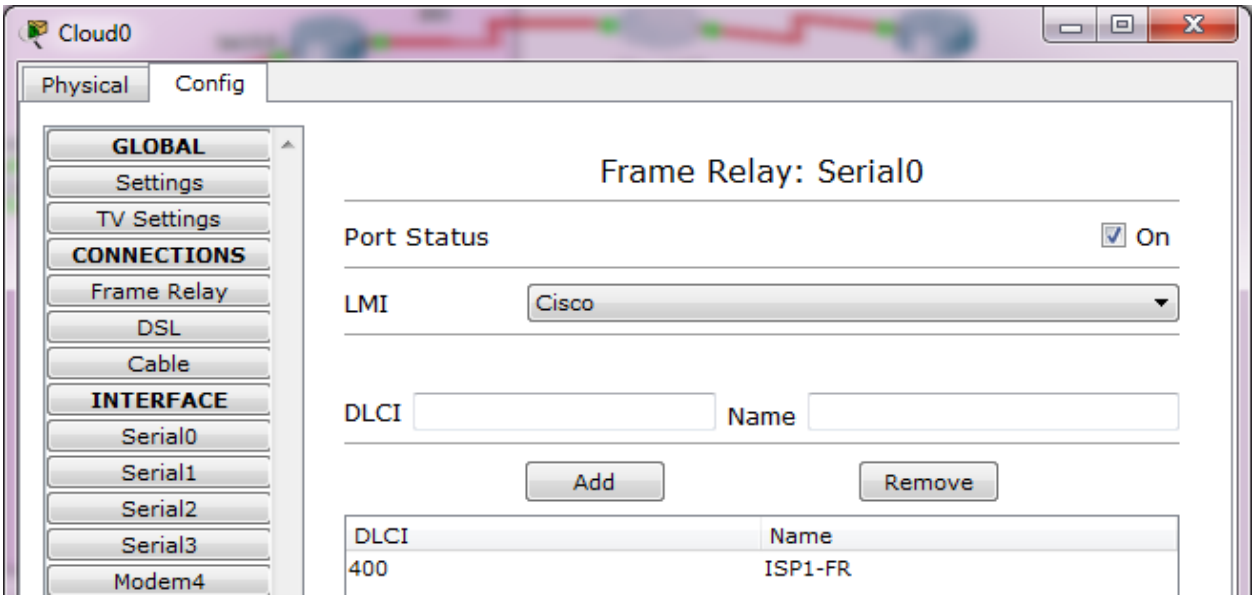
سوال 3: با استفاده از پروتکل PPP ارتباط روتر 2 با 4 و روتر 5 با 6 را راه اندازی نموده و مکانیزم احراز هویت Chap استفاده گردد.

سوال 4: پروتکل‌های مسیریابی مطابق با دیاگرام را پیاده‌سازی نموده و برای ارتباط روتر 2 با 4 از مکانیزم MD5 با پسورد ccna و برای ارتباط روتر 2 با 3 از مکانیزم MD5 با پسورد ccna استفاده نمایید.

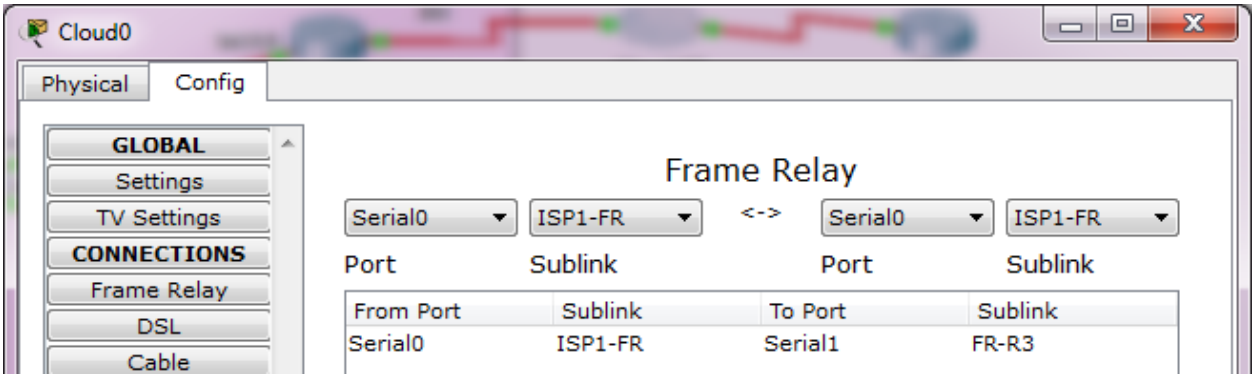
سوال 5: دسترسی روترهای 3 و 4 را با ISP برقرار نموده و دسترسی کاربران سوئیچ 1 را به هر دوی این‌ها مقدور نمایید.

جواب 1:

Cloud 0:

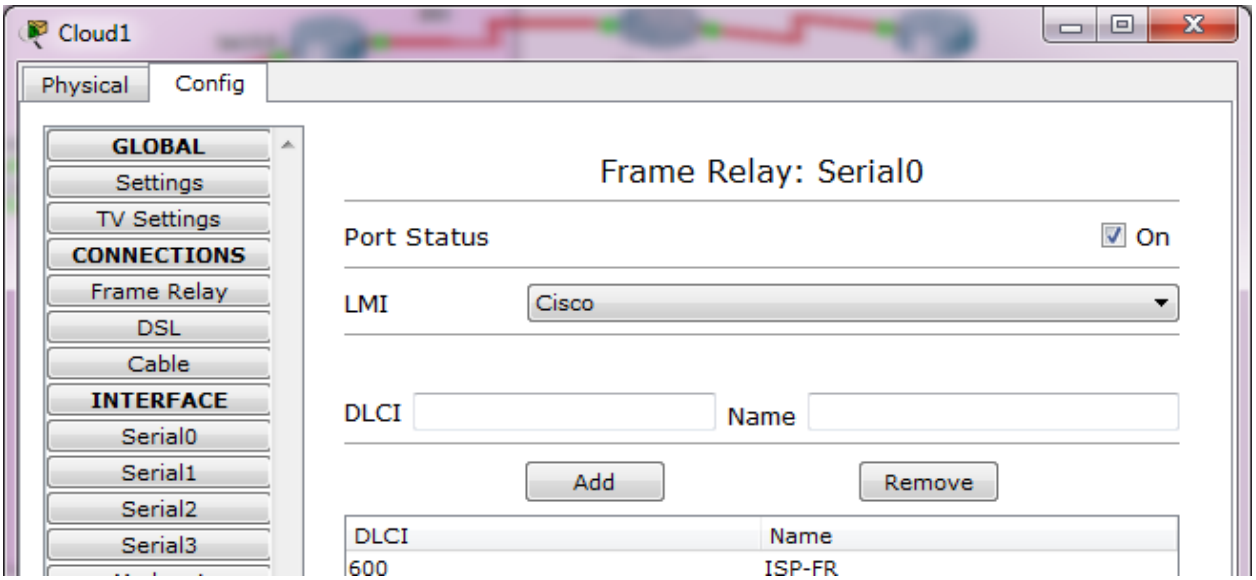


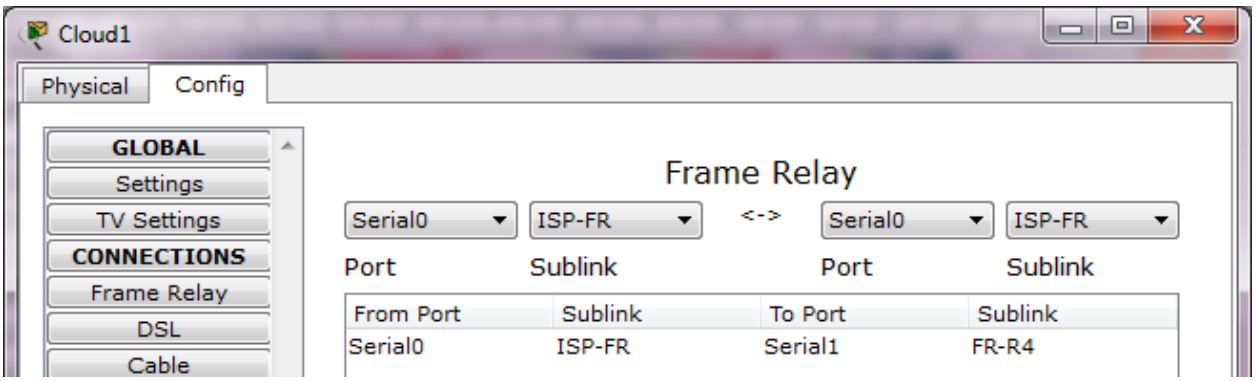
شکل 13-3 تنظیم DLCI برای اینترفیس در Cloud 0



شکل 13-4 تنظیم Framerelay در

Cloud1:





شکل 13-5 تنظیمات DLCI و Framerelay در Cloud1

ج 1:

R1:

```
1  Router(config)#ip dhcp pool test
2  Router(dhcp-config)#network 192.168.1.0 255.255.255.0
3  Router(dhcp-config)#default-router 192.168.1.1
4
5  Router(config)#interface fastEthernet 0/0
6  Router(config-if)#ip address 192.168.1.1 255.255.255.0
7  Router(config-if)#no shutdown
```

8	
9	Router(config)#**interface fastEthernet 0/1**
10	Router(config-if)#**ip address 192.168.12.1 255.255.255.0**
11	Router(config-if)#**no shutdown**

R2:

1	Router(config)#**hostname R2**
2	R2(config)# **interface FastEthernet0/0**
3	R2(config-if)#**ip address 192.168.12.2 255.255.255.0**
4	R2(config-if)#**no shutdown**
5	
6	R2(config)#**interface Serial0/0/0**
7	R2(config-if)# **ip address 192.168.23.1 255.255.255.0**
8	R2(config-if)#**clock rate 64000**
9	R2(config-if)#**no shutdown**
10	
11	R2(config)# **interface Serial0/0/1**
12	R2(config-if)# **ip address 192.168.24.1 255.255.255.0**
13	R2(config-if)# **clock rate 64000**
14	R2(config-if)#**no shutdown**

R3:

1	Router(config)# **interface Serial0/0/0**
2	Router(config-if)# **ip address 192.168.23.2 255.255.255.0**
3	Router(config-if)#**no shutdown**
4	
5	Ruter(config)# **interface Serial0/0/1**
6	Router(config-if)# **ip address 100.10.1.1 255.255.255.0**
7	Router(config-if)#**no shutdown**

R4:

```
1  Router(config)#hostname R4
2
3  R4(config)# interface Serial0/0/0
4  R4(config-if)# ip address 192.168.24.2 255.255.255.0
5  R4(config-if)#no shutdown
6
7  R4(config)#interface Serial0/0/1
8  R4(config-if)#ip address 192.168.45.1 255.255.255.0
9  R4(config-if)# clock rate 64000
10 R4(config-if)#no shutdown
11
12 R4(config)# interface Serial0/2/0
13 R4(config-if)#ip address 200.20.2.1 255.255.255.0
14 R4(config-if)#no shutdown
```

R5:

```
1  Router(config)#interface FastEthernet0/0
2  Router(config-if)#ip address 192.168.5.1 255.255.255.0
3  Router(config-if)#no shutdown
4
5  Router(config)#interface Serial0/0/0
6  Router(config-if)#ip address 192.168.45.2 255.255.255.0
7  Router(config-if)#no shutdown
8
9  Router(config)#interface Serial0/0/1
10 Router(config-if)#ip address 192.168.56.1 255.255.255.0
11 Router(config-if)#clock rate 64000
12 Router(config-if)#no shutdown
```

R6:

```
1  Router(config)#interface FastEthernet0/0
2  Router(config-if)#ip address 192.168.6.1 255.255.255.0
3  Router(config-if)#no shutdown
4
5  Router(config)#interface Serial0/0/0
6  Router(config-if)#ip address 192.168.56.2 255.255.255.0
7  Router(config-if)#no shutdown
```

ISP1:

```
1  Router(config)#interface Serial0/0/0
2  Router(config-if)#ip address 100.10.1.2 255.255.255.0
3  Router(config-if)#no shutdown
```

ISP2:

```
1  Router(config)#interface Serial0/0/0
2  Router(config-if)# ip address 200.20.2.2 255.255.255.0
3  Router(config-if)#no shutdown
```

جواب2: ارتباط سوئیچ‌های 1 با 2 را با استفاده از پروتکل PAGP پیاده سازی نمایید.

SW1:

```
1  Switch(config)#interface port-channel 1
2  Switch(config)#no shutdown
3
4  Switch(config)#interface FastEthernet0/2
5  Switch(config-if)#channel-group 1 mode desirable
6
7  Switch(config)#interface FastEthernet0/3
8  Switch(config-if)#channel-group 1 mode desirable
9
10 Switch(config)#interface FastEthernet0/4
11 Switch(config-if)#channel-group 1 mode desirable
```

SW2:

```
1  Switch(config)#interface port-channel 1
2  Switch(config)#no shutdown
3
4  Switch(config)# interface FastEthernet0/2
5  Switch(config-if)# channel-group 1 mode auto
6
7  Switch(config)# interface FastEthernet0/3
8  Switch(config-if)# channel-group 1 mode auto
9
10 Switch(config)# interface FastEthernet0/4
11 Switch(config-if)# channel-group 1 mode auto
```

جواب 3: با استفاده از پروتکل ppp ارتباط روتر 2 با 4 و روتر 5 با 6 را راه اندازی نموده و از مکانیزم احراز هویت chap استفاده گردد.

R2:

```
1  R2(config)# username R4 password 0 1234
2
3  R2(config)# interface Serial0/0/1
4  R2(config-if)# encapsulation ppp
5  R2(config-if)# ppp authentication chap
```

R4:

```
1  R4(config)#username R2 password 0 1234
2
3  R2(config)#interface Serial0/0/0
4  R2(config-if)#encapsulation ppp
5  R2(config-if)#ppp authentication chap
```

R5, R6:

R5:

```
1  Router(config)#hostname R5
2  R5(config)#username R6 password 0 1234
3
4  R5(config)#interface Serial0/0/1
5  R5(config-if)#encapsulation ppp
6  R5(config-if)#ppp authentication chap
```

R6:

```
1  R4(config)#hostname R6
2  R4(config)#username R5 password 0 1234
3
4  R2(config)#interface Serial0/0/0
5  R2(config-if)#encapsulation ppp
6  R2(config-if)#ppp authentication chap
```

جواب 4: پروتکل‌های مسیریابی مطابق با دیاگرام را پیاده سازی نموده و برای ارتباط روتر 2 با 4 از مکانیزم MD5 با پسورد ccna و برای ارتباط روتر 2 با 3 از مکانیزم MD5 با پسورد ccna استفاده نمایید.

R1:

```
1  Router(config)# router eigrp 50
2  Router(config-router)#network 192.168.1.0
3  Router(config-router)#network 192.168.12.0
```

R2:

```
1  R2(config)#interface Serial0/0/0
2  R2(config-if)#ip ospf authentication message-digest
3  R2(config-if)#ip ospf authentication-key ccna
4
5  R2(config)#router eigrp 50
```

6	R2(config-router)#**network 192.168.12.0**
7	
8	R2(config-router)#**redistribute ospf 1 metric 1 1 1 1 1**
9	
10	R2(config)#**router ospf 1**
11	R2(config-router)#**router-id 2.2.2.2**
12	R2(config-router)#**network 192.168.24.1 0.0.0.0 area 20**
13	R2(config-router)#**network 192.168.23.1 0.0.0.0 area 20**
14	R2(config-router)#**redistribute eigrp 50 metric 1 subnets**

R3:

1	Router(config)#**interface Serial0/0/0**
2	Router(config-if)#**ip ospf authentication message-digest**
3	Router(config-if)#**ip ospf authentication-key ccna**
4	
5	Router(config)#**router ospf 1**
6	Router(config-router)#**router-id 3.3.3.3**
7	Router(config-router)#**network 192.168.23.2 0.0.0.0 area 20**
8	Router(config-router)#**network 100.10.1.1 0.0.0.0 area 20**

R4:

1	R4(config)#**interface Serial0/0/0**
2	R4(config-if)#**ip ospf authentication message-digest**
3	R4(config-if)#**ip ospf authentication-key ccnp**
4	
5	R4(config)#**router ospf 1**
6	R4(config-router)#**router-id 4.4.4.4**
7	Router(config-router)#**network 192.168.24.2 0.0.0.0 area 20**
8	Router(config-router)#**network 192.168.45.1 0.0.0.0 area 20**
9	Router(config-router)#**network 200.20.2.1 0.0.0.0 area 20**

R5:

1	R5(config)#**router eigrp 100**
2	R5(config-router)#**network 192.168.5.0**
3	R5(config-router)#**network 192.168.56.0**
4	R5(config-router)#**redistribute ospf 1 metric 1 1 1 1 1**
5	
6	R5(config)#**router ospf 1**
7	R5(config-router)#**router-id 5.5.5.5**
8	R5(config-router)#**network 192.168.45.2 0.0.0.0 area 20**
9	R5(config-router)#**redistribute eigrp 100 metric 1 subnets**

R6:

```
1  R6(config)#router eigrp 100
2  R6(config-router)#network 192.168.6.0
3  R6(config-router)#network 192.168.56.0
```

ISP1:

```
1  Router(config)#interface Serial0/0/0
2  Router(config-if)#ip address 100.10.1.2 255.255.255.0
3  Router(config-if)#encapsulation frame-relay
4  Router(config-if)#frame-relay map ip 100.10.1.1 400 broadcast
```

ISP2:

```
1  Router(config)#interface Serial0/0/0
2  Router(config-if)# ip address 200.20.2.2 255.255.255.0
3  Router(config-if)#encapsulation frame-relay
4  Router(config-if)# frame-relay map ip 200.20.2.1 600 broadcast
```

جواب 5: دسترسی روترهای 3 و 4 را با ISP برقرار نموده و دسترسی کاربران سوئیچ 1 را به هر دوی این‌ها مقدور نمایید.

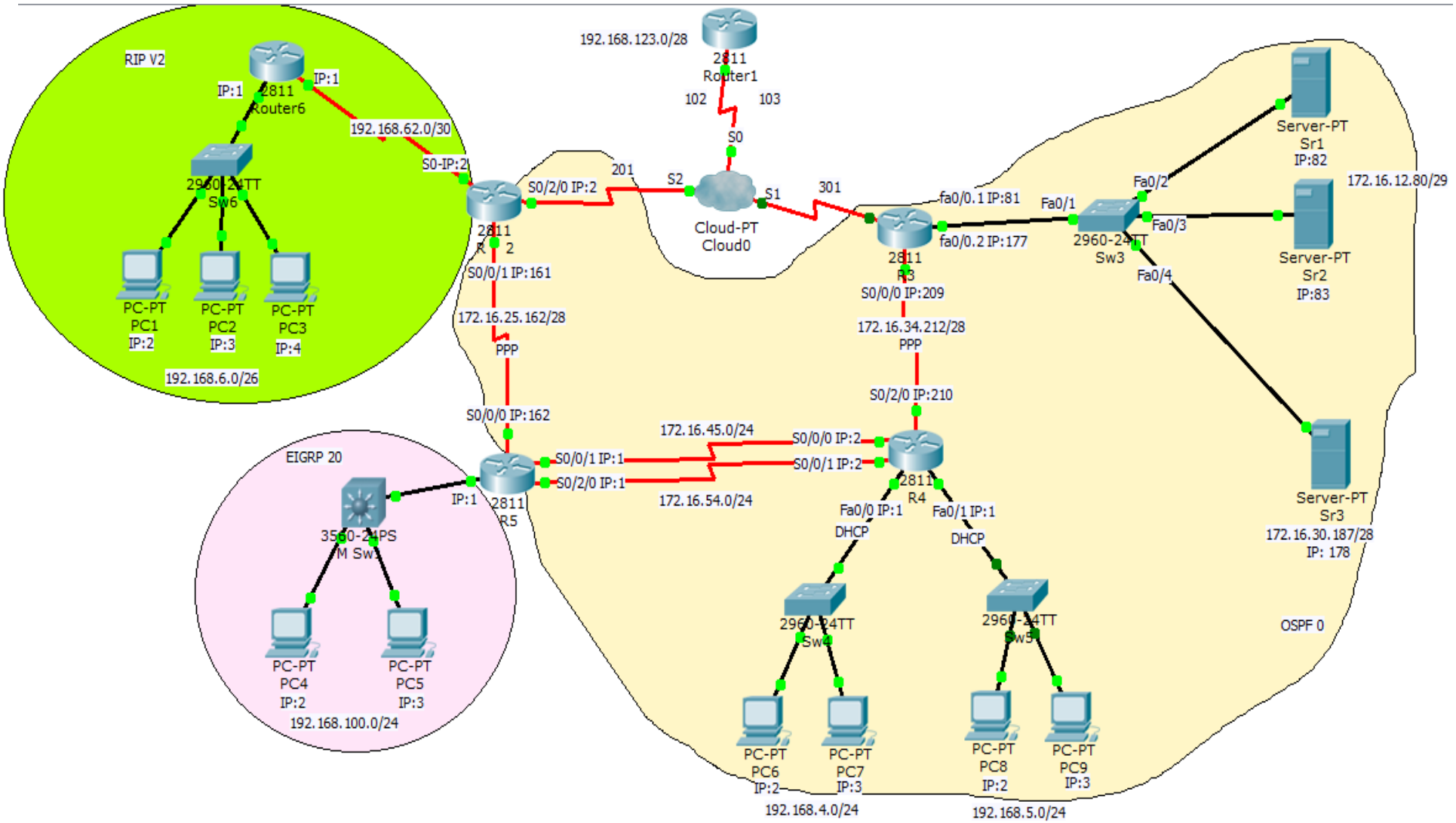
R3:

```
1  Router(config)#access-list 1 permit 192.168.1.0 0.0.0.255
2
3  Router(config)#interface Serial0/0/0
4  Router(config-if)#ip nat inside
5
6  Router(config)#interface Serial0/0/1
7  Router(config-if)#encapsulation frame-relay
8  Router(config-if)#frame-relay map ip 100.10.1.2 300 broadcast
9  Router(config-if)#ip nat outside
10
11 Router(config-if)# ip nat inside source list 1 interface Serial0/0/1 overload
```

R4:

```
1  R4(config)#access-list 1 permit 192.168.1.0 0.0.0.255
2
3  R4(config)#interface Serial0/0/0
4  R4(config-if)#ip nat inside
5
6  R4(config)#interface Serial0/2/0
7  R4(config-if)#encapsulation frame-relay
8  R4(config-if)#frame-relay map ip 200.20.2.2 500 broadcast
9  R4(config-if)#ip nat outside
10 R4(config-if)#ip nat inside source list 1 interface Serial0/2/0 overload
```

سناریو : Dynamic Rout.-Redi-ACL -PPP-Frame -DHCP -Subnetting



شکل 13-6 سناریو : Subnetting- DHCP- Frame-PPP- ACL-Redi-
Dynamic Rout

سوال 1: با استفاده از IP هاي داده شده در شكل(13-6) به اختصاص آدرس‌ها پرداخته و در روتر 4 سرويس DHCP براي سوئيچ‌هاي 4و 5 پياده‌سازي گردد.

سوال 2: از پروتكل PPP براي ارتباط روتر 3 با 4 و روتر 2 با 5 استفاده شده و از ارتباط روتر 3 با 4 با مكانيزم احراز هويت Chap پياده‌سازي گردد.

سوال 3: براي روترهاي R3,R2,R1 پروتكل‌هاي Frame relay به روش Hub&spoke پياده سازي شده و از DLCI هاي داده‌شده استفاده گردد.

سوال 4: پروتكل‌هاي مسيريابي مطابق شكل پياده‌سازي گردد و براي ارتباط روتر 3 و 4 از مكانيزم MD5 استفاده گردد.

سوال 5: دسترسي PC1 به سرور 1 از طريق Web و به سرور 2 از طريق پروتكل ICMP و نسبت به سرور 3 كلا مسدود باشد.

سوال 6: قابليت SSH نسبت به روتر 2براي PC2,5,6 كلا مسدود باشد.

جواب 1: با استفاده از IP هاي داده شده به اختصاص آدرس‌ها پرداخته و در روتر 4 سرويس DHCP براي سوئيچ‌هاي 4و 5 پياده‌سازي گردد.
ابتدا Subnetها را محاسبه مي‌كنيم.

Sw6:
192.168.6.0/26

S:

8	8	8	3
255.	255.	255.	192
11111111	11111111	11111111	11000000

Net-ID: 192.168.6.0
Net-Mask: 255.255.255.192

255-31=224

R1,R3:
192.168.123.0/28

S:

8	8	8	4
255.	255.	255.	240
11111111	11111111	11111111	11110000

Net-ID: 192.168.123.0
Net-Mask: 255.255.255.240

255-15=240

R1,R6:
192.168.62.0/30

S:

8	8	8	6
255.	255.	255.	224
11111111	11111111	11111111	11111100

Net-ID: 192.168.62.0
Net-Mask: 255.255.255.252

255-3=252

R2,R5:
172.16.25.162/28

S:

8	8	8	4
255.	255.	255.	240
11111111	11111111	11111111	11110000

Net-ID: 172.16.25.160
Net-Mask: 255.255.255.240

255-15=240

1. $2^4 = 16\ Subnets$
2. $2^4 - 2 = 14\ Host$
3. $256 - 240 = 16\ Step$
4. .

Step 16	16×0	16×1	16×2		16×10	16×11
Net_ID	0	16	32		160	176
First					161	
2th					162	
Last					174	
Broadcast					175	

R3,R4:

172.16.34.212/28

S:

8	8	8	4
255.	255.	255.	240
11111111	11111111	11111111	11110000

Net-ID: 172.16.25.208
Net-Mask: 255.255.255.240

255-15=240

1. $2^4 = 16\ Subnets$
2. $2^4 - 2 = 14\ Host$
3. $256 - 240 = 16\ Step$
4. .

Step 16	16×0	16×1	16×2		16×13	16×14
Net_ID	0	16	32		208	224
First					209	
…					212	
Last					222	
Broadcast					223	

Server 1, Server2:

172.16.12.80/29

S:

8	8	8	4
255.	255.	255.	248
11111111	11111111	11111111	11111000

Net-ID: 172.16.12.80
Net-Mask: 255.255.255.248

255-7=248

1. $2^5 = 32$ ***Subnets***
2. $2^3 - 2 = 6$ ***Host***
3. $256 - 248 = 8$ ***Step***
4. .

Step 16	8×0	8×1	8×2	…	8×10	8×11
Net_ID	0	8	18	…	80	88
First				…	81	
…				…		
Last				…	86	
Broadcast				…	87	

Server3

172.16.30.187/28

S:

8	8	8	4
255.	255.	255.	240
11111111	11111111	11111111	11110000

Net-ID: 172.16.30.176

Net-Mask: 255.255.255.240

255-15=240

1. $2^4 = 16$ ***Subnets***
2. $2^4 - 2 = 14$ ***Host***
3. $256 - 240 = 16$ ***Step***
4. .

Step 16	16×0	16×1	16×2		16×11	16×12
Net_ID	0	16	32		176	192
First					177	
…th					187	
Last					…	
Broadcast					191	

اختصاص IP به Interface ها :

R6

```
1  Router(config)#interface fastEthernet 0/0
2  Router(config-if)#ip add 192.168.6.1 255.255.255.192
```

```
3  Router(config-if)#no shutdown
4
5  Router(config)#interface serial 0/0/0
6  Router(config-if)#ip address 192.168.62.1 255.255.255.252
8  Router(config-if)#clock rate 64000
9  Router(config-if)#no shutdown
```

R2:

```
1  Router(config)#interface serial 0/0/0
2  Router(config-if)#ip address 192.168.62.2 255.255.255.252
3  Router(config-if)#no shutdown
4
5  Router(config-if)#inte ser 0/0/1
6  Router(config-if)#ip address 172.16.25.161 255.255.255.240
8  Router(config-if)#clock rate 64000
9  Router(config-if)#no shutdown
```

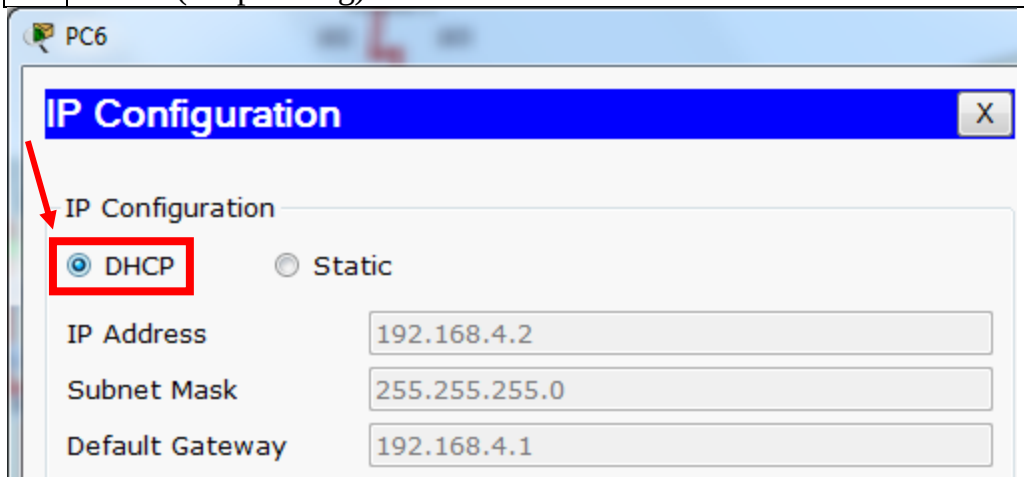
R5:

```
1  Router(config-if)#int fa 0/0
2  Router(config-if)#ip add 192.168.100.1 255.255.255.0
3  Router(config-if)#no shutdown
4
5  Router(config)#interface serial 0/0/0
6  Router(config-if)#ip address 172.16.25.162 255.255.255.240
8  Router(config-if)#no shutdown
9
10 Router(config-if)#in ser 0/0/1
11 Router(config-if)#ip add 172.16.45.1 255.255.255.0
12 Router(config-if)#clock rate 64000
13 Router(config-if)#no shutdown
14
15 Router(config-if)#int ser 0/2/0
16 Router(config-if)#ip add 172.16.54.1 255.255.255.0
17 Router(config-if)#clock rate 64000
18 Router(config-if)#no shutdown
```

R4

```
1  Router(config)#int s0/0/0
2  Router(config-if)#ip add 172.16.45.2 255.255.255.0
3  Router(config-if)#no shutdown
```

```
4
5   Router(config-if)#int ser 0/0/1
6   Router(config-if)#ip add 172.16.54.2 255.255.255.0
8   Router(config-if)#no shutdown
9
10  Router(config-if)#int s0/2/0
11  Router(config-if)#ip add 172.16.34.210 255.255.255.240
12  Router(config-if)#no shutdown
13
14  Router(config-if)#int f0/0
15  Router(config-if)#ip add 192.168.4.1 255.255.255.0
16  Router(config-if)#no shutdown
17
18  Router(config-if)#int f0/1
19  Router(config-if)#ip add 192.168.5.1 255.255.255.0
20  Router(config-if)#no shutdown
21
22  DHCP Sw4
23  Router(config)#ip dhcp pool Test1
24  Router(dhcp-config)#network 192.168.4.2 255.255.255.0
25  Router(dhcp-config)#default-router 192.168.4.1
26
27  DHCP Sw5
28  Router(config)#ip dhcp pool Test2
29  Router(dhcp-config)#network 192.168.5.2 255.255.255.0
30  Router(dhcp-config)#default-router 192.168.5.1
```



شکل 13-7 اختصاص IP با استفاده از

SW3:

```
1   Switch(config)#vlan 10
2   Switch(config-vlan)#vlan 20
3
```

```
4  Switch(config)#interface range fa 0/2-3
5  Switch(config-if-range)#switchport mode access
6  Switch(config-if-range)#switchport access vlan 10
8
9  Switch(config)#int f0/4
10 witch(config-if)#switchport mode access
11 Switch(config-if)#switchport access vlan 20
12
13 Switch(config-if)#int f0/1
14 Switch(config-if)#switchport mode trunk
15
```

R3:

```
1  Router(config)#int s0/0/0
2  Router(config-if)#ip add 172.16.34.209 255.255.255.240
3  Router(config-if)#clock rate 64000
4
5  Router(config-if)#interface fastEthernet 0/0.1
6  Router(config-subif)#encapsulation dot1Q 10
8  Router(config-subif)#ip add 172.16.12.81 255.255.255.248
9
10 Router(config)#interface fastEthernet 0/0.2
11 Router(config-subif)#encapsulation dot1Q 20
12 Router(config-subif)#ip add 172.16.30.177 255.255.255.240
13
14 Router(config)#int f0/0
15 Router(config-if)#no shutdown
```

جواب 2: از پروتکل PPP براي ارتباط روتر 3 با 4 و روتر 2 با 5 استفاده شده و از ارتباط روتر 3 با 4 با مکانیزم احراز هویتChap پیاده‌سازي گردد.

R3⇨R4: PPP Protocol & Chap Authentication

R3:

```
1  Router(config)#hostname r3
2  r3(config)#username r4 password 123
3
4  r3(config)#int s0/0/0
5  r3(config-if)#encapsulation ppp
6  r3(config-if)#ppp authentication chap
```

7	r3(config-if)#**no shutdown**

R4:

1	Router(config)#**hostname r4**
2	r4(config)#**username r3 password 123**
3	
4	r4(config)#**int s0/2/0**
5	r4(config-if)#**encapsulation ppp**
6	r4(config-if)#**ppp authentication chap**
7	r4(config-if)#**no shutdown**

R2⇨R5: PPP Protocol

R2:

1	Router(config)#**hostname r2**
2	r2(config)#**username r5 password 123**
3	
4	r2(config)#**int s0/0/0**
5	r2(config-if)#**encapsulation ppp**
6	r2(config-if)#**no shutdown**

R5:

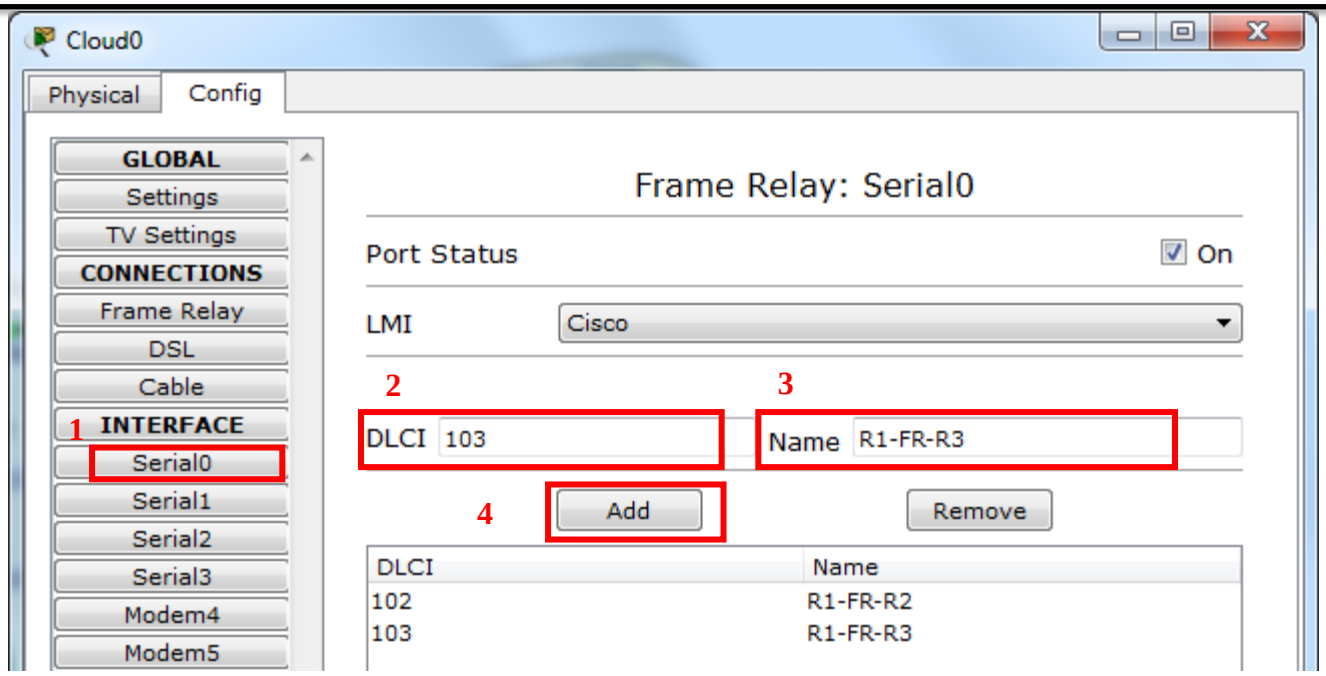
1	Router(config)#**hostname r5**
2	r5(config)#**username r2 password 123**
3	
4	r5(config)#**int s0/0/0**
5	r5(config-if)#**encapsulation ppp**
6	r5(config-if)#**no shutdown**

جواب 3: براي روترهاي R3,R2,R1 پروتكل‌هاي Frame relay به روش Hub&spoke پياده‌سازي شده و از DLCI هاي داده‌شده استفاده گردد.

ب 1- بر روي ابر كليک كرده و DLCI را از قسمت Config و Interface تعريف مي‌كنيم.

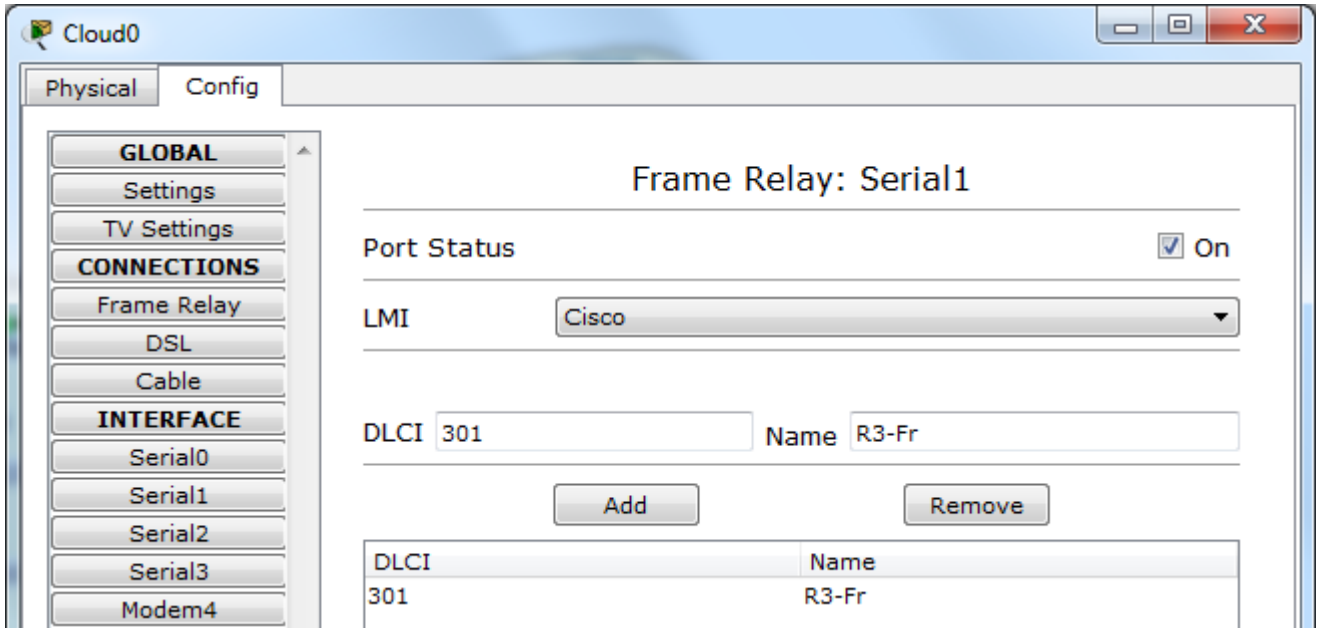
a. Serial 0 را كليک مي‌كنيم.

b. DLCI هائيكه به پورت سريال ابر متصل هستند را وارد مي‌كنيم و براي آن‌ها نام انتخاب كرده و سپس در هر مرحله كليد ADD را مي‌زنيم.



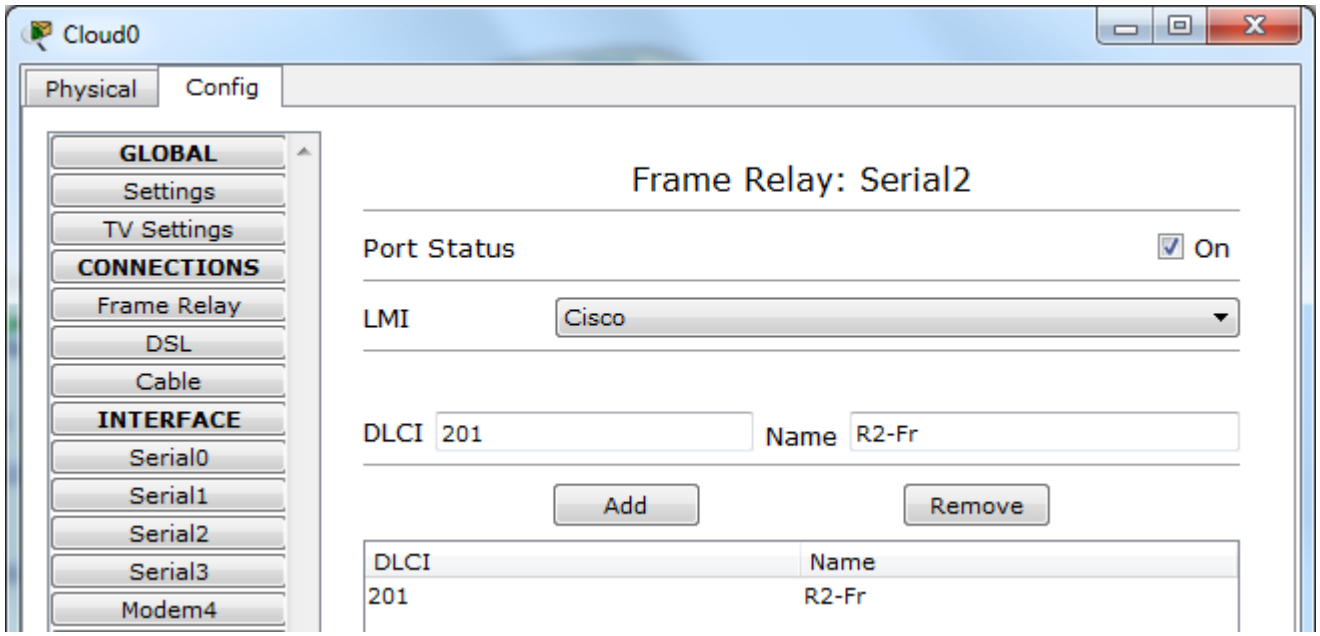
شکل 13-8 تنظیمات DLCI برای اینترفیس Serial0

c. پورت Serial 1 را کلیک کرده و مانند بالا DLCI مرتبط به این پورت را Add میکنیم.



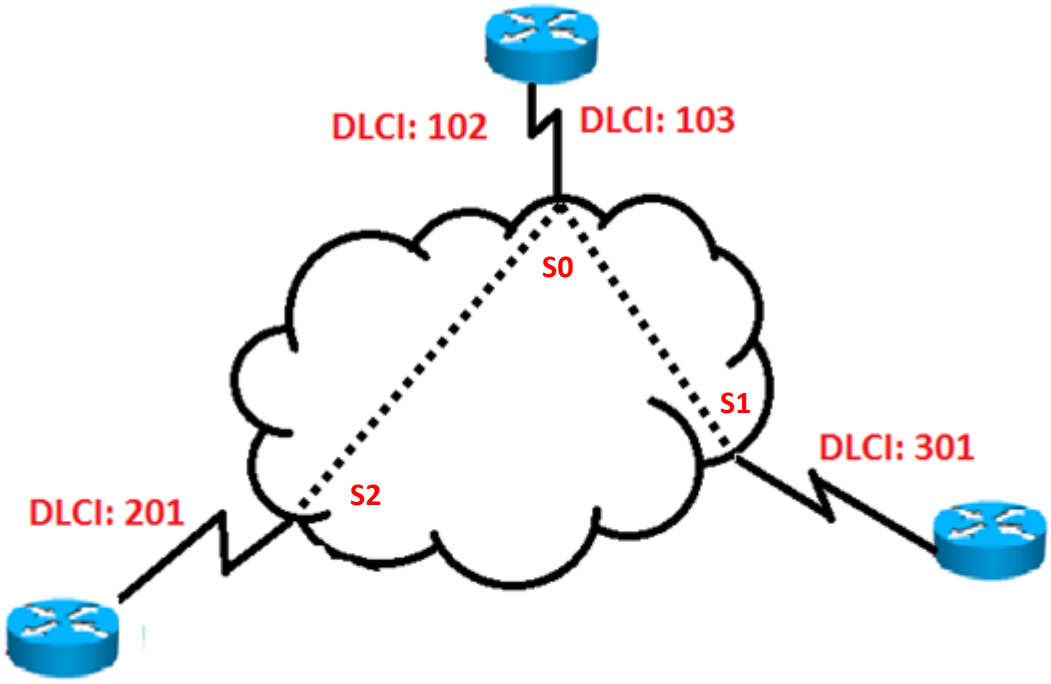
شکل 13-9 تنظیمات DLCI برای

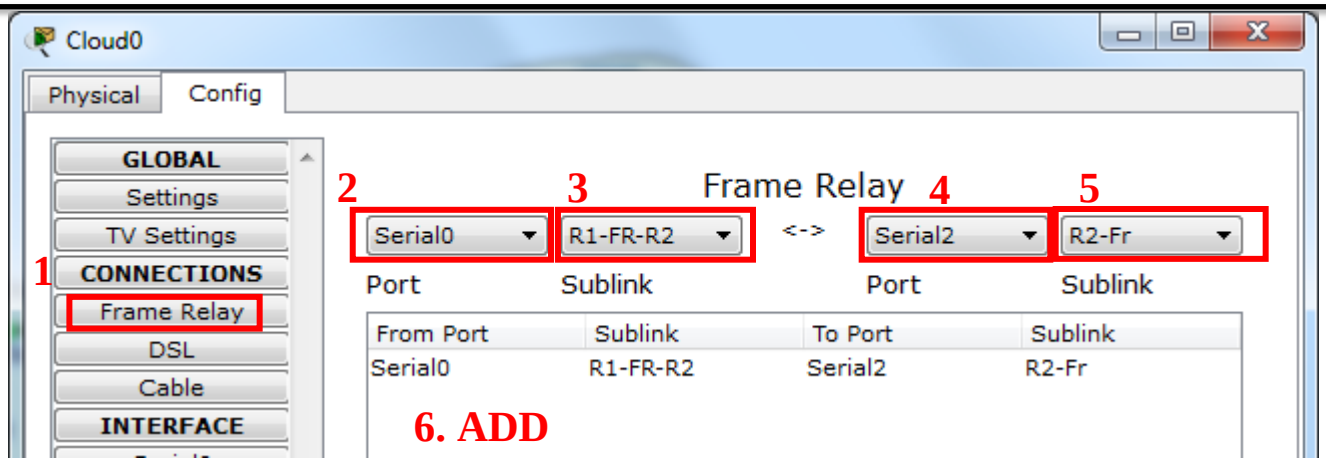
d. و پورت سریال Se2



شکل 13-10 تنظیمات DLCI برای

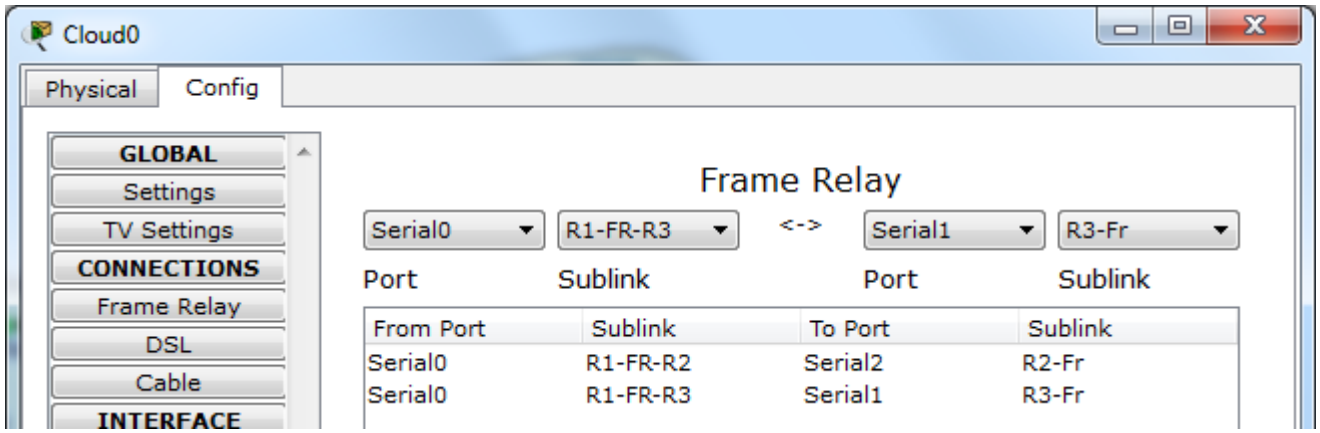
ب 2- مجددا بر روي ابر كليک كرده و Frame Relaye ها را دقيقا مطابق به شكل زير تعريف مي‌كنيم.





شکل 13-11 تنظیمات Frame-relay بین S0 و S2

در سمت اول از پورت سریال Se0 ابر با نام R1-FR-R2 و در سمت دیگر ابر از طریق پورت سریال Se2 با نام R2-Fr به روتر R2 متصل میشویم.



شکل 13-12 تنظیمات Frame-relay بین S0 و S1

در سمت اول از پورت سریال Se0 ابر با نام R1-FR-R3 و در سمت دیگر ابر از طریق پورت سریال Se1 با نام R3-Fr به روتر R3 متصل میشویم.

ب3- حال باید روترها را کانفیگ کنیم و به پورتهاي روتر IP بدهیم.

R1:

```
1  Router(config)#int s0/0/0
2  Router(config-if)#encapsulation frame-relay
3  Router(config-if)#ip address 192.168.123.1 255.255.255.240
4
5  Router(config-if)#frame-relay map ip 192.168.123.3 103 broadcast
6  Router(config-if)#frame-relay map ip 192.168.123.2 102 broadcast
7  Router(config-if)#no shutdown
```

R3:

```
1  r3(config)#int s0/0/1
2  r3(config-if)#encapsulation frame-relay
3  r3(config-if)#ip address 192.168.123.3 255.255.255.240
4
5  r3(config-if)#frame-relay map ip 192.168.123.1 301 broadcast
6  r3(config-if)#frame-relay map ip 192.168.123.2 301 broadcast
7
8  r3(config-if)#no shutdown
```

R2:

```
1  r2(config)#int s0/2/0
2  r2(config-if)#encapsulation frame-relay
3  r2(config-if)#ip address 192.168.123.2 255.255.255.240
4
5  r2(config-if)#frame-relay map ip 192.168.123.2 201 broadcast
6  r3(config-if)#frame-relay map ip 192.168.123.3 201 broadcast

   r2(config-if)#no shutdown
```

ج 4: پروتکل‌هاي مسيريابي مطابق شکل پياده‌سازي گردد و براي ارتباط روتر 3 و 4 از مکانيزم MD5 استفاده گردد.

راه اندازي Dynamic Routing:

R6:

```
1  Router(config)#router rip
2  Router(config-router)#ver 2
3  Router(config-router)#network 192.168.6.0
4  Router(config-router)#network 192.168.62.0
```

R2:

```
1  Router(config)#router rip
2  Router(config-router)#version 2
3  Router(config-router)#network 192.168.62.0
4
5  Router(config)#router ospf 1
6  Router(config-router)#network 172.16.25.161 0.0.0.0 area 0
7  Router(config-router)#network 192.168.123.2 0.0.0.0 area 0
8  Router(config-router)#redistribute rip metric 1 subnets
9
10 Router(config)#router rip
11 Router(config-router)#version 2
12 Router(config-router)#redistribute ospf 1 metric 1
```

R5:

```
1  Router(config)#router eigrp 20
2  Router(config-router)#network 192.168.100.0
3
4  Router(config)#router ospf 1
5  Router(config-router)#network 172.16.25.162 0.0.0.0 area 0
6  Router(config-router)#network 172.16.45.1 0.0.0.0 area 0
7  Router(config-router)#network 172.16.54.1 0.0.0.0 area 0
8  Router(config-router)#redistribute eigrp 20 metric 1 subnets
9
10 Router(config)#router eigrp 20
11 Router(config-router)#redistribute ospf 1 metric 1 1 1 1 1
```

R4:

```
1  Router(config)#router ospf 1
2  Router(config-router)#network 172.16.45.2 0.0.0.0 area 0
3  Router(config-router)#network 172.16.54.2 0.0.0.0 area 0
4  Router(config-router)#network 192.168.4.1 0.0.0.0 area 0
5  Router(config-router)#network 192.168.5.1 0.0.0.0 area 0
6  Router(config-router)#network 172.16.34.210 0.0.0.0 area 0
```

R3:

```
1  Router(config)#router ospf 1
2  Router(config-router)#network 172.16.12.81 0.0.0.0 area 0
3  Router(config-router)#network 172.16.30.177 0.0.0.0 area 0
4  Router(config-router)#network 192.168.123.3 0.0.0.0 area 0
5  Router(config-router)#network 172.16.34.209 0.0.0.0 area 0
```

:Md5 Authentication

R3:

```
1  r3(config)#int s0/0/0
2  r3(config-if)#ip ospf authentication-key ccna
3  r3(config-if)#ip ospf authentication message-digest
```

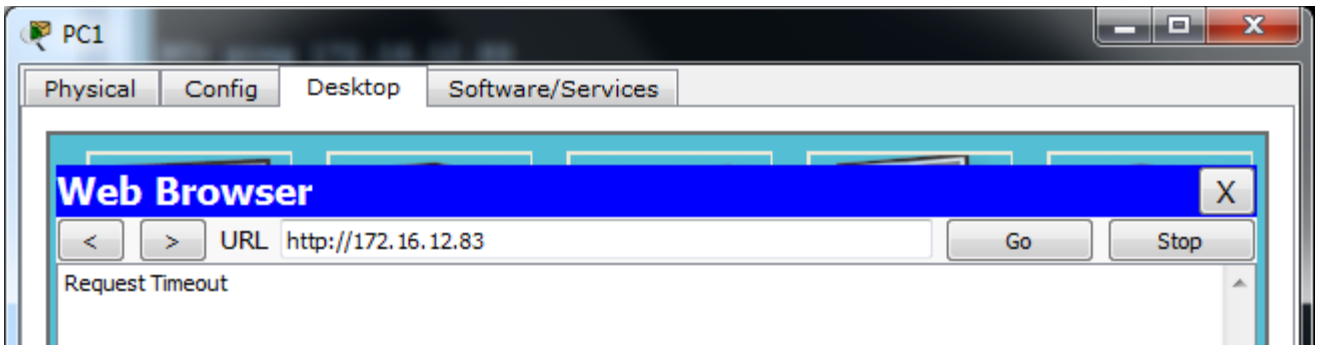
R4:

```
1  r4(config)#int s0/2/0
2  r4(config-if)#ip ospf authentication-key ccna
3  r4(config-if)#ip ospf authentication message-digest
```

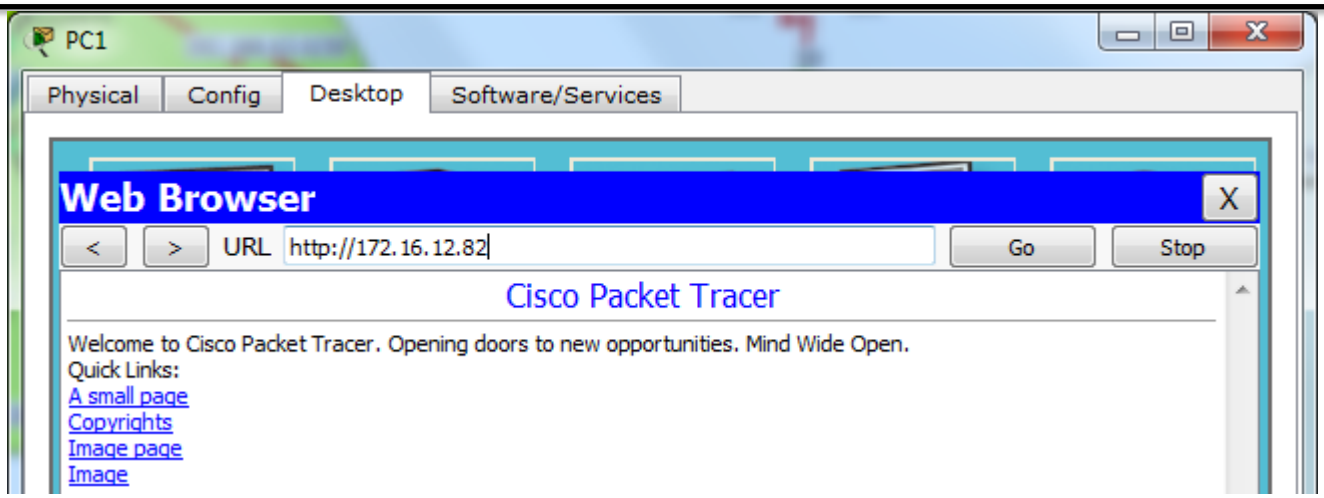
ج **5-** دسترسی PC1 به سرور 1 از طریق Web و به سرور 2 از طریق پروتکل ICMP مقدور بوده و نسبت به سرور 3 کلا مسدود باشد. (بخش 1- خط 1و2) (بخش 2- خط 4و5) (بخش 3- خط 7)

R6:

```
1  Router(config)#access-list 180 permit tcp host 192.168.6.2 host 172.16.12.82 eq 80
2  Router(config)#access-list 180 deny ip host 192.168.6.2 host 172.16.12.82
3
4  Router(config)#access-list 180 permit icmp host 192.168.6.2 host 172.16.12.83
5  Router(config)#access-list 180 deny ip host 192.168.6.2 host 172.16.12.83
6
7  Router(config)#access-list 180 deny ip host 192.168.6.2 host 172.16.30.178
8
9  Router(config)#access-list 180 permit ip any any
10
11 Router(config-if)#inter fa 0/0
12 Router(config-if)#ip access-group 180 in
```



شکل 13-13 عدم دسترسی از PC1 به Server2 از طریق Web



شکل 13-14 دسترسی از PC1 به Server1 از

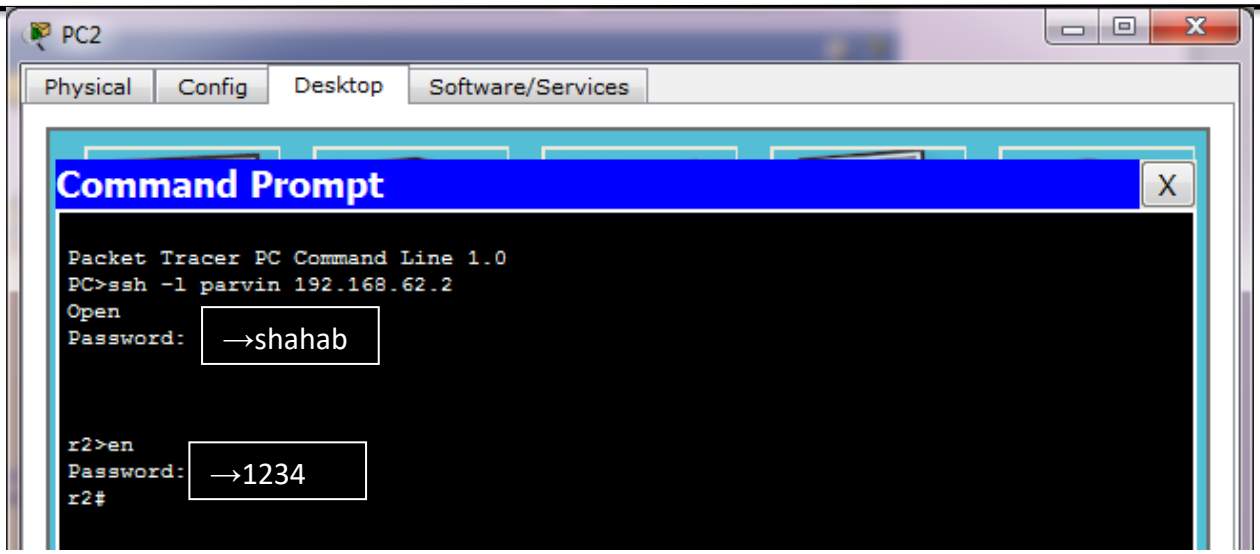
و . . .

جواب 6: قابلیت SSH نسبت به روتر 2 براي PC2,5,6 کلا مسدود باشد.

ب1. ابتدا SSH را بر روی روتر فعال می کنیم:

```
1  r2(config)#ip domain-name cisco.com
2  r2(config)#crypto key generate rsa
3  The name for the keys will be: r2.cisco.com
4  Choose the size of the key modulus in the range of 360 to 2048 for your   General Purpose
5  Keys. Choosing a key modulus greater than 512 may take  a few minutes.
6  How many bits in the modulus [512]: 1024
7  % Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
8
9  r2(config)#ip ssh version 2
10 r2(config)#username parvin password shahab
11 r2(config)#enable secret 1234
12 r2(config)#line vty 0 4
13 r2(config-line)#login local
14
15 r2(config-line)#transport in
   r2(config-line)#transport input ssh
```

PC2>ssh –L parvin 192.168.62.2



شکل 13-15 قابلیت SSH نسبت به روتر2 برای PC2

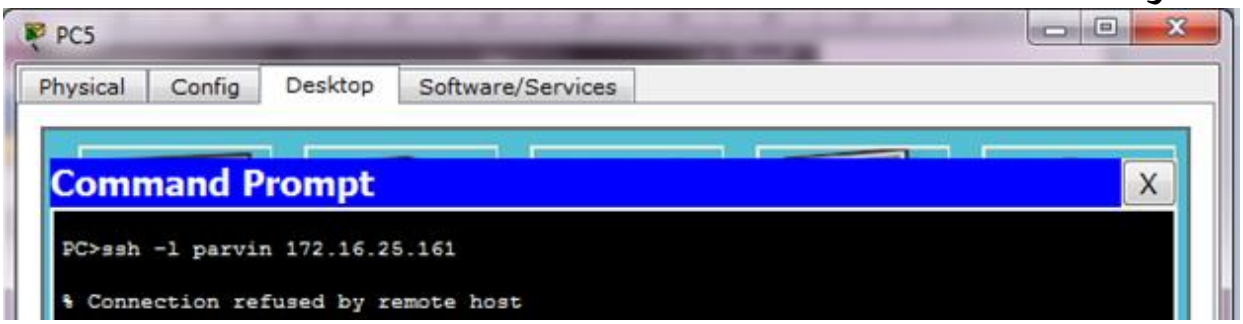
ب2. حال ACL مورد نظر را جهت بستن دسترسی PC ها از نوع استاندارد می‌نویسیم که آن‌را باید در مقصد (یعنی روتر R2 اعمال نماییم):

IP PC2:192.168.6.3
IP PC5:192.168.100.3
IP PC6:192.168.4.2

R2:

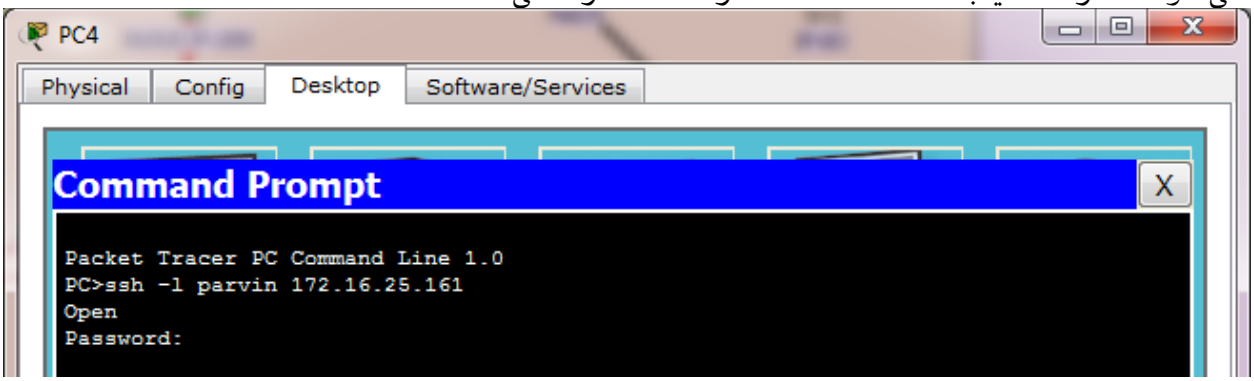
```
1  r2(config)#access-list 20 deny host 192.168.6.3
2  r2(config)#access-list 20 deny host 192.168.100.3
3  r2(config)#access-list 20 deny host 192.168.4.2
4  r2(config)#access-list 20 permit any
5
6  r2(config)#line vty 0 4
7  r2(config-line)#access-class 20 in
```

ب3. تست از PC5:



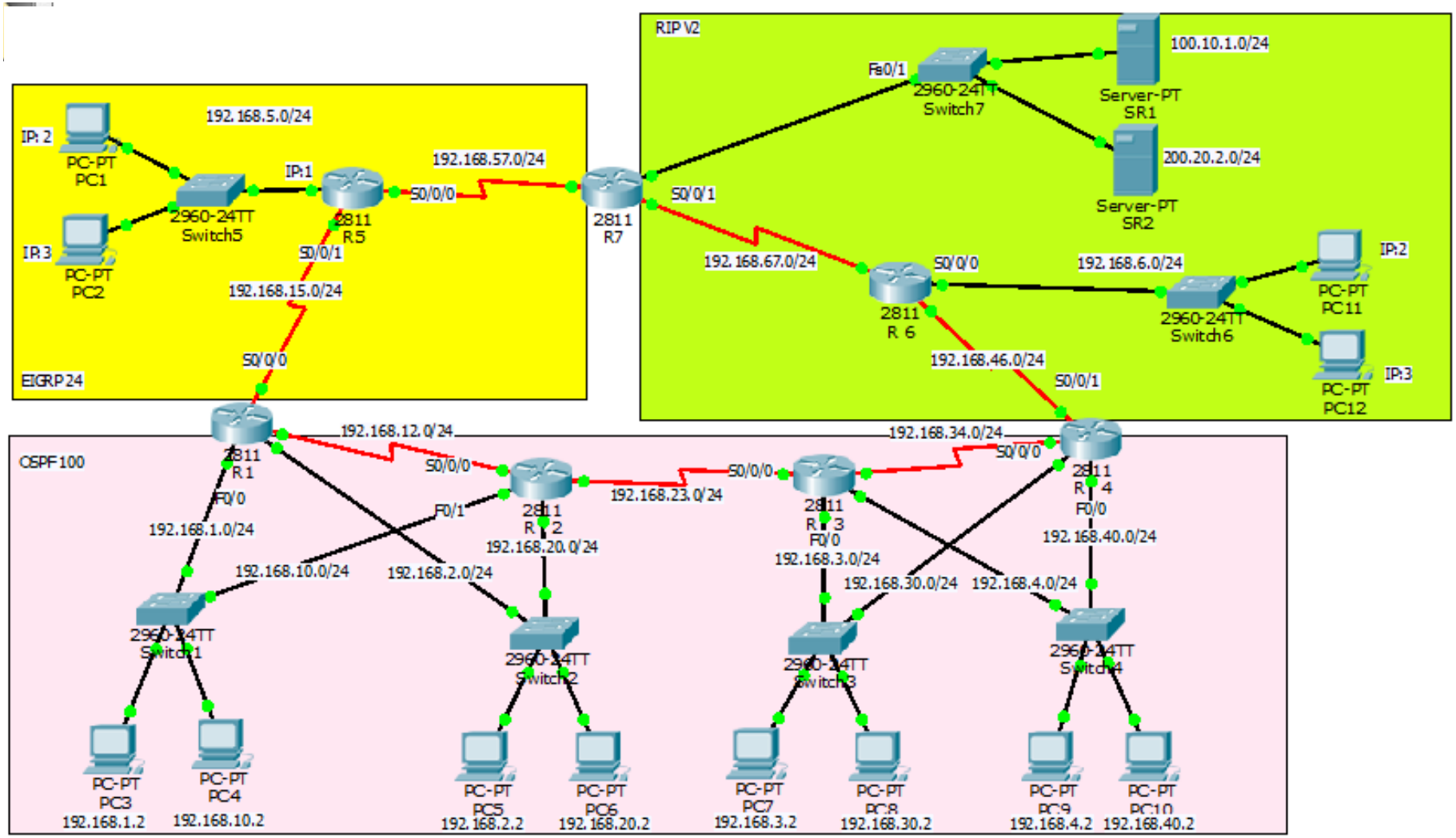
شکل 13-16 عدم قابلیت SSH نسبت به روتر 2 برای PC5

در حالیکه از PC4 بخواهیم از طریق SSh به روتر R2 وصل شویم، امکان پذیر می‌شود در نتیجه ACL ما درست کار می‌کند.



شکل 13-17 قابلیت SSH نسبت به روتر2 برای PC4

سناریو : SSH-Telnet-ACL – V.Interface و . . .



شکل 13-18 سناریو ACL، Telnet، SSH، V.interface

سوال 1: با استفاده از IP های داده شده در شکل(13-18)، ارتباط اولیه شبکه را راه اندازی نموده و پروتکل‌های مسیریابی را مطابق با شکل پیاده‌سازی نمایید.
سوال 2: دسترسی PC1 نسبت به Server 1,2 فقط از طریق Web مقدور باشد.
سوال 3: دسترسی PC1 نسبت به PC11 فقط از طریق پروتکل ICMP مسدود باشد.
سوال 4: دسترسی کاربران SW6/SW3 / SW1 از طریق SSH نسبت به Router 7 مسدود باشد.
سوال 5: قابلیت Telnet نسبت به روتر R1رو فقط برای PC12 مقدور باشد.

جواب 1- اختصاص IP: با استفاده از IP های داده شده ، ارتباط اولیه شبکه را راه اندازی نموده و پروتکل‌های مسیریابی را مطابق با شکل پیاده‌سازی نمایید.

R1:

```
1  R1(config)#int s0/0/0
2  R1 (config-if)#ip address 192.168.15.2 255.255.255.0
3  R1 (config-if)#no shutdown
4
5  R1 (config-if)#int s0/0/1
6  R1 (config-if)#ip  address 192.168.12.1 255.255.255.0
7  R1 (config-if)#clock rat 64000
8  R1 (config-if)#no shutdown
9
10 R1(config)#int f0/0
11 R1 (config-if)#ip address 192.168.1.1 255.255.255.0
12 R1(config-if)#no shutdown
13
14 R1(config)#int f0/1
15 R1 (config-if)#ip address 192.168.2.1 255.255.255.0
16 R1(config-if)#no shutdown
```

R2:

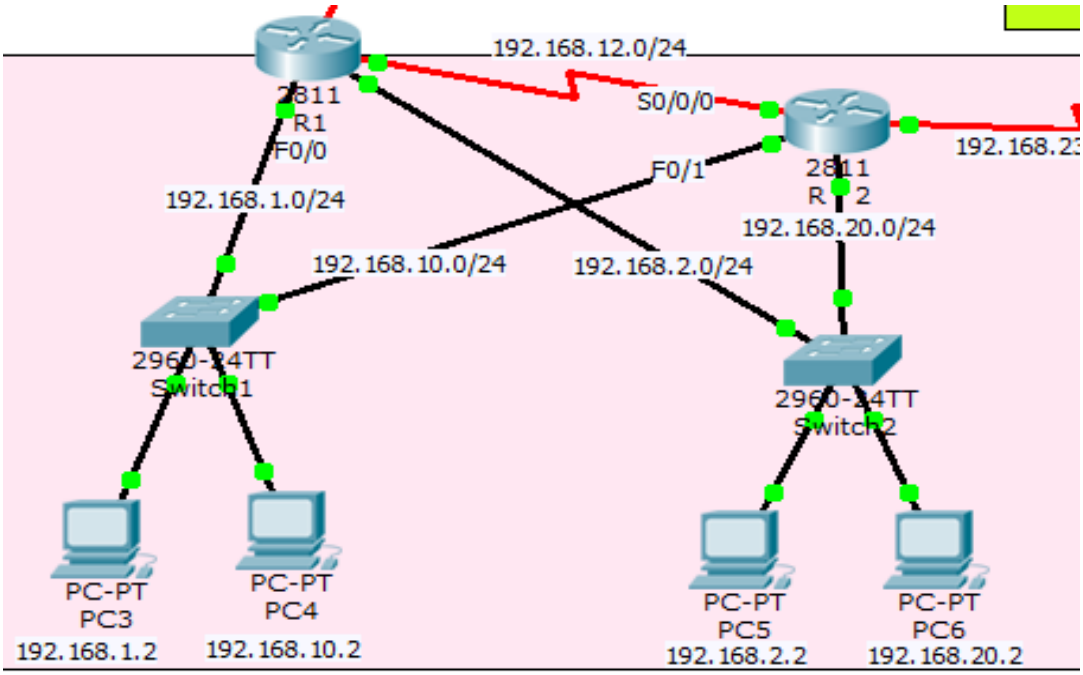
```
1  Router(config)#int s0/0/0
2  Router(config-if)#ip address 192.168.12.2 255.255.255.0
3  Router(config-if)#no shutdown
4
5  Router(config-if)#int s0/0/1
6  Router(config-if)#ip address 192.168.23.1 255.255.255.0
7  Router(config-if)#clock rat 64000
8  Router(config-if)#no shutdown
9
10 R2(config)#int f0/0
11 R2(config-if)#ip address 192.168.20.1 255.255.255.0
```

```
12  R2(config-if)#no shutdown
13
14  R2(config-if)#int f0/1
15  R2(config-if)#ip address 192.168.10.1 255.255.255.0
16  R2(config-if)#no shutdown
```

این قسمت که به‌صورت ضدربدری IP داده شده است نیز به هر کدام از Interface های روتر مطابق شکل IP اختصاص می‌دهیم و به هر کدام از PC ها نیز مطابق با آنچه خواسته شده است می‌توان IP اختصاص داد.

PC3: IP: 192.168.1.2 Gateway: 192.168.1.1
PC4: IP: 192.168.10.2 Gateway: 192.168.10.1

PC5: IP:192.168.2.2 Gateway:192.168.2.1
PC6: IP:192.168.20.2 Gateway:192.168.20.1



R3:

```
1   R3(config)#int s0/0/0
2   R3(config-if)#ip address 192.168.23.2 255.255.255.0
3   R3(config-if)#no shutdown
4
5   R3(config-if)#int s0/0/1
6   R3(config-if)#ip address 192.168.34.1 255.255.255.0
7   R3(config-if)#no shutdown
8
9   R3(config)#int f0/0
10  R3(config-if)#ip address 192.168.3.1 255.255.255.0
```

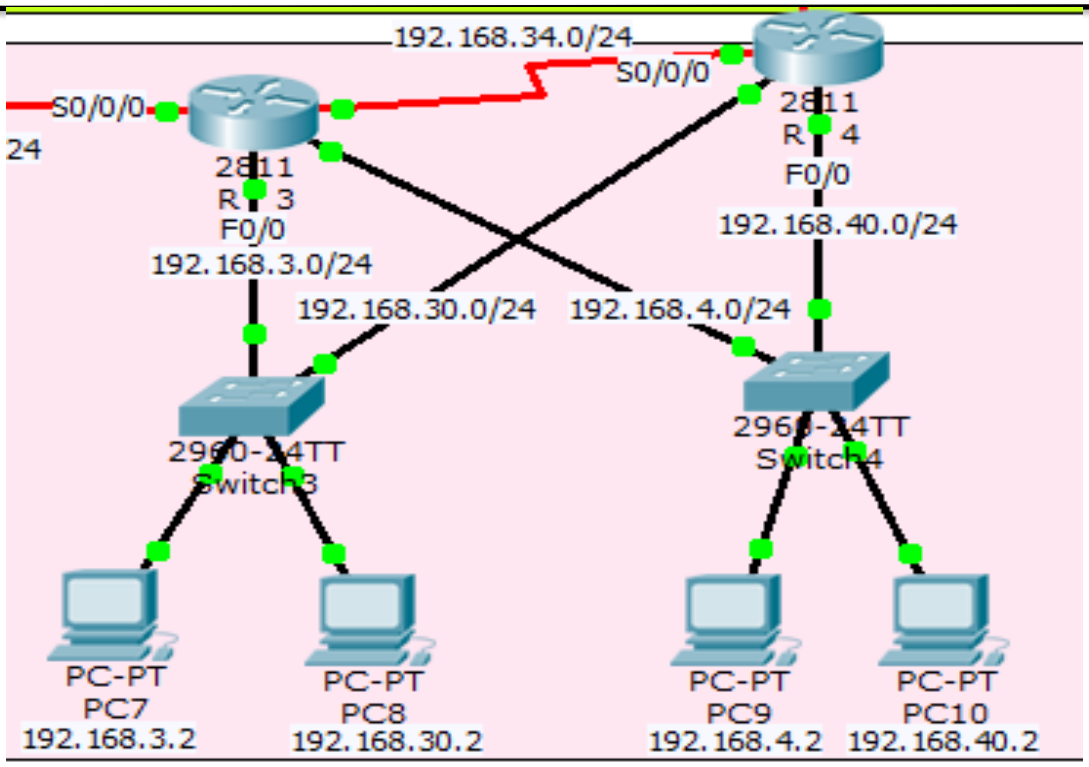
```
11  R3(config-if)#no shutdown
12
13  R3(config-if)#int f0/1
14  R3(config-if)#ip address 192.168.4.1 255.255.255.0
15  R3(config-if)#no shutdown
```

R4

```
1   Router(config)#int s0/0/1
2   Router(config-if)#ip address 192.168.46.2 255.255.255.0
3   Router(config-if)#no shutdown
4
5   Router(config-if)#int s0/0/0
6   Router(config-if)#ip address 192.168.43.2 255.255.255.0
7   Router(config-if)#no shutdown
8
9   R4(config)#int f0/0
10  R4(config-if)#ip address 192.168.40.1 255.255.255.0
11  R4(config-if)#no shutdown
12
13  R4(config-if)#int f0/1
14  R4(config-if)#ip address 192.168.30.1 255.255.255.0
15  R4(config-if)#no shutdown
```

PC7: IP: 192.168.3.2 Gateway: 192.168.3.1
PC8: IP: 192.168.30.2 Gateway: 192.168.30.1

PC9: IP: 192.168.4.2 Gateway: 192.168.4.1
PC10: IP: 192.168.40.2 Gateway: 192.168.40.1



اعمال پروتکل مسیریابی و **redistribute**

R5:

```
1  R5(config)#router eigrp 24
2  R5(config-router)#network 192.168.5.0
3  R5(config-router)#network 192.168.15.0
4  R5(config-router)#network 192.168.57.0
```

R7:

```
1  R7(config)#router eigrp 24
2  R7 (config-router)#network 192.168.57.0
3
4  R7 (config)#router rip
5  R7 (config-router)#version 2
6  R7 (config-router)#network 192.168.67.0
7  R7 (config-router)#network 100.10.1.0
8  R7 (config-router)#network 200.20.2.0
9  R7(config-router)#redistribute eigrp 24 metric 1
10
11 R7 (config)#router eigrp 24
12 R7(config-router)#redistribute rip metric 1 1 1 1 1
```

R6:

```
1  R6(config)#router rip
2  R6(config-router)#version 2
3  R6(config-router)#network 192.168.6.0
4  R6(config-router)#network 192.168.46.0
5  R6(config-router)#network 192.168.67.0
```

R2:

```
1  R2(config)#router ospf 1
2  R2(config-router)#network 192.168.23.0 0.0.0.255 area 100
3  R2(config-router)#network 192.168.12.0 0.0.0.255 area 100
4  R2(config-router)#network 192.168.10.0 0.0.0.255 area 100
5  R2(config-router)#network 192.168.20.0 0.0.0.255 area 100
```

R3:

```
1  R3(config)#router ospf 1
2  R3(config-router)#network 192.168.23.0 0.0.0.255 area 100
3  R3(config-router)#network 192.168.34.0 0.0.0.255 area 100
4  R3(config-router)#network 192.168.3.0 0.0.0.255 area 100
5  R3(config-router)#network 192.168.4.0 0.0.0.255 area 100
```

R1:

```
1  R1(config)#router eigrp 24
2  R1(config-router)#network 192.168.15.0
3
4  R1(config-router)#router ospf 1
5  R1(config-router)#network 192.168.1.0 0.0.0.255 area 100
6  R1(config-router)#network 192.168.12.0 0.0.0.255 area 100
7  R1(config-router)#network 192.168.2.0 0.0.0.255 area 100
8  R1(config-router)#redistribute eigrp 24 metric 1 subnets
9
10 R1(config)#router eigrp 24
11 R1(config-router)#redistribute ospf 1 metric 1 1 1 1 1
```

R4:

```
1  R4(config)#router rip
2  R4(config-router)#version 2
3  R4(config-router)#network 192.168.46.0
4
5  R4(config)#router ospf 1
6  R4(config-router)#network 192.168.34.0 0.0.0.255 area 100
7  R4(config-router)#network 192.168.40.0 0.0.0.255 area 100
8  R4(config-router)#network 192.168.30.0 0.0.0.255 area 100
9  R4(config-router)#redistribute rip metric 1 subnets
```

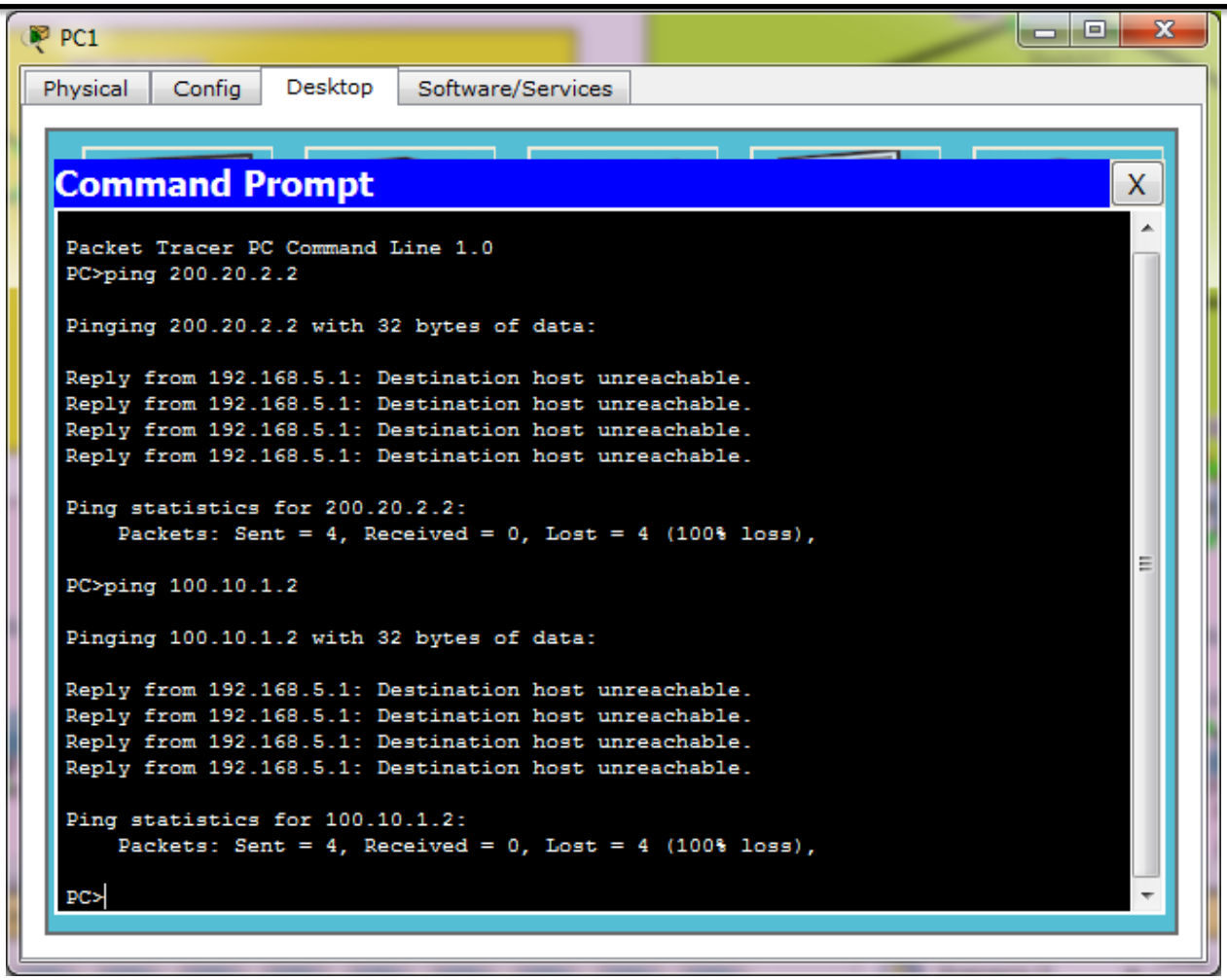
```
10
11  R4(config)#router rip
12  R4(config-router)#version 2
13  R4(config-router)#redistribute ospf 1 metric 1
```

جواب 2: دسترسی PC1 نسبت به Server 1,2 فقط از طریق Web مقدور باشد.

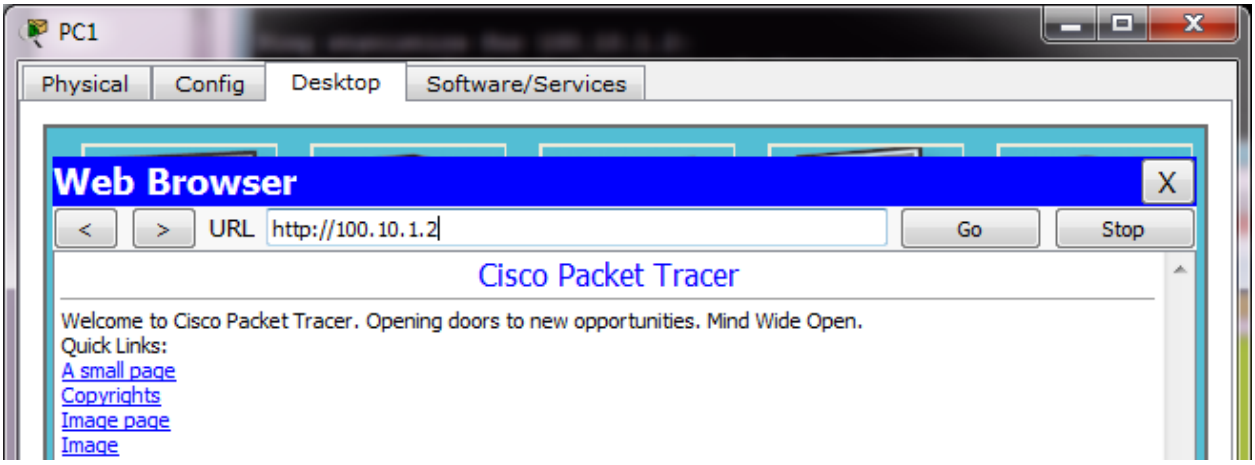
Source	Access Type	Destination	In
PC 1	**Web**	**Server 1,2**	**Near Source**
192.168.5.2	**Permit TCP … Eq80**	**100.10.1.2**	**R5-Inbound Fa0/0**
192.168.5.2	**Permit TCP … Eq80**	**200.20.2.2**	**R5-Inbound Fa0/0**

R5:

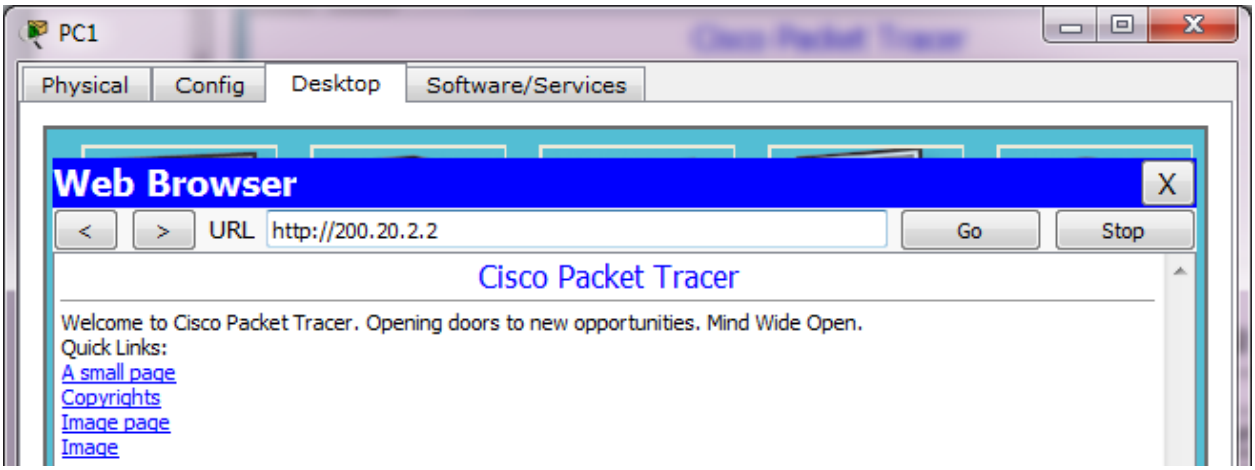
```
1   R5(config)#access-list 120 permit tcp host 192.168.5.2 host 100.10.1.2 eq 80
2   R5(config)#access-list 120 deny ip host 192.168.5.2 host 100.10.1.2
3
4   R5(config)#access-list 120 permit tcp host 192.168.5.2 host 200.20.2.2 eq 80
5   R5(config)#access-list 120 deny ip host 192.168.5.2 host 200.20.2.2
6
7   R5(config)#access-list 120 permit ip any any
8
9   R5(Config)#int f0/0
10  R5(Config-if)#ip access-group 120 in
```



شکل 13-19 عدم Ping از PC1 به Server1 و Server2



شکل 13-20 دسترسی به Server1 از PC1 از طریق Web



شکل 13-21 دسترسی به Server2 از PC1 از طریق Web

جواب 3: دسترسی PC 1 نسبت به PC11 فقط از طریق پروتکل ICMP مسدود باشد.

نکته بسیار مهم: در این قسمت مبدا با سوال قبل دقیقا یکسان است اما مقصدها یکسان نیست و باید در اینجا نیز ACL Extended بنویسیم و قاعدتا در روتر مبدا (R5) و در ورودی Fa0/0 باید اعمال کنیم. اما اگر این کار را بکنیم ACL جدید روی ACL ای که برای سوال قبل نوشتیم Over write می شود و ← اشتباه است و باید راه حل دیگری بیابیم.

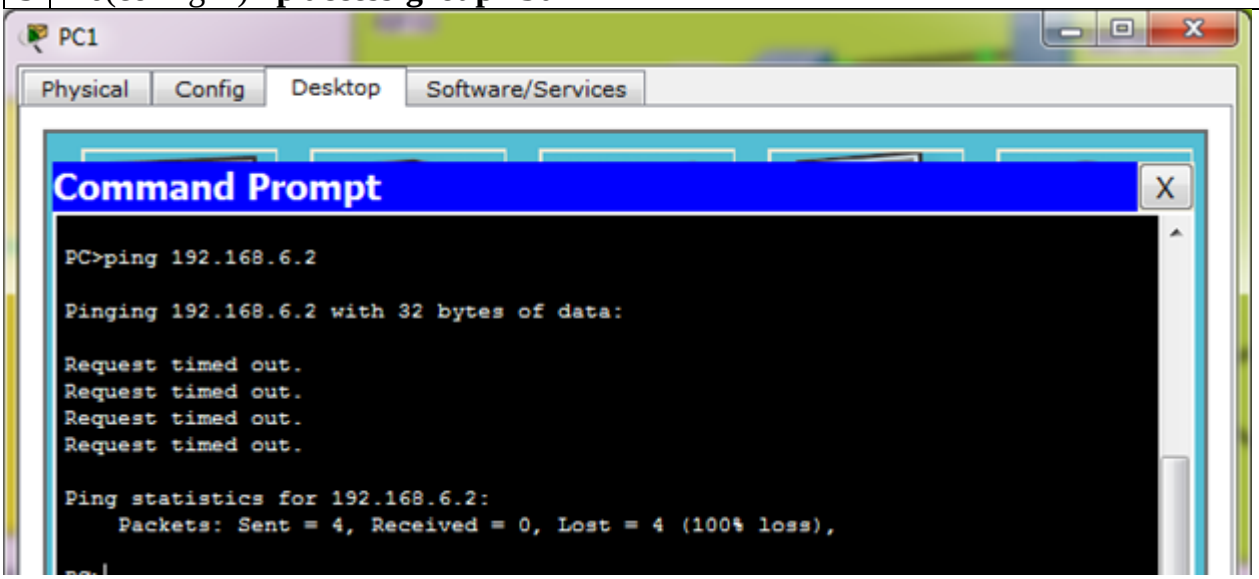
Source	Access Type	Destination	In
PC 1	Deny ICMP	PC11	Near Source
192.168.5.3	Deny ICMP	192.168.6.2	~~R5-Inbound Fa0/0~~

برای اینکه این مشکل حل گردد جای مبدا و مقصد را عوض می‌کنیم که مشکل حل می‌شود و ACL را بر روی روتر R6 و ورودی اینترفیس Fa0/0 اعمال می‌کنیم.

Source	Access Type	Destination	In
PC11	Deny ICMP	PC 1	Near Source

192.168.6.2	Deny ICMP	192.168.5.2	R6-Inbound Fa0/0

```
1  R6(config)#access-list 150 deny icmp host 192.168.6.2 host 192.168.5.2
2  R6(config)#access-list 150 permit ip any any
3
4  R6(config)#interface fa 0/0
5  R6(config-if)#ip access-group 150 in
```



شکل 13-22 عدم Ping از PC1 نسبت به PC11

جواب 4: دسترسی کاربران SW6/SW3 / SW1 از طریق SSH نسبت به Router 7 مسدود باشد.
ابتدا باید SSH را باید در روتر R7 فعال کنیم. (مثل تمرین‌های قبل)

R7:

```
1  R7(config)#ip domain-name cisco.com
2  R7(config)#crypto key generate rsa
3  The name for the keys will be: R7.cisco.com
4  Choose the size of the key modulus in the range of 360 to 2048 for your
5    General Purpose Keys. Choosing a key modulus greater than 512 may take
6    a few minutes.
7
8  How many bits in the modulus [512]: 1024
9  % Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
10
11 R7(config)#ip ssh version 2
12 R7(config)#username parvin password shahab
13 R7(config)#enable secret 123456
```

```
14  R7(config)#line vty 0 4
15  R7(config-line)#login local
16  R7(config-line)#transport input ssh
```

در اینجا سوئیچ Sw1 و Sw3 دو IP دارد.

IP SW1: 192.168.1.0, 192.168.10.0
IP SW3: 192.168.3.0, 192.168.30.0
IP Sw6: 192.168.6.0

R7:

```
1   R7(config)#access-list 10 deny 192.168.1.0 0.0.0.255
2   R7(config)#access-list 10 deny 192.168.10.0 0.0.0.255
3
4   R7(config)#access-list 10 deny 192.168.3.0 0.0.0.255
5   R7(config)#access-list 10 deny 192.168.30.0 0.0.0.255
6
7   R7(config)#access-list 10 deny 192.168.6.0 0.0.0.255
8
9   R7(config)#access-list 10 permit any any
10
11  R7(config)#line vty 0 4
12  R7(config-line)#access-class 10 in
```

و یا اگر فقط بخواهیم یک کامپیوتر را از کاربر یک سوئیچ ببندیم:
مثلا یکی از IP های سوئیچ SW1 را ببندیم:

```
1   R7(config)#access-list 10 deny host 192.168.1.2
```

جواب 5: قابلیت Telnet نسبت به روتر R1 فقط برای PC12 مقدور باشد.
ابتدا Telnet را بر روي روتر R1 فعال مي‌كنيم.

```
1   R1(config)#username test password 123
2   R1(config)#line vty 0 4
3   R1(config-line)#login local
4   R1(config-line)#transport input telnet
```

سپس ACL را مي‌نويسيم و دسترسي PC12 را به R1 از طريق Telnet باز مي‌كنيم.

```
1   R1(config)#access-list 25 permit host 192.168.6.3
2   R1(config)#line vty 0 4
3   R1(config-line)#access-class 25 in
```