آزمایشگاه شبکه های کامپیوتری

مهندس حمید ریاضی

توجه :

این کتاب توسط دانشجویان استاد ریاضی با اجازه استاد ، نشر پیدا کرده است و هر گونه استفاده از مطالب فوق با ذکر منبع بلا مانع است.

رزومه مهندس حمید ریاضی :

۱- دارای مدرک CCIE به شماره CSCO10364288 از Cisco

۲- دارای مدرک MCITP Servsr 2008 از Microsoft

۳- تدریس و تالیف شبکه های کامپیوتری و CCNA و CCNP و CCIE و Windows Server 2008 و امنیت شبکه

۴- مبتکر پروژه شبکه های خانگی (Home Networking)

۵- تالیف بیش از چهل کتاب و ebook در زمینه IT

دیگر کتاب های تالیف شده مهندس حمید ریاضی به روش تدرس همراه آزمایش :

۱- آزمایشگاه CCNA با نرم افزار Packet Tracer

۲- آزمایشگاه CCNP SWITCH با نرم افزار GNS3

۳- آزمایشگاه CCNP ROUTER با نرم افزار GNS3

۴- آزمایشگاه CCNP TS با نرم افزار GNS3

۵- آزمایشگاه MCSE 2003 با نرم افزار VMWare

۶- آزمایشگاه MCITP 2008 با نرم افزار VMWare

۷- آزمایشگاه CCIE با نرم افزار GNS3

مقدمه

از آنجایی که دشواری درک مفاهیم شبکه های کامپیوتر ی، انتقال این مفاهیم توسط نویسنده و اساتید را به خواننده و دانشجویان دچار مشکل کرده و همچنین عدم دسترسی ملزومات و ابزار شبکه برای همگان ، آموزش آنرا منحصراً محدود به آموزش تئوری ساخته ، در حال آنکه این آموزش لزوماً تمرین عملی و ممارست می طلبد . وجود این مشکلات مرا بر آن داشت تا حاصل تجربیات و تدریس ها و تالیفات خود را در یک سلسه از آموزش های شبکه به نام آزمایشگاه شبکه های کامپیوتری جمع آوری و در خدمت شما عزیزان قرار دهم . در این کتاب روش جدید و کار آمد تدریس همراه آزمایش را بکار گرفته ام تا شما عزیزان ضمن آشنایی با مباحث شبکه ، کار عملی را به بهترین شکل فراگیرید . همچنین در گتاب با بیان پرسش کلیدی سعی در رفع ابهام در مفاهیم شبکه را داشته ام. امید است چراغی روشن برای شما خوانندگان و طالبان علم شبکه باشد . شما عزیزان می توانید سوالات و مشکلات و مسائل خود را در مورد مباحث فوق را از طریق تلفن ۰۹۱۲۷۵۳۶۸۵۴ یا ایمیل hamidriazi@yahoo.com با من مطرح کنید.

مهندس حمید ریاضی

خصوصیات کتاب آزمایشگاه شبکه های کامپیوتری :

۱- کاملا مفهومی و قابل درک آسان

۲- بدون نیاز به تجربه قبلی در شبکه

۳- شامل توضیحات واضح و ساده

۴- بیان سخت ترین مفاهیم به ساده ترین روش

۵- از نظر محتوایی نیازهای خواننده را مرتفع میکند.

۶- بیان جدید ترین مفاهیم شبکه

۷- زبان نگارش و تنوع در آموزش و دوری از آموزش خشک و کسل کننده به گونه ای که خواننده را به خود جذب می کند.

۸- وقت خواننده را بیخودی تلف نکرده و مباحث را در عین جامع و کامل بودن بطور خلاصه مطرح می کند .

۹- استفاده از یک نرم افزار شبیه سازی شبکه به اسم **Cisco Packet Tracer** برای کار عملی و آموزش آن نرم افزار

۱۰- ارائه آزمایش همراه تدریس و توانایی امتیاز دهی به کار و اعلام اینکه آیا آزمایش فوق درست انجام شده است یا خیر

۱۱- بیان پرسش های کلیدی در نقاط حساس آموزش و ارائه جواب آن در آخر کتاب برای درک مفهومی مطلب فوق

۱۲- دسته بندی مطالب بگونه ای که باعث درک بهتر مفاهیم می شود

۱۳- ارائه مطالب صحیح و درست در مورد مفاهیم شبکه تا خلا آموزش اشتباهی که این روزها زیاد شده است را جبران شود

۱۴- خواننده در انتهای کتاب احساس رضایت و خرسندی دارد

روش استفاده از کتاب :

این کتاب روش جدیدی را برای آموزش شبکه دارد. به همراه آموزش شما تمرین آنچه که آموزش دیده اید را انجام می دهید. کتاب در سه بخش که عبارت است از : درس ، آزمایش و پرسش ، برنامه ریزی شده است . به همراه کتاب یک نرم افزار به نام **Cisco Packet Tracer** که یک نرم افزار شبیه سازی شبکه می باشد نیز موجود است شما باید قبل از خواندن این کتاب آن نرم افزار را نصب کرده و آموزش این نرم افزار را همراه آزمایش های انجام شده ، فرا خواهید گرفت .

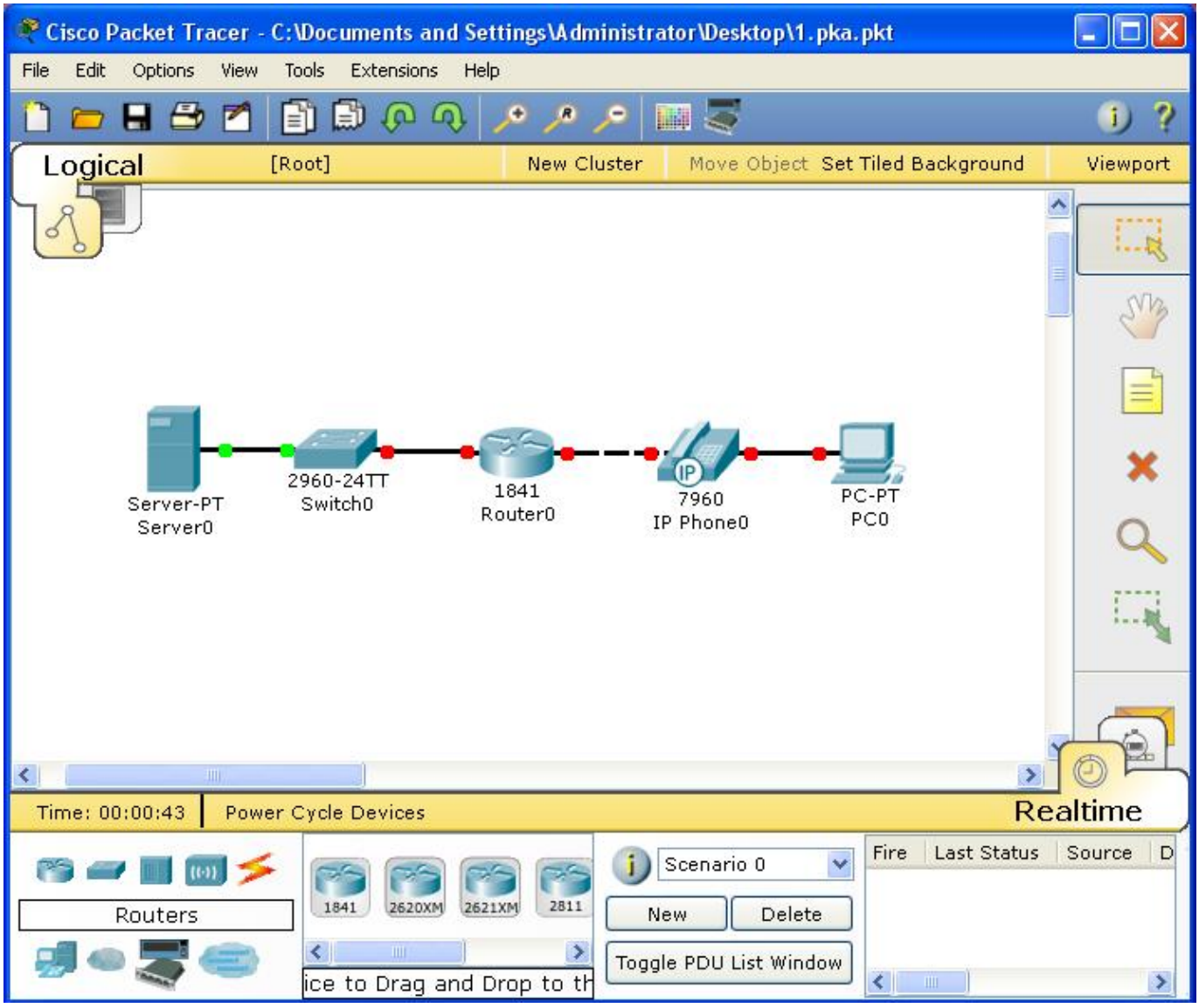
Activity Wizard : به غیر از خود نرم افزار ، برای هر آزمایش یک سری فایل های **Pka** موجود است که شما باید آنها را همراه آزمایش های کتاب حل کنید و انجام دهید. برای هر آزمایش یک **Activity Wizard** ارائه شده است. (به غیر از آزمایش ۵ که یک آزمایش محاسباتی است) . نرم افزار این قابلیت را دارد که بعد از انجام آن آزمایش ، به شما اعلام کند درست انجام داده اید یا نه و اگر درست انجام داده اید تا چند در صد درست انجام داده اید. همچنین در نقاط کلیدی آموزش و آزمایش پرسش های بیان شده است . سعی کنید به آنها حواب داده و جواب خود را در آخر کتاب با جواب درست مقایسه کنید تا مفهوم را بصورت درست درک کنید. فایل های **Activity Wizard** در فولدر **LAB_ACTIVITIES** می باشند که با نرم افزار **Packet Tracer** اجرا می شود.

فهرست :

آزمایش ۱-۱ : آشنایی با نرم افزار Packet Tracer ---------- Page7
آزمایش ۱-۲ : استفاده از مدل OSI و پروتکل TCP/IP ---------- Page14
آزمایشگاه ۱-۳ : آشنایی با توپولوژی شبکه و ساختمان یک شبکه کوچک ---------- Page22
آزمایشگاه ۱-۴ : کلاس های IP و دستورات Ping و Traceroute ---------- Page31
آزمایش ۱-۵ : آدرس IPv4 Subnetting ---------- Page38
آزمایشگاه ۱- ۶ : تقسیم بندی شبکه و Subnetting و Configuration Router ---------- Page49
آزمایشگاه ۱-۷ : تفاوت های Hub و Switch ---------- Page55
آزمایشگاه ۱-۸ : Address Resolution Protocol (ARP) و MAC Table ---------- Page60
آزمایشگاه ۱-۹ : شبکه Wireless (بی سیم) و امنیت شبکه ---------- Page66
آزمایشگاه ۱-۱۰ : ایجاد یک توپولوژی کوچک و VLSM ---------- Page74
ضمیمه ۱ - تجهیزات شبکه ---------- Page85
ضمیمه ۲ - تکنولوژیهای انتقال اطلاعات چیست ؟ ---------- Page92
ضمیمه ۳ – انواع کابل های شبکه ---------- Page95
جواب سوالات کتاب ---------- Page104

آزمایش ۱: آشنایی با نرم افزار Packet Tracer

Topology Diagram



درس :

شبکه کامپیوتری چیست ؟

شبکه کامپیوتری، مجموعه ای از کامپیوترهای مستقل است که از طریق یک رسانه انتقال (**Transmission media**) مثلا یک کابل با یکدیگر به تبادل اطلاعات داده می پردازد.

مزایا و فواید شبکه:

۱- استفاده مشترک از منابع:

استفاده مشترک از یک منبع اطلاعاتی یا امکانات جانبی کامپیوتر ، بدون توجه به محل جغرافیایی آن

۲- کاهش هزینه:

متمرکز نمودن منابع واستفاده مشترک از آنها وپرهیز از پخش آنها در واحدهای مختلف باعث کاهش هزینه می شود.

۳- قابلیت اطمینان:

در صورت عدم دسترسی به یک از منابع اطلاعاتی در شبکه (بعلت از کارافتادن سیستم) از نسخه های پشتیبان استفاده کرد.

۴- کاهش زمان :

بدون محدودیت جغرافیایی تبادل اطلاعات وجود دارد. به این ترتیب زمان تبادل اطلاعات و استفاده از منابع خود بخود کاهش می یابد.

۵- قابلیت توسعه:

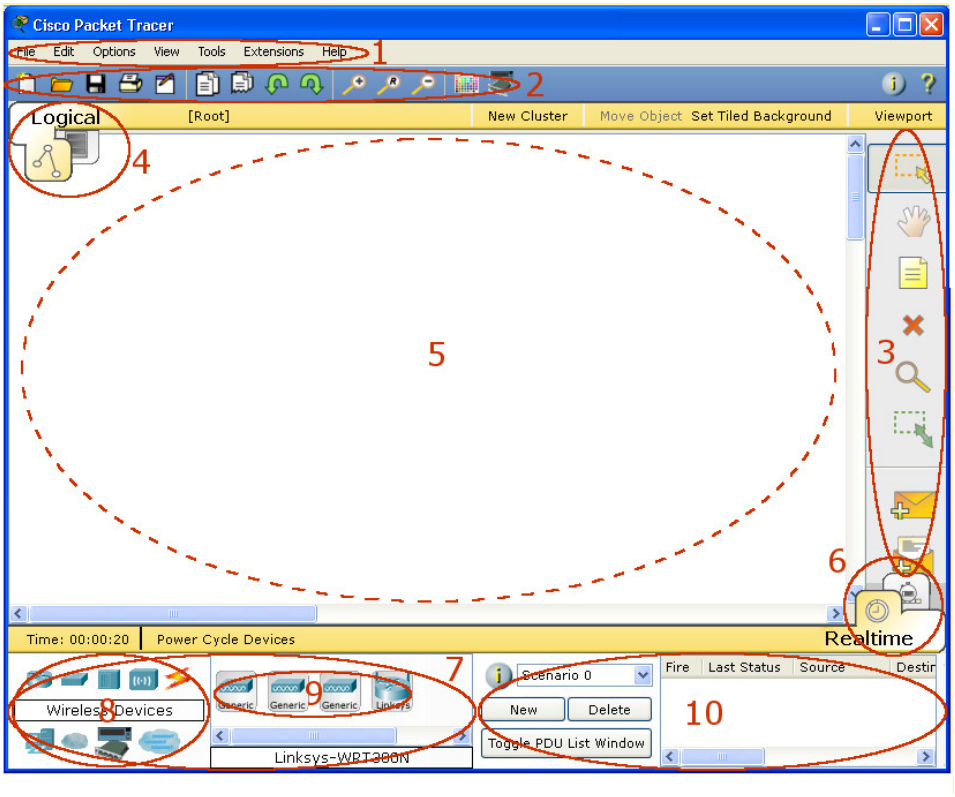
یک شبکه محلی می تواند بدون تغییر در ساختار سیستم توسعه یابد وتبدیل به یک شبکه بزرگتر شود.

۶- ارتباطات:

کاربران می توانند از طریق مثلا پست الکترونیکی ویا دیگر سیستم های اطلاع رسانی پیغام هایشان را مبادله کنند .

نرم افزار Packet Tracer چیست ؟

نرم افزار **Packet Tracer** یک نرم افزار شبیه ساز شبکه است که اجازه می دهد تا یک شبکه شبیه سازی شده ایجاد کنید ، پیکربندی سیستم ها در شبکه ، تست شبکه ، تعیین ترافیک شبکه از جمله خصوصیات این نرم افزار است . نرم افزار شامل بخش های زیر است :



۱- **Menu Bar** : این نوار منو های **Extensions, Tools, View, Options , Edit, File** و **Help** را فراهم می کند. که شما دستورات **Print , Save, Open** و **Preferences** را در این دستورات می توانید ببینید.

۲- **Main Tool Bar** : در این منو شما **shortcut** دستورات **Menu Bar** را مشاهده می کنید .

۳- **Common Tools Bar :** این نوار ابزارهای عمومی **workspace** را فراهم می کند.

۴- **Logical/Physical Workspace:** در اینجا شما شبکه خود را به صورت فیزیکی و منطقی می توانید ببینید . که با کلیک بروی آنها می توانید از یکی به دیگری بروید.

۵- **Workspace :** در این ناحیه شما می توانید شبکه خود را پیاده سازی کرده و شبیه سازی کنید.

۶- **Realtime/Simulation Bar :** شما با کلیک در این ناحیه می توانید زمان شبیه سازی را متوقف و یا به زمان واقعی ببرید. در حالت شبیه سازی جزئیاتی که در شبکه اتفاق می افتد را دقیقتر می توانید بررسی کنید.

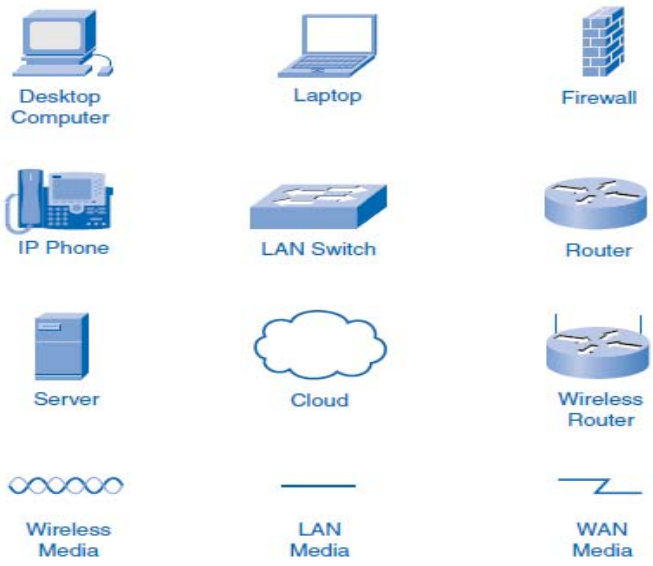
۷- **Network Component Box :** این کادر جایی است که شما **device** ها را انتخاب می کنید و ودر **workspace** آنها را بهم ارتباط می دهید.

۸- **Device-Type Selection Box :** این کادر شامل انواع **device** ها و **connection** های موجود در **Packet Tracer** می شود.

۹- **Device-Specific Selection Box :** این کادر برای انتخاب نوع خاصی از یک **device** می باشد.

۱۰- **User Created Packet Window :** اگر در مد شبیه سازی باشید مشخصات باشید مشخصات بسته های اطلاعاتی در شبکه خود را مشاهده می کنید.

اولین قدم در ایجاد یک شبکه شبیه سازی شده ، قرار دادن **Devices** (دستگاه ها) در **Logical Workplace** و **Connect** (ارتباط دادن) آنها به هم می باشد . **Packet Tracer** با استفاده از **Symbols** (نمادها) ، **Device** ها مختلف را شبیه سازی کرده است که تعدادی از این **Symbol** ها عبارت است از :



Device مهم در Packet Tracer :

Devices ها در سمت چپ پایین نرم افزار قرار دارد که که عبارت از :

- **End Devices** : دستگاه هایی که به عنوان **Source** (منبع) ویا به عنوان **Destination** (مقصد) در شبکه استفاده می شوند که شامل **PC** (کامپیوتر) ها  و **Laptop** ها  و **Server** ها  (کامپیوتر سرویس دهنده به شبکه) و... می باشد.

- **Router** : همانطورکه ازاسمشان پیداست کارشان مسیر یابی برای بسته ها**(Packet)** ی اطلاعات در شبکه می باشد و وسیله ای است که طریقه انتقال اطلاعات را مشخص می کند . بطور مثال وظیفه روتر یافتن کوتاه ترین مسیر برای دسترسی به مطلبی ازسرورربه کامپیوترماست.

- **Switch** : برای اتصال دستگاهای مختلف از قبیل کامپیوتر ها , مسیریاب ها , **Printer** ها تحت شبکه , دوربین های مدار بسته و .... در شبکه ها مورد استفاده واقع می شود.

- **Hubs :** رابطی سخت افزاری است که برای متصل کردن کامپیوتر های موجود در یک شبکه به یکدیگر از آن استفاده می شود. همانند **Switch** ولی خیلی ساده تر و ارزان تر و میزان هوشمندی پایین می باشند .

- **Wireless Devices :** به تکنولوژی ارتباطی اطلاق می شود که در آن از امواج رادیویی، مادون قرمز و مایکروویو ، به جای سیم و کابل ، برای انتقال سیگنال بین دو دستگاه استفاده می شود.

- **Connection :** کابل های اتصال بین **Devices** ها می باشد که بسته به دستگاهها کابل ها متفاوت می شوند.

سناریو :

در این آزمایش شما با محیط نرم افزار **Packet Tracer** آشنا شده و **Device** ها مختلفی از جمله **PC** ها و **Switch** ها و **Router** ها را در **Logical Workplace** اضافه می کنید و به وسیله اتصال خودکار به همدیگر وصل می کنید.

فعالیت ۱ : بررسی نرم افزار **Packet Tracer**

مرحله ۱ – **Logical Workplace**

هنگامی که **Packet Tracer** شروع می شود ، صفحه سفید و بزرگی که روبرو شما است ، فضای **Logical Workplace** می باشد که شما می توانید **Device** ها را به آن اضافه کرده و بهم وصل کنید.

مرحله ۲ – **Device Symbols**

قسمت سمت چپ پایین نرم افزار ، در زیر نوار زرد ، بخشی است که مجموعه از به **Device** ها متفاوت وجود دارد که شما می توانید با انتخاب هر کدام از آنها و در گ کدن آن به **Logical Workplace** اضافه کنید . همانطور که شما اشاره گر ماوس بر سر این نماد حرکت می دهید ، نام گروه آنها در جعبه متن مرکزی آن نمایش داده می شود . هنگامی که شما یکی از این نمادها را کلیک کنید ، دستگاه های خاص در این گروه در جعبه سمت راست ظاهر می شود . بر روی هر یک از گروه ها کلیک کنید و با انواع دستگاه های که در دسترس هستند آشنا شوید نمادهای مربوط به هر کدام را را گیرید.

فعالیت ۲ : افزودن **Device** به **Logical Workplace**

مرحله ۱ – انتخاب و قرار دادن دستگاه

برای اضافه کردن یک دستگاه به **Logical Workplace** بر روی سمبل دستگاه خاص کلیک کنید ، اشاره به محلی که می خواهید **Device** در **Logical Workplace** قرار گیرد بکنید و کلیک کنید. **Device** های زیر را با فاصله یک اینچ از هم از چپ به راست در یک ردیف قرار دهید.

- **A Server**
- **A 2960 Switch**
- **An 1841 Router**
- **A Hub**
- **An IP Phone**
- **A PC**

مرحله ۲ – دستگاه ها را با **Auto Connect** به هم اتصال دهید

با کلیک بر روی نماد گروه **Connect** ، انواع کابل های مختلف است که برای اتصال **Device** ها می باشد در سمت راست آن نمایان می شود شما اولین نوع آن که ، **Auto Connec** می باشد و به طور خودکار نوع ارتباط بر اساس رابط های موجود در دستگاه می باشد را انتخاب کنید.هنگامی که شما این نماد را انتخاب می کنید ، اشاره گر ماوس شبیه یک کانکتور کابل می شود . بعد با کلیک بر روی دستگاه اول ، و سپس با کلیک بر روی دستگاه دوم ، ارتباط بین دو دستگاه به طور خودکار بر قرار می شود . از **Server** شروع کنید و هر دستگاه را دو به دو بهم وصل کنید .

مرحله ۳– اطلاعاتی از **Device** ها

با موس بروی هر کدام از **Device** ها بروید و موس را بروی آن نگه دارید . اطلاعاتی مختصر از مشخصات آن **Device** و همچنین تنظیمات آن خواهید دید .

مرحله ۴ – تب های **Phsical** و **Config** و **Desktop**

بروی **Server** یا **PC** کلیک کنید سه تب می بینید . در تب **Phsical** تصویر فیزیکی آن را خواهید دید ، شما می توانید با دکمه **Zoom in** و **Zomm out** آن را کوچک و بزرگ کنید و همچنین با زدن دکمه **Power** بروی آن ، **Server** را خاموش و روشن کنید. در تب **Config** می توانید تنظیمات نرم افزاری آن را انجام دهید و در تب **Desktop** می توانید **Desktop** سرور را دیده و از امکانات آن استفاده کنید . امکاناتی همچون **Web Browser** و **Command Prompt** و **IP Configuration**

مرحله ۵ - تب **CLI**

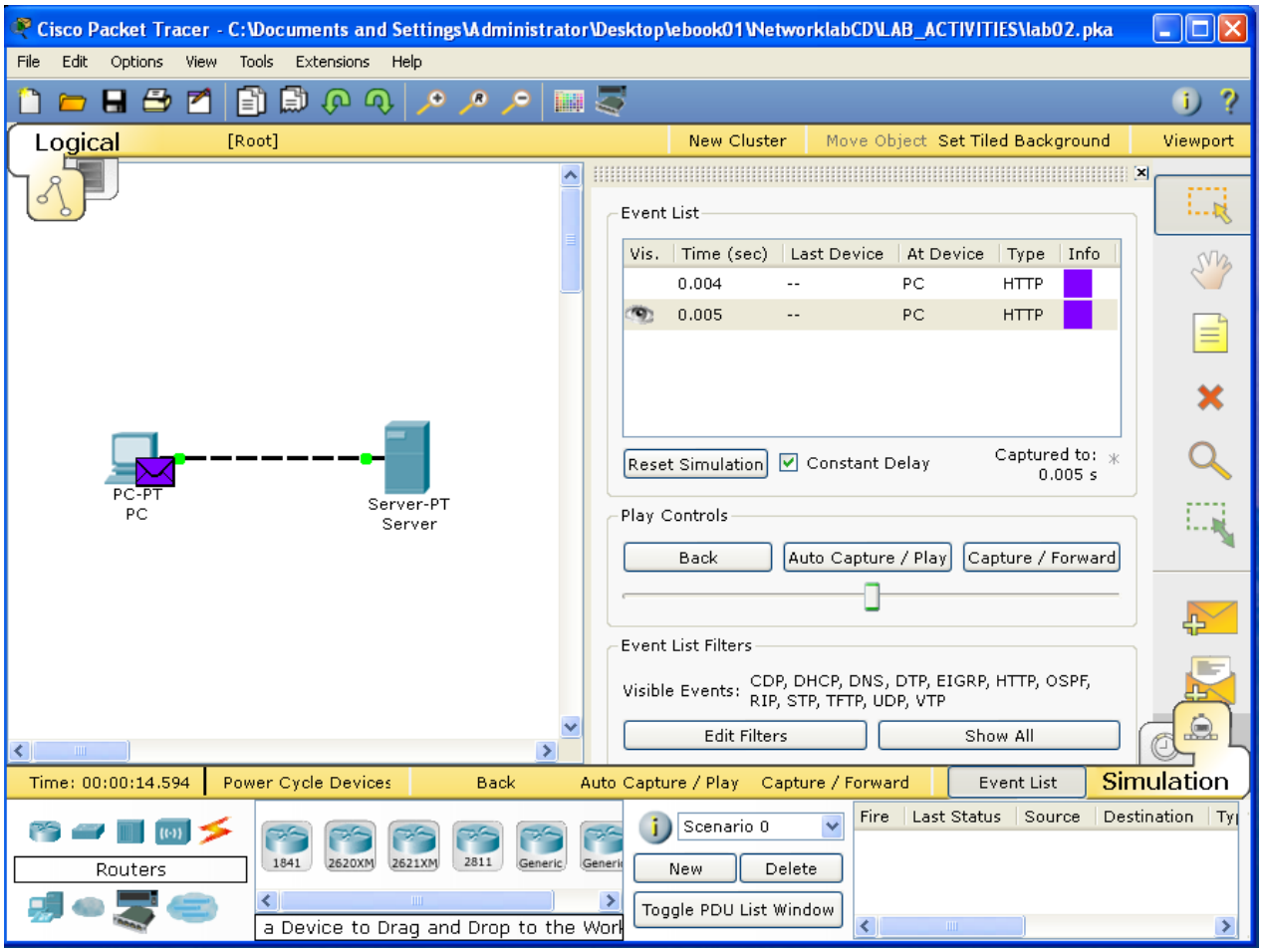
بروی **Switch** یا **Router** کلیک کنید در اینجا نیز سه تب می بینید با این تفاوت که تب سوم ، تب **CLI** می باشد که ما را به سیستم عامل روتر یا سوییچ وصل می کند.

مرحله ۶– امتیاز دهی **Packet Tracer**

نرم افزار **Packet Tracer** می تواند به کار شما نمره بدهد . برای چک کردن کار خود می توانیددر **Packet Tracer activities** با کلیک بر روی دکمه **Check Results** نتایج را ببینید.

آزمایش ۲ : استفاده از مدل OSI و پروتکل TCP/IP

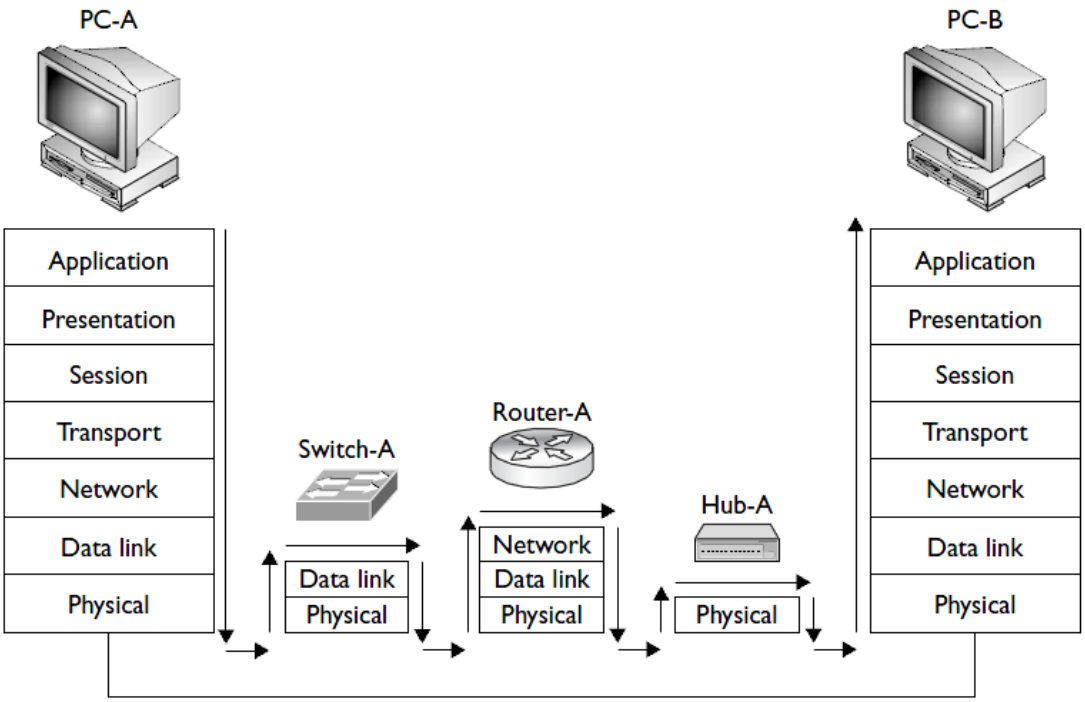
Topology Diagram



درس :

مدل OSI

انتقال اطلاعات بین کامپیوترهای مختلف در شبکه وابسته به انتقال اطلاعات بین بخش های نرم‌افزاری و سخت‌افزاری درون هر یک از کامپیوترها است. هر یک از فرایندهای انتقال اطلاعات را می توان به بخش‌های کوچک‌تری تقسیم کرد. هر یک از این فعالیت‌های کوچک را سیستم عامل براساس دسته‌ای از قوانین مشخص انجام می‌دهد. این قوانین را پروتکل (**Protocol**) می‌نامند. پروتکل مجموعه‌ای از قوانین است که با اصطلاحات فنی چگونگی انجام گرفتن کاری را توصیف می‌کند. برای استانداردسازی پروتکل‌های ارتباطی، سازمان استانداردهای بین‌المللی **OSI** اقدام به تعیین مدل مرجع **OSI** یا **Open SystemsInterconnection** نمود. مدل مرجع **OSI** ارائه‌دهنده چارچوب طراحی محیط‌های شبکه‌ای است. در این مدل، جزئیات بخش‌های نرم افزاری و سخت افزاری برای ایجاد سهولت انتقال اطلاعات مطرح شده است و در آن کلیه فعالیت‌های شبکه‌ای در هفت لایه مدل‌سازی می‌شود. هنگام بررسی فرآیند انتقال اطلاعات بین دو کامپیوتر، مدل هفت لایه‌ای **OSI**روی هر یک از کامپیوترها پیاده‌سازی می‌گردد. در تحلیل این فرایندها می‌توان عملیات انتقال اطلاعات را بین لایه‌های متناظر مدل **OSI** واقع در کامپیوترهای مبدا و مقصد در نظر گرفت. در کامپیوتر مبدا اطلاعات از لایه فوقانی به طرف لایه تحتانی مدل **OSI** حرکت کرده و از آن جا به لایه زیرین مدل **OSI** واقع در کامپیوتر مقصد ارسال می‌شوند. در کامپیوتر مقصد اطلاعات از لایه‌های زیرین به طرف بالاترین لایه مدل **OSI** حرکت می کنند.



بالاتری لایه ، لایه هفت، لایه کاربرد یا **Application** است. این لایه تأمین‌کننده سرویس‌های پشتیبانی برنامه های کاربردی نظیر انتقال فایل، دسترسی به بانک اطلاعاتی و پست الکترونیکی است.

لایه شش، لایه نمایش یا **Presentation** است. این لایه تعیین‌کننده فرمت یا قالب انتقال داده‌ها بین کامپیوترهای واقع در شبکه است. این لایه در کامپیوتر مبدا داده‌هایی که باید انتقال داده شوند را به یک قالب میانی تبدیل می‌کند. این لایه در کامپیوتر مقصد اطلاعات را از قالب میانی به قالب اولیه تبدیل می کند.

لایه پنجم ، لایه جلسه یا **Session** است. این لایه بر برقراری اتصال بین دو برنامه کاربردی روی دو کامپیوتر مختلف واقع در شبکه نظارت دارد. همچنین تأمین کننده همزمانی فعالیت های کاربر نیز هست.

لایه چهارم ، لایه انتقال یا **Transmission** مسؤول ارسال و دریافت اطلاعات و کمک به رفع خطاهای ایجاد شده در طول ارتباط است. هنگامی که حین یک ارتباط خطایی بروز کند، این لایه مسؤول تکرار عملیات ارسال داده است.

لایه سوم ، لایه شبکه یا **Network** نام دارد.در مدل **OSI**، مسؤول آدرس یا نشانی گذاری پیام‌ها و تبدیل نشانی‌های منطقی به آدرس‌های فیزیکی است. این لایه همچنین مسؤول مدیریت بر مشکلات مربوط به ترافیک شبکه نظیر کند شدن جریان اطلاعات است.

لایه دوم ، لایه پیوند یا **Data link** است. این لایه وظیفه دارد تا اطلاعات دریافت شده از لایه شبکه را به قالبی منطقی به نام فریم (**frame**) تبدیل کند. در کامپیوتر مقصد این لایه همچنین مسؤول دریافت بدون خطای این فریم‌ها است.

لایه زیرین ، لایه فیزیکی یا **Physical** است. این لایه اطلاعات را به صورت جریانی از رشته های داده ای و به صورت الکتریکی روی کابل هدایت می کند. این لایه تعریف کننده ارتباط کابل و کارت شبکه و همچنین تعیین‌کننده تکنیک ارسال و دریافت داده ها نیز هست.

TCP/IP چیست ؟

TCP علامت اختصاری **Transmission Control Protocol** و **IP** علامت اختصاری **Internet Protocol** می باشد. که **TCP/IP** نام متداولی برای مجموعه‌از بیش از ۱۰۰ پروتکل می‌باشد که برای متصل ساختن کامپیوترها و شبکه‌ها استفاده می‌شود.

پروتکل های موجود در لایه Transmission از مجموعه TCP/IP

TCP(**Transmission Control Protocol**) ، مهمترین وظیفه پروتکل فوق اطمینان از صحت ارسال اطلاعات است . پروتکل فوق اصطلاحا" **Connection-oriented** نامیده می شود یعنی به عنوان یک پروتکل قابل اطمینان یاد می شود. علت این امر ارسال اطلاعات و کسب آگاهی لازم از گیرنده اطلاعات به منظور اطمینان از صحت ارسال توسط فرستنده است . در صورتی که بسته های اطلاعاتی بدرستی دراختیار فرستنده قرار نگیرند، فرستنده مجددا" اقدام به ارسال اطلاعات می نماید.

UDP(**User Datagram Protocol**) ، این پروتکل شبیه پروتکل **TCP** است با این تفاوت که بر خلاف پروتکل **TCP** بصورت **Connection-less** یا بدون اتصال است . بدیهی است که سرعت پروتکل فوق نسبت به **TCP** سریعتر بوده ولی از بعد کنترل خطاء تظمینات لازم را ارائه نخواهد داد. بهترین جایگاه استفاده از پروتکل فوق در مواردی است که برای ارسال و دریافت اطلاعات به یک سطح بالا از اطمینان ، نیاز نداشته باشیم .

پروتکل های موجود در لایه Network از مجموعه TCP/IP

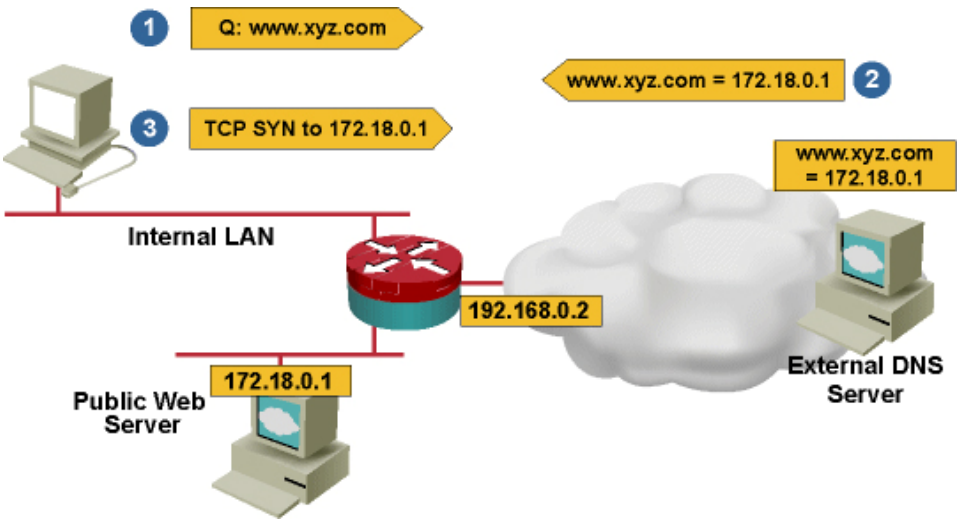
IP(**Internet Protocol**) ، **IP Address** یک عددی ۳۲ بیتی است که به هر سیستم برای شناسایی و منحصر به فرد بودن در شبکه به آن اختصاص داده می شود مهمترین مسئولیت آن دریافت و ارسال بسته های اطلاعاتی به مقاصد درست است . پروتکل فوق با استفاده از آدرس های نسبت داده شده منطقی، عملیات روتینگ (مسیر یابی) بسته های اطلاعاتی را انجام خواهد داد.

پروتکل های موجود در لایه Application از مجموعه TCP/IP

پروتکل **HTTP**(**HyperText Transfer Protocol**) مشهورترین پروتکل در این گروه بوده و از آن برای رایج ترین سرویس اینترنت یعنی وب استفاده می گردد. با استفاده از پروتکل فوق کامپیوترها قادر به مبادله فایل ها با فرمت های متفاوت (متن، تصاویر ،گرافیکی ، صدا، ویدئو و...) خواهند بود. برای مبادله اطلاعات با استناد به پروتکل فوق می بایست ، کاربران با استفاده از یک مرورگر وب قادر به استفاده از سرویس فوق خواهند بود.

پروتکل **DHCP** (**Dynamic Host Configuration Protocol**) به شما اجازه می دهد آدرسهای **IP** را بصورت اتوماتیک به کامپیوترها و وسایل جانبی روی شبکه اختصاص دهید. آدرس های **IP** از مخزنی از آدرس های تهیه شده و به کامپیوترها اختصاص داده می شوند و نیاز به وارد کردن دستی آدرسهای **IP** نباشد.

پروتکل **DNS** (**Domain Name System**) هر کامپیوتر در شبکه یک **Host** نامیده می شود و علاوه بر آدرس **IP** دارای یک عنوان مشخص کننده دیگر به نام **Host Name** می باشد. از پروتکل فوق به منظور ترجمه **Host Name** به آدرس های **IP** استفاده می گردد. یک کامپیوتر برای بدست آوردن **IP Address** متناظر با **Host Name** ، از کامپیوتری در شبکه با نام **DNS Server** کمک می گیرد. **DNS Server** حاوی نام و **IP Address** کامپیوتر مورد نظر می باشد که پس از مقایسه درخواست با اطلاعات موجود در **Database** (پایگاه داده) خود ، **IP Address** مورد نظر را بر میگرداند.



پروتکل TCP/IP در نرم افزار Packet Tracer

در داخل شبکه ، اطلاعات به صورت جریان ثابتی از **Host** (میزبان) به **Host** منتقل نمی‌شود. بلکه داده‌ها به بسته‌های کوچکی به نام **packet** (بسته) شکسته می‌شوند و بعد از آن منتقل می شوند . در نرم افزار **Packet Tracer** ، جزئیات مربوط به بسته های اطلاعاتی و چگونگی پردازش آنها را توسط دستگاه های شبکه های می توان مشاهده کرد .پروتکل **TCP/IP** در نرم افزار **Packet Tracer** مدل شده است ، که شامل **DNS, HTTP, TCP, UDP** و .. می باشد که با مدل **OSI** نمایش می دهد ونشان می دهد که چگونه این پروتکل ها توسط دستگاه های شبکه در ایجاد و پردازش بسته های اطلاعاتی استفاده می شود . به این بسته های اطلاعاتی ، پروتکل واحد داده یا **PDU** (**Protocol Data Units**) که به قطعه داده ای که در هر لایه (طبق پروتکل مربوطه) سازماندهی و تحویل لایه زیرین میشود گفته می شود و در هر لایه نام خود را دارد به عنوان مثال **segments** در لایه **transport** ، **packets** در لایه **network** ، و **frames** در لایه **Data link** می باشد. که **frame** در این لایه توسط **Ethernet** (یک نوع تکنولوژی انتقال اطلاعات می باشد که مشخص می کند فریم ها چگونه و چطور بروی کابل انتقال داده جایگذاری شوند) در شبکه قرار می گیرند.

سناریو :

در این آزمایش می خواهیم یک **PDU** ساده ایجاد کرده و بعد از حالت **Realtime** به حالت **Simulation** (شبیه سازی) رفته و با دسترسی به پنجره **PDU Information** مدل **OSI** را مشاهده کنید و سپس الگوریتم **Device** در مدل **OSI** بررسی می کنیم و **PDU** ورودی و خروجی را مشاهده کرده و حرکت **packet** (بسته اطلا عاتی) را مشاهده کنید .

فعالیت ۱ : بررسی **interface** (رابط) های نرم افزار **Packet Tracer**

مرحله ۱ – بررسی فایل های کمکی و آموزش ها

از منو بالا نرم افزار **Packet Tracer** ، گزینه **Help->Contents** را انتخاب کنید ، صفحه وبی باز خواهد شد .از قاب سمت چپ **Operating Modes->Simulation Mode** را انتخاب کنید و در مورد حالت **Simulation** مطالعه کنید.

مرحله ۲ – تعویض از حالت **Realtime** به حالت **Simulation**

در سمت راست پایین نرم افزار شما می توانید از حالت **Realtime** به حالت **Simulation** یروید ویا برعکس . نرم افزار همیشه در حالت **Realtime** می با شد که در آن پروتکل های شبکه با زمان واقعی شروع می شود .با این حال ، یکی از ویژگی های قدرتمند**Packet Tracer** این است امکان می دهد تا کاربر زمان را توسط تعویض به حالت **Simulation** متوقف کند .در حالت شبیه سازی ، بسته های اطلاعاتی به عنوان پاکت متحرک نمایش داده می شود ، و کاربر می تواند قدم به قدم اتفاقات پیش آمده در این انتقال را مشاهده کند .

فعالیت ۲ : بررسی محتویات بسته و پردازش

مرحله ۱ – ایجاد یک **Packet** (بسته) و دسترسی به پنجره اطلاعات **PDU** ها

بروی کامپیوتر **Web Client** کلیک کنید . **Desktop** ، **Tab** را انتخاب کنید . **Web Browser** (مرورگر وب) باز کنید .آدرس آی پی **Web Server** (سروری که ارائه دهنده خدمات وب است) یعنی **192.168.1.2** را در مرورگر خود تایپ کنید . با کلیک کردن روی دکمه **Go** درخواست شما آغاز می شود . صفحه مورد نظر را **Minimize** کنید. از زمان که این شبیه سازی اتفاق میفتد ، شما با استفاده از دکمه **Capture/Forward** در حالت **Simulation** می توانید رویدادهای شبکه را مشاهده کنید . برای حرکت هر بار بسته اطلاعاتی در یک مسیر باید دکمه **Capture/Forward** را کلیک کنیم و برای دیدن حرکت بعدی آن دو باره باید **Capture/Forward** را کلیک کنیم .دو **packets** (بسته) را در **Event List** (لیست رویداد) به نظر می رسد که یک علامت چشم در کنار آن قرار دارد . چشم کنار بسته به معنی است که آن **packets** در صفحه نمایش داده می شود . اولین **packets** در **Event List** را پیدا کنید و بروی و بر روی مربع رنگی در ستون **Info** کلیک کنید .

مرحله ۲ – بررسی الگوریتم های دستگاه را در **Modelview OSI**

هنگامی که برای اطلاعات بسته بروی مربع رنگی در **Event list** کلیک کنید ، پنجره **PDU** اطلاعات باز می شود و مدل **OSI** سازماندهی شده را در این پنجره می بینید .در مورد بسته اول ما درخواست **HTTP** (در لایه ۷) را می بینیم و سپس ، **Encapsulated** (بسته بندی شده) در لایه های ۴ ، ۳ ، ۲ و ۱ مشاهده می کنید .

مرحله ۳ – **PDU** های داخلی و خارجی

هنگام باز کردن پنجره اطلاعات **PDU** ، به طور پیش فرض مدل **OSI** مشاهده می شود . بروی **Tab** ، **Outbound PDU Details** کلیک کنید . به پایین پنجره بیایید .در آنجا شما درخواست **HTTP** که در **TCP segment** بسته بندی شده است را خواهید دید ، که به نوبه خود در **IP packet** محصور شده ، که باز به نوبه خود در **Ethernet frame** محصور شده ، که باز به نوبه خود است به عنوان بیت در رسانه منتقل می شود .اگر **Device** اولین دستگاه در مجموعه ای انتقال بسته های اطلاعاتی باشد دارای **Tab** ، **Outbound PDU Details** می باشد . اما اگر آخرین **Device** در مجموعه ای انتقال بسته های اطلاعاتی باشد دارای **Tab** ، **Inbound PDU Details** می باشد . عمو ما شما می توانید **Outbound PDU details** و **Inbound PDU details** را مشاهده کنید .

مرحله ۴ – انیمیشن از جریان **packet** ها در لایه هفت

شما با زدن دکمه **Capture/Forward** در حالت **Simulation** می توانید قدم به قدم ، حرکت **packet** ها را مشاهده کنید وقتی شما درخواست صفحه وب را می کنید .توجه داشته باشید که شما فقط نمایش بسته های مربوط به **HTTP** را مشاهده می کنید.یعنی حرکت پکت از نگاه لایه هفت ، لایه **Application** را می بینید همچنین شما می توانید در هر مرحله پنجره **PDU Information** را باز کنید و مدل **OSI** را مشاهده کنید و خواهید دید که این پکت در لایه هفت قرار دارد و پیش بینی کنید آینده چه اتفاقی خواهد افتاد .

مرحله ۵– انیمیشن از جریان **packet** ها در لایه چهار

می خواهیم این انمیشن را در لایه **Transmission** ببینم حالا فعالیت فوق را تکرار کنید با این تفاوت که در تب **Simulation** بر روی دکمه **Edit Filter** کلیک کرده و تیک **HTTP** را برداشته و به جای آن تیک **TCP** را بگذارید و حالا این انمیشن را از دید لایه چهار خواهید دید . بعد از دیدن انمیشن همه چیز را به حالت اول بر گردانید یعنی تیک **TCP** را برداشته و به جای آن تیک **HTTP** را بگذارید

فعالیت ۳ : استفاده از DNS Server

چون استفاده از اسم وب سایت هم معمول تر است و هم ساده تر است به جای تایپ آدرس **IP** از اسم **Web Server** استفاده می کنیم . برای این کار از یک **DNS Server** که در این آزمایش سرور ما هم **Web Server** است و هم **DNS Server** است استفاده می کنیم . به حالت **Simulation** رفته و سپس در مرورگر ، **www.example.com** را تایپ می کنیم و صفحه مورد نظر را **Minimize** کنید. بعد با زدن دکمه **Capture/Forward** می توانید قدم به قدم ، حرکت **packet** ها را مشاهده کنید . اول یک پکت **DNS** برای پیدا کردن آدرس **IP**، اسمی که تایپ شده ایجاد می شود و سپس بعد از بدست آوردن آدرس **IP** ، پکت **HTTP** را ارسال می کند. توجه داشته باشید که درخواست **DNS** که در **UDP segment** بسته بندی شده است و از دید لایه چهار یک **UDP** می باشد.

فعالیت ۴ : استفاده از DHCP Server

وظیفه **DHCP Server** اختصاص **IP Address** به سیستم ها موجود در آن شبکه می باشد . شما اول در حالت **Simulation** قرار بگیرید و سپس بروی **Server** کلیک کنید و در تب **Config** بروی **DHCP** کلیک کنید و با **On** یا روشن کردن این سرویس بر روی سرور خود آن را تبدیل به یک **DHCP Server** کنید . حالا بروی **PC** به قسمت **Desktop** رفته و بروی **IP Configuration** کلیک کرده و با زدن گزینه **DHCP** ، آدرس **IP** آن را از حالت دستی به حالت گرفتن **IP** از **Server** در آورید. چگونگی کارکرد آن را در چهار مرحله می بینید :

۱. **DHCP Discover** : در این مرحله **Client** درخواست خود را جهت دریافت **IP**در شبکه پخش میکند.

۲. **DHCP Offer** : در این مرحله **DHCP Server**هائیکه **DHCP Discover** انجام شده در مرحله اول را دریافت میکنند از رنج **IP** تعریف شده بر روی خود یک **IP** انتخاب نموده و آن را برای **Client** می فرستد.

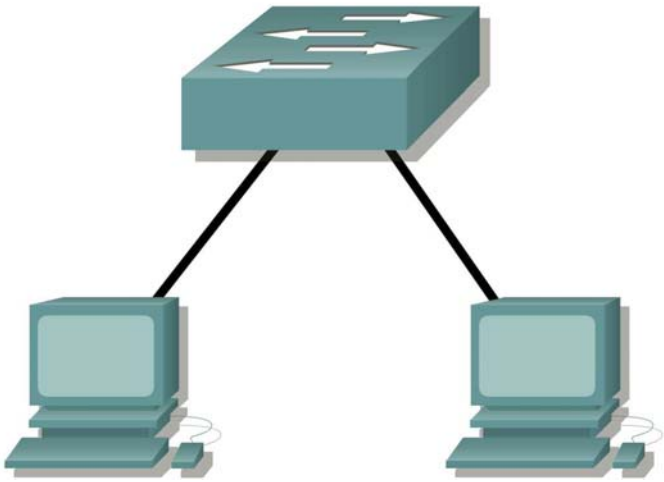
۳. **DHCP Request** : **Client** درخواست کننده پس از دریافت **DHCP Offer** ، قبول کردن آنرا توسط یک پکت به سرور **DHCP** اعلام می کند .

۴. **DHCP Ack,DHCP Nack** : **DHCP Server** در صورتیکه هنوز **IP** که **Offer** شده در **Range** او وجود داشته باشد و توسط **Admin**حذف نشده باشد **DHCP Server** با **DHCP Ack** تایید خود را مبنی بر اختصاص **IP** به **Client** اعلام میکند. ولی اگر **IP** توسط **Admin** از **Range** مربوطه حذف شده باشد **DHCP** به **Client** درخواست کننده پیغام **DHCP Nack**را ارسال میکند و **Client** مجبور میشود که تمام مراحل را دوباره طی کند.

آزمایشگاه ۳ : آشنایی با توپولوژی شبکه و ساختمان یک شبکه کوچک

Topology Diagram

Peer to Peer Network



Switched Network

Addressing Table

PC Name	IP Address	Subnet Mask
PC1	192.168.1.2	255.255.255.0
PC2	192.168.1.3	255.255.255.0

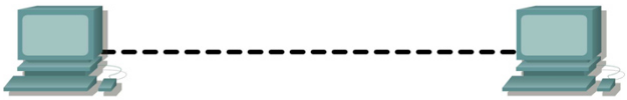
درس :

Topology (پیکر بندی) شبکه و انواع آن :

Server(کامپیوتری که یک سرویس خاصی را به شبکه می دهند) ها و **Client** (کامپیوتری که از شبکه سرویس می گیرد) ها باید طبق یک طرح و نقشه مشخص به وسیله محیط انتقال به یکدیگر متصل شوند که به این طرح و نقشه پیکر بندی (**Topology**) شبکه می گویند .

انواع توپولوژی شبکه :

۱- **peer-to-peer** : یک مدل برقراری ارتباط بین **Device** ها است که در آن هر طرف توانایی های یکسانی دارد و هر طرف بطور مستقیم و بدون واسط بهم وصل می شوند .

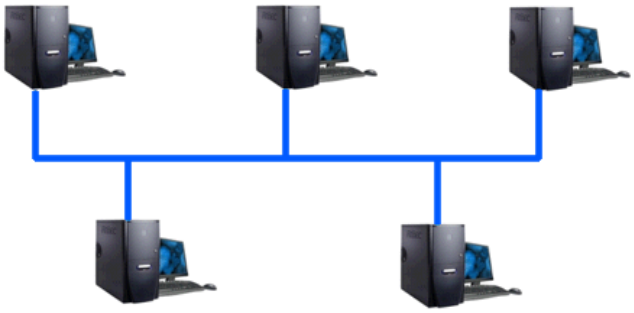


۲- **Bus** : در یک شبکه خطی چندین کامپیوتر به یک کابل به نام **Bus** متصل میشود. در این توپولوژی رسانه انتقال بین کلیه کامپیوتر ها مشترک است. عمده این شبکه این است که اگر **Back bone** (کابل اصلی) که پل ارتباطی بین کامپیوتر های شبکه است ، قطع شود ، کل شبکه از کار خواهد افتاد.

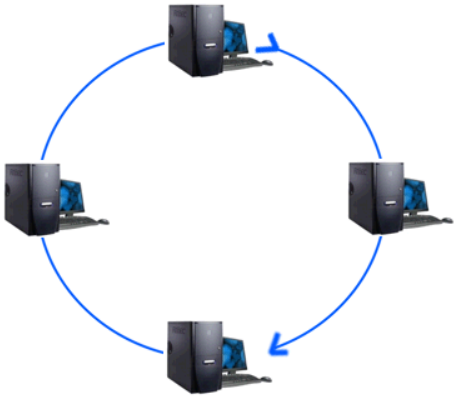
۳- **Ring** : در این نوع توپولوژی تمام کامپیوترها بصورت یک حلقه به یکدیگر مرتبط می گردند. داده ها فقط در یک جهت حرکت کرده و از ایستگاهی به ایستگاه دیگر انتقال پیدا می کنند.

۴- **Star** : کلیه **Device** ها به یک نقطه مر کزی به اسم **Hub** یا **Switch** متصل می شوند . شبکه های متوسط و بزرگ اغلب از توپولوژی ستاره ای استفاده میکنند. در این پیکر بندی مدیریت آسانتر و احتمال خرابی آن کمتر است. کابل مورد استفاده توپولوژی ستاره ای اترنت کابل زوج بهم تابیده بدون حفاظ است. توپولوژی ستاره ای به کابل بسیار زیاد و یک هاب یا سویتچ نیاز دارد. تمامی اینها منجر به بالا رفتن هزینه شبکه میشود با این مزیت که این روش بسیار مفید است.

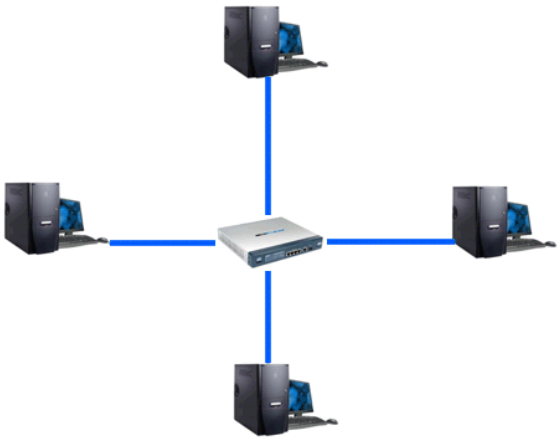
۵- **Mesh** : یک شبکه ارتباطی که در آن دویا بیش از دو مسیر برای هر گره وجود دارد. در این توپولوژی هر کامپیوتری مستقیما به کلیه کامپیوترهای شبکه متصل می شود. مزیت این توپولوژی آن است که هر کامپیوتر با سایر کامپیوتر ها ارتباطی مجزا دارد. بنابراین ، این توپولوژی دارای بالاترین درجه امنیت واطمینان می باشد.



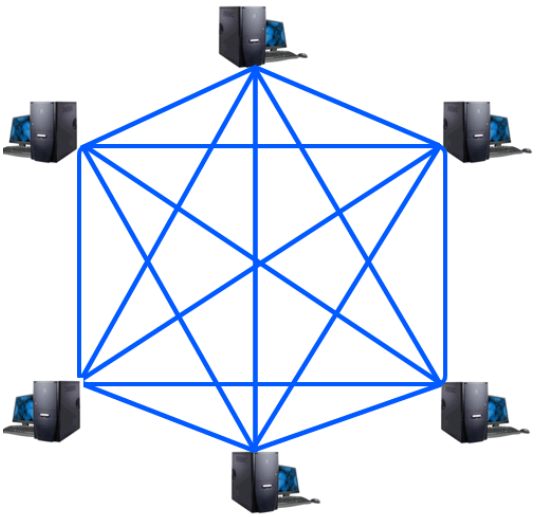
Ring



Bus



Star



Mesh

انواع کابل های شبکه :

در لایه یک ، لایه فیزیکی از مدل **OSI** ، **Device** ها باید توسط رسانه ها (کابل) بهم متصل شود. نوع رسانه مورد نیاز بستگی به نوع **Device** دارد . کابل های موجود در شبکه ، کابل های **UTP (Unshielded Twisted-pair)** از نوع **CAT5** برای شبکه های با سرعت **100mbps** و **CAT6** برای سرعت **1000mbps** می باشد. (**mbps** : مگابیت در ثانیه) این کابل از کنتاکتور **RJ-45** برای اتصال به دستگا ههای استفاده می کند .

این کابل ها که به دو صورت زیر می باشد.

۱. کابل **crossover**

کابل **crossover** جهت ارتباط دو **Device** مشابه (مانند دو کامپیوتر) از طریق پورت **Ethernet** خودکارت شبکه می باشد.

۲. کابل **straight-through**

کابل **straight-through** جهت ارتباط دو **Device** غیر مشابه (مانند کامپیوتر به سوییچ) می باشد.

IP چیست ؟

در لایه ۳ ، لایه **Network** نیاز به یک آدرس منحصر به فرد **IP Address** (کامپیوترها برای حضور در شبکه نیاز به آدرس شناسایی دارند. این آدرس **IP** یا **Internet Protocol** نامیده می‌شود) که اجازه رسیدن داده ها به دستگاه مقصد را می دهد. یک آدرس **IP** ممکن است بصورت **216.27.61.137** باشد که این صورت از مقادیر در مبنای ۱۰ نوشته می‌شود و همانطور که می‌بینید دارای سه نقطه و چهار ناحیه مختلف است. البته آدرس‌های **IP** به این صورت برای کامپیوترها قابل درک نیستند.کامپیوترها هر کدام از قسمت‌های بین دو نقطه را در مبنای دو می‌بینند. برای مثال آدرس **IP** که در بالا مشاهده کردید برای کامپیوترها به شکل **11011000.00011011.00111101.10001001** می باشد . هر کدام از قسمت‌های آدرس یک هشت‌تایی یا یک **Octet** نامیده می‌شود. هر کدام از این قسمت‌ها ۸ حالت متفاوت دارد. وقتی همه حالات را با هم جمع کنیم ۳۲ ترکیب مختلف ایجاد می‌شود. به همین دلیل هم آدرس‌های **IP** با چنین فرمتی را آدرس‌های ۳۲ بیتی می‌نامند. در مبنای دو نیز هر عدد دو حالت(۱ یا ۰) و هر قسمت از آدرس ۸ ترکیب مختلف دارد. به این ترتیب تمام ترکیب‌های هر قسمت ۲۵۶ است. حدود ۴.۳ میلیارد ترکیب مختلف از اکتت‌ها می‌توان بدست آورد. البته تمام حالات این ترکیب‌ها قابل استفاده نیستند. برای مثال **0.0.0.0** به صورت قراردادی برای پیش‌فرض شبکه و آدرس **255.255.255.255** نیز برای انتشار در شبکه **(Broadcast)** یا جهت ارسال اطلاعات برای تمامی گره های موجود در یک شبکه مورد استفاده قرار می گیرد.

Subnet Mask چیست ؟

Subnet Mask مشخص میکند که محدوده شبکه ای که کامپیوترشما در ان قرار دارد کجاست . به عنوان مثال **Subnet Mask** **255.255.255.0** شبکه ای مشتمل از ۲۵۴ کامپیوتر است ، حال اگر **Subnet** با یک **IP** همراه باشد میتوان فهمید **IP** کامپیوترهای ان شبکه در چه محدوده ای هست .مثلا **192.168.0.24** با **subnet** ، **255.255.255.0** نشان میدهد کامپیوترهای ان شبکه میتوانند **IP** هایی از محدوده **192.168.0.1** الی **192.168.0.254** داشته باشند. اولین آدرس یعنی **192.168.0.0** به عنوان **IP** آن شبکه مشخص می شود و آخرین آدرس یعنی**192.168.0.255** به عنوان **IP** ، **Broadcast** در آن شبکه می باشد. برای وارد کردن **Subnet Mask** یک **Device** باید آن را در سطر بعد از **IP** وا رد کنیم .

دستور ping چیست ؟

ping دستوری است که مشخص می‌کند که آیا یک کامپیوتر خاص که ما آدرس **IP** آن را می‌دانیم، روشن و **Active** (فعال) هست یا نه. و اینکه اگر فعال باشد مدت زمان رسیدن بسته‌های **Tcp/Ip** از آن کامپیوتر به کامپیوتر ما چقدر است. کاربرد این دستور به صورت **Ping Ip** است که به جای **Ip** باید شماره **Ip** آنرا می‌گذاریم.مثلا**ping 192.168.1.1** را در **CMD** (**command prompt**) تایپ می کنیم . طرز کار **ping** بدین صورت است که ابتدا بسته **ICMP Echo Request** (**ICMP (Internet Control Massage Protocol)** پکتی است توسط دستور **Ping** تولید می شود) را به سمت کامپیوتر مقصد ارسال می کند. اگر کامپیوتر مقابل این بسته را دریافت کند بسته ای به نامه **ICMP Echo Reply** را به سمت مبدا ارسال می کند و خبر دریافت پاکت اطلاعاتی اولیه را در مدت مشخص تعیین شده بطور خودکار می دهد. بطور پیش فرض تعداد ارسال بسته **Echo Request** چهار عدد است. به طور کلی ، سه حالت جواب ممکن است اتفاق بیفتد که عبارت است از :

1- Reply from 192.168.1.1: bytes=32 time=54ms TTL=127

این پیغام نشاندهنده این است که در مدت مشخص تعیین شده ، خبر دریافت پاکت اطلاعاتی اولیه دریافت شده و ارتباط با سیستم مقصد کاملا برقرار است .

2- Request timed out

این پیغام نشاندهنده این است که کامپیوتر شما در مدت مشخص تعیین شده ای پاسخ پاکت ارسال شده را دریافت نکرده است.

3- Destination host unreachable

این پیغام نشاندهنده این است که مسیری به کامپیوتر مقصد پیدا نشده است.

سناریو :

این آزمایشگاه با ساده ترین شکل از شبکه ، شبکه همسان (**peer-to-peer**) شروع می شود و با آزمایشگاه اتصال از طریق یک سوئیچ به پایان می رسد.

فعالیت ۱ : ایجاد یک شبکه **peer-to-peer**

مرحله ۱ – تجهیزات مورد نیاز زیر را برای آزمایش تهیه کنید.

تجهیزات مورد نیاز:

- **2 workstations**
- **2 straight through (patch) cables**
- **1 crossover cable**
- **1 switch (or hub)**

فعالیت ۲ : شناسایی کابل های مورد استفاده در شبکه.

قبل از اینکه **Device** را از طریق کابل بهم ارتباط دهید باید بدانید که با چه نوع کابلی می توان این ارتباط را برقرار کرد و نوع کابل به نوع **Device** هایی که با هم قرار است ارتباط اشته باشند نیز بستگی دارد . اما کابل های مورد استفاده در این آزمایش کابل **crossover** و کابل **straight-through** می باشد . که کابل **crossover** جهت ارتباط دو **Device** مشابه و کابل **straight-through** جهت ارتباط دو **Device** غیر مشابه می باشد.

فعالیت ۳ : شبکه **peer-to-peer** را کابل کشی کنید .

مرحله ۱ – دو **workstation** (ایستگاههای کاری: هر **End Device** در شبکه را می گویند) را بهم اتصال دهید.

از کابل **Ethernet** استفاده کنید و دو **workstation** را بهم متصل کنید . یک سر کابل را به **Port** (محلی است که داده‌ها وارد یا خارج می‌شوند) **NIC** یا **Network Interface Card** (کارت شبکه : برای استفاده از شبکه وبرقراری ارتباط بین کامپیوتر ها از کارت شبکه ای استفاده می شود که در داخل یکی از شیارهای برد اصلی کامپیوتر های شبکه بصورت سخت افزاری وبرای کنترل ارسال ودریافت داده نصب می گردد) در **PC1** و سر دیگر کابل را به به پورت **NIC** در **PC2** اتصال دهید. .

سوال ۱–۳ : از چه کابلی استفاده کنیم ؟_____

مرحله ۲ – **IP Address** و **Subnet Mask** را وارد کنید.

آدرس لایه ۳ (**IP**) هر کدام از **PC** ها را طبق **Addressing Table** جدول زیر وارد کنید . برای این کار بر روی **PC** مورد نظر کلیک کنید و به تب **Desktop** رفته و بروی **Ip Configuration** کلیک کنید و **IP Address** و **Subnet Mask** مورد نظر را وارد کنید.

فعالیت ۳ : بررسی تصدیق ارتباط بین **workstation** ها .

مرحله ۱ – با استفاده از دستور **Ping** که در **Command Prompt** در تب **Desktop** از **PC1** ، تایپ می کنید **PC2** را **Ping** کنید.

شما باید دستور زیر را تایپ کنید : **Ping 192.168.1.3**

مرحله ۲ – با استفاده از دستور **Ping** که در **Command Prompt** در تب **Desktop** از **PC2** ، تایپ می کنید **PC1** را **Ping** کنید . شما باید دستور زیر را تایپ کنید : **Ping 192.168.1.2**

سوال ۲–۳ : خروجی دستور **Ping** چیست؟

_____
_____
_____
_____

اگر دستور **Ping** ، پیغام خطا داد ویا پاسخی از **workstation** دیگر دریافت نکردید ، **Troubleshoot** (عیب یابی) ضروری می باشد .

برای **Troubleshoot** موارد زیر را بررسی کنید:

- بررسی کنید ، **IP addresses** را درست در هر دو **PC** وارد کرده اید .
- اطمینان حاصل کنید که نوع کابل صحیح را بین **PC** ها استفاده شده است .

سوال ۳- ۳ : اگر کابل شبکه را از **PC** ها جداکنید و دستور **Ping** را در یکی از **workstation** ها تایپ کنید، خروجی دستور **Ping** چیست ؟

_____
_____
_____
_____

فعالیت ۴ : **workstation** ها را به **switch** اتصال دهید.

مرحله ۱ – PC ها را به **switch** متصل کنید.

کابل متصل قبلی را با کلیک بر **Delete** ( ) و بعد کلیک بروی کابل متصل حذف و با انتخاب کابل صحیح از **NIC port** کامپیوتر ها به **switch** ارتباط برقرار کنید .

سوال ۴- ۳ : در این آزمایش از چه کابلی استفاده می کنید ؟_____

مرحله ۲ – تصدیق برقراری ارتباط .

با دستور **Ping** ارتباط بین **workstation** ها را بررسی کنید .

سوال ۵- ۳ : خروجی دستور **Ping** چیست؟

_____
_____
_____
_____

سوال ۶- ۳ : اگر شما **Ip Address** را که در این شبکه نباشد را **Ping** کنید خروجی دستور **Ping** چه می شود ؟

_____
_____
_____
_____

فعالیت ۵ : انعکاس

سوال ۷- ۳ : چه عواملی می تواند از **Ping** بین دو **workstation** زمانی که آنها را به طور مستقیم بهم وصل شده اند ، جلوگیری می کند ؟

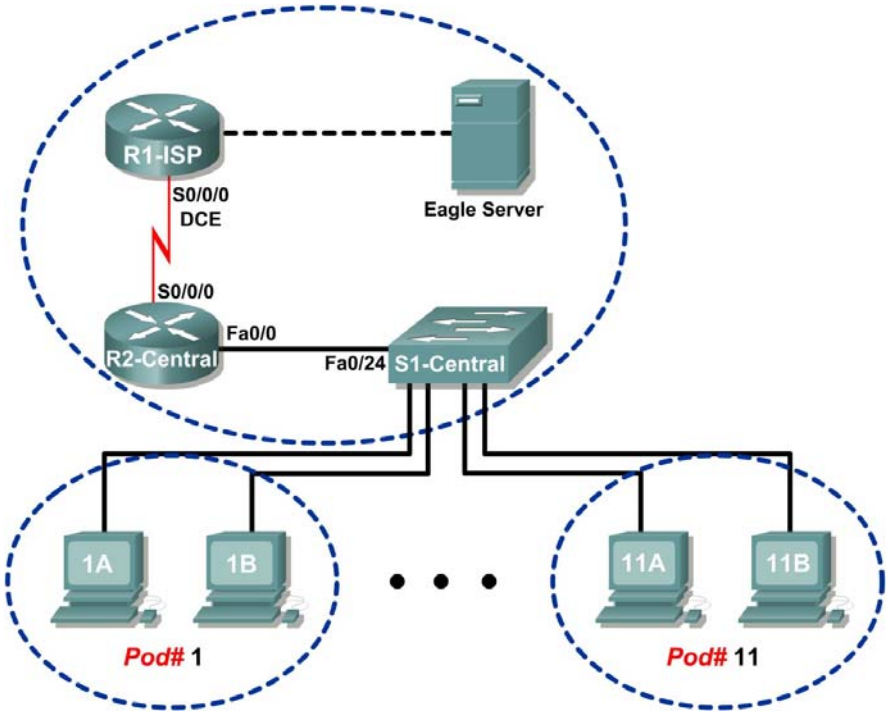
_____
_____
_____
_____

سوال ۸- ۳ : چه عواملی می تواند از **Ping** بین دو **workstation** زمانی که آنها را به وسیله **switch** بهم وصل شده اند ، جلوگیری می کند ؟

_____
_____
_____
_____

آزمایشگاه ۴-۱ : کلاس های IP و دستورات Ping و Traceroute

Topology Diagram



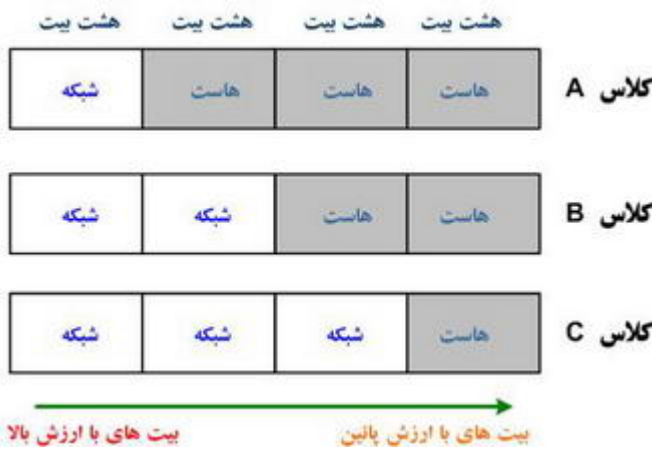
Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1-ISP	S0/0/0	10.10.10.6	255.255.255.252	N/A
	Fa0/0	192.168.254.253	255.255.255.0	N/A
R2-Central	S0/0/0	10.10.10.5	255.255.255.252	10.10.10.6
	Fa0/0	172.16.255.254	255.255.0.0	N/A
Eagle Server	N/A	192.168.254.254	255.255.255.0	192.168.254.253
	N/A	172.31.24.254	255.255.255.0	N/A
host*Pod*#A	N/A	172.16.*Pod*#.1	255.255.0.0	172.16.255.254
host*Pod*#B	N/A	172.16.*Pod*#.2	255.255.0.0	172.16.255.254
S1-Central	N/A	172.16.254.1	255.255.0.0	172.16.255.254

درس :

کلاس های IP

هر آدرس **IP** به دو قسمت **Net** و **Host** تقسیم می‌شود. قسمت **Net** بیانگر آدرس شبکه‌ای است که آدرس به آن تعلق دارد و **Host** هر آدرس در شبکه **Net** را مشخص می‌کند. ترتیب مورد استفاده برای تخصیص **Net** و **Host** به یک آدرس**IP** ، بستگی به کلاس **(Class)** آن آدرس دارد.



در کل ۵ کلاس و تعدادی آدرس **IP** ثابت وجود دارد:

- **0.0.0.0** : پیش‌فرض شبکه

- کلاس **A** : این نوع کلاس بیشتر برای تخصیص **IP** در شبکه‌های بزرگ مورد استفاده قرار می‌گیرد. اکتت اول این کلاس‌ها از ۱ تا ۱۲۶ متفاوت می‌باشد. از باقی اکتت‌ها برای **Host** استفاده می‌شود. به این ترتیب ۱۲۶ شبکه، ۱۶۷۷۷۲۱۴ هاست و ۲۱۴۷۴۸۳.۶۴۸ آدرس در کلاس **A** تعریف می‌شود. حدود نیمی از ترکیب‌های موجود برای تمام آدرس‌هایIP ، در این کلاس قرار می‌گیرند.

- **Loopback** : آدرس **127.0.0.1** برای عملیاتی به نام **Loopback** استفاده می‌شود. **Loopback** زمانی انجام می‌شود که یکی از کامپیوترهای میزبان بسته‌ای را برای خودش می‌فرستد. کاربرد این متد در رفع مشکل و تست اتصالات شبکه در خود سیستم است است.

- کلاس **B** : معمولاً شبکه‌های متوسط از این نوع کلاس بهره می‌برند. آدرس‌هایی که اولین اکتت آن‌ها از ۱۲۸ تا ۱۹۱ تغییر می‌کند عضو این کلاس هستند. اکتت دوم این آدرس‌ها نیز برای تعیین**Net** ، و دو اکتت دیگر برای مشخص کردن آدرس **Host** مورد استفاده قرار می‌گیرد. به این ترتیب ۱۶۳۴۸ شبکه با ۶۵۵۳۴ هاست و ۱۰۷۳۷۴۱۸۲۴ آدرس **IP** مختلف در این کلاس قابل تخصیص است.

• کلاس **C :** شبکه‌های کوچک می‌توانند از این کلاس استفاده کنند. آدرس‌های که اکتت اول آن‌ها از ۱۹۲ تا ۲۲۳ است در این کلاس قرار می‌گیرند. اکتت‌های اول تا سوم برای معین کردن آدرس **Net** و باقی برای تخصیص آدرس به **Host** مورد استفاده قرار می‌گیرد. می‌توان ۲۰۹۷۱۵۲ شبکه با ۲۵۴ **Host** و ۵۳۶۸۷۰۹۱۲ آدرس **IP** در کلاس **C** ایجاد کرد.

• کلاس **D :** از این کلاس برای **Mulsticast** (جهت ارسال اطلاعات برای گروهی از **Nod** های موجود در یک شبکه مورد استفاده قرار می‌گیرد) استفاده می‌شود و کمی با کلاس‌ها و آدرس‌ها قبلی تفاوت دارد. آدرس‌های که اکتت اول آن‌ها از ۲۲۴ تا ۲۳۹ است .

• کلاس **E :** این کلاس شباهتی زیادی به کلاس **D** دارد و بیشتر در موارد آزمایشی مورد استفاده قرار می‌گیرد. آدرس‌های که اکتت اول آن‌ها از ۲۴۰ تا ۲۵۴ است.

• **Broadcast :** آدرس **255.255.255.255** که برای ارسال به همه **Nod** های شبکه می باشد.

نکته : آدرس های بالا برای استفاده در اینترنت می باشد و یک سری از آدرس خصوصی از داخل کلاس های IP برای شبکه های خصوصی خارج می شود که عبارت است از :

PRIVATE IP ADDRESS		
Class A	10.0.0.0	10.255.255.255
Class B	172.16.0.0	172.31.255.255
Class C	192.168.0.0	192.168.255.255

آدرس‌هایی که بررسی کردیم دارای ۳۲ (2^4) بیت رقم بودند به همین دلیل آن‌ها را بیشتر به آدرس‌های **IPv4** می‌شناسند. در سال‌های اخیر به دلیل گسترش شبکه‌های کامپیوتری و اینترنت، نیاز به گستره جدیدی از آدرس‌های **IP** احساس شد به همین دلیل قراردادهایی برای ایجاد آدرس‌های ۱۲۸ بیتی تولید شد. این آدرس‌ها **IPv6** نامیده می‌شوند. این آدرس‌ها در مبنای ۱۶ نوشته می‌شوند . یکی دیگر از مسایلی که در ساخت **IPv6** مورد نظر بوده‌است، استفاده از بلوک‌ها بزرگ عدد برای مشخص کردن مواردی مانند مسیریابی شبکه است.

Ping و Tracert :

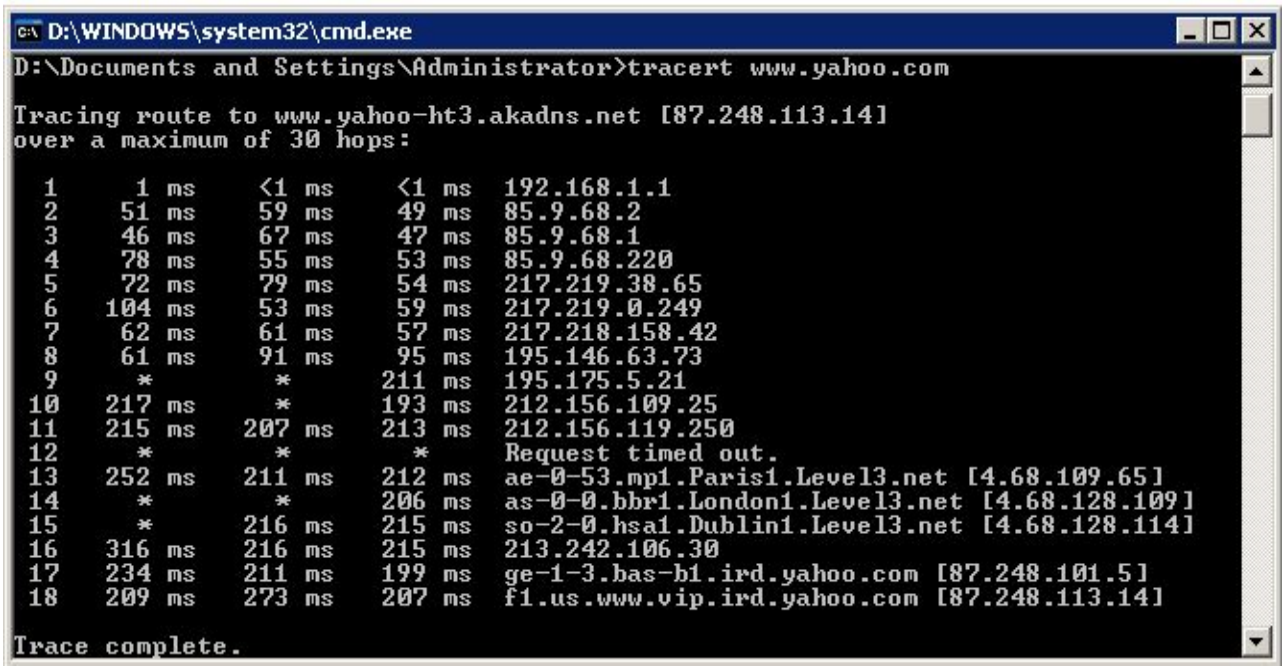
Ping و **Tracert** دو ابزار ضروری برای تست در شبکه های **TCP/IP** می باشند . ابزار های **Ping** و **Tracert** در تمام سیتم عامل ها و **Cisco IOS** (سیستم عامل **Cisco**) قابل دسترس می باشد . با دستور **Ping** در درس قبل آشنا شدید . اما دستور **Tracert** یا **Traceroute** : همانطور که از نام این ابزار پیداست از **tracert** برای پیدا کردن مسیر بین دو **Host** یا به عبارتی دو دستگاه دارای آدرس شبکه که همدیگر را می بینند استفاده می شود و این دستور از طریق پروتکل **ICMP** این عمل را انجام می دهد و آن بدین صورت است که پاکت **echo request** توسط کامپیوتر ما به دستگاه مقصد ارسال می شود و در هر مرحله ای از این مسیر پاکت **echo reply** ایجاد شده و به کامپیوتر مبدا (کامپیوتر ما) ارسال می شود. و به ما نشان می دهد فاصله بین شما تا مقصد در شبکه چقدر است و چند **hop** (مسیری است که داده در آن توسط **Router** انتقال پیدا می کند) در میان است. هر چه این اعداد و ارقام پایین تر باشد سرعت دسترسی به مقصد بیشتر است. طریقه نوشتن این دستور به این صورت است که **Tracert IP** ، مثلا **Tracert 192.168.1.250**

نحوه عملکرد دستور Tracert :

دستور فوق از فیلد **TTL** (**Time to live**) یا زمان زنده ماندن مربوط به **IP** در **ICMP Echo Request** و پیام های **ICMP Time Exceeded** به منظور تعیین مسیر مبداء تا مقصد یک بسته اطلاعاتی استفاده می نماید . عملکرد این دستور نیز مشابه **ping** است و وی نیز از پیام های مبتنی بر **ICMP** برای یافتن هر یک از دستگاه های موجود در مسیر یک بسته اطلاعاتی ، استفاده می نماید . برای تشخیص مسیر حرکت ، به **TTL** موجود در بسته اطلاعاتی یک مقدار اولیه نسبت داده می شود . **TTL** ، یک عدد صحیح است که حداکثر تعداد **hop** را که یک بسته اطلاعاتی در مسیر خود با آنان برخورد می نماید را مشخص می نماید (قبل از این که توسط **IP** ، **Drop** (دورانداخته) شود. مقدار **TTL** در ابتدا یک خواهد بود و هر روتر و دستگاه موجود در مسیر بسته اطلاعاتی ، یک واحد به آن اضافه می نماید . بدین ترتیب برنامه **tracert** قادر به دریافت پیام **ICMP Time Exceeded** از هر یک از روترها و یا سایر دستگاه های موجود در مسیر یک بسته اطلاعاتی می باشد . شکل زیر نحوه عملکرد دستور **tracert** را نشان می دهد .

خروجی دستور Tracert :

۱ – اگر مشکلی در شبکه مباشد و در صورتی که آخرین گره مشاهده شده در خروجی دستور **tracert** مقصد نهائی باشد ، تمامی گره ها و یا روترهای موجود در مسیر نمایش داده شده اند . خروجی به عنوان مثال زیر را داریم :



۲- در مواردی که در مسیر یک بسته اطلاعاتی مشکل خاصی ایجاد شود و یا پیام **ICMP Time Exceeded** برگردانده نشود ، در خروجی علامت "ستاره" نشان داده خواهد شد . در چنین مواردی یک پیام **Request timed out** در قسمت سمت راست نمایش داده می شود .

۳ - اگر به دلایلی مقصد غیر قابل دسترس بود ، زمانی که بسته اطلاعاتی **ICMP** به مقصد نهائی خود می رسد ، یک پیام **ICMP DESTINATION UNREACHABLE** توسط کامپیوتر مقصد برگردانده می شود .

سناریو :

در این آزمایشگاه ، دستورات **Ping** و **Tracert** را مورد بررسی قرار می گیرد .د ر این آزمایش شما با این دستورات آشنا می شوید . تاخیر در زمان احتمالا خیلی کم در شبکه تولید می شود .دلیل این است که ترافیک شبکه در آزمایش **Eagle 1** کم است

فعالیت ۱ : استفاده از دستور **Ping** برای تایید اتصال در شبکه **TCP/IP**

مرحله ۱ – استفاده از دستور **Ipconfig**

با استفاده از دستور **Ipconfig** در **command prompt** که در **Desktop** موجوی در یکی از **host** ها ، اتصال **Tcp/Ip** لایه شبکه را در **Host** مورد نظر ، بررسی کنید که **Tcp/Ip** درست کار می کند یا نه .

مرحله ۲ – استفاده از دستور **Ping** برای **Lan**

با استفاده از دستور **Ping** در **command prompt** در یکی از **host** ها ، اتصال **Tcp/Ip** لایه شبکه را در **Lan** مورد نظر ، بررسی کنید که **Tcp/Ip** درست کار می کند یا نه . در اینجا ما آدرس **Interface** روتر را که **172.16.255.254** است ، **Ping** می کنیم.

مرحله ۳ – استفاده از دستور **Ping** برای شبکه راه دور

با استفاده از دستور **Ping** در **command prompt** در یکی از **host** ها ، اتصال **Tcp/Ip** لایه شبکه را در شبکه راه دور (**Remote network**) مورد نظر ، بررسی کنید که **Tcp/Ip** درست کار می کند یا نه . که در اینجا ما **Eagle Server** را **Ping** می کنیم .(**ping 192.168.255.254**)

فعالیت ۲ : استفاده از دستور **Tracert** برای تایید اتصال **TCP/IP**

مرحله ۱ – استفاده از دستور **Tracert**

با استفاده از دستور **Tracert** در **command prompt** در یکی از **host** ها ، اتصال **Tcp/Ip** لایه شبکه را ، بررسی کنید . برای این کار **command prompt** را باز کرده و در آن این دستور را تایپ کنید :

tracert 192.168.254.254

فعالیت ۳: برسی بسته **ICMP** با دستور **Ping**

مرحله ۱ – تولید پکت **ICMP** با استفاده از دستور **Ping**

به حالت **Simulation** وارد شوید ، در **command prompt** یکی از **Host** ها دستور زیر را تایپ کنید و تولید پکت **ICMP** را مشاهده کرده و آن را در شبکه با زدن هر بار دکمه **Capture/Forward** دنبال کنید و عملکرد دستور **ping** را مشاهده کنید.

ping 192.168.254.254

فعالیت ۴: برسی بسته **ICMP** با دستور **tracert**

مرحله ۱ – تولید پکت **ICMP** با استفاده از دستور **Tracert**

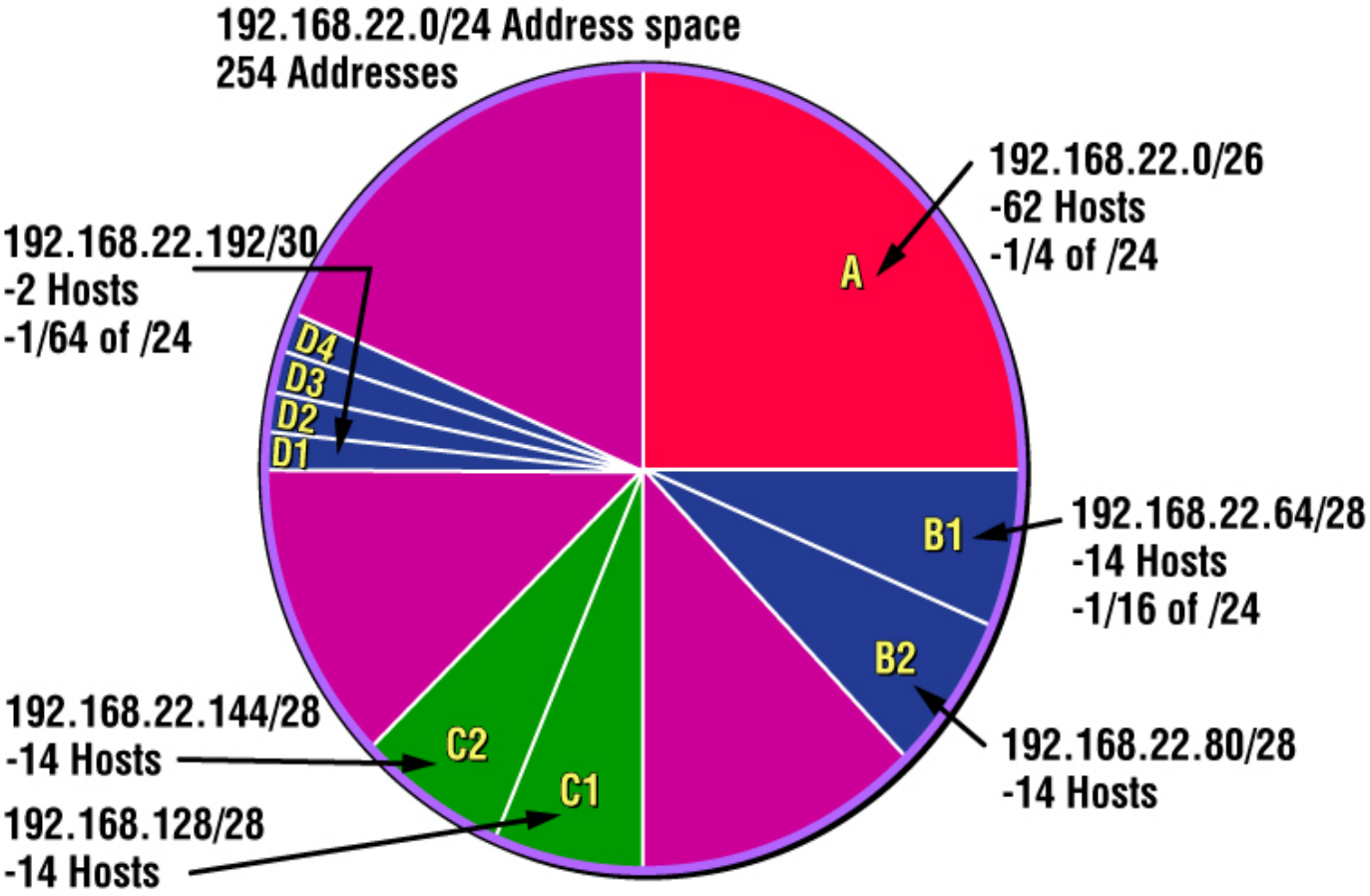
به حالت **Simulation** وارد شوید ، در **command prompt** یکی از **Host** ها دستور زیر را تایپ کنید و تولید پکت **ICMP** را مشاهده کرده و آن را در شبکه با زدن هر بار دکمه **Capture/Forward** دنبال کنید و عملکرد دستور **Tracert** را مشاهده کنید.

tracert 192.168.254.254

فعالیت ۵: انعکاس

مرحله ۱ – خروجی دستور **Tracert** را با **Ping** را مقایسه کنید .

آزمایش ۵ : آدرس IPv4 Subnetting



درس :

Subnetting چیست؟

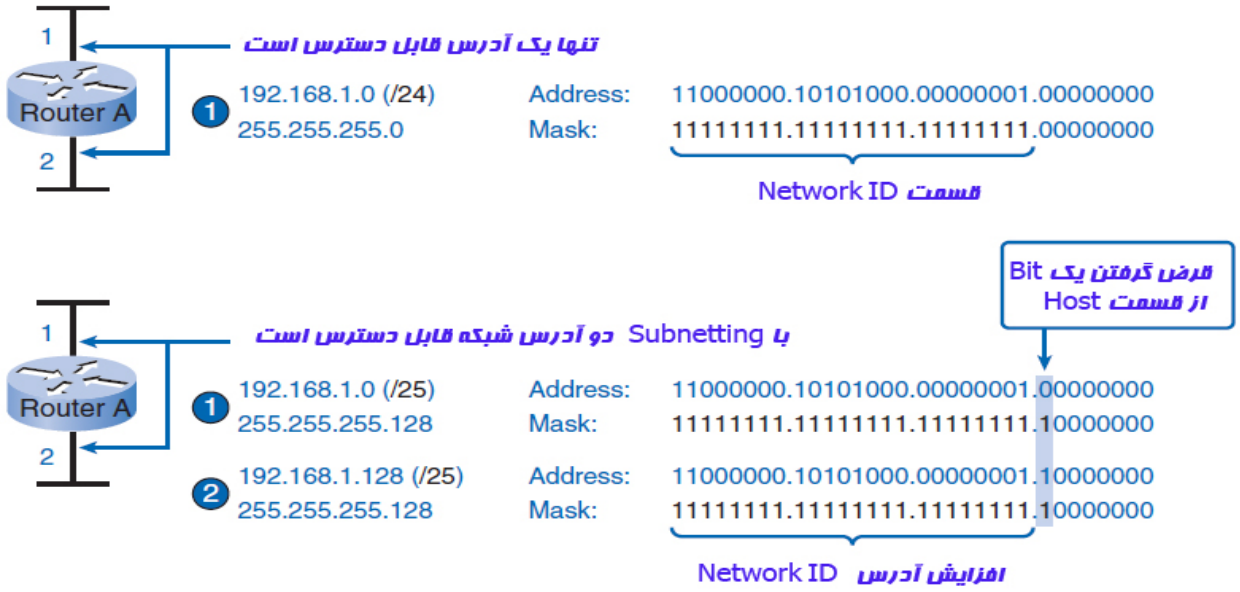
در یک سازمان جدا کردن بخشی از شبکه مثل بخش مالی یک شبکه برای حفظ امنیت از یک سو و از سوی دیگر نیاز به استفاده بهینه از **IP** برای اختصاص دادن به نودهای (**Node**) شبکه نیاز به استفاده از **Subnetting** را پی ریزی کرد. **IP Address** دارای دو بخش **Network ID** و **Host ID** می باشد. به عمل قرض دادن بیتهای (**bit**) **Net ID** به **Host ID** در اصطلاح **Subnetting** می گویند. در واقع عمل **Subnetting** بر روی **Host Address** صورت می گیرد. بیتهای **Network ID** همه یک می باشد و بیتهای **host ID** می تواند صفر یا یک باشند . در حقیقت با تغییر در این بیتها،**IP Address** های مختلف ساخته می شود. برای مثال، در آدرس (**11111111.11111111.11111111.00000000**)۲۴ بیت اول جزء **Network ID** هستند و ۸ بیت آخر جزء **Host ID** می باشد. به عبارتی این **Range** می تواند یک سگمنت (**Subnet**) با حداکثر تعداد ۲-۲۸ باشد. (هشت بیت که هر کدام ۲ حالت دارد و ۲ عدد از **IP Address** ها را نمی توان به **Node** اختصاص داد که یکی **Network Address** و دیگری **Broadcast Address** می باشد) .توجه داشته باشید که در هر بار عمل **Subnetting** دو عدد از **IP** ها غیرقابل استفاده می شوند و این به آن دلیل است که هر کدام از زیرشبکه ها دارای یک **Network Address** و یک **Broadcast Address** جدا می شوند و همانطور که گفته شد این دو عددIP غیر قابل اختصاص هستند. و همچنین توجه داشته باشید برای اتصال زیرشبکه ها به یکدیگر از یک روتر بهره ببرید.

(**C**lassless **I**nter-**D**omain **R**outing) **CIDR**

در این روش از نشانه (**/**)**slash** برای **Subnetting Mask** استفاده می شود و به معنای این است که چه مقدار از بیت ها یک است . بدیهی است که بیشترین**/32** است زیرا یک **byte** است . اما بخاطر داشته باشید که بیشترین **subnet mask** میتواند باشد **/30** است زیرا شما باید حداقل دو **bits** برای **host bits** نگه دارید. بطور مثال در کلاس **A** ، **subnet mask 255.0.0.0** است این بدین معنی است که اولین **byte** از **subnet mask** همگی یک است (**11111111**) وقتی استناد به علامت **slash** کنیم بطور مسلم **255.0.0.0** است **/8** زیرا این هشت **bits** دارد .

همچنین در کلاس **B** ، **defulf subnet mask 255.255.0.0** (**1111111.1111111.00000000.00000000**) است و همجنین میتوانیم تعریف کنیم ۱۶/ زیرا ۱۶ بیت یک است .

ساختن دو Subnet :



ما در این جا در دو طرف **Router** دو **interface** (رابط نقطه تعامل بین دو سیستم و یا گروه های کاری) دارد که به دو شبکه متصل است . ما یک آدرس **192.168.1.0 /24** داریم و می خواهیم دو **subnet** از آن درست کنیم . همانطور که ذکر شد فرمت یک **IP** در کلاس **C** به شکل **11111111.11111111.11111111.00000000** میباشد **Subnet Mask** نشان دهنده ارزش تعداد بیتهای جزء **Network ID** یک کلاس می باشد. در کلاس بالا **Subnet mask** برابر با **255.255.255.0** می باشد. حالا برای تغییر این کلاس به ۲ زیرشبکه یکی از بیتهای **Host ID** را یک می کنید تا **IP** به شکل **11111111.11111111.11111111.10000000** تبدیل شود. حالا ۲۵ بیت اول را جزء **Network ID** می گیریم و ۷ بیت آخر را جزء **host ID** که با این تعریف **Subnetting** در **IP** جدید برابر با **255.255.255.128** می باشد که می تواند ۲ الی ۲۷ **nod** را آدرس دهی کند. شما در شکل زیر می تولنید این دو **Subnetting** را مشاهده کنید. که یکی عبارت است از **192.168.1.0 /25** و دیگری **192.168.1.128 /25** می باشد.۰ حال با اختصاص یکی از **Range** ها به Subnet اول و اختصاص **Range** دیگر به **Subnet** دوم شبکه مذکور در هر **Subnet** ، ۲ الی ۲۷ آدرس خواهیم داشت.

Subnet	Network Address	Host Range	Broadcast Address
1	192.168.1.0/25	192.168.1.1–192.168.1.126	192.168.1.127
2	192.168.1.128/25	192.168.1.129–192.168.1.254	192.168.1.255

ساختن سه Subnet :

ما در این جا. یک آدرس **192.168.1.0 /24** داریم و می خواهیم سه **subnet** از آن درست کنیم . این مثال شبیه مثال قبل می باشد که با این تفاوت دو تا **Bit** از **Host** قرض گرفته می شود و به صورت زیر می شود . اگر دقت کنید خواهید فهمید که چهار **subnet** تولید شده است و یکی از آنها در این مثال استفاده نمی شود . علت یک **subnet** اضافی 2^2 که چهار می شود و باز به این نکته باید توجه داشته باشد که در هر **subnet** دوآدر س از **Host Range** کم می شود یکی برای **Network Address** و دیگری برای **Broadcast Address** می باشد.

Subnet	Network Address	Host Range	Broadcast Address
0	192.168.1.0/26	192.168.1.1–192.168.1.62	192.168.1.63
1	192.168.1.64/26	192.168.1.65–192.168.1.126	192.168.1.127
2	192.168.1.128/26	192.168.1.129–192.168.1.190	192.168.1.191
3	192.168.1.192/26	192.168.1.193–192.168.1.254	192.168.1.255

سناریو :

زمانی که به شما **IP address** و **network mask** و **subnetwork mask** را بدهند . شما این توانایی را دارید که اطلاعاتی **IP address** را را تعیین کنید . این اطلاعات عبارت است از :

- **Network address**
- **Network broadcast address**
- **Total number of host bits**
- **Number of hosts**
- **The subnet address of this subnet**
- **The broadcast address of this subnet**
- **The range of host addresses for this subnet**
- **The maximum number of subnets for this subnet mask**
- **The number of hosts for each subnet**
- **The number of subnet bits**
- **The number of this subnet**

فعالیت ۱ : برای **IP address** داده شده ، اطلاعات خواسته شده شبکه آن را تعیین کنید .

با توجه به :

Host IP Address	**172.25.114.250**
Network Mask	**255.255.0.0 (/16)**

اطلاعات زیر را پیدا کنید :

Network Address	
Network Broadcast Address	
Total Number of Host Bits	
Number of Hosts	

مرحله ۱ – **Host IP address** و **network mask** به **Binary** تبدیل کنید .

	172	25	114	250
IP Address	10101100	11001000	01110010	11111010
Network Mask	11111111	11111111	00000000	00000000
	255	255	0	0

مرحله ۲ – تعیین **network address**

۱ . زیر **Mask** یک خط بکشید .

۲ . **IP Address** و **Network Mask** را باهم جمع منطقی کنید . در جمع منطقی ۱ و ۱ ، یک می شود و صفر با هر چیزی صفر می شود .

1 AND 1 = 1 , 0 AND 0 (or) 1 = 0

۳ . نتیجه **Network Address** برای این **Host** ، **172.25.0.0** می شود.

	172	25	114	250
IP Address	10101100	11001000	01110010	11111010
Subnet Mask	11111111	11111111	00000000	00000000
Network Address	10101100	11001000	00000000	00000000
	172	25	0	0

مرحله ۳– **Broadcast Address** برای **Network Address** تعیین کنید .

Mask جدا کننده قسمت **Network** از **Host** می باشد . **Broadcast Address** شبیه **Network Address** فقط با این تفاوت که در قسمت **Host** هر کجا **Network Add** صفر است ، **Broadcast** یک می باشد .

	172	25	114	250
IP Address	10101100	11001000	01110010	11111010
Subnet Mask	11111111	11111111	00000000	00000000
Network Address	10101100	11001000	00000000	00000000
	172	25	0	0

با شمارش تعداد بیت های **host**، ما می توانیم تعداد کل **Host** ها را برای این شبکه مشخص کنیم.

Host bits: 16 , Total number of hosts: 216 = 65,536

65,536 – 2 = 65,534 (آدرس های **Network** و **Broadcast** کم می شود)

سوال ۱– ۵ : بااطلاعات فوق جدول زیر را پر کنید :

Host IP Address	**172.25.114.250**
Network Mask	**255.255.0.0 (/16)**
Network Address	
Network Broadcast Address	
Total Number of Host Bits **Number of Hosts**	

فعالیت ۲ : با داشتن **IP Address** و **Subnet Mask**، اطلاعات **Subnet** را تعیین کنید .

با توجه به :

Host IP Address	**172.25.114.250**
Network Mask	**255.255.0.0 (/16)**
Subnet Mask	**255.255.255.192 (/26)**

سوال ۲– ۵ : اطلاعات زیر را پیدا کنید :

Number of Subnet Bits	
Number of Subnets	
Number of Host Bits per Subnet	
Number of Usable Hosts per Subnet	
Subnet Address for this IP Address	
IP Address of First Host on this Subnet	
IP Address of Last Host on this Subnet	
Broadcast Address for this Subnet	

مرحله ۱ : **Host IP address** و **network mask** به **Binary** تبدیل کنید .

	172	**25**	**114**	**250**
IP Address	**10101100**	**11001000**	**01110010**	**11111010**
	11111111	**11111111**	**11111111**	**11000000**
Subnet Mask	**255**	**255**	**255**	**192**

مرحله ۲ : آدرس شبکه یا **Subnet** که به این **host address** تعلق دارد را تعین کنید .

۱ . زیر **Mask** یک خط بکشید .

۲ . **IP Address** و **Subnet Mask** را باهم جمع منطقی کنید . در جمع منطقی ۱ و ۱ ، یک می شود و صفر با هر چیزی صفر می شود .

1 AND 1 = 1 , 0 AND 0 (or) 1 = 0

۳ . نتیجه **Subnet Address** برای این **Subnet** ، **172.25.114.192** می شود.

	172	**25**	**114**	**250**
IP Address	**10101100**	**11001000**	**01110010**	**11111010**
Subnet Mask	**11111111**	**11111111**	**11111111**	**11000000**
Subnet Address	**10101100**	**11001000**	**01110010**	**11000000**
	172	**25**	**114**	**192**

این اطلاعات را به جدول اضافه کنید:

Subnet Address for this IP Address	172.25.114.192

مرحله ۳ : مشخص است که کدام بیت دراین آدرس مربوط به **Network ID** و کدام مربوط به **Host ID** می باشد.

۱. با یک خط موج دار (***Major Divide*** (**M.D.**)) که جدا کننده اصلی یک های **Network Mask** که در مثال ما **255.255.0.0** می باشد ، جدا کنید .

۲. با یک خط صاف (***Subnet Divide*** (**S.D.**)) که جدا کننده ***Subnet*** یک های ***Subnet Mask*** جدا کنید .

			M.D.	S.D.	
IP Address	10101110	11001000	01110010	11	111010
Subnet Mask	11111111	11111111	11111111	11	000000
Subnet Add.	10001010	11001000	01110010	11	000000
			← 10 bits →		

۳. نتیجه بیت های **Subnet** را مشخص می کند که از شمارش بیت های بین **M.D.** و **S.D.** بدست می آید . در این جا ۱۰ بیت می باشد.

مرحله ۴- تعیین محدوده های بیت برای **subnet** ها و **Host**

۱. محدوده **subnet** عبارت است از بیت های بین **M.D.** و **S.D.** که برای ایجاد آدرس **Subnet** ، این محدوده شامل بیت است که در حال افزایش میابد.

۲. محدوده **Host** ها عبارت است از بیت های بین **S.D.** و آخرین بیت که برای ایجاد آدرس **Host** ها ، این محدوده شامل بیت است که در حال افزایش میابد.

			M.D.	S.D.	
IP Address	10101110	11001000	01110010	11	111010
Subnet Mask	11111111	11111111	11111111	11	000000
Subnet Add.	10001010	11001000	01110010	11	000000
			← subnet counting range →		←host→ counting range

مرحله ۵ - تعیین محدوده از آدرس **Host** ها قابل دسترس در این **subnet** و آدرس **broadcast** دراین **subnet**

۱. برای بدست آوردن اولین **Host** در هر **subnet** باید همه بیت های **Ip Address** تا خط **S.D.** را نوشته و از آنجا به بعد اولین شماره را که در اینجا **000001** می باشد به آن اضافه کرد که در این صورت اولین **Host** می شود : **172.25.114.193**

۲. برای بدست آوردن آخرین **Host** در هر **subnet** باید همه بیت های **Ip Address** تا خط **S.D.** را نوشته و از آنجا به بعد آخرین شماره منهای یک را که در اینجا **111110** می باشد به آن اضافه کرد که در این صورت آخرین **Host** می شود : **172.25.114.254**

۳. برای بدست آوردن **Broadcast Address** در هر **subnet** باید همه بیت های **Ip Address** تا خط **S.D.** را نوشته و از آنجا به بعد همه بیت ها را یک کرد که در اینجا **111111** می باشد به آن اضافه کرد که در این صورت **Broadcast Address** می شود : **172.25.114.255**

		M.D.	S.D.		
IP Address	10101100	11001000	01110010	11	111010
Subnet Mask	11111111	11111111	11111111	11	000000
Subnet Add.	10101100	11001000	01110010	11	000000
			← **subnet →** **counting range**		← **host →** **counting range**
First Host	10101100	11001000	01110010	11	000001
	172	25	114		193
Last Host	10101100	11001000	01110010	11	111110
	172	25	114		254
Broadcast	10101100	11001000	01110010	11	111111
	172	25	114		255

اطلاعات فوق را به جدول اضافه می کنیم:

Host IP Address	**172.25.114.250**
Major Network Mask	**255.255.0.0 (/16)**
Major (Base) Network Address	**172.25.0.0**
Major Network Broadcast Address	**172.25.255.255**
Total Number of Host Bits **Number of Hosts**	**16 bits or 2^{16} or 65,536 total hosts** **65,536 – 2 = 65,534 usable hosts**
Subnet Mask	**255.255.255.192 (/26)**
Number of Subnet Bits **Number of Subnets**	
Number of Host Bits per Subnet **Number of Usable Hosts per Subnet**	
Subnet Address for this IP Address	
IP Address of First Host on this Subnet	
IP Address of Last Host on this Subnet	
Broadcast Address for this Subnet	

مرحله ۶ – تعیین تعداد **subnet** ها

تعداد **subnet** ها با استفاده تعداد بیت های محدوده **subnet** مشخص می شود که در اینجا ۱۰ بیت می باشد که شما می توانید آن را در فرمول زیر بگذارید : 2^n $2^{10} = 1024$

Number of Subnet Bits	**10 bits**
Number of Subnets **(all 0s used, all 1s not used)**	**2^{10} = 1024 subnets**

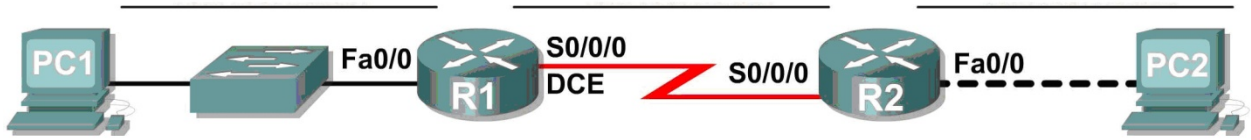
مرحله ۷ – تعیین تعداد **Host** قابل استفاده در **subnet**

تعداد **Host** ها با استفاده تعداد بیت های محدوده **Host** مشخص می شود که در اینجا ۶ بیت می باشد که شما می توانید آن را در فرمول زیر بگذارید : 2^m- 2 **2^6 – 2 = 64 – 2 = 62 hosts per subnet**

Number of Host Bits per Subnet	**6 bits**
Number of Usable Hosts per Subnet	**2^6 – 2 = 64 – 2 = 62 hosts per subnet**

آزمایشگاه ۶- ۱ : تقسیم بندی شبکه و Subnetting و Configuration Router

Topology Diagram



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	Fa0/0			N/A
	S0/0/0			N/A
R2	Fa0/0			N/A
	S0/0/0			N/A
PC1	NIC			
PC2	NIC			

درس :

تقسیم بندی شبکه از نظر ابعاد :

- **Lan** (شبکه محلی) چیست ؟

که مخفف **Local Aria Network** میباشد ، شبکه ای است با سرعت بالا که به منظور برقراری ارتباط و مبادله داده ها بین کامپیوترها در یک محدوده جغرافیایی کوچک مثل یک اداره ، یک ساختمان و یا یک طبقه از یک برج طراحی شده است .

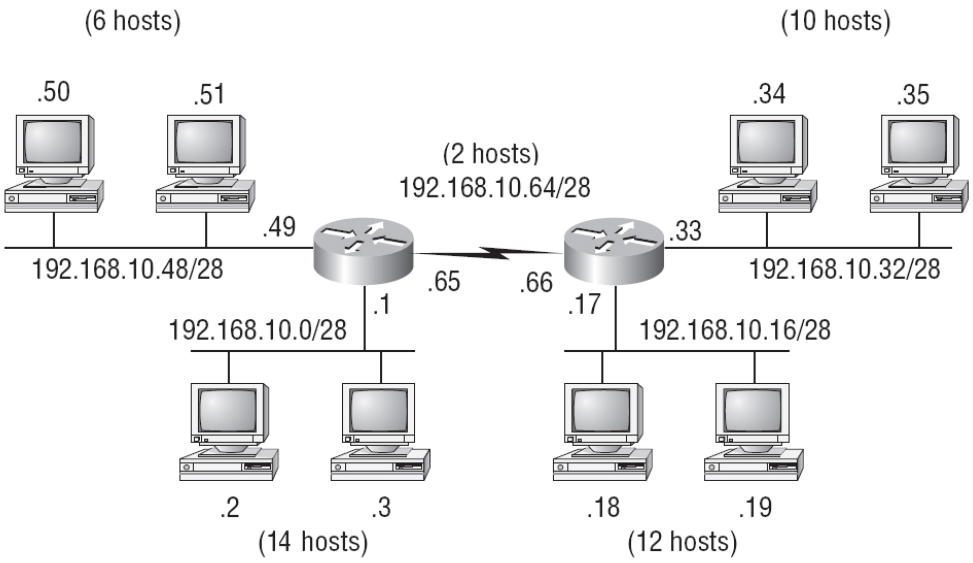
- **Wan** (شبکه بندی وسیع) چیست ؟

که مخفف **Wide Aria Network** میباشد ، جهت مبادله اطلاعات بین فواصل بسیار دور بکار میرود .این شبکه ناحیه جغرافیایی وسیعی مانند کل یک کشور و یا کل یک قاره را در بر میگیرد .شبکه های **WAN** ممکن است از خطوط استیجاری شرکت مخابرات و یا ماهواره های مخابراتی جهت مبادله اطلاعات استفاده کنند.

تخصیص Network Address و Subnet Mask به شبکه

مراحل تخصیص **Ip Address** و **Subnet Mask** به شبکه با یک مثال توضیح می دهیم :

ما یک شبکه با آدرس **192.168.10.0/24** داریم و طبق شکل زیر می خواهیم آن را به **Subnet 1** دارای شش **Host** و **Subnet 2** دارای چهارده **Host** و **Subnet 3** دارای دوازده **Host** و **Subnet 4** دارای ده **Host** و یک لینک بین دو **Router** که دارای دو **Host** است که **Subnet 5** نام دارد ، تقسیم کنیم .



مراحل زیر را انجام می دهیم :

۱- می آییم **Subnet** ها را از بیشترین **Host** مرتب می کنیم مثلا در این مثال **Subnet 2** دارای **15 Host** و **Subnet 3** دارای **12 Host** و **Subnet 4** دارای **10 Host** و **Subnet 1** دارای **6 Host** و **Subnet5** که دارای دو **Host** ترتیب این شبکه می باشد .

۲- بررسی می کنیم عدد بیشترین **Host** به علاوه دو (**Network Address** و **Broadcast Address**) با کدام 2^n مساوی و یا کوچکترین در کمترین فاصله است ($2^1=2$ و $2^2=4$و $2^3=8$ و $2^4=16$ و $2^5=32$ و $2^6=64$ و $2^7=128$ و $2^8=256$ و $2^9=512$ و $2^{10}=1024$) در مثال فوق بیشترین **Host**، ۱۵ است که به ۱۶ نزدیک است که می شود 2^4

۳- عدد **n** بدست آمده تعداد بیت های **Host** را نشان می دهد که باید از کل یعنی ۳۲ کم شود تا **Subnet Mask** شبکه را بدهد در مثال فوق ۲۸= ۴-۳۲ پس **Subnet Mask** می شود : **255.255.255.240**

۴- با بدست آمدن **Subnet Mask** ، تعداد **Host** ها در هر **Subnet** مشخص میشود و پس می توانیم **Network Address** هر **Subnet** را مشخص کنیم . در مثال فوق **Network Address** عبارت است از **192.168.10.0/28** که ۱۶ تا ۱۶ تا برای هر **Subnet** زیاد می شود .

Network Address :

Subnet 2 : 192.168.10.0/28
Subnet 3 : 192.168.10.16/28
Subnet 4 : 192.168.10.32/28
Subnet 1 : 192.168.10.48/28
Subnet 5 : 192.168.10.64/28

در کل آدرسهای **IP** به سه دسته تقسیم می شوند :

۱) اولین **IP Address** هر زیردامنه را **Network Address** می نامند.

این **IP** را نمی توان به هیچ یک از **node** (نودهای) شبکه اختصاص داد.

۲) **Broadcast Address**: آخرین **IP Address** هر زیردامنه را **Broadcast Address** می نامند. این **IP** تنها در مواقعی استفاده می شود که قصد ارسال **Data** به تمام نودهای شبکه را داشته باشیم.

۳) **Host Address** : تمام آدرسهایی (**IP Address**) را که می توان به نودهای شبکه اختصاص داد، **Host Address** می گویند.

Configuration (تنظیمات) Router :

از روترها برای اتصال شبکه ها و مسیریابی بسته های اطلاعاتی از یک شبکه به شبکه دیگر استفاده می گردد . روترها به صورت پیش فرض باعث تفکیک Broadcast Domain می گردند . به مجموعه ای از دستگاه های موجود بر روی یک شبکه که به Broadcast ارسالی بر روی سگمنت (Subnet یا Domain) گوش می دهند ، Broadcast Domain گفته می شود . تفکیک Broadcast Domain در یک شبکه بسیار حائز اهمیت است چراکه پس از ارسال Broadcast توسط یک Host و یا سرویس دهنده ، هر دستگاه موجود در شبکه می بایست آن را دریافت و پردازش نماید . در صورت استفاده از روتر ، زمانی که Interface آن یک Broadcast را دریافت می نماید ، می تواند آن را بدون نیاز Forwarding به شبکه دیگر ، دور بیاندازد . با این که روترها به صورت پیش فرض به عنوان دستگاه هائی جهت تفکیک Broadcast Domain مطرح و شناخته شده می باشند ولی لازم است به این نکته مهم نیز توجه گردد که روترها قادر به تفکیک Collision Domains نیز می باشند . (در صورت بروز یک تصادم (Collision) بین دو پکت ، سایر کامپیوترهای موجود در Domain آن را شنیده و آگاهی لازم در خصوص آن چیزی که اتفاق افتاده است را پیدا خواهند کرد . کامپیوترهای فوق عضوء یک Collision Domain یکسان می باشند.)

تفاوت Device ها از نظر Collision Domain و Broadcast Domain :

Hub به همراه تمام پورت هایش و اجزاء متصل به خودش در یک Collision Domain و Broadcast Domain قرار دارد.

در سوئیچ به ازای هر پورت یک Collision Domain وجود دارد و تمام پورت های آن نیز در یک Broadcast Domain وجود دارد.

در روتر به ازای تک تک پورت هایش Collision Domain و Broadcast Domain وجود دارد.

Interface های روتر:

روتر از طریق Interface به شبکه های پیرامون وصل میشود. یکی از این درگاهها Ethernet و FastEthernet است. شبکه LANی که اغلب همه جا در دسترس است از این درگاهها بهره میبرد. کافیست کابل شبکه را به پورت RJ45 وصل کرده و آن Interface را درون روتر فعال کنیم. یکی دیگر Serial Interface است که برای اتصال به شبکه های Wan از قبیل Point to Point (نقطه به نقطه) مخابراتی و Leased Line (خطوط استیجاری) استفاده میشود یا مثلا برای اتصال ADSL از ATM Interface استفاده میکنیم. روتر در زمان بوت شدن Interface ها را شناسایی و در داخل فایل تنظیمات (Configuration) نمایش میدهد. همانطور که اشاره کردیم Interface, روتر را به شبکه های پیرامون وصل میکند. روتر بدون Interface قادر نیست به هیچ شبکه ای وصل شود. Interface ها در روتر های Fixed روی روتر قراردارند و در روترهای Modular (ماژولار) توسط ماژول یا Interface Card به روتر وصل میشوند.

Serial و FastEthernet در روتر چیست ؟

این دو ، دو Interface بروی روتر می باشد که Serial برای اتصال Wan به روتر می باشد که از کابل Serial برای اتصال به آن استفاده می شود و FastEthernet با سرعت 100 Mbps برای اتصال Lan به روتر استفاده می شود .

سناریو :

در این آزمایش ، شما طراحی و به کار بردن آدرس دهی **IP** را برای یک توپولوژی خاص را می آموزید . شما یک بلوک آدرس خواهید داشت که باید آن را با **Subnet Mask** برای **Subnet**ها تامین کنید . بعد از آن **Interface** های **Router** را **Configure** کنید. و عملکرد شبکه را بررسی کنید .

فعالیت ۱ : **Subnet** کردن فضای **Address**

مرحله ۱ : الزامات شبکه تعیین کنید.

برای استفاده در طراحی شبکه ، به شما آدرس **192.168.1.0/24** داده شده است .

شبکه متشکل از بخش های زیر است :

- شبکه ای که متصل به روتر **R1** است نیاز به **IP addresses** برای **15 Host**دارد.
- شبکه ای که متصل به روتر **R2** است نیاز به **IP addresses** برای **30 Host**دارد.
- ارتباط بین روتر **R1** و روتر **R2** ، نیاز به **IP addresses** برای هر انتهای لینک دارد.

مرحله ۲ : سوالات زیر در هنگام طراحی شبکه در نظر بگیرید.

سوال ۱- ۶ : چند **subnet** برای این شبکه نیاز است؟ _____

سوال ۲- ۶ : **subnet mask** برای این شبکه در قالب **Dotted Decimal** چیست؟_____

سوال ۳- ۶ : **subnet mask** برای شبکه در قالب **Slash (CIDR)** چیست؟_____

سوال ۴- ۶ : چند **Host** در هر **subnet** وجود دارد ؟ _____

مرحله ۳ : اختصاص آدرس **subnetwork** به **Topology Diagram**.

۱. اختصاص **subnet 1** به شبکه متصل به **R1**.

۲. اختصاص **subnet 2** به لینک بین **R1** و **R2** .

۳. اختصاص **subnet 3** به شبکه متصل به **R2**.

فعالیت ۲ : تعیین آدرس های **Interface** ها .

مرحله ۱ : اختصاص مناسب آدرس به **Interface** های **device** ها .

۱. انتساب اولین آدرس **Host** در **subnet 1** به **Lan Interface** در **R1**.

۲. انتساب آخرین آدرس **Host** در **subnet 1** به **PC1**.

۳. انتساب اولین آدرس **Host** در **subnet 2** به **WAN Interface** در **R1**.

۴. انتساب آخرین آدرس **Host** در **subnet 2** به **WAN Interface** در **R2**.

۵. انتساب اولین آدرس **Host** در **subnet 3** به **Lan Interface** در **R2**.

۶. انتساب آخرین آدرس **Host** در **subnet 3** به **PC2**.

مرحله ۲ : آدرس بدست آمده را در جد ول **Topology Diagram** بنویسید .

فعالیت ۳ : **Configure** (پیکربندی) آدرس های **Serial** و **FastEthernet** .

مرحله ۱ : پیکربندی **Interface** های روتر .

Interface های روتر ها را با **IP addresses** بدست آمده از طراحی شیکه پیکربندی کنید .برای این کار بروی روتر مورد نظر رفته و کلیک کنید و به **Config Tab** رفته و با انتخاب **Interface** های **Serial** و **FastEthernet** آدرس هارا وارد کنید . لطفا توجه داشته باشید هنگامی که کار شما به پایان رسید ، حتما **configuration** انجام شده را در **NVRAM** (حافظه روتر که با قطع برق پاک نمی شود) کنید. برای این کار در **Config Tab** روتر بروی **Global Settings** دکمه **Save** را بزنید.

مرحله ۲ : پیکربندی **Interface** های کامپیوتر ها .

configure کنید **Ethernet interfaces** های **PC1** و **PC2** با **IP addresses** و **gateway default** که از طراحی خود بدست آورده اید .

فعالیت ۴ : بررسی **Configuration** ها .

به سوالات زیر جواب دهید تا متوجه شوید که شبکه به آن صورتی که انتظار می رود کار می کند.

سوال ۵- ۶ : از host متصل به R1 ، امکان ping به default gateway است ؟_____

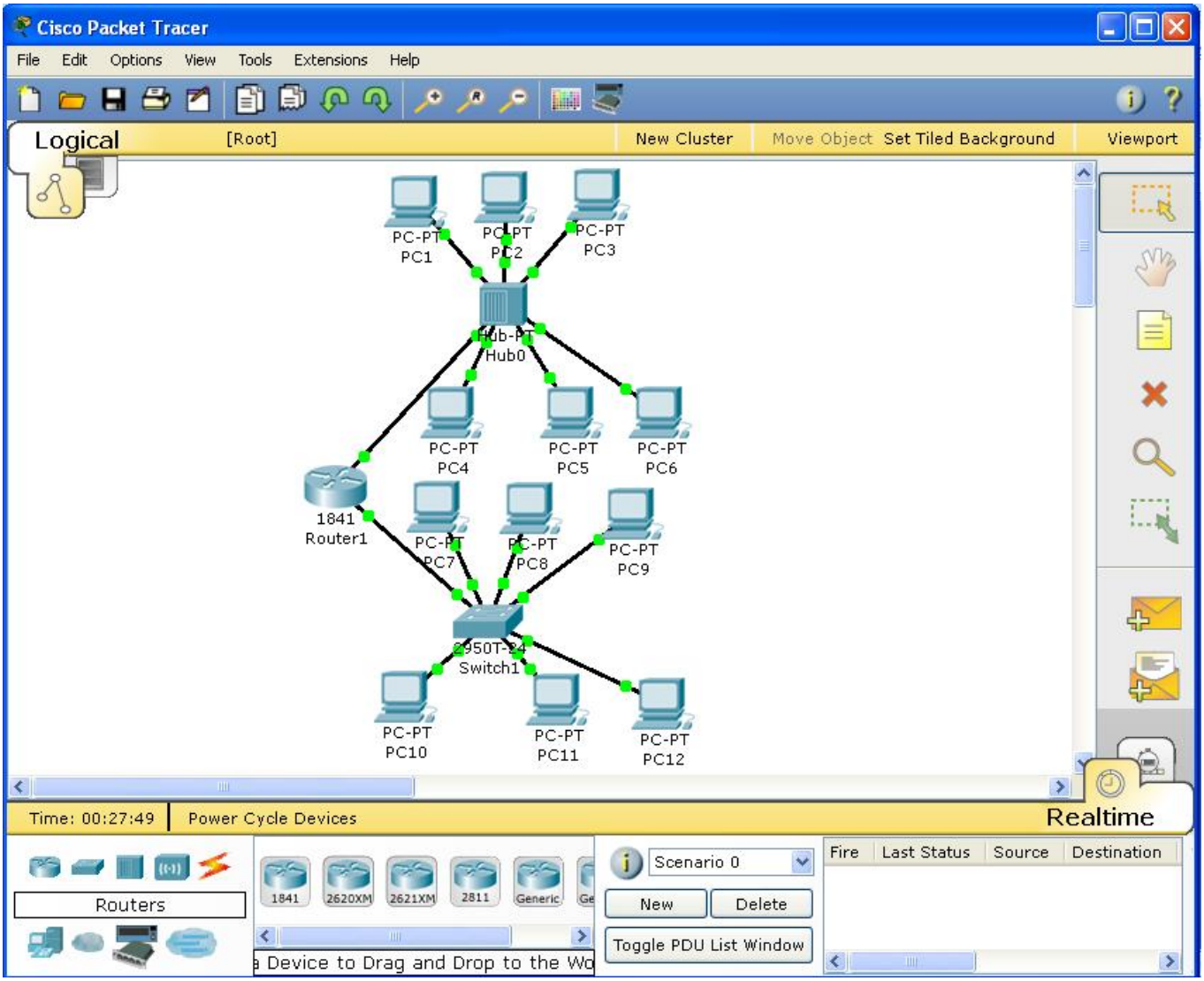
سوال ۶- ۶ : از host متصل به R2 ، امکان ping به default gateway است ؟_____

فعالیت ۵ : انعکاس

آیا device هایی در شبکه است که نمی تواند همدیگر را ping کنند ، اگر هست علت را پیدا کنید ؟

آزمایشگاه ۷-۱ : تفاوت های Hub و Switch

Topology Diagram



درس :

تفاوت های بین هاب و سوئیچ :

هاب و سوئیچ در اصل عملکرد یکسانی را انجام می دهند ، اگرچه روشهای انجام کار آنها متفاوت می باشد. از هر دو آنها در جهت احیای سیگنالهای ضعیف شده استفاده می شود ، همچنین هر دو آنها توانایی تقسیم و جداسازی یک سیگنال به چند سیگنال را نیز دارا می باشند.

هاب چیست ؟

هاب در مدل **OSI** در لایه فیزیکی عمل می کند. زمانیکه هاب از یک پورت اطلاعات را دریافت می کند، سپس اطلاعات آن اطلاعات را به همه پورتها پخش می کند. این عملکرد در هاب باعث هدر رفتن پهنای باند و ایجاد تداخل می شود. تصور کنید که دو کامپیوتر به صورت همزمان اقدام به ارسال اطلاعات کنند ، بسته های اطلاعات با یکدیگر برخورد کرده و در اثر این تداخل ، اطلاعات دچار مشکل می شوند. (**Collision** یعنی برخورد بسته های اطلاعاتی و ازبین رفتن آنها) تداخل ها معمولا مسئله ای در هاب ها می باشند. اما مسئله مهمتر این است که هاب ها پهنای باند را نیز هدر می دهند. هاب ها بصورت یکطرفه عمل می کنند، بدین معنی که در یک زمان اطلاعات فقط می توانند در یک مسیر حرکت کنند. از آنجاییکه هاب بصورت یکطرفه عمل می کند، پهنای باند باید بین هر پورت در هاب تقسیم بندی شود.

سوئیچ چیست؟

سوئیچ در مدل **OSI** در لایه پیوند داده (**Data Link**) عمل می کند. این بدان معنی است که سوئیچ هوشمندتر از هاب می باشد، بطوریکه سوئیچ در یک سطح دینامیک داده ها را مسیر دهی نماید. اگر اطلاعات بطور مثال مقصد معینی برای کامپیوتر **A** دارند سوئیچ فقط اطلاعات را به سمت کامپیوتر **A** مسیردهی می کند.

Hub

Switch

Half-Duplex و Full-Duplex چیست ؟

در استفاده از تلفن، هر دو طرف می توانند به طور همزمان با هم صحبت کرده و صدای یکدیگر را دریافت کنند، درواقع صوت به طور همزمان هم می آید و هم می رود .این یعنی ارتباطات دو طرفه **یا Full-Duplex** می باشد . یعنی به انتقال داده ها در دو جهت در هر لحظه دلالت می کند. اما در استفاده از بی سیم، ابتدا یک نفر صحبت می کند و در انتها می گوید "تمام" سپس طرف مقابل می تواند شروع به صحبت کند، به بیان دیگر در آن فقط یکی از دو طرف می تواند صحبت کند . این یعنی ارتباطات یک طرفه یا **Half-Duplex** می باشد. یعنی به انتقال داده ها در یک جهت در هر لحظه دلالت می کند. **Switch** می تواند هم ارتباط **Full-Duplex** و هم ارتباط **Half-Duplex** داشته باشد ولی در **Hub** تنها ارتباط **Half-Duplex** می تواند داشته باشد . علت ایجاد **Collision** در هاب همین **Half-Duplex** بودن آن است .

سناریو :

در این آزمایش می خواهیم یک شبکه مبتنی بر هاب و سوییچ را بررسی کرده و تفاوت های آنها را در حالت شبیه سازی مشاهده کنیم

فعالیت ۱ : مشاهده عملکرد **Hub**

مرحله ۱ – وارد حالت **Simulation** شوید.

مرحله ۲– **Event List Filters** را تنظیم کنید.

ما در اینجا تنها می خواهیم پکت های **ICMP** را بررسی کنیم برای این منظور بروی **Edit Filters** در **Event List Filters** کلیک کرده و سپس از لیست باز شده باید تنها تیک **ICMP** فعال باشد که باعث می شود که تنها پکت های **ICMP** نمایش داده شوند.

مرحله ۳– از **PC1** ، **PC6** را **Ping** کنید .

مدل دیگر **Ping** کردن سیستم ها با استفاده از **Add Simple PDU** () که در سمت راست نرم افزار به شکل یک پاکت در بسته است می باشد . شما با کلیک کردن بروی **Add Simple PDU** و سپس کلیک بروی **PC** مبدا و بعد از آن کلیک بروی **PC** مقصد از **PC** مبدا (**PC1**) ، **PC** مقصد (**PC6**) را **Ping** کنید . پکتی را شما در **Event List** مشاهده می کنید که شامل **ICMP echo request** می باشند. شما با کلیک بروی مربع رنگی کنار آنها می توانید اطلاعاتی در مورد هر یک بدست آورید .

مرحله ۴ – ایجاد انمیشن شبیه سازی

با کلیک بروی دکمه **Capture / Forward** شما می توانید در هر مرحله حرکت پکت ها در شبکه **Hub** را مشاهده کنید . برای هر بار کلیک بروی **Capture / Forward** یک جابجایی پکت ها را مشاهده می کنید. همانطور که مشاهده می کنید وقتی پکتی به هاب می رسد ، **Hub** آن پکت را در به تمام پورت های خود می فرستد و در تمام شبکه پخش می کند.

فعالیت ۲ : مشاهده عملکرد **Switch**

مرحله ۱ – از **PC7** ، **PC12** را **Ping** کنید .

شما با کلیک کردن بروی **Add Simple PDU** و سپس کلیک بروی **PC** مبدا و بعد از آن کلیک بروی **PC** مقصد از **PC** مبدا (**PC7**) ، **PC** مقصد (**PC12**) را **Ping** کنید .

مرحله ۲ – ایجاد انمیشن شبیه سازی

با کلیک بروی دکمه **Capture / Forward** شما می توانید در هر مرحله حرکت پکت ها در شبکه **Switch** را مشاهده کنید . برای هر بار کلیک بروی **Capture / Forward** یک جابجایی پکت ها را مشاهده می کنید. همانطور که مشاهده می کنید وقتی پکتی به هاب می رسد ، **Switch** آن پکت را در به تمام پورت های خود می فرستد و در تمام شبکه پخش می کند.

فعالیت ۳ : مشاهده **collision** در شبکه مبتنی بر **Hub**

مرحله ۱ – **Simulation** را **Restet** کنید .

با کلیک بر دکمه **Reset Simulation** ، **Simulation** را **Restet** کنید .

مرحله ۲ – به طور همزمان چند سیستم همدیگر را Ping کنند.

شما با کلیک کردن بروی **Add Simple PDU** و سپس کلیک بروی **PC** مبدا و بعد از آن کلیک بروی **PC** مقصد از **PC** مبدا (**PC1**) ، **PC** مقصد (**PC6**) را **Ping** کنید و همچنین همزمان شما با کلیک کردن بروی **Add Simple PDU** و سپس کلیک بروی **PC3** و بعد کلیک بروی **PC4** از **PC3** ، **PC4** را **Ping** کنید. حالا شما مشاهده خواهید کرد پکت شما **Drop** می شود .

مرحله ۳ – ایجاد انمیشن شبیه سازی

با کلیک بروی دکمه **Capture / Forward** شما می توانید در هر مرحله حرکت پکت ها در شبکه **Hub** را مشاهده کنید . برای هر بار کلیک بروی **Capture / Forward** یک جابجایی پکت ها را مشاهده می کنید. مشاهده می کنید که در این شبکه **collision** رخ می دهد.

فعالیت ۴ : مشاهده **collision** در شبکه مبتنی بر **Switch**

مرحله ۱ – **Simulation** را **Restet** کنید .

با کلیک بر دکمه **Reset Simulation** ، **Simulation** را **Restet** کنید .

مرحله ۲ – به طور همزمان چند سیستم همدیگر را **Ping** کنند.

شما با کلیک کردن بروی **Add Simple PDU** و سپس کلیک بروی **PC** مبدا و بعد از آن کلیک بروی **PC** مقصد از **PC** مبدا (**PC7**) ، **PC** مقصد (**PC12**) را **Ping** کنید و همچنین همزمان شما با کلیک کردن بروی **Add Simple PDU** و سپس کلیک بروی **PC9** و بعد کلیک بروی **PC10** از **PC9** ، **PC10** را **Ping** کنید.

مرحله ۳ – ایجاد انمیشن شبیه سازی

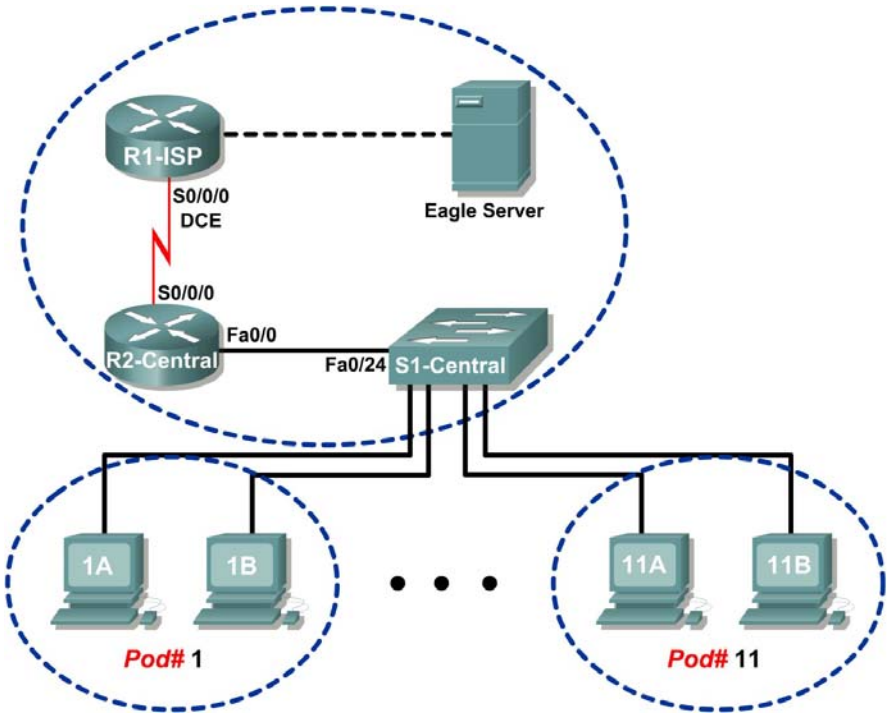
با کلیک بروی دکمه **Capture / Forward** شما می توانید در هر مرحله حرکت پکت ها در شبکه **Switch** را مشاهده کنید . برای هر بار کلیک بروی **Capture / Forward** یک جابجایی پکت ها را مشاهده می کنید. مشاهده می شود در این شبکه **collision** رخ نمی دهد.

مرحله ۴ – پورت های **Switch** را **Half-Duplex** کنید .

با کلیک بروی سوییچ و سپس رفتن به تب **Config** و در قسمت **Interface** ، بروی **FastEthernet0/1** تا **FastEthernet0/24** کلیک کرده و در هر قسمت در بخش **Duplex** آنها را با برداشتن تیک **Auto** و زدن تیک **Half-Duplex** آنها را **Half-Duplex** کرده و مرحله ۲ و ۳ را تکرار کنید . مشاهده می کنید که در این صورت در سوییچ **collision** رخ می دهد .

آزمایشگاه ۸-۱ : Address Resolution Protocol (ARP) و MAC Table

Topology Diagram



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1-ISP	S0/0/0	10.10.10.6	255.255.255.252	N/A
	Fa0/0	192.168.254.253	255.255.255.0	N/A
R2-Central	S0/0/0	10.10.10.5	255.255.255.252	10.10.10.6
	Fa0/0	172.16.255.254	255.255.0.0	N/A
Eagle Server	N/A	192.168.254.254	255.255.255.0	192.168.254.253
	N/A	172.31.24.254	255.255.255.0	N/A
host*Pod*#A	N/A	172.16.*Pod*#.1	255.255.0.0	172.16.255.254
host*Pod*#B	N/A	172.16.*Pod*#.2	255.255.0.0	172.16.255.254
S1-Central	N/A	172.16.254.1	255.255.0.0	172.16.255.254

درس :

MAC Address چیست ؟

هر کامپیوتر موجود در شبکه به منظور ایجاد ارتباط با سایر کامپیوترها ،می بایست شناسائی و دارای یک آدرس منحصربفرد باشد . آدرس های IP و MAC (Media Access Control) همان آدرس های منحصر بفرد می باشند و شاید این سوال برای شما مطرح شده باشد که اولا" ضرورت وجود دو نوع آدرس چیست و ثانیا" جایگاه اسفاده از آنان چیست ؟

MAC Address ، یک آدرس فیزیکی است در حالی که آدرس های **IP** ، به منزله آدرس های منطقی می باشند. آدرس های منطقی شما را ملزم می نمایند که به منظور پیکربندی کامپیوتر و کارت شبکه ، درایورها و یا پروتکل های خاصی را در حافظه مستقر نمائید (مثلا" استفاده از آدرس های **IP**) . این وضعیت در رابطه با **MAC Address** صدق نخواهد کرد و اینگونه آدرس ها نیازمند درایور های خاصی نخواهند بود ، چراکه آدرس های فوق درون تراشه کارت شبکه قرار می گیرند .

دلیل استفاده از MAC Address

هر کامپیوتر موجود در شبکه ، می بایست با استفاده از روش هائی خاص شناسائی گردد . برای شناسائی یک کامپیوتر موجود در شبکه ، صرف داشتن یک آدرس IP به تنهائی کفایت نخواهد کرد . حتما" علاقه مندید که علت این موضوع را بدانید . بدین منظور، لازم است نگاهی به مدل معروف **OSI** :

مدل OSI		
Network Layer	لایه سوم	آدرس IP در این لایه قرار دارد
DataLink Layer	لایه دوم	آدرس MAC در این لایه قرار دارد
Physical Layer	لایه اول	شبکه فیزیکی

همانگونه که مشاهده می نمائید ، **MAC Address** در لایه **DataLink** (لایه دوم مدل **OSI**) قرار دارد و این لایه مسئول بررسی این موضوع خواهد بود که داده متعلق به کدامیک از کامپیوترهای موجود در شبکه است . زمانی که یک بسته اطلاعاتی (**Packet**) به لایه **Datalink** می رسد (از طریق لایه اول) ، وی آن را در اختیار لایه بالائی خود (لایه سوم) قرار خواهد داد . بنابراین ما نیازمند استفاده از روش خاصی به منظور شناسائی یک کامپیوتر قبل از لایه سوم هستیم . **MAC Address** ، در پاسخ به نیاز فوق در نظر گرفته شده و با استقرار در لایه دوم ، وظیفه شناسائی کامپیوتر قبل از لایه سوم را بر عهده دارد. تمامی ماشین های موجود بر روی یک شبکه ، اقدام به بررسی بسته های اطلاعاتی نموده تا مشخص گردد که آیا

MAC Address موجود در بخش "آدرس مقصد " بسته اطلاعاتی ارسالی با آدرس آنان مطابقت می نماید؟ لایه فیزیکی (لایه اول) قادر به شناخت سیگنال های الکتریکی موجود بر روی شبکه بوده و فریم هائی را تولید می نماید که در اختیار لایه **Datalink** ، گذاشته می شود . در صورت مطابقت **MAC Address** موجود در بخش "آدرس مقصد " بسته اطلاعاتی ارسالی با **MAC Address** یکی از کامپیوترهای موجود در شبکه ، کامپیوتر مورد نظر آن را دریافت و با ارسال آن به لایه سوم ، آدرس شبکه ای بسته اطلاعاتی (**IP**) بررسی تا این اطمینان حاصل گردد که آدرس فوق با آدرس شبکه ای که کامپیوتر مورد نظر با آن پیکربندی شده است بدرستی مطابقت می نماید .

ساختار MAC Address

یک **MAC Address** بر روی هر کارت شبکه همواره دارای طولی مشابه و یکسان می باشند . (شش بایت و یا ۴۸ بیت) . در صورت بررسی **MAC Address** یک کامپیوتر که بر روی آن کارت شبکه نصب شده است ، آن را با فرمت مبنای شانزده (**Hex**) ، مشاهده خواهید دید . مثلا" **MAC Address** کارت شبکه موجود بر روی یک کامپیوتر می تواند به صورت زیر باشد :

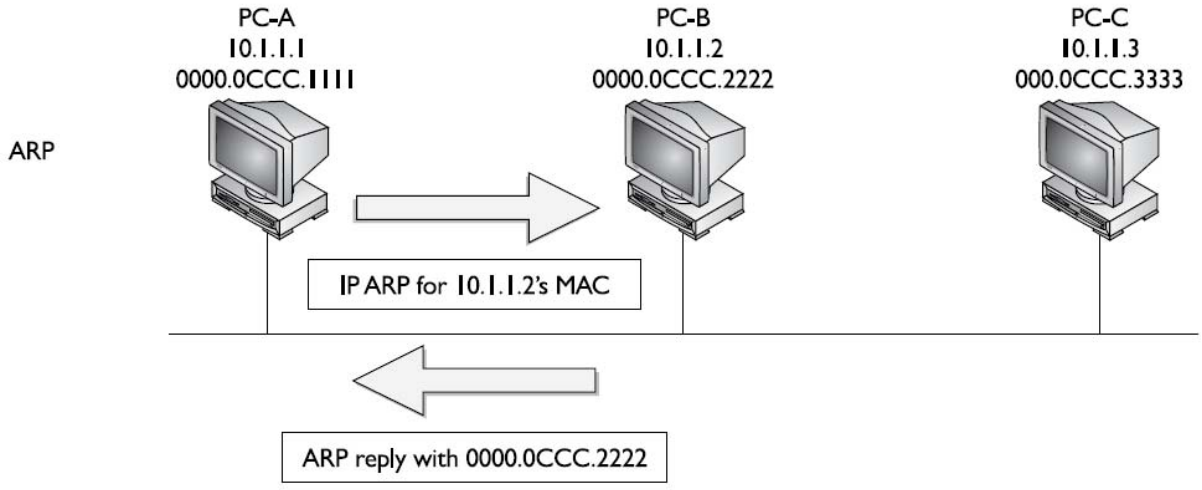
مشاهده MAC Address					
استفاده از دستور IPconfig / all و مشاهده بخش Physical address:					
00	50	BA	79	DB	6A
تعریف شده توسط IEEE		تعریف شده توسط تولید کننده			

زمانی که یک تولید کننده نظیر اینتل ، کارت ها ی شبکه خود را تولید می نماید ، آنان هر آدرس دلخواهی را نمی توانند برای **MAC Address** در نظر بگیرند . در صورتی که تمامی تولید کنندگان کارت های شبکه بخواهند بدون وجود یک ضابطه خاص ، اقدام به تعریف آدرس های فوق نمایند ، قطعا" امکان تعارض بین آدرس های فوق بوجود خواهد آمد . (عدم تشخیص تولید کننده کارت و وجود دو کارت شبکه از دو تولید کننده متفاوت با آدرس های یکسان).حتما" این سوال برای شما مطرح می گردد که **MAC Address** توسط چه افراد و یا سازمان هائی و به چه صورت به کارت های شبکه نسبت داده می شود ؟ به منظور برخورد با مشکلات فوق ، گروه **IEEE** ، هر **MAC Address** را به دو بخش مساوی تقسیم که از اولین بخش آن به منظور شناسائی تولید کننده کارت و دومین بخش به تولید کنندگان اختصاص داده شده تا آنان یک شماره سریال را در آن درج نمایند کد تولید کنندگان بر اساس **RFC-1700** به آنان نسبت داده می شود . در صورت مشاهده **RFC** فوق حتما" متوجه خواهید شد که برخی از تولید کنندگان دارای بیش از یک کد می باشند .علت این امر به حجم گسترده محصولات تولیدی آنان برمی گردد .

با این که **MAC Address** در حافظه کارت شبکه ثبت می گردد ، برخی از تولید کنندگان به شما این اجازه را خواهند داد که با دریافت و استفاده از یک برنامه خاص ، بتوانید بخش دوم **MAC Address** کارت شبکه خود را تغییر دهید(شماره سریال کارت شبکه) . علت این موضوع به استفاده مجدد از سریال های استفاده شده در سایر محصولات تولید شده توسط آنان برمی گردد (تجاوز از محدود مورد نظر) . در حال حاضر احتمال این که شما دو کارت شبکه را خریداری نمائید که دارای **MAC Address** یکسانی باشند، بسیار ضعیف و شاید هم غیرممکن باشد.

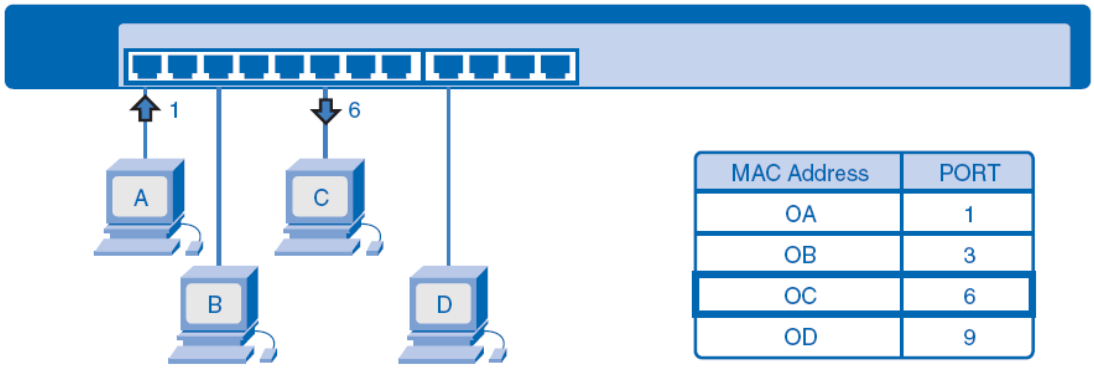
ARP چیست ؟

ARP مخفف سه کلمه **Address Resolution Protocol** است . وظیفه آن شناخت وتشخیص **MAC Address** است در صورتی سیستم با دانستن **IP** بخواهد با یک سیستم ارتباط برقرار کند. برای ارتباط با سیستم در یک محدوده شبکه ای (یک **Subnet**) باید حتما **Mac address** آن سیستم را بدانیم و ارتباط با آن سیستم فقط با **Mac address** انجام می شود . وقتی سیستمی **IP** مقصد را دارد ولی **Mac address** مقصد را ندارد (مثلا زمان **ping** کردن یک سیستم دیگر) یک پکت به اسم **ARP** تولید می کند که در آن **MAC** ، **IP** که دارد را درخواست می دهد و به صورت **BroadCast** برای همه سیستمها می فرستد و سیستمی که **IP** آن را دارد بر می دارد و در جواب **Mac** خود را برای پروتکل **ARP** سعی در تشخیص **IP** آن سیستم میکند و در پاسخ به آن سیستم (سیستمی که این **IP** مورد نظر برای ارتباط ما را دارد) به درخواست **Mac** خود را به سیستم ما اعلام میکند و سیستم ما این **Mac** را در جدولی با نام **ARP Table** که بر روی سیستم خودمان است ذخیره میشود .که مدت ذخیره شدن این اطلاعات در صورت دوباره نویسی و بروز نشدن آن فقط ۱۲۰ ثانیه است.



Mac address Table در سوییچ ها :

در یک سوییچ که یکی از مهمترین تفاوت های آن با **HUB** همین داشتن **Mac Table** است یعنی در هنگام **ARP** کردن سیستم ها وقتی پکتهای **ARP** از سوییچ می گذرند ، سوییچ لایه دوم پکتهای دریافتی را میخواند و مک آدرس مبدا را در این جدول به همراه پورت مربوطه قرار میدهد و این باعث میشود در صورتی که درخواستی را بخواهد به این آدرس بفرستد بداند از کدام پورت باید ارسال کند و مجبور به ارسال آن به تمامی پورتهای خروجی نمیشود. برای دیدن **Mac Table** سوییچ باید دستور **show mac-address-table** در سوییچ تایپ کنیم .



MAC Address	PORT
OA	1
OB	3
OC	6
OD	9

Telnet چیست ؟

Telnet یا **Telecommunication network** نرم افزاری است که به افراد توانایی کنترل قسمت های مختلف یک **Device** را از راه دور می دهد. تمام این توانایی ها در محیط متنی صورت می گیرد و تنها به وسیله ی یک سری دستورات است که می توانیم به اهداف خود برسیم. این دستورات جا به جا شده بین **Device** میزبان و میهمان، به صورت متن منتقل می شود و بنابراین امنیت کمی خواهند داشت. اگر واقعن نگران اطلاعات جا به جا شده هستید، می توانید از **SSH** یا **Secure Shell** استفاده کنند. که مانند **Telnet** می باشد با این تفاوت که اطلاعات در هنگام نقل و انتقال بصورت کد جابجا می شود .

استفاده از **Telnet**:

برای استفاده از **Telnet**، بعد از وارد شدن به محیط **Command Prompt** به صورت زیر عمل کنید:

Telnet Host name (or) Host IP

به جای **Host name** نام **Device** که قصد متصل شدن به آن دارید را بنویسید. در این صورت، اگر سرویس **Telnet** بر روی **Device** میزبان روشن باشد، شما به **Command Prompt** آن کامپیوتر دسترسی خواهید داشت . البته قبل از متصل شدن ممکن است از شما تقاضای نام کاربری و رمز عبور کند که باید نام و پسورد اکانت **Device** میزبان را وارد کنید. به این نکته نیز توجه داشته باشید که هنگام تایپ کلمه ی عبور، بر روی صفحه ی نمایش کلمه ای ظاهر نمی شود.

سناریو :

از دستور **show mac-address-table** در **Cisco IOS** (سیستم عامل سیسکو) برای دیدین **MAC Table** ، استفاده کنید. با استفاده از دستور **Telnet** به **Switch** وصل شوید و **Cisco IOS** باز کرده و **Mac Table** را ببینید.

فعالیت ۱ : با استفاده از پروتکل **Telnet** ، به سوئیچ سیسکو وارد شوید.

مرحله ۱ – دسترسی به **Terminal** ویندوز.

بروی یکی از **Host** ها کلیک کنید و وارد **Desktop** آن شده و دکمه **Command Prompt** زده وارد محیط **Terminal** می شوید.

مرحله ۲ – از دستور **Telnet** برای دسترسی به **S1-Central** (سوئیچ) استفاده کنید.

اول برای تولید پکتهای **ARP** و پر شدن جدول **Mac Table** سوئیچ آدرس **IP** سوئیچ که **172.16.254.1** را **Ping** کنید و بعد با دستور **telnet 172.16.254.1** به سیستم عامل سوئیچ وصل شده و سپس از شما **Password** می خواهد که شما **cisco** را تایپ می کنید و سپس وارد آن می شوید .

مرحله ۳ – دیدن پکتهای **ARP**

شما می توانید برای دیدن پکتهای **ARP** و دیدن عملکرد آنها می توانید قبل از دستور **Ping** ، به حالت **Simulation** رفته وسپس از دستور **Ping** استفاده کرده و بعد از دیدن پروسه **ARP** به حالت **RealTime** برگردید .

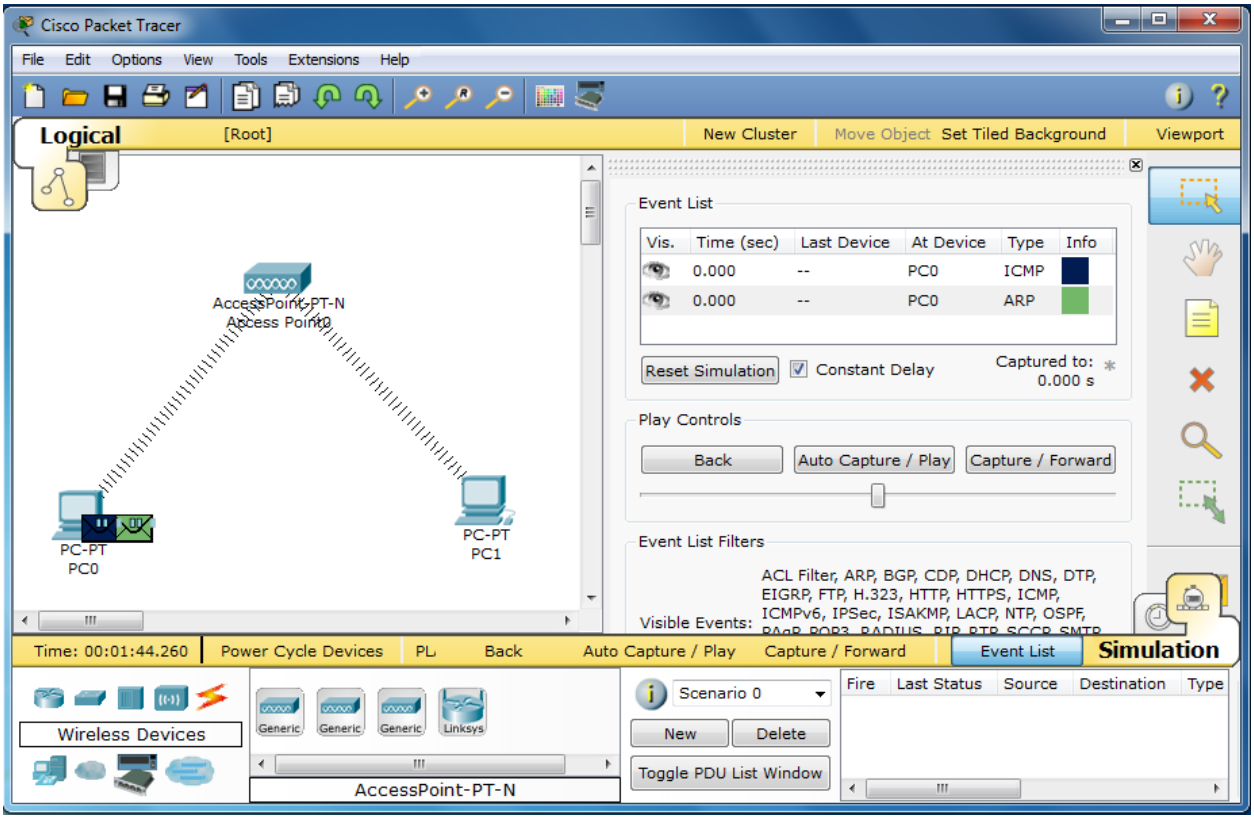
فعالیت ۲ : استفاده از دستور **show mac-address-table** برای نشان دادن **MAC address table**

مرحله ۱ – بررسی **MAC address table**

دستور **show mac-address-table** به شما تمام **Port** ها سوئیچ و چه سیستمی به کدام پورت آن وصل است را نشان می دهد .

آزمایشگاه ۹-۱ : شبکه Wireless (بی سیم) و امنیت شبکه

Topology Diagram



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
PC0	NIC	192.168.1.1	255.255.255.0	N/A
PC1	NIC	192.168.1.2	255.255.255.0	N/A

درس :

تجهیزات و پیکربندی یک شبکه Wireless :

سخت افزار مورد نیاز به منظور پیکربندی یک شبکه بدون کابل به ابعاد شبکه مورد نظر بستگی دارد . علیرغم موضوع فوق ، در این نوع شبکه ها اغلب و شاید هم قطعا" به یک **access point** و یک اینترفیس کارت شبکه نیاز خواهد بود . در صورتی که قصد ایجاد یک شبکه موقت بین دو کامپیوتر را داشته باشید ، صرفا" به دو کارت شبکه بدون کابل نیاز خواهید داشت .

Access Point چیست ؟

سخت افزار فوق ، به عنوان یک پل ارتباطی بین شبکه های کابلی و دستگاههای بدون کابل عمل می نماید . با استفاده از سخت افزار فوق ، امکان ارتباط چندین دستگاه به منظور دستیابی به شبکه فراهم می گردد .**access point** می تواند دارای عملکردی مشابه یک روتر نیز باشد . در چنین مواردی انتقال اطلاعات در محدوده وسیعتری انجام شده و داده از یک **access point** به **access point** دیگر ارسال می گردد .

یک نمونه دستگاه access point

کارت شبکه بدون کابل

هر یک از دستگاههای موجود بر روی یک شبکه بدون کابل ، به یک کارت شبکه بدون کابل نیاز خواهند داشت . یک کامپیوتر **Laptop** ، عموما" دارای یک اسلات **PCMCIA** است که کارت شبکه درون آن قرار می گیرد . کامپیوترهای شخصی نیز به یک کارت شبکه داخلی که معمولا" دارای یک آنتن کوچک و یا آنتن خارجی است ، نیاز خواهند داشت .آنتن های فوق بر روی اغلب دستگاهها ،اختیاری بوده و افزایش سیگنال بر روی کارت را بدنبال خواهد داشت .

یک نمونه کارت شبکه بدون کابل

پیکربندی یک شبکه بدون کابل :

به منظور پیکربندی یک شبکه بدون کابل از دو روش متفاوت استفاده می گردد :

۱- روش **Infrastructure** : به این نوع شبکه ها، **hosted** و یا **managed** نیز گفته می شود . در این روش از یک و یا چندین **access point** (موسوم به **gateway** و یا روترهای بدون کابل) که به یک شبکه موجود متصل می گردند ، استفاده می شود . بدین ترتیب دستگاههای بدون کابل، امکان استفاده از منابع موجود بر روی شبکه نظیر چاپگر و یا اینترنت را بدست می آورند .

۲- روش **Ad-Hoc** : به این نوع شبکه ها ، **unmanaged** و یا **peer to peer** نیز گفته می شود . در روش فوق هر یک از دستگاهها مستقیما" به یکدیگر متصل می گردند.مثلا" یک شخص با دارا بودن یک دستگاه کامپیوتر **laptop** مستقر در محوطه منزل خود می تواتند با کامپیوتر شخصی موجود در منزل خود به منظور دستیابی به اینترنت ، ارتباط برقرار نماید .

پس از تهیه تجهیزات سخت افزاری مورد نیاز به منظور ایجاد یک شبکه بدون کابل ، در ادامه می بایست تمامی تجهیزات تهیه شده را با هدف ایجاد و سازماندهی یک شبکه به یکدیگر متصل تا امکان ارتباط بین آنان فراهم گردد . قبل از نصب و پیکربندی یک شبکه بدون کابل ، لازم است به موارد زیر دقت نمائید :

۱- تهیه درایورهای مربوطه از فروشنده سخت افزار و کسب آخرین اطلاعات مورد نیاز

۲- فاصله بین دو کامپیوتر می بایست کمتر از یکصد متر باشد .

۳- هر یک از کامپیوترهای موجود می بایست بر روی یک طبقه مشابه باشند .

مراحل لازم به منظور نصب یک شبکه (فرضیات : ما دارای یک شبکه کابلی موجود هستیم و قصد پیاده سازی یک شبکه بدون کابل به منظور ارتباط دستگاههای بدون کابل به آن را داریم) :

۱- اتصال **point access** به برق و سوکت مربوط به شبکه اترنت

۲- پیکربندی **access point** (معمولا" از طریق یک مرورگر وب) تا امکان مشاهده آن توسط شبکه موجود فراهم گردد . نحوه پیکربندی **point access** بستگی به نوع آن دارد.

۳- پیکربندی مناسب کامپیوترهای سرویس گیرنده به منظور ارتباط با **access point** (در صورتی که تمامی سخت افزارهای شبکه بدون کابل از یک تولید کننده تهیه شده باشند ، عموما" با تنظیمات پیش فرض هم می توان شبکه را فعال نمود . به هر حال پیشنهاد می گردد همواره به راهنمای سخت افزار تهیه شده به منظور پیکربندی بهینه آنان ، مراجعه گردد) .

SSID چیست؟

مخفف عبارت **Service Set Identifier** می باشد . یک سرویس گیرنده شبکه، از **AP** مربوط به شبکه، یک نام دریافت می کند که همان **SSID** است. بصورت پیش فرض **SSID** برای همه ی سیستم های اطراف ارسال می شود. نام **SSID** بصورت پیش فرض از جمله اطلاعاتی است که در وضعیت **Broadcast** قرار دارد. زمانی که وارد یک هتل دارای اینترنت بی سیم می شوید در سیستمتان نام شبکه ی بی سیم موجود را می توانید ببینید. این نام همان **SSID** است که **AP** آن هتل برای شما **Broadcast** می کند.

امنیت شبکه

امنیت شبکه یا **Network Security** پرسه ای است که طی آن یک شبکه در مقابل انواع مختلف تهدیدات داخلی و خارجی امن می شود.

مفاهیم امنیت شبکه :

الف- منابع شبکه

در یک شبکه منابع بسیاری جهت محافظت وجود دارند. لیست ذیل مجموعه ای از منابع شبکه را معرفی می کند که باید در مقابل انواع حمله ها مورد حفاظت قرار گیرند.

۱- تجهیزات شبکه مانند روترها، سوئیچ ها و فایروالها (سیستم های امنیتی که بر ورود اطلاعات به یک شبکه نظارت داشته و جلوی بعضی از اطلاعات خاص را که توسط مدیر شبکه مشخص می شود را می گیرد) .

۲- اطلاعات عملیات شبکه مانند جداول مسیریابی و پیکربندی لیست دسترسی که بر روی روتر ذخیره شده اند.

۳- اطلاعات و منابع اطلاعاتی متصل به شبکه مانند پایگاه های داده و سرورهای اطلاعاتی

۴- اطلاعات در حال تبادل بر روی شبکه در هر لحظه از زمان

ب- حمله

حمله تلاشی خطرناک یا غیر خطرناک است تا یک منبع قابل دسترسی از طریق شبکه ، به گونه ای مورد تغییر یا استفاده قرار گیرد. برای فهم بهتر بد نیست حملات شبکه را به سه دسته عمومی تقسیم کنیم:

۱- دسترسی غیرمجاز به منابع و اطلاعات از طریق شبکه

۲- دستکاری غیرمجاز اطلاعات بر روی یک شبکه

۳- حملاتی که منجر به اختلال در ارائه سرویس می شوند و اصطلاحا (**Denial of Service (DOS** نام دارند.

ج- تحلیل خطر

پس از تعیین دارایی های شبکه و عوامل تهدیدکننده آنها ، باید خطرات مختلف را ارزیابی کرد. در بهترین حالت باید بتوان از شبکه در مقابل تمامی انواع خطا محافظت کرد، اما امنیت ارزان به دست نمی آید. بنابراین باید ارزیابی مناسبی را بر روی انواع خطرات انجام داد تا مهمترین آنها را تشخیص دهیم و از طرف دیگر منابعی که باید در مقابل این خطرات محافظت شوند نیز شناسایی شوند. دو فاکتور اصلی در تحلیل خطر عبارتند از :

۱- احتمال انجام حمله

۲- خسارت وارده به شبکه درصورت انجام حمله موفق

۳- سیاست امنیتی

پس از تحلیل خطر باید سیاست امنیتی شبکه را به گونه ای تعریف کرد که احتمال خطرات و میزان خسارت را به حداقل برساند. سیاست امنیتی باید عمومی و در حوزه دید کلی باشد و به جزئیات نپردازد. جزئیات می توانند طی مدت کوتاهی تغییر پیدا کنند اما اصول کلی امنیت یک شبکه که سیاست های آن را تشکیل می دهند ثابت باقی می مانند.در واقع سیاست امنیتی سه نقش اصلی را به عهده دارد:

۱- چه و چرا باید محافظت شود.

۲- چه کسی باید مسئولیت حفاظت را به عهده بگیرد.

۳- زمینه ای را بوجود آورد که هرگونه تضاد احتمالی را حل و فصل کند.

د- طرح امنیت شبکه

با تعریف سیاست امنیتی به پیاده سازی آن در قالب یک طرح امنیت شبکه می رسیم. المانهای تشکیل دهنده یک طرح امنیت شبکه عبارتند از :

۱- ویژگیهای امنیتی هر دستگاه مانند کلمه عبور مدیریتی

۲- فایروالها .

۳- تشخیص نفوذ

۴- سرورهای امنیتی **AAA** (**Authorization and Accounting،Authentication**) و سایر خدمات **AAA** برای شبکه

۵- مکانیزمهای کنترل دسترسی و محدودکننده دسترسی برای دستگاههای مختلف شبکه

ذ- نواحی امنیتی

تعریف نواحی امنیتی نقش مهمی را در ایجاد یک شبکه امن ایفا می کند. در واقع یکی از بهترین شیوه های دفاع در مقابل حملات شبکه ، طراحی امنیت شبکه به صورت منطقه ای و مبتنی بر توپولوژی است و یکی از مهمترین ایده های مورد استفاده در شبکه های امن مدرن ، تعریف نواحی و تفکیک مناطق مختلف شبکه از یکدیگر است. تجهیزاتی که در هر ناحیه قرار می گیرند نیازهای متفاوتی دارند و لذا هر ناحیه حفاظت را بسته به نیازهای امنیتی تجهیزات نصب شده در آن ، تامین می کند. همچنین منطقه بندی یک شبکه باعث ایجاد ثبات بیشتر در آن شبکه نیز می شود.

امنیت در شبکه بی سیم

بطور کلی تضمین امنیت در شبکه های بی سیم خیلی پیچیده تر از شبکه های سیمی می باشد. چرا که رسانه انتقال در اینجا محیط اطراف است و کنترل آن بسیار سخت است . **WEP**، **WPA**،**WPA2** سه روش مختلف کد گذاری اطلاعات در شبکه های بسیم قبل از ارسال می باشد که اطمینان در روش کد گذا ری **WPA2** بیشتر از **WPA** و اطمینان در روش کد گذا ری **WPA** بیشتر از **WEP** می باشد .

سناریو :

در این آزمایش می خواهیم با یک **AP** یک شبکه خیلی ساده **Wireless** را راه اندازی کرده و برای امنیت در این شبکه از روش های کد گذاری اطلاعات استفاده کنیم .

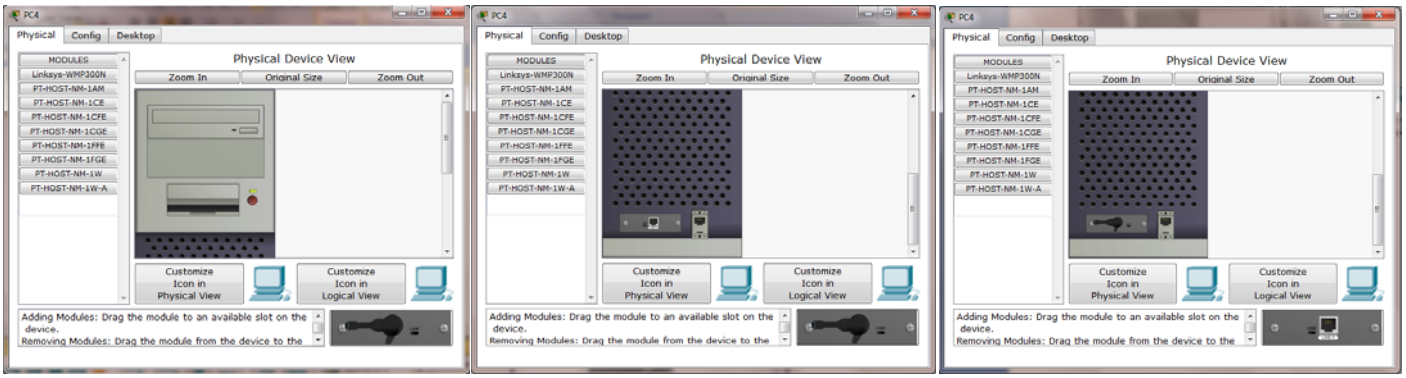
فعالیت ۱ : ایجاد فیزیکی یک شبکه **Wireless**

مرحله ۱ – اضافه کردن یک **AP (Access Point)**

از قسمت **Device** ها و بخش **Wireless** ، یک **Access Point-PT-N** را انتخاب کرده و به **Workspace** اضافه کنید.

مرحله ۲– اضافه کردن دو **PC** که دارای کارت شبکه بی سیم می باشند

از قسمت **Device** ها و بخش **Custom Made Devices** ، دو **Wireless Pc** را انتخاب کرده و به **Workspace** اضافه کنید. توجه داشته باشید که می تواتید این کار را از طریق **End Devices** و انتخاب دو **PC** و کلیک کردن بر روی **Pc** ها و رفتن به تب **Physical** و سپس خاموش کردن آن و جابجایی کارت شبکه آن با یک کارت شبکه **Wireless** نیز می توانستید انجام دهید.



فعالیت ۲ : تنظیم **AP (Access Point)**

مرحله ۱ – تنظیم نام **AP**

با کلیک بروی **AP** و رفتن به تب **Config** و انتخاب **Setting** ، در جلوی گزینه **Desplay name** نام **AP1** را وارد کنید.

مرحله ۲ – تنظیم **SSID** برای **AP**

با کلیک بروی **AP** و رفتن به تب **Config** و انتخاب **Port 1** ، در جلوی گزینه **SSID** نام **Network1** را وارد کنید.

مرحله ۳ – تنظیم امنیت **AP**

با کلیک بروی **AP** و رفتن به تب **Config** و انتخاب **Port 1** و انتخاب **WEP** در جلوی آن رمز **1234567890** را وارد کنید.

فعالیت ۳ : تنظیمات **PC** ها برای شبکه **Wireless**

مرحله ۱- تنظیمات **IP** برای **PC** ها

طبق **Addressing Table** ، **IP** کامپیوتر ها را وارد کنید .

مرحله ۲- تنظیمات **Wireless** برای **PC** ها

با کلیک بروی **PC** ها و رفتن به تب **Desktop** و انتخاب **PC Wireless** وارد قسمت تنظیمات **Wireless** شوید. سپس انتخاب تب **Profiles** و کلیک بروی گزینه **New** و تایپ یک نام دلخواه و **OK** کردن آن در لیست مقابل آن نام **SSID** شبکه خود که **Network** انتخاب شده بود را خواهید دید . بروی آن کلیک کرده و دکمه **Connect** را فشار دهید و سپس از شما کد رمز **WEP** را خواسته می شود که شما باید عدد **1234567890** را وارد کنید . بعد از آن با کلیک بروی دکمه **Connect** به شبکه وصل خواهید شد.

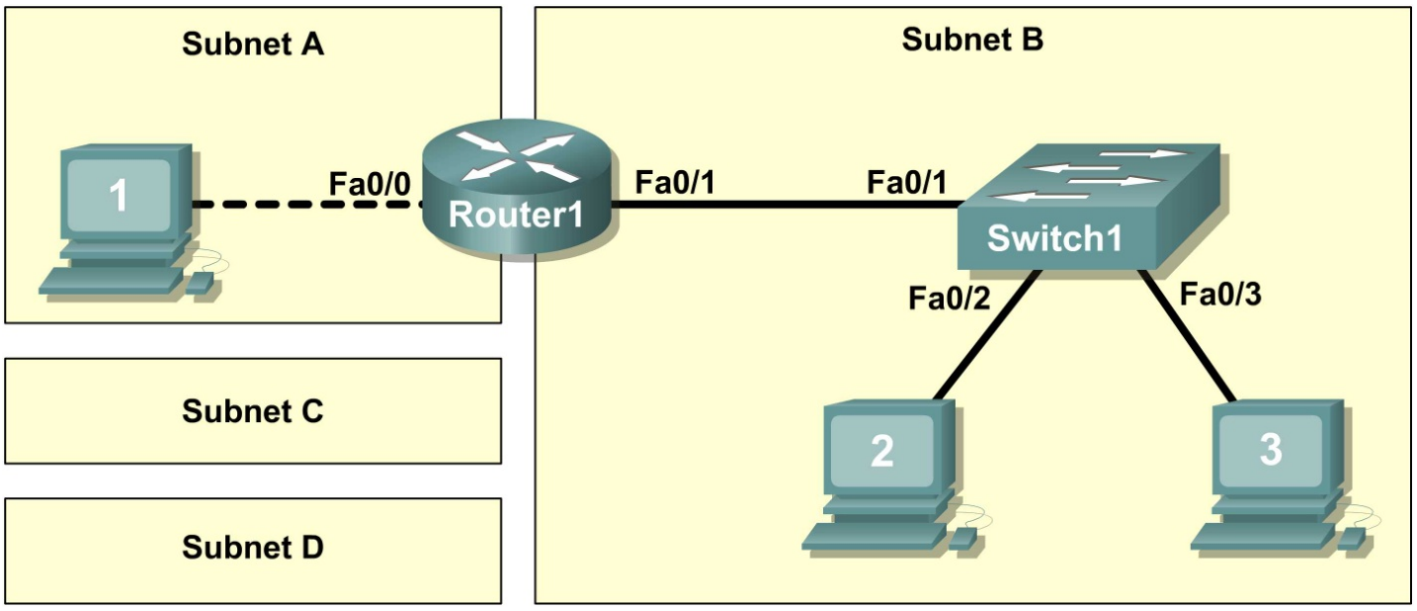
فعالیت ۴ : مشاهده حالت **Simulation**

مرحله ۱- پکت های **ICMP** و **ARP** در شبکه **Wireless**

در حالت **Simulation** رفته و با **Ping** کردن **PC1** در **PC0** ، جابجایی و عملکرد پکت های **ICMP** و **ARP** در شبکه **Wireless** مشاهده کنید .

آزمایشگاه ۱۰-۱ : ایجاد یک توپولوژی کوچک و VLSM

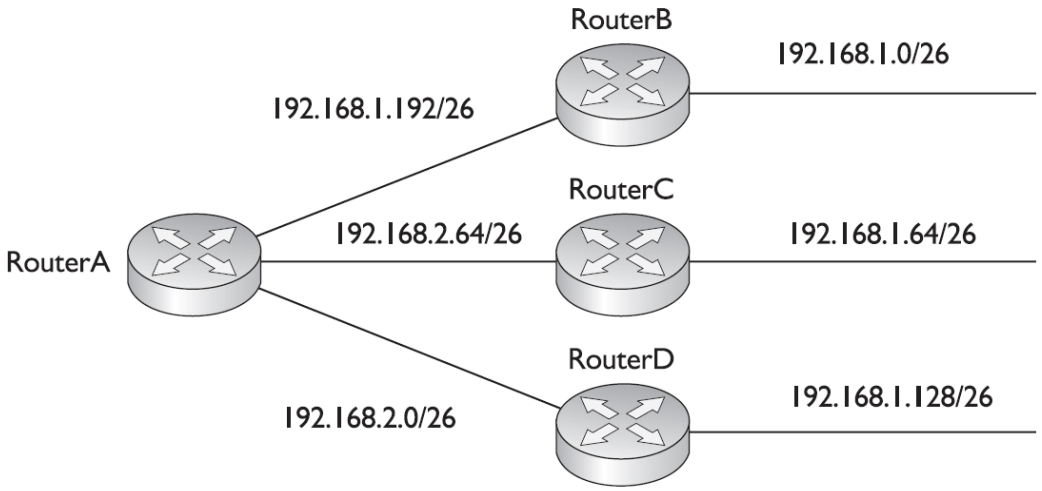
Topology Diagram



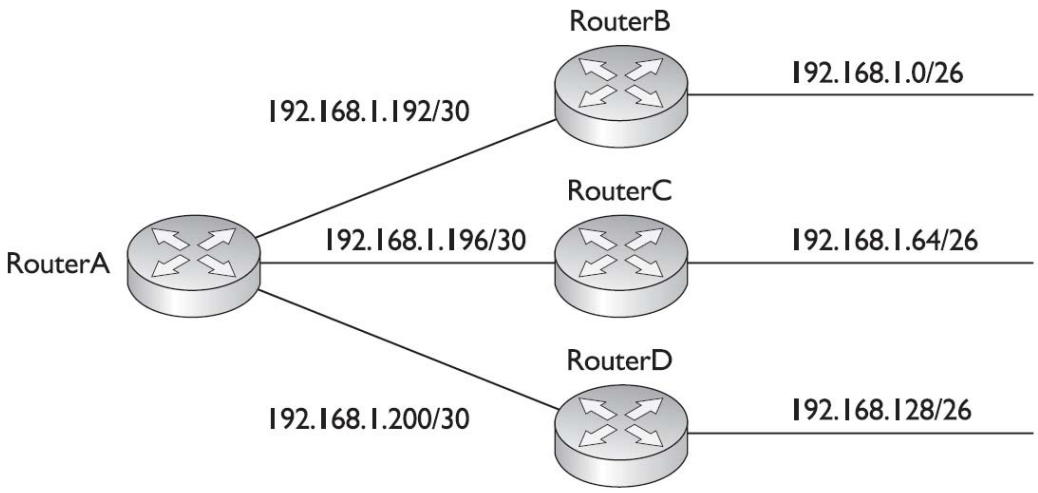
درس :

VLSM چیست ؟

Subnet mask معمولی ،به مدیران شبکه این اجازه را می دهد که بر مبنای اینکه چطور میزبان ها بصورت فیزیکی به شبکه متصل هستند به آنها آدرس **IP** تخصیص دهد، در شبکه های بزرگ نیاز است که تمام شبکه را فقط به یک سطح زیر شبکه تقسیم کنیم که این بهترین استفاده از آدرس های **IP** را بیان نمی کند، اگر ما زیر شبکه هایی با تعداد میزبان های مختلفی در آنها داشته باشیم ، ما ممکن است دچار مشکلاتی شویم . **IP** زیر شبکه باید بر مبنای اینکه هرکدام از زیر شبکه ها بیشترین مقدار میزبان را داشته باشد، انتخاب شود. این حتی در شبکه های کوچک هم بی بهره است و ممکن است منجر به استفاده از آدرس اضافی و هدر رفتن مقدار زیادی از آدرس در **Subnet** ها شود. برای مثال در شکل زیر ما **3 Subnet** داریم که در هر کدام **50 Host** و در بین **Router** ها هم هر کدام **2 Host** وجود دارد در نتیجه **Subnet mask** ، **/26** می شود یعنی برای هر **Subnet** ، ما ۶۴ آدرس خواهیم داشت ولی در بین **Router** ها فقط چهار آدرس مورد نیاز است و ۶۰ آدرس هدر می رود.



راه حل این وضعیت بالا بردن طرح آدرس دهی پایه زیر شبکه است که **(Variable Length Subnet Mask) VLSM** نامیده میشود، **VLSM** در ابتدا پیچیده بنظر میرسد اما اگر شما درک خوبی از **Subnetting** داشته باشید.فهمیدن آن بسیار سادست . **VLSM subnetting** به همان روش **Subnetting** معمولی انجام میشود با این تفاوت که شما برای هر **Subnet** به تعداد مورد نیاز **Host** ، آدرس خواهید داشت و آدرس هدر نمی رود . شما در شکل صفحه بعد می توانید **VLSM** مثال بالا را ببینید.



برای VLSM مراحل زیر را انجام دهید :

۱. تعداد کل آدرسی که احتیاج است تعیین کنید .

۲. تعداد **Network** که احتیاج است و تعداد **Host** که در هر شبکه نیاز است را تعیین کنید .

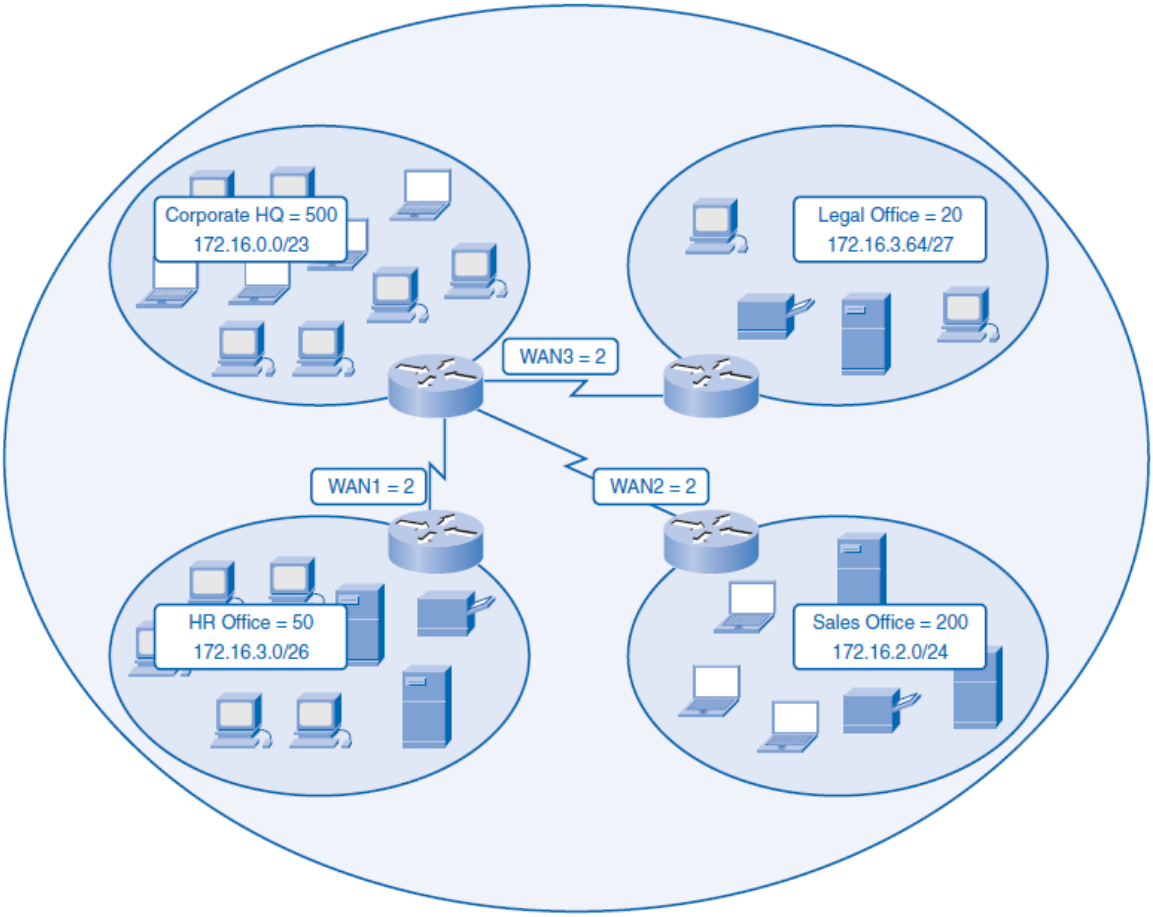
۳. مشخص کنید که بزرگترین **Subnet** کدام است و **Subnet Mask** می تواند همه **Host** این **Subnet** را در خود جای دهد .

۴. مرحله سه را برای **Subnet** کوچکتر را هم پیاده کنید . و همینطور این کار تکرار کنید تا همه **Subnet** ها دارای آدرس شوند.

برای بدست آورن **Subnet Mask** باید به این نکته توجه کنید که در هر **Subnet** باید اول ما ببینیم که تعداد هر **Host** با کدام 2^n مساوی و یا کوچکترین در کمترین فاصله است و بعد **n** بدست آمده را از ۳۲ کم کرده تا عدد **Subnet Mask** بصورت **CIDR** مشخص شود .

برای بدست آورن **Network Address** باید به این نکته توجه کنید که می آیم از **Subnet** با بیشترین **Host** شروع می کنیم که آدرسی را که داریم به علاوه آن کرده تا به مضرب 2^n برسد وبعد از آن را برای شبکه بعدی می گذاریم و به همین صورت ادامه می دهیم .

به عنوان مثال ، با توجه به شکل زیر ، ما یک **IP** در کلاس **B** داریم که عبارت است از **172.16.0.0 /16** که ۴ شبکه با نام **corporate HQ** که پانصد **Host** و **Sales Office** با دویست **Host** و **HR Office** با پنجاه **Host** و **Legal Office** با بیست **Host** و **Wan1** و **Wan2** و **Wan3** دارای دو **Host** می باشد که می خواهیم به این شبکه ها **IP Address** و **Subnet Mask** اختصاص دهیم .



۱- اول می رویم سراغ شبکه **corporate HQ** که پانصد **Host** داشت 2^9 می شود ۵۱۲ پس ۲۳=۹-۳۲ و در مورد آدرس شبکه چون بیشترین **Host** را دارد از آدرس اولیه شروع می شود و تا ۵۰۰ تا ادامه دارد و چون به ۵۱۲ نزدیک است تا ۵۱۲ می رود . پس آدرس شبکه و **CIDR** آن می شود : **172.16.0.0/23**

۲- شبکه **Sales Office** که دویست **Host** دارد 2^8 می شود ۲۵۶ پس ۲۴= ۸-۳۲ و در مورد آدرس شبکه چون **Subnet** قبلی تا ۵۱۲ داشت از **172.16.2.0** شروع می شود و تا ۲۰۰ تا ادامه دارد که به ۲۵۶ نزدیک است ادامه پیدا می کند. پس آدرس شبکه و **CIDR** آن می شود : **172.16.2.0 /24**

۳- شبکه **HR Office** دارای پنجاه **Host** می باشد که 2^6 می شود ۶۴ پس ۲۶=۶-۳۲

پس آدرس شبکه و **CIDR** آن می شود : **172.16.3.0/26**

۴- شبکه **Legal Office** دارای بیست **Host** می باشد که 2^5 می شود ۳۲ پس ۲۷=۵-۳۲

پس آدرس شبکه و **CIDR** آن می شود : **172.16.3.64/27**

۵- شبکه **Wan 1** دارای دو **Host** می باشد که 2^1 می شود ۲ پس ۳۰=۲-۳۲

پس آدرس شبکه و **CIDR** آن می شود : **172.16.3.128/30**

۶- شبکه **Wan 2** دارای دو **Host** می باشد که 2^1 می شود ۲ پس ۳۰=۲-۳۲

پس آدرس شبکه و **CIDR** آن می شود : **172.16.3.132/30**

۷- شبکه **Wan 3** دارای دو **Host** می باشد که 2^1 می شود ۲ پس ۳۰=۲-۳۲

پس آدرس شبکه و **CIDR** آن می شود : **172.16.3.136/30**

در جدول زیر این اطلاعات کاملتری را می توانید ببینید .

Corporate Net	HQ	Sales	HR	Legal	WAN1	WAN2	WAN3	Unused
172.16.0.0/22	172.16.0.0/23	172.16.2.0/24	172.16.3.0/26	172.16.3.64/27	172.16.3.128/30	172.16.3.132/30	172.16.3.136/30	
172.16.0.1	172.16.0.1							
	172.16.1.255							
		172.16.2.0						
		172.16.2.255						
			172.16.3.0					
			172.16.3.63					
				172.16.3.64				
				172.16.3.127				
					172.16.3.128			
					172.16.3.131			
						172.16.3.132		
						172.16.3.135		
							172.16.3.136	
							172.16.3.139	
								172.16.3.140
172.16.3.255								172.16.3.255

physical topologyچیست ؟

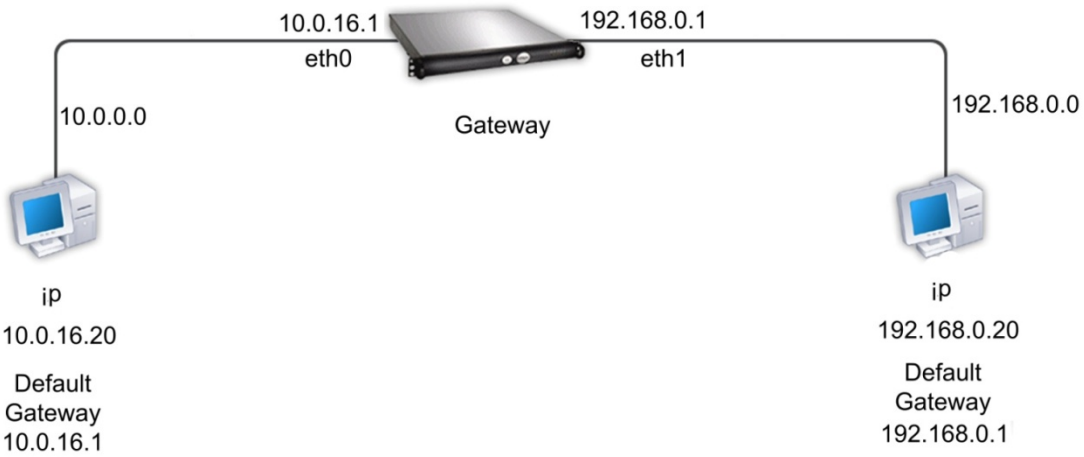
اتصال فیزیکی در یک شبکه چگونگی اتصال کامپیوترها و سخت افزارهای موجود در یک شبکه را از نظر فیزیکی مورد بحث قرار می دهد

Logical topology چیست ؟

اتصال منطقی نحوه رفتار کامپیوترهای موجود در شبکه را مورد بحث قرار می دهد و تشریح کننده چگونگی عبور منطقی **Packet Frame** بر اساس **Topology** می باشد .

Default Gateway چیست ؟

در شبکه **Gateway** به سیستمی گفته می شود که توانایی آن را دارد تا دو شبکه متفاوت را که از پایه از دو پروتکل متفاوت تشکیل شده است یا دارای **Subnet** های متفاوتی می باشند را به یکدیگر متصل کند. یا به عبارت دیگر **Gateway** نقطه ای از شبکه است که به عنوان ورودی به شبکه دیگر عمل می کند و **Default gateway** عددی **(IP)** است که نشان می دهد ما به کدام سیستم متصل هستیم و از آن سرویس برای وصل شدن به یک شبکه متفاوت دیگر، می گیریم.



سناریو :

در این آزمایشگاه شما یک شبکه های کوچک را ایجاد می کنید که نیاز به اتصال **device** های شبکه و پیکربندی **host** دارد در حال حاضر **SubnetA** و **SubnetB** مورد نیاز است و **SubnetC** و **SubnetD** به شبکه متصل نشده است .

فعالیت ۱ : طراحی **Logical Network**

با توجه به **IP address** و **Mask** **172.20.0.0 / 24** آدرس های **IP** ، **Subnet** های مورد نیاز را پیدا کنید :

Subnet	Number of Hosts
SubnetA	2 maximum
SubnetB	6 maximum
SubnetC	47 maximum
SubnetD	125 maximum

اولین آدرس در هر **Subnet** را به کامپیوتر **Host** و آخرین آدرس را به **interfaces** روتر موجود در آن **Subnet** بدهید .

مرحله ۱ : طراحی بلوک آدرس **SubnetD**

چون **SubnetD** دارای بیشترین **Host** می باشد ، طراحی منطقی را از **SubnetD** آغاز می کنیم .

سوال ۱- ۱۰ : جدول زیر را با اطلاعات **IP address** برای **SubnetD** را پر کنید .

Network Address	Mask	First Host Address	Last Host Address	Broadcast

سوال ۲- ۱۰ : چه **Mask** به باینری استفاده شده ؟_____

مرحله ۲: طراحی بلوک آدرس **SubnetC**

سوال ۳- ۱۰: جدول زیر را با اطلاعات **IP address** برای **SubnetC** را پر کنید .

Network Address	Mask	First Host Address	Last Host Address	Broadcast

سوال ۴- ۱۰: چه **Mask** به باینری استفاده شده ؟_____

مرحله ۳: طراحی بلوک آدرس **SubnetB**

سوال ۵- ۱۰: جدول زیر را با اطلاعات **IP address** برای **SubnetB** را پر کنید .

Network Address	Mask	First Host Address	Last Host Address	Broadcast

سوال۶- ۱۰: چه **Mask** به باینری استفاده شده ؟_____

مرحله ۴: طراحی بلوک آدرس **SubnetA**

سوال ۷- ۱۰: جدول زیر را با اطلاعات **IP address** برای **SubnetA** را پر کنید .

Network Address	Mask	First Host Address	Last Host Address	Broadcast

سوال ۸- ۱۰: چه **Mask** به باینری استفاده شده ؟_____

فعالیت ۲ : پیکربندی **Physical Topology**

مرحله ۱ : از لحاظ فیزیکی **device** ها را بهم ارتباط دهید .

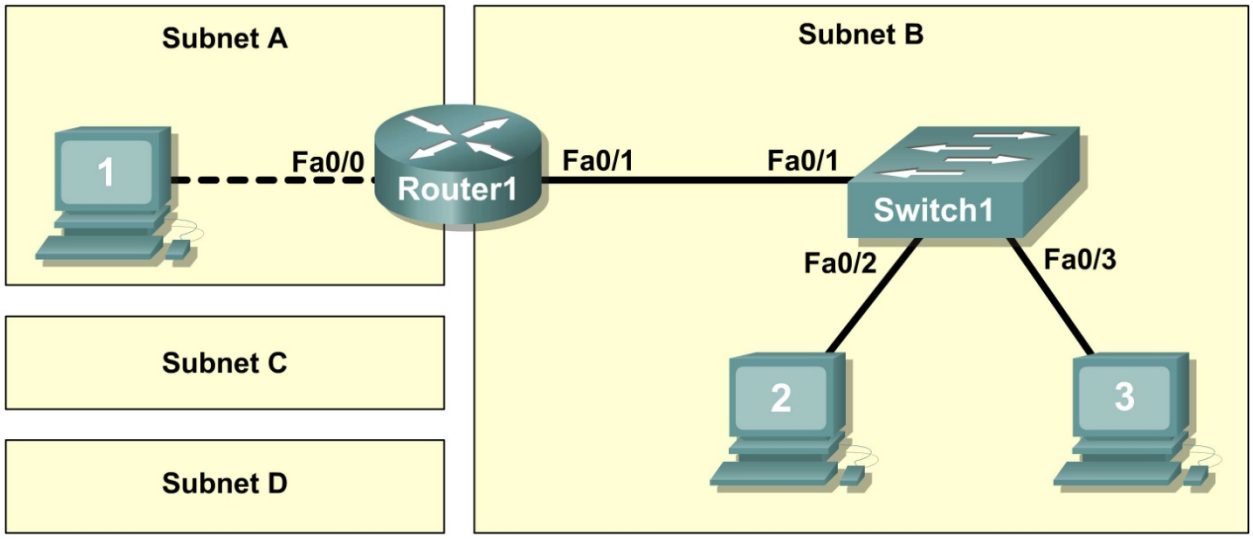


Figure 1. Cabling the Network

با توجه به شکل **device** ها را کابل کشی کنید.

سوال ۹- ۱۰ : چه نوع کابلی برای اتصال **Host1** به **Router1** مورد نیاز است و چرا؟

سوال ۱۰- ۱۰ : چه نوع کابلی برای اتصال **Host3**، **Host2** به **Switch1** و **router1** به **Switch1** مورد نیاز است و چرا؟

مرحله ۲ : بازرسی اتصالات شبکه .

بعد از کابل کشی دستگاه های شبکه، بازرسی کنید که اتصالات درست است یا نه . باید دقت کنید که همه **interface** دستگاه ها سبز باشند و همچنین توجه داشته باشید وقتی کابلی را به **Switch** وصل می کنید اول رنگ آن **interface** سوییچ کهربایی بوده و بعد از مدتی سبز می شود علت این است که **Switch** هر زمان که به **device** وصل می شود قبل از ارتباط با آن سرعت خود را با آن تنظیم می کند و این زمان رنگ آن ، کهربایی است .

سوال ۱۱- ۱۰ : چه نوع کابلی از رابط **Fa0/0** روتر به **Host1** متصل است ؟_____

سوال ۱۲- ۱۰ : چه نوع کابلی از رابط **Fa0/1** روتر به **Host2** متصل است ؟_____

سوال ۱۳ - ۱۰ : آیا تمام تجهیزات روشن است ؟_____

فعالیت ۳: پیکربندی **Logical Topology**

مرحله ۱ : تنظیمات **Logical Topology** یادداشت کنید .

از آدرس **Gateway IP** در کامپیوتر **Host** ، برای ارسال بسته های اطلاعاتی به شبکه های دیگر استفاده می شود. بنابراین در هر **subnet**، آدرس **Gateway** را آدرس **interface** روتری که به آن متصل است را می دهیم . که این کار یکی دیگر از کاربرد های روتر می باشد.

سوال ۱۴ - ۱۰ : از اطلاعات بدست آمده از فعالیت ۱ جدول مربوط به **Host** ها را پر کنید .

Host1	
IP Address	
IP Mask	
Gateway Address	

Host2	
IP Address	
IP Mask	
Gateway Address	

Host3	
IP Address	
IP Mask	
Gateway Address	

مرحله ۲ : با استفاده از اطلاعات بالا پیکربندی **Host1** ، **Host2** ، **Host3** را انجام دهید.

با استفاده از دکمه **IP Configuration** در **Desktop** هر کدام از **Host** ها این کار را انجام دهید .

فعالیت ۴ : بررسی مجدد اتصالات شبکه با استفاده از دستور **Ping** .

سوال ۱۵ – ۱۰ : با استفاده از دستور **Ping** ، جدول زیر (که مشخص شده است از چه سیستمی و کدام سیستم را **Ping** شود) را پر کنید :

From	To	IP Address	Ping Results
Host1	Gateway (Router1,Fa0/0)		
Host1	Router1, Fa0/1		
Host1	Host2		
Host1	Host3		
Host2	Host3		
Host2	Gateway (Router1,Fa0/1)		
Host2	Router1, Fa0/0		
Host2	Host1		
Host3	Host2		
Host3	Gateway (Router1,Fa0/1)		
Host3	Router1, Fa0/0		
Host3	Host1		

توجه داشته باشید برای عیب یابی قطع اتصالات ، **Topology Diagram** می تواند کمک خیلی خوبی باشد .

سوال ۱۶ – ۱۰ : در سناریوی فوق ، چگونه می توان درستی عملکرد **Gateway** را بررسی کرد ؟

ضمیمه ۱ - تجهیزات شبکه

انواع تجهیزات شبکه :

۱- تجهیزلت فعال (**Active**) ۲- تجهیزلت غیر فعال (**Passive**)

تجهیزلت فعال (Active)

۱- سرور : سرور ها در انواع مختلف ، سرویس های گونا گون را به کاربران ارائه می دهند .

۲- سرور تیغه ای : کامپیوتر سرور را می توان در نوع تیغه ای (**blade**) که مناسب نصب در رک هست تهیه نمود.

۳- سوییچ : همان قلب تپنده شبکه **Star** هست که وظیفه انتقال ترافیک را بر عهده دارد

۴- روتر : مسیر یاب ها به عنوان ادواتی که در لایه ۳ شبکه کار می کنند ، وظیفه ایجاد ارتباط بین شبکه های مختلف را دارند.

۵- **Access Point (AP)** : نقاط دسترسی که مشابه سوییچ و روتر در شبکه بی سیم عمل می کنند.

۶- فایروال : دیواره های آتش ، محافظ کننده شبکه از حملات ویروسی ، نفوذ گران و کرم های آسیب رسان .

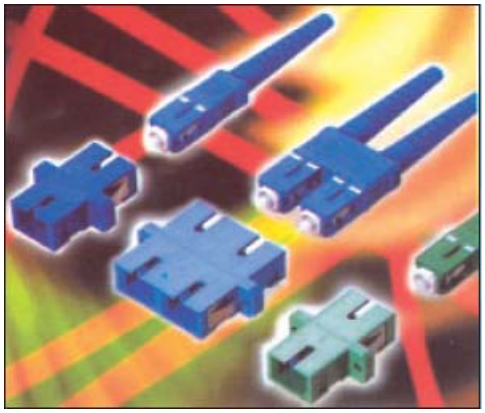
۷- کارت شبکه : رابط گرافیکی ایستگاه های کاری با شبکه که به آن **NIC** نیز معروف است .

۸- کارت شبکه بی سیم : کارت شبکه ای که در شبکه های بیسیم استفاده می شود.

۹- آنتن : برای دریافت امواج رادیویی در شبکه های بی سیم به صورت **Outdoor** (بیرون ساختمان) نصب می شود .

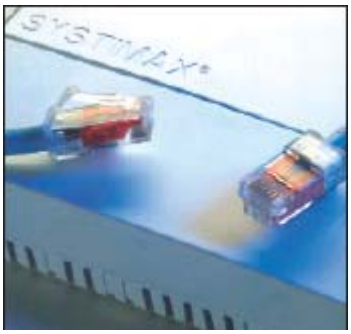
تجهیزلت غیر فعال (Passive) :

۱- کنتاکتور فیبر نوری : قطعه ای برای برقراری ارتباط فیبر نوری با سایر ادوات می باشد .



۲- کابل مسی **UTP** : کابل های مسی از چهار رشته بهم تابیده تشکیل شده اند را با نام **UTP** می شنلسیم .

۳- سرکابل مسی یا سوکت : قطعه ای برای برقراری ارتباط کابل مسی با سایر ادوات می باشد .

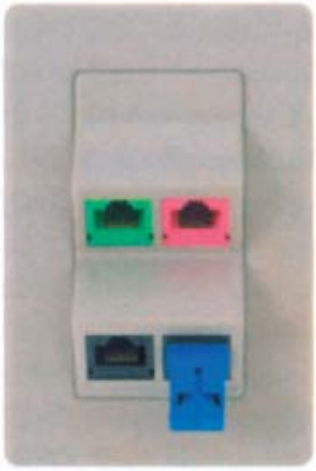


۴- رک (**Rack**): محفظه ای فلزی که محل قرار گرفتن سوییچ ها ، روتر ها ، سرور ها ، **UPS** (برق اضطراری برای زمان قطع برق) و سایر ادوات شبکه می تواند باشد .

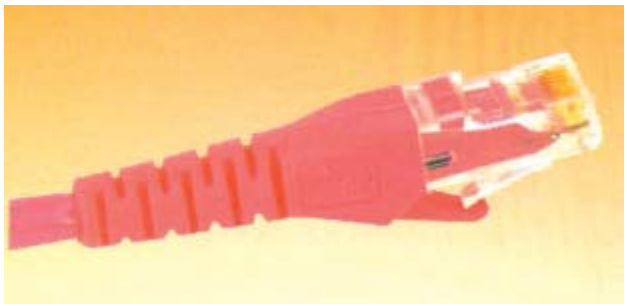
۵- فیبر نوری : رشته ای از شیشه یا پلاستیک که به جای الکترون ها ، پرتوهای نور را عبور می دهد .

۶- **Keystone** کابل مسی : مکانیزم داخل هر پریز شبکه که در حکم مادگی آن است .

۷- پریز دیواری مسی : هر ایستگاه شبکه برای برقراری ارتباط با شبکه باید با استفاده از پریز اتصال فیزیکی خود را برقرار کند.



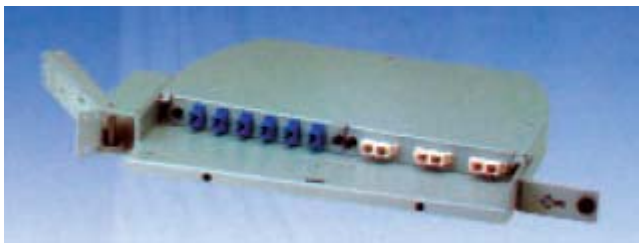
۸- **Patch Cord** مسی : در کابل کشی ساخت یافته ، برای ایجاد اتصال بین ایستگاه های کاری و پریز شبکه یا اتصال تجهیزات فعال به **Patch Panel** داخل رک از این کابل ها استفاده می شود .



۹- داکت یا کانال دیواری : مسیری برای عبور کابل شبکه که در انواع فلزی یا پلاستیکی و در اندازه های مختلف ساخته می شود .

۱۰- **Patch Cord** فیبر نوری : در کابل کشی ساخته یافته برای برقراری ارتباط بین تجهیزات فعال با **Patch Panel** در داخل رک از قطعات کابلی به این شکل استفاده می کنند.

۱۱- **Patch Panel** فیبر نوری : محل برقراری ارتباط بین کابل های فیبر نوری و تجهیزات اکتیو در داخل **Rack**



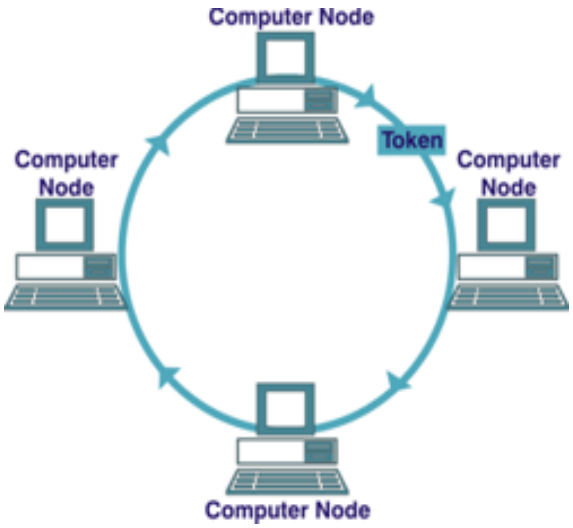
۱۲ - **Patch Panel** برای اتصالات کابل مسی : محل برقراری ارتباط بین رشته کابل های مسی سمت کاربران و تجهیزات اکتیو در داخل **Rack**

ضمیمه۲- تکنولوژیهای انتقال اطلاعات چیست ؟

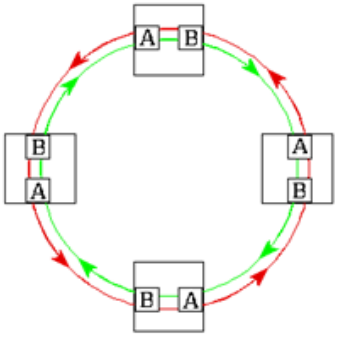
در تکنولوژیهای انتقال اطلاعات مشخص می شود فریم ها چطور قالب بندی می شوند تا بروی سیم قرار گیرند .

۱- تکنولوژیهای انتقال اطلاعات در Lan :

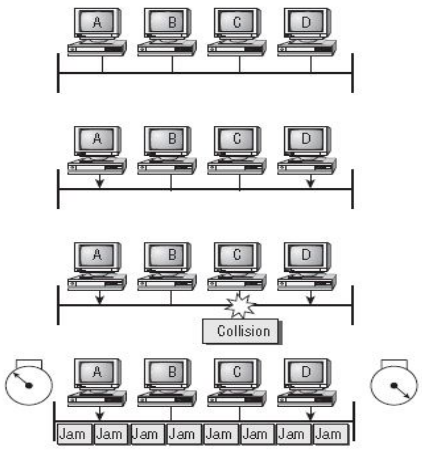
Token Ring : در تکنولوژی **Token Ring** بر اساس **Token-passing** (گذر علامت) صورت می پذیرد که انتقال داده ها توسط **Token** (یک حامل الکترونیکی = نشانه) که در حلقه تشکیل دهنده کامپیوترها گردش می کند ، کنترل میشود. در این شبکه یک حلقه منطقی به وجود می آید و نشانه در امتداد حلقه حرکت کرده و به کامپیوتر ها می رسد . هر کامپیوتری که به ارسال اطلاعات نیاز داشته باشد ، نشانه را نگه داشته و اطلاعات خود را به سوی مقصد ارسال می کند . اطلاعات ارسال شده در همان حلقه مجازی و در امتداد حرکت نشانه مسر خود را طی می کند تا به کامپیوتر مقصد برسد . کامپیوتر مقصد در صورت صحیح بودن اطلاعات ارسالی ، در جواب یک بسته به نام **Acknowledge** (تصدیق کردن) به کامپیوتر مبدا ارسال می کند . کامپیوتر مبداء نیز **Token** (نشانه اصلی) را از بین برده و یک **Token** جدید تولید می نماید و آن را در امتداد مسیر نشانه قبلی به حرکت در می آورد . این روند به همین صورت ادامه خواهد داشت . هیچ گونه **Collision** (تصادم بین **Packet** ها) یا تداخل سیگنا ل در یک حلقه **Token Ring** به وجود نمی آید ، چرا که هر کامپیوتر نوبت خود را برای انتقال دارد و هیچ کامپیوتر دیگری در آن زمان داده ارسال نمی کند. در این تکنولوژی از کابل **UTP** استفاده می شود . این پروتکل با سرعتی حدود **4Mbps** تا **16Mbps**عمل می کند.



FDDI: مخفف **Fiber Distributed Data Interface** می باشد و روش دستیابی در این تکنولوژی بر اساس **Token-passing** که عملکرد همان **Token Ring** است ، می باشد. **FDDI** از یک حلقه دوتایی فیزیکی استفاده می کند. انتقال روی یکی از حلقه ها انجام می گیرد و چنانچه در حلقه اول قطعی صورت بگیرد سیستم بطور اتوماتیک اطلاعات را روی حلقه دوم جابجا کرده و حلقه ی کاملاً جدیدی ایجاد می کند. مزیت عمده **FDDI** سرعت آن است که روی فیبرنوری **100 Mbps** می باشد.



Ethernet : اترنت از یک روش دستیابی که **CSMA/CD** (**carrier sence Multiple Access/collision Detection**) نامیده می شود استفاده می کند و مفهوم آن این است که هر کامپیوتری قبل از فرستادن داده ای در شبکه به کابل گوش می کند. اگر شبکه خالی باشد، کامپیوتر داده ها را می فرستد و اگر **Nod** (به هر عنصری در شبکه که دارای یک کارت شبکه می باشد یک **Nod** یا گره نامیده می شود). دیگری در همان زمان، بر روی کابل چیزی فرستاده باشد، کامپیوتر منتظر خالی شدن خط می ماند و دوباره برای فرستادن سعی می کند. بعضی مواقع دو کامپیوتر همزمان داده های خود را ارسال می کنند که در چنین حالتی برخورد رخ می دهد و در نتیجه هر کامپیوتر مدت زمانی را منتظر مانده و سپس مجدداً داده های خود را روی کابل شبکه ارسال می کند. به هر حال تاخیر به علت برخورد و فرستادن دوباره اطلاعات بسیار کم است و اثر چندانی بر روی سرعت انتقال در شبکه ندارد.



Carrier Sense Multiple Access with Collision Detection (CSMA/CD)

انواع Ethernet عبارت است از :

10 Base T = Ethernet =10 Mbps (Mega byte per second)

100 Base T = Fast Ethernet = 100 Mbps

1000 Base T = Gigabit Ethernet = 1 Gbps

10GB Bast T = 10GB Ethernet = 10 Gbps

۲- تکنولوژیهای انتقال اطلاعات در Wan :

ATM : مخفف **Asynchronous Transfer Mode** می باشد و تکنولوژی است که انتقال اطلاعات را با سرعت **155 Mbps**یا بالاتر انجام می دهد. **ATM** انتقال اطلاعات را دربسته های کوچک با اندازه ثابت انجام می دهد. در حالی که بقیه پروتکل ها بسته هایی با طول متفاوت انتقال می دهند. این پروتکل رسانه های مختلفی مثل ویدیو، صدا و تصویر را پشتیبانی می کند.**ATM** توپولوژی ستاره ای را بکار می گیرد که می تواند با فیبرنوری به خوبیِ کابل زوج به هم تابیده کارکند. **ATM** اغلب برای به هم پیوستن دو یا چند **LAN** بکار می رود. همچنین توسط فراهم کننده سرویس های اینترنت **ISP(Internet Service Provider)** جهت دسترسی پرسرعت به اینترنت بکار می رود.

Frame Relay : تکنولوژی انتقالی برای ارسال اطلاعات با سرعت و با هزینه ی کمتر در چند **frame** از یک یا چند مقصد به یک یا چند نقطه ی پایانی، می باشد. معمولاً فراهم کننده های شبکه ، **frame relay** را برای انتقال صدا و داده ها به صورت تکنیک ارسال فریم بین شبکه های **LAN** و **WAN** به کار می برند

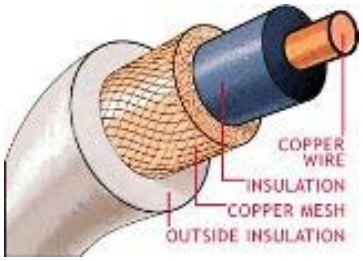
PPP: مخفف **Point-To-Point Protocol** می باشد و تکنولوژی می باشند که امکان استفاده از **TCP/IP** بر روی کابل های سریال نظیر خطوط تلفن را فراهم می نمایند. با استفاده از پروتکل های فوق ، کاربران می توانند توسط یک کامپیوتر و مودم به اینترنت متصل شوند .

ضمیمه ۳ – انواع کابل های شبکه

انواع کابل های (رسانه انتقال) شبکه :

۱- کابل coaxial

یکی از مهمترین محیط های انتقال در مخابرات کابل کواکسیال و یا هم محور می باشد . این نوع کابل ها از سال ۱۹۳۶ برای انتقال اخبار و اطلاعات در دنیار به کار گرفته شده اند. در این نوع کابل ها، دو سیم تشکیل دهنده یک زوج ، از حالت متقارن خارج شده و هر زوج از یک سیم در مغز و یک لایه مسی بافته شده در اطراف آن تشکیل می گردد. ماده ای پلاستیکی این دو هادی را از یکدیگر جدا می کند. این کابل تا مسافت ۵۰۰ متر کاربرد دارد.



کانکتور استاندارد برای کابل های کواکسیال، از نوع **BNC** (**Bayone -Neill - Concelman**) می باشد.

۲- فیبر نوری

یکی از محیط های انتقال در شبکه های کامپیوتری، فیبر نوری است. فیبر نوری را هنگامی استفاده می کنیم که نیاز به ارتباط بین مسافت های بیش از ۱۰۰ متر تا ۱۰ کیلومتر و پهنای باند زیاد داریم. در این فیبرها، نور در اثر انعکاسات کلی در فصل مشترک هسته(**core**) و غلاف (**cladding**)، انتشار پیدا خواهد کرد. منابع نوری در این نوع کابل ها، دیود لیزری و یا دیودهای ساطع کننده نور می باشند.

فیبر های نوری در دو گروه عمده ارائه می گردند:

فیبرهای تک حالته (**Single-Mode**): بمنظور ارسال یک سیگنال در هر فیبر استفاده می شود.

فیبرهای چندحالته (**Multi-Mode**) : بمنظور ارسال چندین سیگنال در یک فیبر استفاده می شود.

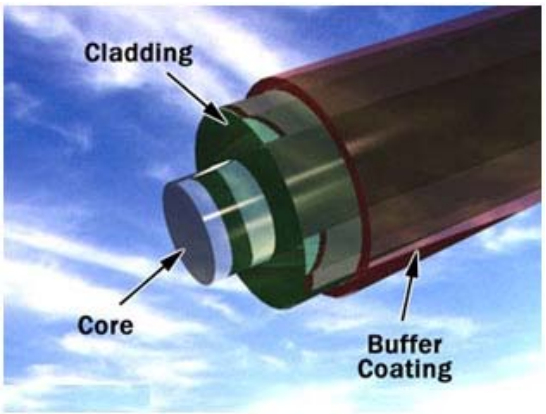
یک فیبر نوری از سه بخش متفاوت تشکیل شده است:

هسته (**Core**): هسته نازک شیشه ای در مرکز فیبر که سیگنا ل های نوری در آن حرکت می نمایند.

روکش (**Cladding**): بخش خارجی فیبر بوده که دورتادور هسته را احاطه کرده و باعث برگشت نورمنعکس شده به هسته می گردد.

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

صدها و هزاران نمونه از رشته های نوری فوق در دسته هائی سازماندهی شده و کابل های نوری را بوجود می آورند. هر یک از کلاف های فیبر نوری توسط یک روکش هائی با نام **Jacket** محافظت می گردند.



۳- کابل Twisted-pair

در ساده ترین شکل کابل **Twisted-pair** دارای یک زوج سیم به هم تابیده از مس که دارای روکش می باشد. دونوع کابل **Twisted-pair** وجود دارد، روکش دار یا **STP** (**Shielded Twisted-pair**)و بدون روکش یا **UTP** (**Unshielded Twisted-pair**). پیچیدگی این کابلها باعث می شود که Noise (سیگنال های نا خواسته) الکتریکی حاصل از جریان واقع در زوج سیمهای دیگر و منابع الکترومغناطیسی مانند، موتورهای الکتریکی، رله ها و ترانسهای برق خنثی گردد.

کابل های UTP (Unshielded Twisted Pair)

کابل **UTP** یکی از متداولترین کابل های استفاده شده در شبکه های مخابراتی و کامپیوتری است . از کابل های فوق ، علاوه بر شبکه های کامپیوتری در سیستم های تلفن نیز استفاده می گردد (**CAT1**). شش نوع کابل **UTP** متفاوت وجود داشته که می توان با توجه به نوع شبکه و اهداف مورد نظر از آنان استفاده نمود . کابل **CAT5** ، متداولترین نوع کابل **UTP** محسوب می گردد .

نکته : منظور از **CAT5** این است که این کابل های داخل این کابل در ۱ اینچ ۵ بار به هم تابیده شده است.

مشخصه های کابل UTP

با توجه به مشخصه های کابل های **UTP** ، امکان استفاده ، نصب و توسعه سریع و آسان آنان ، فراهم می آورد . جدول زیر انواع کابل های **UTP** را نشان می دهد :

موارد استفاده	سرعت انتقال اطلاعات	گروه
سیستم های قدیمی تلفن ، **ISDN** و مودم	حداکثر تا یک مگابیت در ثانیه	**CAT1**
شبکه های **Token Ring**	حداکثر تا چهار مگابیت در ثانیه	**CAT2**
شبکه های **Token Ring** و **10BASE-T**	حداکثر تا ده مگابیت در ثانیه	**CAT3**
شبکه های **Token Ring**	حداکثر تا شانزده مگابیت در ثانیه	**CAT4**
اترنت (ده مگابیت در ثانیه) ، اترنت سریع (یکصد مگابیت در ثانیه) و شبکه های **Token Ring** (شانزده مگابیت در ثانیه)	حداکثر تا یکصد مگابیت در ثانیه	**CAT5**
شبکه های **Gigabit Ethernet**	حداکثر تا یکهزار مگابیت در ثانیه	**CAT5e**
شبکه های **Gigabit Ethernet**	حداکثر تا یکهزار مگابیت در ثانیه	**CAT6**

توضیحات :

- تقسیم بندی هر یک از گروه های فوق بر اساس نوع کابل مسی و **Jack** انجام شده است .
- از کابل های **CAT1** ، به دلیل عدم حمایت ترافیک مناسب، در شبکه های کامپیوتری استفاده نمی گردد .
- از کابل های گروه **CAT4, CAT5 ,CAT2, CAT3** و **CAT6** در شبکه ها استفاده می گردد .کابل های فوق ، قادر به حمایت از ترافیک تلفن و شبکه های کامپیوتری می باشند .
- از کابل های **CAT2** در شبکه های **Token Ring** استفاده شده و سرعتی بالغ بر ۴ مگابیت در ثانیه را ارائه می نمایند .
- برای شبکه هائی با سرعت بالا (یکصد مگا بیت در ثانیه) از کابل های **CAT5** و برای سرعت ده مگابیت در ثانیه از کابل های **CAT3** استفاده می گردد.
- در کابل های **CAT4, CAT3** و **CAT5** از چهار زوج کابل مسی استفاده شده است . **CAT5** نسبت به **CAT3** دارای تعداد بیشتری پیچش در هر اینچ می باشد . بنابراین این نوع از کابل ها سرعت و مسافت بیشتر ی را حمایت می نمایند .
- از کابل های **CAT3** و **CAT4** در شبکه های **Token Ring** استفاده می گردد .
- حداکثر مسافت در کابل های **CAT3** ، یکصد متر است .
- حداکثر مسافت در کابل های **CAT4** ، دویست متر است .
- کابل **CAT6** با هدف استفاده در شبکه های اترنت گیگابیت طراحی شده است . در این رابطه استانداردهائی نیز وجود دارد که امکان انتقال اطلاعات گیگابیت بر روی کابل های **CAT5** را فراهم می نماید(**CAT5e**) .کابل های **CAT6** مشابه کابل های **CAT5** بوده ولی بین ۴ زوج کابل آنان از یک جداکننده فیزیکی به منظور کاهش پارازیت های الکترومغناطیسی استفاده شده و سرعتی بالغ بر یکهزار مگابیت در ثانیه را ارائه می نمایند.

کابل کشی شبکه :

کابل کشی شبکه یکی از مراحل مهم در زمان پیاده سازی یک شبکه کامپیوتری است که می بایست با دقت،ظرافت خاص و پایبندی به اصول کابل کشی ساختیافته ، انجام شود. یکی از عوامل تاثیر گذار در پشتیبانی و نگهداری یک شبکه ، نحوه کابل کشی آن است . با رعایت اصول کابل کشی ساختیافته ، در صورت بروز اشکال در شبکه ، تشخیص و اشکال زدائی آن با سرعتی مناسبی انجام خواهد شد .

کانکتور استاندارد برای کابل های **UTP** ، از نوع **RJ-45** می باشد. کانکتور فوق شباهت زیادی به کانکتورهای تلفن (**RJ-11**) دارد. هر یک از پین های کانکتور فوق می بایست بدرستی پیکربندی گردند.(**Registered Jack**:**RJ**)

RJ11

RJ45

برای ایجاد کابل های **UTP** از تجهیزات زیر استفاده می گردد :

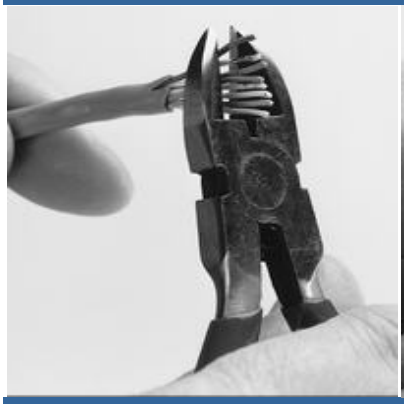
تجهیزات مورد نیاز	
کانکتورهای RJ-45	**کابل** UTP
آچار پرس RJ-45	**سیم لخت کن**

مراحل ایجاد یک کابل :

مرحله اول

مرحله دوم

مرحله سوم



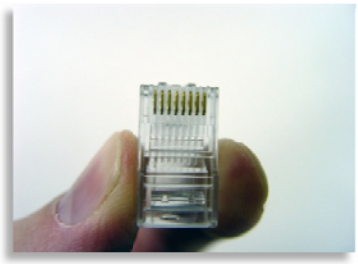
مرحله چهارم

مرحله پنجم

مدل های متفاوت کابل کشی کابل های UTP

به منظور کابل کشی کابل های **UTP** از دو استاندارد متفاوت **T-568A** و **T-568B** استفاده می گردد . نحوه عملکرد دو مدل فوق یکسان بوده و تنها تفاوت موجود به رنگ زوج هائی است که به یکدیگر متصل می شوند.

اگر سوکت شبکه را طوری در دست بگیریم که **Jack** آن به سمت پایین باشد، شماره های کابل از سمت چپ از ۱ تا ۸ می باشد.

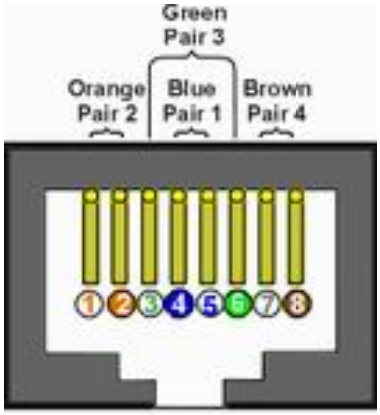


شماره پین های استاندارد T568B

همانگونه که در جدول زیر مشاهده می گردد ، شماره پین های فرد همواره سفید بوده که با یک نوار رنگی پوشش داده می شوند .

کد رنگ ها در استاندارد T568B			
کاربرد	زوج	رنگ	شماره پین
TxData+	دوم	سفید/ نارنجی	یک
TxData-	دوم	نارنجی	دو
RecvData+	سوم	سفید / سبز	سه
	یک	آبی	چهار
	یک	سفید /آبی	پنج
RecvData-	سوم	سبز	شش
	چهارم	سفید/قهوه ای	هفت
	چهارم	قهوه ای	هشت

استاندارد T568B

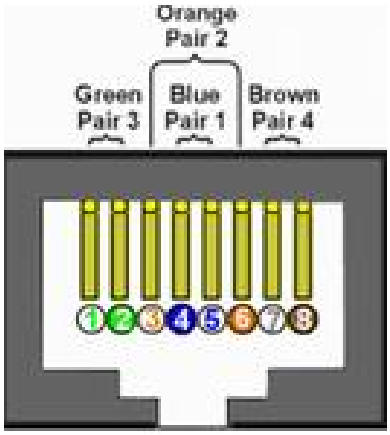


شماره پین های استاندارد T568A

در استاندارد **T568A** ، اتصالات سبز و نارنجی برعکس شده است ، بنابراین زوج های یک و دو بر روی چهار پین وسط قرار می گیرند .

کد رنگ ها در استاندارد T568A			
کاربرد	زوج	رنگ	شماره پین
RecvData+	سوم	سفید / سبز	یک
RecvData-	سوم	سبز	دو
TxData+	دوم	سفید / نارنجی	سه
	یک	آبی	چهار
	یک	سفید /آبی	پنج
TxData-	دوم	نارنجی	شش
	چهارم	سفید/قهوه ای	هفت
	چهارم	قهوه ای	هشت

استاندارد T568A



در شبکه های **10/100Mbit** از زوج های دو و سه استفاده شده و زوج های یک و چهار رزو شده می باشند . در شبکه های گیگااترنت از تمامی چهار زوج استفاده می گردد. کابل های **CAT5** متداولترین نوع کابل **UTP** بوده که دارای انعطاف مناسب بوده و نصب آنان بسادگی انجام می شود .

ایجاد کابل های Straight

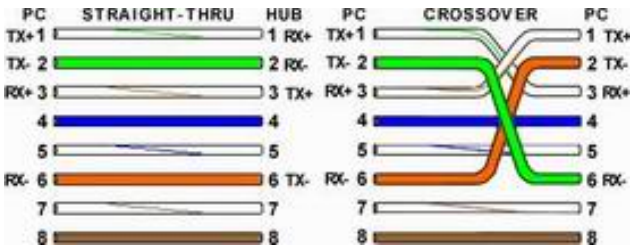
کابل **straight-through** جهت ارتباط دو **Device** غیر مشابه (مانند کامپیوتر به سوییچ) این هم یک کابل **Ethernet** می باشد باز اگر دقت کنید رنگ سیم ها در دو طرف یکسان است . یعنی هر دو طرف استاندارد **A** یا هر دو طرف استاندارد **B** می باشد .

ایجاد کابل X-Over یا Cross Over

کابل **crossover** جهت ارتباط دو **Device** مشابه (مانند دو کامپیوتر با هم) از طریق پورت **Ethernet** خود **NIC** این یک کابل **Ethernet** (کابل **LAN** با کانکتور **RJ-45**) است .هنگامی که شما در رنگ های سیم های آن دقت می کنید متوجه می شوید رنگ نارنجی و سبز در دو طرف کابل در موقعیت مخالف هم قرار دارد . یعنی یک طرف استاندارد A و طرف دیگر استاندارد B می باشد .

شکل زیر تفاوت موجود بین شماره پین های یک کابل **Straight** و **X-over** را نشان می دهد :

تفاوت شماره پین های بین کابلX-over و Straight



جواب سوالات کتاب

جواب های آزمایش ۳ :

جواب ۱- ۳:

Crossover cable

جواب ۲- ۳ :

Answer for PC1:

Reply from 192.168.1.3: bytes=32 time<1ms TTL=128

Reply from 192.168.1.3: bytes=32 time<1ms TTL=128

Reply from 192.168.1.3: bytes=32 time<1ms TTL=128

Reply from 192.168.1.3: bytes=32 time<1ms TTL=128

جواب ۳- ۳ :

Answer for PC1:

Destination host unreachable.

Destination host unreachable.

Destination host unreachable.

Destination host unreachable.

جواب ۴- ۳ :

Straight-through cable

جواب ۵- ۳:

Answer for PC1:

Reply from 192.168.1.3: bytes=32 time<1ms TTL=128

Reply from 192.168.1.3: bytes=32 time<1ms TTL=128

Reply from 192.168.1.3: bytes=32 time<1ms TTL=128

Reply from 192.168.1.3: bytes=32 time<1ms TTL=128

جواب ۶- ۳:

Answer for PC1:

Request timed out.

Request timed out.

Request timed out.

Request timed out.

جواب ۷- ۳ :

IP address اشتباه در **workstation** ، **ping** کردن اشتباه **IP address**، قطع شدن **media** (رسانه) انتقال

جواب ۸- ۳ :

IP address اشتباه در **workstation** ، قطع شدن **media** (رسانه) انتقال ، **switch** خاموش باشد ، **configuration** (پیکربندی) **switch** اشتباه باشد.

جواب های آزمایش ۵ :

جواب ۱- ۵:

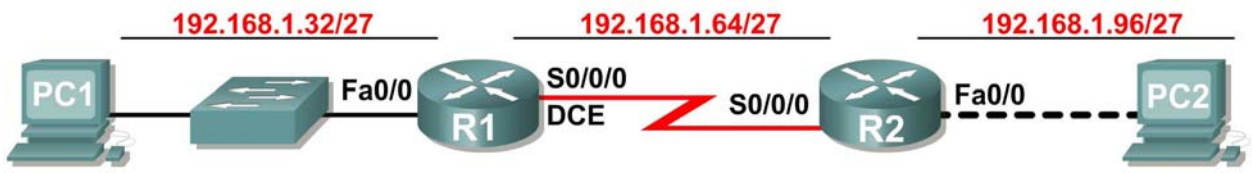
Host IP Address	**172.25.114.250**
Network Mask	**255.255.0.0 (/16)**
Network Address	**172.25.0.0**
Network Broadcast Address	**172.25.255.255**
Total Number of Host Bits **Number of Hosts**	**16 bits or 2_{16} or 65,536** کل **host** ها **65,536 – 2 = 65,534** **host** های قابل استفاده

جواب ۲- ۵ :

Host IP Address	**172.25.114.250**
Subnet Mask	**255.255.255.192 (/26)**
Number of Subnet Bits **Number of Subnets**	**26 bits** **210 = 1024 subnets**
Number of Host Bits per Subnet **Number of Usable Hosts per Subnet**	**6 bits** **26 – 2 = 64 – 2 = 62 hosts per subnet**
Subnet Address for this IP Address	**172.25.114.192**
IP Address of First Host on this Subnet	**172.25.114.193**
IP Address of Last Host on this Subnet	**172.25.114.254**
Broadcast Address for this Subnet	**172.25.114.255**

جواب های آزمایش ۶ :

Topology Diagram



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	Fa0/0	192.168.1.33	255.255.255.224	N/A
	S0/0/0	192.168.1.65	255.255.255.224	N/A
R2	Fa0/0	192.168.1.97	255.255.255.224	N/A
	S0/0/0	192.168.1.94	255.255.255.224	N/A
PC1	NIC	192.168.1.62	255.255.255.224	192.168.1.33
PC2	NIC	192.168.1.126	255.255.255.224	192.168.1.97

جواب ۱-۶ : 3 subnets

جواب ۲-۶ : 255.255.255.224

جواب ۳-۶ : /27

جواب ۴-۶ : 30

جواب ۵-۶ : بله

جواب ۶-۶ : بله

جواب های آزمایش ۱۰ :

جواب ۱- ۱۰ :

Network Address	Mask	First Host Address	Last Host Address	Broadcast
172.20.0.0	255.255.255.128	172.20.0.1	172.20.0.126	172.20.0.127

جواب ۲- ۱۰ : **11111111.1111111.11111111.10000000**

جواب ۳- ۱۰ :

Network Address	Mask	First Host Address	Last Host Address	Broadcast
172.20.0.128	255.255.255.192	172.20.0.129	172.20.0.190	172.20.0.191

جواب ۴- ۱۰ : **11111111.1111111.11111111.11000000**

جواب ۵-۱۰ :

Network Address	Mask	First Host Address	Last Host Address	Broadcast
172.20.0.192	255.255.255.248	172.20.0.193	172.20.0.198	172.20.0.207

جواب ۶- ۱۰ : **11111111.1111111.11111111.11111000**

جواب ۷- ۱۰:

Network Address	Mask	First Host Address	Last Host Address	Broadcast
172.20.0.200	255.255.255.252	172.20.0.201	172.20.0.202	172.20.0.203

جواب ۸- ۱۰ : **11111111.1111111.11111111.11111100**

جواب ۹-۱۰: چون دو **device** شبیه هم هستند پس کابل استفاده شده **crossover** می باشد .

جواب ۱۰- ۱۰ : چون این **device** ها شبیه هم نیستند پس کابل استفاده شده **straight-through** می باشد.

جواب ۱۱- ۱۰ : **Crossover cable**

جواب ۱۲-۱۰ : **Straight-through cable**

جواب ۱۳- ۱۰ : بله

جواب ۱۴- ۱۰ :

Host1	
IP Address	172.20.0.201
IP Mask	255.255.255.252
Gateway Address	172.20.0.202

Host2	
IP Address	172.20.0.193
IP Mask	255.255.255.248
Gateway Address	172.20.0.198

Host3	
IP Address	172.20.0.194
IP Mask	255.255.255.248
Gateway Address	172.20.0.198

جواب ۱۵- ۱۰ :

From	To	IP Address	Ping Results
Host1	Gateway (Router1, Fa0/0)	172.20.0.202	Should be successful
Host1	Router1, Fa0/1	172.20.0.198	Should be successful
Host1	Host2	172.20.0.193	Should be successful
Host1	Host3	172.20.0.194	Should be successful
Host2	Host3	172.20.0.194	Should be successful
Host2	Gateway (Router1, Fa0/1)	172.20.0.198	Should be successful
Host2	Router1, Fa0/0	172.20.0.202	Should be successful
Host2	Host1	172.20.0.201	Should be successful
Host3	Host2	172.20.0.193	Should be successful
Host3	Gateway (Router1, Fa0/1)	172.20.0.198	Should be successful
Host3	Router1, Fa0/0	172.20.0.202	Should be successful
Host3	Host1	172.20.0.201	Should be successful

جواب ۱۶- ۱۰ : در صورتی که **Ping** کردن ، **Host1** و **Host2** موفقیت آمیز باشد .