

بسمه الله الرحمن الرحيم

شبیه سازی شبکه های کامپیوتری توسط نرم افزار Packet Tracer همراه با آموزش مفاهیم کاربردی شبکه

تالیف و ترجمه:

مرتضی سرگلزایی جوان
دانشگاه صنعتی امیرکبیر

احمد بختیاری شهری
دانشگاه سیستان و بلوچستان

این کتاب آموزشی یک کتاب رایگان است و میتوان مطالب موجود در آن را با بدون اجازه مولف، توزیع کرده و یا تغییر داد. این کتاب به این امید تهیه شده است که بتواند در ارتقای سطح علمی دوستان موثر واقع شود، اما هیچ تضمینی در مورد آن و یا در مورد مناسب بودن مطالب موجود برای اهداف خاص وجود ندارد. از خواننده محترم تقاضا می شود با ارسال نظرات و پیشنهادات خود در مورد این کتاب و یا اشکالات موجود در محتوی یا متن آن به آدرس info@msjavan.tk در بهبود این کتاب سهیم شود.

با تشکر

احمد بختیاری، مرتضی سرگلزایی جوان

زمستان ۱۳۸۸

عنوان کتاب: شبیه سازی شبکه های کامپیوتری توسط نرم افزار Packet Tracer

همراه با آموزش مفاهیم کاربردی شبکه

تالیف و ترجمه: احمد بختیاری شهری - مرتضی سرگلزایی جوان

نوع نشر: Open Source

تعداد صفحات: ۳۲۲

قطع: وزیری

تاریخ نشر: اول - زمستان ۱۳۸۸



✓ شبیه سازی شبکه های کامپیوتری

✓ عناوین اصلی:

- IX ✓ مقدمه
- X ✓ چگونه کار با رایانه را یاد بگیریم؟
- ۱ ✓ فصل اول: آموزش مفاهیم کاربردی شبکه
- ۴۹ ✓ فصل دوم: شبیه سازی شبکه توسط نرم افزار Packet Tracer
- ۱۹۰ ✓ ضمائم



✓ شبیه سازی شبکه های کامپیوتری

۱	مفاهیم اولیه شبکه
۳	الف- اجزای منطقی شبکه
۳	ب- اجزای فیزیکی
۳	کابل شبکه
۱۰	آشنایی با مفهوم CLIENT / SERVER
۱۱	آشنایی با تفاوت DEDICATED و NON DEDICATED و مقایسه آنها
۱۱	۱- پروتکل NETBEUI
۱۴	۲- IPX/SPX
۱۵	۳- پروتکل TCP/IP
۱۵	سرویس های TCP/IP
۱۶	HTTP (HYPER TEXT TRANSFER PROTOCOL)
۱۷	TELNET
۲۰	TCP/IP HOST
۲۴	شروع مکانیزم ارسال اطلاعات در TCP/IP
۲۹	پروتکل ARP (ADDRESS RESOLUTION PROTOCOL)
۳۱	نکاتی دیگر در مورد IP ADDRESS
۳۳	مدیریت فضای IP در جهان
۳۴	DHCP SERVER مسأله ای دیگر در TCP/IP
۳۵	سرویس DNS
۳۸	لایه های شبکه در مدل مرجع OSI
۴۱	مدل TCP/IP
۴۳	نحوه عملکرد سوئیچ در شبکه
۴۵	پیکربندی سوئیچ
۴۵	ارسال و دریافت همزمان در سوئیچ
۴۵	PORT TRUNKING
۴۶	اندازه فیزیکی سوئیچ
۴۶	اولویت بندی ترافیک شبکه
۴۶	رمزنگاری
۴۹	آشنایی با نرم افزار PACKET TRACER
۵۰	شروع کار با PACKET TRACER



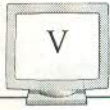
✓ شبیه سازی شبکه های کامپیوتری

۵۲	فضاهای کاری و حالت ها
۵۲	تنظیم علاقه مندی ها
۵۵	تنظیم پس زمینه
۵۵	اصطلاحات مهم
۵۶	ایجاد اولین شبکه
۵۸	ارسال پیغام های ساده در حالت REAL TIME
۵۹	ثبت رویداد ها و مشاهده انیمیشن در حالت شبیه سازی
۶۰	مشاهده داخل بسته ها در حالت شبیه سازی
۶۲	مشاهده جدول دستگاه ها و تنظیم مجدد شبکه
۶۳	مرور مطالب
۶۴	فضاهای کار فیزیکی و منطقی
۶۴	فضای کار منطقی
۶۴	ایجاد دستگاه ها
۶۵	ایجاد دستگاه های سفارشی
۶۶	افزودن ماژول ها
۶۷	ایجاد اتصالات
۶۸	ابزارهای ویرایش توپولوژی منطقی
۶۹	پیکربندی دستگاه ها
۶۹	CISCO IOS مسیریاب ها و سوئیچ ها
۶۹	گروه بندی دستگاه ها (CLUSTERING)
۷۱	فضای کار فیزیکی
۷۳	جابجا کردن اشیاء در فضای کار فیزیکی
۷۵	دستگاه های بی سیم در فضای کار فیزیکی
۷۶	نکات مهم در فضای کار فیزیکی
۷۷	حالت های عملکرد
۷۷	حالت REALTIME
۷۷	کسب اطلاعات از دستگاه ها
۷۸	ارسال گرافیکی PDU ها



✓ شبیه سازی شبکه های کامپیوتری

۷۸	خاموش و روشن کردن دستگاه ها (POWER CYCLE DEVICES)
۷۹	حالت شبیه سازی (SIMULATION).....
۸۰	EVNT LIST و روند زمانی رویداد
۸۱	اجرای مجدد سناریو
۸۱	ارسال PDU های ساده (PING)
۸۲	اطلاعات بسته در حالت شبیه سازی.....
۸۳	حالت CHALLENGE.....
۸۵	مدیریت سناریو ها در حالت شبیه سازی.....
۸۷	COMPLEX PDU در حالت شبیه سازی.....
۸۸	انواع اتصالات.....
۸۹	وضعیت اتصال
۹۰	دستگاه ها و ماژول ها.....
۹۰	لیست ماژول ها و پیکربندی های فیزیکی
۹۱	پیکربندی دستگاه ها.....
۹۱	ترتیب BOOTING و بارگزاری تصویر IOS در مسیریاب ها و سوئیچها
۹۱	گزارشگیری دستورات IOS
۹۳	پیکربندی مسیریاب
۹۷	پیکربندی سوئیچ
۱۰۰	پیکربندی LINKSYS WRT300N
۱۰۶	پیکربندی PC
۱۱۱	پیکربندی سرورها
۱۱۵	پیکربندی ابر (CLOUD)
۱۱۷	پیکربندی دستگاه های دیگر
۱۱۷	پل ها
۱۱۷	تکرار کننده
۱۱۷	هاب



✓ شبیه سازی شبکه های کامپیوتری

۱۱۷	نقطه دسترسی
۱۱۷	چاپگر
۱۱۷	IP PHONE
۱۱۷	DSL MODEM
۱۱۷	CABLE MODEM
۱۱۸	مثال عملی) قسمت اول- ایجاد یک شبکه
۱۲۸	مثال عملی) قسمت دوم- توسعه توپولوژی شبکه
۱۳۶	مثال عملی) قسمت سوم- شبیه سازی یک شبکه ISP و شبکه خانگی
۱۶۶	ACTIVITY WIZARD
۱۶۸	پانل دستورالعمل ها (INSTRUCTIONS)
۱۶۹	پانل شبکه پاسخ (ANSWER NETWORK)
۱۷۰	تنظیم آیتم های ارزیابی
۱۷۰	تنظیمات زمان
۱۷۰	بررسی اتصالات
۱۷۱	فیدبک کلی (OVERALL FEEDBACK)
۱۷۲	پانل شبکه اولیه (INITIAL NETWORK)
۱۷۳	استفاده از LOCKING TREE
۱۷۳	تعیین کلمه عبور
۱۷۴	آزمایش فعالیت (TEST THE ACTIVITY)
۱۷۴	اجرای فایل فعالیت
۱۷۵	OVERALL FEEDBACK
۱۷۵	آیتم های ارزیابی
۱۷۶	بررسی اتصال
۱۷۷	مدیریت متغیر ها (VARIABLE MANAGER)
۱۷۷	ایجاد استخر (POOL)
۱۷۸	ایجاد متغیرها
۱۷۹	اختصاص متغیرها
۱۷۹	نحوه افزودن متغیرها به آیتم های ارزیابی
۱۷۹	انواع آیتم های ارزیابی



شبیه سازی شبکه های کامپیوتری

ضمیمه ۱- مسیر یاب و ماژول های مرتبط با آن..... ۱۹۰

۱۹۰	مسیر یاب 1841
۱۹۱	مسیر یاب 20XM 2
۱۹۴	مسیر یاب 21XM 2
۱۹۴	مسیر یاب 2821
۱۹۸	مسیر یاب ROUTER-PT
۲۰۰	سوئیچ ها و ماژول های مرتبط با آن
۲۰۰	سوئیچ 24 2950
۲۰۰	سوئیچ 24-2950T
۲۰۰	سوئیچ 24TT 0 29
۲۰۰	سوئیچ SWITCH-PT
۲۰۱	پل BRIDGE-PT
۲۰۲	دستگاه های نهایی (END DEVICES) و ماژول های مرتبط با آنها
۲۰۲	PC-PT
۲۰۴	SERVER-PT
۲۰۴	PRINTER-PT
۲۰۴	IPPHONE-PT
۲۰۵	سایر دستگاه ها و ماژول های مرتبط با آنها
۲۰۵	HUB-PT
۲۰۶	REPEATER-PT
۲۰۶	ACCESSPOINT-PT
۲۰۶	LINKSYSWRT300N
۲۰۷	CLOUD
۲۰۸	DSL-MODEM-PT
۲۰۹	CABLE-MODEM-PT

ضمیمه ۲- کلیدهای میانبر..... ۲۱۰

ضمیمه ۳- ثابت های زمانی..... ۲۱۲

ضمیمه ۴- دستورات IOS مسیر یاب..... ۲۱۵

ضمیمه ۵- دستورات IOS سوئیچ..... ۲۴۰

ضمیمه ۶- فلوچارت های نحوه پردازش در دستگاه ها..... ۲۵۰

۲۵۰	لایه ۱ الگوریتم پردازش بسته در هاب در زمان دریافت بسته
۲۵۰	لایه ۱ الگوریتم پردازش بسته در تکرار کننده در زمان دریافت بسته
۲۵۰	لایه ۲ الگوریتم پردازش فریم های دریافتی در سوئیچ
۲۵۲	لایه ۲ الگوریتم چگونگی ارسال فریم در سوئیچ
۲۵۳	لایه ۲ الگوریتم چگونگی ایجاد درخت پوشا (پروتکل STP)
۲۵۴	لایه ۲ نحوه عملکرد امنیت پورت
۲۵۵	لایه ۲ چگونگی تصمیم گیری DTP در مورد حالت پورت
۲۵۶	لایه ۲ چگونگی پردازش فریم های VTP ورودی در سوئیچ
۲۵۷	لایه ۲ چه زمانی سوئیچ ها فریم های VTP ارسال می کنند؟
۲۵۷	لایه ۳ چگونگی پردازش بسته های RIP ورودی توسط روتر
۲۵۸	لایه ۳ چگونگی پردازش بسته های EIGRP ورودی توسط روتر
۲۶۱	لایه ۳ چگونگی پردازش بسته های OSPF ورودی توسط روتر
۲۶۳	لایه ۳ چگونگی پردازش بسته های ICMP ورودی در دستگاه ها
۲۶۳	لایه ۴ چگونگی پردازش سگمنت های UDP توسط دستگاه ها
۲۶۵	لایه ۴ چگونگی پردازش سگمنت های TCP توسط دستگاه ها
۲۶۶	لایه ۷ چگونگی پردازش بسته های دریافتی توسط کلاینت های DHCP
۲۶۶	لایه ۷ چگونگی پردازش بسته های دریافتی توسط سرور DHCP
۲۶۷	لایه ۷ چگونگی عملکرد کلاینت TELNET
۲۶۷	لایه ۷ چگونگی عملکرد سرور TELNET
۲۶۸	لایه ۷ چگونگی عملکرد DNS
۲۶۸	لایه ۷ چگونگی عملکرد HTTP
۲۷۰	لایه ۷ چگونگی عملکرد TFTP SERVER
۲۷۰	لایه ۷ چگونگی پردازش بسته های ورودی توسط سرور و کلاینت TFTP
۲۷۱	چگونگی پردازش بسته های ورودی توسط مسیریاب (پردازش NAT)
۲۷۱	چگونگی پردازش بسته های خروجی توسط مسیریاب (پردازش NAT)
۲۷۳	چگونگی استفاده از ARP برای ارسال بسته های IP توسط دستگاه ها
۲۷۳	چگونگی ارسال تقاضاهای ARP توسط دستگاه ها
۲۷۳	چگونگی پردازش بسته های ورودی ARP توسط دستگاه ها
۲۷۴	چگونگی پردازش درخواست های ARP توسط مسیریاب
۲۷۵	نحوه عملکرد ACL



✓ شبیه سازی شبکه های کامپیوتری

۲۷۶	ضمیمه ۷) آزمایشگاه (CCNA)
۲۷۶	CCNA1-5.1.12) ایجاد یک شبکه PEER TO PEER
۲۷۸	CCNA1-5.1.13A) ایجاد یک شبکه مبتنی بر هاب
۲۸۰	CCNA1-5.1.13B) ایجاد یک شبکه مبتنی بر سوئیچ
۲۸۲	CCNA1-5.1.5-5.1.7) تکرار کننده ها و هاب ها ۱
۲۸۴	CCNA1-5.1.) تکرار کننده
۲۸۶	CCNA1-5.1.8) بی سیم
۲۸۷	CCNA1-5.1.9-5.1.10) پل ها و سوئیچ ها
۲۸۹	CCNA1-5.2.3A) اتصال واسط های مسیریاب ها
۲۹۰	CCNA2-4.2.) رفع اشکال مربوط به آدرس IP
۲۹۲	CCNA2-1.3-1.4) پیکربندی مسیره های پیشفرض و استاتیک
۲۹۴	CCNA2-3.2) پیکربندی مسیریابی
۲۹۵	CCNA2-7.2.2) پیکربندی RIP
۲۹۷	CCNA2-7.2.9) تعدیل بار بین چند مسیر (LOAD BALANCING)
۲۹۹	ضمیمه ۸- نصب DHCP SERVER
۳۰۲	ضمیمه ۹- راه اندازی ACTIVE DIRECTORY
۳۰۶	ضمیمه ۱۰- تنظیم ویندوز XP برای اتصال به VPN سرور

به نام او که زیباست و زیبایی را دوست دارد

مقدمه:

مدیریت شبکه های کامپیوتری هنری است که لازمه هر مدیر شبکه است در صورتی که یک شخص به عنوان مدیر شبکه از توانمندی هایی از جمله تقسیم ترافیک ورودی، آشنایی با خطوط ارتباطی مختلف، ارائه پیکر بندی مناسب، تنظیم دقیق سوئیچ ها و روترها، سطح دسترسی کاربران جهت استفاده از امکانات شبکه، تنظیمات فایروال جهت جلوگیری از نفوذ ویروس ها، هکرها و نیز پیکر بندی سرورها برخوردار نباشد، مسلماً مدیر موفق در این زمینه نخواهد بود.

در این کتاب سعی گردیده است که ضمن بیان مفاهیم کاربردی شبکه به صورت مختصر و مفید، ایده های عملی جهت دستیابی به حداکثر توانایی برای پیاده سازی و اجرای یک شبکه مطلوب و بهینه ارائه گردد. برای همین منظور از نرم افزار Packet Tracer که یک محیط شبیه سازی جهت طراحی، پیاده سازی توپولوژی، پیکربندی، بررسی مشکلات و ... در شبکه می باشد، استفاده گردیده است. کاربران می توانند با استفاده از ابزارهای مورد نظر در محیط شبیه سازی، به راحتی توپولوژی دلخواه خود را ایجاد و پس از پیکربندی شبکه ایجاد شده، به بررسی، تحلیل و رفع مشکلات آن پردازند.

استفاده از این کتاب برای مدیران شبکه جهت تحلیل و بررسی قبل از راه اندازی یک شبکه حقیقی و نیز اساتید جهت ارائه دروس آزمایشگاهی شبکه توصیه می شود، و نیز به عنوان یک محیط آزمایشگاهی ایده آل برای دانشجویان رشته های مرتبط با فن آوری اطلاعات و کامپیوتر قابل استفاده می باشد.



✓ شبیه سازی شبکه های کامپیوتری

چگونه کار با رایانه را یاد بگیریم :

۱- واقع بین باشید!

در زمان شروع کار با رایانه اصطلاحات فنی و دشوار زیادی را پیش روی خود خواهید دید. یادگیری رایانه همانند رانندگی به زمان نیاز دارد. همانطور که رانندگان نیازی به دانستن مکانیزم داخلی خودروها ندارند، لازم نیست برای کار با رایانه بیش از حد به جزئیات مربوط به نحوه عملکرد سیستم پردازید (گرچه عده زیادی از کاربران به این مورد نیز جذب میشوند)

۲- نگران از کار افتادن رایانه نباشید!

فقط مراقب باشید که مانیتور از روی میز به زمین پرتاب نشود و یا فنجان قهوه (چای) روی صفحه کلید نریزد. در صورت نیاز، مربی یا معلم در راه اندازی مجدد رایانه به شما کمک خواهند کرد.

۳- از برداشتن گام های بزرگ اجتناب کنید!

سعی کنید مدت زمان فراگیری از ۱ تا ۱/۵ ساعت در روز تجاوز نکند. بین ساعات کار با رایانه، حتما زمان تنفس و استراحت داشته باشید. برای کاهش فشار به چشم سعی کنید به دفعات زیاد پلک بزنید تا چشمهایتان خشک نشده و بتوانند دوباره تمرکز کنند.

۴- تمرین کنید!

برای کسب توانایی لازم در هر زمینه ای نیاز به تمرین دارید چه یادگیری رایانه باشد و چه یادگیری درس ریاضی، یا زبان انگلیسی و یا یک رشته ورزشی!

۵- به آسانی مایوس نشوید!

احساس ناتوانی در مقابل انجام یک کار، واکنشی عادی است. شما فرصت های متنوعی در زمینه کار با رایانه و یا اینترنت دارید. فرصت کافی به خودتان بدهید و سعی کنید از این تجربه لذت ببرید.

۶- از کمکهای جانبی استفاده کنید!

کمک گرفتن از دیگران خارج از محیط کلاس طی سالهای تحصیل، امری بسیار عادی است. بنابراین برای یادگیری رایانه نیز به کمک نیاز دارید. از طرف دیگر، بسیاری از برنامه های آموزشی نیز خدمات آموزش خصوصی مفیدی ارائه میکنند.

۷- از سؤال کردن در کلاس واهمه نداشته باشید!

اگر فکر میکنید کلاس سریع پیش می رود و در بخشی عقب ماندید، از معلم بخواهید دوباره توضیح دهد. اگر برایتان سئوالی پیش می آید آنرا سریع یادداشت کنید تا در وقت مناسب از معلم پرسید و تا جواب سؤال خود را نگرفتید قانع نشوید. یک برنامه آموزشی خوب، برنامه ای است که حداکثر بهره برداری را از آن بکنید.



۸- نگران تفاوت های موجود بین رایانه خانگی خود و رایانه های کلاس درس نباشید!
احتمال وجود تفاوت بین مدل های رایانه موجود در خانه کاربران و کلاس های درسی بسیار بالاست. زیرا تولید کنندگان رایانه در سال، چنین مرتبه مدل های خود را تغییر میدهند. همواره سعی کنید از یک برنامه آموزشی استاندارد با سیستم عامل های همسان بهره ببرید.

۹- در انتخاب یک برنامه آموزشی دقت کنید!

قبل از ثبت نام، برای درک برنامه آموزشی و خصوصیات برنامه و مربی آن، بطور آزمایشی یک جلسه در کلاس شرکت کنید. یک مربی خوب باید به جدیدترین فناوری ها و نرم افزارها تسلط داشته باشد و از یادگیری از کارآموزان خود هراسی نداشته باشد.

۱۰- پس از کلاس، نظرتان را با مربی خود در میان بگذارید!

از ابراز اظهار نظرهای منطقی خود هراس نداشته باشید. از آموزش لذت ببرید و تجربه های موفقیت آمیز خود را به دیگران بگویید.



✓ فصل اول: آشنایی با مفاهیم کاربردی شبکه

مفاهیم اولیه شبکه

مجموعه‌ای از کامپیوترهای خود مختار متصل به هم که امکان تبادل اطلاعات بین آنها وجود دارد. برخی از مزایای تشکیل شبکه‌ها عبارتند از:

- امکان ارتباط کامپیوترها در نقاط مختلف و حذف مسافت‌های فیزیکی
- امکان تبادل اطلاعات و منابع برای بهره‌برداری مشترک با اطمینان بالاتر
- افزایش کارایی، سرعت و دقت در تبادل اطلاعات
- امکان مدیریت متمرکز اطلاعات و اعمال سیاست‌های امنیتی

شبکه‌ها از نظر نوع ارتباط به دو دسته تقسیم می‌شوند:

- شبکه نظیر به نظیر^۱
- شبکه مشتری کارگزار^۲

همچنین شبکه‌ها را از لحاظ گستردگی و وسعت نیز می‌توان به ترتیب زیر تقسیم نمود:

الف- شبکه‌های محلی^۳ یا LAN

ب- شبکه‌های بین‌شهری^۴ یا MAN

ج- شبکه‌های گسترده^۵ یا WAN

شبکه‌های درون سازمان اینترنت^۶ و اگر به شبکه بیرونی مثلا اینترنت وصل شود اکسترانت^۷ نامیده می‌شود.

¹ - Peer- to -Peer

² - Client /Server

³ - Local Area Network

⁴ - Metropolitan Area Network

⁵ - Wide Area Network

⁶ -Intranet

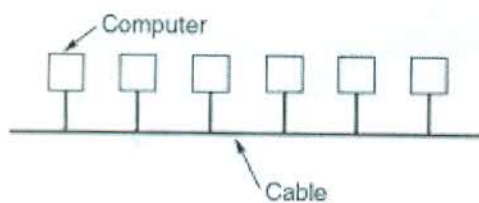
⁷ -Extranet



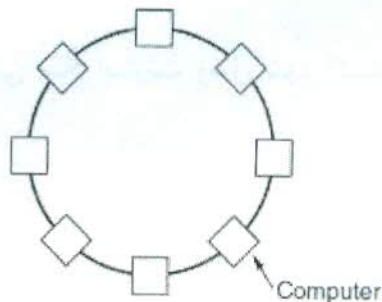
✓ فصل اول: آشنایی با مفاهیم کاربردی شبکه

Interprocessor distance	Processors located in same	Example
1 m	Square meter	Personal area network
10 m	Room	
100 m	Building	Local area network
1 km	Campus	
10 km	City	Metropolitan area network
100 km	Country	Wide area network
1000 km	Continent	
10,000 km	Planet	The Internet

شبکه های محلی دارای سه خصوصیت متمایز کننده هستند: اندازه مشخص دارند در نتیجه حداکثر تاخیر آنها مشخص است. تکنولوژی انتقال در آنها بر اساس انتشار عمومی^۱ می باشد. معمولا همبندی یا توپولوژی Bus یا Ring دارند.



(a)



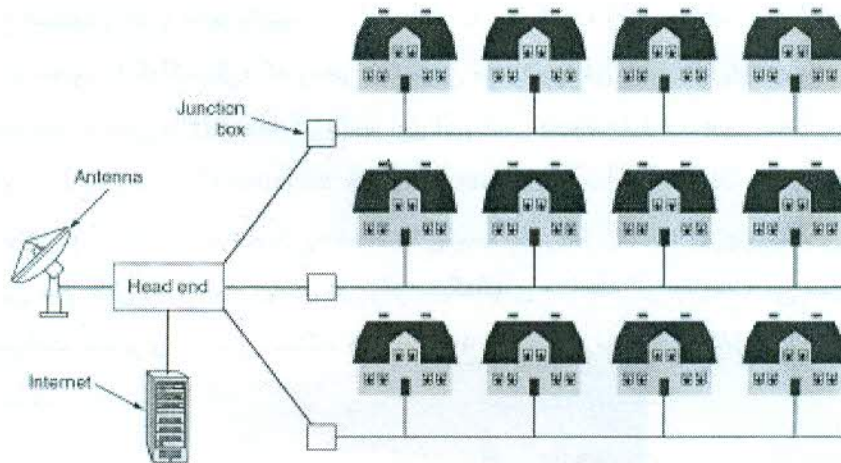
(b)

شکل ۲: (a) شبکه بر اساس توپولوژی BUS، (b) شبکه بر اساس توپولوژی Ring

شبکه های شهری دارای یک یا چند مسیر و المان سوئیچینگ هستند لذا در این شبکه ها حداکثر میزان تاخیر به طور مشخص قابل تعیین نیست. شبکه اینترنت مجموعه ای از شبکه های شهری متصل به هم می باشد.



✓ فصل اول: آشنایی با مفاهیم کاربردی شبکه



الف - اجزای منطقی شبکه

پروتکل شبکه: به معنی قواعد و قوانین خاصی که ارتباط کامپیوترها بر اساس آن صورت می‌گیرد مانند پروتکل های TCP/IP و IPX / SPX.

سیستم عامل: سیستم عامل شبکه که بر روی سرور نصب شده و مدیریت شبکه را به عهده دارد.

ب - اجزای فیزیکی

اجزاء فیزیکی شبکه ها نیز به ترتیب زیر طبقه بندی می شوند:

کامپیوترهای سرور، ایستگاه های کاری و امکانات جانبی مانند چاپگر محیط ارتباطی باسیم یا بی سیم

سایر اجزاء مانند: مودم، روتر، پل یا بریج، کارت شبکه، هاب، سوئیچ و غیره. که هر یک بر حسب اهمیت کاربرد در شبکه، تشریح می گردند.

کابل شبکه

کابل شبکه، رسانه ای است که از طریق آن اطلاعات از یک دستگاه موجود در شبکه به دستگاه دیگر انتقال می یابد. انواع مختلفی از کابل ها به طور معمول در شبکه های محلی استفاده می شوند. در برخی موارد شبکه تنها از یک نوع کابل استفاده می کند و در مواقعی نیز انواع مختلفی از کابل ها در شبکه به کار گرفته می شود. غیر از عامل توپولوژی، پروتکل و اندازه شبکه نیز در انتخاب کابل شبکه مؤثرند. آگاهی از ویژگی های انواع مختلف کابل ها و ارتباط آنها با دیگر



✓ فصل اول: آشنایی با مفاهیم کاربردی شبکه

جنبه های شبکه برای توسعه یک شبکه موفق ضروری است. امروزه سه گروه از کابل ها، در ایجاد شبکه مطرح هستند:

کابل های هم محور یا کواکسیال؛ که زمانی بیشترین مصرف را در میان کابل های موجود در شبکه داشتند. چند دلیل اصلی برای استفاده زیاد از این نوع کابل وجود دارد:

- قیمت ارزان آن.
- سبکی و انعطاف پذیری.
- این نوع کابل به نسبت زیادی در برابر سیگنالهای مداخله گر مقاومت می نماید.
- مسافت بیشتری را بین دستگاه های موجود در شبکه، نسبت به کابل UTP پشتیبانی می نماید.



شکل ۴: تصویر کابل کواکسیال و اجزاء آن

اجزای کابل کواکسیال به شرح زیر می باشد:

- هسته مرکزی^۱ که معمولاً از یک رشته سیم جامد مسی تشکیل می گردد.
- عایق^۲ که معمولاً از جنس پی وی سی یا تفلون است.
- Copper WireMesh که از سیم های بافته شده تشکیل می شود و کار آن جمع آوری امواج الکترومغناطیسی است.
- Jacket که جنس آن اغلب از پلاستیک بوده و پوشش خارجی سیم در برابر خطرات فیزیکی است.

کابل کواکسیال به دو دسته تقسیم می شود:

- Thin net: کابلی است بسیار سبک، انعطاف پذیر و ارزان قیمت، قطر سیم در آن ۶ میلیمتر معادل ۰/۲۵ اینچ است. مقدار مسیری که توسط آن پشتیبانی می شود ۱۸۵ متر است.

^۱ - Conducting Core

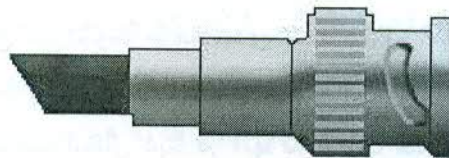
^۲ - Insulation



✓ فصل اول: آشنایی با مفاهیم کاربردی شبکه

• Thick net: این کابل قطری تقریباً ۲ برابر Thin net دارد. کابل مذکور، پوشش محافظی را (علاوه بر محافظ خود) داراست که از جنس پلاستیک بوده و بخار را از هسته مرکزی دور می سازد.

رایج ترین نوع اتصال دهنده مورد استفاده در کابل کوکسیال، BNC می باشد. انواع مختلفی از سازگارکننده ها برای BNC ها شامل: Barrel connector، Tconnector و Terminator وجود دارند. در شبکه هایی با توپولوژی Bus از کابل کوکسیال استفاده می شود.



شکل ۵: اتصال دهنده BNC

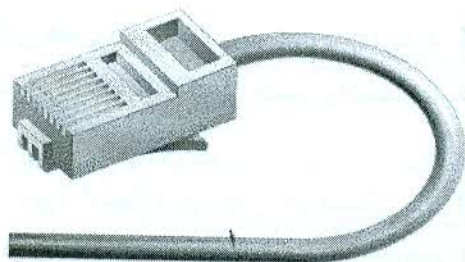
در طراحی جدید شبکه معمولاً از کابل های زوج سیم به هم تابیده شده، استفاده می گردد. قیمت آن ارزان بوده و از نمونه های آن می توان به کابل تلفن اشاره کرد. کابل های مورد استفاده در شبکه های کامپیوتری که از چهار جفت سیم به هم تابیده تشکیل می گردد، خود به دو دسته تقسیم می شود:

UTP: کابل ارزان قیمتی است که نصب آسانی دارد و برای شبکه های محلی باسیم، بسیار مناسب است، همچنین نسبت به نوع دوم کم وزن تر و انعطاف پذیرتر است. مقدار سرعت دیتای عبوری از آن ۴ مگابیت در ثانیه تا ۱۰۹۰ مگابیت در ثانیه می باشد. این کابل می تواند تا مسافت حدوداً ۱۰۰ متر یا ۳۲۸ فوت را بدون افت سیگنال انتقال دهد. کابل مذکور نسبت به تداخل امواج الکترومغناطیس حساسیت بسیار بالایی دارد و در نتیجه در مکان های دارای امواج الکترومغناطیس، امکان استفاده از آن وجود ندارد.

در سیم تلفن که خود نوعی از این کابل است از اتصال دهنده RJ11 استفاده می شود، اما در کابل شبکه اتصال دهنده ای با شماره RJ45 بکار می رود که دارای هشت مکان برای چهار زوج سیم است.

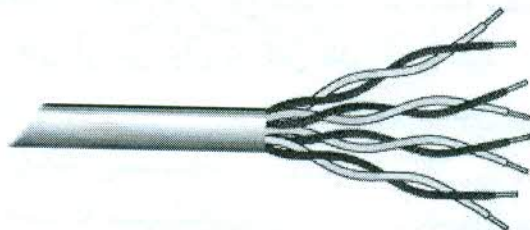


✓ فصل اول: آشنایی با مفاهیم کاربردی شبکه



شکل ۶: اتصال دهنده شبکه RJ45

کابل های زوج به هم تابیده^۱ با توجه به ضخامت و میزان به هم تابیدگی آنها، در گروه های مختلفی که با CAT^۲ شروع می شوند طبقه بندی شده اند. CAT1 یا نوع اول کابل UTP برای انتقال صدا بکار می رود، اما CAT2 تا CAT7 برای انتقال دیتا در شبکه های کامپیوتری مورد استفاده قرار می گیرند و سرعت انتقال دیتا در آنها به ترتیب عبارتست از: ۴، ۱۰، ۱۶، ۱۰۰ و ۱۰۰۰ مگابیت در ثانیه. لازم به ذکر است که برای شبکه های کوچک و خانگی استفاده از کابل CAT3 توصیه می شود.



شکل ۷: کابل هم محور CAT5

STP: در این کابل سیم های انتقال دیتا مانند UTP هشت سیم و یا چهار جفت دوتایی هستند. باید دانست که تفاوت آن با UTP در این است که پوسته ای به دور آن پیچیده شده که از اثرگذاری امواج بر روی دیتا جلوگیری می کند. از لحاظ قیمت، این کابل از UTP گران تر و از فیبر نوری ارزان تر است. مقدار مسافتی که کابل مذکور بدون افت سیگنال طی می کند برابر با ۵۰۰ متر معادل ۱۶۴۰ فوت است. در شبکه هایی با توپولوژی BUS و RING از دو نوع اخیر استفاده می شود. گفته شد که در این نوع کابل، ۴ جفت سیم به هم تابیده بکار می رود که از دو جفت آن یکی برای فرستادن اطلاعات و دیگری برای دریافت اطلاعات عمل می کند.

^۱ - Twisted Pair

^۲ - Category



✓ فصل اول: آشنایی با مفاهیم کاربردی شبکه

دلیل تابیده بودن زوج‌ها در کابل‌های زوج بهم تابیده، کم کردن اثر نویز محیط است. زیرا دو کابل به هم تابیده به دلیل تاثیر مشابه از محیط، نویز مساوی دریافت نموده و بدین ترتیب در گیرنده، چون سیگنال منتقل شده، از تفاضل ولتاژ دو رشته حاصل می‌شود بنابراین نویز حذف می‌شود. در شبکه‌هایی با نام اینترنت سریع، دو نوع کابل به چشم می‌خورد: 100Base TX: یعنی شبکه‌ای که در آن از کابل UTP نوع CAT5 استفاده شده و عملاً دو زوج سیم در انتقال دیتا دخالت دارند (دو زوج دیگر فعلاً بلا استفاده می‌باشد)، سرعت در آن ۱۰۰ مگابیت در ثانیه و روش انتقال مبتنی بر باند است. 100 Base T4: تنها تفاوت آن با نوع بالا این است که هر چهار جفت سیم در آن بکار گرفته می‌شوند.

شاخص کیفیت کابل CAT5 میزان تابیده بودن کابل‌ها به هم می‌باشد هرچه میزان تابیده بودن بیشتر باشد کابل از کیفیت بالاتری برخوردار می‌باشد. در کابل‌های UTP وجود یک نخ برای استحکام کابل ضروری و عدم وجود آن نشانگر عدم مرغوبیت کابل است. اتصال Cross و مستقیم^۱، دو نوع اتصال روی کابل CAT5 است که رنگ بندی سیم‌ها در آن مطابق جدول ذیل است. کابل مستقیم، برای اتصال دو سیستم غیر هم جنس مانند کامپیوتر به سوئیچ استفاده شده و کابل Cross برای اتصال دو سیستم هم جنس مانند دو کامپیوتر کاربرد دارد. رنگ بندی و نوع سیگنال‌ها در در شکل ذیل مشخص شده است.

توضیحات	مستقیم	Cross	Color
+ دریافت	3	1	سبز / سفید
- دریافت	6	2	سبز
+ ارسال	1	3	سفید / نارنجی
بدون استفاده	4	4	آبی
بدون استفاده	5	5	سفید / آبی
- ارسال	2	6	نارنجی
بدون استفاده	7	7	سفید / قرمزی
بدون استفاده	8	8	قرمزی

جدول ۱: رنگ بندی در دو نوع کابل Cross و مستقیم

^۱ - Straight



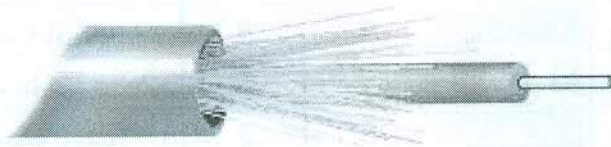
✓ فصل اول: آشنایی با مفاهیم کاربردی شبکه

سیم بندی کابل Straight و Cross در جدول ذیل مشخص شده است:

Pin1	Pin2	Pin3	Pin4	Pin5	Pin6	Pin7	Pin8
کابل Straight در هر دو سر کابل مطابق زیر (هر دو سر سیم بندی T568B)							
سفید نارنجی	نارنجی	سفید سبز	آبی ۱	سفید آبی	سبز	سفید قهوه‌ای	قهوه‌ای
سفید نارنجی	نارنجی	سفید سبز	آبی	سفید آبی	سبز	سفید قهوه‌ای	قهوه‌ای
کابل Cross یک سر ردیف اول و سر دیگر ردیف دوم (یک سر T568B، سر دیگر T568A)							
سفید سبز	سبز	سفید نارنجی	آبی	سفید آبی	نارنجی	سفید قهوه‌ای	قهوه‌ای
سفید نارنجی	نارنجی	سفید سبز	آبی	سفید آبی	سبز	سفید قهوه‌ای	قهوه‌ای

جدول ۲: نحوه اتصال در کابل های Cross و مستقیم

کابل فیبر نوری کاملاً متفاوت از نوع کواکسیال و زوج سیم به هم تابیده شده عمل می کند. به جای اینکه سیگنال الکتریکی در داخل سیم انتقال یابد، پالس هایی از نور در میان پلاستیک یا شیشه انتقال می یابد این کابل در برابر امواج الکترومغناطیس کاملاً مقاومت می کند و نیز تأثیر افت سیگنال بر اثر انتقال در مسافت زیاد را بسیار کم در آن می توان دید. لازم به ذکر است که کابل فیبرنوری از جنس شیشه است و در هنگام کار و تماس با مغزی آن خطر بریدگی و نفوذ شیشه در بدن وجود دارد که مرگبار است.



شکل ۸: نمایی از فیبر نوری و قسمت های مختلف آن

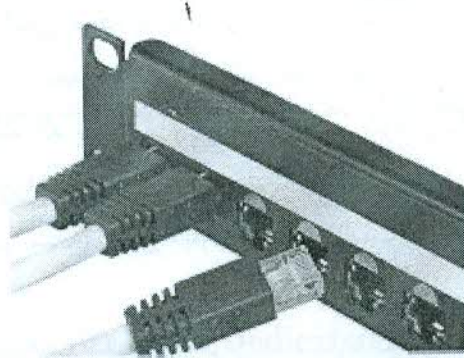
کابل کشی ساختار یافته

یک کابل کشی، منظم و قابل توسعه است که کشف و رفع خرابی در آن به سهولت انجام می پذیرد. در کابل کشی مبتنی بر کابل های CAT5 و یا CAT6 اجزاء زیر وجود دارد:



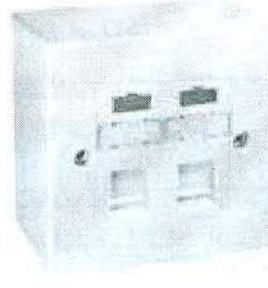
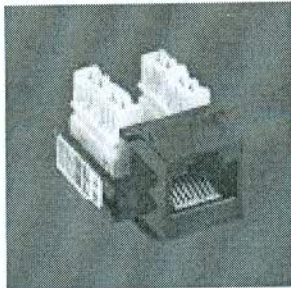
✓ فصل اول: آشنایی با مفاهیم کاربردی شبکه

- ۱- پچ پانل^۱ یک پانل شماره گذاری شده است که اتصالات مادگی^۲ در آن قرار می‌گیرد و داخل رک^۳ (قفسه فلزی) بسته می‌شوند.
- ۲- پچ کورد^۴ که کابل رابط بین پچ پانل و سوئیچ یا هاب می‌باشد.
- ۳- یک اتصال مادگی دیگر که داخل پچ پانل قرار می‌گیرد.



شکل ۹: پچ پانل و پچ کورد متصل به آن

- ۴- جعبه ای عموماً سفید رنگ^۵ که یک عدد اتصال مادگی جهت اتصال کابل رابط کامپیوتر در آن قرار می‌گیرد.
- ۵- کابل رابط بین اتصال مادگی موجود در پچ پانل و اتصال مادگی درون جعبه سفید.
- ۶- پچ کورد دیگری که کابل رابط بین جعبه سفید و کامپیوتر خواهد بود.



شکل ۱۰: جعبه ای سفید رنگ و اتصال مادگی درون آن جهت اتصال کابل رابط

¹ - Patch Panel
² - Keystone
³ - Rack
⁴ - Patch Cord
⁵ - Outlet

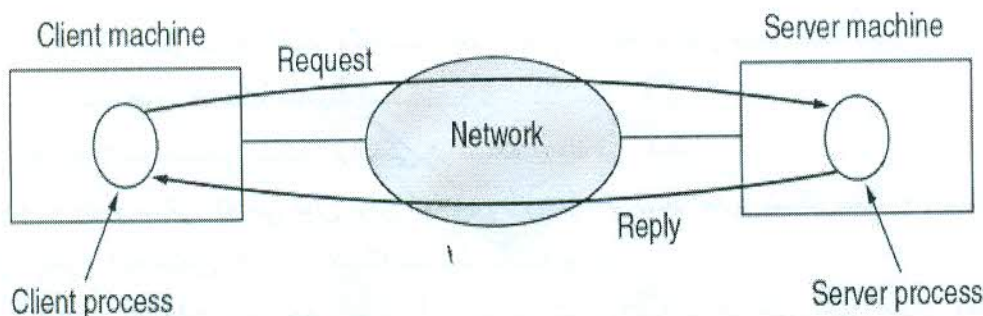
معمولا روی جعبه ها شماره معادل روی پچ پانل نوشته می شود تا رفع خرابی به سهولت انجام پذیرد. مدیر شبکه باید همیشه یک جدول از شماره جعبه ها و موقعیت آنها در ساختمان داشته باشد؛ تا به آسانی بتواند ارتباط فیزیکی یک کاربر مشخص را قطع و وصل نماید و یا در رفع خرابی وی اقدام نماید.

به طور کلی در هنگام کابل کشی توجه به نکات زیر لازم است:

- همیشه باید بیشتر از مقدار مورد نیاز کابل تهیه شود.
- هر بخشی از شبکه که نصب می گردد، آزمایش شود. زیرا ممکن است بخش هایی در شبکه وجود داشته باشند که خارج ساختن آنها پس از مدتی دشوار باشد.
- اگر کابل کشی در سطح زمین نیاز باشد لازم است تا کابل ها توسط محافظ مطمئن پوشانده شود.
- دو سر هر کابل باید نشانه گذاری و ترجیحا شماره گذاری گردد.

آشنایی با مفهوم Client / Server

در شبکه های کامپیوتری با ارزان شدن سخت افزار، الگوی شبکه از سیستم های مبتنی بر Mainframe که در آن یک کامپیوتر مرکزی همه پردازش ها را انجام می داد و ترمینال ها که توان پردازشی نداشته و فقط اطلاعات پردازش شده را از کامپیوتر مرکزی دریافت و نشان می دادند، به سیستم های مبتنی بر Client/Server منتقل شده است. در این الگو که عمدتا در شبکه مبتنی بر TCP/IP مطرح است یک دستگاه به عنوان سرویس دهنده بر روی یک نشانی IP و یک پورت سرویس دهی مشخص (مثلا ۸۰ برای وب)؛ که زوج IP و پورت اصلاحا سوکت نامیده می شود؛ آماده ارائه خدمات است. دستگاه سرویس گیرنده از نشانی IP خود و یک پورت که معمولا از شماره های بالای ۱۰۰۰ می باشد، درخواست خدمات خود را پس از ارسال درخواست برقراری ارتباط از سوکت خود به سوکت سرویس دهنده می کند. و پس از برقراری ارتباط اقدام به تبادل فرامین و دریافت نتایج آنها و در نتیجه دریافت سرویس مورد نظر می نماید.



شکل ۱۱: ارتباط بین پروسه ها در کلاینت و سرور

جهت مشاهده ارتباطات بین سوکت ها، بر روی دستگاهی که به شبکه متصل است، دستور netstat را در محیط DOS اجرا کنید.

آشنایی با تفاوت Dedicated و Non Dedicated و مقایسه آنها

در مدل Client/Server شبکه های کامپیوتری امکان توزیع و یا تخصیص سرویس های مختلف مانند فایل سرویس، Web، FTP، Email و ... به Serverهای مختلف وجود دارد و مدیر شبکه با توجه به نیازها و منابع موجود سرویس ها را بین سرورها تقسیم می کند. این کار امکان توزیع بار را در میان سرورهای مختلف و همچنین ایجاد سرورهای پشتیبان برای خدمات حساس را فراهم می نماید. چنانچه فقط و فقط یک سرویس به یک سرور تخصیص یابد و آن سرور هیچ گونه خدمات دیگری را ارائه ندهد اصطلاحاً به آن Dedicated Server گویند ولی چنانچه ارائه چندین سرویس به یک سرور محول گردد، به آن Non Dedicated گویند.

ایجاد شبکه که در آن تمام امور به صورت Dedicated انجام شود به علت نیاز به سرورهای متعدد بسیار پرهزینه است. در عمل مدیر شبکه با توجه به بار و حساسیت سرویس، اقدام به توزیع خدمات بین سرورها نموده و تنها سرویس هایی که بسیار مهم بوده و بار زیادی دارند را به صورت Dedicated اعمال می کنند.

همانگونه که گفته شد پروتکل یکی از اجزاء منطقی شبکه و مجموعه ای از قراردادهای بین دو ماشین برای مشخص نمودن نحوه ارتباط با یکدیگر می باشد؛ و به دلیل اینکه پروتکل مورد استفاده و ساختار شبکه، به یکدیگر وابسته می باشند برخی از پروتکل های مهم به طور مختصر بیان می گردد.

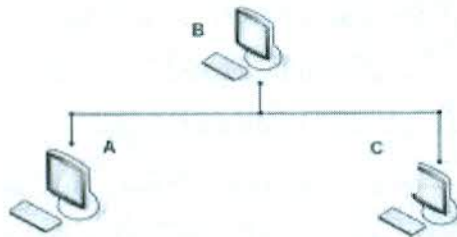
۱- پروتکل NetBEUI

این پروتکل دارای خصوصیات زیر می باشد:

- ۱- این پروتکل بسیار ساده^۱ است. و کفایت بعد از معرفی سخت افزار فقط نصب شود.
- ۲- برای شبکه های کوچک مناسب است.
- ۳- ارسال یا انتشار عمومی بسته^۲ ترافیکی در شبکه ایجاد می کند. با توجه به خصوصیتی که می توان برای انواع پروتکل ها ذکر نمود، مدیر شبکه همیشه باید نکات بسیار مهمی را به عنوان ابزار، در شبکه مد نظر داشته باشد:
- الف : admin, admin است چه بسا نام آن تعویض شده باشد؛ اما در حین حال همان وظایف و سطح دسترسی را دارا می باشد.
- ب: به بیان بسیار ساده، اعلان یا انتشار عمومی بسته ها چیز بدی است؛ چون ترافیک شبکه را بالا برده و باعث مرگ تدریجی شبکه می گردد. اما در مواردی می توان گفت که انتشار عمومی بسته خوب و لازم است مثلا:
- الف: وقتی می خواهیم اصطلاحا چشم بسته، چیزی را درون شبکه بیابیم.
- ب: برای اعلان مطلبی عمومی به بقیه اعضاء شبکه می توان از آن استفاده نمود.

به عنوان مثال شبکه های زیر را در نظر بگیرید:

- در شبکه ای به شکل ۱۲ وقتی ماشین A بسته ای را به طور خصوصی برای ماشین B ارسال نماید^۳ C هم می تواند آن را بگیرد ولی آیا می تواند از آن استفاده نماید؟



شکل ۱۲: یک شبکه ساده

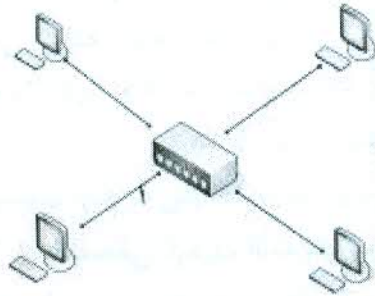
در شبکه زیر اگر توزیع کننده، هاب باشد و ماشینی بسته ای را برای ماشین دیگر، به شکل عمومی^۴ ارسال کند، همه ماشین ها آن را دریافت می کنند. اما اگر توزیع کننده سوئیچ باشد فقط ماشین مقصد آن را دریافت می کند.

^۱ - Very Simple Configuration

^۲ - Broadcast

^۳ - Unicast

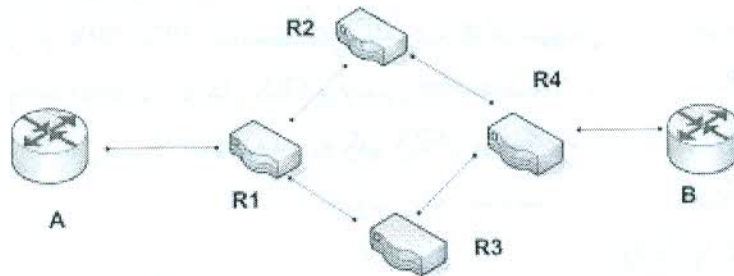
^۴ - Broadcast



شکل ۱۳: شبکه با استفاده از هاب/سوئیچ

وقتی بسته ای به شکل عمومی ارسال می شود این بسته به همه کامپیوترها رسیده و آنها بسته را به لایه های بالاتر می دهند. اما وقتی بسته به طور خصوصی ارسال می شود سایر کامپیوترها اهمیت زیادی به آن نداده و لذا ترافیک کمتری ایجاد می گردد. اگر انتشار بسته به شکل عمومی از حد مشخصی بالاتر رود طوفان انتشار^۱ ایجاد می گردد.

ذکر این نکته لازم است که پروتکل Net BEUI قابلیت مسیریابی ندارد^۲. به مثال زیر در این مورد دقت کنید:



شکل ۱۴- نحوه ارتباط در شبکه توسط پروتکل NetBEUI

این دو شبکه با پروتکل NetBEUI نمی توانند ارتباط برقرار کنند چون در این پروتکل مسیریابی پیش بینی نشده است. در این پروتکل تنها وسیله برای دریافت و ارسال اطلاعات، نام ماشین است.

1 - BroadCast Storm

2 -Non Routable



✓ فصل اول: آشنایی با مفاهیم کاربردی شبکه

در این شبکه روتر اجازه عبور بسته را نمی دهد البته می تواند بسته های اطلاعاتی را برای همه پخش کند. ولی این اجازه از آن گرفته شده است. زیرا در این صورت در اینترنت همه افراد، اطلاعات بقیه را می دانستند.

۲- IPX/SPX

این پروتکل در شبکه های ناول استفاده می گردید. البته ناول جدید از پروتکل TCP/IP استفاده می کند.

این پروتکل خصوصیات زیر را دارا می باشد:

پیکر بندی آن ساده، قابلیت مسیریابی داشته، هر زمان لازم باشد بسته اطلاعاتی را به صورت عمومی و هر جا لازم باشد آن را به شکل خصوصی منتشر می کند.
در توپولوژی شبکه های کوچک و بزرگ استفاده می شود.

با تمام مزایای ذکر شده در فوق به دلیل عدم سرمایه گذاری روی آن، پروتکل TCP/IP عرف گردید و لذا از آن در شبکه ها استفاده نمی گردد.

با استفاده از این پروتکل به دو طریق ارسال اطلاعات داریم:

→ IPX ۱- بدون تضمین Connection less عادی

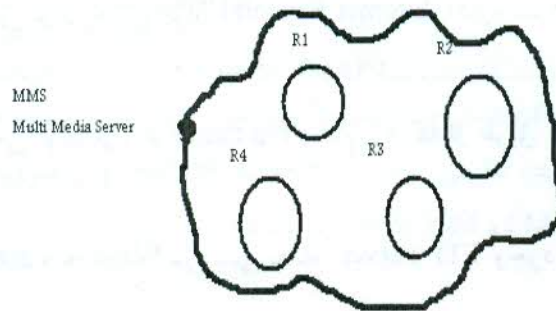
→ SPX ۲- با تضمین Connection Oriented سفارشی

در حالت سفارشی، یک رسید^۱ به دست فرستنده می رسد که اگر رسید در هر صورت دریافت نشود، بسته دوباره ارسال می گردد.

همچنین می توان از IPX/ SPX خواست که بسته را با کدام سرویس ارسال نماید، در شبکه ناول دستوری به نام Rconsole با پروتکل SPX و دستور file Transfer با پروتکل IPX کار می کند. لازم به ذکر است که در صورت استفاده از پروتکل SPX، ترافیک شبکه بالا می رود.

۳- پروتکل TCP/IP

این پروتکل پیکر بندی پیچیده ای داشته و سرویس های فراوان و متنوعی را فراهم می کند. یعنی پیچیدگی آن به تنوع سرویس هایش بر می گردد. این پروتکل در سیستم عامل یونیکس متولد شد ولی هر همه سیستم عامل ها استفاده می شود. در شبکه های کوچک قابلیت پیکر بندی اتوماتیک و در شبکه های بزرگ قابلیت مسیریابی را نیز دارد. علاوه بر خصوصیات پروتکل های قبلی، قابلیت ارسال بسته به گروهی خاص^۱ را نیز دارد.



شکل ۱۵: استفاده از Multicast برای ارسال پیام

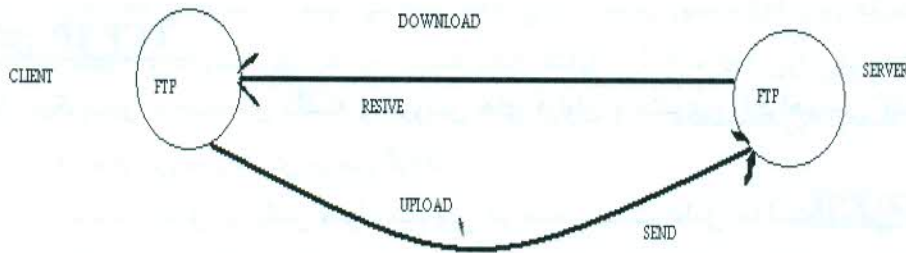
به عنوان مثال در شبکه فوق بسته ای باید برای ۲۰ ماشین ارسال شود. پس باید برای هر کدام به شکل خصوصی ارسال شده، که کار دشواری است و یا باید به شکل عمومی پخش گردد که در این صورت همه به آن دسترسی دارند و از طرف دیگر ترافیک شبکه نیز بسیار بالا می رود. در این حالت می توان از قابلیت ارسال بسته به گروهی خاص استفاده نمود. باید اذعان داشت که TCP/IP مجموعه ای از سرویس هاست، لذا باید فلسفه و هدف از اجرای شبکه را دانست به عنوان مثال اهداف زیر را می توان در نظر داشت:

- اشتراک منابع جهت استفاده از سرویس های متعدد
- کنترل و عملیات از راه دور
- ارسال پیغام برای اعضاء شبکه

سرویس های TCP/IP

File Transfer Protocol : FTP که برای انتقال فایل بین دو ماشین استفاده می گردد. چنین سرویسی هم در سمت سرویس دهنده و هم در سرویس گیرنده وجود دارد.

1 - Multicasting



شکل ۱۶: نحوه استفاده از سرویس FTP

برای FTP Client می توان به نرم افزار Internet Explorer اشاره نمود که به شکل زیر بکار گرفته می شود:

Ftp: //.....

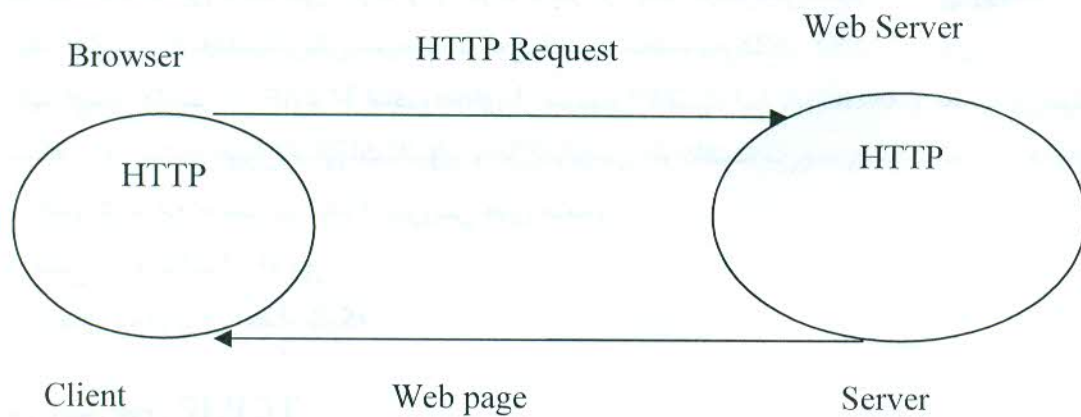
به عنوان مثال دیگر می توان نرم افزار Ftp.exe را نام برد که از طریق Command ویندوز قابل اجرا می باشد.

از طرف دیگر در Windows 2000 سرویسی به نام FTP Server وجود دارد.

(Hyper Text Transfer Protocol) HTTP

این پروتکل، سرویسی برای انتقال اطلاعات است. و می توان بلوک دیاگرامی به شکل زیر برای آن متصور شد.

(Web Client)



شکل ۱۷: نحوه استفاده از سرویس HTTP

که HTTP Request ممکن است یکی از موارد زیر باشد:

✓ فصل اول: آشنایی با مفاهیم کاربردی شبکه

- درخواست صفحات HTML باشد.
- اجرای یک برنامه کاربردی مانند جستجو در میان صفحات وب باشد.
- انتقال یک فایل باشد که این مطلب را می توان در زمان دانلود یا ایمیل دید.
- پس بنابراین می توان گفت که پروتکل HTTP یک پروتکل همه کاره است.

پروتکل های مورد استفاده در ایمیل

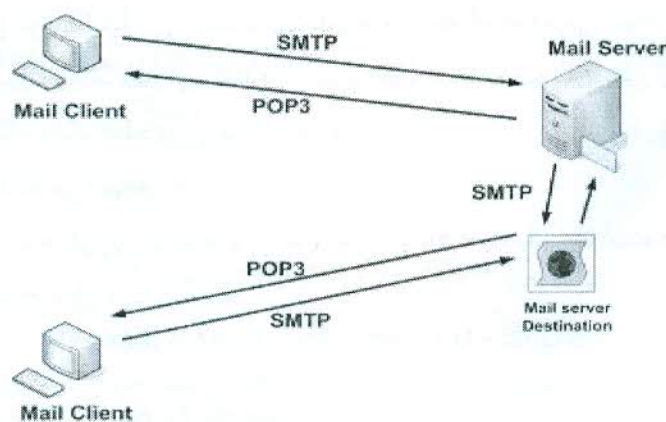
سه پروتکلی معروفی که در ایمیل استفاده می شود به شرح ذیل می باشد:

Simple Mail Transfer Protocol: SMTP

Post Office Protocol v3: Pop3

Internet Mail (message) Access Protocol: IMAP4

نرم افزارهای ایمیل هم به دو گروه سرویس دهنده^۱ و سرویس گیرنده^۲ تقسیم می شوند. از نرم افزارهای سرویس گیرنده ها می توان به Outlook Express و از سرویس دهنده ها به نرم افزارهای MD Daemon، I Mail و Web Mail اشاره نمود.



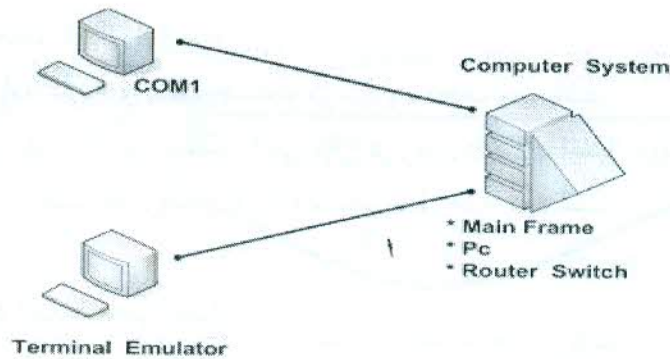
شکل ۱۸: نحوه استفاده از پروتکل های ایمیل در شبکه

Telnet

ترمینال یک وسیله ورودی یا خروجی بوده و بر دو نوع متنی و گرافیکی می باشد.

^۱ - Mail Server

^۲ - Mail Client



شکل ۱۹: ارتباط بین دو سیستم از طریق شبکه

Telnet: اگر ارتباط بین ترمینال و سیستم کنترل از طریق شبکه بوده و پروتکل مورد استفاده TCP باشد در این صورت Telnet یک Terminal Emulator Text تعریف می شود. بعضی از ترمینال ها به قرار زیر هستند:

Hyper Terminal, RAdmin, Term95, PC Anywhere

Simple Network Management Protocol : SNMP

از این پروتکل که از نوع UDP می باشد برای مدیریت شبکه استفاده می شود. در جهت تحقق این کار بر روی هر ماشین شبکه، باید نرم افزاری^۱ نصب نمود تا اطلاعات مدیریتی را از آن ماشین جمع آوری نموده و در یک بانک اطلاعاتی قرار دهد. مدیر سیستم نیز نرم افزار دیگری^۲ جهت مشاهده بانک اطلاعاتی استفاده می نماید.

مایکروسافت چنین نرم افزاری نداشته و از سرویس های بقیه کمپانی ها استفاده می کند. برخی از این نرم افزارها به شرح ذیل می باشند:

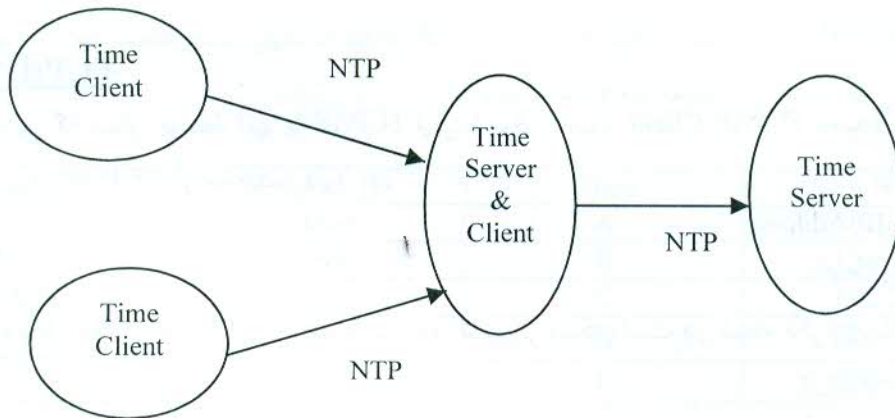
Cisco Works - What's Up Gold - Hp Open View - Solar Winds

Simple Network Time Protocol : SNTP

این پروتکل قابلیت همزمان نمودن ساعت را در بین تمام اجزاء شبکه فراهم می کند.

^۱ - SNMP Agent

^۲ - Management Information Base (MTB)



بلوک دیاگرام کاربرد پروتکل SNTP

در مایکروسافت چنین سرویسی به نام Windows time در مسیر زیر وجود دارد:
 Administrator tools → Service
 این سرویس را می توان با اجرای دستورات زیر در Command ویندوز مشاهده نمود:
 Net time /query sntp

و با دستور زیر پیکربندی نمود:
 Net time/set sntp:192.168.10.1
 Server
 Time.nist.gov

- ۱- در یک شبکه مبتنی بر ویندوز 2000 که کامپیوترها در گروه کاری قرار دارند به صورت پیش فرض سرویس Windows Time غیر فعال است.
- ۲- در یک شبکه مبتنی بر ویندوز 2000 که کامپیوترها در یک حوزه قرار دارند به صورت پیش فرض این سرویس فعال است. و در این صورت Domain Control به عنوان Time Server و بقیه کامپیوترها به عنوان Time Client عضو این حوزه هستند.
- ۳- در سیستم عامل های ویندوز 2003 و XP چه در گروه کاری و چه در حوزه این سرویس فعال است.
- ۴- برای کارکرد صحیح سرویس Windows time اختلاف ساعت بین سرویس دهنده و سرویس گیرنده نباید از ۱۲ ساعت بیشتر باشد یعنی باید گزینه Date در پنجره Time Zone یکسان باشد.



✓ فصل اول: آشنایی با مفاهیم کاربردی شبکه

TCP/IP Host

ماشین هایی که بتوان توسط آنها با TCP/IP ارتباط برقرار نمود TCP/IP Client نامیده می شوند. هر Host روی TCP/IP دو مشخصه دارد.

Address: IP Address

Name: نام ماشین

در این پروتکل ملاک عمل IP می باشد؛ زیرا نام کامپیوتر ممکن است در شبکه تکراری باشد:

www.usb.ac.ir

Fully Qualified Domain Name (FQDN)

اسامی کامپیوترها از چند قسمت تشکیل شده است:

WWW.Host Role.mail

نقشی که اعمال می کند

Site Name .usb .com

دامنه فعالیت و یا وابستگی

Computer Name یا Net Bios Name نام کامپیوتر بوده که حداکثر ۱۵ کاراکتر بوده و معمولاً در زمان نصب سیستم عامل ویندوز به کامپیوتر داده می شود. لازم به ذکر است که علامت نقطه در نامگذاری مجاز نیست.

Net Bios Name = Computer Name

TCP/IP Name = Full Computer Name

اما هنگامی که در نظر است یک کامپیوتر در شبکه ای دیگر قابل دسترسی باشد باید FQDN را توسط IP Address تصحیح نمود. که این کار توسط سرویسی به نام DNS انجام می گیرد. در ادامه و به تفصیل در مورد آن توضیح داده خواهد شد.

اما IP Address که ملاک عمل می باشد یک عدد ۴ بیتی به شکل زیر است:

$W.X.Y.Z \quad 0 < \{W.X.Y.Z\} < 255$

که به این نوع IP Address ، IP.V4 گویند. نوع دیگری از IP که ۱۲۸ بیت یا ۱۶ بیتی است به IPNG یا IPV6 معروف است.



✓ فصل اول: آشنایی با مفاهیم کاربردی شبکه

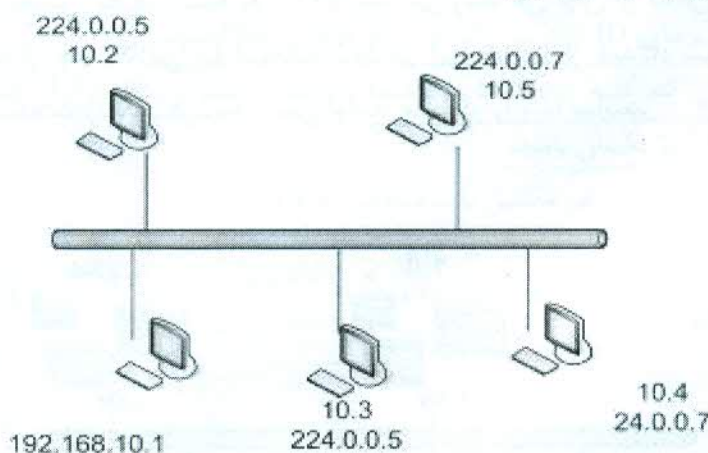
هر IP Address از دو قسمت Network ID و Host ID تشکیل شده است. این آدرس ها به کلاس هایی به ترتیب زیر طبقه بندی شده اند:

Host ID	Network ID	Class	W
3 byte	1 byte	A	0-126
2 byte	2 byte	B	128-191
1 byte	3 byte	C	192-223
	Multicast	D	224-239
		E	240-255

جدول ۳: کلاس بندی آدرس های مختلف با فرمت W. X. Y. Z

به آدرس 127. X. Y. Z، Loop Back Adders گفته می شود که برای بررسی کامپیوترهای شخصی استفاده می شود. یعنی با دستور Ping 127.0.0.1 می توان TCP/IP هر کامپیوتر را چک نمود.

برای مثال شبکه زیر را در نظر بگیرید:



شکل ۲۰: شبکه ای که در آن یک سرویس گیرنده دو آدرس دارد.

در این شبکه می توان دید که یک سرویس گیرنده دو آدرس IP داشته، که از یکی از آنها برای ارسال بسته به گروهی خاص استفاده می شود. حال این سوال پیش می آید که از چه کلاس آدرسی باید در هر شبکه استفاده نمود؟ واضح است که کلاس شبکه به تعداد ماشین های موجود در شبکه بستگی دارد.



✓ فصل اول: آشنایی با مفاهیم کاربردی شبکه

به عنوان مثال برای یک شرکت که ۲۰ کامپیوتر داشته و تا چند سال دیگر قرار است به ۲۵ عدد برسد بهتر است از کلاس C استفاده نمود.

ذکر این نکته ضروری است که بایت های Host ID نمی تواند همگی با هم صفر یا همگی با هم ۲۵۵ باشد. اگر بایت های Host ID همگی با هم ۲۵۵ باشد به آن انتشار عمومی^۱ گفته می شود.

به آدرس های صحیح (■) و نادرست (x) در جدول زیر دقت نمائید:

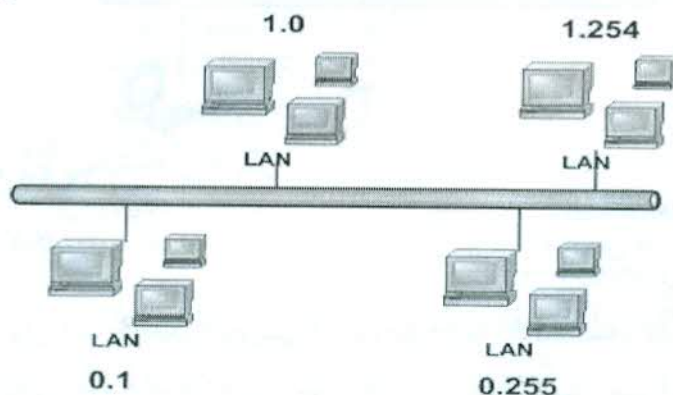
192.168.0.1	■	18.255.0.255	■	10.0.0.0	x
192.168.10.0	x	192.168.10.255	x	172.16.255.255	x
130.145.0.0	x	172.16.255.255	x	172.16.255.0	■
10.0.0.0	x	10.255.255.255	x	18.0.0.255	■
18.0.255.0	■	172.16.0.255	■		

جدول ۴: مثال هایی از آدرس های مجاز و غیرمجاز

برای حدود ۱۰۰ ماشین که در آینده به ۵۰۰۰ عدد می رسد می توان از کلاس B استفاده نمود. اگر در این حالت از چند کلاس C استفاده شود در این صورت از دیدگاه شبکه، کامپیوترهای موجود به چند شبکه مجزا تقسیم شده و نمی توانند همدیگر را پیدا نمایند.

N.I : 140.150.X.Y

N.N : 140.150.0.0

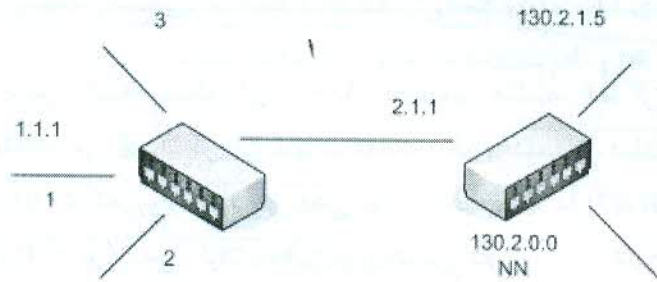


شکل ۲۱: استفاده از چند کلاس مختلف برای یک شبکه

^۱ - Broadcast

شروع مکانیزم ارسال اطلاعات در TCP/IP

شبکه های زیر را در نظر بگیرید:



شکل ۲۲: نحوه تبادل بسته در دو شبکه مختلف

در شکل فوق بسته ای را فرض کنید که قرار است از آدرس 130.1.1.2 به یک Web server به آدرس http://130.2.1.5 ارسال گردد. در این صورت اولین کاری که ماشین مبدا انجام می دهد این است که آدرس شبکه مقصد را نگاه کرده و با آدرس شبکه خودش مقایسه می کند. اگر این پارامتر یکسان باشد می توان فهمید که ماشین مبدا و مقصد در یک شبکه قرار دارند. در غیر این صورت آن را به روتر ارسال می کند. روترها جدولی به نام جدول مسیریابی^۱ به شکل زیر داشته و از روی آن می فهمد که بسته را به چه مقصدی ارسال نماید.

شماره پورت	شماره شبکه
۲	۱۳۰.۲.۱.۵

جدول ۵: مثالی از جدول مسیریابی

به عنوان مثالی دیگر، شبکه شکل ۲۳ را در نظر بگیرید:

در این شبکه برای ارسال داده کدام یک از دو پورت ۲ یا ۳ بهتر است؟

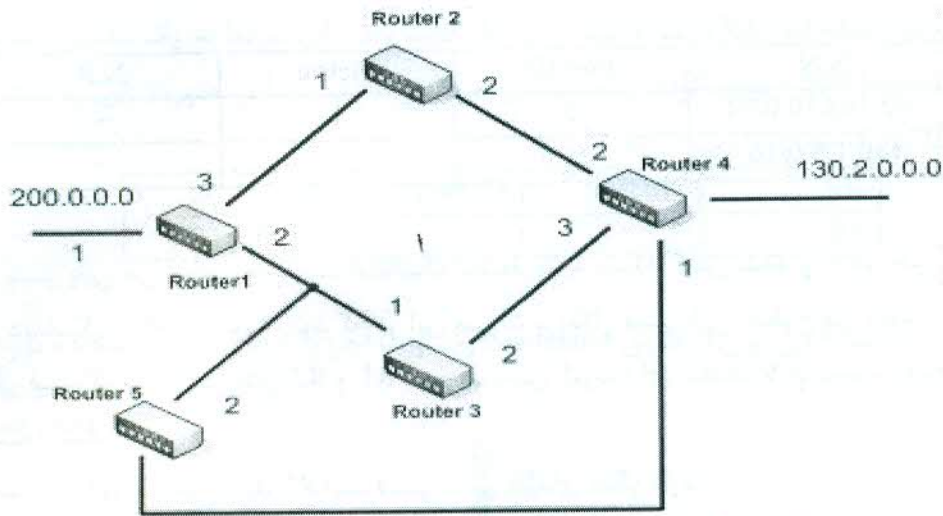
ارزش مسیریابی^۲ پارامتر دیگری در شبکه می باشد؛ هر چه این عدد کوچکتر باشد مسیر بهتر بوده و ترافیک آن کمتر است. پس با توجه به این مسئله ارسال از پورت ۲ بهتر به نظر می رسد.

^۱ - Routing Table

^۲ - metric



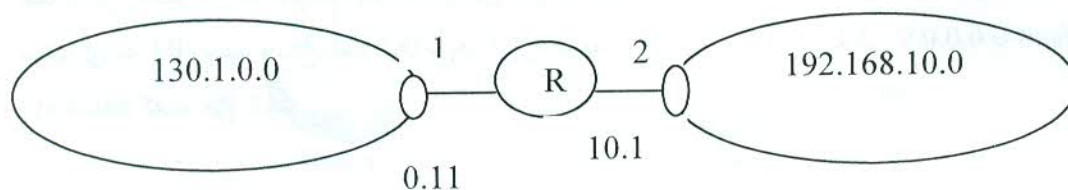
✓ فصل اول: آشنایی با مفاهیم کاربردی شبکه



شکل ۲۳: چندین شبکه که توسط روترهای مختلف در ارتباطند.

شماره شبکه	شماره پورت	ارزش مسیر	روتر
130.2.0.0	2	1	R5
130.2.0.0	3	20	R3

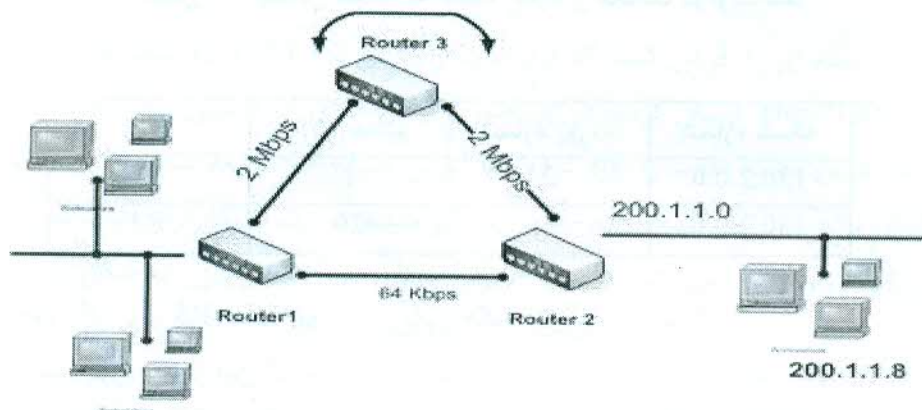
در مثال فوق اگر روتر R5 اضافه شود مسیریابی چگونه انجام می شود؟ در این حالت چون بعد از این که بسته از پورت ۲ خارج گردید، باید مشخص شود که باید از کدام روتر عبور نماید لذا پارامتر دیگری نیز اضافه می شود و آن روتر گیرنده اطلاعات است. همچنین می توان به جای آدرس روتر، IP آنرا داد و می توان به جای شماره پورت، IP اینترفیسی را که به آن وصل شده را وارد نمود. اگر ارزش دو مسیر یکسان باشد دیگر مهم نیست بسته ها از چه مسیری ارسال گردد. و حتی می تواند در هر دو مسیر اطلاعات ارسال گردد. سوال دیگری که ممکن است به ذهن خطور کند این است که جدول مسیریابی چگونه و کی ساخته می شود؟



شکل ۲۴: نمای کلی یک شبکه با جدول مسیریابی به شکل زیر

N.N	Port ID	Metric	N.R
192.168.10.0/24	2	1	-
130.1.0.0/16	1	1	-

جدول مسیریابی می تواند به صورت استاتیک توسط مدیر شبکه کامل شده و یا در حین کار به صورت دینامیکی ساخته و بروز شود که در این صورت پروتکل مسیریابی^۱ مطرح می شود. در مثال قبل اگر بین روتر های R1 و R2 هیچ سرویس گیرنده ای نباشد، لازم نیست روترها حتی IP داشته باشند. در ادامه مثال فوق، فرض کنید R2 اینترفیسی برای جاهای دیگر دارد.



شکل ۲۵: نحوه ارسال بسته به ماشینی که آدرس آن در جدول مسیریاب نیست.

در این صورت بسته ای که به روتر ۱ می رسد و قرار است به آدرس 124.4.7.3 برود چون در جدول مسیریاب مشخص نشده پیغام Destination Host unreachable ظاهر می شود (یعنی به روتر دسترسی داشته ولی پاسخی دریافت نمی گردد) و برای مقاصد 180.1.1.7 و 215.43.21.2 هم چنین مشکلی وجود دارد. بنابراین باید این آدرس ها را نیز در جدول مسیریاب وارد نمود که وقتی تعداد این مسیرها زیاد شود، دیگر انجام این کار مشکل می باشد. لذا مشخص می گردد که اگر بسته ی به R1 رسید و ندانست کجا برود، آن را به بعدی ارسال نماید که به آن 0.0.0.0 یا Default gateway گفته می شود.

^۱ - Routing protocol



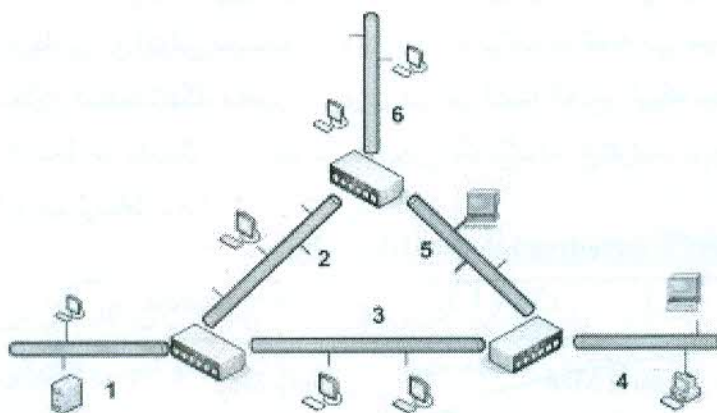
✓ فصل اول: آشنایی با مفاهیم کاربردی شبکه

حال اگر در شبکه قبل R3 را نیز داشته و در نظر است بسته ای سریعاً به یک ماشین مشخص به آدرس 200.1.1.8/32 ارسال گردد و مسیر نیز مشخص باشد در این صورت آن را وارد جدول مسیریاب می کنیم.

N.N	Port ID	Metric	NR
200.1.1.8/32	3	1	R3

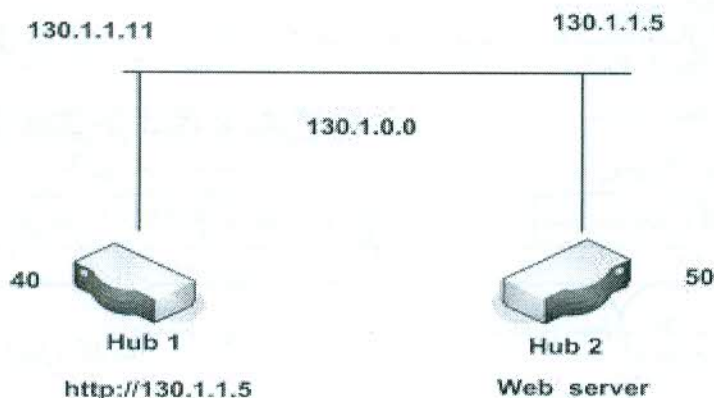
جدول مسیریاب را می توان از طریق Command ویندوز با اجرای دستورات زیر مشاهده نمود.

```
C:\netstat -r  
C:\route print
```



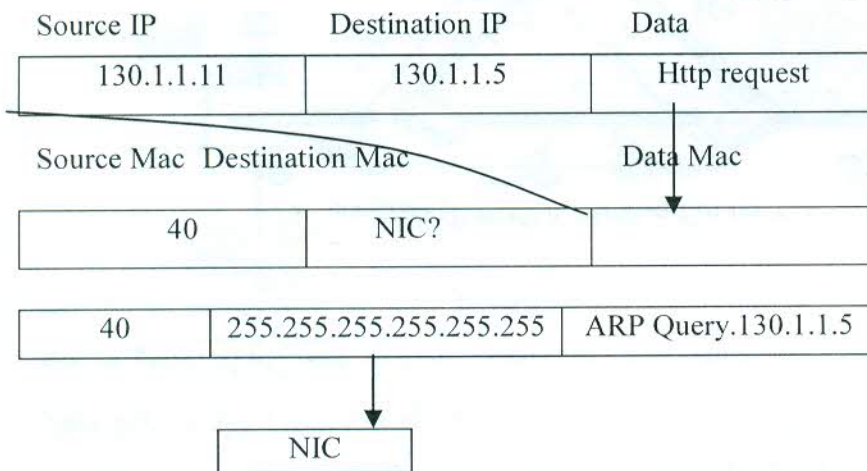
شکل ۲۶: شبکه ای مبتنی بر سوئیچ هایی با قابلیت مسیریابی

شکل ۲۶ در صورتی شبکه می باشد که سوئیچ ها، روتر هم باشند که در این صورت به آنها سوئیچ لایه سه گویند. در این بخش به بررسی چگونگی دریافت بسته در کارت شبکه پرداخته می شود. به عنوان مثال شبکه زیر را در نظر بگیرید:



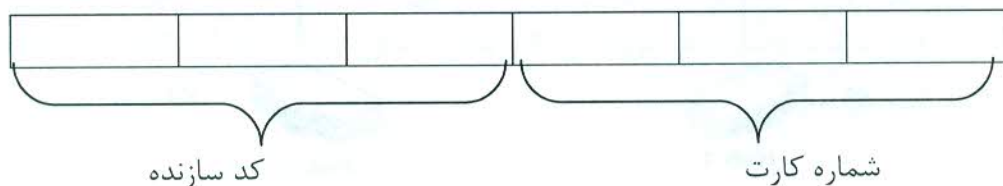
شکل ۲۷: مثالی از ارسال یک بسته TCP/IP

یک بسته TCP/IP مانند شکل ۲۸ می باشد. یعنی یک بسته برای ارسال به ماشینی با IP مشخص ابتدا باید به کارت شبکه ارسال گردد. اما این کار امکان پذیر نیست زیرا کارت شبکه مفهوم IP را نمی فهمد و فقط آدرس فیزیکی^۱ را می داند. لذا به کمک آن، اقدام به ارسال بسته می نماید. هر کارت شبکه اعم از باسیم و بی سیم دارای یک شماره سریال شش بایتی منحصر به فرد جهانی به نام آدرس فیزیکی است که در زمان تولید کارت شبکه در آن تعریف می شود. به هر شرکت تولید کننده یک رنج بزرگ از سریال ها تخصیص داده شده است که آن شرکت فقط مجاز است از رنج مشخص شده، سریالی به کارت های تولیدی خود اختصاص دهد. این آدرس در پروتکل شبکه، در لایه فیزیکی قرار گرفته است و به همین دلیل به آن آدرس فیزیکی گفته می شود. آدرس فیزیکی یا منطقی، به آدرس سیستم در لایه های بالاتر شبکه گفته می شود. نکته کلیدی و متمایز کننده شبکه محلی و شهری در این است که در شبکه محلی سیستم های کامپیوتری برای ارتباط با یکدیگر باید آدرس فیزیکی یکدیگر را به ترتیب زیر یافته و در لایه فیزیکی مستقیماً با هم ارتباط برقرار کنند.



شکل ۲۸: یک بسته TCP/IP که قرار است از طریق کارت شبکه ارسال گردد.

آدرس فیزیکی هر ماشین در شبکه به شکل زیر است:



^۱ - Mac Address



✓ فصل اول: آشنایی با مفاهیم کاربردی شبکه

از روی کد سازنده می توان فهمید کارت شبکه محصول چه شرکتی است. آدرس فیزیکی کارت شبکه را می توان با اجرای دستور `IPConfig /all` در محیط DOS، مشاهده نمود. آدرس فیزیکی در قسمت Physical Address نتیجه اجرای دستور فوق، با یک مقدار ۶ بایتی و به صورت هگزا دسیمال نمایش داده می شود.

قبل از آنکه TCP/IP بسته ای را به کارت شبکه تحویل دهد، باید IP Address را به آدرس فیزیکی تبدیل نماید که به این عمل Address Regulation گفته می شود.

سه روش برای یافتن آدرس فیزیکی مقصد وجود دارد:

اول این که روی ماشین مبدا جدولی شامل کلیه آدرس های فیزیکی ماشین های شبکه موجود باشد. روش دوم این است که به کمک فراخوان یا اعلان عمومی، آدرس فیزیکی آن را جو یا شد. و در نهایت روش سوم بدین ترتیب است که کامپیوتری به عنوان سرور وجود داشته باشد و در صورت نیاز برای یافتن آدرس فیزیکی خاصی، به آن مراجعه نمود.

پروتکل (ARP (Address Resolution Protocol

این پروتکل جهت مشخص کردن نشانی آدرس فیزیکی از روی آدرس IP بکار می رود. هر کامپیوتر یک جدول به نام جدول ARP در حافظه خود دارد که نشانی IP و آدرس فیزیکی کامپیوترهایی را که اخیرا با آنها کار کرده است را برای یک مدت کوتاه نگهداری می کند. چنانچه کامپیوتر بخواهد با کامپیوتری دیگر که در جدول ARP رکوردی برای آن وجود ندارد کار کند، یک درخواست برای تمام کامپیوترهای شبکه ارسال و آدرس فیزیکی مرتبط با IP را سوال می کند. دستگاهی که آدرس IP مورد نظر را داراست به عنوان پاسخ، آدرس فیزیکی خود را اعلام می کند و دستگاه متقاضی ارتباط، پس از اضافه کردن یک رکورد برای آن در جدول ARP خود، از نشانی فیزیکی برای ارتباط با دستگاه مقابل بهره می برد.

در شبکه های مبتنی بر میکروسافت هر ۱۰ دقیقه یک بار درخواست خود برای تمام کامپیوترهای شبکه ارسال می کند و در شبکه های مبتنی بر Com3 هر ۱۵ دقیقه این عمل انجام می گیرد. که این موضوع به دلیل افزایش ترافیک شبکه، یک نقطه ضعف محسوب می گردد. بنابراین این زمان را که به Time out معروف است باید (البته روی هر سیستم جداگانه) زیاد گردد. که عملی وقت گیر است.

جدول ARP هر دستگاه با اجرای دستور ذیل قابل مشاهده می باشد:

```
C:\arp -a
```



✓ فصل اول: آشنایی با مفاهیم کاربردی شبکه

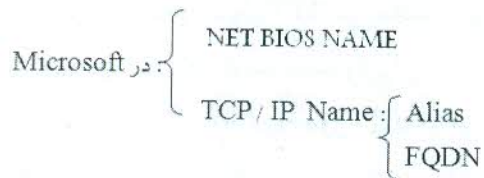
چنانچه می‌خواهید آدرس فیزیکی یک IP مشخص (مثلا 10.10.10.5) را در شبکه محلی خود پیدا کنید ابتدا دستور ذیل را اجرا کرده و سپس دستور قبل را وارد نمایید:

```
C:\ping 10.10.10.5
```

در ادامه مثالی را فرض کنید که در آن وب سرور در شبکه دیگری است. پس باید آدرس فیزیکی روتر را یافته و فریم را تحویل روتر داد. روتر این فریم را گرفته و با توجه به قسمت دیتای فریم، بسته را به ماشینی به IP Address مقصد تحویل می‌دهد.

همانطور که گفته شد به کمک دستور `arp -a` می‌توان جدول آدرس‌های فیزیکی^۱ را مشاهده کرد. برای وارد نمودن این آدرس‌ها در این جدول به صورت استاتیکی، از دستور `arp -s` می‌توان استفاده نمود.

حال اگر آدرس IP بین چند ماشین تکراری باشد هر ماشینی که زودتر به درخواست عمومی پاسخ دهد بسته را دریافت می‌کند. پس از ۱۰ دقیقه دوباره درخواست عمومی ارسال می‌گردد و در این مرحله ممکن است ماشین بعدی به آن پاسخ دهد، لذا در شبکه اختلال ایجاد شود. برای ارتباط در شبکه‌ها باید نام کامپیوتر به آدرس IP تبدیل شود، اسامی کامپیوترها به دو شکل زیر هستند:



این دو را تفکیک نموده و هر کدام را با درخواست^۲ مربوط به خودش به یکی از دو شکل زیر می‌توان یافت.

۱- از درون فایل درون خود کامپیوتر در مسیر زیر:

```
Windows Directory\System32\Drivers\etc\hosts
```

۲- از سرویس دهنده‌ای به نام DNS Server

۳- توسط درخواست عمومی از کلیدهای ماشین‌های شبکه سوال شود.

که روش ایده آل این است که همه کامپیوترهای شبکه به سراغ DSN Server بروند.

برای یافتن اسامی Net Bios Name نیز سه روش وجود دارد :

الف: از درون فایل درون خود کامپیوتر در مسیر زیر:

^۱ - Mac Address Table

^۲ -TCP/IP Request



✓ فصل اول: آشنایی با مفاهیم کاربردی شبکه

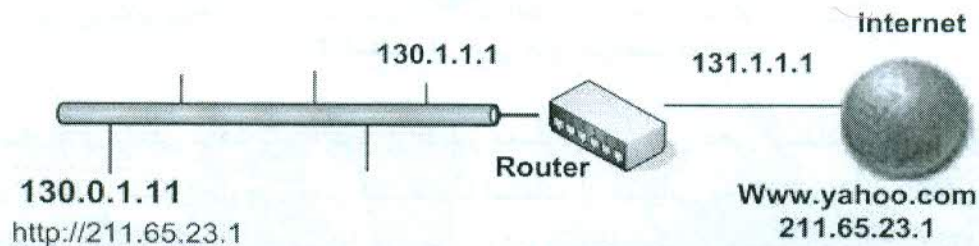
Windows Directory\System32\Drivers\etc\lmhosts

ب: از یک کامپیوتر سروری به نام Wins server

ج: توسط درخواست عمومی از کلیه ماشین های شبکه سوال شود.

نکاتی دیگر در مورد IP Address

هر ماشین در شبکه ی مبتنی بر پروتکل TCP/IP برای ارتباط نیازمند استفاده از IP Address می باشد. شبکه زیر را در نظر بگیرید:



شکل ۲۹: اختصاص آدرس های IP

دو نوع IP Address معتبر^۱ و غیرمعتبر^۲ وجود دارد. با توجه به تعداد کامپیوترهای موجود در شبکه، یک رنج IP ثبت شده از شرکت ثبت کننده منطقه ای یا RIR گرفته و به عنوان IP معتبر به هر ماشین اختصاص داده می شود. این روش آدرس دهی دو مشکل دارد: اولاً باید هزینه زیادی برای ثبت IP صرف نمود.

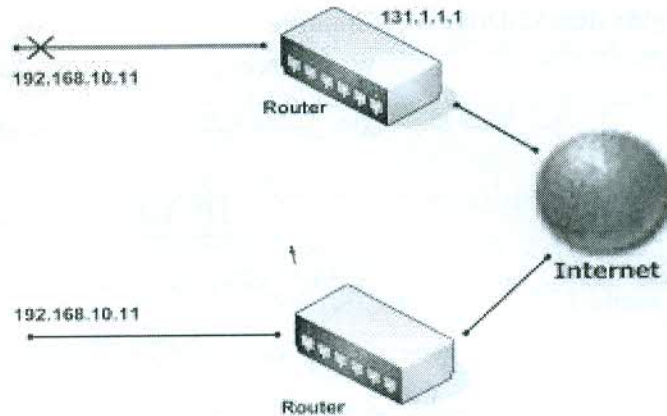
ثانیاً این که با توجه به محدودیت این آدرس ها در جهان، مشکل کمبود IP به وجود می آید. اما می توان بدون صرف هزینه به کامپیوترهای شبکه IP اختصاص داد. برای این کار می توان از IP های غیر معتبر استفاده نمود. این IP Address به شکل زیر در کلاس های مختلف طبقه بندی شده اند و هرگز رجیستر نمی گردد و می توان آنها را در شبکه متعدد استفاده نمود.

- A: 10.X.Y.Z
- B: 172.16.X.Y
- C: 192.168.0.X

192.168.255.X

^۱ - Valid IP Address

^۲ - Invalid IP Address



شکل ۳۰: استفاده از آدرس های غیرمعتبر در شبکه

در شبکه های داخلی مانند شبکه فوق از IP غیر معتبر برای آدرس دهی استفاده شده است و فقط برای ارتباط با شبکه خارجی نظیر اینترنت با استفاده از عملیاتی به نام NAT^۱ از IP های معتبر استفاده می شود؛ که طی آن یک IP غیر معتبر داخلی به IP معتبر ترجمه شده و ارتباط با اینترنت از طریق آن انجام می پذیرد. بدین صورت که روتر IP خود را که یک آدرس معتبر می باشد روی بسته قرار داده و ارسال می کند. پاسخ دریافت شده از شبکه خارجی نیز به روتر ارسال می گردد. لذا با نصب NAT می توان آدرس های غیر معتبر را به آدرس معتبر تبدیل نمود. این کار سرعت انتقال داده را در شبکه کاهش می دهد اما مزایایی فراوانی هم دارد. NAT در مواردی که تعداد IP های معتبر در دسترس، کم است و نیاز به برقراری ارتباط تعداد زیادی دستگاه با اینترنت است کاربرد دارد. همچنین به عنوان یک روش مناسب جهت ایمن سازی شبکه قابل استفاده است زیرا کامپیوتری که از طریق NAT با شبکه اینترنت در ارتباط است به دلیل عدم ارتباط مستقیم از امنیت بیشتری برخوردار خواهد بود.

برای آگاهی از این مسئله که IP یک کامپیوتر معتبر می باشد یا نه، کافی است پس از اتصال به شبکه دستور ذیل را اجرا نمود:

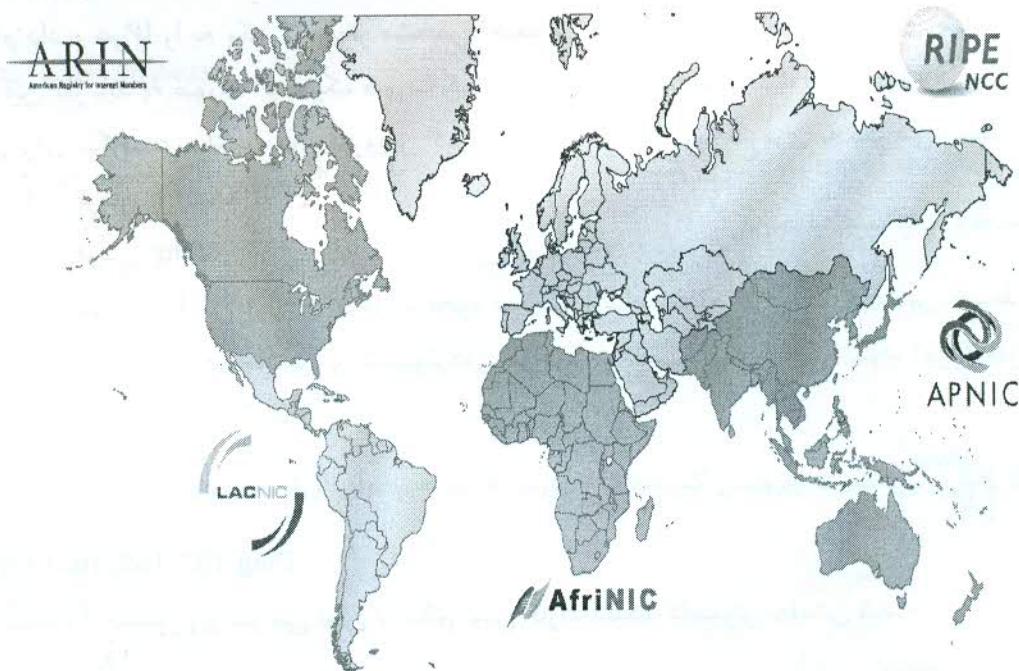
C:\ipconfig

همچنین برای کشف IP معتبری که خدمات را به کامپیوتر ما ارائه می دهد می توان به سایت www.myipaddress.com رجوع نمود.

^۱ - Network Address Translation

مدیریت فضای IP در جهان

فضای IP در جهان توسط چهار سازمان منطقه‌ای که اصطلاحاً ثبت کننده منطقه‌ای^۱ RIR نامیده می‌شوند مدیریت می‌شود. این سازمان‌ها که به صورت جغرافیایی عمل می‌کنند در محدوده جغرافیایی خود مسولیت تخصیص و مدیریت IPها را برعهده دارند. در هر کشوری سرویس دهندگان اینترنت^۲ پس از عضویت در سازمان مربوط به منطقه جغرافیایی خود به عنوان یک تخصیص دهنده محلی^۳ می‌توانند از طریق RIR نشانی‌ها را دریافت کرده و در اختیار کاربران خود قرار دهند. لیست RIRها در جدول ۶ به تفکیک منطقه جغرافیایی تحت پوشش آورده شده است.



شکل ۳۱: چهار سازمان ثبت کننده منطقه‌ای IP در جهان

جهت اطلاع از اینکه یک نشانی IP معتبر واقعا به نام چه شبکه‌ای ثبت شده است می‌توان با توجه به جدول زیر و منطقه‌ای که در آنجا نشانی IP فعال شده است به نشانی‌های اینترنتی مشخص شده مراجعه نمود و آدرس IP مورد نظر را در قسمت جستجو آن سایت وارد کرد.

^۱ - Regional Internet Registry
^۲ - Internet Service Provider
^۳ - Local Internet Registry (LRI)



✓ فصل اول: آشنایی با مفاهیم کاربردی شبکه

RIRs	Region	Site
AFRINIC	Africa	www.afrinic.net
APNIC	Asian Pacific Network Information Center	www.apnic.net
ARIN	American Registry for Internet Numbers	www.arin.net
LACNIC	Latin American and Caribbean Internet Address Registry	www.lacnic.net
RIPE NCC	Europe, the Middle East and parts of Central Asia	www.ripe.net

جدول ۶: لیست RIR ها به تفکیک منطقه جغرافیایی

TCP/ IP مسأله ای دیگر در DHCP Server

در صورتی که تعداد ماشین در یک شبکه کم باشد می توان پیکربندی شبکه را به صورت دستی انجام داد و هر IP را به یک کامپیوتر مشخص اختصاص داد. اما اگر تعداد ماشین های شبکه زیاد بود این کار باید به صورت اتوماتیک صورت گیرد. این وظیفه را DHCP Server بر عهده دارد. پس برای پیکربندی ماشین های سرویس گیرنده دانستن فرامین زیر ضروری به نظر می رسد:

۱- فرمان IP Config

۲- فرمان Ping

با دستور Ping می توان از شکل و نحوه سلامت ارتباط مطلع گردید و همچنین توسط آن می توان ارتباط دو ماشین و کامپیوترهای موجود در مسیر آنها را چک نمود. این فرمان به صورت زیر اجرا می گردد:

```
Ping [name  
IP]
```

مثال: Ping 192. 168. 10. 1

با استفاده از دستور زیر نیز می توان از سالم بودن کارت شبکه کامپیوتر مطمئن شد.

```
{ ping 127.0.0.1  
ping local Host }
```

و به کمک دستور زیر مدت زمانی بر حسب میلی ثانیه برای دریافت پاسخ تعیین می گردد.

```
Ping -w [name  
IP]
```

بعضی مواقع ممکن است یک شرکت فراهم کننده اینترنت، پروتکل Ping را مسدود کرده باشند. در این صورت سیستم به Ping جواب نمی دهد ولی به http پاسخ خواهد داد.



✓ فصل اول: آشنایی با مفاهیم کاربردی شبکه

استفاده از دستور زیر سبب می گردد تا هنگام دریافت پاسخ سیستم نسبت به ارسال بسته به صورت نامحدود اقدام نماید.

```
Ping -t [name  
IP]
```

و حتی توسط دستور ذکر شده در زیر می توان تعداد بسته های ارسالی را هم مشخص نمود:

```
ping -n [name  
IP]
```

دستور زیر طول بسته ارسالی را برحسب بایت نیز مشخص می کند:

```
ping -L [name  
IP]
```

و این دستور نام ماشین را ارسال می نماید:

```
ping -a IP Address
```

برای *travel shooting* و ردگیری شبکه WAN و پی بردن به روترهای موجود در مسیر می توان از دستورهای زیر استفاده نمود:

```
Tracert {Name  
IP}
```

```
Tracert -d WWW.Yahoo.com
```

برای آگاهی از وضعیت سرویس گیرنده ها و پورت ها نیز می توان از دستورهای زیر استفاده نمود.

```
arp -a
```

```
netstat -n
```

```
netstat -a
```

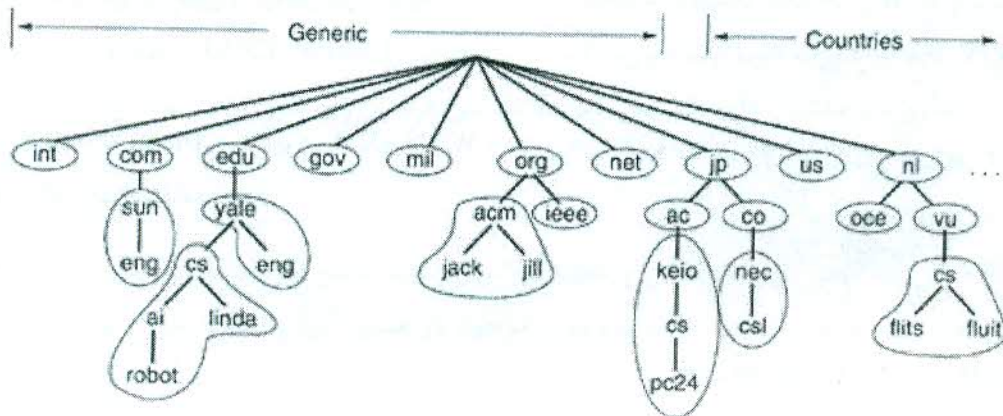
سرویس DNS

همان گونه که در ابتدا بیان گردید ¹ DNS یکی از سرویس های اصلی و پایه در شبکه های مبتنی بر IP و از جمله اینترنت است. به گونه ای که بدون وجود آن عملا کلیه سرویس های دیگر از کار خواهند افتاد. به همین جهت یکی از چهار پارامتر اصلی ² در تنظیمات شبکه مبتنی بر TCP/IP، تعریف یا مشخص کردن سرویس دهنده DNS است.

¹ - Domain Name Service

² - IP, Subnet, Gateway, DNS

فسفله اصلی سرویس DNS جهت حل مسائل آدرس دهی است. سیستم های کامپیوتری از اعداد برای آدرس دهی استفاده می کنند در حالی که انسان ها با اسامی راحت تر هستند؛ بنابراین سرویس DNS مانند یک دفترچه تلفن برای اینترنت است که در آن اسامی افراد یا اسامی مقصدها و شماره تلفن ها با نشانی های IP متناظرند. سرویس دهنده DNS نام سایتی مانند www.yahoo.com را دریافت نموده و نشانی IP متناظر آن، مثلا 87.248.113.14 را برمی گرداند. DNS در حقیقت یک پایگاه داده توزیع شده است. به این معنی که اطلاعات آن در تعداد زیادی دستگاه در سراسر جهان پخش شده اند به همین جهت، این ساختار قابل توسعه است. نحوه اسم گذاری و مدیریت اسامی دارای ساختاری سلسله مراتبی و درختی است که در شکل ذیل نمایش داده شده است.

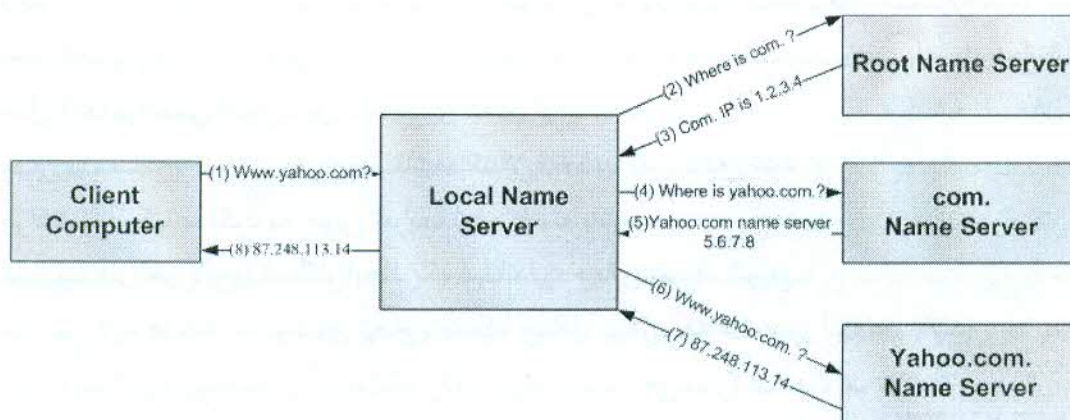


شکل ۳۲: ساختار درختی در نام گذاری اینترنتی

همان طور که در شکل ۳۲ نشان داده شده است نام گذاری از یک ریشه شروع می شود که آن را با نقطه (.) نشان می دهند و به دو شکل نام گذاری عمومی و کشوری انشعاب می یابد: در نام گذاری عمومی، با توجه به موضوع، پسوند خاصی تعریف می شود برخی پسوندهای معروف عبارتند از COM؛ مخفف Commercial برای نشانی های تجاری، org مخفف Organization برای سازمان ها، NET مخفف Network برای شبکه ها و سرویس دهنده ها، EDU برای دانشگاه ها و.... در نام گذاری کشوری به هر کشور دو کاراکتر اختصاص داده می شود و سطح اول نام گذاری با این دو کاراکتر مشخص می شود. مانند ir برای ایران، ca برای کانادا، uk برای انگلستان و سطح دوم نام گذاری مشابه حالت عمومی با توجه به موضوع پسوند داده می شود. مثلا برای تجاری com و برای دانشگاهی ac.

نام گذاری عمومی توسط سازمان های جهانی مدیریت می شوند و برای این که بتوان یک نام از این گروه در اختیار گرفت باید از طریق این سازمان ها یا کارگزاران آنها اقدام به ثبت دامنه^۱ نمود. نام گذاری کشوری توسط خود همان کشور مدیریت می شود به عنوان مثال در ایران ir توسط مرکز تحقیقات فیزیک نظری مدیریت شده و برای ثبت دامنه می باید از طریق آن یا کارگزاران آن اقدام نمود برای اطلاع بیشتر به سایت www.nic.ir رجوع کنید.

نحوه مدیریت اطلاعات DNS مشابه نام گذاری، یک مدیریت سلسله مراتبی است به این معنی که در سطح اول Name Server های ریشه قرار دارند برای اسامی با ساختار عمومی که به صورت جهانی مدیریت می شوند در حال حاضر ۱۳ Name Server وجود دارند که با اسامی a.root-servers.net الی m.root-servers.net مشخص می شوند. این سرورها در نقاط مختلف جهان قرار گرفته اند و در هر لحظه یک کپی از اطلاعات سطح اول اسامی را در بر دارند. اطلاعات سطح اول مشخص می کند که نشانی های IP مربوط به هر یک از سرورهای اسامی سطح بالا^۲ مانند com. ، org. ، net. و.... در کجا قرار دارند. این سرورهای اسامی سطح بالا، نیز هر کدام نشانی های IP مربوط به Name Server های Domain های تعریف شده را نگه می دارند مثلا TLD Server مربوط به com نشانی یا نشانی های IP تمام Domain هایی که با com ختم می شوند را در بردارد. در سطح آخر، Name Server های Domain ها قرار دارند مانند Name Server سایت yahoo.com این Name Server ها توسط خود سازمان یا شرکت مربوطه مدیریت می شوند و شرکت می تواند برای خود اسامی مختلف با نشانی IP متناظر ایجاد کند مثلا www.yahoo.com را تعریف نماید. با توجه به توضیحات فوق در شکل ۳۳ مراحل تبدیل یک اسم اینترنتی، به IP مشخص شده است.



شکل ۳۳: مراحل تبدیل یک اسم اینترنتی به IP

^۱ - Domain Registration

^۲ - Top Lever Domains



✓ فصل اول: آشنایی با مفاهیم کاربردی شبکه

- همان طور که در شکل فوق مشخص گردیده است تبدیل یک نام به IP که اصطلاحاً Resolve گفته می شود در ۸ مرحله انجام می پذیرد:
۱. دستگاه سرویس گیرنده تقاضای تبدیل نام (مثلاً www.yahoo.com) به IP را به DNS Server محلی خود، که همان IP می باشد که در تنظیمات شبکه دستگاه Client به عنوان DNS Server تعریف شده است، ارسال می کند.
 ۲. Name Server محلی، از Root Server تقاضای ارسال نشانی IP مربوط به Name Server Com را می کند.
 ۳. Root Server در پاسخ نشانی TLD Name Server COM را بر می گرداند.
 ۴. Name Server محلی، از Name Server COM می خواهد تا نشانی Name Server Yahoo.com را ارسال کند.
 ۵. Name Server COM نشانی Name Server Yahoo.com را بر می گرداند.
 ۶. Name Server محلی، از Name Server Yahoo.com نشانی IP مربوط به www.yahoo.com را سوال می کند.
 ۷. Name Server Yahoo.com نشانی IP متناظر با www.yahoo.com را بر می گرداند.
 ۸. Name Server محلی، نشانی یافته شده را در اختیار Client قرار می دهد.

لایه های شبکه در مدل مرجع OSI

مدل OSI^۱ که در حدود سال های ۱۹۸۳ توسط ISO^۲ مطرح شد سعی دارد تا یک الگوی جامع ارائه نماید تا شبکه های کامپیوتری بتوانند از طریق آن با یکدیگر ارتباط برقرار کنند. (چنین شبکه های کامپیوتری را که تمایل به برقراری ارتباط با هم دارند اصطلاحاً سیستم های باز^۳ نامیده اند) در مدل OSI بر اساس اصول ذیل لایه بندی انجام گرفته است:

وقتی یک سطح جدید از انتزاع نیاز باشد یک لایه جدید تعریف می شود.

هر لایه باید یک عملکرد به خوبی تعریف شده داشته باشد.

عملیات های هر لایه با دیدگاه ایجاد یک استاندارد جهانی تعریف شوند.

مرز بین لایه ها باید به گونه ای انجام شود که حداقل تبادل اطلاعات بین آنها نیاز باشد.

^۱ - Open Systems Interconnection

^۲ - International Standard Organization

^۳ - Open System



تعداد لایه ها باید به اندازه ای باشد که نیاز به قراردادن عملیات های قابل تفکیک در یک لایه وجود نداشته باشد و از طرفی تعداد لایه ها آنقدر زیاد نباشد که باعث شود معماری ارائه شده بیش از حد لایه بندی گردد (تعداد لایه ها باید لازم و کافی باشد).

از آنجا که دانستن اینکه هر یک از تجهیزات شبکه در چه لایه ای از شبکه و چگونه کار می نماید ضروری می باشد لذا در این بخش به مدل OSI که شبکه را به هفت لایه به ترتیب زیر تقسیم می کند اشاره می گردد.

- 7- Application
- 6- Presentation
- 5- Session
- 4- Transport
- 3- Network
- 2- Data link
- 1- Physical

وظایف هر کدام به طور مختصر به شرح زیر می باشد:

لایه ۷: این لایه وظیفه برقراری ارتباط کاربر یا برنامه کاربردی را با شبکه بر عهده دارد. این لایه مجموعه متنوعی از پروتکل ها را شامل می شود در واقع هر کاربردی برای خود یک پروتکل دارد. نمونه های متداول کاربردها مانند (http) Web، FTP، Telnet، Email و همگی در این لایه مطرح می شوند.

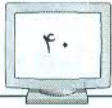
لایه ۶: عملیات اصلی این لایه امکان برقراری ارتباط میان دو سیستم با ساختار اطلاعات متفاوت است (مثلا یک طرف از ساختار عدد صحیح و طرف دیگر از ساختار Character Set استفاده کند). در این لایه مجموعه ای از ساختارهای داده ای انتزاعی^۱ ایجاد می گردد که اطلاعات در سمت فرستنده از فرمت فرستنده به آن تبدیل شده و در سمت گیرنده از فرمت انتزاعی به فرمت گیرنده. به عبارت دیگر در این لایه نحوه کدینگ و نمایش اطلاعات مشخص می گردد و در همین لایه، رمزنگاری هم انجام می شود.

لایه ۵: این لایه آداب و رسوم یک ارتباط را بر عهده دارد و از آنجائی که شروع ارتباط ممکن است با نام کاربری و کلمه عبور باشد لذا امنیت نیز در این لایه مطرح می شود.

لایه ۴: این لایه که به لایه انتقال معروف است، نحوه انتقال اطلاعات^۲ را مشخص می کند. در این لایه واحد انتقال اطلاعات، قطعه^۱ می باشد. عمل اصلی در این لایه دریافت اطلاعات از لایه

^۱ - abstract data structures

^۲ - Connection Oriented Connection Less



✓ فصل اول: آشنایی با مفاهیم کاربردی شبکه

Session و تبدیل آن به قطعه یا قطعات (شکستن بسته اطلاعاتی لایه Session در صورت لزوم) دیگر است.

لایه ۳: وظیفه این لایه مسیریابی و کنترل عملیات Subnet در شبکه می باشد. در این لایه واحد انتقال اطلاعات، بسته^۲ می باشد. محور اصلی عملکرد، مسیریابی بسته‌ها می باشد که این کار می تواند به صورت ثابت و از پیش تعریف شده^۳، در ابتدای هر اتصال و یا به صورت کاملاً پویا^۴ عمل کند.

مساله مدیریت ازدحام^۵ که به واسطه ایجاد تراکم بسته‌ها در گلوگاه‌ها حاصل می‌گردد؛ همچنین تضمین کیفیت سرویس QoS^۶ برعهده این لایه است.

باید توجه داشت که در شبکه‌هایی با تکنولوژی انتقال Broadcast، این لایه بسیار نازک بوده و یا اصلاً وجود ندارد (زیرا همان گونه که قبلاً گفته شد در این شبکه‌ها بحث مسیریابی مطرح نیست و همه پیام را دریافت می‌کنند)

لایه ۲: در این لایه فریم تشکیل و مکانیزمی برای تشخیص خطا^۷ در فریم فراهم می‌شود. یعنی در این لایه داده‌ها در فریم منتقل می‌شوند. فریم‌ها به صورت فریم‌های داده یا فریم‌های تأییدیه^۸ می‌باشند.

برای مشخص کردن فریم‌ها از یک سری الگوهای بیتی خاص به نام جداکننده^۹ استفاده می‌شود. مشکلات مربوط به انتقال فریم‌ها مانند گم شدن، تخریب و یا تکراری شدن آنها (که به واسطه از دست رفتن تأییدیه حاصل می‌شود) باید در این لایه حل شوند. در این لایه همچنین مکانیزم‌هایی جهت همگام کردن دو طرف لینک به صورت Flow Regulation وجود دارد.

در شبکه‌هایی که از تکنولوژی Broadcast استفاده می‌کنند یک زیر لایه به نام Media Access Sub layer اضافه می‌شود که مسولیت مدیریت محیط انتقال مشترک را برعهده دارد.

لایه ۱: واحد انتقال اطلاعات در این لایه بیت می‌باشد یعنی در این لایه فریم تبدیل به بیت و سپس به سیگنال تبدیل می‌شود. کلیه مسائل در این لایه حول موضوع نحوه انتقال بیت‌های خام روی محیط فیزیکی انتقال، واسط‌های مکانیکی و الکتریکی می‌باشد.

¹ - Segment

² - Packet

³ - static routing

⁴ - Dynamic routing

⁵ - Congestion

⁶ - Quality of Service

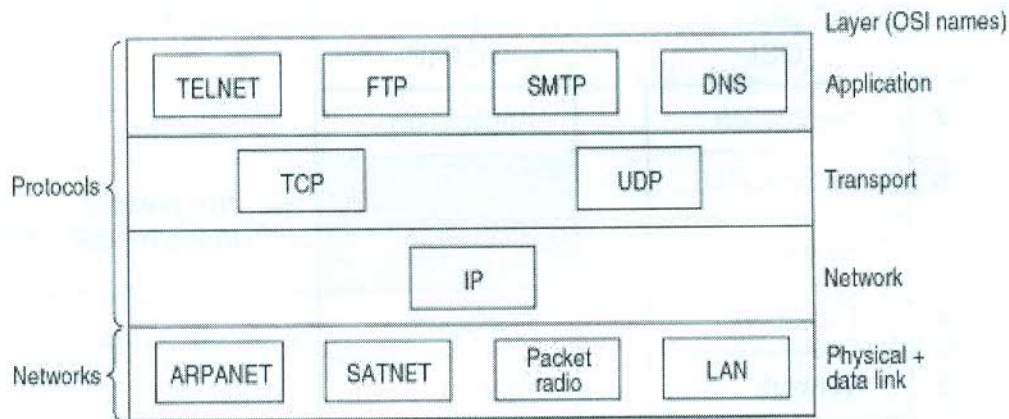
⁷ - Error Detection

⁸ - Acknowledge

⁹ - Delimiter

مدل TCP/IP

مدل کاربردی امروزی است که شبکه اینترنت بر آن استوار است، این مدل TCP/IP از شبکه ARPANET برگرفته شده که نخستین بار در سال ۱۹۷۴ مطرح شد. مدل اساسا توسط وزارت دفاع آمریکا طراحی شد و هدف اصلی آن ایجاد شبکه ای بود که در شرایط سخت و حتی بروز جنگ هسته ای از کار نیفتد؛ یعنی با قطع یک نقطه از شبکه، کل شبکه مختل نشود. این امر منجر به طراحی یک شبکه، مبتنی بر سوئیچ بسته ای^۱ شد که با گسترش و توسعه آن در کل دنیا امروزه به شبکه اینترنت تبدیل شده است.



شکل ۳۴: لایه های شبکه بر اساس مدل TCP/IP

مدل TCP/IP که در شکل ۳۴ مشخص شده است دارای چهار لایه است: لایه Host-to-Network: در این لایه ارتباط یک سیستم با شبکه به طوری که قابلیت تبادل بسته IP را داشته باشد تامین می گردد. در این لایه که تلفیق دو لایه فیزیکی و لینک داده در مدل OSI است استاندارد عمومی را TCP/IP تعریف نمی کند و شرایط از شبکه به شبکه دیگر و سیستم به سیستم دیگر متدوال است لذا TCP/IP به لحاظ تعریف ساختاری، در این لایه بسیار مبهم است. لایه شبکه یا Network:

این لایه یک لایه بدون اتصال است^۲ می باشد. پروتکل این لایه IP^۳ نام دارد و ساختار بسته ها در قالب IP Packet مشخص می شوند. متقابلا با مدل OSI مساله مسیر یابی بسته ها، موضوع اصلی این لایه است.

^۱ - Packet Switched Network

^۲ - Connection Less

^۳ - Internet Protocol



✓ فصل اول: آشنایی با مفاهیم کاربردی شبکه

لایه انتقال یا Transport:

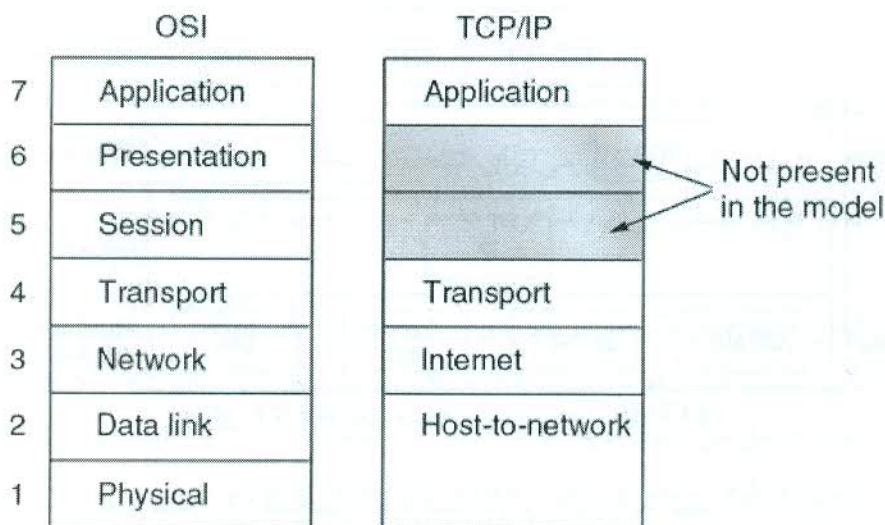
در این لایه ارتباط به صورت انتها به انتها^۱ مطرح است و دو نوع پروتکل در این لایه وجود دارد:

TCP^۲: که یک ارتباط از نوع اتصال محور مطمئن^۳ ایجاد می کند.

UDP^۴: یک ارتباط از نوع ارتباط بدون اتصال غیر مطمئن^۵ ایجاد می کند.

لایه کاربرد یا Application:

شامل تمامی پروتکل های لایه بالا مانند: FTP (پروتکل انتقال فایل)، SMTP (پروتکل انتقال mail)، DNS (پروتکل تبدیل اسامی به IP)، NNTP (پروتکل سرویس News)، HTTP (پروتکل Web) و



شکل ۴۵: مقایسه دو مدل OSI و TCP/IP

مقایسه OSI و TCP/IP:

مدل TCP/IP دارای ۴ لایه است ولی OSI دارای ۷ لایه می باشد.

در OSI سه مفهوم Service, Interface, Protocol به طور صریح از هم تفکیک شده اما در TCP/IP آنقدر صریح نیست.

در OSI ابتدا لایه ها طراحی شده و سپس پروتکل ها بر اساس آن تعریف شده اند ولی در TCP/IP ابتدا پروتکل ها طراحی شده اند و سپس لایه ها با آنها تطابق یافته اند.

¹ - End-to-End

² - Transmission Control Protocol

³ - Reliable Connection-Oriented

⁴ - User Datagram Protocol

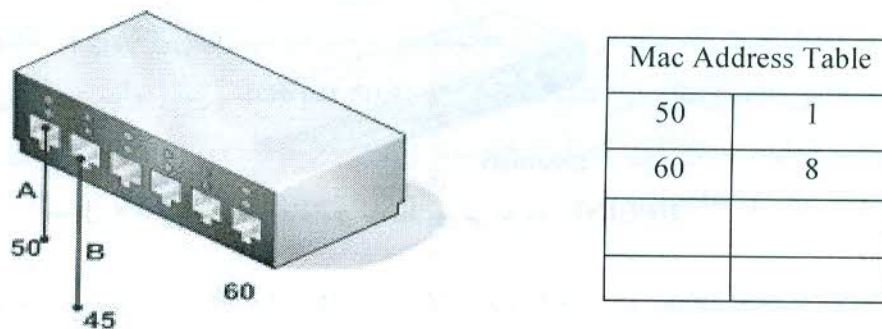
⁵ - Unreliable Connection-less

در OSI لایه شبکه هم امکان هر دو سرویس بدون اتصال و با اتصال را فراهم می کند ولی در TCP/IP لایه شبکه فقط بدون اتصال است و این لایه انتقال است که این دو سرویس را فراهم می کند. در این مدل لایه بندی به خوبی انجام شده ولی پروتکل ها بر خلاف مدل TCP/IP آن طور که باید، توصیف و پیاده سازی نشده اند.

لازم است بدانید که روتر در لایه ۱، ۲ و ۳ کار می کند. سوئیچ هم وقتی یک فریم به آن می رسد آدرس فیزیکی مقصد را چک کرده و سپس آن را ارسال می کند. پس سوئیچ در لایه ۲، ۱، کار نموده، کارت شبکه و مودم هم در لایه ۱ و ۲ کار می کنند. و از آنجا که وقتی یک فریم به هاب و تکرار کننده می رسد، آن را به همه جا ارسال می کند لذا می توان فهمید که هاب در لایه یک کار می کند. تکرار کننده^۱ وظیفه تقویت سیگنال را برعهده دارد. در تکنولوژی Bus اگر فاصله از ۱۸۵ متر بیشتر باشد از تکرار کننده استفاده می گردد.

نحوه عملکرد سوئیچ در شبکه

نحوه عمل سوئیچ در ابتدای کار، همانند هاب بوده یعنی در هنگام ارسال بسته تمام پورت های آن باز می باشد. اما در همان لحظه آدرس فیزیکی هر پورت را دانسته و جدول آدرس های فیزیکی خود را جهت ارسال داده های در دفعات بعدی کامل می کند. به مثال زیر دقت نمایید:



شکل ۳۶: یک سوئیچ با جدول آدرس های فیزیکی

ظرفیت جدول آدرس های فیزیکی سوئیچ در کاتالوگ آن نوشته شده است. در نظر بگیرید که یک هکر روی یک پورت نشسته و جدول آدرس های فیزیکی را در سوئیچ به هم بریزد لذا بحث امنیت در سوئیچ هم مطرح می باشد.

^۱ - Repeater

سوئیچ های عادی را سوئیچ لایه ۲ گویند و این سوئیچ ها روی آدرس فیزیکی تصمیم می گیرند اما سوئیچ های دیگری معروف به سوئیچ لایه ۳ وجود دارد که روی IP Address تصمیم می گیرند. هنگام انتخاب سوئیچ و کارت شبکه موارد زیر را باید در نظر گرفت:

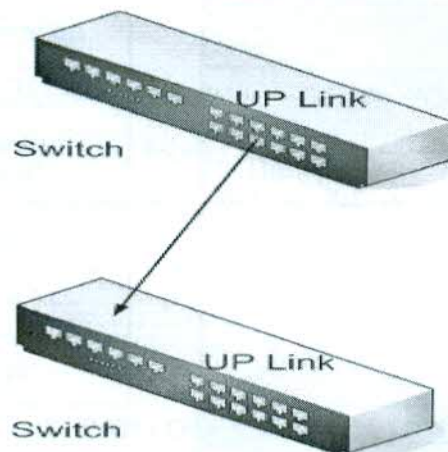
۱- سرعت و تعداد پورت ها

۲- قابلیت توسعه و ارتباط با ماشین های دیگر^۱

۳- مدیریت^۲

۴- روش های دسترسی به سوئیچ

در صورتی که در نظر است سوئیچ های یک رک به هم متصل گردد از قابلیت توسعه آنها استفاده می شود. لازم به ذکر است که پورتی به نام UPLINK به همین منظور در سوئیچ ها تعبیه شده است. ممکن است این اتصال توسط پورتی بجز UPLINK هم به صورت سالم و بدون خطا برقرار شود که به این حالت سوئیچ ها AutoSense هستند.



شکل ۳۷: نحوه اتصال سوئیچ توسط پورتی به نام UPLINK

به عنوان مثال توسط سوئیچ های 3 com مدل ۴۴۰۰ حداکثر ۸ قابل توسعه دارند به شرطی که مجموع پورت ها از ۱۹۲ عدد بیشتر نشود.

ویژگی بعدی سوئیچ ها، قابل مدیریت و برنامه ریزی بودن و نیز همچنین هوشمند یا غیر هوشمند بودن آنهاست.

یک دیگر از ویژگی های سوئیچ، چگونگی دستیابی ماشین ها به محیط انتقال^۳ است. برای این کار روش های متعددی وجود دارد. نخستین روش Carrier Sense می باشد یعنی اگر خط آزاد بود

^۱ - Stackable

^۲ - Management

^۳ - Access method



✓ فصل اول: آشنایی با مفاهیم کاربردی شبکه

داده ارسال می گردد. روش دیگر CDMA بوده که این روش به دلیل اینکه قابل پیش بینی نبوده، فاقد نظم است و مدیریتی روی آن نیست، اولویتی ندارد.

پیکربندی سوئیچ

با استفاده از پورت کنسول RS232 و همچنین سرویس های RMON , SNMP , HTTP , Telnet می توان سوئیچ ها را پیکربندی نمود. موارد مهمی که در پیکربندی یک سوئیچ باید مورد توجه قرار گیرند به شرح زیر می باشد:

هوشمند بودن^۱ سوئیچ: یعنی این که اگر یک کامپیوتر به کمک کارت شبکه به یک سوئیچ متصل گردد و به هر دلیلی کارت شبکه معیوب شود به طوری که باعث ایجاد تصادم^۲ شود هاب و سوئیچ هوشمند این تصادم را منتقل نمی کند.

ارسال و دریافت همزمان^۳ در سوئیچ

نکته دیگر در مورد سوئیچ ها، قابلیت ارسال و دریافت همزمان داده در آنها طبق بلوک دیاگرام زیر است:



لازم به ذکر است که هاب از چنین خصوصیتی برخوردار نیست زیرا چون در تکنولوژی هاب وقتی یک ماشین داده ارسال می کند، تمام پورت های آن باز است و نمی تواند هم زمان داده ای دیگر را دریافت نماید. ضمن این که این خاصیت زمانی خوب کار می کند که تمامی تجهیزات مدنظر محصول یک کارخانه باشد.

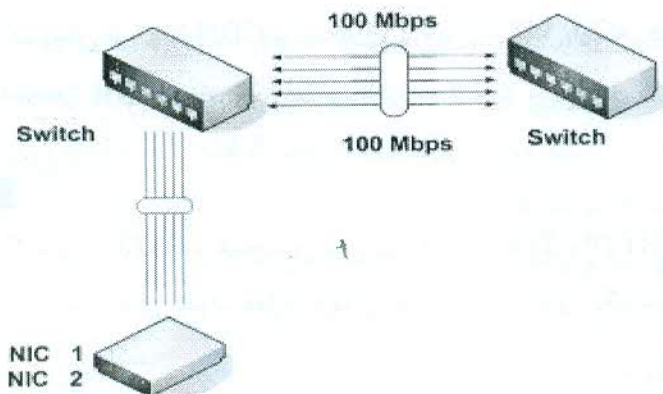
Port Trunking

این قابلیت فقط مختص سوئیچ می باشد. این ویژگی اجازه می دهد بین دو سوئیچ مطابق شکل زیر دو لینک یا بیشتر داشته داشته تا تشکیل کانال دهیم.

¹ -Smart

² -Collision

³ -Full Doublex



شکل ۳۸: استفاده از قابلیت Port Trunking برای اتصال دو سوئیچ

اندازه فیزیکی سوئیچ

سوئیچ‌ها را از نظر اندازه فیزیکی به دو دسته رومیزی^۱ و قابل نصب در رک^۲ وجود دارد.

اولویت بندی ترافیک شبکه^۳

این سرویس اجازه می‌دهد تا ترافیکی را که به سوئیچ می‌رسد بررسی نموده و آن را اولویت بندی نماید. برای این کار در سوئیچ‌ها چند صف تشکیل می‌دهد (به عنوان مثال در سوئیچ‌های 3Com چهار صف) و ترافیک اولویت بندی شده در صف‌ها ارسال می‌گردد. معمولاً ترافیک‌های صدا و تصویر در اولویت بالاتر قرار دارند.

رمزنگاری^۴

بعضی سوئیچ‌ها قابلیت رمزنگاری دارند. کارت شبکه نیز می‌تواند از چنین قابلیت‌هایی برخوردار باشد. اکنون چند سوال مهم مطرح و به آنها پاسخ داده می‌شود.

در شبکه زیر اگر لینک ارتباطی ۱۰۰۰ مگا بیت در ثانیه، به ۱۰۰ تبدیل شود چه تاثیری در کل شبکه دارد؟

پاسخ: چون ترافیک Broadcast روی سایت ۱ زیاد است وقتی سرعت بالایی Broadcast نیز با سرعت بیشتری به Control Site می‌رسد لذا باید به فکر کاهش Broadcast بود.

^۱-Desktop

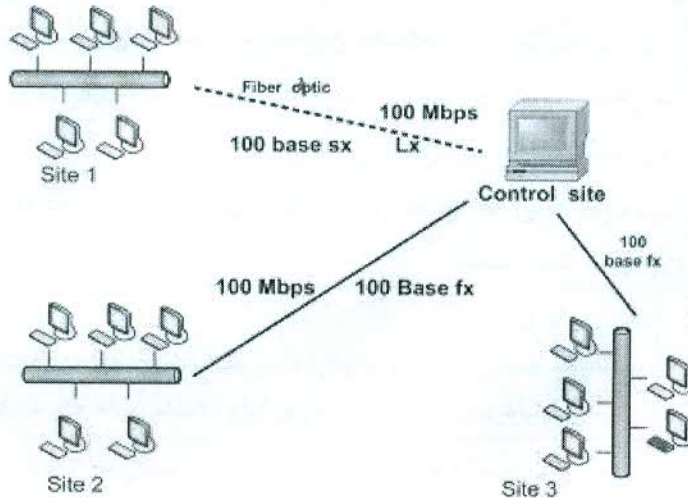
^۲-Rack Mount

^۳-Quality of Service

^۴-Encryption

✓ فصل اول: آشنایی با مفاهیم کاربردی شبکه

سوال: آیا خرابی یا کثیف بودن یک کانکتور تاثیری در سرعت شبکه دارد؟
 پاسخ: خرابی کانکتور باعث می شود که برای فرستادن بسته، دوباره سعی شود^۱ و این کار باعث کندی شبکه می شود.



شکل ۳۹: مثالی از یک شبکه جهت بررسی مشکلات احتمالی

سوال: آیا یک فن کویل در شبکه تاثیر دارد؟
 پاسخ: هر چیزی که سیم پیچ داشته باشد در شبکه موثر است. به همین خاطر توصیه شده که فاصله بین سیم های برق و کابل شبکه حداقل ۲۰ الی ۳۰ سانتی متر باشد.
 برای داشتن یک شبکه خوب توجه به نکات زیر ضروری است:
 طراحی توپولوژی در آن به درستی انجام شود یعنی تجهیزات اکتیو و پسیو به درستی انتخاب شوند.
 قطعات و تجهیزات، اعم از اکتیو و پسیو به دقت نصب شود و نگهداری و نظافت آنها نیز طبق دستورالعملی در فواصل زمانی مشخص ادامه داشته باشد.
 یک سوکت RG45 اگر به طور کامل پرس نگردد نویز و پارازیت، مخصوصا در فرکانس های ۱۰۰ و ۱۰۰۰ ایجاد می گردد.
 - پیکربندی تجهیزات اکتیو و مونیتورینگ آنها به دقت و مستمر انجام شود.
 - نوع پروتکل، سیستم عامل ایستگاه ها، سرورها، نوع نرم افزار و سرویس ها به دقت انتخاب و نصب شود و پیکربندی آنها بر اساس نیاز صورت پذیرفته و به طور مستمر مانیتور شوند.

^۱ - Retry



✓ فصل اول: آشنایی با مفاهیم کاربردی شبکه

- عدم توانایی کاربر در تغییر پیکربندی، حذف و نصب برنامه ها و سرویس ها.
- کنترل دسترسی به اینترنت
- استفاده از ضد ویروس های مطمئن و به روز بر روی سرویس دهنده ها و سرویس گیرنده ها
- آموزش کاربران و مسئولین کامپیوتر در سطوح مختلف.

آشنایی با نرم افزار Packet Tracer

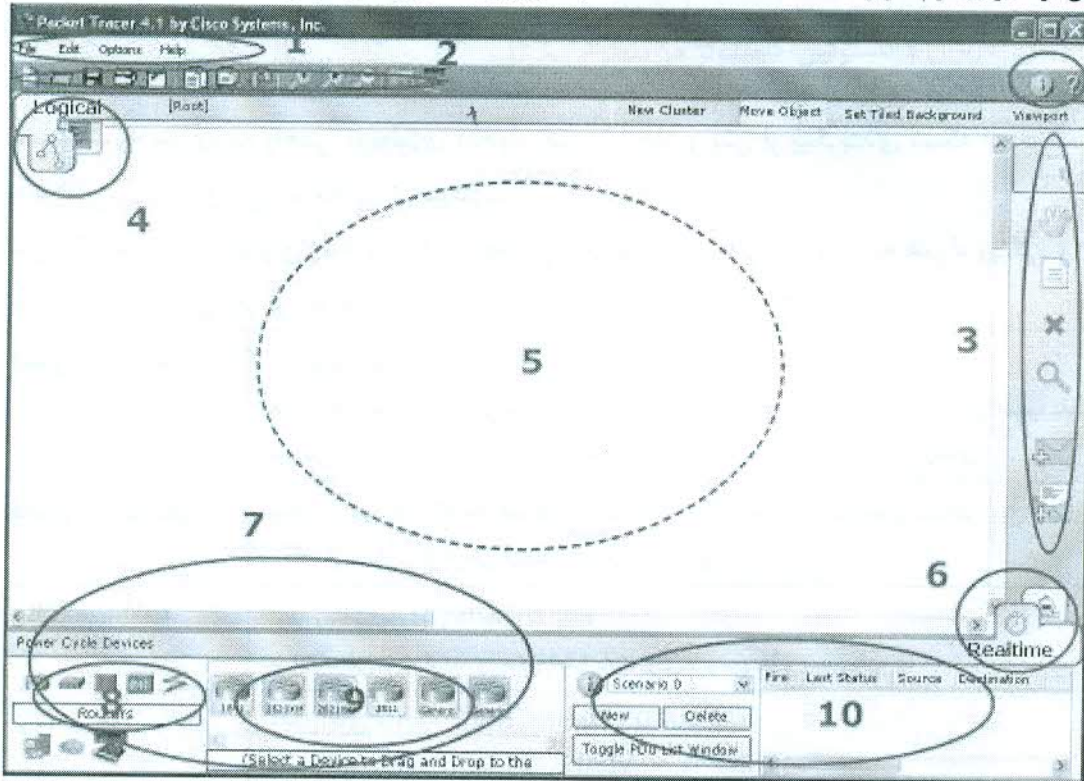
نرم افزار Packet Tracer یک محیط شبیه سازی جهت طراحی، پیاده سازی توپولوژی، پیکربندی، بررسی مشکلات و ... را در شبکه دارند. کاربران می توانند با استفاده از ابزارهای مورد نظر در محیط شبیه سازی، به راحتی توپولوژی دلخواه خود را ایجاد و پس از پیکربندی شبکه ایجاد شده، به بررسی، تحلیل و رفع مشکلات آن پردازند.

انواع تکنولوژی ها و توپولوژی هایی که توسط این نرم افزار پشتیبانی می شود به همراه ویژگی های اصلی آن در جدول زیر آورده شده است:

<p>ایجاد توپولوژی شبکه دستگاه ها: عمومی، واقعی و ماژولار، مسیریاب، سوئیچ، میزبان، هاب، پل، بی سیم، نقطه دسترسی، ارتباط بین دستگاه ها از طریق انواع مختلف رسانه های شبکه بندی</p>	<p>فضای کار منطقی</p>
<p>سلسله مراتب دستگاه ها، فضاهای سیم بندی، ساختمان ها، شهرها و نماهای بین شهری، استفاده از تصاویر گرافیکی ایجاد شده توسط کاربر</p>	<p>فضای کار فیزیکی</p>
<p>به روز رسانی پروتکل ها بصورت زنده حد متوسطی از پیکربندی های IOS CLI برای سوئیچ ها و مسیریاب ها</p>	<p>حالت Realtime</p>
<p>پروتکل های LAN : CSMA/CD*, Ethernet, DHCP سوئیچینگ : VLANs, 802.1q, trunking TCP/IP : ARP, IP, ICMP, UDP, TCP* مسیریابی : static, default, RIPv1, RIPv2, EIGRP, inter-VLAN routing NAT : static, dynamic, overload ACLs: standard, extended, named WAN : HDLC, PPP, Frame Relay* * نشان دهنده این است که شامل محدودیت های قابل ملاحظه ای هستند</p>	<p>پروتکل ها</p>
<p>Packet animation Global event list (packet sniffer) OSI Model, Detailed PDU, and Device Table Views User-defined multiple packet scenarios</p>	<p>حالت شبیه سازی (Simulation)</p>
<p>گزینه های متنوع ذخیره سازی فایل Activity Wizard برای فعالیت های تمرینی با تصحیح اتوماتیک Challenge Mode با امکان تصمیم گیری کاربران در مورد نحوه اجرای الگوریتم روی بسته ها ویژگی های متنوع برای توضیحات متنی و گرافیکی</p>	<p>طراحی و به اشتراک گذاری</p>

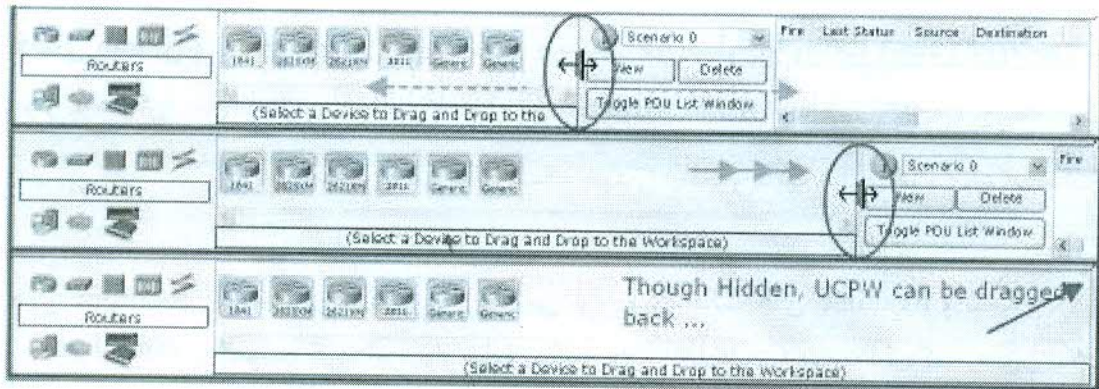
شروع کار با Packet Tracer

پس از اجرای نرم افزار Packet Tracer 4.1، محیط زیر رابه طور پیش فرض مشاهده خواهید کرد:



این واسط آغازین شامل ۱۰ جزء است. برای آگاهی از عملکرد هر جزء خاص، تنها کافیست نشانگر ماوس را بر روی آن حرکت داده تا توضیح مربوط به آن نمایش داده شود.

شامل منو های File ، Options و Help که دستورات رایجی نظیر Open، Save ، Print و Preferences در این منوها قرار گرفته اند.	نوار منو
شامل آیکن های میانبر برای دستورات منوی File و Edit و شامل دکمه هایی برای بزرگنمایی، پالت ترسیم، و مدیریت الگوها (Device Template Manager) است. در سمت راست آن دکمه Network Information قرار دارد که می توانید توضیحات دلخواه خود را در مورد شبکه جاری در آن وارد کنید.	نوار ابزار اصلی
شامل دسترسی به ابزارهای رایج فضای کار: انتخاب، جابجایی لایه، درج توضیح، حذف، بررسی، افزودن PDU های ساده و افزودن PDU های پیچیده.	نوار ابزارهای رایج
می توان بین فضای فیزیکی و منطقی توسط این برگه ها سوئیچ نمود.	فضای فیزیکی /

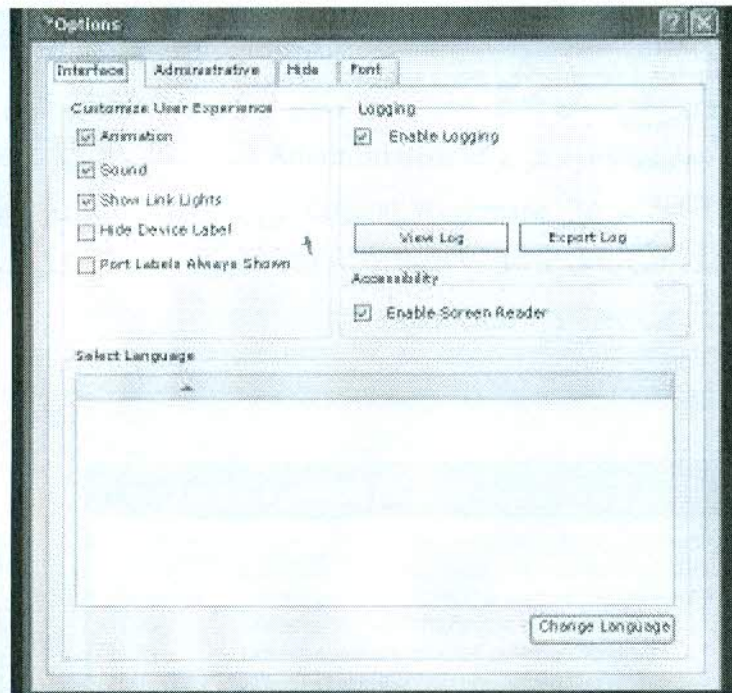


فضاهای کاری و حالت ها

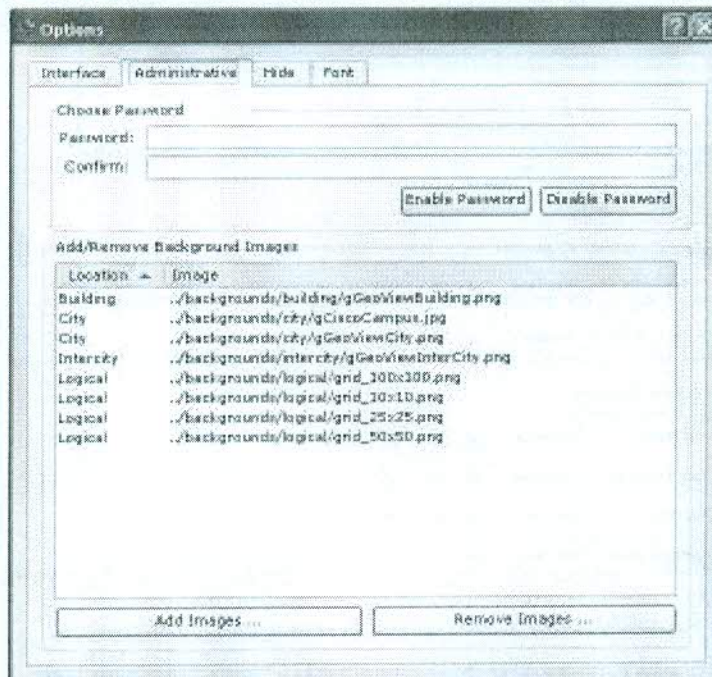
نرم افزار Packet Tracer 4.1 شامل دو فضای کاری منطقی و فیزیکی، و دو حالت Realtime و شبیه سازی است. هر شبکه را می توان در نمای منطقی ایجاد کرده و در حالت real time اجرای آن را مشاهده نمود. همچنین می توان برای اجرای سناریو های کنترل شده به حالت شبیه سازی سوئیچ نمود. برای تنظیم چیدمان فیزیکی وسایل، به حالت Physical Workspace می توان رفت. ذکر این نکته لازم است که امکان اجرای شبکه در حالت فیزیکی وجود نداشته و باید برای این منظور دوباره به فضای منطقی برگشت.

تنظیم علاقه مندی ها

نرم افزار Packet Tracer 4.1 را می توان به دلخواه تنظیم کرد. برای این کار از منوی Option دستور Preferences را اجرا، تا تنظیمات برنامه را مشاهده نمایید. در برگه Interface می توان تنظیمات صدا، انیمیشن و چراغ های اتصال را انجام داد تا با عملکرد سیستم شما متناسب شود. همچنین می توانید برچسب های ابزارها یا پورت ها را نیز مخفی نموده و یا نمایش داد. ویژگی logging امکان ثبت همه دستورات IOS وارد شده را فراهم می کند. ویژگی Enable Screen Reader Support نیز همه عنوان ها و توضیحات پنجره در حال نمایش را می خواند. زبان برنامه را نیز از قسمت Language می توان تغییر داد.



در برگه Administrative تصاویر زمینه ای که در برنامه فعال است را می توان مدیریت نمود. در این برگه امکان تعیین کلمه عبور برای جلوگیری از تغییرات ناخواسته نیز وجود دارد.



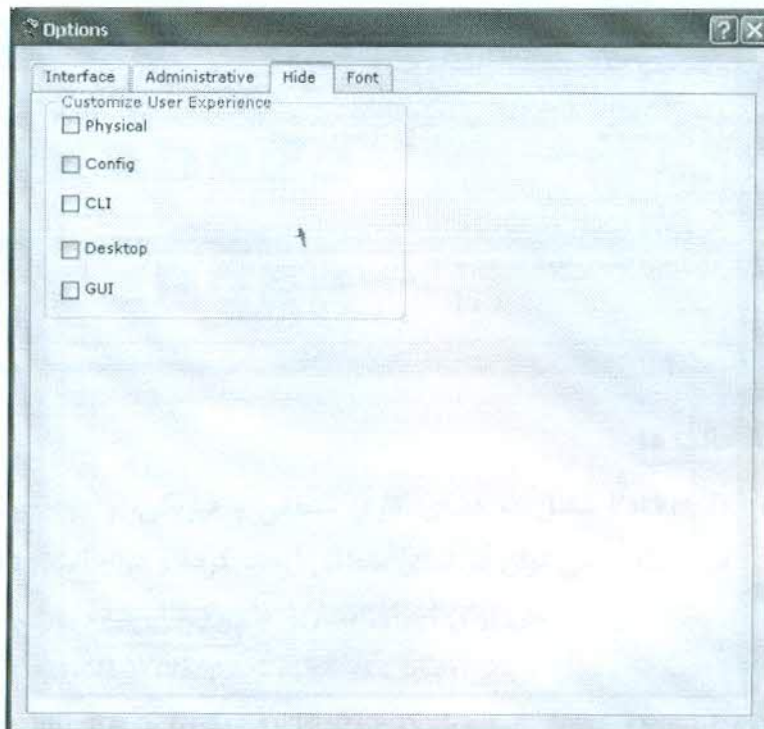
در برگه Hide هر یک از موارد مشخص شده را از پنجره برنامه یا کادرهای مختلف، می توان پنهان نمود.

فضای منطقی و نوار پیمایش	همچنین این نوار امکان پیمایش در سطوح گره ها، ایجاد گروه جدید، جابجایی اشیاء، تنظیم پس زمینه و دیدن پورت ها را می دهد.
فضای کار	در این محدوده می توان شبکه خود را ایجاد و شبیه سازی ها و انواع اطلاعات و آمار مربوط به آن را مشاهده نمود.
نوار Realtime /Simulation	توسط برگه های این نوار می توان بین حالت های Realtime و شبیه سازی سوئیچ کرد. این نوار شامل دکمه Power Cycle Devices ، دکمه های Play Control و نیز Event List در حالت شبیه سازی می باشد.
جعبه اجزای شبکه	جعبه ای است که توسط آن می توان دستگاه ها و اتصالات را برای قرار دادن در فضای کار انتخاب نمود. این جعبه شامل کادر انتخاب نوع وسیله و کادر انتخاب یک وسیله خاص می باشد.
جعبه انتخاب نوع دستگاه	این جعبه شامل انواع دستگاه ها و اتصالات موجود در Packet Tracer 4.1 می باشد. کادر Device-Specific Selection بر اساس نوع وسیله مورد انتخاب تغییر می کند.
جعبه انتخاب یک دستگاه خاص	کادری است که توسط آن می توان دستگاه یا اتصال مورد نظر شبکه خود را انتخاب نمود.
پنجره بسته های ایجاد شده توسط کاربر	این پنجره بسته هایی که در سناریوهای شبیه سازی در شبکه قرار می گیرند را مدیریت می کند.

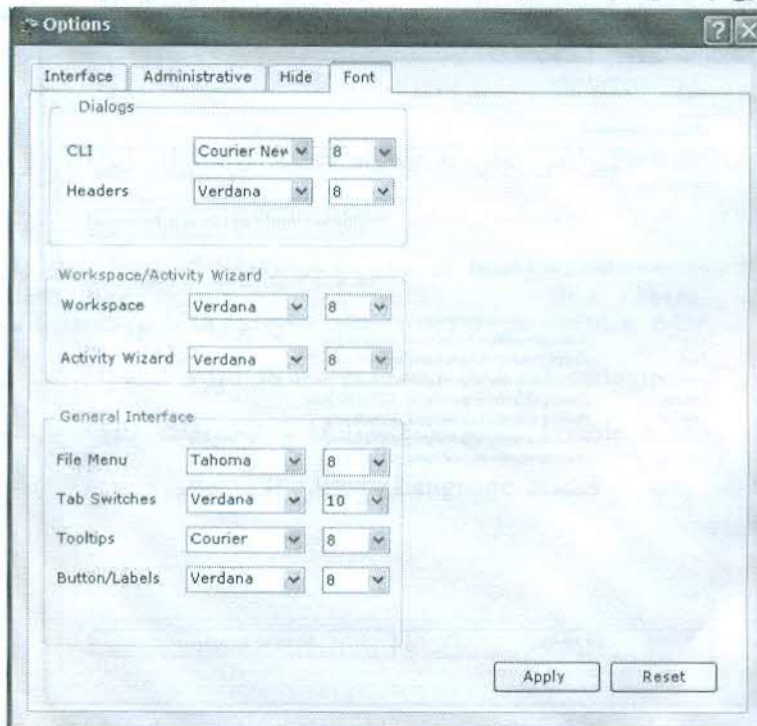
پنجره ها را توسط ماوس می توان به راحتی تغییر اندازه داده و همچنین با حرکت دادن آن به سمت راست پنهان نمود.



✓ فصل دوم: شبیه سازی شبکه توسط نرم افزار Packet Tracer

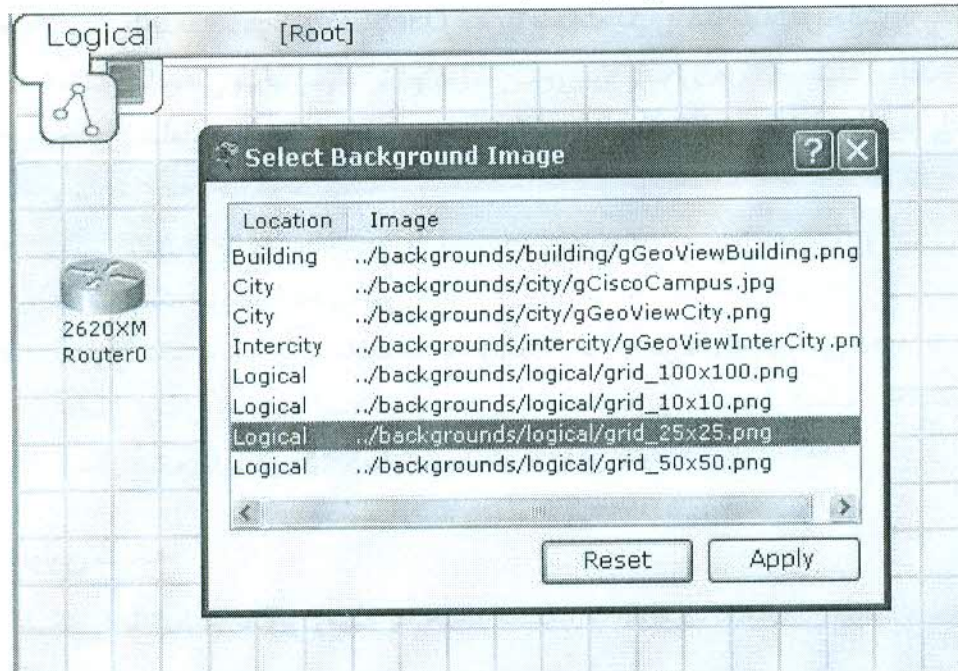


در برگه Font، نوع و اندازه فونت کادرها و واسط های مختلف تعیین می گردد.



تنظیم پس زمینه

در این بخش می توان یک فضای کاری سفید را با تصویر پس زمینه دلخواه جایگزین نمود. تصویر پس زمینه فقط از تصاویر موجود در برگه Administrative قابل انتخاب است. با کلیک روی دکمه Set Tiled Background در نوار Logical Workspace می توان تصویر زمینه را تنظیم نمود. از لیست تصاویر باز شده تصویر مورد نظر را انتخاب و دکمه Apply را کلیک کنید. برای برگشت به حالت اولیه کافیست دکمه Reset را کلیک کنید.



برای استفاده از تصاویر زمینه دلخواه، می توان آنها را در پوشه background/logical قرار داده و سپس به لیست موجود در برگه Administrative اضافه نمود. توجه کنید که این تصاویر تاثیری در عملکرد شبکه ندارند. قالب پیشنهادی برای این تصاویر png یا bmp (برای ترسیمات یا متن) و jpg (برای تصاویر حقیقی) می باشد.

اصطلاحات مهم

- ICMP Ping: دستوری که شامل یک پیغام تقاضای echo از یک وسیله به وسیله دیگر و پاسخ آن می باشد.
- آدرس IP: همانگونه که قبلا گفته شد یک آدرس ۳۲ بیتی است که به دستگاه ها برای شناسایی آنها در شبکه اختصاص داده شده است.



✓ فصل دوم: شبیه سازی شبکه توسط نرم افزار Packet Tracer

- اترنت: یکی از رایج ترین استانداردهای LAN برای سخت افزار، ارتباطات و کابل کشی می باشد.
- Fast Ethernet Interface: پورت اترنت با سرعت 100 Mbps است.
- مدل OSI: چهارچوب ۷ لایه ای برای بررسی پروتکل های شبکه و دستگاه ها است و شامل لایه های فیزیکی، پیوند داده، شبکه، انتقال، جلسه، ارائه، کاربرد می باشد.
- PDU: واحد داده پروتکل، یک گروه از داده متناسب با لایه در مدل OSI
- بسته: واحد داده در لایه سوم OSI که به صورت یک پاکت نامه در حالت Simulation نمایش داده می شود.
- جداول: شامل جداول مسیریابی، سوئیچینگ و ARP که شامل اطلاعات مرتبط با دستگاه و پروتکل های شبکه هستند.
- جدول ARP: جدول Address Resolution Protocol جفت آدرس IP و آدرس MAC کارت شبکه اترنت را ذخیره می کند.
- سناریو: یک توپولوژی با مجموعه ای از PUD ها که در شبکه قرار می دهید تا در زمان خاصی ارسال شوند. با استفاده از سناریو ها مختلف می توانید ترکیبات و حالت مختلف ارسال بسته ها را در یک توپولوژی یکسان بررسی کنید.

ایجاد اولین شبکه

ایجاد شبکه را با تنظیم تصویر زمینه به حالت مشبک از طریق دکمه Set Tiled Background شروع کنید

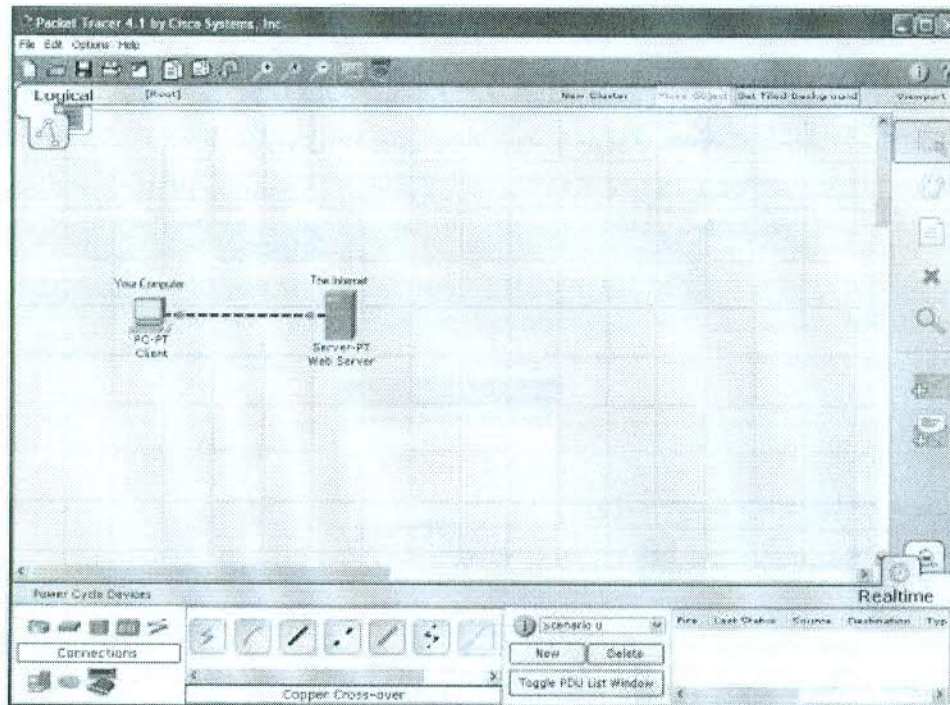
Generic PC را از End Devices انتخاب و آن را در فضای کاری قرار دهید. سه روش برای کسب اطلاعات بیشتر در مورد این وسیله وجود دارد. اول این که نشانگر ماوس را روی وسیله قرار داده تا اطلاعات پایه پیکربندی آن را مشاهده گردد. دوم این که با ابزار Select روی آن کلیک تا پنجره تنظیمات آن باز شود. سوم این که از ابزار Inspect استفاده کنید تا جداولی که این وسیله ایجاد می کند را مشاهده کنید. مثلاً در مورد این وسیله، جدول ARP نمایش داده خواهد شد. همیشه به خاطر داشته باشید که پس از مشاهده جداول، برای این که فضای کاری شلوغ نشود، آنها را ببندید.

پنجره تنظیمات PC را باز کنید و با رفتن به برگه Config تنظیمات آن، همچون نام آن را تغییر دهید. در قسمت Interface روی FastEthernet کلیک و آدرس IP را به صورت 192.168.1.1

✓ فصل دوم: شبیه سازی شبکه توسط نرم افزار Packet Tracer

تنظیم کنید. مطمئن شوید که وضعیت پورت On است. سایر ویژگی ها نظیر ماسک شبکه، آدرس MAC، پهنای باند و duplex نیز در هر زمان در این قسمت قابل تغییر است. رایانه دیگری را به فضای کار اضافه کنید. آدرس IP آن را 192.168.1.2 قرار داده و مطمئن شوید وضعیت پورت آن On است.

در قسمت Connections، کابل Copper Straight-through (خط مشکی) را انتخاب و اتصال بین این دو رایانه را برقرار کنید. خط قرمز نشان دهنده این است که اتصال کار نمی کند. حالا با استفاده از ابزار Delete این اتصال را حذف و از کابل Copper Crossover به جای آن برای برقرار ارتباط استفاده کنید. چراغ های سبز باید روشن شوند و اگر ماوس را روی هر یک از رایانه ها قرار دهید، می بایست وضعیت اتصال را به صورت up مشاهده کنید. شبکه شما باید شبیه تصویر باشد.



دستگاه ها را با درگ کردن جابجا کنید. با استفاده از دکمه i در گوشه بالا سمت راست نرم افزار، یک توضیح کلی ایجاد نمایید. سپس تعدادی برچسب متنی با استفاده از ابزار Place Note در Logical Workspace اضافه کنید.

روی رایانه اول یک بار کلیک نموده و در حالی که وضعیت چراغ های اتصال را مشاهده می کنید، رایانه را خاموش و سپس روشن نمایید.

همین کار را برای رایانه دوم نیز انجام دهید. مشاهده می کنید که خاموش کردن رایانه سبب قرمز شدن چراغ اتصال می شود که به معنای down شدن اتصال است.

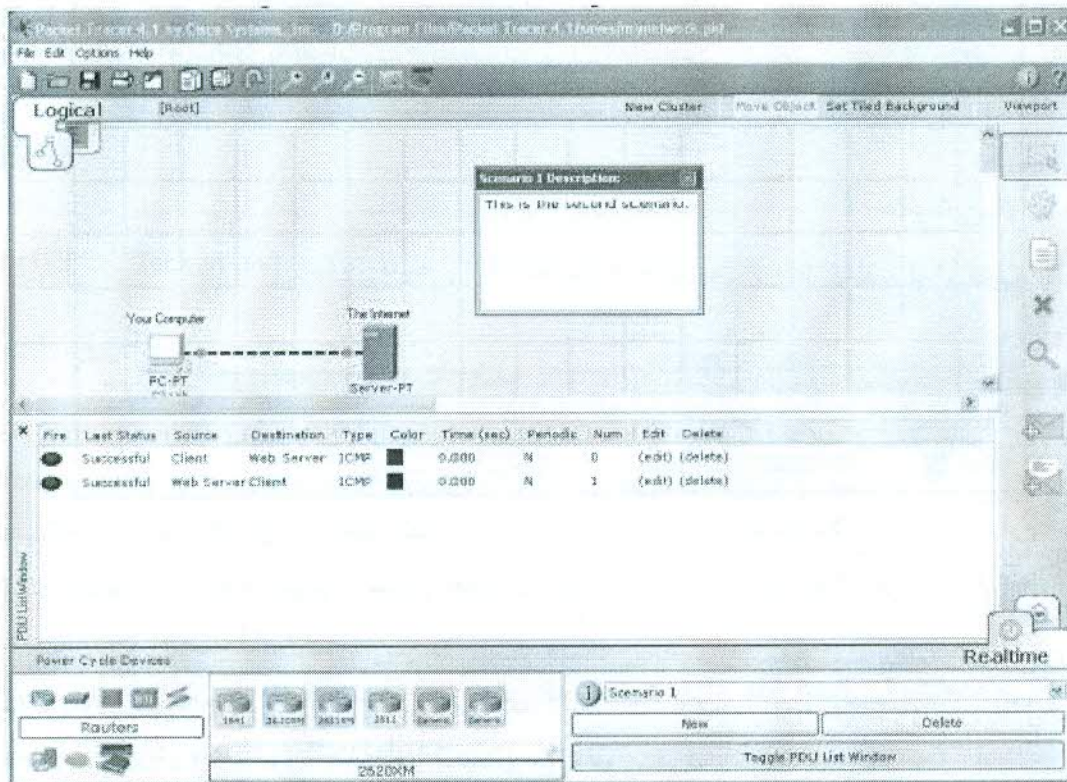


✓ فصل دوم: شبیه سازی شبکه توسط نرم افزار Packet Tracer

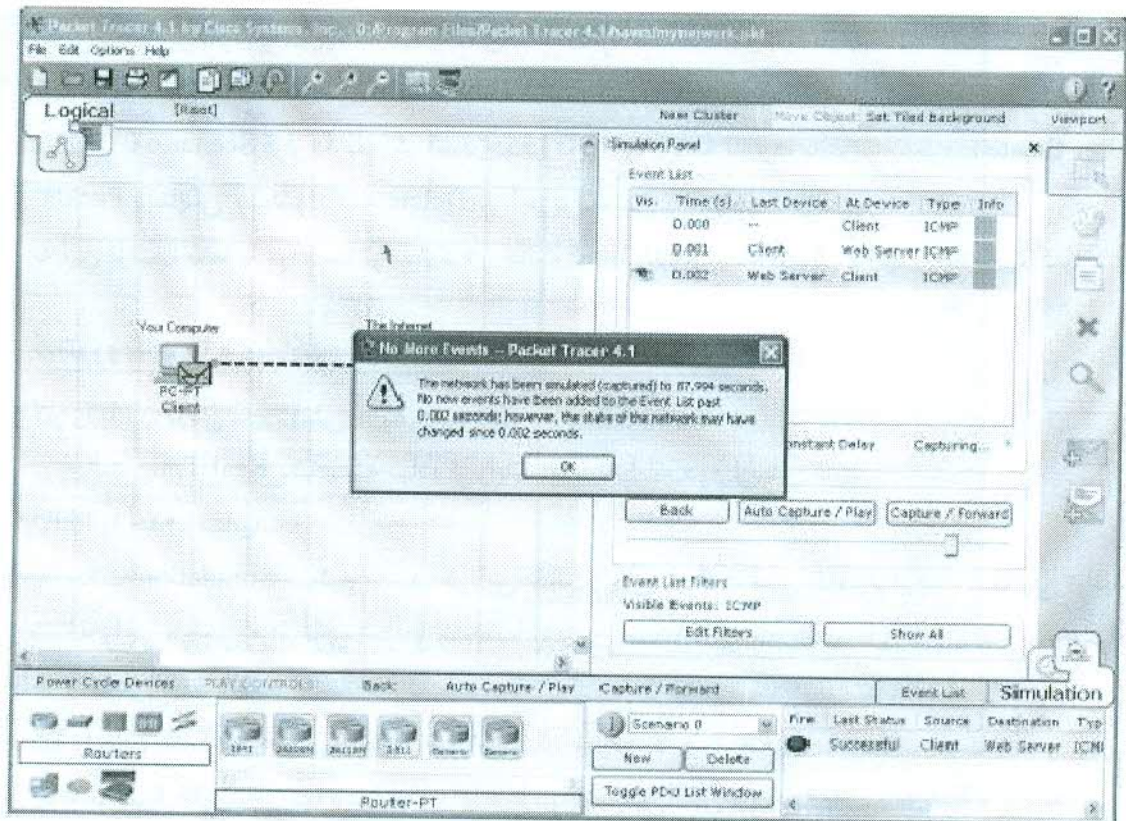
با استفاده از دستور Save as در منوی File می توان شبکه خود را ذخیره نمود.
به این ترتیب اولین شبکه با موفقیت ایجاد می گردد.

ارسال پیغام های ساده در حالت Real Time

کار خود را با باز کردن شبکه قبل ادامه دهید.
دقت کنید که در حالت Real Time قرار داشته باشید. با استفاده از ابزار Add Simple PDU بسته Ping ساده از یک رایانه به رایانه دیگر ایجاد کنید.
در پنجره User Created Packet پیمایش کنید تا حالت های مختلف این پیغام Ping را مشاهده کنید. از جمله، موردی که نشان می دهد Ping موفقیت آمیز بوده است.¹
به روش مشابه، روی دکمه toggle the PDU List Window کلیک، تا پنجره را بزرگتر مشاهده نمایید. می توان یک یا چند مورد از این پیغام ها را به عنوان یک سناریو ذخیره نمود.
روی New کلیک کرده تا سناریوی جدیدی ایجاد شود. سناریوی جدید در ابتدا خالی خواهد بود.
با استفاده از ابزار Simple PDU دو بسته جدید از هر رایانه به رایانه دیگر ایجاد کنید.



¹ - Successful



به این ترتیب با موفقیت رویدادها را ثبت کرده و انیمیشن‌ها را در حالت شبیه‌سازی مشاهده نموده‌اید.

مشاهده داخل بسته‌ها در حالت شبیه‌سازی

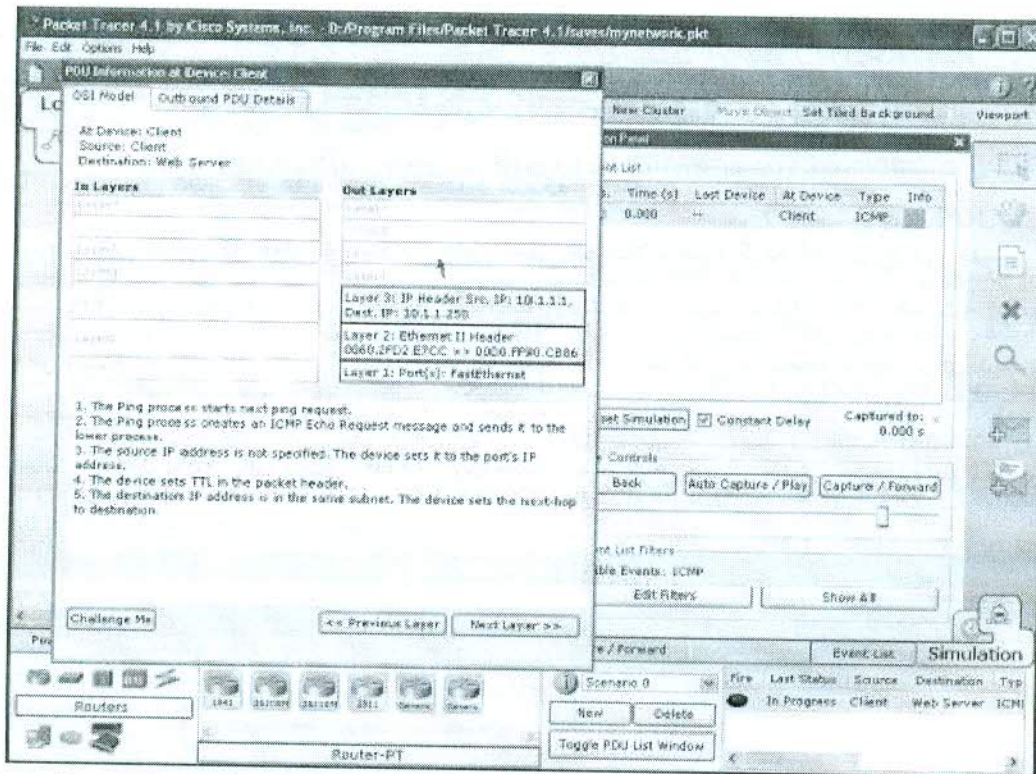
فعالیت قبلی را ادامه دهید. روی **Reset Simulation** کلیک کنید. تمام **Event List** بجز بسته اصلی پاک خواهد شد.

روی پاکت‌نامه در فضای کاری کلیک کنید تا پنجره اطلاعات PDU نمایش داده شود. این پنجره شامل برگه OSI Model است که چگونگی پردازش بسته را در هر لایه OSI در وسیله فعلی نمایش می‌دهد. این پنجره را ببندید و دقت کنید که بسته در لیست رویدادها با آیکن چشم نمایش داده شده است. روی مربع رنگی در ستون **Info** این ردیف کلیک کنید. این کار معادل کلیک کردن مستقیم بر روی پاکت‌نامه است.

بین دو سناریو سوئیچ نمایید تا حالت های مختلف را مشاهده کنید. سناریوی دوم را با استفاده از دکمه Delete حذف کنید. حالا در Scenario 0 قرار دارید. اگر قصد حذف PDU را داشته باشید، باید در پنجره User Created Packet پیمایش کنید و دکمه Delete در آخرین ستون را کلیک کنید. به این ترتیب شما با موفقیت توانستید در حالت Real Time بسته ارسال و آنها را مدیریت کنید.

ثبت رویدادها و مشاهده انیمیشن در حالت شبیه سازی

کار را با باز کردن فایل قبلی ادامه دهید. در حالت Real Time یک بسته ساده از رایانه اول به رایانه دوم ارسال کنید. PDU را حذف نمایید. به حالت Simulation سوئیچ کنید. در این حالت زمان حرکت نمی کند. بنابراین شما می توانید شبکه را در مراحل آرام تری اجرا و مشاهده نموده و مسیرهایی که بسته طی می کند را به همراه جزئیات آن ها مشاهده کنید. در Event List Filters روی All/None کلیک نموده تا همه فیلدها غیرفعال شوند. سپس روی ICMP کلیک کنید تا تنها بسته های ICMP در انیمیشن قابل مشاهده باشند. یک بسته PDU ساده از بسته اول به بسته دوم ایجاد کنید. دقت کنید که بسته جدید به لیست بسته های ایجاد شده توسط کاربر اضافه می شود. این بسته در اولین رویداد در لیست رویدادها ثبت می شود و یک آیکن پاکت نامه در فضای کاری نشان داده خواهد شد. آیکن چشم در سمت چپ Event List نشان دهنده این است که بسته در حال حاضر در حال نمایش است. روی دکمه Capture/Forward یک بار کلیک کنید. به این ترتیب رویداد دوم که در شبکه اتفاق می افتد ثبت می شود. دقت کنید که پس از کلیک بر روی این دکمه، پاکت نامه در فضای کاری از یک وسیله به دیگری حرکت می کند (این پیغام ICMP echo است). سرعت انیمیشن را با حرکت دادن لغزنده Play Speed به سمت راست افزایش دهید. برای بار دوم روی Capture/Forward کلیک کنید. رویداد بعدی شبکه ثبت خواهد شد (پاسخ echo). دوباره روی Capture/Forward کلیک کنید. در این حالت چون بسته دیگر وجود ندارد، کادر No More Events نمایش داده خواهد شد.



از دکمه های Previous Layer و Next Layer برای مشاهده جزئیات پردازش بسته در لایه های مختلف استفاده کنید. باید به این نکته توجه داشت که فقط Out Layers قابل مشاهده است. روی برگه Outbound PDU Details کلیک کنید. این برگه دقیقاً سرآمد PDU را نمایش می دهد. پنجره PDU Information را ببندید. یک بار روی دکمه Capture/Forward کلیک کنید. دوباره روی بسته در فضای کاری کلیک کنید تا پنجره باز شود. (دقت کنید که این بار اطلاعات In Layers و Out Layers با هم قابل مشاهده است) روی برگه Inbound PDU Details کلیک کنید. در این حالت جزئیات درخواست echo ورودی نمایش داده شده است. اگر روی برگه Outbound PDU Details کلیک کنید، اطلاعات مشابهی نمایش داده خواهد شد، اما این بار شامل بسته پاسخ echo است. دوباره روی دکمه Reset Simulation کلیک کنید. این بار روی دکمه Capture/Play کلیک کنید. ارسال پیغام echo و ارسال پاسخ echo به طور اتوماتیک ثبت می شود و در انتها پنجره No More Events نمایش داده می شود. روی دکمه Back دوبار کلیک کنید تا هر بار انیمیشن یک مرحله به عقب برود. حالا روی دکمه Capture/Forward دوبار کلیک کنید تا بسته دوباره به جلو حرکت داده شود. به رویدادهایی که مشخص می گردند دقت کنید.

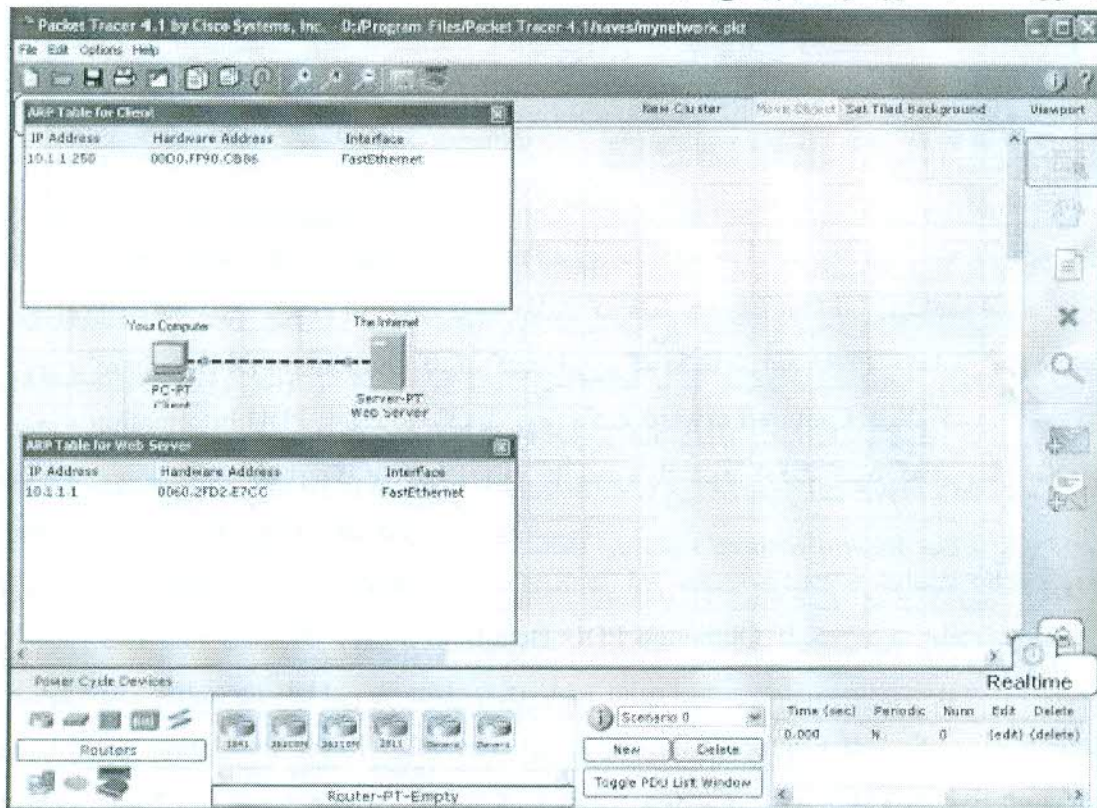


✓ فصل دوم: شبیه سازی شبکه توسط نرم افزار Packet Tracer

به این ترتیب شما با موفقیت توانستید داخل یک بسته را مشاهده کنید، منطقی را که دستگاه ها در زمان پردازش بکار میگیرند مشاهده و پخش انیمیشن را به دلخواه مدیریت نمایید.

مشاهده جدول دستگاه ها و تنظیم مجدد شبکه

کار را با بستن فضای کار فعلی و بازکردن فایل اصلی که قبلا ذخیره کرده اید شروع می کنیم. با استفاده از ابزار Inspect، جدول ARP دو رایانه را مشاهده کنید. جدول ARP همیشه در نقطه یکسانی ظاهر می شوند. یکی از آنها را جابجا کنید تا هر دو قابل مشاهده شوند. برای دید بهتر می توانید آنها را تغییر اندازه دهید. در حالت Real Time یک بسته PDU از یک رایانه به دیگری ارسال کنید. مشاهده می کنید که جدول ARP به طور خودکار پر می شوند.



PDU را حذف کنید. مشاهده می کنید که جدول ARP پاک نمی شود. به این دلیل که ورودی های ARP هم اکنون در رایانه ها ذخیره شده است و حذف PDU ها آنچه که در شبکه اتفاق افتاده است را reset نمی کند.



✓ فصل دوم: شبیه سازی شبکه توسط نرم افزار Packet Tracer

بر روی Power Cycle Devices کلیک کنید تا شبکه Reset شود. به این ترتیب که تمام دستگاه ها خاموش و سپس روشن می شوند و اطلاعات موقت آنها و جداولی که یادگرفته اند پاک می شود. به حالت Simulation بروید. در Event List Filters مطمئن شوید که ICMP و ARP فعال هستند. بسته PDU دیگری ایجاد کنید.

با توجه به این که اخیرا شبکه reset شده است، جداول ARP خالی هستند. بنابراین لازم است قبل از ارسال بسته های Ping، بسته های تقاضای ARP ارسال شوند تا رایانه ها از وجود همدیگر مطلع شوند. روی Auto Capture/Play کلیک کنید تا انیمیشن را مشاهده کنید.

روی Reset Animation کلیک کنید. مشاهده می کنید که لیست رویدادها پاک می شوند (بجز PDU های ایجاد شده توسط کاربر)، ولی جداول ARP هنوز پر هستند. روی Capture/Play کلیک کنید. در این زمان، با توجه به این که جداول ARP قبلا پر هستند، دیگر بسته ARP ارسال نمی شود.

اگر شبکه را Reset کنید، بسته های ARP جدید به طور خودکار در لیست رویدادها ظاهر خواهند شد.

به این ترتیب شما توانسته اید جداول دستگاه ها را مشاهده کنید و نیز شبیه سازی و شبکه را reset کنید.

مرور مطالب

یک بار کلیک بر روی دکمه Delete کل یک سناریو با همه PDU های آن را حذف خواهد کرد. دوبار کلیک بر روی Delete در آخرین ستون در پنجره PDU List بسته ها را حذف خواهد کرد. دکمه Reset Simulation همه محتوای Even List، بجز PDU های ایجاد شده توسط کاربران را حذف خواهد کرد و به شما امکان مشاهده مجدد انیمیشن را می دهد ولی جداول دستگاه ها را پاک نمی کند.

دکمه Reset Network همه دستگاه ها را خاموش، و دوباره روشن خواهد کرد. به این ترتیب جداول دستگاه ها و نیز تنظیماتی که ذخیره نشده است از بین خواهد رفت. با ذخیره کردن فایل در فواصل معین، می توانید از حذف شدن تنظیمات و تغییراتی که در شبکه می خواهید نگه دارید جلوگیری کنید.

حال شما آماده هستید تا شبکه های مختلفی را در نرم افزار Packet Tracer 4.1 ایجاد و تحلیل کنید. ویژگی های بسیار دیگری وجود دارد که در ادامه شرح داد خواهد شد.



فضاهای کار فیزیکی و منطقی

نرم افزار Packet Tracer 4.1 شامل دو الگوی نمایشی برای شبکه است: فضای منطقی و فضای فیزیکی. فضای منطقی به شما امکان ایجاد توپولوژی منطقی شبکه را بدون در نظر گرفتن مقیاس فیزیکی و چیدمان آن می دهد. فضای فیزیکی به شما امکان چیدن دستگاه ها به صورت فیزیکی در شهرها، ساختمان ها و فضاهای سیم بندی را می دهد. مسافت ها و دیگر اندازه های فیزیکی در عملکرد شبکه و دیگر مشخصه های آن تاثیر خواهد گذاشت. در این نرم افزار شما باید ابتدا شبکه منطقی را ایجاد کنید و سپس آن را در فضای فیزیکی مرتب نمایید.

فضای کار منطقی

فضای کار منطقی جایی است که شما بیشتر زمان خود را برای ایجاد و پیکربندی شبکه در آن سپری می کنید. در ترکیب با حالت Realtime می توانید از این فضا برای تکمیل بسیاری از آزمایش های دوره CCNA استفاده کنید.

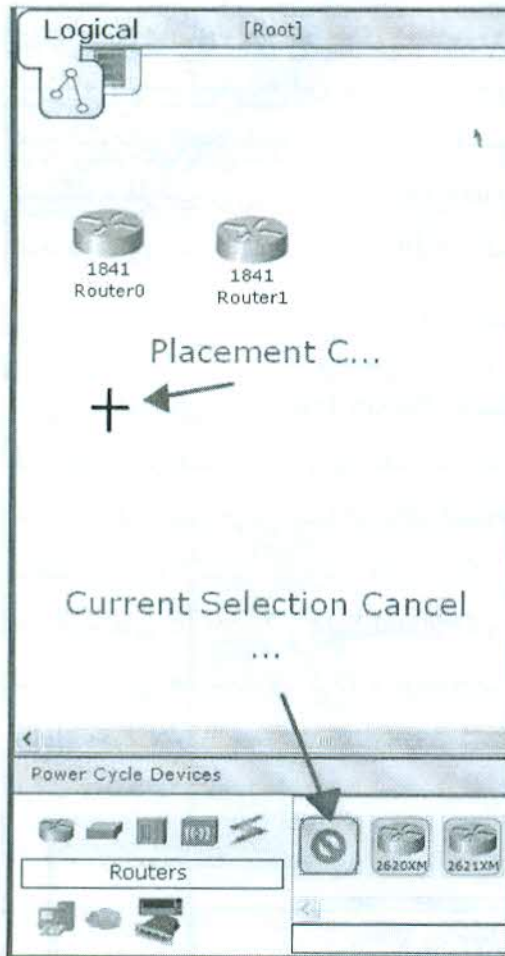
ابتدا شما باید دستگاه ها را ایجاد کنید. این کار با انتخاب دستگاه از کادر Network Component انجام می شود. سپس می توانید هر یک از موارد زیر را انجام دهید:

- افزودن ماژول جدید به دستگاه ها برای دستیابی به واسط های بیشتر (دقت کنید که قبل از افزودن ماژول باید دستگاه را با کلیک بر روی دکمه Power خاموش کنید)
- اتصال دستگاه ها به همدیگر با انتخاب کابل مناسب.
- پیکربندی های پارامترهای دستگاه ها (نظیر نام و آدرس IP) در کادرهای گرافیکی یا با استفاده از دستورات IOS سیسکو (در مورد مسیریاب ها و سوئیچ ها)
- ایجاد تنظیمات پیشرفته و مشاهده اطلاعات شبکه از واسط CLI مسیریاب یا سوئیچ

ایجاد دستگاه ها

برای قرار دادن یک دستگاه در فضای کار، ابتدا نوع دستگاه را از کادر Device-Type Selection انتخاب و سپس روی مدل مورد نظر از قسمت Device-Specific Selection کلیک کنید. در نهایت روی مکانی از فضای کار که می خواهید دستگاه را قرار دهید کلیک کنید. برای انصراف از انتخاب، روی آیکن Cancel همان دستگاه کلیک کنید. به روش دیگر شما می توانید ایجاد وسیله را با

کشیدن و انداختن آن به داخل فضای کار انجام دهید. همچنین اگر دستگاه ها را از کادر DeviceType Selection درآگ نمایید، مدل پیشفرض انتخاب خواهد شد.



برای ایجاد تعداد زیادی از یک وسیله یکسان، دکمه Ctrl را نگه داشته و روی دستگاه مورد نظر کلیک کنید و سپس دکمه Ctrl را رها کنید. به این ترتیب وسیله مورد نظر قفل خواهد شد و شما می توانید چندین بار در فضای کار کلیک نمایید تا کپی های زیادی از آن ایجاد شود. برای انصراف از عملیات روی آیکن Cancel کلیک کنید. برای تکثیر یک دستگاه می توانید دکمه Ctrl را نگه داشته و دستگاه مورد نظر را فضای کاری درآگ کنید یا این که از Copy و Paste استفاده کنید.

ایجاد دستگاه های سفارشی

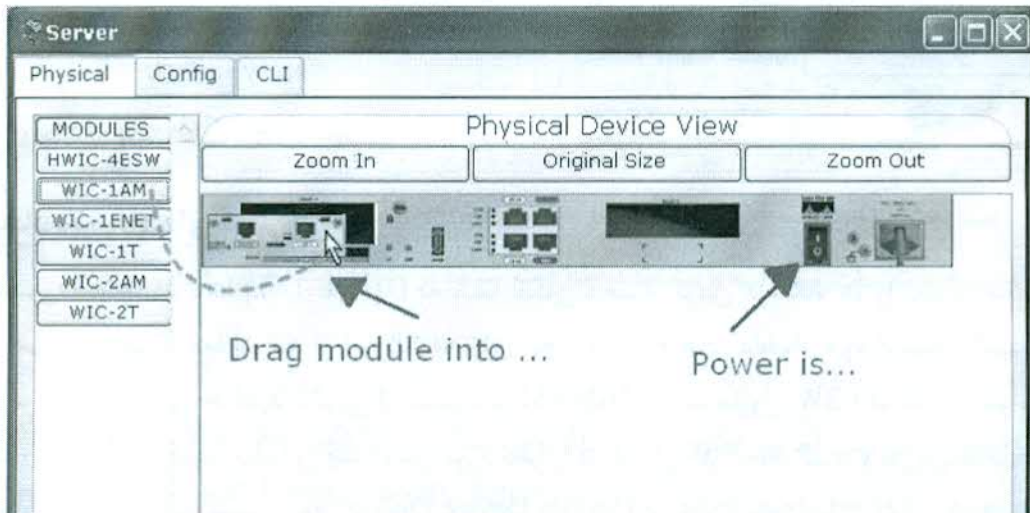
دستور Device Template Manager به شما امکان ذخیره کردن دستگاه ها را بعنوان الگوهایی فراهم می کند تا بعدا بتوانید از این الگوها برای ایجاد دستگاه های دلخواه خود استفاده کنید. مثلا فرض کنید که می خواهید الگویی از مسیریاب 2621XM با یک ماژول NM-2FE2W و دو ماژول WIC-2T ایجاد کنید. بنابراین ابتدا مدل مورد نظر را در فضای کار ایجاد کنید و ماژول ها دلخواه را به آن اضافه نمایید. سپس روی Custom Device Dialog در نوار منوی اصلی کلیک کنید. پس از انتخاب دکمه Select در کادر باز شده، روی وسیله مورد نظر کلیک کرده و سپس توضیحی را برای

آن اضافه کنید. در نهایت روی دکمه Add کلیک کنید و در کادری که باز می شود الگوی خود را در پوشه template در مسیر نصب برنامه ذخیره نمایید.

برای استفاده از این الگو در نمای منطقی روی آیکن Custom Made Device در کادر انتخاب نوع دستگاه کلیک کنید. به این ترتیب دستگاه های سفارشی شما ظاهر خواهد شد. حال می توانید همه الگوهای ایجاد شده را پیدا کنید و سپس آنها را به فضای کار اضافه کنید. برای حذف یک دستگاه سفارشی روی دکمه Custom Devices Dialog در نوار ابزار اصلی کلیک کرده و پس از انتخاب الگوی مورد نظر از قسمت Edit، دکمه Remove را کلیک کنید.

افزودن ماژول ها

اکثر دستگاه های Packet Tracer 4.1 محفظه های ماژولار دارند که شما می توانید ماژولها را در آنها قرار دهید. در فضای کار، روی یک دستگاه کلیک کنید تا پنجره پیکربندی های آن نمایش داده شود. به طور پیش فرض شما در برگه Physical خواهید بود. یک تصویر محاوره ای از وسیله نیز در سمت راست و لیستی از ماژول های سازگار با آن در سمت چپ قرار دارد. شما می توانید تصویر را با دکمه های Zoom in ، Original Size ، و Zoom out تغییر اندازه دهید. همچنین می توانید لیست ماژول ها پیمایش کرده و توضیحات و اطلاعات آنها را در کادر پایین مطالعه کنید. وقتی ماژول مورد نظر را پیدا کردید آن را از لیست روی محفظه سازگار با آن در تصویر درآگ کنید. با درآگ مجدد یک ماژول به این لیست، امکان حذف آن نیز وجود دارد.

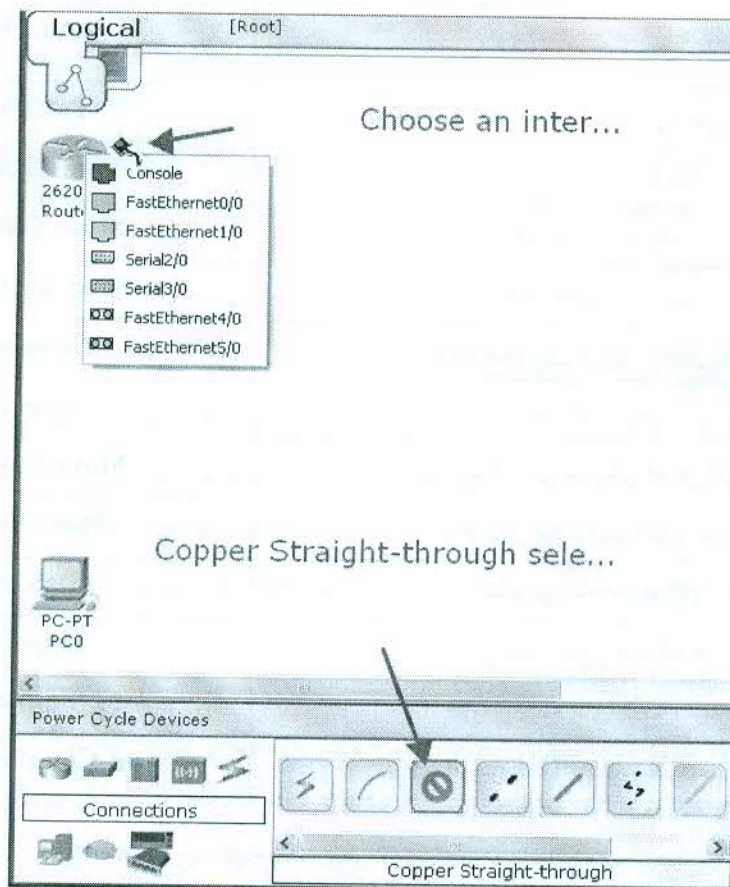


دقت کنید که قبل از افزودن یا حذف ماژول، باید دستگاه را خاموش کنید و پس از انجام کار مجدداً آنرا روشن نمایید.

ایجاد اتصالات

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

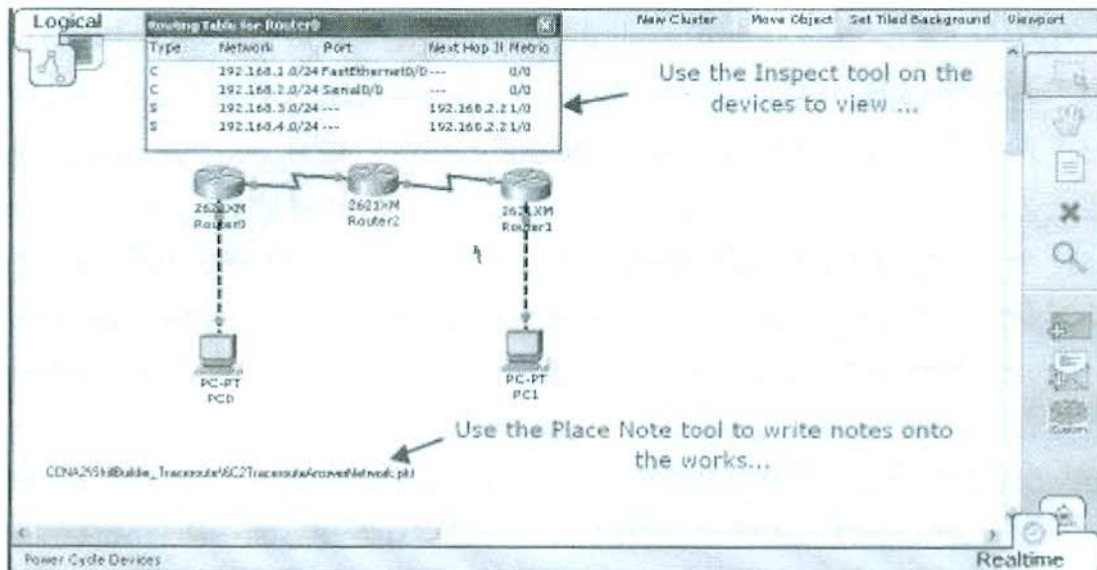
برای ایجاد سریع اتصالات مختلف از نوع یکسان، دکمه Ctrl را نگه دارید و روی اتصال مورد نظر کلیک کنید. سپس دکمه Ctrl را رها کنید تا بتوانید مکرراً از اتصال یکسان بین دستگاه ها استفاده نمایید. برای اتمام عملیات روی آیکن Cancel کلیک کنید.



ابزارهای ویرایش توپولوژی منطقی

شما می توانید از نوار ابزار اصلی ، نوار فضای کار Logical/Physical و نوار ابزار رایج برای ویرایش و نیز افزودن توضیحات به توپولوژی استفاده کنید.

ابزار	کاربرد
Copy	کپی آیتم های انتخاب شده
Paste	الصاق آیتم های کپی شده
Undo	برگرداندن عمل قبلی
Zoom In	بزرگ کردن تصویر
Zoom Reset	تنظیم بزرگ نمایی به حالت پیش فرض
Zoom Out	کوچک کردن فضای کار
Palette	ایجاد خط، مستطیل و بیضی
New Cluster	ایجاد گروه های جدید
Move Object	جابجا کردن اشیاء
Set Tiled Background	تنظیم تصویر پس زمینه
Viewport	مشاهده فضای کار در یک مقیاس کوچک
Select	انتخاب اشیاء
Move Layout	جابجا کردن محتوای فضای کار
Place Note	افزودن توضیح به فضای کار
Delete	حذف اشیاء از فضای کار
Inspect	مشاهده جداول دستگاه ها
Add Simple PDU	افزودن بسته های PDU ساده
Add Complex PDU	افزودن PDU های پیشرفته تر



پیکربندی دستگاه ها

برای استفاده از دستگاه ها، باید برخی تنظیمات پایه نظیر آدرس IP و ماسک شبکه را تنظیم کنید. پارامترهای پایه را می توانید از طریق واسط گرافیکی پیکربندی دستگاه انجام دهید. (روی برگه Config در پنجره پیکربندی دستگاه کلیک کنید). دستگاه های مختلف تنظیمات مختلفی دارند که بعدا شرح داده خواهد شد.

Cisco IOS مسیریاب ها و سوئیچ ها

برای مسیریاب ها و سوئیچ ها شما دسترسی محدودی به IOS های سیسکو دارید. در حالت Realtime می توانید از این نرم افزار برای ایجاد تنظیمات پیشرفته و نیز مشاهده اطلاعات مختلف شبکه استفاده کنید. مثلا دستوراتی نظیر Ping ، traceroute ، show interfaces ، ip access-list و switchport access vlan که شرح بیشتری از دستورات بعدا ارائه خواهد شد.

گروه بندی دستگاه ها (Clustering)

گروه بندی دستگاه ها به شما امکان ایجاد ظاهری بهتر از فضای کار با کاهش گروهی از دستگاه ها به یک تصویر را فراهم می کند. به طور پیش فرض همه دستگاه ها در نمای منطقی در سطح ریشه (Root) قرار می گیرند. شما می توانید تعدادی از موارد موجود در صفحه را که سبب آشفتگی فضا می شوند با ایجاد یک گروه جدید در سطح بعدی کاهش دهید. برای این کار دستگاه های مورد نظر را انتخاب کنید و روی New Cluster کلیک کنید. حال می توانید با کلیک بر روی گروه ایجاد

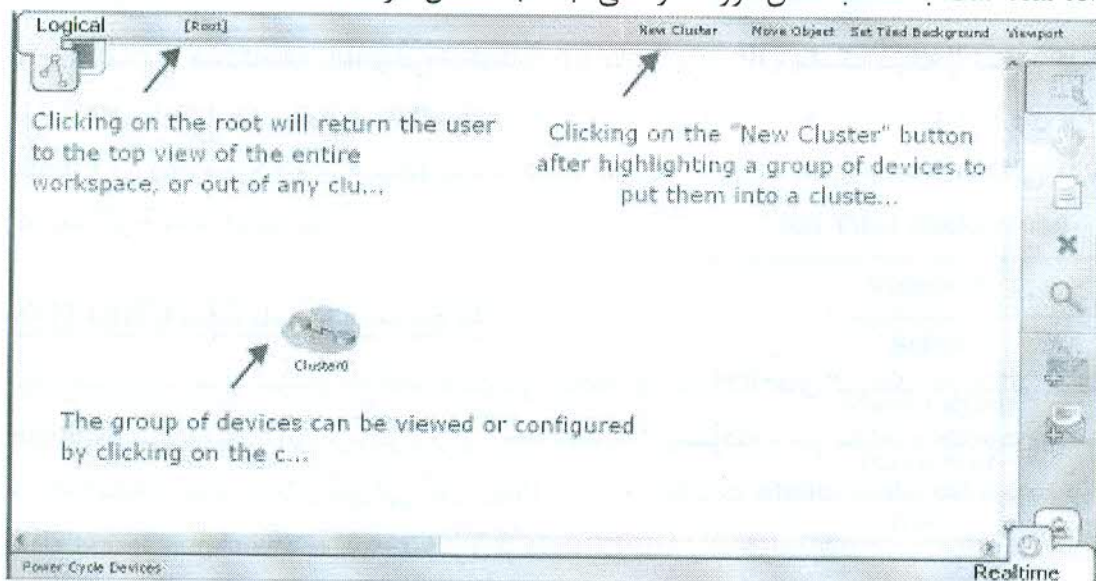


✓ فصل دوم: شبیه سازی شبکه توسط نرم افزار Packet Tracer

شده وارد آن شوید و نیز گروه های جدیدی داخل آن ایجاد کنید. همچنین می توان یک گروه را تغییر نام داد یا با کلیک بر روی سطح مورد نظر در نوار پیمایش، بین آنها سوئیچ کرد. دقت کنید که در فضای منطقی می توانید تا ۴ سطح گروه ایجاد کنید. برای خارج کردن دستگاه ها از گروه می توانید از ابزار Delete استفاده کنید.

وقتی یک گروه ایجاد شد، می توانید اتصالاتی را به دستگاه های داخل گروه ایجاد کنید. برای اینکار پس از انتخاب اتصال مورد نظر روی گروه کلیک کنید تا لیستی از دستگاه های داخل آن را مشاهده کنید که به شما امکان انتخاب دستگاه را می دهد. پس از انتخاب دستگاه مورد نظر می توانید واسط مورد نظر را نیز انتخاب کنید.

همچنین علاوه بر ایجاد گروه، شما می توانید توسط دکمه Move Object، دستگاه ها و اشیاء را در بین آنها جابجا کنید. برای اینکار روی دکمه Move Object کلیک کنید و سپس شیء یا دستگاه مورد نظر را انتخاب کنید. منویی ظاهر خواهد که سلسله مراتب سطوح و گروه ها در آن نمایش داده شده است. با انتخاب مکان مورد نظر، شیء به آنجا منتقل خواهد شد.

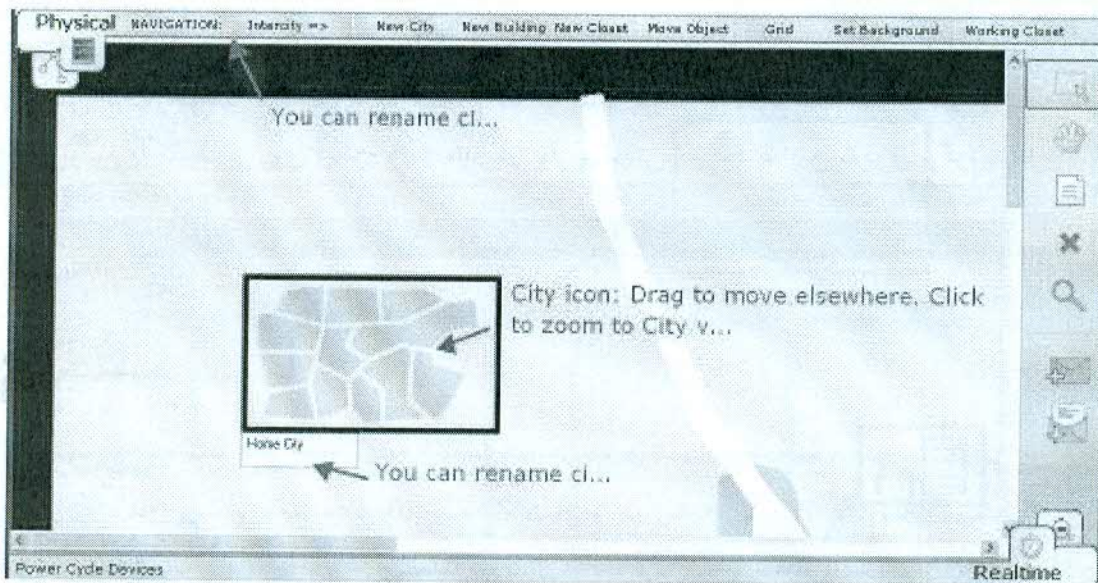




فضای کار فیزیکی

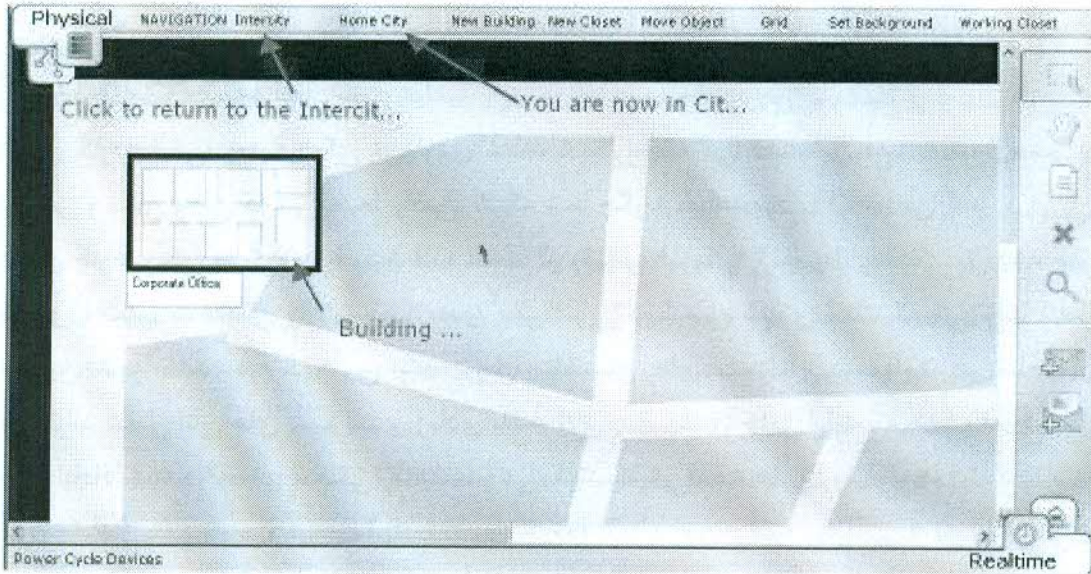
فضای کار فیزیکی، بعد فیزیکی توپولوژی شبکه شما را ارائه می دهد. این فضا به شما حسی از مقیاس و مکان و این که در محیط واقعی، شبکه شما چگونه خواهد بود را فراهم می کند. فضای کار فیزیکی به ۴ لایه تقسیم شده است که مقیاس^۱ فیزیکی ۴ محیط را نشان می دهد: بین شهری^۱، شهر، ساختمان و اتاق سیم بندی^۲. بزرگترین فضا، بین شهری است که می تواند شامل چندین شهر باشد. هر شهر می تواند شامل ساختمان های متعدد و در نهایت هر ساختمان می تواند شامل اتاق های سیم بندی زیادی باشد. اتاق سیم بندی جایی است که شما واقعا دستگاه های ایجاد شده در فضای منطقی را مشاهده می کنید که در قفسه ها^۳ و روی میزها قرار داده شده اند.

وقتی که اولین بار وارد فضای کار فیزیکی می شود، در نمای Intercity قرار دارید.

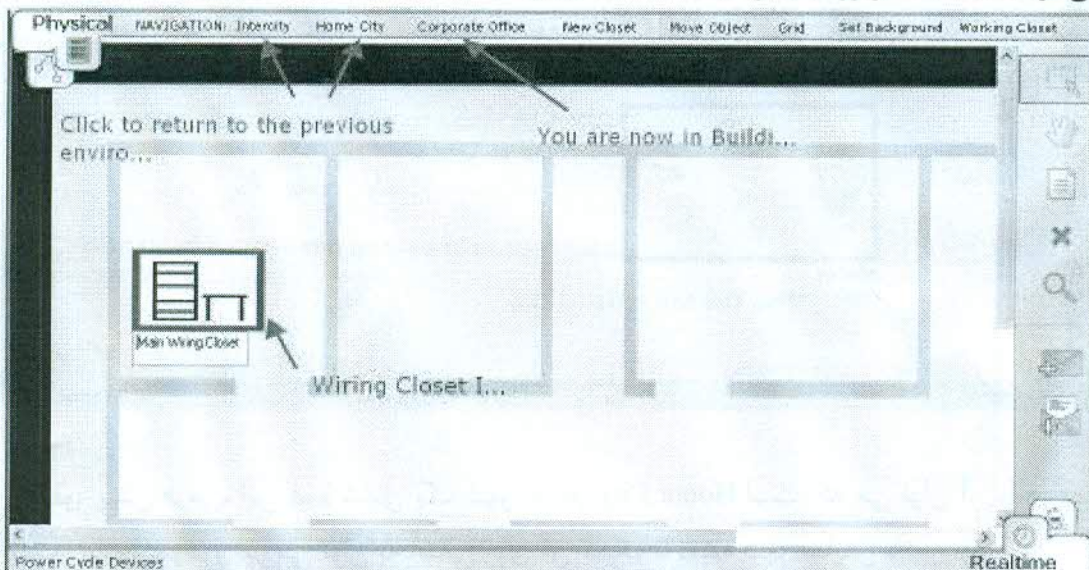


به طور پیش فرض، این فضا شامل یک شهر به نام Home City است. که می توان آن را در روی نقشه جابجا نمود. و نیز می توان به آسانی روی آن کلیک تا نقشه شهر نمایش داده شود.

- 1- Intercity
- 2- wiring closet
- 3- Racks



شهر Home City شامل یک ساختمان پیش فرض به نام Corporate Office است. این ساختمان نیز می تواند در شهر جابجا شود. با کلیک بر روی آیکن ساختمان، نمای داخلی ساختمان بزرگتر نمایش داده خواهد شد. همه ساختمان ها به یک طبقه محدود هستند. از نمای شهر شما می توانید با کلیک بر روی آیکن Intercity در نوار پیمایش، به محیط بین شهری برگردید.



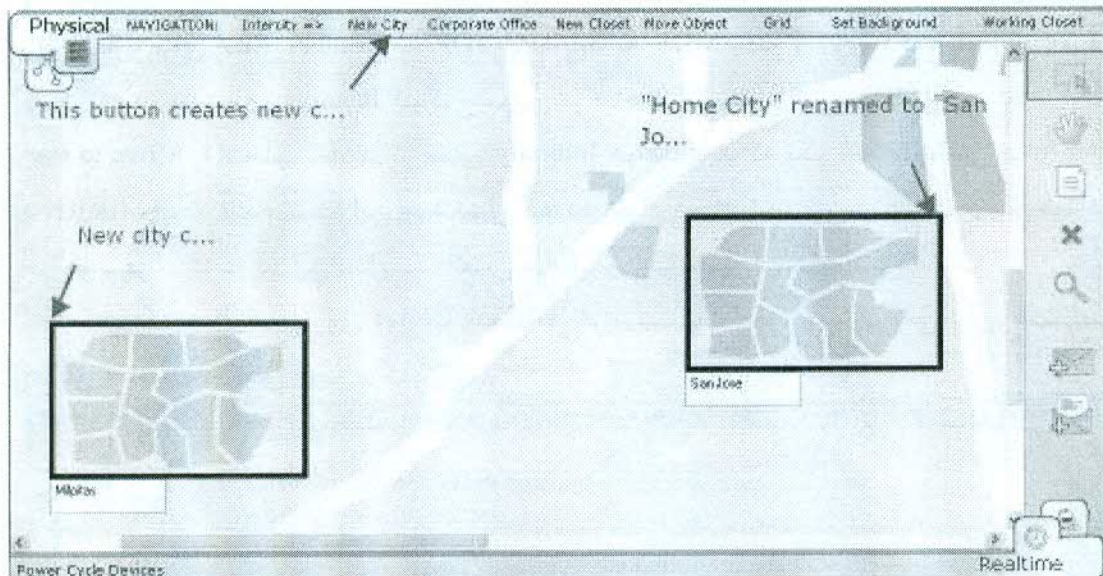
ساختمان Corporate Office شامل یک اتاق پیش فرض به نام Main wiring closet است. با کلیک بر روی آن می توانید محتوای اتاق را مشاهده نموده و سپس توسط نوار پیمایش به هر یک از محیط های قبلی برگردید.



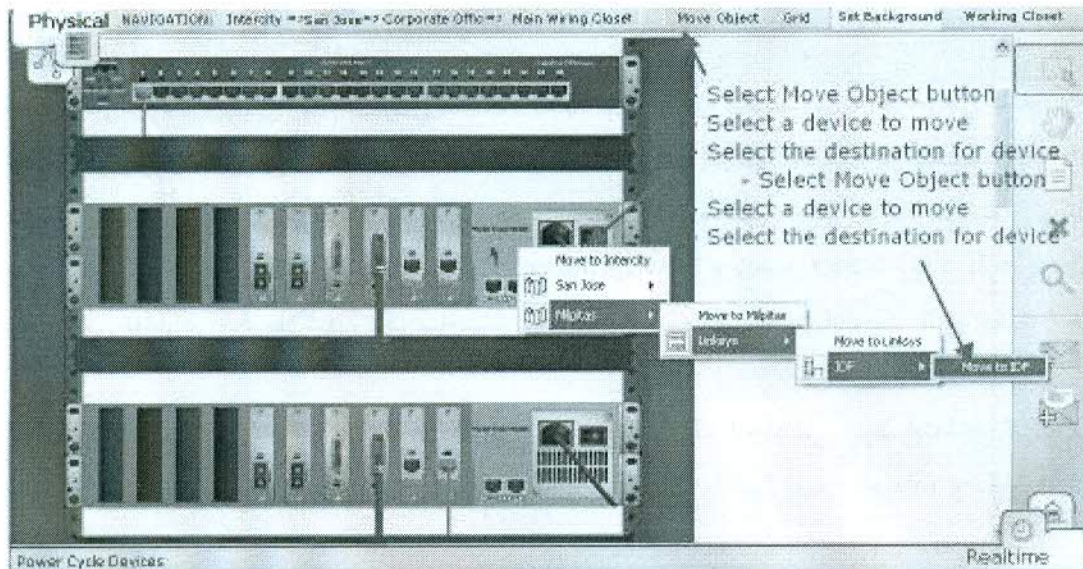
جابجا کردن اشیاء در فضای کار فیزیکی

فضای کار فیزیکی امکان جابجا کردن دستگاه ها به مکان های مختلف را به طراح می دهد. برای توسعه توپولوژی فیزیکی، ابتدا نیازمند ایجاد یک مکان جدید می باشیم. در محیط Intercity می توان توسط دکمه New City یک شهر جدید ایجاد کرد. همچنین امکان ایجاد ساختمان و اتاق سیم بندی نیز در این فضا توسط دکمه های New Building و New Closet وجود دارد. به طور مشابه می توان در محیط شهر، یک ساختمان جدید و در محیط ساختمان، یک اتاق جدید ایجاد کنید.

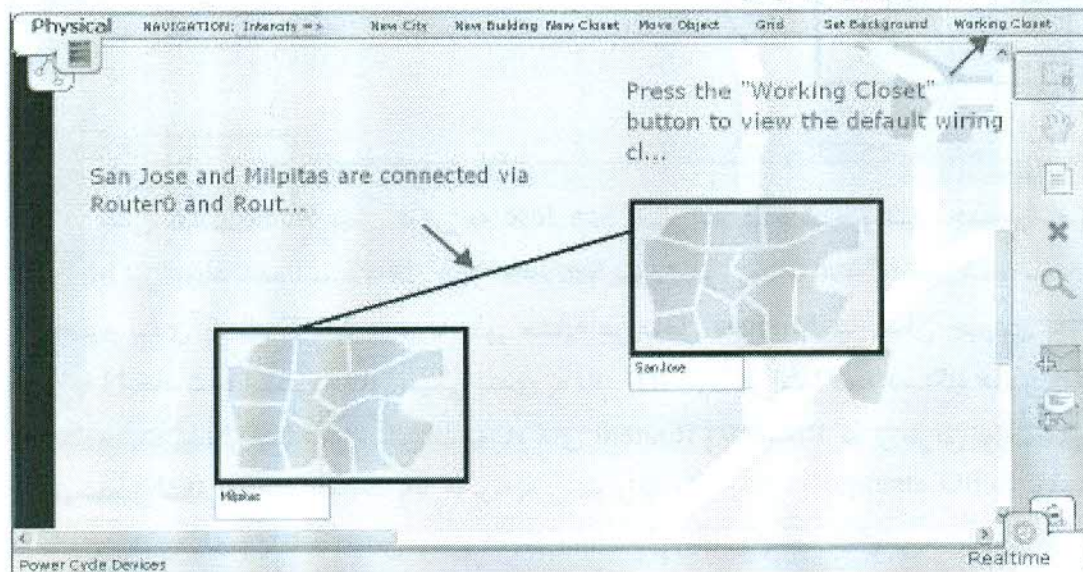
البته باید دقت کرد که هر شهر، ساختمان و یا اتاق جدیدی که ایجاد می شود، ابتدا در گوشه بالا سمت چپ ظاهر شود. برای جلوگیری از سردرگمی، باید آنها را فوراً تغییر نام داده و مکان آنها را تعیین کنید.



در این مثال، Home City پیش فرض به San Jose تغییر نام داده شده و شهر جدیدی به نام Milpitas نیز ایجاد شده است. داخل شهر San Jose ساختمانی به نام Cisco ایجاد شده است که اتاق سیم بندی به نام MDF دارد. به طور مشابه در داخل Milpitas ساختمان جدیدی به نام Linksys ایجاد شده است که اتاق سیمی بندی به نام IDF دارد. در ابتدا همه دستگاه ها در MDF قرار داده شده اند، از جمله دو مسیریاب به نام های Router0 و Router1 که از طریق پورت سریال به هم متصل شده اند.



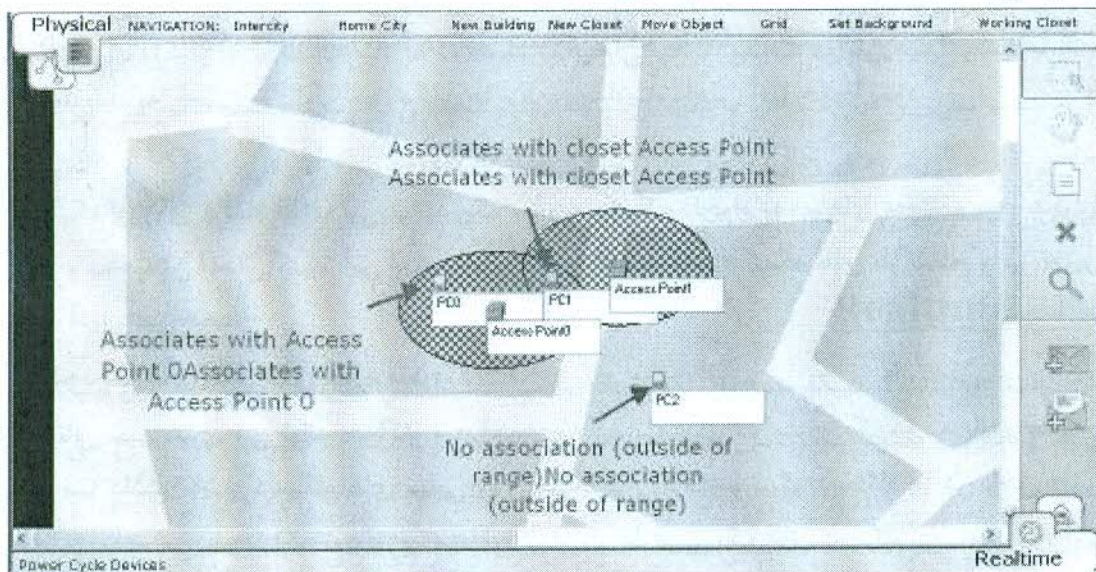
برای مثال، برای انتقال Router1 به IDF، ابتدا باید به MDF رفته و روی دکمه Move object کلیک کنید. حال روی Router1 کلیک و سپس در ساختار سلسله مراتبی، IDF را پیدا کنید، آنگاه Move to IDF را انتخاب نمایید. در نمای Intercity خواهید دید که یک خط سیاه بین San Jose و Milpitas ایجاد شده است. این خط نشان دهنده اتصال ایجاد شده بین دستگاه های موجود در این دو شهر است که در این مثال یک اتصال سریال بین دو مسیریاب می باشد. دقت کنید که با کلیک بر روی Working Closet در سمت راست نوار پیمایش می توان، به سرعت به اتاق سیم بندی پیش فرض برگشت.



علاوه بر جابجا کردن دستگاه ها توسط دکمه Move Object، می توان ساختمان ها و اتاق ها را نیز به همین روش جابجا نمود. به روشی دیگر، از دکمه Navigation نیز می توان برای جابجا کردن اشیاء استفاده کرد.

دستگاه های بی سیم در فضای کار فیزیکی

فضای کار فیزیکی برای دستگاه های بی سیم مشخصه بعد مسافت را نیز فراهم کرده است. نقاط دسترسی می توانند بین دستگاه های بیسیم که در محدوده معینی هستند اتصال برقرار کنند. این محدوده با شبکه خاکستری رنگ پیرامون نقطه دسترسی مشخص می شود. بر اساس ابعاد تصویر زمینه، این محدوده می تواند دایره یا بیضی باشد. اگر تصویر زمینه مربع باشد، شبکه دایره ای خواهد بود. اگر تصویر زمینه مستطیل باشد، شبکه با توجه به نسبت طول و عرض تصویر بیضی شکل خواهد شد.



- در این مثال، سه رایانه با قابلیت بی سیم و دو نقطه دسترسی ایجاد شده اند که به منظور نمایش تاثیر مسافت، همه آنها از اتاق سیم بندی پیشفرض مستقیماً در خیابانهای شهر قرار داده شده اند.
- PC0 در محدوده Access Point 0 قرار دارد بنابراین به آن مرتبط است.
 - PC1 در محدوده هر دو نقطه دسترسی قرار دارد. به هر حال چون به Access Point1 نزدیکتر است، در ارتباط با آن است.
 - PC2 در محدوده هیچ کدام نیست، بنابراین اتصالی برای آن وجود ندارد.



نکات مهم در فضای کار فیزیکی

استفاده از تصاویر زمینه دلخواه :

در فضای فیزیکی تعدادی تصویر زمینه برای نماهای مختلف قرار دارد که می توان زمینه هر یک از محیط ها را همانند فضای منطقی با تصاویر زمینه دلخواه خود جایگزین نمود. مثلا برای تغییر تصویر زمینه شهر مانند زیر عمل کنید:

- تصویر را در پوشه background/city قرار دهید

- تصویر را به قسمت Administrative اضافه کنید.

- در نمایش هر، دکمه background را کلیک کنید و تصویر را اعمال کنید.

توجه داشته باشید که ابعاد تصویر زمینه، در مقیاس نمایشی برخی اشیاء تاثیر می گذارد.

استفاده از Navigation :

با کلیک بر روی دکمه Navigation در نوار پیمایش، یک ساختار درختی از مکان ها نمایش داده خواهد شد. به راحتی می توان بین مکان ها پرش و یا اشیاء را بین آنها جابجا نمود.

استفاده از Grid :

با کلیک بر روی دکمه Grid می توانید یک صفحه مشبک دلخواه به نماهای مختلف بین شهری، شهر و ساختمان اعمال کنید. این ابزار به شما امکان تنظیم فاصله شبکه های هر سطح و نیز تعیین رنگ آنها را می دهد.

محدودیت های اتاق های سیم بندی :

هر اتاق سیم بندی می تواند حداکثر سه قفسه یا رک، سه میز، دو میز و یک قفسه یا دو قفسه و یک میز داشته باشد. دستگاه های نهایی روی میزها قرار گرفته و دیگر دستگاه ها در داخل قفسه ها قرار داده می شود. اگر توپولوژی منطقی بیش از ظرفیت یک اتاق دستگاه داشته باشد، اتاق دیگر به طور خودکار در همان ساختمان پیش فرض ایجاد خواهد شد و اتاق سیم بندی جدید به طور پیش فرض تنظیم خواهد شد.

حذف اشیاء :

توسط ابزار Delete می توان هر شهر، ساختمان و اتاق سیم بندی را حذف کرد. اما امکان حذف دستگاه ها در این فضا وجود ندارد. اگر یک اتاق سیم بندی را حذف گردد، دستگاه های موجود در آن به طور خودکار مستقیما در کف ساختمان قرار گرفته و اگر یک ساختمان حذف شود، دستگاه ها در خیابان های شهر قرار می گیرد.



حالت های عملکرد

حالت های عملکرد نرم افزار Packet Tracer 4.1 الگوی زمانی شبکه را نشان می دهد. در حالت Realtime شبکه به صورت زنده کار می کند. شبکه به فعالیت های خود همچون یک شبکه واقعی فوراً پاسخ می دهد. برای مثال، به محض ایجاد یک اتصال اترنت، چراغ های لینک برای اتصال ظاهر و وضعیت اتصال را نمایش می دهند. وقتی که یک دستور نظیر ping یا show در CLI تایپ می کنید، نتیجه یا پاسخ به صورت زنده تولید شده و می توان آن را مشاهده کرد. همه فعالیت های شبکه، مخصوصاً جریان PDU ها در شبکه به صورت زنده اتفاق می افتد. در حالت شبیه سازی (Simulation) کنترل مستقیم بر روی زمان داشته و می توان اجرای شبکه را قدم به قدم یا رویداد به رویداد با سرعتی دلخواه مشاهده نمود. می توانید سناریوهای مختلفی ایجاد کنید. ضمن این که هر کاری که انجام دهید تا زمانی که آن را play ننمائید اجرا نخواهد شد. پس از play شبیه سازی، نمایش گرافیکی حرکت بسته ها در بین دستگاه ها را می توان مشاهده کرد. شبیه سازی را متوقف، جلو و عقب برد تا اطلاعات مختلفی را از موضوعات خاص در زمان های خاص بدست آورد. به هر حال، دیگر موارد شبکه هنوز به صورت زنده کار می کنند. مثلاً اگر پورتهی خاموش گردد، چراغ آن فوراً قرمز می شود.

حالت Realtime

در حالت Realtime، شبکه همچون یک شبکه واقعی همیشه در حال اجراست چه روی شبکه کار کنید و چه کار نکنید. پیکربندی ها به صورت زنده اعمال و شبکه به صورت زنده پاسخ می دهد. آمار شبکه نیز به صورت زنده نشان داده می شوند. علاوه بر این که می توان از دستورات IOS سیسکو برای پیکربندی و خطایابی شبکه استفاده نمود، و نیز می توان از دکمه های Add Simple PDU و User Created PDU List برای ارسال ping به صورت گرافیکی استفاده کرد.

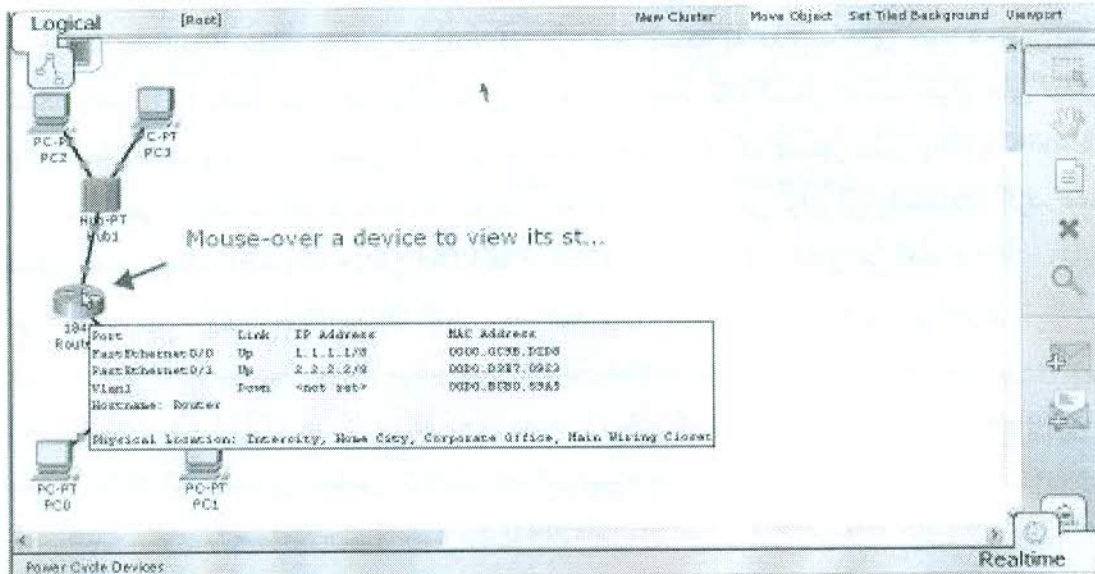
کسب اطلاعات از دستگاه ها

در هنگامی که شبکه کار می کند، از ابزار Inspect می توان برای مشاهده جداول دستگاه ها در حال پر شدن و به روز رسانی استفاده نمود. مثلاً برای مشاهده اطلاعات جدول ARP مسیریاب، روی ابزار Inspect کلیک، سپس روی مسیریاب کلیک تا لیست جداول موجود آن نمایش داده شود و سپس شما ARP Table را انتخاب کنید.



✓ فصل دوم: شبیه سازی شبکه توسط نرم افزار Packet Tracer

علاوه بر ابزار Inspect، برای مشاهده جزئیات یک دستگاه نظیر آدرس IP و آدرس فیزیکی همه پورت های آن، می توان ماوس را روی دستگاه قرار داد.



ارسال گرافیکی PDU ها

اگرچه حالت Simulation برای ارسال بسته ها ترجیح داده می شود، اما از دستورات PDU Simple Add و نیز User Created PDU List برای ping کردن یا ارسال دیگر بسته ها در این حالت می توان استفاده کرد. لذا شما می توانید PDU را که در شبکه حرکت کند مشاهده نخواهید کرد. کل مراحل به صورت زنده اتفاق افتاده و نتیجه را می توان در پنجره User Created Packet مشاهده نمود.

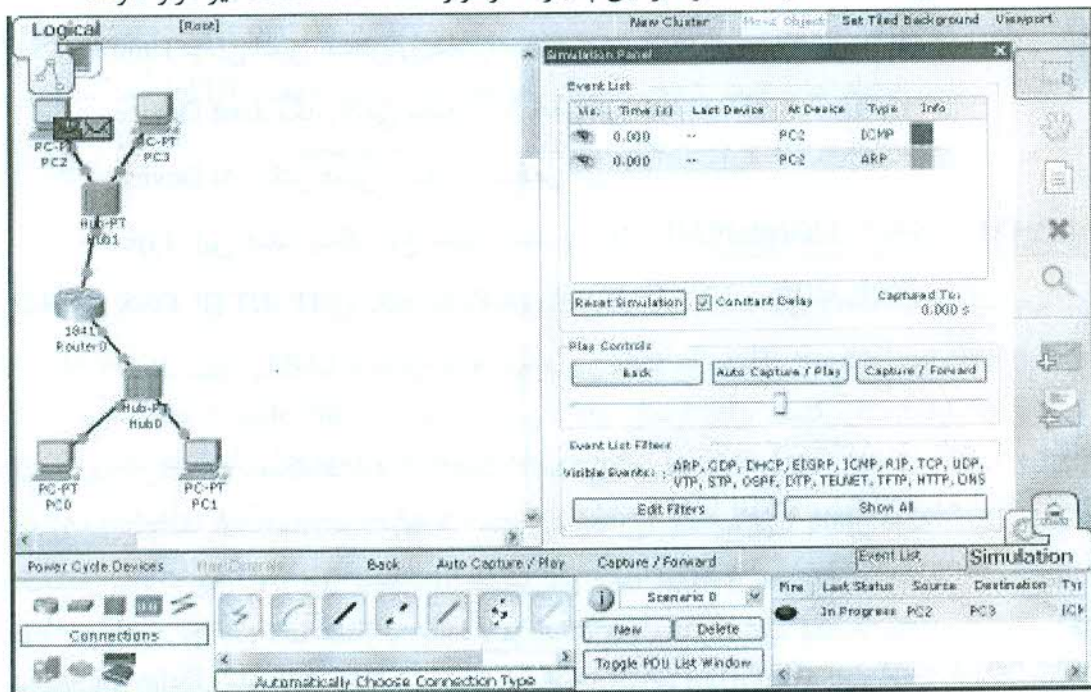
خاموش و روشن کردن دستگاه ها (Power Cycle Devices)

دکمه Power Cycle Devices در نوار ابزار Realtime امکان خاموش و روشن کردن همه دستگاه های شبکه را می دهد. در نتیجه فشار این دکمه سبب پاک شدن همه رویدادها در حال شبیه سازی نیز خواهد شد.

چنانچه توسط این دکمه شبکه را Reset کنید، همه پیکربندی های در حال اجرا در مسیریاب ها و سوئیچ ها را از دست خواهید داد. بنابراین قبل از فشار این دکمه، مطمئن شوید که دستور run start copy را در همه مسیریاب ها و سوئیچ ها اجرا کرده اید.

حالت شبیه سازی (Simulation)

در حالت شبیه سازی شما می توانید شبکه خود را با اجرای آهسته تر مشاهده کنید، مسیری را که بسته طی می کند را دیده و اطلاعات مورد نیاز را با جزئیات دریافت کنید. وقتی به این حالت سوئیچ می کنید، کادر شبیه سازی^۱ ظاهر خواهد شد که می توانید به صورت گرافیکی PDU ها را با استفاده از دکمه Add Simple Button برای ارسال بین دستگاه ها ایجاد کنید و سپس با کلیک بر روی دکمه Auto Capture/Play سناریوی شبیه سازی را اجرا کنید. پنجره Even List هر آنچه که در طی انتشار PDU در شبکه رخ می دهد را ثبت می کند. شما می توانید سرعت شبیه سازی را با لغزنده Play Speed کنترل و اگر نیاز به کنترل بیشتر شبیه سازی دارید می توانید از دکمه Capture/Forward برای شبیه سازی دستی استفاده کنید. دکمه Back نیز می توانید به زمان های قبلی برگشته و رویدادهای قبل را مجددا مشاهده نمایید. ضمناً دکمه های Play Control علاوه بر این پنجره، در نوار Simulation bar نیز قرار دارند.



شما می توانید سناریو را توسط دکمه Reset Simulation پاک کنید و از اول اجرا کنید که با این کار هر آنچه در Event List ثبت شده است پاک خواهد شد. دقت کنید که در حین اجرای شبیه سازی، ممکن است بسته هایی را مشاهده کنید که خود شما آنها را ایجاد نکرده اید. علت این است

^۱ - Simulation Panel



✓ فصل دوم: شبیه سازی شبکه توسط نرم افزار Packet Tracer

که برخی دستگاه ها می توانند خودشان در حین اجرای شبکه بسته هایی نظیر CDP ایجاد کنند. همچنین می توان نوع بسته هایی را که منتشر می شوند را در قسمت Type مشاهده نمود و برای مخفی کردن آنها باید از دکمه Edit Filter استفاده کرد. برای مشاهده همه انواع بسته ها کافیست بر روی دکمه Show All کلیک نمود.

Evnt List و روند زمانی رویداد

نرم افزار Packet Tracer 4.1 شبیه سازی را در مقیاس زمانی خطی انجام نمی دهد. زمان، بستگی به رویدادهایی دارد که اتفاق می افتد. یک رویداد می تواند در حالات مختلفی و برای هر نوع از PDU که تولید می شود، تعریف گردد. لیست رویدادها اطلاعات مربوط به همه نمونه ها را ثبت می کند. فیلدهای این پنجره به شرح زیر هستند:

- Visible: آیکن یک چشم در این فیلد به معنای این است که رویداد در زمان فعلی شبیه سازی اتفاق افتاده است. همه بسته هایی که در حال نمایش هستند، این آیکن را دارند.
- Time: زمان اتفاق افتادن رویداد را مشخص می کند.
- Last Device: مکان قبلی بسته را مشخص می کند.
- At Device: مکان فعلی بسته را مشخص می کند.
- Type: این فیلد بیانگر نوع بسته است (ARP, CDP, DHCP, EIGRP, ICMP, RIP,) (TCP, UDP, VTP, STP, OSPF, DTP, Telnet, TFTP, HTTP, DNS)
- Info: نمایش اطلاعات جزئی تر در مورد نوع بسته به تفکیک لایه های مدل OSI.

برخی رویدادها بسیار رایج بوده و به طور متداول و برخی رویدادها کمتر اتفاق می افتد. در فضای کاری، رویدادهای شبکه پشت سرهم و با سرعت مشابه (که با لغزنده مشخص شده است) اتفاق می افتند، در حالی که واقعا ممکن است بر حسب میلی ثانیه یا حتی دقیقه فاصله داشته باشند. با مشاهده فیلد Time می توان زمان واقعی رخداد را مشاهده نمود. با فعال کردن گزینه Delay Constant زمان تاخیر 1 ms بین رویدادها لحاظ می شود. اما اگر این گزینه غیرفعال باشد، عوامل مختلفی نظیر تاخیر انتقال، تاخیر انتشار و ... در این تاخیر تاثیر خواهند داشت.

در صورتی که شما برخی از انواع PDU را فیلتر کنید، در لیست رویدادها نمایش داده نخواهند شد ولی هنوز در شبکه وجود داشته و فقط شما آنها را نمی بینید. این کار تنها باعث می شود که شبیه سازی سریعتر اجرا شود.



اجرای مجدد سناریو

وقتی که شبیه سازی مجددا اجرا شود، زمان شبیه سازی صفر شده و لیست رویدادها پاک خواهد شد. شبیه سازی را می توان به شکل های زیر از اول اجرا کرد:

- کلیک بر روی دکمه Reset Simulation
- کلیک بر دکمه Power Cycle Devices
- سوئیچ بر روی حالت Realtime
- تغییر شبکه (حذف، اضافه یا تغییر پیکربندی)
- وارد کردن یک دستور در تنظیمات حالت global یک دستگاه (در CLI)
- سوئیچ به یک سناریوی دیگر
- حذف PDU از لیست داده PDU ها

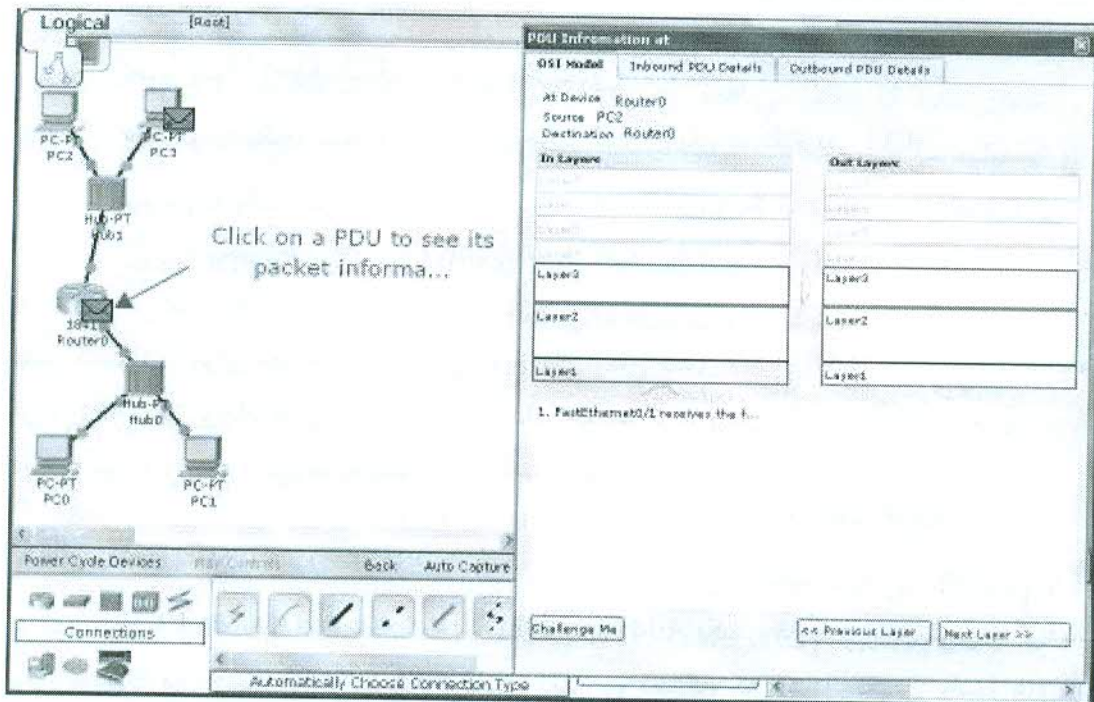
دقت کنید که اجرای مجدد شبیه سازی رویه های زمان بندی شده PDU فعلی را حذف نخواهد کرد، بلکه تنها رویداد های ثبت شده را حذف خواهد کرد. برای حذف PDU ها باید به صورت دستی آنها را از پنجره مربوط به بسته های ایجاد شده کاربر حذف کنید.

ارسال PDU های ساده (Ping)

در نرم افزار Packet Tracer 4.1 دکمه Add Simple PDU یک روش ضروری، سریع و گرافیکی برای ping کردن است. می توانید ping هایی را بین دو دستگاه که حداقل یکی از واسط های آنها آدرس IP دارد ارسال کنید. برای ارسال Ping روی دکمه Add Simple Button کلیک کنید (نشانگر ماوس به آیکن پاکت نامه تغییر می کند). ابتدا روی دستگاه مبدا و سپس روی دستگاه مقصد کلیک کنید. ping تنها در صورتی کار می کند که پورت های دستگاه ها پیکربندی شده باشد. بعد از ایجاد درخواست، دستگاه مبدا یک بسته ICMP یا ARP (یا هر دو) در صف قرار خواهد داد و منتظر خواهد ماند تا دکمه Auto Capture/Play یا Capture/Forward را کلیک کنید. وقتی یکی از این دکمه ها را کلیک کنید، بسته شروع به حرکت خواهد کرد و شما روند ping را مشاهده خواهید کرد. شما می توانید انواع بسته های خاصی را توسط Event List Filters مخفی کنید تا از سردرگمی ایجاد شده توسط تعداد زیاد بسته ها در شبکه جلوگیری شود.

اطلاعات بسته در حالت شبیه سازی

در طول شبیه سازی، می توانید روی یک بسته کلیک نموده (در توپولوژی یا رویداد متناظر آن در لیست رویدادها) تا پنجره اطلاعات آن با جزئیات ظاهر شود. پنجره جزئیات شامل ۳ برگه است. Outbound ODU Details و Inbound PDU Details ، OSMI Model



برگه OSI Model نشان می دهد که چگونه بسته در دستگاه جاری در هر یک از لایه های مدل OSI پردازش می شود. پردازش با توجه به جهت بسته، فرق خواهد داشت. لایه های ورودی (Layer In) نشان می دهند که چگونه یک بسته ورودی یا بافر شده پردازش می شود و لایه های خروجی (Out Layer) نشان می دهند که وقتی قرار است دستگاه بسته ای را از یکی از پورت های خود ارسال کند، چگونه پردازش را انجام می دهند.

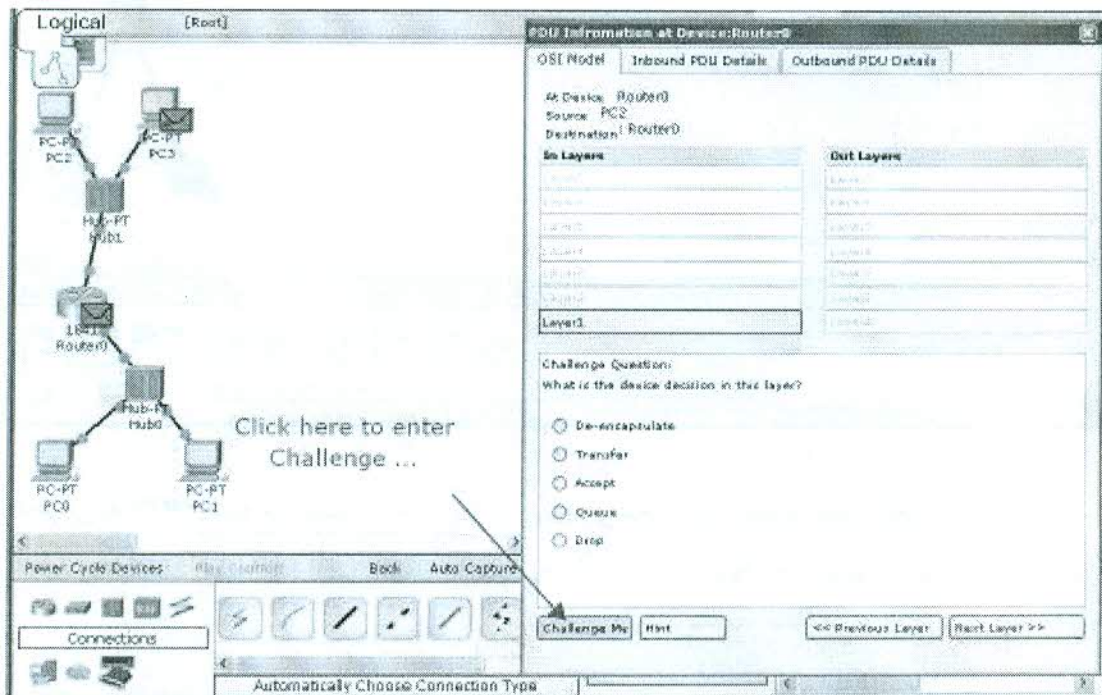
In Layer به معنای این است که از پایین به بالا خوانده می شود (از لایه ۱ تا ۷) و Out Layer از بالا به پایین خوانده می شود (لایه ۷ تا ۱). به این دلیل که لایه فیزیکی اولین لایه ای است که بسته های PDU ورودی با آن مواجه می شوند و آخرین لایه ای است که PDU های خروجی از آن رد خواهند شد تا از دستگاه خارج شوند.

برگه Inbound PDU Details تنها در صورتی وجود دارد که PDU مورد نظر توسط دستگاه دریافت شده باشد. اگر خود دستگاه تولید کننده بسته باشد، این برگه ظاهر نمی شود. این برگه نشان می دهد که دقیقا چه چیزی در سرآمد PDU وجود دارد. برگه Outbound PDU Details اطلاعات مشابهی برای بسته های خروجی دارد. این برگه نیز تنها در صورتی وجود دارد که PDU جهت ارسال وجود داشته باشد.

اکثر اوقات، یک دستگاه PDU ای را دریافت خواهد کرد و سپس بسته ای دیگر را ارسال خواهد کرد. در این حالات هر دو برگه وجود خواهند داشت.

حالت Challenge

شما می توانید از خودتان در مورد رویه های انجام شده در لایه های مختلف آزمون به عمل آورید. برای این منظور باید روی Challenge Me کلیک کنید. جزئیات لایه پنهان خواهد شد و اطلاعات پنجره با سؤال جایگزین خواهد شد و از شما سؤال می شود که دستگاه با PDU چه عملی انجام می شود. شما باید یک گزینه را انتخاب کنید. اگر پاسخ صحیح باشد، جزئیات آن لایه نمایش داده خواهد شد و سؤال مربوط به لایه بعدی پرسیده خواهد شد. برای کسب راهنمایی می توانید از Hint استفاده کنید.



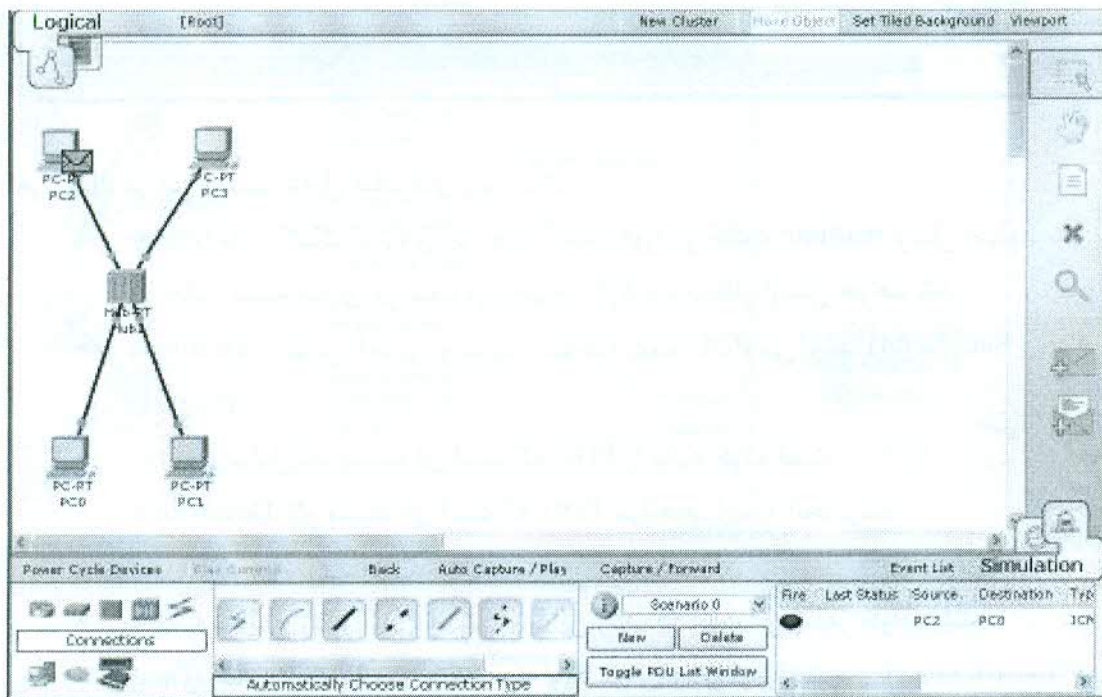


هر سؤال ممکن است شامل پاسخ های زیر باشد:

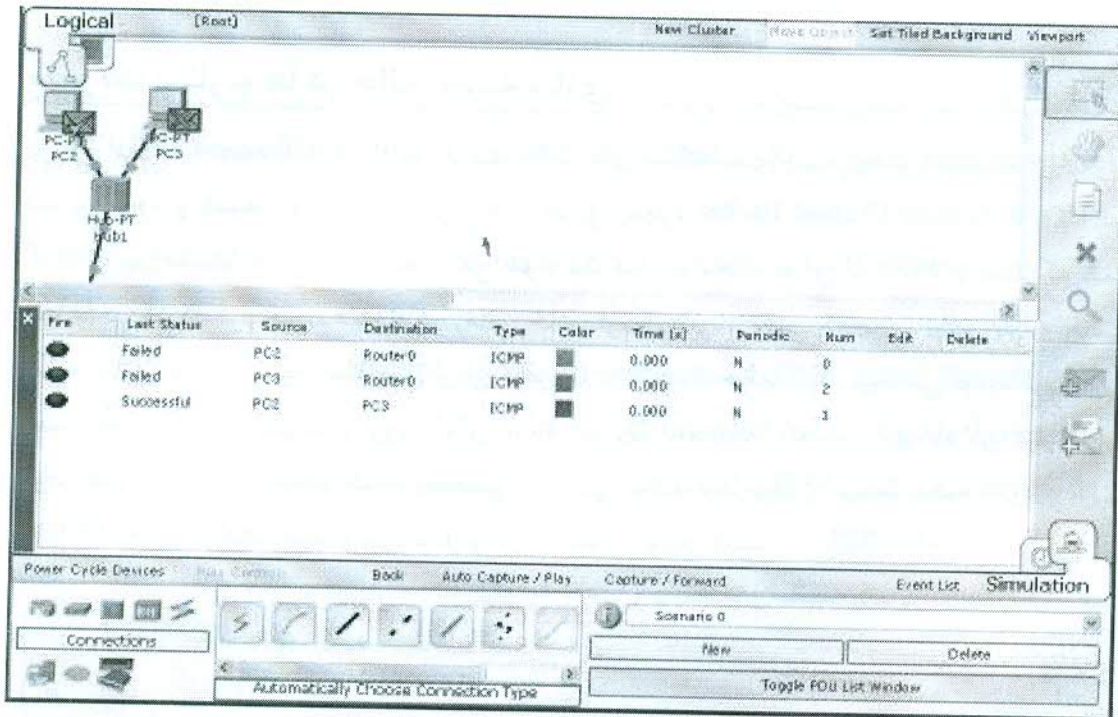
- Encapsulate: افزودن یک header یا یک trailer و header به PDU مربوط به این لایه برای ایجاد PDU ارسالی به لایه پایینتر
- De-encapsulate: حذف header یا trailer از PDU مربوط به این لایه و ایجاد PDU برای لایه بالاتر
- Transfer: انتقال PDU از قسمت inbound به قسمت outbound
- Accept: پذیرش بسته و پایان پردازش آن
- Queue: قرار دادن PDU در صف جهت پردازش یا ارسال در زمانی جلوتر
- Drop: حذف PDU
- Transmit: ارسال سیگنال به خارج از رسانه فیزیکی

مدیریت سناریو ها در حالت شبیه سازی

در نرم افزار Packet Tracer 4.1 می توانید حالت های شبکه بندی (سناریوهای) پیچیده ای را راه اندازی کرده و شبیه سازی کنید. این کار از طریق پنجره User Created Packet یا UCPW در گوشه پایین سمت راست برنامه انجام می شود. یک سناریو مجموعه ای از PDU ها است که شما آنها را در شبکه قرار می دهید تا در زمانی خاص ارسال شوند. وقتی که برای اولین بار به حالت شبیه سازی سوئیچ کنید، سناریوی پیش فرض Scenario 0 خواهد بود. شما می توانید نام آن را تغییر دهید و یا با کلیک بر روی آیکن Scenario Description که در کنار نام آن قرار دارد، توضیحاتی را برای آن ایجاد کنید. همچنین شما می توانید سناریوها را توسط دکمه های New و Delete ایجاد یا حذف کنید و بین سناریوهای مختلف سوئیچ کنید.









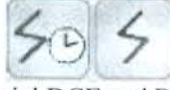
لیست PDU ها ایجاد شده توسط کاربر بخش مهمی در این پنجره است که همه PDU های ایجاد شده در سناریوی جاری را ثبت می کند. با کلیک بر روی Toggle PDU List Windows می توانید این لیست را در پنجره جداگانه خودش مشاهده کنید.



- هر PDU در این لیست شامل فیلدهای زیر است.
- **Fire**: با دابل کلیک بر روی این فیلد، بسته فوراً در حالت realtime ارسال خواهد شد یا در حالت شبیه سازی در صف قرار خواهد گرفت و منتظر ارسال خواهد شد.
 - **Last Status**: شامل آخرین وضعیت شناخته شده PDU می باشد (Successful ، Fail یا Progress)
 - **Source**: شامل نام وسیله ای است که PDU را تولید کرده است
 - **Destination**: نام وسیله ای است که PDU سرانجام باید به آنجا برسد
 - **Type**: نام پروتکل PDU است
 - **Color**: نمایش رنگ PDU است که با این رنگ در انیمیشن ظاهر خواهد شد.
 - **Time**: زمانی از شبیه سازی که بسته باید در آن زمان ارسال شود
 - **Periodic**: این فیلد نشان می دهد که آیا بسته باید به صورت متناوب ارسال شود (Y) یا خیر (N)
 - **Num**: شماره اندیس عددی PDU
 - **Edit**: با دابل کلیک بر روی این دکمه می توانید مشخصه های PDU را ویرایش کنید.
 - **Delete**: با دابل کلیک بر روی این دکمه می توانید PDU را از لیست حذف کنید.

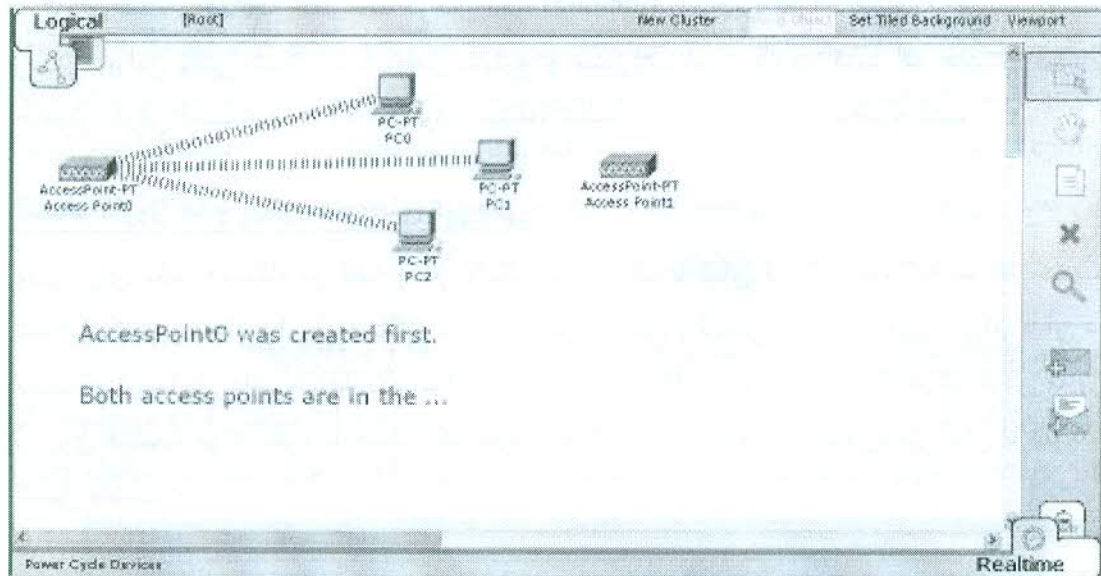
انواع اتصالات

نرم افزار Packet Tracer 4.1 از اتصالات مختلفی پشتیبانی می کند.

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

اتصالات بیسیم

بین نقاط دسترسی و دستگاه های پایانی (نظیر رایانه، سرور، چاپگر) می توان اتصال بی سیم برقرار کرد؛ برای این کار باید مازول فعلی دستگاه را برداشته و بجای آن مازول بی سیم قرار داد. اگر دو یا چند نقطه دسترسی در یک اتاق سیم بندی قرار داشته باشد، مسافت دستگاه از نقاط دسترسی یکسان است، بنابراین اتصال با نقطه دسترسی که زودتر ایجاد شده است برقرار می شود.



وضعیت اتصال

وقتی که دو وسیله به هم متصل می شوند، معمولا چراغ هایی را در دو سمت اتصال مشاهده می گردد. البته برخی اتصالات این چراغ ها را ندارند.

- سبز روشن: اتصال فیزیکی up است.
- سبز چشمک زن: اتصال فعال است.
- قرمز: اتصال down است. سیگنالی پیدا نمی شود.
- کهربایی: پورت در وضعیت بلاک است. (فقط برای سوئیچ ها ظاهر می شود)

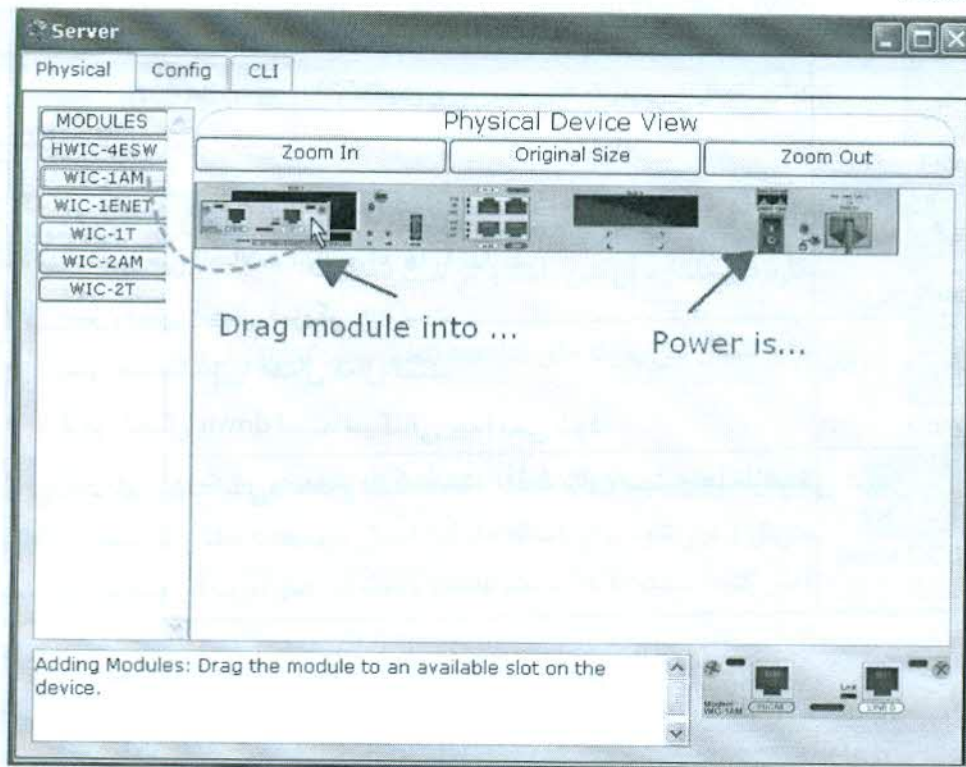


دستگاه ها و ماژول ها

نرم افزار Packet Tracer 4.1 از انواع مختلف ماژول ها برای دستگاه های مختلف پشتیبانی می کند. برای حذف و اضافه کردن ماژول ها باید ابتدا دستگاه خاموش شود. همچنین وقتی که سوئیچ و یا روتر خاموش و سپس مجددا روشن می شود، فایل های پیکربندی startup آنها بارگزاری شده و چنانچه تنظیمات در حال اجرا (running) را ذخیره نکرده باشید، از دست خواهند رفت. بنابراین وقتی شبکه شما شامل سوئیچ و مسیریاب است عادت کنید که همیشه قبل از خاموش کردن دستگاه ها یا Reset کردن شبکه، تنظیمات در حال اجرا را ذخیره کنید.

لیست ماژول ها و پیکربندی های فیزیکی

وقتی روی یک دستگاه در فضای کار کلیک کنید، ابتدا با نمای فیزیکی دستگاه مواجه خواهید شد. یک تصویر محاوره ای از دستگاه در پانل اصلی نمایش و لیستی از ماژول های سازگار با آن در سمت چپ نمایش داده خواهد شد. با فشردن دکمه Power و افزودن ماژول (با درگ کردن ماژول بر روی قسمت مورد نظر) یا حذف یک ماژول (درگ کردن ماژول به بیرون) می توان با دستگاه تعامل داشت.





پیکربندی دستگاه ها

همانند شبکه های واقعی، شبکه هایی که با نرم افزار Packet Tracer 4.1 ایجاد می شوند نیز باید قبل از این که کارکنند، بدرستی پیکربندی شوند. برای دستگاه های ساده این کار به صورت وارد کردن چند فیلد ساده (نظیر آدرس IP و subnet mask) و یا انتخاب گزینه هایی در صفحه گرافیکی پیکربندی (در برگه config) می باشد. از طرف دیگر مسیریاب ها و سوئیچ ها دستگاه های پیشرفته ای هستند که تنظیمات پیچیده تری دارند. برخی از این تنظیمات می تواند در برگه config انجام شود، اما اکثر پیکربندی های پیشرفته باید توسط دستورات IOS سیسکو انجام شوند. این بخش برگه config را برای همه دستگاه ها شرح می دهد. همچنین لیست کامل دستورات IOS پشتیبانی شده مسیریاب و سوئیچ را مشاهده خواهید کرد.

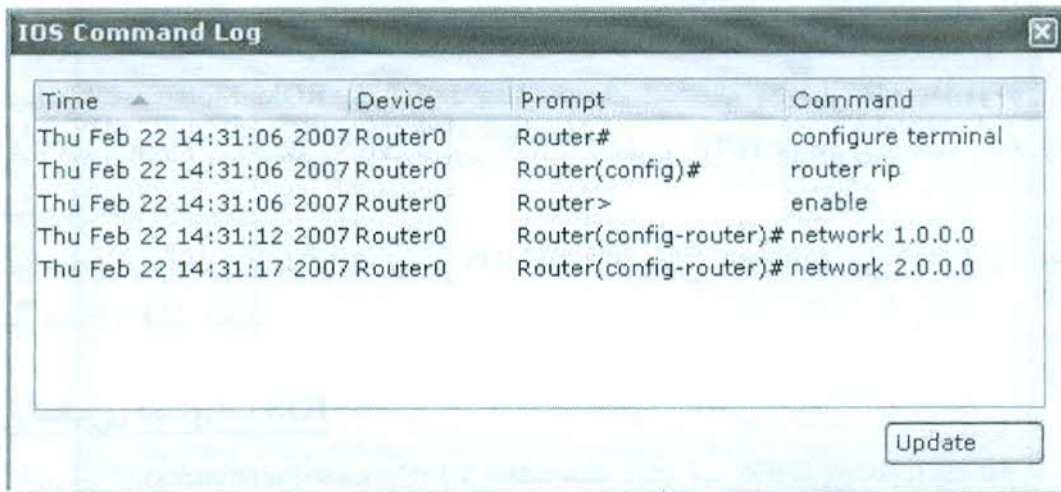
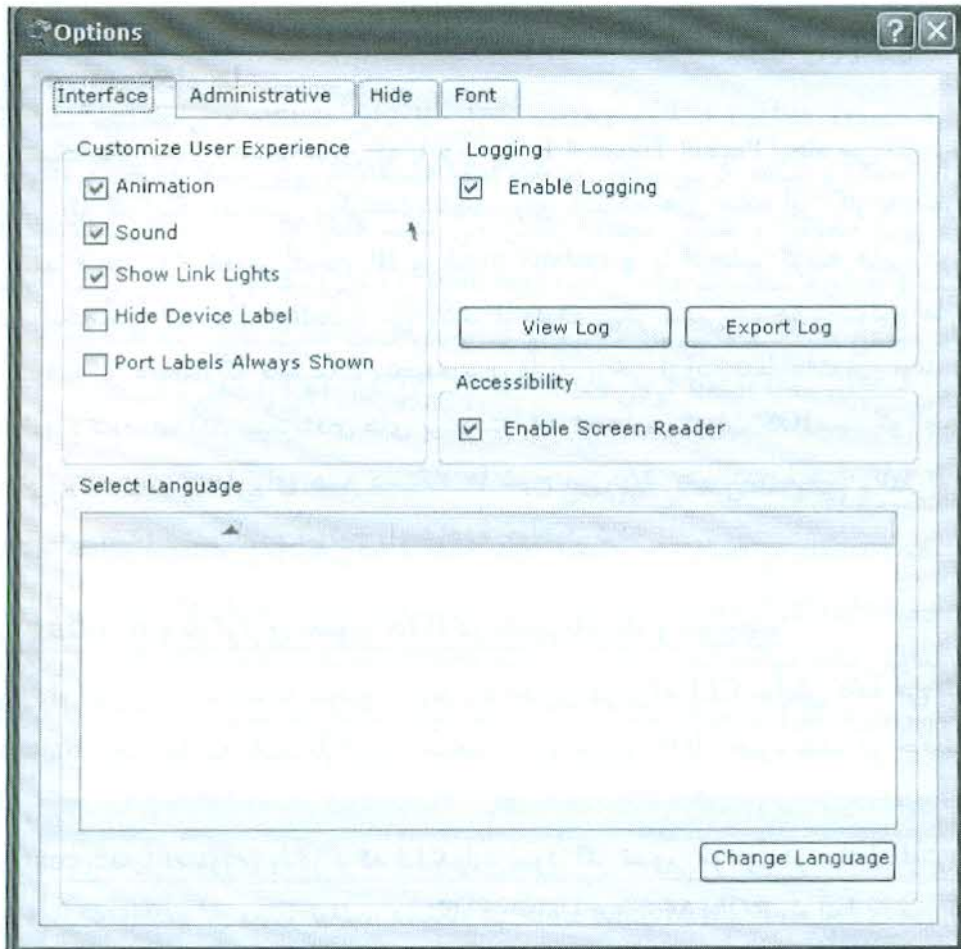
ترتیب Booting و بارگزاری تصویر IOS در مسیریاب ها و سوئیچها

در حین راه اندازی مسیریاب یا سوئیچ، روند راه اندازی در برگه CLI نمایش داده می شود، اگر فایل startup وجود داشته باشد بارگزاری خواهد شد و تصویر IOS ذخیره شده در حافظه فلش، برای اجرا در RAM بارگزاری می شود. در حالی که تصویر IOS بارگزاری می شود، نمی توان وارد برگه config شد یا دستوری را در برگه CLI وارد نمود. اگر تصویر موجود در حافظه فلش نامعتبر باشد یا فایل مربوط به آن معتبر نباشد، دستگاه در حالت ROM Monitor راه اندازی می گردد. در صورت فشار کلید های Ctrl+Break یا Ctrl+C (در ۶۹ ثانیه اول راه اندازی دستگاه) نیز می توان وارد این حالت شد. البته پس از گذشت ۱۰ ثانیه می توانید سریعتر به دستگاه دسترسی داشته باشید. حالت ROM Monitor یک محیط بسیار کوچک است که می توان فایل ها موجود در NVRAM و Flash را دستکاری کرد، تصاویر IOS را از طریق TFTP بارگزاری و نحوه راه اندازی دستگاه را انتخاب کنید.

وقتی مراحل راه اندازی و بارگزاری تصویر IOS کامل شد، حالت logout بار می شود. برای شروع کلید Enter را فشار دهید.

گزارشگیری دستورات IOS

اگر این ویژگی (Options>Preferences) فعال باشد همه دستورات IOS وارد شده را می توان ثبت کرد. با کلیک بر روی دکمه View پنجره گزارش دستورات باز خواهد شد.

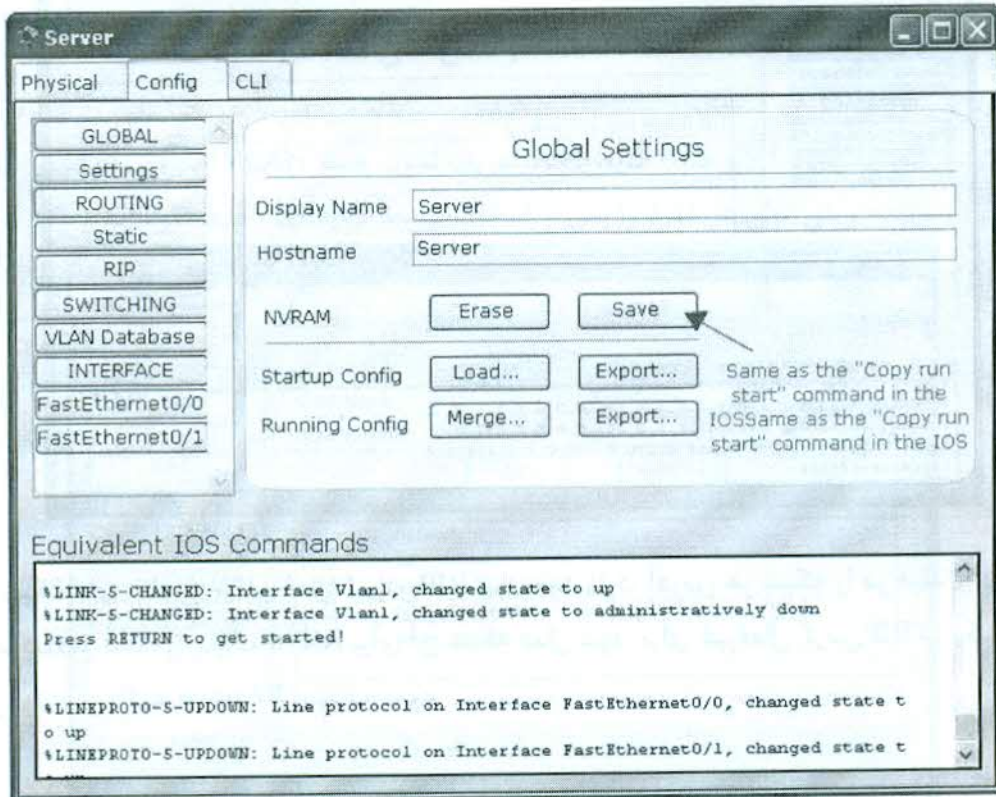


پیکربندی مسیریاب

در برگه Config امکان انجام ۴ سطح پیکربندی global ، routing ، switching ، و interface وجود دارد. برای انجام یک پیکربندی global، روی دکمه GLOBAL کلیک تا دکمه Settings نمایش داده شود. برای پیکربندی مسیریاب، دکمه ROUTING را کلیک و Static یا RIP را انتخاب کنید. برای پیکربندی سوئیچ، دکمه SWITCHING را کلیک تا Vlan Database نمایش داده شود. برای پیکربندی یک واسط، دکمه INTERFACE را کلیک تا لیست واسط ها نمایش داده شود. کادر پایین پنجره پیکربندی ها در برگه Config ، دستورات IOS معادل اعمالی که انجام می دهید را نمایش می دهد.

تنظیمات Global:

در تنظیمات Global شما می توان نام مسیریاب (جهت نمایش در فضای کاری) و نام میزبان (جهت نمایش در IOS) را تعیین نمود. همچنین می توان فایل های پیکربندی مسیریاب را به شکل های مختلف دستکاری کرد:

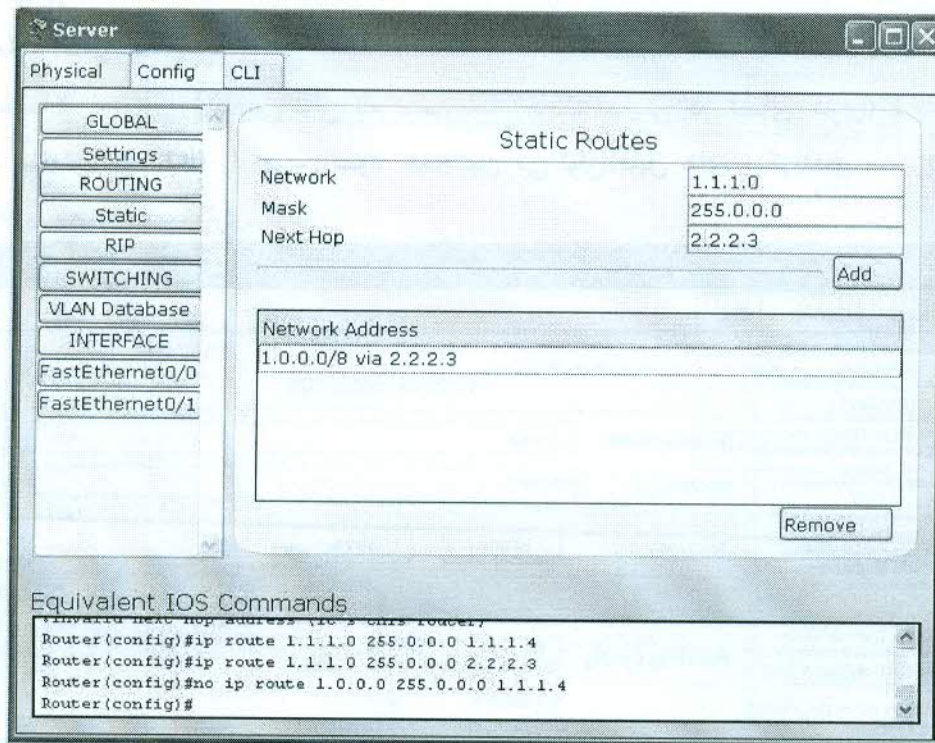


- حذف NVRAM (جایی که تنظیمات Startup ذخیره می شوند)
- ذخیره کردن تنظیمات در حال اجرای فعلی در NVRAM

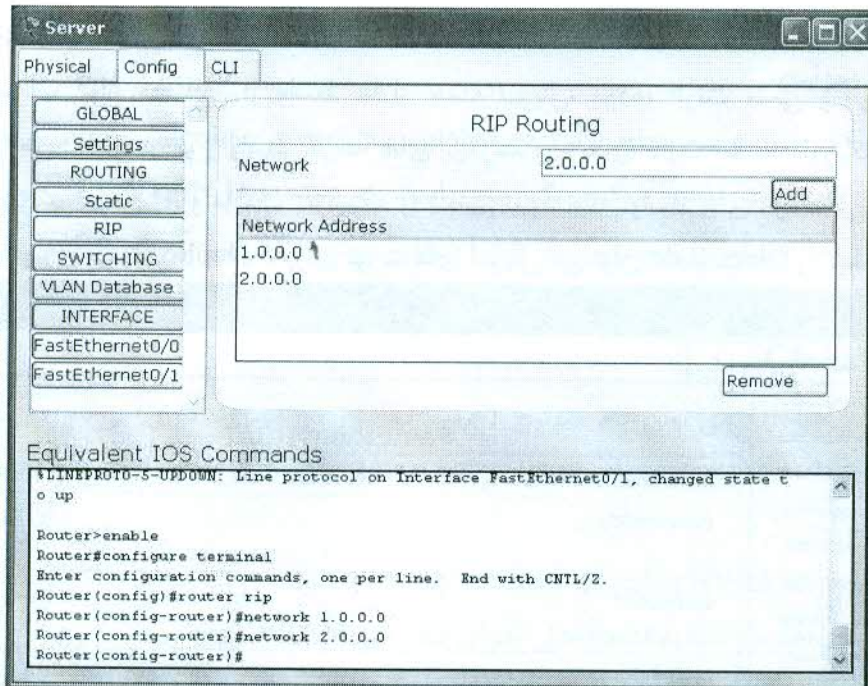
- استخراج تنظیمات startup و running در یک فایل متن
- بارگزاری یک فایل پیکربندی (با فرمت متنی)
- ادغام تنظیمات در حال اجرای فعلی با یک فایل پیکربندی دیگر

پیکربندی مسیریابی:

با انتخاب Static مسیریابی را می توان به روش استاتیگ انجام داد. هر مسیر استاتیکی که اضافه می گردد نیازمند یک آدرس IP، ماسک زیرشبکه و آدرس گام بعدی می باشد. همچنین default gateway را نیز می توان تنظیم نمود.

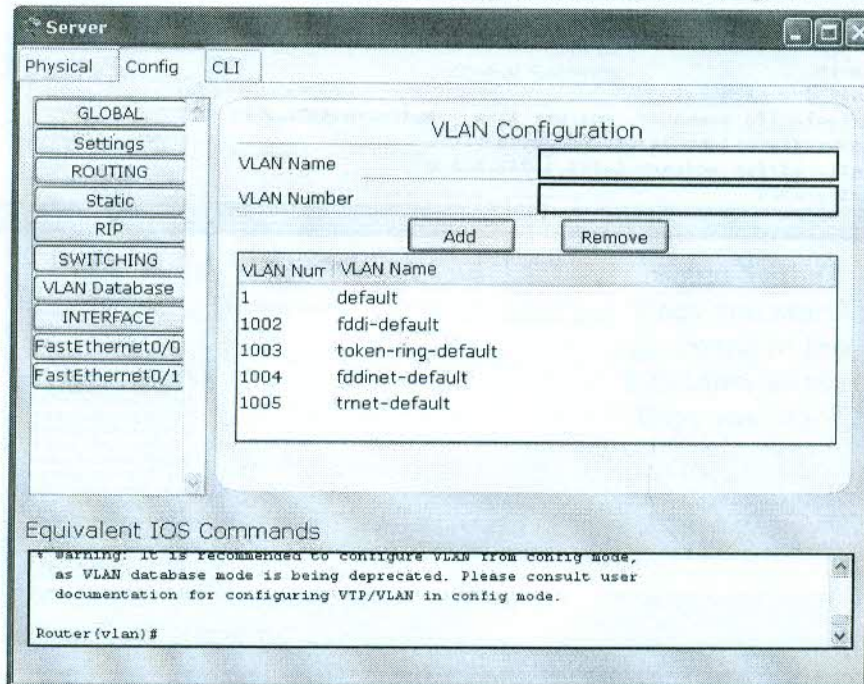


در شبکه های خاصی امکان فعال نمودن RIP نیز وجود دارد. آدرس هر شبکه را در فیلد Network وارد کنید و Add را کلیک تا RIP برای آن شبکه فعال شود. برای غیرفعال کردن RIP در یک شبکه می توانید از دکمه Remove استفاده نمود.



پیکربندی های پایگاه داده VLAN (فقط در مدل های 1481 و 2811):

VLAN مسیریاب ها در قسمت VLAN Database مدیریت می شود. هر VLAN را می توان با وارد کردن نام و شماره آن و فشار کلید Add تعریف نمود. همه VLAN های موجود، در لیست نمایش داده شده و می توان هر مورد را پس از انتخاب توسط Remove حذف کرد.



پیکربندی واسط:

یک مسیریاب انواع مختلفی از واسط ها از جمله سریال، مودم، اترنت مسی و اترنت فیبر را پشتیبانی می کند. هر نوع واسط گزینه های پیکربندی زیادی دارد. اما به طور کلی می توان وضعیت پورت، آدرس IP و ماسک زیرشبکه را تنظیم نمود. برای واسط های اترنت می توان آدرس فیزیکی، پهنای باند و Duplex و برای پورت های سریال می توان Clock Rate را تنظیم نمود.

The screenshot shows the configuration window for a Server's FastEthernet0/0 interface. The window is titled "Server" and has tabs for "Physical", "Config", and "CLI". The "Config" tab is active, showing the configuration for the "FastEthernet0/0" interface. The configuration includes:

- Port Status: On
- Bandwidth: Auto
- Duplex: Auto
- MAC Address: 0000.0C9B.D2D8
- IP Address: 1.1.1.1
- Subnet Mask: 255.0.0.0

Below the configuration, there is a section for "Equivalent IOS Commands" which shows the following commands:

```

o up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state t
o up

Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface FastEthernet0/0
Router(config-if)#ip address 1.1.1.1 255.0.0.0
Router(config-if)#
  
```

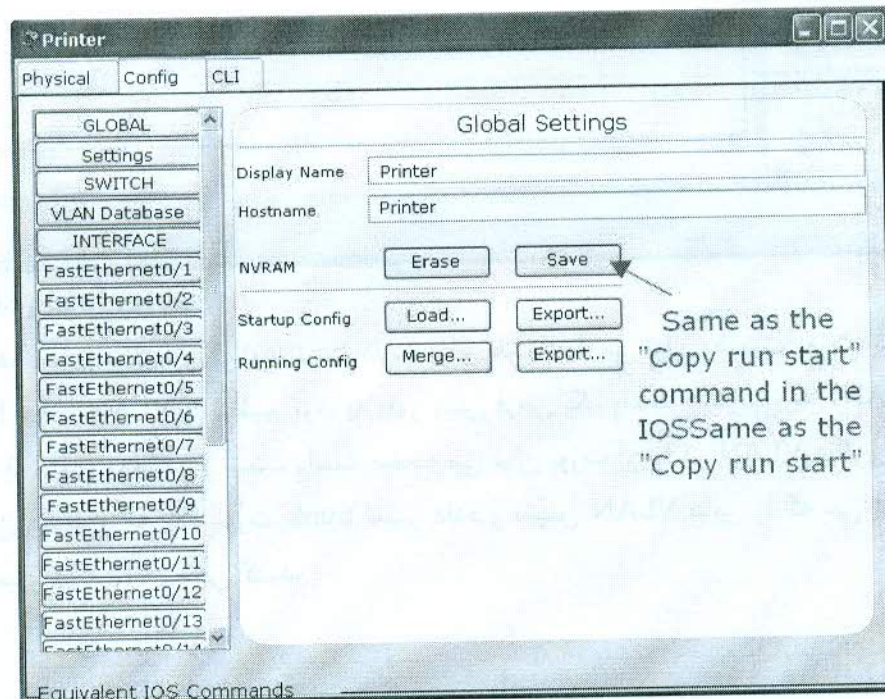
پیکربندی سوئیچ

برگه Config در سوئیچ سه سطح پیکربندی global، switching، interface را دارد. سطح global همانند مسیریاب است. سطح سوئیچینگ جایی است که VLAN Database را می توان مدیریت کرد. سطح واسط هم امکان دسترسی به VLAN های سوئیچ را فراهم می آورد. کادر پایین پنجره پیکربندی در برگه Config، دستورات IOS معادل اعمالی که انجام می دهید را نمایش می دهد.

تنظیمات Global:

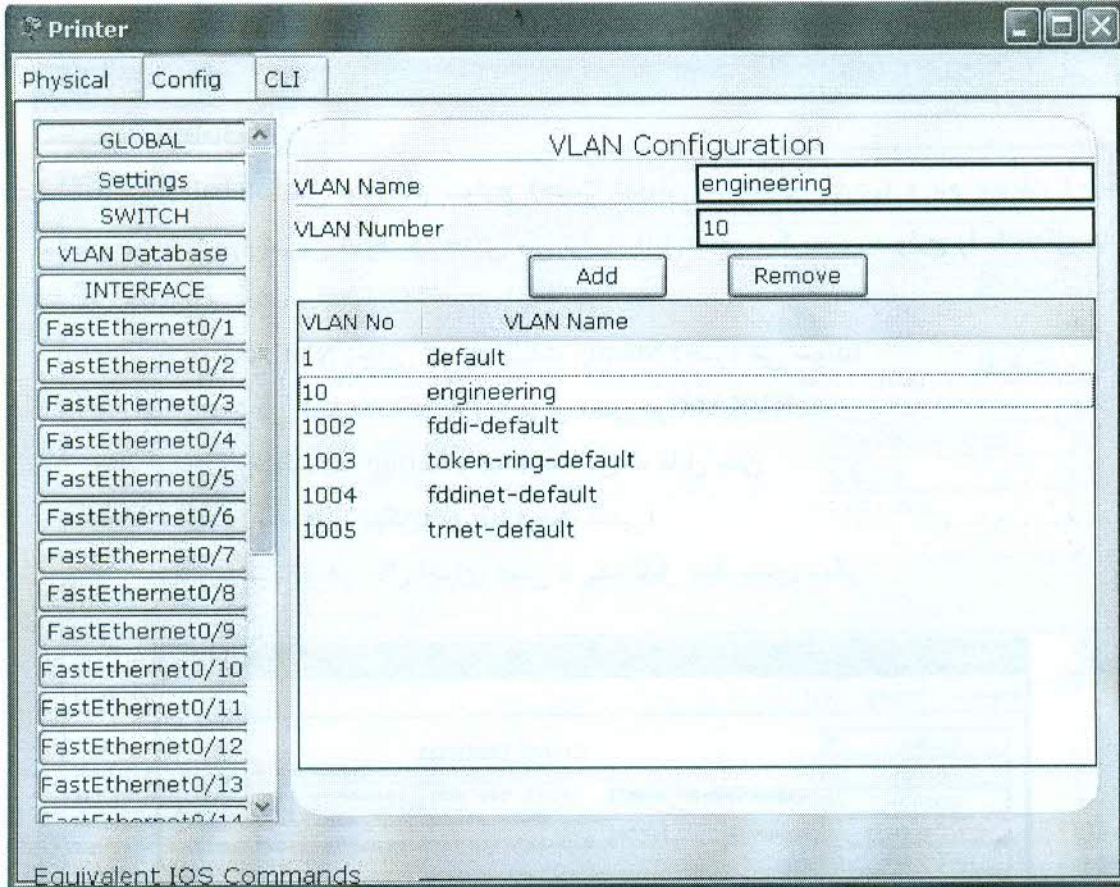
در تنظیمات Global می توان نام سوئیچ (جهت نمایش در فضای کاری) و نام میزبان (جهت نمایش در IOS) را تعیین نمود. همچنین می توانید فایل های پیکربندی سوئیچ را به شکل های مختلف دستکاری کرد:

- حذف NVRAM (جایی که تنظیمات Startup ذخیره می شوند)
- ذخیره کردن تنظیمات در حال اجرای فعلی در NVRAM
- استخراج تنظیمات startup و running در یک فایل متن
- بارگزاری یک فایل پیکربندی (با فرمت متنی)
- ادغام تنظیمات در حال اجرای فعلی با یک فایل پیکربندی دیگر



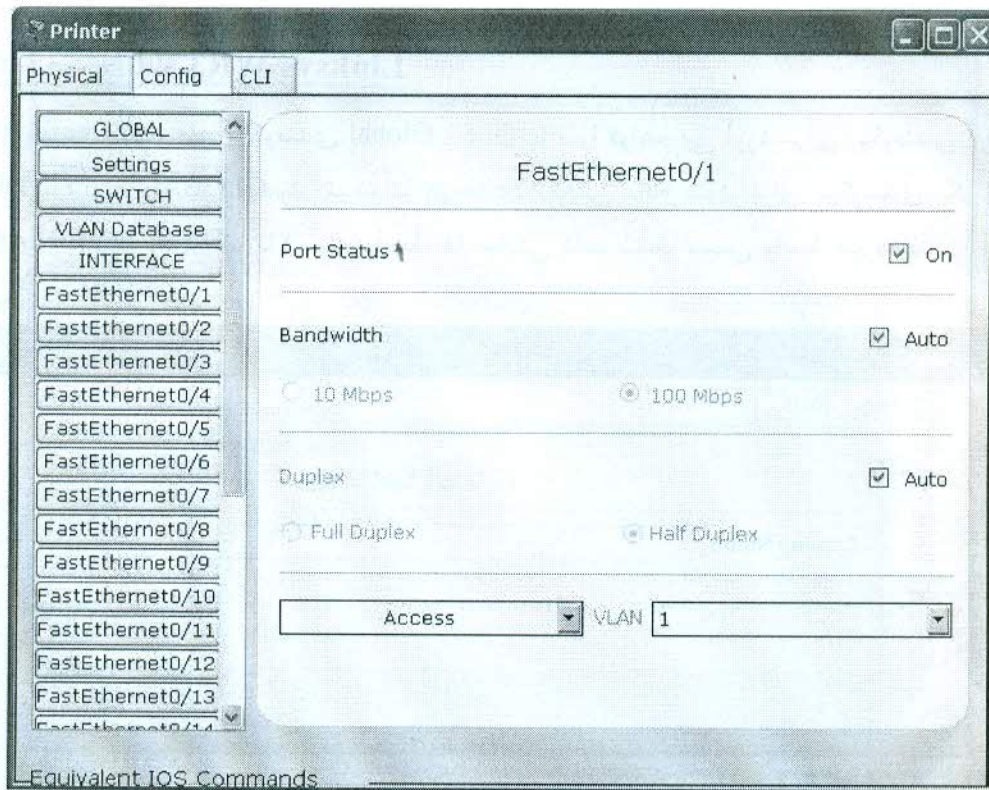
پیکربندی VLAN Database:

VLAN های سوئیچ را از قسمت VLAN Database می توان مدیریت نمود. تعریف هر VLAN با وارد کردن نام و شماره آن و فشار کلید Add انجام می گیرد. همه VLAN های موجود، در لیست نمایش داده شده و هر مورد را پس از انتخاب آن توسط Remove می توان حذف کرد.



پیکربندی Interface:

سوئیچ ها فقط واسط های از نوع اترنت دارند. برای هر واسط می توان وضعیت پورت، پهنای باند و Duplex حالت VLAN را تنظیم کرد. به طور پیش فرض یک واسط دسترسی به VLAN1 دارد. با استفاده از منوی موجود در سمت راست صفحه می توان پورت آن را در VLAN دیگری قرار دهید. همچنین واسط را به یک پورت trunk تغییر داده و سپس VLAN هایی را که می توانند از این trunk عبور کنند را مشخص کنید.

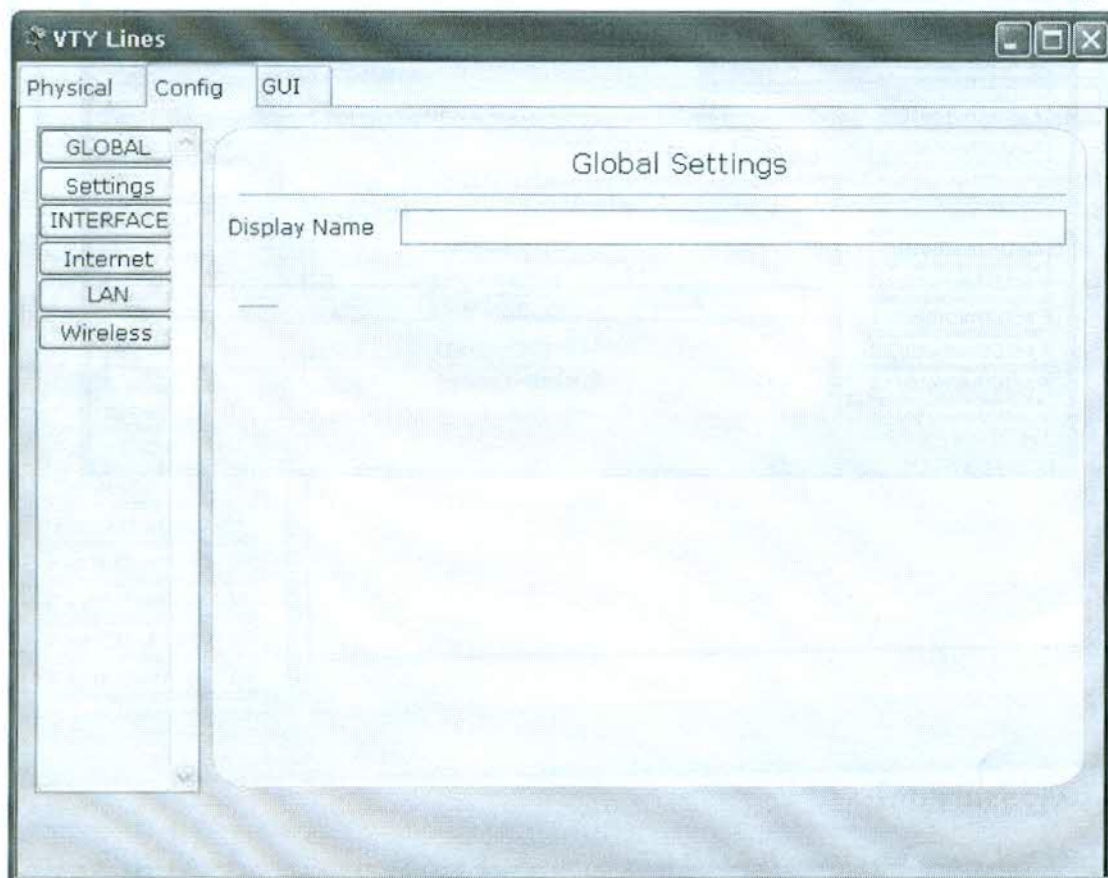




✓ فصل دوم: شبیه سازی شبکه توسط نرم افزار Packet Tracer

پیکربندی Linksys WRT300N

برگه Config دو سطح پیکربندی Global و interface را فراهم می آورد. برای پیکربندی در سطح global، دکمه GLOBAL را کلیک تا Settings نمایش داده شود. برای پیکربندی یک واسط، INTERFACE را کلیک تا لیست واسط ها نمایش داده شده، سپس واسط مورد نظر را انتخاب کنید.

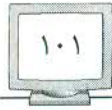


تنظیمات Global:

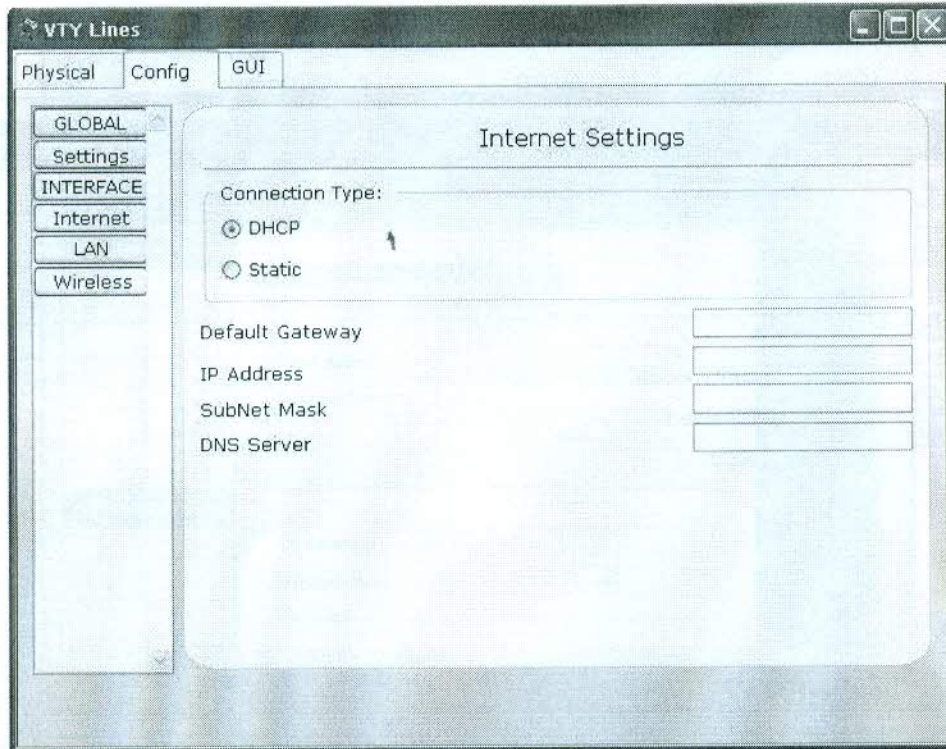
در تنظیمات Global می توان نام نمایش داده شده در صفحه را تغییر داد.

تنظیمات واسط اینترنت:

در تنظیمات Internet نوع اتصال و این که IP به صورت اتوماتیک از DHCP گرفته شود یا به طور دستی، می توان تنظیم نمود.

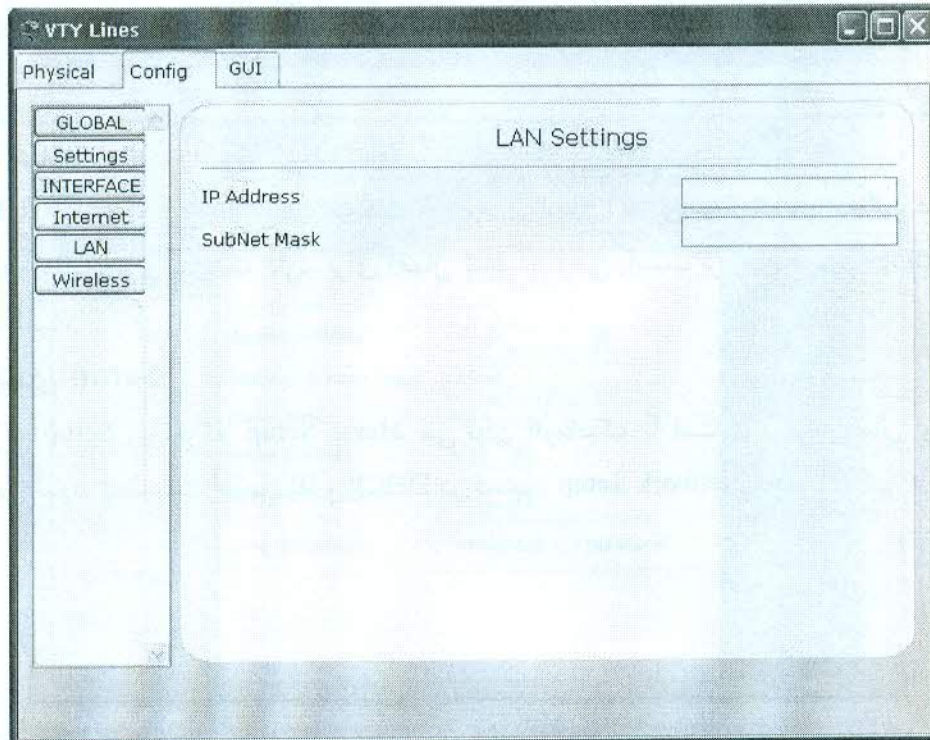


✓ فصل دوم: شبیه سازی شبکه توسط نرم افزار Packet Tracer



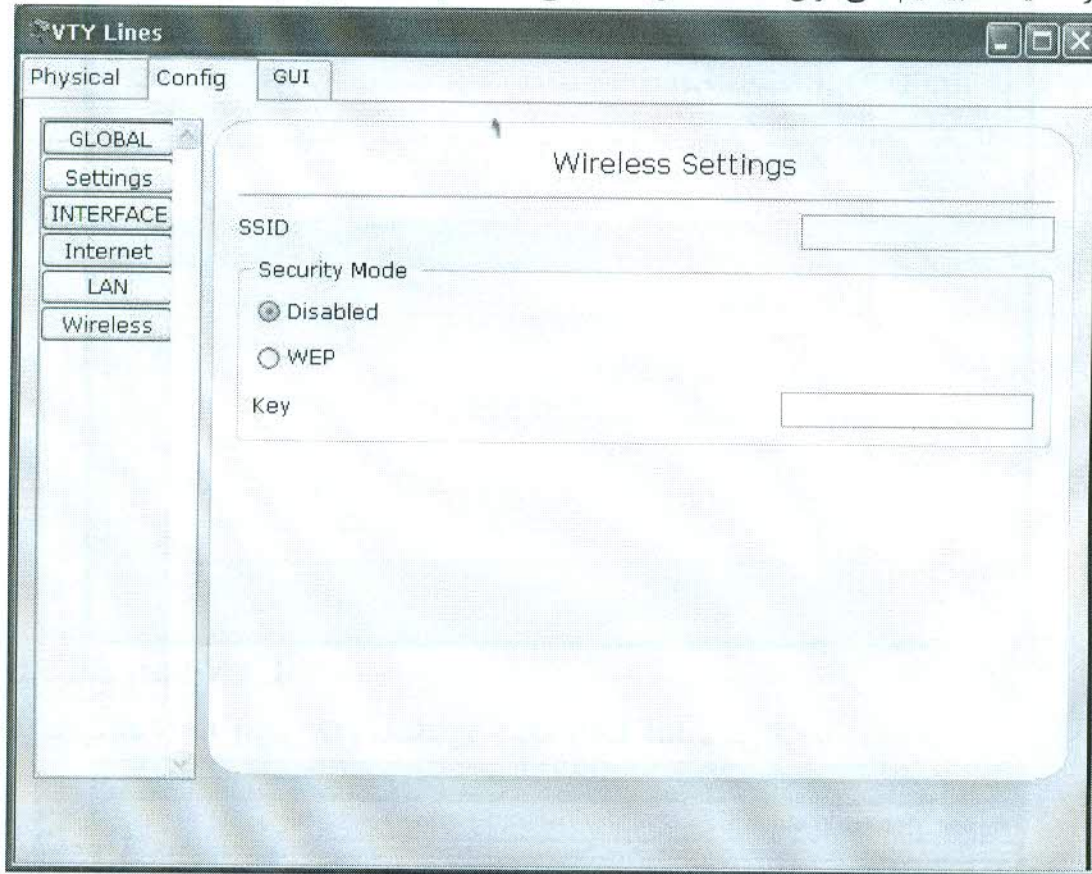
تنظیمات واسط LAN:

در تنظیمات LAN آدرس IP و ماسک زیر شبکه LAN تنظیم می گردد.



پیکربندی واسط Wireless:

در تنظیمات بیسیم، می توان SSID، گزینه امنیتی WEP، و کلید احراز هویت را تنظیم نمود.



واسط گرافیکی Linksys WRT300N:

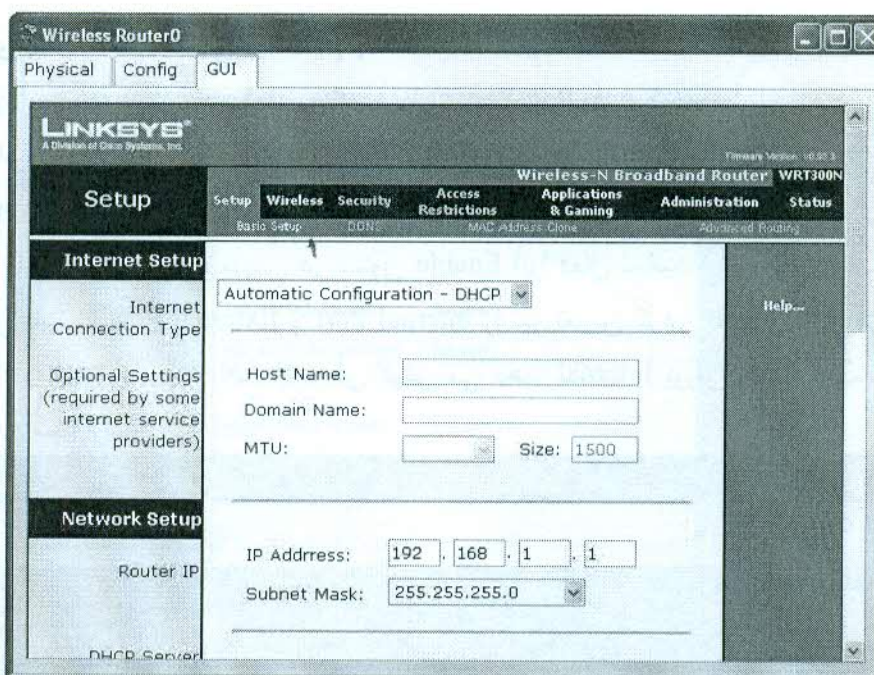
برگه GUI، پیکربندی ها و تنظیمات مشابه برگه Config و همچنین تعدادی ویژگی دیگر برای port forwarding و مدیریت دارد. برای اعمال تنظیمات می بایست بر روی دکمه Save Settings کلیک کنید.

پیکربندی Setup:

در برگه Setup زیر برگه Basic Setup، می توان اتوماتیک یا استاتیک نوع اتصال اینترنت را مشخص نمود. تنظیمات آدرس IP و DHCP در قسمت Network Setup انجام می گیرد.

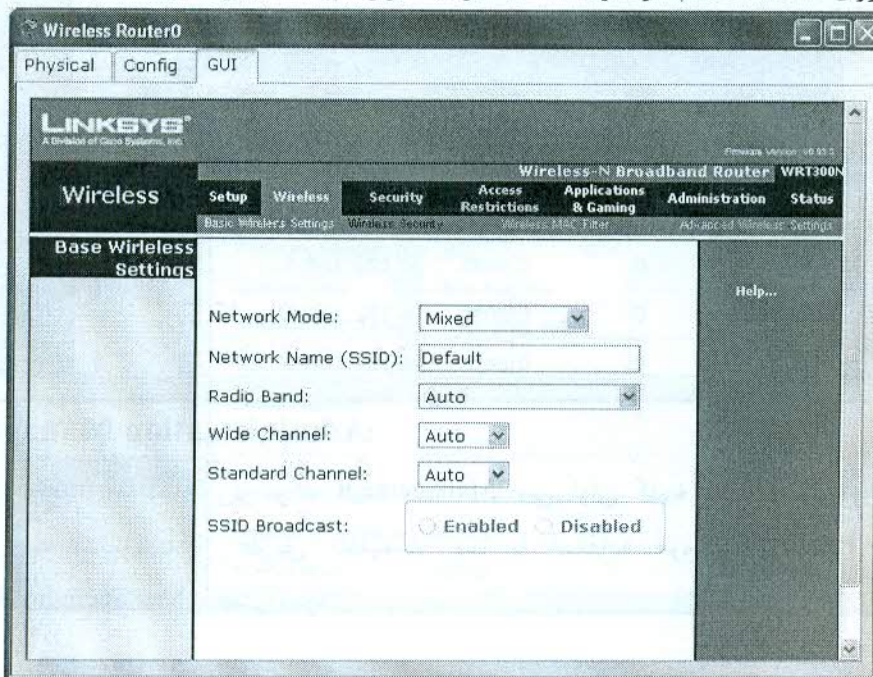


✓ فصل دوم: شبیه سازی شبکه توسط نرم افزار Packet Tracer



پیکربندی Wireless:

در برگه Wireless زیر برگه Basic Wireless Settings، تنها تنظیمی که قابل تغییر است Network Name (SSID) است. در زیر برگه Wireless Security حالت امنیتی را می توان غیرفعال یا آن را بر روی WEP تنظیم کرد. و یک کلید برای احراز هویت تعیین نمود.





✓ فصل دوم: شبیه سازی شبکه توسط نرم افزار Packet Tracer

پیکربندی Application & Gaming:

در برگه Application & Gaming زیر برگه Single Port Forwarding می توان بسته ها را به آدرس IP دلخواه ارسال کرد. برای forward کردن یک بسته، برنامه مورد نظر را از قسمت Name Application انتخاب و آدرس IP را که قصد دارید بسته ها به آنجا ارسال شوند را در ستون To IP Address وارد کنید. سپس در ستون Enable آنرا فعال نمائید. برای ارسال به یک پورت دلخواه می بایست External Port و Internal Port را نیز تعیین کرد. External پورتی است که مسیریاب Linksys از سمت WAN به آن گوش می دهد. Internal پورتی است که بسته ها را به سرور محلی شما ارسال می کند.

The screenshot shows the configuration page for a Linksys WRT300N router. The 'Applications & Gaming' section is active, specifically the 'Single Port Forwarding' sub-section. On the left, there are five dropdown menus for 'Application Name', all set to 'None'. Below them are three empty text input fields. The main table lists forwarding rules with columns for 'External Port', 'Internal Port', 'Protocol', 'To IP Address', and 'Enabled'. The first five rows have '---' for ports and '192.168.1.' for the IP address. The last three rows have '0' for both ports and 'Both' for the protocol, with the IP address '192.168.1.'. All 'Enabled' checkboxes are currently unchecked.

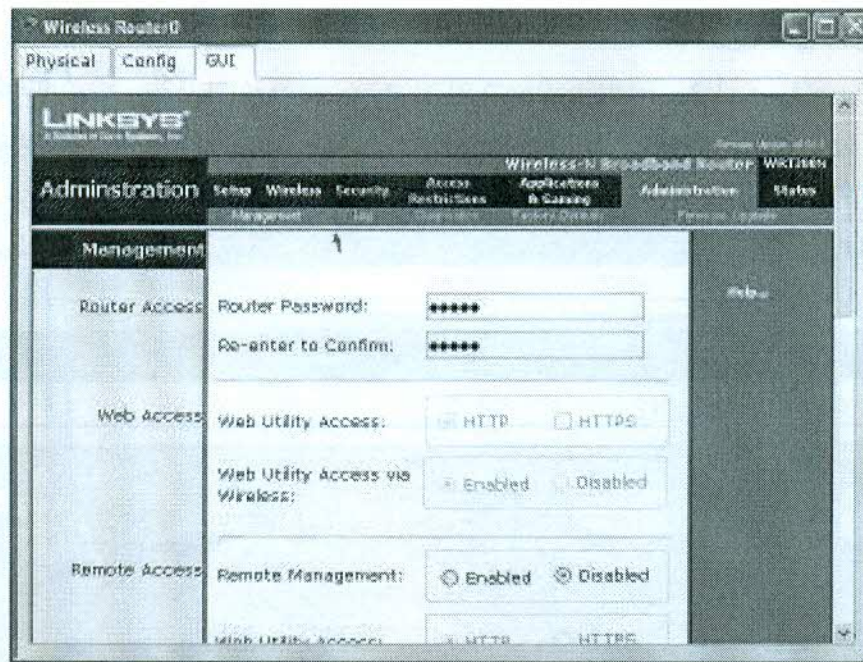
External Port	Internal Port	Protocol	To IP Address	Enabled
---	---	---	192.168.1.	<input type="checkbox"/>
---	---	---	192.168.1.	<input type="checkbox"/>
---	---	---	192.168.1.	<input type="checkbox"/>
---	---	---	192.168.1.	<input type="checkbox"/>
---	---	---	192.168.1.	<input type="checkbox"/>
0	0	Both	192.168.1.	<input type="checkbox"/>
0	0	Both	192.168.1.	<input type="checkbox"/>
0	0	Both	192.168.1.	<input type="checkbox"/>

Administration Management:

در برگه Administration زیر برگه Management، می توان کلمه عبور پیش فرض را برای دسترسی به مسیریاب از طریق تنظیمات وب با استفاده مرورگر وب PC انجام داد. و Management Remote را فعال نمود.

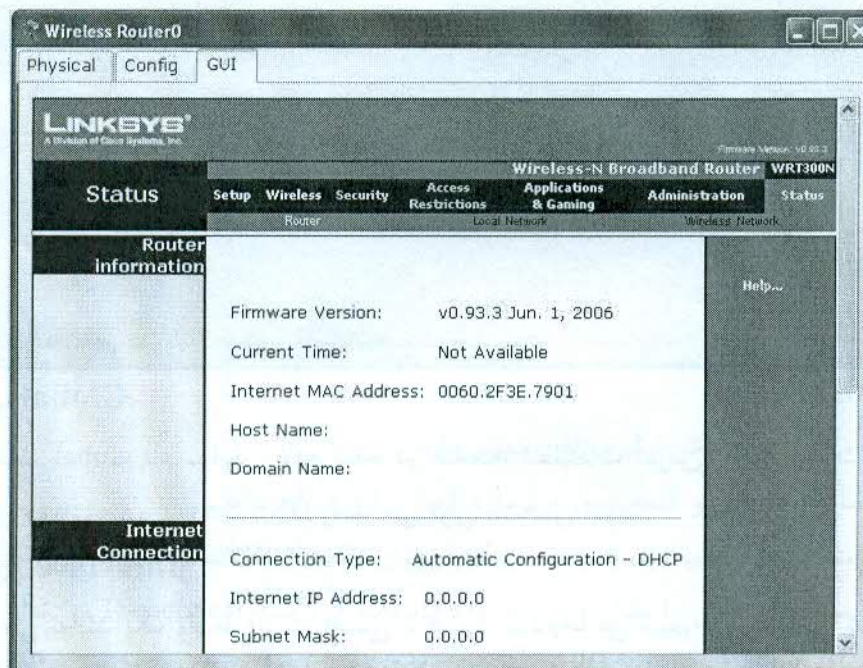


✓ فصل دوم: شبیه سازی شبکه توسط نرم افزار Packet Tracer



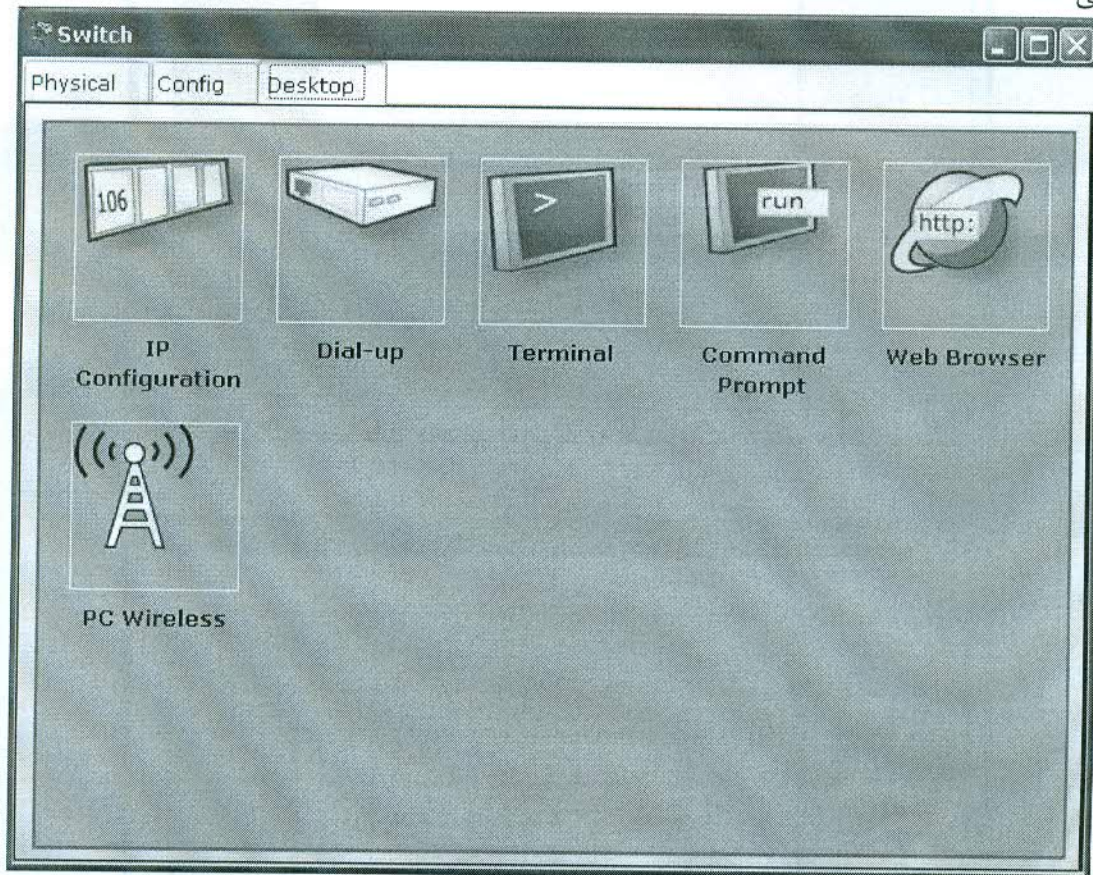
:Status

در برگه Status می توانید اطلاعات مختلف مربوط به مسیریاب، شبکه محلی و شبکه بی سیم را مشاهده کنید.



پیکربندی PC

در برگه Config شما می توانید تنظیمات Global و Interface را انجام دهید. علاوه بر این برگه Desktop ابزارهایی را برای پیکربندی IP، پیکربندی diul-up، استفاده از پنجره terminal، باز کردن واسط خط فرمان، بازکردن مرورگر وب و پیکربندی تنظیمات بی سیم Linksys فراهم می کند.



تنظیمات Global:

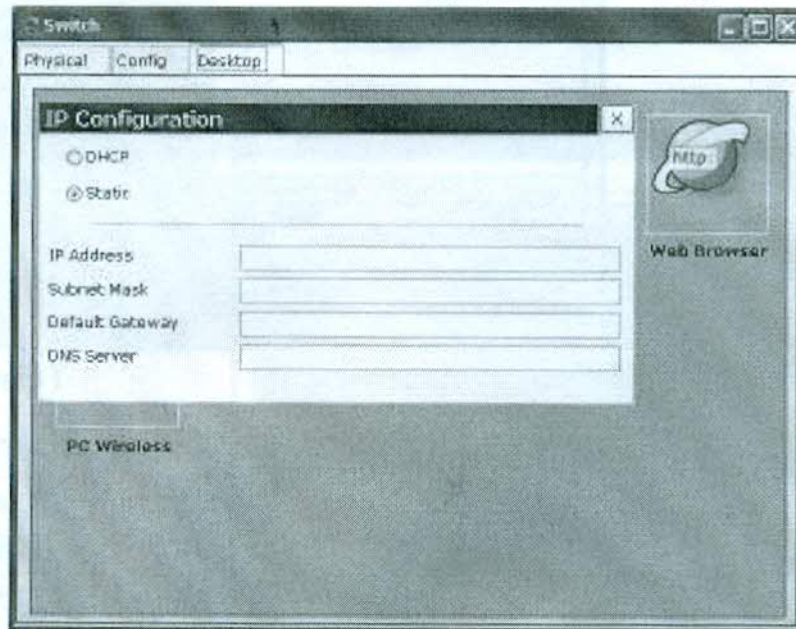
در تنظیمات global نام نمایش داده شده در صفحه، تنظیمات آدرس IP به صورت استاتیک یا پویا، و نیز Gateway و DNS Server را نیز می توان مشخص نمود.

پیکربندی Interface:

رایانه ها می توانند یک واسط اترنت (مسی یا فیبر)، مودم یا بی سیم را پشتیبانی کنند. وضعیت پورت، پهنای باند، Duplex و آدرس MAC، آدرس IP و ماسک زیرشبکه را برای واسط می توان تنظیم کرد که البته با توجه به نوع واسط متغیر است.

ابزار IP Configuration:

در برگه Desktop روی آیکن IP Configuration کلیک نموده تا این ابزار باز شود. اگر PC به یک مسیریاب یا سرور DHCP متصل باشد، با استفاده از DHCP به طور خودکار IP می گیرد، در غیر اینصورت باید IP به صورت استاتیک تنظیم شود.



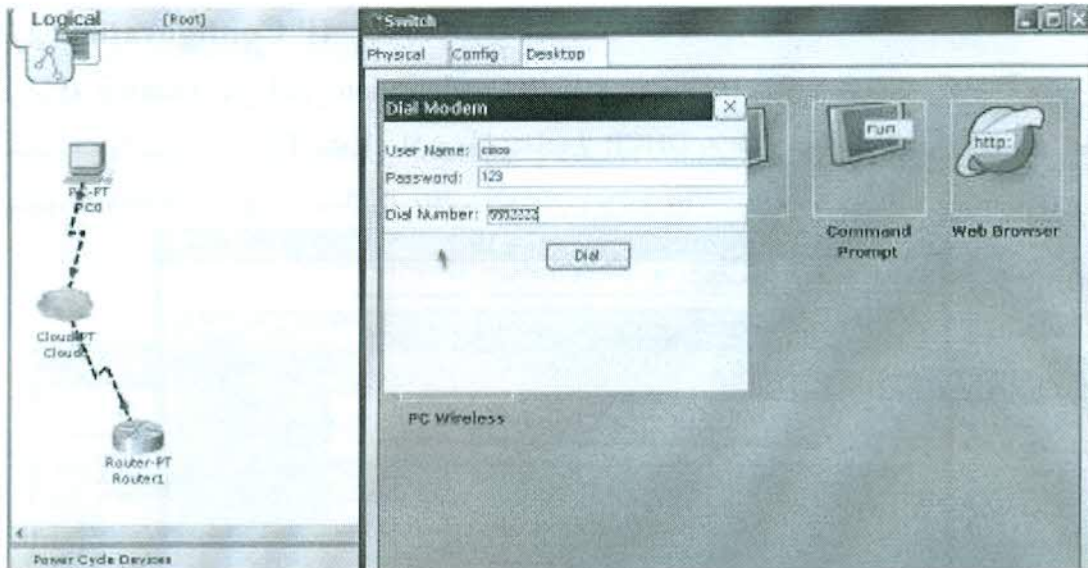
ابزار Modem Dial-Up:

در برگه Desktop، بر روی آیکن Dial-up کلیک کنید تا ابزار آن باز شود. اتصال مودم را می توان با اتصال PC به یک ابر که به روتر متصل است برقرار نمود. ابر مانند یک شرکت تلفن بین PC و مسیریاب عمل می کند. برای برقراری تماس باید شرایط مختلفی برقرار باشد.

- مسیریاب یک مودم دارد و شما احراز هویت با نام کاربری را در مسیریاب راه اندازی کرده اید (با استفاده از دستور LINE password WORD username در حالت global IOS)

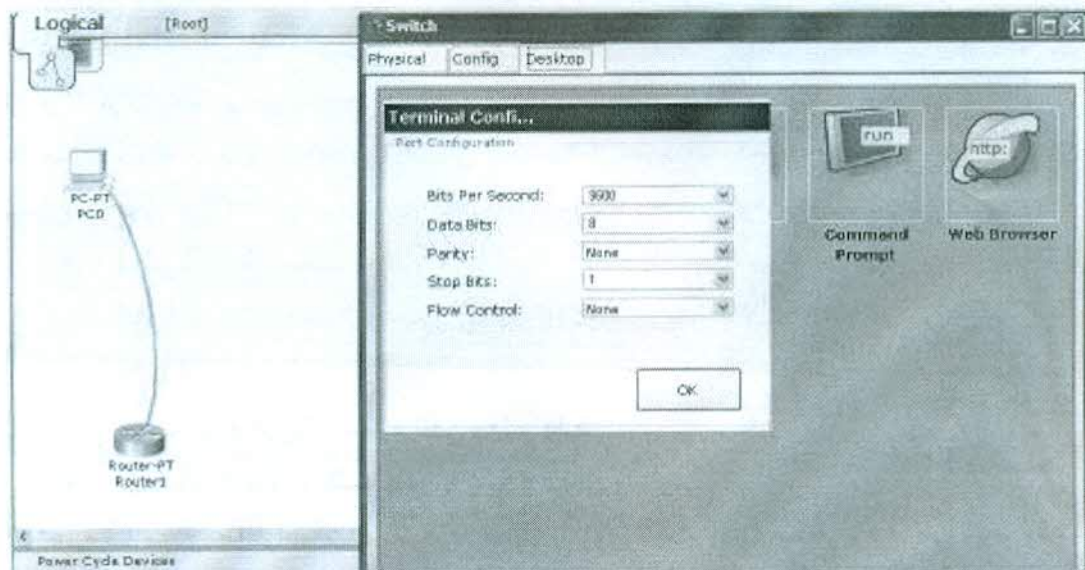
- پورت مودم ابر یک شماره تلفن معتبر دارد
- شما نام کاربری و کلمه عبور و شماره اتصال را وارد کرده اید.

اگر همه نیازمندی ها فراهم شده باشد، با کلیک بر روی دکمه Dial اتصال برقرار می شود. وضعیت خط به شما موفقیت اتصال را نشان می دهد و با استفاده از دکمه Disconnect می توان به اتصال خاتمه داد. برای Ping کردن بین PC و مسیریاب باید دقت نمود تا همه تنظیمات IP مربوطه به طور دستی انجام شود.



ابزار Terminal:

رایانه متصل به یک مسیریاب یا سوئیچ از طریق اتصال کنسول (پورت RS 232) از برنامه Terminal برای دسترسی به CLI دستگاه مورد نظر استفاده می کند. در برگه Desktop روی آیکن Terminal کلیک نموده تا این ابزار باز شود. پارامترهای مناسب را برای بخش کنسول تنظیم و سپس Ok را کلیک کنید تا پنجره Terminal با CLI دستگاه راه دور باز شود.



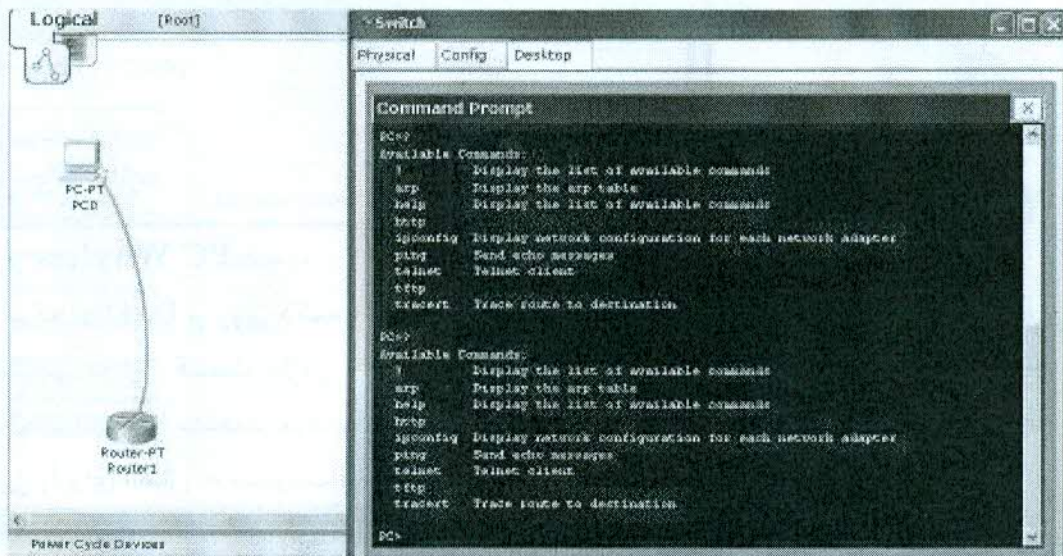
ابزار خط فرمان:

در برگه Desktop بر روی دکمه Command Prompt کلیک تا خط فرمان باز شود. در خط فرمان شما می دستورات زیر را صادر کنید:



✓ فصل دوم: شبیه سازی شبکه توسط نرم افزار Packet Tracer

- ?
- arp
- help
- ipconfig
- netstat
- ping
- telnet
- tracert

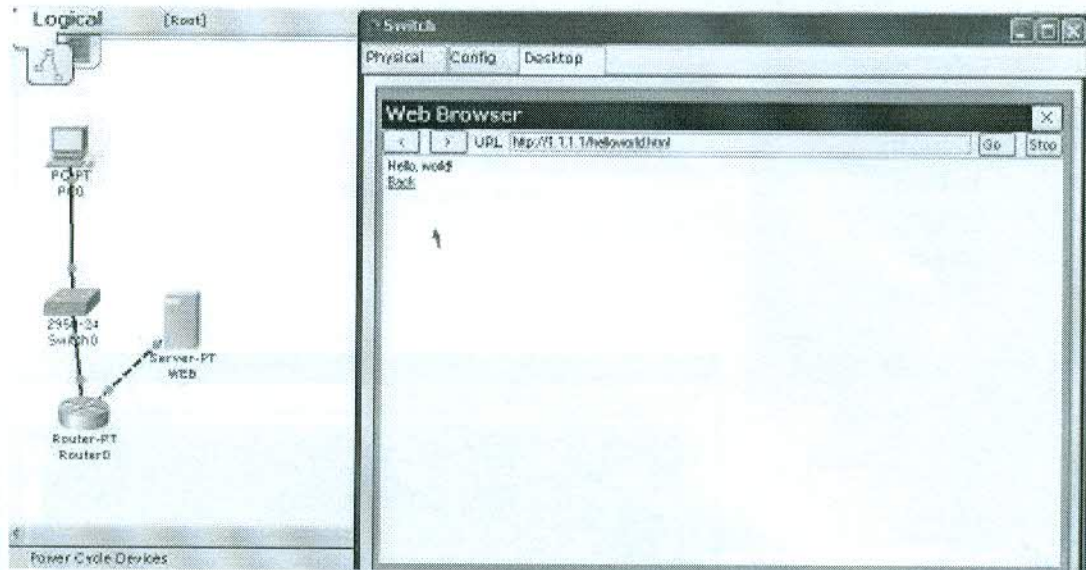


ابزار مرورگر وب:

در برگه Desktop با کلیک روی دکمه Web Browser مرورگر وب را باز نمایید. مرورگر وب امکان دسترسی به پیکربندی های وب سرور Linksys را می دهد. اگر PC مستقیم یا غیرمستقیم به سرور با سرویس فعال HTTP متصل باشد، می توانید نام دامنه یا آدرس IP آن را برای دسترسی به وب سایت سرور وارد کنید. اگر رایانه به مسیریاب بی سیم Linksys WRT300N متصل باشد، می توانید آدرس IP مسیریاب را برای دسترسی به پیکربندی های وب آن وارد کنید. که در این حالت یک اعلان ورود نام کاربری و کلمه عبور ظاهر می شود (به طور پیش فرض هر دو admin است)

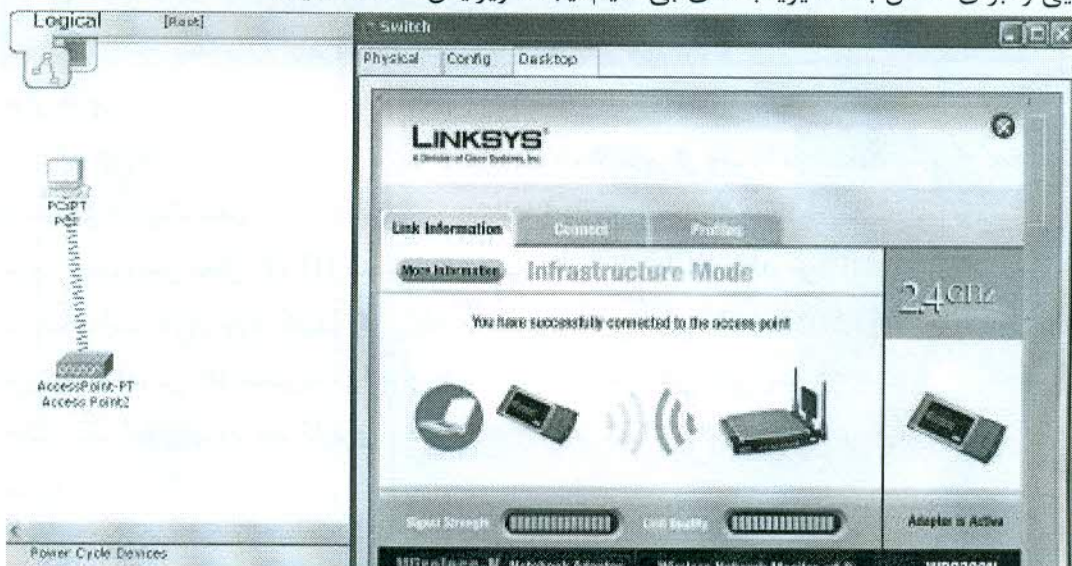


✓ فصل دوم: شبیه سازی شبکه توسط نرم افزار Packet Tracer



ابزار Wireless PC:

در برگه Desktop بر روی دکمه PC Wireless کلیک تا نرم افزار کلاینت بی سیم باز شود. برای دسترسی به این قسمت ماژول Linksys-WMP300N مورد نیاز است. در این قسمت می توان اطلاعات اتصال را مشاهده نمود. به هر شبکه بیسیم موجود در محدوده خود متصل شوید و پروفایل هایی را برای اتصال به مسیریاب های بی سیم ایجاد/ ویرایش/ حذف کنید.

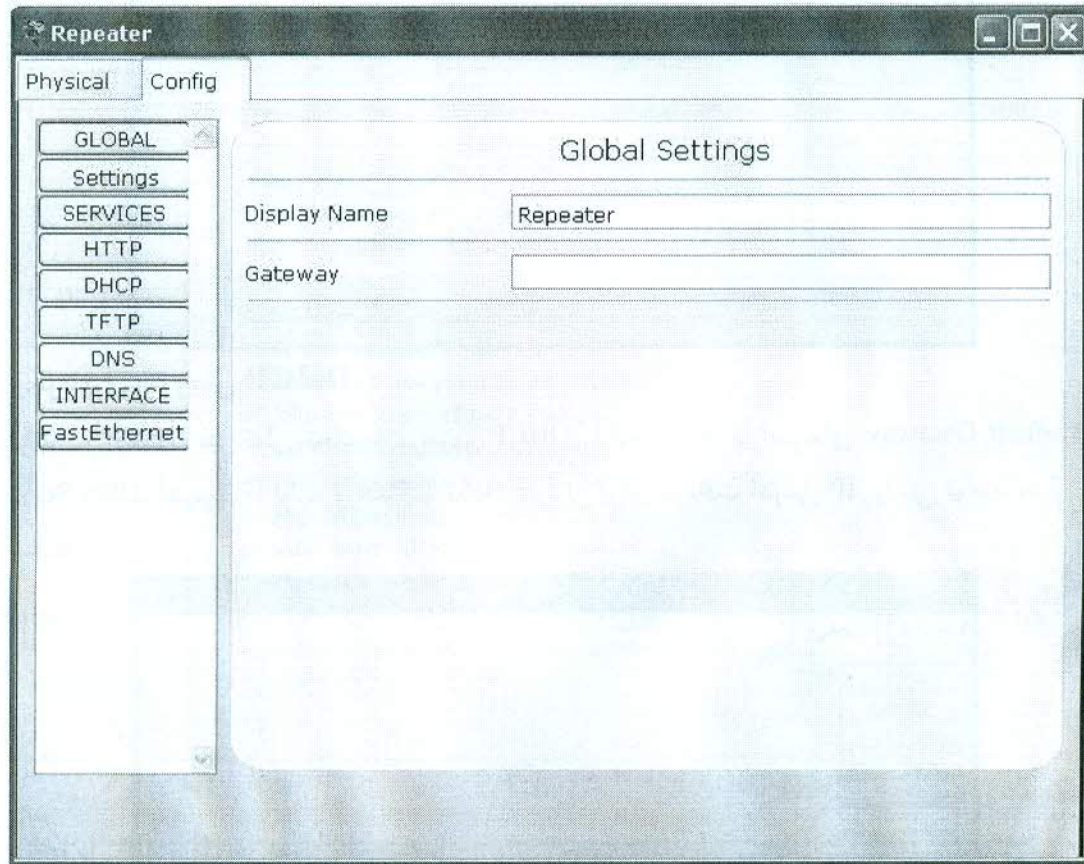




✓ فصل دوم: شبیه سازی شبکه توسط نرم افزار Packet Tracer

پیکربندی سرورها

در برگه Config سه سطح پیکربندی global ، services و interface وجود دارد. برای پیکربندی در سطح global دکمه GLOBAL را کلیک کنید تا settings نمایش داده شود. برای پیکربندی سرویس ها بر روی دکمه SERVICES برای پیکربندی واسط ها بر روی دکمه INTERFACE کلیک کنید.

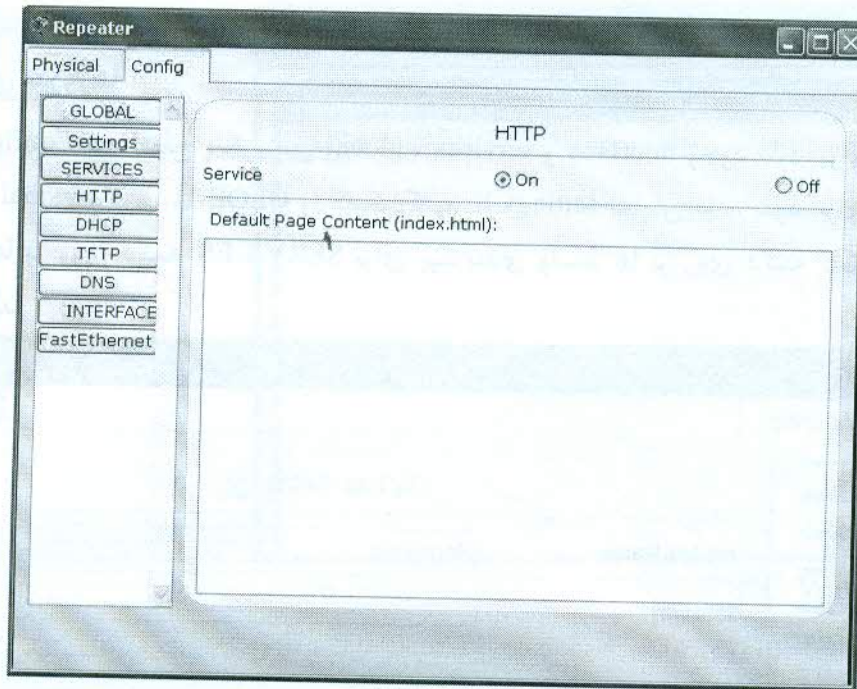


تنظیمات Global:

در تنظیمات global می توان نام و Gateway را تنظیم نمود.

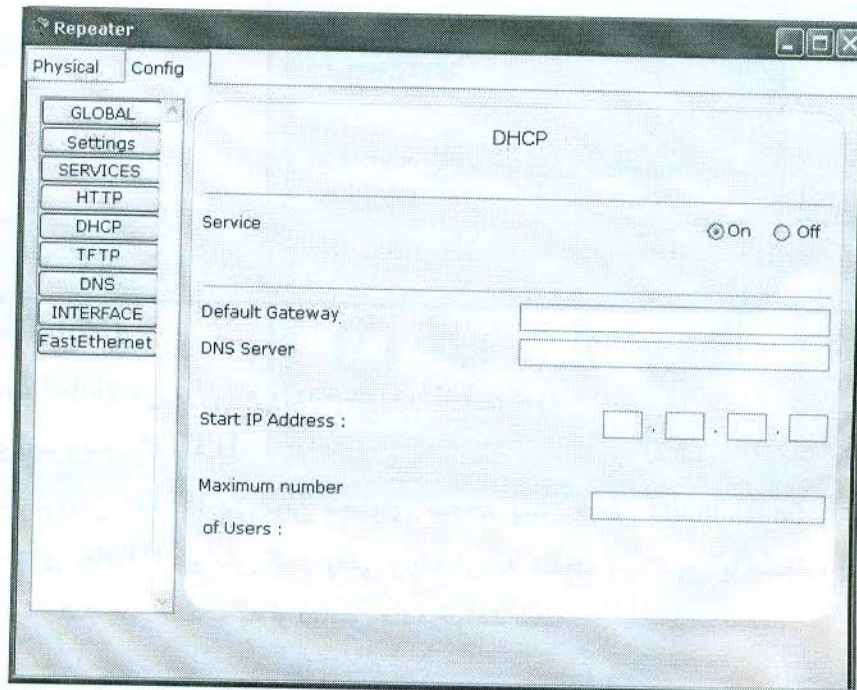
پیکربندی سرویس HTTP:

در قسمت سرویس HTTP می توان محتوای صفحه پیش فرض (index.html) را با استفاده از برخی تگ های HTML ویرایش کرد. وقتی رایانه ای به صفحه وب سرور با استفاده از مرورگر وب دسترسی پیدا کند، این صفحه به او نمایش داده خواهد شد.



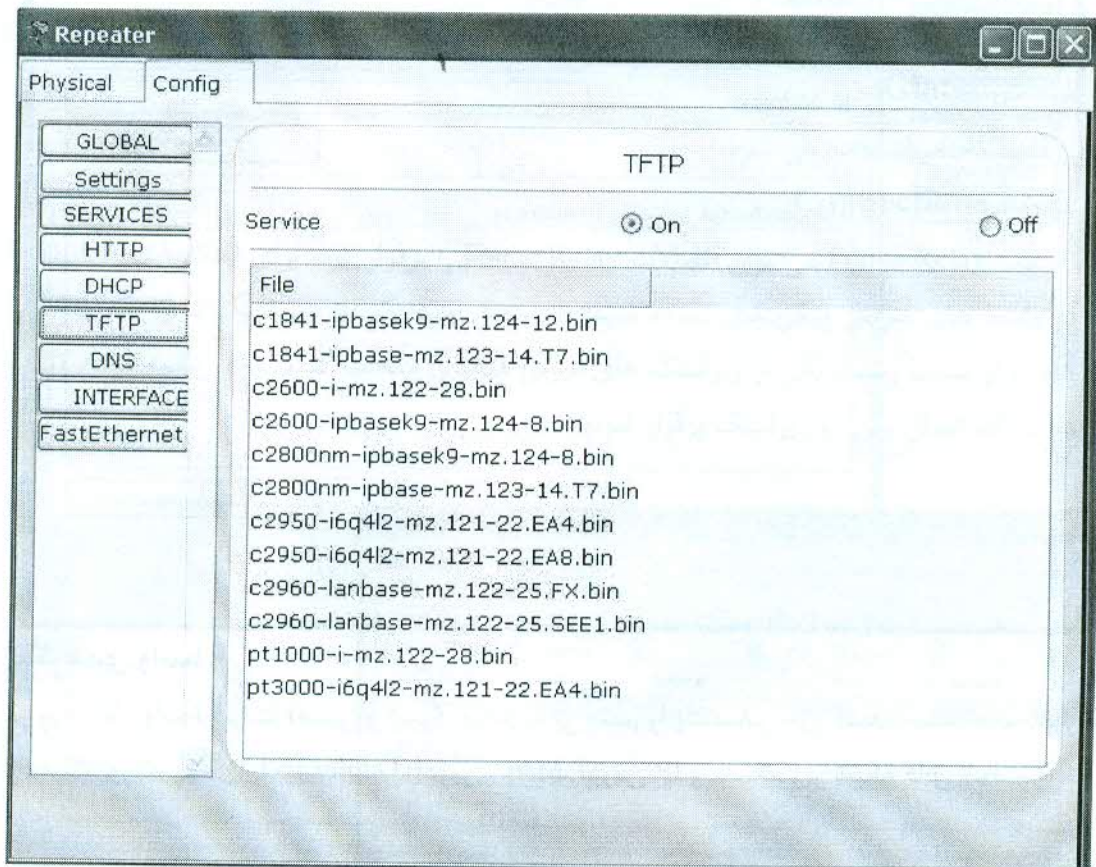
پیکربندی سرویس DHCP:

در برگه DHCP می توان تنظیمات سرور DHCP را انجام داد. پارامترهای Default Gateway ، DNS Server، آدرس IP اولیه و حداکثر تعداد کاربران برای دریافت آدرس IP را می توانید ویرایش نمایید.



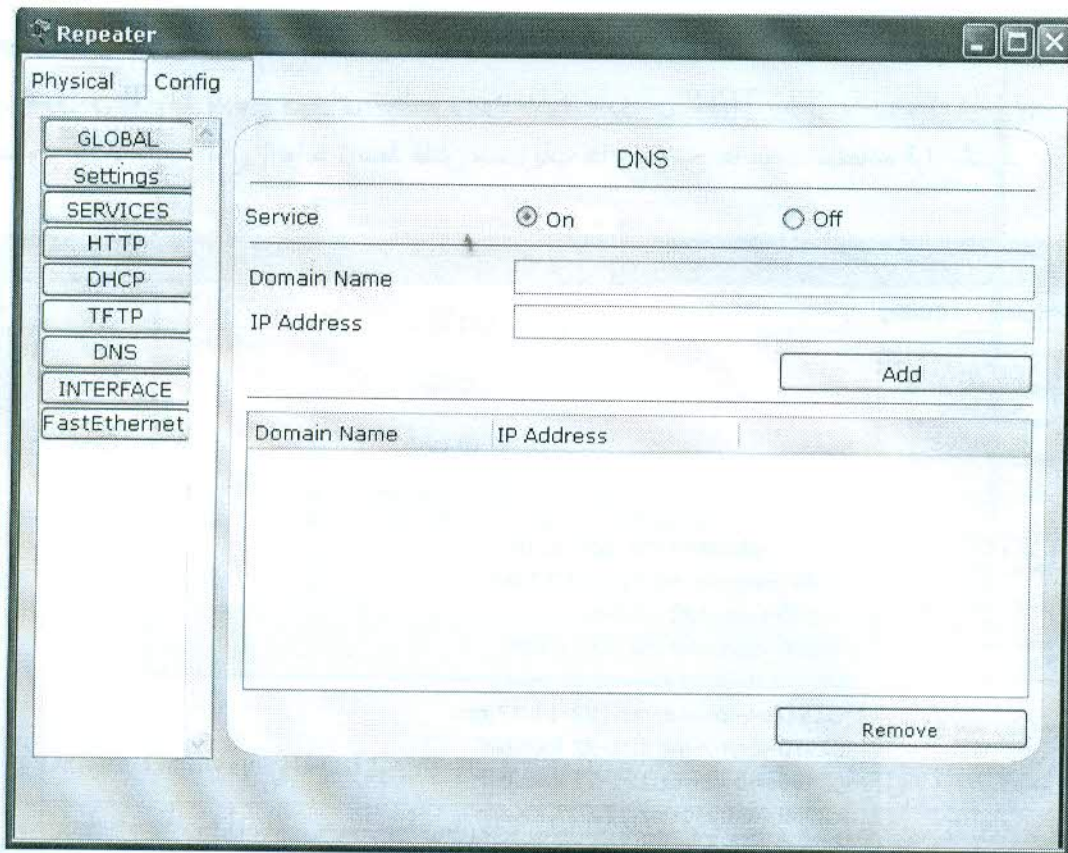
پیکربندی سرویس TFTP:

در سرویس TFTP پارامتری برای تنظیم وجود ندارد. سرویس TFTP شامل یک پایگاه داده ثابت از تصاویر IOS است که می تواند توسط فلش مسیریاب ها و سوئیچ ها مورد استفاده قرار بگیرد.



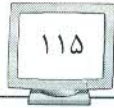
پیکربندی سرویس DNS:

در پیکربندی سرویس DNS می توان DNS سرور را برای ترجمه نام دامنه به آدرس IP راه اندازی کرد. برای این کار نام دامنه را در Domain Name و آدرس IP آن را در IP Address وارد و سپس دکمه Add را کلیک نمایید. برای حذف هر آیتم از DNS از دکمه Remove استفاده می شود.



پیگر بندی واسط:

سرورها یک واسط اترنت (مسی و فیبر)، مودم یا بی سیم را پشتیبانی می کنند. بسته به نوع پورت وضعیت پورت، پهنای باند، Duplex، آدرس MAC، آدرس IP و ماسک زیر شبکه قابل تنظیم است.



پیکربندی ابر (cloud)

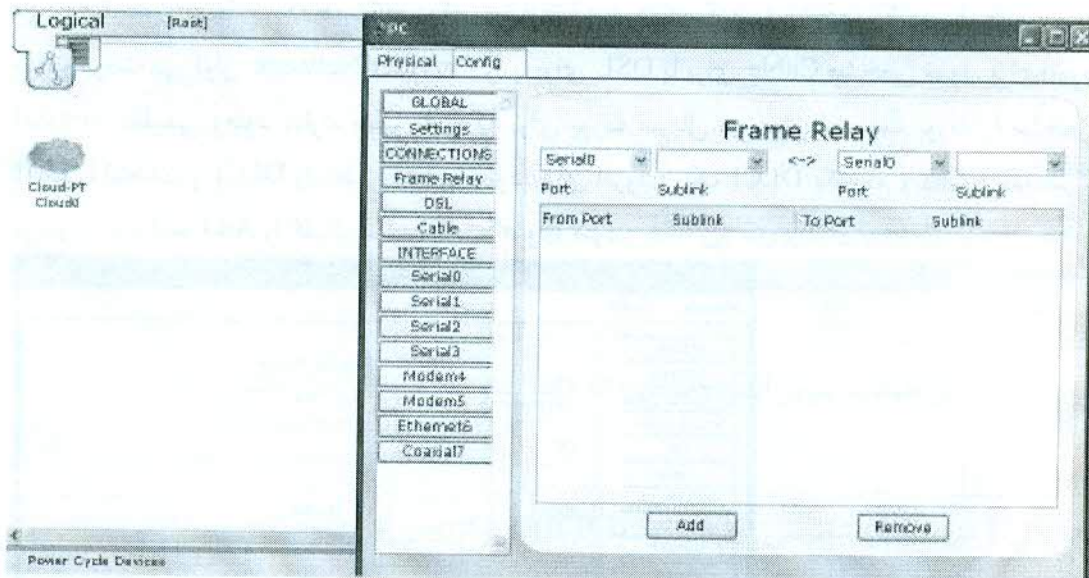
برگه Config سه سطح تنظیمات global, connections و interface را فراهم می کند که برای پیکربندی هر سطح باید بر روی دکمه های GLOBAL, CONNECTIONS یا INTERFACE کلیک کنید.

تنظیمات Global:

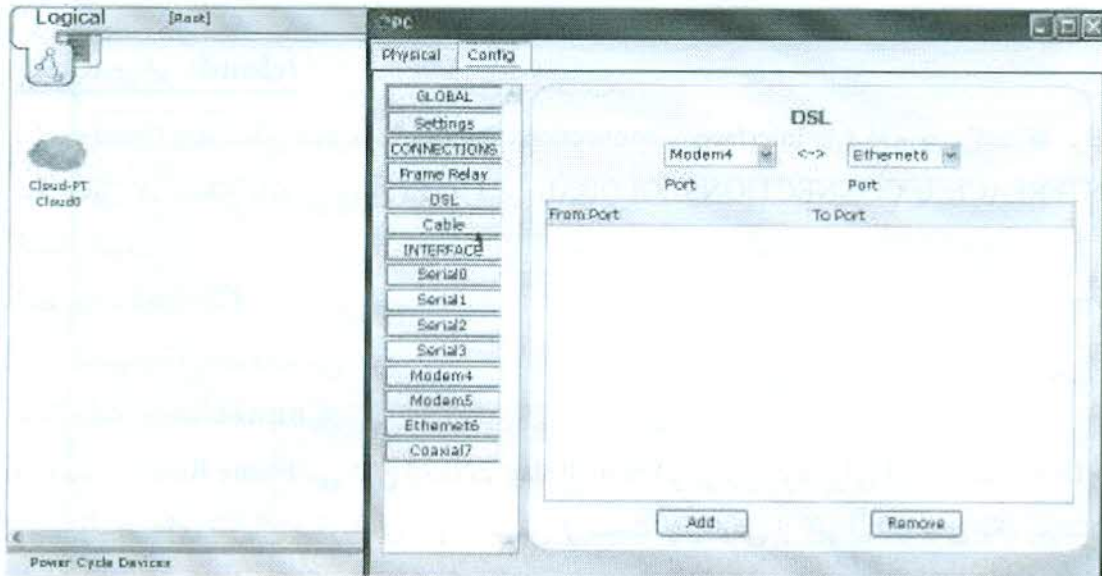
برای تغییر نام ابر استفاده می شود.

تنظیمات Connections:

در قسمت Frame Relay می توان اتصالات Frame Relay را برقرار کرد. برای اینکار ابتدا DLCI ها را در واسط های سریال پیکربندی نموده سپس از سمت چپ یکی از زیر لینک های یک پورت را انتخاب و از سمت راست یکی از زیرلینک های پورتی دیگر را انتخاب کنید. روی دکمه Add کلیک کنید تا یک اتصال بین دو زیرلینک برقرار شود.

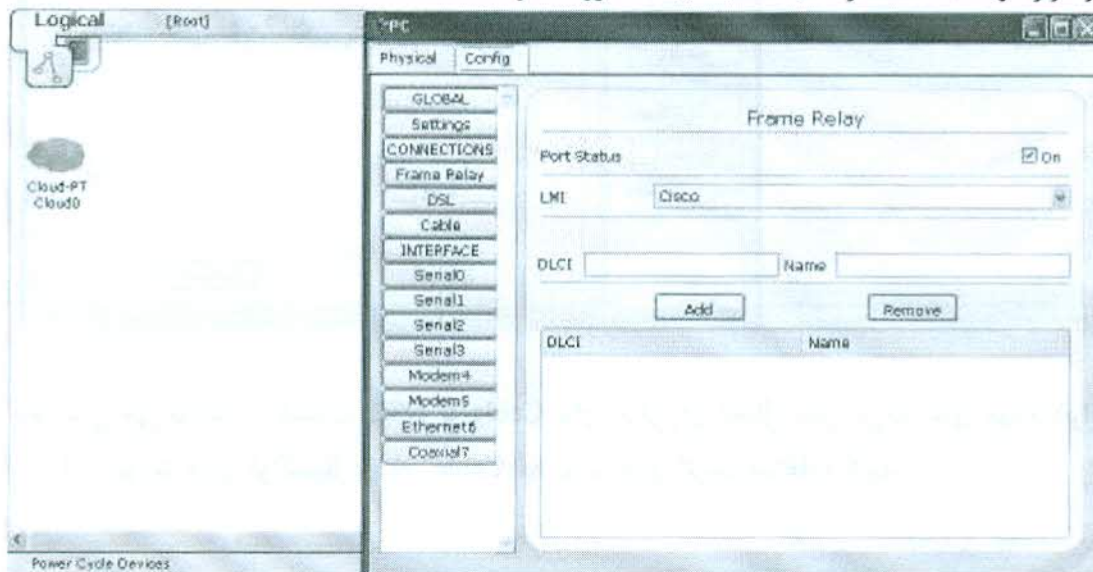


همچنین می توانید از قسمت DSL یا Cable برای برقراری اتصال بین پورت های مودم (برای DSL) یا پورت های کواکسیال (برای Cable) به پورت های اترنت استفاده کنید.



پیگر بندی Interface:

ابر می تواند ۴ نوع واسط مودم، اترنت، کوکسیال و سریال را پشتیبانی کند. برای پورت مودم می توانید شماره تلفنی که دستگاه دیگر بتواند از آن استفاده کند را مشخص کنید. همچنین برای پورت اترنت می توان Provider Network را یا برای DSL یا برای Cable مشخص نمود. برای پورت coaxial تنظیمی وجود ندارد. ضمن این که برای پورت سریال می توان وضعیت پورت را مشخص، LMI را انتخاب و DLCI واسط را تنظیم نمود. برای افزودن یک DLCI یک نام و شماره منحصر به فرد وارد و دکمه Add را کلیک تا به لیست افزوده شود.





✓ فصل دوم: شبیه سازی شبکه توسط نرم افزار Packet Tracer

پیکربندی دستگاه های دیگر

تنظیمات پیکربندی برای سایر دستگاه ها نسبتا ساده است. نام آنها را می توان تغییر داده و یا تنظیمات پایه را برای هر واسط انجام داد.

پل ها

پل مثل سوئیچ دو پورت داشته و فاقد VLAN و trunk می باشد.

تکرار کننده

وسیله ای ساده با دو پورت است که سیگنال دریافت شده در یک پورت را از پورت دیگر مجددا ارسال می کند. تنظیمات پورت این وسیله قابل تغییر نیست.

هاب

مانند تکرار کننده دارای چند پورت است و سیگنال دریافتی را به همه پورت های دیگر ارسال می کند.

نقطه دسترسی

همچون تکرار کننده با یک پورت بی سیم و یک پورت اترنت است.

چاپگر

تنظیمات چاپگر همانند سرور است بجز این که فاقد سرویس های آن می باشد.

IP Phone

IP Phone گزینه قابل تنظیمی ندارد و توسط DHCP پیکربندی می شود.

DSL Modem

این مودم گزینه قابل تنظیمی ندارد.

Cable Modem

این مودم گزینه قابل تنظیمی ندارد.