

شبیه سازی شبکه های کامپیوتری

توسط نرم افزار Packet Tracer

به همراه آموزش مفاهیم کاربردی شبکه



تالیف و ترجمه

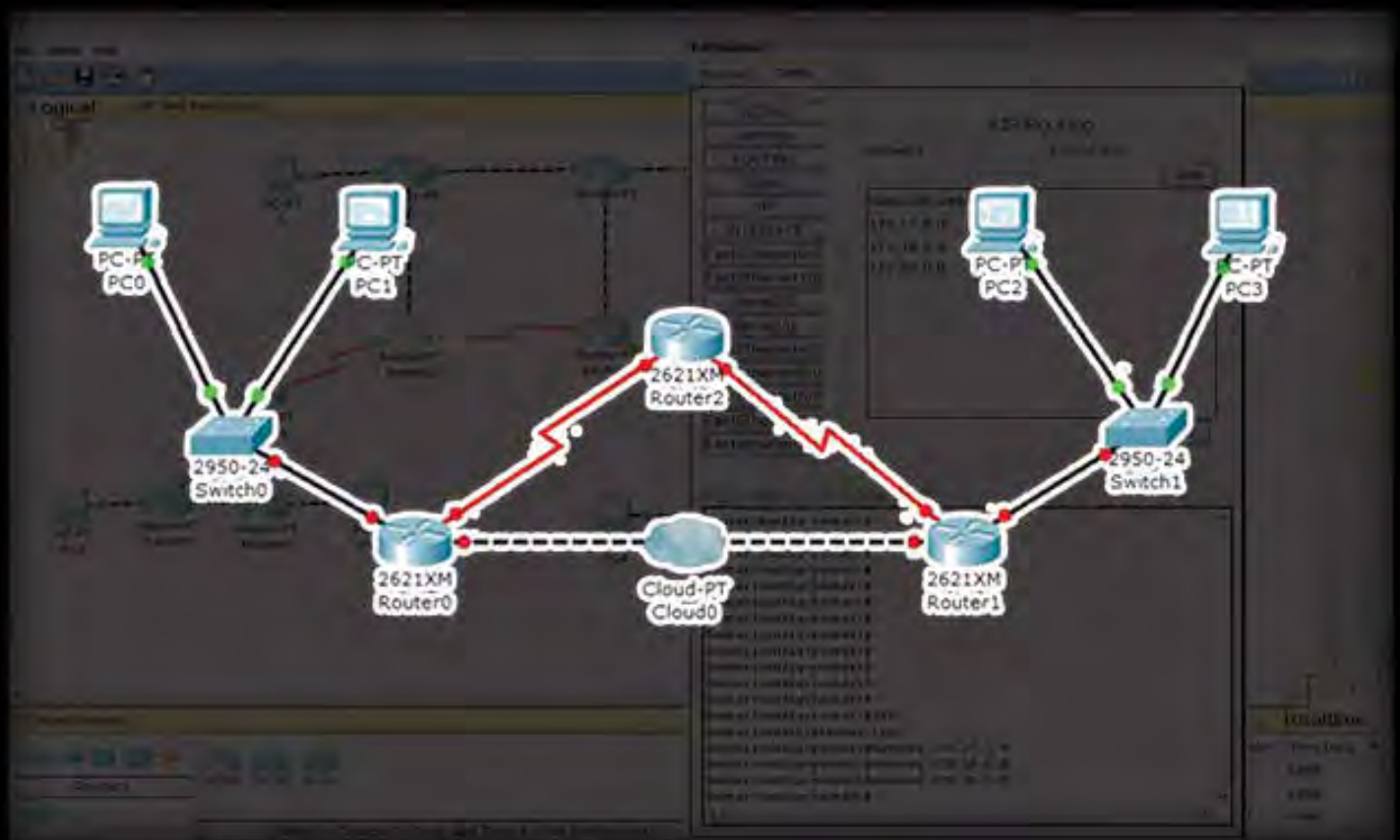
مرتضی سرگلزایی جوان

احمد بختیاری شهری

دانشگاه صنعتی امیرکبیر

دانشگاه سیستان و بلوچستان

Network Simulation using Packet Tracer



Written by:

Ahmad Bakhtiyari Shahri

University of Sistan and Balouchistan

Morteza Sargolzaei Javan

Amirkabir University of Technology

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	احمد بختیاری شهری
دانشگاه صنعتی امیرکبیر	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 پیام 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 متغیر ها
۱۷۹	اختصاص متغیر ها
۱۷۹	نحوه افزودن متغیر ها به آیتم های ارزیابی
۱۷۹	انواع آیتم های ارزیابی



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

۱۹۰	مسیر یاب 1841
۱۹۱	مسیر یاب 2 20XM
۱۹۴	مسیر یاب 2 21XM
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



۲۷۶	ضمیمه ۷) آزمایشگاه (CCNA).....
۲۷۶	۱۲.۱.۵-۱-۱ CCNA1) ایجاد یک شبکه PEER TO PEER
۲۷۸	A) ۱۳.۱-۵-۱-۱ CCNA1) ایجاد یک شبکه مبتنی بر هاب
۲۸۰	B) ۱۳.۱-۵-۱-۱ CCNA1) ایجاد یک شبکه مبتنی بر سوئیچ
۲۸۲	۱.۷-۵-۱-۱-۵ CCNA1) تکرار کننده ها و هاب ها
۲۸۴	۱.۱-۵-۱-۱ CCNA1) تکرار کننده
۲۸۶	۸.۱-۵-۱-۱ CCNA1) بی سیم
۲۸۷	۱۰.۱-۵-۱-۱-۹ CCNA1) پل ها و سوئیچ ها
۲۸۹	A) ۳.۲-۵-۱-۱ CCNA1) اتصال واسط های مسیریاب ها
۲۹۰	۲.۴-۴-۲-۲ CCNA2) رفع اشکال مربوط به آدرس IP
۲۹۲	۴.۱-۳-۲-۱ CCNA2) پیکربندی مسیرهای پیشفرض و استاتیک
۲۹۴	۲.۳-۲-۱ CCNA2) پیکربندی مسیریابی
۲۹۵	۲.۲-۲-۱-۷ CCNA2) پیکربندی RIP
۲۹۷	۹.۲-۲-۱-۷ CCNA2) 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.....

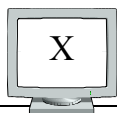
به نام او که زیباست و زیبایی را دوست دارد

✍ 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 بپردازند.

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.



کلمه 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 سؤالی 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 شبکه ها عبارتند از:

- امکان ارتباط کامپیوترها در نقاط مختلف و حذف مسافت های فیزیکی
- امکان تبادل اطلاعات و منابع برای بهره برداری مشترک با اطمینان بالاتر
- افزایش کارائی، سرعت و دقت در تبادل اطلاعات
- امکان مدیریت متمرکز اطلاعات و اعمال سیاست های امنیتی

شبکه ها از نظر نوع ارتباط به دو دسته تقسیم می‌شوند:

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

همچنین شبکه ها را از لحاظ گستردگی و وسعت نیز می توان به ترتیب زیر تقسیم نمود:

الف- شبکه های محلی^۳ یا LAN

ب- شبکه های بین شهری^۴ یا MAN

ج- شبکه های گسترده^۵ یا WAN

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

^۱ - Peer- to – Peer

^۲ - Client /Server

^۳ - Local Area Network

^۴ - Metropolitan Area Network

^۵ - Wide Area Network

^۶ -Intranet

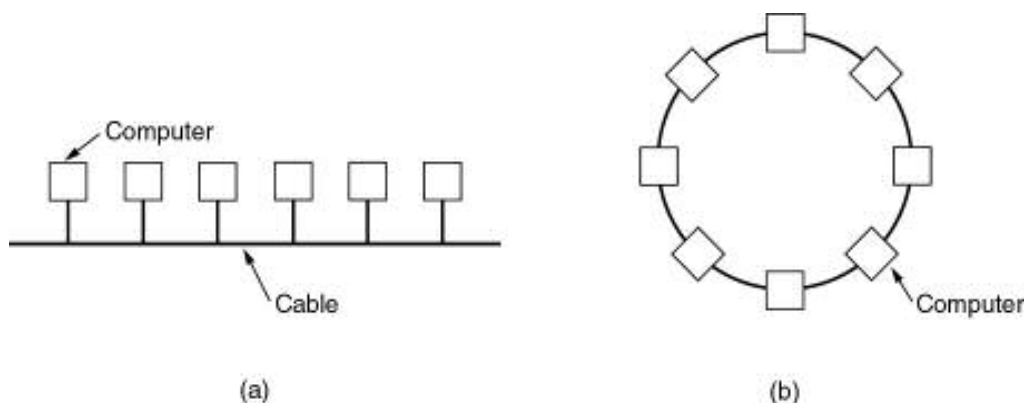
^۷ -Extranet



✓ فصل اول: آشنایی با مفاهیم کاربردی شبکه

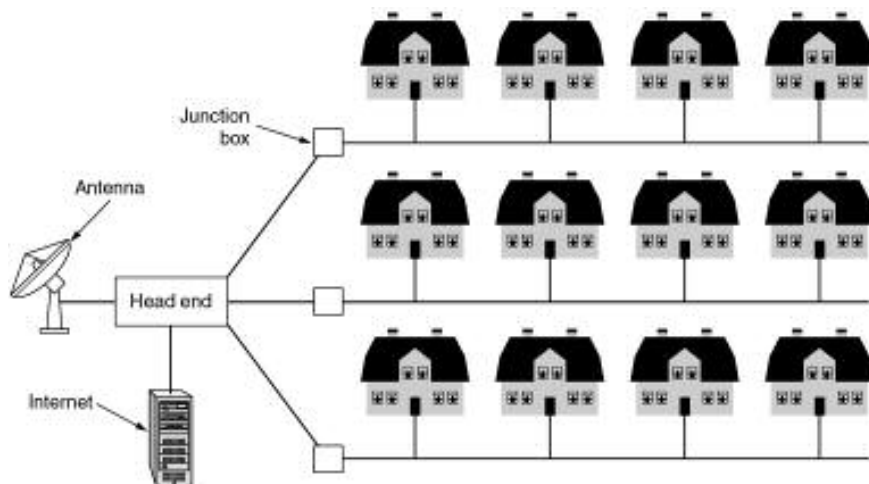
Interprocessor distance	Processors located in same	Example
1 m	Square meter	Personal area network
10 m	Room	
100 m	Building	Local area network
1 km	Campus	
10 km	City	Metropolitan area network
100 km	Country	Wide area network
1000 km	Continent	
10,000 km	Planet	The Internet

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.



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.



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 SPX / IPX.

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 کواکسیال، 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 کواکسیال 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.

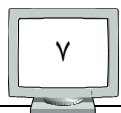


شکل ۷: کابل هم محور CAT5

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 زوج ها در کابل های 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 می شود بنابراین نویز حذف می شود.

در شبکه هایی با نام اترنت سریع، دو نوع کابل به چشم می خورد:

100Base TX: یعنی شبکه ای 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 می باشد)، 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 می شوند.

شاخص کیفیت کابل CAT5 میزان تابیده بودن کابل ها به هم می باشد هرچه میزان تابیده بودن بیشتر باشد کابل از کیفیت بالاتری برخوردار می باشد. در کابل های 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 سیم ها 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 سیگنال ها 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 / قهوه ای
بدون استفاده	8	8	قهوه ای

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	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

^۱ - Patch Panel
^۲ - Keystone
^۳ - Rack
^۴ - Patch Cord
^۵ - Outlet



✓ فصل اول: آشنایی با مفاهیم کاربردی شبکه

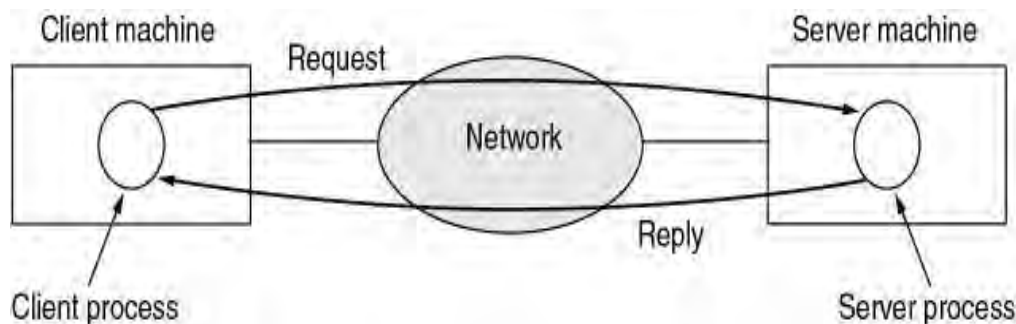
معمولا روی جعبه ها شماره معادل روی پچ پانل نوشته می شود تا رفع خرابی به سهولت انجام پذیرد. مدیر شبکه باید همیشه یک جدول از شماره جعبه ها و موقعیت آنها در ساختمان داشته باشد؛ تا به آسانی بتواند ارتباط فیزیکی یک کاربر مشخص را قطع و وصل نماید و یا در رفع خرابی وی اقدام نماید.

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.

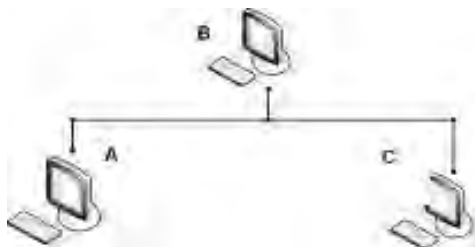
۱- پروتکل NetBEUI

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 مثلاً:
- الف: وقتی می خواهیم اصطلاحاً 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

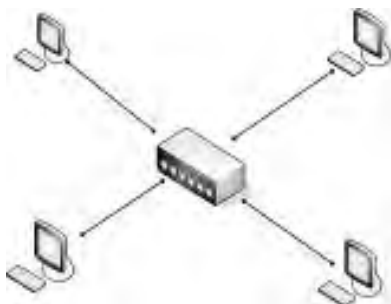
در شبکه زیر اگر توزیع کننده، هاب باشد و ماشینی بسته ای را برای ماشین دیگر، به شکل عمومی^۴ ارسال کند، همه ماشین ها آن را دریافت می کنند. اما اگر توزیع کننده سوئیچ باشد فقط ماشین مقصد آن را دریافت می کند.

^۱ - Very Simple Configuration

^۲ - Broadcast

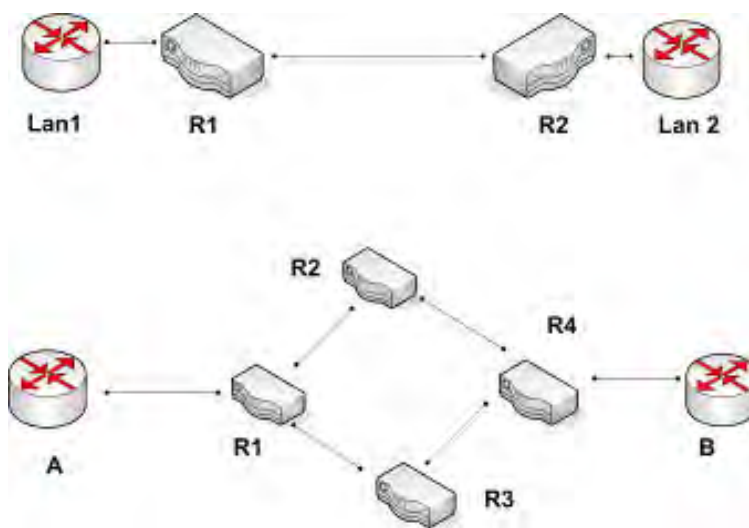
^۳ - Unicast

^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

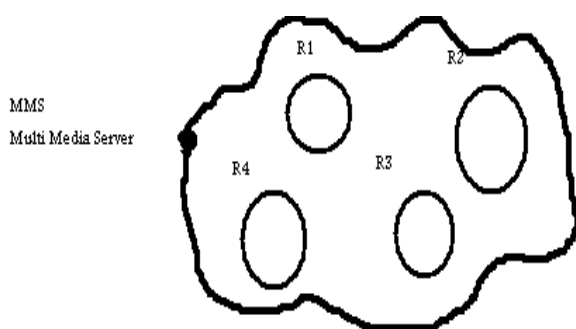
→ SPX ۲- با تضمین Connection Oriented سفارشی

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 پیکربندی پیچیده‌ای داشته و سرویس‌های فراوان و متنوعی را فراهم می‌کند. یعنی پیچیدگی آن به تنوع سرویس‌هایش بر می‌گردد. این پروتکل در سیستم عامل یونیکس متولد شد ولی در همه سیستم عامل‌ها استفاده می‌شود. در شبکه‌های کوچک قابلیت پیکربندی اتوماتیک و در شبکه‌های بزرگ قابلیت مسیریابی را نیز دارد. علاوه بر خصوصیات پروتکل‌های قبلی، قابلیت ارسال بسته به گروهی خاص^۱ را نیز دارد.



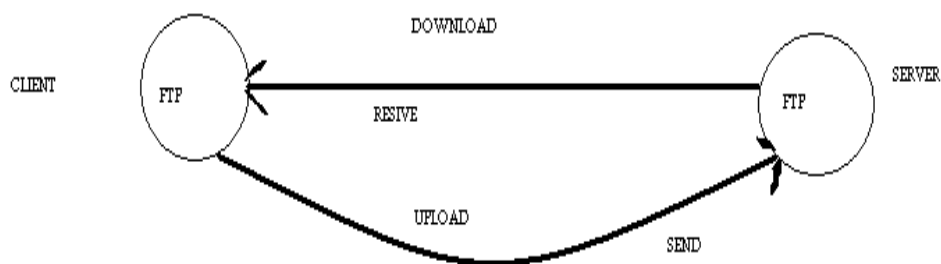
شکل ۱۵: استفاده از Multicast برای ارسال پیام

به عنوان مثال در شبکه فوق بسته‌ای 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 می‌رود. در این حالت می‌توان از قابلیت ارسال بسته به گروهی خاص استفاده نمود. باید اذعان داشت که TCP/IP مجموعه‌ای از سرویس‌هاست، لذا باید فلسفه و هدف از اجرای شبکه را دانست به عنوان مثال اهداف زیر را می‌توان در نظر داشت:

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

سرویس‌های TCP/IP

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



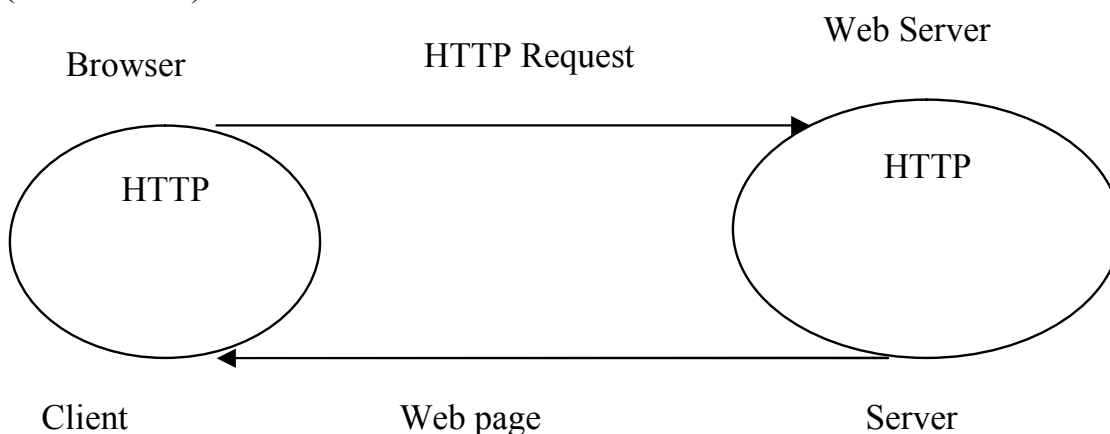
شکل ۱۶: نحوه استفاده از سرویس FTP

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:

- 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

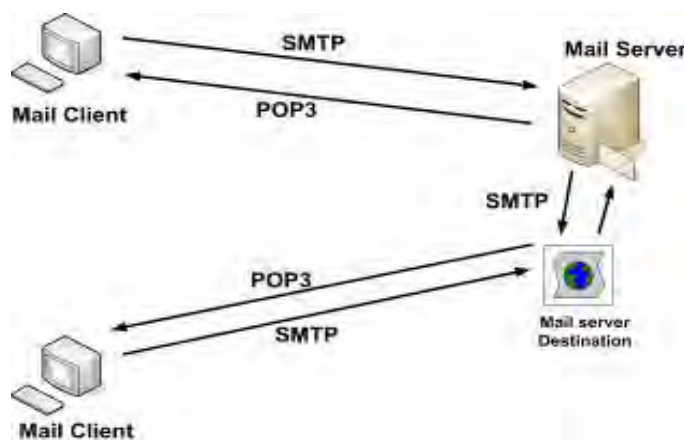
سه پروتکلی معروفی که در ایمیل استفاده می شود به شرح ذیل می باشد:

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.



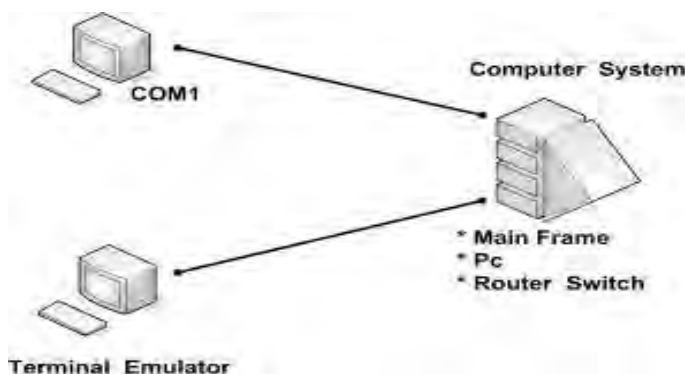
شکل ۱۸: نحوه استفاده از پروتکل های ایمیل در شبکه

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:

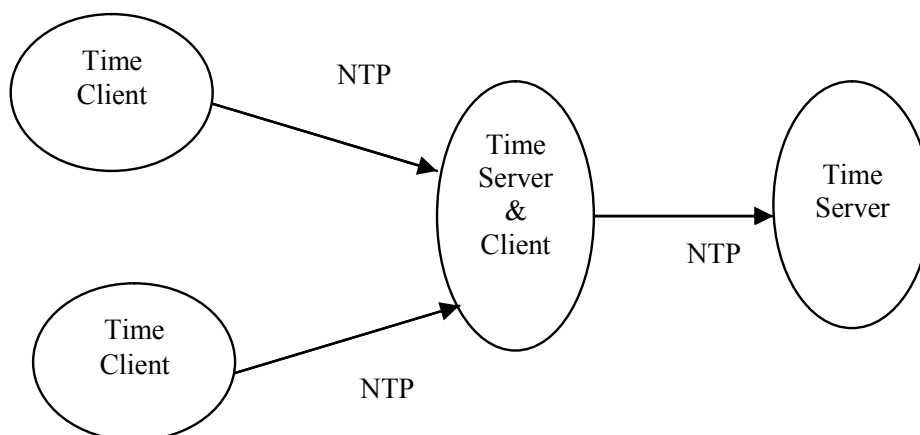
Cisco Works - What's Up Gold - Hp Open View - Solar Winds

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 کامپیوتر ها 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 بایتی 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 بایتی است به IPNG یا IPV6 معروف است.



✓ فصل اول: آشنایی با مفاهیم کاربردی شبکه

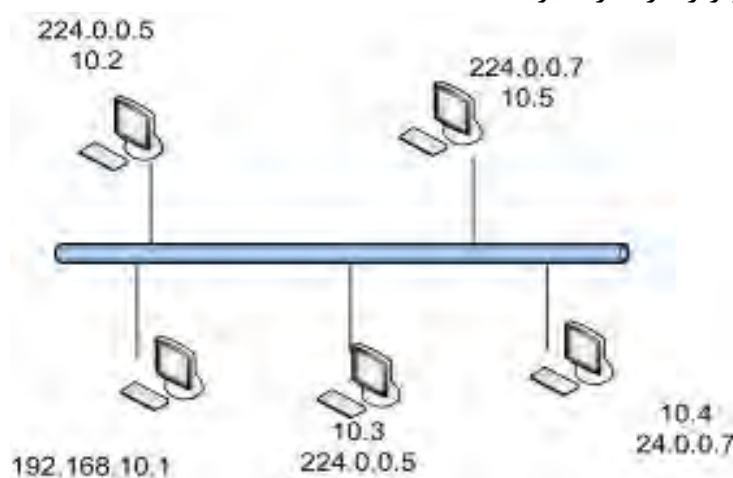
هر IP Address از دو قسمت Network ID و Host ID تشکیل شده است. این آدرس ها به کلاس هایی به ترتیب زیر طبقه بندی شده اند:

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 (×) در جدول زیر دقت نمائید:

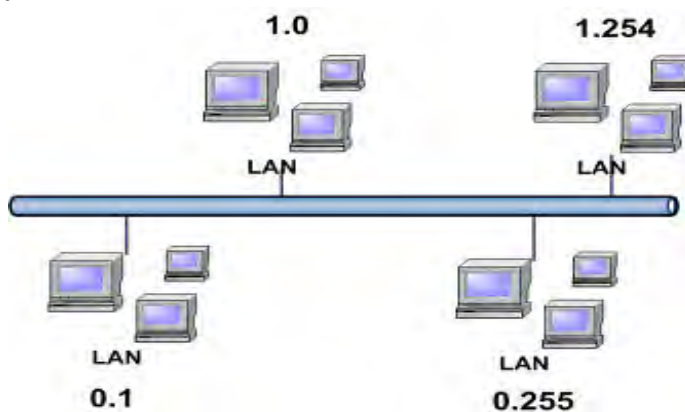
192.168.0.1	■	18.255.0.255	■	10.0.0.0	×
192.168.10.0	×	192.168.10.255	×	172.16.255.255	×
130.145.0.0	×	172.16.255.255	×	172.16.255.0	■
10.0.0.0	×	10.255.255.255	×	18.0.0.255	■
18.0.255.0	■	172.16.0.255	■		

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



✓ فصل اول: آشنایی با مفاهیم کاربردی شبکه

$2^{16} - 2$	در کلاس B حداکثر Host ها	$2^{14} = 16384$	در کلاس B حداکثر Network
$2^{24} - 2$	در کلاس A حداکثر Host ها	126	در کلاس A حداکثر Network
$2^8 - 2$	در کلاس C حداکثر Host ها	2^{21}	در کلاس C حداکثر Network

Subnet mask: فرض کنید شبکه ای ۵۰۰۰ کامپیوتر داشته، لذا از کلاس B به شکل 130.131.X.Y استفاده می گردد. در این صورت تعداد زیادی آدرس از دست می رود. زیرا فقط با ۱۳ بیت می توان ۵۰۰۰ کامپیوتر را آدرس دهی نمود و بقیه بیت ها را به Net ID اضافه و تعداد شبکه ها بیشتری را آدرس دهی کرد. به این نوع آدرس دهی، Classless و به حالت نرمال آن Full Class گفته می شود.

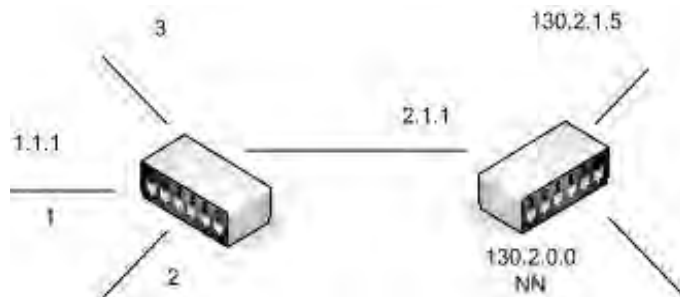
TCP از روی Subnet mask پی می برد که از ۳۲ بیت مربوط به آدرس چند بیت Net ID و چند بیت Host ID است. بدین ترتیب که بیت های صفر آن مربوط به Host ID و بیت های یک آن مربوط به Net ID است.

همواره باید نکات زیر را مورد توجه قرار داد:

- همه بایت های Net ID نمی تواند با هم صفر یا ۲۵۵ شود.
- برای این که کلیه Host ها مستقیماً بتوانند با هم ارتباط برقرار کنند لازم است تا Net ID آنها یکسان باشد.
- IP Address برای هر ماشین باید منحصر به فرد باشد.

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

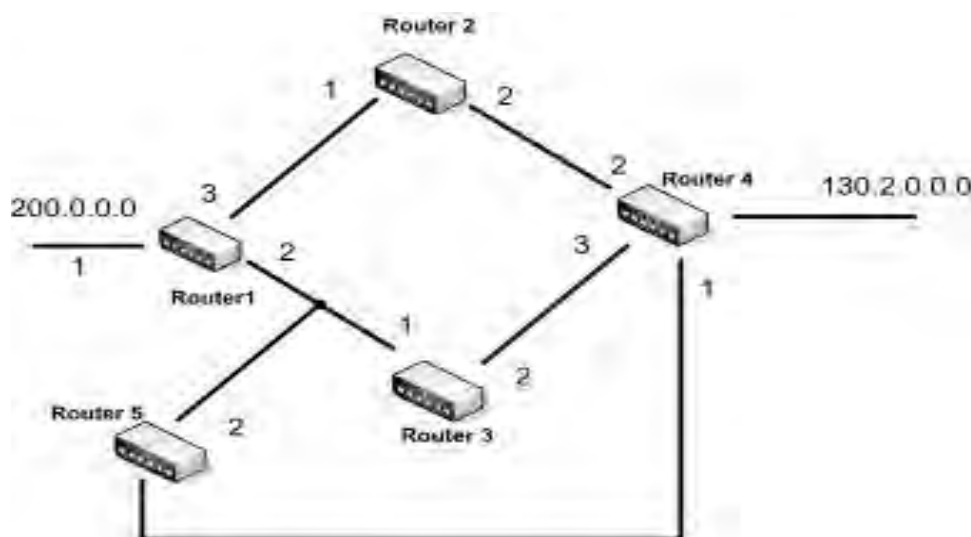
به عنوان مثالی دیگر، شبکه شکل ۲۳ را در نظر بگیرید:

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

ارزش مسیر^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

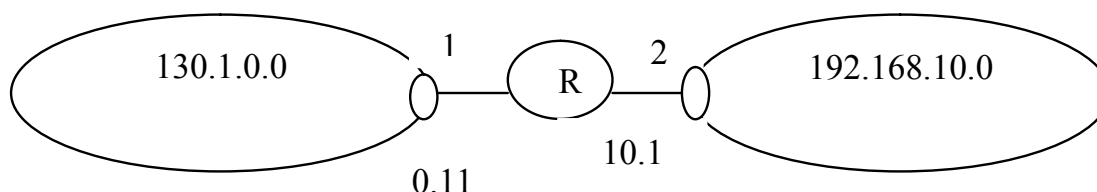
^۲ - metric



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

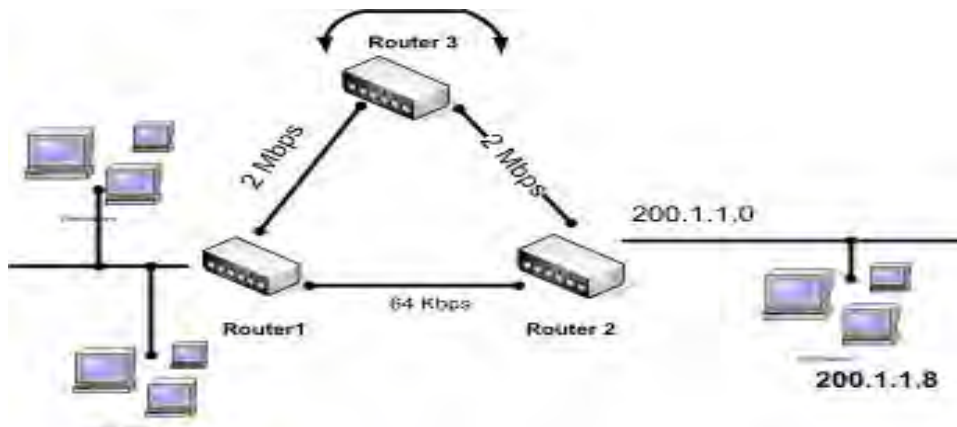
در مثال فوق اگر روتر R5 اضافه شود مسیریابی چگونه انجام می شود؟ در این حالت چون بعد از این که بسته از پورت ۲ خارج گردید، باید مشخص شود که باید از کدام روتر عبور نماید لذا پارامتر دیگری نیز اضافه می شود و آن روتر گیرنده اطلاعات است. همچنین می توان به جای آدرس روتر، IP آنرا داد و می توان به جای شماره پورت، 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 پیام unReachable Destination Host 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

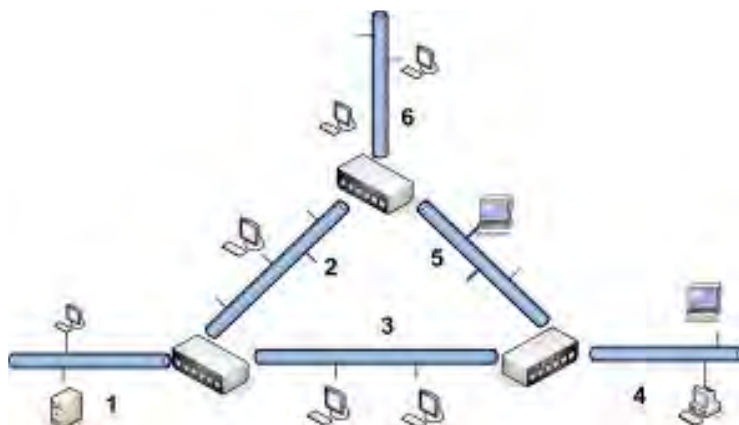
حال اگر در شبکه قبل R3 را نیز داشته و در نظر است بسته ای سریعاً به یک ماشین مشخص به آدرس 200.1.1018 ارسال گردد و مسیر نیز مشخص باشد در این صورت آن را وارد جدول مسیریاب می کنیم.

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.

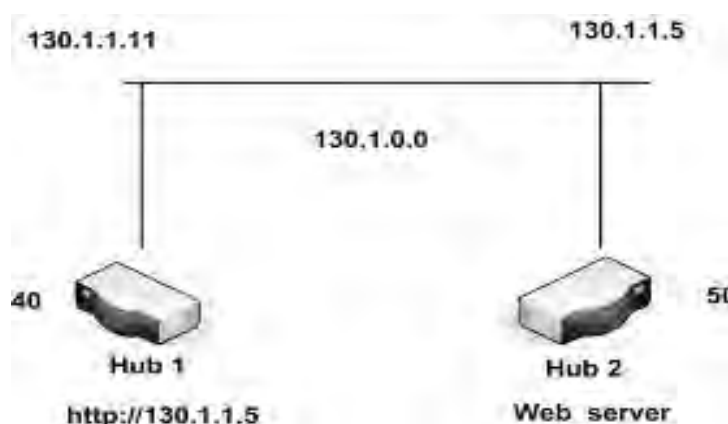
C:\netstat -r

C:\route print



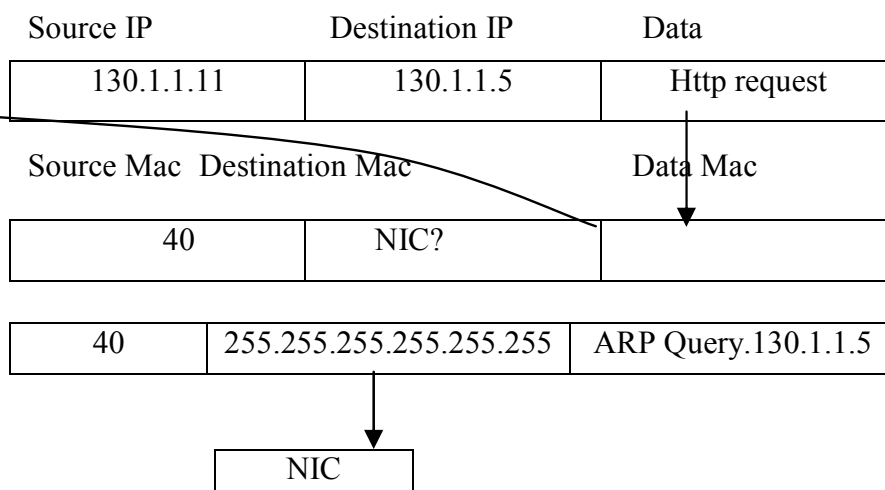
شکل ۲۶: شبکه ای مبتنی بر سوئیچ هایی با قابلیت مسیریابی

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:



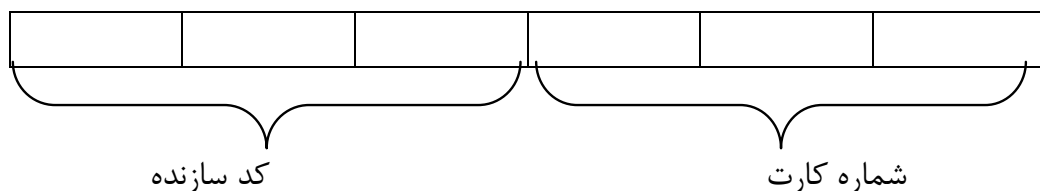
شکل ۲۷: مثالی از ارسال یک بسته TCP/IP

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 جویا 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 3Com 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

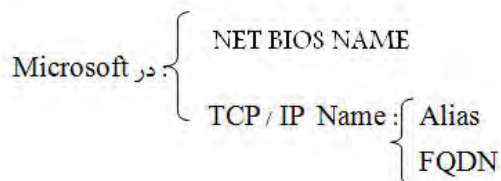
چنانچه می‌خواهید آدرس فیزیکی یک IP مشخص (مثلا 10.10.10.5) را در شبکه محلی خود پیدا کنید ابتدا دستور ذیل را اجرا کرده و سپس دستور قبل را وارد نمایید:

```
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 کلیه 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

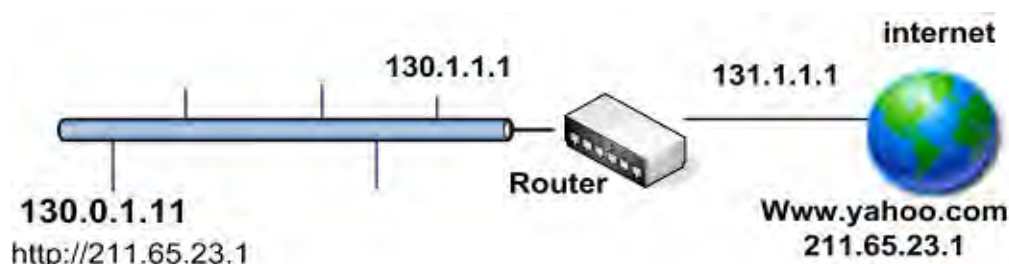
Windows Directory\System32\Drivers\etc\lmhosts

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

.

.

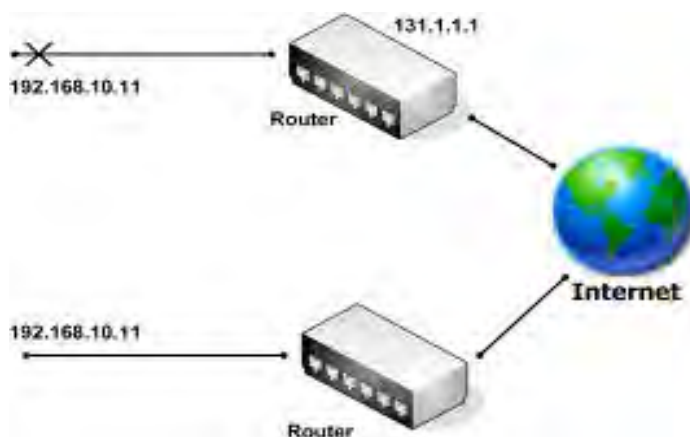
.

.

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:

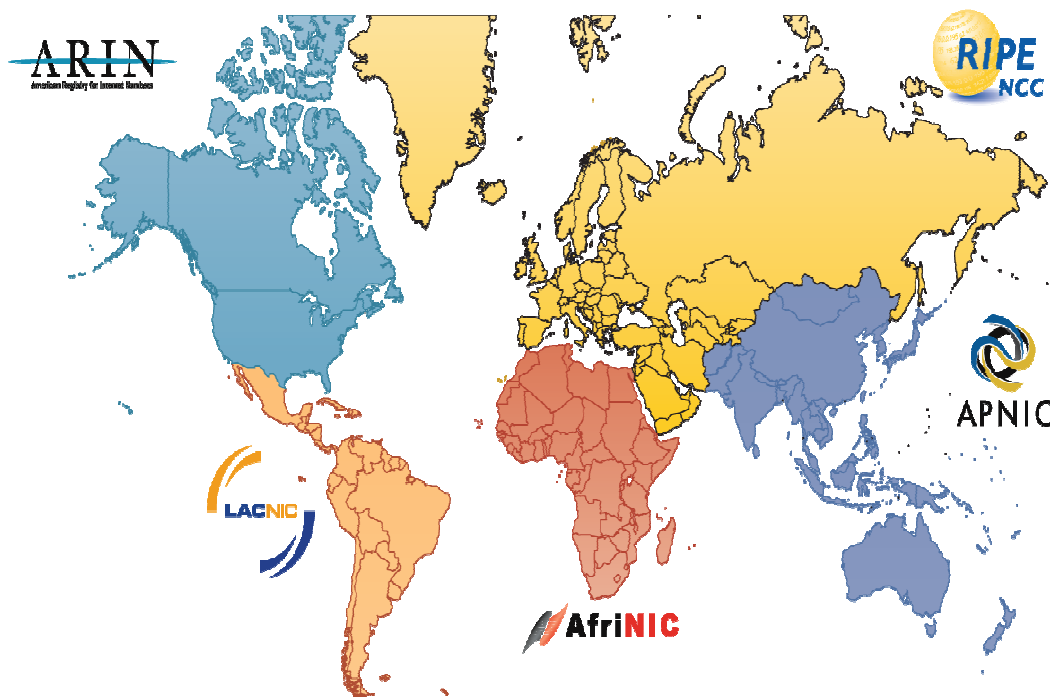
C:\ipconfig

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 ثبت‌کننده منطقه‌ای^۱ RIR نامیده می‌شوند مدیریت می‌شود. این سازمان‌ها که به صورت جغرافیایی عمل می‌کنند در محدوده جغرافیایی خود مسئولیت 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 ثبت‌کننده منطقه‌ای IP در جهان

جهت اطلاع از اینکه یک نشانی IP معتبر واقعاً 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 جغرافیای

DHCP Server مسأله ای دیگر در TCP/ IP

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:

$Ping \begin{bmatrix} name \\ IP \end{bmatrix}$

مثال: Ping 192. 168. 10. 1

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

$\left\{ \begin{array}{l} ping \quad 127.0.0.1 \\ ping \quad local \ Host \end{array} \right\}$

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

$Ping -w \begin{bmatrix} name \\ IP \end{bmatrix}$

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.

$Ping -t \begin{bmatrix} name \\ IP \end{bmatrix}$

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

$ping -n \begin{bmatrix} name \\ IP \end{bmatrix}$

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

$ping -L \begin{bmatrix} name \\ IP \end{bmatrix}$

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:

$Tracert \begin{Bmatrix} Name \\ IP \end{Bmatrix}$

$Tracert -d WWW.Yahoo.com$

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

$arp -a$

$netstat -n$

$netstat -a$

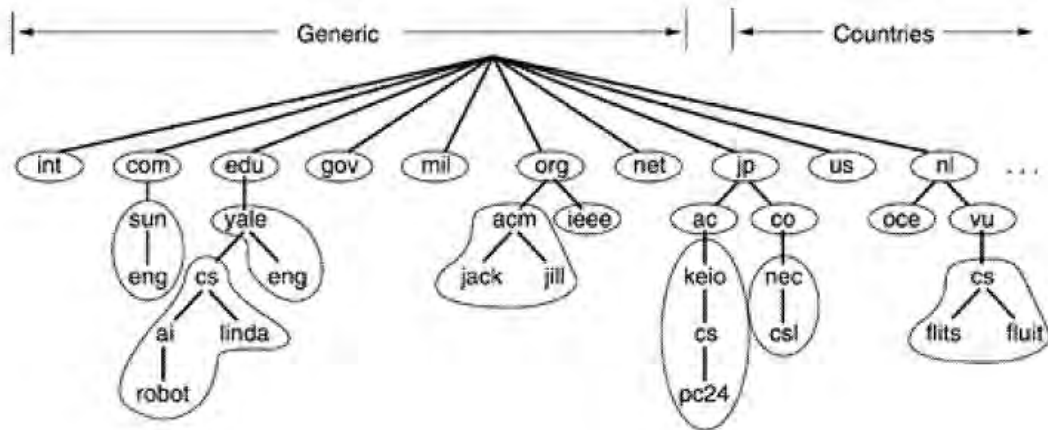
سرویس DNS

همان گونه که در ابتدا بیان گردید DNS¹ 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 عملاً کلیه سرویس های دیگر از کار خواهند افتاد. به همین جهت یکی از چهار پارامتر اصلی² 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 با 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.

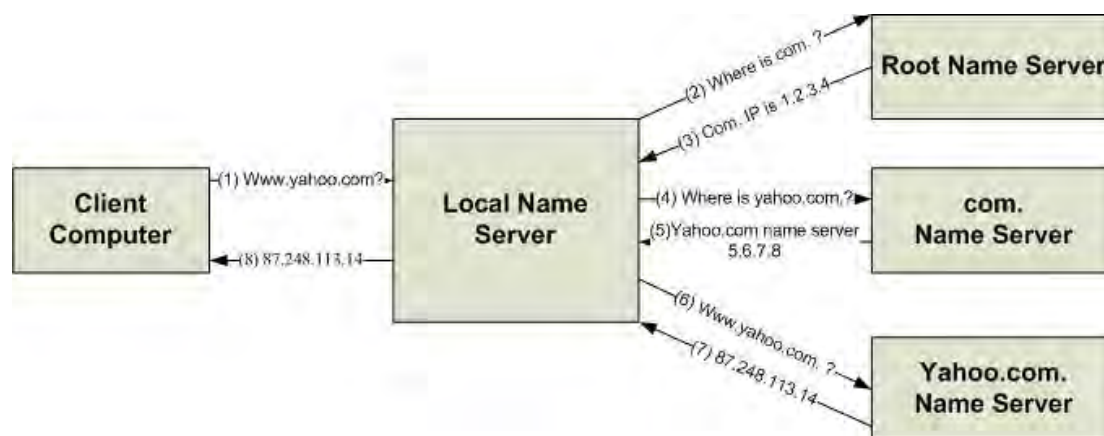


شکل ۳۲: ساختار درختی در نام گذاری اینترنتی

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. 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

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 بسته ها 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 بسته ها در گلوگاه ها حاصل می گردد؛ همچنین تضمین کیفیت سرویس QoS^۶ برعهده این لایه است.

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

لایه ۲: در این لایه فریم تشکیل و مکانیزمی برای تشخیص خطا^۷ در فریم فراهم می شود. یعنی در این لایه داده ها در فریم منتقل می شوند. فریم ها به صورت فریم های داده یا فریم های تأییدیه^۸ می باشند.

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

در شبکه هایی که از تکنولوژی Broadcast استفاده می کنند یک زیر لایه به نام Media Access Sub layer اضافه می شود که مسولیت مدیریت محیط انتقال مشترک را برعهده دارد.

لایه ۱: واحد انتقال اطلاعات در این لایه بیت می باشد یعنی در این لایه فریم تبدیل به بیت و سپس به سیگنال تبدیل می شود. کلیه مسائل در این لایه حول موضوع نحوه انتقال بیت های خام روی محیط فیزیکی انتقال، واسط های مکانیکی و الکتریکی می باشد.

^۱ - Segment

^۲ - Packet

^۳ - static routing

^۴ -Dynamic routing

^۵ - Congestion

^۶ - Quality of Service

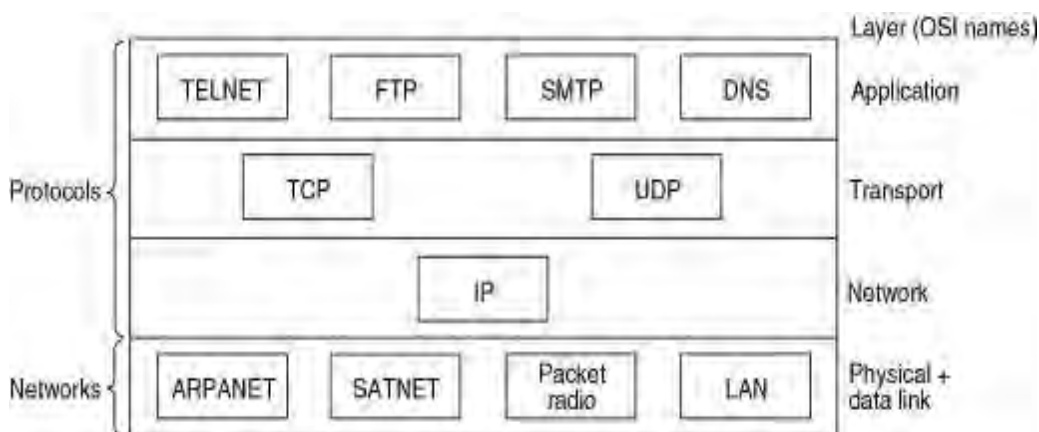
^۷ - Error Detection

^۸ - Acknowledge

^۹ - 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

لایه انتقال یا Transport:

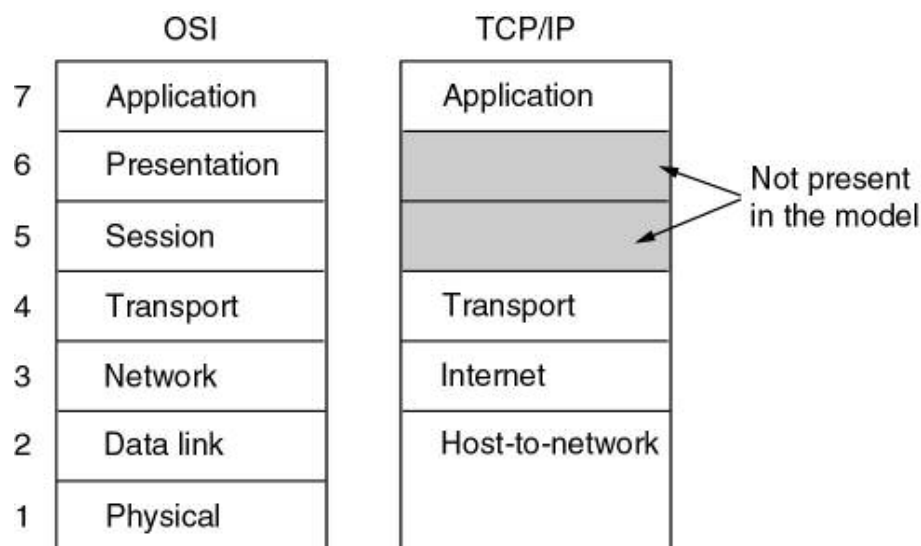
در این لایه ارتباط به صورت انتها به انتها^۱ مطرح است و دو نوع پروتکل در این لایه وجود دارد:

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 ۳۵: 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.

^۱ - End-to-End

^۲ - Transmission Control Protocol

^۳ - Reliable Connection-Oriented

^۴ - User Datagram Protocol

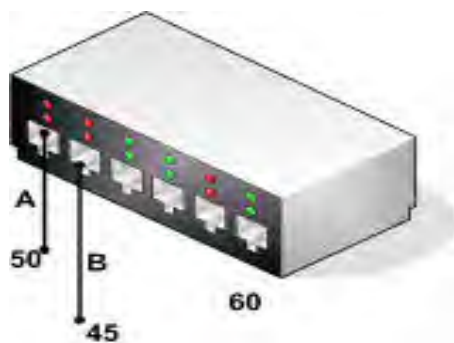
^۵ - Unreliable Connection-less

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 نمائید:



Mac Address Table	
50	1
60	8

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:

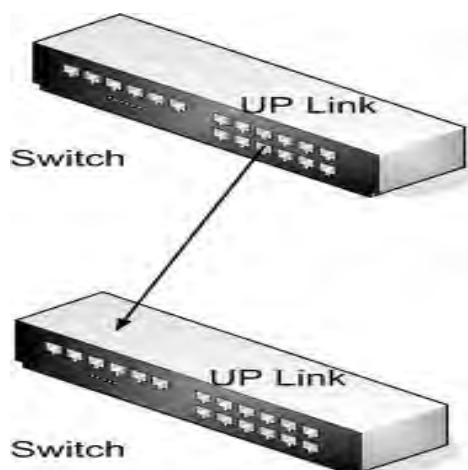
۱- سرعت و تعداد پورت ها

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 Telnet , HTTP , SNMP , RMON 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 خصوصیاتی 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.

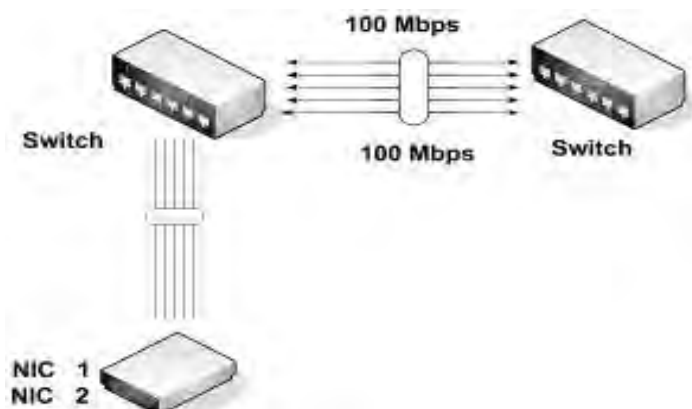
Port Trunking

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

سوئیچ ها 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 می دهد تا ترافیکی را که به سوئیچ می رسد بررسی نموده و آن را اولویت بندی نماید. برای این کار در سوئیچ ها چند صف تشکیل می دهد (به عنوان مثال در سوئیچ های 3Com چهار صف) و ترافیک اولویت بندی شده در صف ها ارسال می گردد. معمولا ترافیک های صدا و تصویر در اولویت بالاتر قرار دارند.

رمزنگاری^۴

بعضی سوئیچ ها قابلیت رمزنگاری دارند. کارت شبکه نیز می تواند از چنین قابلیتی برخوردار باشد. اکنون چند سوال مهم مطرح و به آنها پاسخ داده می شود. 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 رود Broadcast نیز با سرعت بیشتری به Control Site می رسد لذا باید به فکر کاهش Broadcast بود.

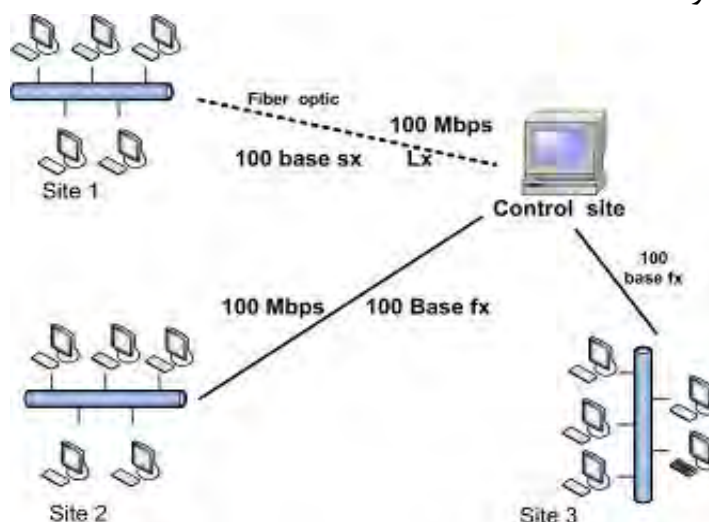
^۱ -Desktop

^۲ -Rack Mount

^۳ -Quality of Service

^۴ -Encryption

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 کوئل 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

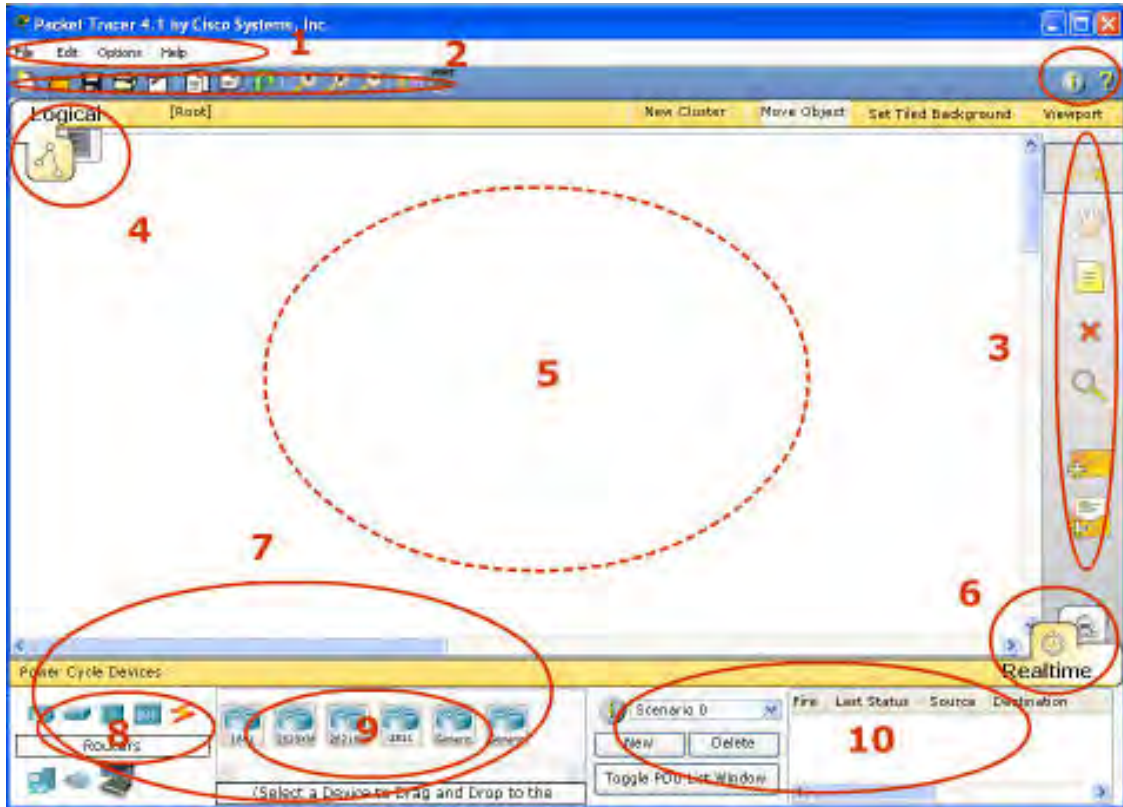
نرم افزار Packet Tracer یک محیط شبیه سازی جهت طراحی، پیاده سازی توپولوژی، پیکربندی، بررسی مشکلات و ... را در شبکه دارند. کاربران می توانند با استفاده از ابزارهای مورد نظر در محیط شبیه سازی، به راحتی توپولوژی دلخواه خود را ایجاد و پس از پیکربندی شبکه ایجاد شده، به بررسی، تحلیل و رفع مشکلات آن بپردازند.

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:

فضای کار منطقی	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
فضای کار فیزیکی	سلسله مراتب دستگاه ها، فضاهای سیم بندی، ساختمان ها، شهرها و نماهای بین شهری، استفاده از تصاویر گرافیکی ایجاد شده توسط کاربر
حالت Realtime	به روز رسانی پروتکل ها بصورت زنده حد متوسطی از پیکربندی های IOS CLI برای سوئیچ ها و مسیریاب ها
پروتکل ها	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
حالت شبیه سازی (Simulation)	Packet animation Global event list (packet sniffer) OSI Model, Detailed PDU, and Device Table Views User-defined multiple packet scenarios
طراحی و به اشتراک گذاری	گزینه های متنوع ذخیره سازی فایل Activity Wizard برای فعالیتهای 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

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.

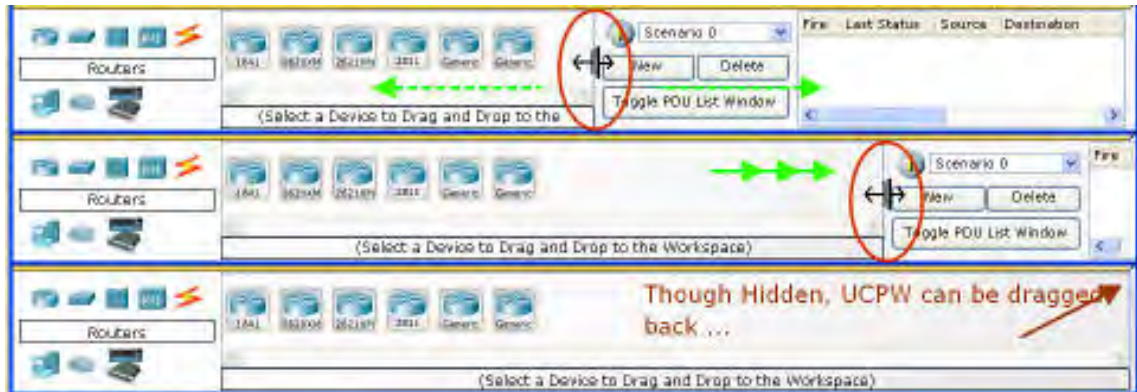
نوار منو	شامل منو های File ، Options و Help که دستورات رایجی نظیر Open، Save ، Print و Preferences در این منوها قرار گرفته اند.
نوار ابزار اصلی	شامل آیکن های میانبر برای دستورات منوی File و Edit و شامل دکمه هایی برای بزرگنمایی، پالت ترسیم، و مدیریت الگوها (Device Template Manager) است. در سمت راست آن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



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

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.

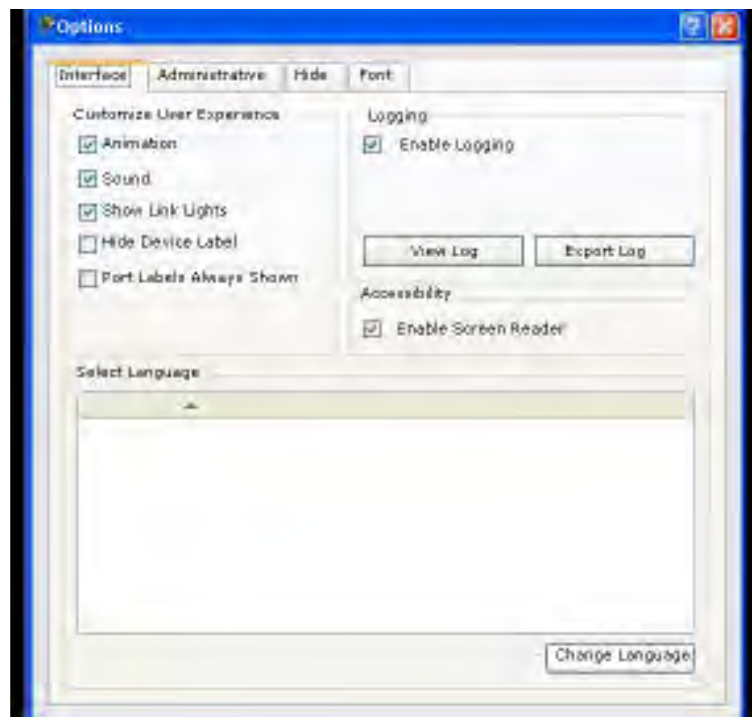


فضاهای کاری و حالت ها

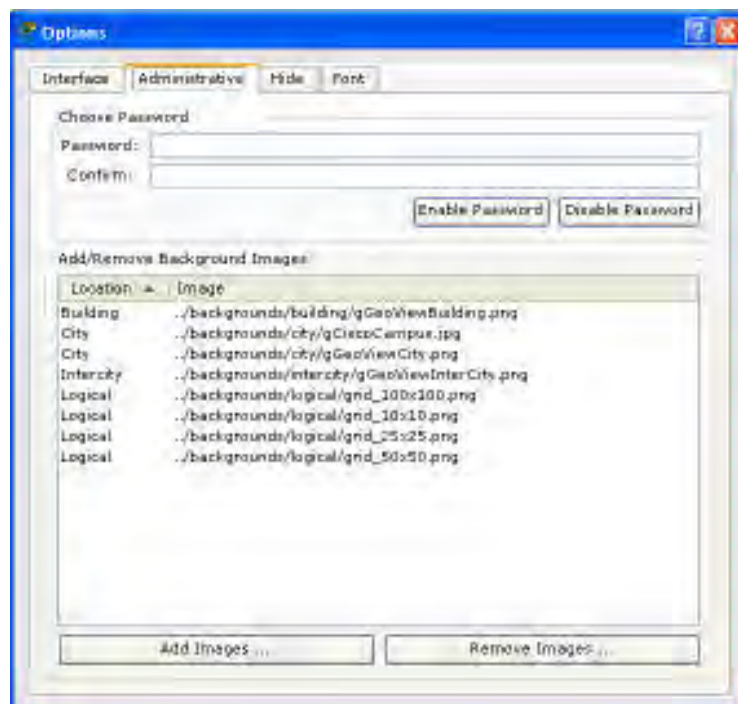
نرم افزار Packet Tracer 4.1 شامل دو فضای کاری منطقی و فیزیکی، و دو حالت Realtime و شبیه سازی است. هر شبکه را می توان در نمای منطقی ایجاد کرده و در حالت real time اجرای آن را مشاهده نمود. همچنین می توان برای اجرای سناریو های کنترل شده به حالت شبیه سازی سوئیچ نمود. برای تنظیم چیدمان فیزیکی وسایل، به حالت 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 داده 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.



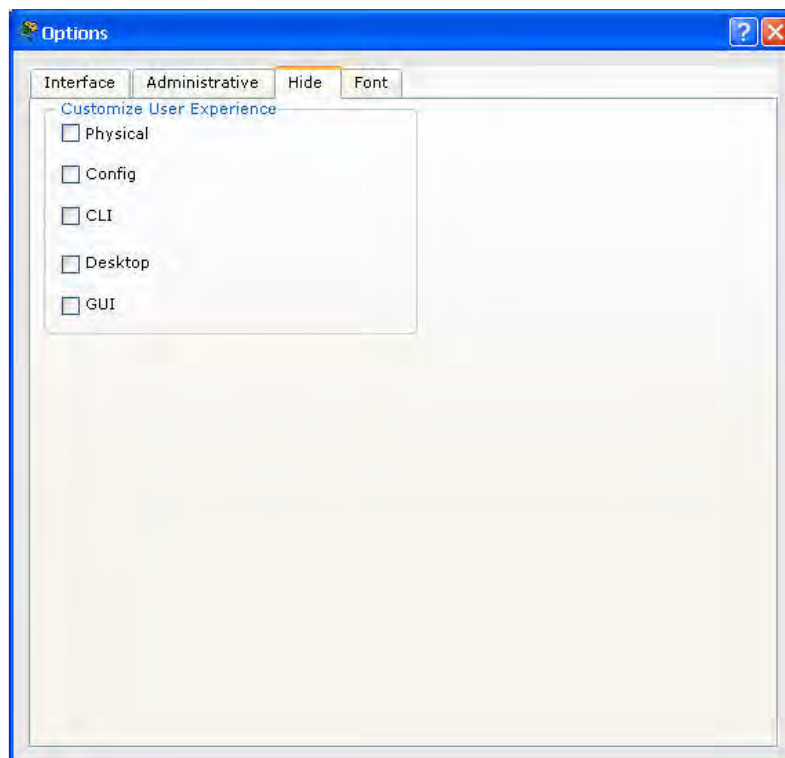
در برگه Administrative تصاویر زمینه ای که در برنامه فعال است را می توان مدیریت نمود. در این برگه امکان تعیین کلمه عبور برای جلوگیری از تغییرات ناخواسته نیز وجود دارد.



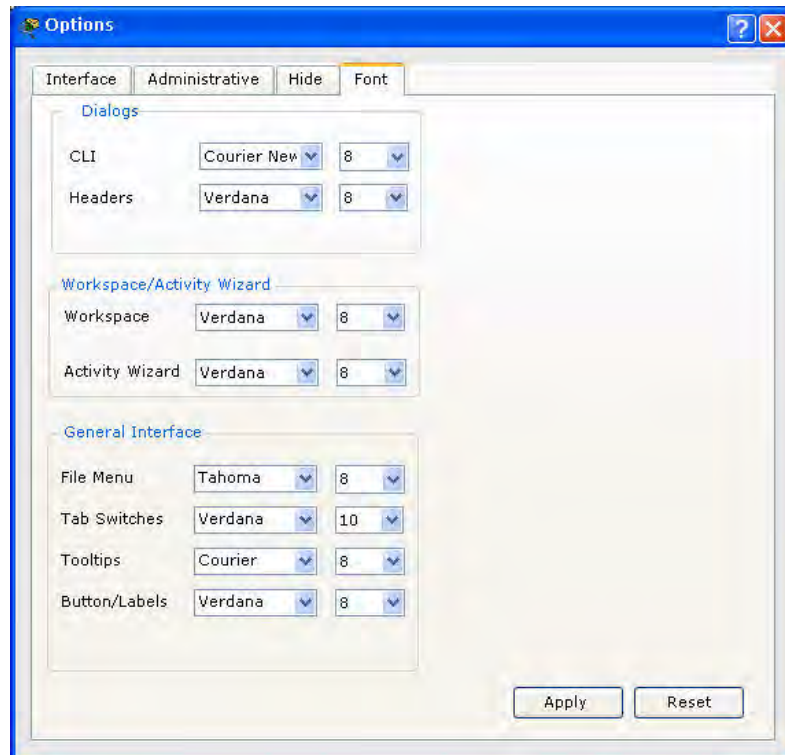
در برگه Hide هر یک از موارد مشخص شده را از پنجره برنامه یا کادرهای مختلف، می توان پنهان نمود.



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

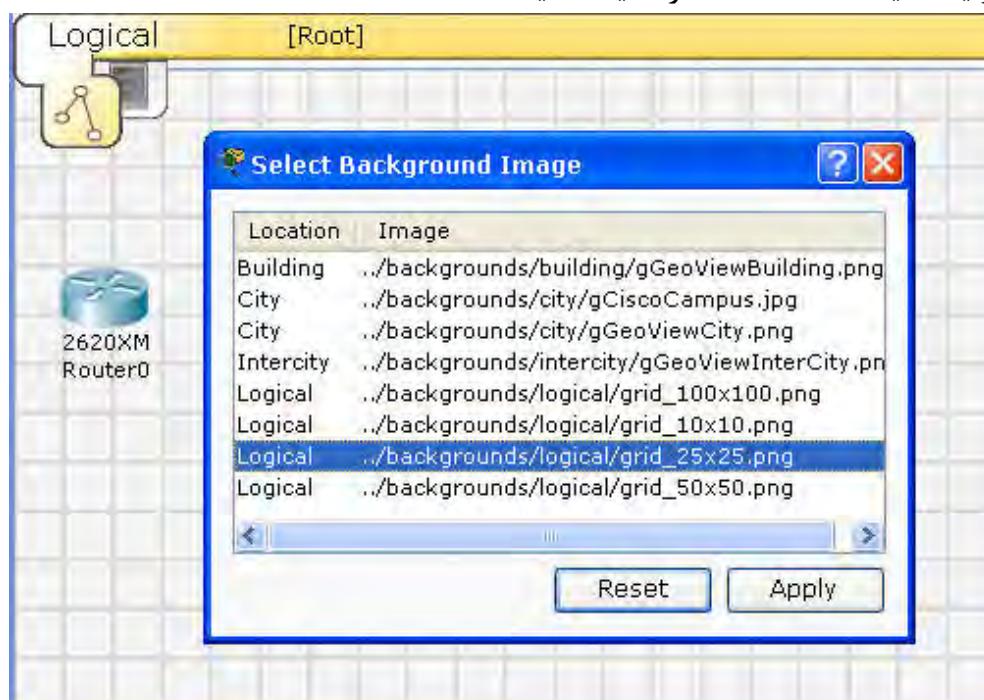


در برگه Font، نوع و اندازه فونت کادرها و واسط های مختلف تعیین می گردد.



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 تأثیری 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 قبلاً گفته شد یک آدرس ۳۲ بیتی است که به دستگاه ها برای شناسایی آنها در شبکه اختصاص داده شده است.

- 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.

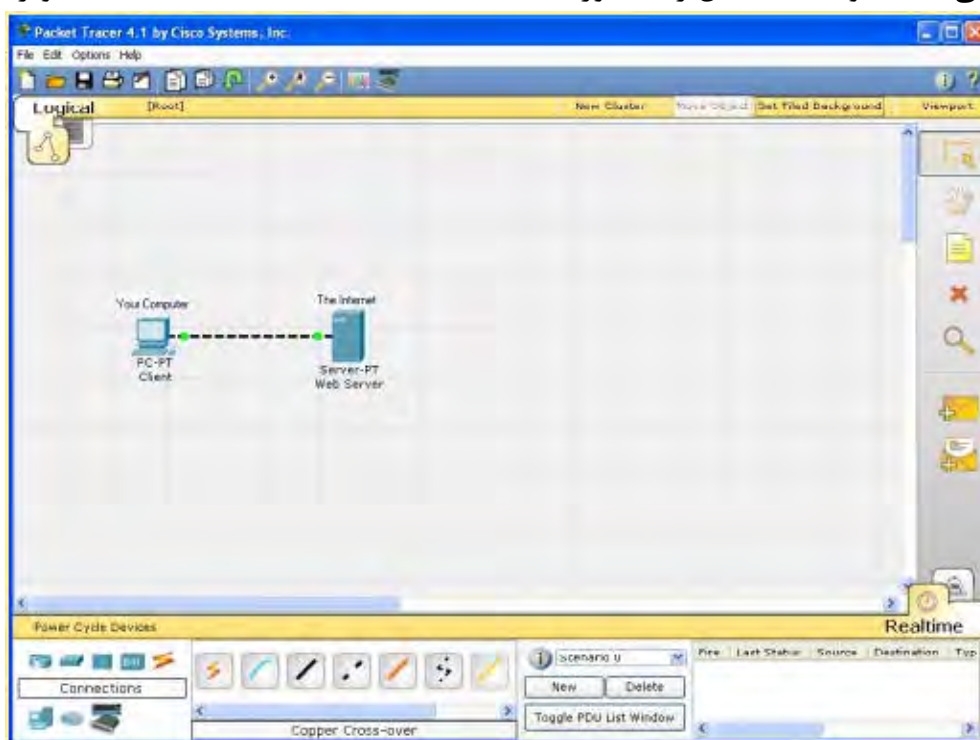
پنجره تنظیمات PC را باز کنید و با رفتن به برگه Config تنظیمات آن، همچون نام آن را تغییر دهید. در قسمت Interface روی FastEthernet کلیک و آدرس IP را به صورت 192.168.1.1



✓ 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 برجسب متنی با استفاده از ابزار Place Note در Logical Workspace اضافه کنید.

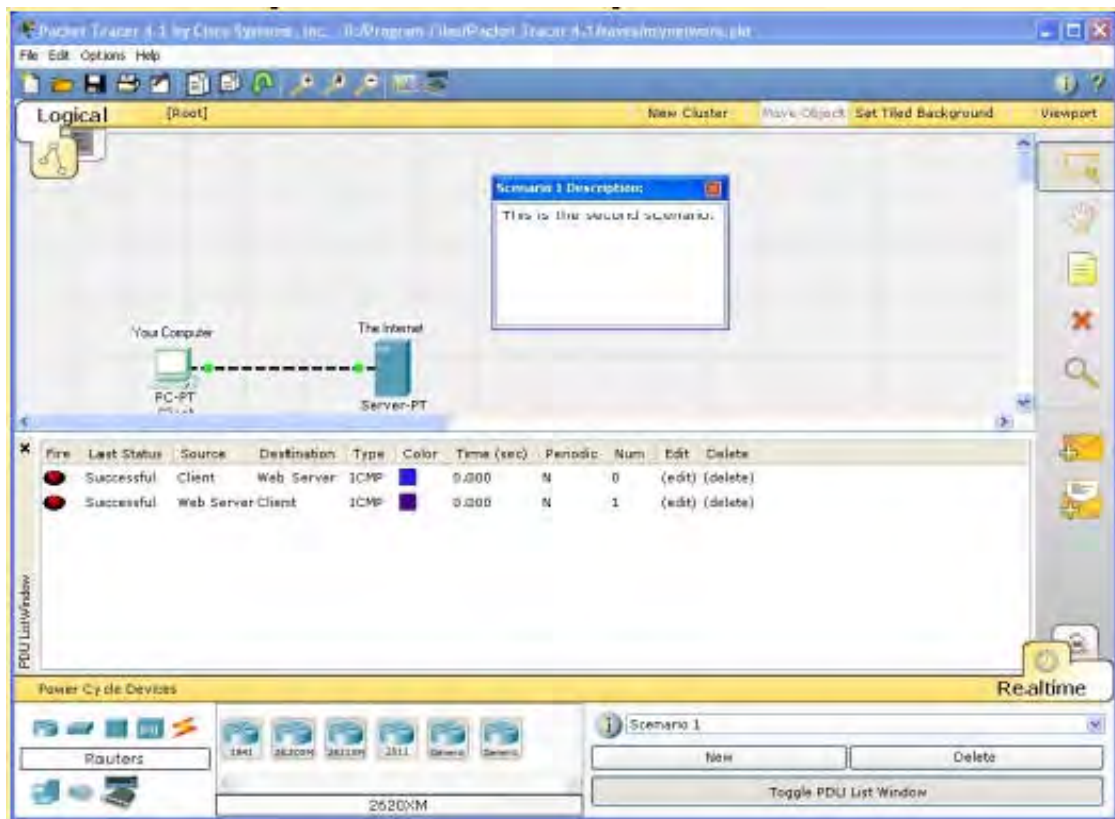
روی رایانه اول یک بار کلیک نموده و در حالی که وضعیت چراغ های اتصال را مشاهده می کنید، رایانه را خاموش و سپس روشن نمایید.

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.

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 یک 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^۱. 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

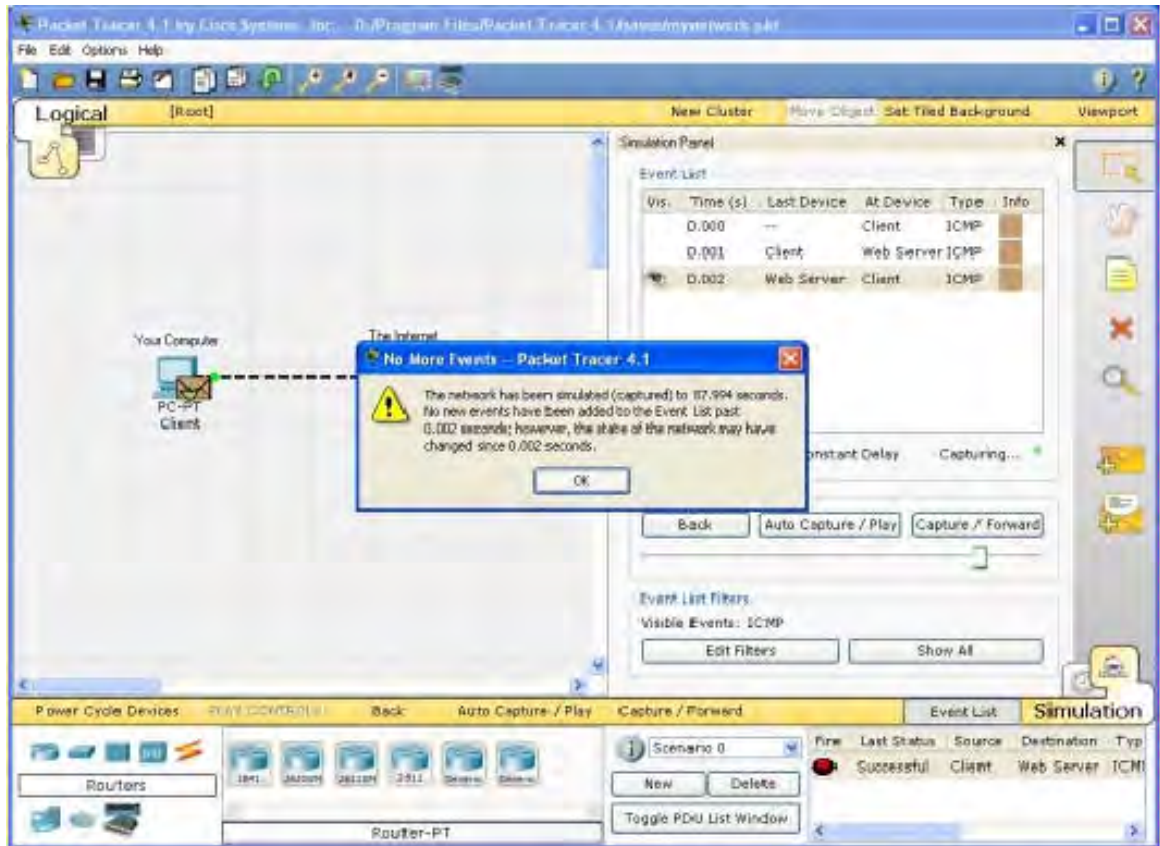


✓ فصل دوم: شبیه سازی شبکه توسط نرم افزار Packet Tracer

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 رویداد ها 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.

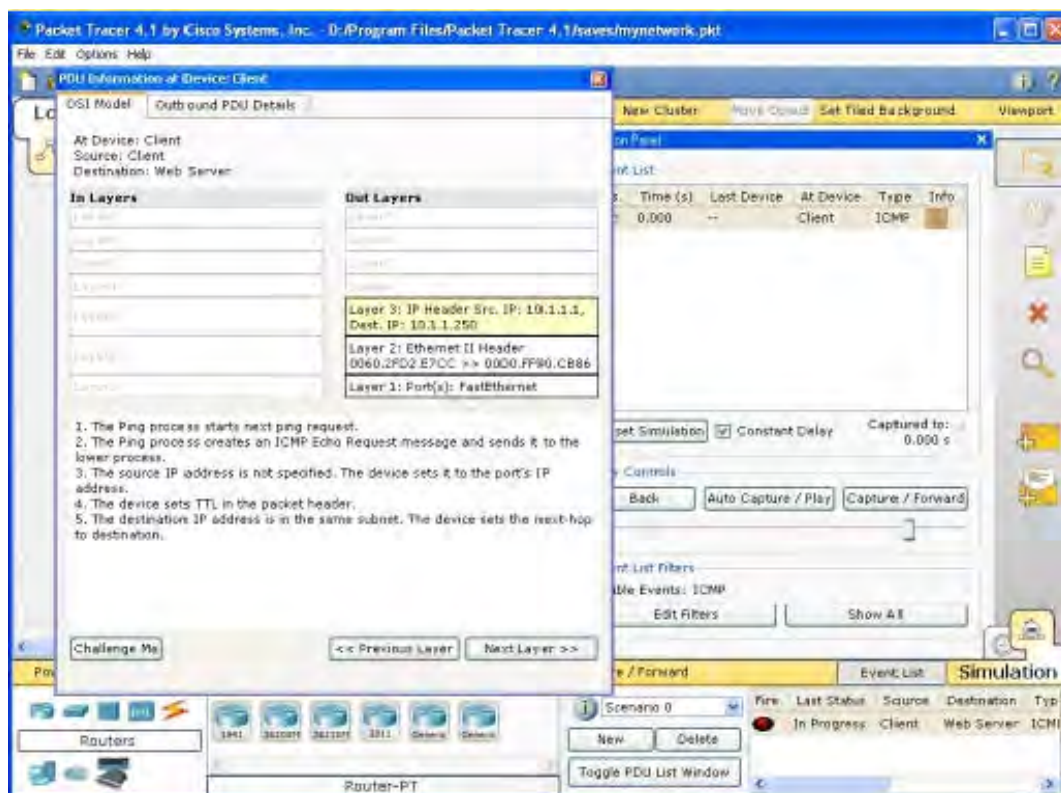


به این ترتیب با موفقیت رویداد ها را ثبت کرده و انیمیشن ها را در حالت شبیه سازی مشاهده نموده اید.

مشاهده داخل بسته ها در حالت شبیه سازی

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

روی پاکت نامه 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 می دهد. 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 پاکت نامه است.

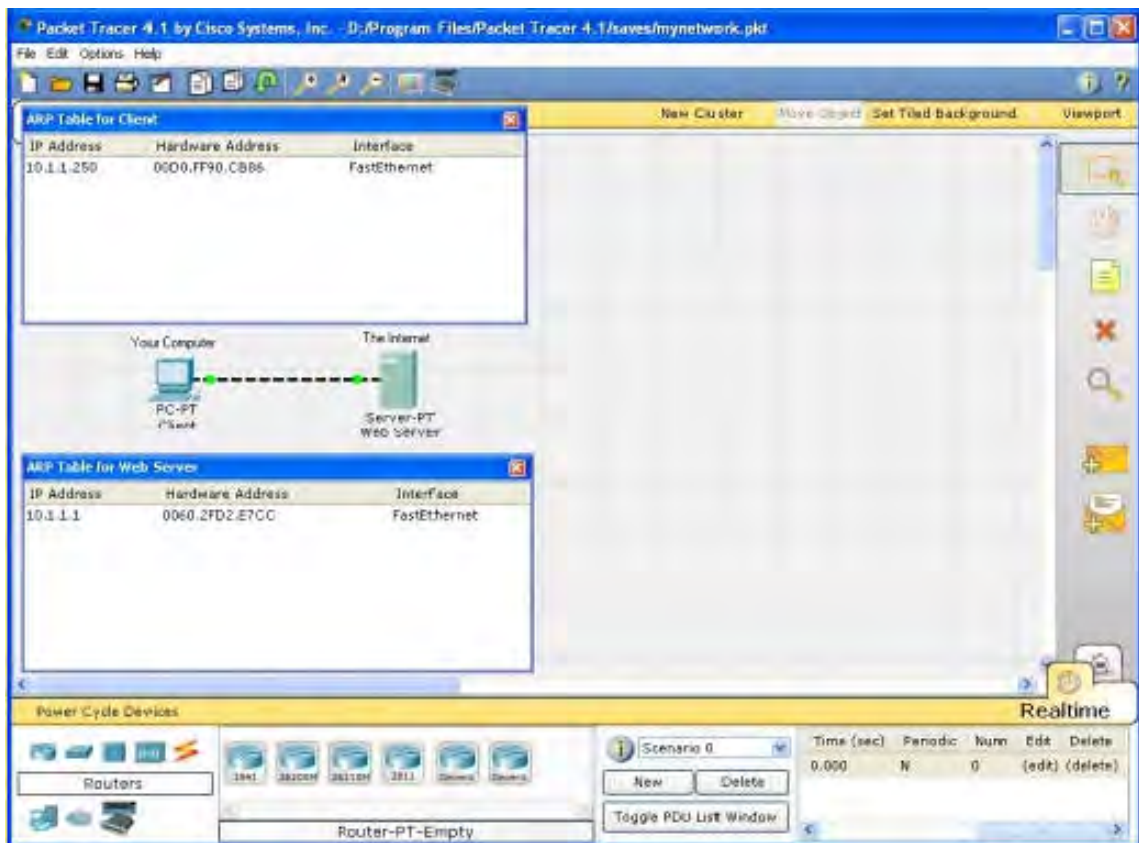


از دکمه های Previous Layer و Next Layer برای مشاهده جزئیات پردازش بسته در لایه های مختلف استفاده کنید. باید به این نکته توجه داشت که فقط Out Layers قابل مشاهده است. روی برگه Outbound PDU Details کلیک کنید. این برگه دقیقاً سرآمد PDU را نمایش می دهد. پنجره PDU Information را ببندید. یک بار روی دکمه Capture/Forward 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 Reset Simulation کلیک کنید. این بار روی Capture/Play کلیک کنید. ارسال پیام 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.

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. جداول 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 جداول 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.

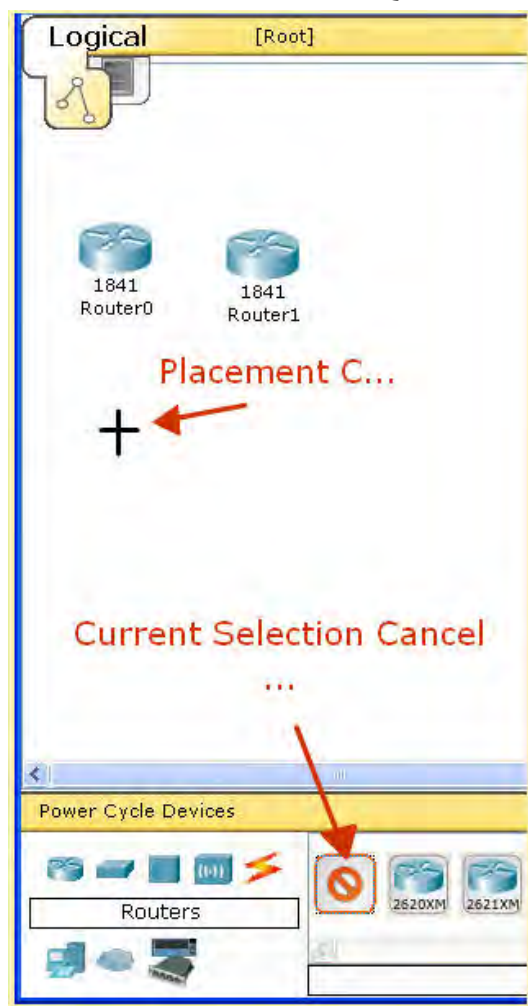
ابتدا شما باید دستگاه ها را ایجاد کنید. این کار با انتخاب دستگاه از کادر Network Component انجام می شود. سپس می توانید هر یک از موارد زیر را انجام دهید:

- 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

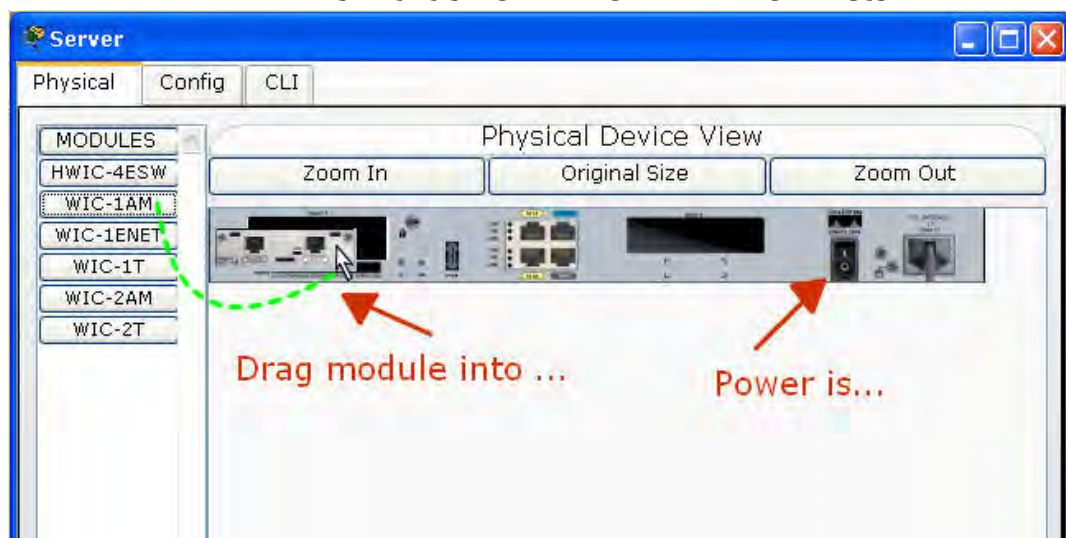
دستور Device Template Manager به شما امکان ذخیره کردن دستگاه ها را بعنوان الگوهایی فراهم می کند تا بعدا بتوانید از این الگوها برای ایجاد دستگاه های دلخواه خود استفاده کنید. مثلا فرض کنید که می خواهید الگویی از مسیریاب 2621XM با یک ماژول NM-2FE2W و دو ماژول WIC-2T ایجاد کنید. بنابراین ابتدا مدل مورد نظر 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 ، Zoom out و Original Size تغییر اندازه دهید. همچنین می توانید در 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 درآید. با درآوردن 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.

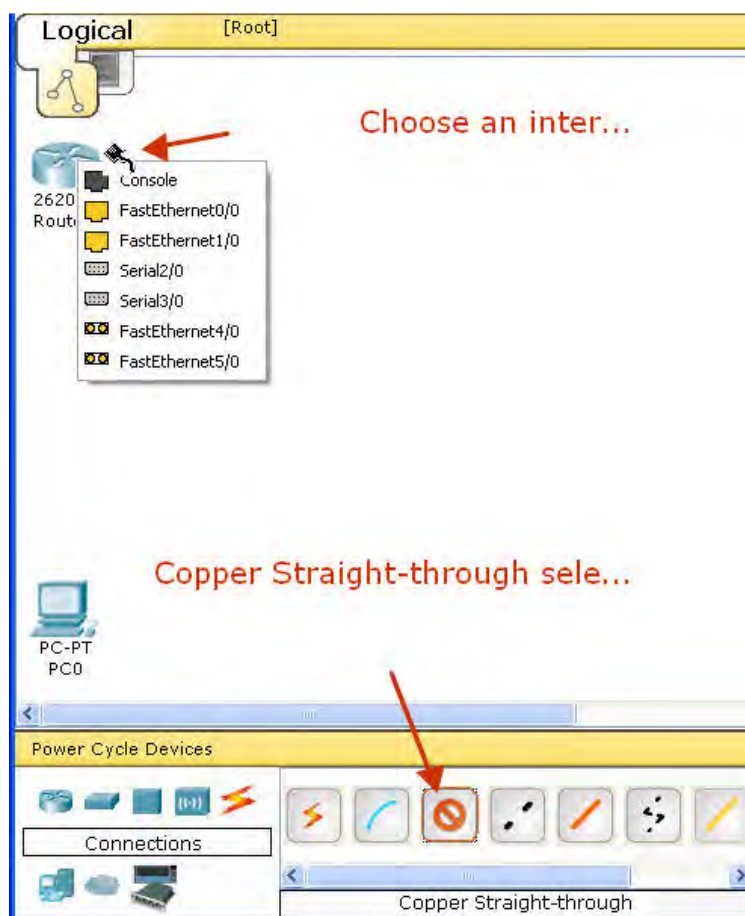


✓ فصل دوم: شبیه سازی شبکه توسط نرم افزار Packet Tracer

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.

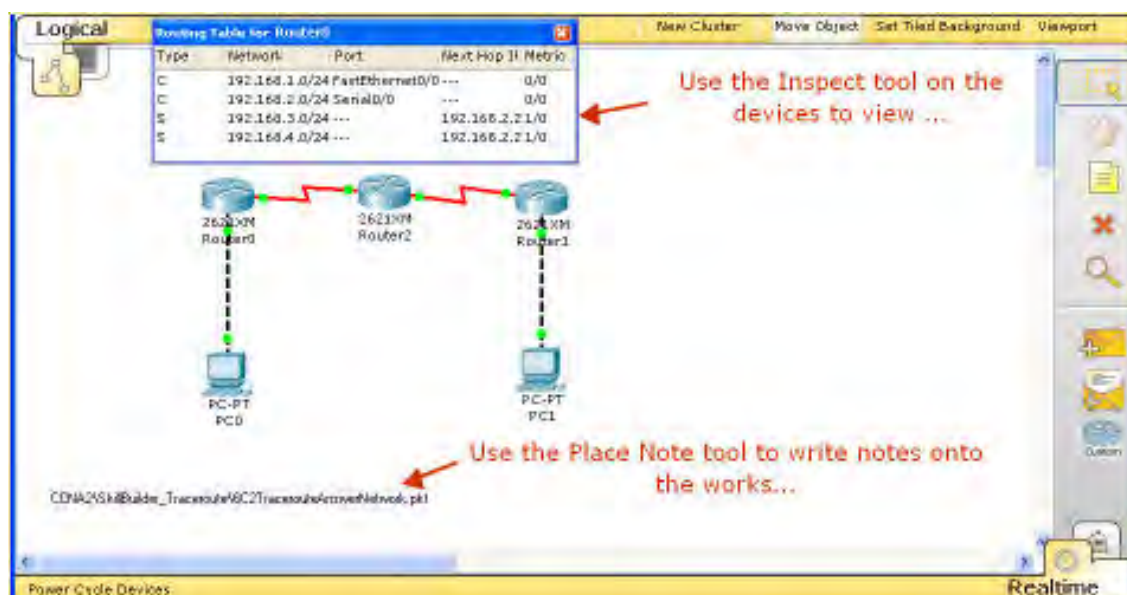
برای ایجاد سریع اتصالات مختلف از نوع یکسان، دکمه Ctrl را نگه دارید و روی اتصال مورد نظر کلیک کنید. سپس دکمه Ctrl را رها کنید تا بتوانید مکرراً از اتصال یکسان بین دستگاه ها استفاده نمایید. برای اتمام عملیات روی آیکن Cancel کلیک کنید.



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.

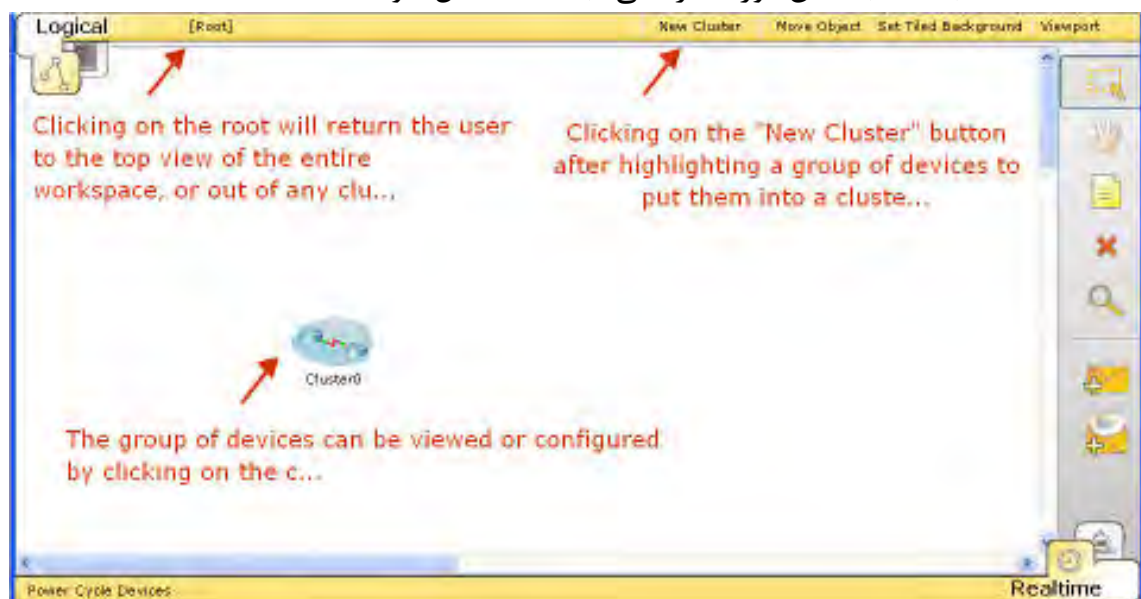
گروه بندی دستگاه ها (Clustering)

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

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.

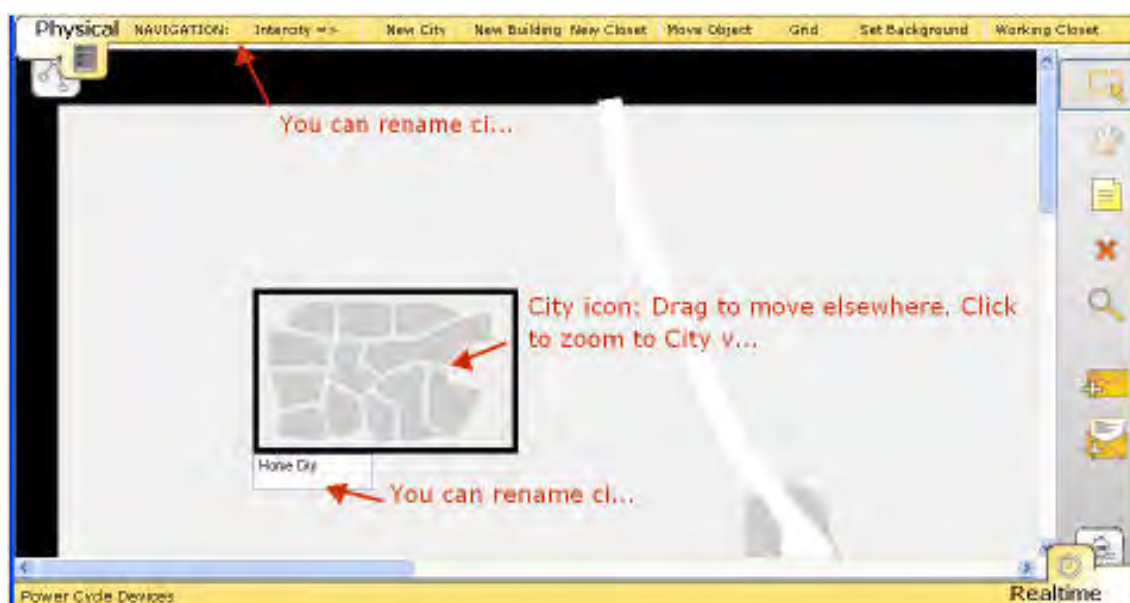




فضای کار فیزیکی

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 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.

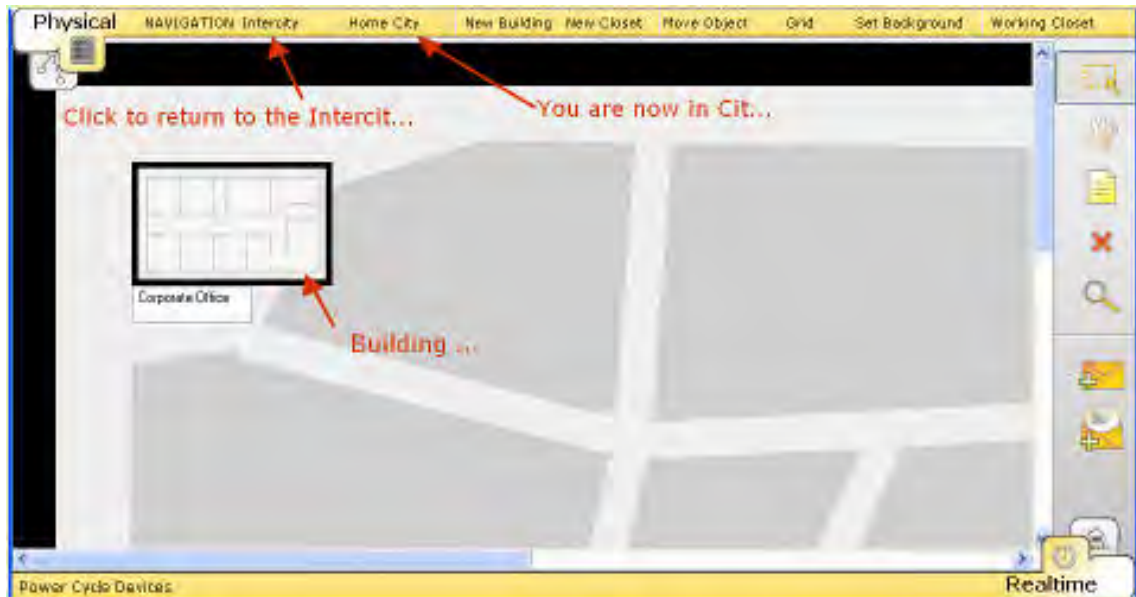


به طور پیش فرض، این فضا شامل یک شهر به نام Home City است. که می توان آن را در روی نقشه جابجا نمود. و نیز می توان به آسانی روی آن کلیک تا نقشه شهر نمایش داده شود.

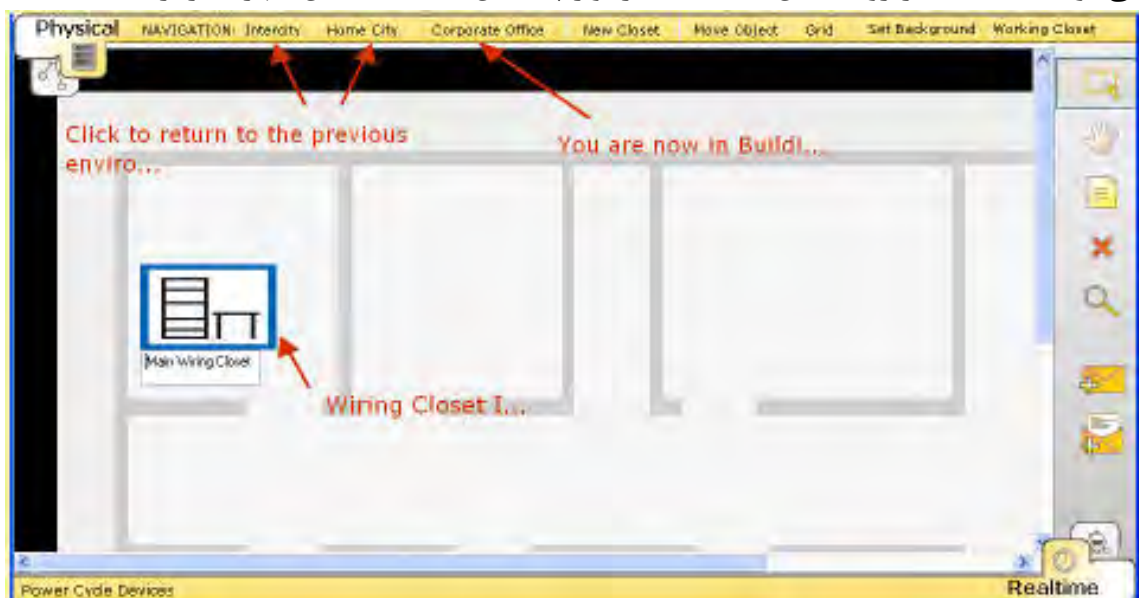
^۱ - Intercity

^۲ - wiring closet

^۳ - 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.

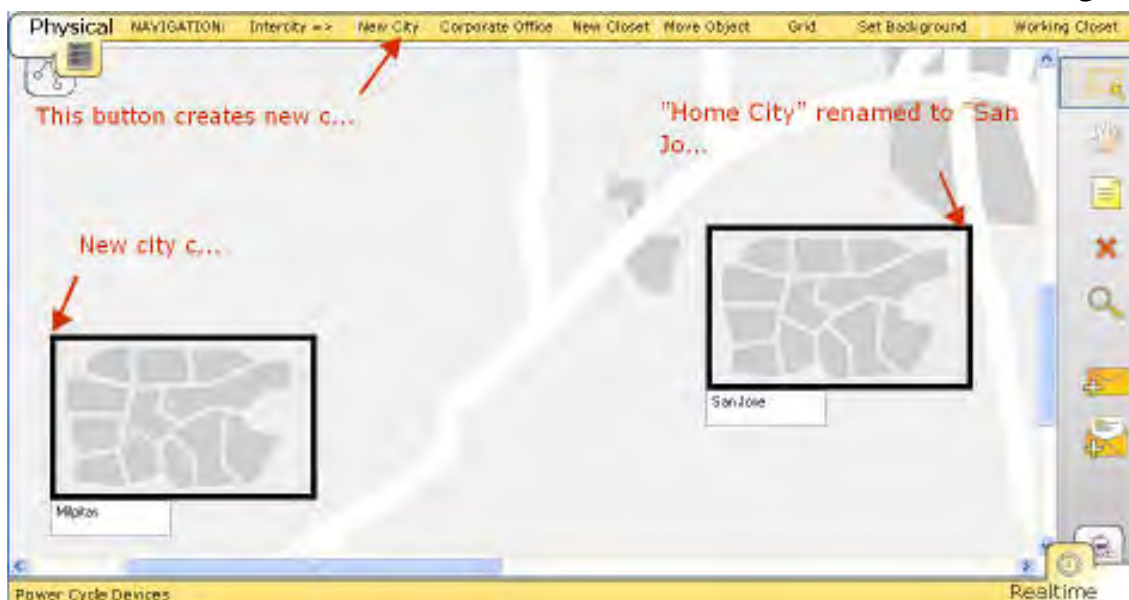


✓ فصل دوم: شبیه سازی شبکه توسط نرم افزار Packet Tracer

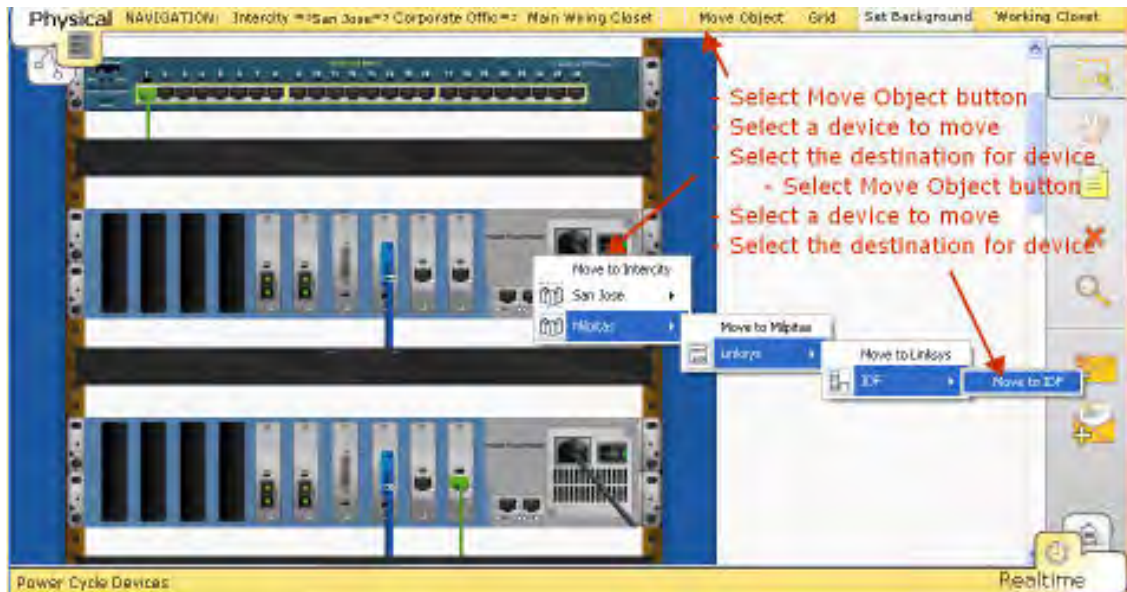
جابجا کردن اشیاء در فضای کار فیزیکی

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.

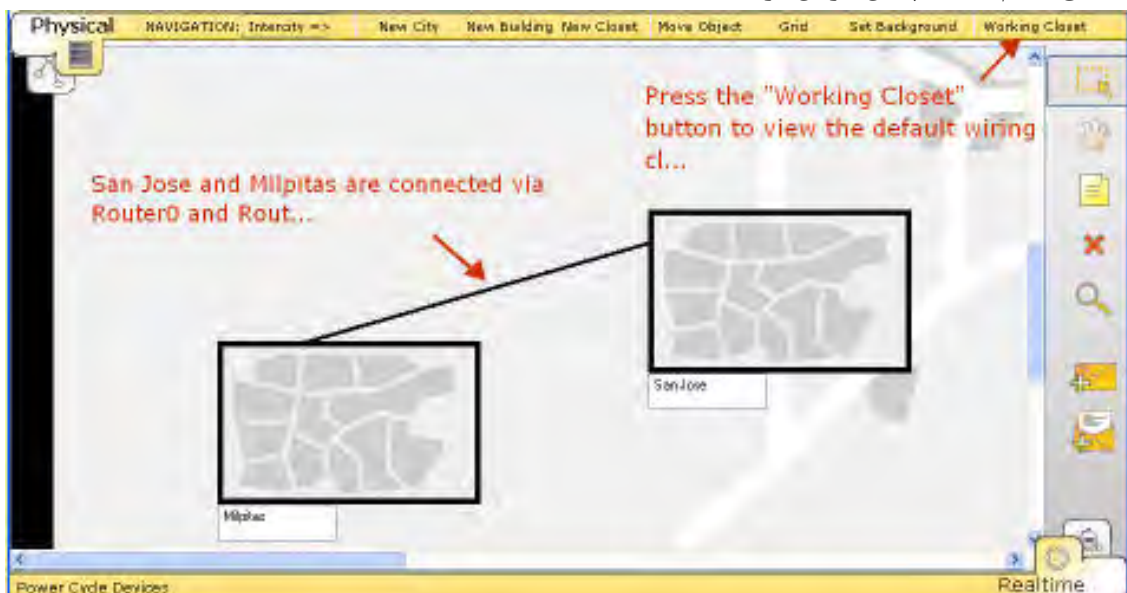
البته باید دقت کرد که هر شهر، ساختمان و یا اتاق جدیدی که ایجاد می شود، ابتدا در گوشه بالا سمت چپ ظاهر شود. برای جلوگیری از سردرگمی، باید آنها را فوراً تغییر نام داده و مکان آنها را تعیین کنید.



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.



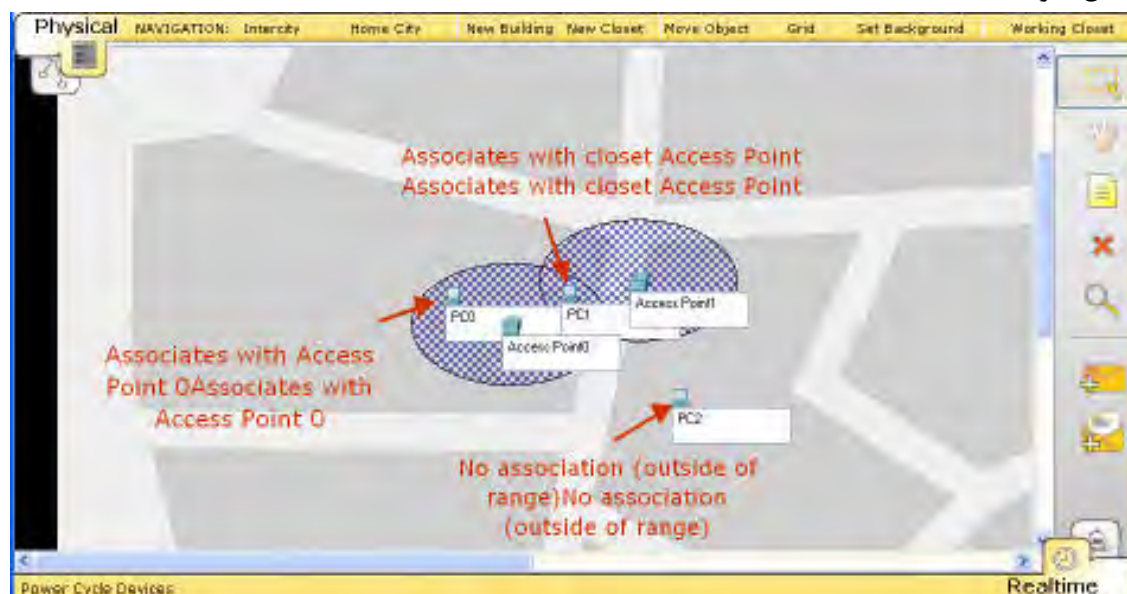
برای مثال، برای انتقال Router1 به IDF، ابتدا باید به MDF رفته و روی دکمه Move object کلیک کنید. حال روی Router1 کلیک و سپس در ساختار سلسله مراتبی، IDF را پیدا کنید، آنگاه Move to IDF را انتخاب نمایید. در نمای Intercity خواهید دید که یک خط سیاه بین San Jose و Milpitas ایجاد شده است. این خط نشان دهنده اتصال ایجاد شده بین دستگاه های موجود در این دو شهر است که در این مثال یک اتصال سریال بین دو مسیر یاب 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 :

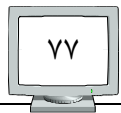
با کلیک بر روی دکمه Grid می توانید یک صفحه مشبک دلخواه به نماهای مختلف بین شهری، شهر و ساختمان اعمال کنید. این ابزار به شما امکان تنظیم فاصله شبکه های هر سطح و نیز تعیین رنگ آنها را می دهد.

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 پورتهای خاموش گردد، چراغ آن فوراً قرمز می شود.

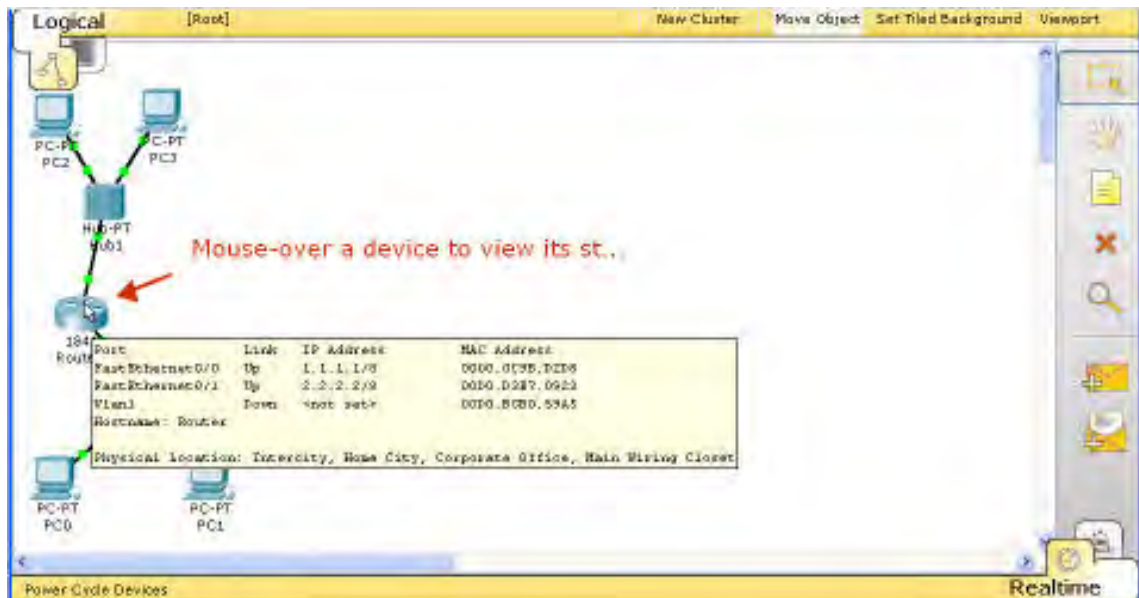
حالت Realtime

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 Creaetd 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 پرسیدن 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.

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 آیکن 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.

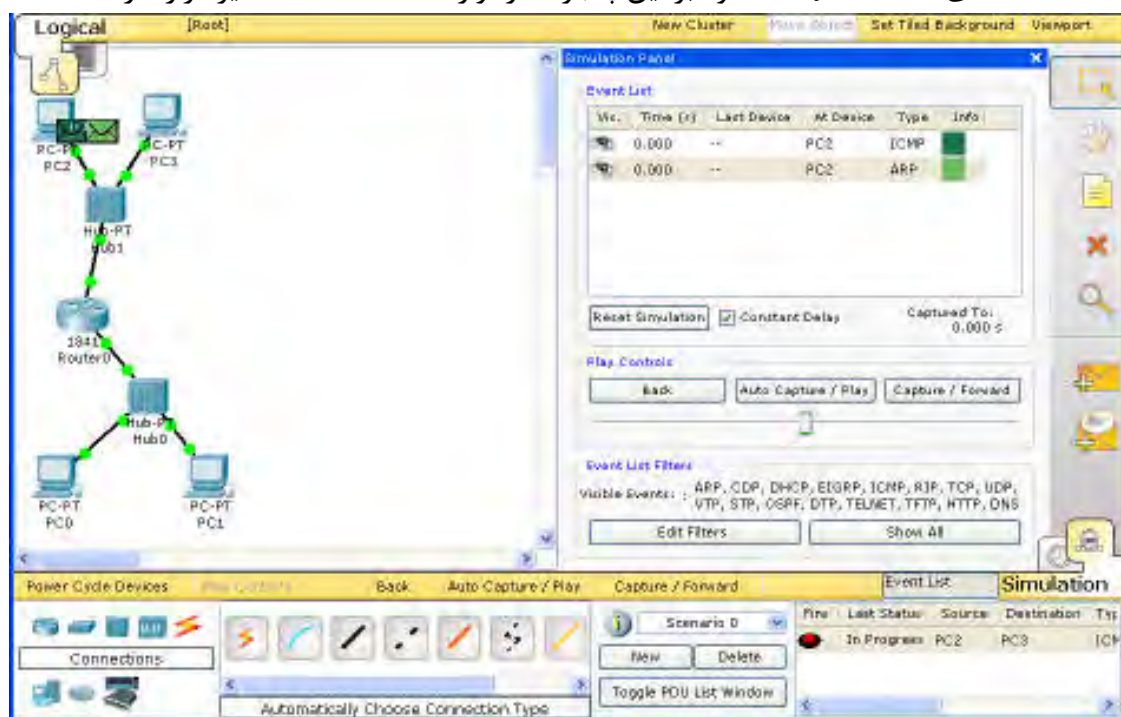
خاموش و روشن کردن دستگاه ها (Power Cycle Devices)

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 مسیر یاب 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 مسیر یاب 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

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 رویداد ها 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.



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

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

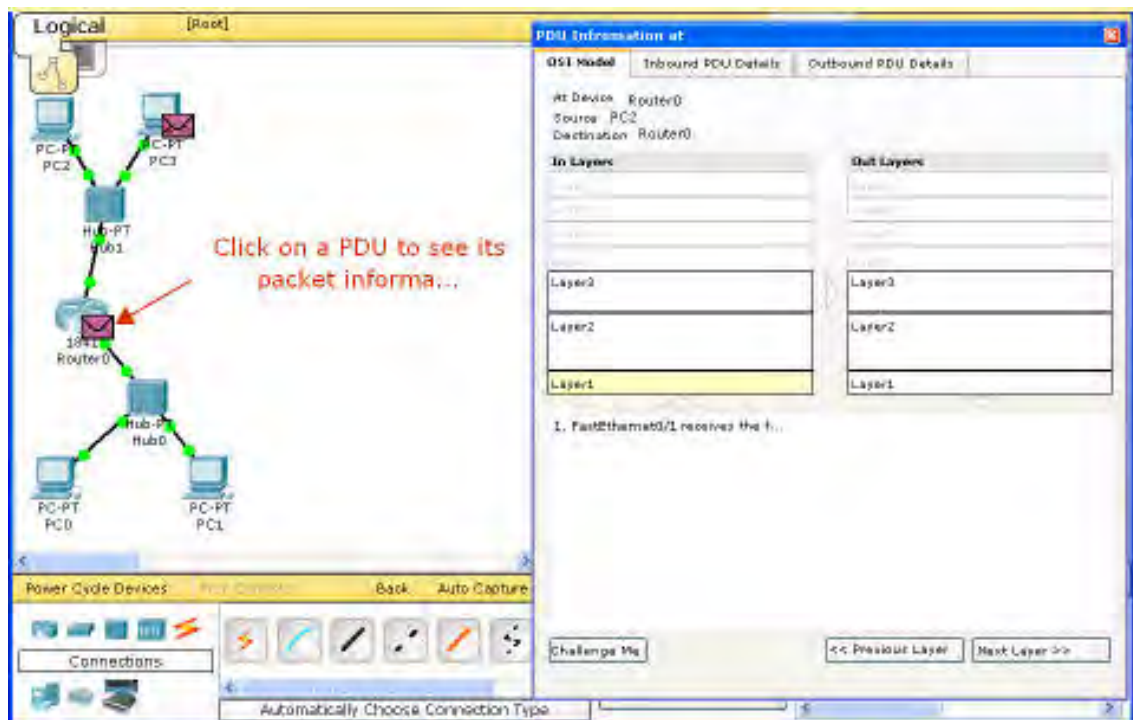
دقت کنید که اجرای مجدد شبیه سازی رویه های زمان بندی شده PDU فعلی را حذف نخواهد کرد، بلکه تنها رویداد های ثبت شده را حذف خواهد کرد. برای حذف PDU ها باید به صورت دستی آنها را از پنجره مربوط به بسته های ایجاد شده کاربر حذف کنید.

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 واسطه 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.

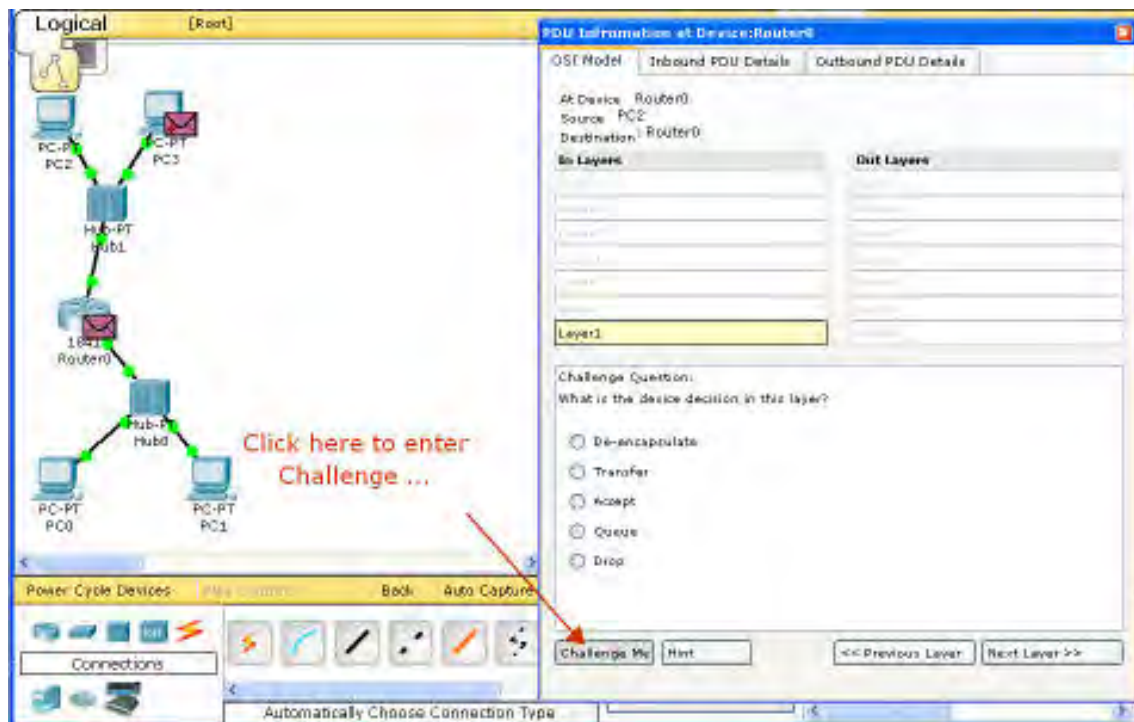
In Layer به معنای این است که از پایین به بالا خوانده می شود (از لایه ۱ تا ۷) و Out Layer از بالا به پایین خوانده می شود (لایه ۷ تا ۱). به این دلیل که لایه فیزیکی اولین لایه ای است که بسته های PDU ورودی با آن مواجه می شوند و آخرین لایه ای است که PDU های خروجی از آن رد خواهند شد تا از دستگاه خارج شوند.

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.





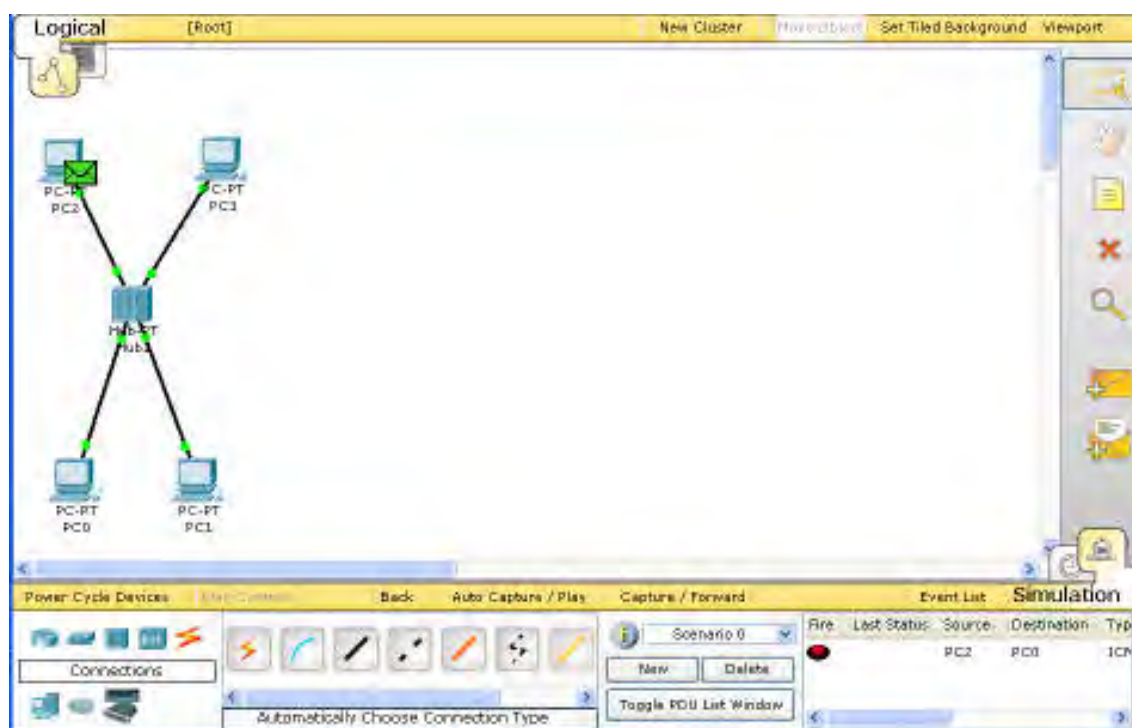
✓ فصل دوم: شبیه سازی شبکه توسط نرم افزار Packet Tracer

هر سؤال ممکن است شامل پاسخ های زیر باشد:

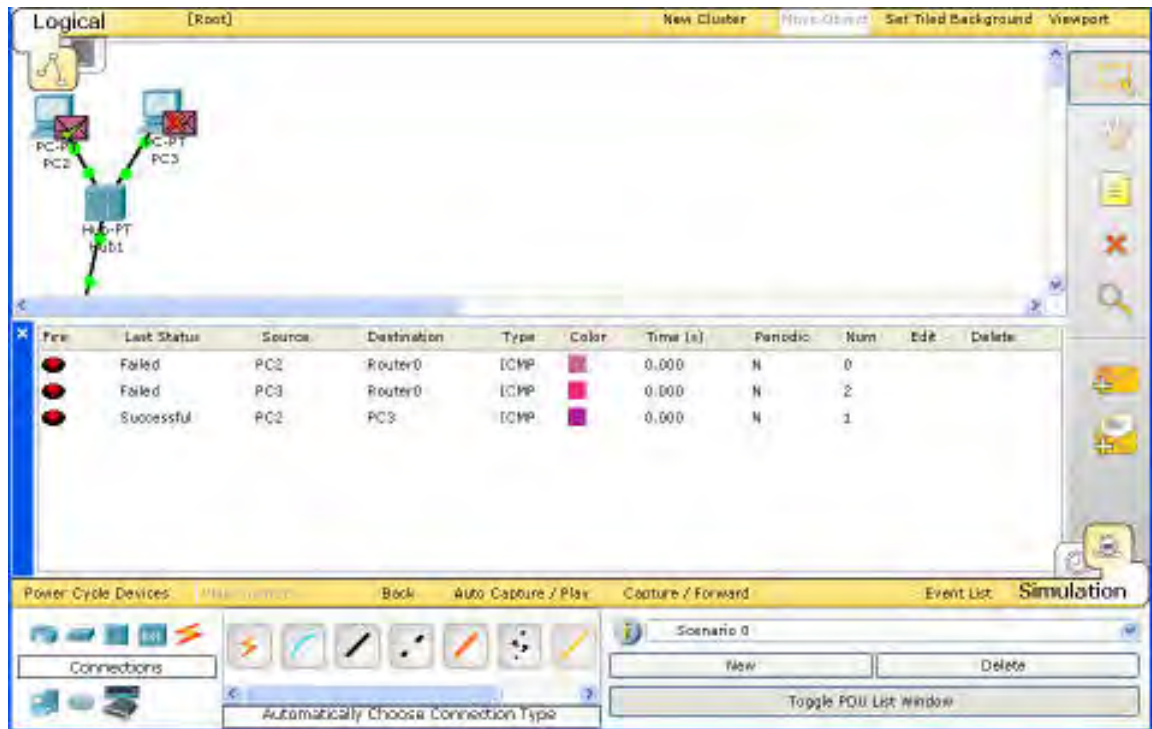
- Encapsulate: افزودن یک header یا یک header و trailer به PDU مربوط به این لایه برای ایجاد PDU ارسالی به لایه پایینتر
- De-encapsulate: حذف header یا header و trailer از PDU مربوط به این لایه و ایجاد PDU برای لایه بالاتر
- Transfer: انتقال PDU از قسمت inbound به قسمت outbound
- Accept: پذیرش بسته و پایان 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.

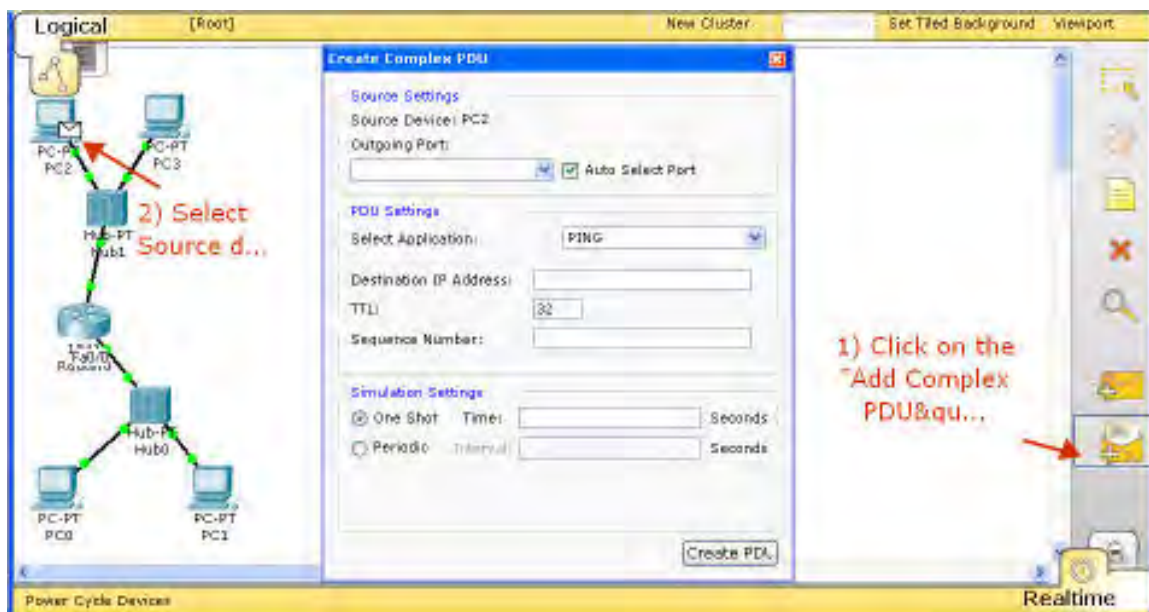


✓ فصل دوم: شبیه سازی شبکه توسط نرم افزار Packet Tracer

PDU های ایجاد شده توسط کاربر در ابتدا یک رنگ تصادفی می گیرند. شما می توانید با دابل کلیک بر روی مربع رنگی مربوط به آن، رنگش را تغییر دهید.

Complex PDU در حالت شبیه سازی

علاوه بر PDU های ساده که برای ping کردن استفاده می شوند، PDU های دلخواه دیگری را نیز می توان ارسال نمود. در نوار ابزار، پس از کلیک روی آیکن Add Complex PDU، دستگاه مبدا را انتخاب کنید. به این ترتیب کادر Create Complex PDU ظاهر می شود. در این کادر شماره پورت خروجی می توان را تعیین و یا نوع PDU را تغییر داد. بسته به برنامه ای که انتخاب می کنید ممکن است نیاز باشد تنظیمات مربوط به آدرس IP مقصد، TTL (زمان حیات)، پورت مبدا، پورت مقصد و شماره ترتیب را انجام دهید.



نرم افزار Packet Tracer 4.1 از بسته های PDU با پورت های مبدا و مقصد مطابق با پروتکل های زیر پشتیبانی می کند:

DNS, Finger, FTP, HTTP, HTTPS, IMAP, NetBIOS, Ping, POP3, SFTP, SMTP, SNMP, SSH, Telnet, TFTP, other

پارامترهای زمانبندی PDU نیز قابل تنظیم هستند. One Shot یعنی این که بسته تنها در زمان تعیین شده (بر حسب ثانیه) ارسال شود و Periodic یعنی بسته به صورت متناوب مطابق آنچه که تنظیم می شود (بر حسب ثانیه) ارسال شود.

انواع اتصالات

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

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

اتصالات بیسیم

بین نقاط دسترسی و دستگاه های پایانی (نظیر رایانه، سرور، چاپگر) می توان اتصال بی سیم برقرار کرد؛ برای این کار باید ماژول فعلی دستگاه را برداشته و بجای آن ماژول 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، معمولاً چراغ هایی را در دو سمت اتصال مشاهده می گردد. البته برخی اتصالات این چراغ ها را ندارند.

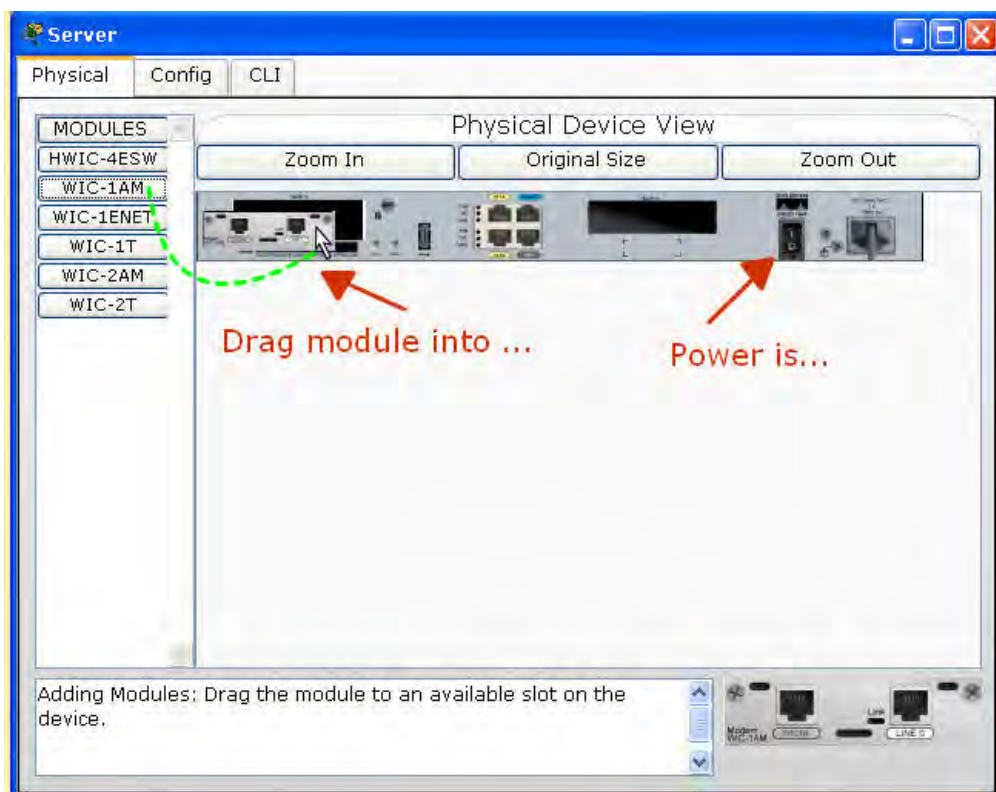
- سبز روشن: اتصال فیزیکی up است.
- سبز چشمک زن: اتصال فعال است.
- قرمز: اتصال down است. سیگنالی پیدا نمی شود.
- کهربایی: پورت در وضعیت بلاک است. (فقط برای سوئیچ ها ظاهر می شود)

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 سپسکو 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.

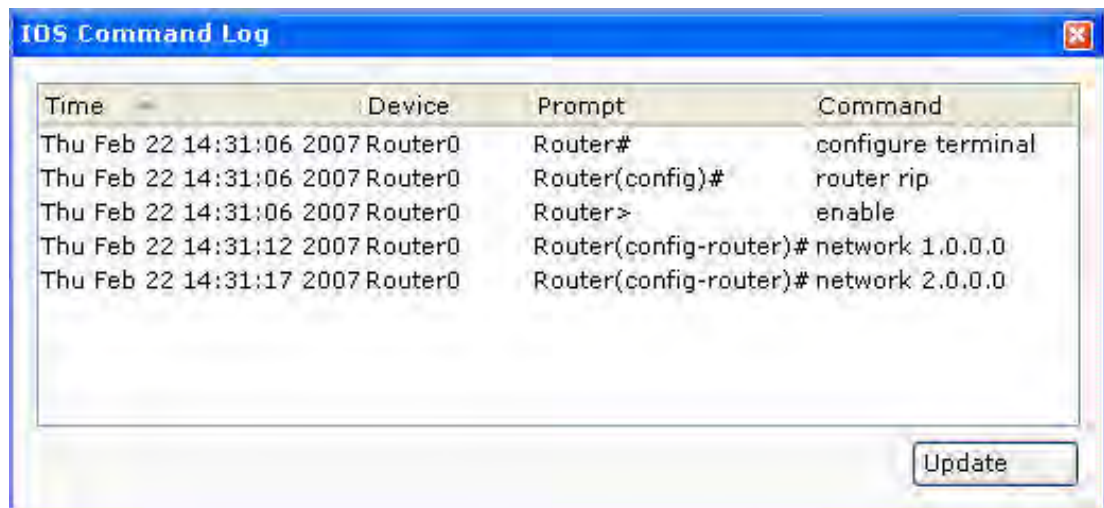
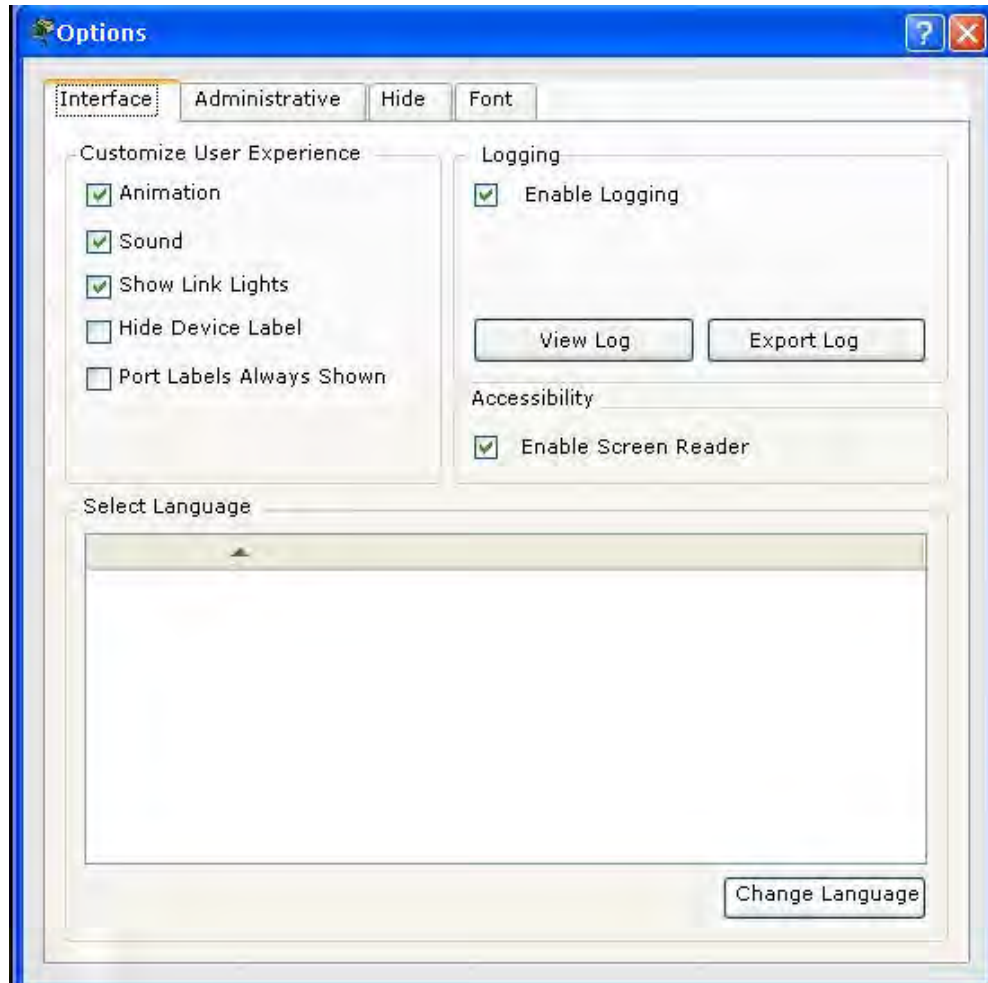
ترتیب Booting و بارگزاری تصویر IOS در مسیریاب ها و سوئیچها

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.

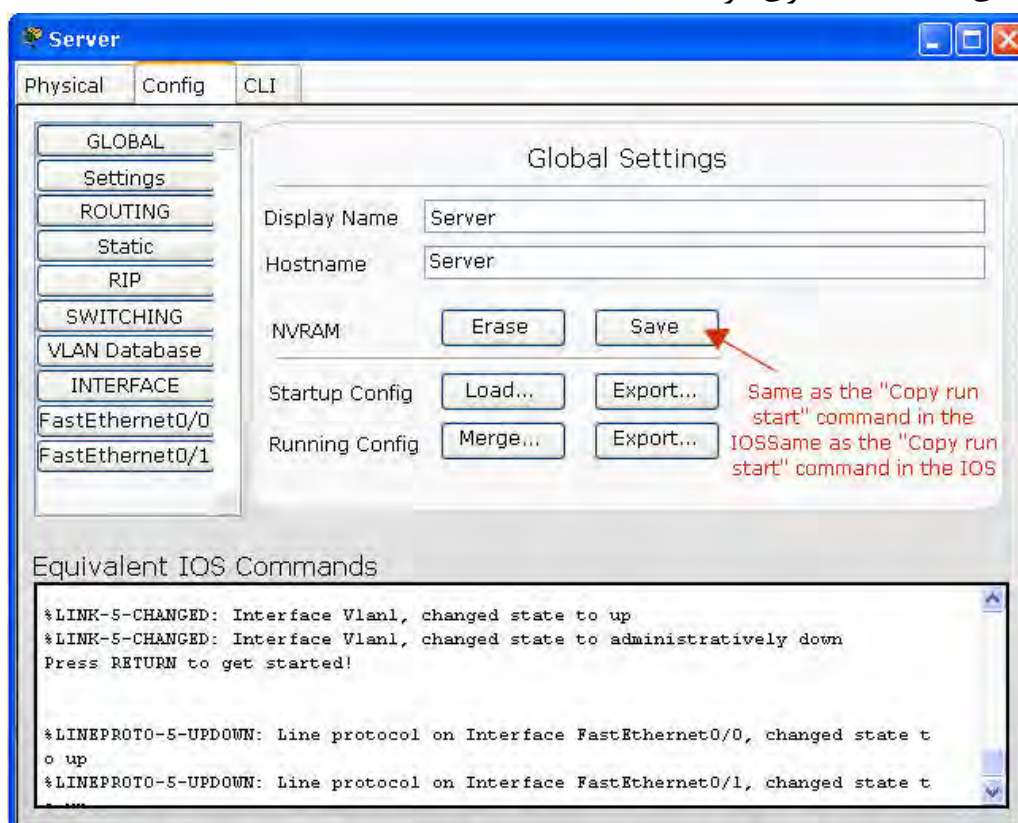


پیکربندی مسیریاب

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 واسطه، دکمه INTERFACE را کلیک تا لیست واسطه 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:

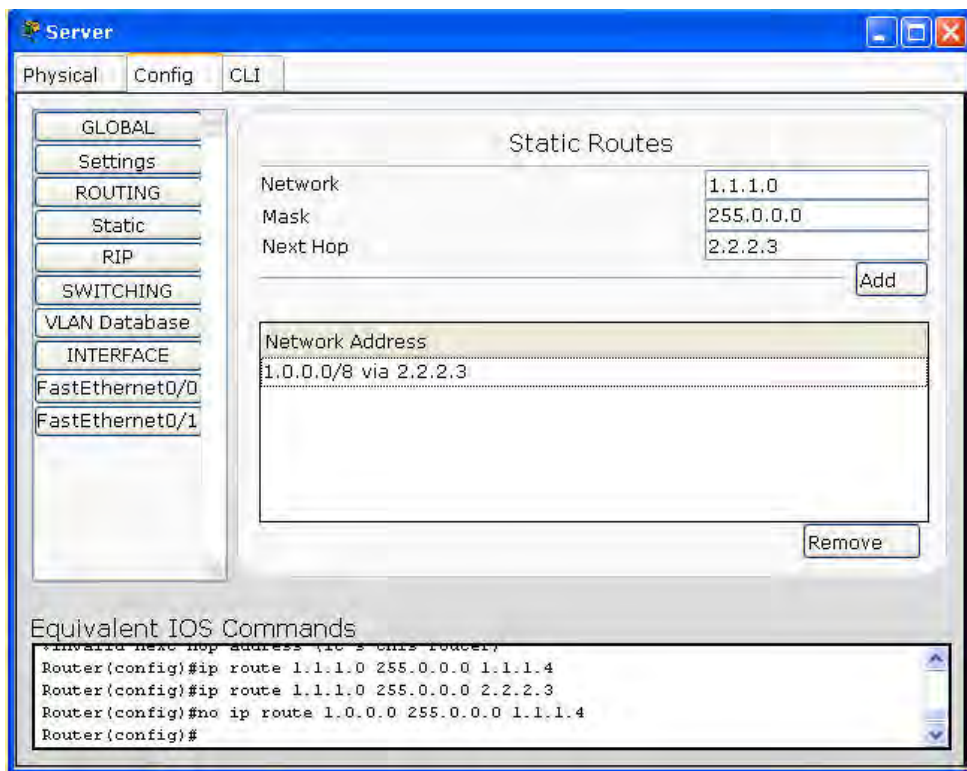


- حذف NVRAM (جایی که تنظیمات Startup ذخیره می شوند)
- ذخیره کردن تنظیمات در حال اجرای فعلی در NVRAM

- 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:

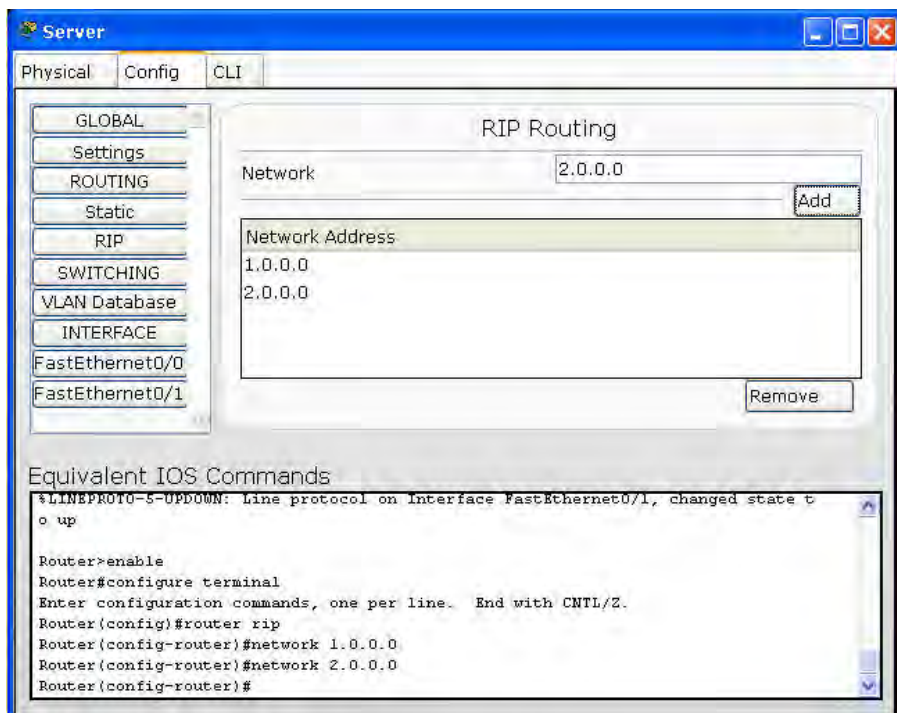
با انتخاب Static مسیریابی را می توان به روش استاتیک انجام داد. هر مسیر استاتیکی که اضافه می گردد نیازمند یک آدرس IP، ماسک زیرشبکه و آدرس گام بعدی می باشد. همچنین default gateway را نیز می توان تنظیم نمود.



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.

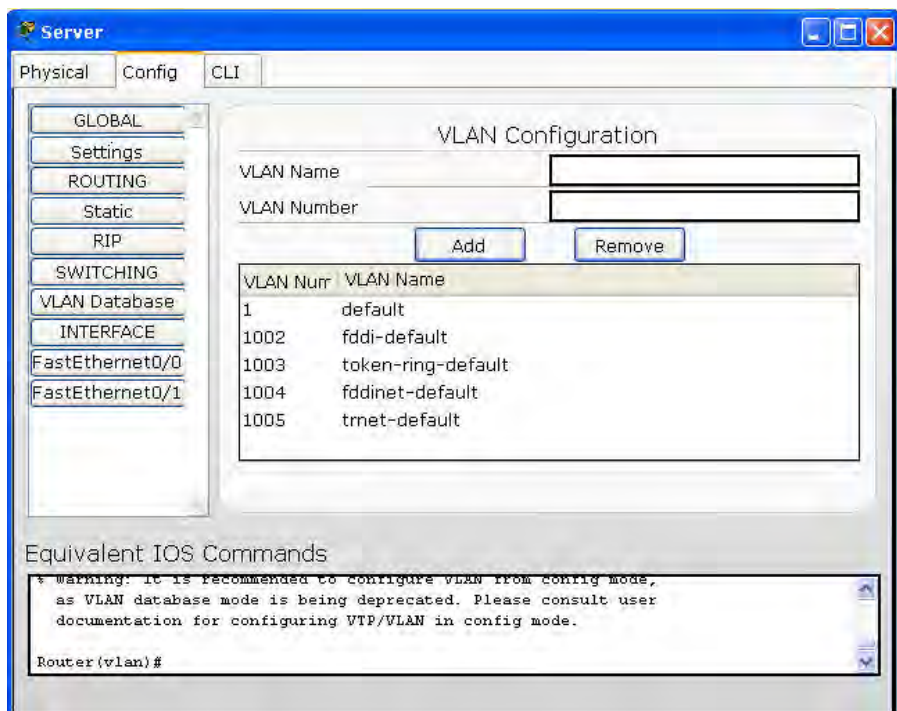


✓ فصل دوم: شبیه سازی شبکه توسط نرم افزار Packet Tracer



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 مسیر یاب 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 زیر شبکه 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 'Server' configuration window in Packet Tracer. The 'Config' tab is selected. On the left, a tree view shows the configuration hierarchy: GLOBAL, Settings, ROUTING, Static, RIP, SWITCHING, VLAN Database, INTERFACE, FastEthernet0/0, and FastEthernet0/1. The 'FastEthernet0/0' interface is selected, showing its configuration details.

FastEthernet0/0 Configuration:

- Port Status: ☒ On
- Bandwidth: ☒ Auto (100 Mbps)
- Duplex: ☒ Auto (Full Duplex / Half Duplex)
- MAC Address: 0000.0C9B.D2D8
- IP Address: 1.1.1.1
- Subnet Mask: 255.0.0.0

Equivalent IOS 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)#
  
```

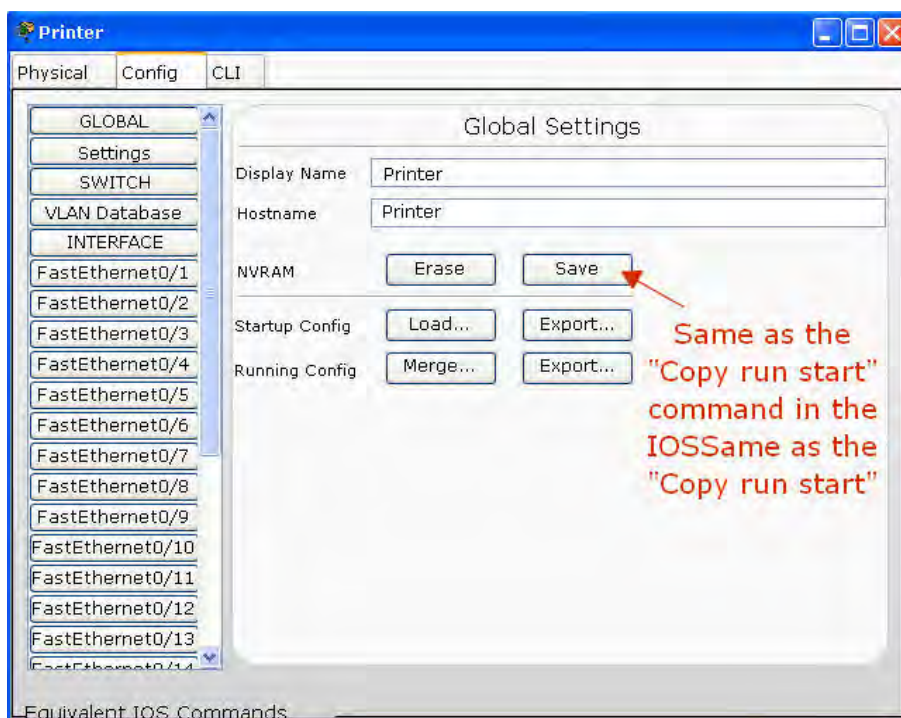
پیکربندی سوئیچ

برگه Config در سوئیچ سه سطح پیکربندی global، switching، interface را دارد. سطح global همانند مسیر یاب 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:

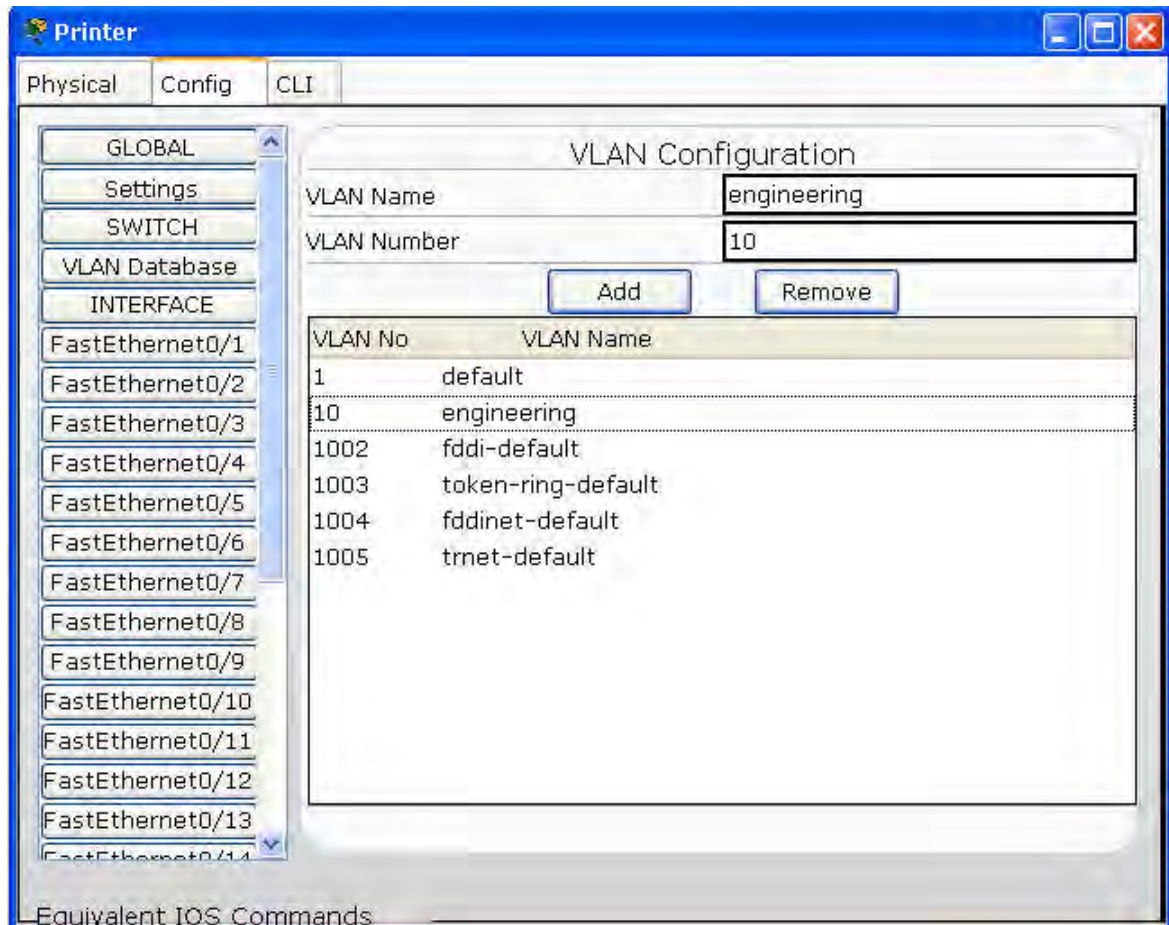
در تنظیمات Global می توان نام سوئیچ (جهت نمایش در فضای کاری) و نام میزبان (جهت نمایش در IOS) را تعیین نمود. همچنین می توانید فایل های پیکربندی سوئیچ را به شکل های مختلف دستکاری کرد:

- 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.

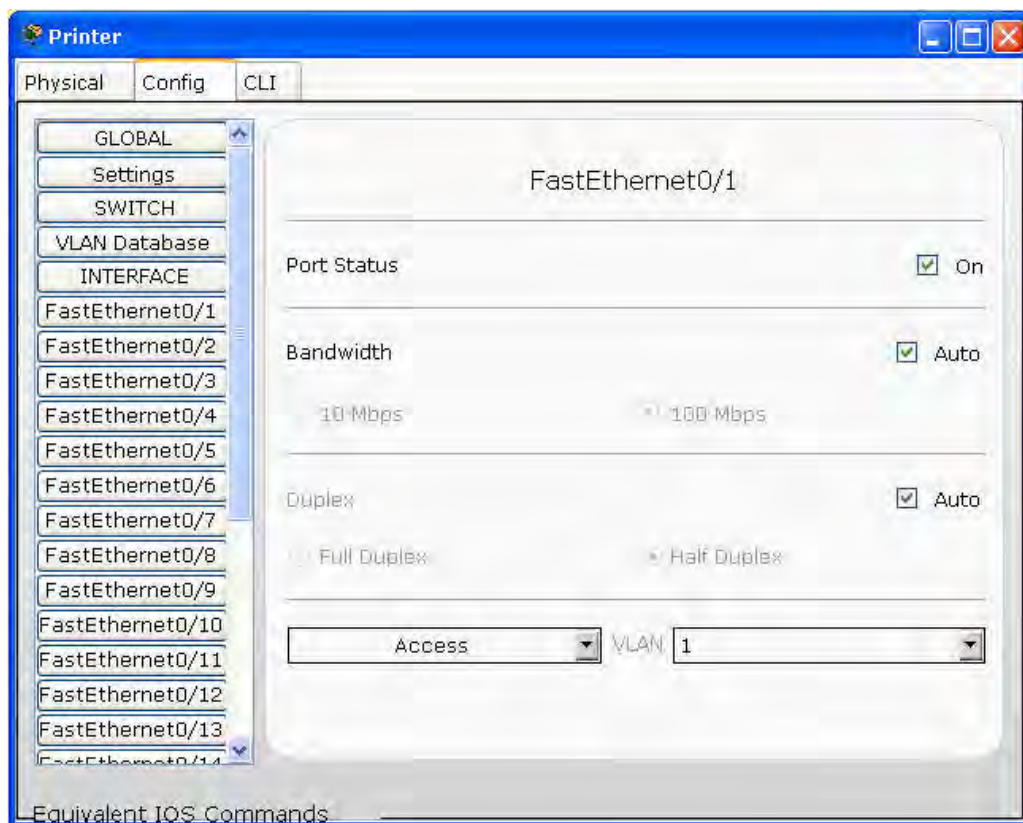


پیکربندی Interface:

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

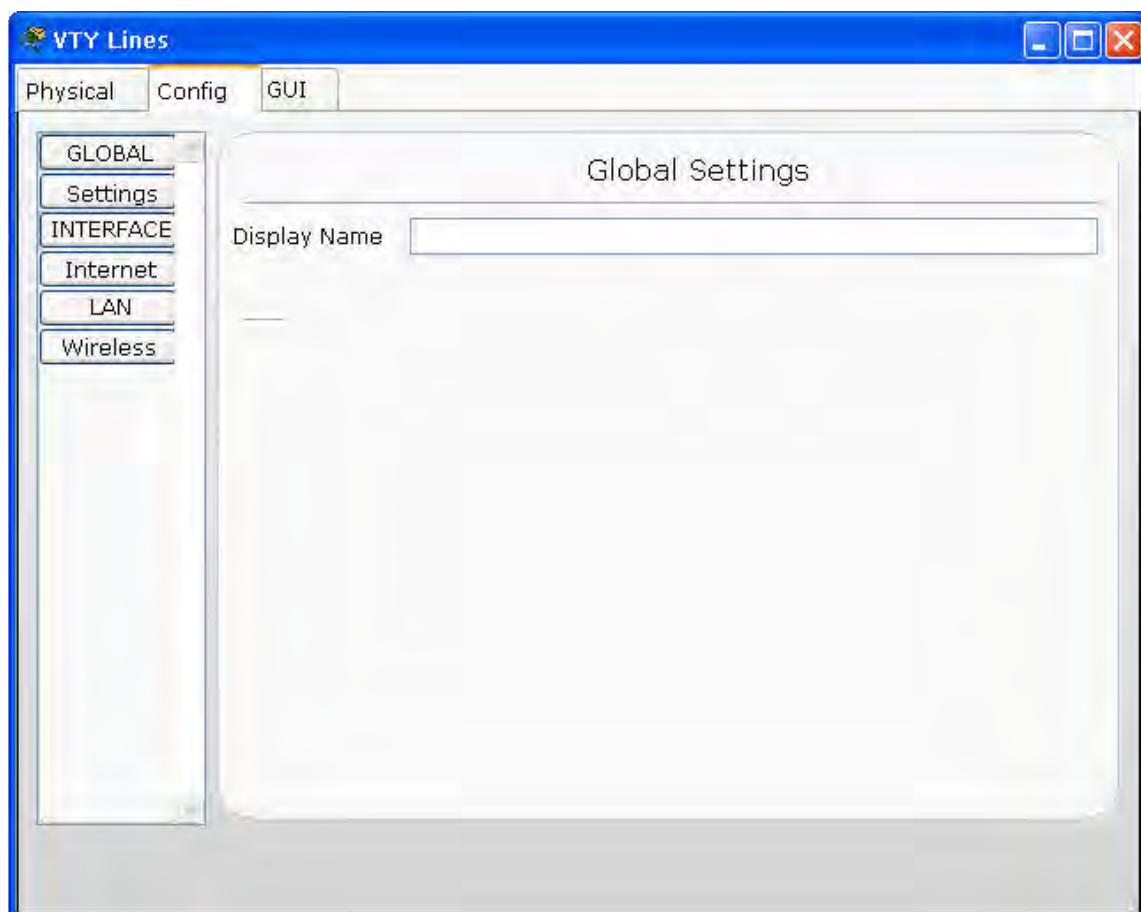




✓ فصل دوم: شبیه سازی شبکه توسط نرم افزار Packet Tracer

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 واسطه، INTERFACE را کلیک تا لیست واسطه ها نمایش داده شده، سپس واسطه مورد نظر را انتخاب کنید.



تنظیمات Global:

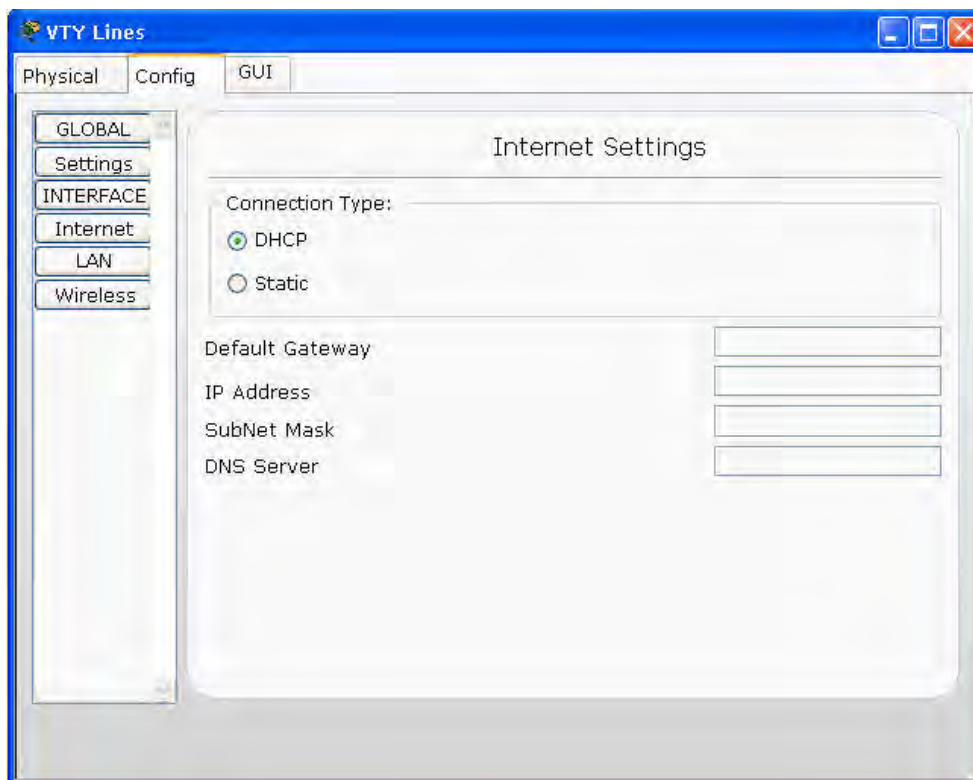
در تنظیمات Global می توان نام نمایش داده شده در صفحه را تغییر داد.

تنظیمات واسطه 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.

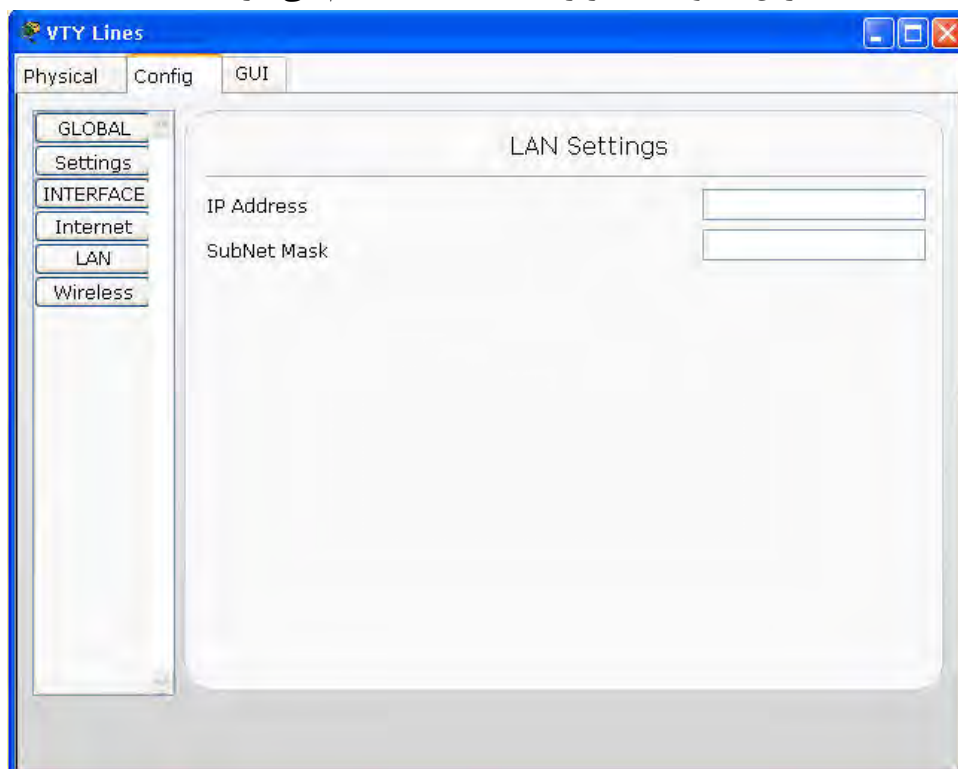


✓ فصل دوم: شبیه سازی شبکه توسط نرم افزار Packet Tracer



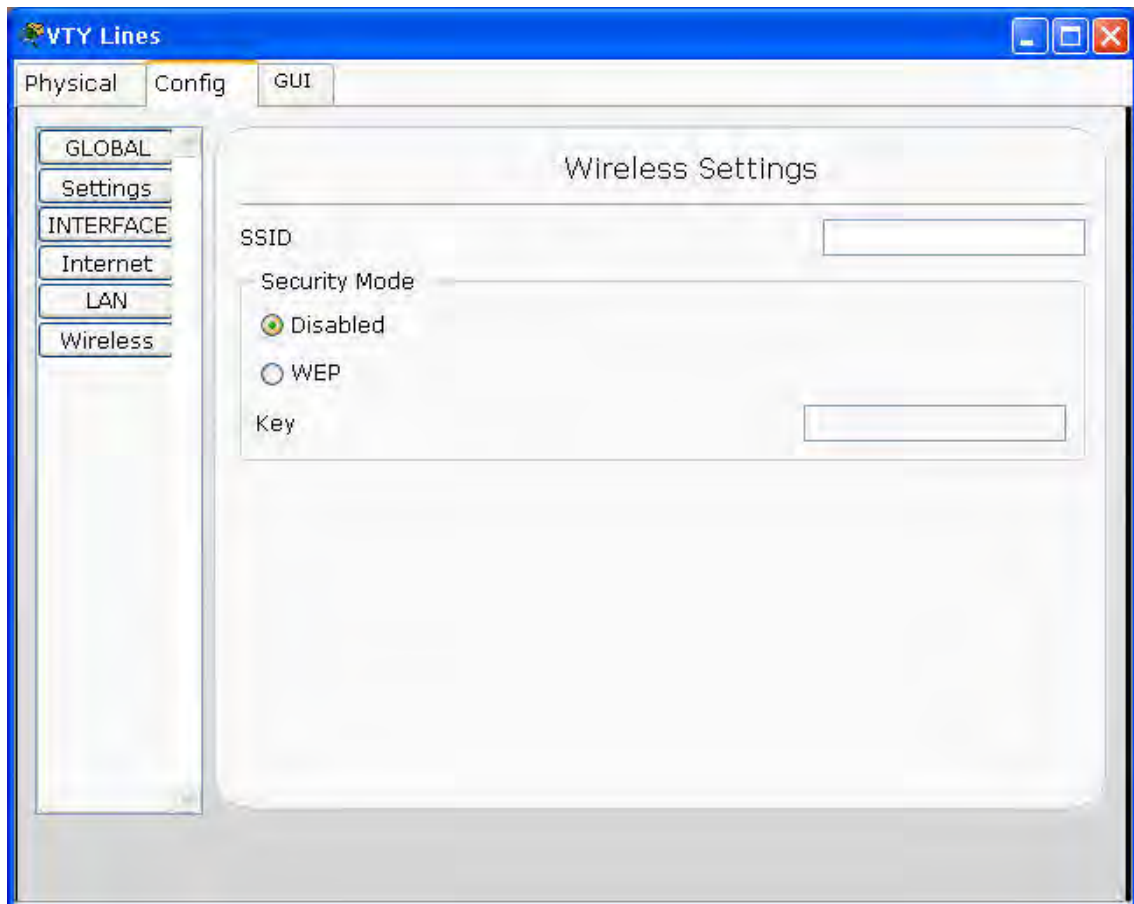
تنظیمات واسط LAN:

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:

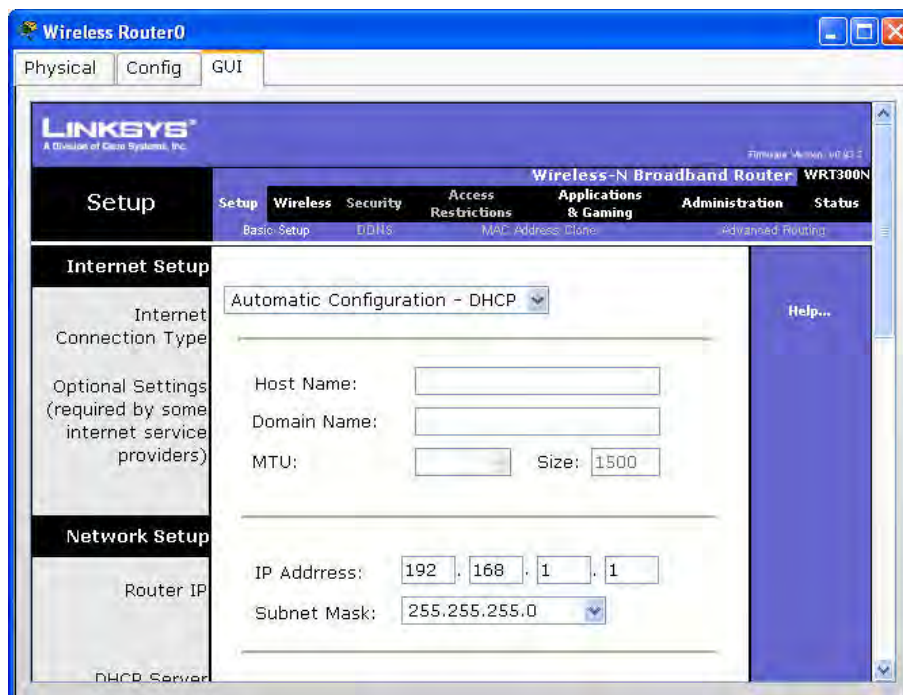
برگه GUI، پیکربندی ها و تنظیمات مشابه برگه Config و همچنین تعدادی ویژگی دیگر برای port forwarding و مدیریت دارد. برای اعمال تنظیمات می بایست بر روی دکمه Save Settings کلیک کنید.

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.

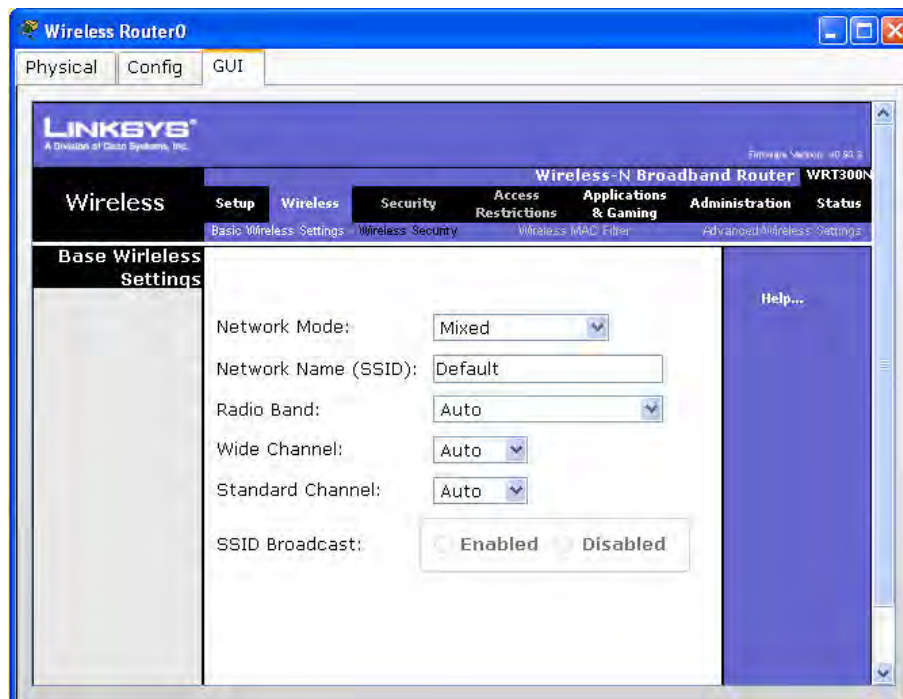


✓ فصل دوم: شبیه سازی شبکه توسط نرم افزار Packet Tracer



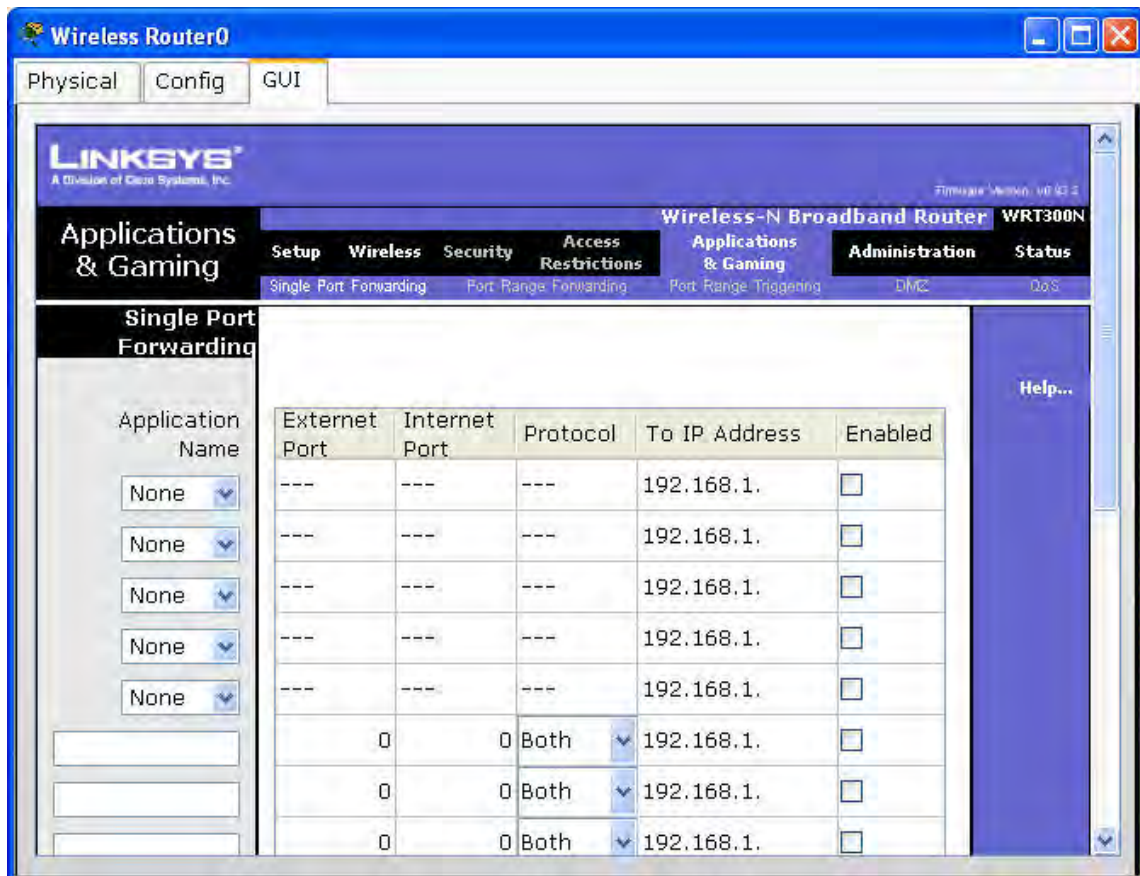
پیکربندی Wireless:

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.



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 پورتهای است که مسیریاب Linksys از سمت WAN به آن گوش می دهد. Internal پورتهای است که بسته ها را به سرور محلی شما ارسال می کند.

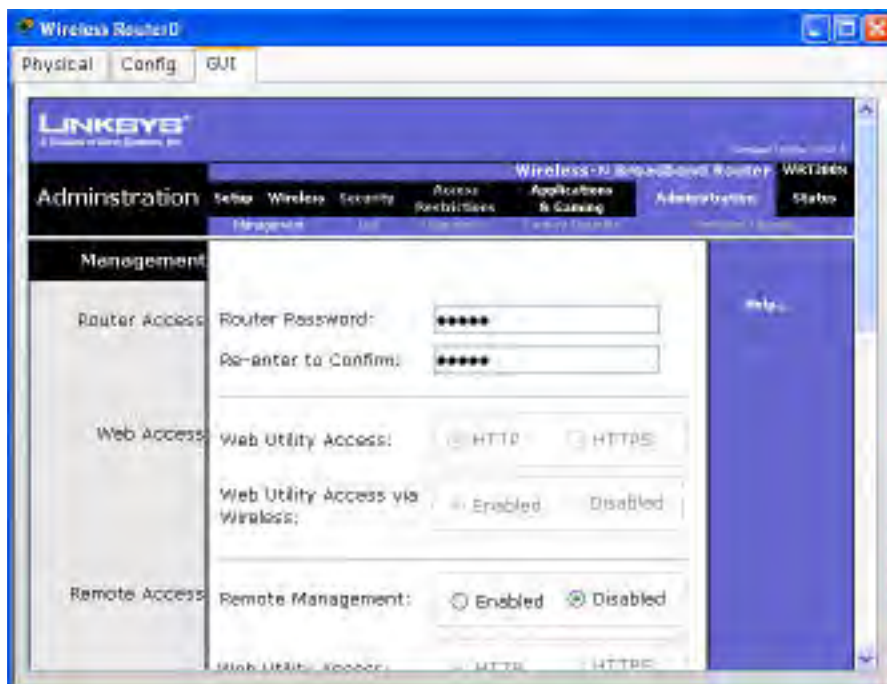


Administration Management:

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.

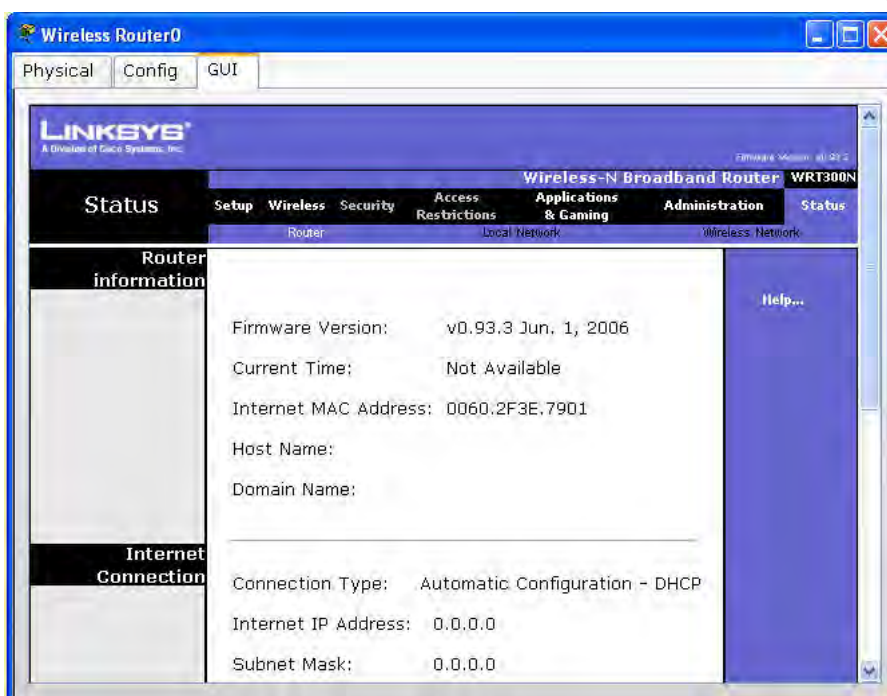


✓ فصل دوم: شبیه سازی شبکه توسط نرم افزار Packet Tracer



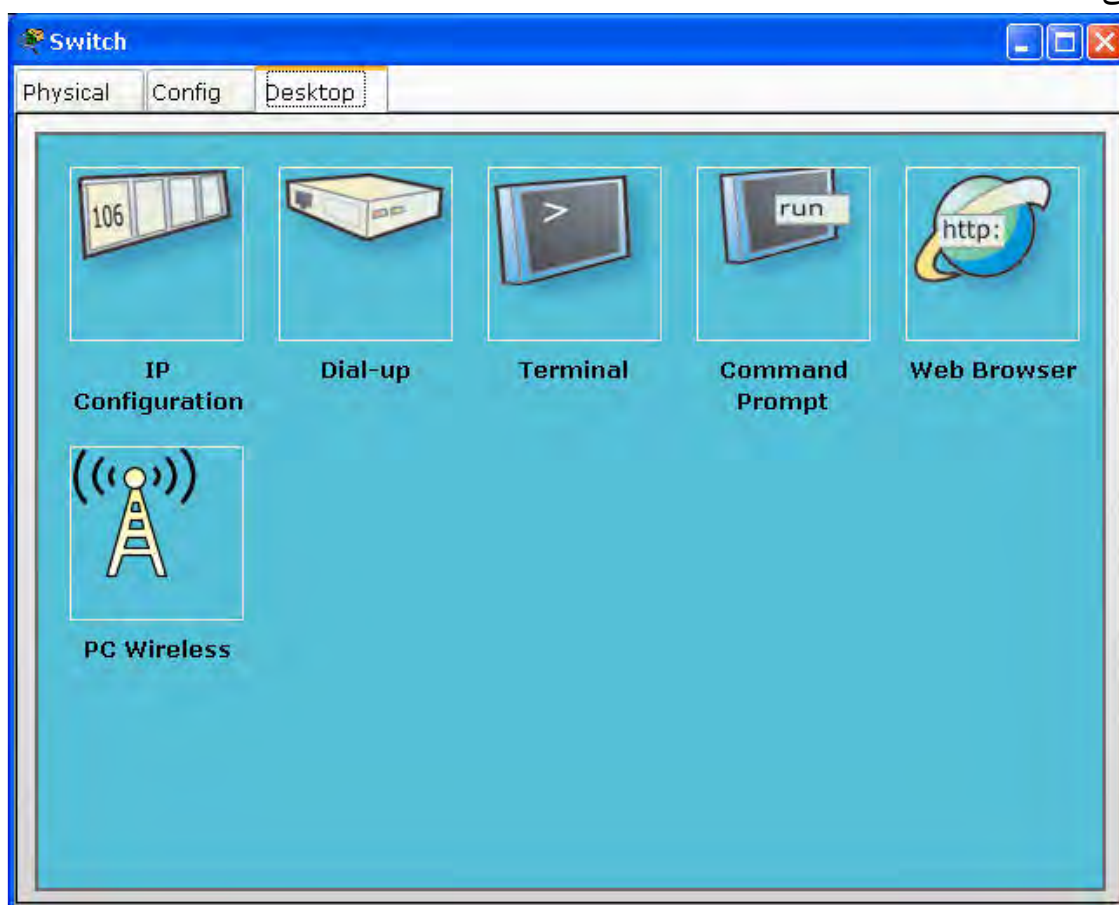
:Status

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 dial-up، استفاده از پنجره terminal، باز کردن واسطه خط فرمان، بازکردن مرورگر وب و پیکربندی تنظیمات بی سیم Linksys فراهم می کند.



تنظیمات Global:

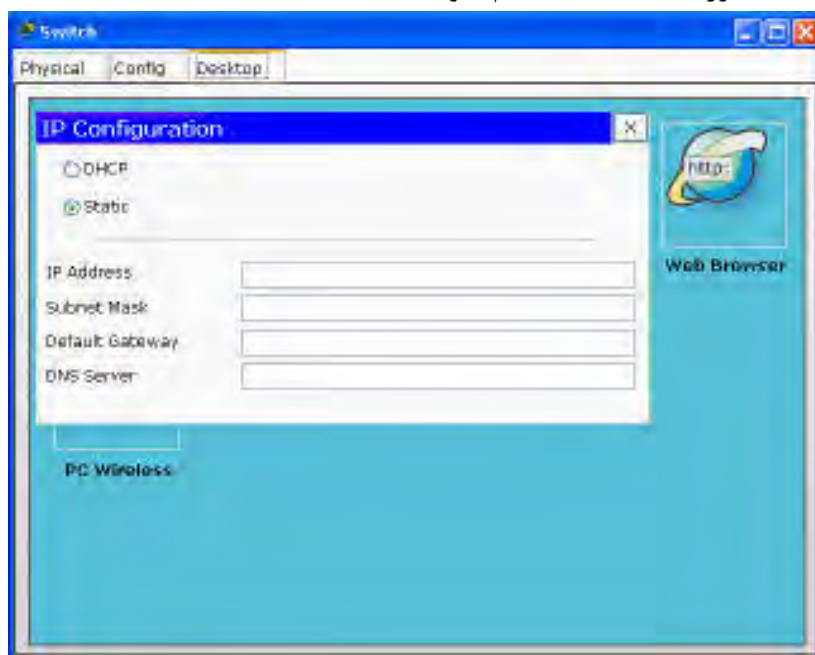
در تنظیمات global نام نمایش داده شده در صفحه، تنظیمات آدرس IP به صورت استاتیک یا پویا، و نیز Gateway و DNS Server را نیز می توان مشخص نمود.

پیکربندی Interface:

رایانه ها می توانند یک واسطه 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 واسطه می توان تنظیم کرد که البته با توجه به نوع واسطه 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:

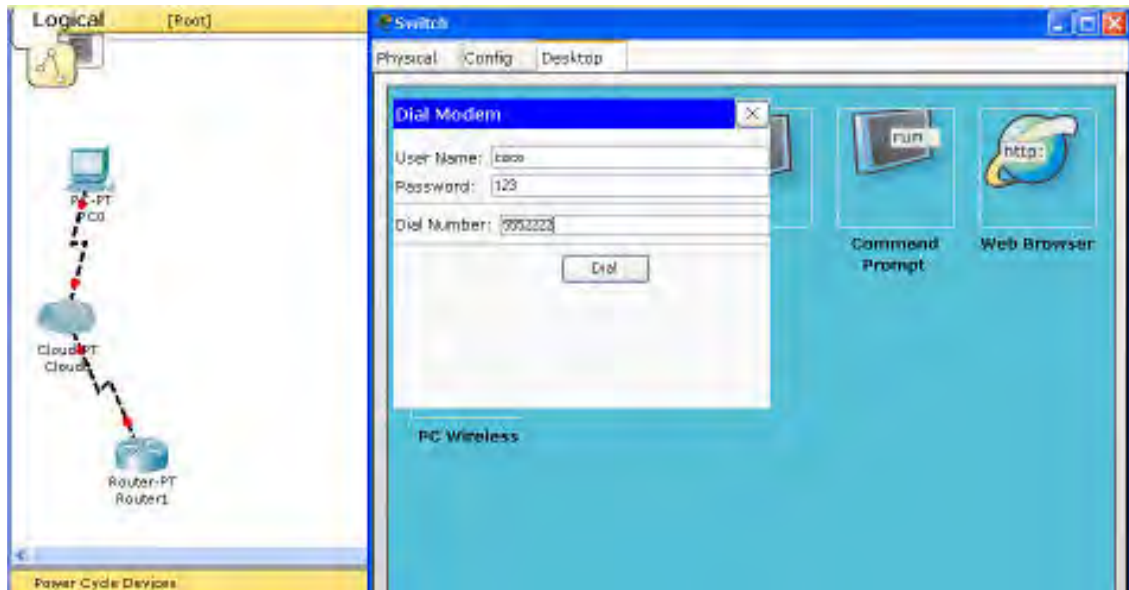
در برگه Desktop، بر روی آیکن Dial-up کلیک کنید تا ابزار آن باز شود. اتصال مودم را می توان با اتصال PC به یک ابر که به روتر متصل است برقرار نمود. ابر مانند یک شرکت تلفن بین PC و مسیریاب عمل می کند. برای برقراری تماس باید شرایط مختلفی برقرار باشد.

- 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

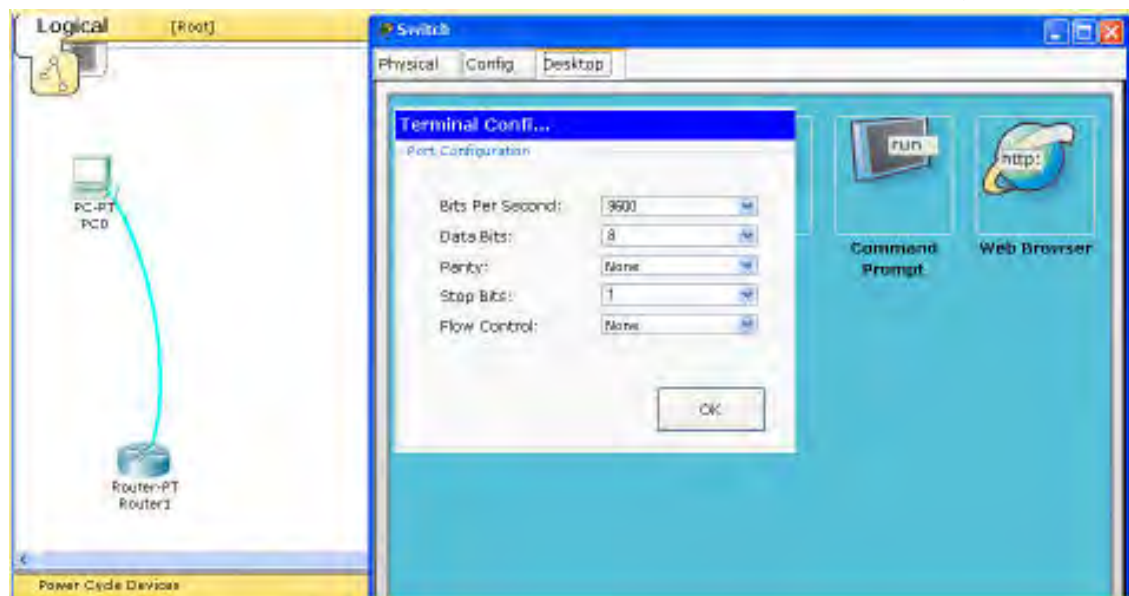
- شما نام کاربری و کلمه عبور و شماره اتصال را وارد کرده اید.

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.



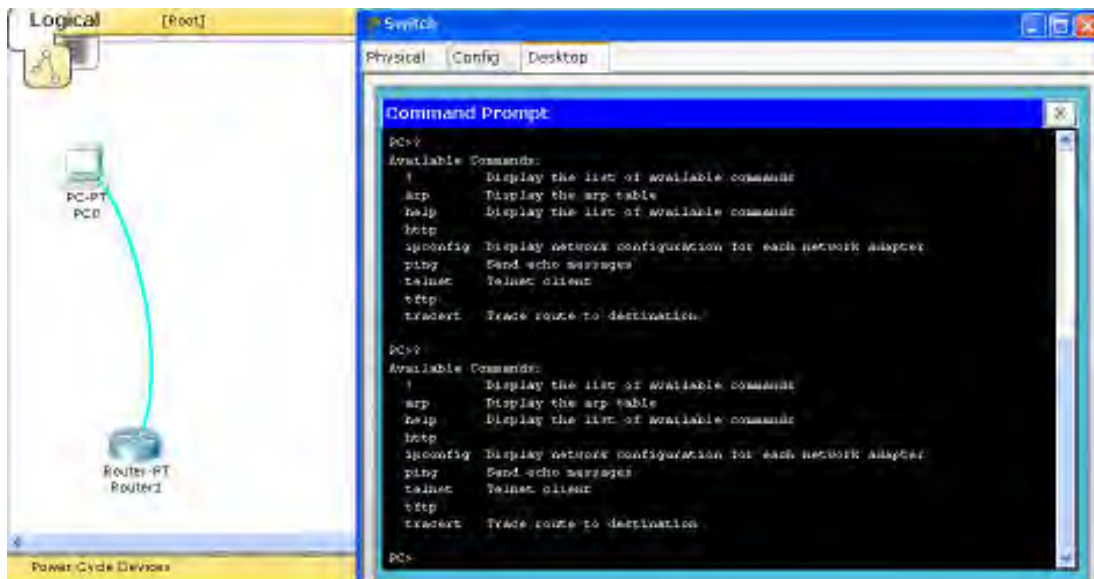
ابزار خط فرمان:

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

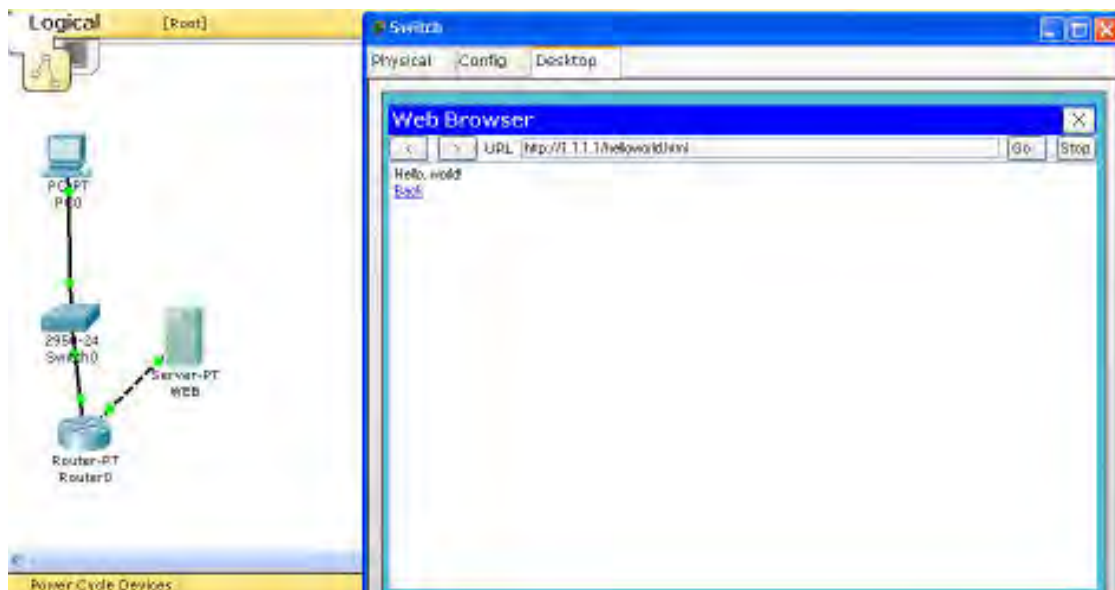


ابزار مرورگر وب:

در برگه Desktop با کلیک روی دکمه Web Browser مرورگر وب را باز نمائید. 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)

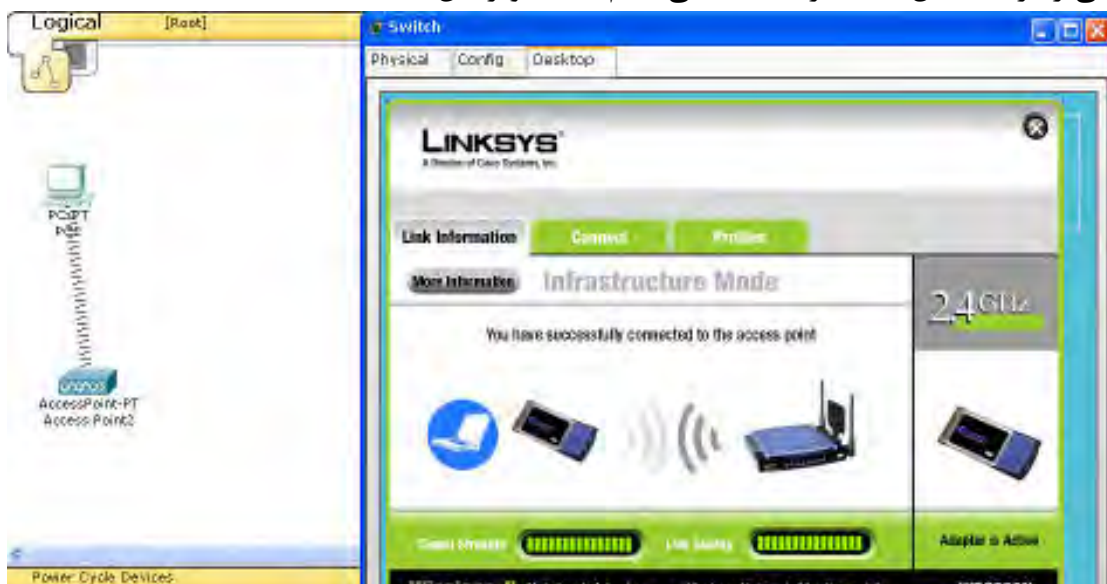


✓ فصل دوم: شبیه سازی شبکه توسط نرم افزار Packet Tracer



ابزار PC Wireless:

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.

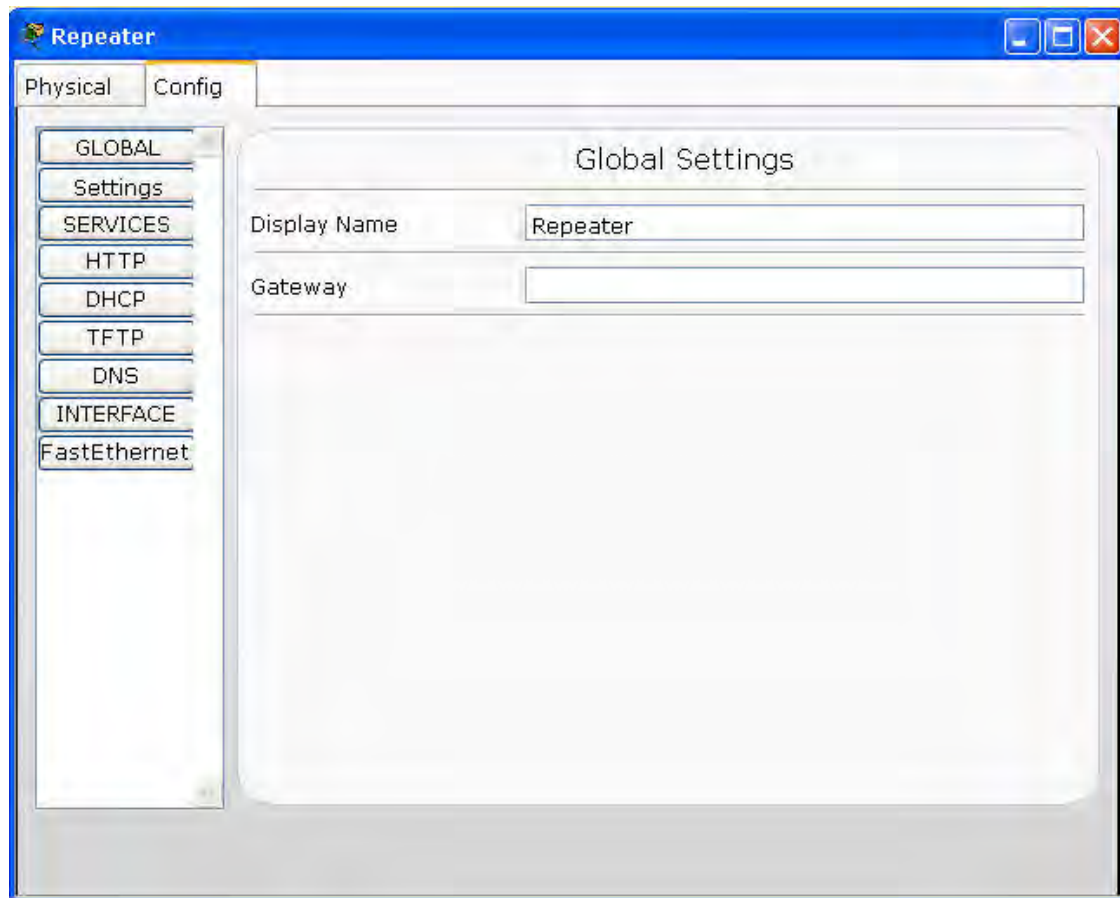




✓ فصل دوم: شبیه سازی شبکه توسط نرم افزار Packet Tracer

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.

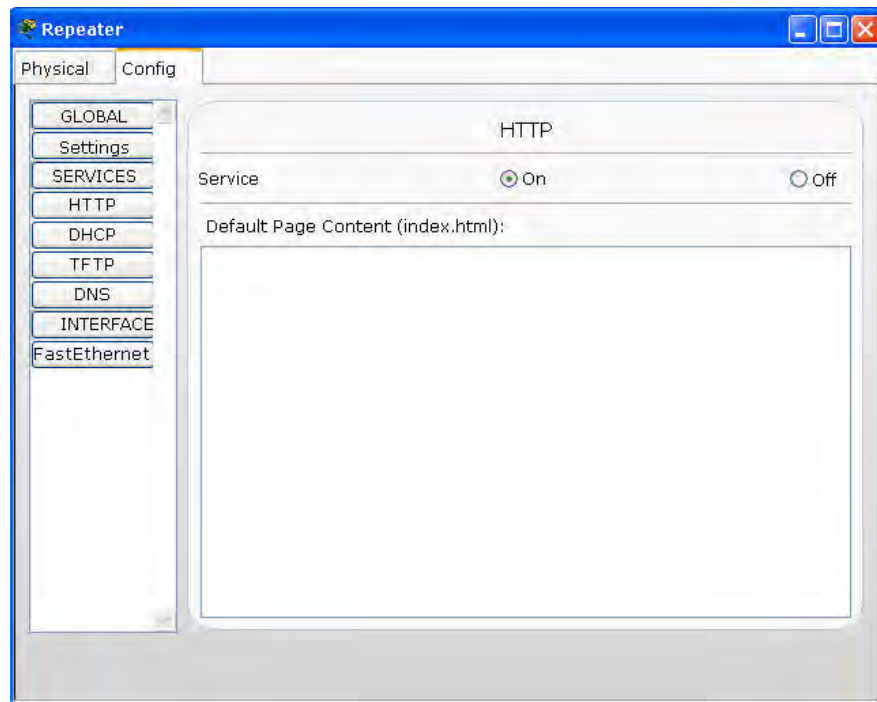


تنظیمات Global:

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

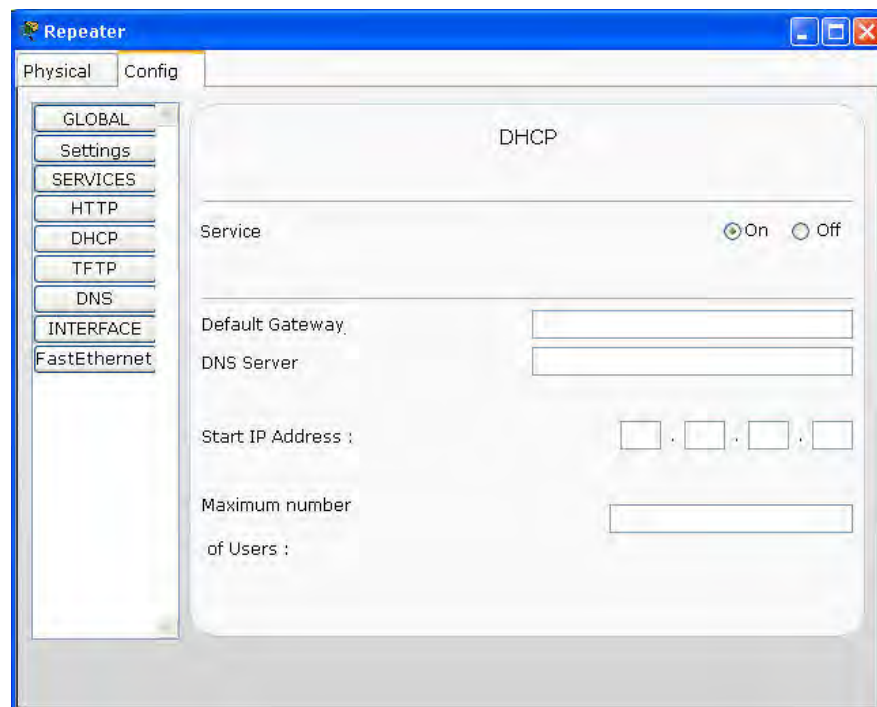
پیکربندی سرویس HTTP:

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.



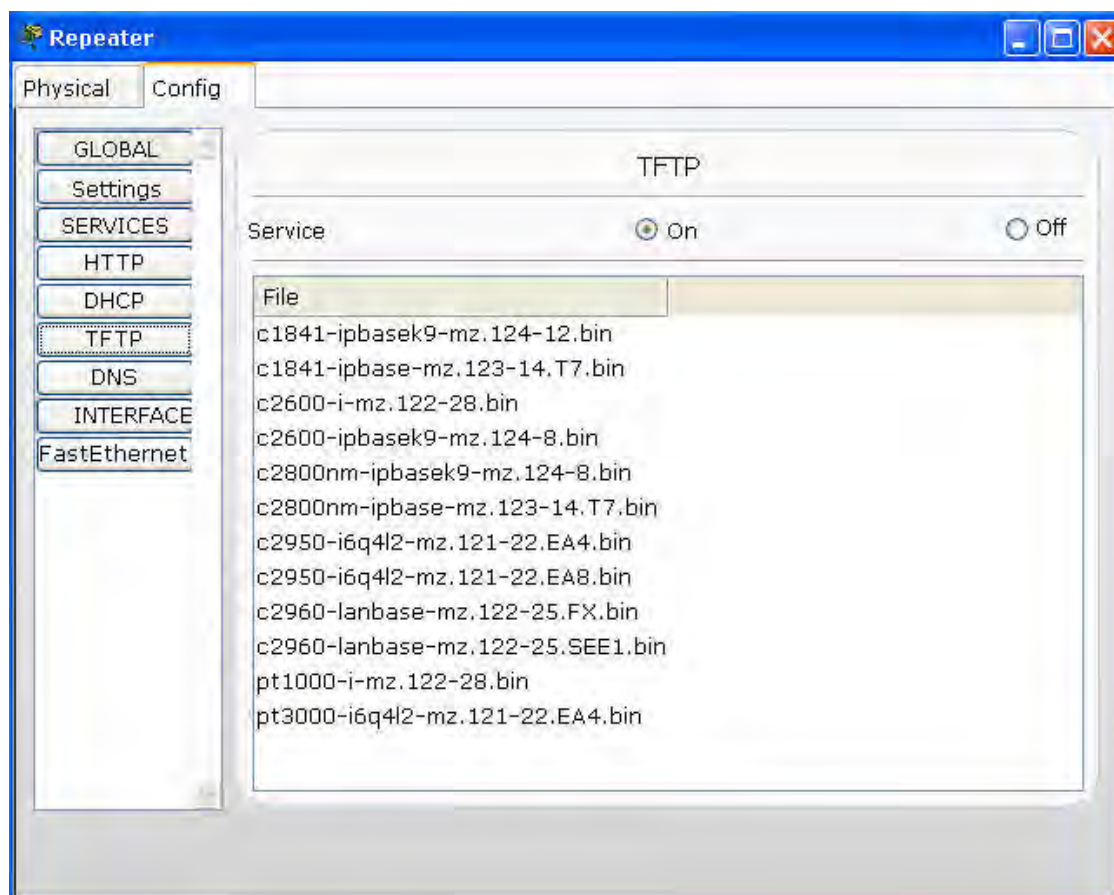
پیکربندی سرویس DHCP:

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.



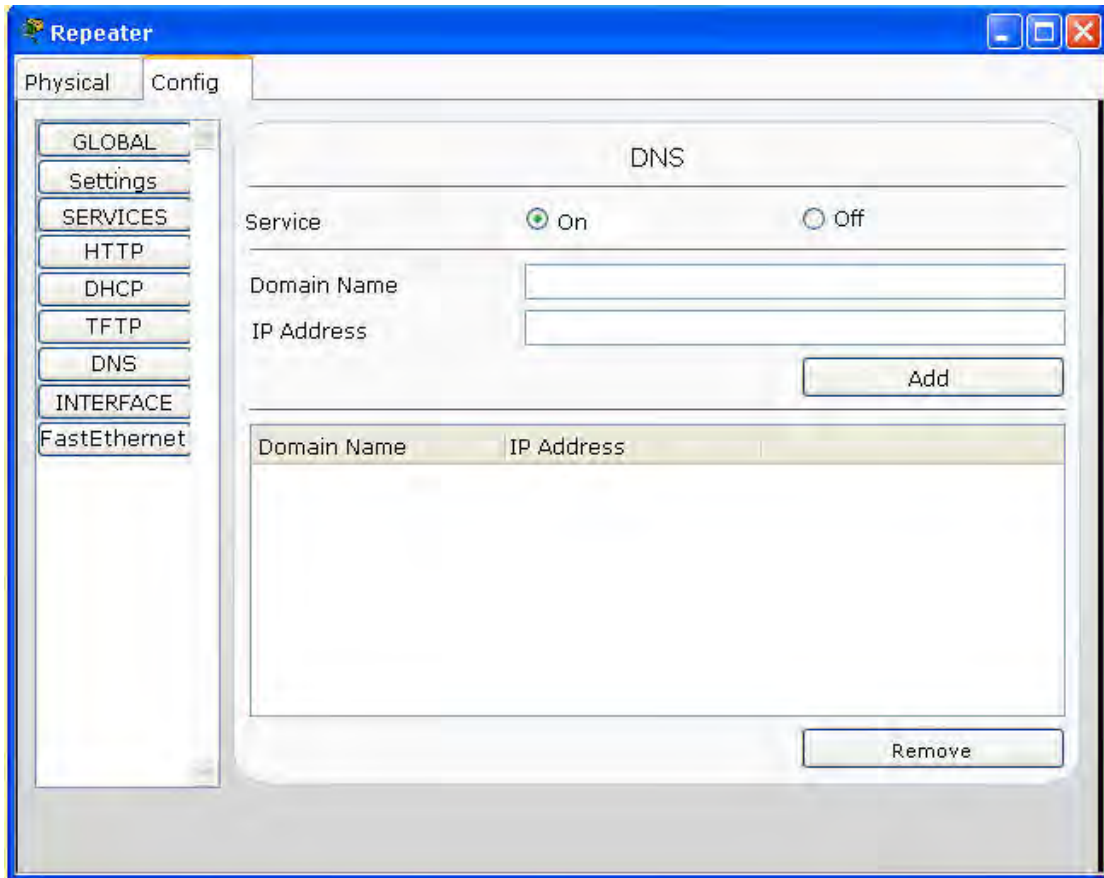
پیکربندی سرویس TFTP:

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.



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

پیکربندی ابر (cloud)

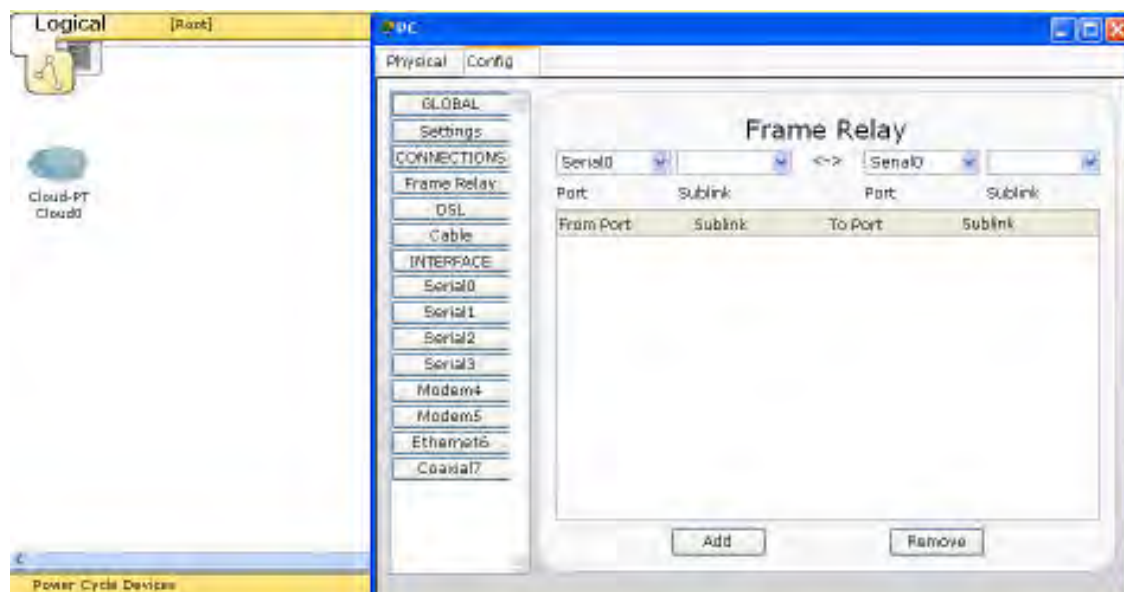
برگه Config سه سطح تنظیمات global، connections و interface را فراهم می کند که برای پیکربندی هر سطح باید بر روی دکمه های GLOBAL، CONNECTIONS یا INTERFACE کلیک کنید.

تنظیمات Global:

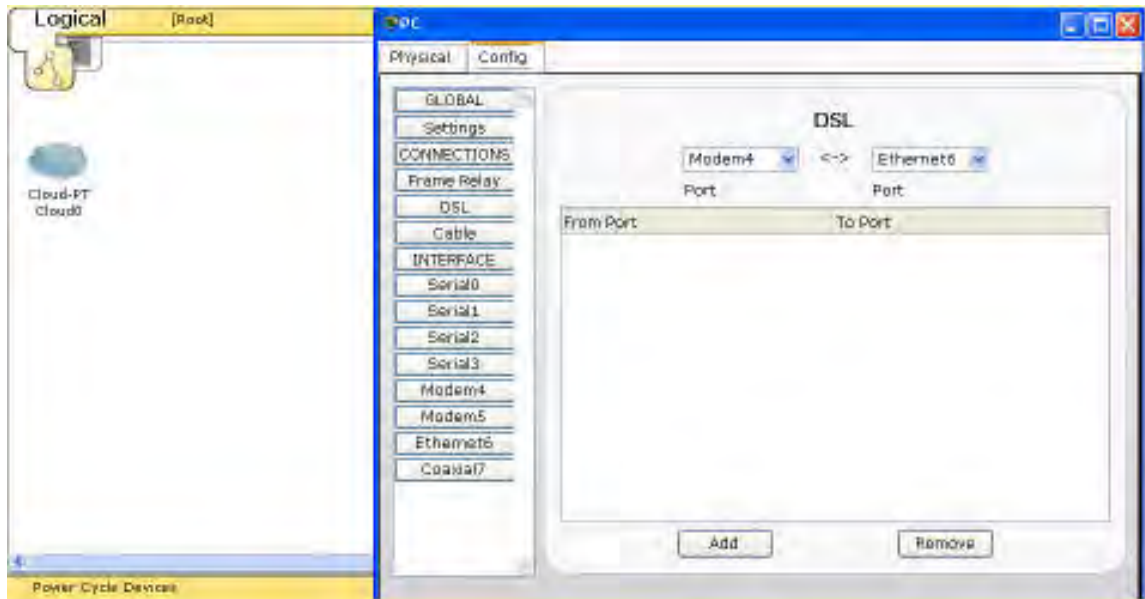
برای تغییر نام ابر استفاده می شود.

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.

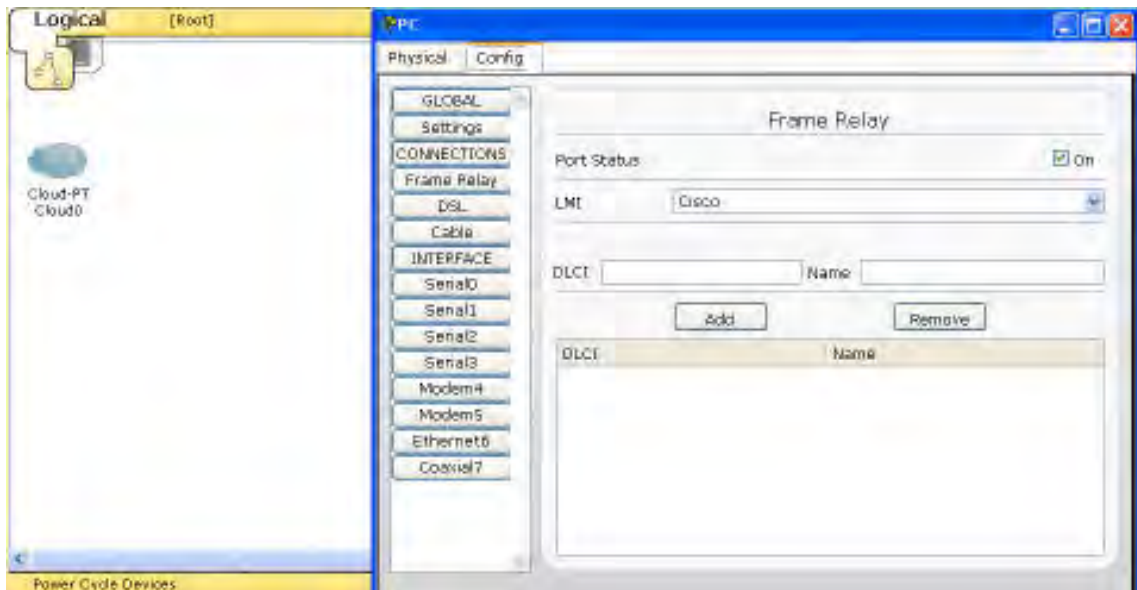


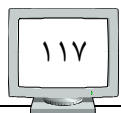
همچنین می توانید از قسمت DSL یا Cable برای برقراری اتصال بین پورت های مودم (برای DSL) یا پورت های کواکسیال (برای Cable) به پورت های اترنت استفاده کنید.



پیکربندی Interface:

ابر می تواند ۴ نوع واسط مودم، اترنت، کواکسیال 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

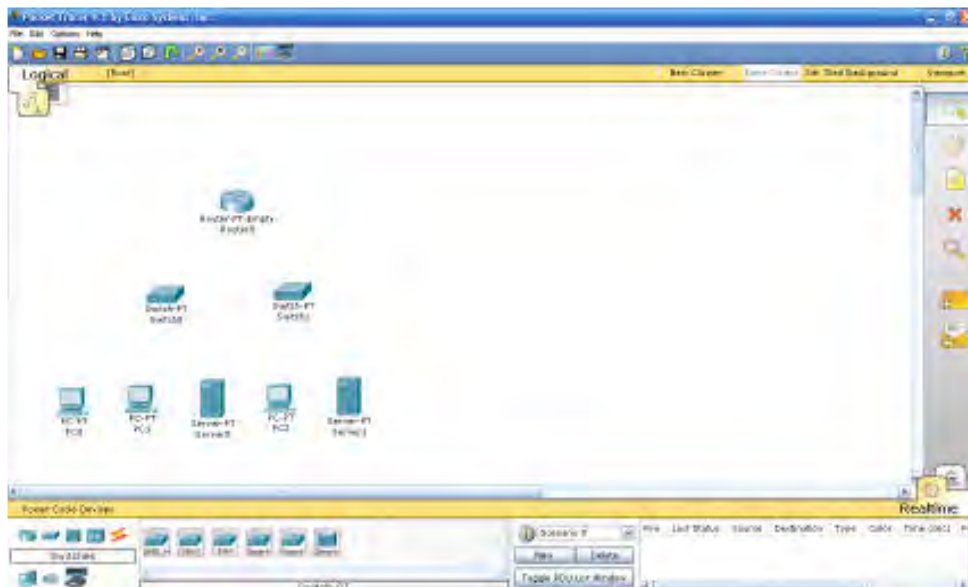
این مودم گزینه قابل تنظیمی ندارد.

Cable Modem

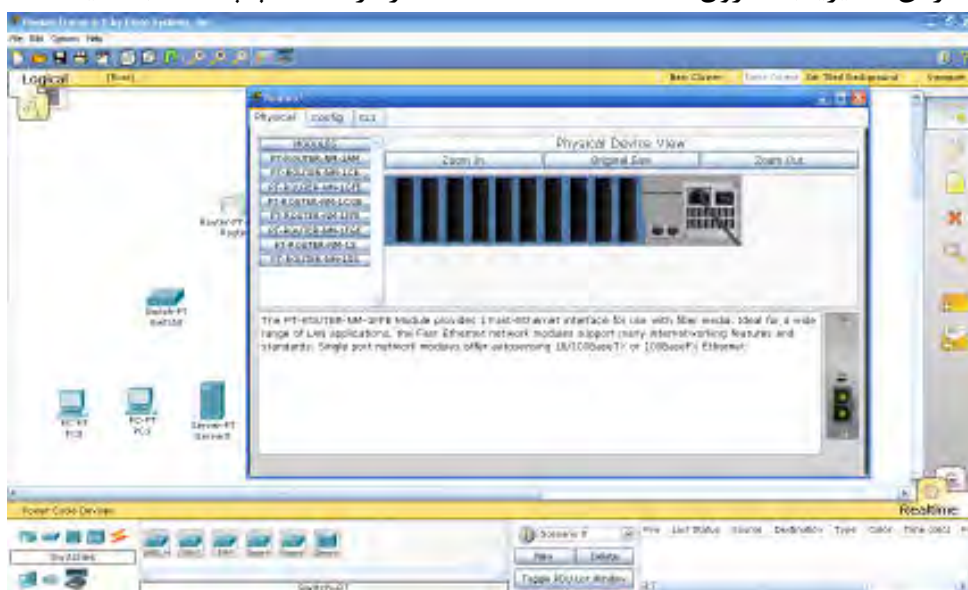
این مودم گزینه قابل تنظیمی ندارد.

مثال عملی) قسمت اول - ایجاد یک شبکه

در این قسمت قصد داریم یک شبکه فرضی با امکانات و ویژگی های مختلف ایجاد کنیم. برای این منظور ابتدا دستگاه های مورد نیاز را وارد فضای کار کنید. این دستگاه ها شامل ۳ رایانه، ۲ سرور، ۲ سوئیچ و یک مسیریاب می باشند.

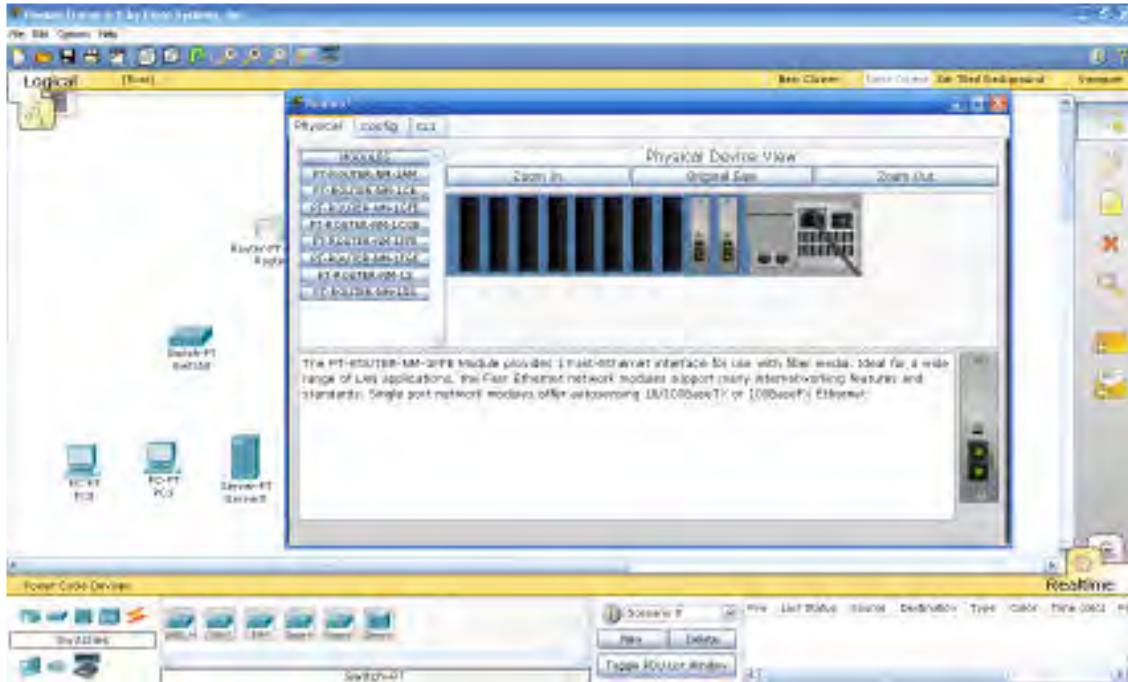


مسیریاب را از نوع Router-PT-Empty انتخاب کرده تا بتوان ماژول های مورد نیاز را به صورت دستی به آن اضافه نمود. بنابراین روی آن کلیک کرده تا صفحه تنظیمات آن باز شود. پس از خاموش کردن مسیریاب، ماژول PT-Router-NM-1FFE را از سمت چپ انتخاب کنید.

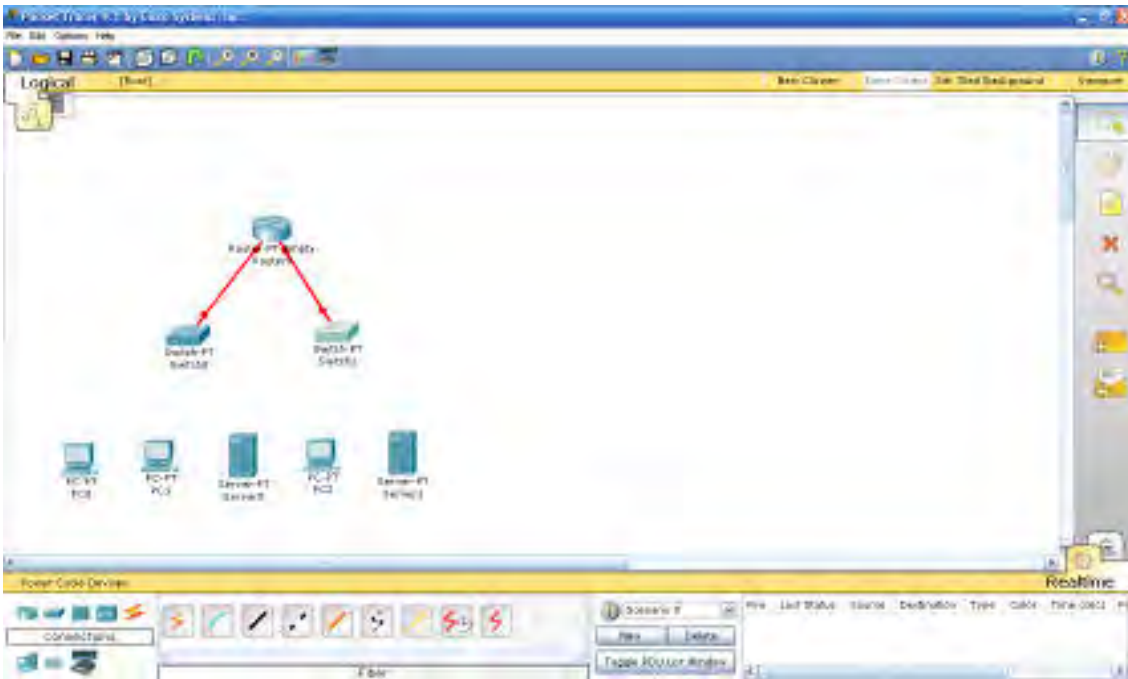


✓ فصل دوم: شبیه سازی شبکه توسط نرم افزار Packet Tracer

این مازول را با درگ کردن در دو شیار از روتر قرار داده و سپس روتر را روشن کنید.

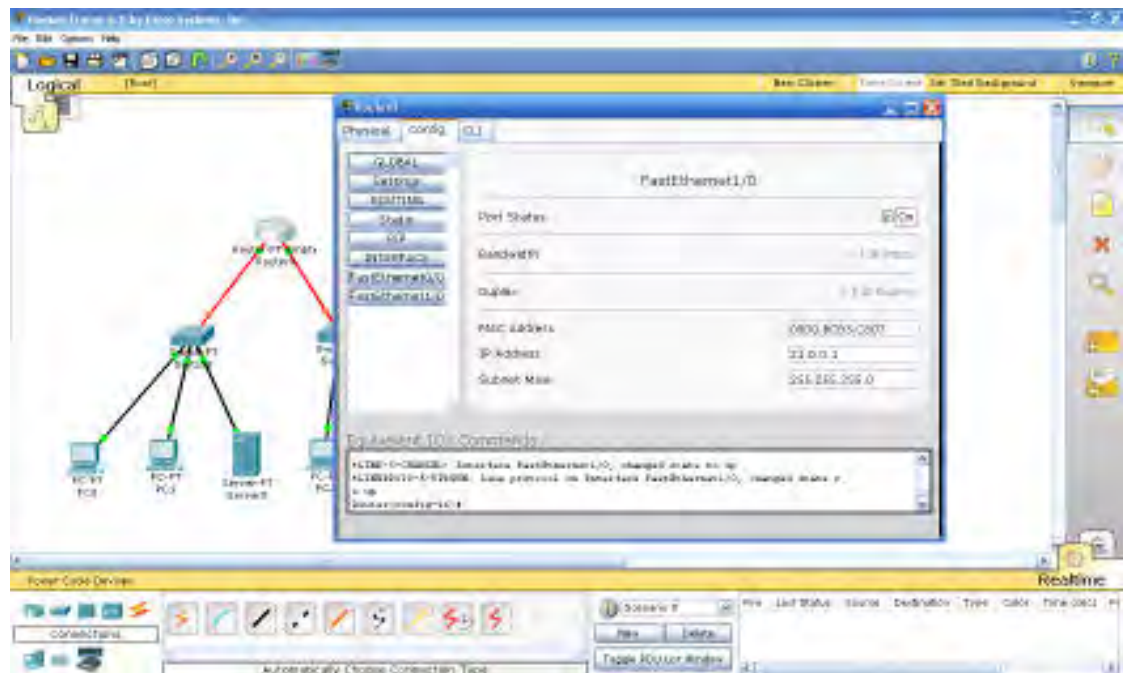
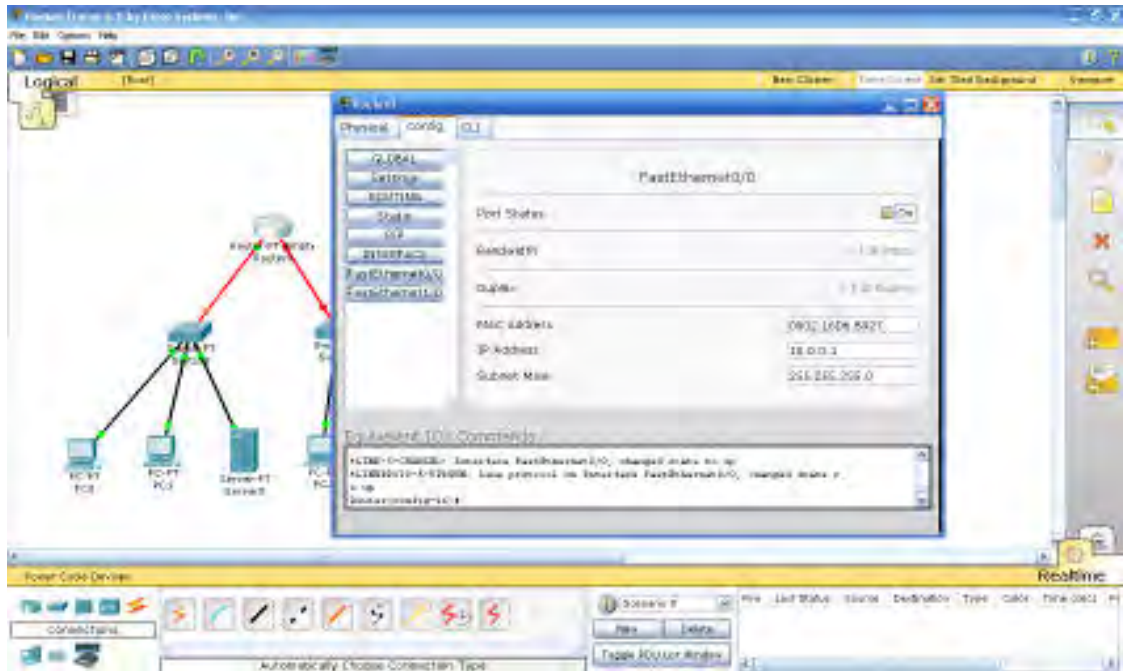


حال با استفاده از کابل فیبرنوری، اتصال بین مسیر یاب و سوئیچ ها را برقرار نمایید.



سپس با استفاده از آیکن اتصال اتوماتیک، اتصال سایر دستگاه ها را به سوئیچ مطابق شکل برقرار کنید. برای فعال کردن اتصال مسیریاب، می بایست واسطه های آن را پیکربندی نمود. بنابراین روی

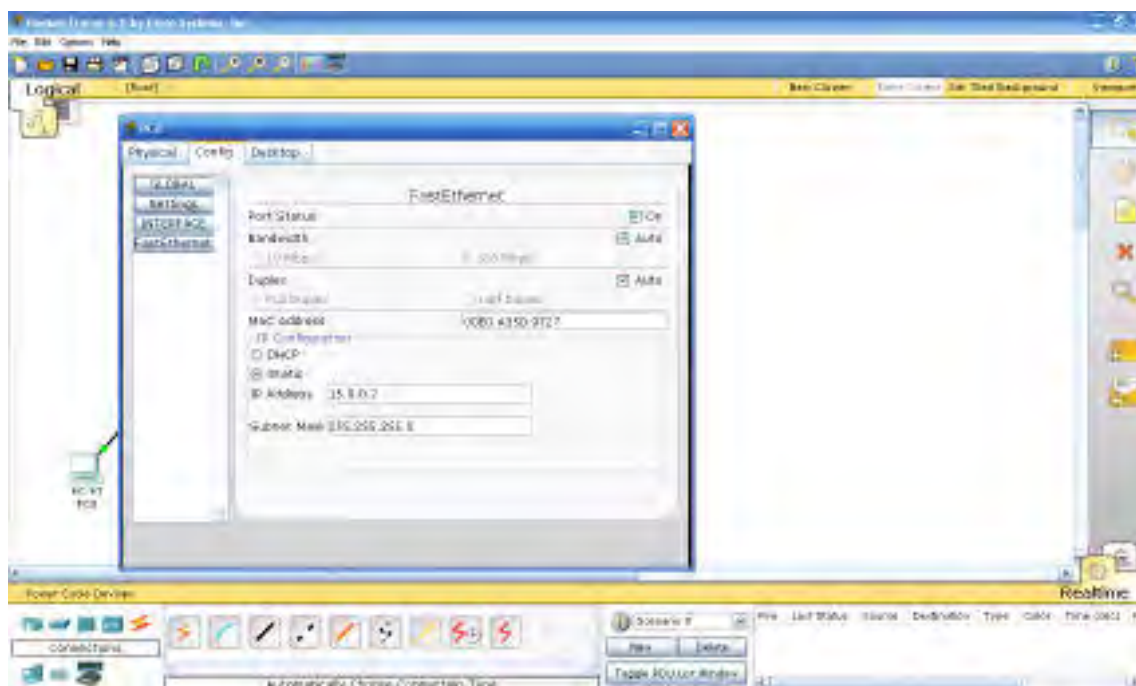
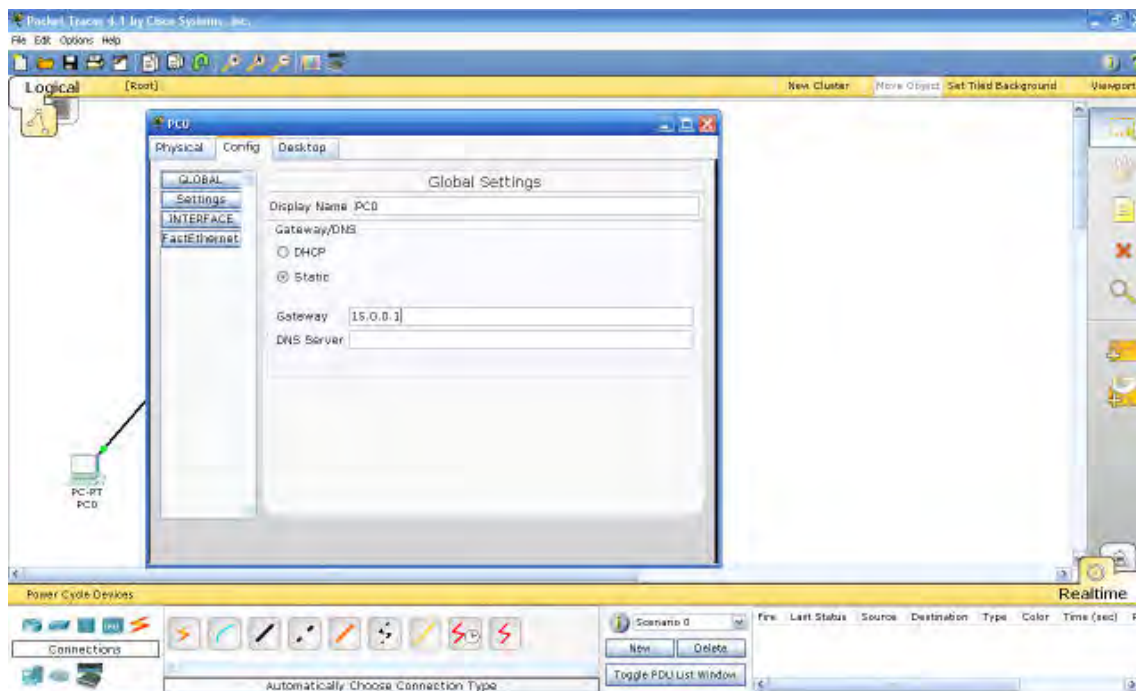
مسیریاب کلیک و در برگه config به ترتیب واسط های FastEthernet0/0 و FastEthernet1/0 را انتخاب کرده و تنظیمات را مطابق شکل انجام دهید.



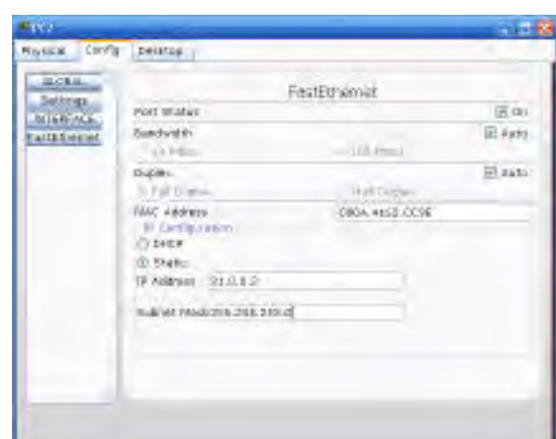
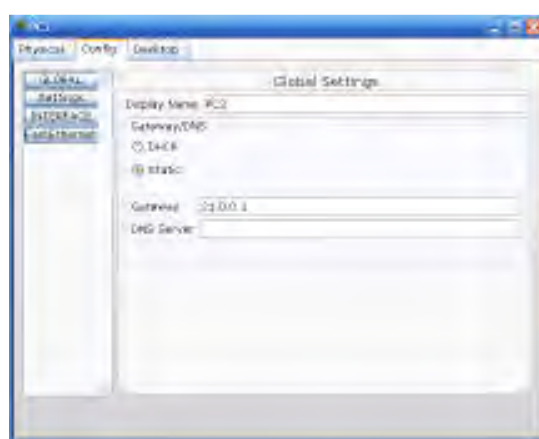
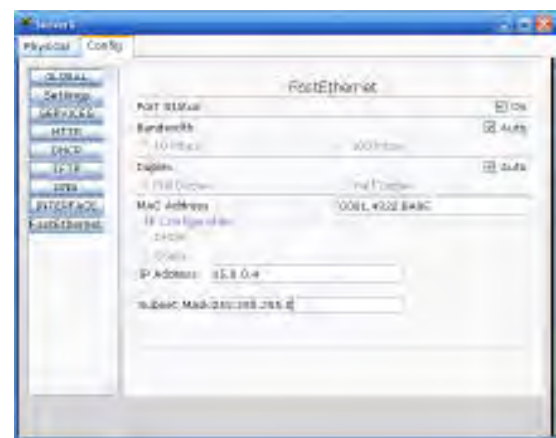
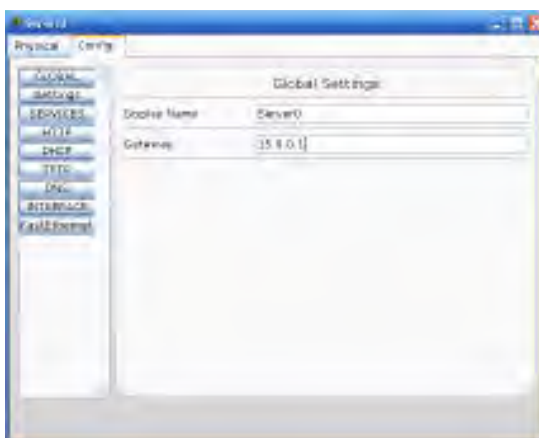
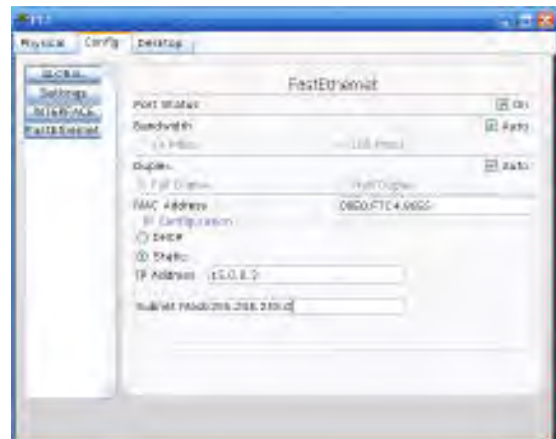
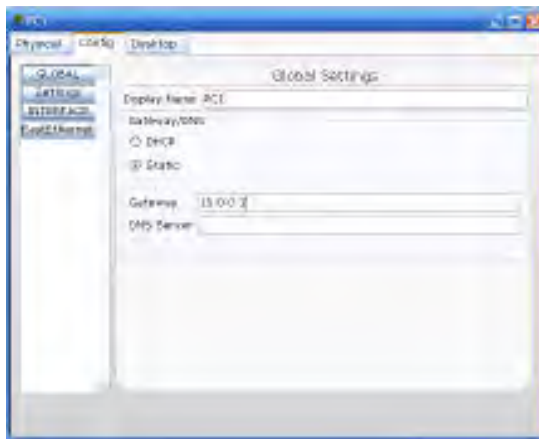


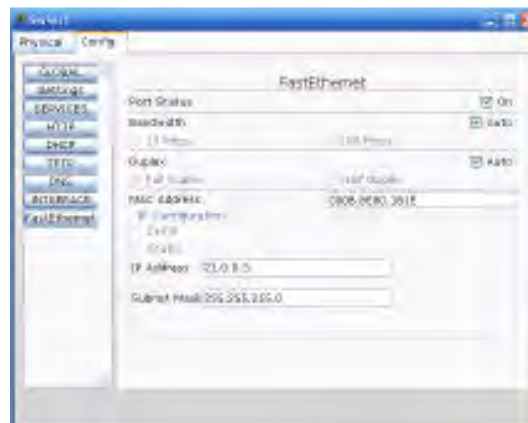
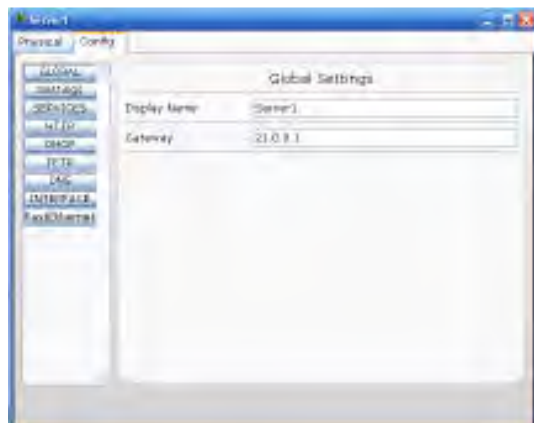
✓ فصل دوم: شبیه سازی شبکه توسط نرم افزار Packet Tracer

حال نوبت به پیکربندی سایر دستگاه ها می رسد. برای این دستگاه ها می بایست آدرس Gateway و IP و ماسک زیر شبکه مشخص شود. تنظیمات PC0 به صورت زیر می باشد.

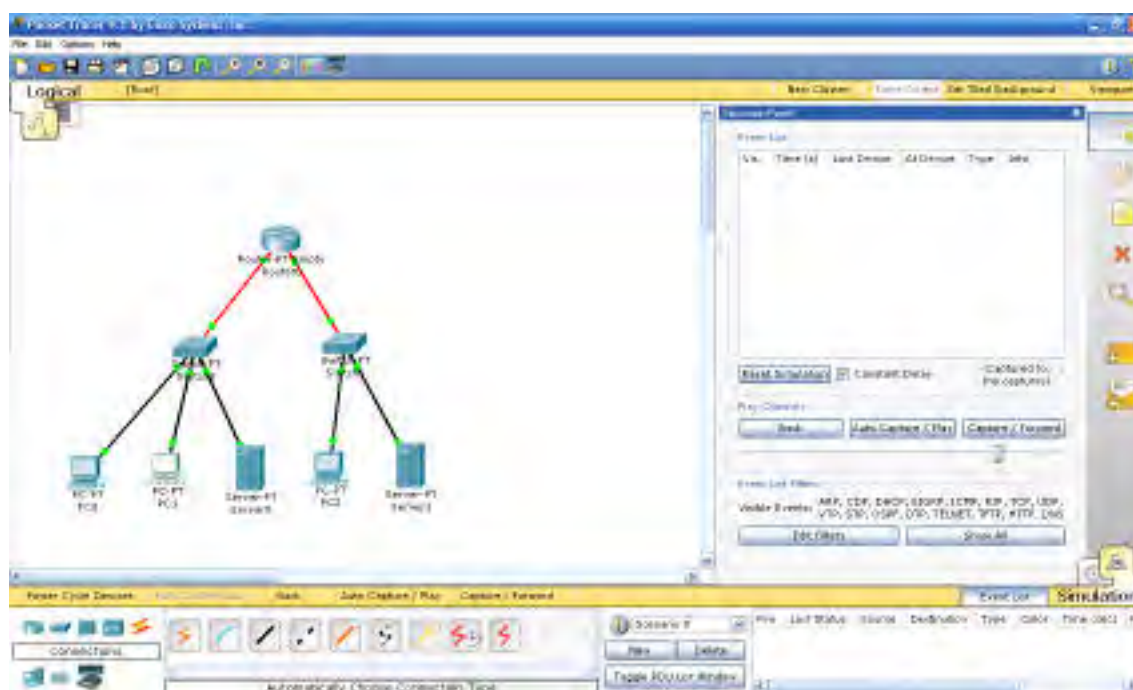


به همین ترتیب تنظیمات PC1 ، Server0 ، PC2 و Server1 به صورت زیر انجام می شود.

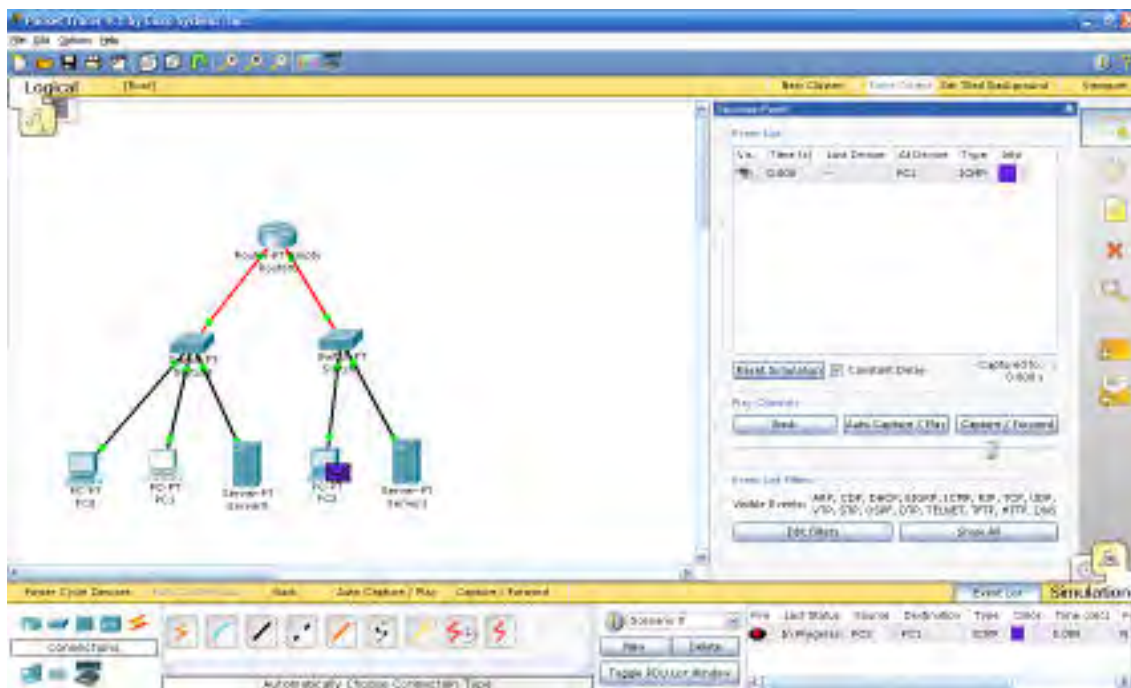




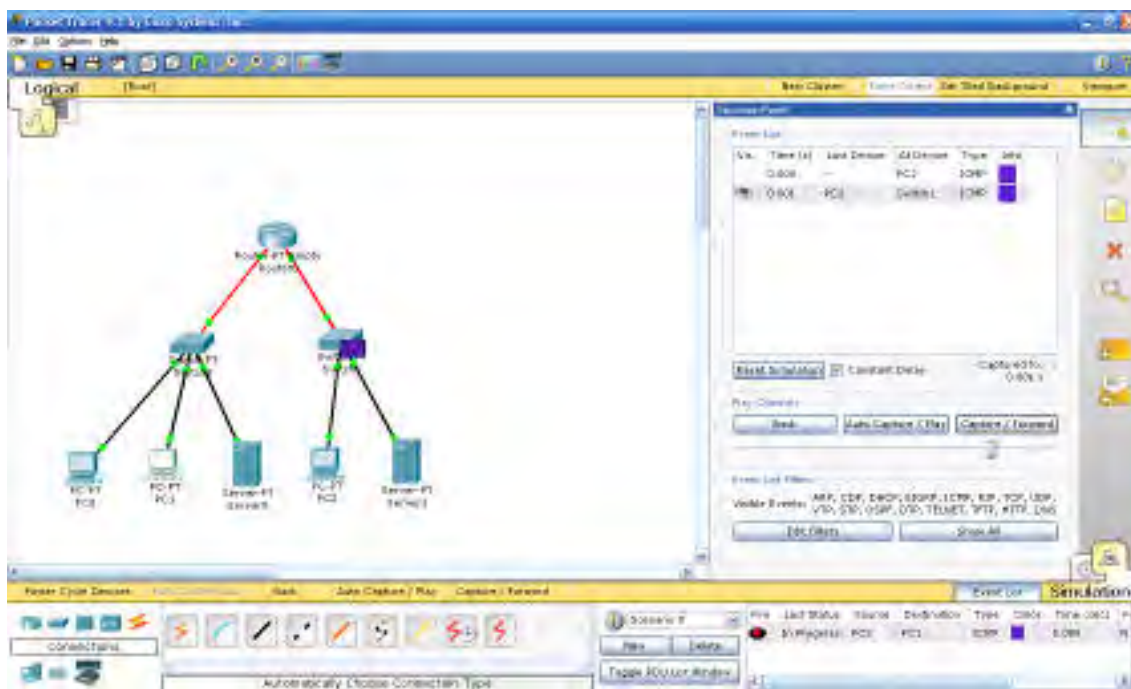
حال توپولوژی منطقی شبکه آماده است و می توانید در بخش شبیه سازی آن را تست کنید.



پس از ورودی به حالت simulation یک بسته از نوع Simple PDU از PC1 به PC2 ایجاد کنید.



به طور منظم بر روی دکمه Capture/Forward کلیک و مراحل را که بسته در شبکه طی می کند دنبال کنید.



The figure displays three sequential screenshots of the Packet Tracer software interface, illustrating the simulation process. Each screenshot shows a network topology with a central router connected to two switches, which are then connected to PCs and servers. The right-hand pane of each screenshot displays the 'Event List' and 'Simulation' controls.

Top Screenshot: The 'Event List' shows the following data:

Time (s)	Last Device	At Device	Type	Info
0.000	---	PC2	ICMP	
0.001	PC2	Switch1	ICMP	
0.002	Switch1	Router0	ICMP	

Middle Screenshot: The 'Event List' shows the following data:

Time (s)	Last Device	At Device	Type	Info
0.000	---	PC2	ICMP	
0.001	PC2	Switch1	ICMP	
0.002	Switch1	Router0	ICMP	

Bottom Screenshot: The 'Event List' shows the following data:

Time (s)	Last Device	At Device	Type	Info
0.000	---	PC2	ICMP	
0.001	PC2	Switch1	ICMP	
0.002	Switch1	Router0	ICMP	
0.003	Router0	Switch0	ICMP	
0.004	Switch0	PC1	ICMP	

The figure displays three sequential screenshots of the Packet Tracer simulation interface, showing a network topology and the Event List panel at different time intervals.

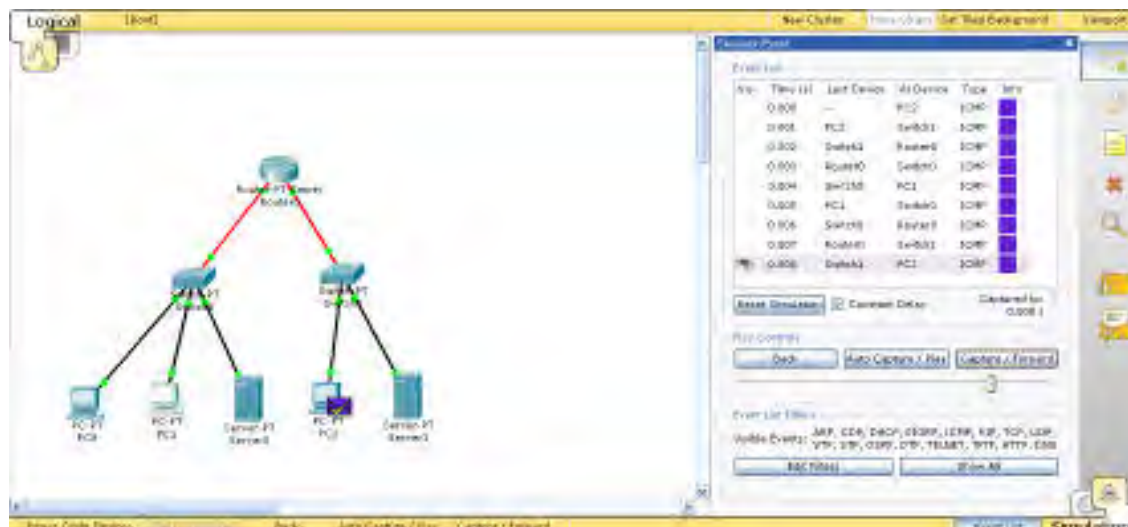
Network Topology: The network consists of a central Router (R1) connected to two Switches (S1 and S2). S1 is connected to PC0, PC1, and Server1. S2 is connected to PC2 and Server2.

Event List Panel: The Event List panel shows the sequence of events captured during the simulation. The events are listed in a table with columns: Vis., Time (s), Last Device, At Device, Type, and Info.

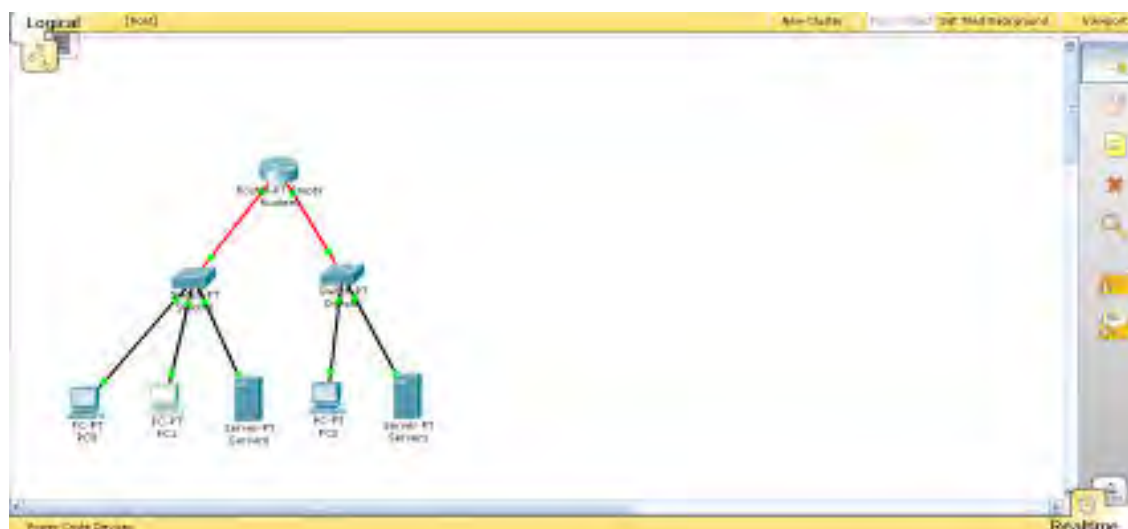
Simulation Panel: The Simulation Panel includes controls for the simulation, such as "Reset Simulation", "Constant Delay", "Captured to", "Play Controls", "Back", "Auto Capture / Play", and "Capture / Forward". It also includes "Event List Filters" and "Visible Events".

Event List Data:

Vis.	Time (s)	Last Device	At Device	Type	Info
	0.000	—	PC2	ICMP	
	0.001	PC2	Switch1	ICMP	
	0.002	Switch1	Router0	ICMP	
	0.003	Router0	Switch0	ICMP	
	0.004	Switch0	PC1	ICMP	
	0.005	PC1	Switch0	ICMP	
	0.006	Switch0	Router0	ICMP	
	0.007	Router0	Switch1	ICMP	

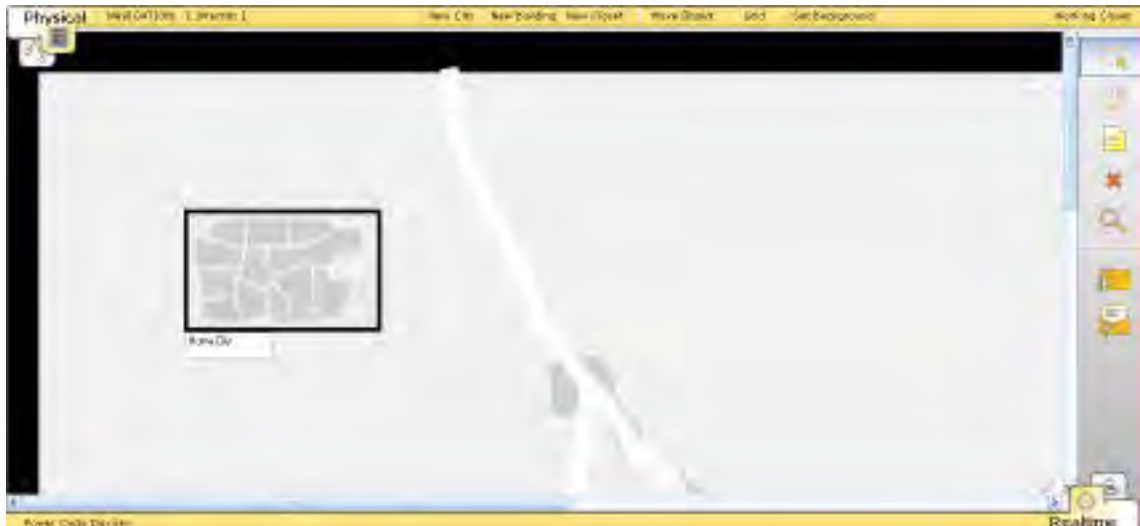


به این ترتیب مشاهده نمودید که یک بسته ICMP برای پینگ کردن PC1 از طریق PC2 ایجاد شد و عملیات با موفقیت به اتمام رسید. PDU ایجاد شده را حذف و مجدد به حالت Realtime بازگردید.

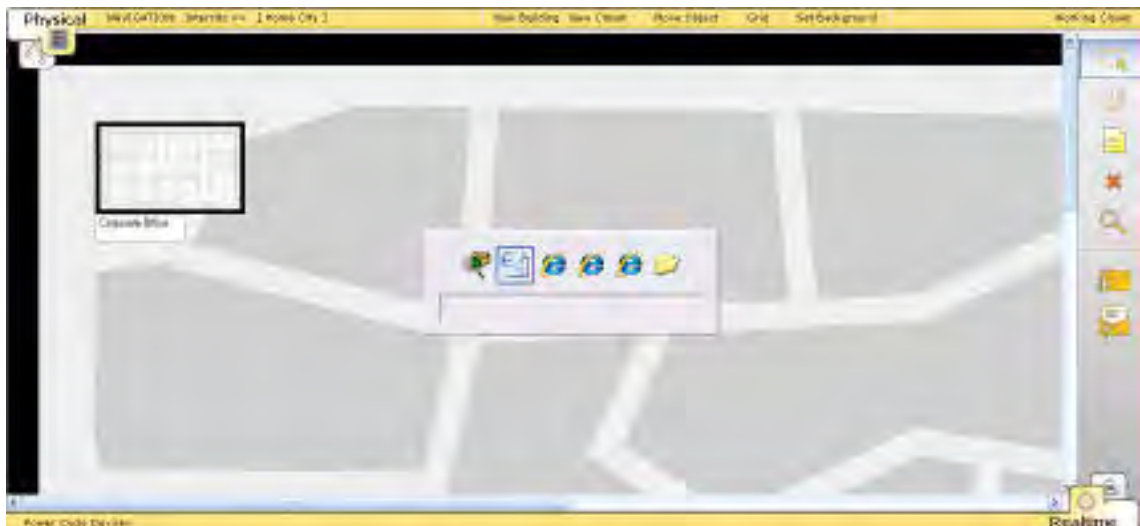


مثال عملی) قسمت دوم - توسعه توپولوژی شبکه

حال قصد داریم توپولوژی شبکه را از نظر فیزیکی بررسی کنیم. روی نمای Physical Workspace کلیک کنید.



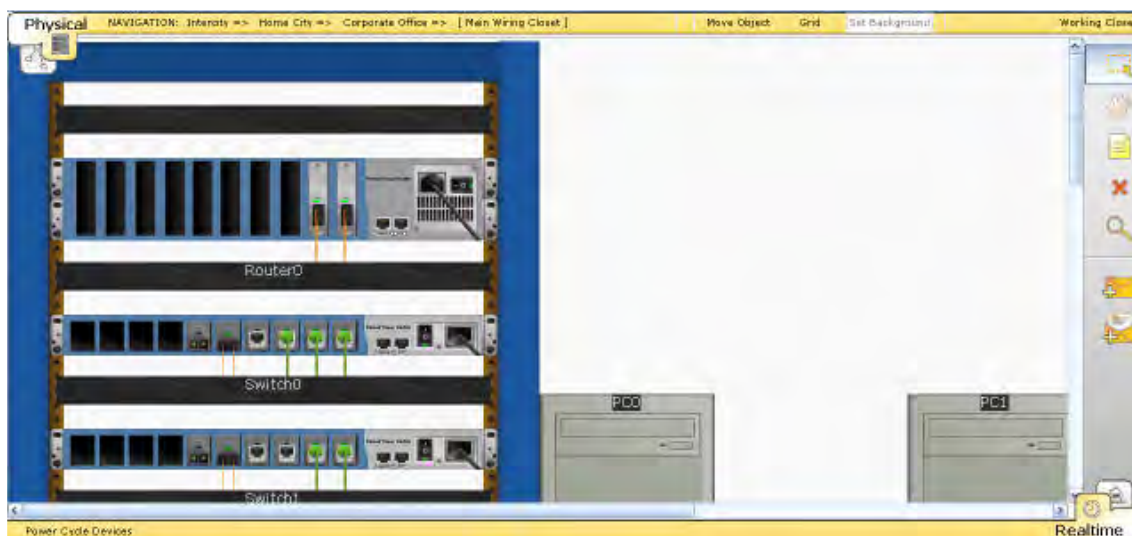
اکنون در ناحیه Intercity قرار دارید، روی Homecity کلیک کنید تا به داخل شهر بروید.



در Homecity ساختمان corporate Office قابل مشاهده است. بر روی آن کلیک کنید تا به داخل ساختمان قرار بگیرید.



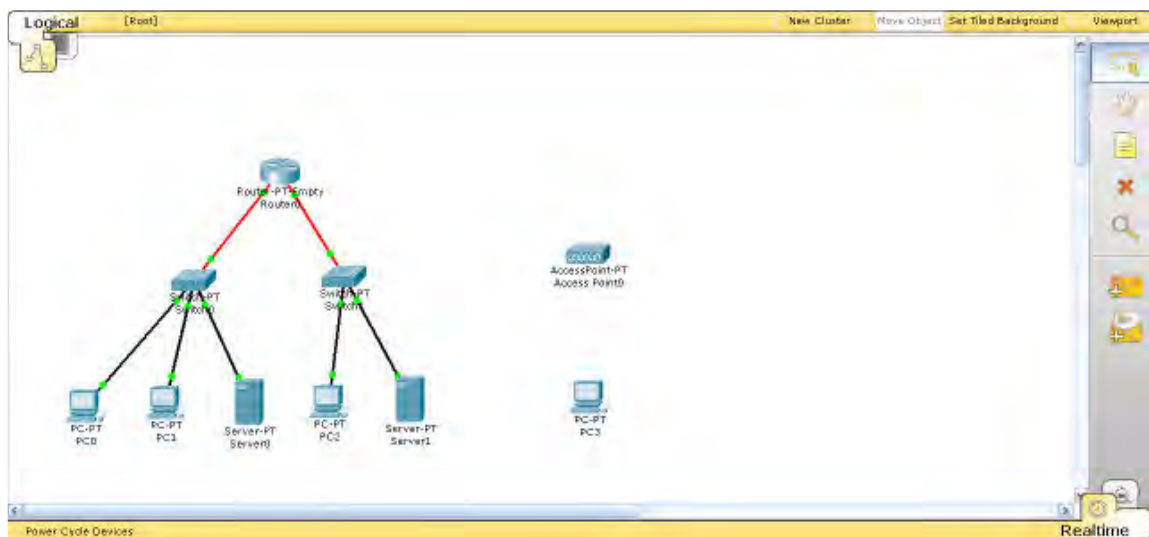
در حال حاضر در داخل ساختمان، اتاق Main Wiring Closet قابل مشاهده است که دستگاههای ما در داخل آن قرار دارد. برای مشاهده تجهیزات شبکه خود بر روی آن کلیک کنید.



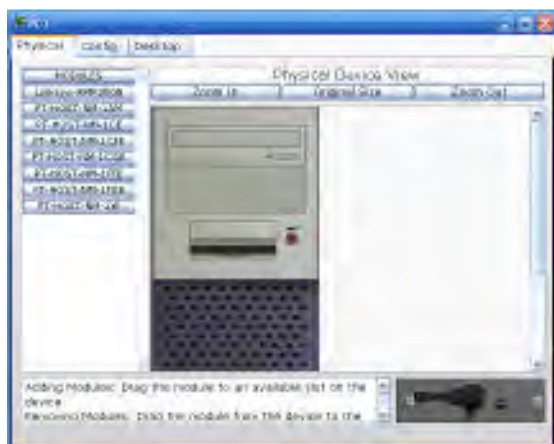
برای این که تجهیزات را بهتر مشاهده کنید، با استفاده از ابزار بزرگ نمایی ، تصویر را کوچک کنید.



مشاهده می کنید که تجهیزات شبکه در داخل قفسه (rack) و دستگاه های رایانه روی میز قرار گرفته اند. حال قصد داریم یک ارتباط بی سیم برقرار کنیم. بدین منظور مجدداً به نمای منطقی شبکه باز گردید. یک AccessPoint جدید به شبکه اضافه نمایید.



برای ایجاد ارتباط بی سیم می بایست ماژول بیسیم را به رایانه خود اضافه کنید. بنابراین روی PC3 کلیک کنید تا پنجره تنظیمات آن باز شود. پس از خاموش کردن رایانه، ماژول فعلی آن را از قسمت پایین چارج ساخته و ماژول بی سیم را در جای آن قرار دهید. سپس مجدداً رایانه را روشن کنید.



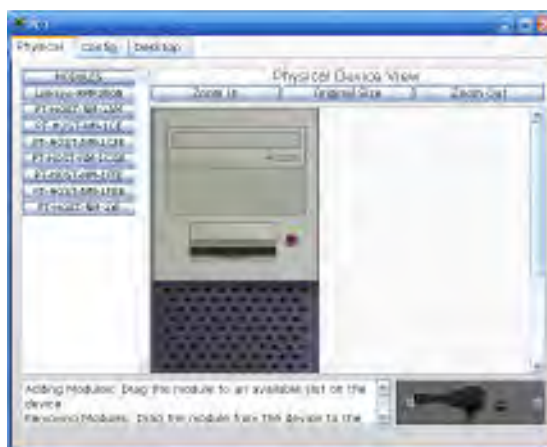
۱



۲

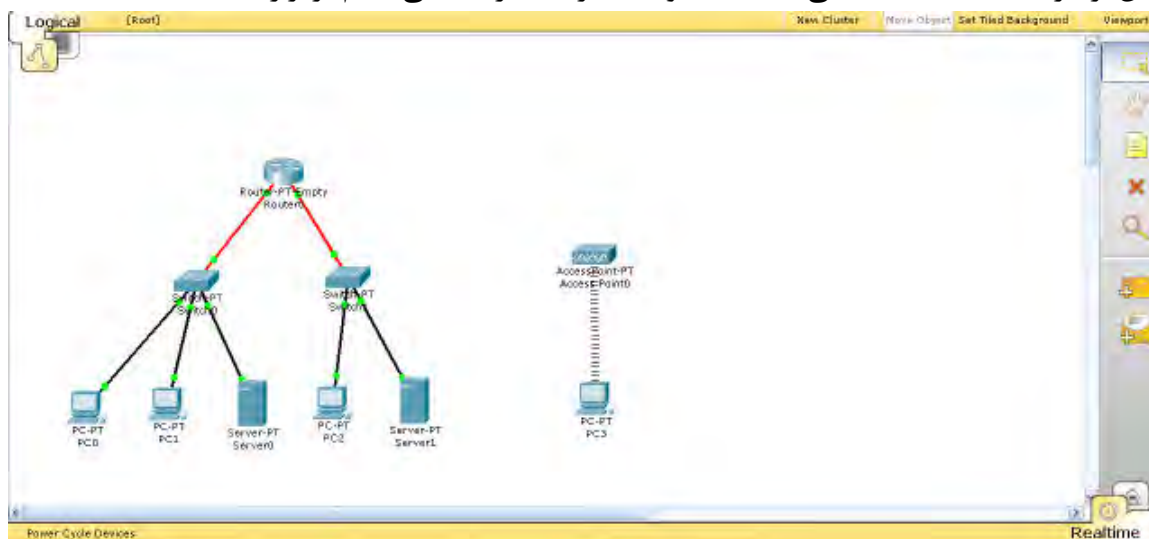


۳

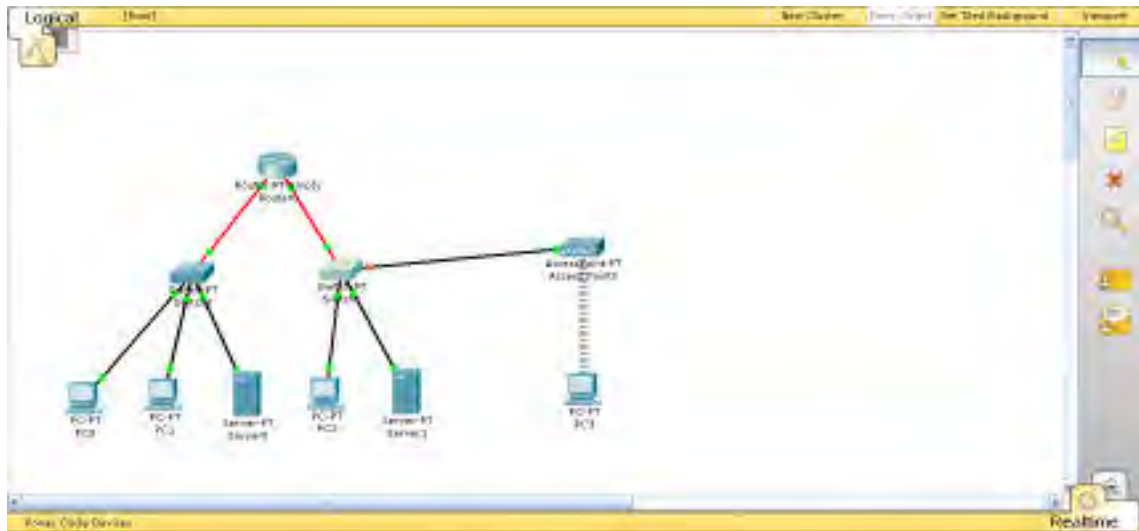


۴

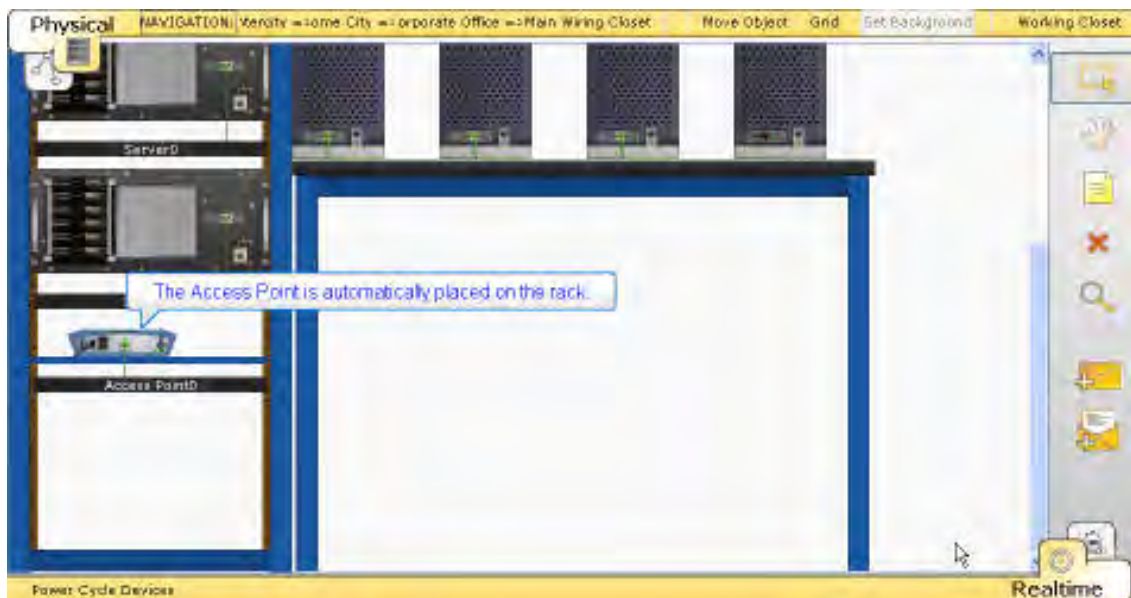
پس از بازگشت به صفحه اصلی مشاهده خواهید کرد که ارتباط بی سیم برقرار شده است.



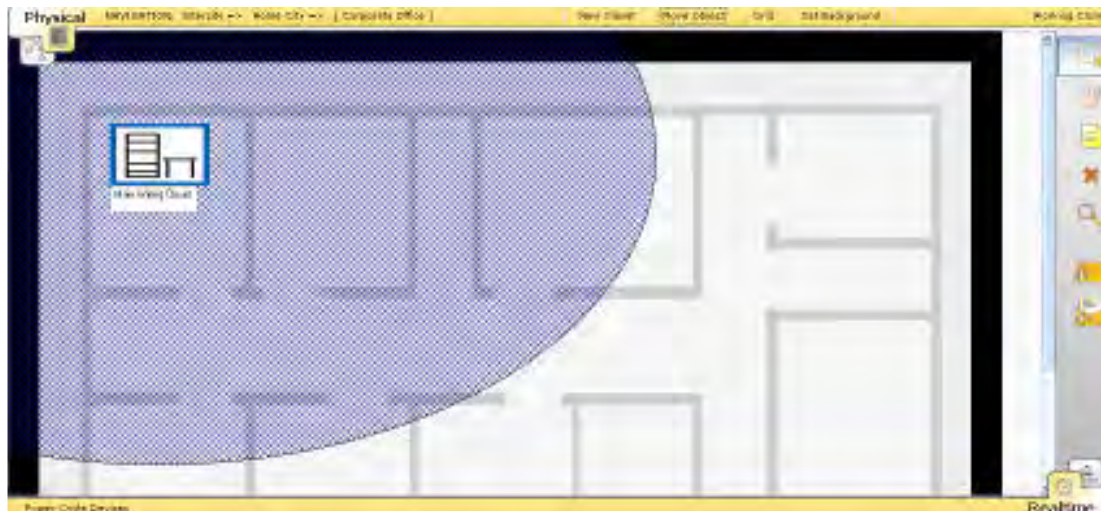
برای اتصال این اجزای جدید به شبکه، با استفاده از کابل Copper Straight یک اتصال بین AccessPoint و سوئیچ مطابق شکل برقرار کنید.



حال برای بررسی توپولوژی فیزیکی به نمای Physical بازگردید. مشاهده می کنید که Point Access به طور خودکار به قفسه افزوده شده است.



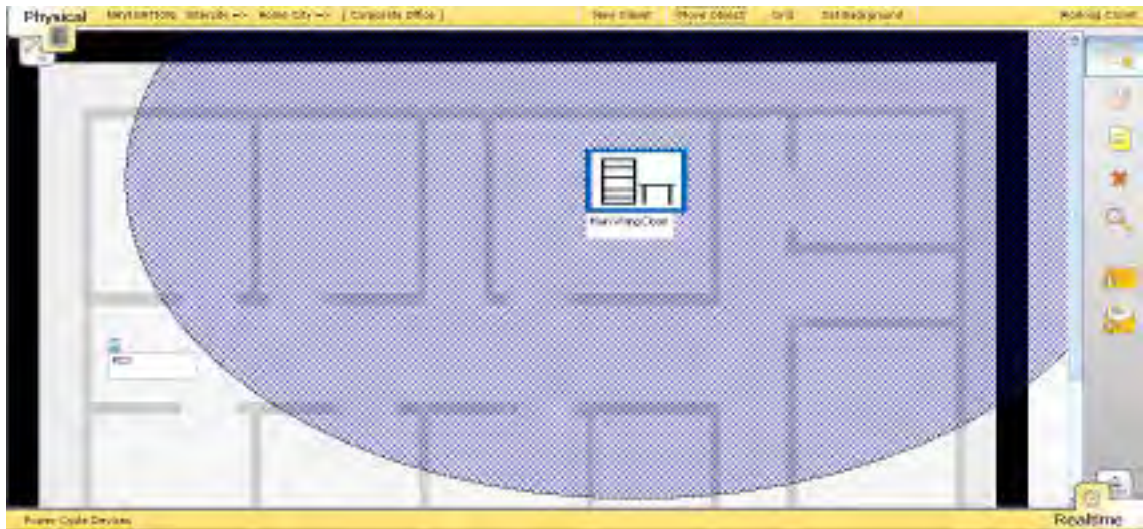
با کلیک بر روی Corporate Office از قسمت نوار پیمایش، به فضای داخل ساختمان بروید. محدوده نمایش داده شده در محوطه ساختمان مربوط به Access Point و فضای تحت پوشش آن می باشد.



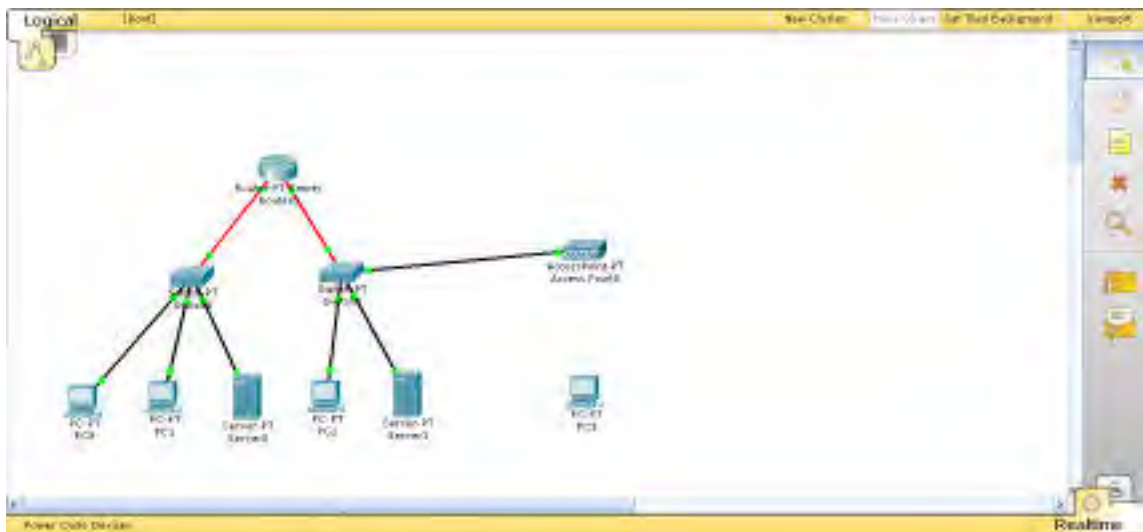
به داخل اتاق رفته و با استفاده از دکمه Move Object، رایانه PC3 را به داخل محوطه ساختمان منتقل کنید.



مجدداً به محوطه ساختمان بروید و با جابجایی اتاق و PC3 آنها را به گونه ای قرار دهید که PC3 در محدوده خارج از پوشش AccessPoint قرار داده شود.



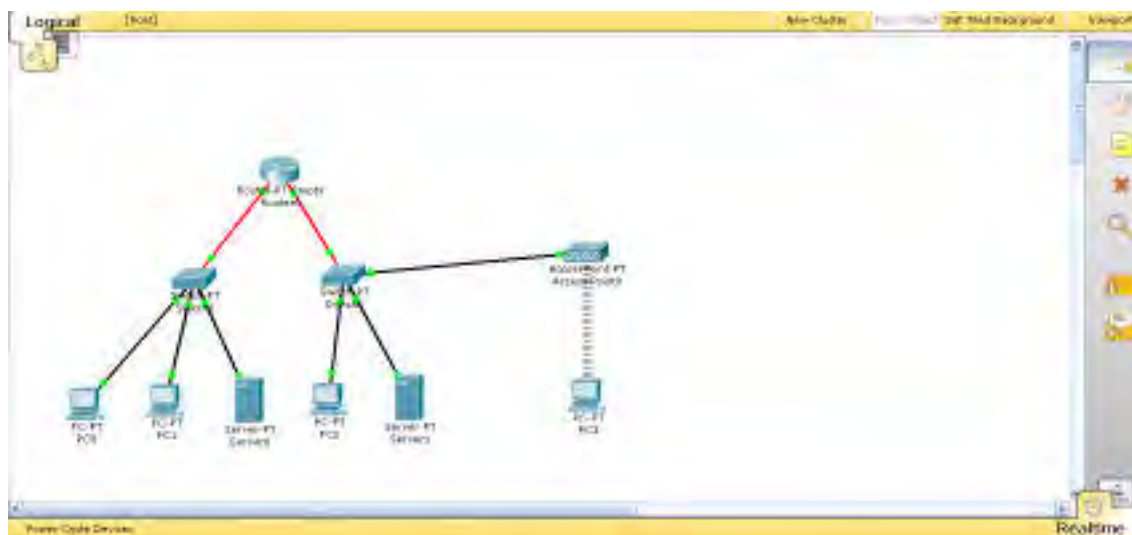
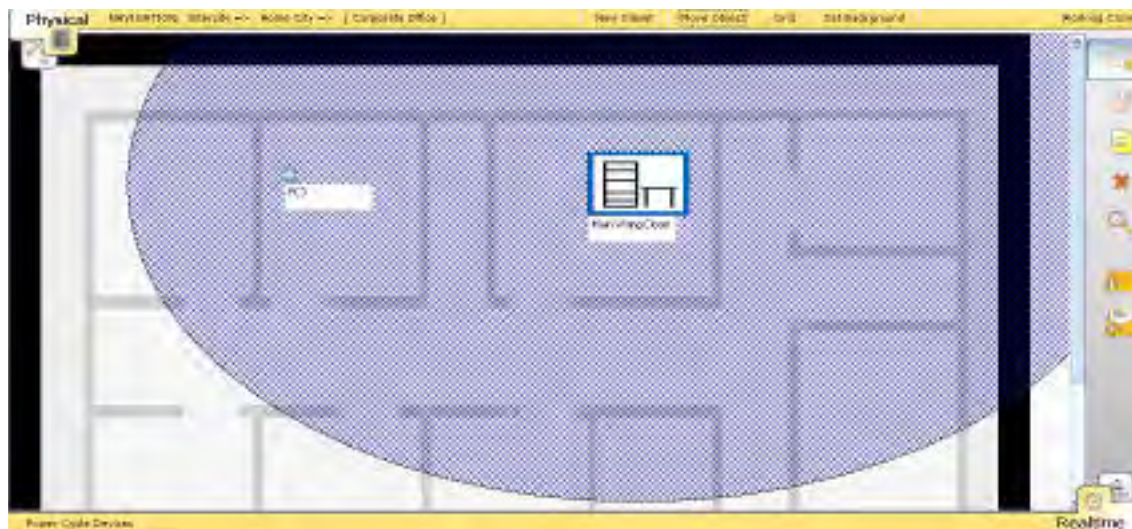
در این حالت اگر به فضای کار منطقی باز گردید مشاهده خواهید کرد که اتصال بین PC3 و AccessPoint قطع شده است.



پس برای برقرار مجدد این اتصال می بایست در فضای فیزیکی، رایانه را در محدوده تحت پوشش بیسیم قرار دهید.

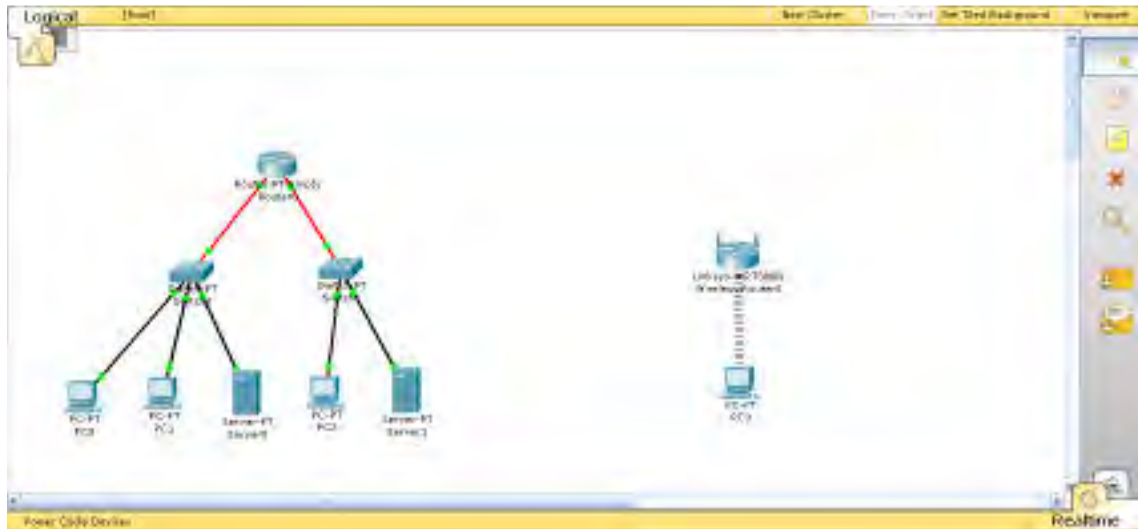


✓ فصل دوم: شبیه سازی شبکه توسط نرم افزار Packet Tracer

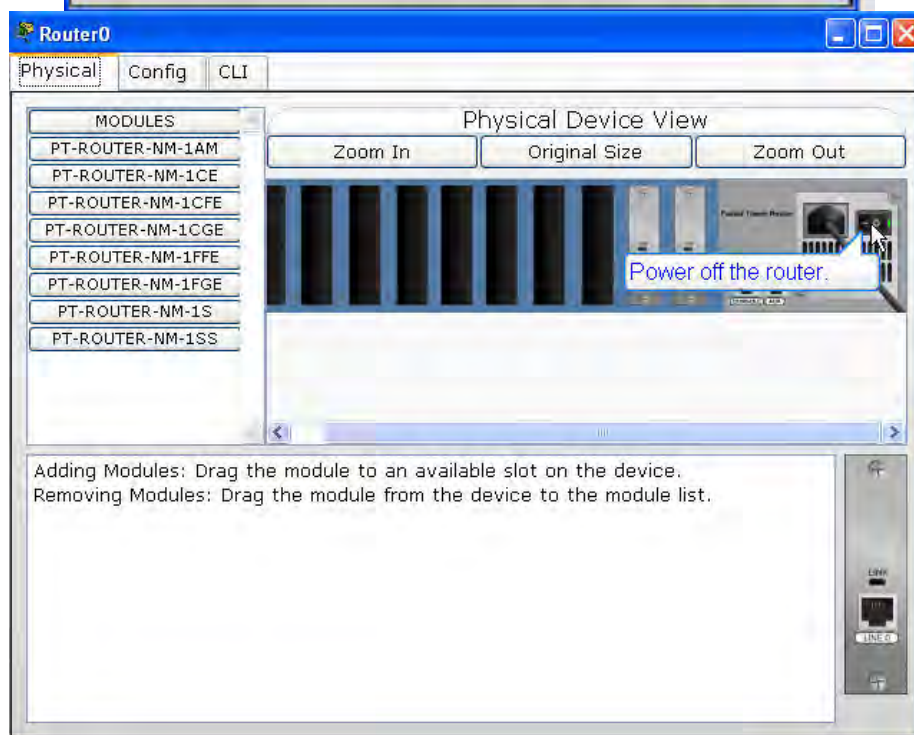
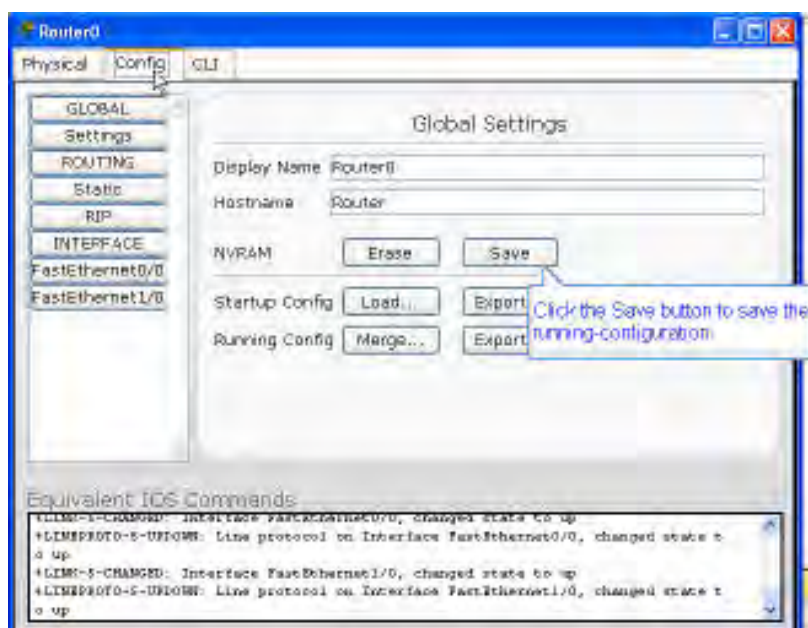


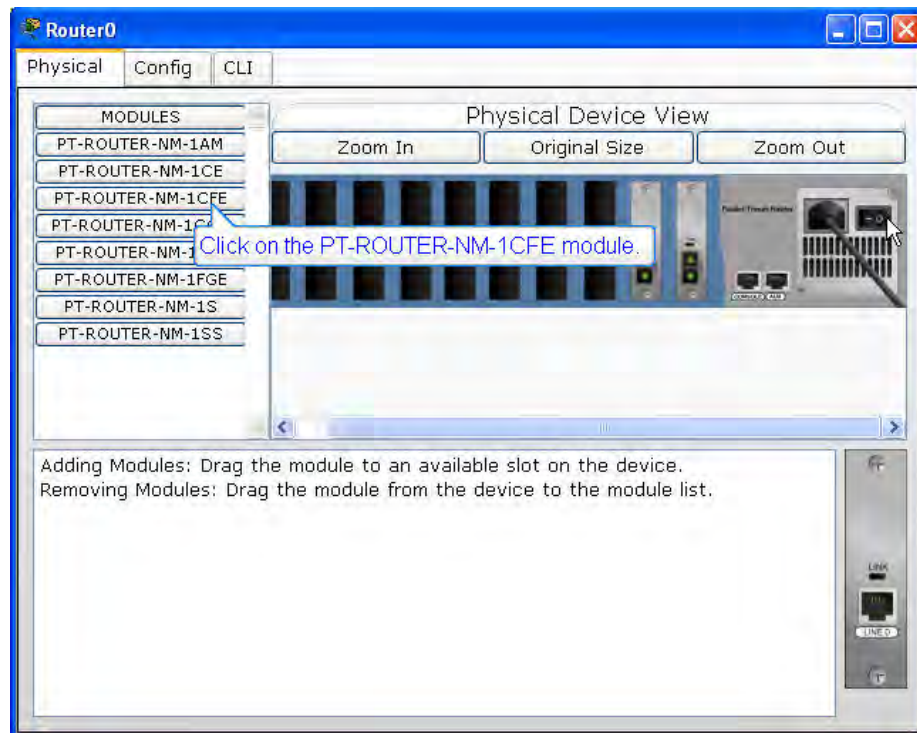
مثال عملی) قسمت سوم – شبیه سازی یک شبکه ISP و شبکه خانگی

در ادامه این تمرین قصد راه اندازی یک شبکه خانگی بیسیم و اتصال آن به یک ISP با استفاده از ارتباط DSL را داریم. برای ادامه کار، AccessPoint موجود را شبکه فعلی را حذف نموده و یک AccessPoint از نوع Linksys-WRT300N بجای آن قرار دهید.

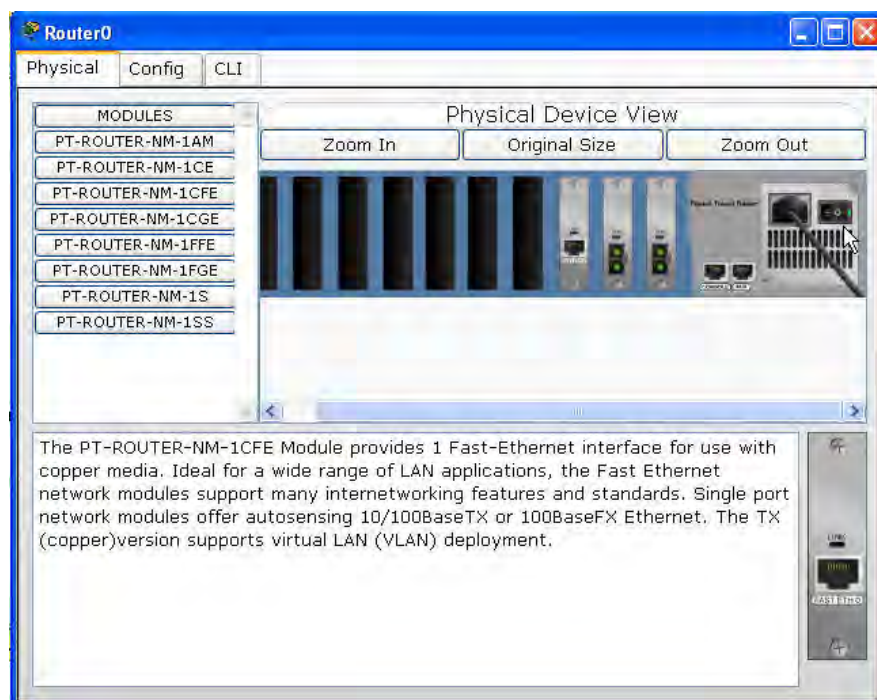


ابتدا باید برای افزودن قابلیت اتصال کاربران به ISP، به Router0 که متعلق به ISP است یک ماژول جدید اضافه کنیم. روی Router0 کلیک کنید. دقت کنید که برای اضافه نمودن ماژول جدید باید روتر خاموش شود، ولی با این کار کلیه تنظیمات آن از بین خواهد رفت. پس ابتدا تنظیمات را مطابق شکل ذخیره کنید. سپس ماژول جدید را اضافه کنید.



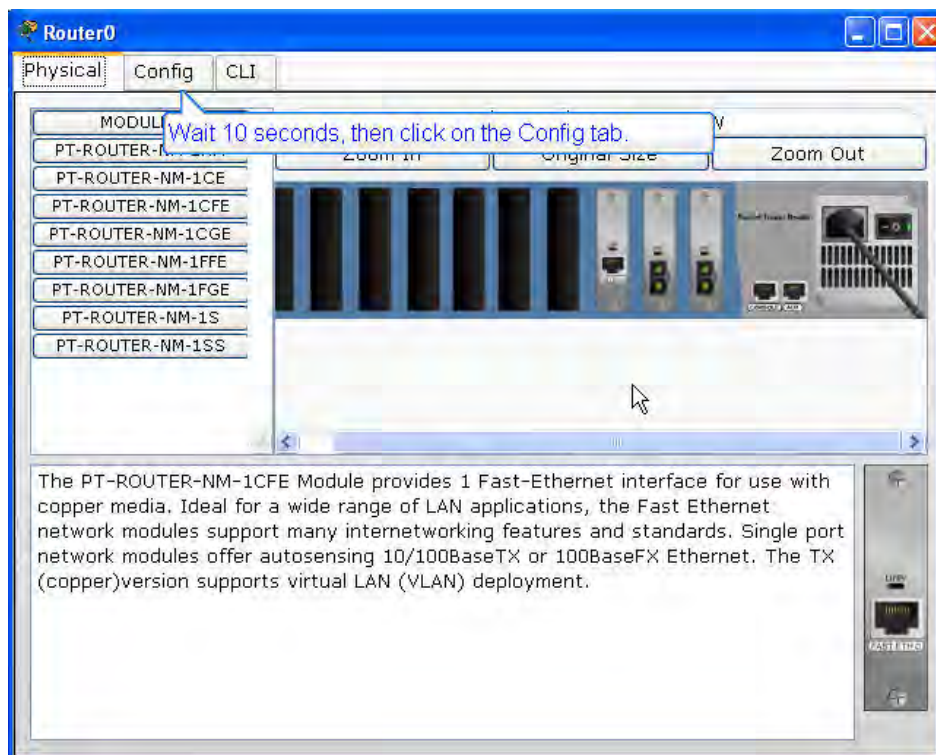
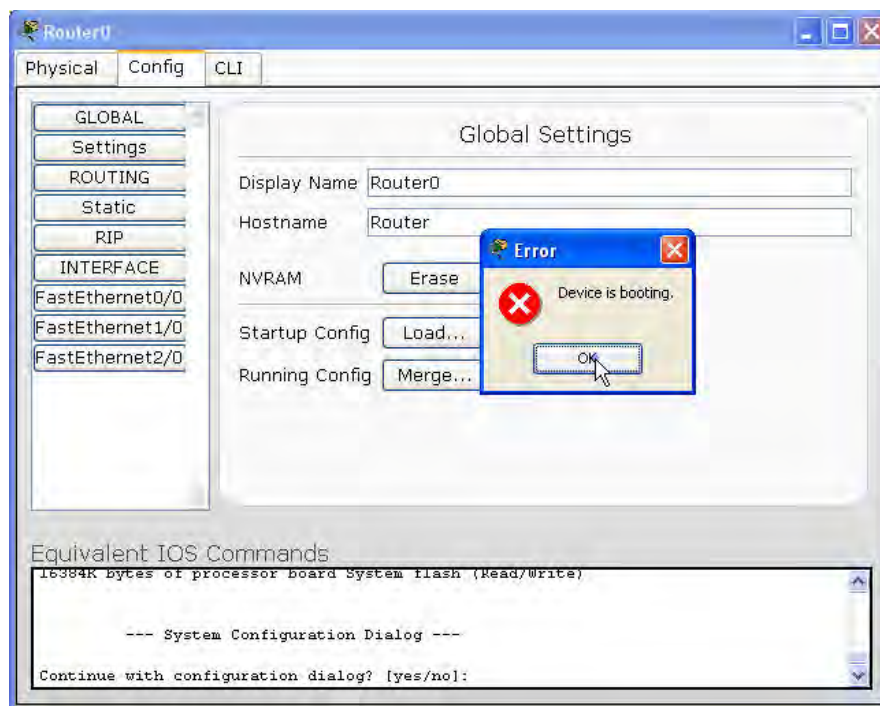


پس از روشن کردن مسیریاب، برای پیکربندی واسط جدید، بر روی برگه config کلیک کنید. یک پیام خطا ظاهر می شود و اطلاع می دهد که مسیریاب در حال راه اندازی است (راه اندازی مسیریاب حدود ۱۰ ثانیه طول می کشد). بنابراین پس از ۱۰ ثانیه مجدداً بر روی این برگه کلیک کنید.

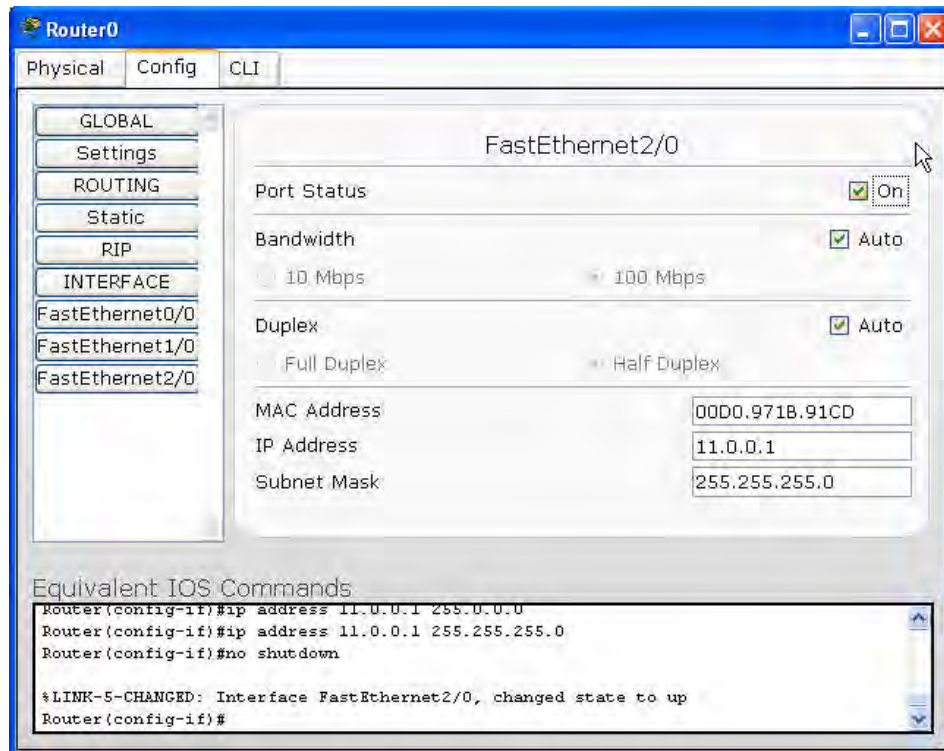




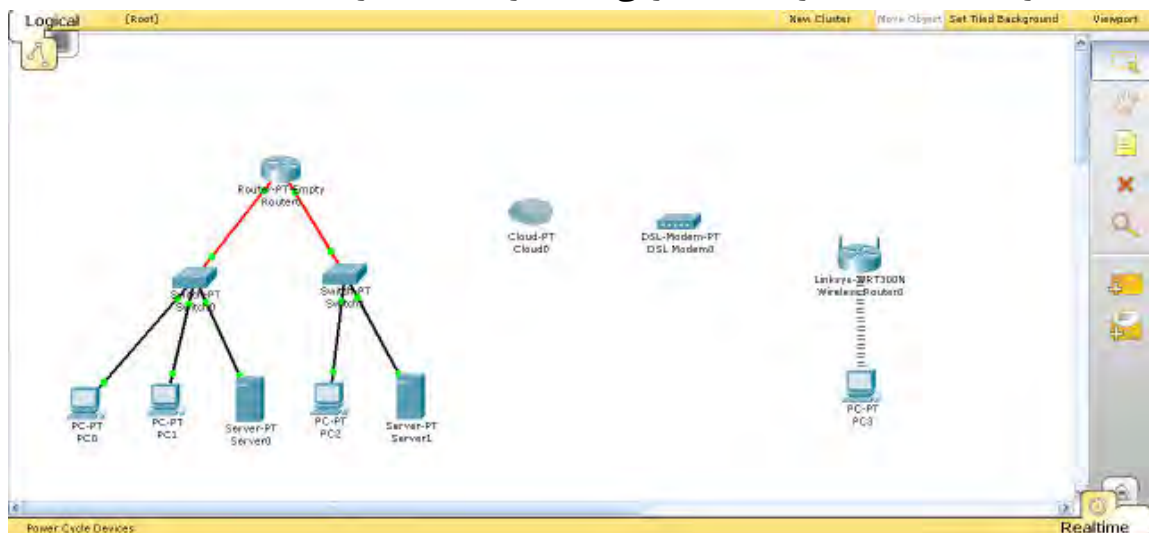
✓ فصل دوم: شبیه سازی شبکه توسط نرم افزار Packet Tracer



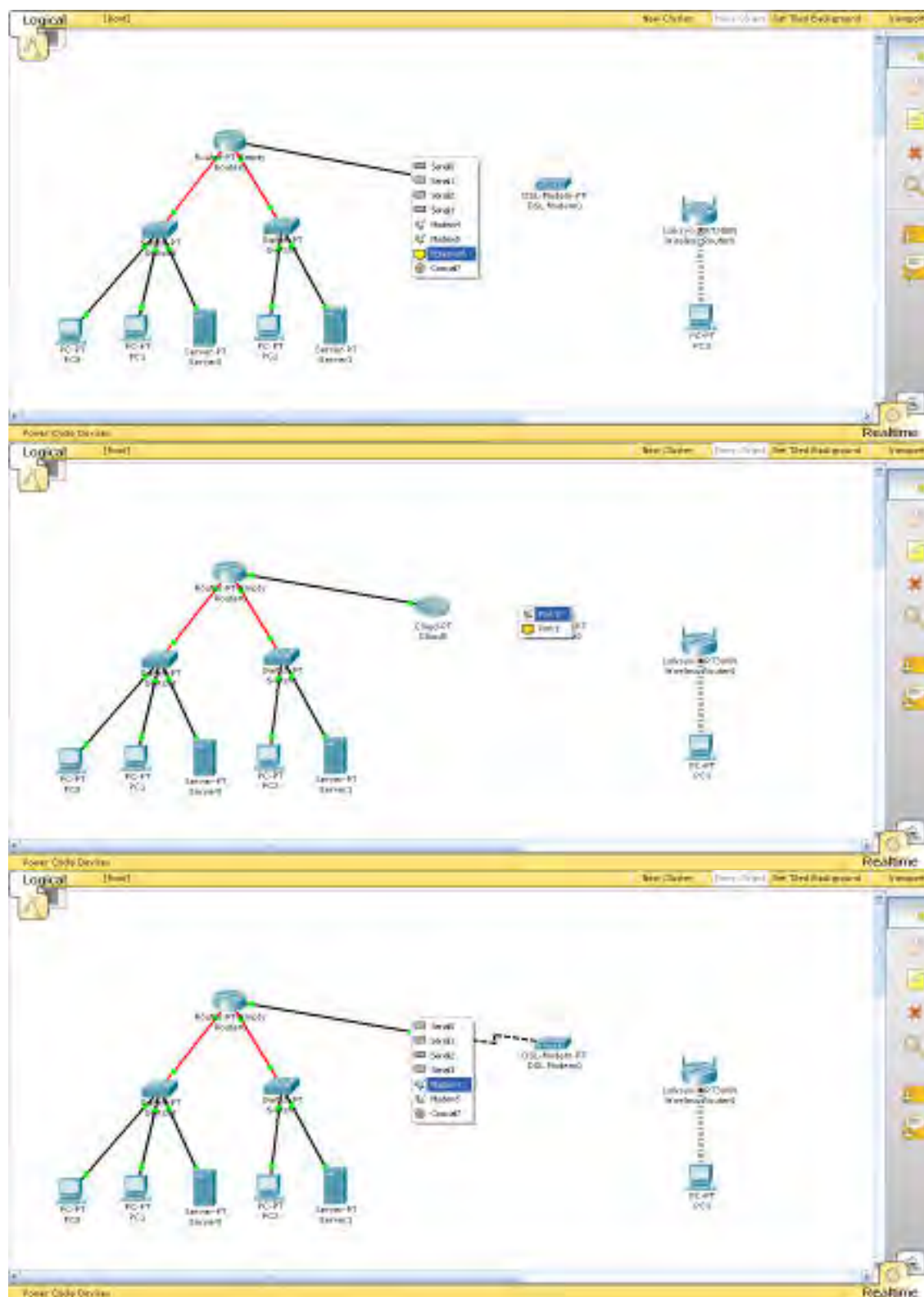
واسط جدیدی که اضافه شده است FastEthernet2/0 است. تنظیمات آن را مطابق شکل انجام دهید.



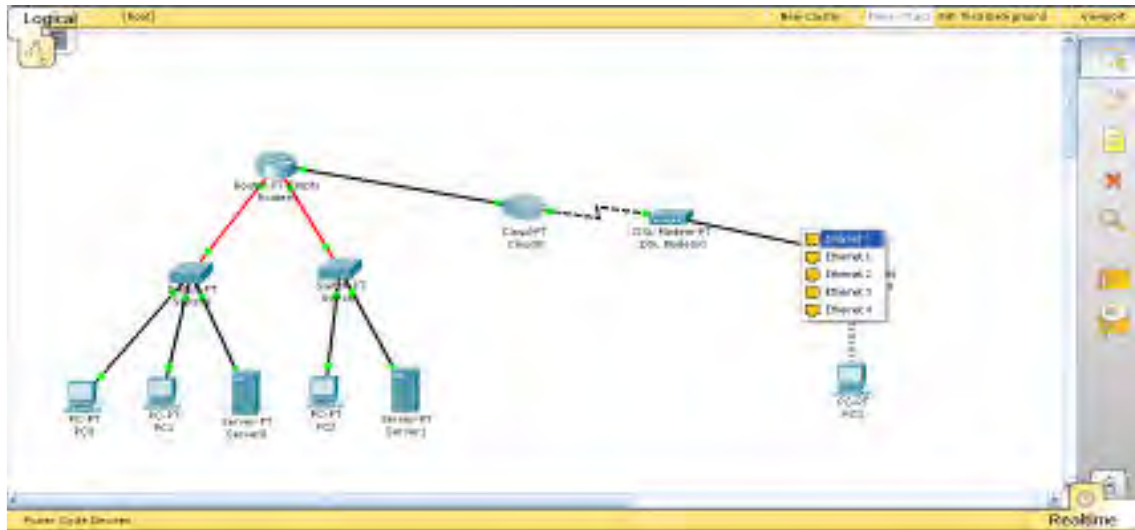
برای ایجاد ارتباط بین شبکه خانگی و ISP یک مودم DSL به محیط کار اضافه کنید. همچنین باید یک ابر (cloud) که نشانگر شبکه مخابراتی است نیز به فضای کار اضافه نمایید.



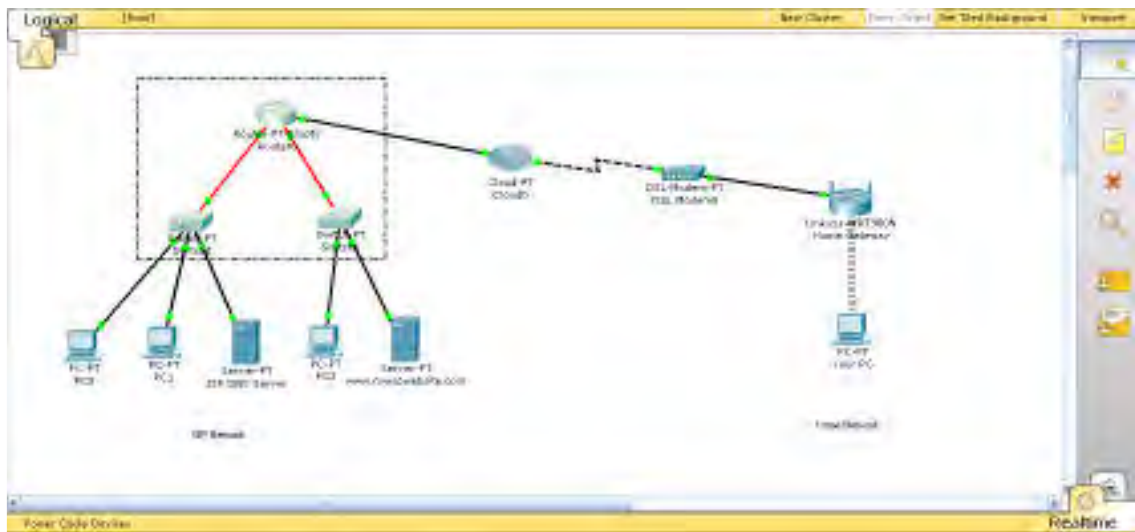
مطابق شکل، مسیریاب را به پورت Ethernet ابر متصل کنید و Port0 مودم را به پورت مودم ابر متصل کنید.

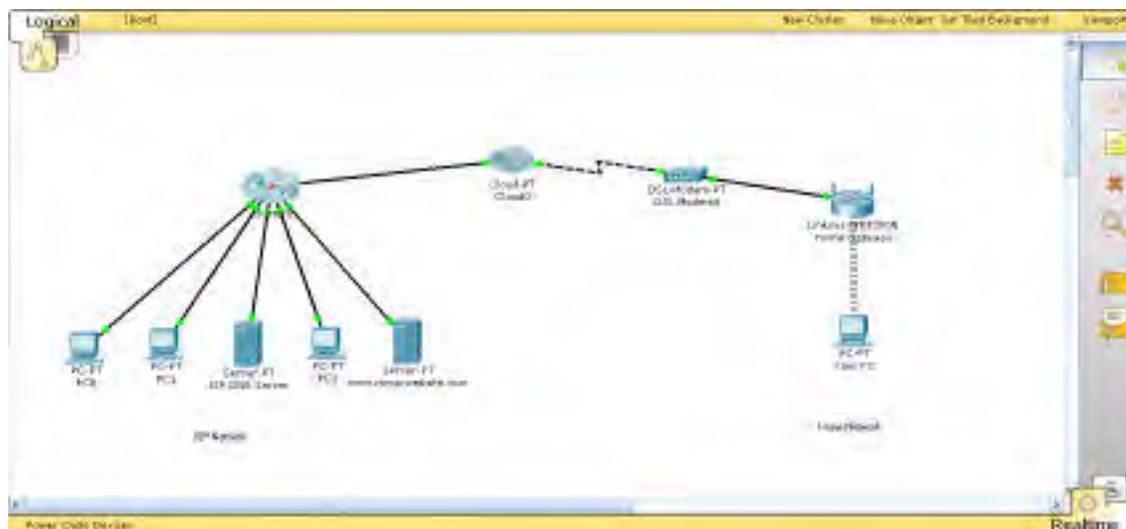


در ادامه می بایست مودم را به پورت اینترنت مسیریاب Linksys متصل کنید.

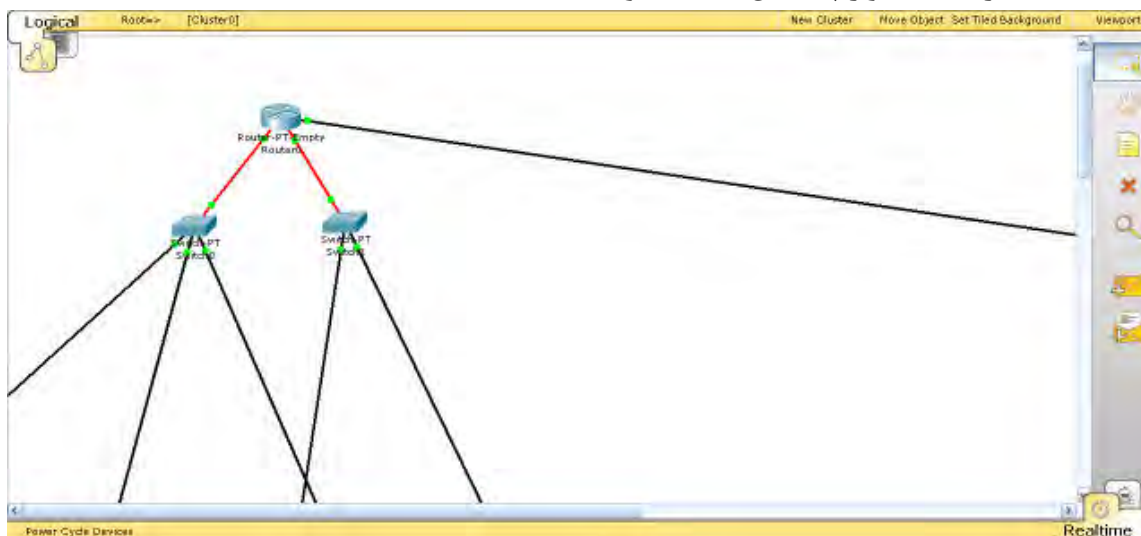


برای این که اجزای داخلی ISP پنهان شود و توپولوژی شبکه منظم تر گردد، مسیر یاب و سوئیچ های شبکه را انتخاب نموده و بر روی دکمه New Cluster کلیک کنید.

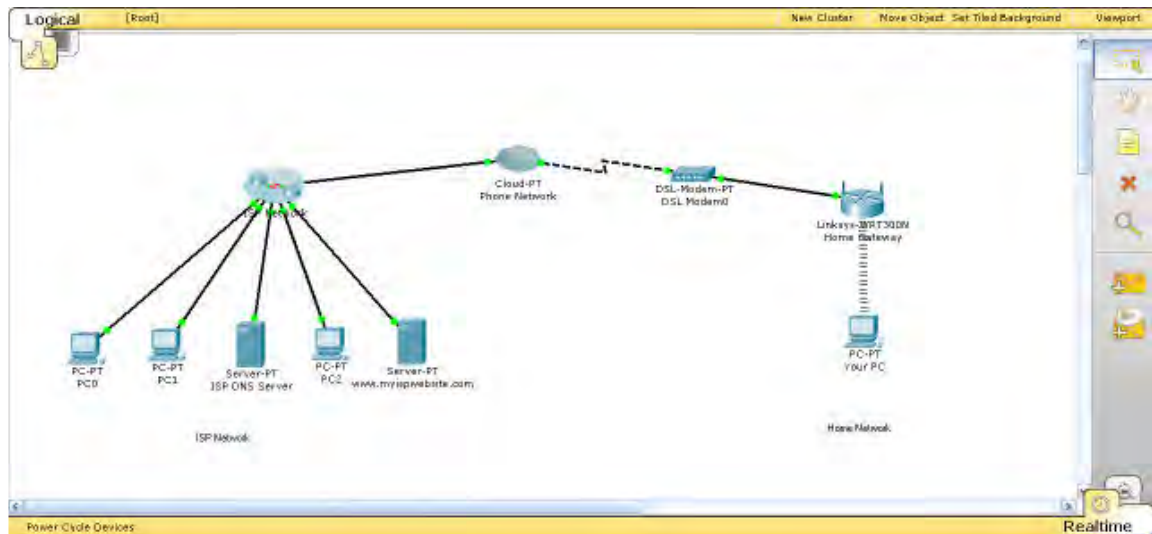




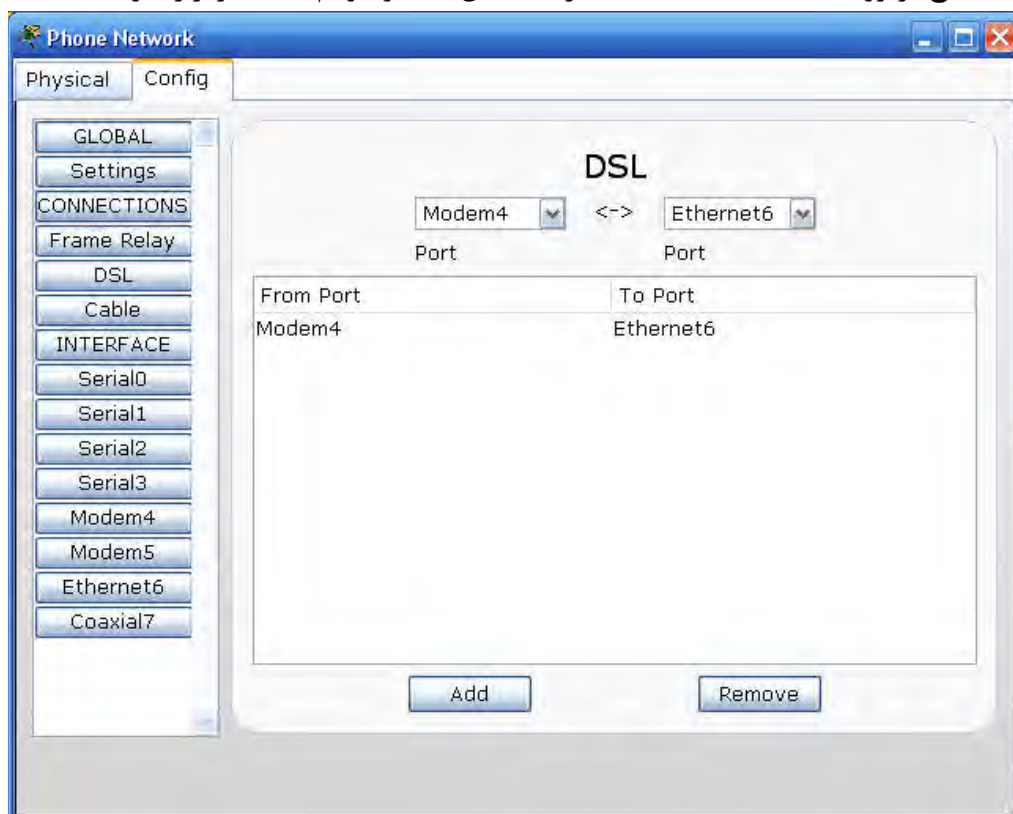
مشاهده می کنید که این اجزا در داخل یک گروه قرار می گیرند. در هر لحظه می توانید با یک کلیک وارد ISP شده و اجزای داخل آن را ویرایش کنید. برای خروج از ISP نیز می توان بر روی دکمه Root در قسمت نوار پیمایش کلیک نمود.



حال برای نظم بهتر شبکه، باید اجزای مختلف شبکه از جمله سرور وب، DNS سرور، نام رایانه شبکه خانگی و ابرهای شبکه مخابراتی و ISP را نام گذاری نمود.



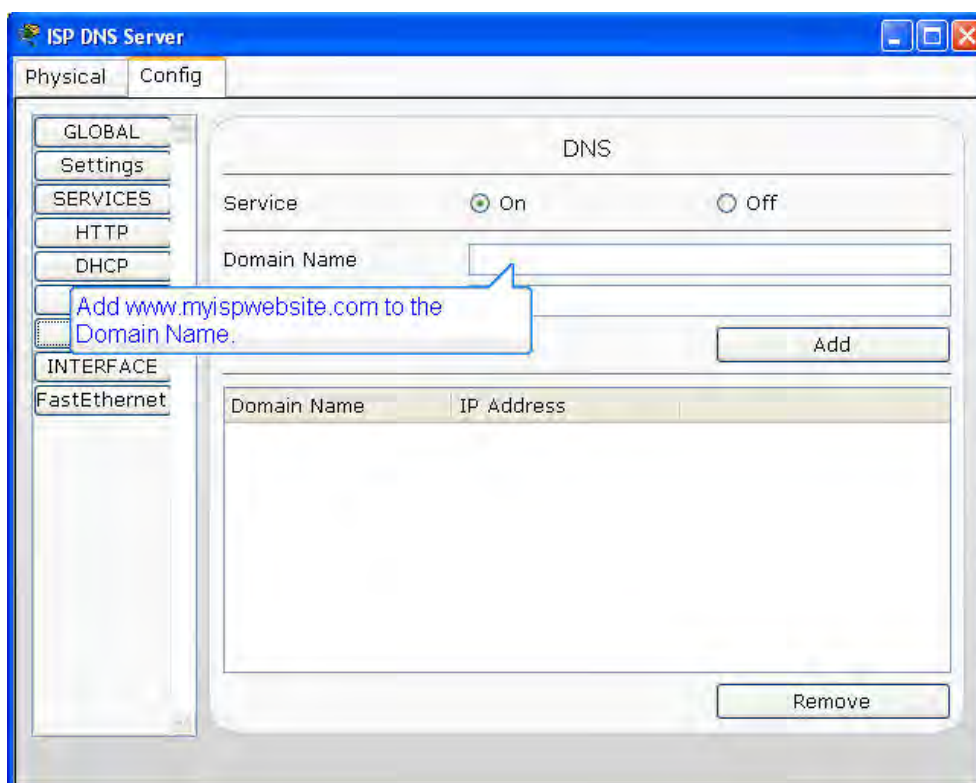
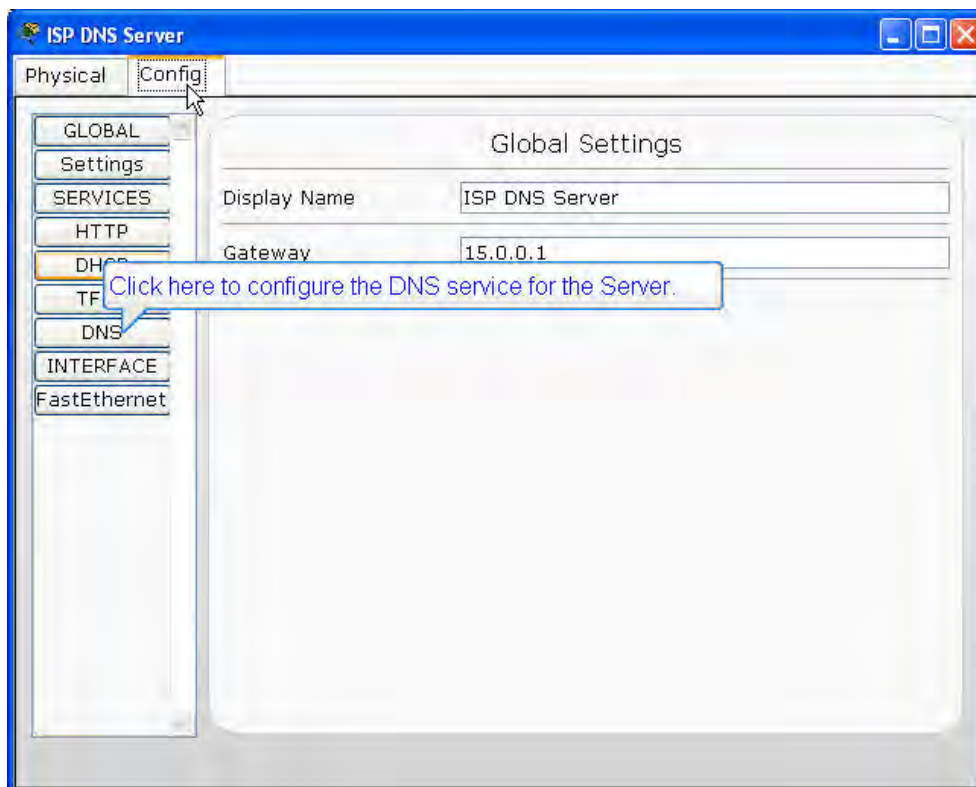
برای تنظیم ارتباط DSL وارد ابر شبکه مخابرات شده و در قسمت DSL پس از مشخص کردن ارتباط صحیح بر روی دکمه Add کلیک، تا ارتباط بین ISP و مودم DSL برقرار شود.

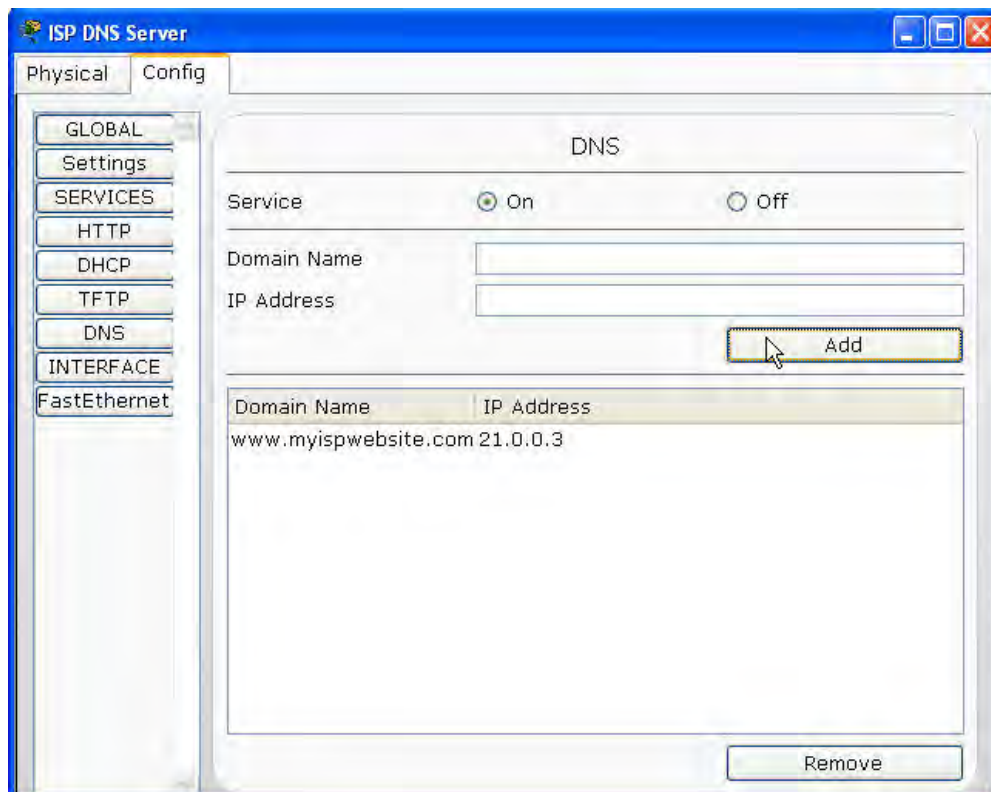
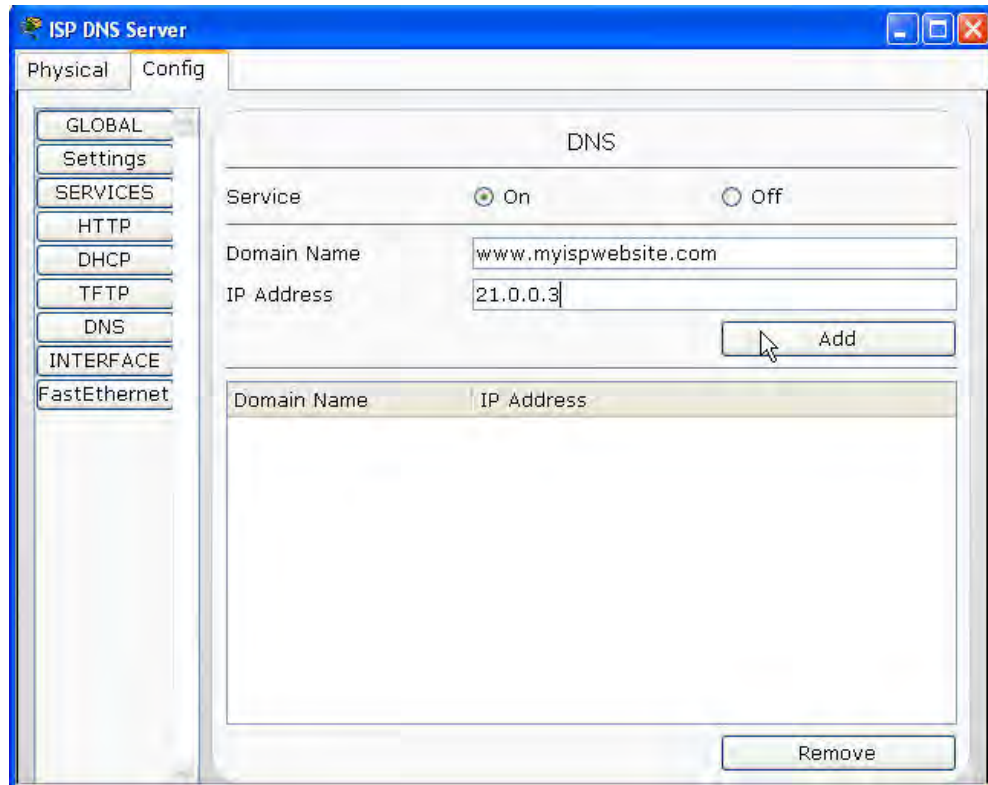


برای تنظیم DNS سرور، بر روی ISP DNS Server کلیک و تنظیمات DNS آن را مطابق شکل انجام دهید.



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



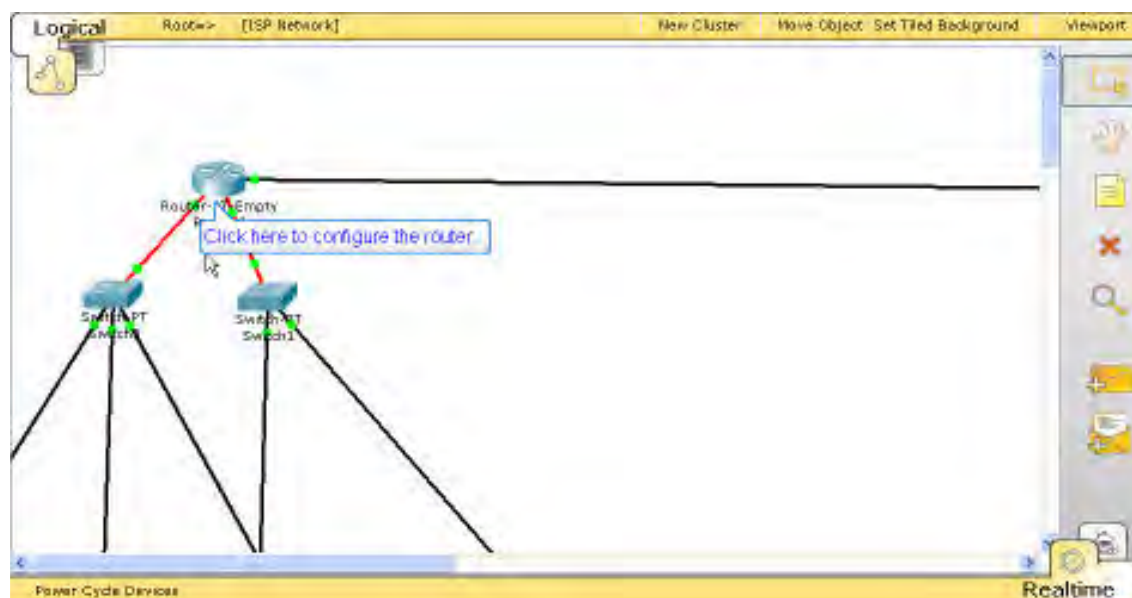


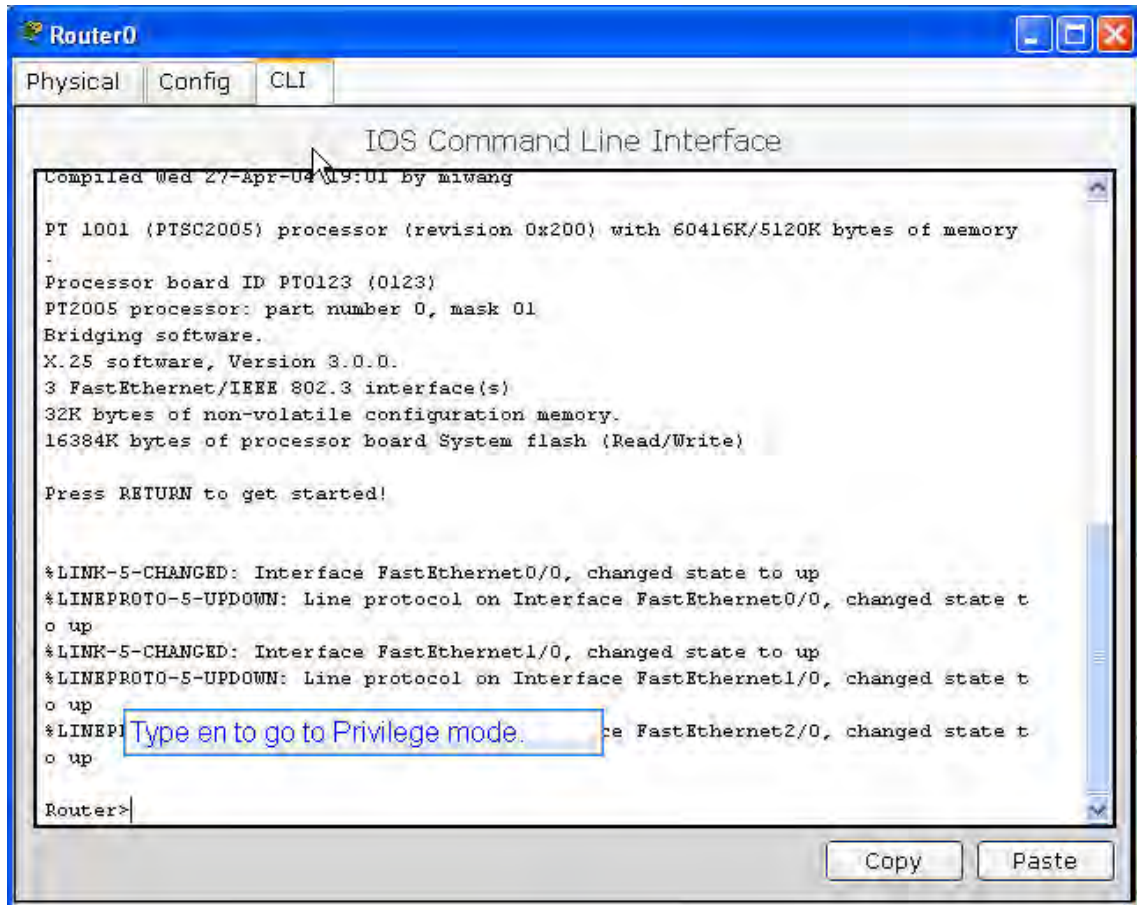


✓ فصل دوم: شبیه سازی شبکه توسط نرم افزار Packet Tracer

برای تنظیم مسیریاب، وارد ISP شده و بر روی مسیریاب کلیک کنید. تنظیمات را مطابق شکل در برگه CLI انجام دهید:

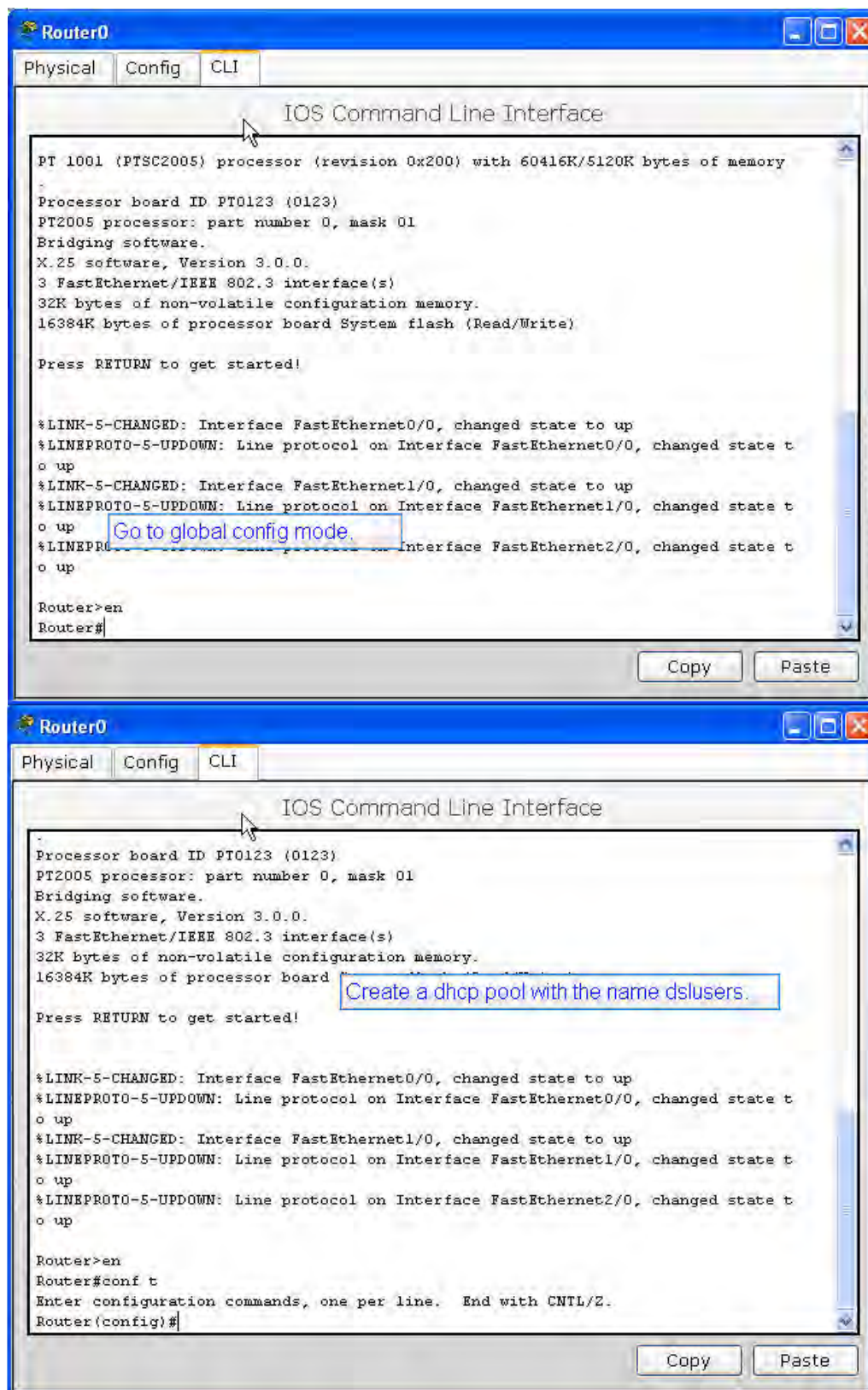
- ورودی به حالت Enable
- ورود به حالت Config
- ایجاد DHCP برای کاربران DSL
- تعیین سرور DNS برای کاربران DSL
- تعیین محدوده آدرس های DHCP
- تعیین gateway برای DHCP

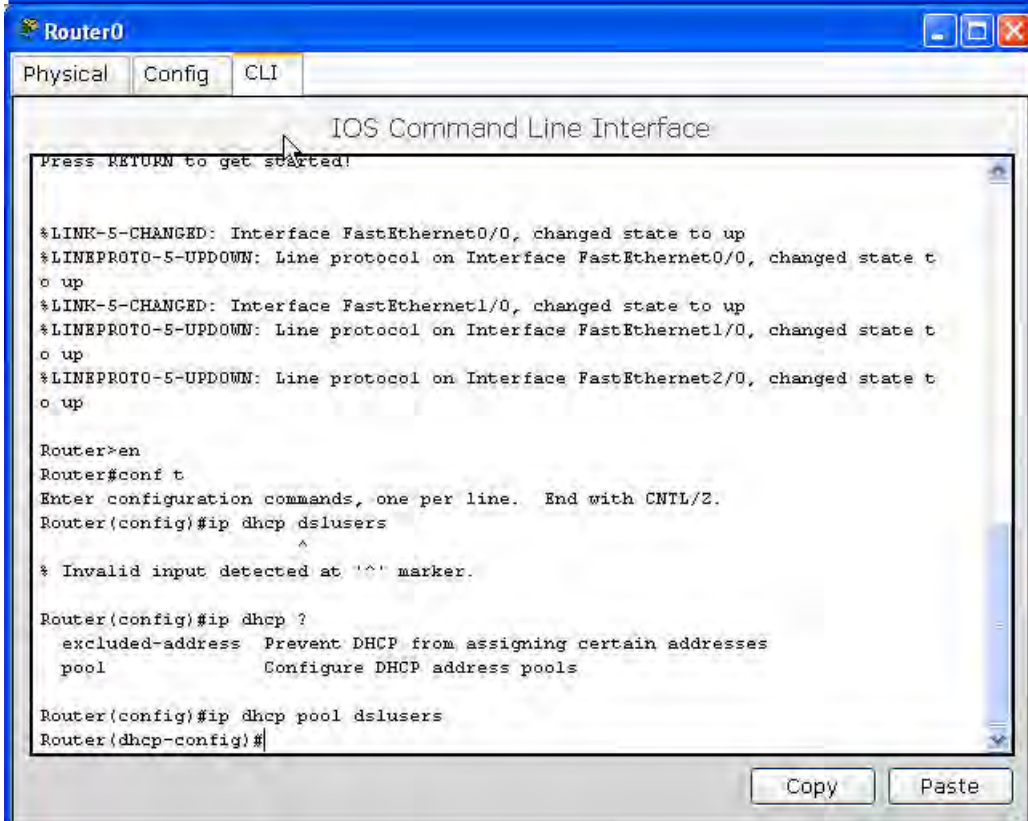
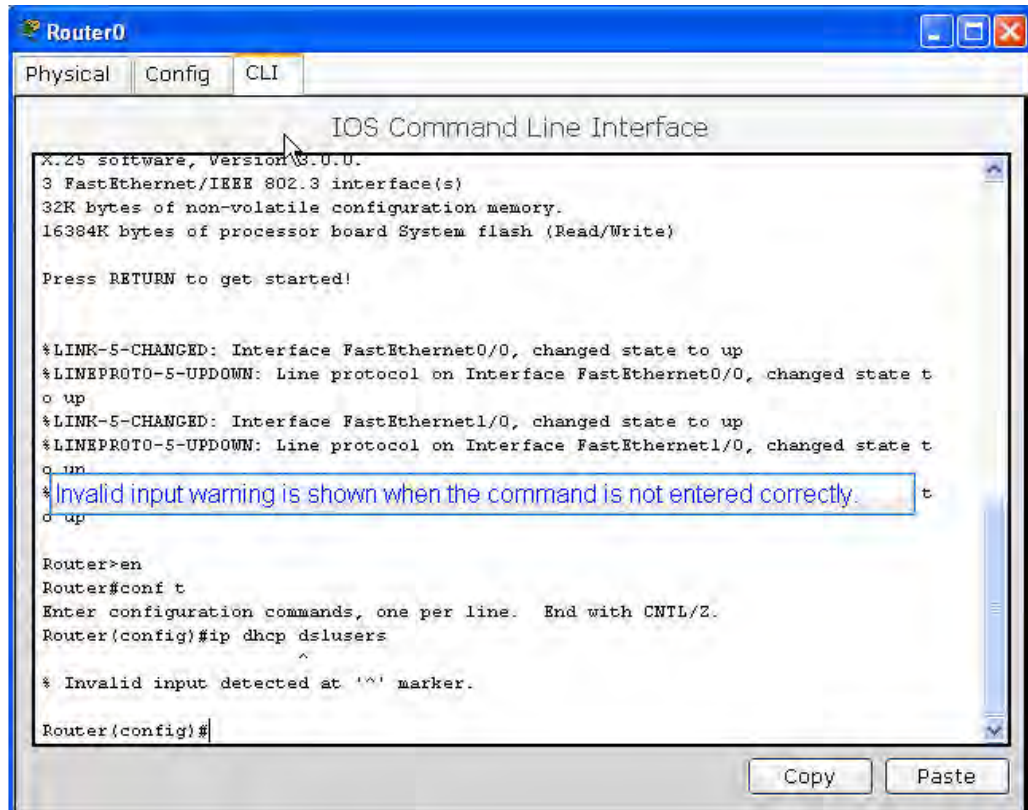






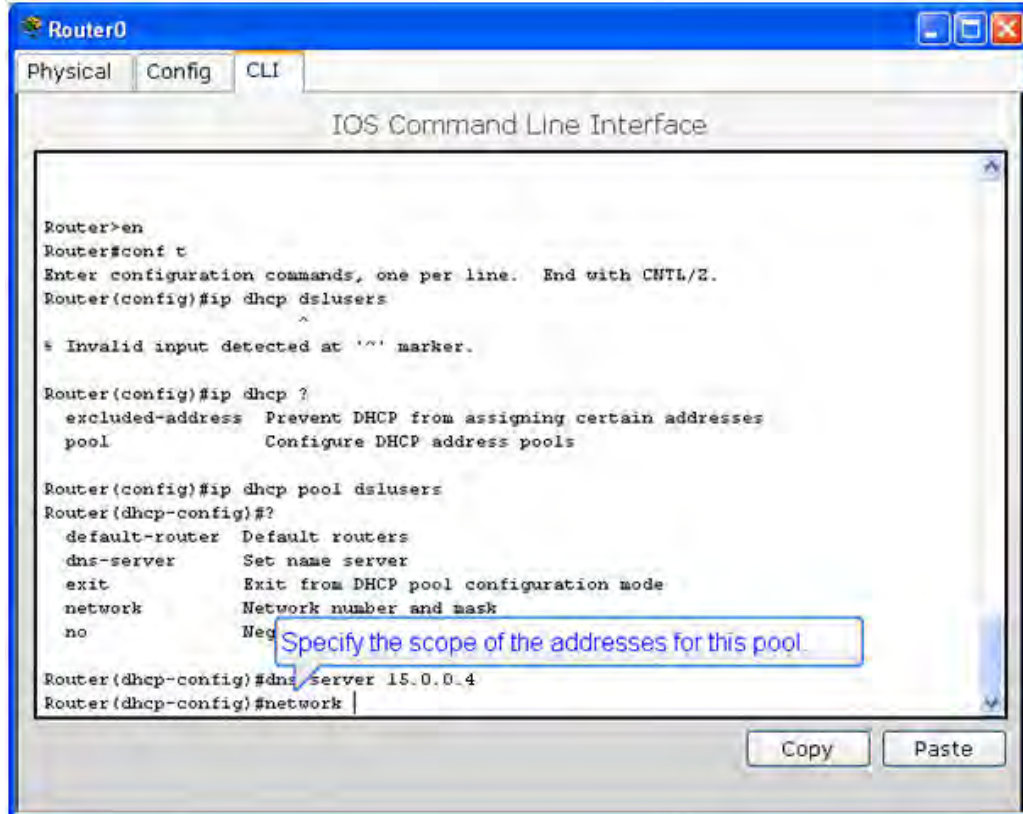
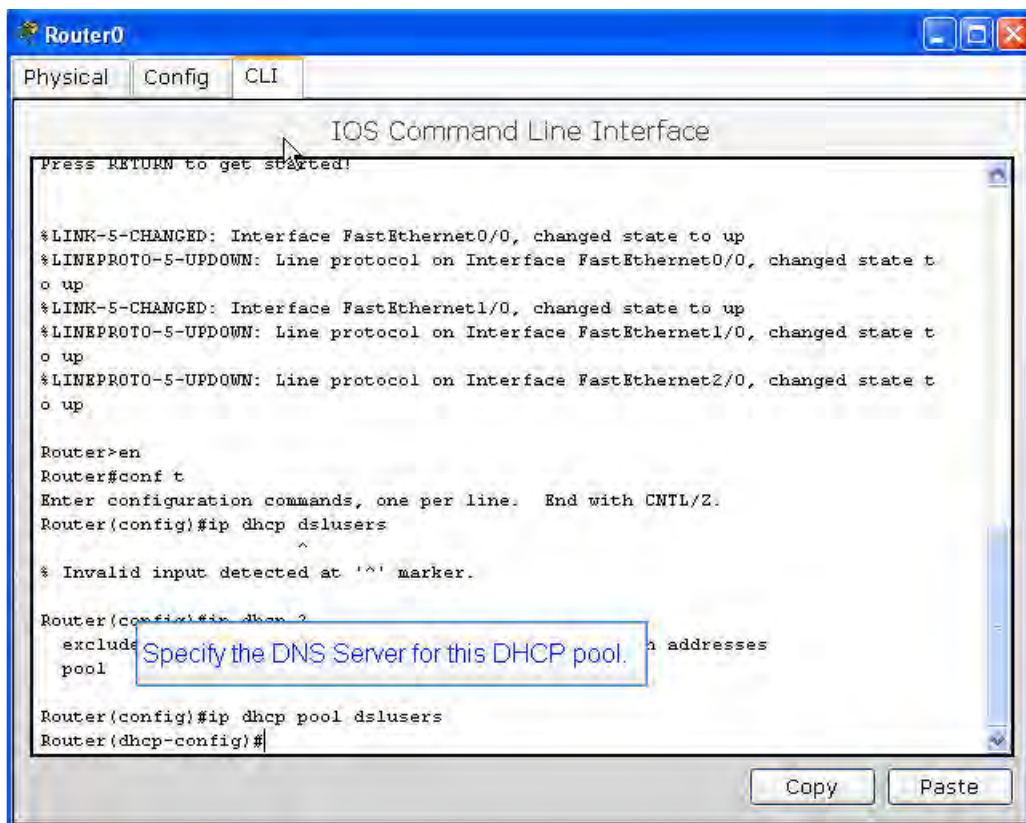
✓ فصل دوم: شبیه سازی شبکه توسط نرم افزار Packet Tracer

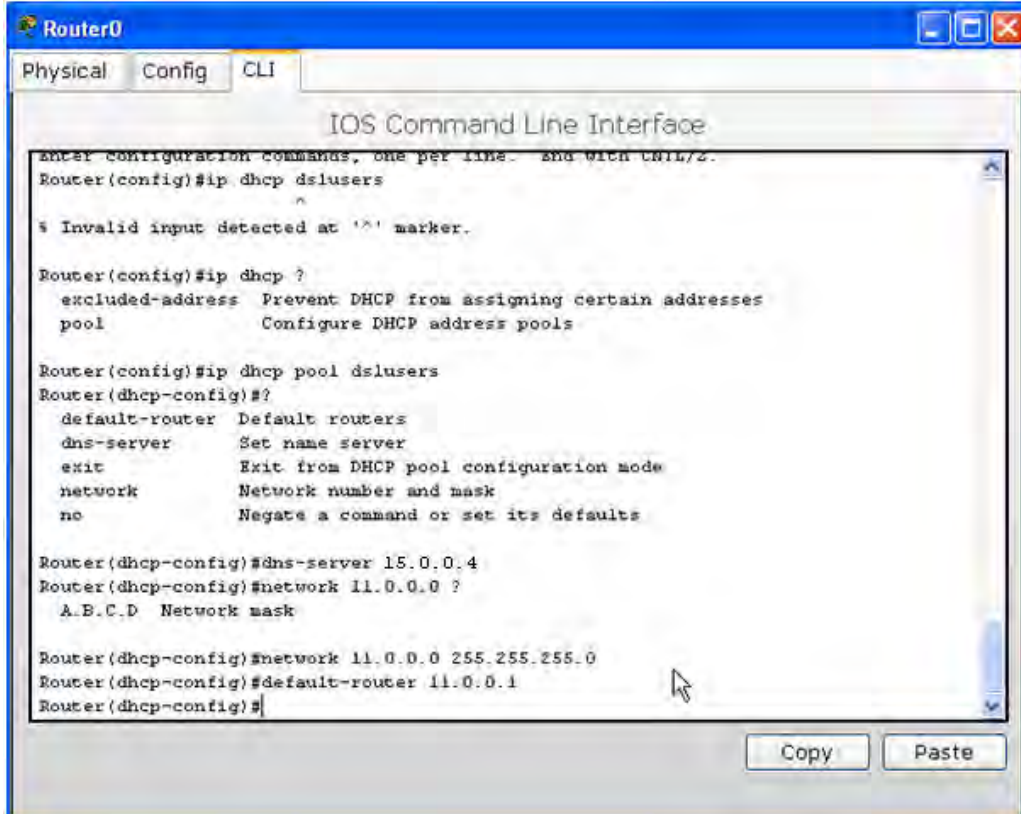
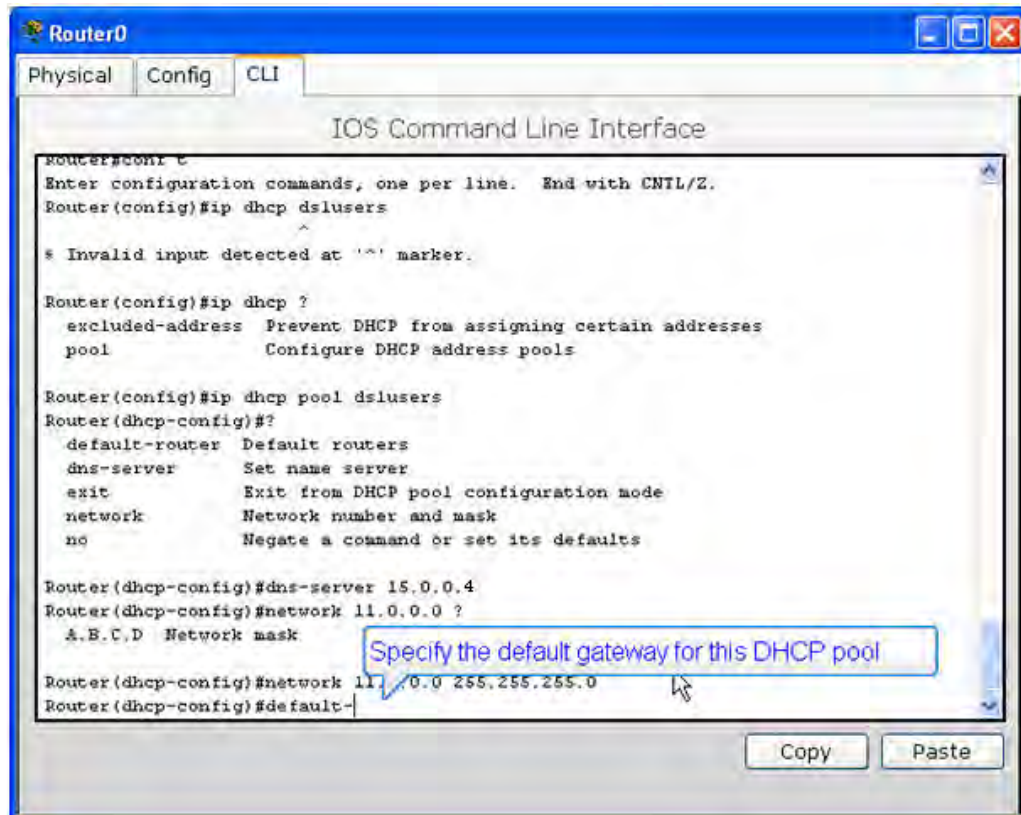




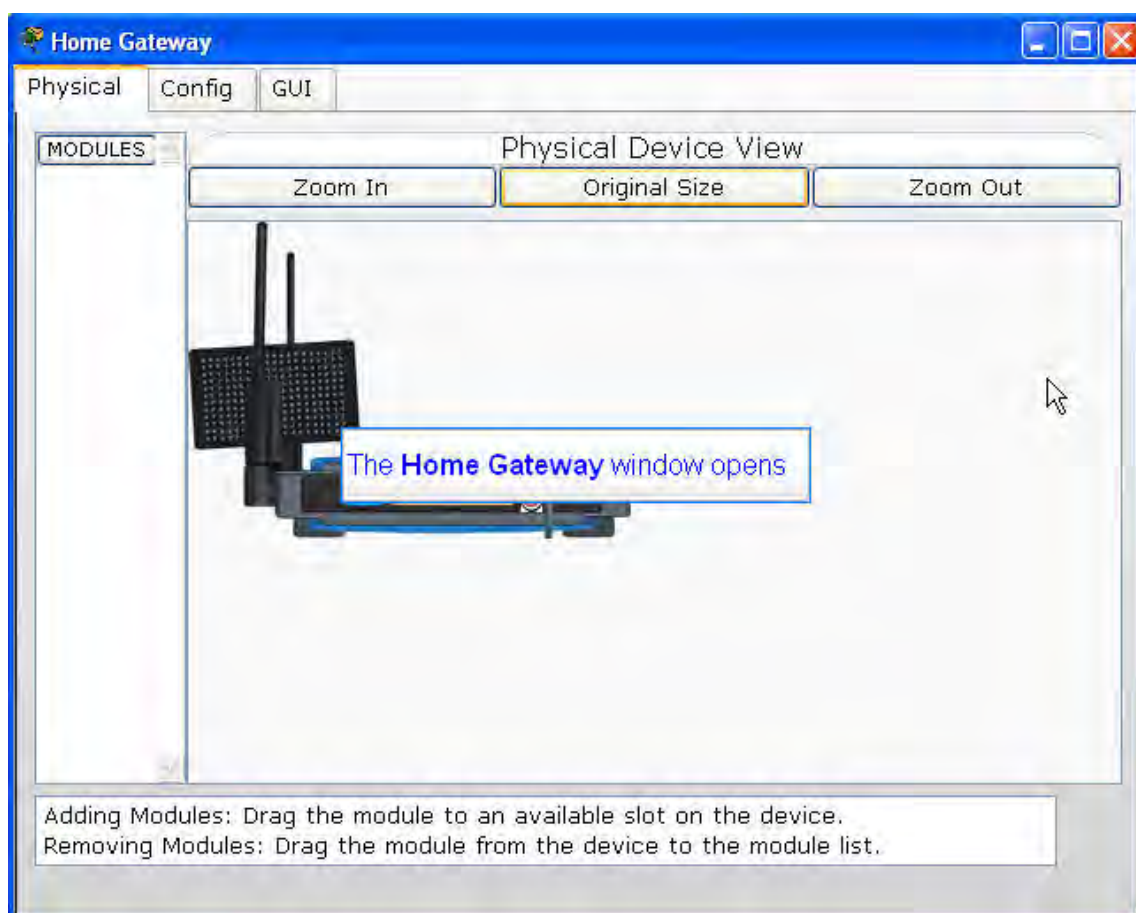


✓ فصل دوم: شبیه سازی شبکه توسط نرم افزار Packet Tracer

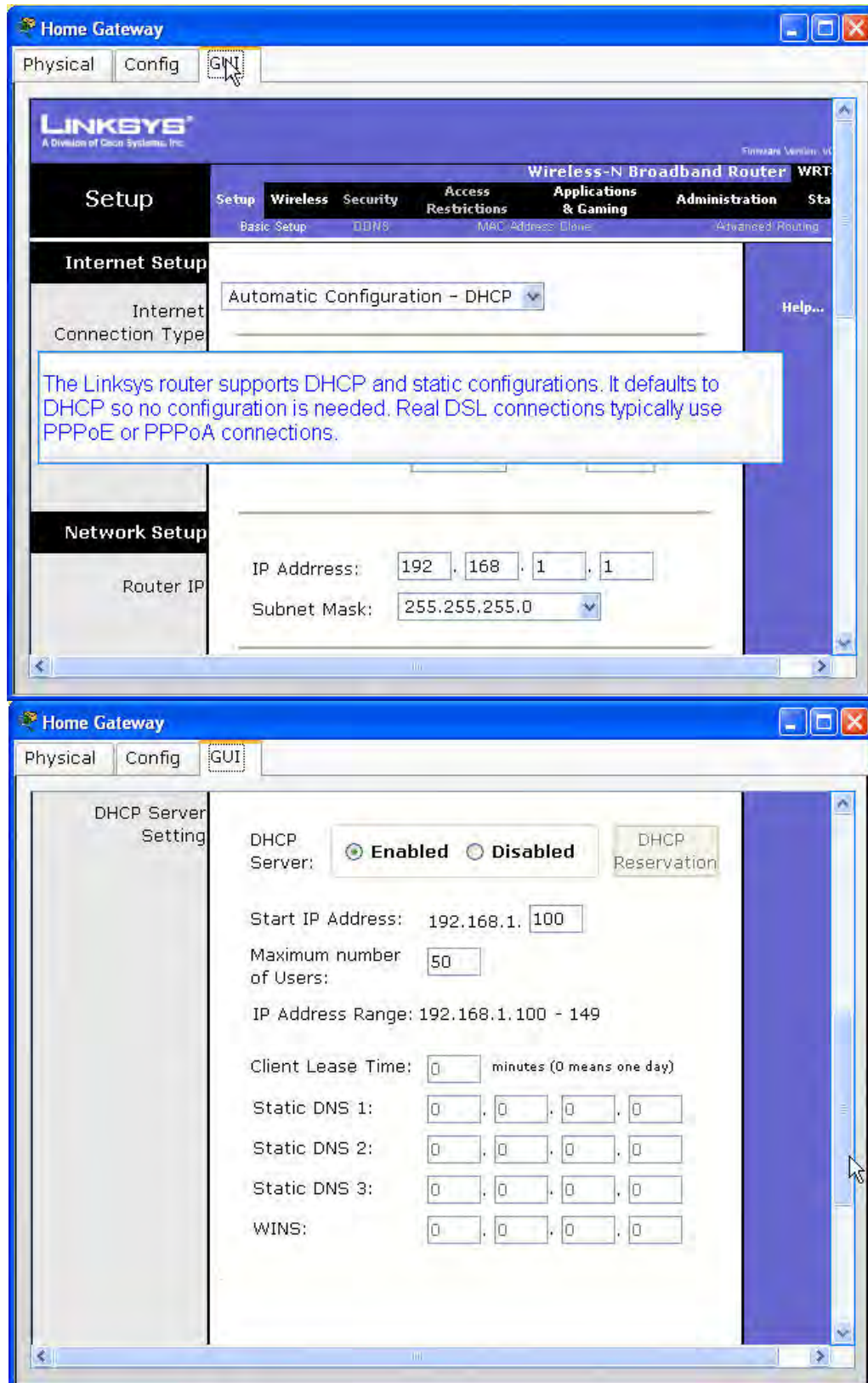




در پایان تنظیمات را ذخیره کنید. حال باید مسیریاب بیسیم Linksys را پیکربندی کنیم. روی آن کلیک کنید تا پنجره تنظیمات آن باز شود. بر روی برگه GUI کلیک کنید و تنظیمات را مطابق تصاویر دنبال کنید.

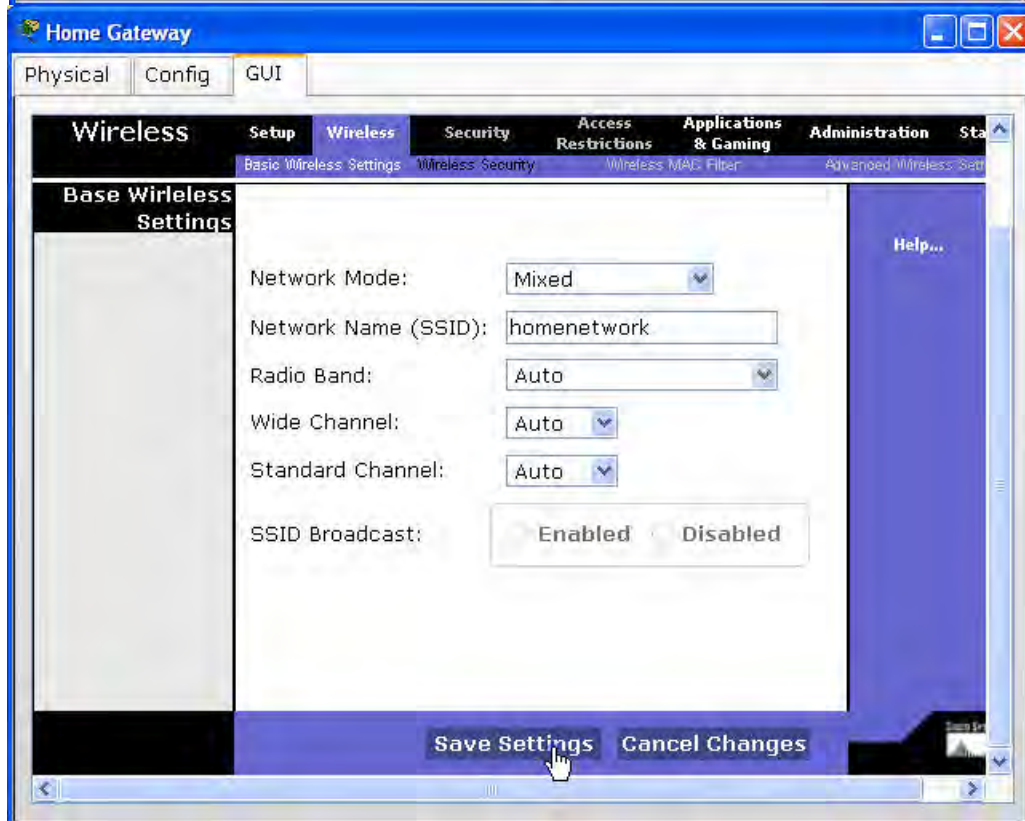
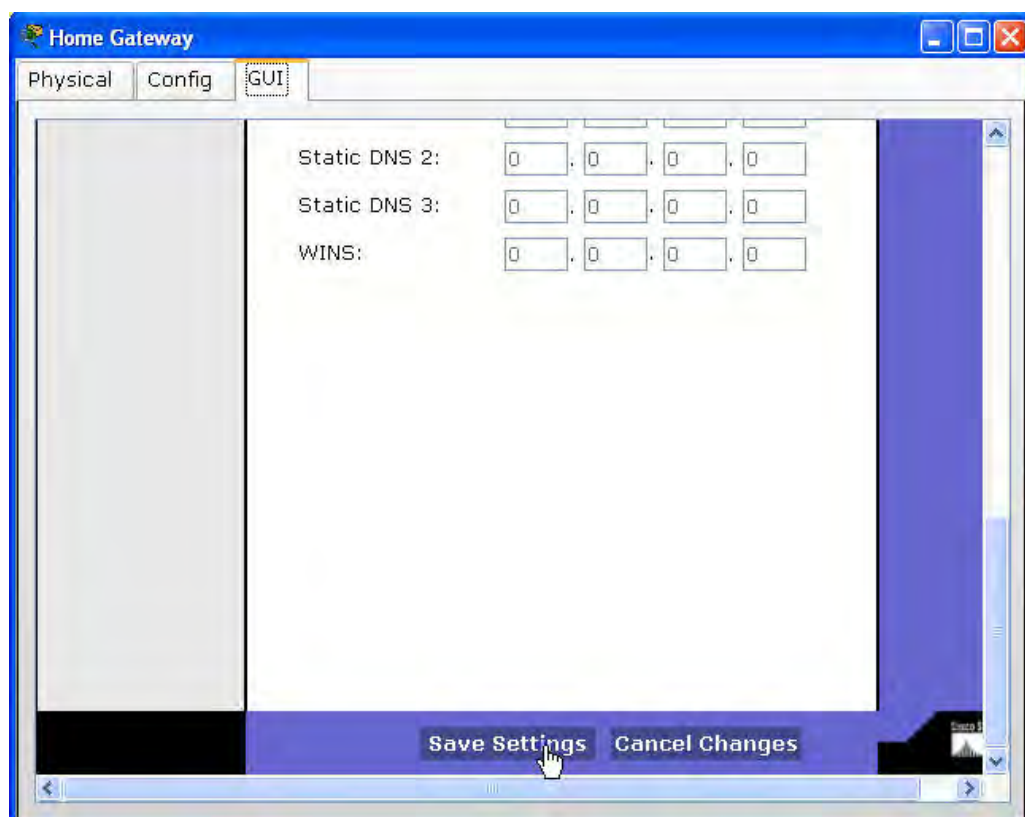


در این قسمت تنظیمات DHCP را می توان در حالت اتوماتیک قرار داد یا به صورت دستی تنظیم کرد. دقت کنید که واسطه Linksys به صورت تحت وب است و در صورت هرگونه تغییر در تنظیمات هر صفحه ، باید همان صفحه به طور جداگانه ذخیره شود.

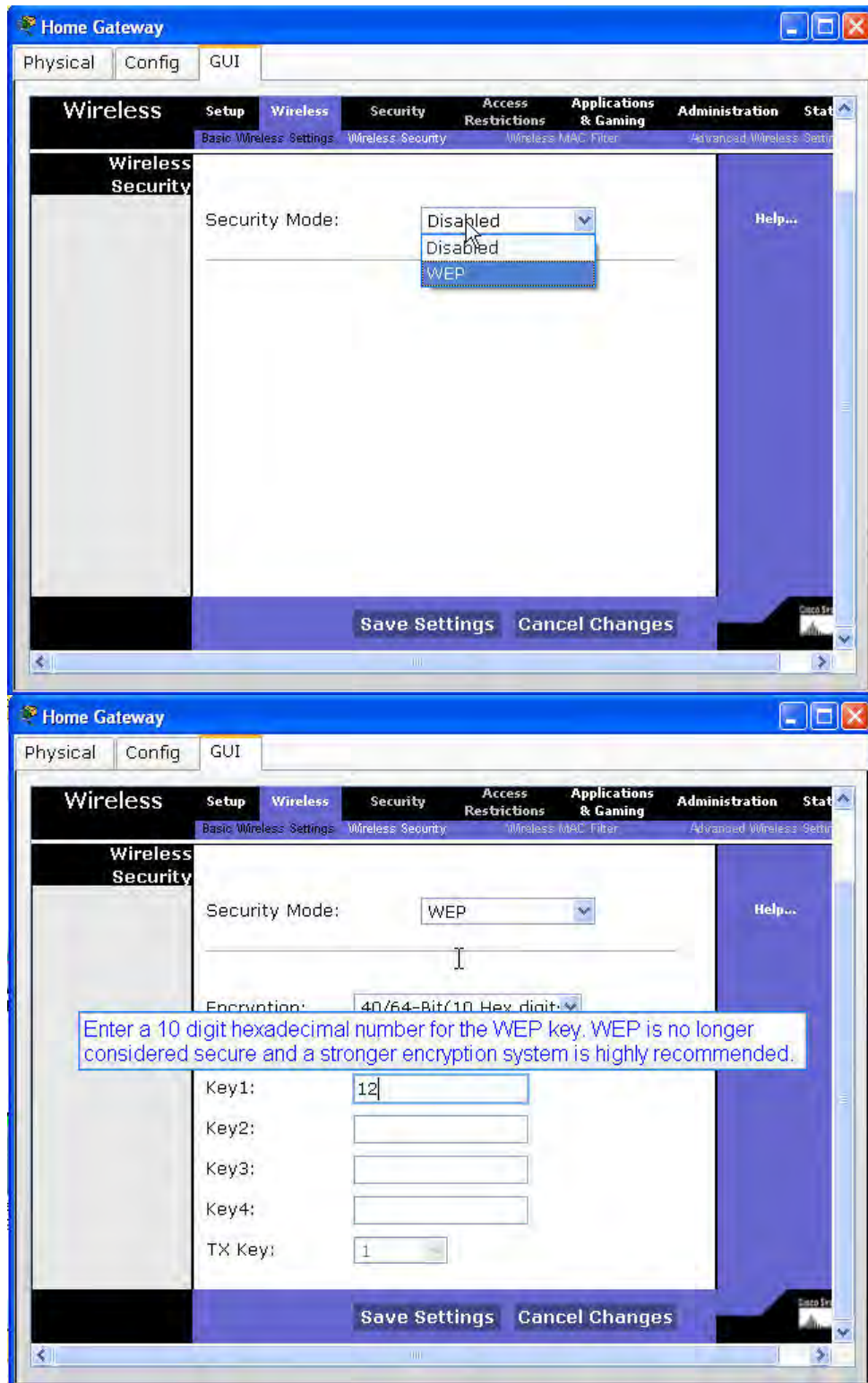


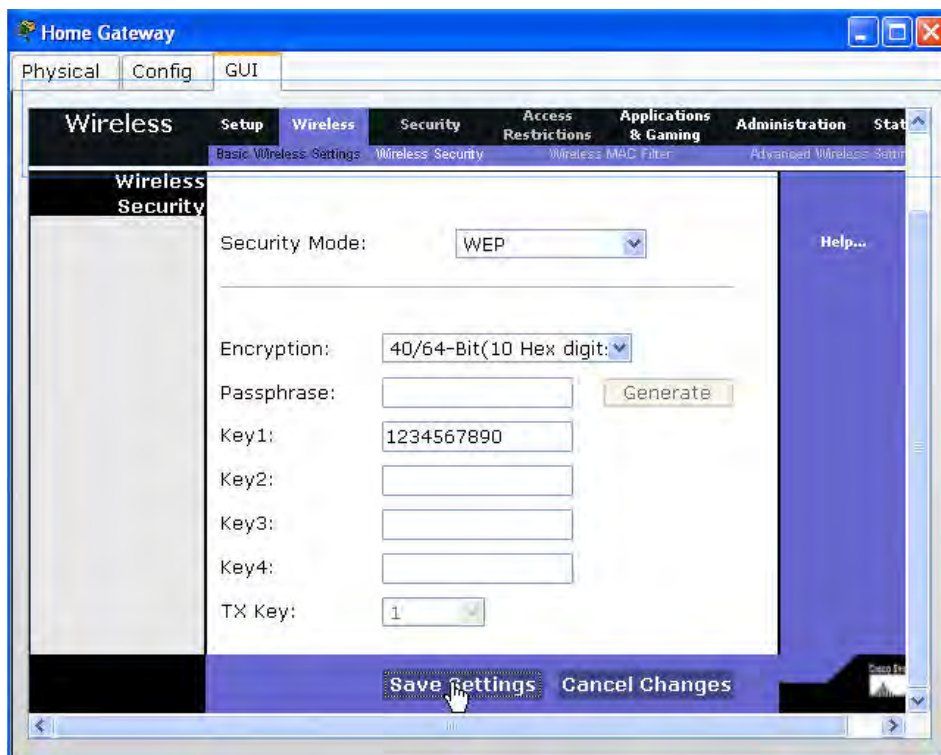


✓ فصل دوم: شبیه سازی شبکه توسط نرم افزار Packet Tracer

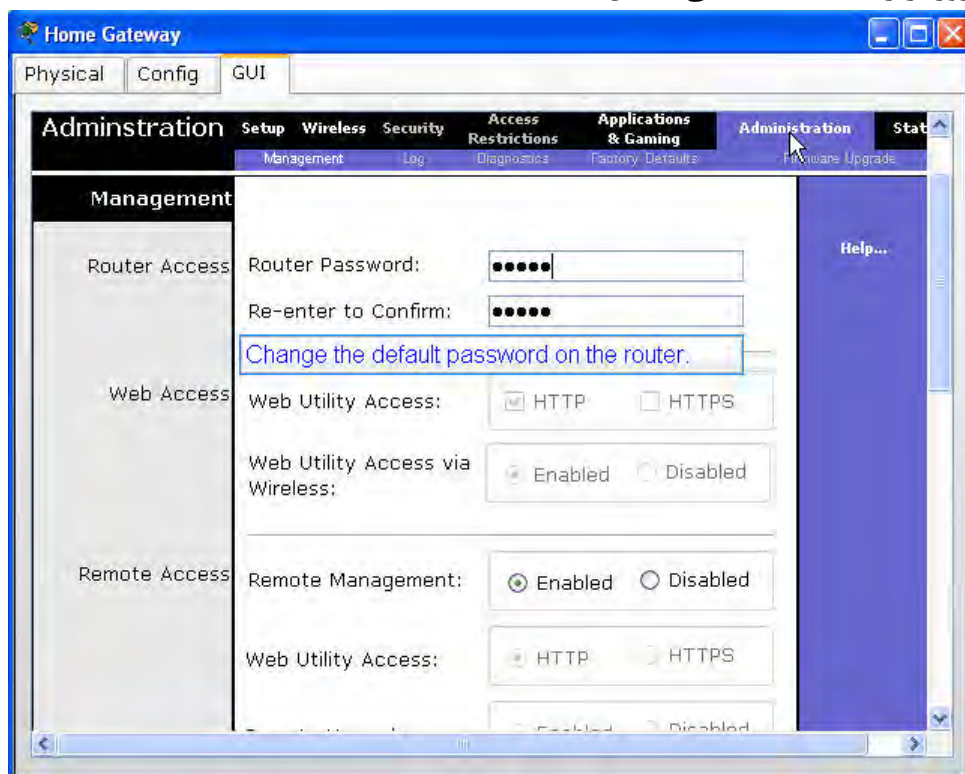


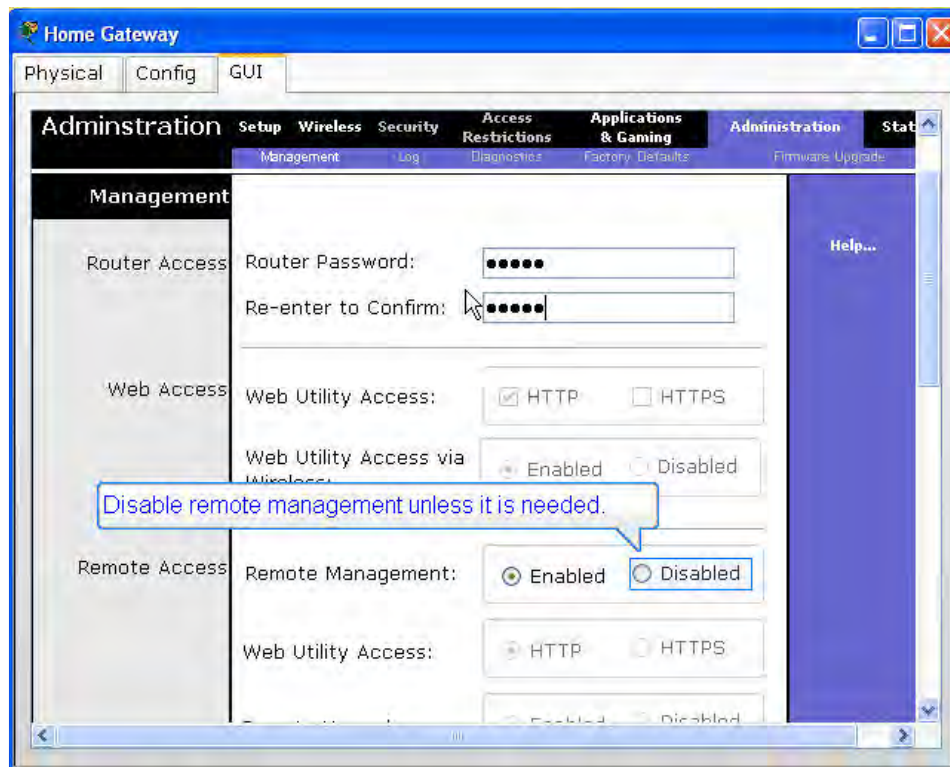
در این قسمت می توانید تنظیمات امنیتی را فعال کرده و یک کلید برای احراز هویت کاربرانی که قصد اتصال به صورت بیسیم دارند تعیین کنید.



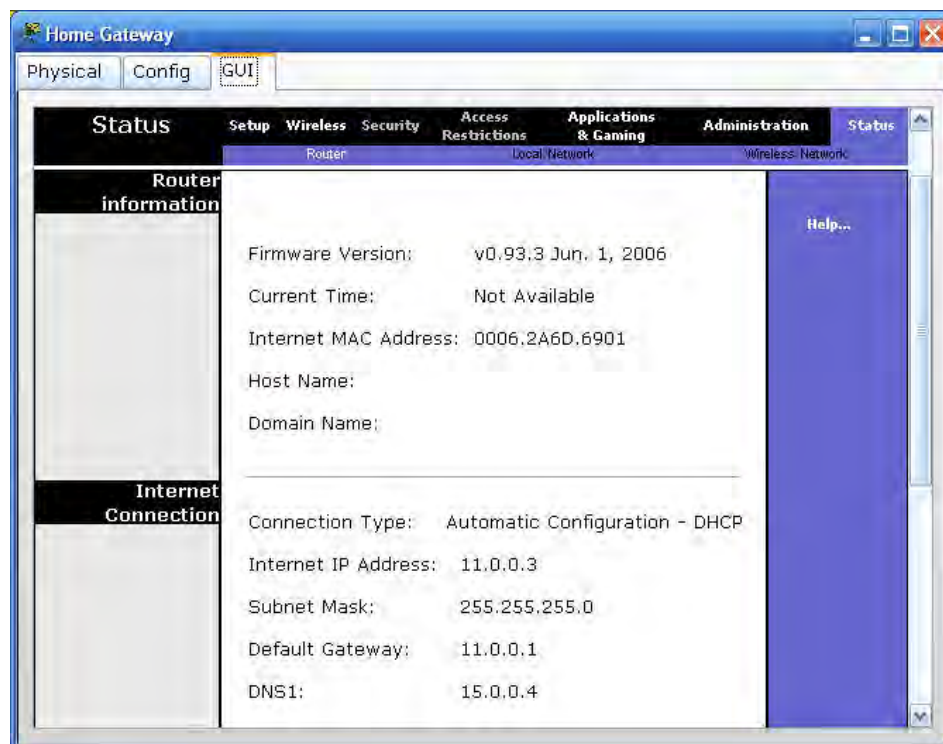


در این قسمت می توانید یک نام و کلمه عبور برای ورودی به تنظیمات Linksys از راه دور و از طریق مرورگر رایانه های شخصی تعیین کنید.

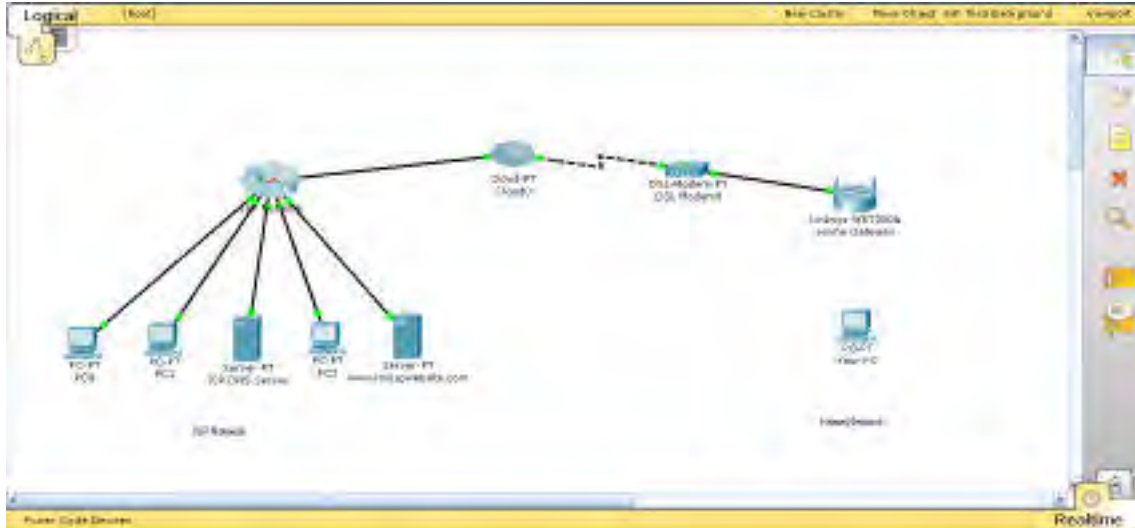




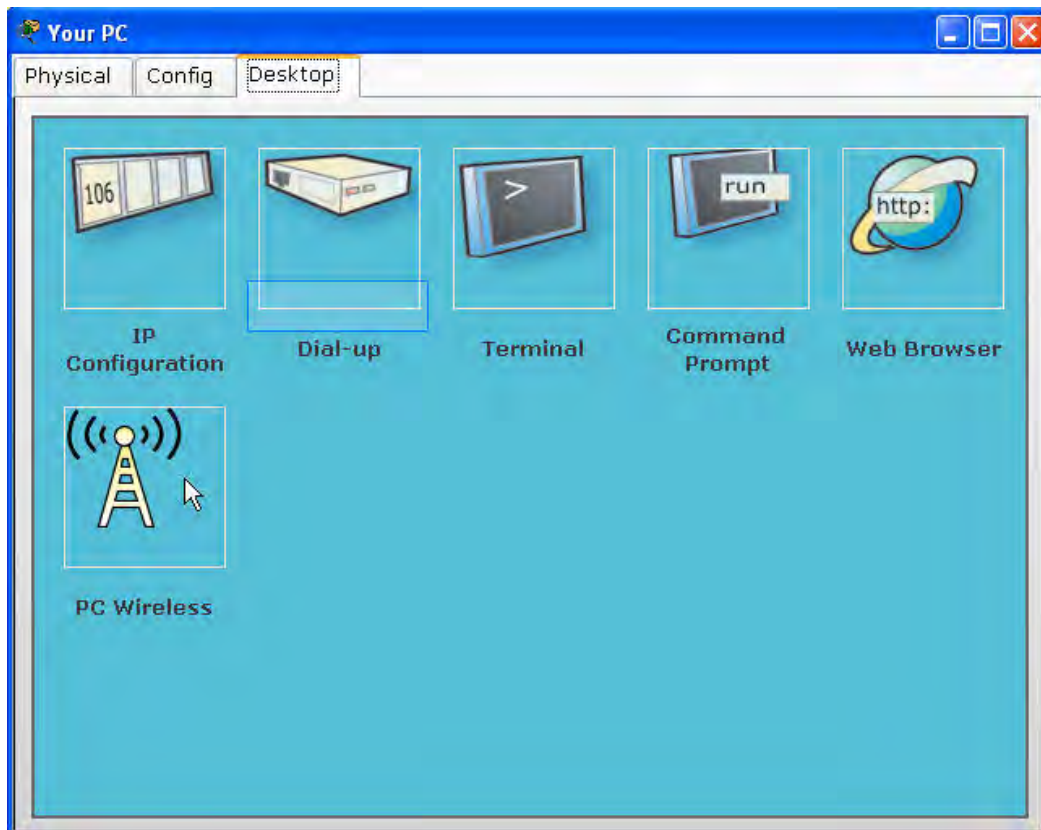
در قسمت Status وضعیت مسیریاب به طور خلاصه نمایش داده شده است.



با مراجعه به صفحه اصلی مشاهده خواهید کرد که ارتباط بین Your PC و مسیریاب LinkSys در شبکه خانگی ما قطع شده است. علت آن فعال کردن تنظیمات امنیتی است که می بایست برای برقراری اتصال پیکربندی شوند.



بر روی YourPC کلیک کنید و سپس وارد برگه Desktop شوید.

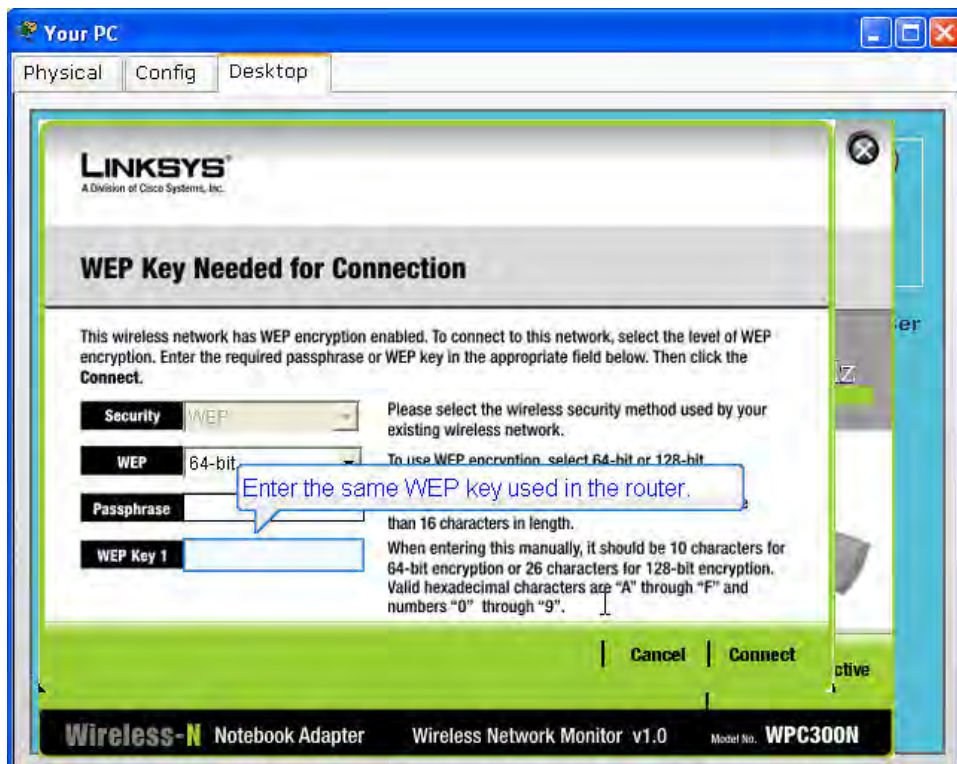


بر روی PC Wireless کلیک کنید تا تنظیمات شبکه بی سیم ظاهر شود.

در برگه Connect روی دکمه refresh کلیک کنید تا شبکه های بی سیم فعلی مشاهده شوند.

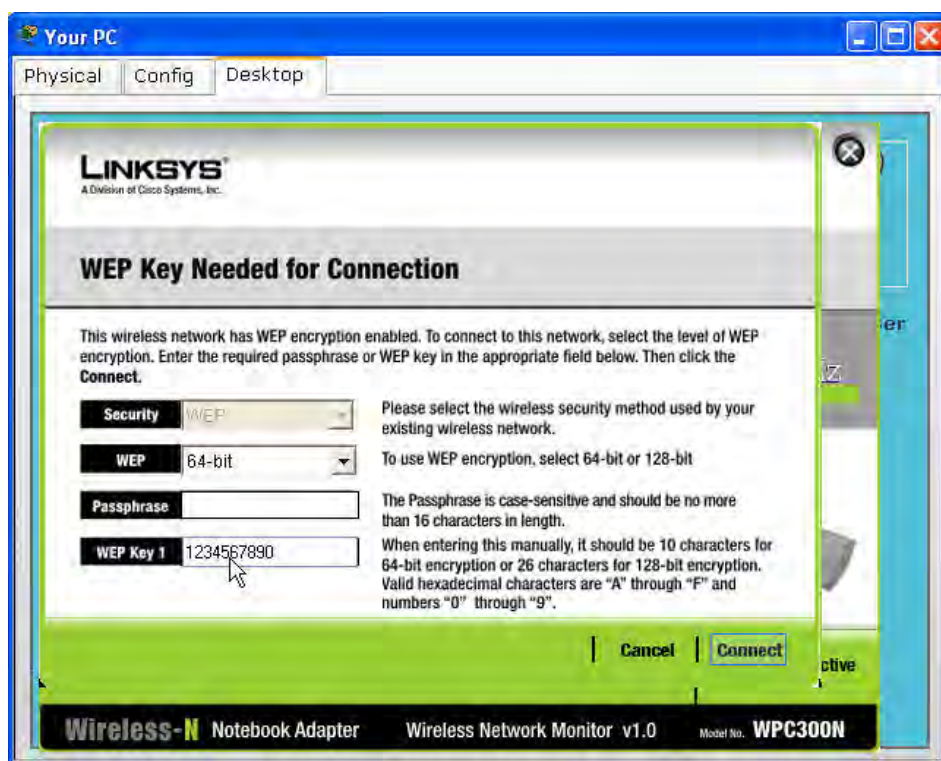


در صورتی که بر روی connect کلیک کنید، کلید احراز هویت از شما درخواست می شود.

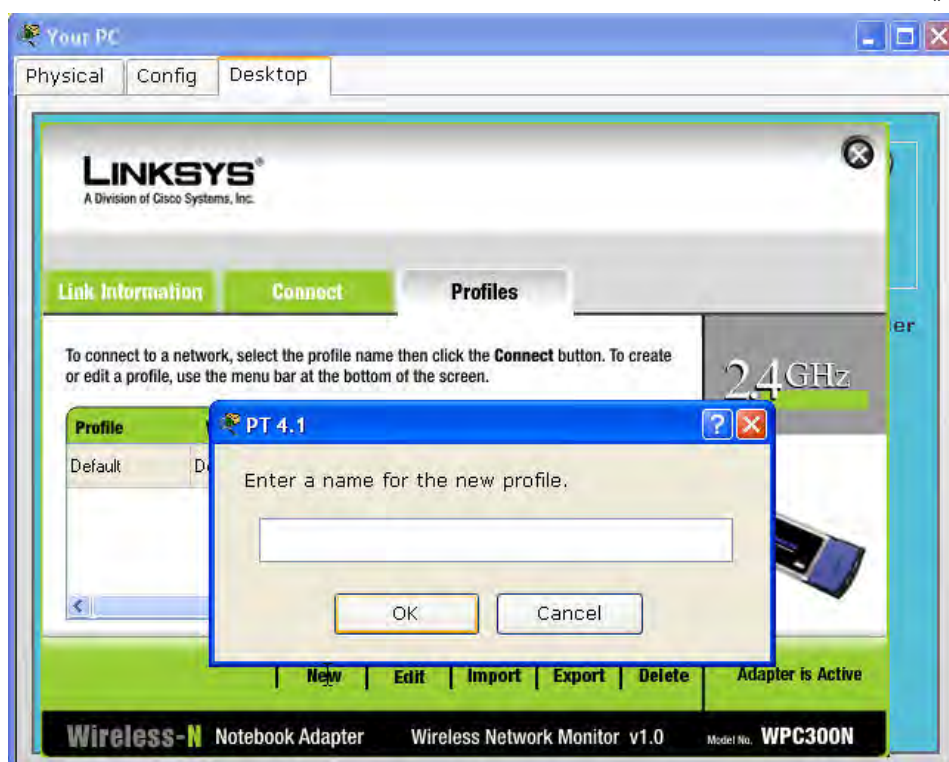


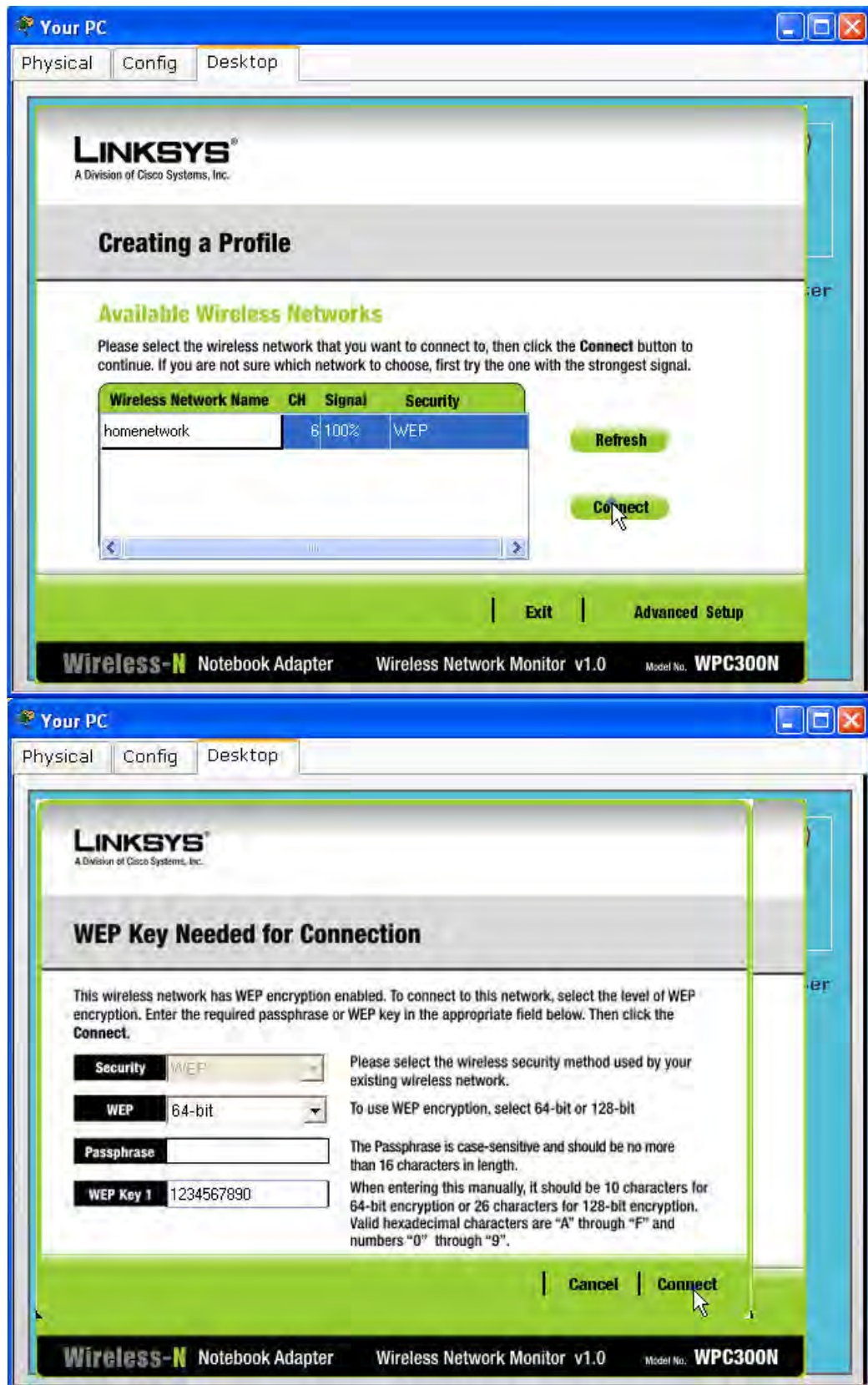


✓ فصل دوم: شبیه سازی شبکه توسط نرم افزار Packet Tracer



شما می توانید تنظیمات مربوط به شبکه را جهت دسترسی سریعتر در آینده در یک Profile ذخیره کنید.



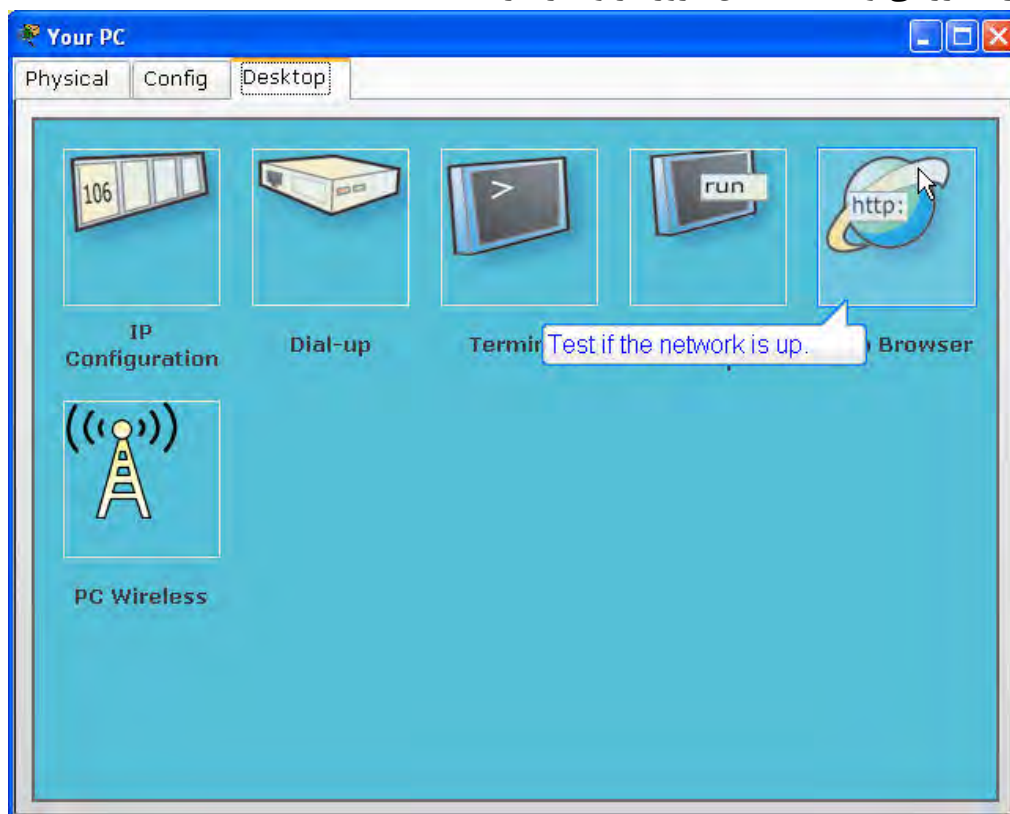




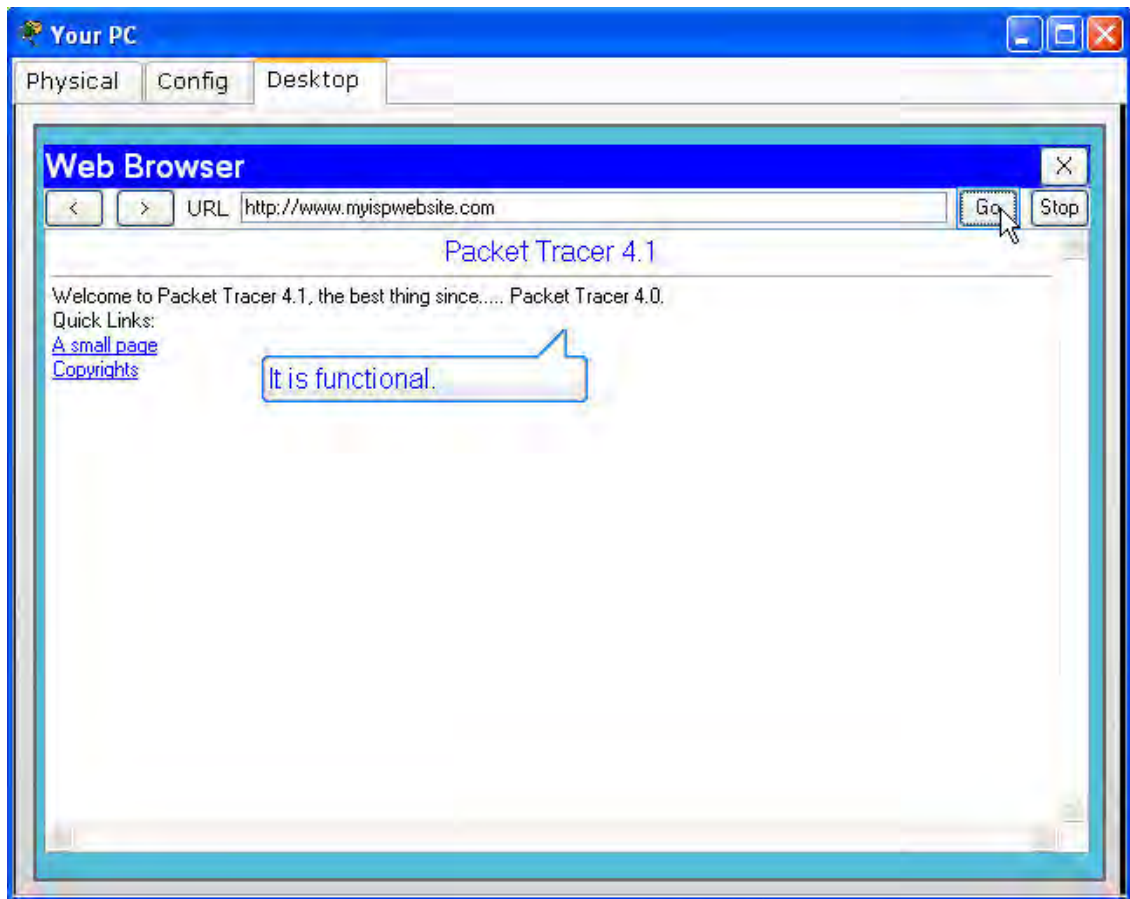
✓ فصل دوم: شبیه سازی شبکه توسط نرم افزار Packet Tracer



حال برای بررسی وضعیت اتصال مرور گر وب را باز کنید.



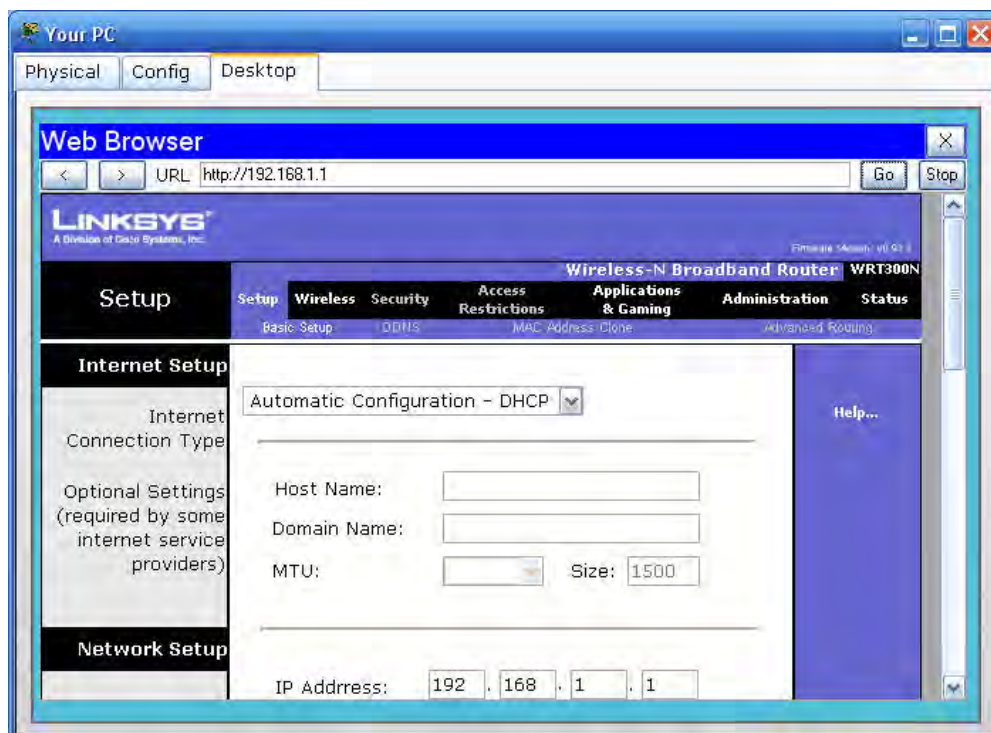
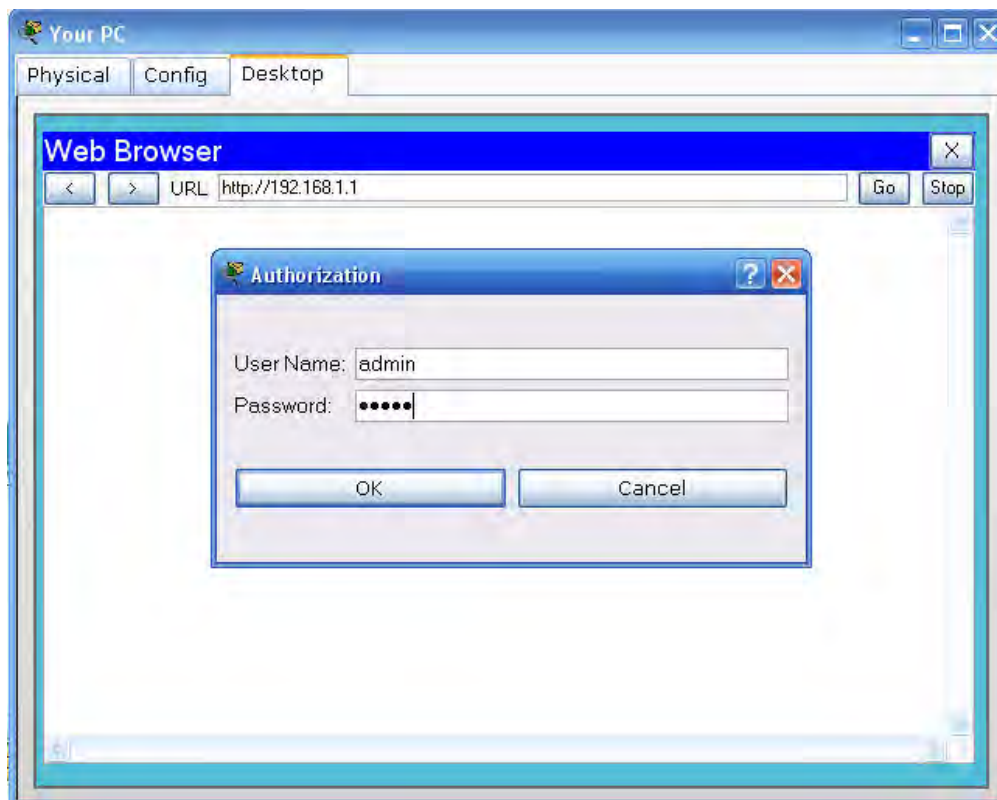
آدرس سایت www.myispwebsite.com را که قبلا در سرور dns نیز آن را اضافه کردید وارد کنید. در صورتیکه تنظیمات شبکه را تا به اینجا به خوبی انجام داده باشید، می بایست صفحه وب به شما نمایش داده شود.



علاوه بر این شما می توانید به تنظیمات مسیریاب Linksys نیز دسترسی داشته باشید. آدرس IP مسیریاب را در نوار آدرس وارد کنید. پس از ورود نام کاربری و کلمه عبور (در حالت پیش فرض هر دو admin هستند) می توانید تنظیمات را از طریق وب انجام دهید.



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



Activity Wizard

Activity Wizard یک ابزار ارزیابی است که به شما امکان ایجاد سناریو های شبکه دلخواه و متنوعی را برای دیگر کاربران فراهم می آورد. این ابزار مخصوصا برای اساتید جهت ایجاد تمرین (فعالیت) برای دانشجویان مفید است. زمانی که دانشجویان یک فعالیت را شروع می کنند، با یک شبکه اولیه و مجموعه ای از دستورالعمل ها مواجه هستند. دانشجویان باید دستورالعمل ها را دنبال کرده و فعالیت را تکمیل کنند. آن ها می توانند شبکه کامل شده خود را با راه حل آن بررسی کنند. نکته مهم این است که استاد بر روی همه حالت های فعالیت کنترل کامل دارد.



ترتیب معمول ایجاد فعالیت به صورت زیر است:

- ۱- ایجاد شبکه پاسخ و تنظیم آیتم های ارزیابی، تست های اتصال و فیدبک کلی
- ۲- ایجاد شبکه اولیه که نقطه شروع دانشجویان است. معمولا مشابه شبکه پاسخ است که برخی ویژگی های آن حذف شده، یا برخی تنظیمات پیکربندی وجود ندارد یا دستگاه ها اشتباه پیکربندی شده اند و...
- ۳- قرار دادن محدودیت هایی بر روی برخی ویژگی ها و قابلیت ها در طول انجام فعالیت
- ۴- تنظیمات متغیرهای مدیریت برای افزودن پویایی به فعالیت
- ۵- نوشتن یا دستورالعمل واضح برای فعالیت



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

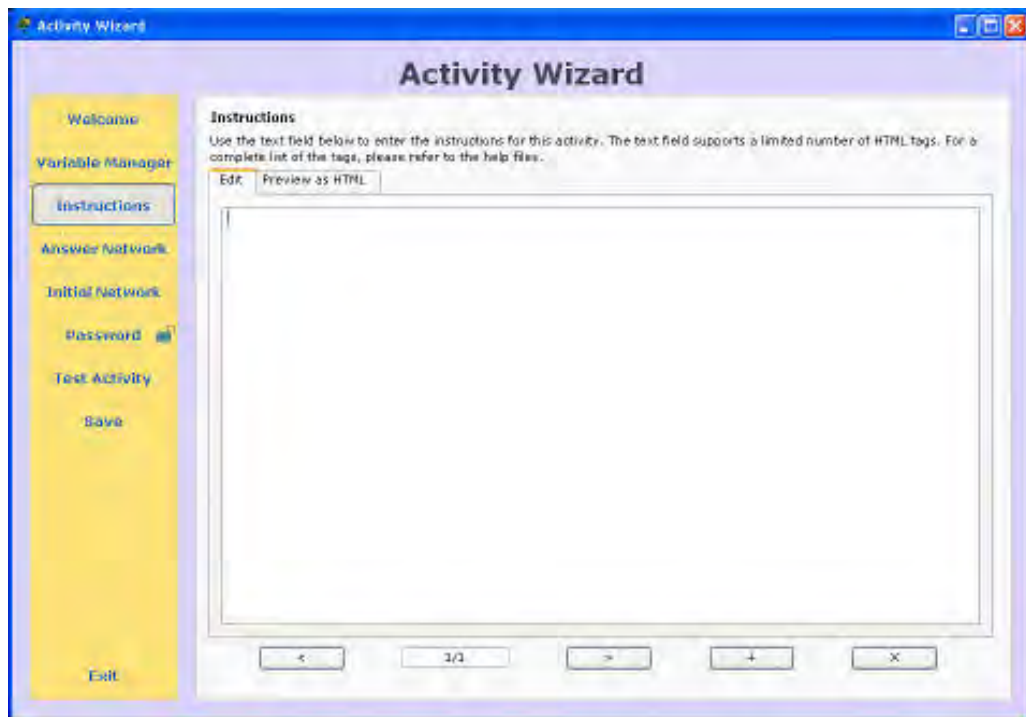
۶- محافظت از فعالیت با کلمه عبور برای جلوگیری از تغییرات ناخواسته

۷- ذخیره کردن فعالیت.

دسترسی به Activity Wizard از منوی file امکان پذیر است. با اجرای این دستور شما می توانید انتخاب کنید که از فضای کار فعلی بعنوان پاسخ استفاده شود یا یک فضای کار جدید ایجاد شود. توسط Activity Menu در سمت چپ می توانید حالت های مختلف فعالیت را تنظیم کنید و بعد از ایجاد فعالیت، با استفاده از Save در Activity Menu می توانید آنرا ذخیره نمایید (با فرمت pka).

پانل دستورالعمل ها (Instructions)

شما دستورالعملهای دانشجویان را جهت انجام فعالیت در این پانل می نویسید. وقتی دانشجویان فایل فعالیت را بازکنند، این دستورالعمل ها در پنجره جداگانه ای نمایش داده خواهد شد تا قابل مشاهده باقی بماند. این دستورالعمل ها باید به وضوح اهداف فعالیت را شرح دهند. اگر محدودیت خاصی وجود دارد باید روش مورد نظر اشاره شود تا موجب سردرگمی دانشجویان با آیتم ها و توابع قفل شده نگردد. برای قالب بندی دستورالعمل شما می توانید از تگ های HTML استفاده کنید. این امکان وجود دارد که دستورالعمل ها را در چندین صفحه جداگانه بنویسید تا شلوغی صفحه کاهش داده شود.

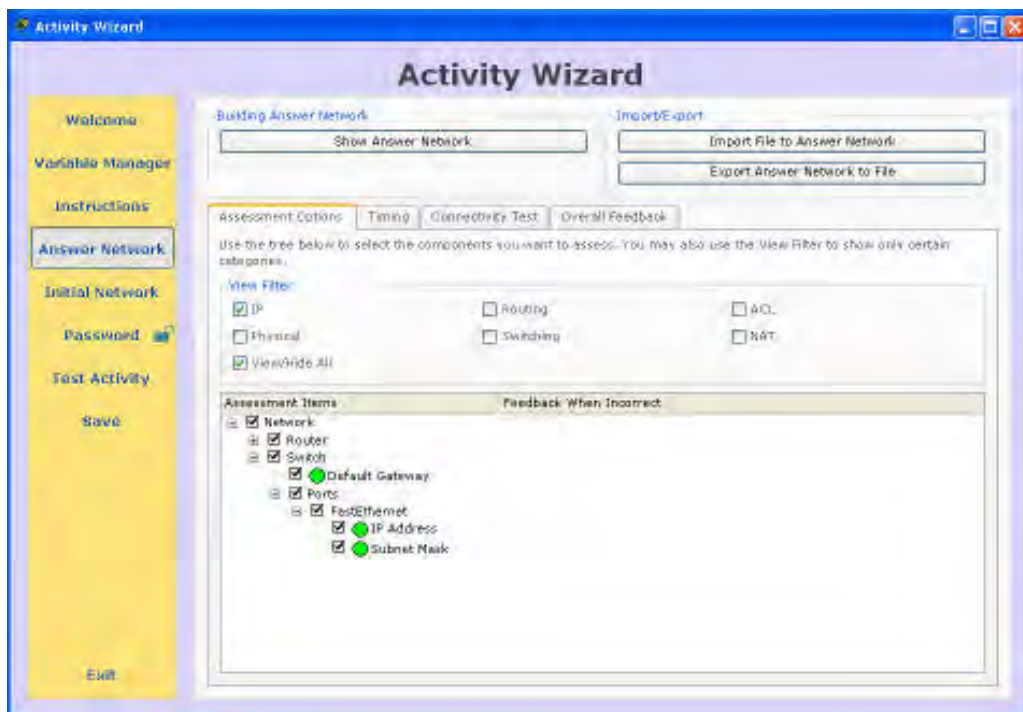


تگ های HTML پشتیبانی شده توسط این قسمت شامل موارد زیر می باشد:

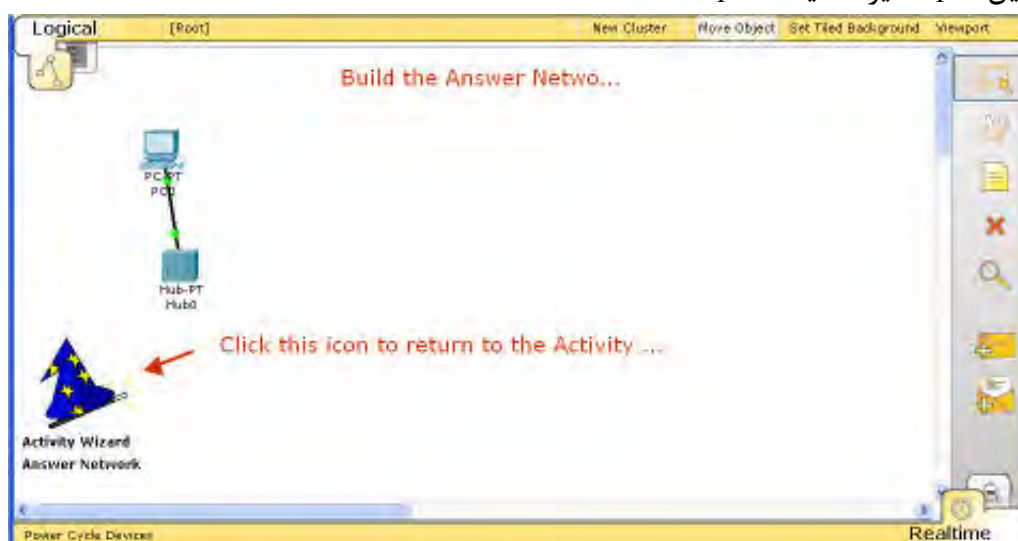
- <p>
-

-
- <i>
- <pre>
-
-

پانل شبکه پاسخ (Answer Network)



در پانل شبکه پاسخ، شما می توانید شبکه نهایی (راه حل) را ایجاد کنید و عناصر مورد ارزیابی را مشخص کنید. روی Show Answer Network کلیک کنید تا فضای کار جهت ایجاد شبکه نمایش داده شود. در این قسمت شما می توانید یک فایل pkt که قبلا ایجاد کرده اید را نیز import کنید و از شبکه آن استفاده نمایید. در هر صورت پس از تکمیل شبکه پاسخ، می توانید آن را به صورت یک فایل pkt ذخیره کنید (export).

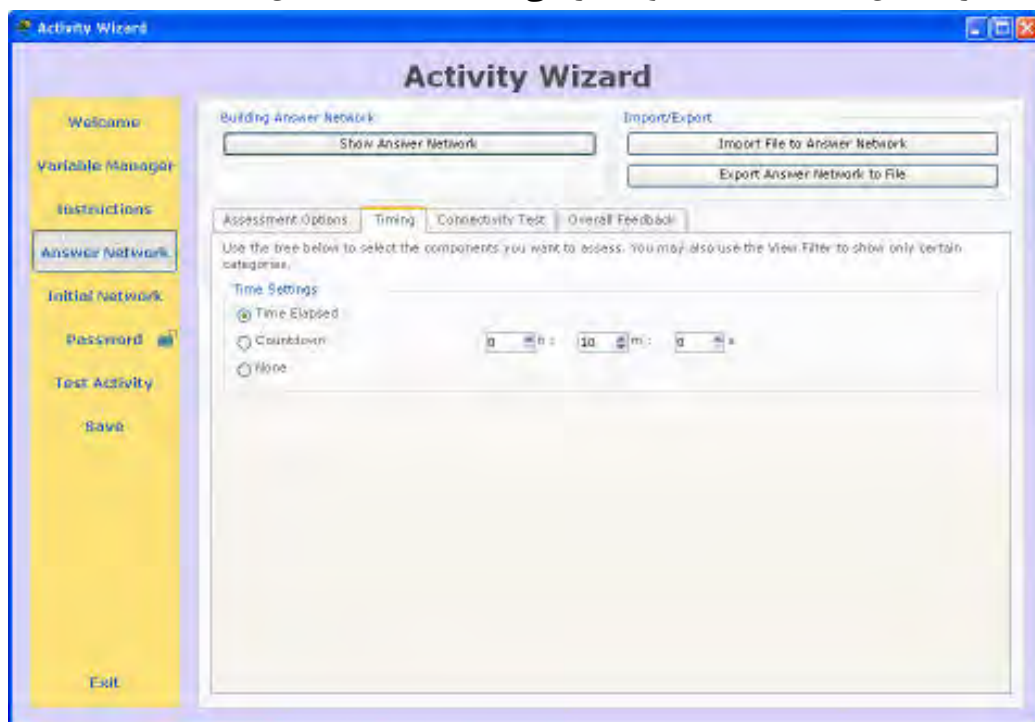


تنظیم آیتیم های ارزیابی

آیتیم های ارزیابی باید با پیکربندی های موجود در شبکه پاسخ منطبق باشد. شما می توانید آیتیم های مورد نظر را در درخت نمایش داده شده فعال کنید. برای راحتی کار می توانید ویژگی های خاصی را از درخت پنهان نمایید. این کار با استفاده از فیلترهای مختلفی که در قسمت بالای کادر قرار دارد انجام می شود. برای مثال با غیر فعال کردن فیلتر Routing همه گروه های مرتبط با مسیریابی از جمله مسیرهای استاتیک، پویا و RIP پنهان خواهد شد. همچنین شما می توانید آیتیم هایی را برای فیدبک مشخص کنید تا امکان راهنمایی دانشجویان در صورت انجام اشتباه فعالیت، در زمان مشاهده نتیجه فراهم آورده شود.

تنظیمات زمان

شما می توانید تنظیماتی را در مورد زمان بندی فعالیت انجام دهید. مثلا زمان سپری شده (Time Elapsed) را نمایش دهید یا یک محدودیت زمانی (Countdown) اعمال کنید.



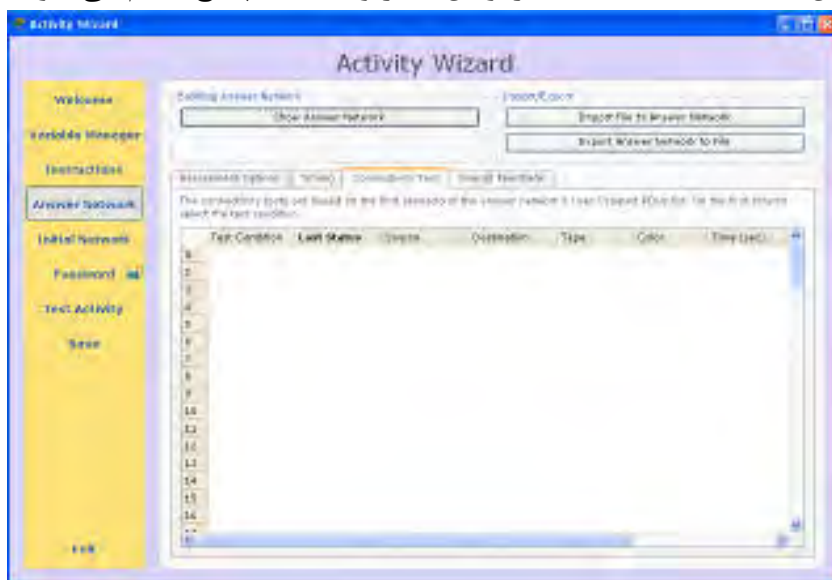
بررسی اتصالات

ویژگی Connectivity Testing روش دیگری برای ارزیابی است. برخلاف آیتیم های ارزیابی که پیکربندی های شبکه را بررسی کرده و آن را با پیکربندی شبکه پاسخ مقایسه می کنند، این



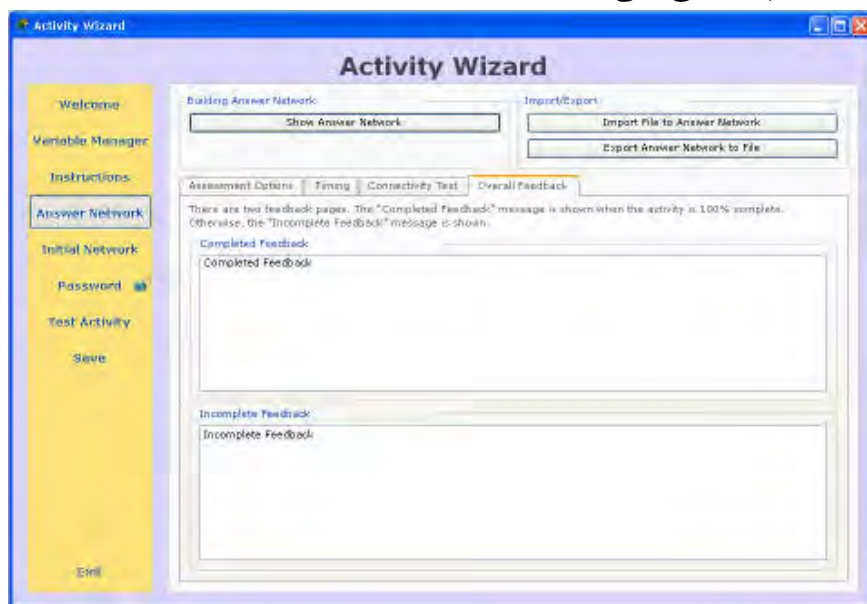
✓ فصل دوم: شبیه سازی شبکه توسط نرم افزار Packet Tracer

قسمت بر اساس PDU های realtime ای است که در حین مشاهده نتیجه بررسی می گردند. این بررسی بر اساس PDU های ایجاد شده در اولین سناریوی شبکه پاسخ انجام می شود.

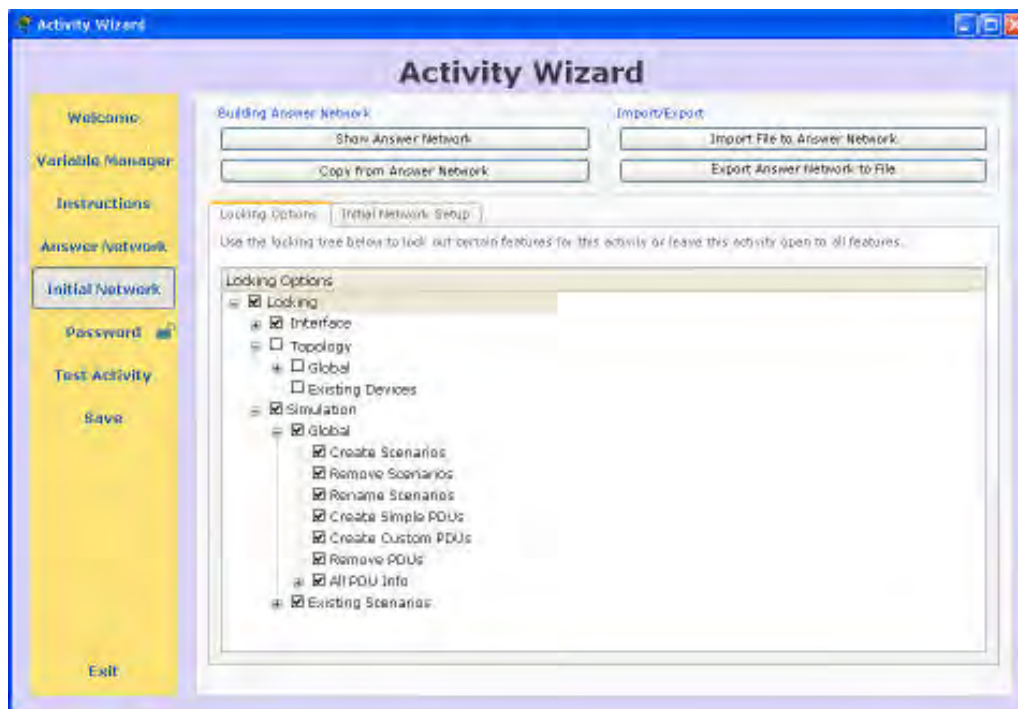


فیدبک کلی (Overall Feedback)

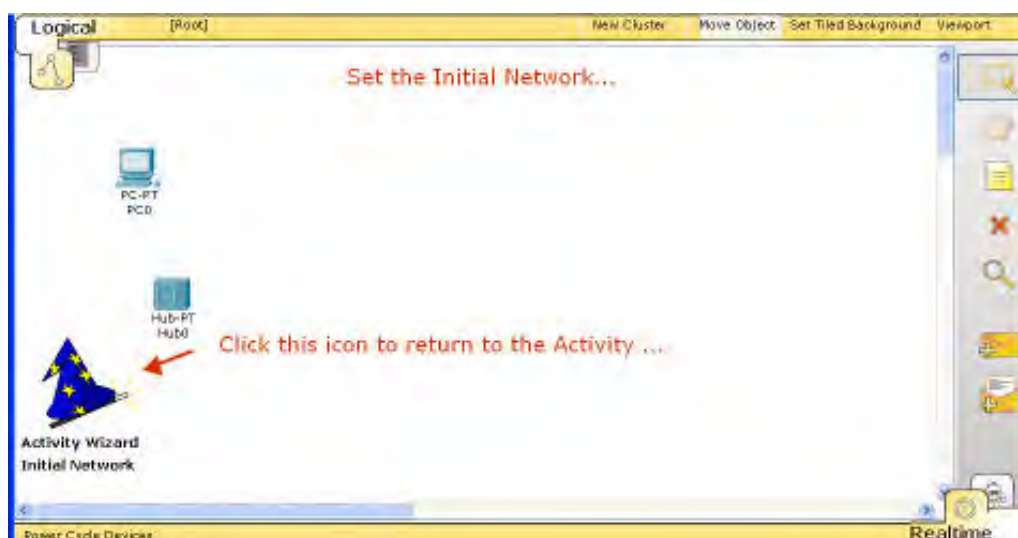
این قسمت به شما امکان تنظیم پیغام های دلخواه را برای فعالیت های کامل شده یا نا تمام فراهم می آورد. پیغام های Completed Feedback زمانی که فعالیت ۱۰۰ درصد کامل شد نمایش داده می شوند. در غیر اینصورت پیغام های Incomplete Feedback نمایش داده خواهد شد. این قسمت از تگ های HTML پشتیبانی نمی کند.



یائل شبکه اولیه (Initial Network)



در این قسمت شما می توانید تعیین کنید که دانشجویان از چه نقطه ای فعالیت خود را آغاز کنند. یک گزینه ساده برای شروع این است که به آسانی شبکه پاسخ را کپی نموده و بخش هایی از آن را ویرایش کنید. این کار با دکمه Show Initial Network انجام می شود. گزینه دیگر وارد کردن فایل با استفاده از Import File to Init Network است. بعد از ایجاد شبکه اولیه می توانید آن را Export کنید.





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

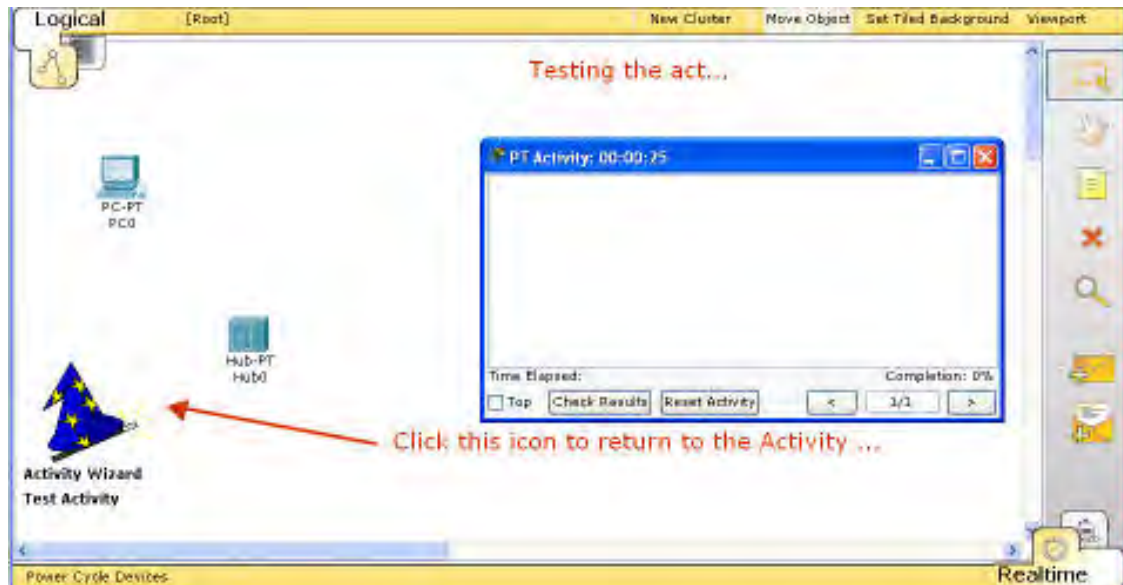
استفاده از Locking Tree

درخت نمایش داده شده در این قسمت برای قفل کردن توابعی است که نمی خواهید دانشجو به آنها دسترسی داشته باشد. برای مثال می توانید از این که دانشجو به فضای کار فیزیکی سوئیچ کند جلوگیری کنید. (در گروه Interface). البته باید مراقب توابعی که قفل می کنید باشید تا مانع از رسیدن به جواب نشوند.

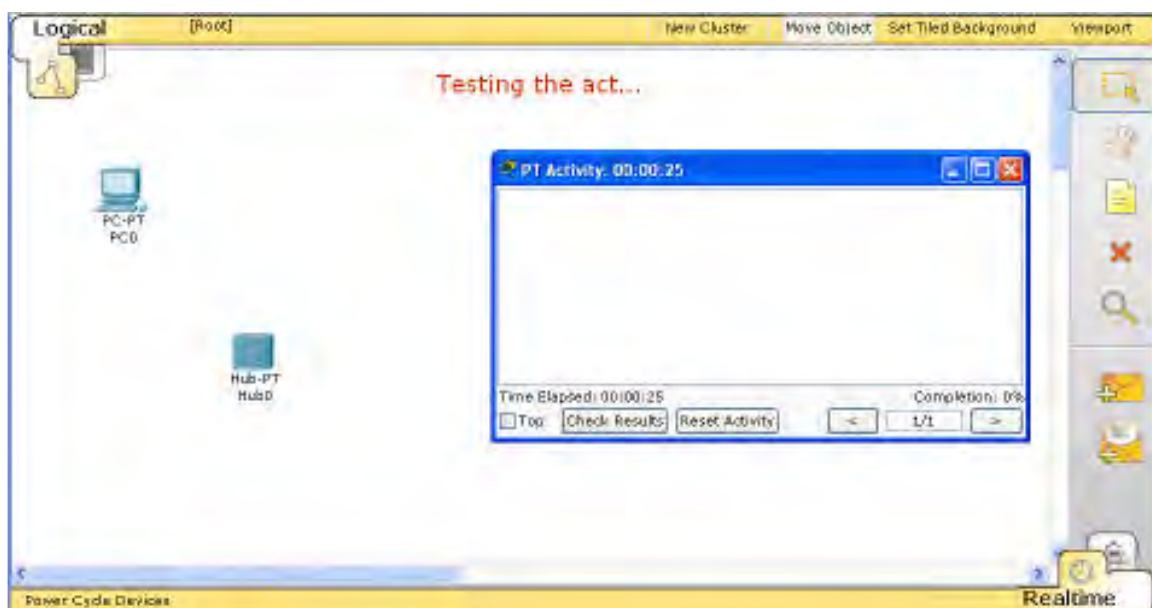
تعیین کلمه عبور



در این پانل شما می توانید برای فایل فعالیت یک کلمه عبور تعیین کنید. در صورت عدم تعیین کلمه عبور، هر کس می تواند این فایل را باز کند و با دسترسی به Activity Wizard پارامترهای آنرا تغییر دهد. این قسمت سبب می شود به طور انحصاری فقط مولف امکان تغییر یک فعالیت را داشته باشد.

آزمایش فعالیت (Test the Activity)

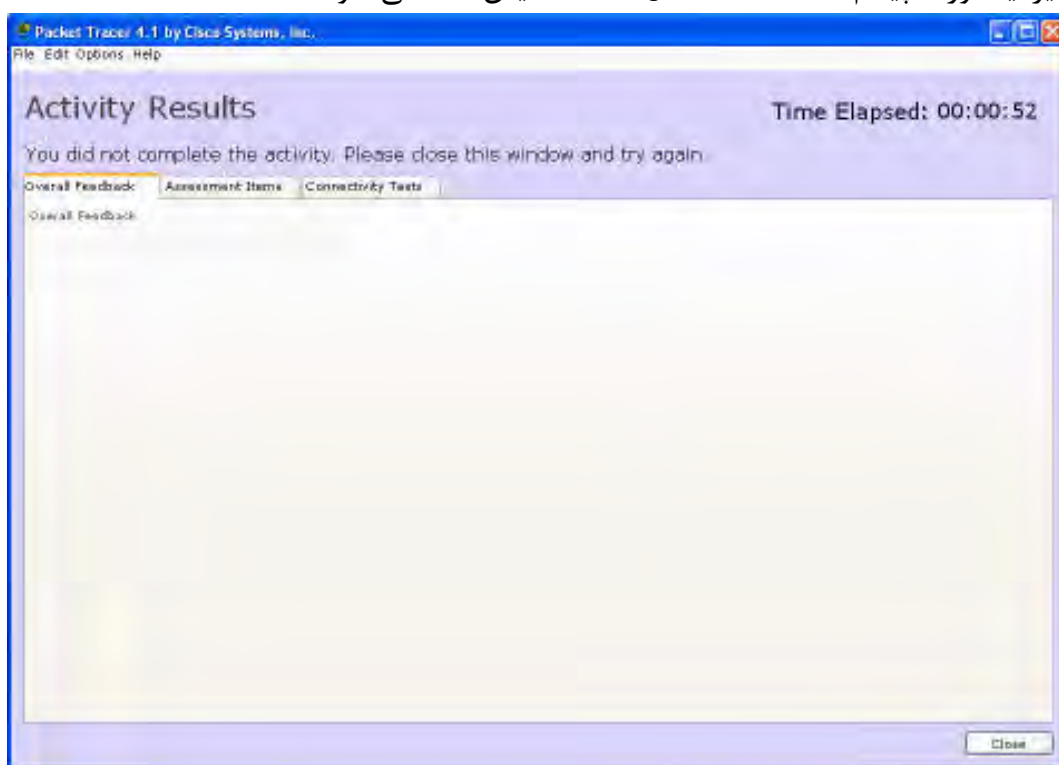
وقتی که شما برگه Test Activity را انتخاب کنید، می توانید به طور آزمایشی فعالیت ایجاد شده را اجرا کنید و آنرا از دیدگاه دانشجو مشاهده کنید. این کار به شما فرصت بررسی نهایی فعالیت را قبل از ذخیره کردن آن می دهد.

اجرای فایل فعالیت

شما می توانید با باز کردن یک فعالیت که قبلا به صورت pka ذخیره کرده اید، فعالیت را آغاز کنید. ابتدا پنجره توضیحات را مشاهده خواهید کرد که به شما نحوه تکمیل فعالیت را شرح می دهد. در این پنجره درصد پیشرفت فعالیت نمایش داده خواهد شد و هر ۳ ثانیه به روز رسانی می شود. با استفاده از دکمه Check Results می توانید پیشرفت فعالیت خود را مشاهده کنید. اگر همه تیک ها سبز باشد، فعالیت کاملا به پایان رسیده است. تیک سفید نشان دهنده ناتمام ماندن است و ضربدر قرمز نشان دهنده اشتباه بود جواب است. با استفاده از Reset Activity می توانید به تنظیمات اولیه برگردید و فعالیت را از ابتدا آغاز کنید.

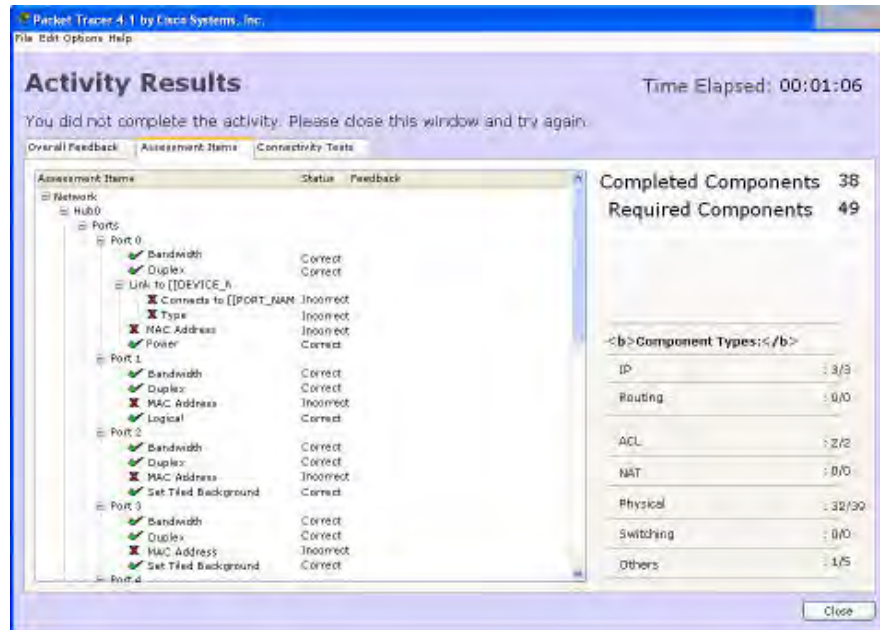
Overall Feedback

اگر فعالیت ۱۰۰ درصد تکمیل شده باشد، پیغام Completed Feedback نمایش داده خواهد شد. در غیر اینصورت پیغام Incomplete Feedback نمایش داده می شود.



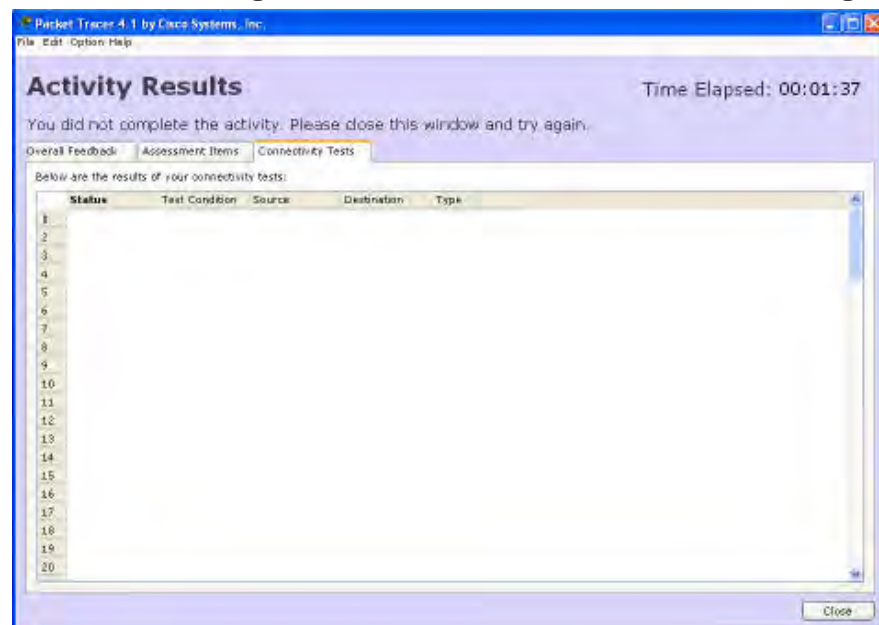
آیتم های ارزیابی

صفحه زیر نتایج آیتمهای ارزیابی را نمایش می دهد. برای هر آیتم یک پیغام نشان می دهد که پاسخ شما صحیح است یا غلط.



بررسی اتصال

صفحه زیر نتایج Connectivity Test است که با شرایط شبکه پاسخ مورد مقایسه قرار میگیرد.



بعنوان یک کاربر عادی می توان از دستور Save برای ذخیره کردن فعالیت جاری استفاده کرد و بعداً آن را تکمیل نمود. در چنین مواقعی بهتر است فایل را با نام جدیدی غیر از فعالیت اصلی ذخیره کنید. البته وقتی فایل را باز کنید خواهید توانست توسط Reset Activity فعالیت را از اول آغاز کنید.



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

مدیریت متغیرها (Variable Manager)



در پانل Variable Manager شما می توانید فعالیت های خود را پویا کنید. اعداد، رشته ها، آدرس های IP می توانند به متغیرها نسبت داده شده و بعداً به صورت تصادفی در هر بار اجرای فعالیت مورد استفاده قرار گیرند. برای فعال کردن Variable Manager گزینه **Show Variable Manager Interface** را فعال کنید.

ایجاد استخر (Pool)

در برگه Pools می توانید تعدادی دسته های عددی، رشته ای و آدرس IP ایجاد کنید. برای نوع عددی می توانید بازه اعداد را مشخص کنید، رشته ها را می توانید توسط ; از هم جدا کنید.

Activity Wizard

Introduction Pools Variables

To Add an Item: Fill in all the fields

Number

Name	Min	Max
1		
2		
3		
4		
5		

Strings

Name	Text
1	
2	
3	
4	
5	

IP Address

Name	Network	Mask	1st IP Addr	Last IP Addr
1				
2				
3				
4				
5				

ایجاد متغیرها

در برگه Variables می توانید متغیرهایی را تعیین کنید که مقدار خود را از دسته های تعریف شده در استخر فوق دریافت می کنند.

Activity Wizard

Introduction Pools Variables

To Add an Item: Fill in all the fields

Variable Name	Pool Name	Value	PoolType
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			
11			
12			
13			
14			
15			
16			
17			
18			
19			
20			
21			
22			



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

اختصاص متغیر ها

وقتی که show Variable Manager Interface فعال باشد، شما می توانید متغیرها را در متن های دستورالعمل، آیتم های ارزیابی و آیتم های اولیه مورد استفاده قرار دهید. در پانل Instruction مکان نما را در جایی که متغیر باید استفاده شود قرار دهید و روی Insert در Variable Manager Interface کلیک کنید. در مورد Assessments Items و Initial Items تنها موارد نشان داده شده با نقطه سبز رنگ می توانند از متغیرها استفاده کنند.

نحوه افزودن متغیرها به آیتم های ارزیابی

بیشتر پیکربندی های شبکه پاسخ آیتم های ارزیابی متناظری دارند. برای ارزیابی هر آیتم دلخواه، آیتم را فعال کنید. رفتار پیشفرض این است که پیکربندی های شبکه کاربر با آنچه در شبکه پاسخ قرار دارد مقایسه می شود. برای فعالیت های پیشرفته تر، آیتمهای ارزیابی می توانند با متغیر جایگزین شوند. در این حالت پیکربندی کاربر با متغیر تعریف شده مقایسه می شود. متغیرهای آنها می توانند با مقادیر پیکربندی شده جایگزین شوند. برای جایگزینی به یکی از دو روش زیر عمل کنید:

- با استفاده از واسط Variable Manager روی ← کلیک کنید.
- روی آیتم ارزیابی یک بار کلیک کنید. یک فیلد متنی ظاهر می شود. متن را با متغیر جایگزین کنید.

انواع آیتم های ارزیابی

آیتم های ارزیابی که می توانند با متغیرها جایگزین شوند انواعی دارند. مقدار متغیر باید متناسب با قوانین زیر تعریف شود:

Boolean: کمتر یا مساوی صفر false و بیشتر یا مساوی یک true است.

Enum: یک عدد مشخص کننده مقدار است (در جداول زیر این اعداد مشخص شده اند)

Number: یک عدد مبنای ۱۰

IP Addresses: باید دارای فرمت مقابل باشند 192.168.1.1

Mac Addresses: باید دارای فرمت ABCD.ABCD.ABCD باشند

Strings: هر رشته دلخواه

Special: رشته های خاصی که باید منطبق با فرمت نمایش داده شده در زیر باشد.



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

<i>Cisco Device</i>			
Name	Variable	Type	Comment
Host Name	y	String	
Startup Config			
Config-Register	y	Number	
Banner MOTD	y	String	
Enable Password	y	String	
Service Password	y	Boolean	
Encryption			
Clock Timezone	y	String	
VTY Lines			
Boot System Files			
<system file>	y	String	
Flash Files			
<flash file names>		String	

<i>Cloud Device</i>			
Name	Variable	Type	Comment
Frame-Relay			
Connections			
<Connection	y	Special	<fromPortName> <sublink> :
Node>			<toPortName> <sublink>
DSL Connections			
<DSL	y	Special	<fromPortName> : <toPortName>
Connections>			
Cable Connections			
<Cable	y	Special	<fromPortName> : <toPortName>
Connections>			

<i>All Devices</i>			
Name	Variable	Type	Comment
Power	y	Boolean	

<i>PC</i>			
Name	Variable	Type	Comment
Default Gateway	y	IP Address	



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

<i>Routers</i>			
Name	Variable	Type	Comment
User Names			
<User Name Password Pair>	y	Special	<username>-<password>

<i>Switches</i>			
Name	Variable	Type	Comment
VLANS		HEAD	
<VlanNumber>		Number	
<VlanName>		String	
VLAN Name			
Default Gateway	y	IP Address	

<i>Terminal Line Devices</i>			
Name	Variable	Type	Comment
Enable Secret	y	String	

Linksys			
Name	Variable	Type	Comment
Internet Connection	y	Enum	Dhcp = 0, 1=PPPoE, 2=Static
Router IP			
Ports			
Internet			
IP Address			
Subnet Mask			
LAN			
IP Address			
Subnet Mask			
Default Gateway	y	IP Address	
DNS Server IP			
Security Mode	y	Enum	0 = None, 1=WEP
Single Port			
Forwarding			
Password	y	String	
Remote	y	Boolean	
Management			



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

<i>Cloud Pots Port</i>			
Name	Variable	Type	Comment
Phone Number		Special	<areacode>-<prefix>-<number>

<i>Cloud Serial Port</i>			
Name	Variable	Type	Comment
Frame Relay			
LMI Type	y	Enum	0 = Ansi, 1= Cisco, 2 = Q933a
Sublinks			
<sublink name>	y	String	

<i>Frame Relay Sub Interface Port</i>			
Name	Variable	Type	Comment
Type (Point-to-Point/ MultiPoint)	y	Enum	0 = Multipoint, PointToPoint = 1

<i>Port</i>			
Name	Variable	Type	Comment
Power	y	Boolean	
Bandwidth	y	Boolean	
Duplex	y	Boolean	
MAC Address	y	Mac Address	
MAC Address	y	Mac Address	
Clock Rate	y	String	
Description	y	String	

<i>Host Port</i>			
Name	Variable	Type	Comment
IP Address	y	IP Address	
Subnet Mask	y	IP Address	



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

Router Port			
Name	Variable	Type	Comment
Access-group In	y		
Access-group Out	y		
CDP Enabled	y	Boolean	
NAT Mode	y	Enum	0 = None, 1 = NatInside, 2 = eNatOutside
Bandwidth Info	y	Number	
Delay	y	Number	
EIGRP Hello Interval			
RIP Split Horizon	y	Boolean	
EIGRP Summary Addresses			
Autonomous System		Number	
OSPF Authentication	y		
OSPF Authentication Key	y	String	
OSPF Cost	y	Number	
OSPF Dead-Interval	y	Number	
OSPF Hello-Interval	y	Number	
OSPF Message Digest Key			
Key ID [[ID]]	y	Number	
OSPF Priority	y	Number	
Keepalive	y	Boolean	
Encapsulation			
Keepalive	y	Boolean	
PPP			
Authentication	y	Enum	0 = No Authentication, 1 =Chap , 2 = Pap, 3 = PapChap, 4 = ChapPap
Frame Relay			
Encapsulation Type	y	Enum	0 = Cisco, 1 = IETF, 2 = Default
LMI Type	y	Enum	0 = Ansi, 1 =Cisco , 2 = Q933a
IP Maps			
802.1Q			
VLAN ID	y	Number	
Native VLAN			



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

<i>Switch Port</i>			
Name	Variable	Type	Comment
Port Mode	y	Boolean	
Access VLAN	y	Number	
Native VLAN	y	Number	
Trunk VLANs			
<name>	y	String	
Voice Vlan	y	Number	
Nonegotiate	y	Boolean	
Dynamic Mode	y	Enum	0 = Dynamic Desirable, 1 = Dynamic Auto, 2 = Operation Trunk, 3 = Operation Access

<i>Terminal Line</i>			
Name	Variable	Type	Comment
RS232			
VTY Line		Number	
Console Line			
Speed	y	Number	
Data Bits	y	Number	
Parity	y	Enum	0 = Even, 1 =Mark , 2 =None , 3 = Odd, 4 =Space
Stop Bits	y	String	
Flow Control	y	Enum	0 = None, 1 = Hardware, 2 =Software
History Size	y	Number	
MOTD Banner	y	Boolean	
Login	y	Enum	0 = No Login, 1 = Login, 3 = Login Local
Password	y	String	
Session Limit	y	Number	
Access Control In	y	String	
Access Control Out	y	String	

<i>Routing</i>			
Name	Variable	Type	Comment
Routes			
Static Routes			



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

<static route>	y	Special	<destinationPrefix>- <destinationPrefixBits>- <forwardRoutersIP>-0
Default Networks <default network>	y	IP Address	

RIP

Name	Variable	Type	Comment
RIP			
Version	y	Number	
Auto Summary	y	Boolean	
Default Information Originate Timers Basic Networks	y	Boolean	
<network address>	y	IP Address	
Passive Interface Default	y	HEAD Boolean	

EIGRP

Name	Variable	Type	Comment
Autonomous System #		Number	
Auto Summary Networks	y	Boolean Head	
<network address String>	y	Special	<networkNumber> <eigrpWildcardBits>
Passive Interface Default Metrics Variance	y	Boolean Number	

OSPF

Name	Variable	Type	Comment
Process ID Area		Number	



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

Authentication			
Area #	y	Number	
Default Information Originate	y	Enum	0 =No Default Info Originate , 1 = Default Info Originate, 2 = Default Info Originate Always
Log Adjacency Changes	y	Enum	0 =No Log Change , 1 = Log Change, 2 = Log Change Detail
Passive Interface Default Networks			
<route String>	y	Special	<networkNumber> <OSPFWildcardMask> <areaIdNumber>

Port Security

Name	Variable	Type	Comment
Static MAC <mac address>	y	Mac Address	
Type	y	Enum	0 = Shutdown, 1 =Protect , 2 =Restrict
Maximum Static MACs	y	Number	

CDP

Name	Variable	Type	Comment
CDP Enabled		Boolean	

ACL

Name	Variable	Type	Comment
<ACL Name>	y	String	

DHCP Pool

Name	Variable	Type	Comment
Pool		String	
DNS server IP	y	IP Address	



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

DHCP Server

Name	Variable	Type	Comment
DHCP Enable	y	Boolean	
Start IP Address	y	IP Address	
Max User	y	IP Address	
Default Gateway	y	IP Address	
DNS Server IP	y	IP Address	
Pools			
Excluded Addresses <addresses>	y	IP Address	

NAT

Name	Variable	Type	Comment
NAT			
Pools			
<pool name>	y	String	
Inside Source List			
<list number>	y	Number	
Inside Source Static			
<static entry>	y	Special	<udp tcp> <insideLocalIP> <portNumber> <InsideGlobalIp> <portNumber>

STP

Name	Variable	Type	Comment
VLANs			
<Vlan Number>	y	Number	
Priority			



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

<i>Wireless</i>			
Name	Variable	Type	Comment
Wireless			
SSID			
Security Mode			
WEP Key			
<i>HTTP Server</i>			
Name	Variable	Type	Comment
HTTP Enable	y	Boolean	
<i>VTP</i>			
Name	Variable	Type	Comment
VTP			
Domain Name	y	String	
VTP Mode	y	Enum	0 =VtpServer , 1 =VtpClient , 2 = VtpTransparent
VTP Password	y	String	
VTP Version	y	Number	
<i>TFTP</i>			
Name	Variable	Type	Comment
TFTP Enable	y	Boolean	
<i>DNS Client</i>			
Name	Variable	Type	Comment
IP Domain-Lookup	y	Boolean	
IP Name Server	y	IP Address	
IP Host			
Host <ipaddress>	y	IP Address	
<i>DNS Server</i>			
Name	Variable	Type	Comment
DNS Enable	y	Boolean	



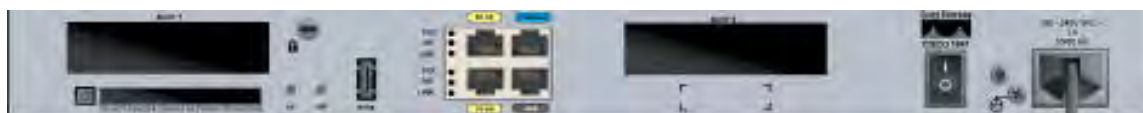
✓ فصل دوم: شبیه سازی شبکه توسط نرم افزار Packet Tracer

Domain Name	
<name>	y String



ضمیمه ۱- مسیریاب و ماژول های مرتبط با آن

مسیریاب 1841



Module Name	Thumbnails	Description
HWIC-4ESW WIC-1AM		The HWIC-4ESW provides 4 switching ports. The WIC-1AM card features dual RJ-11 connectors, which are used for basic telephone service connection. The WIC-1AM uses one port for connection to a standard telephone line, and the other port can be connected to a basic analog telephone for use when the modem is idle.
WIC-1ENET		The WIC-1ENET is a single-port 10 Mbps Ethernet interface card, for use with 10BASE-T Ethernet LANs.
WIC-1T		The WIC-1T provides a single port serial connection to remote sites or legacy serial network devices such as Synchronous Data Link Control (SDLC) concentrators, alarm systems, and packet over SONET (POS) devices.
WIC-2AM		The WIC-2AM card features dual RJ-11 connectors, which are used for basic telephone service connection. The WIC-2AM has two modem ports to allow multiple data communication connections.
WIC-2T		The 2-port asynchronous/synchronous serial network module provides flexible multi-protocol support, with each port individually configurable in synchronous or asynchronous mode, offering mixed-media dial support in a single chassis. Applications for Asynchronous/Synchronous support include: Low speed WAN aggregation (up to 128 Kbps), dial-up modem support, Async or Sync



✓ ضمائم: شبیه سازی شبکه های کامپیوتری

WIC-Cover		connections to management ports of other equipment, and transport of legacy protocols such as Bi-sync and SDLC. The WIC-Cover is a standard WAN Interface Card cover.
------------------	---	--

مسیر یاب 2620XM



<i>Module Name</i>	<i>Thumbnails</i>	<i>Description</i>
NM-1E		The NM-1E features a single Ethernet port that can connect a LAN backbone which can also support either six PRI connections to aggregate ISDN lines, or 24 synchronous/asynchronous ports.
NM-1E2W		The NM-1E2W provides a single Ethernet port with two WIC slots that can support a single Ethernet LAN, together with two serial/ISDN backhaul lines, and still allow multiple serial or ISDN in the same chassis.
NM-1FE-FX		The NM-1FE-FX Module provides 1 Fast-Ethernet interface for use with fiber media. Ideal for a wide range of LAN applications, the Fast Ethernet network modules support many internetworking features and standards. Single port network modules offer autosensing 10/100BaseTX or 100BaseFX Ethernet.
NM-1FE-TX		The NM-1FE-TX Module provides 1 Fast-Ethernet interface for use with copper media. Ideal for a wide range of LAN applications, the Fast Ethernet network modules support many internetworking features and standards. Single port network modules offer autosensing 10/100BaseTX or 100BaseFX Ethernet. The TX (copper) version supports virtual LAN

NM-1FE2W		(VLAN) deployment. The NM-1FE2W Module provides 1 Fast-Ethernet interface for use with copper media, in addition to 2 Wan Interface Card expansion slots. Ideal for a wide range of LAN applications, the Fast Ethernet network modules support many internetworking features and standards. Single port network modules offer autosensing 10/100BaseTX or 100BaseFX Ethernet. The TX (copper) version supports virtual LAN (VLAN) deployment.
NM-2E2W		The NM-2E2W provides two Ethernet ports with two WIC slots that can support two Ethernet LANs, together with two serial/ISDN backhaul lines, and still allow multiple serial or ISDN in the same chassis.
NM-2FE2W		The NM-2FE2W Module provides 2 Fast-Ethernet interface for use with copper media, in addition to 2 Wan Interface Card expansion slots. Ideal for a wide range of LAN applications, the Fast Ethernet network modules support many internetworking features and standards.
NM-2W		The NM-2W Module provides 2 Wan Interface Card expansion slots. It can be used with a broad range of interface cards supporting a diverse array of physical media and network protocols.
NM-4A/S		The 4-port asynchronous/synchronous serial network module provides flexible multi-protocol support, with each port individually configurable in synchronous or asynchronous mode, offering mixed-media dial support in a single chassis. Applications for Asynchronous/Synchronous support include: Low speed WAN aggregation (up to 128 Kbps), dial-up modem support, Async or Sync connections to management ports of other equipment, and transport of legacy protocols such as Bi-sync and SDLC.



NM-4E		The NM-4E features four Ethernet ports for multifunction solutions that require higher-density Ethernet than the mixed-media network modules.
NM-8A/S		The 8-port asynchronous/synchronous serial network module provides flexible multi-protocol support, with each port individually configurable in synchronous or asynchronous mode, offering mixed-media dial support in a single chassis. Applications for Asynchronous/Synchronous support include: Low speed WAN aggregation (up to 128 Kbps), dial-up modem support, Async or Sync connections to management ports of other equipment, and transport of legacy protocols such as Bi-sync and SDLC.
NM-8AM		The NM-8AM Integrated V.92 analog modem network module provides cost-effective analog telephone service connectivity for lower-density remote-access service (RAS), dial-out and fax-out modem access, asynchronous dial-on-demand routing (DDR) plus dial backup, and remote router management. Both the 8-port and 16-port versions use RJ-11 jacks to connect the integrated modems to basic analog telephone lines on the public switched telephone network (PSTN) or private telephony systems.
NM-Cover WIC-1AM		The NM-Cover is a standard network module cover. The WIC-1AM card features dual RJ-11 connectors, which are used for basic telephone service connection. The WIC-1AM uses one port for connection to a standard telephone line, and the other port can be connected to a basic analog telephone for use when the modem is idle.
WIC-1T		The WIC-1T provides a single port serial connection to remote sites or legacy serial network devices such as

WIC-2AM		Synchronous Data Link Control (SDLC) concentrators, alarm systems, and packet over SONET (POS) devices. The WIC-2AM card features dual RJ-11 connectors, which are used for basic telephone service connection. The WIC-2AM has two modem ports to allow multiple data communication connections.
WIC-2T		The 2-port asynchronous/synchronous serial network module provides flexible multi-protocol support, with each port individually configurable in synchronous or asynchronous mode, offering mixed-media dial support in a single chassis. Applications for Asynchronous/Synchronous support include: Low speed WAN aggregation (up to 128 Kbps), dial-up modem support, Async or Sync connections to management ports of other equipment, and transport of legacy protocols such as Bi-sync and SDLC. The WIC-Cover is a standard WAN Interface Card cover.
WIC-Cover		

مسیریاب 2621XM



ماژول های مربوط به این مسیریاب همانند مدل 2620XM می باشد.

مسیریاب 2821

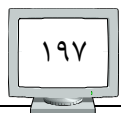




✓ ضمائم: شبیه سازی شبکه های کامپیوتری

<i>Module Name</i>	<i>Thumbnails</i>	<i>Description</i>
NM-1E		The NM-1E features a single Ethernet port that can connect a LAN backbone which can also support either six PRI connections to aggregate ISDN lines, or 24 synchronous/asynchronous ports.
NM-1E2W		The NM-1E2W provides a single Ethernet port with two WIC slots that can support a single Ethernet LAN, together with two serial/ISDN backhaul lines, and still allow multiple serial or ISDN in the same chassis.
NM-1FE-FX		The NM-1FE-FX Module provides 1 Fast-Ethernet interface for use with fiber media. Ideal for a wide range of LAN applications, the Fast Ethernet network modules support many internetworking features and standards. Single port network modules offer autosensing 10/100BaseTX or 100BaseFX Ethernet.
NM-1FE-TX		The NM-1FE-TX Module provides 1 Fast-Ethernet interface for use with copper media. Ideal for a wide range of LAN applications, the Fast Ethernet network modules support many internetworking features and standards. Single port network modules offer autosensing 10/100BaseTX or 100BaseFX Ethernet. The TX (copper) version supports virtual LAN (VLAN) deployment.
NM-1FE2W		The NM-1FE2W Module provides 1 Fast-Ethernet interface for use with copper media, in addition to 2 Wan Interface Card expansion slots. Ideal for a wide range of LAN applications, the Fast Ethernet network modules support many internetworking features and standards. Single port network modules offer autosensing 10/100BaseTX or 100BaseFX Ethernet. The TX (copper) version supports virtual LAN (VLAN) deployment.

NM-2E2W		The NM-2E2W provides two Ethernet ports with two WIC slots that can support two Ethernet LANs, together with two serial/ISDN backhaul lines, and still allow multiple serial or ISDN in the same chassis.
NM-2FE2W		The NM-2FE2W Module provides 2 Fast-Ethernet interface for use with copper media, in addition to 2 Wan Interface Card expansion slots. Ideal for a wide range of LAN applications, the Fast Ethernet network modules support many internetworking features and standards.
NM-2W		The NM-2W Module provides 2 Wan Interface Card expansion slots. It can be used with a broad range of interface cards supporting a diverse array of physical media and network protocols.
NM-4A/S		The 4-port asynchronous/synchronous serial network module provides flexible multi-protocol support, with each port individually configurable in synchronous or asynchronous mode, offering mixed-media dial support in a single chassis. Applications for Asynchronous/Synchronous support include: Low speed WAN aggregation (up to 128 Kbps), dial-up modem support, Async or Sync connections to management ports of other equipment, and transport of legacy protocols such as Bi-sync and SDLC.
NM-4E		The NM-4E features four Ethernet ports for multifunction solutions that require higher-density Ethernet than the mixed-media network modules.
NM-8A/S		The 8-port asynchronous/synchronous serial network module provides flexible multi-protocol support, with each port individually configurable in synchronous or asynchronous mode, offering mixed-media dial support in a single chassis. Applications for Asynchronous/Synchronous support



NM-8AM		include: Low speed WAN aggregation (up to 128 Kbps), dial-up modem support, Async or Sync connections to management ports of other equipment, and transport of legacy protocols such as Bi-sync and SDLC. The NM-8AM Integrated V.92 analog modem network module provides cost-effective analog telephone service connectivity for lower-density remote-access service (RAS), dial-out and fax-out modem access, asynchronous dial-on-demand routing (DDR) plus dial backup, and remote router management. Both the 8-port and 16-port versions use RJ-11 jacks to connect the integrated modems to basic analog telephone lines on the public switched telephone network (PSTN) or private telephony systems.
NM-Cover		The NM-Cover is a standard network module cover.
NM-ESW-161		The NM-ESW-161 provides 16 switching ports.
HWIC-4ESW WIC-1AM		The HWIC-4ESW provides 4 switching ports. The WIC-1AM card features dual RJ-11 connectors, which are used for basic telephone service connection. The WIC-1AM uses one port for connection to a standard telephone line, and the other port can be connected to a basic analog telephone for use when the modem is idle.
WIC-1ENET		The WIC-1ENET is a single-port 10 Mbps Ethernet interface card, for use with 10BASE-T Ethernet LANs.
WIC-1T		The WIC-1T provides a single port serial connection to remote sites or legacy serial network devices such as Synchronous Data Link Control (SDLC) concentrators, alarm systems, and packet over SONET (POS) devices.



✓ ضمايم: شبیه سازی شبکه های کامپیوتری

WIC-2AM		The WIC-2AM card features dual RJ-11 connectors, which are used for basic telephone service connection. The WIC-2AM has two modem ports to allow multiple data communication connections.
WIC-2T		The 2-port asynchronous/synchronous serial network module provides flexible multi-protocol support, with each port individually configurable in synchronous or asynchronous mode, offering mixed-media dial support in a single chassis. Applications for Asynchronous/Synchronous support include: Low speed WAN aggregation (up to 128 Kbps), dial-up modem support, Async or Sync connections to management ports of other equipment, and transport of legacy protocols such as Bi-sync and SDLC.
WIC-Cover		The WIC-Cover is a standard WAN Interface Card cover.

مسیر یاب Router-PT



<i>Module Name</i>	<i>Thumbnail</i>	<i>Description</i>
PT-ROUTER-NM-1AM		The PT-ROUTER-NM-1AM card features dual RJ-11 connectors, which are used for basic telephone service connection. The WIC-1AM uses one port for connection to a standard telephone line, and the other port can be connected to a basic analog telephone for use when the modem is idle.
PT-ROUTER-NM-1CE		The PT-ROUTER-NM-1CE features a single Ethernet port that can connect a LAN backbone which can also support either six PRI connections to aggregate ISDN lines, or 24 synchronous/asynchronous ports.



PT-ROUTER-NM-1CFE		The PT-ROUTER-NM-1CFE Module provides 1 Fast-Ethernet interface for use with copper media. Ideal for a wide range of LAN applications, the Fast Ethernet network modules support many internetworking features and standards. Single port network modules offer autosensing 10/100BaseTX or 100BaseFX Ethernet. The TX (copper) version supports virtual LAN (VLAN) deployment.
PT-ROUTER-NM-1CGE		The single-port Cisco Gigabit Ethernet Network Module (part number PT-ROUTER-NM-1CGE) provides Gigabit Ethernet copper connectivity for access routers. The module is supported by the Cisco 2691, Cisco 3660, Cisco 3725, and Cisco 3745 series routers. This network module has one gigabit interface converter (GBIC) slot to carry any standard copper or optical Cisco GBIC.
PT-ROUTER-NM-1FFE		The PT-ROUTER-NM-1FFE Module provides 1 Fast-Ethernet interface for use with fiber media. Ideal for a wide range of LAN applications, the Fast Ethernet network modules support many internetworking features and standards. Single port network modules offer autosensing 10/100BaseTX or 100BaseFX Ethernet.
PT-ROUTER-NM-1FGE		The single-port Cisco Gigabit Ethernet Network Module (part number PT-ROUTER-NM-1FGE) provides Gigabit Ethernet copper connectivity for access routers. The module is supported by the Cisco 2691, Cisco 3660, Cisco 3725, and Cisco 3745 series routers. This network module has one gigabit interface converter (GBIC) slot to carry any standard copper or optical Cisco GBIC.
PT-ROUTER-NM-1S		The PT-ROUTER-NM-1S provides a single port serial connection to remote sites or legacy serial network devices such as Synchronous Data Link Control (SDLC) concentrators, alarm systems, and packet over SONET (POS) devices.
PT-ROUTER-NM-1SS		The 2-port asynchronous/synchronous serial network module provides flexible multi-protocol support, with each port individually configurable in synchronous or asynchronous mode, offering mixed-media dial support in a single chassis. Applications for Asynchronous/Synchronous support include: Low speed WAN aggregation (up to 128 Kbps), dial-up modem support, Async or

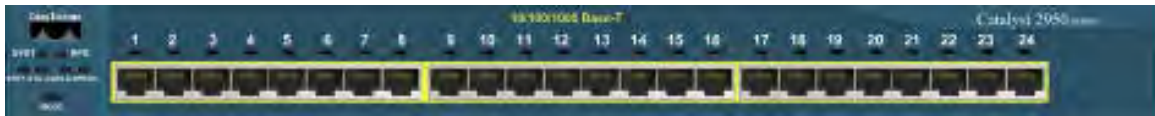


✓ ضمايم: شبیه سازی شبکه های کامپیوتری

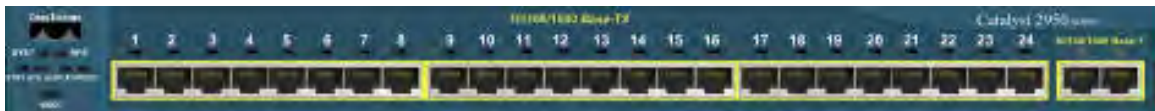
	Sync connections to management ports of other equipment, and transport of legacy protocols such as Bi-sync and SDLC.
--	--

سوئیچ ها و ماژول های مرتبط با آن

سوئیچ 2950-24



سوئیچ 2950T-24



سوئیچ 2960-24TT



سوئیچ Switch-PT



PT-SWITCH-NM-1CE



The PT-SWITCH-NM-1CE features a single Ethernet port that can connect a LAN backbone which can also support either six PRI connections to aggregate ISDN lines, or 24 synchronous/asynchronous ports.

PT-SWITCH-NM-1CFE



The PT-SWITCH-NM-1CFE Module provides 1 Fast-Ethernet interface for use with copper media. Ideal for a wide range of LAN applications, the Fast Ethernet network modules support many internetworking features and standards. Single port network modules offer autosensing 10/100BaseTX or 100BaseFX Ethernet. The TX (copper) version supports virtual LAN (VLAN) deployment.

PT-SWITCH-NM-1CGE



The single-port Cisco Gigabit Ethernet Network Module (part number PT-SWITCH-NM-1CGE) provides

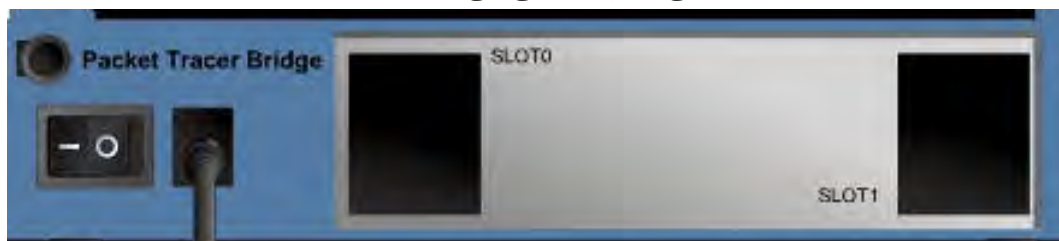


✓ ضمائم: شبیه سازی شبکه های کامپیوتری

PT-SWITCH-NM-1FFE	 Gigabit Ethernet copper connectivity for access routers. The module is supported by the Cisco 2691, Cisco 3660, Cisco 3725, and Cisco 3745 series routers. This network module has one gigabit interface converter (GBIC) slot to carry any standard copper or optical Cisco GBIC.
PT-SWITCH-NM-1FGE	 The PT-SWITCH-NM-1FFE Module provides 1 Fast-Ethernet interface for use with fiber media. Ideal for a wide range of LAN applications, the Fast Ethernet network modules support many internetworking features and standards. Single port network modules offer autosensing 10/100BaseTX or 100BaseFX Ethernet. The single-port Cisco Gigabit Ethernet Network Module (part number PT-SWITCH-NM-1FGE) provides Gigabit Ethernet optical connectivity for access routers. The module is supported by the Cisco 2691, Cisco 3660, Cisco 3725, and Cisco 3745 series routers. This network module has one gigabit interface converter (GBIC) slot to carry any standard copper or optical Cisco GBIC.

پل Bridge-PT

پل شامل ۲ اسلات است و ماژول هایی که پشتیبانی می کند همانند Switch-PT است.





✓ ضمائم: شبیه سازی شبکه های کامپیوتری

دستگاههای نهایی (End Devices) و ماژول های مرتبط با آنها

PC-PT

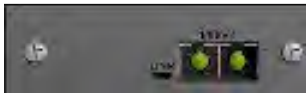
شامل پورت کنسول و یک اسلات است.



<i>Module Name</i>	<i>Thumbnail</i>	<i>Description</i>
Linksys-WMP300N		The wireless interface module provides one 2.4GHz wireless interface suitable for connection to 802.11b networks. The module operates at 11 Megabits/second and supports protocols that use Ethernet for LAN access.
PC-HOST-NM-1AM		The PT-HOST-NM-1AM card features dual RJ-11 connectors, which are used for basic telephone service connection. The WIC-1AM uses one port for connection to a standard telephone line, and the other port can be connected to a basic analog telephone for use when the modem is idle.



✓ ضمائم: شبیه سازی شبکه های کامپیوتری

PC-HOST-NM-1CE		The PT-HOST-NM-1CE features a single Ethernet port that can connect a LAN backbone which can also support either six PRI connections to aggregate ISDN lines, or 24 synchronous/asynchronous ports.
PC-HOST-NM-1CFE		The PT-HOST-NM-1CFE Module provides 1 Fast-Ethernet interface for use with copper media. Ideal for a wide range of LAN applications, the Fast Ethernet network modules support many internetworking features and standards. Single port network modules offer autosensing 10/100BaseTX or 100BaseFX Ethernet. The TX (copper) version supports virtual LAN (VLAN) deployment.
PC-HOST-NM-1CGE		The single-port Cisco Gigabit Ethernet Network Module (part number PT-HOST-NM-1CGE) provides Gigabit Ethernet copper connectivity for access routers. The module is supported by the Cisco 2691, Cisco 3660, Cisco 3725, and Cisco 3745 series routers. This network module has one gigabit interface converter (GBIC) slot to carry any standard copper or optical Cisco GBIC.
PC-HOST-NM-1FFE		The PT-HOST-NM-1FFE Module provides 1 Fast-Ethernet interface for use with fiber media. Ideal for a wide range of LAN applications, the Fast Ethernet network modules support many internetworking features and standards. Single port network modules offer autosensing 10/100BaseTX or 100BaseFX Ethernet.
PC-HOST-NM-1FGE		The single-port Cisco Gigabit Ethernet Network Module (part number PT-HOST-NM-1FGE) provides Gigabit Ethernet optical connectivity for access routers. The module is supported by the Cisco 2691, Cisco 3660, Cisco 3725, and Cisco 3745 series routers. This network module has one gigabit interface converter (GBIC) slot to carry any standard copper or optical



✓ ضمائم: شبیه سازی شبکه های کامپیوتری

PC-HOST-NM-1W	 Cisco GBIC. The wireless interface module provides one 2.4GHz wireless interface suitable for connection to 802.11b networks. The module operates at 11 Megabits/second and supports protocols that use Ethernet for LAN access.
----------------------	---

Server-PT

سرور شامل یک اسلات است و بجز ماژول PC-HOST-NM-1AM از بقیه ماژول های PC-PT پشتیبانی می کند.

Printer-PT

شامل یک اسلات است و بجز PC-HOST-NM-1AM از سایر ماژول های PC-PT پشتیبانی می کند.

IPPhone-Pt

این دستگاه شامل هیچ اسلاتی نیست.





✓ ضمائم: شبیه سازی شبکه های کامپیوتری

سایر دستگاه ها و ماژول های مرتبط با آنها

Hub-PT



Module Name	Thumbnail	Description
PT-REPEATER-NM-1CE		The PT-REPEATER-NM-1CE features a single Ethernet port that can connect a LAN backbone which can also support either six PRI connections to aggregate ISDN lines, or 24 synchronous/asynchronous ports.
PT-REPEATER-NM-1CFE		The PT-REPEATER-NM-1CFE Module provides 1 Fast-Ethernet interface for use with copper media. Ideal for a wide range of LAN applications, the Fast Ethernet network modules support many internetworking features and standards. Single port network modules offer autosensing 10/100BaseTX or 100BaseFX Ethernet. The TX (copper) version supports virtual LAN (VLAN) deployment.
PT-REPEATER-NM-1CGE		The single-port Cisco Gigabit Ethernet Network Module (part number PT-REPEATER-NM-1CGE) provides Gigabit Ethernet copper connectivity for access routers. The module is supported by the Cisco 2691, Cisco 3660, Cisco 3725, and Cisco 3745 series routers. This network module has one gigabit interface converter (GBIC) slot to carry any standard copper or optical Cisco GBIC.
PT-REPEATER-NM-1FFE		The PT-REPEATER-NM-1FFE Module provides 1 Fast-Ethernet interface for use with fiber media. Ideal for a wide range of LAN

PT-REPEATER-NM-1FGE



applications, the Fast Ethernet network modules support many internetworking features and standards. Single port network modules offer autosensing 10/100BaseTX or 100BaseFX Ethernet.

The single-port Cisco Gigabit Ethernet Network Module (part number PT-REPEATER-NM-1FGE) provides Gigabit Ethernet optical connectivity for access routers. The module is supported by the Cisco 2691, Cisco 3660, Cisco 3725, and Cisco 3745 series routers. This network module has one gigabit interface converter (GBIC) slot to carry any standard copper or optical Cisco GBIC.

Repeater-PT



شامل دو اسلات است و ماژولهایی که پشتیبانی می کند مانند Hub-PT است.

AccessPoint-PT

شامل یک آنتن است و یک اسلات دارد و ماژولهایی که پشتیبانی می کند مانند Hub-PT است.



LinkSysWRT300N

یک مسیریاب بیسیم است که شامل یک آنتن، ۴ پورت ثابت اترنت و ۱ پورت ثابت اینترنت است و ماژولی را پشتیبانی نمی کند.



Cloud

اگرچه ابر یک دستگاه نیست، اما در این نرم افزار به صورت یک دستگاه نمایش داده شده است.



Device Name	Thumbnail	Description
PT-CLOUD-NM-1AM		The PT-CLOUD-NM-1AM card features dual RJ-11 connectors, which are used for basic telephone service connection. The WIC-1AM uses one port for connection to a standard telephone line, and the other port can be connected to a basic analog telephone for use when the modem is idle.
PT-CLOUD-NM-1CE		The PT-CLOUD-NM-1CE features a single Ethernet port that can connect a LAN backbone which can also support either six PRI connections to aggregate ISDN lines, or 24 synchronous/asynchronous ports.
PT-CLOUD-NM-1CX		The PT-CLOUD-NM-1CX card features a single coaxial connector, which are used for cable modem service connection.

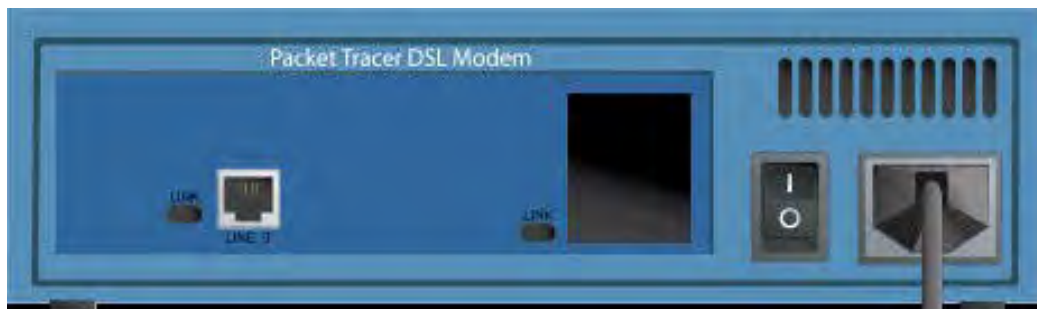


✓ ضمائم: شبیه سازی شبکه های کامپیوتری

PT-CLOUD-NM-1S		The PT-CLOUD-NM-1S provides a single port serial connection to remote sites or legacy serial network devices such as Synchronous Data Link Control (SDLC) concentrators, alarm systems, and packet over SONET (POS) devices.
-----------------------	---	--

DSL-Modem-PT

این مودم از یک اسلات پشتیبانی می کند.



<i>Device Name</i>	<i>Thumbnail</i>	<i>Description</i>
PT-MODEM-NM-1CE		The PT-MODEM-NM-1CE features a single Ethernet port that can connect a LAN backbone which can also support either six PRI connections to aggregate ISDN lines, or 24 synchronous/asynchronous ports.
PT-MODEM-NM-1CFE		The PT-MODEM-NM-1CFE Module provides 1 Fast-Ethernet interface for use with copper media. Ideal for a wide range of LAN applications, the Fast Ethernet network modules support many internetworking features and standards. Single port network modules offer autosensing 10/100BaseTX or 100BaseFX Ethernet. The TX (copper) version supports virtual LAN (VLAN) deployment.
PT-MODEM-NM-1CGE		The single-port Cisco Gigabit Ethernet Network Module (part number PT-MODEM-NM-1CGE) provides Gigabit Ethernet copper connectivity for access routers. The module is supported by the Cisco 2691, Cisco 3660, Cisco 3725, and Cisco 3745 series routers. This network module has one gigabit interface converter (GBIC) slot to carry any standard copper or optical Cisco GBIC.



✓ ضمائم: شبیه سازی شبکه های کامپیوتری

Cable-Modem-PT

یک اسلات دارد و ماژولهایی مشابه DSL-PT را پشتیبانی می کند.





ضمیمه ۲ - کلیدهای میانبر

عمل	میانبر
رفتن به فضای کار منطقی	Shift + L
رفتن به فضای کار فیزیکی	Shift + P
سوئیچ به حالت Realtime	Shift + R
سوئیچ به حالت شبیه سازی	Shift + S
شروع یک شبکه جدید	Ctrl + N
باز کردن یک شبکه	Ctrl + O
ذخیره کردن شبکه جاری	Ctrl + S
ذخیره کردن شبکه جاری با یک نام جدید	Ctrl + Shift + S
چاپ شبکه	Ctrl + P
اجرای Activity Wizard	Ctrl + W
خروج از برنامه	Alt + F4
کپی آیتم های مورد نظر	Ctrl + C
الصاق آیتم های کپی شده	Ctrl + V
برگرداندن عمل قبلی	Ctrl + Z
بزرگ کردن فضای کار	Ctrl + I
بزرگنمایی پیش فرض	Ctrl + T
کوچک کردن فضای کار	Ctrl + U
باز کردن پالت ترسیم	Ctrl + D
مشاهده علاقه مندی ها	Ctrl + R
نمایش روتر ها	Alt + R



✓ ضمائم: شبیه سازی شبکه های کامپیوتری

Alt + S	نمایش سوئیچ ها
Alt + U	نمایش هاب ها
Alt + W	نمایش دستگاه های بی سیم
Alt + C	نمایش اتصالات
Alt + D	مشاهده رایانه/سرور/چاپگر
Alt + A	مشاهده ابر/مودم
Alt + T	مشاهده دستگاه های سفارشی
Alt + i (i is the number other than 0)	افزودن i امین دستگاه در فضای کار
Esc	انتخاب ابزار Select
M	انتخاب ابزار جابجایی
N	انتخاب ابزار Place Note
Del	حذف اشیاء
I	انتخاب ابزار Inspection
P	انتخاب ابزار Simple PDU
C	انتخاب ابزار Complex PDU
C	انصراف در کادر ها
N	انتخاب No در کادرها
Y	انتخاب Yes در کادرها



ضمیمه ۳ - ثابت های زمانی

RIP default update	30 sec
RIP default timeout	3 min
RIP default flush timeout	4 min
RIP default hold-down	3 min
MAC table entry timeout	5 min
ARP request timer	2 sec
ARP table entry timeout	4 hrs
CDP update timer	1 min
CDP neighbor hold-down timer	3 min
DHCP client timeout	5 sec
CSMA/CD waiting time to resend	random
LMI timeout	15 sec
LMI signaling	5 sec
Inverse ARP	30 sec
HDLC keepalive	5 sec
HDLC timeout	15 sec
NAT entries timeout	Depends on the encapsulation protocol
NAT entry encapsulated in a UDP	5 min
NAT entry encapsulated in a TCP	24 hrs
NAT entry encapsulated in a IC	1 min



✓ ضمائم: شبیه سازی شبکه های کامپیوتری

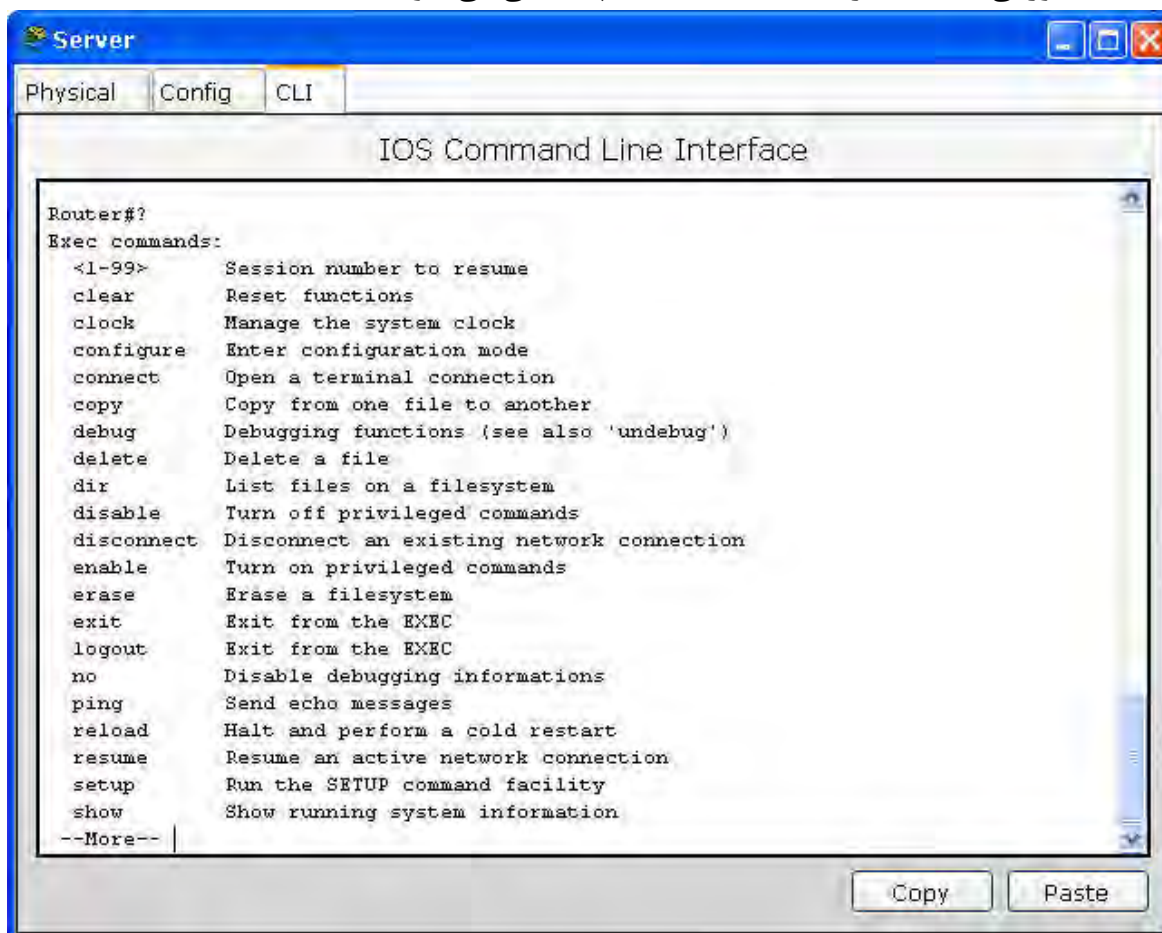
CHAP timeout	5 sec
CHAP re-authenticate timeout	10 sec
DIALING no answer timeout	5 sec
DIALING no dial tone timeout	2 sec
PPP keepalive interval	5 sec
Timeout	15 sec
EIGRP Hello time interval period	5 sec
EIGRP Hold time interval period	15 sec
ICMP	1 ms
STP Max Age	20 sec
STP Hello	2 sec
STP Forward Delay	15 sec
STP Topolgy Change Notify Timer	2 sec
STP Topolgy Change Timer	35 sec
OSPF SPF Hold Time	10 sec
OSPF LS Refresh Time	30 min
OSPF SPF Delay Timer	5 sec
OSPF LSA Retransmission Time	5 sec
OSPF minimum LSA Arrival Time	1 sec
OSPF Delayed Acknowledgment Timer	2.5 sec
OSPF Dead Interval	40 sec
OSPF Hello	10 sec
OSPF Wait Interval	40 sec
TCP Connection Timeout	60 sec
TCP Retransmission Timeout	0.1 sec



TCP Inactivity Timeout	5 min
TCP Close Timeout	10 sec
DNS Request Timeout	3 sec
DHCP Timeout	5 sec
DHCP Discovery Timeout	55 sec
DTP Hello	30 sec
DTP Timeout	5 min
Password Timeout	30 sec

ضمیمه ۴ - دستورات IOS مسیریاب

روی برگه CLI در پنجره تنظیمات مسیریاب کلیک کنید تا به واسط خط فرمان دستورات IOS وارد شوید. در خط فرمان می توانید از دکمه های Copy و Paste استفاده کنید. این بخش شامل لیست دستوراتی است که در Packet Tracer 4.1 پشتیبانی می شود.



User Mode

- **<1-99>**
- **connect**
- **disconnect**
- **enable**
- **exit**
- **logout**
- **ping WORD**
- **resume [<1-16> | WORD]**
- **show**



- cdp
 - entry
 - * [protocol | version]
 - WORD [protocol | version]
 - interface
 - Ethernet <0-9>/<0-24>[.][<0-4294967295>]
 - FastEthernet <0-9>/<0-24>[.][<0-4294967295>]
 - GigabitEthernet <0-9>/<0-24>[.][<0-4294967295>]
 - Serial <0-9>/<0-24>
 - neighbors [detail]
- clock
- controllers
 - Ethernet <0-9>/<0-24>
 - FastEthernet <0-9>/<0-24>
 - GigabitEthernet <0-9>/<0-24>
 - Serial <0-9>/<0-24>
- flash:
- frame-relay
 - lmi
 - map
 - pvc
 - <16-1022>
 - interface Serial <0-9>/<0-24> [<16-1022>]
- history
- hosts
- interfaces
 - Ethernet <0-9>/<0-24>[.][<0-4294967295>] [switchPort]
 - FastEthernet <0-9>/<0-24>[.][<0-4294967295>] [switchPort]
 - GigabitEthernet <0-9>/<0-24>[.][<0-4294967295>] [switchPort]
 - Loopback <0-2147483647>
 - Serial <0-9>/<0-24>
 - Vlan <1-1005>
 - switchport
 - trunk
- ip
 - dhcp binding
 - eigrp
 - interfaces [<1-65535>]
 - neighbors [<1-65535>]
 - topology [<1-65535>] [A.B.C.D A.B.C.D]
 - all-links



```

    traffic [ <1-65535> ]
  interface
    Ethernet <0-9>/<0-24>[ . ][ <0-4294967295> ]
    FastEthernet <0-9>/<0-24>[ . ][ <0-4294967295> ]
    GigabitEthernet <0-9>/<0-24>[ . ][ <0-4294967295> ]
    Loopback <0-2147483647>
    Serial <0-9>/<0-24>
    Vlan <1-1005>
    brief
  nat translations
  ospf
    <1-65535>
    <0-4294967295>
    database
    interface
      Ethernet <0-9>/<0-24>[ . ][ <0-4294967295> ]
      FastEthernet <0-9>/<0-24>[ . ][ <0-4294967295> ]
      GigabitEthernet <0-9>/<0-24>[ . ][ <0-4294967295> ]
      Loopback <0-2147483647>
      Serial <0-9>/<0-24>
      neighbor [ detail ]
      Ethernet <0-9>/<0-24>[ . ][ <0-4294967295> ]
      FastEthernet <0-9>/<0-24>[ . ][ <0-4294967295> ]
      GigabitEthernet <0-9>/<0-24>[ . ][ <0-4294967295> ]
      Loopback <0-2147483647>
      Serial <0-9>/<0-24>
    A.B.C.D
    database
    interface
      Ethernet <0-9>/<0-24>[ . ][ <0-4294967295> ]
      FastEthernet <0-9>/<0-24>[ . ][ <0-4294967295> ]
      GigabitEthernet <0-9>/<0-24>[ . ][ <0-4294967295> ]
```



▪	Loopback <0-2147483647>
▪	Serial <0-9>/<0-24>
▪	neighbor [detail]
▪	Ethernet <0-9>/<0-24>[.]
▪	[<0-4294967295>]
▪	FastEthernet <0-9>/<0-24>[.]
▪	[<0-4294967295>]
▪	GigabitEthernet <0-9>/<0-24>[.]
▪	[<0-4294967295>]
▪	Loopback <0-2147483647>
▪	Serial <0-9>/<0-24>
▪	database
▪	interface
▪	Ethernet <0-9>/<0-24>[.]
▪	[<0-4294967295>]
▪	FastEthernet <0-9>/<0-24>[.]
▪	[<0-4294967295>]
▪	GigabitEthernet <0-9>/<0-24>[.]
▪	[<0-4294967295>]
▪	Loopback <0-2147483647>
▪	Serial <0-9>/<0-24>
▪	neighbor [detail]
▪	Ethernet <0-9>/<0-24>[.]
▪	[<0-4294967295>]
▪	FastEthernet <0-9>/<0-24>[.]
▪	[<0-4294967295>]
▪	GigabitEthernet <0-9>/<0-24>[.]
▪	[<0-4294967295>]
▪	Loopback <0-2147483647>
▪	Serial <0-9>/<0-24>
▪	database
▪	interface
▪	Ethernet <0-9>/<0-24>[.]
▪	[<0-4294967295>]
▪	FastEthernet <0-9>/<0-24>[.]
▪	[<0-4294967295>]
▪	GigabitEthernet <0-9>/<0-24>[.]
▪	[<0-4294967295>]
▪	Loopback <0-2147483647>
▪	Serial <0-9>/<0-24>
▪	neighbor [detail]
▪	Ethernet <0-9>/<0-24>[.]



- 4294967295>]
 - FastEthernet <0-9>/<0-24>[.][<0-4294967295>]
 - GigabitEthernet <0-9>/<0-24>[.][<0-4294967295>]
 - Loopback <0-2147483647>
 - Serial <0-9>/<0-24>
- protocols
- rip database
- route [WORD | connected | eigrp | ospf <1-65535> | rip | static]
- protocols
- sessions
- users
- version
- vlan-switch [brief | id <1-1005> | name WORD]
- vtp
 - counters
 - status
- telnet [WORD]
- traceroute WORD

Enable Mode

- <1-99>
- clear
 - access-list counters [<1-199> | <1300-2699> | WORD]
 - arp-cache
 - cdp table
 - frame-relay inarp
 - ip
 - nat translation *
 - route [* | A.B.C.D | A.B.C.D A.B.C.D]
 - mac-address-table dynamic
 - vtp counters
- clock set hh:mm:ss [<1-31> MONTH <1993-2035> | MONTH <1-31> <1993-2035>]
- configure [terminal]
- connect [WORD]
- copy
 - running-config
 - startup-config
 - tftp:



- startup-config
 - running-config
 - tftp:
- tftp:
 - flash:
 - running-config
 - startup-config
- **debug**
 - eigrp
 - fsm
 - packets
 - ip
 - ospf
 - adj
 - events
 - packet
 - rip [events]
 - routing
- **delete**
 - WORD
 - flash:
- **dir [flash:]**
- **disable**
- **disconnect <1-16>**
- **enable**
- **erase startup-config**
- **exit**
- **logout**
- **no**
 - debug
 - all
 - eigrp
 - fsm
 - packets
 - ip
 - ospf
 - adj
 - events
 - packet
 - rip [events]
 - routing
- **ping [WORD]**
 - [Protocol] [Target IP address] [Repeat count] [Datagram size] [



- Timeout in seconds] [Extended commands] [Sweep range of sizes]
- **reload**
- **resume** [<1-16> | WORD]
- **setup**
- **show**
 - access-lists [<1-999> | WORD]
 - arp
 - cdp
 - entry
 - * [protocol | version]
 - WORD [protocol | version]
 - interfaces
 - Ethernet <0-9>/<0-24>[.][<0-4294967295>]
 - FastEthernet <0-9>/<0-24>[.][<0-4294967295>]
 - GigabitEthernet <0-9>/<0-24>[.][<0-4294967295>]
 - Serial <0-9>/<0-24>
 - neighbors [detail]
 - clock
 - controllers
 - Ethernet <0-9>/<0-24>
 - FastEthernet <0-9>/<0-24>
 - GigabitEthernet <0-9>/<0-24>
 - Serial <0-9>/<0-24>
 - debugging
 - flash:
 - frame-relay
 - lmi
 - map
 - pvc
 - <16-1022>
 - interface Serial <0-9>/<0-24> [<16-1022>]
 - history
 - hosts
 - interfaces
 - Ethernet <0-9>/<0-24>[.][<0-4294967295>] [switchPort]
 - FastEthernet <0-9>/<0-24>[.][<0-4294967295>] [switchPort]
 - GigabitEthernet <0-9>/<0-24>[.][<0-4294967295>] [switchPort]
 - Loopback <0-2147483647>
 - Serial <0-9>/<0-24>
 - Vlan <1-1005>
 - switchport



- trunk
- ip
 - access-lists [<1-199> | WORD]
 - dhcp binding
 - eigrp
 - interfaces [<1-65535>]
 - neighbors [<1-65535>]
 - topology [<1-65535>] [A.B.C.D A.B.C.D]
 - all-links
 - traffic [<1-65535>]
 - interface
 - Ethernet <0-9>/<0-24>[.][<0-4294967295>]
 - FastEthernet <0-9>/<0-24>[.][<0-4294967295>]
 - GigabitEthernet <0-9>/<0-24>[.][<0-4294967295>]
 - Loopback <0-2147483647>
 - Serial <0-9>/<0-24>
 - Vlan <1-1005>
 - brief
 - nat translations
 - ospf
 - <1-65535>
 - <0-4294967295>
 - database
 - interface
 - Ethernet <0-9>/<0-24>[.][<0-4294967295>]
 - FastEthernet <0-9>/<0-24>[.][<0-4294967295>]
 - GigabitEthernet <0-9>/<0-24>[.][<0-4294967295>]
 - Loopback <0-2147483647>
 - Serial <0-9>/<0-24>
 - neighbor [detail]
 - Ethernet <0-9>/<0-24>[.][<0-4294967295>]
 - FastEthernet <0-9>/<0-24>[.][<0-4294967295>]
 - GigabitEthernet <0-9>/<0-24>[.][<0-4294967295>]
 - Loopback <0-2147483647>
 - Serial <0-9>/<0-24>



```

    A.B.C.D
    database
    interface
        Ethernet <0-9>/<0-24>[ . ][ <0-4294967295> ]
        FastEthernet <0-9>/<0-24>[ . ][ <0-4294967295> ]
        GigabitEthernet <0-9>/<0-24>[ . ][ <0-4294967295> ]
        Loopback <0-2147483647>
        Serial <0-9>/<0-24>
    neighbor [ detail ]
        Ethernet <0-9>/<0-24>[ . ][ <0-4294967295> ]
        FastEthernet <0-9>/<0-24>[ . ][ <0-4294967295> ]
        GigabitEthernet <0-9>/<0-24>[ . ][ <0-4294967295> ]
        Loopback <0-2147483647>
        Serial <0-9>/<0-24>
    database
    interface
        Ethernet <0-9>/<0-24>[ . ][ <0-4294967295> ]
        FastEthernet <0-9>/<0-24>[ . ][ <0-4294967295> ]
        GigabitEthernet <0-9>/<0-24>[ . ][ <0-4294967295> ]
        Loopback <0-2147483647>
        Serial <0-9>/<0-24>
    neighbor [ detail ]
        Ethernet <0-9>/<0-24>[ . ][ <0-4294967295> ]
        FastEthernet <0-9>/<0-24>[ . ][ <0-4294967295> ]
        GigabitEthernet <0-9>/<0-24>[ . ][ <0-4294967295> ]
        Loopback <0-2147483647>
        Serial <0-9>/<0-24>
    database
    interface
        Ethernet <0-9>/<0-24>[ . ][ <0-
```



- 4294967295>]
 - FastEthernet <0-9>/<0-24>[.][<0-4294967295>]
 - GigabitEthernet <0-9>/<0-24>[.][<0-4294967295>]
 - Loopback <0-2147483647>
 - Serial <0-9>/<0-24>
 - neighbor [detail]
 - Ethernet <0-9>/<0-24>[.][<0-4294967295>]
 - FastEthernet <0-9>/<0-24>[.][<0-4294967295>]
 - GigabitEthernet <0-9>/<0-24>[.][<0-4294967295>]
 - Loopback <0-2147483647>
 - Serial <0-9>/<0-24>
 - protocols
 - rip database
 - route [WORD | connected | eigrp | ospf <1-65535> | rip | static]
- mac-address-table [static]
- protocols
- running-config
- sessions
- spanning-tree [vlan <1-1005>]
- startup-config
- users
- version
- vlan-switch [brief | id <1-1005> | name WORD]
- vtp
 - counters
 - status
- telnet [WORD]
- traceroute [WORD]
 - [Protocol] [Target IP address] [Source address] [Numeric display] [Timeout in seconds] [Probe count] [Minimum Time to Live] [Maximum Time to Live]
- undebg
 - all
 - eigrp
 - fsm
 - packets
 - ip
 - ospf



- adj
- events
- packet
- rip [events]
- routing
- **vlan** database
- **write** [erase | memory | terminal]

Global Mode

- **access-list** (named ACL is under the "ip access-list" branch in Global Mode)
 - <1-99>
 - [deny | permit] [A.B.C.D | any | host A.B.C.D]
 - [deny | permit] [A.B.C.D A.B.C.D]
 - remark LINE
 - <100-199>
 - [deny | permit] [icmp | ip] [A.B.C.D A.B.C.D | any | host A.B.C.D] [A.B.C.D A.B.C.D | any | host A.B.C.D]
 - [deny | permit] [tcp | udp] [A.B.C.D A.B.C.D | any | host A.B.C.D] [A.B.C.D A.B.C.D | any | eq <0-65535> | host A.B.C.D | gt <0-65535> | lt <0-65535> | neq <0-65535> | range <0-65535> <0-65535>] [eq <0-65535> | gt <0-65535> | lt <0-65535> | neq <0-65535> | range <0-65535> <0-65535>]
 - remark LINE
- **banner** motd LINE
- **boot** system flash WORD
- **cdp** run
- **clock** timezone WORD <-23 - 23> [<0-59>]
- **config-register** WORD
- **enable**
 - password
 - 7 WORD
 - LINE
 - secret [0 | 5] LINE
- **end**
- **exit**
- **hostname** WORD
- **interface**
 - Ethernet <0-9>/<0-24>[.][<0-4294967295>]
 - FastEthernet <0-9>/<0-24>[.][<0-4294967295>]
 - GigabitEthernet <0-9>/<0-24>[.][<0-4294967295>]
 - Loopback <0-2147483647>
 - Serial <0-9>/<0-24> [multipoint | point-to-point]



- Vlan <1-1005>
- **ip**
 - access-list
 - extended
 - <100-199>
 - WORD
 - standard
 - <1-99>
 - WORD
 - default-network A.B.C.D
 - dhcp
 - excluded-address A.B.C.D [A.B.C.D]
 - pool WORD
 - domain-lookup
 - host WORD A.B.C.D [A.B.C.D] [A.B.C.D]
 - name-server A.B.C.D
 - nat
 - inside source
 - list [<1-199> | WORD] interface [Ethernet | FastEthernet | GigabitEthernet | Serial] <0-9>/<0-24>[.][<0-4294967295>] [overload]
 - list [<1-199> | WORD] pool WORD [overload]
 - static
 - A.B.C.D A.B.C.D
 - tcp A.B.C.D <1-65535> A.B.C.D <1-65535>
 - udp A.B.C.D <1-65535> A.B.C.D <1-65535>
 - pool WORD A.B.C.D A.B.C.D netmask A.B.C.D
 - route A.B.C.D A.B.C.D
 - A.B.C.D [<1-255>]
 - Ethernet <0-9>/<0-24>[.][<0-4294967295>] [<1-255>]
 - FastEthernet <0-9>/<0-24>[.][<0-4294967295>] [<1-255>]
 - GigabitEthernet <0-9>/<0-24>[.][<0-4294967295>] [<1-255>]
 - Loopback <0-2147483647> [<1-255>]
 - Serial <0-9>/<0-24> [<1-255>]
 - Vlan <1-1005> [<1-255>]
- **line**
 - <0-81> [<1-81>]
 - console <0-0>
 - vty <0-15> [<1-15>]
- **mac-address-table** static H.H.H interface



- Ethernet <0-9>/<0-24>[.][<0-4294967295>] vlan <1-1005>
- FastEthernet <0-9>/<0-24>[.][<0-4294967295>] vlan <1-1005>
- GigabitEthernet <0-9>/<0-24>[.][<0-4294967295>] vlan <1-1005>
- **no**
 - access-list [<1-99> | <100-199>]
 - banner motd
 - boot system flash WORD
 - cdp run
 - clock timezone
 - config-register
 - enable
 - password [7 WORD]
 - secret
 - hostname
 - interface
 - Ethernet <0-9>/<0-24>[.][<0-4294967295>]
 - FastEthernet <0-9>/<0-24>[.][<0-4294967295>]
 - GigabitEthernet <0-9>/<0-24>[.][<0-4294967295>]
 - Loopback <0-2147483647>
 - Serial <0-9>/<0-24>
 - Vlan <1-1005>
 - ip
 - access-list
 - extended [<100-199> | WORD]
 - standard [<1-99> | WORD]
 - default-network A.B.C.D
 - dhcp
 - excluded-address A.B.C.D [A.B.C.D]
 - pool WORD
 - domain-lookup
 - host WORD [A.B.C.D] [A.B.C.D] [A.B.C.D]
 - name-server
 - nat
 - inside source
 - list [<1-199> | WORD]
 - static
 - A.B.C.D A.B.C.D
 - tcp A.B.C.D <1-65535> A.B.C.D <1-65535>
 - udp A.B.C.D <1-65535> A.B.C.D <1-65535>
 - route A.B.C.D A.B.C.D <1-255>



- A.B.C.D [<1-255>]
- Ethernet <0-9>/<0-24>[.][<0-4294967295>] [<1-255>]
- FastEthernet <0-9>/<0-24>[.][<0-4294967295>] [<1-255>]
- GigabitEthernet <0-9>/<0-24>[.][<0-4294967295>] [<1-255>]
- Loopback <0-2147483647> [<1-255>]
- Serial <0-9>/<0-24> [<1-255>]
- Vlan <1-1005> [<1-255>]
- mac-address-table static H.H.H int
 - Ethernet <0-9>/<0-24>[.][<0-4294967295>] vlan <1-1005>
 - FastEthernet <0-9>/<0-24>[.][<0-4294967295>] vlan <1-1005>
 - GigabitEthernet <0-9>/<0-24>[.][<0-4294967295>] vlan <1-1005>
- router
 - eigrp <1-65535>
 - ospf <1-65535>
 - rip
- service password-encryption
- spanning-tree vlan <1-1005> priority
- username WORD
- **router**
 - eigrp <1-65535>
 - ospf <1-65535>
 - rip
- **service password-encryption**
- **spanning-tree** vlan <1-1005> priority <0-61440>
- **username** WORD password
 - 0 LINE
 - 7 WORD
 - LINE

Standard Access List Configuration Mode

- **default**
 - deny
 - A.B.C.D [A.B.C.D]
 - any
 - host A.B.C.D
 - permit



- A.B.C.D [A.B.C.D]
- any
- host A.B.C.D
- **deny**
 - A.B.C.D [A.B.C.D]
 - any
 - host A.B.C.D
- **exit**
- **no**
 - deny
 - A.B.C.D [A.B.C.D]
 - any
 - host A.B.C.D
 - permit
 - A.B.C.D [A.B.C.D]
 - any
 - host A.B.C.D
- **permit**
 - A.B.C.D [A.B.C.D]
 - any
 - host A.B.C.D
- **remark** LINE

Extended Access List Configuration Mode

- **default**
 - [deny | permit] [icmp | ip] [A.B.C.D A.B.C.D | any | host A.B.C.D] [A.B.C.D A.B.C.D | any | host A.B.C.D]
 - [deny | permit] [tcp | udp] [A.B.C.D A.B.C.D | any | host A.B.C.D] [A.B.C.D A.B.C.D | any | eq <0-65535> | host A.B.C.D | gt <0-65535> | lt <0-65535> | neq <0-65535> | range <0-65535> <0-65535>] [eq <0-65535> | gt <0-65535> | lt <0-65535> | neq <0-65535> | range <0-65535> <0-65535>]
- **deny**
 - [icmp | ip] [A.B.C.D A.B.C.D | any | host A.B.C.D] [A.B.C.D A.B.C.D | any | host A.B.C.D]
 - [tcp | udp] [A.B.C.D A.B.C.D | any | host A.B.C.D] [A.B.C.D A.B.C.D | any | eq <0-65535> | host A.B.C.D | gt <0-65535> | lt <0-65535> | neq <0-65535> | range <0-65535> <0-65535>] [eq <0-65535> | gt <0-65535> | lt <0-65535> | neq <0-65535> | range <0-65535> <0-65535>]
- **exit**
- **no**



- [deny | permit] [icmp | ip] [A.B.C.D A.B.C.D | any | host A.B.C.D] [A.B.C.D A.B.C.D | any | host A.B.C.D]
- [deny | permit] [tcp | udp] [A.B.C.D A.B.C.D | any | host A.B.C.D] [A.B.C.D A.B.C.D | any | eq <0-65535> | host A.B.C.D | gt <0-65535> | lt <0-65535> | neq <0-65535> | range <0-65535> <0-65535>] [eq <0-65535> | gt <0-65535> | lt <0-65535> | neq <0-65535> | range <0-65535> <0-65535>]
- **permit**
 - [icmp | ip] [A.B.C.D A.B.C.D | any | host A.B.C.D] [A.B.C.D A.B.C.D | any | host A.B.C.D]
 - [tcp | udp] [A.B.C.D A.B.C.D | any | host A.B.C.D] [A.B.C.D A.B.C.D | any | eq <0-65535> | host A.B.C.D | gt <0-65535> | lt <0-65535> | neq <0-65535> | range <0-65535> <0-65535>] [eq <0-65535> | gt <0-65535> | lt <0-65535> | neq <0-65535> | range <0-65535> <0-65535>]
- **remark** LINE

Ethernet / FastEthernet / GigabitEthernet Interface Mode

- **arp** timeout <0-2147483>
- **bandwidth** <1-10000000>
- **cdp** enable
- **delay** <1-16777215>
- **description** LINE
- **duplex** [auto | full | half]
- **exit**
- **ip**
 - access-group [<1-199> | WORD] [in | out]
 - address
 - A.B.C.D A.B.C.D
 - dhcp
 - hello-interval eigrp <1-65535> <1-65535>
 - nat [inside | outside]
 - ospf
 - authentication [message-digest | null]
 - authentication-key LINE
 - cost <1-65535>
 - dead-interval <1-65535>
 - hello-interval <1-65535>
 - message-digest-key <1-255> md5 LINE
 - priority <0-255>
 - split-horizon
 - summary-address eigrp <1-65535> A.B.C.D A.B.C.D [<1-255>



-]
- **mac-address** H.H.H
- **no**
 - arp timeout
 - bandwidth
 - cdp enable
 - delay
 - description
 - duplex
 - ip
 - access-group [<1-199> | WORD] [in | out]
 - address [dhcp]
 - hello-interval eigrp <1-65535>
 - nat [inside | outside]
 - ospf
 - authentication
 - authentication-key
 - cost
 - dead-interval
 - hello-interval
 - message-digest-key <1-255>
 - priority
 - split-horizon
 - summary-address eigrp <1-65535> A.B.C.D A.B.C.D [<1-255>]
 - mac-address
 - shutdown
 - speed
- **shutdown**
- **speed** [10 | 100 | 1000 | auto] *(10/100 options are only available for FastEthernet and GigabitEthernet interfaces and 10/100/1000 options are only available for GigabitEthernet interfaces respectively)*

Ethernet / FastEthernet / GigabitEthernet Sub-Interface Mode

- **arp** timeout <0-2147483>
- **bandwidth** <1-10000000>
- **delay** <1-16777215>
- **description** LINE
- **encapsulation** dot1Q <1-1005> [native]
- **exit**
- **ip**
 - access-group [<1-199> | WORD] [in | out]



- address
 - A.B.C.D A.B.C.D
 - dhcp
- hello-interval eigrp <1-65535> <1-65535>
- nat [inside | outside]
- ospf
 - authentication [message-digest | null]
 - authentication-key LINE
 - cost <1-65535>
 - dead-interval <1-65535>
 - hello-interval <1-65535>
 - message-digest-key <1-255> md5 LINE
 - priority <0-255>
- split-horizon
- summary-address eigrp <1-65535> A.B.C.D A.B.C.D [<1-255>
-]
- **no**
 - arp timeout
 - bandwidth
 - delay
 - description
 - encapsulation dot1Q
 - ip
 - access-group [<1-199> | WORD] [in | out]
 - address [dhcp]
 - hello-interval eigrp <1-65535>
 - nat [inside | outside]
 - ospf
 - authentication
 - authentication-key
 - cost
 - dead-interval
 - hello-interval
 - message-digest-key <1-255>
 - priority
 - split-horizon
 - summary-address eigrp <1-65535> A.B.C.D A.B.C.D [<1-255>]
 - shutdown
- **shutdown**

Serial Interface Mode



- **bandwidth** <1-10000000>
- **cdp** enable
- **clock rate** <1200-4000000> *(only certain clock rates that are listed are valid)*
- **delay** <1-16777215>
- **description** LINE
- **encapsulation**
 - hdlc
 - ppp
 - frame-relay [ietf]
- **exit**
- **frame-relay**
 - interface-dlci <16-1007>
 - lmi-type [ansi | cisco | q933a]
 - map ip A.B.C.D <16-1007>
 - broadcast [cisco | ietf]
 - cisco [broadcast]
 - ietf [broadcast]
- **ip**
 - access-group [<1-199> | WORD] [in | out]
 - address A.B.C.D A.B.C.D
 - hello-interval eigrp <1-65535> <1-65535>
 - nat [inside | outside]
 - ospf
 - authentication [message-digest | null]
 - authentication-key LINE
 - cost <1-65535>
 - dead-interval <1-65535>
 - hello-interval <1-65535>
 - message-digest-key <1-255> md5 LINE
 - priority <0-255>
 - split-horizon
 - summary-address eigrp <1-65535> A.B.C.D A.B.C.D [<1-255>]
- **keepalive**
- **no**
 - bandwidth <1-10000000>
 - cdp enable
 - clock rate
 - delay
 - description
 - encapsulation
 - frame-relay



▪	interface-dlci <16-1007>
▪	lmi-type [ansi cisco q933a]
▪	map ip A.B.C.D
○	ip
▪	access-group [<1-199> WORD] [in out]
▪	address [dhcp]
▪	hello-interval eigrp <1-65535>
▪	nat [inside outside]
▪	ospf
▪	authentication
▪	authentication-key
▪	cost
▪	dead-interval
▪	hello-interval
▪	message-digest-key <1-255>
▪	priority
▪	split-horizon
▪	summary-address eigrp <1-65535> A.B.C.D A.B.C.D [<1-255>]
○	keepalive
○	ppp
▪	authentication
▪	pap sent-username
○	shutdown
•	ppp
○	authentication chap [pap]
○	authentication pap [chap]
•	shutdown

VLAN Interface Mode

- **arp** timeout <0-2147483>
- **bandwidth** <1-10000000>
- **delay** <1-16777215>
- **description** LINE
- **exit**
- **ip**
 - access-group [<1-199> | WORD] [in | out]
 - address
 - A.B.C.D A.B.C.D
 - dhcp
 - hello-interval eigrp <1-65535> <1-65535>
 - nat [inside | outside]



- ospf
 - authentication [message-digest | null]
 - authentication-key LINE
 - cost <1-65535>
 - dead-interval <1-65535>
 - hello-interval <1-65535>
 - message-digest-key <1-255> md5 LINE
 - priority <0-255>
- split-horizon
- summary-address eigrp <1-65535> A.B.C.D A.B.C.D [<1-255>]
- **mac-address** H.H.H
- **no**
 - arp timeout
 - bandwidth
 - delay
 - description
 - ip
 - access-group [<1-199> | WORD] [in | out]
 - address [dhcp]
 - hello-interval eigrp <1-65535>
 - nat [inside | outside]
 - ospf
 - authentication
 - authentication-key
 - cost
 - dead-interval
 - hello-interval
 - message-digest-key <1-255>
 - priority
 - split-horizon
 - summary-address eigrp <1-65535> A.B.C.D A.B.C.D [<1-255>]
 - mac-address
 - shutdown
- **shutdown**

VLAN Configuration Mode

- **exit**
- **no**
 - vlan <1-1005>
 - vtp



- client
- password
- transparent
- v2-mode
- **vlan** <1-1005> [name] [WORD]
- **vtp**
 - client
 - domain WORD
 - password WORD
 - server
 - transparent
 - v2-mode

Line Configuration Mode

- **access class** [<1-199> | <1300-2699> | WORD] [in | out]
- **databits** [5 | 6 | 7 | 8]
- **default** [databits | flowcontrol | history size | parity | speed | stopbits]
- **exit**
- **flowcontrol** [NONE | hardware | software]
- **history size** <0-256>
- **login** [local]
- **motd-banner**
- **no** [access-class [<1-199> | <1300-2699> | WORD] [in | out] | databits | flowcontrol | history size | login | motd-banner | parity | password | session-limit | speed | stopbits]
- **parity** [even | mark | none | odd | space]
- **password**
 - 7 WORD
 - LINE
- **session-limit** <0-4294967295>
- **speed** <0-4294967295>
- **stopbits** [1 | 1.5 | 2]

Router EIGRP Mode

- **auto-summary**
- **exit**
- **metric weights** <0-8> <0-256> <0-256> <0-256> <0-256> <0-256>
- **network** A.B.C.D [A.B.C.D]
- **no**
 - auto-summary



- metric weights
- network A.B.C.D [A.B.C.D]
- passive-interface
 - Ethernet <0-9>/<0-24>[.][<0-4294967295>]
 - FastEthernet <0-9>/<0-24>[.][<0-4294967295>]
 - GigabitEthernet <0-9>/<0-24>[.][<0-4294967295>]
 - Loopback <0-2147483647>
 - Serial <0-9>/<0-24>
 - default
- variance <1-128>
- **passive-interface**
 - Ethernet <0-9>/<0-24>[.][<0-4294967295>]
 - FastEthernet <0-9>/<0-24>[.][<0-4294967295>]
 - GigabitEthernet <0-9>/<0-24>[.][<0-4294967295>]
 - Loopback <0-2147483647>
 - Serial <0-9>/<0-24>
 - default
- **variance <1-128>**

Router OSPF Mode

- **area** [<0-4294967295> | A.B.C.D] authentication [message-digest]
- **default-information** originate
- **exit**
- **log-adjacency-changes** [detail]
- **network** A.B.C.D A.B.C.D area [<0-4294967295> | A.B.C.D]
- **no**
 - area [<0-4294967295> | A.B.C.D] authentication [message-digest]
 - default-information
 - log-adjacency-changes [detail]
 - network A.B.C.D A.B.C.D area [<0-4294967295> | A.B.C.D]
 - passive-interface
 - Ethernet <0-9>/<0-24>[.][<0-4294967295>]
 - FastEthernet <0-9>/<0-24>[.][<0-4294967295>]
 - GigabitEthernet <0-9>/<0-24>[.][<0-4294967295>]
 - Loopback <0-2147483647>
 - Serial <0-9>/<0-24>
 - default
- **passive-interface**
 - Ethernet <0-9>/<0-24>[.][<0-4294967295>]
 - FastEthernet <0-9>/<0-24>[.][<0-4294967295>]
 - GigabitEthernet <0-9>/<0-24>[.][<0-4294967295>]



- Loopback <0-2147483647>
- Serial <0-9>/<0-24>
- default

Router RIP Mode

- **auto-summary**
- **default-information** originate
- **distance** <1-255>
- **exit**
- **network** A.B.C.D
- **no**
 - auto-summary
 - default-information
 - distance <1-255>
 - network A.B.C.D
 - passive-interface
 - Ethernet <0-9>/<0-24>[.][<0-4294967295>]
 - FastEthernet <0-9>/<0-24>[.][<0-4294967295>]
 - GigabitEthernet <0-9>/<0-24>[.][<0-4294967295>]
 - Loopback <0-2147483647>
 - Serial <0-9>/<0-24>
 - default
 - timers basic
 - version <1-2>
- **passive-interface**
 - Ethernet <0-9>/<0-24>[.][<0-4294967295>]
 - FastEthernet <0-9>/<0-24>[.][<0-4294967295>]
 - GigabitEthernet <0-9>/<0-24>[.][<0-4294967295>]
 - Loopback <0-2147483647>
 - Serial <0-9>/<0-24>
 - default
- **timers** basic <0-4294967295> <1-4294967295> <0-4294967295> <1-4294967295>
- **version** <1-2>

DHCP Pool Configuration Mode

- **default-router** A.B.C.D
- **dns-server** A.B.C.D
- **exit**
- **network** A.B.C.D A.B.C.D

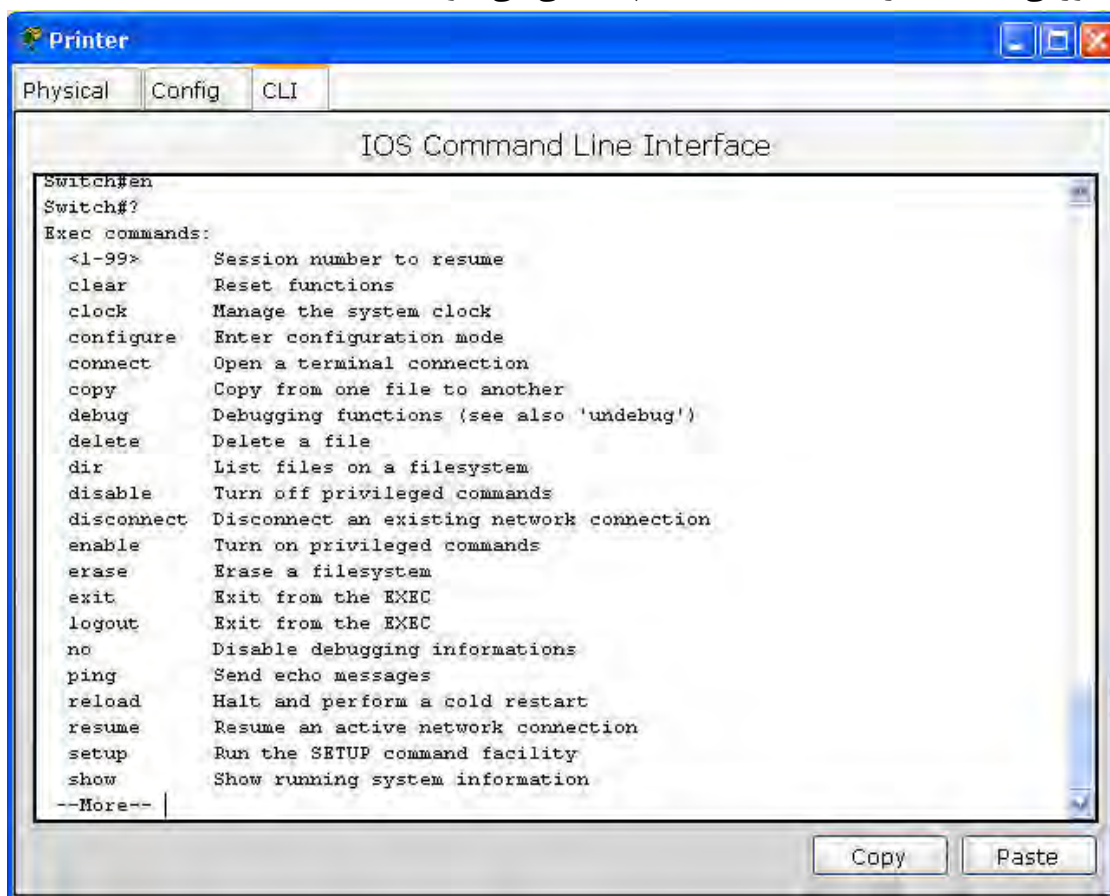


✓ ضمائم: شبیه سازی شبکه های کامپیوتری

- no dns-server

ضمیمه ۵ - دستورات IOS سوئیچ

روی برگه CLI در پنجره تنظیمات سوئیچ کلیک کنید تا به واسط خط فرمان دستورات IOS وارد شوید. در خط فرمان می توانید از دکمه های Copy و Paste استفاده کنید. این بخش شامل لیست دستوراتی است که در Packet Tracer 4.1 پشتیبانی می شود.

**User Mode**

- **<1-99>**
- **connect**
- **disconnect**
- **enable**
- **exit**
- **logout**
- **ping WORD**
- **resume [<1-16> | WORD]**
- **show**



- cdp
 - entry
 - * [protocol | version]
 - WORD [protocol | version]
 - interface
 - Ethernet <0-9>/<0-24>[.][<0-4294967295>]
 - FastEthernet <0-9>/<0-24>[.][<0-4294967295>]
 - GigabitEthernet <0-9>/<0-24>[.][<0-4294967295>]
 - neighbors [detail]
- clock
- dtp
- flash:
- history
- interfaces
 - Ethernet <0-9>/<0-24> [switchPort]
 - FastEthernet <0-9>/<0-24> [switchPort]
 - GigabitEthernet <0-9>/<0-24> [switchPort]
 - Vlan <1-1005>
 - Switchport
 - trunk
- ip interface
 - Vlan <1-1005>
 - brief
- mac-address-table
- version
- vlan
- telnet [WORD]
- traceroute WORD

Enable Mode

- <1-99>
- clear
 - arp-cache
 - cdp table
 - mac-address-table dynamic
 - vtp counters
- clock set hh:mm:ss [<1-31> MONTH <1993-2035> | MONTH <1-31> <1993-2035>]
- configure terminal
- connect [WORD]



- **copy**
 - running-config
 - startup-config
 - tftp:
 - startup-config
 - running-config
 - tftp:
 - tftp:
 - flash:
 - running-config
 - startup-config
- **debug sw-vlan**
 - packets
 - vtp
 - events
- **dir [flash:]**
- **disable**
- **disconnect <1-16>**
- **enable**
- **erase startup-config**
- **exit**
- **logout**
- **no debug**
 - all
 - sw-vlan
 - packets
 - vtp
 - events
- **ping [WORD]**
 - [Protocol] [Target IP address] [Repeat count] [Datagram size] [Timeout in seconds] [Extended commands] [Sweep range of sizes]
- **reload**
- **resume [<1-16> | WORD]**
- **setup**
- **show**
 - arp
 - cdp
 - entry
 - * [protocol | version]
 - WORD [protocol | version]
 - interfaces
 - Ethernet <0-9>/<0-24>[.][<0-4294967295>]
 - FastEthernet <0-9>/<0-24>[.][<0-



```
4294967295> ]
  ■ GigabitEthernet <0-9>/<0-24>[ . ][ <0-
4294967295> ]
  ■ neighbors [ detail ]
○ clock
○ dtp
○ flash:
○ history
○ hosts
○ interfaces
  ■ Ethernet <0-9>/<0-24> [ switchPort ]
  ■ FastEthernet <0-9>/<0-24> [ switchPort ]
  ■ GigabitEthernet <0-9>/<0-24> [ switchPort ]
  ■ Vlan <1-1005>
  ■ Switchport
  ■ trunk
○ ip interface
  ■ Vlan <1-1005>
  ■ brief
○ mac-address-table [ static ]
○ port-security
  ■ interface
    ■ Ethernet <0-9>/<0-24>
      ■ address
        ■ |
          ■ begin LINE
          ■ exclude LINE
          ■ include LINE
        ■ |
          ■ begin LINE
          ■ exclude LINE
          ■ include LINE
      ■ FastEthernet <0-9>/<0-24>
        ■ address
          ■ |
            ■ begin LINE
            ■ exclude LINE
            ■ include LINE
          ■ |
            ■ begin LINE
            ■ exclude LINE
            ■ include LINE
        ■ GigabitEthernet <0-9>/<0-24>
```



		address	
			begin LINE
			exclude LINE
			include LINE
			begin LINE
			exclude LINE
			include LINE
		begin LINE	
		exclude LINE	
		include LINE	
○	running-config		
○	sessions		
○	spanning-tree		
▪	vlan WORD		
○	startup-config		
○	tcp [brief]		
○	users		
○	version		
○	vlan [brief id <1-1005> name WORD]		
○	vtp		
▪	counters		
▪	password		
▪	status		
•	telnet [WORD]		
•	traceroute [WORD]		
○	[Protocol] [Target IP address] [Source address] [Numeric display] [Timeout in seconds] [Probe count] [Minimum Time to Live] [Maximum Time to Live]		
•	undebug		
○	all		
○	sw-vlan		
▪	packets		
▪	vtp		
▪	events		
•	vlan database		
•	write [erase memory terminal]		

Global Mode

•	banner motd LINE
---	------------------



- **boot system flash WORD**
- **cdp run**
- **clock timezone WORD <-23 - 23> [<0-59>]**
- **enable**
 - password
 - 7 WORD
 - LINE
 - secret [0 | 5] LINE
- **end**
- **exit**
- **hostname WORD**
- **interface**
 - Ethernet <0-9>/<0-24>
 - FastEthernet <0-9>/<0-24>
 - GigabitEthernet <0-9>/<0-24>
 - Vlan <1-1005>
- **ip**
 - default-gateway A.B.C.D
 - domain-lookup
 - host WORD A.B.C.D [A.B.C.D] [A.B.C.D]
 - name-server A.B.C.D
- **line**
 - <0-16> [<1-16>]
 - console <0-0>
 - vty <0-15> [<1-15>]
- **mac-address-table static H.H.H vlan <1-1005> interface**
 - Ethernet <0-9>/<0-24>
 - FastEthernet <0-9>/<0-24>
 - GigabitEthernet <0-9>/<0-24>
- **no**
 - banner motd
 - boot system flash WORD
 - cdp run
 - clock timezone
 - enable
 - password [7 WORD]
 - secret
 - hostname
 - interface Vlan <1-1005>
 - ip
 - default-network A.B.C.D
 - domain-lookup
 - host WORD [A.B.C.D] [A.B.C.D] [A.B.C.D]



- name-server
- mac-address-table static H.H.H vlan <1-1005> int
 - Ethernet <0-9>/<0-24>
 - FastEthernet <0-9>/<0-24>
 - GigabitEthernet <0-9>/<0-24>
- service password-encryption
- spanning-tree vlan WORD priority
- vlan <1-1005>
- vtp [mode | password | version <1-2>]
- **service password-encryption**
- **spanning-tree vlan WORD priority <0-61440>**
- **vlan <1-1005>**
- **vtp**
 - domain WORD
 - mode
 - client
 - server
 - transparent
 - password WORD
 - version <1-2>

Ethernet / FastEthernet / GigabitEthernet Interface Mode

- **cdp enable**
- **description LINE**
- **duplex [auto | full | half]**
- **exit**
- **mac address H.H.H**
- **no**
 - cdp enable
 - description
 - duplex
 - mac-address
 - shutdown
 - speed
 - switchport
 - access vlan
 - mode
 - native vlan
 - negotiate
 - port-security
 - mac-address H.H.H



- sticky [H.H.H]
- maximum
- violation
- trunk [allowed | native] vlan
- voice vlan
- **shutdown**
- **speed** [10 | 100 | 1000 | auto] (*10/100 options are only available for FastEthernet and GigabitEthernet interfaces and 10/100/100 options are only available for GigabitEthernet interfaces respectively*)
- **switchport**
 - access vlan <1-1005>
 - mode
 - access
 - dynamic [auto | desirable]
 - trunk
 - native vlan <1-1005>
 - nonegotiate
 - port-security
 - mac-address
 - H.H.H
 - sticky [H.H.H]
 - maximum <1-132>
 - violation shutdown
 - trunk
 - allowed vlan
 - WORD
 - add <1-1005>
 - all
 - except <1-1005>
 - none
 - remove <1-1005>
 - native vlan <1-1005>
 - voice vlan <1-1005>

VLAN Interface Mode

- **arp** timeout <0-2147483>
- **description** LINE
- **exit**
- **ip** address [A.B.C.D A.B.C.D | dhcp]
- **mac-address** H.H.H
- **no**
 - arp timeout



- description
- ip address [dhcp]
- mac-address
- shutdown
- **shutdown**

VLAN Configuration Mode

- **exit**
- **no**
 - vlan <1-1005>
 - vtp
 - client
 - password
 - transparent
 - v2-mode
- **vlan <1-1005> [name] [WORD]**
- **vtp**
 - client
 - domain WORD
 - password WORD
 - server
 - transparent
 - v2-mode

Line Configuration Mode

- **access class** [<1-199> | <1300-2699> | WORD] [in | out]
- **databits** [5 | 6 | 7 | 8]
- **default** [databits | flowcontrol | history size | parity | speed | stopbits]
- **exit**
- **flowcontrol** [NONE | hardware | software]
- **history size** <0-256>
- **login** [local]
- **motd-banner**
- **no** [access-class [<1-199> | <1300-2699> | WORD] [in | out] | databits | flowcontrol | history size | login | motd-banner | parity | password | session-limit | speed | stopbits]
- **parity** [even | mark | none | odd | space]
- **password**
 - 7 WORD
 - LINE



✓ ضمائم: شبیه سازی شبکه های کامپیوتری

- **session-limit** <0-4294967295>
- **speed** <0-4294967295>
- **stopbits** [1 | 1.5 | 2]



ضمیمه ۶- فلوچارت های نحوه پردازش در دستگاه ها

لایه ۱ الگوریتم پردازش بسته در هاب در زمان دریافت بسته

- If two or more ports receive frames at the same time, a collision occurs and the hub forwards a jam signal to all ports.
- If one port receives a frame, the hub forwards the frame to all ports except the receiving port..

لایه ۱ الگوریتم پردازش بسته در تکرار کننده در زمان دریافت بسته

- The repeater forwards the frame to the other port.

لایه ۲ الگوریتم پردازش فریم های دریافتی در سوئیچ

- It compares the receiving port's type (trunk or access) to the frame's format.
 - It drops the frame if (any):
 - The port is an access port while the frame has a Dot1q encapsulation format.
 - The port is a trunk port and the frame is not a Dot1q frame
 - Otherwise, continue to process the frame.
- It drops the frame if the receiving port is a blocking port (set by the Packet Tracer Layer 2 Loop Breaking Protocol [PTL2LBP]) and the frame is not a PTL2LBP frame.
- It determines which VLAN the frame is destined.
 - If the receiving port is a trunk (and so the frame is a Dot1q frame):
 - It gets the frame's destination VLAN number from the VLAN tag in the Dot1q header.
 - It checks if it (the switch itself) has that particular VLAN configured.
 - If that VLAN is configured, it refers to that VLAN's MAC table:
 - If the frame's source MAC address is in the MAC table, it resets the entry's timer.
 - If not, it creates a new MAC entry in the table and starts a timer for it. When the timer expires (5 min), it removes the entry.



- If that VLAN is not configured, the switch broadcasts the frame to all trunk ports (except the receiving port) that allows that VLAN number.
- If the receiving port is an access VLAN (the frame is destined for that VLAN), it continues to process it. It sends it to a higher process if (any):
 - The frame is a PTL2LBP frame.
 - The frame's destination MAC address is a CDP multicast address.
 - The frame's destination MAC address is a broadcast MAC address.
 - The frame's destination MAC address matches the active VLAN interface's MAC address.



لایه ۲ الگوریتم چگونگی ارسال فریم در سوئیچ

- If the frame came from a higher-level process:
 - It checks if the outgoing port is up.
 - If outgoing port is up, send the frame out.
 - If outgoing port is not up:
 - It tries to find the active VLAN interface that is up, and then sends it out that interface.
 - If it cannot find such an interface, it finds the first VLAN that is allowed in the trunk that is configured on the switch.
 - If it can find such an interface, it encapsulates the frame with a Dot1q header with that VLAN number tag and sends it out to the trunk.
 - If no such trunk is configured, it drops the frame.
- If the frame came from a same-level process:
 - If the outgoing port is not up (not configured), it drops the frame.
 - Otherwise, it continues the process
- It checks if the frame's destination MAC address is a unicast. If so:
 - If the outgoing port is the same as the incoming port, it drops the frame.
 - If the outgoing port is not the incoming port:
 - If the outgoing port is a trunk port:
 - If the frame is a Dot1q frame
 - If the trunk port allows the tag in the frame, it sends the frame.
 - If the trunk port does not allow the frame's tag, it drops the frame.
 - If the frame is not a Dot1q frame
 - If the trunk port allows the VLAN that the frame is destined for:
 - The switch encapsulates the Ethernet frame with a Dot1q header and sends it out the trunk port.
 - If the trunk port does not allow the VLAN that the frame is destined for, it drops the frame.
 - If the outgoing port is an access port:
 - If the frame is a Dot1q frame
 - If the frame's tag is the same as the port's VLAN, it de-encapsulates the frame (to an Ethernet frame) and sends it out.
 - If the frame's destination tag is different from the port's VLAN number, it drops the frame.



- If the frame is a regular Ethernet frame:
 - If the receiving port's VLAN is the same as the outgoing port's VLAN, it forwards the frame..
 - If not, it drops the frame.
- If the frame's destination MAC address is a multicast address:
 - For each and every port (trunk and access):
 - It checks if the destination VLAN is allowed in that port. If so, it sends the frame out that port with the appropriate format (see the unicast frame sending logic).
 - If the destination VLAN is not allowed, or if the port is the same as the receiving port, the switch will not forward the frame out that port.

لایه ۲ الگوریتم چگونگی ایجاد درخت پوشا (پروتکل STP)

- The STP is a technology that allows switches and bridges to communicate with each other to prevent loops in the network.
- When a switch/bridge is added to a network, it sends out Bridge Protocol Data Units (BPDU) announcing itself as root.
- If the switch/bridge has the lowest ID, it becomes the root.
- The root marks its ports as designated ports.
- None-root switches/bridges mark the port closest to the root as root port. Every none-root switch/bridge will select one root port.
- Each segment of the network will elect one designated ports:
 - If the port has the lowest root ID, it becomes the designated port.
 - If the port has the lowest path cost to the root, it becomes the designated port.
 - If the port has the lowest send ID, it becomes the designated port.
 - If the port has the lowest port ID, it becomes the designated port.
- Ports not marked as root or designated are marked as blocked.

When a switch receives a STP frame:

- If STP is disabled on that port, it drops the frame.
- Otherwise, it checks the frame type.
 - If the frame type is configuratoin BPDU:
 - If the frame does not contain superior information, the switch drops the frame. The information is superior if it contains lower root ID, lower root path cost, lower bridge ID, or lower port ID.



- Records the superior information and selects new root bridge and designated port if necessary. If the device was the root, sends a TCN BPDU through the root port.
- If the BPDU is received on the root port, forward the frame out through designated ports.
- If the frame type is Topology Change Notification (TCN) BPDU:
 - If the frame is received on a none-designated port, the switch drops the frame.
 - If the device is the root, the switch sets topology change flag to true in the BPDU.
 - If the device is not the root, the switch forward the frame out through root port.

لایه ۲ نحوه عملکرد امنیت پورت

When switch receives a frame :

- If port security is on and the receiving port is not in the dynamic mode port security processes the frame.
 - It sets the last source MAC address and VLAN on the port from the received frame information.
 - If any Mac entry exists with the same source MAC address :
 - If the interface of the MAC entry is the same as the receiving interface and same VLAN as the receiving interface, the frame passes port security.
 - Otherwise
 - If the MAC entry is a dynamic entry then removes the dynamic entry and:
 - If the maximum allowed secure MAC addresses is reached it drops the frame and goes to the violation mode.
 - If the maximum allowed secure MAC addresses is not reached the frame passes the port security process.
 - If the MAC entry is a static entry then it applies the violation mode because another port in the same VLAN has the same static MAC address.
 - If MAC entry with the same source MAC does not exist:
 - If the maximum allowed secure MAC addresses is reached drops the frame
 - Otherwise frame passes the port security process.

If the frame passes the security process and the sticky MAC address is on, on the received interface. The Mac entry gets added to the MAC table as a static entry.



A switch port can be configured with secure MAC addresses even if the port's line protocol is down.

When the port's line protocol changes from down to up if there is a list of secure MAC addresses for the port waiting to be added to the MAC table, the port security checks the MAC entries with the same VLAN address as the current port.

- If there is a same MAC address on the current port which is an sticky MAC, port security deletes the secure MAC from the list and does not add it to the MAC table.
- If the MAC address does not exist in the MAC table then it adds a MAC entry for that secure MAC to the MAC table.

لایه ۲ چگونگی تصمیم گیری DTP در مورد حالت پورت

When the switch port on the other side of the link receives the DTP update it :

- If there is a VTP domain name mismatch it drops the frame
- If the port is configured to be in access or trunk administrative mode it drops the frame.
- If the port is dynamic and is not in the nonegiate state it processes the frame.
 - If the same MAC entry (with the same source MAC address as the received frame) exists on the receiving port then restart the timer for that entry.
 - DTP process updates the port's operational mode based on the received DTP port status.
 - Otherwise it adds a new MAC entry to the MAC table and set a timer for it.
 - DTP process updates the port's operational mode based on the received DTP port status.

To update the port operational mode DTP :

- If the number of neighbors on that port which are sending DTP frame are more than one or is equal to zero.
 - Change the operational mode of the receiving port to static access.
- If the number of neighbors is equal to 1
 - If local port's administrative mode is dynamic auto
 - If remote neighbor's port is in the administrative mode of desirable or trunk set the operation mode of local port to trunk, otherwise to static access.
 - If local port's administrative mode is dynamic desirable



- If remote neighbor's port is in administrative mode of desirable or trunk or auto set the operation mode of local port to trunk, otherwise to static access.
- If the local port's administrative mode is access then drop the frame and do not process any DTP frame.

لایه ۲ چگونگی پردازش فریم های VTP ورودی در سوئیچ

- If the switch is in VTP Transparent mode:
 - Forwards VTP frame to all other trunk ports
- If the VTP frame is an Advertisement Request frame:
 - If the domain name on the VTP frame does not match the switch's, then drop the frame, and stop.
 - Send out a Summary Advertisement frame.
 - Send out a Subset Advertisement frame.
- If the VTP frame is a Summary Advertisement frame:
 - If the switch's domain name is set and the one in the VTP frame is different, then drop the frame, and stop.
 - If the switch's domain name is not set, then set the domain name to be the one in the VTP frame, and recalculate MD5.
 - If the MD5 in the VTP frame does not match the one on the switch's, then drop the frame, and stop.
 - If the version is different, then take the one in the VTP frame.
 - If the config revision in the VTP frame is smaller than the one on the switch:
 - Send out a Summary Advertisement frame
 - If the config revision in the VTP frame is larger than the one on the switch:
 - If the followers field is 0:
 - Send out an Advertisement Request frame
 - Wait for the Subset Advertisement frames
 - If the config revision in the VTP frame is the same as the one on the switch:
 - Drop the frame
- If the VTP frame is a Subset Advertisement frame:
 - If the domain name on the VTP frame does not match the switch's, then drop the frame, and stop.
 - If not expecting a Subset Advertisement, then drop the frame, and stop.
 - If the config revision in the VTP frame is different than the expecting one, then drop the frame, and stop.
 - If the sequence number in the VTP frame is different than the expecting one, then drop the frame, and stop.



✓ ضمائم: شبیه سازی شبکه های کامپیوتری

- Add the subset to the reply
- If the VTP frame is the last expecting subset:
 - Update the vlan database with the received subsets
 - Send out a Summary Advertisement frame
 - Send out a Subset Advertisement frame

لایه ۲ چه زمانی سوئیچ ها فریم های VTP ارسال می کنند؟

When do switches send out Advertisement Requests:

- ☐ When the switch detects a VTP configuration change and it is in VTP Client mode
- ☐ When receiving a Summary Advertisement but there is no subset following it

When do switches send out Summary Advertisements:

- ☐ When a trunk port comes up and the switch is already advertising VTP
Every 5 minutes
- ☐ When receiving a Summary Advertisement with its config revision smaller than the switch's

When do switches send out Subset Advertisements:

- ☐ When a trunk port comes up and the switch is not already advertising VTP
- ☐ When a local VLAN change is detected and the switch is in VTP Server mode
- ☐ When the switch detects a VTP configuration change and it is in VTP Server mode
- ☐ After updating vlan database on the receiving of Subset Advertisements
- ☐ When receiving a Advertisement Request

- HDLC is the default data link protocol for serial interfaces.
- Sends keepalives periodically to the other end of the link.
- When it receives a keepalive, it brings up the line protocol.
- If it does not receive a keepalive from the other end for a certain period of time, it brings down the line protocol.
- If the interface is configured to not use keepalives, it would bring up the line protocol even if it does not receives keepalives from the other end.

لایه ۳ چگونگی پردازش بسته های RIP ورودی توسط روتر

- It drops the packet if (any):
 - The incoming port does not have a valid IP address or is not RIP-enabled.
 - The source IP address is not from a directly connected network.
 - The packet came from the router itself.
 - The packet's RIP version does not match the router's RIP version.



- If the packet is a request packet,
 - Check the port to see if it is a passive interface.
 - If it is, drop the packet.
 - If it is not a passive interface, process the packet:
 - Create a RIP response packet, which contains information about a route or the entire routing table (depending on the request).
 - Send the RIP response out the same port.
- If the packet is a response packet, process it:
 - Look through each RIP route portion of the packet (the portion from address family identifier, or AFI, to the metric). A RIP packet can contain up to 25 RIP route portions.
 - Ignore any portions where (any):
 - The metric is greater than infinity.
 - The AFI is not the IP family.
 - It is a broadcast, Class D, or Class E address.
 - Set the next hop to the incoming port's address.
 - For new routes, ignore the route portion if the metric is now 16.
 - For existing routes, the metric is set to 16.
 - If the packet contains information about a network that does not exist in the RIP database, it is added to the database.
 - If a network already has an entry in the RIP database, update it with the latest information.
 - Send out new and updated routes on the next triggered update.

لایه ۳ چگونگی پردازش بسته های EIGRP ورودی توسط روتر

When a router receives an EIGRP packet:

- It checks to see if the EIGRP process for the autonomous system that is specified in the packet is enabled.
 - If it is not enabled, then the router drops the packet.
 - Otherwise, it sends the packet to that EIGRP process.

When an EIGRP process receives an EIGRP packet:

- It makes the following checks and drops the packet if (any):
 - The receiving interface does not have EIGRP enabled.
 - The packet does not come from the same subnet as the receiving interface.
 - The receiving interface is passive.
- It checks if the packet is a Hello packet.



- If so, then it processes the Hello packet (skip to next section).
- Otherwise, it checks if the packet came from an existing neighbor.
 - If not, then it drops the packet.
 - If the packet did come from an existing neighbor:
 - It checks if the packet is an Acknowledgment packet.
 - If so, then it removes the acknowledged packet from the neighbor's output queue.
 - Otherwise, it checks the sequence number on the packet and the neighbor's last heard sequence number.
 - If the sequence number on the packet is larger than the last heard, then update the last heard.
 - If the sequence numbers are the same or the one on the packet is smaller than the last heard, then it drops the packet.
 - It checks if the packet piggybacks an Acknowledgment.
 - If so, it removes the acknowledged packet from the neighbor's output queue.
 - It checks if there are any packets in the neighbor's output queue.
 - If there are not, then it sends an Acknowledgment packet back to the neighbor.
 - It checks if the packet is an Update packet. If so, then it processes the Update packet.
 - It checks if the packet is an Query packet. If so, then it processes the Query packet.
 - It checks if the packet is an Reply packet. If so, then it processes the Rep

When an EIGRP process processes a Hello packet:

- It checks if the Hello packet has matching K values as the EIGRP process.
 - If not, then it removes neighbor from the router's neighbor table.
- It checks if the neighbor already exists in the neighbor table.
 - If so, then it updates the last-heard time and hold timer.
 - If not, it add the new neighbor to the neighbor table, and send a full update of its topology table to the new neighbor.

When an EIGRP process processes an Update packet:



- It goes through all routes in the Update packet and updates the topology table.

When an EIGRP process processes a Query packet:

- It updates the topology table with the route in the query.
- It checks if updating the topology table does not cause the process to query other neighbors.
- If it does not, then reply the best route to the queried neighbor.

When an EIGRP process processes a Reply packet:

- It makes the following checks and drops the packet if (any):
 - The replied route does not exist.
 - The network is not in ACTIVE state.
 - The neighbor who replied was not queried.
- It checks if the replied route is better than the best heard in the reply table.
 - If so, then it replaces the best heard in the reply table with the replied route.
- It checks if the replied route is the last expected reply.
 - If it is, then processes the last Reply packet to a query.

When an EIGRP process processes a last Reply packet to a query:

- It replies to all queried neighbors with the best-heard route from the reply table.
- It sets the network to PASSIVE state.
- It updates the topology table with the best route.

When an EIGRP process updates the topology table with a route:

- Checks if the network is in ACTIVE state.
 - If so, it ignores the update.
- It gets the old best route and old best metric to the network.
- It adds the route to the topology table.
- It gets the new best route and new best metric to the network.
- It checks if the new best route is unreachable or there is no feasible successor.
 - If either is true, then it queries neighbors about the route.



- If there is no neighbor to query, then it removes the network from topology and routing table.
- If the new best route is feasible, then it adds all successors for the network to the routing table.
- Update neighbors.

لایه ۳ چگونگی پردازش بسته های OSPF ورودی توسط روتر

When a router receives an OSPF packet:

- It checks to see if an OSPF process is enabled on the port that received the packet.
 - If it is not enabled, then the router drops the packet.
 - Otherwise, it sends the packet to that OSPF process.

When an OSPF process receives an OSPF packet:

- It makes the following checks and drops the packet if (any):
 - The receiving interface does not have OSPF enabled.
 - The packet does not come from the same subnet as the receiving interface.
 - The receiving interface is passive.
 - The packet is for (backup) designated router and the router is not.
 - The authentication failed for the packet.
- It checks if the packet is a Hello packet.
 - If so, then it processes the Hello packet (skip to next section).
 - Otherwise, it checks if the packet came from an existing neighbor.
 - If not, then it drops the packet.
 - If the packet did come from an existing neighbor:
 - It checks if the packet is a Database Description packet (DDP). If so, then it processes the DDP.
 - It checks if the packet is a Link State Request (LSR) packet. If so, then it processes the LSR.
 - It checks if the packet is a Link State Update (LSU) packet. If so, then it processes the LSU.
 - It checks if the packet is a Link State Acknowledgment (LSAck) packet. If so, then it processes the LSAck.

When an OSPF process processes a Hello packet:



- It checks if the Hello packet has matching hello & dead timer values as the OSPF process.
 - If not, then it prints out a warning message and drops the packet.
- It checks if the neighbor already exists in the neighbor table.
 - If so, then it resets the dead timer.
 - If not, it adds the new neighbor to the neighbor table and sets the neighbor state to 2-WAY.
 - The adjacency is established with the neighbor if:
 - The underlying network is point-to-point.
 - The underlying network is broadcast and the router itself is designated router, backup designated router, the neighboring router is designated router, or the neighboring router is backup designated router.
- It checks if backup designated router is present.
 - If not, then it performs designated router election after wait timer expires.

When an OSPF process processes a Database Description packet:

- If the state is exstart, the master/slave relationship is formed based on router ID. The neighbor state is updated to exchange.
- During the exchange state, the OSPF process goes through all the link state advertisement (LSA) headers stored in the packet. If the router does not have the LSA described in the header, it stores the header in the queue.
- If there are no more DDPs, the neighbor state transitions to loading. The headers stored in the queue are used to generate LSRs.

When an OSPF process processes a Link State Request (LSR) packet:

- It looks up its Link State Database and puts the information in the Link State Update (LSU) packet and sends to the adjacent neighbor.
- After all the corresponding LSUs are received for the LSRs, the neighbor state transitions to full.

When an OSPF process processes a Link State Update (LSU) packet:

- It validates the LSA's checksum. If the checksum is invalid, discard the LSA.
- It checks the LSA's type. If the type is unknown, discard the LSA.
- It checks the LSA's age. If the age is equal to maximum allowed value and there is currently no instance of the LSA in the router's database, and none of



✓ ضمائم: شبیه سازی شبکه های کامپیوتری

router's neighbors are in states exchange or loading, then the router sends an acknowledge.

- If the LSA is not in the database or is newer, add to the database.
- If the LSA is the same instance as the database copy, and the LSU is not used as implied acknowledgment, send a LSAck to the neighbor.
- If the database copy is more recent, discard the LSA without acknowledging it.

When an OSPF process processes a Link State Acknowledgment packet:

- It checks neighbor's state. If the neighbor is in a lesser state than exchange, discards the packet.
- It checks if the acknowledgment is for an instance of LSA stored in the retransmission list for the neighbor. If yes, the OSPF process removes the LSU from the retransmission list.

When an OSPF process updates the routing table with a route:

- All routers in the same autonomous system belonging to the same area should have identical database.
- After a LSA has been added to the database, the OSPF process starts a timer. The router performs shortest path first (SPF) calculation after the timer expires. The SPF algorithm uses LSAs stored in the database to generate OSPF routes. The routes are added to the routing table.

لایه ۳ چگونگی پردازش بسته های ICMP ورودی در دستگاه ها

When a device receives an ICMP packet:

- It checks the ICMP message contained in the packet.
 - If the packet contains the message "TTL Exceeded" or "Echo Reply."
 - It checks to see if it has recently sent an ICMP message with the same identification as the received ICMP message.
 - If so, it sends out the ICMP.

لایه ۴ چگونگی پردازش سگمنت های UDP توسط دستگاه ها

This procedure explains how a device sends and receives UDP segments.

- When the device receives a segment:
 - It de-encapsulates it and examines the UDP header for port information.



- It then maps the local port information and sends the payload up to a higher layer (the application layer) for processing.
 - If it cannot find the upper process based on the port information, it drops the segment.
- When the device wants to send a segment:
 - It encapsulates the payload with a UDP header.
 - It sends the segment to the lower layer for processing.



لایه ۴ چگونگی پردازش سگمنت های TCP توسط دستگاه ها

When the device receives a TCP segment:

- If there is no socket listening at the destination port or no connections matching the source and destination IPs and ports:
 - Drop the segment and stop
- If the connection is not in LISTEN state:
 - If the sequence number in the received TCP header is 1 less than the connection's sequence number
 - Mark this as a duplicate segment
 - If the sequence numbers are the same
 - If the TCP header is not an empty ACK:
 - Increment the sequence number
 - Otherwise:
 - Drop the segment and stop
 - If the ack number in the received TCP header is 1 more than the connection's sequence number
 - Increment the connection's sequence number
 - Pop out the last sent segment in buffer
 - If there are more segments in buffer
 - Send the next segment
 - If the TCP header is not an empty ACK
 - Send an ACK
 - If this is a duplicate segment
 - Drop segment and stop
- If the connection is in LISTEN state:
 - Start a new connection
 - Send a SYN + ACK
 - Set the new connection's state to SYN_RECEIVED
- If the connection is in SYN_SENT state:
 - If the TCP header is a SYN + ACK
 - Send an ACK
 - Set the connection's state to ESTABLISHED
- If the connection is in SYN_RECEIVED state:
 - If the TCP header is an ACK
 - Set the connection's state to ESTABLISHED
- If the connection is in ESTABLISHED state:
 - If the TCP header's PUSH flag is set:
 - Send the data to the higher layer
 - Otherwise, buffer the data
- If the connection is in FIN_WAIT1 state:
 - If the TCP header is a FIN



- Set the connection's state to CLOSING
- If the TCP header is an ACK
 - Set the connection's state to FIN_WAIT_2
- If the connection is in FIN_WAIT_2 state:
 - If the TCP header is a FIN
 - Set the connection's state to TIMED_WAIT
- If the connection is in LAST_ACK state:
 - If the TCP header is an ACK
 - Set the connection's state to CLOSED
- If the connection is in CLOSING state:
 - If the TCP header is an ACK
 - Set the connection's state to TIMED_WAIT

لایه ۷ چگونگی پردازش بسته های دریافتی توسط کلاینت های DHCP

When a DHCP client device receives a packet:

- It drops the packet if (any):
 - The packet is not a valid DHCP packet.
 - The packet's destination MAC address does not match its own MAC address.
- It checks the packet's DHCP type (its DHCP message).
 - If the packet is a DHCP-OFFER packet, it uses the information in the packet (including client IP address, offered IP address, server IP address, and gateway address) to construct a DHCP-REQUEST packet and sends it back to the server.
 - If the packet is a DHCP-ACK packet, it gets the IP address, subnet mask, and the gateway IP address from the packet and sets its IP address configuration accordingly.
 - If the packet is not a DHCP-OFFER or a DHCP-ACK packet, it will drop the packet.

لایه ۷ چگونگی پردازش بسته های دریافتی توسط سرور DHCP

When a DHCP server device receives a packet:

- It drops the packet if:
 - The packet is not a valid DHCP packet.
- It checks the packet's DHCP type (its DHCP message).
 - If the packet is a DHCP-OFFER packet, it uses the information in the packet (including client IP address, offered IP address, server IP address, and gateway address) to construct a DHCP-REQUEST packet and sends it back to the server.



- If the packet is a DHCP-ACK packet, it gets the IP address, subnet mask, and the gateway IP address from the packet and sets its IP address configuration accordingly.
- If the packet is not a DHCP-OFFER or a DHCP-ACK packet, it will drop the packet.

لایه ۷ چگونگی عملکرد کلاینت TELNET

- TELtype NETwork is a network protocol that utilizes TCP/IP protocol stack to establish a client/server connection. The user starts a TELNET client process on a PC or a Cisco device using telnet command with server IP address. The TELNET server, usually listens on TCP port 23, awaits client connection requests. A TELNET packet is generated from the client process when a key is pressed.

When a TELNET client receives a packet:

- If the packet is not a valid TELNET packet, it drops the packet.
- Otherwise, it writes the received information stored in the packet onto the screen.

لایه ۷ چگونگی عملکرد سرور TELNET

- TELtype NETwork is a network protocol that utilizes TCP/IP protocol stack to establish a client/server connection. The user starts a TELNET client process on a PC or a Cisco device using telnet command with server IP address. The TELNET server is started automatically on a Cisco router or switch. The server listens on TCP port 23 awaiting client connection requests.

When a TELNET server receives a packet:

- If the packet is not a valid TELNET packet it drops the packet.
- Otherwise, it checks the packet and:
 - If the information received is part of a command, it sends an echo back to the client.
 - If the server is able to determine the command entered by the client, it sends the result back to the client.
 - If the server does not understand the information received, it sends an error message back to the client.



لایه ۷ چگونگی عملکرد DNS

When DNS client needs to find the IP address of a domain name:

- If the DNS client is enabled on the client:
 - If DNS client finds the IP address of the domain in its cache it resolves the domain address.
 - DNS client constructs a query with the domain name and sends the query through a DNS resolver to:
 - If the client is configured with a valid DNS server address, it constructs a query with a unicast address.
 - Otherwise to broadcast address.
 - DNS resolver sets a timer
 - If the received DNS response contains a resolved IP address for the queried domain. then it stops timer and segment passes the DNS resolver process.
 - If the received DNS response does not contain a resolved IP (invalid IP) it drops the segment.
 - If the DNS resolver does not receive any response packet and timer expires:
 - DNS resolver tries to resend the query up to 5 times.
 - If the response is not received after 5 retry it gives up and send a message to the client that it did not find any IP address for the domain name.

When a DNS server device receives a packet:

- If the DNS service is enabled on the device and the received packet is a DNS query:
 - If the DNS server finds a domain name in its database with the name in the query packet, it constructs the response packet with the IP address and sends it back .
 - Otherwise it sends an empty response packet back to the sender.
- Otherwise it drops the frame.

لایه ۷ چگونگی عملکرد HTTP

When a client needs to find a webpage from a server:

- If the address is empty or starts with anything else rather than http protocol it drops the request since it is not supported in the PT4.1
- If the address is an IP address or starts with http:// the HTTP client processes it



- The HTTP client first finds the server IP through the server name by parsing the address in the address bar and:
 - If server name is not found it tries to resolve the domain name through a DNS query.
 - If server name is found it gets the IP address.
- HTTP client constructs a request HTTP segment and connects the server through TCP sockets and starts a timer for its request.

When a HTTP client receives a packet:

- If the HTTP message has the HTTP OK code it fetch the page from the message and displays the message
- Otherwise HTTP page displays an error page.

When HTTP server receives a request:

- If the HTTP service is enabled and a TCP connection with HTTP client is established:
 - If the HTTP request is HTTP GET:
 - If the username and password in the HTTP request is not correct:
 - The server sends back an unauthorized error message to the client.
 - Otherwise:
 - If the requested page exists on the server:
 - The server creates a response packet and sends back a HTTP reply to the client.
 - If the requesting page does not exist on the server:
 - The server sends back an error message to the client.
 - Other message codes are not supported in this version of PT and server drops the packet.



لایه ۷ چگونگی عملکرد TFTP Server

When a TFTP server receives a packet:

- If the packet is a READ request:
 - If the file with the requested name exists on the TFTP server:
 - Start a write session with the client
 - If the file with the requested name does not exist on the TFTP server:
 - Send back a TFTP ERROR packet to the client
- If the packet is a WRITE request:
 - Start a read session with the client
- If the packet is anything else:
 - Drop the packet and stop

لایه ۷ چگونگی پردازش بسته های ورودی توسط سرور و کلاینت TFTP

When a TFTP server or client receives a packet during a session:

- If the packet is a READ or WRITE request:
 - Drop the packet and stop
- If the packet is a DATA packet:
 - If the session is a WRITE session or the block number on the packet is not the expecting one:
 - Drop the packet and stop
 - Save the data on the packet
 - Send back an ACK packet
 - Increment the block number
 - If this is the last packet:
 - Write data to file
 - Stop the TFTP session
- If the packet is an ACK packet:
 - If the session is a READ session or the block number on the packet is not the expecting one:
 - Drop the packet and stop
 - If this is not the last packet:
 - Increment the block number
 - Send the next block of data in a DATA packet
 - If this is the last packet:
 - Stop the TFTP session
- If the packet is an ERROR packet:
 - Stop the TFTP session



✓ ضمايم: شبیه سازی شبکه های کامپیوتری

چگونگی پردازش بسته های ورودی توسط مسیریاب (پردازش NAT)

When a router receives a packet:

- It checks if the receiving port is a NAT outside port.
 - If so:
 - It checks to determine whether the packet is UDP, TCP or ICMP to get the packet's source and destination port.
 - It refers to the NAT table (using the global addresses) for the necessary translation.
 - If it finds a match for the packet (a translation exists):
 - It replaces the inside address and port with the local version.
 - It translates the destination IP address and port
 - If the receiving port is not a NAT outside port, or if it is a NAT outside port but the requested IP address is not in the NAT table:
 - The router checks to see if there is a route to the destination IP.
 - It drops the packet if (any):
 - There is no route.
 - It finds a route, but the outgoing port of that route entry is the same as the receiving port.
 - If there is a route, it sends a reply with the receiving port's MAC address.

چگونگی پردازش بسته های خروجی توسط مسیریاب (پردازش NAT)

When a router wants to send a packet out a port:

- It checks if the outgoing port is a NAT inside port.
 - If so:
 - It looks up its NAT table for the necessary translations.
 - It captures the packet's source and destination ports and sets a timer for the packet (depending on the packet's encapsulation type).
 - For a TCP packet the timer is 24 hours.
 - For a UDP packet the timer is 5 minutes.
 - For an ICMP packet the timer is 1 minute.
 - It looks up the NAT table
 - If the receiving port is not a NAT outside port, or if it is a NAT outside port but the requested IP address is not in the NAT table:
 - The router checks to see if there is a route to the destination IP.



✓ ضمائم: شبیه سازی شبکه های کامپیوتری

- It drops the packet if (any):
 - There is no route.
 - It finds a route, but the outgoing port of that route entry is the same as the receiving port.
- If there is a route, it sends a reply with the receiving port's MAC address.



✓ ضمايم: شبیه سازی شبکه های کامپیوتری

چگونگی استفاده از ARP برای ارسال بسته های IP توسط دستگاه ها

When a device sends an IP packet:

- If the destination IP is a broadcast, it sets the packet's destination MAC address to the broadcast MAC address and sends the packet out.
- If the destination IP is a multicast, it sets the packet's destination MAC address to the multicast MAC address and sends the packet out.
- If the destination IP is a unicast, it looks up the ARP table to see if the destination IP matches an entry's IP address in the ARP table.
 - If a match exists, it:
 - Sets the packet's destination MAC address to the entry's MAC address.
 - Sends out the IP packet.
 - If a match does not exist, it:
 - Drops the IP packet.
 - Sends an ARP request out.
 - Adds that request to the list of ARP requests.
 - Sets and starts the timer for it as it waits for an ARP reply.

چگونگی ارسال تقاضاهای ARP توسط دستگاه ها

When a device wants to send an ARP request:

- It will NOT send the request if (any):
 - The sending port is down.
 - The sending port does not have a valid IP address.
 - A request for the same IP address is already sent.
- If none of the above is true, it proceeds with the ARP request. It:
 - Constructs an ARP request for the IP address in question.
 - Sets the destination MAC address to the broadcast address.
 - Adds the request to the list of existing requests.
 - Sets and starts a timer for this request.
 - Sends the request.
 - Waits for an ARP reply.
 - Drops the request from the list if time expires.

چگونگی پردازش بسته های ورودی ARP توسط دستگاه ها

When a device receives an ARP packet:

- It drops the packet if (any):
 - The receiving port is not up.
 - The device is a switch and an active VLAN interface is not up.



- The packet's source IP is not in the same subnet as the receiving port's subnet.
- If the above is not true, it proceeds to process the packet:
 - It checks to see if the packet is an ARP request or an ARP reply.
 - If the packet is an ARP request, it checks to see if the packet's destination IP matches the receiving port's IP address.
 - If they match, the device sends a reply with the receiving port's MAC address.
 - If they do not match:
 - If the device is not a router, it drops the packet.
 - If the device is a router, refer to "How routers process ARP requests."
 - If the packet is an ARP reply, the device checks if it submitted a request for the IP address found in the reply.
 - It drops the packet if there is no such request in the list.
 - If the packet is in the ARP request list:
 - The device now removes the request from the list.
 - If the ARP table does not contain an entry with the IP and MAC addresses found in the packet, it will make a new entry with those addresses.
 - If the ARP table already contains an entry with the IP and MAC addresses found in the packet, it just resets that entry's timer. That entry will be removed from the table when its timer expires.

چگونگی پردازش درخواست های ARP توسط مسیریاب

When a router receives an ARP packet (continuing from "How devices process incoming ARP packets"):

- It checks the NAT status on the receiving port.
 - If the receiving port is a NAT outside port, the router checks the NAT table for the packet's destination IP.
 - If the requested IP address is in the NAT table, the router sends a reply with the receiving port's MAC address.
 - If the receiving port is not a NAT outside port, or if it is a NAT outside port but the requested IP address is not in the NAT table:
 - The router checks to see if there is a route to the destination IP.
 - It drops the packet if (any):
 - There is no route.
 - It finds a route, but the outgoing port of that route entry is the same as the receiving port.



- If there is a route, it sends a reply with the receiving port's MAC address.

نحوه عملکرد ACL

When a Router receives a packet on an interface:

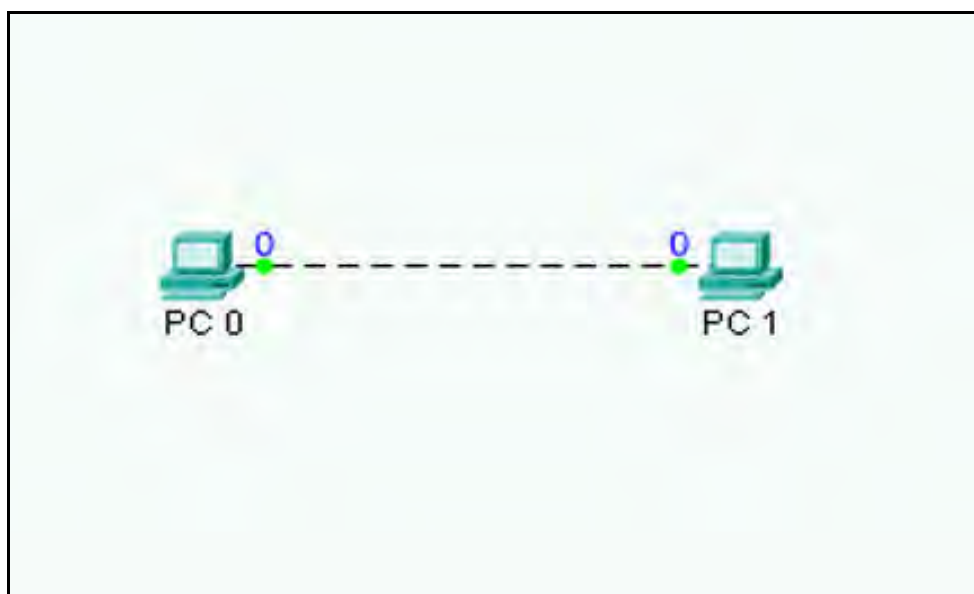
- ACL checks for inbound ACL and if inbound ACL is configured on the interface:
 - If inbound ACL is empty, it permits the packet.
 - If inbound ACL contains statements:
 - If the packet matches the criteria of any of the statements and:
 - If the statement permits the packet, it passes the ACL process.
 - If the statement denies the packet it drop the packet.
 - if there is no match in the list ACL drops the packet by default.

When a Router sends a packet on an interface:

- ACL checks for outbound ACL and if outbound ACL is configured on the interface:
 - If the packet is generated locally it permits the packet.
 - If the outbound ACL is empty, it permits the packet.
 - If outbound ACL contains statements:
 - If the packet matches the criteria of any of the statements
 - If the statement permits the packet, packet passes the ACL process.
 - If the statement denies the packet it drop the packet.
 - if there is no match in the list ACL drops the packet by default.

ضمیمه ۷) آزمایشگاه (CCNA)

peer to peer (CCNA1-5.1.12) ایجاد یک شبکه



اهداف)

ایجاد یک شبکه peer to peer ساده بین دو رایانه شخصی

تعیین آدرس IP ایستگاه ها

بررسی اتصال در توپولوژی شبیه سازی شده

مرحله ۱)

توپولوژی نمایش داده شده در شکل فوق را ایجاد کنید

بعد از اتصال دستگاه ها، آدرس های IP را مطابق جدول زیر اعمال کنید

Computer	IP Address	Subnet mask
PC – 0	192.168.1.1	255.255.255.0
PC – 1	192.168.1.2	255.255.255.0

مرحله ۲)

روی برگه Simulation کلیک کنید



✓ ضمائم: شبیه سازی شبکه های کامپیوتری

یک بسته از PC0 به PC1 اضافه کنید
Play را کلیک کنید تا اتصال را بررسی کنید

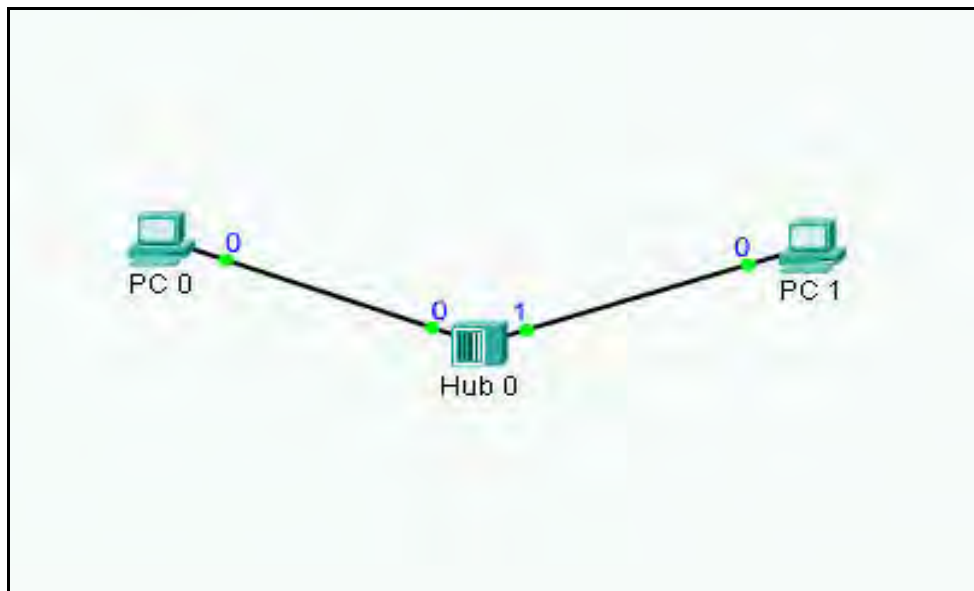
مرحله ۳)

روی PC0 کلیک کنید و آنرا به صورت half duplex تنظیم کنید
همین کار را برای PC1 نیز انجام دهید
یک بسته از PC1 به PC0 ایجاد کنید
Play را کلیک کنید تا شبیه سازی را مشاهده کنید
وقتی دو ایستگاه همزمان سیگنال ارسال می کنند، تصادم در اتصال half duplex اتفاق می افتد (داده در هر لحظه در یک سمت ارسال می شود)

مرحله ۴)

روی PC0 کلیک کنید و آنرا به صورت full duplex تنظیم کنید
همین کار را برای PC1 نیز انجام دهید
Play را کلیک کنید تا شبیه سازی را مشاهده کنید
تصادم در اتصال full duplex اتفاق نمی افتد. (داده همزمان در دو جهت ارسال می شود)

CCNA1-5.1.13a) ایجاد یک شبکه مبتنی بر هاب



اهداف)

ایجاد یک شبکه ساده بین دو رایانه شخصی با استفاده از hub

اعمال آدرس IP با ایستگاه ها

بررسی اتصال در توپولوژی شبیه سازی شده

مرحله ۱)

توپولوژی نمایش داده شده در شکل فوق را ایجاد کنید

بعد از اتصال دستگاه ها، آدرس های IP را مطابق جدول زیر اعمال کنید

Computer	IP Address	Subnet mask
PC – 0	192.168.1.1	255.255.255.0
PC – 1	192.168.1.2	255.255.255.0

مرحله ۲)

روی برگه Simulation کلیک کنید

یک بسته از PC0 به PC1 اضافه کنید

Play را کلیک کنید تا اتصال را بررسی کنید



✓ ضمائم: شبیه سازی شبکه های کامپیوتری

مرحله ۳)

رایانه دیگری را اضافه کنید و آن را به hub متصل کنید. آدرس IP آن را 192.168.1.3 با ماسک شبکه 255.255.255.0 بگذارید.

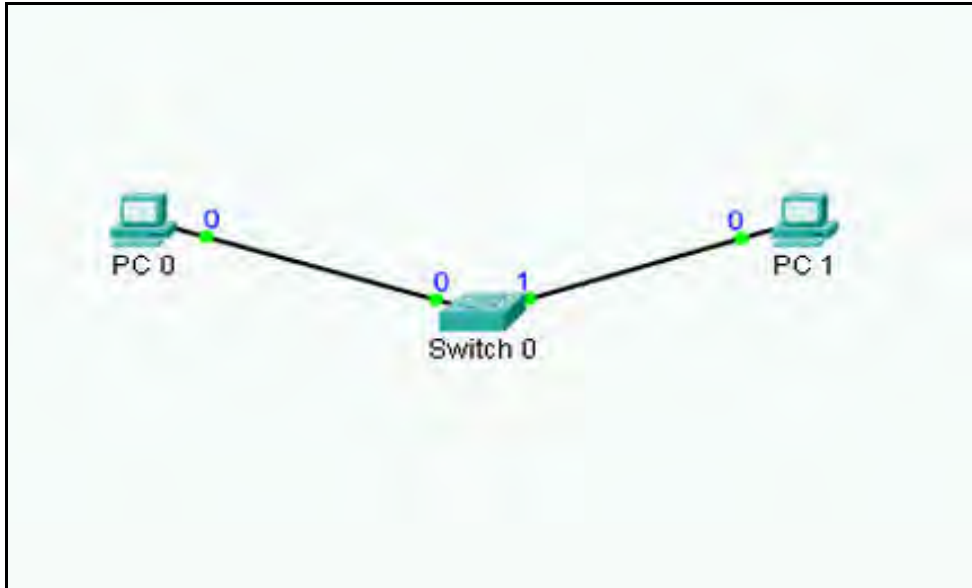
Play را بزنید تا شبیه سازی را دوباره مشاهده کنید. (هابها ترافیک را فیلتر نمی کنند.

آنها بسته را به هر ایستگاهی که به آنها متصل باشد ارسال می کنند)

یک بسته از PC0 به PC1 و ی: بسته از PC2 به PC0 اضافه کنید

روی Play کلیک کنید (بدلیل فیلتر نشدن ترافیک، تصادم رخ می دهد)

CCNA1-5.1.13b (ایجاد یک شبکه مبتنی بر سوئیچ



(اهداف)

ایجاد یک شبکه ساده بین دو رایانه شخصی با استفاده از سوئیچ

اعمال آدرس IP با ایستگاه ها

بررسی اتصال در توپولوژی شبیه سازی شده

(مرحله ۱)

توپولوژی نمایش داده شده در شکل فوق را ایجاد کنید

بعد از اتصال دستگاه ها، آدرس های IP را مطابق جدول زیر اعمال کنید

Computer	IP Address	Subnet mask
PC – 0	192.168.1.1	255.255.255.0
PC – 1	192.168.1.2	255.255.255.0

(مرحله ۲)

یک بسته از PC0 به PC1 اضافه کنید

Play را کلیک کنید تا اتصال را بررسی کنید

روی سوئیچ کلیک کنید تا جدول MAC آنرا مشاهده کنید (آدرس های MAC مربوط به

PC0 و PC1 در جدول قرار دارند)



✓ ضمائم: شبیه سازی شبکه های کامپیوتری

مرحله ۳)

رایانه دیگری را اضافه کنید و آن را به سوئیچ متصل کنید. آدرس IP آن را 192.168.1.3 با ماسک شبکه 255.255.255.0 بگذارید.

Play را بزنید تا شبیه سازی را دوباره مشاهده کنید. (سوئیچ ها پورتهای را که وسیله مقصد به آن متصل است انتخاب می کنند. آنها بسته را فقط به سمت مقصد خودش ارسال می کنند)

روی سوئیچ کلیک کنید تا جدول MAC آن را مجددا مشاهده کنید. آدرس MAC مربوط به PC2 نیز اکنون در جدول قرار دارد.

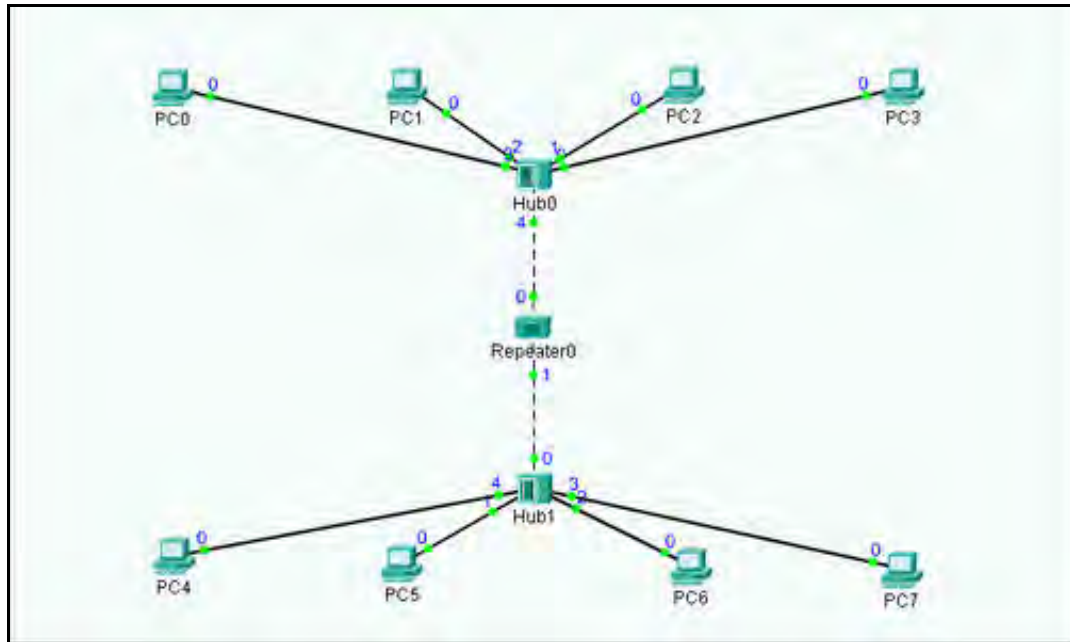
مرحله ۴)

یک بسته از PC0 به PC1 و از PC1 به PC2 و از PC2 به PC0 اضافه کنید

روی Play کلیک کنید

تصادم رخ نمی دهد. حتی اگر همه PC ها همزمان بسته ارسال کنند. به این دلیل که سوئیچ ها تصادم را با ایجاد بخش های مختلف از بین می برند.

CCNA1-5.1.5-5.1.7 (تکرار کننده ها و هاب ها



(توضیح)

این توپولوژی شامل ۸ میزبان است که از طریق ۲ هاب و یک تکرار کننده تشکیل شبکه داده اند

(رویه ها)

در حالت توپولوژی، ۳ تکرار کننده بیشتر بین دو هاب اضافه کنید
 در حالت شبیه سازی، یک سناریوی جدید بسازید
 یک بسته از PC4 به PC0 و از PC5 به PC1 در زمان های مختلف ارسال کنید به طوری
 که تصادم اتفاق نیفتد.
 قبل از اجرای شبیه سازی، روی بسته مربوط به PC4 و PC5 کلیک کنید تا اطلاعات
 بسته و OSI را مشاهده کنید. سپس شبیه سازی را اجرا کنید
 بعد از اولین شبیه سازی، مرحله ۳ را تکرار کنید ولی بگونه ای که این بار تصادم اتفاق
 بیفتد. سپس مرحله ۴ را تکرار کنید



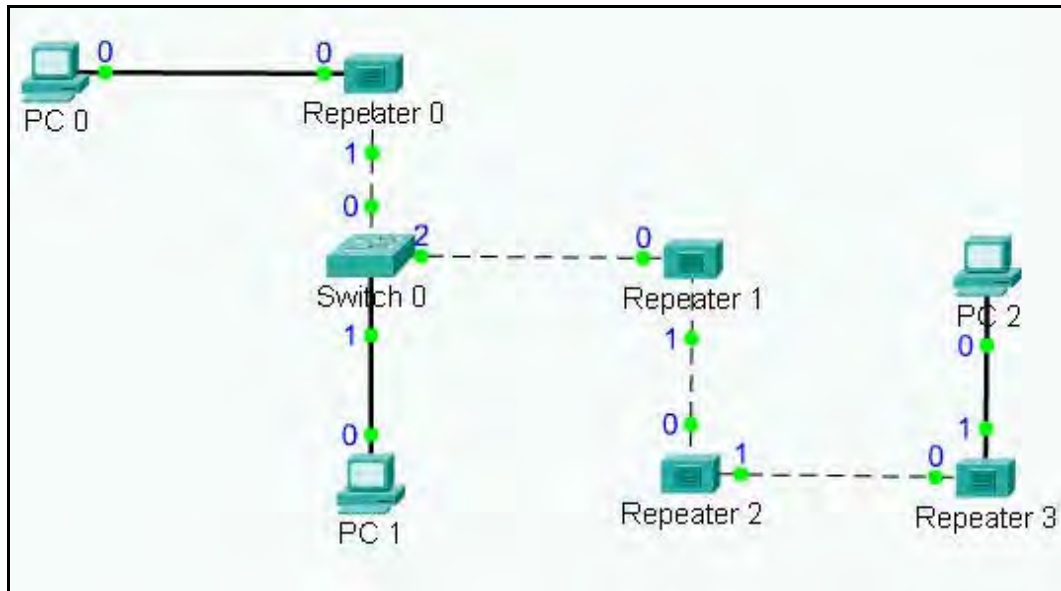
✓ ضمائم: شبیه سازی شبکه های کامپیوتری

سئوالات)

هدف از هاب و تکرار کننده در این شبکه چیست؟

از چه وسیله ای برای اتصال میزبان ها به هاب ها و تکرار کننده ها به هاب ها استفاده شده است؟

این شبکه شامل چه تعداد حوزه تصادم می باشد؟

CCNA1-5.1.6 (تکرار کننده

(اهداف)

ایجاد یک توپولوژی شبکه شبیه سازی شده

اعمال آدرس IP به ایستگاه ها

آشنا شدن با عملکرد یک تکرار کننده

فهمیدن قانون ۴ تکرار کننده

آزمایش توپولوژی شبکه سازی شده

(مرحله ۱)

توپولوژی نمایش داده شده در شکل فوق را ایجاد کنید. بعد از اتصال همه دستگاه ها، به آنها آدرس IP معتبر با ماسک زیر شبکه بدهید.

(مرحله ۲)

روی برگه Simulation کلیک کنید.

یک بسته از PC0 به PC1 ایجاد کنید. بسته دیگری از PC1 به PC2 ایجاد کنید.

Play را کلیک کنید



✓ ضمائم: شبیه سازی شبکه های کامپیوتری

به زمان طی شده برای رسیدن بسته به مقصد دقت کنید. (تکرار کننده های بیشتر بین ایستگاه ها تاخیر بیشتری را سبب می شوند)

مرحله ۳)

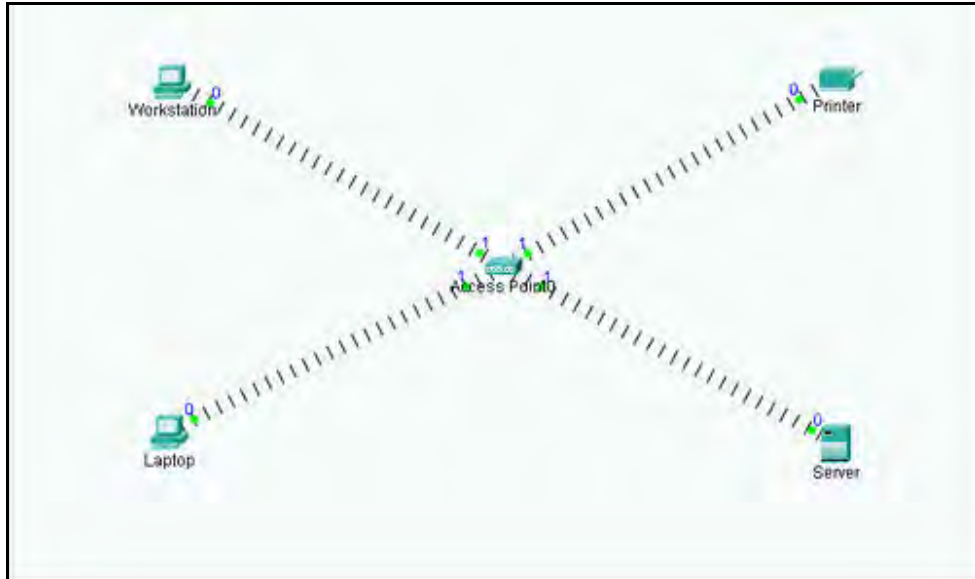
یک مرحله به عقب برگردید

بسته ای را از PC2 به PC1 اضافه کنید

یک اتصال را حذف کنید و تکرار کننده دیگری را هرجایی بین switch0 و PC2 قرار

دهید. مجدداً دستگاه ها را به هم متصل کنید

روی Simulation کلیک کنید و Play را بزنید. (تاخیر منجر به تصادم می شود)

CCNA1-5.1.8 (بی سیم

(توضیح)

این توپولوژی شامل یک ایستگاه کاری، یک لپ تاپ، یک سرور، یک چاپگر و یک access point می باشد. کل شبکه بی سیم است.

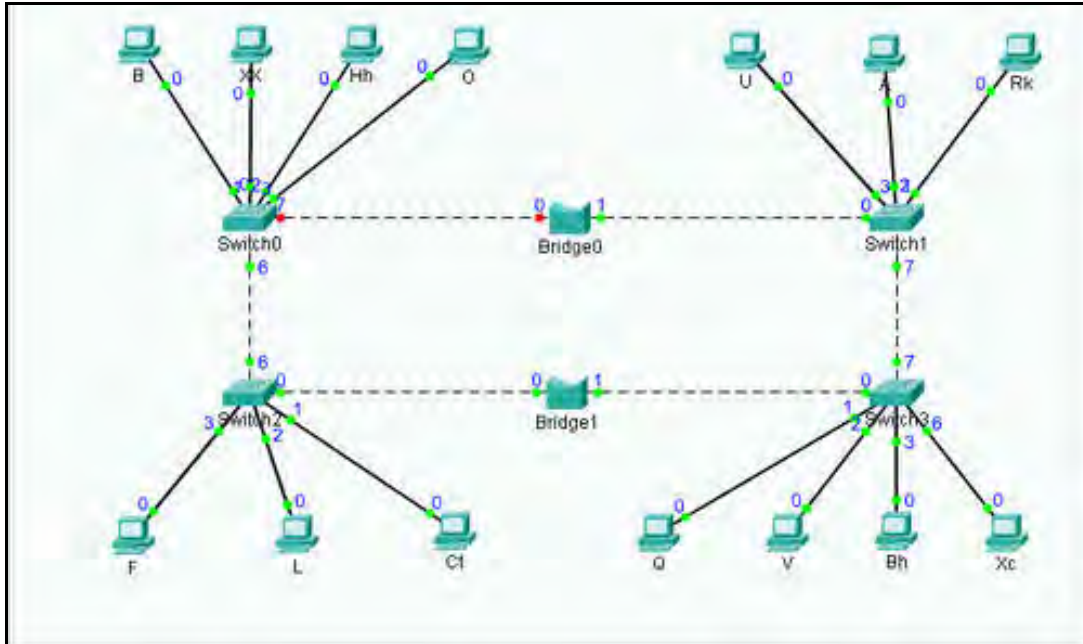
(رویه ها)

سناریوی ۲ را در حالت Simulation مرور کنید.
توجه کنید که دستگاه های متصل به هم متوجه بروز تصادم نمی شوند.
چه اتفاقی می افتد اگر دستگاه ها مداوم برای هم بسته ارسال کنند؟

(سئالات)

اتصالات بی سیم ظرفیت چه نوع سیگنال هایی را دارند؟
تفاوت و تشابه access point با دیگر دستگاه ها نظیر hub یا switch چیست؟
چه موضوعات امنیتی در اتصال بی سیم وجود دارد؟
مزیت اتصال بی سیم نسبت به اتصال سیمی و برعکس چیست؟

CCNA1-5.1.9-5.1.10 (پل ها و سوئیچ ها)



(توضیح)

این توپولوژی شامل ۱۴ میزبان است که توسط ۴ سوئیچ و ۲ پل به هم متصل شده اند.

(رویه ها)

در حالت توپولوژی، پورت ۶ از نوع Fast Ethernet در switch0 غیرفعال است. در نتیجه اتصال بین switch0 و Bridge0 قطع است.

هنوز در حالت توپولوژی، روی Switch0 کلیک کنید و سپس روی Fast Ethernet port 6 کلیک کنید. آنرا فعال کنید.

به حالت Simulation بروید. اتصال فعال شده خودش غیرفعال می شود. علت آن حلقه ایجاد شده در توپولوژی است و درخت پوشای پروتکل از این حلقه جلوگیری می کند.

یک بسته از میزبان Xc به میزبان XX ارسال کنید. مسیری که بسته طی می کند را بررسی کنید. با توجه به این که اتصال بین switch0 و bridge0 غیرفعال است، switch3 مجبور است بسته را به bridge1 ارسال کند تا سپس به switch2 و پس از آن به switch0 ارسال شود و به میزبان XX برسد.



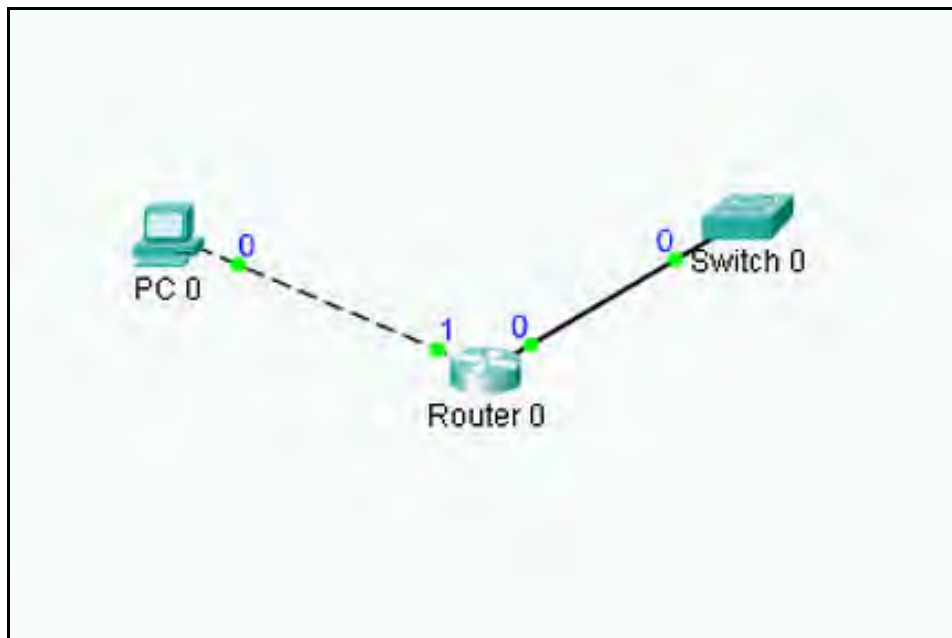
✓ ضمائم: شبیه سازی شبکه های کامپیوتری

دو پل را حذف کنید و یک اتصال بین دو شبکه جدا شده ایجاد کنید به طوریکه بسته ها بتوانند از طریق آن ارسال شوند.

سئوالات)

- هدف از پل و سوئیچ در این توپولوژی چیست؟
- سوئیچ و پل در کدام لایه از OSI کار می کنند؟
- مزایای استفاده از پل و سوئیچ در مقایسه با هاب و تکرار کننده چیست؟
- این شبکه شامل چه تعداد حوزه تصادم است؟

CCNA1-5.2.3a) اتصال واسط های مسیریاب ها



اهداف)

شناختن واسط های مختلف در مسیر یاب

شناختن کابل های صحیح برای اتصال به دستگاه های LAN

مرحله ۱)

توپولوژی نمایش داده شده در بالا را ایجاد کنید

اتصال بین مسیریاب و PC و بین مسیریاب و سوئیچ متفاوت است. اتصال مسیریاب به

سوئیچ با کابل straight است و اتصال بین مسیریاب و PC با کابل کراس است.

یک هاب اضافه کنید و آن را با کابل مستقیم به مسیریاب متصل کنید.

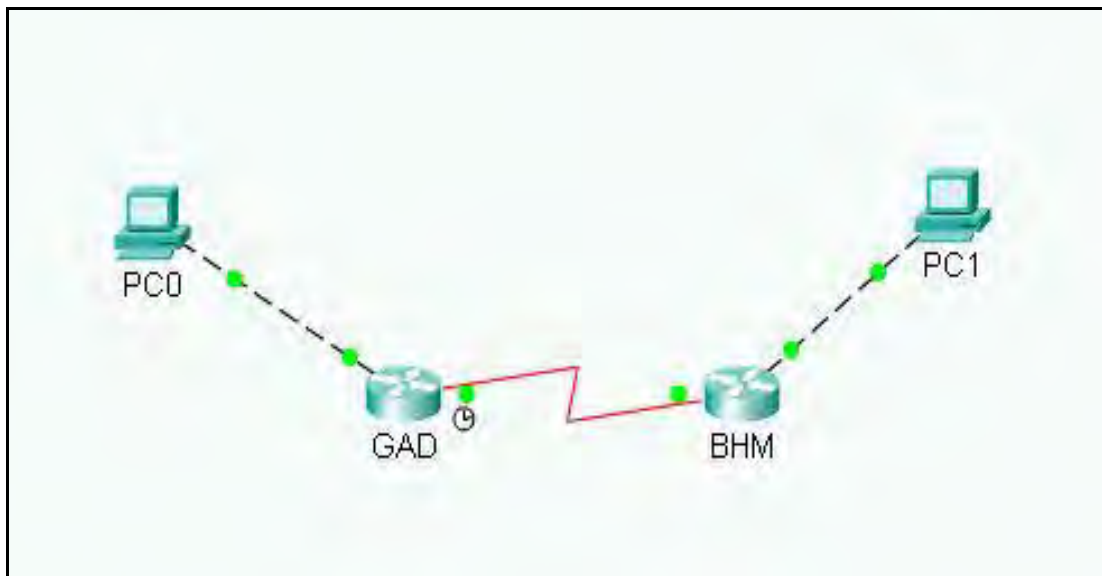
یک PC دیگر اضافه کنید و آن را با کابل مستقیم به هاب متصل کنید.

یک مسیر یاب دیگر اضافه کنید و آنرا با کابل سریال به Router0 متصل کنید.

روی مسیریاب کلیک کنید و به واسط های پورت آن نگاه کنید. ۰ و ۱ پورت های اترنت

هستند، ۲ و ۳ پورت های سریال هستند، ۴ و ۵ پورت های فیبر نوری هستند.

CCNA2-4.2.6) رفع اشکال مربوط به آدرس IP



(اهداف)

پیکربندی دو مسیریاب و دو ایستگاه کاری در یک WAN کوچک
عیب زدایی مشکلات بوجود آمده در اثر پیکربندی نادرست

(مرحله ۱)

حالت Simple و Auto DHCP را غیرفعال کنید

حالت Console و Auto DHCP را فعال کنید

یک بخش terminal به مسیریاب باز کنید و با اجرای دستور show running-config
پیکربندی های هر کدام از مسیریاب ها را بررسی کنید. اگر صحیح نیست، اشکالات آنها
را حل کنید.

(مرحله ۲)

موارد زیر تنظیمات میزبان متصل به GAD Router است:

IP Address	192.168.14.2
IP subnet mask	255.255.255.0
Default gateway	192.168.15.1



✓ ضمائم: شبیه سازی شبکه های کامپیوتری

موارد زیر تنظیمات میزبان متصل به BHM Router است:

IP Address	192.168.16.2
IP subnet mask	255.255.255.0
Default gateway	192.168.15.2

مرحله ۳)

وارد حالت Simulation شوید

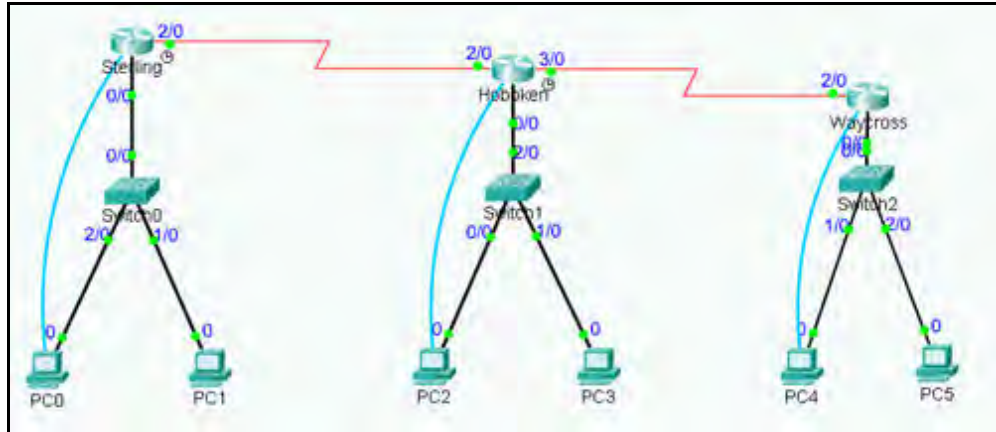
یک بسته از هر کدام از میزبان ها به مسیر یاب متصل به آنها ارسال کنید. چه اتفاقی برای بسته ها می افتد؟

دو مشکل در تنظیمات وجود دارد. تنظیمات را اصلاح کنید تا بسته ها بتوانند به مقصد برسند.

مشکل اول چیست؟

مشکل دوم چیست؟

۶.۱.۳-۶.۱.۴ (CCNA2-6.1.3-6.1.4) پیکربندی مسیرهای پیشفرض و استاتیک



(اهداف)

پیکربندی استاتیک و پیش فرض مسیرهای بین مسیریاب ها برای این که تبادل داده بین مسیریاب ها با پروتکل های پویا انجام نشود
آدرس های IP و Subnet mask هر دستگاه از قبل اعمال شده است.

(مرحله ۱)

در حالت Simulation، یک بسته از PC0 به PC2 ارسال کنید. دقت کنید که مسیریاب Sterling نمی تواند بسته را به گام بعدی ارسال کند.

(مرحله ۲)

در حالی که در حالت Simulation هستید، یک بخش terminal برای هر مسیریاب باز کنید. جدول مسیریابی هر روتر را با دستور Show ip route مشاهده کنید. دقت کنید که مسیری به شبکه های دیگر تعریف نشده است

(مرحله ۳)

یک بخش terminal برای مسیریاب sterling باز کنید.
وارد حالت global configuration شوید و مسیرهای استاتیک زیر را وارد کنید:

```
ip route 172.16.3.0 255.255.255.0 172.16.2.2
ip route 172.16.5.0 255.255.255.0 172.16.2.2
```



✓ ضمائم: شبیه سازی شبکه های کامپیوتری

```
ip route 0.0.0.0 0.0.0.0 172.16.2.2
```

در حالت privileged exec ، دستور copy run start را وارد کنید تا تنظیمات در startup ذخیره شود.

یک بخش terminal به مسیر یاب Hoboken باز کنید.

وارد حالت global configuration شوید و مسیرهای استاتیک زیر را وارد کنید:

```
ip route 172.16.1.0 255.255.255.0 172.16.2.1
```

```
ip route 172.16.5.0 255.255.255.0 172.16.4.2
```

در حالت privileged exec ، دستور copy run start را وارد کنید تا تنظیمات در startup ذخیره شود.

یک بخش terminal به مسیر یاب Waycross باز کنید.

وارد حالت global configuration شوید و مسیرهای استاتیک زیر را وارد کنید:

```
ip route 172.16.1.0 255.255.255.0 172.16.4.1
```

```
ip route 172.16.3.0 255.255.255.0 172.16.4.1
```

```
ip route 0.0.0.0 0.0.0.0 172.16.4.1
```

در حالت privileged exec ، دستور copy run start را وارد کنید تا تنظیمات در startup ذخیره شود.

مرحله (۴)

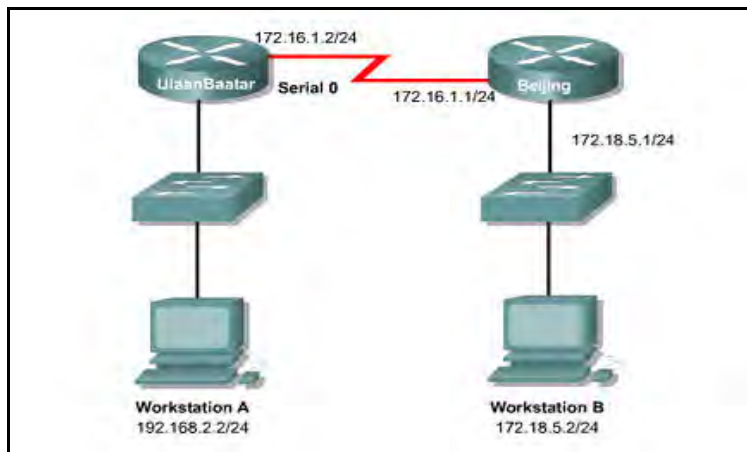
در حالی که در حالت Simulation هستید، یک بخش terminal به هر یک از مسیر یاب ها باز کنید. جداول مسیریابی را با دستور show ip route بررسی کنید. مسیرهای استاتیکی که در بالا وارد شدند باید در خروجی ظاهر شوند.

دستور Show running-config نیز مسیرهای استاتیک جدید را در خروجی نمایش خواهند داد.

مرحله (۵)

در حالت Simulation یک بسته از PC0 به PC2 ارسال کنید. بسته با موفقیت به PC2 ارسال خواهد شد.

CCNA2-6.3.2 (پیکربندی مسیریابی)



(اهداف)

پیکربندی مسیریاب ها برای شروع یک پردازش مسیریابی
افزودن شبکه هایی که انتشار می دهند

(مرحله ۱)

توپولوژی نشان داده شده در تصویر فوق را مجدداً ایجاد کنید. نیاز به تنظیم آدرس IP
برای این فعالیت وجود ندارد

(مرحله ۲)

روی مسیریاب Beijing کلیک کنید.

وارد حالت privileged exec شوید.

وارد حالت global configuration شوید

برای فرآیند مسیریابی RIP وارد حالت router configuration شوید.

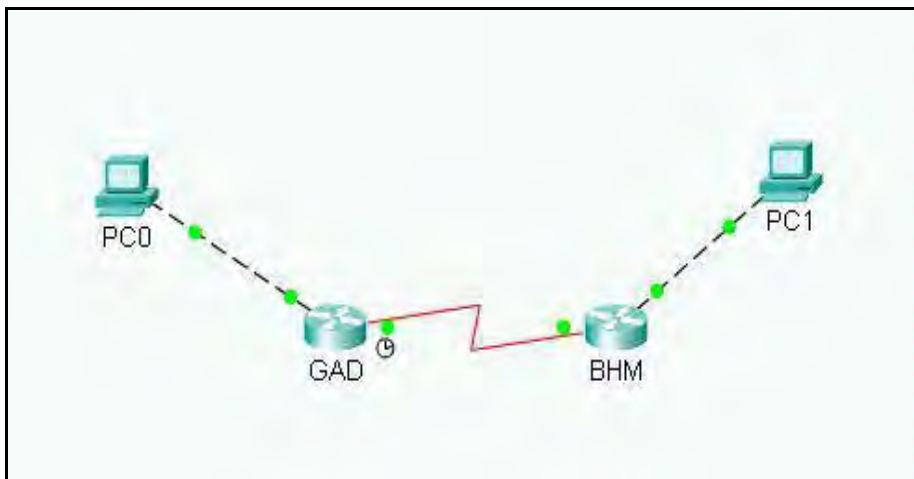
با استفاده از دستورات، شبکه های 172.16.0.0 و 172.18.0.0 را اضافه کنید.

با دستور exit به حالت privileged exec بروید.

برای مشاهده تنظیمات در حال اجرای فعلی Show run را اجرا کنید. شبکه های

172.16.0.0 و 172.18.0.0 باید نشان داده شوند.

RIP (CCNA2-7.2.2) پیکربندی



اهداف)

راه اندازی الگوی آدرس IP با استفاده از شبکه کلاس B
پیکربندی مسیریابی پویا با پروتکل RIP در مسیریاب ها

مرحله ۱)

یک بخش terminal به مسیریاب ها باز کنید و در حالت global configuration ، نام
میزبان ها را مطابق فوق تنظیم کنید.

مرحله ۲)

در حالت global configuration دستورات زیر را وارد کنید:

```

GAD(config)#router rip
GAD(config-router)#network 172.16.0.0
GAD(config-router)#network 172.17.0.0
GAD(config-router)#exit
GAD(config)#exit
  
```

```
GAD#copy running-config startup-config
```

مرحله ۳)

در حالت Global Configuration دستورات زیر را وارد کنید

```
BHM(config)#router rip
```




✓ ضمائم: شبیه سازی شبکه های کامپیوتری

```
BHM(config-router)#network 172.17.0.0
```

```
BHM(config-router)#network 172.18.0.0
```

```
BHM(config-router)#exit
```

```
BHM(config)#exit
```

```
BHM#copy running-config startup-config
```

(مرحله ۴)

میزبان ها را با آدرس IP صحیح، subnet mask و default gateway صحیح تنظیم کنید.

(مرحله ۵)

وارد حالت Simulation شوید

بسته ای را از یک میزبان به دیگری ایجاد کنید و جزئیات اطلاعات بسته را در هر مرحله

مشاهده کنید

(مرحله ۶)

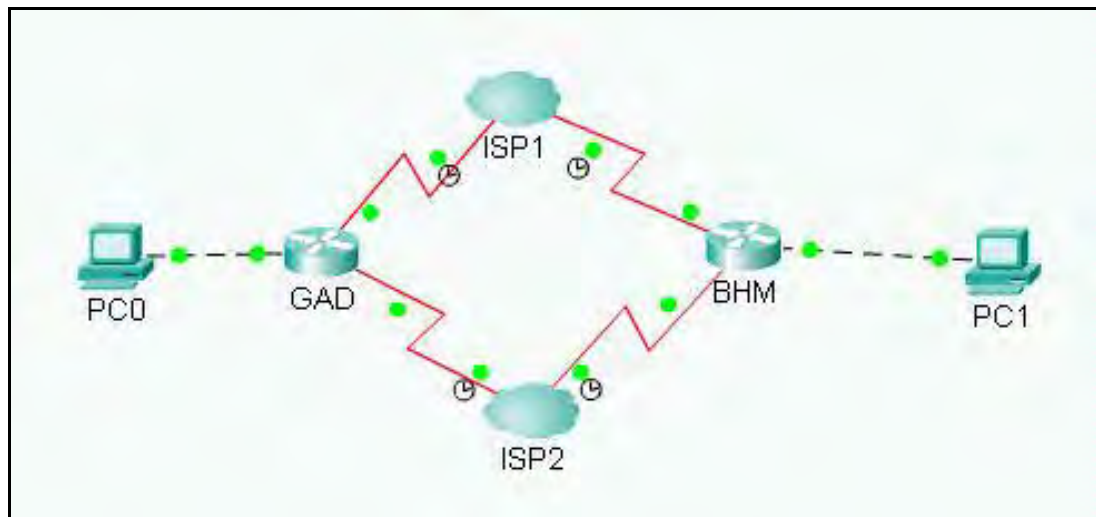
در حالت Simulation، پنجره terminal مسیریاب را باز کنید و جدول مسیریابی آن را

مشاهده کنید

آیتم های جدول مسیریابی GAD چه مواردی هستند؟

آیتم های جدول مسیریابی BHM چه مواردی هستند؟

CCNA2-7.2.9 (تعدیل بار بین چند مسیر (Load Balancing)



اهداف)

پیکربندی تعدیل بار بین چند مسیر
مشاهده روند تعدیل بار

مرحله ۱)

توپولوژی فوق را ایجاد کنید
آدرس های IP مسیریاب ها را بر اساس آدرس های ابرها تنظیم کنید.

مرحله ۲)

میزبان ها را با آدرس IP و subnet mask و default gateway صحیح پیکربندی کنید و
اتصال بین دو میزبان را آزمایش کنید.

مرحله ۳)

مسیریاب را بگونه ای پیکربندی کنید که به صورت per-packer بار را تعدیل کند. هر دو
واسط سریال باید از فرآیند switching استفاده کنند. این فرآیند مسیریاب را مجبور می
کند که شبکه مقصد هر بسته را در جدول مسیریابی جستجو کند. در مقابل fast-
switching که انتخاب پیش فرض است، جدول اولیه را در حافظه کش سریع ذخیره می
کند و از اطلاعات آن برای تعیین مسیر بسته ها به مقصد یکسان استفاده می کند



✓ ضمائم: شبیه سازی شبکه های کامپیوتری

فرآیند switching را در هر دو واسطه سریال فعال کنید:

GAD(config-if)# no ip route-cache

BHM(config-if)# no ip route-cache

مرحله ۴)

وارد حالت Simulation شوید

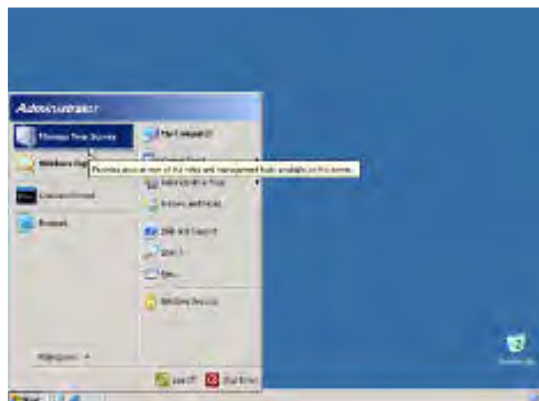
عملکرد تعدیل بار را به ازای هر بسته بررسی کنید. این کار را با ایجاد یک بسته از یک میزبان به میزبان دیگر انجام دهید. یک مرحله در خط زمانی جلو رفته و بسته دیگری با مبدا و مقصد مشابه ایجاد کنید.

روی play کلیک کنید تا مسیری که هر بسته طی می کند مشاهده کنید. آیا از مسیر مشابهی حرکت می کنند؟



✓ ضامئ: شبیه سازی شبکه های کامپیوتری

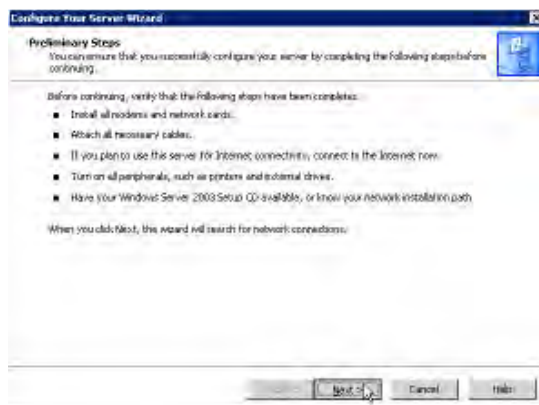
ضمیمه ۸- نصب DHCP Server



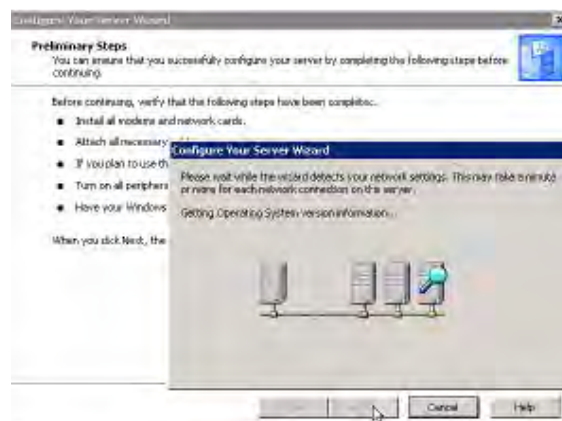
۱



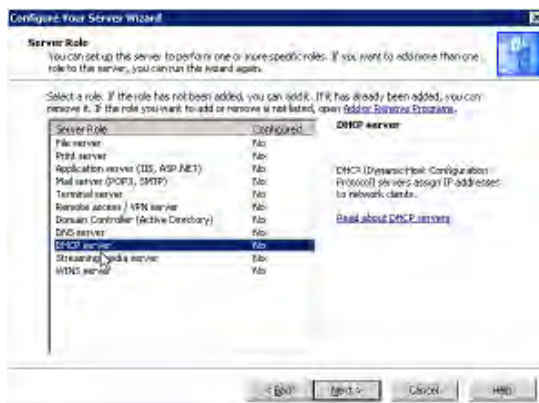
۲



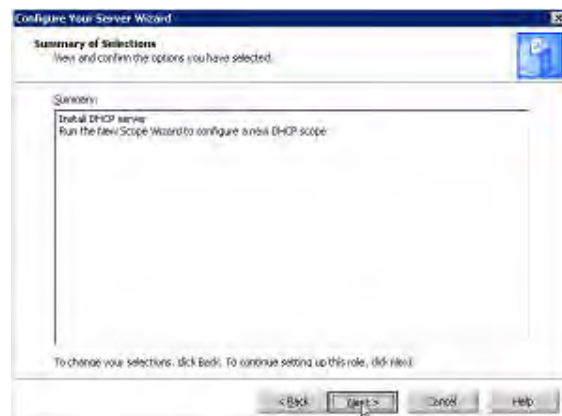
۳



۴



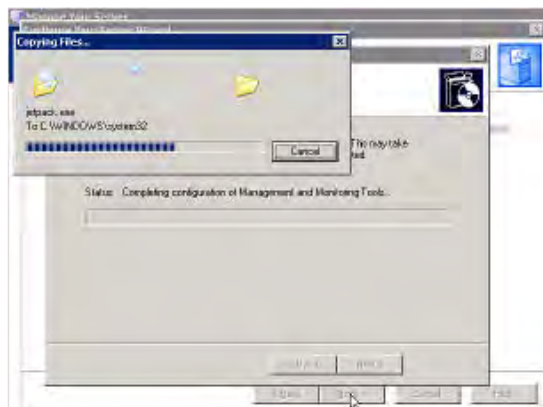
۵



۶



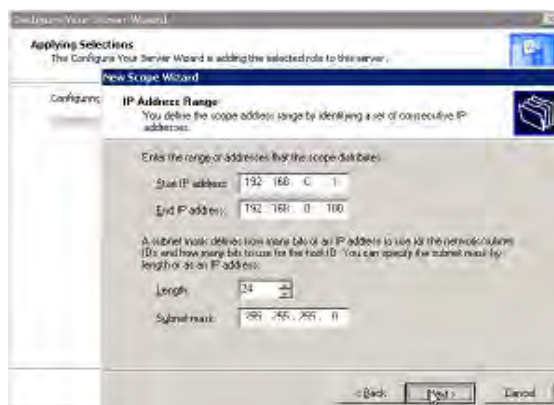
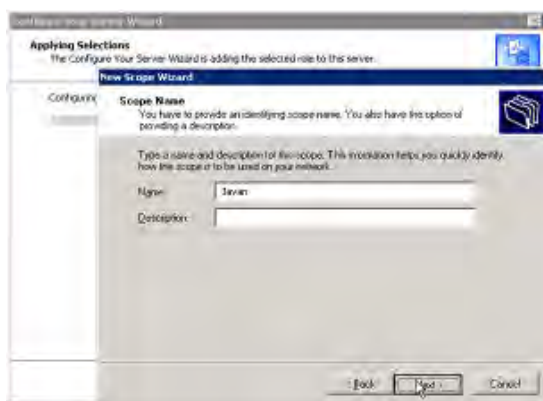
✓ ضوابط: شبیه سازی شبکه های کامپیوتری



۷



۸

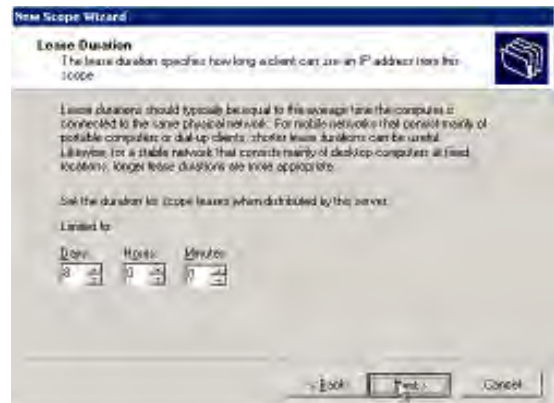


۹- تعیین محدوده آدرس IP کلاینت ها

۱۰- رزرو کردن برخی از آدرس های IP



۱۱



۱۲



✓ ضامئ: شبیه سازی شبکه های کامپیوتری



۱۳



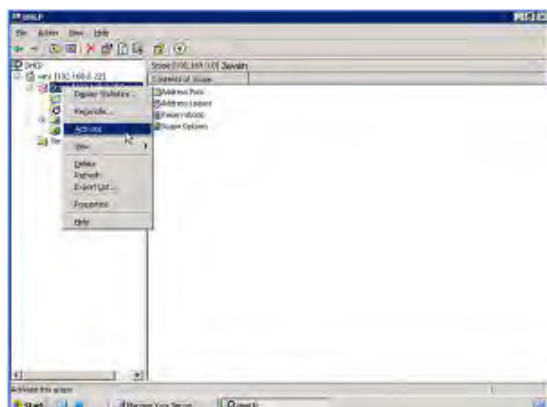
۱۴



۱۵



۱۶



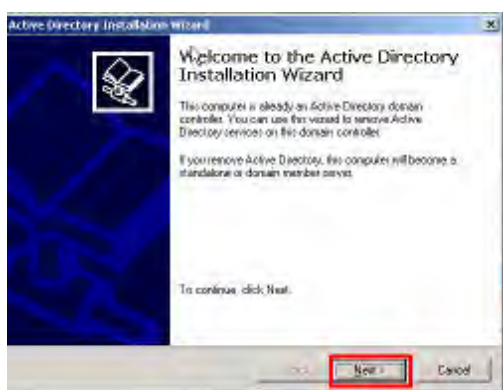
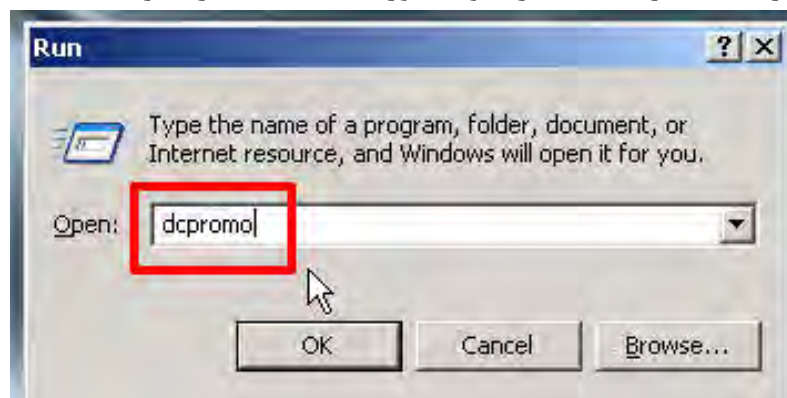
۱۷



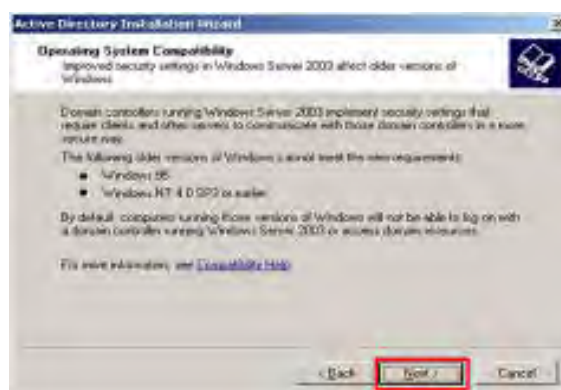
✓ ضوابط: شبیه سازی شبکه های کامپیوتری

ضمیمه ۹- راه اندازی Active Directory

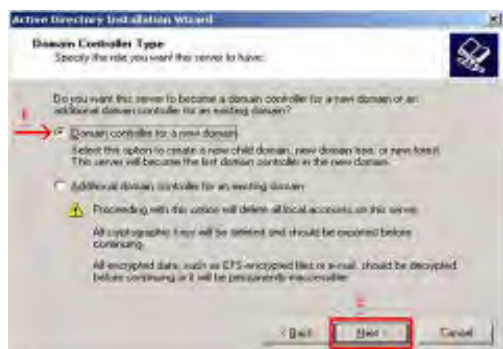
از منوی شروع گزینه Run را انتخاب کرده و دستور DCPROMO را اجرا کنید:



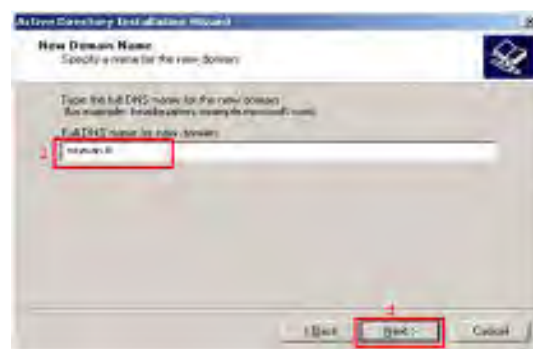
۱



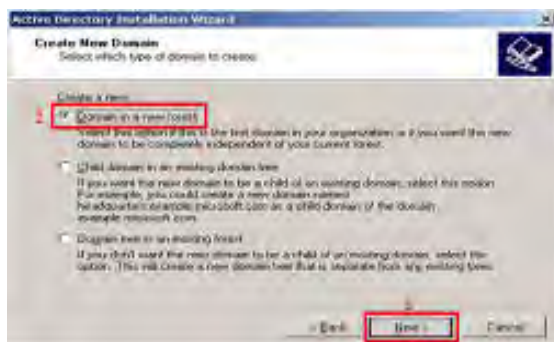
۲



۳- ساختن دامنه جدید یا اضافه کردن به
Domain موجود.



۴- وارد کردن نام دامنه جدید



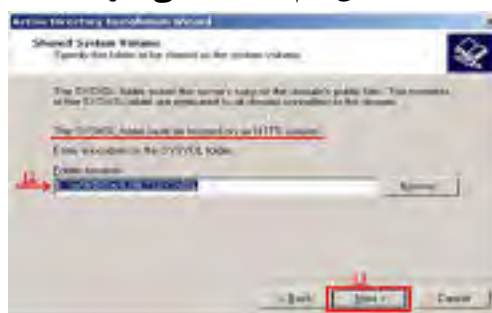
۵- تعیین نوع دامنه و چگونگی آن



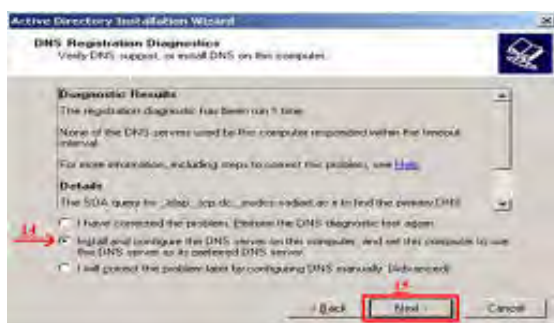
۶- تعیین نام NetBIOS. این نام برای اتصال کلاینت ها به دامین کاربرد دارد و دامین کنترلر ما با این نام شناخته می شود.



۷- تعیین محل ذخیره فایل ها اطلاعاتی و فایل log



۸- تعیین محل ذخیره فایل های سرور و دامنه های انتشار یافته (نوع پارتیشن حتما باید NTFS باشد). این پوشه توسط Active Directory به صورت share در می آید.



۹- بررسی پشتیبانی از DNS یا نصب DNS بر روی سیستم.

- گزینه اول: مشکل DNS حل شده است و

دوباره تست کن

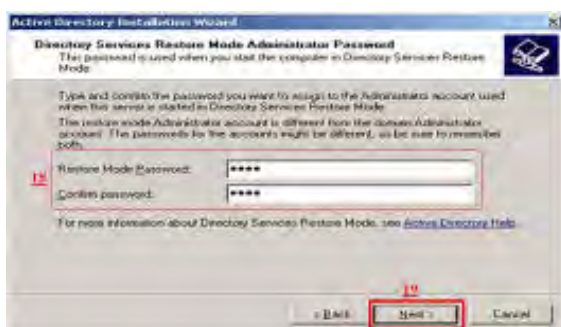
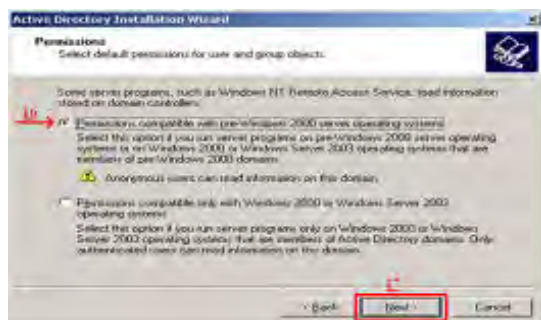
- گزینه دوم: DNS توسط Active

Directory نصب شود

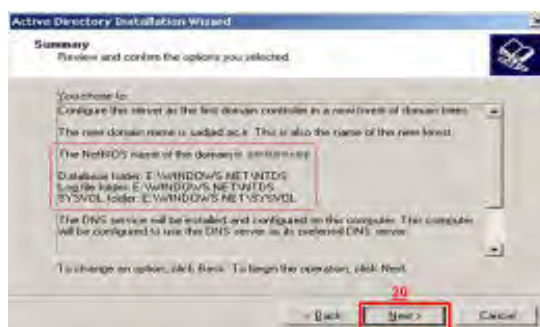
- گزینه سوم: بعدا به صورت دستی DNS

نصب می شود.

۱۰- تعیین نوع دسترسی در شبکه. این گزینه تعیین می کند که کلاینت های ما از چه نوع ویندوزی استفاده می کنند؟ (گزینه مشخص شده را برای سازگاری بیشتر انتخاب کنید)



۱۱- تعیین کلمه عبور مدیر سیستم



۱۲- بررسی نهایی پیکربندی و تنظیمات



۱۳- آغاز نصب و کپی کردن فایل های مربوط



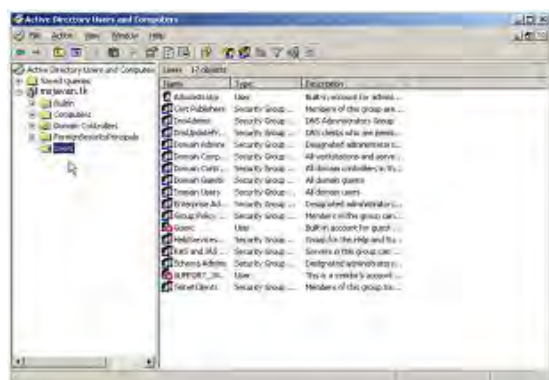
۱۴- پایان نصب بر روی این کامپیوتر

به Active Directory

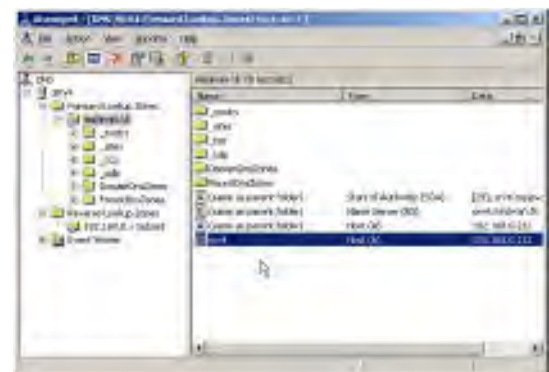




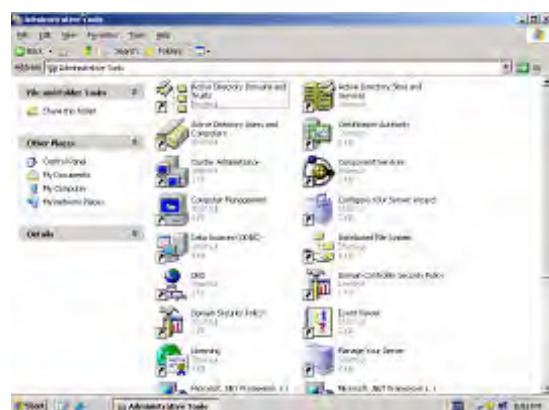
۱۶- پس از بالا آمدن مجدد سیستم، برای اطمینان از نصب شدن Active Directory به Administrative Tools مراجعه کنید و Active Directory User And Computer را اجرا کنید. یا از قسمت RUN دستور dsa.msc را اجرا کنید.



۱۷- به این ترتیب پنجره Active Directory Users and Computers ظاهر می شود



۱۸- برای این که بفهمید مراحل نصب به خوبی انجام شده باید بر روی سرور کلیک کنید. اگر پوشه هایی مثل شکل زیر بود یعنی مراحل نصب با موفقیت انجام شده در غیر اینصورت نصب به خوبی انجام نشده است.



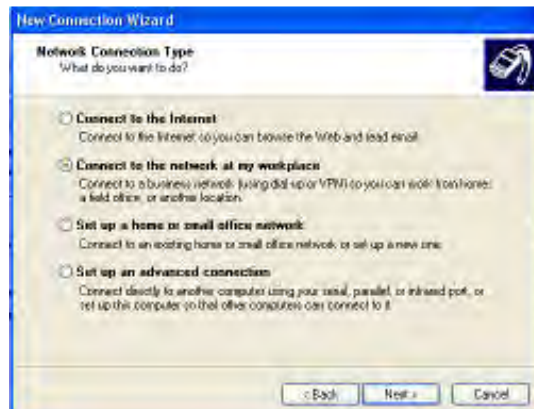
۱۹- در صورت نصب صحیح می توانید از کنترل پانل گزینه Administrative Tools را انتخاب کرده و با ابزارهایی که در اختیار دارید شبکه خود را کنترل کنید.

ضمیمه ۱۰- تنظیم ویندوز XP برای اتصال به VPN سرور

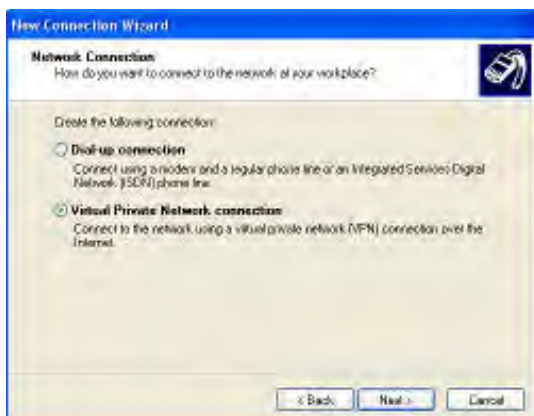
Click on New Connection Wizard .click Start | Control Panel | Network Connections



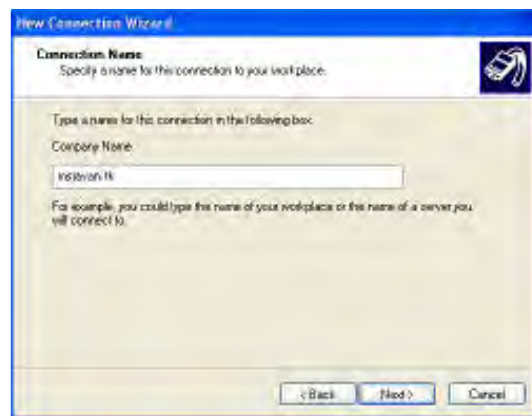
۱



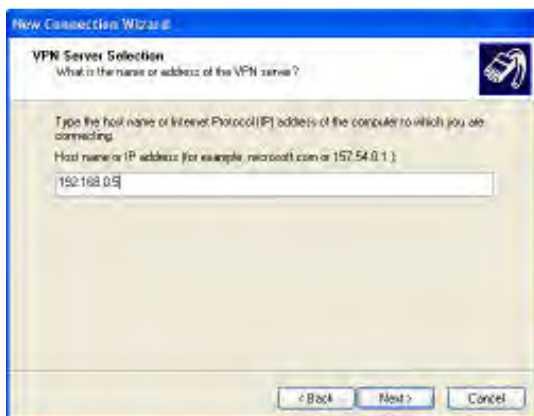
۲



۳



۴



۵- آدرس سرور VPN خود را وارد کنید



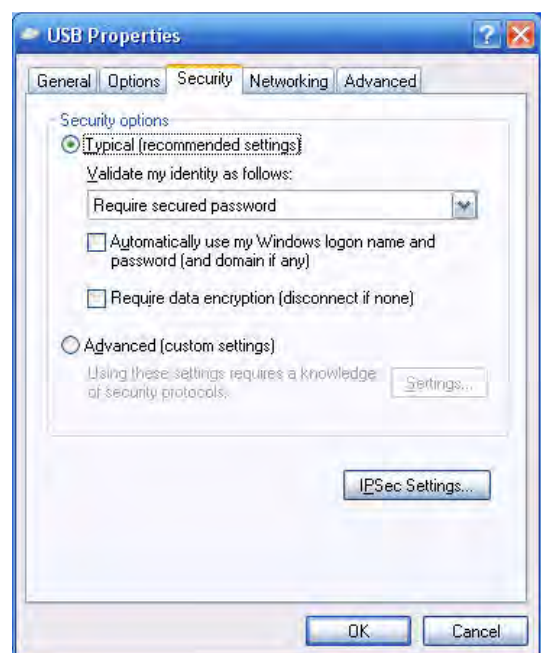
۶



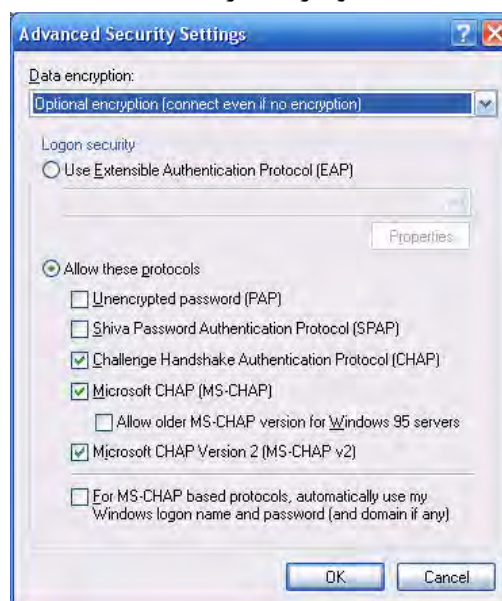
۷- نام کاربری و پسورد خود را وارد کنید



۸- از این قسمت هم می توانید آدرس سرور خود را تغییر دهید



۹



۱۰- تنظیمات امنیتی مناسب با تنظیمات سرور خود را در این قسمت به اجرا در آورید



مراجع:

- *Computer Networks, 4th Edition, Andrew S. Tanenbaum. 2003*
- *Computer Networks & Internets, 2nd Edition, Douglas E. Comer, 1999*
- *Packet Tracer 3.2 Totutorial, Cisco Systems, USA, 2004*
- *Packet Tracer 4.1 Totutorial, Networking Academic Program, Cisco Systems, USA, 2005*



✓ ضمائم: شبیه سازی شبکه های کامپیوتری
