آزمایشگاه های شبکه های کامپیوتری

امیر فرمانبر، بهروز رضاسروش، داوود کریم زادگان
اعضای هیئت علمی دانشگاه پیام نور

مقدمه مولفان

این کتاب چگونگی استفاده از بعضی تجهیزات و ابزارهای مورد استفاده در شبکه های کامپیوتری را بدون نیاز به تجربه شبکه بندی، آموزش می دهد. (البته داشتن یک پیش زمینه در شبکه های کامیوتری مفید خواهد بود.) کتاب با مفاهیم مقدماتی شروع شده شده است - مباحثي که بصورت پیش نیاز براي شروع راه اندازي شبکه مورد نیاز است، بطور اختصار توضیح داده شده است. - تا زمانیکه مطالعه ی این کتاب را به پایان برسانید، دارای دانش کافی برای استفاده و بهره گیری از تجهیزات شبکه بندی خواهید شد.
به نظر نگارندگان، کتوب فراوانی به تشریح تئوری شبکه های کامپیوتری پرداخته اند و دانشجویان و علاقمندان درس شبکه های کامپیوتری در قسمت کاربردی و عملی این درس، دچار کمبود منابع و کتوب می باشند. در این کتاب سعي شده است که مباحث مورد گفتگو در کلاس شبکه هاي کامپیوتري، بطور ساده، کاربردی و قابل درک توضیح داده شود. بر اساس سیاست هاي بکار گرفته شده در کلاس هايIT که دانشجو را تشویق به خودآموزي مي کند، پیشنهاد مي شود که این کتاب، تنها بعنوان منبعي جهت یادگیري اولیه استفاده شود و دانشجو خود نسبت به فراگیري کامل این مباحث اقدام نماید. یکی از عوامل مهم در تالیف و تدوین این کتاب، دانشجویان عزیز بوده اند. همچنین از زحمات اساتید بزرگواری که مستقیم یا غیر مستقیم از محضرشان بهره برده ایم، بی نهایت تشکر می کنم.

تقدیم به ساحت مقدس امام زمان (عج)

با احترام
امیر فرمانبر
بهروز رضاسروش
داوود کریم زادگان
طهران-1389

2-1- سرفصل مطالب مطرح شده

مبحث اول: آشنايي با تجهيزات ايجاد شبكه محلي و ابزارهاي تست شبكه

- تعداد جلسات مورد نياز : 1 جلسه
- پيش نياز تئوري: مفاهيم پايه اي در لايه هاي فيزيكی و Data link ، اترنت
- مطالب تئوري
  - ياد آوري انواع توپولوژيهاي محلي
    - BUS، STAR، MESH، RING
  - رسانه ها
    - رسانه با سيم
      - انواع كابلها(CAT5، CAT6، COAX، Fiber) و استفاده هريک در توپولوژيهاي فوق
      - استاندارد و انواع كابلهاي فوق
    - رسانه بيسيم و استانداردهاي آن
- دستور كار عملي آزمايشگاه
  - آشنايي با RJ45 TESTER، RJ11 و BNC.
  - آشنايي با RJ45 CRIMP Tool.
  - ايجاد كابل CAT5 بصورت مستقيم و Cross با توجه به استاندارد EIA/TIA 568B.
  - كار با Wireless Access Point
  - اين جلسه گزارش كتبي ندارد.
- ارزيابي دانشجويان
  - ارزيابي دانشجويان بر اساس كار عملي صورت گرفته در كلاس انجام مي شود، هر گروه 2 يا 3 نفره يک كابل مستقيم يا Cross ايجاد ميكند، كه مربي آن را با Tester تست كرده و نمره مي دهد.
- تجهيزات مورد نياز

- نمونه اي از انواع كابلها، فيبر نوري، سوكتها و تجهيزات ايجاد شبكه هاي محلي شامل هاب و سوييچ
- آچار RJ-45 جهت كابل زني و Tester (به تعداد گروهها)
- كابل CAT5 و سوكت(متناسب با تعداد گروهها)

مبحث دوم: آشنايي با TCP/IP و نحوه پيكربندي آن در سيستم عامل ويندوز

- تعداد جلسات مورد نياز : 1 جلسه
- پيش نياز تئوري: مفاهيم پروتكلهاي TCP و IP ، آشنايي با سيستم عامل ويندوز و پيكربندي آن
- مطالب تئوري
  - معرفي اجمالي مدل 4 لايه TCP/IP و وظيفه هر لايه.
  - پروتكلهاي پركاربرد در هر لايه. (CSMA-CD، ARP، DHCP، IP، TCPو UDP، HTTP، FTP و...)
  - معرفي آدرسهاي IP، آدرسهاي IP اختصاصي و روش آدرس دهي CIDR.
  - مفاهيم Subnet Mask و Default Gateway.
  - پيكربندي TCP/IP در سيستم عامل ويندوز.
  - ابزارها و نرم افزارهاي استاندارد TCP/IP موجود در ويندوز(ping، tracert، route، ipconfig، netstat، arp، telnet)
  - معرفي ابزار Ethearea‌l.
- دستور كار عملي آزمايشگاه
  - نصب كارت شبكه و درايور آن و راه اندازي TCP/IP.
  - هر گروه دو سيستم ويندوز را پيكربندي TCP/IP كرده و با استفاده از كابل Cross به هم مرتبط مي نمايد.

- با استفاده از دستور ipconfig خروجي پيكربندي IP مشخص مي شود.
- با استفاده از ابزار ping ارتباط اين دو سيستم تست مي شود. خروجي ping در هريک از حالات زير بررسي مي شود:
  - غير فعال بودن كارت شبكه و يا پروتكل TCP/IP.
  - قطع كابل.
  - عدم پيكربندي مناسب.(دو سيستم NETID مشترک نداشته باشند)
  - ping به يک آدرس IP كه در شبكه موجود نيست.
- با استفاده از دستور arp ، arp table سيستم مشخص مي شود و از ساير امكانات اين ابزار استفاده مي شود.
- **گزارش كار**
  - با استفاده از دستور Ipconfig پيكربندي TCP/IP سيستم خود را مشخص نماييد.
  - با استفاده از ابزار ping ارتباط سيستم خود با يک سيستم ديگر را كنترل نماييد. (10 بسته ICMP بطول هركدام 64 بايت)
  - با استفاده از ابزار netstat كليه پورتهاي TCP كه در سيستم شما در حالت Listen قرار دارد، مشخص نماييد.
  - با استفاده از دستور arp جدول arp سيستم خود را مشخص نماييد. چگونه مي توان محتويات اين جدول را پاک نمود؟
  - Etherreal را اجرا نماييد.
    - بسته هاي HTTP REQ وHTTP RESP را مشخص نماييد.(تكميل شود)
    - در لايه كاربرد موارد زير را مشخص نماييد.

- در لايه انتقال موارد زير را مشخص نماييد.
- در لايه اينترنت موارد زير را مشخص كنيد.
- در لايه Network Interface موارد زير را مشخص نماييد.
- طول كل بسته Request و بستهResponse .
- طول header هر لايه.

- با استفاده از ابزار ethereal كليه فريمهاي مبادله شده بين سيستم دانشجو و يكي از سرويس دهنده هاي موجود در دانشكده استخراج شده و با توجه به RFC826 مورد بررسي و تجزيه و تحليل قرار مي گيرد.

o ارزيابي دانشجويان

- ارزيابي دانشجويان بر اساس فعاليت در كلاس و همچنين گزارش دستور كار صورت مي گيرد.

o تجهيزات و نرم افزارهاي مورد نياز

- هر گروه دو سيستم(يك سيستم براي انجام آزمايش، يك سيستم جهت گزارش نويسي و جستجو بر روي اينترنت)
- كليه سيستم هاي موجود در آزمايشگاه مي بايست داراي مشخصات ذيل باشند:
  - حداقل دو كارت شبكه بر روي هر سيستم
  - داراي سيستم عاملهاي Windows 2000 Server يا بالاتر، Windows XP و Linux .
  - كابل Cross
  - نرم افزار Ethereal بر روي كليه سيستم عاملها

- مجـوز Admin بـراي كليـه گروههـا مـورد نيـاز است

مبحث سـوم: آشـنايي بـا TCP/IP و نحـوه پيكربنـدي آن در سيسـتم عامل لينوكس

- همانند جلسه دوم
- تعداد جلسات مورد نياز : 1 جلسه
- پـيش نيـاز تئـوري: مفـاهيم پروتكلهـاي TCP و IP ، آشـنايي بـا سيستم عامل لينوكس و پيكربندي آن

مبحث چهارم: آشنايي با سرويس‌هاي لايه كاربرد و نحـوه پيكربنـدي آن در سيستم عامل ويندوز(DNS Server, DHCP Server, Web Server, Terminal Service)

- تعداد جلسات مورد نياز: 2 جلسه
- پيش نياز تئوري: مفاهيم DNS، DHCP ، HTTP و ساير پروتكلهـاي مهم در لايه كاربرد
- مطالب ارائه شده و كليات دستور كار
  - DNS
    - معرفـي سـاختار DNS (مفـاهيم Zone، Domain، DomainName و...)
    - نحـوه نصـب سـرويس DNS بـر روي سيسـتم عامـل ويندوز
    - آناليز ترافيك توسط نرم افزار Ethereal
    - تست DNS راه اندازي شده توسط دستور nslookup
  - DHCP
    - معرفي پروتكل DHCP، كاربردها و قابليتهاي آن
    - نحوه نصب و راه اندازي سـرويس DHCP در سيسـتم عامل ويندوز
    - آناليز ترافيك توسط نرم افزار Ethereal
    - تست DHCP راه اندازي شده

- Terminal Service
  - معرفي كلي سرويسها و نرم افزارهاي Remote Management
  - معرفي سرويس Terminal در ويندوز و نحوه نصب و پيكربندي آن
  - تست Terminal Service راه اندازي شده
  - آناليز ترافيك توسط نرم افزار Ethereal
- Web Server
  - معرفي پروتكل HTTP و نحوه عملكرد آن
  - معرفي سرويس IIS در سيستم عامل ويندوز و نحوه نصب و پيكربندي آن
  - تست Web Server راه اندازي شده
  - آناليز ترافيك توسط نرم افزار Ethereal
- تجهيزات و نرم افزارها
  - CD سيستم عاملها(ويندوز 2000 و لينوكس)

مبحث پنجم: آشنايي با مسيريابي و پروتكلهاي مربوط به آن

- تعداد جلسات مورد نياز: 2 جلسه
- پيش نياز تئوري: مفاهيم IP Routing ، Sub netting، CIDR، IP Address Lookup
- مطالب ارائه شده و كليات دستور كار
  - پروتكلهاي مسيريابي
  - مفاهيم Routing Table، Forwarding Table
  - CIDR
  - راه اندازي يك شبكه اينترنت فرضي شامل دو شبكه محلي و تعدادي مسيرياب مياني با استفاده از سيستم عامل ويندوز و لينوكس به عنوان مسيرياب
  - پيكربندي ايستاي جداول مسيريابي
  - تست ارتباطات گام به گام و انتها به انتها

- تست مسيريابي با استفاده ازدستورات Ping و Traceroute

- سخت افزار و نرم افزارهاي مورد نياز
  - نرم افزار Microsoft Visio
  - CD سيستم عاملها

مبحث ششم: آشنايي با مسيريابهاي سخت افزاري (Cisco)

- تعداد جلسات مورد نياز: 2 جلسه
- پيش نياز تئوري: مفاهيم IP Routing ، Sub netting، CIDR، IP Address Lookup
- مطالب ارائه شده و كليات دستور كار
  - مزيت اين نوع مسيريابها نسبت به انواع نرم افزاري
  - آشنايي با سخت افزار، انواع حافظه اين نوع مسيريابها
  - نرم افزارهاي مورد استفاده در مسيريابها
  - نحوه پيكربندي مسيرياب
  - راه اندازي يك شبكه اينترنت فرضي شامل دو شبكه محلي و تعدادي مسيرياب ميداني با استفاده از مسيريابهاي Cisco
  - پيكربندي ايستاي جداول مسيريابي
  - تست ارتباطات گام به گام و انتها به انتها
  - تست مسيريابي با استفاده ازدستورات Ping و Traceroute

- سخت افزار و نرم افزارهاي مورد نياز
  - مسيرياب Cisco 3 دستگاه (هر دو گروه يك مسيرياب)
  - كابل Console جهت پيكربندي مسيريابها

مبحث هفتم: معرفي پروژه برنامه نويسي و پروتكل مورد استفاده در آن

در اين جلسه با توجه به موضوع پروژه مطرح شده براي دانشجويان، نحوه انجام پروژه، پروتكل مورد استفاده در آن و Socket Programming بطور كلي براي دانشجويان مطرح مي‌شود تا دانشجويان براي انجام پروژه آمادگي كسب كنند.

- تعداد جلسات مورد نياز: 1 جلسه

مبحث هشتم: مفاهيم پيشرفته در شبكه هاي كامپيوتري

- تعداد جلسات مورد نياز: 2 جلسه
- پيش نياز تئوري: مفاهيم NAT، VPN و فايروال
- مطالب ارائه شده و كليات دستور كار
  - NAT
    - آشنايي با مفهوم NAT
    - راه اندازي NAT در سيستم عامل ويندوز و يا لينوكس
    - آناليز ترافيك در دروازه NAT
  - VPN
    - آشنايي با مفهوم VPN
    - راه اندازي يك VPN در سيستم عامل ويندوز و يا لينوكس
    - آناليز ترافيك VPN
  - Firewall
    - آشنايي با مفهوم Firewall
    - راه اندازي و پيكربندي IPtables در سيستم عامل لينوكس

پروژه‌هاي آزمايشگاه

پروژه‌هاي پيشنهادي شامل موارد ذيل است:

HTTP Server

متن کامل پروژه در ضمیمه آمده است.

FTP Server

متن کامل پروژه در ضمیمه آمده است.

دستور كار جلسه اول

آشنايي با تجهيزات ايجاد شبكه محلي و ابزارهاي تست شبكه

دانشجوي گرامي، اين دستور كار را بدقت مطالعه كرده، آزمايش را انجام داده و پس از تكميل، براي مربي خود ارسال نماييد.

نيازمنديها

سخت افزار

- كابل CAT5 بدون سوكت
- سوكت RJ-45 ، 3 عدد
- آچار Crimp ، 1 عدد
- Tester شبكه، 1 عدد

زمان مورد نياز

- 30 دقيقه

دستور كار

با توجه به نحوه اصولي اتصال سوكت به كابل كه توسط مربي آموزش داده مي‌شود، يك كابل مستقيم(Straight) و يك كابل ضربدري(Cross) آماده كنيد و پس از تست آنها توسط Tester، به مربي تحويل دهيد. بديهي است رعايت اصول مذكور جهت ايجاد كابلها ضروري بوده و در نمره عملي جلسه موثر است.

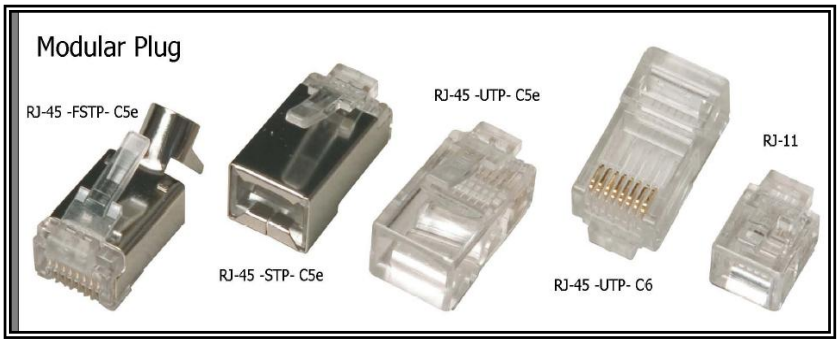
مطالب تكميلي

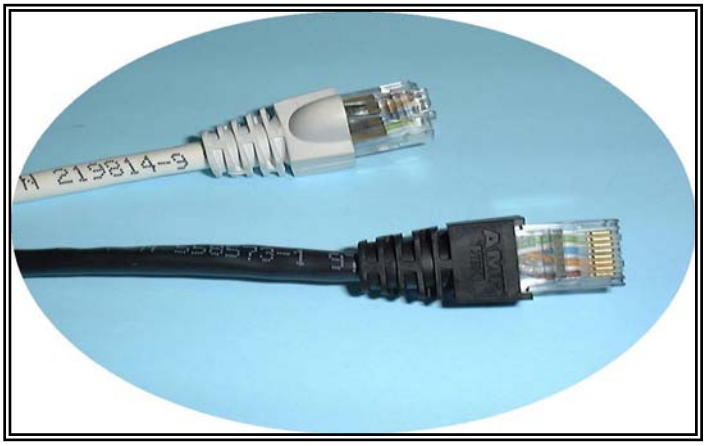
آشنايي با ابزارهاي مورد استفاده

Crimp tool

انواع سوکت

Patch cord





طراحي ، نصب و راه‌اندازي شبكه

در ایجاد و یا ارتقای یک شبکه کامپیوتری، برنامه‌ریزی درست از اهمیت خاصی برخوردار است. قبل از نصب و یا حتی انتخاب سخت‌افزارهای جدید باید مسائلی از قبیل سازگاری سخت‌افزاری، انتخاب قطعات و دستگاه‌های مناسب و قرار دادن آنها در مکانی مناسب را مد نظر داشته داشت. در این قسمت به بررسی بعضی از معیارهایی که در مرحله‌ی برنامه‌ریزی برای ایجاد شبکه باید مورد توجه قرار بگیرند و اینکه تصمیمات شما چطور می‌توانند آینده‌ی شبکه را تحت تأثیر قرار دهند، می‌پردازیم.

اولین گام در برنامه‌ریزی برای ایجاد یک شبکه تعیین نیازهای شرکت و یا سازمانی می‌باشد که قرار است از آن شبکه استفاده کند. بعد از آن نیازهای کاربران شبکه باید در نظر گرفته شود. سپس با داشتن اطلاعات کافی در مورد نیازهای شرکت و کاربران می‌توانید بنابر آن نیازها ایجاد شبکه را به صورت تکنیکی شروع کنید.
بعد از مطالعه این بخش قادر خواهید بود:

- مشخص کنید که یک شرکت و یا سازمان بخصوص به چه نوع شبکه-ای نیاز دارد.
- سایتی که قرار است شبکه در آن نصب شود را ارزیابی کنید و توضیح دهید که شرایط محیطی چطور می‌توانند روند برنامه‌ریزی برای نصب شبکه را تحت تأثیر قرار دهند.
- بنابر نوع شبکه و امکانات مورد نیاز، سخت‌افزارهای مناسبی انتخاب کنید.

ارزیابی نیازهای شرکت کارفرما

دلیل اینکه شرکتی از شما درخواست کرده است در آن یک شبکه‌ی جدید نصب کنید چیست؟ ممکن است قرار باشد یک شبکه‌ی جدید نصب کنید و یا اینکه از شما درخواست شود که یکسری از کامپیوترهای موجود در شرکت را به همدیگر شبکه کنید. امکان سومی هم وجود دارد و آن اینکه شرکت در حال حاضر دارای شبکه‌ای می‌باشد که می‌خواهد آنرا ارتقاء دهد و یا از یک تکنولوژی دیگری از آن استفاده کند.
در صورتیکه شرکت کارفرما در حال حاضر دارای شبکه باشد (یا تعدادی کامپیوتر که بخواهد آنها را شبکه کند) به احتمال زیاد می‌داند که انتظار چه سرویس‌هایی از شبکه‌ی جدید دارد. اما شرکتی که از شما درخواست ایجاد یک شبکه‌ی جدید را کرده است احتمالاً از نیازهای خود دقیقاً مطلع نمی-باشد. اما بطور کلی امکانی که اصولاً در همه‌ی شبکه‌ها باید وجود داشته باشد، امکان دستیابی کاربران به اینترنت و درایوها و چاپگرهای مشترک می‌باشد. این معیارها خود به تنهایی می‌تواند مدیر شبکه را در اتخاذ یکسری تصمیمات پایه یاری کند. امکان مشترک کردن درایوها و چاپگرها هدف اصلی همه‌ی شبکه‌ها می‌باشد و تقریباً به وسیله‌ی همه‌ی تکنولوژیهای شبکه‌ای قابل پیاده‌سازی می‌باشند، اما شما می‌دانید که برای دسترسی به اینترنت کامپیوترهای شبکه باید از TCP/IP استفاده کنند و به یکی از انواع مسیریابها برای متصل شدن به یک ISP مجهز باشند. باید توجه داشته باشید که وقتی صحبت از کامپیوترها به میان می‌آید کاسبان و تاجران می‌دانند که به چه چیزی احتیاج دارند ولی نمی‌دانند که چطور باید آنرا بدست آورند. بعنوان مثال، ممکن است در یک شرکت نیاز به پایگاه‌های داده پیچیده‌ای باشد که طبیعتاً نگهداری و کار با آنها نیاز به سرورهای قدرتمند با پردازنده‌های سریع، هزینه‌ی بالا و هارد دیسک‌های حجیم دارد. در جای

دیگری ممکن است نیاز به کار روی تصاویر گرافیکی حجیم و یا تصاویر ویدیوئی با کیفیت بالا باشد که در اینصورت باید پهنای باند و فضای ذخیره‌ی بسیار بالایی در اختیار قرار گیرد. یک شرکت تجاری بزرگ ممکن است بخواهد برای کاربران خود دستیابی بلادرنگ به اطلاعات بازارهای بورس مناطق مختلف روی زمین مهیا کند، که در این صورت نیاز پهنای باند داخلی بسیار بالا و دستیابی پرسرعت به اینترنت می‌باشد. بنابراین اول باید ببینید که نیاز شرکت کارفرما چیست و تا چه حد می‌تواند هزینه کند، سپس سعی کنید بنابر این اطلاعات راه‌حل مناسبی برای آن شرکت پیدا کنید.
علاوه بر مشورت با سرپرستان شرکت در مورد نیازهای آنها، بد نیست صحبتی هم با کاربرانی که قرار است از شبکه استفاده کنند داشته باشید. بدین وسیله ممکن است با مواردی برخورد کنید که انتخاب شما در تجهیزات شبکه و محل قرار گرفتن هر یک را تحت تأثیر قرار دهند. بعنوان مثال ممکن است مالک شرکت بتواند تصمیم بگیرد که چه تعداد و چه نوع چاپگرهایی برای سرویس‌دهی به کل کاربران شبکه کافی است اما کاربران بهتری می‌توانند محل مناسب برای قرار گرفتن چاپگرها را تعیین کنند.

ارزیابی محل (سایت) نصب شبکه

گام بعدی در برنامه‌ریزی برای ساخت یک شبکه، بررسی سایتی که شبکه باید در آن نصب شود و شرایط محیطی که تجهیزات شبکه باید در آن شرایط کار کنند می‌باشد. با انجام این بررسی شما راحتتر می‌توانید نوع شبکه، رسانه‌ی شبکه‌ی مورد نیاز و روش نصب آن را انتخاب کنید.
با این اطلاعات شما می‌توانید با در نظر گرفتن نیازهای کاربران شروع به انتخاب سخت‌افزار مناسب کنید. در بخش‌های بعدی به بررسی بعضی از فاکتورهایی که در زمان ارزیابی محل نصب شبکه باید مورد توجه قرار گیرد می‌پردازیم.

فاصله بین اجزای مختلف

یکی از مهمترین نکات در ارزیابی سایت، ایجاد یک تصویر کلی از محل قرار گرفتن کامپیوترهای مختلف و تجهیزات شبکه نسبت به همدیگر می‌باشد. در یک شبکه‌ی اترنت 10Base-T یا 100Base-Tx حداکثر فاصله‌ی مجاز هر کامپیوتر از هاب 100 متر می‌باشد که در اغلب موارد بیش از حد مورد نیاز است. معهذا علاوه بر فاصله‌ی بین تجهیزات مختلف مسیر کابل‌ها را هم باید مورد توجه قرار دهید. در بسیاری از موارد لازم است که کابل‌ها از روی دیوارها، از میان سقف‌ها، از کنار لامپ‌ها و تجهیزات روشنایی و موانع دیگر عبور کنند تا یک ارتباط برقرار شود. مسیر نهایی یک کابل ممکن است بسیار بیشتر از فاصله‌ای باشد که با تخمین به وسیله‌ی قدمزدن از هاب به کامپیوتر بدست آمده است. در موارد دیگر ممکن است مجبور شوید کامپیوترهایی که در فواصل طولانی از همدیگر قرار دارند و یا در ساختمانهای

متفاوتی مستقر هستند را به همدیگر متصل کنید. در چنین شرایطی می‌توانید از فیبر نوری که فواصل گسترده‌تری را می‌تواند تحت پوشش قرار دهد استفاده کنید.
مسئله دیگری که باید مورد توجه قرار گیرد موانعی می‌باشد که بین کامپیوترهایی که باید به شبکه متصل شوند قرار می‌گیرند. به عنوان مثال، اگر همه‌ی کامپیوترهای شبکه مستقر در تنها یک اتاق باشند می‌توانید از کابل‌های پیش‌ساخته استفاده کنید و آنها را با کمی فاصله از سطح زمین، دور تا دور اتاق بکشید. البته این مورد یک پروژه‌ی ساده می‌باشد که نیازی به تجهیزات بخصوصی ندارد. اما اگر شبکه بزرگ باشد و کامپیوترها در اتاق‌های متعددی پخش شده باشند و یا اینکه شکل ظاهری کابل‌کشی دارای اهمیت باشد، مجبور خواهید شد از کابل‌کشی توکار استفاده کنید. در این روش کابل‌ها از داخل دیوار و سقف‌ها عبور داده می‌شوند و از یک طرف به یک پنل رابط (این پنل در واقع صفحه‌ای است که کابل‌ها به پشت آن وصل می‌شوند و روی آن سوکت‌های ساده‌ای وجود دارد که با استفاده از کابل‌های رابط یا patch به هاب متصل می‌شوند) و از طرف دیگر به پریزهای نصب شده روی دیوار متصل می‌شوند. در روش کابل‌کشی توکار احتیاج به برنامه‌ریزی دقیق‌تر، تجهیزات بیشتر و افراد متخصص می‌باشد. علاوه بر این هزینه‌ی نصب هم در این روش به مراتب بالاتر است.
در روند نصب همه‌ی شبکه‌ها نیاز به بررسی محل قرار گرفتن ایستگاه‌های کاری و دیگر تجهیزات سرویس‌گیرنده وجود دارد، اما در شبکه‌هایی که کمی پیچیده‌تر هستند باید بررسی شود که برای استقرار تجهیزات سرویس‌دهنده مثل هابها، سرورها، مسیریابها و غیره چه مکانهایی مناسب‌تر هستند. در همه‌ی انواع شبکه‌ها، حتی کوچکترین آنها، بهترین کار اینست که این تجهیزات سرویس‌دهنده را در مکانهای امنی مثل یک اتاق مخصوص و یا محفظه‌های قفل‌دار قرار دهید تا در برابر صدمه‌های احتمالی، چه عمدی و چه غیرعمدی، مصون باشند. بنابراین بنابر اندازه‌ی شبکه ممکن است نیاز به چندین محفظه‌ی قفل‌دار برای قرار دادن سرورها، هابها و پنل‌های رابط داشته باشید.

انتخاب تجهیزات مختلف و محل قرار گیری مناسب برای هر یک

بخش مهمی از کار برنامه‌ریزی برای نصب یک شبکه انتخاب تجهیزات مناسب با محیط کار و قرار دادن آنها در مکانهایی می‌باشد که به بهترین نحو قابل بهره‌برداری باشند. بعنوان مثال ، کاربری را در نظر بگیرید که چاپگر لیزری مورد استفاده‌ی شرکت روی میز او قرار دارد. شما می‌توانید با انتقال آن چاپگر به نقطه‌ای مناسب‌تر که قابل دسترسی همه‌ی کاربران هم باشد، آن کاربر را خوشحال کنید. گرچه ممکن است برای انجام چنین کاری مجبور شوید یک چاپگر خارجی خریداری کنید که مستقیماً قابل اتصال به شبکه

باشد، اما اگر نسبت به حالت قبل افراد بیشتری بتوانند راحت‌تر به چاپگر دسترسی داشته باشند، انجام این کار ارزش دارد.
نكته‌ي ديگري كه بايد مورد توجه قرار گيرد تعيين محل ايستگاه‌هاي كاري مي‌باشد. اكثر كامپيوترهايي كه براي استفاده در اداره‌ها و شركت‌ها طراحي مي‌شوند داراي كيس‌هاي كوچكي مي‌باشند كه روميزي هستند. حتي آن كيس‌هاي كوچك هم فضاي زيادي از ميز كاربر را اشغال مي‌كنند. ممكن است براي اينكه جاي زيادي اشغال نشود مجبور شويد كامپيوترهايي خريداري كنيد كه به راحتي قابل قرار دادن روي زمين باشند و يا زير ميز كاربران جا شوند.

شرايط محيطي
علاوه بر مكان فيزيكي تجهيزات شبكه بايد شرايط محيطي محل قرارگيري هر يك از آنها را هم مد نظر قرار دهيد. البته اين كار ممكن است در مورد ساختمانهايي كه داراي دما و رطوبت ثابتي مي‌باشند به نظر لازم نيايد، اما چند نكته‌ي مهم وجود دارد كه بايد مورد توجه قرار گيرد. يكي از اين نكات مهم اين است كه آيا هواي مطلوب دوره ساعت كاري شركت در ساعات غيركاري تغيير مي‌كند يا خير. در بعضي از شركت‌ها سيستم تهويه در طول شب خاموش مي‌شود و اگر قرار باشد كامپيوتري در ساعات غيركاري به كار خود ادامه دهد و روشن باشد دماي آن در شب‌هاي تابستاني به راحتي از حد مجاز بالاتر مي‌رود و دچار مشكل مي‌شود. دماي به شدت سرد هم مي‌تواند روي بازدهي تجهيزات كامپيوتري تأثير بگذارد. نكته‌ي ديگري كه بايد مورد توجه قرار گيرد اينست كه ممكن است دماي محفظه‌اي كه قرار است سرورها و تجهيزات ديگر در آن قرار گيرند كنترل‌شده نباشد. در صورتيكه لازم باشد تعداد زيادي كامپيوتر، مسيرياب و يا هر دستگاه ديگري كه حرارت توليد مي‌كند را در يك نقطه‌ي مركزي جمع كنيد به احتمال زياد براي به اندازه‌ي كافي خنك نگه‌داشتن محيط نياز به سيستم كنترلي دماي مستقلي خواهيد داشت. نكته‌ي ديگر اينكه براي پشتيباني از اين تعداد تجهيزات الكتريكي نياز به دستگاه‌هاي لازم براي توليد نيروي الكتريكي ثابت مي‌باشد. در اينصورت ممكن است به يك منبع تغذيه يدك و محافظ نوسان برق براي كل شبكه نياز داشته باشيد. براي تأمين چنين شرايطي مي‌توانيد از UPS ها استفاده كنيد. البته همه‌ي شبكه‌ها در ساختمانهاي بي‌دردسر نصب نمي‌شوند. ممكن است در شرايطي از قبيل نواحي صنعتي قرار گيريد كه تجهيزات شبكه در معرض مقدار نامتعادلي گرما، سرما، رطوبت، غبار، اختلالات الكترومغناطيسي، گازهاي شيميايي و غيره قرار گيرند. محصولات گوناگوني وجود دارند كه كامپيوترها را قادر مي‌سازند در چنين شرايطي كار كنند. از جمله اين محصولات مي‌توان صفحه كليدهاي ضد آب، كامپيوترهاي مجهز به سيستم تصفيه هوا كه گرد و غبار و آلودگيهاي ديگر را از سيستم دور

مي‌كند، تكنولوژيهاي مناسب با شرايط گوناگون مثل رسانه‌هاي بي‌سيم و فيبر نوري را نام برد.

اختلالات الكترومغناطيسي

اگر قرار باشد از كابل‌كشي توكار استفاده كنيد بايد محل عبور كابل‌ها را بررسي كنيد كه با مانع و يا ميدان‌هاي الكترومغناطيسي برخورد نكنيد. كابل‌هاي مسي به شدت در مقابل ميدان‌هاي الكترومغناطيسي كه توسط لامپهاي فلورسنت، موتورهاي الكتريكي و يا تجهيزات الكتريكي ديگر توليد مي‌شوند حساس هستند. مواردي بسيار ساده كه ممكن است اصلاً جلب توجه نكنند از قبيل محل قرار گرفتن تلويزيون، راديو و بخاريهاي برقي مي‌توانند بازدهي شبكه را تحت تأثير قرار دهند. اگر قرار باشد شبكه‌اي را ارتقاء دهيد، به احتمال زياد متوجه خواهيد شد كه دليل دريافت بعضي از پيغام‌هاي خطا و مشكلات ديگر شبكه همين نكته‌هاي ذكر شده بوده است. براي گريز از چنين مسائلي سعي كنيد از مسيرهايي براي كابل‌كشي استفاده كنيد كه حتي‌الامكان در معرض اختلالات الكترومغناطيسي قرار نگيريد در غير اينصورت مجبور خواهيد بود از فيبر نوري و يا كابل‌هايي استفاده كنيد كه براي شيلد اضافه مي‌باشند. نكته‌ي ديگر اينكه در صورتيكه قرار باشد كابل‌كشي روكار انجام شود بايد از كابل‌هايي استفاده كنيد كه با بالارفتن بيش از حد دما و يا آتش‌سوزي از خود گازهاي سمي خطرناك متصاعد نكنند. حتي اگر قرار باشد از شركت ديگري بخواهيد كه كار كابل‌كشي را انجام دهد بايد از شرايطي كه هزينه‌ها را تحت تأثير قرار مي‌دهد مطلع باشيد.

انتخاب سخت‌افزار

بعد از تعيين نيازهاي شركت و يا مؤسسه‌ي كارفرما، مي‌توانيد طراحي شبكه و انتخاب تجهيزات مورد نياز را شروع كنيد. اگر قرار بر نصب شبكه‌اي جديد باشد، احتمالاً مسئول خريد و يا انتخاب كامپيوترهاي شبكه هم خواهيد بود. بايد توجه داشته باشيد كه بنابر نيازهاي شبكه مدل كامپيوترها را انتخاب كنيد. اما اگر قرار است شبكه‌اي را ارتقاء دهيد بايد بررسي كنيد كه آيا كامپيوترهاي فعلي جوابگوي نيازهاي شبكه خواهند بود و يا نياز به ارتقاء دارند. مطمئناً نصب يك شبكه‌ي پرسرعت حرفه‌اي براي متصل كردن تعدادي كامپيوتر 486 قديمي اشتباه است. سازگاري سخت‌افزاري هميشه مسئله‌ي مهمي در نصب شبكه‌ها بوده است. اما اگر قرار است با تجهيزات فعلي شبكه‌اي كار كنيد اين مسئله از اهميت بيشتري برخوردار مي‌شود. اغلب انتخاباتي كه براي خريد تجهيزات شبكه بايد اتخاذ كنيد بر مبناي پروتكل‌هاي شبكه، بخصوص پروتكل‌هاي لايه‌ي پيوند- داده خواهد بود. اغلب محصولات اترنتي، حتي اگر ساخت توليدكننده‌هاي متفاوتي باشند، با همديگر خوب كار مي‌كنند،اما به هر حال بايد مطمئن باشيد كه محصولات

انتخاب شده همگي از يك نوع اترنت پشتيباني مي‌كنند. بعنوان مثال، اگر قرار باشد شبكه‌اي را گسترش دهيد، ممكن است بخواهيد در كامپيوترهاي جديد از Fast Ethernet استفاده كنيد و كامپيوترهاي موجود را بعداً از اترنت به Fast Ethernet ارتقاء دهيد. اگر براي كامپيوترهاي جديد كارت شبكه dual-speed خريداري كنيد ولي كارتهاي شبكه‌ي 10MBPS كامپيوترهاي موجود را تغيير ندهيد، مجبور خواهيد شد يك هاب dual-speed هم خريداري كنيد چون، اگرچه يك هاب Fast Ethernet از كامپيوترهاي جديد در سرعت 100MBPS پشتيباني مي‌كند اما نمي‌تواند از كامپيوترهاي٠ قديمی در سرعت 10MBPS پشتيبانی كند . در واقع نمی توان يک هاب 10MBPS را به يک هاب 100MBPS متصل كرد، بنابراين كامپيوترهاي قديمي و جديد قادر به برقراري ارتباط با همديگر نخواهند بود. يك هاب dual-speed با پورتهاي مناسب براي Fast Ethernet و اترنت معمولي مي‌تواند همه‌ي كامپيوترها را به يك شبكه متصل كند. علاوه بر چنين مسائل مربوط به سازگاري سخت‌افزاري، موارد كوچك ديگري هم وجود دارند كه براي اينكه همه‌ي اجزاي شبكه بدون مشكل با همديگر كار كنند، بايد مورد توجه قرار گيرند. بعنوان مثال كانكتور و گذرگاه كارت شبكه‌ي منتخب شما بايد با كامپيوتر و رسانه‌ي شبكه سازگار باشد. همچنين اطمينان حاصل كنيد كه كارت شبكه‌ي شما داراي درايوري مناسب با سيستم عامل منتخب باشد. زمان انتخاب گروه كابل (مثلاً Category 5) توجه داشته باشيد كه همه‌ي اجزاي درگير در كابل‌كشي كه سيگنال‌هاي شبكه را حمل مي‌كنند، (مثلاً كانكتورها، پريزهاي ديواري، پنل‌هاي رابط و كابل‌هاي رابط) بايد از يك گروه باشند.

نصب و راه‌اندازی شبکه

- كابل‌كشي
- ايجاد اتصالات

بعد از طراحي شبكه و انتخاب سخت‌افزار لازم، زمان نصب شبكه فرامي‌رسد. در اين فصل به بررسي كابل‌كشي و روش استفاده از كابل‌ها براي متصل كردن كامپيوترها به اجزاي ديگر شبكه و ايجاد يك شبكه‌ي محلي مي‌پردازيم.

كابل‌كشي

نصب كابل‌هاي شبكه را به اصطلاح «كابل‌كشي» مي‌گويند. چون در بسياري از موارد براي عبور كابل از بعضي از مكان‌هاي بخصوص لازم است يك سر آن را به وسيله‌ي طناب يا ابزار ديگري به سمت ديگر بكشيد. (به عنوان مثال: براي عبور كابل از سقف يا ديوار). كابل‌كشي يك شبكه بنابر نوع كابل‌ها و ماهيت محلي كه قرار است شبكه در آن مستقر شود مي‌تواند بسيار ساده و يا به طرز چشم‌گيري پيچيده و مشكل باشد. در اين درس عمدتاً به نصب

كابل‌هاي UTP كه امروزه متداول‌ترين رسانه‌ي شبكه به شمار مي‌رود مي‌پردازيم.
بعد از مطالعه اين درس قادر خواهيد بود:
1- توضيح دهيد كه كابل‌كشي روكار و محكم كردن آنها به چه صورت انجام مي‌شود.
2- مراحل مختلف كابل‌كشي توكار را شرح دهيد.
3- تكنيك‌هاي مختلفي كه براي نصب انواع مختلف كابل‌ها وجود دارد را نام ببريد.

كابل‌كشي روكار

در كابل‌كشي روكار از كابل UTP پيش‌ساخته براي متصل كردن هر يك از كامپيوترها به هاب استفاده مي‌شود. در اين روش نيازي نيست كه كابل‌ها از ميان سقف و ديوارها كشيده شوند، به انتهاي كابل‌ها كانكتور متصل شود و يا تجهيزات اضافي از قبيل پريزهاي ديواري و پنل رابط (patch panel) خريداري شود. از جمله مزاياي اين روش اين است كه در صورتيكه بخواهيد شبكه را تغيير مكان دهيد مي‌توانيد كابل‌هاي آنرا جمع كنيد و از آنها در محل جديد مجدداً استفاده كنيد. كه عيب اين روش اين است كه معمولاً كابل‌ها در معرض ديد قرار دارند و عبور كابل‌ها از موانع موجود در بين تجهيزات شبكه مشكل است. معهذا روش‌هايي وجود دارد كه با استفاده از آنها مي‌توان چنين مسائلي را در حد امكان به حداقل رساند. مراحل اصلي كابل‌كشي روكار شامل موارد زير مي‌باشد :

1.مكان هر يك از كامپيوترها، هاب و هر وسيله‌ي ديگري از قبيل پرينترها كه به نوعي به شبكه متصل مي‌شوند را تعيين كنيد. هاب بايد نسبت به كامپيوترهاي شبكه در مركز قرار گيرد. به اينصورت طول كابل‌ها به حداقل مي‌رسد و مجبور به تعداد زيادي را از يك مسير عبور دهيد.

2.دقيقاً مشخص كنيد كه كابل‌هاي بين كامپيوترها و هاب از چه مسيري بايد عبور كنند. تمام موانع موجود در مسير از قبيل اثاثيه‌ي موجود در محل، ديوارها و چهارچوب درها را مورد بررسي قرار دهيد و روشي براي عبور كابل‌ها از ميان يا كنار آنها پيدا كنيد.

3.طول كابل لازم براي متصل كردن هر يك از كامپيوترها به هاب را محاسبه كنيد. در اين محاسبه بايد مسيرهاي عمودي دور چهارچوب درها، ضخامت ديوارها و موانع ديگر را در نظر داشته باشيد. براي اطمينان حداقل يك يا دو متر از هر يك از مقادير محاسبه شده اضافه‌تر اختيار كنيد تا در حين نصب دقيق هاب و كامپيوترها و احياناً برخورد با موانع پيش‌بيني نشده، مشكلي پيش نيايد.

4.بنابر محاسباتي كه در مرحله‌ي قبل انجام داديد، كابل‌هاي از پيش‌ساخته‌ي لازم را خريداري كنيد. در صورت استفاده از كابل‌هاي UTP بايد

حداقل از كابل‌هاي گروه 5 خريداري شود. بهتر است از كابل‌هايي استفاده كنيد كه كانكتورهاي آنها داراي محافظ پلاستيكي مي‌باشند.
5.كابل‌ها را بدون محكم كردن در محل خود و متصل كردن به تجهيزات شبكه روي زمين بخوابانيد. (در واقع هر يك از كابل‌ها را در مسيري كه بايد از آن عبور كند، بدون محكم كردن بخوابانيد) مقدار كابل لازم براي دور زدن چهارچوب درها و موانع ديگر را فراموش نكنيد. كابل‌ها بايد بدون هيچ مشكلي به هاب و كامپيوترها برسند.
6.از يك سر هر يك از كابل‌ها شروع كنيد و تا انتهاي ديگر آنها را در محل خود محكم كنيد. مراقب باشيد كه هيچيك از كابل‌ها در مسير خود تحت هيچگونه فشاري نباشند و تاب نخورده باشند. مسير كابل‌ها بايد طوري باشد كه در معرض عبور و مرور افراد قرار نگيرند.
7.بعد از محكم كردن كابل‌ها، يك سر هر يك به هاب و سر ديگر را به كامپيوترها يا دستگاه‌هاي ديگر متصل كنيد. وقتي هاب به يك منبع تغذيه متصل شود و كامپيوترها روشن شوند. چراغ‌هاي سيگنال link pulse روي هاب و كارت شبكه‌ي كامپيوترها بايد به نشانه‌ي برقرار بودن و صحت ارتباطات روشن شوند.
همانطور که مشاهده می‌کنید، کابل‌کشی روکار برای شبکه‌هایی مناسب‌تر است که همه‌ی کامپیوترها و تجهیزات آن در یک اتاق مستقر هستند چون در این صورت دیگر نیازی به عبور کابل‌ها از دیوار و سقف‌ها که از جمله مشکل‌ترین مسائل کابل‌کشی روکار به شمار می‌رود، نمی‌باشد. در شبکه-های کوچکی که فقط به یک اتاق محدود می‌شوند معمولاً بهترین کار اینست که کابل‌ها از کنار دیوارها عبور داده شوند و یا از پشت اثاثیه‌ی موجود در محل عبور داده شوند.
توجه: از جمله مواردی که در نصب کابل‌ها باید در نظر داشته باشید اینست که هیچ کابلی نباید به صورتی آزاد و در معرض عبور مرور رها شود. اگر روی کابل‌ها پا گذاشته شود پس از مدتی آسیب می‌بینند و نهایتاً شبکه از کار می‌افتد.
از جمله مسائلی که در کابل‌کشی روکار ممکن است با آن مواجه شوید اینست که کامپیوترها و یا هر یک از تجهیزات دیگر شبکه کنار دیوار نباشند. البته بنابر موقعیت فیزیکی محل، روش‌های مختلفی برای برخورد با این مسئله وجود دارد. بعنوان مثال می‌توانید از محافظهای لاستیکی که برای این منظور ساخته شده‌اند استفاده کنید. در این روش کابل‌ها از میان این محافظهای لاستیکی عبور داده می‌شوند و به این صورت در مقابل عبور و مرور افراد محافظ می‌شوند. بعنوان روشی دیگر می‌توانید کابل‌های پیش-ساخته‌ی خود را تا محل مورد نظر از سقف عبور دهید و بعد یا استفاده از تیرهای چوبی یا پلاستیکی مخصوص آنها را از سقف به کف زمین بکشید. البته اگر قرار باشد کابل‌ها را از سقف عبور دهید شاید بهتر باشد کلاً از کابل‌کشی توکار استفاده کنید.

محکم کردن کابل‌های روکار

گرچه می‌توان کابل‌ها را در محل خود آزادانه رها کرد ولی بهتر است آنها را محکم کنید تا در محل خود ثابت باشند و به نواحی که عبور و مرور انجام می‌شود کشیده نشوند و آسیب نبینند. اگر کابل‌ها آزادانه رها شوند مسئله‌ی دیگری که ممکن است به وجود بیاید اینست که پای شخصی به آنها گیر کند و کابل‌ها کشیده شوند و به این صورت کانکتورهای کابل‌ها آسیب ببینند. برای محکم کردن کابل‌ها و قرار دادن آنها در مسیر خود انجام شود. هرگز در حین کابل‌کشی، آنها را محکم نکنید چون اگر کابلی کوتاه باشد مجبور خواهید شد کار را مجدداً از اول شروع کنید. ساده‌ترین و معمولاً کم‌هزینه‌ترین روش برای محکم کردن کابل‌ها استفاده از بست‌های دو پایه یا منگنه می‌باشد. معهذا از منگنه‌های استانداردی که اغلب دستگاه‌های منگنه زنی بکار می‌رود استفاده نکنید، چون این نوع منگنه ممکن است کابل‌ها را زخمی کنند و به سیم‌های داخل آن آسیب وارد کنند. در عوض می‌توانید از بست‌های تکی استفاده کنید که برای اینکه ضربه زدن رو ی آنها ساده‌تر شود روی خود دارای کلاهکی می‌باشند و یا از بست‌هایی استفاده کنید که دارای یک نگهدارنده کابل می‌باشند. این نگهدارنده در واقع شامل یک نوار پلاستیکی می‌باشد که از داخل آن رشته سیم محکمی عبور کرده است. با ضربه زدن روی این بست، نوار پلاستیکی داخل آن کابل را به دیواره محکم می‌کند.

در صورتیکه کابل‌کشي شبکه زیاد باشد مي‌توانید يك دستگاه بست‌زني (منگنه) که مخصوصاً براي زدن بست روي کابل‌ها طراحي شده است خريداري کنيد. در اين دستگاه از بست‌هاي سرگِرد استفاده مي‌شود و امکان تنظيم عمق فرورفتگي بست وجود دارد. در واقع هدف از استفاده از چنين ابزاريهايي اينست که در ضمن اينکه بست‌ها به ديوار محکم شده‌اند، کابل‌ها را بتوان از ميان آنها به راحتي بالا و پايين کشيد. در غيراينصورت بست بيش از حد به ديوار فشار داده شده است. اگر کابل در هنگام بست‌زني تصادفاً زخمي شود بايد آنرا کنار بگذاريد و از يك کابل جديد استفاده کنيد. دستگاه‌هاي منگنه‌ي خوب معمولاً علاوه بر سوزن منگنه‌هاي سرگرد داراي قابليت استفاده از سوزن منگنه‌هاي مستطيلي هم مي‌باشند بنابراين از آنها در کارهاي ديگر هم مي‌توان استفاده کرد.

روش ديگر براي محکم کردن کابل‌ها استفاده از بست‌هاي نواري مي‌باشد. اين نوع بست‌ها روي سطح محل مورد نظر نصب مي‌شوند و مي‌توانند يك يا چند کابل را نگه دارند. بعضي از انوع بست‌هاي نواري داراي سيستم قلاب و چرخ‌دنده‌ي ضامن‌دار (مانند دست‌بندهاي پليسي که اندازه‌ي آنها قابل تنظيم است)مي‌باشند و بعضي ديگر متشکل از يك حلقه پارچه‌اي يا پلاستيکي مي‌باشند که دو سر آنها مانند سگك کمربند و يا پارچه‌هاي وِلکرو (پارچه‌هاي چسبنده) به همديگر بسته مي‌شوند. از اين نوع بست‌ها معمولاً براي

نگهداري تعداد زيادي كابل استفاده مي‌شود و ويژگي آنها اينست كه همچنانكه شبكه گسترده‌تر مي‌شود مي‌توان آنهات را باز كرد و كابل‌هاي بيشتري را به آنها اضافه كرد.
نكته: بست‌هاي منگنه‌اي و نواري هر دو ابزار مناسبي براي محكم كردن كابل‌ها به ديوار يا سطوح ديگر مي‌باشند ولي كابل‌ها را در مقابل اشيايي كه ممكن است به ديوار برخورد كنند و به آنها فشار وارد آورند محافظت نمي‌كنند كابل‌كشي بايد طوري انجام شود كه در حد امكان از برخورد اثاثيه و اشياي ديگر با آنها ممانعت به عمل آيد.
روش ديگر براي محافظت و محكم كردن كابل‌ها استفاده از داكت‌هاي مخصوص كابل‌كشي روكار مي‌باشد كه نسبت به منگنه و بست‌هاي نواري از كابل‌ها بهتر محافظت مي‌كنند. داكت پوششي است پلاستيكي كه روي ديوار نصب مي‌شوند و سطح پشتي بعضي ديگر مانند چسب برگردان به سطح مورد نظر چسبانده مي‌شود (مطمئناً نوع اول محكمتر است). چون كابل‌هاي داخل داكت در محفظه‌اي كاملاً پوشيده قرار مي‌گيرند از ضربات خارجي كاملاً در امان هستند.
نصب داكت‌ها نسبت به بست‌هاي منگنه‌اي و نواري مشكل‌تر و پرهزينه‌تر مي‌باشند. زمان خريد بايد دقت كنيد سايز مناسبي را انتخاب كنيد چون داكت‌ها انعطاف‌پذير نمي‌باشند و تعداد كابل مشخصي را در خود جا مي‌دهند. براي اينكه كار تميزتر انجام شود مي‌توانيد از اتصالاتي از قبيل زانو و سه راه مناسب با داكت انتخاب شده استفاده كنيد. داكت‌ها معمولاً به رنگ شيري يا سفيد عرضه مي‌شوند.
نكته: علاوه بر اتصالاتي از قبيل زانو و سه راهي، پريزهاي روكاري هم مناسب با داكت انتخاب شده عرضه مي‌شود كه در صورت تمايل مي‌توانيد از آنها استفاده كنيد. روي اين پريزها سوكت‌هايي وجود دارد و شما مي‌توانيد كابل‌هاي داخل داكت را مستقيماً به آنها وصل كنيد. اين روش معادل روش كابل‌كش روكار مي‌باشد و معمولاً در ساختمانهايي كه داراي ديوارهاي يا سقف‌هاي بتوني مي‌باشند استفاده مي‌شوند.

كابل‌كشي دور چارچوب درها

از جمله موانعي كه معمولاً در كابل‌كشي يك اتاق وجود دارد، ورودي آن مي‌باشد. بطور كلي در حد امكان نبايد كابل را از بالا يا پايين چهارچوب در عبور داد، حتي اگر مجبور باشيد دور تا دور اتاق را كابل‌كشي كنيد. معهذا گاهي هيچ چاره‌اي نيست مگر عبور كابل از ورودي اتاق،براي اين كار دو راه وجود دارد: يكي اينكه كابل را از بالا و دور چهارچوب در عبور دهيد و يا اينكه آنرا از جلوي در ورودي از روي زمين عبور دهيد. اما در حد امكان نبايد كابل‌ها را از جلوي در عبور داد چون حتي اگر آنها را كاملاً به زمين محكم كرده باشيد پس از مدتي عبور و مرور، سيم‌هاي داخل آنها آسيب مي‌بينند. در صورت امكان مي‌توانيد كابل‌ها را از زير آستانه‌ي در عبور دهيد. در بعضي موارد هم

هيچ راهي وجود ندارد مگر عبور كابل‌ها از دور چهارچوب در و محكم كردن آنها توسط يكي از انواع بست‌هاي مناسب اينكار به سادگي قابل انجام است بخصوص اگر چهارچوب در از جنس چوب باشد، اما چون كابل‌ها در معرض ديد قرار مي‌گيرند، اين روش شكيل نمي‌باشد. البته مي‌توانيد در صورت نياز بعد از كابل‌كشي، آنها را مناسب با چهارچوب و ديوارها رنگ كنيد.
توجه داشته باشيد كه هر چه تعداد كابل‌هاي لازم براي عبور از دور چهارچوب‌ها زيادتر شود، كار مشكل‌تر مي‌شود. در اينصورت مي‌توانيد با استفاده از يك هاب اضافي فقط يك كابل از دور در عبور دهيد و يا از يك داكت با سايز مناسب استفاده كنيد. از آنجا كه طول زيادي از كابل صرف عبور آن از چهارچوب در مي‌شود بايد زمان تخمين اندازه‌ي لازم، اين مسئله را در نظر بگيريد.

كشيدن كابل‌ها به اتاق‌هاي ديگر

اگر كامپيوترها در چندين اتاق پخش شده باشند، حتي كابل‌كشي روكار هم مشكل مي‌شود. بطور كلي دو راه براي كشيدن كابل از اتاقي به اتاق ديگر وجود دارد: از در و يا از ميان ديوار. همانطور كه قبلاً متذكر شديم كشيدن كابل در راستاي عرض در (منظور در حالت بسته مي‌باشد) مشكل‌زا است، اما اگر براي كشيدن كابل از اتاقي به اتاق دگير آنرا از زير در عبور دهيم مسئله‌اي نيست، البته به شرط آنكه بين در و سطح زمين فاصله به اندازه‌ي كافي وجود داشته باشد تا در صورت بسته شدن در، كابل صدمه نبيند. اما اگر تصميم گرفتيد كه كابل را از ميان ديوار عبور دهيد معمولاً بهترين كار اينست كه نقطه‌اي را براي سوراخ كردن انتخاب كنيد كه در هر دو طرف به وسيله شئي پوشيده باشد و سوراخ ايجاد شده در معرض ديد نباشد. توجه داشته باشيد كه در صورت استفاده از كابل‌هاي از پيش‌ساخته، سوراخ ايجاد شده بايد به اندازه‌اي باشد كه كانكتور سر كابل به راحتي از آن عبور كند.
توجه: زمان سوراخ كردن ديوار مواظب لوله و كابل‌هايي كه ممكن است از داخل ديوار رد شده باشند باشيد. گرچه استفاده از مته‌اي كه از عرض ديوار بزرگتر باشد ساده‌تر است و به اينصورت به يكباره مي‌توان سوراخ را ايجاد كرد، اما معمولاً بهتر است كه يك طرف ديوار را سوراخ كنيد و با استفاده از يك پيچ‌گوشتي بلند در حين توجه به اينكه لوله و يا كابلي آسيب نبيند روي آن ضربه بزنيد تا ديوار سوراخ شود (به اينصورت پس از هر ضربه مي‌توانيد با نگاه كردن به داخل سوراخ از عدم وجود لوله و يا كابل اطمينان حاصل كنيد)

كشيدن كابل‌ها بين طبقات

در نصب كابل‌هاي يك شبكه معمولاً مشكلترين بخش، عبور كابل‌ها از سقف و كف طبقات مي‌باشد. در چنين شرايطي معمولاً نمي‌توان به راحتي محل مناسبي را براي عبور كابل‌ها پيدا كرد و در بيشتر موارد نياز به ابزار مخصوصي مي‌باشد. در ساختمانهايي كه بناي آنها چوبي است مي‌توان با

استفاده از مته، نقطه‌ي مورد نظر را از پايين و بالا سوراخ كرد و كابل را عبور داد فقط بايد مواظب باشيد كه هر دوي اين سوراخ‌ها روبروي همديگر ايجاد شوند تا كابل در ميان فضاي خالي سقف رها نماند. اگر ديوارهاي دو طبقه‌ي مورد نظر زير همديگر بنا شده باشند در بعضي از موارد مي‌توانيد از طريق سوراخي كه براي نصب پريز روي ديوار ايجاد كرده‌ايد، سقف را از بالا و از ميان دو جدار ديوار سوراخ كنيد. البته براي انجام اينكار نياز به دريلي مجهز به سر نظام مخصوص و مته‌اي بلند خواهيد داشت. كار ديگري كه مي‌توان انجام داد اينست كه سقف را از پايين سوراخ كنيد. در اينصورت يك روش براي پيدا كردن دقيق نقطه‌اي كه بايد سوراخ شود اينست كه از طبقه‌ي بالا سوراخي به قطر يك هشتم اينچ دقيقاً در مرز بين ديوار و سقف به طرف پايين ايجاد كنيد سپس يك وسيله‌ي نوك‌تيز در سوراخ وارد كنيد و آنقدر فشار دهيد تا در طرف ديگر سقف به عنوان علامت، سوراخي كوچك ايجاد شود. بعد از طبقه‌ي پايين به فاصله‌ي حدوداً دو اينچ از علامت به سمت ديوار، سوراخي به قطر سه چهارم اينچ به طرف بالا بزنيد و كابل را از پايين رد كنيد و از بالا آنرا بگيريد و به اندازه‌ي لازم بكشيد.
در ساختمان‌هاي اداري، احتمال اينكه سوراخ‌ها يا مسيرهاي از قبيل تعبيه شده‌اي بين طبقات وجود داشته باشد زياد است و شما مي‌توانيد از آنها براي عبور كابل‌ها استفاده كنيد. البته ممكن است كه مسير موجود بخشي از مثلاً سيستم تهويه‌ي ساختمان باشد كه در اينصورت بايد از كابل‌هاي مخصوص استفاده كنيد (بعنوان مثال شايد لازم باشد از كابل‌هاي plenum استفاده كنيد) و گرنه مجبور خواهيد شد كل كابل‌كشي شبكه را از اول انجام دهيد و متحمل هزينه‌هاي سنگيني شويد. اما اگر در ساختمان چنين مسيرهاي از قبيل تعبيه شده‌اي وجود نداشته باشد كار بسيار مشكل مي‌شود چون معمولاً سقف ساختمان‌هاي اداري و تجاري از جنس بتون و به ضخامت چندين اينچ است و براي سوراخ كردن چنين سقف‌هايي نياز به ابزار سنگين مخصوصي مي‌باشد.

كابل‌كشي توكار

اغلب كابل‌كشي‌هاي حرفه‌اي به صورت توكار انجام مي‌شوند. يعني كابل‌ها از ميان ديوارها، كف و سقف‌ها كشيده مي‌شوند. برخلاف كابل‌كشي روكار كه در آن براي وصل كردن هر كامپيوتر به هاب فقط نياز به يك تكه كابل پيش‌ساخته مي‌باشد در كابل‌كشي توكار همانطور كه در شكل زير نشان داده شده است نياز به سه تكه كابل مي‌باشد. بخش اصلي اتصال هر كامپيوتر با هاب كابلي مي‌باشد كه از پريز ديواري مجاور هر كامپيوتر به پنل رابط مجاور هاب كشيده مي‌شود. دو كابل ديگر، كابل‌هاي پيش‌ساخته‌ي نسبتاً كوتاهي هستند كه كابل رابط يا patch ناميده مي‌شوند و كامپيوتر را به پريز روي ديوار و يكي از سوكت‌هاي پنل رابط را به يكي از پورت‌هاي هاب متصل مي‌كنند.

نكته: هدف از اين درس معرفي روند كابل‌كشي از پريز نصب شده روي ديوار به محل پنل رابط مي‌باشد. براي اطلاعات بيشتر در زمينه‌ي پريزهاي ديواري، پنل‌هاي رابط و طريقه‌ي نصب كابل‌ها به آنها به درس دوم از همين فصل تحت عنوان «ايجاد اتصالات» رجوع كنيد.
كابل‌ها كه در كابل شبكه توكار استفاده مي‌شوند. كانكنتور و به صورت پيچيده شده دور قرقره‌هاي بزرگي عرضه مي‌شوند. نصاب به اندازه‌ي لازم كابل را از دور قرقره باز و جدا مي‌كند و يك سر آنرا به سوكت پريز روي ديوار و سر ديگر را به يكي از سوكت‌هاي پنل رابط متصل مي‌كند. كابل‌هاي پيش‌ساخته با رابط، خود داراي كانكتورهاي RJ-45 مي‌باشند. اما در صورت نياز مي‌توانيد كانكتورهاي RJ-45 را جداگانه خريداري كنيد و كابل‌هاي و كابل‌هاي رابطي به طول دلخواه بسازيد به اينصورت در مصرف كابل نسبت به زمانيكه از كابل‌هاي پيش‌ساخته استفاده مي‌شود،بطور قابل توجهي صرفه‌جويي مي‌شود. در كابل‌كشي توكار براي متصل كردن كانكتور به دو انتهاي كابل‌ها، بايد مجهز به ابزار مخصوص اينكار باشيد. مزيت استفاده از اين نوع كابل‌ها اينست كه چون بدون كانكتور هستند كار با آنها ساده‌تر است، در انتخاب كانكتورها محدوديت كمتري وجود دارد و با خريد كابل به صورت عمده در هزينه صرفه‌جويي مي‌شود. رشته سيم‌هاي داخل كابل‌هاي رابط معمولاً از نوع افشان هستند، در نتيجه اين نوع كابل‌ها انعطاف‌پذير هستند. اما استفاده از از اين كابل‌ها در كابل‌كشي توكار بدين دليل نياز به استفاده از اتصالات Punchodown (كانكتورهاي مادگي RJ-45 به دو سر هر كابل توكار متصل شوند و با آچار مخصوص پرس شوند) مشكل است.
رشته سيم‌هاي كابل‌هايي كه در كابل‌كشي توكار استفاده مي‌شوند معمولاً از نوع غيرافشان هستند كه براي استفاده در كانكتورهاي punchdowm مناسبترند. اين كابل‌ها كمي از كابل‌هاي متشكل از سيم‌هاي افشان ارزانتر هستند و در مقابل تضعيف مقاومت بيشتري دارند. در نتيجه فواصل طولاني‌تري را مي‌توان با استفاده از آنها كابل‌كشي كرد.
نكته: گرچه در استاندارد اترنت استفاده از كابل‌هايي با حداكثر طول 100 متر مجاز است اما بندرت مي‌توان كابل‌هاي پيش‌ساخته‌اي به اين طول پيدا كرد. در يكي از دلايل عدم وجود چنين كابل‌هايي اينست كه كابل‌هاي پيش‌ساخته متشكل از سيم‌هاي افشان مي‌باشند. براي فواصل بيش از 30 متر (در واقع كابل‌هاي بيش از 30 متر) بايد از كابل‌هاي متشكل از سيم‌هاي غيرافشان استفاده كرد. البته گاهي مي‌توان كابل‌هاي پيش‌ساخته‌ي غيرافشان هم از توليدكنندگان بخصوصي تهيه كرد.
اغلب كارهاي كابل‌كشي توكار را كساني انجام مي‌دهند كه هم در كابل‌كشي خطوط تلفن هم كابل‌هاي شبكه مهارت دارند. همانطور كه قبلاً اشاره شد هر جا كه امكان داشته باشد كابل‌كشي تلفن و شبكه همزمان انجام مي‌شود. در چنين شرايطي چون كابل‌ها در كنار همديگر كشيده مي‌شوند و معمولاً مشابه همديگر هستند برچسب‌زدن به تك‌تك كابل‌ها از

اهميت خاصي برخوردار است تا بعد از نصب مجبور نشويد براي پيدا كردن دو سر هر يك از كابل‌ها كار خود را از اول و مرحله به مرحله دنبال كنيد.
بطور كلي كابل‌كشي توكار شامل مراحل زير مي‌شوند:
1-محل كامپيوترها و دستگاه‌هاي ديگري كه بايد به شبكه متصل شوند را تعيين كنيد و نقطه‌اي مركزي و ايمن براي استقرار هاب‌ها و پنل رابط در نظر بگيريد يك سر از همه‌ي كابل‌ها بايد به پنل رابط متصل شود بنابراين در انتخاب محل نصب آن دقت كنيد كه فضاي كافي براي كار را داشته باشد و احتمالاً نزديك منابع توليدكننده‌ي اختلالات الكترومغناطيسي نباشد.
2-مسير تك‌تك كابل‌ها از پنل رابط به پريزهاي نصب شده روي ديوارها را با توجه به موانع سر راه از قبيل وسايل روشنايي، كانال‌هاي كولر و تهويه‌ي مطبوع، مشخص كنيد.
3-قرقره‌ي كابل را نزديك محل نصب پنل رابط قرار دهيد و سر كابل آنرا با نام نقطه‌ي مورد نظر (جايي كه مي‌خواهيد كابل را به آن نقطه بكشيد) برچسب بزنيد.
4-سر كابل را از مسير خود به پريز مقصد از ميان ديوار، سقف يا كف ساختمان عبور دهيد و تا زمانيكه دقيقاً به پريز مورد نظر نرسيده‌ايد آنرا از قرقره جدا نكنيد. براي اطمينان بيشتر حدود يك يا دو متر طول هر يك از كابل‌ها را اضافه بگيريد تا زمان ايجاد اتصالات يا استقرار تجهيزات دچار مشكل نشويد.
5-كابل‌ها را در مسير خود محكم بصورتيكه از جاي خود نتوانند تكان بخورند و يا توسط افراد ديگري كه ممكن است بعداً در همان مسير كاري انجام دهند آسيب نبينند.
6-انتهاي ديگر كابل را با نام محل پريز برچسب بزنيد و آنرا از قرقره جدا كنيد. هرگز قبل از برچسب زدن، كابل را از قرقره جدا نكنيد.
7-روند ايجاد اتصالات را همانطور كه در درس بعد توضيح داده شده است دنبال كنيد.
پيچيدگي كار كابل‌كشي به اندازه‌ي زيادي به بناي سايت بستگي دارد. كم‌دردسرترين سايت‌ها آنهايي هستند كه با ديوارهاي از جنس تخته‌هاي گچي و سقف‌هاي دو جداره بنا شده‌اند. در اين سايت‌ها معمولاً براحتي مي‌توانيد كابل‌ها را از ميان سقف تا اتاق مورد نظر عبور دهيد و از ميان ديوار پايين بياندازيد و به پريز نصب شده روي ديوار وصل كنيد. البته چنين پروژه‌هايي كه هيچ دردسري نداشته باشند بندرت پيدا مي‌شوند و معمولاً موانع زيادي وجود دارد كه نصاب در حين كار با آنها مواجه مي‌شود. از جمله‌ي اين موانع مي‌توان منابع توليدكننده‌ي اختلالات الكترومغناطيسي كه روي سيگنال‌هاي داده تأثير مي‌گذارند، آتش‌شكن‌ها كه از عبور كابل از سقف به پايين جلوگيري مي‌كنند. عايق‌بندي‌ها، كانال‌هاي سيستم تهويه‌ي ساختمان، تجهيزات روشنايي، تيرچه‌هاي بتوني و تيرآهن را نام برد. تمام اين موانع بايد در طول مرحله‌ي برنامه‌ريزي براي ايجاد شبكه مورد بررسي

قرار گرفته باشند و مسير مناسبي براي هر يك از كابل‌ها مشخص شده باشد.
در بعضي از ساختمانها ممكن است شرايطي حاكم باشد كه با كابل‌كشي توكار اصلاً امكانپذير نباشد و يا حداقل بسيار مشكل باشد. اگر به هيچ صورتي به داخل سقف و ديوارها دسترسي وجود ندارد از روش‌هاي ديگري مثل داكت‌هايي كه روي سطح نصب مي‌شوند و قبلاً هم در همين فصل مورد بررسي قرار گرفتند استفاده كنيد.

نصب كابل‌ها

همانطور كه قبلاً گفته شد براي كشيدن يك كابل از پنل رابط به يكي از پريزها بايد قرقره‌ي كابل را كنار پنل رابط قرار دهيد. مقداري از كابل آنرا باز كنيد و با در نظر گرفتن مقداري اضافه آنرا از سقف به محل مورد نظر بكشيد و سپس از قرقره جدا كنيد برچسب يا نشانه‌گذاري روي دو سر هر كابل را فراموش نكنيد. بگونه‌اي كه بتوانيد كابل‌ها را به راحتي از همديگر تشخيص دهيد. رسم يك نقشه يا نمودار از كل كابل‌كشي ساختمان همراه با نام و مسير تك‌تك كابل‌ها نه تنها در حين كابل‌كشي بسيار مهم است بلكه بعداً زمان اشكال‌زدايي شبكه هم كمك بزرگي خواهد بود.
نكته: در حين كابل‌كشي بد نيست كه هر يك از كابل‌ها را مقداري اضافه بگيريد تا اگر به هر دليلي شما يا شخص ديگري بخواهد جاي يكي از پريزها يا پنل رابط را تغيير دهد مشكلي وجود نداشته باشد. اين مقدار اضافه را مي‌توانيد به راحتي در سقف يا داخل ديوار پنهان كنيد. مشكل‌ترين بخش كابل‌كشي توكار، كشيدن كابل‌ها از ميان سقف است. براي انجام اينكار اگر دو نفر حضور داشته باشند، كار به مراتب ساده‌تر مي‌شود. به اينصورت كه يك نفر كابل را از ميان سقف به شخص ديگر كه در طرف ديگر است مي‌دهد. ابزاري كه براي اينكار استفاده مي‌شوند در حين سادگي داراي اهميت خاص خود مي‌باشند. علاوه بر دو يا چند نردبان نصاب‌هاي حرفه‌اي از ابزار ديگري هم استفاده مي‌كنند كه ممكن است باعث تعجب شما شوند. از جمله ابزار با ارزش براي يك نصاب يك تكه ريسمان يا كامواي محكم مي‌باشد. در صورتيكه قرار باشد چند كابل به نقاطي نزديك به همديگر كشيده شوند مي‌توانيد يك سر ريسمان را به يكي از كابل‌ها ببنديد و بعد از كشيدن آن كابل به مقصد مورد نظر سر ديگر ريسمان را به كابل ديگري ببنديد و آنرا از ميان سقف به همان نقطه‌ي قبلي بكشيد. البته ابزار آماده‌اي به اين نيت در بازار وجود دارد
براي عبور كابل از سقف مي‌توانيد از اين روش استفاده كنيد يك نفر از يك طرف سقف مقداري از كابل را كلاف كند و به سمت نفر ديگر پرت كند. البته پرت كردن اين كلاف در سقف‌هايي كه فضاي بين دو جدا آنها كم است

مشكل مي‌باشد و در چنين شرايطي از روش‌هاي ديگري استفاده مي‌شود كه معمولاً ابتكاري هستند.
ابزاري كه از آن بصورت عمومي براي عبور كابل از ميان فضاي سقف استفاده مي‌شود telepole نام دارد. telepole ميله‌اي است تلسكوپي از جنس پلاستيك با نوعي فلز كه بيشتر شبيه به ميله‌هاي ماهيگيري مي‌باشد و طول آنها را مي‌توان با جمع كردن و باز كردن كم و يا زياد كرد. در انتهاي اين وسيله قلابي براي گرفتن كابل وجود دارد . طريقه‌ي استفاده از telepole به اينصورت است كه به آن يك سر كابل را بايد ببنديد و در حالت جمع شده داخل سقف وارد كنيد و آنرا آنقدر باز كنيد تا به نفر دوم كه در سمت ديگر است برسد. اين روش بسيار كارا است ولي بسياري از نصاب‌ها به اين نتيجه رسيده‌اند كه بدون telepole هم مي‌توان اينكار را انجام داد و به جاي آن مثلاً از يك تكه چوب يا ميله‌اي پلاستيكي استفاده مي‌كنند. با كمي تمرين اينكار را حتي با يك توپ تنيس هم مي‌توان انجام داد. به اينصورت كه مقداري از تكه‌اي به حد لازم ريسمان را به دور آن بپيچيد، سر ديگر ريسمان را به يك كابل ببنديد، بعد توپ را به سمت ديگر پرت كنيد و از آنطرف با كشيدن ريسمان متصل به كابل، كابل را به سمت خود بكشيد، و از سقف عبور دهيد.

محكم كردن كابل‌ها

محكم كردن كابل‌هايي كه به صورت توكار نصب شده‌اند هم به اندازه‌ي كابل‌هاي روكار داراي اهميت است. توجه داشته باشيد كه تنها شما نيستيد كه به داخل سقفهاي ساختمان دسترسي داريد. سرويس كارهاي ديگر هم به تجهيزات روشنايي، كانال‌هاي تهويه‌ي هوا و بخش‌هاي ديگر دسترسي دارند و با محكم كردن كابل‌ها اين تضمين بوجود مي‌آيد. كه در آينده از جاي خود تكان نمي‌خورند و آسيب نخواهند ديد و يا در ميدان‌هاي الكترومغناطيسي قرار نخواهند گرفت.
بعد از عبور كابل‌ها از ميان سقف بايد آنها را از ميان ديوار به پايين يعني جايي كه قرار است پريز روي ديوار نصب شود بياندازيد. در بناي ديوارهاي اغلب ساختمانهاي تجاري تيرهاي آهني عمودي استفاده مي‌شود كه معمولاً تيرهاي افقي وجود ندراد. در نتيجه در چنين بناهايي براي عبور كابل از سقف به پشت پريزهاي ديواري با مانعي برخورد نخواهيد كرد. سوراخي براي نصب پريز روي ديوار ايجاد كنيد، كابل را از سقف به پايين و از سوراخ بيرون بكشيد و به كانكتور پريز وصل كنيد، اضافه‌ي كابل را داخل ديوار كنيد و سوراخ را با نصب پريز روي ديوار بپوشانيد.
اگر با تير افقي ديوار برخورد كرديد كه مانع از عبور كابل بشود چندين راه وجود دارد. اول اينكه مي‌توانيد سوراخ ديگري در ديوار ايجاد كنيد تا بتوانيد از طريق آن تير افقي را سوراخ كنيد. اگر اين تير از جنس چوب باشد كار بسيار راحت‌تر است اما به هر حال بعداً بايد ديوار را وصله كنيد و روي سوراخ

اضافي را بپوشانيد راه ديگر اينست كه پريز را به جاي ديگري كه احتمال مي‌دهيد از آن مسير تير افقي عبور نكرده است و يا حداقل راهي براي عبور كابل وجود دارد تغيير مكان دهيد و بعنوان آخرين چاره مي‌توانيد از عبور كابل از داخل ديوار بگذريد و بجاي آن از داكت استفاده كنيد. گرچه اين روش به تميزي عبور كابل از داخل ديوار نمي‌باشد ولي به هر حال از آويزان كردن كابل از سقف بهتر است.
همانند عبور كابل‌ها به صورت افقي ابزاري هم براي كابل‌كشي عمودي از ميان ديوار وجود دارد كه به عنوان مثال مي‌توان Fish tape را نام برد. Fish tape در واقع نواري است انعطاف‌پذير از جنس آهن يا فايبرگلاس كه دور حلقه‌اي پيچيده است و به سر آن قلابي متصل است. روش استفاده از اين وسيله به اينصورت است كه نوار آنرا بايد با كمي فشار كمي از سوراخ ايجاد شده روي ديوار به سقف بفرستيد، كابل را به قلاب سر نوار ببنديد و با جمع كردن نوار به پايين بكشيد و از سوراخ خارج كنيد. از اين وسيله مي‌توانيد براي كشيدن كابل از سوراخ روي ديوار به سقف و يا از سقف به طبقه‌ي بالا هم استفاده كنيد. بنابر نوع و محل نصب پنل رابط ممكن است لازم باشد انتهاي ديگر كابل را هم از ميان ديوار عبور دهيد. در شبكه‌هاي كوچك معمولاً از پنل‌هاي رابطي استفاده مي‌شود كه روي ديوار نصب مي‌شوند و شما مي‌توانيد كابل‌ها را به پشت سوراخي كه پنل نهايتاً روي آنرا مي‌پوشاند بياندازيد. در شبكه‌هاي بزرگتر معمولاً از تجهيزاتي استفاده مي‌شود كه داخل Rack (قفسه‌اي مخصوص براي تجهيزات شبكه) سوار مي‌شوند. در اينصورت هم سر ديگر كابل‌ها بايد از سقف به پشت Rack كشيده شوند.

طريقه‌ي نصب كابل‌هاي ديگر

نصب كابل‌هاي UTP به دليل نازكي و انعطاف‌پذيري ساده است. اما كابل‌هاي ديگر داراي ويژگيهاي مخصوص به خود مي‌باشند كه روند نصب را كمي مشكل مي‌كند. كابل‌هاي كواكسيال RG-58 كه در شبكه‌هاي اترنت نازك به كار مي‌روند در مقايسه با كابل‌هاي UTP ، سنگين‌تر و داراي قابليت انعطاف پايين‌تر مي‌باشند ولي قطر آنها تقريباً يكسان است. بنابراين از اين كابل‌ها هم مي‌توان به صورت توكار استفاده كرد اما نصب آنها به سادگي كابل‌هاي UTP نمي‌باشد. بزرگترين مشكل در كابل‌كشي توكار كابل‌هاي كواكسيال اينست كه شبكه‌هاي اترنت نازك از توپولوژي باس استفاده مي‌كنند. در نتيجه در چنين شبكه‌هايي بايد يك تكه كابل از كامپيوتري به كامپيوتر دگير و سپس از كامپيوتر دوم تكه‌اي به كامپيوتر سوم و همينطور الي آخر كشيده شود. بنابراين در اين آرايش به ازاي هر كامپيوتر دو كابل از ديوار بيرون مي‌آيد كه بايد به كانكتور T شكل متصل به كارت شبكه‌ي آن كامپيوتر متصل شوند.
در شبكه‌هاي اترنت Thick (ضخيم) از كابل‌هاي كواكسيال RG-8 استفاده مي‌شود كه قطر آنها تقريباً نيم اينچ و بسيار خشك مي‌باشند. از اين نوع

كابل‌ها امروزه ديگر استفاده نمي‌شود ولي حتي در دوران خود هم بندرت بصورت توكار نصب مي‌شدند. مزيت اترنت Thick بر اترنت Thin (نازك) اينست كه هر كامپيوتر از يك قطعه كابل مجزا كه كارت شبكه را به خط RG-8 اصلي وصل مي‌كند استفاده مي‌كند. در نتيجه در اين شبكه‌ها فقط يك كابل از ديوار بيرون مي‌آيد. نصب كابل‌هاي فيبر نوري تقريباً مشابه با كابل‌هاي UTP مي‌باشد. فيبرهاي چند مدي كه از آنها در اغلب ارتباطات LAN استفاده مي‌شود به حد كافي انعطاف‌پذير مي‌باشند، اما بدليل ماهيت فيزيكي رسانه، شعاع انحناي كابل در جايي كه لازم است خم شود بايد حساب شده باشد. مزيت كابل‌هاي فيبر نوري بر كابل‌هاي مسي اينست كه تداخلات الكترومغناطيسي روي آنها تأثير ندارد و در نتيجه بسياري از موانعي كه در نصب كابل‌هاي مسي بايد دور زده شده شوند (مثل تجهيزات روشنايي فلورسانت) در نصب كابل‌هاي فيبر نوري اهميت ندارند.

کابل کشی شبکه

ایجاد کابل اتصال کامپیوتر به هاب (معروف بـه کابـل هـایstraight-through)

کابـل کشـی شـبکه یکـی از مراحـل مهـم در زمـان پیـاده سـازی یـک شـبکه کامپیوتری است که می بایست با دقـت، ظرافـت خـاص و پایبنـدی بـه اصـول کابل کشی ساختیافته ، انجام شود. برای ایجاد کابـل هـای UTP از تجهیـزات زیر استفاده می گردد:

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

یکی از عوامـل تـاثیر گـذار در پشـتیبانی و نگهـداری یـک شـبکه ، نحـوه کابـل کشی آن است . بـا رعایـت اصـول کابـل کشـی سـاختیافته ، در صـورت بـروز اشکال در شبکه ، تشخیص و اشکال زدائـی آن بـا سـرعتی مناسـبی انجـام خواهد شد .

مراحل ایجاد یک کابل : بدون هیچگونه توضیح اضافه !

مرحله اول مرحله دوم مرحله سوم مرحله چهارم مرحله پنجم





مدل های متفاوت کابل کشی کابل های UTP

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

- زوج اول : آبی و سفید/ آبی
- زوج دوم : نارنجی و سفید /نارنجی
- زوج سوم : سبز و سفید/ سبز
- زوج چهارم : قهوه ای و سفید / قهوه ای

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

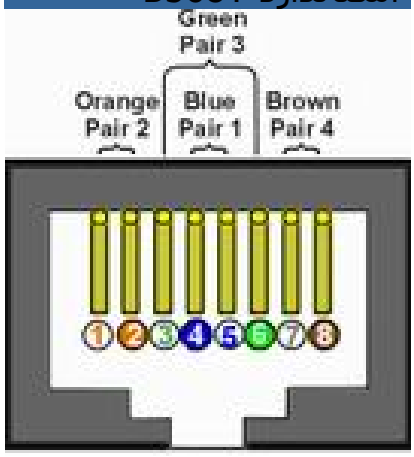
ایجاد یک کابل UTP به منظور اتصال کامپیوتر به هاب (معروف به کابل های Straight)

اترنت عموما" با استفاده از هشت کابل هادی به همراه هشت پین ماژولار plugs/jacks ، داده را حمل می کند . کانکتور استاندارد، RJ-45 نامیده شده و مشابه کانکتور استاندارد RJ-11 است که در تلفن استفاده می گردد. یک رشته کابل CAT5 شامل چهار زوج سیم بهم تابیده است که هر زوج دارای دو رشته سیم با رنگ هائی خاص است . (یک رشته رنگی و یک رشته سفید با نواری به رنگ رشته زوج مربوط) . به منظور تسهیل در امر نگهداری ، می بایست به اندازه ضروری سیم های بهم تابیده را از حالت پیچش خارج نمود (مثلا" حدود یک سانتیمتر) . زوج های در نظر گرفته شده برای اترنت ده و یکصد مگابیت به رنگ نارنجی و سبز می باشند . از دو زوج دیگر (رنگ قهوه ای و آبی) می توان به منظور یک خط اترنت دوم و یا اتصالات تلفن استفاده نمود .

به منظور کابل کشی کابل های UTP از دو استاندارد متفاوت با نام T-568B (یا EIA) و T-568A (یا T&AT ، A258) ، استفاده می گردد . تنها تفاوت موجود بین آنان ترتیب اتصالات است.

شماره پین های استاندارد T568B
همانگونه که در جدول زیر مشاهده می گردد ، شماره پین های فرد همواره سفید بوده که با یک نوار رنگی پوشش داده می شوند.

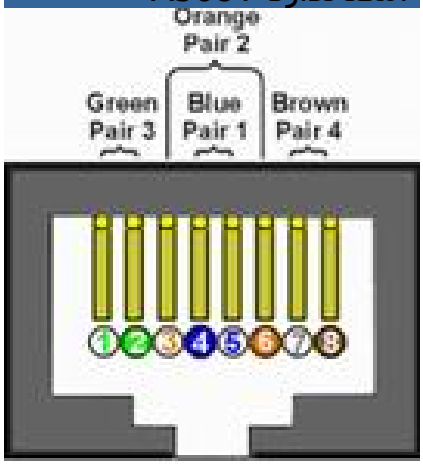
استاندارد B568T



کد رنگ ها در استاندارد B568T			
شماره پین	رنگ	زوج	کاربرد
یک	سفید/ نارنجی	دوم	Tx Data+
دو	نارنجی	دوم	TX Data-
سه	سفید / سبز	سوم	RecvData+
چهار	آبی	یک	
پنج	سفید /آبی	یک	
شش	سبز	سوم	RecvData-
هفت	سفید/قهوه ای	چهارم	
هشت	قهوه ای	چهارم	

شماره پین های استاندارد T568A
در استاندارد T568A ، اتصالات سبز و نارنجی برعکس شده است ، بنابراین زوج های یک و دو بر روی چهار پین وسط قرار می گیرند (سازگاری با اتصالات telco voice) .

استاندارد A568T

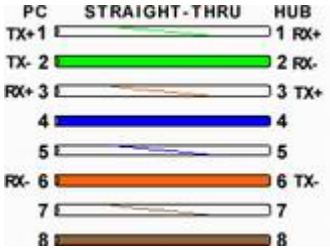


کد رنگ ها در استاندارد A568T			
شماره پین	رنگ	زوج	کاربرد
یک	سفید/ سبز	سوم	RecvData+
دو	سبز	سوم	RecvData-
سه	سفید / نارنجی	دوم	TX Data+
چهار	آبی	یک	
پنج	سفید /آبی	یک	
شش	نارنجی	دوم	TX Data-
هفت	سفید/قهوه	چهارم	

	ای		
هشت	قهوه ای	چهارم	

موارد استفاده

متداولترین کاربرد یک کابل straight ، اتصال بین یک کامپیوتر و هاب /سوئیچ است . در چنین مواردی ، کامپیوتر مستقیما" به هاب و یا سوئیچ متصل شده که به صورت اتوماتیک و با استفاده از مداراتی خاص، کابل cross over می گردد .



شکل فوق یک اتصال استاندارد straight در کابل های CAT5 را نشان می دهد که از آن به منظور اتصال یک PC به هاب استفاده می گردد . ممکن است با مشاهده شکل فوق انتظار داشته باشید که +TX یک طرف به +TX طرف دیگر متصل گردد(عملا" این اتفاق نیافتاده است) . زمانی که یک PC به هاب متصل می گردد ، هاب به صورت اتوماتیک و با استفاده از مدارات داخلی خود کابل را X-over نموده و بدین ترتیب ، پین شماره یک از کامپیوتر (TX +) به پین شمار یک هاب (RX +) متصل می گردد .
در صورتی که هاب عملیات x-over را انجام ندهد (در زمان استفاده از پورت Uplink) ، پین شماره یک کامپیوتر (+ TX) به پین شماره یک هاب (+ TX) متصل می گردد . بنابراین مهم نیست که چه نوع عملیاتی را با پورت HUB انجام می دهیم (Uplink و یا نرمال) ، سیگنال های نسبت داده شده به هشت پین سمت PC ، همواره یکسان باقی مانده و هاب با توجه به نوع استفاده از پورت (نرمال و یا Uplink) عملیات لازم را انجام خواهد داد .

ایجاد اتصالات

بعد از انجام كابل كشي نوبت آن مي رسد كه براي اينكه كامپيوتر ها بتوانند از طريق هاب با همديگر ارتباط برقرار كنند، اتصالات لازم را انجام دهيد. بنابر نوع كابل كشي كه انجام داده ايد (روكار و يا توكار) ايجاد چنين اتصالاتي مي‌تواند بسيار ساده و يا كاملا پيچيده باشد. در بعضي شرايط بايد با كار هر يك از سيمها ي داخل كابل UTP آشنا باشيد و در بعضي از موارد هم حتي نيازي به مشاهده آن سيم ها نمي باشد.
بعد از مطالعه اين درس قادر خواهيد بود:
روش سيم كشي يك كابل ضربدري (crossover) را توضيح دهيد.

اتصالات لازم در كابل هايي كه بصورت روكار كشيده شده اند را تكميل كنيد.
با استفاده از آچار Punchdown به سر كابل ها سوكت بزنيد.
با استفاده از كانكتورهاي RJ-45 كابل رابط بسازيد.
شبكه اي متشكل از فقط دو كامپيوتر
ساده ترين نوع شبكه متشكل از دو كامپيوتر مجهز به كار ت شبكه مي باشد كه بوسيله يك كابل به همديگر متصل شده اند. اگر هر دو كامپيوتر ها در يك اتاق مستقر باشند، كابل كشي بين آنها بايد ساده باشد. اما اگر فاصله آنها از همديگر زياد باشد و بخصوص در طبقات مختلفي از يك ساختمان قرار داشته باشند، كابل كشي بين آنها نياز به كمي دقت و حوصله خواهد داشت.
زماني كه در شبكه هاي اترنت از كابل هاي كواكسيال استفاده مي شد، اين امكان وجود داشت كه كارتهاي شبكه دو كامپيوتر را فقط به وسيله يك كابل اترنت نازك (thin Ethernet) به همديگر متصل كنيم و يك شبكه ساده ايجاد كنيم. اما امروزه كابل استاندارد براي شيكه هاي اترنت كابل هاي UTP مي باشد و براي استفاده از آنها اصولا به هاب هم نياز است.
اگر دو كارت شبكه اترنت را مستقيما و بدون استفاده از هاب با يك كابل UTP به همديگر متصل كنيد، اين عمل جابجايي سيگنال ها صورت نمي گيرد در چنين شرايطي براي اينكه اين دو كامپيوتر بتوانند با همديگر كار كنند بايد از يك كابل ضربدري (crossover) استفاده كنيد. با استفاده از كابل هاي ضربدري، پايه هاي فرستنده هر يك از كانكتورها به پايه هاي گيرنده كانكتور ديگر متصل مي شود.
نكته: يكي از محدوديت هاي استفاده از اترنت در يك شبكه فاقد هاب اينست كه فاصله بين اين دو كامپيوتر نمي تواند بيش از 100 متر باشد. در يك شبكه UTP استاندا‌د، هاب كار يك تكراركننده را انجام مي دهد. در نتيجه هر كابل متصل شده به هاب مي تواند 100 متر باشد. بنابراين اگر فقط از يك هاب در شبكه خود استفاده كنيم فاصله بين هر دو كامپيوتر تا حداكثر 200 متر باشد.
اگر دو كامپيوتري را كه قرار است به همديگر متصل كنيد در يك اتاق قرار دارند مي توانيداز كابل هاي ضربدري آماده كه در بازار موجود مي باشد استفاده كنيد. البته توجه داشته باشيد كه اگر به كابل طولاني احتياج داشته باشيد احتمالا مجبور خواهيد شد سفارش دهيد تا كابل مورد نظرتان ساخته شود.
اما اگر قرار است دو كامپيوتري را به همديگر متصل كنيد كه در يك اتاق قرار ندارند، احتمالا مجبور خواهيد شد از كابل كشي توكار استفاده كنيد و كابل را از ديوار، سقف و يا كف زمين رد كنيد. كابل مورد استفاده در يك ارتباط ضربدري با كابل مورد استفاده در شبكه هايي كه با هاب پياده ساري مي شوند تفاوت ندارد و روش كشيدن آن به همامن صورتي است كه در درس اول تحت عنوان كابل كشي آموزش داده شد. تنها تفاوت بين كابل هاي

ضربدري و كابل كشي استاندارد در آرايش و نحوه وصل كردن سيم هاي آنها به كانكتورهاي انتهايي كابل مي باشد.
يك كابل UTP متشكل از هشت رشته سيم مي باشد كه دو به دو به همديگر پيچيده اند. كانكتورهاي RJ- 45ي كه به دو انتهاي كابل متصل مي شودند(اگر كابل از نوع كابل رابط باشد اين كانكتورها نري و اگر پريزهاي رو ديواري و يا پنل رابط باشد، اين كانكتور مادگي مي باشند) داراي هشت پايه هادي هستند.كه هشت رشته سيم كابل بايد به آنها متصل شوند. به اينصورت وقتي يك كانكتور نري را به يك كانكتور مادگي مي زنيد ارتباط بين تك تك پايه هاي هادي برقرار مي شود.
نكته: در شبكه هاي 10Base-T و 100Base-TX فقط از چهار رشته سيم از هشت رشته كابل UTP استفاده مي شود. ولي در شبكه هاي 10Base-T4 هر هشت رشته بكار رفته مي شود. چهار پايه اي كه بعنوان بي استفاده معرفي در يك شبكه 10Base-T يا 100Base-T4 براي انتقال سيگنال در هر دو جهت بكار مي روند.
در كابل كشي استاندارد و كابل هاي رابط از روش Straight-through براي متصل كردن پايه هاي دو كانكتور به همديگر استفاده مي شود. در اين روش دو انتهاي هر رشته سيم به پايه هاي يكسان در هر دو كانكتور متصل مي شود. بعنوان مثال پايه هاي فرستده در يك طرف به پايه هاي فرستنده طرف ديگر متصل مي شوند. دليل ايجاد چنين آرايشي اين است كه عمل جابجايي سيگنال ها بين سيم هاي فرستده يك كامپيوتر و سيم هاي فرستده كامپيوتر ديگر توسط مدار ضربدري هاب انجام مي شود. به اينصورت كار كسي كه كابل كشي را انجام مي دهد به مراتب ساده تر مي شود.
براي ايجاد يك كابل ضربدري بايد دو پايه فرستنده را با پايه هاي گيرنده مشابه خود در طرف ديگر متصل كنيد.
پايه +TD يك طرف به +RD طرف ديگر به همين طورت دو پايه -TD به دو پايه -RD متصل مي شوند. توجه داشته باشيد كه نمي توان يك كابل ضربدري را به هاب متصل كرد، چون مدار ضربدري داخل هاب و مدار ضربدري كابل همديگر را خنثي مي كنند. بعبارت ديگر پايه +TD كه در كابل به پايه +RD متصل شده با عبور از مدار ضربدري هاب دوباره به پايه +TD داخل هاب متصل مي شود. تنها وقتي مي توانيد از يك كابل ضربدري با هاب استفاده كنيد (بعنوان مثال براي گسترش شبكه) كه آنرا به پورت Uplink هاب متصل كنيد، چون اين پورت هاي از مدار ضربدري هاب نمي گذرد.

Pin 1	TD+
Pin 2	TD-
Pin 3	RD+
Pin 4	UnUsed
Pin 5	UnUsed

Pin 6	RD-
Pin 7	UnUsed
Pin 8	UnUsed

ايجاد اتصالات لازم در كابل كشي روكار

اگر از كابل كشي روكار و كابل هاي از پيش ساخته استفاده كرده باشيد فقط كافي است كه آنها را به كامپيوترها و هاب متصل كنيد تا انجام اتصالات لازم تكميل شود. هاب خود را در مكاني مركزي قرار دهيد(ترجيحا جايي كه عبور و مرور حدلقل ممكن باشد) و آنرا به برق بزنيد و كانكتورهاي كابل ها را يكي يكي به پورتهاي آن وارد كنيد. توجه داشته باشيد كه براي متصل كردن يك كامپيوتر به هاب از پورت Uplink نمي توانيد استفاده كنيد مگر اينكه اين پورت مجهز به سوئيچي براي فعال كردن مدار ضربدري باشد. در اغلب هاب ها به ازاي هر يك از پورت ها يك LED وجود دارد. اين LED در صورتي روشن مي شوند كه طرف ديگر كابل ها به كامپيوتر متصل شده و كامپيوتر ها روشن باشد. طرف ديگر هر يك از كابل ها بايد به يك كامپيوتر متصل باشدو كامپيوترها را خاموش كنيد و كابل ها را يكي يكي به كارتهاي شبكه هر يك از آنها متصب كنيد. هم در مورد هاب و هم در مورد كارتهاي شبكه وقتي كابل درست در آنها وارد شود يك صداي تيك شنيده مي شود. در اغلب كارتهاي شبكه، كنار كانكتور RJ-45 يك LED وجود دارد، البته در مادربوردهايي كه خود مجهز به آداپتور رابط شبكه مي باشند ممكن است كه اين LED قابل رويت نباشد. زمانيكه كارت شبكه به يك هاب در حال كار وصل شود،LED آن روشن مي شود. زمانيكه كامپيوتر روشن مي شود، كارت شبكه سيگنالي به نام Link pulse ايجاد مي كند و روي كابل مي فرستد، هاب با دريافت اين سيگنال بوسيله سيگنال ديگري به كارت شبكه پاسخ مي دهد. اگر هاب و يا كارت شبكه از نوع Fast Ethernet باشند از سيگنال Link pulse براي توافق بر سر سريعترين سرعت مشترك استفاده مي كنند. بعنوان مثال اگر يك كارت شبكه dual – speed را به يك هاب Fast Ethernet وصل كنيد، سيگنال Link pulse آنها را قادر مي سازد، تشخيص دهند كه هر دو مي توانند در سرعت 100Mbps كار كنند سپس خود را طوري پيكر بندي مي كنند كه بتوانند از اين سرعت استفاده كنند.

اما اگر يك كارت شبكه dual – speed را به يك هاب اترنت استاندارد متصل كنيد، كارت شبكه متوجه مي شود كه بايد در سرعت 10Mbps كار كند و خود را با اين شرايط وفق مي دهد. پس از اتمام تبادل سيگنال هاي Link pulse حتي اگر درايور كارت شبكه نصب نشده باشد هم LED هاب و هم كارت شبكه بايد روشن شوند. در بعضي از كارتهاي شبكه dual – speed دو LED وجود دارد. با فرض اينكه LED هاي روي هاب و كارت شبكه روشن شده

باشند، نصب سخت افزاري شبكه كامل شده است. بعد از نصب مولفه هاي نرم افزاري مربوط به شبكه بندي، شبكه شما بايد بكار بيفتد.

ايجاد اتصالات لازم در كابل كشي توكار

اگر كابل كشي شما بصورت توكار انجام شده باشد ايجاد اتصالات لازم براي اتمام نصب سخت افزاري شبكه كمي از حالت كابل كشي روكار پيچيده تر است. مراحلي كه بايد براي متصل كردن هر يك از كابل ها به كامپيوترها و هاب، انجام شوند از قرار زير مي باشد:

1- يك طرف كابل را به يكي از پورتهاي روي پنل رابط وصل كنيد.
2- با استفاد از يك كابل رابط، پورت پنل رابط را به يكي از پورتهاي هاب وصل كنيد.
3- طرف ديگر كابل را به پورت پريز روي ديوار وصل كنيد.
4- پريز را روي ديوار نصب كنيد.
5- با استفاده از يك كابل رابط، پورت پريز روي ديوار را به كارت شبكه وصل كنيد.

كانكتورها و ابزار لازم

در كابل كشي توكار نياز به ابزار خاصي براي نصب كانكتورها و ايجاد اتصالات مي باشد. در اغلب كابل كشي هاي توكار در سمتي كه قرار است كامپيوتر مستقر شود از پريزهاي ديواري و در طرف ديگر از پنل هاي رابط استفاده مي شود. پريزهاي ديواري كه در شبكه ها بكار برده مي شوند مشابه با پريزهاي برق مي باشند با اين تفاوت كه داراي كانكتور مادگي RJ-45 هستند. پشت اين پريزها كانكتوري وجود دارد كه به سيم هاي داخل كابل UTP وصل مي شود. پس از نصب پريز روي ديوار فقط روي پريز قابل رويت مي باشد و كابل ها داخل ديوار مخفي مي شوند. سپس مي توانيد با استفاده از يك كابل رابط، كامپيوتر مورد نظر را به سوكت موجود روي پريز متصل به ديوار وصل كنيد. پريزهاي در انواع مختلفي عرضه مي شوند. شما مي توانيد از پريزهايي استفاده كنيد كه در خود داراي يك، دو، چهار و يا بيشتر سوكت با كاربردهاي متفاوت مي باشند. بعنوان مثال اين امكان وجود دارد كه كابل هاي داده و خطوط تلفن كنار همديگر نصب شوند و از يك پريز بعنوان پايانه هر دو استفاده شود. در اينصورت براي اينكه كاربران دچار مشكل نشوند برچسبي به نشانه كاربرد هر يك از سوكت ها روي آنها بچسبانيد. توجه: گرچه ترجيح داده مي شود كه از يك پريز هم براي خطوط تلفن و هم كابل هاي شبكه استفاده شود، اما كابل هاي اين دو سرويس بايد مجزا باشند، بعضي از افراد تصور مي كنند كه چون در كابل هاي UTP شبكه هاي اترنت معمولي دو زوج از سيم ها بلااستفاده رها مي شوند، مي توان از آنها بعنوان خطوط تلفن استفاده كرد. اما اين تصور كاملا غلط است و در صورت انجام چنين كاري ، سيگنال هاي در حال عبور در خطوط تلفن با سيگنالهاي

داده تداخل پيدا مي كنند. به پنل رابط، بلاك Punchdown هم اطلاق مي شود. اين پنل شبيه به پريز هاي ديواري است با اين تفاوت كه داراي پورتهاي بيشتري مي باشد. توجه داشته باشيد كه اين پنل، هاب نمي باشد بلكه فقط محلي است انتهايي براي همه كابل هايي كه بايد به هاب متصل شوند. براي اتصال پورتهاي اين پنل به هاب بايد از كابل هاي رابط (Patch) استفاده كنيد تا به اينصورت ايجاد اتصال بين كامپيوتر و هاب كامل شود. پنل هاي رابط در انواع و اندازه هاي مختلف در بازار عرضه مي شوند، اين پنل ها يا روي ديوار و يا روي قفسه هاي مخصوص نگهداري هاب (rack) نصب مي شوند. توجه: فراموش نكنيد كه همه سوكت هايي كه در شبكه خود استفاده كرده ايد بايد مطابق با گروه كابل هاي استفاده شده باشند. بعنوان مثال در صورت بكار بردن كابل هاي گروه 5 بايد از سوكت هايي استفاده كنيد كه با اين گروه مطابقت داشته باشند.

سوكت زدن به كابل ها

در شبكه بندي به روند متصل كردن كابل ها به سوكت ها روي پنل هاي رابط و پريزهاي ديواري، Punching down گفته مي شود. هر سوكت داراي هشت پايه مطابق با هشت رشته سيم موجود در كابل مي باشد. Punch كردن يك كابل شامل مراحل زير مي شود.

1- قسمتي از پوشش عايق كابل را بصورتي كه سيم هاي آن كمي بيرون بيايند جدا كنيد.
2- زوج هاي بهم پيچيده در قسمت بيرون آمده از پوشش عايق كابل را از هم جدا كنيد.
3- سيمها را وارد پايه هاي مناسب با هر يك كنيد.
4- سيم هاي لخت شده را بين زوج پايه هاي آهني سوكت فشار دهيد تا در جاي خود قرار بگيرند.
5- سيم هاي اضافي بيرون آمده از پايه را كوتاه كنيد.

به خاطر داشته باشيد كه اين مراحل را براي هر دو سر هر يك از كابل ها بايد تكرار كنيد. خوشبختانه ابزارهايي وجود دارند كه به كمك آنها اين مراحل را مي توان ساده تر انجام داد. بعنوان مثال وسيله اي بنام Punchdown block وجود دارد كه از آن براي وارد كردن سيم ها بين پايه هاي مربوطه روي سوكت استفاده مي شود. اين وسيله عايق دور سيم ها را جدا مي كند، آنها را بين پايه هاي سوكت قرار مي دهد و سيم هاي اضافه را كوتاه مي كند. توجه داشته باشيد كه آچار Punchdown block شما بايد با نوع سوكت هايي كه قرار است استفاده كنيد، مناسب باشد. معمولا فرق بين آچارها در شكل تيغه هاي قطع كننده اضافه هاي سيم ها مي باشد. سوكت هايي (يا بلاك ها) كه امروزه مورد استفاده قرار مي گيرند 110-style نام دارند. شما مي توانيد آچاري خريداري كنيد كه فقط مخصوص اين نوع

بلاك ها باشد و يا از انواع ديگري كه داراي بخش هاي قابل تعويض براي كار با چند نوع بلاك مي باشند، خريداري كنيد.
مهمترين بخش متصل كردن انتهاي كابل به سوكت RJ-45 ، تنظيم كردن سيم ها با پايه هاي مناسب در سوكت مي باشد. سيم هاي داخل كابل UTP داراي كدهاي رنگي نارنجي، سبز، آبي و قهوه اي مي باشند. رشته مثبت هر يك از زوج ها داراي رنگي يكدست و رشته منفي داراي يك خط سفيد رنگ مي باشد. سعي كنيد از سوكت هايي استفاده كنيد كه رنگ هر يك از پايه هاي روي آنها مشخص باشد تا براحتي بتوانيد سيم ها را با پايه هاي مناسب با هر يك روي هم منطبق كنيد.
براي اتصال كردن كابل به سوكت، حدود دو اينچ از روكش عايق كابل را جدا كنيد و زوج سيم هاي بهم پيچيده را از هم باز كنيد، سپس كابل را در وسط سوكت قرار دهيد و هر يك از رشته سيم ها را بين پايه هاي مناسب بگذاريد. روكش كابل نبايد از سوكت بيش از يك هشتم اينچ فاصله داشته باشد تا سيم ها محافظت شده باشند. همچنين توجه داشته باشيد كه پيچ سيم ها را فقط در حد لازم با يد از همديگر باز كنيد چون دليل پيچ هر يك از اين زوج ها اينست كه تداخل سيگنال هاي در حال عبور از زوج هاي مختلف با همديگر جلوگيري شود. نسبت پيچش هر يك از اين زوج ها در واحد طول، با همديگر تفاوت دارد و اين آرايش بايد در حد امكان حفظ شود. بعد از اينكه رشته سيم ها را به بين پايه هاي مناسب قرار داديد با استفاده از آچار مخصوص(Punchdown) سيم ها را به سوكت محكم پرس كنيد. بدين شكل سيم ها به مقدار كافي لخت و در جاي خود پرس مي شوند و اضافه آنها چيده مي شود. البته مدتي طول مي كشد كه به انجام اين كار عادت كنيد بنابراين بد نيست تعدادي سوكت اضافي خريداري كنيد و كمي تمرين كنيد. اين مسئله همچنين دليل خوب ديگري براي كمي بلندتر گرفتن كابل ها مي باشد تا در صورت وقوع اشتباه، جاي لازم براي قطع كردن سر كابل و استفاده از يك سوكت ديگر وجود داشته باشد.
بعد از اينكه كابل به سوكت پرس شد مي توانيد در صورت نياز سوكت را داخل پريز ديواري و يا پنل رابط وارد كنيد. سپس مي توانيد كابل هاي اضافي را داخل ديوار فرو كنيد. و پريز را در داخل محلي كه قبلا روي ديوار كنده ايد فشار دهيد تا در جاي خود قرار بگيرد. پنل رابط را هم بعد از سوكت زدن به همه كابل ها، روي ديوار و يا داخل قفسه مخصوص (Rack) نصب كنيد .

ساخت كابل هاي رابط

كابل رابط و يا كابل Patch ، كابلي است كه در دو سر آن كانكتورهاي نري RJ-45 پرس شده است و از آن براي برقراري ارتباط بين پريز روي ديوار و كارت شبكه كامپيوتر و يا ارتباط بين سوكت هاي روي پنل Patch و هاب استفاده مي شود. اين نوع كابل ها هم بصورت آماده در بازار عرضه مي شوند و هم خودتان مي توانيد آنها را بسازيد. همانند زمانيكه كابل كشي بصورت روكار

انجام شده است وقتي كار برقراري اتصالات فيزيكي بين دو كامپيوتر و هاب تمام شد، LED هاي روي هاب و كارت شبكه بايد به نشانه برقراري ارتباط روشن شوند. اما اگرLED ها روشن نشدند چون در كابل كشي توكار قطعات بيشتري نسبت به كابل كشي روكار بكار مي رود، روند عيب يابي و رفع آن كمي مشكل تر است.

استانداردهاي سيم كشي

در حال حاضر از دو استاندارد براي مشخص كردن اينكه هر يك از رشته سيم هاي رنگي كابل UTP به كداميك از پايه هاي روي كانكتور بايد متصل شود، وجود دارد. اين دو استاندارد 568A و 568B نام دارند وت توسط EIA/TIA (Electronics Industry Association/Telecommunication Industry Association)معرفي شده اند.

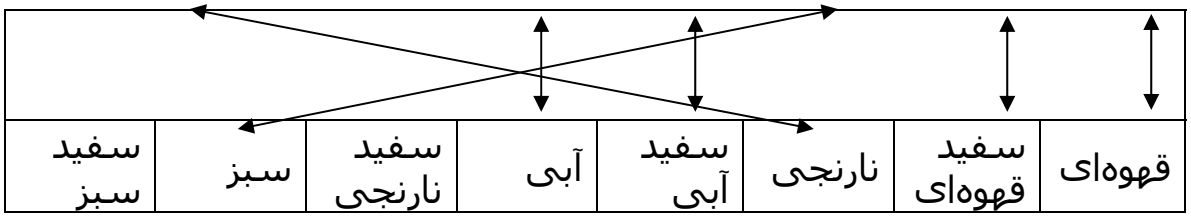
براي سيم‌كشي كانكتورها مهم نيست كه از كدام استاندارد استفاده كنيد، هر دو از نظر عملكرد دقيقاً مشابه همديگر هستند. حتي شما هم مي‌توانيد براي خود يك استاندارد جديد ايجاد كنيد. آنچه در اينجا اهميت دارد اينست كه فقط از يك استاندارد در كل سيم‌كشي كانكتورهاي شبكه‌ي خود استفاده كنيد. كابلي كه در يك طرف آن از استاندارد 568A و در طرف ديگر از استاندارد 568B استفاده شده است ، كار نخواهد كرد. از آنجا كه در كابل‌هاي از پيش‌ساخته هر يك از پايه‌هاي كانكتورها به پايه‌ي قرينه‌ي خود در كانكتور طرف ديگر متصل است نيازي نيست كه نگران استاندارد استفاده شده در آنها باشيد.

رنگ بندی کابل استاندارد
PC – Hub

سفید نارنجی	نارنجی	سفید سبز	آبی	سفید آبی	سبز	سفید قهوه‌ای	قهوه‌ای
↕	↕	↕	↕	↕	↕	↕	↕
سفید نارنجی	نارنجی	سفید سبز	آبی	سفید آبی	سبز	سفید قهوه‌ای	قهوه‌ای

رنگ بندی کابل CrossOver
PC – PC

سفید نارنجی	نارنجی	سفید سبز	آبی	سفید آبی	سبز	سفید قهوه‌ای	قهوه‌ای
↕		↕					



روش پرس كردن كانكتورهاي RJ-45

گرچه استفاده از پريزهاي ديواري و پنل‌هاي رابط منجر به كابل‌كشي تميزتري مي‌شود اما الزاماً مجبور نيستيد كه از آنها استفاده كنيد. بلكه مي‌توانيد از انتهاي كابل خود كانكتورهاي نري RJ-45 بزنيد و آنها را مستقيماً به هاب و كامپيوترهاي خود متصل كنيد. همچنين شما مي‌توانيد با استفاده از اين كانكتورها براي شبكه‌ي خود كابل‌هاي ارتباطي به طول و تعداد لازم بسازيد.

براي كابل‌هاي UTP سه نوع كانكتورRJ-45 وجود دارد، توجه داشته باشيد كه كانكتورهاي شما بايد با كابل انتخاب شده سازگار باشد. اين سه نوع كابل از قرار زير مي‌باشند:

1. كابل‌های گرد با رشته سيم‌های افشان
2. كابل‌های گرد با رشته سيم‌های مفتولی (غير افشان)
3. كابل‌های تخت با رشته سيم‌های افشان (به اين نوع كابل‌ها معمولا" Sliver Stain گفته می‌شود)

توجه: كابل‌هاي تخت براي شبكه‌هاي تلفن طراحي شده‌اند و نبايد از آنها در شبكه‌هاي اطلاعاتي استفاده كرد.

براي پرس كردن كانكتورهاي RJ-45 به كابل‌هاي UTP به ابزار بخصوصي احتياج است كه آچار سوكت Crimper· نام دارد. اين وسيله شبيه به انبردست است و داراي دو زبانه مي‌باشد. علاوه بر اين در آچار سوكت حديده‌هايي وجود دارد كه رشته سيم‌هاي كابل UTP را در داخل سوكت پرس مي‌كنند. مانند مراحلي كه براي وصل كردن سوكت‌هاي مادگي RJ-45 به كابل‌هاي توكار طي گرديد، مقداري از روكش كابل را جدا كنيد و رشته سيم‌ها را بنابر يك استاندارد مشخص وارد سوكت كنيد و با استفاده از آچار مخصوص، سوكت را پرس كنيد تا سيم‌ها را محكم در بر بگيرد. توجه داشته باشيد كه اولاً در دو سر كابل بايد از يك استاندارد براي سيم‌كشي استفاده شود و دوم اينكه قبل از پرس كردن سوكت هر رشته بايد در جاي خود قرار گرفته باشد. البته مدتي طول خواهد كشيد كه به انجام اين كار عادت كنيد. اگر غير از زماني كه تلف مي‌شود هزينه‌ي خريد يك آچار سوكت (حدوداً 50 دلار) و سوكت‌ها و كابل‌هايي كه ممكن است در حين كار از بين بروند را با هزينه‌ي كابل‌هاي رابط آماده مقايسه كنيد. به احتمال زياد متوجه خواهيد شد كه از نظر اقتصادي خريد كابل‌هاي رابط آماده به صرفه‌تر است.

نكته: تست كابل‌هاي كشيده شده در يك شبكه و كابل‌هاي رابط از اهميت خاصي برخوردار است. گرچه اين امكان وجود دارد كه با وصل كردن كامپيوترها به هاب و بررسي اينكه آيا LED روي هر دوي آنها روشن مي‌شود يا خير، كابل‌ها را تست كنيد، اما نصاب‌هاي حرفه‌اي از ابزار مخصوصي براي تست مشكلات احتمالي كه ممكن است در كار خود سريعاً نشان ندهند، استفاده مي‌كنند.

برقراري اتصالات لازم در كابل‌هاي فيبر نوري

كابل‌هاي فيبر نوري در اغلب موارد با كابل‌هاي مسي تفاوت دارند كه يكي از آنها روش برقراري اتصالات لازم در آنها مي‌باشد. برخلاف كانكتورهايي كه در كابل‌هاي مسي استفاده مي‌شود و انتهاي كابل را كاملاً مي‌پوشانند، كانكتورهايي كه در فيبرهاي نوري به كار مي‌رود (به اين كانكتورها ST(Straight Tip) و SC(Subscriber Connectors) گفته مي‌شود) فقط دور كابل را در برمي‌گيرد به شكلي كه مغزي كابل از ميان كانكتور بيرون مي‌آيد و قابل رؤيت مي‌باشد. تنها وظيفه‌ي اين كانكتورها اين است كه وقتي كابل داخل سوكت مي‌رود مغزي در حال حمل سيگنال را محكم نگه دارند. براي متصل كردن يك كانكتور به يك كابل فيبر نوري چند مد مقداري از پوشش انتهايي كابل بايد جدا شود. سپس كانكتور با استفاده از چسب پلاستيك در محل خود چسبانده شود و پس از خشك شدن چسب، مغزي بيرون آمده از كانكتور صيقل داده شود تا سيگنال‌هاي نوري در حال عبور در كابل در بهترين شرايط به انتهاي كابل برسند. اما در كابل‌هاي فيبر نوري تك مد به انتهاي كابل، تكه‌اي كابل كوتاه كه سر ديگر آن داراي كانكتور مي‌باشد، چسبانده مي‌شود.

دستور كار جلسه دوم

آشنايي با TCP/IP و نحوه پيكربندي آن در سيستم عامل ويندوز

دانشجوي گرامي، اين دستور كار را بدقت مطالعه كرده، آزمايش را انجام داده و پس از تكميل، براي مربي خود ارسال نماييد.

نيازمنديها

سخت افزار
يك PC با سيستم عامل ويندوز 2000 يا XP براي انجام آزمايش و يك PC براي تهيه گزارش
كارت شبكه جدا (10، 10/100، 1000 و يا Fiber) كه در PC نصب شده است.
كابل Cross
نرم افزار
Ethereal
درايور كارت شبكه (در صورتيكه در سيستم عامل موجود نباشد.)
مجوز Admin بر روي PC آزمايش
زمان مورد نياز
حداكثر 2 ساعت

دستور كار
مراحل ذيل را دنبال كنيد:

- در صورتي كه كامپيوترهاي شما به Switch و يا Hub شبكه متصل مي باشد، آنها را قطع كرده و توسط كابل Cross به يكديگر متصل نماييد.
- از سالم بودن و اتصال كابل و فعال بودن كارت شبكه اطمينان حاصل كنيد.
- حال از آدرسهاي Private يك Subnet با چهار آدرس بدلخواه انتخاب نموده و Subnet Mask مربوطه را محاسبه كنيد. توجه كنيد كه از اين 4 آدرس، آدرس اول و آخر قابل استفاده نيستند.(آدرسها و Subnet Mask را در گزارش بنويسيد)
- 2 آدرس باقيمانده را بر روي سيستمهاي گروه خود قرار دهيد.

- در صورتي كه نرم‌افزار فايروال بر روي سيستم شما فعال است، آن را از كار بياندازيد.

<u>در هر مرحله از مراحل ذيل، دستور مورد استفاده و خروجي آن را بنويسيد.</u>

با استفاده از دستور ipconfig پيكربندي TCP/IP سيستمهاي خود را مشخص نماييد.(با جزيي ترين اطلاعات ممكن)
با استفاده از ابزار ping ارتباط دو سيستم را كنترل نماييد. (10 بسته ICMP بطول هركدام 64 بايت)
با استفاده از ابزار ping مقدار MTU (Maximum Transmission Unit) شبكه را پيدا كنيد. (دستور اجرا شده و نتيجه اجرا و MTU را در كادر زير بنويسيد.)
با استفاده از دستور ARP جدول ARP سيستم خود را مشخص نماييد. چگونه مي‌توان محتويات اين جدول را پاک نمود؟
با استفاده از ابزار netstat كليه پورتهاي TCP كه در سيستم شما در حالت Listen قرار دارد، مشخص نماييد.
هدف از اين بخش آشنايي با مدل چهار لايه TCP/IP و برخي پروتكلهاي هر لايه مي باشد. ابتدا سيستم خود را به شبكه دانشكده متصل نماييد. پيكربندي TCP/IP را در حالت خودكار قرار دهيد. از دريافت IP جديد توسط سيستم خود اطمينان حاصل كنيد. حال Ethereal را اجرا نماييد (پيش از انجام اين مرحله Proxy مرورگر را غير فعال نماييد)

لايه كاربرد

HTTP Request و HTTP Response را مشخص كنيد.
در اين لايه از چه پروتكلي و چه نسخه اي از اين پروتكل استفاده شده است.
فيلد User-Agent و Connection در HTTP Request چه نقشي دارند؟

لايه انتقال

در لايه انتقال از چه پروتكلي استفاده شده است. RFC مربوطه را مشخص نماييد.
پورتهاي مبدا و مقصد در HTTP Request و HTTP Response كدام است.
فيلدهاي Checksum و Window Size در لايه انتقال چه نقشي دارند. مقدار هر كدام را مشخص نماييد.

لايه اينترنت

در اين لايه از چه پروتكلي و چه نسخه اي از اين پروتكل استفاده شده است. RFC مربوطه را مشخص نماييد.
آدرسهاي IP مبدا و مقصد را در درخواست و پاسخ مشخص نماييد.
فيلد هاي Time To Live و Protocol چيست و چه نقشي دارند؟

لايه Network Interface

- آدرسهاي Mac مبدا و مقصد را در درخواست و پاسخ مشخص نماييد.
- فيلد Type چيست و چه نقشي دارد؟

سوالات كلي

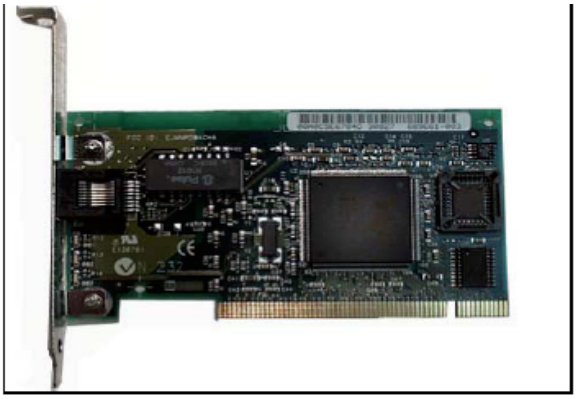
- طول كل بسته Request و بستهResponse را مشخص نماييد.
- طول header هر لايه را مشخص نماييد.

مطالب تكميلي

گره[1]: هر ابزاري متصل به شبكه كه داراي پورتي براي ورود يا خروج داده باشد. مثل switch و Router و ...

سخت‌افزار شبكه:

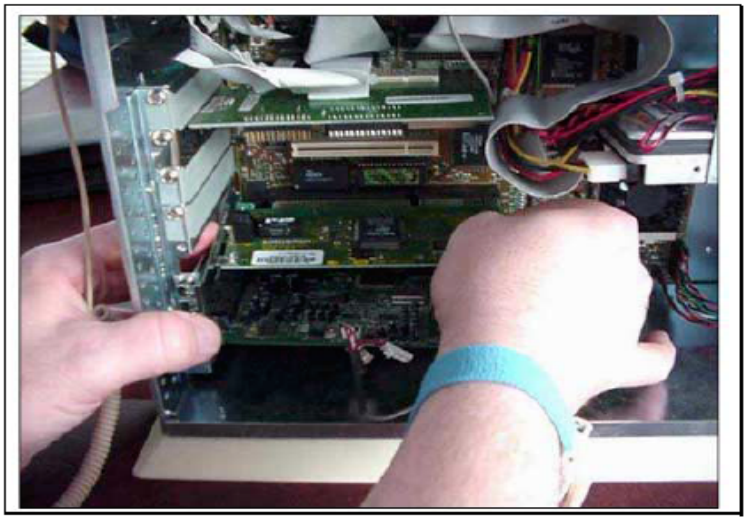
NIC يا كارت شبكه[2] : محل آن بين كامپيوتر و رسانه شبكه است و توسط مادربرد پشتيباني مي‌شود و متناسب و موافق با توپولوژي فيزيكي شبكه بايد باشد.



كارت شبكه يا NIC پشتيباني از كارت شبكه بر عهده main board است.
محل آن برروي يكي از اسلاتهاي مادربرد است يا بصورت on board است.
نكته: بيشتر كارتهاي شبكه روي اسلات PCI نصب مي شود.
انواع اسلاتها : 1) ISA 2) (سفيد) PCI 3) AGP (قهوه اي) مي باشند.
وظيفه كارت شبكه : محل منطقي كارت شبكه بين كامپيوتر و رسانه است.
(تكنولوژي ارتباطي بين كامپيوتر ها را رسانه گوييم)

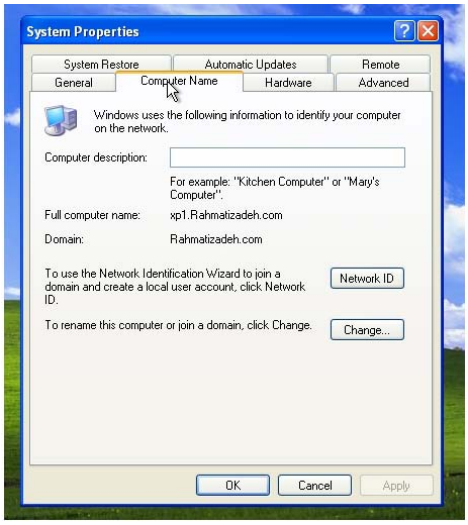
---

[1] node
[2] Network Interface Card

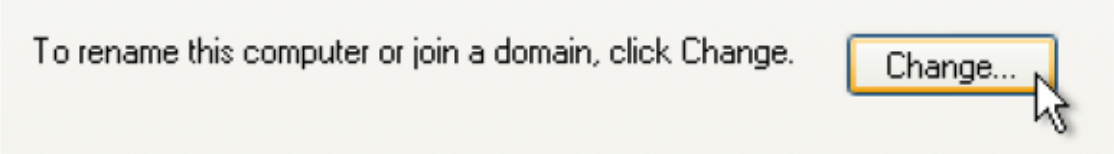


نام كامپيوتر
هر كامپيوتر در شبكه، داراي نام منحصر بفرد مي باشد. از اين نام مي توان جهت ارتبا ط با
كامپيوتر، در داخل شبكه استفاده كرد. جهت مشاهده يا تغيير نام كامپيوتر، پس از لاگين كردن با كاربر Administrator ، به روش زير عمل كنيد:

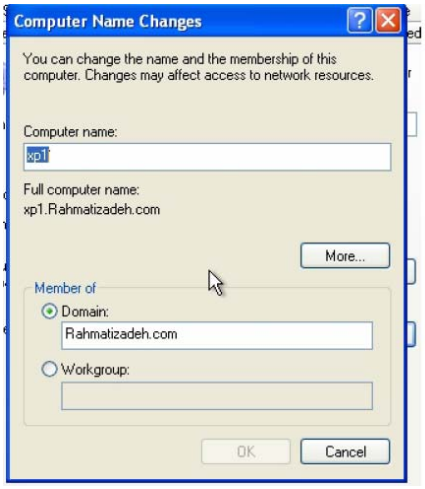
بر روي دكمة Start كليک كرده و بر روي علامت My Computer ، دكمة سمت راست
موس را بزنيد. سپس گزينة Properties را انتخاب كنيد.



پس از ظاهر شـدن پنجـرة System Properties ، سـربرگ Computer Name را انتخـاب كنيد.
در قسـمت Full computer name، نام كامل كامپيوتر را مي توانيـد مشـاهده كنيد. نـام كامـل كـامپيوتر، شـامل نـام كـامپيوتر بـه همـراه Domain ي كـه كامپيوتر در آن عضو مـي باشـد اسـت. كـه توسـط نقطـه از هـم جـدا شـده انـد. نـام كـامپيوتري كـه در شـكل آمـده اسـت، "xp1 " بـوده است.
جهت تغيير نام كامپيوتر بر روي دكمة Change كليک كنيد:



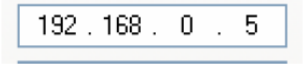
در قسـمت Computer name ، نـام كـامپيوتر و در قـسـمت Domain نـام Domainاي را كـه كامپيوتر عضو آن مي باشـد، وارد كنيد.



در تعويض نام كامپيوتر، نكات زير را مد نظر داشته باشيد:
الف- جهت تعويض نام كامپيوتر، بايد حتما Administrator و يا عضوي از گروه Administrators باشيد.
ب- در صورتيكه كامپيوتر در شبكه باشد، ممكن است سياست هاي اعمال شده بر روي شبكه، از تغيير نام كامپيوتر جلوگيري كند.
ج- در صورتيكه كامپيوتر عضوي از يک Domain باشد، ممكن است نام و رمز كاربري كه اجازة تغيير نام كامپيوتر در Domain را دارد، از شما خواسته شود .
د- فقط در شرايط خاص كه در توضيحات مربو ط بهDNS خواهد آمد، طول نام كامپيوتر مي تواند از15 حرف بيشتر باشد.
پس از تعويض نام كامپيوتر، به شرطي كه كامپيوتر هم نامي در شبكه وجود نداشته باشد، كامپيوتر بايد Restart شده تا نام جديد مورد استفاده قرار گيرد.

IP يا اينترنت پروتكل

هر كامپيوتر موجود در شبكه، با يک عدد منحصر بفرد شناخته مي شود. اين عدد از چهار قسمت تشكيل شده است كه هر قسمت آن توسط نقطه از هم جدا شده و مي تواند عددي بين صفر و 255 باشد. نمونه اي از اين عدد را در شكل ملاحظه مي كنيد:



درحقيقت، اين عدد از چهار بايت تشكيل شده كه هر بايت نشانگر يک عدد از مجموع چهارعدد فوق است. كامپيوتر از اين عدد براي ارتباط برقرار كردن با كامپيوترهاي ديگر شبكه استفاده مي كند. اين عدد يک عدد ۳۲ بيتي است و براي راحتي بصورت زير نوشته ميشود:
xxx.xxx.xxx.xxx كه منظور از xxx عددي بين ۰ تا ۲۵۵ است (البته بعضي شماره‌ها قابل استفاده نيست). مثلا ممكن است آدرس شما به صورت 195.219.176.69 باشد. حتي اسمهايي مثل http://www.yahoo.com كه براي اتصال استفاده ميكنيد، در نهايت بايد به يک IP تبديل شود، تا شما سايت ياهو را ببينيد
در IP معمولا xxx اولي معناي خاصي دارد، كه بعدا توضيح ميدهم... فقط اين را بگويم كه اگر به روش Dial Up به اينترنت وصل شويد، معمولا عددي كه به عنوان xxx اول ميگيريد، مابين 192 تا 223 خواهد بود.اين توضيح براي تشخيص كامپيوترهاي كلاينت از سرور (حداقل در ايران) بسيار ميتواند مفيد باشد

كلاس‌هاي آدرس IP

هر ماشين در شبكه بايد با آدرس يكتا شناخته شود و هيچ دو ماشيني داراي آدرس مشابه نباشند پس در اختيار داشتن آدرس يك ماشين موقعيت آن را در شبكه مشخص خواهد كرد، اين آدرس كليد مسيريابي و هدايت شبكه ها محسوب مي شوند، اين آدرس مورد نظر را IP Address گويند و شامل: آدرس ماشين/ آدرس زير شبكه/ آدرس شبكه .
يك آدرس IP بطوركلي و عام داراي 2 بخش است كه بخشي از فضاي 32 بيتي آدرس به شماره شناسايي يك شبكه خاص اختصاص يافته و مابقي بيت ها آدرس ماشين را مشخص مي كند. از آنجائي كه شبكه هاي مختلف داراي تعداد ماشينهاي متفاوتي هستند لذا طول بخش شماره شناسايي شبكه در يك آدرس IP متغير بوده و به كلاس آدرس بستگي دارد.
پرارزش‌ترين بايت يعني اولين بايت سمت چپ از آدرس IP، كلاس آدرس را مشخص ميكند. وقتي يك ماشين به شبكه اينترنت متصل ميشود بايستي آدرس IP آن منحصر بفرد باشد براي اطمينان از يكتا بودن آدرس هاي IP براي ارتباط عمومي، مركز Inter NIC (Internet Network Information Center) كنترل و نظارت بر روي آدرس هاي IP را به عمده گرفته است.
IANA(Internet Assigned Number Authority) نيز قدرت اجرائي و تصميم گيري براي اختصاص آدرس هاي IP منحصر بفرد را فراهم كرده است. هر چند شبكه‌هاي خصوصي كه به اينترنت وصل نيستند مي توانند از آدرس هاي IP دلخواه استفاده كنند ولي اگر اين شبكه هاي زماني بخواهند به اينترنت متصل شوند دوگانگي آدرس هاي غيريكتا و نهايتاً تناقض و اشكال در مسيريابي رخ خواهد داد. به همين دليل حتي شبكه هاي خصوصي نيز براي اختصاص آدرس به ماشين هاي ميزبان از مركز InterNIC مجوز مي گيرند و از

آدرسهاي معتبر و اختصاصي استفاده كنند. اساس آدرس هاي IP قالبي بصورت مقابل دارند: آدرس ماشين / آدرس زير شبكه / آدرس شبكه
از آنجائيكه قرارداد TCP/IP براي شبكه هاي با مقياس بزرگ طراحي شده است لذا نمي توان انتظار داشت كه فضاي 32 بيتي آدرس كه حدود چهارميليارد و سي صد ميليون آدرس را بدون هيچ نظم و سياقي خاص به ماشين هاي شبكه اختصاص داده شود. آدرس هاي IP بخودي خود اطلاعات ارزشمندي را در مورد نقشه شبكه و محل يك ماشين در شبكه اينترنت با خود حمل مي كند. مسيريابها بر اساس اين آدرس به سرعت موقعيت ماشين مقصد را يافته و بسته را به سمت آن هدايت مي كنند. ساختار يك آدرس IP سلسله مراتبي است.
با توجه به آنكه اينترنت مجموعه اي از شبكه هاي متصل شده به هم مي باشد، براي آدرس دادن به ماشين هاي ميزبان بهتر است 32بيت آدرس IP به قسمتهاي زير تقسيم شود:
الف) آدرس شبكه ب) آدرس زير شبكه(درصورت لزوم) ج)آدرس ماشين ميزبان
آدرسهاي IP درپنج كلاس E,D,C,B,A معرفي شده اند.در زير قالب كلاس پنج گانة آدرسIP مشخص شده است:

آدرسهاي كلاس A :
در كلاس A، پرازش ترين بيت از آدرس ،مقدار صفر دارد و اين بيت، كلاس A را از ديگر كلاسها متمايز مي كند؛ 7بيت بعدي " مشخصةآدرس شبكه" وسه بايت باقيمانده، آرس ماشين ميزبان را تعيين مي كند.بنابراين در كلاس A بايت پر ارزش در محدودة صفر تا 127 تغيير مي كند.
مشخصة شبكه به هيچ وجه نميتوان اعداد صفر يا 127 انتخاب شود چرا كه اين دو عدد در شبكه معناي ديگري خواهند داشت و بعدا به آن اشاره خواهيم كرد.
اگر آدرس IP به صورت دهدهي نوشته شودوعدد سمت چپ آن بين صفر تا 127 باشد ، آن آدرس از كلاس A خواهد بود:
74. 14. 103. 74 Host ID . Network ID

آدرسهاي كلاسB:
هر گاه دو بيت پرازش از آدرس IP مقدار10 داشته باشد آن آدرس از كلاس B خواهد بود.14 بيت باقيمانده از 2 بايت سمت چپ، آدرس شبكه را تعيين ميكند و دو بايت اول از سمت راست(16 بيت) آدرس ماشين ميزبان خواهد بود.در آدرس كلاس B ، تعداد 16382 شبكة گوناگون قابل تعريف خواهد بود و هر شبكه مي تواند 65534 ماشين ميزبان تعريف نمايد.
اگر آدرس IP به صورت دهدهي نوشته شودوعدد سمت چپ آن بين 128 تا 191 باشد ، آن آدرس از كلاس B خواهد بود:

Host ID Network ID 138. 14. 103. 134

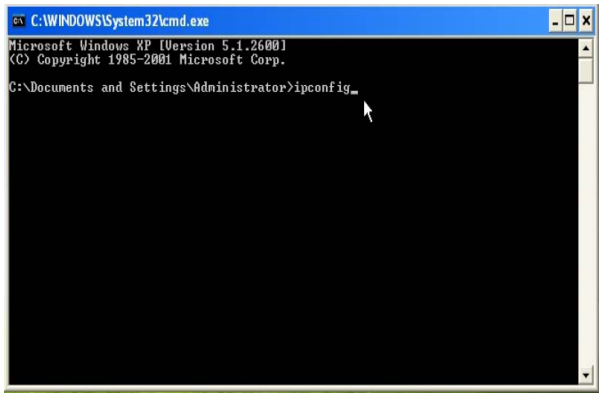
آدرسهاي كلاسC:
كلاس C مناسبترين و پركاربردترين كلاس از آدرس هـاي IP اسـت. همانگونـه كه از مشخص است در اين كلاس، سه بيت با ارزش داراي مقـدار110 اسـت و 21 بيت بعدي از سمت چپ براي تعيين آدرس شـبكة مـورد نظـر بكـار رفتـه است .بنابراين در ايـن كـلاس مـي تـوان حـدود دو ميليـون شـبكه را در جهـان آدرس دهي كرد وهر شبكه مي تواند تا254 عدد ماشين ميزبان تعريف نمايد.
اگر آدرس IP به صورت دهدهي نوشته شودوعدد سمت چپ آن بـين 192 تـا 223 باشـد ، آن آدرس از كلاس C خواهد بود:
Host ID Network ID 222. 14. 103. 199

آدرسهاي كلاس D :
در اين كلاس ، چهار بيت پر ارزش داراي مقدار 1110 است و28 بيت باقيمانده از كل آدرس براي تعيين آدرسـهاي"چند مقصده" (آدرسـهاي گروهي) اسـت. از اين آدرسـها براي ارسـال يك ديتاگرام به طـور هـم زمـان بـراي چنـدين ماشـين ميزبان كاربرد دارد و به منظور عمليات رسانه اي و چند پخشي بكار مي رود.

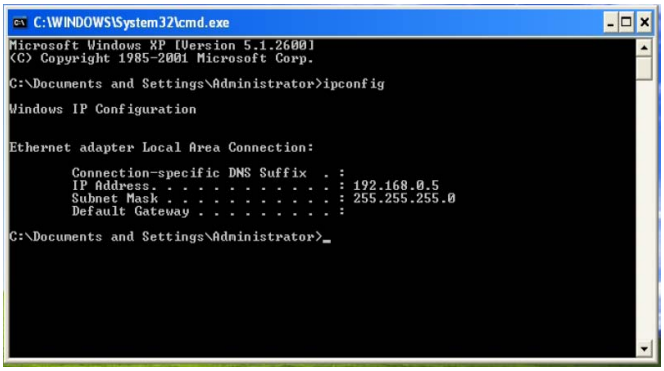
آدرسهاي كلاس E :
فعلا اين دسته آدرسـها كه پنج بيت با ارزش آنها در سـمت چـپ11110 اسـت كاربرد خاصي ندارند و براي اسـتفاده در آينده بدون اسـتفاده رهاشـده اند.

جهت مشاهدة IP كامپيوتر خود به چند روش ميتوانيد عمل كنيد:
1- در رو ش اول از منوي Start گزينة Run را انتخاب كنيد و كلمـة cmd را تايپ كنيد و كليد OK را فشار دهيد.
2-

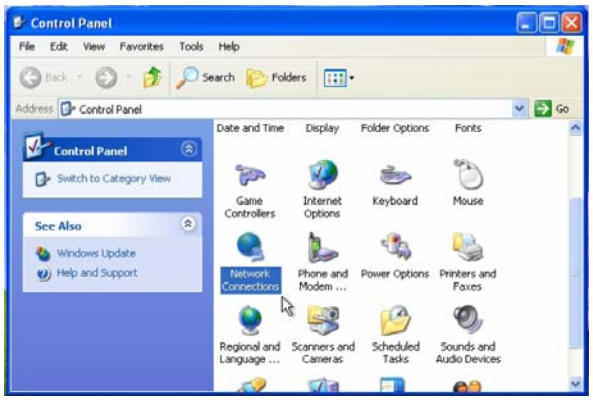
در پنجرة ظاهر شده عبارت ipconfig را تايپ كنيد و كليدenter را بزنيد.



عبارت نمایش داده شده در مقابل IPAddress، ip کامپیوتر شماست.

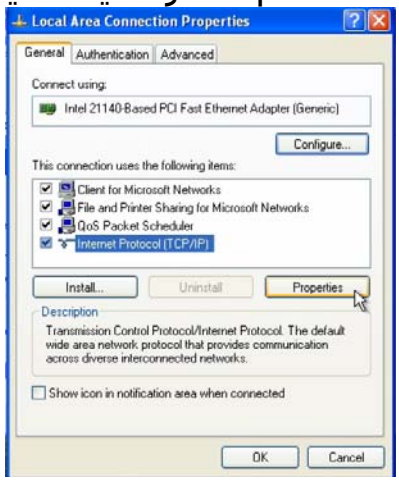


3- در روش دوم، از منـــوي Startوارد controlpanel شـــويد و علامـــت network connections را انتخاب کنید.

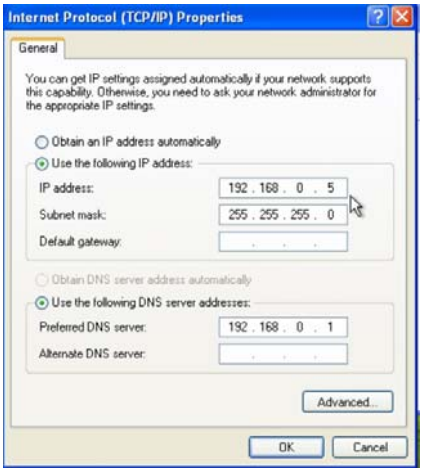


سپس در پنجرة ظاهر شده، بر روي علامت کارت شبکه، دکمة سمت راست موس را بزنيد و گزينة properties را انتخاب کنيد.

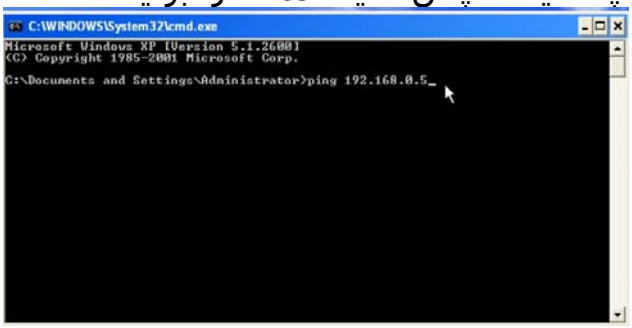
در پنجرة ظاهر شـــده، از لیـــست موجـــود، گزینـــة Internet Protocol (TCP/IP) را انتخـاب کنید و دکمة Properties را کلیک کنید.



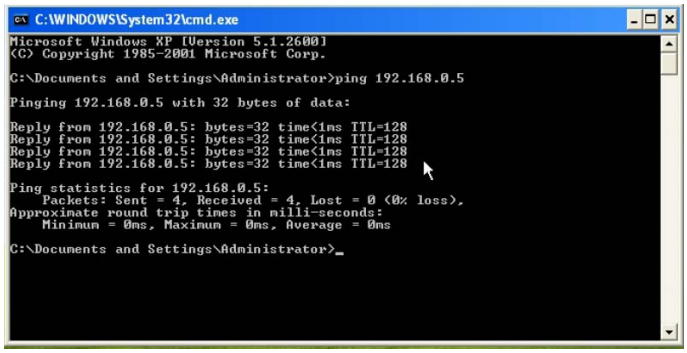
در پنجـــرة بعـــدي، اعـــداد ذکـــر شـــده در روبـــروي IPAddress، نـــشان دهنـــدة ip کامپیوتر شماست.



در این پنجره با وارد کردن اعداد جدید، مي توانيد IP کامپيوتر خود را تغيير دهيد. فقط بايد توجه داشته باشيد که اين IP، نبايد براي کامپيوتر ديگري استفاده شده باشد. براي اعما ل تغييرات IP نيازي به Restart کردن کامپيوتر نيست. به عنوان يک تمرين ساده، مي توانيد بر روي يک کامپيوتر ديگر در شبکه، گزينة Run را انتخاب کنيد و کلمة cmd را تايپ کنيد و کليد OKرا فشار دهيد.
در پنجرة ظاهر شده، عبارت Ping xxxx را وارد کنيد بجاي xxxx ، IP کامپيوتر خود را تايپ کنيد سپس کليد Enter را بزنيد.



در صورتيکه ارتباطات شبکه مشکلي نداشته باشد، چهار پيغام از طرف کامپيوتر فعلي، به کامپيوتر شما فرستاده مي شود و جوا ب دريافتي از کامپيوتر شما نمايش داده مي شود.



در تعويض IP کامپيوتر، نکات زير را مد نظر داشته باشيد:
الف- جهت تعويض IP کامپيوتر بايد حتما Administrator و يا عضوي از گروه Administrators باشيد.
ب- در صورتيکه کامپيوتر در شبکه باشد، ممکن است سياست هاي اعمال شده بر روي شبکه، از تغيير IP جلوگيري کند.

Subnet Mask

Subnet mask مانند IP از چهار عدد يک بايتي تشکيل شده است. پس اعداد تشکيل دهندة Subnet mask نيز هرکدام بين صفر تا 255 مي باشند. هدف از subnet mask ، تعيين دامنة شبکه و يا تقسيم شبکه به چند شبکة کوچکتر مي باشد. در حقيقت ترکيب IP با Subnet mask

مشخص ميكند كه چه محدوده IP در داخل شبكه بكار رفته است .به عنوان مثا ل، تركيب زير را در نظر بگيريد:

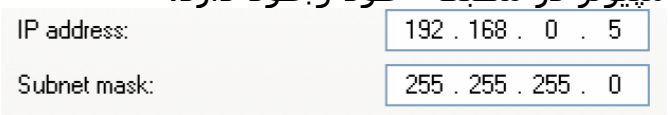
اعداد موجود در Subnet mask ، يک به يک با اعداد موجود در IP ، متنا ظر مي باشند. عدد255 موجود در Subnet mask نشاندهندة ثابت بودن عدد متناظر آن در IP ، در كل شبكه است. به عبارت ديگر، IP كلية كامپيوترهاي موجود در شبكه در مثا ل بالا با اعداد 0 . 168 . 192 شروع مي شوند. تنها عدد چهارم اين IP ها متغير است. به قسمت هايي از IPكه در شبكه ثابت است،Network ID گويند و به قسمت هايي كه در هر كامپيوتر متغير است Host ID مي گويند.
اگر عدد Host ID را به همراه اعداد متنا ظر آن در Subnet mask ، تبديل به باينري كنيم و
با هم جمع نماييم، بيت هاي عدد بدست آمده نمي تواند همگي 1 يا صفر باشد. در مثال بالا:

Host ID=5=00000101

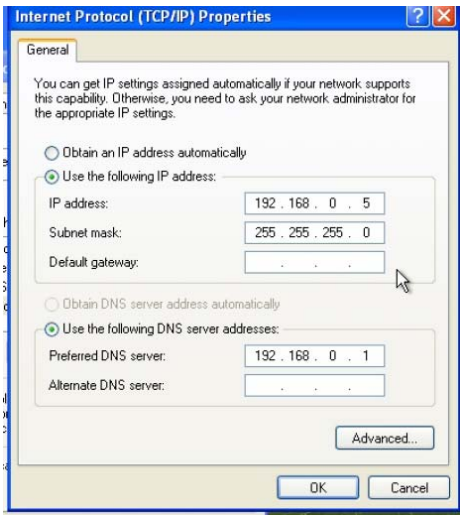
پس جمع هر كدام از اعداد موجود در Host ID و عدد متناظر آن در Subnet mask، نمي تواند مساوي صفر يا مساوي255 يا بيشتر از 255 باشد. به همين دليل در مثال اول، 254 كامپيوتر مجزا مي تواند در شبكه موجود باشد.
در مثال چهارم با فرض Subnet mask برابر با 252 . 255 . 255 . 255، تنها دو كامپيوتر با IP هاي 1 . 0 . 168 . 192 و 2 . 0 . 168 . 192 مي توانند در شبكه وجود داشته باشند.
شرط ديگر براي اعداد Subnet mask ، ترتيب 1 هاي موجود در باينري آن ها مي باشد. اولا تبديل باينري هر كدام از اعداد موجود در Subnet mask بايد با 1 شروع شده باشد. پس كوچكترين عدد ممكن براي Subnet mask ، عدد 128 (10000000 binary) است. ثانيا كلية 1 هاي بعدي بايد متصل به 1 اول باشند. يعني عدد 160 (10100000 binary) غلط و عدد192 (11000000 binary)صحيح مي باشد.
هنگام برقراري ارتباط، كامپيوتر به تركيب IP و Subnet mask خود نگاه مي كند. از اين تركيب، كامپيوترهايي را كه در شبكة خود وجود دارند تشخيص داده و با آن ها مستقيما ارتباط برقرار مي كند.

Gateway

در بخش مربوط به IP ، توضيح داده شد كه كامپيوتر از تركيب IP و Subnet maskخود، مي تواند تشخيص دهد كه چه IP هايي در شبكة خود وجود دارد. به عنوان مثال، هنگاميكه كامپيوتري با مشخصات زير بخواهد با كامپيوتري با IP ، 18 . 0 . 168 . 192 ارتباط برقرار كند، مي تواند تشخيص دهد كه اين كامپيوتر در شبكة خود وجود دارد.



پس مستقيما با آن كامپيوتر ارتباط برقرار مي كند. حا ل اگر همين كامپيوتر، بخواهد با كامپيوتري كه IP آن 18 . 5 . 168 . 192 است ارتبا ط برقرار كند چه اتفاقي مي افتد ؟
كامپيوتر اين IP را با IP و Subnet mask خود مقايسه مي كند. اين IP در شبكة تعريف شده براي اين كامپيوتر وجود ندارد پس اين كامپيوتر نمي تواند مستقيما با آن ارتباط برقرار كند. كامپيوتر مجبور است براي برقراري ارتباط از يک واسطه بنام Gateway استفاده كند.
در واقع، كامپيوتر اين درخواست را براي gateway فرستاده و gateway بجاي كامپيوتر اين ارتباط را برقرار مي كند. هنگام تعريف IP ، مكاني براي تعريف gateway IPوجود دارد.



در شكل بالا، در قسمت Default gateway ، آدرس gateway شبكه وارد مي شود. اينGateway مي تواند يک كامپيوتر و يا يک router باشد. IP ي كه براي gateway وارد مي شود بايد از جنس IP خود كامپيوتر باشد يعني بايد در همان شبكه اي باشد كه كامپيوتر در آن قرار گرفته تا كامپيوتر بتواند مستقيم با آن ارتباط برقرار كند.

تنظيماتDNS

استفاده از IP ، هنگام برقراري ارتباَط بين دو كامپيوتر مشكل است. مخصوصا در شبكه هايي كه تعداد كامپيوترهاي آن ها زياد است. بخاطر سپردن IP هاي كامپيوترهاي مختلف، كار ساده اي نيست. معمولا به خاطر سپردن اسامي، راحتتر از IP است. به همين دليل در شبكه از سرويسي بنام DNSاستفاده مي شود كه اين سرويس، وظيفة تبديل اسامي به IP را در شبكه دارد. اين سرويس، معمولا بر روي يک كامپيوتر مجزا در شبكه وجود دارد.

هنگاميكه كامپيوتر ما بخواهد، مثلا با كامپيوتري بنام "xp2" ارتبا ط برقرار كند، ابتدا اين نام را به كامپيوتري كه سرويس DNS بر روي آن وجود دارد فرستاده و از آن IP اين كامپيوتر را دريافت مي كند ساير مراحل مانند قبل انجام مي گيرد. در پنجرة تعريف IP دو مكان براي تعريف دوDNS مجزا، تحت عنوان Preferred DNS Serverو Alternate DNS Server وجود دارد.

دستورات TCP/IP:

ping:1

ping IP / Domain (destination address)

يكي از ابزارهاي خطايابي خوب است، ping ابزار استفاده شده براي بازبيني پشته TCP/IP از نظر صحت و وجود است، بعلاوه تعيين آنكه آيا يك سيستم دور روشن و در حال پاسخگويي است يا خير، ping بسته هاي ICMP را براي بازبيني اينكه يك آدرس IP يا Domain به ارتباطات پاسخ مي دهد يا خيز، استفاده مي كند. اگر يك پاسخ از آن ماشين دريافت شود ping آمار مربوط به آن پاسخ را محاسبه مي كند (مثل زماني كه براي دريافت پاسخ طول مي كشد) اين اطلاعات مي تواند براي شناخت كيفيت ارتباط بين دو سيستم استفاده شوند. شما مي توانيد ping را براي شناسائي وضعيت ارتباطي شبكه با دنبال كردن مراحل زير استفاده كنيد:

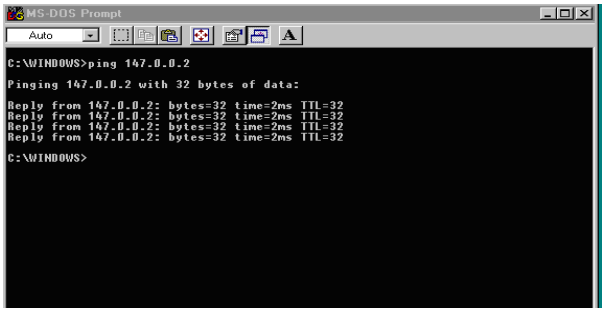
1) به آدرس ميزبان محلي (loop Back) (127.0.0.1) (پشته IP محلي شما) ping كنيد و بدين وسيله شما مي توانيد بفهميد كه آيا پشته TCP/IP شما به درستي كار مي كند يا خير. (اطلاعات فرستاده شده به يك آدرس loop back بدون خروج از رسانه فيزيكي مسيريابي مي شود)

2) به آدرس IP معرفي شده به كارت شبكه خود ping كنيد. اگر ping به ميزبان محلي كار كرده ولي با اين كار نكرد بايد بدانيد كه پيكربندي شبكه شما غلط است.

3) به يك آدرسIP محلي ping كنيد. اگر آن هم كار كرد مي توانيد مطمئن شويد كه حداقل سيستم هاي روي زير شبكه خود را خواهيد ديد ولي اگر تا مرحله قبل پيش رفتيد ولي در اين مرحله ناكام مانديد، احتمالاً مشكل

پيكربندي يك آدرس يا مشكل سخت افزاري بين شما و شبكه (مثل كابل يا پورت هاب خراب است) و يا احتمالاً نهانگاه ARP (cache) خراب شده است.
4) به آدرس دروازه پيش فرضي ping كنيد، اگر شما بتوانيد آدرسهاي IP محلي را ping كنيد ولي دروازه شما جواب ندهد به احتمال زياد آدرس دروازه غلط است، يك پورت بد روي دروازه وجود دارد و يا اينكه دروازه خاموش است و يا بد پيكربندي شده است.
5) به يك آدرس IP دور ping كنيد، اگر قادر به ping كردن دروازه شديد اما يك آدرس راه دور را نبينيد، ابزار دروازه شما بدرستي پيكربندي نشده يا اينكه بدرستي كار نمي كند و يا الگوي زير شبكه شما بدرستي پيكربندي نشده است.
6) يك نام ميزبان IP را ping كنيد. بدين ترتيب شما مي توانيد تعيين كنيد كه آيا تبديل نام TCP/IP به درستي كار مي كند يا خير.
7) اگر NetBT را روي شبكه خود استفاده مي كنيد، يك نام ميزبان Net BIOS را ping كنيد، بدين ترتيب شما متوجه مي شويد كه آيا تبديل نام Net BIOS به آدرس IP به درستي كار مي كند يا خير. اگر ارتباط شبكه به درستي بود، ping مي تواند براي اينكه بفهميد يك سيستم دور روشن است يا خير و به درستي پاسخ مي دهد يا خير هم استفاده شود.

اين دستور معلوم مي‌كند كه آيا بين دو سيستم اتصالي برقرار است يا نه. اگر اتصال برقرار بود جواب آن را مي‌دهد يعني بيان مي‌كند در چه مدت زماني Datagram از فرستنده به گيرنده ارسال شده و برمي‌گردد.



Tracert .2

اين دستور براي پيمايش يك مسير از فرستنده به گيرنده استفاده مي‌شود و اين دستور در unix به شكل Trace Route است. در Windows به صورت Trace Route.Exe و در Novell Netware به فرم IP Trace مي باشد.

IP Config .3

يك ابزار مناسب و براي بررسي پيكربندي پشته TCP/IP شما است، خواه اين پيكربندي بصورت دستي انجام شده باشد و خواه از طريق DHCP ، آن همچنين شما را قادر به تلاش براي بازسازي مجدد (renew) ارتباطات DHCP lease مي كند. اگر از سوئيچ All/ استفاده گردد ليست ظاهر شده شامل همه اطلاعات پيكربندي مربوط به پشته TCP/IP است كه عبارتند از:

1. نام ميزبان يا Domain
2. سرويس دهنده هاي اوليه و ثانويه DNS و WINS .
3. اطلاعات پيكربندي Net BIOIS شامل پيكربندي تبديل نام.
4. آدرس IP محلي، الگوي زير شبكه و دروازه براي هر كارت شبكه.
5. آدرس MAC و درايور هر كارت شبكه.

IP config روشي براي گرفتن ليست كامل از داده هاي پيكر بندي پشته TCP/IP و باز بيني سريع آنهاست. بطور نرمال براي مشاهده همه اين اطلاعات شما بايد چندين صفحه مختلف در Network NT Diagnostic و حتي Registry را مشاهده كنيد. همچنين IP config براي وقتي مفيد است كه شما در حال استفاده از DHCP باشيد چرا كه آن يك ليست جمع و جو از همه تنظيمات ارائه شده توسط سرويس DHCP به سيستم محلي شما را مي دهد. و بويژه بدان وسيله شما مي توانيد آدرس DHCP lease خود را مجدداً نوسازي (با سوئيچ Renew) يا آدرس اجاره اي را به پشته آدرس (address pool) برگردانيد (با سوئيچ IRelease).

IP config به شما امكان بازبيني پيكربندي پشته TCP/IP ماشين خودتان را ميدهد و روشي سريع براي مديريت آدرس DHCP اجاره اي را در صورت لزوم ميدهد.

اين دستور براي مشخص كردن تنظيمات TCP/IP از جمله Ip Address و ... مي‌باشد كه بيان كننده Interface Configuration مي‌باشد. به عبارت ديگر اين دستور تنظيمات كارت شبكه را بيان مي‌كند.

Net Stat .4

يك ابزار قدرتمند در بازبيني وضعيت آماري ارتباطات شبكه اي TCP/IP و اينترنت شما است. اين امكان را فراهم مي آورد كه بازبيني كنيد كدام پورت ها روي سيستم شما در حال شنيدن ارتباطات روي شبكه هستند و ميتوانيد وضعيت ارتباطات TCP برقرار شده فعلي را مورد بررسي قرار دهيد. Netstat يك ابزار حساس براي شناسائي ارتباطات شبكه اي روي ماشين

شما و نمايش اطلاعات روي شبكه است. شما مي توانيد اين آمارها را براي مشاهده اطلاعات مربوط به تعداد خطاهاي انتقال داده شده روي شبكه استفاده كنيد. مثلاً براي تعيين ترافيك overload روي شبكه يا ابزارهاي خرابي كه بار منفي به شبكه اعمال مي كنند. شما مي توانيد آن آمار و ارقام را روي ارتباطات پورت فعال براي بررسي وضعيت ارتباطي به سيستم هاي دور و نمايش حمله هاي شبكه اي استفاده كنيد.
Netstat امكان مشاهده اطلاعات فعلي جداول مسيريابي سيستم شما را مي دهد.

Netstat [بازه زماني] [-a] [-p پروتكل] [-n] [-e] [-r] [-s]

بازه زماني: تا زمانيكه كاربر اجراي دستور را متوقف كند، اطلاعات روي صفحه را در هر ثانيه به تعداد دفعات مشخص شده در بازه زماني تازه مي كند.
-a : ارتباطات شبكه فعلي و پورت هايي كه در حال گوش دادن به ارتباطات ورودي هستند را نمايش مي دهد.
-p پروتكل : ارتباطات فعال فعلي را براي پروتكل مشخص شده توسط متغير پروتكل نمايش مي دهد.
-n : وقتي با پارامترهاي ديگر تركيب شود باعث مي شود كه برنامه كامپيوترهاي را به جاي نام با آدرس IP مشخص كند.
-e : اطلاعات آماري ترافيك ورودي و خروجي كارت شبكه را نمايش ميدهد، اين اطلاعات شامل بايت ها، بسته هاي تك پخش، بسته هاي غير تك پخش، بسته هاي دور انداخته شده و پروتكل ناشناخته ورودي و خروجي مي باشد.
-r : جدول مسيريابي و ارتباطات فعال فعلي را نمايش مي دهد.
-s : اطلاعات آماري ترافيك شبكه مربوط به پروتكل UDP, TCP, ICMP, IP را نمايش مي دهد.
اين دستور براي مشخص كردن وضعيت آماري شبكه استفاده مي‌شود.
Netstat هم مثل Netbios يک برنامه خدماتي هست كه در خود سيستم عاملها گذاشته شده است. مثلاً در ويندوز 98 و Me در پوشه Windows \ با اسم Netstat.exe قرار گرفته شده است. در ويندوزهاي بر پايه NT مثل 2000 نيز در پوشه WinNT\System32\ قرار گرفته شده است. كلاً براي نمايش تمام ارتباطات ما در شبكه و فهميدن پورتها و IP هاي سيستمها و ماشين هايي كه ما با آنها در ارتباط هستيم بكار مي رود. براي استفاده از Netstat احتياج به هيچ برنامه كمكي و اضافي نداريد.
دستور Netstat، فرمان اصلي اين برنامه است كه با تايپ اين دستور شما متوجه IP سيستمها و پورتهايي كه با آنها در ارتباط هستيد را بدست مي آوريد. همچنين مشاهده مي كنيد كه چه پورتهايي Listening يا Established هستند.

ستون اول	ستون دوم	ستون سوم	ستون چهارم
اسم پروتكل	آدرس محلي	آدرس خارجي	وضعيت اتصال

اطلاعـــاتي كـــه
اين دستور مي دهد. عبارتند از:
1) اسم پروتكل 2) آدرس محلي 3) آدرس خارجي 4) وضعيت اتصال

بطور مثال :

TCP com61:1095 199. 199. 199. 68: 5405

اين سطر نشان مي دهد كه پروتكل كه داراي وضعيت برقراري اتصال است چه آدرسهاي محلي و خارجي دارد.

دستور Netstat -n
همانطوركه در بالا توضيح داده شد با استفاده از Netstat مي توانيد آدرس IP و پورت سيستمي كه شما با آن در ارتباط هستيد را بدست آوريد. حتي مي توانيد آدرس IP كسي كه با شما از طريق PM در مسنجر چت مي كند را بدست آورد. چون وقتي شما مسنجرها را باز مي كنيد با يک پورت خاصي شما با مسنجر ارتباط برقرار مي كنيد كه مثلاً شما با پورت 5050 با ياهو مسنجر ارتباط برقرار مي كنيد.

دستور Netstat -na
با تايپ كردن اين دستور در MS-DOS Prompt تمام پورتهايي كه داده ها و بسته ها را مي فرستند، مشخص مي شود. نشان " na " در تمام دستورات به معني نمايش همه پورتها و ليست كردن آدرسهاي شبكه و شماره فرمها در يک قالب عددي مي باشد.

دستور Netstat -a
اين دستور نيز مثل دستور Netstat -an يا na- عمل مي كند. فقط فرق آنها در اين است كه اين دستور پورتها را با معادل اسمي شان نشان مي دهد.

5. NS Lookup:

اين دستور براي توليد پيامهاي درخواست DNS استفاده مي‌شود، به طور كلي‌تر اين دستور به شكل رو به رو است:
NS Lookup DNS Name DNS Server

دستور كار جلسه سوم

آشنايي با TCP/IP و نحوه پيكربندي آن در سيستم لينوكس

دانشجوي گرامي، اين دستور كار را بدقت مطالعه كرده، آزمايش را انجام داده و پس از تكميل، براي مربي خود ارسال نماييد.

نيازمنديها

سخت افزار

- يك PC با سيستم عامل لينوكس براي انجام آزمايش و يك PC براي تهيه گزارش
- كارت شبكه جدا (10، 10/100، 1000 و يا Fiber) كه در PC نصب شده است.
- كابل Cross

نرم افزار

- Ethereal
- درايور كارت شبكه (در صورتيكه در سيستم عامل موجود نباشد.)
- مجوز root بر روي PC آزمايش
- يك نرم افزار Mail Client مانند Thunderbird بر روي لينوكس

زمان مورد نياز

- حداكثر 2 ساعت

دستور كار

مراحل ذيل را دنبال كنيد:

- در صورتي كه كامپيوترهاي شما به Switch و يا Hub شبكه متصل مي باشد، آنها را قطع كرده و توسط كابل Cross به يكديگر متصل نماييد. (توجه كنيد كه حداقل يكي از اين سيستمها مي‌بايست لينوكس باشد، سيستم ديگر مي تواند لينوكس يا ويندوز باشد)

- از سالم بودن و اتصال كابل و فعال بودن كارت شبكه اطمينان حاصل كنيد.
- حال از آدرسهاي Private يك Subnet با چهار آدرس به دلخواه انتخاب نموده و Subnet Mask مربوطه را محاسبه كنيد. توجه كنيد كه از اين 4 آدرس، آدرس اول و آخر قابل استفاده نيستند.(آدرسها و Subnet Mask را در گزارش بنويسيد)
- در صورتي كه نرمافزار فايروال بر روي سيستم شما فعال است، آن را از كار بياندازيد. (نرم افزار فايروال موجود در لينوكس غالبا با نام iptables شناخته مي شود).

<u>در هر مرحله از مراحل ذيل، دستور مورد استفاده و خروجي آن را بنويسيد.</u>

با استفاده از دستور ipconfig، دو آدرس معتبر (با توجه به توضيحات بالا) را به سيستمهاي گروه خود اختصاص دهيد

با استفاده از دستور ipconfig پيكربندي TCP/IP سيستمهاي خود را مشخص نماييد.(با جزيي ترين اطلاعات ممكن)
چندين آدرس ipconfigدر سيستم عامل لينوكس چگونه مي‌توان با دستور به يك كارت شبكه اختصاص داد؟ دو آدرس دلخواه ديگر به كارت شبكه IP خود اختصاص دهيد.
با استفاده از ابزار ping ارتباط دو سيستم را كنترل نماييد. (10 بسته ICMP بطول هركدام 64 بايت)
با استفاده از ابزار ping مقدار MTU (Maximum Transmission Unit) شبكه را پيدا كنيد. (دستور اجرا شده و نتيجه اجرا و MTU را در كادر زير بنويسيد.)
- راهنمايي: از گزينه اي استفاده نماييد كه بيت Don't Fragment را در سرآيند بسته IP فعال نمايد، سپس سايز بسته ICMP را تا اندازه اي افزايش دهيد كه نيازي به شكسته شدن بسته وجود نداشته باشد.(با خطا مواجه نشويد)

سيستم خود را مشخص نماييد. چگونه ARP جدول ARPبا استفاده از دستور مي‌توان محتويات اين جدول را پاک نمود؟
با استفاده از ابزار netstat كليه پورتهاي TCP كه در سيستم شما در حالت Listen قرار دارد، مشخص نماييد.
هدف از اين بخش آشنايي با مدل چهار لايه TCP/IP و برخي پروتكلهاي هر لايه مي‌باشد. مراحل ذيل را دنبال نماييد:
- ابتدا سيستم خود را به شبكه دانشكده متصل نماييد.

- پيكربنـدي TCP/IP را در حالـت خودكـار قـرار دهيـد. از دريافـت IP جديد توسط سيستم خود اطمينان حاصل كنيد.
- نرم افزار Ethereal را بـر روي سيسـتم خـود نصـب كـرده و تسـت نماييد.
- يـك نـرم افـزار پسـت الكترونيـك ماننـد Thunderbird را بـر روي سيستم خود نصب نموده و اجرا كنيد.
- مشخصات صندوق پسـتي كـه از طـرف دانشـگاه در اختيـار شـما قرار گرفته را بر روي Thunderbird تنظيم نماييد.

o پروتكل دريافت Email را POP3 و پروتكل ارسال Email را SMTP قرار دهيد.

- حـال Ethereal را فعـال كـرده و توسـط Thunderbird يـك Email متني سـاده براي يك آدرس دلخواه ارسـال نماييد.
- پس از اطمينان از اينكه Email مورد نظر ارسـال شـد، Ethereal را غير فعال نماييد.

با توجه به Packet هايي كه توسط Ethereal شنود شده به سوالات ذيل پاسخ دهيد. پيش از شروع پاسخگويي به سوالات بسته ها را بنحوي فيلتر نماييد تا تنها بسته هاي پروتكل SMTP نمايش داده شود.

لايه كاربرد

- اسـتاندارد پروتكـل SMTP در چـه RFC يـا RFC هـايي بيـان شـده اسـت.
- مراحل و پيامهاي مـورد نيـاز بـراي ارسـال يـك Email از Client بـه Server را استخراج كنيد.
- در هـر مرحلـه Server در پاسـخ بـه هـر پيـام دريـافتي از Client پاسخي حاوي كدي سه رقمي به آن ارسال مي‌كند، مفهـوم هـر يك از كدهاي ارسـالي چيسـت؟
- انتهاي بخش Data در Email چگونه مشخص شده است؟
- در صورتيكه Email شما داراي يـك ضـميمه (Attachment) باشـد، آن ضميمه چگونه ارسال مي‌شود؟

لايه انتقال

- در لايه انتقال از چه پروتكلي استفاده شده است. RFC مربوطه را مشخص نماييد.
- پورتهاي مبدا و مقصد در ارتباط بين Client و Server كدام است؟

- فیلدهاي Sequence No. و Acknowledge No. در لایه Transport چه نقشي دارند. مقدار هر کدام را مشخص نمایید.

لایه اینترنت

- در این لایه از چه پروتکلي و چه نسخه اي از این پروتکل استفاده شده است. RFC مربوطه را مشخص نمایید.
- آدرسهاي IP مبدا و مقصد را در درخواست و پاسخ مشخص نمایید.
- فیلد هاي IHL و Identification چیست و چه نقشي دارند؟

لایه Network Interface

- آدرسهاي Mac مبدا و مقصد را در درخواست و پاسخ مشخص نمایید.

دستور کار جلسه چهارم

آشنايي با سرويس‌هاي لايه كاربرد و نحوه پيكربندي آن در سيستم عامل ويندوز
DNS Server, DHCP Server, Web Server, Terminal Service

دانشجوي گرامي، اين دستور كار را بدقت مطالعه كرده، آزمايش را انجام داده و پس از تكميل، براي مربي خود ارسال نماييد.

1.نيازمنديها

سخت افزار

- PC با سيستم عامل ويندوز 2003 سرور.
- كارت شبكه (10، 10/100، 1000 و يا Fiber)
- [كابل Cross]
- شبكه محلي مرتبط با شبكه دانشكده
- CD ويندوز 2003 سرور.

نرم افزار

- Ethereal
- درايور كارت شبكه (در صورتيكه در سيستم عامل موجود نباشد.)

زمان مورد نياز

- حداكثر 5 ساعت

دستور كار

DNS

مراحل ذيل را دنبال نماييد.
بر روي ويندوز 2003 خود، DNS Server را راه‌اندازي نماييد و سرويس آن را در حالت اجرا قرار دهيد (براي راهنمايي مي‌توانيد به مستندات و اسلايدهاي پيوست دستور كار اين جلسه مراجعه كنيد).

يک Zone با عنوان NetLab#.edu ايجاد کنيد. بجاي # شماره گروه خود را قرار دهيد. بر روي اينZone دو ميزبان با نام group1 و group2 با آدرسهاي IP سيستمهاي خود تعريف کنيد.
براي هريک از ميزبانهاي تعريف شده, يک نام مستعار نيز تعريف کنيد.
نتيجه انجام مراحل فوق را در گزارش خود نشان دهيد. (يك Screen Shot از صفحه مديريتيDNS در گزارش قرار دهيد)
بررسي کنيد که چه حروفي در نام DNS قابل قبول نيست.(در گزارش مشخص کنيد)
نوع رکورد منبع (RR) هر يک از رکوردهاي تعريف شده فوق را بيان کنيد.
رکورد مناسب را جهت جستجوي معکوس اضافه کنيد و مشخص کنيد که چه نوع رکوردي براي اين منظور استفاده شده است. در سيستم سرويس گيرنده، با استفاده از group1.netlab#.edu ping و ping group2.netlab#.edu صحت عمليات خود را بررسي کنيد و نتيجه را در گزارش بياوريد. (براي اينکار مي بايست ابتدا در تنظيمات TCP/IP سرويس گيرنده خود آدرس IP سرويس دهنده DNS را قرار دهيد).
با استفاده از دستور NSLOOKUP به DNS Server خود متصل شويد و رکوردهاي تعريف شده
در آن سيستم را براي ناحيه NetLab#.edu به تفکيک انواع رکوردهاي DNS پرس و جو کنيد. در هر مرحله دستور اجرا شده و نتيجه اجراي آنرا بيان کنيد.

- راهنمايي: پس از اجراي nslookup با استفاده از دستور Server سرويس دهنده خود را مشخص کنيد و سپس با استفاده از دستور set type=A و set type=CNAME و مشخص نمودن Host مربوطه ،خروجي را ببينيد.

با استفاده از Ethereal ترافيک توليد شده پس از اجراي دستور NSLOOKUP و ارسالدرخواست DNS و پاسخ سرور را capture کنيد. معين کنيد DNS از چه شماره پورتي و از چه پروتکلي در لايه انتقال استفاده مي‌کند.

با استفاده از اين سرويس در ويندوز, مي‌توان از راه دور به يک ميزبان متصل شد و پس از مراحل تصديق اصالت, کارها و تنظيمات مورد نظر را روي ميزبان راه دور انجام داد.
Terminal Server را روي کامپيوتر سرويس دهنده خود فعال نماييد.
با استفاده از ابزار Remote Desktop که در کليه نسخه هاي ويندوز XP و بالاتر، تعبيه شده، به
سرويس دهنده خود متصل شويد.

- با استفاده از دستور mstsc در منوي Run مي توانيد Remote Desktop را اجرا نماييد.

پس از برقرار ارتباط و تصديق اصالت در سرويس دهنده، يك Screen Shot از اتصال خود با
سرويس دهنده در گزارش بياوريد.
در حين كار، Ethereal را در وضعيت شنود قرار دهيد و به سوالات ذيل پاسخ دهيد:

- Terminal Service از چه پورتي براي مبادله اطلاعات استفاده مي‌كند؟

در سمت سرويس دهنده با استفاده از ابزار Terminal Service Manager كاربراني كه در حال
استفاده از سيستم هستند را مشخص نماييد.(Screen Shot در گزارش)
يكي از كاربراني كه از راه دور به سرور متصل است را انتخاب نماييد و نشان دهيد كه چه پروسسهايي
را در حال اجرا دارد. (Screen Shot در گزارش)

به دليل اينكه نصب DHCP server جديد, باعث عوض شدن تنظيمات سيستمهاي شبكه مي‌شود به همين دليل در اين آزمايش, ارتباط hub آزمايشگاه را با شبكه دانشكده قطع مي‌كنيم تا اختلالي در شبكه دانشكده پيش نيايد و در انتهای آزمایش نیز سرویس DHCP server را غیر فعال کنید.
مراحل ذيل را دنبال نماييد:
سرويس دهنده را با استفاده از ويندوز Boot 2003 نماييد. سرويس گيرنده مي تواند هر سيستم عاملي باشد.
در صورتي كه كامپيوترهاي شما به Switch و يا Hub شبكه متصل مي باشد، آنها را قطع كرده و توسط كابل Cross به يكديگر متصل نماييد.
سرويس DHCP Server را در سرويس دهنده خود نصب كرده و كنسول مديريتيDHCP را اجرا نماييد.
دو محدوده جديد IP براي 128 ميزبان و Subnet mask مناسب هر يک را تعريف كنيد. (Screen Shot در گزارش)
تنظيمات TCP/IP را در سرويس گيرنده در حالت خودكار قرار دهيد. پس از دريافت IP بررسي كنيد كه آيا IP جديد, در محدوده تعريف شده هست يا نه. (Screen Shot در گزارش)
يک آدرس IP براي سيستم سرويس گيرنده (بر اساس MAC address) رزرو كنيد و در سمت سرويس گيرنده با استفاده از دستور ipconfig /renew ببينيد كه آيا آدرس جديد به سرويس گيرنده اختصاص مي يابد يا نه. (Screen Shot در گزارش)
اين امكان در DHCP Server وجود دارد كه بخشي از محدوده آدرس تعيين شده را براي منظور هاي خاصي كنار گذاشت و به هيچ سرويس گيرنده اي اختصاص نداد. 10 آدر س IP را Exclude كرده و در گزارش با Screen Shot نشان دهيد.

پيامهاي DHCP مبادله شـده بـين Client و Server را بـا اسـتفاده از Ethereal شنود نماييد.
معين كنيد كه DHCP از چه پروتكلي در لايه انتقال استفاده مي‌كند و در server و client بر روي چه پورتي كار مي‌كند.
سرويس دهنده DHCP را غير فعال نماييد. در اين حالت به سرويس گيرنده چه آدرس IP اختصاص داده مي شود.

Web Server (IIS)
در اين قسمت يک وب سايت بسيار ساده (متشكل از يک صفحه وب) ايجاد مي‌كنيد و بر روي سيستم خود براي مشاهده ديگران قرار مي‌دهيد. از سيستم سرويس گيرنده گروه خود جهت ديدن و تست وب سايت استفاده كنيد. در اين مرحله از نامهاي DNS كه در مراحل قبل براي سيستم خود ثبت كرديد, استفاده نماييد.
- IIS را نصب و كنسول مديريتي Internet Information Services(IIS) آن را اجرا نماييد.
- يک صفحه ساده html كه حاوي شماره و نام اعضاي گروه مي‌باشد را ايجاد كرده و بگونه‌اي عمل كنيد كه اين صفحه از طريق هر يک از آدرس‌هاي تايپ شده در مرورگر قابل دسترس باشد:
http://www.netlab#.edu/
www يك نام مستعار براي group2 است.(سيستم سرويس دهنده)
- ترافيک مبادله شده بين وب سرور و مرورگر خود را capture كنيد و سرآيند درخواست ارسال شده, سرآيند پاسخ دريافت شده را مشخص كنيد.
- Status Code پاسخ دريافت شده را مشخص كنيد. اگر صفحه مورد نظر شما پيدا نشود اين كد چه مقداري خواهد داشت؟
- در صورتيكه دسترسي بدون نام(Anonymous) را به سايت, غيرفعال كنيد و تنها اجازه بازديد پس از تصديق اصالت داده شود, سرور با چه پيامي از مرورگر تقاضاي user و password مي‌كند؟

مطالب تكميلي

نرم‌افزار شبکه

1. پروتکل
2. سيستم عامل شبکه[3]: سيستم عاملي است که روي سرور نصب شده است.
3. سيستم عامل client[4]: سيستم عاملي است که بر روي dientها نصب شده است.
4. شبکه ترکيبي: شبکه‌اي که متشکل از NOS و COS مي‌باشد.

NOS سيستم عاملي است که باعث ارائه سرويس تخصصي و با کيفيتي به ديگر سيستم‌ها مي‌شود. مثل Linux، Win 2000 server، Win 2003 server، Win NTو ...

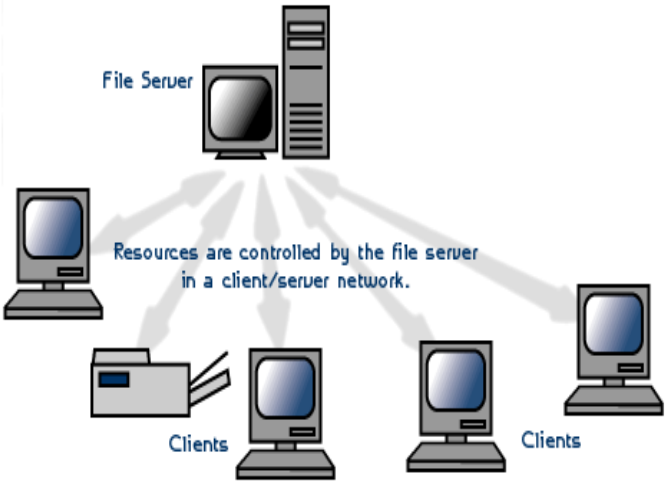
COS سيستم عاملي است که بر روي clientها نصب مي‌شود تا بتوانند با سيستم عامل شبکه ارتباط برقرار کند. مثل Win xp.

روش‌هاي مديريت شبکه:

1. Client / Server (server based):

در این مدل یک ایستگاه در خواست انجام کارش را به سرویس دهنده ارائه می دهد و سرویس دهنده پس از اجرای وظیفه محوله ، نتایج حاصل را به ایستگاه در خواست کننده عودت می دهد . در این مدل حجم اطلاعات مبادله شده شبکه ، در مقایسه با مدل مبتنی بر سرویس دهنده کمتر است و این مدل دارای کارایی بالاتری می باشد . مانند وب سرورها

در استاندارد مايکروسافت به اينگونه از شبکه‌ها,Domain گفته مي‌شود.



2. Peer-to-peer:

در این شبکه ایستگاه ویژه ای جهت نگهداری فایل های اشتراکی و سیستم عامل شبکه وجود ندارد. هر ایستگاه می تواند به منابع سایر ایستگاه ها در شبکه دسترسی پیدا کند . هر ایستگاه خاص می تواند هم بعنوان Server و

---

[3] NOS
[4] COS

هم بعنوان Client عمل کند . در این مدل هر کاربر خود مسئولیت مـدیریت و ارتقـاء دادن نـرم افزارهـای ایسـتگاه خـود را بعهـده دارد . از آنجـایی کـه یـک ایستگاه مرکزی برای مـدیریت عملیـات شـبکه وجـود نـدارد ، ایـن مـدل بـرای شبکه ای با کمتر از 10 ایستگاه بکار می رود.
در استاندارد مایکروسافت به آن شبکه‌هاي work group گویند.

سرور[5]: يك برنامه است كه در حال اجرا است.
سه ويژگي كه در مدل client/server مهم است:
1. امنيت
2. سرعت پردازش
3. تعداد clientها

[5] Server

سرويس[6]:

يك برنامه است كه به طور پيوسته در Background اجرا مي‌شود در حالي كه در همان زمان برنامه‌هاي ديگر در حال اجرا است. در اصل سرويس‌ها قابليت شبكه‌بندي هستند. سرويس‌ها اصولا به دو دسته تقسيم مي‌شوند. اولين گروه سرويس‌ها ضروري هستند كه هسته اصلي شبكه‌بندي مي‌باشند. سرويس‌هاي ضروري عبارتند از:

1) سرور: توانايي سيستم براي به اشتراك گذاشتن منابع اش از قبيل فايل‌ها و Printer و...
2) ايستگاه كاري: توانايي سيستم براي دسترسي به منابع اشتراك گذاشته در شبكه مي‌باشد.
3) مرورگر كامپيوتر[7]: ليستي از منابع به اشتراك گذاشته در شبكه را نشان مي‌دهد.
4) Net logon: يك كانال امن براي ارتباط بين كامپيوترهاي ويندوز فراهم مي‌كند.
5) Messenger: توانايي سيستم براي نمايش ساختارهاي Pop-Up مي باشد.
6) Alerter: همراه با سرويس Messenger براي اعلان كاربران مديريتي انتخاب شده، استفاده مي‌شود.

نكته: با long on كردن، سرويسها شروع مي‌شوند. اتمام سرويس‌ها با انجام عمل log off كردن صورت مي‌گيرد.

گروه دوم سرويس‌هاي اختياري هستند اما مهم مي‌باشند كه عبارتند از:

1) IIS (Internet Information Service):
سرويسي كه براي ايجاد سرويس‌هاي اينترنت از قبل FTP و WWW استفاده مي‌شود.

2) WINS (Windows Internet Naming Service) :
براي انجام Resolve كردن اسم‌هاي كامپيوترهاي ويندوز (NetBios) به آدرس‌هاي اينترنت (IP) استفاده مي‌شوند.

3) DNS (Domain Name System):
براي Resolve كردن اسم‌هاي ميزبان DNS به آدرس‌هاي IP مي‌باشند.

4) DHCP (Dynamic Host Configuration Protocol):
به طور اتوماتيك تنظيمات TCP/IP را به روي چندين Client پيكربندي مي‌كند.

---

[6] Service
[7] Computer Browser

5) RRAS (Routing and Remote Access Service):
سرويسي است كه براي مسيريابي، اتصال بين شبكه LAN با يك LAN و يا با يك WAN استفاده مي‌شود. همچنين از پروتكل‌هاي مسيريابي پيشتيباني مي‌كند.

6) DFS (Distributated File System):
اعمال يك Drive مشترك بين تمامي سرورها در شبكه است به طوري كه Client فكر كند كه دارد با يك سرور واحد مشترک كار مي‌كند.

7) MCS (Microsoft Cluster Server):
توانايي در Windows 2000 Advance Server و Windows NT Version 4.0interprise server مي‌باشد كه موجب مي‌شود چندين سرور به صورت گروهي با يكديگر كار كرد. اين امر باعث بالا رفتن Performance و اعمال مقابله با خطا[8] مي‌شود.

DHCP :
خانواده پروتكل هايTCP/IP(به دليل استفاده شان در اينترنت و سازگاري آنها با تقريباً تمام سيستم عامل هاي شبكه مورد استفاده) در حال حاضر، تقريباً در همهLANهاي كوچک مورد استفاده قرار مي گيرند. مهمترين مشكل مديريتي برقراري و نگهداري يک شبكهTCP/IP آن است كه بايد به هر گروه يک آدرسIP ي منحصر به فرد اختصاص داده شود. پارامترهاي ديگرTCP/IP نيز با مقادير مناسب پيكربندي شوند. دريک شبكه بزرگ انجام اين اعمال براي تک تک ايستگاههاي كاري به صورت دستي نه تنها طاقت فرساست، بلكه به طراحي دقيق نياز دارد تا هيچ دو آدرسIP مثل هم نباشند.

در ادامه در مورد سرورهاي پركاربرد صحبت مي نماييم.

چند server مهم، عبارتنداز :
http server – email server- Ftp server – Print server – File server
Win Server 2003 داراي 4 version خاص مي باشد.
1) Web (2 Server (3 Enterprise (4 Data Center
به ترتيب از تعداد 1 تا 4 توانايي آنها بيشتر و بيشتر مي شود.

نسخه ويندوز 2003	حداكثر تعداد پردازنده	حداكثر فاصله قابل پشتيباني

Web	2	2 G
Standard	4	4G
EnterPrise	8	32G
DataCenter	16	64G

نسخه وب : نقطه سرويسهاي پشتيباني از شبكه (سروسيسهاي عام تر) را انجام مي دهد و سرويسهاي پيشرفته شبكه را پشتيباني نمي كند بطور مثال در مورد امنيت زياد قوي نيست . نسخه استاندارد نسبت به نسخه web توابع بيشتري را فراهم كرده است.

دستور كار جلسه پنجم

آشنايي با مسيريابي و پروتكلهاي مربوط به آن

دانشجوي گرامي، اين دستور كار را بدقت مطالعه كرده، آزمايش را انجام داده و پس از تكميل، براي مربي خود ارسال نماييد.

نيازمنديها

سخت افزار

- PC سرويس دهنده با سيستم عامل ويندوز 2003 و لينوكس.
- PC سرويس گيرنده با سيستم عامل ويندوز XP.
- كارت شبكه (10، 10/100، 1000 و يا Fiber) بر روي سرويس دهنده
- يك كابل Cross و يك كابل مستقيم.
- CD هاي لينوكس Fedora و ويندوز 2003.
- HUB يا سوييچ.

نرم افزار

- Ethereal
- درايور كارت شبكه (در صورتيكه در سيستم عامل موجود نباشد.)
- نرم افزار Visio.

زمان مورد نياز

- حداكثر 5 ساعت

دستور كار

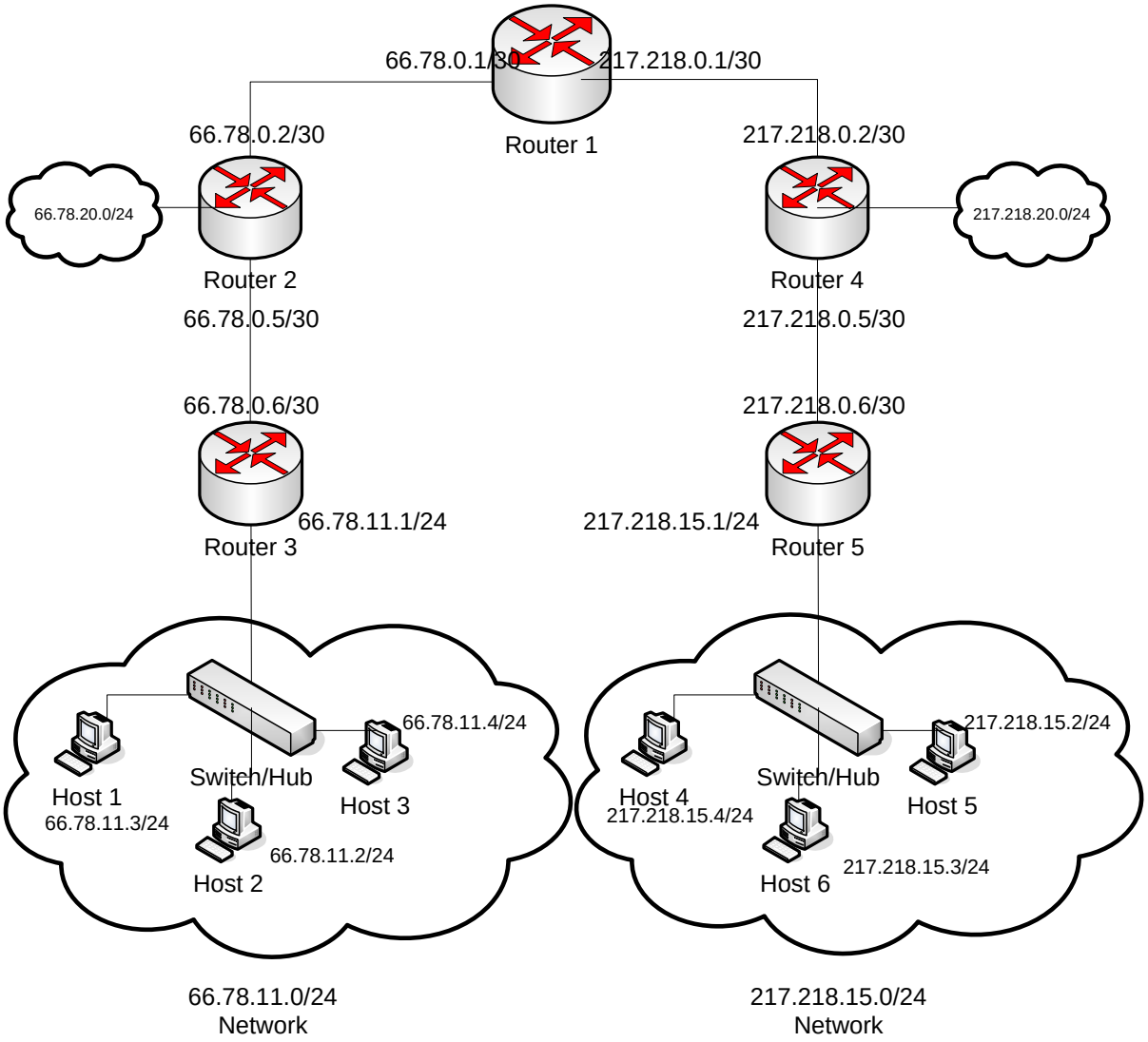
يكي از اساسي‌ترين نيازهاي در شبكه‌ها، مسيريابي است. مسيريابي (routing) روندي براي پيش بردن (forwarding) يک بسته برمبناي آدرسهاي مبدا و مقصد مي باشد. به عبارت ديگر يک مسير براي انتقال يک بسته مي باشد. هردستگاه متصل به شبكه از نوع TCP/IP كار مسيريابي را حداقل براي بسته هايي كه خودش توليد كرده است، انجام مي دهد. اگر دستگاهي بسته هايي را مسيريابي كند كه خود توليد نكرده است به آن

دستگاه **مسيرياب** گفته مي شود. عمل مسيريابي براساس آدرس مقصد انجام مي گيرد. به اين نوع مسيريابي، **مسيريابي ساده** گفته مي شود.
مسيرياب مي تواند يک کامپيوتر و يا يک تکنولوژي سخت افزاري باشد که مي تواند عمل مسيريابي را انجام دهد. يک دستگاه لينوکسي به طور پيش فرض يک مسيرياب نيست. به اين معني که فقط بسته هايي که خودش توليد کرده است را مسيريابي ميکند.
در اين جلسه يك شبکه نمونه نسبتا" بزرگ شامل تعدادي مسيرياب را پيکربندي مي نماييد(پيکربندي ايستاي جداول مسيريابي). در بخش اول آزمايش از ويندوز 2003 بعنوان مسيرياب استفاده مي‌شود و در بخش دوم آزمايش از لينوکس بعنوان مسيرياب استفاده خواهد شد. در جلسه بعدي آزمايشگاه با مسيريابهاي سخت افزاري آشنا خواهيد شد.

نقشه شبکه فرضي

در ذيل نقشه شبکه فرضي را مشاهده مي‌کنيد

Sample Network Topology



در ايـن آزمـايش هـدف ايـن اسـت كـه بـا پيكربنـدي درسـت مسـيريابها كليـه سيستم ها و مسيريابها بتوانند با ساير سيستمها ارتباط برقرار كنند. مراحل كلي كـه در هـر دو بخـش ايـن آزمـايش (مسـيريابهاي ويـندوز و مسـيريابهاي لينوكس) مي بايست انجام شود به اين صورت است:

- اتصال فيزيكي سيستمها به هـم بـر اسـاس نقشـه ارائـه شـده. توجـه داشته باشيد كه ارتباطات دو كـارت شـبكه بـا هـم مـي‌بايسـت توسـط كابل Cross صورت پذيرد.
- پيكربندي TCP/IP كليه كارتهاي شبكه مشخص شده در نقشه فوق.

- راه اندازي سرويس مسيريابي در سيستم عامل.
- پيكربندي جداول مسيريابي در مسيريابها
- پيكربندي درست Default Gateway در سيستمهاي موجود در هر LAN.

راه اندازي شبكه فرضي با استفاده از مسيريابهاي ويندوز

در اين بخش از آزمايش، مسيريابها داراي سيستم عامل ويندوز 2003 هستند. مراحل ذيل را دنبال نماييد.
اتصال فيزيكي سيستمها و مسيريابها را برقرار نماييد.
پيكربندي TCP/IP هر يك از كارتهاي شبكه مربوط به گروه خود را انجام دهيد.
تست اتصال مستقيم ليتكها: با استفاده از دستور ping ارتباط كارتهاي شبكه گروه خود را با كارتهاي شبكه سيستم مجاور كه با آن بطور مستقيم در ارتباط هستيد، كنترل نماييد.
سرويس مسيريابي را در سيستم عامل ويندوز 2003 فعال نماييد. براي انجام اين كار از كنسول مديريتي Routing and remote access (RRAS) استفاده نماييد.
مسيرياب خود را بدين صورت پيكربندي نماييد:

- در مسيريابهاي 2،3،4،5 آدرس Default Gateway را معادل آدرس IP مسيرياب بالاي آن قرار دهيد.
- در مسيرياب 2 يك Route Entry براي شبكه 66.78.11.0/24 اضافه نماييد.
- در مسيرياب 4 يك Route Entry براي شبكه 217.218.15.0/24 اضافه نماييد.
- در مسيرياب 1 يك Route Entry براي شبكه 217.218.0.0/16(با گام بعدي روتر 4) و يك Route Entry براي شبكه 66.78.0.0/16(با گام بعدي روتر 2) اضافه نماييد.

Default Gateway ميزبانها را معادل آدرس IP مسيرياب بالايي قرار دهيد. (روتر 5 يا روتر 3)
حال كليه گرههاي شبكه(مسيريابها و ميزبانها) مي بايست با همديگر ارتباط برقرار نمايند. اين مساله را مي توانيد با دستور ping بررسي نماييد.
موارد ذيل در گزارش آورده شود:

- پيكربندي TCP/IP كليه كارتهاي شبكه مربوط به گروه خود.(ipconfig /all)

- جدول مسيريابي سيستم.(route print)
- خروجي دستور ping براي ارتباط با تك تك گرههاي موجود در شبكه. (حداقل 6 مورد)
- خروجي دستور tracert براي ارتباط با تك تك گرههاي موجود در شبكه(حداقل 6 مورد)

نكته: فايروال موجود در سيستمهاي ويندوز XP ممكن است جلوي بسته هاي ورودي از ساير LAN ها را بگيرد. لذا در حين آزمايش فايروال را پيكربندي كرده و يا غيرفعال نماييد.

راه اندازي شبكه فرضي با استفاده از مسيريابهاي لينوكس

در اين بخش از آزمايش، مسيريابها داراي سيستم عامل لينوكس هستند. كليه مراحل با استفاده از دستورات Shell (از محيط گرافيكي استفاده نشود) انجام شود. مراحل ذيل را دنبال نماييد.
اتصال فيزيكي سيستمها و مسيريابها را برقرار نماييد.
پيكربندي TCP/IP هر يك از كارتهاي شبكه مربوط به گروه خود را انجام دهيد.
نمونه:

```
ipconfig eth0 192.168.12.2 netmask 255.255.255.0
```

تست اتصال مستقيم ليتكها: با استفاده از دستور ping ارتباط كارتهاي شبكه گروه خود را با كارتهاي شبكه سيستم مجاور كه با آن بطور مستقيم در ارتباط هستيد، كنترل نماييد.
سرويس مسيريابي را در سيستم عامل لينوكس فعال نماييد. اي كار مي تواند بصورت موقتي يا بصورت دائم انجام شود:
روش موقت:

- echo 1>/proc/sys/net/ipv4/ip_forward

روش دائم:

- پيكربندي فايل /etc/sysctl.conf (Net.ipv4.ip_forward=1)
- راه اندازي مجدد سرويس شبكه: Service network restart

در اين آزمايش از روش موقت استفاده نماييد. در صورتيكه مي خواهيد از روش دائم استفاده كنيد، مي بايست پيكربندي TCP/IP كارتهاي شبكه را نيز در فايل مربوطه اصلاح كنيد تا پس از راه اندازي مجدد سرويس شبكه آدرسهاي IP بدرستي تنظيم شود.
مسيرياب خود را بدين صورت پيكربندي نماييد:

- در مسيريابهاي 2،3،4،5 آدرس Default Gateway را معادل آدرس IP مسيرياب بالاي آن قرار دهيد.

Sample: route add default gw *ip_address*

- در مسيرياب 2 يك Route Entry براي شبكه 66.78.11.0/24 اضافه نماييد.

Sample: route add *networkaddress/prefix nexthop_ip*

- در مسيرياب 4 يك Route Entry براي شبكه 217.218.15.0/24 اضافه نماييد.
- در مسيرياب 1 يك Route Entry براي شبكه 217.218.0.0/16(با گام بعدي روتر 4) و يك Route Entry براي شبكه 66.78.0.0/16(با گام بعدي روتر 2) اضافه نماييد.

Gateway ميزبانها را معادل آدرس IP مسيرياب بالايي قرار دهيد. (روتر 5 يا روتر 3)
حال كليه گره‌هاي شبكه(مسيريابها و ميزبانها) مي بايست با همديگر ارتباط برقرار نمايند. اين مساله را مي توانيد با دستور ping بررسي نماييد.
موارد ذيل در گزارش آورده شود:

- پيكربندي TCP/IP كليه كارتهاي شبكه مربوط به گروه خود.(ifconfig -a)
- جدول مسيريابي سيستم.(route)
- خروجي دستور ping براي ارتباط با تك تك گرههاي موجود در شبكه. (حداقل 6 مورد)
- خروجي دستور traceroute براي ارتباط با تك تك گرههاي موجود در شبكه(حداقل 6 مورد)

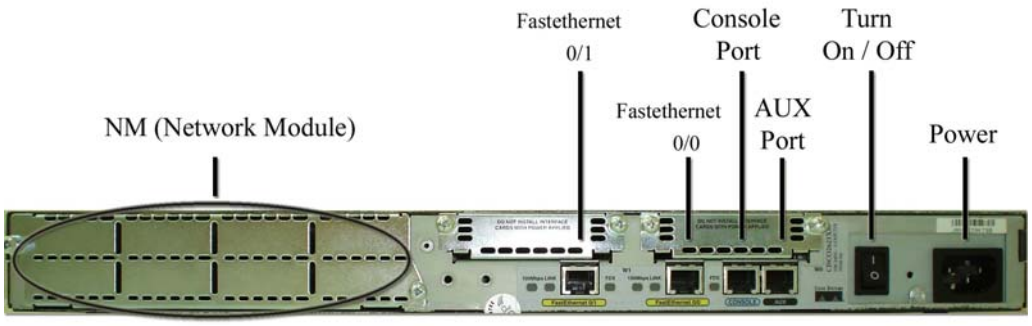
نكته: در سيستمهاي لينوكس يك نرم افزار فايروال به اسم iptables وجود دارد. پيش از انجام آزمايش با استفاده از دستور زير اين فايروال را از غيرفعال نماييد:

service iptables stop

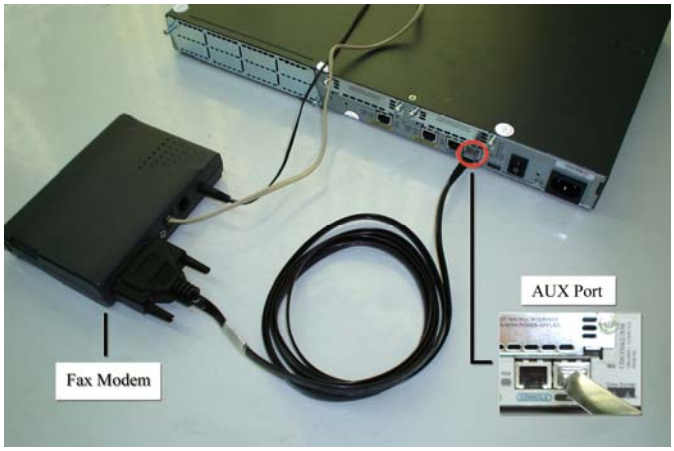
نكته: فايروال موجود در سيستمهاي ويندوز XP ممكن است جلوي بسته هاي ورودي از ساير LAN ها را بگيرد. لذا در حين آزمايش فايروال را پيكربندي كرده و يا غيرفعال نماييد.

مطلب تكميلی
آموزش مقدماتي پيكربندی روتر

قبـل ازبرنامـه ريـزي وپيکـره بنـدي(Config) مسـيرياب cisco نگـاهي گـذرا بـه بعضي ازمولفه هائي که درپشـت روترتعبيه شـده اسـت مي اندازيم.



اين مولفه هاعبارتنداز:
1. محل اتصال برق وکليدخاموش وروشـن
2. پورت کنسـول: اين پورت ابتدائي ترين راه برقراري ارتبـاط بامسـير يـاب مـي باشـد. ازطريق اتصال يک کابل مخصـوص(Console Cable) بـه ايـن پـورت مـي توان مسـيرياب رابه يکPC متصل نمود. پورت کنسـول ازلحاظ ظاهري شـبيه بـه پورت RJ-45 اسـت.
3. پورتهاي اترنت: ايـن پورتهـا جهـت اتصـال بـه Lan مـي باشـد. تحـت عنـوان FastEthernet 0/0 وFastEthernet 0/1 درپشـت روترشـناخته مي شـود.
4. پورت AUX: اين پـورت جهـت اتصـال يـک مـودمExternal بـه مسـيرياب مـي باشـد(مطابق شـکل زير)

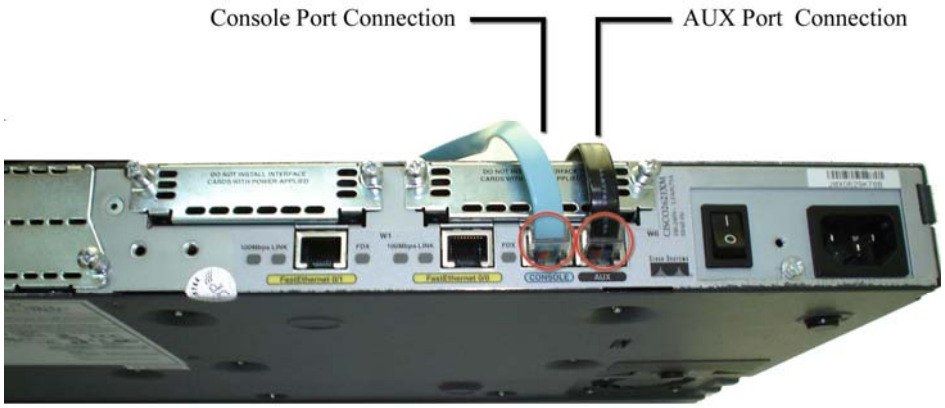


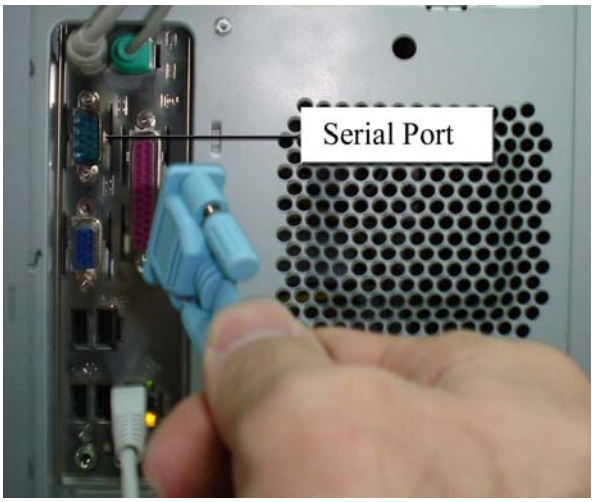
5. پورت توسعه WAN(WIC): درپشت مسيرياب دوتيغه فلزي وجوددارد.اين دوتيغه محافظي براي محل قرارگرفتن WIC است. وقتي اين تيغه ها از روتر جدا گردد. يکي از مهمترين کارتهاي توسعه مسيريابهاي سيسکو آشکارميگردد.

6. Slat جهت ماژول NM: با برداشتن تيغه فلزي بزرگي که در پشت روتر تعبيه شده مي توان ماژولهاي NM را که جهت اتصال خطوط تلفن به روتر براي Dial کردن وتماس با مسيرياب است درون Slat اش قرارداد.

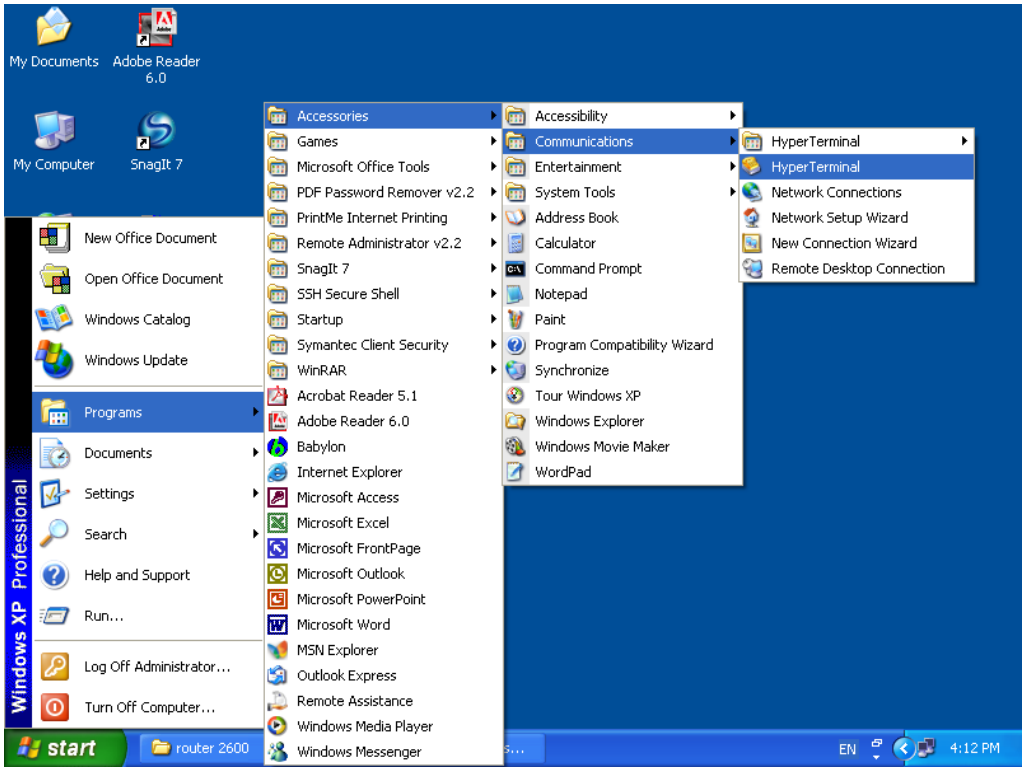
مراحل پيش از پيکربندی مسيرياب

درهنگامي که به مسيرياب دسترسي داشته باشيم، مي توانيم با استفاده از کابل کنسول تنظيمات و پيکربندي لازم را روي مسيرياب انجام دهيم.
يک سمت کابل را به پورت کنسول (RJ-45) مسيرياب وصل نموده، سمت ديگرآن را به يکي از پورتهاي سريال PC وصل مي کنيم.





HyperTerminal که يکي از متداول ترين آنها Hyper Emulation توسـط يکـي از برنامه هاي است، مراحل کاررا آغازمي کنيم.

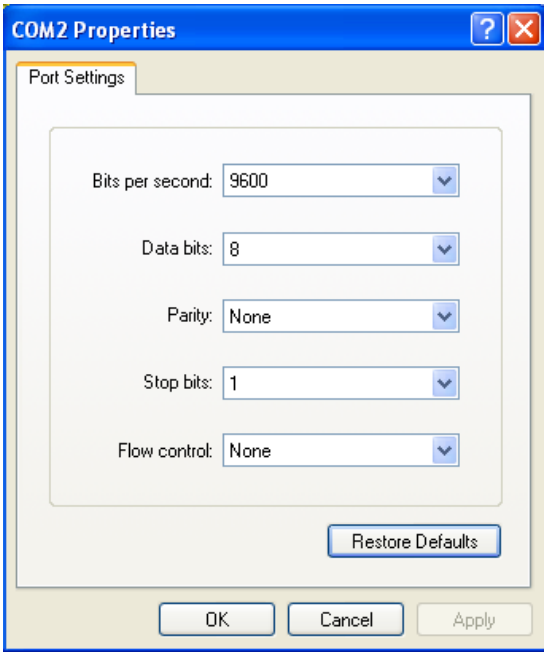


آدرس HyperTerminal درويندوز

در اين محيط، براي ارتباط به مسيرياب، ابتدا از كاربرنامي خواسته مي شود، كه كاربر با وارد كردن يک نام دلخواه وارد مرحله بعد مي شود.

درمرحله بعد، كاربر با انتخاب پورتي از كامپيوتركه كابل كنسول را به آن متصل نموده وارد گام بعدي مي شود.

درگام بعدي، كاربر با كليک نمودن دكمه Restore Defaults و مشاهده تنظيمات مطابق باشكل زير مي تواند به مسيرياب متصل شود.



راه اندازي وفعال نمودن مسيرياب

الف) دراين قسمت، ابتدا به پيكربندي يک مسيريابي كه تاكنون تنظيماتي روي آن انجام نگرفته است مي پردازيم.
نكته: همواره وقتي مي خواهيم يک مسيرياب را براي نخستين بار، پيكربندی نمائيم، بايد از كابل كنسول استفاده نمائيم.)

كابل كنسول رابه روش گفته شده درصفحات قبل به مسيرياب وPC متصل مي كنيم. مسيرياب را روشن كرده و وارد برنامه HyperTerminal مي گردد. هنگامي كه مسيرياب كاملا راه اندازي گرديد، تشخيص خواهد داد كه هيچگونه پيكربندي قبلي وجودندارد. بطور خودكار وارد setup dialog ميشود.

(درصفحه بعد مراحل راه اندازي يک مسيرياب براي اولين بارنشان داده شده است)

```
program load complete, entry point: 0x80008000, size: 0x59421c
Self decompressing the image : ########################################################
######################################### [OK]

Smart Init is enabled
smart init is sizing iomem
  ID            MEMORY_REQ                  TYPE
00036D          0X00103980 C2621XM Dual Fast Ethernet
                0X000F3BB0 public buffer pools
                0X00211000 public particle pools
TOTAL:          0X004085

If any of the above Memory Requirements are
"UNKNOWN", you may be using an unsupported
configuration or there is a software problem and
system operation may be compromised.
Rounded IOMEM up to: 5Mb.
Using 15 percent iomem. [5Mb/32Mb]

              Restricted Rights Legend

Use, duplication, or disclosure by the Government is
subject to restrictions as set forth in subparagraph
(c) of the Commercial Computer Software - Restricted
Rights clause at FAR sec. 52.227-19 and subparagraph
(c) (1) (ii) of the Rights in T
Software clause at DFARS sec. 252.227-7013.

           cisco Systems, Inc.
           170 West Tasman Drive
           San Jose, California 95134-1706


Cisco Internetwork Operating System Software
IOS (tm) C2600 Software (C2600-I-M), Version 12.2(8)T5,  RELEASE SOFTWARE (fc1)
TAC Support: http://www.cisco.com/tac
Copyright (c) 1986-2002 by cisco Systems, Inc.
Compiled Fri 21-Jun-02 08:50 by ccai
Image text-base: 0x80008074, data-base: 0x80A2BD40

cisco 2621XM (MPC860P) processor (revision 0x100) with 27648K/5120K bytes of mem
ory.
Processor board ID JAE07140916 (2834058322)
M860 processor: part number 5, mask 2
Bridging software.
X.25 software, Version 3.0.0.
2 FastEthernet/IEEE 802.3 interface(s)
32K bytes of non-volatile configuration memory.
16384K bytes of processor board System flash (Read/Write)


         --- System Configuration Dialog ---

Would you like to enter the initial configuration dialog? [yes/no]:
```

براي اينكه مراحل پيكربندي خودكار را ادامه بدهيد درجواب آخرين سطرمراحل boot شدن مسيرياب، yes را واردكنيد.
پس از پاسخ مثبت به سوال بالا ازكاربر سوال مي شود كه آيا مي خواهي تنظيمات مقدماتي انجام دهي ياخير؟

```
Would you like to enter basic management setup? [yes/no]:
```

اگرهدف از پيكربندی مسيرياب، تنها دادن نام وكلمه عبوروتنظيمات ip جهت interface هاباشد به سوال بالا جواب مثبت مي دهيم و اگرتنظيمات دقيق تري نيازداشته باشيم، جواب منفي مي دهيم.

تنظيم دقيق و مبسوط مسيرياب

براي ورود به اين برنامه درپاسخ به سوال بالا no را وارد مي كنيم. اگردر پاسخ به پرسش بعد، جواب مثبت دهيم، مشخصات كارتهاي واسط شبكه (Interface) درخروجي ظاهرمي شود.

```
First, would you like to see the current interface summary? [yes]: y

Any interface listed with OK? value "NO" does not have a valid configuration

Interface                  IP-Address      OK? Method Status
ocol
FastEthernet0/0            unassigned      NO  unset  up

FastEthernet0/1            unassigned      NO  unset  up
```

پس از مشاهده وضعيت كارتهاي شبكه، از كاربرخواسته مي شود تا نام انتخابي خود (host name) را وارد نمايد. اگر در اين مرحله نامي تايپ نشود وكليدEnter زده شود. سيستم عامل نام پيش فرض خود را كه همان كلمه Router است جهت نام روتر درج مي كند.

```
Enter host name [Router]:

The enable secret is a password used to protect access to
privileged EXEC and configuration modes. This password, after
entered, becomes encrypted in the configuration.
```

پس از اين مرحله از كاربر يک كلمه عبورخواسته مي شود تا هر شخصي نتواند پيكربندي مسيرياب را تغييردهد.

```
Enter enable secret: 246

The enable password is used when you do not specify an
enable secret password, with some older software versions, and
some boot images.
```

درادامه پرسش و پاسخها از كاربرخواسته مي شود كه اگر در مرحله قبل كلمه عبوري انتخاب نكرده است با وارد كردن عبارت Enable كلمه عبورپوچ را فعال نمايد. سپس كلمه عبوري جهت Telnet كردن (ارتباط بامسيرياب ازراه دور) از كاربرخواسته مي شود.

```
Enter virtual terminal password:
```

سوال بعدي درخصوص پيكربندي پروتكلSNMP است. فعال كردن اين پروتكل زماني مفيد است كه ما در محيط شبكه بيش از يک مسيرياب داشته باشيم

و بخواهيم بر وضعيت آنها نظارت نمائيم. براي اينكه پيكربندي مسرياب زياد پيچيده نشود به اين سوال پاسخ منفي مي دهيم. به چند پرسش بعد همانند زيرپاسخ مي دهيم.

```
Configure IP? [yes]: y
  Configure IGRP routing? [yes]: n
  Configure RIP routing? [no]: n
Configure bridging? [no]: n
```

در ادامه، جهت پيكربندي مودمهاي مسيرياب سوالاتي پرسيده مي شود كه اگرروي مسيرياب ماژول NM نصب شده باشد، طبق نمونه زيرشروع به پيكربندی آن مي نمائيم. **(درصورت نياز)**

```
Configure Async lines? [yes]: y
  Async line speed [115200]:
  Will you be using the modems for inbound dialing? [yes]:
    Would you like to put all async interfaces in a group and configure
    them all at one time ? [yes]:
    Allow dial-in users to choose a static IP address? [no]:
    Configure for TCP header compression? [yes]:
    Configure for routing updates on async links? [no]:
    Enter the starting address of IP local pool? [X.X.X.X]: 10.10.10.200
    Enter the ending address of IP local pool? [X.X.X.X]: 10.10.10.215

    You can configure a test user to verify that
    your dial-up service is working properly
  Would you like to create a test user? [no]: y
    What is the username of the test user?: ali
    What is the password of the test user?: 246
  Will you be using the modems for outbound dialing? [no]:
```

ابتدا سوال مي شود كه آيا مي خواهيد خطهاي Async را پيكربندی نمائيد. پس از دادن جواب مثبت از كاربر سرعت ارتباطي خطوط سوال مي شود. درپاسخ به اين سوال كليد Enter را فشارمي دهيم تا مقدار پيش فرض آن كه 115200 است ذخيره گردد. سوال بعدي را با yes جواب مي دهيم تا كاربران بتوانند از بيرون با مسيرياب تماس بگيرند و ارتباط برقرارکنند. دوپرسش بعدي را با زدن كليدEnetr جواب مي دهيم تا اولا اينكه اين امكان وجودداشته باشد كه همگي مودمها را با هم پيكربندي كنيم. ثانيا IP هارا خود مسيرياب به صورت Dynamic به كاربران اختصاص دهد و كاربران نتوانندIP شان را دستي واردنمايند. دوسوال بعدي را با no پاسخ مي دهيم. بعد از آن محدوده تخصيص IP را جهت كاربران يک نام كاربر وكلمه عبور براي كساني كه مي خواهند توسط خطوط تلفن با شبكه ما ارتباط برقرارنمايند، تعريف مي نمائيم. درآخر اين قسمت به سوال اينكه توسط مودمها بتوان با بيرون مسيرياب تماس گرفت، جواب منفي مي دهيم. پس از پيكربندي مودمها نوبت به پورتهاي فيزيكي قابل اتصال به شبكه (FastEthernetها) مي

رسد. در اين قسمت، ابتدا FastEthernet 0/0 پيكربندي مي شود و درصورت تمايل به پيكربندی اين پورت، سوالات زيرمطرح مي شود كه به آنها بصورت پيش فرض پاسخ داده مي شود.

```
Do you want to configure FastEthernet0/0  interface? [yes]:
  Use the 100 Base-TX (RJ-45) connector? [yes]:
  Operate in full-duplex mode? [no]:
  Configure IP on this interface? [yes]:
    IP address for this interface: 10.10.10.1
    Subnet mask for this interface [255.0.0.0] : 255.255.255.0
    Class A network is 10.0.0.0, 24 subnet bits; mask is /24
```

و كاربرIP و Subnetmask اين پورت رامشخص مي نمايد. (درمثال بالا IP:10.10.10.1 وSubnetmask:255.255.255.0 است)FastEthernet 0/1 را نيز مانند بالاتنظيم مي كنيم.

```
Do you want to configure FastEthernet0/1  interface? [yes]:
  Use the 100 Base-TX (RJ-45) connector? [yes]:
  Operate in full-duplex mode? [no]:
  Configure IP on this interface? [yes]:
    IP address for this interface: 20.20.20.1
    Subnet mask for this interface [255.0.0.0] : 255.255.255.0
    Class A network is 20.0.0.0, 24 subnet bits; mask is /24
```

درانتها، جهت ذخيره نمودن تنظيمات انجام شده از كاربرسوال مي شود.

```
[0] Go to the IOS command prompt without saving this config.
[1] Return back to the setup without saving this config.
[2] Save this configuration to nvram and exit.

Enter your selection [2]:
```

اگركاربرعدد صفر را وارد كند، تنظيمات اعمال شده ولي ذخيره نگرديده است. (يعني با خاموش-روشن كردن، پيكربندي انجام شده ازبين مي رود)
اگركاربرعدد يک را واردكند، سيستم عامل مسيرياب بدون هيچگونه تنظيماتي مجددا به مرحله setup
بازمي گردد.
اگر كاربرعدد دو را واردكند، پيكربندي انجام شده، ذخيره مي گردد.

تغييرآيتمهاي پيكربندي مسيرياب به صورت مجزا وبدون استفاده ازSetup

تغييردرنام مسيرياب(Hostname)

براي اعمال اين تغيير، ابتدا با استفاده ازكلمه enable و رمز ورودي به مسيرياب (درصورتي كه ازقبل به مسيرياب كلمه عبورداده باشيم) مفسرفرمان را به حالت ممتازمي بريم. سپس با اجراي فرمان config terminal مفسرفرمان را به وضعيت پيكربندي واردمي نمائيم و مطابق با دستور زيرنام مسيرياب راتغييرمي دهيم.

Hostname نام جديد

در مثال زيرنام مسيرياب را از Router به Test1 تغييرمي دهيم.

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname Test1
Test1(config)#exit
Test1#
```

تنظيم كلمات عبور(Password)

كلمه عبورمحرمانه

براي اينكه هركاربري نتواند پس از اتصال به مسيرياب به مد ممتاز (Privilage mode) واردشود و پيكربندي مسيرياب را تغييردهد اين كلمه عبور را روي مسيرياب تنظيم مي كنيم. با set كردن اين كلمه عبور هنگامي كه كاربركلمه enable را واردمي كند از او يک رمز خواسته مي شود تا وارد مرحله اي شود كه بتواند به اطلاعات پيكربندي مسيرياب دسترسي داشته باشد وآن راتغييردهد. براي تنظيم اين كلمه عبور پس ازورود به مد config ازدستور زيراستفاده مي كنيم.

رمز ورودي enable secret

درمثال زيركلمه عبور456 را روي مسيرياب تنظيم مي كنيم.

```
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#enable secret 456
```

كلمه عبورترمينال مجازي(Virtual Terminal Passord)

كاربرد اين كلمه عبور زماني است كه كاربران بخواهندازراه دورازطريق Telnet كردن به مسيرياب دسترسي داشته باشند. براي تنظيم اين كلمه عبور پس از ورود به مدconfig با استفاده از گزينه line تنظيمات زير را انجام مي دهيم.

```
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#line vty 0 15
Router(config-line)#password 456
Router(config-line)#^Z
Router#
```

تعريف عدد صفرتا پانزده يعني اينكه در يک زمان شانزده user بتوانند با هم به مسيرياب Telnet كنند. درمثال بالا، رمزورودي جهت Telnet ، 456 است.
نكته: جهت حذف password هاي گفته شده در بالا، كلمه no را پيش از عبارت ورود رمز مي آوريم. به عنوان مثال no enable secret 456 رمز ورود به مسيرياب را حذف مي نمايد.

دادنIP به كارتهاي واسط شبكه(پورتها)

جهت IP دادن به FastEthernet هاي مسيرياب پس از ورود به مد config وارد پورت مورد نظرشده و مطابق دستور زيرIP راتخصيص مي دهيم.

Ip address موردنظرip موردنظر mask

به عنوان مثال:

```
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#interface fastethernet 0/0
Router(config-if)#ip address 10.10.10.1 255.255.255.0
Router(config-if)#^Z
Router#
```

تذكر: براي اينكه بتوان از پورتها استفاده نمود حتما بايد آنها را فعال نمود. براي اينكار پس از ورود به پورت مورد نظر از فرمان no shutdown استفاده مي كنيم. به عنوان مثال پورت 1 مسيرياب را فعال مي نمائيم.

```
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#interface fastethernet 0/1
Router(config-if)#no shutdown
Router(config-if)#^Z
Router#
```

دستورWrite

پس از پيكربندي مسيرياب به صورت دستي جهت ذخيره نمودن تغييرات و تنظيمات در مد ممتاز مسيرياب از فرمان write استفاده مي كنيم.

```
test1#write
Building configuration...
[OK]
```

درانتها، جهت مشاهده تنظيمات و پيكربندي انجام گرفته از فرمان show running-config استفاده مي كنيم. به عنوان مثال، پیکربندی یک مسیریاب در زیر آورده شده است.

```
test1#show running-config

Current configuration : 557 bytes
!
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname test1
!
enable secret 5 $1$/lA5$.Lq9ocLVlR8UDwrOBXE3z1
!
ip subnet-zero
!
!
!
!
!
!
interface FastEthernet0/0
 ip address 10.10.10.1 255.255.255.0
 shutdown
 duplex auto
```

```
 speed auto
!
interface FastEthernet0/1
 ip address 20.20.20.1 255.255.255.0
 shutdown
 duplex auto
 speed auto
!
ip classless
ip http server
ip pim bidir-enable
!
!
!
line con 0
line aux 0
line vty 0 4
 password 456
 login
line vty 5 15
 password 456
 login
!

!
end

test1#
```

دستور كار جلسه ششم

آشنايي با مسيرياب هاي Cisco و كار با آنها

دانشجوي گرامي، اين دستور كار را بدقت مطالعه كرده، آزمايش را انجام داده و پس از تكميل، براي مربي خود ارسال نماييد.

نيازمنديها

سخت افزار

- PC جهت پيكربندي مسيرياب با سيستم عامل ويندوز XP و يا لينوكس.
- يكي از مسيريابهاي Cisco با حداقل دو پورت LAN. نمونه:
  - Cisco 2600 series(2611)
  - Cisco 3600(3640)
- كابل كنسول جهت ارتباط با مسيرياب.
- يك كابل Cross و يك كابل مستقيم.

نرم افزار

- سي دي ويندوز XP يا لينوكس جهت نصب نرم افزار ترمينال.(در صورت نياز)
- يكي از نرم افزارهاي شبيه ساز ترمينال ذيل:
  - HyperTerminal در ويندوز.
  - Minicom در لينوكس.
- نرم افزار Visio.

زمان مورد نياز

- حداكثر 5 ساعت

دستور كار

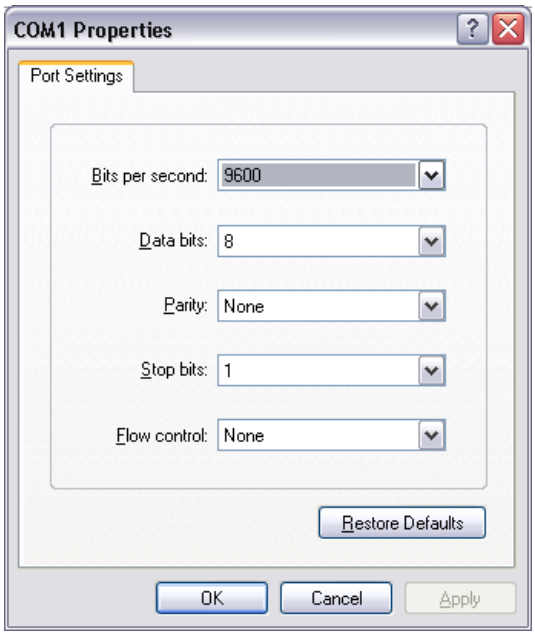
اتصال به مسيرياب از طريق پورت Console

اغلب مسيريابها فاقد هرگونه صفحه نمايش و صفحه كليد مستقل هستند. لذا براي ايجاد هر گونه تغيير در تنظيمات يا پيكربندي، بايد مسيرياب را به يك دستگاه خارجي (مثل يك PC ، كامپيوتر كيفي يا يك ترمينال) متصل كنيد.

در اغلب مسيريابها، يك پورت Rj45 مشاهده مي كنيد. اين پورتها براي اتصال به شبكه و مسيريابي داده ها نيستند، بلكه اين پورت كه يك پورت كنسول نام دارد. براي اتصال يك PC يا ترمينال به مسيرياب و ارتباط مستقيم با آن تدارك ديده شده است . هرگاه شما بخواهيد با يك مسيرياب كه تا كنون پيكربندي نشده است كاركنيد هيچ راهي براي ارتباط با آن مگر از طريق پورت كنسول وجود ندارد .

مراحل ذيل را دنبال نماييد:

1. كابل كنسول را از يك طرف به مسيرياب و از سوي ديگر به پورت سريال PC متصل نماييد.
2. در سيستم عامل ويندوز، نرم افزار Hyper terminal كه در پوشه Accessories > Communications وجود دارد، اجرا نماييد.
3. پورت سريال مورد استفاده مي‌تواند COM1 يا COM2 باشد.
4. پورت را بصورت ذيل پيكربندي كنيد:



توجه نماييد كه سرعت پيش فرض در اغلب مسيريابهاي سيسكو 9600 bps مي باشد، اما اين سرعت مي تواند در تنظيمات مسيرياب تغيير داده شود. لذا در صورتيكه نتوانستيد با مسيرياب ارتباط برقرار نماييد، ساير سرعت ها را نيز امتحان كنيد.

5. با زدن چند بار كليد Enter مي بايست كنسول متني مسيرياب را مشاهده كنيد.

RouterName >

البته در حالات كاري مختلف مسيرياب ممكن است با Promptهاي متفاوتي روبرو شويد. (در صفحات قبلی توضیح داده شده است.)

فرايند بازيابي كلمه عبور (Password Recovery)

اگر براي اولين بار در حال پيكربندي مسيرياب هستيد، بايد كلمه عبور پيش فرض مسيرياب را از مستندات آن بدست آوريد. در صورتيكه نتوانستيد كلمه عبور پيش فرض مسيرياب را پيدا كنيد، و يا اينكه كلمه عبور پيش فرض تغيير داده شده باشد، بايد فرايند Password Recovery را دنبال نماييد. اين فرآيند در مدلهاي مختلف مسيريابها، متفاوت است. براي آشنايي با فرآيند بازيابي كلمه عبور مدل مسيرياب مورد نظر مي توانيد از سايت سيسكو كمك بگيريد. در ذيل، به عنوان نمونه فرايند Password Recovery در مسيريابهاي Cisco سري 2600 آورده شده است. لازم به ذكر است كه براي انجام اين فرايند، بايد دسترسي فيزيكي به مسيرياب داشته باشيد.
مراحل:

1. مسيرياب را از طريق پورت كنسول به يك Terminal و يا يك PC كه داراي يك نرم افزار Terminal Emulator مي‌باشد، متصل نماييد. (طبق روالي كه قبلا گفته شد.)
2. اگر به روتر دسترسي داريد، دستور show register را تايپ نماييد و تنظيمات Configuration Register را در جايي ذخيره كنيد.

نكته: Configuration Register معمولا داراي مقدار 0x2102 و يا 0x102 است. اكر به مسيرياب دسترسي نداريد مي‌توانيد فرض كنيد كه مقدار آن برابر 0x2102 است.

3. از كليد power براي خاموش و روشن كردن مجدد مسيرياب استفاده نماييد.
4. با فشردن كليد Break در ترمينال (براي آگاهي از كليد Break در ترمينال مورد استفاده به مستندات آن مراجعه نماييد) در 60 ثانيه اول فرايند بوت شدن مسيرياب، آن را در حالت ROMMON قرار دهيد.
5. در اعلان rommon 1> ، دستور Confreg 0x2142 را تايپ نماييد تا مسيرياب را از روي حافظه Flash بوت كند. اين مرحله باعث مي شود كه تنظيمات Startup ناديده گرفته شوند.
6. در اعلان rommon 2> ، دستور reset را وارد نماييد. مسيرياب مجددا بوت مي شود ولي تنظيمات ذخيره شده را ناديده مي گيرد. در حقيقت مسيرياب وارد پروسه پيكربندي اوليه مي شود و تنظيمات موجود مانند كلمه عبور را مجددا سوال مي كند.

7. در مراحل مختلف پيكربندي اوليه، No را تايپ كنيد و يا از ctrl+c استفاده نماييد تا مسيرياب از آن مرحله عبور كند.
8. دستور enable را در اعلان < route وارد نماييد.
9. مسيرياب بدون خواستن كلمه عبور وارد حالت كاري Privileged مي شود.(#Router)
10. دستور copy startup-config running-config را اجرا نماييد.
11. show running-config را اجرا نماييد تا كلمه عبورهاي رمز نشده را مشاهده كنيد. البته كلمه عبور enable از اين طريق قابل مشاهده نيست و مي بايست مجددا تنظيم شود.
12. .configure terminal را اجرا نماييد.
13. با استفاده از دستو.ر <enable secret <password كلمه عبور مورد نظر را انتخاب نماييد. مثلا":

hostname(config)#enable secret cisco

14. دستور <config-register <configuration_register_setting را اجرا نماييد. مقدار اين رجيستر هماني است كه در مرحله 2 ديده ايد و يا مقدار 0x2102 است. مثال:

hostname(config)#config-register 0x2102

15. با استفاده از Ctrl+Z و يا end از حالت پيكربندي خارج شويد.
16. يكي از دو دستور ذيل را اجرا نماييد تا تنظيمات جديد ذخيره گردد.

write memory
copy running-config startup-config

آشنايي با IOS و حالات كاري مختلف آن

پيش از انجام اين بخش از گزارش كار، با مطالعه ضمائم با حالتهاي كاري مسيريابهاي Cisco آشنا شويد. جدول ذيل برخي از امكانات اوليه محيط دستور IOS را نشان مي دهد.

Cisco Command	Requirement
Enter privileged mode	Enable
disable	Return to user mode from privileged
Logout or exit or quit	Exit Router

Recall last command	up arrow or <Ctrl-P>
Recall next command	down arrow or <Ctrl-N>
Suspend or abort	<Shift> and <Ctrl> and 6 then x
Refresh screen output	<Ctrl-R>
Complete Command	TAB

پس از ورود اوليه به محيط سيستم عامل IOS در حالت User Mode قرار مي‌گيريد. مراحل ذيل را دنبال نماييد.

1. با استفاده از دستور ذيل ليست دستوراتي را كه در اين حالت كاري قابل اجرا است را ليست كرده و در گزارش كار بياوريد.

```
Router> show ?
```

2. در گزارش خروجي دستورات ذيلا را آورده و بطور خلاصه بيان كنيد كه هريك چه عملي انجام مي دهد:

```
Router> show version
Router> show ip interfaces brief
Router> show ip route
```

3. با استفاده از دستور enable وارد حالت كاري Privileged شويد:

```
Router > enable
```

بعد از اجراي موافقيت آميز دستور فوق Prompt محيط دستور IOS به شكل ذيل تغيير مي‌يابد:

```
Router#
```

4. در گزارش خروجي دستورات ذيلا را آورده و بطور خلاصه بيان كنيد كه هريك چه عملي انجام مي دهد:

```
Router# show running-config
Router# show startup-config
Router# show flash
Router# show log
```

5. حال با استفاده از دستور config terminal وارد محيط پيكربندي سيستم عامل IOS شويد. در اين بخش شما قادر خواهيد بود مسيرياب را پيكربندي نماييد. مثلا" اينترفيس هاي مختلف مسيرياب را فعال يا غيرفعال نماييد و يا پيكربندي TCP/IP آنها را تنظيم نماييد.

```
Router# config terminal
```

پس از اجراي دستور فوق Prompt محيط دستور IOS به شكل ذيل تغيير مي‌يابد:

Router(config)#

6. يكي از اينترفيسهاي مسيرياب را بصورت ذيل پيكربندي نماييد:

```
Router(config)# interface ethernet0/0
Router(config-if)# ip address 192.168.1.10 255.255.255.0
```

7. از محيط پيكربندي خارج شده و پيكربندي TCP/IP انجام شده را برروي اينترفيس مذكور با استفاده از دستور show ليست كرده و در گزارش كار بياوريد.
8. حال مجددا وارد محيط config شده و اينترفيس قبلي را انتخاب نماييد. با استفاده از دستور ذيل اين اينترفيس را غير فعال نماييد:

```
Router(config-if)# shutdown
```

9. از محيط پيكربندي خارج شده و با استفاده از دستور show interface غيرفعال بودن اينترفيس مورد نظر را چك كرده و خروجي اين دستور را در گزارش كار بياوريد.
10. در نهايت وارد محيط config شده و اينترفيس قبلي را انتخاب نماييد. با استفاده از دستور ذيل اين اينترفيس را مجددا فعال نماييد:

```
Router(config-if)# no shutdown
```

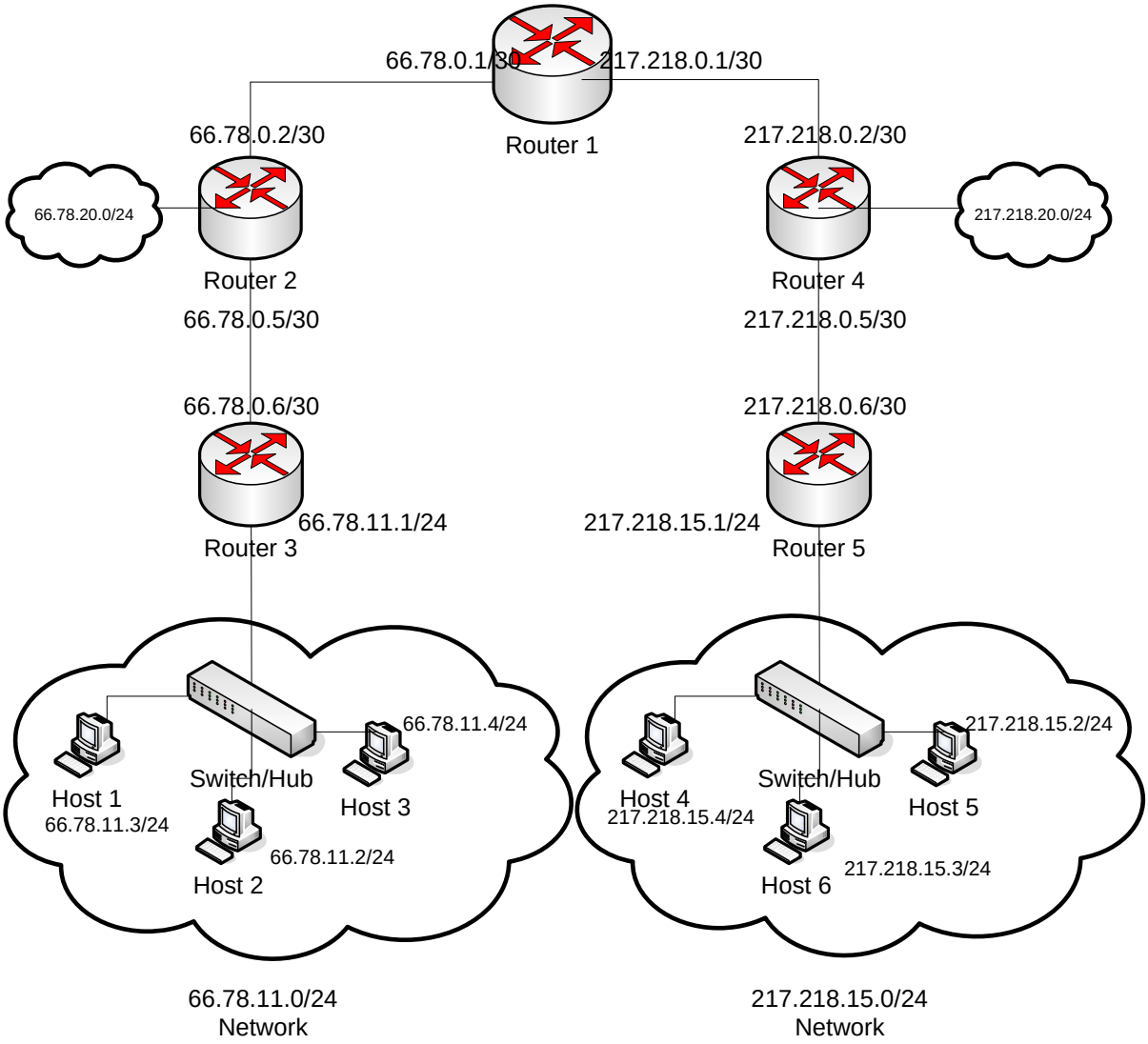
نكته: با استفاده از كلمه no بصورت ذيل مي توانيد اثر يك دستور را كه قبلا اجرا كرده ايد، خنثي نماييد

```
Router(config-if)# no [previous command]
```

تست و راه‌اندازي شبكه نمونه با استفاده از مسيريابهاي Cisco

نقشه شبكه فرضي مورد نظر همانند، آزمايشهاي قبلي است. در اين آزمايش در صورتيكه مسيريابهاي Cisco كافي نبوند از مسيريابهاي با سيستم عامل لينوكس استفاده نماييد. شكل ذيل نقشه شبكه فرضي را نشان مي دهد:

Sample Network Topology



مراحل ذيل را دنبال نماييد:

1. اتصال فيزيكي سيستمها و مسيريابها را برقرار نماييد.
2. پيكربندي TCP/IP هر يك از كارتهاي شبكه مربوط به گروه خود را انجام دهيد.
3. تست اتصال مستقيم لينكها: با استفاده از دستور ping ارتباط كارتهاي شبكه گروه خود را با كارتهاي شبكه سيستم مجاور كه با آن بطور مستقيم در ارتباط هستيد، كنترل نماييد.

4 سرويس مسيريابي در مسيريابهاي سيسكو غالبا" فعال است. اما براي اطمينان از اين موضوع در حالت كاري Config دستور ذيل را اجرا نماييد:

Router(config)# ip routing

5 مسيرياب خود را بدين صورت پيكربندي نماييد:

- در مسيريابهاي 2،3،4،5 آدرس Default Gateway را معادل آدرس IP مسيرياب بالاي آن قرار دهيد.
- در مسيرياب 2 يك Route Entry براي شبكه 66.78.11.0/24 اضافه نماييد.
- در مسيرياب 4 يك Route Entry براي شبكه 217.218.15.0/24 اضافه نماييد.
- در مسيرياب 1 يك Route Entry براي شبكه 217.218.0.0/16(با گام بعدي روتر 4) و يك Route Entry براي شبكه 66.78.0.0/16(با گام بعدي روتر 2) اضافه نماييد.

نكته: براي پيكربندي جدول مسيريابي در مسيريابهاي سيسكو، در حالت كاري Config، از دستور ip route استفاده نماييد.

6 Default Gateway ميزبانها را معادل آدرس IP مسيرياب بالايي قرار دهيد. (روتر 5 يا روتر 3)

7 حال كليه گره‌هاي شبكه(مسيريابها و ميزبانها) مي بايست با همديگر ارتباط برقرار نمايند. اين مساله را مي توانيد با دستور ping بررسي نماييد. موارد ذيل در گزارش آورده شود:

- پيكربندي TCP/IP كليه كارتهاي شبكه مربوط به گروه خود
- جدول مسيريابي سيستم.(show ip route)
- خروجي دستور ping براي ارتباط با تك تك گرههاي موجود در شبكه. (حداقل 6 مورد)
- خروجي دستور traceroute براي ارتباط با تك تك گرههاي موجود در شبكه(حداقل 6 مورد)

نكته: فايروال موجود در سيستمهاي ويندوز XP ممكن است جلوي بسته هاي ورودي از ساير LAN ها را بگيرد. لذا در حين آزمايش فايروال را پيكربندي كرده و يا غيرفعال نماييد.

مطالب تكميلي

IOS (Internetwork Operating System) نرم افزاري است كه از آن به منظور كنترل روتينگ و سوئيچينگ دستگاه هاي بين شبكه اي استفاده مي گردد. آشنائي با IOS براي تمامي مديران شبكه و به منظور مديريت و پيكربندي دستگاه هائي نظير روتر و يا سوئيچ الزامي است.
در اين مطلب پس از معرفي اوليه IOS به بررسي برخي از ويژگي هاي آن خواهيم پرداخت.

IOS و ضرورت استفاده از آن

يك روتر و يا سوئيچ بدون وجود يك سيستم عامل قادر به انجام وظايف خود نمي باشند. (همانند يك كامپيوتر) شركت سيسكو، سيستم عامل Cisco IOS را براي طيف گسترده اي از محصولات شبكه اي خود طراحي و پياده سازي نموده است. نرم افزار فوق، جزء لاينفك در معماري نرم افزار روترهاي سيسكو مي باشد و همچنين به عنوان سيستم عامل در سوئيچ هاي Catalyst ايفاي وظيفه مي نمايد. بدون وجود يك سيستم عامل، سخت افزار قادر به انجام هيچگونه عملياتي نخواهد بود. (عدم تامين شرايط لازم براي بالفعل شدن پتانسيل هاي سخت افزاري)
IOS ، سرويس هاي شبكه اي زير را ارائه مي نمايد :

- عمليات روتينگ و سوئيچينگ
- دستيابي ايمن و مطمئن به منابع شبكه
- قابليت توسعه و تغيير پيكربندي شبكه

ماهيت اينترفيس IOS

نرم افزار IOS از يك اينترفيس خط دستوري و يا CLI (command-line interface) استفاده مي نمايد. IOS يك تكنولوژي كليدي است كه از آن در اكثر خطوط توليد محصولات شركت سيسكو استفاده مي گردد. عملكرد IOS با توجه به نوع دستگاه هاي بين شبكه اي متفاوت مي باشد. براي دستيابي به محيط IOS از روش هاي متعددي استفاده مي گردد.

session console

در اين روش با استفاده از يك اتصال سريال با سرعت پائين، كامپيوتر و يا دستگاه ترمينال را مستقيما" به پورت كنسول روتر متصل مي نمايند. (سرويس شبكه اي خاصي بر روي روتر پيكربندي نشده است)

ارتباط Dialup

در اين روش با استفاده از مودم و از طريق پورت كمكي (AUX) با روتر ارتباط برقرار مي گردد. (سرويس شبكه اي خاصي بر روي روتر پيكربندي نشده است)

استفاده از telnet

در اين روش مي بايست حداقل يكي از اينترفيسها با يك آدرسIP پيكربندي گردد و terminal sessions virtual براي login و رمز عبور پيكربندي شده باشد.
براي دستيابي به بخش رابط كاربر روتر و يا سوئيچ از يك برنامه ترمينال استفاده مي گردد. HyperTerminal متداولترين گزينه در اين رابطه مي باشد. اينترفيس خط دستور و يا CLI روترهاي سيسكو از يك ساختار سلسله مراتبي تبعيت مي نمايد. ساختار فوق كاربران را ملزم مي نمايد كه براي انجام هر نوع عمليات خاص به يك مد بخصوص وارد شوند.
مثلا" براي پيكربندي يك اينترفيس روتر، كاربر مي بايست به مد پيكربندي اينترفيس و يا configuration mode interface وارد شود. هر mode پيكربندي داراي يك prompt مختص به خود مي باشد كه از طريق آن مي توان دستورات مربوطه را تايپ و از توان عملياتي آنان استفاده نمود. IOS يك سرويس مفسر دستور با نام EXEC را ارائه مي نمايد. پس از درج هر دستور، EXEC صحت آن را بررسي و پس از تائيد آن را اجراء مي نمايد. نرم افزار IOS در جهت افزايش امنيت، دو سطح متفاوت دستيابي user EXEC mode و privileged EXEC mode با ويژگي زير را براي سرويس مفسر دستور (EXEC) در نظر مي گيرد.

user EXEC mode

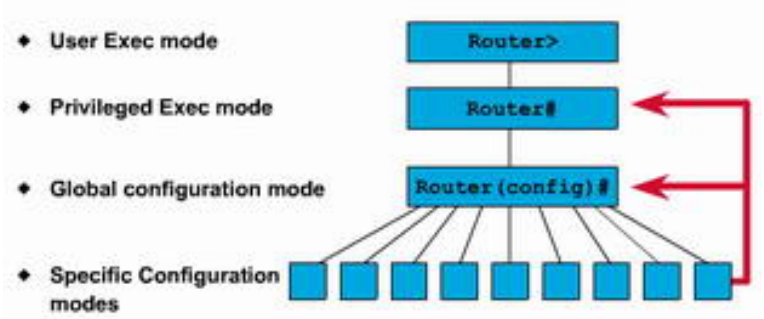
در اين مد، صرفا" مي توان تعداد محدودي از دستورات مانيتورينگ را اجرا نمود. به اين مد view only نيز گفته شده و نمي توان دستوراتي را كه باعث تغيير در پيكربندي روتر مي گردند، اجراء نمود.

privileged EXEC mode

در اين مد مي توان به تمامي دستورات روتر دستيابي داشت. براي استفاده از اين مد و در جهت افزايش امنيت، مي توان روتر را بگونه اي پيكربندي نمود كه كاربران را ملزم به درج نام و رمز عبور جهت دستيابي به روتر نمايد. Global configuration mode و ساير حالات متفاوت پيكربندي صرفا" از طريق privileged EXEC mode قابل دستيابي مي باشند.

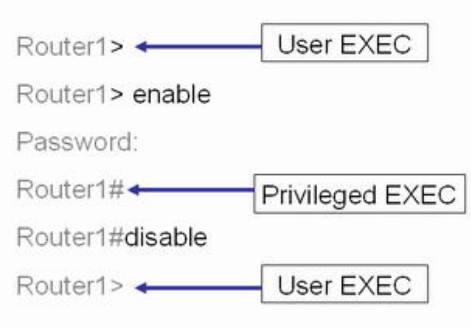
EXEC Mode	Prompt	كاربرد
User	Router1>	بررسي وضعيت روتر
privileged	Router1#	دستيابي به حالات متفاوت پيكربندي روتر

شكل زير حالات متفاوت پيكربندي روتر را نشان مي دهد.



Configuration Mode	Prompt
Interface	Router(config-if)#
Subinterface	Router(config-subif)#
Controller	Router(config-controller)#
Map-list	Router(config-map-list)#
Map-class	Router(config-map-class)#
Line	Router(config-line)#
Router	Router(config-router)#
IPX-router	Router(config-ipx-router)#
Route-map	Router(config-route-map)#

همانگونه كه در شكل فوق مشاهده مي گردد، جهت فلش قرمز رنگ به سمت Global Configuration Mode و Privileged mode است. اين بدان معني است كه جهت ورود به برخي حالات خاص پيكربندي مي توان از طريق Global Configuration Mode اقدام نمود و در برخي موارد ديگر اين كار از طريق Privileged mode انجام مي گردد.
به منظور دستيابي به privileged EXEC mode از طريق user EXEC mode از دستور enable استفاده مي گردد. در صورتي كه روتر بگونه اي پيكربندي شده است كه جهت ورود به privileged EXEC mode كاربران را ملزم به درج نام و رمز عبور مي نمايد، مي بايست در اين مرحله رمز عبور را نيز وارد نمود. پس از درج صحيح رمز عبور، به EXEC mode privileged وارد شده و با درج يك علامت سوال مي توان دستورات و گزينه هاي متعدد موجود در اين مد را مشاهده نمود. شكل زير نحوه حركت بين user EXEC mode و privileged EXEC mode را نشان مي دهد.

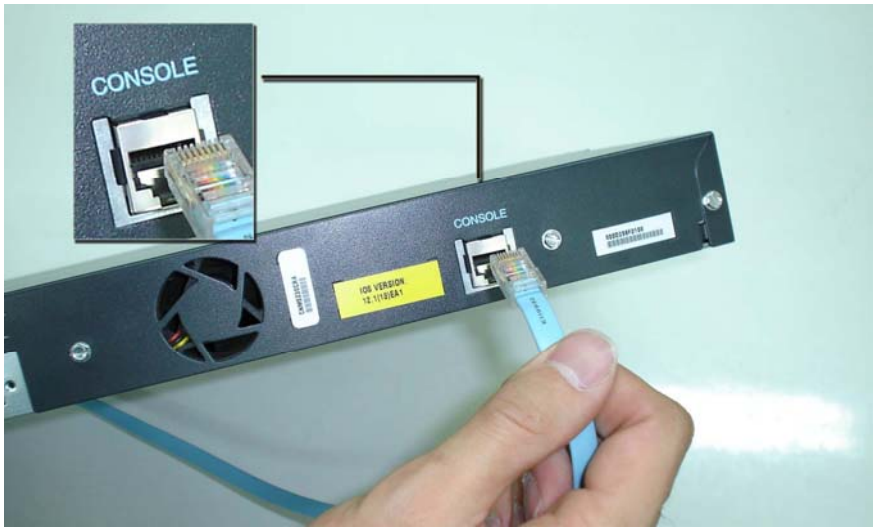


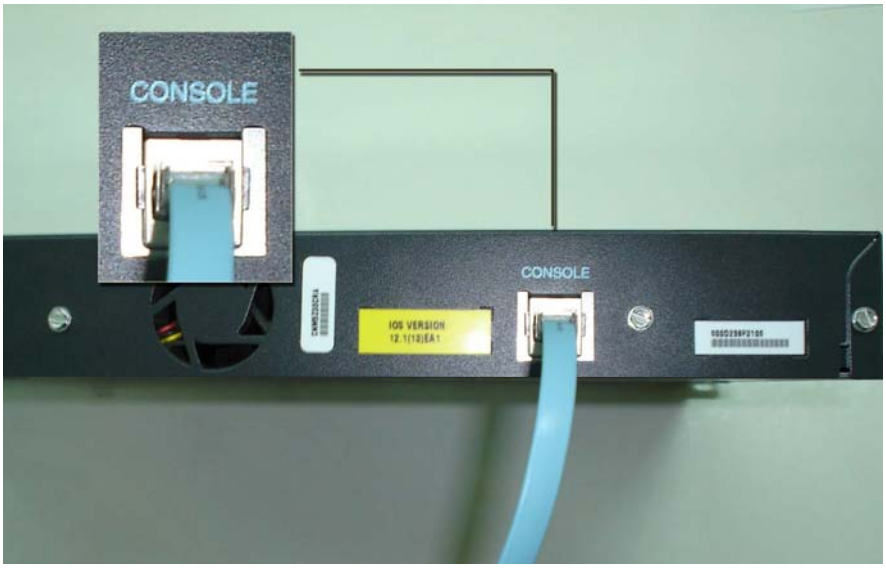
مطالب تکمیلی

مستندات مربوط به پیکربندی پایه cisco switch 2950

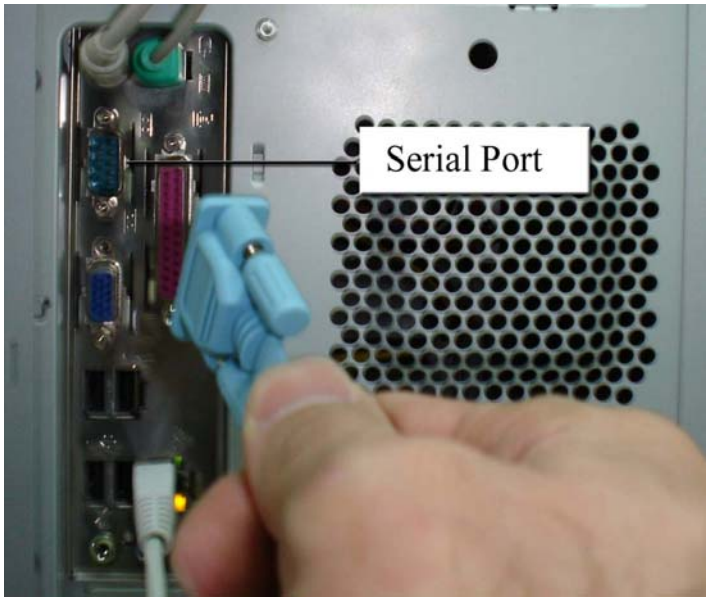
جهت برنامه ريزي يک سوئيچ نياز به يک عدد کابل مخصوص به نام console مي باشد. يک سر اين کابل کانکتور rj-45 و سر ديگر آن پورت سريال مي باشد . (مطابق شکل زير)

جهت اتصال سوئيچ به کامپيوتر قسمت rj-45 کابل را به پورت کنسول سوئيچ مانند شکل زير وصل مي کنيم.

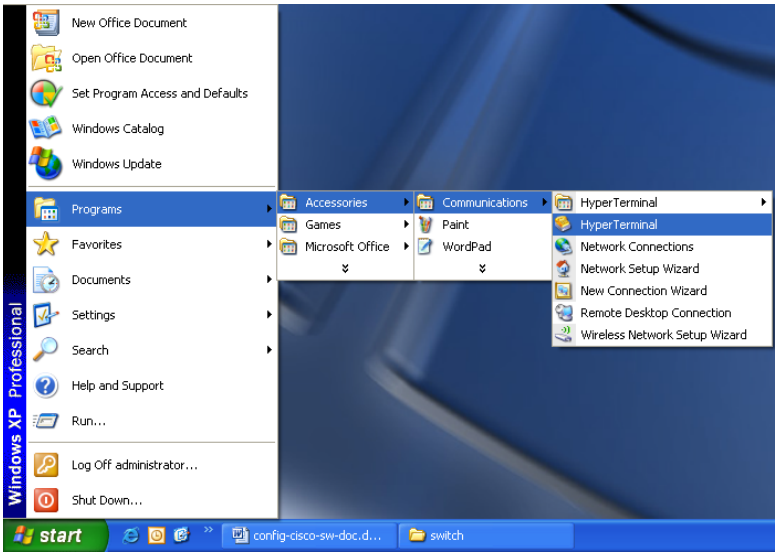




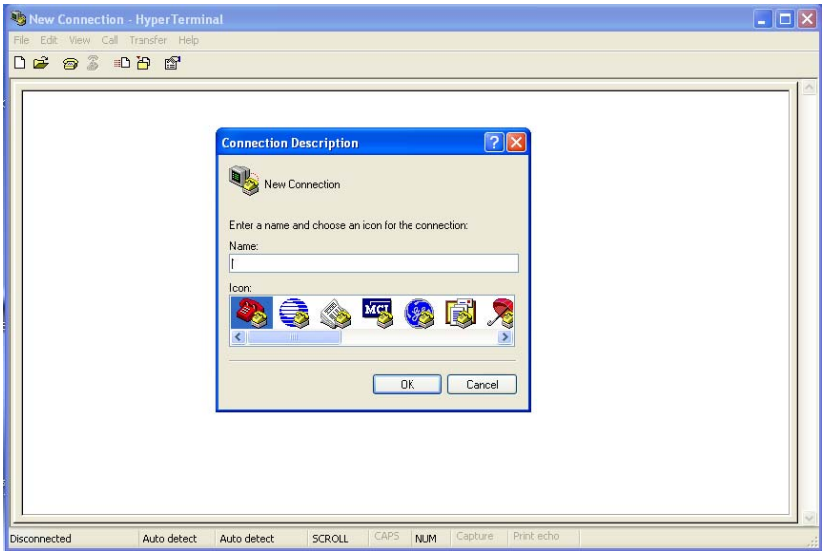
حال قسمت ديگر كابل (پورت سريال) را به يكي از پورتهاي سريال كامپيوتر مانند اشكال زير اتصال مي دهيم :



پس از برقراري اتصالات فوق و روشن نمودن سوئيچ بعد از چند دقيقه جهت وصل شدن به سوئيچ طبق مسير زير گزينه hyperterminal را انتخاب كرده و ادامه مي دهيم.

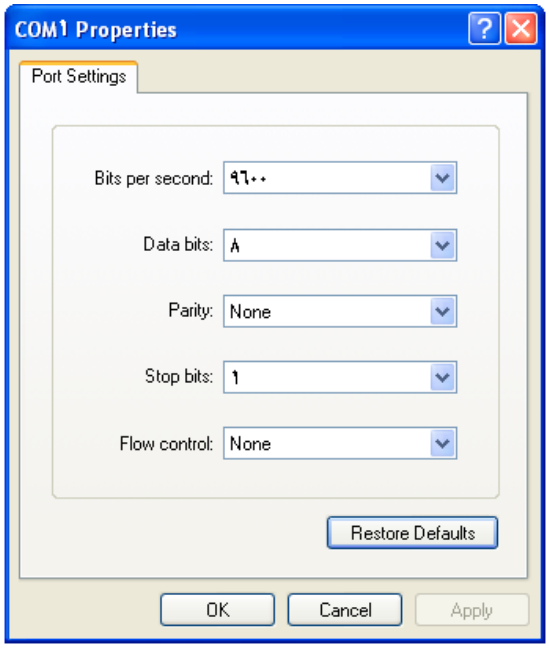


پس از باز شدن پنجره زير در قسمت name يک اسم به دلخواه وارد مي کنيم و سپس کليد ok را ميزنيم:

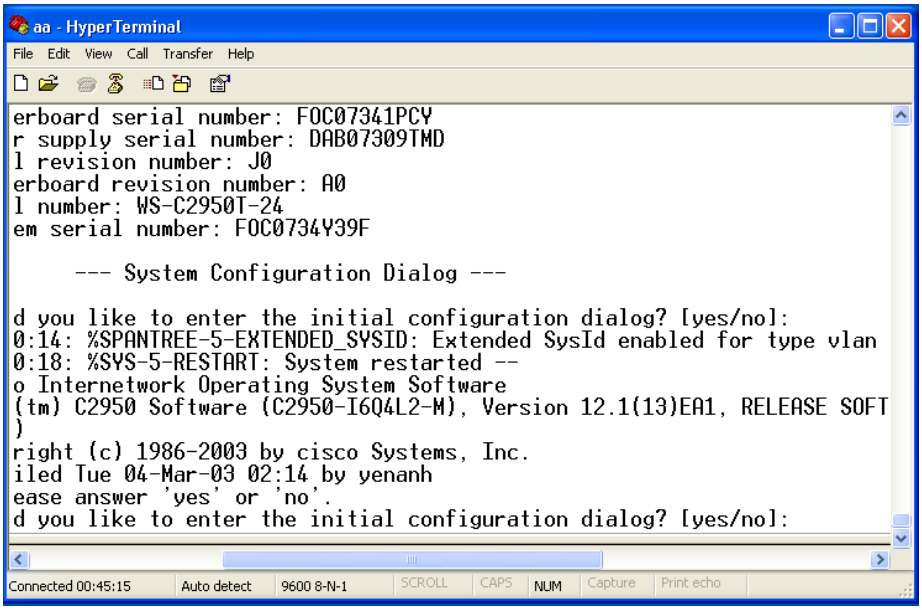


در قسمت connect using پورت سريالي را که به سوئيچ وصل شده انتخاب کرده و ok مي کنيم.

سپس در پنجره زير گزينه restore defaults را انتخاب كرده تا مقادير زير نشان داده شوند سپس ok مي كنيم.



پس از اين مرحله پنجره زير باز شده و بعد از boot شدن سوئيچ سئوال زير پرسيده مي شود كه به منظور پيكربندی بايد no را تايپ كرده و كليد enter را فشار دهيم.



در اين مرحله، حالت زير نمايان مي شود كه در حالت switch> فقط مي توان پيكربندی انجام شده را نمايش داد و دستورات مختصري دارد.

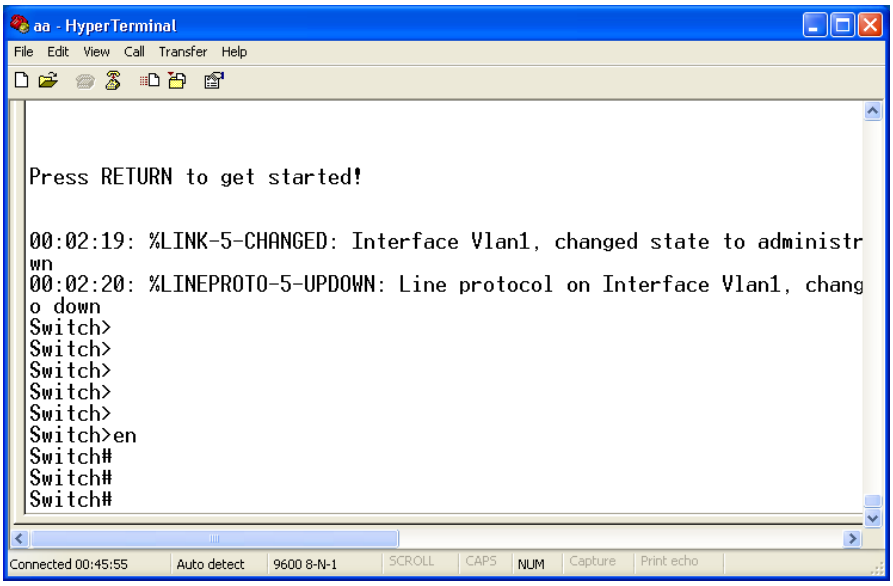
حالت switch # كه اصطلاحا enable mode گفته مي شود و توانائيهاي بيشتري نسبت به حالت قبل دارد و در نهايت جهت پيكربندی به مد switch (config)# وارد مي شويم و مي توانيم دستورات مورد نياز را به سوئيچ بدهيم. بنابراين به طور كلي سه حالت خواهيم داشت :

1- general mode : switch>

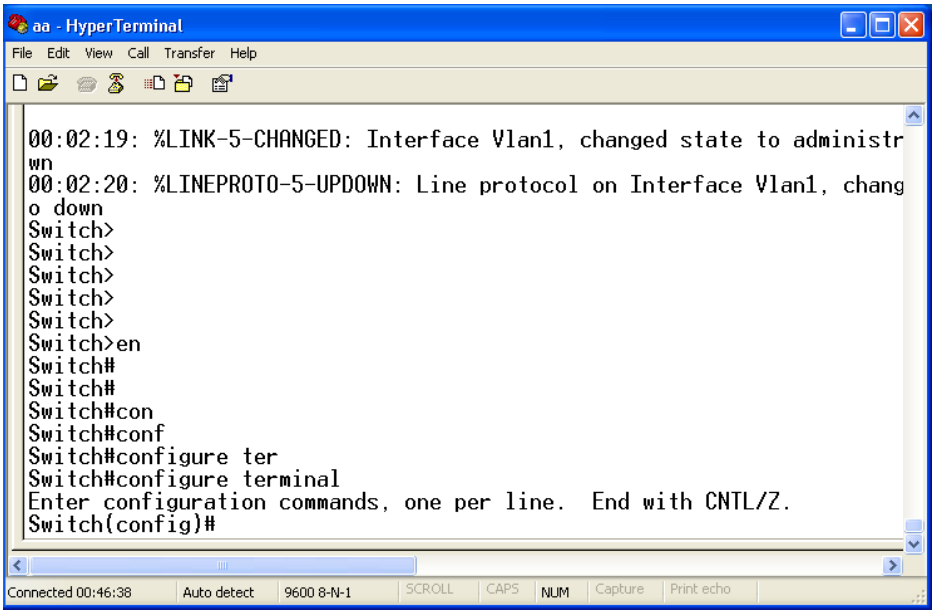
2- enable mode : switch#

3- global config mode : switch (config)#

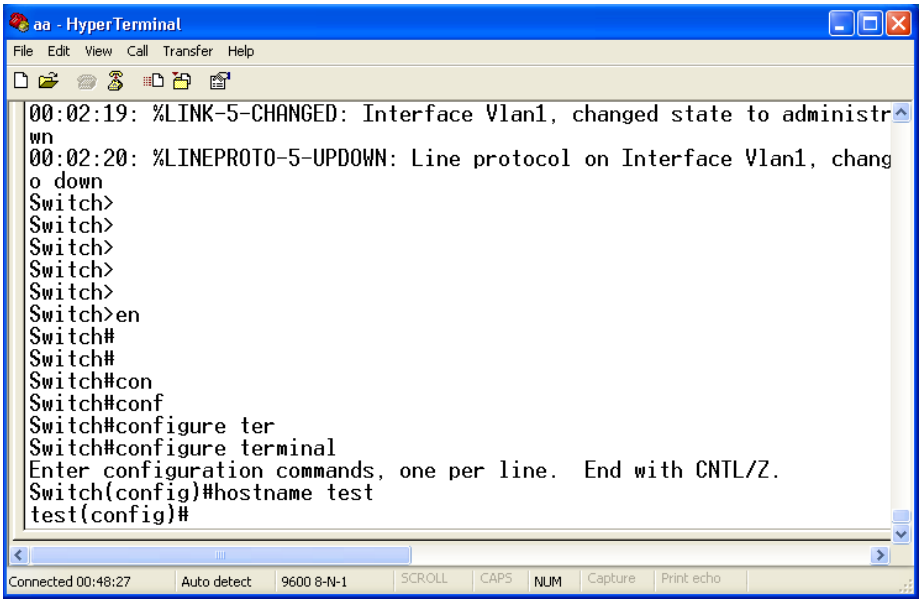
كه با دستور enable مي توان از حالت 1 به حالت 2 رفت. لازم بذكر است كه دستورات را تا جايي كه ديگر دستور مشابهي وجود نداشته باشد، مي پذيرد. بنابراين مي توان با تايپ en همان دستور را اجرا كرد. ضمنا بعد از تايپ بخشي از يک دستور با زدن كليد tab مابقي دستور حک مي شود.



سپس با تايپ دستور configure terminal يا (conf t) وارد config mode سوئيچ مي شويم.

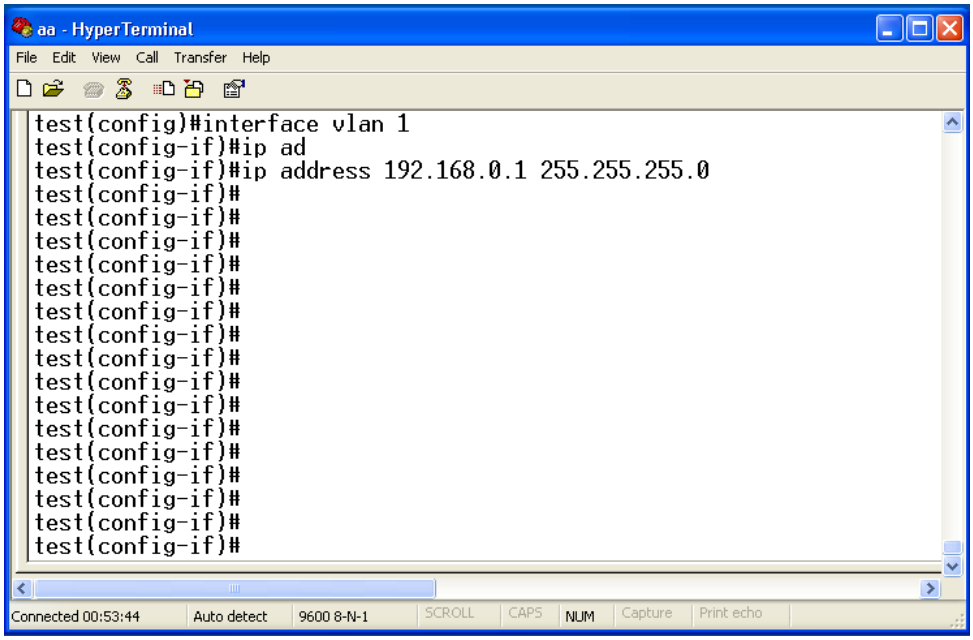


جهت نام گذاري سوئيچ طبق حالت زير عمل مي كنيم :

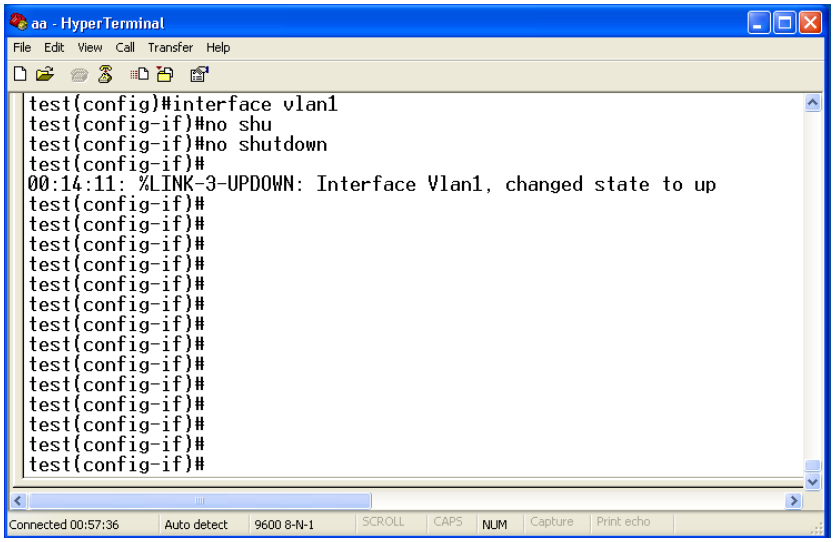


به منظور IP دادن به سوئیچ به صورت زیر عمل مي كنيم :

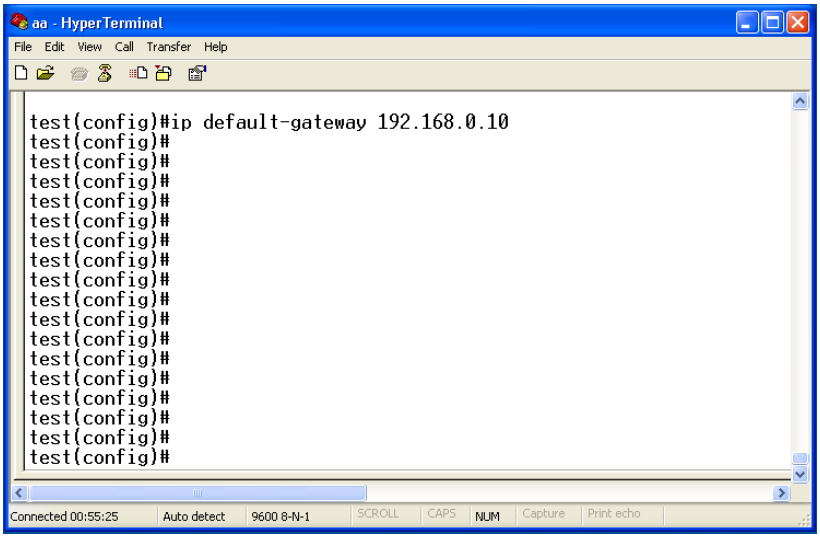
به دليل اينكه مي خواهيم يک ip به كل سوئيچ اختصاص دهيم. بنابراين كل سوئيچ را به عنوان يک vlan (virtual lan) در نظر گرفته و دستور interface vlan 1 را تايپ مي كنيم. ip را به همراه subnet mask آن مانند مثال زير تايپ مي كنيم.



به منظور اطمینان از up بودن vlan حتما باید دستور زیر اجرا شود.



در صورتي كه بخواهيم از شبكه ديگري به سوئيچ وصل شويم بايد gateway مربوطه طبق روش زير تنظيم شود:



به منظور خارج شدن از مرحله قبل با كليد ctrl + z خارج شده و مجددا به حالت config رفته و مراحل بعد را انجام مي دهيم.

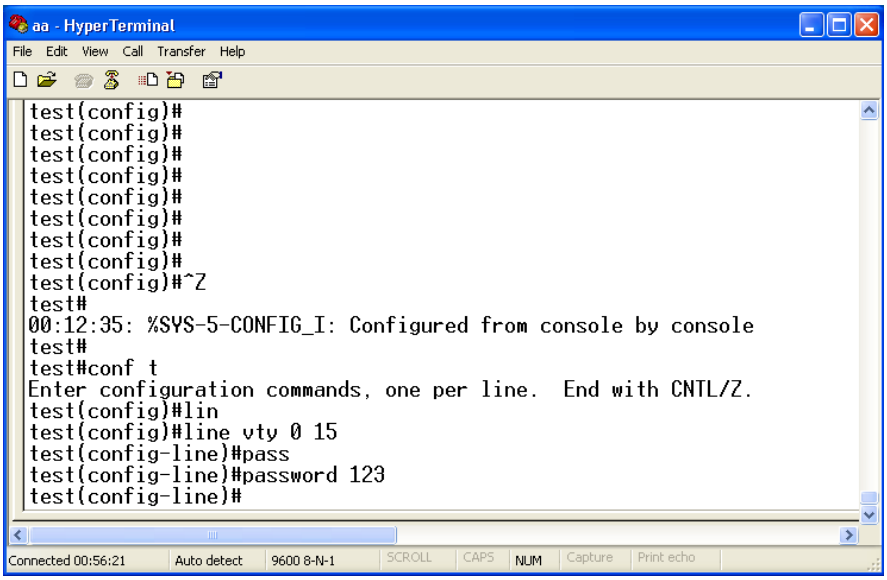
براي اينكه بتوانيم از راه دور و يا به عبارتي از داخل شبكه به سوئيچ وصل شويم (telnet ip) و ديگر نيازي نباشد، براي هربار وصل شدن از طريق پورت كنسول اقدام كنيم. به همين منظور از دستورات به شكل زير استفاده مي كنيم.

به طور كلي دو نوع ترمينال داريم :

1- tty : true terminal ترمينال واقعي

2- vty : virtual terminal ترمينال مجازي

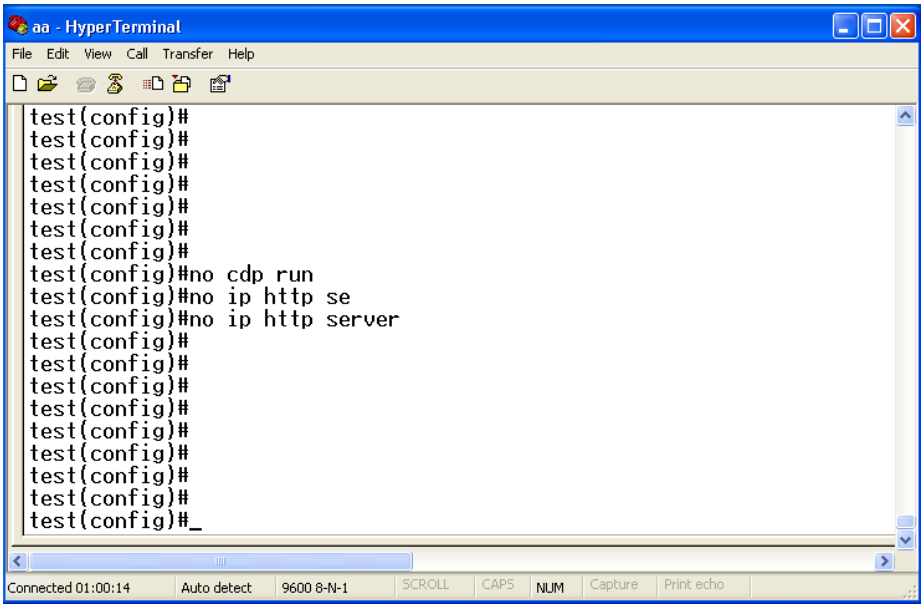
كه براي telnet از ترمينال مجازي استفاده مي كنيم و حتما بايد password روي آن set شود.



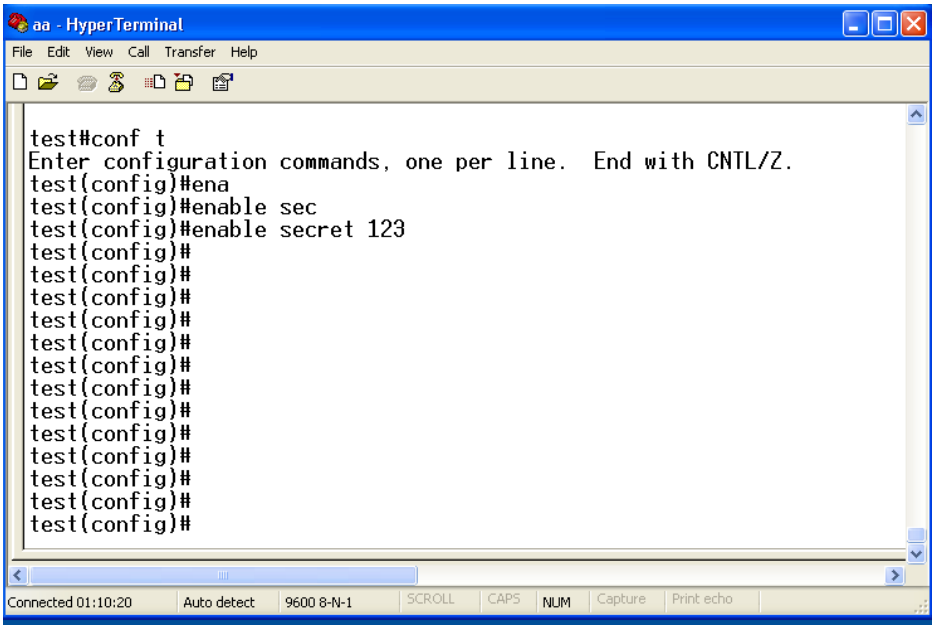
CDP (cisco discovery protocol)

پروتكلي است كه توسط آن تجهيزات cisco يكديگر را شناسائي مي كنند و به منظور جلوگيري از ترافيک هاي اضافي آن را disable مي كنيم.

پروتکل http را نیز به دلایل امنیتي که به راحتـي نتـوان بـه سـوئیچ از طریـق مرورگر وب وصل شد، غیر فعال مي کنـیم. (البتـه لازم بـذکر اسـت در شـبکه هاي کوچک و اینترانت بهتر اسـت ایـن دسـتور اسـتفاده نشـود تـا راحـت تـر بتوان گراف شبکه را بدست آورد.)



براي اینکه هنگام ورود به حالت enable از ما کلمه عبـور پرسـیده شـود، بایـد به روش زیر عمل کنیم:

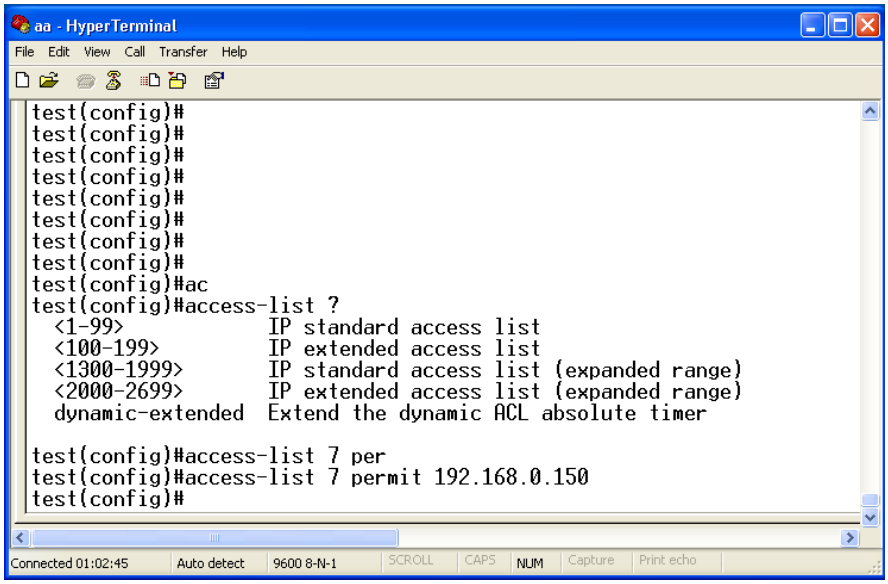


جهت اعمال يک سري قوانين بر روي قسمتهاي مختلف سوئيچ از access list استفاده مي کنيم که به طور کلي دو نوع extended و standard مي باشد که نوع extended قابليت هاي بيشتري دارد.

نوع دستور بدين شکل مي باشد:

Access-list (1-99) permit .....ip .....

در صورتي که بخواهيم به يک ip مجوز بدهيم از کلمه permit و درصوتي که بخواهيم محدود کنيم از کلمه deny استفاده مي کنيم .لازم بذکر است در صورتي که 10 عدد ip را بخواهيم permit کنيم بايد با دستور deny any مابقي را محدود کنيم . ضمنا عددهاي مورد نظر فقط نمايانگر نوع access-list هستند.

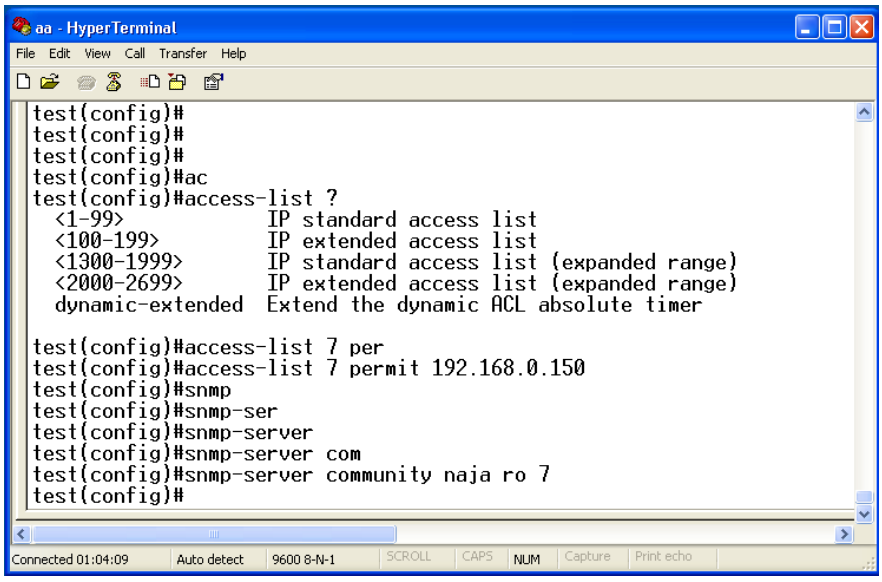


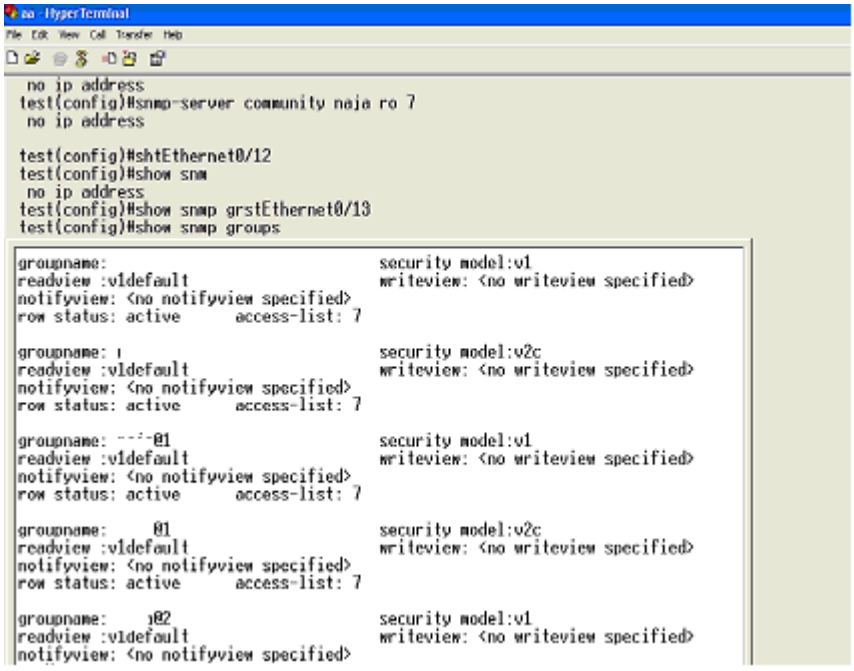
Snmp (simple network management protocol)

يک پروتکل جهت مديريت تجهيزات cisco مي باشد که در صورت فعال شدن با نرم افزارهايي مانند solarwinds و غيره مي توان سوئيچ را مديريت کرد.

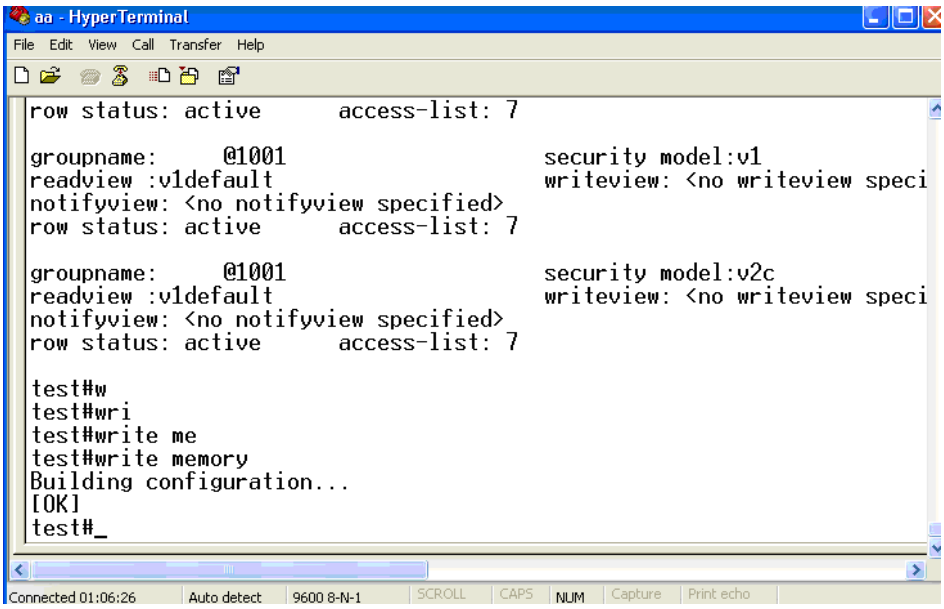
به طور کلي دو نوع مي توانيم تعريف کنيم : 1- ro (read only) 2- rw (read & write)

براي اينکه بتوانيم اين ابزار مديريتي را امن کنيم، مي توانيم يک access-list را بر روي آن اعمال کنيم که براي اين منظور نياز به يک نام داريم که در اينجا amir در نظر گرفته شده ولي بهتر است از کلمات نامتعارف جهت اين نام استفاده شود.





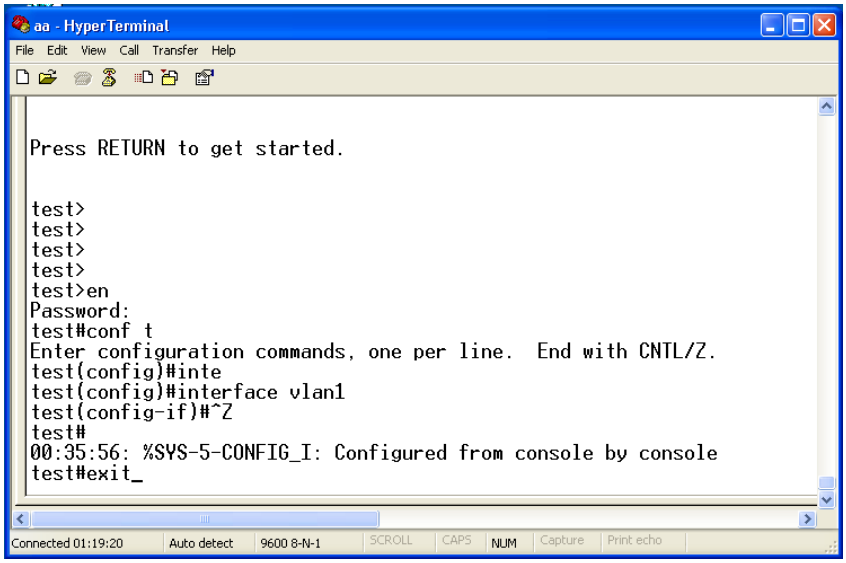
جهت ذخیره شدن پیکربندی انجام شده، به شکل زیر عمل مي کنیم :



برا ي نمايش تغييرات انجام شده به شكل زير عمل مي كنيم :

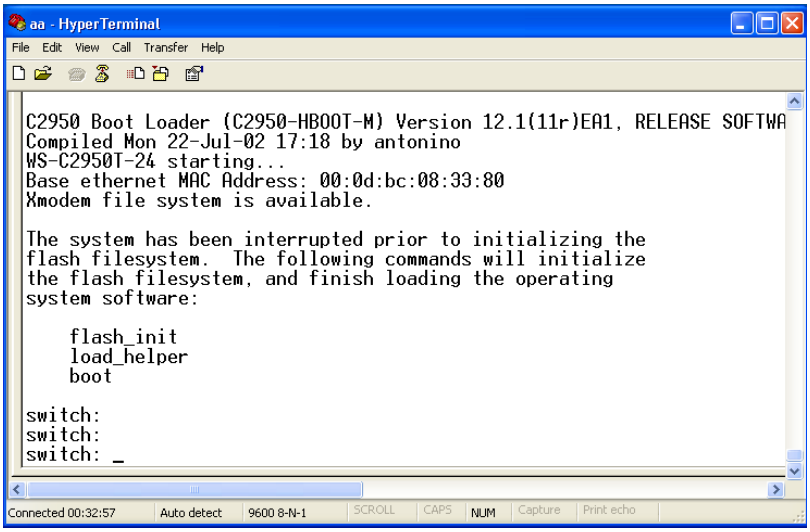
Show running config test&#

كه با اين دستور كليه پيكربندی سوئيچ نمايش داده مي شود. براي خارج شدن از هر مرحله با دستور exit و يا كليدهاي ctrl+z استفاده مي كنيم.

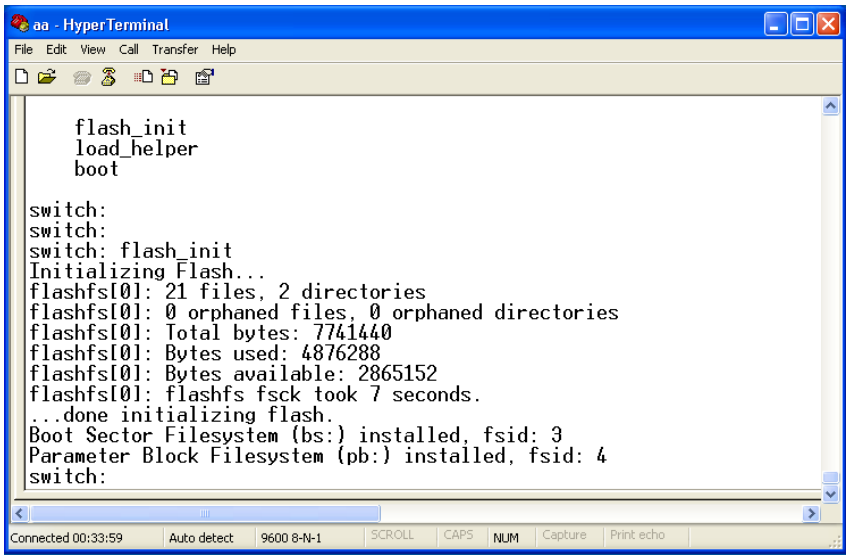


نحوه عوض كردن پيكربندی سوئيچ و يا password recovery

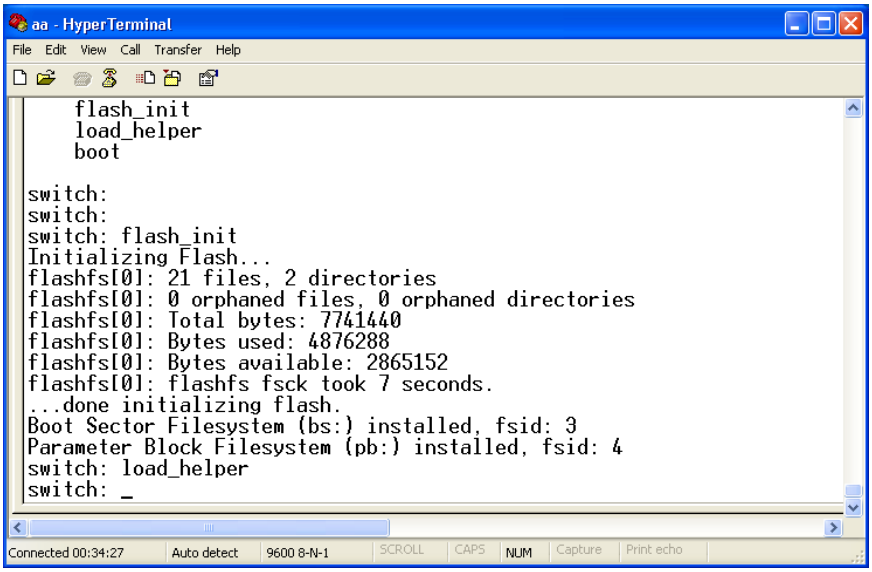
براي اين منظور، ابتدا در زمانboot شدن سوئيچ، كليدي را كه در چپ panel جلويي قرار گرفته را نگه مي داريم تا سوئيچ به مرحلـه rommon وارد شـود. در اين حالت هنوز هيچگونه پيكربندی اجرا نشده است.



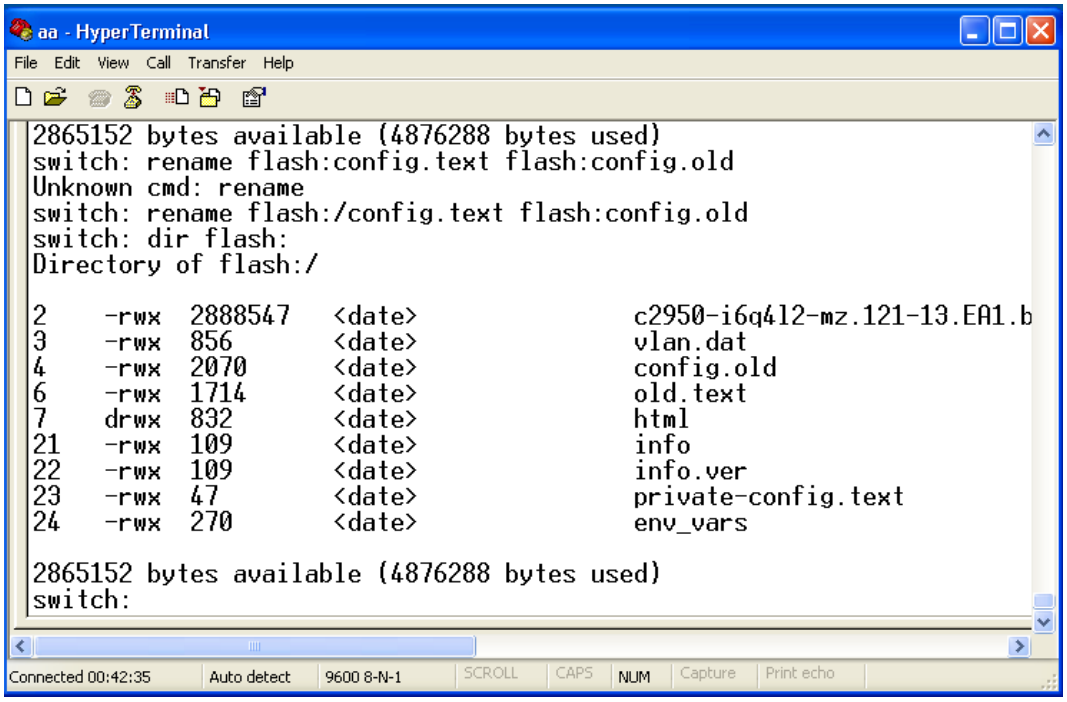
ابتدا فايل flash_init را اجرا مي كنيم. (مانند شكل زير) :



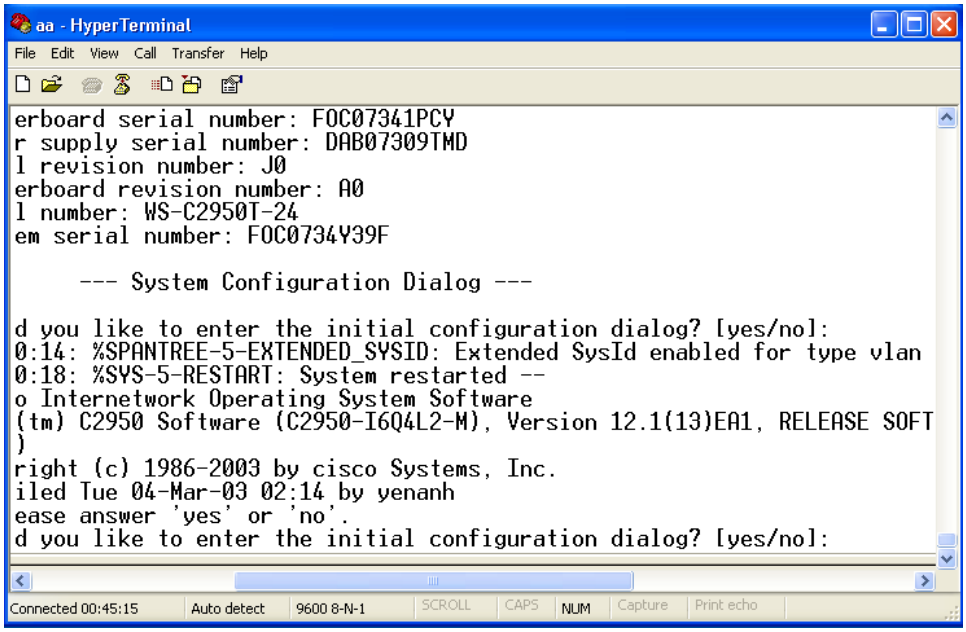
سپس فايل load_helper را اجرا مي كنيم :



سپس با دستور زیر فایل config را rename مي كنيم.



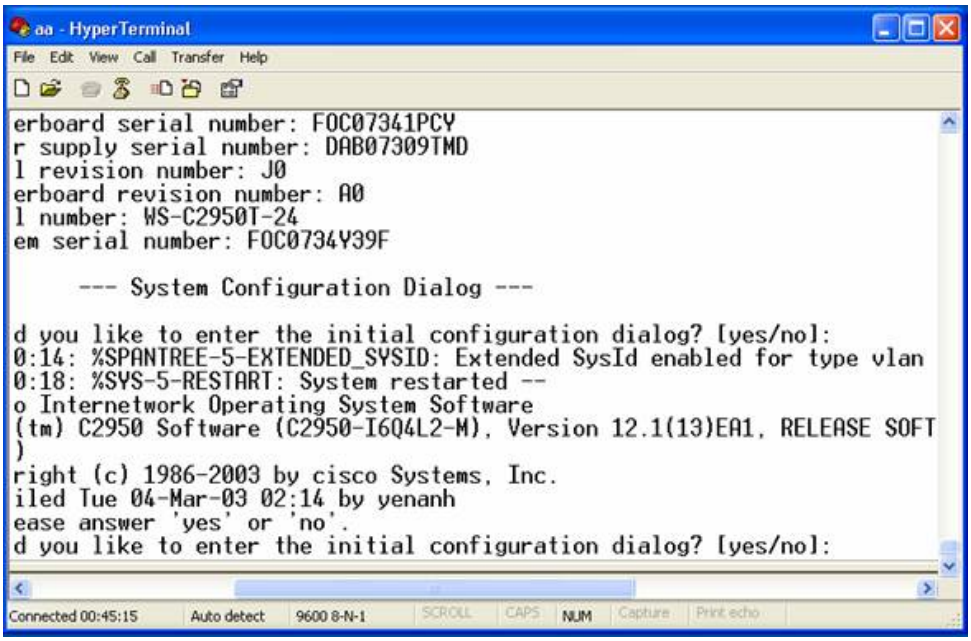
در نهايت سوئيچ را خاموش و روشن مي كنيم تا به حالت زير برسد كه اين همان حالت خام سوئيچ بوده و مي توان از ابتدا شروع به پيكربندی نمود.



در مرحله بعد، به پیکربندی سوئیچ دیگری از محصولات سیسکو رفته به پیکربندی آن می پردازیم.

پیکربندی سوئیچ Cisco 3750

پس از طی مراحل اولیه و اتصال به سوئیچ از طریق hyperterminal، پنجره زیر باز شده و بعد از boot شدن سوئیچ، سئوال زیر پرسیده می شود (درصورتیکه prompt سوئیچ ظاهرنشده باشد چند بارenter رابزنید) که به منظور پیکربندی باید no را تایپ کرده و کلید enter را فشار دهید.



در این مرحله، prompt سوئیچ بصورت<switch نمایان مي شود که دراین مد کاري فقط مي توان پیکربندی انجام شده را مشاهده کرد.
دستورات مختصري در دسترس قرار دارد. (general mode) براي اینکه بتوانیم سوئیچ را پیکربندی کنیم باید وارد مد ممتاز شویم. نحوه ورود بدین شکل است که در جلوي promp سوئیچ enable را تایپ مي کنیم و پس ازآن دکمه enter رامي زنیم. (enable mode)
در این حالت، شما اجازه هر نوع تغییري را درسوئیچ دارید. براي پیکربندی پورتها و تعریف Route باید واردمد config interface که به شکل زیر خواهد بود، شوید.

switch#config terminal <press enter>
switch(config)#interface gigabitethernet 1/0/1 <press enter>
switch(config-if)#

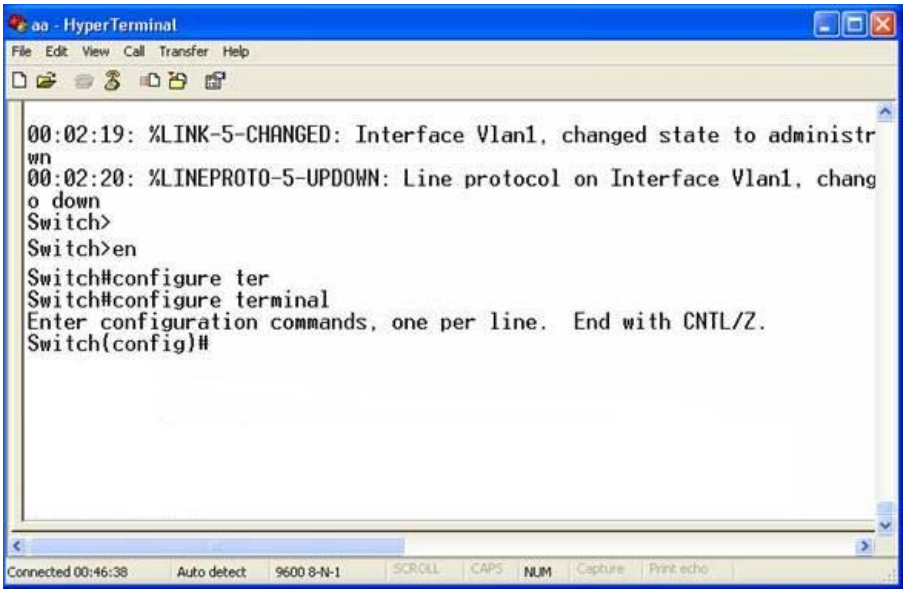
لازم بذکر است که سوئیچ، خلاصه دستورات را تا جایي که دستور، مشابه دستور دیگري نشود را مي پذیرد. ضمنا وقتي قسمتي از دستور را تایپ کردیم، با زدن کلیدTab ادامه دستور را سوئیچ کامل خواهد کرد.

switch#en <press tab>

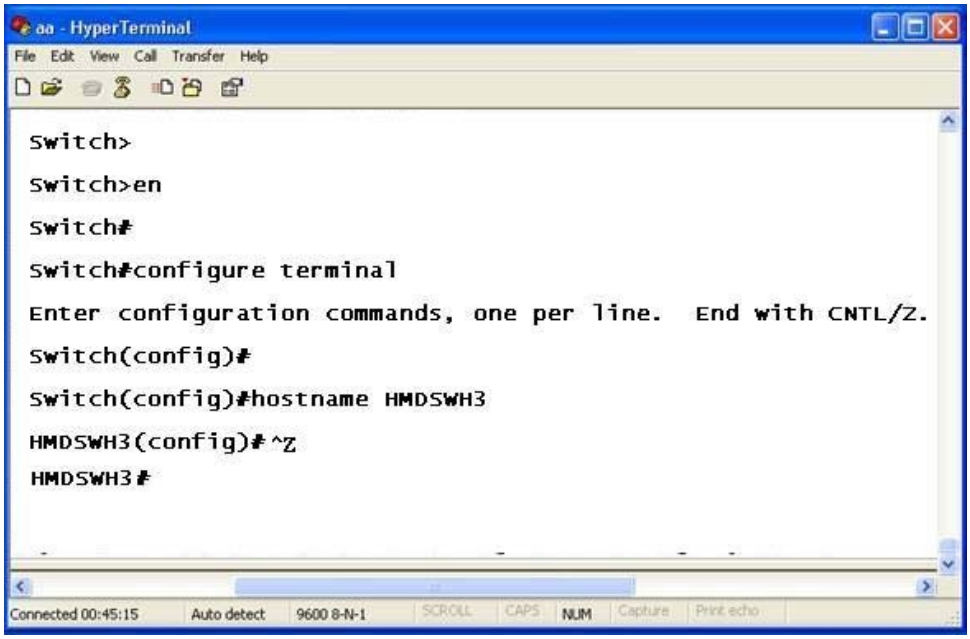
switch#enable

نامگذاري سوئيچ

با تايپ دستور configure terminal وارد config mode سوئيچ مي شويم.



جهت نام گذاري سوئيچ طبق حالت زير عمل مي كنيم.

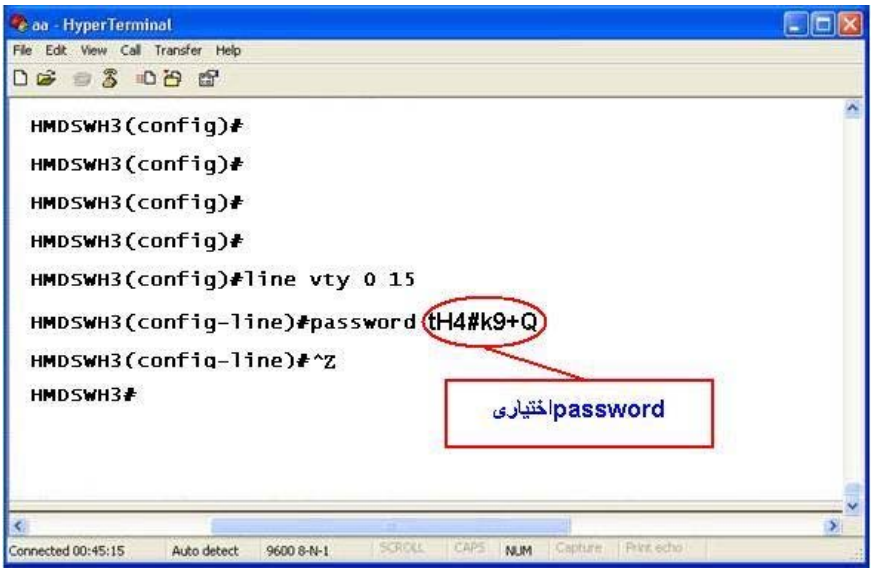


تغییرEnable Paswword

براي اينكه بخواهيد وارد حالت enable شويد. سوئيچ از شما يک password درخواست خواهد كرد. تا اينجا بازدن دكمه<enter> وارد سوئيچ مي شديد. ولي براي حفظ امنيت بايد حتما اين password را تغييردهيد.
Passwordبايد حداقل 8 كاراكترداشته باشد و شامل حروف كوچک و بزرگ و اعداد وعلائم باشد. نحوه تعريف اين password در زيرآمده است. اين password درسوئيچ بصورت رمزشده ذخيره مي شود.

Telnet Password

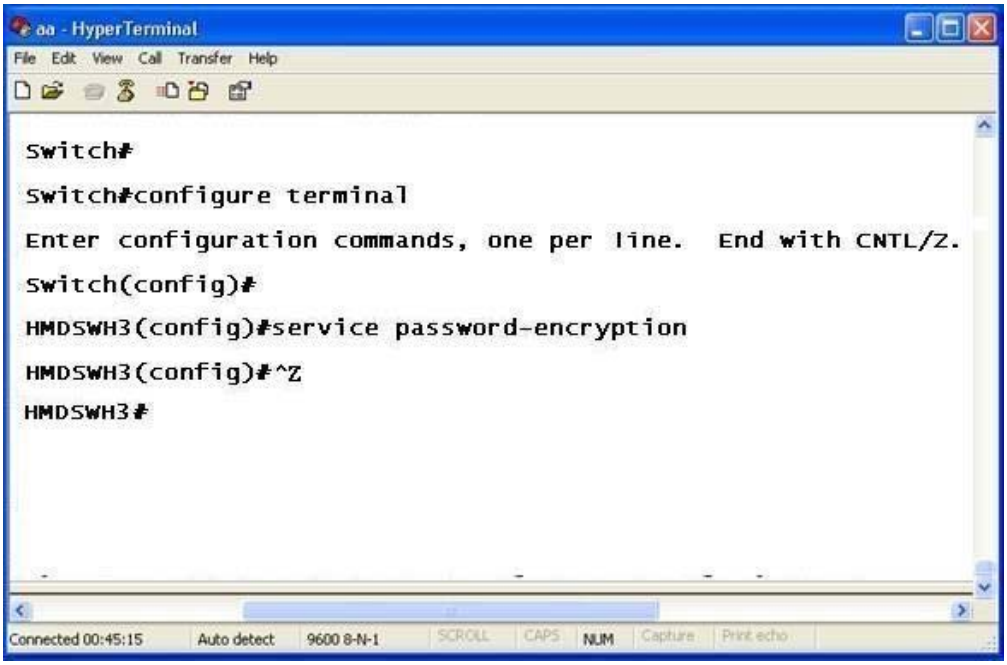
وقتي بخواهيم سوئيچ را از راه دور (ازطريق شبكه) پيكربندی كنيم از telnet استفاده مي كنيم. براي اينكه بتوانيم از طريق telnet به سوئيچ وصل شويم، حتما بايد برروي سوئيچtelnet password تعريف كنيم وگرنه سوئيچ به telnetجواب نمي دهد. جهت تعريف telnet password از دستورات زيراستفاده مي كنيم.



بطورهمزمان چندين نفرمي توانند ازطريق telnet سوئيچ را پيكربندی كنند. جهت داشتن امنيت بالا در password مورد نظرخود، حتما از تركيب حروف كوچک و بزرگ، اعداد وعلائم استفاده نمائيد وطول آنها حداقل 8 كاراكترباشد.

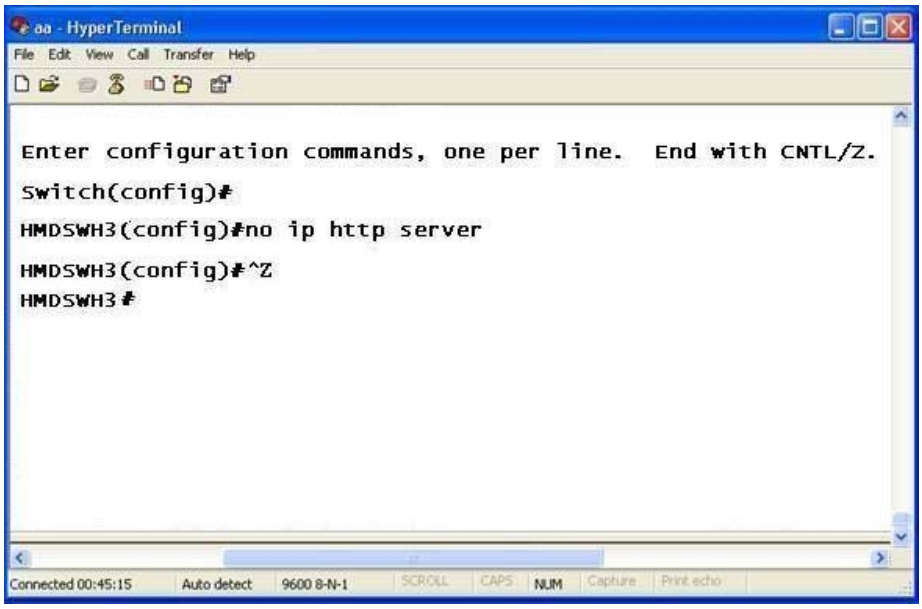
Password Encription

براي اينكه تمامي password هاي داخل سوئيچ بصورت رمز شده نمايش داده شوند و توسط افراد مختلف غيرقابل خواندن نباشند از دستور زير استفاده مي شود.



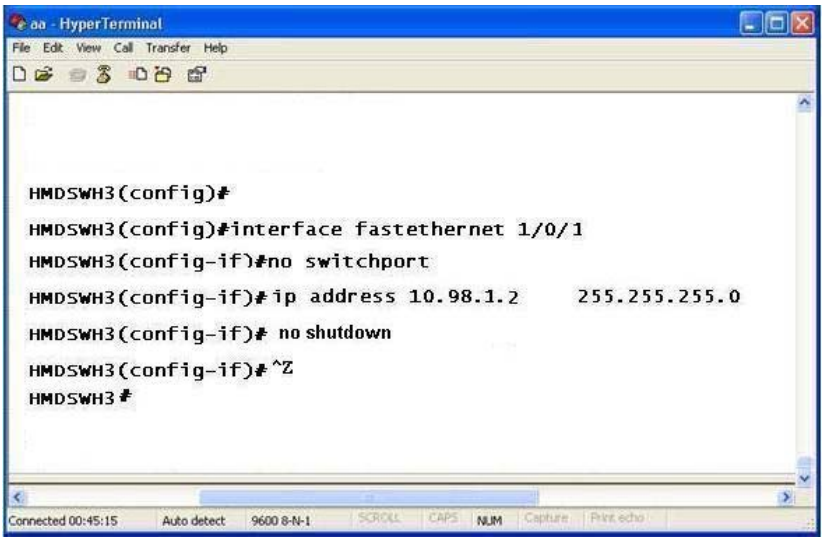
http Server

به دلايل امنيتي براي اينكه نتوان از طريق web browser به سوئيچ وصل شد. http server را روي آن غير فعال مي كنيم. (زيرا امكان اتصال به سوئيچ ازطريق web نيز وجود دارد)

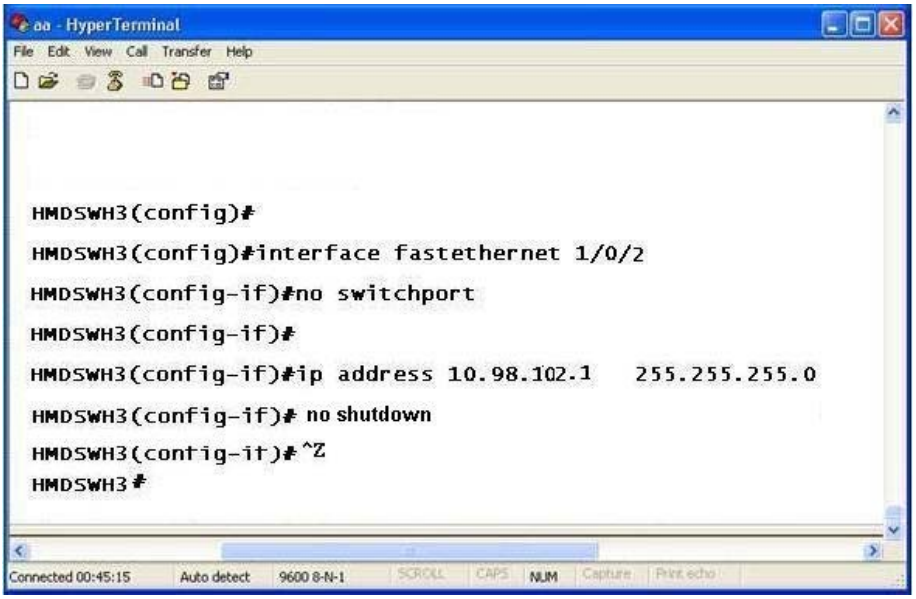


تعريف پورتهاي سوئيچ لايه 3 به عنوان روتر وIP دادن به آنها

هر پورت سوئيچ مي تواند بعنوان سوئيچ لايه 2 يا اينكه لايه 3 بكار روند. وقتي مي خواهيم از هرپورت سوئيچ لايه 3 به عنوان روتر استفاده كنيم در مد interface از دستور no switchport استفاده مي كنيم. حال مي خواهيم به پورتهاي سوئيچ، IP address بدهيم براي اين منظور وارد مد interface مي شويم.

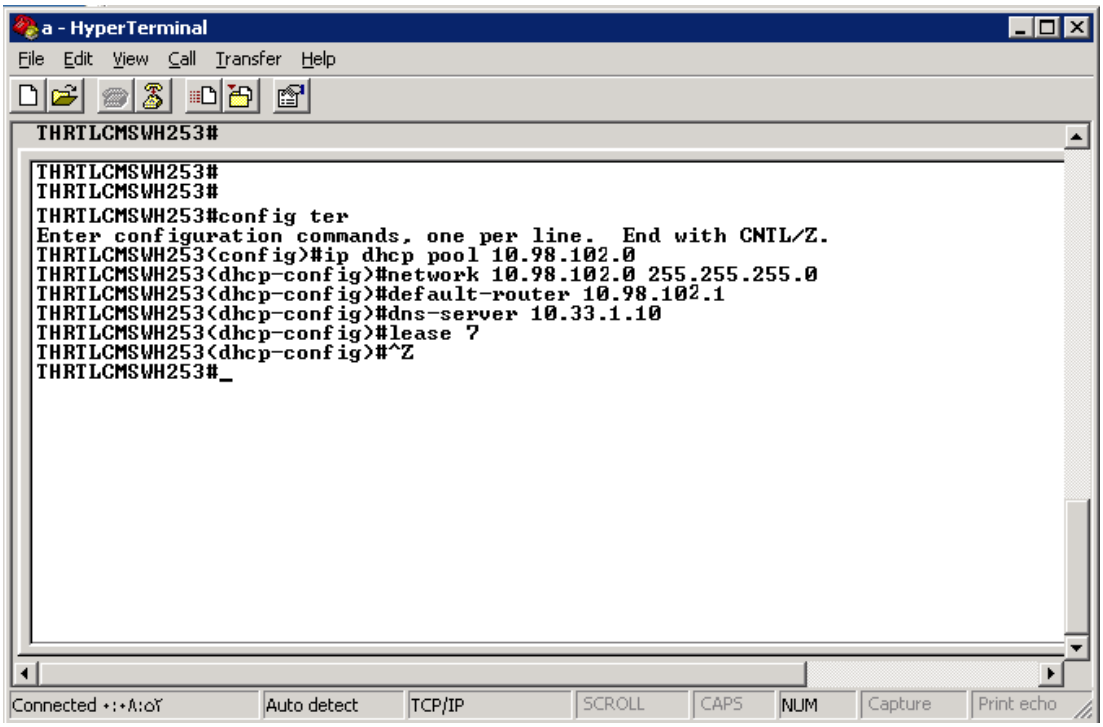


تـا وقتيكـه دسـتور no shutdown را بـرروي interface نزنيـد پـورت مربوطـه غيرفعال خواهد بود. همچنين پس از اتصال كابل بايد پورت شماره يک سـوئيچ روشـن شـود. سـپس به پورتهاي ديگر سوئيچ، IP مي دهـيم. بـراي پـورت دوم IP:10.98.102.1 بـراي پـورت سـوم IP:10.98.103.1 و بـراي پـورت چهـارم IP:10.98.104.1 و الي آخررا در نظر مي گيريم.

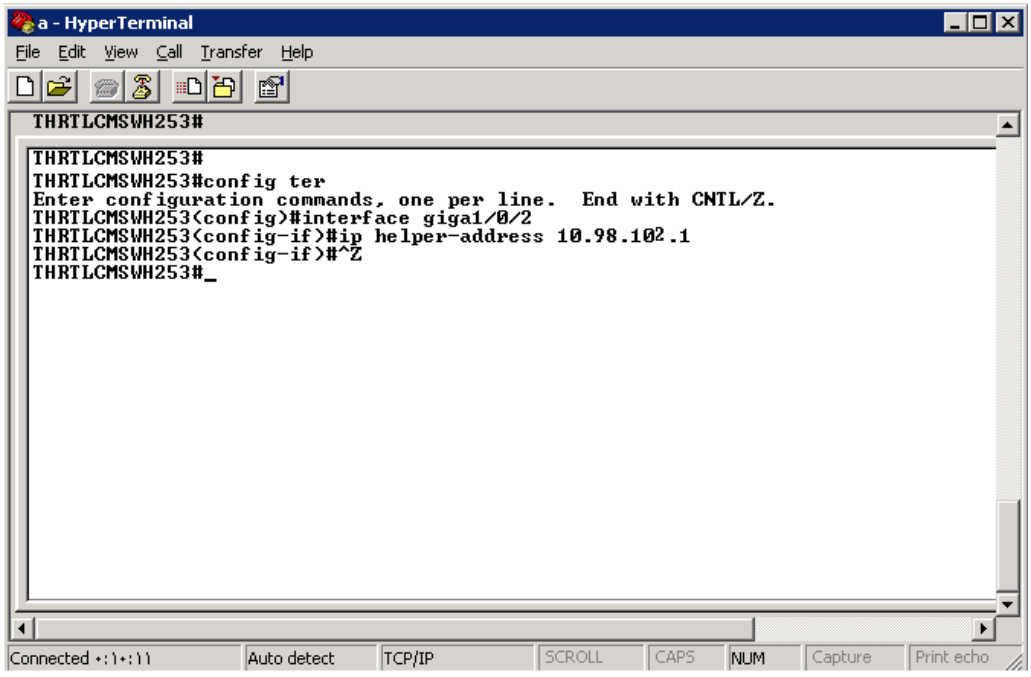


راه اندازي DHCP Server برروي سوئيچ

سوئيچهاي لايه 3 اين قابليت را دارند كه بتوان بر روي هـر پـورت آن DHCP راه اندازي كرد تا شبكه اي كـه بـه آن پـورت وصـل مـي شـود، IP, MASK, DNS, Gateway را بطـور اتوماتيـک دريافـت نمايـد. فـرض كنيـد بـر روي پـورت دوم سوئيچ، مي خـواهيم DHCP Server راه انـدازي كنـيم. ابتـدا دسـتورات زيـر را اجرا مي كنيم.

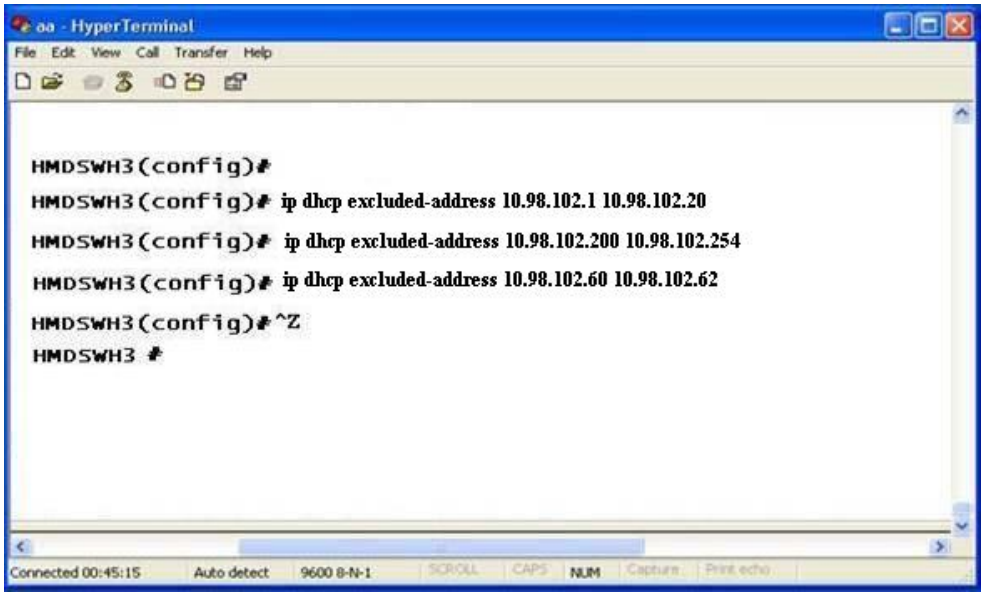


سپس دستورات زير را مي زنيم:



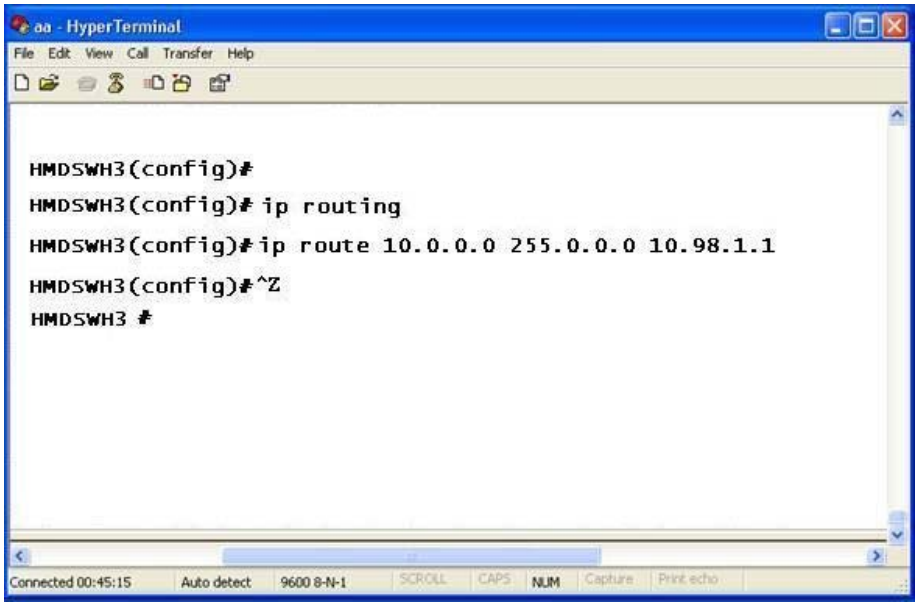
نحوه حذف کردن محدوده IP ها از DHCP Server

وارد مد config مي شويم و دستورات زير را مي زنيم:



Routing

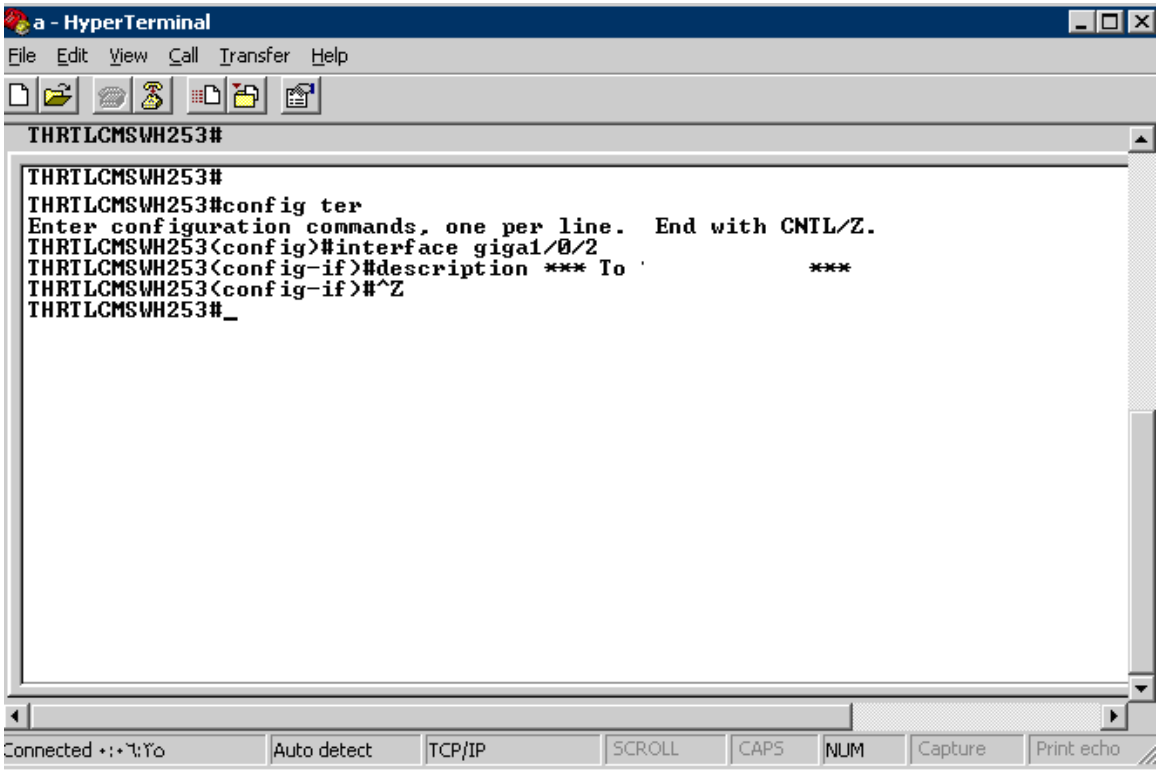
براي اينكه Routing را برروي سوئيچ فعال نمائيد ازدستور زير استفاده مي نمائيم.



براي اينكه برروي سوئيچ بتوان Routing را فعال كرد بايد دستور ip routing برروي سوئيچ يكبار اجرا شود.

description

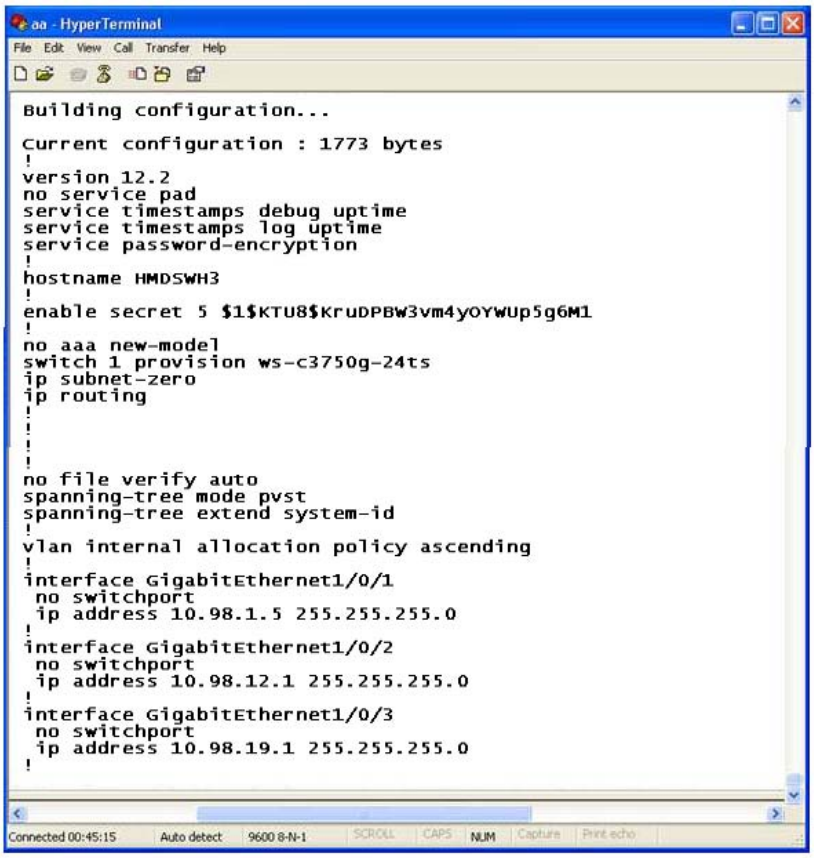
مي خواهيم براي هر يک از پورتهاي سوئيچ، توضيحي بنويسيم تا خيلي راحت با نگاه به پيکربندی داخل سوئيچ، بدانيم هر پورت به کجا وصل شده است. همچنين اين توضيحات توسط نرم افزار solarwinds بصورت اتوماتيک قابل خواندن مي باشد. وقتي روي سوئيچي در solarwinds کليک مي کنيم، اطلاعات پورتهاي آنرا نشان مي دهد.



برای اضافه کردن توضيح برای هر پورت، وارد پورت موردنظر مي شويم واطلاعات مورد نظر خود را درفاصله بين دوتا سه ستاره اي که در بالا، مشاهده مي نمائيد، وارد مي کنيم.

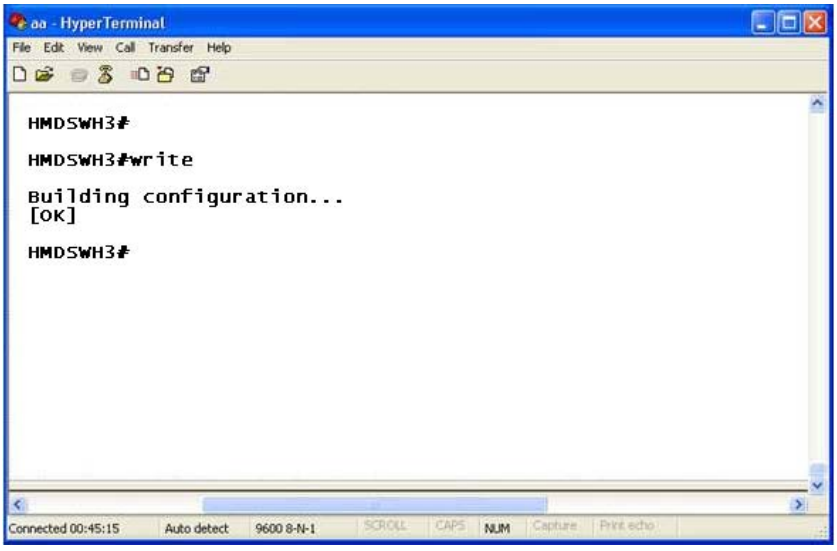
بررسي پيکربندی انجام شده

قبل ازذخيره نمودن پيکربندی هاي انجام شده از دستور show running-config جهت مشاهده پيکربندی انجام شده، استفاده مي کنيم.



ذخیره پیکربندی انجام شده

پس از آنکه پیکربندی انجام شده سوئیچ را بررسي كرديم. با دستورwrite آنرا ذخیره مي كنيم تا وقتيكه سوئيچ reset شد، پیکربندی آن پاک نشود.

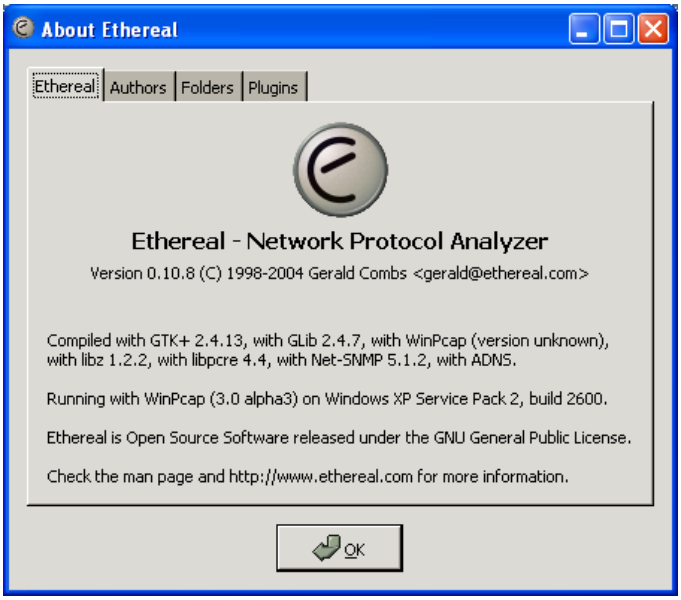


ضميمه 1

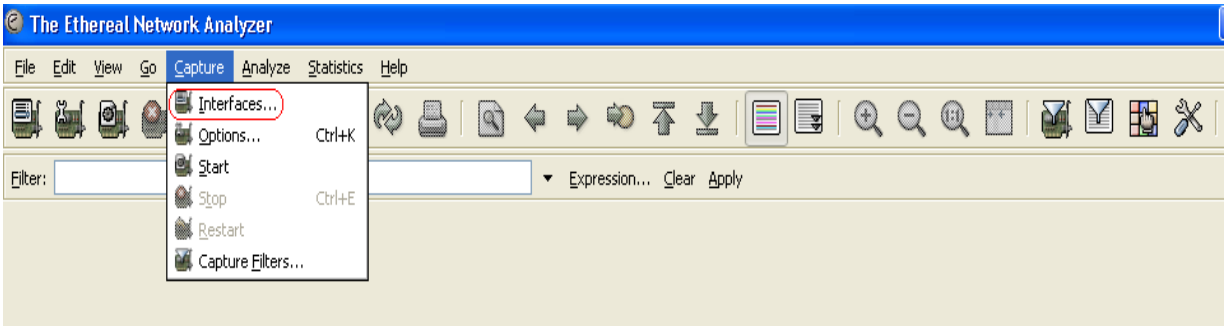
مونيتور كردن بسته هاي ارسالي در محيط LAN و معرفي Ethereal و بررسي DNS server

Ethereal

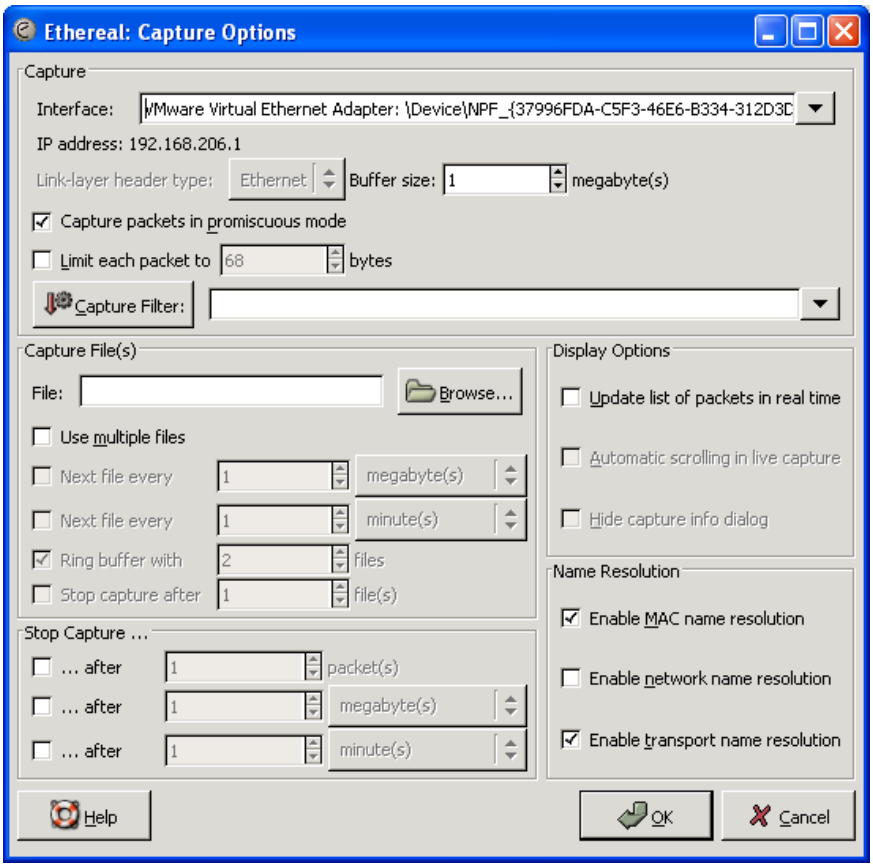
نرم افزار Ethereal جهت بررسي و تشخيص بسته هايي كه از كارت شبكه عبور مي كنند، استفاده می شود. این نرم افزار به کمک WinPcap قادر به انجام این عملیات است. این نرم افزار از نوع OpenSource بوده و تحت ليسانس GNU (General Public License) منتشر مي‌شود.

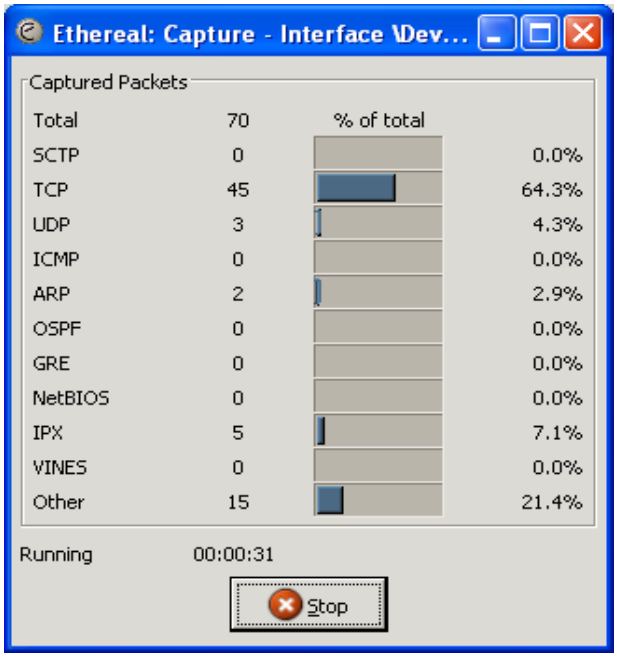


براي اين كه بين Interfaceهاي مختلف يكي را انتخاب كنيم بايد از قسمت Capture بخش Interface را انتخاب كنيم.

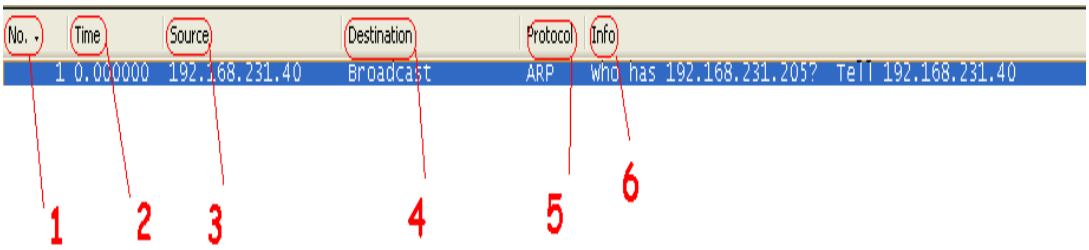


سپس پس از انتخاب Interface مورد نظر روي Capture كليک مي‌كنيم. براي اينكه اين عمليات را متوقف كنيم نيز مي‌توانيم روي Stop كليک كنيم و سپس يک مسير را براي ذخيره‌ي اطلاعات معرفي كنيم.





در ادامه، براي آشنايي بيشتر با اين نرم افزار و آشنايي با طرز تحليل اين نرم افزار به تحليل تعدادي از Packet هاي Capture شده توسط اين نرم افزار مي پردازيم. اين نرم افزار، اطلاعات مربوط به هر Packet را در3 قسمت نشان مي‌دهد. قسمت اول كه اطلاعات كلي راجع به كليه‌ي Packetها را نشان مي‌دهد. مانند شكل زير:



1- قسمت "No." شماره‌ي Packet را از زماني كه شروع به Capture كردن كرده است را نشان مي‌دهد.
2- قسمت"Time" زمان دريافت Packet را نشان مي‌دهد كه زمان شروع آن آغاز زمان Capture كردن است.
3- قسمت "Source" آدرس فيزيكي مبدأ را نشان مي‌دهد.
4- قسمت "Destination" آدرس فيزيكي مقصد را نشان مي‌دهد.
5- قسمت "Protocol" پروتكلي را كه Packet تحت آن ساخته و فرستاده شده است را نشان مي‌دهد.
6- قسمت"Info" اطلاعاتي را راجع به محتواي Packet بيان مي‌كند.

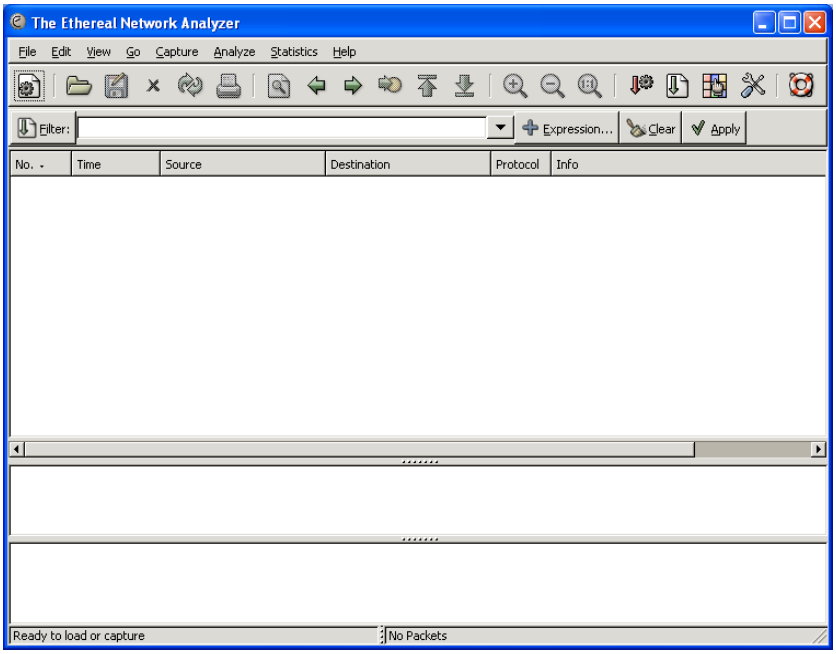
```
Frame 1 (60 bytes on wire, 60 bytes captured)
    Arrival Time: Jul  5, 2005 14:21:50.742580000
    Time delta from previous packet: 0.000000000 seconds
    Time since reference or first frame: 0.000000000 seconds
    Frame Number: 1
    Packet Length: 60 bytes
    Capture Length: 60 bytes
    Protocols in frame: eth:arp
Ethernet II, Src: 00:e0:7d:ce:93:a7, Dst: ff:ff:ff:ff:ff:ff
    Destination: ff:ff:ff:ff:ff:ff (Broadcast)
    Source: 00:e0:7d:ce:93:a7 (192.168.231.40)
    Type: ARP (0x0806)
    Trailer: 20202020202020202020202020202020
Address Resolution Protocol (request)
    Hardware type: Ethernet (0x0001)
    Protocol type: IP (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (0x0001)
    Sender MAC address: 00:e0:7d:ce:93:a7 (192.168.231.40)
    Sender IP address: 192.168.231.40 (192.168.231.40)
    Target MAC address: 00:00:00:00:00:00 (00:00:00_00:00:00)
    Target IP address: 192.168.231.205 (192.168.231.205)
```

1- در قسمت Frame، اطلاعاتي راجع به طول Frame و زمان بندي آن و پروتكل آن بيان مي‌كند.
2- در قسمت دوم، اطلاعاتي راجع به مبدا و مقصد Frame و همچنين Trailer آن بيان مي‌كند.
3- در اين قسمت Mac Address و IP Address فرستنده و گيرنده بيان مي‌شود.

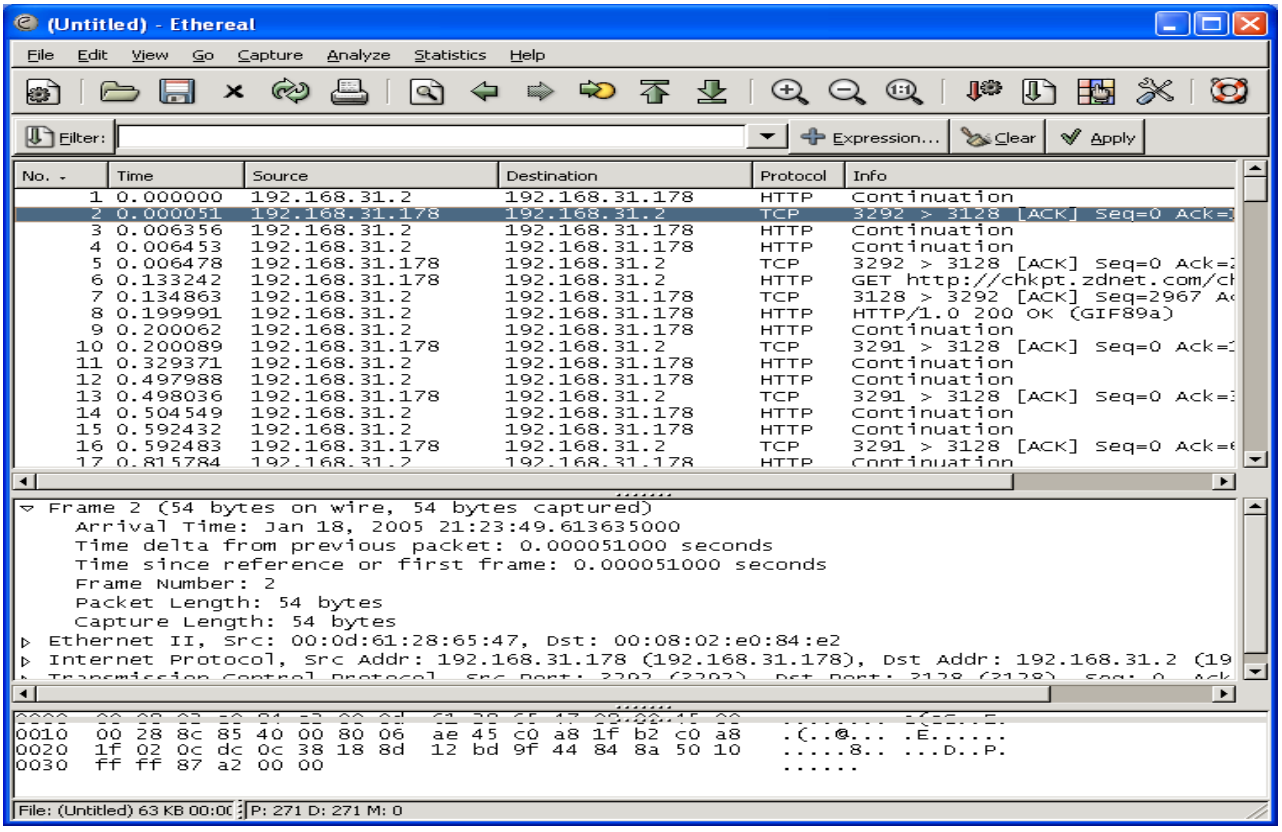
```
0000  ff ff ff ff ff ff 00 e0  7d ce 93 a7 08 06 00 01   ........ }.......
0010  08 00 06 04 00 01 00 e0  7d ce 93 a7 c0 a8 e7 28   ........ }......(
0020  00 00 00 00 00 00 c0 a8  e7 cd 20 20 20 20 20 20   ........ ..
0030  20 20 20 20 20 20 20 20  20 20 20 20

Target IP address (arp.dst.proto_ipv | P: 2258 D: 2258 M: 0
```

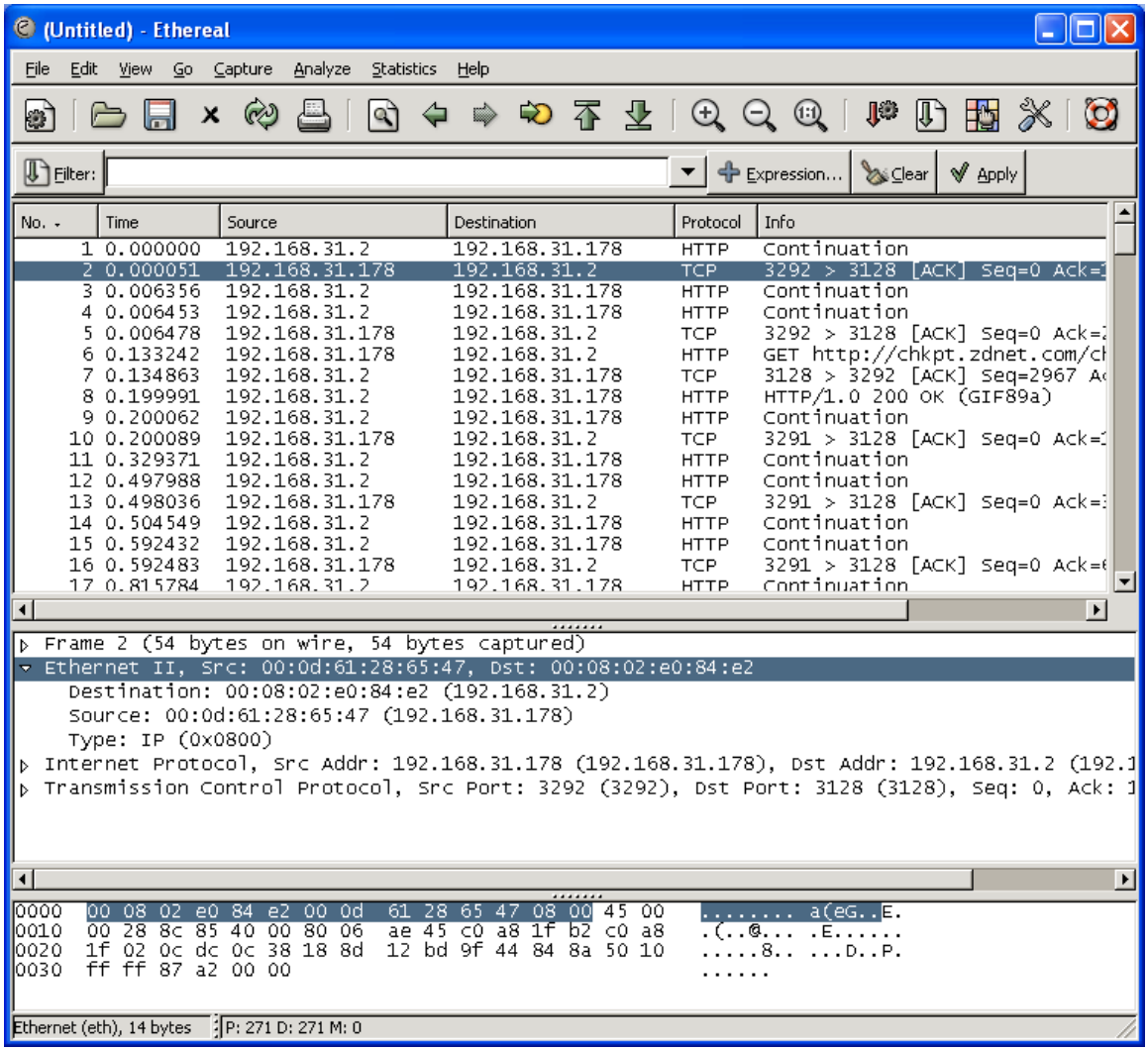
در اين بخش، معادل عددي (در مبناي 16) هركدام از قسمتهاي گفته شده در بالا را نشان مي‌دهد.
حال در اين قسمت، از هر پروتكل يک Packet به عنوان نمونه، بررسي مي-شود.



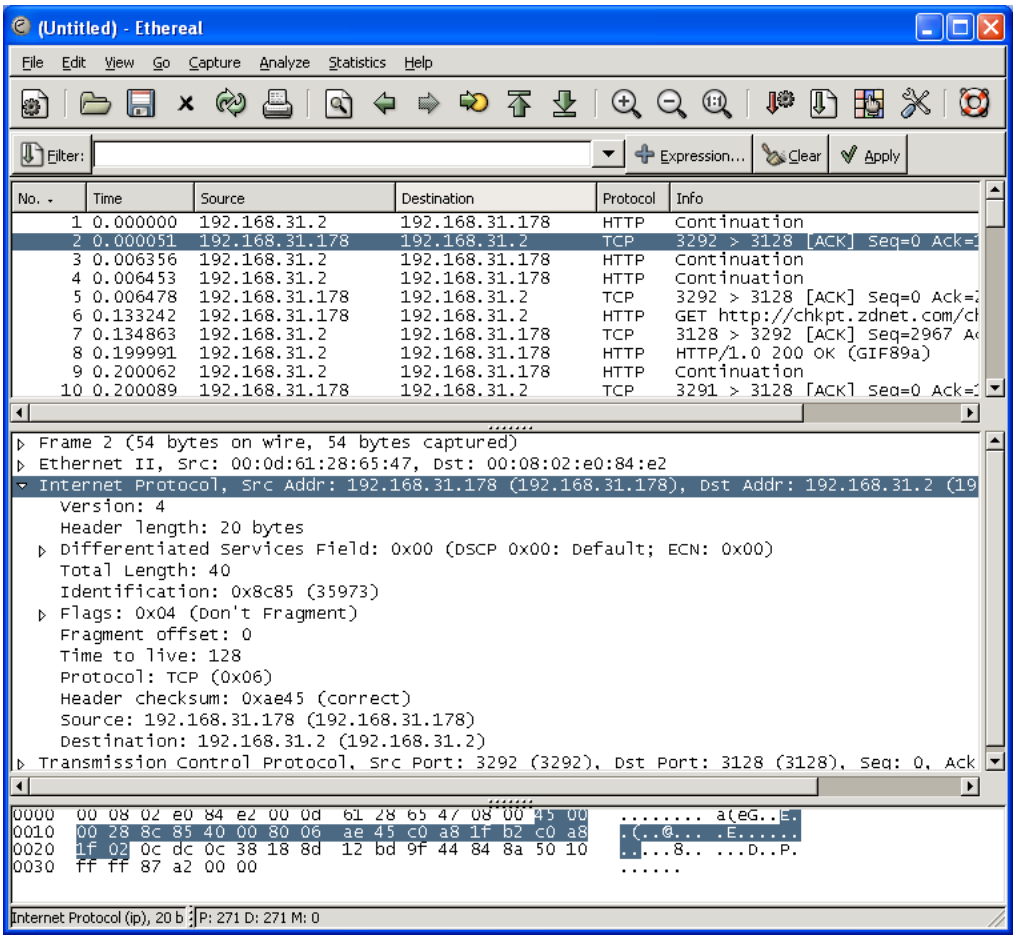
در این قسمت، یک Frame که طول آن 54 بایت است. مورد بررسي قرار گرفته شده است.



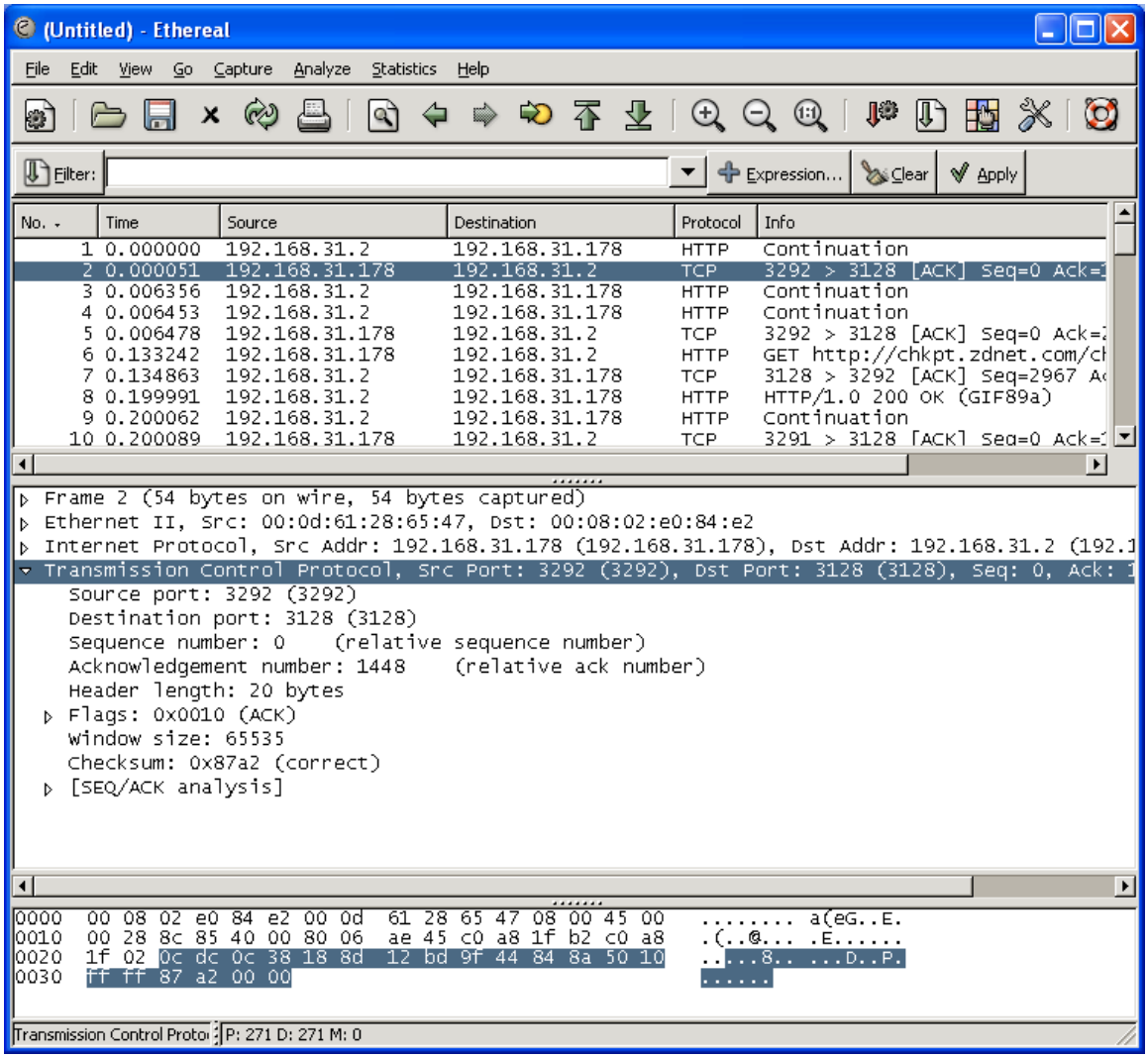
14 بايت از frame ذكر شـده، مربـوط بـه اطلاعـات Ethernet مـي باشـد, كـه شـامل آدرسـهاي فيزيكي براي مبدا و مقصد مي باشد.



سـپس لايـه سـوم (Internet Layer) را مـورد بررسـي قـرار ميـدهيم. در ايـن بخش، 20 بايت شـامل اطلاعـاتي از قبيـل آدرسـهاي IP بـراي مبـدا و مقصـد وجود دارد.



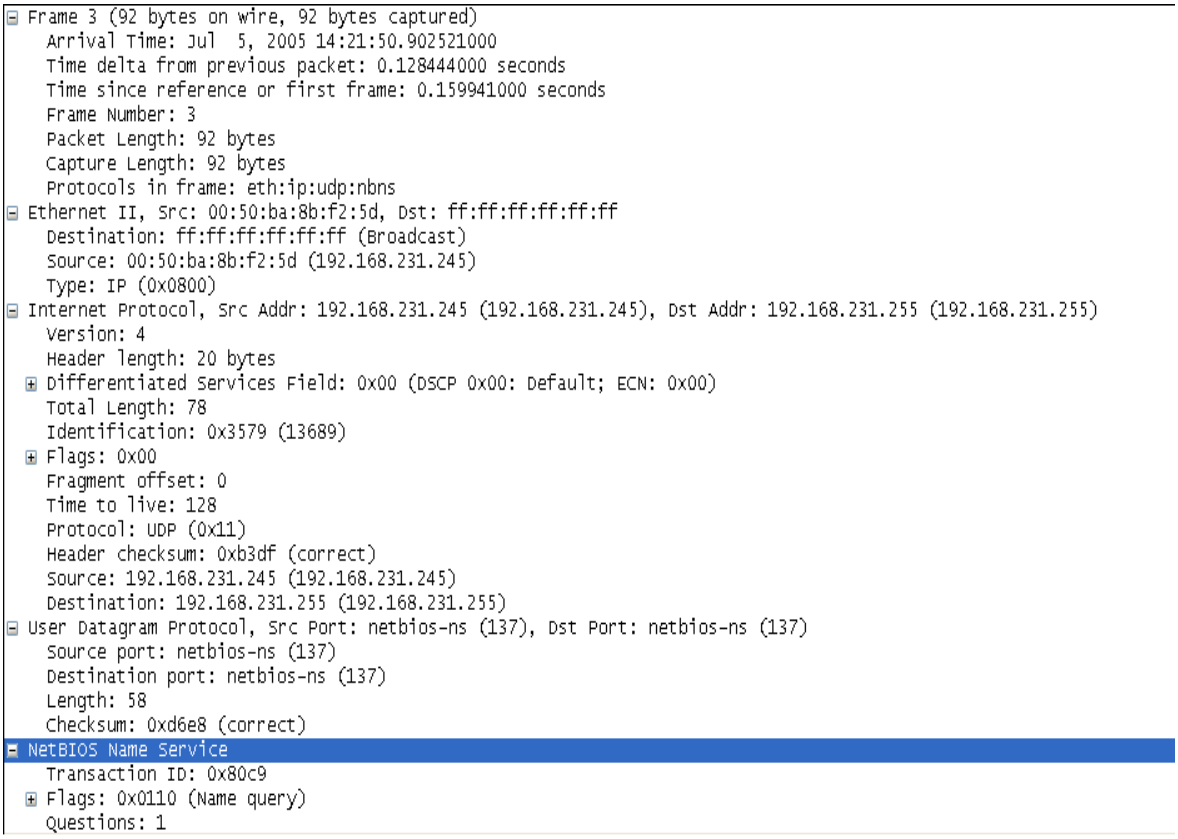
نهايتا، اطلاعات مربوط به لايه چهارم (لايـه انتقـال) در 20 بايـت شـامل آدرس درگاه هاي مربوطه نشان داده مي شود.



ARP

1- شماره‌ي اين Packet "2" است
2- زمان دريافت آن 0.031497 (زمان دريافت نسبت به زمان آغاز Capture كردن سنجيده مي‌شود.) مى باشد.
3- آدرس فرستنده، 192.168.231.40 مى باشد.
4- آدرس گيرنده = Broadcast (يعني به همه‌ي Nodeها ارسال مي‌شود.)
5- پروتكل مورد استفاده، ARP است.

6- محتـــوا= چـــه كســـي داراي آدرس 192.168.231.251 اســـت بـــه من(192.168.231.40) بگويد.(يعني آدرس فيزيكي خود را ارسال كند.)

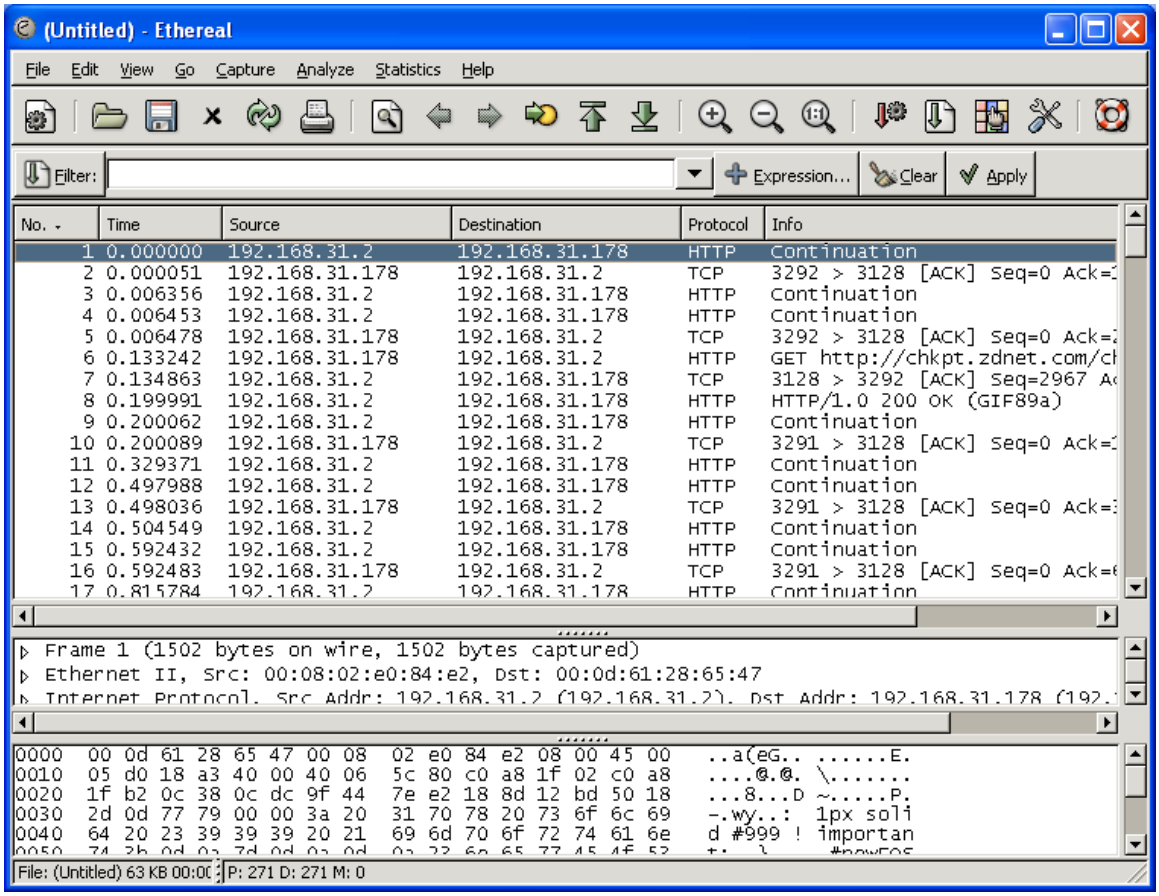


1- زمان رسيدن Packet و فاصله‌ي آن از Packet قبلي و شـماره‌ي Frame آن و فاصله‌ي آن از Packet اول و طول Packet بيان شده است.

2- مقصـــد آن 0000(ff ff ff ff ff ff) و مبـــدا آن و مقصـــد آن (00:50:ba:8b:f2:5d) بيان شده است.

3- طول Header و Flagهـا و Checksum موجـود در Header و همچنـين Port مبدا و مقصد مشخص شده است.

HTTP



1- شماره‌ي اين Packet "803"است.

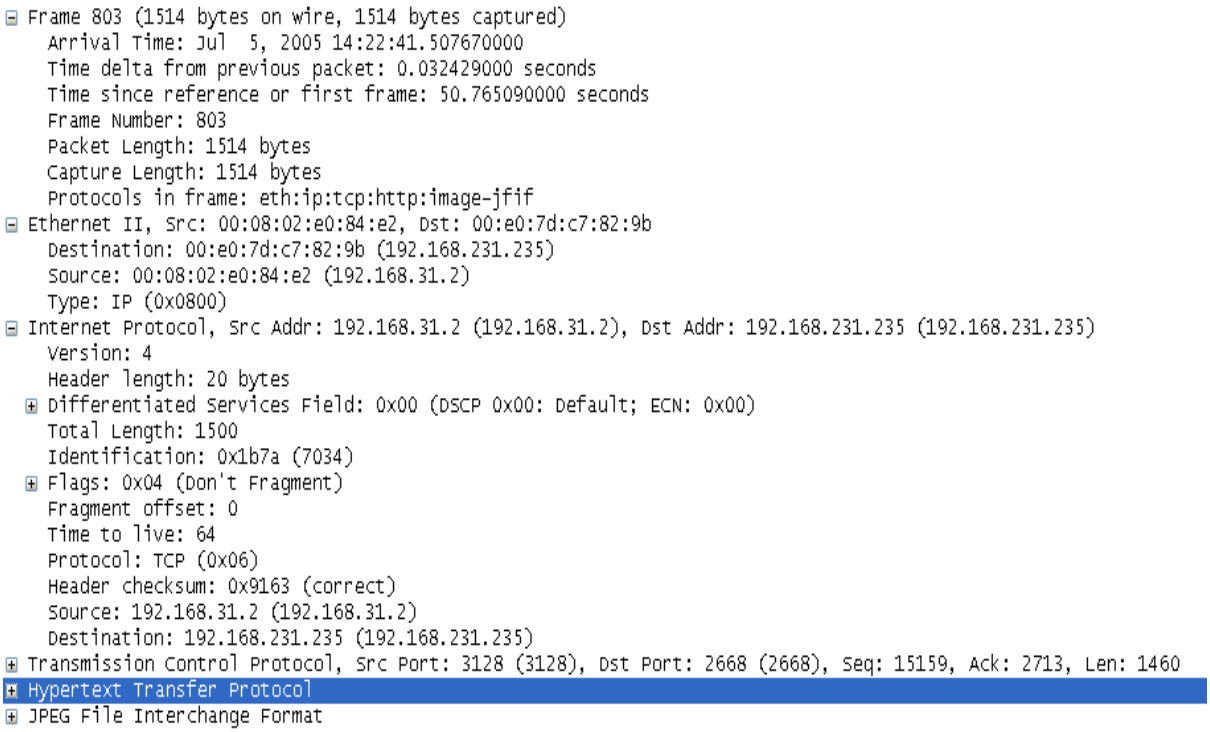
2- زمان دريافت آن 50.765090 است.

3- آدرس فرستنده 192.168.31.2 است.

4- آدرس گيرنده 192.168.231.235 است.

5- پروتكل مورد استفاده، HTTP است.

6- محتوا، يک تصوير JPEG است.



1- اطلاعات مربوط به این قسمت مانند Packet قبلي است.

2- در قسمت Ethernet نیز مانند قسمت قبل آدرس مبدا و مقصد و پروتکل ارتباط مشخص شده است.

3- در قسمت Internet Protocol، Versionپروتکل ، تعداد بایتهاي موجود در Header، Flagها، زمان وجود داشتن،Checksum موجود در Header، اعلام درست یا نادرست بودن Packet، پروتکل مورد استفاده، آدرس مبدا و مقصد موجود است.

4- در قسمت پروتکل کنترل انتقال شمارهي پورت مبدا و مقصد، شمارهي ترتیبي بعدي، شمارهي Ack، طول Header،محتواي Flagها که در اینجا به عنوان Ack به کار رفته است، طول پنجرهي ارسال و دریافت، Checksum و اعلام درستي یا نادرستي آن وجود دارد.

5- در بخش پروتکل انتقال Hypertext محتواي Packet و اطلاعاتي راجع به Serverي که اطلاعات در آنجا قرار دارد موجود است.

6- در قسمت آخر، نيز اطلاعاتي راجع به تصويري كه در واقع محتـواي اصـلي Packet اسـت موجود مي‌باشـد.

ضميمه 2

آشنايي با شبكه هاي بي سيم

اجزاي شبكه بي سيم

شبكه هاي با سيم و بي سيم هر دو از يک سري از قطعات اساسي براي بوجود آوردن شبكه استفاده مي كنند.

كارت بي سيم

هر كامپيوتر كه مي خواهد به شبكه وصل شود احتياج به يک كارت شبكه دارد كه درون آن نصب شده است. در يک كامپيوتر روميزي ,كارت شبكه معمولاً درون كامپيوتر و به غالباً در PCI Slot كه در كامپيوتر هاي شخصي رايج هستند نصب مي شود. در يک كارت شبكه، يک آنتن معمولاً 10 سانتي وجود دارد كه بيرون كامپيوتر قرار دارد و قابليت چرخش براي دريافت بهتر را دارد.

كارتهاي بيسيم بر روي PCI Slot قرار دادند وكارت هاي بي سيم لپ تاپ ها بر روي PCMCIA SLOT قرار دارند كه احتمالاً PCMCIA SLOT در يک طرف لپ تاپ ها نصب مي شوند. در يک كارت شبكه بي سيم حدود25 سانتي متر از قسمتي از كارت بيرون آمده كه به عنوان آنتن عمل مي كند در كامپيوتر هاي Apple Macintosh كارت(Air port) در داخل كامپيوتر نصب مي شوند كه از بيرون غير قابل مشاهده است.

يک كارت شبكه كه از طريق يک گذرگاه USB به كامپيوتر وصل مي شود، سومين امكان اتصال را از طريق USB به كامپيوتر فراهم مي كند. در اين مورد، آنتن بر روي كارت قرار دارد, كه مي تواند در هر كجا كه كابل USB به آن

A wireless card which connects to a USB port

Wireless card for a PCI Expansion Slot

Wireless card for a PCMCIA Slot

اين امكان را مي دهد، قرار گيرد. اين كارت شبكه، نيروي خود را از گذرگاه USB مي گيرد و احتياج به يک منبع تغذيه اضافه ندارد.
كارتهاي شبكه از طريق نرم افزار نصب خواهند شد. همچنين ابزاري براي كنترل كارت براي برقراري ارتباط با شبكه فراهم مي آورند. اين نرم افزار معمولاً يک سري از نشانه هاي تصويري از قدرت سيگنال را نمايش مي دهند كه به كمک اين نرم افزار شما مي توانيد تنظيمات آنتن را براي گرفتن بهترين سيگنال انجام دهيد.

Access Point هاي بي سيم (Wireless Access Point)

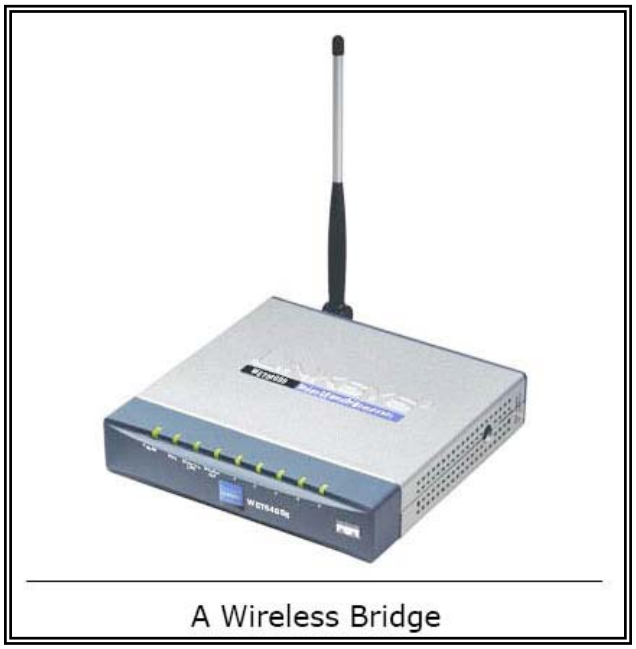
راه حل جايگزين به جاي هاب در شبكه های بی سيم، استفاده از Access Point بي سيم(WAP) است. وقتي كه (WAP) روشن ميشود نقطه ارتباطي براي پيكر بندي اتصال كارتهاي شبكه هر كامپيوتر با آن مي شود. همه تجهيزات بي سيم قادر هستند كه با استاندارد هاي سازگار و يا استاندارد خودشان كار كرده و سپس براي اتصال به اين WAP پيكربندي شود. اگر يک WAP به يک هاب كه سرويسهاي از قبيل فايل ,چاپگر و اتصالات اينترنتي را به اشتراک گذاشته متصل شود تمام اين سرويسها فوراً در اختيار يک كامپيوتر Wireles قرار خواهند گرفت. تمام اينها مستلزم پيكر بندي نرم افزاري است و نه به كار بردن و نصب سيمها.

A wireless access point

پلهاي بي سيم (Wireless Bridge)

يک پل بي سيم، گذرگاهي براي اتصال دو LAN به صورت بي سيم با يكديگر است. يک نمونه كاربردي، ممكن است جايي باشد كه شما مي خواهيد دو ساختمان جدا از يكديگر را بدون استفاده از سيم به يكديگر متصل

کنید. یک پل بي سيم در هر شبکه LAN نیاز است و لازم است که هر دو پل در یک دامنه قرار داشته باشد .



A Wireless Bridge

گستره یک پل بي سيم، معمولاً بیشتر از (WAP) است. پلهاي بي سيم معمولاً به همراه یک آنتن بزرگ طراحي شده اند که براي دستیابي به حداکثر پهناي باند میتوانند در بیرون نصب شوند.

ضميمه 3

FTP Server

پروژه آزمايشگاه پياده سازي يک FTP Server ساده، بر اساس استاندارد پروتکل FTP(RFC959) است. اين نرمافزار مي بايست يک Configuration File و يک User File را خوانده و بر اساس آن يک FTP Server بر روي پورت مورد نظر بالا بياورد. براي پشتيباني از درخواستهاي همزمان اين سرويس دهنده مي بايست بصورت Multi-Thread يا Multi-Process و يا Select-Based نوشته شود.
هدف از انجام اين پروژه آشنايي با مدل 4 لايه TCP/IP و مفاهيم Socket Programming و همچنين آشنايي با پروتکل FTP و تکنيکهاي پياده سازي آنها است.

- محيط اجرا: ويندوز يا لينوکس(در صورتي که در هر دو محيط قابل اجرا باشد، امتياز مثبت منظور مي‌شود)
- زبان برنامه نويسي: جاوا و يا C (براي زبانهاي ديگر هماهنگ کنيد)
- دستورات FTP که مي بايست پشتيباني شوند:
  - کليه دستورات مربوط به تصديق هويت با نام کاربري و کلمه عبور شامل:
    - USER, PASS
  - تعويض دايرکتوري شامل:
    - CWD, CDUP,
  - خروج از سيستم (LOGOUT)
  - دستورات انتقال
    - PORT, PASV, TYPE, MODE,
  - دستورات سرويس FTP
    - RETR, STOR, RNFR, DELE, RMD,MKD, PWD, LIST
- از RFC959 ، Reply Code هايي که مربوط به دستورات بالا است مي بايست به سمت Client بدرستي ارسال شوند.

- حداقل موارد مورد نياز در Configuration File: دايركتوري كه فايلهاي FTP قرار دارد (FTP_ROOT) و همچنين پورت سرويس دهنده(پيش فرض: 21)
- در USER FILE نام كاربري و كلمه عبور كاربران به همراه ميزان دسترسي آنها (READ/READ-Write) نوشته ميشود.
- يک سند حاوي نحوه پياده سازي و استفاده از FTP Server پس از انجام پروژه مي بايست تحويل داده شود.

ضميمه 4

HTTP SERVER

پروژه درس پياده سازي يک HTTP Server(Web Server) ساده، بر اساس استاندارد RFC2616 است. اين نرم افزار مي بايست يک Configuration File را خوانده و بر اساس آن يک HTTP Server بر روي پورت مورد نظر بالا بياورد. براي پشتيباني از درخواستهاي همزمان اين سرويس دهنده مي بايست بصورت Multi-Thread يا Multi-Process و يا Select-Based نوشته شود.

- محيط اجرا: ويندوز يا لينوکس(در صورتي که در هر دو محيط قابل اجرا باشد، امتياز مثبت منظور مي شود)
- زبان برنامه نويسي: جاوا و يا C (براي زبانهاي ديگر هماهنگ کنيد)
- متودهاي HTTP که مي بايست پياده شوند: GET و HEAD
- پشتيباني از فايلهاي HTML و Image
- نسخه HTTP: هم 1.0 HTTP و هم 1.1 HTTP ميبايست پشتيباني شوند.
- Status Code هاي پشتباني شده: 200, 400, 404, 500, 501
- حداقل موارد مورد نياز در Configuration File: دايرکتوري که فايلهاي HTML قرار دارد و همچنين پورت سرويس دهنده
- يک سند حاوي نحوه پياده سازي و استفاده از Web Server
- مواردي که نمره اضافه خواهد داشت:
  - پشتباني از ساير متود ها و Status code هايي که در RFC آمده
  - Directory Browsing
  - Basic Authentication
  - پشتيباني از ساير مديا فايلها
  - Server Scripting براي محتواي ديناميک