فصل ششم

آشنایی با پروتکل TCP/ IP و سرویس‌های آن

هدف‌های رفتاری: هنرجو پس از پایان این فصل می‌تواند:

- سرویس‌های رایج در پروتکل TCP/IP را شناسایی کند.
- سرویس‌های رایج در شبکه اینترنت را شرح دهد.
- مفهوم Host در پروتکل TCP/IP را بیان کند.
- انواع دامنه‌های رایج را بیان کند.
- مراحل ثبت Domain را شرح دهد.
- انواع کلاس‌های IP را شناسایی کند.

۱ـ۶ـ نقش پروتکل در شبکه

بهره‌برداری از امکانات سخت‌افزاری و برقراری ارتباط بین اجزای مختلف شبکه نیاز به یک مجموعه از قوانین و دستورالعمل‌های مشترک دارد که به آن قوانین اصطلاحاً پروتکل می‌گوییم.

پروتکل مجموعه قوانینی است که اگر آنها را رعایت نکنیم ارائهٔ سرویس (یعنی هدف از برقراری شبکه) غیرممکن خواهد شد.

تعریف : پروتکل مجموعه قوانینی نرم‌افزاری است که رعایت آنها باعث بهره‌برداری از امکانات سخت‌افزاری و برقراری سرویس در شبکه می‌شود.

نقش پروتکل در رایانه ارسال کننده داده :

- شکستن داده‌ها به بخش‌های کوچکتر، به نام بسته[1]
- اضافه‌کردن اطلاعات آدرس مقصد به بسته
- آماده‌سازی داده‌ها برای انتقال از طریق کارت شبکه بر روی کابل شبکه.

۱ـ Packet

نقش پروتکل در رایانه دریافت کننده داده

- دریافت بسته‌های داده از کابل شبکه
- ایجاد نواری از بسته‌های ارسالی از رایانه فرستنده
- کپی کردن بسته‌ها به بافر برای دوباره اسمبل کردن به عنوان داده
- پذیرش داده‌ها به شکل برنامه قابل استفاده

توجه اگر پروتکل‌های استفاده شده در رایانه‌های فرستنده و گیرنده با هم متفاوت باشند امکان دریافت درست داده‌ها در رایانه گیرنده وجود نخواهد داشت و یا اینکه بسته‌های دریافتی در رایانه گیرنده قابل استفاده نخواهد بود.

زمانی که داده‌ها بخواهند در یک شبکه LAN بین رایانه‌ها منتقل شوند کار چندان پیچیده نیست، اما اگر شما بخواهید بین چند شبکه LAN ارتباط بر قرار کنید، ممکن است از پروتکل‌های مختلفی استفاده نمایید که در اینجا باید یک هماهنگ کننده پروتکل‌ها وجود داشته باشد نتایج این هماهنگی به عنوان لایه‌بندی شناخته شده است.

۲ـ۶ـ پروتکل TCP/IP[۱]

TCP/IP، یکی از مهم‌ترین پروتکل‌های استفاده شده در شبکه‌های کامپیوتری است و اولین بار در سیستم عامل UNIX مورد استفاده قرار گرفت. اینترنت بعنوان بزرگترین شبکه موجود، از پروتکل فوق به منظور ارتباط دستگاه‌های متفاوت استفاده می‌نماید. در اهمیت TCP/IP توجه به این نکته کافی است که ارتباط در اینترنت بدون TCP/IP تقریباً غیرممکن است و اکثر سرویس‌های اینترنت تحت قوانین TCP/IP عرضه می‌شوند.

TCP/IP مجموعه کاملی از پروتکل‌های تعریف شده برای استفاده در شبکه‌های خصوصی و اینترنت می‌باشد، ولی نام آن در واقع ترکیبی از دو پروتکل زیر می‌باشد :

الف) پروتکل کنترل انتقال TCP

ب) پروتکل اینترنت IP

مهم‌ترین خصوصیات این پروتکل به‌طور خلاصه عبارتند از :

۱ـ قابل استفاده در انواع شبکه‌ها

۲ـ پشتیبانی به وسیله انواع سیستم عامل‌ها

۱ـ Transmission Control Protocol / Internet Protocol

۳ــ مورد استفاده به عنوان پروتکل اصلی[1] اینترنت

۴ــ قابلیت مسیر یابی

۵ــ حق انتخاب در انتقال اطلاعات به صورت اتصال گرا[2] و بدون اتصال[3]

۶ــ ارسال گروهی

۷ــ پیکربندی پیچیده

از ویژگی‌های مهم پروتکل TCP/IP می‌توان به موارد زیر اشاره کرد :

- اولین ویژگی در TCP/IP آن است که می‌تواند در هر ابعادی از شبکه استفاده شود (از شبکه‌های کوچک یا بزرگ، با ترافیک کم یا ترافیک زیاد، با اتصال به اینترنت و بدون اتصال به اینترنت)
- چون TCP/IP در کلیهٔ سیستم عامل‌های مدرن امروزی پشتیبانی می‌شود بنابراین زبان مشترک ارتباط بین سیستم عامل‌ها می‌باشد.
- TCP/IP از ابتدا تا به امروز بعنوان پروتکل اصلی مورد استفاده در اینترنت بوده است.
- در TCP/IP الگوریتم‌های متنوع مسیریابی[4] برای انتخاب مسیر بهینه از میان روترها(مسیریاب‌ها) تعبیه شده و به همین خاطر یکی از مهم‌ترین پروتکل‌ها برای استفاده در شبکه‌های WAN به شمار می‌رود. همان طور که قبلاً اشاره شد هم بندی غالب شبکه‌های WAN از نوع Mesh می‌باشد و در نقاط مرزی مابین شبکه‌ها از Router استفاده می‌شود لذا پروتکل مورد استفاده باید دارای قابلیت مسیریابی (Routing) باشد.
- سرویس انتقال اطلاعات بصورت سفارشی یا اتصال گرا «Connection Oriented» معروف به TCP و سرویس انتقال اطلاعات بصورت عادی یا بدون اتصال «Connection less» معروف به UDP از دیگر بخش‌های متنوع این پروتکل می‌باشد.
- Multicasting به معنی ارسال اطلاعات برای گروهی از استفاده‌کنندگان (مخاطبین) می‌باشد.
- بالاخره آخرین خصوصیت TCP/IP که درواقع عیب آن به شمار می‌رود این است که پیکربندی پیچیده‌ای دارد. علت این پیچیدگی را می‌توان در تنوع سرویس‌های ارائه شده جستجو کرد. TCP/IP پروتکل بسیار کامل و متنوعی‌است، در نتیجه این تنوع، پیچیدگی در پیکربندی را به دنبال خواهد داشت.

۱ــ Primary Protocol

۲ــ Connection Oriented

۳ــ Connection less

۴ــ Routing

البته با توجه به وجود امکان پیکربندی خودکار و پویا[1] در TCP/IP در اکثر مواقع، کاربران نیازی به درگیر شدن با پیچیدگی‌های پیکربندی ندارند.

۳ـ۶ـ سرویس‌های TCP/IP

TCP/IP از سرویس‌های متنوعی تشکیل شده که اغلب نیازهای کاربران در شبکه‌ها را مستقیماً و بدون نیاز به هرگونه برنامه‌نویسی اضافی پاسخ می‌دهد. اغلب این سرویس‌ها برای کاربران آشنا بوده و در کاربردهای روزمره خود در اینترنت از آن‌ها استفاده می‌کنند. به موارد زیر توجه کنید :

۱ـ۳ـ۶ـ FTP[2] : یکی از کارهای ضروری که اغلب کاربران در شبکه بدان نیاز دارند انتقال پرونده است. TCP/IP مستقیماً دارای سرویسی است که انتقال پرونده را به‌راحتی بین ماشین‌های مختلف با سخت‌افزارهای متنوع و سیستم‌عامل‌های گوناگون امکان‌پذیر می‌سازد و آن FTP است.

FTP از دو قسمت تشکیل شده :

الف) FTP Client

ب) FTP Server

کاربر با اجرای نرم‌افزار FTP Client به FTP Server متصل شده و با توجه به مجوزهای امنیتی مربوطه می‌تواند پرونده‌های موردنیاز را از سرویس‌دهنده دریافت کرده (Download_Receive) یا آن‌ها را روی سرویس‌دهنده ذخیره کند. (Upload_Send)

در سیستم عامل‌های مایکروسافت نرم‌افزارهای گوناگونی به عنوان FTP Client وجود دارند مثلاً می‌توانیم به IE (Internet Explorer) اشاره کنیم که از خود مایکروسافت است یا دستور ftp.exe که در حالت Text از Command_Prompt اجرا می‌شود. نرم‌افزارهای دیگر مانند Cute FTP، FTP Pro، DAP و ... نیز همگی نقش FTP Client را بازی می‌کنند.

نرم‌افزارهایی که به‌عنوان FTP Server در مایکروسافت استفاده می‌شوند نیز موجود بوده و به‌عنوان مثال می‌توان به IIS اشاره کرد. IIS بسته‌ای است شامل چندین سرویس که یکی از آن‌ها FTP Server است.

۱ـ Automatic/Dynamic Configuration

۲ـ File Transfer Protocol در درس بسته‌های نرم‌افزاری (۳) با FTP به‌طور مشروح‌تر آشنا می‌شوید.

فعالیت عملی

آشنایی با سرویس FTP

در این بخش هنرآموز درس FTP Server را از قبل روی یک رایانه با سیستم‌عامل 2000 یا 2003 سرور پیکربندی کرده و هنرجویان با اجرای FTP Client در رایانه‌های خود (ترجیحاً IE) چند پرونده را از سرویس‌دهنده دریافت (Download) کنند. در این مرحله به هیچ عنوان نیازی به فراگیری پیکربندی FTP Server نبوده و هنرجویان فقط از آن استفاده می‌کنند.

۲ـ۳ـ۶ـ HTTP[1] : یک راه بسیار رایج برای دستیابی به اطلاعات که همگی با آن آشنا هستیم استفاده از سرویس HTTP است. همانند FTP، این سرویس نیز از دو بخش تشکیل شده :

الف) HTTP Client : که به Web Client، Web Browser یا به اختصار Browser هم مشهور است.

ب) HTTP Server : که به Web Server نیز معروف است.

کاربران نرم‌افزار HTTP Client را (مانند IE، Netscape، Fire Fox و ...) اجرا کرده و درخواست دسترسی به اطلاعات یا حتی اجرای برنامه را به سرویس‌دهنده ارسال می‌کنند (HTTP Request). سرویس‌دهنده این درخواست را بررسی کرده و پس از آماده کردن پاسخ، آن‌ها را در قالب خاصی معروف به Web Page به سمت سرویس‌گیرنده ارسال می‌کند. سرویس گیرنده این صفحات را دریافت کرده و با قالب مناسب به کاربر نشان می‌دهد. همان‌طور که می‌دانیم زبان مورد استفاده در صفحات وب اکثراً HTML یا XML است.

فعالیت عملی

آشنایی با سرویس HTTP

هر چند اغلب هنرجویان و حتی کاربران عادی با این سرویس آشنا هستند اما برای حفظ انسجام مطالب بیان شده، هنرآموز درس می‌تواند Web Server را به همراه یک Web Page بسیار ساده از قبل آماده کرده و کاربران با HTTP Client (ترجیحاً IE) به آن دسترسی پیدا کنند. شایان ذکر است که Web Server در مایکروسافت، بخشی از بستهٔ IIS است.

۱ـ Hyper Text Transfer Protocol

۳ـ۳ـ۶ـ POP3[1] و SMTP[2] : هر دو سرویس فوق برای EMail استفاده می‌شوند. کاربر برای تهیه، ارسال، دریافت و خواندن نامه از نرم‌افزار Mail Client استفاده می‌کند. دو مورد از نرم‌افزارهای معروف که به عنوان Mail Client در مایکروسافت استفاده می‌شوند عبارتند از Outlook Express و Outlook ـ Microsoft (به اختصار OE و MO). پس از اجرای Mail Client و پیکربندی آن، کاربر می‌تواند متن نامه خود را تایپ کرده، در صورت نیاز عکس یا پرونده‌های دیگری را به آن پیوست کرده[3] و پس از تعیین گیرنده و موضوع نامه[4] آن را ارسال کند. به محض فشردن کلید Send تمامی محتوای نامه به همراه ضمائم پیوست، با پروتکل SMTP به سمت Mail Server ارسال می‌شود. Mail Server پس از دریافت‌نامه از سوی کاربر به بررسی آدرس گیرنده می‌پردازد و اگر گیرنده شخصی خارج از حوزهٔ پستی خودش باشد آن‌را با SMTP به Mail Server حوزه گیرنده تحویل می‌دهد. Mail Server گیرنده پس از دریافت نامه از Mail Server فرستنده آن‌را در پوشه مناسب که در واقع صندوق‌پستی شخص گیرنده است ذخیره می‌کند و فرایند ارسال‌نامه به اتمام می‌رسد. حال از اینجا به بعد شخص گیرنده خودش وظیفه دارد که در صورت تمایل به Mail Server حوزه خود متصل شده و با پروتکل POP3 نامه‌هایش را از سرویس‌دهنده دریافت کرده و در صندوق پستی محلی واقع در رایانه خودش منتقل کند. همان‌طور که می‌بینیم فرایند فوق تا حدی با روش عمومی اداره پست در ارسال‌نامه متفاوت است چرا که پستچی نامه را تا دم در منزل می‌آورد اما در Email ما باید خودمان به ادارهٔ پست (Mail Server) مراجعه و پس از نشان دادن مجوز، نامه را از صندوق پستی برداریم.

پژوهش

پروتکل HTTP از آن دسته پروتکل‌هایی است که برای انتقال Email نیز از آن بهره می‌برند. به عنوان مثال می‌توان انتقال نامه از طریق yahoo یا Gmail را نام برد. برای تبادل‌نامه از طریق yahoo چگونه عمل می‌کنیم؟

۱ـ Post Office Protocol (version3)

۲ـ Simple Mail Transfer Protocol

۳ـ Attachment

۴ـ Subject

مطالعه آزاد

۴ــ۳ــ۶ــNNTP[1] : سرویس دسترسی به گروه‌های خبری (News Groups)، به زبان ساده NNTP سرویسی است برای دسترسی به اطلاعاتی که به وسیلهٔ افراد مختلف ارسال شده و مشترکاً مورد استفاده قرار می‌گیرد. این سرویس نیز از دو قسمت تشکیل شده :

الف) NNTP Client : که به News Client نیز معروف است.

ب) NNTP Server : که به News Server نیز مشهور است.

روال کار بدین صورت است که ابتدا به‌وسیلهٔ News Client به یک News Server متصل شده سپس گروه خبری را انتخاب و در آن عضو می‌شویم (Subscribe) پس از عضویت در گروه خبری، اطلاعات و اخبار متنوع در زمینه موردنظر از Server به سرویس گیرنده انتقال پیدا کرده و اعضا در صورت تمایل می‌توانند نظرات یا پرسش‌های خود را در مورد خبرها ارسال کنند یا خبر و سؤال جدیدی را به سرویس‌دهنده ارسال کنند. در مایکروسافت، نرم‌افزاری که به عنوان News Client مورد استفاده قرار می‌گیرد همان Mail Client است یعنی Outlook Express منتهی به‌جای پیکربندی برای Mail Account باید آن‌را برای News Account تنظیم کنیم.

۵ــ۳ــ۶ــ Telnet[2] : ترمینال عبارت است از وسیله‌ای که برای ارسال و دریافت اطلاعات استفاده می‌شود (مثلاً یک Keyboard و یک Monitor) اما هیچ‌گونه پردازشی روی اطلاعات در آن صورت نمی‌گیرد و اصولاً پردازش اطلاعات در سیستم مرکزی (Central System) انجام می‌شود.

مطالعه آزاد

منظور از سیستم مرکزی، مجموعه‌ای است دارای توانایی برای پردازش اطلاعات و اجرای دستورالعمل‌ها یعنی مجموعه‌ای که شامل CPU، RAM، HDD و ... است. سیستم مرکزی می‌تواند یک رایانه شخصی باشد، می‌تواند یک Mini Computer، Main Frame یا یک Super Computer باشد. سیستم مرکزی حتی می‌تواند یکی از تجهیزات فعال مورد استفاده در شبکه باشد مثلاً یک Router، سوئیچ یا Hub. البته

۱ــ Network News Transfer Protocol

۲ــ Tele Network

بدیهی است که در مورد اخیر (تجهیزات شبکه) هدف ما از اتصال ترمینال به مثلاً یک روتر، پردازش اطلاعات و اجرای Application برای کاربر نیست بلکه هدف پیکربندی یا کنترل آن است.

مثال ۱ : در برخی از بانک‌ها، جلوی هر کارمند باجه، فقط یک صفحه نمایش، صفحه کلید و یک چاپگر کوچک قرار دارد اما خبری از کیس و ملحقات داخلی آن نیست! چرا؟ پردازش کجا انجام می‌شود؟ تجهیزات جلوی کارمند فقط به عنوان ترمینال استفاده می‌شوند. پس سیستم مرکزی کجاست؟ اگر دقت کنیم در گوشه‌ای از بانک یک رایانه شخصی قرار دارد که به عنوان سرویس‌دهنده عمل کرده و نقش سیستم مرکزی را بازی می‌کند و در واقع محل اجرای نرم‌افزارهای بانکی و پردازش اطلاعات است. ترمینال‌ها از طریق سخت‌افزار و کنترلر مناسب به آن متصل می‌شوند.

راه‌های متنوعی برای اتصال ترمینال‌ها به سیستم مرکزی وجود دارد، که عبارتنداز :

Serial Port

USB

Network

از نظر نحوهٔ نمایش اطلاعات، ترمینال‌ها به دو دسته کلی تقسیم می‌شوند :

الف) ترمینال‌های Text : فقط به صورت «متنی» اطلاعات را نمایش می‌دهند.

ب) ترمینال‌های Graphic : علاوه بر «متن»، دارای توانایی ترسیم اشکال گرافیکی با رنگ‌های متنوع نیز هستند.

تعریف Terminal Emulator : ممکن است در شبکه‌ای به‌جای ترمینال از یک رایانه شخصی استفاده کنند. مزیت استفاده از رایانه شخصی به‌جای ترمینال آن است که این رایانه خود دارای توانایی پردازش اطلاعات است بنابراین می‌توان علاوه بر کاربرد آن به عنوان یک ترمینال، نرم‌افزارهای متنوع دیگری را نیز مستقیماً روی آن اجرا کرد. اما در صورت نیاز چگونه می‌توان رایانه شخصی را تبدیل به یک ترمینال برای اتصال به سیستم مرکزی کرد؟ پاسخ بسیار ساده است : کافی است نرم‌افزار مناسب را روی آن اجرا کرد. این نرم‌افزارها در حالت کلی به «شبیه‌ساز ترمینال» یا «مقلد ترمینال» یا به زبان

انگلیسی Terminal Emulator مشهورند و همچون ترمینال‌ها دارای دو دستهٔ کلی Text و Graphic در زمینهٔ نحوهٔ نمایش اطلاعاتند. طریقه اتصال سخت‌افزاری یک رایانه شخصی که به عنوان ترمینال استفاده می‌شود با Central System همچون نحوهٔ ارتباط ترمینال‌هاست .

نرم‌افزارهای Terminal Emulator که اطلاعات را به صورت Text نشان می‌دهند بسیار متنوعند، از آن جمله می‌توان به Term ۹۵، PC Anywhere ، Kermit ، Closeup و Hyper Terminal اشاره کرد. می‌دانیم که Hyper_Terminal تحت Windows اجرا می‌شود اما در واقع فقط به‌صورت Text می‌تواند اطلاعات را نمایش دهد.

با توجه به مقدمهٔ فوق می‌توانیم Telnet را که از سرویس‌های TCP/IP است تعریف کنیم.

اگر راه ارتباطی یک رایانه شخصی با Central System از طریق شبکه باشد و پروتکل مورد استفاده نیز TCP/IP باشد در آن صورت Telnet عبارت است از یک سرویس Terminal Emulator که اطلاعات را به صورت Text نشان می‌دهد.

همچون دیگر سرویس‌ها، Telnet نیز از دو بخش تشکیل شده :

الف) Telnet Client : که روی رایانه شخصی اجرا می‌شود و آن‌را تبدیل به ترمینال می‌کند (در مایکروسافت : Telnet.exe).

ب) Telnet Server : یا Telnet Doemon یا به اختصار telnetd که روی Central System اجرا شده و اطلاعات را از ترمینال Telnet سرویس گیرنده دریافت و پس از پردازش به‌وسیلهٔ سیستم مرکزی، برای ترمینال (کلاینت) Client ارسال می‌کند.

فعالیت عملی **آشنایی با سرویس Telnet**

ابتدا باید سیستم مرکزی را انتخاب کرد. (مثلاً یک رایانه با سیستم عامل UNIX، یک رایانه با سیستم‌عامل NT، یک Router، یک Wireless Access Point، ...) سپس باید مطمئن شد که سرویس Telnet Server روی آن نصب و فعال است. (تا این جای کار باید به وسیلهٔ هنرآموز درس انجام شود.). سپس هنرجویان نرم‌افزار Telnet Client را روی رایانه‌های خود اجرا کرده (Telnet.exe) و بدین ترتیب رایانه آن‌ها

تبدیل به یک ترمینال می‌شود. قدم بعدی آن است که به سیستم مرکزی متصل شده و با آن به تبادل اطلاعات پرداخت. (اگر به اینترنت متصل هستید، می‌توانید سایت‌های بسیاری را پیدا کنید که با telnet می‌توان با آن‌ها ارتباط گرفت منتهی باید مجوز ورود را هم در صورت درخواست وارد کنید. برخی از سایت‌ها اجازه می‌دهند با کاربر guest به سیستم Login کنیم. به عنوان مثال می‌توانید از طریق Run فرمان زیر را تایپ کرده و نتیجه را ببینید، (کاربر را guest وارد کنید) :

telnet victoria.tc.ca

۶ــ۳ــ۶ــ RDP[1] : همانند Telnet است با این تفاوت که گرافیکی است. در مایکروسافت، برنامه Remote Desktop از سرویس RDP استفاده کرده و رایانه شخصی را تبدیل به یک ترمینال گرافیکی می‌کند.

همچون دیگر سرویس‌های TCP/IP، RDP نیز از دو بخش تشکیل شده :

الف) RDP Client : که به Terminal Client نیز معروف بوده و در مایکروسافت، همان برنامه Remote–Desktop است (mstsc.exe)[2].

ب) RDP Server : که به Terminal Server نیز مشهور بوده و در مایکروسافت، همان سرویس Remote–Desktop است که از طریق System Properties فعال می‌شود. البته در ویندوزهای سرور 2000 یا 2003 یک نسخه کامل‌تر از این سرویس به نام Terminal Service از طریق زیر نصب و فعال می‌شود :

Add/Remove Programs → Windows Components → Terminal Service

فعالیت عملی

آشنایی با سرویس RDP

روی رایانه سرویس‌دهنده، سرویس Remote Desktop server را به کمک هنرآموز درس فعال کرده، سپس روی سرویس گیرنده برنامه Remote Desktop Client را اجرا کنید (دستور Mstsc.exe)

۱ــ Remote Desktop Protocol

۲ــ شکل کلی این دستور در فصل ۱۴ آمده است.

حال به سرویس‌دهنده متصل شده با نام Administrator وارد شده و میز کار مربوط به سرویس‌دهنده را در اختیار بگیرید.

۷ـ۳ـ ۶ ـ SNMP[1] : یکی از مسایل مهمی که هر Administrator در شبکه‌های متوسط و بزرگ با آن مواجه است، مدیریت شبکه به شکل جامع و حتی‌المقدور یکپارچه است.

مثال : برای مدیریت از راه دور یک رایانه با سیستم عامل ویندوز اکس پی، علاوه بر بهره‌گیری از Remote Desktop، می‌توان از برنامه Computer Management نیز استفاده کرد. برای این کار با Administrator وارد سیستم شده، برنامه مذکور را اجرا کنید(برای این کار روی My Computer کلیک راست و گزینه Computer Management را انتخاب و پس از اجرای آن، Connect to another Computer را انتخاب کنید). سپس با تایپ کردن نام یا آدرس رایانه مقصد به آن متصل شده و از این به بعد می‌توانیم آن‌را مدیریت کنیم. برای عملکرد صحیح لازم است تا password مربوط به Administrator روی هر دو رایانه مبدأ و مقصد دقیقاً یکسان باشد.

در مثال فوق ارتباط ما از طریق سرویس‌های خاصی که مایکروسافت تعبیه کرده برقرار شده است.

نتیجه‌گیری : برای مدیریت راه‌های گوناگونی وجود دارد که بستگی به تجهیزات، سیستم عامل، پروتکل مورد استفاده و پارامترهای دیگر دارد اما آیا راه یکپارچه‌ای نیز هست؟ پاسخ مثبت بوده و راه‌حل، استفاده از SNMP است.

SNMP از دو بخش تشکیل شده :

الف) SNMP Agent : که مسئول جمع‌آوری اطلاعات بوده و باید روی هر سیستم، تک به تک فعال شود.

ب) SNMP Viewer : که به SNMP Manager نیز مشهور بوده و مسئول گردآوری و تجزیه و تحلیل اطلاعات جمع‌آوری شده به وسیلهٔ کلیه Agentها در تمامی شبکه است.

هر سیستمی که بخواهد با SNMP مدیریت شود باید Agent را روی آن نصب و فعال کرد. کار Agent آن است که اطلاعات مدیریتی را جمع‌آوری کرده و آنها را در یک بانک اطلاعاتی محلی (Local Database) معروف به MIB[2] ذخیره می‌کند. به عنوان مثال اگر در یک شبکه ۱۰۰۰ سیستم داریم که می‌خواهیم آنها را با SNMP مدیریت کنیم باید روی همگی آنها Agent را فعال کنیم. در

۱ـ Simple Network Management Protocol

۲ـ Management Information Base

ویندوز Agent از طریق زیر نصب و فعال می‌شود :

Add/Remove Programs → Windows Components → Management& Monitoring Tools

(وارد قسمت Details شده و فقط Simple Network Management Protocol را انتخاب کنید.)

برای پیکربندی آن نیز باید از طریق سرویس‌های ویندوز وارد عمل شد (در صورت نیاز با کمک هنرآموز درس انجام شود).

و اما اطلاعات جمع‌آوری شده به وسیلهٔ Agent را چگونه گردآوری و تجزیه تحلیل کنیم؟ کافی است روی یک رایانه مثلاً متعلق به مدیر شبکه، نرم‌افزار SNMP Manager را نصب کنیم. یکی از نرم‌افزارهای مناسب در این زمینه Solarwinds است (www.solarwinds.net). پس از پیکربندی نرم‌افزار می‌توان به سایر سیستم‌های مجهز به Agent در شبکه متصل شده و اطلاعات جمع‌آوری شده در MIB را گردآوری و تجزیه و تحلیل کرد.

فعالیت عملی

آشنایی با سرویس SNMP

با توجه به این‌که مدیریت شبکه نیاز به تجربه و دانستن مقدمات پیشرفته‌تری دارد لذا در این مرحله نیازی به آشنایی عملی با SNMP نیست، با این حال در صورت تمایل و داشتن فرصت کافی، هنرآموز محترم می‌تواند، خود Agent و Viewer را نصب و پیکربندی کرده و نحوهٔ مدیریت شبکه را در حالات بسیار ساده به هنرجویان نشان دهد.

۸ــ۳ــ۶ــ SNTP(NTP)[1] : ساعت دقیق در شبکه‌هایی که اطلاعات مالی، پرسنلی، مدیریت پروژه و ... در آن‌ها نگهداری می‌شود بسیار مهم است. در یک شبکه چگونه می‌توان مطمئن شد که ساعت در کلیه سیستم‌ها به‌طور صحیح تنظیم شده است؟

در این‌جا NTP به کمک آمده و زمان را بین سرویس گیرنده و سرویس دهنده یکسان (Synchronize) می‌کند. در واقع NTP از دو بخش تشکیل شده :

الف) NTP Client : که به Time Client هم معروف است.

ب) NTP Server : که به آن Time Server نیز می‌گویند.

پس از پیکربندی، NTP Client در زمان‌های مشخص با NTP Server ارتباط برقرار کرده و

۱ــ Simple Network Time Protocol

ساعت خود را با ساعت سرویس‌دهنده تنظیم می‌کند و بدین ترتیب ساعت تمام رایانه‌های شبکه دقیقاً یکسان شده و نیازی به تنظیم دستی نیست.

بد نیست بدانیم که Time Server خود می‌تواند یک Time Client باشد برای یک سرویس‌دهنده دیگر. خوشبختانه در اینترنت، مراجع دقیقی به عنوان NTP Server وجود دارند (معروف به ساعت اتمی) که سرویس‌دهنده‌های محلی می‌توانند زمان دقیق را از آن‌ها دریافت کنند به عنوان مثال می‌توان به time.nist.gov اشاره کرد.

فعالیت عملی

آشنایی با سرویس NTP

با کاربر Administrator وارد ویندوز اکس پی شده و روی نشانه Time واقع در سمت راست Taskbar دوبار ــ کلیک کنید.

سومین قسمت از صفحه Time با نام Internet Time را باز کنید. لیستی از سرویس‌دهنده‌های مرجع را می‌بینید که می‌توانید یکی از آن‌ها را انتخاب و ساعت خود را با آن Update کنید. در شبکه‌های متوسط و بزرگ نیز می‌توان یک سرور 2000 یا 2003 را به عنوان Time Server در نظر گرفته و سپس کلیه سیستم‌های دیگر را با آن به هنگام (Update) کرد.

البته این امر در صورتی با موفقیت انجام می‌شود که :

۱ــ سرویسی معروف به Windows Time در لیست سرویس‌های ویندوز Start باشد.

۲ــ Date (روز و ماه و سال) از قبل صحیح باشد.

۳ــ Time Zone را Tehran انتخاب کرده باشیم.

۴ــ اختلاف ساعت ما با ساعت واقعی بیش از ۱۲ ساعت نباشد.

۵ــ در بین راه یا حتی روی ماشین خودمان UDP Port 123 باز باشد.

۴ــ۶ــ آشنایی با مفهوم Host در پروتکل TCP/IP

Host را در فارسی به «میزبان» ترجمه می‌کنند. حال باید دید که «میزبان TCP/IP» به چه معنی است.

تعریف : به هر سیستم در شبکه که از TCP/IP برای ارتباط استفاده کند اصطلاحاً یک TCP/IP Host یا «میزبان TCP/IP» می‌گوییم.

مثال۱ : کلیه رایانه‌های شخصی در یک شبکه که پروتکل TCP/IP روی آن‌ها تنظیم و فعال

شده اعم از این‌که سرویس گیرنده باشند یا سرویس دهنده، هر کدام برای خود یک Host مستقل به حساب می‌آیند.

مثال۲ : یک روتر را می‌توان یک TCP/IP Host بشمار آورد، به دلیل این که می‌توان TCP/IP را روی آن پیکربندی و فعال کرد و روتر را از طریق آن کنترل کرد.

مثال۳ : برخی از سوئیچ های حرفه‌ای توانایی پیکربندی و کنترل خود را از طریق TCP/IP به مدیر شبکه می‌دهند، پس این سوئیچ‌ها نیز TCP/IP Host هستند.

مثال ۴ : برخی ازUPSها توانایی اتصال مستقیم به شبکه را دارند. می‌توان از طریق یک رایانه شخصی و پروتکل TCP/IP آن‌ها را کنترل کرد. چنین UPSهایی در واقع مثال دیگری از TCP/IP Host هستند.

مثال ۵ : چاپگرهایی هستند که مستقیماً به شبکه متصل شده و رایانه‌های شخصی می‌توانند کارهای چاپی خود را از طریق TCP/IP به آن‌ها ارسال کنند، پس این چاپگرها نیز بیانگر TCP/IP Host هستند.

هر Host در TCP/IP دارای دو مشخصه اصلی و بارز است. به عبارت دیگر هر Host را می‌توان با دو خصوصیت از بقیه Hostها تفکیک کرد. این دو مشخصه عبارتند از :

الف) نام (Host Name = TCP/IP Name)

ب) آدرس (Host Address = IP Address)

نکته : اگر بخواهیم اصل ماجرا را در نظر بگیریم، آدرس در اولویت اول قرار داشته و هر Host باید حداقل یک آدرس منحصر به‌فرد داشته باشد. مشخصه «نام» برای سهولت در کار کاربران بوده اما برای پروتکل TCP/IP چندان مهم نیست. در واقع هنگامی که یک کاربر برای برقراری ارتباط با یک TCP/IP Host از «نام» استفاده می‌کند (مثلاً http: // www.yahoo.com) پروتکل TCP/IP به زحمت افتاده و باید آدرس مربوط به نام را پیدا کند چون مهم برای او IP Address است. به عبارت دیگر پروتکل با مکانیزم‌هایی که بعداً مورد بحث قرار می‌گیرد ابتدا اسم را به IP تبدیل کرده (مثلاً آدرس http: // www.sanjesh.org می‌شود ۹۲.۲۴۲.۱۹۵.۱) و بعد ارتباط با سایت آغاز می‌شود.

۱ـ۴ـ۶ـ Host Name : گفتیم که برای سهولت بیشتر کاربران، برای اکثر «میزبان‌های مهم» (Host) یک یا چند نام انتخاب می‌شود. بدیهی است که این نام‌ها باید از قوانینی تبعیت کرده و

ضمناً مورد تأیید «مراکز ثبت اسامی» نیز قرار بگیرند، به زبان دیگر باید اسم را ثبت (Register) کرد. چنان‌چه اسم یک Host ثبت نشود در آن‌صورت استفاده از نام معمولاً محدود به کاربردهای داخلی شده و اغلب کاربران «خارج از شبکه داخلی» نام را نمی‌شناسند چرا که رسماً ثبت نشده است.

مثال : فرض کنید کسی در محدوده خانوادگی خود یا میان دوستان وآشنایان نام «نرگس» را برای خود انتخاب کند اما نام شناسنامه‌ای وی «فرزانه» باشد. طبیعی است هنگامی که می‌خواهد خود را رسماً به همه معرفی کند «اسم شناسنامه‌ای» خودش که در اداره ثبت احوال درج شده به کار می‌برد زیرا همگان «اداره ثبت احوال» را به عنوان «مرکز معتبر ثبت اسامی» قبول دارند. اما افراد خانواده وی یا دوستان نزدیک وی می‌توانند با نام مستعار او را صدا بزنند.

اکنون نگاهی دقیق‌تر به قالب اسامی داشته باشیم، به‌طورکلی می‌توانیم دو قالب را برای نامگذاری تصور کنیم. با دقت به مثال‌های زیر موضوع روشن می‌شود :

قالب اول : هر یک از اسامی زیر به عنوان یک Host Name می‌تواند در پروتکل TCP/IP استفاده شود :

Narges	Reza	Server22	Client80	PC1
C2	C1	Palang	Moon	Star

قالب دوم :

www.tamin.org	7)	www.yahoo.com	(1
www.sharif.edu	8)	mail.yahoo.com	(2
sina.sharif.ac.ir	9)	www.neda.net.ir	(3
www.itrc.ac.ir	10)	ftp.dlink.com	(4
time.nist.gov	11)	ftp.microsoft.com	(5
www.dci.ir	12)	www.sanjesh.org	(6

پرسش

تفاوت بین قالب اول و دوم در چیست؟به‌روشنی پیداست که قالب دوم کامل‌تر است،اصطلاحاً اگراسمی در قالب اول باشد به آن اسم مستعار Alias یا Unqualified و اگر در قالب دوم باشد به آن FQDN = Fully Qualified Domain Name می‌گویند.

معمولاً اسامی قالب اول در محدودهٔ داخلی شبکه‌ها استفاده شده، نیازی به ثبت ندارند اما اسامی قالب دوم عمدتاً ثبت شده و در این صورت چه در محدوده داخلی و چه افراد خارج از شبکه داخلی می‌توانند از آن‌ها برای مراجعه به Host استفاده کنند (همان‌طور که تأکید شد، اسامی اعم از قالب اول یا دوم در ابتدای کار به‌وسیلهٔ TCP/IP به آدرس تبدیل می‌شوند).

اگر بخواهیم بگوییم یک اسم در قالب دوم (FQDN) معمولاً از چه قسمت‌هایی تشکیل می‌شود؟در جواب می‌توان گفت به ترتیب از سمت چپ :

الف) نام یا سرویسی که Host ارائه می‌دهد یا نقشی که Host بازی می‌کند[1].

مثال :

www=	Web Server	mail =	Mail server
ftp =	FTP Server	time =	Time Server
news =	News (NNTP) Server		

ب) نام شرکت، سازمان، مجموعه یا شخصی که Host بدان تعلق دارد. (Company Name)

مثال :

yahoo, google, sun, microsoft, IRIB, Bank_Keshavarzi, . . .

ج) حوزهٔ فعالیت میزبان. (Activities)

مثال :

com, net, org, gov, mil, edu, ac, info, int, biz, tv, ws, . . .

د) وابستگی منطقه‌ای و محلی اعم از فرهنگی، اجتماعی، ... یا زبان استفاده شده در سایت. (Locality)

مثال :

ir = Iran	tr = Turkey	uk = United Kingdom	ca = Canada
iq = Iraq	tw = Taiwan	us = United States	fr = France

نکته ۱ : برای دیدن لیست کاملی از کدهای دو حرفی مربوط به کشورهای مختلف کافی است در google عبارت زیر را جستجو کنید : "Country codes" یا مستقیماً به سایت www.iana.org مراجعه کنید.

۱ـ Host Role or Host Service

نکته ۱ : با توجه به مثال‌های قالب دوم ممکن است برخی از اجزای یاد شده در FQDN موجود نباشد مثلاً در اکثر آن‌ها «بند د» (Locality) دیده نمی‌شود یا یکی از اسامی دانشگاه شریف با sina شروع می‌شود و «سینا» بیانگر سرویس نیست بلکه فقط یک اسم است. در مثال دیگری مربوط به سایت شرکت دیتا www.dci.ir می‌بینیم که حوزهٔ فعالیت در آن دیده نمی‌شود اما به هر حال FQDN هر چه‌قدر هم که ناقص باشد، اجزای آن باید از چپ به راست ترتیب یاد شده رارعایت کنند و نباید آن‌ها را جابه‌جا کرد مثلاً www.com.yahoo صحیح نیست.

به این مثال‌ها توجه کنید :

www.microsoft.com ↓ Domain

www.neda.net.ir ↓ Domain

در یک FQDN چنانچه بخش ابتدایی سمت چپ را که (بیانگر نام سرویس است) کنار بگذاریم، به مجموع بقیه قسمت‌ها Domain گفته می‌شود که شامل نام شرکت، حوزه فعالیت و کشور می‌شود.

بنابراین FQDN به‌طورکلی از دو بخش تشکیل شده :

جدول ۱ــ۶

FQDN =	Service Name	+	Domain Name
	www		microsoft. com
	time		dlink.com
	msnews		microsoft. com

به زیرمجموعه‌های یک Domain اصطلاحاً SubDomain می‌گویند. در عمل معمولاً از SubDomain برای نشان دادن شرکت‌ها، زیرگروه‌ها یا ساختارهای فرعی در یک مجموعهٔ بزرگ استفاده می‌شود.

مثال : یک شرکت بزرگ رایانه‌ای را در نظر بگیرید که علاوه بر شرکت اصلی، از سه شرکت زیرمجموعه برای فعالیت‌های سخت‌افزار، نرم‌افزار و شبکه استفاده می‌کند. برای شرکت اصلی، یک

Domain به‌نام a.net را در نظر گرفته آن‌را ثبت می‌کنیم. حال با توجه به گستردگی فعالیت‌های شرکت بزرگ‌رایانه‌ای و طبیعتاً شرکت‌های زیرمجموعه، بد نیست که برای هر کدام از زیرمجموعه‌ها نیز یک domain در نظر بگیریم :

برای شرکت سخت‌افزار : hardware.a.net

برای شرکت نرم‌افزار : software.a.net

برای شرکت شبکه : network.a.net

هر یک از domainهای فوق را اصطلاحاً یک SubDomain از a.net می‌نامیم.

اگر شرکت اصلی و بخش‌های تابعه، هر یک برای خود Web_Server داشته باشند در آن صورت دارای اسامی زیر خواهند بود :

وب سرور شرکت اصلی	www.a.net
وب سرور شرکت سخت‌افزار	www.hardware.a.net
وب سرور شرکت نرم‌افزار	www.software.a.net
وب سرور شرکت شبکه	www.network.a.net

در رایانه‌هایی که از سیستم‌عامل‌های خانوادهٔ مایکروسافت بهره برده و در ضمن پروتکل TCP/IP روی آن‌ها فعال می‌شود، دو اسم مدنظر قرار می‌گیرد :

الف) هنگام نصب OS یک اسم حداکثر ۱۵ کاراکتری به رایانه داده می‌شود که باید در محدوده شبکه داخلی منحصر به‌فرد بوده و تکراری نباشد. این اسم به Computer Name یا NetBIOS Name معروف است (لزومی ندارد که حتماً پروتکل NetBIOS روی رایانه نصب باشد، در هر صورت به آن NetBIOS Name می‌گویند). می‌دانیم که در سیستم‌عامل XP یا 2003 برای تغییر NetBIOS Name از System Properties وارد عمل شده، قسمت Computer Name را انتخاب و پس از فشردن کلید Change، نام رایانه را تغییر داده و تأیید OK می‌زنیم.

ب) TCP/IP Name که همان Host Name در پروتکل TCP/IP بوده و به Full Computer Name نیز معروف است و ممکن است قالب اول یا دوم باشد. به صورت پیش‌فرض در رایانه‌هایی که عضو Work Group باشند TCP/IP Name دقیقاً برابر با NetBIOS Name است از طرفی چون NetBIOS Name عمدتاً ساده و تک قسمتی بوده لذا TCP/IP Name هم به صورت تک قسمتی برابر با آن می‌شود یعنی در قالب اول است.

اگر رایانه به عضویت Domain در Active Directory درآید آنگاه TCP/IP Name به صورت زیر درمی‌آید :

TCP/IP Name = NetBIOS Name + Active Directory Domain Name

یعنی TCP/IP Name در قالب دوم می‌شود.

فعالیت عملی

هر گروه از هنرجویان که یک دستگاه رایانه مستقل در اختیار دارند به‌دلخواه یک Domain Name انتخاب کرده سپس Full Computer Name را در سیستم خود تغییر دهند.

برای تغییر Domain در TCP/IP Name از طریق System Properties وارد عمل شده و قسمت Computer Name را انتخاب و پس از فشردن کلید Change و متعاقب آن کلید More، نام Domain را در قسمت Primary DNS Suffix for this computer وارد کرده و تأیید (OK) کنید. با تأیید مجدد (OK)، سیستم‌عامل از شما می‌خواهد تا رایانه را Restart کنید. پس از Restart، وارد Command Prompt شده و با اجرای دستور ipconfig/all و بررسی خطوط اولیه، نتیجه کار خود را بررسی کنید.

البته همان‌طور که گفته شده اسامی TCP/IP در قالب دوم تا هنگامی که رسماً در «مراکز شناخته شده ثبت اسامی» یا به زبان فنی (DNS Server) ثبت نشوند نمی‌توانند مورد استفاده بقیه قرار گیرند، لذا فعالیت عملی فوق صرفاً برای آشنایی بیشتر هنرجو با Full Computer Name و مفهوم FQDN بوده، توصیه می‌شود که حتماً انجام شود.

در این قسمت به توضیحات پیرامون Host Name خاتمه داده و مبحث IP Address را آغاز می‌کنیم :

۲ـ۴ـ۶ـ Host Address = IP Address : در پروتکل TCP/IP دو نوع آدرس برای IP وجود دارد :

الف) آدرس IP نسخه ۴ که به آن IPv4 می‌گویند.

ب) آدرس IP نسخه ۶ که به آن IPv6 می‌گویند.

در این کتاب ما به تشریح کامل IPv4 خواهیم پرداخت (ویندوز XP فقط از IPv4 پشتیبانی می‌کند که به صورت IP نمایش داده می‌شود)

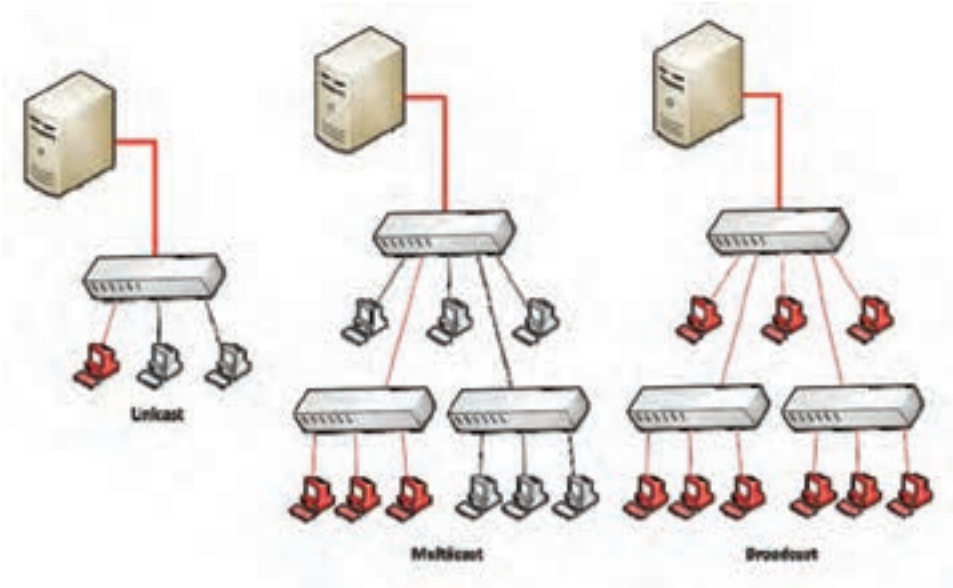
استانداردهای اینترنت برای انواع آدرس‌های IPv4 عبارتند از :

الف) Unicast : برای یک رابط شبکه در یک زیر شبکه اختصاص می‌یابد (یک مخاطب) برای ارتباط یک به یک استفاده می‌شود مانند آدرس یک منزل در شهر به عنوان یک گیرنده.

ب) Multicast : به یک یا چند رابط شبکه واقع در زیرشبکه‌های مختلف اختصاص می‌یابد(چند مخاطب) و برای ارتباط یک به چند استفاده می‌شود.

ج) Broadcast : به تمام رابط‌های شبکه در یک زیر شبکه اختصاص داده می‌شود (برای تمام مخاطب‌های یک زیر شبکه) و برای ارتباط یک به همه در یک زیر شبکه مورد استفاده قرار می‌گیرد.

شکل ۱ــ۶ مقایسه گرافیکی بین انواع ارسال در شبکه را نشان می‌دهد رایانه‌هایی که با رنگ قرمز مشخص شده اند به عنوان دریافت کننده (مخاطب) می‌باشند :



شکل ۱ــ۶ــ استانداردهای اینترنت

۳ــ۴ــ۶ــ آدرس‌های Unicast در IPv4 : آدرس‌های Unicast در IPv4 محل قرار گرفتن مخاطب را در شبکه تعیین می‌کنند، مانند آدرس منزل یک شخص در یک شهر. بنابراین آدرس‌های Unicast در IPv4 باید در سطح جهان منحصر به فرد بوده و دارای قالب یکسان باشد.

(البته می‌توان برای چند شبکه مستقل که قرار نیست با هم در ارتباط باشند آدرس‌های IP یکسانی در نظر گرفت).

هر آدرس IPv4 دارای دو بخش پیشوند زیر شبکه و ID میزبان به صورت زیر می‌باشد :

IPv4 Address = Subnet prefix + host ID

Subnet prefix (پیشوند زیر شبکه) به عنوان شناسه شبکه[1] یا آدرس شبکه[2] شناخته می‌شود و تمام گره‌های شبکه در یک زیر شبکه باید دارای Subnet prefix یکسانی بوده. و پیشوند زیر شبکه باید در کل شبکه‌های TCP/IP منحصر به فرد باشد با توجه به مطالب فوق می‌توان IPv4 Address = Subnet prefix + host ID را به صورت زیر نیز تعریف نمود :

IPv4 Address = Network ID + Host ID

Host ID (ID میزبان) غالباً به عنوان آدرس میزبان[3] شناخته می‌شود و برای شناسایی گره‌ها در زیر شبکه به کار می‌رود. ID میزبان نیز باید در یک زیر شبکه منحصر به فرد باشد. می‌توان به جای Host ID از Node ID نیز استفاده نمود.

IP Address در مجموعه یک عدد ۳۲ بیتی یا ۴ بایتی است که به فرم w.x.y.z تنظیم می‌شود. به طوری که ممکن است از ۴ بایت ممکن یک تا ۳ بایت برای پیشوند زیر شبکه و یا یک تا ۳ بایت برای ID میزبان در نظر گرفته شود.

۴ـ۴ـ۶ـ کلاس‌های آدرس در IPv4 : آدرس‌های IPv4 دارای کلاس‌های مختلفی است که میزان بیت یا بایت اختصاص یافته به پیشوند زیر شبکه و Host ID را مشخص می‌کند. این کلاس‌ها همچنین تعداد شبکه‌ها و تعداد میزبان‌ها را نیز تعیین می‌کنند. به طور کلی پنج نوع کلاس در IPv4 داریم که با نام‌های کلاس A، B، C، D و E شناخته می‌شود. کلاس A ، B و C برای Unicast می‌باشد . کلاس D برای Multicast رزرو شده و کلاس E نیز برای کارهای آزمایشگاهی رزرو شده است.

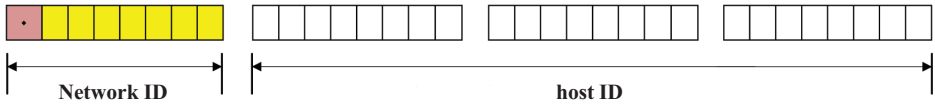
الف) کلاس A : برای شبکه‌هایی که دارای میزبان‌های خیلی زیاد هستند مورد استفاده قرار می‌گیرد، به طوری که ۸ بیت اول برای پیشوند زیر شبکه و ۲۴ بیت باقیمانده برای میزبان مورد استفاده قرار می‌گیرد قالب آدرس دهی در کلاس A به صورت زیر است :

۱ـ Network identifier

۲ـ Network Address

۳ـ Host Address

Network.host.host.host



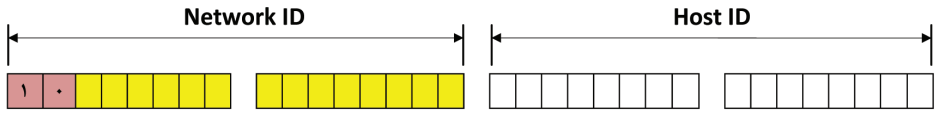
شکل ۲ــ۶ــ کلاس آدرس A

کلاس A تا ۱۶۷۷۷۲۱۴ میزبان را می‌تواند آدرس‌دهی کند و بجای هر host در قالب آدرس‌دهی می‌توان از اعداد ۱ تا ۲۵۴ را استفاده نمود. توجه داشته باشید در واقع اعداد اختصاص یافته به هر host در قالب کلی $۲^۸$ یعنی از ۰ تا ۲۵۵ می‌باشد ولی اعداد ۰ و ۲۵۵ در شرایط خاصی استفاده می‌شود.

کلاس A تا ۱۲۶ شبکه را پشتیبانی می‌کند یعنی به جای Network می‌توان از اعداد ۱ تا ۱۲۶ را استفاده نمود. در کلاس A اولین بیت سمت چپ همیشه باید صفر باشد با توجه به صفر بودن اولین بیت سمت چپ پس ما ۷ بیت داریم که می‌توانند ۱ باشند بنابراین $۲^۷-۱$ یعنی ۱۲۷ شبکه خواهیم داشت اما چون عدد ۱۲۷ برای Loop back ذخیره شده است ما فقط می‌توانیم تا عدد ۱۲۶ را برای کلاس A استفاده نماییم.

ب) کلاس B : کلاس B برای شبکه‌های متوسط تا بزرگ مورد استفاده قرار می‌گیرد به طوری که ۱۶ بیت اول برای شبکه و ۱۶ بیت باقیمانده برای میزبان مورد استفاده قرار می‌گیرد. قالب آدرس‌دهی در کلاس B به صورت زیر است :

Network.Network.host.host



شکل ۳ــ۶ــ کلاس آدرس B

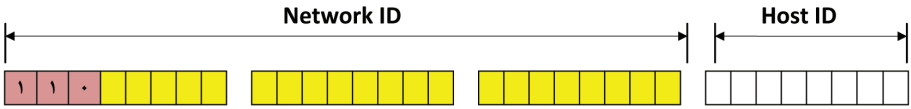
در کلاس B اولین بیت سمت چپ در Network ID همیشه 1 و دومین بیت همیشه 0 می‌باشد یعنی بایت اول در حالت حداکثری برابر 10111111 می‌باشد (یعنی عدد ۱۹۱) پس نتیجه می‌گیریم که در کلاس B اولین بایت یا همان w می‌تواند اعداد ۱۲۸ تا ۱۹۱ باشد

کلاس B تا ۱۶۳۸۴ شبکه را پشتیبانی می‌کند همچنین می‌توان در کلاس B تا ۶۵۵۳۴ میزبان را آدرس دهی نمود.

(۶۵۵۳۴ = ۲ − $۲^{۱۶}$ تمام صفر و تمام یک استفاده نمی‌شود.)

ج) کلاس C : کلاس C برای آدرس دهی شبکه‌های کوچک استفاده می‌شود به طوری که ۲۴ بیت (۳ بایت) اول برای شبکه و ۸ بیت (۱ بایت) باقیمانده برای میزبان مورد استفاده قرار می‌گیرد. قالب آدرس دهی در کلاس C به صورت زیر است :

Network.Network.Network.host



شکل ۴ــ۶ــ کلاس آدرس C

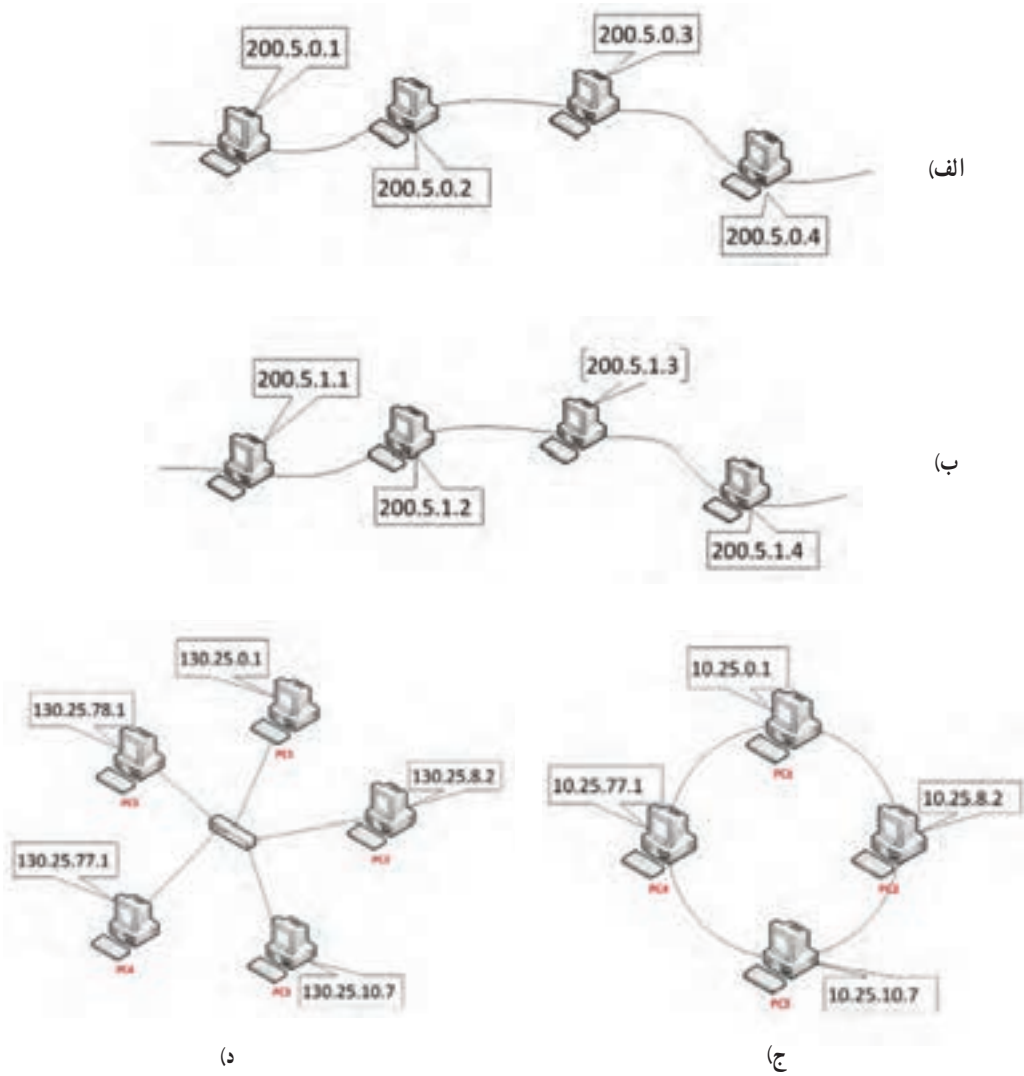
در کلاس C اولین و دومین بیت سمت چپ در Network ID همیشه 1 و سومین بیت همیشه 0 می‌باشد یعنی بایت اول در حالت حداکثری برابر 11011111 می‌باشد (یعنی عدد ۲۲۳) پس نتیجه می‌گیریم که در کلاس C اولین بایت یا همان w می‌تواند اعداد ۱۹۲ تا ۲۲۳ باشد.

کلاس C تا ۲۰۹۷۱۵۲ شبکه را پشتیبانی می‌کند همچنین در این کلاس می‌توان تا ۲۵۴ میزبان را آدرس دهی نمود.

جدول ۱ــ۶ ــ خلاصه کلاس‌های Unicast

نام کلاس	مقدار W	بخش شبکه	بخش میزبان	آدرس‌های شبکه	آدرس‌های میزبان
A	۱ــ۱۲۶	w	x.y.z	۱۲۶	۱۶۲۷۷۲۱۴
B	۱۲۸ــ۱۹۱	w.x	y.z	۱۶۳۸۴	۶۵۵۳۴
C	۱۹۲ــ۲۲۳	w.x.y	z	۲۰۹۷۱۵۲	۲۵۴

به شکل ۵ــ۶ توجه کنید :



شکل ۵ــ۶

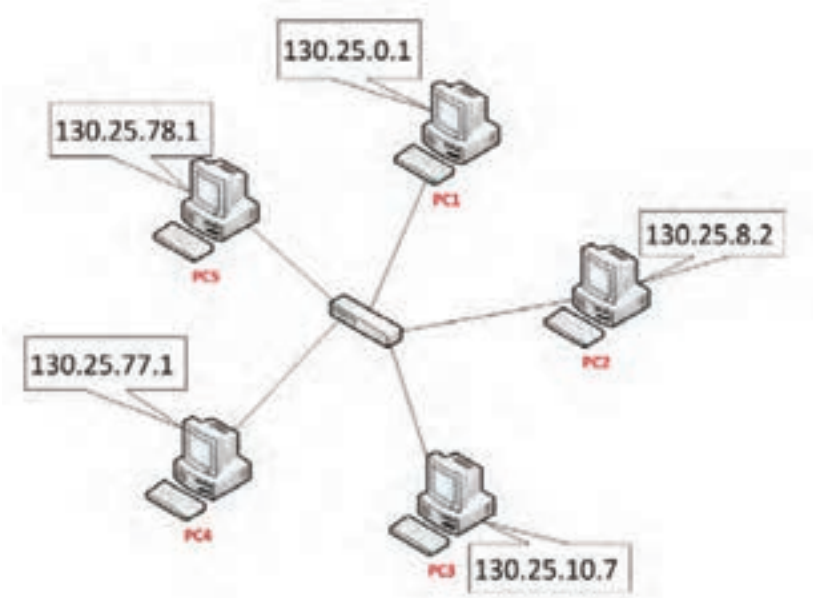
در شکل ۵ــ۶ــالف w برابر ۲۰۰ می‌باشد در نتیجه از کلاس C در IPv4 استفاده شده است بنابراین می‌توان نتیجه گرفت که Network ID=200.5.0 می‌باشد و Host ID هر گره ۱،۲،۳ و ۴ می‌باشد.

در شکل۵ــ۶ــب w برابر ۲۰۰ می‌باشد در نتیجه از کلاس C در IPv4 استفاده شده است بنابراین می‌توان نتیجه گرفت که Network ID=200.5.1 می‌باشد و Host ID هر گره ۱،۲،۳ و ۴ می‌باشد.

در شکل ۵ـ۶ـ ج w برابر ۱۰ می‌باشد در نتیجه از کلاس A در IPv4 استفاده شده است بنابراین می‌توان نتیجه گرفت که Network ID=10 می‌باشد و Host ID (PC1)=25.0.1 و Host ID (PC2)=25.8.2 و Host ID (PC3)=25.10.7 و Host ID (PC4)=25.77.1 می‌باشد.

در شکل ۵ـ۶ـ د w (برابر 130 می‌باشد در نتیجه از کلاس B در IPv4 استفاده شده است بنابراین می‌توان نتیجه گرفت که Network ID=130.25 می‌باشد و Host ID (PC1)= 0.1 و Host ID (PC2)= 8.2 و Host ID (PC3)=10.7 و Host ID (PC4)=77.1 و Host ID (PC5)=78.1 می‌باشد.

نکته ۱ : چنانچه تمام بیت‌های مربوط به Host ID برابر 0 باشد در آن صورت به IP آدرس شماره شبکه یا Network Number که به اختصار به آن NN می‌گویند برای مثال در شکل۶ـ۶ Network ID= 130.25 در نتیجه NN= 130.25.0.0 خواهد بود. از شماره شبکه یا NN نمی‌توان برای یک گره استفاده نمود.



شکل ۶ـ۶

نکته ۲ : اگر اعداد مربوط به Host ID برابر ۲۵۵ باشد عدد حاصله برای Broadcast Address نامیده می‌شود و برای ارسال به تمام سیستم‌های موجود در همان شبکه مورد استفاده قرار می‌گیرد که اصطلاحاً به آن BA گفته می‌شود. با توجه به مثال قبل می‌توان گفت که BA= 130.25.255.255 می‌باشد.

اگر کاربری فرمان ارسال اطلاعات را برای 130.25.10.7 صادر کند فقط یک Host یا Node که دارای آدرس مشخص شده می‌باشد اطلاعات را دریافت (پردازش) خواهد کرد که اصطلاحاً Unicast گفته می‌شود ولی اگر فرمان ارسال اطلاعات برای 130.25.255.255 صادر شود ، تمام گره‌های متصل به شبکه‌های با آدرس شبکه Network ID=130.25 اطلاعات را دریافت و پردازش خواهد نمود. که اصطلاحاً Broadcast نامیده می‌شود.

د) کلاس D : همان طور که قبلاً اشاره شد کلاس D برای Multicast رزرو شده است. 4 بیت اول در کلاس D به صورت 1110 می‌باشد یعنی بایت اول در حالت حداکثری برابر 11101111 می‌باشد (یعنی عدد 239) پس نتیجه می‌گیریم که در کلاس D اولین بایت یا همان w می‌تواند اعداد ۲۲۴ تا ۲۳۹ باشد یعنی کلاس D از رنج 224.0.0.0 تا 239.255.255.255 می‌باشد.

هـ) کلاس E : برای کارهای آزمایشگاهی(تحقیقاتی) رزرو شده است ۴ بیت اول در کلاس E همیشه به صورت 1111 می‌باشد یعنی بایت اول در حالت حداقلی برابر 11110000 می‌باشد (یعنی عدد ۲۴۰) و حداکثر مقدار برابر 11111111 می‌باشد(یعنی عدد 255) پس نتیجه می‌گیریم که در کلاس E اولین بایت یا همان w می‌تواند اعداد ۲۴۰ تا ۲۵۵ باشد.

آدرس‌های IPv4 در شبکه به وسیله رایانه‌ها به صورت رشته ای از بیت‌ها دیده می‌شود که به صورت ۴ گروه ۸ تایی می‌باشند از بیت‌ها،به عنوان مثال : 130.1.16.1 به صورت زیر دیده می‌شود :

10000010 00000001 00010000 00000001

IPv4 از آدرس چندپخشی(Multicast) برای ارائه بسته‌های اطلاعاتی از یک منبع به چند مقصد استفاده می‌کند .همچنین IPv4 آدرس‌های Broadcast را برای ارائه بسته‌های اطلاعاتی از یک منبع به همه رابط‌های بر روی زیر شبکه به کار می‌برد .

۵ـ۴ـ۶ـ آدرس‌های ویژه در IPv4

۱ـ آدرس 0.0.0.0 : به آدرس IPv4 نامشخص معروف می‌باشد و فقط برای آدرس منبع ،

زمانی که گره با IPv4 پیکربندی نشده باشد و با استفاده از سرویس DHCP بخواهد IPv4 خود را به دست آورد مورد استفاده قرار می‌گیرد.

۲ــ آدرس 127.0.0.1 : به نام آدرس Loop back معروف می‌باشد و یک گره را برای ارسال بسته‌ها به خودش فعال می‌کند.

۶ ــ۴ــ۶ــ ماسک زیر شبکه یا Subnet Mask : ماسک زیر شبکه برای نشان دادن شناسه مربوط به شبکه و همچنین شناسه مربوط به میزبان می‌باشد. که بیت‌های هر بخش آن یا همه صفر و یا همه ۱ هستند (یعنی اعداد ۰ و ۲۵۵) به طوری که برای تعیین شناسه شبکه ، به ازای هر بخش آدرس شبکه ؛ عدد ۲۵۵ قرار می‌گیرد و به ازای هر بخش میزبان عدد صفر جایگزین می‌شود و عدد ۲۵۵ به مفهوم ثابت بودن آدرس IP در یک زیر شبکه می‌باشد و عدد ۰ به مفهوم عدد متغیر ۱ تا ۲۵۴ می‌باشد. ضمناً با استفاده از ماسک زیر شبکه می‌توان کلاس شبکه را تعیین نمود. به مثال‌های زیر توجه کنید :

۱ــ اگر آدرس IPv4 یک گره برابر عدد 192.168.1.1 باشد در آن صورت Subnet Mask آن به صورت 255.255.255.0 خواهد بود. و آدرس IP از نوع کلاس C می‌باشد.

۲ــ اگر آدرس IPv4 یک گره برابر عدد 10.10.1.1 باشد در آن صورت Subnet Mask آن به صورت 255.0.0.0 خواهد بود. و آدرس IP از نوع کلاس A می‌باشد.

حتماً مشاهده کرده‌اید که هنگام واردکردن IP بخشی نیز برای واردکردن آدرس Default Gateway داریم. این آدرس معمولاً دو کاربرد اصلی دارد :

ــ آدرس کامپیوتری که اینترنت را برای کلاینت Share کرده است.

هنگامی که یک کامپیوتر در شبکه به اینترنت وصل است و باید اینترنت را در اختیار بقیه قرار دهد چنین حالتی پیش می‌آید. البته همیشه به این سادگی و فقط با تنظیم Gateway کارها انجام نمی‌شود اما این یکی از ساده‌ترین حالت‌هاست.

ــ آدرس پورت روتر در سمتی از سگمنت[1] که کلاینت در آن قرار دارد تا بدین وسیله به روتر وصل شود و در نتیجه با سگمنت‌های دیگر ارتباط برقرار کند.

نوع کلاس مورد استفاده برای آدرس‌دهی شبکه خود بستگی به تعداد Hostهای به‌کار رفته در شبکه دارد. به مثال زیر دقت کنید :

مثال : شبکه‌ای داریم متشکل از ۱۶۰ Host که با توجه به توسعه آن ممکن است به ۲۳۰ Host

---

۱ــ Segment : به بخشی از شبکه که سیستم‌های آن دارای یک Network ID هستند اشاره می‌کند و گاهی به بخشی از شبکه که بین تجهیزات شبکه‌ای مثل دو روتر یا دو سوئیچ قرار دارد گفته می‌شود.

افزایش پیدا کند از کدام کلاس استفاده کنیم؟ هر یک از کلاس‌های A,B,C را می‌توان به کار برد اما نظر به اینکه تعداد Host از ۲۳۰ عدد بیشتر نمی‌شود بهتر است از کلاسC استفاده کنیم و به عبارت دیگر آدرس‌ها را هدر ندهیم. بنابراین باید یک Net ID منحصر به‌فرد در کلاس C را که در شبکه‌های دیگر استفاده نشده باشد انتخاب کرده و آن را به شبکه خود اختصاص دهیم اما از کجا بدانیم که NetID آزاد و استفاده نشده کدام است؟ برای این کار خوشبختانه یک متولی وجود دارد که مسؤولیت تخصیص فضای آدرس‌ها را به عهده داشته و برای انتخاب NetID به آن مراجعه می‌کنند. این متولی همان IANA است (www.IANA.org) که البته برای منطقه اروپا کار را به www.ripe.net تفویض کرده است و چون در ایران معمولاً از آدرس‌های اروپایی استفاده می‌شود لذا به ripe مراجعه کرده و فرم درخواست IP را تکمیل می‌کنیم و پس از طی تشریفات مربوطه یک NetID منحصر به‌فرد در اختیار ما قرار داده می‌شود. فرض کنیم که در مثال یاد شده، NetID اختصاص یافته برای شرکت ما عدد ۲۱۳,۲۱۷,۲۴ باشد. بهتر است بگوییم شماره شبکه ما (Network Number) برابر با ۲۱۳,۲۱۷,۲۴,۰ است. با در اختیار داشتن Network Number مذکور به‌راحتی می‌توانیم کلیهٔ Hostها را از ۱ تا حداکثر ۲۵۴ شماره‌گذاری کنیم. به ترتیب زیر:

First Host = ۲۱۳,۲۱۷,۲۴,۱ Second Host = ۲۱۳,۲۱۷,۲۴,۲

Third Host = ۲۱۳,۲۱۷,۲۴,۳

:

Last Host = ۲۱۳,۲۱۷,۲۴,۲۵۴

البته در مثال فوق ۲۳۰ هاست داشتیم و بنابراین آدرس آخرین Host می‌شود: 213.217.24.230، اما با توجه به توان بالقوهٔ کلاس C، برای هر NetID می‌توانیم تا حداکثر ۲۵۴ Host را شماره‌گذاری کنیم و لذا آدرس آخرین Host را 213.217.24.254 نوشتیم و از این پس در بقیهٔ مثال‌ها نیز چنین خواهیم کرد.

بدیهی است طبق قوانین گفته شده اعداد 0 و 255 کاربرد خاص خود را داشته و نمی‌توانند برای شماره‌گذاری Host استفاده شوند:

Network Number = 213.217.24.0

Broadcast Address = 213.217.24.255

به‌طورکلی در حل این‌گونه مسائل باید ۴ مرحله را طی کنیم:

مرحله اول: تعیین کلاس با توجه به حداکثر تعداد Host.

مرحله دوم : اخذ شماره شبکه معتبر یا به زبان فنی : (Valid Network Number) یا (Valid IP Address).

مرحله سوم : تعیین آدرس اولین Host الی آخرین Host.

مرحله چهارم : تعیین Broadcast Address.

مطالعه آزاد

تا قبل از ویندوز ویستا ، فقط نسخه ۴ آدرس IP در شبکه ها استفاده می‌شد (IPv4) که تا حدود ۴ میلیارد آدرس IP را پشتیبانی می کرد با توجه به افزایش تعداد شبکه‌ها ، در ویندوز ویستا، ویندوز ۷ و ویندوز ۲۰۰۸ سرورنسخه ۶ برای IP ایجاد شد (IPv6).

IPv6 به جای ۳۲ بیت از ۱۲۸بیت برای آدرس دهی IP استفاده می کند و در واقع از ۸ بخش۱۶بیتی تشکیل شده است. و مقداردهی آن به صورت هگزا دسیمال می‌باشد و با : از یکدیگر جدا می شوند.

FE80: BA98: 7654: 3210: FEDC: BA98: 7654: 3210

آدرس دهی درIPv6 به دو قسمت تقسیم می شود به طوری که ۶۴ بیت اول (۸ بخش اول) برای آدرس دهی شبکه و ۶۴بیت دوم (۸ بخش دوم) برای آدرس دهی میزبان استفاده می شود :

بخش آدرس دهی شبکه در واقع همان Prefix Subnet (پیشوند زیر شبکه) می‌باشد.

IPv6 ایمن تر از IPV4 می باشد. پروتکل IPv6 قادر به حمایت از ۵۰ اکتیلیون (هر اکتیلیون معادل یک عدد به همراه ۴۸ صفر است) آدرس IP است.

خودآزمایی و پژوهش

۱ــ پروتکل چیست؟ انواع رایج آن را نام ببرید.

۲ــ سرویس‌های رایج در پروتکل TCP/IP را نام ببرید.

۳ــ تفاوت عمده و اساسی ترمینال با یک رایانه PC چیست؟

۴ــ کدام سرویس TCP/IP از ترمینال استفاده می‌کند؟ برای اتصال به سیستم مرکزی به چه چیزهایی نیاز دارد؟

۵ــ وظیفه Windows time چیست؟

۶ــ نام پروتکلی که ارسال ایمیل را انجام می‌دهد چیست؟

۷ــ وظیفه Terminal Service را شرح دهید.

۸ــ Host چیست؟ خصوصیت اصلی هر Host را نام ببرید.

۹ــ مراحل ثبت Domain را شرح دهید.

۱۰ــ کار SubDomain چیست؟

۱۱ــ پژوهش کنید آدرس Loop Back چیست؟

۱۲ــ پژوهش کنید که TCP/IP نسخه ۶ چیست و چه تفاوتی با نسخه ۴ دارد؟

۱۳ــ پژوهش کنید که چند کاربر می‌توانند به طور هم‌زمان از RDP استفاده کنند.

۱۴ــ پژوهش کنید که چه دستوراتی در محیط FTP رایج است؟

۱۵ــ پژوهش کنید که Domainهای .org,.inf,.prof,.gov,.ac,.com,.net,.edu در چه حوزه‌هایی مورد استفاده قرار می‌گیرند.

۱۶ــ پژوهش کنید که تفاوت Valid IP و InValid IP در چیست؟