مهندسی اینترنت

فهرست مطالب

فهرست اشکال

فهرست جداول

فصل اول

۱ یادآوری مفاهیم شبکه‌های کامپیوتری

۱-۱ دلایل استفاده از شبکه:

۱-استفاده از منابع اشتراکی

۲-کاهش هزینه‌ها

۳-دسترسی آسان و سریع‌تر

۴-دسترسی راه دور به منابع

۵-تبادل اطلاعات

۶-افزایش اطمینان

۷-حذف محدودیت‌های جغرافیایی در تبادل داده‌ها

۱-۲ اجزای اصلی شبکه:

- فرستنده و گیرنده
- داده
- رسانه
- پروتکل
- نرم‌افزار
- سخت‌افزار شبکه :

۱. تکنولوژی انتقال: شبکه از چه نوع کانالی به عنوان واسط انتقال استفاده می‌کند.

۲. مقیاس شبکه و ناحیه‌ی تحت پوشش آن: شبکه چه مسافت جغرافیایی را پوشش می‌دهد و حداکثر چند ایستگاه می‌تواند در شبکه وجود داشته باشد.

۱-۳ تقسیم‌بندی شبکه از نظر گستردگی جغرافیایی:

- PAN (Personal Area Network)

شبکه‌های زیر ۱۰ متر یا شبکه‌های شخصی در حد ۲ یا ۳ کامپیوتر

- LAN (Local Area Network)

شبکه‌های زیر ۵۰۰ متر که حداکثر در حد یک یا دو ساختمان مجاور می‌باشند و یا در فواصل جغرافیایی محدود (حداکثر تا چند کیلومتر) قرار دارند.

- CAN (Campus Area Network)

این شبکه‌ها از لحاظ وسعت بزرگتر از LAN کوچکتر از MAN هستند و به یک منطقه جغرافیایی محدود می‌شوند. مانند دانشگاه‌هایی که شامل چندین دانشکده در یک محیط هستند ولی در چند ساختمان مجزا قرار دارند.

- MAN (Metropolitan Area Network)

شبکه‌های شهری که در سطح یک منطقه‌ی وسیع در حد یک شهر و یا با اتصال چندین شبکه‌ی محلی به وجود می‌آیند.

- WAN(Wide Area Network)

شبکه‌های گسترده، در گستره‌ی جغرافیایی یک کشور یا جهان پیاده‌سازی می‌شود و شبکه‌های شهری و بین‌شهری را به هم مرتبط می‌کند.

۱-۳-۱ رسانه‌های مورد استفاده در این شبکه‌ها:

- PAN: سیم مسی، امواج رادیویی (مانند شبکه‌های Bluetooth)، Infrared
- LAN: سیم مسی، امواج رادیویی، فیبر نوری
- CAN: رسانه‌های ارتباطی آن تقریبا مانند LAN می‌باشد و معمولا از فیبر نوری استفاده می‌کنند، چون پهنای باند بیشتری در اختیارمان قرار می‌دهد و سرعت بیشتر و noise کمتری دارد.
- MAN: خطوط تلفن (Leased line)، فیبرنوری، در شبکه‌های بی‌سیم شهری (برد و سرعت بیشتر) IEEE 802.16
- WAN: از ماهواره یا دکل‌های Point To Point استفاده می‌شود (یعنی از آنتی به آنتن دیگر که در دید مستقیم آن است.)

نکته: استاندارد IEEE 802 در مورد شبکه‌های کامپیوتری است. تجهیزاتی که طبق یک استاندارد تولید می‌شوند قادر خواند بود با یکدیگر به طور سازگار کار کنند. نیاز به استاندارد زمانی مطرح می‌شود که ارتباط بین چند سیستم (از تولیدکنندگان مختلف) وجود دارد.

۱-۴ تقسیم‌بندی شبکه از نظر مالکیت:

۱- شبکه‌های عمومی (Public Networks)

۲- شبکه‌های خصوصی (Private Networks)

۳- شبکه‌های خصوصی مجازی (Virtual Private Networks)

۱-۴-۱ شبکه‌های عمومی:

شبکه‌هایی که متعلق به یک شرکت خاص نیست و همه می‌توانند از آن استفاده کنند و همه برای اشتراک هزینه می‌پردازند، مانند شبکه‌ی تلفن.

مزایا:

از تجهیزات استفاده‌ی مشترک می‌شود و در نتیجه هزینه کاهش می‌یابد، ارتباط گسترده است زیرا همه می‌توانند از آن استفاده کنند و به عبارتی محدود به یک حوزه نمی‌شود.

معایب:

امنیت پایین می‌آید چون همه از یک تجهیزات مشترک استفاده می‌کنند و می‌توانند به اطلاعات دیگران دسترسی داشته باشند، سرعت نیز پایین می‌آید چون امکانات باید بین همگان تقسیم شود.

۱-۴-۲ شبکه‌های خصوصی:

شبکه‌ای که مختص یک شرکت خاص است و تجهیزات آن متعلق به همان شرکت خصوصی است مثلا اگر دو شبکه‌ی یک شرکت را در دو طرف شهر به هم وصل کنیم می‌توانیم همه‌ی تجهیزات آن را خود تهیه کرده که در این صورت فقط خود اجازه‌ی استفاده از آن را داریم.

مزایا:

دارای امنیت بالاتر است چون دیگران نمی‌توانند اطلاعات را شنود کنند و سرعت نیز بالاتر است.

معایب:

بالا بودن هزینه‌ها، چه در راه‌اندازی و چه در نگهداری (پرسنلی که باید آن را اداره کنند)

۱-۴-۳ شبکه‌های خصوصی مجازی:

اتصال دو یا چند شبکه‌ی خصوصی از طریق شبکه‌ی عمومی است (با استفاده از تجهیزات شبکه‌ی عمومی). به آن مجازی می‌گوییم زیرا آن را شبیه‌سازی کرده و از تجهیزات شبکه‌ی عمومی استفاده می‌کنیم تا به مقصود برسیم.

امنیت در شبکه‌های خصوصی: اطلاعات را رمز گذاری می‌کنیم تا از طریق آن محرمانگی حفظ شود و اگر کسی در بین راه شنود کرد، متوجه نشود.

۱-۵ رسانه‌ی ارتباطی

۱- نقطه به نقطه: بین هریک از اعضای شبکه یک کانال مجزا وجود دارد.

۲- پخشی (Broadcast): انتقال اطلاعات از طریق یک کانال فیزیکی که بین تمام ایستگاه‌های شبکه مشترک است، انجام می‌شود.

۱-۶ انواع ارتباط

- اتصال‌گرا (Connection Oriented)

قبل از اینکه ارسال اطلاعات داشته باشیم باید یک گفتگو بین فرستنده و گیرنده انجام شود و پس از برقراری ارتباط فرستنده و گیرنده تبادل اطلاعات انجام دهند، در واقع قبل از ارسال فرستنده از آمادگی گیرنده برای دریافت مطلع می‌شود.(مانند گفتگوی تلفنی)

- بدون اتصال (Connection Less)

فرستنده هر وقت بخواهد بدون اینکه مسیر ارتباطی را قبلا ایجاد کند اطلاعاتش را ارسال می‌کند و گیرنده هم بدون اینکه بداند چیزی قرار است به او برسد همیشه در حال گوش دادن است (مانند نامه‌ی پستی)

۱-۷ انواع ارتباط از نظر قابلیت اطمینان

- قابل اعتماد (Reliable)

در این نوع ارتباط، فرستنده از رسیدن یا نرسیدن داده‌ی ارسالی به گیرنده مطلع می‌شود. به عبارتی دیگر گیرنده دریافت هر داده را به فرستنده اطلاع می‌دهد (با ارسال تصدیق دریافت یا Acknowledgement).

این نوع ارتباط برای کاربردهایی مناسب است که سالم و کامل رسیدن داده‌ها اهمیت زیادی دارد، مثل انتقال فایل، چون اگر قسمتی از اطلاعات از بین برود دیگر قابل استفاده نخواهد بود.

- غیر قابل اعتماد (Unreliable)

فرستنده از سرنوشت بسته ارسالی به گیرنده، مطلع نمی‌شود. در مواردی کاربرد دارد که نرسیدن بخشی از داده‌ها به گیرنده قابل چشم‌پوشی است (در واقع تاخیر نداشتن مهمتر از سالم رسیدن است). مثل انتقال Video یا صوت، چون اگر قسمتی از اطلاعات از بین برود بقیه‌اش قابل فهم خواهد بود.

۱-۸ انواع معماری سرویس‌دهی در شبکه‌ها

۱. Peer-to-Peer (نظیر به نظیر)

۲. Client – Server (سرویس‌دهنده/سرویس گیرنده)

سرویس دهنده/ سرویس گیرنده: بیشتر مفهوم نرم‌افزاری دارد و نه سخت‌افزاری، یعنی سرور برنامه‌ای است که به درخواست‌های رسیده پاسخ می‌دهد، بعنوان مثال در web، مرورگر نقش client را دارد که از طریق آن درخواست‌ها به سرور وب ارسال می‌شود و سرور نیز پاسخ را به مرورگر می‌دهد..

۱-۹ انواع توپولوژی (هم‌بندی) شبکه:

- Bus: یک کانال فیزیکی مشترک داریم و تمام ایستگاه‌های کاری به این رسانه وصل می‌شوند.
- Star: اتصال ایستگاه‌های کاری از طریق یک متمرکز کننده (Concentrator) به نام Hub یا Switch انجام می‌گیرد.
- Ring: یک حالت خاصی از Bus که دو سر سیم به هم وصل می‌شود (ایستگاه‌ها در یک ساختار بسته‌ی حلقوی به یکدیگر متصل‌اند.)
- Tree: در هم‌بندی درختی یا سلسله‌مراتبی، ارتباط nodeها از طریق گره‌های بالایی است.
- ترکیبی یا Hybrid: ترکیب دو یا چند توپولوژی
- Mesh: تمام گره‌های شبکه را یک رسانه‌ی مجزا دو به دو و به صورت مستقیم به هم وصل می‌کند.

Mesh کامل: تمام گره‌ها باید دو به دو بهم متصل باشند.

Mesh ناقص: ممکن است تمام گره‌ها بهم وصل نباشند یعنی تعدادی از ایستگاه‌های کاری یا گره‌ها به طور مستقیم بهم وصل نیستند.

اگر بخواهیم تعداد سیم‌کشی ها را درMesh کامل به دست آوریم، هر شبکه با n ایستگاه کاری دارای n(n-1)/2 سیم‌کشی می‌باشد.

۱-۹-۱ مزایا و معایب هر کدام از توپولوژی‌های فوق

Bus: هزینه‌ی راه‌اندازی پایین (مثلا با استفاده از یک کابل coaxial همه‌ی کامپیوترها را به هم وصل می‌کنیم، سرعت پایین، چون داده‌ها به طور همزمان ارسال می‌شوند و تنها یک مسیر وجود دارد و تصادم باعث می‌شود که داده‌ها از بین بروند.

Star: پهنای باند افزایش می‌یابد. اضافه و یا حذف کردن ایستگاه‌های کاری آسان است و فقط کافی است یک portخالی پیدا کنیم ولی در Bus باید کابل قطع شود و این خودش هزینه و زمان می‌برد.

Ring: در این توپولوژی دوسیم داریم که معمولا از یکی در جهت عقربه‌های ساعت استفاده می‌شود ولی اگر بر اثر یک حادثه کابل آن قطع شود ارتباط از طریق سیم دیگر و در خلاف جهت عقربه‌های ساعت انجام می‌گیرد.

Tree: مدیریت در بخش‌های مختلف راحت‌تر می‌شود و می‌توان مدیریت هر قسمت را به واگذار کرد.

Mesh: اگر بخواهیم یک node دیگر اضافه کنیم مشکل خواهیم داشت و باید به تمام nodeهای دیگر وصل کنیم و هزینه و سیم‌کشی زیاد می‌شود بخصوص درMesh کامل.

و از مزایای آن این است که قابلیت اطمینان بالا می‌رود یعنی اگر یک کابل قطع شود راه‌های دیگری برای انتقال وجود دارد و همچنین بیشتر در کامپیوترهای سرور به کار می‌رود.

و در مواقعی که ترافیک شبکه بالاست و یا حجم اطلاعات زیاد است، می‌توان بخشی از داده‌ها را از یک لینک و بخش دیگر را از لینک‌های دیگر منتقل کرد، یعنی توزیع بار (Load Balancing) صورت می‌گیرد.

تفاوت اصلی Hub و Switch

درHub، فریم دریافت شده بدون توجه به آدرس مقصد آن به همه‌ی portها (غیر پورتی که فریم از آن دریافت شده) ارسال می‌شود. ولی در Switch با توجه به آدرس گیرنده (آدرس MAC گیرنده)، فریم تنها روی پورتی ارسال می‌شود که به مقصد متصل است (بنابراین بقیه پورت‌ها مشغول نمی‌شوند).

نکته: پهنای باند شبکه‌ای که از یک Switch با n پورت با پهنای باند B استفاده می‌کند برابر n/2*B است درحالی‌که پهنای باند همان شبکه زمانی که از یک Hub با n پورت استفاده می‌کند، برابر B است.

نکته: در حالتی که رسانه‌ها مشترک است ، امکان تصادم (Collision) وجود دارد ولی در حالتی که رسانه Point To Point است امکان تصادم کم است.

۱-۱۰ شبکه اترنت (Ethernet)

معادل با استاندارد 802.3 است با اندکی تفاوت جزئی.

۱- شبکه‌هایی که از کابل Coaxial (هم محور) استفاده می‌کنند.

Thick Ethernet (10Base2): کابل RG-8

Thin Ethernet (10Base5): کابل RG-58

۲- شبکه‌هایی که از کابل زوج سیم به هم تابیده (Twisted pair) استفاده می‌کنند. توپولوژی این شبکه‌ها Star است. (کابل Cat7, Cat6, Cat5e, Cat5)

۳- فیبر نوری

	Thin Ethernet	Thick Ethernet	شبکه‌ی Starبا کابل cat5
حداکثر طول سیم	185m	500m	100m
حداکثر سرعت	10Mbps	10Mbps	100Mbps
حداکثر تعداد ایستگاه‌ها	30	100	1024

*درون ساختمان از کابل بدون محافظ (UTP) استفاده می‌کنند چون noise آن پایین است و زیر آفتاب دوام نمی‌آورد (بیرون ساختمان از STP و فیبر نوری استفاده می‌کنند.)

Base Band: یعنی از هیچ تسهیم سازی (Multiplexing) استفاده نمی‌کنیم.

اگر بخواهیم چند قسمت از شبکه BUS را به هم متصل کنیم از Repeater استفاده می‌کنیم تا افت سیگنال را جبران کند.

* یادآوری: بر اساس CSMA/CD هر کامپیوتری که قصد ارسال اطلاعات دارد ابتدا به خط گوش می‌دهد و اگر خط مشغول نباشد و تصادمی رخ نداده باشد آن‌گاه به ارسال می‌پردازد ولی اگر طول سیم زیاد باشد این کار مشکل می‌شود.

۱-۱۱ مفاهیم Service، Interface و Protocol:

۱-۱۱-۱ سرویس

خدماتی که لایه‌ی پایین‌تر به لایه‌ی بالاتر می‌دهد.

۱-۱۱-۲ رابط Interface

رابط بین لایه‌ی پایین‌تر یا بالاتر

نحوه‌ی دسترسی به خدمات، تعیین پارامترهای مورد نیاز برای ایجاد ارتباط و چگونگی دسترسی به سرویس‌ها را برای لایه‌های همسایه تعریف می‌کند (مثلا چگونگی فراخوانی پارامترهای مورد نیاز)

۱-۱۱-۳ پروتکل

نحوه‌ی برقراری ارتباط بین دو لایه متناظر در دو طرف ارتباط را تعریف می‌کند.

مثال: برنامه‌نویسی شیءگرا:

به جای استفاده از توابع از شیء استفاده می‌کنیم و هر Object یک method دارد که هر method شامل یک سری توابع است که هر تابع پارامترهایی دارد.

```
Screen.print("text",x,y)
```

۱-۱۱-۴ مدل

یک سری کلیات را در مورد کل لایه‌ها بیان می‌کند.

۱-۱۱-۵ پشته پروتکل (Stack Protocol)

به مجموعه پروتکل‌های استفاده شده در تمامی لایه‌ها گفته می‌شود.

۱-۱۲ معماری OSI

نام لایه‌ها و نام واحد اطلاعاتی در هر لایه

لایه‌ی ۷- کاربرد: پیام(Message)

لایه‌ی ۶- ارائه: پیام

لایه‌ی ۵- جلسه: پیام

لایه‌ی ۴- انتقال: سگمنت(Segment)

لایه‌ی ۳- شبکه: دیتاگرام(Datagram) یا بسته (Packet)

لایه‌ی ۲- پیوند داده‌ها: قاب (Frame)

لایه‌ی ۱- فیزیکی: بیت(Bit)، گاهی سیگنال (Signal) نیز گفته می‌شود.

۱-۱۳ تعریف میزبان (Host) و مسیریاب (Router):

میزبان یا Host تنها ارسال کننده و یا دریافت کننده‌ی بسته‌های اطلاعاتی است و هیچ نقشی در هدایت بسته‌های گره‌های دیگر ندارد در حالیکه مسیریاب وظیفه‌ی هدایت و مسیریابی گره‌های دیگر را بر عهده دارد و خود، داده‌ای برای ارسال و یا دریافت ندارد.

۱-۱۴ روش‌های برقراری ارتباط بین دو ماشین در شبکه

- سوئیچینگ مداری
- سوئیچینگ پیام
- سوئیچینگ بسته و سلول

۱-۱۵ طراحی شبکه‌ها و اصول لایه‌بندی:

۱- وظیفه‌ی هر لایه کاملا مشخص باشد.

۲- سرویس‌هایی با ماهیت متفاوت، لایه به لایه و جداگانه طراحی شود.

۳- وظیفه‌ی هر لایه با توجه به قراردادها و استانداردهای جهانی مشخص شود.
۴- تعداد لایه‌ها نباید آنقدر زیاد باشد که تمایز لایه‌ها از دیدگاه سرویس‌های ارائه شده نامشخص باشد و نه آنقدر کم باشد که وظیفه‌ی و خدمات یک لایه ، پیچیده و نامشخص باشد.
۵- در هر لایه جزئیات لایه‌ی زیرین نادیده گرفته می‌شود و لایه‌ی بالایی به سادگی و ماجولار از خدمات لایه‌ی پایین استفاده می‌کند.(مانند برنامه‌نویسی ماجولار یا تابعی ...)
۶- مرزهای هر لایه به گونه‌ای باشد که جریان اطلاعات بین لایه‌ها، حداقل باشد.

۱-۱۶ مدل مرجع OSI

لایه‌ی فیزیکی:

وظیفه‌ی اصلی آن، انتقال بیت‌ها به صورت سیگنال الکتریکی و ارسال آن روی کانال است

پارامترهایی که در این لایه مورد نیاز است:

- ظرفیت کانال فیزیکی و نرخ ارسال
- نوع مدولاسیون
- چگونگی کوپلاژ با خط انتقال
- مسائل مکانیکی و الکتریکی مانند نوع کابل، باند فرکانس، نوع رابط (کانکتور کابل) و ...

لایه‌ی پیوند داده‌ها:

- استفاده از مکانیزم‌های کشف و کنترل خطا، جهت ارسال بدون خطا و مطمئن داده‌ها به مقصد.
- فریم‌بندی داده‌ها (داده‌های لایه‌ی بالاتر را به واحدهای کوچکتر بسته‌بندی می‌کند.)
- کنترل جریان (دستگاه کند هیچ‌گونه فریمی را به خاطر آهسته بودن از دست ندهد)
- اعلام وصول داده‌ها با عدم رسید داده‌ها به فرستنده
- جلوگیری از تصادم

لایه‌ی شبکه:

(سرویس بدون اتصال و نامطمئن)

- سازماندهی اطلاعات به صورت بسته‌ها

- مسیریابی و هدایت بسته به مقصد از میان چندین شبکه
- جلوگیری و اجتناب از ازدحام

لایه‌ی انتقال:

- ارائه‌ی سرویس مطمئن و اتصال‌گرا
- شماره‌گذاری بسته‌ها جهت گم نشدن آن‌ها و عدم دریافت تکراری
- مطمئن شدن از آماده بودن گیرنده
- ترتیب جریان بسته‌ها

لایه‌ی جلسه:

(فراهم آوردن شرایط یک جلسه همانند ورود به سیستم از راه دور، تصدیق اصالت)

- برقراری و مدیریت یک جلسه
- شناسایی طرفین
- مشخص کردن اعتبار پیام‌ها
- اتمام جلسه
- حسابداری مشتری‌ها

لایه‌ی ارائه(نمایش):

- فشرده سازی
- رمزنگاری و رمزگشایی
- تبدیل کدها به یکدیگر (مثلا EBCDIC به ASCII)

لایه‌ی کاربرد:

استاندارد مبادله‌ی پیام بین نرم‌افزارهایی که در اختیار کاربر بوده و به نحوی با شبکه در ارتباطند. مانند نامه‌های الکترونیکی، انتقال مطمئن فایل، دسترسی به بانک اطلاعاتی راه دور، انتقال صفحات وب

۱-۱۷ مدل ۴لایه‌ای TCP/IP

در اواخر دهه‌ی شصت، آژانس پروژه‌های پیشرفته‌ی تحقیقاتی دولت ایالات متحده(ARPA) با بودجه‌ی دولتی تصمیم به پیاده‌سازی یک شبکه‌ی WAN در نه ایالت آمریکا گرفت، این شبکه اهداف نظامی را دنبال می‌کرد. کمیته‌ی ARPA که به ICCB معروف شد روز به روز شهرت یافت و رشد کرد. این کمیته با همکاری بقیه‌ی آژانس‌های تحقیقاتی، کار مشترک تبدیل تکنولوژی ARPA به یک پروتکل شبکه‌ای استاندارد به نام TCP/IP را شروع کردند.

در سال ۱۹۸۳ کمیته‌ی ICCB به عنوان گروه طراحی اینترنت یا IAB به جهان معرفی شد. این کمیته یک سازمان مستقل برای طراحی استانداردها و ترویج تحقیقات در زمینه‌ی تکنولوژی اینترنت است.

ARPA: Advanced Research project Agency

ICCB: Internet Control and Configuration Board

TCP/IP: Transport Control Protocol/Internet Protocol

IAB: Internet Architecture Board

کمیته‌ی IAB اکنون نیز وجود دارد و در دو قسمت فعالیت می‌کند:

- گروه IETF: موارد فنی و مشکلات استانداردها و تکنولوژی به‌کار رفته دز شبکه‌ی اینترنت را بررسی و حل می‌کند و جزئیات پروتکل‌های فعلی را در اختیار عموم قرار می‌دهد.
- گروه IRTF: کار تحقیقات به منظور بهبود و ارتقاء اینترنت را بر عهده دارد.

IETF: Internet Engineering Task Force

IRTF: Internet Research Task Force

مدیریت روزانه و پشتیبانی فنی شبکه‌ی اینترنت، توسط مرکزی در آمریکا به نام INTERNIC انجام می‌شود. این مرکز مدیریت سطح بالای شبکه، ثبت اسامی نمادین در اینترنت و ثبت کلاس‌های آدرس یکتا را بر عهده دارد. این مرکز، استانداردهای اینترنت و تکنولوژی‌های مرتبط با آن را که مورد تایید IAB است، تحت مستندات دقیق و کاملی به نام RFC به دنیا عرضه می‌کند.

INTERNIC: Internet Network Information Center

RFC: Request For Comment

مدل TCP/IP:

Application layer	**لایه‌ی کاربرد**
Transport layer	**لایه‌ی انتقال**

لایه‌ی اینترنت **Internet layer**

لایه‌ی دسترسی به شبکه (لایه واسط شبکه) **Network Interface**

لایه‌ی واسط شبکه:

- این لایه درگیر با مسائل فیزیکی؛ الکتریکی و مخابراتی کانال انتقال، نوع کارت شبکه و راه‌اندازی‌های لازم برای کارت شبکه است.
- الزام ویژه‌ای برای بکارگیری سخت‌افزار در ارتباطی خاص در این لایه وجود ندارد.

لایه‌ی اینترنت (شبکه):

- وظیفه دارد بسته‌های اطلاعاتی را روی شبکه هدایت کرده و از مبدا تا مقصد پیش ببرد.
- مهمترین پروتکل: IP
- پروتکل‌های دیگر: RARP – Bootp – ARP – ICMP
- واحد اطلاعاتی که باید تحویل مقصد داده شود "دیتاگرام" نامیده می‌شود.
- وظیفه‌ی قطعه‌قطعه کردن و بازسازی داده‌ها که روی شبکه منتقل می‌شوند را بر عهده دارد.
- ارسال چند پخشی

لایه‌ی انتقال:

- برقراری ارتباط انتهایی (ماشین‌های میزبان)
- ارائه‌ی سرویس‌های مطمئن و اتصال‌گرا
- برای عملیاتی نظیر صوت و تصویر که سرعت مهمتر از دقت است، سرویس بدون اتصال، سریع و نامطمئن نیز ارائه می‌کند.

لایه‌ی کاربرد:

سرویس سطح بالا جهت خلق برنامه‌های کاربردی ویژه مانند HTTP,E-mail,FTP,Telnet و ...

فصل دوم

۲ پروتکل IP (Internet Protocol):

قراردادی که حمل و تردد بسته‌های اطلاعاتی و همچنین مسیریابی صحیح آن‌ها را از مبدا به مقصد مدیریت و سازماندهی می‌کند، پروتکل IP نام دارد.

مسیریاب Router:

ماشینی است که تعدادی ورودی/خروجی داشته و بسته‌های اطلاعاتی را از ورودی‌ها تحویل گرفته و بر اساس آدرس مقصد، یکی از کانال‌های خروجی را برای انتقال بسته انتخاب می‌نماید. به نحوی که بسته را به مقصد نزدیک نماید.

میزبان (Host):

ماشینی است که هیچ نقشی در هدایت بسته‌های اطلاعاتی روی شبکه ندارد و فقط تولید کننده یا دریافت کننده‌ی بسته‌های اطلاعاتی است.

دیتاگرام:

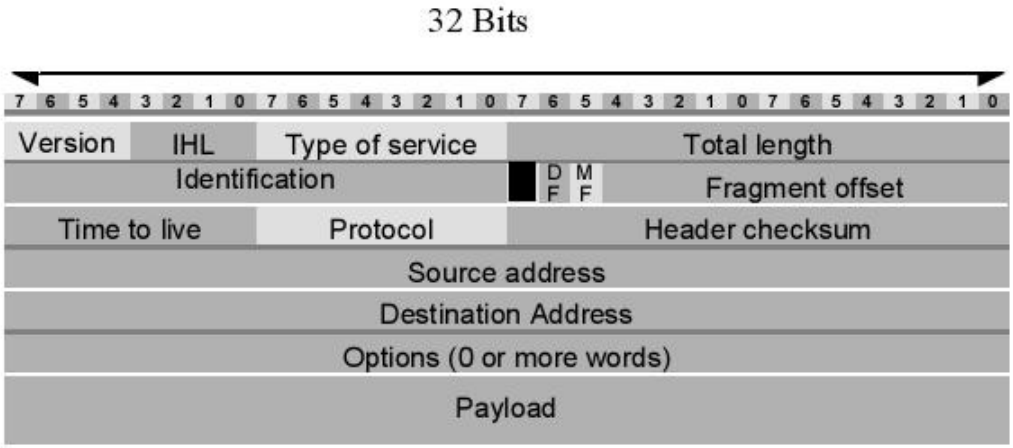
یک واحد اطلاعاتی است که به صورت یکجا از لایه‌ی IP به لایه‌ی انتقال تحویل داده می‌شود و یا بالعکس لایه‌ی انتقال آن‌را جهت ارسال روی شبکه به لایه‌ی IP تحویل داده و ممکن است شکسته شود.

پروتکل IP (Internet Protocol):

عمده‌ترین پروتکل مورد استفاده در لایه شبکه (لایه اینترنت در مدل TCP/IP) در اینترنت است و وظیفه اصلی آن آدرس‌دهی و رساندن بسته‌ها به مقصد از میان شبکه‌های مختلف است. در حال حاضر پروتکل IP دارای نسخه‌های ۴ و ۶ است. IPv4 بصورت گسترده در شبکه اینترنت مورد استفاده قرار می‌گیرد، در حالیکه IPv6 هنوز رایج نشده است زیرا نیاز به تغییرات در سخت افزار و نرم افزار شبکه دارد.

قالب یک بسته‌ی IP نسخه ۴(IP_{V4} Header):

یک بسته‌ی IP از دو قسمت سرآیند و قسمت حمل داده تشکیل شده است. مجموعه اطلاعاتی که در قسمت سرآیند بسته‌ی IP درج می‌شود توسط مسیریاب‌ها مورد استفاده و پردازش قرار می‌گیرد.



شکل ۲-۱: ساختار بسته IP

معرفی فیلدها:

Version:

شماره‌ی نسخه‌ی IP را مشخص می‌کند. به طور مثال IPv4 یا IPv6

IHL: Internet Header Length

طول سرآیند IP است که واحد آن بر اساس 4 byte است. که طول حداقل آن باید 20 byte باشد یعنی عدد 5 ، و طول حداکثر آن 60 byte یعنی عدد 15 می‌باشد. زیرا فیلد IHL ، 8 bit ای است و حداکثر عددی را که می‌تواند در خود جای دهد عدد 15 است.

TOS: Type Of Service

نوع سرویس را مشخص می‌کند و 8 bit است و توسط آن ماشین میزبان یا فرستنده از مجموعه‌ی زیر شبکه (مجموعه‌ی مسیریاب‌های بین راه) تقاضای سرویس ویژه‌ای (مثلا ارسال با حداقل تاخیر) را برای ارسال یک بسته می‌نماید. کاربرد هریک از این ۸ بیت در جدول زیر آمده است:

P2	P1	P0	D	T	R	_	_
تقدم بسته			**تأخیر**	**توان خروجی**	**قابلیت اطمینان**	**بلااستفاده**	

Total Length:

طول کل بسته‌ی IP را مشخص می‌کند و واحد آن bit است که 16 bit می‌باشد.

Identification:

شماره‌ی یک دیتاگرام واحد را مشخص می‌کند. این فیلد برای تمام قطعاتی که متعلق به یک بسته IP هستند (و در بین مسیر fragment شده است) یکسان است.

DF: Don't Fragment

با یک شدن این بیت در یک بسته‌ی IP هیچ مسیریابی حق ندارد آن را قطعه‌قطعه کند چرا که مقصد قادر به بازسازی دیتاگرام‌های تکه‌تکه شده نیست. حال اگر این بیت به ۱ تنظیم شده باشد و مسیریابی نتواند آن را به دلیل بزرگی اندازه‌ی آن، انتقال دهد به ناچار آن را حذف خواهد کرد.

MF: More Fragments

این فیلد نشان می‌دهد که آیا بسته‌ی IP آخرین قطعه از یک دیتاگرام محسوب می‌شود یا باز هم قطعه‌ی بعدی وجود دارد. در آخرین قطعه از یک دیتاگرام، بیت MF صفر خواهد بود و در بقیه الزاما ۱ است.

Fragment Offset:

شماره‌ی ترتیب هر قطعه در یک دیتاگرام شکسته شده را مشخص می‌کند به همین دلیل یک دیتاگرام حداکثر می‌تواند به ۸۱۹۲ تکه تقسیم شود. چون عددی که در این فیلد قرار می‌گیرد ضریب ۸ دارد (بعنوان مثال اگر عدد ۹ قرار گیرد یعنی این قطعه از ابتدای بسته ۷۲ بایت فاصله دارد)، بنابراین اندازه هر قطعه باید ضریبی از ۸ باشد.

TTL: Time To Live

این فیلد که 8 bit است طول عمر بسته (در واقع Hop count) را مشخص می‌کند. فرستنده‌ی هر بسته یک مقدار اولیه داخل این فیلد قرار می‌دهد و هر یک از مسیریاب‌های بین راه یک واحد از مقدار آن کم کرده و آن را به سمت مقصد هدایت می‌کنند. هرگاه مقدار این فیلد به صفر رسید مسیریاب‌های بین راه بسته را دور می‌ریزند. با استفاده از این فیلد امکان تشخیص بسته‌های سرگردان و خارج کردن آن‌ها از شبکه به وجود می‌آید.

این فیلد مکانیزمی برای تشخیص بسته‌های سرگردان در شبکه است.

Protocol:

این فیلد که 8 bit است نوع پروتکل‌های لایه‌ی بالاتر را مشخص می‌کند. در واقع گیرنده‌ی بسته‌ی IP از روی این فیلد تشخیص می‌دهد که Payload بسته را به کدام پروتکل لایه‌ی انتقال باید تحویل دهد.

Header Checksum:

16 bit است و وظیفه‌ی آن کشف خطاست. برای محاسبه‌ی کد کشف خطا، کل Header به صورت ۲ بایت، ۲ بایت با یکدیگر جمع می‌شود و نهایتا حاصل جمع به روش مکمل ۱ منفی می‌شود. و این عدد منفی در این فیلد قرار می‌گیرد. در هر مسیریاب قبل از پردازش و مسیریابی مجددا checksum به روش گفته شده (البته با در نظر گرفتن کم شدن مقدار TTL) محاسبه شده و با عدد قبلی جمع می‌شود. اگر حاصل صفر بود یعنی اینکه بسته بدون خطا دریافت شده است در غیر این صورت خطایی رخ داده است.

Source Address:

هر ماشین میزبان در شبکه‌ی اینترنت یک آدرس جهانی و یکتای ۳۲ بیتی دارد. بنابراین هر ماشین میزبان در هنگام تولید یک بسته‌ی IP باید آدرس خودش را در این فیلد قرار بدهد.

Destination Address:

در این فیلد آدرس ۳۲ بیتی مربوط به ماشین مقصد که باید بسته‌ی IP تحویل آن بشود، قرار می‌گیرد.

Options:

این فیلد اختیاری است و حداکثر می‌تواند 40 byte باشد. و شامل اطلاعاتی است که می‌تواند به مسیریاب‌ها در مورد یافتن مسیر مناسب کمک کند.

Payload:

در این فیلد داده‌های دریافتی از لایه‌ی بالاتر قرار می‌گیرد.

۲-۱ آدرس‌های IP

پروتکل اینترنت در ارتباطات بین شبکه‌ای از آدرس‌های منحصر به فرد و یکتای ۳۲ بیتی بهره می‌برد.که به IPv4 معروف است.(هرچند نسل دوم آدرس‌های IP که به IPv6 معروفند و ۱۲۸ بیتی می‌باشند نیز به وجود آمده است که در مراحل آغازین استفاده است و هنوز همه‌گیر نشده است. به همین دلیل ما به معرفی IPv4 می‌پردازیم)

آدرس‌های IP درون یک عدد دودویی ۳۲ بیتی درج می‌شوند ولیکن برای سادگی نمایش به چهار قسمت ۸ بیتی تقسیم و به صورت چهار عدد دهدهی که با نقطه از هم جدا شده‌اند، نوشته می‌شود. یعنی معادل هر یک از بایت‌های آدرس به صورت مجزا نوشته شده و هر عدد با یک علامت نقطه از دیگری تفکیک می‌شود. به عنوان مثال آدرس زیر یک آدرس IP معتبر می‌باشد که در قالب چهار قسمت دهدهی نوشته شده است.

34.21.255.1

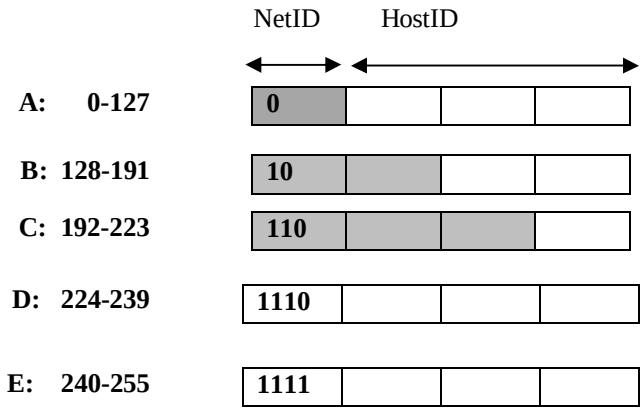
این آدرس به صورت زیر در فیلد آدرس از یک بسته‌ی IP تنظیم می‌شود:

0	0	1	0	0	0	1	0	0	0	0	1	0	1	0	1	1	1	1	0	0	0	0	1	0	0	0	0	0	0	0	1

پرارزش‌ترین بایت، یعنی اولین بایت سمت چپ از آدرس IP ، کلاس‌های آدرس را مشخص می‌کند و از این رو دارای اهمیت ویژه است.

۲-۲ کلاس‌های آدرس IP:

- آدرس‌های IP سلسله‌مراتبی هستند. یعنی آدرس IP از دو بخش تشکیل شده است. بخش اول از آدرس IP مشخص کننده‌ی NetID (شماره شبکه) و بخش دوم مشخص‌کننده‌ی HostID (شماره میزبان در شبکه) است. تمام آدرسهایی که بخش NetID آنها با هم برابرند مربوط به یک شبکه هستند
- IPv4 دارای کلاس‌های A,B,C,D,E می‌باشد. IPهای کلاس E رزرو شده‌اند و برای مقاصد تحقیقاتی و آزمایش پروتکل‌های جدید مورد استفاده قرار می‌گیرند. IP های کلاس D برای Multi Cast (چند پخشی) به کار می‌روند. برای تشخیص اینکه یک آدرس IP در کدام کلاس قرار دارد، کافیست به اولین عدد سمت چپ آن نگاه کنید و بر اساس مقادیر مذکور در جدول زیر، کلاس آنرا تشخیص دهید.



کلاس IP	محدوده IP (دهدهی)	محدوده IP (بیت)	تعداد شبکه	تعداد Host
A	0 127	00000000 01111111	2^7-2	2^{24}-2
B	128 191	10000000 10111111	2^{14}	2^{16}-2
C	192 223	11000000 11011111	2^{21}	2^8-2
D	224 239	11100000 11101111	–	–
E	240 255	11110000 11110111	–	–

۲-۲-۱ آدرس‌های خاص

آدرسهای خاص آدرسهایی هستند که کاربرد ویژه‌ای دارند و نمی‌توان آنها را به میزبانی در شبکه تخصیص داد، بطور کلی این آدرسها عبارتند از:

۱- تمام بیت‌ها صفر باشند.(یعنی خود شبکه یا خود میزبان). اگر بیت‌های مربوط به شماره شبکه را دست نخورده باقی بگذاریم و تمام بیت‌های مربوط به شماره میزبان را صفر قرار دهیم، آدرس IP بدست آمده را آدرس آن شبکه گویند. به عنوان مثال آدرس 192.168.11.10 را در نظر بگیرید، این آدرس در کلاس C قرار دارد، بنابراین ۲۴ بیت سمت چپ مربوط به شماره شبکه است و ۸ بیت (۱ بایت) سمت راست شماره میزبان در شبکه است که با صفر قرار دادن قسمت HostID آدرس شبکه 192.168.11.0 بدست می‌آید. اگر تمام بیتهای بخش NetID و HostID را صفر قرار دهیم، آدرس به دست آمده (0.0.0.0) به معنی آدرس خود میزبان (فرستنده) است، به عبارتی دیگر اگر آدرس IP

مقصد بسته‌ای 0.0.0.0 باشد، آن بسته بر روی شبکه نخواهد رفت. کاربرد این آدرس زمانی است که فرستنده بسته هنوز آدرس خود را نمی داند و آنرا بعنوان آدرس IP مبدا بسته‌های ارسالی خود درج می‌کند.

۲- تمام بیت‌ها یک باشند.(یعنی آدرس BroadCast و به معنی آن است که مقصد بسته تمام میزبانهای داخل آن شبکه می‌باشند) اگر بیت‌های مربوط به شماره شبکه را دست نخورده باقی بگذاریم و تمام بیت‌های مربوط به شماره میزبان را 1 قرار دهیم، آدرس IP بدست آمده را آدرس Broadcast آن شبکه گویند. به عنوان مثال آدرس 192.168.11.10 را در نظر بگیرید، این آدرس در کلاس C قرار دارد، بنابراین ۲۴ بیت سمت چپ مربوط به شماره شبکه است و ۸ بیت (۱ بایت) سمت راست شماره میزبان در شبکه است که با 1 قرار دادن تمام بیتهای قسمت HostID آدرس Broadcast شبکه 192.168.11.255 بدست می‌آید. اگر تمام بیتهای بخش NetID و HostID را 1 قرار دهیم، آدرس به دست آمده (255.255.255.255) به معنی آدرس Broadcast در تمام شبکه‌ها است، به عبارتی دیگر اگر آدرس IP مقصد بسته‌ای 255.255.255.255 باشد، آن بسته برای تمام میزبانهای همه شبکه‌ها ارسال شده است (البته در عمل، معمولا مسیریابها اجازه عبور بسته‌های Broadcast به خارج شبکه و برعکس را نمی‌دهند). کاربرد این آدرس زمانی است که فرستنده بسته هنوز آدرس خود را نمی‌داند و می‌خواهد بسته‌ای را برای تمام میزبانهای شبکه ارسال کند.

۳- آدرس IP (127.*.*.*) آدرس میزبانی را تعیین نمی‌کند بلکه به صورت قراردادی به عنوان آدرس " حلقه‌ی بازگشت" یا Loop Back جهت اهداف اشکال‌زدایی و نیز تست نرم‌افزارهای تحت شبکه کاربرد دارد است و به معنی آدرس همان میزبان است. وقتی آدرس مقصد بسته‌ای 127.*.*.* باشد (جای * هر عددی بین ۰-۲۵۵ می‌تواند باشد) پروتکل IP آن بسته را تحویل لایه پایین‌تر نمی‌دهد، بلکه آنرا دوباره به لایه بالایی (انتقال) برمی‌گرداند و لایه انتقال نیز تحویل لایه کاربرد می دهد، بدین ترتیب برنامه لایه کاربرد، تصور می‌کند که داده‌ای از شبکه دریافت شده است.

- نکته: در هر محدوده آدرس IP، دو آدرس اول و آخر محدوده (یعنی تمام بیت‌های بخش HostID صفر و یا تمام بیت‌های بخش HostID برابر ۱) را نمی‌توان به هیچ میزبانی اختصاص داد زیرا به ترتیب آدرس خود شبکه و آدرس همه‌پخشی در شبکه می باشند.

۲-۳ آدرس‌دهی بدون کلاس (CIDR): assless InterDomain Routing

در این شیوه‌ی آدرس‌دهی IP، مرز بین NetID و HostID از پیش تعین شده نیست (برخلاف کلاس‌های IP،) بلکه یک عدد ۳۲ بیتی دیگری به نام الگوی زیر شبکه یا Subnet Mask وجود دارد که مشخص می‌کند چه بخشی از آدرس IP مربوط به NetID و چه بخشی مربوط به HostID است.

برای به دست آوردن آدرس شبکه، آدرس IP و Subnet Mask با هم and منطقی می‌شوند.(Boolean and) حاصل آدرس شبکه است.

- نکته: بیت‌های ۱ درSubnet Mask مشخص‌کننده‌ی بیت‌های مربوط به NetID هستند و بیت‌های صفر در آن مشخص‌کننده‌ی بیت‌های مربوط به HostID در آدرس IP هستند.
- نکته:

0 and y = 0

1 and y = y

مثال:

IP : 68.101.29.4

Subnet Mask : 255.0.0.0

NetID : 68.0.0.0

و به صورت باینری:

01000100 . 01100101 . 00011101 . 00000100

11111111 . 00000000 . 00000000 . 00000000

01000100 . 00000000 . 00000000 . 00000000

- نکته: اگر تعداد بیت‌های ۱ در **subnet mask** بعد از علامت / جلوی آدرس **IP** نوشته شود، این فرمت نمایش را فرمت پیشوندی یا **Prefix** گویند. بعنوان نمونه، آدرس **IP** و ماسک زیرشبکه آنرا در مثال قبل، می‌توان بصورت **68.101.29.4/8** می‌توان نمایش داد.

۲-۳-۱ کاربردهای عمده‌ی CIDR

- تقسیم یک شبکه به چند زیرشبکه (Subnetting)
- ترکیب چند شبکه و تشکیل یک شبکه‌ی واحد (Supernetting)

۲-۳-۱-۱ Subnetting

مثال برای Subnetting: می‌خواهیم شبکه‌ی زیر را به ۸ زیرشبکه تقسیم کنیم: 172.31.0.0/16

الف) محاسبه کنید Subnet Maskای را که این شبکه را به ۸ زیرشبکه تقسیم کند.

ب) آدرس ۸ زیر شبکه را به دست آورید.

ج) آدرس‌های Broad Cast آن‌ها را به دست آورید.

د) محدوده‌ی مجاز آدرس‌های هر زیر شبکه را به دست آورید.

جواب:

الف) برای ایجاد ۸ آدرس زیر شبکه به ۳ بیت نیاز داریم یعنی باید ۳ بیت از HostID کم کنیم و به NetID اضافه نماییم.

$2^3 = 8$ 3 bit

16+3=19

172.31.0.0/19

Subnet Mask: 255.255.224.0 11100000=224

ب و ج)

172.31.00000000.00000000	172.31.0.0	172.31.31.255
172.31.00100000.00000000	172.31.32.0	172.31.63.255
172.31.01000000.00000000	172.31.64.0	172.31.95.255
172.31.01100000.00000000	172.31.96.0	172.31.127.255
172.31.10000000.00000000	172.31.128.0	172.31.159.255
172.31.10100000.00000000	172.31.160.0	172.31.191.255
172.31.11000000.00000000	172.31.192.0	172.31.223.255
172.31.11100000.00000000	172.31.224.0	172.31.255.255

د)

172.31.0.1 تا 172.31.31.254

172.31.32.1 تا 172.31.63.254

172.31.64.1 تا 172.31.95.254

172.31.96.1 تا 172.31.127.254

172.31.128.1 تا 172.31.159.254

172.31.160.1 تا 172.31.191.254

172.31.192.1 تا 172.31.223.254

172.31.224.1 تا 172.31.255.254

۲-۱-۳-۲ Supernetting

مثال برای Super netting: ۴ آدرس در زیر داده شده است بزرگترین Subnet Mask را پیدا کنید که این چهار آدرس را به یک شبکه‌ی واحد تبدیل کند.

192.168.160.0/24
192.168.176.0/24
192.168.180.0/24
192.168.191.0/24

جواب: باید یک Subnet Mask طراحی کنیم که با هرکدام از آن‌ها and شود یک جواب واحد بدست آید. قسمت‌های مشترک همه‌ی آدرس‌ها را یکسان در نظر می‌گیریم، یعنی در مثال بالا فقط ۸ بیت سوم است که با هم متفاوتند. پس آن‌ها را به مبنای ۲ برده و همین عمل اشتراک را در مبنای ۲ انجام می‌دهیم یعنی از هر ۴ عدد در مبنای ۲ مشترک‌ها را برای Subnet انتخاب می‌کنیم. به این صورت که قسمت‌های مشترک آدرس‌ها را یک و قسمت‌هایی که مشترک نیستند را صفر می‌گذاریم.

160 10100000
176 10110000
180 10110100
191 10111111

11100000 = 224

Subnet Mask: 255.255.224.0

آدرس شبکه: 192.168.160.0/19

NetID:

- مشخص شدن محدوده‌ی آدرس‌های IP شبکه (تخصیص آدرس‌ها را ساده‌تر می‌کند.)
- خلاصه‌سازی جداول مسیریابی در مسیریاب‌های میانی و بین راه
- می‌توان تشخیص داد که دو میزبان (فرستنده و گیرنده) در یک شبکه هستند یا در دو شبکه‌ی مجزا

۲-۳-۲ Default Gateway (دروازه‌ی پیش‌فرض)

کار مسیریابی را انجام می‌دهد به این صورت که اگر یک میزبان بخواهد به یک میزبان دیگر داده ارسال کند به طوری که فرستنده و گیرنده در دو شبکه‌ی مجزا قرار داشته باشند(یعنی NetID آن‌ها با هم متفاوت باشد)، فرستنده داده را به دروازه‌ی پیش‌فرض ارسال می‌کند (یعنی آدرس MAC دروازه‌ی پیش‌فرض را روی فریم ارسالی خود قرار می‌دهد ولی آدرس **IP** مقصد نهایی بر روی بسته درج می‌شود) و دروازه‌ی پیش‌فرض آن را به سمت گیرنده (مقصد) هدایت می‌کند.

نکته: وقتی پروتکل IP می‌خواهد یک بسته‌ی اطلاعاتی را روی شبکه بفرستد باید به نحوی آدرس فیزیکی اولین ماشینی که با آن باید ارتباط برقرار کند را بداند، که این ماشین می‌تواند مسیریاب پیش‌فرض یا آدرس فیزیکی مقصد روی همان شبکه‌ی محلی باشد.

نکته:

آدرس IP گیرنده در کل مسیر ثابت است ولی آدرس MAC گیرنده، گام به گام (**Hop by Hop**) تغییر می‌کند.

۲-۳-۳ آدرس‌های معتبر (Valid IP) و آدرس‌های شخصی (Private IP)

آدرس‌های معتبر IP آدرس‌هایی هستند که در کل شبکه اینترنت شناخته شده هستند و در مراجع مربوطه مالکیت IP ثبت شده است و مسیریاب‌ها می‌توانند میسر مناسب به آدرس‌های معتبر را پیدا کنند.

آدرس‌های Private IP آدرس‌هایی هستند که تنها در شبکه محلی معتبر هستند و در اینترنت اعتبار ندارند. این آدرس‌ها برای شبکه‌هایی طراحی شده که نمی‌خواهند بطور مستقیم به اینترنت متصل باشند (اتصال این شبکه‌ها به

اینترنت از طریق Gateway و ترجمه آدرس و یا از طریق پروکسی صورت می‌گیرد). هرگاه بسته با آدرس مقصد یک IP نامعتبر به یک مسیریاب در اینترنت برسد، دور ریخته می‌شود و به مقصد نمی‌رسد.

محدوده آدرس‌های شخصی که در استاندارد تعریف شده است عبارتند از:

10.0.0.0/ 8

176.16.0.0/ 12 (یعنی 176.16.0.0 تا 176.31.255.255)

192.168.0.0/ 16

نکته:

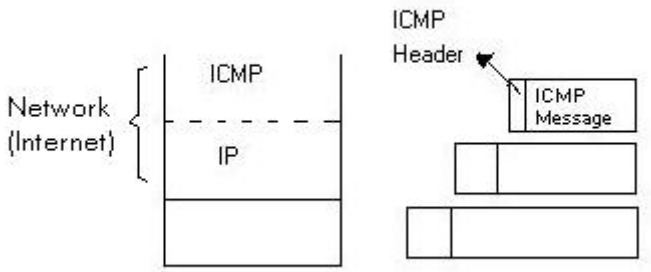
- پروتکل IP یک پروتکل بدون اتصال و نامطمئن است و در هنگام بروز هرگونه خطا، پروتکل IP هیچ گونه اطلاعاتی به فرستنده و در مورد سرنوشت بسته نخواهد داد.
- عدم گزارش خطا به تولیدکننده یک بسته، منجر به تکرار خطا و حمل بیهوده‌ی بسته‌ها می‌شود.

۴-۲ پروتکل ICMP:

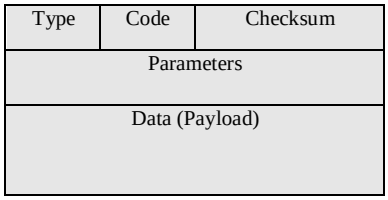
Internet Control Message Protocol

پروتکل مدیریتی (کنترلی) لایه‌ی IP است و در کنار پروتکل IP ، برای گزارش انواع خطا و ارسال پیام به مبدا بسته در هنگام بروز مشکلات، استفاده می‌شود. در حقیقت ICMP یک سیستم گزارش خطاست که بر روی پروتکل IP نصب می‌شود تا در صورت بروز خطا به فرستنده پیام مناسب بدهد. در واقع مانع از ادامه یافتن خطا می‌شود ولی خطا تصحیح نمی‌کند.

این پروتکل اشکالات موجود را در قالب یک سری پیام گزارش می‌کند. هر پیام در داخل یک بسته‌ی IP حمل می‌شود.



ساختار کلی پیام ICMP:



شکل ۲-۲: ساختار پیام ICMP

Type:

داخل این فیلد یک عدد قرار می‌گیرد که نوع پیام را مشخص می‌کند و ساختار فیلدهای پارامتر و دیتا به این فیلد بستگی دارد. به طور مثال ممکن است نوع پیام Destination Unreachable باشد.

Code: هر نوع پیام ممکن است چند زیرگروه داشته باشد. مثلا در مثال بالا ممکن است شبکه غیرقابل دسترس باشد و یا Host مورد نظر در دسترس نباشد.

Checksum: همانند IP عمل می‌کند. برای کنترل خطا.

Parameters: گاه در یک سری از پیام‌ها استفاده می‌شود و گاه ممکن است هیچ نوع کاربردی نداشته باشد و خالی بماند.

Data: داده‌ای که قرار است ارسال شود.

انواع پیام‌های ICMP:

- Destination Unreachable: مقصد غیر قابل دسترس است.
- Time Exceed: یعنی در زمان پیش‌بینی شده‌ی TTL به مقصد نمی‌رسد پس دور ریخته می‌شود و در نتیجه یک پیام ICMP فرستاده می‌شود.
- Source Quench: با دریافت این پیام مبدا یا مسیریاب باید حجم و سرعت ارسال بسته‌ها را پایین بیاورد.
- Redirect: زمانی ارسال می‌شود که یکی از مسیریاب‌های شبکه بسته‌ی دریافتی‌اش را باز باید به همان مسیریاب یا گره‌ای که بسته را از آن دریافت کرده است بازگرداند.

- Echo Request & Echo Reply: در Ping استفاده می‌شود، یعنی فرستنده این پیام را می‌فرستد(Echo Request) و گیرنده همان پیام را بازمی‌گرداند(Echo Reply)
- Timestamp Request & Timestamp Reply: علاوه بر مورد بالا زمان دریافت و ارسال مجدد بسته را نیز درج می‌کند.

در دستورات Echo Request ,Echo Reply , Timestamp Request, Timestamp Reply برای هرکدام یک شماره ترتیب در یک فیلد جداگانه قرار می‌دهند تا بفهمند که کدام پاسخ به کدام سوال و درخواست مربوط می‌شود.

۵-۲ پروتکل ARP:

Address Resolution Protocol

هرگاه بخواهیم آدرس MAC یک کامپیوتر را از روی آدرس IP آن به دست آوریم از پروتکل ARP استفاده می‌کنیم برای این‌کار کامپیوتر فرستنده یک ARP Request تولید کرده و داخل آن پیامی به این مضمون (چه کسی آدرس MAC کامپیوتری با آدرس IP ... را دارد؟) را در شبکه Broad Cast می‌نماید. (یعنی آدرس MAC آن را ۱ می‌گذارد.) تمام کامپیوترهای شبکه این پیام را دریافت کرده و تنها کامپیوتری به آن پاسخ می‌دهد که صاحب آدرس IP فوق است. و گیرنده یک پیام ARP Reply تولید می‌کند و آدرس MAC خود را در آن قرار می‌دهد و آن را به تولید کننده‌ی پیام ARP Request ارسال می‌کند.

در هنگام به کارگیری پروتکل ARP وقتی آدرس فیزیکی مربوط به ایستگاهی روی شبکه سوال می‌شود، ممکن است آن ایستگاه روی شبکه‌ی محلی دیگری باشد و بالطبع پاسخی نمی‌رسد. در چنین حالتی دو راه حل وجود دارد:

الف) وقتی مسیریابی که به آن شبکه متصل است می‌بیند آدرس مقصدی که توسط ARP سوال شده روی یک شبکه‌ی محلی دیگر واقع است در پاسخ به آن، آدرس فیزیکی خودش را به ایستگاه فرستنده ارسال می‌کند به این روش **Proxy ARP** گفته می‌شود.

ب) ایستگاه‌ها خود موظفند که محلی یا خارجی بودن ماشین مقصد را با توجه به الگوی زیر شبکه تشخیص داده و در صورت خارجی بودن آدرس فیزیکی یک مسیریاب مناسب را انتخاب کنند.

ARP Table:

آدرس‌های به دست آمده از طریق پروتکل‌های ARP در این جدول ذخیره می‌شوند تا در دفعات بعدی برای به دست آوردن MAC نیاز به عملیات ARP نداشته باشیم (ARP cache) که باعث بالارفتن سرعت پروتکل ARP می‌شود

ARP cache هر دقیقه یک بار Update می‌شود.

IP	MAC	Expire
192.168.1.18	EF-FB-AB-00-AA	...
192.168.1.31	ED-99-09-33-00-09	...

۲-۶ پروتکل DHCP:

Dynamic Host Configuration Protocol

- پروتکلی است جهت تخصیص دادن آدرس‌های IP و سایر تنظیمات شبکه (نظیر دروازه‌ی پیش‌فرض، الگوی زیرشبکه، آدرس سرور DNS، آدرس سرور WINS و ...) به تجهیزات شبکه به صورت خودکار(Automatic) و پویا.
- آدرس IP می‌تواند به صورت دائمی تخصیص بیابد یا برای مدت زمانی معین در اختیار Client قرار بگیرد (Lease)
- این پروتکل بر پایه‌ی پروتکل قدیمی‌تر Bootp ، ایجاد شده و از پروتکل UDP جهت انتقال پیام‌های خود استفاده می‌کند.
- این پروتکل نیز ماهیت Client/Serverای دارد، سرور روی پورت UDP Port 67 و Client بر روی UDP Port 68 ، این پروتکل را اجرا می‌کند.

۲-۶-۱ مکانیزم کاری DHCP

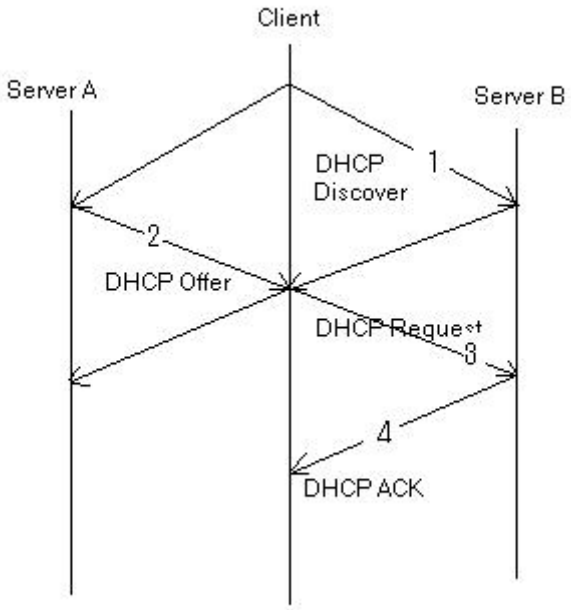
۱- Client در هنگام بوت شدن، یک پیغام DHCP Discover تولید کرده و آن را در شبکه Broad Cast می‌کند.(فاز شناسایی تمام DHCP Serverهای شبکه)

۲- سپس تمام DHCP Serverهای شبکه، آدرس پیشنهادی خود را درون یک پیام به Client ارسال می‌کنند.

۳- Client پس از جمع‌آوری تمام پیشنهادها، یکی را انتخاب کرده و یک پیام DHCP Request تولید می‌کند و آدرس را از سرور درخواست می‌نماید. این پیام در شبکه Broad Cast می‌شود(جهت اطلاع تمام سرورها)

۴- سروری که Client به آن درخواست داده، با دادن پیام DHCP ACK به صورت Uni Cast ، IP را به Client تخصیص می‌دهد. در اینجا مراحل تخصیص آدرس کامل شده است.

۵- Client می‌تواند با دادن درخواست DHCP Release به سرور، IP گرفته شده را آزاد کند.



شکل ۲-۳: فرایند تخصیص IP در DHCP

۲-۶-۲ مکانیزم تمدید IP در DHCP

زمان **T**: حداکثر زمان تعیین شده برای اجاره‌ی IP

زمان $\mathbf{T_1}$: معمولا 1/2 زمان T است.

زمان $\mathbf{T_2}$: معمولا 7/8 زمان T است.

- پس از زمان T_1 ، Client سعی می‌کند تا با ارسال پیام DHCP Request به سروری که IP را از آن اجاره کرده، مدت زمان اجاره را تمدید کند. اگر سرور در پاسخ به این درخواست DHCP ACK بفرستد، IP برای مدت زمان معین تعیین شده، دوباره در اختیار Client باقی می‌ماند.
- در صورتی که زمان T_2 سپری شود، Client موفق به تمدید اجاره‌ی IP از سرور نشود، یک پیام به تمام سرورها به صورت Broad Cast ارسال می‌کند تا IP جدیدی دریافت کند.
- در صورتی که مدت تعیین شده پایان یابد، IP از Client پس گرفته می‌شود.

۲-۶-۳ DHCP Relay

معمولا مسیریاب‌ها به پیام‌های Broad Cast اجازه عبور نمی‌دهند (از جمله پیام‌های DHCP). بنابراین اگـر لازم بود که به nodeهای یک شبکه که توسط Routerها به چندین زیرشبکه تقسیم شده است، توسط DHCP ، آدرس IP به صورت خودکار تخصیص داده شود مسیریاب‌ها باید پیام‌های DHCP را به سمت DHCP Server عبور دهند. به این کار DHCP Relay گویند.(مسیریاب پیام DHCP را به صورت Uni Cast به سرور می‌فرستد.)

تنظیمات DHCP Relay در مسیریاب‌های CISCO با دستور IP Helper صورت می‌گیرد.

نکته:

پروتکل RARP برعکس پروتکل ARP ، MAC Address را به IP تبدیل می‌کند.

فصل سوم

۳ مسیریابی در شبکه:

تعریف مسیریابی: پیدا کردن مسیر بهینه از مبدا به مقصد اصلی‌ترین وظیفه‌ی الگوریتم مسیریابی است به گونه‌ای که هزینه‌ی کل مسیر حداقل شود(هزینه ممکن است تعداد هاب‌ها، طول مسیر، پهنای باند و... باشد)

مسیریابی در دو بخش صورت می‌گیرد.

۱- Routing
۲- Forwarding

Routing:

الگوریتم‌های مسیریابی را اجرا می‌کنند و اطلاعات شبکه بین مسیریاب‌ها مبادله می‌شود و بر اساس این اطلاعات جداول مسیریابی را تشکیل می‌دهند. معمولا بطور پیوسته در حال اجرا است یعنی به طور مثال هر چند ثانیه یک بار اطلاعات را بین یکدیگر رد و بدل می‌کنند.

Forwarding:

در این فاز تنها، پورت خروجی بر اساس اطلاعات موجود در جداول مسیریابی انتخاب می‌شود فاز Forwarding به صورت همیشگی نیست و فقط زمانی شروع می‌شود که یک بسته به مسیریاب برسد و قرار است که پورت خروجی‌اش انتخاب شود.

۳-۱ روش‌های عمده‌ی مسیریابی در شبکه‌های کامپیوتری

۱- مدار مجازی (Virtual Circuit Switching) **VC**

در این روش برای اولین ارسال عملیات مسیریابی انجام می‌گیرد و یک مسیر بین فرستنده و گیرنده برقرار می‌شود و بسته‌های بعدی همگی از این مسیر عبور خواهند کرد.

۲- دیتاگرام یا سوئیچینگ بسته

در این روش به ازای هر بسته عملیات مسیریابی صورت می‌گیرد و ممکن است مسیر بسته‌های مختلف متفاوت باشد. این مسیریابی بر اساس پارامترهای شبکه انجام می‌شود.

۳-۲ تقسیم‌بندی الگوریتم‌های مسیریابی

۳-۲-۱ تقسیم‌بندی روش‌های مسیریابی بر اساس هوشمندی الگوریتم‌ها و روش تصمیم‌گیری

- ایستا(Static):

در الگوریتم‌های ایستا مسیر به صورت دستی تنظیم می‌شود و تمام مسیریابی‌ها از روی مسیرهای تنظیم شده صورت می‌گیرد و هیچ اعتنایی به توپولوژی شبکه و وضعیت ترافیکی مسیرها صورت نمی‌گیرد.

- پویا (Dynamic):

در الگوریتم پویا مسیریابی بر اساس آخرین وضعیت توپولوژی شبکه و ترافیک شبکه انجام می‌شود در این نوع الگوریتم‌ها جداول مسیریابی هر T ثانیه یک بار Update می‌شوند.

۳-۲-۲ تقسیم‌بندی الگوریتم‌های مسیریابی بر اساس جمع‌آوری و پردازش اطلاعات زیرشبکه‌ها

- الگوریتم‌های متمرکز(سراسری):

به الگوریتم‌هایی که برای مسیریابی به اطلاعات کاملی از شبکه و هزینه‌ی ارتباط بین دو مسیریاب نیازمندند، الگوریتم‌های متمرکز گفته می‌شود. این الگوریتم‌ها را Link State نیز می‌گویند.

- الگوریتم‌های غیرمتمرکز:

در این الگوریتم‌ها مسیریاب اطلاعات کاملی از شبکه ندارد بلکه فقط قادر است هزینه‌ی ارتباط به مسیریاب‌هایی که به طور مستقیم با آن‌ها در ارتباط است را به دست آورد. هر مسیریاب جداول مسیریابی خود را برای مسیریاب‌های مجاور ارسال می‌کند.(Distance Vector بردار فاصله)

۳-۲-۳ تقسیم‌بندی الگوریتم‌های مسیریابی بر اساس زمان اجرا

- **پروتکل‌های مسیریابی Proactive (پیش‌دستانه):**

در پروتکل‌های مسیریابی proactive، اطلاعات کنترلی مسیریابی در دوره‌های معین زمانی، مبادله می‌شوند تا گره‌ها قادر باشند که اطلاعات مناسبی از توپولوژی شبکه بدست آورند. در دسترس بودن فوری مسیرها در آغاز برقراری ارتباط بین گره‌ها، از مزایای اصلی این نوع پروتکلها می‌باشد.

- **پروتکل‌های مسیریابی Reactive (واکنشی):**

پروتکلهای مسیریابی واکنشی یا reactive به روش پاسخ به تقاضا (On demand) عمل می‌کنند. اطلاعات مسیریابی تنها زمانی ارسال می‌شوند که یک گره، داده‌ای برای ارسال دارد ولی مسیر مناسبی در اختیار ندارد. این نوع پروتکل‌های مسیریابی برای شبکه‌های بزرگ مناسب هستند و ترافیک کنترلی ضروری برای مسیریابی، کمتر از پروتکلهای مسیریابی proactive است.

۳-۳ مسیریابی سیل‌آسا (Flooding)

در مسیریابی سیل‌آسا هر بسته‌ی ورودی روی تمام لینک‌های خروجی غیر از لینکی که بسته از آن وارد شده است ارسال می‌شود. تمام مسیریاب‌های بین راه نیز این کار را انجام می‌دهند تا بسته به مقصد برسد. و کاربرد آن بیشتر برای ارسال‌های Broad Cast یا پخش فراگیر است. و از خصوصیات آن این است که سریع‌ترین الگوریتم مسیریابی است. و اگر مسیری وجود داشته باشد آن را پیدا می‌کند. ولی دارای اشکالاتی نیز می‌باشد: تحمیل بار زیاد روی شبکه، ممکن است بیش از یک نسخه به مقصد برسد و نیز ممکن است حلقه ایجاد شود(که یک سری الگوریتم‌هایی برای جلوگیری از این روش وجود دارد.)

۴-۳ الگوریتم‌های LS (Link State)

این نوع الگوریتم‌ها به جمع‌آوری اطلاعات در مورد مسیریاب‌های مجاور می‌پردازند و اطلاعات جداول مسیریابی را برای تمامی مسیریاب‌های شبکه ارسال می‌کنند.

در الگوریتم‌های LS هر الگوریتم باید پنج عمل زیر را انجام دهد:

۱- مسیریاب‌های مجاور را به صورت فیزیکی به آن‌ها متصل است شناسایی کرده و آدرس آن‌ها را به دست آورد .
۲- تاخیر (هزینه) مسیریاب‌های مجاور خود را اندازه‌گیری نماید.
۳- یک بسته بسازد و تمامی اطلاعاتی را که از مسیریاب‌های مجاور خود به دست آورده است را در آن قرار دهد.
۴- بسته‌های ایجاد شده را برای تمامی مسیریاب‌های شبکه ارسال کند.(با استفاده از روش سیل‌آسا) همچنین بسته‌هایی را که از مسیریاب‌های دیگر می‌رسد دریافت و ذخیره نماید.
۵- با استفاده از الگوریتمی مناسب بهینه‌ترین مسیر را بین هر دو مسیریاب در شبکه به دست آورد.

راه حل بروز رسانی جداول:

- به صورت دوره‌ای (در زمان‌های خاص)
- در صورت بروز یک رویداد (مثلا تغییرات در وضعیت شبکه)

محتوای بسته‌های LS:

۱- آدرس جهانی مسیریاب تولید کننده‌ی بسته
۲- شماره ترتیب هر بسته (جهت تشخیص قدیمی و جدید بودن و تکراری نبودن بسته)
۳- طول عمر بسته (بسته‌هایی که سرگردان هستند را بالاخره از بین می‌برد.)
۴- آدرس مسیریاب‌های مجاور و هزینه‌ی رسیدن به آن‌ها

نکته: در الگوریتم LS در شبکه‌هایی که دارای n مسیریاب و هر مسیریاب حداکثر دارای k کانال ورودی/ خروجی است در بدترین حالت به فضای n*k رکورد اطلاعاتی برای ذخیره‌سازی جداول LS نیاز خواهد بود که برای شبکه‌های وسیع با هزاران مسیریاب مشکل‌ساز خواهد شد.

۳-۵ الگوریتم DV (Distance Vector)

در این الگوریتم‌ها هر مسیریاب تخمینی از هزینه‌ی رسیدن به تمام مسیریاب‌های دیگر شبکه را به دست می‌آورد و اطلاعات جمع‌آوری شده‌ی خود را تنها به مسیریاب‌های مجاور خود ارسال می‌کند. در جدول مسیریابی این الگوریتم‌ها به ازای هر مسیریاب در شبکه یک رکورد وجود دارد این رکوردها دارای ۲ فیلد پورت خروجی و هزینه‌ی تقریبی برای رسیدن به یک مقصد خاص است.

مراحل الگوریتم DV:

۱- هر مسیریاب هزینه‌ی خطوطی را که به صورت فیزیکی با مسیریاب‌های دیگر دارد حساب کرده و جدول خود می‌نویسد هزینه‌ی خطوطی که مسیریاب مستقیما با آن‌ها در ارتباط نیست در این جدول بی‌نهایت در نظر گرفته می‌شود.
۲- هر مسیریاب به صورت دوره‌ای (در زمان‌های مشخص) جدول مسیریابی خود را برای مسیریاب‌های مجاور ارسال می‌کند.
۳- هر مسیریاب پس از دریافت جداول مسیریابی از مسیریاب‌های همسایه، طبق یک الگوریتم ساده هزینه‌ی مسیرها را محاسبه می‌کند

مشکل پروتکل DV عدم همگرایی سریع جداول مسیریابی در هنگام خرابی یک مسیر است(شمارش تا بی‌نهایت)

راه‌حل: وقتی یک مسیریاب می‌خواهد اطلاعاتش را به همسایه‌اش بدهد هزینه‌ی رسیدن به آن‌هایی را که قطعا باید از همان مسیریاب‌ها بگذرند، اعلام نمی‌کند.

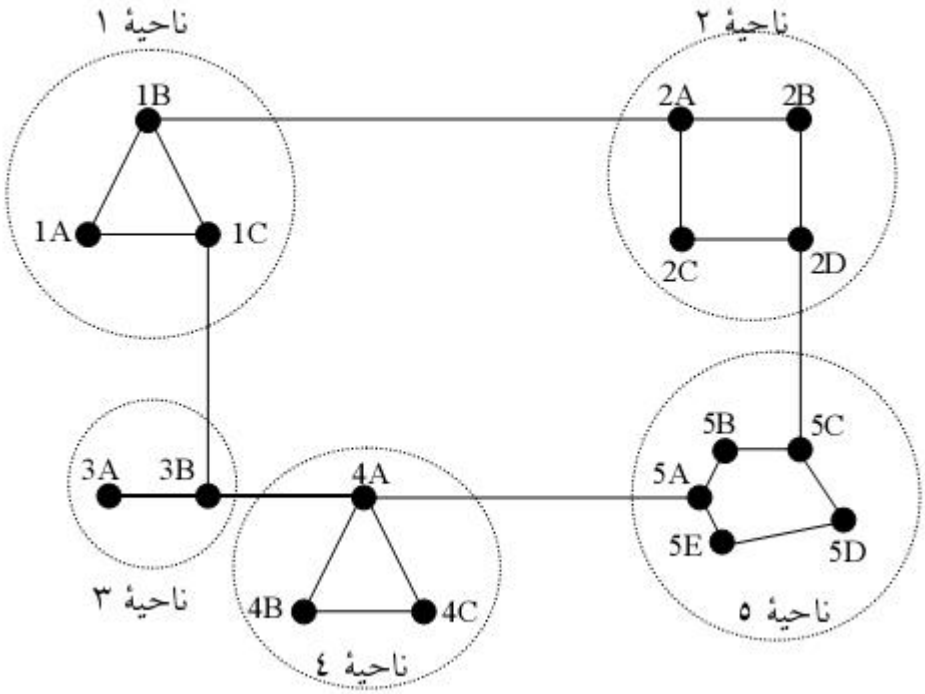
الگوریتم DV در عین سادگی، پویاست و تغییرات ترافیکی شبکه با زمان را در جداول مسیریابی دخالت می‌دهد.

حجم جدولی که باید هر مسیریاب در خود نگه دارد (درجه۱) به ازای n مسیریاب فقط n رکورد.

نکته: الگوریتم DV در شبکه‌های کوچک خوب جواب می‌دهد زیرا اگر تعداد nodeها افزایش یابد تعداد جداول هم افزایش پیدا می‌کند. ولی الگوریتم LS در شبکه‌های بزرگ استفاده می‌شود.

۳-۶ مسیریابی سلسله‌مراتبی

در این نوع مسیریابی، مسیریاب‌ها در گروه‌هایی به نام "ناحیه" دسته‌بندی می‌شوند و هر مسیریاب فقط ۱- نواحی و ۲- مسیریاب‌های درون ناحیه‌ی خود را می‌شناسد و هیچ اطلاعی در مورد مسیریاب‌های درون نواحی دیگر ندارد.



شکل ۳-۱: مسیریابی سلسله مراتبی

مقصد	خطّ	هزینه
1A	–	–
1B	1B	1
1C	1C	1
Region	1B	2
Region	1C	2
Region	1C	3
Region	1C	4

جدول مسیریابی 1A

۳-۶-۱ مسیریابی در اینترنت

- IGP (Interior Gateway Protocol) مسیریابی درون ناحیه‌ای
- EGP (Exterior Gateway Protocol) مسیریابی بین ناحیه‌ای

اینترنت از مجموعه‌ای از شبکه‌های "خودمختار" و مستقل (AS) تشکیل شده است. هر AS تحت مـدیریت و سرپرستی یک نهاد یا سازمان قرار دارد و به صورت مستقل عمل می‌کند. (Autonomous Systems)

۳-۶-۲ مراحل مسیریابی در اینترنت (میسریابی سلسله مراتبی)

۱- مسیریابی در درون شبکه (داخل ناحیه‌ای) تا رسیدن به مسیریاب مرزی (مسیریاب مرزی، مسیریابی است که ارتباط بین دو شبکه‌ی خودمختار(ناحیه) را برقرار می‌کندو تمامی ارتباطات بین شبکه‌ای از طریق آن انجام می‌شود.Border Router یا Border Gateway.)

۲- مسیریابی روی خطوط ارتباطی بین شبکه‌ای تا رسیدن به ناحیه‌ی مقصد

۳- مسیریابی درون ناحیه‌ی مقصد تا رسیدن به ماشین مقصد

نمونه‌ای از الگوریتم‌های LS: OSPF پروتکل مسیریابی درونی که پروتکل پرسابقه‌ی مسیریابی در اینترنت است.(Open Shortest Path First)

نمونه‌ای از الگوریتم‌های DV: RIP پروتکل مسیریابی درونی(Routing Information Protocol)

BGP (Border Gateway Protocol) پروتکل مسیریابی برونی):

پروتکل مسیریابی بین ASهاست. مسیریابی برونی نه تنها تابع شرایط ترافیکی، توپولوژی، پهنای باند و سرعت پردازش مسیریاب‌هاست بلکه از یک سری سیاست‌های اقتصادی، امنیتی و ملی تاثیر می‌پذیرد. به عنوان مثال کشور A برای ارسال اطلاعات به کشور C نمی‌خواهد که اطلاعات از کشور B عبور کند این سیاست ممکن است مسیر ارسال اطلاعات از A به C را تغییر دهد.

در پروتکل BGP به جای اینکه جداول مسیریابی و هزینه‌ها بین مسیریاب‌های مجاور مبادله شود، در بازه‌های زمانی t ثانیه فهرستی از مسیرهای کامل بین هر دو مسیریاب در شبکه برای مسیریاب‌های مجاور ارسال می‌شود.(بدون تعیین هزینه)

فصل چهارم

۴ لایه انتقال در شبکه‌ی اینترنت

۴-۱ وظیفه‌ی لایه‌ی انتقال:

فراهم آوردن خدمات سازماندهی شده، مطمئن و مبتنی بر اصول سیستم عامل، برای برنامه‌های کاربردی در لایه‌ی بالاتر است، به گونه‌ای که مشکلات و ناکار آمدی لایه‌ی شبکه (مثلا پروتکلIP) جبران و ترمیم شود. خدماتی که لایه‌ی انتقال به لایه‌ی بالاتر ارائه می‌کند باید به‌گونه‌ای باشد که برنامه‌نویس از درگیری با جزئیات زیرشبکه و مشکلات کانال‌های انتقال و مسائلی از این قبیل دور باشد.

۴-۲ پروتکل TCP:

پروتکل TCP عمده‌ترین پروتکل مورد استفاده لایه انتقال در اینترنت است. از اینرو، این پروتکل باید وظایف لایه انتقال را انجام دهد و خدمات پروتکل IP (در لایه شبکه) را کامل کند.

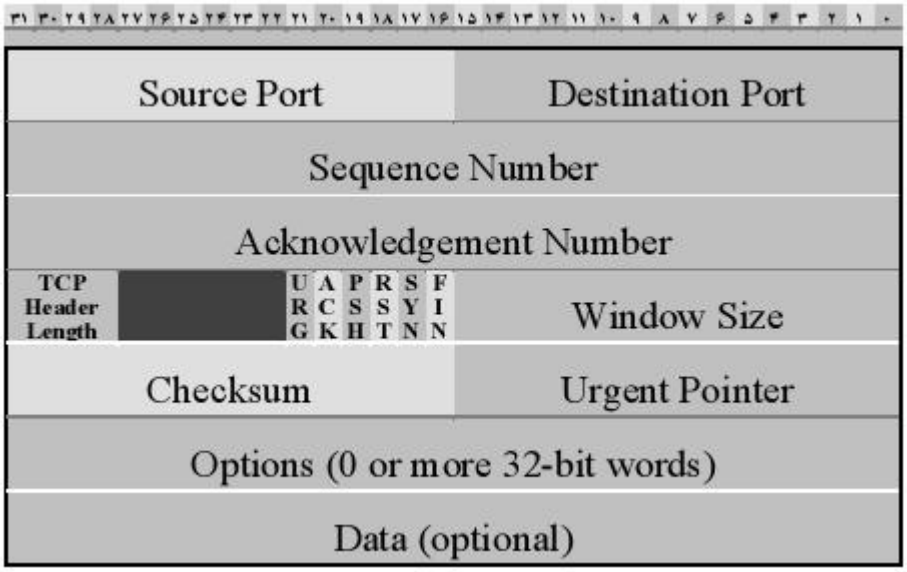
۴-۲-۱ کاستی‌هایIP :

- عدم آگاهی از آمادگی گیرنده
- عدم حفظ ترتیب بسته‌ها در گیرنده
- IP هیچ مکانیزمی جهت توزیع داده‌ها بین پروسه‌های مختلف ندارد.
- عدم هماهنگی سرعت ارسال و دریافت بین فرستنده و گیرنده
- عدم اطمینان از رسیدن بسته‌ها به مقصد
- عدم تشخیص بسته‌های تکراری

۴-۲-۲ راهکار TCP:

- دست‌تکانی سه مرحله‌ای(Three Ways Hand Shaking)
- درج شماره ترتیب روی بسته‌ها (Seq-No)
- شماره پورت
- اعلام بافر خالی گیرنده (توسطWindow-Size)
- ارسال تایید دریافت توسط گیرنده(ACK)
- درج شماره ترتیب

ساختار سگمنت پروتکل TCP:



شکل ۴-۱: ساختار سگمنت TCP

Source Port:

شماره‌ی شناسایی برنامه‌ای است که در ماشین مبدا، داده‌ها را تولید می‌کند.

Destination Port:

شماره‌ی شناسایی برنامه‌ای(یا پروسه‌ای) است که باید داده‌ها به آن تحویل داده شود.

Sequence Number:

۱- جهت مشخص کردن ترتیب بسته‌های ارسالی

۲- جهت تشخیص تکراری بودن یا جدید بودن بسته‌ی دریافتی

شماره ترتیب برحسب شماره‌ی آخرین بایتی است که در بسته‌ی جاری قرار گرفته و ارسال شده است.

شماره ترتیب اولین بایت، از صفر شروع نمی‌شود بلکه از یک عدد تصادفی که در هنگام برقراری ارتباط به اطلاع طرفین می‌رسد شروع خواهد شد.

Acknowledgement Number:

شماره ترتیب بایتی است که فرستنده‌ی بسته منتظر دریافت آن است مـثلا اگـر Ack=1800 باشـد یعنـی از رشته‌ی داده‌ها، تا شماره‌ی 1800 را کامل دریافت کرده است و منتظر بایت‌های 1801 به بعد می‌باشد.

TCP Header Length:

طول سرآیند بسته‌ی TCP را مشخص کرده و واحد آن ۳۲ بیتی است. عددی که در این فیلد قرار مـی‌گیـرد می‌تواند به عنوان یک اشاره‌گر، محل شروع داده‌ها را در یک بسته‌ی TCP تعیین کند.

نکته: در قسمت تیره شده ۶ بیت فضای خالی و بدون استفاده برای استفاده در آینده رزرو شده است.

بیت‌های Flag:

هر کدام نقض یک بیت پرچم را که معنا و کاربرد مختلفی دارند بازی می‌کند.

URG (Urgent):

در صورتی که این بیت مقدار ۱ داشته باشد، معین می‌کند که در فیلد Urgent Pointer مقداری معتبـر قـرار دارد که باید مورد پردازش قرار گیرد و اگر مقدار صفر باشد یعنی این فیلد شامل مقدار معتبر و قابل استفاده‌ای نیست و از آن چشم‌پوشی می‌شود.

ACK:

اگر این بیت ۱ باشد مشخص می‌کند که مقدار داخـل Acknowledgement Number معتبـر اسـت و موقـع برقراری اتصال مورد استفاده قرار می‌گیرد.

PSH (Push):

در صورت ۱ بودن این بیت، فرستنده از گیرنده تقاضا می‌کند داده‌های موجود در این بسته را بافر نکندو سریعا آن را جهت پردازش به برنامه‌ی کاربردی دهد.

:(Reset) RST

در صورت ۱ بودن، ارتباط به صورت یک‌طرفه و ناتمام قطع خواهد شد.

:SYN

نقشی اساسی را در برقراری یک ارتباط ایفا می‌کند. اگر بسته‌ای دارای بیت SYN با مقدار ۱ باشد آن بسته به عنوان درخواست برقراری ارتباط تلقی می‌شود.

:(Finish) FIN

اگر یکی از طرفین ارتباط داده، داده‌ی دیگری برای ارسال نداشته باشد، در هنگام ارسال آخرین بسته‌ی خود، این بیت را ۱ می‌کند و در حقیقت ارسال اطلاعات خودش را یک‌طرفه قطع می‌کند در این حالت اگرچه ارسال اطلاعات قطع شده، ولیکن طرف مقابل هنوز ممکن است به ارسال اطلاعات مشغول باشد بنابراین ارتباط زمانی قطع می‌شود(کاملا) که طرف مقابل نیز در یک بسته با ۱ کردن بیت FIN، ارسال اطلاعات را خاتمه دهد.

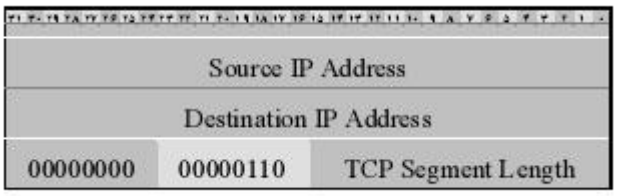
:Window Size

این فیلد برای کنترل جریان (Flow Control) استفاده می‌شود. مقدار قرار گرفته در این فیلد مشخص می‌کند که فضای بافر گیرنده چند بایت دیگر ظرفیت خالی دارد. فرستنده نیز حداکثر به اندازه‌ی مقداری که در این فیلد درج شده به گیرنده ارسال می‌کند پس در واقع فیلد Window Size برای جهت کنترل جریان (Flow Control) استفاده می‌شود. ضمنا اگر مقدار این فیلد صفر شود، یعنی بافر گیرنده تماما پر شده و امکان دریافت داده‌های بعدی وجود ندارد و پروسه‌ی فرستنده متوقف می‌شود.

Flow Control: برای ایجاد هماهنگی بین Server و Client از این مکانیزم استفاده می‌کنیم یعنی هر داده‌ای که Client می‌گیرد، مقدار فضای خالی‌اش را برای Server می‌فرستد و Server هم در همان حد فضا به فرستادن اطلاعات می‌پردازد. به این ترتیب فرستنده مجبور می‌شود که حداکثر با سرعتی داده‌ها را ارسال کند که گیرنده توانایی دریافت آن را داشته باشد.

:Checksum

در این فیلد کد کشف خطا قرار می‌گیرد و گیرنده Header فرضی ایجاد می‌کند که ساختار آن به شکل زیر است:



شکل ۴-۲: ساختار شبه سرآیند (Psuedo Header) در TCP

در هنگام ارسال داده اگر خطایی بروز نکند، پس از دریافت بسته در مقصد، جمع کل کلمات ۱۶ بیتی در یک بسته‌ی TCP به همراه سرآیند فرضی بایستی صفر شود در غیر این صورت داده غیر معتبر و خراب است

- کل بسته‌ی TCP در قالب کلمات ۱۶ بیتی در نظر گرفته می‌شود.
- سرآیند فرضی ساخته می‌شود و به صورت کلمات ۱۶ بیتی در نظر گرفته می‌شود.
- تمامی کلمات در مبنای مکمل ۱ با هم جمع و عدد به دست آمده در مبنای مکمل ۱ منفی می‌شود.

سرآیند فرضی شامل فیلدهای زیر است:

- ۳۲ بیت آدرس IP مربوط به ماشین مبدا
- ۳۲ بیت آدرس IP مربوط به ماشین مقصد
- یک بیت ۸ بیتی کاملا صفر
- فیلد ۸ بیتی پروتکل که برای پروتکل TCP یقینا مقدار ۶ دارد
- فیلد TCP Segment Length که در آن طول کل بسته‌ی TCP مشخص می‌شود.

:Urgent Pointer

در این فیلد یک عدد قرار می‌گیرد که موقعیت داده‌های Urgent یا اضطراری را درون بسته‌های TCP معین می‌کند. این داده‌ها زمانی اتفاق می‌افتند و ارسال می‌شوند که عملی شبیه وقوع وقفه‌ها در هنگام یک برنامه‌ی کاربردی رخ بدهد. بدون آنکه ارتباط قطع شود داده‌های لازم در همین بسته‌ی جاری ارسال خواهد شد.

:Options

اختیاری است و مقداری نظیر حداکثر طول بسته‌ی TCP در آن قرار می‌گیرد.

۳-۴ مکانیزم برقراری ارتباط در پروتکل TCP (Three ways Hand Shaking)

۱- فرستنده یک درخواست برای برقراری ارتباط با گیرنده می‌دهد که شامل یک بسته‌ی خالی TCP با SYN=1 و Ack=0 وSeq=x می‌باشد. x یک عدد تصادفی است که در واقع با این عدد نشان می‌دهد که ترتیب داده‌های ارسالی از x+1 شروع خواهد شد.

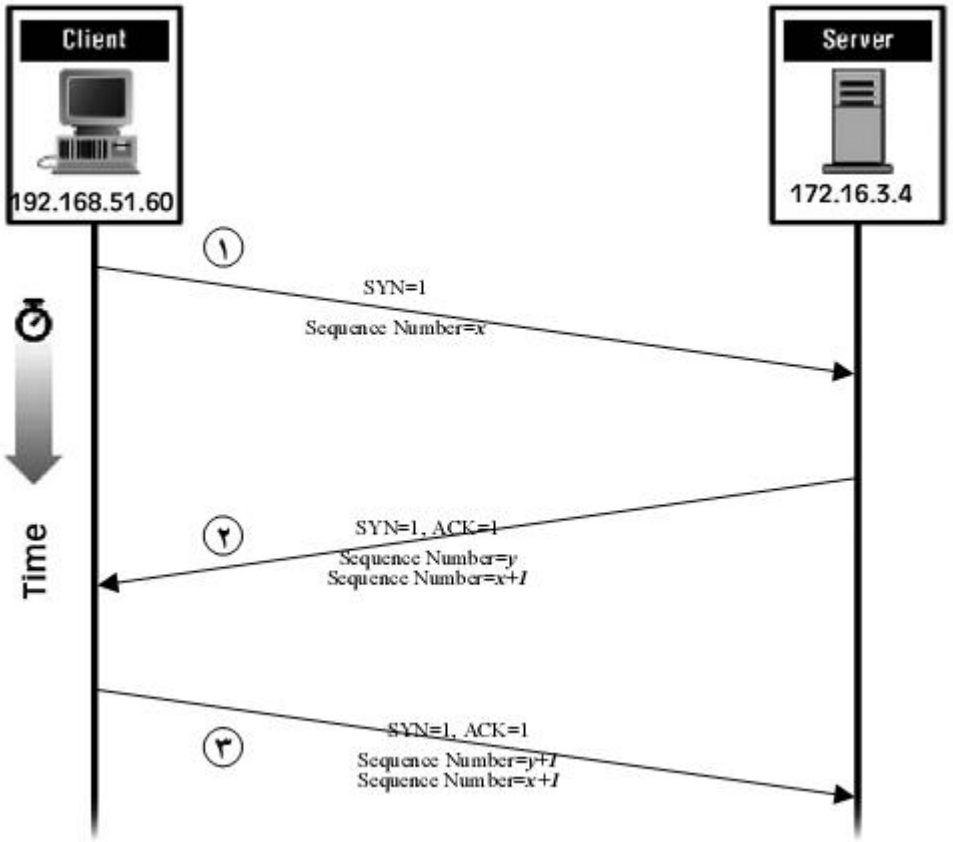
۲- اگر گیرنده تمایلی به برقراری ارتباط نداشته باشد با ارسال یک بسته‌ی TCP خالی که در آن بیت RST به ۱ تنظیم شده، این درخواست را رد می‌کند و در و صورت تمایل یک بسته‌ی خالی TCP با مشخصات زیر تولید میکند:

- بیت SYN را ۱ می‌کند
- بیت ACK را ۱ می‌کند
- مقدار فیلد Acknowledgement Number را x+1 قرار می‌دهد. این قسمت نشان می‌دهدکه گیرنده مقدار x+1 را برای شماره ترتیب ارسال داده‌های بعدی پذیرفته است.
- مقدار فیلد Sequence Number را مقدار تصادفی y قرار می‌دهد. و به فرستنده اعلام می‌کند که شماره ترتیب داده‌های ارسالی از سمت گیرنده از y خواهد بود.

۳- فرستنده با قرار دادن مقادیر زیر شروع ارتباط را تصدیق می‌کند:

- بیت SYN را ۱ می‌کند
- بیت ACK را ۱ می‌کند
- فیلد Seq. No.=x+1 را قرار می‌دهد.
- فیلد ACK را y+1 قرار می‌دهد.

و به این ترتیب دو طرف بر سر پارامترهای شماره ترتیب توافق داشته و ارسال و دریافت داده‌ها تا هنگامی که ارتباط با اطلاع طرفین خاتمه نیافته، آزاد است.



شکل ۴-۳: فرایند دست تکانی سه مرحله‌ای در TCP

نکته: برای خاتمه‌ی ارتباط روند زیر صورت می‌گیرد:

طرفی که داده‌هایش برای ارسال تمام شده است، یک بسته‌ی TCP را ارسال می‌نماید که در آن بیت FIN را ۱ قرار داده است. طرف مقابل این درخواست را دریافت و با ختم یک‌طرفه‌ی ارتباط موافقت می‌کند. ولی همچنان خود می‌تواند تا جایی که داده دارد آن‌ها را ارسال کند. و نهایتا در آخرین بسته، بیت FIN را ۱ بگذارد تا پس از تصدیق آن، ارتباط به صورت دو طرفه پایان یابد.

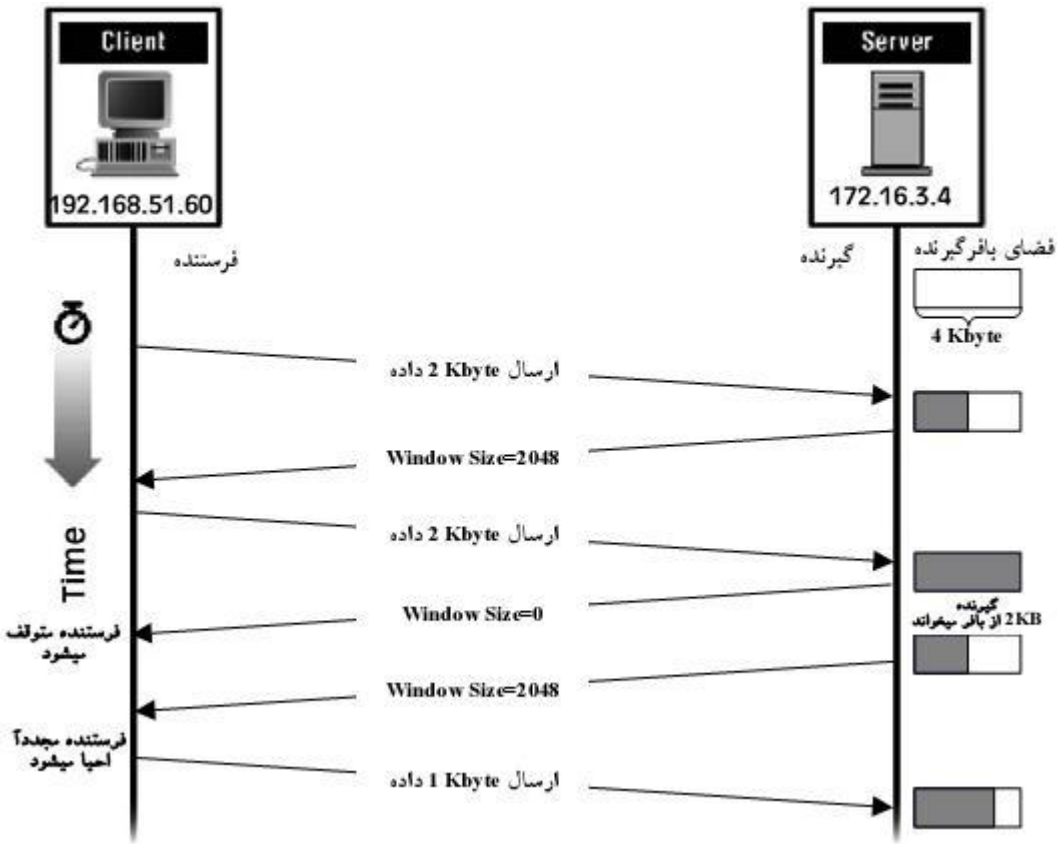
نکته: دلیل اینکه .Seq. No از صفر شروع نمی‌شود برای پیشگیری از مشکلات احتمالی ناشی از مساوی بودن شماره ترتیب بسته‌های ارسالی است.

نکته: اگر FIN فرستاده شود و ACK به هر دلیل دریافت نشود: تا یک Time خاص صبر می‌کند و اگر پاسخی دریافت نشود دوباره FIN را ارسال می‌کند در صورت عدم دریافت ACK چندین بار FIN را می‌فرستد اگر باز پاسخی دریافت نکرد چون دارای Timer است و زمان آن به پایان می‌رسد، ارتباط کاملا قطع می‌گردد.

۴-۴ کنترل جریان در پروتکل TCP

در پروتکل TCP برای کنترل جریان داده‌ها از بافر استفاده می‌شود و داده‌ها قبل از ارسال به برنامه‌ی کاربردی لایه‌ی بالاتر بافر شده و به صورت دسته‌ای تحویل خواهد شد. و گاها ممکن است که برنامه‌ی کاربردی اقدام به دریافت داده‌های بافر شده‌ی خود در مهلت مقرر نکند و بافر پر شود. در این حالت گیرنده دیگر قادر به دریافت و ذخیره‌ی داده‌ها در بافر خود نخواهد بود به همین دلیل در هر بسته‌ی TCP که به طرف دیگر ارسال می‌شود حجم فضای آزاد بافر در فیلد Window Size اعلام خواهد شد.

اگر Window Size=0 باشد یعنی بافر پر است و دیگر نمی‌تواند داده‌ای را دریافت کند در این حالت ارسال داده توسط فرستنده متوقف می‌شود و فرستنده منتظر دریافت بسته‌ای است که گیرنده مجددا آمادگی خود را جهت دریافت اعلام کند.(Window Size≠0)



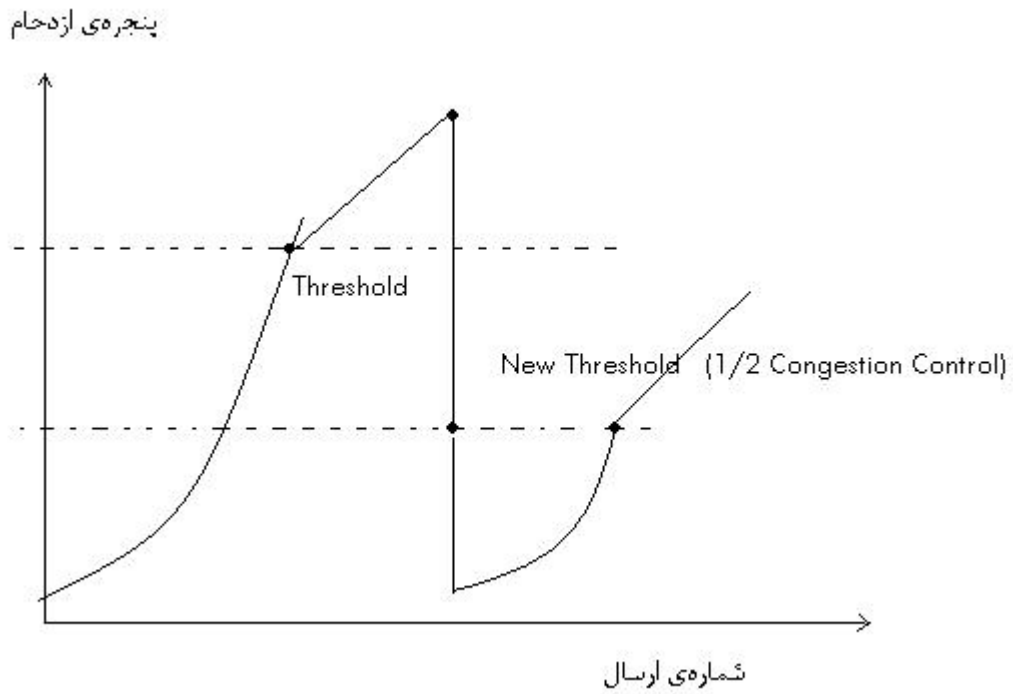
شکل ۴-۴: فرایند کنترل جریان در TCP

نکته: اگر گیرنده فضای خالی ایجاد کرد و آمادگی خود را نیز توسط ارسال بسته‌ای اعلام کرد اما بسته در وسط راه به هر دلیل گم شد باز هم نیاز به Timer است. اگر مدت زمان انتظار فرستنده انقضا شود دوباره یک بسته‌ی

خالی می‌فرستد اگر گیرنده جواب دهد نشان دهنده‌ی آن است که هنوز ارتباط برقرار است. ولی اگر جواب نداد ارتباط قطع شده، به همین دلیل ارتباط از طرف Server هم قطع می‌شود.

نکته: پورت باز، یعنی یک برنامه که روی آن پورت منتظر دریافت درخواست است.

۵-۴ مکانیزم کنترل ازدحام در TCP:



اندازه Congestion Window توسط فرستنده نگه‌داری می‌شود و مربوط به ظرفیت حمل زیرشبکه در مسیر مبدا به مقصد است. مقدار Window Size داخل ACK از گیرنده به فرستنده ارسال می‌شود و مربوط به ظرفیت گیرنده است.

- وقتی اتصال برقرار می‌شود فرستنده مقدار پنجره‌ی ازدحام را برابر یک سگمنت قرار می‌دهد (طول سگمنت در حین اتصال توافق شده) اگر اعلام وصول این قطعه قبل از انقضای مهلت مقرر انجام و دریافت شد، اندازه‌ی طول پنجره‌ی ازدحام به اندازه‌ی یک سگمنت اضافه می‌شود (یعنی در واقع اگر تمام سگمنت‌ها اعلام وصول شوند، اندازه‌ی پنجره‌ی ازدحام دو برابر می‌شود.) به این الگوریتم Slow Start گویند. هنگامیکه طول پنجره‌ی ازدحام به اندازه‌ی Threshold رسید، با اعلام وصول تمام سگمنت‌ها، تنها یک سگمنت به اندازه‌ی پنجره‌ی ازدحام اضافه می‌شود. این روال ادامه می‌یابد تا اندازه‌ی پنجره‌ی ازدحام حداکثر به اندازه‌ی Window Size برسد.
- در صورتی که مهلت اعلام وصول منقضی شود، اندازه‌ی Threshold به اندازه‌ی نصف پنجره‌ی ازدحام فعلی تنظیم می‌شود و پنجره‌ی ازدحام مجددا به یک سگمنت تنظیم می‌شود.

نکته:

در صورتی که پیام ICMP Source Quench دریافت و تحویل TCP شود، این رخداد معادل انقضای مهلت تلقی می‌شود. (راهکار جدیدتر در RFC 3168 تشریح شده است.)

۶-۴ زمان‌سنج‌ها در پروتکل TCP:

- (RT) Retransmission Timer
- Keep Alive Timer
- Persistence Timer
- Quiet Timer
- Idle Timer

Retransmission Timer:

در TCP پس از برقراری اتصال، فرستنده پس از ارسال هر سگمنت داده، به مدت زمان معینی منتظر دریافت تایید آن (ACK) از گیرنده می‌ماند، اگر این زمان منقضی شود (RTO) و فرستنده ACK دریافت نکند، آن سگمنت را دوباره ارسال می‌کند. مدت زمان انتظار توسط RT مشخص می‌شود.

$RTT = \alpha \cdot RTT + (1-\alpha)M \qquad \alpha=7/8 \quad M: \text{Current RTT}$

$D = \alpha \cdot D + (1-\alpha)\,|RTT - M| \quad \alpha=1/4$

$RTO_{New} = RTT + 4*D$

Keep Alive Timer:

ممکن است طرفین ارتباط موقتا داده‌ای برای ارسال نداشته باشند ولی ارتباط همچنان باز است و ادامه دارد. از طرف دیگر ممکن است یکی از طرفین، به دلیل خرابی (نرم‌افزاری یا سخت‌افزاری) بدون اطلاع، ارتباط را رها کرده باشد برای تمایز بین این دو حالت، فرستنده با استفاده از این زمان‌سنج در بازه‌های زمانی یک بسته‌ی خالی به طرف مقابل می‌فرستد، اگر پاسخ برگشت، نشان می‌دهد که ارتباط برقرار است. مقدار پیش‌فرض این تایمر بین ۵ الی ۴۵ ثانیه است.

Persistence Timer:

هنگامیکه گیرنده مقدار فضای آزاد بافر خود را صفر اعلام میکند (Window Size=0) فرستنده متوقف می‌ماند و در حالت بلوک(Block) قرار می‌گیرد تا اینکه گیرنده فضای آزاد بافر خود را مجددا اعلام نماید تا فرستنده دوباره ارسال را شروع کند. Persistence Timer مدت زمانی را مشخص می‌کند که فرستنده باید منتظر آمادگی مجدد گیرنده باشد. اگر در این مدت خبری از گیرنده نرسد، در پایان این زمان، فرستنده با ارسال بسته‌ای وضعیت گیرنده را جویا می‌شود، اگر جوابی از گیرنده دریافت کند، کار را ادامه می‌دهد (یعنی باز هم منتظر می‌ماند و یا ارسال را شروع می‌کند) در غیر این صورت ارتباط قطع خواهد شد.

Quiet Timer:

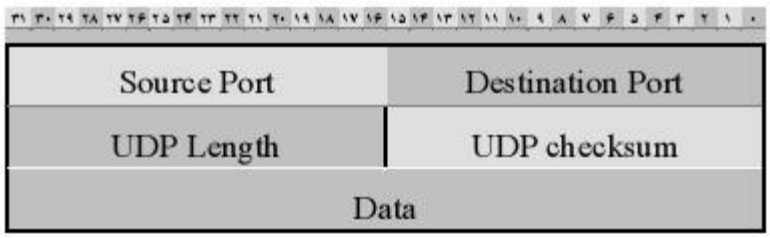
پس از بسته شدن یک ارتباط با یک شماره پورت، بقیه‌ی برنامه‌ها تا مدتی حق استفاده از شماره پورتی که اخیرا بسته شده را ندارند. این مدت زمان را Quiet Timer معین می‌کند. دلیل صبر کردن این است که ممکن است یک ارتباط TCP بسته شود ولی هنوز بسته‌های سرگردان آن ارتباط، بر روی شبکه وجود داشته باشند و پس از بسته شدن ارتباط TCP به مقصد برسند.(مقدار پیش‌فرض این تایمر بین ۳۰ الی ۱۲۰ ثانیه)

Idle Timer:

این زمان‌سنج برای آن است که اگر تلاش برای ارسال مجدد یک بسته، بیش از حد متعارف انجـام گرفـت، ارتباط TCP به صورت یک‌طرفه از سوی فرستنده قطع شود. مقدار پیش‌فرض ۳۶۰ ثانیه است.

۷-۴ پروتکل UDP (User Datagram Protocol)

پروتکلی است بدون اتصال و غیر قابل اعتماد که همان چیزی را که IP به ما می‌دهد را ارائه می‌دهد. (تمام کاستی‌های لایه‌ی IP را دارد بجز نظارت بر خطای کانال که می‌تواند وجود داشـته باشـد.) و بـدون هـیچ اطلاعـی از سرنوشتی که در انتظار یک بسته است، به سمت مقصد ارسال می‌شود. ولی در این پروتکل سرعت ارسال افـزایش و تاخیرات ناشی از نظارت بر جریان بسته‌ها کاهش می‌یابد.



شکل ۴-۵: ساختار دیتاگرام UDP

جهت کاربردهایی استفاده می‌شود که سرعت و زمان رسـیدن داده‌هـا مهمتـر از درسـت رسـیدن داده‌هاسـت. مناسب‌ترین کاربرد پروتکل UDP برای برنامه‌هایی است که عملیاتشان مبتنی بر یک تقاضا و پاسخ است.

فصل پنجم

۵ سیستم نام‌گذاری دامنه: DNS (Domain Name System):

DNS "یا سیستم نام‌گذاری حوزه"، روشی سلسله‌مراتبی است که بانک اطلاعاتی مربوط به نام‌های نمادین و معادل IP آن‌ها را روی کل شبکه‌ی اینترنت توزیع کرده است و هر ایستگاه می‌تواند در یک روال منظم و سلسله‌مراتبی آدرس IP معادل با ایستگاه مورد نظرش را در نقطه‌ای از شبکه پیدا کند.

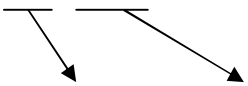
Resolve: فرایند به دست آوردن (تبدیل یا ترجمه) آدرسIP از روی آدرس DNS.

C:/my folders/my picture/pic.jpg

_____._____._____._____

- روش نام‌گذاری مورد استفاده در اینترنت سیستم نام‌گذاری دامنه یا DNS خوانده می‌شود، نام هر کامپیوتر شامل دنباله‌ای از حروف و اعداد است که به وسیله‌ی نقطه از هم جدا می‌شوند.
- نام‌ها به صورت سلسله‌مراتبی هستند و هر سطح به وسیله‌ی نقطه از سطوح دیگر جدا می‌شود، بالاترین سطح (قسمت مهم‌تر و یا با ارزش‌تر) سمت راست قرار می‌گیرد.
- قسمت قرار گرفته در آخرین نقطه سمت چپ، نام کامپیوتر یا ماشین را مشخص می‌کند و قسمت‌های دیگر نام دامنه یا گروهی را مشخص می‌کنند.

Ce .aut.ac.ir



نام ماشین محل یا ناحیه‌ای را مشخص می‌کند

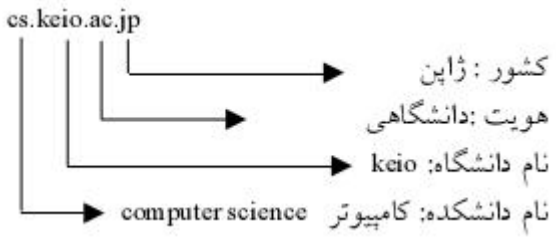
هر ماشین میزبان برای Resolve کردن به یک DNS سرور محلی متصل می‌شود.

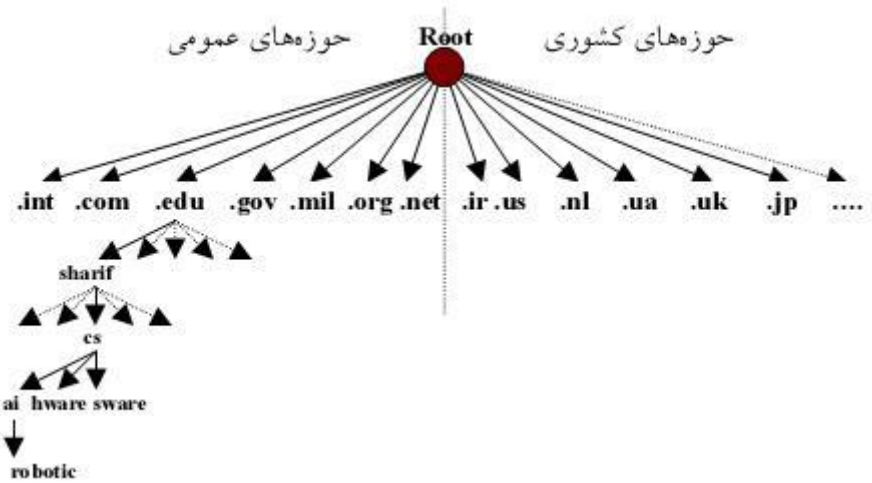
هفت حوزه‌ی عمومی که همه‌ی آن‌ها سه حرفی هستند عبارتند از :

- **Com**. صاحب این نام جز موسسات اقتصادی و تجاری به شمار می‌آید.
- **Edu**. صاحب این نام جز موسسات علمی یا دانشگاهی به شمار می‌آید.

- **Gov.** این مجموعه از نام‌ها برای آژانس‌های دولتی آمریکا اختصاص داده شده است.
- **Int.** صاحب این نام یکی از سازمان‌های بین‌المللی محسوب می‌شود.
- **Mil.** صاحب این نام یکی از سازمان‌های نظامی دنیا به شمار می‌آید.
- **Net.** صاحب این نام جز یکی از ارائه‌دهندگان خدمات شبکه به شمار می‌آید.
- **Org.** صاحب این نام جز یکی از سازمان‌های عام‌المنفعه و غیرانتفاعی محسوب می‌شود.

حوزه‌های کشوری که یک رشته‌ی دو حرفی هستند مخفف نام کشوری است که آن آدرس و ماشین صاحب آن نام، در آن کشور واقع است. مانند:





سلسله‌مراتب در DNS:

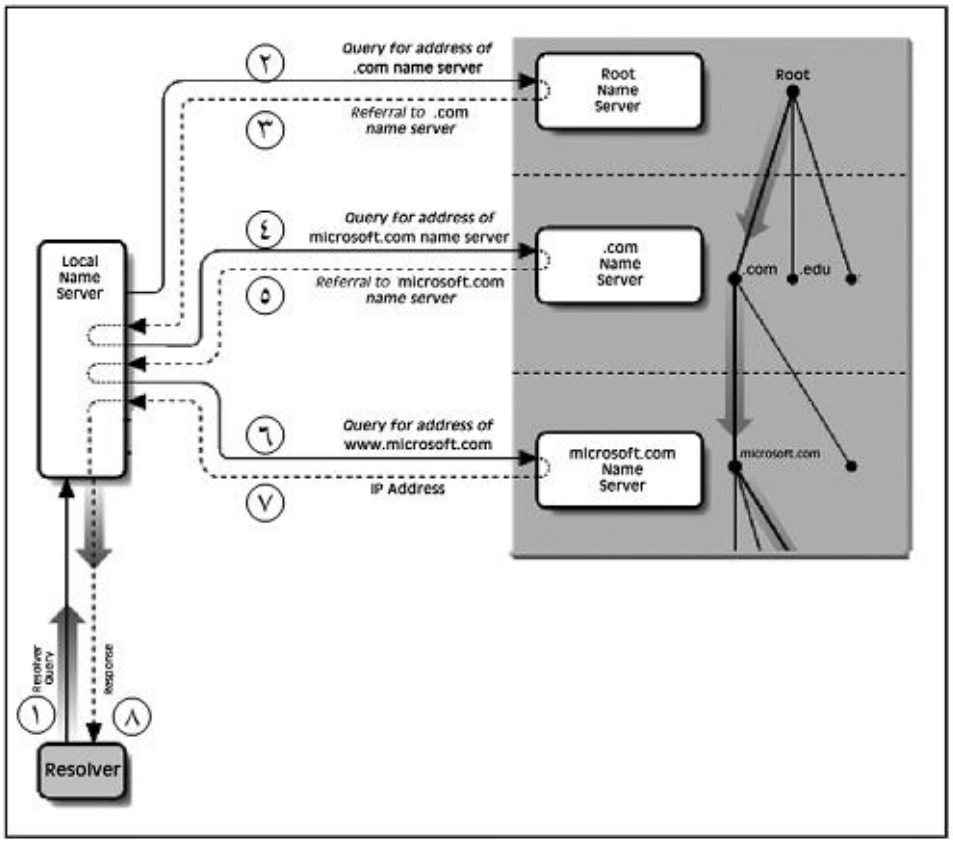
سیستم DNS یک سیستم سلسله‌مراتبی است یعنی هر DNS سرور مسئول دامنه‌ی زیرمجموعه‌ی خود است. یک سرور ریشه (Root Server) مسئولیت تمام دامنه‌های سطح بالا (Top Level) را بر عهده دارد.

Root Server اطلاعات نام‌های زیرمجموعه‌ی هر دامنه را ندارد و تنها اطلاعاتی راجع به چگونگی دسترسی به سرورهای دیگر را دارد.

۵-۱ انواع روشهای جستجو(Resolve) در DNS

- تکراری (Iterative)
- بازگشتی (Recursive)
- معکوس (Reverse)

۵-۱-۱ روش تکراری (Iterative)

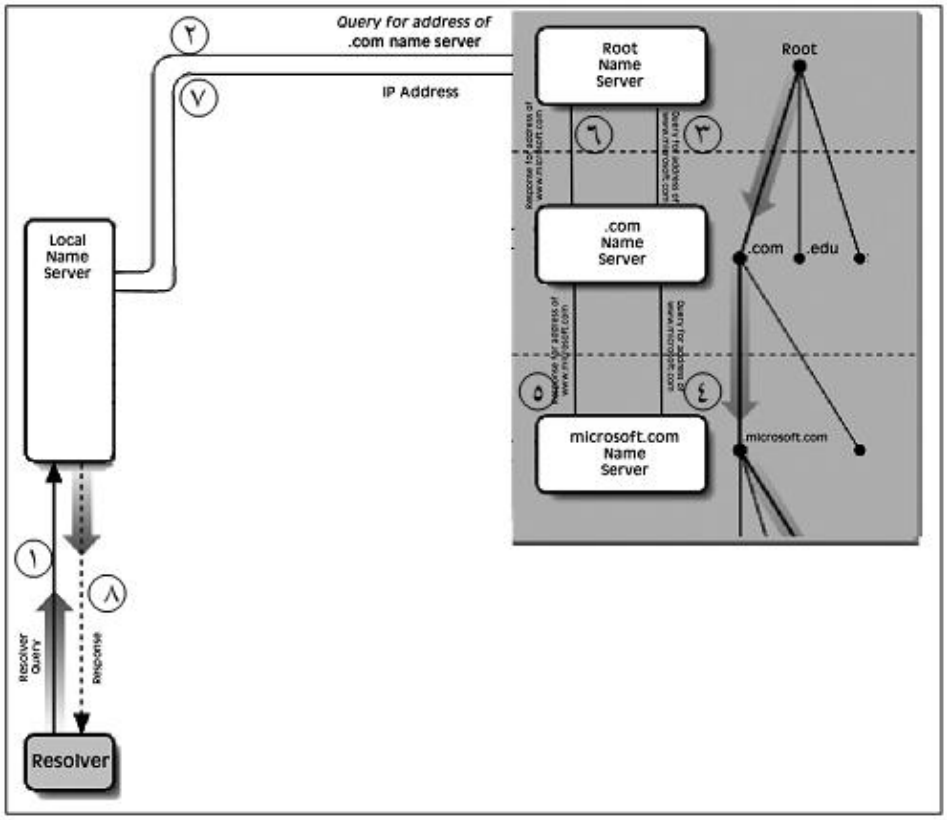


شکل ۵-۱: روش جستجوی تکراری در DNS

در این روش DNS Server محلی مسوول پیگیری و در نهایت بدست آوردن آدرس نهایی است و تمام بار پردازشی بر عهده DNS Server محلی است.

۵-۱-۲ روش بازگشتی (Recursive):

در این روش، قسمت اعظم فرایند Resolve بر عهده Top level domain است.



شکل ۵-۲: روش جستجوی بازگشتی در DNS

۵-۱-۳ روش معکوس:

آدرس IP را داریم و می‌خواهیم آدرس DNS را به دست آوریم:

۵-۲ مفهوم URL (Uniform Resource Locator)

آدرسی است با یک Format خاص که تمام اطلاعات لازم (نوع پروتکل، آدرس ماشین مقصد، شماره‌ی پورت ماشین مقصد و منبع مورد نظر) جهت دسترسی به منابع را در اینترنت فراهم می‌کند.

Http://www.google.com:80/search.htm

پروتکل آدرس ماشین مقصد آدرس فایل مورد نظر/ شماره پورت مقصد

Zone:

یک زیرمجموعه که مسئولیت آن به شخصی دیگر واگذار شده است. در واقع یک زیردرخت یا شاخه‌ای است که مدیریت آن واگذار شده است.

Domain:

کل زیرمجموعه یک Node را یک ناحیه یا Domain گویند.

۳-۵ ساختار بانک اطلاعاتی سرویس‌دهنده‌های نام

یک سرویس‌دهنده‌ی نام در دو قسمت سازمان‌دهی می‌شود:

- پروسه‌ی سرویس‌دهنده: یک برنامه‌ی اجرایی است که تقاضای ترجمه‌ی نام را از ماشین‌های دیگر گرفته، و پس از پردازش پاسخ مناسب را برای آن‌ها برمی‌گرداند.
- بانک اطلاعاتی: در این بانک اطلاعاتی داده‌های لازم برای تحلیل یک نام نمادین، ذخیره می‌شود. هر سرویس‌دهنده می‌تواند بنابر روش مورد نظر خود، این بانک اطلاعاتی را ایجاد کرده از آن استفاده کند. به این بانک اطلاعاتی "**بانک رکوردهای منبع**" گویند. که به اختصار "**فایل RR** " گفته می‌شود. که معمولا در حافظه‌ی اصلی نگهداری می‌شوند. هر رکورد درون فایل RR دارای زمان اعتبار است و پس از انقضای زمان باید از آن فایل حذف شده، یا آنکه با پرس‌وجوی مجدد به‌هنگام گردد. هر رکورد درون این فایل دارای پنج فیلد است:

Domain Name	Time To Live	Class	Type	Value

Domain Name:

در این قسمت نام حوزه، یا نام مربوط به یک ماشین (نام نمادین) قرار می‌گیرد. چندین رکورد می‌توان وجود داشته باشد که نام نمادین آن‌ها یکسان باشد! به همین دلیل این فیلد منحصر به فرد نیست.

Time To Live:

این گزینه نشان می‌دهد که رکورد تا چه مدت معتبر و قابل استناد است. معمولا در این فیلد مقدار ۸۶۴۰۰ قرار می‌گیرد که معادل یک شبانه‌روز است.

Class:

این فیلد مشخص می‌کند که ماهیت نام نمادین مربوط به چه شبکه‌ای است. اگر رکوردی مربوط به یک نام در شبکه‌ی اینترنت باشد، در این فیلد رشته‌ی دو حرفی in قرار می‌گیرد.

Type:

این فیلد نوع رکورد و معنای آن را مشخص می‌کند. مهمترین مقادیری که در این فیلد قرار می‌گیرد در جدول زیر مشخص است. در این فیلد می‌تواند یک گزینه‌ی حرفی یا معادل عددی آن قرار بگیرد

جدول ۵-۱: انواع رکوردهای منابع

Number	*Code*	*Description*
1	A	Network address
2	NS	Authoritative name server
3	MD	Mail destination; now replaced by MX
4	MF	Mail forwarder; now replaced by MX
5	CNAME	Canonical alias name
6	SOA	Start of zone authority
7	MB	Mailbox domain name
8	MG	Mailbox member
9	MR	Mail rename domain
10	NULL	Null resource record
11	WKS	Well-known service
12	PTR	Pointer to a domain name
13	HINFO	Host information
14	MINFO	Mailbox information
15	MX	Mail exchange
16	TXT	Text strings
17	RP	Responsible person
18	AFSDB	AFS-type services
19	X.25	X.25 address
20	ISDN	ISDN address
21	RT	Route through

SOA: یک سری اطلاعات ابتدایی پیرامون "ناحیه‌ی آدرس نمادین"، یک شماره سریال، مدیر مسئول و مهلت اعتبار ارائه می‌کند.

A: معادل IP نامی را که در فیلد اول آمده است، تعیین می‌کند.

NS: یک ماشین سرویس‌دهنده‌ی نام، ویژه‌ی یک حوزه را مشخص می‌کند.

CNAME: نام‌های مستعار و راحت‌تر را برای یک آدرس تعیین می‌کند.

فصل ششم

۶ پروتکل Telnet و پروتکل انتقال فایل

۶-۱ Telnet

برنامه یا ترمینالی است که از طریق آن، می‌توان از راه دور به یک کامپیوتر دیگر متصل شد، و کارهایی نظیر اجرا کردن یک برنامه، تغییر تنظیمات سیستم، حذف و ایجاد فایل‌ها و .. را انجام داد. روی پورت 23 کار می‌کند. از دو طریق می‌توان Telnet کرد:

۱. آدرس سرور
۲. شماره‌ی پورت مقصد

فرامین Telnet به دو دسته تقسیم می‌شوند:

۱. فرامین داخلی (پروتکل)

این فرامین از Client به Server فرستاده می‌شود. فرامین استانداردی هستند که بین سرور Telnet و Client مبادله می‌شوند و کاربر دخالتی در مبادله‌ی این فرامین ندارد.

۲. فرامین کاربری

فرامینی هستند که کاربر با استفاده از آن‌ها عملیات خود را به اطلاع برنامه‌ی Client می‌رساند.

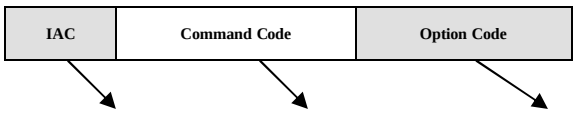
فرمان Toggle Option: یک فرمان کاربری است، وقتی یک دستور کاربری را تایپ می‌کنیم و بعد این دستور را می‌نویسیم، تمام دستورات (داخلی) پروتکل را که در حال رد و بدل شدن است، نشان می‌دهد.

Telnet > toggle option

نکته: Telnet تمام دستورات خود را به صورت Text مبادله می‌کند(رشته‌ای از کاراکترها) که باعث می‌شود پروتکل راحت‌تر باشد و همچنین اشکال‌یابی آسان‌تر صورت گیرد.

۶-۱-۱ قالب فرامین داخلی

برای تمایز بین داده‌ها و فرامین، یک سری کدهای فرمان تعریف شده‌اند:



نشان‌دهنده‌ی فرمان کد فرمان یکی از کدهای اختیاری(برای فرامین داخلی)

۲-۶ FTP (File Transfer Protocol):

پروتکل انتقال فایل یا FTP ابزار مناسبی برای کامپیوترهایی که به شبکه‌ی اینترنت متصل هستند می‌باشد. و خدمات زیر را ارائه می‌دهد:

- تهیه‌ی لیستی از فایل‌های موجود از سیستم فایل کامپیوتر راه دو
- حذف، تغییر نام و جابجا کردن فایل‌های کامپیوتر راه دور
- جستجو در شاخه‌های (دایرکتوری‌های) کامپیوتر راه دور
- ایجاد یا حذف شاخه در کامپیوتر راه دور
- انتقال فایل از کامپیوتر راه دور به کامپیوتر میزبان
- انتقال فایل و ذخیره‌ی آن از کامپیوتر میزبان به کامپیوتر راه دور

FTP روی دو پورت شماره‌ی ۲۰ و ۲۱ کار می‌کند که از شماره‌ی ۲۰ برای انتقال داده و از شماره‌ی ۲۱ برای انتقال فرامین لازم جهت مدیریت فایل‌ها استفاده می‌کند.

در واقع در FTP برای هر ارتباط به دو اتصال نیاز داریم یکی برای فرامین داخلی(پورت ۲۱) و یکی برای انتقال فایل(پورت۲۰) و این برای این است که بتوان بدون قطع جریان داده‌ها و فرامین را به طور همزمان مبادله کرد.

۱-۲-۶ روش‌های برقراری اتصال در FTP

- روش معمولی یا Normal Mode
- روش غیرفعال یا Passive Mode

۶-۲-۱-۱ مراحل برقراری یک ارتباط با استفاده از روش معمولی(Normal mode)

در روش معمولی برای برقراری یک اتصال FTP (یا نشست) مراحل زیر انجام می‌شود:

الف) در سمت Client ابتدا دو Socket از نوع TCP با شماره‌ی پورت تصادفی بالای ۱۰۲۴ ایجاد می‌شود.

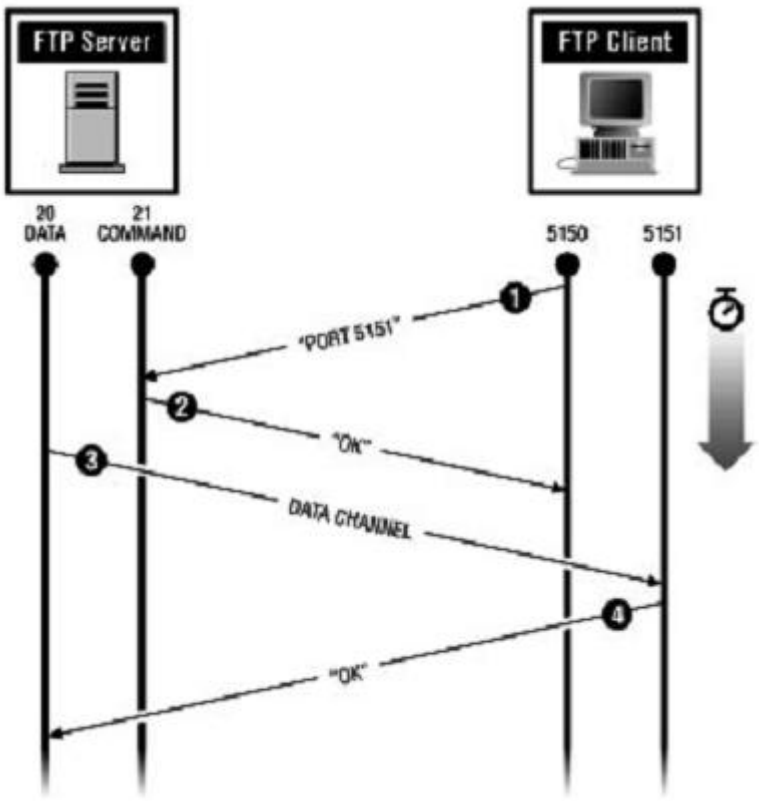
ب) Client سعی می‌کند با استفاده از دستور ( )Connect ارتباط یکی از Socketهای ایجاد شده‌ی خود را با پورت شماره ۲۱ از سمت Server برقرار کند. اگر این ارتباط برقرار شود در حقیقت کانال فرمان باز شده است.

ج) Client با فرمان "PORT" شماره پورت Socket دوم خود را اعلام می‌کند

د)Server یک ارتباط TCP با شماره‌ی پورت اعلام شده برقرار می‌کند

ه) Client ارتباط TCP شروع شده از سمت Server را تایید کرده و ارتباط FTP برقرار می‌شود.

نکته: مبدا می‌تواند با انتخاب چندین پورت همزمان چندین صفحه را مشاهده کند.



شکل ۶-۱: Normal FTP

۶-۲-۱-۲ مراحل برقراری یک ارتباط با استفاده از روش غیرفعال یا Passive

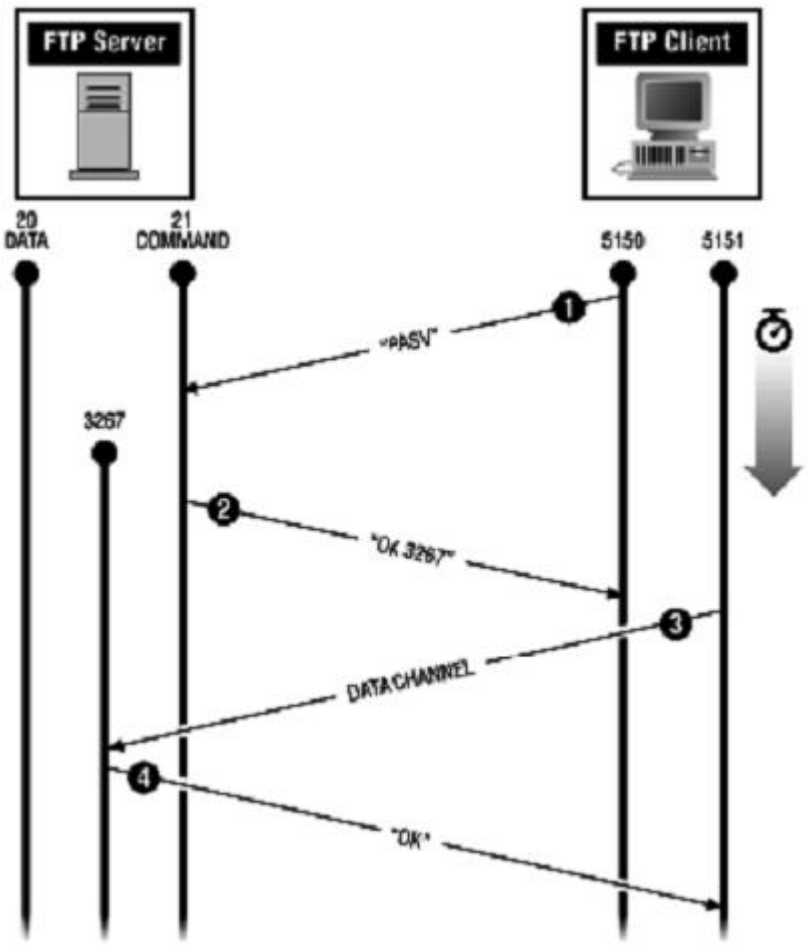
الف) در سمت Client ابتدا دو Socket از نوع TCP با شماره‌ی پورت تصادفی بالای ۱۰۲۴ ایجاد می‌شود.

ب) Client سعی می‌کند با استفاده از دستور ( )Connect ارتباط یکی از Socketهای ایجاد شده‌ی خود را با پورت شماره ۲۱ از سمت Server برقرار کند. اگر این ارتباط برقرار شود در حقیقت کانال فرمان باز شده است.

ج) Client با فرمان PASV به Server اعلام می‌کند که خواهان یک ارتباط غیرفعال است.

د) Server یک Socket با شماره‌ی پورت تصادفی (بالای ۱۰۲۴) ایجاد کرده و آن را به Client اعلام می‌کند.

ه) Client ارتباط Socket شماره‌ی دوم خود را با شماره پورت اعلام شده برقرار کرده، پس از تایید ارتباط از سوی سرور، نشست آغاز می‌شود.



شکل ۶-۲: Passive FTP

جدول ٦-١: فرامین کاربری **FTP**

فرامین کاربری	معنای فرمان
Ascii	تنظیم حالت انتقال فایل به حالت متنی
Binary	تنظیم حالت انتقال فایل به حالت دودویی
Cd	تغییر شاخه جاری به شاخه جدید بر روی سرویس دهنده
Close	ختم نشست
Del	حذف یک فایل از روی سرویس دهنده
Dir	فهرست گیری از شاخه جاری سرویس دهنده
Get	تقاضای انتقال یک فایل از سرویس دهنده
Hash	هرگاه یک بلوک داده از یک فایل در حال انتقال سالم رسید علامت ویژه ای را نشان بدهد
Help	راهنمایی
Lcd	تقاضای تغییر شاخه جاری بر روی ماشین محلی کاربر
Mget	دریافت چندین فایل از روی سرویس دهنده
Mput	ارسال چندین فایل بر روی سرویس دهنده
Open	تقاضای برقراری یک نشست و وصل به یک سرویس دهنده
Put	ارسال یک فایل بر روی سرویس دهنده
Pwd	نمایش شاخه جاری از سرویس دهنده
Qoute	ارسال مستقیم یکی از فرامین داخلی
Quit	تقاضای ختم نشست

۳-۶ TFTP (Trivial File Transfer Protocol)

یک مدل ساده شده از FTP است. ولی در زمینه‌هایی با FTP متفاوت است:

۱- TFTP نیازی به برقراری نشست و عملیات ورود به سیستم ندارد. به این ترتیب مشکلاتی نظیر دسترسی کاربران غیرمجاز محتمل خواهد بود.

۲- TFTP از پروتکل UDP که یک پروتکل بدون اتصال است به جای TCP استفاده می‌کند. و چون پروتکل UDP نظارتی بر ترتیب داده‌ها اعمال نمی‌کند بنابراین TFTP مجبور است برای تضمین صحت و ترتیب داده‌ها الگوریتم‌هایی را به کار گیرد.(TFTP شماره‌ی پورت ۶۹ را به کار می‌برد.)

۳- در TFTP عملیاتی نظیر فهرست‌گیری از فایل‌ها و شاخه‌ها، تغییر شاخه‌ی جاری و احراز هویت کاربر امکان‌پذیر نیست.

۴- ولی با تمام مشکلات آن نسبت به FTP مزایایی نیز دارد مثلا هنگام کار با ماشین‌های بدون دیسک یا ایستگاه‌های کاری TFTP کارآمدتر است. در واقع مهم‌ترین کاربرد این پروتکل برای بوت کردن سیستم‌هایی است که بدون دیسک بوده و مجبورند از طریق ROM بوت شوند. اندازه‌ی کوچک برنامه‌ی اجرایی TFTP و نیاز کم آن به حافظه باعث شده که بتوان آن را در BOOTROM جا داد.

۵- کاربرد دیگر آن برای دانلود فایل روی ماشین‌های کوچک است مانند موبایل‌ها.

فصل هفتم

۷ سیستم پست الکترونیکی در شبکه‌ی اینترنت

سیستم پست الکترونیک در دو برنامه‌ی مجزا سازماندهی می‌شود:

- User Agent یا عامل کاربر: در سمت Client اجرا شده و پیغامی را با فرمت استاندارد تولید می‌کند، امکان خواندن، نوشتن و ارسال و دریافت نامه را برای کاربر فراهم می‌کند.
- Message Transfer Agent یا عامل انتقال: انتقال نامه‌ها را از مبدا به مقصد بر عهده دارد.

۷-۱ تعیین قالب یک نامه‌ی ساده‌ی الکترونیکی(RFC 822)

در این استاندارد یک نامه‌ی الکترونیکی به صورت زیر سازماندهی می‌شود:

- تعدادی فیلد مشخص و تعریف شده، که برای انتقال فایل لازم است. این قسمت سرآیند نامه را تشکیل می‌دهد (این فیلدها متنی هستند)
- یک سطر خالی (به عنوان مرز قسمت سرآیند و بدنه‌ی نامه)
- بدنه‌ی پیام(شامل متن اصلی نامه)

جدول ۷-۱: فیلدهای اجباری سرآیند **EMail**

فیلد	شرح
To:	آدرس پست الکترونیکی گیرنده اصلی نامه
Cc:	آدرس پست الکترونیکی گیرنده یا گیرندگان ثانویه
Bcc:	آدرس پست الکترونیکی گیرنده یا گیرندگان ثانویه بدون اطلاع از آدرس یکدیگر
From:	آدرس پست الکترونیکی صاحب اصلی (نویسنده) نامه
Sender:	آدرس پست الکترونیکی فرستنده اصلی نامه
Received:	خطی که توسط سیستمهای پست الکترونیکی در بین مسیر اضافه می‌شود.
Return-path:	مسیر برگشت نامه را تعریف می‌کند.

جدول ۷-۲: فیلدهای اختیاری سرآیند EMail

فیلد سرآیند	شرح
Date:	تاریخ و زمان ارسال پیام (نامه)
Replay-To:	آدرس پست الکترونیکی کسی که باید پاسخ این نامه را دریافت نماید.
Message-Id:	یک شماره منحصر بفرد برای آنکه بتوان بعداً به آن شماره استناد کرد.
In-Replay-To:	شماره نامه‌ای که این نامه در پاسخ به آن نامه می‌باشد.
References:	شماره های دیگری که این نامه با آنها مرتبط است.
Keywords	برخی از کلمات کلیدی از مضمون نامه که توسط نویسندهٔ نامه انتخاب می‌شود.
Subjects	موضوع نامه (خلاصه بسیار کوتاهی از نامه فقط در یک خط)

۷-۱-۱ استاندارد MIME

سیستم نامه‌رسانی توسعه‌یافته در اینترنت.

استانداردی است جهت انتقال فایل‌های غیر ASCII مانند فایل‌های اجرایی، صدا و تصویر. به گونه‌ای که در بدنه‌ی نامه قرار گیرد که بر اساس سرویس‌دهنده‌های قدیمی قابل ارسال و دریافت باشد. استاندارد MIME پنج فیلد جدید در سرآیند نامه تعریف کرده که به صورت زیر هستند:

جدول ۷-۳: فیلدهای اختیاری سرآیندMIME در EMail

سرآیند	توضیح
MIME-Version:	شمارهٔ نسخهٔ MIME
Content-Description:	یک سطر که مضمون کلّی نامه را مشخص می‌نماید.
Content-Id:	یک مشخصه یا شماره منحصر به فرد
Content-Transfer-Encoding:	طریقه کدگذاری محتوای نامه
Content-Type:	نوع و محتوای نامه

MIME-Version:

این فیلد به برنامه‌ی نامه‌خوان در سمت کاربر تفهیم می‌کند که این نامه‌ی الکترونیکی با استاندارد MIME سازماندهی و ارسال شده است و نسخه‌ی استاندارد آن را نیز مشخص می‌کند.

Content-Description:

متنی که در جلوی این فیلد قرار می‌گیرد مضمون و محتوای نامه را مشخص می‌کند. گیرنده‌ی نامه با استفاده از این فیلد می‌تواند تشخیص دهد که آیا رمزگشایی و خواندن پیام ارزشمند است یا نه.

:Content-Id

شماره یا رشته‌ای است منحصر به فرد که می‌توان به عنوان شماره‌ی نامه در نامه‌های بعدی به آن استناد کرد.

:Content-Transfer-Encoding

در جلوی این فیلد عبارتی قرار می‌گیرد که به برنامه‌ی نامه‌خوان در سمت کاربر تفهیم می‌کند که چه قاعده‌ای را برای Decoding بدنه‌ی نامه به کار ببرد. به گونه‌ای که اشاره شد برخلاف استاندارد RFC 822 در بدنه‌ی نامه‌های مبتنی بر MIME می‌توان کدهای غیر اَسکی، فایل‌های صدا ، تصویر و کلا هر فایل دودویی قرار بگیرد. بنابراین در مقصد قبل از نمایش محتوای نامه، باید قسمت بدنه‌ی آن پردازش و Decode شود.

انواع کدگذاری در استانداردMIME:

- کدگذاری Bsae-64: داده‌های پیام را ۶ بیت، ۶ بیت از هم جدا می‌کند
- کدگذاری Qouted-Printable: کاراکترهایی که زیر ۱۲۷ هستند را تغییر نمی‌دهد ولی کاراکترهایی را که بالای ۱۲۷ هستند با یک درصد و کد هگزا مشخص می‌کند. مانند FF%

:Content-Type

آخرین فیلد سرآیند در استاندارد MIME یکی از کاربردی‌ترین فیلدها خواهد بود که مشخصات محتوای نامه را تشریح می‌کند. انواع محتویات متن یک نامه‌ی الکترونیکی با استاندارد MIME در جدول زیر آمده است:

جدول ۷-٤ انواع محتویات متن یک نامه‌ی الکترونیکی با استاندارد **MIME**

نوع کلّی	نوع دقیق	شرح
Text	Plain	متن ساده معمولی
	Richtext	متن حاوی دستورات قالب بندی
Image	Gif	فایل تصویر با قالب GIF
	Jpeg	فایل تصویر با قالب JPEG
Audio	Basic	فایل صوتی با قالب snd
Video	Mpeg	فایل ویدئوئی با قالب MPEG
Application	Octet-stream	دنباله‌ای از بایتهای تفسیر نشده
	Postscript	متن تنظیم شده در پست اسکریپت
Message	Rfc822	متن تنظیم شده در استاندارد RFC822
	Partial	متن به منظور انتقال تکه تکه شده است.
	External-body	متن پیام باید از شبکه اینترنت بارگذاری شود.
	Mixed	متن دارای چندقسمت است که ترتیب مشخص دارد.
Multipart	Alternative	متن دارای چند قسمت با قالبهای متفاوت است.
	Parallel	قسمتهای مختلف متن باید همزمان ملاحظه شود.
	Digest	متن شامل چندقسمت است و هر قسمت از نوع RFC822 است.

۷-۲ پروتکل SMTP (Simple Mail Transfer Protocol)

پروتکل ارسال نامه‌های الکترونیکی در پست الکترونیک است. با پورت شماره‌ی ۲۵ کار می‌کند یعنی هنگامی‌که کاربر می‌خواهد ایمیل بفرستد به پورت ۲۵ وصل می‌شود مانند Outlook Express

مراحل عملیات:

- ماشین مبدا با پورت شماره‌ی ۲۵ به ماشین مقصد که سرویس دهنده‌ی SMTP روی آن اجرا شده است یک ارتباط TCP برقرار می‌کند. پس از برقراری ارتباط و پذیرش آن توسط سرویس‌دهنده، شروع کننده‌ی ارتباط باید آنقدر صبر کند تا سرویس‌دهنده با اعلام یک پیغام اعلام آمادگی کند
- سرویس‌دهنده با ارسال یک رشته‌ی متنی که معمولا به صورت زیر است به برنامه‌ی مبدا اعلام آمادگی می‌کند

220 آدرس نام حوزه‌ی خود SMTP service ready

- پس از اعلام آمادگی، برنامه‌ی مبدا با ارسال یک رشته که حاوی کلمه‌ی HELO و همچنین آدرس نام حوزه‌ی خودش می‌باشد هویت خود را برای سرویس‌دهنده آشکار می‌کند.
- پس از آنکه سرویس‌دهنده هویت فرستنده‌ی پیام را ارزیابی کرد در صورتیکه مایل به دریافت نامه باشد با کد ۲۵۰ و رشته‌ای که در ادامه‌ی آن می‌آید اعلام آمادگی می‌کند
- سرویس دهنده صاحب نامه را بررسی کرده و در صورتی که منعی برای دریافت نامه‌ی چنین شخصی وضع نشده باشد مجددا با کد ۲۵۰ و رشته‌ای که در ادامه می‌آید اعلام آمادگی می‌کند.
- برنامه‌ی مبدا، گیرنده‌ی نامه را معرفی می‌کند.
- بار دیگر سرویس‌دهنده گیرنده‌ی نهایی نامه را ارزیابی می‌کند و بررسی می‌کند که آیا چنین شخصی وجود دارد یا خیر. در صورتی که امکان دریافت نامه وجود داشته باشد برای بار سوم با کد ۲۵۰ اعلام آمادگی می‌کند
- برنامه‌ی مبدا اعلام می‌کند که برای ارسال داده‌ها که کلا کاراکترهای اسکی با کد زیر ۱۲۸ هستند آماده است کلمه‌ی DATA بدون هیچ حرف اضافه‌ای به عنوان علام آمادگی ارسال می‌شود.
- سرویس‌دهنده ضمن اعلام آمادگی برای دریافت داده‌ها به مبدا اعلام می‌کند که پس از آخرین سطر نامه یک خط که فقط شامل تک کاراکتر "." است ارسال کند که انتهای نامه مشخص باشد.
- مبدا نامه‌ای را که با استاندارد RFC 822 یا MIME تنظیم شده است ارسال می‌کند
- سرویس‌دهنده دریافت موفقیت آمیز نامه را اعلام می‌دارد.
- مبدا با ارسال رشته‌ی QUIT اعلام خروج می‌کند
- فرستنده ضمن تایید خروج و معرفی مجدد خود اعلام می‌کند که ارتباط TCP را قطع خواهد کرد و در این جا کار انتقال خاتمه یافته است.

۳-۷ پروتکل POP3

پروتکلی است که برای دریافت ایمیل‌های کاربر از Mail Box او استفاده می‌شود.

این پروتکل مجموعه‌ای از فرامین برای برقراری اتصال، قطع اتصال، دریافت پیام‌ها و حذف آن‌ها می‌باشد. این پروتکل نیز همانند SMTP فرامین متنی دارد.

۴-۷ پروتکل IMAP (Internet Message Access Protocol)

این پروتکل برای دریافت ایمیل‌های کاربر از Mail Server استفاده می‌شود. تفاوت آن با POP3 آن است که IMAP پس از انتقال ایمیل‌ها به کاربر آن‌ها را از روی سرور خود حذف نمی‌کند مگر اینکه خود کاربر این کار را انجام دهد. پروتکل IMAP امکان ساخت پوشه ونیز آرشیو E-Mail ها را فراهم می‌کند.

۵-۷ امکانات سیستم پست الکترونیک:

- **فیلترکردن (غربال کردن):**

شما از سیستم پست الکترونیکی می‌خواهید که نامه‌های دریافتی از یک آدرس خاص را اصلا تحویل نگیرد یا نامه‌هایی که قسمت موضوع آن شامل کلمات کلیدی خاص است را حذف کند. یا مثلا نامه‌هایی که کلمه‌ای خاص در آدرس فرستنده‌اش است را حذف کند. (این امکان برای رهایی از شر مزاحمت شرکت‌های تبلیغاتی که پیاپی نامه ارسال می‌کنند مفید است.)

- **ارسال نامه‌های رسیده به آدرسی دیگر به صورت خودکار(Forwarding):**

این امکان وجود دارد که یک نامه را بدون دخل و تصرف به یک آدرس دیگر ارسال کنید.

- **Vacation Daemon:**

می‌توانید سیستم پستی را وادار کنید که ضمن دریافت نامه‌ها یک پیغام برای ارسال کنندگان نامه بفرستد مثلا یک شرکت هر روز نامه‌های زیادی دریافت می‌کند و ممکن است پاسخ دستی به آن‌ها طولانی مدت شود می‌تواند از سیستم پستی بخواهد که به صورت خودکار برای فرستندگان نامه پیامی را ارسال کند و به پرسش‌های متداول آن‌ها پاسخ بدهد

۶-۷ HTML

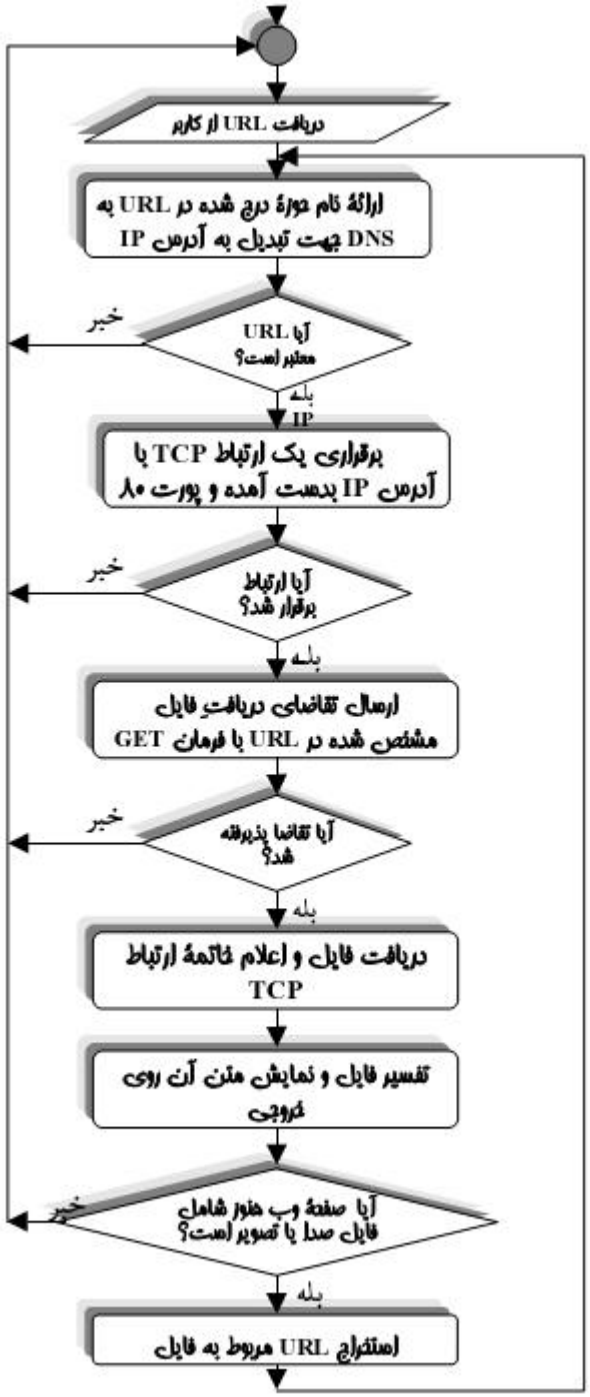
زبانی است که فرمت و شیوه‌ی نمایش اسناد وب را مشخص می‌کند یعنی به وسیله‌ی آن می‌توان متون خالص و معمولی را صفحه‌آرایی کرد و عواملی مثل صدا ، تصویر و ... را به متن اضافه کرد.

۷-۷ WWW (World Wide Web) تور جهان گستر

تور جهان‌گستر یا وب یک روش معماری یا به عبارتی یک نظام برای ذخیره‌سازی و دسترسی به مستندات به هم پیوند خورده‌ای است که روی هزاران ماشین در کل جهان پراکنده و توزیع شده‌اند. هر یک از این مستندات پیوند خورده که شامل متن، صدا و تصاویر گرافیکی و تصاویر متحرک‌اند، می‌تواند به یک سند دیگر در محلی متفاوت در جهان اشاره نماید. بزرگترین حسن وب، سادگی استفاده از آن است.

۸-۷ پروتکل HTTP (Hyper Text Transfer Protocol):

مجموعه‌ای فرامین استاندارد است که از سمت Client به Server ارسال می‌شود. در حقیقت این پروتکل طریقه‌ی صحبت کردن بین Server و Client را مشخص می‌کند. فرامین این پروتکل در استاندارد RFC 822 " متود" نامیده شده است.



فلوچارت عملیات مرورگر برای دریافت یک صفحه‌ی وب

مراحل بارگذاری صفحه(Loading) یا اسناد وب:

۱. وارد کردن URL سند مورد نظر توسط کاربر

۲. مرورگر آدرس وارد شده را پردازش می‌کند و اطلاعات پروتکل، ماشین مقصد، شماره‌ی پورت و آدرس فایل‌های درخواستی را استخراج می‌نماید.

۳. ترجمه‌ی آدرس(Resolve) نام DNS به آدرس IP ماشین مقصد

۴. مرورگر(سمت Client) با پورت 80 با سرور یک اتصال TCP برقرار می‌کند.

۵. مرورگر یک درخواست HTTP تولید کرده و صفحه‌ی مورد نظر را از Web Server درخواست می‌کند.

۶. سرور نتیجه‌ی درخواست را به Client ارسال می‌کند.

۷. قطع اتصال TCP

۸. نتیجه‌ی پردازش روی جواب اطلاعاتی است که از سرور می‌گیرد.

۹. اگر یک Link روی صفحه وجود داشته باشد با کلیک روی آن همه‌ی مراحل تکرار می‌شود.

جدول ۷-۵: فرامین تعریف شده در پروتکل **HTTP**

نام فرمان	توضیح
GET	تقاضا برای دریافت یک صفحه وب از سرویس‌دهنده
HEAD	تقاضا برای دریافت سرآیند[1] یک صفحه وب
PUT	تقاضا برای ذخیره کردن یک صفحه وب روی یک سرویس‌دهنده
POST	تقاضا برای ضمیمه کردن اطلاعاتی به یک منبع (مثل فایل یا صفحه وب)
DELETE	تقاضا برای حذف یک صفحه وب
LINK	تقاضای برقراری پیوند بین دو منبع موجود
UNLINK	تقاضای خاتمه پیوند دو منبع موجود

۷-۸-۱ متودهای HTTP

- **متود GET**: مرورگر با ارسال این متود به سرور تقاضا می‌کند که یک صفحه‌ی وب یا یک فایل دودویی مثل فایل تصویر یا صدا برایش ارسال شود.
- **متود HEAD**: این متود از سرور تقاضا می‌کند که فقط سرآیند صفحه‌ی وبی را که نام آن در جلوی متود درج شده ، ارسال نماید این متود چند کاربرد دارد:

اول آنکه مشخصات صفحه‌ی وب، شامل تاریخ آخرین تغییر، عنوان صفحه، نام تدوین کننده و صاحب اصلی آن و برخی از مشخصات اختیاری که در سرآیند صفحه‌ی وب درج شده ، ارسال می‌شود و این اطلاعات می‌تواند برای مقاصدی همانند تهیه‌ی بانک‌های اطلاعاتی از صفحات وب و طراحی جستجوگرهای وب مفید واقع شود.

دوم آنکه می‌توان با این متود صحیح بودن یک URL و وجود یک صفحه‌ی وب را ارزیابی کرد.

- **متود PUT**: این متود عکس عمل GET است یعنی مرورگر تقاضا می‌کند که یک صفحه‌ی وب را بـر روی سرور ذخیره نماید. این متود را سرورهایی حمایت می‌کننـد کـه بخواهنـد صـفحات برخـی از کـاربران را دریافت کرده ضمن ذخیره‌ی آن‌ها، آن‌ها را در اختیار دیگران قرار بدهند.

- **متود POST**: از سرور تقاضا می‌کند که داده‌هایی را به یک منبع موجود (مثل یـک صـفحه‌ی وب یـا یـک فایل) اضافه کند. برای ایجاد صفحات آزاد خبری، تابلو اعلانات، محیط‌های نظرخواهی یا ارسال برای یـک پروسه‌ی تحت وب همانند برنامه‌های CGI مورد استفاده قرار می‌گیرد.

- **متود DELETE**: از سرور تقاضا می‌کند که یک صفحه‌ی وب را با نام مشخص از روی ماشین سرور حذف نماید.

دقت شود که بسیاری از سـرورها بـه دلایـل امنیتـی از متودهـای PUT ، POST و DELETE پشـتیبانی نمی‌کنند.

- **متودهای LINK و UNLINK**: این دو متود اجازه می‌دهند که بین دو صفحه‌ی وب (یا دو منبع) ارتبـاط و پیوند برقرار شده یا پیوند قبلی خاتمه داده شود.

وقتی تقاضا به سمت سرور ارسال می‌شود چه پذیرفته شـود و چـه پذیرفتـه نشـود، پاسـخی متنـی دریافت می‌شود که معمولا با فرمت زیر است:

رشته‌ی متنی	شماره‌ی وضعیت	شماره نسخه/ پروتکل

شماره‌ی نسخه/ پروتکل: نسخه‌ی پروتکل را مشخص می‌کند

شماره‌ی وضعیت: شماره‌ای است سه رقمی که وضعیت اجرای فرمان ارسالی را مشخص می‌نماید. ایـن شماره‌ی سه رقمی بر اساس رقم صدگان به پنج دسته تقسیم می‌شود:

- **1xx**: اطلاعاتی(پاسخی جهت آگاهی بیشتر Client)
- **2xx**: عمل درخواستی موفقیت‌آمیز اجرا شده است.
- **3xx**: URL مورد تقاضا، تغییر آدرس داشته است.
- **4xx**: در تقاضای ارسال شده از طرف Client خطایی وجود دارد.
- **5xx**: در سرویس‌دهنده خطایی داخلی رخ داده است.

در صورتی که رقم صدگان ۳، ۴ یا ۵ باشد وضعیت فرمان ارسالی ناموفق بوده است.

رشته‌ی متنی: متن کوتاهی که وضعیت اجرای فرمان را به زبان طبیعی توصیف می‌کند

مثال:

HTTP/1.0 200 OK

HTTP/1.0 304 Not Modified یا

Set-Cookie: سرور بخواهد چیزی روی Client بنویسد.

Last-Modified: تاریخ آخرین تغییر روی صفحه:

۱- برای موتورهای جستجو

۲- Caching اطلاعات مربوط به یک صفحه روی خود سرور نیز Cache می‌شود (یعنی هم روی Client صورت می‌گیرد و هم روی Proxy Server)

Cookie:

اطلاعاتی است که از طرف سرور روی کامپیوتر Client ذخیره می‌شود و این امکان را فراهم می‌کند که سرور بتواند اطلاعات اتصال‌های قبلی آن Client را بازیابی نماید. مرورگر قبل از اتصال به یک سرور وب به دنبال کوکی‌های قبلی آن سرور بر روی حافظه‌ی خود می‌گردد و در صورت موجود بودن کوکی مربوط به آن سرور، آن را همراه درخواست خود ارسال می‌کند.

- کوکی جلسه Per Session Cookie : داخل حافظه‌ی مرورگر (RAM) ذخیره می‌شود با بستن مرورگر این اطلاعات حذف می‌شود.

- کوکی دائمی Persistent Cookie : به صورت فایل متنی روی هارد کامپیوتر کاربربصورت فایـل متنـی ذخیره می‌شود و محتویات آن به همراه هر درخواست به سرور ارسال می‌شود.

جزوه درس مهندسی اینترنت

منابع و مراجع

[۱] اصول مهندسی اینترنت، مهندس احسان ملکیان، ویراست دوم، انتشارات نص، ۱۳۸۵.

[۲] شبکه‌های کامپیوتری، ا.اس.تننباوم، ترجمه دکتر حسین پدرام، ویراست چهارم، انتشارات نص، ۱۳۸۴.

[۳] Communication Networks, A. Leon-Garcia, McGraw-Hill, 2000.