
بسم الله الرحمن الرحيم

پروتکل SMTP :

احتمالا شما تا به حال بارها از پست الکترونیکی (E.Mail) برای برقراری ارتباط با دیگران استفاده کرده اید. پست الکترونیکی مجموعه ای از برنامه ها است که توسط آن می توانید متن و اسناد خود را تحت شبکه انتقال دهید، برای ارسال و دریافت پست الکترونیکی پروتکل های متفاوتی وجود دارد، ما در این قسمت به پروتکل SMTP (Semple Mail Transfer Protocol)، که برای ارسال E.Mail از آن استفاده می شود را توضیح می دهیم.

پروتکل SMTP به صورت استاندارد بر روی پورت ۲۵ فعالیت می کند. و تحت این پورت به ارسال پست الکترونیکی می پردازد.

در پروتکل SMTP برای ارسال یک Mail قوانینی در نظر گرفته شده است. اگر شخصی یا برنامه ای بخواهد تحت این پروتکل متنی را به آدرس خواصی ارسال کند باید این قوانین را در نظر داشته باشد.

قوانین ارسال پست الکترونیکی در پروتکل SMTP :

برای ارسال یک E.Mail در اولین گام شما باید به ماشینی در شبکه که این سرویس بر روی آن فعال است متصل شوید. برای این منظور می توانید از ماشین های سرویس دهنده پست الکترونیکی معرف دنیا استفاده نمایید. یا اینکه بر روی شبکه به دنبال ماشینی که پورت ۲۵ باز دارد بگردید.

در زیر آدرس بعضی از سرویس دهنده های بزرگ پست الکترونیکی نوشته شده است:

www.mail.yahoo.com

www.gmail.com

www.hotmail.com

www.mailcity.com

بعد از پیدا کردن یک میزبان در شبکه که سرویس پست الکترونیکی به کاربران می دهد، نوبت به برقراری اتصال با این ماشین است. برای این کار شما باید با استفاده از یک نرم افزار مشتری پست الکترونیکی یا اینکه به وسیله یک برنامه کلاینت متنی (مثل نرم افزارTelnet سیستم عامل ویندوز) که دستورات را به طرف سرور ارسال می کند با ماشین میزبان ارتباط برقرار کنید.

نحوه برقراری ارتباط با سرویس خواصی از یک ماشین توسط برنامه Telnet در زیر نشان داده شده است:

telnet شماره پورت ۲۵ آدرس ماشین سرویس دهنده

در مثال زیر به سرویس SMTP ماشینی با آدرس mail.yahoo.com به وسیله برنامه telnet متصل می شویم:

telnet mail.yahoo.com 25

بعد از اتصال به ماشین برای پذیرفته شدن در سرویس SMTP شما باید از دستور HELO استفاده کنید.

مثال:

HELOآدرس ماشین میزبان

بعد از اتصال شما به سرویس SMTP باید قبل از هر کار دیگری آدرس پست الکترونیکی خود و آدرس پست الکترونیکی شخصی که مایل به ارسال اطلاعات به او هستید را مشخص کنید. برای مشخص کردن آدرس پست الکترونیکی خود از از دستور :MAIL FROM و برای مشخص کردن آدرس گیرنده از دستور :RCPT TO استفاده می شود.

مثال زیر نحوه نوشتن این دستورات را نمایش می دهد:

آدرس پست الکترونیکی فرستنده : MAIL FROM

آدرس پست الکترونیکی گیرنده : RCPT TO

در هر پست الکترونیکی می توان چندین کلمه را به عنوان موضوع پیام مشخص کرد. برای تنظیم موضوع پست الکترونیکی می توانید از دستور :SUBJECT استفاده کنید.

مثال:

موضوع پست الکترونیکی : SUBJECT

در نهایت با استفاده از دستور data می توانید متن E.Mail خود را بنویسید:

مثالی از نحوه کاربرد دستور data :

DATA:

This is a Test

This is a Test

.

برای مشخص کردن پایان متن Mail نیز باید از یک نقطه استفاده کرد.

حال با استفاده از دستور QUIT می توانید میل خود را ارسال کنید و اتصال خود را به سرویس دهنده پست الکترونیکی قطع نمایید.

مثالی از چگونگی ارسال یک پست الکترونیکی :

telnet gmail.com 25

HELO gmail.com

MAIL FROM : test@gmail.com

RCPT TO : Ali@yahoo.com

SUBJECT: This is a Test

DATA:

Hi Ali

How are You?

.

QUIT

نکته:

سرویس دهنده SMTP در هر مرحله ارسال پست الکترونیکی برای شما پیغام های مناسبی صادر می کند.

نکته:

سرویس SMTP مشکلاتی دارد که این مشکلات در نسخه دیگری از این سرویس به نام ESMTP برطرف شده است (ESMTP در RFC 2821 شرح داده شده است) در هنگام برقراری ارتباط با یک سرویس دهنده SMTP اگر به جای پیام HELO دستور EHELO را بنویسید و این دستور پذیرفته شود، سرویس دهنده از ESMTP پشتیبانی می کند.

نکته:

در بعضی از سرویس دهنده های SMTP به جای دستور HELO باید از دستور HELLO استفاده کرد. اگر با نوشتن دستور HELO نتیجه ای نگرفتید دستور HELLO را امتهان کنید.

پروتکل POP3 :

پروتکل SMTP برای ارسال پست الکترونیکی بکار می رود. اما برای دریافت و خواندن نامه ها دریافت شده باید از پروتکل POP3 (Post Office Protocol) استفاده کرد. نوع قدیمی تر پروتکل POP3 به نام POP2 شناخته می شود.

سرویس POP3 به صورت استاندارد بر روی پورت شماره ۱۱۰ فعالیت می کند. و پورتی که برای سرویس POP2 در نظر گرفته شده است پورت شماره ۱۰۹ است.

برای اینکه بتوانید به صندوق پستی خود در یک سرویس دهنده پست الکترونیکی متصل شوید فرمان زیر را صادر کنید:

telnet شماره پورت ۱۱۰ آدرس سرویس دهنده پست الکترونیکی

مثال:

telnet gmail.com 110

با اجرای دستور فوق در صورتی که سرویس دهنده شما آماده فعالیت باشد، برنامه Telnet به سرویس POP3 که بر روی پورت ۱۱۰ فعال است متصل می شود.در این زمان شما باید با استفاده از دستورات POP3 کلمه عبور و رمز پست الکترونیکی خود را وارد کنید تا بتوانید نامه ها موجود در صندوق پستی خود را مدیریت کنید.

دستورات پروتکل POP3 به شرح زیر است:

- برای نوشتن نام کاربری از دستور USER استفاده می شود.
- با استفاده از دستور PASS کلمه عبور خود را وارد کنید.
- دستور LIST از نامه های موجود در صندوق پستی لیست تهیه می کند.
- دستور DELE xxx برای حذف نامه بکار می رود. xxx در اینجا شماره نامه ای است که با استفاده از دستور LIST مشخص می شود.
- برای خاوندن نامه می توان از دستور RETR xxx استفاده کرد. در این دستور xxx شماره نامه است.
- QUIT برای خروج از صندوق پستی بکار می رود.

- QUIT برای خروج از صندوق پستی بکار می رود.

مثال زیر نحوه کار با پروتکل POP3 را نشان می دهد:

telnet gmail.com 110

+OK POP3 server ready (پیام سرویس دهند)

USER Test

+OK

PASS XXXXXX

+OK login successful

LIST

1 2536

2 4563

3 8955

4 4122

5 6333

RETR 1

Salam

Hal Shoma

…

…

…

Bye

DELE 3

QUIT

+OK POP3 server disconnecting

نکته:

شما با فراگیری اصول برنامه نویسی شبکه می توانید با استفاده از دستورات و قوانین پروتکل های لایه کاربرد برنامه های دلخواه خود را برای این قراردادها بنویسید و از آنها استفاده کنید.

پروتکل TELNET :

با استفاده از پروتکل TELNET می توانید به وسیله یک ماشین از راه دور دستورات خود را در ماشین مقصد اجرا کنید. این خصوصیت به مدیران شبکه اجازه می دهد، بدون اینکه در مقابل ماشین سرور بنشینند، به وسیله یک کامپیوتر متصل به شبکه در هر کجای دنیا که باشند دستورات خود را اجرا کنند.

پروتکل TELNET بر روی پورت شماره ۲۳ فعالیت می کند. این پروتکل به دلیل ماهیتی که دارد، ممکن است از نظر امنیتی برای یک شبکه مشکل ایجاد کند. به همین دلیل است که اکثر مدیران شبکه این سرویس مفید را از سیستم حذف می کنند یا آن را به حالت غیر فعال در می آورند.

برای اتصال به سیستمی که سرویس TELNET بر روی آن فعال است می توانید دستور زیر را اجرا کنید:

telnet آدرس ماشین سرور ۲۳

مثال:

telnet sharef.edu 23

دستور بالا سعی می کند که به سرویس TELNET دانشگاه صنعتی شریف متصل شود.

پشته پروتکلی TCP/IP :

پشته پروتکلی TCP/IP :

مدل مرجع OSI یک مدل استاندارد است که تمامی جزئیات طراحی یک رویه ارتباطی در شبکه های کامپیوتری را در خود گنجانده است و برای هماهنگی در طراحی مدل های مختلف توسط سازمان جهانی استاندارد (ISO) ایجاد شده است. اما به دلیل پیچیدگی های فراوان و همچنین جزئیات خیلی زیاد هیچ گاه به صورت واقعی برای کار در شبکه های کامپیوتری پیاده سازی نشده است.

از نقاط ضعف مدل OSI می توان موارد زیر را ذکر کرد :

در مدل OSI انتخاب هفت لایه بیشتر جنبه نمایشی داسته است تا تکنیکی، زیرا دو لایه جلسه و نمایش تقریبا بدون استفاده هشتند.

مدل OSI به دلیل پیچیدگی بیش از حد آن مبهم است و نمی توان به راحتی تمام استاندارد های موجود در آن را پیاده سازی کرد.

در این مدل (OSI) بعضی از موارد نظیر آدرس دهی و همچنین خطا یابی در لایه های مختلف تکرار شده است.

مجموع معایب فوق و همچنین نقاط ضعف دیگری ازاین مدل باعث کندی بیش از حد این مدل شبکه ای شده و همین امر موجب شد تا هیچگاه به صورت عمومی از این استاندارد استفاده نشود. ولی این مدل به دلیل جامعیتش به صورت یک استاندارد برای بقیه مدل های تولیدی شبکه قرار گرفته است.

برای کار درشبکه به صورت واقعی نیاز به این همه جزئیات احساس نمی شود و پروتکل هایی که در شبکه های واقعی مورد استفاده قرار می گیرند اغلب به حداقل جزئیات در هر قسمت قناعت می کنند. IPX/SPX ، TCP/IP و Apple Talk نمونه هایی از پشته های پروتکلی هستند که در شبکه های واقعی مورد استفاده قرار گرفته اند.

در این قسمت ما قصد داریم پشته پروتکل TCP/IP را شرح دهیم. دلیل این امر این است که امروزه پشته پروتکلی TCP/IP مدلی استاندارد و عمومی در شبکه های مختلف است و همچنین شبکه اینترنت نیز بر مبنای این مدل فعالیت می کند.

در شکل زیر مدل OSI در کنار مدل TCP/IP آمده است شما در این شکل می توانید تفاوت این دو مدل را در نوع و تعداد لایه ها شماهده کنید:

شکل ۲۵-۱:
مقایسه ساختار TCP/IP و ساختار OSI (شکل سمت چپ مدل OSI و شکل سمت راست مدل TCP/IP)

لایه میزبان شبکه :

همانطور که در شکل فوق مشاهده می کنید ، در مدل TCP/IP دو لایه فیزیکی و لایه پیوند دادها در مدل OSI با یکدیگر ادغام شده اند و لایه میزبان شبکه را در مدلTCP/IP به وجود آورده اند. در مدل TCP/IP به دلیل به وجود آوردن هماهنگی با سخت افزار های متفاوت در لایه میزبان شبکه قسمت اتصال به سخت افزار را به صورت Protocol Free معرفی کرده اند یعنی این مدل می تواند با هر گونه سخت افزاری هماهنگ شود و تحت هر شبکه ای به وظایف خود عمل کند. این قابلیت باعث شده است تا این مدا در شبکه اینترنت به خوبی کار کند و مورد استفاده قرار گیرد.

لایه اینترنت :

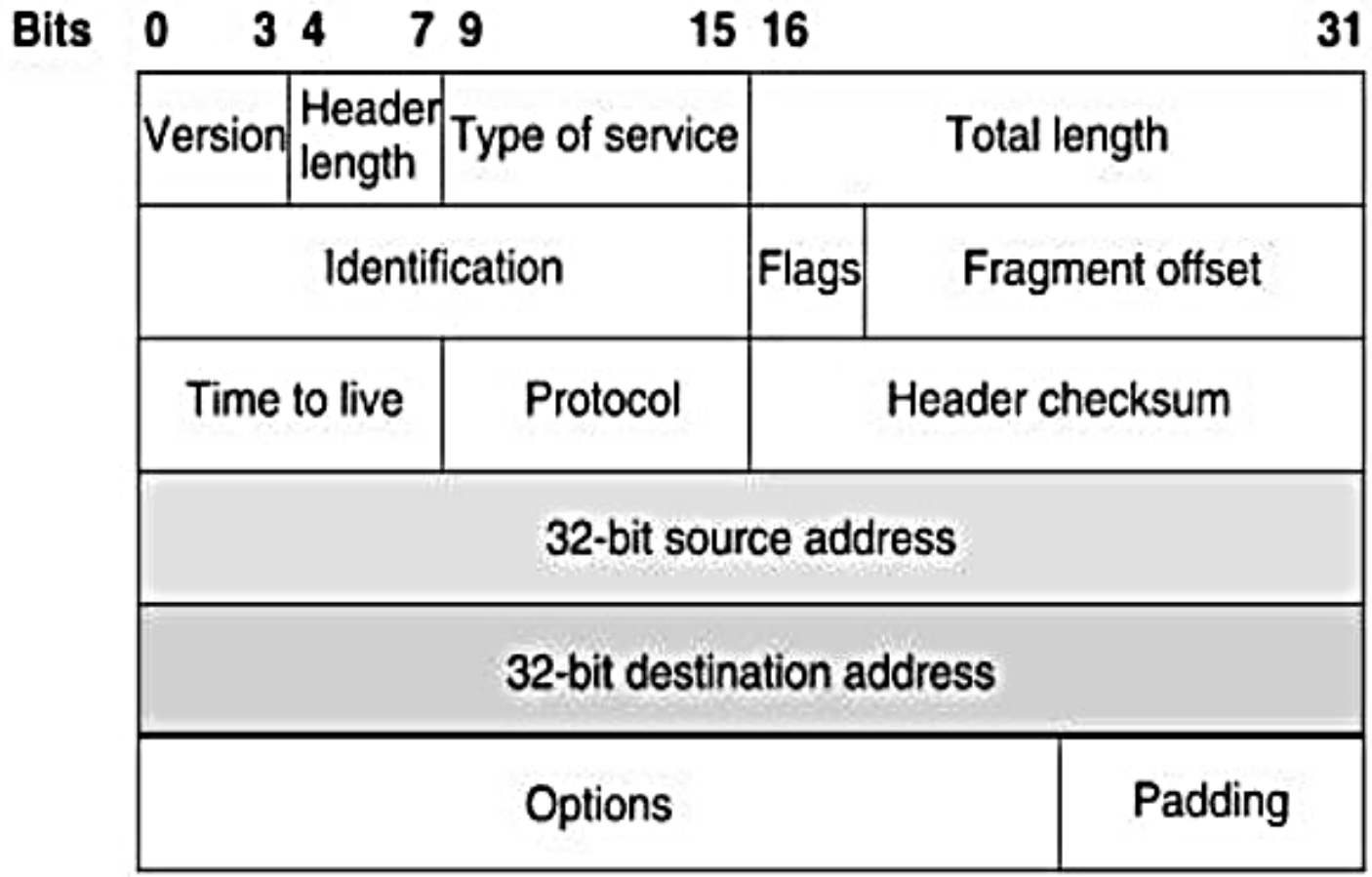
لایه شبکه در مدل OSI جای خود را به لایه اینترنت در مدل TCP/IP داده است. لایه اینترنت در مدل TCP/IP وظیفه مسیریابی بسته های TCP را به عهده دارد. این لایه یک لایه Hop To Hop است و در هر مرحله بسته های TCP را به مسیریاب بعدی انتقال می دهد، این روند تا جایی ادامه می یابد که بسته ها به مقصد برسند. در این لایه با استفاده از پروتکل IP (Internet Protocol) آدرس ماشین های موجود در شبکه را مشخص می کنند.

پروتکل IP :

پروتکل IP یک پروتکل برای آدرس دهی و انتقال بسته ها در شبکه اینترنت است. این پروتکل به هر بسته ای که می خواهد بر روی شبکه ارسال شود یک هدر اضافه می کند. این هدر در مسیر یاب ها و همچنین سویچ ها موجود در مسیر تجزیه و تحلیل می شود و در هر مرحله تحویل گام بعدی داده می شود. پروتکل IP درحال حاضر در دو ویرایش موجود است :

- IPv4
- IPv6

IPv4 ویرایش قدیمی تر این پروتکل می باشد که هم کنون در شبکه اینترنت مورد استفاده قرار می گیرد. هدر این نسخه را می توانید در شکل ۲۶-۱ مشاهده می کنید.



شکل ۲۶-۱) نمایش هدر IPv4

شرح فیلد های مختلف هدر IPv4 :

- فیلد Version مشخص می کند که این بسته تحت کدام ویرایش از پروتکل IP قرار دارد.
- فیلد IHL مشخص می کند که طول هدر چند کلمه 32 بیتی است.
- Type of Service برای تنظیم قابلیت اطمینان یا انتقال با سرعت بالا مورد استفاده قرار می گیرد.
- فیلد Total Lengthطول کل بسته به همراه هدر را مشخص می کند.
- فیلد Identification در صورتی که بسته به قطعاتی شکسته شود ، مشخص می کند که هر قطعه مربوط به کدام بسته است.
- فیلد Flags شامل ۲ بیت است: بیت DF و بیت MF . اگر بیت DF برابر یک شود، هیچ مسیریابی حق شکستن بسته را ندارد. و اگر MF یک شود، بسته به قطعاتی شکسته شده است که همه قطعات یک مشخصه منحصربه فرد خواهند داشت که در فیلد Identification ذکر می شود.
- فیلد Fragment Offset شماره قطعه را مشخص می کند.
- فیلد Time to Live یک شمارنده است که طول عمر بسته را مشخص می کند. این شمارنده بعد ازعبور از هر مسیریاب یک واحد کاهش می یابد، و هنگامی که به صفر برسد بسته حذف خواهد شد. از این مکانیزم می توان برای حذف بسته های سرگردان از شبکه استفاده کرد.

- فیلد Protocol تعیین می کند، که این بسته تحت پروتکل TCP کار می کند یا UDP.
- Check Sum برای کنترل خطا در نظر گرفته شده است.
- فیلد Source Address آدرس IP کامپیوتر مبداء را مشخص می کند.
- Destination Address آدرس IP ماشین مقصد را نگهداری می کند.
- فیلد Options برای کاربرد های خاص و شخصی در نظر گرفته شده است.

اگر در هدر IPv4 دقت کنید، می بینید که در این هدر حداکثر ۳۲ بیت برای آدرس دهی IP در نظر گرفته شده است. همانطور که می دانید با این مقدار بیت تنها می توان دو به توان ۳۲ ماشین در شبکه را آدرس دهی کرد. امروزه به دلیل گسترش بیش از حد شبکه جهانی اینترنت دیگر این مقدار ماشین جوابگوی نیاز روز افزون جهان نمی باشد به همین دلیل ویرایش جدیدتری از پروتکل IP مطرح شده است. این ویرایش IPv6 است. اگر چه تا کنون به صورت عمومی و تجاری از پروتکل IPv6 استفاده نشده است، ولی در آینده نزدیک باید شاهد رشد و همه گیر شدن ویرایش جدید پروتکل IP باشیم.

در شکل ۲۷-۱ می توانید هدر IPv6 را مشاهده کنید:

Version	Priority	Flow Label	
Pay Land Length	Next Header	Hop Limit	
Source Address			
Destination Address			

شکل ۲۷-۱ نمایش هدر IPv6

شرح قسمت های مختلف هدر IPv6 :

- فیلد Version حاوی عدد ۶ برای تعیین ویرایش هدر IP می باشد.

- فیلد Priority حاوی اولویت بسته می باشد. برای امور عادی ۰ تا ۷ و برای کارهای بلادرنگ ۸ تا ۱۵. طول این فیلد ۴ بیت می باشد.

- فیلد Priority حاوی اولویت بسته می باشد. برای امور عادی ۰ تا ۷ و برای کارهای بلادرنگ ۸ تا ۱۵. طول این فیلد ۴ بیت می باشد.

- فیلد Flow Label جریان بسته را مشخص می کند.

- فیلد Pay Land Length مش خص می کند، که طول بسته بدون ۴۰ بایت مربوط به اولین هدر چقدر می باشد.

- فیلد Next Header مشخص می کند که هدر بعدر وجود دارد یا خیر.

- Hop Limit طول عمر بسته را مشخص می کند. این فیلد مشابه فیلد Time to Live هدر بسته IPv4 است.

- فیلد Source Address مشخص کننده ادرس مبدا می باشد. در IPv6 این فیلد ۱۲۸ بیت طول دارد که به وسیله ان می توان ۲ به توان ۱۲۸ ماشین را آدرس دهی کرد.
- فیلد Destination Address مشخص کننده آدرس مقصد است. طول این فیلد ۱۲۸ بیت می باشد.

نکته:

در سیستم IPv6 هر بسته می تواند تا شش هدر اضافی دیگر نیز داشته باشد که از این هدر ها می توان برای عملیات مسیریابی، رمزنگاری، تایید هویت ، قطعه بندی و ... استفاده کرد.

نکته:

آدرس هر هدر به وسیله فیلد Next Header در هدر بسته های IPv6 مشخص می شود.

نکته:

در لایه اینترنت جهت عیب یابی شبکه و بررسی عملیات، پروتکل های دیگری نیز وجود دارد. از این نوع پروتکل ها می توان ICMP و IGMP و در IPv6 می توان، ICMPv6 ، MLD و ND را نام برد.

پروتکل ICMP :

به دلیل اهمییت این پروتکل به شرح مختصری از این پروتکل می پردازیم.

این پروتکل بیشتر جهت عیب یابی در شبکه کاربرد دارد. بسته های این نوع پروتکل از بین مسیریاب های مختلف شبکه عبور می کنند، و به وسیله آنها می توان فهمید که چه ماشینی در شبکه فعال است ، سرعت انتقال داده ها در بین کانال های مختلف شبکه چقدر است و همچنین آدرس ماشین های مختلف را در شبکه بدست آورد.

ار ابزارهای که بر مبنای این نوع پروتکل فعالیت می کنند می توان موارد زیر را نام برد:

ابزار Ping که با استفاده از این ابزار می توان سرعت انتقال اطلاعات را در شبکه مشخص کرد. نمونه ای از خروجی این ابزار را در زیر مشاهده می کنید:

```
C:\ ping   192.168.5.63

Pinging 192.168.5.63 with 32 bytes of data:

Reply from 192.168.5.63: bytes=32 time=1ms TTL=128

Reply from 192.168.5.63: bytes=32 time<10ms TTL=128

Reply from 192.168.5.63: bytes=32 time<10ms TTL=128
```

Reply from 192.168.5.63: bytes=32 time<10ms TTL=128

Ping statistics for 192.168.5.63:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

Minimum = 1ms, Maximum = 1ms, Average = 1ms

در مثال بالا ابزار Ping سیستم عامل ویندوز مورد استفاده قرار گرفته است و همانطور که شماهده می کنید با استفاده از این ابزار به ماشینی با آدرس 192.168.5.63 پینگ شده است. این برنامه با ارسال ۴ بسته ICMP و در نهایت مشخص کردن سرعت ارسال و تعداد خطاهای روی داده میزان خوبی برای قضاوت در مورد کارایی شبکه در اختیار ما قرار می دهد.

لایه انتقال :

در مدل TCP/IP لایه انتقال را لایه TCP نیز می گویند. زیرا عملیات کنترل در این لایه انجام می شود. در این لایه قرارداد هایی که در لایه انتقال مدل OSI وجود داشت تعریف شده اند.

در این لایه پورت های نوع UDP و TCP برای انتقال اطلاعات از ماشین مبدا به ماشین مقصد تعریف شده اند (شرح این موارد در صفحات قبلی آمده است).

در این لایه عملیات شکستن بسته ها نیز انجام می شود. و هر بسته که آماده ارسال شده است را به لایه اینترنت جهت ارسال تحویل می دهد.

برای مشاهده وضعیت پورت های باز و فعال ماشین خود و همچنین آدرس و مشخصات ماشین های راه دوری که به این پورت ها متصل هستند می توانید از ابزار NetStat که همراه پشته پروتکلی TCP/IP است استفاده کنید.

در زیر خروجی این ابزار را در سیستم عامل ویندوز مشاهده می کنید:

```
C:\NetStat /na
Active Connections
  Proto   Local Address          Foreign Address        State
```

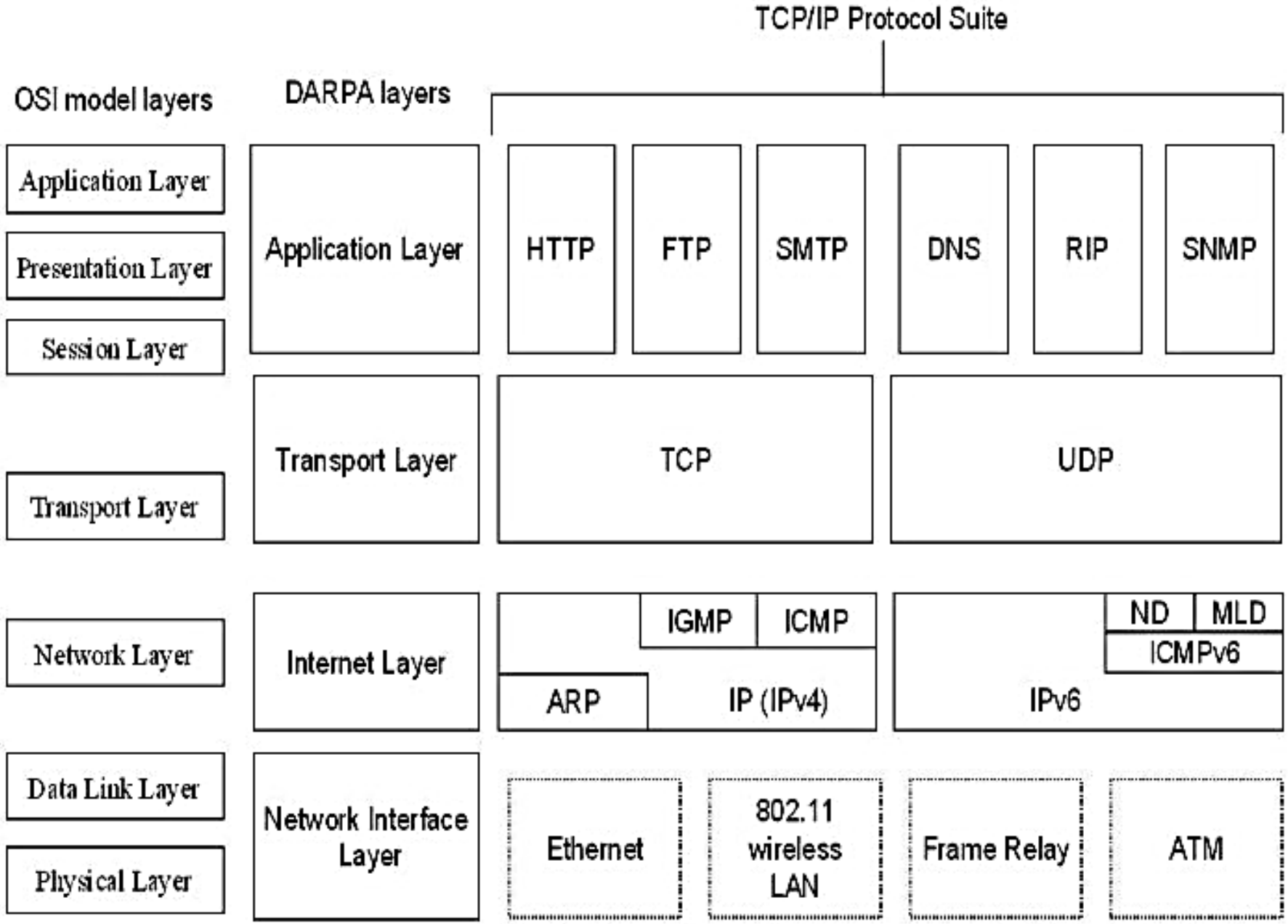
TCP	0.0.0.0:135	0.0.0.0:0	LISTENING
TCP	127.0.0.1:1025	0.0.0.0:0	LISTENING
TCP	169.254.183.114:137	0.0.0.0:0	LISTENING
TCP	169.254.183.114:138	0.0.0.0:0	LISTENING
TCP	169.254.183.114:139	0.0.0.0:0	LISTENING
UDP	169.254.183.114:137	*:*	
UDP	169.254.183.114:138	*:*	

همانطور که در مثال بالا مشاهده می کنید خروجی ابزار NetStat در چهار بخش زیر تنظیم شده است:

- Proto .
- Local Address .
- Foreign Address .
- State .

در قسمت Proto پروتکل ارتباطی نمایش داده شده است، در قسمت Local Address آدرس ماشین محلی همراه با شماره پورت ارتباطی آمده است، در قسمت Foreign Address شماره پورت همراه با آدرس IP ماشین راه دوری که به پورت مورد نظر در ماشین محلی متصل است نشان داده می شود. و در نهایت در قسمت State وضعیت پورت که می تواند حالت های Listing ، Closed ، Connect و... را داشته باشد را نمایش می دهد.

شکل ۲۸-۱ قسمت های مختلف پروتکل TCP را نشان می دهد.



شکل ۲۸-۱ نمایش ساختار TCP/IP

لایه کاربرد :

در بالاترین قسمت پشته پروتکل TCP/IP لایه کابرد قراردارد. این لایه یک لایه با مکانیزم End to End است. در این لایه پروتکل های مختلفی برای مدیریت بر برنامه های کابردی و اداره آنها پیش بینی شده است.

تعدادی از این نوع پروتکل ها را در قسمت های قبلی مورد بررسی قرار دادیم وبه نحوه انجام کار و همچنین قوانین تعریف شده در آنها آشنا شده ایم اکنون در این قسمت به معرفی برخی دیگر از این پروتکل ها می پردازیم:

پروتکل DNS (Domain Name Service) :

به خاطر سپردن نام ها برای انسان خیلی راحتر از اعداد است به همین دلیل می بایست مکانیزمی در نظر گرفت تا شماره IP ماشین های مختلف در شبکه را که معرف آدرس آن ماشین در شبکه است به یک نام خاص نگاشت شود. این وظیفه پروتکل DNS است که یک نام خاص را به یک آدرس IP مبدل کند. مثلا شما در مرورگر اینترنتی خود عبارت google.com را می نویسید و مرورگر صفحات مربوط به سرویس دهنده وب این ماشین را در مرورگر شما نمایش می دهد. می دانیم که تنها در شبکه برای پروتکل های دیگر ادرس IP معنا

دارد نه مثلا رشته کاراکتری google.com پس در این وسط چه اتفاقی افتاده؟ این همان کاری است که سرویس DNS انجام می دهد، یعنی تبدیل یک رشته به آدرس IP آن ماشین.

نکته:

پروتکل DNS به صورت استاندارد بر روی پورت UDP 53 فعالیت می کند.

لایه کاربرد در مدل TCP/IP شامل پروتکل های گوناگون دیگری برای سهولت استفاده از شبکه می باشد نظیر:

- DHCP با استفاده از این پروتکل می توان به ماشین های متصل به یک شبکه به صورت خودکار یک آدرس IP از اختصاص داد.

- پروتکل USENET که پروتکلی برای پیام رسانی در شبکه می باشد.

تا بدین جا شما مختصری در مورد نحوه پیاده سازی و تئوری شبکه های کامپیوتری فرا گرفته اید. ولی همان طور که می دانید با مطالعه یک مقدمه کوتاه نمی توان همه موارد را به خوبی درک کرد و یاد گرفت. این مختصر از تئوری سیستم های شبکه برای درک مفاهیم بعدی این کتاب مورد نیاز بود. چناچه مایل هستید که در این زمینه اطلاعات بیشتری کسب کنید، باید به مراجع معتبر جهانی نظیر RFC مراجعه کنید و اطلاعات هر جزء از شبکه را به طور دقیق و موشکافانه مطالعه نمایید.