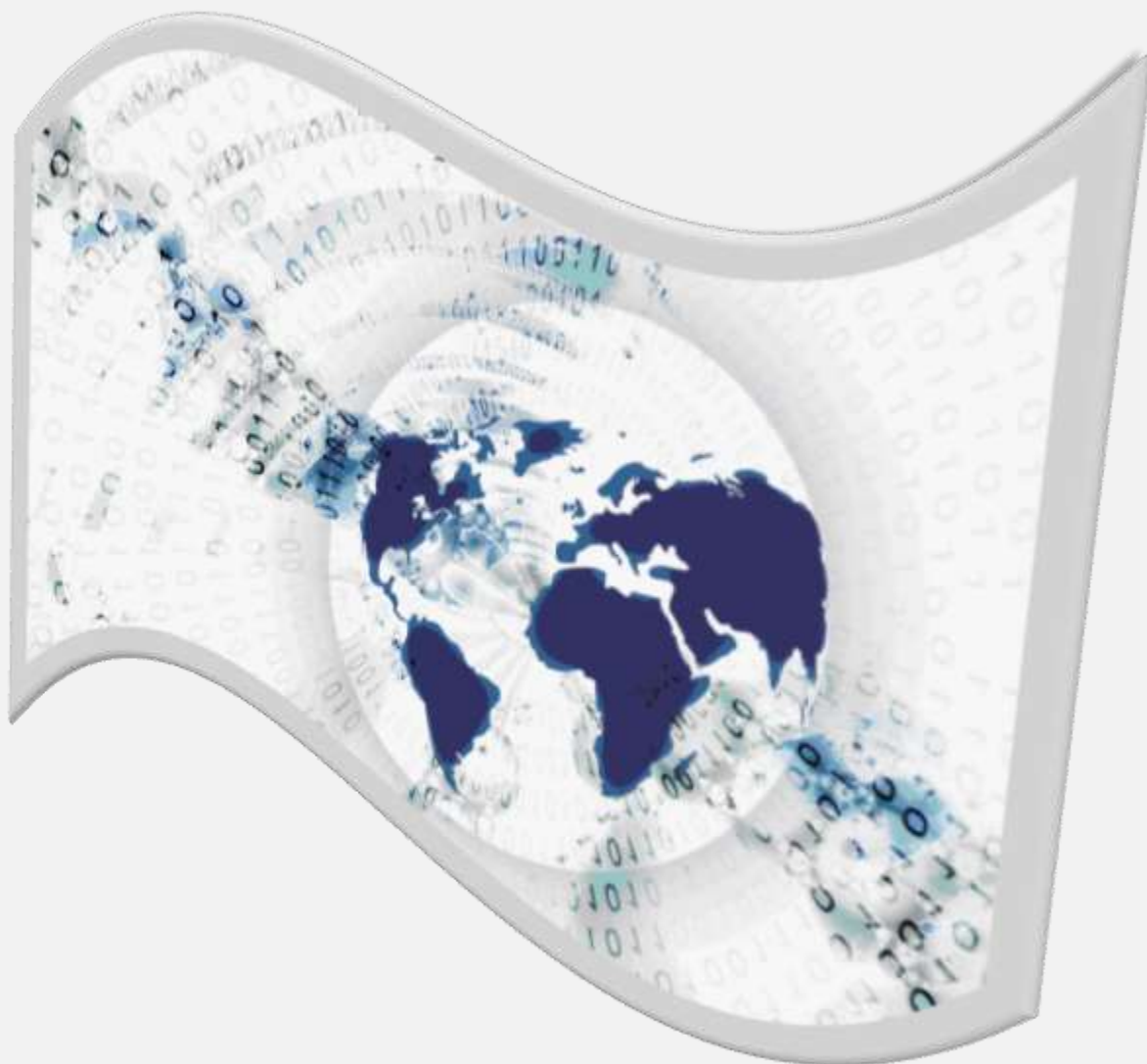


مفهوم و کاربرد شبکه های کامپیوتر



تألیف و گرد آوری: میثاق نوازی

ویرایش اول

هو العالم

سرشناسه : نوازی، میثاق

عنوان و نام پدیدآور: مفهوم و کاربرد شبکه های کامپیوتر / تالیف و گردآوری میثاق نوازی

مشخصات ظاهری: ۳۶۱ ص

شابک: ۹۷۸-۶۰۰-۰۴-۲۵۰۷-۴

وضعیت فهرست نویسی: فیپا

موضوع: شبکه های کامپیوتری

موضوع: شبکه های کامپیوتری - معماری

رده بندی کنگره: ۷۱۳۹۳م۹/ن۵/TK۵۱۰۵

رده بندی دیویی: ۰۰۴/۶

شماره کتابشناسی ملی: ۳۷۳۴۲۸۰

فهرست مطالب:

۷.....	مقدمه:
۸.....	: Network history
۱۱.....	: Networking Basics-۱/۰
۱۲.....	: Network communication-۱/۱
۳۶.....	:OSI model -۱/۲
۵۵.....	:TCP/IP-۱/۳
۶۵.....	:Network cables-۲/۱
۷۶.....	:Network Interface Adapters-۲/۲
۸۰.....	:Network Hubs-۲/۳
۸۴.....	:Network Connections-۳/۰
۸۶.....	:Switching-۳/۱
۱۰۳.....	:Routing-۳/۲
۱۰۹.....	: Networking Software-۴/۰
۱۱۱.....	:Operating Systems-۴/۱
۱۱۶.....	:Directory Services-۴/۲
۱۲۳.....	: Data-Link Layer Protocol-۵/۰
۱۲۵.....	:Ethernet-۵/۱

۱۳۹..... :Token Ring-۵/۲

۱۶۴..... :Wireless Networking-۵/۳

۱۷۰..... : network layer-۶/۰

۱۷۲..... :ip-۶/۱

۱۷۶..... : ip address-۶/۲

۱۸۱..... : ip address classes-۶/۳

۱۸۶..... :subnetmask-۶/۴

۱۸۸..... :ARP-۶/۵

۱۹۱..... :ICMP-۶/۶

۱۹۲..... :IGMP-۶/۷

۱۹۳..... :transport layer-۷/۰

۱۹۴.....:TCP-۷/۱

۲۰۴.....:UDP-۷/۲

۲۰۸..... :routing-۸/۰

۲۰۹..... : routing-۸/۱

۲۱۱..... :Routing Protocol-۸/۲

۲۱۴..... :TCP/IP Applications-۹/۰

۲۱۵..... :DHCP-۹/۱

۲۲۱.....:DNS-۹/۲

۲۳۰.....:FTP-۹/۳

۲۴۱.....:HTTP-۹/۴

۲۵۵.....:HTTPS-۹/۵

۲۵۸.....:IMAP-۹/۶

۲۶۰.....:POP۳-۹/۷

۲۶۶.....:SMTP-۹/۸

۲۷۰.....:SOAP-۹/۹

۲۷۶.....:SSH VS FTP-۹/۱۰

۲۷۹.....:SSL-۹/۱۱

۲۸۵.....:TCP/IP Utilities-۱۰/۰

۲۸۷.....:Ping-۱۰/۱

۲۸۸.....:Tracert/traceroute-۱۰/۲

۲۹۰.....:ifconfig-۱۰/۳

۲۹۲.....:netstat-۱۰/۴

۲۹۳.....:Telnet-۱۰/۵

۲۹۸.....:NSLookup-۱۰/۶

۳۰۲.....Remote Network Access-۱۱/۰

۳۰۴..... : Using Remote Connections-۱۱/۱

۳۳۳..... :SLIP and PPP-۱۱/۲

۳۳۷.....wan technology-۱۱/۳

۳۴۱..... :Network Security-۱۲/۰

۳۴۳..... :Firewall-۱۲/۱

۳۴۹..... :ids-۱۲/۲

۳۶۰..... :Security Protocols-۱۲/۳

۳۶۷..... منابع

مقدمه

قصه داشتیم مقدمه ای بنویسیم اما بعد از دیدن این مقدمه در کتابی دیگر...

مرا مجبور به مقدمه گویی و مقدمه نویسی و مقدمه خوانی و هر آنچه مقدمه ای می طلبد مکن! من خیلی وقت است هر چه می کشم از همین "من" است. اما چه می شود کرد؟ نمی شود جایگزینی برای این کلمه ی دو حرفی سرشار از تهی یافت که دلیل بر وجود کسی باشد که خیلی خیلی شبیه درونیات یک نفر که باز هم می شود "من" باشد.

با من مثل خدا "تا" نکن که هر واجبی را برایش مقدمه ی واجبی بگذاری. آن که خدا گفت شرط فرض است و آنچه تو از باب مقدمات می طلبی شرط دل دادگی است. آدم دل داده شاید "من" گفتنش پا برجا باشد اما دلش می لرزد به هر نگاهی که یار برقد و قامتش بیندازد اما حساب و کتاب "من" با مقدمه های واجب واجب الوجود توفیر دارد! او مقدمه ای را از باب وجوب موخره اش واجب کرده ولی راه را باز گذاشته که میخواهی عبادت احرار را داشته باشی یا تجار! به حال او فرقی نمی کند نخ کدام مقدمه را بگیری و به کدام واجب بررسی. واجب الوجود فقط نخ مقدمه می دهد که پای "من" را به وادی عبادت بکشاند. این هم از کریمانه بودنش است. اما تو وقتی نخ مقدمه می دهی من هی یاد "من" می افتم و یاد سر به سر گذاشتن ...

بگذر از این بحث مقدمات ... من مات من العشق فقد مات شهیدا!

: Network history

در سال ۱۹۵۷ نخستین ماهواره، یعنی اسپوتنیک توسط اتحاد جماهیر شوروی سابق به فضا پرتاب شد. در همین دوران رقابت سختی از نظر تسلیحاتی بین دو ابرقدرت آن زمان جریان داشت و دنیا در دوران رقابت سختی از نظر تسلیحاتی بین دو ابرقدرت آن زمان جریان داشت و دنیا در دوران جنگ سرد به سر می برد. وزارت دفاع امریکا در واکنش به این اقدام رقیب نظامی خود، آژانس پروژه های تحقیقاتی پیشرفته یا آرپا (ARPA) را تاسیس کرد. یکی از پروژه های مهم این آژانس تامین ارتباطات در زمان جنگ جهانی احتمالی تعریف شده بود. در همین سال ها در مراکز تحقیقاتی غیر نظامی که بر امتداد دانشگاه ها بودند، تلاش برای اتصال کامپیوترها به یکدیگر در جریان بود. در آن زمان کامپیوتر های Mainframe از طریق ترمینال ها به کاربران سرویس می دادند. در اثر اهمیت یافتن این موضوع آژانس آرپا (ARPA) منابع مالی پروژه اتصال دو کامپیوتر از راه دور به یکدیگر را در دانشگاه MIT بر عهده گرفت. در اواخر سال ۱۹۶۰ اولین شبکه کامپیوتری بین چهار کامپیوتر که دو تای آنها در MIT، یکی در دانشگاه کالیفرنیا و دیگری در مرکز تحقیقاتی استنفورد قرار داشتند، راه اندازی شد. این شبکه آرپانت نامگذاری شد. در سال ۱۹۶۵ نخستین ارتباط راه دور بین دانشگاه MIT و یک مرکز دیگر نیز برقرار گردید. در سال ۱۹۷۰ شرکت معتبر زیراکس یک مرکز تحقیقاتی در پالوآلتو تاسیس کرد. این مرکز در طول سال ها مهمترین فناوری های مرتبط با کامپیوتر را معرفی کرده است و از این نظریه به یک مرکز تحقیقاتی افسانه ای بدل گشته است. این مرکز تحقیقاتی که پارک (PARC) نیز نامیده می شود، به تحقیقات در زمینه شبکه های کامپیوتری پیوست. تا این سال ها شبکه آرپانت به امور نظامی اختصاص داشت، اما در سال ۱۹۲۷ به عموم معرفی شد. در این سال شبکه آرپانت مراکز کامپیوتری بسیاری از دانشگاه ها و مراکز تحقیقاتی را به هم متصل کرده بود. در سال ۱۹۲۷ نخستین نامه الکترونیکی از طریق شبکه منتقل گردید. در این سال ها حرکتی غیر انتفاعی به نام MERIT که چندین دانشگاه بنیان گذار آن بوده اند، مشغول توسعه روش های اتصال کاربران ترمینال ها به کامپیوتر مرکزی یا میزبان بود. مهندسان پروژه MERIT در تلاش برای ایجاد ارتباط بین کامپیوترها، مجبور شدند تجهیزات لازم را خود طراحی کنند. آنان با طراحی تجهیزات واسطه برای مینی کامپیوتر DEC PDP-11 نخستین

بستر اصلی یا Backbone شبکه کامپیوتری را ساختند. تا سال ها نمونه های اصلاح شده این کامپیوتر با نام PCP¹ نقش میزبان را در شبکه ها ایفا می کرد. نخستین شبکه از این نوع که چندین ایالت را به هم متصل می کرد Michne نام داشت. روش اتصال کاربران به کامپیوتر میزبان در آن زمان به این صورت بود که یک نرم افزار خاص بر روی کامپیوتر مرکزی اجرا می شد. و ارتباط کاربران را برقرار می کرد. اما در سال ۱۹۷۶ نرم افزار جدیدی به نام Hermes عرضه شد که برای نخستین بار به کاربران اجازه می داد تا از طریق یک ترمینال به صورت تعاملی مستقیماً به سیستم MERIT متصل شوند. این، نخستین باری بود که کاربران می توانستند در هنگام برقراری ارتباط از خود بپرسند: کدام میزبان؟ از وقایع مهم تاریخچه شبکه های کامپیوتری، ابداع روش سوئیچینگ بسته ای یا Switching Packet است. قبل از معرفی شدن این روش از سوئیچینگ مداری یا Switching Circuit برای تعیین مسیر ارتباطی استفاده می شد. اما در سال ۱۹۷۴ با پیدایش پروتکل ارتباطی IP/TCP از مفهوم Switching Packet استفاده گسترده تری شد. این پروتکل در سال ۱۹۸۲ جایگزین پروتکل NCP شد و به پروتکل استاندارد برای آرپانت تبدیل گشت. در همین زمان یک شاخه فرعی بنام MILnet در آرپانت همچنان از پروتکل قبلی پشتیبانی می کرد و به ارائه خدمات نظامی می پرداخت. با این تغییر و تحول، شبکه های زیادی به بخش تحقیقاتی این شبکه متصل شدند و آرپانت به اینترنت تبدیل گشت. در این سال ها حجم ارتباطات شبکه ای افزایش یافت و مفهوم ترافیک شبکه مطرح شد. مسیر یابی در این شبکه به کمک آدرس های IP به صورت ۳۲ بیتی انجام می گرفته است. هشت بیت اول آدرس IP به شبکه های محلی تخصیص داده شده بود که به سرعت مشخص گشت تناسبی با نرخ رشد شبکه ها ندارد و باید در آن تجدید نظر شود. مفهوم شبکه های LAN و شبکه های WAN در سال دهه ۷۰ میلادی از یکدیگر تفکیک شدند. در آدرس دهی ۳۲ بیتی اولیه، بقیه ۲۴ بیت آدرس به میزبان در شبکه اشاره می کرد. در سال ۱۹۸۳ سیستم نامگذاری دامنه ها (System Name Domain) به وجود آمد

¹ Processor Communications Pri

و اولین سرویس دهنده نامگذاری (Server Name) راه اندازی شد و استفاده از نام به جای آدرس های عددی معرفی شد. در این سال تعداد میزبان های اینترنت از مرز ده هزار عدد فراتر رفته بود.

فصل ۱

Networking Basics

: Networking Basics

درباره ی این فصل

در این فصل به معرفی اصول اساسی و ساختار معماری از ارتباطات شبکه میپردازیم. این مفاهیم در بقیه این کتاب و همچنین در زندگی واقعی بارها و بارها با آن روبرو خواهید شد. شما این مطالب را باید کامل خوانده و درک کنید تا در ادامه کتاب به مشکل بر نخورید همچنین درک این اصول در زندگی روزمره خالی از لطف نیست.

لذا مهمترین فصل این کتاب همین فصل است.

درس ۱:

ارتباطات شبکه

در این درس به مفاهیم اصلی از ارتباطات شبکه و برخی از ساختارهایی برای ساخت داده های شبکه مورد استفاده قرار می گیرند میپردازیم. انواع بسیاری از داده های شبکه وجود دارند از شبکه های سازمانی که توسط شرکت های بزرگ مورد استفاده قرار میگیرند گرفته تا به یک شبکه ساده متشکل از دو گره که در یک منزل شخصی استفاده می شود.

با این حال، بسیاری از اصول همان اصول اولیه و مفاهیم ارسال و دریافت اطلاعات میباشد، صرف نظر از اندازه و پیچیدگی.

Protocol

قرارداد یا پروتکل در شبکه های رایانه ای به مجموعه قوانینی اطلاق می گردد که نحوه ارتباطات را قانونمند می نماید. نقش پروتکل در کامپیوتر نظیر نقش زبان برای انسان است. برای مطالعه یک کتاب نوشته شده به فارسی می بایست خواننده شناخت مناسبی از زبان فارسی را داشته باشد. به منظور ارتباط موفقیت آمیز دو دستگاه در شبکه نیز باید هر دو دستگاه از یک پروتکل مشابه استفاده کنند.

در علوم رایانه و ارتباطات، پروتکل عبارت است از استاندارد یا قراردادی که برای ارتباط میان دو ند برقرار می شود. پروتکل اتصال بین دو ند، انتقال داده بین آن دو و تبادلات میان آنها را ممکن کرده و آن را کنترل می کند. پروتکل در ساده ترین حالت می تواند به عنوان قوانین اداره منطق، ترکیب و همزمانی ارتباطات در نظر گرفته شود. پروتکل ها ممکن در سخت افزار یا نرم افزار یا ترکیبی از این دو پیاده سازی شوند. پروتکل در پایین ترین سطح رفتار اتصال سخت افزاری را تعریف می کند. معنی لغوی پروتکل مجموعه قوانین است.

از آن جا که پروتکل ها در کارکرد و پیچیدگی بسیار متفاوتند و انواع زیادی دارند، بیان کردن تعریف یا توصیفی عام در مورد آنها دشوار است. بیشتر پروتکل ها یک یا چند مورد از ویژگی های زیر دارا هستند:

- شناسایی بستر فیزیکی اتصال (سیم یا بی سیم) و یا تشخیص وجود نقطه مقصد یا ند مقصد
- توافق مراده اتصال (هندسیکینگ)
- مذاکره در مورد ویژگی های مختلف اتصال
- شروع کردن و پایان دادن به پیام های رد و بدل شده و فراهم کردن نیاز ناشی از آن
- پایان دادن به جلسه گفتگو و یا اتصال
- قالب بندی پیام ها

- اصلاح پیام‌های دریافتی ناقص یا بدقالب بندی شده (تصحیح خطا)
- فهمیدن قطع ناگهانی ارتباط و یا اتصال
- رمزنگاری داده ها
- فشرده سازی داده ها

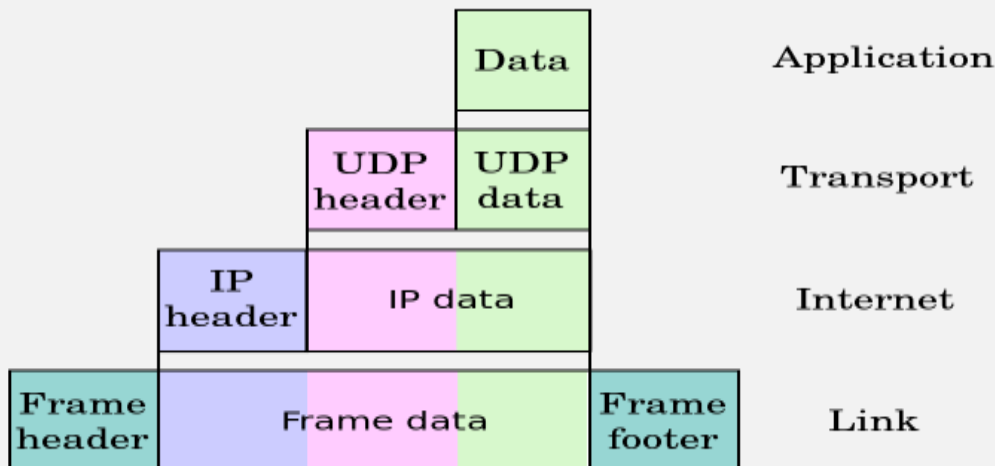
پروتکل های پشته ای^۱

یک پروتکل پشته ای، شامل مجموعه ای از پروتکل ها است که با یکدیگر فعالیت نموده تا امکان انجام یک عملیات خاص را برای سخت افزار و یا نرم افزار فراهم نمایند.

که برای درک این مفهوم میتوان خشاب یک اسلحه را تصور کرد که هر گلوله وظیفه ای خاص بر عهده دارد.

پروتکل TCP/IP نمونه ای از پروتکل های پشته ای است. پروتکل فوق از چهار لایه استفاده می نماید.

شکل زیر یک پروتکل پشته ای میباشد.



^۱protocol stack

شبکه محلی LAN¹:

ارتباط و اتصال بیش از دو یا چند رایانه در فضای محدود یک سازمان از طریق کابل شبکه و پروتکل بین رایانه ها و با مدیریت نرم افزاری موسوم به سیستم عامل شبکه را شبکه محلی گویند. کامپیوتر سرویس گیرنده باید از طریق کامپیوتر سرویس دهنده به اطلاعات و امکانات به اشتراک گذاشته دسترسی یابند. همچنین ارسال و دریافت پیام به یکدیگر از طریق رایانه سرویس دهنده انجام می گیرد. از خصوصیات شبکه های محلی می توان به موارد ذیل اشاره کرد:

۱ - اساسا در محیط های کوچک کاری قابل اجرا و پیاده سازی می باشند.

۲ - از سرعت نسبتا بالایی برخوردارند.

۳ - دارای یک ارتباط دائمی بین رایانه ها از طریق کابل شبکه می باشند.

اجزای یک شبکه محلی عبارتند از :

الف - سرویس دهنده

ب - سرویس گیرنده

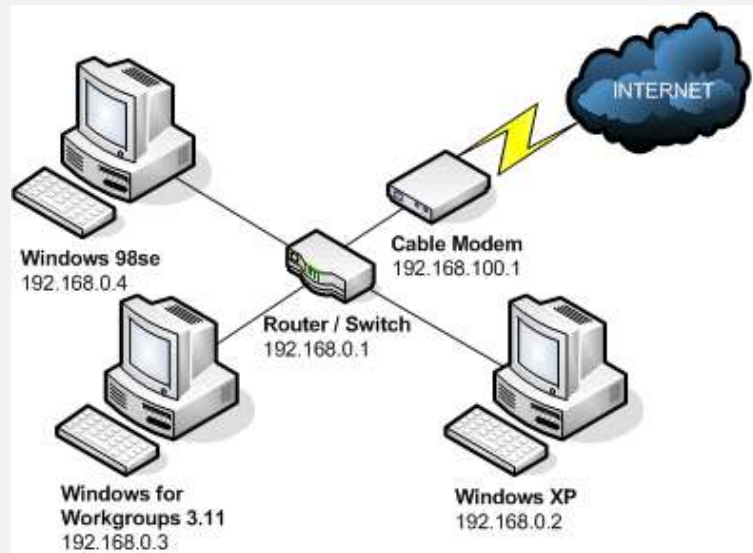
ج - پروتکل

د- کارت واسطه شبکه

ط - سیستم ارتباط دهنده

شکل زیر یک شبکه محلی میباشد.

¹Local Area Network



شبکه گسترده¹ WAN:

WAN برگرفته از (wide-area network) ، يك شبکه ارتباطی است که يك حوزه جغرافیائی گسترده نظیر يك شهرستان ، استان و یا کشور را تحت پوشش قرار می دهد. این نوع شبکه ها دارای مشخصات منحصر بفرد مختص به خود می باشند که آنان را از يك شبکه محلی متمایز می نماید.

کاربردها

شبکه های گسترده برای اتصال شبکه های محلی یا دیگر انواع شبکه به یکدیگر استفاده می شوند. بنابراین کاربران و رایانه های یک مکان می توانند با کاربران و رایانه هایی در مکانهای دیگر در ارتباط باشند. بسیاری از شبکه های گسترده برای یک سازمان ویژه پیاده سازی می شوند و خصوصی

¹Wide Area Network

هستند. بعضی دیگر به وسیله « سرویس دهندگان اینترنت » (ISP) پیاده سازی می شوند تا شبکه های محلی سازمانها را به اینترنت متصل کنند.

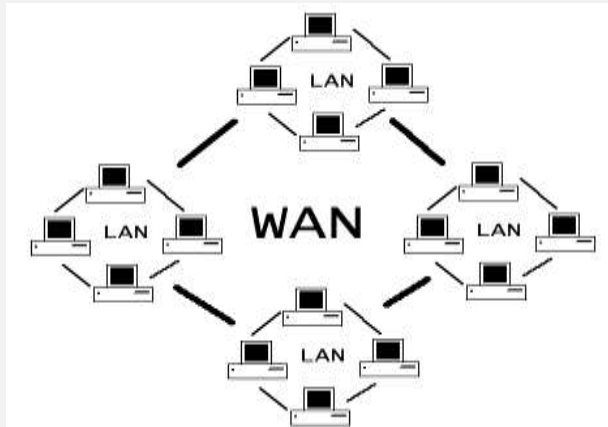
انواع:

اغلب جهت پیاده سازی شبکه های گسترده از « خطوط استیجاری » استفاده می شود. در هر انتهای خط اجاره ای یک دستگاه « مسیریاب » قرار داده می شود که از یک طرف به شبکه محلی آن سمت و از طرف دیگر به وسیله یک هاب به آن سوی شبکه گسترده متصل است. خطوط استیجاری می تواند بسیار گران باشند. همچنین شبکه های گسترده می توانند بجای استفاده از آنها با استفاده از روشهای به صرفه تر « راهگزینی مداری » و « راهگزینی بسته » پیاده سازی شوند. « قرارداد » های شبکه مانند قرارداد مجموعه پروتکل اینترنت وظایف انتقال و آدرس دهی را برعهده دارند. قراردادهایی مانند « انتقال بسته بر سونت / اس دی اچ » (Packet over SONET/SDH)، « حالت انتقال ناهمگام »^۱، « راهگزینی برچسب چند قرارداری » (MPLS)، « رله فریم » (Frame Relay) اغلب به وسیله سرویس دهنده ها استفاده می شوند تا لینک هایی که در شبکه های گسترده استفاده می شوند را تامین کنند. قرارداد X ۲۵ یکی از قراردادهای اولیه مهم شبکه های گسترده بوده است و اغلب از آن به عنوان پدر بزرگ قرارداد « رله فریم » یاد می شود، چراکه امروزه هنوز بسیاری از اصول و وظایف بنیادی پروتکل X ۲۵ با اعمال تغییراتی که جهت بروز در آوردن آن صورت گرفته در قرارداد « رله فریم » بکار می رود.

حق دارید که درک این قسمت قدری سخت باشد در فصلهای بعدی در این باره مفصل تر توضیح خواهیم داد (تکرار میکنم هدف این فصل تنها دادن یک دید کلی میباشد).

در شکل زیر یک شبکه wan را ملاحظه میکنید که اینترنت را میتواند چند هزار بزرگ تر از این تجسم کنید.

^۱ ATM



شبکه باند پایه^۱:

شبکه باند پایه شبکه ای است که در آن کابل (رسانه شبکه) هر بار تنها یک سیگنال را می تواند منتقل کند. شبکه های باند پایه در فواصل نسبتا کوتاهی گسترده می شوند زیرا به دلیل تداخل الکتریکی و عوامل دیگر در معرض تضعیف هستند. با افزایش نرخ انتقال ، حداکثر طول کابل (رسانه شبکه) کاهش می یابد.

باند پهن^۲:

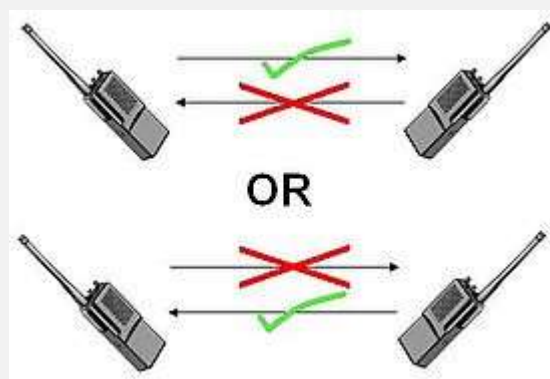
شبکه باند پهن شبکه ای است که چند سیگنال را می تواند بطور همزمان منتقل کند ، و بدین ترتیب هر سیگنال از یک قسمت مجزای عرض باند کابل استفاده می کند. مثالی از شبکه باند پهن سرویس تلویزیون کابلی است که در آن واحد چندین کانال برنامه را تنها از طریق یک کابل در اختیار کاربر قرار می دهد.

^۱Base Band

^۲Broad and

فول دوبلکس و هالف دوبلکس

در هالف دوبلکس در یک واحد زمانی فقط می توانی یا ارسال یا دریافت نمایی (مته واکی تاکی یا همان بی سیم پلیس ها) اما در فول دوبلکس میتوانی هم دریافت و هم ارسال را در یک واحد زمانی داشته باشیم مانند تمام شبکه های lan ,wan wirless و مثل تلفن دوطرفه.



تصویری ساده از سامانه ارتباطی نیمه دوطرفه



تصویری ساده از یک سامانه ارتباطی کاملاً دوطرفه.

سامانه های ارتباطی کاملاً دوطرفه به دلیل هزینه و پیچیدگی در رادیوهای دستی رایج نیستند.

Backbone Network

یک شبکه ستون فقراتی بخشی از زیر ساخت یک شبکه رایانه ای است که قطعه های مختلف شبکه را به هم وصل می کند و مسیری برای مبادله اطلاعات بین شبکه های محلی و زیرشبکه های مختلف را ارائه می کند. یک ستون فقرات شبکه های گوناگونی را که در یک ساختمان یا در ساختمانهای مختلف، در کل محوطه و یا در ناحیه گسترده جغرافیایی قرار دارند به یکدیگر گره می زند. معمولاً ظرفیت ستون فقرات از شبکه هایی که به آن متصل اند بیشتر است.

مدل های شبکه

در یک شبکه ، یک کامپیوتر می تواند هم سرویس دهنده وهم سرویس گیرنده باشد. یک سرویس دهنده (Server) کامپیوتری است که فایل های اشتراکی وهمچنین سیستم عامل شبکه که مدیریت عملیات شبکه را بعهده دارد - را نگهداری می کند.

برای آنکه سرویس گیرنده " Client " بتواند به سرویس دهنده دسترسی پیدا کند ، ابتدا سرویس گیرنده باید اطلاعات مورد نیازش را از سرویس دهنده تقاضا کند. سپس سرویس دهنده اطلاعات در خواست شده را به سرویس گیرنده ارسال خواهد کرد.

سه مدل از شبکه هایی که مورد استفاده قرار می گیرند ، عبارتند از :

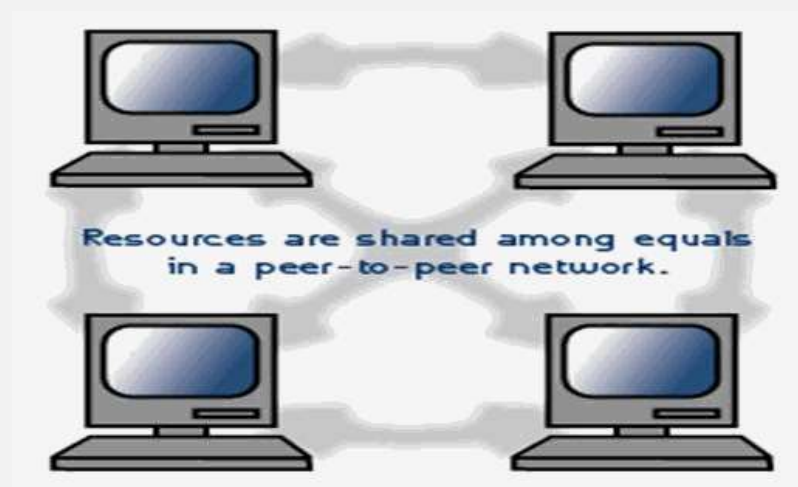
۱ - شبکه نظیر به نظیر " Peer- to- Peer "

۲ - شبکه مبتنی بر سرویس دهنده " Server- Based "

۳ - شبکه سرویس دهنده / سرویس گیرنده " Client Server "

۱- شبکه نظیر به نظیر^۱

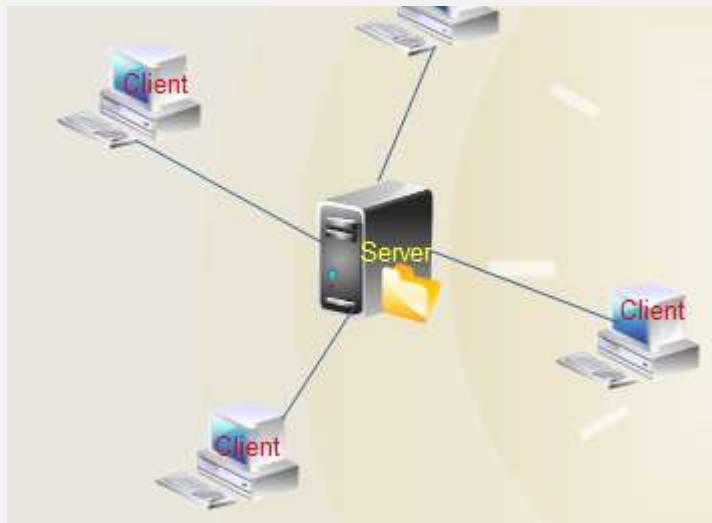
در این شبکه ایستگاه ویژه ای جهت نگهداری فایل های اشتراکی و سیستم عامل شبکه وجود ندارد. هر ایستگاه می تواند به منابع سایر ایستگاه ها در شبکه دسترسی پیدا کند. هر ایستگاه خاص می تواند هم بعنوان Server و هم بعنوان Client عمل کند. در این مدل هر کاربر خود مسئولیت مدیریت و ارتقاء دادن نرم افزارهای ایستگاه خود را بعهده دارد. از آنجایی که یک ایستگاه مرکزی برای مدیریت عملیات شبکه وجود ندارد ، این مدل برای شبکه ای با کمتر از ۱۰ ایستگاه بکار می رود .



^۱Peer- to- Peer

۲- شبکه مبتنی بر سرویس دهنده^۱

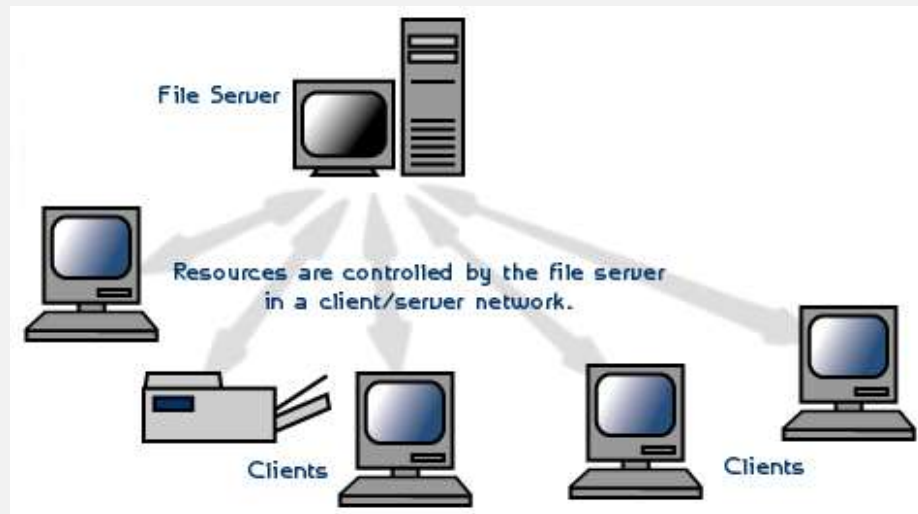
در این مدل شبکه ، یک کامپیوتر بعنوان سرویس دهنده کلیه فایل ها و نرم افزارهای اشتراکی نظیر واژه پردازها، کامپایلرها ، بانک های اطلاعاتی و سیستم عامل شبکه را در خود نگهداری می کند. یک کاربر می تواند به سرویس دهنده دسترسی پیدا کرده و فایل های اشتراکی را از روی آن به ایستگاه خود منتقل کند.



^۱Server- Based

۳ - شبکه سرویس دهنده / سرویس گیرنده^۱

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



^۱Client Server

هر شبکه اساسا از سه بخش ذیل تشکیل می شود:

۱-ابزارهایی که به پیکربندی اصلی شبکه متصل می شوند به عنوان مثال : کامپیوترها ، چاپگرها، هاب ها^۱ ”

۲-سیم ها ، کابل ها وسایر رسانه هایی که برای اتصال ابزارهای شبکه استفاده می شوند.

۳-سازگار کننده ها^۲ یا کارت شبکه.

که بعنوان اتصال کابل ها به کامپیوتر هستند . اهمیت آنها در این است که بدون وجود آن ها شبکه تنها شامل چند کامپیوتر بدون ارتباط موازی است که قادر به سهیم شدن منابع یکدیگر نیستند . عملکرد سازگارکننده در این است که به دریافت و ترجمه سیگنال های درون داد از شبکه از جانب یک ایستگاه کاری و ترجمه و ارسال برون داد به کل شبکه می پردازد.

MAC Address چیست ؟

هر کامپیوتر موجود در شبکه به منظور ایجاد ارتباط با سایر کامپیوترها ، می بایست شناسایی و دارای یک آدرس منحصر بفرد باشد . قطعا^۳ تاکنون با آدرس های IP و یا MAC^۳ برخورد داشته اید و شاید این سوال برای شما مطرح شده باشد که اولاً " ضرورت وجود دو نوع آدرس چیست و ثانياً " جایگاه اسفاده از آنان چیست ؟

MAC Address ، یک آدرس فیزیکی است در حالی که آدرس های IP ، به منزله آدرس های منطقی می باشند. آدرس های منطقی شما را ملزم می نمایند که به منظور پیکربندی کامپیوتر و کارت شبکه ، درایورها و یا پروتکل های خاصی را در حافظه مستقر نمائید (مثلا^۳ استفاده از

^۱Hubs

^۲Adaptor

^۳Media Access Control

آدرس های IP) . این وضعیت در رابطه با MAC Address صدق نخواهد کرد و اینگونه آدرس ها نیازمند درایور های خاصی نخواهند بود ، چراکه آدرس های فوق درون تراشه کارت شبکه قرار می گیرند .

دلیل استفاده از MAC Address

هر کامپیوتر موجود در شبکه ، می بایست با استفاده از روش هایی خاص شناسائی گردد . برای شناسائی یک کامپیوتر موجود در شبکه ، صرف داشتن یک آدرس IP به تنهایی کفایت نخواهد کرد.

مدل OSI		
...		
آدرس IP در این لایه قرار دارد	لایه سوم	Network Layer
آدرس MAC در این لایه قرار دارد	لایه دوم	DataLink Layer
	لایه اول	Physical Layer
شبکه فیزیکی		

همانگونه که مشاهده می نمائید ، MAC Address در لایه DataLink (لایه دوم مدل OSI) قرار دارد و این لایه مسئول بررسی این موضوع خواهد بود که داده متعلق به کدامیک از کامپیوترهای موجود در شبکه است . زمانی که یک بسته اطلاعاتی (Packet) به لایه Datalink می رسد (از طریق لایه اول) ، وی آن را در اختیار لایه بالائی خود (لایه سوم) قرار خواهد داد .

بنابراین ما نیازمند استفاده از روش خاصی به منظور شناسائی یک کامپیوتر قبل از لایه سوم هستیم . MAC Address ، در پاسخ به نیاز فوق در نظر گرفته شده و با استقرار در لایه دوم ، وظیفه شناسائی کامپیوتر قبل از لایه سوم را بر عهده دارد. تمامی ماشین های موجود بر روی یک شبکه ، اقدام به بررسی بسته های اطلاعاتی نموده تا مشخص گردد که آیا MAC Address موجود در بخش "آدرس مقصد" بسته اطلاعاتی ارسالی با آدرس آنان مطابقت می نماید؟ لایه فیزیکی (لایه اول) قادر به شناخت سیگنال های الکتریکی موجود بر روی شبکه بوده و فریم هایی را تولید می نماید که در اختیار لایه Datalink ، گذاشته می شود . در صورت مطابقت MAC Address موجود در بخش "آدرس مقصد" بسته اطلاعاتی ارسالی با MAC Address یکی از کامپیوترهای موجود در شبکه ، کامپیوتر مورد نظر آن را دریافت و با ارسال آن به لایه سوم ، آدرس شبکه ای بسته اطلاعاتی (IP) بررسی تا این اطمینان حاصل گردد که آدرس فوق با آدرس شبکه ای که کامپیوتر مورد نظر با آن پیکربندی شده است بدرستی مطابقت می نماید .

ساختار MAC Address:

یک MAC Address بر روی هر کارت شبکه همواره دارای طولی مشابه و یکسان می باشند . (شش بایت و یا ۴۸ بیت) . در صورت بررسی MAC Address یک کامپیوتر که بر روی آن کارت شبکه نصب شده است ، آن را با فرمت مبنای شانزده (Hex) ، مشاهده خواهید دید . مثلاً " MAC Address کارت شبکه موجود بر روی یک کامپیوتر می تواند به صورت زیر باشد :

مشاهده MAC Address					
استفاده از دستور IPconfig/all و مشاهده بخش Physical address :					
۰۰	۵۰	BA	۷۹	DB	۶A
تعریف شده توسط IEEE			تعریف شده توسط تولید کننده		
با توجه به RFC ۱۷۰۰					

زمانی که یک تولید کننده نظیر اینتل ، کارت های شبکه خود را تولید می نماید ، آنان هر آدرس دلخواهی را نمی توانند برای MAC Address در نظر بگیرند . در صورتی که تمامی تولید کنندگان کارت های شبکه بخواهند بدون وجود یک ضابطه خاص ، اقدام به تعریف آدرس های فوق نمایند ، قطعاً امکان تعارض بین آدرس های فوق بوجود خواهد آمد . (عدم تشخیص تولید کننده کارت و وجود دو کارت شبکه از دو تولید کننده متفاوت با آدرس های یکسان) . حتماً این سوال برای شما مطرح می گردد که MAC Address توسط چه افراد و یا سازمان هائی و به چه صورت به کارت های شبکه نسبت داده می شود ؟ به منظور برخورد با مشکلات فوق ، گروه IEEE ، هر MAC Address را به دو بخش مساوی تقسیم که از اولین بخش آن به منظور شناسائی تولید کننده کارت و دومین بخش به تولید کنندگان اختصاص داده شده تا آنان یکشماره سریال را در آن درج نمایند . کد تولید کنندگان بر اساس RFC-۱۷۰۰ به آنان نسبت داده می شود . در صورت مشاهده RFC فوق حتماً متوجه خواهید شد که برخی از تولید کنندگان دارای بیش از یک کد می باشند . علت این امر به حجم گسترده محصولات تولیدی آنان بر می گردد .

با این که MAC Address در حافظه کارت شبکه ثبت می گردد ، برخی از تولید کنندگان به شما این اجازه را خواهند داد که با دریافت و استفاده از یک برنامه خاص ، بتوانید بخش دوم MAC Address کارت شبکه خود را تغییر دهید (شماره سریال کارت شبکه) . علت این موضوع به استفاده مجدد از سریال های استفاده شده در سایر محصولات تولید شده توسط آنان برمی گردد (تجاوز از محدود مورد نظر) .

در حال حاضر احتمال این که شما دو کارت شبکه را خریداری نمایید که دارای MAC Address یکسانی باشند، بسیار ضعیف و شاید هم غیرممکن باشد.

مختصری در مورد کانالهای انتقال:

وظیفه سخت افزار مخابراتی در لایه ی واسط شبکه آنست که بدون توجه به نوع و محتوای داده ها، بیت های داده را بر روی کانال فیزیکی منتقل کند. سخت افزارانتقال در این لایه ، بیشتر با مسائل مخابراتی و الکتریکی سروکار دارد.

سه جز اصلی این سخت افزار ، عبارتند از:

گیرنده

فرستنده

کانال فیزیکی

مباحث مربوط به گیرنده/فرستنده در محدوده ی این کتاب نیست ، تنها به معرفی کانال های ارتباطی که برای اتصال بین ماشین ها استفاده میشود ، اکتفا می کنیم. این کانال ها عبارتند از:

خطوط تلفن:

سیم های به هم بافته شده زوجی (در UTP که یک زوج سیم معمولی به هم بافته شده است و

انواع STP که یک زوج سیم معمولی به هم بافته شده به همراه یک پوشش آلومینیمی بر روی

آنها جهت کاهش اثر نویزهای محیطی بر روی سیم میباشد).

کابل های هم محور (کواکسیال) (در انواع مختلف مثل کابل کواکس ۵۰ اهم ضخیم کابل کواکس ۵۰ اهم نازک و کابل کواکس ۷۵ اهم معمولی)

فیبرهای نوری (در انواع مختلف مثل فیبر تک موده و چند موده)

کانال های ماهواره‌ای : در باندهای فرکانسی مختلف مثل :

باند C ارسال از زمین به ماهواره در باند : ۶/۴۲۵~۵/۹۲۵GHz

دریافت از ماهواره در باند ۴/۲~۳/۷GHz

باند Ku ارسال از زمین به ماهواره در باند : ۱۴/۵~۱۴/۰GHz

دریافت از ماهواره در باند ۱۲/۲~۱۱/۷GHz

باند Ka ارسال از زمین به ماهواره در باند : ۳۰/۵~۲۷/۵GHz

دریافت از ماهواره در باند ۲۱/۷~۱۷/۷GHz

کانال های رادیویی (شامل باندهای فرکانسی مختلف مثل UHF, VHF)

امواج طیف نوری شامل نور مادون قرمز (با استفاده از این امواج که خاصیت نور دارند می توان داده ها را به فاصله ی چند متر عبور داد. این امواج فقط از محیط های شفاف عبور میکنند و بیشتر برای انتقال اطلاعات در فواصل بسیار کوتاه کاربرد دارد. مثلاً در کامپیوترهای کیفی برای ارتباط بیسیم با یک کامپیوتر دیگر مناسب است. تمام کانال ها دارای مشخص های به نام پهنای باند هستند.

در یک عبارت ساده و غیر دقیق ، پهنای باند هر کانال را می توان ، توانایی و ظرفیت آن در ارسال اطلاعات با نرخ بیت در هر ثانیه ، تعریف کرد.

بنابراین وقتی گفته می شود پهنای باند یک کانال یک مگابیت بر ثانیه است یعنی با سرعت بالاتر از یک مگابیت بر ثانیه نمی توان اطلاعات را سالم به مقصد رساند.

در این خصوص رابطه معروفی بنام رابطه شانون وجود دارد:

$$C=B.\log_2(1+S/N)$$

C : ظرفیت کانال بر حسب بیت بر ثانیه

S : متوسط توان سیگنال

N : متوسط توان نویز

B : پهنای باند کانال بر حسب هرتز

به عنوان مثال اگر پهنای باند کانالهای تلفن معمولی را حداکثر توان 4KHz فرض کنیم و نسبت سیگنال به توان نویز بطور تقریبی 1000 باشد ، در چنین حالتی با استفاده از خط تلفن حداکثر 39000 بیت در ثانیه را میتوان انتقال داد و انتقال اطلاعات در بالاتر از این نرخ منجر به خرابی دادهها خواهد شد. انتقال یک فایل یک مگابایتی از طریق خط تلفن با این سرعت مشخصات برخی از کانالهای انتقال با - حدوداً 210 ثانیه طول خواهد کشید. در جدول یکدیگر مقایسه شده است. معیار خطا در کانالهای انتقال ، احتمال بروز یک بیت خطا روی کانال تعریف میشود؛ یعنی

احتمال آنکه در فرستنده بیت 1 ارسال و در گیرنده اشتباهاً بیت 0 آشکارسازی بشود.

توضیح	قیمت	بیاده سازی	خطا	پهنای باند	
از قبل وجود دارد	ارزان	ساده	زیاد	کم (حدود 4KHz)	خطوط تلفن معمولی
برای فواصل کوتاه مناسب است.	ارزان	ساده	متوسط	متوسط (حدود چند ده تا صد مگاهرتز)	زوج سیم
	متوسط	متوسط	کم	حدود چند صد مگاهرتز	کابلهای کواکس
بهترین کارایی	متوسط	پیچیده	بسیار کم	حدود چند گیگا هرتز	فیبرهای نوری
در همه جا تحت پوشش	گران	بسیار پیچیده	متوسط	حدود چند صد مگاهرتز	کانالهای ماهواره
در جایی که کابل کشی عملی نیست مناسب می باشد.	نسبتاً گران	نسبتاً پیچیده	زیاد	حدود چند مگاهرتز	کانالهای رادیویی

مقایسه مشخصات برخی از کانالهای انتقال

با توجه به آنکه پهنای باند بعضی از کانال ها بسیار زیاد است (مثل کانال های ماهواره ای) می توان یک کانال فیزیکی را بین چندین ایستگاه تقسیم کرد. این تقسیم باعث می شود که از یک کانال مشترک چندین ایستگاه استفاده کنند و هزینه های ارتباط کاهش یابد. به عمل تقسیم پهنای باند یک کانال بین چند ایستگاه عمل مالٹیپلکس یا تسهیم گفته میشود. تسهیم به دو روش قابل انجام است:

تسهیم در میدان زمان یا TDM و تسهیم در میدان فرکانس یا FDM

در FDM با فرض آنکه حداکثر N ایستگاه در شبکه وجود داشته باشد؛ پهنای باند فرکانسی روش کانال به N باند مجزا تقسیم می شود. هر ایستگاه موظف است در یکی از این باندهای فرکانسی ارسال و دریافت داشته باشد و چون این باند فرکانسی به صورت ثابت ، متعلق به خودش خواهد بود ، هرگونه تصادم و تداخل سیگنال منتفی است.

در TDM زمان به بازه های کوچکی تقسیم شده و هر ایستگاه مجاز است فقط در بازه زمانی روش متعلق به خودش ، اطلاعات را روی کانال بفرستد.

این دو زمانی کارآمد و مفید خواهند بود که : اولاً تعداد ایستگاه ها ثابت و محدود می باشد.

ثانیاً هر ایستگاه حجم ثابت و در عین حال دائمی ارسال داده بر روی کانال داشته باشد. در شبکه های کامپیوتری ایستگاه ها از نظر تعداد ، نامشخص و زیادند و ارسال داده ها نیز "انفجاری" است. انفجاری بودن ترافیک بدین معناست که ایستگاه در لحظاتی ، به صورت ناگهانی حجم انبوهی از فریم ها را برای ارسال روی کانال تولید می کند و سپس متوقف شده و تا لحظات متمادی هیچ داده ای برای ارسال تولید نمی کند. در شبکه ها تقاضای ارسال روی کانال پدیده ایست تصادفی و هیچ قاعده ی از پیش تعیین شده ای ندارد. آمارها نشان می دهد که انفجاری بودن ترافیک روی شبکه ، نسبت $1/1000$ دارد؛ یعنی :

Peak Traffic 1000

Mean Traffic 1

با این توصیف برای تسهیم کانال های مشترک باید به سمت روشهای پویا حرکت کرد. در این خصوص پروتکل های متفاوتی عرضه شده که در این فصل شناخته شده ترین آن ها را که استانداردهای IEEE 802.x هستند ، معرفی خواهیم کرد.

مختصری در مورد خطا در شبکه های کامپیوتری

خطا در خطوط انتقال جزو حقایقی است که به هیچ وجه نمی توان بطور کامل آن را برطرف کرد و همیشه جزو مشکلات عمده سیستم های مخابراتی بوده است. ماهیت خطا و علل به وجود آمدن آن را میتوان در موارد زیر خلاصه کرد:

۱- نویز حرارتی : این نویز به دلیل حرکت اتفاقی الکترون ها بوجود می آید و با افزایش دما ، شدت این نویز هم به صورت خطی تقویت میشود. بخصوص در مدارهایی مثل تقویت کننده های نیمه هادی با ضریب تقویت و بهره ی بالا ، تاثیر این نویز حساسیت بیشتری دارد. اثر این خطا کاملا تصادفی است.

۲- شوک های الکتریکی : این نوع از نویز بدلیل قطع و وصل کلیدها ، سیم ها و سوئیچ های الکتریکی یا رعد و برق بوجود آمده و نوعی خطای انفجاری را باعث می شود؛ یعنی مجموعه ی گسترده ای از بیت ها که روی کانال در جریانند ، به یکباره خراب می شوند. به عنوان مثال اگر یک شوک الکتریکی به اندازه ۱۰ms ادامه یابد و اطلاعات روی کانال با سرعت ۱ Mbps در جریان باشد ، با فرض آنکه طول متوسط فریم ها ۱ KB در نظر گرفته شود ، این شوک می تواند تا ده فریم را بطور کلی نابود کند؛ به این معنا که فرستنده ده فریم را فرستاده ولی گیرنده هیچ فریمی دریافت نکرده است.

۳- نویز کیهانی: این نوع خطاها ناشی از حرکات کیهانی ، کهکشان ها ، وضعیت ستارگان و خورشید و امثال آن می باشد و تاثیر آن بیشتر بر روی کانال های رادیویی است. ساده ترین روش کشف خطا ، اضافه کردن بیت توازن به داده هاست. در این روش به ازای هر بیت از اطلاعات یک بیت توازن اضافه می شود؛ این بیت باید به گونه ای انتخاب و اضافه شود که مجموع تعداد بیت های ۱ ، همیشه زوج یا فرد باشد.

مثال:

بایت اصلی : ۰۱۱۰۱۰۰۱

۱ Odd Parity

بیت توان فرد: ۰۱۱۰۱۰۰۱

Even Parity ۰

بیت توان زوج: ۰۱۱۰۱۰۰۱

بنابراین گیرنده می تواند با بررسی بیت توازن ، خطای احتمالی را کشف کند ، ولی این روش در

صورتی موثر است که تعداد خطاهای رخ داده زوج نباشد.

روش Checksum:

در این روش تمامی بایتهای یک فریم که باید توسط فرستنده ارسال شود بصورت بیت بیت با هم جمع یا (XOR) شده و یک بایت به نام Checksum بدست می آید. این بایت در انتهای فریم به مقصد ارسال می شود. در مقصد مجدداً بایت Checksum محاسبه و سپس مقایسه می شود. این روش در صورتی قادر به کشف خطا است که تعداد خطاهای رخ داده در بیت ها هم ارزش زوج نباشد.

روش های کنترل خطا:

در روش CRC، به ازای مجموعه ای از بیت ها (مثلاً ۵۱۲ بیت یا ۱۰۲۴ بیت ...) تعدادی بیت کنترلی به نام CRC محاسبه و به انتهای فریم اضافه می شوند. روش محاسبه کدهای CRC با استفاده از تقسیم های چند جمله ای است که روش آن در زیر آمده است:

داده اصلی : 11100101

7	6	5	4	3	2	1	0
1	1	1	0	0	1	0	1

اولین مرحله برای نمایش ریاضی چگونگی محاسبه CRC ابتدا بیت ها از راست به چپ ضرایب یک چند جمله که توان هر جمله را موقعیت بیت مشخص می کند قرار می گیرد بنابراین Data به صورت یک چند جمله ای نمایش داده خواهد شد. برای مولد کد CRC چند جمله ای هایی وجود دارد که تقریباً در سراسر دنیا استانداردند. چند جمله ای Data پس از ضرب در n (بالاترین توان چند جمله ای مولد است) در مبنای ۲ تقسیم بر چند جمله ای CRC شده و باقیمانده آن به عنوان کدهای کنترل خطا بدست می آید.

$$\text{CRC مولد} = X^2 + 1 \rightarrow 101$$

$$\text{Data} = x^7 + x^6 + x^5 + x^2 + 1 \xrightarrow{\cdot x^2} X^9 + X^8 + X^7 + X^4 + X^2$$

$$X^9 + X^8 + X^7 + X^4 + X^2 \overline{)X^2 + 1}$$

$$\text{باقیمانده} : +1 = 01$$

در روشی که خواهیم به صورت باینری (به جای چند جمله ای) کد CRC را حساب کنیم به تعداد بزرگ ترین جمله مولد در سمت راست Data صفر اضافه می کنیم پس در مثال بالا باید دو صفر به سمت راست Data اضافه شود. پس Data ای که به آن اضافه شده است را بر چند جمله ای مولد تقسیم کنیم. در تقسیم به نکات زیر باید توجه داشته باشیم.

- تقسیم از این لحاظ با تقسیم معمولی متفاوت است که شما باید از سمت چپ بیت های باقیمانده را صفر کنیم.

- جمع در مبنای ۲ و به صورت XOR انجام می شود.

- نهایتاً بیت های باقیمانده تقسیم در سمت راست بیت های Data قرار می گیرد.

درس ۲: مدل مرجع OSI

مدل مرجع OSI نشان دهنده این است که روند شبکه را به هفت لایه تقسیم میکند. این ساختار که از مفهوم پشته استفاده کرده است درک مفهوم شبکه را آسان تر کرده. در این مدل ، نرم افزار که نیاز به دسترسی به یک منبع بر روی شبکه دارد، و در پایین، وابسته به شبکه خود است از این مدل استفاده می کند. مطابق این مدل اطلاعات از طریق لایه های پایین حرکت می کند، که در مسیر خود به پروتکل های مختلف که وجود دارد بر خورده و آماده سازی و بسته بندی آن برای انتقال بر روی شبکه را بر عهده می گیرند. هنگامی که داده ها به مقصد خود می رسند، از طریق لایه ها بر روی سیستم دریافت کننده دریافت میشود، که در این فرایند (فرستادن و دریافت) عمل معکوس هم صورت میگیرند.

لایه فیزیکی^۱:

در مدل OSI این لایه اولین و پایین ترین لایه می باشد. این لایه برای انتقال یکسری از بیت های نامنظم از یک کامپیوتر به کامپیوتر دیگر تعریف شده است. در این لایه مشخص می شود که هر بیت اطلاعات تا چه مسافتی در محیط شبکه می تواند منتقل شود. رمزگذاری و همزمان سازی اطلاعات از وظایف این لایه است. در حقیقت لایه فیزیکی از تباط الکترونیکی و یا نوری با کابل شبکه دارد. به این لایه ، لایه Hardware نیز گفته می شود.

لایه پیوند داده^۲:

در این لایه اطلاعات از لایه شبکه گرفته شده و به لایه فیزیکی تحویل داده می شود. کامپیوتر گیرنده این اطلاعات را از لایه فیزیکی دریافت کرده و به صورت فریم داده (Data Frame) تبدیل می کند. (فریم داده یک ساختار منظم از داده می باشد که بسته های اطلاعاتی توسط این فریم به

^۱Physical
^۲Data Link

کامپیوتر گیرنده فرستاده می شود). آدرس فیزیکی شبکه یا همان Mac Address در این لایه قرار دارد. همچنین دستگاه های Bridge (پل) در این لایه فعالیت می کنند.

لایه شبکه^۱:

این لایه مسئول مشخص کردن مسیر مبدا و مقصد اطلاعات می باشد. تبدیل منطقی آدرس ها برای قابل فهم بودن برای لایه فیزیکی در این لایه انجام می شود. همچنین کنترل ترافیک شبکه در این لایه صورت می گیرد. یکی از دستگاه های بسیار مهم در شبکه های کامپیوتر به نام روتر (Router) در این لایه فعالیت می کند ، چرا که در این لایه بسته های اطلاعاتی (Packets) با پروتکل IP برای مسیر سر و کار دارند و روتر با IP کار می کند.

لایه انتقال^۲:

کنترل جریان داده ها و پاسخگویی به خطاهای بوجود آمده در محیط شبکه توسط این لایه مدیریت و پاسخ داده می شود. در این لایه صحت اطلاعات نیز چک می شود. از وظایف بسیار مهم این لایه این است که در صورت سالم دریافت کردن اطلاعات یک پیام Acknowledge برای کامپیوتر فرستنده ارسال می شود. هر گونه تغییری که در این لایه بر روی اطلاعات جهت

ارسال داده شود در مقصد در همین لایه به حالت عادی برگردانده می شود.

لایه نشست^۳:

این لایه می تواند به دو نرم افزار بر روی دو کامپیوتر مختلف امکان برقراری ارتباط را بدهد. در این لایه سیاست های امنیتی برای حفاظت از نرم افزارهای موجود در شبکه تعریف می شود. در خواست های کاربران توسط کانالهای ارتباطی در این لایه نگهداری می شود و در صورتی که

^۱Network

^۲Transport

^۳Session

یکی از کانال های ارتباطی به صورت کامل به مقصد نرسیده باشد مجددا همان کانال برای کاربر ارسال می گردد.

لایه نمایش^۱:

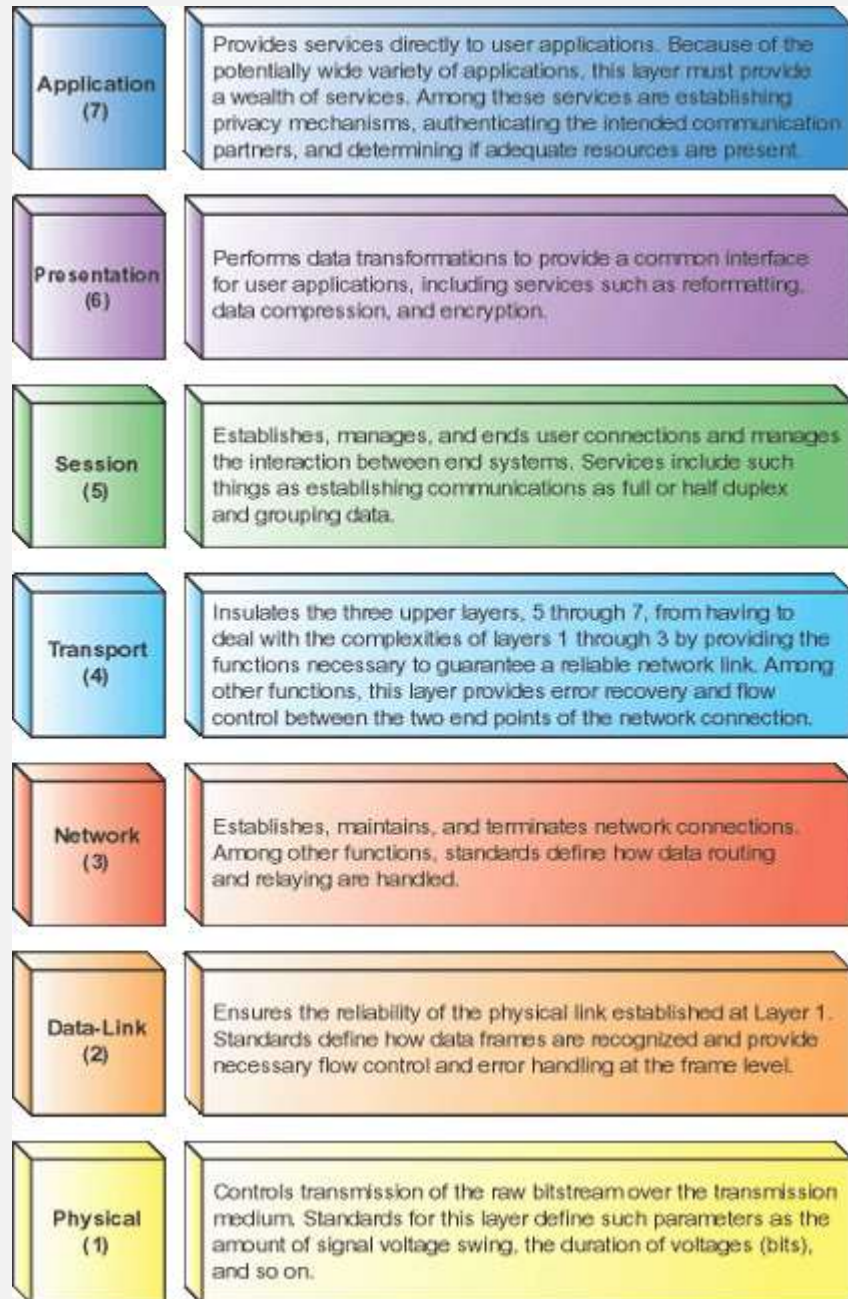
این لایه وظیفه تبدیل پروتکل ها ، فشرده سازی اطلاعات برای کاهش حجم اطلاعات و مشخص کردن قالب تبادل اطلاعات بین دو کامپیوتر می باشد. به اصطلاح به این لایه ، لایه مترجم شبکه نیز گفته می شود و همچنین قسمتی از رمزگذاری اطلاعات در این لایه صورت می گیرد.

لایه کاربرد^۲:

این لایه مربوط به سرویس هایی می شود که مستقیما با برنامه های کاربر در ارتباط هستند. در واقع این لایه ، بالاترین لایه در مدل OSI می باشد که وظیفه مدیریت و کنترل نرم افزارها را برعهده دارد. بطور کلی این لایه مسئول کنترل سرویس هایی که مستقیما با نرم افزارهای کاربردی کار می کنند را دارد. در واقع این لایه مسئولیت پوشش دادن به خطاهای نرم افزاری برای برنامه های کاربردی می باشد. در این لایه می توانیم به قسمت های نرم افزاری امکان استفاده از سرویس های شبکه را بدهیم. همچنین کنترل دسترسی عمومی به شبکه از وظایف این لایه می باشد.

^۱Presentation

^۲Application



که در ادامه به توضیح هر لایه و پروتکل های آن می پردازیم.

لایه فیزیکی

لایه فیزیکی پایین ترین لایه در مدل مرجع ارتباط سامانه های باز (OSI) می باشد. این لایه وظیفه انتقال بیت ها از طریق کانال مخابراتی را عهده دار می شود. مسائل طراحی در این لایه عمدتاً از نوع فیزیکی، الکتریکی، تایمینگ، رسانه فیزیکی انتقال است. در این لایه باید نقش عوامل طبیعی را نیز در نظر داشته باشیم. در این بخش بیشتر درباره نحوه انتقال فیزیکی اطلاعات بحث می گردد. این رسانه ها را می توان در دو دسته تقسیم بندی نمود:

- رسانه های هدایت پذیر همچون سیم مسی و فیبر نوری.
- رسانه های هدایت ناپذیر همچون بیسیم، امواج رادیوی زمینی و ماهواره.

رسانه های فیزیکی مختلف با توجه پارامترهای پهنای باند، تأخیر انتشار، سهولت نصب و نگهداری مقایسه می گردند.

لایه پیوند داده:

لایه پیوند داده دومین سطح از مدل مرجع OSI می باشد. در این لایه بر روی الگوریتم های دستیابی به ارتباطات قابل اعتماد بین دو کامپیوتر همسایه بحث می شود. این لایه دارای وظایفی به قرار زیر است:

- ارائه سرویس های مشخص به لایه شبکه
- مدیریت خطاهای انتقال
- تنظیم جریان داده ها

برای تحقق این اهداف این لایه اقدام به فریم بندی اطلاعات می نماید.

ارائه سرویس های مشخص به لایه شبکه

از مهم ترین وظایف لایه پیوند داده انتقال داده ها از لایه شبکه ی ماشین مبدا به لایه شبکه ماشین مقصد می باشد. این ارتباط (بخش الف) در شکل مقابل نشان داده شده است. البته این اتصال ارتباطی همچون بخش (ب) که ارتباطی واقعی است، را دنبال می نماید. سرویس هایی که لایه پیوند داده ارائه می کند، از سیستمی تا سیستم دیگر متفاوت است. اما از مهم ترین سرویس ها عبارت اند از:

- سرویس غیر متصل بدون تصدیق دریافت: این سرویس در اکثر LAN ها مورد استفاده قرار می گیرد.
 - سرویس غیر متصل با تصدیق دریافت: این سرویس برای کانال های غیر اعتمادی مثل سیستم های بسیم مناسب است.
- سرویس اتصال گرا با تصدیق دریافت: این سرویس که مناسب ترین سرویس این لایه است در سه مرحله انجام می گیرد.

۱. مقدار دهی متغیرهای لازم برای شمارش فریم ها و غیره.

۲. انتقال فریم ها.

۳. قطع اتصال و آزاد سازی متغیرها و بافرها.

فریم بندی

جهت فریم بندی روش های زیر وجود دارد:

۱. شمارش کاراکترها: در این روش تعداد کاراکترهای فریم در یکی از فیلدهای سرآیند آن نوشته می شود. وقتی این فریم به مقصد برسد، لایه پیوند داده مقابل به کمک آنها فریم داده ای را مشخص می کند. شکل زیر مثالی از فریم بندی به کمک شمارش کاراکترها می باشد.

البته در این روش ممکن است بیت مشخص کننده آغاز و انتهای فریم هم آسیب ببیند. در این صورت راهی باقی نمی ماند جز این که به فکر روش مورد اعتماد دیگری باشیم.

۱. بایت های پرچم، با لاگذاری بایت: در این روش فلگ هایی (نشانه) برای مشخص کردن ابتدا و انتهای فریم داده ای استفاده می شود. این روش هم مشکلات خاص خود را دارد چون که ممکن است بخشی از داده ها شامل بایت های پرچم قراردادی باشد.

۲. پرچم های شروع و پایان، با لاگذاری بیت: در این شیوه هر فریم با طرح بیتی ۰۱۱۱۱۱۱۰ شروع می گردد و در سمت فرستنده به محض مشاهده ۵ بیت ۱ پشت سرهم یک ۰ قرار می دهد. عکس این رویداد در قسمت گیرنده رخ می دهد.

۳. حالت های غیر مجاز گذرانی لایه فیزیکی: در این روش در اصل نوعی افزونگی داریم. مثلاً در برخی LAN ها هر بیت داده با دو بیت فیزیکی نشان داده می شود: بیت ۱ با زوج بالا-پایین و بیت ۰ با زوج پایین-بالا.

در بسیاری از پروتکل های لینک داده برای اطمینان بیشتر از ترکیب روش های گفته شده استفاده می شود.

کنترل خطا:

جهت کنترل خطای دریافت اطلاعات معمولاً از دو مکانیزم استفاده می شود.

- تصدیق دریافت: گیرنده دریافت بسته را تصدیق می کند.
- استفاده از زمان سنج: هر بسته اگر در مدت زمان معینی به مقصد نرسید، دوباره ارسال می شود.

کنترل جریان:

برای یکی کردن سرعت ارسال و دریافت بسته های اطلاعاتی معمولاً از راهکارهای کنترل جریان استفاده می شود. در زیر چند راهکار را بیان می کنیم.

- کنترل جریان بر اساس بازخورد: گیرنده آمادگی خود را برای دریافت بسته ها اعلام می کند.
- کنترل جریان بر اساس نرخ

در شبکه های فراگیر که از یک کانال مشترک استفاده می کنند، اولین مسئله ای که پیش می آید این است که چه کسی از این کانال استفاده کند. به این کانال گاهی کانال های با دسترسی چند گانه یا کانال های با دسترسی تصادفی گوئیم. حال وظیفه ما است که کلاه مان را قاضی نموده و به ایستگاه های مختلف این اجازه را بدهیم که از کانال مشترک موجود استفاده بهینه را ببرند. وظیفه این عمل در دنیای شبکه بر عهده نرم افزارهای زیر لایه نظارت بر دسترسی به رسانه انتقال (MAC) می باشد. این زیر لایه وظیفه دارد که به کمک پروتکل هایی که در زیر ذکر می کنیم عدالت را بین ایستگاه ها پیاده نماید. حال فرض کنیم این کنترل انجام نگردد، در این حالت ممکن است چند ایستگاه به طور هم زمان نسبت به قرار دادن بسته های اطلاعاتی بر روی کانال اقدام کنند (این سناریو یادآور پاسخگویی هم زمان دانشجویان یک کلاس به یک پرسش استاد است). طبیعی است که هیچ یک از این بسته های اطلاعاتی قابل بازیافت توسط گیرنده (استاد در مثال ما) نیست. به این رویداد را تصادم گوئیم. در کانال های شبکه می توان با بررسی توان مصرفی یا اندازه گیری و مقایسه پهنای پالس سیگنال دریافتی از کانال و مقایسه آن با سیگنال ارسالی تشخیص داده می شود. این فرآیند تشخیص، به صورت آنالوگ انجام می شود.

پروتکل های ALOHA:

نورمن آبرامسون و همکاران او این روش را ایجاد کردند و دانشمندان دیگر به مرور به تکمیل آن پرداختند. دو نوع از این پروتکل ها در زیر بیان می شود.

:Pure ALOHA

در این روش که می توان آنرا بی منطق ترین حالت هم دانست، تمام ایستگاه ها به محض آماده شدن بسته های اطلاعاتی شان، آن را به کانال انتقال می فرستند. اگر تصادم رخ نداد که چه بهتر ولی اگر تصادمی رخ داد آنرا توسط کانال مستقلی گزارش می کند. بعد از گزارش تصادم این

فرآیند دوباره تکرار می شود. بعد محاسبات آماری مشخص شده است که در این حالت تنها ۱۸ درصد از کانال بهره برداری می شود. max کارایی در این روش وقتی است طول فریم ها یکسان باشد. زمانی که برخورد به وجود می آید فرستنده زمانی تصادفی صبر می کند و داده ها را دوباره منتقل می کند. منتظر ACK می ماند اگر ACK دریافت نکرد دوباره داده ها را ارسال می کند.

:Slotted ALOHA

در این روش از برش های زمانی استفاده می شود. الگوریتم این روش به قرار زیر است:

- بعد از مهیا شدن اطلاعات، ایستگاه باید آنقدر منتظر بماند تا به آغاز برش زمانی بعدی برسد.
- بعد از اتمام برش زمانی بسته اطلاعاتی به روی کانال ارسال می گردد.
- در صورت بروز تصادم این فرآیند دوباره تکرار می شود.

این پروتکل دو برابر بهتر از روش قبل است بنابراین میزان بهره کانال به ۳۷ درصد می رسد.

پروتکل های دسترسی چند گانه با قابلیت شنود سیگنال (CSMA):

به مجموعه این پروتکل ها، پروتکل های شنود سیگنال نیز گوییم. این پروتکل ها مناسب تر بوده و کاربردی تر هستند. چراکه بدون تحقیق حکم صادر نمی کنند.

:Persistent CSMA

به این پروتکل که گاهی به آن Persistent CSMA-1 نیز گوییم طبق الگوریتم زیر کار می کند.

۱. به کانال گوش بده.
۲. اگر کانال خالی است اطلاعات را به سوی کانال ارسال کن.
۱. در غیر این صورت به مرحله ۱ بازگرد.

در این روش نیز امکان تصادم وجود دارد. دو حالت زیر سناریوهای احتمالی وقوع این رویداد است:

- تاخیر انتشار وجود داشته باشد.
- انتظار هم زمان برای خالی شدن کانال.

Nonpersistent CSMA:

این پروتکل مبتنی بر شنود سیگنال است و طبق الگوریتم زیر است:

۱. به کانال گوش بده.
۲. اگر کانال خالی است اطلاعات را به سوی کانال ارسال کن.
 ۱. در غیر این صورت زمان تصادفی را صبر کن.
 ۳. بازگشت به مرحله ۱.

این روش با حالت قبل دو تفاوت دارد:

- تاخیر بیشتری نسبت به روش قبل دارد.
- زمان انتظار به صورت تصادفی محاسبه می گردد.

p-Persistent CSMA:

این پروتکل برای کانال های زمان بندی مناسب است و دارای الگوریتم زیر است:

۱. شنود کانال.
۲. اگر کانال اشغال نیست آنرا با احتمال p به روی کانال قرار بده (این امر قطعی نیست).
 ۱. در غیر این صورت تا بعد از اسلات بعدی صبر کن و به مرحله ۱ بازگرد.

تا اینجا چند پروتکل را بررسی کردیم، قبل از بحث در مورد ادامه پروتکل ها این نکته را خاطر نشان می کنیم که تمام پروتکل هایی که تا اینجا بررسی کردیم دسترسی تصادفی را به کانال دارند.

CSMA با تشخیص تصادم:

در این پروتکل به محض تشخیص تصادم ادامه ارسال فریم آسیب دیده متوقف می گردد. این قطع شدن سریع، باعث می شود که در پهنای باند به میزان زیادی سرفه جویی شود. چنین پروتکلی را به اختصار CSMA/CD یا پروتکل دسترسی چندگانه با قابلیت شنود سیگنال حامل همراه با تشخیص تصادم نامیم. CSMA/CD می تواند در سه وضعیت باشد:

- رقابت
- ارسال
- بیکار

لایه شبکه (سوم)

لایه شبکه (networklayer) به عنوان لایه سوم ارجاع داده شده است.

وظایف این لایه به ترتیب زیر است:

۱. کنترل عملکرد زیر شبکه
۲. مسیریابی
۳. کنترل گلوگاه ها
۴. کیفیت سرویس دهی
۵. به پیوستن شبکه های نا همگن
۶. آدرس دهی

پروتکل های عمومی لایه شبکه شامل:

^۱IP

^۲IPX

^۳ICMP

لایه شبکه (networklayer) عموماً به عنوان لایه سوم از مدل مرجع OSI ارجاع داده شده است و مسئولیت های زیر را دارد:

مسیریابی (Routing):

زمانی که یک میزبان در یک شبکه تمایل به تبادل اطلاعات با یک میزبان دیگری کند ، بسته ها به یک اینترفیس روتر فرستاده خواهد شد . پس از تعیین جایی که بسته باید فرستاده شود این اطلاعات درجدول مسیریابی شان بنیاد نهاده میشود. یک روتر بسته ها را به اینترفیس مربوط سوئیچ خواهد کرد . این روند برای هر روتری که با مسافرت بسته ها تا میزبان مقصد مواجه شود انجام خواهد شد. پروتکل های مسیریابی برای اجازه مسیریاب ها به تبادل اطلاعات با یکدیگر استفاده شده اند.

^۱Internet Protocol

^۲Internetwork Packet Excahnge

^۳Internet Control Message Protocol

بسته سازی

داده های پروتکل لایه فوقانی، داخل برنامه ها و بسته هایی قرار می گیرند که نقش هم زمان دارند. هیچ نصب مداری قبل از ارسال بسته ها به یک میزبان نیاز نیست. ارتباط در این شرایط از نوع پروتکل بدون ارتباط می باشد. شبکه های تلفنی کلیدی می توانند نصب مدار را عملی سازند قبل از آن که تلفن زنگ بزند.

لایه انتقال (لایه چهار):

لایه انتقال عموماً به لایه چهارم مرجوع داده میشود.

مسئولیت لایه برای قطعه قطعه سازی اطلاعات، استقرار از اتصالات سر-به-سر بین میزبان ها و کنترل جریان است.

پروتکل های لایه انتقال رایج شامل:

Transmission Control Protocol(TCP)

User Datagram Protocol (UDP)

لایه انتقال سه وظیفه عمده بر حسب تعویض داده ها بین سیستم ها دارد. این وظایف شامل:

قطعه قطعه کردن اطلاعات

استقرار از اتصالات سر-به-سر بین میزبان ها

استفاده مکانیزم های کنترل جریان برای اطمینان از اینکه اطلاعات به میزبان فرستاده شده باشند که گیرنده بتواند بکار ببرد.

لایه transport:

در شبکه های رایانه ای، لایه انتقال سرویس های ارتباطی مبدأ به مقصد یا end-to-end را برای برنامه های کاربردی موجود در معماری لایه بندی شده پروتکل ها و اجزاء شبکه فراهم می آورد. لایه انتقال سرویس های مطمئنی از قبیل پشتیبانی از جریان داده اتصال گرا، قابلیت اطمینان، کنترل جریان و تسهیم یا مالتی پلکسینگ را ارائه می نماید.

لایه های انتقال هم در (RFC ۱۱۲۲) مدل TCP/IP ، که مبنا و بنیان اینترنت می باشد، و هم مدل OSI موجود می باشند. تعریف لایه انتقال در این دو مدل کمی با یکدیگر تفاوت دارد.

معروف ترین پروتکل لایه انتقال پروتکل کنترل انتقال (tcp)Transmission Control Protocol می باشد. این پروتکل نام خود را از مجموعه پروتکل اینترنت یا همان TCP/IP وام گرفته است. از این پروتکل در انتقالات اتصال گرا استفاده می شود در حالیکه پروتکل بدون اتصال UDP برای انتقالات پیام ساده مورد استفاده قرار می گیرد. TCP پروتکل پیچیده تری است و این پیچیدگی به واسطه طراحی وضعیت محوری است که در سرویس های انتقالات قابل اطمینان و جریان داده تعبیه شده است.

جلسه های اتصال گرا:

جلسه های اتصال گرا احتیاج به گیرنده اطلاعات به فرستادن یک تصدیق به فرستنده دارند. اگر تصدیق دریافت نشد ، ارسال مجدد رخ می دهد. TCP یک مثال از یک پروتکل اتصال -گرا است.

زمانی که یک جلسه اتصال گرا بین سیستم ها مقرر شد ، تصدیقات به فرستنده به عنوان گواه این که سگمنت ها به مقصد شان رسیده اند برگرداننده میشود. اگر یک تصدیق دریافت نشده بود ، داده های هم دست شده مجددا فرستاده میشود. این سیستم به عنوان تصدیق مثبت با مخابره مجدد معروف است . به این ترتیب ، ارتباطات اتصال گرا معمولا به عنوان قابل اعتماد بودن ذکر شده اند . همچنین جلسه های اتصال گرا از شماره های دنباله دار استفاده میکنند که یک سیستم به وسیله کدام بسته ها شمارش شده ، که از باز هم گزارده شدن ترتیب صحیح به دریافت کننده استفاده کنند بالاترین قسمت از این تکنیک ها آن ها تهیه تائید اینکه در حقیقت سگمنت ها رسیده اند و درست سگمنت بندی شده اند است .

لایه جلسه (SessionLayer)

لایه جلسه (SessionLayer) به عنوان لایه پنج ارجاع داده شده است.
مسئولیت لایه برای ایجاد، اداره و پایان یابی از جلسه های بین سیستم ها است.
پروتکل های عمومی لایه جلسه شامل:

Network File System (NFS)

Structured Query Language (SQL)

Remote Procedure Call (RPC)

مسئولیت لایه جلسه (sessionlayer) برای ایجاد، اداره و پایان یابی از جلسه های بین سیستم ها است.

یک جلسه به عنوان یک نوع از ارتباط اداره شده بین سیستم ها به مقصود یک نوع خاص از ارتباط توصیف شده است. به طور مثال، ممکن است یک جلسه به مقصود تصدیق کاربر یا شروع یک انتقال فایل ایجاد شده باشد. همچنین لایه جلسه (session) مسئولیت هماهنگ کردن چگونگی قرار گیری اتصال بین سیستم ها را که به عنوان کنترل محاوره شناخته شده است می باشد.

در بعضی جلسات، تنها یک سیستم منفرد اجازه ارتباط در هر نقطه در یک زمان را دارد که به عنوان half-duplex ذکر شده است.

لایه جلسه (sessionlayer) برای تعیین اینکه چه کسی این وضعیت ها را روشن و برای چه مدت هر سیستم اجازه ارتباط دارند را مسئول خواهد بود. در مورد دیگر، هر دو سیستم در یک زمان میتوانند ارتباط داشته باشند که به عنوان Full duplex شناخته شده است.

اگر جریان ارتباط به نحوی قطع شده بود، لایه جلسه (sessionlayer) برای این تشخیص و ایجاد دوباره این جلسه مسئول خواهد بود.

جدول زیر شکل اجمالی مثالهایی از پروتکل های عمومی لایه جلسه را نشان میدهد.

هدف	پروتکل
دستیابی سیستم فایل UNIX	network file system(NFS)
نمایش های پایگاه داده محلی یا از راه دور	Structure Query Language(SQL)
مکانیزم ارتباط سرور- سرویس گیرنده	Remote Procedure Protocol (RPC)
مکانیزم ارتباط سرور- Apple سرویس گیرنده talk	Apple Talk Session Protocol (ASP)
جلسه های دسکتاپ از راه دور	X windo

لایه نمایش:

لایه نمایش اصولاً مسئولیت برای نمایش اطلاعات ، قالب بندی ، اطمینان از اینکه اطلاعات میتواند درست نمایش داده شود است. این قالب بندیها گاهی به عنوان نحو اطلاعات از برنامه ها در حال استفاده ارجاع داده شده است. برای مثال ، سیستم های مختلف ممکن است از تمهید

\presentationlayer

مختلفی برای نمایش اطلاعات استفاده کنند. در حالی که یک سیستم امکان دارد از ASCII یا EBCDIC, سیستم دیگر از UNICODE استفاده کند. از اینرو این تمهیدات احتمال محتوای کارکترهای مختلف را دارد. این مسئولیت لایه نمایش (presentation) برای اطمینان حاصل کردن از نمایش قالب صحیح یا عمومی بین سرویس گیرنده و سرور است. بیشتر از این, لایه نمایش همچنین جایی است که برای فشرده سازی, رمزگزاری اطلاعات در نظر گرفته شده است.

جدول زیر شکل اجمالی مثالهایی از قالب بندیهای اطلاعات لایه نمایش مدل مرجع OSI را که بنیاد نهاده شده اند را نشان می دهد.

هدف	قالبندی های اطلاعات
قالب بندی های رمزگذاری متن	ASCII, EBCDIC, UNICODE, RTF
قالب بندی های رمزگذاری ویدئو	MPEG, AVI, Quick Time
قالبندی های گرافیکی	JPEG, PNG, TIFF
قالب صدا	MIDI

لایه کاربردی (لایه هفت):

لایه Application همچنین به عنوان لایه هفت ارجاع داده شده است

برنامه های کاربردی و کاربران در این لایه با شبکه تعامل دارند.

مثال های متداول پروتکل ها و برنامه های لایه application شامل :

پست الکترونیکی مشتریان (SMTP, POP3, IMAP)

جستجوگرهای وب و سرورها (HTTP)

انتقال فایل (FTP)

لایه application (کاربردی) لایه بالایی از مدل مرجع OSI, و مکانی که کاربران با شبکه تعامل دارند در نظر گرفته شده است. این تعامل معمولاً بوسیله فعالیت یک برنامه از قبیل یک جستجوگر وب یا یک برنامه صفحه گسترده رخ می دهد. این لایه واقعا نگرانی درباره شبکه ندارد. در عوض, به سادگی میداند چگونه تقاضای چیزی (این اطلاعات است) و سپس چه کاری باید با پاسخ (اطلاعاتی که تقاضا شده بود) انجام دهد.

در مورد جستجوی یک وب سایت توسط یک کاربر, جستجوگر وب یک تقاضای HTTP که بوسیله برنامه دریافت شونده در انتهای دیگر (وب سرور) درک شده است را میسازد. این گاهی مواقع به عنوان یک ارتباط برنامه - به - برنامه ذکر شده است. لایه های پایین تر از مدل مرجع با چگونگی این وضعیت که این اطلاعات چگونه بسته بندی و انتقال یافته اند بستگی دارند.

جدول زیر شکل اجمالی مثالهای عمومی از پروتکل ها و برنامه های که در لایه کاربردی (application) مدل مرجع OSI بنیاد نهاده شده اند را نشان می دهد.

هدف	برنامه
ایجاد سنده های , احتمال نگهداری در یک سرور شبکه	واژه پرداز
دستیابی به سرویس های وب اینترنت	جستجوگر وب (http)
پست الکترونیک مشتریان (SMTP,POP۳,IMAP)	فرستادن و دریافت پست الکترونیکی
جلسه ترمینال از راه دور	Telnet
انتقال فایل	انتقال (FTP) فایل

درس ۳

مدل TCP/IP یا Internet protocol /Transmission Control Protocol

مفهوم TCP/IP:

TCP/IP مجموعه قراردادهایی هستند که در جهت اتصال کامپیوترها در شبکه مورد استفاده قرار می گیرند. وبه تعریف دیگر قرارداد کنترل انتقال اطلاعات می باشد. مدل چهار لایه TCP/IP از لایه های زیر تشکیل شده است.

لایه کاربرد

لایه انتقال

لایه شبکه

لایه واسطه شبکه

لایه واسط شبکه

در این لایه تمام استانداردهای سخت افزاری و انواع پروتکل شبکه تعریف شده که خاصیت بزرگ این لایه این موضوع می باشد که در آن می توان بین نرم افزار و سخت افزار شبکه ارتباط برقرار کرد.

لایه شبکه:

در این لایه پروتکل IP آدرس دهی و تنظیم می شود. (توضیحات در قسمت IP) و همچنین دیگر پروتکل ها مانند ARP, ICMP که در این میان نقش هیچکدام به اندازه ICMP, IP مهم نیست در کل وظیفه این لایه دادن اطلاعات در مورد شبکه و آدرس دهی در آن می باشد که مسیر یابها از آن بسیار استفاده می کنند.

لایه انتقال:

ابتدایی ترین وظیف این لایه آگاهی از وضعیت بسته ها می باشد که بسیار مهم نیز هست. و در مرحله بعد وظیفه این لایه انتقال اطلاعاتی می باشد که نیاز به امنیت ندارند و سرعت برای آنها مهم تر است.

لایه کاربرد:

این لایه دارای امکانات زیادی برای هنر نمایی متخصصان می باشد. در این لایه برنامه های کاربردی قرار دارند و در کل این لایه لایه ی نرم افزارهای شبکه می باشد و همچنین لایه پروتکل های نرم افزاری نیز می باشد. از مهم ترین نکات در خصوص این لایه قراردادن: انتقال فایل (FTP) و مدیریت پست (SMTP) و بقیه برنامه های کاربردی می باشد.

مقایسه مدل های OSI و TCP/IP:

شاید بزرگترین دستاورد مدل OSI روشن ساختن مفاهیم فوق (و تفکیک آنها) باشد. هر لایه سرویس هایی در اختیار لایه های بالاتر از خود قرار می دهد. تعریف این سرویس ها فقط می گوید که یک لایه چه کاری انجام می دهد، و هیچ حرفی در مورد نحوه انجام آنها و چگونگی استفاده از سرویس ها نمی زند.

تعریف چگونگی دسترسی به سرویس های یک لایه بر عهده واسط است. واسط پارامترهای ورودی لازم، و نتیجه ای را که باید منتظر آن باشید، تعریف می کند. حتی واسط هم نمی گوید که یک لایه کار خود را چگونه انجام می دهد. و بالاخره، کاری را که یک لایه انجام می دهد را پروتکل های آن لایه تعریف می کنند. یک لایه مادامی که کار خود را درست انجام دهد، می تواند از هر پروتکلی استفاده کند. تغییر پروتکل های یک لایه هیچ تاثیری روی ارتباط آن با لایه های بالاتر نخواهد گذاشت.

ایده های فوق بسیار شبیه به مفاهیم مدرن برنامه نویسی شی گرا هستند. هر شی، مانند یک لایه، متدها (عملکردها) یی دارد که اشیا دیگر از آن استفاده می کنند. نحوه استفاده از این متدها در واقع همان سرویس هایی است که این شی در اختیار دیگران می گذارد. ورودی ها و خروجی های شی واسط آن با دنیای خارج هستند. کد اجرایی شی نیز شبیه همان پروتکل است، که نحوه عملکرد آن از دید دیگران مخفی است.

در مدل اولیه TCP/IP تمایز بین سرویس ها، واسطها و پروتکل ها واضح و مشخص نبود، اگر چه افرادی (با توجه به تجربه موفق OSI) سعی کرده بودند آن را هر چه بیشتر شبیه OSI کنند. برای مثال لایه اینترنت فقط دو سرویس واقعی به نامهای SEND IP PACKET و RECEIVE IP PACKET داشت. با توجه به این وضع، پروتکل های OSI بهتر از TCP/IP مخفی شده اند، و امکان تغییر آنها به راحتی وجود دارد، چیزی که هدف نهایی طراحی لایه ای محسوب می شود. مدل OSI قبل از اختراع پروتکل های آن طراحی و ابداع شد. این بدان معناست که مدل OSI وابستگی و تمایل خاصی به هیچ مجموعه پروتکلی ندارد، چیزی که در سایر مدل ها بسیار دیده می شود. البته این وضعیت یک نقطه ضعف نیز دارد و آن این است که طراحان تجربه چندانی در زمینه موضوع کار ندارند، و واقعا نمی دانند کدام عملکرد را باید در کدام لایه قرار دهند. برای مثال، لایه پیوند داده در ابتدا فقط برای شبکه های نقطه-به-نقطه طراحی شده بود، وقتی شبکه های بخشی وارد بازار شد، مجبور شدند یک زیر لایه به آن اضافه کنند.

وقتی که افراد شروع به طراحی شبکه با استفاده از مدل OSI و پروتکل های موجود کردند، به زودی دریافتند که این شبکه ها با سرویس های مورد نیاز انطباق ندارند. بنابر این مجبور شدند زیر لایه های زیادی به آن وصله پینه کنند. بالاخره، کمیته استاندارد مقرر کرد که هر کشور برای خود یک مدل منطبق با مدل OSI (تحت نظارت دولت) داشته باشد، شبکه ای که به هیچ عنوان آینده (اینترنت) در آن دیده نشده بود. خلاصه، کارها آنطوری که انتظار داشتند از آب در نیامد. در مورد TCP/IP وضع بر عکس بود: اول پروتکل ها اختراع و توسعه داده شدند، و سپس مدلی برای

توصیف آنها ساخته شد. هیچ مشکلی در زمینه انطباق پروتکل ها با مدل وجود نداشت. همه چیز جفت و جور بود، تنها مشکل این بود که این مدل با هیچ مجموعه پروتکل دیگری جور در نمی آمد.

این بدان معنا بود که مدل TCP/IP به درد توصیف شبکه های غیر TCP/IP نمی خورد. جدای از مسایل فلسفی قضیه، تفاوت دیگر در تعداد لایه های این دو مدل است: مدل OSI هفت لایه دارد و مدل TCP/IP چهار لایه. لایه های شبکه، انتقال و کاربرد در هر دو مشترک اند، ولی لایه های دیگر فرق دارند. تفاوت دیگر در زمینه اطلاعات اتصال-گرا و غیر متصل است. مدل OSI از هر دو نوع ارتباط اتصال-گرا و متصل در لایه شبکه پشتیبانی می کند، ولی در لایه انتقال فقط سرویس اتصال-گرا دارد (چون این سرویس در معرض دید کاربران است). مدل TCP/IP در لایه شبکه فقط سرویس غیر متصل دارد، ولی در لایه انتقال از هر دو نوع ارتباط پشتیبانی می کند، و دست کاربر را برای انتخاب باز می گذارد (که به ویژه برای پروتکل های ساده درخواست -پاسخ بسیار مهم است).

نقد مدل OSI و پروتکل های آن :

مدل OSI و TCP/IP (و پروتکل هایشان) هیچکدام کامل نیستند و جا دارد برخی از نقاط ضعف آنها را برشماریم. در این قسمت، برخی از نقاط ضعف مدل های OSI و TCP/IP را بررسی خواهیم کرد. با مدل OSI شروع می کنیم. در سال ۱۹۸۹، بسیاری متخصصان برجسته شبکه بر این باور بودند که آینده در بست متعلق به مدل OSI و پروتکل های آن است، و هیچ چیز نمی تواند در مقابل پیشرفت آن مقاومت کند. اما این اتفاق نیفتاد. چرا؟ نگاهی به گذشته درسهای بسیاری را برای چشمان عبرت بین دارد، که می توان آنها را چنین خلاصه کرد: ۱. زمان نامناسب ۲. تکنولوژی نامناسب ۳. پیاده سازی نامناسب ۴. سیاست های نامناسب .

زمان نامناسب :

اولین عامل شکست مدل OSI زمان نامناسب بود. زمانی که یک استاندارد وضع می شود، اهمیت حیاتی در موفقیت و عدم موفقیت آن دارد. دیوید کلارک از دانشگاه M.I.T فرضیه ای در زمینه

استانداردها دارد که ملاقات فیل ها معروف است. این نظریه میزان فعالیت های حول یک موضوع جدید را نشان می دهد. وقتی موضوعی برای اولین بار کشف می شود، گرداگرد آن سیلی از فعالیت های تحقیقی (به شکل بحث، مقاله و سخنرانی) فرا می گیرد. بعد از مدتی این فروکش می کند و بعد از اینکه صنعت به این موضوع علاقه مند شد، موج سرمایه گذاری ها از پی می آید. بسیار مهم است که در محل تلاقی این دو فیل (موج تحقیق و موج سرمایه گذاری) استانداردها به طور کامل وضع شوند. اگر استاندارد زودتر از موعد (قبل از پایان تحقیقات) نوشته شود، خطر آن هست که موضوع به درستی درک نشده باشد و استاندارد ضعیف از آب در آید. اگر استاندارد دیرتر از موعد (بعد از شروع موج سرمایه گذاری) نوشته شود، شرکتهای بسیاری قبلا -از مسیرهای مختلف- در آن سرمایه گذاری کرده اند، و این خطر هست که استانداردهای آنها را نادیده بگیرد. اگر فاصله این دو فیل خیلی کم باشد (همه عجله داشته باشند که کار را زودتر شروع کنند)، خطر آن هست که استاندارد نویسان بین آنها له شوند. اکنون معلوم شده است که پروتکل های استاندارد OSI بین فیل ها له شده اند. وقتی که پروتکل های OSI پا به عرصه وجود گذاشتند، پروتکل های رقیب (TCP/IP) مدت ها بود که در مراکز تحقیقاتی و دانشگاه ها پذیرفته شده بودند. با اینکه هنوز موج سرمایه گذاری صنعتی در TCP/IP شروع نشده بود. اما بازار آکادمیک آنقدر بزرگ بود که شرکتهای بسیاری را تشویق به تولید محصولات TCP/IP کند. و وقتی OSI بالاخره از راه رسید، کسی نبود که داوطلبانه از آن پشتیبانی کند. همه منتظر بودند دیگری قدم اول را بردارد. قدمی که هرگز برداشته نشد. OSI در نطفه خفه شد.

تکنولوژی نامناسب:

دلیل دیگری که OSI هرگز پا نگرفت آن بود که، این مدل و پروتکل های آن هر دو ناقص و معیوب بودند. انتخاب هفت لایه برای این مدل بیشتر یک انتخاب سیاسی بود تا فنی، و در حالی که دو لایه آن (نشست و نمایش) تقریبا خالی بودند، در لایه های دیگر (لینک داده و شبکه) جای نفس کشیدن نبود. مدل OSI (و سرویس ها و پروتکل های آن) به طور باور نکردی پیچیده است. اگر کاغذهای چاپی این استاندارد را روی هم بچینید. ارتفاع آن از نیم متر هم بیشتر خواهد شد. پیاده سازی

پروتکل های OSI بسیار دشوار، و عملکرد آنها ناقص است. در این رابطه، نقل جمله جالبی از پاول موکاپتریس (Rose، ۱۹۹۳) خالی از لطف نیست: سوال: از ترکیب یک گانگستر با یک استاندارد بین المللی چه چیزی بدست می آید؟ جواب: کسی پیشنهادی به شما می کند که از آن سر در نمی آورید. مشکل دیگر مدل OSI، علاوه بر غیر قابل فهم بودن آن، این است که برخی از عملکرد های آن (مانند آدرس دهی، کنترل جریان داده ها و کنترل خطا) در تمام لایه ها تکرار می شود. برای مثال، سالتزر و همکارانش (۱۹۸۴) نشان دادند که کنترل خطا باید در بالاترین لایه انجام شود تا بیشترین تاثیر را داشته باشد. بنابراین تکرار آن در لایه های پائین تر نه تنها غیر ضروری است، بلکه باعث افت کارایی هم خواهد شد.

ارسال داده : شکل زیر نحوه ارسال داده توسط یک کامپیوتر را نشان می دهد :



توضیحات :

- کامپیوتر موجود در شبکه ، قصد ارسال داده برای کامپیوتر دیگر را دارد . در لایه Application ، رابط کاربر وجود داشته و از طریق آن کاربر با برنامه مورد نظر ارتباط برقرار می نماید .
- پس از ارسال داده از لایه Application ، داده ارسالی به ترتیب لایه های Presentation و Session را طی می نماید . هر یک از لایه های فوق اطلاعات اضافه ای را به داده اولیه اضافه نموده و در نهایت داده در اختیار لایه Transport قرار داده می شود .

- در لایه Transport ، داده به بخش های کوچکتری تقسیم و هدر TCP به آن اضافه می گردد . به داده موجود در لایه Transport ، "سگمنت" گفته می شود . هر سگمنت شماره گذاری شده تا امکان بازسازی مجدد آنان در مقصد وجود داشته باشد (انتظار داریم داده دریافتی توسط گیرنده همان داده ارسالی توسط فرستنده باشد) .
- هر سگمنت در ادامه به منظور آدرس دهی شبکه (منظور آدرس دهی منطقی است) و روتینگ مناسب در اختیار لایه Network قرار داده می شود . به داده موجود در لایه Network ، بسته اطلاعاتی و یا Packet گفته می شود . لایه Network ، هدر IP خود را به آن اضافه نموده و آن را برای لایه DataLink ارسال می نماید .
- در لایه DataLink به داده ئی که هم اینک شامل هدر لایه های Transport و Network است ، "فریم" گفته می شود . در این لایه ، هر یک از بسته های اطلاعاتی دریافتی، کپسوله شده و در یک فریم به همراه آدرس سخت افزاری (آدرس MAC) کامپیوترهای فرستنده و گیرنده سازماندهی می شوند . در فریم فوق اطلاعات مربوط به LLC (نوع پروتکل ارسالی توسط لایه قبلی زمانی که به کامپیوتر مقصد می رسد)، نیز اضافه می شود . در بخش انتهائی فریم ، فیلدی با نام FCS که از کلمات Frame Check Sequence اقتباس شده است به منظور بررسی خطاء اضافه می گردد .
- در صورتی که کامپیوتر مقصد بر روی یک کامپیوتر از راه دور باشد ، فریم به روتر و یا gateway به منظور مسیریابی مناسب ارسال می گردد .
- به منظور استقرار فریم بر روی شبکه می بایست اطلاعات موجود به صورت سیگنال های دیجیتال تبدیل شوند . با توجه به این که یک فریم مشتمل بر مجموعه ای از صفر و یک است ، لایه Physical عملیات کپسوله نمودن ارقام موجود در فریم به یک سیگنال دیجیتال را انجام خواهد داد .
- در ابتدای فریم و به منظور انجام عملیات همزمان سازی (هماهنگ شدن دریافت کننده با فرستنده) ، تعداد اندکی صفر و یک اضافه می گردد .

دریافت داده : شکل زیر نحوه دریافت داده توسط یک کامپیوتر را نشان می دهد :



توضیحات :

- کامپیوتر دریافت کننده در ابتدا به منظور هماهنگ کردن خود با کامپیوتر فرستنده در جهت خواندن سیگنال دیجیتال، تعداد محدودی از بیت ها را می خواند . پس از اتمام عملیات همزمان سازی و دریافت تمامی فریم آن را به لایه بالاتر (لایه DataLink)، ارسال می نماید .
- لایه DataLink، در ابتدا بررسی لازم در رابطه با وجود خطاء (CRC) و یا همان Cyclic Redundancy Check را در خصوص اطلاعات دریافتی انجام خواهد داد . محاسبات فوق توسط کامپیوتر دریافت کننده انجام شده و ماحصل کار با مقدار موجود در فیلد FCS مقایسه شده و بر اساس آن تشخیص داده خواهد شد که آیا فریم دریافتی بدون بروز خطاء دریافت شده است ؟ در ادامه لایه DataLink، اطلاعات اضافه و یا هدری را که توسط لایه DataLink کامپیوتر از راه دور به آن اضافه شده است را برداشته و مابقی داده را که به آن Packet اطلاق می گردد برای لایه Network ارسال می نماید .
- در لایه Network، آدرس IP موجود در بسته اطلاعاتی با آدرس IP کامپیوتر دریافت کننده مقایسه شده و در صورت مطابقت، هدر لایه Network و یا هدر IP از بسته اطلاعاتی برداشته شده و مابقی بسته اطلاعاتی برای لایه بالاتر (لایه Transport)، ارسال می گردد . به داده موجود در این لایه، سگمنت گفته می شود .
- سگمنت در لایه Transport پردازش و عملیات بازسازی مجدد داده دریافتی، انجام خواهد شد . در زمان بازسازی مجدد داده دریافتی توسط کامپیوتر گیرنده به فرستنده اطلاع داده

می شود که وی هر یک از بخش ها را دریافت نموده است تا خللی در بازسازی مجدد داده ایجاد نگردد . با توجه به ارسال یک ACK برای فرستنده (اعلام وضعیت سگمنت دریافتی به کامپیوتر فرستنده) ، از پروتکل TCP در مقابل UDP استفاده شده است . پس از انجام عملیات فوق ، داده دریافتی در اختیار لایه Application گذاشته می شود .

در زمان مبادله اطلاعات بین کامپیوترهای موجود در شبکه ، کاربران درگیر جزئیات مسئله نشده و تمامی فرآیندهای اشاره شده به صورت اتوماتیک انجام خواهد شد .

فصل ۲

Network Hardware

درس ۱: کابل های شبکه

اکثر شبکه های محلی با استفاده از برخی از انواع کابلها به عنوان رسانه شبکه خود را مدیریت میکنند . اگر چه انواع بسیاری از رسانه های بی سیم وجود دارد اما کابل مطمئن ترین نوع رسانه هستند و به طور کلی ارائه سرعت های بالاتر تنها از طریق کابلها امکان پذیر میباشد. پروتکل های لایه پیوند داده ها مشخصات کابل را انتخاب میکند. هر ویژگی کابل نسبت به نوع کابل و کلاس کابل، مشخص میشود. نوع کابلی که شما انتخاب می کنید باید در مورد نیاز های خود و محل نصب آن اطلاعات لازم را داشته باشید و از همه مهمتر بودجه.

رسانه انتقال^۱:

رسانه انتقال کامپیوتر ها را به یکدیگر متصل کرده و موجب برقراری ارتباط بین کامپیوتر های یک شبکه می شود . برخی از متداولترین رسانه های انتقال عبارتند از : کابل زوج سیم بهم تابیده " Twisted- Pair" ، کابل کواکسیال " Coaxial " و کابل فیبر نوری " Fiber- Optic"

توپولوژی کابل های شبکه:

همانطور که در بخش قبلی توضیح داده شده است، "مبانی شبکه یا توپولوژی شبکه ، الگوی مورد استفاده برای اتصال رایانه ها و دستگاه های دیگر با استفاده از شبکه کابل و یا دیگر اجزا میباشد.. توپولوژی شبکه مستقیما متناظر است با نوع کابل. شما می توانید نوع خاصی از کابل را انتخاب کنید و آن را نصب کنید فقط باید با توپولوژی شما سازگار باشد گرچه شما می توانید یک شبکه انحصاری با توپولوژی خاص خود و با به کمک گیری کابلها و روترها و سویچها بسازید اما این کار معقولانه نیست . در هنگام ساخت یک شبکه انتخاب توپولوژی مناسب یکی از مهمترین قسمتها میباشد. در ادامه به انواع توپولوژی ها میپردازیم.

^۱Transmission Medium

۱- توپولوژی ستاره ای:

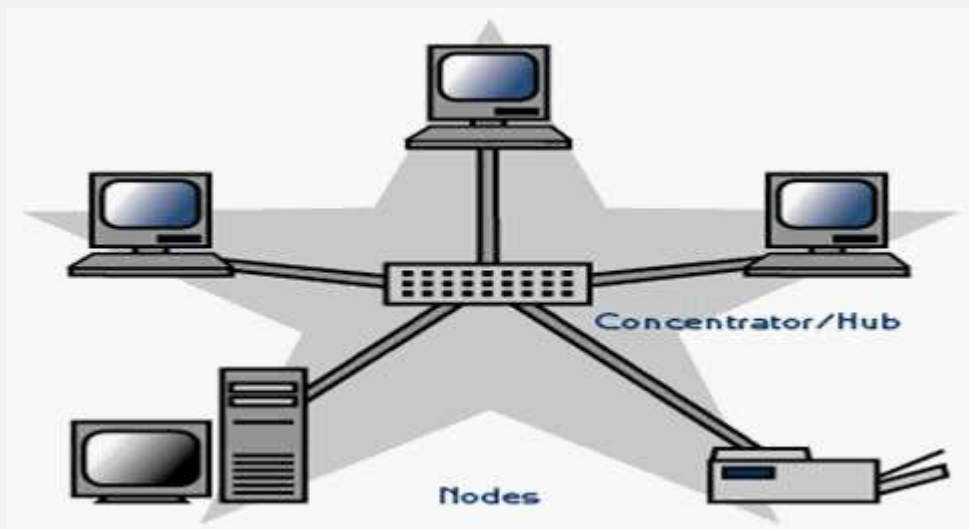
در این توپولوژی ، کلیه کامپیوتر ها به یک کنترل کننده مرکزی با هاب متصل هستند. هرگاه کامپیوتری بخواهد با کامپیوتری دیگری تبادل اطلاعات نماید، کامپیوتر منبع ابتدا باید اطلاعات را به هاب ارسال نماید. سپس از طریق هاب آن اطلاعات به کامپیوتر مقصد منتقل شود. اگر کامپیوتر شماره یک بخواهد اطلاعاتی را به کامپیوتر شماره ۳ بفرستد ، باید اطلاعات را ابتدا به هاب ارسال کند، آنگاه هاب آن اطلاعات را به کامپیوتر شماره سه خواهد فرستاد.

نقاط ضعف این توپولوژی آن است که عملیات کل شبکه به هاب وابسته است. این بدان معناست که اگر هاب از کار بیفتد، کل شبکه از کار خواهد افتاد . نقاط قوت توپولوژی ستاره عبارتند از:

نصب شبکه با این توپولوژی ساده است.

توسعه شبکه با این توپولوژی به راحتی انجام می شود.

اگر یکی از خطوط متصل به هاب قطع شود ، فقط یک کامپیوتر از شبکه خارج می شود.



توپولوژی حلقوی!:

این توپولوژی توسط شرکت IBM اختراع شد و بهمین دلیل است که این توپولوژی بنام IBM Tokenring " مشهور است.

در این توپولوژی کلیه کامپیوترها به گونه ای به یکدیگر متصل هستند که مجموعه آنها یک حلقه را می سازد. کامپیوتر مبدا اطلاعات را به کامپیوتری بعدی در حلقه ارسال نموده و آن کامپیوتر آدرس اطلاعات را برای خود کپی می کند، آنگاه اطلاعات را به کامپیوتر بعدی در حلقه منتقل خواهد کرد و بهمین ترتیب این روند ادامه پیدا می کند تا اطلاعات به کامپیوتر مبدا برسد. سپس کامپیوتر مبدا این اطلاعات را از روی حلقه حذف می کند.

نقاط ضعف توپولوژی فوق عبارتند از:

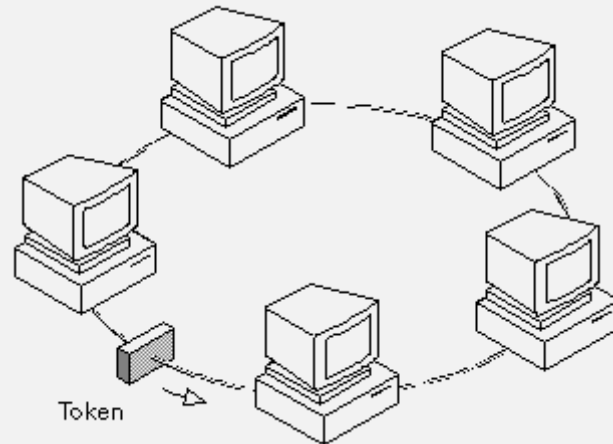
اگر یک کامپیوتر از کار بیفتد ، کل شبکه متوقف می شود.

به سخت افزار پیچیده نیاز دارد " کارت شبکه آن گران قیمت است ".
برای اضافه کردن یک ایستگاه به شبکه باید کل شبکه را متوقف کرد.

نقاط قوت توپولوژی فوق عبارتند از :

نصب شبکه با این توپولوژی ساده است.

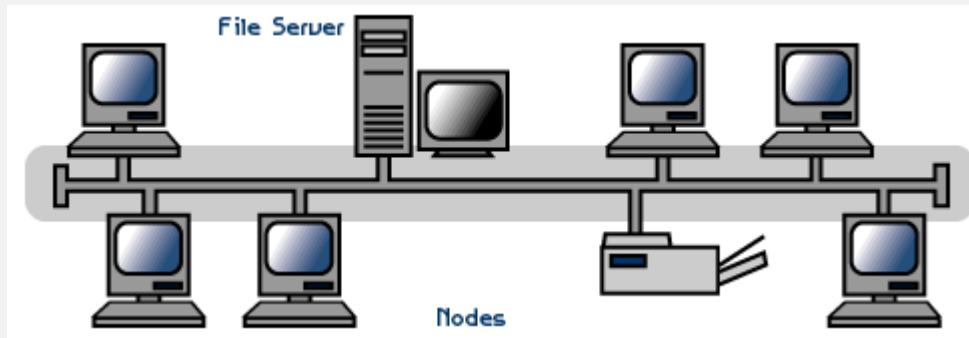
توسعه شبکه با این توپولوژی به راحتی انجام می شود.
در این توپولوژی از کابل فیبر نوری میتوان استفاده کرد.



توپولوژی اتوبوسی^۱:

در یک شبکه خطی چندین کامپیوتر به یک کابل بنام اتوبوسی متصل می شوند. در این توپولوژی ، رسانه انتقال بین کلیه کامپیوترها مشترک است. یکی از مشهورترین قوانین نظارت بر خطوط ارتباطی در شبکه های محلی اترنت است. توپولوژی اتوبوس از متداولترین توپولوژی هایی است که در شبکه محلی مورد استفاده قرار می گیرد. سادگی ، کم هزینه بودن و توسعه آسان این شبکه ، از نقاط قوت توپولوژی اتوبوسی می باشد. نقطه ضعف عمده این شبکه آن است که اگر کابل اصلی که بعنوان پل ارتباطی بین کامپیوترهای شبکه می باشد قطع شود، کل شبکه از کار خواهد افتاد.

^۱Bus

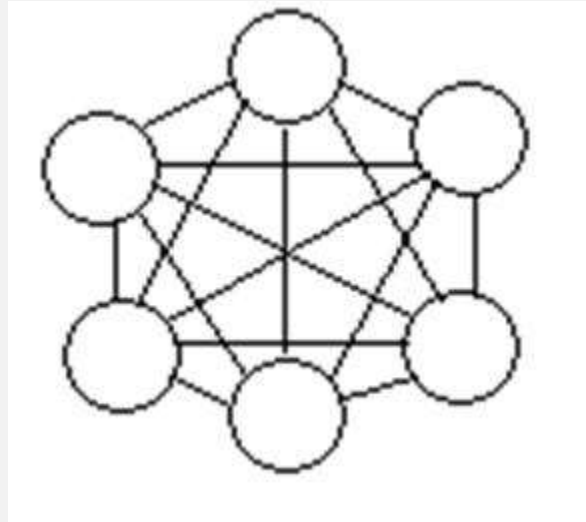


توپولوژی توری^۱:

در این توپولوژی هر کامپیوتری مستقیماً به کلیه کامپیوترهای شبکه متصل می شود. مزیت این توپولوژی آن است که هر کامپیوتر با سایر کامپیوترها ارتباطی مجزا دارد. بنابراین، این توپولوژی دارای بالاترین درجه امنیت و اطمینان می باشد. اگر یک کابل ارتباطی در این توپولوژی قطع شود، شبکه همچنان فعال باقی می ماند.

از نقاط ضعف اساسی این توپولوژی آن است که از تعداد زیادی خطوط ارتباطی استفاده می کند، مخصوصاً زمانی که تعداد ایستگاهها افزایش یابند. به همین جهت این توپولوژی از نظر اقتصادی مقرون به صرفه نیست. برای مثال، در یک شبکه با صد ایستگاه کاری، ایستگاه شماره یک نیازمند به نود و نه می باشد. تعداد کابل های مورد نیاز در این توپولوژی با رابطه $N(N-1)/2$ محاسبه می شود که در آن N تعداد ایستگاه های شبکه می باشد.

^۱Mesh



توپولوژی درختی^۱:

این توپولوژی از یک یا چند هاب فعال یا تکرار کننده برای اتصال ایستگاه ها به یکدیگر استفاده می کند. هاب مهمترین عنصر شبکه مبتنی بر توپولوژی درختی است: زیرا کلیه ایستگاه ها را به یکدیگر متصل می کند. وظیفه هاب دریافت اطلاعات از یک ایستگاه و تکرار و تقویت آن اطلاعات و سپس ارسال آنها به ایستگاه دیگر می باشد.

توپولوژی ترکیبی^۲:

این توپولوژی ترکیبی است از چند شبکه با توپولوژی متفاوت که توسط یک کابل اصلی بنام استخوان بندی "boneBack" به یکدیگر مرتبط شده اند. هر شبکه توسط یک پل ارتباطی "Bridg" به کابل استخوان بندی متصل می شود.

^۱Tree
^۲Hybrid

کابل شبکه:

کابل شبکه، رسانه ای است که از طریق آن، اطلاعات از يك دستگاه موجود در شبکه به دستگاه دیگر انتقال می یابد. انواع مختلفی از کابلها بطور معمول در شبکه های LAN استفاده می شوند. در برخی موارد شبکه تنها از يك نوع کابل استفاده می کند، اما گاه انواعی از کابلها در شبکه به کار گرفته می شود. غیر از عامل توپولوژی، پروتکل و اندازه شبکه نیز در انتخاب کابل شبکه مؤثرند. آگاهی از ویژگیهای انواع مختلف کابلها و ارتباط آنها با دیگر جنبه های شبکه برای توسعه يك شبکه موفق ضروری است.

امروزه سه گروه از کابلها، در ایجاد شبکه مطرح هستند:

کابلهای Coaxial زمانی بیشترین مصرف را در میان کابلهای موجود در شبکه داشت. چند دلیل اصلی برای استفاده زیاد از این نوع کابل وجود دارد:

۱- قیمت ارزان آن.

۲- سبکی و انعطاف پذیری.

۳- این نوع کابل به نسبت زیادی در برابر سیگنالهای مداخله گر مقاومت می نماید.

۴- مسافت بیشتری را بین دستگاههای موجود در شبکه، نسبت به کابل UTP پشتیبانی می نماید. قسمتهای یک کابل Coaxial:

(۱) Conducting Core یا هسته مرکزی که معمولاً از يك رشته سیم جامد مسی تشکیل می گردد.

(۲) Insulation یا عایق که معمولاً از جنس PVC یا تفلون است.

(۳) Copper Wire Mesh که از سیمهای بافته شده تشکیل می شود و کار آن جمع آوری امواج الکترومغناطیسی است.

(۴) Jacket که جنس آن اغلب از پلاستیک بوده و نگهدارنده خارجی سیم در برابر خطرات فیزیکی است.

کابل Coaxial به دو دسته تقسیم می شود:

- Thin net: کابلی است بسیار سبک، انعطاف پذیر و ارزان قیمت، قطر سیم در آن ۶ میلیمتر معادل ۰/۲۵ اینچ است. مقدار مسیری که توسط آن پشتیبانی می شود ۱۸۵ متر است.

- Thick net: این کابل قطری تقریباً ۲ برابر Thin net دارد. کابل مذکور، پوشش محافظی را (علاوه بر محافظ خود) داراست که از جنس پلاستیک بوده و بخار را از هسته مرکزی دور می سازد.

رایج ترین نوع اتصال دهنده (connector) مورد استفاده در کابل coaxial،

Bayonet-Neill-Concelman (BNC) می باشد. انواع مختلفی از سازگار کننده ها برای BNCها

وجود دارند شامل: Barrel connector , Tconnector

در شبکه هایی با توپولوژی اتوبوسی از کابل coaxial استفاده می شود.

استفاده از کابل coaxial در شبکه اتوبوسی:

باید دانست که از عبارتهایی مانند "Base10۵" برای توضیح اینکه چه کابلی در ساخت شبکه بکار رفته استفاده می گردد. عبارت مذکور بدان معناست که از کابل coaxial و از نوع Thicknet استفاده شده، علاوه بر آن روش انتقال در این شبکه، روش Baseband است و نیز سرعت انتقال ۱۰ مگابیت در ثانیه (mbps) می باشد. همچنین "Base10۲" یعنی اینکه از کابل Thinnet استفاده شده، روش انتقال Baseband و سرعت انتقال ۱۰ مگابیت در ثانیه است.

در طراحی جدید شبکه معمولاً از کابل های Twisted Pair استفاده می گردد. قیمت آن ارزان بوده و از نمونه های آن می توان به کابل تلفن اشاره کرد. این نوع کابل که از چهار جفت سیم بهم تابیده تشکیل می گردد،

خود به دو دسته تقسیم می شود:

UTP^۱: کابل ارزان قیمتی است که نصب آسانی دارد و برای شبکه های LAN سیم بسیار مناسبی است، همچنین نسبت به نوع دوم کم وزن تر و انعطاف پذیرتر است. مقدار سرعت دیتای عبوری از آن ۴ مگابیت در ثانیه تا ۱۰۰ مگابیت در ثانیه می باشد. این کابل می تواند تا مسافت حدوداً ۱۰۰ متر یا ۳۲۸ فوت را بدون افت سیگنال انتقال دهد. کابل مذکور نسبت به تداخل امواج الکترومغناطیس^۲ حساسیت بسیار بالایی دارد و در نتیجه در مکانهای دارای امواج الکترومغناطیس، امکان استفاده از آن وجود ندارد.

در سیم تلفن که خود نوعی از این کابل است از اتصال دهنده RJ۱۱ استفاده می شود، اما در کابل شبکه اتصال دهنده ای با شماره RJ۴۵ بکار می رود که دارای هشت مکان برای هشت رشته سیم است

کابل Utp و Stp

کابل UTP دارای پنج طبقه مختلف است (که البته امروزه CAT ۶ و CAT ۷ هم اضافه شده است: CAT ۱ یا نوع اول کابل UTP برای انتقال صدا بکار می رود، اما CAT ۲ تا CAT ۵ برای انتقال دیتا در شبکه های کامپیوتری مورد استفاده قرار می گیرند و سرعت انتقال دیتا در آنها به ترتیب عبارتست از: ۴ مگابیت در ثانیه، ۱۰ مگابیت در ثانیه، ۱۶ مگابیت در ثانیه و ۱۰۰ مگابیت در ثانیه.

برای شبکه های کوچک و خانگی استفاده از کابل CAT ۳ توصیه می شود.

^۱Unshielded Twisted Pair

^۲Magnetic InterferenceElectrical

STP: در این کابل سیم های انتقال دیتا مانند UTP هشت سیم و یا چهار جفت دوتایی هستند. باید دانست که تفاوت آن با UTP در این است که پوسته ای به دور آن پیچیده شده که از اثرگذاری امواج بر روی دیتا جلوگیری می کند. از لحاظ قیمت، این کابل از UTP گرانتر و از فیبر نوری ارزان تر است. مقدار مسافتی که کابل مذکور بدون افت سیگنال طی می کند برابر با ۵۰۰ متر معادل ۱۶۴۰ فوت است.

در شبکه هایی با توپولوژی اتوبوسی و حلقه ای از دو نوع اخیر استفاده می شود. گفته شد که در این نوع کابل، ۴ جفت سیم بهم تابیده بکار می رود که از دو جفت آن یکی برای فرستادن اطلاعات و دیگری برای دریافت اطلاعات عمل می کنند.

در شبکه هایی با نام اترنت سریع^۱ دو نوع کابل به چشم می خورد:

Base TX ۱۰۰: یعنی شبکه ای که در آن از کابل UTP نوع ۵ Cat استفاده شده و عملاً دو جفت سیم در انتقال دیتا دخالت دارند (دو جفت دیگر بیکار می ماند)، سرعت در آن ۱۰۰ مگابیت در ثانیه و روش انتقال Baseband است.

Base T۴ ۱۰۰: تنها تفاوت آن با نوع بالا این است که هر چهار جفت سیم در آن بکار گرفته می شوند.

کابل فیبر نوری کاملاً متفاوت از نوع Coaxial و Twisted Pair عمل می کند. به جای اینکه سیگنال الکتریکی در داخل سیم انتقال یابد، پالس هایی از نور در میان پلاستیک یا شیشه انتقال می یابد. این کابل در برابر امواج الکترومغناطیس کاملاً مقاوم می کند و نیز تأثیر افت سیگنال بر اثر انتقال در مسافت زیاد را بسیار کم در آن می توان دید. برخی از انواع کابل فیبر نوری می توانند تا ۱۲۰ کیلومتر انتقال داده انجام دهند. همچنین امکان به تله انداختن اطلاعات در کابل فیبر نوری بسیار کم است. کابل مذکور دو نوع را در بر می گیرد:

^۱Shielded Twisted Pair

^۲Fast Ethernet

1- Single Mode : که در این کابل دیتا با کمک لیزر انتقال می یابد و بصورت ۸/۳/۱۲۵ نشان داده می شود که در آن ۸/۳ میکرون قطر فیبر نوری و ۱۲۵ میکرون مجموع قطر فیبر نوری و محافظ آن می باشد. این نوع که خاصیت انعطاف پذیری کم و قیمت بالایی دارد برای شبکه های تلویزیونی و تلفنی استفاده می گردد.

۲- Multi Mode : که در آن دیتا بصورت پالس نوری انتقال می یابد و بصورت ۶۲/۵/۱۲۵ نشان داده می شود که در آن ۶۲/۵ میکرون قطر فیبر نوری و ۱۲۵ میکرون مجموع قطر فیبر نوری و محافظ آن می باشد. این نوع مسافت کوتاهتری را نسبت به Single Mode طی می کند و قابلیت انعطاف پذیری بیشتری دارد. قیمت آن نیز ارزان تر است و در شبکه های کامپیوتری استفاده می شود. بطور کلی کابل فیبر نوری نسبت به دو نوع Coaxial و Twisted pair قیمت بالایی دارد و نیز نصب آن نیاز به افراد ماهری دارد.

شبکه های Base FX ۱۰۰ شبکه هایی هستند که در آنها از فیبر نوری استفاده می شود، سرعت انتقال در آنها ۱۰۰ مگابیت در ثانیه بوده و روش انتقال Baseband می باشد. امروز، با پیشرفت تکنولوژی در شبکه های فیبر نوری می توان به سرعت ۱۰۰۰ مگابیت در ثانیه دست یافت.

درس ۲

Network Interface Adapters

کارت شبکه ، یکی از مهمترین عناصر سخت افزاری در زمان پیاده سازی یک شبکه کامپیوتری است. هر کامپیوتر موجود در شبکه (سرویس گیرندگان و سرویس دهندگان) ، نیازمند استفاده از یک کارت شبکه است . کارت شبکه ، ارتباط بین کامپیوتر و محیط انتقال (نظیر کابل های مسی و یا فیبر نوری) را فراهم می نماید .

اکثر مادربردهای جدیدی که از آنان در کامپیوترهای شخصی استفاده می گردد ، دارای یک اینترفیس شبکه ای onboard می باشند . کامپیوترهای قدیمی و یا کامپیوترهای جدیدی که دارای اینترفیس شبکه ای onboard نمی باشند ، در زمان اتصال به شبکه ، می بایست بر روی آنان یک کارت شبکه نصب گردد.

شکل زیر یک نمونه کارت شبکه را که دارای یک پورت RJ-۴۵ است را نشان می دهد .



کامپیوترها جهت اتصال به هم و استفاده از برنامه های هم و اشتراک برنامه ها از نظر سخت افزاری احتیاج به کارت شبکه یا LAN Card دارند. که بطور معمول در بازار دو نوع کارت معمول می باشد. یک قسم آنها کارتهای ۱۰ در ۱۰ بوده و قسم دیگر کارتهای ۱۰ در ۱۰۰ میباشند.

وظایف کارت شبکه

- برقراری ارتباط لازم بین کامپیوتر و محیط انتقال
- تبدیل داده : داده ها بر روی گذرگاه (bus) کامپیوتر به صورت موازی حرکت می نمایند . نحوه حرکت داده ها بر روی محیط انتقال شبکه به صورت سریال است . ترانسیور کارت شبکه (یک ارسال کننده و یا دریافت کننده) ، داده ها را از حالت موازی به سریال و بالعکس تبدیل می نماید .
- ارائه یک آدرس منحصر بفرد سخت افزاری : آدرس سخت افزاری (MAC) درون تراشه ROM موجود بر روی کارت شبکه نوشته می گردد . آدرس MAC در واقع یک زیر لایه از لایه Data Link مدل مرجع OSI می باشد . آدرس سخت افزاری موجود بر روی کارت شبکه ، یک آدرس منحصر بفرد را برای هر یک از کامپیوترهای موجود در شبکه ، مشخص می نماید . پروتکل هائی نظیر TCP/IP از یک سیستم آدرس دهی منطقی (آدرس IP) ، استفاده می نمایند . در چنین مواردی قبل از دریافت داده توسط کامپیوتر ، می بایست آدرس منطقی به آدرس سخت افزاری ترجمه گردد .

کارت های شبکه دارای وظایف گوناگونی هستند که برای فرستادن اطلاعات به شبکه و دریافت اطلاعات از آن حیاتی بشمار می روند. در اینجا وظایف یک کارت شبکه آورده شده است.

کپسوله کردن داده ها: کارت شبکه و درایور آن مجموعاً قبل از انتقال اطلاعات باید داده هایی را که توسط پروتکل لایه شبکه تولید شده است، در یک فریم کپسوله کنند. عمل دیگری که کارت شبکه در این زمینه انجام می دهد خواندن محتوای فریم های دریافت شده از شبکه و انتقال داده های آنها به پروتکل مناسب در لایه شبکه می باشد.

کد گذاری و کد گشایی سیگنال ها : کارت شبکه مسئول پیاده سازی روش کد گذاری لایه شبکه می باشد که در آن اطلاعات باینری تولید شده در لایه شبکه که حالا در فریم کپسوله شده است را به بارهای الکتریکی یعنی ولتاژهای الکتریکی، پالسهای نور یا هر نوع سیگنالی که

رسانه شبکه استفاده می کند تبدیل می کند. از طرف دیگر کارت شبکه سیگنال های دریافتی از شبکه را برای پروتکل های لایه بالاتر به اطلاعات باینری تبدیل می کند.

دریافت و انتقال اطلاعات : مهمترین وظیفه کارت شبکه تولید و ارسال سیگنال های مناسب روی شبکه و دریافت سیگنال های موجود در شبکه میباشد. ماهیت سیگنال ها به رسانه شبکه و پروتکل لایه پیوند-داده بستگی دارد. در Lan های متداول امروزی، هریک از کامپیوترهای موجود در شبکه همه بسته های فرستاده شده روی شبکه را دریافت می کنند و سپس کارت شبکه آدرس مقصد لایه پیوند-داده هر یک از آنها را بررسی میکند تا بسته هایی که به مقصد آن کامپیوتر تولید شده اند را برای پردازش به لایه بعدی از پشته پروتکل منتقل کند، در غیر اینصورت بسته دور انداخته میشود.

بافر کردن داده ها: کارتهای شبکه هر زمان فقط یک فریم داده را روی شبکه می فرستند یا از آن دریافت می کنند، بنابراین در خود بافری دارند که تا زمان کامل و آماده شدن یک فریم برای پردازش، داده هایی که از طرف کامپیوتر یا شبکه در یافت میکنند را ذخیره کنند. تبدیل سریال به موازی و برعکس: ارتباطات بین کامپیوتر و کارت شبکه بصورت موازی انجام می شود، مگر در کارتهای شبکه Usb که ارتباط با کامپیوتر در آنها بصورت سریال است. اما ارتباطات شبکه ای بصورت سریال انجام میشوند، بنابراین کارت شبکه مسئول تبدیل این دو نوع روش انتقال اطلاعات به همدیگر میباشد.

کنترل دستیابی رسانه : (mac) از وظایف دیگر کارت شبکه پیاده سازی مکانیزم mac می باشد که پروتکل لایه پیوند-داده از آن برای منظم کردن دستیابی به رسانه شبکه استفاده می کند. ماهیت مکانیزم Mac مورد استفاده به نوع پروتکل این لایه بستگی دارد.

روند نصب یک کارت شبکه، شامل قراردادن کارت داخل کامپیوتر، پیکربندی کارت برای استفاده از منابع سخت افزاری مناسب، و نهایتاً نصب درایور کارت می باشد که بسته به توانایی

ها و نوع کامپیوتر از نظر قدیمی یا جدید بودن این پروسه می تواند بسیار ساده و یا بسیار پر در دسر باشد.

توجه: قبل از لمس کردن قطعات داخلی کامپیوتر یا درآوردن کارت شبکه از بسته محافظ مخصوص آن، دست خود را با ورقه فلزیدور منبع تغذیه کامپیوتر تماس دهید یا اینکه از دستکش های مخصوص استفاده کنید تا بدلیل تخلیه الکترواستاتیکی به قطعات آسیبی وارد نشود.

درس ۳

Network Hubs

هاب و نحوه عملکرد آن

هاب از جمله تجهیزات سخت افزاری است که از آن به منظور برپاسازی شبکه های کامپیوتری استفاده می شود. گرچه در اکثر شبکه هائی که امروزه ایجاد می گردد از سوئیچ در مقابل هاب استفاده می گردد، ولی ما همچنان شاهد استفاده از این نوع تجهیزات سخت افزاری در شبکه های متعددی می باشیم. در این مطلب قصد داریم به بررسی هاب و نحوه عملکرد آن اشاره نمائیم. قبل از پرداختن به اصل موضوع لازم است در ابتدا با برخی تعاریف مهم که در ادامه بدفعات به آنان مراجعه خواهیم کرد، بیشتر آشنا شویم.

- Domain: تمامی کامپیوترهای عضو یک domain هر اتفاق و یا رویدادی را که در domain اتفاق می افتد، مشاهده و یا خواهند شنید.
- Collision Domain: در صورت بروز یک تصادم (Collision) بین دو کامپیوتر، سایر کامپیوترهای موجود در domain آن را شنیده و آگاهی لازم در خصوص آن چیزی که اتفاق افتاده است را پیدا خواهند کرد. کامپیوترهای فوق عضو یک Collision Domain یکسان می باشند. تمامی کامپیوترهایی که با استفاده از هاب به یکدیگر متصل می شوند، عضو یک Collision Domain یکسان خواهند بود (بر خلاف سوئیچ).
- Broadcast Domain: در این نوع domain، یک پیام broadcast (یک فریم و یا داده که برای تمامی کامپیوترها ارسال می گردد) برای هر یک از کامپیوترهای موجود در domain ارسال می گردد. هاب و سوئیچ با موضوع broadcast domain برخورد مناسبی نداشته (ایجاد حوزه های مجزاء) و در این رابطه به یک روتر نیاز خواهد بود.

به منظور برخورد مناسب (ایجاد حوزه های مجزاء) با collision domain ، broadcast domain و افزایش سرعت و کارایی یک شبکه از تجهیزات سخت افزاری متعددی استفاده می شود . سوئیچ ها collision domain مجزائی را ایجاد می نمایند ولی در خصوص broadcast domain بدین شکل رفتار نمی نمایند . روترها ، broadcast domain و collision domain مجزائی را ایجاد نموده و در مقابل هاب ، قادر به ایجاد broadcast domain و collision domain جداگانه نمی باشد . شکل زیر یک نمونه هاب هشت پورت را نشان می دهد .



منبع : سایت D-Link

آشنائی با نحوه عملکرد هاب :

هاب ، یکی از تجهیزات متداول در شبکه های کامپیوتری و ارزاترین روش اتصال دو و یا چندین کامپیوتر به یکدیگر است . هاب در اولین لایه مدل مرجع OSI فعالیت می نماید . آنان فریم های داده را نمی خوانند (کاری که سوئیچ و یا روتر انجام می دهند) و صرفاً این اطمینان را ایجاد می نمایند که فریم های داده بر روی هر یک از پورت ها ، تکرار خواهد شد .

گره هائی که یک اترنت و یا FastEthernet را با استفاده از قوانین CSMA/CD به اشتراک می گذارند ، عضوی یک Collision Domain مشابه می باشند . این بدان معنی است که تمامی گره های متصل شده به هاب بخشی از Collision domain مشابه بوده و زمانی که یک collision اتفاق می افتد ، سایر گره های موجود در domain نیز آن را شنیده و از آن متاثر خواهند شد .

کامپیوترها و یا گره های متصل شده به هاب از کابل های UTP¹ استفاده می نمایند . صرفاً یک گره می تواند به هر پورت هاب متصل گردد . مثلاً با استفاده از یک هاب هشت پورت ، امکان

¹Unshielded Twisted Pair

اتصال هشت کامپیوتر وجود خواهد داشت. زمانی که هاب ها به متداولی امروز نبودند و قیمت آنان نیز گران بود، در اکثر شبکه های نصب شده در ادارات و یا منازل از کابل های کواکسیال، استفاده می گردید.

نحوه کار هاب بسیار ساده است. زمانی که یکی از کامپیوترهای متصل شده به هاب اقدام به ارسال داده ئی می نماید، سایر پورت های هاب نیز آن را دریافت خواهند کرد (داده ارسالی تکرار و برای سایر پورت های هاب نیز فرستاده می شود). شکل زیر نحوه عملکرد هاب را نشان می دهد.



همانگونه که در شکل فوق مشاهده می نمائید، گره یک داده ئی را برای گره شش ارسال می نماید ولی تمامی گره های دیگر نیز داده را دریافت خواهند کرد. در ادامه، بررسی لازم در خصوص داده ارسالی توسط هر یک از گره ها انجام و در صورتی که تشخیص داده شود که داده ارسالی متعلق به آنان نیست، آن را نادیده خواهند گرفت. عملیات فوق از طریق کارت شبکه موجود بر روی کامپیوتر که آدرس MAC مقصد فریم ارسالی را بررسی می نماید، انجام می شود. کارت شبکه بررسی لازم را انجام و در صورت عدم مطابقت آدرس MAC موجود در فریم، با آدرس MAC کارت شبکه، فریم ارسالی دور انداخته می گردد.

اکثر هاب ها دارای یک پورت خاص می باشند که می تواند به صورت یک پورت معمولی و یا یک پورت uplink رفتار نماید. با استفاده از یک پورت uplink می توان یک هاب دیگر را به هاب موجود، متصل نمود. بدین ترتیب تعداد پورت ها افزایش یافته و امکان اتصال تعداد بیشتری کامپیوتر به شبکه فراهم می گردد. روش فوق گزینه ای ارزان قیمت به منظور افزایش تعداد گره ها در یک شبکه است ولی با انجام این کار شبکه شلوغ تر شده و همواره بر روی آن حجم بالائی داده غیر ضروری در حال جابجائی است. تمامی گره ها، عضو یک Broadcast domain و

collision domain یکسانی می باشند ، بنابراین تمامی آنان هر نوع collision و یا Broadcast را که اتفاق خواهد افتاد ، می شنوند .

در اکثر هاب ها از یک LED به منظور نشان دادن فعال بودن ارتباط برقرار شده بین هاب و گره و از LED دیگر به منظور نشان دادن بروز یک collision ، استفاده می گردد . (دو LED مجزاء) . در برخی از هاب ها دو LED مربوط به فعال بودن لینک ارتباطی بین هاب و گره و فعالیت پورت با یکدیگر ترکیب و زمانی که پورت در حال فعالیت است ، LED مربوطه چشمک زن شده و زمانی که فعالیت انجام نمی شود، LED فوق به صورت پیوسته روشن خواهد بود .



LED مربوط به Collision موجود بر روی هاب ها زمانی روشن می گردد که یک collision بوجود آید . Collision زمانی بوجود می آید که دو کامپیوتر و یا گره سعی نمایند در یک لحظه بر روی شبکه صحبت نمایند . پس از بروز یک Collision ، فریم های مربوط به هر یک از گره ها با یکدیگر برخورد نموده و خراب می گردند . هاب به منظور تشخیص این نوع تصادم ها به اندازه کافی هوشمند بوده و برای مدت زمان کوتاهی چراغ مربوط به collision روشن می گردد . (یک دهم ثانیه به ازای هر تصادم) .

تعداد اندکی از هاب ها دارای یک اتصال خاص از نوع BNC بوده که می توان از آن به منظور اتصال یک کابل کواکسیال ، استفاده نمود . پس از اتصال فوق ، LED مربوط به اتصال BNC روی هاب روشن می گردد.

فصل ۳

Network Connections

با استفاده از هاب، کابل، و برخی از آداپتورهای رابط شبکه شما می توانید گروهی از کامپیوترها را در یک شبکه محلی (LAN) به یکدیگر وصل کنید اما در شبکه های بزرگتر، انواع دیگری از دستگاه های سخت افزاری مورد نیاز است. هنگامی که یک شبکه فراتر از یک نقطه خاص رشد می کند، ترافیک به وجود می آید. شما باید از دستگاههایی استفاده کنید که این مشکلات را برای شما حل کنند. در این فصل به بررسی برخی از اجزای پیچیده تر برای اتصالات وسیعتر میپردازیم. با استفاده از این ابزار، شما می توانید اندازه شبکه را بدون کاهش کارایی آن را افزایش دهید، حتی زمانی که ترافیک شبکه بالا رود.

درس ۱

Switching

سوئیچ برای اتصال دستگاههای مختلف از قبیل رایانه، مسیریاب، چاپگرهای تحت شبکه، دوربینهای مدار بسته و در شبکه های کابلی مورد استفاده واقع می شود.

در وجه ظاهری سوئیچ همانند جعبه ایست متشکل از چندین درگاه اترنت که از این لحاظ شبیه هاب (Hub) می باشد، با وجود آنکه هر دو اینها وظیفه برقراری ارتباط بین دستگاههای مختلف را بر عهده دارند، تفاوت از آنجا آغاز می شود که هاب بسته های ارسالی از طرف یک دستگاه را به همه درگاه های خود ارسال می کند و کلیه دستگاه های دیگر علاوه بر دستگاه مقصد این بسته ها را دریافت می کنند در حالیکه در سوئیچ ارتباطی مستقیم بین درگاه دستگاه مبدا با درگاه دستگاه مقصد برقرار شده و بسته ها مستقماً فقط برای آن ارسال می شود.

این خصوصیت از آنجا می آید که سوئیچ می تواند بسته ها را پردازش کند، در سوئیچ های معمولی که به سوئیچ لایه دوم معروفند این پردازش تا لایه دوم مدل OSI پیش می رود و نتیجه این پردازش جدولی است که در سوئیچ با خواندن آدرس سخت افزاری (MAC) فرستنده بسته و ثبت درگاه ورودی تشکیل می شود.

سوئیچ با رجوع به این جدول عملیات آدرس دهی بسته ها در لایه دوم را انجام می دهد، بدین معنا که این جدول مشخص می کند بسته ورودی می بایست فقط برای کدام درگاه ارسال شود.

در شبکه های بزرگ Switchها جدول های خود را به اشتراک می گذارند تا هر کدام بدانند چه دستگاهی به کدام سوئیچ متصل است و با این کار ترافیک کمتری در شبکه ایجاد کنند.

سوئیچ بطور معمول در لایه دوم مدل OSI کار می کند ولی سوئیچ هایی با قابلیت کارکرد در لایه های مختلف حتی لایه هفتم هم وجود دارد. پرکاربردترین سوئیچ در بین لایه های مختلف بجز لایه دوم می توان به سوئیچ لایه سه اشاره کرد که در بسیاری موارد جایگزین مناسبی برای روتر می باشند. از سوئیچ می توان در یک شبکه خانگی کوچک تا در شبکه های بزرگ با Backbone های چند گیگابیتی استفاده کرد.

برخی مزیت های و قابلیت های سوئیچ :

- امکان برقراری ارتباط بین ده ها و گاهی صدها دستگاه را به طور مستقیم و هوشمند به ما می دهد.
- امکان برقراری ارتباط با سرعت بسیار بالا را فراهم می کند.
- امکان نظارت و مدیریت بر عملکرد کاربران را فراهم می کند.
- امکان کنترل پهنای باند مصرفی کاربران را فراهم می کند.
- امکان تفکیک شبکه به بخش های کوچکتر و مشخص کردن نحوه دسترسی افراد به قسمت های مختلف را فراهم می کند.
- و ده ها مزیت دیگر...

در یک شبکه مبتنی بر سوئیچ ، برای هر گره یک سگمنت اختصاصی ایجاد خواهد شد. سگمنت های فوق به یک سوئیچ متصل خواهند شد. در حقیقت سوئیچ امکان حمایت از چندین (در برخی حالات صدها) سگمنت اختصاصی را دارا است . با توجه به اینکه تنها دستگاه های موجود در هر سگمنت سوئیچ و گره می باشند ، سوئیچ قادر به انتخاب اطلاعات ، قبل از رسیدن به سایر گره ها خواهد بود. در ادامه سوئیچ، فریم های اطلاعاتی را به سگمنت مورد نظر هدایت خواهد کرد. با توجه به اینکه هر سگمنت دارای صرفاً یک گره می باشد ، اطلاعات مورد نظر به مقصد مورد نظر ارسال خواهند شد. بدین ترتیب در شبکه های مبتنی بر سوئیچ امکان چندین مبادله اطلاعاتی بصورت همزمان وجود خواهد داشت .

با استفاده از سوئیچ ، شبکه های اترنت بصورت full-duplex خواهند بود. قبل از مطرح شدن سوئیچ ، اترنت بصورت half-duplex بود. در چنین حالتی داده ها در هر لحظه امکان ارسال در یک جهت را دارا می باشند . در یک شبکه مبتنی بر سوئیچ ، هر گره صرفاً با سوئیچ ارتباط برقرار می نماید (گره ها مستقیماً با یکدیگر ارتباط برقرار نمی نمایند) . در چنین حالتی اطلاعات از گره به سوئیچ و از سوئیچ به گره مقصد بصورت همزمان منتقل می گردند .

در شبکه های مبتنی بر سوئیچ امکان استفاده از کابل های بهم تابیده و یا فیبر نوری وجود خواهد داشت . هر یک از کابل های فوق دارای کانکتورهای مربوط به خود برای ارسال و دریافت اطلاعات می باشند. با استفاده از سوئیچ ، شبکه ای عاری از تصادم اطلاعاتی بوجود خواهد آمد. انتقال دو سویه اطلاعات در شبکه های مبتنی بر سوئیچ ، سرعت ارسال و دریافت اطلاعات افزایش می یابد .

اکثر شبکه های مبتنی بر سوئیچ بدلیل قیمت بالای سوئیچ ، صرفاً از سوئیچ به تنهایی استفاده نمی نمایند. در این نوع شبکه ها از ترکیب هاب و سوئیچ استفاده می گردد. مثلاً یک سازمان می تواند از چندین هاب بمنظور اتصال کامپیوترهای موجود در هر یک از دپارتمانهای خود استفاده و در ادامه با استفاده از یک سوئیچ تمام هاب ها(مربوط به هر یک از دپارتمانها) به یکدیگر متصل می گردد .

تکنولوژی سوئیچ ها :

سوئیچ ها دارای پتانسیل های لازم بمنظور تغییر روش ارتباط هر یک از گره ها با یکدیگر می باشند. تفاوت سوئیچ با روتر چیست ؟ سوئیچ ها معمولاً در لایه دوم (Data layer) مدل OSI فعالیت می نمایند. در لایه فوق امکان استفاده از آدرس های (MAC آدرس ها ی فیزیکی) وجود دارد. روتر در لایه سوم (Network) مدل OSI فعالیت می نمایند. در لایه فوق از آدرس های IP و IPX یا Appeltalk استفاده می شود. (آدرس های منطقی) . الگوریتم

استفاده شده توسط سوئیچ بمنظور اتخاذ تصمیم در رابطه با مقصد یک بسته اطلاعاتی با الگوریتم استفاده شده توسط روتر ، متفاوت است .

یکی از موارد اختلاف الگوریتم های سوئیچ و هاب ، نحوه برخورد آنان با Broadcast است . مفهوم بسته های اطلاعاتی از نوع Broadcast در تمام شبکه ها مشابه می باشد. در چنین مواردی ، دستگاهی نیاز به ارسال اطلاعات داشته ولی نمی داند که اطلاعات را برای چه کسی می بایست ارسال نماید. بدلیل عدم آگاهی و دانش نسبت به هویت دریافت کننده اطلاعات ، دستگاه مورد نظر اقدام به ارسال اطلاعات بصورت broadcast می نماید. مثلا" هر زمان که کامپیوتر جدید ویا یکدستگاه به شبکه وارد می شود ، یک بسته اطلاعاتی از نوع Broadcast برای معرفی و حضور خود در شبکه ارسال می دارد. سایر گره ها قادر به افزودن کامپیوتر مورد نظر در لیست خود و برقراری ارتباط با آن خواهند بود. بنابراین بسته های اطلاعاتی از نوع Broadcast در مواردی که یک دستگاه نیاز به معرفی خود به سایر بخش های شبکه را داشته و یا نسبت به هویت دریافت کننده اطلاعات شناخت لازم وجود نداشته باشند ، استفاده می گردند .

هاب و یا سوئیچ ها قادر به ارسال بسته ای اطلاعاتی از نوع Broadcast برای سایر سگمنت های موجود در حوزه Broadcast می باشند. روتر عملیات فوق را انجام نمی دهد. در صورتیکه آدرس یکدستگاه مشخص نگردد ، روتر قادر به مسیریابی بسته اطلاعاتی مورد نظر نخواهد بود. ویژگی فوق در مواردیکه قصد جداسازی شبکه ها از یکدیگر مد نظر باشد ، بسیار ایده آل خواهد بود .ولی زمانیکه هدف مبادله اطلاعاتی بین بخش های متفاوت یک شبکه باشد ، مطلوب بنظر نمی آید. سوئیچ ها با هدف برخورد با مشکل فوق عرضه شده اند .

سوئیچ های LAN بر اساس تکنولوژی packet-switching فعالیت می نمایند. سوئیچ یک ارتباط بین دو سگمنت ایجاد می نماید. بسته های اطلاعاتی اولیه در یک محل موقت (بافر) ذخیره می گردند ، آدرس فیزیکی (MAC) موجود در هدر خوانده شده و در ادامه با لیستی از آدرس های موجود در جدول Lookup (جستجو) مقایسه می گردد. در شبکه های LAN مبتنی

بر اترنت ، هر فریم اترنت شامل یک بسته اطلاعاتی خاص است . بسته اطلاعاتی فوق شامل یک عنوان (هدر) خاص و شامل اطلاعات مربوط به آدرس فرستنده و گیرنده بسته اطلاعاتی است.

سوئیچ های مبتنی بر بسته های اطلاعاتی بمنظور مسیریابی ترافیک موجود در شبکه از سه روش زیر استفاده می نمایند .

Cut-Through

Store-and-forward

Fragment-free

سوئیچ های Cut-through ، بلافاصله پس از تشخیص بسته اطلاعاتی توسط سوئیچ ، آدرس MAC خوانده می شود. پس از ذخیره سازی شش بایت اطلاعات که شامل آدرس می باشند ، بلافاصله عملیات ارسال بسته های اطلاعاتی به گره مقصد آغاز می گردد. (همزمان با دریافت سایر بسته های اطلاعاتی توسط سوئیچ) . با توجه به عدم وجود کنترل های لازم در صورت بروز خطا در روش فوق ، سوئیچ های زیادی از روش فوق استفاده نمی نمایند .

سوئیچ های store-and-forward ، تمام بسته اطلاعاتی را در بافر مربوطه ذخیره و عملیات مربوط به بررسی خطا (CRC) و سایر مسائل مربوطه را قبل از ارسال اطلاعات انجام خواهند داد. در صورتیکه بسته اطلاعاتی دارای خطا باشد ، بسته اطلاعاتی دور انداخته خواهد شد. در غیر اینصورت ، سوئیچ با استفاده از آدرس MAC ، بسته اطلاعاتی را برای گره مقصد ارسال می نماید. اغلب سوئیچ ها از ترکیب دو روش گفته شده استفاده می نمایند. در این نوع سوئیچ ها از روش cut-through استفاده شده و بمحض بروز خطا از روش-store-and-forward استفاده می نمایند .

یکی دیگر از روش های مسیریابی ترافیک در سوئیچ ها که کمتر استفاده می گردد ، -fragment free است . روش فوق مشابه cut-through بوده با این تفاوت که قبل از ارسال بسته اطلاعاتی ۶۴ بایت آن ذخیره می گردد .

سوئیچ های LAN دارای مدل های متفاوت از نقطه نظر طراحی فیزیکی می باشند. سه مدل رایج در حال حاضر بشرح زیر می باشند :

Shared memory - این نوع از سوئیچ ها تمام بسته های اطلاعاتی اولیه در بافر مربوط به خود را ذخیره می نمایند. بافر فوق بصورت مشترک توسط تمام پورت های سوئیچ (اتصالات ورودی و خروجی) استفاده می گردد. در ادامه اطلاعات مورد نظر بکمک پورت مربوطه برای گره مقصد ارسال خواهند شد .

Matrix- این نوع از سوئیچ ها دارای یک شبکه (تور) داخلی ماتریس مانند بوده که پورت های ورودی و خروجی همدیگر را قطع می نمایند. زمانیکه یک بسته اطلاعاتی بر روی پورت ورودی تشخیص داده شد ، آدرس MAC آن با جدول lookup مقایسه تا پورت مورد نظر خروجی آن مشخص گردد. در ادامه سوئیچ یک ارتباط را از طریق شبکه و در محلی که پورت ها همدیگر را قطع می کنند ، برقرار می گردد .

Bus Architecture - در این نوع از سوئیچ ها بجای استفاده از یک شبکه (تور) ، از یک مسیر انتقال داخلی (Bus) استفاده و مسیر فوق با استفاده از TDMA توسط تمام پورت ها به اشتراک گذاشته می شود. سوئیچ های فوق برای هر یک از پورت ها دارای یک حافظه اختصاصی می باشند .

Transparent Bridging

اکثر سوئیچ های LAN مبتنی بر اتترنت از سیستم ی با نام transparent bridging برای ایجاد جداول آدرس lookup استفاده می نمایند. تکنولوژی فوق امکان یادگیری هر چیزی در رابطه با

محل گره های موجود در شبکه ، بدون حمایت مدیریت شبکه را فراهم می نماید. تکنولوژی فوق داری پنج بخش متفاوت است:

Learning

Flooding

Filtering

Forwarding

Aging

نحوه عملکرد تکنولوژی فوق بشرح زیر است:

-سوئیچ به شبکه اضافه شده و تمام سگمنت ها به پورت های سوئیچ متصل خواهند شد .
-گره A بر روی اولین سگمنت (سگمنت A) ، اطلاعاتی را برای کامپیوتر دیگر (گره B) در سگمنت دیگر (سگمنت C) ارسال می دارد .

-سوئیچ اولین بسته اطلاعاتی را از گره A دریافت می نماید. آدرس MAC آن خوانده شده و آن را در جدول Lookup سگمنت A ذخیره می نماید. بدین ترتیب سوئیچ از نحوه یافتن گره A آگاهی پیدا کرده و اگر در آینده گره ای قصد ارسال اطلاعات برای گره A را داشته باشد ، سوئیچ در رابطه با آدرس آن مشکلی نخواهد داشت . فرآیند فوق را Learning می گویند .

-با توجه به اینکه سوئیچ دانشی نسبت به محل گره B ندارد ، یک بسته اطلاعاتی را برای تمام سگمنت های موجود در شبکه (بجز سگمنت A که اخیراً یکی از گره های موجود در آن اقدام به ارسال اطلاعات نموده است .) فرآیند ارسال یک بسته اطلاعاتی توسط سوئیچ ، بمنظور یافتن یک گره خاص برای تمام سگمنت ها ، Flooding نامیده می شود .

-گره B بسته اطلاعاتی را دریافت و یک بسته اطلاعاتی را بعنوان Acknowledgement برای گره A ارسال خواهد کرد .

-بسته اطلاعاتی ارسالی توسط گره B به سوئیچ می رسد. در این زمان ، سوئیچ قادر به ذخیره کردن آدرس MAC گره B در جدول Lookup سگمنت C می باشد. با توجه به اینکه سوئیچ از آدرس گره A آگاهی دارد ، بسته اطلاعاتی را مستقیماً برای آن ارسال خواهد کرد. گره A در سگمنتی متفاوت نسبت به گره B قرار دارد ، بنابراین سوئیچ می بایست بمنظور ارسال بسته اطلاعاتی دو سگمنت را به یکدیگر متصل نماید. فرآیند فوق Forwarding نامیده می شود .

-در ادامه بسته اطلاعاتی بعدی از گره A بمنظور ارسال برای گره B به سوئیچ می رسد ، با توجه به اینکه سوئیچ از آدرس گره B آگاهی دارد ، بسته اطلاعاتی فوق مستقیماً برای گره B ارسال خواهد شد .

-گره C اطلاعاتی را از طریق سوئیچ برای گره A ارسال می دارد. سوئیچ آدرس MAC گره C را در جدول Lookup سگمنت A ذخیره می نماید ، سوئیچ آدرس گره A را دانسته و مشخص می گردد که دو گره A و C در یک سگمنت قرار دارند. بنابراین نیازی به ارتباط سگمنت A با سگمنت دیگر بمنظور ارسال اطلاعات گره C نخواهد بود. بدین ترتیب سوئیچ از حرکت بسته های اطلاعاتی بین گره های موجود در یک سگمنت ممانعت می نماید. فرآیند فوق را Filtering می گویند .

Learning - و Flooding ادامه یافته و بموازات آن سوئیچ ، آدرس های MAC مربوط به گره ها را در جداول Lookup ذخیره می نماید. اکثر سوئیچ ها دارای حافظه کافی بمنظور ذخیره سازی جداول Lookup می باشند. بمنظور بهینه سازی حافظه فوق ، اطلاعات قدیمی تر از جداول فوق حذف تا فرآیند جستجو و یافتن آدرس ها در یک زمان معقول و سریعتر انجام پذیرد. بدین منظور سوئیچ ها از روشی با نام aging استفاده می نمایند. زمانیکه یک Entry برای یک گره در جدول Lookup اضافه می گردد ، به آن یک زمان خاص نسبت داده می شود.

هر زمان که بسته ای اطلاعاتی از طریق یک گره دریافت می گردد ، زمان مورد نظر بهنگام می گردد. سوئیچ دارای یک تایمر قابل پیکربندی بوده که باعث می شود، Entry های موجود در جدول Lookup که مدت زمان خاصی از آنها استفاده نشده و یا به آنها مراجعه ای نشده است ، حذف گردند . با حذف Entry های غیرضروری ، حافظه قابل استفاده برای سایر Entry ها بیشتر می گردد .

در مثال فوق ، دو گره سگمنت A را به اشتراک گذاشته و سگمنت های A و D بصورت مستقل می باشند. در شبکه های ایده آل مبتنی بر سوئیچ ، هر گره دارای سگمنت اختصاصی مربوط بخود است . بدین ترتیب امکان تصادم حذف و نیازی به عملیات Filtering نخواهد بود .

فراوانی و آشفته‌گی انتشار :

در شبکه های با توپولوژی ستاره (Star) و یا ترکیب Bus و Star یکی از عناصر اصلی شبکه که می تواند باعث از کار افتادن شبکه گردد ، هاب و یا سوئیچ است .

Spanning tress:

بمنظوری پیشگیری از مسئله " آشفته‌گی انتشار" و سایر اثرات جانبی در رابطه با Looping شرکت DEC پروتکلی با نام STP¹ را ایجاد نموده است . پروتکل فوق با مشخصه ۸۰۲/۱ توسط موسسه IEEE استاندارد شده است Spanning tree از الگوریتم STA² استفاده می نماید. الگوریتم فوق بررسی خواهد کرد آیا یک سوئیچ دارای بیش از یک مسیر برای دستیابی به یک گره خاص است . در صورت وجود مسیرهای متعدد ، بهترین مسیر نسبت به سایر مسیرها کدام است ؟ نحوه عملیات STP بشرح زیر است:

¹Spanning-tree Protocol

²Spanning-tree algorithm

به هر سوئیچ ، مجموعه ای از مشخصه ها (ID) نسبت داده می شود. یکی از مشخصه ها برای سوئیچ و سایر مشخصه ها برای هر یک از پورت ها استفاده می گردد. مشخصه سوئیچ ، BID^۱ نامیده شده و دارای هشت بایت است . دو بایت بمنظور مشخص نمودن اولویت و شش بایت برای مشخص کردن آدرس MAC استفاده می گردد. مشخصه پورت ها ، شانزده بیتی است . شش بیت بمنظور تنظیمات مربوط به اولویت و ده بیت دیگر برای اختصاص یک شماره برای پورت مورد نظر است .

برای هر مسیر یک Path Cost محاسبه می گردد. نحوه محاسبه پارامتر فوق بر اساس استانداردهای ارائه شده توسط موسسه IEEE است . بمنظور محاسبه مقادیر فوق ، ۱/۰۰۰ مگابیت در ثانیه (یک گیگابیت در ثانیه) را بر پهنای باند سگمنت متصل شده به پورت ، تقسیم می نمایند. بنابراین یک اتصال ۱۰ مگابیت در ثانیه ، دارای Cost به میزان ۱۰۰ است (۱/۰۰۰ تقسیم بر ۱۰) . بمنظور هماهنگ شدن با افزایش سرعت شبکه های کامپیوتری استاندارد Cost نیز اصلاح می گردد. جدول زیر مقادیر جدید STP Cost را نشان می دهد. (مقدار Path cost می تواند یک مقدار دلخواه بوده که توسط مدیریت شبکه تعریف و مشخص می گردد).

هر سوئیچ فرآیندی را بمنظور انتخاب مسیرهای شبکه که می بایست توسط هر یک از سگمنت ها استفاده گردد ، آغاز می نمایند. اطلاعات فوق توسط سایر سوئیچ ها و با استفاده از یک پروتکل خاص با نام BPUD^۲ به اشتراک گذاشته می شود. ساختار یک BPUD بشرح زیر است:

Root BID: پارامتر فوق BID مربوط به Root Bridge جاری را مشخص می کند .

Path Cost to Bridge: مسافت root bridge را مشخص می نماید. مثلا "در صورتیکه داده از طریق طی نمودن سه سگمنت با سرعتی معادل ۱۰۰ مگابیت در ثانیه برای رسیدن به Root

^۱Bridge ID

^۲Bridge protocol data units

bridge باشد ، مقدار cost بصورت $(19+19+0=38)$ بدست می آید . سگمندی که به Root Bridge متصل است دارای Cost معادل صفر است .

Sender BID: مشخصه BID سوئیچ ارسال کننده BPDU را مشخص می کند .

Port ID: پورت ارسال کننده BPDU مربوط به سوئیچ را مشخص می نماید .

تمام سوئیچ ها بمنظور مشخص نمودن بهترین مسیر بین سگمنت های متفاوت ، بصورت پیوسته برای یکدیگر BPDU ارسال می نمایند . زمانیکه سوئیچی یک BPDU را (از سوئیچ دیگر) دریافت می دارد که مناسبتر از آن چیزی است که خود برای ارسال اطلاعات در همان سگمنت استفاده کرده است ، BPDU خود را متوقف (به سایر سگمنت ها ارسال نمی نماید) و از BPDU سایر سوئیچ ها بمنظور دستیابی به سگمنت ها استفاده خواهد کرد .

یک- Root bridge بر اساس فرآیندهای BPDU بین سوئیچ ها ، انتخاب می گردد . در ابتدا هر سوئیچ خود را بعنوان Root در نظر می گیرد . زمانیکه یک سوئیچ برای اولین بار به شبکه متصل می گردد ، یک BPDU را به همراه BID خود که بعنوان Root BID است ، ارسال می نماید . زمانیکه سایر سوئیچ ها BPDU را دریافت می دارند ، آن را با BID مربوطه ای که بعنوان Root BID ذخیره نموده اند ، مقایسه می نمایند . در صورتیکه Root BID جدید دارای یک مقدار کمتر باشد ، تمام سوئیچ ها آن را با آنچیزی که قبلاً " ذخیره کرده اند ، جایگزین می نمایند . در صورتیکه Root BID ذخیره شده دارای مقدار کمتری باشد ، یک BPDU برای سوئیچ جدید به همراه BID مربوط به Root BID ارسال می گردد . زمانیکه سوئیچ جدید BPDU را دریافت می دارد ، از Root بودن خود صرفنظر و مقدار ارسالی را بعنوان Root BID در جدول مربوط به خود ذخیره خواهد کرد .

- با توجه به محل Root Bridge ، سایر سوئیچ ها مشخص خواهند کرد که کدامیک از پورت های آنها دارای کوتاهترین مسیر به Root Bridge است . پورت های فوق ، Root Ports نامیده شده و هر سوئیچ می بایست دارای یک نمونه باشد .

- سوئیچ ها مشخص خواهند کرد که چه کسی دارای پورت های designated است . پورت فوق ، اتصالی است که توسط آن بسته های اطلاعاتی برای یک سگمنت خاص ارسال و یا از آن دریافت خواهند شد. با داشتن صرفاً یک نمونه از پورت های فوق ، تمام مشکلات مربوط به Looping برطرف خواهد شد .

- پورت های designated بر اساس کوتاه ترین مسیر بین یک سگمنت تا root bridge انتخاب می گردند. با توجه به اینکه Root bridge دارای مقدار صفر برای path cost است ، هر پورت آن بمنزله یک پورت designated است . (مشروط به اتصال پورت مورد نظر به سگمنت) برای سایر سوئیچ ها ، Path Cost برای یک سگمنت بررسی می گردد. در صورتیکه پورتی دارای پایین ترین path cost باشد ، پورت فوق بمنزله پورت designated سگمنت مورد نظر خواهد بود. در صورتیکه دو و یا بیش از دو پورت دارای مقادیر یکسان path cost باشند ، سوئیچ با مقدار کمتر BID انتخاب می گردد .

- پس از انتخاب پورت designated برای سگمنت شبکه ، سایر پورت های متصل شده به سگمنت مورد نظر بعنوان non-designated port در نظر گرفته خواهند شد. بنابراین با استفاده از پورت های designated می توان به یک سگمنت متصل گردید .

هر سوئیچ دارای جدول BPDU مربوط به خود بوده که بصورت خودکار بهنگام خواهد شد. بدین ترتیب شبکه بصورت یک spanning tree بوده که root bridge که بمنزله ریشه و سایر سوئیچ ها بمنزله برگ خواهند بود. هر سوئیچ با استفاده از Root Ports قادر به ارتباط با root bridge بوده و با استفاده از پورت های designated قادر به ارتباط با هر سگمنت خواهد بود .

روترها و سوئیچینگ لایه سوم

همانگونه که قبلا "اشاره گردید ، اکثر سوئیچ ها در لایه دوم مدل OSI فعالیت می نمایند اخیراً" برخی از تولیدکنندگان سوئیچ، مدلی را عرضه نموده اند که قادر به فعالیت در لایه سوم مدل OSI است (Network Layer) . این نوع سوئیچ ها دارای شباهت زیادی با روتر می باشند .

زمانیکه روتر یک بسته اطلاعاتی را دریافت می نماید ، در لایه سوم بدنبال آدرس های مبداء و مقصد گشته تا مسیر مربوط به بسته اطلاعاتی را مشخص نماید. سوئیچ های استاندارد از آدرس های MAC بمنظور مشخص کردن آدرس مبداء و مقصد استفاده می نمایند. (از طریق لایه دوم) مهمترین تفاوت بین یک روتر و یک سوئیچ لایه سوم ، استفاده سوئیچ های لایه سوم از سخت افزارهای بهینه بمنظور ارسال داده با سرعت مطلوب نظیر سوئیچ های لایه دوم است. نحوه تصمیم گیری آنها در رابطه با مسیریابی بسته های اطلاعاتی مشابه روتر است . در یک محیط شبکه ای LAN ، سوئیچ های لایه سوم معمولاً" دارای سرعتی بیشتر از روتر می باشند. علت این امر استفاده از سخت افزارهای سوئیچینگ در این نوع سوئیچ ها است . اغلب سوئیچ های لایه سوم شرکت سیسکو، بمنزله روترهایی می باشند که بمراتب از روترها سریعتر بوده (با توجه به استفاده از سخت افزارهای اختصاصی سوئیچینگ) و دارای قیمت ارزانهتری نسبت به روتر می باشند. نحوه Pattern matching و caching در سوئیچ های لایه سوم مشابه یک روتر است . در هر دو دستگاه از یک پروتکل روتینگ و جدول روتینگ، بمنظور مشخص نمودن بهترین مسیر استفاده می گردد. سوئیچ های لایه سوم قادر به برنامه ریزی مجدد سخت افزار بصورت پویا و با استفاده از اطلاعات روتینگ لایه سوم می باشند و همین امر باعث سرعت بالای پردازش بسته های اطلاعاتی می گردد. سوئیچ های لایه سوم ، از اطلاعات دریافت شده توسط پروتکل روتینگ بمنظور بهنگام سازی جداول مربوط به Caching استفاده می نمایند .

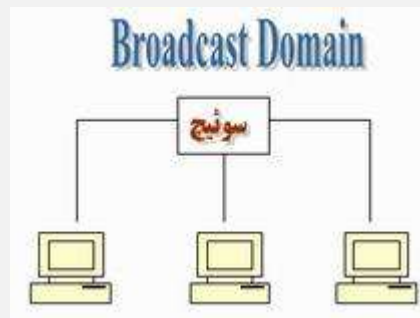
همانگونه که ملاحظه گردید ، در طراحی سوئیچ های LAN از تکنولوژی های متفاوتی استفاده می گردد. نوع سوئیچ استفاده شده ، تاثیر مستقیم بر سرعت و کیفیت یک شبکه را بدنبال خواهد داشت.

VLAN چیست ؟

VLAN^۱، یکی از جدیدترین و جالبترین تکنولوژی های شبکه است که اخیراً^۲ مورد توجه بیشتری قرار گرفته است . رشد بدون وقفه شبکه های LAN و ضرورت کاهش هزینه ها برای تجهیزات گرانبه بدون از دست دادن کارآئی و امنیت ، اهمیت و ضرورت توجه بیشتر به VLAN را مضاعف نموده است .

وضعیت شبکه های فعلی :

تقریباً^۳ در اکثر شبکه ها امروزی از یک (و یا چندین) سوئیچ که تمامی گره های شبکه به آن متصل می گردند ، استفاده می شود . سوئیچ ها روشی مطمئن و سریع به منظور مبادله اطلاعات بین گره ها در یک شبکه را فراهم می نمایند. با این که سوئیچ ها برای انواع شبکه ها ، گزینه ای مناسب می باشند ، ولی همزمان با رشد شبکه و افزایش تعداد ایستگاهها و سرویس دهندگان ، شاهد بروز مسائل خاصی خواهیم بود . سوئیچ ها ، دستگاه های لایه دوم (مدل مرجع OSI) می باشند که یک شبکه Flat را ایجاد می نمایند .



^۱VirtualLocal Area Networks

همانگونه که در شکل فوق مشاهده می نمائید ، به یک سوئیچ ، سه ایستگاه متصل شده است . ایستگاههای فوق قادر به ارتباط با یکدیگر بوده و هر یک به عنوان عضوی از یک Broadcastdomain مشابه می باشند. بدین ترتیب ، در صورتی که ایستگاهی یک پیام broadcast را ارسال نماید ، سایر ایستگاههای متصل شده به سوئیچ نیز آن را دریافت خواهند داشت. در یک شبکه کوچک ، وجود پیام های Broadcast نمی تواند مشکل و یا مسئله قابل توجهی را ایجاد نماید، ولی در صورت رشد شبکه ، وجود پیام های broadcast می تواند به یک مشکل اساسی و مهم تبدیل گردد . در چنین مواردی و در اغلب مواقع ، سیلابی از اطلاعات بی ارزش بر روی شبکه در حال جابجائی بوده و عملاً " از پهنای باند شبکه، استفاده مطلوب نخواهد شد. تمامی ایستگاههای متصل شده به یک سوئیچ ، پیام های Broadcast را دریافت می نمایند . چراکه تمامی آنان بخشی از یک Broadcast domain مشابه می باشند .

در صورت افزایش تعداد سوئیچ ها و ایستگاهها در یک شبکه ، مشکل اشاره شده ملموس تر خواهد بود . همواره احتمال وجود پیام های Broadcast در یک شبکه وجود خواهد داشت .

یکی دیگر از مسائل مهم ، موضوع امنیت است . در شبکه هائی که با استفاده از سوئیچ ایجاد می گردند ، هر یک از کاربران شبکه قادر به مشاهده تمامی دستگاههای موجود در شبکه خواهند بود . در شبکه ای بزرگ که دارای سرویس دهندگان فایل ، بانک های اطلاعاتی و سایر اطلاعات حساس و حیاتی است ، این موضوع می تواند امکان مشاهده تمامی دستگاههای موجود در شبکه را برای هر شخص فراهم نماید . بدین ترتیب منابع فوق در معرض تهدید و حملات بیشتری قرار خواهند گرفت. به منظور حفاظت این چنین سیستم هائی می بایست محدودیت دستیابی را در سطح شبکه و با ایجاد سگمنت های متعدد و یا استقرار یک فایروال در جلوی هر یک از سیستم های حیاتی ، انجام داد .

معرفی VLAN

تمامی مسائل اشاره شده در بخش قبل را و تعداد بیشتری را که به آنان اشاره نشده است را می توان با ایجاد یک VLAN به فراموشی سپرد . به منظور ایجاد VLAN ، به یک سوئیچ لایه دوم که این تکنولوژی را حمایت نماید ، نیاز می باشد . تعدادی زیادی از افرادی که جدیداً با دنیای شبکه آشنا شده اند ، اغلب دارای برداشت مناسبی در این خصوص نمی باشند و اینگونه استنباط نموده اند که صرفاً " می بایست به منظور فعال نمودن VLAN ، یک نرم افزار اضافه را بر روی سرویس گیرندگان و یا سوئیچ نصب نمایند . (برداشتی کاملاً اشتباه !) . با توجه به این که در شبکه های VLAN ، میلیون ها محاسبات ریاضی انجام می شود ، می بایست از سخت افزار خاصی که درون سوئیچ تعبیه شده است ، استفاده گردد (دقت در زمان تهیه یک سوئیچ). در غیر اینصورت امکان ایجاد یک VLAN با استفاده از سوئیچ تهیه شده ، وجود نخواهد داشت .

هر VLAN که بر روی سوئیچ ایجاد می گردد ، به منزله یک شبکه مجزا می باشد . بدین ترتیب برای هر VLAN موجود یک broadcast domain جداگانه ایجاد می گردد . پیام های broadcast ، به صورت پیش فرض ، از روی تمامی پورت هائی از شبکه که عضوی از یک VLAN مشابه نمی باشند، فیلتر می گردند . ویژگی فوق ، یکی از مهمترین دلایل متداول شدن VALN در شبکه های بزرگ امروزی است (تمایز بین سگمنت های شبکه) . شکل زیر یک نمونه شبکه با دو VLAN را نشان می دهد :



در شکل فوق ، یک شبکه کوچک با شش ایستگاه را که به یک سوئیچ (با قابلیت حمایت از vlan) متصل شده اند ، مشاهده می نمائیم . با استفاده از پتانسیل VLAN سوئیچ ، دو VLAN ایجاد شده است که به هر یک سه ایستگاه متصل شده است (VLAN1 و VLAN2) . زمانی که ایستگاه شماره یک متعلق به VLAN1 ، یک پیام Broadcast را ارسال می نماید (نظیر : FF:FF:FF:FF:FF:FF) ، سوئیچ موجود آن را صرفاً برای ایستگاههای شماره دو و سه فوروارده می نماید . در چنین مواردی سایر ایستگاههای متعلق به VLAN2 ، آگاهی لازم در خصوص پیام های broadcast ارسالی بر روی VLAN1 را پیدا نکرده و درگیر این موضوع نخواهند شد .

در حقیقت ، سوئیچی که قادر به حمایت از VLAN می باشد ، امکان پیاده سازی چندین شبکه مجزا را فراهم می نماید (مشابه داشتن دو سوئیچ جداگانه و اتصال سه ایستگاه به هر یک از آنان در مقابل استفاده از VLAN) . بدین ترتیب شاهد کاهش چشمگیر هزینه های برپاسازی یک شبکه خواهیم بود .

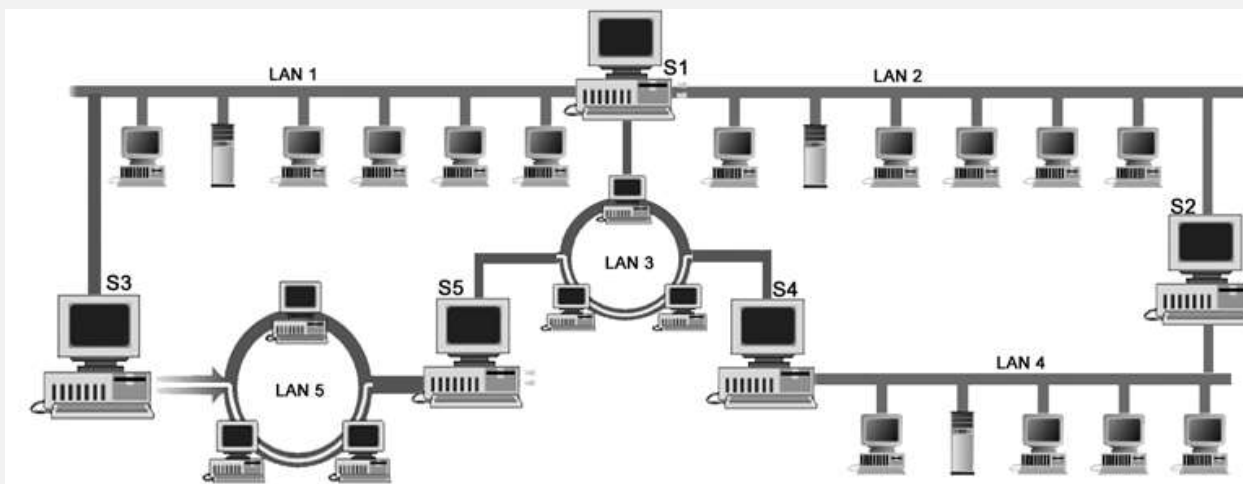
فرض کنید قصد داشته باشیم زیر ساخت شبکه موجود در یک سازمان بزرگ را به دوازده شبکه جداگانه تقسیم نمائیم . بدین منظور می توان با تهیه دوازده سوئیچ و اتصال ایستگاههای مورد نظر به هر یک از آنان ، دوازده شبکه مجزا که امکان ارتباط بین آنان وجود ندارد را ایجاد نمائیم . یکی دیگر از روش های تامین خواسته فوق ، استفاده از VLAN است . بدین منظور می توان از یک و یا چندین سوئیچ که VLAN را حمایت می نمایند ، استفاده و دوازده VLAN را ایجاد نمود . بدیهی است ، هزینه برپاسازی چنین شبکه هایی به مراتب کمتر از حالتی است که از دوازده سوئیچ جداگانه ، استفاده شده باشد .

در زمان ایجاد VALN ، می بایست تمامی ایستگاه ها را به سوئیچ متصل و در ادامه ، ایستگاه های مرتبط با هر VLAN را مشخص نمود. هر سوئیچ در صورت حمایت از VLAN ، قادر به پشتیبانی از تعداد مشخصی VLAN است . مثلاً یک سوئیچ ممکن است ۶۴ و یا ۲۶۶ VLAN را حمایت نماید.

درس ۲

Routing

Routing چیست ؟



مسیریابی، عملیات انتقال اطلاعات از مبدأ به مقصد است. Routing معمولاً با Bridging مقایسه می‌شود. اولین تفاوت این است که Bridging متعلق به Data Link Layer می‌باشد. در صورتیکه Routing متعلق به Network Layer است. این تفاوت باعث می‌شود که در فرآیند انتقال اطلاعات از اطلاعات متفاوتی استفاده شود.

اجزاء Routing:

Routing وظیفه انجام دو کار عمده را دارد، تعیین بهینه ترین مسیر و انتقال گروههای اطلاعاتی (Packets) از طریق شبکه که این موضوع Switching نامیده می‌شود. بر خلاف Switching، تعیین مسیر کمی پیچیده است.

تعیین مسیر:

يك متريك، يك استاندارد برای سنجیدن است. مثل طول مسیر که در الگوریتمهای مسیریابی استفاده می شود. برای مسیر یابی این الگوریتمها جدولهای مسیر یابی دارند و اطلاعات مسیر با توجه به الگوریتم تغییر می کنند.

این جدولها، اطلاعات متنوعی دارند. مثلاً next hop به يك Router می گوید که يك به مقصد مشخص می توان بصورت بهینه از طریق يك Router مشخص که همان hop بعدی است رسید. وقتیکه يك Router يك Packet را می گیرد، آدرس مقصد را چك می کند و سعی می کند رابطه ای بین آن و hop بعدی را برقرار کند.

مثل جدول زیر:

Net. No.	Send to
۲۷	Node A
۵۷	Node B
۱۷	Node C

Router ها با هم رابطه برقرار می کنند و از طریق رد و بدل کردن پیام، جدولهای Routing را می سازند. پیام Routing update، معمولاً تمام یا قسمتی از جدول Routing را در بر دارد. با بررسی جدول بقیه Routerها، هر Router، می تواند يك توپولوژی دقیق از شبکه برای خود ترسیم کند. نوع دیگری از پیامها، اعلام عمومی Link – State است. که به بقیه Routerها در مورد وضعیت رابطهای فرستنده اطلاعات می دهد.

Switching:

الگوریتمهای Switching معمولاً ساده و یکسان هستند. در بیشتر مواقع، يك host معین می کند که باید به يك host دیگر يك Packet بفرستد و هنگامیکه آدرس Router را بدست آورد. host

مبدأ يك Packet آدرس داده شده را به يك آدرس فیزیکی می فرستد و یا پرتو کل و آدرس مقصد. حال Router نگاه می کند که ببیند آیا می تواند آنرا forward کند یا نه. اگر نتوانست آنرا رها می کند اگر نتوانست به hop بعدی می فرستد. و این کار در hop های بعدی بصورت مشابه تکرار می شود.

الگوریتمهای Routing :

این الگوریتمها با توجه به چندین مشخصه ممکن است تغییر کنند: اول هدف طراح باعث تغییر الگوریتم خواهد شد. دوم اینکه چندین روش مسیریابی وجود دارد که هر کدام تأثیر خاص بر شبکه می گذارند .

اهداف طراحی:

- ۱- بهینه بودن، به معنی انتخاب بهترین مسیر است، که وابسته به میزان متریکها خواهد بود مثل تعداد hop ها و یا تأخیری که ایجاد می شود توسط هر hop.
- ۲- ساده بودن، به این معنی که این الگوریتمها باید تا حد ممکن کار آمد باشند در حالیکه نرم افزار آنها پیچیده نباشد و هزینه بالایی هم نداشته باشد.
- ۳- همگرایی سریع: به معنی این است که اگر در کار شبکه اختلالی ایجاد شد. مثل اشکال در کار سخت افزار شرایط بار زیاد، Router همچنان با کار کردن صحیح ادامه دهد. به دلیل اینکه از کار افتادن Routerها ممکن است خسارتهای سنگینی به بار آورد.
- ۴- انعطاف پذیری: به معنی این است که باید به سرعت و دقت با محیط اطراف خود سازگار شوند.

انواع الگوریتمها:

این الگوریتمها بر اساس انواع تفاوت های زیر می توانند تغییر کنند:

- ۱- استاتیک یا دینامیک باشند.
- ۲- يك مسیر یا چند مسیر باشند.

۳- host هوشمند و یا Router داشته باشند.

۴- Link State یا distance Vector باشند.

متریک های Routing:

جدولهای Routing اطلاعاتی دارند که نرم افزار با استفاده از آنها بهترین مسیر را انتخاب می کند. این اطلاعات می توانند شامل متریک های زیر باشند: طول مسیر، قابلیت اطمینان، تأخیر، پهنای باند و هزینه ارتباطات.

IP Routing Protocols:

پروتوکل های مسیر یابی مبتنی بر IP، به دو دسته کلی تقسیم می گردند:

(IGPs^۱)

(EGPs^۲)

IGPs در شبکه هایی که زیر نظر یک شبکه مشترک اداره می شوند استفاده می گردد. انواع

پروتوکل های IGP عبارتند از:

(BGPs^۳)

Enhanced IGRP

(OSPF^۴)

(RIP^۵)

^۱Interior Gateway Protocols

^۲Exterior Gateway Protocols

^۳Border Gateway Protocol

^۴Open shortest Path

^۵Routing Information Protocol

(Is-Is^۱)

EGPs برای مسیر یابی بین شبکه‌هایی که اشتراکی با هم ندارند استفاده می‌گردد، این پروتکل‌ها قبل از اینکه عمل مسیر یابی را انجام دهند، سه نوع اطلاعات نیاز دارند:

لیستی از مسیر یابی‌های همسایه (neighbor routers).

لیستی از شبکه‌هایی که به صورت مستقیم قابل دسترسی هستند.

شماره سیستم مستقل (autonomous system number) مسیر یابی محلی.

پروتکل‌های EGP نیز به دو دسته کلی زیر تقسیم می‌گردند:

(BGP^۲)(EGP^۳)

علاوه بر این‌ها پروتکل‌هایی هم برای شناسایی مسیر یابی‌ها (router discovery) وجود دارد که

از بین آنها می‌توان به ICMP Router Discovery p (RFC۱۲۵۶) اشاره کرد.

برای کار، از کدام یک از پروتکل‌ها استفاده کنیم؟ در واقع برای انتخاب پروتکل باید پارامترهای

زیر را در نظر گرفت:

اندازه و پیچیدگی شبکه

پشتیبانی از (VLSM) Routing Variable Length Subnet Masks , IS-IS , OSPf

میزان reliability , security مورد نیاز.

مشخصه تأخیر (delay) شبکه مورد استفاده.

^۱Intermediate System to Intermediate System

^۲Border Gateway Protocol

^۳Exterior Gateway protocol

قابلیت تغییر پذیری پروتکل به صورت سازمان یافته، به طوری که بتوان آن را با شرایط مختلف سازگار نمود.

فصل ۴

Networking Software

شما در یک شبکه به سخت افزارهایی از قبیل کابلها و روترها و غیره نیاز دارید اما علاوه بر اینها به نرم افزار هم نیاز دارید که یکی از مولفه های مهم میباشد. در این فصل به بررسی عناصر نرم افزارهای مختلف که برای اتصال به شبکه به ما کمک میکنند، از جمله سیستم های عامل، و دایرکتوری میپردازیم. این اجزا با پروتکل های پشته، شبکه را تشکیل می دهند. اگر چه ممکن است با برخی از اجزای مورد بحث در این فصل آشنا باشید اما خواندن آنها خالی از لطف نیست.

درس ۱

Operating Systems

کاربران اینترنت و سایر شبکه های کامپیوتری به منظور استفاده از منابع موجود بر روی شبکه از امکانات سخت افزاری و نرم افزاری متعددی استفاده می نمایند . آشنائی با عناصری که دارای جایگاهی اساسی در ایمن سازی یک شبکه کامپیوتری می باشند از زاویه امنیتی بسیار حائز اهمیت است . اگر قرار است ما چیزی را ایمن نمائیم ، اولاً" باید بدانیم چه چیزی مشمول این موضوع می شود و ثانیاً" شناخت مناسبی را نسبت به آنان پیدا نمائیم . نمی شود اقدام به ایمن سازی یک شبکه نمود بدون این که نسبت به عناصر درگیر در فرآیند ارتباطی شناخت مناسبی وجود داشته باشد.

اجازه دهید این سوال را مطرح نمائیم که در زمان اتصال به اینترنت ، کدامیک از عناصر سخت افزاری و یا نرم افزاری دارای استعداد لازم به منظور آسیب رساندن به اطلاعات بوده و ممکن است امنیت شبکه و اطلاعات را به مخاطره بیندازد ؟ در صورت ارائه پاسخ مناسب به سوال فوق ، محدوده و نوع ایمن سازی و ایمن نگه داشتن سیستم های کامپیوتری ، مشخص خواهد شد . ما نمی توانیم قدم در جاده ای بگذاریم که خطرات و یا تهدیدات امنیتی متعددی در کمین ما می باشد ، بدون این که نسبت به نقاط آسیب پذیر و یا بهتر بگوئیم ضربه پذیر آگاهی مناسبی را داشته باشیم .

تعداد بسیار زیادی از کاربران اینترنت را افرادی تشکیل می دهند که فاقد مهارت های خاصی در زمینه فن آوری اطلاعات بوده و از امکانات حمایتی مناسبی نیز برخوردار نمی باشند . سیستم های اینگونه کاربران دارای استعداد لازم به منظور انواع تهاجمات بوده و بطور غیر مستقیم شرایط مناسبی را برای مهاجمان به منظور نیل به اهداف مخرب ، فراهم می نمایند . به نظر می بایست طرحی نو در اندازیم و یک مرتبه و برای همیشه و بصورت کاملاً" اصولی و علمی با عناصر درگیر در ایمن سازی یک شبکه کامپیوتری آشنا شده و به بررسی دقیق نقاط حساس و آسیب پذیر در این رابطه بپردازیم .

به منظور ایمن سازی و ایمن نگه داشتن یک شبکه کامپیوتری می بایست هم در سطح و هم در عمق حرکت کرد .

- حرکت در عمق ، ارتقاء سطح علمی و بروز نگه داشتن دانش کارشناسان امنیت اطلاعات و شبکه های کامپیوتری است تا آنان بتوانند با استفاده از آخرین فن آوری های موجود نسبت به برپاسازی و نگهداری یک شبکه ایمن اقدام نمایند . فراموش نکنیم که امنیت یک فرآیند است و نه یک محصول ، بنابراین ارتقاء سطح علمی کارشناسان امنیت اطلاعات، می بایست به صورت مستمر و بر اساس یک برنامه کاملاً مدون و مشخص دنبال شود.
- حرکت در سطح ، افزایش دانش عمومی کاربران اینترنت در جهت استفاده ایمن از شبکه های کامپیوتری است . با آموزش مناسب این نوع کاربران، می توان از آنان به منظور ایمن نگه داشتن یک شبکه کامپیوتری استفاده نمود. امنیت در شبکه های کامپیوتری نظیر یک تابلو نقاشی است که تصویر امنیت جزء با همیاری تمامی عناصر در گیر در یک سازمان بر روی آن نقش نخواهد بست . هیچ سازمان و یا کارشناس امنیت اطلاعاتی نمی تواند بدون در نظر گرفتن جایگاه عوامل انسانی وظایف تعریف شده خود را در جهت ایمن نگه داشتن یک شبکه کامپیوتری بدرستی انجام دهد . اگر قرار است در این رابطه دور خود نچرخیم و در مسیرهای بسته و تکراری گرفتار نشویم ، می بایست حرکاتی منسجم و کاملاً سازمان یافته را در این راستا انجام دهیم .

عدم توجه به هر یک از موارد اشاره شده ما را در برپاسازی و نگهداری ایمن شبکه های کامپیوتری با شکست مواجه نموده و شاید زمانی فرارسد که ما قادر به پرداخت تاوان چیزی که از دست داده ایم ، نباشیم (اطلاعات و داده های ارزشمند ، عدم ارائه سرویس های online و ...) . مخاطب این مطلب و سایر مطالبی که با این مضمون تهیه و بر روی سایت منتشر خواهد شد ، کاربران عمومی اینترنت می باشد . با این مقدمه طولانی و شاید خسته کننده و تکراری ! به بررسی اولین و مهمترین عنصر تاثیرگذار در امنیت شبکه های کامپیوتری یعنی سیستم عامل ، خواهیم پرداخت .

سیستم عامل چیست ؟

سیستم عامل برنامه کلی است که وظیفه دارد تا انواع منابع سخت افزاری و نرم افزاری را مدیریت کند، رابط بین اپلیکیشن ها و سخت افزارها را با استفاده از هسته خود مدیریت کند، رابط مستقیم و غیرمستقیم بین کاربر و سخت افزار را ایجاد کرده و دستوراتی که به RAM برای نگه داری یا به CPU برای پردازش ارسال می شوند را مدیریت کرده، برنامه ها و فایل ها را سازماندهی و امکان اتصال دستگاه های ورودی یا خروجی را به کاربر می دهد.

همچنین فایل ها و داده های حافظه های جانبی را مدیریت کرده، استفاده از شبکه ها را آسان تر می کند و در کل استفاده از سیستم را برای کاربران آسان کرده و از اطلاعات آن ها محافظت کند.

سیستم عامل مهمترین ترین برنامه ای است که بر روی کامپیوتر شما اجراء شده و خدمات متنوعی را در ابعاد متفاوت ارائه می نماید . بد نیست به برخی از این نوع خدمات اشاره ای مختصر داشته باشیم :

- نوع نرم افزاری را که شما می توانید بر روی سیستم خود نصب نمائید، مشخص می نماید .
- هماهنگی لازم به منظور اجرای برنامه ها را انجام می دهد .
- حصول اطمینان از این موضوع که عناصر سخت افزاری نظیر صفحه کلید ، چاپگر و هارد دیسک دارای عملکردی عاری از خطاء بوده و امکان ارتباط با آنان وجود دارد .
- ایجاد شرایط و امکانات لازم به منظور اجرای صحیح برنامه های کامپیوتری نظیر واژه پردازها (نظیر MsWord) ، برنامه های سرویس گیرنده پست الکترونیکی (نظیر Outlook) ، مرورگرهای وب (نظیر Internet Explorer) . در صورتی که برنامه ها نیازمند استفاده از منابع سیستم نظیر چاپگر و یا هارد دیسک باشند ، با مدیریت سیستم عامل این امر میسر می گردد.
- ارائه پیام های خطاء متناسب با مسائل ایجاد شده .

سیستم عامل ، نوع و نحوه مشاهده اطلاعات و انجام عملیات مورد نظر را نیز مشخص می نماید . برخی از سیستم های عامل از یک رابط کاربر گرافیکی معروف به GUI که از کلمات Graphical User Interface اقتباس شده است ، استفاده می نمایند . در این نوع از سیستم های عامل ،

اطلاعات با استفاده از تصاویر (آیکون ، دکمه ها ، جعبه های محاوره ای ، پنجره ها ، ...) و کلمات ارائه می گردد (ویندوز نمونه ای از اینگونه سیستم های عامل است) . سایر سیستم های عامل ممکن است از یک رابط کاربر مبتنی بر متن به منظور تعامل با کاربر استفاده نمایند .

چگونه یک سیستم عامل را انتخاب نمایم

زمانی که شما یک کامپیوتر را خریداری می نمائید ، انتخاب خود را در خصوص نوع سیستم عامل نیز انجام داده اید، چراکه سیستم عامل بر روی کامپیوتر خریداری شده نصب و در اختیار شما قرار داده می شود . شما می توانید هر زمان که تشخیص دادید سیستم عامل نصب شده بر روی کامپیوتر خود را تغییر دهید . در برخی از کشورها ، همزمان با ارائه کامپیوتر سیستم عامل آن نیز عرضه می شود (مثلاً " کامپیوترهای شرکت Dell و Gateway به همراه ویندوز مایکروسافت عرضه می گردند) .

تاکنون سیستم های عامل متداولی در سطح دنیا طراحی و پیاده سازی شده است . هر سیستم عامل دارای ویژگی ها ، مزایا و محدودیت های مختص به خود می باشد . در این رابطه می توان به متداولترین سیستم های عامل موجود اشاره نمود :

- ویندوز (Windows) : ویندوز که دارای نسخه های متعددی است متداولترین سیستم عامل استفاده شده توسط کاربران می باشد. این سیستم عامل توسط شرکت مایکروسافت ارائه شده و دارای یک رابط کاربر گرافیکی است که استفاده از آن را برای اکثر کاربران راحت تر می نماید (نسبت به سیستم های عاملی که دارای رابط کاربر مبتنی بر متن می باشند) . ویندوز دارای نسخه های جداگانه ای برای کاربران معمولی و نسخه هائی مختص سرویس دهندگان می باشد .
- Mac OS X : سیستم عامل فوق توسط شرکت اپل ارائه شده است و از آن بر روی کامپیوترهای مکینتاش استفاده می گردد . این سیستم عامل از لحاظ شکل ظاهری و رابط کاربر گرافیکی دارای شباهت های زیادی با ویندوز می باشد (با تغییراتی اندک) .
- لینوکس و سایر سیستم های عامل مبتنی بر یونیکس : از لینوکس و سایر سیستم های عاملی که از یونیکس مشتق شده اند عموماً در ایستگاههای شبکه ای خاص و یا سرویس دهندگان شبکه نظیر سرویس دهندگان وب و پست الکترونیکی ، استفاده می گردد .

استفاده از اینگونه سیستم های عامل توسط کاربران معمولی عمدتاً " مشکل بوده و به منظور استفاده از آنان به دانش و یا مهارت های خاصی نیاز می باشد . همین موضوع یکی از دلایل اصلی در رابطه با عدم گسترش عمومی آنان محسوب می گردد . نسخه هائی از سیستم های عامل فوق در حال پیاده سازی است تا کاربران معمولی نیز بتوانند بسادگی از آنان استفاده نمایند .

درس ۲

Directory Services

دایرکتوری سرویس یک نرم افزار کاربردی و یا مجموعه ای از نرم افزارهای کاربردی است که وظیفه ذخیره و سازمان دهی اطلاعات مربوط به کاربران و منابع یک شبکه رایانه ای را به عهده داشته و به مدیر شبکه این امکان را می دهد که دسترسی کاربران به منابع شبکه را مدیریت نماید. دایرکتوری سرویس در عین حال به عنوان یک لایه محافظ بین کاربران و منابع مشترک شبکه عمل می کند.

دایرکتوری سرویس را نباید با منبع ذخیره دایرکتوری که در واقع محل نگهداری اطلاعات مربوط به اجزای نامگذاری شده که توسط دایرکتوری سرویس مدیریت می شوند، اشتباه نمود. در دایرکتوری سرویس مدل پراکنده X.500، از تعداد یک یا بیش از یک فضای تخصیص یافته برای نام (درخت اجزاء) جهت تشکیل دایرکتوری سرویس استفاده می شود. دایرکتوری سرویس به عنوان واسطی برای دسترسی به اطلاعات موجود در یک یا بیش از یک فضای تخصیص یافته در دایرکتوری عمل می نماید. واسط دایرکتوری سرویس نقش مسئولیت مرکزی و مشتری را ایفا می نماید که می تواند امنیت کافی را برای آن دسته از منابع سیستم که مدیریت اطلاعات دایرکتوری را انجام می دهند فراهم آورد.

همچون یک بانک اطلاعاتی، دایرکتوری سرویس به نحوی طراحی شده که می تواند به شکلی کارآمد اطلاعات را خوانده و امکانات پیشرفته جستجو در بین خصیصه های مختلفی که می توانند به شی های موجود در دایرکتوری مرتبط شوند را فراهم سازد. اطلاعاتی که در دایرکتوری ذخیره شده اند با استفاده از طراحی براساس خصیصه های قابل تغییر تعریف می شوند. سرویس های دایرکتوری از مدل پراکنده برای ذخیره سازی اطلاعات خود استفاده می کنند و این اطلاعات معمولاً بین دایرکتوری سرورها دوباره سازی می شوند.

معرفی

یک دایرکتوری سرویس که "سرویس نامگذاری" خوانده می شود مانند نقشه راهنمایی عمل می کند که منابع شبکه را به آدرس های مربوط به آن ها در شبکه مرتبط نموده و آنها را به این ترتیب مورد شناسائی قرار میدهد. با استفاده از دایرکتوریهای از نوع "سرویس نامگذاری" کاربر نیاز ندارد تا آدرس فیزیکی منابع شبکه را به خاطر بسپارد، چرا که تنها نام منبع کفایت تا محل آن را مشخص نماید. هریک از منابع در شبکه به عنوان یک شیء در دایرکتوری سرور محسوب میگردند. اطلاعات مربوط به هر منبع شبکه تحت عنوان خصیصه شیء مربوط به آن منبع در دایرکتوری سرور ذخیره میشود. سطح امنیت اطلاعات هر شیء میتواند به نحوی تعیین شود که فقط کاربرانی قابلیت دسترسی به آنها را داشته باشند که دارای مجوز لازم هستند. دایرکتوری های پیچیده تری با فضاهای نامگذاری مختلفی تحت عنوان "مشترکین"، "دستگاهها"، "میزان مالکیت"، "ترجیحات"، "محتوا" و غیره طراحی شده اند. فرایند این طراحی تا حد بسیار زیادی بستگی به مدیریت "شناسه" دارد.

دایرکتوری سرویس "فضای نامگذاری" را برای شبکه تعریف میکند. یک "فضای نامگذاری" در این مقوله عبارتی است که از آن برای نگهداری یک یا چند شیء تحت عنوان "ورودی نامگذاری شده" استفاده میشود. فرایند طراحی دایرکتوری معمولاً دارای مجموعه ای از قوانین است که چگونگی نامگذاری و شناسایی منابع شبکه را تعریف میکنند. این قوانین مشخص میکنند که نامها باید منحصر به فرد بوده و گنگ نباشند. در X.500 (مجموعه استانداردهای دایرکتوری سرویس) و LDAP نام منبع شبکه "نام مشخصه" خوانده می شود و از آن برای اشاره به مجموعه ای از خصیصه ها ("نامهای مشخصه نسبی") که نام یک ورودی دایرکتوری را تشکیل میدهند استفاده میگردد.

یک دایرکتوری سرویس ساختاری از اطلاعات به اشتراک گذاشته شده است که از آن برای پیدا کردن، مدیریت، اداره کردن، و سازمان دهی اجزاء مشترک و منابع شبکه مانند دیسکها، پوشه ها، فایلها، چاپگرها، کاربران، گروهها، دستگاهها، شماره های تلفن و شیء های دیگر استفاده میشود.

دایرکتوری سرویس بخش مهمی از سیستم عامل شبکه است. در موارد پیچیده تر دایرکتوری سرویس مخزن اصلی برای ارائه خدمات شبکه میباشد. به عنوان مثال جستجوی کلمه "کامپیوترها" با استفاده از دایرکتوری سرویس ممکن است پاسخی شامل فهرستی از کامپیوترها و اطلاعات مربوط به نحوه دسترسی به آنها را ارائه نماید.

"دوباره سازی" و "پراکندگی" دارای معانی کاملاً مشخص و منحصر به فردی در طراحی و مدیریت یک دایرکتوری سرویس هستند. عبارت "دوباره سازی" به این معنی است که یک "فضای نامگذاری" (یا شیء) موجود در یک دایرکتوری در دایرکتوری سرورهای دیگر نیز کپی می شود تا هم به عنوان نسخه پشتیبان از آنها استفاده شود و هم به دلیل وجود نسخه محلی از ایجاد ترافیک غیر ضروری در شبکه خودداری گردد. "فضای نامگذاری" دوباره سازی شده توسط مقام مسئول نسخه اصلی مدیریت میشود. عبارت "پراکنده" به معنی این است که دایرکتوری سرورهای متعددی که هر یک "فضای نامگذاری" مختلفی را در خود جای داده اند به یکدیگر متصل شده اند تا یک دایرکتوری سرویس پراکنده را بوجود آورند. در این حالت هر "فضای نامگذاری" مستقل میتواند از طرف مقامات مسئول مختلفی مدیریت شود.

نرم افزار دایرکتوری سرویس

دایرکتوری سرویسهای تولید شده توسط تولید کنندگان و نهادهای استاندارد مختلف عبارتند از انواع قدیمی و جدید ارائه شده زیر:

• Banyan VINES

اولین دایرکتوری سرویس ارائه شده که قابلیت تغییر متناسب با مقیاس مورد نیاز را داشت.

• دایرکتوری سرور Sun Java System

• دایرکتوری سرور IBM Tivoli

• NTDS (Windows NT Directory Services) برای Windows NT

- Server ۲۰۰۳ و Windows ۲۰۰۰ برای Active Directory
- Mac OS X Server در سیستم عامل Apple Open Directory
- Critical Path Directory Server
- Novell eDirectory، که قبلاً بنام NDS (Novell Directory Services) خوانده میشد.
- OpenLDAP
- Fedora Directory Server

طراحی دایرکتوری‌ها تفاوت بسیاری با طراحی بانکهای اطلاعاتی نسبی دارد. طراح بانکهای اطلاعاتی سعی در طراحی مدل اطلاعاتی برای مسائل تجاری و نیازهای فرایندی دارد که غالباً در آن ملاحظات مربوط به مشتریان آنلاین، سرویس، مدیریت کاربران، میزان نسبی حضور و سیستم از قلم انداخته میشوند. حال آنکه در مورد دایرکتوری اگر بنا بر این است که اطلاعات در یک منبع ذخیره قابل استفاده برای بسیاری از برنامه‌های کاربردی و کاربران قرار گیرند، باید طراحی اطلاعات (و شناسه‌ها) و ساختار آن به گونه‌ای انجام شود که منعکس کننده نقش شی‌ها در دنیای واقعی باشد. در بسیاری از موارد این شی‌ها معرف کاربران، دفاتر آدرس، لیستهای اسامی، ترجیحات، تعاریف میزان مالکیت، محصولات و خدمات، دستگاهها، پرونده‌های اطلاعات، سیاستها، شماره تلفن‌ها، اطلاعات مسیر دهی، و غیره میباشند. افزون بر این طراح باید به ملاحظات کاربردی طراحی در رابطه با کارایی و مقیاس کار نیز توجه داشته باشد. برای یک بررسی سریع در خصوص طراحی کاربردی به این مثال فکر کنید: ۵۰ شی و ۱ میلیون کاربر دارید که هریک از کاربران یا برنامه‌های کاربردی آنها نیاز خواهند داشت تا ۵۰۰۰ بار در ثانیه یا دقیقه یا در ساعت (به منظور دریافت مجوز و بروز رسانی فضای خدمات گیری خود) به این شی‌ها دسترسی یابند. حال ببینید آیا سرور و سایر تجهیزات شبکه‌ای که در نظر گرفته اید قادر به پاسخگویی به چنین حجمی از کار می‌باشد یا خیر.

تفاوت اساسی بین بانکهای اطلاعاتی و دایرکتوری‌ها در سطح سیستم است، جایی که یک بانک اطلاعاتی با استفاده از یک مدل اطلاعات تخصیص یافته (نسبی) برای خودکار نمودن یک فرآیند مورد استفاده قرار میگیرد اما یک دایرکتوری برای نگهداری از شی‌های "شناخته شده" ای که

میتوانند توسط برنامه های کاربردی مختلفی به صورت تصادفی مورد استفاده قرار گیرند به کار برده میشود. یک دایرکتوری سرویس در جایی به کار می آید که "مدیریت متعدد" (توسط کاربران و برنامه های کاربردی متعدد) از اطلاعات یکسان به منظور اطمینان از صحت و کارائی، استفاده میکنند. این دیدگاه در طراحی سیستم انعطاف پذیری و مقیاس بندی را ارائه میدهد که توسط آن میتوان کارکردهایی همچون "سیستمهای ارائه خدمات" را که دارای مقیاس وسیعی میباشد به درستی مشخص نمود. "سیستمهای ارائه خدمات" امروزه صدها میلیون شی (HSS/HLR)، دفاتر آدرس، میزان مالکیت کاربران، شماره تلفنهای VOIP، اطلاعات کاربران و دستگاهها، و غیره) را به صورت لحظهای و روشهای انفاقی پشتیبانی میکنند و میتوانند از طریق سیستمهای BSS/OSS/CRM و یا برنامه های کاربردی خود گردان توسط کاربران مدیریت شوند.

از آثار بارز در خصوص طراحی بانکهای اطلاعاتی میتوان به این مسئله اشاره نمود که کمپانی های بزرگ دارای صدها (اگر نه هزارها) از این بانکهای اطلاعاتی برای فرایندهای مختلف هستند و اکنون سعی بر این دارند تا کاربران و اطلاعات شناسائی خدمات و محصولات آنلاین و مدیریت خدمات خود را در یکجا گرد آورده و آنها را به صورت لحظه ای و هزینه اقتصادی با صرفه ارائه دهند. بنا بر این یک دایرکتوری سرویس در مقیاس بزرگ باید در معماری راه حل آنها جای گیرد.

پیاده سازی دایرکتوری سرویس

دایرکتوری سرویس بخشی از لایحه «ارتباط باز سیستمها» بود که به منظور رسیدن به موافقت همه جانبه ای در استانداردهای مشترک شبکه برای ایجاد امکان کارکرد بین تولید کنندگان مختلف ارائه شده بود. در دهه ۸۰ میلادی ITU و ISO مجموعه ای از استانداردها را به نام X.۵۰۰ برای دایرکتوری سرویسها ارائه دادند که هدف اولیه آن پاسخگوئی به نیازهای تعریف شده برای ارسال و دریافت پیغامهای الکترونیکی بین کاربرهای متفاوت و جستجو برای نامهای شبکه بود. «پروتکل سبک دسترسی به دایرکتوری» یا LDAP بر اساس سرویسهای اطلاعات دایرکتوری X.۵۰۰ طراحی شده، اما از مجموعه TCP/IP و طرح کد بندی X.۵۰۹ پروتکل DAP استفاده می کند که این باعث می شود تا بیشتر با اینترنت همخوانی و مرتبط باشد.

انواع بسیار زیادی از پیاده سازی های دایرکتوری سرویس توسط تولید کنندگان مختلف وجود داشته که از آن جمله می توان به موارد زیر اشاره نمود:

- NIS¹: پروتکل یا خدمات اطلاعات شبکه، که در ابتدا «صفحات زرد» (دفتر لیست تلفن عمومی) نام گذاری شده بود، توسط کمپانی Sun Microsystems برای پیاده سازی دایرکتوری سرویس در محیطهای شبکه UNIX طراحی شد. (Sun در اوایل سال ۲۰۰۰ بخش Netscape خود را که در اتحاد با iPlanet بود یکپارچه نمود و دایرکتوری سرویس خود بر پایه LDAP را تولید کرد که به صورت بخشی از Sun ONE درآمد و این طرح اکنون به نام Sun Java Enterprise شناخته می شود).
- eDirectory: این پیاده سازی دایرکتوری سرویس توسط Novell می باشد. این نوع از دایرکتوری سرویس معماریهای متعددی را پشتیبانی می کند که از بین آنها می توان به Windows, NetWare, Linux، و گونه های مختلفی از Unix اشاره کرد و این محصول مدتهاست که برای راهبری کاربران، مدیریت تنظیمات، و مدیریت نرم افزارها بکار برده می شود. eDirectory به صورت بخش مرکزی گستره وسیعی از محصولات مدیریت شناسائی درآمده است. این محصول قبلاً به نام Novell Directory Service شناخته می شد.
- Red Hat Directory Server: Red Hat دایرکتوری سرویسی را که آنرا از واحد راه حل های امنیتی Netscape دریافت کرده بود به عنوان محصول تجاری ارائه داد که در سیستم Red Hat Enterprise Linux تحت نام Red Hat Directory Server و به عنوان بخشی از هسته مرکزی Fedora تحت نام Fedora Directory Server کار می کند.
- Active Directory: دایرکتوری سرویس Microsoft به نام Active Directory خوانده می شود و در سیستم عاملهای Windows ۲۰۰۰ و Windows Server ۲۰۰۳ موجود است.
- Open Directory: سیستم عامل Apple Mac OS X Server دایرکتوری سرویس خود را تحت نام Open Directory ارائه می دهد که این محصول بسیاری از پروتکل های استاندارد

¹Network Information Services

باز همچون LDAP و Kerberos را در کنار راه حل های اختصاصی مانند Active Directory و eDirectory به صورت تلفیقی در خود دارد.

- Apache Directory Server: Apache Software Foundation دایرکتوری سرویسی به نام ApacheDS ارائه می دهد.

- Oracle Internet Directory: OID Oracle Corporation دایرکتوری سرویس کمپانی Oracle Corporation است که با LDAP ویرایش ۳ همخوانی دارد.

- CA Directory: CA Directory موتور پیش-جمع آوری (Pre-caching) دارد که تمام خصیصه های مورد استفاده در فیلترهای جستجوی LDAP را فهرست نموده و آنها را در نتیجه جستجو نمایش می دهد.

- Sun Java System Directory Server: این دایرکتوری سرویس ارائه شده توسط Sun Microsystems است که آن را می توان در آدرس اینترنتی

- http://www.sun.com/software/products/directory_srvr_ee/ یافت.

- OpenDS: این دایرکتوری سرویس که از پایه و در محیط جاوا به صورت مرجع آزاد (Open Source) طراحی گردیده، توسط کمپانی Sun Microsystems پشتیبانی شده و

- در آدرس اینترنتی <http://opends.dev.java.net/> قابل دسترسی می باشد.

افزون بر این موارد، تعداد زیادی از ابزارهای مرجع آزاد وجود دارند که با استفاده از آنها می توان دایرکتوری سرویسهای مختلفی شامل پروتکل های LDAP و Kerberos، و همچنین نرم افزار Samba را که با پروتکل های یاد شده نقش کنترلر Domain را ایفا می کند را بوجد آورد.

فصل ۵

Data-Link Layer Protocol

پروتکل‌های لایه پیوند داده از توصیف ماهیت محیط شبکه و انجام آماده سازی نهایی از داده های خروجی قبل از انتقال آن سخن میگوید. این پروتکل ها همچنین دریافت اطلاعات ورودی را ارزیابی میکنند، و در صورت لزوم بستر عبور آن را به پروتکل لایه شبکه فراهم میکنند. در این فصل به بررسی رایج ترین پروتکل های لایه پیوند داده و چگونگی عملکرد آنها در شبکه میپردازیم. مطالعه این پروتکلها در شبکه بسیار حیاتی میباشد چرا که آنها، تعیین میکنند که چگونه یک شبکه ساخته شده است و این که چگونه رایانه ها داده ها را دریافت و منتقل میکنند.

درس ۱

Ethernet

مبانی اترنت

اترنت ، متداولترین فناوری استفاده شده در دنیای شبکه های محلی است که خود از مجموعه ای تکنولوژی دیگر تشکیل شده است . یکی از بهترین روش های آشنائی اصولی با اترنت ، مطالعه آن با توجه به مدل مرجع OSI است . اترنت از رسانه های انتقال داده و پهنای باند متفاوتی حمایت می نماید ولی در تمامی نمونه های موجود از يك قالب فریم و مدل آدرس دهی مشابه استفاده می گردد .

به منظور دستیابی هر يك از ایستگاه ها و یا گره های موجود در شبکه به محیط انتقال ، استراتژی های کنترل دستیابی مختلفی تاکنون ابداع شده است . آگاهی از نحوه دستیابی دستگاه های شبکه ای به محیط انتقال امری لازم و ضروری به منظور شناخت عملکرد شبکه و اشکال زدائی منطقی و اصولی آن می باشد .

اترنت چیست ؟

- اکثر ترافیک موجود در اینترنت از اترنت شروع و به آن نیز خاتمه می یابد . اترنت در سال ۱۹۷۰ ایجاد و از آن زمان تاکنون به منظور تامین خواسته های موجود برای شبکه های محلی با سرعت بالا رشد و ارتقاء یافته است . زمانی که يك رسانه انتقال داده جدید نظیر فیبر نوری تولید می گردید ، اترنت نیز متأثر از این تحول می شد تا بتواند از مزایای برجسته پهنای باند بالا و نرخ پائین خطاء در فیبر نوری استفاده نماید . هم اینك پروتکل هائی که در سال ۱۹۷۲ صرفاً قادر به حمل داده با نرخ سه مگابیت در ثانیه بودند ، می توانند داده را با سرعت ده گیگابیت در ثانیه حمل نمایند .

- سادگی و نگهداری آسان ، قابلیت ترکیب و تعامل با تکنولوژی های جدید ، معتبر بودن و قیمت پائین نصب و ارتقاء از مهمترین دلایل موفقیت اترنت محسوب می گردد .
- امکان استفاده دو و یا بیش از دو ایستگاه از يك محیط انتقال بدون تداخل سیگنال ها با یکدیگر ، از مهمترین دلایل ایجاد اترنت می باشد . استفاده چندین کاربر از يك محیط انتقال مشترك در ابتدا و در سال ۱۹۷۰ در دانشگاه هاوایی مورد توجه قرار گرفت . حاصل مطالعه فوق ، ابداع روش دستیابی اترنت بود که بعداً "CSMA/CD نامیده شد .
- اولین شبکه محلی در جهان ، نسخه ای اولیه از اترنت بود که Robert Metcalfe و همکاران وی در زیراکس آن را در بیش از سی و چهار سال قبل طراحی نمودند. اولین استاندارد اترنت در سال ۱۹۸۰ توسط کنسرسیومی متشکل از اینتل ، Digital Equipment و زیراکس و با نام اختصاری DIX ایجاد گردید . مهمترین هدف کنسرسیوم فوق ، ارائه يك استاندارد مشترك بود تا تمامی علاقه مندان بتوانند از مزایای آن بدون محدودیت های مرسوم استفاده نمایند و به همین دلیل بود که آنان بر روی يك استاندارد باز متمرکز شدند. اولین محصول پیاده سازی شده با استفاده از استاندارد اترنت در اوائل سال ۱۹۸۰ به فروش رفت . اترنت اطلاعات را با سرعت ده مگابیت درثانیه بر روی کابل کواکسیال و حداکثر تا مسافت دو کیلومتر ارسال می نمود . به این نوع کابل کواکسیال ، thicknet نیز گفته می شود .
- در سال ۱۹۹۵ ، موسسه IEEE کمیته هائی را به منظور استاندارد سازی اترنت ایجاد نمود . استاندارد های فوق با ۸۰۲ شروع می شود و این استاندارد برای اترنت ۳ . ۸۰۲ می باشد . موسسه IEEE درصدد بود که استانداردهای ارائه شده با مدل مرجع OSI سازگار باشند . به همین دلیل لازم بود به منظور تامین خواسته های لایه يك و بخش پائینی لایه دوم مدل مرجع OSI ، تغییراتی در استاندارد ۳ . ۸۰۲ داده شود . تغییرات اعمال شده در نسخه اولیه اترنت بسیار اندك بود بگونه ای که هر کارت شبکه اترنت قادر به ارسال و یا دریافت فریم های اترنت و استاندارد ۳ . ۸۰۲ بود . در واقع ، اترنت و ۳/۸۰۲ IEEE ، استانداردهای مشابه و یکسانی می باشند .

- پهنای باند ارائه شده توسط اترنت در ابتدا ده مگابیت در ثانیه بود و برای کامپیوترهای شخصی دهه هشتاد که دارای سرعت پائین بودند ، کافی بنظر می آمد ولی در اوایل سال ۱۹۹۰ که سرعت کامپیوترهای شخصی و اندازه فایل ها افزایش یافت ، مشکل پائین بودن سرعت انتقال داده بهتر نمایان شد . اکثر مشکلات فوق به کم بودن پهنای باند موجود مربوط می گردید . در سال ۱۹۹۵ ، موسسه IEEE ، استاندارد را برای اترنت با سرعت یکصد مگابیت در ثانیه معرفی نمود . این روال ادامه یافت و در سال های ۱۹۹۸ و ۱۹۹۹ استانداردهائی برای گیگابیت نیز ارائه گردید .
- تمامی استانداردهای ارائه شده با استاندارد اولیه اترنت سازگار می باشند . یک فریم اترنت می تواند از طریق یک کارت شبکه با کابل کواکسیال ۱۰ مگابیت در ثانیه از یک کامپیوتر شخصی خارج و بر روی یک لینک فیبر نوری اترنت ده گیگابیت در ثانیه ارسال و در انتها به یک کارت شبکه با سرعت یکصد مگابیت در ثانیه برسد . تا زمانی که بسته اطلاعاتی بر روی شبکه های اترنت باقی است در آن تغییری داده نخواهد شد . موضوع فوق وجود استعداد لازم برای رشد و گسترش اترنت را به خوبی نشان می دهد . بدین ترتیب امکان تغییر پهنای باند بدون ضرورت تغییر در تکنولوژی های اساسی اترنت همواره وجود خواهد داشت .

قوانین نامگذاری اترنت توسط موسسه IEEE

اترنت صرفاً " یک تکنولوژی نمی باشد و خانواده ای مشتمل بر مجموعه ای از تکنولوژی های دیگر نظیر:

Gigabit Ethernet و Legacy, FastEthernet را شامل می شود . سرعت اترنت می تواند ده ، یکصد ، یکهزار و یا ده هزار مگابیت در ثانیه باشد . قالب اساسی فریم و زیر لایه های IEEE لایه های اول و دوم مدل مرجع OSI در تمامی نمونه های اترنت ثابت و یکسان می باشد .

زمانی که لازم است اترنت به منظور اضافه کردن یک رسانه انتقال داده جدید و یا قابلیتی خاص توسعه یابد ، موسسه IEEE یک ضمیمه جدید را برای استاندارد ۳ . ۸۰۲ ارائه

می نماید. ضمیمه فوق دارای يك و یا دو حرف تکمیلی است . در چنین مواردی يك نام کوتاه شده نیز بر اساس مجموعه قوانین زیر به ضمیمه نسبت داده می شود :

- عددی که نشاندهنده تعداد مگابیت در ثانیه داده انتقالی است .

- حرفی که نشاندهنده استفاده از سیگنالینگ Baseband می باشد .

- يك و یا چندین حرف الفبائی که نوع رسانه انتقال داده را مشخص می نماید (مثلاً " از حرف F برای فیبر نوری و یا T برای کابل های مسی بهم تابیده)

اترنت در ارتباط با سیگنالینگ Baseband می باشد که از تمامی پهنای باند رسانه انتقال داده استفاده نموده و سیگنال داده مستقیماً" بر روی رسانه انتقال داده ارسال می گردد . در سیگنالینگ Broadband که توسط اترنت استفاده نمی گردد ، سیگنال داده هرگز مستقیماً" بر روی محیط انتقال داده قرار نمی گیرد . يك سیگنال آنالوگ (Carrier Signal) ، با سیگنال داده مدوله شده و سیگنال فوق ارسال می گردد . شبکه های رادیویی و شبکه های کابلی تلویزیون از سیگنالینگ broadband استفاده می نمایند .

موسسه IEEE نمی تواند تولید کنندگان تجهیزات شبکه ای را مجبور نماید که بطور کامل هر نوع استاندارد ارائه شده را رعایت نمایند ولی امیدوار است به اهداف زیر نائل گردد :

- ارائه اطلاعات مهندسی مورد نیاز برای ایجاد دستگاه هائی که متناسب با استانداردهای اترنت باشند .

- ترویج ابداعات جدید و استفاده از آنان توسط تولید کنندگان .

اترنت و مدل مرجع OSI

- اترنت در دو ناحیه از مدل مرجع OSI کار می کند : لایه فیزیکی و بخش پائینی لایه Data Link (زیر لایه MAC نامیده می شود) .

- برای انتقال داده بین يك ايستگاه اترنت و ايستگاه ديگر ، عموماً " داده از طريق يك Repeater ارسال می گردد . در چنین مواردی سایر ايستگاه های موجود در يك Collision domain مشابه ، ترافیک عبوری از طريق Repeater را مشاهده خواهند کرد . Collision domain يك منبع مشترك است که مسائل ایجاد شده در بخشی از آن سایر عناصر موجود در collision domain را تحت تاثیر قرار خواهد داد .
- Repeater ، مسئولیت فورواردینگ تمامی ترافیک بر روی سایر پورت ها را برعهده دارد . ترافیک دریافتی توسط يك Repeater بر روی پورت اولیه ارسال نخواهد شد . هر سیگنال تشخیص داده شده توسط يك Repeater فوروارد خواهد شد . در صورت افت سیگنال (نویز و یا میرائی) ، Repeater مجدداً آن را احیاء و تولید می نماید .
- با استفاده از استانداردهای موجود حداکثر تعداد ايستگاه در هر سگمنت ، حداکثر طول هر سگمنت و حداکثر تعداد Repeater بین ايستگاه ها مشخص می گردد . ايستگاه هائی که توسط Repeater از یکدیگر جدا می شوند ، جملگی در يك Collision Domain مشابه قرار می گیرند (توجه داشته باشید که ايستگاه هائی که توسط Bridge و روتر از یکدیگر جدا می گردند در Collision Domain متفاوتی قرار می گیرند) .
- در لایه اول (فیزیکی) و بخش پائینی لایه دوم (Data link) مدل مرجع OSI از تکنولوژی های متفاوت اترنت استفاده می گردد . اترنت در لایه اول شامل ارتباط با رسانه انتقال داده ، سیگنال ها ، جریان پیوسته انتقال داده ، عناصری که سیگنال ها را بر روی رسانه انتقال داده قرار می دهند و تکنولوژی های متعدد دیگری است . اترنت لایه اول دارای يك نقش اساسی در مبادله اطلاعات بین دستگاه ها می باشد. در این رابطه محدودیت های خاصی نیز وجود دارد که لایه دوم با هدف غلبه بر محدودیت های فوق ، امکانات خاصی را ارائه می نماید :

لایه اول ، نمی تواند با لایه های بالاتر ارتباط برقرار نماید .
 لایه دوم از طریق LLC¹ با لایه بالاتر ارتباط برقرار می نماید .

لایه اول ، قادر به شناسائی کامپیوترها نمی باشد .
 لایه دوم از يك فرآیند آدرس دهی خاص استفاده می نماید .

لایه اول ، صرفاً قادر به تشریح جریان مستمر داده های صفر و يك است .

لایه دوم از فریم به منظور سازماندهی و گروه بندی بیت ها استفاده می نماید .

- زیر لایه های Data Link به منظور سازگاری بین تکنولوژی ها و مبادله اطلاعات بین کامپیوترها مطرح می گردند .
- زیر لایه MAC ، در ارتباط با عناصر فیزیکی است که از آنان به منظور مبادله اطلاعات استفاده می گردد .
- زیر لایه LLC ، مستقل از تجهیزات فیزیکی است و از آن به منظور فرآیند مبادله اطلاعات استفاده می گردد .

نامگذاری

- برای عرضه محلی فریم ها در اترنت ، می بایست از يك مدل آدرس دهی به منظور شناسائی کامپیوترها و اینترفیس ها استفاده گردد . اترنت از آدرس های MAC که طول آنان چهل و هشت بیتی است و به صورت دوازده رقم مبنای شانزده نمایش داده می شوند ، استفاده می نماید . اولین شش رقم مبنای شانزده که توسط موسسه IEEE مدیریت می گردد ،

¹Logical Link Control

- مسئولیت شناسائی تولید کننده را برعهده دارد . این بخش از آدرس MAC را OUI^۱ می گویند . شش رقم باقیمانده مبنای شانزده ، شماره سریال اینترفیس را مشخص می نماید .
- آدرس های MAC ، درون حافظه ROM نوشته شده و در زمان مقداردهی اولیه کارت شبکه در حافظه RAM مستقر می گردند . به آدرس های فوق BIA^۲ نیز گفته می شود.
- در لایه DataLink ، اطلاعات موردنیاز MAC (هدر و دنباله) به داده دریافتی از لایه بالاتر اضافه خواهد شد . اطلاعات فوق شامل اطلاعات کنترلی برای لایه Data در سیستم مقصد می باشد .
- کارت شبکه از آدرس MAC به منظور تشخیص محل ارسال پیام در لایه های بالاتر مدل مرجع OSI استفاده می نماید . کارت شبکه برای تشخیص فوق از پردازنده کامپیوتر استفاده نخواهد کرد . بدین ترتیب زمان مبادله اطلاعات در شبکه های اترنت بهبود پیدا خواهد کرد .
- در یک شبکه اترنت ، زمانی که یک دستگاه اقدام به ارسال داده می نماید ، می تواند یک مسیر ارتباطی را با سایر دستگاه ها با استفاده از آدرس MAC مقصد فعال نماید . دستگاه مبداء یک هدر را به آدرس MAC مقصد مورد نظر اضافه می نماید و داده را بر روی شبکه ارسال می نماید . به موازات انتشار داده بر روی محیط انتقال شبکه ، کارت شبکه هر یک از دستگاه های موجود در شبکه ، آدرس MAC اطلاعات ارسالی را بررسی تا تشخیص دهد که آیا این بسته اطلاعاتی برای وی ارسال شده است و یا خیر . در صورتی که آدرس MAC موجود در فریم با آدرس MAC کامپیوتر دریافت کننده مطابقت نماید ، کامپیوتر و یا دستگاه مقصد آن را دور خواهد انداخت . زمانی که داده به مقصد مورد نظر خود می رسد ، کارت شبکه یک نسخه از فریم را تکثیر و آن را در اختیار لایه های OSI قرار می دهد. در یک شبکه اترنت ، تمامی گره ها می بایست هدر MAC را بررسی نمایند (حتی در مواردی که گره های درگیر در مبادله اطلاعات در مجاورت فیزیکی یکدیگر باشند) .

^۱Organizational Unique Identifier

^۲burned-in addresses

- تمامی دستگاه های متصل شده به يك شبکه محلی اترنت دارای آدرس MAC می باشند (ایستگاه ها ، چاپگرها ، روترها و سوئیچ ها) .

فریم در لایه دوم

- برای رمز کردن و ارسال جریان مستمر بیت ها (داده) بر روی رسانه انتقال داده فیزیکی ، عملیات گسترده ای می بایست انجام شود ولی برای مبادله اطلاعات عملیات فوق به تنهایی کافی نمی باشد . با تعریف يك ساختمان داده خاص، امکان دریافت و ذخیره اطلاعات ضروری که امکان بدست آوردن آنان توسط بیت های رمز شده وجود ندارد ، فراهم می گردد . اطلاعات زیر نمونه هائی در این زمینه می باشد :

- کدام کامپیوتر در حال مبادله اطلاعات با کامپیوتر دیگری است .

- چه زمانی مبادله اطلاعات بین کامپیوترها شروع و چه زمانی خاتمه می یابد .

- ارائه روشی برای تشخیص خطاء که در زمان مبادله اطلاعات ممکن است اتفاق بیافتد .

- کدام کامپیوتر امکان استفاده از محیط انتقال را برای برقراری يك مبادله اطلاعات بدست گرفته است .

- فریم ، واحد داده در لایه دوم بوده و با استفاده از فرآیند framing تمامی عملیات کپسوله می گردد . هر استاندارد ممکن است ساختار خاصی را برای فریم تعریف کرده باشد . يك فریم از چندین بخش (فیلد) تشکیل می گردد . هر فیلد نیز از مجموعه ای بایت تشکیل شده است :

F	E	C	B	A
فیلد FCS	فیلد داده	فیلد نوع / طول	فیلد آدرس	فیلد شروع فریم

- زمانی که کامپیوترها به یک رسانه انتقال داده متصل می گردند ، می بایست آنان از روشی به منظور استفاده از محیط انتقال برای ارسال پیام و آگاهی به سایر کامپیوترها استفاده نمایند . در این رابطه از تکنولوژی های متعددی استفاده می گردد که هر یک دارای روشی مختص به خود برای انجام این فرآیند می باشند . تمامی فریم ها ، صرفنظر از نوع تکنولوژی ، دارای یک سیگنال آغازین مشتمل بر دنباله ای از بایت ها می باشند .
- تمامی فریم ها شامل اطلاعات نامگذاری نظیر نام گره مبداء (آدرس MAC) و نام گره مقصد (آدرس MAC) می باشند .
- اکثر فریم ها دارای تعدادی فیلد خاص نیز می باشند . در برخی تکنولوژی ها ، یک فیلد طول مسئولیت مشخص نمودن طول واقعی یک فریم بر حسب بایت را برعهده دارد . برخی فریم ها دارای یک فیلد "نوع" می باشند که پروتکل لایه سوم که درخواست را ارسال نموده است ، مشخص می نماید .
- علت ارسال فریم ها ، دریافت داده لایه های بالاتر از مبداء به مقصد مورد نظر است . بسته داده دارای دو بخش مجزاء می باشد : داده User Application و بایت های کپسوله شده برای ارسال به کامپیوتر مقصد . در این رابطه ممکن است بایت های دیگری نیز اضافه گردد. فریم ها دارای یک حداقل طول برای فرآیند تنظیم زمان می باشند . در فریم های استاندارد IEEE ، بایت های LLC نیز در فیلد داده قرار می گیرند . زیر لایه LLC ، داده پروتکل شبکه ، یک بسته اطلاعاتی IP را دریافت و اطلاعات کنترلی را به آن اضافه نموده تا شرایط مناسب برای توزیع بسته های اطلاعاتی به مقصد مورد نظر فراهم گردد .
- تمامی فریم ها به همراه بیت ها ، بایت ها و فیلدهای مربوطه مستعد خطا از منابع متعددی می باشند. فیلد FCS¹ شامل یک مقدار عددی است که توسط گره مبداء و بر اساس داده

¹Frame Check Sequence

موجود در فریم محاسبه می گردد . پس از محاسبه FCS ، مقدار استخراج شده به انتهای فریم ارسالی اضافه خواهد شد . زمانی که گره مقصد ، فریم را دریافت می نماید ، مجدداً مقدار FCS محاسبه و با مقدار موجود در فریم مقایسه می گردد . در صورتی که دو عدد با یکدیگر متفاوت باشند ، نشاندهنده بروز خطا در زمان ارسال اطلاعات می باشد . در چنین مواردی ، فریم دورانداخته شده و از گره مبدا درخواست می شود که مجدداً اطلاعات را ارسال نماید .

- برای محاسبه FCS از سه روش عمده استفاده می گردد :
روش اول : (CRC)^۱ ، محاسبات را بر روی داده انجام می دهد .
روش دوم : Two-dimensional parity : در این روش با اضافه کردن بیت هشتم ، زوج و یا فرد بودن تعداد یک های موجود در فریم مشخص می گردد .
روش سوم : Internet checksum : در این روش مقدار تمامی بیت های داده با یکدیگر جمع می گردد .

فریم ، واحد داده در لایه دوم مدل مرجع OSI است . در واقع ، فریم یک ساختمان داده خاص مشتمل بر چندین فیلد است که هر یک از آنان به منظور انجام وظایف تعریف شده ، تعداد مشخصی بایت را به خدمت خواهند گرفت . در ادامه به بررسی ساختمان داده فوق ، خواهیم پرداخت .

ساختار فریم اترنت :

- ساختار فریم در لایه Data Link ، تقریباً برای تمامی سرعت های اترنت (از ده تا ده هزار مگابیت در ثانیه) یکسان می باشد . این وضعیت در لایه فیزیکی وجود نداشته و هر یک از نسخه های اترنت دارای یک مجموعه قوانین جداگانه و مختص به خود می باشند .

^۱Cyclic Redundancy Check

FCS	محاسبه FCS					مقدمه
	Pad Data	طول / نوع	مبدأ	مقصد	شروع	
۴	۱۵۰۰ تا ۴۶	۲	۶	۶	۱	۷

- مقدمه (۵۶ بیت معادل هفت octet)
- شروع فریم (۸ بیت معادل يك octet)
- آدرس MAC مقصد (۴۸ بیت معادل شش octet)
- آدرس MAC مبدأ (۴۸ بیت معادل شش octet)
- طول / نوع (۱۶ بیت معادل دو octet)
- در صورتی که مقدار موجود در این فیلد کمتر از ۰۶۰۰ (مبنای شانزده) باشد، مقدار طول و در غیر اینصورت نوع پروتکل مشخص می گردد.
- داده (بین ۳۶۸ تا ۱۲۰۰۰ بیت، معادل چهل و شش تا یکهزار و پانصد octet)
- در صورتی که مقدار موجود در این فیلد کمتر از چهل و هشت octet باشد، می بایست يك Pad به انتها اضافه گردد.
- FCS (سی و دو بیت معادل چهار octet)

- در نسخه اترنت که توسط DIX پیاده سازی شده بود (قبل از ارائه نسخه ۸۰۲/۳ IEEE) ، مقدمه و شروع فریم در يك فیلد ترکیب می شدند . فیلد "طول / نوع" در نسخه های اولیه IEEE به عنوان "طول" و صرفاً در نسخه DIX به عنوان "نوع" در نظر گرفته شده بود .

FCS	محاسبه FCS				مقدمه
	Pad Data	نوع	مبداء	مقصد	
۴	۱۵۰۰ تا ۴۶	۲	۶	۶	۸

- مقدمه (۶۴ بیت معادل هشت octet)
- آدرس MAC مقصد (۴۸ بیت معادل شش octet)
- آدرس MAC مبداء (۴۸ بیت معادل شش octet)
- نوع (۱۶ بیت معادل دو octet)
- داده (بین ۳۶۸ بیت تا ۱۲۰۰۰ معادل چهل و شش تا یکهزار و پانصد octet)
- در صورتی که مقدار موجود در این فیلد کمتر از چهل و هشت octet باشد ، می بایست يك Pad به انتها اضافه گردد .
- FCS (سی و دو بیت معادل چهار octet)

- در اترنت II ، فیلد "نوع" ، در تعریف فریم ۳ . ۸۰۲ مورد توجه قرار گرفت . گره دریافت کننده با بررسی مقدار فیلد " طول / نوع " ، می بایست نوع پروتکل استفاده شده در لایه بالاتر موجود در فریم را تعیین نماید (مثلاً " x۰۸۰۰۰ ، پروتکل IPV۴ و X۸۰۶۰ پروتکل ARP) .
- در صورتی که مقدار موجود در این فیلد معادل X۶۰۰۰ (مبنای شانزده) و یا بزرگتر از آن باشد ، فریم بر اساس سیستم کدینگ اترنت دو تفسیر می گردد .

فیلدهای فریم اترنت

برخی فیلدهای ضروری در فریم های استاندارد ۳ . ۸۰۲ عبارتند از :

IEEE ۸۰۲/۳						
FCS	Data / Pad	طول / نوع	مقدمه	شروع	مقصد	مبداء
۴	۴۶ تا ۱۵۰۰	۲	۶	۶	۱	۷

Ethernet						
FCS	Data / Pad	طول / نوع	مقدمه	شروع	مقصد	مبداء
۴	۴۶ تا ۱۵۰۰	۲	۶	۶	۸	

- مقدمه (Preamble) ، يك الگوی متناوب مشتمل بر مجموعه ای از صفر و يك است که از آن برای همزمانی در سرعت های ده مگابیت در ثانیه و یا سرعت های پائین تر استفاده می شود . با توجه به این که نسخه های سریع تر اترنت همزمان می باشند به اطلاعات فوق نیاز نبوده و صرفاً جهت سازگاری با نسخه های قبلی استفاده می گردد.

PreambleField
۱۰۱۰۱۰ ۱۰۱۰۱۰ ۱۰۱۰۱۰ ۱۰۱۰۱۰ ۱۰۱۰۱۰ ۱۰۱۰۱۰
۱۰۱۰۱۰

- شروع فریم یا SFD^۱ از هشت بیت تشکیل شده است و مسئولیت آن مشخص کردن انتهای اطلاعات مربوط به زمانبندی است الگوی فوق به صورت ۱۰۱۰۱۱ می باشد .
- آدرس مقصد ، شامل آدرس MAC مقصد است . آدرس مقصد می تواند به صورت تکی (Unicast) ، گروهی (Multicast) و یا برای تمامی گره ها (broadcast) باشد .

^۱Start Frame Delimiter

- آدرس مبدا ، شامل آدرس MAC مبدا است . آدرس مبدا همواره به صورت تکی (Unicast) بوده و آدرس گره ارسال کننده اطلاعات را مشخص می نماید .
- طول / نوع برای دو هدف متفاوت استفاده می گردد . در صورتی که مقدار این فیلد کمتر از ۱۵۳۶ (مبنای ده) و یا ۶۰۰۰x (مبنای شانزده) باشد ، طول را مشخص می نماید . از فیلد فوق به عنوان "طول" زمانی استفاده می گردد که مسئولیت مشخص کردن پروتکل استفاده شده بر عهده لایه LLC باشد . مقدار موجود در این فیلد به عنوان "طول" ، تعداد بایت های داده را مشخص می نماید .
- در صورتی که مقدار این فیلد به عنوان "نوع" در نظر گرفته شود ، پروتکل لایه بالاتر که پس از تکمیل پردازش اترنت داده را دریافت می نماید ، مشخص می گردد .
- داده و Pad، هر طولی را می تواند داشته باشد مشروط به این که از حداکثر اندازه فریم تجاوز ننماید . حداکثر اطلاعاتی را که می توان در هر مرتبه ارسال نمود، یکهزار و پانصد octet می باشد. در صورتی که داده موجود در فیلد "داده" به حداقل مقدار لازم (چهل و شش octet) نرسیده باشد ، می بایست از Pad استفاده گردد .
- FCS از چهار octet تشکیل و شامل مقدار CRC است که توسط دستگاه فرستنده محاسبه و توسط دریافت کننده به منظور تشخیص بروز خطا در زمان ارسال اطلاعات ، مجدداً محاسبه می گردد . با توجه به این که خرابی صرفاً یک بیت از ابتدای فیلد "آدرس مقصد" تا انتهای فیلد "FCS" باعث محاسبه Checksum متفاوتی خواهد شد ، تشخیص این موضوع که اشکال مربوط به فیلد FCS و یا سایر فیلدهای شرکت کننده در محاسبه CRC است را غیر ممکن می نماید .

درس ۲

Token Ring

فن آوری Token Ring ابتدا توسط IBM در دهه ی ۱۹۷۰ ایجاد و گسترش یافت . TokenRing یک توپولوژی توانمند برای شبکه LAN بوده و برای مبادله ی حجم زیادی از اطلاعات طراحی شده است .

شبکه Token Ring در سال ۱۹۸۵ با سرعت ۴ Mbps عرضه شد . استاندارد IEEE ۸۰۲/۵ بر اساس مدل Token Ring شرکت IBM تعیین شد .

در سال ۱۹۸۹ شرکت IBM نوع دومی از Token Ring را با سرعت ۱۶ Mbps معرفی کرده و اخیرا ، استفاده از واژه Token Ring هم برای شبکه Token Ring شرکت IBM و هم برای استاندارد IEEE ۸۰۲/۵ شبکه ها مورد استفاده قرار می گیرد . البته بین استاندارد فوق و شبکه Token Ring شرکت IBM تفاوت زیادی وجود ندارد .

فن آوری Token Ring شامل یک حلقه و یک رسانه انتقال است . اتصال ایستگاه ها به حلقه از نظر فیزیکی شبیه توپولوژی ستاره ایی و از نظر منطقی شبیه توپولوژی حلقوی می باشد ، و در واقع دارای ترکیبی است .

شبکه Token Ring چگونه کار می کند ؟

شبکه Token Ring از نظر ظاهری یک شبکه ستاره ای است ولی به صورت TokenPassing کار می کند. در این شبکه یک حلقه منطقی به وجود می آید و Token در امتداد حلقه حرکت کرده و

به کامپیوترها می رسد. هر کامپیوتری که به ارسال اطلاعات نیاز داشته باشد، Token را نگه داشته و اطلاعات خود را به سوی مقصد ارسال می کند. اطلاعات ارسال شده در همان حلقه مجازی و در امتداد حرکت Token مسیر خود را طی می کند تا به کامپیوتر مقصد برسد، کامپیوتر مقصد در صورت صحیح بودن اطلاعات ارسالی، در جواب یک بسته به نام Acknowledge به کامپیوتر مبدأ ارسال می کند. کامپیوتر مبدأ نیز Token اصلی را از بین برده و یک Token جدید تولید می نماید و آن را در امتداد مسیر Token قبلی به حرکت در می آورد. این پروسه به همین صورت ادامه خواهد یافت.

در شبکه Token Ring در محل اتصال کامپیوترها به جای هاب از دستگاهی به نام MAU استفاده می شود. سرعت انتقال اطلاعات در این شبکه ۴ Mbps یا ۱۶ Mbps است. کارت های ۱۶ Mbps می توانند با سرعت ۴ Mbps نیز فعالیت کنند.

در شبکه Token Ring از کابل های زوج به هم تابیده استفاده می شود. اگر از کابل UTP در این توپولوژی استفاده شود، حداکثر طول کابل می تواند ۴۵ متر باشد و این شبکه فقط با سرعت ۴ مگابیت در ثانیه کار می کند و اگر از کابل STP استفاده شود، حداکثر طول کابل ۱۰۱ متر و با سرعت ۱۶ مگابیت در ثانیه اطلاعات منتقل می شود.

نمای ظاهری شبکه Token Ring

انواع کابل ها Token Ring :

در پیاده سازیهای Token Ring اصلی IBM، از یک سیستم کابل اختصاصی که توسط IBM طراحی شده است استفاده می شود. که آنها آن را Type ۱ خویش می نامند.

Type ۱. (ICSIBM Cabling System) یک کابل زوج به هم تابیده حفاظدار (STP) ۱۱۵۰ اهمی است که حاوی دو جفت سیم می باشد.

درگاههای یک MAU ۱ Type از اتصال دهنده های اختصاصی تحت عنوان (UDC) Universal Data Connector یا IBM Data Connector (IDC) استفاده می کنند و کارتهای واسط شبکه اتصال دهنده های DB۹ استاندارد را به کار می گیرند. کابلی که در دو سر خود IDC دارد و برای وصل کردن MAU ها به هم به کار می رود کابل تکه ای نامیده می شود. کابلی که در یک سر IDC و در سر دیگر DB۹ دارد و برای وصل کردن یک ایستگاه کاری به یک MAU به کار می رود کابل آویز نامیده می شود.

سیستم کابل کشی دیگری که در شبکه های Token Ring به کار می رود و IBM آن را ۳ Type نامیده است. از کابل زوج به هم تابیده بدون حفاظ (UTP) استاندارد استفاده می کنند. و برای آن Category توصیه می شود. مثل اترنت، Token Ring هم فقط از دو جفت از سیم های کابل استفاده می کند، یک جفت برای ارسال و جفت دیگر برای دریافت داده. سیستمهای کابل Type ۳ نیز، هم برای کابل های تکه ای و هم برای کابل های آویز از اتصال دهنده های RJ-۴۵ استاندارد استفاده می کنند. اما سیستم سیگنال رسانی که در لایه فیزیکی شبکه های Token Ring به کار می رود با اترنت متفاوت است، Token Ring از سیگنال رسانی منچستر تفاضلی، و اترنت از سیگنال رسانی منچستر استفاده می کند.

در دنیای Token Ring کابل کشی UTP ۳ Type تا حدود زیادی عرصه رقابت را بر ۱ Type تنگ کرده است. بیشتر به این دلیل که نصب آن خیلی آسانتر است. کابل ۱ Type در مقایسه با ۳ کلفت و نسبتاً نامنعطف می باشد و اتصال دهنده های IDC بزرگ هستند، به طوری که کابل کشی داخلی را با مشکل مواجه می کنند. اما کابل ۱ Type نسبت به ۳ Type می تواند در فواصل طولانی تری گسترده شود.

استانداردهای لایه فیزیکی برای شبکه های Token Ring به اندازه اترنت به طور دقیق مشخص نشده اند. در حقیقت استاندارد IEEE ۸۰۲/۵ یک جزوه کوچک است که اصولاً حاوی هیچ مشخصه لایه فیزیکی نمی باشد. انواع کابل و استانداردهای سیم کشی برای Token Ring از تجربیات لحاظ شده در محصولات ساخت IBM، ابداع کننده اولیه و پشتیبان پروتکل Token

Ring، اقتباس می شوند. در نتیجه در محصولاتی که سایر سازندگان می سازند ممکن است عناصر لایه فیزیکی متفاوتی توصیه شده باشند، مثلاً ممکن است طول کابل ها و حداکثر تعداد ایستگاههای کاری مجاز روی شبکه فرق داشته باشند.

NIC های Token Ring :

کارت های واسط شبکه برای سیستم های Token Ring از نظر ظاهری شبیه به NIC های اترنت هستند. در بیشتر کارت هایی که در حال حاضر در بازار وجود دارند از اتصال دهنده های RJ-45 برای کابل UTP استفاده می شود. هر چند اتصال دهنده های DB9 هم وجود دارند و اتصال دهنده های داخلی، همه سیستم های باس مهم، از جمله PCI و ISA را پشتیبانی می کنند.

هر آداپتور Token Ring یک مجموعه تراشه VLSI^۱ دارد، که از پنج CPU های مجزا تشکیل می شود و هر CPU دارای کد اجرایی، ناحیه ذخیره داده و فضای حافظه خاص خود می باشد. هر CPU با حالت یا عملکرد خاصی از آداپتور متناظر است. این پیچیدگی یکی از مهمترین دلایل گرانتر بودن NIC های Token Ring نسبت به NIC های اترنت است.

MAU های Token Ring :

برای حفظ همبندی حلقه، همه MAU های یک شبکه Token Ring باید با استفاده از درگاههای Ring in و Ring out که خاص این منظور است به هم وصل شوند.

MAU های یک شبکه Token Ring حلقه اصلی را تشکیل می دهند، که با اضافه شدن ایستگاههای کاری به شبکه، توسعه می یابد.

MAU های Token Ring (که نباید با هاب اترنت اشتباه شوند، زیرا آن را هم گهگاه MAU می خوانند، که به معنی واحد دستیابی به رسانه است) از چندین جنبه با هاب های اترنت تفاوت

^۱Very Large Scale Integration

اساسی دارند. اول اینکه MAU معمولاً یک وسیله غیرفعال است یعنی عمل تکرارکننده را انجام نمی دهد. دستورالعمل های کابل کشی شبکه های Token Ring بر اساس استفاده از MAU های غیر فعال هستند. اما MAU های تکرار کننده هم در بازار هستند، که با استفاده از آنها می توان طول کابل های شبکه را به بیش از آنچه که در استانداردها آمده است افزایش داد.

دوم اینکه درگاههای همه MAU ها در یک حالت دوربرگردان می مانند، تا اینکه توسط ایستگاه کاری که به آنها وصل شده است. مقداردهی اولیه شوند. در حالت دور برگردان، MAU سیگنال-هایی را که از یک درگاه دریافت می کند به طور مستقیم و بدون فرستادن آنها به روی کابل آویز به درگاه بعدی می فرستد. وقتی ایستگاه کاری راه اندازی مجدد می شود چیزی را تحت عنوان ولتاژ فانتوم به MAU ارسال می کند. ولتاژ فانتوم داده منتقل نمی کند. بلکه فقط MAU را از وجود ایستگاه کاری آگاه می نماید، تا MAU آن را به حلقه اضافه کند.

در شبکه های قدیمی تر 1 Token Ring Type باید هر درگاه MAU پیش از اتصال کابل آویز به آن، توسط مدیر و با استفاده از یک فیش «کلیدی» خاص به صورت دستی مقدار دهی اولیه شود. این مقدار دهی اولیه در Token Ring از اهمیت خاصی برخوردار است، زیرا شبکه به ایستگاه های کاری قبلی پس نگرفته است نمی تواند آن را برای ایستگاه کاری بعدی بفرستد. اگر قرار بود MAU بسته ای را از طریق یک درگاه به یک ایستگاه کاری خاموش و یا به جایی که ایستگاه کاری وجود ندارد بفرستد، بسته هرگز بر نمی گشت، حلقه شکسته می شد و شبکه از کار می افتاد، به دلیل نیاز به فرآیند مقدار دهی اولیه است که وصل کردن دو شبکه Token Ring به هم بدون MAU غیر ممکن است، کاری که با اترنت و یک کابل تقاطع می توان انجام داد.

بالاخره اینکه MAU ها همیشه دو درگاه برای وصل شدن به MAU های دیگر شبکه دارند. هاب های سیستم های اترنتی که همبندی ستاره دارند در یک ساختار ستاره سلسله مراتبی به هم وصل می شوند (که درخت شاخه کننده نیز نامیده می شود). که در آن هر هاب می تواند به چند هاب دیگر وصل شود. و هر یک از آنها نیز به نوبه خود به هاب های دیگری وصل می شوند. اما MAU های Token Ring همیشه به صورت حلقه به هم وصل می شوند. به این ترتیب که درگاه

Ring In هر MAU به MAU قبلی و درگاه Ring out به MAU ی بعدی وصل می شود. حتی اگر شبکه فقط دو MAU داشته باشد، باید با استفاده از دو کابل تکه ای درگاه Ring In هر یک را به درگاه Ring out دیگری وصل کرد.

هاب های اترنت با یک ساختار درخت شاخه کننده به هم وصل می شوند (چپ)، در حالی که MAU های Token Ring با یک حلقه به هم وصل می شوند.

اتصالات بین MAU های Token Ring تکراری هستند. یعنی اگر خرابی یک کابل یا اتصال دهنده باعث قطع اتصال بین دو تا از MAU ها شود. MAU های مجاور داده هایی که به آنها می رسند را در جهت دیگر در حلقه ارسال می نمایند، به طوری که بسته ها همیشه به همه ایستگاه های کاری وصل شده به شبکه می رسند. استانداردهای Token Ring در صورت وقوع این نوع خرابی برای تعیین کل طول مسیر داده از مشخصه ای تحت عنوان طول تنظیم شده حلقه (ARL) استفاده می کنند.

تبادل توکن :

درباره دستیابی به رسانه شبکه در یک شبکه Token Ring از طریق استفاده از یک بسته سه بیتی تحت عنوان توکن تصمیم گیری می شود. وقتی شبکه بی کار است گفته می شود که ایستگاههای کاری در مد تکرار بیت هستند، و به انتظار دریافت داده می باشند. توکن مرتباً از گره ای به گره دیگر به دور حلقه می چرخد، تا به یک ایستگاه کاری برسد که داده ای برای ارسال دارد. این ایستگاه کاری برای ارسال داده خویش یک بیت واریسی را در توکن تغییر می دهد تا نشان دهنده اشغال بودن شبکه باشد. و توکن را و بلافاصله پس از آن بسته داده خویش را به ایستگاه کاری بعدی می فرستد.

بسته ارسالی نیز به دور حلقه می چرخد. هر گره آدرس مقصد واقع در سرآیند فریم بسته را می خواند و یا پیش از ارسال آن به گره بعدی بسته را برای پردازش در بافرهای حافظه خود

می نویسد و یا اینکه آن را بدون پردازش ارسال می کند (این عمل را با عمل سیستم های اتونت مقایسه کنید که بسته هایی را که به مقصد آنها نیستند دور می ریزند.)

به این ترتیب بسته از تمام گره های شبکه می گذرد تا اینکه بازهم به دست ایستگاه کاری می رسد که آن را تولید کرده بود.

با دریافت بسته پس از پیمایش حلقه توسط آن، گره فرستنده، داده ورودی را با داده ای که در ابتدا ارسال کرده بود مقایسه می کند، تا ببیند که آیا در حین ارسال خطایی به وقوع پیوسته است یا خیر، اگر خطایی رخ داده باشد، کامپیوتر بسته را دوباره ارسال می کند در غیر این صورت کامپیوتر بسته را از روی شبکه بر می دارد و آن را دور می ریزد و سپس بیت واریسی توکن را به مقدار اولیه بر می گرداند تا آزاد بودن شبکه را نشان دهد، و توکن را ارسال می کند. این فرآیند همچنان در شبکه ادامه می یابد، در حالی که همه سیستم ها شانس مساوی برای ارسال خواهند داشت.

بیشتر سیستم های Token Ring ۱۶Mbps امروزی دارای یک ویژگی تحت عنوان آزادسازی زود رس توکن (ETR) هستند که در استاندارد اصلی وجود نداشته است و سیستم ارسال کننده را قادر می سازد که بلافاصله پس از بسته داده، و بدون اینکه صبر کند تا داده حلقه را ببیند، توکن «آزاد» را بفرستد (به جای اینکه قبل از بسته داده خویش را بفرستد و پس از آن یک توکن آزاد دیگر را ارسال نماید)، به این ترتیب وجود همزمان چند بسته داده روی شبکه ممکن خواهد بود، اما همچنان فقط یک توکن وجود خواهد داشت، آزادسازی زودرس بسته بعضی از تأخیرهای شبکه را که به هنگام انتظار سیستم ها برای فرا رسیدن توکن آزاد پیش می آید از بین می برد.

(آزاد سازی زود رس بسته فقط در شبکه های Token Ring ۱۶ Mbps ممکن است. سیستم هایی که از ETR استفاده می کنند می توانند با سیستم هایی که این کار را نمی کنند روی یک شبکه وجود داشته باشند)

از آنجا که فقط کامپیوتری که توکن را در دست دارد می تواند داده ارسال کند، در شبکه های Token Ring برخورد رخ نمی دهد، مگر اینکه یک اشکال جدی وجود داشته باشد، این بدان معنی است که شبکه می تواند بدون کاهش کارایی با حداثر ظرفیت خود کار کند، همان طور که یک شبکه اترنت چنین است. سیستم تبادل توکن، قطعی هم هست و این بدان معنی است که می تواند حداکثر مدت زمانی را که پیش از اینکه یک گره خاص بتواند به ارسال پردازد سپری می شود را محاسبه کند.

Token Ring تنها پروتکل لایه پیوند داده ای نیست که به عنوان روش کنترل دستیابی به رسانه خود از تبادل توکن استفاده می کند، FDDI و همچنین پروتکل های مهجوری همچون ARcent نیز از تبادل توکن استفاده می کنند. حتی لازم نیست که همبندی حلقه باشد تا بتوان از تبادل توکن استفاده کرد. استاندارد IEEE ۸۰۲/۴ مشخصه های یک شبکه تبادل توکن با همبندی باس را تعریف می کند، هر چند که چنین ساختاری در حال حاضر به ندرت به کار می رود.

وارد کردن سیستم به شبکه :

پیش از پیوستن به حلقه، هر ایستگاه کاری باید یک عملیات ۵ مرحله ای را بگذراند، که قابلیت سیستم برای کارکردن بر روی شبکه را مورد بررسی قرار می دهد این پنج مرحله عبارتند از :

۱- بررسی آویز رسانه : بررسی آویز رسانه قابلیت آداپتور شبکه برای ارسال و دریافت داده، و قابلیت کابل برای انتقال داده به MAU را تست می کند، بدین منظور در حالی که MAU سیگنال های ورودی را از طریق همان کابل که وارد می شود مرتباً برای سیستم پس می فرستد، ایستگاه کاری یک سری فریم های MAC Lobe Media Test را به آدرس همگانی می فرستد و آدرس خود را به عنوان آدرس مبدأ آنها قرار می دهد، سپس سیستم یک فریم MAC Duplication Address Test را که آدرس خودش هم به عنوان مبدأ و هم به عنوان مقصد در آن ذکر شده است ارسال می نماید، برای ورد به مرحله بعد سیستم باید توانسته باشد ۲۰۴۷ فریم MAC Lobe Media Test و یک فریم MAC Duplication Address Test را با موفقیت ارسال کند. این عمل

تست تنها می تواند دوباره تکرار شود و در صورتی که هر دوبار با شکست مواجه شود آدابتور از کار افتاده تلقی می شود.

۲- وارد کردن فیزیکی : در مدت فرآیند وارد کردن فیزیکی، ایستگاه کاری یک ولتاژ فانوم (یک سیگنال DC با ولتاژ کم که برای همه سیگنال های داده روی کابل نامرئی است) را از طریق کابل آویز به MAU می فرستد تا مداری که باعث می شود MAU سیستم را به حلقه اضافه کند را به کار اندازد.

پس از این کار ایستگاه کاری به انتظار علامتی به فریم^۱ AMP، SMP^۲ یا Ring Purge می ماند که نشان می دهد یک بازرس فعال روی شبکه حاضر است. اگر سیستم در مدت ۱۸ ثانیه یکی از این فریم ها را دریافت نکند یک فرآیند تعیین بازرس را به راه می اندازد. اگر فرآیند تعیین در مدت یک ثانیه به پایان نرسد، یا اگر ایستگاه کاری مزبور بازرس فعال شود و یک فرآیند تصفیه حقه را به راه اندازد که در عرض یک ثانیه به پایان نرسد، یا اگر ایستگاه کاری یک فریم MAC Beacon یا Remove Station را دریافت کند، اتصال به MAU باز نمی شود و سیستم به شبکه وارد نخواهد شد.

۳- درستی یابی آدرس : در این مرحله بررسی می شود که آیا ایستگاه کاری دیگری از حلقه دارای همین آدرس می باشد یا خیر، از آنجا که Token Ring آدرس های با مدیریت محلی (LAA) را پشتیبانی می کند، امکان این اتفاق وجود دارد . سیستم یکسری فریم های MAC DublicationAddress Test را مثل فریم های مرحله ۱ تولید می کند، فقط این فریم ها در کل شبکه توزیع می شوند. اگر سیستم دیگری با همین آدرس وجود نداشته باشد فریم های تست بر میگردند در حالی که مقدار بیت های ARI و FCI آنها صفر است، که در این صورت سیستم به مرحله بعد پیشروی می کند. اما اگر سیستم دو فریم تست با مقدار ۱ در بیت های ARI و FCI

^۱Active Monitor Present

^۲Standby Monitor Present

دریافت کند، یا اگر فریم های تست در مدت ۱۸ ثانیه برنگردند، فرآیند وارد کردن با شکست مواجه می شود و ایستگاه کاری از حلقه حذف می گردد.

۴- شرکت در عملیات حلقه : سیستم باید با موفقیت در یک عملیات حلقه شرکت نماید. به این ترتیب که یک فریم AMP یا SMP را که بیت های ARI و FCI آن صفر هستند بگیرد، این بیت ها را به ۱ تغییر دهد و فریم SMP خود را ارسال نماید. اگر ایستگاه کاری در عرض ۱۸ ثانیه یک فریم AMP یا SMP دریافت نکند فرآیندها وارد کردن با شکست مواجه می گردد و ایستگاه کاری از حلقه حذف می شود.

۵- تقاضا برای مقدار دهی اولیه : ایستگاه کاری چهار فریم MAC Request Initialization را به آدرس عملیاتی سرویس دهنده پارامتر حلقه شبکه (C ۰۰ ۰۰ ۰۰ ۰۰) ارسال می کند. اگر فریم ها با مقدار صفر در بیت های ARI و PCI برای سیستم پس فرستاده شوند که نشان دهنده عدم وجود سرویس دهنده پارامتر حلقه در حال کار است، آداپتور شبکه سیستم مقادیر پیش فرض خود را به کار می گیرد و مقداردهی اولیه (و همچنین کل فرآیند وارد نکردن سیستم) موفقیت آمیز تلقی می شود. اما اگر سیستم یکی از فریم ها را با مقدار ۱ در بیت های ARI و FCI آن دریافت کند (به نشانه اینکه یک سرویس دهنده پارامتر حلقه، فریم را دریافت کرده است) دو ثانیه به انتظار جواب می نشیند اگر پاسخی نیامد سیستم تا چهار بار دیگر سعی می کند، که اگر همگی با شکست مواجه شوند، مقدار دهی اولیه با شکست مواجه می گردد و ایستگاه کاری از حلقه حذف می شود.

حالت های سیستم :

هر سیستم Token Ring در طی عملکرد عادی خود وارد سه حالت عملیاتی مختلف می شود، که عبارتند از:

تکرار - در حالت تکرار، ایستگاه کاری تمام داده هایی را که از طریق درگاه دریافت به آن می‌رسند برای گره بعدی ارسال می‌کند، هرگاه خود ایستگاه کاری بسته ای برای ارسال داشته باشد بیت توکن بایت کنترل دستیابی فریم را به مقدار ۱ تغییر می‌دهد و به حالت ارسال وارد می‌گردد. در همین حین، تایمر حفظ توکن (THT) که ۸/۹ میلی ثانیه فرصت ارسال به سیستم می‌دهد مقدار صفر می‌گیرد.

ارسال - در حالت ارسال، ایستگاه کاری یک فریم را به روی شبکه می‌فرستد و توکن را آزاد می‌کند. پس از ارسال موفقیت آمیز فریم، ایستگاه کاری، پرکننده در حالت بیکاری (یک دنباله از یکها) را ارسال می‌کند تا اینکه به حالت تکرار باز گردد. اگر سیستم در حال ارسال، فریم MAC Beacon , Ring Purge یا Claim Token را دریافت کند، در ارسال وقفه وارد می‌کند و یک فریم Abort Delimiter را می‌فرستد تا حلقه را پاک کند.

پاک کردن - در همان زمان که درگاه ارسال ایستگاه کاری در حالت ارسال است. درگاه دریافت آن در حالت پاک کردن می‌باشد. با بازگشت داده ارسالی به ایستگاه کاری پس از پیمایش حلقه، سیستم آن را از روی شبکه پاک کند تا به چرخش خود ادامه ندهد، به محض اینکه سیستم، فیلد مرز پایان را در درگاه دریافت تشخیص بدهد، می‌فهمد که فریم با موفقیت پاک شده است و به حالت تکرار بر می‌گردد. اگر ۸/۹ میلی ثانیه فرصت ارسالی که THT داده است به پایان برسد ولی مرز پایان وارد نشود، سیستم پیش از بازگشت به حالت تکرار یک خطای فریم مفقود را در یک فریم Self ErrorReport برای ارسال در آینده ثبت می‌کند.

عملیات وارد کردن ایستگاه کاری به TokenRing تضمین می‌کند که تمام سیستم هایی که به حلقه وصل هستند درست کار می‌کنند

بازرسان Token Ring:

هر شبکه Token Ring سیستمی دارد که بازرسی فعال است و وظیفه آن حصول اطمینان از کارایی مناسب شبکه می‌باشد.

بازرس فعال هیچ برنامه یا سخت افزار خاصی ندارد و صرفاً تحت فرآیندی با عنوان تعیین بازرس به این سمت منصوب می شود. در این حالت همه سیستم های دیگر شبکه بازرس آماده باش هستند، تا اگر کامپیوتری که بازرس فعال است از کار افتاد وارد عمل شوند. عملیاتی که بازرس فعال انجام می دهد عبارتند از:

ارسال فریم های Active Monitor Present - هر هفت ثانیه یک بار، بازرس فعال (AM) قادر خواهد بود تا یک فریم MAC Active Monitor Present را ارسال کند که این فریم، فرآیند عملیات حلقه را به کار می اندازد.

نظارت بر عملیات حلقه AM- باید در عرض هفت ثانیه، پس از به راه اندازی فرآیند عملیات حلقه از گره ای که بلافاصله قبل از آن قرار دارد Active Monitor Present یا Standbymonitor Present را دریافت کند. اگر چنین نشود، AM یک خطای عملیات حلقه را ثبت می نماید.

تولید ساعت اصلی AM- یک سیگنال ساعت اصلی را تولید می کند که سایر ایستگاههای کاری شبکه از آن برای همگام کردن ساعتهاشان استفاده می کنند به این ترتیب اطمینان حاصل می شود که همه سیستم های شبکه می دانند هر بیت ارسالی چه زمانی شروع می شود و چه زمانی خاتمه می یابد. در ضمن به این ترتیب جیتر شبکه کاهش می یابد. جیتر عبارت است از شیفت فاز اندکی که با تکرار داده ارسالی توسط گره ها در شبکه به وقوع می پیوندد.

در اختیار گذاشتن بافر تاخیر- اگر حلقه کوچک باشد این مکان وجود دارد که یک ایستگاه کاری شروع به ارسال توکن نماید و پیش از اینکه ارسال به پایان برسد اولین بیت ارسال شود. AM با معرفی تاخیر انتشار حداقل ۲۴ بیت (که بافر تاخیر خوانده می شود) از این اتفاق جلوگیری می کند، تا اطمینان حاصل شود که توکن به درستی به دور شبکه می چرخد.

نظارت بر فرآیند تبادل توکن - بازرس فعال باید هر ۱۰ میلی ثانیه یکبار یک توکن خوب را دریافت نماید، که حاکی از عملکرد صحیح مکانیزم تبادل توکن است، اگر یک ایستگاه کاری اولویت توکن را بالا ببرد و نتواند آن را پایین بیاورد، یا اگر نتواند بسته خود را به طور کامل از روی حلقه پاک

کند، AM مشکل را تشخیص می دهد و با تصفیه حلقه تولید یک توکن جدید در صدد حل این مشکل بر می آید. تمام گره ها با دریافت فریم MACRing Purge از AM، کار خود را متوقف می کنند، تایمرهای خود را به مقدار اولیه بر می گردانند و به مد تکرار بیت وارد می گردد، تا برای دریافت یک بسته جدید آماده باشند.

عملیات حلقه :

عملیات حلقه فرآیندی است که طی آن هر گره شبکه Token Ring نزدیکترین همسایه فعال قبلی (NAUN) خود را شناسایی می کند. ایستگاه های کاری از این اطلاعات در طی فرآیند علامت دهی استفاده می کنند. تا محل یک خرابی شبکه را مجزا نمایند.

فرآیند عملیات حلقه توسط فریم MAC(AMP) Active Monitor Present که بازرسی فعال ارسال می کند به راه می افتد. این فریم حاوی دو بیت AddressRecognized(ARI) و Frame Copied(FCI) است، که هر دو مقدار صفر دارند.

اولین سیستم بعد از AM که این فریم را دریافت می کند مقدار بیت های ARI و FCI را یک می کند. در ضمن سیستم دریافت کننده آدرس سیستم فرستنده را به عنوان NAUN خود ثبت می نماید. این از آن روست که اولین ایستگاهی که فریم AMP را دریافت می کند می فهمد که فرستنده، نزدیکترین همسایه قبلی فعال اوست.

سیستم پس از ثبت آدرس NAUN خود یک فریم MAC از همین نوع را تولید می کند، فقط این فریم Standby Monitor Present(SMP) است، نه Active Monitor Present سیستم فریم SMP را ذخیره می کند تا آن را پس از یک تاخیر ۲۰ میلی ثانیه ای ارسال نماید، تا به سایر سیستم ها شانس برای فرستادن داده داده باشد. بدون این تاخیر، احتمال دارد که حلقه از بار

مربوط به عملیات حلقه انباشته شود، که این امر از ارسال به موقع بسته های داده جلوگیری به عمل می آورد.

سیستم پس از ذخیره، SMP، فریم AMP اصلی را برای سیستم بعدی ارسال می کند، از آنجا که اکنون مقدار بیت های ARI و FCI، یک است، هیچ یک از سیستم های بعدی کار خاصی انجام نمی دهند، غیر اینکه هر یک فریم را به سیستم بعدی تحویل دهند تا دور حلقه را بپیماید و دوباره به دست بازرسی فعال برسد، تا او آن را از روی شبکه پاک کند.

وقتی تاخیره ۲۰ میلی ثانیه ای به پایان برسد سیستم دوم بسته SMP را ارسال می کند و کل این فرآیند در مورد سیستم بعدی تکرار می شود سرانجام هر یک از سیستم های شبکه یک فریم SMP یا AMP را تولید خواهد کرد تا خود را به عنوان NAUN به سیستم بعدی بشناساند. هر گاه بازرسی فعال، یک بسته SMP با مقدار صفر در بیت های ARI و FCI را دریافت کند، می فهمد که فرآیند سرکشی به پایان رسیده است.

کل این عملیات نباید بیشتر از هفت ثانیه طول بکشد، در غیر اینصورت AM پیش از به راه اندازی مجدد این فرآیند یک خطای عملیات حلقه را ثبت می نماید. اگر هر یک از سیستم های شبکه نتواند در مدت ۱۵ ثانیه یک بسته AMP را دریافت نماید، فرض را بر این می گذارد که بازرسی فعال درست کار نمی کند و فرآیند تعیین را برای انتخاب یک AM جدید به راه می اندازد.

علامت دهی :

هر گاه یک ایستگاه شبکه Token Ring نتواند سیگنالی را روی درگاه دریافت خود تشخیص دهد، فرض را بر این می گذارد که شبکه مشکلی دارد و فرآیندی را تحت عنوان علامت دهی به راه می اندازد. این سیستم هر ۲۰ میلی ثانیه یکبار فریم های MAC علامت دهی را برای کل شبکه ارسال می کند (بدون اینکه توکنی را تسخیر کند) تا اینکه سیگنال دریافت دوباره ظاهر شود. هر ایستگاهی که به ارسال فریم علامت دهی می پردازد به طور خلاصه می گوید که نزدیکترین همسایه فعال قبلی او مشکلی دارد زیرا او سیگنالی را دریافت نمی کند. اگر NAUN هم شروع به

علامت دهی کند. معلوم می شود که مشکل از قبلی هاست. با ملاحظه اینکه کدامیک از ایستگاههای شبکه در حال علامت دهی هستند می توان سیستم یا قطعه کابل خراب را مجزا کرد. فریم های علامت دهی MAC چهار نوع هستند :

Set Recovery Mode (اولویت اول) – فریم SetRecovery Mode به ندرت دیده می شود زیرا توسط آداپتور Token Ring ایستگاه کاری ارسال نمی شود. این فریم فقط در فرآیند بازیابی که توسط یک محصول مدیریت شبکه متصل به شبکه آغاز می شود مورد استفاده قرار می گیرد.

Signal Loss (اولویت دوم) – فریم Signal loss وقتی تولید می شود که فرآیند تعیین بازرس به دلیل تمام شدن مهلت با شکست مواجه شده و سیستم در نتیجه عدم دریافت هیچ گونه سیگنالی از بازرس فعال به مد تعیین وارد شود وجود این فریم در شبکه معمولاً به معنی وقوع یک خرابی کابل یا یک خرابی سخت افزاری است.

Streaming Signal, Not Claim Token (اولویت سوم) – این فریم وقتی تولید می شود که فرآیند تعیین بازرس به دلیل تمام شدن مهلت با شکست مواجه شده و سیستم در مدت تعیین، هیچ فریم Claim Token-MAC دریافت نکرده باشد. اما اگر سیستم سیگنال ساعت را از بازرس فعال دریافت کرده باشد این فریم را تولید می کند و در غیر اینصورت فریم Signal loss تولید خواهد شد.

Claim token, Streaming Signal (اولویت چهارم) – این فریم وقتی تولید می شود که فرآیند تعیین بازرس به دلیل تمام شدن مهلت با شکست مواجه شده باشد و سیستم فریم های MAC-Claim Token را در مدت تعیین، دریافت کرده باشد. این فریم معمولاً نشان دهنده بروز یک مشکل گذاری ناشی از یک کابل خیلی دراز یا تداخل سیگنال به دلیل وجود نویز محیطی می باشد.

اگر سیستمی احتمال بدهد که ممکن است خود او منشأ مشکل شبکه باشد که منجر به علامت دهی شده است، خود را از روی حلقه بر می دارد تا ببیند آیا مشکل بر طرف می شود یا خیر، اگر سیستم به مدت بیش از ۲۶ ثانیه به ارسال فریم های علامت دهی بپردازد، یک تست خود حذفی با ارسال

علامت انجام می دهد. اگر سیستم ۸ فریم علامت متوالی را دریافت کند که او را به عنوان NAUN یک سیستم علامت دهنده مشخص می کنند، یک تست خود حذفی با دریافت علامت را انجام می دهد.

با تحلیل بسته های ارسالی در مدت علامت دهی می توان اطلاعات بیشتری درباره مشکل شبکه Token Ring کسب کرد.

فریم های TokenRing:

برخلاف شبکه های اتترنت که فقط یک فرمت فریم دارند، در شبکه های Token Ring از چهار نوع مختلف فریم استفاده می شود. نوع فریم داده تنها نوعی است که واقعاً به انتقال داده تولید شده توسط پروتکل های لایه های بالاتر می پردازد، فریم فرمان عملیات نگهداری و کنترل حلقه را انجام می دهد. فریم توکن ساختار دیگری است که فقط برای قضاوت درباره دستیابی به رسانه به کار می رود. و فریم abort delimiter فقط وقتی به کار می رود که انواع خاصی از خطا رخ داده باشد.

فریم داده :

فریم های داده Token Ring اطلاعات تولید شده توسط پروتکل های لایه های بالاتر را در واحد داده پروتکل (PDU) کنترل پیوند منطقی (LLC) استاندارد منتقل می کنند، درست همان طور که در استاندارد IEEE ۸۰۲/۲ تعریف شده است آنها عبارتند از :

مرز آغاز (SD) یک بایت - این فیلد آغاز فریم را مشخص میکند .

الگوی بیتی بایت به کاررفته در این فیلد JK۰JK۰۰۰۰ است، که در آن J ها نقص مقدار صفر و K ها نقش مقدار یک را کد می کنند.

فریم داده Token Ring اطلاعات تولید شده توسط پروتکل های لایه های بالاتر را منتقل می کند.

کنترل دستیابی (AC) یک بایت -الگوی بیتی بایت کنترل دستیابی PPPTMRRR است، که در آن P ها سه بیت اولویت هستند و R ها سه بیت رزرو می باشند که برای اولویت دهی به داده های ارسال شده به روی شبکه های Token Ring به کار می روند، سطح اولویت ایستگاه های کاری Token Ring می تواند از صفر تا ۷ باشد، که ۷ بالاترین اولویت است. هر سیستم تنها وقتی می تواند یک توکن آزاد را تسخیر کند و به ارسال داده بپردازد که اولویت آن توکن کمتر از اولویت خودش باشد. هر گاه اولویت گره از اولویت توکن آزاد بیشتر باشد او می تواند با تغییر بیت های اولویت توکن، اولویت او را افزایش دهد تا بسته های بعدی با سرعت بیشتری ارسال شوند.

وقتی توکن دوباره به دست سیستمی که اولویت را افزایش داده است می رسد، آن سیستم می تواند بسته دیگری را با همان اولویت ارسال کند و یا توکن را به اولویت قبلی اش بازگرداند و وضعیت او را به «آزاد» تغییر دهد. هرگاه سیستمی به دلیل پایین بودن اولویت خود توکن را نپذیرد می تواند بیت های رزرو را تغییر دهد و به این ترتیب توکنی با اولویت کمتر درخواست نماید. دو بیت دیگر فیلد AC، عبارتند از M, T. T به معنی بیت توکن است، که مقدار آن نشان می دهد فریم از نوع داده / فرمان است (1) یا یک فریم توکن است (0). M به معنی بیت نظارت می باشد و توسط سیستمی از شبکه که بازرس فعال است مقدار آن از صفر به یک تغییر داده می شود.

از آنجا که بازرس فعال تنها سیستمی است که قادر به تغییر مقدار این بیت می باشد. اگر بسته ای با مقدار یک در این بیت را دریافت کند فرض را بر این می گذارد که این بسته به دلیلی توسط گره فرستنده از روی شبکه برداشته نشده است و اشتباهاً در حال پیمایش حلقه برای دومین بار می باشد.

کنترل فریم (FC)، یک بایت -الگوی بیتی بایت کنترل فریم، TT00AAAA است، که T ها نشان می دهند حاوی فریم داده است یا فریم فرمان، بیت های سوم و چهارم بلا استفاده هستند و

همیشه مقدارشان صفر است. A ها بیت های کد توجه هستند که نوع خاصی از فریم MAC را مشخص می کنند که باید فوراً در بافر سریع سیستم دریافت کننده نوشته شود.

آدرس مقصد (DA)، شش بیت - این فیلد، با استفاده از آدرس سخت افزاری که در کارت واسط شبکه حک شده است و یا با استفاده از یک آدرس همگانی یا چند مقصدی دریافت کننده بسته را مشخص می کند.

آدرس مبدأ (SA)، شش بیت - این فیلد، با استفاده از آدرس سخت افزاری که در کارت واسط شبکه حک شده است، فرستنده بسته را مشخص می کند.

اطلاعات (INFO)، متغیر- در فریم داده، فیلد اطلاعات، حاوی واحد داده پروتکل است که از یک پروتکل لایه شبکه به پایین تحویل داده شده است، به علاوه یک سرآیند LLC استاندارد حاوی فیلدهای DSAP، SSAP و کنترل، اندازه فیلد اطلاعات می تواند تا ۳۵۰۰ بیت باشد و عامل محدود کننده آن زمان نگهداری توکن شبکه می باشد، که آن عبارت است از حداکثر مدت زمانی که یک ایستگاه کاری می تواند توکن را نگه دارد.

دنباله بررسی فریم (FCS) ۴ بیت - این فیلد حاوی ۴ بیت نتیجه محاسبه CRC بر روی فیلدهای کنترل فریم، آدرس مقصد، آدرس مبدأ و اطلاعات است. و برای بررسی ارسال موفقیت آمیز بسته به کار می رود. مقدار CRC توسط گره فرستنده محاسبه می شود و در فیلد FCS ذخیره می گردد. در مقصد، دوباره همین محاسبه بر روی فیلدها انجام می شود و با نتایج ذخیره شده مقایسه می گردد. همخوانی دو مقدار نشان دهنده ارسال موفقیت آمیز است.

مرز پایان (ED)، یک بیت - این فیلد، پایان بسته را مشخص می کند، به این ترتیب که قوانین سیگنال رسانی منچستر تفاضلی را نقض می کند، الگوی بیتی آن JKJKIE است. که J ها و K ها به ترتیب نقض یکها و صفرها را کد می کنند (مثل فیلد مرز آغاز).

I بیت فریم میانی است که اگر بسته های دیگری از همین دنباله متظر ارسال باشند مقدار آن ۱ می باشد. E بیت تشخیص خطاست، که سیستم دریافت کننده مقدار آن را ۱ می کند اگر یک خطای CRC را در ارسال تشخیص دهد. این کار سیستم های بعدی را از گزارش دادن همین خطا باز می دارد.

وضعیت فریم (FS)، یک بایت -الگوی بیتی این فیلد AF^{۰۰}AF^{۰۰} است، که A و F به ترتیب ARI^۱ و FCI^۲ می باشند. مقدار این بیت ها به این دلیل تکرار شده است که فیلد وضعیت فریم در بررسی CRC ی دنباله بررسی فریم لحاظ نمی شود. به هر دوی ARI و PCI توسط ایستگاه کاری فرستنده مقدار صفر داده می شود. اگر گره دریافت کنند، فریم را تشخیص دهد، مقدار ARI را ۱ می کند، اگر گره دریافت کننده بتواند فریم را در حافظه بافر آداپتور کپی کند مقدار FCI را ۱ می کند. عدم تغییر ای FCI نشان دهنده آن است که بررسی CRC روی فریم موفقیت آمیز نبوده یا بسته به طریقی آسیب دیده است و باید دوباره ارسال شود.

در مشخصه Token Ring چند آدرس عملیاتی فهرست شده است که نقشهای خاصی را که سیستم های خاصی از شبکه ایفا می کنند تعریف می کند. با استفاده از این آدرسها یک گره می-تواند پیغامها را به طور مستقیم به سیستمی که کار خاصی را انجام می دهد بفرستد، بدون اینکه لازم باشد آدرس سخت افزاری آن دستگاه را بداند این آدرس های از پیش تعریف شده عبارتند از:

بازرس فعال ۰۱ ۰۰ ۰۰ ۰۰ ۰۰ ۰۰ C

سرویس دهنده پارامتر حلقه ۰۲ ۰۰ ۰۰ ۰۰ ۰۰ ۰۰ C

بازرس خطای حلقه ۰۸ ۰۰ ۰۰ ۰۰ ۰۰ ۰۰ C

^۱Address Recognized Indicator

^۲Frame Copied Indicator

سرویس دهنده گزارش پیکربندی ۱۰۰۰۰۰۰۰۰۰ C

پل مسیر مبدأ ۱۰۰۰۰۰۰۰۰۰۰۰ C

فریم فرمان :

فریم های فرمان که فریم های MAC نیز خوانده می شوند، فقط در فیلد اطلاعات و گاهی فیلد کنترل فریم با فریم های داده فرق دارند. فریم های MAC سرآیند LLC ندارند. در عوض حاوی یک PDU ی دوبایتی هستند که طول اطلاعات کنترلی را که در ادامه می آیند نشان می دهد، و یک ID بردار اصلی دو بایتی که عملکرد کنترلی فریم را مشخص می کند و تعدادی متغیری بایت که حاوی خود اطلاعات کنترلی هستند .

فریم های MAC فقط عملیات نگهداری و کنترل حلقه را انجام می دهند. آنها هرگز به انتقال داده های لایه های بالاتر نمی پردازند و توسط پلها، سوئیچ ها یا مسیریابها به دامنه برخورد های دیگر انتشار نمی یابند. بعضی از رایجترین این عملیاتها فقط توسط یک کد چهاربیتی واقع در فیلد کنترل فریم مشخص می شوند، که از آن جمله می توان به موارد زیر اشاره کرد :

۰۰۱۰ Beacon

۰۰۱۱ Claim Token

۰۱۰۰ Ring purge

۰۱۰۱ Active Monitor Present

۰۱۱۰ Standby Monitor Present

بعضی از فریم های MAC که عملکرد خاصی دارند توسط آداپتورهای شبکه و با استفاده از ناحیه خاصی از حافظه به نام بافر سریع پردازش می شوند. به این ترتیب گره قادر خواهد بود فریم های MAC حاوی فرمانهای کنترلی مهم را در هر زمانی پردازش کند، حتی اگر مشغول دریافت تعداد زیادی فریم داده باشد.

فریم فرمان Token Ring پیغامهای کنترلی را منتقل می کند که برای انجام عملیات نگهداری حلقه به کار می روند.

فریم توکن :

فریم توکن بسیار ساده می باشد، و فقط از سه بایت تشکیل می شود: رمز آغاز، کنترل دستیابی و رمز پایان، بیت توکن واقع در فیلد کنترل دستیابی همیشه مقدار ۱ دارد .

فریم توکن برای کنترل دستیابی به رسانه شبکه به کار می رود.

فریم abort delimiter :

فریم abort delimiter فقط شامل فیلدهای رمز آغاز و رمز پایان است که همان فرمت فیلدهای معادل در فریم های داده و فرمان را دارند این نوع فریم اساساً وقتی به کار می رود که یک اتفاق غیر اتفاق غیرعادی رخ داده باشند، مثلاً وقتی ارسال یک بسته دچار وقفه و توقف زود هنگام شود. در این صورت بازرس فعال، یک فریم abortdelimiter را ارسال می کند که حلقه را تمیز می کند، به این ترتیب که همه داده هایی را که ارسال نامناسبی داشته اند بر می دارد و حلقه را برای ارسال بعدی آماده می کند.

فریم abort delimiter برای تمیز کردن حلقه پیش از تولید یک توکن جدید توسط بازرس فعال به کار می رود.

خطاهای TokenRing:

استاندارد IEEE ۸۰۲/۵ چند نوع خطای قابل حل را تعریف می کند که سیستم های شبکه می-توانند آنها را با استفاده از فریم های MAC به ایستگاه کاری که بازرس خطای حلقه است گزارش کنند، وقتی آداپتور Token Ring یک خطای قابل حل را تشخیص می دهد یک شمارش معکوس دو ثانیه ای را آغاز می کند، که در طی آن صبر می کند تا ببیند آیا خطای دیگری رخ می دهد، پس از آنکه دو ثانیه تمام شد، سیستم یک پیغام گزارش خطای قابل حل را به آدرس بازرس خطای حلقه (۰۸ ۰۰ ۰۰ ۰۰ ۰۰ ۰۰) می فرستد، انواع خطاهای قابل تشخیص توسط سیستم های Token Ring عبارتند از:

خطای فوران

خطای فوران وقتی اتفاق می افتد که سیستمی پنج نیمه زمان بیت (یعنی سه بیت ارسال شده) را تشخیص دهد که تغییر ساعت وسط بیت که لازمه سیستم کدگذاری منچستر تفاضلی است را نداشته باشند. این نوع خطا معمولاً ناشی از نویز روی کابل است که در نتیجه سخت افزار خراب یا تاثیرات محیطی دیگر حاصل می شود.

خطای خطی

خطای خطی وقتی اتفاق می افتد که یک ایستگاه کاری فریمی را دریافت کند که مقدار بیت تشخیص خطای آن (واقع در فیلد مرز پایان) ۱ باشد، یا به دلیل یک خطای CRC در دنباله بررسی فریم، و یا به خاطر اینکه یک بیت ناقص سیستم کدگذاری منچستر تفاضلی در فیلدی غیر از مرز آغاز و مرز پایان تشخیص داده شده است. شبکه ای که مشکلات نویزی دارد معمولاً به ازای هر ده خطای فوران یک خطای خطی خواهد داشت.

خطای فریم مفقود

خطای فریم مفقود وقتی اتفاق می افتد که سیستمی در مدت ۳ میلی ثانیه پس از ارسال یک فریم مهلتی که توسط تایمر بازگشت به تکرار (RRT) داده می شود. نتواند آن فریم را دریافت کند. علت این خطا می تواند نویز زیاد شبکه باشد.

خطای توکن

این خطا وقتی اتفاق می افتد که ۱۰ میلی ثانیه مهلتی که تایمر ارسال معتبر (VTX) بازرسی فعال می دهد به پایان برسد بدون اینکه فریمی دریافت شود، و لازم باشد که AM یک توکن جدید تولید کند. علت این خطا می تواند نویز زیاد شبکه باشد.

خطای داخلی

این خطا وقتی اتفاق می افتد که سیستمی در مدت عمل دستیابی مستقیم به حافظه (DMA) که بین آداپتور شبکه و کامپیوتر انجام می شود یک خطای توازن را تشخیص دهد. در این حالت ممکن است، مشکل ناشی از حافظه خود آداپتور و یا حافظه کامپیوتر باشد. اگر آداپتور را در سیستم دیگری نصب گردید و خطا تکرار شد، مشکل از خود کارت است.

خطای فرکانس

خطای فرکانس وقتی اتفاق می افتد که یک بازرسی آماده باش سیگنالی را دریافت کند که با فرکانس مورد انتظار بیشتر از یک مقدار خاص فرق داشته باشد. این خطا ممکن است به معنی این باشد که بازرسی فعال، سیگنال ساعت درستی را تولید نمی کند. در این صورت باید بازرسی فعال را خاموش کرد تا یک فرآیند تعیین آغاز شود. اگر دیگر خطای فرکانس رخ نداد معلوم می شود که آداپتور شبکه سیستمی که قبلاً بازرسی فعال بوده است بد کار می کرده است.

خطای AC

این خطا وقتی اتفاق می افتد که سیستمی دو فریم سرکشی شبکه متوالی با مقدار صفر در بیت های ARI و FCI را دریافت کند، و فریم اول آن AMP یا SMP باشد. از آنجا که نزدیکترین همسایه بعدی سیستم ارسال کننده فریم AMP یا SMP باید مقدار این بیت ها را تغییر دهد، هرگز نباید سیستمی دو فریم تغییر داده نشده را به این ترتیب دریافت کند. این خطا بدان معنی است که سیستمی که بلافاصله قبل از کامپیوتر تشخیص دهنده خطا قرار دارد احتمالاً به دلیل آداپتور شبکه خراب خود از تغییر بیت های ARI و FCI بازمانده است.

خطای FC

خطای FC^۱ وقتی اتفاق می افتد که سیستمی یک فریم MAC تک مقصدی با مقدار ۱ در بیت ARI را دریافت کند، که نشان دهنده وجود مشکل نویز یا وجود آدرس تکراری در شبکه است.

خطای ارسال abort delimiter

این خطا وقتی اتفاق می افتد که اوضاع شبکه، یک ایستگاه کاری را وادار کند تا ارسال را در وسط یک فریم متوقف کند و یک فریم abort delimiter تولید نمایند. این اتفاق وقتی می افتد که سیستم ارسال کننده، توکنی با رمز پایان نامعتبر یا یک فریم مطالبه توکن، علامت دهی و یا تصفیه حلقه را زمانی دریافت کند که منتظر رمز آغاز فریم ارسالی خودش است.

خطای تراکم دریافت

خطای تراکم دریافت وقتی اتفاق می افتد که سیستمی یک فریم تک مقصدی را دریافت کند، ولی به دلیل اینکه انباشته از فریم های ورودی است فضای بافری نداشته باشد تا بسته را در آن ذخیره کند.

درس ۳

Wireless Networking

تجهیزات و پیکربندی یک شبکه Wireless

سخت افزار مورد نیاز به منظور پیکربندی یک شبکه بدون کابل به ابعاد شبکه مورد نظر بستگی دارد. علیرغم موضوع فوق ، در این نوع شبکه ها اغلب و شاید هم قطعا" به یک access point و یک اینترفیس کارت شبکه نیاز خواهد بود . در صورتی که قصد ایجاد یک شبکه موقت بین دو کامپیوتر را داشته باشید ، صرفا" به دو کارت شبکه بدون کابل نیاز خواهید داشت .

Access Point چیست ؟

سخت افزار فوق ، به عنوان یک پل ارتباطی بین شبکه های کابلی و دستگاههای بدون کابل عمل می نماید . با استفاده از سخت افزار فوق ، امکان ارتباط چندین دستگاه به منظور دستیابی به شبکه فراهم می گردد . access point می تواند دارای عملکردی مشابه یک روتر نیز باشد . در چنین مواردی انتقال اطلاعات در محدوده وسیعتری انجام شده و داده از یک access point به access point دیگر ارسال می گردد .

یک نمونه دستگاه access point



کارت شبکه بدون کابل

هر یک از دستگاههای موجود بر روی یک شبکه بدون کابل ، به یک کارت شبکه بدون کابل نیاز خواهند داشت . یک کامپیوتر Laptop ، عموماً دارای یک اسلات PCMCIA است که کارت شبکه درون آن قرار می گیرد . کامپیوترهای شخصی نیز به یک کارت شبکه داخلی که معمولاً دارای یک آنتن کوچک و یا آنتن خارجی است ، نیاز خواهند داشت . آنتن های فوق بر روی اغلب دستگاهها ، اختیاری بوده و افزایش سیگنال بر روی کارت را بدنبال خواهد داشت .

یک نمونه کارت شبکه بدون کابل



پیکربندی یک شبکه بدون کابل

به منظور پیکربندی یک شبکه بدون کابل از دو روش متفاوت استفاده می گردد :

- روش Infrastructure: به این نوع شبکه ها، hosted و یا managed نیز گفته می شود . در این روش از یک و یا چندین access point (موسوم به gateway و یا روترهای بدون کابل) که به یک شبکه موجود متصل می گردند ، استفاده می شود . بدین ترتیب دستگاههای بدون کابل، امکان استفاده از منابع موجود بر روی شبکه نظیر چاپگر و یا اینترنت را بدست می آورند .

• روش Ad-Hoc : به این نوع شبکه ها ، unmanaged و یا peer to peer نیز گفته می شود. در روش فوق هر یک از دستگاهها مستقیما" به یکدیگر متصل می گردند. مثلا" یک شخص با دارا بودن یک دستگاه کامپیوتر laptop مستقر در محوطه منزل خود می توانند با کامپیوتر شخصی موجود در منزل خود به منظور دستیابی به اینترنت ، ارتباط برقرار نماید .

پس از تهیه تجهیزات سخت افزاری مورد نیاز به منظور ایجاد یک شبکه بدون کابل ، در ادامه می بایست تمامی تجهیزات تهیه شده را با هدف ایجاد و سازماندهی یک شبکه به یکدیگر متصل تا امکان ارتباط بین آنان فراهم گردد . قبل از نصب و پیکربندی یک شبکه بدون کابل ، لازم است به موارد زیر دقت نمائید :

- تهیه درایورهای مربوطه از فروشنده سخت افزار و کسب آخرین اطلاعات مورد نیاز.
- فاصله بین دو کامپیوتر می بایست کمتر از یکصد متر باشد .
- هر یک از کامپیوترهای موجود می بایست بر روی یک طبقه مشابه باشند .
- استفاده از تجهیزات سخت افزاری مربوط به یک تولید کننده ، دارای مزایا و معایبی است .
- در این رابطه پیشنهاد می گردد لیستی از ویژگی های هر یک از سخت افزارهای مورد نیاز عرضه شده توسط تولید کنندگان متعدد تهیه شود تا امکان مقایسه و اخذ تصمیم مناسب، فراهم گردد .

مراحل لازم به منظور نصب یک شبکه (فرضیات : ما دارای یک شبکه کابلی موجود هستیم و قصد پیاده سازی یک شبکه بدون کابل به منظور ارتباط دستگاههای بدون کابل به آن را داریم) :

- اتصال accesspoint به برق و سوکت مربوط به شبکه اترنت .
- پیکربندی access point (معمولا" از طریق یک مرورگر وب) تا امکان مشاهده آن توسط شبکه موجود فراهم گردد . نحوه پیکربندی accesspoint بستگی به نوع آن دارد.
- پیکربندی مناسب کامپیوترهای سرویس گیرنده به منظور ارتباط با access point (در صورتی که تمامی سخت افزارهای شبکه بدون کابل از یک تولید کننده تهیه شده باشند ،

عموماً با تنظیمات پیش فرض هم می توان شبکه را فعال نمود . به هر حال پیشنهاد می گردد همواره به راهنمای سخت افزار تهیه شده به منظور پیکربندی بهینه آنان ، مراجعه گردد) .

انواع شبکه های Wireless

امروزه از شبکه های بدون کابل (Wireless) در ابعاد متفاوت و با اهداف مختلف، استفاده می شود . برقراری یک تماس از طریق دستگاه موبایل ، دریافت یک پیام بر روی دستگاه pager و دریافت نامه های الکترونیکی از طریق یک دستگاه PDA ، نمونه هایی از کاربرد این نوع از شبکه ها می باشند . در تمامی موارد فوق ، داده و یا صوت از طریق یک شبکه بدون کابل در اختیار سرویس گیرندگان قرار می گیرد. در صورتی که یک کاربر ، برنامه و یا سازمان تمایل به ایجاد پتانسیل قابلیت حمل داده را داشته باشد، می تواند از شبکه های بدون کابل استفاده نماید . یک شبکه بدون کابل علاوه بر صرفه جوئی در زمان و هزینه کابل کشی ، امکان بروز مسائل مرتبط با یک شبکه کابلی را نخواهد داشت .

از شبکه های بدون کابل می توان در مکان عمومی ، کتابخانه ها ، هتل ها ، رستوران ها و مدارس استفاده نمود . در تمامی مکان های فوق ، می توان امکان دستیابی به اینترنت را نیز فراهم نمود . یکی از چالش های اصلی اینترنت بدون کابل ، به کیفیت سرویس (QoS) ارائه شده برمی گردد . در صورتی که به هر دلیلی بر روی خط پرازیت ایجاد گردد ، ممکن است ارتباط ایجاد شده قطع و یا امکان استفاده مطلوب از آن وجود نداشته باشد .

انواع شبکه های wireless

- **Wireless Local Area Networks :WLANS** . شبکه های فوق ، امکان دستیابی کاربران ساکن در یک منطقه محدود نظیر محوطه یک دانشگاه و یا کتابخانه را به شبکه و یا اینترنت ، فراهم می نماید .
- **Wireless Personal Area Networks :WPANS** . در شبکه های فوق ، امکان ارتباط بین دستگاههای شخصی (نظیر laptop) در یک ناحیه محدود (حدود ۹۱۴ سانتی متر) فراهم می گردد . در این نوع شبکه ها از دو تکنولوژی متداول IR^۱ و (Bluetooth) IEEE ۸۰۲/۱۵ ، استفاده می گردد .
- **Wireless Metropolitan Area Networks :WMANS** . در شبکه های فوق ، امکان ارتباط بین چندین شبکه موجود در یک شهر بزرگ فراهم می گردد . از شبکه های فوق، اغلب به عنوان شبکه های backup کابلی (مسی ، فیبر نوری) استفاده می گردد .
- **Wireless Wide Area Networks :WWANS** . در شبکه های فوق ، امکان ارتباط بین شهرها و یا حتی کشورها و از طریق سیستم های ماهواره ای متفاوت فراهم می گردد . شبکه های فوق به سیستم های G۲ (نسل دوم) معروف شده اند .

امنیت:

برای پیاده سازی امنیت در شبکه های بدون کابل از سه روش متفاوت استفاده می شود :

- **Wired Equivalent Privacy : WEP** . در روش فوق ، هدف توقف ره گیری سیگنال های فرکانس رادیویی توسط کاربران غیر مجاز بوده و برای شبکه های کوچک مناسب است . علت این امر به عدم وجود پروتکل خاصی به منظور مدیریت "کلید" بر می گردد. هر "کلید" می بایست به صورت دستی برای سرویس گیرندگان تعریف گردد. بدیهی است در صورت بزرگ بودن شبکه ، فرآیند فوق از جمله عملیات وقت گیر برای هر مدیر شبکه خواهد بود . WEP ، مبتنی بر الگوریتم رمزنگاری RC۴ است که توسط RSA Data System ارائه

^۱Infra Red

شده است . در این رابطه تمامی سرویس گیرندگان و AccessPoint ها بگونه ای پیکربندی می گردند که از یک کلید مشابه برای رمزنگاری و رمزگشائی استفاده نمایند .

- SSID^۱: روش فوق به منزله یک "رمزعبور" بوده که امکان تقسیم یک شبکه WLAN به چندین شبکه متفاوت دیگر که هر یک دارای یک شناسه منحصر بفرد می باشند را فراهم می نماید . شناسه های فوق، می بایست برای هر access point تعریف گردند. یک کامپیوتر سرویس گیرنده به منظور دستیابی به هر شبکه ، می بایست بگونه ای پیکربندی گردد که دارای شناسه SSID مربوط به شبکه مورد نظر باشد . در صورتی که شناسه کامپیوتر سرویس گیرنده با شناسه شبکه مورد نظر مطابقت نماید ، امکان دستیابی به شبکه برای سرویس گیرنده فراهم می گردد .

- فیلترینگ آدرس های MAC^۲: در روش فوق ، لیستی از آدرس های MAC مربوط به کامپیوترهای سرویس گیرنده، برای یک AccessPoint تعریف می گردد . بدین ترتیب ، صرفاً به کامپیوترهای فوق امکان دستیابی داده می شود . زمانی که یک کامپیوتر درخواستی را ایجاد می نماید ، آدرس MAC آن با آدرس MAC موجود در Access Point مقایسه شده و در صورت مطابقت آنان با یکدیگر ، امکان دستیابی فراهم می گردد . این روش از لحاظ امنیتی شرایط مناسبی را ارائه می نماید ، ولی با توجه به این که می بایست هر یک از آدرس های MAC را برای هر Access point تعریف نمود ، زمان زیادی صرف خواهد شد . استفاده از روش فوق، صرفاً در شبکه های کوچک بدون کابل پیشنهاد می گردد .

^۱Service Set Identifier

^۲Media AccessControl

فصل ۶

لایه شبکه

پروتکل لایه شبکه مسئول مشخص کردن مسیر مبداء و مقصد اطلاعات میباشد. تفاوت این لایه با لایه پیوند داده ها این است که در لایه پیوند داده ، که تنها با انتقال بسته ها به سیستم های دیگر بر روی شبکه محلی (LAN) کار خود را به پایان میرسانند اما این لایه پا را از شبکه های محلی فراتر می گذارد. در این فصل به بررسی پروتکل های لایه شبکه میپردازیم.

درس ۱

ip

پروتکل اینترنت که به آن IP گفته می شود یکی از مهم ترین چارچوب های فناوری اطلاعات است که قرار گرفتن آن کنار پروتکل TCP و ایجاد TCP / IP به شکل گیری پروتکل اینترنت منجر شده است. این پروتکل یکی از پرکاربردترین پروتکل هاست و به همین دلیل اطلاعات کافی از اجزای تشکیل دهنده آن، در امنیت فناوری اطلاعات بسیار لازم و ضروری به شمار می رود؛ چرا که امروزه بسیاری از حملات بزرگ اینترنتی با تغییر در فیلدهای آن صورت می گیرند.

پروتکل اینترنت

IP نشانی عددی است که به هر سیستم در شبکه، برای ارتباط با سایر اجزای آن شبکه اختصاص داده می شود. منظور از اجزای شبکه، مسیریاب ها، سوئیچ ها، مودم ها، رایانه های سرویس دهنده و رایانه های سرویس گیرنده هستند. این نشانی عددی می تواند ثابت بوده یعنی به صورت دستی روی تک تک اجزای شبکه تنظیم شود یا به صورت متغیر و پویا باشد و توسط سرور DHCP که وظیفه اختصاص IP را دارد، به اجزای شبکه تخصیص داده شود.

پروتکل اینترنت، وظیفه حمل و انتقال بسته های حاوی اطلاعات و مسیریابی آنها را در یک شبکه، از مبدا تا مقصد به عهده دارد IP. پس از دریافت اطلاعات از TCP، به قطعه قطعه کردن و تبدیل آنها به بسته های کوچک تری به نام FRAGMENT اقدام کرده سپس برای هر یک از این فراگمنت ها، یک بسته IP می سازد که حاوی اطلاعات مورد نیاز بسته برای حرکت در طول شبکه است. آن گاه این بسته ها را به بسته TCP اضافه کرده و شروع به ارسال آنها می کند. سپس این بسته ها بر اساس تنظیم های قسمت ابتدایی شان، از طریق مسیریاب های موجود در شبکه به مقصد خود هدایت می شوند.

با توجه به این که IP بر اساس ساختاری استاندارد شکل گرفته است، بنابراین با تمام سیستم های عامل موجود در شبکه بخوبی کار کرده و نیاز به هیچ نوع سخت افزاری در شبکه ندارد. نمونه های خاصی از آدرس های IP وجود دارند که برای هدف های ویژه ای در نظر گرفته شده اند و برای تعریف اجزای شبکه نمی توان از آنها استفاده کرد.

از نمونه این نشانی ها می توان به ۰/۰/۰ (برای زمانی که سیستم میزبان از IP خود بی اطلاع است که البته اگر از آن به عنوان نشانی فرستنده استفاده شود، هیچ جوابی برای فرستنده ارسال نمی شود)، ۲۵۵/۲۵۵/۲۵۵ (برای ارسال پیام به صورت عمومی و فراگیر در شبکه)، ...

ساختار بسته های IP

بسته های ساخته شده توسط IP، از تعدادی فیلد مجزا تشکیل شده که هر کدام در بردارنده اطلاعات ویژه ای است. این اطلاعات، در زمان های لازم از فیلدهای قرار داده شده در داخل بسته ها استخراج شده و مورد استفاده قرار می گیرند. این اطلاعات شامل مواردی همچون آدرس IP رایانه فرستنده و گیرنده، نوع پروتکل IP و... است که در قسمت های بعدی، این فیلدها بررسی می شوند.

0				1					2					3							
0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1
Version				IHL					TOS/DSCP/ECN					Total Length							
Identification										Flags		Fragment Offset									
Time To Live				Protocol					Header Checksum												
Source Address											Destination Address										
Options										Padding											

فیلد VERSION

این فیلد وظیفه مشخص کردن نوع پروتکل IP را به عهده دارد. قابل ذکر است اکنون دو نسخه از IP وجود دارد که با نام های ۴ و ۶ شناخته می شوند. نسخه IP۴، حداکثر ۶۴ کیلوبایت فضا را اشغال می کند که این تعداد در نسخه ۶، دو برابر است (هر چند در حالت عادی حجم بسته ها در IP نسخه ۴ حدود ۱۶۰۰ بایت است و از آن بیشتر نمی شود!). اندازه فیلد VERSION، چهار بیت است.

فیلد IHL

این فیلد وظیفه نگهداری اندازه قسمت بالایی بسته را دارد که از آن برای تعیین مرز بین اطلاعات و محتویات بسته IP استفاده می شود. اندازه این فیلد نیز چهار بیت است.

فیلد TYPE OF SERVICE

این فیلد وظیفه تعیین نوع سرویس انتقال بسته ها را به عهده دارد که این نوع سرویس، «کم سرعت و مطمئن (TCP)» و «پرسرعت و نامطمئن (UDP)» یا ترکیبی از این دو (RTP) را شامل می شود. اندازه این فیلد، هشت بیت است.

فیلد TOTAL LENGTH

در این فیلد اندازه کل بسته IP قرار دارد که شامل قسمت های سرآیند داده است و می تواند ۶۵۵۳۵ بیت باشد. اندازه این فیلد، ۱۶ بیت است.

فیلد FRAGMENT OFFSET

این فیلد به سه بخش تقسیم می شود که عبارت است از:

۱. بیت: Dont Fragment (DF) اگر مقدار این بیت یک باشد به معنای آن است که هیچ مسیریابی حق شکستن این بسته را ندارد.

۲. بیت: More Fragment (MF) اگر مقدار این بیت صفر باشد به معنای آن است که این قطعه، آخرین قطعه ارسال شده از اطلاعات است.

۳. بیت: Fragment Offset (FO) این بیت دربردارنده شماره قطعه های شکسته شده است. از آنجا که اندازه این فیلد، ۱۳ بیت است اطلاعات می توانند تا ۸۱۹۲ قطعه شکسته شوند که البته اندازه هر قطعه غیر از قطعه آخر باید ضربی از ۸ باشد.

فیلد TIME TO LIVE

این فیلد وظیفه تعیین زمان سرگردانی بسته در شبکه را به عهده دارد. به این معنی که آن بسته برای رسیدن به مقصد می تواند از چند مسیر عبور کند، که البته بیشترین مقدار آن ۲۵۵ است. معمولاً از این فیلد برای از بین بردن بسته های سرگردان در شبکه استفاده می شود.

فیلد PROTOCOL

این فیلد، شماره پروتکلی را مشخص می کند که قرار است بسته به آن برسد.

فیلد HEADER CHECKSUM

از این فیلد برای کشف خطا استفاده می شود.

فیلد SOURCE ADDRESS

این فیلد وظیفه نگهداری نشانی IP مبدا را به عهده دارد. فایروال ها و نرم افزارهای فیلترینگ از این فیلد برای مسدود کردن نشانی های اینترنتی استفاده می کنند.

فیلد DESTINATION ADDRESS

در این فیلد، نشانی IP سیستم مقصد وجود دارد.

فیلد OPTION

این فیلد به صورت خالی بوده و از آن برای نوشتن توضیحات دلخواه استفاده می شود.

فیلد PAYLOAD

در این فیلد، داده ها بین لایه های مختلف و از لایه های بالایی به سمت لایه های پایینی، رد و بدل می شوند.

درس ۲

آدرس دهی IP

بمنظور مدیریت و اشکال زدائی شبکه های مبتنی بر پروتکل TCP/IP ، می بایست شناخت مناسبی نسبت به تمامی جنبه های آدرس دهی IP وجود داشته باشد. یکی از مهمترین عملیات مدیریتی در شبکه های مبتنی بر پروتکل TCP/IP ، نسبت دهی آدرس های IP مناسب و منحصر بفرد به تمامی گره های موجود در شبکه است . با اینکه مفهوم نسبت دهی آدرس IP ، ساده بنظر می آید ولی مکانیزم واقعی اختصاص آدرس IP موثر با استفاده از Subnetting ، پیچیدگی های خاص خود را بدنبال دارد. علاوه بر موارد فوق ، ضروری است که شناخت مناسبی نسبت به جایگاه IP Broadcast ، ترافیک multicast و نحوه تطبیق آدرس های فوق به آدرس های لایه اینترفیس شبکه نظیر آدرس های MAC اترنت و Token Ring ، وجود داشته باشد .

انواع آدرس های IP

آدرس IP ، یک آدرس منطقی سی و دو بیتی است که می تواند یکی از انواع زیر باشد :

- Unicast . یک آدرس IP از نوع Unicast ، به یک اینترفیس شبکه متصل شده به یک شبکه مبتنی بر IP نسبت داده می شود. آدرس های IP از نوع Unicast در ارتباطات "یک به یک" (One-To-One) استفاده می گردند .
- Broadcast . یک آدرس IP از نوع Broadcast بمنظور پردازش توسط هر گره موجود بر روی سگمنت یکسان شبکه ، طراحی شده است . آدرس های IP از نوع Broadcast در ارتباطات از نوع "یک به همه" (one-to-everyone) ، استفاده می گردند .
- Multicast . یک آدرس IP از نوع Multicast ، آدرسی است که یک و یا چندین گره را قادر به گوش دادن به سگمنت های مشابه و یا متفاوت می نماید. آدرس های فوق ، ارتباط از نوع "یک به چند" (one-to-many) را فراهم می نمایند .

تبدیل از باینری به دهدهی:

بمنظور تبدیل یک عدد باینری به معادل دهدهی ، با توجه به ارزش مکانی هر رقم از توان های متفاوت دو استفاده می گردد . در چنین حالتی در صورتیکه یک رقم دارای مقدار یک باشد ، از معادل ارزش مکانی آن (توان های متفاوت دو) استفاده می گردد . شکل زیر یک عدد هشت بیتی و ارزش مکانی هر رقم با توجه به موقعیت آن در عدد باینری را نشان می دهد .

7	6	5	4	3	2	1	0
2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
128	64	32	16	8	4	2	1

مثلاً ، عدد هشت بیتی ۰۱۰۰۰۰۱۱ ، معادل ۶۷ ($۱ + ۲ + ۶۴$) می باشد . حداکثر عددی را که می توان توسط هشت بیت نشان داد (۱۱۱۱۱۱۱) ، ۲۵۵ است ($۱ + ۲ + ۴ + ۸ + ۱۶ + ۳۲ + ۶۴ + ۱۲۸$) .

تبدیل از دهدهی به باینری :

برای تبدیل یک عدد دهدهی به باینری ، عدد دهدهی را بمنظور آگاهی از وجود توان های متفاوت دو و از بیت با ارزش بالا ، آنالیز می نمائیم . از بیت با ارزش بالاتر شروع می کنیم (۱۲۸) ، در صورتیکه مقدار مربوط در عدد دهدهی موجود باشد ، بیت مورد نظر در آن موقعیت معادل یک در نظر گرفته خواهد شد . مثلاً عدد ۲۱۱ شامل حاصل جمع اعداد ۱۲۸ ، ۶۴ ، ۱۶ و ۲ است ، بنابراین شکل باینری آن بصورت ۱۱۰۱۰۰۱۱ خواهد بود .

آدرس های IP در IP Header:

آدرس های IP استفاده شده در IP Header ، شامل فیلدهای مربوط به آدرس مبدا و مقصد می باشد :

- فیلد آدرس مبدا IP Header ، همواره یک آدرس از نوع Unicast و یا آدرس خاصی بصورت IP: ۰/۰/۰/۰ است . آدرس نامشخص IP ۰/۰/۰/۰ ، صرفاً زمانی که گره مربوطه با یک آدرس IP پیکربندی نشده باشد و گره در تلاش برای بدست آوردن یک

آدرس از طریق یک پروتکل پیکربندی نظیر DynamicHost Configuration (DHCP Protocol) باشد، استفاده می گردد.

- فیلد آدرس مقصد IPHeader، یک آدرس Unicast و یا یک آدرس از نوع Broadcast می باشد.

آدرس های IP از نوع Unicast

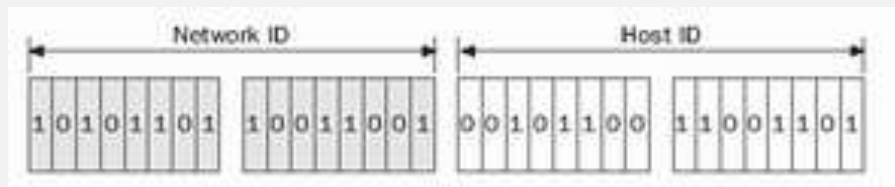
هر اینترفیس شبکه که TCP/IP در ارتباط با آن فعال شده باشد، می بایست دارای یک آدرس IP منحصر بفرد، منطقی و Unicast باشد. آدرس منحصر بفرد Unicast، بمنزله یک آدرس منطقی خواهد بود. چراکه آدرس فوق در لایه اینترنت بوده که هیچگونه ارتباط مستقیمی با آدرس استفاده شده در لایه اینترفیس شبکه ندارد. مثلاً "آدرس IP نسبت داده شده به یک میزبان (host) بر روی یک شبکه اترنت، هیچگونه ارتباطی با آدرس MAC چهار و هشت بیتی استفاده شده توسط آداپتور شبکه اترنت ندارد.

آدرس IP از نوع Unicast، یک آدرس منحصر بفرد برای گره های موجود در یک شبکه مبتنی بر پروتکل TCP/IP بوده و از دو بخش مشخصه شبکه (network ID) و مشخصه میزبان (host ID)، تشکیل می گردد.

- مشخصه شبکه (network ID) و یا آدرس شبکه، گره هائی را که بر روی شبکه منطقی یکسانی قرار دارند، مشخص می نماید. در اکثر موارد، یک شبکه منطقی مشابه یک سگمنت فیزیکی شبکه بوده که محدوده های مرزی آن توسط آدرس IP روترها تعریف می گردد. در برخی موارد، چندین شبکه منطقی بر روی شبکه فیزیکی یکسانی وجود داشته که از روشی با نام Multinetting استفاده می نمایند. تمامی گره ها در یک شبکه منطقی یکسان، مشخصه شبکه (Network ID) یکسانی را به اشتراک می گذارند. در صورتیکه تمامی گره ها بر روی یک شبکه منطقی یکسان، بدرستی پیکربندی نگردند (عدم لحاظ نمودن مشخصه شبکه یکسان)، عملیات روتینگ و عرضه بسته های اطلاعاتی با مشکل مواجه خواهد شد. مشخصه شبکه، می بایست منحصر بفرد در نظر گرفته شود.

- مشخصه میزبان (host ID) و یا آدرس میزبان ، یک گره موجود در شبکه را مشخص می نماید . یک گره می تواند یک روتر و یا یک میزبان (یک ایستگاه کاری ، سرویس دهنده و یا سایر سیستم های مبتنی بر TCP/IP) باشد . مشخصه میزبان ، می بایست در هر سگمنت شبکه منحصر بفرد باشد .

شکل زیر ، نمونه ای از یک آدرس IP به همراه مشخصه های شبکه و میزبان را نشان می دهد :



درس ۳

کلاس های آدرس دهی IP

در ابتدا لازم است به این نکته اشاره گردد که شبکه های مدرن ، مبتنی بر کلاس های آدرس اینترنت نمی باشد . با توجه به رشد سریع اینترنت ، ساختار اولیه ارائه شده مبتنی بر کلاس ، شرایط لازم بمنظور گسترش و پاسخگویی به یک شبکه گسترده جهانی را دارا نمی باشد. مثلاً" در صورتیکه همچنان از آدرس دهی مبتنی بر کلاس ، استفاده شود، می بایست صدها و یا هزاران روتر در جداول روتینگ مربوط به روترهای ستون فقرات اینترنت وجود داشته باشد . بمنظور پیشگیری و ممانعت از این موضوع ، آدرس دهی در اینترنت مدرن بصورت Classless خواهد بود. علیرغم موارد فوق ، آشنائی و آگاهی لازم در خصوص کلاس های آدرس دهی ، یکی از عناصر مهم در زمینه شناخت آدرس دهی IP محسوب می گردد.

RFC ۷۹۱ ، آدرس های IP از نوع Unicast را کلاس های آدرس دهی خاصی تعریف می نماید که از آنان بمنظور ایجاد شبکه ها با ابعاد و اندازه های متفاوت استفاده می گردد(توانائی تعریف مناسب شبکه ها) . اهداف اولیه طراحی کلاس های آدرس دهی ، نیل به خواسته های زیر بود :

- ایجاد تعدادی اندک از شبکه های وسیع (شبکه هائی با تعداد زیادی از گره ها) .
- ایجاد تعدادی متوسط از شبکه هائی با ابعاد متوسط (نه خیلی زیاد و نه خیلی کم) .
- ایجاد تعدادی زیاد از شبکه های کوچک .

برای تامین اهداف فوق ، کلاس های متفاوت آدرس دهی ایجاد گردید . بدین ترتیب ، زیر شاخه (نوع) یک آدرس سی و دو بیتی IP از طریق تنظیم بیت های با ارزش بالا مشخص و سایر بیت های باقیمانده به دو بخش مشخصه شبکه و مشخصه میزبان ، تقسیم می گردند .

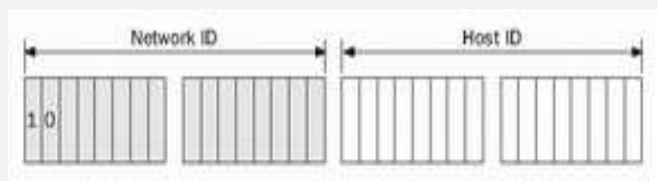
کلاس A

آدرس های کلاس A ، برای شبکه هائی که دارای تعداد بسیار زیادی میزبان می باشند، طراحی شده است (ایجاد تعدادی اندک از شبکه هائی که دارای میزبانان زیادی می باشند) . بیت با ارزش بالا مقدار صفر را دارا خواهد بود . اولین گروه هشتگانه (اولین octet) ، بعنوان مشخصه شبکه و آخرین بیست و چهار بیت (سه octet بعد) بعنوان مشخصه میزبان تعریف می گردد . شکل زیر ساختار آدرس های کلاس A را نشان می دهد .



کلاس B

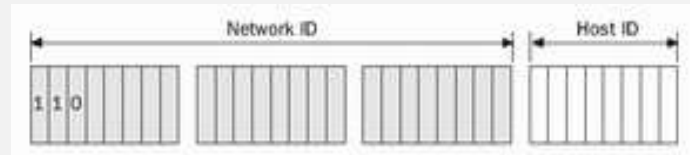
آدرس های کلاس B ، برای شبکه هائی با ابعاد متوسط که دارای تعداد متوسطی (نه خیلی زیاد و نه خیلی کم) از میزبانان می باشند ، طراحی شده است (ایجاد تعدادی متوسط از شبکه هائی که دارای میزبانان متوسطی می باشند) . دو بیت با ارزش بالا ، دارای مقدار ۱۰ می باشد . اولین شانزده بیت (دو octet اولیه) بعنوان مشخصه شبکه و آخرین شانزده بیت (دو octet آخر) بعنوان مشخصه میزبان در نظر گرفته می شوند. شکل زیر ساختار آدرس های کلاس B را نشان می دهد .



کلاس C

آدرس های کلاس C برای شبکه های کوچک که دارای تعداد اندکی از میزبانان می باشند ، طراحی شده است . (ایجاد تعدادی زیادی از شبکه هائی که دارای میزبانان اندکی می باشند) . سه بیت با ارزش بالا ، دارای مقدار ۱۱۰ می باشد . اولین بیست و چهار بیت (سه octet اولیه) بعنوان

مشخصه شبکه و هشت بیت آخر (آخرین Octet) بعنوان مشخصه میزبان در نظر گرفته می شوند. شکل زیر ساختار آدرس های کلاس C را نشان می دهد .



کلاس های آدرس دهی اضافه : علاوه بر کلاس های آدرس دهی A, B و C ، با توجه به ضرورت های

مربوطه کلاس D و E ، نیز تعریف شده اند .

کلاس D : آدرس های کلاس D بمنظور Multicast طراحی شده اند . چهار بیت با ارزش بالا، دارای مقدار ۱۱۱۰ می باشد. بیست و هشت و بیت بعد بمنظور آدرس های multicast در نظر گرفته شده است .

کلاس E : آدرس های کلاس E ، آدرس های رزرو شده برای استفاده آتی می باشند . پنج بیت با ارزش بالا، دارای مقدار ۱۱۱۱۰ می باشد .

قوانین مشخصه شبکه (Network ID)

در زمان استفاده از مشخصه شبکه ، قوانین زیر رعایت می گردد:

- مشخصه شبکه نمی تواند با ۱۲۷ بعنوان اولین Octet آغاز گردد . تمامی آدرس های IP: ۱۲۷.x.x.x ، بعنوان آدرس های Loopback رزرو شده می باشند .
- تمامی بیت های مشخصه شبکه ، نمی تواند ارزش یک را داشته باشد. مشخصه های شبکه که مقدار تمامی بیت های آن یک است ، بمنظور آدرس های Broadcast رزرو شده اند .
- تمامی بیت های مشخصه شبکه ، نمی تواند ارزش صفر را داشته باشد. مشخصه های شبکه که مقدار تمامی بیت های آن صفر است ، یک میزبان بر روی شبکه محلی را مشخص می نمایند.
- مشخصه شبکه در شبکه های مبتنی بر IP عمومی ، می بایست منحصر بفرد باشد .

جدول زیر محدوده کلاس های آدرس دهی برای مشخصه شبکه را نشان می دهد.

تعداد شبکه ها	آخرین مشخصه شبکه	اولین مشخصه شبکه	کلاس
۱۲۶	۱۲۶/۰/۰	۱/۰/۰	A
۱۶۳۸۴	۱۹۱/۲۵۵/۰	۱۲۸/۰/۰	B
۲۰۹۷۱۵۲	۲۲۳/۲۵۵/۲۵۵	۱۹۲/۰/۰	C

IP مربوط به مشخصه های شبکه ، حتی اگر بصورت اعداد دهدهی که توسط نقطه از یکدیگر جدا شده اند ، ارائه گردد ، بمنزله آدرس های IP نسبت داده شده به اینترفیس های شبکه در نظر گرفته نخواهد شد . IP مشخصه شبکه ، آدرس شبکه ای است که برای تمامی اینترفیس های شبکه متصل شده به یک شبکه منطقی یکسان ، مشترک خواهد بود .

قوانین مشخصه های میزبان (Host ID)

در زمان استفاده از مشخصه میزبان ، قوانین زیر رعایت می گردد :

- تمامی بیت های مشخصه میزبان ، نمی تواند ارزش یک را داشته باشد . مشخصه های میزبان که مقدار تمامی بیت های آن یک است ، برای آدرس های Broadcast رزو شده اند .
- تمامی بیت های مشخصه میزبان ، نمی تواند ارزش صفر را داشته باشد . مشخصه های میزبان که مقدار تمامی بیت های آن صفر است ، برای ارائه IP مربوط به مشخصه های شبکه ، رزو شده اند .
- مشخصه میزبان می بایست در شبکه ، منحصر بفرد باشد .

جدول زیر محدوده کلاس های آدرس دهی برای مشخصه میزبان را نشان می دهد.

تعداد میزبانان	آخرین مشخصه میزبان	اولین مشخصه میزبان	کلاس
۱۶'۷۷۷'۲۱۴	w.۲۵۵/۲۵۵/۲۵۴	w.۰/۰/۱	A
۶۵'۵۳۴	w.x.۲۵۵/۲۵۴	w.x.۰/۱	B
۲۵۴	w.x.y.۲۵۴	w.x.y.۱	C

درس ۴

SubnetMask

سیستم ها برای تشخیص تعلق یا عدم تعلق به يك شبکه از مفهومی به نام Subnet Mask استفاده می کند. به این صورت که تمام بیت های Network را ۱ و تمام بیت های Host را ۰ در نظر می گیرد تا Subnet mask را بسازد .

در نظر داشته باشید که هر کلاسی که ما میتونیم از شون به عنوان یک آدرس استفاده کنیم یک SubnetMask استاندارد داره به عبارت دیگر هر ip دارای یک SubnetMask است و برای کلاس هایی که در بالا گفته شد این SubnetMask ها به صورت استاندارد زیر هستند :

Standard Subnet Masks:

Class A : ۲۵۵/۰/۰

Class B : ۲۵۵/۲۵۵/۰

Class C: ۲۵۵/۲۵۵/۲۵۵/۰

نکته: IP هادر صورت قابل نمایش هستند

۱. subnet mask format

۲. prefix format

در subnet mask format ، آی پی مربوطه را به صورت یک ip به همراه subnet mask آن به صورت جداگانه نمایش می دهیم. یعنی یک عدد که IP را نشان میدهد و عددی دیگر یا IP دیگر subnet mask را به عنوان مثال :

IP: ۱۹۲,۱۶۸,۱,۲

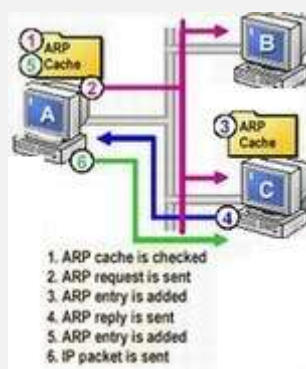
Subnet mask: ۲۵۵,۲۵۵,۲۵۵,۰

در prefix format آی پی و subnet mask آن را با هم در یک ip نشان می‌دهید ، یعنی بعد از ip ، یک / (که جداکننده Ip از عدد مربوط به subnet mask هست) قرار می‌دهیم و سپس یک عدد نوشته میشود که این عدد تعداد ۱ هایی که در subnet mask همان ip داریم می باشد به طور مثال :

۱۹۲,۱۶۸,۱,۲/۲۴

درس ۵

پروتکل ARP



پروتکلی است که مسئولیت مسئله " نام به آدرس " (ARP) Address Resolution Protocol را در رابطه با بسته های اطلاعاتی خروجی (Outgoing)، برعهده دارد. ماحصل فرآیند فوق Mapping آدرس IP به آدرس (Media Access Control) MAC، مربوطه است. کارت شبکه از آدرس MAC، بمنظور تشخیص تعلق یک بسته اطلاعاتی به کامپیوتر مربوطه، استفاده می نمایند. بدون آدرس های MAC، کارت های شبکه، دانش لازم در خصوص ارسال بسته های اطلاعاتی به لایه بالاتر بمنظور پردازش های مربوطه را دارا نخواهند بود. همزمان با رسیدن بسته های اطلاعاتی به لایه IP بمنظور ارسال در شبکه، آدرس های MAC مبداء و مقصد به آن اضافه می گردد.

ARP، از جدولی خاص بمنظور ذخیره سازی آدرس های IP و MAC مربوطه، استفاده می نماید. محلی از حافظه که جدول فوق در آنجا ذخیره می گردد، ARP Cache نامیده می شود. ARP Cache هر کامپیوتر شامل mapping لازم برای کامپیوترها و روترهایی است که صرفاً بر روی یک سگمنت مشابه قرار دارند.

پروتکل ARP ، آدرس IP مقصد هر یک از بسته های اطلاعاتی خروجی را با ARP Cache مقایسه تا آدرس MAC مقصد مورد نظر را بدست آورد . در صورتیکه موردی پیدا گردد ، آدرس MAC از Cache بازیابی می گردد . در غیر اینصورت ؛ ARP درخواستی را برای کامپیوتری که مالکیت IP را برعهده دارد ، Broadcast نموده و از وی می خواهد که آدرس MAC خود را اعلام نماید . کامپیوتر مورد نظر (با IP مربوطه) ، در ابتدا آدرس MAC کامپیوتر ارسال کننده درخواست را به Cache خود اضافه نموده و در ادامه پاسخ لازم را از طریق ارسال آدرس MAC خود ، به متقاضی خواهد داد . زمانیکه پاسخ ARP توسط درخواست کننده ، دریافت گردید ، در ابتدا با استناد به اطلاعات جدید دریافتی، Cache مربوطه بهنگام و در ادامه بسته اطلاعاتی به مقصد کامپیوتر مورد نظر ارسال می گردد .

در صورتیکه مقصد یک بسته اطلاعاتی ، سگمنتی دیگر باشد ، ARP ، آدرس MAC را به روتر مسئول در سگمنت مربوطه ، تعمیم خواهد داد (در مقابل آدرس مربوط به کامپیوتر مقصد) . روتر ، در ادامه مسئول یافتن آدرس MAC مقصد و یا Forwarding بسته اطلاعاتی برای روتر دیگر است .

در شکل زیر ساختار درونی بسته ARP تشریح شده است

Hardware type (16 bits)	
Protocol type (16 bits)	
Length of hardware address	Length of protocol address
Operator (16 bits)	
Hardware address of the sender	
IP address of the sender	
Hardware address of the receiver	
IP address of the receiver	

Hardware Type: شماره مشخصه نوع سخت افزار کارت شبکه که در لایه اول وظیفه انتقال اطلاعات روی کانال فیزیکی را بر عهده دارد.

Protocol Type: نوع پروتکلی که در لایه اینترنت از آن استفاده می شود. برای شبکه های مبتنی بر TCP/IP این شماره ۲۰۴۸ است.

Hardware Address Length: با توجه به آنکه طول آدرس های فیزیکی در شبکه ها، متفاوت است در این فیلد طول آدرس (بر حسب بایت) مشخص می شود.

Protocol Address Length: طول آدرس های IP که در پروتکل TCP/IP مقدار ۴ است.

Operation Code: ۱ برای ARP request و مقدار ۲ برای ARP reply

Source Hardware Address: آدرس فیزیکی مبدا

Source IP Address: آدرس IP ماشین مبدا

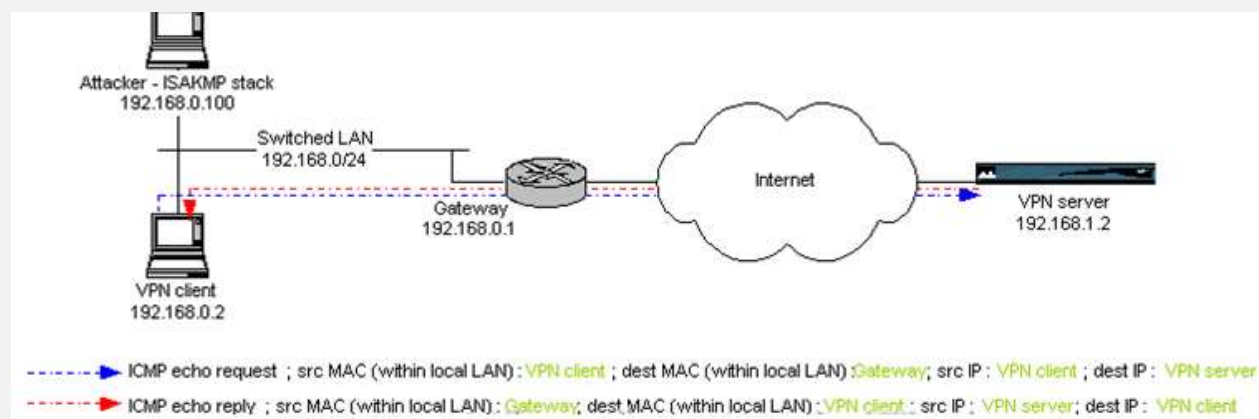
Destination Hardware Address: آدرس فیزیکی ماشین مقصد

Destination IP Address: آدرس IP ماشین مقصد

درس ۶

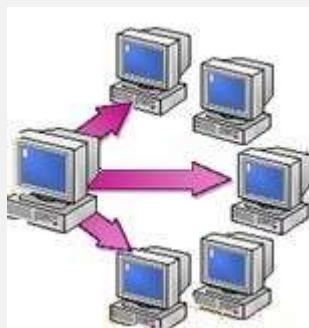
پروتکل ICMP

وظیفه این پروتکل ارائه گزارش خطا و عیب یابی در صورتی که اطلاعات به صورت صحیح توزیع نشوند را دارد این سیستم گزارش خطا بر روی IP نصب می شود تا در صورت وقوع هرگونه خطا به فرستنده پیام مناسب را بدهد که این گزارشات برای مدیران شبکه دارای اهمیت است. البته میتوانیم بگوییم تعدادی از این پیام ها بین دستگاه های شبکه مثل روترها ارسال و دریافت میشود تا این دستگاه ها بتوانند همدیگر را از بروز خطا مطلع کنند ، حالا اگر بخواهیم بدونیم این پیام ها چه هستند باید بگوییم پیام Echo یکی از مهم ترین آنها است و همچنین دستور پرکاربرد PING. ضمناً دستور PING را در محیط Command Prompt (CMD) باید اجرا کرد .



درس ۷

پروتکل IGMP



IGMP (Internet Group Management Protocol) ، پروتکلی است که مدیریت لیست اعضا برای IP Multicasting ، در یک شبکه TCP/IP را بر عهده دارد . IP Multicasting ، فرآیندی است که بر اساس آن یک پیام برای گروهی انتخاب شده از گیرندگان که گروه multicast نامیده می شوند ؛ ارسال می گردد . IGMP لیست اعضا را نگهداری می نماید .

مدیریت IP Multicasting

تمامی اعضا یک گروه multicast ، به ترافیک IP هدایت شده به یک آدرس MulticastIP ، گوش داده و بسته های اطلاعاتی ارسال شده به آن آدرس را دریافت می نمایند. زمانیکه چندین کامپیوتر نیازمند دستیابی به اطلاعاتی نظیر Streaming media باشند، یک آدرس IP رزوشده برای multicasting استفاده می گردد. روترها که بمنظور پردازش multicast پیکربندی می گردند، اطلاعات را انتخاب و آنها را برای تمامی مشترکین گروه multicast ارسال (Forward) می نمایند . بمنظور رسیدن اطلاعات Multicast به گیرندگان مربوطه ، هر یک از روترهای موجود در مسیر ارتباطی می بایست ، قادر به حمایت از Multicasting باشند . کامپیوترهای مبتنی بر سیستم عامل وینوز ۲۰۰۰ ، قادر به ارسال و دریافت IP Multicast ، می باشند .

فصل ۷

لایه انتقال

در این فصل به بررسی دو پروتکل که در لایه حمل و نقل با پروتکل های لایه شبکه برای ارائه خدمات مورد استفاده قرار میگیرند میپردازیم.

درس ۱

TCP

در شبکه های رایانه ای، لایه انتقال سرویس های ارتباطی مبدأ به مقصد یا end-to-end را برای برنامه های کاربردی موجود در معماری لایه بندی شده پروتکل ها و اجزاء شبکه فراهم می آورد. لایه انتقال سرویس های مطمئنی از قبیل پشتیبانی از جریان داده اتصال گرا، قابلیت اطمینان، کنترل جریان و تسهیم یا مالتی پلکسینگ را ارائه می نماید.

لایه های انتقال هم در (RFC ۱۱۲۲) مدل TCP/IP، که مبنا و بنیان اینترنت می باشد، و هم مدل OSI موجود می باشند. تعریف لایه انتقال در این دو مدل کمی با یکدیگر تفاوت دارد.

معروف ترین پروتکل لایه انتقال پروتکل کنترل انتقال یا (TCP) Transmission Control Protocol می باشد. این پروتکل نام خود را از مجموعه پروتکل اینترنت یا همان TCP/IP وام گرفته است. از این پروتکل در انتقال های اتصال گرا استفاده می شود در حالیکه پروتکل بدون اتصال UDP برای انتقال های پیام ساده مورد استفاده قرار می گیرد. پروتکل پیچیده تری است و این پیچیدگی به واسطه طراحی وضعیت محوری است که در سرویس های انتقال قابل اطمینان و جریان داده تعبیه شده است. از دیگر پروتکل های عمده در این گروه می توان به پروتکل کنترل ازدحام دیتاگرام.

(Stream) (DCCP) Datagram Congestion Control Protocol و پروتکل انتقال کنترل جریان (Control Transmission Protocol) اشاره نمود.

سرویس ها:

سرویس های زیادی وجود دارد که می تواند توسط یک پروتکل در لایه انتقال ارائه شود که می توان به موارد زیر اشاره نمود:

- ارتباط اتصال گرایا : Connection-oriented communication این نوع ارتباط را که می توان آنرا جریان داده نیز تفسیر کرد می تواند مزایای متعددی را برای برنامه کاربردی به ارمغان بیاورد. در حالت عادی کار کردن با آن راحتتر از کار کردن با ارتباط بدون اتصال یا Connection-less است. یکی از پروتکل هایی که این نوع سرویس را ارائه می دهد پروتکل TCP می باشد.
- مرتب سازی بایتی یا : Byte Orientation به جای اینکه برنامه کاربردی پیام های دریافت شده از سیستم ارتباطی را بر اساس فرمتی نامشخص پردازش کند، اغلب جریان داده را به صورت ترتیبی از بایت های خواند که این کار به مراتب آسان تر خواهد بود. این ساده سازی به برنامه کاربردی امکان می دهد که بتواند با فرمت های مختلفی از پیام ها کار کند.
- تحویل با ترتیب یکسان : لایه شبکه معمولاً قادر به تضمین این مسئله نیست که داده های بسته های دریافت شده دقیقاً همان ترتیبی را دارند که از سیستم ارسال کننده فرستاده شده اند. وظیفه مرتب سازی بسته معمولاً در لایه انتقال صورت می پذیرد.
- قابلیت اطمینان : به دلیل خطاها و تراکم های شبکه ای احتمال اینکه بسته های اطلاعاتی از بین بروند وجود دارد. با استفاده از تکنیک های کد شناسایی خطا از قبیل مجموع مقابله ای یا checksum ، پروتکل انتقال بررسی می کند که آیا داده ها سالم هستند یا خیر. این پروتکل نتیجه بررسی خود را بوسیله ارسال کند (ACK) به معنای صحت داده ها و (NACK) به معنای خرابی داده ها به فرستنده اعلام می کند. ممکن است طرح های درخواست تکرار خودکار برای ارسال دوباره اطلاعات آسیب دیده و یا از بین رفته مورد استفاده قرار گیرد.
- کنترل جریان یا : Flow Control بعضی اوقات نرخ انتقال اطلاعات بین دو نود بایستی مدیریت شود تا از ارسال سریع تر فرستنده نسبت به گیرنده اطلاعات که می تواند منجر به سرریز بافر داده ای گیرنده شود جلوگیری به عمل آید.
- پیشگیری از تراکم یا : Congestion Avoidance کنترل تراکم می تواند ترافیک وارد شده به شبکه مخابراتی را مدیریت کرده و با اعمال ممنوعیت ورود هر نوع امکان ارتباطی و یا

پردازشی از سوی نودهای شبکه تصادم و یا تراکم را کاهش دهد. همچنین این سرویس می تواند با در اختیار گرفتن منابع، باعث کاهش نرخ ارسال بسته های اطلاعاتی شود. برای مثال، درخواست تکرار خودکاری تواند شبکه را در حالتی متراکم نگه دارد؛ این موقعیت می تواند با اعمال پیشگیری های تراکمی به کنترل جریان به حداقل برسد. با این کار مصرف پهنای باند از همان ابتدای انتقال اطلاعات و یا بعد از ارسال مجدد بسته ها در سطحی پایین و ایمن باقی خواهد ماند.

- تسهیم یا مالتی پلکسینگ (Multiplexing) پورتهایی تواند چندین مقصد پایانی را بر روی یک نود فراهم آورد. برای مثال، نام موجود در آدرس پستی می تواند نمایانگر نوعی از تسهیم و تفکیک بین چندین گیرنده در یک محل باشد. برنامه های کاربردی بر روی پورت های مخصوص به خودشان به اطلاعات گوش می دهند که این کار این امکان را فراهم می آورد که از چندین سرویس شبکه به صورت همزمان استفاده کنیم. این سرویس بخشی از لایه انتقال در مدل TCP/IP است، اما در مدل OSI این سرویس بخشی از لایه نشست می باشد.

لایه انتقال مسئولیت تحویل اطلاعات به پردازش کاربردی مناسب بر روی کامپیوتر میزبان را بر عهده دارد. این کار شامل تسهیم آماری داده ها از پردازش های کاربردی مختلف می شود، به عبارت ساده تر تشکیل بسته های داده ای و افزودن شماره پورت های مبدأ و مقصد در هدر لایه انتقال هر یک از بسته های داده ای به عهده این لایه می باشد. شماره پورت ها به همراه شماره IP مبدأ و مقصد یک سوکت شبکه را شکل می دهند. سوکت آدرسی تشخیصی متعلق به ارتباطات پردازش به پردازش است. در مدل OSI این کار توسط لایه نشست صورت می پذیرد.

برخی از پروتکل های لایه انتقال نظیر TCP، و نه UDP، از مدارهای مجازی Virtual circuit پشتیبانی می کنند؛ یعنی ارتباطی اتصال گرا را بر روی شبکه دیتاگرام فراهم می آورند. زمانیکه ارتباطات بسته ای از دید پردازش های کاربردی پنهان هستند از یک جریان بایتی استفاده خواهد شد. این کار از مراحل زیر تشکیل می شود: برقراری ارتباط، تقسیم جریان داده ای به بسته هایی که بخش یا segment نامیده می شوند، شماره گذاری بخش ها و مرتب سازی مجدد ترتیب داده ها.

در نهایت، بعضی از پروتکل های لایه انتقال نظیر TCP و نه UDP، ارتباط مبدأ به مقصد قابل اطمینانی را فراهم می آورند. عمل کشف خطا با استفاده از تکنیک هایی مانند کد شناسایی خطا و پروتکل درخواست تکرار خودکار (ARQ) انجام می پذیرد. پروتکل ARQ عمل کنترل جریانرا نیز برعهده دارد که ممکن است با سرویس پیشگیری از تراکم ترکیب شود.

UDP پروتکل بسیار ساده ای است. از UDP می توان در Broadcasting و Multicasting استفاده جست زیرا انتقال دوباره برای بخش اعظمی از نودها امکان پذیر نیست. معمولاً خروجی بالاتر و میزان تأخیر کمتری را تولید می کند و بنابراین از آن می توان در ارتباطات چندرسانه ای زنده که در آن دست رفتن معقول بسته های اطلاعاتی قابل پذیرش باشد استفاده کرد، مانند IP-TV و IP-telephony و نیز بازی های رایانه ای برخط.

در بسیاری از شبکه های رایانه ای که مبتنی بر IP نیستند نظیر اکس ۲۵ (X.۲۵)، بازپخش قاب (Frame Relay) و ATM یا حالت انتقال ناهمگام، ارتباط اتصال گرا در به جای اینکه در لایه انتقال پیاده سازی شود در لایه شبکه و یا لایه پیوند داده تعبیه می شود. در اکس ۲۵، در مودم های شبکه تلفنی و نیز در سیستم های ارتباطی بی سیم، ارتباط نود به نود قابل اطمینان در پروتکل های لایه های پایین تر تعبیه می شوند.

مدل OSI پنج کلاس از پروتکل های انتقال را تعریف می کند، TP با کمترین امکان کشف خطا تا ۴TP که برای شبکه های با قابلیت اطمینان پایین تر طراحی شده است.

پروتکل ها

تعریف دقیقی که بتوان بواسطه آن پروتکل های لایه انتقال را توصیف کرد وجود ندارد. موارد زیر فهرست کوچکی از پروتکل های این لایه هستند:

- ATP، پروتکل تراکنش AppleTalk
- DCCP، پروتکل کنترل ازدحام دیتاگرام
- FCP، پروتکل کانال فیبری
- IL، پروتکل IL
- NBF، پروتکل فریم های NetBIOS

- RDP، پروتکل دیتاگرام قابل اطمینان
- SCTP، پروتکل انتقال کنترل جریان
- SPX، تبادل بسته مرحله‌ای
- SST، انتقال جریان ساختاریافته
- TCP، پروتکل کنترل انتقال
- UDP، پروتکل داده‌نگار کاربر
- UDP Lite
- μTP، پروتکل میکرو انتقال

مقایسه پروتکل‌های انتقال در مدل OSI

مدل OSI پنج کلاس از پروتکل‌های انتقال مبتنی بر اتصال را تعریف کرده که از کلاس ۰ (TP۰) تا کلاس ۴ (TP۴) شماره گذاری می شوند. کلاس ۰ هیچگونه بازیابی خطایی ندارد و برای استفاده در لایه شبکه که ارتباط های عاری از خطا را فراهم می آورد طراحی شده است. کلاس ۴ نزدیکترین پروتکل به TCP است، با این وجود TCP دارای عملیاتی نظیر بستن ارتباط است که مدل OSI آنرا به لایه نشست نسبت داده است.

ساختار بسته های پروتکل TCP:

در این بخش يك دید کلی از پروتکل TCP ارائه می نماییم و ساختار سرآیند بسته ها را در این پروتکل ، توضیح خواهیم داد .

در زیر ساختار يك بسته TCP به تصویر کشیده شده است .

Source port							Destination Port
Sequence Number							
Acknowledgment Number							
TCP Header Length	URG	ACK	PSH	RST	SYN	FIN	Windows Size
Checksum							Urgent Pointer
Options) • or more ۳۲-bit words)							
Data) optional)							

فیلد Source Port: در این فیلد يك شماره ۱۶ بیتی بعنوان آدرس پورت پروسه مبدأ (که این بسته را جهت ارسال تولید کرده) ، قرار خواهد گرفت .

فیلد Destination Port: در این فیلد ، آدرس پورتِ پروسه مقصد که آنرا تحویل خواهد گرفت تعیین خواهد شد .

همانگونه که در بخش قبلی اشاره شد این دو آدرس مشخص می کنند که این بسته ، از چه برنامه کاربردی در لایه بالاتر تولید شده و باید به چه برنامه ای در ماشین مقصد تحویل داده شود. برخی از پروسه های کاربردی و استاندارد و جهانی هستند ، مثلا سرویس دهنده

پست الکترونیکی دارای شماره پورت ۲۵ است . به جدول شماره پورت های استاندارد در دیسک جانبی کتاب نگاهی بیندازید .

فیلد Sequence Number: این فیلد سی و دو بیتی ، شماره ترتیب آخرین بایتی را که در " فیلد داده " از بسته جاری قرار دارد ، نشان می دهد .

در پروتکل TCP شماره ترتیب ، بر حسب شماره آخرین بایتی است که در بسته جاری قرار گرفته و ارسال شده است . به عنوان مثال اگر در این فیلد عددی معادل ۱۹۳۴۱ درون فیلد داده قرار دارد . دقت کنید که این عدد به معنای آن نیست که به تعداد ۱۹۳۴۱ بایت ، درون قسمت داده قرار دارد ، بلکه همیشه به شماره ترتیب آخرین بایت داده ، اشاره مینماید . یعنی ممکن است که کلاً درون فیلد داده فقط یک بایت قرار داشته باشد در حالی که در فیلد شماره ترتیب عدد ۱۹۳۴۱ قرار داشته باشد . دقت شود که شماره ترتیب اولین بایت ، از صفر شروع نمی شود بلکه از یک عدد تصادفی که در هنگام برقراری ارتباط به اطلاع طرفین میرسد شروع خواهد شد.

فیلد Acknowledgment Number: این فیلد ۳۲ بیتی نیز شماره ترتیب بایتی که فرستنده بسته منتظر دریافت آن است را تعیین میکند . بعنوان مثال اگر در این فیلد عددی معادل ۳۴۲۳۱۰ قرار گرفته باشد بدین معناست که از رشته داده ها (که مشخص نیست چند بایت است) تا شماره ۳۴۲۳۱۰ صحیح و کامل دریافت شده است و منتظر بایتهای از ۳۴۲۳۱۱ به بعد می باشد .

فیلد TCP Header Length: عددی که در این فیلد قرار می گیرد ، طول سرآیند بسته TCP را بر مبنای کلمات ۳۲ بیتی تعیین می کند . بعنوان مثال اگر در این فیلد عدد ۷ قرار بگیرد طول سرآیند مقدار $7 * 4 = 28$ بایت خواهد بود (این فیلد کلاً چهار بیتی است) دقت کنید که قسمت ثابت و اجباری در یک بسته TCP حداقل ۲۰ بایت است ولی در فیلد اختیاری میتواند اطلاعاتی قرار بگیرد و بنابر این گیرنده یک بسته TCP باید بتواند مرز بین سرآیند بسته و قسمت داده را تشخیص بدهد . پس عددی که در این فیلد قرار می گیرد می تواند بعنوان یک "اشاره گر" ، محل شروع داده ها را در یک بسته TCP تعیین کند (توجه دارید که مبنای این عدد کلمات ۳۲ بیتی (۴ بایتی) هستند)

بیت‌های ۶: (Code Bits) Flag بیت بعدی در بسته TCP هر کدام نقش يك بیت پرچم را که معنا و کاربرد مختلفی دارند بازی میکنند .

URG	ACK	PSH	RST	SYN	FIN
-----	-----	-----	-----	-----	-----

این بیتها و معنای آنها را بترتیب بررسی میکنیم :

بیت URG: در صورتی که که این بیت مقدار ۱ داشته باشد ، معین میکند که در فیلد Urgent Pointer که در ادامه معرفی خواهد شد مقداری قابل استناد و معتبر قرار دارد و بایستی مورد پردازش قرار گیرد . در صورتی که این بیت صفر باشد فیلد Urgent Pointer شامل مقدار معتبر و قابل استنادی نیست و از آن چشم پوشی میشود .

بیت ACK: اگر در این بیت مقدار ۱ قرار گرفته باشد ، نشان می دهد که عددی که در فیلد Acknowledgement Number قرار گرفته است ، دارای مقداری معتبر و قابل استناد است . بیت ACK و بیت SYN نقش دیگری نیز دارد که در ادامه بدان اشاره خواهد شد .

بیت PSH: اگر در این بیت مقدار ۱ قرار گرفته باشد فرستنده اطلاعات از گیرنده تقاضا میکند که داده های موجود در این بسته را بافر نکند و در اسرع وقت آنرا جهت پردازشهای بعدی تحویل برنامه کاربردی صاحب آن بدهد . این عمل گاهی برای برنامه های مشابه Telnet ضروری است .

بیت RST: اگر در این بیت مقدار ۱ قرار بگیرد ارتباط بصورت یکطرفه و نا تمام قطع خواهد شد ، بدین معنا که به هر دلیلی (اعم از نقص سخت افزاری یا نرمافزاری) اشکالی بوجود آمده که یکی از طرفین ارتباط مجبور به خاتمه ارتباط فعلی شده است . همچنین بیت RST میتواند بعنوان علامت عدم پذیرش برقراری ارتباط بکار برود . اگر یکی از طرفین ارتباط يك بسته دریافت کند که در آن بیت RST مقدار ۱ داشته باشد ، ارتباط بصورت نا هماهنگ و نا متعادل ، قطع خواهد شد .

بیت SYN: این بیت نقش اساسی در برقراری يك ارتباط بازی میکند . برقراری يك ارتباط TCP از روند زیر طبیعت میکند :

شروع کننده ارتباط يك بسته TCP بدون هیچگونه داده و با تنظیم بیت‌های (ACK=0, SYN=1) ، برای طرف مقابل ارسال میکند . در حقیقت ارسال چنین بسته ای به معنای “تقاضای برقراری ارتباط ” تلقی میشود .

در پاسخ به درخواست ارتباط ، در صورتی که طرف مقابل به برقراری ارتباط تمایل داشته باشد بسته ای برمی گرداند که در آن بیت SYN=1 و بیت ACK=1 است . این بسته نقش “پذیرش يك ارتباط ” را بازی میکند .

بیت FIN: اگر یکی از طرفین ارتباط ، داده دیگری برای ارسال نداشته باشد در هنگام ارسال آخرین بسته خود این بیت را می کند و در حقیقت ارسال اطلاعات خودش را يك طرفه قطع می کند . در این حالت اگر چه ارسال اطلاعات قطع شده ولیکن طرف مقابل هنوز ممکن است به ارسال اطلاعات مشغول باشد . زمانی ارتباط کاملاً خاتمه می یابد که طرف مقابل نیز در يك بسته با يك کردن بیت FIN ، ارسال اطلاعات را خاتمه بدهد .

فیلد WindowSize: مقدار قرار گرفته در این فیلد مشخص میکند که فضای بافر گیرنده چند بایت دیگر ظرفیت خالی دارد . یعنی به طرف مقابل اعلام می کند که مجاز است از بایت با شماره ترتیبی که در فیلد Acknowledgement مشخص شده است ، حداکثر به اندازه مقداری که در این فیلد درج شده ، ارسال داشته باشد و در غیر اینصورت فضای کافی برای دریافت داده ها وجود نداشته و ناگزیر دور ریخته خواهد شد. اگر مقدار این فیلد صفر باشد بدین معناست که بافر گیرنده تماماً پر شده است و امکان دریافت داده های بعدی وجود ندارد و پروسه فرستنده متوقف خواهد شد .

فیلد Checksum: در این فیلد ۱۶ بیتی ، کد کشف خطا قرار می گیرد .

فیلد TCPsegmentLength: که در آن طول کل بسته TCP مشخص می شود .

فیلد Urgent Pointer: در این فیلد يك عدد بعنوان اشاره گر قرار می گیرد که موقعیت داده های اضطراری را درون بسته TCP معین می کند . این داده ها ، زمانی اتفاق می افتد و ارسال می شود که عملی شبیه وقوع وقفه ها در هنگام اجرای يك برنامه کاربردی رخ بدهد . بدون آنکه ارتباط قطع شود داده های لازم در همین بسته جاری ارسال خواهد شد.

دقت کنید که داده های اضطراری توسط برنامه کاربردی در لایه بالاتر پردازش خواهد شد و برای پروتکل TCP کاربردی ندارد .

فیلد Options: در این فیلد اختیاری است و مقداری نظیر حداکثر طول بسته TCP در آن قرار میگیرد. برای آنکه طول بسته ضریبی از ۴ باقی بماند از این فیلد با کدهای بی ارزش استفاده می شود. گزینه خاص دیگری در این فیلد تعریف نشده است .

درس ۲

UDP

UDP از حروف اول کلمات User Datagram Protocol گرفته شده و یک پروتکل غیر اتصال گرا (Connectionless) است که مثل TCP در بالاترین لایه اجرا می شود. برخلاف TCP در پروتکل UDP امکان بروز خطا وجود دارد.

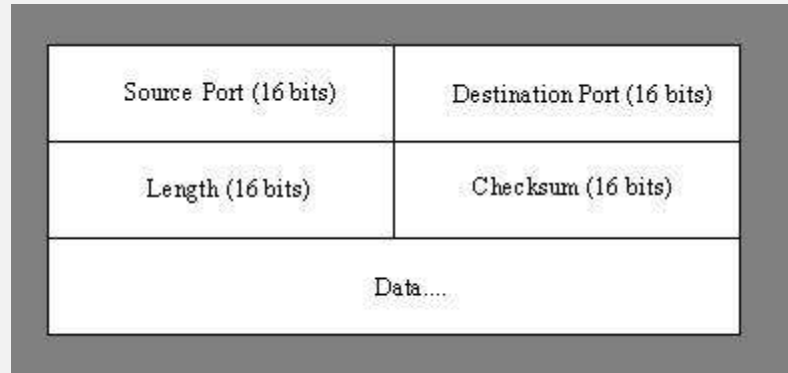
تشریح کامل آن در RFC ۷۶۸ آمده. یک ارتباط غیراتصال گرا بین دو هاست برقرار می کنه و هر بسته از داده کاربر و کمترین میزان سرایند تشکیل شده که به آن UDP دیتاگرام گفته می شود. UDP غیراتصال گرا است. یعنی یک دیتاگرام در هر لحظه ای میتونه ارسال بشه، بدون نیاز به هر گونه اعلام قبلی، مذاکره و یا هیچ آماده سازی از قبل. فقط داده رو ارسال می کنه و امیدواره که گیرنده داده ها رو دریافت کنه.

یک ارتباط غیرقابل اعتماد ایجاد می کنه. یعنی هیچ تضمینی برای اطمینان از تحویل داده ها در مقصد وجود ندارد. نه تنها هیچ اطمینانی از رسیدن داده ها به مقصد وجود نداره بلکه حتی به صحت و درستی داده هائی که به مقصد رسیده هم همیشه اطمینان داشت. ممکنه بسته ای رو دو بار دریافت کنیم!! برنامه ما که بر اساس این پروتکل کار میکنه باید آمادگی مواجه شدن با تمام این موقعیت ها رو داشته باشه: از دست دادن دیتاگرام، دیتاگرام تکراری و یا دریافت دیتاگرام با ترتیب غلط.

مهمترین محاسن UDP اینه که محدوده داده ها در ائن مشخص شده، در ارسال های broadcast همیشه از این پروتکل استفاده کرد و همچنین سریع.

و مهمترین معایب غیرقابل اعتماد بودن آن و در نتیجه پیچیده بودن برنامه نویسی در سطح لایه application است.

و اما قالب بسته UDP:



همین طور که در شکل می بینید :

Source Port: یک فیلد اختیاری برای شماره پورت فرستنده. اگر شماره پورت مشخص نشه در این فیلد ۰ قرار میگیره.

Destination Port: شماره پورت مقصد.

Length: طول دیتاگرام، شامل Header و داده اصلی.

Checksum: کد کشف خطا. این فیلد در Header بسته UDP اختیاریست.

آدرس دهی

TCP و UDP از یک مدل آدرس دهی استفاده می کنند: یک آدرس IP و شماره پورت مورد نظر. آدرس IP برای هدایت بسته به هاست منظور در شبکه ی مشخص شده و شماره پورت برای هدایت به پروسه منتظر. معمولاً یک پورت برای یک برنامه اختصاص داده.

محاسن TCP

- سیستم عامل همه کار را برای شما انجام میدهد. دیگر باگهای ابتدائی که هر کس در اولین کارش با آن ها روبرو میشود را مرتکب نمیشوید. برای اینکه تمام این ها برای ما توسط سیستم عامل انجام و رفع شده است.
- کارهائی که سیستم عامل برای دریافت و ارسال بسته های TCP انجام میدهد نیازی به سوئیچ لز مود کرنل به مود کاربر ندارد. چرا که اغلب کارها مثل اسمبل کردن مجدد بسته

های رسیده، پاسخ مبنی بر دریافت بسته ها (ACK)، گزارش خطاها، و... توسط کرنل انجام می شود.

- TCP سه چیز را برای شما گارانتی میکند: داده های ما به مقصد برسد، داده ها با ترتیب صحیحی برسد، داده ها بدون تکرار در مقصد دریافت شود.
- مسیریاب ها در مواجهه با بسته های TCP رفتارهای خاص متناسب رو انجام میدهند. مثلا در صورت لزوم می توانند تقاضای ارسال مجدد بسته کنند.

محاسن UDP

- محدود و ملزم به رعایت از مدل ارتباطی connection oriented نیستیم.
- کنترل خطاها، پاسخ به فرستنده (ACK) و... به برنامه بستگی دارد و ما به عنوان برنامه نویس ویژگیهایی را که نیاز داریم پیاده سازی و استفاده می کنیم.
- انتقال های broadcast و multicast در UDP امکان پذیره.

معایب TCP

- اگر سیستم عامل باگ داشته باشد، ما نمیتوانیم از دست این باگ راحت بشویم. ممکن است برای چیزی که ما می خواهیم موثر نباشد و کارا نباشد ولی ما مجبوریم که از همان استفاده کنیم.
- TCP ویژگیهای فوق العاده ای را برای شما فراهم می کند که شاید خیلی از آنها را نیاز نداشته باشید. در نتیجه برای کار شما، پهنای باند و یا زمان را هدر میدهد.
- در TCP داده ها هیچ محدوده ای مشخص نشده و ما باید خودمان محدوده داده را مشخص کنیم.
- TCP برای انتقال های broadcast و multicast نمیتواند مورد استفاده قرار بگیرد.

معایب UDP

- با وجود UDP هیچ گارانتی وجود ندارد. ممکن است بسته ای تحویل مقصد داده شود ، یا دو بار داده شود و یا اینکه به ترتیب تحویل داده نشود. و با بروز هر یک از این خطاها ما متوجه نمیشویم، مگر اینکه برنامه ای که به داده ها گوش می دهد، در صورت بروز هر یک از خطاها بخواهد کاری انجام دهد.
- UDP برای خطاهای احتمالی هیچ گونه مکانیزمی ندارد و پیاده سازی کشف و رفع خطاها به عهده برنامه نویس است.

فصل ۱

مسیر یابی

در این فصل روتینگ را تعریف میکنیم و انواع پروتکل های روتینگ را توضیح میدهیم.

درس ۱

روتینگ

روتینگ (Routing) یکی از مهمترین ویژگیهای مورد نیاز در یک شبکه به منظور ارتباط با سایر شبکه ها است. در صورتی که امکان روتینگ پروتکل ها وجود نداشته باشد ، کامپیوترها قادر به مبادله داده نخواهند بود .

تعریف

از روتینگ به منظور دریافت یک بسته اطلاعاتی (packet) از یک دستگاه و ارسال آن از طریق شبکه برای دستگاهی دیگر و بر روی شبکه ای متفاوت ، استفاده می گردد . در صورتی که شبکه شما دارای روتر نباشد ، امکان روتینگ داده بین شبکه شما و سایر شبکه ها وجود نخواهد داشت . یک روتر به منظور مسیریابی یک بسته اطلاعاتی ، می بایست آگاهی لازم در خصوص اطلاعات زیر را داشته باشد :

- آدرس مقصد
- روترهای مجاور که با استفاده از آنان امکان اخذ اطلاعات لازم در خصوص شبکه های از راه دور، فراهم می گردد .
- مسیرهای موجود به تمامی شبکه های از راه دور .
- بهترین مسیر به هر یک از شبکه های از راه دور .
- نحوه نگهداری و بررسی اطلاعات روتینگ .

همگرایی (Convergence)

فرآیند مورد نیاز برای تمامی روترهای موجود در یک شبکه به منظور بهنگام سازی جداول روتینگ و ایجاد یک نگرش سازگار از شبکه با استفاده از بهترین مسیرهای موجود . در زمان انجام فرآیند فوق (همگرایی) ، داده کاربر ارسال نخواهد شد .

مسیر پیش فرض (Default Route)

یک مسیر استاندارد درج شده در جدول روتینگ که به عنوان اولین گزینه در نظر گرفته می شود . هر بسته اطلاعاتی که توسط یک دستگاه ارسال می گردد در ابتدا به مسیر پیش فرض ارسال خواهد شد . در صورتی که مسیر فوق مشکل داشته باشد ، یک مسیر دیگر انتخاب می گردد .

مسیر ایستا (Static Route)

یک مسیر دائم که به صورت دستی درون یک جدول روتینگ درج می گردد . مسیر فوق حتی در مواردیکه ارتباط غیر فعال است در جدول روتینگ باقی مانده و صرفاً" به صورت دستی حذف می گردد .

مسیر پویا (Dynamic Route)

یک مسیر که به صورت پویا (اتوماتیک) و متناسب با تغییرات شبکه ، بهنگام می گردد . مسیرهای پویا نقطه مقابل مسیرهای ایستا می باشند .

درس ۲

پروتکل های روتینگ:

Static routing این قابلیت را به مدیریت شبکه می دهد که بتواند بصورت دستی یک سری Route های خاص را در Routing Table روتر ایجاد کند. Dynamic Routing از پروتکل های مسیریابی یا Routing Protocol برای شناسایی شبکه ها و مقصدها و همچنین پیدا کردن بهترین مسیر برای رساندن بسته اطلاعاتی به مقصد استفاده می کنند. Dynamic Routing این قابلیت را به Routing Table می دهد که بتواند زمانیکه یک Router خاموش است یا در دسترس نیست یا اینکه یک شبکه جدید به مجموعه اضافه می شود این تغییرات را در Routing Table اضافه کند. Dynamic Routing با استفاده از Routing Protocol ها این قابلیت را دارند که بصورت مستمر با شبکه تبادل اطلاعات داشته باشند و وضعیت هر یک از Router های شبکه را بررسی کنند و با استفاده از Broadcast و یا Multicast با هم ارتباط برقرار کنند و اطلاعات Routing Table را بروز کنند. با این روش همیشه توپولوژی شبکه بروز باقی می ماند و همگی دستگاه های روتر شبکه از آخرین Routing Table بروز استفاده می کنند. از پروتکل های Dynamic Routing می توان به Routing Information Protocol یا RIP ، Enhanced Interior Gateway Routing Protocol یا EIGRP و Open Shortest Path First یا OSPF اشاره کرد. اما بصورت کلی ما Routing Protocol ها را به سه دسته کلی تقسیم بندی می کنیم.

Distance-Vector Routing Protocol ها:

پروتکل های Distance Vector از معیار Hop Count یا تعداد روترهای مسیر برای Metric در Routing Table های خود استفاده می کنند. الگوریتم مورد استفاده در اینگونه از پروتکل ها بسیار ساده است و Routing Table با محاسبات ساده ریاضی ایجاد می شود. پروتکل های Distance Vector معمولا برای شبکه های کوچکی که کمتر از ۱۶ عدد Router در آنها وجود دارد مورد استفاده قرار می گیرند در واقع این نوع پروتکل ها با کم کردن تعداد Router های مسیر از به وجود آمدن Loop در شبکه یا بهتر بگوییم Routing Loop در شبکه جلوگیری

می کنند. این پروتکل ها در وهله های زمانی معین Routing Table های خود را با یکدیگر یکسان سازی می کنند ، یکی از مشکلات الگوریتم های Distance Vector در این است که کلیه اطلاعات موجود در Routing Table را حتی با کوچکترین تغییر برای سایر روترهای مجموعه ارسال می کنند و Incremental Update را در واقع پشتیبانی نمی کردند که در نسخه های جدید الگوریتم های Distance Vector این مشکل حل شد. الگوریتم های مسیریابی مثل RIPv1 و IGRP از این نوع Routing protocol ها هستند.

Link-State Routing Protocol های:

در پروتکل های Routing ای که بصورت Link State کار می کنند تفاوت محسوسی با حالت Distanced Vector وجود دارد. الگوریتم های مورد استفاده در این نوع پروتکل ها نسبت به Distanced Vector ها کاملا متفاوت عمل می کند و دارای پیچیدگی های خاص خود می باشد ، در این الگوریتم ها از فاکتورهایی مثل Hop Count ، فاصله ، سرعت لینک و ترافیک بصورت همزمان برای تعیین بهترین مسیر و بهترین cost برای انجام عملیات Routing استفاده می شود. آنها از الگوریتمی به نام Dijkstra برای تعیین پایینترین cost برای Route ها استفاده می کنند. روترهایی که از پروتکل های Link State استفاده می کنند فقط زمانی Routing Table های همدیگر را یکسان سازی می کنند که چیز جدیدی به Routing Table یکی از Router ها اضافه شده باشد. به همین دلیل هم کمترین ترافیک را در هنگام یکسان سازی Routing Table با همدیگر ایجاد می کنند. الگوریتم های مسیریابی مثل OSPF و IS-IS از این نوع پروتکل های Link State هستند.

Hybrid Routing Protocol های:

همانطور که از نام این نوع پروتکل Routing نیز پیداست این نوع پروتکل ترکیبی از پروتکل های Distance Vector و Link State است و در واقع مزایای هر یک از این نوع پروتکل ها را در خود جای داده است. زمانیکه صحبت از قدرت پردازشی روترها می شود از قابلیت های Distance Vector ها و زمانیکه صحبت از تبادل Routing Table ها در شبکه می باشد از قابلیت های Link State ها استفاده می کند. امروزه تقریبا همه شبکه های بزرگ در دنیا از

پروتکل های Hybrid استفاده می کنند ، الگوریتم مسیریابی مثل EIGRP از انواع پروتکل های Hybrid Routing هستند.

فصل ۹

TCP/IP

Applications

در این فصل به برخی از مهمترین پروتکل‌های لایه کاربرد میپردازیم.

پروتکل‌هایی که یک کاربر ساده بیشتر اسم آنها را شنیده و بیشتر با آنها سرو کار دارد.

درس ۱

DHCP

با استفاده از یک سرویس دهنده DHCP که تنظیمات پیگر بندی را به صورت اتوماتیک اختصاص می دهد ، کاربران و مدیران TCP/IP می توانند خود را از دردسر پیگر بندی دستی آدرس های IP ، ماسک زیر شبکه ، آدرس سرویس دهنده های DNS ، آدرس سرویس دهنده های WINS ، و سایر جنبه های TCP/IP برهاند.

DHCP یک استاندارد باز است که در RFC ۲۱۳۲ تعریف شده است . سازندگان دیگر نیز سرویس دهنده DHCP به بازار عرضه کرده اند .

DHCP به حل برخی از بزرگترین مشکلات نهفته در TCP/IP می پردازد. با وجود DHCP ، تکلیف سخت پیگر بندی تک تک ایستگاههای کاری از دوش مدیران برداشته می شود ، و تخصیص آدرس های IP تکراری تقریباً غیر ممکن می شود.

تاریخچه DHCP

Dhcp ریشه در bootp دارد، که یک پروتوکل قدیمی است. و برای استفاده با ایستگاههای کاری بدون دیسک طراحی شده است. سرویس دهنده bootp آدرس های ip و سایر تنظیمات پیکربندی ایستگاه کاری را، بر اساس آدرس mac حک شده در آداپتور واسط شبکه هرایستگاه کاری ذخیره می کرد. هرکامپیوتر شبکه که بوت می شد تنظیمات tcp/ip آن توسط سرویس دهنده به او تحویل داده می شد. به محض اینکه پشته tcp/ip به کار می افتاد bootp یک فایل قابل اجرای بوت سیستم عامل را با استفاده از tftp به ایستگاه کاری تحویل می داد آنگاه ایستگاه کاری برای استفاده آماده بود bootp. یکی از مشکلات tcp/ip را حل کرد به این ترتیب که نیاز به پیکربندی دستی تک تک ایستگاههای کاری توسط مدیر یا یک کاربر را مرتفع می نمود. اما bootp مشکل مدیریتی تخصیص آدرس های ip را واقعاً برطرف نکرد زیرا صرفاً یک محل مرکزی را برای ذخیره تنظیمات پیکربندی در اختیار می گذاشت. هنوز هم تنظیمات ip مربوط به تک تک ایستگاههای کاری باید توسط مدیر مشخص می شدند و در سرویس دهنده به صورت دستی ذخیره می گشتند. اگر آدرس های ip تکراری به صورت اتفاقی در پیکربندی دو ایستگاه مختلف وارد می شدند bootp برای تشخیص پیشگیری یا حل این مشکل هیچ کاری نمی توانست بکند.

تخصیص آدرس ip

Dhcp برای آن طراحی شد که bootp را بهبود بخشد. در DHCP بهترین جنبه های bootp یعنی ذخیره سازی و تحویل اتوماتیک داده های پیکربندی tcp/ip حفظ شده اند و در ضمن توسعه یافته است تا ابزار بهتری نسبت به bootp باشد.

Dhcp به سه طریق مختلف می تواند آدرس های ip را به سرویس گیرنده هایش تخصیص دهد :

تخصیص دستی :

آدرس های ip و سایر تنظیمات پیکربندی توسط مدیر به صورت تک تک وارد شده روی سرور دهنده ذخیره می گردند و به سرور گیرنده های از پیش تعیین شده تحویل داده می شوند.

تخصیص اتوماتیک:

این آن چیزی است که مخزن ایستا خوانده می شود. وقتی که یک ایستگاه کاری سرور گیرنده dhcp، برای اولین بار در شبکه بوت می شود، سرور دهنده dhcp از مخزنی از آدرس های موجود که مدیر برای استفاده او تنظیم کرده است، یک آدرس ip و سایر تنظیمات پیکربندی را به آن ایستگاه کاری اختصاص می دهد، و اینها تنظیمات دائمی آن ایستگاه می شوند. این را می گردن یک آدرس رزرو شده می خوانند.

تخصیص پویا :

این مثل تخصیص اتوماتیک است، با این تفاوت که تنظیمات tcp/ip به صورت دائمی تخصیص داده نمی شوند، بلکه صرفاً برای مدت زمان مشخصی اجاره داده می شوند. اجاره باید به صورت منظم از طریق مذاکره (اتوماتیک) بین سرور گیرنده و سرور دهنده dhcp تمدید شود. این سه روش می توانند به صورت همزمان مورد استفاده قرار گیرند تا همه انتخاب هایی را که ممکن است مدیران شبکه نیاز داشته باشند در اختیارشان بگذارند.

سایر قابلیت های DHCP

تخصیص کنترل شده آدرس های IP نقطه قوت DHCP محسوب می شود، اما یک آدرس IP به تنهایی برای پیکربندی کامل پشته TCP/IP یک سرور گیرنده کافی نیست. DHCP می تواند

تنظیمات بیش از ۵۰ پارامتر دیگر مربوط به TCP/IP را نیز در اختیار هر سرویس گیرنده قرار دهد. رایجترین پارامترهایی که به سرویس گیرنده ها تحویل داده می شوند عبارتند از:

آدرس IP

ماسک زیر شبکه

آدرس های WINS/NBNS :

آدرس های IP سرویس دهنده های WINS که توسط سرویس گیرنده ها برای سرویس های ثبت و تبدیل اسامی نت بایوس مورد استفاده قرار می گیرند.

پیکربندی اتوماتیک سرویس گیرنده :

پیشرفت قابل توجه دیگری که در DHCP ویندوز سرور ۲۰۰۳ ایجاد شده است مربوط به سرویس گیرنده DHCP می باشد. سرویس گیرنده های ویندوز ۲۰۰۰ و ویندوز ۹۸ ای که برای استفاده از DHCP پیکربندی شده اند اگر نتوانند با سرویس گیرنده های DHCP تماس بگیرند می توانند به صورت اتوماتیک خود را با یک آدرس IP و ماسک زیر شبکه پیکربندی کنند. فرآیندی که سرویس گیرنده DHCP پیش از اینکه اطلاعات را به خود اختصاص دهد پشت سر می گذارد بستگی به این دارد که قبلا با سرویس دهنده DHCP ای تماس گرفته شده است یا خیر.

پس از نصب کامل سرویس گیرنده DHCP- سعی می کند که یک سرویس دهنده DHCP را پیدا کند تا همه اطلاعات TCP/IP لازم برای کاردر شبکه را در اختیار او قرار دهد. اگر این جست و جو با شکست مواجه شود سرویس گیرنده به صورت اتوماتیک خود را با یک آدرس IP و ماسک زیر شبکه کلاس B پیکربندی می کند. سپس او این آدرس را به دنیا اعلام می کند تا ببیند که آیا کامپیوتر دیگری از قبل این آدرس را به خود گرفته است یا خیر.

سرویس گیرنده به طور منظم سعی می کند که با یک سرویس دهنده DHCP تماس بگیرد تا زمانی که موفق به این کار بشود.

حالت دیگر وقتی است که سرویس گیرنده قبلا با یک سرویس دهنده DHCP تماس گرفته و اطلاعات TCP/IP را از او دریافت کرده است در این صورت سرویس گیرنده برای تمدید اجاره با سرویس دهنده DHCP تماس می گیرد اگر سرویس گیرنده نتواند با سرویس دهنده DHCP تماس بگیرد دروازه پیش فرضی که در اختیار او قرار داده شده است را پینگ می کند اگر پینگ موفقیت آمیز باشد سرویس گیرنده ارتباط شکست خورده با سرویس دهنده DHCP را یک تاخیر موقتی تلقی می کند و به استفاده از اطلاعات اجاره ای که داشته است ادامه می دهد.

تشخیص و جلوگیری از کار سرویس دهنده های DHCP غیرمجاز:

سرویس DHCP یک پیشرفت فوق العاده نسبت به پیکربندی دستی آدرس های IP و سایر تنظیمات مربوط به TCP/IP در تک تک کامپیوتر های شبکه محسوب می شود. اما اگر سرویس دهنده های DHCP غیرمجازی وجود داشته باشند که با سرویس دهنده های DHCP مجاز برسر اینکه چه کسی اطلاعات را به سرویس گیرنده ها بدهد رقابت کنند، مدیریت شبکه می تواند خیلی سخت شود. به عنوان مثال، کاربری تصمیم می گیرد که سرویس DHCP سرور را روی کامپیوتر خود نصب کند تا اطلاعات را به چند کامپیوتر که در آزمایشگاه واقع هستند تحویل بدهد. ولی این طور می شود که چیزی که قرار بوده یک سرویس دهنده DHCP محلی باشد، در واقع به سایر سرویس گیرنده های شبکه سرویس می دهد. این تغییر ممکن است سرویس گیرنده ها را بی فایده کند. چنین اوضاعی معمولا به صورت اتفاقی پیش می آید، ولی در هر حال روی شبکه اثر می گذارد. نگارش های قبلی DHCP نمی توانستند به خوبی چنین مشکلاتی را حل کنند. مدیران باید مرتبا مواظب می بودند که فقط DHCP سرورهایی که آنها ایجاد یا مدیریت کرده اند مجاز به کار در شبکه باشند.

یکی از پیشرفت های زیادی که در DHCP ایجاد شده است قابلیت تشخیص و جلوگیری از کار سرویس دهنده های DHCP غیرمجاز در شبکه است . یکی از مراحل نصب هر DHCP سرور مرحله کسب جواز است که یا با بررسی AD و یا با هدایت کسی که جوازهای مدیریتی دارد به انجام می رسد. در غیراین صورت DHCP سرور اجازه سرویس دادن به سرویس گیرنده ها را نخواهد داشت. AD می تواند فهرستی از سرویس دهنده های DHCP مجاز را ذخیره کند تا وقتی که سرویس دهنده DHCP جدیدی به کار می افتد ، بتواند بفهمد که او مجاز است یا خیر .

درس ۲

DNS

ساناد، سرواژه سامانه نام دامنه، DNS^۱ خوانده می‌شود. نظامی، سلسله مراتبی، برای نام‌گذاری رایانه‌ها و دیگر منابع متصل به اینترنت یا دیگر شبکه‌های رایانه‌ای که در سال ۱۹۸۴ معرفی شده‌است.

وقتی می‌خواهید وارد وبگاهی شوید، باید نشانی کارساز وبش را بدانید. نشانی کارساز وب با نشانی آی‌پی مشخص می‌شود. اما به خاطر سپردن نشانی آی‌پی، دشوار است. می‌توان به جای نشانی آی‌پی، از نام‌های دامنه استفاده کرد. برای هر نشانی آی‌پی یک نام دامنه در نظر گرفته شده‌است. مثلاً نشانی آی‌پی وبگاه گوگل ۱۷۳/۱۹۴/۳۳/۱۰۴ است. برای دسترسی به گوگل، می‌توانید از این نشانی آی‌پی یا نام دامنه آن یعنی www.google.com استفاده کنید.

در ساناد، کل نشانی‌های اینترنت درون بانک‌های اطلاعاتی توزیع شده‌ای هستند که هیچ تمرکزی روی نقطه‌ای خاص از شبکه ندارند. روش ترجمه نام بدین صورت است که وقتی یک برنامه کاربردی مجبور است برای برقراری یک ارتباط، معادل نشانی آی‌پی از یک ماشین با نامی مثل cs.ucsb.edu را بدست بیاورد، قبل از هر کاری یک تابع کتابخانه‌ای (Library Function) را صدا می‌زند، به این تابع کتابخانه‌ای تابع تحلیلگر، نام (Name Resolver) گفته می‌شود.

تابع تحلیلگر، نام یک نشانی نمادین را که بایستی ترجمه شود، بعنوان پارامتر ورودی پذیرفته و سپس یک بسته درخواست (Query Packet) به روش UDP تولید کرده و به نشانی یک کارساز DNS (که به صورت پیش فرض مشخص می‌باشد) ارسال می‌کند. همه ماشین‌های میزبان، حداقل باید یک نشانی آی‌پی از یک سرویس دهنده ساناد را در اختیار داشته باشند. این «سرویس دهنده محلی» پس از جستجو، نشانی آی‌پی معادل با یک نام نمادین را برمی‌گرداند.

«تابع تحلیلگر نام» نیز آن نشانی آی‌پی را به برنامه کاربردی تحویل می‌دهد با پیدا شدن نشانی آی‌پی، برنامه کاربردی می‌تواند عملیات مورد نظرش را ادامه دهد.

^۱Domain Name System

کاربرد حوزه ها :

برای تحلیل یک نام حوزه، سطوح از سمت راست به چپ تفکیک می شوند و در یک روند سلسله مراتبی، سرویس دهنده متناظر با آن سطح پیدا می شود.

نام های حوزه به هفت منطقه عمومی و حدود صد و اندی منطقه کشوری تقسیم بندی شده است. حوزه بدین معناست که شما با یک نگاه ساده به انتهای نشانی نمادین، می توانید ماهیت آن نام و سرویس دهنده متناظر با آن را حدس بزنید. یعنی اگر انتهای نام های حوزه متفاوت باشد منطقه جستجو برای یافتن نشانی آی پی معادل نیز متفاوت خواهد بود.

هفت حوزه عمومی که همه آنها سه حرفی هستند عبارتند از :

.com. صاحب این نام جزو موسسات اقتصادی و تجاری به شمار می آید.

.edu. صاحب این نام جزو موسسات علمی یا دانشگاهی به شمار می آید.

.gov. این مجموعه از نام ها برای آژانس های دولتی آمریکا اختصاص داده شده است.

.int. صاحب این نام یکی از سازمان های بین المللی (مثل یونسکو، فائو، ...) است.

.mil. صاحب این نام یکی از سازمان های نظامی دنیا به شمار می آید.

.net. صاحب این نام جزو یکی از «ارائه دهندگان خدمات شبکه» به شمار می رود.

.org. صاحب این نام جزو یکی از سازمان های غیر انتفاعی محسوب می شوند

نام های حوزه بسیار زیادی در اینترنت تعریف شده اند که هیچیک از حوزه های سه حرفی هفتگانه را در انتهای آنها نمی بینید. معمولاً در انتهای این نشانی ها یک رشته دو حرفی مخفف نام کشوری است که آن نشانی و ماشین صاحب آن، در آن کشور واقع است.

ساختار سلسله مراتبی DNS

هر حوزه می تواند به زیر حوزه های کوچکتری تقسیم شود، که به آن دامنه سطح دوم نیز گفته می شود.

به عنوان مثال، نام های مربوط به حوزه ایران، که با مخفف .ir مشخص می شود، به ۷ زیرحوزه، به شرح زیر تقسیم می شود:

.ac.ir : فقط برای دانشگاه ها یا موسسه های آموزشی

.co.ir : فقط برای شرکت های سهامی خاص، سهامی عام، مسوولیت محدود و تضامنی

.gov.ir : فقط برای موسسه ها یا سازمان های دولتی

.id.ir : فقط برای افراد دارای ملیت ایرانی

.net.ir : فقط برای سرویس دهندگان رسمی اینترنت

.org.ir : فقط برای موسسه ها و سازمان های خصوصی

.sch.ir : فقط برای مدارس

بعنوان مثال: <http://eng.ut.ac.ir>

کشور: ایران

هویت: دانشگاه

نام دانشگاه: ut مخففی برای نام دانشگاه تهران

نام دانشکده: eng مخففی برای بخش فنی مهندسی

حوزه ها با دامنه ها یکسان نبوده و یک حوزه می تواند شامل مقادیری در رابطه با چندین دامنه باشد.

برفرض، دامنه www.google.com دارای زیردامنه ای به نام news است (news.google.com).

در صورتیکه زیردامنه mail آن (mail.google.com) از دامنه اختصاصی www.gmail.com نیز قابل دسترسی می باشد.

روش های جستجو:

نحوه دسترسی به یک سرور از طریق سامانه DNS

همانگونه که اشاره شد، اسامی نمادین در شبکه اینترنت که خود در قالب حوزه‌ها و زیر حوزه‌ها سازماندهی شده‌اند، در یک فایل متمرکز ذخیره نمی‌شوند بلکه روی کل شبکه اینترنت توزیع شده‌اند، به همین دلیل برای ترجمه یک نام به نشانی آی‌پی ممکن است چندین مرحله «پرس و جو» صورت بگیرد تا یک نشانی پیدا شود.

طبیعی است که یک پرس و جو برای تبدیل یک نام حوزه همیشه موفقیت آمیز نباشد و ممکن است به پرس و جوهای بیشتری نیاز شود یا حتی ممکن است یک نشانی نمادین اشتباه باشد و هیچ معادل نشانی آی‌پی نداشته باشد.

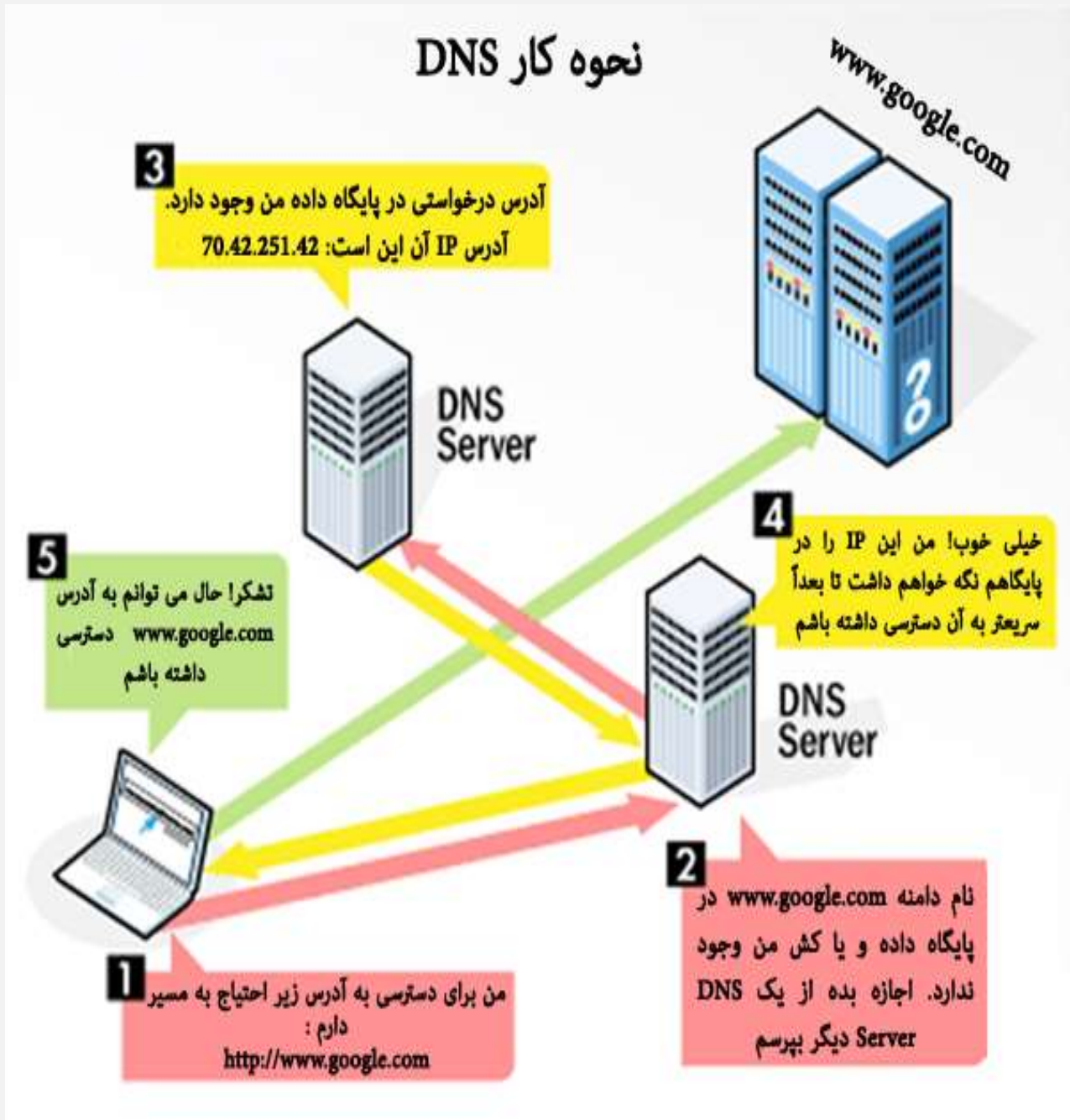
سه روش برای پرس و جو نام در سرویس دهنده‌های نام وجود دارد :

پرس و جو تکراری (Iterative Query)

پرس و جو بازگشتی (Recursive Query)

پرس و جو معکوس (Reverse Query)

نحوه دسترسی به یک سرور از طریق سامانه DNS



پرس و جوی تکراری

در پرس و جوی تکراری قسمت اعظم تلاش برای تبدیل یک نام بر عهده سرویس دهنده محلی است؛ این DNS حداقل به نشانی ماشین Root، به عنوان نقطه شروع نیاز دارد. وقتی یک تقاضای

ترجمه نشانی به سرویس دهنده محلی ارسال می شود در صورتی که قادر به ترجمه نام به معادل نشانی آی پی آن باشد، معادل نشانی آی پی نام مورد نظر را به تقاضا کننده برمی گرداند. (این حالت وقتی است که سرویس دهنده محلی قبلاً آن نام را ترجمه و در یک فایل ذخیره کرده باشد.) در غیر این صورت سرویس دهنده محلی خودش یک تقاضا برای DNS سطح بالا ارسال می کند. این سرویس دهنده، نشانی ماشینی را که می تواند برای ترجمه نام مورد نظر مفید باشد، به سرویس دهنده محلی معرفی می کند؛ سرویس دهنده محلی مجدداً یک تقاضا به ماشین معرفی شده در مرحله قبل ارسال می کند.

در این حالت هم سرویس دهنده نام می تواند در صورت یافتن نشانی آی پی با آن نام حوزه، آنرا ترجمه کند و یا آنکه نشانی سرویس دهنده سطح پایینتری را به او برگرداند.

این روند ادامه می یابد تا DNS نهایی نام مورد نظر را به نشانی آی پی ترجمه نماید. برای درک بهتر از روند کار به شکل زیر دقت کنید. در این مثال فرض شده است که یک برنامه کاربردی با فراخوانی «تابع تحلیلگر نام»، تقاضای ترجمه نام www.microsoft.com را می نماید. مراحل که انجام می شود به شرح زیر است :

در مرحله اول برنامه کاربردی با فراخوانی «تابع تحلیل نام»، تقاضای ترجمه نشانی www.microsoft.com را برای سرویس دهنده محلی ارسال کرده و منتظر می ماند.

در مرحله دوم، سرویس دهنده محلی از سرویس دهنده Root (که حوزه های متفاوت را تفکیک می کند) نشانی ماشینی یک DNS که متولی حوزه com است را سؤال می کند.

در مرحله سوم، نشانی سرویس دهنده مربوط به حوزه com برمی گردد.

در مرحله چهارم، سرویس دهنده محلی، از ماشین معرفی شده در مرحله قبلی، نشانی سرویس دهنده مربوط به حوزه Microsoft.com را سؤال می نماید.

در مرحله پنجم فهرستی از سرویس دهنده های DNS مربوط به Microsoft.com برمی گردد.

در مرحله ششم، سرویس دهنده محلی تقاضای ترجمه نشانی نمادین www.microsoft.com را از DNS متعلق به حوزه Microsoft.com می کند.

در مرحله هفتم، معادل نشانی آی پی نام www.microsoft.com برمی گردد.
در مرحله هشتم، نشانی آی پی خواسته شده در اختیار برنامه کاربردی قرار می گیرد.

پرس و جوی بازگشتی

در این روش هر گاه برنامه ای بخواهد نشانی آی پی معادل یک نام مثل cs.yale.edu را بدست آورد، بگونه ای که قبلاً اشاره شد، «تابع سیستمی تحلیل نام» را فراخوانی می کند. این تابع یک ماشین را بعنوان سرویس دهنده محلی از قبل می شناسد و بنابراین تقاضای تبدیل نام را به روش UDP برای آن ارسال کرده و منتظر جواب می ماند (پاسخ نهایی DNS طبیعتاً باید یک نشانی ۳۲ بیتی معادل نشانی آی پی یک ماشین باشد)

دو حالت ممکن است اتفاق بیفتد :

ممکن است در بانک اطلاعاتی مربوط به سرویس دهنده محلی، نشانی آی پی معادل با آن نام از قبل وجود داشته و بالطبع به سرعت مقدار معادل نشانی آی پی آن برمی گردد.

ممکن است در بانک اطلاعاتی سرویس دهنده محلی، معادل نشانی آی پی آن نام وجود نداشته باشد. مثلاً سرویس دهنده محلی در بانک اطلاعاتی خودش معادل نشانی آی پی نام cs.mit.edu را نداشته و طبیعتاً نمی تواند آن را ترجمه کند.

در چنین حالتی سرویس دهنده محلی موظف است بدون آنکه به تقاضا دهنده خبر بدهد، خودش رأساً به سرویس دهنده سطح بالاتر تقاضای ترجمه نشانی بدهد. در این حالت هم DNS سطح بالاتر به همین نحو، ترجمه نشانی را پیگیری می کند. یعنی اگر معادل نشانی آی پی آن نام را داشته باشد آنرا برمی گرداند و در غیر اینصورت خودش از سرویس دهنده سطح پایینتر تقاضای ترجمه آن نام را می نماید و این مراحل تکرار می شود. در روش پرس و جوی بازگشتی ماشین سرویس دهنده محلی این مراحل متوالی را نمی بیند و هیچ کاری جز ارسال تقاضای ترجمه یک نشانی بر عهده ندارد و پس از ارسال تقاضا برای سرویس دهنده سطح بالا منتظر خواهد ماند.

بازهم تکرار می‌کنیم، روشی که DNS برای ترجمه نشانی بکار می‌برد می‌تواند بدون اتصال (UDP) باشد که این کار به سرعت عمل ترجمه نشانی می‌افزاید.

دقت کنید که در روش پرس و جوی تکراری نسبت به روش پرس و جوی بازگشتی، حجم عمده عملیات بر عهده سرویس دهنده DNS محلی است و مدیریت خطاها و پیگیری روند کار ساده تر خواهد بود و روش منطقی تری برای بکارگیری در شبکه اینترنت محسوب می‌شود. روش پرس و جوی بازگشتی برای شبکه های کوچک کاربرد دارد. برای درک بیشتر این روش به شکل زیر دقت کنید.

پرس و جوی معکوس :

فرض کنید حالتی بوجود بیاید که یک سرویس دهنده DNS، نشانی آی پی یک ماشین را بداند ولی نام نمادین معادل با آن را نداند. بعنوان مثال DNS مایل است بداند که چه نامی در شبکه اینترنت معادل با ۱۹۵/۱۳/۴۲/۷ می‌باشد.

در چنین حالتی مسئله کمی حادثر به نظر می‌رسد، چرا که برای ترجمه نامهای نمادین، چون این نامها دارای حوزه و زیرحوزه هستند، تحلیل نشانی ها ساده‌است. ولی ترجمه نشانی آی پی به معادل نام حوزه، از چنین روابطی تبعیت نمی‌کند؛ بعبارت بهتر هیچ ارتباط مستقیم و متناظری بین نشانی های آی پی و اسامی انتخاب شده در اینترنت وجود ندارد. برای یافتن نامهای متناظر با یک نشانی آی پی باید یک جستجوی کامل و در عین حال وقت گیر، انجام بشود.

روش کار بدین صورت است که سرویس دهنده محلی یک تقاضا برای DNS متناظر با شبکه‌ای که مشخصه آن در نشانی آی پی، مشخص شده، ارسال می‌کند.

بعنوان مثال نشانی آی پی شبکه‌ای را ۱۳۸/۱۴/۷/۱۳ در نظر بگیرید، نشانی کلاس B و مشخصه آن ۱۳۸/۱۴/۰/۰ است. زمانی که مؤسسه‌ای یک کلاس نشانی آی پی ثبت می‌دهد یک سرویس دهنده DNS، متناظر با شبکه خود ایجاد کرده و آنرا نیز معرفی می‌کند. سرویس دهنده محلی بایستی نشانی DNS متناظر با شبکه ۱۳۸/۱۴/۰/۰ را پیدا کرده و سپس برای آن یک تقاضا ارسال کند. DNS مربوط به این شبکه، براساس زیر شبکه‌هایی که دارد، این سؤال را از طریق سرویس

دهنده های متناظر با هر زیر شبکه پیگیری می کند. (چون هر زیر شبکه یک سرویس دهنده DNS مخصوص به خود دارد) نهایتاً یک نام نمادین حوزه معادل با آن نشانی آی پی بر خواهد گشت.

ساختار دامنه :

نام دامنه از ارقام و حروفی تشکیل شده است. یکی قسمت نام کارساز است، دیگری نام دامنه و دیگری زیر دامنه است.

مثلا <http://www.google.com> را در نظر بگیرید:

http پروتکل انتقال اطلاعات در وب است. نشانه های //: جهت جداسازی پروتکل از دامنه استفاده می شود. http:// جزء سامانه نام دامنه قرار نمی گیرد. قسمت www نام زیر دامنه است. قسمت google نام دامنه و قسمت .com کارساز می باشد. هر زیر دامنه می تواند آدرس IP متفاوتی با نام دامنه داشته باشد.

نام دامنه و زیر دامنه را صاحب دامنه انتخاب و ثبت می کند.

این قسمت ها شامل حروف و اعداد انگلیسی و علامت منقی (-) نیز می تواند در میان اعداد و حروف (و نه در ابتدا و انتها) قرار گیرد.

کارسازهای مختلف، توسط آیکان (Icann) تصویب و در دسترس قرار می گیرد و شامل ۲ تا ۶ حرف انگلیسی می باشد.

ثبت دامنه در بسیاری از کارسازها نیاز به مجوزهای مخصوص دارد.

کارسازهای ۲ حرفی، در اختیار کشورهای صاحب آنها قرار می گیرد و قوانین ثبت در این کارسازها، توسط حکومت ها تعیین می گردد.

مثلا us در اختیار کشور آمریکا، ir در اختیار کشور ایران و fr در اختیار کشور فرانسه می باشد.

آیکن پروژه ای را در دست دارد تا ثبت نام های دامنه را به زبان های مختلف بین المللی امکان پذیر نماید. این پروژه هم اکنون در حالت آزمایش و بررسی قرار دارد.

درس ۳

FTP

امروزه از پروتکل های متعددی در شبکه های کامپیوتری استفاده می گردد که صرفاً تعداد اندکی از آنان به منظور انتقال داده طراحی و پیاده سازی شده اند . اینترنت نیز به عنوان يك شبکه گسترده از این قاعده مستثنی نبوده و در این رابطه از پروتکل های متعددی استفاده می شود.

برای بسیاری از کاربران اینترنت همه چیز محدود به وب و پروتکل مرتبط با آن یعنی HTTP است ، در صورتی که در این عرصه از پروتکل های متعدد دیگری نیز استفاده می گردد. FTP نمونه ای در این زمینه است .

پروتکل FTP چیست ؟

تصویر اولیه اینترنت در ذهن بسیاری از کاربران، استفاده از منابع اطلاعاتی و حرکت از سایتی به سایت دیگر است و شاید به همین دلیل باشد که اینترنت در طی سالیان اخیر به سرعت رشد و متداول شده است . بسیاری از کارشناسان این عرصه اعتقاد دارند که اینترنت گسترش و عمومیت خود را مدیون سرویس وب می باشد .

فرض کنید که سرویس وب را از اینترنت حذف نمائیم . برای بسیاری از ما این سوال مطرح خواهد شد که چه نوع استفاده ای را می توانیم از اینترنت داشته باشیم ؟ در صورت تحقق چنین شرایطی یکی از عملیاتی که کاربران قادر به انجام آن خواهند بود ، دریافت داده ، فایل های صوتی ، تصویری و سایر نمونه فایل های دیگر با استفاده از پروتکل FTP^۱ است.

^۱File Transfer Protocol

ویژگی های پروتکل FTP

- پروتکل FTP ، اولین تلاش انجام شده برای ایجاد يك استاندارد به منظور مبادله فایل بر روی شبکه های مبتنی بر پروتکل TCP/IP است که از اوایل سال ۱۹۷۰ مطرح و مشخصات استاندارد آن طی RFC ۹۵۹ در اکتبر سال ۱۹۸۵ ارائه گردید .
- پروتکل FTP دارای حداکثر انعطاف لازم و در عین حال امکان پذیر به منظور استفاده در شبکه های مختلف با توجه به نوع پروتکل شبکه است .
- پروتکل FTP از مدل سرویس گیرنده - سرویس دهنده تبعیت می نماید . برخلاف HTTP که يك حاکم مطلق در عرصه مرورگرهای وب و سرویس دهندگان وب است ، نمی توان ادعای مشابهی را در رابطه با پروتکل FTP داشت و هم اینک مجموعه ای گسترده از سرویس گیرندگان و سرویس دهندگان FTP وجود دارد .
- برای ارسال فایل با استفاده از پروتکل FTP به يك سرویس گیرنده FTP نیاز می باشد . ویندوز دارای يك برنامه سرویس گیرنده FTP از قبل تعبیه شده می باشد ولی دارای محدودیت های مختص به خود می باشد . در این رابطه نرم افزارهای متعددی تاکنون طراحی و پیاده سازی شده است:

ulletProofFTP ، WS FTP Professional ، FTP Explorer و Smart FTP نمونه هایی در این زمینه می باشند .

پروتکل FTP را می توان به عنوان يك سیستم پرس وجو نیز تلقی نمود چراکه سرویس گیرندگان و سرویس دهندگان گفتگوی لازم به منظور تأیید یکدیگر و ارسال فایل را انجام می دهند. علاوه بر این، پروتکل فوق مشخص می نماید که سرویس گیرنده و سرویس دهنده، داده را بر روی کانال گفتگو ارسال نمی نمایند . در مقابل ، سرویس گیرنده و سرویس دهنده در خصوص نحوه ارسال فایل ها بر روی اتصالات مجزا و جداگانه (يك اتصال برای هر ارسال داده) با یکدیگر گفتگو خواهند کرد (نمایش لیست فایل های موجود در يك دایرکتوری نیز به عنوان يك ارسال فایل تلقی می گردد) .

پروتکل FTP امکان استفاده از سیستم فایل را مشابه پوسته یونیکس و یا خط دستور ویندوز در اختیار کاربران قرار می دهد .

سرویس گیرنده در ابتدا يك پیام را برای سرویس دهنده ارسال و سرویس دهنده نیز به آن پاسخ خواهد داد و در ادامه ارتباط غیرفعال می گردد . وضعیت فوق با سایر پروتکل هائی که به صورت تراکنشی کار می کنند ، متفاوت می باشد (نظیر پروتکل HTTP) . برنامه های سرویس گیرنده زمانی قادر به شبیه سازی يك محیط تراکنشی می باشند که از مسائلی که قرار است در آینده محقق شوند ، آگاهی داشته باشند . در واقع ، پروتکل FTP يك دنباله stateful از يك و یا چندین تراکنش است .

سرویس گیرندگان ، مسئولیت ایجاد و مقداردهی اولیه درخواست ها را برعهده دارند که با استفاده از دستورات اولیه FTP انجام می گردد. دستورات فوق ، عموماً سه و یا چهار حرفی می باشند (مثلاً برای تغییر دایرکتوری از دستور CWD استفاده می شود) . سرویس دهنده نیز بر اساس يك فرمت استاندارد به سرویس گیرندگان پاسخ خواهد داد (سه رقم که به دنبال آن از space استفاده شده است به همراه يك متن تشریحی) . سرویس گیرندگان می بایست صرفاً به کد عددی نتیجه استناد نمایند چراکه متن تشریحی تغییر پذیر بوده و در عمل برای اشکال زدائی مفید است (برای کاربران حرفه ای) .

پروتکل FTP دارای امکانات حمایتی لازم برای ارسال داده با نوع های مختلف می باشد . دو فرمت متداول ، اسکی برای متن (سرویس گیرنده با ارسال دستور TYPE A ، موضوع را به اطلاع سرویس دهنده می رساند) و image برای داده های باینری است (توسط TYPE I مشخص می گردد) . ارسال داده با فرمت اسکی در مواردی که ماشین سرویس دهنده و ماشین سرویس گیرنده از استانداردهای متفاوتی برای متن استفاده می نمایند ، مفید بوده و يك سرویس گیرنده می تواند پس از دریافت داده آن را به فرمت مورد نظر خود ترجمه و استفاده نماید . مثلاً در نسخه های ویندوز از يك دنباله carriage return و linefeed برای نشان دادن انتهای خط استفاده می گردد در صورتی که در سیستم های مبتنی بر یونیکس صرفاً از يك

linefeed استفاده می شود. برای ارسال هر نوع داده که به ترجمه نیاز نداشته باشد، می توان از ارسال باینری استفاده نمود.

اتخاذ تصمیم در رابطه با نوع ارسال فایل ها در اختیار سرویس گیرنده است (برخلاف HTTP که می تواند به سرویس گیرنده نوع داده ارسال را اطلاع دهد). معمولاً " سرویس گیرندگان ارسال باینری را انتخاب می نمایند و پس از دریافت فایل ، ترجمه لازم را انجام خواهند داد . ارسال باینری ذاتاً دارای کارآئی بیشتری است چراکه سرویس دهنده و سرویس گیرنده نیازی به انجام تراکنش های on the fly نخواهند داشت . ارسال اسکی گزینه پیش فرض انتخابی توسط پروتکل FTP است و در صورت نیاز به ارسال باینری ، سرویس گیرنده می بایست این موضوع را از سرویس دهنده درخواست نماید .

یک اتصال پروتکل TCP/IP (نسخه شماره چهار) شامل دو نقطه مجزا می باشد که هر نقطه از یک آدرس IP و یک شماره پورت استفاده می نماید . برقراری ارتباط بین یک سرویس گیرنده و یک سرویس دهنده منوط به وجود چهار عنصر اطلاعاتی است : آدرس سرویس دهنده ، پورت سرویس دهنده ، آدرس سرویس گیرنده و پورت سرویس گیرنده . در زمان برقراری یک ارتباط ، سرویس گیرنده از یک شماره پورت استفاده می نماید . این شماره پورت می تواند متناسب با نوع عملکرد برنامه سرویس گیرنده به صورت اختیاری و یا اجباری باشد . مثلاً " برخی برنامه های سرویس گیرنده به منظور ارتباط با سرویس دهنده ، نیازمند استفاده از یک شماره پورت خاص می باشند (نظیر برنامه های سرویس گیرنده وب و یا مرورگرهای وب که از پورت شماره ۸۰ به منظور ارتباط با سرویس دهنده وب استفاده می نمایند) . در مواردی که الزامی در خصوص شماره پورت وجود ندارد از یک شماره پورت موقتی و یا ephemeral استفاده می گردد . این نوع پورت ها موقتی بوده و توسط IP stack ماشین مربوطه به متقاضیان نسبت داده شده و پس از خاتمه ارتباط ، پورت آزاد می گردد . با توجه به این که اکثر IP Stacks بلافاصله از پورت موقت آزاد شده استفاده نخواهند کرد (تا زمانی که تمام pool تکمیل نشده باشد) ، در

صورتی که سرویس گیرنده مجدداً درخواست برقراری يك ارتباط را نماید ، يك شماره پورت موقتی دیگر به وی تخصیص داده می شود .

پروتکل FTP منحصرأ از پروتکل TCP استفاده می نماید(هرگز از پروتکل UDP استفاده نمی شود) . معمولاً پروتکل های لایه Application (با توجه به مدل مرجع OSI) از یکی از پروتکل های TCP و یا UDP استفاده می نمایند (به جزء پروتکل DNS) . پروتکل FTP نیز از برخی جهات شرایط خاص خود را دارد و برای انجام وظایف محوله از دو پورت استفاده می نماید . این پروتکل معمولاً از پورت شماره ۲۰ برای ارسال داده و از پورت ۲۱ برای گوش دادن به فرامین استفاده می نماید . توجه داشته باشید که برای ارسال داده همواره از پورت ۲۰ استفاده نمی گردد و ممکن است در برخی موارد از پورت های دیگر استفاده شود .

اکثر سرویس دهندگان FTP از روش خاصی برای رمزنگاری اطلاعات استفاده نمی نمایند و در زمان login سرویس گیرنده به سرویس دهنده ، اطلاعات مربوط به نام و رمز عبور کاربر به صورت متن معمولی در شبکه ارسال می گردد . افرادی که دارای يك Packet sniffer بین سرویس گیرنده و سرویس دهنده می باشند ، می توانند به سادگی اقدام به سرقت نام و رمز عبور نمایند . علاوه بر سرقت رمزهای عبور ، مهاجمان می توانند تمامی مکالمات بر روی اتصالات FTP را شنود و محتویات داده های ارسالی را مشاهده نمایند . پیشنهادات متعددی به منظور ایمن سازی سرویس دهنده FTP مطرح می گردد ولی تا زمانی که رمزنگاری و امکانات حفاظتی در سطح لایه پروتکل IP اعمال نگردد (مثلاً رمزنگاری توسط IPsec) ، نمی بایست از FTP استفاده گردد خصوصاً اگر بر روی شبکه اطلاعات مهم و حیاتی ارسال و یا دریافت می گردد .

همانند بسیاری از پروتکل های لایه Application ، پروتکل FTP دارای کدهای وضعیت خطاء مختص به خود می باشد (همانند HTTP) که اطلاعات لازم در خصوص وضعیت ارتباط ایجاد شده و یا درخواستی را ارائه می نماید . زمانی که يك درخواست (GET , PUT) برای يك سرویس دهنده FTP ارسال می گردد ، سرویس دهنده پاسخ خود را به صورت يك رشته اعلام

می نماید . اولین خط این رشته معمولاً " شامل نام سرویس دهنده و نسخه نرم افزار FTP است . در ادامه می توان دستورات GET و یا PUT را برای سرویس دهنده ارسال نمود . سرویس دهنده با ارائه يك پیام وضعیت به درخواست سرویس گیرندگان پاسخ می دهد . کدهای وضعیت برگردانده شده را می توان در پنج گروه متفاوت تقسیم نمود :

کدهای xx1 : پاسخ اولیه

کدهای xx2 : درخواست بدون خطاء اجراء گردید .

کدهای xx3 : به اطلاعات بیشتری نیاز است .

کدهای xx4 : يك خطاء موقت ایجاد شده است .

کدهای xx5 : يك خطاء دائمی ایجاد شده است .

FTP ، يك پروتکل ارسال فایل است که با استفاده از آن سرویس گیرندگان می توانند به سرویس دهندگان متصل و صرفنظر از نوع سرویس دهنده اقدام به دریافت و یا ارسال فایل نمایند . پروتکل FTP به منظور ارائه خدمات خود از دو حالت متفاوت استفاده می نماید : Active Mode و Passive Mode . مهمترین تفاوت بین روش های فوق جایگاه سرویس دهنده و یا سرویس گیرنده در ایجاد و خاتمه يك ارتباط است .

همانگونه که قبلاً اشاره کردیم ، يك اتصال پروتکل TCP/IP (نسخه شماره چهار) شامل دو نقطه مجزا می باشد که هر نقطه از يك آدرس IP و يك شماره پورت استفاده می نماید . برقراری ارتباط بین يك سرویس گیرنده و يك سرویس دهنده منوط به وجود چهار عنصر اطلاعاتی است : آدرس سرویس دهنده ، پورت سرویس دهنده ، آدرس سرویس گیرنده و پورت سرویس گیرنده . در زمان برقراری يك ارتباط ، سرویس گیرنده از يك شماره پورت استفاده می نماید . این شماره پورت می تواند متناسب با نوع عملکرد برنامه سرویس گیرنده به صورت اختیاری و یا اجباری باشد . مثلاً " برخی برنامه های سرویس گیرنده به منظور ارتباط با سرویس دهنده ، نیازمند استفاده از يك

شماره پورت خاص می باشند (نظیر برنامه های سرویس گیرنده وب و یا مرورگرهای وب که از پورت شماره ۸۰ به منظور ارتباط با سرویس دهنده وب استفاده می نمایند) . در مواردی که الزامی در خصوص شماره پورت وجود ندارد از يك شماره پورت موقتی و یا ephemeral استفاده می گردد. این نوع پورت ها موقتی بوده و توسط IPstack ماشین مربوطه به متقاضیان نسبت داده شده و پس از خاتمه ارتباط ، پورت آزاد می گردد . با توجه به این که اکثر IP Stacks بلافاصله از پورت موقت آزاد شده استفاده نخواهند کرد (تا زمانی که تمام pool تکمیل نشده باشد) ، در صورتی که سرویس گیرنده مجدداً درخواست برقراری يك ارتباط را نماید ، يك شماره پورت موقتی دیگر به وی تخصیص داده می شود .

در ادامه به بررسی هر يك از روش های Active و Passive در پروتکل FTP خواهیم پرداخت .

:Active Mode

Active Mode ، روش سنتی ارتباط بین يك سرویس گیرنده FTP و يك سرویس دهنده می باشد که عملکرد آن بر اساس فرآیند زیر است :

- سرویس گیرنده يك ارتباط با پورت ۲۱ سرویس دهنده FTP برقرار می نماید . پورت ۲۱ ، پورته ای است که سرویس دهنده به آن گوش فرا می دهد تا از صدور فرامین آگاه و آنان را به ترتیب پاسخ دهد . سرویس گیرنده برای برقراری ارتباط با سرویس دهنده از يك پورت تصادفی و موقتی (بزرگتر از ۱۰۲۴) استفاده می نماید (پورت x) .
- سرویس گیرنده شماره پورت لازم برای ارتباط سرویس دهنده با خود را از طریق صدور دستور PORTN+۱ به وی اطلاع می دهد (پورت x+۱)
- سرویس دهنده يك ارتباط را از طریق پورت ۲۰ خود با پورت مشخص شده سرویس گیرنده (پورت x+۱) برقرار می نماید .

سرور	لطفاً به من از طریق پورت ۱۹۳۱ بر روی آدرس
گیرنده	IP: ۱۹۲/۱۶۸/۱/۲ متصل و سپس داده را ارسال
	نمائید .
سرور	
دهنده	تأیید دستور

در فرآیند فوق ، ارتباط توسط سرور گیرنده آغاز و پاسخ به آن توسط سرور دهنده و از طریق پورت $x+1$ که توسط سرور گیرنده مشخص شده است ، انجام می شود . در صورتی که سرور گیرنده از سیستم ها و دستگاه های امنیتی خاصی نظیر فایروال استفاده کرده باشد ، می بایست تهدیدات لازم به منظور ارتباط کامپیوترهای میزبان راه دور به سرور گیرنده پیش بینی تا آنان بتوانند به هر پورت بالاتر از ۱۰۲۴ سرور گیرنده دستیابی داشته باشند . بدین منظور لازم است که پورت های اشاره شده بر روی ماشین سرور گیرنده open باشند . این موضوع می تواند تهدیدات و چالش های امنیتی متعددی را برای سرور گیرندگان به دنبال داشته باشد .

Passive Mode

در Passive Mode ، که به آن " مدیریت و یا اداره سرور گیرندگان FTP " نیز گفته می شود از فرآیند زیر استفاده می گردد :

- سرور گیرنده دو پورت را فعال می نماید (پورت x و $x+1$)
- ارتباط اولیه از طریق پورت x سرور گیرنده با پورت ۲۱ سرور دهنده آغاز می گردد .
- سرور دهنده يك پورت را فعال (Y) و به سرور گیرنده شماره پورت را اعلام می نماید .
- در ادامه سرور گیرنده يك اتصال از طریق پورت $x+1$ با پورت y سرور دهنده برقرار می نماید .

سرویس گیرنده	لطفاً به من بگوئید که از کجا می توانم داده را دریافت نمایم
سرویس دهنده	با من از طریق پورت ۴۰۲۳ بر روی آدرس IP: ۱۹۲/۱۶۸/۱/۲۵ ارتباط برقرار نمائید .

در فرآیند فوق ، سرویس گیرنده دارای نقش محوری است و فایروال موجود بر روی سرویس گیرنده می تواند درخواست های دریافتی غیرمجاز به پورت های بالاتر از ۱۰۲۴ را به منظور افزایش امنیت بلاک نماید . در صورتی که بر روی کامپیوترهای سرویس دهنده نیز فایروال نصب شده باشد ، می بایست پیکربندی لازم به منظور استفاده از پورت های بالاتر از ۱۰۲۴ بر روی آن انجام و آنان open گردند . باز نمودن پورت های فوق بر روی سرویس دهنده می تواند چالش های امنیتی خاصی را برای سرویس دهنده به دنبال داشته باشد .

متأسفانه تمامی سرویس گیرندگان FTP از Passive Mode حمایت نمی نمایند . اگر يك سرویس گیرنده بتواند به يك سرویس دهنده login نماید ولی قادر به ارسال داده بر روی آن نباشد ، نشاندهنده این موضوع است که فایروال و یا Gateway برای استفاده از Passive Mode به درستی پیکربندی نشده است .

ملاحظات امنیتی :

در صورتی که فایروال های موجود بر روی کامپیوترهای سرویس گیرنده به درستی پیکربندی نگردند آنان نمی توانند از ActiveMode استفاده نمایند . در Passive Mode استحکام سیستم امنیتی در سمت سرویس دهنده و توسط فایروال مربوطه انجام خواهد شد . بنابراین لازم است به سرویس دهنده اجازه داده شود که به اتصالات هر پورت بالاتر از ۱۰۲۴ پاسخ دهد . ترافیک فوق ، معمولاً توسط فایروال سرویس دهنده بلاک می گردد . در چنین شرایطی امکان استفاده از Passive Mode وجود نخواهد داشت .

Passive Mode و یا Active Mode ؟

با توجه به مستندات درج شده در RFC ۱۵۷۹ ، استفاده از Passive Mode به دلایل متعددی به Active Mode ترجیح داده می شود :

- تعداد سرویس دهندگان موجود بر روی اینترنت به مراتب کمتر از سرویس گیرندگان می باشد .
- با استفاده از امکانات موجود می توان سرویس دهندگان را پیگیری تا بتوانند از مجموعه پورت های محدود و تعریف شده ای با در نظر گرفتن مسائل امنیتی ، استفاده نمایند.

پیگیری فایروال

جدول زیر پیگیری فایروال در Active Mode و Passive Mode را نشان می دهد .

Active Mode	
from any client port >۱۰۲۴ to port ۲۱ on the server	Server Inbound
from port ۲۰ on the client on any port > ۱۰۲۴	Server Outbound
ports ۲۰ from the server to any port >۱۰۲۴ on client	Client Inbound
from any port >۱۰۲۴ to port ۲۱ on the server	Client Outbound
Passive Mode	
port ۲۱ and any port >۱۰۲۴ from client/anywhere, from any port >۱۰۲۴	Server Inbound
port ۲۱ and any port >۱۰۲۴ to client/anywhere,	Server

to any port >۱۰۲۴	Outbound
Return traffic, any port > ۱۰۲۴ from server using any port >۱۰۲۴	Client Inbound

و اما يك نکته ديگر در رابطه با پروتکل FTP !

در صورتی که در زمان دریافت يك فایل با استفاده از پروتکل FTP مشکلات خاصی ایجاد که منجر به قطع ارتباط با سرویس دهنده FTP گردد ، سرویس گیرنده می تواند با مشخص کردن يك offset از فایل دریافتی به سرویس دهنده اعلام نماید که عملیات ارسال را از جایی که ارتباط قطع شده است ، ادامه دهد (سرویس گیرنده از محلی شروع به دریافت فایل می نماید که ارتباط غیرفعال شده بود) . استفاده از ویژگی فوق به امکانات سرویس دهنده FTP بستگی دارد .

درس ۴

HTTP

در اینترنت همانند سایر شبکه های کامپیوتری از پروتکل های متعدد و با اهداف مختلف استفاده می گردد. هر پروتکل از يك ساختار خاص برای ارسال و دریافت اطلاعات (بسته های اطلاعاتی) استفاده نموده و ترافیک مختص به خود را در شبکه ایجاد می نماید. HTTP (برگرفته از Hyper Text Transfer Protocol) ، یکی از متداولترین پروتکل های لایه application است که مسئولیت ارتباط بین سرویس گیرندگان و سرویس دهندگان وب را برعهده دارد.

در ادامه با پروتکل فوق بیشتر آشنا خواهیم شد.

پروتکل HTTP چیست ؟

دنیای شبکه های کامپیوتری دارای عمری چند ساله است و بسیاری از کاربران ، ضرورت استفاده از شبکه را همزمان با متداول شدن اینترنت در اوایل سال ۱۹۹۰ دریافتند . عمومیت اینترنت، رشد و گسترش شبکه های کامپیوتری را به دنبال داشته است . اینترنت نیز با سرعتی باورنکردنی رشد و امروزه شاهد ایجاد ده ها میلیون وب سایت در طی يك سال در این عرصه می باشیم . تمامی وب سایت های موجود بر روی اینترنت از پروتکل HTTP استفاده می نمایند . با این که پروتکل HTTP با استفاده از پروتکل های دیگری نظیر IP و TCP مأموریت خود را انجام می دهد ، ولی این پروتکل HTTP است که به عنوان زبان مشترک ارتباطی بین سرویس گیرنده و سرویس دهنده وب به رسمیت شناخته شده و از آن استفاده می گردد . در واقع مرورگر وب صدای خود را با استفاده از پروتکل HTTP به گوش سرویس دهنده وب رسانده و از وی درخواست يك صفحه وب را می نماید.

به منظور انجام يك تراكنش موفقیت آمیز بین سرویس گیرندگان وب (نظیر IE) و سرویس دهندگان وب (نظیر IIS) ، به اطلاعات زیادی نیاز خواهد بود . پس از handshake پروتکل TCP/IP ، مرورگر اطلاعات گسترده ای را برای سرویس دهنده وب ارسال می نماید .

يك بسته اطلاعاتی نمونه در شكل زیر نشان داده شده است :

```

0x0010: 480e cf63 06ba 0050 bb3d ff46 e67d 0e87 H...P...F)..
0x0020: 5018 ffff 899f 0000 4745 5420 2f20 4854 P.....GET /HT
0x0030: 5450 2f31 2e31 040a 486f 7374 3a20 7777 TP/1.1.Host:ww
0x0040: 772e 676f 6f67 6c65 2e63 610d 0a55 7365 w.google.ca Usa
0x0050: 722d 4167 656e 743a 204d 6f7a 696c 6c61 r-Agent:Mozilla
0x0060: 2f35 2e30 2028 5769 6e64 6f77 733b 2055 /5.0.(Windows:U
0x0070: 3b20 5769 6e64 6f77 7320 4e54 2035 2e31 ;.Windows.NT.5.1
0x0080: 3b20 656e 2d55 533b 2072 763a 312e 372e ;.en-US;rv:1.7
0x0090: 3130 2920 4765 636b 6f2f 3230 3035 3037 10).Gecko/200507
0x00a0: 3136 2046 6972 6566 6f78 2f31 2e30 2e36 16.Firefox/1.0.6
0x00b0: 0d0a 4163 6365 7074 3a20 7465 7874 2f78 ..Accept:text/x
0x00c0: 6d6c 2c61 7070 6c69 6361 7469 6f6e 2f78 ml.application/x
0x00d0: 6d6c 2c61 7070 6c69 6361 7469 6f6e 2f78 ml.application/x
0x00e0: 6874 6d6c 2b78 6d6c 2e74 6578 742f 6874 html+xml;text/ht
0x00f0: 6d6c 3b71 3d30 2e39 2e74 6578 742f 706c ml;q=0.9;text/pl
0x0100: 6169 6e3b 713d 302e 382c 696d 6167 652f am;q=0.8,image/
0x0110: 706e 672c 2a2f 2a3b 713d 302e 350d 0a41 png;*/q=0.5;A
0x0120: 6363 6570 742d 4c61 6e67 7561 6765 3a20 ccept-Languag
0x0130: 656e 2d75 732c 656e 3b71 3d30 2e35 0d0a en-us,en;q=0.5;
0x0140: 2d2d 2d2d 2d2d 2d2d 2d2d 2d2d 2d2d 2d3a .....:
0x0150: 202d 2d2d 2d2d 2d2d 2d2d 2d0d 0a41 .....:A
0x0160: 6363 6570 742d 4368 6172 7365 743a 2049 ccept-Charset:1
0x0170: 534f 2d38 3835 392d 312c 7574 662d 383b SO-8859-1:utf-8;
0x0180: 713d 302e 372c 2a3b 713d 302e 370d 0a4b q=0.7;*/q=0.7;.k
0x0190: 6565 702d 416c 6976 653a 2033 3030 0d0a eep-Alive:300.
0x01a0: 436f 6e6e 6563 7469 6f6e 3a20 6b65 6570 Connection:keep
0x01b0: 2d61 6c69 7665 0d0a 436f 6f6b 6965 3a20 -Alive;Cooker:
0x01c0: 5052 4546 3d49 443d 3031 6130 3832 3234 PRF=ID=01a0822d
0x01d0: 3534 6163 6232 3933 3a4c 443d 656e 3a54 S4acb293;ID=en:1
0x01e0: 4d3d 3131 3231 3633 3830 3934 3a4c 4d3d M=1121638094;LM=
0x01f0: 3131 3231 3633 3830 3934 3a53 3d6a 2d30 1121638094;S=j-0
0x0200: 3970 3851 6870 5953 5f43 7253 500d 0a0d 9a8QhpyS CrSP...
0x0210: 0a

```

توضیحات :

داده مربوط به پروتکل لایه application (در این مورد خاص پروتکل HTTP) ، پس از هدر TCP/IP قرار می گیرد . جدول زیر برخی اطلاعات مبادله شده بین سرویس گیرنده و سرویس دهنده وب را نشان می دهد .

نوع اطلاعات	عملکرد
GET /HTTP/۱.۱	سرویس گیرنده وب يك درخواست GET را برای سرویس دهنده وب ارسال و از وی درخواست اطلاعاتی را با

	<p>استفاده از پروتکل ۱/۱ HTTP می نماید.</p> <p>پروتکل HTTP دارای نسخه شماره يك نیز می باشد که امروزه عموماً از نسخه فوق استفاده نمی گردد و در مقابل از نسخه ۱.۱ استفاده می شود.</p>
<p>Host: www.google.ca</p>	<p>وب سایتی است که سرویس گیرنده قصد ارتباط با آن را دارد .</p>
<p>User-agent: Mozilla/۵٫۰ (Windows; U; Windows NT ۵٫۱;</p>	<p>به سرویس دهنده وب ، نوع نرم افزار سرویس گیرنده (در این مورد خاص Mozilla version ۵٫۰) و نوع سیستم عامل نصب شده بر روی کامپیوتر (در این مورد خاص Windows version NT ۵٫۱ و یا همان ویندوز XP) اعلام می گردد.</p>
<p>en-US; rv: ۱٫۷٫۱۰)</p>	<p>نوع character set استفاده شده به سرویس دهنده اعلام می گردد (در این مورد خاص از en:us و نسخه شماره ۷ . ۱۰</p>

	<p>۱. استفاده شده است) .</p>
Gecko/۲۰۰۵۰۷۱۶ Firefox/۱/۰/۶	<p>نام مرورگر استفاده شده توسط سرویس گیرنده به سرویس دهنده وب اعلام می گردد (در این مورد خاص از مرورگر FireFox استفاده شده است) .</p>
<p>Accept: text/xml, application/xml, application/xhtml+xml</p>	<p>سرویس گیرنده به سرویس دهنده وب فرمت اطلاعاتی را که می تواند دریافت نماید ، اعلام می نماید (در این مورد خاص هم برای متن و هم برای application از فرمت xml استفاده می گردد) .</p>
text/html; q=۰/۹, text/plain; q=۰/۸, image/png, */*;q=۰/۵	<p>سرویس گیرنده به سرویس دهنده نوع فرمت متن دریافتی را اعلام می نماید (در این مورد خاص html و یا plaintext) . همچنین فرمت فایل های گرافیکی (در این مورد خاص png و سایر فرمت های متداول) نیز اعلام می گردد .</p>
Accept-Charset:	لیست character set که

<p>ISO-۸۸۵۹-۱, utf-۸; q=۰/۷, *;q=۰/۷</p>	<p>سرویس گیرنده وب قادر به فهم آنان است، اعلام می گردد (در این مورد خاص ISO-۸۸۵۹ , و یا utf-۸) .</p>
<p>Keep-Alive: ۳۰۰ Connection: keep-alive</p>	<p>به سرویس دهنده وب مدت زمان نگهداری session اعلام می گردد (در این مورد خاص ۳۰۰ ثانیه) . سرویس گیرندگان می توانند با صراحت پایان يك session را اعلام نمایند . در نسخه شماره ۱.۱ پروتکل HTTP ، ارتباط و یا اتصال برقرار شده فعال و یا open باقی خواهد ماند تا زمانی که سرویس گیرنده خاتمه آن را اعلام و یا مدت زمان حیات آن به اتمام رسیده باشد . در نسخه شماره يك پروتکل HTTP ، پس از هر درخواست و اتمام تراکنش ، ارتباط ایجاد شده غیرفعال و یا close می گردد .</p>
<p>Cookie:</p>	<p>cookie و مقدار مربوطه به آن</p>

PREF=ID=۰۱a۰۸۲۲۴۵۴acb۲۹۳:	اعلام می گردد. کوکی يك متن
LD=en:TM=۱۱۲۱۶۳۸۰۹۴	اسکی فلت می باشد که اطلاعات متفاوتی را در خود نگهداری می نماید . مدت زمان حیات يك کوکی می تواند موقت (تا زمانی که مرورگر فعال است) و یا دائم () ذخیره بر روی هارد دیسک کامپیوتر و در يك محدوده زمانی تعریف شده) باشد .

Useragent نوع مرورگر و سیستم عامل سرویس گیرنده را مشخص می نماید و این موضوع می تواند مواد اولیه لازم برای تدارک برخی حملات توسط مهاجمان را تامین نماید

حال با نوع و ماهیت اطلاعات ارسالی سرویس دهندگان وب به منظور پاسخ به درخواست سرویس گیرندگان آشنا خواهیم شد.

مرورگر وب ، صدای خود را با استفاده از پروتکل HTTP به گوش سرویس دهنده وب می رساند و از وی درخواست يك صفحه وب را می نماید.

سرویس دهنده وب علاوه بر این که با این صدا آشنا است خود نیز برای پاسخ به مرورگر وب از مجموعه قوانین آن تبعیت می کند .

پروتکل HTTP : يك معماری سرویس گیرنده و سرویس دهنده

سرویس گیرنده وب ، مقادیر خاصی را با اهداف کاملاً مشخص شده برای سرویس دهنده وب ارسال می نماید (حصول اطمینان از وجود يك زبان مشترك برای گفتگو بین سرویس گیرنده و سرویس دهنده وب) . سرویس دهنده پس از بررسی اطلاعات ارسالی ، آنان را تفسیر و متناسب با آن اطلاعاتی را برای سرویس گیرنده ارسال می نماید . در معماری فوق يك نرم افزار در سمت سرویس گیرنده و به عنوان يك سرویس گیرنده وب (نظیر IE و یا Mozilla Firefox) ایفای وظیفه می نماید و در سمت سرویس دهنده يك نرم افزار به عنوان سرویس دهنده وب (نظیر : IIS و یا Apache) وظایف تعریف شده خود را انجام می دهد.

سناریوی فوق مدل و یا معماری سرویس گیرنده - سرویس دهنده را در ذهن تداعی می نماید (معماری مبتنی بر درخواست و پاسخ) .

پاسخ سرویس دهنده :

شکل زیر يك بسته اطلاعاتی HTTP از مبداء يك سرویس دهنده به مقصد يك سرویس گیرنده را نشان می دهد (پاسخ سرویس دهنده) .

```

0x0020: 5010 1920 be07 0000 4854 5450 2f31 2e31 P.....HTTP/1.1
0x0030: 2032 3030 204f 4b0d 0a43 6163 6865 2643 .200_OK_Cache-C
0x0040: 6f6e 7472 6f6c 3a20 7072 6976 6174 650d ontrol:private;
0x0050: 0a43 6f6e 7465 6e74 2d54 7970 653a 2074 .Content-Type:t
0x0060: 6578 742f 6874 6d6c 0d0a 5365 7276 6572 ext/html.Server
0x0070: 3a20 4757 532f 322e 310d 0a54 7261 6e73 :.GWS/2.1.Trans
0x0080: 6665 722d 456e 636f 6469 6e67 3a20 6368 fer-Encoding:ch
0x0090: 756e 6b65 640d 0a44 6174 653a 2053 6174 unked_Date:Sat
0x00a0: 2c20 3330 204a 756c 2032 3030 3520 3134 .,30 Jul 2005 14
0x00b0: 3a31 343a 3530 2047 4d54 0d0a 0d0a 6132 :14:50 GMT...a2
0x00c0: 630d 0a3c 6874 6d6c 3e3c 6865 6164 3e3c c.<html><head><
0x00d0: 6d65 7461 2068 7474 702d 6571 7569 763d meta.http-equiv=
0x00e0: 2263 6f6e 7465 6e74 2d74 7970 6522 2063 "content-type"e

```

توضیحات :

جدول زیر برخی اطلاعات ارسالی توسط سرویس دهنده را نشان می دهد .

نوع اطلاعات	عملکرد
HTTP/۱.۱ ۲۰۰ OK	<p>به سرویس گیرنده اعلام می گردد که :</p> <ul style="list-style-type: none"> • سرویس دهنده وب از پروتکل HTTP نسخه ۱.۱ استفاده می نماید. • فایل درخواستی وی توسط سرویس دهنده پیدا شده است . <p>۲۰۰ ، يك كد وضعیت است که وضعیت پاسخ به درخواست را مشخص می نماید .</p>
Cache-Control: private	<p>مستند و یا فایل درخواستی سرویس گیرنده توسط يك پراکسی cache نخواهد شد و هدف آن صرفاً " برای کاربر متقاضی فایل است .</p>
Content-type: text/html	<p>فرمت ارسال فایل و یا مستند درخواستی به سرویس گیرنده وب اعلام می شود . در این مورد خاص ، اطلاعات با فرمت text/html ارسال می گردند .</p> <p>سرویس گیرنده وب دارای دانش لازم به منظور بررسی و نمایش اطلاعات با</p>

	فرمت اشاره شده می باشد .
Server: GWS/۲/۱	نوع سرویس دهنده و یا نرم افزار سرویس دهنده (سرویس دهنده وب) مشخص می گردد . در این مورد خاص ، سرویس دهنده وب Google نمایش داده شده است .
Transfer-Encoding: chunked	پروتکل HTTP نسخه شماره ۱.۱ از ارسال اطلاعات به صورت chunked حمایت می نماید. در روش فوق ، بدنه يك پیام به منظور ارسال مجموعه ای از ماژول ها اصلاح می گردد . مسولیت مشخص کردن اندازه هر ماژول ارسالی بر عهده یکی از فیلدهای موجود در این ساختار گذاشته می شود . در صورت ارسال معمولی اطلاعات توسط پروتکل HTTP ، از يك فیلد با نام "Content-Length" به منظور مشخص نمودن حجم داده ارسالی، استفاده می گردد .
Date: Sat ۳۰ Jul ۲۰۰۵ ۱۴:۱۴:۵۰ GMT	زمان و تاریخ سرویس دهنده وب مشخص می گردد.
<html><head><meta.http-equiv="content-type"	تگ های HTML ارسالی توسط سرویس دهنده وب به مقصد سرویس

گیرنده وب می باشند که توسط سرویس گیرندگان وب (نظیر IE) تفسیر و نمایش داده می شوند . با استفاده از گزینه view موجود در برنامه های مرورگر ، می توان تگ های HTML يك صفحه وب را مشاهده نمود .

HTTP ، پروتکلی با قابلیت های فراوان است که علیرغم برخی محدودیت ها ، دارای سابقه درخشانی در عرصه شبکه های کامپیوتری (اینترانت ، اینترنت) است .

HTTP پروتکلی است که امکان ارتباط بین سرویس گیرندگان و سرویس دهندگان وب را فراهم می نماید .
يك سرویس دهنده وب در واقع به عنوان يك سرویس دهنده HTTP نیز ایفای وظیفه می نماید .

زمانی که مرورگر وب درخواست يك صفحه را از سرویس دهنده وب می نماید، در واقع يك HTTPrequest را ارسال و سرویس دهنده وب نیز پاسخ آن را با يك HTTP response خواهد داد. يك پیام HTTP ، يك درخواست (request) و يا پاسخ (response) است که از يك ساختار خاص تبعیت می نماید .

HTTP به يك پروتکل خاص لایه حمل وابستگی نداشته و عموماً از پروتکل TCP استفاده می نماید (پورت شناخته شده ۸۰) .

کدهای وضعیت:

همانند بسیاری از پروتکل ها ، پروتکل HTTP بر اساس يك مدل سرویس گیرنده - سرویس دهنده کار می کند . کدهای وضعیت توسط تعداد زیادی از پروتکل های لایه application استفاده می گردد و می توان آنان را به پنج گروه عمده تقسیم نمود . جدول زیر گروه های پنج گانه کدهای وضعیت را در ارتباط با پروتکل HTTP نشان می دهد .

کد	عملکرد
۱XX	اطلاع رسانی برای استفاده در آینده
۲XX	انجام موفقیت آمیز تراکنش
۳XX	راهنمایی مجدد
۴XX	بروز خطاء سمت سرویس گیرنده
۵XX	بروز خطاء سمت سرویس دهنده

هر يك از پنج گروه فوق، دارای کدهای وضعیت زیر مجموعه ای می باشند که بیانگر جزئیات عملیات است . جدول زیر برخی از کدهای وضعیت هر يك از گروه های پنج گانه فوق را در ارتباط با پروتکل HTTP نشان می دهد .

کد	عملکرد
۲۰۰	تراکنش با موفقیت انجام شده است
۲۰۱	دستور POST با موفقیت انجام شده است
۲۰۲	درخواست ارسالی دریافت گردید.
۳۰۰	منبع درخواستی در مکان های مختلفی پیدا شده است

۳۰۱	منبع درخواستی به صورت دائم منتقل شده است
۳۰۲	منبع درخواستی به صورت موقت منتقل شده است
۴۰۰	درخواست نامناسب از جانب سرویس گیرنده
۴۰۱	درخواست غیرمجاز
۴۰۴	منبع درخواستی پیدا نگردید
۵۰۰	بروز خطاء بر روی سرویس دهنده
۵۰۱	متد استفاده شده ، پیاده سازی نشده است

درخواست های سرویس گیرندگان و دستورات :

سرویس گیرندگان وب به منظور استفاده از خدمات سرویس دهندگان وب از مجموعه پتانسیل های ارائه شده (دستورات) توسط پروتکل HTTP استفاده می نمایند :

- GET : سرویس گیرنده وب درخواست يك منبع موجود بر روی سرویس دهنده وب را می نماید .
- POST : سرویس گیرنده وب اطلاعاتی را برای سرویس دهنده وب ارسال می نماید .
- PUT : سرویس گیرنده وب يك مستند جایگزین را برای سرویس دهنده وب ارسال می نماید .
- HEAD : سرویس گیرنده وب اطلاعات خاصی را در ارتباط با يك منبع موجود بر روی سرویس دهنده درخواست می نماید (عدم نیاز به خود منبع)
- DELETE : سرویس گیرنده وب درخواست حذف يك سند موجود بر روی سرویس دهنده را می نماید .
- TRACE : سرویس گیرندگان وب ، پراکسی مربوط به خود را تعریف می نمایند . از متد فوق اغلب در موارد اشکال زدائی استفاده می گردد .

• **OPTIONS** : سایر پتانسیل های موجود به منظور کار بر روی يك سند توسط يك سرویس گیرنده وب درخواست می گردد .

• **CONNECT** : سرویس گیرنده وب به عنوان يك پراکسی به يك سرویس دهنده HTTPS متصل می گردد .

در اغلب موارد صرفاً" از متد GET و در برخی موارد از HEAD استفاده می گردد (در صورت اشکال زدائی يك برنامه وب از تمامی امکانات فوق استفاده می شود) .

مراحل ایجاد يك تراکنش :

يك سرویس گیرنده وب قبل از این که بتواند با يك سرویس دهنده وب داده ئی را مبادله نماید ، می بایست با آن ارتباط برقرار نماید . بدین منظور از پروتکل TCP/IP استفاده می گردد . همانگونه که اشاره گردید سرویس گیرنده و سرویس دهنده وب برای ارسال يك درخواست و پاسخ به آن از پروتکل HTTP استفاده نموده و ارتباط ایجاد شده بین خود را صرفاً" برای يك تراکنش نگهداری می نمایند (HTTP يك پروتکل Stateless است) .

فرآیند ایجاد يك تراکنش بین سرویس گیرنده و سرویس دهنده وب را می توان در چهار مرحله زیر خلاصه نمود:

• مرحله اول ، برقراری ارتباط : در ابتدا می بایست يك ارتباط و یا اتصال مبتنی بر پروتکل TCP/IP بین يك سرویس دهنده و يك سرویس گیرنده وب ایجاد گردد . به منظور تشخیص نوع پروتکل استفاده شده ، برنامه ها از يك عدد منحصر بفرد با نام شماره پورت استفاده می نمایند . (پروتکل FTP از پورت ۲۱ ، پروتکل Telnet از پورت ۳۲ ، پروتکل SMTP از پورت ۲۵ ، پروتکل HTTP از پورت ۸۰) .

• مرحله دوم : ایجاد و یا صدور يك درخواست توسط سرویس گیرنده

• مرحله سوم : پاسخ سرویس دهنده به درخواست سرویس گیرنده

- **مرحله چهارم ، خاتمه و یا توقف ارتباط : سرویس دهنده مسئولیت خاتمه ارتباط TCP با سرویس گیرنده وب را پس از پاسخ به درخواست سرویس گیرنده برعهده دارد . به منظور برخورد با مسائل غیرقابل پیش بینی ، هم سرویس گیرنده و هم سرویس دهنده می بایست قادر به مدیریت يك ارتباط باشند . مثلاً" پس از فعال نمودن دکمه stop در مرورگر ، می بایست به ارتباط ایجاد شده توسط سرویس گیرنده خاتمه داده شود .**

درس ۵

https

پروتکل https مانند پروتکل http پروتکلی است برای استفاده از وب سایت ها اما تفاوت https با http در این است که https میان کلاینت کاربر و سرور وب اطلاعات را رمز نگاری می کند و این رمز نگاری توسط certificate ای که آن سایت به شما می دهد اتفاق می افتد . اما در صورت استفاده از پروتکل http دیتای تبادل شده ی شما به سرور وب به صورت plain text تبادل شده و اگر شخصی میان کلاینت شما و به طور مثال مودم اینترنت شما (می تواند isp و ... باشد) واقع شود و شروع به عملیات arp poisoning نماید (در این روش مهاجم آدرس مک gateway شما رو جای مک آدرس کارت شبکه ی خودش جا میزنه و به اصلاح شروع به sniff کردن میکنه یعنی تمامی ترافیک ای که قرار است به سمت مودم اینترنت برود ابتدا به سمت این شخص مهاجم می رود و سپس پکت ها از سیستم هکر به سمت gateway واقعی ورانه می شوند . به این نوع حمله man in themiddle(mitm) attack می گویند می تواند پکت های ارسالی شما به سرور وب را دیده و اگر این دیتا ها رمز نگاری نباشند خواندن محتوی آنها برای هکر کار بسیار راحتی می شود . برای همین امر است که اکثر وب سایت های مهم (مانند سرویس دهنده گان ایمیل و یا اینترنت بانک ها و یا ...) حداقل هنگامی که به صفحه ی لاگین و ورود نام کاربر و رمز عبور می رسیم از پروتکل https استفاده می کنند .

این نکته را اضافه می کنیم که به صادر کنند های Certificate Authority (CA) می گویند و هر شخصی که بخواهد در وب سایت خودش از certificate استفاده نماید بهتر است از ca های شناخته شده certificate بخرد و در وب سایت خودش قرار دهد . برخی از این ca های معروف عبارتند از godaddy - verisign - ...

حال این سوال مطرح می شود که مگر نمی شود ما خودمان ca باشیم؟! در پاسخ باید گفت که بله این امکان هست اما اگر certificate مورد استفاده ی ما توسط ca های متفرقه صادر شده باشد کلاینت هنگامی که می خواهد صفحه ی https ما را browse کند browser آن به او هشدار می دهد که certificate مورد استفاده در این وب سایت valid نیست! پس این نکته را باید بدانیم که سیستم عامل ها و browser ها از قبل به تعداد مشخص و معینی ca اطمینان دارند و زمانی که صفحه ای که از certificate استفاده می کند (ssl page) را باز نماییم ممکن است که مشاهده

کنیم در محیط url بالای صفحه ی مرورگر به رنگ سبز رنگ در آید و این به معنی اطمینان داشتن سیستم ما به certificate مورد استفاده در آن سایت است و اگر محیط url مرورگر به رنگ قرمز درآمد این بدین معنی ست که سیستم ما به آن certificate مورد استفاده اطمینان ندارد (که دلایل آن را کاملا در ادامه ی مطلب شرح می دهیم) پس می بینیم که اگر برای وب سایت مان که قرار است در محیطی عمومی publish شود از ca معتبری استفاده نکنیم کاربران هنگام ورود به صفحه ی امن سایت ما هشدار valid بودن cerfitiface را می گیرند و احتمالا به آن trust نمیکنند اطلاعات مربوط به Certificate را می تواند در همان url در قسمت certificate information دید که صادر کننده ی این certificate کیست ؟ برای کجا صادر شده و در چه بازه ی زمانی ای valid است . این نکته را نیز اضافه میکنیم که ما میتوانیم certificate هر ca را روی سیستم خود در لیست trust ها قرار دهیم تا سیستم ما به آن certificate و صادر کننده ی اطمینان داشته باشد (اما هنگام add کردن Certificate در trust های سیستم باید دقت داشته باشیم و ca مزبور را بشناسیم) .

در بالا اشاره کردیم که اگر هنگام باز کردن صفحه ی ssl محیط url امان به رنگ قرمز درآمد یعنی که این Certificate مورد اطمینان سیستم ما نیست . حال میخواهیم دلایل این مورد را بررسی نماییم :

۱- ممکن است تاریخ سیستم عامل ما تاریخ روز نباشد برای مثال ممکن است تاریخ سیستم ۳ سال اختلاف داشته باشد و certificate مورد استفاده در بازه ی زمانی ۲ ساله valid باشد .

۲- ممکن است صاحب سایت از certificate متفرقه ای استفاده کرده باشد (که در بالا اشاره کردیم اگر آن سایت و ca آن را می شناختیم می توانیم آن را در لیست trust های خود add نماییم)

۳- ممکن است مورد حمله ی MITM واقع شده باشیم و شخصی دارد پکت های ما را sniff میکند و این بدین معنی ست که ممکن است شخصی یک certificate جعلی را به ما بدهد تا بتواند پسورد و سایر اطلاعات مهم ما را بدست آورد . پس باید دقت کنیم که هر certificate ای رو در trust های سیستم خود قرار ندهیم که چه بسا ممکن است آن Certificate مربوط به یک هکر ای باشد که میان ما و اینترنت واقع شده است .

از موارد بالا موارد ۱ و ۲ به ترتیب می توانند بیشتر برای ما اتفاق رخ دهند پس خیلی خیلی باید به مورد ۳ دقت داشته باشیم ! و توصیه برای کاربران عادی این است که اگر در محیط url خود دیدند که certificate مورد اطمینان نیست (به اصطلاح failed میشود) در صورتی که از تاریخ

سیستم خود اطمینان دارند که به روز است بدون این که پسورد و نام کاربر خود را وارد کنند آن صفحه را ببندند . و اگر به اشتباه لاگین کردند سریعاً از آن محیط sign out کنند و از محیطی که این مشکل را ندارد مجدداً لاگین کرده و تمامی پسوردها و ایمیل های recovery و ... را تعویض کنند . این نکته را اضافه می کنم که اگر هکرایبی شبکه ی ما را sniff کند آن شبکه بسیار کند می شود . و در آخر این نکته را اضافه میکنیم که عملیات sniff کردن و arp poisoning جرم حساب می شود .

درس ۶

IMAP

پروتکل IMAP یکی از پروتکل های نسبتا جدید مورد استفاده در محیط وب (اینترنت) است. از این پروتکل برای انتقال و ارتباطات چند رسانه ای در وب بهره می گیرند. بطور مثال در سرویس های صندوق پست الکترونیکی و یا وب سایت های جدید که امروزه فایل های صوتی و تصویری در آن ها بصورت آنلاین Online مورد استفاده قرار می گیرند از این پروتکل بهره گرفته اند. این پروتکل در لایه کاربردی بر روی port ۱۴۳ قرار دارد و به سرویس گیرنده ها اجازه دسترسی به ایمیل بر روی سرویس دهنده از طریق کنترل از راه دور را میدهد.

نسخه اصلی IMAP

نسخه اصلی imap به نام پروتکل دسترسی به میل به طور موقت بود که به عنوان سرویس گیرنده xerox lips machine و سرویس دهنده ۲۰- tops تکمیل شد. هیچ کپی از نسخه اول پروتکل دسترسی موقت وجود ندارد و تنظیمات پروتکل نسخه اصلی به ۲ imap برگردانده شده است، گر چه بعضی از فرمان ها و جواب ها شبیه به ۲ imap است. اما پروتکل دسترسی موقت فاقد فرمان ها و پاسخ ها است اما با این حال با ترکیب این فرمان ها و علامت ها باعث ایجاد یک نسخه از imap شده است که سازگار با تمام نسخه های imap می باشد.

معایب IMAP

یک سری نقاط ضعف در این پروتکل وجود دارد که باعث افزایش پیچیدگی می شود مثلا دسترسی همزمان چند سرویس گیرنده به یک mail box که این کار توسط سرویس دهنده جانبی مانند (database, maildir) صورت می گیرد و باعث رفع و تصحیح ضعف می شود. اما در این حالت لازم است که الگوریتم جستجو و ذخیره یک میل بر روی سرویس دهنده با دقت کافی صورت گیرد

که سرویس گیرنده نهائی می تواند تعداد زیادی از منابع را در زمان جستجوی mail box معرفی کند . سرویس گیرنده imap برای دسترسی به محتوی پیام جدید می باید در خواستی را اعلام کند که این کار باعث افزایش تاخیر در یک ارتباط کند مانند موبایل می شود، که برای رفع آن از طرحی به نام push imap را پیشنهاد شد که این طرح به طور کلی مورد تأیید قرار نگرفت . بر خلاف بعضی از پروتکل های اختصاصی که عمل ارسال و بازیابی را به صورت ترکیبی انجام می دادند . ارسال یک پیام و ذخیره ای از کپی آن بر روی پوشه ای در سرویس دهنده های جانبی (server – side) باعث می شود که سرویس گیرنده برای انتقال محتوی پیام دو بار درخواست دهد اولی برای smtp و دومی را برای imap جهت ذخیره و ارسال به پوشه میل است . که این مشکل با یک سری تنظیمات مورد تأیید ietf lemonade در مورد قطعات موبایل (rfc-) ۴۴۶۷urlauth ، (catenate) ۴۴۶۹، در (rfc) ۴۴۶۸imap burl در smtp-submission رفع شده است . سرویس دهنده های pop^۳ پوشه های سرویس دهنده های جانبی را حمایت نمی کنند پس بنابراین این سرویس گیرنده هاق انتخاب ندارند اما می توانند موارد ارسال شده را بر روی سرویس گیرنده ذخیره کند. خیلی از سرویس گیرنده های imap می توانند پوشه های سرویس گیرنده جانبی را برای ذخیره میل های ارسال شده قالب بندی کنند . در آخر (lemonade trio) ماهواره مخابراتی سرویس گیرنده میل که کپی فایل های ارسال شده را در یک پوشه تحت نام out box ذخیره می کند .

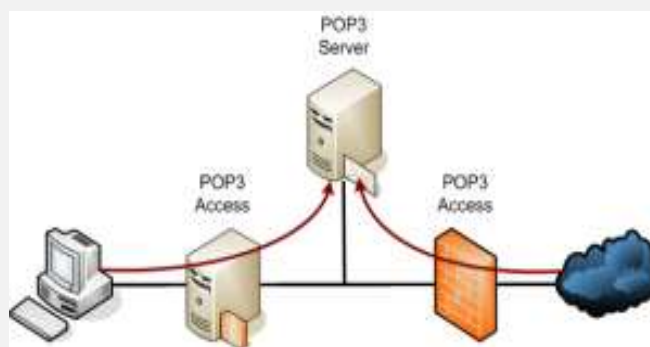
ویژگی های imap

در pop^۳ پس از دریافت ایمیل ها، ایمیل ها از روی سرور حذف میشود در صورتی که در IMAP اینگونه نیست و ایمیل ها پس از دریافت از روی سرور حذف نمی شوند. از طریق IMAP این امکان وجود دارد که کاربر بدون دانلود نمودن پیغام از روی سرور درون پیغامهای خود جستجو انجام دهد، پوشه ایجاد نماید، تغیر نام دهد و Mailbox خود را برای پیغام های جدید کنترل نماید. یکی از پر استفاده ترین موارد استفاده از IMAP حالت اشتراکی آن است بعنوان مثال در شرکتی که باید چند نفر اجازه دسترسی به پست الکترونیک شرکت را داشته باشند IMAP راه حل مناسبی است .

درس ۷

POP۳

POP۳ یکی از مهمترین سرویس های ارسال ایمیل است از این سرویس جهت دریافت و ویرایش پست الکترونیکی استفاده می شود. وقتی این سرویس بر روی سرور شما نصب و پیکربندی شده باشد کاربران می توانند از طریق نرم افزاری که مربوط به دریافت و ارسال Email به سرویس دهنده E-mail وصل شوند و ایمیل های خود را دریافت کنند.



پروتکل دیگری که در کنار POP۳ فعالیت می کند SMTP است که وظیفه ارسال پست الکترونیکی را به سرور بر عهده دارد.

POP۳ در اصل یک پروتکل دریافت ایمیل بر روی شبکه اینترنت است و اصولاً در لایه Application در پروتکل TCP/IP قرار می گیرد. با استفاده از این امکان شما می توانید در کامپیوتر خود، بدون نیاز به مراجعه به سایت سرویس دهنده ایمیل هایتان را دریافت و ذخیره کنید. برای دریافت ایمیل به صورت POP۳ باید شما به صورت Local دارای یک client دریافت ایمیل باشید. مثل Microsoft Outlook یا برنامه ی MozillaThunderbird.

^۳ Post Office Protocol

POP3 این قابلیت را به کاربرانش می دهد که به اینترنت وصل شوند و ایمیل هایشان را گرفته و در حالت آفلاین آنها را ویرایش کنند. در حالت عادی وقتی شما ایمیلی رو از طریق POP3 دریافت می کنید، ایمیل از روی سرور پاک می شود. البته اکنون اکثر سرویس دهنده های POP3 قابلیتی به نام Leave onServer دارند که اصطلاحاً به آن 'UIDL' POP3 می گویند.

معایب POP3:

با وجود مزایای چشمگیر و بالای پروتکل POP3، برخی معایب نیز در مورد این پروتکل موجود می باشد:

باز شدن الحاقیه ها، مشکلات javascript، فلدرهای ایمیل آسیب دیده، عدم وجود Privacy، داشتن پتانسیل برای آلوده شدن ایمیل ها، مصرف بالای منابع، دانلود کردن فایل های حجیم.

زمانیکه فایلی حاوی ویروس آپلود می شود، کارآیی به شدت کاهش می یابد. از دیگر معایب مشکلات مربوط به javascript می باشد، در صورتی در نرم افزار ایمیل این گزینه فعال باشد، در کامپیوتر شما یک حفره امنیتی ایجاد شده است. به علاوه فلدرهای ایمیل گاهی اوقات آسیب می بینند و محتوای آنها حذف می شود. از آنجایی که POP3 پیام ها را در سیستم لوکال ذخیره می کند، حریم شخصی شما به خطر می افتد چرا که شخص دیگری در صورتی که از کامپیوتر شما استفاده کند، آنها را خواهد دید. حتی اگر کلاینت ایمیل دارای پسورد باشد، فردی دیگری از راه های دیگر می تواند لاگین شده و ایمیل ها را بخواند.

حتی اگر تمام ایمیل های شما بر روی لوکال قرار گرفته باشند، می توانند توسط روش هایی آلوده به ویروس شوند. استفاده از یک آنتی ویروس قطعاً مفید خواهد بود اما فقط در ۶۰ درصد موارد مفید می باشد.

دانلود فایل های حجیم با سایر ایمیل ها انجام می شود که زمان زیادی را رزرو می کنند. دستگاه های موبایل و اتصالات dial up هنگام کار کردن با این پروتکل مشکلاتی را خواهند داشت. بنابراین POP3 نیاز به روزآوری و جلو رفتن با تکنولوژی های مدرن را دارد.

نکاتی که هنگام انتخاب تنظیمات ارسال و دریافت باید به آن توجه نمود.

اگر رایانه شما که دارای برنامه ایمیل POP3 یا IMAP4 است همیشه به اینترنت وصل باشد، ممکن است بخواهید برنامه ایمیل جهت ارسال و دریافت پیام ها را در بازه های زمانی مختلف دریافت کنید. اتصال مداوم به سرور به شما کمک می کند برنامه ایمیل خود را با اکثر اطلاعات فعلی روی سرور به روز نگه دارید. اما اگر دستگاه شما که دارای برنامه ایمیل POP3 یا IMAP4 است همیشه به اینترنت وصل نباشد (برای مثال، در صورت اتصال به اینترنت از طریق شماره گیری تلفنی)، ممکن است بخواهید برنامه ایمیل را روی ارسال و دریافت بصورت دستی پیکربندی نمایید. ارسال و دریافت پیام ها بصورت دستی هنگام اتصال از طریق شماره گیری تلفنی بطور بالقوه زمان اتصال به اینترنت را کاهش می دهد.

تفاوت POP3 و IMAP :

به طور مثال در POP3 پس از دریافت ایمیل ها، آنها از روی سرور پاک شده در صورتی که در IMAP اینگونه نیست و ایمیل ها پس از دریافت از روی سرور پاک نمی شوند. شما از طریق IMAP این امکان را خواهید داشت که بدون دانلود کردن ایمیل های خود از روی سرور درون ایمیل های خود جستجو کنید پوشه بسازید تغییر نام دهید و حتی ایمیل ها را پاک کنید ، mailbox خود را برای ایمیل های جدید چک کنید و کلی امکانات دیگر. این امکانات به تدریج باعث جایگزینی IMAP به جای POP3 می شود. یکی از پر استفاده ترین موارد استفاده از IMAP حالت اشتراکی است مثلاً در شرکتی که باید چند نفر اجازه دسترسی به پست الکترونیک شرکت را داشته

باشند IMAP راه حل مناسبی است چرا که همه می توانند ایمیل های موجود در سرور را دانلود نمایند.

کار با POP3 در کلاینت ها:

اگر حساب ایمیل شما از POP3 و IMAP4 پشتیبانی می کند، می توانید از برنامه های ایمیل POP3 و IMAP4 برای اتصال به حساب خود استفاده کنید. این برنامه ها شامل Outlook، Windows Mail، برنامه های Outlook Express، Entourage و Mozilla Thunderbird و Eudora می باشند. این قابلیت ها توسط هر برنامه ی ایمیل متفاوتی پشتیبانی می شوند.

جدول زیر برخی برنامه های ایمیل سازگار با POP3 و IMAP4 را نشان می دهد.

Windows	Outlook 2010 Microsoft
Windows	Microsoft Outlook 2007
Windows	Microsoft Outlook Express
Windows	Microsoft Windows Live Mail 2011
Windows	Microsoft Windows Mail
Macintosh	Microsoft Entourage 2008
Macintosh	Mail (نیز به عنوان Apple Mail 3.0 شناخته شده است)
Windows/Macintosh	Thunderbird
Windows/Macintosh	Pine
Windows/Macintosh	Alpine
Windows/Macintosh	Eudora
Macintosh	<u>iPhone Mail</u>
Windows Mobile 5 با نسخه های بالاتر	Windows Mobile Mail

مقایسه ی پروتکل IMAP و POP3

۱- پروتکل POP3 نامه های الکترونیکی موجود در پوشه ی Inbox روی سرویس دهنده را مرور کرده و تمام پیام های جدید را يك مرتبه و خیل سریع بر روی کامپیوتر شما دانلود می کند. پروتکل IMAP سربرگ (Headers) تمام پیام های جدید را دانلود کرده و زمانی که شما قصد خواندن آن پیام را دارید و بر روی آن کلیک می کنید آنگاه پیام را بر روی سیستم شما دانلود می کند. به همین دلیل سرعت بازیابی پیام ها در IMAP کم تر می باشد.

۲- پروتکل POP3 پیام ها به صورت OffLine (زمانی که با سرویس دهنده ی پست الکترونیکی ارتباط ندارید) نیز قابل دسترس خواهد بود ولی در پروتکل IMAP حتماً باید با سرویس دهنده ی پست الکترونیکی در ارتباط باشید.

۳- پروتکل POP3 در مواردی مفید است که شما نامه های پستی خود را تنها از روی يك کامپیوتر بررسی می کنید ولی مواقعی که می خواهید از روی چند کامپیوتر (منزل، اداره و ...) نامه های پستی خود را بررسی کنید استفاده از پروتکل imap مفیدتر خواهد بود.

۴- در پروتکل IMAP پیام های شما از جمله پیام هایی که در پوشه ی Sent-mail ذخیره شده است از روی کامپیوتر دیگر قابل مشاهده نیست.

۵- در پروتکل POP3 پیام های پوشه ی Inbox از روی سرویس دهنده پاک می شود و شما تنها به همان پیام ها دسترسی دارید ولی در پروتکل IMAP تمام پوشه های ایجاد شده بر روی سرویس دهنده قابل مشاهده و قابل پیمایش خواهد بود و تغییرات انجام شده بر روی سرویس دهنده نیز اعمال می گردد.

۶- در پروتکل POP3 برای دستیابی به آخرین بروزرسانی باید بر روی دکمه ی Send/Receive کلیک کنید ولی در پروتکل IMAP همواره با رسیدن پیام جدید خود به صورت خودکار بروزرسانی می گردد.

۷- در پروتکل pop^۳ به دلیل اینکه پیامها بر روی فضای هارد دیسک ذخیره می‌شوند مشکل محدودیت فضای جعبه پستی را نخواهید داشت، اما در پروتکل IMAP به دلیل اینکه پیامها فضای MailBox را اشغال می‌کند ممکن با مشکل محدودیت فضا روبرو می‌شوید.

۸- تمام ISPها و برنامه‌های پست الکترونیکی پروتکل POP^۳ را پشتیبانی می‌کنند ولی به دلیل پیچیدگی پروتکل IMAP تعداد کمی از ISPها و برنامه‌های پست الکترونیکی پروتکل IMAP را پشتیبانی می‌کنند.

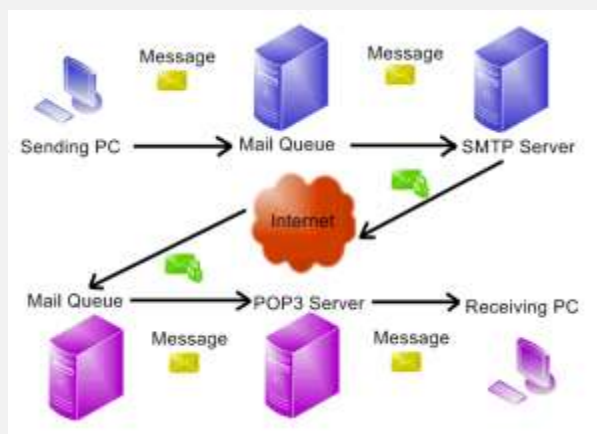
۹- در پروتکل IMAP انتقال حساب کاربری میل از یک سیستم به سیستم دیگر آسان است، ولی در پروتکل POP^۳ به دلیل اینکه میلها به صورت فایل بر روی سیستم ذخیره می‌شود مشکل است و ممکن است انتقال میلها از یک برنامه به برنامه‌ی دیگر به دلیل پشتیبانی نکردن از آن نوع سیستم فایل امکان پذیر نباشد.

درس ۸

SmtP

SMTP^۱ یا یکی از پروتکل های TCP/IP برای ارسال و دریافت نامه های الکترونیکی است. این پروتکل به دلیل محدودیت هایی در نگهداری نامه ها، معمولا با پروتکل های POP^۳ یا IMAP^۲ استفاده می شود.

SMTP برای کاربران امکان ذخیره نامه ها را روی یک سرور یا دانلود آنها را از سرور فراهم می کند. در حقیقت می توان گفت، SMTP برای ارسال نامه ها و POP^۳ یا IMAP برای دریافت نامه ها به کار می روند.



SMTP معمولا از پورت ۲۵ برای ارسال نامه ها استفاده می کند. POP^۳ رایج ترین پروتکل استاندارد برای دریافت نامه ها به شمار می آید که از پورت ۱۱۰ برای دریافت نامه استفاده می کند. در کنار این پروتکل IMAP هم وجود دارد. SMTP در واقع پروتکلی است که جهت انتقال پست الکترونیکی استفاده می شود. این پروتکل استاندارد اینترنتی برای ارسال پست الکترونیکی در میان

^۱ simple mail transfer protocol

^۲ Internet message access protocol

پروتکل های شبکه است. این تعریف جز تعاریف اولیه SMTP در علم شبکه بود و آخرین تعریف و نسخه به روزرسانی شده آن SMTP گسترش یافته (ESMTP) را شامل می شود. امروزه این پروتکل به طور گسترده استفاده می شود. تعداد زیادی سرور SMTP به صورت رایگان وجود دارد که می توان به خوبی از آنها استفاده کرد.

SMTP توسط RFC ۸۲۱ تعریف گردید و در RFC ۵۳۲۱ به روز آوری شده است که همان SMTP پیشرفته می باشد که امروزه بسیار مورد استفاده قرار می گیرد این نوع از پورت شماره ۵۸۷ برای ارسال ایمیل استفاده می کند. اتصالات SMTP توسط SSL امن می شوند که این پروتکل به شکل SMTPs تغییر می یابد. SMTP یک پروتکل ویژه انتقال پست الکترونیکی است. به عبارت ساده تر، سرور SMTP، مانند وب سرور، یک رایانه است که مانند مسیریاب عمل می کند. هنگامی که پیام های پست الکترونیکی را از کاربران دریافت می کند آنها را به گیرندگان مورد نظر می فرستد. سرورهای SMTP از پروتکل های ساده انتقال پست الکترونیکی یا برنامه ارسال پست الکترونیکی یونیکس استفاده می کنند. اغلب پیام ها باید از میان سرورهای مختلفی عبور کنند تا به مقصدشان برسند. قبل از برقراری ارتباط با افراد از طریق پست الکترونیکی لازم است دستوراتی برای تنظیم و آزمایش سرور SMTP و همچنین تغییراتی را در ISS اعمال کنید.

تنظیمات سرور SMTP

شما با استفاده از مراحل زیر می توانید خدمات سرویس SMTP نصب شده روی ویندوز را فعال کنید. برای نصب خدمات SMTP به منوی start بروید و روی کنترل پنل کلیک کنید. سپس روی «Add or Remove Programs» کلیک کنید. در قسمت سمت چپ روی گزینه «Add/Remove Windows Components» کلیک کنید. در محتوای فهرست گزینه «Application Server» را خواهید دید روی Application Server سپس روی Details کلیک کنید. در این فهرست شما (IIS) را می بینید پس از کلیک روی آن، Details را کلیک کنید. در زیر منوهای (IIS) گزینه SMTP را انتخاب و سپس ok را کلیک کنید. حال با انتخاب گزینه Next به مرحله بعد بروید.

البته ممکن است لازم باشد که ویندوز سرور ۲۰۰۳ یا مسیر نصب شبکه را دنبال کنید. در آخر روی Finish کلیک کنید.

دستورات ابتدایی SMTP :

پس از نصب سرویس SMTP ، این سرور به طور پیش فرض فعال می شود. ذخیره پیام در LocalDrive:\Inetpub\Mailroot واقع شده است. اگر برای اولین بار می خواهید تنظیمات مربوط به سرور مجازی SMTP یا تنظیمات کامپوننت های آن را پیکربندی کنید آشنایی با دستورات سرور SMTP لازم است. برخی از این دستورات عبارتند از:

EHLO / HELO: این دستوری جهت شناساندن فرستنده (client) به سرور SMTP است.

MAIL FROM: محل آدرس پست الکترونیکی فرستنده را مشخص می کند.

RCPT TO: با استفاده از این دستور آدرس گیرندگان پست الکترونیکی مشخص می شود.

DATA: شامل داده های واقعی (بدنه متن، ضمیمه و...) است.

RSET (RESET): این دستور مشخص کننده تراکنش پست الکترونیکی جاری، ارسال شده یا به طور غیرعادی خاتمه یافته است.

VRFY (VERIFY): این دستور جهت تایید کاربر استفاده می شود.

HELP: با این دستور سرور اطلاعات کمکی را به فرستنده ارسال می کند.

QUIT: این دستور به این معنی است که سرور فضای تخصیص داده شده به آن را آزاد می کند.

تعدادی سرور SMTP رایگان برای ارسال پست الکترونیکی به طور مستقیم وجود دارد. بیشتر این برنامه ها کار پشتیبانی را انجام می دهند، برنامه های پست الکترونیکی مانند Outlook Express و

Eudora از جمله این برنامه هاست که در مقایسه با Outlook Express ساده تر می باشد. امروزه یکی از سرورهای SMTP رایج، سرور SMTP جی میل است. سرور SMTP حتی برای مواقعی که در مکان های عمومی به اینترنت دسترسی دارید، یا مجبور به ارسال پست الکترونیکی حجیمی هستید بهترین گزینه است زیرا این سرور، امنیت و پوشیدگی اطلاعات را تضمین می کند. GSM سرور نیز یکی دیگر از این سرویس های رایگان است .

برخی ویژگی های SMTP :

برخی توابع ارسال ایمیل را پشتیبانی نمی کند .

مسائل امنیتی مشخص شده در X.400 در smtp رعایت نمی شود.

این پروتکل بسیار ساده می باشد.

از دیگر محدودیت های این پروتکل این است که تنها برای ارسال ایمیل استفاده می شود و توانایی دریافت آنها را ندارد. به علاوه استفاده از آن بستگی به تنظیمات ISP و یا شبکه دارد. در مقابل آن مهمترین مزیت IMAP سرعت آن است و تنها با یک درخواست کوچک ایمیل ها دانلود می شوند. SMTP جهت رساندن ایمیل به سرور گیرنده از MTA¹ استفاده می کند.

¹mail transfer agent

درس ۹

Soap

SOAP^۱ یک پادمان مبتنی بر XML است، برای رد و بدل کردن اطلاعات بین برنامه ها. اطلاعات در SOAP به صورت پیام (Message) و از طریق پادمان های موجود در اینترنت مانند HTTP منتقل می شود (SOAP در سایر پادمان ها، مانند SMTP یا MIME نیز قابل استفاده است). به زبان ساده تر، SOAP یک پادمان است برای دستیابی به یک سرویس ارایه شده در وب (Web Service). آخرین نسخه SOAP، نسخه ۱/۲ می باشد.

ویژگی های SOAP

۱. یک پادمان ارتباطی است.
۲. برای ارسال پیام استفاده می شود.
۳. برای محیط اینترنت و شبکه طراحی شده است.
۴. وابسته به محیط پیاده سازی و اجرا نیست. (Platform Independent)
۵. مبتنی بر XML است.
۶. از دیوارهای آتش (Firewall) گذر می کند و دیوارهای آتش مانع آنها نمی شوند (Block نمی شوند).

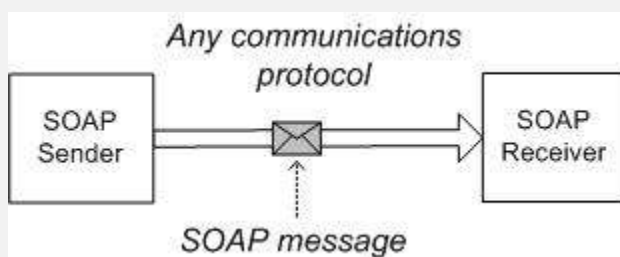
یکی از مسایلی که در دهه اخیر از اهمیت خاصی برخوردار بوده، چگونگی ارتباط برنامه های تحت اینترنت با یکدیگر بوده است. همانطور که می دانید برنامه های عادی از ^۲ RPC برای فراخوانی

^۱Simple Object Access Protocol

^۲Remote Procedure Call

اشیاء DCOM یا CORBA، استفاده می کنند. اما مشکلی که در این نوع فراخوانی ها در بستر اینترنت وجود دارد، مسدود شدن این نوع ترافیک ها در Server ها و دیوارهای آتش (Firewall) است. (ها)

در صورت استفاده از SOAP با این مشکل روبرو نخواهید بود. SOAP به راحتی شما را قادر خواهد کرد تا بین برنامه هایی که در بسترهای متفاوت طراحی شده اند و در بسترهای متفاوتی در حال سرویس دهی هستند، ارتباط برقرار کنید.



ساختار SOAP

پیام ها (Message ها) در SOAP یک فایل XML هستند که از ساختار زیر پیروی می کنند:

. یک بخش ضروری که به آن Envelope (پاکت نامه) گفته می شود که مشخص می کند که این XML یک پیام SOAP است.

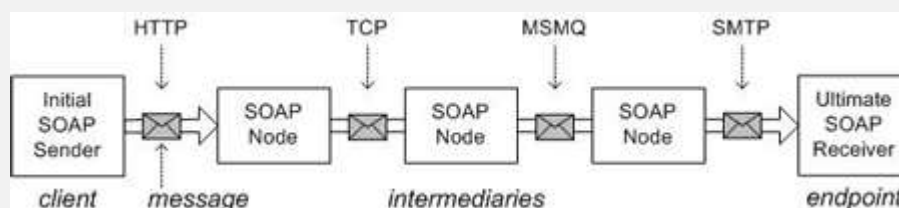
. قسمت سرآیند (Header) که اختیاری است. این بخش شامل اطلاعاتی در مورد خود برنامه است. در صورتی که از سرآیند استفاده شود، باید اولین عنصر در ساختار Envelope باشد.

قسمت بدنه که ضروری است و شامل Call یا Response است. در واقع مشخص

کننده درخواست برنامه‌ی سرویس گیرنده یا پاسخ برنامه سرویس دهنده است.

قسمت Fault که قسمت خطا است و اختیاری است و اطلاعاتی درباره خطاهای

وجود آمده در هنگام پردازش پیام در خود دارد.



قوانین مهم در ساختار پیام

پیام حتماً باید در قالب XML باشد.

باید از Namespace تعریف شده در Envelope پیروی کند.

فقط باید از نوع داده های تعریف شده و مجاز استفاده کند.

در قالب پیام، نباید از DTD استفاده شود. DTD برای یک XML ، مانند

Design View یک جدول در Database است و مشخص می کند که فیلدهای

آمده در XML از چه نوع هستند و با چه ترتیبی می آیند. برای مثال:

<ELEMENT note (to,from,heading,body!)>

<ELEMENT to (#PCDATA!)>

<ELEMENT from (#PCDATA!)>

<ELEMENT heading (#PCDATA!)>

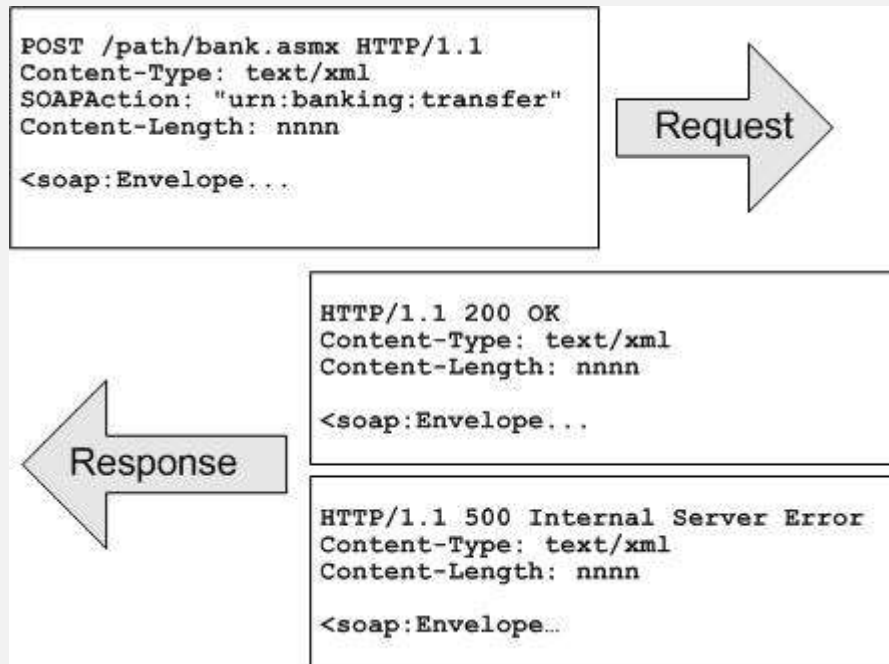
<ELEMENT body (#PCDATA!) >

نباید شامل دستورات پردازشی باشد.

هنگام استفاده از پادمان HTTP، در هر درخواست باید Content-Type و Content-Length مشخص شود. که برای SOAP، موارد ارسالی در مثال زیر، به طور معمول مورد استفاده قرار می گیرند.

در این مثال ، درخواست قیمت سیب و پاسخ آن آورده شده است. مشتری (Client) یک XML را به کارگزار می فرستد که در آن قالب مشخص شده توسط برنامه کارگزار (Server) رعایت شده است و در خواست مشتری در آن قرار دارد. در این مثال، قیمت سیب، موردنظر است که در برچسب m:GetPrice ، آمده است. در صورتی که قالب تعیین شده توسط سرور این اجازه را به شما بدهد که چند مورد را در یک درخواست بفرستید، می توانید این کار را انجام دهید.

برنامه کارگزار نیز، با استفاده از یک فایل XML پاسخ مشتری را می دهد و قیمت را در یک برچسب با عنوان m:GetPriceResponse به مشتری تحویل می دهد.



معایب SOAP

همانطور که می‌دانید اولین حرف از حروف تشکیل دهنده ی SOAP، S است که حرف اول Simple است. همین مورد، باعث شده است تا سادگی بر هرچیز در این سیستم، مقدم باشد. برای همین در SOAP بسیاری از کاستی ها دیده می‌شود، که یکی از مهمترین آنها امنیت و قابلیت اعتماد پایین در SOAP است.

همین کاستی باعث شده است که تولیدکنندگان نرم‌افزار به این فکر بیفتند تا SOAP را توسعه دهند و استانداردهای جدیدتری با امکانات بیشتری تولید کنند. استاندارد تولید شده توسط میکروسافت با نام ¹GXA¹ارایه شد. که یک پیاده‌سازی از آن ²WSE² است. WSE یک ابزار قدرتمند است که شما با استفاده از DotNet Framework و WSE می‌توانید وب سرویس های

¹Global XML Web Services Architecture

²Web Services Enhancements

امن و قدرتمند بنویسید. به بیان ساده تر WSE ابزار شما برای طراحی و ساخت وب سرویس ها با NET. می باشد. WSE را می توانید از سایت Microsoft بارگیری کرده و نصب کنید.

درس ۱۰

اس اس اچ چیست و چه تفاوتی با اف تی پی دارد؟

هر دو پروتکل هایی تحت شبکه هستند که درست مانند HTTP بالای لایه TCP/IP اجرا می گردند. به زبان ساده این یک راه شناخته شده برای ابزارها است، تا درون شبکه با یکدیگر تماس برقرار کنند.

شیوه های مختلف برقراری تماس، ویژگی ها و شرایط استفاده متفاوت و ویژه ای دارند. کاربردهای مختلف و توانایی های گوناگونی در هر کدام گنجانده شده است. اما اینکه SSH و FTP دقیقاً چه تفاوت ها و کارکردهایی دارند، برای بسیاری هنوز مبهم و گنگ است.

برنامه واسط (Shell) و اکانت های برنامه واسط:

بگذارید ابتدا به اصطلاحات فنی پایه و زیرساخت ها بپردازیم. برای فهمیدن هدف SSH، نیاز دارید با برخی عناصر اصولی و زیرساخت آن آشنا شوید.

Shell کامپیوتر، یک قطعه نرم افزاری است که به کاربر اجازه می دهد مستقیماً با کرنل یا هسته اصلی سیستم عامل ارتباط برقرار کند. Shell می تواند دارای رابط گرافیکی یا محیط خط فرمان باشد و یا اینکه هر دو را با هم داشته باشد.

```

tim@hoopoe ~$ find /tmp/dir -
[tm@hoopoe ~]$ find /tmp/dir -
  -amin      -empty      -fstype      -iregex      -mtime      -print      -uid
  -anewer    -exec       -gid         -links       -name       -print0     -used
  -atime     -false      -group       -lname       -newer      -printf     -user
  -cmin      -fls        -help        -ls          -nogroup    -prune      -version
  -cnewer    -follow     -ilname      -maxdepth    -noleaf     -regex      -xdev
  -ctime     -fprint     -iname       -mindepth    -nouser     -size       -xtype
  -daystart  -fprint0    -inum        -min         -ok         -true
  -depth     -fprintf    -ipath       -mcount      -perm       -type
[tm@hoopoe ~]$ find /tmp/dir -user r
root      rpc      rpcuser   rpm
[tm@hoopoe ~]$ find /tmp/dir -user root -type
b c d f l p s
[tm@hoopoe ~]$ find /tmp/dir -user root -type f
[tm@hoopoe ~]$ grep --fi
--file=          --files-without-match
--files-with-matches  --fixed-strings
[tm@hoopoe ~]$ grep --fi

```

اکانت Shell یک اکانت شخصی است که به کاربر اجازه دسترسی به Shell را از طریق کامپیوترهای مختلف و راه دور می دهد. از این اکانت ها معمولا می توان برای کار با فایل های ذخیره شده، اکانت های ایمیل، گروه های خبری و مانند آن استفاده کرد. نقطه مشترک همه کاربردهای Shell هم در این است که معمولا برای استفاده از اکانت Shell دستورات را از راه دور و توسط خط فرمان ارسال می کنیم.

پروتکل برنامه واسط امن (Secure Shell Protocol - SSH)

همانطور که مرورگرهای وب از پروتکل HTTP برای صحبت و ارتباط با سایت ها استفاده می کنند، اکانت شل هم نیاز دارد تا از یک پروتکل مشخص برای ممکن ساختن انتقال اطلاعات (یا همان ارتباطات میان دو ابزار درون شبکه استفاده کند. افتخار دارم SSH¹ یا پروتکل برنامه واسط امن را خدمت تان معرفی کنم.

SSH از یک کلید رمزنگاری عمومی استفاده می کند و هدف اولیه توسعه آن، خلق جایگزینی به جای ارتباطات ناامن و حفاظت نشده ای همچون Telnet بود. این پروتکل دارای دو نسخه اصلی SSH-1 و SSH-2 است که هم اکنون پروتکل های عمده و حاکم بر دنیای دسترسی اکانت های شل هستند.

امروزه از SSH برای لاگین و اجرای کدها از طریق کامپیوترهای راه دور، جستجوی وب با استفاده از کلاینت های پروکسی رمزنگاری شده و انتقال فایل استفاده می شود. همچنین برای تنظیم و آماده سازی شبکه خصوصی مجازی یا همان VPN هم می توان از SSH بهره برد.

کلاینت های SSH یا برنامه های دسکتاپ اس اس اچ برای همه سیستم عامل های اصلی در دسترس هستند. سیستم های بر پایه یونیکس، مانند لینوکس و مک او اس ایکس، می توانند از OpenSSH استفاده کنند. همچنین در سایت OpenSSH می توانید برنامه های SSH مناسبی برای مک و ویندوز پیدا کنید. PuTTY هم یکی از برجسته ترین کلاینت های ویژه تحت ویندوز است.

¹Secure Shell Protocol

پروتکل انتقال فایل امن یا SFTP در برابر FTP

انتقال فایل و اجرای VPN به صورت پیش فرض بر روی SSH فعال نیستند. به یاد داشته باشید که SFTP پروتکل اف تی پی قابل اجرا بر روی SSH نیست. بلکه یک پروتکل متفاوت انتقال فایل (file transfer protocol) است که به عنوان یک اکستنشن یا افزونه برای SSH-2 توسعه یافته است. SFTP همیشه برای انتقال فایل روی اس اس اچ استفاده می شود، اما در حقیقت به گونه ای طراحی شده که می تواند توسط دیگر پروتکل ها هم مورد استفاده قرار گیرد.

البته جدای از صحبت های فنی، SFTP برای کاربر نهایی می تواند یک جایگزین امن و مطمئن برای FTP باشد. اف تی پی تمامی اطلاعات را به صورت متن ساده و بدون رمزنگاری انتقال می دهد. بنابراین سرقت بسته های اطلاعاتی می تواند باعث بروز مشکلات وخیمی برای اطلاعات شخصی شما از قبیل نام کاربری و رمزهای عبورتان گردد. SFTP که تبدیل به یک افزونه برای SSH-2 شده، از شیوه امنیتی کلید رمز عمومی برای انتقال اطلاعات استفاده می کند. این بدان معنی است که اطلاعات به صورت رمزنگاری شده ارسال می گردند و خطر بالقوه نفوذ بین مسیر به اطلاعات تقریباً منتفی می گردد.

SFTP معمولاً در بسیاری از برنامه های مشهور FTP قابل استفاده است. البته در این حالت، دیگر قابلیت های SSH در این حالت غیر فعال خواهند بود.

درس ۱۱

SSL

SSL^۱ راه حلی جهت برقراری ارتباطات ایمن میان یک سرویس دهنده و یک سرویس گیرنده است که توسط شرکت Netscape ارائه شده است. در واقع SSL پروتکلی است که پایین تر از لایه کاربرد (لایه ۴ از مدل TCP/IP) و بالاتر از لایه انتقال (لایه سوم از مدل TCP/IP) قرار می گیرد. مزیت استفاده از این پروتکل، بهره گیری از موارد امنیتی تعبیه شده آن برای امن کردن پروتکل های غیرامن لایه کاربردی نظیر HTTP، LDAP، IMAP و... می باشد که براساس آن الگوریتم های رمزنگاری بر روی داده های خام (plain text) که قرار است از یک کانال ارتباطی غیرامن مثل اینترنت عبور کنند، اعمال می شود و

محرمانه ماندن داده ها را در طول کانال انتقال تضمین می کند.

به بیان دیگر شرکتی که صلاحیت صدور و اعطای گواهی های دیجیتال SSL را دارد برای هر کدام از دو طرفی که قرار است ارتباطات میان شبکه ای امن داشته باشند، گواهی های مخصوص سرویس دهنده و سرویس گیرنده را صادر می کند و با مکانیزم های احراز هویت خاص خود هویت هر کدام از طرفین را برای طرف مقابل تایید می کند، البته غیر از این کار می بایست تضمین کند که اگر اطلاعات حین انتقال مورد سرقت قرار گرفت، برای رباینده قابل درک و استفاده نباشد که این کار را با کمک الگوریتم های رمزنگاری و کلیدهای رمزنگاری نامتقارن و متقارن انجام می دهد.

ملزومات یک ارتباط مبتنی بر پروتکل امنیتی SSL عبارتند از :

برای داشتن ارتباطات امن مبتنی بر SSL عموماً به دو نوع گواهی دیجیتال SSL یکی برای سرویس دهنده و دیگری برای سرویس گیرنده و یک مرکز صدور و اعطای گواهینامه دیجیتال یا CA نیاز

^۱Secure Socket Layer

می باشد. وظیفه CA این است که هویت طرفین ارتباط، نشانی ها، حساب های بانکی و تاریخ انقضای گواهینامه را بداند و براساس آن ها هویت ها را تعیین نماید .

مکانیزم های تشکیل دهنده SSL

۱- تایید هویت سرویس دهنده

با استفاده از این ویژگی در SSL ، یک کاربر از صحت هویت یک سرویس دهنده مطمئن می شود. نرم افزارهای مبتنی بر SSL سمت سرویس گیرنده، مثلا یک مرورگر وب نظیر Internet Explorer از تکنیک های استاندارد رمزنگاری مبتنی بر کلید عمومی و مقایسه با کلیدهای عمومی یک سرویس دهنده، (مثلا یک برنامه سرویس دهنده وب نظیر IIS می تواند از هویت او مطلع شود و پس از اطمینان کامل، کاربر می تواند نسبت به وارد نمودن اطلاعات خود مانند شماره کارت های اعتباری و یا گذرواژه ها اقدام نماید) .

۲- تایید هویت سرویس گیرنده

برعکس حالت قبلی در اینجا سرویس دهنده است که می بایست از صحت هویت سرویس گیرنده اطمینان یابد. طی این مکانیزم، نرم افزار مبتنی بر SSL سمت سرویس دهنده پس از مقایسه نام سرویس گیرنده با نام های مجاز موجود در لیست سرویس گیرنده های مجاز که در داخل سرویس دهنده تعریف می شود و در صورت وجود، اجازه استفاده از سرویس های مجاز را به او می دهد .

۳- ارتباطات رمز شده

کلیه اطلاعات مبادله شده میان سرویس دهنده و گیرنده می بایست توسط نرم افزارهای موجود در سمت سرویس دهنده و سرویس گیرنده رمزنگاری (Encrypt) شده و در طرف مقابل رمزگشایی (Decrypt) شوند تا حداکثر محرمانگی (Confidentiality) در این گونه سیستم ها لحاظ شود .

اجزای پروتکل SSL

پروتکل SSL دارای دو زیرپروتکل تحت عناوین زیر می باشد :

۱ SSL Record Protocol - که نوع قالب بندی داده های ارسالی را تعیین می کند .

۲ SSL Handshake Protocol - که براساس قالب تعیین شده در پروتکل قبلی، مقدمات ارسال داده ها میان سرویس دهنده ها و سرویس گیرنده های مبتنی بر SSL را تهیه می کند . بخش بندی پروتکل SSL به دو زیرپروتکل دارای مزایای چندی است از جمله :
اول: در ابتدای کار و طی مراحل اولیه ارتباط (Handshake) هویت سرویس دهنده برای سرویس گیرنده مشخص می گردد .

دوم: در همان ابتدای شروع مبادلات، سرویس دهنده و گیرنده بر سر نوع الگوریتم رمزنگاری تبدلی توافق می کنند .

سوم: در صورت لزوم، هویت سرویس گیرنده نیز برای سرویس دهنده احراز می گردد .
چهارم: در صورت استفاده از تکنیک های رمزنگاری مبتنی بر کلید عمومی، می توانند کلیدهای اشتراکی مخفی را ایجاد نمایند .

پنجم: ارتباطات بر مبنای SSL رمزنگاری می شود .

الگوریتم های رمزنگاری پشتیبانی شده در SSL

در استاندارد SSL ، از اغلب الگوریتم های عمومی رمزنگاری و مبادلات کلید (Key Exchange Algorithm) نظیر RSA Key Exchange, KEA, DSA, DES ۵, MD۲, RC۴RSA, RC۴, Skipjack و DES ۳ پشتیبانی می شود و بسته به این که نرم افزارهای سمت سرویس دهنده و سرویس دهنده نیز از موارد مذکور پشتیبانی نمایند، ارتباطات SSL می تواند براساس هر کدام از این الگوریتم ها صورت پذیرد. البته بسته به طول کلید مورد استفاده در الگوریتم و قدرت ذاتی الگوریتم می توان آن ها را در رده های مختلفی قرار داد که توصیه می شود با توجه به

سناریوهای موردنظر، از الگوریتم های قوی تر نظیر DES ۳ با طول کلید ۱۶۸ بیت برای رمزنگاری داده ها و همچنین الگوریتم SHA-1 برای مکانیزم های تایید پیغام MD۵ استفاده شود و یا این که اگر امنیت در این حد مورد نیاز نبود، می توان در مواردی خاص از الگوریتم رمزنگاری RC۴ با طول کلید ۴۰ بیت و الگوریتم تایید پیغام MD۵ استفاده نمود .

نحوه عملکرد داخلی پروتکل SSL :

همان طور که می دانید SSL می تواند از ترکیب رمزنگاری متقارن و نامتقارن استفاده کند. رمزنگاری کلید متقارن سریع تر از رمزنگاری کلید عمومی است و از طرف دیگر رمزنگاری کلید عمومی تکنیک های احراز هویت قوی تری را ارائه می کند. یک جلسه (SSL Session) با یک تبادل پیغام ساده تحت عنوان SSL Handshake شروع می شود. این پیغام اولیه به سرویس دهنده این امکان را می دهد تا خودش را به سرویس دهنده دارای کلید عمومی معرفی نماید و سپس به سرویس گیرنده و سرویس دهنده این اجازه را می دهد که یک کلید متقارن را ایجاد نمایند که برای رمزنگاری ها و رمزگشایی سریع تر در جریان ادامه مبادلات مورد استفاده قرار می گیرد. گام هایی که قبل از برگزاری این جلسه انجام می شوند براساس الگوریتم RSA Key Exchange عبارتند از :

۱- سرویس گیرنده، نسخه SSL مورد استفاده خود، تنظیمات اولیه درباره نحوه رمزگذاری و یک داده تصادفی را برای شروع درخواست یک ارتباط امن مبتنی بر SSL به سمت سرویس دهنده ارسال می کند .

۲- سرویس دهنده نیز در پاسخ نسخه SSL مورد استفاده خود، تنظیمات رمزگذاری و داده تصادفی تولید شده توسط خود را به سرویس گیرنده می فرستد و همچنین سرویس دهنده گواهینامه خود را نیز برای سرویس گیرنده ارسال می کند و اگر سرویس گیرنده از سرویس دهنده، درخواستی

داشت که نیازمند احراز هویت سرویس گیرنده بود، آن را نیز از سرویس گیرنده درخواست می کند .

۳- سپس سرویس گیرنده با استفاده از اطلاعاتی که از سرویس دهنده مجاز در خود دارد، داده ها را بررسی می کند و اگر سرویس دهنده مذکور تایید هویت شد، وارد مرحله بعدی می شود و در غیر این صورت با پیغام هشدار به کاربر، ادامه عملیات قطع می گردد .

۴- سرویس گیرنده یک مقدار به نام Secret Premaster را برای شروع جلسه ایجاد می کند و آن را با استفاده از کلید عمومی (که اطلاعات آن معمولاً در سرویس دهنده موجود است) رمزنگاری می کند و این مقدار رمز شده را به سرویس دهنده ارسال می کند .

۵- اگر سرویس دهنده به گواهینامه سرویس گیرنده نیاز داشت می بایست در این گام برای سرویس دهنده ارسال شود و اگر سرویس گیرنده نتواند هویت خود را به سرویس دهنده اثبات کند، ارتباط در همین جا قطع می شود .

۶- به محض این که هویت سرویس گیرنده برای سرویس دهنده احراز شد، سرویس دهنده با استفاده از کلید اختصاصی خودش مقدار Premaster Secret را رمزگشایی می کند و سپس اقدام به تهیه مقداری به نام Master Secret می نماید .

۷- هم سرویس دهنده و هم سرویس گیرنده با استفاده از مقدار Master Secret کلید جلسه (Session Key) را تولید می کنند که در واقع کلید متقارن مورد استفاده در عمل رمزنگاری و رمزگشایی داده ها حین انتقال اطلاعات است و در این مرحله به نوعی جامعیت داده ها بررسی می شود .

۸- سرویس گیرنده پیغامی را به سرویس دهنده می فرستد تا به او اطلاع دهد، داده بعدی که توسط سرویس گیرنده ارسال می شود به وسیله کلید جلسه رمزنگاری خواهد شد و در ادامه، پیغام رمز شده نیز ارسال می شود تا سرویس دهنده از پایان یافتن Handshake سمت سرویس گیرنده مطلع شود .

۹- سرویس دهنده پیغامی را به سرویس گیرنده ارسال می کند تا او را از پایان Handshake سمت سرویس دهنده آگاه نماید و همچنین این که داده بعدی که ارسال خواهد شد توسط کلید جلسه رمز می شود .

۱۰- در این مرحله SSL Handshake تمام می شود و از این به بعد جلسه SSL شروع می شود و هر دو عضو سرویس دهنده و گیرنده شروع به رمزنگاری و رمزگشایی و ارسال داده ها می کنند.

در زیر برای جمع بندی و درک مطالب در ذهن شما شکل زیر را قرار میدهم.

Internet protocols

Application layer

DHCP · DHCPv6 · DNS · FTP · HTTP · IMAP · IRC · LDAP · MGCP · NNTP · NTP · POP · RPC · RTP · RTSP · SIP · SMTP · SNMP · SOCKS · SSH · Telnet · TLS/SSL · XMPP · (more)

Transport layer

TCP · UDP · DCCP · SCTP · RSVP · (more)

Internet layer

IP (IPv4 · IPv6) · ICMP · ICMPv6 · RIP · OSPF · BGP · ECN · IGMP · IPsec · (more)

Link layer

ARP/InARP · NDP · Tunnels (L2TP) · PPP · Media access control (Ethernet · DSL · ISDN · FDDI) · (more)

فصل ۱۰

TCP/IP Utilities

شبکه علاوه بر قابلیت های ارتباطی خود (پروتکل کنترل انتقال ؛ پروتکل اینترنت (TCP / IP)) شامل مجموعه تعدادی از برنامه های کاربردی که طیف وسیعی از ابزارها میباشند نیز است. در این فصل به بررسی برخی از مهم ترین این ابزارها که مدیران شبکه برای حفظ و عیب یابی از سیستم های TCP / IP از آن استفاده میکنند میپردازیم.

درس ۱

پینگ

پینگ یک ابزار شبکه‌ای است که برای آزمایش میزان دسترسی پذیری یک میزبان در شبکه پروتکل اینترنت به کار می‌رود و می‌تواند زمان رفت و برگشت برای بسته‌های فرستاده شده از میزبان عامل تا یک رایانه مقصد را محاسبه کند.

ping به وسیله فرستادن یک بسته درخواست انعکاس با استاندارد ICMP به هدف منتظر ماندن برای گرفتن پاسخ از نوع ICMP عمل می‌کند. در این فرایند زمان رفت و برگشت محاسبه می‌شود و هر گونه از دست دادن بسته ثبت می‌شود. در آخر نتیجه چاپ شده از این فرآیند، جمع‌بندی‌های آماری از پاسخ بسته‌های رسیده شامل بیشترین، کمترین، میانگین زمان رفت و برگشت بسته‌ها و گاهی انحراف معیار از این میانگین خواهد بود.

کاربرد ابزار ping بیشتر برای ping کردن کامپیوتر میزبان است. ping گزینه‌های خط فرمانی مختلفی دارد که در هر سیستم عاملی متفاوت است که می‌تواند بنا به نیاز ما حالت‌های خاص عملیاتی را فعال کند. این گزینه‌ها می‌توانند سائز بسته آزمایشی را تغییر اندازه دهد، یا انجام ping به صورت تکراری برای دفعات محدود یا انجام دادن ping flood (نوعی از حملات Dos) هست.

درس ۲

Tracert/traceroute

همانطور که از نام این ابزار پیداست از tracert برای پیدا کردن مسیر بین دو Host یا به عبارتی دو دستگاه دارای آدرس شبکه که همدیگر را می بینند استفاده می شود و این دستور از طریق پروتکل ICMP این عمل را انجام میدهد و آن بدین صورت است که پکت echo request توسط کامپیوتر ما به دستگاه مقصد ارسال می شود و در هر مرحله ای از این مسیر پکت exho reply ایجاد شده و به کامپیوتر مبدا (کامپیوتر ما) ارسال می شود.

موارد استفاده از دستور tracer:

جدول زیر برخی از سوئیچ های متداول آن را به همراه دستور گرامر عملکرد tracer نشان می دهد.

دستور گرامر tracer در ویندوز	
Tracert [-d][-h maximum_hops] [-j host-list] [-w timeout] target-name	
عملکرد	سوئیچ
آدرس IP را به نام Host ترجمه می نماید.	-d
حداکثر برای تعداد hop	-h
مقصد مشخص را جستجو می نماید.	Maximum_hops
مدت زمان انتظار را برای دریافت پاسخ بر حسب میلی ثانیه مشخص می نماید.	-w timeou

نحوه عملکرد دستور tracer :

دستور فوق از فیلد TTL مربوط به IP در ICMP Echo Request و پیام های ICMP Time Exceeded به منظور تعیین مسیر مبداء تا مقصد یک بسته اطلاعاتی استفاده می نماید . عملکرد این دستور نیز مشابه ping است و وی نیز از پیام های مبتنی بر ICMP برای یافتن هر یک از

دستگاه های موجود در مسیر یک بسته اطلاعاتی ، استفاده می نماید . برای تشخیص مسیر حرکت ، به TTL موجود در بسته اطلاعاتی یک مقدار اولیه نسبت داده می شود TTL . ، یک عدد صحیح است که حداکثر تعداد hop گره و یا روتر را که یک بسته اطلاعاتی در مسیر خود با آنان برخورد می نماید را مشخص می نماید (قبل از این که توسط IP دورانداخته شود) . مقدار TTL در ابتدا یک خواهد بود و هر روتر و دستگاه موجود در مسیر بسته اطلاعاتی ، یک واحد به آن اضافه می نماید .

بدین ترتیب برنامه tracert قادر به دریافت پیام TIME_EXCEEDED ICMP از هر یک از روترها و یا سایر دستگاه های موجود در مسیر یک بسته اطلاعاتی می باشد.

درس ۳

ifconfig

در سیستم های یونیکس ، لینوکس و مکینتاش از دستور ifconfig به جای ipconfig باید استفاده کنید. برای اینکه صفحه help مربوط به این دستور را نگاه کنید باید از دستور – ifconfig help استفاده کنید. خروجی زیر پس از استفاده تنها از دستور ifconfig حاصل شده است.

```
eth0 Link encap:Ethernet HWaddr 00:60:08:17:63:A0
inet addr:192.168.1.101 Bcast:192.168.1.255 Mask:255.255.255.0
UP BROADCAST RUNNING MTU:1500 Metric:1
RX packets:911 errors:0 dropped:0 overruns:0 frame:0
TX packets:804 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:100
Interrupt:5 Base address:0xe400

lo Link encap:Local Loopback
inet addr:127.0.0.1 Mask:255.0.0.0
UP LOOPBACK RUNNING MTU:3924 Metric:1
RX packets:18 errors:0 dropped:0 overruns:0 frame:0
TX packets:18 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
```

دستور ifconfig آدرسی IP ، subnet mask و default gateway را برای کارت شبکه های محلی و loopback نشان می دهد اما اطلاعات مربوط به وضعیت dhcp را نمایش نمی دهد. برای این

منظور باید از دستور دیگری به شکل "pump s" استفاده کنید Pump. همچنین قادر است IP آدرس شبکه ای را که با DHCP و DNS تنظیم شده است release و renew نماید.

در زیر مواردی را که می توانید از دستور ipconfig استفاده کرده و رفع عیب کنید آورده ام:

۱- کاربر امکان ارتباط با کامپیوترهای دیگر را ندارد.

مطمئن شوید آدرس TCP/IP و Subnet mask دستگاه کامپیوتر شما درست هستند. در صورتیکه

شبکه از DHCP استفاده می کند مطمئن شوید که DHCP بر روی کامپیوتر شما enable است.

۲- امکان ارتباط با کامپیوترهای محلی وجود دارد اما ارتباط با کامپیوترهای دور میسر نیست.

(کامپیوترهای خارج شبکه محلی)

Default gateway را بررسی کنید و ببینید آیا آدرس درست به آن داده شده است.

۳- کاربر امکان ارتباط با اینترنت را ندارد.

پارامترهای مربوط به DNS را بررسی کنید و درستی آن را چک کنید.

۴- کاربر امکان browse کردن را در subnet های غیر از شبکه محلی ندارد.

پارامترهای مربوط به DNS و WINS را بررسی کنید.

با افزودن سوئیچ به دستور Ipconfig می توانید از این دستور بیشتر بهره ببرید.

?این سوئیچ صفحه help را نمایش می دهد.

all این سوئیچ تنظیمات کامل آدرس شبکه را نشان می دهد.

release آدرس IP کارت شبکه با این سوئیچ پاک می شود.

renew آدرس IP کارت شبکه پاک شده و دوباره ایجاد می گردد.

درس ۴

netstat چیست ؟

یکی دیگر از دستوراتی که برای خطایابی TCP/IP می شود از آن استفاده کرد netstat می باشد. این دستور وضعیت پروتکل و کلیه ی ارتباطات و تنظیمات در حال حاضر TCP/IP شبکه ، کلیه ی پورتهایی که در حال استفاده هستند و همچنین جداول مسیریابی (routing table) را نشان میدهد. در واقع این کامند کلیه ی ورودی ها و خروجی ها به کامپیوتر شما را کنترل و بررسی می کند netstat اطلاعات مربوط به هر session ، کارت شبکه ، و اینکه اینها به چه صورت در حال استفاده هستند را نشان می دهد .

به صورت پیش فرض اطلاعاتی که netstat به شما میدهد شامل انواع پروتکل هایی که در آن زمان استفاده می کنید ، local address ها و اطلاعات مربوط به پورتها یی که استفاده می کنند remote address ها و اطلاعات مربوط به پورتهایی که آنها نیز استفاده می کنند و در نهایت وضعیت جاری را نمایش می دهد. همانطور که پیداست این اطلاعات مشخص می کنند که چه ارتباطاتی برقرار و چه عملیاتی در حال انجام است و در زمان جاری کدام پورتهای سیستم باز و در حال تبادل اطلاعات و برقراری session هستند. در واقع ترافیک شبکه را کنترل می کند و به شما می گوید که به طور کلی در شبکه چه خبر است!

درس ۵

Telnet

شبکه راه دور

شبکه راه دور (Telnet) شبکه ای است که در اینترنت و بخش های داخلی استفاده می شود. این در سال ۱۹۶۹ توسعه یافت و ۱۵ RFC در آن استفاده شد. استاندارد آن به صورت IETFSTP۸ می باشد. اصطلاح Telenet به یک نرم افزار اشاره دارد که اجرای بخش سرویس گیرنده است. مشتریان می توانند از سیستم UNIX به مدت چندین سال استفاده کنند، بیشتر تجهیزات شبکه ای و OS که TCP/IP دارند حامی Telenet هستند. اخیراً SecureShell از دسترسی راه دور برای unix استفاده می کند. این اصطلاح به برقراری روابط Telnet و TCP اشاره دارد. در واقع سرور می تواند از یک رمز عبور استفاده کند، یک کاربر می تواند سیستم سرور Unix را ساده کند و مانند کلید عمل نماید. به عنوان مثال کاربر می تواند پست الکترونیکی خود را در مدرسه کنترل کند، به این طریق می تواند ارتباطات کامپیوتری را با سرور برقرار کرد. در این حالت باید اطلاعات و اجرای سیستم عامل از راه دور در نظر گرفته شوند. مانند ls یا CD. در سیستم های زیادی، سرویس گیرنده می تواند از جلسات تعاملی TCP استفاده نماید. در این زمینه جلسات Telnet در واقع TCP خام را با ۲۵۵ بایت عرضه می کنند.

جزئیات پروتکل

Telnet یک پروتکل سرویس دهنده و سرویس گیرنده است و براساس انتقال ارتباطی عمل می کند. این TCP به صورت Port ۲۳ است. اگر چه telnet می تواند TCP/IP را بر NCP اجرا کند. پروتکل ها چند پسوند دارند و هر یک استاندارد اینترنت می باشند. IETF به STD ۲۷ اشاره می کند. STB ۳۲ نیز در تعریف پسوندها کاربرد داشته است. دیگر پسوندهای IETF یک استاندارد هستند.

امنیت

وقتی Telnet در سال ۱۹۶۹ طراحی شد بیشتر کاربرهای شبکه در حوزه های کامپیوتر موسسات آکادمیک، یا در تسهیلات تحقیق دولتی و خصوصی فعال بودند. در این محیط (سال ۱۹۶۹) امنیت خیلی مورد توجه نبود تا اینکه سال ۱۹۹۰ انفجار پهنای باند شد. با افزایش تعداد مردم در دسترسی به اینترنت، و با توسعه، تعدادی تلاش می کنند تا به سرویس دهنده های دیگر نفوذ (crack) کنند که (سرویس دهنده ها) به طور متناوب رمزگذاری شدند حتی بیشتر از یک ضرورت. کارشناسان ایمنی مانند موسسه Sans و اعضای Compoos معتقدند که استفاده از Telnet برای ثبت راه دور می تواند در شرایط عادی متوقف شود. این به دلایل زیر گزارش شده است. کارشناسان ایمنی مانند موسسه Sans و اعضای Compoos معتقدند که استفاده از Telnet برای ثبت راه دور می تواند در شرایط عادی متوقف شود. این به دلایل زیر گزارش شده است. Telnet نمی تواند رمزبرداری داده های ارسال شده را انجام دهد. بنابراین می توان روابط را با یک رمز عبور رشد داد. این عامل دسترسی به یک ردیاب است. آنها بین دو میزبان قرار دارند و Telnet می تواند بسته ها را با اطلاعات کافی عرضه کند. برنامه های کمکی مانند Tcdump و Wircshark از این نوع هستند. این نوع فرآیندهای اجرایی Telnet می توانند بدون طرح اعتبارسازی توصیف شوند. بنابراین باید ارتباطات بین دو میزبان برقرار شوند. در Telnet چندین آسیب پذیری نیز دیده شده است. این نوع نقایص در استفاده پروتکل Telnet زیاد هستند به خصوص در اینترنت و پروتکل SSH که ابتدا در سال ۱۹۹۵ گزارش شد. SSH می تواند قابلیت Telnet را افزایش دهد. این اعتبارسازی کلیدی می تواند متضمن دسترسی به ادعاهای واقعی باشد. این پروتکل ها تعمیم Telnet هستند و می توانند اعتبار sasl و امنیت TLS را به دنبال داشته باشند. با این وجود بیشتر این فرآیندها حامی این تعمیم نمی باشند. علاوه بر اجرای SSH می تواند کافی باشد. مزیت اصلی TLS- TENET شامل توانایی استفاده از گواهی نامه سرور می باشد. آنها دارای کلید ذخیره می باشند. در SSH ضعفهای کاربر باید به خوبی شناخته شوند.

Telnet ۵۲۵۰

IBM۵۲۵۰ یا ۳۲۷۰ می تواند از طریق سرویس گیرنده telnet مایت شود: ۵۲۰۱۰ TN و سرورهای IBM نیز نقش مهم دارند. سرویس دهنده و سرویس گیرنده از داده های ۵۲۵ IBM بر telnet استفاده می کنند. البته حمایت از رمزبرداری SSL نیز عملی است. SSH دارای تقلید ۵۲۵۰ نمی باشد. در OS / ۴۰۰ وردی ۹۹۲ می تواند ایمن سازی telnet را عملی کند.

وضعیت فعلی:

از اواسط ۲۰۰۰ اگر چه پروتکل telnet مورد حمایت زیادی بوده است. سرویس گیرنده ها توانسته اند تمام سرویس ها را دریافت کنند. بدون آنکه از نرم افزار خاص استفاده شود. گاهی اوقات خدمات شبکه ای اشکال زدایی مانند SMTP، IRC، HTTP و FTP یا DOP۳ یک روش ساده برای ارسال دستور و بررسی واکنش هستند. با این وجود دیگر نرم افزارها مانند NC و Socat می توانند مورد توجه بیشتر مجریان سیستم قرار گیرند. این نوع مباحث مربوط به ارسال داده های کنترل ترمینال می باشند. نرم افزار telnet بسته به یک استاندارد عملی می شود. telnet هنوز در شبکه های شرکتی استفاده می شود. و می تواند برنامه های میزبان را در دسترس قرار دهد مانند شبکه های اصلی IBM. Telnet در اجرای عناصر شبکه نقش مهم دارد مانند شکل گیری کمیسیون، هماهنگی و تعمیرات عناصر شبکه اصلی در شبکه های متحرک. telnet می تواند برای بازی های MUD در اینترنت استفاده شود مانند talkers، mushes، muck، moo و جامعه BBS، در ویندوز میکروسافت ۲۰۰۷ ویندوز Vista نتوانست طبق پیش فرض نصب شود.

سیستم مکینتاش

۳۲۷۰ tn یک نوع سرویس گیرنده بدون telnet برای مکینتاش می باشد. طراحی سیستم اصلی IBM با استفاده از ۳۲۷۰ tn عملی است. ترمینال می تواند دستور telnet را برای برنامه رابط گزارش کند. این بخشی از ترمینال مکینتاش osx می باشد. Nifty telnet یک سرویس گیرنده

کوچک telnet برای نسخه های mocos معرفی شده است و آنها حامی SSH هستند. Data comet
یک برنامه SSH&telnet برای مکینتاش است

سیستم چندگانه

- Putt یک نوع SSH، Telnet و rlogin و یا tcp خام برای ویندوز، linux و unix می باشد.
- M telnet یک سرویس گیرنده ۱۵ صفحه نمایش بزرگ می باشد. این می تواند در اجرای OS/۲ مفید باشد. سهولت استفاده مربوط به قابلیت پیاده کردن Zmodem می باشد.
- Twisted conch دارای یک روند اجرایی سرویس دهنده و سرویس گیرنده است.
- LVT نیز یک سیستم چند جلسه ای می باشد. آنها برای ویندوز DOS کاربرد داشته اند.
- حمایت SSH و Kerberos مربوط به این فرآیند است. ویژگی های مفید مانند نسخه برداری و ثبت خودکار در این زمینه نقش مهم دارند.
- Synct ERM یک نوع ترمینال و سرویس گیرنده Telnet/ Rlogin/SSH می باشد که در ویندوز و سیستم nix رایج می باشد. حمایت zomdem با صفحه نمایش کامل از این فرآیند است.
- Rove mobile SSH یک بر مبنای دستور و یک سرویس گیرنده Telnet برای unix و linux می باشد. حمایت bluet.th نیز از این دسته است.

رهایی از کد مبدا

- D telnet یک سرویس گیرنده telnet آزاد برای ویندوز است.
- Pueblo/UE یک سرویس گیرنده telnet آزاد برای ویندوز است و حمایت HTML را انجام می دهد.
- Console telnet یک صفحه نمایش بزرگ است و برای محیط های ۳۲ mswin کاربرد دارد.

کد مبدا غیرآزاد

Whitehorn secure یک سرویس گیرنده بدون telnet برای ویندوز است.

- Simpterm یک سرویس گیرنده تک کدی برای محیط ۳۲ mswin است و می تواند برای چینی ها استفاده شود.
- Simplemu یک سرویس گیرنده telnet مشترک است. و می تواند قابلیت های نوشتاری در vb script جاوا perl داشته باشد.

سرور telnet**بدون کد مبدا**

- telnetd یک telnet داخلی به زبان جاوا می باشد.
- Poor woman's یک سرور telnet جاوا مستقل است. telnet server
- Synchronet یک سرور BBS linux و ۳۲ win است. که حامی http, nntp, pop3, ftp و دیگر پروتکل ها است.

درس ۶

NSLookup

NSLookup یک برنامه از نوع خط فرمان (command-line) است که مخفف Name Server Lookup می باشد. به وسیله NSLookup می توان از Name Server های مختلف اطلاعات مربوط به دامنه های مورد نظر را در صورت امکان بدست آورد. اطلاعاتی که درباره دامنه از طریق NSLookup مشاهده می کنیم، در واقع همان اطلاعاتی است که در ZoneFile مربوط به دامنه وجود دارد.

اجرای برنامه NSLookup

Command Shell را باز می کنیم و دستور nslookup را تایپ می کنیم.



```

c:\utils>nslookup
*** Can't find server name for address 192.168.200.192: Non-existent domain
Default Server: UnKnown
Address: 192.168.200.192
>

```

هنگام اجرا، NSLookup سروری را که به عنوان DNS Server کامپیوتر شما تعریف شده است را به عنوان سرور پیش فرض تعیین می کند. این آدرس را می توانید در تنظیمات شبکه خود در بخش TCP/IP مشاهده کنید. برای مثال در شکل بالا سروری که پرسش های ما را جواب می دهد، دارای آدرس ۱۹۲/۱۶۸/۲۰۰/۱۹۲ است که یک Name Server در شبکه داخلی می باشد.

حال آدرس font.ir را وارد می کنیم.

```

c:\ Command Shell - nslookup
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.

c:\utils>nslookup
*** Can't find server name for address 192.168.200.192: Non-existent domain
Default Server: UnKnown
Address: 192.168.200.192

> font.ir
Server: UnKnown
Address: 192.168.200.192

Non-authoritative answer:
Name: font.ir
Address: 217.218.60.151

>

```

دو خط اول پاسخ مشخص می کند که کدام سرور و با چه آدرسی پاسخ را ارائه کرده است.

خط سوم عبارت Non-authoritative را مشاهده می کنیم. این عبارت به این معنی است که سرور ۱۹۲/۱۶۸/۲۰۰/۱۹۲، مرجع پایه اطلاعات دامنه font.ir نیست و آن را در اختیار ندارد، لذا فرایند resolve را برای دریافت آنها آغاز کرده است و اطلاعات مربوط به این دامنه را از سرور دیگری دریافت کرده است.

در خط چهارم و پنجم نام دامنه و آدرس هاست آن ۲۱۷/۲۱۸/۶۰/۱۵۱ را مشاهده می کنیم. که مطابق با آدرسی است که در ابتدای صفحه در جدول ZoneFile مربوط به دامنه font.ir در رکورد A مشاهده کردیم.

برای اینکه از یک سرور دیگر پرس و جو کنیم، در خط فرمان عبارت server و نام سرور مورد نظر یا آدرس IP آن را می نویسیم.

این بار از سرور ns۴.com.parsihost.com درباره دامنه font.ir می پرسیم.

```

C:\ Command Shell - nslookup
> server ns4.parsihost.com
Default Server: ns4.parsihost.com
Address: 217.218.60.151

> font.ir
Server: ns4.parsihost.com
Address: 217.218.60.151

Name: font.ir
Address: 217.218.60.151

>

```

همانطور که در شکل می بینید، به کمک دستور `server ns4.parsihost.com`، سرور پیش فرض را به `ns4.parsihost.com` تغییر می دهیم. این بار در جوابی که برای `font.ir` مشاهده می کنیم عبارت `Non-authoritative` دیده نمی شود. در واقع در اینجا `ns4.parsihost.com` مرجع پایه اطلاعات دامنه `font.ir` است.

همانطور که در جدول مربوط به `ZoneFile` دامنه دیدید، در این جدول انواع مختلفی از اطلاعات وجود دارد که می توان نوع آنها را در ستون `Recordtype` مشاهده کرد.

برای بدست آوردن سایر اطلاعات دامنه می توانیم از دستور `set type` استفاده کنیم. این دستور دارای ساختاری طبق عبارت ذیل می باشد.

Settype=NAME
(where NAME is the type of record to look at for example, A, ANY, CNAME, MX,
NS, PTR, SOA, SRV)

به جای عبارت `NAME` میتوان یکی از انواع داده موجود در `ZoneFile` را نوشت. به طور مثال `A, MX, NS, TXT, ...`

برای مثال دستور `set type=txt` را تایپ می کنیم و مجدداً درباره دامنه `font.ir` پرس و جو می کنیم.

```

c:\ Command Shell - nslookup
ns28.DNSLake.com internet address = 66.207.222.170
> set type=txt
> font.ir
Server: ns4.parsihost.com
Address: 217.218.60.151

font.ir text =

"v=spf1 mx -all"
font.ir nameserver = ns28.DNSLake.com
font.ir nameserver = ns4.parsihost.com
font.ir nameserver = ns2.parsihost.com
ns2.parsihost.com internet address = 206.223.171.254
ns4.parsihost.com internet address = 217.218.60.151
ns28.DNSLake.com internet address = 66.207.222.170
>

```

همانطور که در شکل می بینید، اطلاعات مربوط به رکورد TXT دامنه را نمایش می دهد، که می توان مقدار نمایش داده شده را با مقدار آن در جدول ابتدای صفحه مقایسه کرد.

NSLookup دارای دو دستور اصلی server و set type می باشد. برای مشاهده فهرست دستورات می توانید در خط فرمان عبارت ? یا help را تایپ کنید.

برای اطلاع بیشتر درباره NSLookup می توانید به این مقاله مراجعه کنید.

(<http://support.microsoft.com/kb/۲۰۰۵۲۵>)

در واقع NSLookup یک ابزار مدیریتی در شبکه برای آزمایش و رفع اشکال Name Server ها می باشد. علاوه بر NSLookup می توان از سایر نرم افزارها مانند DIG استفاده کرد. (Domain Information Groper - کاوشگر اطلاعات دامنه)

در این فصل جای خالی دستور آرپ حس میشود اما قبلا راجع به آن صحبت کردیم.

فصل ۱۱

Remote Network Access

اگر چه بیشتر مردم عبارت "شبکه های کامپیوتری" را با شبکه های محلی (LAN)، یا انواع دیگر ارتباطات کامپیوتر شبکه می شناسند. اما به عنوان مثال، هنگام استفاده از مودم dial-up برای اتصال به اینترنت، شما در واقع به یک شبکه از راه دور متصل شده اید. در این مورد، پورت سریال و یا اسلات bus بر روی کامپیوتر شما رابط شبکه و سیستم تلفن است که شما را به شبکه وصل کرده است. که کامپیوتر شما با کمک isp شما را به شبکه متصل کرده است. که در این فصل به این تکنولوژی ها می پردازیم.

تکنولوژی هایی که شما را از راه دور به یک شبکه متصل میکنند.

در هنگام تالیف این فصل مردد بودم که آن را در فصل ۵ بیان کنم یا در این فصل که صلاح بر این دیدم در اینجا بازگو کنم و امیدوارم شما را به درک این موضوعات نزدیک کرده باشم.

درس ۱

Using Remote Connections

فن آوریهای زیادی وجود دارد که شما میتوانید با استفاده از آنها به شبکه های راه دور متصل شوید. از لایه بالای شبکه یک ارتباط از راه دور میتوان زد که تفاوتی با شبکه های محلی مستقیم ندارد اما لایه های فیزیکی و پیوند داده میتوانند فرم دیگری پیدا کنند. اینجا همان نکته است که گفتم میشد این بحث را در فصل ۵ بیان کرد چرا که در درس بعدی به پروتکل های این دو لایه مجدد میپردازیم اما با این تفاوت که دیگر برای شبکه های محلی نیستند بلکه برای ارتباطات راه دور میباشند.

PSTN چیست ؟

Public Switched Telephone Network یا شبکه سوئیچینگ تلفن عمومی وظیفه ارتباط دهی تماسهای تلفنی و انتقال پیامهای صوتی را بر عهده دارد . واقعیت آن است که PSTN از گذشته های دور و از همان ابتدا بصورت ساده وجود داشته است و امروزه با گذشت زمان و ظهور تکنولوژی های جدید به شکل کنونی خود رسیده است تا ما در هر منطقه مخابراتی شاهد يك PSTN مجهز باشیم .

سابقه PSTN

در ابتدا هدف از ایجاد PSTN ایجاد يك ارتباط بین دو دستگاه تلفن می بود . این مدار از نقطه تماس گیرنده شروع و تا نقطه مقصد ادامه پیدا می کرد . در حقیقت يك سیم از تلفن مبدأ تا دفتر PSTN و يك سیم هم از مقصد تا دفتر PSTN رد و بدل می شد و در آخر سیم بوسیله يك لامپ وضعیت گوشی نمایان می شد . به عبارتی همه مشترکین بر روی تابلو سوئیچ PSTN يك لامپ داشتند . کارمند PSTN پس از روشن شدن لامپ خط با مشترک صحبت می کرد و از او مقصد ارتباط را سوال می کرد . پس از مشخص شدن مقصد ، کارمند PSTN بوسیله يك کابل ارتباط مورد نیاز را بین دو مشترک برقرار می کرد . اولین بار PSTN توسط شرکت الکساندر گراهام بل و قبل از اینکه کامپیوتری حتی با لامپ خلاء هم وجود داشته باشد راه اندازی شد . این دفترهای PSTN با گذشت زمان و افزایش مشترکین، دیگر جوابگوی نیازها نبودند . در نتیجه مجبور به تغییر در سیگنالینگ يك ارتباط تلفنی شدند و تلفن ها به يك شماره گیر گردان بر روی خود مجهز شد . این شماره گیر ها بصورت PULL و با صداهای بیپ مانند به PSTN شماره مقصد را اعلام می کردند و دفتر PSTN بصورت خودکار ارتباط مبدأ را با مقصد درخواستی برقرار می کرد . از آنجایی که شماره گیری با شماره گردانها زمانبر بود و برای شماره هایی که تعداد زیادی ۸ ، ۹ و یا صفر در خود دارند زمانی بالغ بر ۳۰ ثانیه صرف می شد، شماره گیر گردان را با يك صفحه کلید عوض کردند تا در وقت نیز صرفه جویی شود . این صفحه کلیدها که هم اکنون هم بر روی تلفن های کنونی نصب و فعال هستند و صدایی با فرکانس متفاوت برای هر شماره ایجاد می کنند. این صداها

استاندارد هستند و PSTN با دریافت صداها و آنالیز آنها مقصد مورد نظر شما را مشخص خواهد کرد. تن های ایجاد شده توسط صفحه کلید در اصطلاح Dual Tone Multi Frequency خوانده می شوند.

تغییر سیگنال در PSTN

PSTN با تغییر در ساختار سیگنالینگ و تبدیل آن به دیجیتال این امکان را فراهم کرد تا بتوان ساختار ارتباط دهی تماس ها را مکانیزه و خودکار نمود. استانداردهای زیادی بمنظور این تبدیل وجود دارد ولی آنچه شایع شده قراردادن ولتاژ V_{5+} برای يك باینری و ولتاژ V_{5-} برای سفر باینری می باشد. گفتنی است که امروزه از استانداردهای دقیقتری استفاده می شود.

تبدیل صدای آنالوگ به صدای دیجیتال

برای صرفه جویی در هزینه ها و جلوگیری از تعویض کابلها و سیم های قدیمی پس از دریافت درخواست ارتباط صوتی از سوی مبدأ به PSTN دستگاه مبدل آنالوگ به دیجیتال (Voice Switch) آدرس مقصد را شناسایی و به مبدل A/D مقصد متصل می شود و با استاندارد معروف به DCM (تبدیل کد پالس) در هر ثانیه ۸۰۰۰ بار از سیگنال آنالوگ نمونه برداری می کند و آن را از نظر مشخصه های گوناگون همچون فرکانس، دامنه و فضا نمونه برداری می کند و در جدولی کدهای دیجیتال برابر با آنها شناسایی می شوند. هدف از ۸۰۰۰ بار نمونه برداری در ثانیه انتخاب بهترین فرکانس، دامنه و فاز انتخاب بهترین بیتهای تعریف کننده صدا می باشد تا در طرف گیرنده صدایی برابر با صدای گوینده دریافت شود. در طرف گیرنده هم عملیاتی مشابه طرف مبدأ انجام می گیرد منتهی نه با این دقت چرا که وضعیت اصلی صدا در طرف فرستنده مشخص شده و در این بخش صدای مورد نظر فقط باید پخش شود.

تبدیل در مودم های آنالوگ :

مودم امکان ارسال و دریافت يك جریان از بیت ها بصورت سریال را به کامپیوتر می دهد. يك مودم يك سیگنال آنالوگ را برای PSTN ارسال می کند و انتظار دریافت سیگنال آنالوگ در جواب آن را دارد. در عوض کلیه فرآیند تبدیل داده در هر مودم انجام می پذیرد. مودم بعد از اتصال به مودم طرف مقصد این توانایی را دارد تا با بررسی استانداردهای مختلف بر سر انتخاب بهترین استاندارد تبدیل با مودم مقصد به توافق برسد و عملیات انتقال داده را شروع نماید.

باتوجه به سابقه طولانی مودم ، استانداردهای گوناگونی برای اتصال طراحی شد. تازه ترین استاندارد ها ۷۹۲ است که به مودم این اجازه را می دهد تا با سرعت نامتقارن ۵۶ kbps برای ارسال داده و ۳۳ kbps برای دریافت داده ها به فعالیت پردازد. همچنین این استاندارد، سرعت متقارن ۴۸ kbps را برای ارسال و دریافت داده فراهم می آورد. از مزایای دیگر استاندارد ۷۹۲ می توان به خاصیت پشتیبانی از Call Waiting اشاره کرد. شما با استفاده از این خصلت می توانید يك تماس کوتاه در حین اتصال مودمها به یکدیگر را تجربه کنید.

VPN

VPN^۱ يك شبکه خصوصی مجازی است که ارتباطات کپسوله شده (Encapsulated) ، رمزنگاری شده (Encrypted) و تصدیق شده (Authenticated) را با استفاده از سیستم مسیریابی زیرساخت شبکه از طریق يك شبکه عمومی مانند اینترنت ایجاد و مدیریت می کند. این ارتباط می تواند بین دو سیستم عادی برقرار شده و یا برای ارتباط امن سرور يك سازمان با شعب آن در سراسر جهان به کار رود. برای کاربران تجاری بیش از يك ضرورت و بلکه نعمتی است که راهی مطمئن، امن و در عین حال ارزان برای دسترسی به فایل هایشان در شبکه محل کار خود (وقتی که آن ها در مسافرت، خانه و یا در راه هستند) در اختیار می گذارد. کاربران در حالت عادی برای تماس به صورت

^۱Virtual Private Network

Remote (راه دور) با سرور نیاز دارند که به صورت مستقیم و توسط يك ارتباط DialUp به سرور RAS متصل شوند.

استفاده از RAS سرور و خط تلفن برای برقراری ارتباط دو مشکل عمده دارد که عبارتند از :
۱- در صورتی که RAS سرور و سیستم تماس گیرنده در يك استان قرار نداشته باشند، علاوه بر لزوم پرداخت هزینه زیاد، سرعت ارتباط نیز پایین خواهد آمد و اینمسأله وقتی بیشتر نمود پیدا می کند که کاربر نیاز به ارتباطی با سرعت مناسب داشته باشد.

۲- در صورتی که تعداد اتصالات راه دور در يك لحظه بیش از يك مورد باشد، RAS سرور به چندین خط تلفن و مودم احتیاج خواهد داشت که باز هم مسأله هزینه مطرح می گردد .

اما با ارتباط VPN مشکلات مذکور به طور کامل حل می شود و کاربر با اتصال به ISP محلی به اینترنت متصل شده و VPN بین کامپیوتر کاربر و سرور سازمان از طریق اینترنت ایجاد می گردد . ارتباط مذکور می تواند از طریق خط DialUp و یا خط اختصاصی مانند Leased Line برقرار شود. به هر حال اکنون مسأله این نیست که طریقه استفاده از VPN چیست، بلکه مسأله این است که کدامیک از تکنولوژی های VPN باید مورد استفاده قرار گیرند. پنج نوع پروتکل در VPN مورد استفاده قرار می گیرد که هر کدام مزایا و معایبی دارند .

ارتباط سیستم ها در يك اینترنت

دربخشی سازمان ها، اطلاعات يك دپارتمان خاص به دلیل حساسیت بالا، به طور فیزیکی از شبکه اصلی داخلی آن سازمان جدا گردیده است. این مسأله علیرغم محافظت از اطلاعات آن دپارتمان، مشکلات خاصی را نیز از بابت دسترسی کاربران دپارتمان مذکور به شبکه های خارجی به وجود می آورد.

VPN اجازه میدهد که شبکه دپارتمان مذکور به صورت فیزیکی به شبکه مقصد مورد نظر متصل گردد، اما به صورتی که توسط VPN سرور، جدا شده است. (با قرار گرفتن VPN سرور بین دو شبکه)

البته لازم به یادآوری است که نیازی نیست VPN سرور به صورت یک Router مسیریاب بین دو شبکه عمل نماید، بلکه کاربران شبکه مورد نظر علاوه بر این که خصوصیات و Subnet شبکه خاص خود را دارا هستند به VPN سرور متصل شده و به اطلاعات مورد نظر در شبکه مقصد دست می یابند.

علاوه بر این تمام ارتباطات برقرار شده از طریق VPN، می توانند به منظور محرمانه ماندن رمزنگاری شوند. برای کاربرانی که دارای اعتبارنامه مجاز نیستند، اطلاعات مقصد به صورت خودکار غیر قابل رویت خواهند بود.

مبانی Tunneling

Tunneling یا سیستم ایجاد تونل ارتباطی با نام کپسوله کردن (Encapsulation) نیز شناخته می شود که روشی است برای استفاده از زیرساخت یک شبکه عمومی جهت انتقال اطلاعات. این اطلاعات ممکن است از پروتکل های دیگری باشد. اطلاعات به جای این که به صورت اصلی و Original فرستاده شوند، با اضافه کردن یک Header (سرایند) کپسوله می شوند.

این سرایند اضافی که به پکت متصل می شود، اطلاعات مسیریابی را برای پکت فراهم می کند تا اطلاعات به صورت صحیح، سریع و فوری به مقصد برسند. هنگامی که پکت های کپسوله شده به مقصد رسیدند، سرایندها از روی پکت برداشته شده و اطلاعات به صورت اصلی خود تبدیل می شوند. این عملیات را از ابتدا تا اتمام کار Tunneling می نامند.

نگهداری تونل

مجموعه عملیات متشکل از پروتکل نگهداری تونل و پروتکل تبادل اطلاعات تونل به نام پروتکل Tunneling شناخته می‌شوند. برای این که این تونل برقرار شود، همکلاینت و هم سرور می‌بایست پروتکل Tunneling یکسانی را مورد استفاده قرار دهند. از جمله پروتکل‌هایی که برای عملیات Tunneling مورد استفاده قرار می‌گیرند PPTP و L2TP هستند که در ادامه مورد بررسی قرار خواهند گرفت.

پروتکل نگهداری تونل

پروتکل نگهداری تونل به عنوان مکانیسمی برای مدیریت تونل استفاده می‌شود. برای برخی از تکنولوژی‌های Tunneling مانند PPTP و L2TP یک تونل مانند یک Session می‌باشد، یعنی هر دو نقطه انتهایی تونل علاوه بر این که باید با نوع تونل منطبق باشند، می‌بایست از برقرار شدن آن نیز مطلع شوند.

هرچند برخلاف یک Session، یک تونل دریافت اطلاعات را به صورتی قابل اطمینان گارانتی نمی‌کند و اطلاعات ارسالی معمولاً به وسیله پروتکلی بر مبنای دیتاگرام مانند UDP هنگام استفاده از L2TP یا TCP برای مدیریت تونل و یک پروتکل کپسوله کردن مسیریابی عمومی اصلاح شده به نام GRE برای وقتی که PPTP استفاده می‌گردد، پیکربندی و ارسال می‌شوند.

ساخته شدن تونل

یک تونل باید قبل از این که تبادل اطلاعات انجام شود، ساخته شود. عملیات ساخته شدن تونل به وسیله یک طرف تونل یعنی کلاینت آغاز می‌شود و طرف دیگر تونل یعنی سرور، تقاضای ارتباط Tunneling را دریافت می‌کند. برای ساخت تونل عملیات ارتباطی مانند PPP انجام می‌شود.

سرور تقاضا می کند که کلاینت خودش را معرفی کرده و معیارهای تصدیق هویت خود را ارائه نماید. هنگامی که قانونی بودن و معتبر بودن کلاینت مورد تأیید قرار گرفت، ارتباط تونل مجاز شناخته شده و پیام ساخته شدن تونل توسط کلاینت به سرور ارسال می گردد و سپس انتقال اطلاعات از طریق تونل شروع خواهد شد.

برای روشن شدن مطلب، مثالی می زنیم. اگر محیط عمومی را، که غالباً نیز همین گونه است، اینترنت فرض کنیم، کلاینت پیام ساخته شدن تونل را از آدرس IP کارت شبکه خود به عنوان مبدا به آدرس IP مقصد یعنی سرور ارسال می کند. حال اگر ارتباط اینترنت به صورت DialUp از جانب کلاینت ایجاد شده باشد، کلاینت به جای آدرس NIC خود، آدرس IP را که ISP به آن اختصاص داده به عنوان مبدا استفاده خواهد نمود.

نگهداری فعال

دربار برخی از تکنولوژی های Tunneling مانند L2TP و PPTP، تونل ساخته شده باید نگهداری و مراقبت شود. هر دو انتهای تونل باید از وضعیت طرف دیگر تونل باخبر باشند. نگهداری یک تونل معمولاً از طریق عملیاتی به نام نگهداری فعال (KA) اجرا می گردد که طی این پروسه به صورت دوره زمانی مداوم از انتهای دیگر تونل آمارگیری می شود. این کار هنگامی که اطلاعاتی در حال تبادل نیست، انجام می پذیرد.

پروتکل تبادل اطلاعات تونل

زمانیکه یک تونل برقرار می شود، اطلاعات می توانند از طریق آن ارسال گردند. پروتکل تبادل اطلاعات تونل، اطلاعات را کپسوله کرده تا قابل عبور از تونل باشند. وقتی که تونل کلاینت قصد ارسال اطلاعات را به تونل سرور دارد، یکسرایند (مخصوص پروتکل تبادل اطلاعات) را بر روی پکت

اضافه می کند. نتیجه این کار این است که اطلاعات از طریق شبکه عمومی قابل ارسال شده و تا تونل سرور مسیریابی می شوند.

تونل سرور پکت ها را دریافت کرده و سرایند اضافه شده را از روی اطلاعات برداشته و سپس اطلاعات را به صورت اصلی درمی آورد.

انواع تونل

تونل ها به دو نوع اصلی تقسیم می گردند: اختیاری و اجباری .

تونل اختیاری

تونل اختیاری به وسیله کاربر و از سمت کامپیوتر کلاینت طی يك عملیات هوشمند، پیکربندی و ساخته می شود. کامپیوتر کاربر نقطه انتهایی تونل بوده و به عنوان تونل کلاینت عمل می کند. تونل اختیاری زمانی تشکیل می شود که کلاینت برای ساخت تونل به سمت تونل سرور مقصد داوطلب شود.

هنگامی که کلاینت به عنوان تونل کلاینت قصد انجام عملیات دارد، پروتکل Tunneling مورد نظر باید بر روی سیستم کلاینت نصب گردد. تونل اختیاری می تواند در هر یک از حالت های زیر اتفاق بیفتد :

- کلاینت ارتباطی داشته باشد که بتواند ارسال اطلاعات پوشش گذاری شده را از طریق مسیریابی به سرور منتخب خود انجام دهد.

- کلاینت ممکن است قبل از این که بتواند تونل را پیکربندی کند، ارتباطی را از طریق DialUp برای تبادل اطلاعات برقرار کرده باشد. این معمول ترین حالت ممکن است. بهترین مثال از این حالت،

کاربران اینترنت هستند. قبل از این که یک تونل برای کاربران بر روی اینترنت ساخته شود، آن‌ها باید به ISP خود شماره گیری کنند و یک ارتباط اینترنتی را تشکیل دهند.

تونل اجباری

تونل اجباری برای کاربرانی پیکر بندی و ساخته می شود که دانش لازم را نداشته و یا دخالتی در ساخت تونل نخواهند داشت. در تونل اختیاری، کاربر، نقطه نهایی تونل نیست. بلکه یک Device دیگر بین سیستم کاربر و تونل سرور، نقطه نهایی تونل است که به عنوان تونل کلاینت عمل می نماید. اگر پروتکل Tunneling بر روی کامپیوتر کلاینت نصب و راه اندازی نشده و در عین حال تونل هنوز مورد نیاز و درخواست باشد، این امکان وجود دارد که یک کامپیوتر دیگر و یا یک Device شبکه دیگر، تونلی از جانب کامپیوتر کلاینت ایجاد نماید.

این وظیفه ای است که به یک متمرکز کننده دسترسی (AC) به تونل، ارجاع داده شده است. در مرحله تکمیل این وظیفه، متمرکز کننده دسترسی یا همان AC باید پروتکل Tunneling مناسب را ایجاد کرده و قابلیت برقراری تونل را در هنگام اتصال کامپیوتر کلاینت داشته باشد. هنگامی که ارتباط از طریق اینترنت برقرار میشود، کامپیوتر کلاینت یک تونل تأمین شده¹ NAS را از طریق ISP احضار می کند.

به عنوان مثال یک سازمان ممکن است قراردادی با یک ISP داشته باشد تا بتواند کل کشور را توسط یک متمرکز کننده دسترسی به هم پیوند دهد. این AC می تواند تونل هایی را از طریق اینترنت برقرار کند که به یک تونل سرور متصل باشند و از آن طریق به شبکه خصوصی مستقر در سازمان مذکور دسترسی پیدا کنند.

¹Network Access Service

این پیگر بندی به عنوان تونل اجباری شناخته می شود، به دلیل این که کلاینت مجبور به استفاده از تونل ساخته شده به وسیله AC شده است. یک بار که این تونل ساخته شد، تمام ترافیک شبکه از سمت کلاینت و نیز از جانب سرور به صورت خود کار از طریق تونل مذکور ارسال خواهد شد.

به وسیله این تونل اجباری، کامپیوتر کلاینت یک ارتباط PPP می سازد و هنگامی که کلاینت به NAS، از طریق شماره گیر متصل می شود، تونل ساخته می شود و تمام ترافیک به طور خود کار از طریق تونل، مسیریابی و ارسال می گردد. تونل اجباری می تواند به طور ایستا و یا خود کار و پویا پیگر بندی شود.

تونل های اجباری ایستا

پیگر بندی تونل های Static معمولاً به تجهیزات خاص برای تونل های خود کار نیاز دارند. سیستم Tunneling خود کار به گونه ای اعمال می شود که کلاینت ها به AC از طریق شماره گیری (Dialup) متصل می شوند. این مسأله احتیاج به خطوط دسترسی محلی اختصاصی و نیز تجهیزات دسترسی شبکه دارد که به این ها هزینه های جانبی نیز اضافه می گردد.

برای مثال کاربران احتیاج دارند که با یک شماره تلفن خاص تماس بگیرند، تا به یک AC متصل شوند که تمام ارتباطات را به طور خود کار به یک تونل سرور خاص متصل می کند. در طرح های Tunneling ناحیه ای، متمرکز کننده دسترسی بخشی از User Name را که Realm خوانده می شود بررسی می کند تا تصمیم بگیرد در چه موقعیتی از لحاظ ترافیک شبکه، تونل را تشکیل دهد.

تونل های اجباری پویا

در این سیستم انتخاب مقصد تونل بر اساس زمانی که کاربر به AC متصل می شود، ساخته می شود. کاربران دارای Realm یکسان، ممکن است تونل هایی با مقصدهای مختلف تشکیل بدهند. البته

این امر به پارامترهای مختلف آنها مانند Username ، شماره تماس، محل فیزیکی و زمان بستگی دارد .

تونل های Dynamic ، دارای قابلیت انعطاف عالی هستند. همچنین تونل های پویا اجازه می دهند که AC به عنوان یک سیستم Multi-NAS عمل کند، یعنی اینکه همزمان همارتباطات Tunneling را قبول می کند و هم ارتباطات کلاینت های عادی و بدون تونل را. در صورتی که متمرکزکننده دسترسی بخواهد نوع کلاینت تماس گیرنده رامبنی بر دارای تونل بودن یا نبودن از قبل تشخیص بدهد، باید از همکاری یک بانک اطلاعاتی سود ببرد.

برای این کار باید AC اطلاعات کاربران رادر بانک اطلاعاتی خود ذخیره کند که بزرگترین عیب این مسأله این است که این بانک اطلاعاتی به خوبی قابل مدیریت نیست.

بهترین راه حل این موضوع، راه اندازی یک سرور RADIUS است، سروری که اجازه می دهد که تعداد نامحدودی سرور، عمل شناسایی User های خود را بر روی یک سرور خاص یعنی همین سرور RADIUS انجام دهند، به عبارت بهتر این سرور مرکزی برای ذخیره و شناسایی واحراز هویت نمودن کلید کاربران شبکه خواهد بود.

پروتکل های VPN

عمده ترین پروتکل هایی که به وسیله ویندوز ۲۰۰۰ برای دسترسی به VPN استفاده می شوند عبارتند از L۲TP ، Ipsec ، PPTP ، IP-IP

پروتکل IP-IP

این پروتکل که با نام IP-in-IP نیز شناخته می شود، یک پروتکل لایه سوم یعنی لایه شبکه است. مهمترین استفاده پروتکل IP-IP برای ایجاد سیستم Tunneling به صورت Multicast است که در شبکه هایی که سیستم مسیریابی Multicast راپشتیبانی نمی کنند کاربرد دارد. ساختار پکت IP-IP

تشکیل شده است از: سرایند IP خارجی، سرایند تونل، سرایند IP داخلی و اطلاعات IP. اطلاعات IP می تواند شامل هر چیزی در محدوده IP مانند TCP، UDP، ICMP و اطلاعات اصلی پکت باشد.

مدیریت VPN

در بیشتر موارد مدیریت يك VPN مانند مدیریت يك RAS سرور (به طور خلاصه، سروریکه ارتباطها و Connection های برقرار شده از طریق راه دور را کنترل و مدیریت می کند)، می باشد. البته امنیت VPN باید به دقت توسط ارتباطات اینترنتی مدیریت گردد.

مدیریت کاربران

VPN

بیشتر مدیران شبکه برای مدیریت کاربران خود از يك پایگاه داده مدیریت کنندگانها بر روی کامپیوتر DC و یا از سرور RADIUS استفاده می نمایند. اینکار به سرور VPN اجازه می دهد تا اعتبارنامه احراز هویت کاربران را به یکسیستم احراز هویت مرکزی ارسال کند.

مدیریت آدرس ها و Name Server ها

سرور VPN باید رشته ای از آدرس های IP فعال را در خود داشته باشد تا بتواند آن ها را در طول مرحله پردازش ارتباط از طریق پروتکل کنترل IP به نام IPCP به درگاه های VPN Server و یا Client ها اختصاص دهد.

در VPN هایی که مبتنی بر ویندوز ۲۰۰۰ پیگیری می شوند، به صورت پیش فرض، IP آدرس هایی که به Client های VPN اختصاص داده می شود، از طریق سرور DHCP گرفته می شوند.

البته همان طور که قبلاً گفته شد شما می توانید يك رشته IP را به صورت دستی یعنی ایستا به جای استفاده از DHCP اعمال کنید. ضمناً VPN Server باید توسط یکسیستم تأمین کننده نام مانند DNS و یا WINS نیز پشتیبانی شود تا بتواند سیستم IPCP را به مورد اجرا بگذارد.

ISDN چیست؟

در گذشته تلفن ها همگی آنالوگ بودند و یک عیب بسیار بزرگ بشمار می آمد. زیرا هنگام ارسال صدا نویز وارد کانال می شد و کیفیت را به شدت کاهش می داد. کدینگ دیجیتال راهی برای کد کردن صدا و تشخیص خطا طراحی کرد. بنابراین شبکه های IDN^۱ طراحی شد و تمام شبکه های تلفنی آنالوگ به دیجیتال تبدیل شد.

ISDN^۲ و بعنوان یک شبکه مخابراتی دیجیتال عمومی به کار می رود .

با استفاده از ISDN امکانات جدیدی برای ارتباط دیتا بوجود می آید اکنون پس از استفاده وسیع ISDN بصورت باند باریک ، زمان اجرای باند پهن ISDN براساس تکنیک ATM ، فرا رسیده که بعنوان یک شبکه باند پهن جامع سرویسهای مخابراتی در نظر گرفته می شود .

وضعیت امروزی در بسیاری از شرکتها ، نشان می دهد که تکنولوژی های مختلف شبکه مانند X.۲۵ ، LAN معمول (Token Ring Ethernet , FODL) ، LAN های مبتنی بر ATM و نیز ISDN برای ارتباط دیتا بکار برده می شود . ISDN می تواند در صورت اتحاد با شبکه های دیگر دیتا مزیت های اضافی دیگری را هم همراه داشته باشد .

^۱Intgrate digital network

^۲Intergeated Service Digital Network

طرح و مفهوم ISDN برای ارتباط دیتا

شبکه ISDN از نظر کاربر یک شبکه ISDN باند باریک می باشد (N-ISDN) که هدف اصلی آن مجتمع نمودن سرویسهای گوناگون مخابراتی بصورت جامع در یک شبکه می باشد. سابق بر این برای اجرای سرویسهای مختلف مانند، انتقال دیتا، مکالمات و غیره قاعدتا نیاز به شبکه های مجزای مخابراتی بود.

در حال حاضر زمان اجرای باند پهن B-ISDN فرارسیده و باید بعنوان یک شبکه جامع سرویس دهی باند پهن بکاربرده شود. باند پهنی قینازیرساخت مخابراتی (TC) و پردازش دیتا (DP) را کنار نخواهد گذاشت، بلکه آن را بصورت مطلوبی کامل خواهد نمود (حفظ سرمایه).

ویژگی های N-ISDN:

دیجیتال نمودن شبکه های تلفنی آنالوگ شرط اجرای ISDN بود. بنابراین ISDN بدنال دیجیتال شدن شبکه های آنالوگ بوجود آمده است. همانند شبکه های تلفنی آنالوگ در ISDN همچنین سوئیچینگ مداری اجرا می گردد. در ISDN یک ارتباط انتها به انتهای فیزیکی (ارتباط ISDN) در صورت لزوم بین دو ترمینال تشکیل می گردد. بدین طریق در واقع یک خط فیزیکی بین ترمینالهای مرتبط به یکدیگر ایجاد می گردد. این خط به هر یک از مراکز ISDN واقع در مسیر ارتباطی متصل می باشد و در طول مسیر ارتباط بطور ثابت به ترمینالهای مرتبته اختصاص داده می شود. علاوه بر این، در حین یک ارتباط ISDN موجود، اطلاعات کنترلی (سیگنالینگ) مربوط به ارتباط بین ترمینالهای مرتبته بطور موازی (همزمان) ارسال می گردند. اطلاعات کنترلی را بطور کلی سیگنالینگ می نامند.

هیچ ارتباط انتها به انتهایی بمنظور سیگنالینگ بین ترمینالهای مرتبته ایجاد نمی گردد، بلکه سیگنالینگ به صورت پیام های سازمان یافته براساس قاعده ارسال بسته ای (forward&Store) از

طریق ISDN ارسال می گردد . سیگنالینگ بین ترمینالها و مراکز تلفن محلی ISDN از طریق کانال D و سیگنالینگ بین مراکز تلفن ISDN از طریق کانالهای سیگنالینگ مرکزی انجام می گردد .

از آنجائی که اطلاعات (دیتا) در مراکز تلفن ISDN با فر نمی شوند ، لذا مدت زمانی دسترسی یک ارتباط ISDN مبنای محاسبه هزینه شارژ ارسال بدست آمده می باشد . بنابراین هزینه ارسال در ISDN وابسته به زمان می باشد . از اینرو ISDN خصوصا برای ارسال فایل بسیار مناسب می باشد ، ISDN بعنوان شبکه ای برای ارتباط دیتا دارای سود و زیان خاصی می باشد .

مضرات :

- هر دو ترمینال دیتا درگیر در ارتباط باید با نرخ بیت یکسانی ارسال و دریافت نمایند .
- در صورت عدم استفاده از مالتیپلکسر ، فقط یک رابطه ارتباطی برای هر ارتباط ISDN امکان پذیر می باشد .
- هنگام خرابی یک ارتباط ISDN ، ارتباط دیتا قطع می گردد .

مزایا :

- از طریق ISDN یک ارتباط شفاف انتها به انتها ایجاد می گردد . (یعنی کلیه فرمت های مختلف دیتا می توانند ارسال گردند)
- از طرف ISDN درخصوص پروتکل ارتباطی بکار برده شده چیزی اضافه نمی گردد (شفافیت پروتکل)
- درواقع انتظار می رود که زمان جریان سیگنال روی یک ارتباط ISDN ثابت باشد.

Dsl چیست؟

^۱DSL یک فناوری مخابراتی است که اولین بار حدود سال ۱۹۹۵ در آمریکا طراحی و استفاده شد، با استفاده از این فناوری با بهره گیری از خطوط تلفن، بستری برای انتقال اطلاعات با سرعت بالا برای کاربران ایجاد می شود.

در این فناوری تجهیزاتی در مرکز تلفن نصب می شود تا برای هر کاربر فرکانس های مربوط به دیتا و صوت از هم جدا شوند و به این ترتیب با استفاده از یک خط تلفن امکان ارتباط همزمان صوت دیتا وجود خواهد داشت در فناوری DSL طول سیم، سرعت تبادل اطلاعات را تحت تأثیر قرار می دهد و فاصله مشترک تا مرکز تلفن نباید بیش از ۵ کیلومتر باشد.

البته فاصله ایده آل ۲ کیلومتر است که در این صورت کاربر با استفاده از ADSL می تواند تا ۸ Mbps اطلاعات دریافت و اگر بخواهید به اینترنت وصل شوید باید از طریق مودم معمولی، یا شبکه محلی LAN محل کارتان یا مودم کابلی و یانهایتا از طریق ^۲DSL این کار را انجام دهید.

این نوع اتصال که به تازگی در تهران راه اندازی شده است، در کانادا بعنوان یکی از انتخابهای بالا پیش روی مصرف کنندگان اینترنت قرار دارد. اما DSL چیست و کارکرد آن به زبان ساده چگونه است. DSL یک اتصال فوق سریع اینترنت میباشد که از همان سیم های تلفن معمولی سود میجوید و فوایدی به شرح زیر دارد ۱۰ Mbps: ارسال کند اما اگر این فاصله به ۵ کیلومتر برسد، سرعت نصف می شود. به طور کلی DSL به چند دسته ADSL، SDSL، HDSL، RADSL، VDSL تقسیم می شود ^۳ADSL به معنای سیستم DSL نامتقارن است که به علت یکسان نبودن سرعت ارسال و دریافت اطلاعات به این نام خوانده می شود.

• اتصال اینترنت و تماس تلفنی در یک زمان برقرار است.

^۱Digital Sub Scriber Line

^۲Digital Subscriber Line

^۳asymmetrical Digitul Subscriber Line

• سرعت از مودم معمولی بسیار بالاتر است (۱/۵ مگا بیت در ثانیه در برابر ۵۶ کیلو بیت در ثانیه)

• با توجه به آنکه از سیم تلفن استفاده میکند نیاز به سیم کشی جدید ندارد.

اما DSL دارای سه نقطه ضعف است :

- هرچه به دفتر مرکزی DSL نزدیکتر باشید، سرویس بهتر است .
- دریافت دیتا سریعتر از ارسال آن است .
- سرویس در همه جا عرضه نمیشود .

چون سیم تلفن ظرفیت انتقالی بیش از فرکانسهای صدای انسان را دارد و صدای انسان دارای فرکانس بین ۵ تا ۳۴۰۰ هرتز است، بقیه ظرفیت انتقال سیم ها که تا چند میلیون هرتز میرسد، خالی میماند DSL. از این ظرفیت خالی بصورت دیجیتالی برای انتقال دیتا استفاده میکند .

DSL نامتقارن یا ADSL

اکثر کاربران از اتصال نوع ADSL برای دسترسی به اینترنت استفاده میکنند. فرض بر اینست که یوزرها حجم اطلاعات دریافتی بیشتری دارند تا ارسال و با این فرض، فرکانس های ارسال و دریافت تنظیم میشوند. مبنای اینطور است که سرعت دریافت دیتا از اینترنت ۳ تا ۴ برابر سریعتر از سرعت ارسال به اینترنت است .

روش های دیگر DSL به شرح زیر هستند :

- VDSL^۱ که سریع است اما در فواصل کوتاه کار میکند .

^۱Very high bit-rate DSL

- ^۱SDSL که سرعت ارسال و دریافت یکسانی دارد اما نمیتوانید همزمان از تلفن استفاده کنید و معمولاً برای دفاتر اداری کوچک کاربرد دارد .
- ^۲RADSL که زیر گروه ADSL است اما این مودم است که بسته به طول و کیفیت خط ، سرعت اتصال را تنظیم میکند .

محدودیت فاصله

اینکه کیفیت اتصال شما به اینترنت چگونه است، بستگی به فاصله شما تا دفتر مرکزی شرکت عرضه کننده سرویس ADSL دارد ADSL. تکنولوژی حساس به فاصله است که هرچند فاصله اتصال زیاد شود کیفیت سیگنال افت میکند و سرعت کند میگردد. حد این فاصله ۵۴۶۰ متر و یا ۱۸۰۰۰ فوت است که در کمتر از آن هنوز کیفیت قابل قبول میباشد. اگر خیلی به دفتر مرکزی نزدیک باشید ممکن است سرعتتان به ۸ مگا بیت در ثانیه نیز برسد. سرعت قابل قبول امروزی معادل ۱/۵ مگابیت در ثانیه است .

وسایل DSL

ADSL دو قطعه دارد که یکی نزد شما و دیگری در دفتر سرویس دهنده و یا شرکت تلفن نصب میشود. آنکه نزد شماست بنام Transceiver است و آنکه شرکت دارد به نام DSLAM^۳ است. اکثر شما به Transceiver ، مودم DSL میگویید. این نقطه ای است که کامپیوتر از آنجا به خط DSL وصل میشود. این مودم میتواند از چندین روش به کامپیوتر شما وصل شود که معمولی ترین آن اتصال USB یا اترنت ۱۰ base-T است. نمونه های خانگی این دستگاه ها فقط یک ترانسپور ساده هستند اما برای شرکتها میتوانند حاوی روتر شبکه، سویچ شبکه و یا امکانات دیگری برای شبکه باشند .

^۱Symmetric DSL

^۲Rate-adaptive DSL

^۳DSL Access Multiplexer

در مورد DSLAM که در طرف سرویس دهنده نصب میشود فقط به ذکر این نکته بسنده میکنم که ADSL برای هر یوزر یک اتصال اختصاصی از یوزر به دستگاه DSLAM برقرار میکند که فرق بزرگ آن با مودم های کابلی است که در آن ها یک حلقه شبکه های بین یوزرها به اشتراک گذاشته میشود و با ورود هر یوزر به این حلقه، کیفیت ارتباطات میکند

محبوبترین تکنولوژی باند پهن در جهان یعنی DSL بیش از ۳۰ میلیون مشترک تا پایان بهار ۲۰۰۴ به کاربران اینترنت افزوده و تعداد بهره‌مندان جهانی رابه ۷۸ میلیون در کل رسانده که این رشد بیش از دو برابر دیگر روش های متکی بر پهنایباند بوده است. تکنولوژی DSL یکی از انواع انتقال پرسرعت بوده است که با تلفن معمولی شما را قادر می‌سازد تا ضمن دسترسی به اینترنت پرسرعت از امکان دریافت صدا و تصویر با کیفیت بالا استفاده کنید. نوع دیگر همین تکنولوژی ADSL است که یکی از انواع فن آوری DSL است، که در این روش سیستمهای سخت افزاری ویژه (DSLAM) باید در پستهای مراکز مخابراتی نصب گردند. پس از نصب این سیستمها و با استفاده از کابل های تلفن، سرویس قابل راه اندازی می‌شود، بدین لحاظ از نظر هزینه برای دولت و مصرف کننده بسیار قابل قبول است. زیرا هزینه کابل کشی مجدد به هیچیک از طرفین تحمیل نمی‌شود. مصرف کننده این سرویس تنها به یک مودم ADSL احتیاج دارد.

قابلیت DSL

با استفاده از زوج سیمهای مخابرات برای تلفن خانگی ما تنها از یک پانصدم امکانات بالقوه این سیمها استفاده می‌کنیم و مابقی بلااستفاده می‌ماند ADSL. پهنای باند ۱/۸ مگاهرتزی خطوط مسی را به کانال های ۴ کیلوهرتزی تقسیم می‌کند و آخرین کانال را جهت ارسال صدا و فاکس معمولی تخصیص می‌دهد و ۲۵۶ کانال دیگر را برای انتقال دو طرفه اطلاعات استفاده می‌کند؛ به این ترتیب که ۶۴ کانال رابرای خط ارسال اطلاعات و ۱۲۸ کانال دیگر را جهت دریافت اطلاعات استفاده می‌کند. در بهترین حالت اگر ۱۹۲ کانال ۴ کیلوهرتزی موجود را استفاده کند، در تئوری سرعت باید به حدود ۹ مگابیت در ثانیه برسد.

در حال حاضر سرعت خطوط ADSL در بهترین حالت ۲ مگابیت در ثانیه می باشد. در عمل، این خطوط اطلاعات زنجیره وار دیجیتالی را به اطلاعات پارالل در دو سر انتقال اطلاع تبدیل می کنند. دقیقاً مشابه کاری که در مودمهای خطوط عادی انجام می شود .

سرعت انتقال اطلاعات در محدوده ذکر شده به عواملی از جمله فاصله ارتباطی و نوع سیم استفاده شده بستگی دارد. حال با استفاده از سخت افزارهایی که بتوانند داده ها را فشرده سازی، ارسال و دریافت نمایند می توانیم این قابلیت بلااستفاده را هم به کار بگیریم. یکی از این سخت افزارها در پست مخابرات نصب و دیگری در محل استفاده کننده نصب می شود. ارتباط از طریق سیم تلفن قبلی شما برقرار می شود بدون اینکه اختلالی در ارتباطات تلفنی بوجود آید. حالا به شرط این که مودم همیشه به خط وصل و روشن باشد ارتباط شما با اینترنت همیشه برقرار خواهد بود درعین حال اینکار برای مکالمات تلفنی مشکلی پیش نمی آورد.

برتری های فنی DSL

- -اتصال دائم و بی وقفه و مطمئن به شبکه مخابرات و شبکه جهانی اینترنت برقرار است.
- -از حداقل تجهیزات در محل کار یا خانه استفاده می شود.
- -سرعت سیستم به قدری بالا خواهد بود که سرویس های دیگر اینترنت نیز مانند صوت و تصویر متحرک، برای استفاده در دسترس خواهند بود
- -نیاز به کابل کشی مجدد نیست.
- -می توان بیش از یک نفر از هر اتصال استفاده نمود.
- -در شرایط ایده آل (نبود نویز بر روی سیمها، فاصله کم تا مرکز مخابراتی) حداکثر سرعت دریافت ۸ Mbps و سرعت ارسال ۱ Mbps خواهد بود.
- -اداره و کنترل کارهای چنین اتصالی نیز به سادگی همان کاری است که با تلفن منزل انجام می دهیم.
- -به علت سرعت بالا (دریافت و ارسال) امکان برقراری جلسات و سمینارهای مجازی با سهولت میسر است.

- باز شدن راه برای انجام پروژه‌هایی مانند دولت الکترونیک، پزشکی الکترونیک، آموزش سمعی بصری الکترونیک، شبکه اختصاصی الکترونیک و مجموعه وسیعی از دیگر کاربردهای الکترونیک

- -مسافت ۱/۸ کیلومتری تحت پوشش شبکه برای تامین سرعت ۸ Mbps
- -ارائه انواع سرویس‌های مختلف براساس بستر شبکه DSL مانند VODSL ، Video on demand ، VOIP.

DSL چگونه کار میکند ؟

به محیطی که داده ها از آن انتقال می یابند مدیا یا رسانه گفته می شود. زوج سیم، کابل‌های کواکسیال (مثل کابل آنتن تلویزیون)، موج برها (لوله هایی فلزی با سطح مقطع مستطیل یا دایره شکل)، هوا و فیبرهای نوری مهمترین رسانه های مخابراتی هستند. برای هر رسانه مخابراتی پارامترهایی به نام کرانه بالایی و پائینی فرکانس تعریف می شود و منظور از آنها حداکثر و حداقل فرکانسی است که آن رسانه می تواند با کیفیت مطلوب از خود عبور دهد. به اختلاف این دو فرکانس پهنای باند یا Band Width می گویند. زوج سیم که در سیستم تلفن شهری استفاده می شود ضعیفترین رسانه مخابراتی از این نظر می باشد و محدوده عبور فرکانسی آن از صفر تا حدود ۲ مگاهرتز می باشد. اما در سیستمهای تلفن ثابت شهری (PSTN) فقط از ۴ کیلو هرتز این محدود برای عبور صدا استفاده می شود و بقیه باند فرکانسی آن آزاد میماند که در واقع استفاده از این باند فرکانسی بلااستفاده ایده اصلی و اولیه ساخت و استفاده از DSL می باشد. در روش اتصال عادی Diap-Up از همان ۴KHz پهنای باندی که در مکالمات صوتی عادی بکاربرده میشود جهت انتقال داده استفاده می شود و با استفاده از روشهای پیچیده مدولاسیون دیجیتال و فشرده سازی اطلاعات، میتوان حداکثر به سرعت ۵۶ کیلو بیت در ثانیه رسید که در عصر انفجار اطلاعات سرعتی لاکپشتی است. حالا اگر باند فرکانسی ما از ۴ KHz به ۲ MHz افزایش پیدا کند! یعنی تقریباً ۵۰۰ برابر خواهد شد، واضح است که سرعت انتقال دادهایمان به شدت افزایش خواهد یافت. برای ADSL در عمل معمولاً باند فرکانسی ۳۰ KHz تا ۱۳۸ KHz برای فرستادن

اطلاعات و باند فرکانسی ۱۳۸ KHz تا ۱/۸ Mhz برای گرفتن اطلاعات استفاده می شود. در این صورت با توجه به روشهای مدولاسیون مورد استفاده می توان به پهنای باند دیجیتال ای تا ۸Mbps دست یافت که معمولا برای بدست آوردن ضریب کیفیت سرویس دهی (QoS) بهتر عملا سرعتی حدود ۱/۵ تا ۲ مگابیت در ثانیه در اختیار کاربران حرفه ای قرار میگیرد.

تجزیه سیگنال :

اغلب منازل و کاربران تجاری کوچک به يك خط DSL نامتقارن (ADSL) متصل میشوند . فرکانسهای موجود در يك خط را براساس این فرض که اغلب کاربران اینترنت اطلاعات بسیار بیشتری را نسبت به آنچه که ارسال میکنند از اینترنت دریافت مینمایند، تقسیم میکنند. دو استاندارد تقریبا " ناسازگار در مورد تکنولوژی ADSL وجود دارد. استاندارد رسمی ANSI که روش DMT را برای تکنولوژی DSL پایه گذاری کرده که البته اغلب تجهیزات ADSL امروزی از این روش استفاده میکنند و استاندارد قدیمی تر بنام Carrie less Amplitude/Phase یا سیستم SCAP که قبلا" از آن استفاده میگردید .

در سیستم ADSL به منظور استفاده بهینه از پهنای باند ۱/۱ مگاهرتزی خطوط مسی، آن را به ۲۵۷ کانال ۴ کیلوهرتزی تقسیم مینمایند. از آنجا که برای انتقال صوت (تلفن) تنها ۴ کیلوهرتز پهنای باند کافی است لذا کانال آخر را برای انتقال فاکس و تلفن (صوت) استفاده مینمایند و ۲۵۶ کانال دیگر را بصورت ۶۴ کانال برای ارسال اطلاعات و ۱۲۸ کانال برای دریافت اطلاعات (و مابقی ۶۴ کانال برای اطلاعات کنترلی) تقسیم بندی مینمایند. بطوریکه در بهترین وضعیت (با در نظر گرفتن ۱۹۲ کانال (۴ khz به سرعتی معادل) ۹ mbps مگابیت بر ثانیه) میرسیم که البته حداکثر سرعت مورد استفاده در ADSL ها معادل ۳/۲ mbps میباشد .

تجهیزات: DSL

مودم DSL یا ATU-R

اغلب مشترکین خانگی به منظور دریافت اطلاعات از اینترنت از این مودم بهره میگیرند. شرکتی که سرویس DSL را ارائه میدهد معمولاً "مودم را بعنوان بخشی از نیازهای نصب سیستم عرضه مینماید .

Splitter

همانطوریکه ذکر شد صوت و data به طور همزمان روی خطوط مسی در تکنولوژی DSL فرستاده میشود. به منظور جدا کردن صوت و data در طرف مشترک از splitter بهره میگیرند تا data را بسمت کامپیوتر و صوت (تلفن و فاکس) رابه سمت تجهیزات مربوطه هدایت کند .

DSLAM

DSLAM، خطوط ارتباطی جهت یافته از سوی تعداد زیادی از مشترکین را دریافت نموده و آنها را روی يك خط ارتباطی واحد با ظرفیت بالا به اینترنت منتقل میکند .

DSLAM قادر به پشتیبانی چندین نوع DSL در يك مرکز تلفن واحد و تعداد گوناگونی از پروتکلها و روشهای مدولاسیون میباشد بعلاوه DSLAM میتواند امکاناتی همچون مسیریابی یا تخصیص آدرس دینامیکی IP نیز برای مشترکین فراهم کند. در واقع DSLAM را میتوان دلیل اصلی تفاوت بین سرویس دهی از طریق ADSL و از طریق مودم کابلی به حساب آورد .

معایب: DSL

عیب اصلی سیستم DSL در این است که میزان بهره گیری شما از DSL مبتنی بر فاصله ایست که شما از سرویس ADSL دارید ADSL. يك سرویس حساس به فاصله میباشد همچنانکه طول

ارتباط افزایش می یابد کیفیت سیگنال کاهش یافته و سرعت ارتباط کم میشود. حداکثر فاصله جهت سرویس دهی توسط سیستم ADSL میتواند به ۵۴۶۰ متر برسد. تکنولوژی ADSL میتواند حداکثر سرعت ۸ Mbps downstream در فاصله حدود ۱۸۲۰ متر و سرعت upstream تا ۶۴۰ kbps را در اختیار کاربران قرار دهد. کهنالبنه در عمل حداکثر سرعت مورد استفاده در ADSL ها ۲/۳ mbps میباشد. اما چرا فاصله يك محدودیت برای سیستم DSL به شمار میرود در حالیکه این محدودیت برای مکالمات تلفنی وجود ندارد؟ جواب این سؤال در تقویت کننده های کوچکی به نام Loading coils میباشد که شرکت تلفن برای تقویت سیگنالهای صوتی استفاده میکند. که این تقویت کننده ها با سیگنالهای ADSL سازگاری ندارند. البته پارامترهای دیگری همچون Bridge Taps و کابلهای فیبرنوری نیز میتوانند تاثیر منفی روی تکنولوژی ADSL بگذارند .

آینده DSL:

روزانه ۲۰٫۰۰۰ نفر به علاقه مندان ارتباط از طریق DSL در سطح جهان افزوده میشود و این به نوبه خود رقابت این تکنولوژی را با تکنولوژی هایی همچون مودم های کابلی و اینترنت ماهواره ای به خوبی نشان میدهد. برطبق تحقیقات انجام گرفته از طرف شرکت IDC تا سال ۲۰۰۳ تعداد مشترکین خانگی استفاده کننده از مودم کابلی فراتر از ۸۹۸۰۰۰۰ خواهد بود در حالیکه DSL در سال ۲۰۰۳ بیش از ۹۳۰۰۰۰۰ مشترک خانگی دارد .

در سالهای اخیر کشور کره تنها با داشتن ۵۵ میلیون جمعیت بشتین مصرف کننده DSL در جهان میباشد به نحوی که سؤال به بهشت DSL مبدل شده است و شرکتهای فعال در زمینه شبکه در کره پیشرو این تکنولوژی در جهان میباشند.

مقایسه انواع DSLها:**• ADSL (Asymmetric DSL):**

این روش نامتقارن نامیده شده و دلیل آن هم تفاوت سرعت دریافت و ارسال است. بیشتر مناسب خانه ها و ادارات کوچک است. و بیشتر مناسب افرادی که دانلود بیشتری دارند. شما می توانید تا ۶/۱ مگابیت بر ثانیه دریافت و ۶۴۰ کیلوبیت بر ثانیه ارسال داشته باشید.

• CDSL (Consumer Digital Subscriber Line):

یا DSL مصرف کننده نوعی دیگر از این تکنولوژی است. از ADSL سرعت کمتری دارد و توانایی دریافت تا ۱ مگابیت بر ثانیه را دارد و همچنین سرعت ارسال بسیار کمتری به نسبت ADSL دارد.

• HDSL (High bit-rate DSL):

سرعت دریافت و ارسال اطلاعات یکسان است. در این روش تا ۱/۵۴۴ مگابیت بر ثانیه بر روی خطوط دابل دریافت و ۲/۰۴۸ مگابیت بر ثانیه ارسال امکان پذیر است.

• ISDL (ISDN DSL):

این روش در اختیار کاربران استفاده کننده از ISDN است. ISDL در مقایسه با سایر روش های DSL دارای پایین ترین سرعت است. سرعت این خطوط ۱۴۴ کیلوبیت بر ثانیه است.

• MSDSL (Multirate Symmetric DSL):

در این روش سرعت ارسال و دریافت اطلاعات یکسان است. نرخ سرعت انتقال اطلاعات توسط مرکز ارائه دهنده سرویس DSL، تنظیم می گردد.

• (Rate Adaptive) RADSL :

در این روش این امکان وجود دارد که سرعت برقراری ارتباط با توجه به مسافت و کیفیت خط تغییر کند.

• (Symmetric DSL) SDLS :

DLS با خطوط متقارن است. سرعت ارسال و دریافت یکسان است و بر خلاف HDSL فقط به یک خط نیاز خواهد بود.

• UDSL :

در حقیقت همان HDSL است ولی با خطوطی یکطرفه. این نوع از DSL توسط شرکت های اروپایی پیشنهاد شد.

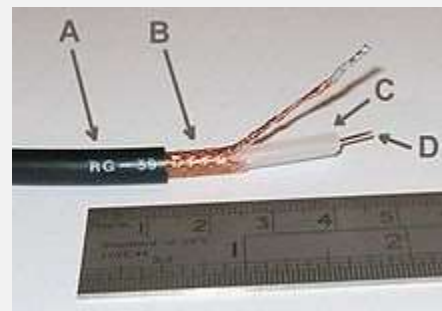
• (Very high bit-rate) VDSL :

این روش نامتقارن است و در مسافت های کوتاه به همراه خطوط مسی تلفن استفاده می گردد.

• (Voice-over DSL)VoDSL :

یک نوع خاص از IP تلفنی است . در این روش چند خط ترکیب و به یک خط تلفن تبدیل تبدیل می شوند.

تلویزیون کابلی



کابل کواکسیال اغلب برای انتقال امواج در سامانه تلویزیونی کابلی به منازل استفاده می شود. پایانه RG-59 از یک کتاب نظامی باستانی به نام رهنمای رادیو می آید، که این عدد شماره صفحه کتاب راهنما است که در این مورد توضیحاتی داده است. (RG مخفف کلمه Radio Guide است به معنی راهنمای رادیو)

تلویزیون کابلی یک نوع سامانه تلویزیونی است که در آن مشترکین سیگنال های رادیویی را از طریق فیبر نوری و کابل کواکسیال دریافت می کنند، که جزو مالکیت مشترک به حساب می آید که شباهت زیادی به روش هوایی دارد. در روش قدیمی تصاویر از طریق امواج رادیویی انتقال می یابند که در آن تلویزیون نیاز به یک آنتن دارد. و به روش هایی از جمله برنامه های رادیویی اف ام، اینترنت پرسرعت و تلفنی شباهت زیادی دارد که گاهی اوقات این روش ها نیز ارائه می شوند و تفاوت اصلی بین رادیویی فرکانسی و ارتباط نوری در مالکیت آن ها است.

در زبان انگلیسی به اختصار از CATV نام می برند که به معنی تلویزیون کابلی به کار می رود ولی در اصل به معنی تلویزیون آنتی مشترک می باشد که از نام شبکه کابلی گرفته شده است که در سال ۱۹۴۸ بنیان گذاری شده است که در روش هوایی گیرندگی به فاصله فرستنده تا گیرنده محدود بود و حتی به پستی و بلندی نیز محدود می شد که مجبور بودند از شبکه کابلی برای انتقال امواج به منازل افراد استفاده کنند. در اصل قدمت تلویزیون کابلی از قدمت رادیو نیز بیشتر است که گفته

می شود در برخی از شهرهای اروپایی که قدمت آن به سال های قبل از ۱۹۲۴ می رسند استفاده می کردند.

این روش پیش پا افتاده در آمریکای شمالی، اروپا، استرالیا و شرق آسیا استفاده می شده اگر چه در حاضر در خیلی از کشورها استفاده می شود که بیشتر در آمریکای جنوبی و خاورمیانه استفاده می شود. تلویزیون کابلی موفقیت های کوچکی نیز در آفریقا داشته است. هر چند در مناطق عامه پسند تأثیر چندانی ندارد و در عوض از سامانه هایی بر مبنای شبکه های بی سیم و امواج ماکروویو استفاده می شود.

درس ۲

SLIP and PPP

(SLIP) (PPP) نیز از لایه پیوند داده هستند ، اما تفاوت زیادی با اترنت، توکن رینگ، (FDDI) دارند. SLIP و PPP، که بخشی از مجموعه پروتکل IP / TCP هستند برای شبکه های محلی اصلا تعریف نشده اند در عوض وظیفه اتصال یک سیستم را به دیگری با استفاده از یک اتصال اختصاص داده شده بر عهده دارند، مانند یک خط تلفن. به همین دلیل، SLIP و PPP پروتکل های end-to-end نامیده می شوند. و از آنجا که رسانه مشترک نیست هیچگونه نیازی به مکانیزم mac نمیباشد. به عنوان یک نتیجه، این پروتکل ها به مراتب ساده تر از پروتکل های اترنت و توکن رینگ. هستند و SLIP و PPP مشخصات لایه فیزیکی را شامل نمی شود، آنها به شدت با لایه پیوند داده درگیر هستند.

مبادله اطلاعات بر روی اینترنت با استفاده از پروتکل TCP/IP انجام می شود . با این که پروتکل فوق یک راه حل مناسب در شبکه های محلی و جهانی را ارائه می نماید ، ولی به منظور ارتباطات از نوع Dial-up طراحی نشده است .

ارتباط Dail-up ، یک لینک نقطه به نقطه (Point-To-Point) با استفاده از تلفن است . در چنین مواردی یک روتر و یا سرویس دهنده، نقطه ارتباطی شما به شبکه با استفاده از یک مودم خواهد بود. سرویس دهنده دستیابی راه دور موجود در مراکز ISP ، مسئولیت ایجاد یک ارتباط نقطه به نقطه با سریس گیرندگان Dial-up را برعهده دارد . در ارتباطات فوق ، می بایست از امکانات خاصی به منظور ارسال IP و سایر پروتکل ها استفاده گردد . با توجه به این که لینک ایجاد شده بین دو نقطه برقرار می گردد ، آدرس دهی مشکل خاصی را نخواهد داشت.

SLIP¹ و PPP² پروتکل هائی می باشند که امکان استفاده از TCP/IP بر روی کابل های سریال نظیر خطوط تلفن را فراهم می نمایند (SLIP و PPP دو روش متفاوت به منظور اتصال به اینترنت). با استفاده از پروتکل های فوق ، کاربران می توانند توسط یک کامپیوتر و مودم به اینترنت متصل شوند . از پروتکل SLIP در ابتدا در سیستم عامل یونیکس استفاده می گردید ولی امروزه تعداد بیشتری از سیستم های عامل نظیر لینوکس و ویندوز نیز از آن حمایت می نمایند . در حال حاضر استفاده از پروتکل SLIP نسبت به PPP به مراتب کمتر است .

PPP نسبت به SLIP دارای مزایای متعددی است :

- امکان مبادله اطلاعات به صورت همزمان و غیر همزمان . در پروتکل SLIP صرفاً امکان مبادله اطلاعات به صورت همزمان وجود دارد .

¹Serial Line Internet Protocol
²Point-To-Point

- ارائه امکانات لازم به منظور تصحیح خطاء . تصحیح خطاء در پروتکل SLIP عموماً مبتنی بر سخت افزار استفاده شده به منظور برقراری ارتباط (نظیر مودم) و یا استفاده از قابلیت های پروتکل TCP/IP است .
- ارائه امکانات لازم برای فشرده سازی . پروتکل SLIP در اغلب بخش های آن چنین ویژگی را دارا نمی باشد . در این رابطه نسخه هائی از SLIP به منظور فشرده سازی نظیر Compressed SLIP و یا CSLIP طراحی شده است ولی متداول نمی باشند .
- ارائه امکانات لازم به منظور نسبت دهی آدرس ها به صورت پویا و اتوماتیک . پروتکل SLIP می بایست به صورت دستی پیکربندی گردد (در زمان Dial-up و یا تنظیم اولیه Session) .
- امکان استفاده از چندین پروتکل بر روی لینک های PPP وجود دارد (نظیر IP و یا IPX) . در پروتکل SLIP صرفاً امکان استفاده از پروتکل IP وجود خواهد داشت .

وجه اشتراک پروتکل های PPP و SLIP

- هر دو پروتکل قابل روتینگ نمی باشند . با توجه به نوع ارتباط ایجاد شده که به صورت نقطه به نقطه است و صرفاً دو نقطه در ارتباط درگیر می شوند ، ضرورتی به استفاده از روتینگ وجود نخواهد داشت .
- هر دو پروتکل قادر به کپسوله نمودن سایر پروتکل هائی می باشند که در ادامه برای روتر و سایر دستگاه ها ارسال می گردند . در مقصد، اطلاعات مربوط به پروتکل های SLIP و یا PPP برداشته شده و پروتکل های ارسالی توسط لینک سریال نظیر IP ، در طول شبکه فرستاده می گردد .

یک کامپیوتر با استفاده از یک ارتباط SLIP و یا PPP قادر به شبیه سازی یک اتصال مستقیم به اینترنت است . در این رابطه به امکانات زیر نیاز می باشد :

- یک کامپیوتر و مودم
- یک account از نوع SLIP و یا PPP از ISP مربوطه
- نصب نرم افزارهای TCP/IP و SLIP/PPP بر روی کامپیوتر کاربر (نرم افزارهای فوق معمولاً در زمان استقرار سیستم عامل بر روی کامپیوتر نصب خواهند شد).
- یک آدرس IP . آدرس فوق ممکن است به صورت دائم و یا پویا (استفاده از سرویس دهنده DHCP) به کامپیوتر کاربر نسبت داده شود.

نحوه عملکرد یک اتصال SLIP و یا PPP

- مودم موجود بر روی کامپیوتر اقدام به شماره گیری یک کامپیوتر از راه دور در یک ISP می نماید .
- نرم افزار SLIP/PPP درخواست یک اتصال SLIP/PPP را می نماید .
- پس از برقراری ارتباط ، ISP مربوطه به کامپیوتر کاربر یک آدرس IP را اختصاص خواهد داد (در مواردی که از یک سرویس دهنده DHCP استفاده می گردد) .
- نرم افزار TCP/IP بر روی کامپیوتر کاربر ، کنترل و مدیریت مبادله اطلاعات بین کامپیوتر کاربر و اینترنت را برعهده خواهد گرفت .

درس ۳

تکنولوژی های WAN

ATM^۱ چیست؟

حالت انتقال ناهمزمان، نوعی تکنولوژی است که قابلیت انتقال بلادرنگ دارد، صدا، تصویر و ترافیک رله قابی را در شبکه های کامپوتری فراهم می کند. واحد اصلی انتقال در این روش بسته ای ۵۳ بیتی با طول ثابت است که از ۵ بایت جهت اعمال کنترلی و از ۴۸ بایت باقیمانده برای انتقال داده استفاده می شود. لایه ای که با عنوان میانجی بین لایه های سطح بالا و پایین عمل کرده و انواع مختلف داده (از جمله صدا، تصویر و قاب داده ها) را به داده های ۴۸ بیتی مورد نیاز ATM تبدیل می کند ATM Adaptation LAYER یا AAL یک استاندارد برای شبکه های سریع است که یک قالب برای ایجاد شبکه های سریع با استفاده از پروتکل های مخابراتی سریع و متنوع به عنوان پروتکل لایه فیزیکی ارائه می کند. این قالب بسیار انعطاف پذیر و قوی بوده و قابلیت ارائه سرویس های متنوعی از لحاظ کیفیت سرویس را دارا می باشد این قالب مبتنی بر ارسال اطلاعات بصورت سلول های بسیار کوچک اطلاعاتی بسته های کوچک با ابعاد ثابت بر روی مسیر های داده ای از قبل ایجاد شده (Connection Oriented) می باشد در هسته شبکه موبایل کاربرد دارد.

FDDI^۲ چیست؟

تکنولوژی یک شبکه با سرعت ۱۰۰ مگابایت در ثانیه است که برای ارتباط از فیبر نوری استفاده می کند. در این تکنولوژی به جای فیبر نوری از کابل مسی نیز می توان استفاده کرد ولی در صورت استفاده از کابل مسی طول کابل کمتر می شود. FDDI به عنوان BACKBONE در محل هایی که تعداد زیادی کامپوتر در آن قرار دارد، استفاده می شود. از جمله این محیطها میتوان به دانشگاه ها اشاره کرد. در می توان ۵۰۰ گره را در مسافت ۱۰۰ کیلومتر به یکدیگر متصل کرد.

^۱Asynchronous Transfer Mode^۲Fiber Distributed Data Interface

توپولوژی فیزیکی این شبکه حلقوی است . نحوه به وجود آمدن این حلقه به این صورت است که یک حلقه ۱۰۰ کیلومتری از فیبر ساخته می شود و در هر ۲ کیلومتر یک تقویت کننده قرار میگیرد. برای جلوگیری از اختلالاتی که در اثر قطع شدن فیبر نوری به وجود می آید از دو حلقه فیبر نوری در کنار هم استفاده می شود تا در صورتی که یکی از رشته ها قطع شود رشته دوم وارد عمل شده و جایگزین رشته اول شود.

Frame Relay چیست؟

در زمینه شبکه های کامپیوتری، frame relay شامل تکنیک انتقالی کارآمدی می باشد و قابل استفاده برای ارسال اطلاعات دیجیتال با سرعت و با هزینه کمتر در چند frome از یک یا چند مقصد به یک یا چند نقطه پایانی می باشد. معمولاً فراهم کننده های شبکه frame relay را برای انتقال صدا و داده ها به صورت تکنیک ارسال فریم بین شبکه های LAN و WAN به کار می برند. هر کار بر پایانی یک خط شخصی از گره frame relay به دست می آورد. از سال ۲۰۰۶ شبکه بومی بر پایه IP شروع به جانشین گزیدن برای frame relay هستند. با ظهور MPLS، VPN و سرویس های پهنای باند اختصاصی همانند DSL پایانی کاری در انتظار پروتکل frame relay و ارسال داده ها به صورت فریم خواهد بود. ولی مناطق روستایی باقی خواهند ماند که از تکنولوژی DSL و سرویس مودم محروم باشد و در این زمان است که قیمتی ترین نوع اتصال خط frame relay ۱۲۸ KB باقی خواهد ماند. بنابراین برای مثال امکان دارد یک زنجیره جزئی از frame relay برای اتصال مناطق روستایی به WAN استفاده شود. روش رله کردن فریم در اثنای دهه ۹۰ میلادی به نوان روشی سریع تر در سویچینگ پاکتی که دارای مزایای جهت اطمینان سرویس های ذاتی شبکه های مدرن داشت توسعه یافت frame relay به ترمینالهای انتهایی اجازه آشکار سازی و تصحیح خط را می دهد بنابراین نیازی به ذخیره و بافر کردن و پردازش تشخیص و تصحیح خط در هر گره نمی باشد این مسئله به میزان قابل ملاحظه ای قابلیت استفاده از دیتا با نرخ های بیت بالا را تا ۲Mps سیستم اروپایی و تا ۱/۵۴۴ Mps برای سیستم امریکایی افزایش می دهد.

SMDS چیست؟

که یک سرویس بدون اتصال برای تبادل اطلاعات در شبکه های LAN و WAN و MAN می باشد. اساس SMDS استاندارد DQDB ۸۰۲/۶ IEEE است که داده ها را به سلولهای کوچک جهت انتقال تبدیل می کند و می تواند جانشینی برای سرویس IP ETHERNET شود.

SMDS به کاربران اجازه می دهد که ارتباط داده ای خود را فراتر از پهنای ناحیه جغرافیای توسعه دهد و سرویس های که تا کنون وجود دارد به وسیله شرکت های مخابراتی ارائه شده است.

^۱Switched multimegabit data service

مزیت	گستره جغرافیایی	سرعت	نام تکنولوژی WAN
برای ارتباط از فیبر نوری و یا کابل مسی (کم شدن فاصله مجاز) استفاده می کند توپولوژی فیزیکی این شبکه حلقوی است	در محلهایی که تعداد زیادی کامپیوتر در آن قرار دارد استفاده می شود مثل دانشگاهها	۱۰۰Mbps	FDDI
تکنولوژی قابل اطمینان مثل ارتباطات ماهواره ای و در سطح شهر قابل اطمینان در فرکانس بالا امنیت تضمین شده ظرفیت بالا پهنای باند کاملا اختصاصی کاهش هزینه راه اندازی	در سطح شرح	۱۰Mbps تا ۶۴Kbps	ATM
ارسال داده ها به صورت فریم ارسال اطلاعات دیجیتال با سرعت و با هزینه کم در چند فریم برای مناطقی که از سرویس مودم محروم اند کاربرد دارد.	اتصال مناطق روستایی به شبکه WAN	سریعتر از ۶۴Kbps	Frame relay

فصل ۱۲

Network Security

امنیت بخشی از کار هر مدیر شبکه است، اعم از اطلاعات محرمانه ذخیره شده بر روی کامپیوتر که باید از آن محافظت شود و یا سیستم عامل و فایل های نرم افزار که باید از حذف شدن توسط کاربران محافظت شود. مکانیزم های مختلف برای تامین امنیت در یک شبکه نسبت به نیاز یک مدیر یا شخص وجود دارد. امنیت شبکه موضوع بسیار بزرگ و پیچیده است. در این فصل به بررسی برخی از ابزار و تکنیک های اساسی که شما می توانید با استفاده از آنها شبکه خود را از آسیب تصادفی یا عمدی محافظت کنید می پردازیم.

درس ۱

Firewall

فایروال چیست؟

فایروال وسیله ای است که کنترل دسترسی به یک شبکه را بنابر سیاست امنیتی شبکه تعریف می کند. علاوه بر آن از آنجایی که معمولا یک فایروال بر سر راه ورودی یک شبکه می نشیند لذا برای ترجمه آدرس شبکه نیز بکار گرفته می شود.

مشخصه های مهم یک فایروال قوی و مناسب جهت ایجاد یک شبکه امن عبارتند از:

۱- توانایی ثبت و اخطار: ثبت وقایع یکی از مشخصه های بسیار مهم یک فایروال به شمار می شود و به مدیران شبکه این امکان را می دهد که انجام حملات را کنترل کنند. همچنین مدیر شبکه می تواند با کمک اطلاعات ثبت شده به کنترل ترافیک ایجاد شده توسط کاربران مجاز بپردازد. در یک روال ثبت مناسب، مدیر می تواند براحتمی به بخشهای مهم از اطلاعات ثبت شده دسترسی پیدا کند. همچنین یک فایروال خوب باید بتواند علاوه بر ثبت وقایع، در شرایط بحرانی، مدیر شبکه را از وقایع مطلع کند و برای وی اخطار بفرستد.

۲- بازدید حجم بالایی از بسته های اطلاعات: یکی از تستهای یک فایروال، توانایی آن در بازدید حجم بالایی از بسته های اطلاعاتی بدون کاهش چشمگیر کارایی شبکه است. حجم داده ای که یک فایروال می تواند کنترل کند برای شبکه های مختلف متفاوت است اما یک فایروال قطعا نباید به گلوگاه شبکه تحت حفاظتش تبدیل شود. عوامل مختلفی در سرعت پردازش اطلاعات توسط فایروال نقش دارند. بیشترین محدودیتها از طرف سرعت پردازنده و بهینه سازی کد نرم افزار بر کارایی فایروال تحمیل می شوند. عامل محدودکننده دیگر می تواند کارتهای واسطی باشد که بر روی فایروال نصب می شوند. فایروالی که بعضی

کارها مانند صدور اخطار ، کنترل دسترسی مبنی بر URL و بررسی وقایع ثبت شده را به نرم افزارهای دیگر می سپارد از سرعت و کارایی بیشتر و بهتری برخوردار است.

۳- سادگی پیکربندی: سادگی پیکربندی شامل امکان راه اندازی سریع فایروال و مشاهده سریع خطاها و مشکلات است. در واقع بسیاری از مشکلات امنیتی که دامنگیر شبکه های می شود به پیکربندی غلط فایروال بر می گردد. لذا پیکربندی سریع و ساده یک فایروال ، امکان بروز خطا را کم می کند. برای مثال امکان نمایش گرافیکی معماری شبکه و یا ابزارای که بتواند سیاستهای امنیتی را به پیکربندی ترجمه کند ، برای یک فایروال بسیار مهم است.

۴- امنیت و افزونگی فایروال: امنیت فایروال خود یکی از نکات مهم در یک شبکه امن است. فایروالی که نتواند امنیت خود را تامین کند ، قطعاً اجازه ورود هکرها و مهاجمان را به سایر بخشهای شبکه نیز خواهد داد. امنیت در دو بخش از فایروال ، تامین کننده امنیت فایروال و شبکه است:

الف- امنیت سیستم عامل فایروال : اگر نرم افزار فایروال بر روی سیستم عامل جداگانه ای کار می کند، نقاط ضعف امنیتی سیستم عامل ، می تواند نقاط ضعف فایروال نیز به حساب بیاید. بنابراین امنیت و استحکام سیستم عامل فایروال و بروزرسانی آن از نکات مهم در امنیت فایروال است.

ب- دسترسی امن به فایروال جهت مقاصد مدیریتی : یک فایروال باید مکانیزم های امنیتی خاصی را برای دسترسی مدیران شبکه در نظر بگیرد. این روشها می تواند رمزنگاری را همراه با روشهای مناسب تعیین هویت بکار گیرد تا بتواند در مقابل نفوذگران تاب بیاورد.

انواع فایروال

انواع مختلف فایروال کم و بیش کارهایی را که اشاره کردیم ، انجام می دهند، اما روش انجام کار توسط انواع مختلف ، متفاوت است که این امر منجر به تفاوت در کارایی و سطح امنیت پیشنهادی فایروال می شود. بر این اساس فایروالها را به ۵ گروه تقسیم می کنند.

۱- فایروالهای سطح مدار (Circuit-Level): این فایروالها به عنوان یک رله برای ارتباطات TCP عمل می کنند. آنها ارتباط TCP را با رایانه پشتشان قطع می کنند و خود به جای آن رایانه به پاسخگویی اولیه می پردازند. تنها پس از برقراری ارتباط است که اجازه می دهند تا داده به سمت رایانه مقصد جریان پیدا کند و تنها به بسته های داده ای مرتبط اجازه عبور می دهند. این نوع از فایروالها هیچ داده درون بسته های اطلاعات را مورد بررسی قرار نمی دهند و لذا سرعت خوبی دارند. ضمناً امکان ایجاد محدودیت بر روی سایر پروتکلها (غیر از TCP) را نیز نمی دهند.

۲- فایروالهای پروکسی سرور : فایروالهای پروکسی سرور به بررسی بسته های اطلاعات در لایه کاربرد می پردازد. یک پروکسی سرور درخواست ارائه شده توسط برنامه های کاربردی پشتش را قطع می کند و خود به جای آنها درخواست را ارسال می کند. نتیجه درخواست را نیز ابتدا خود دریافت و سپس برای برنامه های کاربردی ارسال می کند. این روش با جلوگیری از ارتباط مستقیم برنامه با سرورها و برنامه های کاربردی خارجی امنیت بالایی را تامین می کند. از آنجایی که این فایروالها پروتکلهای سطح کاربرد را می شناسند ، لذا می توانند بر مبنای این پروتکلها محدودیتهایی را ایجاد کنند. همچنین آنها می توانند با بررسی محتوای بسته های داده ای به ایجاد محدودیتهای لازم پردازند. البته این سطح بررسی می تواند به کندی این فایروالها بیانجامد. همچنین از آنجایی که این فایروالها باید ترافیک ورودی و اطلاعات برنامه های کاربردی کاربر انتهایی را پردازش کند، کارایی آنها بیشتر کاهش می یابد. اغلب اوقات پروکسی سرورها از دید کاربر انتهایی شفاف نیستند و کاربر مجبور است تغییراتی را در برنامه خود ایجاد کند تا بتوان داین فایروالها را به کار

بگیرد. هر برنامه جدیدی که بخواهد از این نوع فایروال عبور کند ، باید تغییراتی را در پشته پروتکل فایروال ایجاد کرد.

۳- فیلترهای Nosstateful packet : این فیلترها روش کار ساده ای دارند. آنها بر مسیر یک شبکه می نشینند و با استفاده از مجموعه ای از قواعد ، به بعضی بسته ها اجازه عبور می دهند و بعضی دیگر را بلوکه می کنند. این تصمیمها با توجه به اطلاعات آدرس دهی موجود در پروتکل های لایه شبکه مانند IP و در بعضی موارد با توجه به اطلاعات موجود در پروتکل های لایه انتقال مانند سرآیندهای TCP و UDP اتخاذ می شود. این فیلترها زمانی می توانند به خوبی عمل کنند که فهم خوبی از کاربرد سرویسهای مورد نیاز شبکه جهت محافظت داشته باشند. همچنین این فیلترها می توانند سریع باشند چون همانند پروکسی ها عمل نمی کنند و اطلاعاتی درباره پروتکل های لایه کاربرد ندارند.

۴- فیلترهای Stateful Packet : این فیلترها بسیار باهوشتر از فیلترهای ساده هستند. آنها تقریباً تمامی ترافیک ورودی را بلوکه می کنند اما می توانند به ماشینهای پشتشان اجازه بدهند تا به پاسخگویی پردازند. آنها این کار را با نگهداری رکورد اتصالاتی که ماشینهای پشتشان در لایه انتقال ایجاد می کنند، انجام می دهند. این فیلترها ، مکانیزم اصلی مورد استفاده جهت پیاده سازی فایروال در شبکه های مدرن هستند. این فیلترها می توانند رد پای اطلاعات مختلف را از طریق بسته هایی که در حال عبورند ثبت کنند. برای مثال شماره پورت های TCP و UDP مبدا و مقصد، شماره ترتیب TCP و پرچمهای TCP. بسیاری از فیلترهای جدید Stateful می توانند پروتکل های لایه کاربرد مانند FTP و HTTP را تشخیص دهند و لذا می توانند اعمال کنترل دسترسی را با توجه به نیازها و سرعت این پروتکلها انجام دهند.

۵- فایروالهای شخصی : فایروالهای شخصی ، فایروالهایی هستند که بر روی رایانه های شخصی نصب می شوند. آنها برای مقابله با حملات شبکه ای طراحی شده اند. معمولاً از برنامه های در حال اجرا در ماشین آگاهی دارند و تنها به ارتباطات ایجاد شده توسط

این برنامه ها اجازه می دهند که به کار پردازند نصب یک فایروال شخصی بر روی یک PC بسیار مفید است زیرا سطح امنیت پیشنهادی توسط فایروال شبکه را افزایش می دهد. از طرف دیگر از آنجایی که امروزه بسیاری از حملات از درون شبکه حفاظت شده انجام می شوند ، فایروال شبکه نمی تواند کاری برای آنها انجام دهد و لذا یک فایروال شخصی بسیار مفید خواهد بود. معمولا نیازی به تغییر برنامه جهت عبور از فایروال شخصی نصب شده (همانند پروکسی) نیست.

موقعیت یابی برای فایروال:

محل و موقعیت نصب فایروال همانند انتخاب نوع صحیح فایروال و پیکربندی کامل آن ، از اهمیت ویژه ای برخوردار است. نکاتی که باید برای یافتن جای مناسب نصب فایروال در نظر گرفت عبارتند از:

- موقعیت و محل نصب از لحاظ توپولوژیکی : معمولا مناسب به نظر می رسد که فایروال را در درگاه ورودی/خروجی شبکه خصوصی نصب کنیم. این امر به ایجاد بهترین پوشش امنیتی برای شبکه خصوصی با کمک فایروال از یک طرف و جداسازی شبکه خصوصی از شبکه عمومی از طرف دیگر کمک می کند.
- قابلیت دسترسی و نواحی امنیتی : اگر سرورهایی وجود دارند که باید برای شبکه عمومی در دسترس باشند ، بهتر است آنها را بعد از فایروال و در ناحیه DMZ قرار دهید. قرار دادن این سرورها در شبکه خصوصی و تنظیم فایروال جهت صدور اجازه به کاربران خارجی برای دسترسی به این سرورها برابر خواهد بود با هک شدن شبکه داخلی. چون شما خود مسیر هکرها را در فایروال باز کرده اید. در حالی که با استفاده از ناحیه DMZ ، سرورهای قابل دسترسی برای شبکه عمومی از شبکه خصوصی شما بطور فیزیکی جدا هستند، لذا اگر هکرها بتوانند به نحوی به این سرورها نفوذ کنند بازهم فایروال را پیش روی خود دارند.

- **مسیریابی نامتقارن :** بیشتر فایروالهای مدرن سعی می کنند اطلاعات مربوط به اتصالات مختلفی را که از طریق آنها شبکه داخلی را به شبکه عمومی وصل کرده است، نگهداری کنند. این اطلاعات کمک می کنند تا تنها بسته های اطلاعاتی مجاز به شبکه خصوصی وارد شوند. در نتیجه حائز اهمیت است که نقطه ورود و خروج تمامی اطلاعات به /از شبکه خصوصی از طریق یک فایروال باشد.
- **فایروالهای لایه ای :** در شبکه های با درجه امنیتی بالا بهتر است از دو یا چند فایروال در مسیر قرار گیرند. اگر اولی با مشکلی روبرو شود، دومی به کار ادامه می دهد. معمولاً بهتر است دو یا چند فایروال مورد استفاده از شرکتهای مختلفی باشند تا در صورت وجود یک اشکال نرم افزاری یا حفره امنیتی در یکی از آنها ، سایرین بتوانند امنیت شبکه را تامین کنند.

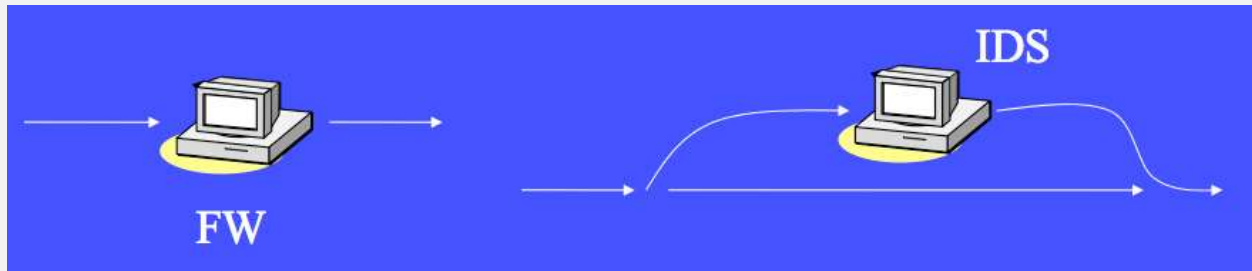
درس ۲

IDS چیست ؟

خلاصه:

IDS یک سیستم محافظتی است که خرابکاریهای در حال وقوع روی شبکه را شناسایی می کند. روش کار به این صورت است که با استفاده از تشخیص نفوذ که شامل مراحل جمع آوری اطلاعات ، پویش پورتهای ، به دست آوری کنترل کامپیوترها و نهایتا هک کردن می باشد ، می تواند نفوذ خرابکاریها را گزارش و کنترل کند.

از قابلیت های دیگر IDS ، امکان تشخیص ترافیک غیرمترعارف از بیرون به داخل شبکه و اعلام آن به مدیر شبکه و یا بستن ارتباطهای مشکوک و مظنون می باشد. ابزار IDS قابلیت تشخیص حملات از طرف کاربران داخلی و کاربران خارجی را دارد.



بر خلاف نظر عمومی که معتقدند هر نرم افزاری را می توان به جای IDS استفاده کرد، دستگاههای امنیتی زیر نمی توانند به عنوان IDS مورد استفاده قرار گیرند:

۱- سیستم هایی که برای ثبت وقایع شبکه مورد استفاده قرار می گیرند مانند : دستگاه هایی که برای تشخیص آسیب پذیری در جهت از کار انداختن سرویس و یا حملات مورد استفاده قرار می گیرند.

۲- ابزارهای ارزیابی آسیب پذیری که خطاها و یا ضعف در تنظیمات را گزارش می دهند.

۳- نرم افزارهای ضدویروس که برای تشخیص انواع کرمها، ویروسها و به طور کلی نرم افزارهای خطرناک تهیه شده اند.

۴- دیوار آتش (Firewall)

۵- مکانیزم های امنیتی مانند SSL و Radius و

چرا دیوار آتش به تنهایی کافی نیست؟

به دلایل زیر دیوار آتش نمی تواند امنیت شبکه را به طور کامل تامین کند :

۱. چون تمام دسترسی ها به اینترنت فقط از طریق دیوار آتش نیست.

۲. تمام تهدیدات خارج از دیوار آتش نیستند.

۳. امنیت کمتر در برابر حملاتی که توسط نرم افزارها مختلف به اطلاعات و داده های سازمان می شود ،

مانند Virus Programs , Java Applet , Active

تکنولوژی IDS

۱- Plain HandWork

۲- Network Based

۳- Host Based

۴- Honey pot

NIDS (NetworkBas)

گوش دادن به شبکه و جمع آوری اطلاعات از طریق کارت شبکه ای که در آن شبکه وجود دارد. به تمامی ترافیک های موجود گوش داده و در تمام مدت در شبکه مقصد فعال باشد.

HIDS (Host Base)

تعداد زیادی از شرکتها در زمینه تولید این نوع IDS فعالیت می کنند.
روی PC نصب می شود و از CPU و هارد سیستم استفاده می کنند.
دارای اعلان خطر در لحظه می باشد.

جمع آوری اطلاعات در لایه Application

مثال این نوع IDS، نرم افزارهای مدیریتی می باشند که ثبت وقایع را تولید و کنترل می کنند.

Honey pot

سیستمی می باشد که عملاً طوری تنظیم شده است که در معرض حمله قرار بگیرد. اگر یک پویشگری از HIDS، NIDS و دیواره آتش با موفقیت رد شود متوجه نخواهد شد که گرفتار یک Honey pot شده است. و خرابکاری های خود را روی آن سیستم انجام می دهد و می توان از روشهای این خرابکاری ها برای امن کردن شبکه استفاده کرد.

حملات به طور کلی به دو بخش تقسیم می شوند:

- ۱- غیرفعال: فکر دسترسی به سیستم های آسیب پذیر بدون دستیابی به اطلاعات .
- ۲- فعال: دستیابی بدون اجازه به همراه تغییر در منابع و اطلاعات یک سازمان .

از نظر شخص نفوذگر حملات به گروههای زیر تقسیم می شوند:

۱- داخلی: یعنی اینکه حملات از طریق کارکنان و یا شرکای تجاری و یا حتی مشتریانی که به شبکه شما متصل می باشند.

۲- خارجی: حملاتی که از خارج سازمان و معمولاً از طریق اینترنت انجام می گیرد.

برای تشخیص خطرات و حملات احتمالی می بایست سیستم خود را در برابر تقاضاهایی که سرویس های نامناسب درخواست می کنند مورد بررسی قرار دهید. این بررسی ها در تشخیص حملات واقعی به ما کمک می کند. با توجه به انواع راه هایی که نفوذ گران برای دسترسی به سیستمها استفاده می کنند نگاهی اجمالی به روشهای آسیب رسانی و نفوذ می اندازیم.

● استفاده از آسیب پذیری های معروف: در اکثر موارد حمله به معنی تلاش برای استفاده از نقص یا ایجاد آن در سیستم امنیتی يك سازمان اطلاق می شود و این یکی از راههای نفوذگری در شبکه می باشد. اغلب خود سازمان ممکن است از ابزاری برای امن کردن شبکه استفاده کند که کار حمله کننده را آسان می سازد به بیان واضح تر اینکه ابزارهای امنیتی نیز خود دارای نواقص و حفره های امنیتی می باشد که اختیارات بیشتری را به نفوذگر می دهد. این نرم افزارها اغلب مانند شمشیر دو لبه عمل می کنند و مورد استفاده هردو گروه کاربران و حمله کنندگان قرار می گیرد مانند نرم افزارهای کنترل صحت و یکپارچگی فایل یا نرم افزارهایی که جهت تست آسیب پذیری شبکه مورد استفاده قرار می گیرند. چك کردن یکپارچگی فایلها با استفاده از روش های سیستمی و با قابلیت ادغام روشهای مختلف با یکدیگر و با ابزارهایی نظیر anti-SATAN یا Courtney امکان پذیر می باشد.

● ترافیک خروجی غیر معمول: يك نفوذگر با استفاده از تعداد زیادی Exploit و حتی نفوذ های ناموفق سعی در به دست آوردن کنترل کامپیوتر مقصد دارد. این عملیات نفوذگرانه، ترافیک معمول شبکه را افزایش می دهد و نشانه وقوع يك حمله در آینده می باشد. هر ابزار تست آسیب پذیری می بایست قابلیت تشخیص فعالیت های مشکوک و غیر متعارف را داشته باشد و با ارائه گزارش ، اعلام خطر لازم را به مدیر شبکه بدهد.

حد تکرار برای کمک به تشخیص فعالیت های واقعی و مشکوک: فعالیت های شبکه بوسیله دریافت و کنترل بعضی پارامترها قابل شناسایی است مانند User Profile یا از Session State

زمان بین تکرار فعالیتها: پارامتری برای تشخیص زمان سپری شده بین دو واقعه متوالی. مثلاً وقتی بخواهید با نام کاربری اشتباه وارد سیستم شوید، سه تلاش برای ورود با نام غلط بین فاصله زمانی ۲ دقیقه يك فعالیت مشکوک به نظر می رسد.

اشتباه در تایپ ویا جوابهایی که در يك Session ایجاد می شود.

پروتکل ها و سرویس های شبکه به صورت کاملا دقیقی مستند شده اند و از ابزارهای نرم افزاری خاص استفاده می کنند. هرگونه ناهماهنگی با قالب شناخته شده (مثل اشتباه در تایپ يك دستور) ممکن است اطلاعاتی برای شناسایی سرویسهای که می توانند مورد حمله يك نفوذگر قرارگیرند باشد. اگر امکان Audit در سیستم فعال شده باشد، مثل Send Mail Relaying، توالی ارتباط Log بصورت معمولی و قابل پیش بینی اتفاق می افتد. هرچند که اگر در Log دریافت شده دستورات غیر مجاز دیده شود ممکن است نتیجه موارد اشتباه غیر عمدی ویا سعی در Spoofing (Spoofing) باشد. به این معنی است که نفوذگر آدرس خود را به آدرسی که برای سیستم شناخته شده است تغییر داده و به این ترتیب به سیستم نفوذ می کند).

تست تلاشهای مخرب ممکن است شامل موارد زیر باشد:

شناسایی تلاشهای متعدد برای جبران خطاهای تایپی و تکرار دستورات.

تشخیص خطاهای مکرر برای یافتن پروتکل ها که بدنبال يك تلاش موفق انجام می شود.

تشخیص خطا و یادگیری در جهت شناسایی نرم افزارهای و یا سیستم عامل های موجود در سایت مقصد.

ناهماهنگی در جهت ارسال و دریافت اطلاعات:

هرگونه ناهماهنگی ترافیکی در Packet ها یا يك Session نشانه ای از يك حمله پنهانی است. بررسی آدرس مبدا و مقصد (به صورت ورودی یا خروجی) میتواند جهت Packet را تشخیص بدهد. روند برقراری يك session با تشخیص اولین پیام ارسال شده شناسایی می شود. يك درخواست برای دریافت يك سرویس از شبکه محلی به صورت يك session ورودی است و پروسه فعال کردن يك سرویس بر پایه Web از يك شبکه محلی يك session خروجی است.

موارد زیر می تواند به عنوان حمله محسوب شود:

Packetهایی که منشاء آنها اینترنت است بدون اینکه در خواستی از سمت شبکه محلی داشته باشد و وارد شبکه شود.

این حالت ممکن است نشان دهنده يك حمله IP Spoofing از خارج باشد. این مشکلات می توانند در Routerهایی که قابلیت مقایسه آدرس مبدا و مقصد را دارند بر طرف شوند. در عمل تعداد اندکی از Router ها در شبکه می توانند به عنوان فایروال عمل کنند.

بر عکس حالت قبل Packetهایی که به صورت خروجی در يك شبکه محلی ایجاد می شوند و به يك شبکه خارجی فرستاده می شوند.

Packet ها با پورت های مبدا و مقصد غیر مشخص. اگر منبع پورت در مورد يك درخواست ورود یا خروج اطلاعات با نوع سرویس یکسان نباشد ممکن است به عنوان يك تلاش برای نفوذ یا پوشش سیستم تلقی شود. بطور مثال در خواست Telnet از روی پورت ۱۰۰ در محیطی که انتظار چنین پشتیبانی برای سرویس وجود ندارد. ترافیک غیر معمول بیشتر توسط فایروال شناسایی شده و Packetهای مشکوک را از بین می برد. با توجه به اینکه فایروالها همیشه با سیستم های تشخیص نفوذ ادغام نمی شوند ، بنابراین ممکن است که سیستمهای تشخیص نفوذ راه حلی برای این مشکل باشد.

علائم نفوذ:

معمولا با اجرای برنامه های خاص در سیستم انتظار مواجهه با رفتارهای خاص و مشابه وجود دارد بعضی از موارد مانند موارد زیر:

مشخصات تاریخ و زمان : در بعضی محیط های خاص بطور معمول بعضی رفتارها در زمان خاصی در شبکه اتفاق می افتد. مثلا فرض کنید بطور معمول شبانه صبح یکسری اطلاعات به بخش مرکزی شرکت ارسال می شود که مربوط به اطلاعات مالی است. چنین ترافیکی در شبانه صبح همیشه اتفاق می افتد و عادی است در صورتیکه چنین ترافیکی روز جمعه اتفاق بیفتد و ثبت شود ، غیر معمول است و باید به عنوان يك رفتار غیر معمول یا نفوذ به سیستم مورد بررسی دقیق قرارگیرد.

- مشخصات منابع سیستم: بعضی نفوذ های خاص باعث خرابی بعضی پارامترهای خاص سیستم میشود مثلاً يك حمله Brute Force برای شکستن حرف رمز باعث در گیر کردن CPU میشود در حالیکه يك حمله DoS همین کار را با سرویس های سیستم انجام میدهد. استفاده سنگین از منابع سیستم (پروسسور، حافظه، دیسک سخت، سرویسها و اتصالات شبکه) که در زمانهای غیر معمول اتفاق می افتد برای شناسایی حمله بسیار مفید هستند و باید به آنها بسیار توجه کرد.

Packet هایی با تایید های TCP غیر معمول: اگر در يك Packet نشانه مربوط به ACK فعال باشد و قبل از آن هیچ SYN-Packet ارسال نشده باشد، ممکن است نتیجه يك حمله در سیستم باشد همچنین این حالت ممکن است اثر يك Packet خراب هم باشد که در يك شبکه با نرم افزار های خراب ایجاد می شود و واقعا " حمله نفوذی نباشد.

سرویس های مختلف با علایم مختلف: ممکن است در بعضی موارد انتظار ایجاد ترافیک خاص از يك کاربر مشخص داشته باشیم مثلاً کاربری که در يك ماموریت اداری بسر می برد معمولاً " فقط نامه های خود را چک می کند و یا فایلی را انتقال می دهد. در صورتیکه دسترسی این کاربر به پورت های مختلف از طریق Tel net، دلیلی بر امکان نفوذ یا حمله است.

موارد غیر معمول - علامت نفوذ:

يك نفوذ کننده بالقوه ممکن است عملیات نفوذ خود را به گونه ای طراحی کند که اثر جانبی آن باعث رفتارهای غیر معمول در سیستم باشد. مانیتورینگ اثرات جانبی بسیار سخت است چون پیدا کردن محل آنها به سادگی امکان پذیر نیست از موارد غیر منتظره سیستم به موارد زیر می توان اشاره کرد:

۱- مشکلات تعریف نشده در سخت افزار یا نرم افزار سیستم مثل خاموشی شدن بدون علت سرور، عدم کارکرد بعضی برنامه های نرم افزاری مانند IIS، موارد غیر معمول restart شدن سیستم ها، تغییرات در تنظیم clock سیستم.

۲- بروز اشکالات نامشخص در منابع سیستم مثل File System Overflow یا مشغول بودن بیش از حد CPU

۳- دریافت پیام های غیر متعارف از بعضی برنامه های خود اجرا ، مثل پیغامهایی که نشان دهنده عدم اجرا و یا خطا در هنگام اجرای يك برنامه ایجاد شده باشد. بخصوص برنامه هایی که برای مانیتور کردن سیستم طراحی شده اند مثل Syslog.

۴- بروز اشکالات نامشخص در کارایی سیستم مثلاً" در Router ها یا سرویس های سیستم مثل کند شدن سرور.

۵- بروز رفتارهای مشکوک در اجرای برنامه های کاربرمثل اشکال در دسترسی به بعضی منابع شبکه
 ۶- عملکرد مشکوک در فایل های ثبت وقایع (Log) (ها) بررسی این فایل ها از نظر سائز برای اینکه حجم فایل از اندازه متعارف خیلی بیشتر یا کمتر نباشد. مگر اینکه مدیر شبکه خود چنین تغییری ایجاد کرده باشد.

چه باید کرد؟

مهمترین کار يك سیستم کشف نفوذ گر، دفاع از کامپیوتر بوسیله شناسایی حمله و جلوگیری از آن است. شناسایی حمله هکر بستگی به نوع و تعداد عکس العمل مورد نظر دارد .

مقابله با نفوذ، نیاز به يك سیستم ترکیبی دام گذاری و تله اندازی دارد که هر دو این پروسه ها باید با بررسی و دقت انجام شود. از کارهای دیگری که باید انجام داد ، تغییر دادن جهت توجه هکر است. هر دوسیستم واقعی و مجازی (HoneyPot) به دام اندازی هکر به طور دائمی دیده بانی (Monitor) می شوند و داده های تولید شده توسط سیستم شناسایی نفوذ گر (IDS) برای شناسایی نحوه عملکرد حمله به دقت بررسی می شود که این مهمترین وظیفه يك IDS جهت شناسایی حملات و یا نفوذهای احتمالی می باشد.

وقتی که يك حمله یا نفوذ شناسایی شد، IDS سرپرست شبکه را مطلع می سازد. مرحله بعدی کار می تواند بر عهده سرپرست شبکه یا خود IDS باشد که از بررسی های به عمل آمده نتیجه گیری کرده و اقدام متقابل را انجام دهد. (مانند جلوگیری از عملکرد يك قسمت بخصوص برای پایان بخشیدن به Session های مشکوک یا تهیه نسخه پشتیبان از سیستم برای حفاظت از اطلاعات ، و

یا انتقال ارتباط به يك سیستم گمراه کننده مانند Honeypot و چیزهای دیگر که بر اساس سیاستهای (Policy) شبکه قابل اجرا باشد. در حقیقت IDS يك از عناصر سیاستهای امنیتی شبکه است. در بین وظایف مختلف IDS، شناسایی نفوذگر از اساسی ترین آنهاست. حتی ممکن است در مراجع قانونی از نتایج و گزارشات حوادثی که IDS اعلام می کند استفاده نمود، و از حملاتی که در آینده اتفاق خواهد افتاد با اعمال وصله های امنیتی مناسب از حمله به يك کامپیوتر بخصوص و یا يك منبع شبکه جلوگیری کرد.

شناسایی نفوذ ممکن است گاهی اوقات زنگ خطر اشتباهی را به صدا در آورد. برای مثال نتیجه خراب کارکردن يك کارت شبکه و یا ارسال شرح يك حمله و یا اثر يك نفوذ از طریق Email.

ساختار و معماری سیستم تشخیص نفوذ:

سیستم تشخیص نفوذ يك هسته مرکزی دارد و يك تشخیص دهنده (موتور تشخیص) است که مسئولیت تشخیص نفوذ را دارد. این سنسور يك مکانیزم تصمیم گیری بر اساس نوع نفوذ دارد.

این سنسور اطلاعات خام را از سه منبع دریافت می کند.

۱- از اطلاعات موجود در بانک اطلاعاتی خود IDS

۲- فایل ثبت وقایع سیستم (syslog)

۳- آثار ترافیک عبوری و دیده بانی شبکه.

فایل ثبت وقایع سیستم (syslog) ممکن است به طور مثال اطلاعات پیکربندی سیستم و دسترسی های کاربران باشد. این اطلاعات اساس تصمیم گیری های بعدی مکانیزم سنسور خواهد بود. این سنسور با يك Event Generator که مسئول جمع آوری اطلاعات است با هم کار می کنند. قوانین جمع آوری اطلاعات که به وسیله سیاست های Event generator مشخص می شود، تعیین کننده نوع فیلترینگ از روی حوادث و اطلاعات ثبت شده است.

Event Generator، مثل سیستم عامل یا شبکه یا یک برنامه اجرایی، تولید کننده Policyهایی هستند که ممکن است یک واقعه ایجاد شده در سیستم عامل یا Packet های شبکه را ثبت کنند. این مجموعه به همراه اطلاعات Policy می تواند در یک سیستم محافظت شده یا خارج از شبکه قرار داده شود. در بعضی شرایط خاص هیچ محل مشخصی به عنوان محل حفظ اطلاعات ایجاد نمی شود مثل وقتی که اطلاعات جمع آوری شده از وقایع مستقیماً به یک سیستم آنالیز ارسال می شود.

وظیفه سنسور فیلتر کردن اطلاعات است و حذف کردن هر داده غیر مرتبط که از طرف منابع دریافت اطلاعات می رسد. تحلیل کننده برای دستیابی به این هدف از Policyهای موجود استفاده می کند. تحلیل گر نکاتی مانند اثر و نتیجه حمله، پرو فایل رفتارهای نرمال و صحیح و پارامترهای مورد نیاز مثل Threshold ها را بررسی می کند.

علاوه بر همه اینها بانک اطلاعاتی که پارامترهای پیکربندی IDS را در خود نگه می دارد، روشهای مختلف ارتباطی را ایجاد می کنند. سنسور یا گیرنده هم بانک اطلاعاتی خاص خود را دارد، که شامل تاریخچه پویایی از نفوذهای پیچیده بوده یا با توجه به تعداد حمله مورد تحلیل قرار گرفته است. سیستم تشخیص نفوذ می تواند به صورت متمرکز مثل برقراری یک فایروال فیزیکی یا به صورت غیر متمرکز انجام شود. یک IDS غیر متمرکز شامل تعداد زیادی سیستم تشخیص نفوذ در یک شبکه بزرگ است که هر کدام از آنها با هم در ارتباط هستند. سیستم های پیچیده تر از ساختاری پیروی می کنند که ماژول های مشابه برنامه های خود اجرایی دارند که روی هر کامپیوتر اجرا می شوند.

عملکرد این سیستم جایگزین، مونیتر و فیلتر کردن تمام فعالیتهای مرتبط با یک بخش محافظت شده است که بتواند یک آنالیز دقیق و پاسخ متناسب از شبکه دریافت کند. یکی از قسمت های بسیار مهم IDS برنامه ای است که به سرور آنالیز کننده گزارش می دهد، Database DIDS (IDS) و دارای ابزار آنالیز پیچیده تری است که حملات غیر متمرکز را نیز شناسایی می کند. دلیل دیگری که وجود دارد مربوط به قابلیت حمل و انتقال در چند منطقه فیزیکی است. علاوه بر این عامل جایگزین مشخص برای تشخیص و شناسایی اثر حمله های شناخته شده می باشد. یک راه حل ساختاری چند برنامه ای که در سال ۱۹۹۴ ایجاد شد.

Autonomous Agent for Intrusion Detection یا AAFID است. این ساختار از يك جاگزین استفاده می کند که بخش به خصوصی از رفتار سیستم را در زمان خاص دیده بانی می کند. به طور مثال يك جاگزین می تواند تعداد دفعاتی را که به سیستم Telnet شده تشخیص داده و در صورتی که این عدد منطقی به نظر نرسد آنرا گزارش کند. يك جاگزین همچنین قابلیت ایجاد زنگ خطر در زمان وقوع يك حادثه مشکوک را دارد. جاگزین ها می توانند مشابه سازی شوند و به سیستم دیگر منتقل گردند. به غیر از جاگزین ها ، سیستم می تواند رابط هایی برای دیده بانی کل فعالیتهای يك کامپیوتر بخصوص داشته باشد. این رابط ها همیشه نتایج عملیات خود را به يك مونیتر مشخص ارسال می کنند. سیستم های مانیتور اطلاعات را از نقاط مختلف و مشخص شبکه دریافت می کنند و این بدین معنی است که می توانند اطلاعات غیر متمرکز را بهم ارتباط دهند و نتیجه گیری نهایی را انجام دهند. به انضمام اینکه ممکن است فیلتر هایی گذاشته شود تا داده های تولید شده را بصورت انتخابی دریافت نماید .

درس ۳

Security Protocols

پروتکل IPsec يك مجموعه پروتکل است که امنیت ارتباطات پروتکل اینترنت (IP) را توسط عملیات احراز هویت و رمزنگاری برای هر بسته IP در يك نشست ارتباطی تامین می کند.

IPsec همچنین شامل پروتکل هایی می شود که برای برقراری يك ارتباط دوطرفه بین عامل ها در ابتدای نشست و مذاکره در مورد کلیدهای رمزنگاری برای استفاده در مدت زمان نشست، استفاده می شوند.

پروتکل IPsec اساسا راهی است که امنیت داده هایی را که در يك شبکه بین کامپیوترها منتقل می شوند، تضمین می کند. IPsec تنها یکی از قابلیت های ویندوز نیست، پیاده سازی ویندوزی IPsec بر اساس استانداردهای توسعه یافته توسط نیروی وظیفه مهندسی اینترنت (IETF) بنا شده است.

پروتکل IPsec در لایه اینترنت از مدل لایه ای پروتکل اینترنت کار می کند. IPsec می تواند از جریان های داده مابین میزبان ها (میزبان به میزبان)، مابین گذرگاه های امنیتی (شبکه به شبکه) یا مابین يك گذرگاه امنیتی به يك میزبان، پشتیبانی کند.

تعدادی از سیستم های امنیتی اینترنتی دیگر که به صورت گسترده کاربرد دارند، مانند لایه سوکت امن (SSL)، لایه امنیت انتقال (TLS) و پوسته امن (SSH) در لایه های بالایی از مدل TCP/IP کار می کنند. در صورتیکه IPsec هر نوع ترافیک در سراسر شبکه های مبتنی بر IP را پشتیبانی می کند. اگر ترافیکی غیر از IP در شبکه وجود داشته باشد، باید از پروتکل دیگری مانند GRE در کنار IPsec استفاده کرد.

پروتکل IPsec توسط سرویس های زیر، امنیت داده های ارسال شده بین دو آدرس IP در شبکه را تامین می کند:

▪ احراز هویت داده

۱. شناسایی مبداء داده: شما می‌توانید از IPsec استفاده کنید تا تضمین کند که هر بسته ای که از يك طرف قابل اعتماد دریافت کردید، در واقع توسط همان مبداء ارسال شده است و جعلی و دستکاری شده نیست.
۲. تمامیت داده: شما می‌توانید از IPsec استفاده کنید تا تضمین کند که داده ها در زمان انتقال تغییر نمی‌کنند.
۳. حفاظت ضد بازپخش: شما می‌توانید از IPsec استفاده کنید تا بررسی کند که هر بسته ای که دریافت می‌کنید یکتا است و کپی برداری نشده است.

▪ رمزگذاری

شما می‌توانید از IPsec به منظور رمزگذاری داده ها در شبکه استفاده کنید تا برای سوء استفاده کنندگان قابل دسترسی نبوده و در طول مسیر، امکان استفاده غیر مجاز از آنها وجود نداشته باشد.

به بیان دیگر، کامپیوتر مبداء بسته اطلاعاتی TCP/IP عادی را به صورت يك بسته اطلاعاتی IPsec بسته بندی می‌کند و برای کامپیوتر مقصد ارسال می‌کند. این بسته‌ها زمانی که به مقصد برسد رمز شده است و طبیعتاً کسی نمی‌تواند از محتوای آنها اطلاعاتی به دست آورد.

در ویندوز سرور ۲۰۰۸ و ویندوز ویستا، IPsec يك اجبار است که باید به وسیله سیاست-های IPsec و یا قوانین امنیت ارتباط، اعمال گردد. سیاست‌های IPsec که به صورت پیش فرض روی سیستم‌ها وجود دارد، تنها بر روی سرویس‌های احراز هویت مذاکره می‌کنند. اگر چه شما می‌توانید با استفاده از سیاست‌های IPsec و یا قوانین ارتباط امن، تنظیماتی را به سیستم اعمال نمایید تا هر ترکیبی از سرویس‌های امنیت داده را فراهم کند.

معماری امنیتی

IPSec يك استاندارد باز است. پروتکل IPsec از پروتکل های زیر برای تامین امنیت داده ها در شبکه استفاده می کند.

- سرآیند احراز هویت (AH): این پروتکل تمامیت و احراز هویت مبداء داده ها را برای بسته های داده IP فراهم کرده و از داده ها در مقابل حملات پخشی محافظت می کند.
- بسته بندی امن داده (ESP): این پروتکل، محرمانگی، احراز هویت مبداء داده ها، تمامیت و يك سرویس ضد بازپخشی را ارائه می نماید.
- مدیریت امنیت (SA): يك مجموعه از الگوریتم ها و داده ها ارائه می دهد که این مجموعه، پارامترهای ضروری برای مدیریت کردن عملکرد پروتکل AH و/یا پروتکل ESP را فراهم می کند. پروتکل ISAKMP، يك چهارچوب برای عملیات احراز هویت و تبادل کلید ارائه می دهد، که در واقع این کلیدها یا به وسیله تنظیم دستی توسط کلیدهایی که از پیش به اشتراك گذاشته شده اند و یا از طریق IKE¹ تهیه می گردند.

مدهای عملیاتی

پروتکل IPsec می تواند برای روش انتقال میزبان به میزبان و روش تونل شبکه مورد استفاده قرار گیرد.

- مد انتقالی: در این مد، معمولاً تنها اطلاعاتی که به صورت بسته های IP ارسال می شوند، رمزنگاری و/یا احراز هویت می گردند. عملیات مسیریابی بدون تغییر باقی می ماند، چرا که سرآیند بسته IP تغییر نکرده و رمز نشده است. هرچند هنگامی که از سرآیند احراز هویت استفاده می شود، آدرس های IP قابل ترجمه نیستند، زیرا توسط الگوریتم درهم سازی اطلاعات آن رمزنگاری می شود. لایه های انتقال و کاربرد همیشه توسط الگوریتم درهم

¹Internet Key Exchange

سازی امن می شوند، در نتیجه تحت هیچ شرایطی نمی توان اطلاعات آنها را تغییر داد. مد انتقال برای ارتباطات میزبان به میزبان استفاده می شود.

▪ مد تونل شبکه:

در این مد، کل بسته IP رمزنگاری و/یا احراز هویت می شود. سپس درون بسته دیگری بسته بندی شده و یک سرآیند جدید می گیرد. این مد برای ایجاد شبکه های خصوصی مجازی برای ارتباطات شبکه به شبکه، ارتباطات میزبان به شبکه و ارتباطات میزبان به میزبان استفاده می شود. این مد، پیمایش NAT را پشتیبانی می کند.

شما می توانید با دادن یک سری دستورالعمل ها به ویندوز، این سیستم عامل را تعلیم دهید که تحت چه شرایطی از IPSec استفاده کند. تحت این شرایط شما در واقع مشخص می کنید که ترافیک کدام گروه از IP ها باید توسط IPSec انجام شود و کدامیک نشود. IPSec به شما امکان می دهد که تعریف کنید چه داده ای و چگونه باید رمزگذاری شود. برای این منظور معمولاً "از روش فیلتر کردن IP استفاده می شود. فهرست خاصی از IP های فیلتر شده که شما تهیه می کنید، می تواند مرجعی برای استفاده از پروتکل IPSec برای ویندوز باشد.

پروتکل PPTP

پروتکل Tunneling نقطه به نقطه، بخش توسعه یافته ای از پروتکل PPP است که فریم های پروتکل PPP را به صورت ip برای تبادل آنها از طریق یک شبکه IP مانند اینترنت توسط یک سرآیند، کپسوله می کند. این پروتکل می تواند در شبکه های خصوصی از نوع LAN-to-LAN نیز استفاده گردد.

پروتکل PPTP به وسیله انجمنی از شرکت های مایکروسافت، Ascend Communications، ۳com، ESI و US Robotics ساخته شد.

PPTP یک ارتباط TCP را (که یک ارتباط Connection Oriented بوده و پس از ارسال پکت منتظر Acknowledgment آن می ماند) برای نگهداری تونل و فریم های PPP کپسوله شده توسط GRE^۱ که به معنی کپسوله کردن مسیریابی عمومی است،

برای Tunneling کردن اطلاعات استفاده می کند. ضمناً اطلاعات کپسوله شده PPP قابلیت رمزنگاری و فشرده شدن را نیز دارا هستند.

تونل های PPTP باید به وسیله مکانیسم گواهی همان پروتکل PPP که شامل EAP، CHAP، PAP، MS-CHAP می شوند، گواهی شوند. در ویندوز ۲۰۰۰ رمزنگاری پروتکل PPP فقط زمانی استفاده می گردد که پروتکل احراز هویت یکی از پروتکل های EAP، TLS و یا MS-CHAP باشد. باید توجه شود که رمزنگاری PPP، محرمانگی اطلاعات را فقط بین دو نقطه نهایی یک تونل تأمین می کند و در صورتی که به امنیت بیشتری نیاز باشد، باید از پروتکل Isec استفاده شود.

پروتکل L۲TP

پروتکل L۲TP ترکیبی است از پروتکل های PPTP و Layer ۲ Forwarding (L۲F) که توسط شرکت سیسکو توسعه یافته است. این پروتکل ترکیبی است از بهترین خصوصیات موجود در L۲F و PPTP.

L۲TP نوعی پروتکل شبکه است که فریم های PPP را برای ارسال بر روی شبکه های IP مانند اینترنت و علاوه بر این برای شبکه های مبتنی بر X.۲۵، Frame Relay و یا ATM کپسوله می کند.

^۱Generic Routing Encapsulation

هنگامی که اینترنت به عنوان زیرساخت تبادل اطلاعات استفاده می گردد، L۲TP می تواند به عنوان پروتکل Tunneling از طریق اینترنت مورد استفاده قرار گیرد.

L۲TP برای نگهداری تونل از یک سری پیغام های L۲TP و نیز از پروتکل UDP پروتکل تبادل اطلاعات به صورت Connection Less که پس از ارسال اطلاعات منتظر دریافت Acknowledgment نمی شود و اطلاعات را، به مقصد رسیده فرض می کند استفاده می کند.

در L۲TP نیز فریم های PPP کپسوله شده می توانند همزمان علاوه بر رمزنگاری شدن، فشرده نیز شوند. البته مایکروسافت پروتکل امنیتی Ipsec را به جای رمزنگاری PPP توصیه می کند. ساخت تونل L۲TP نیز باید همانند PPTP توسط مکانیسم (PPP EAP ، CHAP ، MS-CHAP ، PAP) بررسی و تأیید شود.

PPTP در مقابل L۲TP

هر دو پروتکل PPTP و L۲TP از پروتکل PPP برای ارتباطات WAN استفاده می کنند تا نوعی اطلاعات ابتدایی برای دیتا را فراهم کنند و سپس یک سرایند اضافه برای انتقال اطلاعات از طریق یک شبکه انتقالی به پکت الحاق بنمایند. هرچند این دو پروتکل در برخی موارد نیز با هم تفاوت دارند. برخی از این تفاوت ها عبارتند از :

۱- شبکه انتقال که PPTP احتیاج دارد، باید یک شبکه IP باشد. ولی L۲TP فقط به یک تونل احتیاج دارد تا بتواند ارتباط Point-to-Point را برقرار کند. حال این تونل می تواند بر روی یک شبکه IP باشد و یا بر روی شبکه های دیگر مانند X.۲۵ و یا ATM ، Frame Relay

۲-L۲TP قابلیت فشرده سازی سرایند را داراست. هنگامی که فشرده سازی سرایند انجام می گیرد، L۲TP با حجم ۴ بایت عمل می کند، در حالی که PPTP با حجم ۶ بایت عمل می نماید.

۳- L۲TP متد احراز هویت را تأمین می کند، در حالی که PPTP این گونه عمل نمی کند، هرچند وقتی که PPTP یا L۲TP از طریق پروتکل امنیتی IPsec اجرا می شوند، هر دو، متد احراز هویت را تأمین می نمایند .

۴- PPTP رمزنگاری مربوط به PPP را استفاده می کند، ولی L۲TP از پروتکل IPsec برای رمزنگاری استفاده می نماید.

منابع

- RFC ۱۲۱۹ "On the Assignment of Subnet Numbers," Tsuchiya, P.F.; ۱۹۹۱
- RFC ۱۱۱۲ "Host Extensions for IP Multicasting," Deering, S.E.; ۱۹۸۹
- RFC ۱۰۸۸ "Standard for the Transmission of IP Datagrams over NetBIOS Networks," McLaughlin, L.J.; ۱۹۸۹
- RFC ۹۵۰ "Internet Standard Subnetting Procedure," Mogul, J.C.; Postel, J.B.; ۱۹۸۵
- RFC ۹۳۲ "Subnetwork Addressing Schema," Clark, D.D.; ۱۹۸۵
- RFC ۹۲۲ "Broadcasting Internet Datagrams in the Presence of Subnets," Mogul, J.C.; ۱۹۸۴
- RFC ۹۱۹ "Broadcasting Internet Datagrams," Mogul, J.C.; ۱۹۸۴
- RFC ۸۸۶ "Proposed Standard for Message Header Munging," Rose, M.T.; ۱۹۸۳
- RFC ۸۱۵ "IP Datagram Reassembly Algorithms," Clark, D.D.; ۱۹۸۲
- RFC ۸۱۴ "Names, Addresses, Ports, and Routes," Clark, D.D.; ۱۹۸۲
- RFC ۷۹۲ "Internet Control Message Protocol," Postel, J.B.; ۱۹۸۱
- RFC ۷۹۱ "Internet Protocol," Postel, J.B.; ۱۹۸۱
- RFC ۱۰۷۲ "TCP Extensions for Long-Delay Paths," Jacobson, V.; Braden, R.T.; ۱۹۸۸
- RFC ۸۹۶ "Congestion Control in IP/TCP Internetworks," Nagle, J.; ۱۹۸۴
- RFC ۸۷۹ "TCP Maximum Segment Size and Related Topics," Postel, J.B.; ۱۹۸۳
- RFC ۸۱۳ "Window and Acknowledgment Strategy in TCP," Clark, D.D.; ۱۹۸۲
- RFC ۷۹۳ "Transmission Control Protocol," Postel, J.B.; ۱۹۸۱
- Cisco ۹۷ "Interior Gateway Routing Protocol and Enhanced IGRP "
- http://www.cisco.com/univercd/cc/td/doc/csintwk/ito_doc/۵۵۱۸۲.htm
- Halabi ۹۷ B. Halabi, Internet Routing Architectures, Cisco Systems Publishing, Indianapolis, ۱۹۹۷.
- Huitema C. Huiteman, Routing in the Internet, Prentice Hall, New Jersey, ۱۹۹۵.
- RFC ۱۰۵۸ "Routing Information Protocol," Hedrick, C.L.; ۱۹۸۸
- RFC ۱۰۷۴ "NSFNET Backbone SPF-Based Interior Gateway Protocol," Rekhter, J.; ۱۹۸۸
- RFC ۱۱۳۶ "Administrative Domains and Routing Domains: A Model for Routing in the Internet," Hares, S.; Katz, D.; ۱۹۸۹
- RFC ۱۱۶۳ "Border Gateway Protocol (BGP)," Lougheed, K.; Rekhter, Y.; ۱۹۹۰
- RFC ۱۱۶۴ "Application of the Border Gateway Protocol in the Internet," Honig, J.C.; Katz, D.; Mathis, M.; Rekhter, Y.; Yu, J.Y.; ۱۹۹۰
- RFC ۱۱۹۵ "Use of OSI IS-IS for Routing in TCP/IP and Dual Environments," Callon, R.W.; ۱۹۹۰
- RFC ۱۲۲۲ "Advancing the NSFNET Routing Architecture," Braun, H.W.; Rekhter, Y.; ۱۹۹۱
- RFC ۱۲۴۷ "OSPF version ۲," Moy, J.; ۱۹۹۱
- RFC ۱۲۵۶ S. Deering, "ICMP Router Discovery Messages," RFC ۱۲۵۶, Sept. ۱۹۹۱.
- RFC ۱۲۶۷ "A Border Gateway Protocol ۳ (BGP-۳)," Lougheed, K.; Rekhter, Y.; ۱۹۹۱
- RFC ۱۵۸۴ J. Moy, "Multicast Extensions to OSPF," RFC ۱۵۸۴, March ۱۹۹۴.
- RFC ۱۷۲۳ G. Malkin, RIP Version ۲ - Carrying Additional Information. RFC ۱۷۲۳, November ۱۹۹۴

- RFC1۷۷1 Y. Rekhter and T. Li, "A Border Gateway Protocol ۴ (BGP-۴)," RFC 1۷۷1, March 1۹۹۵.
- RFC1۷۷۲ Y. Rekhter and P. Gross, "Application of the Border Gateway Protocol in the Internet," RFC 1۷۷۲, March 1۹۹۵.
- RFC1۷۷۳ P. Traina, "Experience with the BGP-۴ protocol," RFC 1۷۷۳, March 1۹۹۵
- RFC۲۰۰۲ C. Perkins, "IP Mobility Support," RFC ۲۰۰۲, 1۹۹۶.
- RFC۲1۷۸ J. Moy, "Open Shortest Path First Version ۲", RFC ۲1۷۸, July 1۹۹۷.
- RFC۸۲۳ "DARPA Internet Gateway," Hinden, R.M.; Sheltzer, A.; 1۹۸۲
- RFC۸۲۷ "Exterior Gateway Protocol (EGP)," Rosen, E.C.; 1۹۸۲
- RFC۸۸۸ "STUB Exterior Gateway Protocol," Seamonson, L.; Rosen, E.C.; 1۹۸۴
- RFC۹۰۴ "Exterior Gateway Protocol Formal Specification," Mills, D.L.; 1۹۸۴
- RFC۹11 "EGP Gateway under Berkeley UNIX ۴.۲," Kirton, P.; 1۹۸۴
- RFC11۰۲ "Policy Routing in Internet Protocols," Clark, D.D.; 1۹۸۹
- RFC11۰۴ "Models of Policy-Based Routing," Braun, H.W.; 1۹۸۹
- RFC11۲۴ "Policy Issues in Interconnecting Networks," Leiner, B.M.; 1۹۸۹
- RFC11۲۵ "Policy Requirements for Inter-Administrative Domain Routing," Estrin, D.; 1۹۸۹
- RFC1۲۴۵ "OSPF Protocol Analysis," Moy, J., ed; 1۹۹1
- RFC1۲۴۶ "Experience with the OSPF Protocol," Moy, J., ed.; 1۹۹1
- RFC1۲۵۴ "Gateway Congestion Control Survey," Mankin, A.; Ramakrishnan, K.K, eds.; 1۹۹1
- IEEE, "IEEE Standards for Local Area Networks: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications", IEEE, New York, New York, 1۹۸۵.
- IEEE, "IEEE Standards for Local Area Networks: Token-Passing Bus Access Method and Physical Layer Specification", IEEE, New York, New York, 1۹۸۵.
- IEEE, "IEEE Standards for Local Area Networks: Token Ring Access Method and Physical Layer Specifications", IEEE, New York, New York, 1۹۸۵.
- IEEE, "IEEE Standards for Local Area Networks: Logical Link Control", IEEE, New York, New York, 1۹۸۵.
- IEEE ۸۰۲/۳/ISO ۸۸۰۲-۳ Information processing systems - Local area networks - Part ۳: Carrier sense multiple access with collision detection (CSMA/CD) access method and physical layer specifications, 1۹۹۳.
- RFC1۶۶1 The Point-to-Point Protocol (PPP). W. Simpson, Editor. July 1۹۹۴.
- RFC1۶۶۳ PPP Reliable Transmission. D. Rand. July 1۹۹۴.
- RFC1۷1۷ The PPP Multilink Protocol (MP). K. Sklower, B. Lloyd, G. McGregor, D. Carr. November 1۹۹۴.
- RFC1۰۴۲ Standard for the transmission of IP datagrams over IEEE ۸۰۲ networks. J. Postel, J.K. Reynolds. Feb-۰1-1۹۸۸.
- RFC1۲۳۰ IEEE ۸۰۲/۴ Token Bus MIB. K. McCloghrie, R. Fox. May-۰1-1۹۹1.
- RFC1۲۳1 IEEE ۸۰۲/۵ Token Ring MIB. K. McCloghrie, R. Fox, E. Decker.
- RFC1۰۵۵ Nonstandard for transmission of IP datagrams over serial lines: SLIP. J.L. Romkey. Jun-۰1-1۹۸۸.

Computer Networking A Top-Down Approach ۵th Edition KUROSE·ROSS

"Computer Networks" , Andrew S.Tanenbaum, Third Edition, Prentice-Hall, ۱۹۹۶.

Network+ Certification Training Kit

آشنایی با سیستمهای نرم افزاری و شبکه تحقیق و گرد آورنده غلام رضا امیریان

www.wikipedia.org

www.ce.sharif.edu

www.ettercap.sourceforge.net

www.srco.ir

www.novell.com

www.itpro.ir

www.payvast.com

www.aftabir.com

www.cloob.com

www.subnet.ir

www.daba.ir

www.barnamenevis.org

www.parsmodir.com

www.persianguig.com

www.shabgard.org

www.mostafanoori.com

www.cisco.parsfa.com

www.mojसान.com

www.iana.org

www.raeissi.com

www.monkey.org

www.misaghnavazeni.com

www.thebends.org

www.oxid.it

www.chrismc.de

www.arpalert.org

www.netqurd.com

www.radcom.ir

www.niksystem.com

www.gtalk.ir

www.hamshahrionline.ir

www.netqurd.com

www.forum.p3.parsi.com