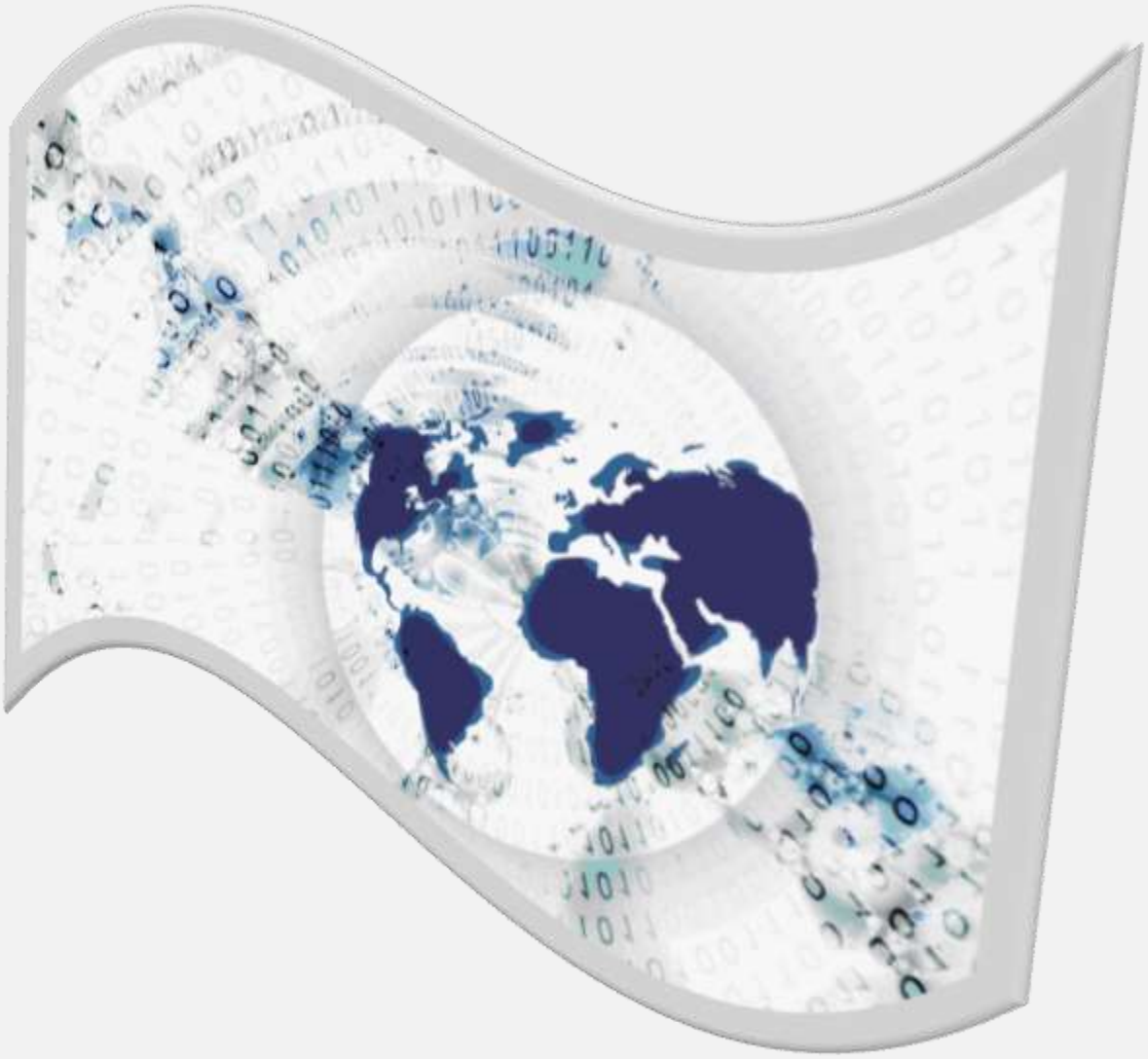
# مفهوم و کاربرد شبکه های کامپیوتر



***تألیف و گرد آوری: میثاق نوازنی***

**ویرایش ۱/۲**

هوالعالم

**سرشناسه : نوازنی، میثاق**

**عنوان و نام پدیدآور: مفهوم و کاربرد شبکه‌های کامپیوتر / تالیف و گردآوری میثاق نوازنی**

**مشخصات ظاهری: ۳۶۱ ص**

**شابک :۴-۲۵۰۷-۰۴-۶۰۰-۹۷۸**

**وضعیت فهرست نویسی: فیپا**

**موضوع: شبکه‌های کامپیوتری**

**موضوع: شبکه‌های کامپیوتری – معماری**

**رده بندی کنگره: TK۵۱۰۵/۵/ن۹م۷۱۳۹۳**

**رده بندی دیویی:۰۰۴/۶**

**شماره کتابشناسی ملی: ۳۷۳۴۲۸۰**

## فهرست مطالب:

# مقدمه

**قصد داشتم مقدمه ایی بنویسم 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 بر قد و قامتش بیندازد اما حساب و کتاب " من " با مقدمه های واجبِ 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 نخِ کدام مقدمه را بگیری و به کدام واجب برسی . واجب الوجود فقط نخِ مقدمه می دهد که پای " من " را به وادی عبادت بکشاند. این هم از کریمانه بودنش است . اما تو وقتی نخِ 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 سال۱۹۵۷ 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 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 سال۱۹۶۰ اولین شبکه کامپیوتری بین چهار کامپیوتر که دو تای آنها درMIT ، یکی در دانشگاه کالیفرنیا و دیگری در مرکز تحقیقاتی استنفورد قرار داشتند، راه اندازی شد. این شبکه آرپانت نامگذاری شد. در سال ۱۹۶۵نخستین ارتباط راه دور بین دانشگاه MIT و یک مرکز دیگر نیز برقرار گردید.در سال۱۹۷۰ 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 سال۱۹۲۷ 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 سال۱۹۲۷ نخستین نامه الکترونیکی از طریق شبکه منتقل گردید.در این سال ها حرکتی غیر انتفاعی به نام MERITکه 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 کامپیوتر ها، مجبور شدند تجهیزات لازم را خود طراحی کنند. آنان با طراحی تجهیزات واسطه**

**برای مینی کامپیوتر DEC PDP-۱۱ نخستین بستر اصلی یا Backdone شبکه کامپیوتری را ساختند. تا سال ها نمونه های اصلاح شده این کامپیوتر با نام[۱]PCP 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 مستقیما به سیستم MERIT متصل شوند.این، نخستین باری بود که کاربران می توانستند در هنگام برقراری ارتباط از خود بپرسند: کدام میزبان؟ازوقایع 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 سال۱۹۷۴با پیدایش پروتکل ارتباطی TCP/IP از مفهوم Switching Packetاستفاده گسترده تری شد. این پروتکل در سال ۱۹۸۲جایگزین 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 ۷۰میلادی از یکدیگر تفکیک شدند.در آدرس دهی ۳۲ بیتی اولیه، بقیه ۲۴بیت آدرس به میزبان در شبکه اشاره می کرد.در سال ۱۹۸۳سیستم نامگذاری دامنه ها (System Name Domain)به وجود آمد و اولین سرویس دهنده نامگذاری (Server Name)**

[۱] Processor Communications Pri

**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 می پردازیم.با این مفاهیم در بقیه این کتاب و همچنین در زندگی واقعی بارها و بارها 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**

**دراین درس به مفاهیم اصلی از ارتباطات شبکه و برخی از ساختارهایی که برای ساخت داده های شبکه مورد استفاده قرار می گیرند می پردازیم. انواع بسیاری از داده های شبکه وجود دارند از شبکه های سازمانی که توسط شرکت های بزرگ مورد استفاده قرار می گیرند 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 شبکه‌های رایانه‌ای به مجموعه قوانینی اطلاق می‌گردد که نحوهٔ ارتباطات را قانونمند می‌نماید. نقش پروتکل در کامپیوتر نظیر نقش زبان برای انسان است. برای مطالعه یک کتاب نوشته شده به فارسی می‌بایست 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 می‌شود. پروتکل اتصال بین دو ند، انتقال داده بین آن دو و تبادلات میان آنها را ممکن کرده و آن را کنترل می‌کند. پروتکل در ساده‌ترین حالت می‌تواند به عنوان قوانین ادارهٔ منطق، ترکیب و همزمانی ارتباطات در نظر گرفته شود. پروتکل‌ها ممکن در سخت‌افزار یا نرم‌افزار یا ترکیبی از این دو پیاده سازی شوند. پروتکل در پایین‌ترین سطح رفتار اتصال سخت‌افزاری را تعریف می‌کند. معنی لغوی پروتکل مجموعه قوانین است.**

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

- **شناسایی بستر فیزیکی اتصال (سیمی یا بی‌سیم) و یا تشخیص وجود نقطهٔ مقصد یا ند مقصد.**
- **توافق مراودهٔ اتصال (هندشیکینگ).**
- **مذاکره در مورد ویژگی‌های مختلف اتصال.**
- **شروع کردن و پایان دادن به پیام‌های رد و بدل شده و فراهم کردن نیاز ناشی از آن.**
- **پایان دادن به جلسهٔ گفتگو و یا اتصال.**
- **قالب بندی پیام‌ها.**

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

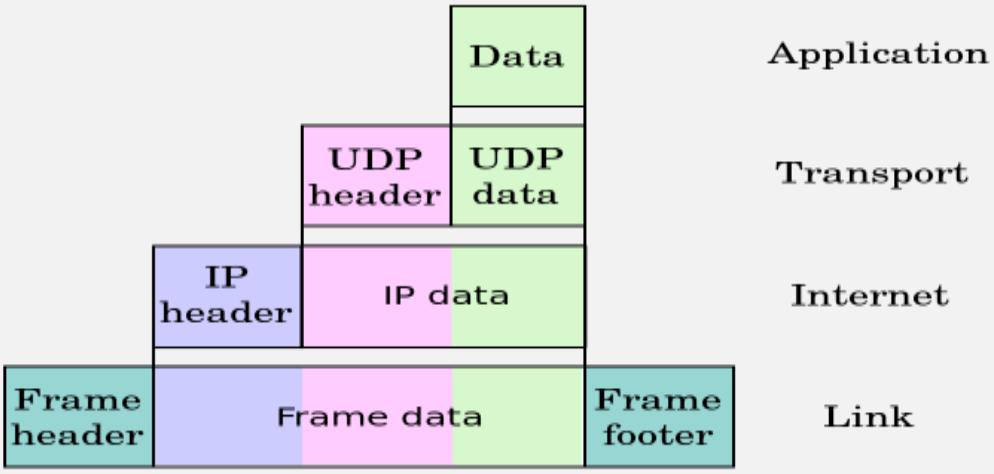
**پروتکل های پشته ای[1]**

**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 برا ی درک این مفهوم میتوان خشاب یک اسلحه را تصور کرد که هر گلوله وظیفه ای خواص 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.**




[1] protocol stack

**شبکه محلی [1]LAN:**

**ارتباط واتصال بیش از دو یا چند رایانه در فضای محدود یک سازمان از طریق کابل شبکه وپروتکل بین رایانه ها وبا مدیریت نرم افزاری موسوم به سیستم عامل شبکه را شبکه محلی گویند. کامپیوتر سرویس گیرنده باید از طریق کامپیوتر سرویس دهنده به اطلاعات وامکانات به اشتراک گذاشته دسترسی یابند. همچنین ارسال ودریافت 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 وپیاده سازی می باشند.**

**۲ - از سرعت نسبتا بالایی برخوردارند.**

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

**اجزای یک شبکه محلی عبارتند از :**

**الف - سرویس دهنده**

**ب - سرویس گیرنده**

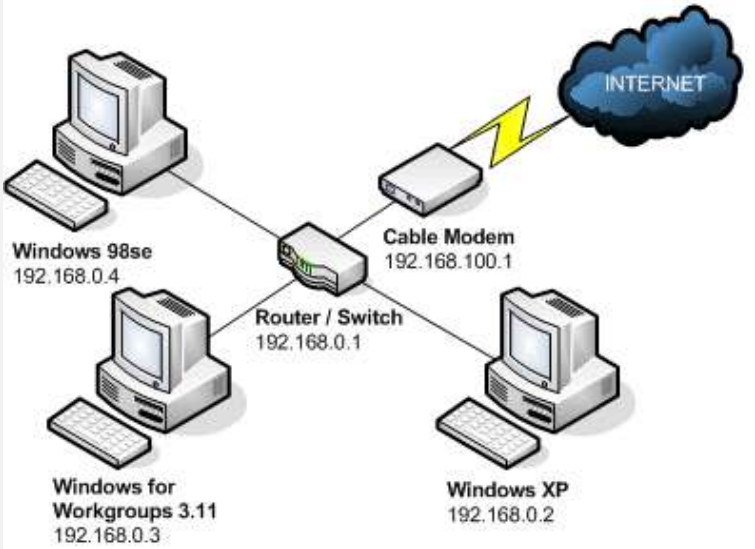
**ج - پروتکل**

**د- کارت واسطه شبکه**

**ط - سیستم ارتباط دهنده**

**شکل زیر یک شبکه محلی میباشد.**

[1] Local Area Network




**شبکه گسترده[1]WAN:**

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

**کاربردها**

**شبکه‌های گسترده برای اتصال شبکه‌های محلی یا دیگر انواع شبکه به یکدیگر استفاده می‌شوند. بنابراین کاربران و رایانه‌های یک مکان می‌توانند با کاربران و رایانه‌هایی در مکانهای دیگر در ارتباط باشند. بسیاری از شبکه‌های گسترده برای یک سازمان ویژه پیاده‌سازی می‌شوند و خصوصی**

[1] Wide Area Network

**هستند. بعضی دیگر به‌وسیله «سرویس دهندگان اینترنت» (ISP) پیاده‌سازی می‌شوند تا شبکه‌های محلی سازمانها را به اینترنت متصل کنند.**

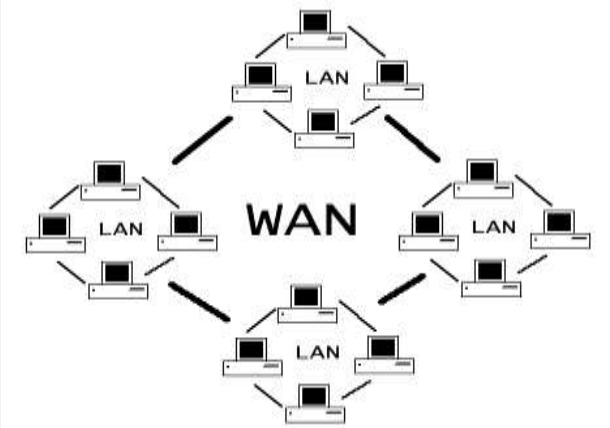
**انواع:**

**اغلب جهت پیاده‌سازی شبکه‌های گسترده از «خطوط استیجاری» استفاده می‌شود. در هر انتهای خط اجاره‌ای یک دستگاه «مسیریاب» قرار داده می‌شود که از یک طرف به شبکه محلی آن سمت و از طرف دیگر به‌وسیله یک هاب به آن سوی شبکه گسترده متصل است. خطوط استیجاری می‌تواند بسیار گران باشند. همچنین شبکه‌های گسترده می‌توانند بجای استفاده از آنها با استفاده از روشهای به صرفه‌تر «راهگزینی مداری» و «راهگزینی بسته» پیاده‌سازی شوند. « قرارداد»های شبکه مانند قرارداد مجموعه پروتکل اینترنت وظایف انتقال و آدرس‌دهی را برعهده دارند. قراردادهایی مانند «انتقال بسته بر سونت/اس‌دی‌اچ» (Packet over SONET/SDH)، «حالت انتقال ناهمگام»[1]، «راهگزینی برچسب چندقراردادی» (MPLS)، «رله فریم» (Frame Relay) اغلب به‌وسیله سرویس دهنده‌ها استفاده می‌شوند تا لینک‌هایی که در شبکه‌های گسترده استفاده می‌شوند را تامین کنند. قرارداد X ۲۵ یکی از قراردادهای اولیه مهم شبکه‌های گسترده بوده است و اغلب از آن به عنوان پدربزرگ قرارداد «رله فریم» یاد می‌شود، چراکه امروزه هنوز بسیاری از اصول و وظایف بنیادی پروتکل X ۲۵ با اعمال تغییراتی که جهت بروز درآوردن آن صورت گرفته در قرارداد «رله فریم» بکار می‌رود.**

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

**در شکل زیر یک شبکه wanرا ملاحضه میکنیدکه اینترنت را میتوانید چند هزار بزرگ تر از این تجسم کنید.**

[1] ATM




**شبکه باندپایه[1]:**

**شبکه باند پایه شبکه ای است که در آن کابل ( رسانه شبکه ) هربار تنها یک سیگنال را می تواند منتقل کند. شبکه های باند پایه در فواصل نسبتاکوتاهی 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.**

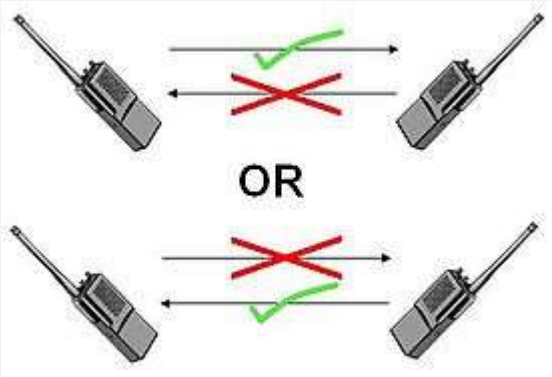
**باند پهن[2] :**

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

[1] Base Band
[2] Broad and

**فول دوبلکس و هالف دوپلکس**

**در هالف دوپلکس در یک واحد زمانی فقط می توانی یا ارسال یا دریافت نمایی ( مثه 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 wirlless **و مثل تلفن دوطرفه.**




**تصویری ساده از سامانه ارتباطی نیمه دوطرفه**

**تصویری ساده از یک سامانه ارتباطی کاملاً دوطرفه.**

**سامانه‌های 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 قطعه‌های مختلف شبکه را به هم وصل می‌کند و مسیری برای مبادله اطلاعات بین شبکه‌های محلی و زیرشبکه‌های مختلف را ارائه می کند. یک ستون فقرات شبکه‌های 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 "

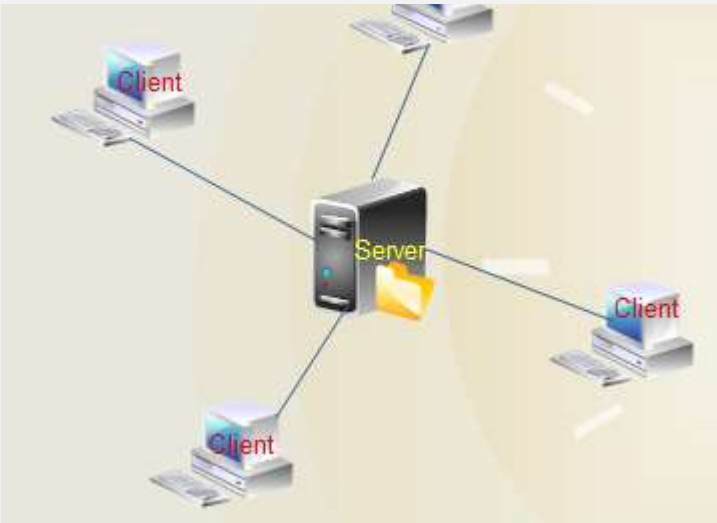
## ۱- شبکه نظیر به نظیر [۱]

**در این شبکه ایستگاه ویژه ای جهت نگهداری فایل های اشتراکی وسیستم 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 **وهم بعنوان** Client **عمل کند. در این مدل هر کاربر خود مسئولیت مدیریت وارتقاء 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 .**


[۱] Peer- to- Peer

## ۲- شبکه مبتنی بر سرویس دهنده [۱]

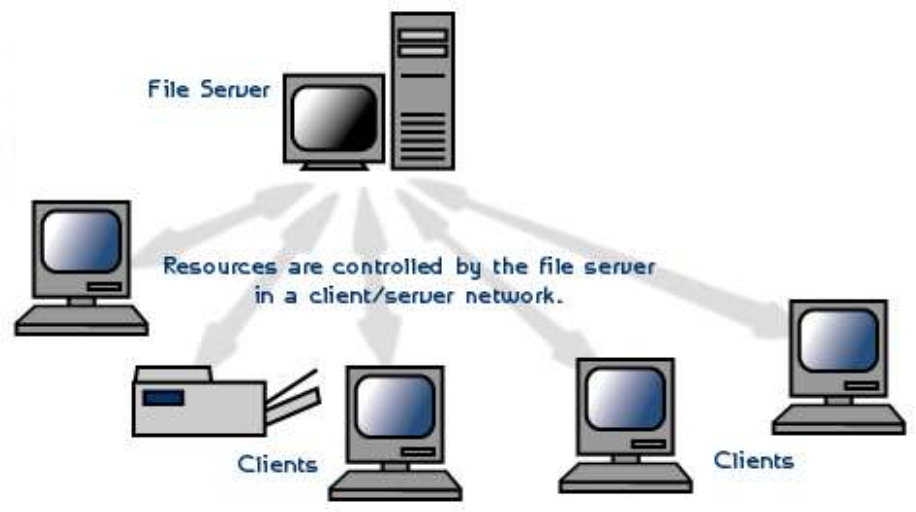
**در این مدل شبکه ، یک کامپیوتر بعنوان سرویس دهنده کلیه فایل ها ونرم افزارهای اشتراکی نظیر واژه پردازها، کامپایلرها ، بانک های اطلاعاتی وسیستم عامل شبکه را در خود نگهداری می کند. یک کاربر می تواند به سرویس دهنده دسترسی پیدا کرده وفایل های اشتراکی را از روی آن به ایستگاه خود منتقل کند.**




[۱] Server- 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.**




[۱] Client Server

**هر شبکه اساسا از سه بخش ذیل تشکیل می شود:**

**۱-ابزارهایی که به پیکربندی اصلی شبکه متصل می شوند به عنوان مثال : کامپیوتر ها ، 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 وترجمه سیگنال ها ی درون داد از شبکه از جانب یک ایستگاه کاری وترجمه وارسال 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 منحصربفرد باشد . قطعا تاکنون با آدرس های IP و یا MAC[۳] برخورد داشته اید و شاید این سوال برای شما مطرح شده باشد که اولا ضرورت وجود دو نوع آدرس چیست و ثانیا 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 استفاده از آدرس**

---

[۱] Hubs
[۲] Adaptor
[۳] Media Access Control

**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 هائی خاص شناسائی گردد . برای شناسائی یک کامپیوتر موجود در شبکه ، صرف داشتن یک آدرس** IP **به تنهائی کفایت نخواهد کرد.**

| **مدل** OSI | | |
|---|---|---|
| ... | | |
| Network Layer | **لایه سوم** | **آدرس** IP **در این لایه قرار دارد** |
| DataLink Layer | **لایه دوم** | **آدرس** MAC **در این لایه قرار دارد** |
| Physical Layer | **لایه اول** | |
| **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** MACAddress **یک کامپیوتر که بر روی آن کارت شبکه نصب شده است ، آن را با فرمت مبنای شانزده (** Hex **) ، مشاهده خواهید دید . مثلا** 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 با توجه به RFC ۱۷۰۰ | | | تعریف شده توسط تولید کننده | | |

**زمانی که یک تولید کننده نظیر اینتل ، کارت ها ی 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 ، قطعا 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 ).حتما 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 حتما 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:**

**وظیفهٔ 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 افزار انتقال 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 شدهٔ 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 آلومینیومی 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 کوآکس ۷۵ اهم معمولی)**

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

**کانال های ماهوارهای : در باندهای فرکانسی مختلف مثل :**

**باندC 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 درکامپیوترهای 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 رابطهٔ معروفی بنام رابطهٔ شانون وجود دارد:**

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

**ظرفیت کانال بر حسب بیت بر ثانیه :** C

**متوسط توان سیگنال :** S

**متوسط توان نویز :** N

**پهنای باند کانال بر حسب هرتز :** B

**به عنوان مثال اگر پهنای باند کانالهای تلفن معمولی را حداکثرتوان** 4KHz **فرض کنیم و نسبت سیگنال به توان نویز بطور تقریبی ۱۰۰۰ باشد ، در چنین حالتی با استفاده از خط تلفن حداکثر ۳۹۰۰۰ بیت در ثانیه را میتوان انتقال داد و انتقال اطلاعات در بالاتر از این نرخ منجربه خرابی داده ها خواهد شد. انتقال یک فایل یک مگابایتی از طریق خط تلفن با این سرعت حدوداً ۲۱۰ ثانیه طول خواهد کشید. که در جدول زیر مشخصات برخی از کانالهای انتقال با یکدیگر مقایسه شده است.معیار خطا در کانالهای انتقال ، احتمال بروز یک بیت خطا روی کانال تعریف میشود؛ یعنی احتمال آنکه در فرستنده بیت ۱ ارسال و در گیرنده اشتباهاً بیت ۰ آشکارسازی شود**

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

مقایسهٔ مشخصاتِ 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 مالتیپلکس 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 روش** FDM **با فرض آنکه حداکثر** N **ایستگاه در شبکه وجود داشته باشد؛ پهنای باند فرکانسی 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 روش TDM زمان به بازه های کوچکی تقسیم شده و هر ایستگاه مجاز است فقط در بازۀ زمانی 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 ۱۰۰۰/ ۱ دارد؛ یعنی :**

Peak Traffic ۱۰۰۰

Mean Traffic ۱

**با این توصیف برای تسهیم کانال های مشترک باید به سمت روشهای پویا حرکت کرد. در این استانداردهای IEEE ۸۰۲.x خصوص پروتکل های متفاوتی عرضه شده است.**

**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 عمدۀ 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 بایت 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**

**بیت توان فرد: ۰۱۱۰۱۰۰۱** ۱ Odd Parity

**بیت توان زوج :۰۱۱۰۱۰۰۱** ۰ Even Parity

**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:**

دادهٔ اصلی : 11100101

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

**ابتدا از روی دادهٔ اصلی یک چندجمله ای تولید میشود .نمایش ریاضی چند جملهای بدین صورت است که بیتها از راست به چپ ضرایب یک چند جمله ای قرار میگیرند که توان هر جمله را موقعیت بیت در رشته مشخص میکند .بدین صورت داده به صورت یک چند جمله ای نمایش داده خواهد شد .رشتهٔ بیت در این مثال برای سادگی عملیات ، هشت بیتی فرض شده است ، ولی در عمل این رشته میتواند دهها هزار بیت طول داشته باشد.**

$$D(X)=1*x^7+1*x^6+1*x^5+0*x^4+0*x^3+1*x^2+0*x+1$$
$$D(X)=x^7+x^6+x^5+x^2+1$$

**برای تولید کد** CRC **چند جمله ای** xn .D(X) **، بر یک" چندجملهای مولد "که بین گیرنده و فرستنده توافق میشود و اختیاری است ، تقسیم میگردد.(** n **بالاترین توان چندجمله ای مولد است)تقسیم در مبنای ۲ انجام میشود ، یعنی ضرایب جملات با توان مساوی با هم** XOR **خواهد شد و تفریق معنا ندارد .باقیماندۀ تقسیم به عنوان کدهای کنترل خطا در انتهای دادهها ارسال خواهند شد.**

CRC مولد = $X^2+1 \rightarrow 101$

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

$X^9+X^8+X^7+X^4+X^2 \,|\, X^2+1$

باقیمانده : $+1 = 01$

**در روشی که بخواهیم به صورت باینری ( به جای چند جمله ای ) کد** CRC**را حساب کنیم به تعداد بزرگ ترین توان 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 فر ایند (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 ازتباط 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**

[۱] **Physical**
[۲] **Data Link**

**می کند. (فریم داده یک ساختار منظم از داده می باشد که بسته های اطلاعاتی توسط این فریم به 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**

---

[۱] **Network**
[۲] **Transport**
[۳] **Session**

**خواست های کاربران توسط کانالهای ارتباطی در این لایه نگهداری می شود و در صورتی که یکی از کانال های ارتباطی به صورت کامل به مقصد نرسیده باشد مجددا همان کانال برای کاربر ارسال می گردد.**

**لایه نمایش[۱] :**

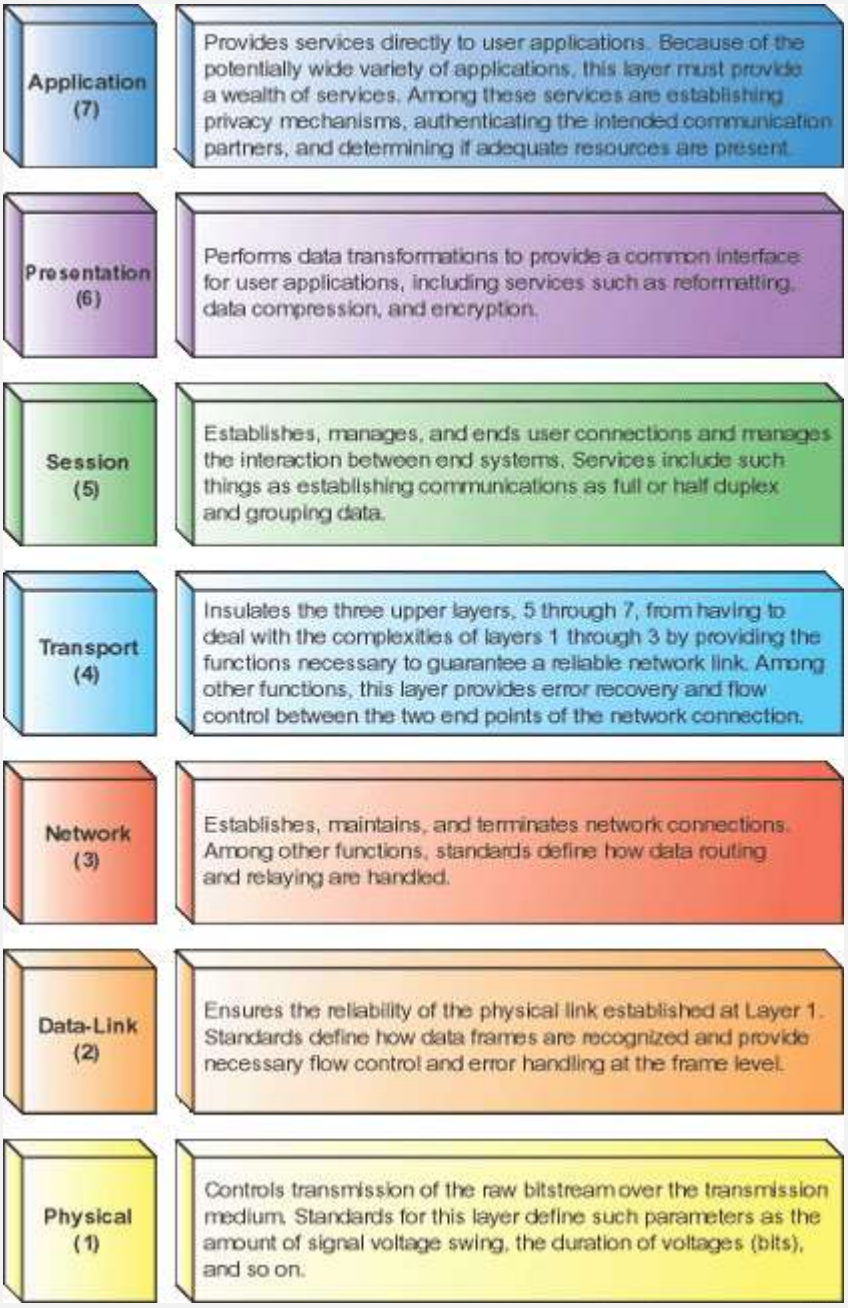
**این لایه وظیفه تبدیل پروتکل ها ، فشرده سازی اطلاعات برای کاهش حجم اطلاعات و مشخص کردن قالب تبادل اطلاعات بین دو کامپیوتر می باشد. به اصطلاح به این لایه ، لایه مترجم شبکه نیز گفته می شود و همچنین قسمتی از رمزگذاری اطلاعات در این لایه صورت می گیرد.**

**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.**

---

[۱] **Presentation**
[۲] **Application**




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

**لایه فیزیکی**

**لایه فیزیکی پایین‌ترین لایه در مدل مرجع ارتباط سامانه‌های باز (OSI) می‌باشد.این لایه وظیفه انتقال بیت ها از طریق کانال مخابراتی را عهده دار می‌شود. 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.**

**این رسانه‌ها را می‌توان در دو دسته تقسیم بندی نمود:**

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

**رسانه‌های فیزیکی مختلف با توجه پارامترهای پهنای باند، تأخیر انتشار، سهولت نصب و نگهداری مقایسه می‌گردند.**

**لایه پیوند داده:**

**لایه پیوند داده دومین سطح از مدل مرجع OSI می‌باشد. در این لایه بر روی الگوریتم‌های دستیابی به ارتباطات قابل اعتماد بین دو کامپیوتر همسایه بحث می‌شود.این لایه دارای وظایفی به قرار زیر است:**

- **ارائه سرویس‌های مشخص به لایهٔ شبکه**
- **مدیریت خطاهای انتقال**
- **تنظیم جریان داده ها**

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

**ارائه سرویس‌های مشخص به لایه شبکه**

**از مهم‌ترین وظایف لایه پیوند داده انتقال داده‌ها از لایه شبکه ی ماشین مبدا به لایه شبکه ماشین مقصد می‌باشد. سرویس هایی که لایه پیوند داده ارائه می‌کند، از سیستمی تا سیستم دیگر متفاوت است. اما از مهم‌ترین سرویس‌ها عبارت‌اند از:**

- **سرویس غیر متصل بدون تصدیق دریافت: این سرویس در اکثر LANها مورد استفاده قرار می‌گیرد.**
- **سرویس غیر متصل با تصدیق دریافت: این سرویس برای کانال های غیر اعتمادی مثل سیستم‌های بسیم مناسب است.**

**سرویس اتصال گرا با تصدیق دریافت:این سرویس که مناسب‌ترین سرویس این لایه است در سه مرحله انجام می‌گیرد.**

۱. **مقدار دهی متغییرهای لازم برای شمارش فریم‌ها و غیره.**
۲. **انتقال فریم ها.**
۳. **قطع اتصال و آزاد سازی متغییرها و بافر ها.**

**فریم بندی**

**جهت فریم بندی روش های زیر وجود دارد:**

۱. **شمارش کاراکتر ها: در این روش تعداد کاراکترهای فریم در یکی از فیلدهای سرآیند آن نوشته می‌شود. وقتی این فریم به مقصد برسد، لایه پیوند داده مقابل به کمک آنها فریم داده‌ای را مشخص می‌کند. شکل زیر مثالی از فریم بندی به کمک شمارش کاراکترها می‌باشد.**

**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.**

1. **بایت های پرچم، با لاگذاری بایت: در این روش فلگ هایی (نشانه) برای مشخص کردن ابتدا و انتهای فریم داده‌ای استفاده می‌شود. این روش هم مشکلات خاص خود را دارد چون که ممکن است بخشی از داده‌ها شامل بایت‌های پرچم قراردادی باشد.**
2. **پرچم‌های شروع و پایان، با لاگذاری بیت: در این شیوه هر فریم با طرح بیتی ۰۱۱۱۱۱۱۰ شروع می‌گردد و در سمت فرستنده به محض مشاهده ۵ بیت ۱ پشت سرهم یک ۰ قرار می‌دهد. عکس این رویداد در قسمت گیرنده رخ می‌دهد.**
3. **حالت‌های غیر مجاز کُدگذاری لایهٔ فیزیکی: در این روش در اصل نوعی افزونگی داریم. مثلاً در برخی LANها هر بیت داده با دو بیت فیزیکی نشان داده می‌شود: بیت ۱ با زوج بالا-پایین و بیت ۰ با زوج پایین-بالا.**

**در بسیاری از پروتکل‌های لینک داده برای اطمینان بیشتر از ترکیب روش های گفته شده استفاده می‌شود.**

**کنترل خطا:**

**جهت کنترل خطای دریافت اطلاعات معمولاً از دو مکانیزم استفاده می‌شود.**

- **تصدیق دریافت: گیرنده دریافت بسته را تصدیق می‌کند.**
- **استفاده از زمان سنج: هر بسته اگر در مدت زمان معینی به مقصد نرسید، دوباره ارسال می‌شود.**

**کنترل جریان:**

**برای یکی کردن سرعت ارسال و دریافت بسته‌های اطلاعاتی معمولاً از راهکارهای کنترل جریان استفاده می‌شود. در زیر چند راهکار را بیان می کنیم.**

- **کنترل جریان بر اساس بازخورد: گیرنده آمادگی خود را برای دریافت بسته‌ها اعلام می‌کند.**
- **کنترل جریان بر اساس نرخ**

**در شبکه‌های فراگیر که از یک کانال مشترک استفاده می‌کنند، اولین مسئله‌ای که پیش می‌آید 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 گوییم. حال وظیفه ما است که کلاه مان را قاضی نموده و به ایستگاه‌های مختلف این اجازه را بدهیم که از کانال مشترک موجود استفاده بهینه را ببرند. وظیفه این عمل در دنیای شبکه بر عهده نرم‌افزارهای زیر لایهٔ نظارت بر دسترسی به رسانه انتقال(MAC) می‌باشد. این زیر لایه وظیفه دارد که به کمک پروتکل هایی که در زیر ذکر می کنیم عدالت را بین ایستگاه‌ها پیاده نماید. حال فرض کنیم این کنترل انجام نگردد، در این حالت ممکن است چند ایستگاه به طور هم‌زمان نسبت به قرار دادن بسته‌های اطلاعاتی بر روی کانال اقدام کنند (این سناریو یادآور پاسخگویی هم‌زمان دانشجویان یک کلاس به یک پرسش استاد است). طبیعی است که هیچ یک از این بسته‌های اطلاعاتی قابل بازیافت توسط گیرنده(استاد در مثال ما) نیست. به این رویداد را تصادم گوییم. در کانال‌های شبکه می‌توان با برسی توان مصرفی یا اندازه گیری و مقایسهٔ پهنای پالس سیگنال دریافتی از کانال و مقایسهٔ آن با سیگنال ارسالی تشخیص داده می‌شود. این فرآیند تشخیص، به صورت آنالوگ انجام می‌شود.**

**پروتکل‌های ALOHA:**

**نورمن آبرامسون و همکاران او این روش را ایجاد کردند و دانشمندان دیگر به مرور به تکمیل آن پرداختند. دو نوع از این پروتکل‌ها در زیر بیان می‌شود.**

**:Pure ALOHA**

**در این روش که می‌توان آنرا بی منطق‌ترین حالت هم دانست، تمام ایستگاه‌ها به محض آماده شدن بسته‌های اطلاعاتی شان، آن را به کانال انتقال می فرستند. اگر تصادمی رخ نداد که چه بهتر ولی اگر تصادمی رخ داد آنرا توسط کانال مستقلی گزارش می‌کند. بعد از گزارش تصادم این**

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

**:Slotted ALOHA**

**در این روش از برش‌های زمانی استفاده می‌شود. 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 می‌گردد.**
- **در صورت بروز تصادم این فرایند دوباره تکرار می‌شود.**

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

**پروتکل‌های دسترسی چند گانه با قابلیت شنود سیگنال(CSMA):**

**به مجموعهٔ این پروتکل ها، پروتکل‌های شنود سیگنال نیز گوییم. این پروتکل‌ها مناسب تر بوده و کاربردی تر هستند. چراکه بدون تحقیق حکم صادر نمی‌کنند.**

**:Persistent CSMA**

**به این پروتکل که گاهی به آن ۱-**Persistent CSMA **نیز گوییم طبق الگوریتم زیر کار می‌کند.**

1. **به کانال گوش بده.**
2. **اگر کانال خالی است اطلاعات را به سوی کانال ارسال کن.**
    1. **در غیر اینصورت 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:**

1. **به کانال گوش بده.**
2. **اگر کانال خالی است اطلاعات را به سوی کانال ارسال کن.**
    1. **در غیر این صورت زمان تصادفی را صبر کن.**
3. **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 می‌گردد.**

**p-Persistent CSMA:**

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

1. **شنود کانال.**
2. **اگر کانال اشغال نیست آنرا با احتمال p به روی کانال قرار بده (این امر قطعی نیست).**
    1. **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 پروتکل‌ها 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 می‌گردد. این قطع شدن سریع، باعث می‌شود 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 **می‌تواند 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. **مسیر یابی**
۳. **کنترل گلوگاه ها**
۴. **کیفیت سرویس دهی**
۵. **به پیوستن شبکه‌های نا همگن**
۶. **آدرس دهی**

**پروتکل های عمومی لایه شبکه شامل:**

IP[1]

IPX[2]

ICMP[3]

**لایه شبکه** (networklayer) **عموما 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 دیگر می 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.**

[1] Internet Protocol
[2] Internetwork Packet Excahnge
[3] Internet Control Message Protocol

**بسته‌سازی**

**داده‌های پروتکل لایهٔ فوقانی، داخل برنامه‌ها و بسته‌هایی قرار می‌گیرند که نقش هم‌زمان دارند. هیچ نصب مداری قبل از ارسال بسته‌ها به یک میزبان نیاز نیست. ارتباط در این شرایط از نوع پروتکل بدون ارتباط می‌باشد. شبکه‌های تلفنی کلیدی می‌توانند نصب مدار را عملی سازند قبل از آن که تلفن زنگ بزند.**

**لایه انتقال (لایه چهار ):**

**لایه انتقال عموما به لایه چهارم مرجوع داده میشود.**

**مسولیت 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 شبکه‌های رایانه‌ای، لایه انتقال سرویس‌های ارتباطی مبدأ به مقصد یا** end-to-end **را برای برنامه‌های کاربردی موجود در معماری لایه بندی شده پروتکل‌ها و اجزاء شبکه فراهم می‌آورد. لایه انتقال سرویس‌های مطمئنی از قبیل پشتیبانی از جریان داده اتصال گرا، قابلیت اطمینان، کنترل جریان و تسهیم یا مالتی پلکسینگ را ارائه می‌نماید.**

**لایه‌های انتقال هم در (RFC ۱۱۲۲) مدلTCP/IP ، که مبنا و بنیان اینترنت می‌باشد، و هم مدل OSIموجود می‌باشند. تعریف لایه انتقال در این دو مدل کمی با یکدیگر تفاوت دارد.**

**معروف ترین پروتکل لایه انتقال پروتکل کنترل انتقال** Transmission Control Protocol(tcp) **می‌باشد. این پروتکل نام خود را از مجموعه پروتکل اینترنت یا همان** TCP/IP **وام گرفته‌است. از این پروتکل در انتقالات اتصال گرا استفاده می‌شود در حالیکه پروتکل بدون اتصال** UDP **برای انتقالات پیام ساده مورد استفاده قرار می‌گیرد.**TCP**پروتکل پیچیده تری است و این پیچیدگی به واسطه طراحی وضعیت محوری است که در سرویس‌های انتقالات قابل اطمینان و جریان داده تعبیه شده‌است.**

**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.**

**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.همچنین‌لایه 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 سیتم 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 . درمورد 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.**

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

**لایه نمایش[1]:**

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

[1] presentationlayer

**مختلفی برای نمایش اطلاعات استفاده کنند.در حالی که یک سیستم امکان دارد از** ASCII **یا** EBCIDC , **سیستم دیگر از** UNICODE **استفاده کند.ازاینرو 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 اطلاعات‌لایه نمایش مدل مرجع** OSI **را که بنیاد نهاده شده اند را نشان می دهد.**

| قالبندی های اطلاعات | هدف |
|---|---|
| ASCII,EBCIDC,UNICODE,RTF | **قالب بندی های رمزگذاری متن** |
| MPEG,AVI,Quick Time | **قالب بندی های رمزگذاری ویدوئی** |
| JPEG,PNG,TIFF | **قالبندی های گرافیکی** |
| MIDI | **قالب صدا** |

**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,POP۳,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 معمولا 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 تقاضا برای اطلاعات و سپس چه کاری باید با پاسخ (اطلاعاتی که تقاضا شده بود)انجام دهد.**

**در مورد جستجوی یک وب سایت توسط یک کاربر , جستجو گر 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.**

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

**درس ۳**

**مدل TCP/IP یا Internet protocol /Transmission Control Protocol**

**مفهوم TCP/IP:**

**TCP/IP مجموعه قراردادهایی هستند که در جهت اتصال کامپیوتر ها 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 IP , ICMP 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 قرارداشتن: انتقال فایل (FTP) و مدیریت پست (SMTP) و بقیه برنامه های کاربردی می باشد.**

**مقایسه مدلهای 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 پارامتر های 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 شئ گرا هستند.هر شئ، 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 شئ در اختیار دیگران می گذارد.ورودی ها و خروجی های شئ واسط آن با دنیای خارج هستند. کد اجرایی شئ 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 داردو 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 درلایه 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 بسیارمهم 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 نا مناسب 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**

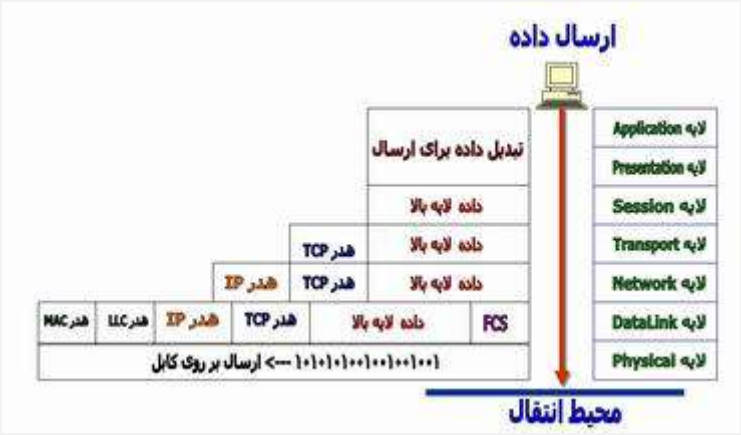
**استانداردها دارد که ملاقات فیل ها معروف استد. این نظریه میزان فعالیت های حول یک موضوع جدید را نشان می دهد.وقتی موضوعی برای اولین بار کشف می شود، گرداگرد آن سیلی از فعالیت های تحقیقی ( به شکل بحث، مقاله و سخنرانی) فرا می گیرد.بعد از مدتی این فروکش می کند و بعد از اینکه صنعت به این موضوع علاقه مند شد، موج سرمایه گذاری ها از پی می آید. بسیار مهم است که در محل تلاقی این دو فیل ( موج تحقیق و موج سرمایه گذری) 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 –ازمسیرهای 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 بر دارد.، قدمی که هرگز برداشته نشد د** 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 سرعتهای 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 وموجب 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" **وکابل فیبر نوری "**Fiber- Optic

**توپولوژی کابل های شبکه:**

**مبانی شبکه یا توپولوژی شبکه ، الگوی مورد استفاده برای اتصال رایانه ها و دستگاه های دیگر با استفاده ازشبکه 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 سوییچها 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.**

[۱] Transmission Medium

**۱- توپولوژی ستاره ای[1]:**

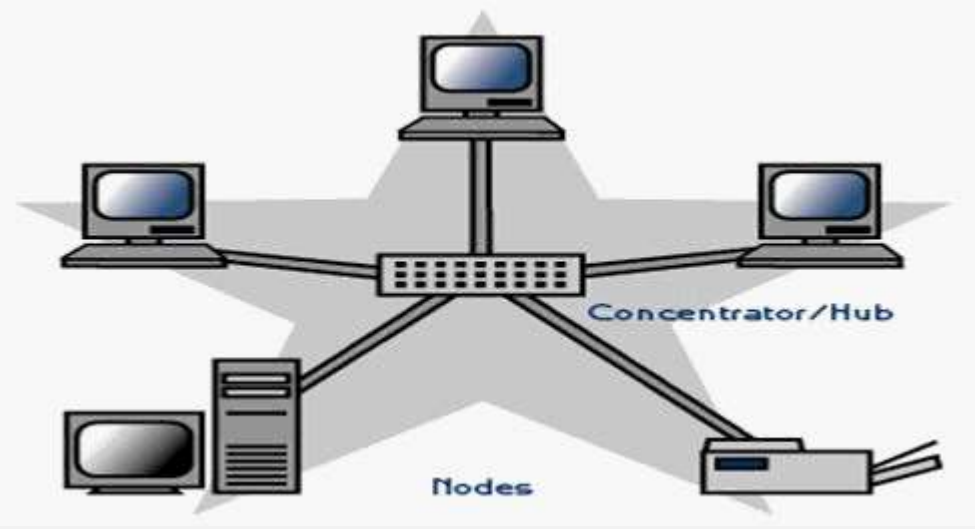
**در این توپولوژی ، کلیه کامپیوتر ها به یک کنترل کننده مرکزی با هاب متصل هستند. هرگاه کامپیوتری بخواهد با کامپیوتر ی دیگری تبادل اطلاعات نماید، کامپیوتر منبع ابتدا باید اطلاعات را به هاب ارسال نماید. سپس از طریق هاب آن اطلاعات به کامپیوتر مقصد منتقل شود. اگر کامپیوتر شماره یک بخواهد اطلاعاتی را به کامپیوتر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




[1] Star

**توپولوژی حلقوی[1]::**

**این توپولوژی توسط شرکت IBM اختراع شد وبهمین دلیل است که این توپولوژی بنام IBM Tokenring " مشهور است.**

**در این توپولوژی کلیه کامپیوتر ها 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 وآن کامپیوتر آدرس اطلاعات رابرای خود کپی می کند، آنگاه اطلاعات را به کامپیوتر بعدی در حلقه منتقل خواهد کرد وبهمین 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:**

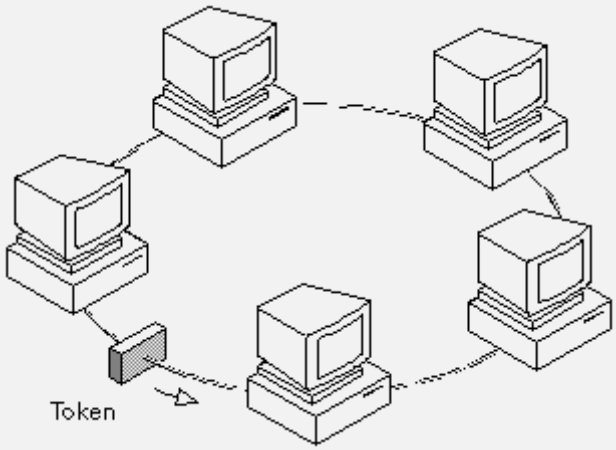
**اگر یک کامپیوتر از کار بیفتد ، کل شبکه متوقف می شود.**

**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.**

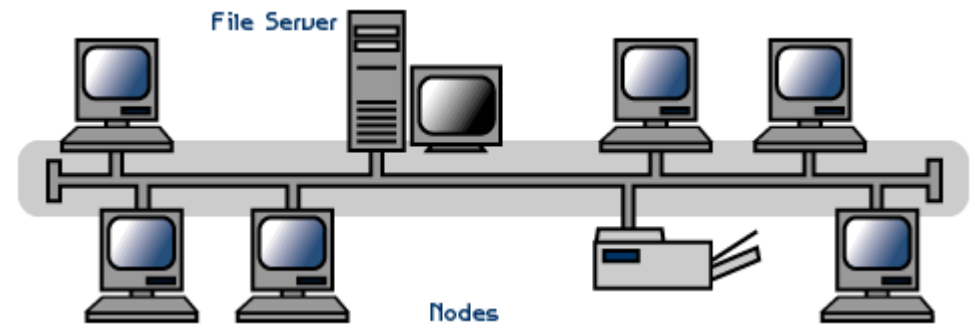
[1] Ring




**توپولوژی اتوبوسی [1]:**

**در یک شبکه خطی چندین کامپیوتر به یک کابل بنام اتوبوسی متصل می شوند. در این توپولوژی ، رسانه انتقال بین کلیه کامپیوتر ها مشترک است. یکی از مشهورترین قوانین نظارت بر خطوط ارتباطی در شبکه های محلی اترنت است. توپولوژی اتوبوس از متداوالترین توپولوژی هایی است که در شبکه محلی مورد استفاده قرار می گیرد. سادگی ، کم هزینه بودن وتوسعه 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 کامپیوتر های شبکه می باشد قطع شود، کل شبکه از کار خواهد افتاد.**

[1] Bus

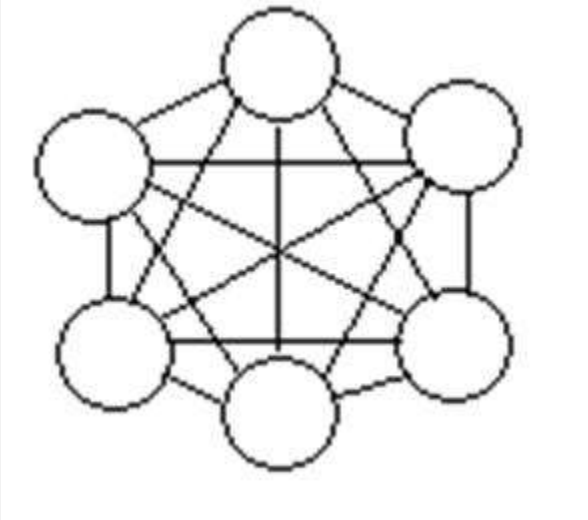



**توپولوژی توری :[1]**

**در این توپولوژی هر کامپیوتری مستقیما به کلیه کامپیوترهای شبکه متصل می شود. مزیت این توپولوژی آن است که هر کامپیوتر با سایر کامپیوتر ها ارتباطی مجزا دارد. بنابراین ، این توپولوژی دارای بالاترین درجه امنیت واطمینان 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، مخصوصا زمانیکه تعداد ایستگاه ها 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 ونه می باشد. تعداد کابل های مورد نیاز در این توپولوژی با رابطه N(N-۱)/۲ محاسبه می شود که در آن N تعداد ایستگاه های شبکه می باشد.**

[1] Mesh



**توپولوژی درختی :[1]**

**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 در ختی است : زیرا کلیه ایستگاه ها را به یکدیگر متصل می کند. وظیفه هاب دریافت اطلاعات از یک ایستگاه و تکرار وتقویت آن اطلاعات وسپس ارسال آنها به ایستگاه دیگر می باشد.**

**توپولوژی ترکیبی[2]:**

**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.**

[1] Tree
[2] Hybrid

**کابل شبکه:**

**کابل شبکه، رسانه ای است که از طریق آن، اطلاعات از یك 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 یك 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 یك 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 انعطاف‌پذیری.**

**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 می‌نماید.**

**قسمتهای یک کابل Coaxial:**

**(۱) ConductingCore یا هسته مرکزی که معمولاً از یك رشته سیم جامد مسی تشکیل می‌گردد.**

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

**(۳) Copper Wire Mesh که از سیم‌های بافته شده تشکیل می‌شود و کار آن جمع‌آوری امواج الکترومغناطیسی است.**

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

**کابل Coaxial به دو دسته تقسیم می‌شود:**

- Thin net: **کابلی است بسیار سبك، انعطاف‌پذیر و ارزان قیمت، قطر سیم در آن ۶ میلیمتر معادل ۰/۲۵ اینچ است. مقدار مسیری که توسط آن پشتیبانی می‌شود 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 پلاستیك بوده و بخار را از هسته مرکزی دور می‌سازد.**

**رایج‌ترین نوع اتصال دهنده (**connector**) مورد استفاده در کابل** coaxial، Concelman (BNC) -Bayonet-Neill **می‌باشد.**

**انواع مختلفی از سازگار کننده‌ها برای**BNC**ها وجود دارند شامل:** Tconnector , Barrel connector

**در شبکه هایی با توپولوژی اتوبوسی از کابل**coaxial **استفاده می‌شود.**

**استفاده از کابل** coaxial **در شبکه اتوبوسی:**

**باید دانست که از عبارتهایی مانند "۵**Base**۱۰ " برای توضیح اینکه چه کابلی در ساخت شبکه بکار رفته استفاده می‌گردد. 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**)می‌باشد. همچنین "۲**Base**۱۰" یعنی اینکه از کابل** Thinnet **استفاده شده، روش انتقال** Baseband **و سرعت انتقال ۱۰ مگابیت در ثانیه است.**

**در طراحی جدید شبکه معمولاً از کابلهای** Twisted Pair **استفاده می‌گردد. قیمت آن ارزان بوده و از نمونه‌های آن می‌توان به کابل تلفن اشاره کرد. این نوع کابل که از چهار جفت سیم بهم تابیده تشکیل می‌گردد،**

**خود به دو دسته تقسیم می‌شود:**

UTP:[1]**کابل ارزان قیمتی است که نصب آسانی دارد و برای شبکه‌های** LAN **سیم بسیار مناسبی است، همچنین نسبت به نوع دوم کم‌وزن‌تر و انعطاف‌پذیرتر است. مقدار سرعت دیتای عبوری از آن ۴ مگابیت در ثانیه تا ۱۰۰ مگابیت در ثانیه می‌باشد. این کابل می‌تواند تا مسافت حدوداً ۱۰۰ متر یا ۳۲۸ فوت را بدون افت سیگنال انتقال دهد. کابل مذکور نسبت به تداخل امواج الکترومغناطیس[2] 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 می‌شود، اما در کابل شبکه اتصال دهنده‌ای با شماره۴۵** RJ **بکار می‌رود که دارای هشت مکان برای هشت رشته سیم است.**

**کابل** Utp **و** Stp

**کابل** UTP **دارای پنج طبقه مختلف است (که البته امروزه۶** CAT **و۷** CAT**هم اضافه شده است)** ۱ CAT **یا نوع اول کابل** UTP **برای انتقال صدا بکار می‌رود، اما۲** CAT**تا۵** CAT **برای انتقال دیتا در شبکه‌های کامپیوتری مورد استفاده قرار می‌گیرند و سرعت انتقال دیتا در آنها به ترتیب عبارتست از: ۴ مگابیت در ثانیه، ۱۰مگابیت در ثانیه، ۱۶مگابیت در ثانیه و ۱۰۰مگابیت در ثانیه.**

**برای شبکه‌های کوچك و خانگی استفاده از کابل ۳**CAT**توصیه می‌شود.**

[1] Unshielded Twisted Pair
[2] Magnatic InterferenceElectrical

**STP :[1]در این کابل سیم‌های انتقال دیتا مانند UTP هشت سیم و یا چهار جفت دوتایی هستند. باید دانست که تفاوت آن با UTP در این است که پوسته‌ای به دور آن پیچیده شده که از اثرگذاری امواج بر روی دیتا جلوگیری می‌کند. از لحاظ قیمت، این کابل از UTP گرانتر و از فیبر نوری ارزان‌تر است. مقدار مسافتی که کابل مذکور بدون افت سیگنال طی می کند برابر با ۵۰۰ متر معادل ۱۶۴۰ فوت است.**

**در شبکه‌هایی با توپولوژی اتوبوسی و حلقه‌ای از دو نوع اخیر استفاده می‌شود. گفته شد که در این نوع کابل، ۴ جفت سیم بهم تابیده بکار می‌رود که از دو جفت آن یکی برای فرستادن اطلاعات و دیگری برای دریافت اطلاعات عمل می‌کنند.**

**در شبکه‌هایی با نام اترنت سریع [2]دو نوع کابل به چشم می‌خورد:**

**۱۰۰ Base TX :یعنی شبکه‌ای که در آن از کابل UTP نوع۵ Cat استفاده شده و عملاً دو جفت سیم در انتقال دیتا دخالت دارند (دو جفت دیگر بیکار می‌مانند)، سرعت در آن ۱۰۰ مگابیت در ثانیه و روش انتقال Baseband است.**

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

**کابل فیبر نوری کاملاً متفاوت از نوع Coaxial و Twisted Pair عمل می‌کند. به جای اینکه سیگنال الکتریکی در داخل سیم انتقال یابد، پالسهایی از نور در میان پلاستیك یا شیشه انتقال می‌یابد. این کابل در برابر امواج الکترومغناطیس کاملاً مقاومت می‌کند و نیز تأثیر افت سیگنال بر اثر انتقال در مسافت زیاد را بسیار کم در آن می‌توان دید. برخی از انواع کابل فیبر نوری می‌توانند 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 می‌گیرد:**

---

[1] Shielded Twisted Pair
[2] Fast Ethernet

**۱-** Single Mode : **که دراین کابل دیتا با کمك لیزر انتقال می‌یابد و بصورت ۸/۳/۱۲۵ نشان داده می‌شود که در آن ۸/۳ میکرون قطر فیبر نوری و ۱۲۵ میکرون مجموع قطر فیبر نوری و محافظ آن می‌باشد. این نوع که خاصیت انعطاف‌پذیری کم و قیمت بالایی دارد برای شبکه‌های تلویزیونی و تلفنی استفاده می‌گردد.**

**۲-:** Multi Mode **که در آن دیتا بصورت پالس نوری انتقال می‌یابد و بصورت ۶۲/۵/۱۲۵ نشان داده می‌شود که در آن ۶۲/۵ میکرون قطر فیبر نوری و ۱۲۵ میکرون مجموع قطر فیبر نوری و محافظ آن می‌باشد. این نوع مسافت کوتاهتری را نسبت به** Single Mode **طی می‌کند و قابلیت انعطاف‌پذیری بیشتری دارد. قیمت آن نیز ارزان‌تر است و در شبکه‌های کامپیوتری استفاده می‌شود. بطورکلی کابل فیبر نوری نسبت به دو نوع** Coaxial **و** Twisted pair **قیمت بالایی دارد و نیز نصب آن نیاز به افراد ماهری دارد.**

**شبکه‌های** Base FX **۱۰۰شبکه‌هایی هستند که در آنها از فیبر نوری استفاده می‌شود، سرعت انتقال در آنها ۱۰۰ مگابیت در ثانیه بوده و روش انتقال** Baseband **می‌باشد. امروز، با پیشرفت تکنولوژی در شبکه‌های فیبر نوری می‌توان 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 ها ی 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 اشتراك برنامه ها از نظر سخت افزاری احتیاج به کارت شبکه یا** LAN Card **دارند. که بطور معمول در بازاردو نوع کارت معمول می باشد. یک قسم آنها کارتهایِ ۱۰ در ۱۰ بوده و قسم دیگرکارتهای 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 منحصربفرد 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 افراری 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 مجموعا قبل ازانتقال 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 کدگذاری 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 وارسال 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 درشبکه همه بسته های فرستاده شده روی شبکه رادریافت 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 وآماده 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 وکارت شبکه بصورت موازی انجام می شود، مگر در کارتهای شبکه Usb که ارتباط باکامپیوتر 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 دسترسی رسانه (mac) : از وظایف دیگر کارت شبکه پیاده سازی مکانیزم mac می باشد که پروتکل لایه پیوند-داده از آن برای منظم کردن دسترسی 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 نهایتا نصب درایور کارت می باشد که بسته به توانایی**

**ها و نوع کامپیوتر از نظر قدیمی یا جدید بودن این پروسه می تواندبسیار ساده و یا بسیار پر دردسر باشد.**

**توجه: قبل از لمس کردن قطعات داخلی کامپیوتر یا درآوردن کارت شبکه از بسته محافظ مخصوص آن، دست خود را با ورقه فلزی دور منبع تغذیه کامپیوتر تماس دهید یا اینکه از دستکش های مخصوص استفاده کنید تابدلیل 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 . 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 عضوء 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 عضوء یک** Collision Domain **یکسان می باشند. تمامی کامپیوترهائی که با استفاده از هاب به یکدیگر متصل می شوند ، عضوء 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** doamin **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 کارائی یک شبکه از تجهیزات سخت افزاری متعددی استفاده می شود . سوئیچ ها** collisiondomain **مجزائی را ایجاد می نمایند ولی در خصوص** broadcastdoamin **بدین شکل رفتار نمی نمایند . روترها ،** broadcastdomain **و** collision domain **مجزائی را ایجاد نموده و در مقابل هاب ، قادر به ایجاد** broadcast doamin **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 ارزانترین 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 صرفا" این اطمینان را ایجاد می نمایند که فریم های داده بر روی هر یک از پورت ها ، تکرار خواهد شد.**

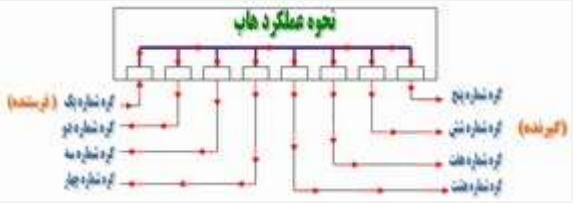
**گره هائی که یک اترنت و یا** FastEthernet **را با استفاده از قوانین** CSMA/CD **به اشتراک می گذارند ، عضوء یک** Collision Domain **مشابه می باشند . این بدان معنی است که تمامی گره های متصل شده به هاب بخشی از** Collision domain **مشابه بوده و زمانی که یک** collision **اتفاق می افتد ، سایر گره های موجود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

**کامپیوترها و یا گره های متصل شده به هاب از کابل های** UTP[1] **استفاده می نمایند. صرفا" یک گره می تواند به هر پورت هاب متصل گردد. مثلا" با استفاده از یک هاب هشت پورت ، امکان**

[1] Unshielded 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 ، عضوء 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 فعالیتی 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 کنیداما 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 اید. شما باید از دستگاه هایی استفاده کنید که این مشکلات را برای شما حل کنند. در این فصل به بررسی برخی از اجزای پیچیده تر برای اتصالهای وسیعتر می پردازیم. با استفاده از این ابزار، شما می توانید اندازه شبکه را بدون کاهش کارایی آن را افزایش دهد، حتی زمانی که ترافیک شبکه بالا رود.**

**درس ۱**

**Switching**

**سوئیچ برای اتصال دستگاهای مختلف از قبیل رایانه, مسیریاب, چاپگرهای تحت شبکه، دوربین‌های مدار بسته و .... در شبکه‌های کابلی مورد استفاده واقع می‌شود.**

**در وجه ظاهری سویئچ همانند جعبه ایست متشکل از چندین درگاه اترنت که از این لحاظ شبیه هاب (Hub) می‌باشد، با وجود آنکه هر دو این‌ها وظیفه برقراری ارتباط بین دستگاه‌های مختلف را بر عهده دارند، تفاوت از آنجا آغاز می‌شود که هاب بسته‌های ارسالی از طرف یک دستگاه را به همهٔ درگاه‌های خود ارسال می‌کند و کلیه دستگاه‌های دیگر علاوه بر دستگاه مقصد این بسته‌ها را دریافت می‌کنند در حالیکه در سوئیچ ارتباطی مستقیم بین درگاه دستگاه مبدا با درگاه دستگاه مقصد برقرار شده و بسته‌ها مستقما فقط برای آن ارسال می‌شود.**

**این خصوصیت از انجا می‌آید که سویئچ می‌تواند بسته‌ها را پردازش کند، در سویئچ‌های معمولی که به سویئچ لایه دوم معروفند این پردازش تا لایه دوم مدل OSI پیش می‌رود و نتیجه این پردازش جدولی است که در سویئچ با خواندن آدرس سخت‌افزاری (MAC) فرستنده بسته و ثبت درگاه ورودی تشکیل می‌شود.**

**سویئچ با رجوع به این جدول عملیات آدرس دهی بسته‌ها در لایه دوم را انجام می‌دهد، بدین معنا که این جدول مشخص می‌کند بسته ورودی می‌بایست فقط برای کدام درگاه ارسال شود.**

**در شبکه‌های بزرگ Switchها جدول‌های خود را به اشتراک می‌گذارند تا هر کدام بدانند چه دستگاهی به کدام سویئچ متصل است و با این کار ترافیک کمتری در شبکه ایجاد کنند.**

**سوئیچ بطور معمول در لایه دوم مدل OSI کار می‌کند ولی سوئیچ‌هایی با قابلیت کارکرد در لایه‌های مختلف حتی لایه هفتم هم وجود دارد. پرکاربردترین سوئیچ در بین لایه‌های مختلف بجز لایه دوم می‌توان به سوئیچ لایه سه اشاره کرد که در بسیاری موارد جایگزین مناسبی برای روتر می‌باشند. از سوئیچ می‌توان در یک شبکه خانگی کوچک تا در شبکه‌های بزرگ با Backboneهای چند گیگابایتی استفاده کرد.**

**برخی مزیت‌های و قابلیت‌های سوئیچ :**

- **امکان برقراری ارتباط بین ده‌ها و گاهی صدها دستگاه را به طور مستقیم و هوشمند به ما می‌دهد.**
- **امکان برقرای ارتباط با سرعت بسیار بالا را فراهم می‌کند.**
- **امکان نظارت و مدیریت بر عملکرد کاربران را فراهم می‌کند.**
- **امکان کنترل پهنای باند مصرفی کاربران را فراهم می‌کند.**
- **امکان تفکیک شبکه به بخش‌های کوچکتر و مشخص کردن نحوه دسترسی افراد به قسمت‌های مختلف را فراهم می‌کند.**
- **و ده‌ها 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 صرفا" 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 صرفا" با سوئیچ ارتباط برقرار می نماید ( گره ها مستقیما" 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 ، صرفا" از سوئیچ به تنهائی استفاده نمی نمایند. در این نوع شبکه ها از ترکیب هاب و سوئیچ استفاده می گردد. مثلا" 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 معمولا" در لایه دوم** (Data layer)**مدل** OSI**فعالیت می نمایند.در لایه فوق امکان استفاده از آدرس ها ی فیزیکی وجود دارد. روتر در لایه سوم** (Network) **مدل** OSI **فعالیت می نمایند. در لایه فوق از آدرس های** IP **ر** IPX **و یا** Appeltalk**استفاده می شود. 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 خطاء 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 خطاء** (CRC ) **و سایر مسائل مربوطه را قبل از ارسال اطلاعات انجام خواهند داد. در صورتیکه بسته اطلاعاتی دارای خطاء 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 خطاء 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 اترنت از سیستمی 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 ( سگمنتA )، اطلاعاتی را برای کامپیوتر دیگر ( گرهB )در سگمنت دیگر ( سگمنتC )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 Aآگاهی 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 اخیرا" یکی از گره های موجود در آن اقدام به ارسال اطلاعات نموده است .) ارسال می کند.فرآیند ارسال یک بسته اطلاعاتی توسط سوئیچ ، بمنظور یافتن یک گره خاص برای تمام سگمنت ها ، Floodingنامیده 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 مستقیما" 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 نمائید. 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 مستقیما" 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 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 آشفتگی 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 " آشفتگی انتشار" و سایر اثرات جانبی در رابطه با** Looping **شرکت** DEC **پروتکلی با نام**[1]STP **را ایجاد نموده است . پروتکل فوق با مشخصه ۸۰۲٫۱ توسط موسسه** IEEE **استاندارد شده است** Spanning tree **از الگوریتم**[2]STA **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:**

[1] Spanning-tree Protocol
[2] Spanning-tree algoritm

**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[1] **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 برا ی 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 تفسیم بر ۱۰ ) . بمنظور هماهنگ شدن با افزایش سرعت شبکه های کامپیوتری استاندارد** Cost **نیز اصلاح می گردد. ( 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[2] **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

[1] Bridge ID
[2] Bridge protocol data units

Root bridge**باشد ، مقدار** cost **بصورت (۱۹+۱۹+۰=۳۸) بدست می آید .سگمنتی 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 اراسال 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 بهمراه** 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 قبلا" ذخیره کرده اند، جایگزین می نمایند .در صورتیکه** Root BID**ذخیره شده دارای مقدار کمتری باشد ، یک** BPDU **برای سوئیچ جدید بهمراه** 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 Portsنامیده 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 صرفا" یک نمونه از پورت های فوق ، تمام مشکلات مربوط به** Loopingبرطرف 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 سسگمنت ) برای سایر سوئیچ ها،** Path Costبرای 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 مقادر کمتر** BID **اتخاب 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** roor bridge **که بمنزله ریشه و سایر سوئیچ ها بمنزله برگ خواهند بود. هر سوئیچ با استفاده از** Root Ports **قادر به ارتباط با** root bridgeبوده 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 اخیرا" برخی از تولیدکنندگان سوییچ، 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 معمولا" 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 روترهائی می باشند که بمراتب از روتر ها سریعتر بوده ( با توجه به استفاده از سخت افزارهای اختصاصی سوئیچینگ ) و دارای قیمت ارزانتری 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 .**

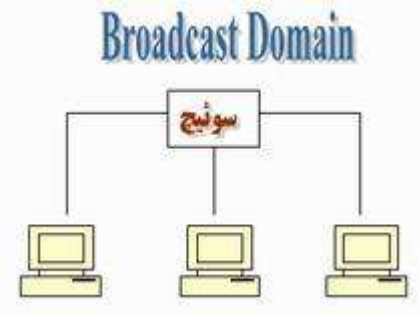
**همانگونه که ملاحظه گردید ، در طراحی سوئیچ های LAN از تکنولوژی های متفاوتی استفاده می گردد. نوع سوئیچ استفاده شده ، تاثیر مستقیم بر سرعت و کیفیت یک شبکه را بدنبال خواهد داشت.**

**VLAN چیست ؟**

**VLAN[1] ، یکی از جدیدترین و جالبترین تکنولوژی های شبکه است که اخیرا" مورد توجه بیشتری قرار گرفته است . رشد بدون وقفه شبکه های LAN و ضرورت کاهش هزینه ها برای تجهیزات گرانقیمت بدون از دست دادن کارآئی و امنیت ، اهمیت و ضرورت توجه بیشتر به VLAN را مضاعف نموده است .**

**وضعیت شبکه های فعلی :**

**تقریبا" 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 .**




[1] VirtualLocal 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** braodcast **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 عملا" از پهنای باند شبکه،استفاده مطلوب نخواهد شد. تمامی ایستگاههای متصل شده به یک سوئیچ ، پیام های** Braodcast **را دریافت می نمایند . چراکه تمامی آنان بخشی از یک** Broadcast doamin **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** Braodcast **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 افرادیکه جدیدا" با دنیای شبکه آشنا شده اند ، اغلب دارای برداشت مناسبی در این خصوص نمی باشند و اینگونه استنباط نموده اند که صرفا" می بایست به منظور فعال نمودن** VLAN **، یک نرم افزار اضافه را بر روی سرویس گیرندگان و یا سوئیچ نصب نمایند . ( برداشتی کاملا" 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 (**VLAN۱ **و** VLAN۲**) . زمانی که ایستگاه شماره یک متعلق به** VLAN۱ **، یک پیام** Braodcast **را ارسال می نماید ( نظیر :** FF:FF:FF:FF:FF:FF **) ، سوئیچ موجود آن را صرفا" برای ایستگاههای شماره دو وسه فوروارد می نماید . در چنین مواردی سایر ایستگاههای متعلق به** VLAN۲ **، آگاهی لازم در خصوص پیام های** broadcast **ارسالی بر روی** VLAN۱ **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 .**

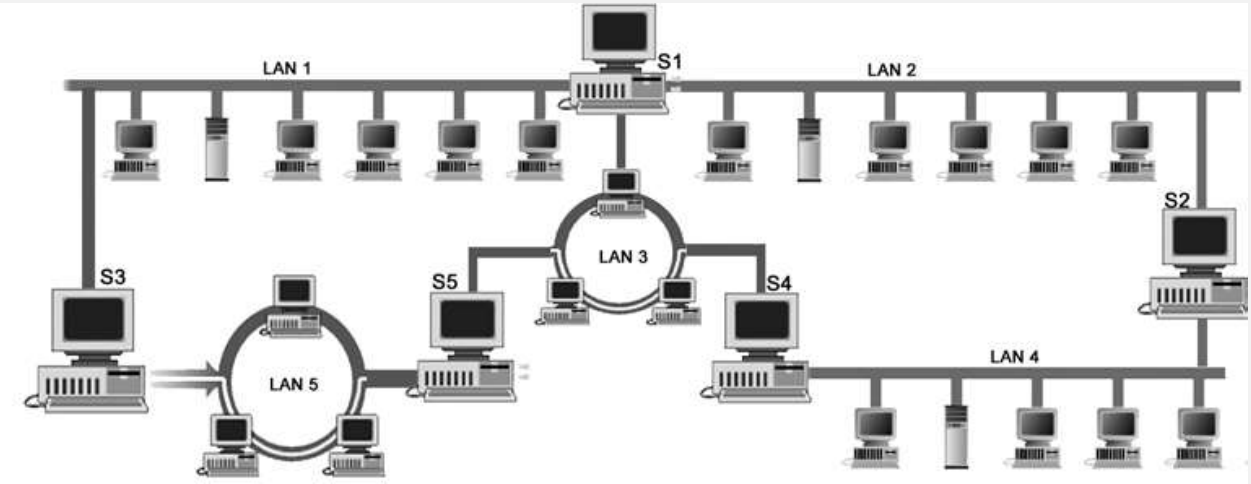
**فرض کنید قصد داشته باشیم زیر ساخت شبکه موجود در یک سازمان بزرگ را به دوازده شبکه جداگانه تقسیم نمائیم . بدین منظور می توان با تهیه دوازده سوئیچ و اتصال ایستگاههای مورد نظر به هر یک از آنان ، دوازده شبکه مجزا که امکان ارتباط بین آنان وجود ندارد را ایجاد نمائیم . یکی دیگر از روش های تامین خواسته فوق ، 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 . مثلا" 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** Switchong **نامیده می‌شود. بر خلاف** Switching، **تعیین مسیر کمی پیچیده است.**

**تعیین مسیر:**

**یك متریك، یك استاندارد برای سنجیدن است. مثل طول مسیر که در الگوریتم های مسیریابی استفاده می‌شود. برای مسیر یابی این الگوریتم ها جدولهای مسیر یابی دارند و اطلاعات مسیر با توجه به الگوریتم تغییر می‌کنند.**

**این جدولها، اطلاعات متنوعی دارند. مثلاً** next hop **به یك** Router **می‌گوید که به یك مقصد مشخص می‌توان بصورت بهینه از طریق یك** Router **مشخص که همان** hop **بعدی است رسید. وقتی که یك** Router **یك** Packet **را می‌گیرد، آدرس مقصد را چك می‌کند و سعی می‌کند 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 می‌کنند و از طریق رد و بدل کردن پیام، جدولهای** Routing **را می‌سازند. پیغام** Routing update**، معمولاً تمام یا قسمتی از جدول** Routing **را در بر دارد. با بررسی جدول بقیه** Router**ها، هر** Router**، می‌تواند یك توپولوژی دقیق از شبکه برای خود ترسیم کند. نوع دیگری از پیغام‌ها، اعلام عمومی**Link – State **است. که به بقیه** Router**ها در مورد وضعیت رابطه ای فرستنده اطلاعات می‌دهد.**

Switching:

**الگوریتم های** Switching **معمولاً ساده و یکسان هستند. در بیشتر مواقع، یك** host **معین می‌کند که باید به یك** host **دیگر یك** Packet **بفرستد و هنگامی که آدرس** Router **را بدست آورد؛**

host **مبدأ یك** Packet **آدرس داده شده را به یك آدرس فیزیکی می‌فرستد و یا پروتوکل و آدرس مقصد. حال** Router **نگاه می‌کند که ببیند آیا می‌تواند آنرا** forward **کند یا نه. اگر نتوانست آنرا رها می‌کند اگر توانست به** hop **بعدی می‌فرستد. و این کار در** hop**های بعدی بصورت مشابه تکرار می‌شود.**

**الگوریتم های** Routing **:**

**این الگوریتم ها 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 می‌گذارند .**

**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 می‌شود توسط هر** hop**.**

**۲- ساده بودن، به این معنی که این الگوریتم ها باید تا حد ممکن کار آمد باشند در حالی که 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 کارکردن صحیح ادامه دهد. به دلیل اینکه از کار افتادن** Router**ها 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 الگوریتم ها:**

**این الگوریتم ها بر اساس انواع تفاوتهای زیر می‌توانند تغییر کنند:**

**۱- استاتیك یا دینامیك باشند.**

**۲- یك مسیر یا چند مسیر باشند.**

۳- host **هوشمند و یا** Router **داشته باشند.**

۴- Link State **یا** distance Vector **باشند.**

**متریك‌های** Routing**:**

**جدولهای** Routing **اطلاعاتی دارند که نرم افزار با استفاده از آنها بهترین مسیر را انتخاب می‌کند.این اطلاعات می‌توانند شامل متریك‌های زیر باشند: طول مسیر، قابلیت اطمینان، تأخیر، پهنای باند و هزینه ارتباطات.**

IP Routing Protocols :

**پروتوکل‌های مسیر یابی مبتنی بر** IP**، به دو دسته کلی تقسیم می‌گردند:**

(IGPs[۱])

(EGPs[۲])

IGPs **در شبکه‌هایی که زیر نظر یك شبکه مشترك اداره می‌شوند استفاده می‌گردد. انواع پروتکل‌های** IGP **عبارتند از:**

(BGPs[۳])

Enhanced IGRP

(OSPF[۴])

(RIP[۵])

[۱] Interior Gateway Protocols
[۲] Exterior Gateway Protocols
[۳] Border Gateway Protocol
[۴] Open shourtest Path
[۵] Routing Information Protocol

(Is-Is[1])

**EGPs برای مسیر یابی بین شکبه‌هایی که اشتراکی با هم ندارند استفاده می‌گردد، این پرتوکل‌ها قبل از اینکه عمل مسیر یاب 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.**

**پرتوکل‌های** EGPs **نیز به دو دسته کلی زیر تقسیم می‌گردند:**

(BGPs[2])

(EGPs[3])

**علاوه بر این‌ها پرتوکل‌هایی هم برای شناسایی مسیر یاب‌ها**(router discovery) **وجود دارد که از بین آنها می‌توان به** (RFC**۱۲۵۶**)ICMP Router Discovery p **اشاره کرد.**

**برای کار، از کدام یك 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.**

[1] Intermediate System to Intermediate System
[2] Border Gateway Protocol
[3] Exterior 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 کابل ها و روترها و غیره نیاز دارید اما علاوه بر این ها به نرم افزار هم نیاز دارید که یکی از مولفه های مهم میباشد. در این فصل به بررسی عناصر نرم افزار های 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 اشنا باشید اما خواندن انها 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 ، اولا" باید بدانیم چه چیزی مشمول این موضوع می شود و ثانیا" 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 بیاندازد ؟ 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 کاملا" 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 کاملا" 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 کاملا" 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 ، 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 اپلیکیشن‌ها 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 RAMبرای نگه داری یا به CPUبرای پردازش ارسال می‌شوند را مدیریت کرده، برنامه‌ها و فایل‌ها را سازماندهی و امکان اتصال دستگاه‌های ورودی یا خروجی را به کاربر می‌دهد.**

**همچنین فایل‌ها و داده‌های حافظه‌های جانبی را مدیریت کرده، استفاده از شبکه‌ها را آسان تر می‌کند و در کل استفاده از سیستم را برای کاربران آسان کرده و از اطلاعات آن‌ها 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 ها ی 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 نمائیم**

**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 ( مثلا" 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 محدویت 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 عموما 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 عمدتا 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 نرم‌افزار کاربردی و یا مجموعه‌ای از نرم‌افزارهای کاربردی است که وظیفهٔ ذخیره و سازمان‌دهی اطّلاعات مربوط به کاربران و منابع یک شبکهٔ رایانه‌ای را به عهده داشته و به مدیر شبکه این امکان را می‌دهد که دسترسی کاربران به منابع شبکه را مدیریت نماید. دایرکتوری سرویس در عین حال به عنوان یک لایهٔ محافظ بین کاربران و منابع مشترک شبکه عمل می‌کند.**

**دایرکتوری سرویس را نباید با منبع ذخیرهٔ دایرکتوری که در واقع محلّ نگهداری اطّلاعات مربوط به اجزای نامگذاری شده که توسط دایرکتوری سرویس مدیریت می‌شوند، اشتباه نمود. در دایرکتوری سرویس مدل پراکندهٔ X.۵۰۰، از تعداد یک یا بیش از یک فضای تخصیص یافته برای نام (درخت اجزاء) جهت تشکیل دایرکتوری سرویس استفاده می‌شود. دایرکتوری سرویس به عنوان واسطی برای دسترسی به اطلاعات موجود در یک یا بیش از یک فضای تخصیص یافته در دایرکتوری عمل می‌نماید. واسط دایرکتوری سرویس نقش مسئولیت مرکزی و مشترکی را ایفا می‌نماید که می‌تواند امنیت کافی را برای آن دسته از منابع سیستم که مدیریت اطلاعات دایرکتوری را انجام می‌دهند فراهم آورد.**

**همچون یک بانک اطلاعاتی، دایرکتوری سرویس به نحوی طراحی شده که می‌تواند به شکلی کارآمد اطلاعات را خوانده و امکانات پیشرفتهٔ جستجو در بین خصیصه‌های مختلفی که می‌توانند به شئ‌های موجود در دایرکتوری مرتبط شوند را فراهم سازد. اطلاعاتی که در دایرکتوری ذخیره شده اند با استفاده از طراحی براساس خصیصه‌های قابل تغییر تعریف می‌شوند. سرویس‌های دایرکتوری از مدل پراکنده برای ذخیره سازی اطلاعات خود استفاده می‌کنند و این اطلاعات معمولاً بین دایرکتوری سرورها دوباره سازی می‌شوند.**

**معرفی**

**یک دایرکتوری سرویس که "سرویس نامگذاری" خوانده می‌شود مانند نقشهٔ راهنمایی عمل می‌کند که منابع شبکه را به آدرس‌های مربوط به آن‌ها در شبکه مرتبط نموده و آنها را به این ترتیب مورد شناسائی قرار میدهد. با استفاده از دایرکتوریهایی از نوع "سرویس نامگذاری" کاربر نیاز ندارد تا آدرس فیزیکی منابع شبکه را به خاطر بسپارد، چرا که تنها نام منبع کافیست تا محل آن را مشخص نماید. هریک از منابع در شبکه به عنوان یک شئ در دایرکتوری سرور محسوب میگردند. اطلاعات مربوط به هر منبع شبکه تحت عنوان خصیصهٔ شئ مربوط به آن منبع در دایرکتوری سرور ذخیره میشود. سطح امنیت اطلاعات هر شئ میتوانند به نحوی تعیین شود که فقط کاربرانی قابلیت دسترسی به آنها را داشته باشند که دارای مجوز لازم هستند. دایرکتوری‌های 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 شئ تحت عنوان "ورودی نامگذاری شده" استفاده میشود. فرایند طراحی دایرکتوری معمولاً دارای مجموعه‌ای 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.۵۰۰ (مجموعهٔ استانداردهای دایرکتوری سرویس) و LDAP نام منبع شبکه "نام مشخصه" خوانده می‌شود و از آن برای اشاره به مجموعه‌ای از خصیصه‌ها ("نامهای مشخصهٔ 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، شمارههای تلفن و شئ‌های دیگر استفاده میشود.**

**دایرکتوری سرویس بخش مهمی از سیستم عامل شبکه است. در موارد پیچیده تر دایرکتوری سرویس مخزن اصلی برای ارائهٔ خدمات شبکه میباشد. به عنوان مثال جستجوی کلمهٔ "کامپیوترها" با استفاده از دایرکتوری سرویس ممکن است پاسخی شامل فهرستی از کامپیوترها و اطلاعات مربوط به نحوهٔ 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 شئ) موجود در یک دایرکتوری در دایرکتوری سرورهای دیگر نیز کپی می‌شود تا هم به عنوان نسخهٔ پشتیبان از آنها استفاده شود و هم به دلیل وجود نسخهٔ محلی از ایجاد ترافیک غیر ضروری در شبکه خودداری گردد. "فضای نامگذاری" دوباره سازی شده توسط مقام مسئول نسخهٔ اصلی مدیریت میشود. عبارت "پراکنده" به معنی این است که دایرکتوری سرورهای متعددی که هریک "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.**

**نرم‌افزار دایرکتوری سرویس**

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

- Banyan VINES

**اولین دایرکتوری سرویس ارائه شده که قابلیت تغییرمتناسب بامقیاس موردنیازراداشت.**

- **دایرکتوری سرور** Sun Java System
- **دایرکتوری سرور** IBM Tivoli
- **(**Windows NT Directory Services) NTDS **برای** Windows NT

- Active Directory **برای** Windows **۲۰۰۰ و** Server **۲۰۰۳**
- Apple Open Directory **در سیستم عامل** Mac OS X Server
- 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 ذخیرهٔ قابل استفاده برای بسیاری از برنامه‌های کاربردی و کاربران قرار گیرند، باید طراحی اطلاعات (و شناسه ها) و ساختار آن به گونه‌ای انجام شود که منعکس کنندهٔ نقش شئ‌ها در دنیای واقعی باشد. در بسیاری از موارد این شئ‌ها 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 شئ 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 شئ‌ها 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 شئ‌های "شناخته شده" ای که**

**میتوانند توسط برنامه‌های 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 برنامه‌های 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 ارائهٔ خدمات" را که دارای مقیاس وسیعی میباشند به درستی مشخص نمود. "سیستمهای ارائهٔ خدمات" امروزه صدها میلیون شئ (HSS/HLR، دفاتر آدرس، میزان مالکیت کاربران، شماره تلفنهای VOIP، اطلاعات کاربران و دستگاهها، و غیره) را به صورت لحظهای و روشهای اتفاقی پشتیبانی میکنند و میتوانند از طریق سیستمهای BSS/OSS/CRM و یا برنامه‌های 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 لحظه‌ای و هزینهٔ 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 لایحهٔ «ارتباط باز سیستم‌ها» بود که به منظور رسیدن به موافقت همه جانبه‌ای در استانداردهای مشترک شبکه برای ایجاد امکان کارکرد بین تولید کنندگان مختلف ارائه شده بود. در دههٔ ۸۰ میلادی ITU و ISO مجموعه‌ای از استانداردها را به نام X.۵۰۰ برای دایرکتوری سرویسها ارائه دادند که هدف اولیهٔ 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 مجموعهٔ TCP/IP و طرح کد بندی X.۵۰۹ پروتکل DAP استفاده می‌کند که این باعث می‌شود 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 می‌توان به موارد زیر اشاره نمود:**

- NIS[1]: **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 شبکهٔ** 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 پایهٔ** LDAP **را تولید کرد که به صورت بخشی از** Sun ONE **درآمد و این طرح اکنون به نام** Sun Java Enterprise **شناخته می‌شود).**
- eDirectory: **این پیاده سازی دایرکتوری سرویس توسط** Novell **می‌باشد. این نوع از دایرکتوری سرویس معماریهای متعددی را پشتیبانی می‌کند که از بین آنها می‌توان به** Windows, NetWare, Linux**، و گونه‌های مختلفی از** Unix **اشاره کرد و این محصول مدتهاست که برای راهبری کاربران، مدیریت تنظیمات، و مدیریت نرم‌افزارها بکار برده می‌شود.** eDirectory **به صورت بخش مرکزی گسترهٔ وسیعی از محصولات مدیریت شناسائی درآمده‌است. این محصول قبلاً به نام** Novell Directory Service **شناخته می‌شد.**
- Red Hat Directory Server: Red Hat **دایرکتوری سرویسی را که آنرا از واحد راه حلهای 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 هستهٔ مرکزی** Fedora **تحت نام** Fedora Directory Server **کار می‌کند.**
- Active Directory: **دایرکتوری سرویس** Microsoft **به نام** Active Directory **خوانده می‌شود و در سیستم عاملهای ۲۰۰۰** Windows **و ۲۰۰۳** Windows Server **موجود است.**
- Open Directory: **سیستم عامل**Apple Mac OS X Server **دایرکتوری سرویس خود را تحت نام** Open Directory **ارائه می‌دهد که این محصول بسیاری از پروتکلهای استاندارد**

[1] Network Information Services

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

- Apache Directory Server: Apache Software Foundation **دایرکتوری سرویسی به نام** ApacheDS **ارائه می‌دهد.**
- Oracle Internet Directory: OID **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 خصیصه‌های مورد استفاده در فیلترهای جستجوی** LDAP **را فهرست نموده و آنها را در نتیجهٔ جستجو نمایش می‌دهد.**
- Sun Java System Directory Server**: این دایرکتوری سرویس ارائه شده توسط** Sun Microsystems **است که آن را می‌توان 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 می‌باشد.**

**افزون بر این موارد، تعداد زیادی از ابزارهای مرجع آزاد وجود دارند که با استفاده از آنها می‌توان دایرکتوری سرویسهای مختلفی شامل پروتکلهای** LDAP **و** Kerberos**، و همچنین نرم‌افزار** Samba **را که با پروتکلهای یاد شده نقش کنترلر** Domain **را ایفا می‌کند را بوجود 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 انها 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 فنآوری 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 یك قالب فریم و مدل آدرس دهی مشابه استفاده می گردد .**

**به منظور دستیابی هر یك 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 ترافیك 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 یك رسانه انتقال داده جدید نظیر فیبر نوری تولید می گردید ، اترنت نیز متاثر 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 صرفا 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 یك محیط انتقال بدون تداخل سیگنال ها با یکدیگر ، از مهمترین دلایل ایجاد اترنت می باشد . استفاده چندین کاربر از یك محیط انتقال مشترك در ابتدا و در سال ۱۹۷۰ در دانشگاه هاوائی مورد توجه قرار گرفت . ماحصل مطالعه فوق ، ابداع روش دستیابی اترنت بود که بعدا** 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 یك 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 یك 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 یك 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 ۸۰۲٫۳** 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 ،استانداردی 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 استادارد‌های ارائه شده با استاندارد اولیه اترنت سازگار می باشند . یك فریم اترنت می تواند از طریق یك کارت شبکه با کابل کواکسیال ۱۰ مگابیت در ثانیه از یك کامپیوتر شخصی خارج و بر روی یك لینك فیبر نوری اترنت ده گیگابیت در ثانیه ارسال و در انتها به یك 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 صرفا" یك تکنولوژی نمی باشد و خانواده ای مشتمل بر مجموعه ای از تکنولوژی های دیگر نظیر:**

Legacy, FastEthernet و Gigabit Ethernet **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 یك رسانه انتقال داده جدید و یا قابلیتی خاص توسعه یابد ، موسسه** IEEE **یك ضمیمه جدید را برای استاندارد ۳ . ۸۰۲ ارائه**

**می نماید. ضمیمه فوق دارای یك و یا دو حرف تکمیلی است . در چنین مواردی یك نام کوته 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 .**

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

**اترنت در ارتباط با سیگنالینگ** Baseband **می‌باشد که از تمامی پهنای باند رسانه انتقال داده استفاده نموده و سیگنال داده مستقیما" بر روی رسانه انتقال داده ارسال می گردد . در سیگنالینگ** Broadband **که توسط اترنت استفاده نمی گردد ، سیگنال داده هرگز مستقیما" بر روی محیط انتقال داده قرار نمی گیرد . یك سیگنال آنالوگ (** Carrier Signal **) ، با سیگنال داده مدوله شده و سیگنال فوق ارسال می گردد . شبکه های رادیوئی 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 منهدسی 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 یك ایستگاه اترنت و ایستگاه دیگر ، عموما" داده از طریق یك** Repeater **ارسال می گردد . در چنین مواردی سایر ایستگاه های موجود در یك** Collistion domain **مشابه ، ترافیك عبوری از طریق** Repeater **را مشاهده خواهند کرد .** Collision domain **یك 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 ترافیك بر روی سایر پورت ها را برعهده دارد . ترافیك دریافتی توسط یك** Repeater **بر روی پورت اولیه ارسال نخواهد شد . هر سیگنال تشخیص داده شده توسط یك** Repeater **فورورد خواهد شد . در صورت افت سیگنال (** Repeater **، نویز و یا میرائی ) مجددا" آن را احیاء و تولید می نماید .**
- **با استفاده از استانداردهای موجود حداکثر تعداد ایستگاه در هر سگمنت ، حداکثر طول هر سگمنت و حداکثر تعداد** Repeater **بین ایستگاه ها مشخص می گردد . ایستگاه هائی که توسط** Repeater **از یکدیگر جدا می شوند ، جملگی در یك** Collision Domain **مشابه قرار می گیرند ( توجه داشته باشید که ایستگاه 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 یك 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 LLC[1] با لایه بالاتر ارتباط برقرار می نماید .**

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

**لایه اول ، صرفا" قادر به تشریح جریان مستمر داده های صفر و یك 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 یك 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 ،**

[1] Logical Link Control

**مسئولیت شناسائی تولید کننده را برعهده دارد . این بخش از آدرس MAC را OUI[1] 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[2] 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 یك شبکه اترنت ، زمانی که یك دستگاه اقدام به ارسال داده می نماید ، می تواند یك مسیر ارتباطی را با سایر دستگاه ها با استفاده از آدرس MAC مقصد فعال نماید . دستگاه مبداء یك 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 یك 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 ننماید ، کامپیوتر و یا دستگاه مقصد آن را دور خواهد انداخت . زمانی که داده به مقصد مورد نظر خود می رسد ، کارت شبکه یك نسخه از فریم را تکثیر و آن را در اختیار لایه های OSI قرار می دهد. در یك 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 ) .**

---

[1] Organizational Unique Identifier

[2] burned-in addresses

- **تمامی دستگاه های متصل شده به یك 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 تنهائی کافی نمی باشد . با تعریف یك 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 یك 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 . یك فریم از چندین بخش ( فیلد ) تشکیل می گردد . هر فیلد نیز از مجموعه ای بایت تشکیل شده است :**

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

- **زمانی که کامپیوترها به یك 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 یك دارای روش مختص به خود برای انجام این فرآیند می باشند . تمامی فریم ها ، صرفنظر از نوع تکنولوژی ، دارای یك 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 ، یك فیلد طول مسئولیت مشخص نمودن طول واقعی یك فریم بر حسب بایت را برعهده دارد . برخی فریم ها دارای یك 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 یك 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 ، یك 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 خطاء از منابع متعددی می باشند. فیلد FCS[1] شامل یك مقدار عددی است که توسط گره مبداء و بر اساس داده**

[1] Frame 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 ،مجددا" مقدار** FCS **محاسبه و با مقدار موجود در فریم مقایسه می گردد . در صورتی که دو عدد با یکدیگر متفاوت باشند ، نشان دهنده بروز خطاء در زمان ارسال اطلاعات می باشد . در چنین مواردی ،فریم دورانداخته شده و از گره مبداء درخواست می شود که مجددا" اطلاعات را ارسال نماید .**

- **برای محاسبه** FCS **از سه روش عمده استفاده می گردد :**
- **روش اول :** (CRC)[1] **، 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 یك 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 یك ساختمان داده خاص مشتمل بر چندین فیلد است که هر یك 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 **، تقریبا 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 یك از نسخه های اترنت دارای یك مجموعه قوانین جداگانه و مختص به خود می باشند .**

[1] Cyclic Redundancy Check

| مقدمه | محاسبه FCS | | | | | FCS |
|---|---|---|---|---|---|---|
| | شروع | مقصد | مبداء | طول / نوع | Pad ا Data | |
| ۷ | ۱ | ۶ | ۶ | ۲ | ۴۶ تا ۱۵۰۰ | ۴ |

- **مقدمه ( ۵۶ بیت معادل هفت** octet**)**
- **شروع فریم ( ۸ بیت معادل یك** octet **)**
- **آدرس** MAC **مقصد ( ۴۸ بیت معادل شش** octet **)**
- **آدرس** MAC **مبداء ( 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 یك** 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** IEEE **۸۰۲٫۳ ) ، مقدمه و شروع فریم در یك فیلد ترکیب می شدند . فیلد "طول / نوع " در نسخه های اولیه** IEEE **به عنوان "طول" و صرفا" در نسخه** DIX **به عنوان "نوع" در نظر گرفته شده بود .**

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

- **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 یك** 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 ( مثلا" 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 :**

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

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

- **مقدمه ( Preamble ) ، یك الگوی متناوب مشتمل بر مجموعه ای از صفر و یك 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 صرفا" جهت سازگاری با نسخه های قبلی استفاده می گردد.**

| PreambleFileld |
|---|
| ۱۰۱۰۱۰۱۰ ۱۰۱۰۱۰۱۰ ۱۰۱۰۱۰۱۰ ۱۰۱۰۱۰۱۰ ۱۰۱۰۱۰۱۰ ۱۰۱۰۱۰۱۰ ۱۰۱۰۱۰۱۰ |

- **شروع فریم یا SFD[1] از هشت بیت تشکیل شده است و مسئولیت آن مشخص کردن انتهای اطلاعات مربوط به زمانبندی است الگوی فوق به صورت ۱۰۱۰۱۰۱۱ 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 .**

[1] Start Frame Delimiter

- **آدرس مبداء ، شامل آدرس MAC مبداء است . آدرس مبداء 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 x۶۰۰۰ ( 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 می‌باشد. 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 خطاء در زمان ارسال اطلاعات ، مجددا محاسبه می گردد . با توجه به این که خرابی صرفا یك 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**Mbps **۴ 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** Mbps **۱۶ 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.**

**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 ۱** Type **خویش می نامند.**

**(**ICSIBM Cabling System) Type ۱ **یک کابل زوج به هم تابیده حفاظدار(**STP**)۱۵۰همی است که حاوی دو جفت سیم می باشد.**

**درگاههای یک** MAU Type ۱ **از اتصال دهنده های اختصاصی تحت عنوان(**UDC**)** Universal Data **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 Categoryتوصیه 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 ۳نیز، هم برای کابل های تکه ای و هم برای کابل های آویز از اتصال دهنده های ۴۵-Rjاستاندارد استفاده می کنند. اما سیستم سیگنال رسانی که در لایه فیزیکی شبکه های Token Ringبه کار می رود با اترنت متفاوت است، Token Ringاز سیگنال رسانی منچستر تفاضلی، و اترنت از سیگنال رسانی منچستر استفاده می کند.**

**در دنیای Token Ringکابل کشی Type۳ UTP 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 Type 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 Typeنسبت به ۳ Type می‌تواند 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 ۸۰۲/۵ IEEE 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 ۴۵-**RJ **برای کابل** UTP **استفاده می شود. هر چند اتصال دهنده های** DB۹ **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[1] **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 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.**

[1] Very Large Scale Integration

**دوم اینکه درگاههای همه MAUها 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 ۱ 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 اهیمت 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 MAUها 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 MAUهای Token Ring همیشه به صورت حلقه به هم وصل می شوند. به این ترتیب که درگاه RingInهر MAU به MAUی 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 درگاهRing Inهر یک را به درگاهRing out دیگری وصل کرد.**

**هاب های اترنت با یک ساختار درخت شاخه کننده به هم وصل می شوند ، در حالی که MAUهای Token Ringبا یک حلقه به هم وصل می شوند.**

**اتصالات بین MAUهای 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 ایستگاه‌های کاری وصل شده به شبکه می رسند. استانداردهای Token Ringدر 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 Ringاز طریق استفاده از یک بسته سه بایتی 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 وارسی 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 می‌خواند 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 اترنت 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 کاریی 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 وارسی 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 ۱۶ Mbps **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 بپیماید، 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. سیستم‌هایی 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 کارآیی 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 می‌تواند حداکثر مدت زمانی را که پیش از اینک یک گره خاص بتواند به ارسال بپردازد 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 فریم‌های** 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 AddressTest**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** MACLobe Media Test **و یک فریم** MAC Dublication 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 آداپتور از کار افتاده تلقی می شود.**

**۲- وارد کردن فیزیکی : در مدت فرآیند وارد کردن فیزیکی، ایستگاه کاری یک ولتاژ فانتوم (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**[1]AMP، [2]SMP**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 **دریافت کند، یا اگر فریم های تست در مدت ۱۸ ثانیه بر نگردند، 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 بیت‌ها 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 فرآینده وارد کردن با شکست مواجه می‌گردد و ایستگاه کاری از حلقه حذف می شود.**

[1] Active Monitor Present
[2] Standby Monitor Present

**۵- تقاضا برای مقدار دهی اولیه : ایستگاه کاری چهار فریم** MAC Request Initialization **را به آدرس عملیاتی سرویس دهنده پارامتر حلقه شبکه (C۰ ۰۰ ۰۰ ۰۰ ۰۲) 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 می‌کند، که اگر همگی با شکست مواجه شوند، مقدار دهی اولیه با شکست مواجه می‌گردد و ایستگاه کاری از حلقه حذف می‌شود.**

**حالتهای سسیستم :**

**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 می کند، هرگاه خود ایستگاه کاری بسته ای برای ارسال داشته باشد بیت توکن بایت کنترل دستیابی فریم را به مقدار ۱ تغییر می دهد و به حالت ارسال وارد می گردد. در همین حین، تایمر حفظ توکن** (THT) **که ۸/۹ میلی ثانیه فرصت ارسال به سیستم می دهد مقدار صفر می گیرد.**

**ارسال –در حالت ارسال، ایستگاه کاری یک فریم را به روی شبکه می‌فرستد و توکن را آزاد می‌کند. پس از ارسال موفقیت‌آمیز فریم، ایستگاه کاری، پر کننده در حالت بیکاری (یک دنباله از یکها) را ارسال می‌کند تا اینکه به حالت تکرار باز گردد. اگر سیستم در حال ارسال، فریم** MAC

Ring Purge , Beacon **یا** Claim Token **را دریافت کند، در ارسال وقفه وارد می کند و یک فریم** Abort Delimiter **را می فرستد 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 می باشد. 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، می فهمد که فریم با موفقیت پاک شده است و به حالت تکرار بر می گردد. 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** Solf ErrorReport **برای ارسال در آینده ثبت می کند.**

**عملیات وارد کردن ایستگاه کاری به** TokenRing **تضمین می کند که تمام سیستم هایی که به حلقه وصل هستند درست کار می کنند.**

**بازرسان Token Ring:**

**هر شبکه** Token Ring **سیستمی دارد که بازرس فعال است و وظیفه آن حصول اطمینان از کارایی مناسب شبکه می باشد.**

**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 بازرسان 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 Peresent - **هر هفت ثانیه یک بار، بازرس فعال** (AM) **قادر خواهد بود تا یک فریم** MAC Active MonitorPresent **را ارسال کند که این فریم، فرآیند عملیات حلقه را به کار می اندزاد.**

**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 ساعت هایشان 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 پیوندند.**

**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 و 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 می‌گردانند 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 علامت‌دهی استفاده می کنند. تا محل یک خرابی شبکه را مجزا نمایند.**

**فرآیند عملیات حلقه توسط فریم** MAC(AMP) Active Monitor Present **که بازرس 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 می‌کند، فقط این فریم** Standby Monitor Present(SMP) **است، نه** Active MonitorPresent **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 شانسی 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 بازرس 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 میکند 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 بازرس فعال، یک بسته SMP با مقدار صفر در بیت های ARI و FCI را دریافت کند، می‌فهمد 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 بازرس 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 می‌گوید 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 شودکه 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** Claim Token-MAC **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 اترنت 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 ۸۰۲٫۲** IEEE **تعریف شده است آنها عبارتند از :**

**مرز آغاز (**SD**) یک بایت : این فیلدآغازفریم رامشخص میکند .**

**الگوی بیتی بایت به کاررفته دراین فیلد**JK۰JK۰۰۰ **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 دسته‌یابی (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 اولویت‌دهی 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 (۱) یا یک فریم توکن است (۰).** 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،TT००AAAA 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 بایت : 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 بایت : 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 بایت 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 بایت :این فیلد حاوی ۴ بایت نتیجه محاسبهCRC بر روی فیلدهای کنترل فریم، آدرس مقصد، آدرس مبدا 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 بایت : 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 Kها 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 می‌باشد. 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 فیلد۰۰AF۰۰AF است، که A و F به ترتیب ARI[1] و FCI[2]می‌باشند. مقدار این بیت ها به این دلیل تکرار شده است که فیلد وضعیت فریم در بررسی CRC 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 می‌کند. 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 سیستم‌های خاصی از شبکه ایفا می‌کنند تعریف می کند. با استفاده از این آدرسها یک گره می‌تواند پیغامها را به طور مستقیم به سیستمی که کار خاصی را انجام می‌دهد 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 C۰**

**سرویس دهنده پارامتر حلقه ۰۲ ۰۰ ۰۰ ۰۰ ۰۰ C۰**

**بازرس خطای حلقه ۰۸ ۰۰ ۰۰ ۰۰ ۰۰ C۰**

[1] Address Recognized Indicator
[2] Frame Copied Indicator

**سرویس دهنده گزارش پیکربندی ۱۰ ۰۰ ۰۰ ۰۰ ۰۰ C۰**

**پل مسیر مبدأ ۰۰ ۰۱ ۰۰ ۰۰ ۰۰ C۰**

**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 **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 می‌دهند. آنها هرگز به انتقال داده های لایه های بالاتر نمی پردازند و توسط پلها، سوئیچ ها یا مسیریابها به دامنه برخوردهای دیگر انتشار نمی یابند. بعضی از رایجترین این عملیاتها فقط توسط یک کد چهاربیتی واقع در فیلد کنترل فریم مشخص می‌شوند، 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 فریم‌های 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 فیلد یک بایتی تشکیل می شود: مرز آغاز، کنترل دستیابی و مرز 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 مرز آغاز و مرز 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 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 می‌کند، 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 می‌توانند 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 می‌کند، که در طی آن صبر می کند تا ببیند آیا خطای دیگری رخ می‌دهد، پس از آنکه دو ثانیه تمام شد، سیستم یک پیغام گزارش خطای قابل حل را به آدرس بازرس خطای حلقه (C۰ ۰۰ ۰۰ ۰۰ ۰۰ ۰۸) 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 ناقض سیستم کد گذاری منچستر تفاضی 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) بازرس 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 بازرس 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 بازرس فعال، سیگنال ساعت درستی را تولید نمی کند. در این صورت باید بازرس 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 بازرس 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 اجتمالاً به دلیل آداپتور شبکه خراب خود از تغییر بیت های ARI و FCI بازمانده است.**

**خطای FC**

**خطای FC[1] 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 مرز پایان نامعتبر یا یک فریم مطالبه توکن، علامت دهی و یا تصفیه حلقه را زمانی دریافت کند که منتظر مرز آغاز فریم ارسالی خودش است.**

[1] Frame Copied

**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 **، عموما دارای یک اسلات** PCMCIA **است که کارت شبکه درون آن قرار می گیرد . کامپیوترهای شخصی نیز به یک کارت شبکه داخلی که معمولا 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 تواتند 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 ،**

**عموما 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 هائی 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 پارازیت ایجاد گردد ، ممکن است ارتباط ایجاد شده قطع و یا امکان استفاده مطلوب از آن وجود نداشته باشد .**

**انواع شبکه های wireless**

- **WLANS: Wireless Local Area Networks ؛ 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 .**
- **WPANS: Wireless Personal Area Networks ؛ 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[1] **و** Bluetooth **(** IEEE **۸۰۲٫۱۵) ، استفاده می گردد .**
- **WMANS: Wireless Metropolitan Area Networks ؛ 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 .**
- **WWANS: Wireless Wide Area Networks؛ 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 :**

- **WEP : Wired Equivalent Privacy ؛ در روش فوق ، هدف توقف ره گیری سیگنال های فرکانس رادیوئی 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**

[1] Infra Red

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

- **SSID[1]: 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 پکربندی 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[2]: در روش فوق ، لیستی از آدرس های** MAC **مربوط به کامپیوترهای سرویس گیرنده، برای یک** AccessPoint **تعریف می گردد . بدین ترتیب ، صرفا 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، صرفا در شبکه های کوچک بدون کابل پیشنهاد می گردد .**

[1] **Service Set Identifier**
[2] **Media 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 IPگفته 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**

**IPنشانی 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.**

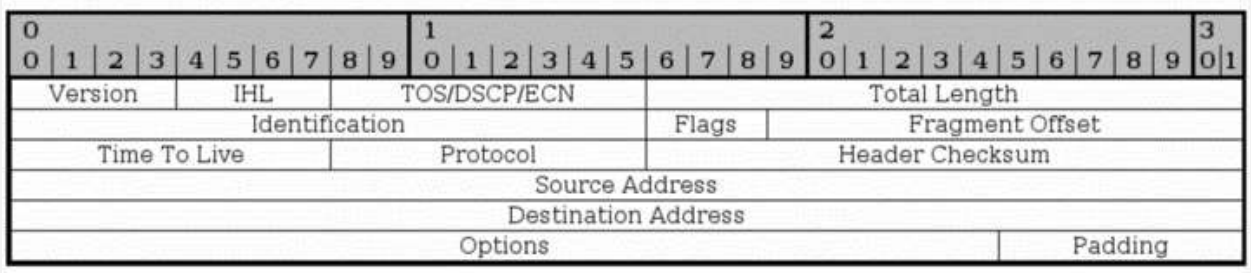
**پروتکل اینترنت، وظیفه حمل و انتقال بسته های حاوی اطلاعات و مسیریابی آنها را در یک شبکه، از مبدا تا مقصد به عهده دارد .پس از دریافت اطلاعات ازTCP ، به قطعه قطعه کردن و تبدیل آنها به بسته های کوچک تری به نام FRAGMENT اقدام کرده سپس برای هر یک از این فراگمنت ها، یک بسته IP می سازد که حاوی اطلاعات مورد 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 ۰٫۰٫۰٫۰(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)، ۲۵۵٫۲۵۵٫۲۵۵٫۲۵۵ (برای ارسال پیام به صورت عمومی و فراگیر در شبکه)، و...اشاره کرد.**

**ساختار بسته هایIP**

**بسته های ساخته شده توسطIP ، از تعدادی فیلد مجزا تشکیل شده که هر کدام دربردارنده 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.**




**فیلد**VERSION

**این فیلد وظیفه مشخص کردن نوع پروتکل IP را به عهده دارد. قابل ذکر است اکنون دو نسخه از IPوجود 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 IPنسخه 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 بایت است.**

**فیلد**TOTAL LENGTH

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

**فیلد** FRAGMENT OFFSET

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

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

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

**۳ .بیت** (FO) Fragment Offset: **این بیت دربردانده 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 ضریبی 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 مسیریاب عبور کند، که البته بیشترین مقدار آن ۲۵۵ است. معمولا 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 ها ی 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 .**

## نمایش آدرس IP

**آدرس IP ، یک مقدار سی و دو بیتی است که کامپیوترها با مهارت خاصی از آن بمنظور انجام عملیات خود در یک شبکه کامپیوتری مبتنی بر TCP/IP استفاده می نمایند . انسان در مقابل استفاده از یک عدد باینری سی و دو بیتی که بخاطر سپردن آن همواره مشکل خواهد بود ، از سیستم دهدهی ، استفاده می نمایند . ( استفاده از سیستم دهدهی در مقابل سیستم باینری ) . بدین دلیل برای نمایش یک آدرس IP از شکل دهدهی ( decimal ) آن استفاده می گردد. آدرس های IP سی و دو بیتی از بیت با ارزش بالا بسمت بیت با ارزش پائین ، به چهار واحد هشت بیتی ( گروه هشتگانه ) که به هر یک از آنان Octet گفته می شود ، تقسیم می شوند . آدرس های IP معمولا بصورت چهار octet دهدهی که توسط یک نقطه از یکدیگر جدا می گردند ، نوشته می شوند .**

**مدل نمایشی فوق را Dotted Decimal می گویند .**

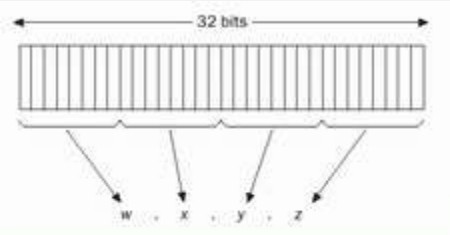
**مثلا" آدرس IP : ۰۰۰۰۱۰۱۰۰۰۰۰۰۰۰۱۱۱۱۱۰۰۰۱۰۱۰۰۰۰۱۱، پس از تقسیم به چهار Octet ( گروه هشتگانه ) ، بصورت زیر نمایش داده می شود:**

**۰۰۰۰۱۰۱۰ ۰۰۰۰۰۰۰۱ ۱۱۱۱۰۰۰۱ ۰۱۰۰۰۰۱۱**

**هر Octet ( گروه هشتگانه ) در ادامه به یک عدد دهدهی تبدیل و پس از جداسازی آنان توسط نقطه از یکدیگر بصورت زیر نمایش داده می شوند :**

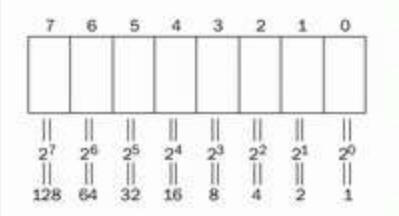
**۱۰٫۱٫۲۴۱٫۶۷**

**یک آدرس عمومی IP بصورت w.x.y.z نشان داده می شود :**



**تبدیل از باینری به دهدهی:**

**بمنظور تبدیل یک عدد باینری به معادل دهدهی ، باتوجه 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 .**




**مثلا" ، عدد هشت بیتی ۰۱۰۰۰۰۱۱ ، معادل ۶۷ ( ۱ + ۲ + ۶۴ ) می باشد . حداکثر عددی را که می توان توسط هشت بیت نشان داد ( ۱۱۱۱۱۱۱۱ ) ، 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 . مثلا 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 مبداء و مقصد می باشد :**

- **فیلد آدرس مبداء 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 ، صرفا 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(**DHCP) DynamicHost Configuration Protocol **باشد ، استفاده می گردد .**

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

**آدرس های** IP **ازنوع** Unicast

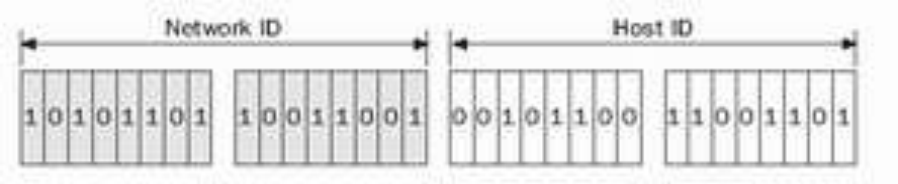
**هر اینترفیس شبکه که** TCP/IP **در ارتباط با آن فعال شده باشد، می بایست دارای یک آدرس** IP **منحصربفرد، منطقی و** Unicast **باشد .آدرس منحصربفرد** Unicast **، بمنزله یک آدرس منطقی خواهد بود. چراکه آدرس فوق در لایه اینترنت بوده که هیچگونه ارتباط مستقیمی با آدرس استفاده شده در لایه اینترفیس شبکه ندارد . مثلا آدرس** IP **نسبت داده شده به یک میزبان (** host**) بر روی یک شبکه اترنت ، هیچگونه ارتباطی با آدرس** MAC **چهل 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 بهمراه 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 پاسخگوئی به یک شبکه گسترده جهانی را دارا نمی باشد. مثلا 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.**

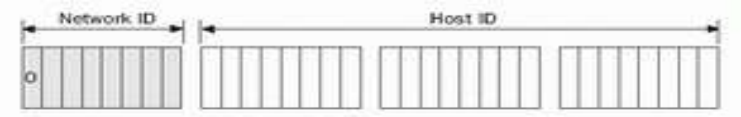
**۷۹۱** RFC **، آدرس های** IP **از نوع** Unicast **را کلاس های آدرس دهی خاصی تعریف می نماید که از آنان بمنظور ایجاد شبکه ها با ابعاد و اندازه های متفاوت استفاده می گردد( توانائی تعریف مناسب شبکه ها ) . اهداف اولیه طراحی کلاس های آدرس دهی ، نیل به خواسته های زیر بود :**

- **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 .**

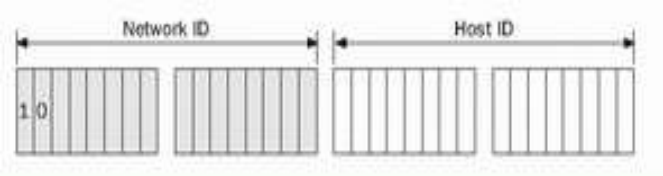
**کلاس A**

**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**

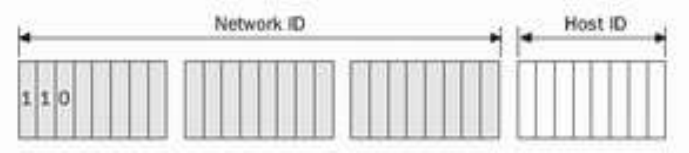
**آدرس های کلاس B ، برای شبکه هائی با ابعاد متوسط که دارای تعداد متوسطی ( نه خیلی زیاد و نه خیلی کم ) از میزبانان می باشند ، طراحی شده است ( ایجاد تعدادی متوسط از شبکه هائی که دارای میزبانان متوسطی می باشند ). دو بیت با ارزش بالا ، دارای مقدار ۱۰ می باشد . اولین شانزده بیت ( دو octet اولیه ) بعنوان مشخصه 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 بیت 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 رزو 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 **رزو 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 **رزو 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 منحصربفرد باشد .**

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

| کلاس | اولین مشخصه شبکه | آخرین مشخصه شبکه | تعداد شبکه ها |
|---|---|---|---|
| A | ۱/۰/۰/۰ | ۱۲۶/۰/۰/۰ | ۱۲۶ |
| B | ۱۲۸/۰/۰/۰ | ۱۹۱/۲۵۵/۰/۰ | ۱۶٬۳۸۴ |
| C | ۱۹۲/۰/۰/۰ | ۲۲۳/۲۵۵/۲۵۵/۰ | ۲٬۰۹۷٬۱۵۲ |

**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 ها ی 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.**

| کلاس | اولین مشخصه میزبان | آخرین مشخصه میزبان | تعداد میزبانان |
|---|---|---|---|
| A | w.۰٫۰٫۱ | w.۲۵۵٫۲۵۵٫۲۵۴ | ۱۶٬۷۷۷٬۲۱۴ |
| B | w.x.۰٫۱ | w.x.۲۵۵٫۲۵۴ | ۶۵٬۵۳۴ |
| C | w.x.y.۱ | w.x.y.۲۵۴ | ۲۵۴ |

**درس ۴**

**SubnetMask**

**سیستم ها برای تشخیص تعلق یا عدم تعلق به یك 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 میتوانیم ازآن به عنوان یک آدرس استفاده کنیم یک** SubnetMask**استاندارد دارد 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 : **۲۵۵.۰.۰.۰**

Class B : **۲۵۵.۲۵۵.۰.۰**

Class C: **۲۵۵.۲۵۵.۲۵۵.۰**

**نکته:** IP **هادر صوورت قابل نمایش هستند**

1. subnet mask format
2. 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**

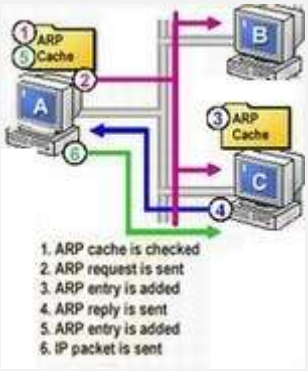
Subnet mask: **۲۵۵٫۲۵۵٫۲۵۵٫۰**

**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



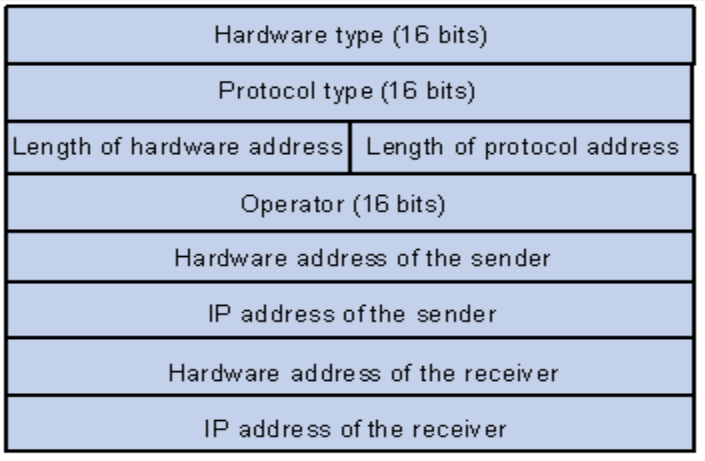

**(ARP) Address Resolution Protocol ، پروتکلی است که مسئولیت مسئله " نام به آدرس" را در رابطه با بسته های اطلاعاتی خروجی (Outgoing) ، برعهده دارد . ماحصل فرآیند فوق Mapping آدرس IP به آدرس MAC(Media Access Control )، مربوطه است . کارت شبکه از آدرس MAC ، بمنظور تشخیص تعلق یک بسته اطلاعاتی به کامپیوتر 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 روترهائی است که صرفا 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: **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**.

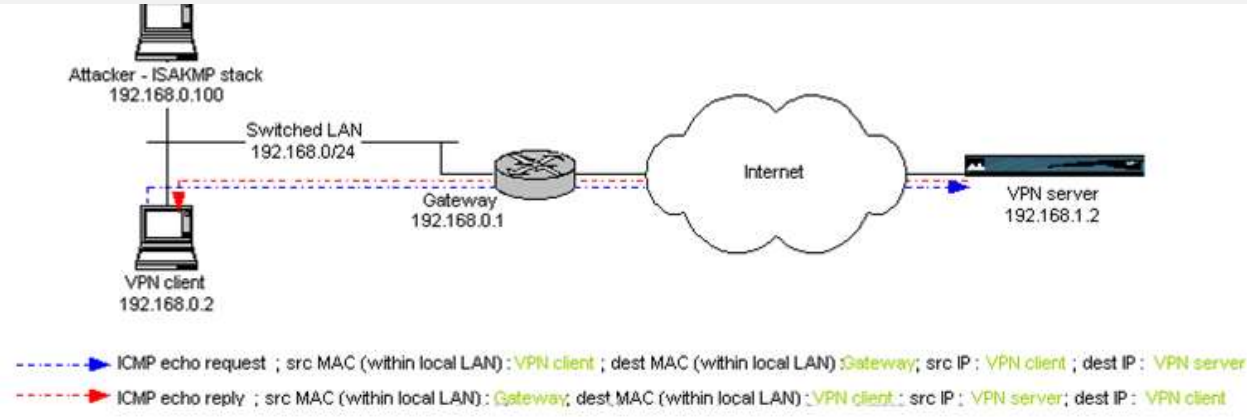
Destination Hardware Address: **آدرس فیزیکی ماشین مقصد.**

Destination IP Address: **آدرس**IP **ماشین مقصد**.

# درس ۶

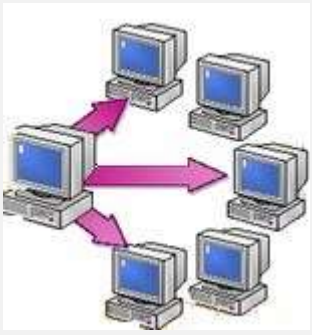
# پروتکل ICMP

**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 رویIP نصب مـی شود تـا در صـورت‌وقوع هرگونه خطا به فرستنده پیام‌مناسب رابدهد که این گزارشات برای مدیران شبکه دارای اهمیت است.البته میتوانیم بگوییم تعدادی ازاین پیغام هابین 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 پیغام ها چه هستند باید بگوییم پیغام** Echo **یکی از مهم ترین آنها است و همچنین دستور پرکاربرد** PING.
**ضمناً دستور** PING**را در محیط** Command Promprt( CMD )**باید اجرا کرد** .



# درس ۷

## پروتکل IGMP



**(IGMP)** Internet Group Managment Protocol **، پروتکلی است که مدیریت لیست اعضاء 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** multicat **نامیده می شوند ؛ ارسال می گردد .** IGMP **لیست اعضاء را نگهداری می نماید .**

**مدیریت** IP Multicasting

**تمامی اعضاء 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 شبکه‌های رایانه‌ای، لایه انتقال سرویس‌های ارتباطی مبدأ به مقصد یا** end-to-end **را برای برنامه‌های کاربردی موجود در معماری لایه بندی شده پروتکل‌هاو اجزاء شبکه فراهم می‌آورد. لایه انتقال سرویس‌های مطمئنی از قبیل پشتیبانی از جریان داده اتصال گرا، قابلیت اطمینان، کنترل جریان و تسهیم یا مالتی پلکسینگ را ارائه می‌نماید.**

**لایه‌های انتقال هم در** (RFC **۱۱۲۲**) **مدل** TCP/IP **، که مبنا و بنیان اینترنت می‌باشد، و هم مدل** OSI**موجود می‌باشند. تعریف لایه انتقال در این دو مدل کمی با یکدیگر تفاوت دارد.**

**معروف ترین پروتکل لایه انتقال پروتکل کنترل انتقال یا** Transmission Control (TCP) Protocol**می‌باشد. این پروتکل نام خود را از مجموعه پروتکل اینترنت یا همان** TCP/IP **وام گرفته‌است. از این پروتکل در انتقالات اتصال گرا استفاده می‌شود در حالیکه پروتکل بدون اتصال** UDP**برای انتقالات پیام ساده مورد استفاده قرار می‌گیرد.** TCP**پروتکل پیچیده تری است و این پیچیدگی به واسطه طراحی وضعیت محوری است که در سرویس‌های انتقالات قابل اطمینان و جریان داده تعبیه شده‌است. از دیگر پروتکل‌های عمده در این گروه می‌توان به پروتکل کنترل ازدحام دیتاگرام** Datagram Congestion Control Protocol (DCCP) **وپروتکل انتقال کنترل جریان** Control Transmission Protocol (Stream) **) 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 بایت‌ها می 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 مسأله 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 مقابله‌ای 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 هابه فرستنده اعلام می کند. ممکن است طرح های درخواست تکرار خودکاربرای 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 بافرداده 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 خودکارمی 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) **پورتها می 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 پورت‌های 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:**

**برقرارسازی 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 خطاو پروتکل درخواست تکرار خودکار** (ARQ) **انجام می پذیرد. پروتکل** ARQ **عمل کنترل جریان را 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** UDP **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 از 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 اکس۲۵**(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 ،** TP۰ **با کمترین امکان کشف خطا تا** TP۴ **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 فریم‌های**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 یك دید کلی از پروتکل** TCP **ارائه می نماییم و ساختار سرآیند بسته ها را در این پروتکل ، توضیح خواهیم داد .**

**در زیر ساختار یك 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) ۰ or more ۳۲-bit words) | | | | | | | | |
| Data ( optional ) | | | | | | | | |

**فیلد** Source Port**: در این فیلد یك 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 پورت 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 .**

**فیلد**Sequence Number**: این فیلد سی ودو 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 می نماید . یعنی ممکن است که کلاً درون فیلد داده فقط یك 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 یك 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 قرارگرفته 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 ۲۸=۷*۴ بایت خواهد بود(این فیلد کلاً چهار بیتی است)دقت کنید که قسمت ثابت و اجباری در یك بسته** TCP **حداقل ۲۰ بایت است ولی در فیلد اختیاری میتواند اطلاعاتی قرار بگیرد و بنابر این گیرنده یك 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 یك اشاره گر ،محل شروع داده هارا در یك بسته** TCP **تعیین کند( توجه دارید که مبنای این عدد کلمات ۳۲ بیتی( ۴ بایتی) هستند)**

**بیتهای ۶:** Flag ( Code Bits ) **بیت بعدی در بسته** TCP **هر کدام نقش یك 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 بایسیتی 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** Acknoledgement Number **قرارگرفته 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 یك 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 یك ارتباط بازی میکند . برقراری یك ارتباط** TCP **از روند زیر طبعیت میکند :**

**شروع کننده ارتباط یك بسته** TCP **بدون هیچگونه داده و با تنظیم بیتهای (**ACK=۰,SYN=۱ **) ، برای طرف مقابل ارسال میکند . در حقیقت ارسال چنین بسته ای به معنای تقاضای برقراری ارتبا ط 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=۱ **و بیت** ACK=۱ **است . این بسته نقش پذیرش یك ارتباط رابازی میکند .**

**بیت** FIN **:اگر یکی از طرفین ارتباط ، داده دیگری برای ارسال نداشته باشد درهنگام ارسال آخرین بسته خود این بیت را ۱ می کند و در حقیقت ارسال اطلاعات خودش را یك 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 یك بسته با یك کردن بیت** FIN **، ارسال اطلاعات را خاتمه بدهد .**

**فیلد** WindowsSize**: 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 شماره‌ء ترتیبی که در فیلد** Acknowledgement **مشخص شده است ، حداکثر به اندازه‌ء 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 یك عدد بعنوان اشاره گر قرار می گیرد که موقعیت داده های اظطراری 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 یك برنامه کاربردی رخ بدهد . بدون آنکه ارتباط قطع شود داده های لازم در همین بسته جاری ارسال خواهد شد.**

**دقت کنید که داده های اظطراری 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

**UDPاز 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 کند و هر بسته از داده کاربر و کمترین میزان سرایند تشکیل شده که به آن** UDP **دیتاگرام گفته می شود.**

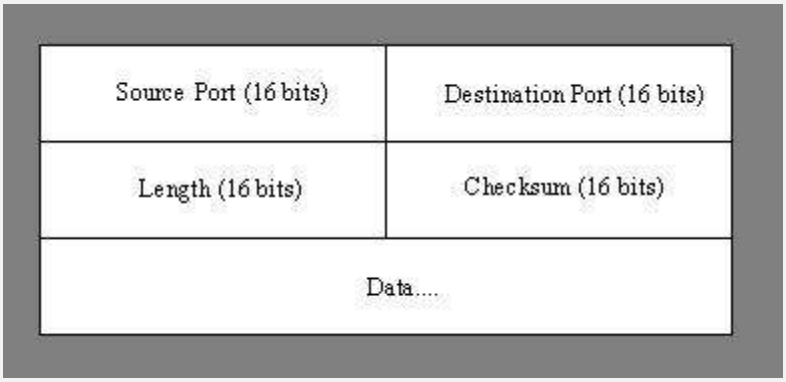
UDP **غیراتصال گرا است .یعنی یک دیتاگرام در هر لحظه ای میتواند ارسال بشود ، بدون نیاز به هر گونه اعلام قبلی، مذاکره و یا هیچ آماده سازی از قبل.فقط داده را ارسال می کند و امیدوارد که گیرنده داده ها رو دریافت کند.**

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

**مهمترین محاسن** UDP **این است که محدوده داده ها در آن مشخص شده است ، در ارسال های** broadcast **میشود از این پروتکل استفاده کرد و همچنین سریع است.**

**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 نشود در این فیلد ۰ قرار میگیرد.**

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. معمولا یک پورت برای یک برنامه اختصاص دارد.**

**محاسن** TCP

- **سیستم عامل همه کار را برای شماانجام 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 مقصدبرسد ، 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 ویژگیهائی 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 یا** 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 هریک از این خطاها ما متوجه نمیشویم، مگر اینکه برنامه ای که به داده ها گوش می دهد، در صورت بروز هر یک از خطا ها 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 ۸

# 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 .**

**همگرائی ( 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 ار بهترین مسیرهای موجود . در زمان انجام فرآیند فوق ( همگرائی ) ، 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 صرفا 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 **ها 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 **(**RIP**)** ، Enhanced Interior Gateway Routing Protocol**(**EIGRP**)و** Open Shortest Path First **(**OSPF**)اشاره کرد. اما بصورت کلی ما** Routing Protocol **ها را به سه دسته کلی تقسیم بندی می کنیم.**

Routing Protocol**های**Distance-Vector:

**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** RIPv۱ **و** IGRP **از این نوع** Routing protocol **ها هستند.**

Routing Protocol**های** Link-State:

**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.**

Routing Protocol**های** Hybrid:

**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 انها را شنیده و بیشتر با انها سر و کار دارد.**

## درس ۱

## DHCP

**بااستفاده از یك سرویس دهنده** DHCP **که تنظیمات پیکر بندی را به صورت اتوماتیك اختصاص می دهد ،کاربران و مدیران** TCP/IP **می توانند خود را از دردسر پیکربندی دستی آدرس های** IP **،ماسك زیر شبکه،آدرس سرویس دهنده های** DNS **، آدرس سرویس دهنده های** WINS **،و سایر جنبه های** TCP/IP **برهاند.**

DHCP**یك استاندارد باز است که در ۲۱۳۲** RFC **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 پیکربندی تک تک ایستگاههای کاری از دوش مدیران برداشته می شود ،و تخصیص آدرس های** IP **تکراری تقریباً غیر ممکن می شود.**

## تاریخچه DHCP

Dhcpریشه در bootp دارد،که یک پروتکل 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. هرکامپیوترشبکه 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 صرفا 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

Dhcpبرای 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 ودر ضمن توسعه یافته است تا ابزار بهتری نسبت به bootpباشد.

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

**تخصیص دستی :**

**آدر س های ip و سایر تنظیمات پیکربندی توسط مدیر به صورت تک تک وارد شده روی سرویس دهنده ذخیره می گردند و به سرویس 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 سرویس گیرنده dhcp ،برای اولین بار در شبکه بوت می شود ،سرویس دهنده dhcp از مخزنی از آدرس های موجود که مدیربرای استفاده او تنظیم کرده است ،یک آدرس ip و سایر تنظیمات پیکربندی را به آن ایستگاه کاری اختصاص می دهد ،واینها تنظیمات دائمی آن ایستگاه می شوند .**

**تخصیص پویا :**

**این مثل تخصیص اتوماتیک است ،با این تفاوت که تنظیمات tcp/ip به صورت دائمی تخصیص داده نمی شوند ،بلکه صرفا برای مدت زمان مشخصی اجاره داده می شوند .اجاره باید به صورت منظم ازطریق مذاکره (اتوماتیک) بین سرویس گیرنده و سرویس دهنده dhcp تمدیدشود.این سه روش می توانند به صورت همزمان مورد استفاده قرار گیرند تاهمه انتخاب هایی راکه ممکن است مدیران شبکه نیاز داشته باشند دراختیارشان 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 سرویس 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 ویندوز۲۰۰۰ 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 اتو ماتیک خود را با یک آدرسIP 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 رار در اختیار او قرار دهداگراین جست و جو با شکست مواجه شودسرویس گیرنده به صورت اتوماتیک خود را با یک آدر سiP و ماسک زیر شبکه کلاس B پیکربندی می کند.سپس او این آدر س را به دنیا اعلام می کند تا ببیند که آیا کامپیوتر دیگری از قبل این آدرس را به خودگرفته است یا خیر .**

**سرویس گیرنده به طور منظم سعی می کند که با یک سرویس دهنده DHCP تماس بگیرد تازمانی 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 داردبه 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،سرواژهٔ سامانهٔ نام دامنه،DNS[1] 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. مثلا 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 ترجمهٔ نام بدین صورت است که وقتی یک برنامهٔ 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 بستهٔ درخواست (**Query Packet**) به روش** UDP **تولید کرده و به نشانی یک کارساز** DNS **(که به صورت پیش فرض مشخص می‌باشد) ارسال می‌کند. همهٔ ماشین‌های میزبان، حداقل باید یک نشانی آی‌پی از یک سرویس دهندهٔ ساناد را در اختیار داشته باشند. این «سرویس دهندهٔ محلی» پس از جستجو، نشانی آی‌پی معادل با یک نام نمادین را بر می‌گرداند.**

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

[1] Domain Name System

**کاربرد حوزه‌ها :**

**برای تحلیل یک نام حوزه، سطوح از سمت راست به چپ تفکیک می‌شوند و در یک روند سلسله مراتبی، سرویس دهندهٔ متناظر با آن سطح پیدا می‌شود.**

**نام‌های حوزه به هفت منطقهٔ عمومی و حدود صد و اندی منطقهٔ کشوری تقسیم بندی شده‌است. حوزه بدین معناست که شما با یک نگاه ساده به انتهای نشانی نمادین، می‌توانید ماهیت آن نام و سرویس دهندهٔ متناظر با آن را حدس بزنید. یعنی اگر انتهای نام‌های حوزه متفاوت باشد منطقهٔ جستجو برای یافتن نشانی آی‌پی 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 می‌آید.**

edu. **صاحب این نام جزو موسسات علمی یا دانشگاهی به شمار می‌آید.**

gov. **این مجموعه از نام‌ها برای آژانس‌های دولتی آمریکا اختصاص داده شده‌است.**

int. **صاحب این نام یکی از سازمان‌های بین‌المللی (مثل یونسکو، فائو، ...) است.**

mil. **صاحب این نام یکی از سازمان‌های نظامی دنیا به شمار می‌آید.**

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

org. **صاحب این نام جزو یکی از سازمان‌های غیر انتفاعی محسوب می‌شوند**

**نام‌های حوزهٔ بسیار زیادی در اینترنت تعریف شده‌اند که هیچیک از حوزه‌های سه حرفی هفتگانه را در انتهای آنها نمی‌بینید. معمولاً در انتهای این نشانی‌ها یک رشتهٔ دو حرفی مخفف نام کشوری است که آن نشانی و ماشین صاحب آن، در آن کشور واقع است.**

**ساختار سلسله مراتبی DNS**

**هر حوزه می‌تواند به زیر حوزه‌های 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 دانشگاه‌ها 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**

**حوزه‌ها با دامنه‌ها یکسان نبوده و یک حوزه می‌تواند شامل مقادیری در رابطه با چندین دامنه باشد.**

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

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

**روش‌های 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.**

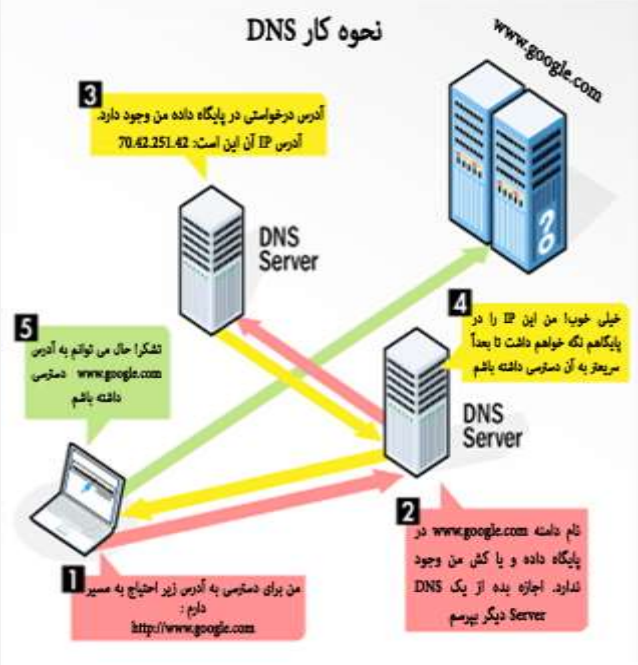
**سه روش برای پرس و جوی نام در سرویس دهنده‌های نام وجود دارد :**

**پرس و جوی تکراری** (Iterative Query)

**پرس و جوی بازگشتی** (Recursive Query)

**پرس و جوی معکوس** (Reverse Query)

**نحوه دسترسی به یک سرور از طریق سامانه** DNS

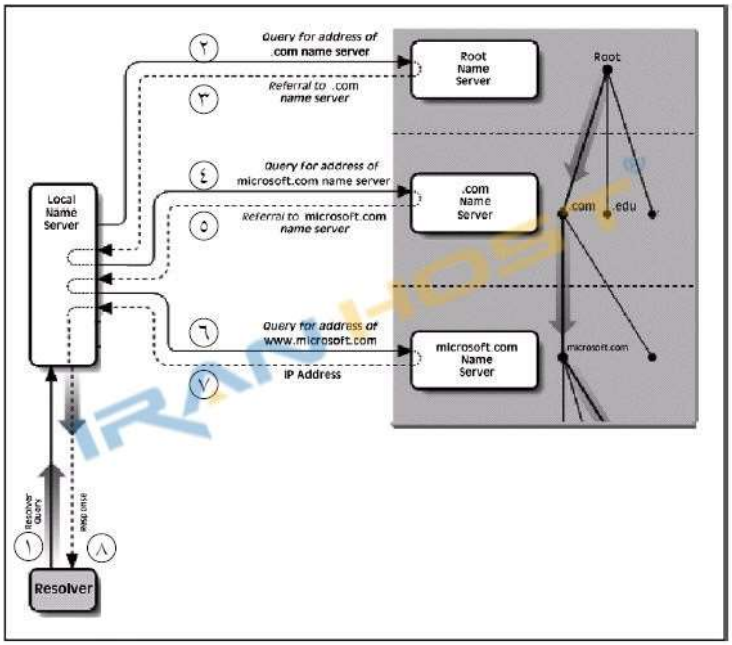



**پرس و جوی تکراری**

**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 می‌شود در صورتی که قادر به ترجمه نام به معادل نشانی آی‌پی آن باشد، معادل نشانی آی‌پی 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 می‌کند. این سرویس دهنده، نشانی ماشینی را که می‌تواند برای ترجمه نام مورد نظر مفید باشد، به سرویس دهنده محلی معرفی می‌کند؛ سرویس دهنده محلی مجدداً یک تقاضا به ماشین معرفی شده در مرحله قبل ارسال می‌کند.**

**در این حالت هم سرویس دهنده نام می‌تواند در صورت یافتن نشانی آی‌پی با آن نام حوزه، آنرا ترجمه کند و یا آنکه نشانی سرویس دهنده سطح پایینتری را به او برگرداند.**

**این روند ادامه می‌یابد تا** DNS **نهایی نام مورد نظر را به نشانی آی‌پی ترجمه نماید. برای درک بهتر از روند کار به شکل زیر دقت کنید. در این مثال فرض شده‌است که یک برنامه کاربردی با فراخوانی «تابع تحلیلگر نام»، تقاضای ترجمه نام** www.microsoft.com **را می‌نماید. مراحلی که انجام می‌شود 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 می‌ماند.**

**در مرحله دوم، سرویس دهنده محلی از سرویس دهنده** Root **(که حوزه‌های متفاوت را تفکیک می‌کند) نشانی ماشین یک** DNS **که متولی حوزه**com **است را سؤال می‌کند.**

**در مرحله سوم، نشانی سرویس دهنده مربوط به حوزه** com **بر می‌گردد.**

**در مرحله چهارم، سرویس دهنده محلی، از ماشین معرفی شده در مرحله قبلی، نشانی سرویس دهنده مربوط به حوزه** Microsoft.com **را سؤال می‌نماید.**

**در مرحله پنجم فهرستی از سرویس دهنده‌های** DNS **مربوط به** Microsoft.com **بر می‌گردد.**

**در مرحله ششم، سرویس دهنده محلی تقاضای ترجمه نشانی نمادین** www.microsoft.com **را از** DNS **متعلق به حوزه** Microsoft.com **می‌کند.**

**در مرحله هفتم، معادل نشانی آی‌پی نام www.microsoft.com برمی گردد.**

**در مرحله هشتم، نشانی آی‌پی خواسته شده در اختیار برنامه کاربردی قرار می‌گیرد.**

**پرس و جوی بازگشتی**

**در این روش هر گاه برنامه‌ای بخواهد نشانی آی‌پی معادل یک نام مثل cs.yale.edu را بدست آورد، بگونه‌ای که قبلاً اشاره شد، «تابع سیستمی تحلیل نام» را فراخوانی می‌کند. این تابع یک ماشین را بعنوان سرویس دهنده محلی از قبل می‌شناسد و بنابراین تقاضای تبدیل نام را به روش UDP برای آن ارسال کرده و منتظر جواب می‌ماند (پاسخ نهایی DNS طبیعتاً باید یک نشانی ۳۲ بیتی معادل نشانی آی‌پی یک ماشین باشد)**

**دو حالت ممکن است اتفاق بیفتد :**

**ممکن است در بانک اطلاعاتی مربوط به سرویس دهنده محلی، نشانی آی‌پی معادل با آن نام از قبل وجود داشته و بالطبع به سرعت مقدار معادل نشانی آی‌پی آن بر می‌گردد.**

**ممکن است در بانک اطلاعاتی سرویس دهنده محلی، معادل نشانی آی‌پی آن نام وجود نداشته باشد. مثلاً سرویس دهنده محلی در بانک اطلاعاتی خودش معادل نشانی آی‌پی نام cs.mit.edu را نداشته و طبیعتاً نمی‌تواند 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 می‌کند. یعنی اگر معادل نشانی آی‌پی آن نام را داشته باشد آنرا برمی گرداند و در غیر اینصورت خودش از سرویس دهنده سطح پایینتر تقاضای ترجمه آن نام را می‌نماید و این مراحل تکرار می‌شود. در روش پرس و جوی بازگشتی ماشین سرویس دهنده محلی این مراحل متوالی را نمی‌بیند 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 شبکه‌های کوچک کاربرد دارد.**

**پرس و جوی معکوس :**

**فرض کنید حالتی بوجود بیاید که یک سرویس دهنده DNS، نشانی آی‌پی 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 حادتر به نظر می‌رسد، چرا که برای ترجمه نامهای نمادین، چون این نامها دارای حوزه و زیرحوزه هستند، تحلیل نشانی ها ساده‌است. ولی ترجمه نشانی آی‌پی به معادل نام حوزه، از چنین روابطی تبعیت نمی‌کند؛ بعبارت بهتر هیچ ارتباط مستقیم و متناظری بین نشانی های آی‌پی و اسامی انتخاب شده در اینترنت وجود ندارد. برای یافتن نامهای متناظر با یک نشانی آی‌پی 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 آی‌پی، مشخص شده، ارسال می‌کند.**

**بعنوان مثال نشانی آی‌پی 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 آی‌پی 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**

**دهنده‌های متناظر با هر زیر شبکه پیگیری می‌کند. (چون هر زیر شبکه یک سرویس دهنده DNS مخصوص به خود دارد) نهایتاً یک نام نمادین حوزه معادل با آن نشانی آی‌پی بر خواهد گشت.**

**ساختار دامنه :**

**نام دامنه از ارقام و حروفی تشکیل شده‌است. یکی قسمت نام حوزه 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. نشانه‌های //: جهت جداسازی پروتکل از دامنه استفاده می‌شود.** http:// **جزء سامانه نام دامنه قرار نمی‌گیرد. قسمت** www **نام زیر دامنه‌است. قسمت** google **نام دامنه و قسمت** .com **حوزه می‌باشد. هر زیردامنه می‌تواند آدرس IP متفاوتی با نام دامنه داشته باشد.**

**نام دامنه و زیر دامنه را صاحب دامنه انتخاب و ثبت می‌کند.**

**این قسمت‌ها شامل حروف و اعداد انگلیسی و علامت منقی (-) نیز می‌تواند در میان اعداد و حروف (و نه در ابتدا و انتها) قرار گیرد.**

**حوزه های مختلف، توسط آیکان (Icann) تصویب و در دسترس قرار می‌گیرد و شامل ۲ تا ۶ حرف انگلیسی می‌باشد.**

**ثبت دامنه در بسیاری از حوزه ها نیاز به مجوزهای مخصوص دارد.**

**حوزه های ۲ حرفی، در اختیار کشورهای صاحب آنها قرار می‌گیرد و قوانین ثبت در این حوزه ها، توسط حکومت‌ها تعیین می‌گردد.**

**آیکان پروژه‌ای را در دست دارد تا ثبت نام‌های دامنه را به زبان‌های مختلف بین‌المللی 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 صرفا تعداد اندکی از آنان به منظور انتقال داده طراحی و پیاده سازی شده اند . اینترنت نیز به عنوان یك 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[1] است.**

[1] File Transfer Protocol

**ویژگی های پروتکل FTP**

- **پروتکل** FTP **، اولین تلاش انجام شده برای ایجاد یك 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 یك حاکم مطلق در عرصه مرورگرهای وب و سرویس دهندگان وب است ، نمی توان ادعای مشابهی را در رابطه با پروتکل** FTP **داشت و هم اینك مجموعه ای گسترده از سرویس گیرندگان و سرویس دهندگان** FTP **وجود دارد .**
- **برای ارسال فایل با استفاده از پروتکل** FTP **به یك سرویس گیرنده** FTP **نیاز می باشد . ویندوز دارای یك 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 هائی در این زمینه می باشند .**

**پروتکل** FTP **را می توان به عنوان یك سیستم پرس وجو نیز تلقی نمود چراکه سرویس گیرندگان و سرویس دهندگان گفتگوی لازم به منظور تائید 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 ( یك اتصال برای هر ارسال داده) با یکدیگر گفتگو خواهند کرد ( نمایش لیست فایل های موجود در یك دایرکتوری نیز به عنوان یك 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 یك 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 یك محیط تراکنشی می باشند که از مسائلی که قرار است در آینده محقق شوند ، آگاهی داشته باشند . در واقع ، پروتکل** FTP **یك دنباله** stateful **از یك 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 ، عموما سه و یا چهار حرفی می باشند (مثلا برای تغییر دایرکتوری از دستور** CWD **استفاده می شود ). سرویس دهنده نیز بر اساس یك فرمت استاندارد به سرویس گیرندگان پاسخ خواهد داد ( سه رقم که به دنبال آن از** space **استفاده شده است به همراه یك متن تشریحی ) . سرویس گیرندگان می بایست صرفا 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 یك سرویس گیرنده می تواند پس از دریافت داده آن را به فرمت مورد نظر خود ترجمه و استفاده نماید . مثلا در نسخه های ویندوز از یك دنباله** carriage return **و** linefeed **برای نشان دادن انتهای خط استفاده می گردد در صورتی که در سیستم های مبتنی بر یونیکس صرفا از یك**

linefeed **استفاده می شود . برای ارسال هرنوع 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 ارسالی را اطلاع دهد ) . معمولا سرویس گیرندگان ارسال باینری را انتخاب می نمایند و پس از دریافت فایل ، ترجمه لازم را انجام خواهند داد . ارسال باینری ذاتا 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 .**

**یك اتصال پروتکل** TCP/IP **( نسخه شماره چهار) شامل دو نقطه مجزا می باشد که هر نقطه از یك آدرس** IP **و یك شماره پورت استفاده می نماید . برقراری ارتباط بین یك سرویس گیرنده و یك 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 یك ارتباط، سرویس گیرنده از یك شماره پورت استفاده می نماید . این شماره پورت می تواند متناسب با نوع عملکرد برنامه سرویس گیرنده به صورت اختیاری و یا اجباری باشد . مثلا برخی برنامه های سرویس گیرنده به منظور ارتباط با سرویس دهنده ، نیازمند استفاده از یك 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 نماید) . در مواردی که الزامی در خصوص شماره پورت وجود ندارد از یك 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 مجددا درخواست برقراری یك ارتباط را نماید ، یك شماره پورت موقتی دیگر به وی تخصیص داده می شود .**

**پروتکل** FTP **منحصرا از پروتکل** TCP **استفاده می نماید( هرگز از پروتکل** UDP **استفاده نمی شود) . معمولا 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 معمولا 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 یك** 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 ( مثلا رمزنگاری توسط** IPsecs **) ، نمی بایست از** FTP **استفاده گردد خصوصا 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 یك درخواست ( PUT , GET ) برای یك سرویس دهنده** FTP **ارسال می گردد ، سرویس دهنده پاسخ خود را به صورت یك رشته اعلام**

**می نماید . اولین خط این رشته معمولا 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 یك پیام وضعیت به درخواست سرویس گیرندگان پاسخ می دهد . کدهای وضعیت برگردانده شده را می توان در پنج گروه متفاوت تقسیم نمود :**

**کدهای** ۱xx **: پاسخ اولیه**

**کدهای** ۲xx **: درخواست بدون خطاء اجراء گردید .**

**کدهای** ۳xx **: به اطلاعات بیشتری نیاز است .**

**کدهای** ۴xx **: یك خطاء موقت ایجاد شده است .**

**کدهای** ۵xx **: یك خطاء دائمی ایجاد شده است .**

**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 یك ارتباط است .**

**در ادامه به بررسی هر یك از روش های** Active **و** Passive **در پروتکل** FTP **خواهیم پرداخت .**

**:Active Mode**

Active Mode **، روش سنتی ارتباط بین یك سرویس گیرنده** FTP **و یك سرویس دهنده می باشد که عملکرد آن بر اساس فرآیند زیر است :**

- **سرویس گیرنده یك ارتباط با پورت ۲۱ سرویس دهنده** FTP **برقرار می نماید . پورت ۲۱ ، پورتی 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 یك 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 یك ارتباط را از طریق پورت ۲۰ خود با پورت مشخص شده سرویس گیرنده ( پورت** x+۱ **) برقرار می نماید .**

| | |
|---|---|
| **لطفا به من از طریق پورت ۱۹۳۱ بر روی آدرس** IP: **۱۹۲٫۱۶۸٫۱٫۲ متصل و سپس داده را ارسال نمائید .** | **سرویس گیرنده** |
| **تائید دستور** | **سرویس دهنده** |

**در فرآیند فوق ، ارتباط توسط سرویس گیرنده آغاز و پاسخ به آن توسط سرویس دهنده و از طریق پورت** x+۱ **که توسط سرویس گیرنده مشخص شده است ، انجام می شود . در صورتی که سرویس گیرنده از سیستم ها و دستگاه های امنیتی خاصی نظیر فایروال استفاده کرده باشد ، می بایست تمهیدات لازم به منظور ارتباط کامپیوترهای میزبان راه دور به سرویس گیرنده پیش بینی تا آنان بتوانند به هر پورت بالاتر از ۱۰۲۴ سرویس گیرنده دستیابی داشته باشند . بدین منظور لازم است که پورت های اشاره شده بر روی ماشین سرویس گیرنده** open **باشند . این موضوع می تواند تهدیدات و چالش های امنیتی متعددی را برای سرویس گیرندگان به دنبال داشته باشد .**

**Passive Mode**

**در** PassiveMode ، **که به آن " مدیریت و یا اداره سرویس گیرندگان** FTP" **نیز گفته می شود از فرآیند زیر استفاده می گردد :**

- **سرویس گیرنده دو پورت را فعال می نماید ( پورت** x **و** x+1 **)**
- **ارتباط اولیه از طریق پورت** x **سرویس گیرنده با پورت ۲۱ سرویس دهنده آغاز می گردد .**
- **سرویس دهنده یك پورت را فعال (** Y **) و به سرویس گیرنده شماره پورت را اعلام می نماید .**
- **در ادامه سرویس گیرنده یك اتصال از طریق پورت** x+1 **با پورت** y **سرویس دهنده برقرار می نماید .**

| | |
|---|---|
| **لطفا به من بگوئید که از کجا می توانم داده را دریافت نمایم** | **سرویس گیرنده** |
| **با من از طریق پورت ۴۰۲۳ بر روی آدرس IP: ۱۹۲٫۱۶۸٫۱٫۲۵ ارتباط برقرار نمائید .** | **سرویس دهنده** |

**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 بلاك نمایند . 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 آنجام 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 .**

**متاسفانه تمامی سرویس گیرندگان** FTP **از** Passive Mode **حمایت نمی نمایند . اگر یك سرویس گیرنده بتواند به یك 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 .**

**ملاحضات 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 . ترافیك فوق ، معمولا توسط فایروال سرویس دهنده بلاك 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 ۱۵۷۹** RFC **، 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 پیکربندی تا بتوانند از مجموعه پورت های محدود و تعریف شده ای با در نظر گرفتن مسائل امنیتی ، استفاده نمایند.**

**پیکربندی فایروال**

**جدول زیر پیکربندی 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, to any port >۱۰۲۴ | Server Outbound |
| Return traffic, any port > ۱۰۲۴ from server using any port >۱۰۲۴ | Client Inbound |

**و اما یك نكته دیگر در رابطه با پروتكل FTP !**

**در صورتی كه در زمان دریافت یك فایل با استفاده از پروتكل** FTP **مشكلات خاصی ایجاد كه منجر به قطع ارتباط با سرویس دهنده** FTP **گردد ، سرویس گیرنده می تواند با مشخص كردن یك** offset **از فایل دریافتی به سرویس دهنده اعلام نماید كه عملیات ارسال را از جائی كه 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 یك ساختار خاص برای ارسال و دریافت اطلاعات (بسته های اطلاعاتی ) استفاده نموده و ترافیك مختص به خود را در شبکه ایجاد می نماید .** HTTP **( برگرفته از** Hyper TextTransfer 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 یك 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 **ماموریت خود را انجام می دهد ، ولی این پروتکل** HTTP **است که به عنوان زبان مشترك 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 یك صفحه وب را می نماید.**

**به منظور انجام یك تراكنش موفقیت آمیز بین سرویس گیرندگان وب ( نظیر** IE **) و سرویس دهندگان وب ( نظیر** IIS **) ، به اطلاعات زیادی نیاز خواهد بود . پس از** handshake **پروتكل** TCP/IP **، مرورگر اطلاعات گسترده ای را برای سرویس دهنده وب ارسال می نماید .**

**یك بسته اطلاعاتی نمونه در شكل زیر نشان داده شده است :**


**توضیحات :**

**داده مربوط به پروتكل لایه** application **( در این مورد خاص پروتكل** 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 .**

| عملكرد | نوع اطلاعات |
|---|---|
| **سرویس گیرنده وب یك درخواست** GET **را برای سرویس دهنده وب ارسال و از وی درخواست اطلاعاتی را با** | GET /HTTP/۱٫۱ |

| | |
|---|---|
| **استفاده از پروتکل ۱٫۱ HTTP می نماید.**<br><br>**پروتکل HTTP دارای نسخه شماره یك نیز می باشد که امروزه عموما از نسخه فوق استفاده نمی گردد و در مقابل از نسخه ۱ . ۱ استفاده می شود.** | |
| **وب سایتی است که سرویس گیرنده قصد ارتباط با آن را دارد .** | **Host:**<br>www.google.ca |
| **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.** | **User-agent:**<br>Mozilla/**۵٫۰** (Windows; U; Windows NT **۵٫۱**; |
| **نوع** character set **استفاده شده به سرویس دهنده اعلام می گردد ( در این مورد خاص** | en-US; rv: **۱٫۷٫۱۰**) |

| | |
|---|---|
| **از** en:us **و نسخه شماره ۱۰ . ۷ . ۱ استفاده شده است ) .** | |
| **نام مرورگر استفاده شده توسط سرویس گیرنده به سرویس دهنده وب اعلام می گردد ( در این مورد خاص از مرورگر** FireFox **استفاده شده است ) .** | Gecko/**۲۰۰۵۰۷۱۶** Firefox/**۱٫۰٫۶** |
| **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 ) .** | **Accept:** text/xml, application/xml, application/xhtml+xml |
| **سرویس گیرنده به سرویس دهنده نوع فرمت متن دریافتی را اعلام می نماید ( در این مورد خاص** html **و یا** plaintext **) .**<br><br>**همچنین فرمت فایل های گرافیکی ( در این مورد خاص** png **. و سایر فرمت های** | text/html; q=٠٫**۹**, text/plain; q=٠٫**۸**, image/png, */*;q=٠٫**۵** |

| | |
|---|---|
| متداول ) نیز اعلام می گردد . | |
| لیست character set که سرویس گیرنده وب قادر به فهم آنان است، اعلام می گردد ( در این مورد خاص ISO-۸۸۵۹ , و یا utf-۸ ) . | **Accept-Charset:** ISO-۸۸۵۹-۱, utf-۸; q=۰/۷, *;q=۰/۷ |
| به سرویس دهنده وب مدت زمان نگهداری session اعلام می گردد ( در این مورد خاص ۳۰۰ ثانیه ) .<br><br>سرویس گیرندگان می توانند با صراحت پایان یك 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 .<br><br>در نسخه شماره یك پروتکل HTTP ، پس از هر درخواست و اتمام تراکنش ، ارتباط ایجاد | **Keep-Alive:** ۳۰۰ Connection: keep-alive |

| | |
|---|---|
| **شده غیرفعال و یا** close **می گردد .** | |
| cookie **و مقدار مربوطه به آن اعلام می گردد. کوکی یك متن اسکی فلت می باشد که اطلاعات متفاوتی را در خود نگهداری می نماید .**<br><br>**مدت زمان حیات یك کوکی می تواند موقت ( تا زمانی که مرورگر فعال است ) و یا دائم ( ذخیره بر روی هارد دیسك کامپیوتر و در یك محدوده زمانی تعریف شده ) باشد .** | **Cookie:**<br>PREF=ID=۰۱a۰۸۲۲۴۵۴acb۲۹۳:<br>LD=en:TM=۱۱۲۱۶۳۸۰۹۴.. |

Useragent **نوع مرورگر و سیستم عامل سرویس گیرنده را مشخص می نماید و این موضوع می تواند مواد اولیه لازم برای تدارك 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 یك 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 : یك معماری سرویس گیرنده و سرویس دهنده**

**سرویس گیرنده وب ، مقادیر خاصی را با اهداف کاملا مشخص شده برای سرویس دهنده وب ارسال می نماید ( حصول اطمینان از وجود یك 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 یك نرم افزار در سمت سرویس گیرنده و به عنوان یك سرویس گیرنده وب ( نظیر IE و یا Mozilla Firefox ) ایفای وظیفه می نماید و در سمت سرویس دهنده یك 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 یك بسته اطلاعاتی HTTP از مبداء یك سرویس دهنده به مقصد یك سرویس گیرنده را نشان می دهد ( پاسخ سرویس دهنده ).**

**توضیحات :**

**جدول زیر برخی اطلاعات ارسالی توسط سرویس دهنده را نشان می دهد .**

| عملکرد | نوع اطلاعات |
|---|---|
| **به سرویس گیرنده اعلام می گردد که :**<br>• **سرویس دهنده وب از پروتکل** HTTP **نسخه ۱.۱ استفاده می نماید.**<br>• **فایل درخواستی وی توسط سرویس دهنده پیدا شده است .**<br>**۲۰۰ ، یك كد وضعیت است كه وضعیت پاسخ به درخواست را مشخص می نماید .** | HTTP/۱٫۱ ۲۰۰ OK |
| **مستند و یا فایل درخواستی سرویس گیرنده توسط یك پراکسی** cache **نخواهد شد و هدف آن صرفا" برای کاربر متقاضی فایل است .** | **Cache-Control:** private |
| **فرمت ارسال فایل و یا مستند درخواستی به سرویس گیرنده وب اعلام می شود . در این مورد خاص ،** | **Content-type:** text/html |

| | |
|---|---|
| **اطلاعات با فرمت** text/html **ارسال می گردند .**<br><br>**سرویس گیرنده وب دارای دانش لازم به منظور بررسی و نمایش اطلاعات با فرمت اشاره شده می باشد .** | |
| **نوع سرویس دهنده و یا نرم افزار سرویس دهنده ( سرویس دهنده وب ) مشخص می گردد .**<br><br>**در این مورد خاص ، سرویس دهنده وب** Google **نمایش داده شده است .** | **Server:**<br>GWS/۲٫۱ |
| **پروتکل** HTTP **نسخه شماره ۱ .۱ از ارسال اطلاعات به صورت** chuncked **حمایت می نماید. در روش فوق ، بدنه یك 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 .**<br><br>**در صورت ارسال معمولی اطلاعات توسط پروتکل** HTTP **، از یك فیلد با نام** "Content-Length" **به منظور** | **Transfer-Encoding:**<br>chunked |

| | |
|---|---|
| **مشخص نمودن حجم داده ارسالی،استفاده می گردد .** | |
| **زمان و تاریخ سرویس دهنده وب مشخص می گردد.** | **Date:**<br>Sat ۳۰ Jul ۲۰۰۵ ۱۴:۱۴:۵۰ GMT |
| **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 **یك صفحه وب را مشاهده نمود .** | <html><head><meta.http-equiv="content-type" |

**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 .**

**یك سرویس دهنده وب در واقع به عنوان یك سرویس دهنده HTTP نیز ایفای وظیفه می نماید .**

**زمانی که مرورگر وب درخواست یك صفحه را از سرویس دهنده وب می نماید، در واقع یك** HTTPrequest **را ارسال و سرویس دهنده وب نیز پاسخ آن را با یك** HTTP response **خواهد داد. یك پیام** HTTP **، یك درخواست (** request **) و یا پاسخ (** response **) است که از یك ساختار خاص تبعیت می نماید .**

HTTP **به یك پروتکل خاص لایه حمل وابستگی نداشته و عموما از پروتکل** TCP **استفاده می نماید (پورت شناخته شده ۸۰ ) .**

**کدهای وضعیت:**

**همانند بسیاری از پروتکل ها ، پروتکل** HTTP **بر اساس یك 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 | راهنمائی مجدد |
| ۴XX | بروز خطاء سمت سرویس گیرنده |
| ۵XX | بروز خطاء سمت سرویس دهنده |

**هر یك از پنج گروه فوق، دارای کدهای وضعیت زیر مجموعه ای می باشند که بیانگر جزئیات عملیات است . جدول زیر برخی از کدهای وضعیت هر یك از گروه های پنج گانه فوق را در ارتباط با پروتکل** HTTP **نشان می دهد .**

| عملکرد | کد وضعیت |
|---|---|
| تراکنش با موفقیت انجام شده است | ۲۰۰ |
| دستور POST با موفقیت انجام شده است | ۲۰۱ |
| درخواست ارسالی دریافت گردید. | ۲۰۲ |
| منبع درخواستی در مکان های مختلفی پیدا شده است | ۳۰۰ |
| منبع درخواستی به صورت دائم منتقل شده است | ۳۰۱ |
| منبع درخواستی به صورت موقت منتقل شده است | ۳۰۲ |
| درخواست نامناسب از جانب سرویس گیرنده | ۴۰۰ |
| درخواست غیرمجاز | ۴۰۱ |
| منبع درخواستی پیدا نگردید | ۴۰۴ |
| بروز خطاء بر روی سرویس دهنده | ۵۰۰ |
| متد استفاده شده ، پیاده سازی نشده است | ۵۰۱ |

**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 یك 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 یك مستند جایگزین را برای سرویس دهنده وب ارسال می نماید .**

- **HEAD: سرویس گیرنده وب اطلاعات خاصی را در ارتباط با یك منبع موجود بر روی سرویس دهنده درخواست می نماید ( عدم نیاز به خود منبع )**
- **DELETE : سرویس گیرنده وب درخواست حذف یك 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 یك سند توسط یك سرویس گیرنده وب درخواست می گردد .**
- **CONNECT : سرویس گیرنده وب به عنوان یك پراکسی به یك سرویس دهنده** HTTPS **متصل می گردد .**

**در اغلب موارد صرفا از متد** GET **و در برخی موارد از** HEAD **استفاده می گردد ( در صورت اشکال زدائی یك برنامه وب از تمامی امکانات فوق استفاده می شود ) .**

**مراحل ایجاد یك تراکنش :**

**یك سرویس گیرنده وب قبل از این که بتواند با یك 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 یك درخواست و پاسخ به آن از پروتکل** HTTP **استفاده نموده و ارتباط ایجاد شده بین خود را صرفا برای یك تراکنش نگهداری می نمایند (** HTTP **یك پروتکل** Stateless **است ) .**

**فرآیند ایجاد یك 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 یك ارتباط و یا اتصال مبتنی بر پروتکل** TCP/IP **بین یك سرویس دهنده و یك سرویس گیرنده وب ایجاد گردد . به منظور تشخیص نوع پروتکل استفاده شده ، برنامه ها از یك 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 یك 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 یك ارتباط باشند . مثلا 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 ست 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 میزند و به اصلاح شروع به** sniff **کردن میکند 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 روانه می شوند . به این نوع حمله** man in themiddle(mitm) attack **می گویند می تواند پکت های ارسالی شما به سرو وب را دیده و اگر این دیتا ها رمز نگاری نباشند خواندن محتوی آنها برای هکر کار بسیار 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** CertificateAuthority( 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** verisign - godaddy - ...

**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 درمحیط** 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 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 **نبودن** cerfitiface **را می گیرند و احتمالا به آن** trust **نمیکنند اطلاعات مربوط به** Cerfiticate **را می تواند در همان** url **در قسمت** cerfiticate information **دید که صادر کنند ه 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 درامد یعنی که این** Cerfiticate **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 شخص یک** certificate **جعلی را به ما بدهد تا بتواند پسورد و سایر اطلاعات مهم ما را بدست آورد . پس باید دقت کنیم که هر** cerfiticate **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 ۳ و 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 سریعا از آن محیط** sign out **کنند و از محیطی که این مشکل را ندارد مجددا لاگین کرده و تمامی پسورد ها و ایمیل های** recovery **و ... را تعویض کنند .این نکته را اضافه می کنم که اگر هکر ایی 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 فایلهای 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 روی۱۴۳** port **قرار دارد وبه 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 دهنده۲۰** -tops **تکمیل شد . هیچ کپی از نسخه اول پروتکل دسترسی موقت وجود ندارد و تنظیمات پروتکل نسخه اصلی به۲** imap **برگردانده شده است، گر چه بعضی از فرمان ها وجواب ها شبیه به۲** imap **است . اما پروتکل دسترسی موقت فاقد فرمان ها وپاسخ ها است اما با این حال با ترکیب این فرمان ها وعلامت ها باعث ایجاد یک نسخه از** imap **شده است که سازگار با تمام نسخه های** imap **می باشد .**

## معایب IMAP

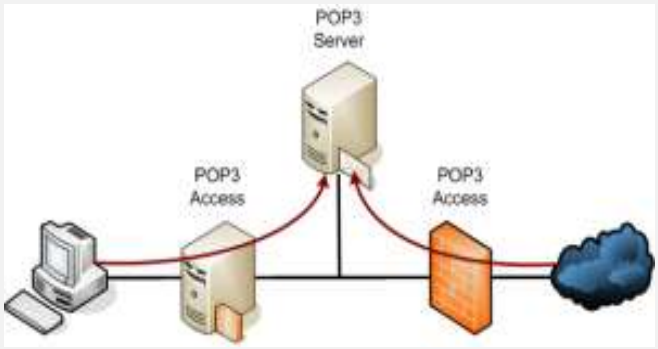
**یک سری نقاط ضعف در این پروتکل وجود دارد که باعث افزایش پیچیدگی می شود مثلا دسترسی همزمان چند سرویس گیرنده به یک** mail box **که این کار توسط سرویس دهنده جانبی مانند (** maildir، database **) صورت می گیرد و باعث رفع و تصحیح ضعف می شود . اما در این حالت لازم است که الگوریتم جستجو و ذخیره یک میل بر روی 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 کنند 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 تائید 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 **ودومی را برای** imap **جهت ذخیره و ارسال به پوشه میل 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 افزار ی 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[1] در اصل یک پروتکل دریافت ایمیل بر روی شبکه اینترنت است و اصولاً در لایه** Application **در پروتکل** TCP/IP **قرار می‌گیرد. با استفاده از این امکان شما می‌توانید در کامپیوتر خود، بدون نیاز به مراجعه به سایت سرویس دهنده ایمیل‌هایتان 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.

[1] Post Office Protcol ۳

**POP۳ این قابلیت را به کاربرانش می‌دهد 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 POP۳ دریافت می‌کنید، ایمیل از روی سرور پاک می شود. البته اکنون اکثر سرویس دهنده‌های POP۳ قابلیتی به نام Leave onServer دارند که اصطلاحاً به آن UIDL[۱] POP۳می گویند.**

**معایب POP۳ :**

**با وجود مزایای چشمگیر و بالای پروتکل POP۳ ، 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 POP۳ 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 قطعا مفید خواهد بود اما فقط در ۶۰ درصد موارد مفید می باشد.**

[۱] Unique IDentificationListing

**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** POP۳ **نیاز به روزآوری و جلو رفتن با تکنولوژی های مدرن را دارد.**

**تفاوت POP۳ و IMAP :**

**به طور مثال در** POP۳ **پس از دریافت ایمیل‌ها، آنها از روی سرور پاک شده در صورتی که در** IMAP **اینگونه نیست و ایمیل‌ها پس از دریافت از روی سرور پاک نمی‌شوند. شما از طریق** IMAP **این امکان را خواهید داشت که بدون دانلود کردن ایمیل‌های خود از روی سرور درون ایمیل‌های خود جستجو کنید پوشه بسازید تغییر نام دهید و حتی ایمیل‌ها را پاک کنید ،** mailbox **خود را برای ایمیل‌های جدید چک کنید و کلی امکانات دیگر. این امکانات به تدریج باعث جایگزینی**IMAP **به جای** POP۳ **می‌شود. یکی از پر استفاده‌ترین 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 POP۳ در کلاینت ها:**

**اگر حساب ایمیل شما از** POP۳ **و** IMAP۴ **پشتیبانی می کند، می توانید از برنامه های ایمیل** POP۳ **و** IMAP۴ **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** POP۳ **و** IMAP۴ **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 | iPhone Mail |
| Windows Mobile 5 یا نسخه های بالاتر | Windows Mobile Mail |

**مقایسه‌ی پروتکل IMAP و POP۳**

**۱- پروتکل pop۳ نامه‌های الکترونیکی موجود در پوشه‌ی Inbox روی سرویس‌دهنده را مرور کرده و تمام پیام‌های جدید را یك مرتبه و خیل سریع بر روی کامپیوتر شما دانلود می‌کند. پروتکل IMAP سربرگ (Headers) تمام پیام‌های جدید را دانلود کرده و زمانی که شما قصد خواندن آن پیام را دارید و بر روی آن کلیك می‌کنید آنگاه پیام را بر روی سیستم شما دانلود می‌کند. به همین دلیل سرعت بازیابی پیام‌ها در IMAP کم‌تر می‌باشد.**

**۲- پروتکل pop۳ پیام‌ها به صورت OffLine (زمانی که با سرویس دهنده‌ی پست الکترونیکی ارتباط ندارید) نیز قابل دسترس خواهد بود ولی در پروتکل IMAP حتماً باید با سرویس دهنده‌ی پست الکترونیکی در ارتباط باشید.**

**۳- پروتکل pop۳ در مواردی مفید است که شما نامه‌های پستی خود را تنها از روی یك کامپیوتر بررسی می‌کنید ولی مواقعی که می‌خواهید از روی چند کامپیوتر (منزل، اداره و ...) نامه‌های پستی خود را بررسی کنید استفاده از پروتکل imap مفیدتر خواهد بود.**

**۴- در پروتکل IMAP پیام‌های شما از جمله پیام‌هایی که در پوشه‌ی Sent-mail ذخیره شده است از روی کامپیوتر دیگر قابل مشاهده نیست.**

**۵- در پروتکل pop۳ پیام‌های پوشه‌ی Inbox از روی سرویس دهنده پاك می‌شود و شما تنها به همان پیام‌ها دسترسی دارید ولی در پروتکل IMAP تمام پوشه‌های ایجاد شده بر روی سرویس دهنده قابل مشاهده و قابل پیمایش خواهد بود و تغییرات انجام شده بر روی سرویس دهنده نیز اعمال می‌گردد.**

**۶- در پروتکل pop۳ برای دستیابی به آخرین بروزرسانی باید بر روی دکمه‌ی Send/Receive کلیك کنید ولی در در پروتکل IMAP همواره با رسیدن پیام جدید خود به صورت خودکار بروزرسانی می‌گردد.**

**۷- در پروتکل pop۳ به دلیل اینکه پیام‌ها بر روی فضای هارد دیسك 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 POP۳ را پشتیبانی می‌کنند ولی به دلیل پیچیدگی پروتکل IMAP تعداد کمی از ISPها و برنامه‌های پست الکترونیکی پروتکل IMAP را پشتیبانی می‌کنند.**

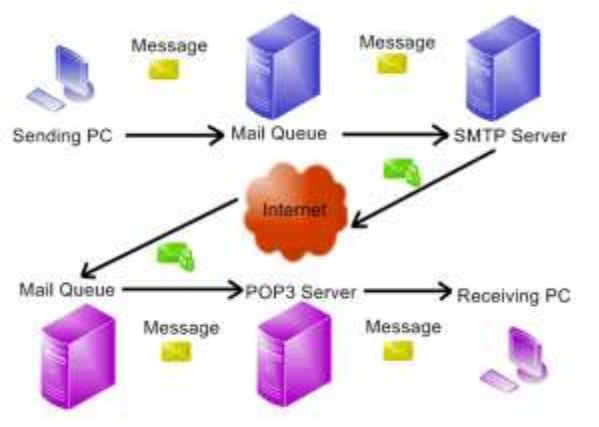
**۹- در پروتکل IMAP انتقال حساب کاربری میل از یك سیستم به سیستم دیگر آسان است، ولی در پروتکل POP۳ به دلیل اینکه میل‌ها به صورت فایل بر روی سیستم ذخیره می‌شود مشکل است و ممکن است انتقال میل‌ها از یك برنامه به برنامه‌ی دیگر به دلیل پشتیبانی نکردن از آن نوع سیستم فایل امکان‌پذیر نباشد .**

# درس ۸

## Smtp

**SMTP[1] یکی از پروتکل‌های TCP/IP برای ارسال و دریافت نامه‌های الکترونیکی است. این پروتکل به دلیل محدودیت‌هایی در نگهداری نامه‌ها، معمولا با پروتکل‌های POP۳ یا (IMAP )[2] استفاده می‌شود.**

**SMTP برای کاربران امکان ذخیره نامه‌ها را روی یک سرور یا دانلود آنها را از سرور فراهم می‌کند. در حقیقت می‌توان گفت، SMTP برای ارسال نامه‌ها و POP۳ یا IMAP برای دریافت نامه‌ها به کار می‌روند.**




**SMTP معمولا از پورت ۲۵ برای ارسال نامه‌ها استفاده می‌کند. POP۳ رایج‌ترین پروتکل استاندارد برای دریافت نامه‌ها به‌شمار می‌آید که از پورت ۱۱۰ برای دریافت نامه استفاده می‌کند. در کنار این پروتکل IMAP هم وجود دارد. SMTP در واقع پروتکلی است که جهت انتقال پست الکترونیکی استفاده می‌شود. این پروتکل استاندارد اینترنتی برای ارسال پست الکترونیکی در میان**

[1] simple mail transfer protocol
[2] Internet message access protocol

**پروتکل‌های شبکه است. این تعریف جز تعاریف اولیه** SMTP **در علم شبکه بود و آخرین تعریف و نسخه به‌روزرسانی شده آن** SMTP **گسترش یافته (**ESMTP**) را شامل می‌شود. امروزه این پروتکل به طور گسترده استفاده می‌شود.تعداد زیادی سرور** SMTP **به صورت رایگان وجود دارد که می‌توان به خوبی از آنها استفاده کرد.**

SMTP **توسط ۸۲۱** RFC **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 ی 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 ساده‌تر، سرور** SMTP**، مانند وب سرور ، یک رایانه است که مانند مسیریاب عمل می‌کند. هنگامی که پیام‌های پست الکترونیکی را از کاربران دریافت می‌کند آنها را به گیرندگان مورد نظر می‌فرستند. سرورهای** SMTP **از پروتکل‌های ساده انتقال پست الکترونیکی یا برنامه ارسال پست الکترونیکی یونیکس استفاده می‌کنند. اغلب پیام‌ها 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** IIS **اعمال کنید.**

**تنظیمات سرور SMTP (اکثر مثالها در ویندوز است چرا که تنظیمات لینوکسی هم کاری حرفه ای می باشد هم خود لازمه یک کتاب چند جلدی است ! )**

**شما با استفاده از مراحل زیر می‌توانید خدمات سرویس** SMTP **نصب‌شده 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 می‌بینید 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 می‌شود. ذخیره پیام در** LocalDrive:\Inetpub\Mailroot **واقع شده است. اگر برای اولین بار می‌خواهید تنظیمات مربوط به سرور مجازی** SMTP **یا تنظیمات کامپوننت های آن‌را 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 می‌کند.**

RCPT TO: **با استفاده از این دستور آدرس گیرندگان پست الکترونیکی مشخص می‌شود.**

DATA: **شامل داده‌های واقعی (بدنه متن، ضمیمه و...) است.**

RSET (RESET): **این دستور مشخص‌کننده تراکنش پست الکترونیکی جاری، ارسال شده یا به‌طور 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 می‌کند.**

QUIT: **این دستور به این معنی است که سرور فضای تخصیص داده‌شده به آن را آزاد می کند.**

**تعدادی سرور** SMTP **رایگان برای ارسال پست الکترونیکی به‌طور مستقیم وجود دارد. بیشتر این برنامه‌ها کار پشتیبانی را انجام می‌دهند، برنامه‌های پست الکترونیکی مانند** Outlook Express **و** Eudora **از جمله این برنامه‌هاست که در مقایسه با** Outlook Express **ساده‌تر می باشد. امروزه یکی از سرورهای** SMTP **رایج، سرور** SMTP **جی‌میل است. سرور** SMTP **حتی برای مواقعی که در مکان‌های 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 می‌کند.**

**برخی ویژگی های SMTP :**

**برخی توابع ارسال ایمیل را پشتیبانی نمی کند .**

**مسائل امنیتی مشخص شده در** X.۴۰۰ **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** MTA[۱] **استفاده می کند.**

[۱] mail 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 پادمان‌های موجود در اینترنت مانند HTTP منتقل می‌شود (SOAP در سایر پادمان ها، مانند SMTP یا MIME نیز قابل استفاده است). به زبان ساده‌تر، SOAP یک پادمان است برای دستیابی به یک سرویس ارایه شده در وب (Web Service). آخرین نسخه SOAP، نسخه ۱٫۲ می‌باشد.**

**ویژگی های SOAP**

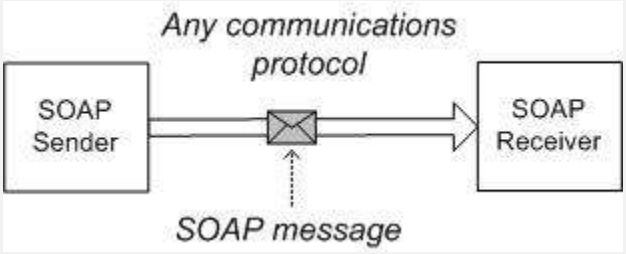
۱. **یک پادمان ارتباطی است.**
۲. **برای ارسال پیام استفاده می‌شود.**
۳. **برای محیط اینترنت و شبکه طراحی شده است.**
۴. **وابسته به محیط پیاده سازی و اجرا نیست. ( Platform Independent)**
۵. **مبتنی بر XML است.**
۶. **از دیوارهای آتش (Firewall) گذر می‌کند ودیوارهای آتش مانع آنها نمی شوند (Block نمی‌شوند).**

**یکی از مسایلی که در دهه اخیر از اهمیت خاصی برخوردار بوده، چگونگی ارتباط برنامه های تحت اینترنت با یکدیگر بوده است. همانطور که می‌دانید برنامه های عادی از RPC[۲] برای فراخوانی**

[۱] Simple Object Access Protocol
[۲] Remote Procedure Call

**اشیاء** DCOM **یا** CORBA**، استفاده می‌کنند. اما مشکلی که در این نوع فراخوانی‌ها در بستر اینترنت وجود دارد، مسدود شدن این نوع ترافیک‌ها در** Server **ها و دیوارهای آتش (**Firewall **ها) است.**

**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.**

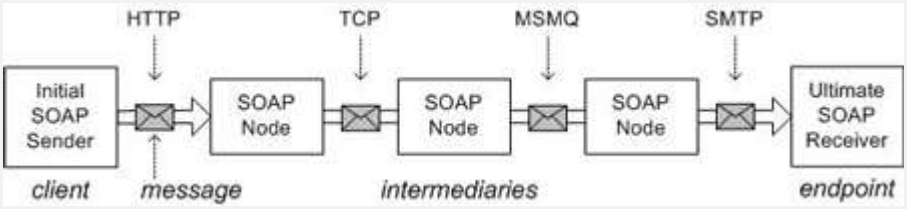



**ساختار SOAP**

**پیام ها (**Message **ها) در** SOAP **یک فایل** XML **هستند که از ساختار زیر پیروی می‌کنند:**

- **یک بخش ضروری که به آن** Envelope **(پاکت نامه) گفته می‌شود که مشخص می‌کند 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 درخواستِ برنامه‌ی سرویس گیرنده یا پاسخ برنامه سرویس دهنده است.**
- **قسمت** Fault **که قسمت خطا است و اختیاری است و اطلاعاتی درباره خطاهای بوجود 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 می‌کند که فیلدهای آمده در** XML **از چه نوع هستند و با چه ترتیبی می‌آیند. 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 می‌گیرند.**

**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 در خواست بفرستید، می توانید این کار را انجام دهید.**

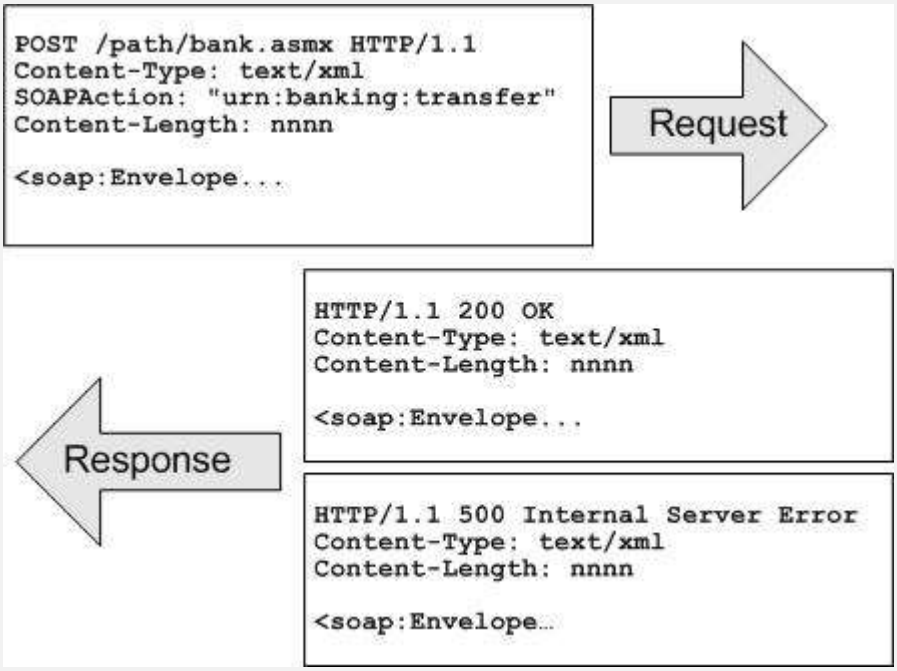
**برنامه کارگزار نیز، با استفاده از یک فایل** XML **پاسخ مشتری را می دهد و قیمت را در یک برچسب با عنوان** m:GetPriceResponse **به مشتری تحویل می دهد.**

```
POST /InStock HTTP/۱,۱
Host: www.stock.org
Content-Type: application/soap+xml; charset=utf-۸
Content-Length: nnn

<?xml version="۱,۰" ?>
<soap:Envelope xmlns:soap="http://www.w۳.org/۲۰۰۱/۱۲/soap-envelope"
soap:encodingStyle="http://www.w۳.org/۲۰۰۱/۱۲/soap-encoding">
    <soap:Body>
          <m:GetPrice xmlns:m="http://www.w۳schools.com/prices">
                <m:Item>Apples</m:Item>
          </m:GetPrice>
    </soap:Body>
</soap:Envelope>
```

```
HTTP/١,١ ٢٠٠ OK
Content-Type: application/soap; charset=utf-٨
Content-Length: nnn

<?xml version="١,٠" ?>
<soap:Envelope xmlns:soap="http://www.w٣.org/٢٠٠١/١٢/soap-envelope"
soap:encodingStyle="http://www.w٣.org/٢٠٠١/١٢/soap-encoding">
    <soap:Body>
          <m:GetPriceResponse xmlns:m="http://www.w٣schools.com/prices">
                <m:Price>١,٩٠</m:Price>
          </m:GetPriceResponse>
    </soap:Body>
</soap:Envelope>
```




## 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 مایکروسافت با نام** GXA[1] **ارایه شد. که یک پیاده‌سازی ازآن** WSE[2] **است.** WSE **یک ابزار قدرتمند است که شما با استفاده از** DotNet Framework **و** WSE **می توانید وب سرویس های امن و قدرتمند بنویسید. به بیان ساده‌تر** 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.**

[1] Global XML Web Services Architecture
[2] Web Services Enhancements

## درس ۱۰

## اس اس اچ چیست و چه تفاوتی با اف تی پی دارد؟

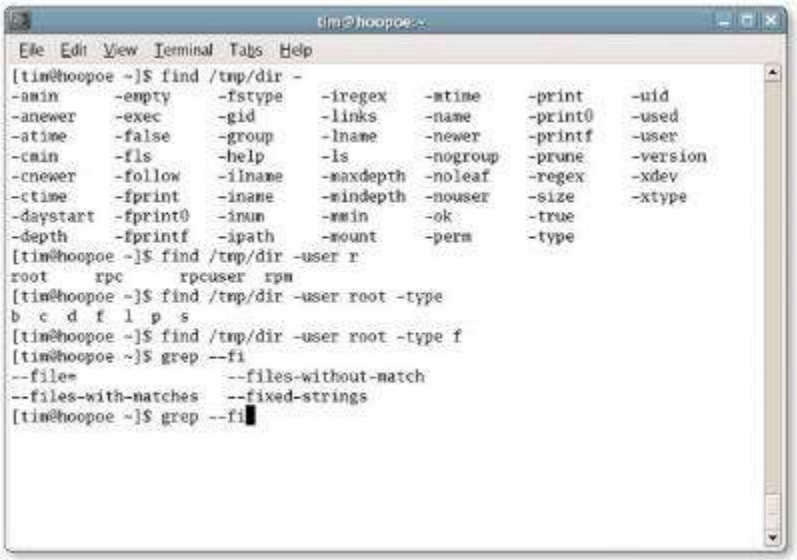
**هر دو پروتکل هایی تحت شبکه هستند که درست مانند HTTP بالای لایه TCP/IP اجرا می گردند. به زبان ساده این یک راه شناخته شده برای ابزارها است، تا درون شبکه با یکدیگر تماس برقرار کنند.**

**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 FTP و SSH دقیقا 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 مستقیما 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.**



**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.**

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-۱ **و** SSH-۲ **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[۱] **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.**

[۱] Secure Shell Protocol

**پروتکل انتقال فایل امن یا STTP در برابر FTP**

**انتقال فایل واجرای** 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 ۲-**SSH **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. بنابرین 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 ۲-**SSH **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 تقریبا منتفی می گردد.**

SFTP **معمولا 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[1] **راه حلی جهت برقراری ارتباطات ایمن میان یک سرویس دهنده و یک سرویس گیرنده است که توسط شرکت** Netscape **ارایه 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 **عموما 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**

[1] Secure 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 Rocord 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 تبادلی 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 Exchcenge Algorithm)**نظیر**:

RSA,RC۴,RC۲,MD۵,KEA,DSA,DES,RSA Key Exchange ،Skipjack, SHA-۱,DES۳

**پشتیبانی می شود و بسته به این که نرم افزارهای سمت سرویس دهنده و سرویس گیرنده 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**DES۳ **با طول کلید ۱۶۸ بیت برای رمزنگاری داده ها و همچنین الگوریتم** SHA-۱ **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 ارایه می کند. یک جلسه** SSL (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 هشداری 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 معمولا 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.**

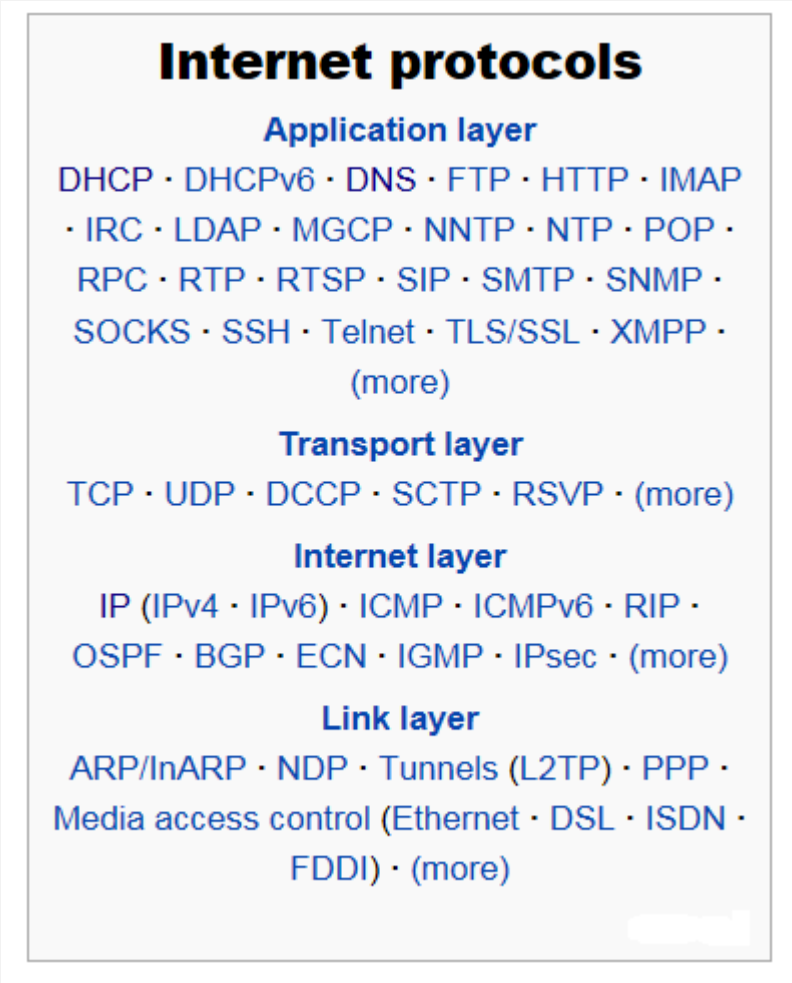
**۸ -سرویس گیرنده پیغامی را به سرویس دهنده می فرستد تا به او اطلاع دهد، داده بعدی که توسط سرویس گیرنده ارسال می شود به وسیله کلید جلسه رمزنگاری خواهد شد و در ادامه،**

**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 این فصل در ذهن شما شکل زیر را قرار میدهم.**



# 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 می باشند 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 می پردازیم.**

## درس ۱

## پینگ

**پینگ یک ابزار شبکه‌ای است که برای آزمایش میزان دسترسی‌پذیری یک میزبان در شبکهٔ پروتکل اینترنت به کار می‌رود و می‌تواند زمان رفت و برگشت برای بسته‌های فرستاده‌شده از میزبان عامل تا یک رایانهٔ 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 سیستم‌عاملی متفاوت است که می تواند بنا به نیاز ما حالت‌های خاص عملیاتی را فعال کند. این گزینه‌ها می توانند سایز بستهٔ آزمایشی را تغییر اندازه دهد، یا انجام** ping **به صورت تکراری برای دفعات محدود یا انجام دادن** ping flood **(نوعی از حملات** Dos**).**

## 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 پاکت** echo request **توسط کامپیوتر ما به دستگاه مقصدارسال می شود و در هر مرحله ای از این مسیر پاکت** exho reply **ایجاد شده و به کامپیوتر مبدا (کامپیوتر ما) ارسال می شود.**

**موارد استفاده از دستور** tracer:

**جدول زیر برخی از سوئیچ های متدوال 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 | |
| **سوئیچ** | **عملکرد** |
| -d | **آدرس** IP **را به نام** Host **ترجمه می نماید.** |
| -h | **حداکثر برای تعداد** hop |
| Maximum_hops | **مقصد مشخص را جستجو می نماید.** |
| -w timeou | **مدت زمان انتظار را برای دریافت پاسخ بر حسب میلی ثانیه مشخص می نماید.** |

**نحوه عملکرد دستور** tracert :

**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 TTLموجود 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 IPدورانداخته شود ). مقدار TTLدر 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**.

eth۰ Link encap:Ethernet HWaddr ۰۰:۶۰:۰۸:۱۷:۶۳:A۰

inet addr:۱۹۲٫۱۶۸٫۱٫۱۰۱ Bcast:۱۹۲٫۱۶۸٫۱٫۲۵۵ Mask:۲۵۵٫۲۵۵٫۲۵۵٫۰

UP BROADCAST RUNNING MTU:۱۵۰۰ Metric:۱

RX packets:۹۱۱ errors:۰ dropped:۰ overruns:۰ frame:۰

TX packets:۸۰۴ errors:۰ dropped:۰ overruns:۰ carrier:۰

collisions:۰ txqueuelen:۱۰۰

Interrupt:۵ Base address:۰xe۴۰۰

lo Link encap:Local Loopback
inet addr:۱۲۷٫۰٫۰٫۱ Mask:۲۵۵٫۰٫۰٫۰

UP LOOPBACK RUNNING MTU:۳۹۲۴ Metric:۱

RX packets:۱۸ errors:۰ dropped:۰ overruns:۰ frame:۰

TX packets:۱۸ errors:۰ dropped:۰ overruns:۰ carrier:۰

collisions:۰ txqueuelen:۰

**دستور** ifconfig **آدرس** 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 کامپیوتر های دیگر را ندارد.**

**مطمئن شوید آدرس** TCP/IP **و** Subnet mask **دستگاه کامپیوتر شما درست هستند. در صورتیکه شبکه از** DHCP **استفاده می کند مطئمن شوید که** DHCP **بر روی کامپیوتر شما**enable **است.**

**۲-امکان ارتباط با کامپیوتر های محلی وجود دارد اما ارتباط با کامپیوتر های 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 چك 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 پاك می شود.**

renew**آدرس** IP **کارت شبکه پاك شده و دوباره ایجاد می گردد.**

## درس ۴

### netstat چیست ؟

**یکی دیگر از دستوراتی که برای خطایابی** TCP/IP **می توان از آن استفاده کرد** netstat **می باشد.این دستور وضعیت پروتکل و کلیه ی ارتباطات و تنظیمات در حال حاضر** TCP/IP **مربوط به شبکه ، کلیه ی پورتهایی که در حال استفاده هستند و همچنین جداول مسیریابی 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 درحال 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 واطلاعات 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

**یک** Syntax **ویژه از پروتکل جهانی و انحصاری** URL **است که بر روی پورت ۲۳ راه اندازی می شود ولی بر این دلیل نیست که نتوانیم بر روی پورتهای دیگر** Telnet **را استفاده نمائیم.**

**تقریباً شماتیک کلی یک** URL **به صورت زیر است:**

```
<scheme>:< scheme-specific-part >

ftp                     File Transfer protocol
http                    Hypertext Transfer Protocol
gopher                  The Gopher protocol
mailto                  Electronic mail address
news                    USENET news
nntp                    USENET news using NNTP access
telnet                  Reference to interactive sessions
wais                    Wide Area Information Servers
file                    Host-specific file names
prospero                Prospero Directory Service
```

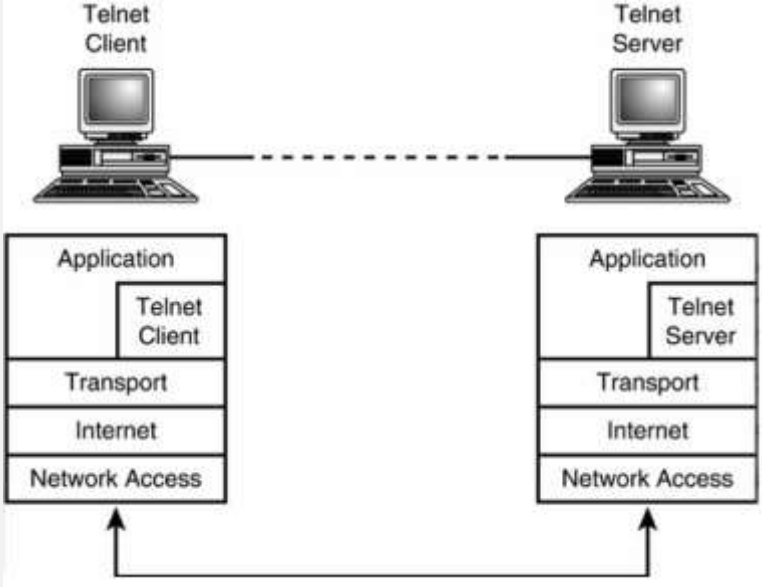
**دستور کلی استفاده از** Telnet**به صورت زیر است:**

```
telneturl       = "telnet://" login [ "/" ]
```

**تعریف عامیانه** Telnet **که کاربرد آن را بیان می کند عبارت است از اینکه دو کامپیوتر به طور مثال از طریق** Telnet **صحبت می کنند .**

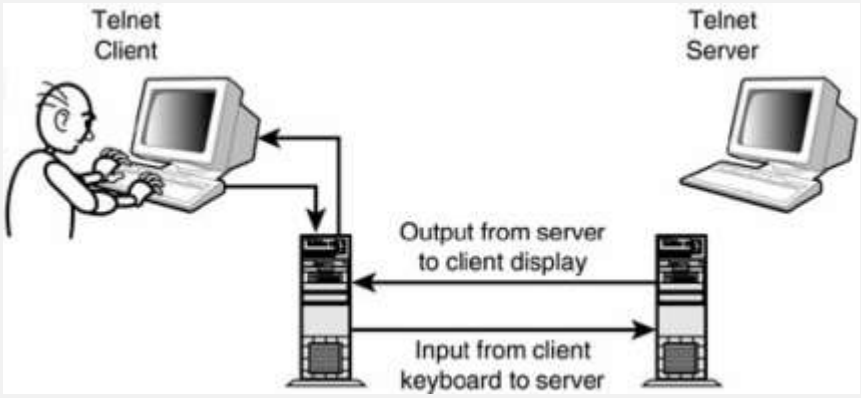
**تعریف دقیق و علمی** Telnet **عبارت است از اجرای جلسات کاری تاثیر گذار بر هم که همانند بیشتر پروتکلها یک سیستم سرویس گیرنده و یک سیستم سرویس دهنده دارد .**

**در شکل زیر سناریوی کارکرد یک جلسه کاری** Telnet **را مشاهده می نمائید و همانطور که در شکل مشاهده می کنید این یک پروتکل خارج از لایه اول** OSI **است و نیاز بنیادی به سخت افزار خاصی ندارد و همچنین اصول فرمانی آن به نرم افزار یا یک سیستم عامل خاص هم محدود نمی شود .**




**همانطور که مشاهده می کنید این یک ارتباط تاثیر گذار دو طرفه است از طرفی دیگر این یک پروتکل بسیار منعطف و باز می باشد که برای طیف وسیعی از کاربردها بر روی شبکه و بر روی بسیاری از سخت افزارها قابل استفاده است .**

**بر طبق شکل زیر یکی از پر کاربردترین استفاده های پروتکل** Telnet **این است که کاربری از طریق کیبورد و با استفاده از سطر فرمان بر روی یک کامپیوتر خارجی و یا سرور** Login **کند .**



**یکی از پر استفاده ترین دستورات بر روی سیستم های NIX * همین Telnet است که به صورت سطر فرمان استفاده می شود ، شکل استفاده بسیار ساده است :**

telnet hostname

hostname **نام کامپیوتری است که قصد اتصال به آن را دارید و یا می توانید شماره IP آن را به منظور اتصال باشد .**

**در یک جلسه کاری Telnet وقتی شما دستوری را اجرا می کنید ، آن دستور بر روی سیستم هدف اجرا می شود و همچنین Telnet فرمان های خاصی را نیز فراهم می نماید که مهمترین آنها :**

- close– Use this command to close the connection.
- display– Use this command to display connection settings, such as the port or terminal emulation.
- environ– Use this command to set environment variables. Environment variables are used by the operating system to provide machine-specific or user-specific information.
- logout– Use this command to log out the remote user and close the connection.
- mode– Use this command to toggle between ASCII or binary file transfer mode
- open– Use this command to connect to a remote computer.
- quit– Use this command to exit Telnet.

- send– Use this command to send special Telnet protocol sequences to the remote computer, such as an abort sequence, a break sequence, or an end-of-file sequence.
- set– Use this command to set connection settings.
- unset– Use this command to unset connection parameters.
- ?– Use this command to print Help information.

**خوب همان طور که قبلاً گفتیم Telnet بر روی پورت ۲۳ راه اندازی می شود که از دسته اول پورتهای شناخته شده است ولی شما میتوانید به هر پورت سیستم هدف Telnet نمائید .**

**هدف از انجام این کار میتواند به چند علت باشد اولین چیز ممکن است زنده یا مرده بودن یک پورت را نشان دهد یعنی در صورت برگشت هر نوع اطلاعاتی از پورت مربوطه نشان از زنده بودن**

**پورت است و در غیر اینصورت پورت بسته است و اگر در صورت** Telnet **به یک** blank screen **برخورد نمودید بدانید آن ارتباط دیگر زنده نیست و بایستی یک پورت دیگر را** Telnet **نمائید .**

**در بعضی از مواقع عدم ارتباط با پورت مربوطه دلیل بر بسته بودن پورت فوق نیست و ممکن است به یکی از دلایل زیر باشد :**

- **فیلتر شدن پروتکل** Telnet **توسط روترهای شبکه .**

- **بسته شدن پروتکل** Telnet **توسط فایروال داخلی سیستم.**

- Block **شدن پورت مربوطه .**

## درس ۶

## ARP

**در فصلهای قبل راجع به این دستور صحبت کرده ایم لذا در این درس به گفتن سوئیچ های این دستور اکتفا می کنیم.**

**شیوه نگارش دستور**: (Syntax)

Arp[-a [InetAddr] [-NIfaceAddr]] [-g [InetAddr] [-NIfaceAddr]] [-dInetAddr [IfaceAddr]] [-sInetAddr EtherAddr [IfaceAddr]]

**سوئیچ ها و پارامترهای دستور:**

-a:**با این دستور اطلاعات موجودیت های جدول** ARP **، نمایش داده می شود . خروجی این سوییچ شامل آدرس کارت شبکه ، آدرس** ip ، MAC**و نوع اتصال ایجاد شده می باشد. استفاده از این دستور به تنهایی سبب نمایش اطلاعات مربوط به تمامی جداول و موجودیت های درون آنها می شود.**

-d:**حذف یک میزبان توسط آدرس** ip **آن . از طریق وارد کردن آدرس کارت تنها یک دستگاه را می توان حذف کرد . جهت حذف تمامی کارت ها بصورت همزمان از کاراکتر * هم می توان استفاده نمود.**

-g:**این دستور مشابه سوییچ** a– **عمل می نماید.**

-inet_addr:**تعیین یک آدرس** ip **. این مقدار معمولا مربوط به کامپیوتری است که میزبان جدول** ARP**می باشد . نکته قابل توجه این که این دستور از** ip V۶ **پشتیبانی نمی کند.**

-N if_addr:**نمایش فهرست موجودیت های جدول** arp **برای یک کارت شبکه خاص . توجه داشته باشید که** N **را حتما بصورت حروف بزرگ تایپ نمایید.**

**-s:با این سوییچ می توان یک** host **جدید را به جدول** ARP **و اختصاص** IP **آدرس آن به آدرس فیزیکی اضافه نمود . برای این منظور باید آدرس** IP **و آدرس فیزیکی کارت شبکه را وارد نمایید . خروجی این دستور دائمی است و جهت حذف آن جدول** ARP**از پارامتر** d– **نیز می توانید استفاده کنید.**

# درس ۷

## NSLookup

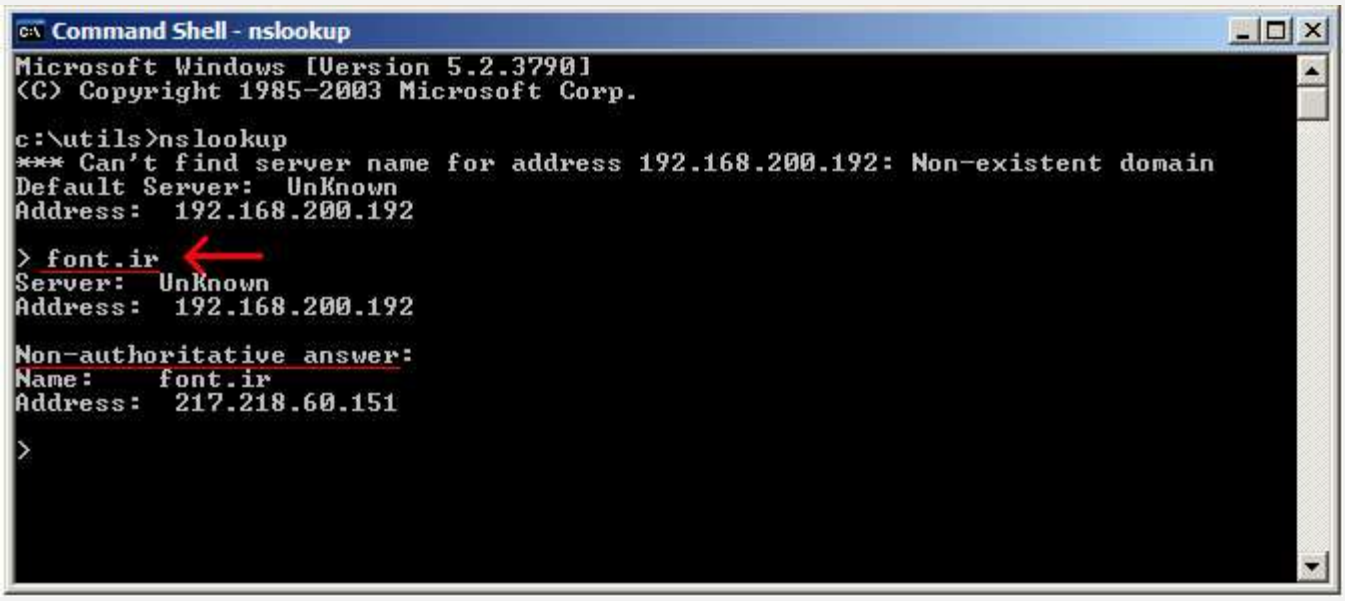
**NSLookupیک برنامه از نوع خط فرمان** (command-line) **است که مخفف** Name Server Lookup **می‌باشد. به وسیله** NSLookup **می‌توان از** Name Server**های مختلف اطلاعات مربوط به دامنه‌های مورد نظر را در صورت امکان بدست آورد. اطلاعاتی که درباره دامنه از طریق** NSLookup**مشاهده می‌کنیم، در واقع همان اطلاعاتی است که در** ZoneFile **مربوط به دامنه وجود دارد.**

**اجرای برنامه** NSLookup

Command Shell**را باز می‌کنیم و دستور** nslookup**را تایپ می‌کنیم.**


**هنگام اجرا،** NSLookup **سروری را که به عنوان** DNS Server**کامپیوتر شما تعریف شده است را به عنوان سرور پیش فرض تعیین می‌کند. این آدرس را می‌توانید 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 می‌باشد.**

**حال آدرس** font.ir **را وارد می‌کنیم.**




**دو خط اول پاسخ مشخص می‌کند که کدام سرور و با چه آدرسی پاسخ را ارائه کرده است.**

**خط سوم عبارت** Non-authoritative **را مشاهده می‌کنیم. 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.**

**درخط چهارم و پنجم نام دامنه و آدرس هاست آن ۲۱۷٫۲۱۸٫۶۰٫۱۵۱ را مشاهده می‌کنیم. 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 سرورمورد نظر یا آدرس** IP**آن را می‌نویسیم.**

**این بار از سرور** ns۴.parsihost.com**درباره دامنه** font.ir **می‌پرسیم.**


**همانطورکه در شکل می‌بینید، به کمک دستور** server ns۴.parsihost.com ، **سرور پیش فرض را به** ns۴.parsihost.com **تغییر می‌دهیم. این بار در جوابی که برای** font.ir **مشاهده می‌کنیم عبارت** Non-authoritative **دیده نمی‌شود. در واقع در اینجا** ns۴.parsihost.com **مرجع پایه اطلاعات دامنه** font.ir **است.**

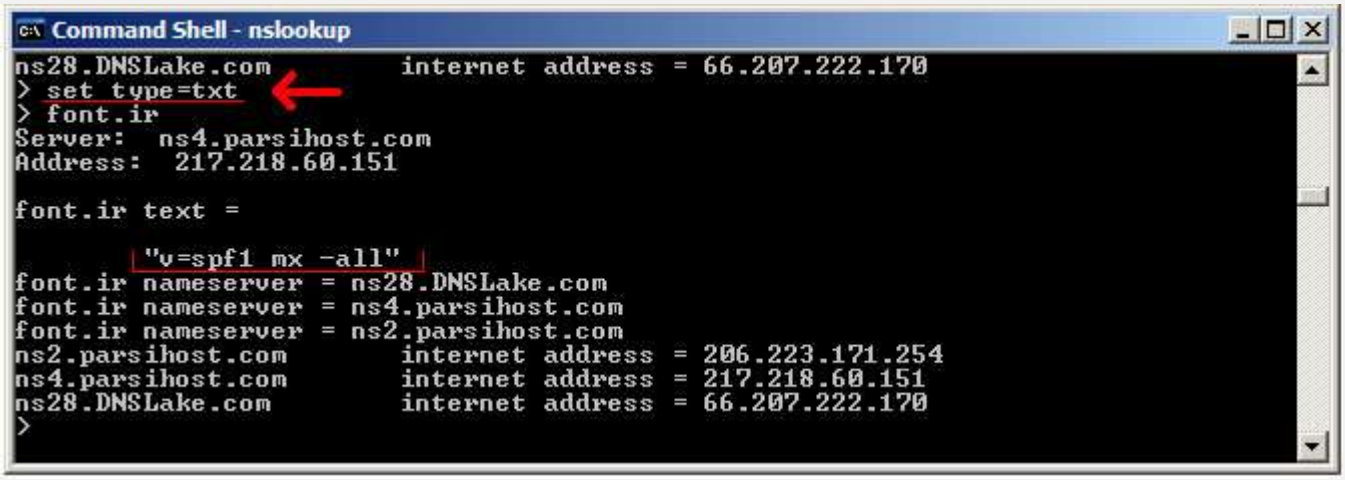
**همانطور که در جدول مربوط به** ZoneFile **دامنه دیدید، در این جدول انواع مختلفی از اطلاعات وجود دارد که می‌توان نوع آنها را در ستون Recordtype مشاهده کرد.**

**برای بدست آوردن سایر اطلاعات دامنه می‌توانیم از دستور** set type**استفاده کنیم. این دستور دارای ساختاری طبق عبارت ذیل می‌باشد.**

Settype=NAME
(where NAME is the type of record to look atfor 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 می‌کنیم و مجدداً درباره دامنه** font.ir **پرس و جو می‌کنیم.**




**همانطور که در شکل می‌بینید، اطلاعات مربوط به رکوردTXT دامنه را نمایش می‌دهد، 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.**

**در واقع** NSLookup **یک ابزار مدیریتی در شبکه برای آزمایش و رفع اشکال** Name Server **ها می باشد. علاوه بر** NSLookup **می‌توان از سایر نرم افزارها مانند** DIG**استفاده کرد.(** Domain Information Groper - **کاوشگر اطلاعات دامنه ).**

# 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 میشناسند. 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 میپردازیم .**

**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 بالا ی 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 مبحث را در فصل ۵ بیان کرد چرا که در درس بعدی به پروتکلهای 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 یك** PSTN **مجهز باشیم .**

**سابقه** PSTN

**در ابتدا هدف از ایجاد** PSTN **ایجاد یك ارتباط بین دو دستگاه تلفن می بود . این مدار از نقطه تماس گیرنده شروع و تا نقطه مقصد ادامه پیدا می کرد . در حقیقت یك سیم از تلفن مبدأ تا دفتر** PSTN **و یك سیم هم از مقصد تا دفتر** PSTN **رد و بدل می شد و در آخر سیم بوسیله یك لامپ وضعیت گوشی نمایان می شد . به عبارتی همه مشترکین بر روی تابلو سوئیچ** PSTN **یك لامپ داشتند . کارمند** PSTN **پس از روشن شدن لامپ خط با مشترك صحبت می کرد و از او مقصد ارتباط را سوال می کرد . پس از مشخص شدن مقصد ، کارمند** PSTN **بوسیله یك کابل ارتباط مورد نیاز را بین دو مشترك 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 یك ارتباط تلفنی شدند و تلفن ها به یك 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 یك 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** V۵+ **برای یك باینری و ولتاژ** V۵- **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 استانداردی 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 بردای 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 یك جریان از بیت ها بصورت سریال را به کامپیوتر می دهد. یك مودم یك 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 V۹۲ 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 بپردازد . همچنین این استاندارد، سرعت متقارن ۴۸ kbps را برای ارسال و دریافت داده فراهم می آورد . از مزایای دیگر استاندارد V۹۲ می توان به خاصیت پشتیبانی از Call Waiting اشاره کرد . شما با استفاده از این خصلت می توانید یك تماس کوتاه در حین اتصال مودمها به یکدیگر را تجربه کنید .**

**VPN**

**VPN[۱] یك شبکه خصوصی مجازی است که ارتباطات کپسوله‌شده(Encapsulated) ، رمزنگاری‌شده (Encrypted)و تصدیق‌شده (Authenticated) رابا استفاده از سیستم مسیریابی زیرساخت شبکه از طریق یك شبکه عمومی مانندااینترنت ایجاد و مدیریت می‌کند. این ارتباط می‌تواند بین دو سیستم عادی برقرار شده و یا برای ارتباط امن سرور یك سازمان با شعب آن در سراسر جهان به‌کار رود. VPN برای کاربران تجاری بیش از یك ضرورت و بلکه نعمتی است که راهی مطمئن، امن و در عین حال ارزان برای دسترسی به فایل‌هایشان در شبکه محل کار خود (وقتی که آن‌ها در مسافرت، خانه و یا در راه هستند) در اختیارمی‌گذارد. کاربران در حالت عادی برای تماس به‌صورت**

[۱] Virtual Private Network

Remote**(راه دور) باسرور نیاز دارند که به‌صورت مستقیم و توسط یك 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 صورتی‌که** RAS **سرور و سیستم تماس‌گیرنده در یك استان قرار نداشته باشند،علاوه بر لزوم پرداخت هزینه زیاد، سرعت ارتباط نیز پایین خواهد آمد و این مسأله وقتی بیشتر نمود پیدا می کند که کاربر نیاز به ارتباطی با سرعت مناسب داشته باشد.**

**۲-در صورتی‌که تعداد اتصالات راه دور در یك لحظه بیش از یك 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 به‌طور کامل حل می‌شود و کاربر با اتصال به** ISP **محلی به اینترنت متصل شده و** VPN **بین کامپیوتر کاربر و سرور سازمان از طریق اینترنت ایجاد می‌گردد . ارتباط مذکور می تواند از طریق خط**DialUp **و یا خط اختصاصی مانند** Leased Line **برقرار شود. به‌هر حال اکنون مسأله این نیست که طریقه استفاده از** VPN **چیست، بلکه مسأله این است که کدامیك از تکنولوژی‌های** VPN **باید مورداستفاده قرار گیرند. پنج نوع پروتکل در** VPN **مورد استفاده قرار می گیرد که هرکدام مزایا و معایبی دارند .**

**ارتباط سیستم‌ها در یك اینترانت**

**دربرخی سازمان‌ها، اطلاعات یك دپارتمان خاص به‌دلیل حساسیت بالا، به‌طورفیزیکی 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 شبکه‌های خارجی به‌وجود می‌آورد.**

VPNاجازه میدهد که شبکه دپارتمان مذکور به‌صورت فیزیکی به شبکه مقصد مورد نظر متصل گردد، اما به‌صورتی‌که توسط VPN سرور، جدا شده است. (با قرار گرفتن VPN سرور بین دو شبکه )

البته لازم به یادآوری است که نیازی نیست VPN سروربه‌صورت یك Router مسیریاب بین دو شبکه عمل نماید، بلکه کاربران شبکه موردنظر علاوه بر این‌که 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 طریقVPN ، می‌توانند به منظور محرمانه ماندن رمزنگاری شوند. برای کاربرانی که دارای اعتبارنامه مجاز نیستند،اطلاعات مقصد به‌صورت خودکار غیر قابل رویت خواهند بود .

**مبانی Tunneling**

Tunnelingیا سیستم ایجاد تونل ارتباطی با نام کپسوله کردن (Encapsulation) نیزشناخته می‌شود که روشی است برای استفاده از زیرساخت یك شبکه عمومی جهت انتقال اطلاعات. این اطلاعات ممکن است از پروتکل‌های دیگری باشد. اطلاعات به‌جای این‌که به‌صورت اصلی و Originalفرستاده شوند، با اضافه کردن یك Header (سرایند) کپسوله می‌شوند .

این سرایند اضافی که به پکت متصل می‌شود، اطلاعات مسیریابی را برای پکت فراهم می کند تا اطلاعات به‌صورت صحیح، سریع و فوری به مقصد برسند. هنگامی که پکت‌های کپسوله شده به مقصد رسیدند، سرایندها از روی پکت برداشته شده و اطلاعات به‌صورت اصلی خود تبدیل می‌شوند. این عملیات را از ابتدا تا اتمام کار Tunneling می‌نامند .

## نگهداری تونل

**مجموعه عملیات متشکل از پروتکل نگهداری تونل و پروتکل تبادل اطلاعات تونل به‌نام پروتکل** Tunneling**شناخته می‌شوند . برای این‌که این تونل برقرار شود، هم کلاینت و هم سرور می‌بایست پروتکل** Tunneling **یکسانی را مورد استفاده قراردهند. از جمله پروتکل‌هایی که برای عملیات** Tunneling**مورد استفاده قرارمی‌گیرند** PPTP **و** L۲TP **هستند که در ادامه مورد بررسی قرار خواهند گرفت.**

## پروتکل نگهداری تونل

**پروتکل نگهداری تونل به‌عنوان مکانیسمی برای مدیریت تونل استفاده می‌شود. برای برخی از تکنولوژی‌های** Tunneling**مانند** PPTP **و** L۲TP **یك تونل مانند یك** Session **می‌باشد، یعنی هر دو نقطه انتهایی تونل علاوه بر این‌که باید با نوع تونل منطبق باشند، می‌بایست از برقرار شدن آن نیز مطلع شوند .**

**هرچند برخلاف یك**Session **، یك تونل دریافت اطلاعات را به‌صورتی قابل اطمینان گارانتی نمی‌کند و اطلاعات ارسالی معمولاً به‌وسیله پروتکلی بر مبنای دیتاگرام مانند** UDP**هنگام استفاده از** L۲TP **یا** TCP **برای مدیریت تونل و یك پروتکل کپسوله کردن مسیریابی عمومی اصلاح شده به‌نام** GRE **برای وقتی که** PPTP **استفاده می گردد، پیکربندی و ارسال می‌شوند.**

## ساخته شدن تونل

**یك تونل باید قبل از این‌که تبادل اطلاعات انجام شود، ساخته شود. عملیات ساخته شدن تونل به‌وسیله یك طرف تونل یعنی کلاینت آغاز می‌شود و طرف دیگرتونل یعنی سرور، تقاضای ارتباط** Tunneling**را دریافت می‌کند. برای ساخت تونل یك عملیات ارتباطی مانند** PPP **انجام می‌شود .**

**سرور تقاضا می‌کند 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 پیغام ساخته شدن تونل توسط کلاینت به سرور ارسال می‌گردد و سپس انتقال اطلاعات از طریق تونل شروع خواهد شد.**

**برای روشن شدن مطلب، مثالی می‌زنیم. اگر محیط عمومی را، که غالبا نیز همین‌گونه است، اینترنت فرض کنیم، کلاینت پیغام ساخته شدن تونل را از آدرس IP کارت شبکه خود به‌عنوان مبدا به آدرس IP مقصد یعنی سرور ارسال می‌کند. حال اگرارتباط اینترنت به‌صورت DialUp از جانب کلاینت ایجاد شده باشد، کلاینت به‌جای آدرس NIC خود، آدرس IP را که ISP به آن اختصاص داده به‌عنوان مبدااستفاده خواهد نمود.**

**نگهداری فعال**

**دربرخی از تکنولوژی‌های Tunneling مانند L۲TP وPPTP ، تونل ساخته شده بایدنگهداری و مراقبت شود . هر دو انتهای تونل باید از وضعیت طرف دیگر تونل باخبر باشند. نگهداری یك تونل معمولا از طریق عملیاتی به‌نام نگهداری فعال (KA) اجرا می‌گردد که طی این پروسه به‌صورت دوره زمانی مداوم از انتهای دیگر تونل آمارگیری می‌شود. این‌کار هنگامی که اطلاعاتی در حال تبادل نیست،انجام می پذیرد.**

**پروتکل تبادل اطلاعات تونل**

**زمانیکه یك تونل برقرار می‌شود، اطلاعات می‌توانند 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، یك سرایند (مخصوص پروتکل تبادل اطلاعات) را بر روی**

**پکت اضافه می‌کند. نتیجه این‌کار این است که اطلاعات از طریق شبکه عمومی قابل ارسال شده و تا تونل سرور مسیریابی می‌شوند.**

**تونل سرور پکت‌ها را دریافت کرده و سرایند اضافه شده را از روی اطلاعات برداشته و سپس اطلاعات را به‌صورت اصلی درمی آورد.**

**انواع تونل**

**تونل‌ها به دو نوع اصلی تقسیم می‌گردند: اختیاری و اجباری .**

**تونل اختیاری**

**تونل اختیاری به‌وسیله کاربر و از سمت کامپیوتر کلاینت طی یك عملیات هوشمند،پیکربندی و ساخته می‌شود. کامپیوتر کاربر نقطه انتهایی تونل بوده وبه‌عنوان تونل کلاینت عمل می‌کند. تونل اختیاری زمانی تشکیل می‌شود که کلاینت برای ساخت تونل به سمت تونل سرور مقصد داوطلب شود.**

**هنگامی‌که کلاینت به‌عنوان تونل کلاینت قصد انجام عملیات دارد، پروتکل** Tunneling **موردنظر باید بر روی سیستم کلاینت نصب گردد. تونل اختیاری می‌تواند در هر یك از حالت‌های 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 این‌که بتواند تونل را پیکربندی کند، ارتباطی رااز طریق** DialUp **برای تبادل اطلاعات برقرار کرده باشد. این معمول‌ترین حالت ممکن است. بهترین مثال از این حالت،**

**کاربران اینترنت هستند. قبل از این‌که یك تونل برای کاربران بر روی اینترنت ساخته شود، آن‌ها باید به** ISP **خودشماره‌گیری کنند و یك ارتباط اینترنتی را تشکیل دهند.**

**تونل اجباری**

**تونل اجباری برای کاربرانی پیکر بندی و ساخته می شود که دانش لازم را نداشته ویا دخالتی در ساخت تونل نخواهند داشت. در تونل اختیاری، کاربر، نقطه نهایی تونل نیست. بلکه یك** Device **دیگر بین سیستم کاربر و تونل سرور، نقطه نهایی تونل است که به‌عنوان تونل کلاینت عمل می‌نماید .**

**اگر پروتکل** Tunneling **بر روی کامپیوترکلاینت نصب و راه اندازی نشده و در عین حال تونل هنوز مورد نیاز و درخواست باشد، این امکان وجود دارد که یك کامپیوتر دیگر ویا یك** Device **شبکه دیگر، تونلی از جانب کامپیوتر کلاینت ایجاد نماید.**

**این وظیفه‌ای است که به یك متمرکزکننده دسترسی** (AC) **به تونل، ارجاع داده شده است. در مرحله تکمیل این وظیفه، متمرکزکننده دسترسی یا همان** AC **باید پروتکل** Tunneling **مناسب را ایجاد کرده و قابلیت برقراری تونل را در هنگام اتصال کامپیوتر کلاینت داشته باشد. هنگامی‌که ارتباط از طریق اینترنت برقرار میشود، کامپیوتر کلاینت یك تونل تأمین شده**[1]NAS **رااز طریق** ISP **احضار می‌کند.**

**به‌عنوان مثال یك سازمان ممکن است قراردادی با یك** ISP **داشته باشد تا بتواند کل کشور را توسط یك متمرکزکننده دسترسی به‌هم پیوند دهد. این** AC **می‌تواند تونل‌هایی را از طریق اینترنت برقرار کند که به یك تونل سرور متصل باشند و از آن طریق به شبکه خصوصی مستقر در سازمان مذکور دسترسی پیدا کنند.**

[1] Network Access Service

**این پیکربندی به‌عنوان تونل اجباری شناخته می‌شود، به‌دلیل این‌که کلاینت مجبور به استفاده ازتونل ساخته شده به‌وسیله AC شده است. یك‌بار که این تونل ساخته شد، تمام ترافیك شبکه از سمت کلاینت و نیز از جانب سرور به‌صورت خودکار از طریق تونل مذکور ارسال خواهد شد .**

**به‌وسیله این تونل اجباری، کامپیوتر کلاینت یك ارتباط PPP می‌سازد و هنگامی‌که کلاینت به NAS، از طریق شماره‌گیری متصل می‌شود، تونل ساخته می‌شود و تمام ترافیك به‌طور خودکار از طریق تونل،مسیریابی و ارسال می‌گردد. تونل اجباری می تواند به‌طور ایستا و یا خودکارو پویا پیکربندی شود.**

**تونل‌های اجباری ایستا**

**پیکربندی تونل‌های Static معمولاً به تجهیزات خاص برای تونل‌های خودکار نیاز دارند .سیستم Tunnelingخودکار به‌گونه‌ای اعمال می‌شود که کلاینت‌ها به AC ازطریق شماره‌گیری (Dialup) متصل می‌شوند. این مسأله احتیاج به خطوط دسترسی محلی اختصاصی و نیز تجهیزات دسترسی شبکه دارد که به این‌ها هزینه‌های جانبی نیز اضافه می‌گردد .**

**برای مثال کاربران احتیاج دارند که با یك شماره تلفن خاص تماس بگیرند، تا به یك AC متصل شوند که تمام ارتباطات رابه‌طور خودکار به یك تونل سرور خاص متصل می‌کند. در طرح‌های Tunnelingناحیه‌ای، متمرکزکننده دسترسی بخشی از User Name را که Realm خوانده می‌شودبازرسی می‌کند تا تصمیم بگیرد در چه موقعیتی از لحاظ ترافیك شبکه، تونل راتشکیل دهد.**

**تونل‌های اجباری پویا**

**دراین سیستم انتخاب مقصد تونل براساس زمانی که کاربر به AC متصل می شود،ساخته می‌شود. کاربران دارای Realm یکسان، ممکن است تونل‌هایی با مقصدهای مختلف تشکیل بدهند. البته**

**این امر به پارامترهای مختلف آن‌ها مانند**UserName ، **شماره تماس، محل فیزیکی و زمان بستگی دارد .**

**تونل‌های**Dynamic ، **دارای قابلیت انعطاف عالی هستند. همچنین تونل‌های پویا اجازه می‌دهند که** AC**به‌عنوان یك سیستم** Multi-NAS **عمل کند، یعنی اینکه همزمان هم ارتباطات** Tunneling **را قبول می کند و هم ارتباطات کلاینت‌های عادی و بدون تونل را. در صورتی که متمرکزکننده دسترسی بخواهد نوع کلاینت تماس‌گیرنده رامبنی بر دارای تونل بودن یا نبودن از قبل تشخیص بدهد، باید از همکاری یك بانك اطلاعاتی سود ببرد.**

**برای این‌کار باید** AC **اطلاعات کاربران رادر بانك اطلاعاتی خود ذخیره کند که بزرگترین عیب این مسأله این است که این بانك اطلاعاتی به خوبی قابل مدیریت نیست.**

**بهترین راه‌حل این موضوع،راه‌اندازی یك سرور** RADIUS **است، سروری که اجازه می‌دهد که تعداد نامحدودی سرور، عمل شناسایی**User **های خود را بر روی یك سرور خاص یعنی همین سرور** RADIUS**انجام دهند، به‌عبارت بهتر این سرور مرکزی برای ذخیره و شناسایی واحراز هویت نمودن کلیه کاربران شبکه خواهد بود.**

**پروتکل‌های VPN**

**عمده‌ترین پروتکل‌هایی که به‌وسیله 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 می‌شود، یك پروتکل لایه سوم یعنی لایه شبکه است. مهمترین استفاده پروتکل** IP-IP **برای ایجاد سیستم** Tunneling **به‌صورت** Multicast **است که در شبکه‌هایی که سیستم مسیریابی** Multicast **راپشتیبانی نمی‌کنند کاربرد دارد. ساختار پکت** IP-IP

**تشکیل شده است از: سرایند** IP **خارجی، سرایند تونل، سرایند** IP **داخلی و اطلاعات**IP. **اطلاعات** IP**می‌تواند شامل هر چیزی در محدوده** IP **مانند** TCP ، UDP، ICMP**و اطلاعات اصلی پکت باشد.**

**مدیریت**VPN

**دربیشتر موارد مدیریت یك** VPN **مانند مدیریت یك** RAS **سرور (به‌طور خلاصه، سروری که ارتباط‌ها و** Connection **های برقرار شده از طریق راه دور را کنترل ومدیریت می‌کند)، می‌باشد. البته امنیت** VPN **باید به دقت توسط ارتباطات اینترنتی مدیریت گردد.**

**مدیریت کاربران**

**VPN**

**بیشتر مدیران شبکه برای مدیریت کاربران خود از یك پایگاه داده مدیریت کننده اکانت‌ها بر روی کامپیوتر** DC **و یا از سرور** RADIUS **استفاده می‌نمایند. اینکار به سرور** VPN **اجازه می‌دهد تا اعتبارنامه احراز هویت کاربران را به یك سیستم احراز هویت مرکزی ارسال کند.**

**مدیریت آدرس‌ها و**Name Server **ها**

**سرور** VPN **باید رشته‌ای از آدرس‌های** IP **فعال را در خود داشته باشد تا بتواندآن‌ها را در طول مرحله پردازش ارتباط از طریق پروتکل کنترل** IP **به‌نام** IPCP **به درگاه‌های** VPN Server **و یا** Client**ها اختصاص دهد.**

**در**VPN **هایی که مبتنی بر ویندوز ۲۰۰۰ پیکربندی می‌شوند، به‌صورت پیش‌فرض،** IP**آدرس‌هایی که به**Client **های** VPN **اختصاص داده می‌شود، از طریق سرور** DHCP **گرفته می‌شوند.**

**البته همان‌طور که قبلاً گفته شد شما می‌توانید یك رشته** IP **را به‌صورت دستی یعنی ایستا به‌جای استفاده از** DHCP **اعمال کنید. ضمناً** VPN Server **باید توسط یك سیستم تأمین‌کننده نام مانند** DNS **و یا** WINS **نیز پشتیبانی شود تا بتواندسیستم** IPCP **را به مورد اجرا بگذارد.**

**چیست؟** ISDN

**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[1] **طراحی شدو تمام شبکه های تلفنی آنالوگ به دیجیتال تبدیل شد.**

ISDN[2] **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 مزیتهای اضافی دیگری‌راهم همراه داشته باشد .**

[1] Intgrate digital network
[2] Intergeated Service Digital Network

**طرح ومفهوم ISDN برای ارتباط دیتا**

**شبکه ISDNاز 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 وباید بعنوان یک شبکه جامع سرویس دهی باند پهن بکاربرده شود . باند پهنی عینازیرساخت 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 بدنبال 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 مرتبطه اختصاص داده می شود . علاوه بر این ، در حین یک ارتباط ISDNموجود ، اطلاعات کنترلی (سیگنالیک) مربوط به ارتباط بین ترمینالهای مرتبطه بطور موازی (همزمان) ارسال می گردند . اطلاعات کنترلیرا بطور کلی سیگنالینگ می‌نامند .**

**هیچ ارتباط انتها به انتهایی بمنظور سیگنالینگ بین ترمینالهای مرتبطه ایجاد نمی گردد ، بلکه سیگنالینگبه 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 درارتباط باید با نرخ بیت یکسانی ارسال و در یافت 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.**

**Dslچیست؟**

**DSL[1]یك فناوری مخابراتی است که اولین بارحدود سال ۱۹۹۵ در امریکا 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 یك 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 مشترك 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 ۸Mbpsاطلاعات دریافت و۱Mbps ارسال کند امااگر این فاصله به ۵ کیلومتر برسد ، سرعت نصف می شود .**
**به طور کلی DSL به چند دسته VDSL , RADSL , HDSL , SDSL , ADSL تقسیم می شود.**
**ADSL[2]به معنای سیستم DSL نامتقارن است که به علت یکسان نبودن سرعت ارسال و دریافت اطلاعات به این نام خوانده می شود .**
**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:**

- **اتصال اینترنت و تماس تلفنی در یک زمان برقرار است.**
- **سرعت از مودم معمولی بسیار بالاتر است (۱/۵ مگا بیت در ثانیه دربرابر ۵۶ کیلو بیت در ثانیه)**
- **با توجه به آنکه از سیم تلفن استفاده میکند نیاز به سیم کشی جدیدندارد.**

[1] Digital Sub Scriber Line
[2] asymmetrical Digitul Subscriber Line

**اما DSL دارای سه نقطه ضعف است :**

- **هرچه به دفتر مرکزی** DSL **نزدیکتر باشید، سرویس بهتر است .**
- **دریافت دیتا سریعتر ازارسال آن است .**
- **سرویس در همه جا عرضه نمیشود .**

**چون سیم تلفن ظرفیت انتقالی بیش از فرکانسهای صدای انسان رادارد و صدای انسان دارای فرکانس بین ۵ تا ۳۴۰۰ هرتز است، بقیه ظرفیت انتقال سیم هاکه تا چند میلیون هرتز میرسد، خالی میماند .**DSL **از این ظرفیت خالی بصورت دیجیتالی برای انتقال دیتا استفاده میکند .**

**DSLنامتقارن یاADSL**

**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. مبنا اینطور است که سرعت دریافت دیتا ازاینترنت 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 .**
- SDSL[۲]**که سرعت ارسال و دریافت یکسانی دارد اما نمیتوانید همزمان از تلفن استفاده کنید و معمولا برای دفاتر اداری کوچک کاربرد دارد .**

[۱] Very high bit-rate DSL
[۲] Symmetric DSL

- RADSL[1]**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 تادفتر 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 دردفتر سرویس دهنده و یا شرکت تلفن نصب میشود. آنکه نزد شماست بنام** Transceiver **است وآنکه شرکت دارد به نا** DSLAM[2] **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 ترانسیورساده هستند اما برای شرکتها میتوانند حاوی روتر شبکه، سویچ شبکه و یا امکانات دیگری برای شبکه باشند .**

**در مورد** DSLAM **که در طرف سرویس دهنده نصب میشود فقط به ذکر این نکته بسنده میکنم که** ASDL **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 ای بین یوزرها به اشتراک گذاشته میشود و با ورود هر یوزر به این حلقه، کیفیت ارتباط افت میکند.**

[1] Rate-adaptive DSL
[2] DSL Access Multiplexer

**قابلیت DSL**

**با استفاده از زوج سیمهای مخابرات برای تلفن خانگی ما تنهااز یک پانصدم امکانات بالقوه این سیمها استفاده می کنیم و مابقی بلااستفاده می‌ماند .ADSL پهنای باند ۱/۱ مگاهرتزی خطوط مسی را به کانال های ۴ کیلوهرتزی تقسیم می کند و آخرین کانال را جهت ارسال صدا و فاکس معمولی تخصیص می دهد و ۲۵۶ کانال دیگر را برای انتقال دو طرفه اطلاعات استفاده می کند; به این ترتیب که ۶۴ کانال رابرای خط ارسال اطلاعات و ۱۲۸ کانال دیگر را جهت دریافت اطلاعات استفاده می کند. دربهترین حالت اگر ۱۹۲ کانال ۴ کیلو هرتزی موجود را استفاده کند، در تئوری سرعت بایدبه حدود ۹ مگابیت در ثانیه برسد.**

**در حال حاضر سرعت خطوط ADSL در بهترین حالت ۲مگابیت در ثانیه می باشد.در عمل، این خطوط اطلاعات زنجیره وار دیجیتال را به اطلاعات پارالل در دو سر انتقال اطلاع تبدیل می کنند. دقیقا 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 ازسخت‌افزارهایی که بتوانند داده‌ها را فشرده‌سازی، ارسال و دریافت نمایند می‌توانیم این قابلیت بلااستفاده را هم به کار بگیریم. یکی از این سخت‌افزارها در پست مخابرات نصب و دیگری در محل استفاده‌کننده نصب می‌شود. ارتباط از طریق سیم تلفن قبلی شمابرقرار می‌شود 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 نمی‌آورد.**

**برتری‌های فنیDSL**

- **-اتصال دائم و بی‌وقفه و مطمئن به شبکه مخابرات و شبکه جهانیاینترنت برقرار است.**
- **–از حداقل تجهیزات در محل کار یا خانه استفاده می‌شود.**

- **–سرعت سیستم به قدری بالا خواهد بود که سرویس‌های 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 ایده‌آل (نبود نویز بر روی سیمها، فاصله کم تا مرکزمخابراتی) حداکثر سرعت دریافت ۸ Mbpsو سرعت ارسال ۱ Mbpsخواهد بود.**
- **–اداره و کنترل کارهای چنین اتصالی نیز به سادگی همان کاری است که با تلفن منزل انجام می‌دهیم.**
- **_به علت سرعت بالا (دریافت و ارسال) امکان برقراری جلسات وسمینارهای مجازی با سهولت میسر است.**
- **بازشدن راه برای انجام پروژه‌هایی مانند دولت الکترونیک، پزشکی الکترونیک، آموزش سمعی بصری الکترونیک، شبکه اختصاصی الکترونیک و مجموعه وسیعی ازدیگر 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.

**DSLچگونه کار میکند ؟**

**به محیطی که داده ها ازآن انتقال می یابند مدیا یا رسانه گفته می شود. زوج سیم، کابلهای کواکسیال (مثل کابل آنتن تلویزیون)، موج بر ها (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 آنهاحداکثر 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 باندفرکانسی 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 تقریبا ۵۰۰ برابر خواهد شد، واضح است که سرعت انتقال دادهایمان به شدت افزایش خواهدیافت. برای** ADSL **در عمل معمولا باند فرکانسی ۳۰** KHz **تا ۱۳۸** KHz **برای فرستادن اطلاعات و باند فرکانسی ۱۳۸** KHz **تا ۱/۱** Mhz **برای گرفتن اطلاعات استفاده می شود. در این صورت با توجه به روشهای مدولاسیون مورد استفاده می توان به پهنای باند دیجیتالی 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 کوچك به یك خط** DSL **نامتقارن** (ADSL) **متصل میشوند** .ADSL **فرکانسهای موجود در یك خط را براساس این فرض که اغلب کاربران اینترنت اطلاعات بسیار بیشتری را نسبت به آنچه که ارسال میکنند از اینترنت دریافت مینمایند, تقسیم میکند. دو استاندارد تقریبا ناسازگار در موردتکنولوژی** 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 واستاندارد 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 کیلو هرتز پهنای باند کافی است لذا کانال آخر را برای انتقال فاکس و تلفن (صوت) استفاده مینمایند و ۲۵۶ کانال دیگر را بصورت ۶۴ کانالبرای ارسال اطلاعات و ۱۲۸ کانال برای دریافت اطلاعات ( و مابقی ۶۴ کانال برایاطلاعات کنترلی) تقسیم بندی مینمایند, بطوریکه در بهترین وضعیت ( با در نظر گرفتن ۱۹۲ کانال** (khz۴ **به سرعتی معادل**) mbps۹ **مگابیت بر ثانیه) میرسیم که البته حداکثرسرعت مورد استفاده در** ADSL **ها معادل** mbps۳/۲ **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 معمولا 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** xDSL**فرستاده میشود. به منظور جدا کردن صوت و** data **در طرف مشترك 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 یك خط ارتباطی واحد با ظرفیت بالا به اینترنت منتقل میکند .**

DSLAM **قادر به پشتیبانی چندین نوع** DSL **در یك مرکزتلفن واحد و تعداد گوناگونی از پروتکلها و روشهای مدولاسیون میباشد بعلاوه** DSLAM **میتواند امکاناتی همچون مسیریابی یا تخصیص آدرس دینامیکی** IP **نیز برای مشرکین فراهم کند. در واقع** DSLAM **را میتوان دلیل اصلی تفاوت بین سرویس دهی از طریق** ADSL **و ازطریق 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 **یك سرویس حساس به فاصله میباشد همچنانکه طول ارتباط افزایش می یابد کیفیت سیگنال کاهش یافته وسرعت ارتباط کم میشود. حداکثر فاصله جهت سرویس دهی توسط سیستم** ADSL **میتواند به ۵۴۶۰ متر برسد. تکنولوژی** ADSL **میتواند حداکثر سرعت ۸** Mbps downstream**درفاصله حدود ۱۸۲۰ متر و سرعت** upstream **تا ۶۴۰**kbps **را در اختیار کاربران قراردهد. که البته در عمل حداکثر سرعت مورد استفاده در** ADSL **ها ۲/۳** mbps**میباشد. اما چرا فاصله یك محدودیت برای سیستم** DSL **به شمار میرود در حالیکه این محدودیت برای مکالمات تلفنی وجود ندارد؟ جواب این سوال در تقویت کننده های کوچکی به نام** Loading coils**میباشدکه شرکت تلفن برای تقویت سیگنالهای صوتی استفاده میکند. که این تقویت کننده ها باسیگنالهای** ADSL **سازگاری ندارند. البته پارامترهای دیگری همچون** Bridge Taps**وکابلهای فیبرنوری نیز میتوانند تاثیر منفی روی تکنولوژی** ADSL **بگذارند .**

**مقایسه انواع DSLها:**

- ADSL (Asymmetric DSL):

**این روش نامتقارن نامیده شده و دلیل آن هم تفاوت سرعت دریافت و ارسال است. بیشتر مناسب خانه‌ها 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 امگابیت بر ثانیه را دارد و همچینین 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 دوبل 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 روش‌های DSL دارای پایین ترین سرعت است. سرعت این خطوط ۱۴۴ کیلوبیت در 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 می‌گردد.**

- (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 شرکت‌های اروپایی پیشنهاد شد.**

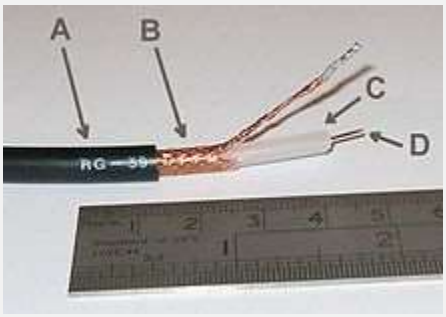
- (Very high bit-rate) VDSL:

**این روش نامتقارن است و در مسافت های کوتاه بهمراه خطوط مسی تلفن استفاده می‌گردد.**

- (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 می‌شود. پایانه۵۹ -RG از یک کتاب نظامی باستانی به نام رهنمای رادیو می‌آید، که این عدد شماره صفحهٔ کتاب راهنما است که در این مورد توضیحاتی داده‌است. (RG مخفف کلمه Radio Guide است به معنی راهنمای رادیو)**

**تلویزیون کابلی یک نوع سامانه تلویزیونی است که در آن مشترکین سیگنال‌های رادیویی را از طریق فیبر نوری و کابل کواکسیال دریافت می‌کنند، که جزو مالکیت مشترک به حساب می‌آید که شباهت زیادی به روش هوایی دارد. در روش قدیمی تصاویر از طریق امواج رادیویی انتقال می‌یابند که در آن تلویزیون نیاز به یک آنتن دارد. و به روش‌هایی از جمله برنامه‌های رادیویی اف ام، اینترنت پرسرعت و تلفنی شباهت زیادی دارد که گاهی اوقات این روش‌ها نیز ارائه می‌شوند و تفاوت اصلی بین رادیوی فرکانسی و ارتباط نوری در مالکیت آن‌ها است.**

**در زبان انگلیسی به اختصار از CATV نام می‌برند که به معنی تلویزیون کابلی به کار می‌رود ولی در اصل به معنی تلویزون آنتی مشترک می‌باشد که از نام شبکه کابلی گرفته شده‌است که در سال ۱۹۴۸ بنیان گذاری شده‌است که در روش هوایی گیرندگی به فاصله فرستنده تا گیرنده محدود بود و حتی به پستی و بلندی نیز محدود می‌شد که مجبور بودند از شبکه کابلی برای انتقال امواج به منازل افراد استفده کنند. در اصل قدمت تلویزیون کابلی از قدمت رادیو نیز بیشتر است که گفته**

**می‌شود در برخی از شهرهای اروپایی که قدمت آن به سال‌های قبل از ۱۹۲۴ می‌رسند استفاده می‌کردند.**

**این روش پیش پا افتاده در آمریکای شمالی، اروپا، استرالیا و شرق آسیا استفاده می‌شده اگر چه در حاضر در خیلی از کشورها استفاده می‌شود که بیشتر در آمریکای جنوبی و خاورمیانه استفاده می‌شود. تلویزیون کابلی موفقیت‌های کوچکی نیز در آفریقا داشته‌است. هر چند در مناطق عامه پسند تأثیر چندانی ندارد و در عوض از سامانه‌هایی بر مبنای شبکه‌های بی سیم و امواج ماکروویو استفاده می‌شود.**

## 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** TCP/IP **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 دارنند، مانند یک خط تلفن. به همین دلیل،** SLIP**و**PPP**پروتکلهای** end-to-end **نامیده می شوند. و از انجا 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.**

SLIP[1] **و** PPP[2] **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 **بمراتب کمتر است .**

**PPP نسبت به SLIP دارای مزایای متعددی است :**

- **امکان مبادله اطلاعات به صورت همزمان و غیر همزمان . در پروتکل** SLIP **صرفا امکان مبادله اطلاعات به صورت همزمان وجود دارد .**

[1] Serial Line Internet Protocol
[2] Point-To-Point

- **ارائه امکانات لازم به منظور تصحیح خطاء . تصحیح خطاء در پروتکل** SLIP **عموما 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 **صرفا امکان استفاده از پروتکل** IP **وجود خواهد داشت .**

**وجه اشتراک پروتکل های PPP و SLIP**

- **هر دو پروتکل قابل روتنیگ نمی باشند . با توجه به نوع ارتباط ایجاد شده که به صورت نقطه به نقطه است و صرفا 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 معمولا 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[1] 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 بایتی 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 بایتی مورد نیاز** ATM **تبدیل می کند.** ATM AdaptationLAYER **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 ارایه می کند. این قالب بسیار انعطاف پذیر و قوی بوده و قابلیت ارایه سرویس های متنوعی از لحاظ کیفیت سرویس را دارا می باشد.**

**این قالب مبتنی بر ارسال اطلاعات بصورت سلول‌های بسیار کوچک اطلاعاتی ( بسته‌های کوچک با ابعاد ثابت ) بر روی مسیرهای داده‌ای از قبل ایجاد شده** ( Connection Oriented ) **می‌باشد. ابعاد کوچک و ثابت سلول‌ها بافر کردن جداگانه سلول بدون پردازش آن‌ها را امکان‌پذیر می‌سازد. همچنین با توجه به این که مسیرها قبل از ارسال ایجاد می‌شوند، نیازی به اعمال الگوریتم‌های پیچیده مسیریابی برای تک تک بسته‌های اطلاعاتی وجود ندارد و مسیریاب‌های شبکه در حین ارسال اطلاعات ( پس از ایجاد مسیر ) عملا تبدیل به سوئیچ‌های ساده** Store & Forward **می‌شوند که نیازمند حداقل قدرت پردازشی هستند.**

ATM **دارای مشخصه‌های فنی‌ای است که باید در تمام شبکه‌های مبتنی بر** ATM **رعایت شده و تضمین شوند:**

[1] Asynchronous Transfer Mode

**•مبتنی بر سئویچینگ بسته‌ها است.**

**•بسته‌های اطلاعات با طول ثابت ۵۳ بایت، شامل ۴۸ بایت داده و ۵ بایت سرآیند که بخاطر ثابت بودن طولشان سلول نامیده می‌شوند.**

**•سرعت مخابره بالا و تاخیر بسیار کم در رئوس میانی شبکه.**

**•سلول‌ها به همان ترتیب ارسال به مقصد می‌رسند.**

**•امکان استفاده از سرعت‌های مختلف، حتی اتصال با سرعت متغییر در شبکه.**

**•انتقال ناهمگام مبتنی بر ایجاد مسیر.**( Connection Oriented )

**•استفاده از کانال‌های مجازی برای ارتباط.**

**•حذف قابلیت بررسی و تصحیح خطا و انتقال این وظایف به لایه‌های بالاتر.**

**•تقسیم ترافیک بر اساس مشخصه‌های مختلف کیفیت سرویس.**

**لایه های مدل** ATM:

**همانطور که گفته شد مدل** ATM **یک قالب را تعریف می‌کند که در داخل این قالب می‌توان از پروتکل‌های مختلفی در لایه‌های مختلف استفاده کرد. بنابراین** ATM **یک مدل لایه‌ای نیز ارایه می‌کند که با اندکی تغییرات در نام و وظیفه‌مندی لایه‌ها هم پایه با مدل** OSI **است .**

**سه لایه پایینی مدل را قالب** ATM **همانطور که توضیح داده خواهد شد، توصیف می‌کند و لایه‌ها بالاتر را پروتکل‌های مختلف سطوح کاربردی تشکیل می‌دهند.**

**لایه فزیکی:**

**لایه فیزیکی ATM می‌تواند از پروتکل‌های متنوع مخابره اطلاعات استفاده کرده و محدوده وسیعی از سرعت‌های مخابره از چند کیلوبیت بر ثانیه تا چند گیگابیت بر ثانیه را تامین کند. وظیفه تصحیح اولیه خطا در سرآیند سلول‌ها نیز بر عهده این لایه است.**

**لایه ATM:**

**لایه ATM با توصیف داده در قالب سلول‌های ۵۳ بایتی با طول ثابت در کنار تحویل گرفتن سلول‌ها از لایه تطبیق و ارسال آنها از طریق لایه فیزیکی، وظیفه‌مندی‌های مختلفی را بشرح زیر عهده‌دار است:**

- **آدرس یابی سلول های.**
- **سوئیچینگ و ارجاع سلول‌ها بر اساس آدرس‌یابی انجام شده.**
- **تضمین ترتیب صحیح رسیدن سلول‌ها به مقصد.**
- **کنترل ترافیک و مقابله با گرفتگی در شبکه.**

**در نقاط داخلی شبکه دارای وظیفه اصلی سوئیچینگ و در نقاط اتصال شبکه به کاربران وظیفه انتقال داده‌های بین دو لایه تطبیق را در مبدا و مقصد بر عهده دارد.**

**لایه تطبیق:**

**این لایه وظیفه ارایه سرویس‌های مختلف ارتباطی با مشخصه‌های بسیار متنوع و تضمین کیفیت سرویس‌ها را بر عهده دارد .چگونگی تقسیم داده به سلول‌ها و نحوه برخورد با سلول‌های گم‌شده و خطادار در شبکه وابسته به پارامترهای سرویس می‌باشد. برای مثال در سرویس‌های چندرسانه‌ای همزمان نیازی به تکرار داده‌های مخدوش نیست، زیرا تاخیر مجاز بسیار کم می‌باشد.**

**ارتباط شبکه های اینترنت و ATM**

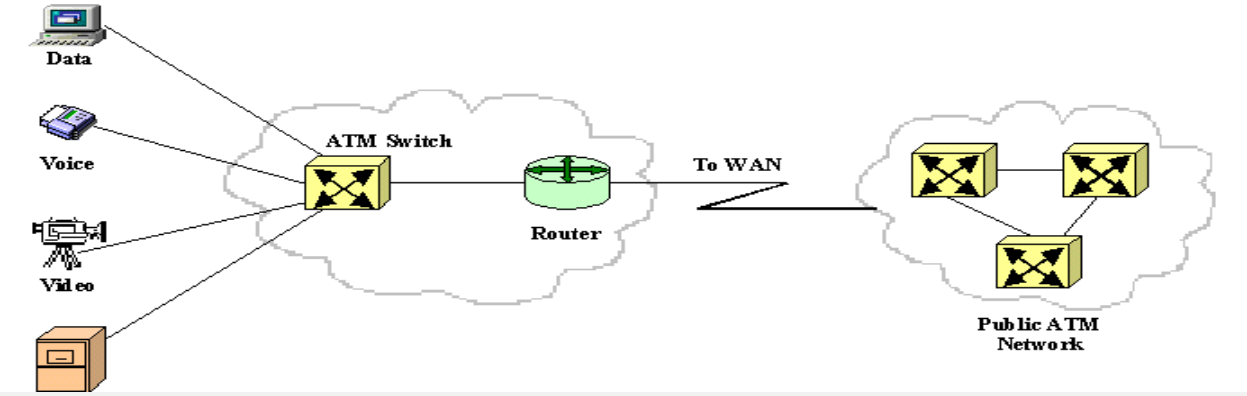
**در حالی که اینترنت از وقایع اخیر دنیای ارتباطات بوده و با گسترش روز افزون خود جهان را در می نوردد ، فراهم کنندگان خدمات همچنان اذعان دارند که در حال حاضر تکمیل ترین شبکه ای که می تواند برای مدیریت پهنای باند قابل انعطاف و پشتیبانی دسته های خدماتی مختلف ، با نیازمندی های کیفیت سرویس متفاوت به کار رود تکنولوژی شبکه ATM است . از سوی دیگر به خاطر محبوبیت و فراگیر شدن اینترنت ، موفقیت ATM نیز به عنوان یک تکنولوژی شبکه داده به مقدار زیادی به پشتیبانی پروتکل IP و توانایی عبور ترافیک IP بستگی دارد . این الزام دو سویه باعث گردیده است که ارتباطات دوربرد تغییری آزمایشی را تجربه نماید . تغییری که باعث می شود ATM براحتی در هسته شبکه قرار گیرد و از پروتکلIP در دستیابی به شبکه استفاده گردد .**

**اینترنت بی سیم:**

**راهکاری است منطبق بر استانداردهای Wireless ATM که می تواند بعنوان جایگزین خطوط پرسرعت مبتنی بر کابل در برقراری ارتباطات پرسرعت استفاده شود. این راهکار ارتباطی به شما اجازه می دهد تا با انعطاف پذیری بسیار زیاد حتی بدون نیاز به داشتن دید مستقیم، گره های شبکه را در کمترین زمان ممکن بصورت بیسیم به یکدیگر متصل نمایید.**

**ATMها چگونه کار می‌کنند؟**

**ATM نمونه یک ترمینال داده با دو قسمت ورودی و چهار قسمت خروجی می‌باشد. مانند دیگر ترمینال‌های داده ،ATM با استفاده رابط‌های ارتباطی به پردازشگر میزبان host processor متصل می‌شود. پردازشگر میزبان مانند یک ارائه کننده خدمات اینترنت ISP می‌باشد که از طریق درگاه‌های مختلف به تمامی شبکه‌های مختلف ATM متصل می‌باشد.**




## FDDI[1] 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**FDDI **می توان ۵۰۰ گره را در مسافت ۱۰۰ کیلومتربه یکدیگر متصل کرد. 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 اید 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.**

[1] Fiber Distributed Data Interface

## 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** Frame **از یک یا چند مقصد به یک یا چند نقطه پایانی می باشد. معمولا 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** VPN،MPLS **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. بنابرین برای مثال امکان دارد یک زنجیره جزئی از** Frame relay **برای اتصال مناطق روستایی به** WAN **استفاده شود.**

## SMDS[1] چیست؟

**که یک سرویس بدون اتصال برای تبادل اطلاعات در شبکه های** LAN **و** WAN **و** MAN **می باشد. اساس** SMDS **استاندارد** DQDB IEEE ۸۰۲/۶ **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.**

[1] Switched multimegabit data service

| نام تکنولوژی WAN | سرعت | گستره جغرافیایی | مزیت |
|---|---|---|---|
| FDDI | ۱۰۰Mbps | **در محلهایی که تعداد زیادی کامپیوتر در آن قرار دارد استفاده می شود مثل دانشگاهها** | **برای ارتباط از فیبر نوری و یا کابل مسی (کم شدن فاصله مجاز)استفاده می کند توپولوژی فیزیکی این شبکه حلقوی است** |
| ATM | ۱۰Mbps **تا** ۶۴Kbps | **در سطح شرح** | **تکنولوژی قابل اطمینان مثل ارتباطات ماهواره ای ودر سطح شهر قابل اطمینان در فرکانس بالا امنیت تضمین شده ظرفیت بالا پهنای باند کاملا اختصاصی کاهش هزینه راه اندازی** |
| Frame relay | **سریعتر از** ۶۴Kbps | **اتصال مناطق روستایی به شبکه** WAN | **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.** |

# 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 ازآنها 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 رود 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 براحتی 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 ابزرای 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 ، قطعا 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. ضمنا 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 بپردازند. 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 بتواندابن 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 پروتکلهای لایه شبکه مانند** IP **و در بعضی موارد با توجه به اطلاعات موجود در پروتکلهای 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 پروتکلهای لایه کاربرد ندارند.**

**۴- فیلترهای** Stateful Packet **: این فیلترها بسیار باهوشتر از فیلترهای ساده هستند. آنها تقریبا تمامی ترافیک ورودی را بلوکه می کنند اما می توانند به ماشینهای پشتشان اجازه بدهند تا به پاسخگویی بپردازند. 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 پروتکلهای لایه کاربرد مانند** FTP **و** HTTP **را تشخیص دهند و لذا می توانندا عمال 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. معمولا 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 بپردازند. 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 وتنظیم 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.**

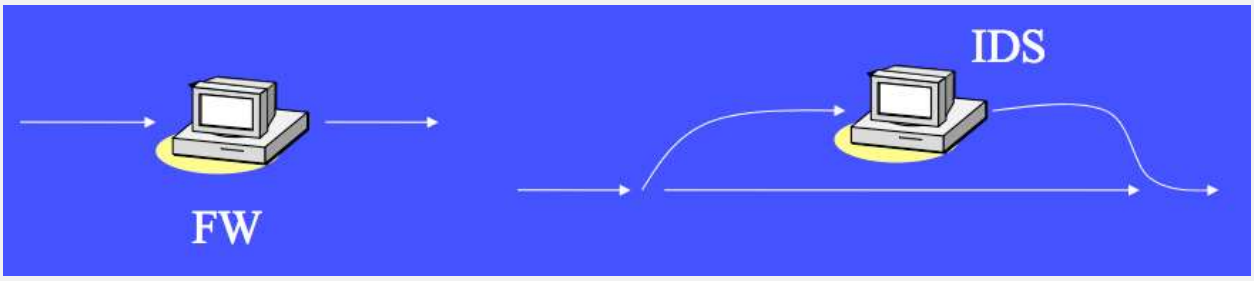
- **مسیریابی نامتقارن : بیشتر فایروالهای مدرن سعی می کنند اطلاعات مربوط به اتصالات مختلفی را که از طریق آنها شبکه داخلی را به شبکه عمومی وصل کرده است، نگهداری کنند. این اطلاعات کمک می کنند تا تنها بسته های اطلاعاتی مجاز به شبکه خصوصی وارد شوند. در نتیجه حائز اهمیت است که نقطه ورود و خروج تمامی اطلاعات 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.معمولا 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

## Idsچیست ؟

IDS یك 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 پورتها ، به دست آوری کنترل کامپیوترها و نهایتا هك کردن می باشد ، می تواند نفوذ خرابکاریها را گزارش و کنترل کند.

از قابلیتهای دیگر IDS ، امکان تشخیص ترافیك غیرمتعارف از بیرون به داخل شبکه و اعلام آن به مدیر شبکه و یا بستن ارتباطهای مشکوك 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 طورکلی نرم افزارهای خطرناك تهیه شده اند.**

**۴-دیواره آتش (**Firewall **)**

**۵-مکانیزم های امنیتی مانند** SSL**و** Radius **و . . . .**

**چرادیواره آتش به تنهایی کافی نیست؟**

**به دلایل زیر دیواره های آتش نمی توانند امنیت شبکه را به طور کامل تامین کنند :**

**۱. چون تمام دسترسی ها به اینترنت فقط از طریق دیواره آتش نیست.**

**۲. تمام تهدیدات خارج از دیواره 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 (Network Based)**

**گوش دادن به شبکه و جمع آوری اطلاعات ازطریق کارت شبکه ای که در آن شبکه وجود دارد.**

**به تمامی ترافیك های موجود گوش داده و در تمام مدت در شبکه مقصد فعال باشد.**

**HIDS (Host Based)**

**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 عملا طوری تنظیم شده است که در معرض حمله قرار بگیرد. اگر یك پویشگری از** NIDS، HIDS **و دیواره آتش با موفقیت رد شود متوجه نخواهد شد که گرفتار یك** Honey pot **شده است. و خرابکاری های خود را روی آن سیستم انجام می دهد و می توان از روشهای این خرابکاریی 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 یك 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 معمولا از طریق اینترنت انجام می گیرد.**

**برای تشخیص خطرات وحملات 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 کمك 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:دراکثر موارد حمله به معنی تلاش برای استفاده از نقص یا ایجاد آن در سیستم امنیتی یك 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 وحمله کنندگان قرارمی گیرد مانند نرم افزارهای کنترل صحت و یکپارچگی فایل یا نرم افزارهایی که جهت تست آسیب پذیری شبکه مورد استفاده قرارمی گیرند.چك کردن یکپارچگی فایلها با استفاده از روش های سیستمی و با قابلیت ادغام روشهای مختلف با یکدیگر و با ابزارهایی نظیر** anti-SATANیا Courtney **امکان پذیر می باشد.**

**●ترافیك خروجی غیر معمول:یك نفوذگر با استفاده از تعداد زیادی** Exploit **و حتی نفوذ های ناموفق سعی در به دست آوردن کنترل کامپیوتر مقصد دارد. این عملیات نفوذگرانه، ترافیك معمول شبکه را افزایش می دهد و نشانه وقوع یك حمله درآینده می باشد. هر ابزار تست آسیب پذیری می بایست قابلیت تشخیص فعالیت های مشکوك و غیر متعارف را داشته باشد و با ارائه گزارش ، اعلام خطر لازم را به مدیر شبکه بدهد.**

**حد تکرار برای کمك به تشخیص فعالیتهای واقعی و مشکوك :فعالیتهای 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. مثلا وقتی بخواهید با نام کاربری اشتباه وارد سیستم شوید، سه تلاش برای ورود با نام غلط بین فاصله زمانی ۲ دقیقه یك فعالیت مشکوك به نظر می رسد.**

**اشتباه در تایپ ویا جوابهایی که در یك** Session **ایجاد می شود.**

**پروتکل ها وسرویس 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 یك دستور) ممکن است اطلاعاتی برای شناسایی سرویسهای که می توانند مورد حمله یك نفوذگر قراربگیرند 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 **باشد.** (Spoofing **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 یك 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 یك** Session **نشانه ای از یك حمله پنهانی است. بررسی آدرس مبداء و مقصد ( به صورت ورودی یا خروجی) میتواند جهت** Packet **را تشخیص بدهد. روند برقراری یك** session **با تشخیص اولین پیام ارسال شده شناسایی می شود. یك درخواست برای دریافت یك سرویس از شبکه محلی به صورت یك** session **ورودی است و پروسه فعال کردن یك سرویس بر پایه** Web**از یك شبکه محلی یك** 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 یك حمله IP Spoofing از خارج باشد. این مشکلات می توانند درRouterهایی که قابلیت مقایسه آدرس مبداء 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 یك شبکه محلی ایجاد می شوند و به یك شبکه خارجی فرستاده می شوند.**

**Packet ها با پورت های مبداء و مقصد غیر مشخص. اگر منبع پورت در مورد یك درخواست ورود یا خروج اطلاعات با نوع سرویس یکسان نباشد ممکن است به عنوان یك تلاش برای نفوذ یا پویش سیستم تلقی شود. بطور مثال در خواست Telnet از روی پورت ۱۰۰ در محیطی که انتظار چنین پشتیبانی برای سرویس وجود ندارد.ترافیك غیر معمول بیشتر توسط فایروال شناسایی شده و Packetهای مشکوك را ازبین 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 شنبه صبح یکسری اطلاعات به بخش مرکزی شرکت ارسال می شود که مربوط به اطلاعات مالی است. چنین ترافیکی در شنبه 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 یك 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 مثلا یك حمله** Brute Force **برای شکستن حرف رمز باعث در گیر کردن** CPU **میشود در حالیکه یك حمله** DoS **همین کاررا با سرویس های سیستم انجام میدهد. استفاده سنگین از منابع سیستم ( پروسسور، حافظه، دیسك 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 یك** Packet **نشانه مربوط به** ACK **فعال باشد و قبل از آن هیچ** SYN-Packet **ارسال نشده باشد، ممکن است نتیجه یك حمله در سیستم باشدهمچنین این حالت ممکن است اثر یك** Packet**خراب هم باشد که در یك 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 ترافیك خاص از یك کاربر مشخص داشته باشیم مثلا کاربری که در یك ماموریت اداری بسر می برد معمولا فقط نامه های خود را چك می کند ویا 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:**

**یك 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 افزارسیستم مثل خاموش 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 -بروزاشکالات 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 یك برنامه ایجاد شده باشد.بخصوص برنامه هایی که برای مانیتور کردن سیستم طراحی شده اند مثل** Syslog.

**۴ -بروز اشکالات نامشخص در کارایی سیستم مثلا در** Router **ها یا سرویس های سیستم مثل کند شدن سرور.**

**۵ -بروز رفتارهای مشکوك در اجرای برنامه های کاربرمثل اشکال در دسترسی به بعضی منابع شبکه ۶ -عملکرد مشکوك در فایلهای ثبت وقایع** (Log )**بررسی این فایل ها از نظر سایز 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 یك سیستم کشف نفوذگر،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 یك سیستم ترکیبی دام گذاری و تله اندازی دارد که هردو 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 یك** IDS **جهت شناسایی حملات و یا نفوذهای احتمالی می باشد.**

**وقتی که یك 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 یك قسمت بخصوص برای پایان بخشیدن به** Session **های مشکوك یا تهیه نسخه پشتیبان از سیستم برا ی حفاظت از اطلاعات ، و یا انتقال ارتباط به یك سیستم گمراه کننده مانند** Honeypot **و چیزهای دیگر که بر اساس سیاستهای** ( Policy) **شبکه قابل اجرا باشد . در حقیقت** IDS **یك 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 یك کامپیوتر بخصوص ویا یك منبع شبکه جلوگیری کرد.**

**شناسایی نفوذ ممکن است گاهی اوقات زنگ خطر اشتباهی را به صدا در آورد. برای مثال نتیجه خراب کارکردن یك کارت شبکه و یا ارسال شرح یك حمله و یا اثر یك نفوذ ازطریق** Email.

**ساختار و معماری سیستم تشخیص نفوذ:**

**سیستم تشخیص نفوذ یك هسته مرکزی دارد و یك تشخیص دهنده.موتور تشخیص است که مسئولیت تشخیص نفوذ را دارد. این سنسور یك مکانیزم تصمیم گیری بر اساس نوع نفوذ دارد.**

**این سنسور اطلاعات خام را از سه منبع دریافت می کند.**

**۱-از اطلاعات موجود در بانك اطلاعلتی خود**IDS **.**

**۲-فایل ثبت وقایع سیستم**(syslog) **.**

**۳-آثار ترافیك 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 یك** 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 یك برنامه اجرایی ، تولید کننده** Policy**هایی هستند که ممکن است یك واقعه ایجاد شده در سیستم عامل یا** Packet **های شبکه را ثبت کنند. این مجموعه به همراه اطلاعات** Policy **می تواند در یك 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 مستقیما به یك 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** Policy**های 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 بانك اطلاعاتی که پارامترهای پیکربندی** IDS **را در خود نگه می دارد، روشهای مختلف ارتباطی را ایجاد می کنند.سنسور یا گیرنده هم بانك اطلاعاتی خاص خود را دارد، که شامل تاریخچه پویایی از نفوذهای پیچیده بوده یا با توجه به تعدد حمله مورد تحلیل قرارگرفته است.سیستم تشخیص نفوذ می تواند به صورت متمرکز مثل برقراری یك فایروال فیزیکی یا به صورت غیر متمرکز انجام شود.یك** IDS **غیر متمرکز شامل تعداد زیادی سیستم تشخیص نفوذ در یك شبکه بزرگ است که هرکدام 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 ، مونیتور و فیلتر کردن تمام فعالیتهای مرتبط با یك بخش محافظت شده است که بتواند یك 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 درچند منطقه فیزیکی است.علاوه بر این عامل جایگزین مشخص برای تشخیص و شناسایی اثر حمله های شناخته شده می باشد.یك راه حل ساختاری چند برنامه ای که در سال ۱۹۹۴ ایجاد شد.**

AAFID**یا** Autonomous Agent for Intrusion Detection **است. این ساختار از یك جایگزین استفاده می کند که بخش به خصوصی از رفتار سیستم را در زمان خاص دیده بانی می کند. به طور مثال یك جایگزین 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. یك جایگزین همچنین قابلیت ایجاد زنگ خطر در زمان وقوع یك حادثه مشکوك را دارد.جایگزین ها می توانند مشابه سازی شوند و به سیستم دیگر منتقل گردند.به غیر از جایگزین ها ، سیستم می تواند رابط هایی برای دیده بانی کل فعالیتهای یك کامپیوتر بخصوص داشته باشد.این رابط ها همیشه نتایج عملیات خود را به یك مونیتور 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 در یافت نماید .**

**درس ۳**

**Security Protocols**

**پروتکل IPsec**

**پروتکل** IPsec **یك مجموعه پروتکل است که امنیت ارتباطات پروتکل اینترنت (**IP**) را توسط عملیات احراز هویت و رمزنگاری برای هر بسته** IP **در یك نشست ارتباطی تامین می‌کند.**

IPsec **همچنین شامل پروتکل‌هایی می‌شود که برای برقراری یك ارتباط دوطرفه بین عامل‌ها در ابتدای نشست و مذاکره در مورد کلیدهای رمزنگاری برای استفاده در مدت زمان نشست، استفاده می‌شوند.**

**پروتکل** IPsec **اساسا راهی است که امنیت داده هایی را که در یك شبکه بین کامپیوترها منتقل می‌شوند، تضمین می‌کند.** IPsec **تنها یکی از قابلیت‌های 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 می‌کند.** IPsec **می‌تواند از جریان‌های داده مابین میزبان‌ها (میزبان به میزبان)، مابین گذرگاه‌های امنیتی (شبکه به شبکه) یا مابین یك گذرگاه امنیتی به یك میزبان، پشتیبانی کند.**

**تعدادی از سیستم‌های 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 می‌کنند. درصورتیکه** IPsec **هر نوع ترافیك در سراسر شبکه های مبتنی بر** IP **را پشتیبانی می‌کند. اگر ترافیکی غیر از** IP **در شبکه وجود داشته باشد، باید از پروتکل دیگری مانند** GRE **در کنار** IPSec **استفاده کرد.**

**پروتکل IPSec توسط سرویس‌های زیر، امنیت داده های ارسال شده بین دو آدرس IP در شبکه را تامین می‌کند:**

- **احراز هویت داده**

1. **شناسایی مبداء داده: شما می‌توانید از IPsec استفاده کنید تا تضمین کند که هر بسته ای که از یك طرف قابل اعتماد دریافت کردید، در واقع توسط همان مبداء ارسال شده است و جعلی و دستکاری شده نیست.**
2. **تمامیت داده: شما می توانید از IPsec استفاده کنید تا تضمین کند که داده ها در زمان انتقال تغییر نمی‌کنند.**
3. **حفاظت ضد بازپخش: شما می توانید 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 یك بسته اطلاعاتی IPSec بسته بندی می‌کند و برای کامپیوتر مقصد ارسال می‌کند. این بسته تا زمانی که به مقصد برسد رمز شده است و طبیعتا کسی نمی تواند از محتوای آنها اطلاعاتی به دست آورد.**

**در ویندوز سرور ۲۰۰۸ و ویندوز ویستا، IPsec یك 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 **یك استاندارد باز است. پروتکل** IPsec **از پروتکل‌های زیر برای تامین امنیت داده ها در شبکه استفاده می‌کند.**

- **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 می‌کند.**
- **بسته بندی امن داده (ESP): این پروتکل، محرمانگی، احراز هویت مبدأ داده ها، تمامیت و یك سرویس ضد بازپخشی را ارائه می‌نماید.**
- **مدیریت امنیت (SA): یك مجموعه از الگوریتم‌ها و داده ها ارائه می‌دهد که این مجموعه، پارامترهای ضروری برای مدیریت کردن عملکرد پروتکل** AH **و/یا پروتکل** ESP **را فراهم می‌کند. پروتکل** ISAKMP**، یك چهارچوب برای عملیات احراز هویت و تبادل کلید ارائه می‌دهد، که در واقع این کلیدها یا به وسیله تنظیم دستی توسط کلیدهایی که از پیش به اشتراك گذاشته شده اند و یا از طریق** IKE[1] **تهیه می‌گردند.**

**مدهای عملیاتی**

**پروتکل** IPsec **می‌تواند برای روش انتقال میزبان به میزبان و روش تونل شبکه مورد استفاده قرار گیرد.**

- **مد انتقالی: در این مد، معمولا تنها اطلاعاتی که به صورت بسته های** IP **ارسال می‌شوند، رمزنگاری و/یا احراز هویت می‌گردند. عملیات مسیریابی بدون تغییر باقی می‌ماند، چرا که**

[1] Internet Key Exchange

**سرآیند بسته IP تغییر نکرده و رمز نشده است. هرچند هنگامی که از سرآیند احراز هویت استفاده می‌شود، آدرس‌های IP قابل ترجمه نیستند، زیرا توسط الگوریتم درهم سازی اطلاعات آن رمزنگاری می‌شود. لایه های انتقال و کاربرد همیشه توسط الگوریتم درهم سازی امن می‌شوند، در نتیجه تحت هیچ شرایطی نمی‌توان اطلاعات آنها را تغییر داد. مد انتقال برای ارتباطات میزبان به میزبان استفاده می‌شود.**

- **مد تونل شبکه:**

**در این مد، کل بسته IP رمزنگاری و/یا احراز هویت می‌شود. سپس درون بسته دیگری بسته بندی شده و یك سرآیند جدید می‌گیرد. این مد برای ایجاد شبکه های خصوصی مجازی برای ارتباطات شبکه به شبکه، ارتباطات میزبان به شبکه و ارتباطات میزبان به میزبان استفاده می‌شود. این مد، پیمایش NAT را پشتیبانی می‌کند.**

**شما می‌توانید با دادن یك سری دستورالعمل‌ها به ویندوز، این سیستم عامل را تعلیم دهید که تحت چه شرایطی از IPSec استفاده کند. تحت این شرایط شما در واقع مشخص می‌کنید که ترافیك کدام گروه از IP ها باید توسط IPSec انجام شود و کدامیك نشود. IPSecبه شما امکان می‌دهد که تعریف کنید چه داده ای و چگونه باید رمزگذاری شود. برای این منظور معمولا از روش فیلتر کردن IP استفاده می‌شود. فهرست خاصی از IP های فیلتر شده که شما تهیه می‌کنید، می‌تواند مرجعی برای استفاده از پروتکل IPSec برای ویندوز باشد.**

**پروتکل PPTP**

**پروتکل Tunneling نقطه به نقطه، بخش توسعه یافته‌ای از پروتکل PPP است که فریم‌های پروتکل PPP را به‌صورت ip برای تبادل آن‌ها از طریق یك شبکه IP مانند اینترنت توسط یك**

**سرایند، کپسوله می‌کند. این پروتکل می‌تواند در شبکه‌های خصوصی از نوع** LAN-to-LAN **نیز استفاده گردد.**

**پروتکل** PPTP **به‌وسیله انجمنی از شرکت‌های مایکروسافت،** Ascend Communications، ۳com ، ESIو US Robotics **ساخته شد.**

PPTP**یك ارتباط** TCP **را (که یك ارتباط** Connection Oriented **بوده و پس از ارسال پکت منتظر** Acknowledgment **آن می‌ماند) برای نگهداری تونل و فریم‌های** PPP **کپسوله شده توسط** GRE[1] **که به معنی کپسوله کردن مسیریابی عمومی است،**

**برای** Tunneling **کردن اطلاعات استفاده می‌کند. ضمناً اطلاعات کپسوله‌شده** PPP **قابلیت رمزنگاری و فشرده شدن را نیز دارا هستند.**

**تونل‌های** PPTP **باید به‌وسیله مکانیسم گواهی همان پروتکل** PPP **که شامل** EAP ،CHAP، MS-PAP،CHAP**می‌شوند، گواهی شوند. در ویندوز ۲۰۰۰ رمزنگاری پروتکل** PPP **فقط زمانی استفاده می‌گردد که پروتکل احراز هویت یکی از پروتکل‌های** EAP ، TLSو **یا** MS-CHAP **باشد.**

**باید توجه شود که رمزنگاری**PPP ، **محرمانگی اطلاعات را فقط بین دو نقطه نهایی یك تونل تأمین می‌کند و در صورتی‌که به امنیت بیشتری نیاز باشد، باید از پروتکل** Ipsec **استفاده شود.**

**پروتکل L۲TP**

**پروتکل** L۲TP **ترکیبی است از پروتکل‌های** PPTP **و** Forwarding **۲** Layer( L۲F) **که توسط شرکت سیسکو توسعه یافته است. این پروتکل ترکیبی است از بهترین خصوصیات موجود در** L۲F **و** PPTP .

[1] Generic Routing Encapsulation

L۲TP**نوعی پروتکل شبکه است که فریم‌های** PPP **را برای ارسال بر روی شبکه‌های** IP **مانند اینترنت و علاوه بر این برای شبکه‌های مبتنی بر**X.۲۵ ، Frame Relay**و یا** ATM **کپسوله می‌کند.**

**هنگامی‌که اینترنت به‌عنوان زیرساخت تبادل اطلاعات استفاده می‌گردد،** L۲TP**می‌تواند به‌عنوان پروتکل** Tunneling **از طریق اینترنت مورد استفاده قرار گیرد.**

L۲TP**برای نگهداری تونل از یك سری پیغام‌های** L۲TP **و نیز از پروتکل** UDP **پروتکل تبادل اطلاعات به‌صورت** Connection Less**که پس از ارسال اطلاعات منتظر دریافت** Acknowledgment**نمی‌شود و اطلاعات را، به مقصد رسیده فرض می‌کند استفاده می‌کند.**

**در** L۲TP **نیز فریم‌های** PPP **کپسوله شده می‌توانند همزمان علاوه بر رمزنگاری شدن، فشرده نیز شوند. البته مایکروسافت پروتکل امنیتی** Ipsec **را به‌جای 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 یك سرایند اضافه برای انتقال اطلاعات از طریق یك شبکه انتقالی به پکت الحاق بنمایند. هرچند این دو پروتکل در برخی موارد نیز با هم تفاوت دارند. برخی از این تفاوت‌ها عبارتند از :**

**۱- شبکه انتقال که** PPTP **احتیاج دارد، باید یك شبکه** IP **باشد. ولی** L۲TP **فقط به یك تونل احتیاج دارد تا بتواند ارتباط** Point-to-Point **را برقرار کند. حال این تونل می تواند بر روی یك شبکه** IP **باشد و یا بر روی شبکه‌های دیگر مانند** X.۲۵ **و یا** ATM ، Frame Relay.

**۲-L۲TP قابلیت فشرده‌سازی سرایند را داراست. هنگامی‌که فشرده‌سازی سرایند انجام می‌گیرد، L۲TP با حجم ۴ بایت عمل می‌کند، در حالی‌که PPTP با حجم ۶ بایت عمل می‌نماید.**

**۳- L۲TP متد احراز هویت را تأمین می‌کند، در حالی‌که PPTP این‌گونه عمل نمی‌کند، هرچند وقتی‌که PPTP یا L۲TP از طریق پروتکل امنیتی IPsec اجرا می‌شوند، هر دو، متد احراز هویت را تأمین می‌نمایند.**

**۴- PPTP رمزنگاری مربوط به PPP را استفاده می‌کند، ولی L۲TP از پروتکل Ipsec برای رمزنگاری استفاده می‌نماید.**

# 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

Cisco۹۷ "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.

RFC۱۰۵۸ "Routing Information Protocol," Hedrick, C.L.; ۱۹۸۸

RFC۱۰۷۴ "NSFNET Backbone SPF-Based Interior Gateway Protocol," Rekhter, J.; ۱۹۸۸

RFC۱۱۳۶ "Administrative Domains and Routing Domains: A Model for Routing in the Internet," Hares, S.; Katz, D.; ۱۹۸۹

RFC۱۱۶۳ "Border Gateway Protocol (BGP)," Lougheed, K.; Rekhter, Y.; ۱۹۹۰

RFC۱۱۶۴ "Application of the Border Gateway Protocol in the Internet," Honig, J.C.; Katz, D.; Mathis, M.; Rekhter, Y.; Yu, J.Y.; ۱۹۹۰

RFC۱۱۹۵ "Use of OSI IS-IS for Routing in TCP/IP and Dual Environments," Callon, R.W.; ۱۹۹۰

RFC۱۲۲۲ "Advancing the NSFNET Routing Architecture," Braun, H.W.; Rekhter, Y.; ۱۹۹۱

RFC۱۲۴۷ "OSPF version ۲," Moy, J.; ۱۹۹۱

RFC۱۲۵۶ S. Deering, "ICMP Router Discovery Messages," RFC ۱۲۵۶, Sept. ۱۹۹۱.

RFC۱۲۶۷ "A Border Gateway Protocol ۳ (BGP-۳)," Lougheed, K.; Rekhter, Y.; ۱۹۹۱

RFC۱۵۸۴ J. Moy, "Multicast Extensions to OSPF," RFC ۱۵۸۴, March ۱۹۹۴.

RFC۱۷۲۳ G. Malkin, RIP Version ۲ - Carrying Additional Information. RFC ۱۷۲۳, November۱۹۹۴

RFC۱۷۷۱ Y. Rekhter and T. Li, "A Border Gateway Protocol ۴ (BGP-۴)," RFC ۱۷۷۱, March ۱۹۹۵.

RFC۱۷۷۲ Y. Rekhter and P. Gross, "Application of the Border Gateway Protocol in the Internet,"

RFC ۱۷۷۲, March ۱۹۹۵.

RFC۱۷۷۳ P. Traina, "Experience with the BGP-۴ protocol," RFC ۱۷۷۳, March ۱۹۹۵

RFC۲۰۰۲ C. Perkins, "IP Mobility Support," RFC ۲۰۰۲, ۱۹۹۶.

RFC۲۱۷۸ J. Moy, "Open Shortest Path First Version ۲", RFC ۲۱۷۸, July ۱۹۹۷.

RFC۸۲۳ "DARPA Internet Gateway," Hinden, R.M.; Sheltzer, A.; ۱۹۸۲

RFC۸۲۷ "Exterior Gateway Protocol (EGP)," Rosen, E.C.; ۱۹۸۲

RFC۸۸۸ "STUB Exterior Gateway Protocol," Seamonson, L.; Rosen, E.C.; ۱۹۸۴

RFC۹۰۴ "Exterior Gateway Protocol Formal Specification," Mills, D.L.; ۱۹۸۴

RFC۹۱۱ "EGP Gateway under Berkeley UNIX ۴٫۲," Kirton, P.; ۱۹۸۴

RFC۱۱۰۲ "Policy Routing in Internet Protocols," Clark, D.D.; ۱۹۸۹

RFC۱۱۰۴ "Models of Policy-Based Routing," Braun, H.W.; ۱۹۸۹

RFC۱۱۲۴ "Policy Issues in Interconnecting Networks," Leiner, B.M.; ۱۹۸۹

RFC۱۱۲۵ "Policy Requirements for Inter-Administrative Domain Routing," Estrin, D.;۱۹۸۹

RFC۱۲۴۵ "OSPF Protocol Analysis," Moy, J., ed; ۱۹۹۱

RFC۱۲۴۶ "Experience with the OSPF Protocol," Moy, J., ed.; ۱۹۹۱

RFC۱۲۵۴ "Gateway Congestion Control Survey," Mankin, A.; Ramakrishnan, K.K, eds.;۱۹۹۱

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, ۱۹۸۵.

IEEE, "IEEE Standards for Local Area Networks: Token-Passing Bus Access Method and Physical Layer Specification", IEEE, New York, New York, ۱۹۸۵.

IEEE, "IEEE Standards for Local Area Networks: Token Ring Access Method and Physical Layer Specifications", IEEE, New York, New York, ۱۹۸۵.

IEEE, "IEEE Standards for Local Area Networks: Logical Link Control", IEEE, New York, New York, ۱۹۸۵.

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, ۱۹۹۳.

RFC۱۶۶۱ The Point-to-Point Protocol (PPP). W. Simpson, Editor. July ۱۹۹۴.

RFC۱۶۶۳ PPP Reliable Transmission. D. Rand. July ۱۹۹۴.

RFC۱۷۱۷ The PPP Multilink Protocol (MP). K. Sklower, B. Lloyd, G. McGregor, D.

Carr. November ۱۹۹۴.

RFC۱۰۴۲ Standard for the transmission of IP datagrams over IEEE ۸۰۲ networks. J.

Postel, J.K. Reynolds. Feb-۰۱-۱۹۸۸.

RFC۱۲۳۰ IEEE ۸۰۲٫۴ Token Bus MIB. K. McCloghrie, R. Fox. May-۰۱-۱۹۹۱.

RFC۱۲۳۱ IEEE ۸۰۲٫۵ Token Ring MIB. K. McCloghrie, R. Fox, E. Decker.

RFC۱۰۵۵ Nonstandard for transmission of IP datagrams over serial lines: SLIP. J.L.

Romkey. Jun-۰۱-۱۹۸۸.

**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**

**اصول مهندسی اینترنت- گرد آوری و تألیف: احسان ملکیان**

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.persiangig.com

www.shabgard.orgF

www.mostafanoori.com

www.cisco.parsfa.com

www.mojsazan.com

www.iana.org

www.raeissi.com

www.monkey.org

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. iranhost.com

www.forum.p۳۰parsi.com

www.raeissi.com