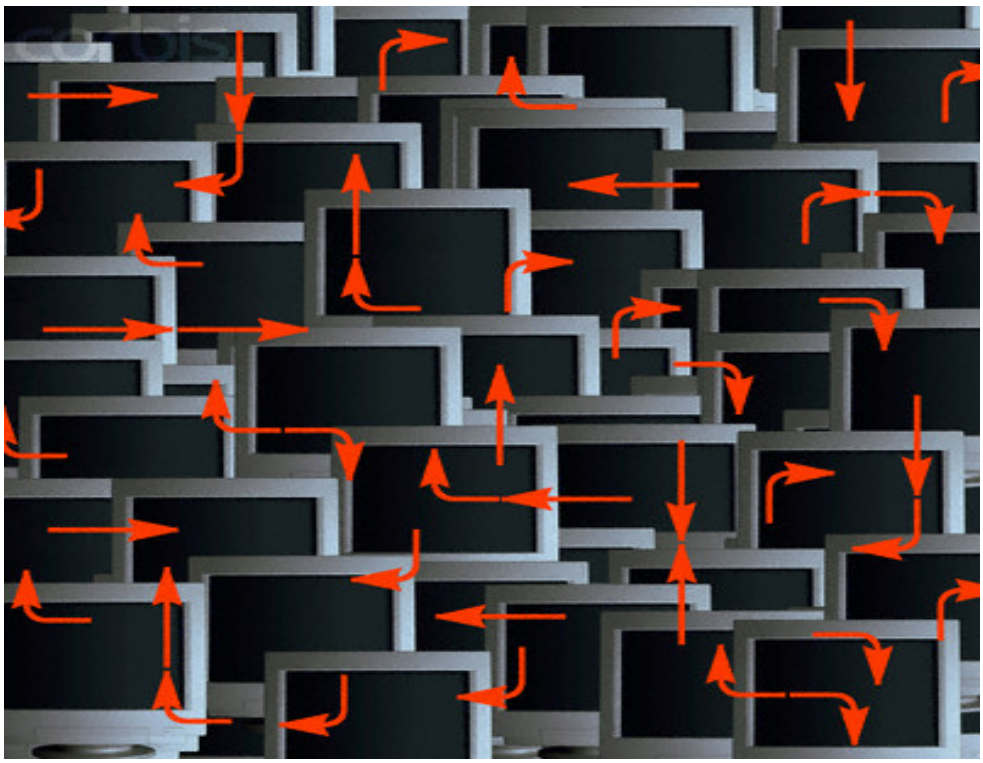
مجموعه Ebook های مهندس حمید ریاضی

آموزش شبکه های کامپیوتری



مقدمه

نبود مرجع کامل علمی بصورت یکجا و ضعف کاربران در تحقیق و پـژوهش ، مـن را بـر آن داشت تا مجموعه از **ebook** های پژوهشی خود را در اختیـار طالبـان علـم قـرار داده تا آنها را در راه تعلـیم و تحقیـق یـاری کـنم .شـما عزیـزان مـی توانیـد نظـرات و پیشنهاد های خـود را بـه آدرس **hamidriazi@yahoo.com** یـا بـا تلفـن ۰۰۹۸۹۱۲۷۵۳۶۸۵۴ تماس گرفته تا من را در این را ه یاری کنید .

مهندس حمید ریاضی

چکیده

استفاده از شبکه های کامپیوتری در چندین سال اخیر رشد فراوانی کرده وسازمانها وموسسات اقدام به برپایی شبکه نموده اند . هر شبکه کامپیوتری باید با توجه به شرایط وسیاست های هر سازمان ، طراحی وپیاده سازی گردد. در واقع شبکه های کامپیوتری زیر ساخت های لازم را برای به اشتراک گذاشتن منابع در سازمان فراهم می آورند؛در صورتیکه این زیر ساختها به درستی طراحی نشوند، در زمان استفاده از شبکه مشکلات متفاوتی پیش آمده و باید هزینه های زیادی به منظور نگهداری شبکه وتطبیق آن با خواسته های مورد نظر صرف شود.

در زمان طراحی یک شبکه سوالات متعددی مطرح می شود:

-برای طراحی یک شبکه باید از کجا شروع کرد؟

-چه پارامترهایی را باید در نظر گرفت ؟

-هدف از برپاسازی شبکه چیست ؟

- انتظار کاربران از شبکه چیست ؟

- آیا شبکه موجود ارتقاء می باید ویا یک شبکه از ابتدا طراحی می شود؟

-چه سرویس ها و خدماتی برروی شبکه ارائه خواهد شد؟

بطور کلی قبل از طراحی فیزیکی یک شبکه کامپیوتری ، ابتدا باید خواسته ها شناسایی وتحلیل شوند، مثلا در یک کتابخانه چرا قصد ایجاد یک شبکه را داریم واین شبکه باید چه سرویس ها وخدماتی را ارائه نماید؛ برای تامین سرویس ها وخدمات مورد نظر اکثریت کاربران ، چه اقداماتی باید انجام داد ؛ مسائلی چون پروتکل مورد نظر برای استفاده از شبکه ، سرعت شبکه واز همه مهمتر مسائل امنیتی شبکه ، هریک از اینها باید به دقت مورد بررسی قرار گیرد. سعی شده است پس از ارائه تعاریف اولیه ، مطالبی پیرامون کاربردهای عملی آن نیز ارائه شود تا در تصمیم گیری بهتر یاری کند.

تاریخچه پیدایش شبکه

در سال ۱۹۵۷ نخستین ماهواره یعنی اسپوتنیک توسط اتحاد جماهیر شوروی سابق به فضا پرتاب شد . در همین دوران رقابت سختی از نظر تسلیحاتی بین دو ابر قدرت آن زمان جریان داشت و دنیا در دوران جنگ سرد به‌سر می برد. وزارت دفاع آمریکا در واکنش به این اقدام رقیب نظامی خود ،آژانس پروژه های تحقیقاتی پیشرفته یا آرپا (ARPA)را تأسیس کرد .

یکی از پروژه های مهم این آژانس تأمین ارتباطات در زمان جنگ جهانی احتمالی تعریف شده بود. در همین سال‌ها در مراکز تحقیقاتی غیرنظامی که در امتداد دانشگاه‌ها بودند، تلاش برای اتصال کامپیوترها به یکدیگر در جریان بود .در آن زمان کامپیوترهای Mainframe از طریق ترمینال‌ها به کاربران سرویس می‌دادند.

در اثر اهمیت یافتن این موضوع آژانس آرپا (ARPA) منابع مالی پروژه اتصال دو کامپیوتر از راه دور به یکدیگر را در دانشگاه MIT بر عهده گرفت . در اواخر سال ۱۹۶۰ اولین شبکه کامپیوتری بین چهار کامپیوتر که دو تای آنها درMIT ، یکی در دانشگاه کالیفرنیا و دیگری در مرکز تحقیقاتی استنفورد قرار داشتند، راه‌اندازی شد. این شبکه آرپانت (ARPAnet) نامگذاری شد . در سال ۱۹۶۵ نخستین ارتباط راه دور بین دانشگاه MIT و یک مرکز دیگر نیز بر قرار گردید.

در سال ۱۹۷۰ شرکت معتبر زیراکس، یک مرکز تحقیقاتی در پالوآلتو تأسیس کرد. این مرکز در طول سال‌ها مهمترین فناوری‌های مرتبط با کامپیوتر را معرفی کرده است و از این نظر به یک مرکز تحقیقاتی افسانه ای بدل گشته است. این مرکز تحقیقاتی که پارک (PARC) نیز نامیده می شود، به تحقیقات در زمینه شبکه‌های کامپیوتری پیوست. تا این سال‌ها شبکه آرپانت به امور نظامی اختصاص داشت، اما در سال ۱۹۷۲ به عموم معرفی شد. در این سال شبکه آرپانت مراکز کامپیوتری بسیاری از دانشگاه ها و مراکز تحقیقاتی را به هم متصل کرده بود. در سال ۱۹۷۲ نخستین نامه الکترونیکی از طریق شبکه منتقل گردید.

در این سال‌ها حرکتی غیرانتفاعی به‌نام MERIT که چندین دانشگاه بنیان‌گذار آن بوده‌اند، مشغول توسعه روش‌های اتصال کاربران ترمینال‌ها به کامپیوتر مرکزی یا میزبان بود. مهندسان پروژه MERIT در تلاش برای ایجاد ارتباط بین کامپیوترها، مجبور شدند تجهیزات لازم را خود طراحی کنند. آنان با طراحی تجهیزات واسطه برای مینی‌کامپیوتر DECPDP-11 نخستین بستر اصلی یا Backbone شبکه‌های کامپیوتری را ساختند. تا سال‌ها نمونه‌های اصلاح شده این کامپیوتر با نام Primary Communications Processor یا PCP نقش میزبان را در شبکه‌ها ایفا می کرد . نخستین شبکه از این نوع که چندین ایالت را به هم متصل می کرد Michnet نام داشت.

در سال ۱۹۷۳ موضوع رساله دکترای آقای باب مت‌کالف (Bob Metcalfe) درباره مفهوم اترنت در مرکز پارک مورد آزمایش قرار گرفت. با تثبیت اترنت تعداد شبکه های کامپیوتری رو افزایش گذاشت . روش اتصال کاربران به کامپیوتر میزبان در آن زمان به این صورت بود که یک نرم افزار خاص بر روی کامپیوتر مرکزی اجرا می‌شد و ارتباط کاربران را برقرار می کرد. اما در سال ۱۹۷۶ نرم‌افزار جدیدی به‌نام Hermes عرضه شد که برای نخستین بار به کاربران اجازه می‌داد تا از طریق یک ترمینال به‌صورت تعاملی مستقیماً به سیستم MERIT متصل شوند. این، نخستین باری بود که کاربران می‌توانستند در هنگام برقراری ارتباط از خود بپرسند : از وقایع مهم تاریخچه شبکه‌های کامپیوتری ، ابداع روش سوئیچینگ بسته‌ای یا Packet Switching است. قبل از معرفی شدن این روش از سوئیچینگ مداری یا Circuit Switching برای تعیین مسیر ارتباطی استفاده می شد. اما در سال ۱۹۷۴ با پیدایش پروتکل ارتباطی TCP/IP از مفهوم Packet Switching استفاده گسترده‌تری شد. این پروتکل در سال ۱۹۸۲ جایگزین پروتکل NCP شد و به پروتکل استاندارد برای آرپانت تبدیل گشت. در همین زمان یک شاخه فرعی بنام MILnet در آرپانت، همچنان از پروتکل قبلی پشتیبانی می‌کرد و به ارائه خدمات نظامی می پرداخت. با این تغییر و تحول، شبکه‌های زیادی به بخش تحقیقاتی

این شبکه متصل شدند و آرپانت به اینترنت تبدیل گشت . در این سال‌ها حجم ارتباطات شبکه‌ای افزایش یافت و مفهوم ترافیک شبکه مطرح شد.

مسیریابی در این شبکه به‌کمک آدرس‌های IP به‌صورت ۳۲ بیتی انجام می‌گرفته است. هشت بیت اول آدرس IPبه شبکه‌های محلی تخصیص داده شده بود که به سرعت مشخص گشت تناسبی با نرخ رشد شبکه‌ها ندارد و باید در آن تجدید نظر شود. مفهوم شبکه‌های LAN و شبکه‌های WAN در سال دهه ۷۰ میلادی از یکدیگر تفکیک شدند.در آدرس‌دهی ۳۲ بیتی اولیه، بقیه ۲۴ بیت آدرس به میزبان در شبکه اشاره می کرد.

در سال ۱۹۸۳ سیستم نامگذاری دامنه‌ها (Domain Name System) به‌وجود آمد و اولین سرویس‌دهنده نامگذاری (Name server)راه‌اندازی شد و استفاده از نام به‌جای آدرس‌های عددی معرفی شد. در این سال تعداد میزبان‌های اینترنت از مرز ده هزار عدد فراتر رفته بود.

شبکه کامپیوتری چیست ؟

اساسا یک شبکه کامپیوتری شامل دو یا بیش از دو کامپیوتر وابزارهای جانبی مثل چاپگرها، اسکنرها ومانند اینها هستند که بطور مستقیم بمنظور استفاده مشترک از سخت افزار ونرم افزار، منابع اطلاعاتی ابزارهای متصل ایجاده شده است توجه داشته باشید که به تمامی تجهیزات سخت افزاری ونرم افزاری موجود در شبکه منبع(Source) گویند. در این تشریک مساعی با توجه به نوع پیکربندی کامپیوتر ، هر کامپیوتر کاربر می تواند در آن واحد منابع خود را اعم از ابزارها وداده ها با کامپیوترهای دیگر همزمان بهره ببرد.

" دلایل استفاده از شبکه را می توان موارد ذیل عنوان کرد" :

۱ – استفاده مشترک از منابع :

استفاده مشترک از یک منبع اطلاعاتی یا امکانات جانبی رایانه ، بدون توجه به محل جغرافیایی هریک از منابع را استفاده از منابع مشترک گویند.

۲ – کاهش هزینه :

متمرکز نمودن منابع واستفاده مشترک از آنها وپرهیز از پخش آنها در واحدهای مختلف واستفاده اختصاصی هر کاربر در یک سازمان کاهش هزینه را در پی خواهد داشت .

۳ – قابلیت اطمینان :

این ویژگی در شبکه ها بوجود سرویس دهنده های پشتیبان در شبکه اشاره می کند ، یعنی به این معنا که می توان از منابع گوناگون اطلاعاتی وسیستم ها در شبکه نسخه های دوم وپشتیبان تهیه کرد ودر صورت عدم دسترسی به یک از منابع اطلاعاتی در شبکه " بعلت از کارافتادن سیستم " از نسخه های پشتیبان استفاده کرد. پشتیبان از سرویس دهنده ها در شبکه کارآیی، فعالیت وآمادگی دایمی سیستم را افزایش می دهد.

۴ – کاهش زمان :

یکی دیگر از اهداف ایجاد شبکه های رایانه ای ، ایجاد ارتباط قوی بین کاربران از راه دور است ؛ یعنی بدون محدودیت جغرافیایی تبادل اطلاعات وجود داشته باشد. به این ترتیب زمان تبادل اطلاعات و استفاده از منابع خود بخود کاهش می یابد.

۵ – قابلیت توسعه :

یک شبکه محلی می تواند بدون تغییر در ساختار سیستم توسعه یابد وتبدیل به یک شبکه بزرگتر شود. در اینجا هزینه توسعه سیستم هزینه امکانات وتجهیزات مورد نیاز برای گسترش شبکه مد نظر است.

۶ – ارتباطات:

کاربران می توانند از طریق نوآوریهای موجود مانند پست الکترونیکی ویا دیگر سیستم های اطلاع رسانی پیغام هایشان را مبادله کنند ؛ حتی امکان انتقال فایل نیز وجود دارد.

در طراحی شبکه مواردی که قبل از راه اندازی شبکه باید مد نظر قرار دهید شامل موارد ذیل هستند:

۱ – اندازه سازمان

۲ – سطح امنیت

۳ – نوع فعالیت

۴ – سطح مدیریت

۵ – مقدار ترافیک

۶ – بودجه

مفهوم گره " Node " وایستگاههای کاری [Work Stations] :

" هرگاه شما کامپیوتری را به شبکه اضافه می کنید ، این کامپیوتر به یک ایستگاه کاری یا گره تبدیل می شود. یک ایستگاه کاری ؛ کامپیوتری است که به شبکه الصاق شده است و در واقع اصطلاح ایستگاه کاری روش دیگری است برای اینکه بگوییم یک کامپیوتر متصل به شبکه است. یک گره چگونگی وارتباط شبکه یا ایستگاه کاری ویا هر نوع ابزار دیگری است که به شبکه متصل است وبطور ساده تر هر چه را که به شبکه متصل والحاق شده است یک گره گویند". برای شبکه جایگاه وآدرس یک ایستگاه کاری مترادف با هویت گره اش 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"

مدل شبکه نظیر به نظیر:

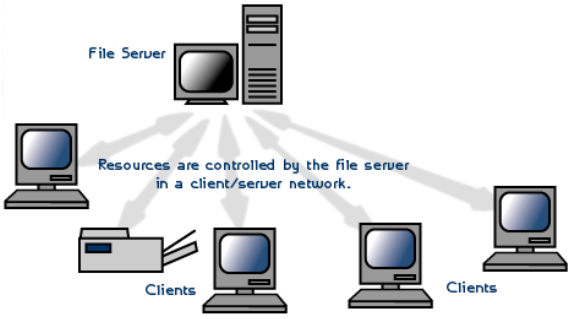
در این شبکه ایستگاه ویژه ای جهت نگهداری فایل های اشتراکی وسیستم عامل شبکه وجود ندارد. هر ایستگاه می تواند به منابع سایر ایستگاه ها در شبکه دسترسی پیدا کند. هر ایستگاه خاص می تواند هم بعنوان Server وهم بعنوان Client عمل کند. در این مدل هر کاربر خود مسئولیت مدیریت وارتقاء دادن نرم افزارهای ایستگاه خود 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 .

مدل شبکه مبتنی بر سرویس دهنده :

در این مدل شبکه ، یک کامپیوتر بعنوان سرویس دهنده کلیه فایل ها ونرم افزارهای اشتراکی نظیر واژه پرداز ها، 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.

مدل سرویس دهنده / سرویس گیرنده :

در این مدل یک ایستگاه در خواست انجام کارش را به سرویس دهنده ارائه می دهد وسرویس 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 واین مدل دارای کارایی بالاتری می باشد.



هر شبکه اساسا از سه بخش ذیل تشکیل می شود:

ابزارهایی که به پیکربندی اصلی شبکه متصل می شوند بعنوان مثال : کامپیوتر ها ، چاپگرها، هاب ها"Hubs " سیم ها ، کابل ها وسایر رسانه هایی که برای اتصال ابزارهای شبکه استفاده می شوند.

سازگار کننده ها [Adaptor]:

که بعنوان اتصال کابل ها به کامپیوتر هستند . اهمیت آنها در این است که بدون وجود آنها 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.

اجزا ءشبکه :

اجزا اصلی یک شبکه کامپیوتری عبارتند از :

۱ – کارت شبکه : " 5[NIC- Network Interface Card]" :

برای استفاده از شبکه وبرقراری ارتباط بین کامپیوتر ها از کارت شبکه ای استفاده می شود که در داخل یکی از شیارهای برد اصلی کامپیوتر های شبکه " اعم از سرویس دهنده وگیرنده " بصورت سخت افزاری وبرای کنترل ارسال ودریافت داده نصب می گردد.

۲ – رسانه انتقال [Transmission Medium]:

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".

۳– سیستم عامل شبکه " NOS- Network [Operating System] :

سیستم عامل شبکه برروی سرویس دهنده اجرا می شود و سرویس های مختلفی مانند: اجازه ورود به سیستم "Login"، رمز عبور "Password"، چاپ فایل ها " Printfiles"، مدیریت شبکه " Net work management " را در اختیار کاربران می گذارد.

انواع شبکه از لحاظ جغرافیایی:

نوع شبکه توسط فاصله بین کامپیوتر های تشکیل دهنده آن شبکه مشخص می شود:

شبکه محلی [LAN= Local Area Network] :

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

ه – سیستم ارتباط دهنده

شبکه گسترده [WAN = Wide Area Network] :

اتصال شبکه های محلی از طریق خطوط تلفنی ، کابل های ارتباطی ماهواره ویا دیگر سیستم هایی مخابراتی چون خطوط استیجاری در یک منطقه بزرگتر را شبکه گسترده گویند. در این شبکه کاربران یا رایانه ها از مسافت های دور واز طریق خطوط مخابراتی به یکدیگر متصل می شوند. کاربران هر یک از این شبکه ها می توانند به اطلاعات ومنابع به اشتراک گذاشته شده توسط شبکه های دیگر دسترسی یابند. از این فناوری با نام شبکه های راه دور " Long Haul Network" نیز نام برده می شود. در شبکه گسترده سرعت انتقال داده نسبت به شبکه های محلی خیلی کمتر است. بزرگترین ومهم ترین شبکه گسترده ، شبکه جهانی اینترنت می باشد.

ریخت شناسی شبکه [Net work Topology]:

توپولوژی شبکه تشریح کننده نحوه اتصال کامپیوتر ها در یک شبکه به یکدیگر است. پارامترهای اصلی در طراحی یک شبکه ، قابل اعتماد بودن ومقرون به صرفه بودن است. انواع متداول توپولوژی ها در شبکه کامپیوتری عبارتند از :

۱ – توپولوژی ستاره ای [Star]:

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.

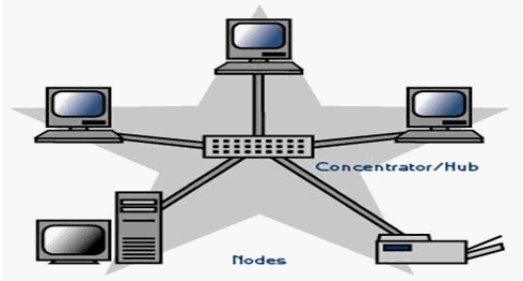
نقاط ضعف این توپولوژی آن است که عملیات کل شبکه به هاب وابسته است. این بدان معناست که اگر هاب از کار بیفتد، کل شبکه از کار خواهد افتاد .

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.



توپولوژی حلقوی [Ring] :

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 ".

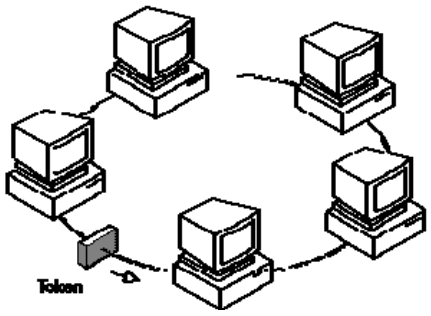
* برای اضافه کردن یک ایستگاه به شبکه باید کل شبکه را متوقف کرد.

نقاط قوت توپولوژی فوق عبارتند از :

* نصب شبکه با این توپولوژی ساده است.

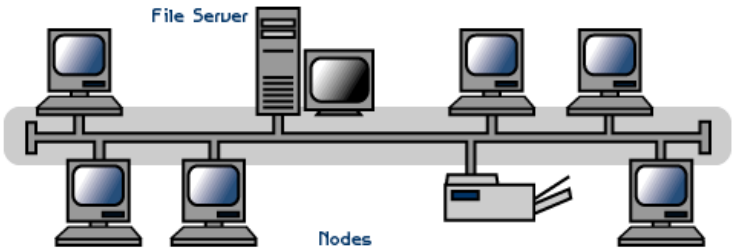
* توسعه شبکه با این توپولوژی به راحتی انجام می شود.

* در این توپولوژی از کابل فیبر نوری میتوان استفاده کرد.



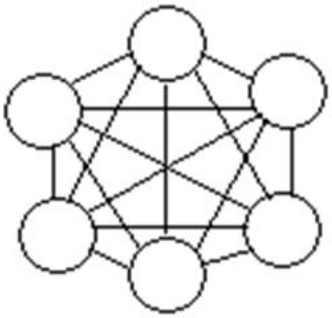
توپولوژی اتوبوسی [BUS]:

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.



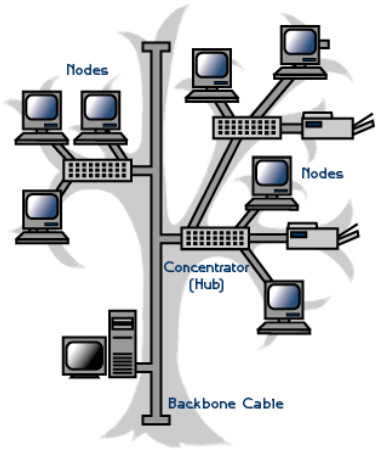
توپولوژی توری [Mesh] :

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-1)/2 محاسبه می شود که در آن N تعداد ایستگاه های شبکه می باشد.



توپولوژی درختی [Tree] :

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 " Hybrid"

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

پروتکل :

برای برقراری ارتباط بین رایانه ها ی سرویس گیرنده و سرویس دهنده قوانین کامپیوتری برای انتقال ودریافت داده مشخص شده اند که به قرارداد یا پروتکل موسومند. این قرارداد ها وقوانین بصورت نرم افزاری در سیستم برای ایجاد ارتباط ایفای نقش می کنند. پروتکل با قرارداد ، در واقع زبان مشترک کامپیوتری است که برای درک وفهم رایانه بهنگام در خواست وجواب متقابل استفاده می شود. پروتکل تعیین کننده مشخصه های شبکه ، روش دسترسی وانواع فیزیکی توپولوژی ها ، سرعت انتقال داده ها وانواع کابل کشی است .

پروتکل های شبکه :

ما در این دستنامه تنها دو تا از مهمترین پروتکل های شبکه را معرفی می کنیم:

" پروتکل کنترل انتقال / پروتکل اینترنت "Protoc l/ Inernet Protocol Tcp / ip= Transmission Control"

پروتکل فوق شامل چهار سطح است که عبارتند از :

الف – سطح لایه کاربرد " Application "

ب – سطح انتقال "Transporter "

ج – سطح اینترنت "Internet "

د – سطح شبکه [Net work]:

" از مهمترین ومشهورترین پروتکل های مورد استفاده در شبکه اینترنت است این بسته نرم افزاری به اشکال مختلف برای کامپیوتر ها وبرنامه ها ی مختلف ارائه می گردد. Tcp/ip از مهمترین پروتکل های ارتباطی شبکه در جهان تلقی می شود ونه تنها برروی اینترنت وشبکه های گسترده گوناگون کاربرد دارد، بلکه در شبکه های محلی مختلف نیز مورد استفاده قرار می گیردو در واقع این پروتکل زبان مشترک بین کامپیوتر ها به هنگام ارسال و دریافت اطلاعات یا داده می باشد. این پروتکل به دلیل سادگی مفاهیمی که در خود دارد اصطلاحا به سیستم باز مشهور است ، برروی هر کامپیوتر وابر رایانه قابل طراحی وپیاده سازی است. از فاکتورهای مهم که این پروتکل بعنوان یک پروتکل ارتباطی جهانی مطرح می گردد، به موارد زیر می توان اشاره کرد:

۱ – این پروتکل در چار چوب UNIX Operating System ساخته شده وتوسط اینترنت بکار گرفته می شود.

۲ – برروی هر کامپیوتر قابل پیاده سازی می باشد.

۳ – بصورت حرفه ای در شبکه های محلی وگسترده مورد استفاده قرار می گیرد.

۴ – پشتیبانی از مجموعه برنامه ها وپروتکل های استاندارد دیگر چون پروتکل انتقال فایل " FTP " وپروتکل دو سویه " Point to point Protcol = PPP ".

بنیاد واساس پروتکل Tcp/ip آن است که برای دریافت و ارسال داده ها یا پیام پروتکل مذکور ؛ پیام ها وداده ها را به بسته های کوچکتر وقابل حمل تر تبدیل می کند ، سپس این بسته ها به مقصد انتقال داده می شود ودر نهایت پیوند این بسته ها به یکدیگر که شکل اولیه پیام ها وداده ها را بخود می گیرد ، صورت می گیرد. یکی دیگر از ویژگی های مهم این پروتکل قابلیت اطمینان آن در انتقال پیام هاست یعنی این قابلیت که به بررسی وبازبینی بسته ها ومحاسبه بسته های دریافت شده دارد. در ضمن این پروتکل فقط برای استفاده در شبکه

اینترنت نمی باشد. بسیاری از سازمان وشرکت ها برای ساخت وزیر بنای شبکه خصوصی خود که از اینترنت جدا می باشد نیز در این پروتکل استفاده می کنند.

- پروتکل سیستم ورودی وخروجی پایه شبکه

Net work basic input/ outputSystem=Net Bios واسطه یا رابطی است که توسط IBM بعنوان استانداردی برای دسترسی به شبکه توسعه یافت . این پروتکل داده ها را از لایه بالاترین دریافت کرده وآنها را به شبکه منتقل می کند. سیستم عاملی که با این پروتکل ارتباط برقرار می کند سیستم عامل شبکه "NOS" نامیده می شود کامپیوتر ها از طریق کارت شبکه خود به شبکه متصل می شوند. کارت شبکه به سیستم عامل ویژه ای برای ارسال اطلاعات نیاز دارد. این سیستم عامل ویژه را Net BIOS می نامند که در حافظه ROM کارت شبکه ذخیره شده است.

BIOS Net همچنین روشی را برای دسترسی به شبکه ها با پروتکل های مختلف مهیا می کند . این پروتکل از سخت افزار شبکه مستقل است . این پروتکل مجموعه ای از فرامین لازم برای در خواست خدمات شبکه ای سطح پایین را برای برنامه های کاربردی فراهم می کند تا جلسات لازم برای انتقال اطلاعات در بین گره ها ی یک شبکه را هدایت کنند.

در حال حاضر وجود "Net BIOS Net BEUI= Net BIOS Enhansed User Interface" امتیازی جدید می دهد که این امتیاز درواقع ایجاد گزینه انتقال استاندارد است و Net BEUI در شبکه های محلی بسیار رایج است. همچنین قابلیت انتقال سریع داده ها را نیز دارد . اما چون یک پروتکل غیر قابل هدایت است به شبکه های محلی محدود شده است.

مدل OSI Open System Interconnection:

این مدل مبتنی بر قراردادی است که سازمان استانداردهای جهانی ایزو بعنوان مرحله ای از استاندارد سازی قراردادهای لایه های مختلف توسعه دارد . نام این مدل مرجع به این دلیل ا اس آی است چونکه با اتصال سیستم های باز سروکار دارد وسیستم های باز سیستم هایی هستند که برای ارتباط باسیستم های دیگر باز هستند این مدل هفت لایه دارد که اصولی که منجر به ایجاد این لایه ها شده اند عبارتند از :

۱ – وقتی نیاز به سطوح مختلف از انتزاع است ، لایه ای باید ایجاد شود.

۲ – هر لایه باید وظیفه مشخصی داشته باشد.

۳ – وظیفه هر لایه باید با در نظر گرفتن قراردادهای استاندارد جهانی انتخاب گردد.

۴ – مرزهای لایه باید برای کمینه کردن جریان اطلاعات از طریق رابط ها انتخاب شوند.

اکنون هفت لایه را به نوبت از لایه پایین مورد بحث قرار می دهیم:

۱ – لایه فیزیکی :

به انتقال بیتهای خام برروی کانال ارتباطی مربوط می شود. در اینجا مدل طراحی با رابط های مکانیکی ، الکتریکی ، ورسانه انتقال فیزیکی که زیر لایه فیزیکی قراردارند سروکار دارد.

۲ – لایه پیوند ها:

مبین نوع فرمت هاست مثلا شروع فریم ، پایان فریم، اندازه فریم وروش انتقال فریم . وظایف این لایه شامل موارد زیر است :

مدیریت فریم ها ، خطایابی وارسال مجدد فریم ها، ایجاد تمایز بین فریم ها داده وکنترل وایجاد هماهنگی بین کامپیوتر ارسال کننده ودریافت کننده داده ها.

پروتکل های معروف برای این لایه عبارتند از :

الف – پروتکل SDLC که برای مبادله اطلاعات بین کامپیوتر ها بکار می رود و اطلاعات را به شکل فریم سازماندهی می کند.

ب – پروتکل HDLC که کنترل ارتباط داده ای سطح بالا زیر نظر آن است وهدف از طراحی آن این است که با هر نو ع ایستگاهی کارکند از جمله ایستگاههای اولیه ، ثانویه وترکیبی.

۳ – لایه شبکه :

وظیفه این لایه ، مسیر یابی می باشد ، این مسیر یابی عبارتست از : تعیین مسیر متناسب برای انتقال اطلاعات لایه شبکه آدرس منطقی هر فریم را بررسی می کند . و آن فریم را بر اساس جدول مسیر یابی به مسیر یاب بعدی می فرستد . لایه شبکه مسئولیت ترجمه هر آدرس منطقی به یک آدرس فیزیکی را بر عهده دارد. پس می توان گفت برقراری ارتباط یا قطع آن ، مولتی پلکس کردن از مهمترین وظایف این لایه است. از نمونه بارز خدمات این لایه ، پست الکترونیکی است.

۴ – لایه انتقال :

وظیفه ارسال مطمئن یک فریم به مقصد را برعهده دارد. لایه انتقال پس از ارسال یک فریم به مقصد ، منتظر می ماند تا سیگنالی از مقصد مبنی بر دریافت آن فریم دریافت کند. در صورتیکه لایه محل در منبع سیگنال مذکور را از مقصد دریافت نکند. مجددا اقدام به ارسال همان فریم به مقصد خواهد کرد.

۵ – لایه اجلاس :

وظیفه برقراری یک ارتباط منطقی بین نرم افزار های دو کامپیوتر ی که به یکدیگر متصل هستند به عهده این لایه است. وقتی که یک ایستگاه بخواهد به یک سرویس دهنده متصل شود ، سرویس دهنده فرایند برقراری ارتباط را

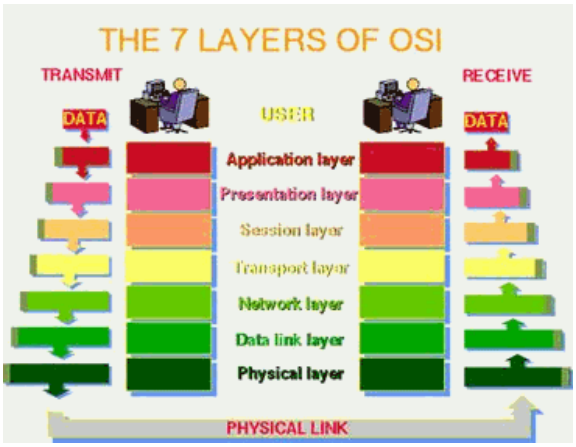
بررسی می کند، سپس از ایستگاه ، درخواست نام کاربر، ورمز عبور را خواهد کرد. این فرایند نمونه ای از یک اجلاس می باشد.

۶ – لایه نمایش :

این لایه اطلاعات را از لایه کاربرد دریافت نموده ، آنها را به شکل قابل فهم برای کامپیوتر مقصد تبدیل می کند . این لایه برای انجام این فرایند اطلاعات را به کدهای ASCII ویا Unicode تبدیل می کند.

۷ – لایه کاربرد :

این لایه امکان دسترسی کاربران به شبکه را با استفاده از نرم افزارهایی چون E-mail- FTP و.... فراهم می سازد.



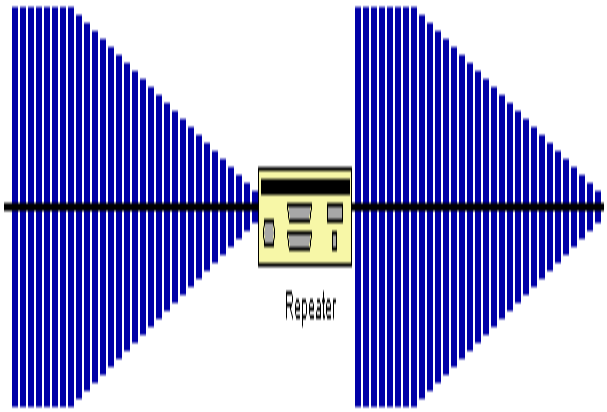
ابزارهای اتصال دهنده : "Connectivity Devices" :

ابزارهای اتصال به یک شبکه اضافه می گردند تا عملکرد وگستره شبکه وتوانایی های سخت افزاری شبکه را ارتقاء دهند .

گستره وسیعی از ابزارهای اتصال در شبکه وجود دارند اما شما احتمالا برای کار خود به ابزارهای ذیل نیازمند خواهید بود:

۱ – کنترل کننده ها [Reapeaters]:

تکرار کننده وسیله ای است که برای اتصال چندین سگمنت یک شبکه محلی بمنظور افزایش وسعت مجاز آن شبکه مورد استفاده قرار می گیرد . هر تکرار کننده از درگاه ورودی " Port " خود داده ها را پذیرفته وبا تقویت آنها ، داده ها را به درگاهی خروجی خود ارسال می کند. یک تکرار کننده در لایه فیزیکی مدل OSI عمل می کند. هر کابل یا سیم بکار رفته در شبکه که بعنوان محلی برای عبور ومرور سیگنال هاست آستانه ای دارد که در آن آستانه سرعت انتقال سیگنال کاهش می یابد ودر اینجا تکرار کننده بعنوان ابزاری است که این سرعت عبور را در طول رسانه انتقال تقویت می کند.



۲ – هاب ها [Hubs]:

ابزاری هستند در شبکه که برای اتصال یک یا بیش از دو ایستگاه کاری به شبکه مورد استفاده قرار می گیرد ویک ابزار معمول برای اتصال ابزارهای شبکه است . هابها معمولا برای اتصال سگمنت های شبکه محلی استفاده می شوند. یک هاب دارای در گاهی های چند گانه است. وقتی یک بسته در یک درگاهی وارد می شود به سایر در گاهی ها کپی می شود تا اینکه تمامی سگمنت های شبکه محلی بسته ها را ببینند. سه نوع هاب رایج وجود دارد:

الف – هاب فعال :

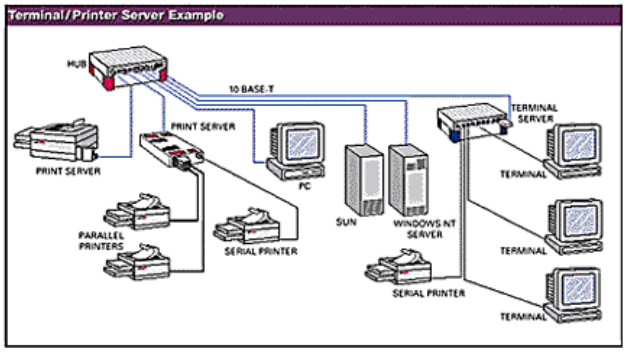
که مانند آمپلی فایر عمل می کند و باعث تقویت مسیر عبور سینگال ها می شود واز تصادم وبرخورد سیگنال ها در مسیر جلوگیری بعمل می آورد . این هاب نسبتا قیمت بالایی دارد.

ب – غیر فعال :

که بر خلاف نوع اول که در مورد تقویت انتقال سیگنال ها فعال است این هاب منفعل است.

ج – آمیخته :

که قادر به ترکیب انواع رسانه ها " کابل کواکسیال نازک ،ضخیم و....." وباعث تعامل درون خطی میان سایر ها بها می شود.



۳ – مسیر یاب ها [Routers]:

در شبکه سازی فرایند انتقال بسته های اطلاعاتی از یک منبع به مقصد عمل مسیر یابی است که تحت عنوان ابزاری تحت عنوان مسیر یاب انجام می شود. مسیر یابی یک شاخصه کلیدی در اینترنت است زیرا که باعث می شود پیام ها از یک کامپیوتر به کامپیوتر دیگر منتقل شوند. این عملکرد شامل تجزیه وتحلیل مسیر برای یافتن بهترین مسیر است. مسیر یاب ابزاری است که شبکه های محلی را بهم متصل می کند یا به بیان بهتر بیش از دو شبکه را بهم متصل می کند.

مسیر یاب بر حسب عملکردش به دونوع زیر تقسیم می شود:

الف – مسیریاب ایستا : که در این نوع ، جدول مسیر یابی توسط مدیر شبکه که تعیین کننده مسیر می باشد بطور دستی مقدار دهی می شود.

ب – مسیر یاب پویا : که در این نوع ، جدول مسیر یابی خودش را، خود تنظیم می کند وبطور اتوماتیک جدول مسیریابی را روز آمد می کند.

۴ – دروازه ها Gateways:

دروازه ها در لایه کاربرد مدل ا اس ای عمل می کنند. کاربرد آن تبدیل یک پروتکل به پروتکل دیگر است. هر هنگام که در ساخت شبکه هدف استفاده از خدمات اینترنت است دروازه ها مقوله های مطرح در شبکه سازی خواهند بود.

پل ها Bridge:

یک پل برای اتصال سگمنت های یک شبکه " همگن " به یکدیگر مورد استفاده قرار می گیرد. یک پل در لایه پیوند داده ها " Data link" عمل می کند.

پل ها فریم ها را بر اساس آدرس مقصدشان ارسال می کنند. آنها همچنین می توانند جریان داده ها را کنترل نموده وخطاهایی را که در حین ارسال داده ها رخ می دهد.

عملکرد این پل عبارتست از تجزیه وتحلیل آدرس مقصد یک فریم ورودی واتخاذ تصمیم مناسب برای ارسال آن به ایستگاه مربوطه . پل ها قادر به فیلتر کردن فریم ها می باشند. فیلتر کردن فریم برای حذف فریم های عمومی یا همگانی که غیر ضروری هستند مفید می باشد، پل ها قابل برنامه ریزی هستند ومی توان آنها را به گونه ای برنامه ریزی کرد که فریم های ارسال شده از طرف منابع خاصی را حذف کنند.

با تقسیم یک شبکه بزرگ به چندین سگمنت واستفاده از یک پل برای اتصال آنها به یکدیگر ، توان عملیاتی شبکه افزایش خواهد یافت . اگر یک سگمنت شبکه از کار بیفتد ، سایر سگمنت ها ی متصل به پل می توانند شبکه را فعال نگه دارند ، پل ها موجب افزایش وسعت شبکه محلی می شوند.

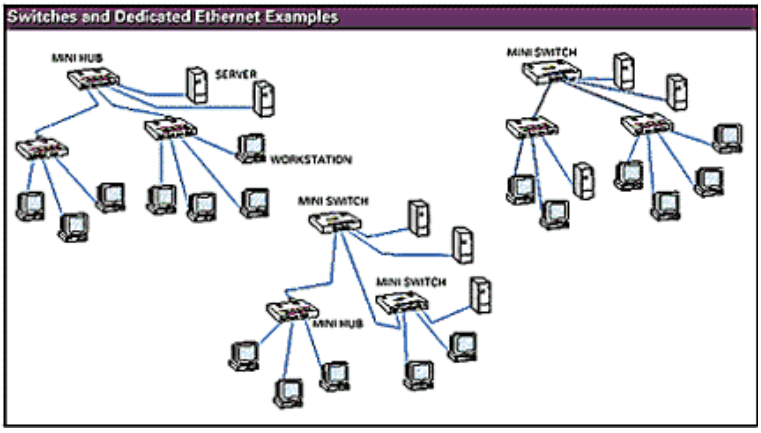
سوئیچ ها Switches:

سوئیچ نوع دیگری از ابزارهایی است که برای اتصال چند شبکه محلی به یکدیگر مورد استفاده قرار می گیرد که باعث افزایش توان عملیاتی شبکه می شود. سوئیچ وسیله ای است که دارای درگاه های متعدد است که بسته ها را از یک درگاه می پذیرد، آدرس مقصد را بررسی می کند وسپس بسته ها را به درگاه مورد نظر " که متعلق به

ایستگاه میزبان با همان آدرس مقصد می باشد" ارسال می کند. اغلب سوئیچ های شبکه محلی در لایه پیوند داده های مدل ا اس آی عمل می کند.

سوئیچ ها بر اساس کاربردشان به متقارن "Symmetric" ونامتقارن " Asymmetric" تقسیم می شوند.

در نوع متقارن ، عمل سوئیچینگ بین سگمنت هایی که دارای پهنای باند یکسان هستند انجام می دهد یعنی 10mbps به 10mbps و.... سوئیچ خواهد شد. اما در نوع نامتقارن این عملکرد بین سگمنت هایی با پهنای باند متفاوت انجام می شود.



دو نوع سوئیچ وجود دارد که عبارتند از :

۱ – سوئیچ Cut - through : این نوع سه یا چهار بایت اول یک بسته را می خواند تا آدرس مقصد آنرا بدست آورد ، آنگاه آن بسته را به سگمنت دارای آدرس مقصد مذکور ارسال می کند این در حالی است که قسمت باقی مانده بسته را از نظر خطایابی مورد بررسی قرار نمی دهد.

۲ – سوئیچ Store- and - forward : این نوع ابتدا کل بسته را ذخیره کرده سپس آن را خطایابی می کند ، اگر بسته ای دارای خطا بود آن بسته را حذف می کند ، در غیر اینصورت آن بسته را به مقصد مربوطه ارسال خواهد کرد. این نوع برای شبکه محلی بسیار مناسبتر از نوع اول است زیرا بسته های اطلاعاتی خراب شده را پاکسازی می کند و بهمین دلیل این سوئیچ باعث کاهش بروز عمل تصادف خواهد شد.

شبکه Fully Switched

در یک شبکه Fully Switched ، سوئیچ ها ، هاب های یک شبکه Ethernet را با یک سگمنت مختص به هر یک از نودها عوض می کند. این سگمنت ها به سوئیچی وصل می باشند که این سوئیچ چندین سگمنت مربوطه را ساپورت می کند. از آنجائیکه سوئیچ و نود تنها قطعات موجود در داخل یک سگمنت هستند. در نتیجه ، سوئیچ هر ارسالی را قبل از رسیدن به نود دیگر ، دریافت می کند و آن را از یک سگمنت مناسب عبور می دهد. از آنجائیکه هر سگمنت فقط یک نود را تحت پوشش قرار می دهد ، در نتیجه دامنه این ساختار به گیرنده مورد نظر ختم می شود. خصوصیت مذکور در یک شبکه سوئیچ دار این امکان را می دهد تا همزمان مکالمات متعددی تحقق یابد. سوئیچینگ ، امکان برقراری یک رابطه کاملا Full Duplex را در شبکه محقق میسازد. قبل از سوئیچینگ، شبکه به صورت half duplex می باشد. بدان معنا که دیتا فقط در یک مسیر می تواند ارسال شود اما در یک شبکه که از سوئیچ استفاده می کند ، در هر یک از نودها که فقط با سوئیچ در ارتباطند و هیچ ارتباطی مستقیمی بین نودها وجود ندارد. در نتیجه اطلاعات می تواند به صورت همزمان از نود به سوئیچ و از سوئیچ به نود ارسال شود یعنی ارتباط Full Duplex است.

در شبکه های کاملا سوئیچ شده از کابل های نوری Fiber ، optic و یا کابل های Twisted Pair استفاده می شود. در چنین محیطی ، نودها می توانند از فرایند تشخیص برخورد اطلاعات با یکدیگر صرف نظر کنند. از آنجائیکه نودها تنها قطعاتی هستند که به کابل یا مدیا دسترسی دارند در نتیجه می توانند از جستجو و آشکار کردن برخورد بسته های اطلاعاتی صرف نظر کنند و بسته ها را به هر جا که می خواهند ارسال کنند. این نوع جریان ترافیک به نودها اجازه می دهد تا اطلاعات را به سمت سوئیچ ارسال کنند همانطور که سوئیچ ها اطلاعات را به طرف نودها ارسال می کنند. این فرایند منجر به محیطی عادی از هر گونه برخورد اطلاعات با یکدیگر می شود. ارسال اطلاعات به صورت دو طرفه ، سرعت شبکه را به شکل موثرتر افزایش می دهد. اگر سرعت شبکه 10Mbps باشد در نتیجه هر یک از نودها اطلاعاتی را همزمان به همین سرعت ارسال می کنند.

شبکه های مختلط

اکثر شبکه ها صرفا فقط از سویچ در شبکه استفاده نمی کنند چون اگر سوئیچ بخواهد جایگزین تمام هاب های شبکه شود ، این کار به قیمت مناسبی تمام نمیشود. در عوض برای رسیدن به یک قیمت مناسب و سودآور ، از ترکیب سوئیچ و هاب استفاده می شود. به طور مثال یک شرکت ممکن است از هاب برای اتصال کامپیوترهای موجود در هر یک از دپارتمان ها استفاده کرده و برای اتصال هاب دپارتمان ها با یکدیگر از سوئیچ استفاده کند.

روتر و سوئیچ

همانطور که گفته شد یک سوئیچ می تواند در نحوه برقراری ارتباط بین نودها تغییر اساسی ایجاد کند. اما شما از وجه تمایز سوئیچ و روتر تعجب می کنید. سوئیچ ها معمولاً با استفاده از آدرس های MAC در لایه دوم مدل مرجع OSI که دیتا لینک است کار می کند در حالیکه روترها در لایه سوم یا Network با آدرس های مربوط به همین لایه مانند آدرس های لایه IP , IPX کار می کنند. مضاف بر این ، الگوریتم سوئیچ در هدایت بسته های اطلاعاتی با الگوریتم روترها متفاوت است. یکی از تفاوت های الگوریتم بین سوئیچ و روترها ، در نحوه دریافت اعلان همگانی (broadcast) می باشد. در هر شبکه ای ، ارسال بسته به تمام نودها (broadcast)یکی از ضروری ترین عواملی است که در نحوه کار شبکه دخالت دارد. هرگاه یکی از نودها بخواهد اطلاعاتی را ارسال کند و گیرنده آن را نشناسد ، در این صورت یک پکت اعلان همگانی یا Broadcast به تمامی نودها ارسال می کند. به طور مثال اگر کامپیوتر جدیدی وارد مجموعه نودهای شبکه شود در این صورت توسط یک پکت Broadcast حضور خود را به تمامی نودها اطلاع می دهد.

هاب ها و سوئیچ ها هر بسته اطلاعاتی اعلان همگان (Broadcast Packet) دریافت شده را به تمامی سگمنت های موجود در محدوده اعلان ارسال می کنند. حال آنکه روترها این گونه عمل نمی کنند. مجددا به مثال چهار راه توجه کنید. اهمیتی ندارد که ترافیک جاری در یک تقاطع ، به کدامین جهت در حرکت می باشد. اگر این تقاطع در یک سرحد بین المللی واقع شده باشد. برای عبور از این تقاطع شما می باید گارد مرزی را از آدرس خود مطلع سازید. اگر شما مقصد خود را مشخص نسازید ، گارد مانع از عبور شما می شود. روترها نیز در شبکه همانند گارد مرزی عمل می کنند ، اگر یک بسته اطلاعاتی آدرس مشخص از گیرنده را نداشته باشد. روتر از عبور دیتا جلوگیری می کند ، این باعث جداسازی شبکه ها از یکدیگر می شود. زمانیکه قسمت های مختلف در یک شبکه بخواهند با هم

صحبت کنند سوئیچ وارد عمل شده و اگر قرار باشد کامپوترها با خارج از شبکه داخلی صحبت کنند روتر وارد عمل می شود.

Packet-Switching

سوئیچ ها بر مبنای Packet-Switching کار می کنند و بین سگمنت هایی که از نظر بعد مکانی از هم به حد کافی دور می باشند ، ارتباط برقرار می سازد. بسته های اطلاعاتی وارده در buffer نگهداری می شوند. آدرس های MAC در قسمت هدر فریم نگهداری می شوند. آدرس های مذکور که در این قسمت قرار دارد ، خوانده می شوند و با جدول مک سوئیچ (MAC Table) مقایسه می گردند. همچنین فریم اترنت در یک شبکه LAN قسمتی به نام Payload دارد. که شامل MAC Address مبدا و مقصد می باشد. همانطور که قبلا گفته شد سوئیچ آدرس مک مبدا و مقصد را چک کرده و در صورتیکه آدرس مقصد را در جدول مک آدرس های خود داشت برای مقصد ارسال می کند.

سوئیچ های Packet-based برای تعیین مسیر ترافیک از یکی از سه روش زیر استفاده می کند:

Cut-through

Store-and-forward

Fragment-free

Cut-through : در این روش ، سوئیچ آدرس های MAC را به محض دریافت بسته می خواند و سپس ۶ بایت MAC اطلاعات مربوط به آدرس را ذخیره کرده و با وجود اینکه ما بقی بسته ها در حال رسیدن به سوئیچ می باشند ، اقدام به ارسال بسته مذکور به سمت نود مقصد می نماید.

Store-and-forward : سوئیچی که از این روش استفاده می کند ، ابتدا تمام اطلاعات داخل بسته را دریافت و نگهداری می کند و قبل از ارسال بسته مورد نظر به دنبال خطای CRC و یا مشکلات دیگر می گردد. در صورتی که بسته دارای خطایی باشد آن بسته را کنار می گذارد. در غیر اینصورت سوئیچ آدرس کارت شبکه گیرنده را جستجو کرده و سپس آن را برای نود مقصد ارسال می دارد. بیشتر سوئیچ ها همزمان از دو روش فوق استفاده می کنند مثلاً ابتدا از روش Cut-through استفاده کرده ولی به محض برخورد با یک خطا ، روش خود را تغییر می دهد و به شیوه Store-and-forward عمل می کند ، از آنجائیکه روش Cut-through قادر به اصلاح خطا نمی باشد در نتیجه سوئیچ های کمتری از این روش استفاده می کنند ولی از سرعت بالاتری برخوردار است.

Fragment-free : سوئیچ ها از این روش کمتر استفاده می کنند. این روش مانند روش اول می باشد با این تفاوت که در این شیوه ، سوئیچ قبل از ارسال بسته ، ۶۴ بایت اول آن را نگه می دارد این کار به خاطر آن است که بیشتر خطا و برخوردها در طول اولین ۶۴ بایت بسته اطلاعاتی اتفاق می افتد.

Switch Configurations

سوئیچ های LAN از نظر شکل فیزیکی با هم متفاوتند ، در حال حاضر ، سوئیچ ها دارای سه شکل عمده می باشند :

Shared memory : این نوع از سوئیچ ها ، بسته رسیده را در یک حافظه مشترک یا بافر که این بافر در بین تمامی درگاه های سوئیچ تقسیم می شود نگهداری می کنند و سپس پکت را از طریق درگاه مناسب برای سمت نود مقصد ارسال می کنند.

Matrix : این نوع سوئیچ ها دارای یک شبکه خطوط داخلی (ماتریکس) با پورت های ورودی و خروجی می باشند. زمانیکه وجود یک بسته اطلاعاتی در پورت ورودی تشخیص داده شود ، آدرس کارت شبکه (MAC) با جدول

جستجوی موجود در سوئیچ (MAC Table) مقایسه می شود تا در نهایت بسته مذکور به پورت خروجی مورد نظر هدایت شود. بنابراین سوئیچ در حد فاصل بین این دو پورت یک خط ارتباطی ایجاد کرده و آن دو پورت را به هم متصل می کند.

Bus architecture : در این دسته از سوئیچ ها یک بافر برای هر یک از درگاه ها در نظر گرفته شده است. که گذرگاه اطلاعات را کنترل می کند.

Transparent Bridging

اکثر سوئیچ ها از سیستمی موسوم به transparent bridgingاستفاده می کنند تا جداولی جهت جستجوی آدرس بسازند. سیستم مذکور یک تکنولوژی می باشد که امکان می دهد تا سوئیچ همه آنچه که در مورد موقعیت نودها در شبکه باید بداند را بدون دخالت مدیر شبکه (network administrator) می آموزند.

این سیستم دارای پنج قسمت زیر می باشد :

Learning

Flooding

Filtering

Forwarding

Aging

Learning : کامپیوتر Aکه در سگمنت A قرار دارد ، دیتایی برای کامپیوتر B واقع در سگمنت C ارسال می کند. پس سوئیچ اولین بسته اطلاعاتی را از روی نود A دریافت می کند. آدرس کارت شبکه یا MAC

Addressآن را می خواند و آن را در جدول مک خود به ثبت می رساند. از این پس سوئیچ به محض دریافت یک بسته اطلاعاتی که آدرس مقصد دستگاه ، نود A آدرس دهی شده باشد می تواند نود A را با توجه به آدرس موجود بیاید. به این عملیات Learning می گویند. یعنی به محض دیدن یک MAC Address جدید سوئیچ آن را یادداشت می کند و آن را یاد می گیرد.

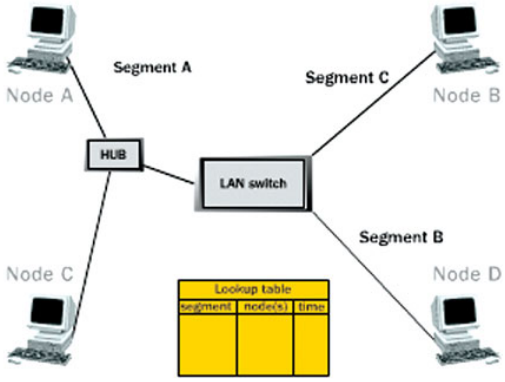
Flooding : با توجه به اینکه سوئیچ ، مک آدرس نود B را نمی شناسد ، بسته را به تمامی سگمنت ها به استثنای سگمنت A می فرستد. هرگاه سوئیچ برای یافتن یک نود مشخص بسته را به تمامی سگمنت ها بفرستد در اصطلاح به این عمل Flooding می گویند.

Forwarding نود B بسته را دریافت کرده و بسته ای را برای شناسایی به سمت نود A می فرستد. بسته ارسالی از سوی نود B به سوئیچ می رسد و سوئیچ نیز آدرس کارت شبکه نود B را به لیست MAC Table خود در سگمنت C اضافه می کند. از آنجائیکه سوئیچ ، آدرس نود A را از قبل می داند در نتیجه بسته را مستقیماً به نود A می فرستد. چون سگمنتی که نود Aمتعلق به آن است با سگمنتی که نود B به آن تعلق دارد با هم متفاوت می باشند. در نتیجه سوئیچ می باید این دو سگمنت را به هم مربوط سازد و سپس اقدام به ارسال بسته نماید که به این عمل Forwarding می گویند. بسته دیگری از سوی نود A به سمت نود B ارسال می گردد، بسته ابتدا به سوئیچ می رسد، سوئیچ نیز آدرس نود B را می داند و بسته را مستقیماً به نود B می فرستد.

Filtering : نود C اطلاعاتی را برای نود A می فرستد. آدرس نود C به سوئیچ نیز از طریق HUB ، ارسال می شود و سوئیچ آدرس نود C را نیز به لیست آدرس های خود در سگمنت A اضافه می کند. پیش از این ، سوئیچ آدرس مربوط به نود A را می دانست و مشخص می سازد که این نودها (A و C) هر دو در یک سگمنت مشابه

قرار دارند ، پس برای ارسال اطلاعات از نود C به نود Aدیگر نیازی نیست تا سوئیچ سگمنتA را با سگمنت دیگری مرتبط سازد. بنابراین سوئیچ در حین انتقال اطلاعات بین نودهای درون یک سگمنت عکس العملی از خود نشان نمی دهد که به این عمل Filtering می گویند.

مراحل Learning و Flooding ادامه می یابد تا اینکه سوئیچ مک آدرس تمامی نودها را به لیست خود اضافه کند. بیشتر سوئیچ ها برای نگهداری لیست آدرس ها از حافظه زیادی برخورد دارند. اما برای استفاده بهتر از این حافظه سوئیچ آدرس های قدیمی را از جدول پاک می کند و برای جلوگیری از اتلاف وقت در آدرس های قدیمی به دنبال آدرسی نمی گردد. برای انجام این کار از تکنیکی موسوم به aging بهره می گیرد. اساساً وقتی اطلاعات یک نود وارد جدول سوئیچ می شود یک Timestamp در مقابل آن اطلاعات نوشته می شود و با دریافت هر بسته اطلاعاتی دیگر ، آن بر چسب زمان (Timestamp) به روز می شود. سوئیچ دارای قابلیتی است که پس از مدتی در صورت عدم فعالیت نود ، اطلاعات مربوط به آن را پاک می کند. این قابلیت باعث میشود تا فضای قابل توجهی از حافظه برای اطلاعات و پکت های دیگر اختصاص داده شود. در نمونه ای که ملاحظه کردید، دو نود (A و C) یک سگمنت را بین خود تقسیم می کنند حال آنکه سوئیچ برای هر یک از نودهای B و D یک سگمنت مستقل میسازد. در یک شبکه ایده آل LAN-Switched هر یک از نودها دارای یک سگمنت جداگانه می باشد که خصیصه مذکور ، احتمال برخورد بین بسته های اطلاعاتی و همچنین نیاز به فیلترینگ را حذف می کند.



Spanning Trees

برای جلوگیری از وقوع طوفان هایی موسوم به Broadcast Storms و همچنین جوانب ناخواسته دیگری که در اثر اتصال حلقه ای سوئیچ ها بوجود می آیند، شرکت Digital Equipment Corporation پروتکلی با نام Spanning-tree Protocol یا STP ساخته است که موسسه IEEE نیز آن پروتکل را با استاندارد 802.id معرفی کرده است .اساساً پروتکل مذکور از یک الگوریتم موسوم به Spanning- tree Algorithm (STA)استفاده می کند. الگوریتم مذکور قادر است تا در بین چندین مسیر منتهی به نود مورد نظر ، بهترین راه را تشخیص داده و مسیر های دیگر که ایجاد حلقه می کند را مسدود می سازد.

روتر و سوییچ های لایه ۳(Router and Layer 3 Switching)

برخی از سوئیچ ها در لایه دوم شبکه یا Data Layer کار می کنند. با افزون روترها به این مجموعه می توانند در لایه سوم شبکه یا Network layer نیز کار کنند. در واقع سوییچ لایه سوم کاملا شبیه روتر است. روتر به محض دریافت پکت اطلاعات به آدرس های مبدا و مقصد نگاهی می اندازد تا مسیری را که بسته می باید طی کند را بیابد. یک سوئیچ استاندارد بر مبنای آدرس های MAC ، مبدا و مقصد بسته را شناسایی می کند.

تفاوت اساسی بین یک روتر و سوئیچ لایه ۳ این است که سوئیچ لایه سوم با همان سرعت سوئیچ لایه دوم کار می کند و برای انتقال دیتا از یک قطعه سخت افزاری استفاده می کند همچنین آنها به مانند روترها در مورد نحوه هدایت ترافیک به لایه سوم تصمیم می گیرند. در داخل یک شبکه LAN سوئیچ های لایه سوم معمولاً سریعتر از روترها کار می کنند زیرا بر مبنای سوئیچینگ سخت افزاری ساخته شده اند. در واقع بیشتر سوئیچ های لایه سوم Ciscoروترهایی می باشند که دارای سوئیچینگ سخت افزاری بوده و در داخل این قطعه سخت افزاری ، تعدادی تراشه وجود دارد که بر حسب نیاز انتخاب می شوند که در مجموع موجب افزایش سرعت این روترها می گردند. نحوه ترکیب و مختص بودن سوئیچ های لایه سوم همانند الگویی است که در روترها دیده می شود. هر دوی آنها از پروتکل ها و جداول مسیریابی (Routing Table) استفاده می کنند تا بهترین مسیر را بیابند. هر چند سوئیچ های لایه سوم قادرند تا به صورت فعالی با استفاده از اطلاعات مسیریابی لایه سوم برای سخت افزار برنامه ریزی کنند که در نهایت منجر به هدایت سریع بسته های اطلاعاتی می گردد.در سوئیچ های لایه سوم کنونی ، اطلاعات بدست آمده از پروتکل های جهت یابی برای روز آمد کردن جداول سخت افزاری استفاده می شوند.

VLAN

با رشد شبکه ها از نظر اندازه و پیچیدگی ، بیشتر شرکت ها به سمت شبکه های محلی مجازی Virtual local Area Network یاVLANS گرایش یافته اند. اساساً یک شبکه مجازی مجموعه ای است از نودهایی که در یک Broadcast Domain قرار دارند. قبلاً در مورد broadcast و همچنین نحوه ممانعت روترها از عبورbroadcast ها مطالبی گفته شد .

در این قسمت با دلایل استفاده از VLAN آشنا می شویم:

Security : سیستم هایی که دارای اطلاعات حساس بوده از سایر قسمت های شبکه جدا می شوند که این پارامتر باعث می شود تا از احتمال دسترسی مردم به اطلاعاتی که مجاز به دیدن آنها نیستند، می کاهد.

Projects / Special application : یک شبکه محلی مجازی با جمع آوری نودهای مورد نیاز در کنار هم می تواند به انجام پروژه و یا کار کردن با یک برنامه ویژه را آسانتر کند.

Performance / Bandwidth : مدیر شبکه با بررسی دقیق کار شبکه ، درصدد بر می آید تا شبکه های VLAN را بسازد و بر میزان عرض باند شبکه می افزاید.

Broadcast / Traffic flow : اساسی ترین فاکتور این شبکه ها این است که از انتشار بسته های اطلاعاتی به سمت نودهایی که جزئی از این شبکه نمی باشند جلوگیری کند. این کار منجر به کاهش Broadcast می شود. همچنین دارای Access lists می باشند، که به کنترل نوع ترافیک توسط مدیر شبکه کمک می کند.

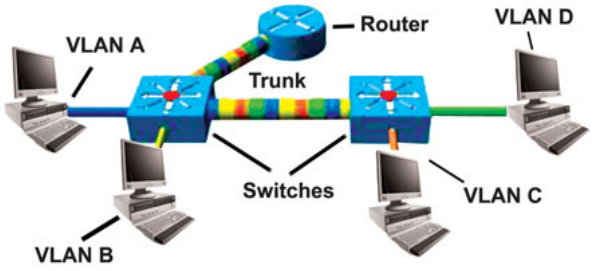
Department / Specific Job types : امکان دارد شرکت ها بخواهند شبکه خود را بر حسب نیاز دپارتمان هایی که کاربران آن قسمت ها از شبکه در زمینه پروژه های سنگین استفاده می کنند و یا دپارتمان های که به کارمندان خاصی اختصاص دارند مانند کارمندان فروش و مدیران طراحی کنند. با استفاده از تعدادی سوئیچ و اتصال به سوئیچ از طریق Telnet به راحتی می توان یک شبکه VLAN را طراحی کرد. بعد از ساخت شبکه مجازی هر یک از سگمنت هایی را که به درگاه های معین وصل می شوند جزئی از این شبکه مجازی می گردند. مادامی که در یک سوئیچ چندین شبکه VLAN داشته باشیم، این شبکه ها نمی توانند به صورت مستقیم با شبکه دیگری که به آن سوئیچ متصل می باشد ارتباط برقرار کنند. در غیر این صورت می توانست

منجر به عدم استفاده از شبکه های مجازی شود البته برای برقراری ارتباط ما بین چندین VLAN به وجود روتر نیاز است.

شبکه های VLAN می توانند از چندین سوئیچ برای برقراری ارتباط استفاده کنند و همچننی چندین شبکه مجازی VLAN می توانند به یک سوئیچ متصل شوند شبکه های مختلفی که به سوئیچ های مختلفی متصل می باشند قادرند تا از طریق لینک ما بین سوئیچ ها با هم ارتباط برقرار کنند. برای تحقق آن از پروتکل موسوم به Trunking بهره می گیرند. پروتکل مذکور تکنولوژیی می باشد که به اطلاعات این امکان را می دهد تا از بین چندین شبکه VLAN و از طریق لینک سوئیچ ها عبور کنند.

پروتکلVLAN Trunking

پروتکل VTP پروتکلی است که سوئیچ ها از آن برای اطلاع رسانی به یکدیگر در مورد ترکیبVLAN ها استفاده می کنند. همانطور که در شکل ۴ مشاهده می کنید هر یک از سوئیچ ها دارای ۲ عدد شبکه مجازی VLAN می باشد، به اولین سوئیچ ، شبکه های A و B که از طریق پورت هایی به روتر و سوئیچ دیگر مرتبط می شوند. شبکه های C و D نیز از طریق سوئیچ دوم به سوئیچ اول وصل می شود و همچنین این شبکه ها می توانند از طریق سوئیچ اول به روتر مرتبط می شوند. شبکه های مجازی از طریق خطوط ارتباطی Trunk موجود در بین سوئیچ ها و با استفاده از روترها ، قادرند با یکدیگر ارتباط برقرار کنند به طور مثال دیتا از کامپیوتر واقع در VLAN (A) به سرعت برای کامپیوتر دیگر مثلا کامپیوتر موجود در VLAN (B) ارسال می شود. این اطلاعات می باید از سوئیچ به طرف روتر رفته و از آنجا نیز دوباره به سوئیچ باز گردد. اما به وسیله الگوریتم transparent bridging algorithmو همچنین پروتکلTrunking، هر دوی کامپیوترها و روتر می دانند که آنها در داخل یک سگمنت مشابه می باشند.

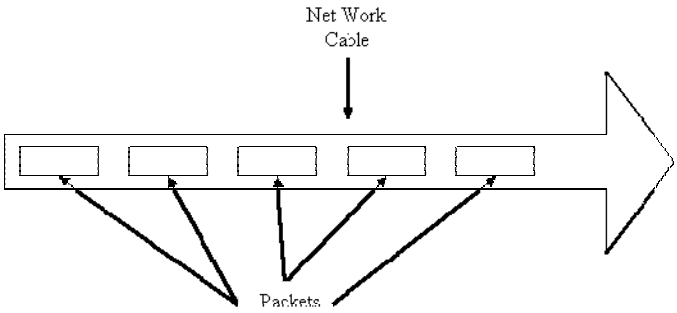


در هرحال باید توجه داشت که هاب ، سوئیچ و روتر هرکدام به منظور خاصی استفاده شده و استفاده آنها در شبکه به پارامترهای بسیاری که در طراحی شبکه مد نظر قرار می گیرد بستگی دارد.

مفاهیم مربوط به ارسال سیگنال و پهنای باند

پهنای باند (Bandwidth) به تفاوت بین بالاترین و پایین‌ترین فرکانسهایی که یک سیستم ارتباطی می‌تواند ارسال کند گفته می‌شود. به عبارت دیگر منظور از پهنای باند مقدار اطلاعاتی است که می‌تواند در یک مدت زمان معین ارسال شود. برای وسایل دیجیتال، پهنای باند برحسب بیت در ثانیه و یا بایت در ثانیه بیان می‌شود. برای وسایل آنالوگ، پهنای باند، برحسب سیکل در ثانیه بیان می‌شود. دو روش برای ارسال اطلاعات از طریق رسانه‌های انتقالی وجود دارد که عبارتند از: روش ارسال باند پایه (Baseband) و روش ارسال باند پهن (Broadband) در یک شبکه LAN، کابلی که کامپیوترها را به هم وصل می‌کند، فقط می‌تواند در یک زمان یک سیگنال را از خود عبور دهد، به این شبکه یک شبکه Baseband می‌گوئیم. به منظور عملی ساختن این روش و امکان استفاده از آن برای همه کامپیوترها، داده‌ای که توسط هر سیستم انتقال می‌یابد، به واحدهای جداگانه‌ای به نام Packet شکسته می‌شود. در واقع در کابل یک شبکه LAN، توالی Packetهای تولید

شده توسط سیستم‌های مختلف را شاهد هستیم که به سوی مقاصد گوناگونی در حرکت‌اند.شکلی که در ادامه خواهد آمد، این مفهوم را بهتر نشان می‌دهد.



عملکرد یک شبکه packet-switching

برای مثال وقتی کامپیوتر شما یک پیام پست الکترونیکی را انتقال می‌دهد، این پیام به Packetهای متعددی شکسته می‌شود و کامپیوتر هر Packet را جداگانه انتقال می‌دهد. کامپیوتر دیگری در شبکه که بخواهد به انتقال داده بپردازد نیز در یک زمان یک Packet را ارسال می‌کند. وقتی تمام Packetهایی که بر روی هم یک انتقال خاص را تشکیل می‌دهند، به مقصد خود می‌رسند، کامپیوتر دریافت کننده آنها را به شکل پیام الکترونیکی اولیه بر روی هم می‌چینند. این روش پایه و اساس شبکه‌های Packet-Switching می‌باشد.

در مقابل روش Baseband، روش Broadband قرار دارد. در روش اخیر، در یک زمان و در یک کابل، چندین سیگنال حمل می‌شوند. از مثالهای شبکه Broadband که ما هر روز از آن استفاده می‌کنیم، شبکه تلویزیون است. در این حالت فقط یک کابل به منزل کاربران کشیده می‌شود، اما همان یک کابل، سیگنالهای مربوط به کانالهای متعدد تلویزیون را بطور همزمان حمل می‌نماید. از روش Broadband به طور روز افزونی در شبکه‌های WAN استفاده می‌شود.

از آنجائیکه در شبکه‌های LAN در یک زمان از یک سیگنال پشتیبانی می‌شود، در یک لحظه داده‌ها تنها در یک جهت حرکت می‌کنند. به این ارتباط half-duplex گفته می‌شود. در مقابل به سیستم‌هایی که می‌توانند بطور همزمان در دو جهت با هم ارتباط برقرار کننده full-duplex گفته می‌شود. مثالی از این نوع ارتباط شبکه تلفن می‌باشد. شبکه‌های LAN با داشتن تجهیزاتی خاص بصورت full-duplex عمل کنند.

کابل شبکه

پیش از اینکه در مورد انواع کابل‌ها و پهنای باند مربوط به آنها، به بحث بپردازیم، ذکر این نکته ضروری است که نوع کابل انتخابی شما بطور مستقیم به توپولوژی شبکه تان وابسته است. در این قسمت سعی گردیده توپولوژی مناسب با هر نوع کابل ذکر شود.

کابل شبکه، رسانه ای است که از طریق آن، اطلاعات از یک 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 یک 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 یک شبکه موفق ضروری است.

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

1- Coaxial Thin net

Thick net

2- Twisted Pair UTP

STP

3- Fiber Optic Single Mode

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:

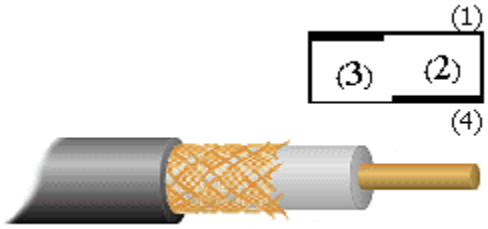
۱- قیمت ارزان آن.

۲- سبکی و انعطاف‌پذیری.

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

۴- مسافت بیشتری را بین دستگاههای موجود در شبکه، نسبت به کابل UTP پشتیبانی می‌نماید.

در شکل زیر ساختار کابل Coaxial مشاهده می‌شود:



(۱) Conducting Core یا هسته مرکزی که معمولاً از یک 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 پلاستیک بوده و نگهدارنده خارجی سیم در برابر خطرات فیزیکی است.

کابل Coaxial به دو دسته تقسیم می‌شود:

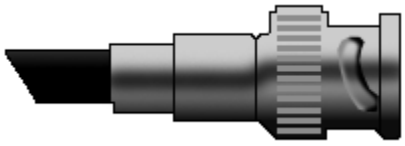
۱- Thin net: کابلی است بسیار سبک، انعطاف‌پذیر و ارزان قیمت، قطر سیم در آن ۶ میلیمتر معادل ۰/۲۵ اینچ است. مقدار مسیری که توسط آن پشتیبانی می‌شود ۱۸۵ متر است.

۲- Thick net: این کابل قطری تقریباً ۲ برابر Thin net دارد. کابل مذکور، پوشش محافظی را(علاوه بر محافظ خود) داراست که از جنس پلاستیک بوده و بخار را از هسته مرکزی دور می‌سازد.رایج‌ترین نوع اتصال دهنده (connector) مورد استفاده در کابل coaxial، (BNC)Bayonet-Neill-Concelman می‌باشد.

انواع مختلفی از سازگار کننده‌ها برایBNCها وجود دارند

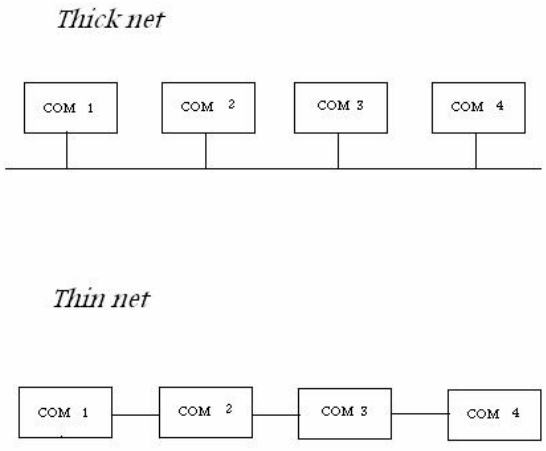
شامل:Tconnector , Barrel connector وTerminator.

تصویر زیر یک BNC connector را نشان می دهد:



BNC connector

در شبکه هایی با توپولوژی اتوبوسی از کابلcoaxial استفاده می‌شود. شکل زیر نمونه استفاده از این نوع کابل در شبکه اتوبوسی است:



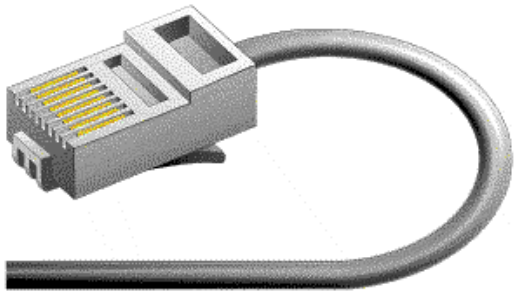
استفاده از کابل coaxial در شبکه اتوبوسی

باید دانست که از عبارتهایی مانند "Base5 " 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 "10Base2" 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:

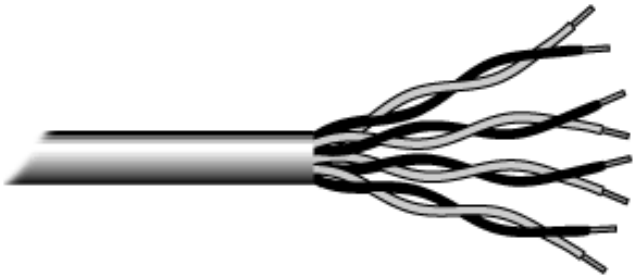
۱-(UTP(Unshielded Twisted Pair: کابل ارزان قیمتی است که نصب آسانی دارد و برای شبکه‌های LAN سیم بسیار مناسبی است، همچنین نسبت به نوع دوم کم‌وزن‌تر و انعطاف‌پذیرتر است. مقدار سرعت دیتای عبوری از آن ۴ مگابیت در ثانیه تا ۱۰۰ مگابیت در ثانیه می‌باشد. این کابل می‌تواند تا مسافت حدوداً ۱۰۰ متر یا ۳۲۸ فوت را بدون افت سیگنال انتقال دهد. کابل مذکور نسبت به تداخل امواج الکترومغناطیس (Electrical Magnatic Interference) 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 RJ11 استفاده می‌شود، اما در کابل شبکه اتصال دهنده‌ای با شماره RJ45 بکار می‌رود که دارای هشت مکان برای هشت رشته سیم است. در شکل زیر یک connector RJ45 دیده می‌شود.



connector RJ45

کابل UTP دارای پنج طبقه مختلف است (که البته امروزه CAT6 و CAT7 هم اضافه شده است):

۱- CAT1 یا نوع اول کابل UTP برای انتقال صدا بکار می‌رود، اما CAT2تا CAT5 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 کوچک و خانگی استفاده از کابل CAT3توصیه می‌شود.



کابل UTP

۲- STP(Shielded Twisted Pair) : 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 (Fast Ethernet) دو نوع کابل به چشم می‌خورد:

- 100Base TX: یعنی شبکه‌ای که در آن از کابل UTP نوع Cat5 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.

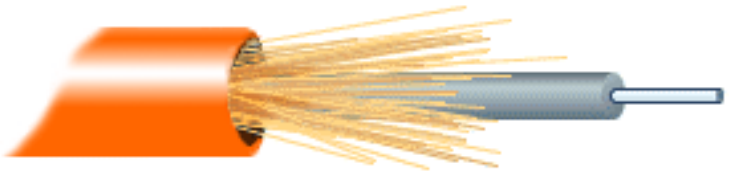
- 100Base T4: تنها تفاوت آن با نوع بالا این است که هر چهار جفت سیم در آن بکار گرفته می‌شوند.

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 پلاستیک 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:

۱- Single Mode: که دراین کابل دیتا با کمک لیزر انتقال می‌یابد و بصورت ۱۲۵/۸.۳ 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- Mode Multi: که در آن دیتا بصورت پالس نوری انتقال می‌یابد و بصورت ۱۲۵/۶۲.۵ 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

100Base FX، شبکه‌هایی 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. در شکل صفحه بعد یک کابل فیبر نوری مشاهده می‌شود.



فیبر نوری

بطور کلی توصیه‌هایی در مورد نصب کابل شبکه وجود دارد:

- همیشه بیشتر از مقدار مورد نیاز کابل تهیه کنید.
- هر بخشی از شبکه را که نصب می‌کنید، آزمایش نمایید. ممکن است بخشهایی در شبکه وجود داشته باشند که خارج ساختن آنها پس از مدتی دشوار باشد.
- اگر لازم است بر روی زمین کابل‌کشی نمایید، کابلها را بوسیله حفاظت‌کننده‌هایی بپوشانید.
- دو سر کابل را نشانه‌گذاری کنید.

دستگاه تست کابل شبکه

همانگونه که می دانید یکی از مهمترین و پیچیده ترین شاخه های دانش کامپیوتر ، بخش شبکه های کامپیوتری می باشد. در این بخش دستگاه های بسیار گوناگونی به کار میرود. یکی از اصلی ترین آنها انواع آزمون کننده های شبکه یا Network testers میباشند. با توجه به پیچیدگی و گستردگی کار در شبکه ها عیب یابی ، کارشناسی و

بررسی آنها مستلزم صرف هزینه و وقت زیادی است. البته باید گفت در برخی موارد که شبکه دارای پیچیدگی باشد یافتن و رفع ایراد بدون مجهز بودن به دستگاه های تستر ، ناممکن می باشد. بویژه اگر به طراح و مجری شبکه نیز دسترسی نباشد .

برای نمونه فرض کنید در ساختمانی ۴ طبقه در هر طبقه ۲۴ گره یا Node شبکه وجود داشته باشد. کابل ها درون کانال های ویژه دیوارها کار گذاری شده اند و حدود ۲۵۰۰ متر کابل مصرف شده است. پس از اتصال رایانه ها به شبکه برخی از آنها به شبکه داخل Login نمی شوند. حتی تصور آن که باید چنین شبکه ای را (که تازه دارای مقیاسی خیلی بزرگی هم نمی باشد.) بدون تستر مورد بررسی قرار داد و پس از عیب یابی به رفع آن اقدام نمود سر را گیج می کند!! اینجاست که اهمیت فوق العاده دستگاه های عیب یاب و تستر شبکه ارزشمندی کار آنان نمایان می گردد.

دستگاه LAN Smart یک تستر دستی کابل چند کاره دیجیتالی با فناوری بسیار پیشرفته می باشد. این وسیله بسیار سودمند علاوه بر عیب یابی ساده اتصالات سیم ها در شبکه نظیر اتصال باز یا کوتاه (Short / Open) ، زوج سیم های از هم جدا شده یا اشتباه بسته شده و غیره را می تواند بصورت بلادرنگ (real time) و با استفاده از فن آوری Time Domain Reflectometers - TDR (بازتاب سنج دامنه زمان) طول یک کابل را نیز محاسبه کرده و ارائه دهد.

نتایج ارائه شده توسط این وسیله بصورت پایه به پایه (pin to pin format) می باشد.

اگر هرگونه ایراد اتصال Short یاOpen درکابل باشد ، LAN Smart آن را پیدا کرده ، مکان یابی نموده و نتیجه را نشان خواهد داد. این وسیله همچنین قادر به ارسال علائم و سیگنال های صوتی است تا بوسیله آن بتوان کابل های نظیر و مشابه را پیدا نمود.

کاربران نیز می توانند با ارسال علائم خودکار auto negation signals پورت های (Ports) نظیر در هاب hub یا سوئیچ را پیدا کنند. به بیان دیگر این وسیله در برگیرنده یک مولد صدا و یک پورت یاب خودکار است که نتایج کار خود را در یک نمایشگر LCD و بصورت پایه به پایه نمایش می دهد. فنوری پیشرفته این وسیله موجب دقت بسیار زیادی در برآورد طول کابل ها و مکان یابی اشکالات حتی در انتهای کابل می گردد . این دستگاه بسیار مناسب و اقتصادی است. کارکرد با آن بسیار ساده می باشد. کارایی ها گوناگون و پیشرفته آن ، دستگاه مزبور را تبدیل به تستری مناسب برای کارشناسان و نصابان حرفه ای شبکه کرده است.

برخی ویژگی های بر جسته آن بصورت فهرست وار عبارتند از:

- دارای فن آوری TDR یا همان بازتاب سنج دامنه زمان می باشد. بوسیله این فناوری می توان با اتصال دستگاه تنها به یک سر کابل ، طول آن را اندازه گرفت.
- اتصال های کوتاه ، باز ، زوج سیم های اشتباه و وارونه بسته شده یا جدا شده از هم و نیز وضعیت پوسته و شیلد Shield کابل را بررسی می کند.
- با فنا وری پورت یاب PORT Finder می تواند سوکت های متناظر را بر روی هاب یا سوئیچ مکان یابی نماید.
- طول کابل های STP و UTP را اندازه گیری می کند.

- (Velocity of Propagation Adjustable Calibrate) دارای قابلیت تنظیم سرعت پخش سنجش و کالیبراسیون برای کابل های غیر استاندارد می باشد تا بوسیله آن دقت اندازه گیری افزایش پیدا کند.
- واحد اندازه گیری آن متر و فوت می باشد.
- مولد صدای آن بر روی کلیه پایه های اتصال و نیز تک تک آنها عمل می کند.
- نتایج آزمون بصورت یک نقشه بر روی تک تک پایه های سیم نشان داده میشود.
- سازگار با کلیه سیم های زوج به هم تابیده از نوع CAT3 , 4 , 5 , 6 میباشد.

طول کابل های توده ای و انباشته را نیز اندازه گیری می کند.

کارت شبکه (Adapter Network Interface)

کارت شبکه یا NIC ، وقتی که در شیار گسترش کامپیوتر(slot expansion: سوکتی در یک کامپیوتر که برای نگهداری بوردهای گسترش و اتصال آنها به باس سیستم (مسیر انتقال داده‌ها) طراحی می‌شود. شیارهای گسترش روشی برای افزایش یا بهبود ویژگیها و قابلیت‌های کامپیوتر هستند) قرار می‌گیرد، وسیله‌ای است که بین کامپیوتر و شبکه‌ای که کامپیوتر جزئی از آن است، اتصال برقرار می‌نماید. هر کامپیوتر در شبکه می‌بایست یک کارت شبکه داشته باشد که به باس گسترش سیستم (Expansion Bus System's) اتصال می‌یابد و برای رسانه شبکه (کابل شبکه) به عنوان یک واسطه عمل می‌کند. در برخی کامپیوترها، کارت شبکه با مادربورد یکی شده است، اما در بیشتر مواقع شکل یک کارت گسترش (Expansion Card) را به خود می‌گیرد که یا به ISA سیستم

Industry Standard Architecture: مجموعه مشخصاتی برای طراحی باس‌ها که امکان می‌دهد قطعات بصورت کارت به شیارهای گسترش استاندارد کامپیوترهای شخصی آی‌بی‌ام و سازگار با آنها افزوده شوند، و یا به PCI (Peripheral Component Interconnect): مجموعه مشخصاتی که توسط شرکت اینتل ارائه شده و سیستم باس محلی را تعریف می‌کند که امکان نصب حداکثر ۱۰ کارت گسترش سازگار با PCI را فراهم می‌کند) متصل می‌گردد.

کارت شبکه به همراه نرم‌افزار راه اندازی (device driver) آن، مسئول اکثر کارکردهای لایه data-link و لایه فیزیکی می‌باشد. کارت‌های شبکه، بسته به نوع کابلی که پشتیبانی می‌کنند، اتصال دهنده‌های (Connectors) خاصی را می‌طلبند. (کابل شبکه از طریق یک اتصال دهنده به کارت شبکه وصل می‌شود) برخی کارت‌های شبکه بیش از یک نوع اتصال دهنده دارند که این شما را قادر می‌سازد که آنها را به انواع مختلفی از کابلهای شبکه اتصال دهید.

عملکردهای اساسی کارت شبکه

کارت شبکه عملکردهای گوناگونی را که برای دریافت و ارسال داده‌ها در شبکه حیاتی هستند، انجام می‌دهد که برخی از آنها عبارتند از:

۱- Data encapsulation: کارت شبکه و درایور (راه‌انداز) آن، مسئول ایجاد فریم در اطراف داده تولید شده توسط لایهٔ شبکه و آماده‌سازی آن برای انتقال هستند.

۲- Signal encoding and decoding: در واقع کارت شبکه طرح کدگذاری لایه فیزیکی را پیاده می‌کند و داده‌های دودویی (binary) تولید شده توسط لایه شبکه را به سیگنال‌های الکتریکی قابل انتقال بر روی

کابل شبکه تبدیل می‌نماید. همچنین سیگنال‌های دریافتی از روی کابل را برای استفاده لایه‌های بالاتر به داده‌های دودویی تبدیل می‌سازد.

۳- Data transmission and reception: کارکرد اساسی کارت شبکه، تولید و انتقال سیگنال‌های متناسب در شبکه و دریافت سیگنال‌های ورودی است. طبیعت سیگنال‌ها به کابل شبکه و پروتکل لایه datalink بستگی دارد. در یک LAN فرضی، هر کامپیوتر هم بسته‌های عبوری در شبکه را دریافت می‌کند و کارت شبکه آدرس مقصد لایه datalink را بررسی می‌کند تا ببیند آیا بسته برای کامپیوتر مذکور فرستاده شده یا خیر. در صورت مثبت بودن پاسخ، کارت شبکه بسته را برای انجام پردازش توسط لایه بعدی از کامپیوتر عبور می‌دهد، در غیر اینصورت بسته را به دور می‌افکند.

کارت شبکه قابل نقل و انتقال (Network Computer Portable Adapters) بسیار احتمال دارد که در شبکه شما یک کامپیوتر کیفی و قابل حمل وجود داشته باشد. گستره وسیعی از کارت شبکه‌های مناسب این کامپیوترها قابل دستیابی است. نوعی از کارت شبکه که در کامپیوترهای کیفی استفاده می‌شود عبارتست از: کارت PCMCIA یا همان PC Card.

کارت PC در یک شیار و یا در یک جفت شیار موجود در کناره کامپیوتر کیفی جای می‌گیرد. کابل شبکه با استفاده از ابزاری به نام "dongle" به کارت PC متصل می‌شود. کارتهای PC جز ابزارهای "Plug-and-Play" هستند، و نیز می‌توان در حالیکه کامپیوتر روشن و در حال فعالیت است، آنها را نصب یا خارج نمود و پس از نصب آنها نیازی به restart کردن کامپیوتر نیست.

نصب کارت شبکه

برای نصب کارت شبکه، توصیه می‌شود که از دستورالعمل‌های همراه کارت شبکه خود پیروی کنید. سعی کنید کارت شبکه‌ای را خریداری نمائید که این دستورالعمل‌ها را با خود داشته باشد. اگر قصد دارید از کارتی استفاده کنید که آن را از کامپیوتر دیگری بیرون کشیده‌اید و یا دوستتان آن را به شما داده است، ابتدا در دو روی آن کارت شبکه نام سازنده و شماره محصول را بررسی کنید. حداقل یافتن نام سازنده - درصورت وجود - آسان است. در درجه دوم، به سایت سازنده در وب مراجعه نموده و اطلاعات فنی دربارهٔ آن کارت شبکه جستجو کنید. سعی کنید شماره محصول، مدل و شماره سریال‌ها را تطبیق دهید. راهی دیگر نیز برای شناختن سازندهٔ کارت شبکه وجود دارد. بر روی کارت شبکه یک کد شش رقمی است که از حروف و عدد تشکیل یافته است (مثل OOAOC9)

شماره مذکور به OUI(Identifier Organizationally Unique) معروف است. در صورت وجود OUI شما قادر هستید سازنده کارت و نیز درایور مناسب را بیابید.

شماره OUI توسط IEEE(Engineers Institute for Electrical and Electronical) تخصیص داده می‌شود و از طریق پایگاه داده‌های آن می‌توان به جستجوی نام سازندگان پرداخت. (www.ieee.org) شما می‌بایست به منظور کارکرد صحیح کارت شبکه در کامپیوترتان، یک درایور برای آن داشته باشید. اگر کارت شبکه‌ای را از یک تولید کننده معروف در دست دارید، این شانس وجود دارد که ویندوز درایور آن را در فایلهای خود داشته باشد. اما در غیر اینصورت یا باید به دریافت درایور از اینترنت اقدام کنید و یا دیسکت و یا CD-ROM مربوط به کارت شبکه را در اختیار داشته باشید. برخی کارت‌های شبکه در دیسکت یا CD-ROM خود، یک نصب نرم‌افزاری را پیش‌بینی می‌کنند. سعی کنید این نصب را پیش از رفتن به مراحل

بعدی کامل کنید. بهترین راه برای پاسخگویی به سؤالاتی که در حین مراحل نصب ممکن است برایتان پیش بیاید، مراجعه به وب سایت سازنده است.

فرایند نصب کارت شبکه شامل مراحل زیر است:

- جایدهی فیزیکی کارت در کامپیوتر.
- پیکربندی (Configuring) کارت برای استفاده از منابع سخت‌افزاری مناسب.
- نصب نرم‌افزاری راه‌اندازی (device driver) کارت.

در مراحل نصب و راه‌اندازی شبکه ابتدا می‌بایست مسیر کابل‌کشی که بطور فیزیکی کامپیوترهای شما را به یکدیگر متصل می‌کند مشخص شود. یک روش آسان ولی مؤثر در طراحی مسیر جایگیری کابل‌ها، این است که با در دست داشتن یک دفترچه یادداشت و یک مداد، از یک مکان دلخواه برای کامپیوتر به سمت مکان دیگر حرکت کنید و بدین شکل یک طرح کلی را از کف خانه خود بدست آورید؛ همینطور که پیش می‌روید هرگونه مانعی را که می‌بایست فکری برایش کرد یادداشت کنید مثل دیوارها، لوله‌ها، لوازم خانه،درخت‌ها و غیره. اگر قصد دارید کابل‌کشی را بر روی زمین و به موازات لبه‌های دیوار انجام دهید، خوب است کابل‌ها را با استفاده از یک سری نگهدارنده‌های پلاستیکی به دیوار محکم کنید. در هنگام نصب کابل در اطراف مجراهای گرمایی یا تهویه، سیستم‌های خلاء مرکزی و یا سیستم‌های برق، دقت لازم را به عمل آورید. پس از طراحی مسیر کابل‌ها، به اندازه‌گیری مسیر واقعی آنها بر روی زمین بپردازید. فراموش نکنید که اگر قرار است یک کامپیوتر بر روی میز قرار گیرد لازم است که فاصله پشت کیس کامپیوتر را تا زمین اندازه بگیرید. همچنین اندازه گوشه‌ها و زوایای دیوارها را بیفزایید. پس از پایان این مرحله مجدداً به اندازه‌گیری مسیر کابل‌ها بپردازید و اندازه‌های قبلی خود را بررسی و اصلاح نمائید. آنگاه همهٔ اندازه‌های بدست آمده را برای بدست آوردن

کل طول کابل مورد نیاز، با هم جمع کنید. اندازه‌ای حدود ده فوت را به کل اندازه کابل مورد نیاز بیفزایید، این طول اضافی بابت موانعی است که به آسانی قابل اندازه‌گیری نیستند مثل زوایا و گوشه‌ها و یا پله‌ها.[۴۷]

برای ادامه کار شما به کابل Cat5 به همراه اتصال دهنده‌های RJ-45 نیاز دارید.

به منظور جایدهی فیزیکی کارت شبکه در کامپیوتر، ابتدا کامپیوتر را خاموش کنید. سپس کیس کامپیوتر را باز نمائید و به دنبال یک شیار (slot) آزاد بگردید. در بازار هر دو نوع کارت شبکه ISA و PCI وجود دارند و شما قبل از انتخاب کارت باید بررسی کنید که کامپیوترتان چه نوع شیاری را دارا می‌باشد. کارت‌های ISA برای استفاده‌های معمولی شبکه کافی هستند اما امروزه این نوع باس‌ها با PCI جایگزین شده‌اند. در صورتیکه بخواهید کامپیوتر خود را به شبکه‌های پر سرعت (۱۰۰-Mbps) وصل کنید، باس PCI را ترجیح دهید. پس از خارج ساختن پوشش شیار، کارت را درون شیار جای دهید و آن را محکم کنید.

در مرحله دوم، پیکربندی کارت شبکه به منظور استفاده آن از منابع سخت‌افزاری خاص صورت می‌گیرد.

مثالهایی از این منابع سخت‌افزاری عبارتند از:

- Interrupt requests (IRQS): یعنی خطوط سخت‌افزاری که وسایل جانبی از آنها برای فرستادن سیگنال‌ها به پردازشگر و درخواست توجه آن، استفاده می‌کنند.
- Input/Output (I/O) port addresses: این مکان‌ها در حافظه برای استفاده وسایل خاص و به منظور تبادل اطلاعات با دیگر بخشهای کامپیوتر، تخصیص داده می‌شوند.
- Memory addresses: این مکانها از حافظه توسط وسایل خاص و به منظور نصب BIOS با هدف خاصی استفاده می‌شوند.
- Direct memory access (DMA) channels: یعنی مسیرهای سیستمی که وسایل از آنها برای تبادل اطلاعات با حافظه سیستم استفاده می‌کنند.

کارت‌های شبکه معمولاً از آدرسهای حافظه یا DMA استفاده نمی‌کنند، اما هر کارت شبکه به یک IRQ و نیز آدرس I/O پورت برای برقراری ارتباط با کامپیوتر نیاز دارد. وقتی شما کامپیوتر و کارت شبکه‌ای را داشته باشید که هر دو از استاندارد "Plug and Play" (یعنی توانایی یک سیستم کامپیوتری برای پیکربندی خودکار وسیله‌ای که به آن افزوده می‌شود) پشتیبانی کنند، فرایند پیکربندی (مرحله دوم) به طور خودکار انجام می‌گیرد. کامپیوتر کارت شبکه را تشخیص داده،آن را شناسایی می‌کند، همچنین منابع آزاد را مکان‌یابی کرده و به پیکربندی کارت شبکه برای استفاده از آنها اقدام می‌کند. عدم وجود مکان "Plug and Play" به معنی آنست که شما باید کارت شبکه را برای استفاده از IRQ خاص و پورت I/O پیکربندی نمائید و سپس این تنظیمات را با تنظیمات درایور کارت شبکه تطبیق دهید. البته این حالت بیشتر در کارت شبکه‌های قدیمی اتفاق می‌افتد. تقریباً از ویندوز ۹۵ به بعد، ابزارهایی به منظور تشخیص برخوردهای سخت‌افزاری در اختیار کاربران قرار گرفته است. "Device Manager" تنظیمات سخت‌افزاری همه اجزاء را در کامپیوتر فهرست می‌کند، و هنگامیکه در مورد کارت شبکه‌ای که به تازگی نصب شده، یک برخورد سخت‌افزاری پیش می‌آید، این ابزار شما را آگاه می‌سازد. شما می‌توانید از "Device Manager" برای تشخیص اینکه کارت شبکه با چه وسیله‌ای برخورد دارد و چه منبعی احتیاج به تنظیم دارد، استفاده نمائید.

مرحله سوم شامل نصب درایوهای کارت شبکه است. نرم‌افزار راه‌اندازی (device driver) بخشی از کارت شبکه است که کامپیوتر را قادر می‌سازد با کارت شبکه ارتباط برقرار کرده و کارکردهای مورد نیاز را اجرا کند. در حقیقت تمامی کارت‌های شبکه برای پشتیبانی از سیستم‌های عامل مطرح، با یک نرم‌افزار راه‌اندازی عرضه می‌شوند، اما در بسیاری از موارد، شما حتی به این نرم‌افزار احتیاج پیدا نخواهید کرد زیرا سیستم‌های عاملی مثل ویندوز، مجموعه‌ای از درایوها را برای مدلهای کارت شبکه پراستفاده و رایج شامل می‌گردند. با وجود امکان "Plug and Play"، علاوه بر تنظیم پیکربندی منابع سخت‌افزاری کارت شبکه، درایور مناسب نیز نصب

می‌شود. شما می‌توانید جدیدترین درایورهای مربوط به کارت شبکه را از سایت سازندهٔ آن بدست آورید. البته نصب درایور جدید تنها در صورت بروز مشکل ضرورت پیدا می‌کند.

تنظیمات مربوط به ویندوز برای ایجاد شبکه

حال وقت آن است که در سیستم عامل خود تنظیماتی را انجام دهید تا کامپیوتر شما بتواند جستجو برای کامپیوترهای دیگر و گفتگو با آنها را آغاز کند.

نحوه پیکربندی تنظیمات مربوط به ویندوز در کامپیوتر شما، توسط این مسأله تعیین می‌شود که آیا در شبکه شما Internet sharing وجود دارد یا خیر. در ادامه بر حسب این مسأله دستورالعمل‌های لازم آورده می‌شود:

Non-Internet Sharing Windows Settings

در مورد هر کامپیوتر مراحل زیر را طی کنید:

۱. بر روی آیکن Neighborhood Network بر روی desktop راست کلیک کنید.

۲. Properties را انتخاب کنید.

۳. بر روی Access Control tab کلیک کرده و Share level access را انتخاب کنید.

۴. Identification tab را انتخاب کنید. در اینجا می‌توانید نامی را برای کامپیوتر خود انتخاب کنید.

۵. Configuration tab را انتخاب کنید.

از Client for Microsoft Networks ،Primary Network Logon را انتخاب کنید.

۶. سپس یک آدرس IP را به کامپیوتر اختصاص دهید، مثلاً X.۱۹۲.۱۶۸ .O.X در هر کامپیوتر منحصر به فرد است و عددی بین ۱ تا ۲۵۴ می‌باشد. در این قسمت عدد Subnet mask را، ۲۵۵.۲۵۵.۲۵۵.۰ بنویسید.

Internet Sharing Windows Setting

در مورد هر کامپیوتر مراحل زیر را اجرا کنید:

- در Control Panel، بر روی آیکن Program Add/Remove دو بار کلیک کنید. بر روی Windows setup tab کلیک کنید.

- پس از گذشت چند لحظه از لیست اجزاء، Internet tools را انتخاب کنید.

- سپس Connection Sharing Internet را انتخاب کنید.

- در اینجا CD مربوط به ویندوز مورد نیاز است. آنگاه Internet Connection Sharing Wizard اجرا می‌گردد که پس از پایان آن، کامپیوتر را Restart نمایید.

- می‌توانید از فلاپی دیسکی که در طی مراحل Wizard ایجاد می‌کنید، در مورد کامپیوترهای دیگر شبکه استفاده کنید (در منوی Run در هر یک از آنها و پس از گذاشتن فلاپی در کامپیوتر اینگونه تایپ کنید: a:\icsclset.exe و سپس Enter را فشار دهید)

لازم به ذکر است در صورتیکه بخواهید شبکه خود را از طریق یک Proxy Server به اینترنت متصل کنید می‌بایست آن را خریداری کرده و تنظیمات مربوطه را انجام دهید. فراهم کننده خدمات اینترنت (ISP) شما باید در مورد استفاده از dynamic IP و یا static IP شما را آگاه سازد. در صورت استفاده از static IP، ISP باید در اختصاص IP به شما کمک کند.

شبکه های بی سیم WirelessNetworking

مفاهیم و تعاریف

وقتی از شبکه اطلاع‌رسانی سخن به میان می‌آید، اغلب کابل شبکه به عنوان وسیله انتقال داده در نظر گرفته می‌شود. در حالیکه چندین سال است که استفاده از شبکه سازی بی‌سیم در دنیا آغازگردیده است. تا همین اواخر یک LAN بی‌سیم با سرعت انتقال پایین و خدمات غیرقابل اعتماد و مترادف بود، اما هم اکنون تکنولوژی‌های LAN بی‌سیم خدمات قابل قبولی را با سرعتی که حداقل برای کاربران معمولی شبکه کابلی پذیرفته شده می‌باشد، فراهم می‌کنند.

WLANها (یا LANهای بی‌سیم) از امواج الکترومغناطیسی (رادیویی یا مادون قرمز) برای انتقال اطلاعات از یک نقطه به نقطه دیگر استفاده می‌کنند. امواج رادیویی اغلب به عنوان یک حامل رادیویی تلقی می‌گردند، چرا که این امواج وظیفه انتقال انرژی الکترومغناطیسی از فرستنده را به گیرنده دورتر از خود بعهده دارند[۵۰]. داده هنگام ارسال برروی موج حامل رادیویی سوار می‌شود و در گیرنده نیز به راحتی از موج حامل تفکیک می‌گردد. به این عمل مدولاسیون اطلاعات به موج حامل گفته می‌شود. هنگامیکه داده با موج رادیویی حامل مدوله می‌شود، سیگنال رادیویی دارای فرکانس‌های مختلفی علاوه بر فرکانس اصلی موج حامل می‌گردد. به عبارت دیگر فرکانس اطلاعات داده به فرکانس موج حامل اضافه می‌شود. در گیرنده رادیویی برای استخراج اطلاعات، گیرنده روی فرکانس خاصی تنظیم می‌گردد و سایر فرکانس‌های اضافی فیلتر می‌شوند.

WLAN

در یک ساختار WLAN، یک دستگاه فرستنده و گیرنده مرکزی، Access Point(AP) خوانده می‌شود. AP با استفاده از کابل شبکه استاندارد به شبکه محلی سیمی متصل می‌گردد. در حالت ساده، گیرنده AP وظیفه دریافت، ذخیره و ارسال داده را بین شبکه محلی سیمی و WLAN بعهده دارد. AP با آنتنی که به آن متصل است، می‌تواند در محل مرتفع و یا هر مکانی که امکان ارتباط بهتر را فراهم می‌کند، نصب شود. هر کاربر می‌تواند از طریق یک کارت شبکه بی‌سیم (Wireless Adapter) به سیستم WLAN متصل شود. این کارت‌ها به صورت استاندارد برای رایانه‌های شخصی و کیفی ساخته می‌شوند. کارت WLAN به عنوان واسطی بین سیستم عامل شبکه کاربر و امواج دریافتی از آنتن عمل می‌کند. سیستم عامل شبکه عملاً درگیر چگونگی ارتباط ایجاد شده نخواهد بود.

امروزه استاندارد غالب در شبکه‌های WLAN، IEEE802.11 می‌باشد. گروهی که بر روی این استاندارد کار می‌کند در سال ۱۹۹۰ با هدف توسعه استاندارد جهانی شبکه سازی بی‌سیم با سرعت انتقال ۱ تا ۲ مگابیت در ثانیه شکل گرفت. استاندارد مذکور با نام IEEE802.11a شناخته می‌شود. استاندارد IEEE802.11b که جدیدتر است، سرعت انتقال را تا ۵/۵ و ۱۱مگابیت در ثانیه می‌افزاید.

WLANها از دو توپولوژی حمایت می‌کنند:

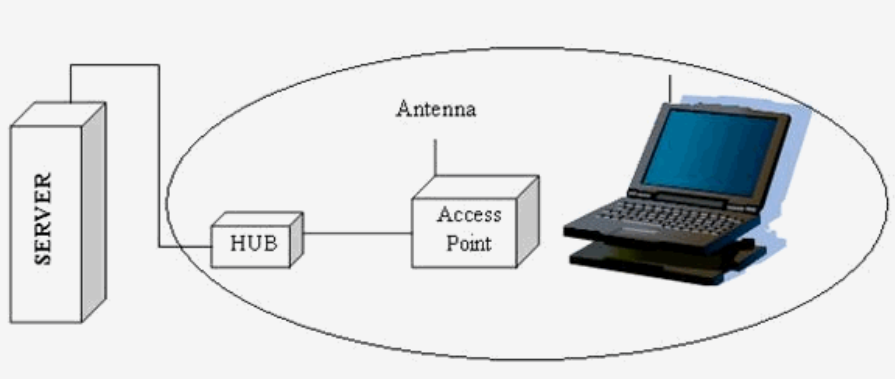
- ad hoc topology

- infrastructure topology

در توپولوژی ad hoc کامپیوترها به شبکه بی‌سیم مجهز هستند و مستقیماً با یکدیگر به شکل Peer- to- peer ارتباط برقرار می‌نمایند.

کامپیوترها برای ارتباط باید در محدوده یکدیگر قرار داشته باشند. این نوع شبکه برای پشتیبانی از تعداد محدودی از کامپیوترها، مثلاً در محیط خانه یا دفاتر کوچک طراحی می‌شود. "امروزه نوعی از توپولوژی ad hoc به نام "peer-to-peer networking ad hoc" مطرح است. این نوع شبکه که به شبکه "Mesh" نیز معروف است، شبکه‌ای پویا از دستگاههای بی‌سیم است که به هیچ نوع زیرساخت موجود یا کنترل مرکزی وابسته نیست. در این شرایط، دستگاههای شبکه همچنین به مانند گرههایی عمل می‌کنند که کاربران از طریق آنها می‌توانند داده‌ها را انتقال دهند، به این معنی که دستگاه هر کاربر بعنوان مسیریاب و تکرارکننده(Repeater) عمل می‌کند. این شبکه نوع تکامل‌یافته شبکه Point-to-multipoint است که در آن همه کاربران می‌بایست برای استفاده از شبکه دسترسی مستقیم به نقطه دستیابی مرکزی داشته باشند. در معماری Mesh کاربران می‌توانند بوسیله Multi-Hopping، از طریق گرههای دیگر به نقطه مرکزی وصل شوند، بدون اینکه به ایجاد هیچگونه پیوند مستقیم RF نیاز باشد.بعلاوه در شبکه Mesh در صورتیکه کاربران بتوانند یک پیوند فرکانس رادیویی برقرار کنند، نیازی به نقطه دسترسی(Access Point) نیست و کاربران می‌توانند بدون وجود یک نقطه کنترل مرکزی با یکدیگر، فایلها، نامه‌های الکترونیکی و صوت و تصویر را به اشتراک بگذارند. این ارتباط دو نفره، به آسانی برای دربرگرفتن کاربران بیشتر قابل گسترش است. توپولوژی infrastructure اصولاً برای گسترش و افزایش انعطاف‌پذیری شبکه‌های کابلی معمولی بکار می‌رود. بدین شکل که اتصال کامپیوترهای مجهز به

تکنولوژی بی‌سیم را با استفاده از Access Point به آن امکان می‌سازد. در برخی موارد، یک AP کامپیوتری است که کارت شبکه بی‌سیم را کنار کارت شبکه معمولی - که آن را به یک LAN کابلی متصل می‌کند - دارا می‌باشد. کامپیوترهای بی‌سیم با استفاده از AP به عنوان واسطه با شبکه کابلی ارتباط برقرار می‌کنند. AP اساساً بعنوان یک Translation Bridge عمل می‌کند، زیرا سیگنال‌های شبکه بی‌سیم را به سیگنال‌های شبکه کابلی تبدیل می‌کند. مانند تمام تکنولوژی‌های ارتباطی بی‌سیم، شرایط مسافتی و محیطی می‌توانند بر روی عملکرد ایستگاههای سیار بسیار تأثیر گذار باشند. یک AP می‌تواند ۱۰ تا ۲۰ کامپیوتر را پشتیبانی کند، بسته به اینکه میزان استفاده آنها از LAN چقدر است. این پشتیبانی تا زمانی ادامه دارد که آن کامپیوترها در شعاع تقریبی ۱۰۰ تا ۲۰۰ فوت نسبت به AP قرار داشته باشند. موانع فیزیکی مداخله کننده این عملکرد را به طرز چشمگیری کاهش می‌دهند.



Cell

شبکهWLANبا یک(AccessPoint(AP

در شکل فوق یک Access Point از طریق یک کابل به شبکه LAN متصل شده است. در اینجا وظیفه یک AP دریافت اطلاعات از سرویس گیرنده‌ها (Clients) از طریق هوا و ارسال آن اطلاعات از طریق یک پورت به

hub می باشد. AP به عنوان یک پل ارتباطی بین شبکه WLAN و شبکه LAN عمل می‌کند. ناحیه‌ای که توسط یک AP تحت پوشش قرار می‌گیرد سلول (Cell) نامیده می‌شود. هر ایستگاه در داخل Cell می‌تواند به AP دسترسی پیدا کند. وظیفه یک AP ایجاد هماهنگی بین سرویس گیرندگان (Clients) شبکه WLAN و یک شبکه LAN می‌باشد.

به منظور گسترش بخش بی‌سیم و تحت پوشش قرار دادن سرویس گیرندگان بیشتر، می‌توان از APهای متعدد در مناطق مختلف استفاده کرد، و یا اینکه یک Extension point را بکار گرفت. Extension point، یک تقویت کننده سیگنال‌های بی‌سیم است که به عنوان ایستگاهی بین سرویس گیرندگان بی‌سیم و AP عمل می‌کند. استاندارد IEEE 802.11 دو سلول را به عنوان یک BSS(Basic Service Set) در نظر می‌گیرد. اگر شبکه از چند Access Point استفاده کند، APها با یک ستون فقرات بنام DS (Distribution System) به هم اتصال می‌یابند. DS معمولاً یک شبکه کابلی است، اما می‌توان آن را بی‌سیم هم در نظر گرفت.

استاندارد IEEE 802.11 از سه نوع سیگنال در لایه فیزیکی پشتیبانی می‌کند:

- (Direct Sequence Spread Spectrum DSSS): یک روش انتقال رادیویی است که در آن سیگنال‌های خروجی با استفاده از یک کد دیجیتال مدوله می‌شوند. در نتیجه هر بیت از دیتا به چند بیت تبدیل می‌شود و سیگنال می‌تواند در فرکانس وسیع‌تر پراکنده شود. استفاده از DSSS به همراه روش CCK (Complimentary Code Keying) باعث می‌شود سیستم‌های IEEE 802.11b به سرعت۱۱ مگابیت در ثانیه انتقال دست یابند. در جائیکه شرایط به نحوی است که امکان تداخل، نویزنپذیری یا وجود دستگاههای کاری هم‌فرکانس در منطقه موجود نباشد یا بسیار کم باشد از شیوه DSSS استفاده می‌شود. در این شیوه می‌توان از تمامی عرض باند موجود در طیف گسترده شده (مثلاً 10MHZ یا بیشتر) بهره جست و لذا به شبکه‌ای با سرعت ۱۰ مگابیت در ثانیه یا بالاتر دست یافت. اما در محیط‌های شلوغ به لحاظ ترافیک امواج مثلاً

محیط‌های شهری بزرگ، بکار بردن این تکنولوژی علیرغم وجود کدینگ‌های پیشرفته و تقسیم‌بندی‌های فرکانسی، خالی از بروز تداخل‌ها و یا اشکالات احتمالی نخواهد بود.

- Frequency Hopping Spread Spectrum(FHSS) : یک روش انتقال رادیویی که در آن انتقال دهنده به طور مداوم تغییرات سریعی را در فرکانس - بر طبق یک الگوریتم موجود - انجام می‌دهد. دریافت کننده برای خواندن سیگنال‌های دریافتی، دقیقاً همان تغییرات را انجام می‌دهد. در IEEE 802.11a می‌توان از FHSS استفاده کرد اما سیستم IEEE 802.11b از این روش حمایت نمی‌کند.

- Infrared: در ارتباطاتinfrared (مادون قرمز) از فرکانسهای بالا - دقیقا زیر طیف نور مرئی- استفاده می‌شود. در این روش سیگنالها نمی‌توانند از اشیاء و دیوارها عبور کنند. این امر بکارگیری تکنولوژی مادون قرمز را محدود می‌سازد. در فناوری مادون قرمز ارسال کننده و دریافت کننده باید یکدیگر را ببینند(در خط دید یکدیگر باشند) همانند یک کنترل کننده راه دور دستگاه تلویزیون. بطور کلی در ارتباطات داخل ساختمان که فاصله ایستگاهها کم باشد از این روش استفاده می‌شود. در اینجا بجای سیم یا فیبر نوری که رسانه‌های انتقال هستند، از امواج رادیویی یا نور مادون قرمز بعنوان رسانه انتقال استفاده می‌شود. امواج رادیویی بخاطر برد، پهنای باند و پوشش مکانی بیشتر، از نور مادون قرمز کاربرد بیشتری دارند. در این قسمت به برخی مزایای یک WLAN نسبت به یک شبکه کابلی می‌پردازیم. از WLANها می‌توان در مکانهایی که امکان کابل‌کشی وجود ندارد استفاده کرد و بدون نیاز به کابل‌کشی آنها را گسترش داد. استفاده کننده WLAN می‌تواند کامپیوتر خود را بدون قطع کابل، به هر نقطه از سازمان منتقل کند. با وجود اینکه سخت‌افزار مورد نیاز برای WLAN گرانتر از تجهیزات شبکه سیمی است، ولی بهره‌وری و انعطاف‌پذیری آن باعث

می‌شود که در طول زمان قیمت تمام شده کمتر شود، بخصوص در محیطهایی که شبکه مورد نظر پیوسته در حال انتقال و تغییر مداوم است.

سیستمهای WLAN می‌توانند با فناوریهای مختلف شبکه ترکیب شوند و شبکه‌هایی با کاربردها و امکانات خاص را به نمو مطلوبی ایجاد کنند. پیکربندی این شبکه‌ها براحتی قابل تغییر است و این شبکه‌ها می‌توانند از حالت نقطه به نقطه تا شبکه‌هایی با زیرساختار پیچیده با صدها کاربر متحرک گسترش یابند. در شبکه‌های بی‌سیم مدیران شبکه می‌توانند جابجایی، گسترش و اصلاح شبکه را آسانتر انجام دهند و با استفاده از این سیستم به نصب کامپیوترهای شبکه در ساختمانهای قدیمی و یا مکانهایی که امکان کابل‌کشی در آنها وجود ندارد و نیز مکانهایی که فاصله آنها از یکدیگر زیاد است بپردازند و بدین شکل امکان دسترسی سریع به اطلاعات را فراهم کنند.

پارامترهای مؤثر در انتخاب و پیاده‌سازی یک سیستم WLAN

۱- برد محدوده پوشش: اثر متقابل اشیاء موجود در ساختمان(نظیر دیوارها، فلزات و افراد) می‌تواند بر روی انرژی انتشار اثر بگذارد و در نتیجه برد و محدوده پوشش سیستم را تحت تأثیر قرار دهد. برای سیگنالهای مادون قرمز، اشیای موجود در ساختمان مانعی دیگر بشمار می‌رود و در نتیجه محدودیتهای خاصی را در شبکه بوجود می‌آورد. بیشتر سیستمهای WLAN از امواج رادیویی RF استفاده می‌کنند، زیرا می‌تواند از دیوارها و موانع عبور کند. برد(شعاع پوشش) برای سیستمهای WLAN بین ۱۰ تا ۳۰ متر متغیر است.

۲- سرعت انتقال داده: همانند شبکه‌های کابلی، سرعت انتقال داده واقعی در شبکه‌های بی‌سیم، به نوع محصولات و توپولوژی شبکه بستگی دارد. تعداد کاربران، فاکتورهای انتشار مانند برد، مسیرهای ارتباطی، نوع سیستم WLAN استفاده شده، نقاط کور و گلوگاههای شبکه، از پارامترهای مهم و تأثیرگذار در سرعت انتقال داده بحساب می‌آیند. بعنوان یک مقایسه با مودمهای امروزی(با سرعت ۵۶ کیلو بیت در ثانیه) سرعت عملکرد WLANها در حدود ۳۰ برابر سریعتر از این مودمهاست.

۳- سازگاری با شبکه‌های موجود: بیشتر سیستمهای WLAN با استانداردهای صنعتی متداول شبکه‌های کابلی نظیر Ethernet و Token Ring سازگار است. با نصب درایورهای مناسب در ایستگاههای WLAN، سیستمهای عامل آن ایستگاهها دقیقا مانند سایر ایستگاههای موجود در شبکه LAN کابلی بکار گرفته می‌شود.

۴- سازگاری با دیگر محصولات WLAN: به سه دلیل مشتریان هنگام خرید محصولات WLAN باید مراقب باشند که سیستم موردنظر بتواند با سایر محصولات WLAN تولیدکنندگان دیگر سازگاری داشته باشد:
- ممکن است هر محصول از تکنولوژی خاصی استفاده کرده باشد، برای مثال سیستمی که از فناوری FHSS استفاده کند نمی‌تواند با سیستمی با فناوری DSSS کار کند.

- اگر فرکانس کار دو سیستم با یکدیگر یکسان نباشد،حتی در صورت استفاده از فناوری مشابه، امکان کارکردن با یکدیگر فراهم نخواهد شد.

- حتی تولیدکنندگان مختلف اگر از یک فناوری و یک فرکانس استفاده کنند، بدلیل روشهای مختلف طراحی ممکن است با سایر محصولات دیگر سازگاری نداشته باشد.

۵- تداخل و اثرات متقابل: طبیعت امواج رادیویی در سیستمهای WLAN ایجاب می‌کند تا سیستمهای مختلف که دارای طیفهای فرکانسی یکسانی هستند، بر روی یکدیگر اثر تداخل داشته باشند. با این وجود اغلب تولیدکنندگان در تولید محصولات خود تمهیداتی را برای مقابله با آن بکار می‌گیرند، به نحوی که وجود چند سیستم WLAN نزدیک به یکدیگر، تداخلی در دیگر سیستمها بوجود نمی‌آورد.

۶- ملاحظات مجوز فرکانسی: در اغلب کشورها ارگانهای ناظر بر تخصیص فرکانس رادیویی، محدوده فرکانس شبکه‌های WLAN را مشخص کرده‌اند. این محدوده ممکن است در همه کشورها یکسان نباشد. معمولا سازندگان تجهیزات WLAN فرکانس سیستم را در محدوده مجاز قرار می‌دهند. در نتیجه کاربر نیاز به اخذ مجوز فرکانسی ندارد. این محدوده فرکانس به ISM معروف است. محدوده بین‌المللی این فرکانسها ۹۲۸-۹۰۲ مگاهرتز،۲/۴۸۳-۲/۴ گیگاهرتز، ۵/۳۵-۵/۱۵ گیگاهرتز و ۵/۸۷۵-۵/۷۲۵ گیگاهرتز است. بنابراین تولیدکنندگان تجهیزات WLAN باید این محدوده مجوز فرکانسی را در سیستمهای خود رعایت کنند.

۷- سادگی و سهولت استفاده: اغلب کاربران در مورد مزیتهای WLANها اطلاعات کمی دارند. می‌دانیم که سیستم عامل اصولاً به نحوه اتصال سیمی و یا بی‌سیم شبکه وابستگی ندارند. بنابراین برنامه‌های کاربردی بر روی شبکه بطور یکسان عمل می‌نمایند. تولیدکنندگان WLAN ابزار مفیدی را برای سنجش وضعیت سیستم و تنظیمات مورد در اختیار کاربران قرار می‌دهند. مدیران شبکه به سادگی می‌توانند نصب و راه‌اندازی سیستم را با توجه به توپولوژی شبکه موردنظر انجام دهند. در WLAN کلیه کاربران بدون نیاز به کابل‌کشی می‌توانند با یکدیگر ارتباط برقرار کنند. عدم نیاز به کابل‌کشی موجب می‌شود که تغییرات، جابجایی و اضافه کردن در شبکه به آسانی انجام شود. در نهایت به موجب قابلیت جابجایی آسان تجهیزات WLANمدیر شبکه می‌تواند قبل از اینکه تجهیزات شبکه را در مکان اصلی خود نصب کند، ابتدا آنها را راه‌اندازی کند و تمامی مشکلات احتمالی شبکه را برطرف سازد و پس از تایید نهایی در محل اصلی جایگذاری نماید و پس از پیکربندی، هرگونه جابجایی از یک نقطه به نقطه دیگر را بدون کمترین تغییرات اصلاح نماید.

۸- امنیت: از آنجایی که سرمنشأ فناوری بی‌سیم در کاربردهای نظامی بوده است، امنیت از جمله مقولات مهم در طراحی سیستمهای بی‌سیم بشمار می‌رود. بحث امنیت هم در ساختار تجهیزات WLAN به نحو مطلوبی پیش‌بینی شده است و این امر شبکه‌های بی‌سیم را بسیار امن‌تر از شبکه‌های سیمی کرده است. برای گیرنده‌هایی که دستیابی مجاز به سیگنالهای دریافتی ندارند، دسترسی به اطلاعات موجود در WLAN بسیار مشکل است. به دلیل تکنیکهای پیشرفته رمزنگاری برای اغلب گیرنده‌های غیرمجاز دسترسی به ترافیک شبکه غیرممکن است. عموما گیرنده‌های مجاز باید قبل از ورود به شبکه و دسترسی به اطلاعات آن، از نظر امنیتی مجوز لازم را دارا باشند.

۹- هزینه: برای پیاده‌سازی یک WLAN هزینه اصلی شامل دو بخش است: هزینه‌های زیرساختار شبکه مانند APهای شبکه و نیز هزینه کارتهای شبکه جهت دسترسی کاربران به WLAN. هزینه‌های زیرساختار شبکه به تعداد APهای موردنیاز شبکه بستگی دارد. قیمت یک AP بین ۱۰۰۰ تا۲۰۰۰ دلار می‌باشد. تعداد APهای شبکه به شعاع عملکرد شبکه، تعداد کاربران و نوع سرویسهای موجود در شبکه بستگی دارد و هزینه کارتهای شبکه با توجه به یک شبکه رایانه‌ای استاندارد حدود ۳۰۰ تا ۵۰۰ دلار برای هر کاربر می‌باشد.

هزینه نصب و راه‌اندازی یک شبکه بی‌سیم به دو دلیل کمتر از نصب و راه‌اندازی یک شبکه سیمی می‌باشد:

- هزینه کابل‌کشی و پیدا کردن مسیر مناسب بین کاربران و سایر هزینه‌های مربوط به نصب تجهیزات در ساختمان، بخصوص در فواصل طولانی که استفاده از فیبر نوری یا سایر خطوط گرانقیمت ضروری است، بسیار زیاد است.

- به دلیل قابلیت جابجایی، اضافه کردن و تغییرات ساده در WLAN، هزینه‌های سربار، برای این تغییرات و تعمیر و نگهداری آن بسیار کمتر از شبکه سیمی است.

۱۰- قابلیت گسترش سیستم: با یک شبکه بی‌سیم می‌توان شبکه‌ای با توپولوژی بسیار ساده تا بسیار پیچیده را طراحی کرد. در شبکه‌های بی‌سیم با افزایش تعداد APها یا WBها می‌توان محدوده فیزیکی تحت پوشش و تعداد کاربران موجود در شبکه را تا حد بسیار زیادی گسترش داد. شعاع عملکرد این شبکه تا حدود ۲۰ کیلومتر می‌باشد.

۱۱- اثرات جانبی: توان خروجی یک سیستم بی‌سیم بسیار پایین است. از آنجایی که امواج رادیویی با افزایش فاصله به سرعت مستهلک می‌گردند و در عین حال، افرادی را که در محدوده تشعشع انرژی RF هستند، تحت تاثیر قرار می‌دهند، باید ملاحظات حفظ سلامت با توجه به مقررات دولتی رعایت گردد. با این وجود اثرات مخرب این سیستمها زیاد نمی‌باشد.

استراتژی حفاظت از اطلاعات در شبکه های کامپیوتری

اطلاعات در سازمان ها و موسسات مدرن، بمنزله شاهرگ حیاتی محسوب می گردد . دستیابی به اطلاعات و عرضه مناسب و سریع آن، همواره مورد توجه سازمان هائی است که اطلاعات در آنها دارای نقشی محوری و سرنوشت ساز است . سازمان ها و موسسات می بایست یک زیر ساخت مناسب اطلاعاتی را برای خود ایجاد و در جهت انظباط اطلاعاتی در سازمان خود حرکت نمایند . اگر می خواهیم ارائه دهنده اطلاعات در عصر اطلاعات بوده و صرفا" مصرف کننده اطلاعات نباشیم ، در مرحله نخست می بایست فرآیندهای تولید ،عرضه و استفاده از اطلاعات را در سازمان خود قانونمد نموده و در مراحل بعد ، امکان استفاده از اطلاعات ذیربط را برای متقاضیان (محلی،جهانی) در سریعترین زمان ممکن فراهم نمائیم . سرعت در تولید و عرضه اطلاعات ارزشمند ، یکی از رموز موفقیت سازمان ها و موسسات در عصر اطلاعات است . پس از ایجاد انظباط اطلاعاتی، می بایست با بهره گیری از شبکه های کامپیوتری زمینه استفاده قانومند و هدفمند از اطلاعات را برای سایرین فراهم کرد . اطلاعات ارائه شده می تواند بصورت محلی (اینترانت) و یا جهانی (اینترنت) مورد استفاده قرار گیرد . فراموش نکنیم در این هنگامه اطلاعاتی، مصرف کنندگان اطلاعات دارای حق مسلم انتخاب می باشند و در صورتیکه سازمان و یا موسسه ای در ارائه اطلاعات سهوا" و یا تعمدا" دچار اختلال و یا مشکل گردد ، دلیلی بر توقف عملکرد مصرف کنندگان اطلاعات تا بر طرف نمودن مشکل ما ، وجود نخواهد داشت . سازمان ها و موسسات می بایست خود را برای نبردی سخت در عرضه و ارائه اطلاعات آماده نمایند و در این راستا علاوه بر پتانسیل های سخت افزاری و نرم افزاری استفاده شده ، از تدبیر و دوراندیشی فاصله نگیرند . در میدان عرضه و ارائه اطلاعات ، کسب موفقیت نه بدلیل ضعف دیگران بلکه بر توانمندی ما استوار خواهد بود. مصرف کنندگان اطلاعات، قطعا" ارائه دهندگان اطلاعاتی را برمی گزیند که نسبت به توان و پتانسیل آنان اطمینان حاصل کرده باشند . آیا سازمان ما در عصر اطلاعات به پتانسیل های لازم در این خصوص دست پیدا کرده است ؟ آیا در سازمان ما بستر و ساختار مناسب

اطلاعاتی ایجاد شده است ؟ آیا گردش امور در سازمان ما مبتنی بر یک سیستم اطلاعاتی مدرن است ؟ آیا سازمان ما قادر به تعامل اطلاعاتی با سایر سازمان ها است ؟ آیا در سازمان ما نقاط تماس اطلاعاتی با دنیای خارج از سازمان تدوین شده است ؟ آیا فاصله تولید و استفاده از اطلاعات در سازمان ما به حداقل مقدار خود رسیده است ؟ آیا اطلاعات قابل عرضه سازمان ما ، در سریعترین زمان و با کیفیتی مناسب در اختیار مصرف کنندگان متقاضی قرار می گیرد ؟ حضور یک سازمان در عرصه جهانی ، صرفا" داشتن یک وب سایت با اطلاعات ایستا نخواهد بود . امروزه میلیون ها وب سایت بر روی اینترنت وجود داشته که هر روز نیز به تعداد آنان افزوده می گردد . کاربران اینترنت برای پذیرش سایت سازمان ما ، دلایل موجه ای را دنبال خواهند کرد . در این هنگامه سایت داشتن و راه اندازی سایت ، اصل موضوع که همانا ایجاد یک سازمان مدرن اطلاعاتی است ، فراموش نگردد. سازمان ما در این راستا چگونه حرکت کرده و مختصات آن در نقشه اطلاعاتی یک سازمان مدرن چیست ؟ بدیهی است ارائه دهندگان اطلاعات خود در سطوحی دیگر به مصرف کنندگان اطلاعات تبدیل و مصرف کنندگان اطلاعات ، در حالات دیگر، خود می تواند بعنوان ارائه دهنده اطلاعات مطرح گردند. مصرف بهینه و هدفمند اطلاعات در صورتیکه به افزایش آگاهی ، تولید و ارائه اطلاعات ختم شود، امری بسیار پسندیده خواهد بود . در غیر اینصورت، مصرف مطلق و همیشگی اطلاعات بدون جهت گیری خاص ، بدترین نوع استفاده از اطلاعات بوده که قطعا" به سرانجام مطلوبی ختم نخواهد شد.

در صورتیکه قصد ارائه و یا حتی مصرف بهینه و سریع اطلاعات را داشته باشیم، می بایست زیر ساخت مناسب را در این جهت ایجاد کنیم . شبکه های کامپیوتری ، بستری مناسب برای عرضه ، ارائه و مصرف اطلاعات می باشند(دقیقا" مشابه نقش جاده ها در یک سیستم حمل و نقل) . عرضه ، ارائه و مصرف یک کالا نیازمند وجود یک سیستم حمل و نقل مطلوب خواهد بود. در صورتیکه سازمان و یا موسسه ای محصولی را تولید ولی قادر به عرضه آن در زمان مناسب (قبل از اتمام تاریخ مصرف) برای متقاضیان نباشد، قطعا" از سازمان ها ئی که تولیدات

خود را با بهره گیری از یک زیر ساخت مناسب ، بسرعت در اختیار متقاضیان قرار می دهند ، عقب خواهند افتاد . شاید بهمین دلیل باشد که وجود جاده ها و زیر ساخت های مناسب ارتباطی، بعنوان یکی از دلایل موفقیت برخی از کشورها در عصر انقلاب صنعتی ، ذکر می گردد. فراموش نکنیم که امروزه زمان کهنه شدن اطلاعات از زمان تولید اطلاعات بسیار سریعتر بوده و می بایست قبل از اتمام تاریخ مصرف اطلاعات با استفاده از زیر ساخت مناسب (شبکه های ارتباطی) اقدام به عرضه آنان نمود. برای عرضه اطلاعات می توان از امکاناتی دیگر نیز استفاده کرد ولی قطعا" شبکه های کامپیوتری بدلیل سرعت ارتباطی بسیار بالا دارای نقشی کلیدی و منحصر بفرد می باشند . مثلا" می توان مشخصات کالا و یا محصول تولید شده در یک سازمان را از طریق یک نامه به متقاضیان اعلام نمود ولی در صورتیکه سازمانی در این راستا از گزینه پست الکترونیکی استفاده نماید ، قطعا" متقاضیان مربوطه در زمانی بسیار سریعتر نسبت به مشخصات کالای تولیده شده ، آگاهی پیدا خواهند کرد .

امنیت اطلاعات در شبکه های کامپیوتری

بموازات حرکت بسمت یک سازمان مدرن و مبتنی بر تکنولوژی اطلاعات، می بایست تدابیر لازم در رابطه با حفاظت از اطلاعات نیز اندیشیده گردد. مهمترین مزیت و رسالت شبکه های کامپیوتری ، اشتراک منابع سخت افزاری و نرم افزاری است . کنترل دستیابی و نحوه استفاده از منابع به اشتراک گذاشته شده ، از مهمترین اهداف یک سیستم امنیتی در شبکه است . با گسترش شبکه های کامپیوتری خصوصا" اینترنت ، نگرش نسبت به امنیت اطلاعات و سایر منابع به اشتراک گذاشته شده ، وارد مرحله جدیدی شده است . در این راستا ، لازم است که هر سازمان برای حفاظت از اطلاعات ارزشمند ، پایبند به یک استراتژی خاص بوده و بر اساس آن سیستم امنیتی را اجراء و پیاده سازی نماید . عدم ایجاد سیستم مناسب امنیتی ، می تواند پیامدهای منفی و دور از انتظاری را بدنبال داشته باشد . استراتژی سازمان ما برای حفاظت و دفاع از اطلاعات چیست؟ در صورت بروز مشکل امنیتی

در رابطه با اطلاعات در سازمان ، بدنبال کدامین مقصر می گردیم ؟ شاید اگر در چنین مواردی ، همه مسائل امنیتی و مشکلات بوجود آمده را به خود کامپیوتر نسبت دهیم ، بهترین امکان برون رفت از مشکل بوجود آمده است ، چراکه کامپیوتر توان دفاع کردن از خود را ندارد . آیا واقعا" روش و نحوه برخورد با مشکل بوجود آمده چنین است ؟ در حالیکه یک سازمان برای خرید سخت افزار نگرانی های خاص خود را داشته و سعی در برطرف نمودن معقول آنها دارد ، آیا برای امنیت و حفاظت از اطلاعات نباید نگرانی بمراتب بیشتری در سازمان وجود داشته باشد ؟

استراتژی

دفاع در عمق ، عنوان یک استراتژی عملی بمنظور نیل به تضمین و ایمن سازی اطلاعات در محیط های شبکه امروزی است . استراتژی فوق، یکی از مناسبترین و عملی ترین گزینه های موجود است که متاثر از برنامه های هوشمند برخاسته از تکنیک ها و تکنولوژی های متفاوت تدوین می گردد . استراتژی پیشنهادی ، بر سه مولفه متفاوت ظرفیت های حفاظتی ، هزینه ها و رویکردهای عملیاتی تاکید داشته و توازنی معقول بین آنان را برقرار می نماید . دراین مقاله به بررسی عناصر اصلی و نقش هر یک از آنان در استراتژی پیشنهادی، پرداخته خواهد شد . دشمنان، انگیزه ها ، انواع حملات اطلاعاتی بمنظور دفاع موثر و مطلوب در مقابل حملات به اطلاعات و سیستم های اطلاعاتی ، یک سازمان می بایست دشمنان، پتانسیل و انگیزه های آنان و انواع حملات را بدرستی برای خود آنالیز تا از این طریق دیدگاهی منطقی نسبت به موارد فوق ایجاد و در ادامه امکان برخورد مناسب با آنان فراهم گردد .اگر قصد تجویز دارو برای بیماری وجود داشته باشد ، قطعا" قبل از معاینه و آنالیز وضعیت بیمار، اقدام به تجویز دارو برای وی نخواهد شد. در چنین مواری نمی توان برای برخورد با مسائل پویا از راه حل های مشابه و

ایستا استفاده کرد .بمنظور ارائه راهکارهای پویا و متناسب با مسائل متغیر، لازم است در ابتدا نسبت به کالبد شکافی دشمنان ، انگیزه ها و انواع حملات ، شناخت مناسبی ایجاد گردد.

دشمنان ، شامل سارقین اطلاعاتی ، مجرمان ،دزدان کامپیوتری ، شرکت های رقیب و ... می باشد . انگیزه ها ی موجود شامل : جمع آوری هوشمندانه، دستبرد فکری (عقلانی) ،عدم پذیرش سرویس ها ، کنف کردن ،احساس غرور و مورد توجه واقع شدن ، با شد.

انواع حملات شامل : مشاهده غیرفعال ارتباطات ، حملات به شبکه های فعال، حملات از نزدیک(مجاورت سیستم ها) ، سوء استفاده و بهره برداری خودیان (محرمان) و حملات مربوط به ارائه دهندگان صنعتی یکی از منابع تکنولوژی اطلاعات ، است.

سیستم های اطلاعاتی و شبکه های کامپیوتری اهداف مناسب و جذابی برای مهاجمان اطلاعاتی می باشند . بنابراین لازم است، تدابیر لازم در خصوص حفاظت سیستم ها و شبکه ها در مقابل انواع متفاوت حملاتی اطلاعاتی اندیشیده گردد. بمنظور آنالیز حملات اطلاعاتی و اتخاذ راهکار مناسب بمنظور برخورد با آنان، لازم است در ابتدا با انواع حملات اطلاعات آشنا شده تا از این طریق امکان برخورد مناسب و سیستماتیک با هریک از آنان فراهم گردد . قطعا" وقتی ما شناخت مناسبی را نسبت به نوع و علل حمله داشته باشیم ، قادر به برخورد منطقی با آن بگونه ای خواهیم بود که پس از برخورد، زمینه تکرار موارد مشابه حذف گردد.

انواع حملات اطلاعاتی بشرح ذیل می باشند :

غیرفعال

فعال

نزدیک (مجاور)

خودی ها (محرمان)

عرضه (توزیع)

ویژگی هر یک از انواع حملات فوق ، بشرح زیر می باشد:

غیر فعال . (Passive) این نوع حملات شامل: آنالیزترافیک شبکه ،شنود ارتباطات حفاظت نشده، رمزگشائی ترافیک های رمز شده ضعیف و بدست آوردن اطلاعات معتبری همچون رمز عبور می باشد . ره گیری غیرفعال عملیات شبکه ، می تواند به مهاجمان، هشدارها و اطلاعات لازم را در خصوص عملیات قریب الوقوعی که قرار است در شبکه اتفاق افتند بدهد(قرار است از مسیر فوق در آینده محموله ای ارزشمند عبور داده شود !) ، را خواهد داد .پیامدهای این نوع حملات ، آشکارشدن اطلاعات و یا فایل های اطلاعاتی برای یک مهاجم ، بدون رضایت و آگاهی کاربر خواهد بود .

فعال. (Active) این نوع حملات شامل : تلاش در جهت خنثی نمودن و یا حذف ویژگی های امنیتی ، معرفی کدهای مخرب ، سرقت و یا تغییر دادن اطلاعات می باشد . حملات فوق ، می تواند از طریق ستون فقرات یک شبکه ، سوء استفاده موقت اطلاعاتی ، نفوذ الکترونیکی در یک قلمرو بسته و حفاظت شده و یا حمله به یک کاربر

تایید شده در زمان اتصال به یک ناحیه بسته و حفاظت شده ، بروز نماید . پیامد حملات فوق ، افشای اطلاعات ، اشاعه فایل های اطلاعاتی ، عدم پذیرش سرویس و یا تغییر در داده ها ، خواهد بود.

مجاور. (Close-in) این نوع حملات توسط افرادیکه در مجاورت (نزدیکی) سیستم ها قرار دارند با استفاده از تسهیلات موجود ، با یک ترفندی خاص بمنظور نیل به اهدافی نظیر : اصلاح ، جمع آوری و انکار دستیابی به اطلاعات باشد، صورت می پذیرد . حملات مبتنی بر مجاورت فیزیکی ، از طریق ورود مخفیانه ، دستیابی باز و یا هردو انجام می شود.

خودی . (Insider) حملات خودی ها ، می تواند بصورت مخرب و یا غیر مخرب جلوه نماید . حملات مخرب از این نوع شامل استراق سمع تعمدی ، سرقت و یا آسیب رسانی به اطلاعات ، استفاده از اطلاعات بطرزی کاملا" شیادانه و فریب آمیز و یا رد دستیابی سایر کاربران تایید شده باشد . حملات غیر مخرب از این نوع ، عموما" بدلیل سهل انگاری (حواس پرتی) ، فقدان دانش لازم و یا سرپیچی عمدی از سیاست های امنیتی صورت پذیرد.

توزیع . (Distribution) حملات از این نوع شامل کدهای مخربی است که در زمان تغییر سخت افزار و یا نرم افزار در محل مربوطه (کارخانه ، شرکت) و یا در زمان توزیع آنها (سخت افزار ، نرم افزار) جلوه می نماید . این نوع حملات می تواند، کدهای مخربی را در بطن یک محصول جاسازی نماید . نظیر یک درب از عقب که امکان دستیابی غیرمجاز به اطلاعات و یا عملیات سیستم در زمان آتی را بمنظور سوء استفاده اطلاعاتی ، فراهم می نماید .

در این رابطه لازم است ، به سایر موارد نظیر آتش سوزی ، سیل ، قطع برق و خطای کاربران نیز توجه خاصی صورت پذیرد . در بخش دوم این مقاله ، به بررسی روش های ایمن سازی اطلاعات بمنظور نیل به یک استراتژی خاص امنیتی ، خواهیم پرداخت.

نقش عوامل انسانی در امنیت شبکه های کامپیوتری

یک سیستم کامپیوتری از چهار عنصر : سخت افزار ، سیستم عامل ، برنامه های کاربردی و کاربران ، تشکیل می گردد. سخت افزار شامل حافظه ، دستگاههای ورودی ، خروجی و پردازشگر بوده که بعنوان منابع اصلی پردازش اطلاعات ، استفاده می گردند. برنامه های کاربردی شامل کمپایلرها ، سیستم های بانک اطلاعاتی ، برنامه های تجاری و بازرگانی ، بازی های کامپیوتری و موارد متنوع دیگری بوده که روش بخدمت گرفتن سخت افزار جهت نیل به اهداف از قبل تعریف شده را مشخص می نمایند. کاربران ، شا مل انسان ، ماشین و دیگر کامپیوترها می باشد . هر یک از کاربران سعی در حل مشکلات تعریف شده خود از طریق بکارگیری نرم افزارهای کاربردی در محیط سخت افزار می نمایند. سیستم عامل ، نحوه استفاده از سخت افزار را در ارتباط با برنامه های کاربردی متفاوتی که توسط کاربران گوناگون نوشته و اجراء می گردند ، کنترل و هدایت می نماید. بمنظور بررسی امنیت در یک سیستم کامپیوتری ، می بایست به تشریح و تبین جایگاه هر یک از عناصر موجود در یک سیستم کامپیوتری پرداخته گردد. در این راستا ، قصد داریم به بررسی نقش عوامل انسانی دررابطه با امنیت اطلاعات پرداخته و جایگاه هر یک از مولفه های موجود را تبین و تشریح نما ئیم . اگر ما بهترین سیستم سخت افزاری و یا سیستم عامل را بخدمت بگیریم ولی کاربران و یا عوامل انسانی درگیر در یک سیستم کامپوتری، پارامترهای امنیتی را رعایت ننمایند ، کاری را از پیش نخواهیم برد. وضعیت فوق مشابه این است که شما بهترین اتومبیل با درجه بالای امنیت را طراحی و یا تهیه نمائید ولی آن را در اختیار افرادی قرار دهید که نسبت به اصول اولیه رانندگی توجیه نباشند (عدم رعایت اصول ایمنی).

ما می بایست به مقوله امنیت اطلاعات در عصر اطلاعات نه بصورت یک کالا و یا محصول بلکه بصورت یک فرآیند نگاه کرده و امنیت را در حد یک محصول خواه نرم افزاری و یا سخت افزاری تنزل ندهیم .هر یک از موارد فوق ، جایگاه خاص خود را با وزن مشخص شده ای دارند و نباید به بهانه پرداختن به امنیت اطلاعات وزن یک پارامتر را بیش از آنچیزی که هست در نظر گرفت و پارامتر دیگری را نادیده گرفته و یا وزن غیر قابل قبولی برای آن مشخص نمائیم . بهرحال ظهور و عرضه شگفت انگیز تکنولوژی های نو در عصر حاضر ، تهدیدات خاص خود را نیز بدنبال خواهد داشت . ما چه کار می بایست بکنیم که از تکنولوژی ها استفاده مفیدی را داشته و در عین حال از تهدیدات مستقیم و یا غیر مستقیم آنان نیز مصون بمانیم ؟ قطعا" نقش عوامل انسانی که استفاده کنندگان مستقیم این نوع تکنولوژی ها می باشند ، بسیار محسوس و مهم است . با گسترش اینترنت و استفاده از آن در ابعاد متفاوت ، سازمانها و موسسات با مسائل جدیدی در رابطه با امنیت اطلاعات و تهاجم به شبکه های کامپیوتری مواجه می باشند. صرفنظر از موفقیت و یا عدم موفقیت مهاجمان و علیرغم آخرین اصلاحات انجام شده در رابطه با تکنولوژی های امنیتی ، عدم وجود دانش و اطلاعات لازم (سواد عمومی ایمنی) کاربران شبکه های کامپیوتری و استفاده کنندگان اطلاعات حساس در یک سازمان ، همواره بعنوان مهمترین تهدید امنیتی مطرح و عدم پایبندی و رعایت اصول امنیتی تدوین شده ، می تواند زمینه ایجاد پتانسیل هائی شود که توسط مهاجمین استفاده و باعث بروز مشکل در سازمان گردد. مهاجمان همواره بدنبال چنین فرصت هائی بوده تا با اتکاء به آنان به اهداف خود نائل گردند. در برخی حالات اشتباه ما زمینه موفقیت دیگران! را فراهم می نماید . اگر سعی نمائیم بر اساس یک روش مناسب درصد بروز اشتباهات خود را کاهش دهیم به همان نسبت نیز شانس موفقیت مهاجمان کاهش پیدا خواهد کرد.مدیران شبکه (سیستم) ، مدیران سازمان و کاربران معمولی جملگی عوامل انسانی در یک سازمان می باشند که حرکت و یا حرکات اشتباه هر یک می تواند پیامدهای منفی در ارتباط با امنیت اطلاعات را بدنبال داشته باشد . در ادامه به بررسی اشتباهات متداول خواهیم

پرداخت که می تواند توسط سه گروه یاد شده انجام و زمینه بروز یک مشکل امنیتی در رابطه با اطلاعات حساس در یک سازمان را باعث گردد .

اشتباهات متداول مدیران سیستم

مدیران سیستم ، به افرادی اطلاق می گردد که مسئولیت نگهداری و نظارت بر عملکرد صحیح و عملیاتی سیستم ها و شبکه موجود در یک سازمان را برعهده دارند.در اغلب سازمانها افراد فوق ، مسئولیت امنیت دستگاهها ، ایمن سازی شبکه و تشخیص ضعف های امنیتی موجود در رابطه با اطلاعات حساس را نیز برعهده دارند. بدیهی است واگذاری مسئولیت های متعدد به یک فرد، افزایش تعداد خطاء و اشتباه را بدنبال خواهد داشت . فشار عصبی در زمان انجام کار مستمر بر روی چندین موضوع متفاوت و بصورت همزمان ، قطعا" احتمال بروز اشتباهات فردی را افزایش خواهد داد. در ادامه با برخی از خطاهای متداولی که ممکن است توسط مدیران سیستم انجام و سازمان مربوطه را با تهدید امنیتی مواجه سازد ، آشنا خواهیم شد.

موردیک : عدم وجود یک سیاست امنیتی شخصی

اکثر قریب به اتفاق مدیران سیستم دارای یک سیاست امنیتی شخصی بمنظور انجام فعالیت های مهمی نظیر امنیت فیزیکی سیستم ها ، روش های بهنگام سازی یک نرم افزار و روشی بمنظور بکارگیری patch های جدید در زمان مربوطه نمی باشند .حتی شرکت های بزرگ و شناخته شده به این موضوع اذعان دارند که برخی از سیستم های آنان با همان سرعت که یک باگ و یا اشکال تشخیص و شناسائی می گردد ، توسط patch مربوطه اصلاح نشده است .در برخی حالات ، مدیران سیستم حتی نسبت به آخرین نقاط آسیب پذیرتشخییص داده شده نیز

آگاهی بهنگام شده ای را نداشته و قطعا" در چنین مواردی انتظار نصب patch مربوطه نیز توقعی بی مورد است . وجود نقاط آسیب پذیر در شبکه می تواند یک سازمان را در معرض تهدیدات جدی قرار دهد . امنیت فرآیندی است که می بایست بصورت مستمر به آن پرداخته شود و هرگز به اتمام نمی رسد.در این راستا لازم است، بصورت مستمرنسبت به آخرین حملات بهمراه تکنولوژی ها ی مربوطه ، آگاهی لازم کسب و دانش خود را بهنگام نمائیم .اکثر مدیران سیستم ، کارشناسان حرفه ای و خبره امنیتی نمی باشند ، در این رابطه لازم است ، بمنظور افزایش حفاظت و ایمن سازی شبکه ، اطلاعات و دانش مربوطه بصورت مستمر ارتقاء یابد .افرادیکه دارای گواهینامه های خاصی امنیتی و یا دانش و اطلاعات اضافه در رابطه با امنیت اطلاعات می باشند ، همواره یک قدم از کسانی مهارت آنان صرفا" محدود به شبکه است ، جلوتر می باشند . در ادامه ، پیشنهاداتی بمنظور بهبود وضعیت امنیتی سازمان و افزایش و ارتقاء سطح معلومات مدیران سیستم ، ارائه می گردد:

بصورت فیزیکی محل کار و سیستم خود را ایمن سازید .زمینه استفاده از سیستم توسط افرادیکه در محدوده کاری شما فعالیت دارند ، می بایست کاملا" کنترل شده و تحت نظارت باشد .

هر مرتبه که سیستم خود را ترک می کنید ، عملیات logout را فراموش نکنید .در این رابطه می توان یک زمان time out را تنظیم تا در صورت فراموش نمودن عملیات logout ، سیستم قادر به حفاظت خود گردد.

خود را عضو خبرنامه ها ی متفاوت امنیتی کرده تا شما را با آخرین نقاط آسیب پذیر آشنا نمایند. درحقیقت آنان چشم شما در این معرکه خواهند بود(استفاده مفید از تجارب دیگران).

سعی گردد بصورت مستمر از سایت های مرتبط با مسائل امنیتی دیدن تا درزمان مناسب با پیام های هشداردهنده امنیتی در رابطه با نرم افزارهای خارج از رده و یا نرم افزارهای غیر اصلاح شده (unpatched) آشنا گردید .

مطالعه آخرین مقالات مرتبط با مسائل امنیتی یکی از مراحل ضروری و مهم در فرآیند خود آموزشی (فراگیری) مدیران شبکه است . بدین ترتیب این اطمینان بوجود خواهد آمد که مدیر مربوطه نسبت به آخرین اطلاعات و مسائل مربوطه امنیتی در کمیته های موجود ، توجیه است.

استفاده از یاداشت ها و مقالات در ارتباط با هر نوع اطلاعات حساس نظیر رمزهای عبور و هر چیزی که ممکن است زمینه ساز ایجاد یک پتانسیل آسیب پذیر و دستیابی به سیستم مطرح گردد را محدود نمائید. در صورتیکه از این نوع اطلاعات استفاده می شود، قبل ازترک محل کار ، آنها را از بین ببرید. افرادیکه دارای سوء نیت بوده در محدوده کاری شما می باشند ، می توانند ازمزایای ضعف های شناخته شده استفاده نمایند، بنابراین ضروری است استفاده از چنین یاداشت هائی محدود و یا بصورت کامل حذف گردد.

مورد دو : اتصال سیستم های فاقد پیکربندی مناسب به اینترنت

همزمان با گسترش نیازهای سازمان، سیستم ها و سرویس دهندگان جدیدی بر اساس یک روال معمول به اینترنت متصل می گردند. قطعا" توسعه سیستم با هدف افزایش بهره وری در یک سازمان دنبال خواهد شد.اکثر اینچنین سیستمهائی بدون تنظیمات امنیتی خاص به اینترنت متصل شده و می تواند زمینه بروز آسیب و حملات اطلاعاتی توسط مهاجمان را باعث گردد (در بازه زمانی که سیستم از لحاظ امنیتی بدرستی ممیزی نشده باشد ، این امر امکان پذیر خواهد بود). مدیران سیستم ممکن است به این موضوع استناد نمایند که سیستم جدید بوده و هنوز کسی آن را نمی شناسد و آدرس IP آن شناخته شده نیست ، بنابراین امکان شناسائی و حمله به آن وجود نخواهد داشت .طرز فکر فوق ، یک تهدید برای هر سازمان بشمار می رود . افراد و یا اسکریپت های پویش اتوماتیک در اینترنت ، بسرعت عملیات یافتن و تخریب این نوع سیستم های آسیب پذیر را دنبال می نمایند. در این راستا ، شرکت هائی خاصی وجود دارد که موضوع فعالیت آنان شبکه بوده و برای تست سیستم

های تولیدی خود بدنبال سیستم های ضعیف و آسیب پذیر می گردند.(سیستم آسیب پذیر ما ابزار تست دیگران خواهد شد). بهرحال همواره ممکن است افرادی بصورت مخفیانه شبکه سازمان شما را پویش تا در صورت وجود یک نقطه آسیب پذیر، از آن برای اهداف خود استفاده نمایند. لازم است در این راستا تهدیدات و خطرات را جدی گرفته و پیگری لازم در این خصوص انجام شود. در این رابطه موارد زیر پیشنهاد می گردد:

قبل از اتصال فیزیکی یک کامپیوتر به شبکه ، مجوز امنیتی لازم با توجه به سیاست های تدوین شده امنیتی برای آن صادر گردد (بررسی سیستم و صدور مجوز اتصال)

کامپیوتر مورد نظر می بایست شامل آخرین نرم افزارهای امنیتی لازم بوده و از پیکربندی صحیح آنان می بایست مطمئن گردید. در صورتیکه لازم است بر روی سیستم مورد نظر تست های شبکه ای خاصی صورت پذیرد ، سعی گردد امکان دستیابی به سیستم فوق از طریق اینترنت در زمان تست ، بلاک گردد . سیستمی را که قصد اتصال آن به اینترنت وجود دارد ، نمی بایست شامل اطلاعات حساس سازمان باشد. سیستم مورد نظر را تحت برنامه های موسوم به Intrusion Detection System قرار داده تا نرم افزارهای فوق بسرعت نقاط آسیب پذیر و ضعف های امنیتی را شناسائی نمایند.

مورد سه : اعتماد بیش از اندازه به ابزارها

برنامه های پویش و بررسی نقاط آسیب پذیر،اغلب بمنظور اخذ اطلاعات در رابطه وضعیت جاری امنیتی شبکه استفاده می گردد . پویشگرهای تشخیص نقاط آسیب پذیر ، اطلاعات مفیدی را در ارتباط با امنیت سیستم نظیر : مجوزهای فایل ، سیاستهای رمز عبور و سایر مسائل موجود، ارائه می نمایند . بعبارت دیگر پویشگران نقاط آسیب پذیر شبکه ، امکان نگرش از دید یک مهاجم را به مدیریت شبکه خواهند داد. پویشگرها ی فوق ، عموما" نیمی از مسائل امنیتی مرتبط را به سیستم واگذار نموده و نمی توان به تمامی نتایج بدست آمده توسط آنان

بسنده و محور عملیات خود را بر اساس یافته های آنان قرار دهیم . در این رابطه لازم است متناسب با نوع سیستم عامل نصب شده بر روی سیستم ها از پویشگران متعدد و مختص سیستم عامل مربوطه استفاده گردد(اخذ نتایج مطلوبتر) . بهرحال استفاده از این نوع نرم افزارها قطعا" باعث شناسائی سریع نقاط آسیب پذیر و صرفه جوئی زمان می گردد ولی نمی بایست این تصور وجود داشته باشد که استفاده از آنان بمنزله یک راه حل جامع امنیتی است . تاکید صرف بر نتایج بدست آمده توسط آنان ، می تواند نتایج نامطلوب امنیتی را بدنبال داشته باشد . در برخی موارد ممکن است لازم باشد ، بمنظور تشخیص نقاط آسیب پذیر یک سیستم ،عملیات دستی انجام و یا حتی تاسکریپت های خاصی در این رابطه نوشته گردد.

مورد چهار : عدم مشاهده لاگ ها(Logs)

مشاهده لاگ های سیستم، یکی از مراحل ضروری در تشخیص مستمر و یا قریب الوقوع تهدیدات است . لاگ ها، امکان شناسائی نقاط آسیب پذیر متداول و حملات مربوطه را فراهم می نمایند. بنابراین می توان تمامی سیستم را بررسی و آن را در مقابل حملات مشخص شده ، مجهز و ایمن نمود. در صورت بروز یک تهاجم ، با استفاده از لاگ های سیستم ، تسهیلات لازم بمنظور ردیابی مهاجمان فراهم می گردد.(البته بشرطی که آنان اصلاح نشده باشند) . لاگ ها را بصورت ادواری بررسی و آنها را در یک مکان ایمن ذخیره نمائید .

مورد پنج : اجرای سرویس ها و یا اسکریپت های اضافه و غیر ضروری

استفاده از منابع و شبکه سازمان ، بعنوان یک زمین بازی شخصی برای تست اسکریپت ها و سرویس های متفاوت ، یکی دیگر از اشتباهات متداولی است که توسط اکثریت قریب به اتفاق مدیران سیستم انجام می شود . داشتن اینچنین اسکریپت ها و سرویس های اضافه ای که بر روی سیستم اجراء می گردند ، باعث ایجاد مجموعه

ای از پتانسیل ها و نقاط ورود جدید برای یک مهاجم می گردد (در صورتیکه سرویس های اضافه و یا اسکریپت ها بر روی سرویس دهنده اصلی نصب و تست گردند ، مشکلات می تواند مضاعف گردد). در صورت نیاز به تست اسکریپت ها و یا اجرای سرویس های اضافه ، می بایست عملیات مورد نظر خود را از طریق یک کامپیوتر ایزوله شده انجام داد (هرگز از کامپیوتری که به شبکه متصل است در این راستا استفاده نگردد).

انواع حملات در شبکه های کامپیوتری

حملات در یک شبکه کامپیوتری حاصل پیوند سه عنصر مهم سرویس ها ی فعال ، پروتکل های استفاده شده و پورت های باز می باشد . یکی از مهمترین وظایف کارشناسان فن آوری اطلاعات ، اطمینان از ایمن بودن شبکه و مقاوم بودن آن در مقابل حملات است (مسئولیتی بسیار خطیر و سنگین) . در زمان ارائه سرویس دهندگان ، مجموعه ای از سرویس ها و پروتکل ها به صورت پیش فرض فعال و تعدادی دیگر نیز غیر فعال شده اند.این موضوع ارتباط مستقیمی با سیاست های یک سیستم عامل و نوع نگرش آنان به مقوله امنیت دارد. در زمان نقد امنیتی سیستم های عامل ، پرداختن به موضوع فوق یکی از محورهائی است که کارشناسان امنیت اطلاعات با حساسیتی بالا آنان را دنبال می نمایند .اولین مرحله در خصوص ایمن سازی یک محیط شبکه ، تدوین ، پیاده سازی و رعایت یک سیاست امنیتی است که محور اصلی برنامه ریزی در خصوص ایمن سازی شبکه را شامل می شود . هر نوع برنامه ریزی در این رابطه مستلزم توجه به موارد زیر است :

- بررسی نقش هر سرویس دهنده به همراه پیکربندی انجام شده در جهت انجام وظایف مربوطه در شبکه
- انطباق سرویس ها ، پروتکل ها و برنامه های نصب شده با خواسته ها ی یک سازمان

- بررسی تغییرات لازم در خصوص هر یک از سرویس دهندگان فعلی (افزودن و یا حذف سرویس ها و پروتکل های غیرضروری ، تنظیم دقیق امنیتی سرویس ها و پروتکل های فعال).

تعلل و یا نادیده گرفتن فاز برنامه ریزی می تواند زمینه بروز یک فاجعه عظیم اطلاعاتی را در یک سازمان به دنبال داشته باشد . متاسفانه در اکثر موارد توجه جدی به مقوله برنامه ریزی و تدوین یک سیاست امنیتی نمی گردد . فراموش نکنیم که فن آوری ها به سرعت و به صورت مستمر در حال تغییر بوده و می بایست متناسب با فن آوری های جدید ، تغییرات لازم با هدف افزایش ضریب مقاومت سرویس دهندگان و کاهش نقاط آسیب پذیر آنان با جدیت دنبال شود . نشستن پشت یک سرویس دهنده و پیکربندی آن بدون وجود یک برنامه مدون و مشخص ، امری بسیار خطرناک بوده که بستر لازم برای بسیاری از حملاتی که در آینده اتفاق خواهند افتاد را فراهم می نماید . هر سیستم عامل دارای مجموعه ای از سرویس ها ، پروتکل ها و ابزارهای خاص خود بوده و نمی توان بدون وجود یک برنامه مشخص و پویا به تمامی ابعاد آنان توجه و از پتانسیل های آنان در جهت افزایش کارائی و ایمن سازی شبکه استفاده نمود. پس از تدوین یک برنامه مشخص در ارتباط با سرویس دهندگان ، می بایست در فواصل زمانی خاصی ، برنامه های تدوین یافته مورد بازنگری قرار گرفته و تغییرات لازم در آنان با توجه به شرایط موجود و فن آوری های جدید ارائه شده ، اعمال گردد . فراموش نکنیم که حتی راه حل های انتخاب شده فعلی که دارای عملکردی موفقیت آمیز می باشند ، ممکن است در آینده و با توجه به شرایط پیش آمده قادر به ارائه عملکردی صحیح ، نباشند .

وظیفه یک سرویس دهنده : پس از شناسائی جایگاه و نقش هر سرویس دهنده در شبکه می توان در ارتباط با سرویس ها و پروتکل های مورد نیاز آن به منظور انجام وظایف مربوطه ، تصمیم گیری نمود .

برخی از سرویس دهندگان به همراه وظیفه آنان در یک شبکه کامپیوتری به شرح زیر می باشد :

Logon Server : این نوع سرویس دهندگان مسئولیت شناسائی و تائید کاربران در زمان ورود به شبکه را برعهده دارند . سرویس دهندگان فوق می توانند عملیات خود را به عنوان بخشی در کنار سایر سرویس دهندگان نیز انجام دهند.

Network Services Server : این نوع از سرویس دهندگان مسئولیت میزبان نمودن سرویس های مورد نیاز شبکه را برعهده دارند . این سرویس ها عبارتند از :

- Dynamic Host Configuration Protocol (DHCP)
- Domain Name System (DNS)
- Windows Internet Name Service(WINS)
- Simple Network Management Protocol (SNMP)

Application Server : این نوع از سرویس دهندگان مسئولیت میزبان نمودن برنامه ها ی کاربردی نظیر بسته نرم افزاری Accounting و سایر نرم افزارهای مورد نیاز در سازمان را برعهده دارند.

File Server :از این نوع سرویس دهندگان به منظور دستیابی به فایل ها و دایرکتوری ها ی کاربران ، استفاده می گردد.

Print Server : از این نوع سرویس دهندگان به منظور دستیابی به چاپگرهای اشتراک گذاشته شده در شبکه ، استفاده می شود.

Web Server : این نوع سرویس دهندگان مسئولیت میزبان نمودن برنامه های وب و وب سایت های داخلی و یا خارجی را برعهده دارند.

FTP Server : این نوع سرویس دهندگان مسئولیت ذخیره سازی فایل ها برای انجام عملیات Downloadingو Uploading را برعهده دارند. سرویس دهندگان فوق می توانند به صورت داخلی و یا خارجی استفاده گردند.

Email Server : این نوع سرویس دهندگان مسئولیت ارائه سرویس پست الکترونیکی را برعهده داشته و می توان از آنان به منظور میزبان نمودن فولدرهای عمومی و برنامه های Gropuware ، نیز استفاده نمود .

News/Usenet (NNTP) Server : این نوع سرویس دهندگان به عنوان یک سرویس دهنده newsgroup بوده و کاربران می توانند اقدام به ارسال و دریافت پیام هائی بر روی آنان نمایند .

به منظور شناسائی سرویس ها و پروتکل های مورد نیاز بر روی هر یک از سرویس دهندگان ، می بایست در ابتدا به این سوال پاسخ داده شود که نحوه دستیابی به هر یک از آنان به چه صورت است ؟ : شبکه داخلی ، شبکه جهانی و یا هر دو مورد . پاسخ به سوال فوق زمینه نصب و پیکربندی سرویس ها و پروتکل های ضروری و حذف و غیر فعال

نمودن سرویس ها و پروتکل های غیرضروری در ارتباط با هر یک از سرویس دهندگان موجود در یک شبکه کامپیوتری را فراهم می نماید.

سرویس های حیاتی و موردنیاز

هر سیستم عامل به منظور ارائه خدمات و انجام عملیات مربوطه ، نیازمند استفاده از سرویس های متفاوتی است . در حالت ایده آل ، عملیات نصب و پیکربندی یک سرویس دهنده می بایست صرفا" شامل سرویس ها و پروتکل های ضروری و مورد نیاز به منظور انجام وظایف هر سرویس دهنده باشد. معمولا" تولید کنندگان سیستم های عامل در مستندات مربوطه به این سرویس ها اشاره می نمایند. استفاده از مستندات و پیروی از روش های استاندارد ارائه شده برای پیکربندی و آماده سازی سرویس دهندگان ،زمینه نصب و پیکربندی مطمئن با رعایت مسائل ایمنی را بهتر فراهم می نماید.

زمانی که کامپیوتری در اختیار شما گذاشته می شود ، معمولا" بر روی آن نرم افزارهای متعددی نصب و پیکربندی های خاصی نیز در ارتباط با آن اعمال شده است . یکی از مطمئن ترین روش ها به منظور آگاهی از این موضوع که سیستم فوق انتظارات شما را متناسب با برنامه تدوین شده ، تامین می نماید ، انجام یک نصب Clean با استفاده از سیاست ها و لیست ها ی از قبل مشخص شده است . بدین ترتیب در صورت بروز اشکال می توان به سرعت از این امر آگاهی و هر مشکل را در محدوده خاص خود بررسی و برای آن راه حلی انتخاب نمود. (شعاع عملیات نصب و پیکربندی را به تدریج افزایش دهیم) .

مشخص نمودن پروتکل های مورد نیاز

برخی از مدیران شبکه عادت دارند که پروتکل های غیرضروری را نیز بر روی سیستم نصب نمایند ، یکی از علل این موضوع ، عدم آشنائی دقیق آنان با نقش و عملکرد هریک از پروتکل ها در شبکه بوده و در برخی موارد نیز بر این اعتقاد هستند که شاید این پروتکل ها در آینده مورد نیاز خواهد بود. پروتکل ها همانند سرویس ها ، تا زمانی که به وجود آنان نیاز نمی باشد ، نمی بایست نصب گردند . با بررسی یک محیط شبکه با سوالات متعددی در خصوص پروتکل های مورد نیاز برخورد نموده که پاسخ به آنان امکان شناسائی و نصب پروتکل های مورد نیاز را فراهم نماید.

- به چه نوع پروتکل و یا پروتکل هائی برای ارتباط سرویس گیرندگان (Desktop) با سرویس دهندگان ، نیاز می باشد ؟
- به چه نوع پروتکل و یا پروتکل هائی برای ارتباط سرویس دهنده با سرویس دهنده ، نیاز می باشد ؟
- به چه نوع پروتکل و یا پروتکل هائی برای ارتباط سرویس گیرندگان (Desktop) از راه دور با سرویس دهندگان ، نیاز می باشد ؟
- آیا پروتکل و یا پروتکل های انتخاب شده ما را ملزم به نصب سرویس های اضافه ای می نمایند ؟
- آیا پروتکل های انتخاب شده دارای مسائل امنیتی خاصی بوده که می بایست مورد توجه و بررسی قرار گیرد؟

در تعداد زیادی از شبکه های کامپیوتری ،از چندین سیستم عامل نظیر ویندوز ، یونیکس و یا لینوکس ، استفاده می گردد . در چنین مواردی می توان از پروتکل TCP/IP به عنوان فصل مشترک بین آنان استفاده نمود. در ادامه می بایست در خصوص فرآیند اختصاص آدرس های IP تصیم گیری نمود (به صورت ایستا و یا پویا و به

کمک DHCP) . در صورتی که تصمیم گرفته شود که فرآیند اختصاص آدرس های IP به صورت پویا و به کمک DHCP ، انجام شود، به یک سرویس اضافه و با نام DHCP نیاز خواهیم داشت . با این که استفاده از DHCPمدیریت شبکه را آسانتر می نماید ولی از لحاظ امنیتی دارای درجه پائین تری نسبت به اختصاص ایستای آدرس های IP ، می باشد چراکه کاربران ناشناس و گمنام می توانند پس از اتصال به شبکه ، بلافاصله از منبع صادرکننده آدرس های IP ، یک آدرس IP را دریافت و به عنوان یک سرویس گیرنده در شبکه ایفای وظیفه نمایند. این وضعیت در ارتباط با شبکه های بدون کابل غیرایمن نیز صدق می نماید. مثلا" یک فرد می تواند با استقرار در پارکینگ یک ساختمان و به کمک یک Laptop به شبکه شما با استفاده از یک اتصال بدون کابل ، متصل گردد. پروتکل TCP/IP ، برای "معادل سازی نام به آدرس " از یک سرویس دهنده DNS نیز استفاده می نماید . در شبکه های ترکیبی شامل چندین سیستم عامل نظیر ویندوز و یونیکس و با توجه به این که ویندوز NT 4.0 و یا ۲۰۰۰ شده است ، علاوه بر DNS به سرویس WINS نیز نیاز می باشد . همزمان با انتخاب پروتکل ها و سرویس های مورد نیاز آنان ، می بایست بررسی لازم در خصوص چالش های امنیتی هر یک از آنان نیز بررسی و اطلاعات مربوطه مستند گردند(مستندسازی ، ارچ نهادن به زمان خود و دیگران است) . راه حل انتخابی ، می بایست کاهش تهدیدات مرتبط با هر یک از سرویس ها و پروتکل ها را در یک شبکه به دنبال داشته باشد.

مزایای غیرفعال نمودن پروتکل ها و سرویس های غیرضروری

استفاده عملیاتی از یک سرویس دهنده بدون بررسی دقیق سرویس ها ، پروتکل ها و پیکربندی متناظر با هر یک از آنان زمینه بروز تهدیدات و حملات را در یک شبکه به دنبال خواهد داشت . فراموش نکنیم که مهاجمان همواره قربانیان خود را از بین سرویس دهندگانی که به درستی پیکربندی نشده اند ، انتخاب می نمایند. بنابراین می بایست به سرعت در خصوص سرویس هائی که قصد غیرفعال نمودن آنان را داریم ، تصمیم گیری شود . قطعا" نصب سرویس ها و یا پروتکل هائی که قصد استفاده از آنان وجود ندارد ، امری منطقی و قابل قبول نخواهد بود. در صورتی که این نوع از سرویس ها نصب و به درستی پیکربندی نگردند ، مهاجمان می توانند با استفاده از آنان ، آسیب های جدی را متوجه شبکه نمایند . تهدید فوق می تواند از درون شبکه و یا خارج از شبکه متوجه یک شبکه کامپیوتری گردد . بر اساس برخی آمارهای منتشر شده ، اغلب آسیب ها و تهدیدات در شبکه یک سازمان توسط کارکنان کنجکا و و یا ناراضی صورت می پذیرد تا از طریق مهاجمان خارج از شبکه .

بخاطر داشته باشید که ایمن سازی شبکه های کامپیوتری مستلزم اختصاص زمان لازم و کافی برای برنامه ریزی است . سازمان ها و موسسات علاقه مندند به موازات عرضه فن آوری های جدید ، به سرعت از آنان استفاده نموده تا بتوانند از مزایای آنان در جهت اهداف سازمانی خود استفاده نمایند. تعداد و تنوع گزینه های انتخابی در خصوص پیکربندی هر سیستم عامل ، به سرعت رشد می نماید . امروزه وجود توانائی لازم در جهت شناسائی و پیاده سازی سرویس ها و پروتکل های مورد نیاز در یک شبکه خود به یک مهارت ارزشمند تبدیل شده است. بنابراین لازم است کارشناسان فن آوری اطلاعات که مسئولیت شغلی آنان در ارتباط با شبکه و ایمن سازی اطلاعات است ، به صورت مستمر و با اعتقاد به اصل بسیار مهم " اشتراک دانش و تجارب " ، خود را بهنگام

نمایند. اعتقاد عملی به اصل فوق ، زمینه کاهش حملات و تهدیدات را در هر شبکه کامپیوتری به دنبال خواهد داشت .

حملات(Attacks)

با توجه به ماهیت ناشناس بودن کاربران شبکه های کامپیوتری ، خصوصا" اینترنت ،امروزه شاهد افزایش حملات بر روی تمامی انواع سرویس دهندگان می باشیم . علت بروز چنین حملاتی می تواند از یک کنجکاوی ساده شروع و تا اهداف مخرب و ویرانگر ادامه یابد .

برای پیشگیری ، شناسائی ، برخورد سریع و توقف حملات ، می بایست در مرحله اول قادر به تشخیص و شناسائی زمان و موقعیت بروز یک تهاجم باشیم . به عبارت دیگر چگونه از بروز یک حمله و یا تهاجم در شبکه خود آگاه می شویم ؟ چگونه با آن برخورد نموده و در سریعترین زمان ممکن آن را متوقف نموده تا میزان صدمات و آسیب به منابع اطلاعاتی سازمان به حداقل مقدار خود برسد ؟ شناسائی نوع حملات و نحوه پیاده سازی یک سیستم حفاظتی مطمئن در مقابل آنان یکی از وظایف مهم کارشناسان امنیت اطلاعات و شبکه های کامپیوتری است .شناخت دشمن و آگاهی از روش های تهاجم وی ، احتمال موفقیت ما را در رویاروئی با آنان افزایش خواهد داد. بنابراین لازم است با انواع حملات و تهاجماتی که تاکنون متوجه شبکه های کامپیوتری شده است ، بیشتر آشنا شده و از این رهگذر تجاربی ارزشمند را کسب تا در آینده بتوانیم به نحو مطلوب از آنان استفاده نمائیم.

آشنایی با غول شبکه: سیسکو

شرکت سیسکو سیستمز (Cisco Systems) شرکت آمریکایی تولیدکنندهٔ تجهیزات شبکه (Network) است که مرکز آن در شهر سن خوزه در ناحیه معروف به سیلیکان ولی در ایالت کالیفرنیا قرار دارد. این شرکت محصولات مربوط به شبکه و ارتباطات را طراحی می‌کند و با سه نام تجاری مختلف سیسکو، لینکسیس و ساینتیفیک آتلانتا به فروش می‌رساند. در ابتدا، سیسکو فقط روترهای چند پروتکل تولید می‌کرد ولی امروز محصولات سیسکو را در همه جا از اتاق نشیمن گرفته تا شرکت‌های ارائه دهنده خدمات شبکه می‌توان پیدا کرد.دید سیسکو این است «تغییر روش زندگی، کار، بازی و آموزش.»

شرکت سیسکو هم اکنون با ۵۱۴۸۰ کارمند دارای بازده ۲۸,۴۸ میلیارد دلار در سال ۲۰۰۶ و سود خالص ۵,۵۸ میلیارد دلار می‌باشد. شعار فعلی سیسکو این است : «به شبکه انسان خوش آمدید». شرکت سیسکو در سال ۲۰۰۳ موفق به دریافت جایزه ریاست جمهوری ران براون برای کیفیت عالی در روابط کارمندان و جامعه گردید. معاون ارشد شرکت سیسکو یک ایرانی‌تبار به نام محسن معظمی است.

تاریچه

لن بزاک و سندی لرنر (دارای مدرک لیسانس از دانشگاه ایالتی کالیفرنیا، فوق لیسانس اقتصادسنجی از دانشگاه کلرمونت و فوق لیسانس علوم کامپیوتر از دانشگاه استنفورد)، زوجی که در بخش کامپیوتر دانشگاه استنفورد کار می‌کردند، Ciscoرا در سال ۱۹۸۴ تأسیس کردند. بزاک نرم افزار روترهای چند پروتکل را که توسط ویلیام یاگر(یک کارمند دیگر که کار سالها قبل از بزاک شروع کرده بود) نوشته شده بود تکمیل کرد.

با این وجود که Cisco اولین شرکتی نبود که Router طراحی و تولید می‌کند، اولین شرکتی بود که یک Routerچند پروتکل موفق تولید می‌کند که اجازهٔ ارتباط بین پروتکل‌های مختلف شبکه را می‌دهد. از زمانی که پروتکل اینترنت (IP) به یک استاندارد تبدیل شد، اهمیتRouter های چند پروتکل کاهش یافت. امروزه بزرگ‌ترین روترهای Cisco طراحی شده‌اند تا پاکت‌های IP و فریمهای MPLS را هدایت کنند. در ۱۹۹۰، شرکت به سهامی عام تبدیل شد و سهام آن در بازار بورس NASDAQ عرضه شد.بزاک و لرنر با ۱۷۰ میلیون دلار از شرکت خارج شدند و بعد از مدتی جدا شدند. زمان انفجار اینترنت در ۱۹۹۹، Ciscoشرکت Cerent واقع در کالیفرنیا را با قیمت ۷ میلیارد دلار خریداری کرد. این شرکت گرانترین خرید Cisco در آن زمان بود. تنها خرید گرانتر مربوط به ساینتیفیک آتلانتا می‌باشد.

در اواخر مارس ۲۰۰۰، در اوج رشد دات کام، Ciscoبا ارزش مالی بالغ بر ۵۰۰ میلیارد دلار ارزشمندترین شرکت دنیا بود.در سال ۲۰۰۷، با ارزشی بالغ بر ۱۶۵ میلیارد دلار همچنان یکی از ارزشمندترین شرکتهاست.

با خرید شرکت‌های دیگر، توسعهٔ داخلی و همکاری با دیگر شرکت‌ها، Ciscoبه بازار بسیاری از قطعات دیگر شبکه (غیر از Router) راه پیدا کرده‌است، مانندEthernet Switching ، دسترسی از راه دور، Routerهای شعبه‌ای، شبکهٔ خودپردازهای بانک‌ها، امنیت، دیواره آتش، تلفن اینترنتی و غیره. در ۲۰۰۳، Ciscoشرکت محبوب LinkSysتولید کنندهٔ سخت افزار شبکه کامپیوتر را خریداری کرد و آن را در صدر تولید کننده‌های قطعات مربوط به کاربران عادی تبدیل کرد.

آموزش

سیسکو در ۱۵۰ کشور دنیا مرکزهایی آموزشی به منظور تعلیم افراد برای طراحی و نگهداری شبکه‌های کامپیوتری تأسیس کرده‌است. سیسکو مدارکی را برای متخصصین در زمینه‌های مختلف شبکه ارائه می‌کند. که شامل این مدارک می‌شود:

- CCIE - Cico Certified Internetwork Expert(متخصص شبکه بندی سیسکو)
- CCNP - Cisco Certified Network Professional(حرفه‌ای شبکه سیسکو)
- CCDP - Cisco Certified Design Professional(حرفه‌ای طراحی سیسکو)
- CCIP - Cisco Certified Internetwork Professional(حرفه‌ای شبکه بندی سیسکو)
- CCSP - Cisco Certified Security Professional(حرفه‌ای امنیت سیسکو)
- CCVP - Cisco Certified Voice Professional(حرفه‌ای تلفن اینترنتی سیسکو)
- CCDA - Cisco Certified Design Associate(همکار طراحی سیسکو)
- CCNA - Cisco Certified Network Associate(همکار شبکه سیسکو)
- CCSI - Cisco Certified Systems Instructor(آموزش دهنده سیستم‌های سیسکو)

مدرک CCIE پیشرفته‌ترین و بالاترین مدرک ارایه شده توسط سیسکو در زمینه شبکه‌های کامپیوتری است. در هرم تحصیلی ارایه شده توسط شرکت سیسکو، مدرک CCNA به عنوان مدرک ورود به چرخه تحصیلی و کسب علوم شبکه‌ای در قاعده هرم قرار گرفته و عنوان نصب و پشتیبانی ادوات شبکه‌ای سیسکو را به خود اختصاص داده‌است. در همین سطح مدرک CCDA که ویژه طراحی مقدماتی شبکه‌های سیسکو می‌باشد نیز وجود دارد. در یک سطح بالاتر سه مدرکCCNP ، CCDPو CCIP لایه میانی این هرم را تشکیل داده و عنوان مدیریت شبکه‌های پیشرفته و پیچیده سیسکو را به خود اختصاص داده‌اند و بالاخره این‌که مدرک CCIE با قرار گرفتن در راس این هرم تحصیلی، به عنوان طراح اصلی و مدیریت رده بالای شبکه‌های سیسکو شناخته می‌شود.

ریشه نام سیسکو

اسم «سیسکو» مخفف سانفرانسیسکو است. با توجه به اظهارات جان مرگریج، کارمند ۳۴ ساله و مدیر پیشین شرکت، موسسان شرکت زمانی که داشتند به سمت ساکرامنتو رانندگی می‌کردند تا شرکت را به ثبت برسانند، با تصویر پل گلدن گیت در نور آفتاب مواجه می‌شوند و اسم و نماد شرکت را بر این اساس انتخاب می‌کنند. نماد شرکت منعکس کننده اصلیت سان فرانسیسکویی آن است، که نشان دهنده پل گلدن گیت است که به سبک خاصی طراحی شده‌است. در اکتبر ۲۰۰۶، سیسکو نماد جدید خود را که از نماد قبلی ساده تر و ساختیافته تر بود به معرض نمایش گذاشت.

انتقادها

یکی از انتقادهایی که به سیسکو وارد می‌شود، همکاری سیسکو با چین برای سانسور اینترنت در آن کشور است. سیسکو تأسیسات زیربنایی لازم را برای بستن وب‌گاه‌ها برای دولت چین تامین می‌کند. با این وجود، سیسکو ادعا می‌کند که تأسیسات و یا خدمات خاصی برای فیلترینگ وب‌گاهها به دولت‌ها نمی‌فروشد و فقط تجهیزاتی را به چین فروخته که در تمام دنیا عرضه می‌کند.به طور کلی سیسکو بهترین سازنده محصولات شبکه است.

سرویس‌های VoIP

سیسکو به یکی از ارائه دهندگان اصلی تلفن اینترنتی در سطح تجاری تبدیل شده‌است و حالا با خرید دو شرکت ساینتیفیک آتلانتا و لینکسیس می‌خواهد پا به بازار خانگی آن نیز بگذارد. ساینتیفیک آتلانتا تجهیزات لازم برای VoIPرا برای سرویس دهنده‌های کابلی مانند تایم وارنر، کابل ویژن، راجرز، UPCو دیگران ارائه می‌کند در حالی که لینکسیس با شرکتهایی مانند اسکایپی و یاهو برای ارائه خدمات VoIP با استفاده از تجهیزات بیسیم برای کاربران عادی همکاری می‌کند.