

انواع کامپیوترها

- ۱- ابر کامپیوترها
- ۲- کامپیوترهای بزرگ Main
- ۳- کامپیوترهای کوچک Mini
- ۴- کامپیوترهای شخصی P.C

انواع برنامه ها

- ۱- سیستم عامل
- ۲- زبانهای برنامه نویسی
- ۳- Package یا برنامه های آماده

تعریف سیستم عامل :

سیستم عامل نرم افزاری است که رابط بین استفاده کننده و کامپیوتر می باشد.

وظایف سیستم عامل :

- ۱- راه اندازی کامپیوتر
- ۲- گرفتن دستورات از User
- ۳- تجزیه و تحلیل دستورات
- ۴- اجرای دستورات
- ۵- مدیریت حافظه اصلی (Ram)
- ۶- مدیریت حافظه های جانبی

انواع سیستم عامل ها :

- ۱- سیستم عامل های تک کاربره Single user
- ۲- سیستم عامل های چند کاربره Multi user
- ۳- سیستم عامل های Multi programming

فصل اول

مزایای سیستم های چند کاربره (Main)

- ۱- دیسکهای پرظرفیت و سریع امکان کار با فایل های بسیار بزرگ را فراهم می کند.
- ۲- ترمینال های مقرون به صرفه تر از میکرو کامپیوترها هستند.
- ۳- سرعت پردازش در سیستم های چند کاربره بیشتر است.
- ۴- عملیات جاری سیستم مانند تهیه پشتیبان در این سیستم ها آسانتر است.

معایب سیستم های چند کاربره (Main)

- ۱- اگر سیستم دچار اشکال شود هیچ کدام از ایستگاه ها کار نمی کنند.
- ۲- هزینه نگهداری این سیستم ها معمولاً از شبکه های میکرو کامپیوتری بیشتر است.
- ۳- تعداد ایستگاه ها محدود تر از شبکه است.
- ۴- بسیاری از کاربران ممکن است از میکرو کامپیوترهایی داشته باشند این میکرو کامپیوترهای در یک سیستم چند کاربره تنها می توانند بصورت ترمینال استفاده شوند که این حداقل استفاده از امکانات وسیع یک میکرو کامپیوتر است.
- ۵- توسعه سیستم مشکل و در برخی موارد غیر ممکن است.
- ۶- افزایش تعداد ایستگاه ها زمان پاسخ سیستم را به سرعت کاهش می دهد زیرا پردازش در سیستم مرکزی صورت می گیرد.
- ۷- به علت استفاده از سیستم های عامل مثل UNIX آموزش کاربران برای استفاده از سیستم و تهیه برنامه های مناسب مشکل می باشد.

تعریف شبکه :

مجموعه ای از چند کامپیوتر مستقل که از طریق یک محیط ارتباطی با یکدیگر ارتباط دارند و می توانند عملیات انتقال داده را انجام دهند.

تقسیم بندی شبکه ها از نظر گستردگی

● شبکه های محلی (Lan) Local Area Network

شبکه محلی عبارتست از ارتباط یک سری کامپیوترهای شخصی یا ادوات کامپیوتری از طریق یک محیط مخابراتی تحت یک قانون و به کمک یک سیستم عامل در یک محدوده جغرافیایی محدود.

● شبکه های گسترده (Wan) Wide Area Network

شبکه های Wan محدودیت جغرافیایی ندارند و در اکثر موارد ، یک Wan از چندین Lan مرتبط با یکدیگر ایجاد می شود - شاید بتوان اینترنت را بزرگترین Wan در نظر بگیریم.

عوامل پیشرفت سریع شبکه عبارتند از :

- ۱- تعداد زیاد میکرو کامپیوترها.
- ۲- شبکه های محلی علاوه بر دارا بودن بسیاری از مزایای مینی کامپیوترها و کامپیوترهای بزرگ توانایی کار در محیط سیستم عامل عادی را نیز دارند.
- ۳- به وجود آمدن استانداردهای ملی و بین المللی در زمینه طراحی و کاربرد شبکه ها .
- ۴- شبکه های محلی دارای قابلیت توسعه خوبی هستند.
- ۵- در یک شبکه محلی سیستم همگام با نیاز سازمان توسعه می یابد و هزینه اضافی را به سازمان مربوطه تحمیل نمی کند.
- ۶- شبکه های محلی انعطاف پذیر و قابل اطمینان هستند.
- ۷- شبکه های محلی امکان استفاده مشترک از سخت افزار گران قیمت مانند هارد دیسکهای بزرگ ، چاپگرهای لیزری و دستگاه های تهیه پشتیبان را فراهم می کند.

تعریف Pack :

در شبکه های محلی برای سهولت در کنترل ترافیک اطلاعاتی در خطوط ارتباطی اطلاعات به بسته هایی با حجم کوچکتر تقسیم می شوند سپس آدرس مبدا، آدرس مقصد و اطلاعات مربوط به تصحیح خطا و ... به آن اضافه می شود. این بسته ها Packet نامیده می شوند.

OPEN SYSTEM

لایه های شبکه و مدل OSI
INTERCONNECT

مدل OSI معروفترین و معتبرترین استاندارد شبکه های محلی می باشد. این استاندارد رسمی به صورت یک مفهوم کلی ارائه شده و به عنوان چهار چوب اصلی برای تعریف بسیاری از قراردادهای ارتباطی (Communication Protocol) در شبکه های کامپیوتری به کار گرفته می شود. این مدل یک چهار چوب و طبقه بندی کلی برای ارتباط ارائه می دهد و به جزئیات و چگونگی برقراری ارتباط نمی پردازد. این مدل از هفت لایه تشکیل شده است. هر لایه از خدمات ارائه شده توسط لایه قبلی استفاده می کند و خدماتی را به لایه بعدی ارائه می دهد.

در حالت کلی وجود تمامی لایه ها الزامی نیست و ممکن است در یک شبکه یک یا چند لایه وجود نداشته باشد. مزیت طبقه بندی در این است که کلیه پردازش و فرایندهای انجام شده در لایه n ام بر اساس خدمات ارائه شده توسط لایه (n-1) ام طراحی می شود و بستگی به ساختار و نوع لایه های n-2 و قبل از آن ندارد. به این ترتیب شبکه هایی با قراردادهای متفاوت تنها در یک یا چند لایه با یکدیگر تفاوت خواهد داشت و ایجاد روشهایی برای برقراری ارتباط بین این شبکه ها ساده تر صورت می گیرد.

لایه های شبکه :

Physical	۱- لایه فیزیکی
Data link	۲- لایه ارتباط داده
Network	۳- لایه شبکه
Transmission	۴- لایه انتقال
Session	۵- لایه تماس
Presentation	۶- لایه نمایش
Application	۷- لایه کاربرد

📌 لایه فیزیکی (Physical) :

لایه فیزیکی با مشخصات الکتریکی و بیتها سر و کار دارد ، این بیتها در اینجا هیچ معنی ندارند و تجزیه و تحلیل این بیتها وظیفه لایه های بالاتر است . قراردادهای مربوط به سطوح و شکل موج ولتاژ و جریان در خط ، نوع مدلاسیون ، فرکانس کار ، نوع اتصالات و میانجی های محیط انتقال به این لایه مربوط است. ارتباط در این لایه ممکن است به صورت سری (یک بیت در لحظه) و یا موازی (چند بیت در یک لحظه) باشد . در هر یک از این دو صورت ممکن است روش انتقال Half Duplex یا Full Duplex باشد . در روش انتقال Half Duplex خط انتقال در آن واحد می تواند یا برای ارسال اطلاعات و یا برای دریافت اطلاعات به کار گرفته شود. در این روش ارسال و دریافت همزمان به وسیله یک خط ممکن نیست. اما در روش انتقال Full Duplex ارسال و دریافت همزمان اطلاعات توسط یک خط امکان پذیر است.

📌 لایه ارتباط داده ای (Data link) :

این لایه برقراری ارتباط بدون خط بین دو ایستگاه را به عهده دارد این لایه دیگر با بیتها سر و کار ندارد بلکه اطلاعات را بصورت Packet می شناسد. این لایه نشانه هایی برای مشخص کردن ابتدا و انتهای Packet به رشته اطلاعات می افزاید . آشکار سازی و اصلاح خطاها نیز در این لایه صورت می گیرد. تعیین زمان و نحوه دستیابی به خط نیز از وظایف این لایه است.

📌 لایه شبکه (Network) :

این لایه ایجاد مسیر مجازی مناسب برای ارسال اطلاعات را به عهده دارد ، در شبکه هایی که از مسیرهای مختلف برای انتقال اطلاعات استفاده می کنند این لایه مسیر مناسب برای برقراری یک ارتباط خاص را تعیین می کند. این لایه در صورت وجود می تواند چندین ارتباط (Connection) در لایه انتقال را به وسیله یک ارتباط در لایه Data link برقرار کند این کار به روش Multiplex صورت می گیرد.

📌 لایه انتقال (Transmission) :

این لایه پایین ترین لایه ای است که خدمات محلی به کاربر ارائه می دهد ، این لایه عمل مدیریت لایه های زیرین را از نظر کنترل فرایند ارتباط و جریان اطلاعات انجام می دهد. در این لایه خطاها آشکار و اصلاح می شوند و Packet هایی که با ترتیب غیر صحیح دریافت شده اند به حالت صحیح برگردانده می شوند به عبارت دیگر در این لایه مراحل نهایی کنترل صحت اطلاعات صورت می گیرد شروع ارتباط ، انتقال اطلاعات به لایه زیرین و ختم ارتباط توسط این لایه صورت می گیرد . وجود این لایه باعث می شود که لایه های بالاتر مستقل از نوع محیط نحوه دسترسی به خط و نحوه کنترل جریان اطلاعات به کار ادامه دهند.

📌 لایه تماس (Session) :

یک شبکه محلی کاربران را از طریق این لایه تشخیص می دهد کد عبور کاربران را کنترل کند و امکان تعویض حالت Half Duplex و Full Duplex را فراهم می کند همچنین این لایه تعیین می کند که چه کسی و در چه زمانی می تواند از شبکه استفاده کند . لایه تماس با مسائل مدیریتی شبکه سر و کار دارد و در صورت بروز اشکال در سیستم خروج از حالت اشکال توسط این لایه انجام می شود. در این لایه کاربران از نظر مقدار و چگونگی استفاده از شبکه کنترل می شوند.

📌 لایه نمایش (Presentation) :

این لایه با امنیت اطلاعات ، انتقال فایلها و قالب اطلاعات (فرمت) سر و کار دارد و به رمز درآوردن اطلاعات مهم ، بازگشایی رمز اطلاعات و ترجمه اطلاعات به قالبهای دیگر در این لایه صورت می گیرد . این لایه وظیفه تبدیل اطلاعات یک قرارداد (Protocol) به قرارداد دیگر را بر عهده دارد. حل مسائلی از قبیل اختلال در خطوط صفحه نمایش و اختلاف در کارکترست (کارکترهای هر کامپیوتر) بین دو ایستگاه از وظایف دیگر این لایه می باشد.

📌 لایه کاربرد (Application) :

این لایه واسطه ارتباطی کاربر با بقیه لایه هاست. ساختار این لایه بستگی زیادی به نیاز کاربران و سیستم عامل مورد استفاده دارد. انتقال پیام کاربران و تشخیص کاربران دیگر در شبکه نیز توسط امکانات این لایه صورت می گیرد. خدمات مربوط به انتقال فایلها ، برنامه های مدیریت بانکهای اطلاعاتی ، برنامه های فایل سرور ، پرینت سرور ، پست الکترونیکی و خط فرمان سیستم عامل در این لایه قرار دارد.

اجزاء شبکه های کامپیوتری :

Servers	۱- سرویس دهنده ها
Work Stations	۲- ایستگاه های کار
Net Work Interface Cards	۳- بردهای میانجی شبکه (کارتهای شبکه)
Communication System	۴- سیستم ارتباطی

📌 سرویس دهنده ها (Servers) :

یک سرویس دهنده عبارت است از سخت افزار و حداقل قسمتی از نرم افزار لازم برای ارائه یک سرویس به کاربران شبکه. در حالت کلی یک شبکه می تواند شامل سرویس دهنده های زیر باشد :

۱- Fail server : عضو لازم و اساسی یک شبکه است که می تواند یک کامپیوتر عادی در حال اجرای برنامه خاص و یا کامپیوتری با ساختار خاص باشد. این کامپیوتر قادر است بسیاری از امکانات سخت افزار خود از قبیل hard disk بزرگ و چاپگر خطی یا لیزری را بین کاربران شبکه به اشتراک بگذارد. سیستم عاملی که بر روی Fail server در حال اجراست تنها مدیریت و نظارت بر نحوه دسترسی کاربران به به فایل ها و امکانات جنبی را بر عهده دارد.

۲- Print server : دستگاه یا برنامه ای است که عملیات مدیریتی برای به اشتراک گذاشتن چاپگر را انجام می دهد.

۳- Data base server : دستگاه یا برنامه ای است که قابلیت به اشتراک گذاشتن hard disk خود با کاربران شبکه را دارد و تسهیلاتی برای بانکهای اطلاعاتی و انجام عملیات بر روی آنها در اختیار کاربر قرار می دهد. این سرویس دهنده ها عموماً دارای قابلیت های Multi tasking هستند و در هنگام استفاده از آنها قسمتی از پردازش در ایستگاه کار و قسمت دیگر در Data base server انجام می شود.

۴- Communication server : دستگاه یا برنامه ای است که خدمات مخابراتی لازم برای ارتباط کاربران شبکه و دستگاه های کامپیوتر خارج از شبکه را تامین می کند.

📌 ایستگاه های کار (Work Stations) :

میکرو کامپیوترهایی هستند که به یک شبکه متصل هستند و از امکانات مشترک آن استفاده می کنند ، اگر چه می توان امکانات سخت افزاری یا ایستگاه را در اختیار ایستگاه دیگر قرار داد اما Work Stations اصولاً برای به اشتراک گذاشتن امکانات در نظر گرفته نمی شوند . مشخصه اساسی ایستگاه های یک شبکه این است

که هوشمند هستند و می توانند پردازش انجام دهند ، این امر فرق اساسی بین ایستگاه های شبکه و ترمینال ها را تشکیل می دهد.

❶ کارتهای شبکه (Net Work Interface Cards) :

وظیفه برقراری ارتباط بین سیستم ارتباطی و ایستگاه های کار و فایل سرور را بر عهده دارند یکی دیگر از وظایف برد شبکه تشخیص زمان مناسب برای ارسال اطلاعات است. برای کنترل ترافیک اطلاعات در خطوط ارتباطی لازم است هر ایستگاه در شبکه در زمان مناسبی اقدام به ارسال اطلاعات کنند.

❷ سیستم ارتباطی شبکه :

وظیفه اصلی برقراری ارتباط بین اجزاء مختلف شبکه را بر عهده دارد . در تشکیل ساختار سیستم ارتباطی عوامل زیر دخالت دارند :

۱- همبندی یا Topology

۲- نحوه دستیابی به خط ارتباطی

۳- کانال ارتباط

❸ همبندی یا Topology : همبندی عبارت است از شکل هندسی اتصال دستگاه های درون شبکه .
اتصالهای رایج عبارتند از :

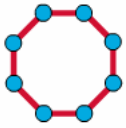
❶- تیپولوژی خطی یا Bus



در این همبندی ارتباط دستگاه ها از طریق یک رشته کابل که به ترتیب از یک دستگاه به دستگاه دیگر کشیده می شود برقرار می شود . پیامی که از طریق یک دستگاه بر روی کابل قرار داده می شود از دو مسیر انتقال یافته و توسط هر یک از دستگاه های دیگر قابل دریافت است از مزایای دیگر این روش راحتی نصب و قیمت ارزان آن است . یک عیب این سیستم این است که هر گاه اشکالی در یک از کابل رخ دهد کلیه ایستگاه های متصل به این کابل ارتباط با شبکه را از دست خواهند داد. در این روش طول کابل از ۱۸۰ متر نباید بیشتر باشد . اگر از طول بیش از ۱۸۰ متر استفاده شود به وسیله دستگاه Repeater که یک تقویت کننده است امواج تقویت می شوند.

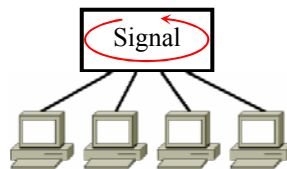


شکل ۱



۲- تیولوژی حلقوی یا Ring

در این همبندی مانند همبندی خطی کابل رابط از یک دستگاه به دستگاه دیگر متصل می شود با این تفاوت که دو سر آزاد کابل نیز به هم متصل هستند. ارسال پیام ها توسط هر دستگاه تنها در یک مسیر حرکت کرده و توسط اولین دستگاه همسایه که در مسیر قرار دارد قابل دریافت است. یک اشکال همبندی حلقوی این است که اضافه کردن و یا کم کردن تعداد ایستگاه های شبکه به سادگی صورت نمی گیرد. مزیت اساسی این سیستم ها کارایی خوب آنها در شبکه هایی با ترافیک بالا است.

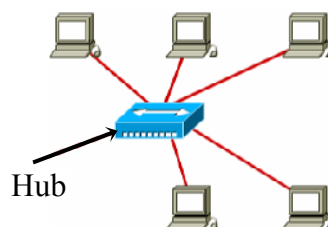


شکل ۲



۳- تیولوژی ستاره ای یا Star

در این همبندی هر دستگاه از طریق کابل رابط خاص خود به یک دستگاه مرکزی یا CENTRAL HUB بسته می شود. همبندی ستاره ای شباهت زیادی به همبندی سیستم های تلفن مرکزی دارد. از مزایای این روش سهولت انتخاب محل کامپیوترها و سرعت ارتباطی بالای آنهاست. و از معایب اینکه هزینه آن زیاد است.



شکل ۳

نحوه به اشتراک گذاشتن خطی :

از آنجا که در اکثر سیستم های شبکه کانال ارتباطی در یک زمان معینی تنها می تواند در اختیار یک ایستگاه باشد و از طرف دیگر هر یک از ایستگاه های شبکه در هر لحظه ممکن است احتیاج به استفاده از کانال ارتباطی داشته باشند لزوم رعایت یک روش و قانون مشخص برای دسترسی به محیط انتقال محسوس است . کارایی این روش می تواند نقش اساسی در کارایی کل شبکه داشته باشد . در یک سیستم شبکه سرعت انتقال اطلاعات بر حسب B/S (بیت بر ثانیه) تنها معیار سنجش سرعت سیستم نیست زیرا یک روش بد دسترسی به خط می تواند سرعت موثر انتقال اطلاعات را به شدت کاهش دهد . روشهای رایج به اشتراک گذاشتن خط عبارتند از :

۱- روش انتقال علامت :

در این روش که بسته (Pocket) خاص به نام علامت (Token) دائماً در محیط ارتباطی از دستگاهی به دستگاه دیگر در حال ارتباط است هر دستگاهی که Token را دریافت کند می تواند یکی از دو عمل زیر را انجام دهد :

۱-۱- در صورتیکه دستگاه مایل به ارسال پیام باشد ابتدا باید Token را از خط خارج کرده و سپس پیام خود را وارد خط کند پس از خاتمه ارسال ، دستگاه فرستنده باید مجدداً Token را وارد خط کرده و آن را به دستگاه بعدی ارسال کند.

۱-۲- در صورتیکه دستگاه مایل به ارسال پیام نباشد تنها باید آدرس علامت (Token) را عوض کرده آن را به دستگاه بعدی ارسال کند . مزیت این روش در این است که حتماً پس از طی زمان مشخص نوبت ارسال پیام به هر دستگاه خواهد رسید. از مزایای این سیستم این است که هر دستگاهی باید از آدرس دستگاه بعدی خود با خبر باشد.

۲- روش گوش دادن به خط Carrier Sense Multiple Access

این روش که نام مخفف آن CSMA/CD می باشد شبیه به روش صحبت کردن در یک اتاق شلوغ است، در چنین اتاقی شخصی که می خواهد صحبت کند باید با گوش دادن مطمئن شود که فرد دیگری در حال صحبت نیست و سپس اقدام به صحبت کند . پس در این روش هر برد میانجی شبکه (کارت شبکه) که در داخل یک کامپیوتر نصب شده است به صورت متوالی خط را تجزیه و تحلیل می کند هرگاه این ایستگاه پیامی برای ارسال داشته باشد پس از خالی شدن خط اقدام به ارسال پیام می کند . در این سیستم هرگاه دو کارت شبکه در یک لحظه پیامی در خط ارسال کنند پدیده برخورد یا Collision به وجود خواهد آمد. دو حرف CD در انتهای این روش مخفف Collision Detect می باشد.

هرگاه که یک برخورد صورت گیرد پیام محسوسی به نام Jam در خط ارسال می شود این پیام با تغییر سطح ولتاژ مستقیم در خط کلیه ایستگاه ها را از برخورد مطلع می کند سپس دو دستگاهی که در برخورد شرکت داشته اند هر یک به اندازه زمان تصادفی صبر می کنند و سپس در صورت خالی بودن خط اقدام به ارسال پیام می کنند . مزیت اساسی این سیستم سادگی و کارایی بسیار خوب در شرایط عادی است و اشکال عمده آن کم شدن کارایی سیستم در ترافیک بالاست.

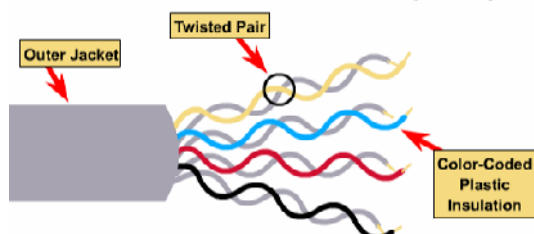
۳- کانال ارتباطی :

منظور از کانال ارتباطی محیط فیزیکی ارتباط دهنده اجزای شبکه است . محیطهای رایج برای ارتباط در شبکه های کامپیوتری عبارتند از :

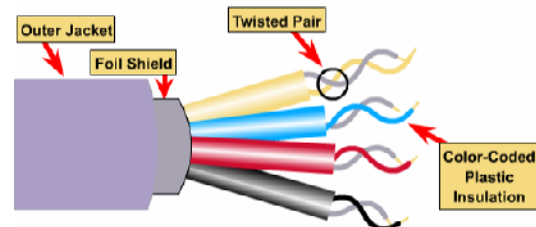
سیم تابیده شده :

ارزان ترین و معمول ترین و قدیمی ترین محیط ارتباطی در تکنولوژی ارتباط ، سیم تابیده شده است. دو رشته سیم روپوش دار برای کاهش نویز به هم تابیده شده اند تعداد کافی از این جفت سیم ها در داخل یک غلاف پلاستیکی قرار می گیرند و یک کابل را تشکیل می دهند . چنین کابلی را UTP (Unshielded Twisted Pair) می نامند . اگر مجموعه سیم های تابیده شده داخل یک غلاف آلومینیمی قرار داده شود ، کابل حاصل را STP (Shielded Twisted Pair) می نامند.

Unshielded Twisted Pair (UTP)



Shielded Twisted Pair (STP)





محدودیت‌های زیر در استفاده از این محیط وجود دارد :

عدم امنیت در مقابل تداخل خارجی و نویز :
به علت ساختار فیزیکی این نوع کابل ، نویز محیط و ارتعاشات الکترو مغناطیسی حاصل از وسایل و ادوات الکتریکی موجود در نزدیکی کابل ، می تواند عملکرد این محیط را با اشکال مواجه کند. این تداخل ممکن است حتی در اثر عبور کابل از نزدیکی یک لامپ فلوروسنت و یا یک دستگاه فتوکپی ایجاد شود . کابل‌های نوع STP از این نظر دارای امنیت نسبتاً بیشتری هستند.

تضعیف سیگنال الکتریکی :
با زیاد شدن طول کابل سیگنال الکتریکی در داخل سیم تضعیف می شود. این امر باعث می شود ارتفاع پالسهای حامل پیام کمتر از حد لازم شود و دستگاه هایی که در انتهای دیگر خط در حال تشخیص 0 و 1 هستند دچار خطا شوند.

خاصیت خازنی کابل :
با افزایش کابل دو سیم به هم تابیده شده با یکدیگر و با غلاف آلومینیمی ، خازنهایی را تشکیل می دهند. این خازنها به همراه مقاومت اهمی سیم یک ثابت زمانی ایجاد می کنند ، این امر باعث پهن شدن و تغییر فرم پالسهای حامل پیام شده و در نهایت موجب محدودیت فرکانس کار کابل می شود.

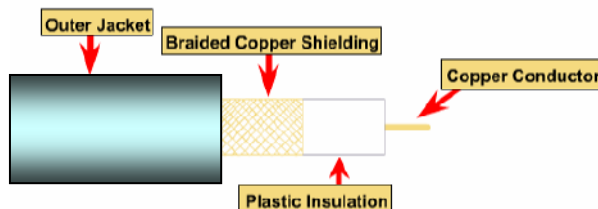
هم شنوایی (Cross talk)
علاوه بر تداخل الکتریکی خارجی ، تداخل حاصل از القای الکتریکی و مغناطیسی بین جفت سیم های داخل یک کابل نیز کار این نوع کابل را محدود می کند . این امر در مورد کابل‌های STP بیشتر رخ می دهد.

با وجود این محدودیتها ، در طول های محدود استفاده از این نوع محیط انتقال به علت قیمت ارزان و آسانی نصب ، بسیار رایج است.

کابل هم محور (Coaxial Cable)

این کابل یک هادی مفتولی نازک است که در داخل یک استوانه فلزی توخالی قرار گرفته است. فاصله بین هادی درونی و استوانه ای با یک عایق پر شده است، این کابل در فرکانس های بسیار بالا (تا حدود گیگا هرتز) قابل استفاده هستند. قابلیت استفاده در فرکانسهای بالا، به علاوه امنیت نسبت به نویز باعث شده که این کابلها کاربردهای بسیاری در تکنولوژی مخابرات پیدا کنند.

Coaxial Cable



در مقابل، اتصال و عملیات نصب این کابلها از سیم به هم تابیده شده مشکل تر و گرانتر می باشد. به علت بالا رفتن فرکانس در این کابلها، قوانین خطوط انتقال مخابراتی بر آنها حاکم است. طبق این قوانین برای هر کابل، از روی ابعاد سطح مقطع کابل و مشخصات فیزیکی بکار رفته در آن، یک مقاومت (بر حسب اهم) به دست می آید. این مقاومت را « مقاومت مشخصه » (Characteristic Impedance) کابل می نامند.

اهمیت این مقدار در این است که، هرگاه یک کابل به مقاومتی برابر با مشخصه اش منتهی شود، پیام الکتریکی فرستاده شده در خط، در برخورد به انتهای خط منعکس نمی شود. در غیر اینصورت در انتهای خط، انعکاس رخ می دهد و پیام منعکس شده با پیام بعدی که در حال ارسال است، تداخل می کند و محیط انتقال غیر قابل استفاده خواهد شد.

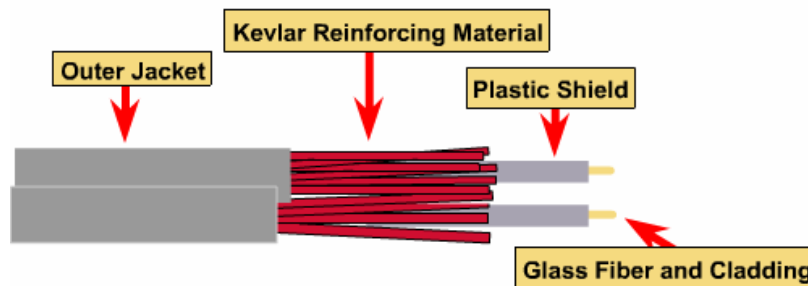
به هم این دلیل دو انتهای کابل هم محور، توسط مقاومتی برابر با مقاومت مشخصه کابل، مسدود می شود. این مقاومت را اصطلاحاً Terminator نامند.

همانطور که گفته شد ، مقاوت مشخصه کابل به ابعاد سطح مقطع آن بستگی دارد. هرگاه به دلیلی از قبیل فشرده شدن و یا خم شدن بیش از حد ، سطح مقطع کابل تغییر شکل یابد ، مقاوت مشخصه در این قسمت عوض شده و این قسمت مانند قطعه کابلی با مشخصه متفاوت عمل می کند.

فیبر نوری (Optical Fiber Cable)

کابل های فیبر نوری از بسیاری از جهات بر کابل های هم محور برتری دارند. این کابل ها به علت استفاده از نور بجای جریان الکتریکی ، از نظر نویز محیط بسیار امن هستند ، به علت پهنای باند بسیار زیاد ، می توانند ارتباط دیجیتال را بدون رابط های آنالوگ انجام دهند. علاوه بر این کابل های فیبر نوری را می توان تا فواصل دورتری به کار برد ، دارای وزن کمتری هستند ، جای کمتری اشغال می کنند و چون فلزی نیستند فرسودگی و زنگ زدگی آنها را تهدید نمی کند.

Fiber Optic Cable



این کابل ها از میله های بسیار نازکی از یک جنس شفاف مانند بروسلیکات ژرمانیم که در یک غلاف با ضرب شکست متفاوت قرار دارند ، ساخته شده اند. مجموعه ای از چند میله فیبر نوری و چند سیم فلزی ، که برای افزایش قدرت مکانیکی اضافه شده اند ، در یک غلاف پلاستیکی قرار می گیرند.

کابل های فیبر نوری به سه دسته اصلی تقسیم می شوند :

- | | |
|-----------------------|----|
| Step- index Multimode | -۱ |
| Grade-index Multimode | -۲ |
| Signal-Mode | -۳ |

کابل های Step- index Multimode دارای قیمت ارزانه تر و کیفیت پایین تری هستند و بیش از انواع دیگر فیبر نوری در شبکه های کامپیوتری مورد استفاده قرار می گیرند.

در کابل‌های Grade-index Multimode ضریب شکست محیط شفاف از مرکز تا سطح جانبی به تدریج کم می‌شود. در چنین کابلی روی دیواره های محیط شفاف بازتابش کلی نور صورت نمی‌گیرد، بلکه نور با بازتابش های جزئی یک مسیر منحنی را طی می‌کند.

کابل‌های Signal-Mode گران قیمت بوده و دارای پهنای باند بسیار زیادی هستند. این کابلها بسیار نازک هستند و انجام اتصالات روی آنها به سختی صورت می‌گیرد.

ارسال سیگنال در یک کابل نوری به وسیله دیودهای نوری LED (Light Emitting Diode) و یا دیودهای لیزری ILD (Injection Laser Diode) انجام می‌گیرد. این دیودها وظیفه تبدیل سیگنالهای الکتریکی به سیگنال نوری را بر عهده دارند. در طرف دیگر خط سیگنال نوری به وسیله دیودهای PIN مجدداً تبدیل به سیگنالهای الکتریکی می‌شود.

برای تقویت علائم ضعیف شده باید علائم نوری به علائم الکتریکی تبدیل شده، تقویت شده و مجدداً به علائم نوری تبدیل شوند. در سال ۱۹۹۰ تقویت کننده نوری که سیگنال نوری را بدون تبدیل به سیگنال الکتریکی تقویت می‌کند ساخته شد.

در صورتیکه مسائل موجود در ایجاد اتصالات انشعابی روی فیبرهای نوری حل شود، این کابل را می‌توان محیط انتقال ایده آلی برای شبکه های کامپیوتری دانست.

فصل دوم

قراردادهای شبکه کامپیوتری

یک قرارداد شبکه مجموعه ای از روشها و ضوابط ارتباطی است که شامل قوانینی در باره چگونگی انجام قسمتی و یا تمامی مراحل ارتباط می شود. وجود این قراردادها تولید کنندگان بردهای شبکه و ادوات سخت افزاری و نرم افزاری دیگر مربوط به شبکه را به رعایت روشهای ثابتی برای انجام قسمتهای مختلف فرایند ارتباط ملزم می کند. این امر موجب می شود که محصولات تولید کنندگان مختلف که برای کار با یک قرارداد بخصوص ساخته شده اند بدون ایجاد مشکل در کنار هم کار کنند.

۱- قرارداد Ethernet :

این قرارداد در لایه فیزیکی مدل OSI کار می کند. در یک سیستم Ethernet که یک سیستم ارتباطی غیر فعال است به این معنی که شبکه به وسیله ایستگاه ها تغذیه می شود از همبندی مسیر و روش دستیابی به خط CSMA/CD استفاده می شود. سرعت انتقال اطلاعات 10Mb/S و هر ایستگاه از طریق یک کنترل کننده و یک Transceiver به کابل اصلی شبکه متصل می شود. این قرارداد چگونگی ارتباط بین ایستگاه ها را مشخص می کند و محیط انتقال در این قرارداد مشخص نمی شود. محیط های زیر برای کار با قرارداد Ethernet در نظر گرفته می شود.

کابل هم محور قطور با مقاومت مشخصه 50Ω RG-8

کابل هم محور نازک با مقاومت مشخصه 50Ω RG-68

سیم تابیده شده (شماره ۲۲ و ۲۴) با مقاومت مشخصه 150Ω

کابل فیبر نوری با قطر ۱۰۰ و ۱۲۰ و ۱۴۰ میکرون

۲- قرارداد IEEE802.3 :

این قرارداد بسیار شبیه به Ethernet است و مانند Ethernet از روش CSMA/CD برای دستیابی به خط ارتباطی استفاده می کند. این قرارداد در لایه فیزیکی و قسمتی از لایه Data Link کار می کند. لایه Data Link در این قرارداد به دو لایه MAC و LLC تقسیم می شود:

MAC → Media Access Control
 LLC → Logical Link Control

نحوه کار لایه MAC در قرارداد IEEE802.3 و چگونگی عمل لایه LLC در لایه IEEE802.2 قرار دارد.

۳- قرارداد IEEE802.5 : سیستم Token Ring

مانند قرارداد IEEE802.3 در لایه فیزیکی و بخش MAC از لایه Data Link کار می کند این سیستم امکان اتصال میکرو کامپیوترها به مینی کامپیوترها و کامپیوترهای بزرگ ساخت شرکت IBM را فراهم می کند.

در Token Ring از همبندی حلقه و روش انتقال علامت استفاده می شود. محیط انتقال سیم به هم تابیده و کابل هم محور است. اگرچه همبندی سیستم از نوع حلقه ای است اما به ظاهر مانند همبندی ستاره به نظر می رسد. زیرا حلقه به همراه دیگر تجهیزات لازم درون دستگاهی به نام MAU (Multi Station Access Unit) قرار گرفته و هریک از ایستگاه ها به وسیله یک خط ارتباطی به MAU متصل می شوند.

۴- قرارداد ARCNET : (Attached Resource Computer Network)

از همبندی Star روش انتقال علامت استفاده می کند. محیط انتقال در این سیستم می تواند سیم به هم تابیده و کابل هم محور RG62 (93Ω) و یا فیبر نوری باشد. انعطاف پذیری، قابلیت گسترش، کارایی خوب و قیمت ارزان Arcnet باعث شده است که این سیستم بعد از Ethernet پر فروش ترین سیستم شبکه باشد.

در این سیستم کلیه دستگاه ها به یک سیستم مرکزی به نام HUB متصل می شوند. با گسترش شبکه می توان HUB های دیگری را نیز به شبکه افزود. حداکثر فاصله یک ایستگاه از یک HUB فعال برابر ۶۰۰ متر می باشد. عیب یابی و رفع اشکالات مربوط به کابل برای Arcnet آسان است زیرا بدون اختلال در کار ایستگاه های شبکه می توان کابل های مربوط به یک ایستگاه را از شبکه جدا کرد.

۵- قرارداد TCO/IP

در اوایل دهه ۱۹۹۰، Vinton cref در دانشگاه Stanford این قرار داد را که نام آن مخفف Transmission Control Protect / Internet Protocol است بنا نهاد. این قرارداد برای ارتباط بین کامپیوترهای مختلف با قراردادهای متفاوت ایجاد شد. امروزه TCP/IP به عنوان بهترین قرارداد بین برای ارتباط بین شبکه ها با قراردادهای مختلف و ارتباط بین شبکه های میکرو کامپیوتری و کامپیوترهای بزرگ شناخته می شود. اگر چه TCP/IP در ابتدا یک مدل ارتباطی مانند مدل OSI بوده است، اما با گسترش استفاده از مدل OSI، امروزه TCP/IP بیش از آنکه بصورت یک مدل ارتباطی شناخته شود به عنوان مجموعه ای از قرارداد در لایه های مدل OSI مورد قبول است.

TCP/IP خدمات ارتباطی را در دو سطح ارائه می دهد. IP در لایه شبکه از مدل OSI کار می کند و خدمات TCP در لایه انتقال آغاز شده و می تواند تا لایه نمایش ادامه یابد. در واقع TCP از خدمات ارائه شده توسط IP استفاده می کند.

TCP در ایستگاه مبدا اطلاعاتی را که از لایه بالاتر دریافت می کند، به بسته هایی به نام Segment تقسیم می کند. IP پس از دریافت این بسته ها اطلاعات مربوط به لایه شبکه را به آنها می افزاید. بسته های اطلاعات در IP را اصطلاحاً Data gram می نامند. این Data gram ها از طریق لایه های زیرین به لایه شبکه در ایستگاه مقصد منتقل می شوند. در ایستگاه مقصد عمل عکس انجام می گیرد و Data gram ها اطلاعات بصورت Segment استخراج شده و از روی Segment ها اطلاعات بازیابی می شود.

IP قراردادی در لایه شبکه است که امکان ارتباط بین شبکه های ناهمگون را ایجاد می کند، با استفاده از این قرارداد ایستگاه های متعلق به دو شبکه متفاوت می توانند با یکدیگر ارتباط برقرار کنند. این قرارداد مستقل از ساختار و قراردادهای موجود در لایه های فیزیکی و Data Link کار می کند. معمولاً قرارداد IEEE802.3 برای کار در کنار TCP/IP در نظر گرفته می شود.

در IP یک مسیر منطقی ثابت بین ایستگاه فرستنده و ایستگاه گیرنده برقرار نمی شود، بلکه ممکن است Data gram ها برای انتقال از مبدا به مقصد مسیرهای مختلفی را طی کنند. هنگامی که چند Data gram به ترتیب از مبدا به مقصد ارسال می شوند، به علت عدم وجود یک مسیر ثابت برای عبور همه آنها، ممکن است با ترتیب نادرست به مقصد برسند.

IP همچنین تضمینی برای رسیدن پیام از مبدا به مقصد نمی دهد و ایجاد اطمینان از رسیدن پیام به مقصد در TCP صورت می گیرد.

TCP ترتیب ارسال Segment ها را در هر Segment ثبت می کند و از روی این اطلاعات، در مقصد Segment هایی را که ممکن است با ترتیب نادرست دریافت شده باشند مرتب می کند. ضمناً با دریافت پیام تایید، از رسیدن پیام به مقصد اطمینان حاصل می شود.

در یک مجموعه از شبکه ها که از TCP/IP استفاده می کنند Data gram مهلتی برای رسیدن به مقصد دارد. اگر پس از انقضای این مهلت Data gram به وسیله ایستگاهی دریافت نشود از بین می رود. این امر برای جلوگیری از وجود Data gram های سرگردان و افزایش بی مورد ترافیک شبکه در نظر گرفته شده است.

فصل سوم

نرم افزار شبکه

قسمتهایی از شبکه محلی که تا کنون بررسی شدند ، مجموعه نیازهای سخت افزاری برای یک شبکه را برطرف می سازند . سیستم عامل شبکه ، به همراه سیستم عامل ایستگاهها و برنامه های کاربردی ، جوابگویی به نیازهای نرم افزاری را به عهده دارد.

نرم افزار File Server

نرم افزار File Server قلب یک شبکه محلی و بخش اساسی نرم افزار شبکه است و خدمات لازم جهت انجام عملیات اساسی شبکه را ارائه میدهند .

به عنوان مثال ، سیستم بایگانی شبکه ، مدیریت حافظه (Memory Management) و نوبت دهی کاربران برای دریافت خدمات را میتوان نام برد . برای ایجاد نرم افزار FILE Server دو راه وجود دارد . راه اول این است که یک سیستم عامل چند کاره (Multitasking) مخصوص اینکار نوشته شود ، و راه دوم آن است که نرم افزار File Server بر روی یکی از سیستم عاملهای چند کاره مانند OS2 , UNIX نوشته شود .

برخی از تولید کنندگان نرم افزار File Server ، مانند Banyan و Microsoft راه حل دوم را برگزیده اند. نرم افزار Vines از شرکت Banyan ، از سیستم عامل UNIX استفاده می کند و LAN Manager محصول Microsoft تحت سیستم عامل OS2 اجرا میشود .

Vines ➡

Vines محصول شرکت Banyan یک نرم افزار مدیر شبکه بر روی سیستم عامل Unix است که از امکانات این سیستم عامل ، به نحو احسن بهره برداری میکند . مزیت استفاده از یک سیستم عامل آماده ، به عنوان بستری برای نرم افزار شبکه این است که ، برنامه های کاربردی موجود بر روی سیستم عامل مزبور به راحتی میتوانند مورد استفاده نرم افزار شبکه قرار گیرند .

از مزایای Vines امکان به اشتراک گذاشتن هارد دیسک ایستگاه ، امکان ارتباط با سیستمهای بزرگ با قراردادهای TCP/IP و SNA ، و امکانات بسیار قوی مخابراتی را میتوان نام برد . در یک سیستم شبکه با نرم افزار Vines ، کاربری که از طریق خط تلفن وارد شبکه می شود ، میتواند از تمامی امکانات یک کاربر در داخل شبکه استفاده کند . Vines اکنون یکی از نرم افزارهای پر فروش شبکه است .

Netware

پرفروشترین نرم افزار شبکه ، سیستم عامل Netware از شرکت Novell است . این شرکت برای تولید یک نرم افزار شبکه ، ایجاد یک سیستم عامل را ترجیح داد از آنجا که Netware سیستم عاملی است که مخصوص شبکه نوشته شده است ، به علت نزدیکی بیشتر به سخت افزار سیستم ، دارای سرعت و کارایی بیشتری است . این سیستم عامل که بر روی اکثر سیستم های سخت افزاری ، با همبندی های مختلف قابل اجراء است ، دارای توانایی های بسیاری است . در ادامه ، به بررسی برخی قابلیت هایی که Netware را به یک نرم افزار شبکه ای ایده آل برای مصارف عمومی تبدیل کرده است ، میپردازیم .

نگهداری دو کپی از جداول محل فایلها (File Allocation Table)

از آنجا که هارد دیسک شبکه حاوی اطلاعات مشترک عده ای از کاربران است و این اطلاعات میتواند بسیار ارزشمند باشد سیستم عامل Netware برای جلوگیری از خطر از دست رفتن اطلاعات به علت از دست رفتن FAT (file Allocation Table) ، یک کپی از FAT را در محل دیگری از هارد دیسک نگهداری می کند . سیستم عامل Netware STF امکان نگهداری کل اطلاعات در دو هارد دیسک مجزا را فراهم می کند . این دو هارد دیسک کاملاً یکسان بوده و عملیات نوشتن بطور همزمان روی هر دو هارد دیسک اجرا می شود . در صورت از دست رفتن اطلاعات موجود بر روی یکی از هارد دیسکها ، اطلاعات موجود بر روی دیگری می تواند مورد استفاده قرار گیرد . این امر امکان دستیابی به شبکه هایی با قابلیت اطمینان بسیار بالا را فراهم می کند .

کنترل کیفیت سطح هارد دیسک هنگام نوشتن و Hot Fix Redirection

Netware پس از نوشتن هر بلوک بر روی هارد دیسک ، آنرا می خواند . چنانچه محتوی بلوک با اطلاعات نوشته شده مطابقت نکند ، آدرس این محل را یادداشت کرده و اطلاعات را در محل دیگری به نام Hot Fix که مخصوص این کار است می نویسد .

این عمل از خراب شدن اطلاعات به علت بروز اشکال در سطح هارد دیسک جلوگیری می کند . در ضمن محل فوق به عنوان Bad Block شناخته شده و از این پس چیزی در آن نوشته نمی شود .

حداکثر استفاده از حافظه

علیرغم سیستم عامل DOS که بطور عادی تنها از 640 KB از حافظه سیستم استفاده می کند. Netware از تمامی حافظه استفاده می کند. این امر توانایی عملیاتی Elevator , Disk Caching , Disk Hashing , Seeking را فراهم می کند . در ضمن این سیستم عامل کلیه عملیات نگهداری موقت اطلاعات (Buffering) و کنترل وضعیت کاربران شبکه را به کمک حافظه انجام می دهد.

Disk Hashing

File Server اطلاعات مربوط به محل فایل های روی دیسک را در RAM نگهداری می کند. هنگامیکه یک کاربر تقاضای دریافت یک فایل را به File Server می فرستد محل این فایل به سرعت در Ram پیدا شده و سرویس دهی به سرعت انجام می گیرد.

Disk Caching

هر گاه یک کاربر تقاضای دریافت فایلی را به File Server بفرستد Netware اطلاعات قسمتی از هارد دیسک را که مربوط به این فایل است کلاً به Ram منتقل می کند هرگاه اطلاعات دیگری مربوط به این قسمت از هارد دیسک تقاضا شود ، سرویس دهی بجای هارد دیسک از Ram صورت می گیرد. از آنجا که زمان دستیابی به اطلاعات در هارد دیسک در حد میلی ثانیه و در Ram در حد میکروثانیه است ، این عمل سرعت جوابگویی File Server را بیش از صد برابر افزایش می دهد . علاوه بر این انجام عملیات نوشتن بر روی هارد دیسک برای یک کاربر ، در حین سرویس دهی به کاربر دیگر امکان پذیر است.

Elevator Seeking

برای درک بهتر مفهوم Elevator Seeking فرض کنید یک کارمند بایگانی در حال پیدا کردن پرونده های افراد موجود در یک لیست است و اسامی این افراد به ترتیب ابطحی ، محمدی ، ثقفی و ... است. کارمند پس از پیدا کردن پرونده ابطحی قبل از آنکه به دنبال پرونده محمدی در انتهای حروف الفبا بگردد ، به دنبال پرونده ثقفی که نزدیک به ابطحی قرار دارد ، خواهد گشت. سپس به سراغ پرونده محمدی خواهد رفت. یک File Server که تحت سیستم عامل Netware کار می کند ، عیناً همین عوامل را در مورد سرویس دهی از هارد دیسک انجام می دهد. گرچه File Server کاربران شبکه را برای دریافت سرویس در نوبت قرار می دهد ، اما سرویس دهی به تقاضاهایی که مربوط به محلی در نزدیکی محل فعلی هد هارد دیسک باشند خارج از نوبت انجام می گیرد.

ارتباط DOS و سیستم عامل شبکه

در یک ایستگاه شبکه، کاربر باید در کنار توانایی انجام عملیات محلی، قادر به برقراری ارتباط با شبکه باشد. در عین حال ایستگاه به علت نیاز به نرم افزارهای استاندارد بر روی سیستمهای عامل رایج، نمی تواند تحت سیستم عامل ویژه ای کار کند. در نتیجه قسمتی از نرم افزار شبکه که در ایستگاه اجرا می شود باید یک برنامه اجرایی تحت یکی از سیستمهای عامل رایج باشد و چون ایستگاه ممکن است متوالیاً عملیات محلی و شبکه ای انجام دهد، این برنامه باید در حافظه ماندگار (Resident) باشد.

سیستم عامل Netware، بر خلاف بسیاری از نرم افزارهای دیگر، استفاده کننده را ملزم به داشتن سیستم عامل خاصی در ایستگاه، نمی کند. این سیستم عامل امکان استفاده از مجموعه ای از سیستمهای عامل مختلف را، در یک شبکه فراهم می کند.

سیستم عامل Netware از مجموعه ای بنام shell استفاده می کند. در شبکه ای که ایستگاههای آن از DOS استفاده می کنند، shell از دو برنامه اجرایی تشکیل شده است، اولین برنامه که IPX.COM نام دارد، وظیفه فرستادن پیامها برای File server، و در برخی موارد برای دیگر ایستگاهها، را به عهده دارد. قسمت دوم NET3.COM و یا NET4.COM است. وقتی که کاربر دستوری را وارد می کند، این برنامه تصمیم می گیرد که این دستور مربوط به عملیات محلی یا مربوطه به شبکه است. اگر دستور وارد شده مربوط به عملیات محلی باشد، عیناً به DOS منتقل می شود، در غیر اینصورت از طریق شبکه اجرا خواهد شد. در فصل ۴ با جزئیات نحوه کار shell در ایستگاه شبکه آشنا خواهید شد.

تدابیر نرم افزاری خاص شبکه

سیستم عامل شبکه امکانات موجود در شبکه را از طریق یکی از مفاهیم قابل درک برای سیستم عامل ایستگاه (مانند Drive) های سیستم عامل ایستگاه رفتار کند.

اما برای یک نرم افزار شبکه ای، تنها قابلیت اجرا از روی Drive شبکه کافی نیست. مزیت اساسی یک شبکه محلی، این است که به چند کاربر امکان کار بر روی یک موضوع واحد را می دهد. برای آن که در یک لحظه، چند کاربر بتوانند روی اطلاعات مشترکی کار کنند، لازم است در برنامه مورد نظر تدابیر خاصی برای کار کردن چند کاربر بر روی یک سری اطلاعات خاص، رعایت شود. به عنوان مثال، فرض کنید در یک شبکه محلی دو نفر در یک لحظه در حال کار روی یک فایل هستند. اگر هر دو کاربر اقدام به ضبط اطلاعات کنند، این امر می تواند باعث از دست رفتن اعتبار اطلاعات و یا از دست رفتن فایل مزبور شود. یک سیستم عامل شبکه، برای جلوگیری از بروز این حالت روشها و امکاناتی ارائه می دهد. این روشها به دو دسته اساسی تقسیم می شوند.

۱- روش قفل (lock) برای ایجاد هماهنگی در دسترسی به اطلاعات موجود در پرونده های مشترک

۲- روش Semaphore برای ایجاد هماهنگی در دسترسی مشترک به سایر امکانات شبکه

♦ روش قفل (Lock)

روش قفل ، روشی است که توسط سیستم عامل شبکه برای ایجاد هماهنگی در دسترسی مشترک به محتویات یک فایل و یا یک رکورد به کار می رود. در این روش هر برنامه ای که بخواهد به یک فایل و یا یک رکورد دسترسی داشته باشد از سیستم عامل می خواهد که فایل یا رکورد مربوطه را قفل کند. اگر فایل یا رکورد مورد درخواست این برنامه توسط برنامه دیگر قفل شده باشد این امر از طرف سیستم عامل به برنامه اعلام می شود. در غیر این صورت قفل گذاری انجام شده و این برنامه با اطمینان از اینکه برنامه دیگری در کار آن دخالت نخواهد کرد ، به کار خود ادامه خواهد داد. در پایان کار برنامه با ارسال درخواست دیگری از سیستم عامل می خواهد که قفل را بردارد.

یک سیستم عامل شبکه ممکن است انواع مختلفی از قفل را در اختیار برنامه ها قرار دهد. یک برنامه می تواند از تمامی و یا بعضی از انواع قفل استفاده کند.

از نظر عملکرد قفل ها را می توان به طریق زیر دسته بندی کرد :

قفل فیزیکی (Physical) و منطقی (Logical)

قفل های باصبر (Wait) و بدون صبر (NO Wait)

قفل های قابل اشتراک (Shareable) و انحصاری (Exclusive)

به عنوان مثال ممکن است یک برنامه از سیستم عامل قفل فیزیکی بدون صبر انحصاری تقاضا کند. در این قسمت در مورد هر یک از این دسته بندی ها توضیحاتی داده می شود.

● قفل های فیزیکی و منطقی

قفل منطقی قفلی است که فقط جنبه اخباری داشته و در آن هماهنگی تنها از طریق اعتماد متقابل رعایت می شود. در صورت استفاده از این نوع قفل حتی اگر برنامه در تقاضای قفل با جواب منفی مواجه شود برنامه خواهد توانست به اطلاعات مورد نظر دسترسی پیدا کند و آن را تغییر دهد. در چنین سیستمی برنامه نویس وظیفه دارد برنامه را طوری تنظیم کند که در صورت موفق نبودن قفل گذاری ، از دسترسی به اطلاعات خود داری کند.

در روش قفل فیزیکی ، سیستم عامل از دستیابی برنامه ها به اطلاعات قفل شده ، عملاً جلوگیری می کند. در این صورت حتی در صورت عدم رعایت قفل توسط یک برنامه امکان تداخل برنامه ها وجود ندارد.

● قفل های باصبر و بدون صبر

در روش قفل بدون صبر ، نتیجه درخواست قفل سریعاً از طرف سیستم عامل به اطلاع برنامه می رسد. نتیجه مثبت به این معنی است که اطلاعات مورد نظر در دسترس بوده و اکنون برای استفاده برنامه قفل شده است. نتیجه منفی به این معنی است که اطلاعات توسط برنامه دیگری قفل شده است و اکنون در دسترس نیست. در

این روش برنامه باید تا حصول نتیجه مثبت درخواست خود را تکرار کند و یا به کاربر اطلاع دهد که اطلاعات مورد نظر در دسترس نیست.

در روش قفل با صبر، اگر اطلاعات مورد نظر توسط کاربر دیگری قفل شده باشد سیستم عامل تا زمان برطرف شدن قفل صبر نموده سپس اطلاعات را برای برنامه قفل می کند و نتیجه مثبت را به برنامه اطلاع می دهد. در سیستم هایی که حداکثر زمان استفاده هر برنامه از اطلاعات، مشخص و قابل قبول است، استفاده از این روش اشکالی ایجاد نمی کند. در غیر این صورت ممکن است یک برنامه مدتها در انتظار قفل کردن اطلاعاتی که توسط برنامه دیگر قفل شده است، باقی بماند.

برخی از نرم افزارهای کاربردی ترکیبی از این دو روش را در اختیار کاربر قرار می دهند. در این نرم افزارها روش قفل گذاری در حالت عادی از نوع بدون صبر است. اما این امکان به برنامه نویس داده می شود که قفل های با صبری، با زمان انتظار قابل تنظیم تقاضا کند.

● قفل های قابل اشتراک و انحصاری

قفل های قابل اشتراک، به هر تعداد برنامه اجازه می دهند که به یک فایل یا رکورد تنها برای خواندن اطلاعات دسترسی داشته باشند. در این حالت امکان نوشتن اطلاعات در فایل یا رکورد مربوطه حداکثر به یکی از برنامه ها داده می شود و بقیه امکان نوشتن را نخواهند داشت. در روش قفل انحصاری اگر اطلاعات توسط یک برنامه قفل شود امکان دسترسی به این اطلاعات حتی برای خواندن از برنامه های دیگر گرفته می شود.

◆ روش (Semaphore)

برای ایجاد هماهنگی در دسترسی به امکاناتی که بطور همزمان در اختیار تعداد مشخصی از برنامه ها قرار گیرند، از روش (Semaphore) استفاده می شود. (Semaphore) در واقع متغیری است که توسط سیستم عامل نگهداری و کنترل می شود و می تواند مقادیر مثبت یا صفر داشته باشد. هر (Semaphore) دسترسی به یکی از امکانات شبکه را کنترل می کند و دارای یک ارزش است. ارزش (Semaphore) مربوط به هر یک از امکانات شبکه برابر حداکثر تعداد برنامه هایی است که می تواند بطور همزمان از آن امکان استفاده کنند. به عنوان مثال اگر یکی از امکانات شبکه بتواند بطور همزمان در اختیار ۵ برنامه قرار گیرد. یک (Semaphore) با ارزش ۵ آن را کنترل خواهد کرد.

در این روش برنامه ای که می خواهد از امکانات شبکه استفاده کند تقاضا برای سیستم عامل می فرستد. سیستم عامل بر اساس مقدار (Semaphore)، در مورد در اختیار دادن این امکان تصمیم می گیرد. اگر مقدار (Semaphore) عددی مثبت باشد، امکان مورد نظر در اختیار برنامه قرار می گیرد و یک واحد از (Semaphore) کم می شود. در صورتیکه مقدار (Semaphore) صفر باشد، امکان مورد نظر در دسترس نیست و برنامه باید تا مثبت شدن مقدار (Semaphore) صبر کند. هر برنامه پس از اتمام کار خود،

رها کردن (Semaphore) را به سیستم عامل اعلام می کند ، این امر باعث افزوده شدن یک واحد به مقدار (Semaphore) می شود.

Deadlock چیست؟

در بسیاری از موارد ممکن است دو برنامه جهت ادامه کار خود احتیاج به قفل کردن انحصاری مجموعه ای از اطلاعات داشته باشند، و هر یک بخشی از این اطلاعات را برای خود قفل کرده و در انتظار قفل کردن بخش دیگر باشند. اگر بخشی از اطلاعات مورد نیاز هر برنامه در اختیار دیگری باشد و هیچ یک از برنامه های فوق نسبت به واگذاری اطلاعات به برنامه دیگر اقدام نکند ، هیچ یک از برنامه ها قادر به ادامه کار نخواهند بود و حالت Deadlock حاصل می شود. این حالت مختص دو برنامه نبوده و می تواند برای بیش از دو برنامه تعمیم یابد.

به عنوان مثال فرض کنید دو برنامه برای ادامه کار باید دو رکورد از یک پرونده به نام های Record1 و Record2 را قفل کنند . اگر برنامه اول Record1 و برنامه دوم Record2 را قفل کنند ، هیچ یک از دو برنامه نمی تواند به کار خود ادامه دهند و حالت Deadlock به وجود خواهد آمد.

یک روش برای جلوگیری از این حالت این است که ، اگر یک برنامه در قفل کردن تمامی اطلاعات مورد نیاز خود موفق نبود ، تمامی اطلاعاتی را که قفل کرده است آزاد کند و سپس مجدد اقدام به قفل نمودن اطلاعات مورد نظر نماید.

روش دیگر که در سیستم عامل Netware در اختیار برنامه قرار دارد این است که ، یک برنامه ابتدا مجموعه اطلاعات مورد نیاز را علامت گذاری کرده و در پایان تقاضای قفل شدن تمامی مجموعه را صادر کند. در صورت موفقیت تمامی اطلاعات قفل شده اند و در صورت عدم موفقیت هیچ قفل گذاشته نمی شود.

Transaction Tracking

یک سیستم بانک اطلاعاتی ممکن است از فایل های مختلف تشکیل شده باشد . به علت ارتباط بین فایلها ، تغییر در یک فایل می تواند باعث تغییر در محتویات فایل های دیگر شود. فرایند بروز در آوردن همزمان همه فایلها را یک Transaction می نامند.

هنگامی که یک برنامه حین انجام یک Transaction دچار اشکال شود ، قسمتی از اطلاعات به روز در آمده و قسمت دیگر هنوز به حالت اولیه باقی مانده اند. به این ترتیب اطلاعات خروجی سیستم قابل اطمینان نبوده و فاقد ارزش هستند.

در سیستمی که از Transaction Tracking استفاده می کند ، یا تمامی اطلاعات در فایل های مختلف به روز در می آیند و یا در صورت به وجود آمدن اشکال ، کلیه فایلها به حالت اولیه برمی گردند.

فرایند بازگشت فایلها به حالت اولیه را اصطلاحاً Automatic Rollback نامیده می شود. 

فصل چهارم

امنیت شبکه (۱)

شبکه کامپیوتری یک سیستم اطلاعاتی گسترده است و افراد می توانند دور از نظر مسئولان سیستم به آن دسترسی داشته باشند، از طرف دیگر ممکن است اطلاعات بسیار مهمی در شبکه ذخیره شده باشد، لذا کنترل شدید بر صلاحیت و چگونگی کار کاربران، امری حیاتی است.

کنترل امکانات و عملکرد کاربران در شبکه به دو شاخه اساسی تقسیم می شود:

الف- چه کسی در شبکه کار می کند؟

ب- اجازه چه کارهایی به او داده می شود؟

در این فصل به بررسی جزئیات شاخه اول خواهیم پرداخت و شاخه دوم در فصل بعدی بررسی خواهد شد.

کاربران شبکه

Netware هنگام ورود هر کاربر به شبکه، یک «نام کاربر» از وی می پرسد. اگر نام کاربر یکی از نامهای تعریف شده توسط مدیر شبکه باشد، به وی اجازه کار در شبکه داده خواهد شد. در ادامه این فصل خواهید دید که امکانات و اختیاراتی که یک کاربر در شبکه دارد، مستقیماً به نامی که هنگام ورود، تایپ کرده است، بستگی دارد.

از این پس هر جا که به «نام کاربر» اشاره شده است، منظور نامی است که توسط مدیر شبکه برای وی در نظر گرفته شده است.

نام کاربر در شبکه باید حتی المقدور متناسب با نام واقعی کاربر باشد، نام کوچک و یا نام فامیلی کاربر معمولاً انتخابهای مناسبی هستند. ارتباط نام کاربر با نام واقعی او این مزیت را دارد که یک کاربر در شبکه به خوبی توسط مدیر شبکه و دیگر کاربران شناخته می شود و این امر در برقراری ارتباط بین کاربران بسیار مفید است.

اما به این ترتیب ممکن است افراد بدون صلاحیت یا کاربران دیگر، به جای یک کاربر خاص وارد شبکه شده و از مجوزهایی که برای او منظور شده است، استفاده کنند. برای جلوگیری از این امر در Netware تدابیر شدیدی در نظر گرفته شده است. در ادامه این فصل به بررسی این تدابیر می پردازیم.

گروه‌ها در شبکه

در بسیاری از موارد در یک شبکه لازم است عملیات و مجوزهای خاصی در مورد تعدادی از کاربران اعمال شود. در این موارد دسته بندی کاربران مفید خواهد بود. سیستم امنیتی Netware امکان دسته بندی کاربران، به صورت «گروه»ها را فراهم می کند. این دسته بندی باید به دقت صورت گیرد و افرادی که در یک دسته قرار می گیرند باید در اطلاعات مورد نیاز و یا عملیاتی که انجام می دهند، با یکدیگر وجه اشتراک داشته باشند، یک گروه ممکن است اعضاء مشترکی با یک گروه دیگر داشته باشد.

یک گروه مهم، گروه Everyone است. این گروه که شامل همه کاربران شبکه می شود، در ابتدای ایجاد سیستم به صورت اتوماتیک ایجاد می شود. یک خاصیت این گروه این است که، هر کاربری که برای سیستم تعریف می شود به صورت اتوماتیک عضوی از این گروه خواهد شد. هر گاه این گروه توسط مدیر شبکه پاک شود و دوباره ایجاد شود، تنها کاربران جدید در این گروه قرار خواهند گرفت. گروه بندی کاربران توسط مدیر شبکه صورت می گیرد و هر کاربر تنها می تواند از نام گروه ها و نام اعضای آنها اطلاع حاصل کند.

امنیت در ورود به شبکه

هر کاربر هنگام ورود به شبکه باید یک «نام کاربر» و کد عبور (password) مربوط به این نام را بداند. هر کاربر با استفاده از دستور Login و یا وارد کردن نام کاربر و کد عبور مربوط به وی وارد شبکه می شود. هر گاه کاربر، نام و یا کد عبور خود را غلط تایپ کند، از ورود وی به شبکه جلوگیری خواهد شد. کسانی که در کنار کاربر هستند ممکن است هنگام ورود، از کد عبور کاربرد مطلع شوند، لذا کد عبور هنگام ورود، روی صفحه ظاهر نمی شود. کد عبور و نام کاربر را می توان هم با حروف بزرگ و هم با حروف کوچک وارد کرد. اگر کسی سعی کند با نام کاربری وارد شبکه شود و کد عبور صحیح را نداند، پیامی شبیه به پیام زیر روی صفحه نمایش دیده خواهد شد.

Access to server denied

You are attached to server SINASOFT.

اگر کسی سعی در ورود داشته باشد و نام او برای شبکه شناخته شده نباشد، از او کد عبور پرسیده می شود و سپس پیامی مشابه بالا را دریافت خواهد کرد.

هر کاربر در شبکه دارای حسابی است که به وسیله این حساب، در صورت لزوم نحوه کار کاربر در شبکه ارزیابی می شود. برای ورود یک کاربر به شبکه لازم است حساب فوق باز بوده و بوسیله مدیر شبکه (یا عوامل دیگر) بسته نشده باشد.

امنیت کد عبور

کد عبور یک کاربر، در واقع نشاندهنده شخصیت کاربر در شبکه است و به این وسیله سیستم عامل از صحت هویت کاربر مطلع می شود. در سیستم عامل Netware تدابیری برای حفظ امنیت کد عبور در اختیار مدیر شبکه قرار دارد. این تدابیر شامل این موارد می شود:

- مدیر شبکه می تواند به کاربران اجازه تعویض کد عبور را بدهد و یا، این حق را از آنها بگیرد. در هر دو صورت مدیر شبکه می تواند کد عبور کاربران را عوض کند.
- مدیر شبکه برای افزایش امنیت کد عبور می تواند کاربران را مجبور به داشتن کد عبور کند. در حالت کلی یک کاربر می تواند کد عبور نداشته باشد.
- مدیر شبکه می تواند حداقل طول مجاز برای کد عبور را مشخص کند. به این ترتیب کاربران ملزم به داشتن کد عبور با طول مساوی و یا بیشتر از این طول، خواهند بود.
- در صورت لزوم، مدیر شبکه می تواند کاربران را به تعویض متوالی کد عبور ملزم کند. در صورت استفاده از این امکان، مدیر شبکه می تواند زمان بین دو بار تعویض کد عبور را تعیین کند.
- پس از انقضای زمان اعتبار یک کد عبور، کاربر می تواند چندین بار با کد عبور قبلی وارد شبکه شود، مدیر شبکه می تواند این تعداد را تعیین کند. ورود کاربر با کد عبور منقضی شده را اصطلاحاً «ورود اعتبار» (Grace login) می نامند.
- در حالت عادی کد عبور جدید می تواند برابر با کد عبور قبلی باشد. در صورت لزوم می توان کاربر را مجبور کرد که هر بار کد عبور جدیدی وارد کند.
- کلیه امکانات فوق، در صورت استفاده، تماماً به وسیله سیستم امنیتی Netware تامین می شود و مدیر شبکه تنها تصمیم گیری راجع به استفاده یا عدم استفاده از آنها را به عهده دارد. در کار عملی این فصل با چگونگی استفاده از این امکانات آشنا خواهید شد.

محدودیت زمانی

در حالت عادی یک کاربر می تواند در هر ساعتی از شبانه روز و در هر روز از هفته وارد شبکه شود. اما مدیر شبکه می تواند هر کاربر را به استفاده از شبکه در ساعات خاصی از شبانه روز محدود کند. این ساعات مجاز با دقت نیم ساعت در هر روز هفته قابل تنظیم است. به عنوان مثال می توان ساعات مجاز را به صورت زیر تعریف نمود.

روزهای شنبه تا چهارشنبه از ساعت ۸/۳۰ تا ۱۶/۳۰

روز پنجشنبه از ساعت ۸/۳۰ تا ۱۳/۳۰

معمولاً ساعات کاری سازمان که در شبکه در آن نصب شده است، به عنوان ساعت مجاز تعریف می شود. در اوقات خارج از ساعات کاری از ورود کاربر به شبکه جلوگیری خواهد شد.

اگر کاربری در ساعات ممنوعه سعی در ورود به شبکه داشته باشد با پیامی شبیه به پیام زیر مواجه خواهد شد.

Attempting to login during an unauthorized time period .
The supervisor has limits the time that you can login to this server.
Access to server denied.
You are attached to server SINASOFT.

اگر کاربر قبلاً وارد شبکه شده و در موقع انقضای زمان مجاز ، در حال کار در شبکه باشد، پیامی شبیه به پیام زیر را دریافت خواهد کرد.

>> SINASOFT CONNECTION TIME EXPIRED, PLEASE LOG OUT.

اگر کاربر از شبکه خارج نشود ، پیامی شبیه به این پیام دریافت خواهد کرد.

>> SINASOFT CONNECTION TERMINATING IN 1 MINUTE.

اگر پس از گذشت یک دقیقه ، کاربر از شبکه خارج نشود ، سیستم عامل شبکه ارتباط وی را با شبکه قطع خواهد کرد. در این حال کلیه فایل های مربوط به کاربر بسته می شود ، اما ممکن است برنامه در حال کار در ایستگاه به محل مناسبی برای قطع ارتباط نرسیده باشد و به این ترتیب به اطلاعات صدمه وارد شود. لذا کاربران باید به پیام های فوق توجه کنند.

در کار عملی این فصل با چگونگی تعیین ساعات مجاز برای کار در شبکه ، آشنا خواهید شد.

محدودیت ایستگاه

در حالت عادی یک کاربر می تواند از هر یک از ایستگاه های شبکه وارد شود. امکانات و اجازه کاربر برای انجام عملیات در شبکه بستگی به نام کاربر و کد عبور او دارد و ارتباطی با ایستگاهی که از آن وارد شبکه شده است ، ندارد.

اما مدیر شبکه می تواند کاربران را به استفاده از یک یا چند کامپیوتر به خصوص برای ورود به شبکه ، محدود کند. اگر کاربری سعی کند از کامپیوتر غیر مجازی وارد شبکه شود ، پیامی شبیه به این پیام ، دریافت خواهد کرد :

Attempting to login from an unapproved station .
The supervisor has limited the stations that you are allowed to login on.
Access to server denied.
You are attached server SINASOFT.

یک کاربرد این امر ، محدود کردن کاربران یک قسمت ، به کار در قسمت خودشان است. در بعضی موارد نیز فلاپی دیسک بعضی از ایستگاه ها به خاطر جلوگیری از کپی شدن اطلاعات موجود در هارد دیسک آنها از کار انداخته می شود. در این موارد برای حفظ امنیت اطلاعات موجود در هارد دیسک اجازه کار با این دستگاه تنها به کاربران ایستگاه داده شود.

محدودیت اتصال همزمان

در حالت عادی یک کاربر می تواند با یک نام کاربر از چندین ایستگاه وارد شبکه شده و از طریق همه ایستگاه ها به صورت همزمان به شبکه متصل باشد. مدیر شبکه می تواند کاربران را از نظر اتصال به شبکه به صورت همزمان از ایستگاه های مختلف ، محدود کند. در صورت استفاده از محدودیت اتصال هم زمان ، مدیر شبکه می تواند تعداد ایستگاه هایی را که یک کاربر می تواند از آنها به صورت هم زمان به شبکه متصل باشد ، تعیین کند.

 در صورتیکه کاربری ، از ایستگاه هایی به تعداد مجاز ، به شبکه متصل باشد و سعی در ورود به شبکه از ایستگاه دیگری داشته باشد ، با پیامی شبیه به این پیام مواجه خواهد شد :

Attempting to simultaneously login on too many work station.
The supervisor limited the number of active connections you may have.
Access to server denied.
You Are Attached To Server SINASOFT.

سیستم INTRUDER DETECTION / LOCKOUT

اگر مدیر شبکه مایل باشد می تواند افراد بدون صلاحیت را که سعی در ورود به شبکه دارند ، تشخیص دهد. برای این کار باید تعداد دفعات متوالی را که یک کاربر می تواند کد عبور را اشتباه وارد کند ، محدود کند. هرگاه شخص بیش از تعداد دفعات تعیین شده ، سعی در ورود به شبکه با یک نام خاص داشته باشد و موفق نشود ، این شخص فرد بدون صلاحیتی در حال حدس زدن کد عبور محسوب خواهد شد. در صورت لزوم مدیر شبکه می تواند سیستم را طوری تنظیم کند که پس از تشخیص فرد بدون صلاحیت حساب کاربر (که به نام او سعی در ورود به شبکه شده بود) بسته شود. در این حالت پیامی شبیه با این پیام روی صفحه ظاهر می شود :

Intruder detection lockout has disabled this account.
Access to server denied.
You Are Attached To Server SINASOFT.

در این حال حساب کاربر مربوطه مسدود می شود و تنها مدیر شبکه می تواند آن را به جریان اندازد. به این ترتیب تا مدت مشخصی از ورود کاربر با این نام حتی با دادن کد عبور صحیح جلوگیری خواهد شد. این مدت زمان به وسیله مدیر شبکه قابل تنظیم است.

کاربر برای ادامه کار در شبکه باید به مدیر شبکه مراجعه کند و مدیر شبکه حساب او را مجدداً به جریان اندازد.

مدیر شبکه می تواند مدت زمان لازم برای نادیده گرفتن ورودهای غیر موفق را تعیین کند. اگر این مقدار زمان از آخرین ورود غیر موفق بگذرد ، کلیه ورودهای غیر موفق قبلی نادیده گرفته می شود.

فصل پنجم

امنیت شبکه (۲)

در فصل گذشته تدابیر امنیتی Netware را در مورد اینکه چه کسی در شبکه کار می کند بررسی کردیم. پس از اینکه کاربر وارد شبکه شد امکانات و توانایی های او در انجام کارهای مختلف باید کنترل شود. در این فصل روشهای کنترل توانایی های کاربران برای انجام عملیات مختلف بررسی می شوند.

تدابیر امنیتی

در سیستم عامل Netware کنترل مجوزهای کاربران برای انجام عملیات روی فایلها در سه سطح صورت می گیرد:

- ۱- مجوزهای (Trustee Assignment) - این مجوزها، در حد کاربر عمل می کنند. هر کاربر ممکن است در یک یا چند کشو دارای مجوز انجام بعضی عملیات باشد. کاربری را که برای او در یک کشو مجوزهایی در نظر گرفته شده باشد، یک عضو از آن کشو می نامند. مجوزهای عضویت یک کاربر، می تواند با مجوزهای عضویت کاربر دیگر متفاوت باشد.
- ۲- مجوزهای معتبر در کشو (Maximum Rights Mask) - این مجوزها در سطح کشو عمل می کنند و اعتبار مجوزهای کاربر را در یک کشو تعیین می کنند. مجوزهای معتبر در کشو از متعلقات هر کشو بوده و از طریق این مجوزها توانایی لازم برای انجام یک عمل، برای کلیه کاربران تعیین می شود. هرگاه مجوزهای معتبر در کشو، شامل مجوز انجام کاری نشود، هیچ کاربری قادر به انجام کار در کشو مربوطه نخواهد بود.
- ۳- مشخصه فایل (file attributes) - این قسمت از تدابیر امنیتی در سطح فایل عمل می کند و اجازه انجام عملیات روی یک فایل خاص را تعیین می کند.

مجوزهای (Trustee Assignment)

این مجوزها ، که اجازه انجام عملیات را در سطح کاربر کنترل می کند ،می توانند از کاربری به کاربر دیگر متفاوت باشند.

هرگاه مجوزهایی در یک کشو به یک کاربر تخصیص داده شده باشد ، این کاربر را یک عضو از این کشو می نامند. توجه کنید مفهوم یک عضو نباید با مفهوم کاربر اشتباه شود. ممکن است کسی کاربر شبکه باشد اما هیچ مجوزی در یک کشو خاص نداشته باشد ، در این صورت او عضو این کشو نیست.



نکته مهم در مورد مجوزهای عضویت این است که این مجوزها مانند کد عبور و محدودیتهای ورود به شبکه از متعلقات بک کاربر هستند و اجازه او برای انجام برخی عملیات در یک کشو خاص را تعیین می کنند :

این مجوزها عبارتند از :

مجوز باز کردن فایلها	(Open) O
مجوز خواندن از فایلی که باز شده است	(Read) R
مجوز نوشتن در فایلی که باز شده است	(Write) W
مجوز ایجاد (و باز کردن هنگام ایجاد) یک فایل	(Create) C
مجوز جستجوی یک کشو (گرفتن لیست فایلها)	(Search) S
مجوز پاک کردن یک فایل یا یک کشو خالی	(Delete) D
مجوز تغییر دادن مشخصه فایلها یا تغییر نام زیر کشو	(Modify) M
مجوز کفالت کشو ، کاربری که داری مجوز کفالت باشد ، می تواند مجوزهای عضویت سایر کاربران در کشو را تغییر دهد و یا مجوزهای کشو را عوض کند.	(Parental) P

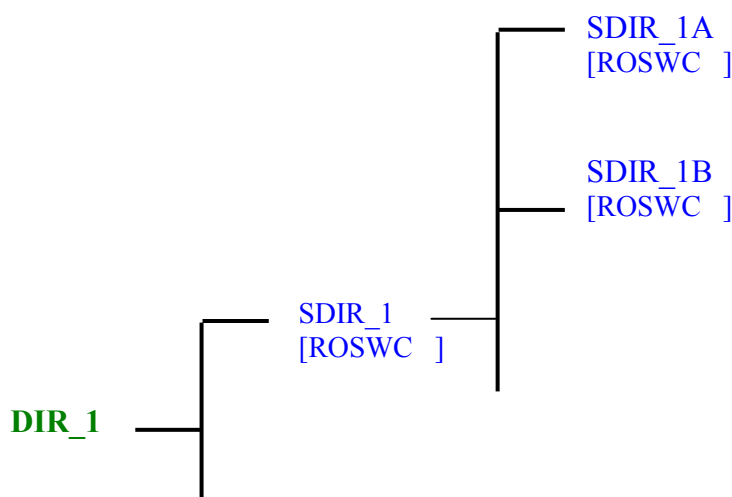
مجوز یک کاربر در یک کشو می تواند یک ، یا ترکیبی از این مجوزها باشد. یکی از ترکیبهای این مجوزها (هیچ مجوز) است. این ترکیب را بصورت [] نشان می دهیم. کاربری که در یک کشو دارای (هیچ مجوز) باشد با کاربری که در این کشو مجوزی ندارد متفاوت است.

به عنوان مثال ، فرض کنید که کاربری به نام user1 در یک کشو دارای مجوزهای [ROSWC] است و user2 در همین کشو دارای مجوز [] است و کاربر دیگری به نام user3 مجوزی در این کشو ندارد. در این حالت کاربران user1 و user2 عضو این کشو هستند اما user3 عضو این کشو نیست. اگرچه در عمل user2 و user3 هر دو در این کشو مجوز انجام هیچ کاری را ندارند اما موقعیت این دو کاربر در شبکه با هم تفاوت هایی دارد که در قسمت بعدی بررسی می شود.

اگر کاربری در یک کشور دارای مجوز C باشد ، می تواند در این کشور یک فایل جدید ایجاد کند اما برای وارد کردن از اطلاعات در این فایل به مجوز W احتیاج دارد. همچنین پس از بستن فایل باز کردن مجدد و دیدن محتوی آن مجوزهای O و R لازم است.

جریان یافتن مجوزهای عضویت

به شکل زیر توجه کنید. فرض کنید به کاربری در کشور DIR_1 مجوزهای عضویت [ROSWC] داده شده است. در این حال کاربر ، در کلیه زیر کشور های این کشور ، تا جایی که مجوزها به صورت دیگری تعریف نشده باشد دارای این مجوزها خواهد بود.



به این ترتیب هنگام دادن مجوزهای عضویت باید به هر کاربر تنها در زیر کشور مورد نظر مجوز داده شود. برای جلوگیری از جریان یافتن مجوزهای کشور قبلی در یک کشور باید در آن کشور مجوزها مجدداً تعریف شوند. به عنوان مثال اگر بخواهیم در مثال قبل کاربر در زیر کشور SDIR_1A اجازه انجام کاری را نداشته باشد باید مجوزهای عوضیت او را در کشور مزبور برابر هیچ مجوز قرار دهیم. در این صورت مجوزهای این کاربر در کشور SDIR_1A و زیر کشورهای آن برابر [] خواهد بود.

با مثال فوق تفاوت میان کاربری که در یک کشور دارای مجوز [] است با کاربری که مجوز در این کشور ندارد (عضو این کشور نیست) ، مشخص می شود. اگر کاربری عضو یک زیر کشور نباشد ، مجوزهای او در

کشو قبلی به این زیر کشو جریان خواهد یافت ، اما کاربری که عضو یک کشو است ، تنها مجوزهای عضویت خود را در این کشو خواهد داشت.

برابری امنیتی

برابری امنیتی به یک کاربر اجازه می دهد کلیه مجوزهای عضویت یک کاربر دیگر را داشته باشد. فرض کنید در کشو DIR-1 کاربری به نام User-1 دارای مجوزهای [ROSWC] باش و User-2 دارای مجوزهای [ROS] باشد. اگر به User-2 برابری امنیتی با User-1 داده شود ، کلیه مجوزهای User-1 به او خواهد رسید و دارای مجوزهای [ROSWC] خواهد شد. توجه کنید برابری امنیتی تنها در مورد مجوزهای اصلی کاربر عمل می کند مثلاً اگر در مثال بالا به User-3 برابری امنیتی با User-2 داده شود ، مجوزهای User-1 به او نخواهد رسید بلکه تنها مجوزهای [ROS] که مربوط به خود User-2 است به وی خواهد رسید. برابری امنیتی یک طرفه است ، یعنی اگر User-2 دارای برابری امنیتی با User-2 است.

به مثال زیر توجه کنید:

Ali در یک کشو دارای مجوزهای [ROSWC] است.

و Babak دارای مجوزهای [ROS MP] است.

اگر به Babak برابری امنیتی با Ali داده شود ، BABAK دارای مجوزهای [ROSWC MP] خواهد شد و مجوزهای Ali همان [ROSWC] باقی خواهد ماند. مجوزهای M و P به Ali نخواهد رسید.

مجوزهای گروه

عضویت در گروه مانند برابری با آن گروه است. در یک گروه مانند یک کاربر می تواند مجوزهایی در یک کشو داشته باشد . این مجوزها عیناً مانند مجوزهای یک کاربر هستند. مجوزهایی که به یک گروه داده می شود ، به کلیه اعضای آن گروه منتقل می شود. هر گاه کاربری عضو یک گروه شود ، با آن گروه برابری امنیتی خواهد داشت و کسی که با یک گروه برابری امنیتی شود ، عضو آن گروه خواهد شد.

مجوزهای معتبر در کشو (MAXIMUM RIGHTS MASK)

این مجوزها ، که در سطح کشو عمل می کنند ، اعتبار اختیارات کاربران در یک کشو را تعیین می کنند. مدیر شبکه از این امر مستثنی بوده و در کلیه کشوها اختیارات را دارد.

این مجوزها مانند مجوزهای عضویت عبارتند از :

مجوز باز کردن فایلها	(Open) O
مجوز خواندن از فایلی که باز شده است	(Read) R
مجوز نوشتن در فایلی که باز شده است	(Write) W
مجوز ایجاد (و باز کردن هنگام ایجاد) یک فایل	(Create) C

S (Search)	مجوز جستجوی یک کشو (گرفتن لیست فایلها)
D (Delete)	مجوز پاک کردن یک فایل یا یک کشو خالی
M (Modify)	مجوز تغییر دادن مشخصه فایلها یا تغییر نام زیر کشو
P (Parental)	مجوز کفالت کشو، کاربری که داری مجوز کفالت باشد، می تواند مجوزهای عضویت سایر کاربران در کشو را تغییر دهد و یا مجوزهای کشو را عوض کند.

هنگام ایجاد یک کشو تمامی مجوزهای عضویت، در آن کشو معتبر هستند و مجوزهای معتبر در کشو، شامل همه مجوزهای فوق می شود. به این ترتیب یک کاربر می تواند همه این حقوق را در این کشو داشته باشد. برای محدود کردن مجوزهای معتبر در این کشو (برای همه کاربران) باید یک یا چند مجوز را از میان مجوزهای معتبر در کشو، حذف کرد.

به عنوان مثال فرض کنید مجوز D از مجوزهای معتبر در یک کشو حذف شود. از آنجا که مجوزهای معتبر در کشو اعتبار مجوزهای کلیه کاربران در یک کشو را تعیین می کنند، از این پس حتی کاربرانی که دارای مجوز عضویت D نیز باشند نمی توانند فایلی را پاک کنند. زیرا مجوز D در مجوزهای معتبر در این کشو وجود ندارد و مجوز D کاربران در این کشو فاقد اعتبار است.

مجوزهای معتبر در کشو، مانند نام کشو جزء متعلقات یک کشو هستند و برخلاف مجوزهای عضویت، به زیرکشوهای یک کشو جریان پیدا نمی کنند.

از آنجا که پس از حذف یک مجوز از مجوزهای معتبر در کشو، هیچ کاربری قادر به انجام عمل مربوطه نخواهد بود، به جز موارد خاص مجوزهای معتبر در کشو برابر [ROSSWCDMP] (کلیه مجوزها) قرارداد می شوند.

مشخصه فایلها (File Attribute)

این قسمت از تدابیر امنیتی Netware، در حد فایل عمل می کنند. هر فایل در سیستم بایگانی Netware دارای یک مشخصه است. این حالات عبارتند از:

■ مشخصه N (Normal)

این مشخصه، مشخصه ای است که سیستم عامل Netware هنگام ایجاد یک فایل، بصورت پیش فرض برای آن در نظر می گیرد فایلهایی که این مشخصه را دارند، قابل اشتراک بین چند کاربر نیستند. اطلاعات درون چنین فایلی قابل خواندن و نوشتن است.

■ مشخصه RO (Read Only)

اگر فایلی دارای این مشخصه باشد، کاربران تنها می توانند این فایل را بخوانند و هیچ کاربری نمی تواند آنرا پاک کند، نام آنرا تغییر دهد و یا چیزی در آن بنویسد. این امر بستگی به مجوزهای کاربر ندارد.

■ مشخصه RW (Read Write)

فایلی که دارای این مشخصه باشد ، می تواند به وسیله کاربرانی که دارای مجوزهای کافی هستند نوشته شود ، نام داده شود و یا پاک شود.

■ مشخصه S (Shareable)

فایلی که دارای این مشخصه باشد می تواند به وسیله چند کاربر به اشتراک گذاشته شود. این مشخصه با مشخصه RO به کار می رود.

■ مشخصه M (Modified)

هر بار که از فایل های شبکه پشتیبان تهیه می شود کلیه فایلها از مشخصه Modified خارج می شوند. پس از این زمان هر گاه محتوی فایلی به هر صورت تغییر پیدا کند این فایل مشخصه Modified پیدا خواهد کرد.

■ مشخصه Execute Only

این مشخصه را تنها می توان برای فایل هایی با دنباله EXE و COM به کار برد. فایلی که دارای چنین مشخصه ای باشد تنها قابل اجراست. در صورت استفاده از این مشخصه از نوشتن در داخل فایل ، پاک کردن فایل ، تعویض نام فایل و کپی کردن فایل جلوگیری خواهد شد.

■ مشخصه System

سیستم عامل Netware برای انجام امور داخلی خود از فایل هایی با مشخصه System استفاده می کند. نام چنین فایل هایی در لیست فایل های یک کشو ظاهر نمی شود. صدمه دیدن چنین فایلی می تواند کار سیستم عامل را دچار اشکال کند.

■ مشخصه I (Indexed)

برای تسریع در دستیابی به قسمت های مختلف فایل هایی که دارای حجمی بیش از ۲ مگا بایت هستند ، از این مشخصه استفاده می شود. سیستم عامل شبکه ، آدرس قطعات مختلف یک فایل را در جدول های مختلف فایلها نگهداری می کند. تعداد قطعات مختلف یک فایل بزرگ می تواند زیاد شود و در این صورت برای دستیابی به یک قطعه از این فایل زمان زیادی برای یافتن آدرس آن صرف می شود. با استفاده از مرتب سازی آدرسها ، می تواند سرعت دستیابی به قطعات مختلف یک فایل بزرگ را به صورت قابل توجهی افزایش داد.

■ مشخصه H (Hiden)

نام فایلی که دارای این مشخصه باشد ، بصورت عادی در لیست فایل های یک کشو ظاهر نخواهد شد. بسیاری از نرم افزارها برای کار خود از فایل هایی با این مشخصه استفاده می کنند. در بسیاری از موارد تغییر در این مشخصه باعث بروز اشکال در کار نرم افزار مربوطه خواهد شد.

اگر در نظر دارید از مشخصه فایلها برای امنیت سیستم استفاده کنید ، لازم است کاربران را در جریان این امر قرار دهید.

مجوزهای موثر (Effective Rights)

مجوزهای موثر یک کاربر در یک کشو ، در عمل تعیین کننده اجازه او برای انجام یک کار هستند. در واقع مجوزهای یک کاربر در یک کشو عبارتند از مجموع مجوزهای عضویت فردی او ، مجوزهایی که از طریق برابری امنیت به او رسیده است و مجوزهایی که از طریق گروه به او رسیده است. مجوزهایی را که ممکن است از طریق کشوی قبلی به این کشو جریان پیدا کرده باشد را نیز باید به این مجموع افزود.

مجوزهای موثر یک کاربر در یک کشو عبارتند از ضرب منطقی مجوزهای معتبر در کشو. به عبارت دیگر مجوزهای موثر یک کاربر در یک کشو عبارتند از آن دسته از مجوزهای عضویت وی که اعتبارشان توسط مجوزهای معتبر در کشو تایید شده باشد.

Bindary چیست ؟

Bindary عبارت است از اطلاعات مربوط به امنیت شبکه که توسط مدیر شبکه قابل تغییر است. این اطلاعات در دو فایل NET\$BIND.SYS و NET\$BVAL.SYS نگهداری می شوند. این دو فایل حاوی اطلاعاتی در مورد کاربران و کد عبور آنان ، گروه ها ، مجوزهای عضویت کاربران در کشو ، کشوها و مجوزهای معتبر در کشوها ، صف ها و ... است. در مواردی که این پرونده ها به دلیلی دچار اشکال شوند مشکلات زیر در شبکه مشاهده خواهد شد.

نام یک کاربر را نمی توان حذف کرد یا تغییر داد. 

کد عبور یک کاربر را نمی توان تغییر داد. 

مجوزهای یک کاربر را نمی توان تغییر داد. 

مجوزهای معتبر در کشو را نمی توان تغییر داد. 

پیام خطا در Bindary روی File Server نمایش داده می شود. 

به دلیل حساس بودن اطلاعات موجود در Bindary مدیر شبکه باید با تهیه پشتیبان از این فایلها از وقفه در کار شبکه جلوگیری کند.

در صورت بروز اشکال در Bindary می توان از برنامه کمکی BINDFIX استفاده کرد. این برنامه ابتدا فایلهای مربوط به Bindary را از دسترس کاربران خارج کرده و سپس عملیات بازسازی را روی آن انجام می دهد . پس از پایان عمل باز سازی این فایلها مجددا در دسترس کاربران قرار می گیرند.

در حین عملیات باز سازی BINDFIX مراحل عمل را گزارش داده و در برخی از موارد از مدیر شبکه کسب تکلیف می کند. اگر در حین باز سازی Bindary ایستگاه مربوطه به دلیلی دچار اشکال شود ، احتمال از دست رفتن فایلها وجود دارد. به علت اهمیت بسیار زیاد Bindary در یک شبکه قبل از شروع عمل باز سازی ،

BINDFIX یک کپی از دو فایل مربوط به Bindary تهیه می کند و در فایل های NET\$BIND.SYS و NET\$BVAL.SYS نگهداری می کند.

در صورت موفق بودن عمل باز سازی ، BINDFIX از کاربر می خواهد که فایل های OLD را پاک کند. در صورت بروز اشکال در عمل باز سازی ، می توان با اجرای دستور BINDREST فایل های مربوط به Bindary را به صورت اول باز گرداند. دستور BINDFIX به وسیله مدیر شبکه قابل اجرا بود و در دسترس کاربران قرار ندارد.