شبکه

علی رضایی

شناسنامه اثر	
نام کتاب	شبکه
گردآوری	علی رضایی
سایت منبع	
آماده‌سازیPDF	www.parstech.org
کد کتاب	۱۲۰۲
تاریخ ثبت در سایت	۱۳۸٤/۰۸/۰۱

انواع کامپیوترها

۱- ابر کامپیوترها
۲- کامپیوترهای بزرگ Main
۳- کامپیوترهای کوچک Mini
٤- 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 می‌باشد.

وظایف سیستم عامل :

۱- راه اندازی کامپیوتر
۲- گرفتن دستورات از User
۳- تجزیه و تحلیل دستورات
٤- اجرای دستورات
٥- مدیریت حافظه اصلی (Ram)
٦- 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 فایلهای بسیار بزرگ را فراهم می کند.
۲- ترمینال های مقرون به صرفه تر از میکروکامپیوترها هستند.
۳- سرعت پردازش در سیستم های چند کاربره بیشتر است.
٤- 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.
٤- بسیاری از کاربران ممکن است از میکرو کامپیوترهایی داشته باشند این میکرو کامپیوترهای در یک سیستم چند کاربره تنها می‌توانند بصورت ترمینال استفاده شوند که این حداقل استفاده از امکانات وسیع یک میکروکامپیوتر است.
۵- توسعه سیستم مشکل و در برخی موارد غیر ممکن است.
٦- افزایش تعداد ایستگاه ها زمان پاسخ سیستم را به سرعت کاهش می‌دهد 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 برنامه‌های مناسب مشکل می‌باشد.

تعریف شبکه :

مجموعه ای از چند کامپیوتر مستقل که از طریق یک محیط ارتباطی با یکدیگر ارتباط دارند و می‌توانند 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 می‌شود ـ شاید بتوان اینترنت را بزرگترین Wan در نظر بگیریم.

عوامل پیشرفت سریع شبکه عبارتند از :

۱- تعداد زیاد میکروکامپیوترها.
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 .
٤- شبکه های محلی دارای قابلیت توسعه خوبی هستند.
٥- در یک شبکه محلی سیستم همگام با نیاز سازمان توسعه می‌یابد و هزینه اضافی را به سازمان مربوطه تحمیل نمی‌کند.
٦- 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 می‌کند.

تعریف **Pack :**

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

لایه های شبکه و مدل **OSI** OPEN SYSTEM INTERCONECT

مدل OSI معروفترین و معتبرترین استاندارد شبکه های محلی می‌باشد . این استاندارد رسمی‌به 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 می‌شود. این مدل یک چهار چوب و طبقه بندی کلی برای ارتباط ارائه می‌دهد و به جزئیات و چگونگی برقراری ارتباط نمی‌پردازد.

این مدل از هفت لایه تشکیل شده است . هر لایه از خدمات ارائه شده توسط لایه قبلی استفاده می‌کند و خدماتی را به لایه بعدی ارائه می‌دهد.

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 می‌شود 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 می‌گیرد.

لایه های شبکه :

۱- لایه فیزیکی	Physical
۲- لایه ارتباط داده	Data link
۳- لایه شبکه	Network
٤- لایه انتقال	Transmission
٥- لایه تماس	Session
٦- لایه نمایش	Presentation
۷- لایه کاربرد	Application

لایه فیزیکی (Physical) :

لایه فیزیکی با مشخصات الکتریکی و بیتها سر و کار دارد ، ایـن بیتهـا در اینجـا هـیچ معنـی ندارنـد و تجزیـه 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 بیـت در یـک لحظـه) باشد . در هر یک از این دو صورت ممکن است روش انتقال Half Duplex یـا Full Duplex باشـد . در روش انتقال Half Duplex خط انتقال در آن واحـــد می‌تواند یا برای ارســال اطلاعات و یا بـرای دریافـت اطلاعــات به کار گرفته شــود. در این روش ارســال و دریافت هــمزمان به وسیله یک خط ممـکن نیست. اما در روش انتـقال 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 نـدارد بلکـه اطلاعات را بصورت Packet می‌شناسد. این لایه نشانه هایی برای مشخص کردن ابتدا و انتهای Packet بـه رشته اطلاعات می‌افزاید . آشکار سازی و اصلاح خطاها نیز در این لایه صورت می‌گیرد. تعیـین زمـان و نحـوه دستیابی به خط نیز از وظایف این لایه است.

لایه شبکه (Network) :

این لایه ایجاد مسیر مجازی مناسب برای ارسال اطلاعات را بـه عهـده دارد ، در شـبکه هـایی کـه از مـسیرهای مختلف برای انتقال اطلاعات استفاده می‌کنند این لایه مسیر مناسب برای برقراری یک ارتبـاط خـاص را تعیـین می‌کند. این لایه در صورت وجود می‌تواند چندین ارتباط (Connection) در لایه انتقال را به وسـیله یـک ارتباط در لایه Data link برقرار کند این کار به روش Multiplex صورت می‌گیرد.

لایه انتقال (Transmission) :

این لایه پایین ترین لایه ای است که خدمات محلی به کاربر ارئه می‌دهد ، این لایه عمـل مـدیریت لایـه هـای زیرین را از نظر کنترل فرایند ارتباط و جریان اطلاعات انجام می‌دهـد. در ایـن لایـه خطاهـا آشـکار و اصـلاح می‌شوند و Packet هایی که با ترتیب غیر صحیح دریافت شده اند به حالت صحیح برگردانـده مـی‌شـوند بـه عبارت دیگر در این لایه مراحل نهایی کنترل صحت اطلاعات صورت می‌گیرد شروع ارتباط ، انتقال اطلاعات به لایه زیرین و ختم ارتباط توسط این لایه صورت می‌گیرد . وجود این لایه باعث می‌شود که لایه های بـالاتر 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 می‌دهد 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 می‌تواند 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 می‌شود. در این لایه کاربران از نظر مقدار و چگونگی استفاده از شبکه کنترل می‌شوند.

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 ترجه 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 کارکتر ست (کارکترهای هر کامپیوتر) بین دو ایستگاه از وظایف دیگر این لایه می‌باشد.

لایه کاربرد (Application) :

این لایه واسط 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 شبكه هاي كامپيوتري :

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

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 می‌تواند شامل سرویس دهنده های زیر باشد :

۱- Fail server : عضو لازم و اساسی یک شبکه است که می‌تواند یک کامپیوتر عادی در حال اجرای برنامه خاص ویا 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 اجزاست 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 می‌دهد.

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 می‌دهد . این سرویس دهنده ها عموماً دارای قابلیتهای Multi tasking هستند و در هنگام استفاده از آنها قسمتی از پردازش در ایستگاه کار و قسمت دیگر در Data base server انجام می‌شود.

٤- 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) :

میکروکامپیوترهایی هستند که به یک شبکه متصل هستند و از امکانات مشترک آن استفاده می کنند ، اگر چه می‌توان امکانات سخت افزاری یا ایستگاه را در اختیار ایستگاه دیگر قرار داد اما Work Stations اصولاً برای به اشتراک گذاشتن امکانات در نظر گرفته نمی‌شوند . مشخصه اساسی ایستگاه های یک شبکه این است که هوشمند هستند و می‌توانند پردازش انجام دهند ، این امر فرق اساسی بین ایستگاه های شبکه و ترمینال ها را تشکیل می‌دهد.

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.

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

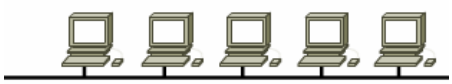
۲- نحوه دستیابی به خط ارتباطی

۳- کانال ارتباط

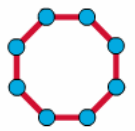
همبندی یا Topology : همبندی عبارت است از شکل هندسی اتصال دستگاه های درون شبکه . اتصالهای رایج عبارتند از :

۱- توپولوژی خطی یا Bus

در این همبندی ارتباط دستگاه ها از طریق یک رشته کابل که به ترتیب از یک دستگاه به دستگاه دیگر کشیده می‌شود برقرار می‌شود . پیامی که از طریق یک دستگاه بر روی کابل قرار داده می‌شود 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 می‌شوند.

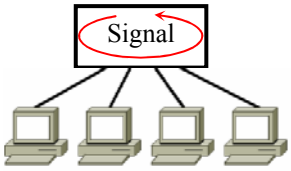


شکل ۱



۲- توپولوژی حلقوی یا Ring

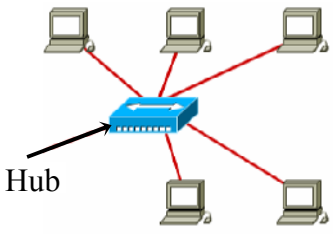
در این همبندی مانند همبندی خطی کابل رابط از یک دستگاه به دستگاه دیگر متصل می‌شود با این تفاوت که دو سر آزاد کابل نیز به هم متصل هستند . ارسال پیام ها توسط هر دستگاه تنها در یک مسیر حرکت کرده و توسط اولین دستگاه همسایه که در مسیر قرار دارد قابل دریافت است. یک اشکال همبندی حلقوی این است که اضافه کردن و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



شکل ۲

۳- توپولوژی ستاره ای یا Star

در این همبندی هر دستگاه از طریق کابل رابط خاص خود به یک دستگاه مرکزی یا CENTRAL HUB بسته می‌شود. 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 می‌تواند 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 می‌تواند 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 می‌تواند 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 می‌تواند 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 می‌باشد شبیه به روش صحبت کردن در یک اتاق شلوغ است، در چنین اتاقی شخصی که می‌خواهد صحبت کند باید با گوش دادن مطمئن شود که فرد دیگری در حال صحبت نیست و سپس اقدام به صبت کند . پس در این روش هر برد میانجی شبکه (کارت شبکه) که در داخل یک کاپیوتر نصب شده است به صورت متوالی خط را تجزیه و تحلیل می‌کند هرگاه این ایستگاه پیامی‌برای ارسال داشته باشد پس از خالی شدن خط اقدام به ارسال پیام می‌کند .در این سیستم هر گاه 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 می‌باشد.

هرگاه که یک برخورد صورت گیرد پیام محسوسی به نام Jam در خط ارسال می‌شود این پیام با تغییر سطح ولتاژ مستقیم در خط کلیه ایستگاه ها را از برخورد مطلع می‌کند سپس دو دستگاهی که در

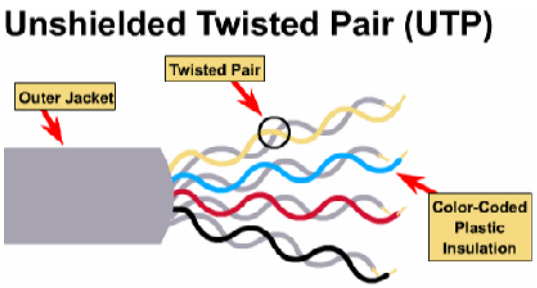
برخورد شرکت داشته اند هر یک به اندازه زمان تصادفی صبر می‌کنند و سپس در صورت خالی بودن خط اقدام به ارسال پیام می‌کنند . مزیت اساسی این سیستم سادگی و کارایی بسیار خوب در شرایط عادی است و اشکال عمده آن کم شدن کارایی سیستم در ترافیک بالاست.

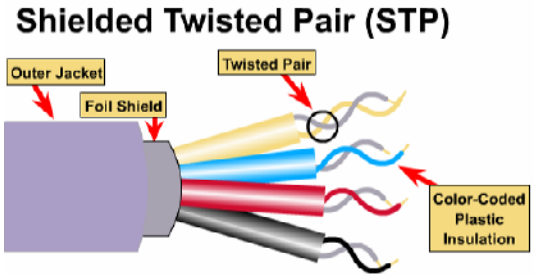
۳-کانال ارتباطی :

منظور از کانال ارتباطی محیط فیزیکی ارتباط دهنده اجزای شبکه است . محیطهای رایج برای ارتباط در شبکه‌های 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 می‌گیرند و یک کابل را تشکیل می‌دهند . چنین کابلی را UTP (Unshielded Twisted Pair) می‌نامند . اگر مجموعه سیم های تابیده شده داخل یک غلاف آلومینیمی قرار داده شود ، کابل حاصل را STP (Shielded Twisted Pair) می‌نامند.





محدودیتهای زیر در استفاده از این محیط وجود دارد :

- عدم امنیت درمقابل تداخل خارجي و نویز :

به علت ساختار فیزیکی این نوع کابل ، نویز محیط و ارتعاشات الکترو مغناطیسی حاصل از وسایل و ادوات الکتریکی موجود درنزدیک کابل ، می‌تواند 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 الکتریکي :

با زیاد شدن طول کابل سیگنال الکتریکی در داخل سیم تضعیف می‌شود. این امر باعث می‌شود 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 خازني کابل :

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

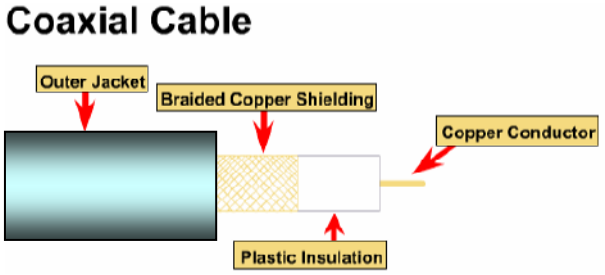
- هم شنوایي (Cross talk)

علاوه بر تداخل الکتریکی خارجی ،تداخل حاصل از القای الکتریکی و مغناطیسی بین جفت سیم‌های داخل یک کابل نیز کار این نوع کابل را محدود می‌کند . این امر در مورد کابلهای STP بیشتر رخ می‌دهد.

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

کـابـل 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 استوانه‌ای 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.



در مقابل ، اتصال و عملیات نصب این کابلها از سیم به هم تابیده شده مشکل تر و گرانتر می‌باشد . به علت بالا رفتن فرکانس در این کابلها ، قوانین خطوط انتقال مخابراتی بر آنها حاکم است.

طبق این قوانین برای هر کابل ، از روی ابعـاد سطح مقـطع کابل و مشـخصات فیزیکی بکار رفته در آن ،یک مقاومـت (بر حسب اهم) به دست می‌آید. این مقاومت را « مقاومت مشخصه » (Characteristic Impedance) کابل می‌نامند.

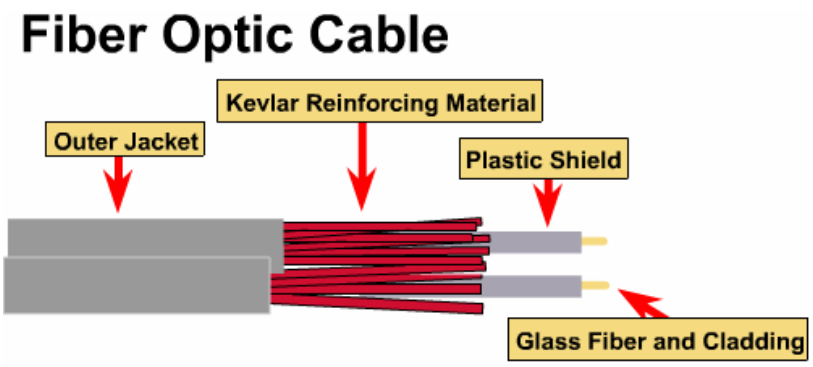
اهمیت این مقدار در این است که ، هرگاه یک کابل به مقاومتی برابر با مشخصه اش منتهی شود ، پیام الکتریکی فرستاده شده در خط ، در برخورد به انتهای خط منعکس نمی‌شود. در غیر اینصورت در انتهای خط ، انعکاس رخ می‌دهد و پیام منعکس شده با پیام بعدی که در حال ارسال است ، تداخل می‌کند و محیط انتقال غیر قابل استفاده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

به هم این دلیل دو انتهای کابل هم محور ، توسط مقاومتی برابر با مقاومت مشخصه کابل ، مسدود می‌شود. 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 ، مقاومت مشخصه در این قسمت عوض شده و این قسمت مانند قطعه کابلی با مشخصه متفاوت عمل می‌کند.

فـيـبر نـوري (Optical Fiber Cable)

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



این کابها از میله های بسیار نازکی از یک جنس شفاف مانند بروسیلیکات ژرمانیم که در یک غلاف با ضرب شکست متفاوت قرار دارند ، ساخته شده اند. مجموعه‌ای از چند میله فیبر نوری و چند سیم فلزی ، که برای افزایش قدرت مکانیکی اضافه شده‌اند ، در یک غلاف پلاستیکی قرار می‌گیرند.

کابلهای فیبر نوری به سه دسته اصلی تقسیم می‌شوند :

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

کابلهای Step- index Multimode دارای قیمت ارزانتر و کیفیت پایین تری هستند و بیش از انواع دیگر فیبر نوری در شبکه های کامپیوتری مورد استفاده قرار می‌گیرند.

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 مجددا 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 تمامی‌مراحل ارتباط می‌شود. وجود این قرارداده ها 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 می‌کند. این امر موجب می‌شود که محصولات تولید کنندگان مختلف که برای کار با یک قرارداد بخصوص ساخته شده اند بدون ایجاد مشکل در کنار هم کار کنند .

۱- قـرارداد Ethernet :

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

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 ۲٤) با مقاومت مشخصه 150Ω	
کابل فیبر نوری با قطر ۱۰۰ و ۱۲۰ و ۱٤۰ میکرون	

۲- قـرارداد IEEE802.3 :

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

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- قـرارداد IEEE802.5 : سیستم Token Ring

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

در Token Ring از همبندی حلقه و روش انتقال علامت استفاده می‌شود. محیط انتقال سیم به هم تابیده و کابل هم محور است . اگرچه همبندی سییستم از نوع حلقه‌ای است اما به ظاهر مانند همبندی ستاره به نظر می‌رسد .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 می‌شوند.

٤- قـرارداد ARCNET : (Attached Resource Computer Network)

از همبندی Star روش انتقال علامت استفاده می‌کند. محیط انتقال در این سیستم می‌تواند 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 می‌شوند . با گسترش شبکه می‌توان HUB های دیگری را نیز به شبکه افزود . حداکثر فاصله یک ایستگاه از یک HUB فعال برابر ٦۰۰ متر می‌باشد. عیب یابی و رفع اشکالات مربوط به کابل برای Arcnet آسان است زیرا بدون اختلال در کار ایستگاه‌های شبکه می‌توان کابلهای مربوط به یک ایستگاه را از شبکه جدا کرد.

٥- قـرارداد 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/IPبه عنوان بهترین قرارداد بین برای ارتباط بین شبکه ها با قراردادهای مختلف و ارتباط بین شبکه های میکروکامپیوتری و کامپیوترهای بزرگ شناخته می‌شود.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 می‌دهد. IP در لایه شبکه از مدل OSI کار می‌کند و خدمات TCP در لایه انتقال آغاز شده و می‌تواند تا لایه نمایش ادامه یابد. در واقع TCP از خدمات ارائه شده توسط IP استفاده می‌کند.

TCP در ایستگاه مبدا اطلاعاتی را که از لایه بالاتر دریافت می‌کند ، به بسته هایی به نام Segment تقسیم می‌کند. IP پس از دریافت این بسته ها اطلاعات مربوط به لایه شبکه را به آنها می‌افزاید.

بسته های اطلاعات در IP را اصطلاحاً Data gram می‌نامند. این Data gram ها از طریق لایه های زیرین به لایه شبکه در ایستگاه مقصد منتقل می‌شوند. در ایستگاه مقصد عمل عکس انجام می‌گیرد و Data gram ها اطلاعات بصورت Segment استخراج شده و از روی Segment ها اطلاعات بازیابی می‌شود.

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

در IP یک مسیر منطقی ثابت بین ایستگاه فرستنده و ایستگاه گیرنده برقرار نمی‌شود ، 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 می‌شوند ، 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 نمی‌دهد و ایجاد اطمینان از رسیدن پیام به مقصد در TCP صورت می‌گیرد.

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

در یک مجموعه از شبکه ها که از TCP/IP استفاده می‌کنند Data gram مهلتی برای رسیدن به مقصد دارد. اگر پس از انقضای این مهلت Data gram به وسیله ایستگاهی دریافت نشود از بین می‌رود. 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 می‌سازند . 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 ارئه 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 می‌کند 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 گذاردن هارد دیسک ایستگاه ، امکان ارتباط با سیستمهای بزرگ با قراردادهای TCP/IPو 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 می‌شود ، 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 قابلیتهایی 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 می‌کند. سیستم عامل STF Netware امکان نگهداری کل اطلاعات در دو هارد دیسک مجزا را فراهم می‌کند. این دو هارد دیسک کاملا یکسان بوده و عملیات نوشتن بطور همزمان روی هر دو هارد دیسک اجرا می‌شود. در صورت از دست رفتن اطلاعات موجود بر روی یکی از هارد دیسکها ، اطلاعات موجود بر روی دیگری می‌تواند مورد استفاده قرار گیرد. این امر امکان دستیابی به شبکه هایی با قابلیت اطمینان بسیار بالا را فراهم می‌کند.

کنترل کیفیت سطح هارد دیسک هنگام نوشتن و Hot Fix Redirection

Netware پس از نوشتن هر بلوک بر روی هارد دیسک ، آنرا می‌خواند. چناچه 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 می‌نویسد.

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

حداکثر استفاده از حافظه

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

Disk Hashing

File Server اطلاعات مربوط به محل فایلهای روی دیسک را در RAM نگهداری می‌کند. هنگامیکه یک کاربر تقاضای دریافت یک فایل را به File Server می‌فرستد محل این فایل به سرعت در Ram پیدا شده و سرویس دهی به سرعت انجام می‌گیرد.

Disk Caching

هر گاه یک کاربر تقاضای دریافت فایلی را به File Server بفرستد Netware اطلاعت قسمتی از هارد دیسک را که مربوط به این فایل است کلا به Ram منتقل می‌کند هرگاه اطلاعت دیگری مربوط به این قسمت از هارد دیسک تقاضا شود ، سرویس دهی بجای هارد دیسک از Ram صورت می‌گیرد. از آنجا که زمان دستیابی به اطلاعات در هارد دیسک در حد میلی ثانیه و درRam در حد میکروثانیه است ، این عمل سرعت جوابگوییFile Server را بیش از صد برابر افزایش می‌دهد . 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 پرونده‌های افراد موجود در یک لیست است و اسامی‌این 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 می‌کند ، عیناً همین عوامل را در مورد سرویس دهی از هارد دیسک انجام می‌دهد. گرچه File Server کاربران شبکه را برای دریافت سرویس در نوبت قرار می‌دهد ، اما سرویس دهی به تقاضاهایی که مربوط به محلی در نزدیکی محل فعلی هد هارد دیسک باشند خارج از نوبت انجام می‌گیرد.

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، نمی‌تواند تحت سیستم عامل ویژه‌ای کار کند. در نتیجه قسمتی از نرم افزار شبکه که در ایستگاه اجرا می‌شود 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، نمی‌کند. این سیستم عامل امکان استفاده از مجموعه‌ای از سیستمهای عامل مختلف را، در یک شبکه فراهم می‌کند.

سیستم عامل Netware از مجموعه ای بنام shell استفاده می‌کند. در شبکه ای که ایستگاه‌های آن از DOS استفاده می‌کنند، 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 می‌کند، این برنامه تصمیم می‌گیرد 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 می‌شود، در غیر اینصورت از طریق شبکه اجرا خواهد شد.

در فصل ٤ 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 شبکه‌ای ، 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 می‌دهد. 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 می‌تواند 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 می‌دهد. این روشها به دو دسته اساسی تقسیم می‌شوند.

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

٢- روش Semaphore برای ایجاد هماهنگی در دسترس 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 می‌رود. در این روش هر برنامه ای که بخواهد به یک فایل و یا یک رکورد دسترسی داشته باشد از سیستم عامل می‌خواهد 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 می‌شود. 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 می‌خواهد که قفل را بردارد.

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

از نظر عملکرد قفل ها را می‌توان 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 می‌شود.

قفل های فیزیکی و منطقی

قفل منطقی قفلی است که فقط جنبه اخباری داشته و در آن هماهنگی تنها از طریق اعتماد متقابل رعایت می‌شود. در صورت استفاده از این نوع قفل حتی اگر برنامه درتقاضای 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 ، عملا جلوگیری می‌کند. در این صورت حتی در صورت عدم رعایت قفل توسط یک برنامه امکان تداخل برنامه ها وجود ندارد.

قفلهای باصبر و بدون صبر

در روش قفل بدون صبر ، نتیجه درخواست قفل سریعا از طرف سیستم عامل به اطلاع برنامه می‌رسد. 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 می‌کند و نتیجه مثبت را به برنامه اطلاع می‌دهد . در سیستم هایی که حداکثر زمان استفاده هر برنامه از اطلاعات ، مشخص و قابل قبول است ، استفاده از این روش اشکالی ایجاد نمی‌کند. 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 می‌دهند. در این نرم افزارها روش قفل گذاری در حالت عادی از نوع بدون صبر است . اما این امکان به برنامه نویس داده می‌شود 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 می‌دهند 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 برنامه‌ها داده می‌شود 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 می‌شود.

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 می‌شود. (Semaphore) در واقع متغیری است که توسط سیستم عامل نگهداری و کنترل می‌شود و می‌تواند مقادیر مثبت یا صفر داشته باشد. هر (Semaphore) دسترسی به یکی از امکانات شبکه را کنترل می‌کند و دارای یک ارزش است. ارزش (Semaphore) مربوط به هر یک از امکانات شبکه برابر حداکثر تعداد برنامه هایی است که می‌تواند 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 می‌خواهد از امکانات شبکه استفاده کند تقاضا برای سیستم عامل می‌فرستد . سیستم عامل بر اساس مقدار (Semaphore) ، در مورد در اختیار دادن این امکان تصمیم می‌گیرد. اگر مقدار (Semaphore) عددی مثبت باشد ، امکان مورد نظر در اختیار برنامه قرار می‌گیرد و یک واحد از (Semaphore) کم می‌شود. 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 می‌کند ، این امر باعث افزوده شدن یک واحد به مقدار (Semaphore) می‌شود.

Deadlock چیست؟

در بسیاری از موارد ممکن است دو برنامه جهت ادامه کار خود احتیاج به قفل کردن انحصاری مجموعه‌ای 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 می‌شود. این حالت مختص دو برنامه نبوده و می‌تواند 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 نمی‌تواند 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 تمامی‌اطلاعات 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 نمی‌شود.

Transaction Tracking

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

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 می‌کند ، یا تمامی اطلاعات در فایلهای مختلف به روز در می‌آیند ویا در صورت به وجود آمدن اشکال ، کلیه فایلها به حالت اولیه برمی‌گردند.

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

فصل چهارم

امنیت شبکه (۱)

شبکه کامپیوتری یک سیستم اطلاعاتی گسترده است و افراد می‌توانند 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 می‌شود:

الف- چه کسی در شبکه کار می کند؟

ب- اجازه چه کارهایی به او داده می‌شود؟

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 می‌پرسد. 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 می‌شود 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 می‌پردازیم.

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 می‌کند. این دسته بندی باید به دقت صورت گیرد و افرادی که در یک دسته قرار می‌گیرند باید در اطلاعات مورد نیاز و یا عملیاتی که انجام می‌دهند، 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 می‌شود، در ابتدای ایجاد سیستم به صورت اتوماتیک ایجاد می‌شود. 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.
گروه‌بندی کاربران توسط مدیر شبکه صورت می‌گیرد و هر کاربر تنها می‌تواند از نام گروه‌ها 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 می‌شود. 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 نمی‌شود. کد عبور و نام کاربر را می‌توان 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 می‌شود و سپس پیامی مشابه پیام 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 می‌شود. 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 می‌شود. در سیستم عامل Netware تدابیری برای حفظ امنیت کد عبور در اختیار مدیر شبکه قرار دارد. این تدابیر شامل این موارد می‌شود :

- مدیر شبکه می‌تواند به کاربران اجازه تعویض کد عبور را بدهد و یا ، این حق را از آنها بگیرد. در هر دو صورت مدیر شبکه می‌تواند کد عبور کاربران را عوض کند.

- مدیر شبکه برای افزایش امنیت کد عبور می‌تواند کاربران را مجبور به داشتن کد عبور کند. در حالت کلی یک کاربر می‌تواند کد عبور نداشته باشد.
- مدیر شبکه می‌تواند 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 می‌تواند کاربران را به تعویض متوالی کد عبور ملزم کند. در صورت استفاده از این امکان، مدیر شبکه می‌تواند زمان بین دو بار تعویض کد عبور را تعیین کند.
- پس از انقضای زمان اعتبار یک کد عبور، کاربر می‌تواند چندین بار با کد عبور قبلی وارد شبکه شود، مدیر شبکه می‌تواند این تعداد را تعیین کند. ورود کاربر با کد عبور منقضی شده را اصطلاحاً «ورود اعتبار» (Grace login) می‌نامند.
- در حالت عادی کد عبور جدید می‌تواند برابر با کد عبور قبلی باشد. در صورت لزوم می‌توان 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 می‌شود 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

درحالت عادی یک کاربر می‌تواند در هر ساعتی از شبانه روز ودر هر روز از هفته وارد شبکه شود. اما مدیر شبکه می‌تواند 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 می‌توان 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 می‌شود. در اوقات خارج از ساعات کاری از ورود کاربر به شبکه جلوگیری خواهدشد.

اگر کاربری در ساعات ممنوعه سعی در ورود به شکبه داشته‌باشد 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 خواهدکرد.

>> 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 فایلهای مربوط به کاربربسته می‌شود ،اما ممکن است برنامه در حال کار در ایستگاه به محل مناسبی برای قطع ارتباط نرسیده‌باشد و به این ترتیب به اطلاعات صدمه وارد شود. لذا کاربران باید به پیام‌های فوق توجه کنند.

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

محدودیت ایستگاه

در حالت عادی یک کاربر می‌تواند از هر یک از ایستگاه‌های شبکه وارد شود. امکانات و اجازه کاربر برای انجام عملیات در شبکه بستگی به نام کاربر و کدعبور او دارد و ارتباطی با ایستگاهی که از آن وارد شبکه شده‌است ، ندارد.

اما مدیر شبکه می‌تواند 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 خواهدکرد :

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 می‌شود. 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 می‌تواند 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 می‌تواند 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 می‌تواند تعداد ایستگاه هایی را که یک کاربر می‌تواند 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 می‌تواند افراد بدون صلاحیت را که سعی در ورود به شبکه دارند ، تشخیص دهد. برای این کار باید تعداد دفعات متوالی را که یک کاربر می‌تواند 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 می‌تواند 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 می‌شود :

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

در این حال حساب کاربر مربوطه مسدود می‌شود و تنها مدیر شبکه می‌تواند 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 مجددا به جریان اندازد.

مدیر شبکه می‌تواند 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 می‌شود.

فصل پنجم

امنیت شبکه (۲)

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

تدابیر امنیتی

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

۱- مجوزهای (Trustee Assignment) ـ این مجوزها ، در حد کاربر عمل می‌کنند. هر کاربر ممکن است دریک 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 می‌نامند. مجوزهای عضویت یک کاربر ، می‌تواند با مجوزهای عضویت کاربر دیگر متفاوت باشد.

۲- مجوزهای معتبر در کشو (Maximum Rights Mask) ـ این مجوزها در سطح کشو عمل می‌کنند و اعتبار مجوزهای کاربر را در یک کشو تعیین می‌کنند. مجوزهای معتبر در کشو از متعلقات هر کشو بوده و از طریق این مجوزها توانایی لازم برای انجام یک عمل ، برای کلیه کاربران تعیین می‌شود. 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) ـ این قسمت از تدابیر امنیتی در سطح فایل عمل می‌کند و اجازه انجام عملیات روی یک فایل خاص را تعیین می‌کند.

مجوزهای (Trustee Assignment)

این مجوزها ، که اجازه انجام عملیات را در سطح کاربر کنترل می‌کند ،می‌توانند 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 می‌نامند.توجه کنید مفهوم یک عضو نباید با مفهوم کاربر اشتباه شود. ممکن است کسی کاربرشبکه باشد اما هیچ مجوزی در یک کشو خاص نداشته باشد ، در این صورت او عضو این کشو نیست.

نکته مهم در مورد مجـوزهای عضویت این است که این مجوزها مانند کد عبور و محـدودیتهای ورود به شبکه از متعلقات بک کاربـر هستند و اجازه او برای انجام برخی عملیات در یک کشـو خاص را تعیین می‌کنند :

این مجوزها عبارتند از :

O	(Open)	مجوز باز کردن فایلها
R	(Read)	مجوز خواندن از فایلی که باز شده است
W	(Write)	مجوز نوشتن در فایلی که باز شده است
C	(Create)	مجوز ایجاد (و باز کردن هنگام ایجاد) یک فایل
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 ، می‌تواند مجوزهای عضویت سایر کاربران درکشو را تغییر دهد و یا مجوزهای کشو را عوض کند.

مجوز یک کاربر در یک کشـو می‌تواند یک , یا ترکیبی از این مجوزها باشد. یکی از ترکیبهای این مجوزها (هیچ مجوز) است. این ترکیب را بصورت [ ] نشان می‌دهیم. کاربری که در یک کشو دارای (هیچ مجوز) باشد با کاربری که در این کشو مجوزی ندارد متفاوت است.

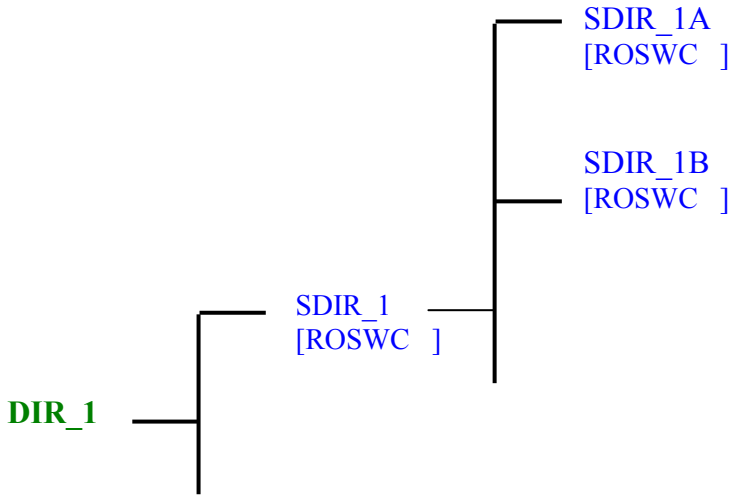
به عنوان مثال ، فرض کنید که کاربری به نام user1 در یک کشو داری مجوزهای[ROSWC] است و user2 در همین کشو دارای مجوز [ ] است و کابر دیگری به نام user3 مجوزی در این کشو ندارد.

در این حالت کاربران user1 و user2 عضو این کشو هستند اما user3 عضو این کشو نیست. اگرچه در عمل user2 و user3 هر 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 می‌شود.

اگر کاربری در یک کشو دارای مجوز C باشد ، می‌تواند در این کشو یک فایل جدید ایجاد کند اما برای وارد کردن ازاطلاعات در این فایل به مجوز W احتیاج دارد. همچنین پس از بستن فایل برای 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 کشو DIR_1 مجوزهای عضویت [ROSWC] داده شده است. در این حال کاربر ، در کلیه زیرکشو های این کشو ، 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 کشو مورد نظر مجوز داده شود.

برای جلوگیری از جریان یافتن مجوزهای کشو قبلی در یک کشو باید در آن کشو مجوزها مجدد تعریف شوند. به عنوان مثال اگر بخواهیم در مثال قبل کاربر در زیر کشو SDIR_1A اجازه انجام کاری را نداشته باشد باید مجوزهای عوضیت او را در کشو مزبور برابر هیچ مجوز قرار دهیم. در این صورت مجوزهای این کاربر در کشو SDIR_1A و زیر کشوهای آن برابر [ ] خواهد بود.

با مثال فوق تفاوت میان کاربری که در یک کشو دارای مجوز [ ] است با کاربری که مجوز در این کشو ندارد (عضو این کشو نیست) ، مشخص می‌شود. اگر کاربری عضو یک زیر کشو 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 می‌دهد کلیه مجوزهای عضویت یک کاربر دیگر را داشته‌باشد. 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 می‌کند 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] خواهدشد و مجوزهای ALI همان [ROSWC] باقی خواهدماند. 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 می‌تواند مجوزهایی در یک کشو داشته باشد . این مجوزها عیناً مانند مجوزهای یک کاربر هستند. مجوزهایی که به یک گروه داده می‌شود ، به کلیه اعضاء آن گروه منتقل می‌شود. هر گاه کاربری عضو یک گروه شود ، با آن گروه برابری امنیتی خواهدداشت و کسی که با یک گروه برابری امنیتی شود ، عضو آن گروه خواهد شد.

مجورهای معتبر در کشو (MAXIMUM RIGHTS MASK)

این مجوزها ، که در سطح کشو عمل می‌کنند ، اعتبار اختیارات کاربران در یک کشو را تعیین می‌کنند. مدیر شبکه از این امر مستثنی بوده و در کلیه کشوها اختیارات را دارد.
این مجوزها مانند مجوزهای عضویت عبارتند از :

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

(سایر کاربران درکشو 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 همهٔ مجوزهای فوق می‌شود. به این ترتیب یک کاربر می‌تواند همهٔ این حقوق را در این کشو داشته‌باشد. برای محدود کردن مجوزهای معتبر در این کشو (برای همهٔ 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 می‌کنند ، از این پس حتی کاربرانی که دارای مجوز عضویت D نیز باشد نمی‌توانند 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 نمی‌کنند.

از آنجا که پس از حذف یک مجوز از مجوزهای معتبر در کشو ، هیچ کاربری قادر به انجام عمل مربوطه نخواهدبود ، به جز موارد خاص مجوزهای معتبر در کشو برابر [ROSSWCDMP] (کلیه مجوزها) قرارداده می‌شوند.

مشخصه فایل‌ها (File Attribute)

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

- **مشخصه N (Normal)**

این مشخصه ، مشخصه‌ای 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 می‌توانندابن فایل را بخوانند و هیچ کاربری نمی‌تواند آنرا پاک کند ، نام آنرا تغییر دهد و یا چیزی در آن بنویسد. این امر بستگی به مجوزهای کاربرندارد.

- **مشخصه RW (Read Write)**

فایلی که دارای این مشخصه باشد ، می‌تواند 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 می‌تواند به وسیله چند کاربر به اشتراک گذاشته شود. این مشخصه با مشخصه RO به کار می‌رود.

مشخصه M (Modified)

هر بار که از فایلهای شبکه پشتیبان تهیه می‌شود کلیه فایلها از مشخصه Modified خارج می‌شوند. 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 می‌توان برای فایلهایی با دنباله EXE و COM به کار برد. فایلی که دارای چنین مشخصه‌ای باشد تنها قابل اجراست. در صورت استفاده از این مشخصه از نوشتن در داخل فایل ، پا ک 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 می‌کند. نام چنین فایلهایی در لیست فایلهای یک کشو ظاهر نمی‌شود. صدمه دیدن چنین فایلی می‌تواند کار سیستم عامل را دچار اشکال کند.

مشخصه I (Indexed)

برای تسریع در دستیابی به قسمتهای مختلف فایلهایی که دارای حجمی بیش از ۲ مگا بایت هستند ، از این مشخصه استفاده می‌شود. سیستم عامل شبکه ، آدرس قطعات مختلف یک فایل را در جدولهای مختلف فایلها نگهداری می‌کند. تعداد قطعات مختلف یک فایل بزرگ می‌تواند زیاد شود و در این صورت برای دستیابی به یک قطعه از این فایل زمان زیادی برای یافتن آدرس آن صرف می‌شود. با استفاده از مرتب سازی آدرسها ، می‌تواند 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 فایلهای یک کشو ظاهر نخواهد شد. بسیاری از نرم افزارها برای کار خود از فایلهایی با این مشخصه استفاده می‌کنند. در بسیاری از موارد تغییردر 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 دریک 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 می‌شوند. 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 نمی‌توان حذف کرد یا تغییر داد.
- کد عبور یک کاربر را نمی‌توان تغییر داد.
- مجوزهای یک کاربر را نمی‌توان تغییر داد.
- مجوزهای معتبر در کشو را نمی‌توان تغییر داد.
- پیام خطا در Bindary روی File Server نمایش داده می‌شود.

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 می‌توان از برنامه کمکی BINDFIX استفاده کرد. این برنامه ابتدا فایلهای مربوط به Bindary را از دسترس کابران خارج کرده و سپس عملیات بازسازی را روی آن انجام می‌دهد . پس از پایان عمل باز سازی این فایلها مجددا در دسترس کاربران قرار می‌گیرند.

در حین عملیات باز سازی BINDFIX مراحل عمل را گزارش داده و در برخی از موارد از مدیر شبکه کسب تکلیف می‌کند. 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 می‌کند و در فایلهای NET$BIND.SYS و NET$BVAL.SYS نگهداری می‌کند.

در صورت موفق بودن عمل باز سازی ، BINDFIX از کاربر می‌خواهد که فایلهای OLD. را پاک کند.

در صورت بروز اشکال در عمل باز سازی ، می‌توان با اجرای دستور BINDREST فایلهای مربوط به Bindary را به صورت اول بازگرداند.

دستور BINFIX به وسیله مدیر شبکه قابل اجرا بود و در دسترس کاربران قرار ندارد.