«بـــــــه نام خـــالق آرامـــش»

نام کتاب: مبانی شبکه

نام نویسنده: هاتور رهانزو

تعداد صفحات: ۶۴ صفحه

تاریخ انتشار: سال ۱۴۸۵

@caffeinebookly caffeinebookly @caffeinebookly caffeinebookly t.me/caffeinebookly

شهر مجازی پارسیان
VIRTUALCITY4PERSIAN

مبانی شبکه

نویسنده : هاتوری هانزو

تقدیم به همه دوستان و همشهریان عزیز شهر مجازی پارسیان

@caffeinebookly caffeinebookly @caffeinebookly caffeinebookly t.me/caffeinebookly

شناسنامه کتاب

نویسنده : هاتوری هانزو
ناشر : شهر مجازی پارسیان
نوع نشر : الکترونیکی
تاریخ انتشار : مهر ۱۳۸۵

تمام حقوق ماده و معنوی این کتاب متعلق به نویسنده و ناشر (شهر مجازی پارسیان) میباشد. استفاده از مطالب و انتشار مجدد به هر صورت با ذکر منبع اثر آزاد است.

@caffeinebookly caffeinebookly @caffeinebookly caffeinebookly t.me/caffeinebookly

فصل ۱ : آشنایی با شبکه

در این فصل میخوانید :

- مقدمه ای بر شبکه های کامپیوتری
- همه چیز در مورد کلاینت ها، سرور ها و Peer ها
- شناخت انواع مختلف شبکه بندی
- مزایا و معایب انواع شبکه بندی

@caffeinebookly caffeinebookly @caffeinebookly caffeinebookly t.me/caffeinebookly

اولین شبکه کامپیوتری هنگامی اختراع شد که ریاضیدانان باستان چرتکه های خود را به کمک کایت به هم متصل کردند و بدین ترتیب آنها بلافاصله از جواب های یکدیگر مطلع میشدند. پس از سالها، شبکه های کامپیوتری بسیار خاص و خاص تر شدند. اکنون به جای نخ های کایت از کابل های الکتریکی، فیبر نوری یا امواج رادیویی استفاده میشود و کامپیوتر های به هم متصل میشوند. بهرحال، هدف همان هدف سابق است یعنی : اشتراک اطلاعات و انجام سریعتر کارها. در این بخش به مبانی شبکه های کامپیوتری و نحوه کار آنها میپردازیم.

شبکه چیست؟

شبکه چیزی جز دو یا چند کامپیوتر متصل به هم نیست که بدین ترتیب قادرند تبادل اطلاعات داشته باشند. اطلاعاتی مانند پیغامهای پست الکترونیکی یا مستندات یا منابع سخت افزاری و نرم افزاری. در بسیاری از حالات، این ارتباط از طریق کابل های الکتریکی حامل اطلاعات بصورت سیگنال الکتریکی انجام میشود. ولی در برخی موارد، سایر انواع انصالات مورد استفاده قرار میگیرند. برای مثال، کابلهای فیبر نوری به سیستم ها اجازه میدهند تا با سرعت بسیار بالا از طریق شعاع های نوری به تبادل اطلاعات بپردازند. شبکه های بی سیم نیز امکان ارتباط سیستم ها را از طریق سیگنال های رادیویی فراهم میکنند که در این حالت کامپیوتر های توسط کابل های فیزیکی محدود نمیشوند و قابلیت جابجایی راحت برای آنها بوجود می آید.

علاوه بر سخت افزاری که مسئول شبکه است، یک شبکه نیاز به نرم افزار خاصی برای ایجاد ارتباط دارد. در ایام قدیم شبکه شما باید این نرم افزار را روی هر کامپیوتر روی شبکه اعمال میکردید. امروزه، پشتیبانی از شبکه ها داخل تمام سیستم عامل های اصلی قرار دارد که میتوان تمام نسخه های جدید ویندوز، سیستم عاملهای مکینتاش و لینوکس را از این جمله نامید.

قطعات سازنده شبکه

تمام شبکه ها، بزرگ یا کوچک، نیاز به سخت افزار مخصوص شبکه برای شروع به کار دارند. برای شبکه های کوچک، سخت افزار ممکن است چیزی جز یک کارت شبکه روی هر سیستم، یک کابل برای هر کامپیوتر و یک سویچ کوچک که تمام کامپیوتر ها به آن متصل میشوند نباشد. در مقابل شبکه های بزرگتر اجزای بیشتری دارند که میتوان روتر ها و تقویت کننده ها را از آن جمله دانست. جدا از بزرگی یا کوچکی، تمام شبکه ها از قطعات اساسی زیر تشکیل میشوند :

- **کامپیوتر های کلاینت (میهمان/سرویس گیرنده)** : کامپیوتر هایی که کاربر نهایی از آنها برای دسترسی به منابع روی شبکه استفاده میکند. کامپیوتر های کلاینت معمولاً روی میزکار

@caffeinebookly caffeinebookly @caffeinebookly caffeinebookly t.me/caffeinebookly

کاربران قرار داده میشوند. این سیستم ها نسخه ی Desktop از سیستم عامل مورد نظر مانند Windows XP Professional را اجرا میکنند و نرم افزار های مورد نیاز هر سازمان برای مثال مانند Microsoft Office نیز روی آنها نصب میشود. کامپیوتر های کلاینت در اصطلاح « ایستگاه کاری » نیز نامیده میشوند.

- **کامپیوتر های سرور (میزبان/سرویس دهنده)** : کامپیوتر هایی که منابع مشترک را فراهم میکنند مانند محل ذخیره روی دیسک ها و چاپگرها. کامپیوترهای سرور معمولاً دارای یک سیستم عامل شبکه خاص مانند Windows 2003 Server، NetWare، یا Linux میباشند که همراه با نرم افزار های خاصی سرویس های شبکه را فراهم میکنند. برای مثال، یک سرور میتواند Microsoft Exchange را برای ایجاد سرویس Email در شبکه اجرا کند و یا از Apache Web Server برای سرویس دهی صفحات وب بهره ببرد.
- **کارت های رابط شبکه (NIC ها)** : سخت افزاری که روی یک کامپیوتر نصب میشود تا کامپیوتر بتواند به شبکه متصل شده و به تبادل اطلاعات بپردازد. تقریباً تمام NIC ها دارای یک استاندارد شبکه بنام Ethernet هستند. کامپیوتر های جدید طوری طراحی شده اند که کارت های Ethernet روی برد اصلی آنها وجود دارد و بدین ترتیب، نصب سخت افزار اضافی مورد نیاز نمی باشد. هر کامپیوتر کلاینت و هر سروری باید کارت رابط شبکه داشته باشد تا بتواند بعنوان بخشی از شبکه فعالیت کند.
- **کابل** : کامپیوتر های موجود در یک شبکه معمولاً بطور فیزیکی از طریق کابل به هم متصل شده اند. با اینکه در طول سالها انواع مختلف کابل ایجاد شده مورد پسند نیز بوده، ولی معمول ترین نوع کابل امروزه « جفت تابیده » نامیده میشود که با کدگذاری رسمی 10BastT نامیده میشود. کابل دیگری نیز که معمولاً مورد استفاده قرار میگیرد کواکسیال نامیده شده و 10Base2 نامیده میشود. برای شبکه های سریعتر، کابل فیبرنوری نیز مورد استفاده قرار میگیرد. در بسیاری از موارد، کابل از درون دیوار های عبور میکند و در یک اتاق مرکزی به هم میرسند که « گنجه کابل » نامیده میشود، ولی در شبکه های کوچک، کابل از روی زمین عبور میکند.
- **سویچ ها** : کابل های شبکه معمولاً کامپیوترها را مستقیماً به هم متصل نمیکنند. در عوض، هر کامپیوتر توسط کابل به دستگاهی بنام Switch متصل میشود. سویچ هم به سایر قسمت های شبکه متصل است. هر سویچ دارای تعداد مشخصی درگاه (Port) میباشد که معمولاً ۸، ۱۶ یا ۳۲ است. پس میتوانید از یک سویچ ۸ پورتی برای اتصال ۸ کامپیوتر به هم استفاده کنید. با اتصال سویچ ها به هم میتوان شبکه های بزرگتری بدست آورد. برای اطلاعات بیشتر در مورد سویچ ها میتوانید از بخش توپولوژی های شبکه کمک بگیرید. شبکه های قدیمی تر از

@caffeinebookly caffeinebookly @caffeinebookly caffeinebookly t.me/caffeinebookly

انواع ابتدایی تری بنام هاب به جای سویچ استفاده میکردند. هاب همان عملکرد سویچ را دارد ولی به اندازه سویچ کارآیی و قابلیت ندارد. عبارت هاب گاهی به مفهوم سویچ بکار میرود در حالیکه سویچ ها و هاب ها از نظر عملکرد کاملاً متفاوتند.

- **شبکه های بی سیم** : در بسیاری از شبکه ها، کابل ها و سویچ ها جای خود را به شبکه ی بی سیم داده اند که بدین ترتیب سیستم ها میتوانند از طریق امواج رادیویی با یکدیگر ارتباط برقرار کنند. در شبکه بی سیم، فرستنده/گیرنده های رادیویی جای کابل را میگیرند. مزیت عمده شبکه بندی بی سیم، قابلیت انعطاف آن است. با یک شبکه بی سیم، نیازی به کابل کشی در دیوار ها و سقف و کف ندارید و کامپیوتر های کلاینت شما میتوانند در محدوده پخش امواج شبکه در هر محلی قرار بگیرند. مهمترین ایراد شبکه های بی سیم نیز این است که امنیت کمتری نسبت به شبکه های سیمی دارد.
- **نرم افزار شبکه** : با اینکه سخت افزار شبکه اساس کار است، ولی چیزی که باعث کار سخت افزار میشود، نرم افزار است. برای بکار انداختن شبکه باید نرم افزار کاملی به این منظور نصب شود. کامپیوتر های سرور معمولا از یک سیستم عامل شبکه استفاده میکنند (که NOS نیز نامیده میشود) تا عملکردی درست داشته باشند و کامپیوتر های کلاینت باید تنظیمات شبکه خاص خودشان را داشته باشند تا به شبکه دسترسی پیدا کنند.
یکی از مهمترین انتخاب ها در شبکه بندی این است که چه سیستم عاملی برای سرور ها و کلاینت ها انتخاب کنید. اهمیت این مطلب در آن است که بیشترین کار در شبکه مربوط به نصب و تنظیمات سیستم عامل برای ساخت شبکه و یا مدیریت و ایجاد سرویس در شبکه موجود میباشد.

اگر بخواهیم واقعیت را بیان کنیم، شبکه بندی کامپیوتر های کاری بسیار خسته کننده و آزار دهنده است. ولی مزایای داشتن شبکه به زحمت و دردسر راه اندازی آن می ارزد. نیازی نیست که مدرک Ph.D داشته باشید تا مزایای استفاده از شبکه را درک کنید. در واقع، شما هر آنچه را که باید در مورد مزایای شبکه بدانید، در مهدکودک یاد گرفته اید. تمام مزیت شبکه ها در اشتراک است. مخصوصاً، شبکه ها میتوانند سه چیز را به اشتراک بگذارند : اطلاعات، منابع و برنامه های کاربردی.

- **اشتراک اطلاعات** : شبکه ها به کاربران این امکان را میدهند تا اطلاعات را به روش های مختلفی به اشتراک بگذارند. معمولترین روش اشتراک اطلاعات روی شبکه، اشتراک فایلها است. برای مثال، دو یا چند نفر با هم روی یک فایل نوشتاری کار میکنند. در بسیاری از شبکه ها، یک هارد دیسک بزرگ مرکزی وجود دارد که بعنوان مرکز ذخیره سازی معمول معرفی شده و تمام کاربران فایلهای اشتراکی خود را روی آن ذخیره میکنند. علاوه بر اشتراک فایلها،

@caffeinebookly caffeinebookly @caffeinebookly caffeinebookly t.me/caffeinebookly

شبکه ها به کاربران این امکان را میدهند تا با هم به روش های مختلف ارتباط برقرار کنند. برای مثال برنامه های پیغام رسان که به کاربران امکان ارسال و دریافت پیغام های الکترونیکی را میدهند. کاربران میتوانند روی شبکه یک ملاقات همزمان نیز داشته باشند. در واقع، با دوربین های ویدئویی ارزان قیمت و نرم افزار مناسب، کاربران میتوانند روی شبکه کنفرانس تصویری برقرار کنند.

- **اشتراک منابع** : منابع خاص کامپیوتری، مانند چاپگرها یا هارد دیسک ها، قابل اشتراک گذاری هستند طوریکه کاربران شبکه میتوانند از آنها استفاده کنند. اشتراک این منابع میتواند باعث صرفه جویی چشمگیری در هزینه های خرید سخت افزار شود. برای مثال، خرید یک چاپگر سریع با امکانات پیشرفته مانند صفحه بندی و چاپ دورو که روی شبکه مشترک باشد، بسیار ارزان تر و اقتصادی تر از خرید چاپگر برای هر کاربر بطور مجزا خواهد بود.

هارد دیسک ها را نیز میتوان به اشتراک گذاشت. در واقع، ایجاد دسترسی کاربران به هارد دیسک های مشترک معمول ترین روش اشتراک فایلها روی اینترنت است. کامپیوتری که هدف اصلی آن داشتن هارد دیسک های اشتراکی است بعنوان سرویس دهنده *فایل* نامیده میشود.

در عمل، کل هارد دیسک ها به اشتراک گذاشته نمیشوند. فقط پوشه های خاصی روی هارد دیسک بین کاربران شبکه مشترک خواهند بود. بدین ترتیب سرپرست شبکه میتواند به کاربران مختلف شبکه دسترسی به پوشه های مختلف را ارائه کند. برای مثال، در یک شرکت، ممکن است پوشه ها بصورت قسمت فروش و قسمت حسابداری طبقه بندی شوند. پس کارمندان فروش میتوانند به پوشه بخش فروش و کارمندان حسابداری میتوانند به پوشه بخش حسابداری دسترسی داشته باشند.

منابع دیگری نیز روی شبکه قابل اشتراک است. برای مثال، یک شبکه میتواند برای اشتراک ارتباط اینترنت مورد استفاده قرار گیرد. در اوایل اینترنت، رسم بود که هر کاربری که نیاز به دسترسی به اینترنت دارد، باید اتصال مودم خاص خود را می داشت. امروزه، اتصال دائم و پرسرعت اینترنت وارد سرور شبکه میشود و همه روی شبکه میتوانند بسته به تنظیمات سرور، میزانی از این اینترنت را در اختیار داشته باشند.

- **اشتراک برنامه های کاربردی** : یکی از عمده ترین علل شبکه بندی در بسیاری از قسمت ها این است که چندین کاربر بتوانند با هم روی یک کاربرد تجاری خاص کار کنند. برای مثال، بخش حسابداری ممکن است نرم افزار حسابداری داشته باشد که قابل استفاده از چندین سیستم بطور همزمان باشد. یک قسمت عملیات فروش ممکن است برنامه ی خرید/فروشی داشته باشد که چندین کامپیوتر وظیفه ثبت و پردازش سفارشات زیادی را عهده دارد شوند.

@caffeinebookly caffeinebookly @caffeinebookly caffeinebookly t.me/caffeinebookly

کلاینت ها و سرورها

نکته : کامپیوتر های شبکه که دارای هارد دیسک، چاپگر و سایر منابع میباشند و آنها را روی شبکه به اشتراک میگذارند، سرور نامیده میشوند. این عبارت همیشه تکرار خواهد شد و باید آنرا به خاطر بسپارید.

نکته : هر کامپیوتری که سرور نباشد، کلاینت است. این عبارت را نیز بیاد داشته باشید.

تشخیص سرور از کلاینت:

- معمولاً، قدرتمند ترین و گرانترین سیستم روی شبکه سرور است.
- کامپیوترهای ارزان تر و کم قدرت تر کلاینت هستند. کلاینت ها کامپیوترهایی هستند که توسط کاربران مختلف برای کارهای روزمره مورد استفاده قرار میگیرند. چون نیازی نیست که منابع کلاینت ها اشتراکی باشند، پس نیازی به قدرتمند بودن و گرانقیمت بودن آنها نیست.
- در بسیاری از شبکه ها تعداد کلاینت ها از شرور ها بیشتر است. برای مثال، شبکه ای میتواند دارای ۱۰ کلاینت باشد در حالیکه فقط ۱ سرور وجود دارد.

سرور های اختصاصی و Peer ها

در برخی از شبکه ها، یک کامپیوتر سرور فقط یک کامپیوتر سرور است و بس. این سرور مختص وظیفه ای مانند اشتراک منابع میباشد. چنین سروری بنام « سرور اختصاصی » نامیده میشود، چون قادر به انجام کاری دیگر بجز فراهم کردن سرویس شبکه نیست. شبکه ای که با اتکا به سرورهای اختصاصی راه اندازی میشود گاهی شبکه کلاینت/سرور (در برخی کتب سرویس گیرنده/سرویس دهنده یا خادم/مخدوم) نامیده میشود.

شبکه های دیگر هدف دیگری را دنبال میکنند، بطوریکه کامپیوتر های روی شبکه هم بعنوان سرور عمل میکنند و هم بعنوان کلاینت. پس هر کامپیوتر میتواند منابع خود را جهت استفاده سایر سیستم های روی شبکه به اشتراک بگذارد. و در حالیکه یک سیستم بعنوان سرور عمل میکند، میتوانید آنرا بعنوان کلاینت و برای کارهایی مانند پردازش متون بکار ببرید. این نوع شبکه را Peer To Peer (در برخی کتب نظیر به نظیر یا همپایه یا P2P) مینامند چون تمام کامپیوتر ها بعنوان Peer یا همتراز عمل میکنند.

پس در اوقات فراغت خود سعی کنید این موارد را در مورد تفاوت بین شبکه های سرور اختصاصی و شبکه های P2P مرور کنید :

@caffeinebookly caffeinebookly @caffeinebookly caffeinebookly t.me/caffeinebookly

- شبکه بندی P2P از ویندوز ۹۵ به بعد در تمام نسخه های ویندوز تعبیه شده است. پس نیازی به خرید نرم افزار اضافی برای تبدیل سیستم خود به سرور ندارید. فقط کافی است تا امکانات سرور ویندوز را فعال کنید.
- امکانات سرور شبکه تعبیه شده در نسخه های دسک تاپ ویندوز (مانند ویندوز XP) زیاد موثر نیستند چون این نسخه ها ذاتاً جهت سرویس دهی ساخته نشده اند. اگر میخواهید کامپیوتری را به کار سرویس دهی تمام وقت منسوب کنید، باید از یک سیستم عامل با امکانات شبکه کامل استفاده کنید که میتوان Windows Server 2003 را مثالی از این سیستم عاملها دانست.

شبکه های بزرگ و کوچک

شبکه ها در سایزها و اشکال مختلف دیده میشوند. در واقع، معمولاً شبکه ها را بر اساس اندازه جغرافیایی تحت پوشش طبقه بندی میکنند که بشرح زیر میباشد :

- **شبکه های محلی (Local Area Networks یا LAN)** : یک شبکه محلی، یا LAN، شبکه ای است که در آن کامپیوتر های نسبتاً نزدیک به هم قرار دارند مانند سیستم های موجود در ساختمان اداره.

البته واژه LAN قطعاً بر کوچک بودن شبکه دلالت ندارد. یک LAN میتواند شامل هزاران کامپیوتر باشد. چیزی که شبکه را به LAN تبدیل میکند این است که کامپیوترهای شبکه در فواصل نسبتاً نزدیک به هم قرار دارند. معمولاً یک LAN درون یک ساختمان واحد قرار میگیرد، ولی میتواند در ساختمان های متعددی در یک محوطه برای مثال دانشگاهی باشد.

- **شبکه های گسترده (Wide Area Network، WAN)** : یک شبکه گسترده، یا WAN، شبکه ای است که یک قلمرو بزرگ جغرافیایی را پوشش میدهد که میتواند یک شهر، یک کشور، ناحیه و یا حتی کل یک کشور باشد. WAN ها معمولاً برای اتصال دو یا چند LAN که فاصله آنها زیاد است بکار میروند. برای مثال، یک WAN ممکن است اداره ای را در ایران به یک اداره در ترکیه متصل کند.

پس این فاصله ی جغرافیایی است که شبکه ای را تبدیل به WAN میکند نه تعداد کامپیوتر های آن. شاید همین اداره در ایران ۱ کامپیوتر و اداره دیگر در ترکیه نیز ۱ کامپیوتر داشته باشد و WAN ما متشکل از ۲ کامپیوتر باشد که با فاصله تقریباً ۲۰۰۰ کیلومتری به هم متصل شده اند.

@caffeinebookly caffeinebookly @caffeinebookly caffeinebookly t.me/caffeinebookly

- **شبکه های شهری (Metropolitan Area Network یا MAN)** : یک شبکه شهری یا MAN شبکه ای است که از یک WAN معمولی کوچکتر است، ولی از LAN بزرگتر است. این شبکه LAN ها را در مقیاس درون شهری به هم متصل میکند.

توپولوژی (همبندی) شبکه

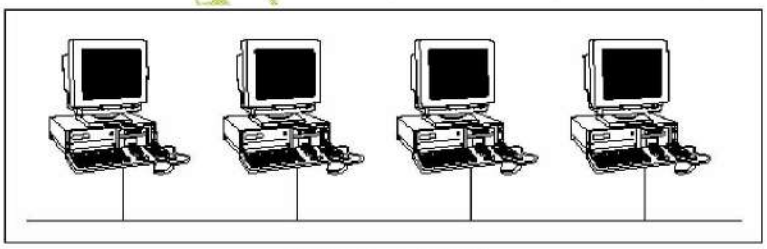
عبارت توپولوژی شبکه به شکل و چگونگی اتصال کامپیوتر ها و سایر اجزای شبکه به یکدیگر اختصاص دارد. چندین نوع مختلف از توپولوژی های شبکه وجود دارند که هریک دارای مزایا و معایب خاص خود میباشند.

در بحثی که از توپولوژی های شبکه خواهیم داشت، از دو کلمه مهم استفاده خواهیم کرد :

- **Node** : یک ناد ابزاری است که به شبکه متصل است. برای ما فعلاً ناد به معنی کامپیوتر است. توپولوژی شبکه در مورد چگونگی اتصال ناد های شبکه به یکدیگر است.
- **Packet** : پکت پیغامی است که روی شبکه از یک ناد به ناد دیگر فرستاده میشود. پکت شامل آدرس ناد فرستنده، آدرس ناد گیرنده و دادهای انتقالی است.

توپولوژی گذرگاهی (خطی یا BUS)

اولین نوع توپولوژی شبکه گذرگاه نامیده میشود که در آن ناد ها در یک خط به هم متصل شده اند که در شکل ۱-۱ نشان داده شده است. توپولوژی معمولاً در مورد LAN ها کاربرد دارد.



شکل ۱-۱ : توپولوژی گذرگاه

کلید شناخت نحوه کار این همبندی این است که کل شبکه را بصورت یک کابل منفرد فرض کنیم که یک ناد به کابل متصل شده است و بدین ترتیب میتواند پکت هایی را که در حال تبادل روی شبکه هستند، ببیند.

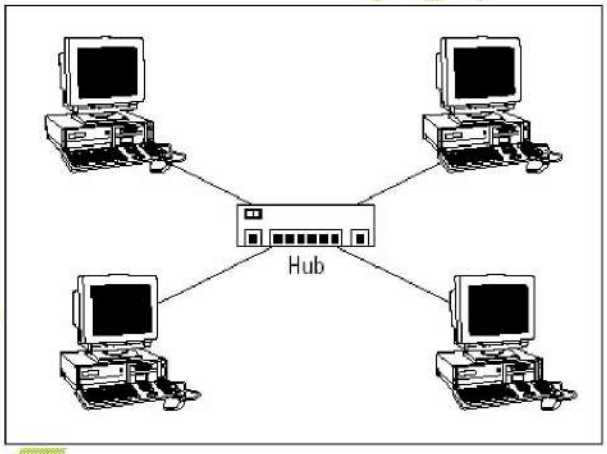
@caffeinebookly caffeinebookly @caffeinebookly caffeinebookly t.me/caffeinebookly

در همبندی گذرگاهی، هر ناد روی شبکه میتواند هر پکتی که روی کابل در حال جابجایی است را ببیند. هر ناد پکت را بررسی میکند تا تشخیص دهد که آیا پکت متعلق به اوست یا نه. اگر اینچنین باشد، ناد پکت را دریافت میکند. درغیر اینصورت، ناد پکت را نادیده میگیرد. بدین ترتیب، هر کامپیوتر میتواند به داده هایی که برایش فرستاده شده پاسخ دهد و سایر داده ها را نادیده بگیرد.

اگر کابل در همبندی خطی قطع شود، شبکه به دو قسمت مجزا تقسیم میشود. هر قسمت کار خود را بطور معمول ادامه میدهد، ولی سیستم های یک سمت قطعی نمیتوانند با سیستم های سمت دیگر ارتباط داشته باشند.

توپولوژی ستاره ای (Star)

در همبندی ستاره ای، هر ناد شبکه به ابزاری مرکزی بنام هاب یا سویچ متصل است که در شکل ۲-۱ نشان داده شده است. همبندی های ستاره ای نیز معمولاً در LAN ها مورد استفاده قرار میگیرند.



شکل ۲-۱ : همبندی ستاره ای

اگر کابل در این توپولوژی قطع شود، فقط نادی قطع میشود که به آن کابل متصل است و از شبکه خارج میشود. ناد های دیگر بدون توقف به کار معمول خود ادامه میدهند.

نکته دیگری که باید به آن دقت کنید، تفاوت فنی میان هاب و سویچ است. با بیان ساده، هاب هیچ اطلاعاتی درباره ابزار متصل به پورت هایش ندارد. پس هنگامی که یک کامپیوتر به یک هاب متصل میشود، کامپیوتر پکتی را به هاب میفرستد تا هاب آنرا به کامپیوتر مقصد برساند. هاب نیز

@caffeinebookly caffeinebookly @caffeinebookly caffeinebookly t.me/caffeinebookly

یک کپی از آن پکت به تمام پورت های خود ارسال میکند. در مقابل، سویچ دقیقاً میداند که کدام وسیله به کدام پورت متصل است. در نتیجه، وقتی سویچ پکتی را دریافت میکند که متعلق به کامپیوتر خاصی است، آنرا دقیقاً به همان پورتی میفرستد که کامپیوتر مورد نظر به آن متصل است. در واقع، فقط شبکه هایی که از سویچ استفاده میکنند، دارای توپولوژی ستاره ای واقعی هستند. اگر شبکه از هاب استفاده کند، شکل فیزیکی ستاره ای برای توپولوژی وجود دارد، در صورتیکه همبندی واقعی آن خطی است. علت امر این است که هنگامی که یک هاب مورد استفاده قرار میگیرد، هر کامپیوتر روی شبکه تمام پکت هایی را که بین سیستم ها ارسال و دریافت میشوند، می بیند که از این لحاظ دقیقاً مانند توپولوژی خطی عمل میشود. در یک همبندی ستاره ای واقعی، هر کامپیوتر فقط پکت هایی را میبیند که مخصوص آن سیستم فرستاده شده اند و پکت هایی را ارسال میکند که فقط مخصوص یک سیستم خاص میباشند.

گسترش ستاره ها

فیزیکدانها میگویند که عالم همواره در حال گسترش است، ولی سرپرستان شبکه نیز گفته آنها را تایید میکنند. یک همبندی ساده خطی یا ستاره ای فقط برای شبکه های کوچک مناسب است که حدود یک دوجین کامپیوتر دارند، ولی شبکه های کوچک روزی رشد کرده و بزرگتر خواهند شد و کامپیوتر های بیشتری به آنها اضافه خواهد شد. برای شبکه های بزرگتر، از همبندی های پیچیده تری استفاده میشود که ترکیبی از ستاره ها و خطوط است.

برای مثال، یک گذرگاه میتواند چندین ستاره را بهم متصل کند. در چنین موردی، دو یا چند هاب یا سویچ به هم با استفاده از گذرگاه متصل میشوند. هریک از این هاب ها یا سویچ ها نیز مرکز ستاره ای هستند که چندین کامپیوتر به آنها متصل است. این نوع شبکه بندی معمولاً در ساختمان هایی مورد استفاده قرار میگیرد که دو یا چند گروه کاری مختلف دارند. گذرگاهی که سویچ ها را به یکدیگر متصل میکند، ستون فقرات (BackBone) شبکه نام دارد.

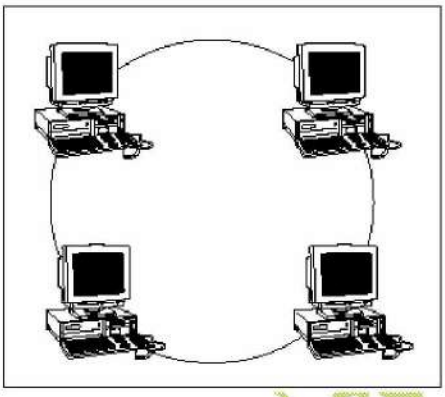
روش دیگر برای گسترش توپولوژی ستاره ای، استفاده از تکنیکی بنام Daisy Chaining میباشد. هنگام استفاده از روش Daisy Chaining، هاب یا سویچ طوری به هاب یا سویچ دیگری متصل میشود که گویی یکی از ناد های ستاره است. سپس، هاب دوم یا سویچ دوم، بعنوان مرکز ستاره بعدی انجام وظیفه میکند.

توپولوژی طلقوی (Ring)

نوع سوم همبندی شبکه حلقه نام دارد که در شکل ۳-۱ نمایش داده شده است. در همبندی حلقوی، پکت ها درون یک دایره از کامپیوتری به کامپیوتر دیگر ارسال میشوند. هر کامپیوتر پکت

@caffeinebookly caffeinebookly @caffeinebookly caffeinebookly t.me/caffeinebookly

ها را بررسی میکند که آیا متعلق به اوست یا نه. اگر نباشد، پکت به کامپیوتر بعدی در حلقه ارسال میشود.



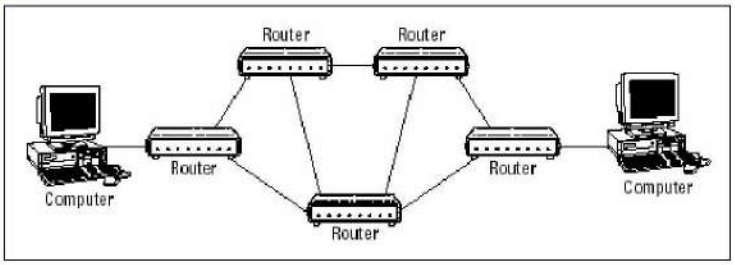
شکل ۳-۱ : همبندی حلقوی

سالها پیش، توپولوژی های حلقوی در LAN ها معمول بود و دو نوع معروف از این همبندی وجود داشت : ARCNET و TOKEN RING. ARCNET هنوز برای کاربردهای خاصی مانند اتوماسیون کارخانه ها مورد استفاده قرار میگیرد، ولی در شبکه های تجاری بسیار کم استفاده میشود. TOKEN RING همبندی معروفی از شبکه است که برای کامپیوترهای رده متوسط IBM درنظر گرفته شده بود. با اینکه شبکه های TOKEN RING زیادی هنوز وجود دارند، ولی شبکه های جدید دیگر با استفاده از این همبندی مورد استفاده قرار نمیگیرند.

توپولوژی حلقوی بوسیله FDDI نیز مورد استفاده قرار میگیرد که یکی از ارتباطات اولیه شبکه ای فیبر نوری بود ولیجای خود را به تکنیک های موثرتر فیبرنوری داد.

توپولوژی توری (Mesh)

نوع چهارم همبندی شبکه بنام Mesh شناخته میشود که چندین ارتباط میان نادهای شبکه برقرار میکند که در شکل ۴-۱ نشان داده شده است. مزیت این همبندی این است که اگر کابلی قطع شود، شبکه میتواند از مسیر دیگری برای نقل و انتقال پکت ها استفاده کند.



شکل ۴-۱ : همبندی توری

@caffeinebookly caffeinebookly @caffeinebookly caffeinebookly t.me/caffeinebookly

شبکه های توری در تنظیمات LAN زیاد مورد استفاده قرار نمیگیرند. برای مثال، برای شبکه کردن ۸ کامپیوتر در همبندی توری، هر کامپیوتر باید دارای ۷ کارت رابط شبکه باشد و ۲۸ کابل برای ارتباط دادن کامپیوتر ها به هم مورد نیاز خواهد بود و البته این حالت زیاد مقیاس پذیر نخواهد بود.

با این وجود، شبکه های توری برای شبکه های WAN یا MAN بسیار مناسبند. این شبکه ها از ابزارهایی بنام مسیریاب (Router) استفاده میکنند تا پکت ها را از شبکه ای به شبکه دیگر مسیردهی کنند. جهت اطمینان و بازدهی بیشتر، روتر ها معمولاً طوری چیده میشوند که چندین مسیر بین هر دو ناد روی شبکه بوجود آید که درست مانند چیدن تورهای سیمی است.

یادداشت

کتابخانه مجازی پارسیان

@caffeinebookly caffeinebookly @caffeinebookly caffeinebookly t.me/caffeinebookly

فصل ۲ : شناخت پروتکل ها و استاندارد های شبکه

در این فصل میخوانید :

- لایه های مختلف مدل مرجع OSI
- شناخت اترنت
- بررسی دقیق TCP/IP و IPX/SPX
- پروتکلهای مهم دیگر

شهرکتابخانی پارسیان

@caffeinebookly caffeinebookly @caffeinebookly caffeinebookly t.me/caffeinebookly

پروتکل ها و استاندارد های شبکه باعث بکار افتادن اجزای شبکه در کنار هم میشوند. پروتکل ها این امکان را فراهم میکنند تا اجزای مختلف شبکه با هم ارتباط برقرار کنند. استاندارد ها نیز باعث میشوند تا اجزای شبکه ای که توسط سازندگان مختلف ساخته شده اند، با هم بخوبی کار کنند. در این فصل شما با پروتکل ها و استاندارد هایی آشنا میشوید که بیشترین برخورد را با آنها هنگام ساخت و نگهداری شبکه خواهید داشت.

شناخت پروتکل ها

پروتکل، مجموعه ای از قوانین است که باعث ایجاد ارتباط موثر میشود. ما هر روزه با پروتکل ها سروکار داریم. برای مثال، شما برای خرید یک وسیله خانگی بوسیله چک، ابتدا در مورد قیمت با فروشنده صحبت میکنید. سپس چک می نویسید که شامل اطلاعاتی مانند نام و تاریخ و مبلغ چک است. فروشنده چک را گرفته و وسیله را به شما تحویل میدهد. و نکته پروتکل ها در تبادلات بینابین است.

شبکه های کامپیوتری به پروتکل های مختلفی برای کارکرد نیاز دارند. این پروتکل ها صریح و دارای چارچوب مشخص میباشند. کارت های شبکه باید بدانند که چگونه با کارت های دیگر شبکه ارتباط برقرار کنند تا بتوانند اطلاعات تبادل کنند، سیستم عامل نیز باید طرز ارتباط با کارت های شبکه را جهت ارسال و دریافت داده ها بداند و سرانجام برنامه های کاربردی نیز باید باید نحوه تبادل اطلاعات با سیستم عامل را بدانند تا بتوانند برای مثال به فایلهای روی سرویس دهنده فایل دسترسی پیدا کنند.

پروتکل ها در انواع مختلفی وجود دارند. در پایین ترین سطح، پروتکل ها دقیقاً تعریف میکنند که چه نوع سیگنال های الکتریکی مولد ۱ و چه نوع آنها مولد ۰ میباشند. در بالاترین سطح، پروتکل این امکان را به کاربر کامپیوتر میدهد تا پیغامی را از طریق پست الکترونیکی به دوست خود در آن سوی دنیا ارسال کند. در این میان، سطوح دیگری از پروتکل ها نیز وجود دارند. بعد ها در مورد این لایه های پروتکل بیشتر خواهید خواند.

نکته : پروتکلهای مختلفی وجود دارند که بصورت سری های هماهنگ کار میکنند و در اصطلاح Protocol Suite نامیده میشوند. دو Suite معروف پروتکلهای شبکه، TCP/IP و IPX/SPX میباشند. TCP/IP در اصل برای شبکه های یونیکس ایجاد شد و پروتکل اینترنت است. IPX/SPX برای شبکه های NetWare ایجاد شد که هنوز هم بصورت گسترده ای در شبکه های ویندوز کاربرد دارد. پروتکل مهم سوم، Ethernet است. پروتکلی سطح پایین که هم با TCP/IP و هم با IPX/SPX مورد استفاده قرار میگیرد.

@caffeinebookly caffeinebookly @caffeinebookly caffeinebookly t.me/caffeinebookly

شناخت استاندارد ها

یک استاندارد، توافقی بر اساس یک پروتکل است. در روزهای آغازین شبکه های کامپیوتری، هر سازنده کامپیوتر پروتکل های شبکه بندی مختص خود را ایجاد میکرد. در نتیجه، امکان ترکیب قطعات از سازندگان مختلف در یک شبکه وجود نداشت.

بنابراین استاندارد ها بوجود آمدند. استاندارد ها پروتکل های تعریف شده در مقیاس صنعتی هستند که به یک سازنده خاص محدود نمیشوند. با پروتکلهای استاندارد، میتوانید قطعات ساخت سازندگان مختلف را با همخوانی کامل استفاده کنید. تا زمانی که قطعه ای از استاندارد های خاص پیروی کند، میتواند درون شبکه قرار گرفته و کار کند.

سازمانهای بسیاری در رابطه را تهیه استاندارد های شبکه بندی فعالیت میکنند که پنج سازمان از مهمترین سازمانهای استاندارد سازی را معرفی میکنیم :

- **انستیتوی استانداردهای ملی امریکا** (ANSI) : سازمان رسمی استانداردها در ایالات متحده.
- **انستیتوی مهندسی الکتریک و الکترونیک** (IEEE) : سازمانی بین المللی که چندین استاندارد کلیدی شبکه را منتشر کرده است. استاندارد رسمی برای سیستم شبکه بندی اترنت که بطور رسمی IEEE 802.3 نام گرفته است، از این جمله میباشد.
- **سازمان بین المللی استاندارد سازی** (ISO) : تشکیلاتی متشکل از بیش از ۱۰۰ سازمان استانداردسازی از سطح جهان.
- **نیروی کاری مهندسی اینترنت** (IETF) : سازمانی که مسئول پروتکلهای کاربردی اینترنت میباشد.
- **کنسرسیوم وب** (W3C) : سازمانی بین المللی که کنترل کننده ایجاد و توسعه استاندارد های وب است.

جدول ۱-۲ لیستی از وب سایت های هریک از این سازمانهای استانداردسازی را ارائه میکند :

سازمان	وب سایت
ANSI	www.ansi.org
IEEE	www.ieee.org
ISO	www.iso.org
IETF	www.ietf.org
W3C	www.w3c.org

@caffeinebookly caffeinebookly @caffeinebookly caffeinebookly t.me/caffeinebookly

هفت لایه مدل مرجع OSI

OSI در دنیای شبکه های کامپیوتر بعنوان ارتباط بینابین آزاد سیستم ها شناخته میشود. مدل OSI مفاهیم مختلف شبکه های کامپیوتری را به هفت لایه مجزا تقسیم میکند. این لایه ها در واقع مانند لایه های پیاز هستند : هر لایه دربر گیرنده لایه زیرین است و جزئیات آنرا از سطوح بالاتر مخفی میکند. مدل OSI از جهت دیگری نیز به پیاز معروف است. چون باید برای دیدن لایه های درونی تر آنرا بشکافید، اشکتان را در خواهد آورد!

مدل OSI یک استاندارد شبکه بندی مانند اترنت یا توکن رینگ نیست. در عوض، مدل OSI چارچوبی است که استاندارد های مختلف شبکه در آن قرار میگیرند. مدل OSI نشان میدهد که چه مفاهیمی از عملکرد های شبکه با چه استاندارد های سازگاری دارند. پس، در عمل، مدل OSI، نوعی استاندارد استانداردها است.

جدول ۲-۲ خلاصه ای از هفت لایه مدل مرجع OSI را نمایش میدهد.

لایه	نام	توضیحات
۱	فیزیکی	**Physical** : در مورد ساختار کابل ها و ابزار هایی مانند تقویت کننده ها و هاب ها اعمال مدیریت میکند.
۲	اتصال داده	**Data Link** : آدرس های MAC خاص هر ناد در شبکه را ایجاد میکند و مفهوم پکت را برای ارسال از طریق لایه فیزیکی، فراهم میکند. بریج ها و سویچ ها از دستگاه های این لایه میباشند.
۳	شبکه	**Network** : مسیردهی داده ها در بخشهای مختلف شبکه را در اختیار دارد.
۴	انتقال	**Transport** : انتقال مطمئن داده ها را تضمین میکند.
۵	نشست	**Session** : جلساتی بین برنامه های کاربردی شبکه ترتیب میدهد.
۶	نمایش	**Presentation** : داده ها را طوری تبدیل میکند که سیستم هایی که از قالب های مختلف داده استفاده میکنند، بتوانند به تبادل اطلاعات بپردازند.
۷	کاربردی	**Application** : به برنامه های کاربردی این امکان را میدهد تا از شبکه درخواست سرویس کنند.

سه لایه اول را گاهی لایه های پایینی نیز مینامند. این لایه ها با مکانیک نحوه ی ارسال اطلاعات از یک کامپیوتر به کامپیوتر دیگر روی شبکه سروکار دارند. لایه های ۴ تا ۷ نیز گاهی لایه های بالایی نامیده میشوند. این لایه ها با نحوه ارتباط برنامه های کاربردی از طریق رابط های برنامه نویسی کاربردی با شبکه سروکار دارند.

نکته : هفت لایه مدل OSI به نوعی نگاه صحیحی به نحوه کار پروتکل های شبکه میباشد. در دنیای واقعی، پروتکل های واقعی شبکه، مدل مرجع OSI را دنبال نمیکنند. دنیای واقعی همیشه به هم

@caffeinebookly caffeinebookly @caffeinebookly caffeinebookly t.me/caffeinebookly

ریخته تر از حالت دلخواه است. با این حال، هنوز مدل OSI نمایی کارآمد از نحوه کار شبکه ارائه میکند.

لایه فیزیکی

پایین ترین لایه از مدل مرجع OSI، لایه فیزیکی نامیده میشود. در این لایه خصوصیات فیزیکی شبکه مانند نوع کابل مورد استفاده برای ارتباط، نوع اتصالات مورد استفاده ، طول کابلها، و ... مطرح میشود. برای مثال، استاندارد اترنت 10BaseT نشانگر خصوصیات الکتریکی کابل جفت تابیده، اندازه و شکل اتصالات، طول حداکثر کابل و ... است. توپولوژی های توضیح داده شده نیز، در این لایه اعمال میشوند.

مفهوم دیگر در لایه فیزیکی، خصوصیات الکتریکی سیگنال هایی است که برای انتقال داده ها در کابل از یک ناد شبکه به ناد دیگر مورد استفاده قرار میگیرد. در این لایه ارزش های اساسی دودویی صفر و یک گنجانده شده در سیگنال ها تعریف میشوند. لایه های بالاتر در مدل OSI به این بیت ها مفهوم میبخشند.

یکی از ابزارهای لایه فیزیکی که معمولاً در شبکه ها استفاده میشود، تقویت کننده نام دارد. تقویت کننده هنگامی استفاده میشود که طول مورد نیاز از حداکثر طول قابل استفاده کابل بیشتر باشد و نیاز به تقویت سیگنال وجود داشته باشد. هاب های 10BaseT نیز از دستگاه های لایه فیزیکی میباشند. اط لحاظ فنی، این دستگاه ها را تقویت کننده های چند درگاهی میگویند چون هاب هر پکت دریافتی را به تمام پورت های خود ارسال میکند. تقویت کننده ها و هاب ها محتویات پکت های دریافتی را کنترل نمیکنند. اگر قرار بود چنین کاری را انجام دهند، در لایه اتصال داده قرار میگرفتند.

کارت شبکه، که روی هر کامپیوتر شبکه نصب میشود، در رده ابزارهای لایه فیزیکی قرار میگیرد. میتوانید اطلاعات مربوط به کارت شبکه خود را که در سیستم ویندوز نصب شده است، با نمایش مشخصات کارت در وسندوز مشاهده نمایید. بطوریکه در شکل ۱-۲ نشان داده شده است، برای دسترسی به این صفحه مشخصات در ویندوز ۲۰۰۰ یا XP، کنترل پنل را باز کرده و روی آیکون سیستم دوبار کلیک میکنیم.سپس وارد بخش سخت افزار شده و روی کلید Device Manager کلیک میکنیم. لیستی از تمام دستگاه های متصل به کامپیوتر نمایش داده میشود. روی قسمت کارت شبکه دوبار کلیک میکنیم تا صفحه مشخصات آن به نمایش درآید.

@caffeinebookly caffeinebookly @caffeinebookly caffeinebookly t.me/caffeinebookly

شکل ۱-۲ : مشخصات کارت شبکه

لایه اتصال داده

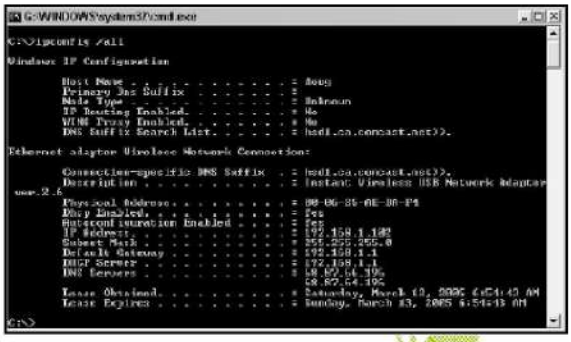
این لایه پایین ترین لایه ای است که مربوط به بیت های در حال جابجایی روی شبکه میباشد. پروتکل های اتصال داده، مواردی مانند اندازه هرپکت داده، رسیدن پکت ها به مقصد مورد نظر و عدم ارسال پکت ها از سوی ناد ها روی شبکه بصورت همزمان را کنترل میکنند.

در این لایه شناسایی و اصلاح خطای ابتدایی نیز انجام میگیرد تا اطمینان حاصل شود که داده های دریافت شده، همان داده های ارسال شده باشند. اگر خطای غیرقابل اصلاحی رخ دهد، استاندارد اتصال داده تعیین میکند که ناد چگونه باید در از خطای رخ داده شده اطلاع پیدا کند و دوباره به انتقال داده ها بپردازد.

در این لایه، هر دستگاه روی شبکه آدرسی بنام آدرس کنترل رسانه یا MAC دارد. این آدرس معمولاً بطور سخت افزاری در هر ابزار شبکه وجود دارد و توسط سازنده در آن تعبیه میشود. آدرس های MAC منحصربفرد هستند. هیچ دو ابزار شبکه ساخت هر سازنده ای در هر جای جهان، نمیتوانند آدرس MAC یکسانی داشته باشند.

برای مشاهده آدرس MAC مربوط به کامپیوتر خود، میتوانید در خط فرمان دستور `ipconfig /all` را تایپ کنید که در شکل ۲-۲ نشان داده شده است. در این دستور آدرس MAC را بعنوان آدرس فیزیکی نمایش داده است.

@caffeinebookly caffeinebookly @caffeinebookly caffeinebookly t.me/caffeinebookly



شکل ۲-۲ : نمایش آدرس MAC کارت شبکه

یکی از مهمترین عملکردهای لایه اتصال داده، فراهم کردن روشی است که پکت ها بتوانند با امنیت روی رسانه فیزیکی ارسال شوند بدون اینکه ناد های دیگر با ارسال همزمان داده ها، ایجاد مزاحمت نمایند. دو روش از معروف ترین روش های این کار CSMA/CD و Token Passing میباشند. شبکه های اترنت از CSMA/CD استفاده میکنند و شبکه های توکن رینگ از روش توکن پسینگ.

دو نوع اصلی ابزارهای لایه اتصال داده که در شبکه ها بطور معمول استفاده میشوند، بریج ها و سویچ ها میباشند. یک بریج تقویت کننده هوشمندی است که آدرس های MAC ناد های آنسوی پل را میشناسد و میتواند پکت ها را با توجه به این آدرس دهی هدایت کند. سویچ، هاب هوشمندی است که آدرس MAC را بررسی میکند و پورتی که باید پکت به آن ارسال شود را شناسایی میکند.

نحوه کار CSMA/CD

یکی از عملکردهای مهم لایه اتصال داده، حصول اطمینان از عدم ارسال پکت ها از سوی دو کامپیوتر بطور همزمان میباشد. اگر چنین حالتی اتفاق بیفتد، سیگنال ها به یکدیگر برخورد کرده و ارتباط قطع میشود. این مشکل در اترنت به کمک تکنیکی بنام CSMA/CD یا « دسترسی چندگانه حس انتقال با اصلاح تصادم » حل شده است. این اصطلاح با اینکه پیچیده است، ولی اگر آنرا به چند قسمت تقسیم کنیم، مفهوم ساده ای بدست خواهد آمد.

حس انتقال، یعنی هنگامی که دستگاهی میخواهد پکتی را روی شبکه بفرستد، ابتدا رسانه شبکه را بررسی میکند تا ببیند که آیا فرد دیگری در حال ارسال داده روی رسانه هست یا نه. اگر هیچ ارسالی احساس نشد، کامپیوتر به آزاد بودن شبکه پی برده و پکت خود را ارسال میکند.

دسترسی چندگانه، یعنی اینکه هیچ چیزی از ارسال پکت ها توسط دو یا چند سیستم بطور همزمان جلوگیری نکند. البته هر وسیله قبل از ارسال داده ها، کابل را از جهت ترافیک کنترل میکند. با این حال، فرض کنید که دو دستگاه هر دو این کنترل را انجام میدهند و بار ترافیکی پیدا نمی کنند و

@caffeinebookly caffeinebookly @caffeinebookly caffeinebookly t.me/caffeinebookly

هر دو همزمان پکت های خود را ارسال میکنند. این مانند حالتی است که شما و یک ماشین دیگر همزمان به تقاطع میرسید. بعد از کمی تعارف، هر دوی شما حرکت کرده و از تقاطع عبور خواهید کرد.

شناسایی تصادم یعنی اینکه پس از ارسال پکت توسط دستگاه، دستگاه دقت میکند که پکت به پکت دیگری برخورد کرده یا نه. اگر احتمال برخورد وجود داشته باشد یا برخورد انجام شود، دستگاه پس از مدت زمانی تصادفی، دوباره بسته خود را ارسال میکند. چون این زمان تصادفی است، پس هرگز دو پکت به هم برخورد نخواهند کرد.

CSMA/CD برای شبکه های کوچک بخوبی کار میکند. پس از اینکه شبکه دارای حدود ۳۰ کامپیوتر شد، تصادم پکت ها بسیار بیشتر خواهد شد و شبکه کند خواهد شد. در چنین حالتی شبکه باید به دو یا چند بخش مجزا از هم تقسیم شود که اصطلاحاً دامنه های تصادم نامیده میشوند.

لایه شبکه

در لایه شبکه، عمل مسیردهی پیغام های شبکه از یک کامپیوتر به کامپیوتر دیگر انجام میشود. دو پروتکل معروف لایه سوم عبارتند از IP (که معمولاً همراه با TCP است)، IPX (که بطور عادی با SPX همراه است که هنگام استفاده از شبکه ناول با ویندوز بکار میرود).

آدرس دهی منطقی

بطوریکه میدانید، هر ابزار شبکه یک آدرس MAC منحصربفرد دارد که در کارخانه و هنگام ساخت به دستگاه اختصاص داده میشود. هنگامی که کارت شبکه ای را در کامپیوتر خود نصب میکنید، آدرس MAC کارت شبکه تثبیت شده و غیرقابل تغییر میشود. ولی آیا شاید شما بخواهید از روش آدرس دهی دیگری برای دسترسی به ابزار های روی شبکه استفاده کنید. در این حالت، مفهوم آدرس دهی منطقی به میان می آید. آدرس منطقی به شما این امکان را میدهد تا به ابزار های شبکه با استفاده از آدرس هایی که خودتان اختصاص میدهید، دسترسی پیدا کنید.

آدرس های منطقی توسط پروتکل های لایه شبکه مانند IP و IPX ایجاد میشوند. پروتکل لایه شبکه آدرس های منطقی را به آدرس های MAC معادل ترجمه میکند. برای مثال، اگر شما از IP بعنوان پروتکل لایه شبکه استفاده کنید، ابزارهای روی شبکه آدرس های IP مانند 207.120.67.32 خواهند داشت. چون پروتکل IP باید از یک پوتکل لایه اتصال داده استفاده کند تا قادر به ارسال پکت ها به ابزارهای مختلف باشد، پس باید دانش ترجمه آدرس های IP را به آدرس های فیزیکی ابزارهای شبکه داشته باشد.

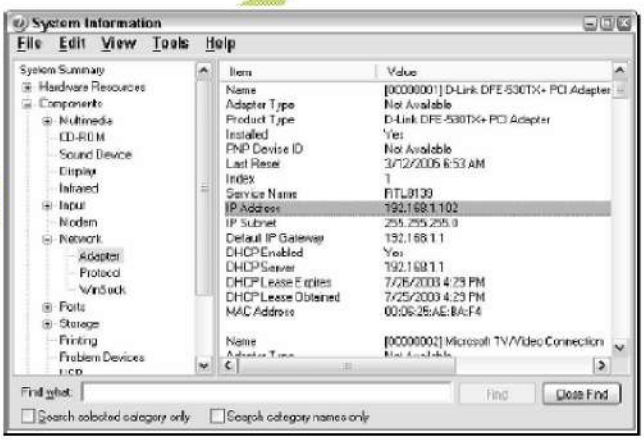
آدرس های لایه اتصال داده (آدرس های MAC) در کارخانه اعمال میشوند و قابل تغییر نمیباشند. آدرس لایه شبکه (IP) در هنگام شبکه بندی اختصاص داده میشود و قابل تغییر است.

@caffeinebookly caffeinebookly @caffeinebookly caffeinebookly t.me/caffeinebookly

میتوانید از دستور ipconfig در خط فرمان که قبلاً در شکل ۲-۲ نشان داده شد، برای دیدن آدرس IP کامپیوتر خود استفاده کنید. آدرس IP نشان داده شده در شکل 192.168.1.102 میباشد. روش دیگر نمایش اطلاعات، استفاده از دستور اطلاعات سیستم است. در منوی شروع، شاخه Programs، Accessories، System Tools، System Information، میتوانیداین اطلاعات را ببینید. آدرس IP در شکل ۳-۲ پررنگ تر نمایش داده شده است. بخاطر داشته باشید که برنامه اطلاعات سیستم، در کنار آدرس IP، اطلاعات کاربردی بسیار زیادی در مورد سیستم شما نمایش میدهد. برای مثال، میتوانید آدرس MAC، پروتکل های مورد استفاده و سایر اطلاعات را نیز در این برنامه ببینید.

قابل دقیق آدرس های منطقی با توجه به پروتکل مورد استفاده متغیر است و بسیاری از پروتکل ها، آدرس منطقی را به دو قسمت تقسیم میکنند : آدرس شبکه و آدرس ابزار. آدرس شبکه، شبکه ای که دستگاه روی آن کار میکند را مشخص میکند و آدرس ابزار، خود قطعه را روی شبکه تعریف میکند. برای مثال، یک آدرس IP معمولی، مانند 192.168.1.102 را در نظر بگیرید. آدرس شبکه 192.168.1 است و آدرس قطعه (آدرس میزبان) 102 است.

به همین ترتیب، آدرس های IPX نیز از دو قسمت تشکیل شده اند. آدرس شبکه و آدرس ناد. در آدرس IPX، آدرس ناد همان آدرس MAC است. درنتیجه، IPX نیازی به ترجمه بین دو آدرس لایه ۲ و لایه ۳ ندارد.



شکل ۳-۲ : استفاده از برنامه اطلاعات سیستم برای نمایش اطلاعات شبکه.

@caffeinebookly caffeinebookly @caffeinebookly caffeinebookly t.me/caffeinebookly

مسیریابی

مسیریابی هنگامی وارد بازی میشود که کامپیوتری روی یک شبکه، نیار به ارسال داده ها به کامپیوتری روی شبکه دیگر داشته باشد. در چنین مواردی، ابزاری بنام مسیریاب برای انتقال پکت ها به شبکه مقصد مورد استفاده قرار میگیرد. در برخی موارد، یک پکت ممکن است نیاز به سفر در چندین شبکه میانی داشته باشد تا به شبکه مقصد برسد.

یکی از قابلیت های مهم روترها این است که میتوانید از آنها برای اتصال شبکه هایی با پروتکل های مختلف لایه ۳ استفاده کنید. برای مثال، یک روتر میتواند برای ارسال و دریافت پکت ها از یک اترنت به توکن رینگ مورد استفاده قرار گیرد. تا زمانی که هر دو شبکه پروتکل لایه ۳ یکسانی را پشتیبانی کنند، مهم نیست که پروتکل های لایه ۱و لایه ۲ متفاوت باشند.

پروتکلی قابل مسیردهی نامیده میشود که از آدرس هایی استفاده کند که شامل یک قسمت شبکه و یک قسمت میزبان باشند. هر پروتکلی که از آدرس های فیزیکی استفاده کند، قابل مسیردهی نیست، چون آدرس های فیزیکی نشان نمیدهند که ابزار به کدام شبکه تعلق دارد.

لایه انتقال

لایه انتقال، لایه ای است که در آن میتوانید دو پروتکل معروف شبکه را پیدا کنید : TCP (بطور عادی همراه با IP) و SPX (بطور عادی همراه با IPX). بطوریکه از نام لایه نیز مشخص است، لایه انتقال در رابطه با انتقال اطلاعات از یک کامپیوتر به کامپیوتر دیگر است.

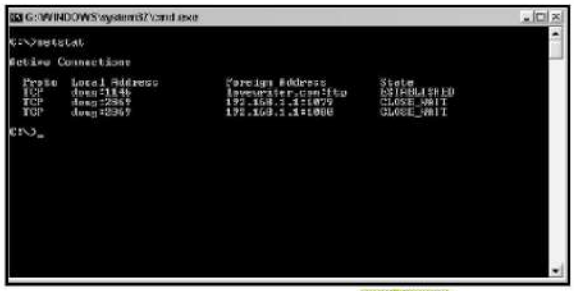
هدف اصلی لایه انتقال حصول اطمینان از انتقال مطمئن و بدون خطای داده ها است. لایه انتقال این کار را با ایجاد ارتباطاتی بین ابزارهای شبکه جهت ارسال رسید پکت های رسیده و درخواست مجدد برای ارسال پکت های ناموفق انجام میدهد.

در بسیاری از موارد، پروتکل لایه انتقال، پیغام های بزرگ را به پکت های کوچکتر تقسیم میکند که میتوانند روی شبکه بهتر جابجا شوند. پروتکل لایه انتقال این پکت های ریز را در مقصد دوباره سرهم بندی کرده و اطمینان حاصل میکند که پکت های ارسالی بدون کم و کسر به مقصد رسیده اند.

برای برخی از کاربردها، سرعت و تاثیرگذاری، مهمتر از قابلیت اطمینان میباشد. در چنین مواردی، یک پروتکل بدون ارتباط مورد استفاده قرار میگیرد. پروتکل بدون ارتباط، نیازی به تحمل دردسر ایجاد ارتباط قبل از ارسال پکت ندارد. TCP یکی از پروتکلهای ارتباطی لایه انتقال است. پروتکل معادل بدون ارتباط در این لایه که همراه با TCP کار میکند، UDP نام دارد.

@caffeinebookly caffeinebookly @caffeinebookly caffeinebookly t.me/caffeinebookly

در ویندوز XP، میتوانید اطلاعات در مورد وضعیت ارتباطات TCP و UDP را با اجرای دستور NETSTAT از خط فرمان مانند شکل ۴-۲ بدست آورید. در این شکل، میبینید که سه ارتباط TCP برقرار شده است.



شکل ۴-۲ : نمایش وضعیت ارتباطات TCP و UDP توسط دستور NETSTAT.

درواقع، میتوانید از دستور NETSTAT /N برای دیدن آدرسهای شبکه عددی بجای نامها استفاده کنید. با سویچ N/، خروجی ۴-۲بشکل زیر خواهد بود :

```
Active Connections
Proto      Local Address          Foreign Address    State
TCP        192.168.1.102:1146     209.68.34.15:21    ESTABLISHED
TCP        192.168.1.102:2869     192.168.1.1:1079   CLOSE_WAIT
TCP        192.168.1.102:2869     192.168.1.1:1080   CLOSE_WAIT
```

TCP پروتکلی بر مبنای ارتباط در لایه انتقال است. UDP پروتکل بدون ارتباط در این لایه میباشد.

لایه نشست

لایه نشست، جلساتی بنام نشست را بین دو وسیله شبکه شده بوجود می آورد. یک نشست، تبادل انتقالات بر مبنای ارتباط بین دو وسیله است. هر یک از انتقالات توسط پروتکل لایه انتقال کنترل میشوند. خود نشست توسط پروتکل لایه نشست مدیریت میشود.

یک نشست منفرد میتواند شامل تبادلات فراوانی از داده با بین دو کامپیوتر دخیل در نشست باشد. پس از اینکه یک نشست بین دو کامپیوتر ترتیب داده شد، این نشست تا زمانی که سیستم ها با اتمام آن موافقت کنند، پایدار خواهد ماند.

لایه نشست، اجازه برقراری سه نوع انتقال را صادر میکند :

- **Simplex** : در این حالت، داده ها فقط در یک جهت حرکت میکنند.
- **Half Duplex** : در این حالت، داده ها در هر دو جهت حرکت میکنند ولی در هر لحظه فقط در یک جهت. یا رفت یا برگشت.

@caffeinebookly caffeinebookly @caffeinebookly caffeinebookly t.me/caffeinebookly

- **Full Duplex** : در این حالت، داده ها در آن واحد میتوانند هم در جهت رفت و هم در جهت برگشت حرکت کنند.

نکته : در عمل، فرق بین لایه های نشست و نمایش و کاربردی بسیار کمرنگ میشود و چند پروتکل معمول در این لایه ها جاری میشوند. برای مثال، SMB (پروتکل مدیریت قطعه سرور که اساس اشتراک فایل در ویندوز است) در هر سه لایه کار میکند.

لایه نمایش

لایه نمایش مسئول نحوه ارائه و نمایش داده ها به برنامه های کاربردی است. بسیاری از کامپیوترها، از « کدهای استاندارد امریکا جهت تبادل اطلاعات (ASCII) » برای نمایش داده ها استفاده میکنند. برخی کامپیوترها مانند مین فریم های IBM، از سیستمی متفاوت بنام « کد تبادلی توسعه یافته مبنای ده کد دهی شده بصورت دودویی (EBCDIC) » بهره میبرند. ASCII و EBCDIC با هم سازگار نیستند. برای تبادل اطلاعات بین مین فریم ها و سیستم های ویندوز، لایه نمایش باید داده ها را از ASCII به EBCDIC و بالعکس تبدیل کند.

همراه با تبدیل ساده داده ها از یک کد به کد دیگر، لایه نمایش میتواند تکنیک های خاص فشرده سازیرا روی داده ها اعمال کند تا بایت های داده کمتری جهت نمایش روی شبکه فرستاده شود. در سوی دیگر انتقال، همین لایه داده ها را از حالت فشرده خارج میسازد.

لایه نمایش همچنین میتواند داده ها را قبل از فرستادن روی شبکه، رمزگذاری کند و در سوی دیگر، عمل رمزگشایی را با تکنیک های بسیار خاص انجام دهد که بهترین کارآگاهان دنیا نیز قادر به کشف رمز آن نیستند.

لایه کاربردی

بالاترین لایه مدل OSI، لایه کاربردی است که با تکنیک هایی سروکار دارد که برنامه های کاربردی برای ایجاد ارتباط با شبکه از آنها استفاده میکنند. نام این لایه کمی گیج کننده است. برنامه های کاربردی مانند Microsoft Office یا QuickBooks بخشی از لایه کاربردی نیستند. این لایه رابط برنامه نویسی ارائه میکند که برنامه های مانند آفیس از آنها برای درخواست سرویس شبکه استفاده میکنند.

تعدادی شناخته شده ترین پروتکلهای لایه کاربردی عبارتند از :

- **DNS** (سیستم نام دامنه) برای تبدیلات دامنه های اینترنت
- **FTP** (پروتکل انتقال فایل) برای انتقال فایل
- **SMTP** (پروتکل ساده انتقال پستی) برای e-mail

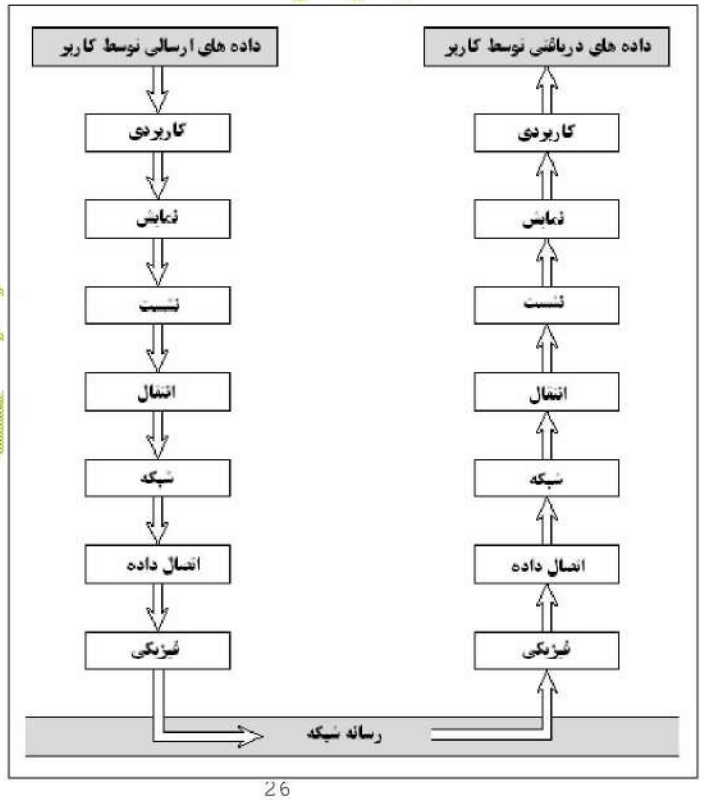
@caffeinebookly caffeinebookly @caffeinebookly caffeinebookly t.me/caffeinebookly

- **SMB** (قطعه پیغام سرور) برای اشترام فایلهای در شبکه ویندوز
- **NFS** (سیستم فایل شبکه) برای اشتراک فایل در یونیکس
- **Telnet** برای شبیه سازی ترمینال

دنبال کردن پکت در لایه ها

شکل ۵-۲ نشانگر نحوه جریان یک پکت داده درون هفت لایه در حین انتقال از یک کامپیوتر به کامپیوتر دیگر است. داده ها، سفر خود را هنگامی آغاز میکنند که کاربر برنامه کاربردی داده را به کامپیوتری دیگر روی شبکه ارسال میکند.

داده از طریق رابط لایه کاربردی مانند SMB، وارد شبکه میشود. سپس داده به مسیر خود ادامه میدهد. در این مسیر، پروتکلهای موجود در هر لایه داده را با افزودن اطلاعات آغازین، تبدیل داده به قالب های مختلف، ترکیب پکت ها برای ایجاد یک پکت بزرگتر و ... تغییر میدهند. وقتی داده به لایه فیزیکی رسید، واقعاً روی رسانه شبکه قرار گرفته است (همان کابل) و به کامپیوتر مقصد فرستاده میشود.



شکل ۵-۲ : نحوه جریان داده در هفت لایه

@caffeinebookly caffeinebookly @caffeinebookly caffeinebookly t.me/caffeinebookly

هنگامی که کامپیوتر دریافت کننده داد ها را دریافت کرد، داده ها راه رفته را بر میگردند و پروتکل های هر لایه روی آنها اعمال میشود. با برعکس شدن تمام مسیر طی شده و اعمال انجام شده، عمل انتقال داده ها جهت پردازش به پایان رسیده است.

پروتکل اترنت

همانطور که میدانید، اولین دو لایه از مدل OSI با ساختار فیزیکی شبکه ارتباط دارند، به این مفهوم که تعیین میکنند کدام ابزارهای شبکه میتوانند اطلاعات را از دستگاهی به دستگاه دیگر ارسال کنند. محبوب ترین پروتکل برای لایه های فیزیکی و اتصال داده، اترنت است.

اترنت از اوایل دهه ۱۹۷۰ تا کنون به شکل های مختلفی ارائه شده است. وضعیت فعلی اترنت توسط استاندارد IEEE بنام 802.3 تعریف شده است. حالات مختلفی از اترنت در سرعت های مختلف و روی رسانه های مختلف مورد استفاده قرار میگیرند. چون تمام نسخه های اترنت باهم سازگاری دارند، میتوانید در یک شبکه با استفاده از ابزارهایی مانند سویچ ها، بریج ها و هاب ها ترکیبی از ارتباطات را با رسانه های مختلف و سرعت های مختلف ایجاد کنید.

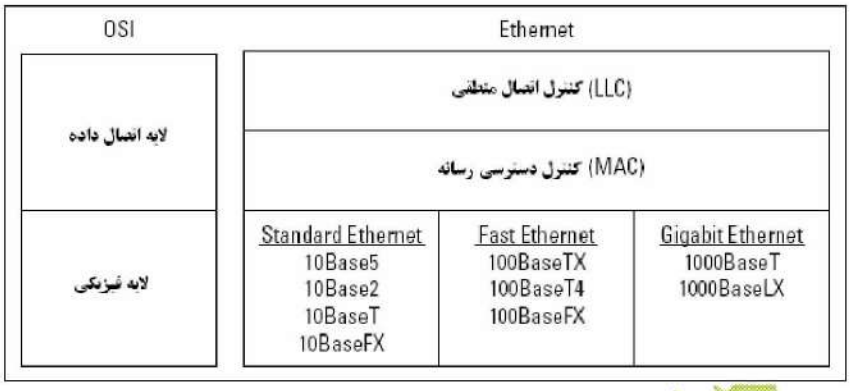
سرعت انتقال واقعی اترنت بصورت میلیون بیت بر ثانیه یا Mbps اندازه گیری میشود. اترنت در سه سرعت مختلف وجود ارد. ۱۰ مگابیت بر ثانیه که اترنت استاندارد است، ۱۰۰ مگابیت بر ثانیه که اترنت سریع است و ۱۰۰۰ مگابیت بر ثانیه که اترنت گیگابیت نامیده میشود. بیاد داشته باشید که سرعت های بیان شده، در واقع سرعت های حداکثری هستند که در شرایط ایده آل شبکه بدست می آیند. در دنیای واقعی، جریان عبوری اترنت به سختی به این میزان ماکزیمم میرسد.

اترنت در دو لایه ابتدایی مدل OSI کار میکند. این استاندارد، لایه اتصال داده را به دو لایه مجزا تقسیم میکند که کنترل اتصال منطقی (LLC) و کنترل دسترسی رسانه (MAC) نامیده میشوند. شکل ۶-۲ نشانگر عناصر مختلف اترنت در هماهنگی با مدل OSI میباشد.

اترنت استاندارد

اترنت استاندارد، اترنت اصلی است. این اترنت با سرعت 10Mbps کار میکند که در دهه ۱۹۷۰ سریع بحساب می آمد، ولی امروزه از استاندارد های بسیار کند است. چون هزینه اترنت سریع در سالهای اخیر بسیار کاهش یافته، بنابراین این استاندارد جایگزین اترنت استاندارد در بسیاری از شبکه های جدید شده است. با این حال، شبکه هایی نیز وجود دارند که هنوز از اترنت استاندارد استفاده میکنند.

@caffeinebookly caffeinebookly @caffeinebookly caffeinebookly t.me/caffeinebookly



شکل ۶-۲ : اترنت و مدل OSI

اترنت استاندارد در چهار طبقه بندی با توجه به نوع کابل مورد استفاده برای شبکه بندی قرار میگیرد:

- **10Base5** : کابل اصلی اترنت که ضخیم (به ضخامت انگشت شست) و سنگین بود و کار با آن بسیار مشکل بود. این کابل امروزه فقط در موزه های IT به چشم میخورد.
- **10Base2** : این نوع نازکتر از کابل کواکسیال (کابل آنتن) در دهه ۸۰ محبوبیت یافت و تا اوایل دهه ۹۰ رایج بود. هنوز هم مقدار زیادی از کابل های 10Base2 مورد استفاده قرار میگیرد، ولی در شبکه های جدید خیلی کم مورد استفاده قرار میگیرد. این کابل نیز مانند کابل استاندارد، اجباراً توپولوژی خطی را تحمیل میکند.
- **10BaseT** : کابل های جفت تابیده بدون پوشش (UTP) در دهه ۹۰ رواج یافتند چون نصب آنها بسیار ساده تر بود و کابلها سبکترو مطمئن تر بودند و انعطاف پذیری را برای طراح شبکه بوجود می آوردند. شبکه های 10BaseT از توپولوژی ستاره ای به کمک هاب ها بعنوان مرکز ستاره استفاده میکنند. حداکثر طول کابل 10BaseT فقط ۱۰۰ متر است و میتوان برای طولانی تر کردن مسیر، هاب ها را بصورت زنجیره ای بهم متصل کرد.
  کابل 10BaseT چهار جفت سیم دارد که دورهم تابیده شده اند. چون 10BaseT فقط از دو جفت سیم استفاده میکند، پس دو جفت دیگر اضافی هستند.
- **10BaseFL** : کابلهای فیبرنوری با استاندارد 10BaseFL در سرعت 10Mbps پشتیبانی میشدند. چون نسخه های جدید و سریع فیبرنوری وجود دارد، 10BaseFL بسیار کم مورد استفاده قرار میگیرد.

@caffeinebookly caffeinebookly @caffeinebookly caffeinebookly t.me/caffeinebookly

اترنت سریع

اترنت سریع به اترنتی اطلاق میشود که با سرعت 100Mbps کار میکند که ۱۰ برابر سریعتر از اترنت استاندارد است. سه نوع مختلف اترنت سریع عبارتند از :

- **100BaseT4** : این پروتکل سرعت انتقال 100Mbps را روی همان کابل UTP شبکه های 10BaseT ایجاد میکند. برای این کار، هر چهار جفت سیم موجود در کابل مورد استفاده قرار میگیرند. 100BaseT4 عمل ارتقای شبکه موجود 10BaseT را به 100Mbps تسهیل میکند.
- **100BaseTX** : معمولترین استاندارد مورد استفاده برای شبکه های اداری امروزی، 100BaseTX میباشد که سرعت 100Mbps را فقط روی دو جفت سیم از کابل UTP درجه بالاتر را امکان پذیر میکند. کابلی که درجه بالاتری نسبت به 10BaseT دارد، Category5 یا در اصطلاح بازار CAT5 نامیده میشود. بسیاری از شبکه های جدید با کابلهای CAT5 یا کابلهای بهتر شبکه بندی میشوند.
- **100BaseFX** : نسخه فیبرنوری اترنت که با سرعت 100Mbps کار میکند. چون کابل فیبرنوری گران است و نصب آن مشکل تر است، زیاد برای کامپیوترها و شبکه های شخصی مورد استفاده قرار نمیگیرد. این اتصال معمولاً بعنوان ستون فقرات شبکه استفاده میشود. برای مثال، یک ستون فقرات فیبرنوری معمولاً برای اتصال گروه های کاری مختلف به سرور ها و روتر ها مورد استفاده قرار میگیرد.

اترنت گیگابیت

اترنت گیگابیت اترنتی است که با سرعت 1000Mbps کار میکند که ۱۰۰ برابر سریعتر از اترنت استاندارد میباشد. این اتصال در شبکه های بسیار بزرگ برای ایجاد ستون فقرات بین سرورها و شبکه مورد استفاده قرار میگیرد. در برخی موارد، اترنت گیگابیت حتی برای اتصال کامپیوترهای رومیزی که نیاز به شبکه بندی سریع دارند مورد استفاده قرار میگیرد. اترنت گیگابیت در دو حالت وجود دارد :

- **1000BaseT** : که میتواند روی کابل CAT5 ایجاد شود، ولی کابلهای درجه بالاتر مانند CAT5e یا CAT6 بهتر عمل میکنند و قابل اطمینان ترند.
- **1000BaseLX** : که همین اتصال از طریق فیبرنوری است.

مجموعه پروتکلهای TCP/IP

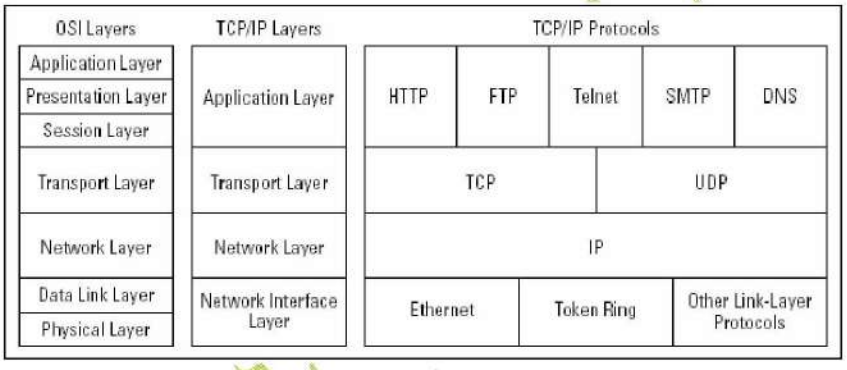
TCP/IP، پروتکلی است که اینترنت بر اساس آن بنا نهاده شده است، و در واقع یک پروتکل واحد نیست بلکه مجموعه ای از پروتکل های مرتبط به هم است. TCP حتی از اترنت نیز قدیمی تر

@caffeinebookly caffeinebookly @caffeinebookly caffeinebookly t.me/caffeinebookly

است. این پروتکل در سال ۱۹۶۹ توسط دپارتمان دفاع ارائه شد. در حال حاضر، نیروی کاری مهندسی اینترنت، یا IETF، مدیریت مجموعه پروتکلهای TCP/IP را بر عهده دارد.

مجموعه TCP/IP بر اساس مدل چهار لایه شبکه مشابه هفت لایه مدل OSI بنا نهاده شده است. شکل ۷-۲ نشانگر نحوه انطباق مدل TCP/IP با مدل OSI است که در آن برخی پرتکلهای کلیدی TCP/IP جایگذاری شده اند. همانطور که مشاهده میکنید، پایین ترین لایه مدل، لایه رابط شبکه است که با لایه های فیزیکی و اتصال داده در مدل OSI همسان است. TCP/IP میتواند روی طیف وسیعی از پروتکل های لایه رابط شبکه اجرا شود که اترنت یا پروتکل هایی مانند توکن رینگ یا FDDI از این جمله اند.

لایه کاربردی مدل TCP/IP با سه لایه بالایی مدل OSI مرتبط است. مهمترین پروتکلهای این بخش نیز HTTP، FTP، Telnet، SMTP، DNS و SNMP میباشند.



شکل ۷-۲ : TCP/IP و مدل OSI

IP

IP، که اختصار عبارت پروتکل اینترنت است، یک پروتکل لایه شبکه است که مسئول جابجایی داده ها به ابزارهای شبکه است. پروتکل IP بجای آدرس فیزیکی، از آدرس های IP منطقی برای مراجعه به ابزارهای گوناگون استفاده میکند. پروتکلی بنام ARP (پروتکل وضوح آدرس) مسئول تبدیل آدرس های IP به آدرس های MAC معادل است.

چون آدرسهای IP از یک بخش شبکه و یک بخش میزبان تشکیل شده اند، IP پروتکلی قابل مسیردهی است. در نتیجه، IP میتواند در صورت عدم حضور میزبان روی شبکه فعلی، پکت را به شبکه دیگری هدایت کند. (توانایی مسیردهی پکت ها بین شبکه ها، مبین نام IP میباشند. یک اینترنت، یک سری از شبکه هاست که توسط TCP/IP متصل شده اند و میتوان با مسیردهی به آنها دسترسی پیدا کرد).

@caffeinebookly caffeinebookly @caffeinebookly caffeinebookly t.me/caffeinebookly

TCP

TCP، که اختصار عبارت پروتکل کنترل انتقال است، پروتکل اتصال محور در لایه انتقال است. TCP به یک ابزار این امکان را میدهد تا با اطمینان پکت ها را به ابزارهای دیگر روی همان شبکه یا شبکه ای دیگر ارسال کند. TCP اطمینان حاصل میکند که هر پکت در صورت امکان به مقصد خود برسد. این کار با ایجاد ارتباط با ابزار مقصد و سپس ارسال پکت انجام میشود. اگر پکت وارد نشود، TCP دوباره پکت را ارسال میکند. ارتباط هنگامی بسته میشود که پکت مورد نظر با موفقیت به مقصد برسد و یا خطایی غیرقابل اصلاح رخ دهد.

بسیاری از پروتکلهای معروف لایه کاربردی براساس TCP میباشند. برای مثال، هنگامی که کاربری کاوشگر اینترنت خود را باز کرده و درخواست یک صفحه میکند، کاوشگر از HTTP برای ارسال درخواست توسط TCP به وب سرور استفاده میکند. هنگامی که وب سرور درخواست را دریافت کرد، از HTTP برای ارسال صفحه وب درخواستی به کاوشگر و باز از طریق TCP استفاده میکند. سایر پروتکلهای لایه کاربردی که از TCP استفاده میکنند میتوان Telnet، FTP و SMTP را نام برد.

UDP

پروتکل داده نمای کاربر (UDP) پروتکل بدون ارتباط لایه انتقال است و هنگامی مورد استفاده قرار میگیرد که وجود یک اتصال مورد نیاز نباشد. پس از اینکه UDP پکتی را روی شبکه قرار داد (توسط پروتکل IP)، دیگر کاری به آن ندارد. UDP هیچ تضمینی در مورد ورود پکت به مقصد ندارد. بسیاری از برنامه های کاربردی که از UDP استفاده میکنند، فقط منتظر پیغام تایید دریافت از سوی مقصد در مدت زمان معینی می مانند و در صورت عدم دریافت این پیغام یا پکت دوباره ارسال میشود و یا عملیات متوقف میشود.

قطعاً بهترین پروتکل لایه کاربردی که از UDP استفاده میکند، DNS است. هنگامی که برنامه ای نیاز به دسترسی به نام دامنه ای مانند www.vc4p.com را دارد، DNS یک پکت UDP را به سرویس دهنده DNS میفرستد تا دامنه را جستجو کند. هنگامی که سرور دامنه را پیدا کرد، آدرس IP مربوط به دامنه را در قابل یک پیغام UDP دیگر، برمیگرداند

مجموعه پروتکلهای IPX/SPX

با اینکه TCP/IP به سرعت تبدیل به پروتکل منتخب بسیاری از شبکه ها میشود، ولی هنوز شبکه های زیادی وجود دارند که از مجموعه پروتکلهای متفاوتی بنام IPX/SPX استفاده میکنند. ناول برای اولین بار مجموعه IPX/SPX را در دهه ۸۰ برای استفاده در سرورهای NetWare ارائه کرد. IPX/SPX با تمام سیستم عامل های ویندوز، OS/2 و حتی یونیکس و لینوکس نیز کار میکند.

@caffeinebookly caffeinebookly @caffeinebookly caffeinebookly t.me/caffeinebookly

نسخه مایکروسافتی IPX/SPX بنامهای متفاوتی عرضه میشود که بستگی به نسخه ویندوز مورد استفاده دارد. میتوانید نامهای NWLink، IPX/SPX Compatible Protocol و یا NWLINK IPX/SPX/NetBIOS Compatible Transport Protocol را ببینید.

نسخه ۵ NetWare و نسخه های بعدی آن، کاملاً از TCP/IP پشتیبانی میکنند، پس نیازی به استفاده از IPX/SPX برای شبکه های ناول وجود ندارد. ولی اگر سرور شبکه NetWare 4.x و یا نسخه 3.x آنرا داشته باشد، اجباراً باید از IPX/SPX استفاده شود. اگر شبکه شما نسخه قدیمی سرورهای ناول را نداشته باشد، استفاده از TCP/IP بهتر از IPX/SPX است.

چند نکته دیگر نیز وجود دارند که باید در مورد IPX/SPX بدانید :

- IPX اختصار عبارات « تبادل بین شبکه ای پکت ها » میباشد. این پروتکل در لایه شکبه قرار دارد و میتوان آنرا با IP مقایسه کرد.
- SPX سرنام عبارت « تبادل پکت ترتیبی » است. این پروتکل در لایه انتقال قرار دارد و قابل قیاس با TCP است.
- برخلاف TCP/IP، IPX/SPX پروتکل استاندارد ارائه شده توسط گروه های استانداردسازی مانند IEEE نیست. در عوض، IPX/SPX استاندارد شخصی ارائه شده توسط ناول است. IPX و IPX/SPX نشانه های تجاری ثبت شده توسط ناول میباشند و نسخه ای که مایکروسافت از این مجموعه ارائه کرده، نمیتواند فقط نام IPX/SPX داشته باشد.

سایر پروتکلهایی که بهتر است بشناسید

سایرپروتکلهای شبکه در کنار اترنت، TCP/IP و IPX/SPX عبارتند از:

- **NetBIOS** : سرنام « سیستم پایه ورودی/خروجی شبکه » که رابط برنامه نویسی کاربردی برای سرویس های شبکه روی کامپیوترهای ویندوز است. این پروتکل هنگام نصب TCP/IP بطور اتوماتیک نصب میشود، ولی هنگام نمایش خصوصیات شبکه پروتکل مجزایی نمایش داده نمیشود. NETBIOS پروتکل لایه نشست است که میتواند با پروتکلهای لایه انتقال مانند TCP، SPX یا NetBEUI کار کند.
- **NetBEUI** : سرنام « رابط کاربر پیشرفته سیستم ورودی/خروجی پایه شبکه » میباشد و پروتکل لایه انتقال است که برای شبکه های مایکروسافت و IBM طراحی شده است.
- **AppleTalk** : کامپیوترهای اپل مجموعه پروتکلهای شبکه خاص خود را دارند که AppleTalk نامیده میشود. مجموعه AppleTalk شامل پروتکلهای لایه های فیزیکی و اتصال داده است که LocalTalk نامیده میشوند، ولی میتوانند با پروتکلهای استاندارد لایه های پایینی کار کنند که شامل اترنت و توکن رینگ نیز میشود.

@caffeinebookly caffeinebookly @caffeinebookly caffeinebookly t.me/caffeinebookly

- **SNA** : « معماری سیستم شبکه » یک معماری شبکه IBM است که به دهه ۷۰، هنگامی که مین فریم ها عمومیت داشتند، برمیگردد. SNA در اصل برای پشتیبانی ترمینالهای بزرگ مانند خطوط هوایی و سیستم های بانکی طراحی شده بود که هزاران ترمینال را به یک میزبان مرکزی متصل میکرد. امروزه که مین فریم های IBM از TCP/IP پشتیبانی میکنند و سیستم های ترمینال برچیده شده اند، این پروتکل نیز در حال فراموش شدن است. هنوز بسیاری از شبکه ها که از مین فریم ها استفاده میکنند، با SNA مدیریت میشوند.

یادداشت

شهر مجازی پارسیان

@caffeinebookly caffeinebookly @caffeinebookly caffeinebookly t.me/caffeinebookly

فصل ۳ : شناخت سخت افزار شبکه

در این فصل میخوانید:

- **معرفی سرویس دهنده ها**
- **کار با کارت های رابط شبکه**
- **آشنایی با کابل شبکه، هاب ها و سویچ ها**
- **بررسی تکرارکننده (تقویت کننده) ها، بریج ها و روترها**
- **آشنایی با ذخیره سازی شبکه**

شهر مجازی پارسیان

@caffeinebookly caffeinebookly @caffeinebookly caffeinebookly t.me/caffeinebookly

قطعات سازنده شبکه ها، سخت افزارهای شبکه مانند سرور ها، کارت های شبکه، کابلها، هاب ها، سویچها، روتر ها و ... میباشند. در این فصل نگاهی به این قطعات سازنده شبکه خواهیم داشت.

سرورها (Servers)

کامپیوترهای سرور جریان حیاتی شبکه هستند. سرورها منابع مشترکی مانند محل ذخیره سازی فایلها، بانکهای اطلاعاتی، پست الکترونیکی، سرویس های وب و ... را فراهم میکنند تا کاربران شبکه از آنها استفاده کنند. انتخاب تجهیزات مناسب برای استفاده در سرور شبکه، یکی از کلیدی ترین تصمیماتی است که هنگام نصب شبکه باید اتخاذ شود. در این بخش، برخی از روشهای تجهیز سرور شبکه تشریح خواهد شد.

نکته : فقط شبکه های کوچک میتوانند بدون حداقل یک سرور اختصاصی کار کنند. برای شبکه های خانگی و شبکه های کوچک اداری دارای تعداد کمی کامپیوتر، میتوانید شبکه بندی ساده P2P را انجام دهید. بدین ترتیب، هر کلاینت منابع خود را مانند فایلها یا چاپگر به اشتراک میگذارد و نیازی به سرور اختصاصی نیست.

چه چیز سرور دارای اهمیت است

چند نکته حائز اهمیت هنگام انتخاب کامپیوتر سرور برای شبکه از این قرارند :

- **مقیاس پذیری** : مقیاس پذیری به توانایی افزایش اندازه و ظرفیت کامپیوتر سرور بطوریکه مشکل خاصی پیش نیاید اطلاق میشود. بزرگترین اشتباه در انتخاب سرور، انتخاب دستگاهی است که نیازهای فعلی شما را برآورده کند. بعد از یک سال خواهید دید که سطح نیازهای شما به دوبرابر میزان فعلی خواهد رسید. پس تا جایی که امکان دارد، سرور خود را با فضای دیسک بیشتر، RAM و قدرت پردازنده بالاتر از نیاز فعلی مجهز کنید.
- **اطمینان** : ضرب المثل مزد به میزان عمل گرفتن در مورد کامپیوترهای سرور کاملاً صادق است. چرا باید بابت سیستمی که میتوان با قطعات ارزان و دست دوم آنرا به قسمت نیم میلیون خرید، ۲ میلیون تومان پرداخت کنیم؟ یکی از علل آن اطمینان است. اگر یکی از کامپیوترهای کلاینت از کار بیفتد، فقط کاربری که با آن کار میکند بیکار میماند. وقتی سرور ایراد پیدا کند، کل شبکه از کار خواهد افتاد و همه بیکار خواهند بود.
- **دسترسی** : این مفهوم نیز بسیار نزدیک به اطمینان است. وقتی یک کامپیوتر سرور ایراد پیدا کند، چقدر طول میکشد تا تعمیر شده و دوباره مانند سابق به کار خود ادامه دهد؟ کامپیوترهای سرور طوری طراحی شده اند که قطعات آنها براحتی معاینه و تعویض شود و بدین ترتیب زمان خرابی هنگام بروز خطا در قطعات کاهش می یابد. در برخی سرورها، قطعات

@caffeinebookly caffeinebookly @caffeinebookly caffeinebookly t.me/caffeinebookly

Hot Swappable هستند، یعنی میتوان آنها را حتی بدون خاموش کردن سرور از سیستم خارج کرده و قطعه جدیدی نصب کرد. برخی سرورها بصورت fault tolerant طراحی شده اند که میتوانند حتی هنگام بروز خطا در قطعات اصلی، به کار خود ادامه دهند.

- **سرویس و پشتیبانی** : سرویس و پشتیبانی از جمله عواملی هستند که هنگام انتخاب هر کامپیوتری به آنها دقت میشود. اگر قطعه ای در یک کامپیوتر سرور ایراد پیدا کند، آیا کسی در محل برای تعمیر کامپیوتر خراب وجود دارد؟ اگر چنین فردی وجود نداشته باشد، باید یک قرارداد نگهداری سیستم نیز با یک متخصص منعقد شود.

اجزای یک کامپیوتر سرور

اجزای سخت افزاری تشکیل دهنده یک کامپیوتر سرور معمولی بسیار شبیه به اجزای مورد استفاده در کامپیوترهای کلاینت عادی است. با این حال، کامپیوترهای سرور معمولاً از قطعاتی با درجه بالاتر نسبت به کامپیوترهای کلاینت برخوردارند. اجزای معمول کامپیوترهای سرور به شرح زیر میباشند :

- **Motherboard** : مادربرد مدار الکترونیکی اصلی کامپیوار است که سایر اجزا روی آن سوار میشوند. مادربورد بیش از سایر قطعات کامپیوتر اهمیت دارد و تمام قطعات به آن متصل میشوند. اجزای اصلی روی مادربرد شامل پردازنده (CPU)، مدارات پشتیبانی بنام Chipset، حافظه، شکاف های توسعه، کنترلگر هارد دیسک IDE استاندارد، درگاه های ورودی/خروجی برای ابزارهایی مانند صفحه کلید، ماوس و چاپگر ها میباشند. برخی مادربرد ها دارای امکانات اضافی مانند کارت گرافیک، کنترلگر دیسک اسکازی و رابط شبکه داخلی نیز میباشند.
- **پردازنده** (CPU) : پردازنده یا CPU، مغز متفکر کامپیوتر است. با اینکه CPU تنها قطعه موثر در بازدهی کل سیستم نیست، ولی بسیاری از افراد هنگام انتخاب سرور، آنرا بعنوان فاکتور اصلی خرید قرار میدهند. هر مادربرد برای پشتیبانی از نوع خاصی از پردازنده طراحی شده است. پردازنده ها به دو صورت قابل نصب میباشند: سوکتی و اسلاتی. پس هنگام انتخاب پردازنده و مادربرد باید به سازگاری پردازنده با مادربرد و محل نصب آن دقت کنید. برخی از مادربرد های سرور دارای دو یا چند سوکت یا اسلات برای قرارگیری پردازنده میباشند.

عبارت سرعت ساعت، سرعت ساعت اصلی پردازنده را که تیک های پردازش پردازنده را ایجاد میکند، اطلاق میشود. در تئوری، هرچه سرعت ساعت بالاتر باشد، پردازنده سریعتر است. با این وجود، سرعت ساعت به تنهایی فقط برای مقایسه پردازنده های هم خانواده مورد استفاده قرار میگیرد. در واقع، پردازنده Xeon بسیار سریعتر از Pentium 4 با سرعت ساعت برابر است. چون Xeon دارای مدارات پیچیده تری نسبت به پنتیوم است و میتواند در هر تیک ساعت، کار بیشتری نسبت به پنتیوم انجام دهد.

@caffeinebookly caffeinebookly @caffeinebookly caffeinebookly t.me/caffeinebookly

- **حافظه** : یکی دیگر از عوامل مهم در کارآیی سرور حافظه آن است. شما باید در میان انواع مختلف حافظه موجود، سازگارترین آنها را با مادربرد خود انتخاب کنید. برخی سرورها میتوانند تا ۱۲ و برخی دیگر تا ۳۲ گیگ حافظه را پشتیبانی کنند.
- **هارد درایو** : بسیاری از کامپیوترهای رومیزی از هارد دیسک های ارزان قیمت بنام درایو های IDE استفاده میکنند (گاهی ATA نامیده میشود). این درایوها برای کاربران عادی کافی است، ولی چون در سرورها بازدهی اهمیت بالایی دارد، نوع دیگری از درایوها بنام SCSI نصب میشود. معمولاً درایوهای اسکازی را با کارت های کنترلگر اسکازی قدرتمند به سیستم متصل میکنند.
- **ارتباط شبکه** : ارتباط شبکه یکی از مهمترین بخش های یک سرور است. بسیاری از سروها دارای رابط شبکه روی مادربرد هستند. اگر سرور دارای چنین امکانی نباشد، باید یک کارت شبکه جدا نیز خریداری و نصب کنید.
- **ویدئو** : گرافیک خیلی بالا برای کامپیوتر سرور اهمیت ندارد. میتوانید برای سرور خود یک کارت گرافیکی ارزان قیمت و معمولی خریداری کنید. کارت گرافیکی ضعیف و مانیتور قدیمی، هیچ تاثیری در بازدهی سرور شما نخواهد داشت.
- **منبع تغذیه** : چون سرور معمولاً ابزارهای بیشتری نسبت به کامپیوتر معمولی دارد، پس نیاز به منبع تغذیه بزرگتری دارد (منبع تغذیه معمولی ۳۰۰ وات است). اگر سرور تعداد زیادی هارد دیسک داشته باشد، نیاز به منبع تغذیه بسیار بزرگتری خواهد داشت.

Form Factor های سرور

عبارت Form Factor مربوط به اندازه، شکل و بسته بندی سخت افزار است. کامپیوترهای سرور معمولاً بصورت یکی از سه فرم زیر میباشند :

- **Tower Case** : بسیاری از سرورها درون تاورهای معمولی مشابه تاورهای کامپیوتر رومیزی قرار میگیرند. یک تاورکیس معمولی سرور ۱۸ اینچ ارتفاع، ۲۰ اینچ عمق و ۹ اینچ عرض دارد و داخل آن فضای کافی برای مادربرد، پنج هارد دیسک یا بیشتر و سایر اجزای مورد نیاز وجود دارد. تاورکیس ها دارای منبع تغذیه داخلی میباشند. برخی از کیس های سرور دارای امکانات جانبی مختص سرور میباشند، مانند منبع تغذیه پشتیبان، فن های قابل تعویض و دیسک های قابل تعویض هنگام روشن بودن سیستم.
- **Rack Mount** : اگر نیاز به استفاده از تعداد کمی سرور باشد، تاور کیس مناسب است و میتوانید کیس ها را در کنار هم زیر میز یا درون یک کابینت قرار دهید. اگر سرورهای بیشتری مورد نیاز باشد، فضای نگهداری آنها بسیار دردسرساز خواهد بود. برای مثال، اگر شبکه شما

@caffeinebookly caffeinebookly @caffeinebookly caffeinebookly t.me/caffeinebookly

نیاز به ده کامپیوترسرور فایل داشته باشد، فضای زیادی برای قرار دادن کیس ها مورد نیاز خواهد بود. سرورهای Rack Mount برای صرفه جویی در فضا طراحی شده اند. یک سرور Rack Mount درون شاسی کوچکی قرار میگیرد که این شاسی نیز درون یک Rack استاندارد ۱۹ اینچی قرار میگیرد. به کمک این Rack میتوانید سرورها را بصورت عمودی روی هم قرار دهید.

- **Blade Server** : این سرورهای طوری طراحی شده اند که جای بسیار کمی اشغال کنند. Blade Server سروری است که روی یک کارت طراحی شده و میتواند همراه تیغه های دیگر در شاسی های مخصوص قرار گیرد. این شاسی ها نیز درون یک رک استاندارد قرار میگیرند. یک شاسی بلید معمولی حدوداً شش سرور را در خود جای میدهد. یکی از مزایای کلیدی سرورهای تیغه ای این است که نیازی به منبع تغذیه مجزا برای هر سرور ندارید. شاسی دارای منبع تغذیه ای است که تمام سرورها را تغذیه میکند. در برخی مواقع خود رک منبع تغذیه دارد که میتواند کل شاسی های بلید را تغذیه کند. بعلاوه، محفظه بلید امکان سویچ KVM را فراهم میکند و شما نیازی به سویچ KVM ندارید. یعنی میتوانید کل سرورهای موجود در شبکه را از طریق یک صفحه کلید، یک نمایشگر و یک ماوس کنترل کنید. یکی از بزرگترین مزایای سرورهای تیغه ای این است که میزان کابل کشی را کاهش میدهند. در رک با سرورهای استاندارد، هر سرور نیاز به کابل برق، کابل صفحه کلید، کابل نمایشگر و سایر کابلهای مورد نیاز را دارد.

کارت های رابط شبکه

هر کامپیوتر روی شبکه، هم کلاینت و هم سرور، نیاز به کارت رابط شبکه (NIC) است تا بتواند به شبکه متصل شده و به آن دسترسی داشته باشد. NIC معمولاً یک کارت مجزاست که در یکی از شکاف های توسعه مادربرد نصب میشود. البته بسیاری از کامپیوترهای امروزی دارای کارت رابط شبکه روی مادربرد میباشند که در این حالت نیازی به نصب کارت اضافی نمیباشد.

برای کامپیوترهای کلاینت، میتوانید با استفاده از NIC های داخلی کار کنید، چون کامپیوتر های کلاینت برای اتصال فقط ۱ کاربر به شبکه مورد استفاده قرار میگیرند. NIC موجود روی سرور تعداد زیادی از کاربران شبکه را به سرور متصل میکند. در نتیجه، برای یک سرور با کارکرد بالا، بهتر است هزینه بیشتری کرده و NIC بهتری خریداری شود. بسیاری از سرپرستان شبکه ترجیح میدهند تا کارت شبکه خود را از مارک های معروف مانند Intel، SMC، 3COM و ... تهیه کنند.

کارت رابط شبکه ای که شما از آن استفاده میکنید، باید رابطی داشته باشد که با کابل مورد استفاده شما همخوانی داشته باشد. اگر میخواهید شبکه خود را بصورت Thinnet کابل کشی کنید،

@caffeinebookly caffeinebookly @caffeinebookly caffeinebookly t.me/caffeinebookly

باید کارت شبکه شما رابط BNC داشته باشد. برای کابل کشی جفت تابیده، کارت شما باید دارای اتصال RJ-45 باشد

برخی از کارت های شبکه، دارای دو یا چند رابط هستند. BNC و AUI، RJ-45 و AUI، BNC و RJ-45 و یا هر سه اتصال همراه هم. انتخاب کارتی که هم دارای رابط BNC بوده و هم سوکت RJ-45 داشته باشد، فکر بدی نیست. بدین ترتیب، میتوانید شبکه خود را از کابل کشی Thinnet بصورت جهت تابیده یا برعکس تبدیل کنید. قیمت هر کارت رابط شبکه، مبلغی از ۵ تا ۱۵ هزار تومان است. در مورد AUI هم حساس نباشید، چون هرگز به آن نیاز پیدا نخواهید کرد.

بسیاری از کارتهای شبکه امروزی هم در سرعت ۱۰ و هم در سرعت ۱۰۰ مگابیت بر ثانیه کار میکنند و بنام کارتهای ۱۰/۱۰۰ معروفند. این کارتها بطور اتوماتیک میتوانند سرعت خود را با سرعت شبکه هماهنگ کنند. بدین ترتیب میتوانید بدون هیچ مشکلی آنرا در شبکه های قدیمی مورد استفاده قرار دهید.

کارتهای 1000BaseT بسیار گران تر از کارت های مذکور میباشند که البته اخیراً افت قیمت بسیاری پیدا کرده اند. کارت های معمولی گیگابیت را میتواند به قیمت های پایین خرید، ولی اگر این کارتها دارای امکانات جانبی بیشتری مانند بافر های بزرگتر و پردازنده ورودی/خروجی شبکه باشند، قیمت آنها میتواند تا ۱۰۰ هزار تومان هم بالا رود.

چند نکته نیز در مورد کارتهای شبکه حائز اهمیت است :

- یک کارت شبکه ابزاری از لایه های فیزیکی و اتصال داده است. چون NIC یک ناد شبکه را ایجاد میکند، باید دارای آدرس شبکه فیزیکی باشد که بنام آدرس MAC معروف است. آدرس MAC در کارخانه روی NIC قرار داده میشود و نمیتوان آنرا تغییر داد. هر NIC که تاکنون تولید شده است، دارای آدرس MAC منحصربفرد خود است.
- برای کامپیوترهای سرور، بیش از یک NIC قرار داده میشود. بدین ترتیب، سرور میتواند ترافیک شبکه بیشتری را مدیریت کند. برخی NIC های سرور دارای دو یا چند کارت شبکه درون یک کارت میباشند.
- شبکه های فیبرنوری نیز به NIC نیاز دارند. کارتهای رابط شبکه فیبرنوری هنوز برای استفاده های خانگی بسیار گرانند. چنین ابزارهایی برای ستون فقرات بسیار سریع مورد استفاده قرار میگیرند. اگر سروری به یک ستون فقرات سریع فیبری متصل شود، نیاز به کارت رابط شبکه ای دارد که با کابل فیبرنوری مورد استفاده همخوانی داشته باشد.

کابل شبکه

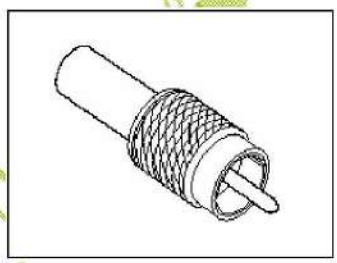
میتوانید یک شبکه اترنت را با استفاده از دو نوع مختلف کابل راه اندازی کنید : کابل کواکسیال که تقریباً همان کابل آنتن تلویزیون است، یا کابل جفت تابیده که مانند کابل تلفن است. کابل جفت

@caffeinebookly caffeinebookly @caffeinebookly caffeinebookly t.me/caffeinebookly

تابیده گاهی بنام UTP یا 10BaseT نیز شناخته میشود. انتخاب سوم عدم استفاده از کابل شبکه و استفاده از شبکه های بیسیم به جای کابلی است.

کابل کواکسیال

نوعی از کابل که زمانی برای شبکه های اترنت بسیار کاربرد داشت، کابل کواکسیال است که گاهی کابل Thinnet یا کابل BNC نامیده میشود. کابل کواکسیال فقط در سرعت ۱۰ مگابیت کار میکند و در شبکه های جدید بسیار کم مورد استفاده قرار میگیرد. با این حال، شبکه های قدیمی بسیاری می بینید که از این طریق کار میکنند.



شکل ۱-۳ : کابل کواکسیال با رابط BNC

چند نکته در مورد کابل کواکسیال :

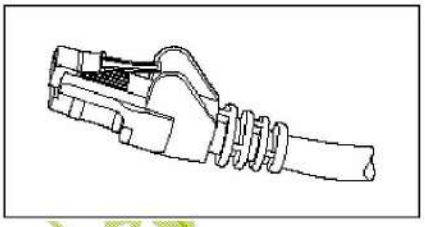
- شما میتوانید Thinnet را با استفاده از استفاده از یک اتصال پیچشی به رابط BNC متصل کنید.
- با کابلهای کواکسیال، کامپیوتر خود را بصورت نظیر به نظیر و با توپولوژی خطی به هم متصل میکنید. در هر کامپیوتر یک رابط T نصب میشود و دو انتهای کابل شبکه به آن متصل میشود.
- یک اتصال خاص بنام ترمیناتور برای هر انتهای کابل کواکسیال مورد نیاز خواهد بود. ترمیناتور باعث میشود تا داده ها در انتهای آزاد کابل خنثی شوند و باصطلاح روی زمین نریزند.
- طول کابل از یک ترمیناتور به ترمیناتور دیگر سگمنت نامیده میشود. حداکثر طول سگمنت Thinnet حدود ۲۰۰ متر است (در عمل ۱۸۵ متر). میتوانید تا ۳۰ کامپیوتر روی سگمنت داشته باشید. برای داشتن کامپیوترهای بیشتر باید از سگمنت های جداگانه استفاده کنید و از دستگاهی بنام تقویت کننده (تکرارکننده) نیز برای اتصال سگمنت ها استفاده کنید.
- با اینکه کابل کواکسیال مشابه کابل آنتن تلویزیون است، ولی کمی با آن متفاوت است و این دو کابل مقاومت های متفاوتی دارند. پس به خاطر ارزان بودن کابل آنتن از آن استفاده نکنید چون جوابگوی شبکه نخواهد بود.

@caffeinebookly caffeinebookly @caffeinebookly caffeinebookly t.me/caffeinebookly

کابل جفت تابیده

محبوب ترین نوع کابل که امروزه مورد استفاده قرار میگیرد، کابل جفت تابیده یا UTP است. U به مفهوم بدون حفاظ استفاده میشود، ولی این کابل را جفت تابیده بدون حفاظ نمی نامند و فقط جفت تابیده کافی است. کابل UTP ارزانتر از کابل کواکسیال است و بازدهی بهتری دارد و بسیاری از ساختمان های جدید، دارای سیمکشی کابل جفت تابیده جهت استفاده از امکانات مختلف آن مانند سیستم های تلفن مودمی میباشند.

شکل ۲-۳ : کابل جفت تابیده



هنگامی که شما از کابل UTP جهت ساخت شبکه اترنت استفاده میکنید، کامپیوترها را بصورت آرایش ستاره ای قرار میدهید. در مرکز این ستاره، ابزاری بنام هاب قرار میگیرد. بسته به مدل هاب، شما این امکان را دارید که از ۴ تا ۲۴ کامپیوتر را با استفاده از کابل جفت تابیده به هم متصل کنید.

یکی از مزایای آرایش ستاره ای UTP این است که اگر یک کابل مشکل داشته باشد، فقط کامپیوتری که با آن کابل شبکه شده، تحت تاثیر قرار میگیرد و بقیه شبکه به کار عادی خود ادامه میدهد. با کابل کواکسیال، کابل خراب کل شبکه را تحت تاثیر قرار میدهد.

جزئیات دیگری که باید در مورد کابل کشی جفت تابیده بدانید از این قرار است :

- کابل UTP بصورت جفت هایی از سیم تابیده به یکدیگر است و چند جفت به این حالت درون یک پوشش بیرونی قرار میگیرند. اترنت از دو یا چهار جفت از این سیم ها استفاده میکند. تعداد جفت های درون این کابل متفاوت است، ولی معمولاً بیش از دو جفت است.
- کابل UTP در درجه های مختلف با عنوان Category عرضه میشود. برای شبکه، کابل پایین از درجه ۵ استفاده نکنید. کابلهای درجه پایین ارزانترند، ولی قابلیت پشتیبانی شبکه های پرسرعت را نخواهند داشت.
- معادل حرفه ای تر عبارت Category 5 ، Cat 5 است.
- کابلهای Cat5 برای سرعت 100Mbps بسیار مناسبند، ولی برای شبکه های گیگابیت، باید از کابلهای Cat5e یا Cat6 استفاده کنید.
- اتصال کابل UTP مانند اتصال تلفن معمولی است ولی کمی بزرگتر. اتصالات UTP را RJ-45 مینامند.

@caffeinebookly caffeinebookly @caffeinebookly caffeinebookly t.me/caffeinebookly

- مانند کابلهای Thinnet، کابلهای UTP نیز بصورت آماده و در اندازه های از پیش تعیین شده فروخته میشوند. نصب اتصالات RJ-45 روی کابل UTP بسیار ساده تر از نصب کابل کواکسیال است. ابزار مورد نیاز برای نصب RJ-45 روی کابل را کریمپر مینامند.
- حداکثر طول کابل مجاز بین هاب و کامپیوتر ۱۰۰ متر میباشد.

هاب ها و سویچ ها

بزرگترین تفاوت میان کابلهای کواکسیال و جفت تابیده این است که هنگامی که از کابل جفت تابیده استفاده میکنید، باید از ابزار دیگری بنام هاب نیز استفاده کنید. سالها پیش، هاب ها دستگاه های بسیار گران قیمتی بودند بطوریکه استفاده از این ابزارها برای کسانی که کار شبکه را در مقیاس کوچک و خانگی انجام میدادند، ناممکن بود.

امروزه، هزینه هاب ها بسیار پایین آمده است بطوریکه خرید یک هاب ارزش استفاده از مزایای شبکه بندی جفت تابیده را دارد. با این روش کابل کشی، میتوانید بسادگی کامپیوترهای جدیدی را به شبکه اضافه کنید، آنها را جابجا کنید و مشکلات کابل کشی را براحتی حل کنید و کامپیوترهایی را که نیاز به سرویس دارند، براحتی از شبکه خارج کنید.

سویچ، نوع بسیار خاصی از هاب است. چون قیمت سویچ ها بسیار پایین آمده است، بسیاری از شبکه های امروزه به جای هاب از سویچ استفاده میکنند. اگر شبکه ای قدیمی دارید که از هاب ها استفاده میکند، با تعویض هاب های قدیمی با سویچ های جدید، میتوانید سرعت شبکه خود را بسیار بهتر کنید.

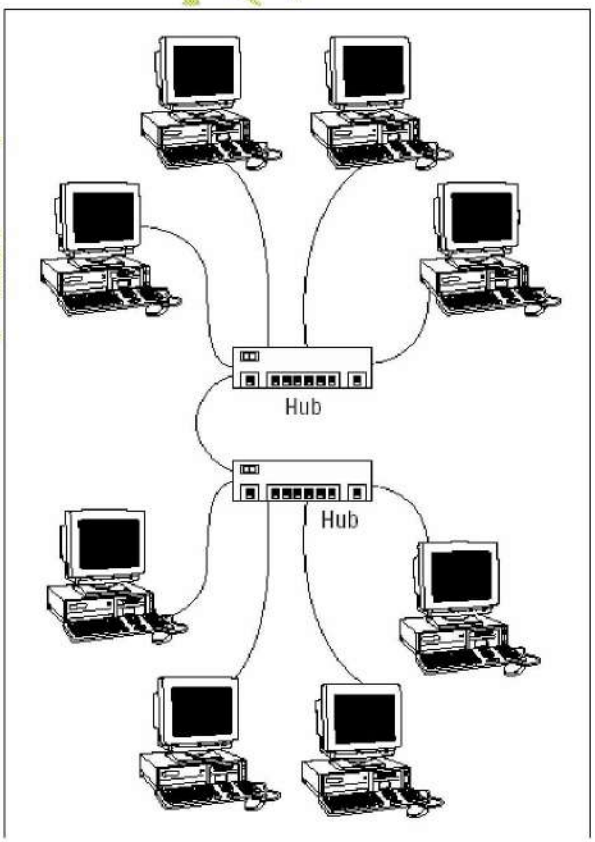
اگر از کابل کشی جفت تابیده استفاده میکنید، دانستن چند نکته در مورد هاب ها الزامی است :

- چون باید کابل را از هر کامپیوتر به هاب یا سویچ بکشید، یک محل مرکزی برای هاب یا سویچ انتخاب کنید بطوریکه بتوانید براحتی کابل کشی را انجام دهید.
- هاب یا سویچ نیاز به برق دارند، پس محل آنرا نزدیک پریز برق انتخاب کنید.
- هنگامی که هاب یا سویچ میخرید، نوعی از آن را بخرید که پورت های آن حداقل دوبرابر میزان مورد نیاز شما باشد. اگر میخواهید چهار کامپیوتر را شبکه کنید، یک هاب چهار پورته نخرید، چون قادر به اتصال کامپیوتر پنجم در صورت نیاز نخواهید بود و باید هاب دیگری خریداری کنید.
- میتوانید دو یا چند هاب یا سویچ را با هم بصورت زنجیره ای قرار دهید. اگر کامپیوترهای بیشتری دارید، میتوانید هاب هایی خریداری کنید که دارای یک ارتباط BNC هستند و به این ترتیب، میتوانید هاب ها را با استفاده ار کابل کواکسیال به هم شبکه کنید و از تمام پورت های آنها استفاده کنید. همچنین هاب هایی وجود دارند که دارای ارتباط سریع با یکدیگر میباشند و

@caffeinebookly caffeinebookly @caffeinebookly caffeinebookly t.me/caffeinebookly

میتوانید آنها را طوری به هم متصل کنید که کل مجموعه بعنوان یک هاب یا سویچ واحد عمل کند.

- هنگامی که هاب های شبکه را خریداری میکنید، میبینید که موارد گرانتر دارای قابلیت مدیریت شبکه میباشند که از چیزی بنام SNMP پشتیبانی میکند. این هاب ها را هاب های مدیریتی میگویند. تا زمانی که شبکه شما بسیار بزرگ نشده و کاملاً از مفهوم SNMP مطلع نشدید، بابت آن هزینه نکنید، چون برای قابلیتی هزینه میکنید که هرگز از آن استفاده نخواهید کرد.
- برای شبکه های بزرگ، ممکن است بخواهید از یک سویچ مدیریتی استفاده کنید. یک سویچ مدیریتی به شما این امکان را میدهد قسمت های مختلف کار سویچ را از طریق یک کامپیوتر راه دور کنترل کنید. سویچ هنگام بروز خطا شما را آگاه خواهد کرد و قادر است تا آماری ارائه دهد که به شما در یافتن گره های شبکه کمک میکند. یک سویچ مدیریتی دو یا سه برابر سویچ معمولی قیمت دارد، ولی برای شبکه های بزرگ، مزیت مدیریت، به هزینه اضافی آن می ارزد.



شکل ۳-۳ : قابلیت اتصال زنجیره ای هاب ها یا سویچ ها به یکدیگر.

@caffeinebookly caffeinebookly @caffeinebookly caffeinebookly t.me/caffeinebookly

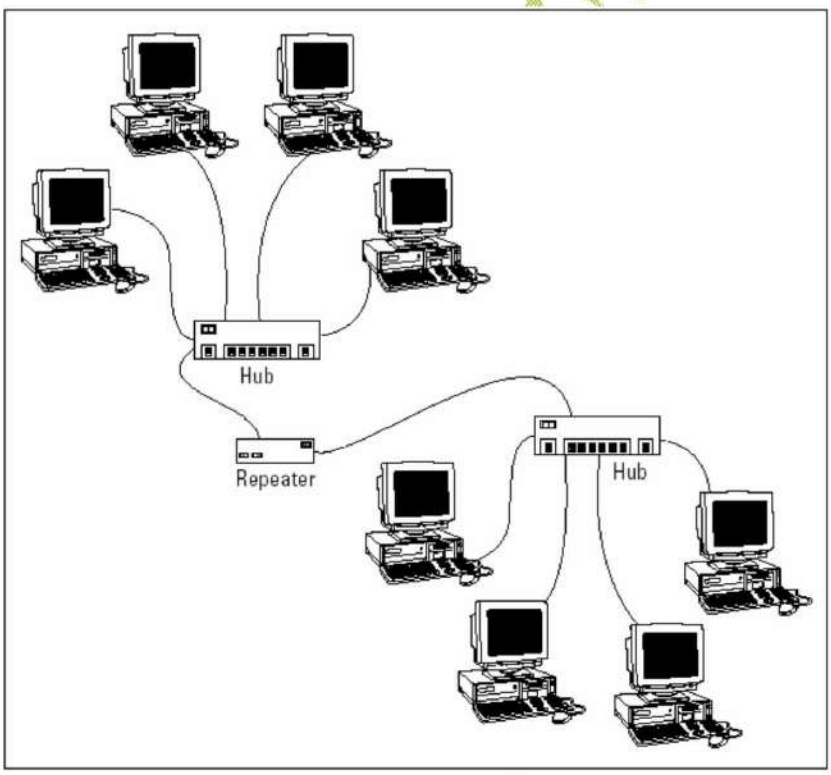
تکرار کنند ها (تقویت کننده)

تکرار کننده ابزاری است که به شما امکان میدهد تا سیگنال های شبکه خود را تقویت کنید، بطوریکه سیگنال ها بتوانند مسیر بیشتری را بپیمایند.

هنگامی که طول کابل شبکه شما باید از حداکثر مقدار مجاز بیشتر باشد، استفاده از تکرار کننده الزامی خواهد شد.

در مورد کابلهای کواکسیال،طول حداکثر مربوط به کل سگمنت است نه طول قطعات کابل و همانگونه که گفته شد، سگمنت کل طول کابل کشی در شبکه است. بعبارت دیگر، شما اگر ده کامپیوتر داشته باشید، میتوانید آنها را حداکثر به فاصله ۱۸/۵ متری از هم قرار دهید. در مورد کابلهای جفت تابیده، این محدودیت در مورد طول کابل از کامپیوتر به هاب یا سویچ است.

شکل ۴-۳ نشان میدهد که چگونه میتوانید دو گروه از کامپیوترها را که فاصله زیادی از هم دارند، با استفاده از تکرارکننده به هم متصل کنید. هنگامی که به این صورت از تکرارکننده استفاده میکنید، کابل به دو سگمنت تقسیم میشود و در دو سوی تکرار کننده، هنوز هم محدودیت طول کابل پابرجاست.



شکل ۴-۳ استفاده از تکرار کننده

@caffeinebookly caffeinebookly @caffeinebookly caffeinebookly t.me/caffeinebookly

چند نکته که در مورد تکرار کننده ها مهم است :

- تکرار کننده ها فقط با شبکه های اترنت که کابل کشی آنها با کابل کواکسیال است کار میکنند. شبکه های 10/100BaseT از تکرار کننده استفاده نمیکنند. (شبکه های 10/100BaseT نیز از تکرار کننده استفاده میکنند، ولی در این شبکه ها، هاب یا سویچ خود به عنوان تکرار کننده عمل میکند و نیاز به دستگاه مجزا برای این کار نیست).
- برخی از هاب های 10/100BaseT دارای ارتباط BNC میباشند. این ارتباط BNC یک تکرارکننده است که به شما این امکان را میدهد تا یک سگمنت کامل ۱۸۵ متری را به آن متصل کنید. این سگمنت میتواند ارتباطی از سایر کامپیوترها و یا هاب ها و یا ترکیبی از این موارد باشد.
- یک قانون اصلی در اترنت این است که سیگنال نمیتواند از بیش از سه تکرار کننده در مسیر رسیدن به ناد مقصد عبور کند. البته منظور این نیست که نمیتوانید در شبکه از سه تکرار کننده استفاده کنید، بلکه باید در طراحی شبکه طوری دقت به خرج دهید که قانون سه تکرار کننده رعایت شود.
- تکرار کننده ها فقط این امکان را فراهم میکنند که سگمنت ها را به هم متصب کنید و قادر به افزایش طول سگمنت نیستند. البته محصولاتی وجود دارند که به کمک آنها میتوان بر محدودیت ۱۸۵ متری کواکس یا ۱۰۰ متری کابلهای جفت تابیده غالب شد، ولی همیشه بیاد داشته باشید که کار کردن براساس قوانین بهترین نتیجه را دربر خواهد داشت.

بریج ها

یک بریج یا پل، ابزاری است که دو شبکه را طوری به هم متصل میکند که بصورت یک شبکه واحد عمل کنند. پلها برای قسمت بندی یک شبکه بزرگ به دو یا چند شبکه کوچکتر جهت بالا رفتن بازدهی مورد استفاده قرار میگیرند. میتوانید پلها را مانند نوعی تکرار کننده هوشمند تصور کنید. تکرار کننده ها به سیگنال های وارده گوش میدهند و آنها را تقویت کرده و دوباره روی کابل ارسال میکنند. این کار تکرار کننده ها کورکورانه است و هیچ توجهی به محتویات پیام ندارند.

در مقابل، یک بریج، کمی هوشمندتر است. برای مبتدیان، بسیاری از بریج ها توانایی گوش فرادادن به شبکه و آدرس دهی اتوماتیک کامپیوتر های هردو سوی پل را دارند. پس بریج ها میتوانند پیام وارده از یک سوی پل را بررسی کرده و آنرا به آنسوی پل ارسال کنند، ولی این کار فقط در مورد پیام هایی انجام میشود که کامپیوتر مقصد آنها در آنسوی پل وجود داشته باشد.

@caffeinebookly caffeinebookly @caffeinebookly caffeinebookly t.me/caffeinebookly

قابلیت کلیدی که به پلها امکان بخش بندی شبکه های بزرگ را میدهد، باعث ایجاد شبکه های بسیار کارآمدی میشود. پلها در شبکه هایی بیشتر کارآیی دارد که از تکه های زیادی تشکیل شده باشند.

یک پل، قادر است شبکه بزرگ را به دو شبکه کوچک تقسیم کند. سپس یاد میگیرد که کدام کامپیوترهای روی شبکه A و کدام روی شبکه B قرار دارند. پس پیام های A به B و برعکس، فقط هنگام نیاز تبادل میشوند. بازدهی کل شبکه در این حالت افزایش می یابد، ولی وقتی نیاز به عبور پیام از پل باشد، عملیات با تاخیر بسیار کمی انجام میگیرد.

نکات دیگری نیز در مورد پلها قابل ذکر است :

- برخی پلها توانایی ترجمه پیامها را از یک قالب به قالب دیگر دارند. برای مثال، اگر شبکه A بصورت اترنت باشد و شبکه B بصورت توکن رینگ، پل میتواند پیامهای این دو شبکه را برای هم ترجمه کند.
- میتوانید پلها را به قیمتهایی در حدود ۵۰۰ هزار تومان خریداری کنید. بریج های بسیار خاص تر و پیچیده تری نیز وجود دارند که قیمتی تا ۵ میلیون تومان دارند.
- میتوانید با استفاده از دو کارت شبکه و یک کامپیوتر نسبتاً ضعیف و نرم افزار مناسب، پل را بصورت نرم افزاری راه اندازی کنید.

مسیریاب ها (روترها)

روتر مانند بریج است، ولی یک تفاوت کلیدی دارد. پلها ابزارهای لایه اتصال داده میباشند، پس میتوانند آدرس MAC ناد های شبکه را اعلام کنند و پیام را به سگمنت مناسب ارسال کنند. با این حال، قادر نیستند خود پیام را دریافت کرده و نوع پیام آنرا مشخص کنند. در عوض، روتر ابزاری متعلق به لایه شبکه است و میتواند با پکت های شبکه در سطح بالاتری کار کند. روتر میتواند آدرس IP پکت عبوری را بررسی کند. چون آدرس IP دربر گیرنده آدرسهای میزبان و شبکه است، روتر میتواند تصمیم گیری کند که پیام از کدام شبکه آمده و به کدام شبکه خواهد رفت. بریجها این اطلاعات را درنظر نمیگیرند.

یکی از تفاوتهای اصلی بین بریج و روتر ایت است که بریج برای شبکه نامرئی است. ولی روتر خودش بعنوان یک ناد محسوب میشود که آدرس MAC و آدرس IP مخصوص خود را دارد. بدین ترتیب پیامها قابل هدایت به روتری هستند که قادر به خواندن محتویات پیام است و میداند با ان چه برخوردی داشته باشد.

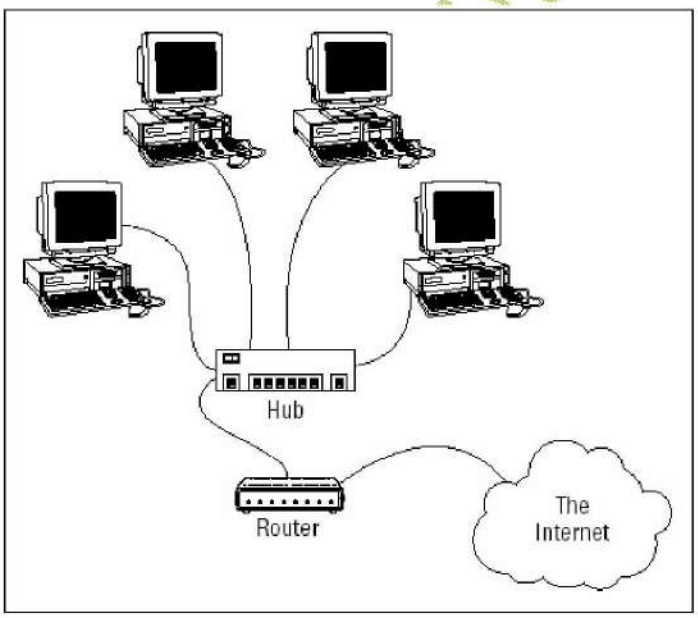
میتوانید شبکه را با چندین روتر طوری پیکربندی کنید که کل شبکه بصورت اشتراکی کار کند. برای مثال، برخی روترها میتوانند شبکه را تحت نظر بگیرند و بهترین مسیر را برای ارسال پیام به

@caffeinebookly caffeinebookly @caffeinebookly caffeinebookly t.me/caffeinebookly

مقصد نهایی انتخاب کنند. اگر بخشی از شبکه زیاد مشغول باشد، روتر میتواند بطور اتوماتیک پیامها را از طریق یک مسیر خلوت تر هدایت کند.

نکاتی دیگری در مورد روتر وجود دارد که دانستن آنها ضروری است :

- روترها ارزان قیمت نیستند ولی برای شبکه های بزرگ ارزش خرید دارند.
- تفاوت کاری بین روترها و بریج ها (و هاب و سویچ) به مرور زمان کمرنگ میشود. با ایجاد هاب ها و سویچ های اختصاصی تر که میتوانند برخی از کارهای روتر را انجام دهند، روترهای زیادی از رده خارج شده اند.
- برخی روترها چیزی بیش از کامپیوترهایی با چندین کارت شبکه و نرم افزاری خاص روتر نیستند.
- روتر میتواند شبکه هایی را که از لحاظ جغرافیایی از هم دورند را از طریق خط تلفن به هم متصل کند.
- میتوانید از یک روتر برای اتصال LAN خود به اینترنت استفاده کنید. شکل ۵-۳ نشانگر استفاده از روتر برای این کار میباشد.



شکل ۵-۳ : استفاده از روتر

@caffeinebookly caffeinebookly @caffeinebookly caffeinebookly t.me/caffeinebookly

محل ذخیره سازی متصل به شبکه

بسیاری از سرورهای شبکه فقط به این علت ساخته میشوند که فضای ذخیره سازی را برای کاربران شبکه ایجاد کنند. با رشد شبکه ها و پشتیبانی آنها از کاربران بیشتر، نیاز کاربران به فضای دیسک بالاتر رفته و سرپرستان شبکه نیز همواره در پی یافتن روشی برای افزودن فضای ذخیره سازی بیشتر به شبکه خود میباشند. ساده ترین و ارزان ترین روش برای این کار، استفاده از فضای ذخیره سازی متصل به سرور میباشد که به NAS معروف است.

NAS ابزاری است که درون آن یک فایل سرور داخلی وجود دارد که از قبل تنظیم شده و آماده استفاده است. تنها چیزی که شما باید انجام دهید این است که آنرا از بسته بندی خارج کرده و در شبکه قرار دهید. نصب و پیکربندی ابزارهای NAS بسیار ساده است و نگهداری آنها ساده تر و ارزانتر از سرورهای فایل عادی است.

دقت کنید که NAS را با عبارت SAN به مفهوم شبکه های ناحیه ذخیره سازی اشتباه نگیرید. SAN یک تکنولوژی بسیار پیچیده و گرانقیمت است که فضاهای ذخیره سازی بسیار بزرگ را برای شبکه های بزرگ فراهم میکند.

یکی از نمونه های سطح معمولی NAS را میتوان Dell 725N ذکر کرد. این ابزار که یک سرور فایل داخلی دارد، درون یک شاسی رک کوچک قرار داده شده است. این دستگاه تا چهار هارد درایو را پشتیبانی میکند که مجموع حجم میتواند تا یک ترابایت نیز بالا رود. مدل 475 دارای یک مادربرد دو پردازنده ای است که میتواند تا ۳ گیگابایت حافظه داشته باشد و دو رابط شبکه داخلی 10/100/1000Mbps دارد. یک نمایشگر LCD در پنل جلو نیز آدرس IP دستگاه را نمایش میدهد.

Dell 725N نسخه خاصی از ویندوز ۲۰۰۳ سرور را اجرا میکند که Windows Storage Server 2003 نامیده میشود. این نسخه از ویندوز مخصوص ابزارهای NAS طراحی شده است. بدین ترتیب میتوانید NAS را از هر کامپیوتری روی شبکه با استفاده از کاوشگر وب تنظیم کنید.

بیاد داشته باشید که برخی ابزارهای NAS از نسخه های ویژه لینوکس بجای Windows Storage Server استفاده میکنند. همچنین، در برخی سیستمها، سیستم عامل روی هارد درایوی مجزا نگهداری میشود که از دیسک های مشترک مجزاست. بدین ترتیب، کاربر قادر به صدمه زدن به سیستم عامل نخواهد بود.

@caffeinebookly caffeinebookly @caffeinebookly caffeinebookly t.me/caffeinebookly

چاپگرهای شبکه

شما میتوانید چاپگر را نیز با اتصال آن به کامپیوتر سرور روی شبکه به اشتراک بگذارید. برخی چاپگرها دارای کارت شبکه داخلی میباشند که دیگر نیازی به اتصال آنها به سرور مجزا وجود نخواهد داشت.

ولی حتی اگر چاپگر توانایی اتصال مستقیم به شبکه را نیز داشته باشد، هنوز استفاده از کامپیوتر سروری که دارای سیستم عامل شبکه باشد، توصیه میشود. بدین ترتیب، سرور میتواند وظایف چاپ را ذخیره کرده و آنها را سازماندهی و صف بندی کند.

یادداشت

شهر مجازی پارسیان

@caffeinebookly caffeinebookly @caffeinebookly caffeinebookly t.me/caffeinebookly

فصل ۴ : شناخت سیستم عامل های شبکه

در این فصل میخوانید :

- درک کارکرد سیستم عامل شبکه
- شناخت مزایای ویندوز ۲۰۰۳ سرور
- بررسی ویندوز ۲۰۰۰ سرور
- نگاهی به ویندوز NT سرور
- بررسی NetWare
- نگاهی به سیستم عاملهای شبکه
- کاوشی در شبکه های نظیر به نظیر

@caffeinebookly caffeinebookly @caffeinebookly caffeinebookly t.me/caffeinebookly

یکی از انتخاب های اساسی که باید قبل از هر کاری انجام شود، تصمیم گیری در مورد سیستم عامل شبکه (NOS) جهت برپایی زیربنای است. این فصل با تشریح امکانات مهم موجود در تمام سیستم عامل های شبکه آغاز میشود. سپس مروری برا مزایا و معایب محبوب ترین سیستم عامل های شبکه خواهیم داشت.

قابلیت های سیستم عاملهای شبکه

تمام سیستم عامل های شبکه، از ساده ترین آنها مانند ویندوز XP نسخه خانگی، تا پیچیده ترین آنها، مانند ویندوز ۲۰۰۳ سرور نسخه مرکز داده ها، باید کارکردهای اساسی مورد نیاز را مانند توانایی اتصال به سایر کامپیوترهای روی شبکه، اشتراک فایلها و منابع، ایجاد امنیت و ... را داشته باشند.

پشتیبانی شبکه

واضح است که سیستم عامل شبکه باید از شبکه پشتیبانی کند. سیستم عامل شبکه باید طیف وسیعی از پروتکلهای شبکه را پشتیبانی کند تا نیاز کاربران مختلف را برآورده سازد. علت این است که شبکه های بزرگ، ممکن است ترکیبی از نسخه های مختلف ویندوز، سیستم عامل مکینتاش و لینوکس و ... باشند. در نتیجه، سرور باید همزمان از پروتکلهایی مانند TCP/IP، NetBIOS و AppleTalk پشتیبانی کند.

بسیاری از سرورها بیش از یک کارت رابط شبکه دارند. در چنین مواردی، NOS باید قادر به پشتیبانی از چندین ارتباط شبکه باشد. NOS باید قابلیت توازن بار شبکه را در بین کارت های رابطش داشته باشد. بعلاوه، در مواقعی که یکی از اتصالات مشکل پیدا کند، NOS باید قادر به سویچ سریع به اتصال دیگر باشد.

و در نهایت، بسیاری از سیستم عاملهای شبکه دارای توانایی درونی برای انجام وظیفه بعنوان روتر را برای اتصال دو شبکه به یکدیگر میباشند. روتر NOS باید دارای قابلیت دیواره آتش باشد تا از عبور پکتهای بدون مجوز در سراسر شبکه محلی جلوگیری کند.

سرویس های اشتراک فایل

یکی از مهمترین عملکردهای سیستم عامل شبکه، توانایی اشتراک منابع با کاربران دیگر شبکه است. معمولترین منبعی که به اشتراک گذاشته میشود، سیستم فایل سرور است. سرور شبکه باید بتواند یک قسمت یا تمام فضای دیسک خود را به اشتراک بگذارد بطوریکه کاربران بتوانند از این فضای دیسک، بصورت فضایی الحاقی به دیسک کامپیوتر خود استفاده کنند.

@caffeinebookly caffeinebookly @caffeinebookly caffeinebookly t.me/caffeinebookly

NOS به سرپرست سیستم این امکان را میدهد که قسمت اشتراکی سیستم فایل را مشخص کند. با اینکه کل هارد دیسک را میتوان به اشتراک گذاشت، ولی معمولاً این کار انجام نمیشود. در عوض، دایرکتوری های خاصی ایجاد شده و به اشتراک گذاشته میشود. سرپرست شبکه میتواند کنترل کند که کدام کاربر به کدام پوشه اشتراکی دسترسی داشته باشد.

چون اشتراک فایل علت وجود بسیاری از سرورهای شبکه است، بنابراین سیستم عامل شبکه نیز باید دارای امکانات تخصصی تر مدیریت دیسک و فایل نسبت به سیستم عامل های رومیزی باشد. برای مثال، سیستم عامل شبکه میتواند چندین هارد دیسک را طوری مدیریت کند که بصورت یک هارد دیسک واحد درنظر گرفته شوند. بعلاوه، بسیاری از سیستم عاملها میتوانند حالت آینه (Mirror) ایجاد کنند که بطور اتوماتیک یک کپی پشتیبان از محتویات هارد درایو اصلی را روی یک درایو ثانویه نگهداری میکند.

چندوظیفگی

فقط یک کاربر در آن واحد میتواند از یک کامپیوتر رومیزی استفاده کند ولی چندین کاربر میتوانند بصورت همزمان از کامپیوتر سرور استفاده کنند. در نتیجه، سیستم عامل شبکه باید از چندین کاربر که از طریق شبکه از سرور استفاده میکنند، پشتیبانی کند. هسته قابلیت پشتیبانی از چند کاربر، چندوظیفگی است که به توانایی یک سیستم عامل برای اجرای بیش از یک برنامه (وظیفه یا پردازه) در آن واحد اطلاق میشود.

با اینکه در حالت چندوظیفگی بنظر میرسد که دو یا چند برنامه بطور همزمان اجرا میشوند، ولی در واقع، کامپیوتری با یک پردازنده، فقط میتواند یک برنامه را در آن واحد اجرا کند. سیستم عامل، پردازنده را از یک برنامه به برنامه دیگر منتقل میکند تا بنظر برسد که چندین برنامه بطور همزمان در حال اجرا میباشد. (اگر کامپیوتری دارای بیش از یک پردازنده باشد، سیستم عامل میتواند به کمک هر پردازنده یک برنامه را اجرا کند و برنامه ها واقعاً بطور همزمان اجرا میشوند که به این عمل چندپردازگی میگویند).

برای دیدن عملیات چندوظیفگی در ویندوز کافی است ترکیب کلیدهای Ctrl+Alt+Del را فشار دهید تا پنجره ای بنام مدیر وظایف (Task Manager) بالا بیاید. در این پنجره با ورود به قسمت Processes، میتوانید تمام کارهایی را که هم اکنون کامپیوتر در حال انجام آنهاست، ببینید.

برای اینکه بطور مطمئن از قابلیت چند وظیفگی استفاده کنیم، سیستم عامل شبکه باید کاملاً برنامه های در حال اجرا را از یکدیگر جدا کند. درغیراینصورت یک برنامه میتواند عملی را انجام دهد که روی برنامه دیگر تاثیر گذارد باشد. سیستم عامل چندکاره این عمل را با اختصاص فضای آدرس به

@caffeinebookly caffeinebookly @caffeinebookly caffeinebookly t.me/caffeinebookly

هر کار انجام میدهد و بدین ترتیب، هیچ پردازه ای نمیتواند روی فضای حافظه پردازه دیگر تاثیرگذار باشد.

نکته فنی : در بسیاری از موارد، هر برنامه بصورت یک وظیفه منفرد اجرا میشود تا در فضای حافظه مختص خود کار کند. با این وجود، یک برنامه منفرد میتواند به چندین وظیفه تقسیم شود. این تکنیک معمولاً چندرشتگی (در دانشگاه چندنخی! یا چندریسمانی! گفته میشود) نامیده میشود و برنامه ها به وظایفی تقسیم میشوند که رشته (نخ یا ریسمان) نامیده میشوند.

نکته فنی : دو حالت از چندوظیفگی وجود دارد که انحصاری و غیرانحصاری نامیده میشود. در چندوظیفگی انحصاری، سیستم عامل تصمیم میگیرد که هر وظیفه چقدر باید اجرا شود و چه زمانی باید متوقف شده و پردازش به وظیفه بعدی منتقل شود. تقریباً تمام سیستم عامل های شبکه از این نوه چندوظیفگی استفاده میکنند.

چندوظیفگی غیرانحصاری نیز در نقطه مقابل قرار دارد. در این حالت، هر وظیفه که کنترل پردازنده را بدست بگیرد، میتواند اجرا شود تا زمانی که دستورالعملی در برنامه این کنترل را از برنامه گرفته و پردازنده را آزاد کند. بدین ترتیب بار زیادی روی سیستم عامل نخواهد بود و برنامه نویس باید در نوشتن برنامه دقت کند تا کنترل پردازنده را بطور کامل در اختیار نگیرد.

سرویسهای دایرکتوری

دایرکتوریها همه جا هستند. هنگامی که میخواهید یک تماس تلفنی برقرار کنید، شماره خود را از دفترچه تلفن پیدا میکنید. یا وقتی ر یک ساختمان چند طبقه دنبال اطاق میگردید، باید به راهنمای طبقات مراجعه کنید.

شبکه ها نیز دارای چنین دایرکتوریهایی میباشند. دایرکتوریهای شبکه اطلاعاتی در باره منابع موجود روی شبکه مانند کاربران، کامپیوترها، چاپگرها، پوشه های مشترک و فایلها را نگهداری میکنند. دایرکتوریها بخش اساسی هر سیستم عامل شبکه میباشند.

در سیستمهای شبکه قدیمی، مانند ویندوز NT 3.1 و NetWare 3.x، هر کامپیوتر سرور بانک اطلاعاتی دایرکتوری منابع خود را که فقط روی آن سرور قرار دارد، نگهداری میکند. مشکل این است که سرپرست شبکه باید هر بانک اطلاعاتی دایرکتوری را بطور مجزا نگهداری کند. این کار برای شبکه هایی با چند سرور بد نیست، ولی نگهداری دایرکتوری روی شبکه ای با چند ده و حتی چند صد سرور تقریباً غیرممکن است.

بعلاوه، سرویسهای دایرکتوری قدیمی براساس کاربرد بودند. برای مثال، یک سرور باید یک بانک اطلاعاتی دایرکتوری برای ورود کاربران، یکی برای اشتراک فایل و یکی دیگر برای آدرس های ایمیل داشته باشد. هر دایرکتوری دارای ابزار افزایش، ارتقا و حذف ورودی ها مختص خود است.

@caffeinebookly caffeinebookly @caffeinebookly caffeinebookly t.me/caffeinebookly

نکته فنی : سیستم عامل های جدید شبکه، سرویسهای دایرکتوری عام ارائه میکنند که اطلاعات دایرکتوری کل شبکه و کل برنامه های کاربردی را یکجا جمع میکند و بدین ترتیب میتواند بعنوان یک بانک اطلاعاتی کامل منفرد عمل کند. این سرویس های دایرکتوری براساس استانداردهای ISO بنام X.500 بنا شده اند. در دایرکتوری X.500، اطلاعات بطور سلسله مراتبی سازماندهی میشوند. برای مثال، یک شرکت چندملیتی میتواند دایرکتوری کاربران خود را به چند کشور تقسیم کند که هر کشور دارای مناطق کجزا، و هر منطقه نیز ادارات مجزای خود را داشته باشد.

سرویسهای امنیتی

تمام سیستم عاملهای شبکه باید میزانی از امنیت را برای محافظت از شبکه در مقابل دسترسی غیرمجاز داشته باشند. امروزه هک کردن، تبدیل به یک وقت گذرانی بین المللی شده است. با افزایش شبکه های متصل به اینترنت، هر کسی میتواند در هرجای جهان برای هک کردن این شبکه ها اقدام کند.

اساسی ترین نوع امنیت توسط حسابهای کاربری کنترل میشود که به کاربران مختلف، اجازه دسترسی به منابع شبکه را میدهد. حسابهای کاربری توسط کلمات عبور ایمن میشوند. پس یک رمز عبور مناسب زیربنای یک سیستم امنیتی مناسب است. بسیاری از سیستم عامل های شبکه به شما این امکان را میدهند که سیاست های مختلف رمزگذاری مانند تعیین حداقل طول کلمه رمز یا ترکیبی بودن حروف و اعداد در رمز را داشته باشید. بعلاوه، رمز های عبور میتوانند پس از تعداد روز های مشخصی نامعتبر شوند و کاربر مجبور خواهد بود بطور مرتب رمز خود را عوض کند.

بسیاری از سیستم عامل های شبکه کدگذاری داده ها را نیز ممکن میسازند که داده ها را قبل از ارسال روی شبکه کدگذاری میکند و بطور دیجیتال آنرا تایید میکند و هنگامی که فایل به مقصد رسید، با اطمینان از مقصد درست و کاربر مجاز، عملیات رمزگشایی انجام میشود.

سیستم عامل های سرور مایکروسافت

مایکروسافت در حال حاضر سه نسخه از سیستم عاملهای قدرتمند شبکه خود را پشتیبانی میکند : Windows NT Server 4، Windows 2000 Server و Windows 2003 Server. ویندوز ۲۰۰۳، آخرین نسخه میباشد. چون ویندوز ۲۰۰۳ جدید است، بسیاری از کاربران هنوز از آن استفاده نمیکنند. پس ویندوز ۲۰۰۰ هنوز بطور معمول مورد استفاده قرار میگیرد. چون مایکروسافت هنوز هم پشتیبانی محدودی از ویندوز NT سرور دارد، بنابراین بسیاری از شبکه های قدیمی هنوز هم از این ویندوز استفاده میکنند.

@caffeinebookly caffeinebookly @caffeinebookly caffeinebookly t.me/caffeinebookly

ویندوز NT سرور ٤

ویندوز NT سرور آخرین ویندوز از سری ویندوزهای NT است که اختصار عبارت New Technology را در نام خود دارد. تکنولوژی جدید که زمانی در ویندوز NT همه را حیرت زده کرد، پردازش ۳۲ بیتی آن بود که گامی بزرگ محسوب میشد. ویندوز NT اولین سیستم عامل مایکروسافت بود که آنقدر مطمئن بود که بعنوان سرویس دهنده شبکه مورد استفاده قرار گیرد. نسخه ۴ در جولای ۱۹۹۶ وارد بازار شد و اکنون بیش از ۹ سال سن دارد. این مدت در دنیای سیستم عامل ها، یک عمر کامل محسوب میشود.

قطعاً مهمترین قابلیت ویندوز NT مدل دایرکتوری آن بود که بر اساس مفهوم دامنه بنا نهاده شده بود. یک دامنه به گروهی از کامپیوترها اطلاق میشود که توسط یک دیتابیس دایرکتوری منفرد مدیریت میشوند. برای دسترسی به منابع مشترک درون یک دامنه، باید یک حساب کاربری معتبر درون آن دامنه داشته باشید و دسترسی به منابعی که به آنها نیاز دارید، به شما داده شود. سیستم دامنه از نامها ۱۵ کاراکتری NetBIOS برای دسترسی به تک تک کامپیوترهای روی دامنه و نامگذاری خود دامنه استفاده میکند.

خلاصه ای از سایر قابلیت های ویندوز NT بشرح زیر است:

- رسماً، مایکروسافت اعلام کرد که ویندوز NT سرور روی هر پردازنده ۴۸۶ با حداقل ۱۶ مگابایت حافظه اجرا میشود. ولی من هرگز آنرا روی سیستمی زیر پنتیوم ۲۰۰ مگاهرتز با حافظه ۶۴ مگابایت امتحان نکردم. البته امروزه، پنتیوم ۲۰۰ مگاهرتزی با ۶۴ مگابایت رم بعنوان جایزه از بسته های چیپس خارج میشود.
- ویندوز NT 4 از همان رابط کاربری استفاده میکرد که برای ویندوز ۹۵ طراحی شده بود. در واقع، تفاوت اصلی بین NT 4 و جدش ویندوز NT 3.51 رابط کاربری جدیدش بود.
- برخی از محدودیت های سیستم فایل :
  - حداکثر تعداد کاربران : نامحدود
  - تعداد دیسک ولوم ها : ۲۵
  - حداکثر اندازه ولوم : ۱۷۰۰۰ گیگابایت
  - حداکثر فضای هارد دیسک برای سرور : ۴۰۸۰۰۰ گیگابایت
  - بزرگترین فایل : ۱۷ میلیون گیگابایت
  - حداکثر رم قابل پشتیبانی : ۴ گیگابایت
  - حداکثر تعداد فایلهای باز : نامحدود

@caffeinebookly caffeinebookly @caffeinebookly caffeinebookly t.me/caffeinebookly

- مایکروسافت بطور رسمی مراحل خروج از رده ویندوز NT 4 را در سال ۲۰۰۲ آغاز کرد. چند تاریخ مهم برای ویندوز NT :
  - اول جولای ۲۰۰۳ : ویندوز NT از این تاریخ به بعد برای سازندگان سیستم قابل دسترسی نبود.
  - اول ژانویه ۲۰۰۴ : مایکروسافت وصله های غیرامنیتی را منتشر نکرد. انتشار وصله های امنیتی با مشاهده ایرادات امنیتی ادامه پیدا کرد.
  - اول ژانویه ۲۰۰۵ : مایکروسافت وصله های امنیتی را نیز منتشر نکرد.

ویندوز ۲۰۰۰ سرور

این نسخه از سیستم عامل ویندوز جدیدتر است و محبوب ترین سیستم عامل سرور مایکروسافت میباشد. ویندوز ۲۰۰۰ سرور بر اساس قدرت ویندوز NT 4 بنا نهاده شده و امکانات جدیدی به آن اضافه شده است که آنرا سریعتر، ساده تر، مطمئن تر و مدیریت پذیر تر کرده است.

درخشان ترین قابلیت جدید ویندوز ۲۰۰۰ سرور، Active Directory است که یک دایرکتوری منفرد برای تمام منابع شبکه فراهم میکند و به برنامه نویسان این امکان را میدهد تا از این دایرکتوری در برنامه های خود استفاده کنند. Active Directory نام های دامنه ۱۵ کاراکتری را بصورت نامهای دامنه مانند اینترنت مانند Marketing.MyCompany.com ساده میکند.

ویندوز ۲۰۰۰ سرور دارای سه نسخه است :

- **Windows 2000 Server** : که سرور ابتدایی است و برای شبکه های کوچک و متوسط ساخته شده است. این نسخه دارای تمام امکانات ابتدایی سرور مانند اشتراک فایل و چاپگر میباشد و میتواند بعنوان سرور وب یا ایمیل مورد استفاده قرار گیرد.
- **Windows 2000 Advanced Server** : این نسخه یک گام بالاتر است و میتواند تا ۸ گیگابایت رم را مدیریت کند و از چهار پردازنده نیز پشتیبانی میکند.
- **Windows 2000 Datacenter Server** : سرورهایی را که تا ۳۲ پردازنده دارند پشتیبانی میکند و میتواند تا ۶۴ گیگابایت رم را مدیریت کند و مخصوص کاربردهای بزرگ بانک اطلاعاتی طراحی شده است.

برای شبکه های کوچک با ۵۰ کامپیوتر یا کمتر، مایکروسافت بسته ای بنام Small Business Server ارائه کرده است که تمام اجزای مورد نیاز را به قیمتی بسیار بسیار پایین (برای کسانی که قانون حق تالیف را رعایت میکنند) ارائه میکند :

- **Windows Server 2000** : سیستم عاملی که برای سرور شبکه شما بکار میرود.
- **Exchange Server 2000** : برای سرور ایمیل و پیام فوری

@caffeinebookly caffeinebookly @caffeinebookly caffeinebookly t.me/caffeinebookly

- **ISA Server 2000** : سرور امنیت و شتابدهی اینترنت که امنیت بهینه و بازدهی بالایی را برای کاربردهای وب شما به ارمغان می آورد.
- **SQL Server 2000** : که سرویس دهنده بانک اطلاعاتی است.
- **FrontPage 2000** : برای ساخت وب سایت.
- **Outlook 2000** : برای خواندن ایمیل.

قیمت گذاری ویندوز ۲۰۰۰ سرور بر اساس تعداد کلاینتی است که از هر سرور استفاده میکند. هر سرور باید دارای یک مجوز سرور و تعداد مطلوب مجوزکلاینت باشد. وقتی ویندوز ۲۰۰۰ سرور را خریداری میکنید، یک مجوز سرور و ۵، ۱۰ یا ۲۵ مجوز کلاینت میگیرید. میتوانید مجوزهای اضافی برای کلاینت ها را هربار به تعداد ۵ یا ۲۰ مجوز خریداری کنید. جدول زیر قیمت انواع مختلف ویندوز ۲۰۰۰ سرور را با مجوزهای لازم نشان میدهد :

محصول	قیمت
Win2K Server + 5Clinet	$999
Win2K Server + 10Client	$1199
Win2K Server + 25Client	$1799
Win2K Adv. Ser. + 25Client	$3999
5 Client License Pack	$199
20 Client Licence Pack	$799

ویندوز ۲۰۰۳ سرور

سیستم عامل جدید، Windows 2003 Server نام دارد. آنقدر از زمان انتشار این سیستم عامل گذشته است که دیگر شبکه های جدید از آن استفاده میکنند. ویندوز ۲۰۰۳ بر اساس ویندوز ۲۰۰۰ بنا نهاده شده است که امکانات زیر به آن افزوده شده اند :

- نسخه جدید و بهینه ای از Active Directory با امنیت بالاتر، رابط کاربر ساده تر و بازدهی بیشتر.
- یک رابط مدیریت سیستم بهتر و ساده تر که Manage My Server نامیده میشود. برای کسانی که دوست دارند سرور خود را از طریق خط فرمان پیکربندی کنند، ابزارهای جامع خط فرمان درنظر گرفته شده است. کنسول مدیریتی مایکروسافت نیز به قوت خود باقی است.
- تغییری اساسی در رابط برنامه نویسی کاربردی ایجاد شده است که بنام چارچوب .NET شناخته میشود.
- کلاسترهای کامپیوتر بیشتری پشتیبانی میشوند. کلاستر، مجموعه ای از کامپیوترها است که همراه هم طوری کار میکنند که بصورت یک سرور واحد بنظر میرسند. ویندوز ۲۰۰۰ سرور نسخه Datacenter و بقیه نسخه ها از ۴ کلاستر پشتیبانی میکنند.

@caffeinebookly caffeinebookly @caffeinebookly caffeinebookly t.me/caffeinebookly

- سیستم فایل توزیعی پیشرفته ای وجود دارد که به شما این امکان را میدهد تا درایوهای روی چند سرور را بصورت یک ولوم مشترک در آورید.
- از SAN پشتیبانی میکند.
- دارای یک دیواره آتش اینترنت داخلی است که ارتباط اینترنت را ایمن میکند.
- نسخه جدیدی از سرویس دهنده مایکروسافت، بنام سرویس های اطلاعاتی اینترنت (IIS) نسخه ۶ را به همراه دارد.

این ویندوز نیز مانند اجدادش، در چند نسخه ارائه میشود که من چهار نسخه تخصصی را معرفی میکنم:

- **Windows Server 2003, Standard Edition** : این نسخه، نسخه ابتدایی ویندوز ۲۰۰۳ است. اگر از ویندوز ۲۰۰۳ بعنوان سرور فایل استفاده میکنید، یا سایر کاربردهای ابتدایی را از سرور میخواهید، این نسخه مناسب شماست. در این نسخه ۴ پردازنده و حداکثر ۴ گیگابایت رم پشتیبانی میشود.
- **Windows Server 2003, Web Edition** : این نسخه از ویندوز ۲۰۰۳ برای سرویس دهنده های وب تنظیم شده است.
- **Windows Server 2003, Enterprise Edition** : برای شبکه های بزرگتر طراحی شده است و میتواند تا ۸ پردازنده و ۳۲ گیگابایت رم، کلاسترهای سرور را پشتیبانی کند و دارای امکانات پیشرفته ای جهت ارتقای بازدهی و اطمینان میباشد.
- **Windows Server 2003, Datacenter Edition** : قدرتمند ترین نسخه ویندوز ۲۰۰۳ است که برای سرورهایی با ۶۴ پردازنده، ۶۴ گیگابایت رم، کلاسترهای سرور طراحی شده است و دارای امکانات پیشرفته ای مانند مقاومت در برابر خطا میباشد و برقراری دائم سرور را تضمین میکند.

قیمت این ویندوز نیز تقریباً مشابه ویندوز ۲۰۰۰ میباشد.

Novell NetWare

NetWare یکی از محبوب ترین سیستم عاملهای شبکه است که مخصوصاً برای شبکه های بزرگ مورد استفاده قرار میگیرد. NetWare دارای درصد اطمینان بسیار بالایی میباشد. در واقع، برخی از سرپرستان شبکه اذعان میکنند که NetWare سالیان سال روی شبکه آنها کار کرده است، بدون اینکه نیاز به یک بار راه اندازی مجدد داشته باشد.

@caffeinebookly caffeinebookly @caffeinebookly caffeinebookly t.me/caffeinebookly

نسخه های NetWare

NetWare اولین نسخه خود را در ۱۹۸۳ ارائه کرد. دو سال قبل از اولین نسخه ویندوز مایکروسافت و چهار سال قبل از ارائه اولین سیستم عامل شبکه مایکروسافت. در طول سالها، NetWare نسخه های بسیاری را پشت سر گذاشت. نسخه هایی که هنوز هم ممکن است آنها را در حال استفاده در شبکه های موجود ببینید :

- Netware نسخه 3.x، نسخه ای بود که NetWare را معروف کرد. NetWare 3.x از یک سیستم دایرکتوری بنام Bindery استفاده میکرد که امروزه دیگر از دور استفاده خارج شده است. هر سرور NetWare 3.x دارای یک فایل Bindery بودند که حای اطلاعاتی در مورد منابع روی آن سرور خاص بود. با Bindery، شما می بایست بطور مجزا وارد هر سرور میشدید تا از منابع دلخواه خود روی آن استفاده کنید.
- NetWare 4.x نسخه ای بود که در آن سرویس دایرکتوری NetWare (NDS) جایگزین Bindery شد. NDS مشابه Active Directory است. این سیستم به جای ایجاد دایرکتوری برای هر سرور، یک دایرکتوری برای کل شبکه ایجاد میکند.
- NetWare 5.x قدم بعدی بود. در این نسخه یک رابط کاربر جدید طراحی شده با جاوا ارائه شد که سرپرستی را بسیار ساده تر میکرد. پروتکلهای اینترنت بهینه و چندپردازندگی تا ۳۲ پردازنده و بسیاری از امکانات دیگر در این نسخه ارائه شد.
- NetWare 6.0 طیفی از امکانات جدید ارائه کرد. سیستم جدید مدیریت دیسک بنام سرویس ذخیره سازی ناول (NSS)، دسترسی به پوشه ها و چاپگر شبکه از طریق وب و پشتیبانی از سیستم فایلهای ویندوز، لینوکس، یونیکس و مکینتاش به آن اضافه شد.
- ناول آخرین نسخه NetWare را در تابستان ۲۰۰۳ با شماره نسخه ۶/۵ منتشر کرد.

NetWare 6.5

جدیدترین نسخه از NetWare، نسخه ۶/۵ است که بر اساس نسخه قبلی بنا نهاده شده است و چند قابلیت جدید بشرح زیر به آن اضافه شده است:

- بهینه سازی ابزارهای مدیریتی براساس کاوشگر
- اجزای Open Source داخلی مانند وب سرور Apache، مدیری بانک اطلاعاتی MySql و Tomcat و PHP برای کاربرد های پویای وب.
- قابلیت Virtual Office که به کاربران این امکان را میدهد تا به ایمیلها، فایلها و سایر منابع شبکه از هر کامپیوتر دارای کاوشگر دسترسی پیدا کنند.
- Nterprise Branch Office، قابلیتی است که به شما امکان میدهد تا یک سرور راه دور را با شبکه مرکزی خود از طریق اینترنت اتصال دهید.

@caffeinebookly caffeinebookly @caffeinebookly caffeinebookly t.me/caffeinebookly

برخلاف ویندوز، قیمت گذاری NetWare بر اساس تعداد کلاینت های مورد پشتیبانی سرور است. ناول برای مجوز سرور، هزینه ای دریافت نمیکند. قیمت این سیستم با ۵ کلاینت ۹۹۵ دلار، با ۱۰ کلاینت ۱۸۴۰ دلار، با ۲۵ کلاینت ۴۶۰۰ دلار و با ۵۰ کلاینت ۹۲۰۰ دلار میباشد که هزینه ارتقا از نسخه های قبلی به نسخه جدید، تقریباً نصف میزان یاد شده است.

سایر سیستم عاملهای سرور

با اینکه NetWare و ویندوز NT/2000 سرور بسیار محبوب میباشند، ولی تنها گزینه های موجود نیستند. علاوه بر اینها، دو گزینه دیگر یعنی Linux و Machintosh OS/X Server را در اختیار داریم.

لینوکس

شاید جالبترین سیستم عامل موجود لینوکس باشد. لینوکس یک سیستم عامل رایگان است که بر اساس یونیکس ، یک سیستم عامل شبکه قدرتمند که در شبکه های بسیار بزرگ استفاده میشود، بنا شده است. لینوکس توسط فردی بنام لینوس تروالز متولد شد. او این کار را در اوقات فراغت خود انجام میداد و نتایج کار خود را با برنامه نویسان داوطلب از سراسر جهان به اشتراک میگذاشت و آنان نیز کدهای خود را به پروژه لینوکس اضافه میکردند.

لینوکس دارای همان مزایای شبکه بندی یونیکس است و میتواند گزینه ای عالی بعنوان سیستم عامل سرور باشد.

Apple Mac OS/X Server

تمام سیستم عاملهای سروری که قبلاً تشریح کردم، روی سیستمهای براساس اینتل با پردازنده های سازگار با پنتیوم کار میکردند. ولی کامپیوترهای مکینتاش نیز به شبکه نیاز دارند. اپل یک سیستم عامل مخصوص سرور بنام Mac OS/X Server ارائه نموده است. این سیستم عامل تمام امکاناتی را که شما از سیستم عامل سرور انتظار دارید در خود جای داده است.

شبکه بندی نظیر به نظیر در ویندوز

اگر نمیخواهید درگیر پیچیدگی سیستم عاملهای شبکه شوید، باید شبکه بندی ساده نظیر به نظیر را از طریق ویندوز امتحان کنید.

@caffeinebookly caffeinebookly @caffeinebookly caffeinebookly t.me/caffeinebookly

مزایای شبکه های نظیر به نظیر

مهمترین مزیت شبکه نظیر به نظیر این است که نصب و استفاده از آن بسیار ساده تر از سرور اختصاصی است. شبکه های نظیر به نظیر بر اساس قابلیت های سرور محدود موجود در ویندوز، مانند توانایی اشتراک فایلها و چاپگرها کار میکنند. نسخه های اخیر ویندوز، مانند ویندوز XP، با برنامه شبکه بندی خاصی ارائه میشوند که بطور اتوماتیک شبکه ای ساده را پیکربندی میکند و شما نیازی به پیکربندی و تنظیم شبکه بطور دستی نخواهید داشت.

مزیت دیگر شبکه های P2P، ارزان قیمت تر بودن آنها نسبت به شبکه های براساس سرور است. چند علت برای ارزان بودن P2P از این قرار است :

- در شبکه نظیر به نظیر نیازی به استفاده از یک کامپیوتر مجزا بعنوان سرور وجود ندارد. هر کامپیوتری روی شبکه میتواند هم بعنوان سرور شبکه عمل کند و هم بعنوان ایستگاه کاری کاربر.
- نصب و استفاده از شبکه های نظیر به نظیر بسیار ساده است یعنی شما نیازی به صرف وقت بیشتر برای یادگیری مفاهیم پیچیده تر شبکه برای راه اندازی و نگهداری شبکه خود نخواهید داشت.
- هزینه خود سیستم عامل شبکه نیز باید در نظر گرفته شود. ویندوز ۲۰۰۰ سرور و NetWare هردو میتوانند در قبال هر کاربر هزینه ای معادل ۲۰۰ دلار داشته باشند. هزینه کل نیز با رشد شبکه بالاتر میرود. در شبکه بندی P2P شما فقط بابت ویندوز هزینه میکنید. دیگر نیازی نیست بابت هر کاربر که به شبکه اضافه میشود، هزینه اضافی بپردازید.

معایب شبکه های نظیر به نظیر

با اینکه نصب و استفاده از شبه های نظیر به نظیر بسیار ساده تر است، ولی معایبی نیز دارد :

- چون شبکه های P2P بر اساس ویندوز میباشند، پس تحت محدودیت های موروثی ویندوز قرار خواهند گرفت. ویندوز در اصل برای یک کاربر منفرد طراحی شده است، پس نمیتواند سرور فایل و چاپگر را بخوبی مدیریت کند.
- اگر سرور اختصاصی شبکه نصب نکنید، برخی از کاربران شاید نخواهند منابع خود را روی شبکه به اشتراک بگذارند. با NetWare و Windows Server، کامپیوترهای سرور برای کار شبکه اختصاص داده میشوند و هیچ کاربری شکایتی نخواهد داشت.
- با اینکه شبکه P2P در شبکه های کوچک هزینه کمتری دارد، ولی با بزرگ شدن شبکه، تفاوت قیمت میان این شبکه و شبکه ای با سرور اختصاصی کمرنگ تر میشود.
- شبکه های P2P با رشد شبکه، قابلیت های کاری خود را از دست میدهند. سرورهای P2P قابلیت های بازدهی و امنیت سرورهای اختصاصی را نخواهند داشت.

@caffeinebookly caffeinebookly @caffeinebookly caffeinebookly t.me/caffeinebookly

ویندوز XP

نسخه فعلی ویندوز مایکروسافت برای کاربردهای Desktop، ویندوز XP است که دارای قابلیتهای قدرتمند P2P میباشد. ویندوز XP به دو صورت ارائه میشود : نسخه خانگی و نسخه حرفه ای. بطوریکه از نام نیز مشخص است، نسخه خانگی برای کاربران خانگی و استفاده های ساده خانگی مناسب است. در این نسخه قابلیت های چندرسانه ای عالی مانند ویرایشگر فیلم خانگی بنام Movie Maker و پشتیبانی داخلی از رایترها، اسکنرها، دوربین های ویدئویی و بسیاری قابلیت های دیگر گنجانده شده است. نسخه حرفه ای ویندوز برای کاربرانی طراحی شده است که نیاز بیشتری به شبکه دارند.

تمام قابلیت های شبکه ویندوز XP، بر اساس TCP/IP است. NetBIOS فقط زمانی مورد نیاز است که کلاینت ویندوز XP بخواهد با کامپیوترهای ویندوز قدیمی تر که TCP/IP را پشتیبانی نمیکنند، ارتباط برقرار کند.

ویندوز XP امکانات شبکه زیر را فراهم میکند :

- اشتراک فایل و چاپگر داخلی که به شما امکان اشتراک فایلها و چاپگر ها را روی شبکه میدهد.
- ساحره نصب شبکه که بطور اتوماتیک بسیاری از تنظیمات شبکه را انجام میدهد.
- قابلیت اشتراک ارتباط اینترنت که به کامپیوتر XP این امکان را میدهد تا ارتباط اینترنت خود را با سایر کاربران به اشتراک بگذارد. این قابلیت همراه با دیواره آتش، شبکه را از دسترسی غیرمجاز از طریق ارتباط اینترنت محافظت میکند.
- یک فایروال داخلی برای محافظت از کامپیوتر هنگامی که به اینترنت متصل است.
- ابزار مدیریت حساب های کاربری ساده که به شما امکان ایجاد چندین کاربر و اختصاص رمز به آنها را میدهد.
- قابلیت بریج که به شما این امکان را میدهد تا از طریق سیستم ویندوز XP، دو شبکه را به هم پل کنید. در این حالت کامپیوتر باید دارای دو کارت شبکه باشد.
- ابزارهای پیشرفته بررسی و ایرادزدایی شبکه که سرعت شما را در یافتن و اصلاح مشکلات شبکه بالا میبرد.

نسخه های قدیمی ویندوز

نسخه های قبلی ویندوز نیز دارای قابلیت شبکه P2P بودند. لیست زیر خلاصه ای از امکانات این ویندوز ها را ارائه میکند :

@caffeinebookly caffeinebookly @caffeinebookly caffeinebookly t.me/caffeinebookly

- Windows Me : این ویندوز برای کاربران خانگی طراحی شده بود. این سیستم عامل دارای ساحره شبکه بندی برای ساده تر کردن پیکربندی شبکه بود. آخرین نسخه از ویندوز بود که تحت سیستم عامل ۱۶ بیتی داس کار میکرد.
- Windows 2000 Professional : نسخه رومیزی ویندوز ۲۰۰۰ سرور است. امکانات P2P قدرتمندی دارد ولی نصب آنها نسبت به ویندوز XP کمی سخت تر است. این نسخه اولین نسخه از ویندوز رومیزی بود که با Active Directory همخوانی خوبی داشت.
- ویندوز ۹۸ و نسخه دوم آن : این ویندوز محبوب ترین ویندوز بعد از ویندوز ۹۵ بود که امکانات شبکه ویندوز ۹۵ را بهینه کرده بود.
- ویندوز ۹۵ : اولین نسخه ۳۲ بیتی ویندوز بود. البته هنوز بر اساس کد های ۱۶ بیتی سیستم عامل داس کار میکرد و بنابراین نسخه ۳۲ بیت کاملی نبود. در این ویندوز قابلیت های ساده شبکه P2P وجود داشت و درایورهای داخلی برای کارتهای شبکه معمول در آن تعبیه شده بود و قابلیت ساده اشتراک فایل و چاپگر را نیز دارا بود.
- Windows For Workgroup : اولین نسخه از ویندوز بود که شبکه را بدون نیاز به برنامه های جانبی پشتیبانی میکرد. عمل ساخت شبکه های براساس NetBIOS برای اشتراک فایل و چاپگر در آن ساده بود. ولی پشتیبانی بسیار ضعیفی از TCP/IP داشت.

یادداشت

@caffeinebookly caffeinebookly @caffeinebookly caffeinebookly t.me/caffeinebookly