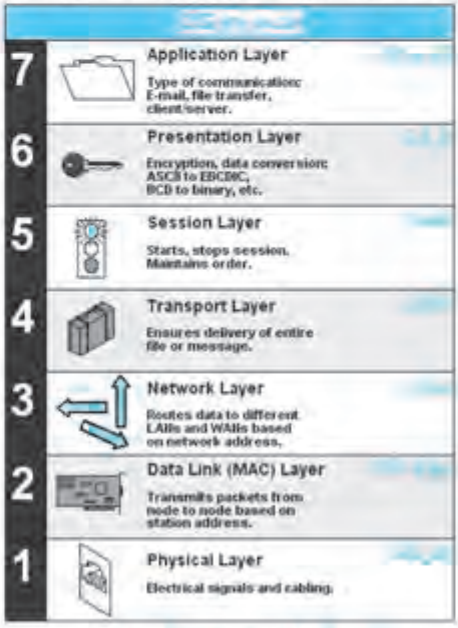
۵-۲ آشنایی با لایه‌های شبکه در مدل مرجع (OSI)

سازمان بین المللی استانداردها **International Organization for Standardization (IOS)** در سال ۱۹۸۳ میلادی اقدام به تهیه مدلی هفت لایه برای مشخص کردن کلیهٔ فعالیت‌های شبکه کرد که به مدل **Open System Interconnection (OSI)** معروف شده است. گرچه این مدل هیچ وقت پیاده سازی نشده است ولی بررسی فعالیت‌های شبکه با این مدل روند تبادل اطلاعات در شبکه را به خوبی نشان می‌دهد و درک سایر مدل‌های عملی امروزی مثل **TCP/IP** و مایکروسافت را آسان می‌کند. در این مدل کلیهٔ فعالیت‌های شبکه به هفت لایه تقسیم می‌شود که خصوصیات، سرویس‌ها و عملیات هر لایه مطابق با تعاریف استاندارد سازمان **IOS** می‌باشد.

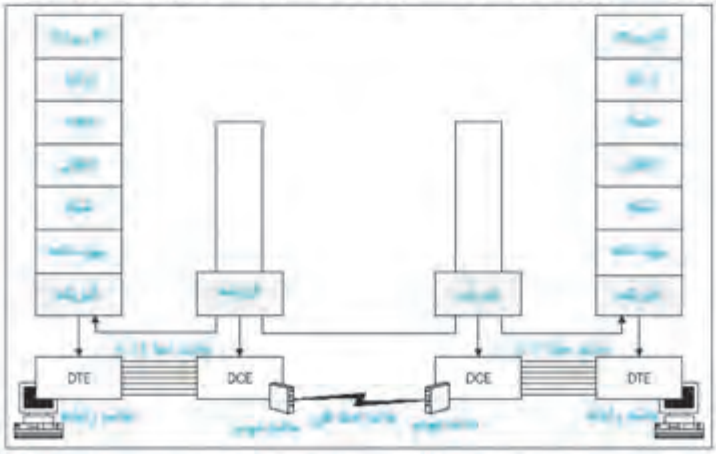
مدل **OSI** مشابه شکل (۲-۵) از هفت لایه تشکیل شده است. هر لایه دارای تعدادی پروتکل است. کار اصلی پروتکل‌های لایه‌های مختلف اضافه کردن **Header** و **Footer** مربوط به همان لایه به داده‌هایی است که قرار است در شبکه مبادله شوند. هر لایه در مدل **OSI** فقط با لایهٔ بالا و پایین خود ارتباط مستقیم دارد. برای برقراری ارتباط بین دو رایانه در شبکه لازم است پروتکل‌های هر لایهٔ مدل **OSI** در رایانه فرستنده و رایانه گیرنده وجود داشته باشد در اینصورت پروتکل‌های لایه‌های مختلف هر دو رایانه نظیر به نظیر با یکدیگر ارتباط منطقی دارند. زیرا داده‌ها در رایانه فرستنده لایه‌های مدل **OSI** را از بالا به پایین طی می‌کنند و در رایانه گیرنده این عمل از پایین به بالا صورت می‌پذیرد.



مثال ۱ وقتی یک برنامهٔ کاربردی می‌خواهد اطلاعاتی را به رایانه‌ای در شبکه ارسال نماید این اطلاعات به بسته‌های کوچکی به نام **Packet** تبدیل می‌شوند و به تدریج ارسال می‌شوند. هر بستهٔ اطلاعاتی از لایه بالایی **(Application)** به سمت پایین حرکت می‌کند و پروتکل‌های هر لایه به این بسته **Header** و **Footer** مربوط به همان لایه را اضافه می‌کند تا به لایه پایین **(Physical)** برسد. این لایه بستهٔ نهایی را به رایانه گیرنده ارسال می‌کند و در رایانه گیرنده این عملیات بطور معکوس انجام می‌شود. فرایند فوق از نظر عملیاتی مانند فرایند تهیه کردن نامه برای پست می‌باشد. بسته‌های اطلاعاتی که یک رایانه می‌خواهد ارسال کند را به خود نامه می‌توان تشبیه کرد که **Header** های پروتکل‌های لایه‌های مختلف مسئول قراردادن نامه در پاکت، نوشتن آدرس بر روی پاکت، الصاق تمبر بر پاکت و ارسال نامه می‌باشند.

۱-۳-۵ لایه فیزیکی (The Physical Layer)

پایین‌ترین لایهٔ شبکه است که مشابه شکل (۳-۵) مسئول برقراری اتصال فیزیکی بین دستگاههای پردازش داده‌های دیجیتال **(DTE)** و دستگاههای مخابراتی تطبیق دهندهٔ نوع داده‌ها با کانال انتقال **(DCE)**، ارتباطات از طریق آنها و سپس فعال کردن آنها است. به عبارت دیگر لایه فیزیکی سیگنالهای الکتریکی یا نوری استفاده شده برای ارتباط بین دو رایانه را توضیح می‌دهد و ماهیت عناصر سخت افزاری شبکه مانند نوع رسانهٔ شبکه و نحوهٔ نصب شبکه را مشخص می‌کند. در این لایه بسته‌های اطلاعاتی دریافت شده از لایهٔ پیوند داده‌ها به سیگنال مناسب تبدیل شده و از طریق کانال ارتباطی به فرستنده ارسال می‌شود و در سمت فرستنده به صورت برعکس سیگنال دریافت شده به صورت بسته‌های اطلاعاتی اولیه بازسازی شده و به لایهٔ انتقال داده تحویل داده می‌شود.



شکل ۳-۵ دستگاههای پردازش داده‌ها (DTE) و دستگاههای مخابراتی تطبیق دهنده داده‌ها یا کانال (DCE)

پروتکلهای لایه فیزیکی موارد زیر را مشخص می‌کنند :

- سیگنالهای الکتریکی (مثلاً ۱ ولت)
- شکل اتصال (مانند V.35)
- نوع رسانه انتقال (مثلاً کابل زوج به هم تابیده یا فیبر نوری)
- مدولاسیون (مثلاً FM یا PM)
- رمز گذاری
- همزمانی (مثلاً ارتباط همزمان یا ناهمزمان)
- دریافت بسته‌های اطلاعاتی از لایهٔ پیوند داده و ارسال آن بر روی رسانه شبکه بصورت سیگنال مناسب و انجام عملیات معکوس در رایانه گیرنده

۵-۳-۲ لایه پیوند داده (The Data Link Layer)

پروتکل لایهٔ پیوند داده رابط بین سخت افزار و نرم افزار شبکه است. در این لایه مطابق شکل (۴-۵) به ابتدا و انتهای بستهٔ دریافت شده از لایهٔ شبکه **Header** و **Footer** مخصوصی اضافه می‌شود تا فریم **(Frame)** لایه پیوند داده ایجاد شود سپس این فریم برای ارسال به لایهٔ فیزیکی تحویل داده می‌شود. در رایانهٔ گیرنده، لایهٔ پیوند داده عکس عمل بالا را انجام می‌دهد. در **Header** این فریم آدرس مبدا و مقصد و سایر اطلاعات کنترلی قرار دارد و در **Footer** این فریم مجموع اطلاعات در حال ارسال **(Checksum)** قرار دارد از روی **Checksum** می‌توان صحت اطلاعات دریافت شده را تعیین کرد.

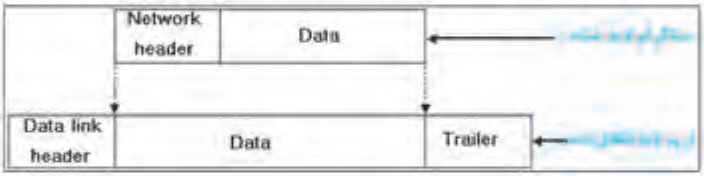
شکل ۴-۵ فریم تولید شده در لایه اتصال داده

مهمترین وظایف لایه پیوند داده عبارتند از :

- دریافت بسته اطلاعاتی از لایهٔ شبکه، ایجاد فریم از روی بستهٔ دریافت شده از لایهٔ شبکه و ارسال آن به لایه فیزیکی و انجام عملیات معکوس در رایانه گیرنده
- مشخص کردن پروتکل لایهٔ شبکه که داده‌های موجود در بسته را تولید کرده است.
- قراردادن اطلاعات مربوط به تشخیص خطا در فریم اطلاعاتی و کنترل صحت آن در رایانه گیرنده
- تعیین نحوهٔ دسترسی به رسانهٔ شبکه با توجه به مشخصات لایه فیزیکی
- در اختیار قراردادن آدرس فیزیکی کارت شبکه رایانه مقصد و مبداء

۵-۳-۲ لایه شبکه (The Network Layer)

پروتکل لایهٔ شبکه، انتقال داده‌ها را بین دو رایانهٔ دوردست درون شبکهٔ **WAN** تضمین می‌کند. سیستم‌های مبداء و مقصد می‌توانند در شبکهٔ **LAN** فعلی یا در شبکه‌ای با هزارها کیلومتر فاصله باشند. در لایهٔ شبکه مطابق شکل (۵-۵) به بستهٔ دریافت شده از لایهٔ انتقال، **Header** خاصی اضافه می‌شود به بسته ایجاد شده **Datagram** گفته می‌شود. هدر پروتکل لایهٔ شبکه مانند پروتکل لایهٔ پیوند داده، شامل آدرس مبداء و مقصد است با این تفاوت که آدرس هدر لایهٔ شبکه شامل آدرس مقصد نهایی است که ممکن است با آدرس مقصد هدر لایه پیوند داده متفاوت باشد زیرا ممکن است رایانه مقصد در شبکهٔ دیگری باشد. از آدرس مقصد هدر لایه شبکه برای مسیریابی در شبکه‌های **WAN** یا چند شبکه **LAN** مرتبط با هم استفاده می‌شود. یکی از وظایف دیگر این لایه قطعه بندی **(Fragmenting)** بسته‌ها است. بسته‌های لایه شبکه **(Datagram)** ممکن برای رسیدن به مقصد از شبکه‌های مختلفی که پروتکل‌های لایهٔ پیوند دادهٔ آنها متفاوت است عبور کند بنابراین لازم است بسته‌ها مطابق با پروتکل شبکه‌های مختلف به قطعات مناسب تبدیل شود.



مثال ۱ طول بسته‌های شبکه‌های **Token Ring**، ۴۵۰۰ بایت است اگر این بسته بخواهد به یک شبکهٔ اترنت منتقل شود باید پروتکل لایهٔ شبکه آن را به قطعات کوچکتر از ۱۵۰۰ بایت که اندازهٔ استاندارد بسته‌های شبکه‌های اترنت است تبدیل کند.

برای اتصال چند شبکهٔ **LAN** از تجهیزاتی به نام مسیریاب **(Router)** استفاده می‌شود مسیریاب‌ها در لایه شبکه کار می‌کنند زیرا آنها برای تبادل بسته‌ها بین دو شبکهٔ **LAN**، آدرس مقصد نهایی بسته را که در **Datagram** تولید شده در لایهٔ شبکه قرار دارد بررسی کرده و در صورتی که این آدرس مربوط به شبکه **LAN** بعدی باشد آن بسته را به آن شبکه عبور می‌دهد در غیر اینصورت از انتقال بسته به شبکهٔ بعدی جلوگیری می‌کند.

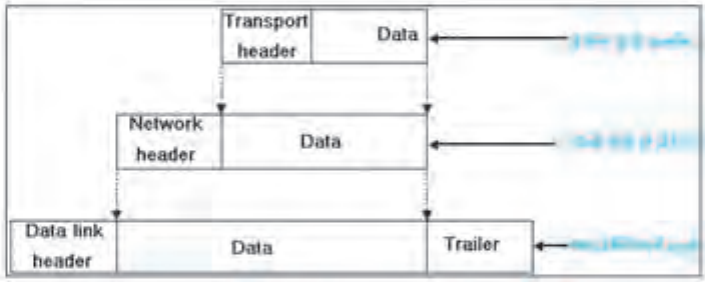
عبارتند از :

- **دریافت بسته اطلاعاتی از لایهٔ انتقال**
- **قطعه بندی بسته‌ها در صورت نیاز**

- ایجاد Datagram از روی بستهٔ دریافت شده از لایهٔ انتقال (افزودن آدرس مقصد نهایی برای مسیریابی)
- تعیین مسیر مناسب انتقال داده‌ها در مسیر یاب‌ها
- ارسال بسته تولید شده لایه پیوند داده و انجام عملیات معکوس در رایانه گیرنده
- مشخص کردن پروتکل لایهٔ انتقال

۴-۳-۵ لایه انتقال (The Transport Layer)

سرویس‌های لایه انتقال، مکمل سرویس‌های لایه شبکه است. دریافت داده‌ها از لایهٔ جلسه، شکست داده‌ها به واحدهای کوچکتر (درصورت نیاز)، انتقال داده‌ها به لایه شبکه، برقراری و قطع ارتباط و تنظیم سرعت ارسال داده‌ها بر اساس مشخصات گیرنده از وظایف مشخص شده برای این لایه است. مطابق این لایه نیز به داده‌های دریافت شده از لایه جلسه **Header** خاصی اضافه می‌کند به بستهٔ تولید شده توسط این لایه **Segment** نیز گفته می‌شود.



پروتکلهای لایه انتقال دو نوع هستند :

- اتصال گرا (Connection-Oriented)
- بی اتصال (Connection-Less)

پروتکل اتصال گرا، پروتکلی است که در آن دو رایانه قبل از انتقال اطلاعات، پیغام‌هایی را برای برقراری اتصال بین خود مبادله می‌کنند. در این حالت این تضمین وجود دارد که هر دو رایانه در حال کار بوده و آمادهٔ مبادله اطلاعات هستند. (مانند پروتکل **TCP**) این پروتکل‌ها سرویس‌های دیگری مانند قطعه‌بندی داده‌ها، کنترل جریان داده‌ها، تشخیص و تصحیح خطا و تایید دریافت بسته‌ها را ارائه می‌کنند. در پروتکل‌های اتصال گرا، برای انتقال هر بسته، از گیرنده پیغامی مبنی بر تحویل درست و بدون خطای آن دریافت می‌شود. بنابراین این پروتکل‌ها مطمئن هستند. پروتکل بی اتصال، پروتکلی است که در آن دو رایانه قبل از انتقال اطلاعات، هیچ پیغامی را برای برقراری اتصال بین خود مبادله

نمی‌کنند. در این حالت فرستنده بدون این که بداند گیرنده آمادهٔ دریافت بسته است یا وجود دارد، بسته را می‌فرستد. (مانند پروتکل **UDP**)

اشکال پروتکلهای اتصال گرا این است که طول بسته‌ها در آنها بیشتر از پروتکلهای بی‌اتصال است و سرعت انتقال داده‌ها در آنها پایین‌تر است.

[illegible] عبارتند از :

- **دریافت بسته اطلاعاتی از لایهٔ جلسه، ایجاد فریم از روی بستهٔ دریافت شده از لایهٔ جلسه و ارسال آن به لایه شبکه و انجام عملیات معکوس در رایانه گیرنده**
- **تضمین رسیدن بسته‌ها بدون خطا به مقصد**
- **کنترل جریان انتقال داده‌ها**

۵-۳-۵ لایه جلسه (The Session Layer)

هیچ پروتکل مخصوصی برای کار در این لایه وجود ندارد. وظایف این لایه توسط پروتکل‌های لایه‌های پایین‌تر انجام می‌شود. عملکرد اصلی این لایه تبادل پیغام بین دو رایانه‌ای است که می‌خواهند اطلاعات مبادله کنند به این تبادل پیغام محاوره **(Dialog)** گفته می‌شود. در این محاوره مشخص می‌شود که نحوهٔ ارتباط بین دو رایانه بصورت دوطرفهٔ همزمان یا دوطرفهٔ نوبتی باشد.

در حالت دوطرفهٔ نوبتی، دو رایانه بسته‌ای به نام **Token** را بین یکدیگر مبادله می‌کنند. رایانه‌ای که **Token** در اختیار اوست می‌تواند بسته‌هایش را ارسال نماید بدین ترتیب در این حالت تداخل **(Collision)** بوجود نمی‌آید. در حالت دوطرفهٔ همزمان، هر دو رایانه می‌توانند بطور هم زمان بسته‌هایشان را ارسال کنند.

[illegible] عبارتند از :

- **برقراری محاوره بین دو رایانه**
- **مشخص کردن نوع محاوره**

۵-۳-۶ لایه نمایش (The Presentation Layer)

ممکن است رایانه‌های متصل به یک شبکه از قواعد دستوری و گرامری متفاوتی استفاده کنند. لایهٔ نمایش توافق دو رایانه‌ای را که می‌خواهند در شبکه با یکدیگر ارتباط برقرار کنند بر سر استفاده از یک قاعده و گرامر انتقال مشترک که هر دو طرف آن را پشتیبانی می‌کنند، جلب می‌کند. با توجه به

نیازهای برنامه‌ها و ماهیت ارتباط بین دو سیستم، در طی عملیات انتقال داده‌ها بین دو رایانه ممکن است عملیات رمز گذاری داده‌ها، فشرده ساختن داده‌ها و یا فقط ترجمهٔ ساده صورت پذیرد.

[illegible] عبارتند از :

- **حصول توافق رایانه فرستنده و گیرنده در زمینهٔ استفاده از یک گرامر انتقال مشترک**
- **رمز گذاری و فشرده سازی داده‌ها در صورت نیاز**

۵-۳-۷ لایه کاربردی (The Application Layer)

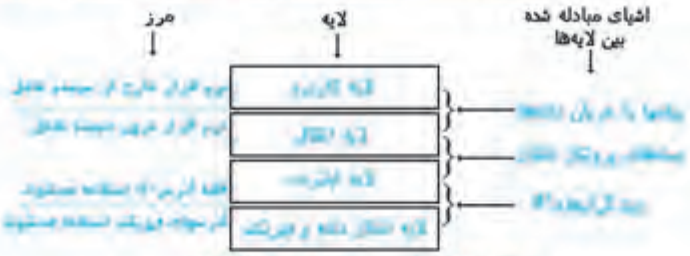
پروتکل لایهٔ کاربردی که بالاترین لایه در مدل **OSI** است، واسطه‌ای است بین برنامهٔ در حال اجرا بر روی رایانه‌ای که درخواست استفاده از منابع یا سرویس‌های شبکه دارد، با پشتهٔ پروتکل که آن تقاضا را به سیگنالهای قابل ارسال بر روی شبکه تبدیل می‌کند. بعضی از برنامه‌های کاربردی درخواست‌های خود را برای استفاده از شبکه به سیستم عامل شبکه می‌دهند تا سیستم عامل آنها را به لایه کاربردی ارائه نماید. برخی دیگر از برنامه‌ها بطور خاص برای دستیابی به منابع موجود در شبکه طراحی شده‌اند. برای این منظور از پروتکل‌هایی که در لایه کاربردی وجود دارند استفاده می‌نمایند.

[illegible] عبارت است از :

- **واسط بین برنامه‌های کاربردی نصب شده بر روی رایانه‌های متصل به شبکه، برای استفاده از منابع مختلف شبکه**

۵-۴ آشنایی با لایه‌های شبکه در مدل TCP/IP

عبارت **Transmission Control Protocol/Internet Protocol (TCP/IP)** مجموعه پروتکلی است که برای ارتباط و مسیر یابی ترافیک از طریق شبکه‌های متصل به هم و گاهی اوقات غیرمشابه با انجام تحقیقات بر روی شبکه‌های سوئیچینگ بسته‌ای و آرپانت ابداع شده است این مجموعه در سیستم یونیکس گنجانیده شده است و به استاندارد غیررسمی انتقال داده‌ها از طریق شبکه‌ها، از جمله اینترنت مبدل شده است. مدل مرجع **TCP/IP** که اغلب مدل مرجع اینترنت نیز نامیده می‌شود برای شبکه‌سازی بر اساس مفهوم تبادل اطلاعات بین شبکه‌های دارای معماریهای متفاوت طراحی شده است و از چهار لایه نسبتاً مستقل مطابق شکل (۷-۵) تشکیل شده است. به جزء موارد خاص خانواده پروتکلهای **TCP/IP** با لایه انتقال داده و فیزیکی سر و کار ندارند و در عمل پروتکلهای اینترنت در این لایه اغلب از استانداردهای تعبیه شده در پروتکلهای **OSI** استفاده می‌کنند. به **TCP/IP** پشتهٔ پروتکل نیز گفته می‌شود پروتکل‌های شبکه می‌توانند بسیار ساده یا کاملاً پیچیده باشند. به مجموعهٔ پروتکل‌های لایه‌های مختلف یک مدل (مانند **TCP/IP** یا **OSI**)، پشتهٔ پروتکل **(Protocol Stack)** می‌گویند.



[illegible]

لایه کاربرد برنامه‌های کاربردی را برای کار در شبکه فعال می‌کند و با پروتکلهای لایهٔ انتقال برای ارسال و دریافت داده‌ها تماس برقرار می‌کند هر برنامهٔ کاربردی خودش روش انتقال داده‌ها را مشخص می‌کند بسته به نوع برنامه کاربردی روش انتقال داده‌ها می‌تواند رشته‌ای از پیامهای مجزا یا جریانی از بایتها باشد. اولین وظیفه لایه انتقال برقراری ارتباط بین دو برنامه کاربردی در شبکه است. یکی از وظایف دیگر این لایه تنظیم جریان داده با توجه به سرعت دریافت رایانه یا وسیله دریافت کننده در مقصد است. لایه انتقال داده‌های چندین برنامه کاربردی یک رایانه را که در حال کار در شبکه است دریافت کرده و با کدگذاری مناسب آنها را برای ارسال به لایه اینترنت تحویل می‌دهد. لایه اینترنت بسته‌های موردنظر برای ارسال را از لایهٔ انتقال گرفته و پس از محصور کردن آنها در دیتاگرامهای خاص و افزودن آدرس گیرنده و فرستنده و اطلاعات مسیریابی آن را برای ارسال به لایهٔ انتقال داده و فیزیکی تحویل می‌دهد. لایه انتقال داده و فیزیکی که در برخی متون به اسامی دیگری مانند لایه واسط شبکه نیز خوانده می‌شود مسئول دریافت دیتاگرامهای **IP** (با **IP** در ادامه فصل آشنا می‌شویم) و ارسال آنها بر روی شبکهٔ مشخص است.

۵-۵ مقایسه مدل OSI و مدل TCP/IP

مطابق شکل (۸-۵) **TCP/IP** از چهار لایه و **OSI** از هفت لایه تشکیل شده است. سیستمهای **TCP/IP** و **OSI** گرچه در لایه‌های انتقال و شبکه خیلی مشابه هستند ولی اختلافهای قابل توجهی دارند. به استثنای برخی از پروتکلها، مدل **TCP/IP** با لایهٔ فیزیکی سر و کار چندانی ندارد و حتی در اینترنت ما از لایه فیزیکی و پیوند داده مدل **OSI** استفاده می‌کنیم. لایه اینترنت از مدل **TCP/IP** برای مسیریابی و کنترل ترافیک داده‌ها در بین شبکه‌های مختلف نظیر اینترنت استفاده می‌شود و در لایه **OSI** وجود ندارد. مدل **OSI** یک مدل مفهومی برای درک بهتر ارتباط بین رایانه‌ها در شبکه است و هیچگاه به صورت واقعی پیاده سازی نشده است لیکن مدل **TCP/IP** مدلی عملیاتی است که امروزه به

عنوان مدل مرجع اینترنت در نظر گرفته می‌شود و حتی در شبکه‌های غیر اینترنتی نیز به وفور مورد استفاده قرار می‌گیرد.

شکل ۸۱-۵ مقایسه لایه‌های مدل مرجع OSI و مدل TCP/IP

۵-۶ آشنایی با انواع پروتکلها

پروتکلهای بسیاری برای لایه‌های مختلف مدلهای **OSI** و **TCP/IP** تعریف شده‌اند که با برخی از مهمترین آنها در این فصل آشنا می‌شویم سایر پروتکلهای مورد نیاز در این کتاب در فصلهای بعدی معرفی خواهد شد.

۵-۶-۱ Internet Protocol (IP)

پروتکل اصلی لایه شبکه و اینترنت در مدلهای **OSI** و **TCP/IP** است در یک شبکه بزرگ متشکل از چندین شبکهٔ محلی، که از پشتهٔ پروتکل **TCP/IP** استفاده می‌کند، دو پروتکل زیر وجود دارد :

- **TCP**
- **IP**

پروتکل **TCP** وظیفه کنترل انتقال را بعهده دارد به نحوی که انتقال صحیح و سالم بسته تضمین شود. این پروتکل را در قسمت بعد بررسی خواهیم کرد. پروتکل **IP** وظیفهٔ انتقال داده از مبدا تا مقصد نهایی را بعهده دارد. پروتکل **IP** یک پروتکل بی اتصال **(Connection Less)** است و بدون برقراری ارتباط با گیرنده، اطلاعات را برای آن ارسال می‌کند.

وظایف لایهٔ پروتکل IP عبارتند از :

- **کپسوله کردن**

داده‌هایی را که از لایه انتقال به لایه شبکه ارسال می‌شود در بسته‌هایی به نام دیتاگرام بسته بندی می‌کند. در دیتاگرام مشخصاتی مانند آدرس **IP** رایانه گیرندهٔ نهایی و رایانه فرستنده قرار داده می‌شود.

- **آدرس دهی**

سیستم‌های شبکه را از طریق آدرس **IP** آنها شناسایی می‌کند. در پروتکل **IP** از روش آدرس دهی **IP** استفاده می‌شود. آدرس **IP** یک عدد ۳۲ بیتی است که بصورت چهار عدد دهدهی (از صفر تا ۲۵۵) نمایش داده می‌شود و دارای دو بخش است که بخش اول آن آدرس منحصر به فرد شبکه است **(Network ID)** و بخش بعدی آن آدرس منحصر به فرد رایانه موجود در شبکه است. **(Host ID)** . چون از آدرس **IP** برای شبکه‌های جهانی استفاده می‌شود لازم است منحصر به فرد باشد برای این منظور باید آدرس‌های مورد نیاز را در مراجع ذیصلاح ثبت کرد.

مثال : آدرس**IP** رایانه‌ای در شبکه‌ای که آدرس شبکه آن **192.168.94** است چنین است : 192.168.94.124

- **مسیر یابی**

مسیریاب‌های بین چند شبکه **LAN**، با خواندن آدرس **IP** رایانه مقصد نهایی، از دیتاگرام **IP**، می‌توانند تشخیص دهند که این بسته به کدام **LAN** منتقل شود.

- **قطعه بندی**

بسته‌های مبادله شده بین چند شبکه **LAN** که با پروتکل‌های متفاوت لایه پیونددداده، به هم متصل شده‌اند(مثلاً یک شبکه اترنت با شبکه**Token Ring**)، دارای اندازه‌های مختلفی است. (بسته‌های اترنت حداکثر ۱۵۰۰ بایت و بسته‌های **Token Ring** ۴۵۰۰ بایت) بنابراین پروتکل **IP** تبدیل این بسته‌ها را متناسب با پروتکل شبکهٔ مقصد انجام می‌دهد.

- **تشخیص پروتکل**

برای پردازش صحیح دیتاگرام‌های دریافت شده توسط یک رایانه، باید مشخص شود که این دیتاگرام با کدام پروتکل لایهٔ انتقال تولید شده است. این کار توسط فیلد دادهٔ دیتاگرام انجام می‌شود.

۵-۶-۲ Transmission Control Protocol (TCP)

پروتکل **TCP** یکی از پروتکل‌های پشتهٔ پروتکل **TCP/IP** است که در لایهٔ انتقال کار می‌کند. اکثر پروتکل‌های لایهٔ کاربردی با توجه به نیازی که دارند از این پروتکل برای تضمین انتقال اطلاعات در شبکه استفاده می‌کنند. این پروتکل یک پروتکل اتصال‌گرا است یعنی قبل از انتقال اطلاعات بین دو رایانه در شبکه، ابتدا ارتباطی را بین آنها برقرار می‌کند و این ارتباط در طول زمان تبادل اطلاعات، برقرار باقی می‌ماند. این ارتباط تضمین می‌کند که هر دو رایانه وجود دارند و برای تبادل اطلاعات آماده هستند. این پروتکل برای تضمین بسته‌های ارسال شده به مقصد، از رایانه مقصد تایید دریافت بسته‌ها را دریافت می‌کند این کار مشابه پست نامه‌ها با سرویس پست سفارشی دوقبضه است که رسید دریافت نامه را از تحویل گیرنده برای ارسال کننده نامه ارائه می‌کند. همچنین در صورت بروز خطا در بسته‌های ارسالی آن را تشخیص می‌دهد. یکی دیگر از وظایف این پروتکل تقسیم بسته‌های بزرگ به بسته‌های مناسب برای انتقال در رایانه فرستنده و عکس این عمل برای دریافت بسته‌ها در رایانه گیرنده است. این پروتکل بر جریان انتقال بسته‌های اطلاعاتی تحویل گرفته شده از لایهٔ کاربردی تا مقصد نظارت می‌کند. سرویس‌هایی از لایهٔ کاربردی که نیاز به ارتباط تضمین شده و تبادل اطلاعات بدون خطا یا اطلاعات زیاد دارند از این پروتکل استفاده می‌کنند. مانند سرویس **FTP** (برای انتقال فایل) و سرویس **SMTP** (برای ارسال نامه‌های الکترونیکی). یکی دیگر از پروتکلهای پشتهٔ **TCP/IP**، پروتکل **UDP** است که پروتکلی بی اتصال است یعنی قبل از انتقال اطلاعات بین دو رایانه در شبکه، ابتدا ارتباطی را بین آنها برقرار نمی‌کند و شروع به ارسال اطلاعات می‌کند. این پروتکل تاییدی برای تک‌تک بسته‌های ارسال شده به مقصد، از رایانه مقصد دریافت نمی‌کند. (گرچه این تایید را برای تمام بسته‌های ارسال شده در پایان کار یکجا می‌گیرد) همچنین در صورت بروزخطا در بسته‌های ارسالی آن را تشخیص می‌دهد. لذا این پروتکل انتقال اطلاعات را تضمین نمی‌کند اما بدلیل ارائه سرویس‌های کمتر نسبت به **TCP** ترافیک کمی دارد و برای تبادل اطلاعات کم کارایی بهتری دارد. سرویس‌هایی از لایهٔ کاربردی که اطلاعات کمی برای مبادله دارند از این پروتکل استفاده می‌کنند. (مانند سرویس **DNS** برای تحلیل نام رایانه میزبان و سرویس **DHCP** برای تخصیص آدرس **IP**)

۵-۶-۳ NetBIOS Enhanced User Interface (NetBEUI)

گرچه در ویندوزهای امروزی، پروتکل پیش فرض، **TCP/IP** است ولی در نسخه‌های قدیم آن مانند **Windows NT** و **Windows 98** از پروتکلی به نام **NetBEUI** استفاده می‌شود که هنوز هم توسط ویندوزهای جدید پشتیبانی می‌شود. پروتکل **NetBEUI** یک پروتکل بی اتصال است و برای شبکه‌های **LAN** کوچک طراحی شده است و در این شبکه‌ها کارایی خوبی دارد. این پروتکل قابلیت تطبیق و تنظیم خودکار خود را با شبکه دارد. این پروتکل قابلیت مسیر یابی ندارد و از روتر عبور نمی‌کند

بنابراین برای ارتباطات اینترنتی مناسب نیست. آدرس دهی کامپیوترها در این پروتکل با یک اسم به طول ۱۶ کاراکتر انجام می‌شود که این اسم همان نام کامپیوتر است که در هنگام نصب ویندوز تعیین می‌شود. این پروتکل آدرس کامپیوتر مقصد را حمل نمی‌کند و بسته‌های ارسالی را بر روی شبکه برای همهٔ کامپیوترها ارسال می‌کند که به آن **Broadcast** گفته می‌شود.

[illegible] عبارتند از :

- **پیکربندی خودکار**
- **عدم قابلیت مسیر یابی**
- **روش ارسال Broadcast**
- **بی اتصال**
- **کارایی خوب در شبکه‌های کوچک**

۴-۴-۵ Internetwork Packet Exchange (IPX)

تا سال ۱۹۹۸ شرکت **Novell** در سیستم عامل شبکهٔ خود که **Netware** نام دارد از پروتکل خاص خود به نام **IPX** استفاده می‌کرد. اما از آن سال به بعد این شرکت نیز از پشته پروتکل **TCP/IP** پشتیبانی می‌کند و پروتکل **IPX** در حال کنار رفتن است. **IPX** در لایه شبکه کار می‌کند و یک پروتکل بی‌اتصال است که مانند پروتکل **IP**، داده‌هایی را که توسط چندین پروتکل دیگر در شبکه ایجاد شده‌اند منتقل می‌کند. پروتکل **IPX** برای شبکه‌های محلی محدود طراحی شده و برای شناسایی رایانه‌ها از آدرس سخت افزاری کارت شبکهٔ هر رایانه استفاده می‌نماید لذا دارای آدرس دهی خاص خود نمی‌باشد. در این پروتکل برای شناسایی شبکه، لازم است در هنگام نصب سیستم عامل **Netware**، آدرس یگانه را به عنوان آدرس شبکه تعیین کرد، تا با استفاده از ترکیب آدرس سخت افزاری و آدرس یگانه شبکه بتوان در چند شبکه **LAN** مسیر یابی را انجام داد.

پروتکل **IPX** نیز به بسته‌های دریافتی از لایه انتقال هدر خاص خود را اضافه می‌کند که به آن دیتاگرام گفته می‌شود. در دیتاگرام برخی اطلاعات مانند آدرس سخت افزاری رایانه گیرنده و فرستنده و فیلد کنترل انتقال قرار دارد. فیلد کنترل انتقال دارای مقدار پیش فرض ۱۶ می‌باشد که با عبور دیتاگرام از یک مسیر یاب مقدار آن یک واحد کم می‌شود. بنا براین در شبکه‌های مبتنی بر **Netware** یک دیتاگرام نمی‌تواند بیشتر از حداکثر از ۱۶ مسیر یاب عبور نماید در صورتی که این عدد برای شبکه‌های مبتنی بر ویندوز ۱۲۸ است. تا قبل از سال ۱۹۹۸ که سیستم عامل نت ور از **TCP/IP** پشتیبانی کند، امکان به اشتراک گذاشتن فایل و چاپگر با پروتکلی غیر از **IPX/SPX** وجود نداشت. برای رفع این مشکل شرکت مایکروسافت در سیستم عامل شبکه ویندوز خود امکان تونل زنی **(Tunneling)** را پیش بینی کرد. در این روش بسته‌های **IPX** در داخل دیتاگرام‌های **IP** قرار گرفته و حمل می‌شوند. مایکروسافت **NWLink** را برای پشتیبانی از پروتکل **IPX/SPX** در ویندوز در نظر گرفته است.

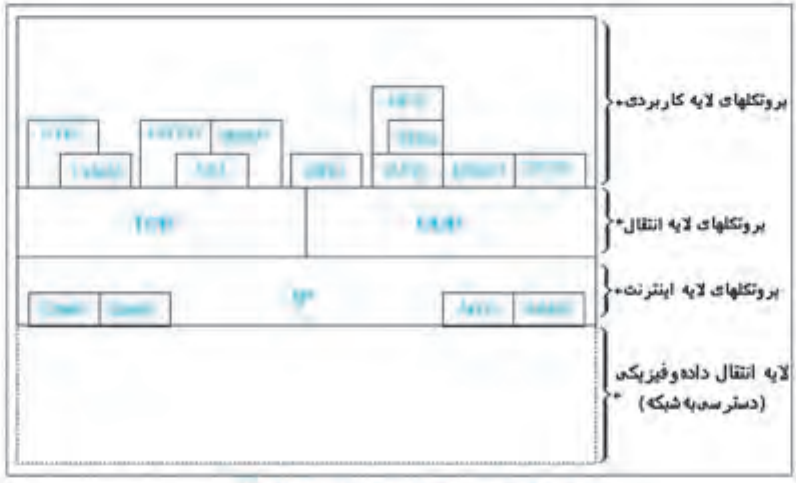
NWLink نمی‌تواند مستقیماً به رایانه‌هایی که با ویندوز کار می‌کنند اجازهٔ دسترسی به سرویس‌های به اشتراک گذاشتن فایل و چاپگر را بدهد. بلکه برای این منظور باید از سرویس‌هایی مانند **CSNW** و **GSNW** به ترتیب در ویندوزهای **Professional** و **Server** استفاده کرد.

۵-۶-۵ Sequenced Packet Exchange (SPX)

پروتکل **SPX** یکی از پروتکل‌های پشتهٔ پروتکل **IPX** سیستم عامل **Netware** است که در لایهٔ انتقال کار می‌کند. این پروتکل یک پروتکل اتصال‌گرا است و اغلب سرویس‌های پروتکل **TCP** مانند : تصدیق دریافت بسته و کنترل جریان انتقال را انجام می‌دهد. سرورهای **Netware** از این پروتکل برای ارتباطات بین صف‌های چاپ، سرورهای چاپ، چاپگرها و سایر برنامه‌های خاص استفاده می‌کنند. از این پروتکل در مقایسه با **TCP** بندرت استفاده می‌شود.

۵-۷ پروتکلهای مدل TCP/IP

در اغلب شبکه‌های امروزه به ویژه اینترنت پروتکلهای **TCP/IP** مورد استفاده قرار می‌گیرند به همین منظور پروتکلهای لایه‌های مختلف این مدل در شکل (۹-۵) ارائه شده است با برخی از این پروتکلها در این فصل آشنا شدیم گرچه بررسی و مطالعه تمام پروتکلهای این مدل در چارچوب این کتاب نیست لیکن با برخی از مهمترین پروتکلهای لایه کاربرد در فصلهای آینده آشنا خواهیم شد.



شکل (۹-۵) پروتکلهای لایه‌های TCP/IP

۵-۸ آشنایی با سرویس‌های TCP/IP

امروزه در اکثر شبکه‌های محلی و اینترنت از **TCP/IP** استفاده می‌شود و اکثر سرویس‌های لایهٔ کاربرد در مدل **OSI** همان سرویس‌های لایهٔ کاربرد مدل **TCP/IP** است. پروتکل‌های این لایه، بین سرویس‌های سرورها، سرویس گیرنده‌ها و کامپیوترها ارتباط برقرار می‌کنند و گاهی برای بدست آوردن یک سرویس از ترکیب سرویس‌های پروتکل‌های دیگر نیز استفاده می‌کنند.

[illegible] عبارتند از :

- **Hyper Text Transfer Protocol (HTTP)**

این پروتکل درخواست‌های یک مرورگر (مانند **IE**) را دریافت‌کرده و آن را به سرویس دهنده وب منتقل می‌کند و سپس صفحه یا فایل مورد درخواست را از سرویس دهنده به مرورگر منتقل می‌کند. برای این منظور بین سرویس دهنده و سرویس گیرنده یک ارتباط **TCP** برقرار می‌شود و تا پایان تبادل اطلاعات برقرار می‌ماند. گرچه این پروتکل تقریباً در سراسر جهان برای استفاده از وب بکار برده می‌شود ولی امنیت چندانی ندارد. یک شکل دیگری از این پروتکل که امکان احراز هویت و رمز گذاری را برای بالابردن امنیت پیش بینی کرده است **HTTPS** نام دارد.

- **File Transfer Protocol (FTP)**

پروتکلی برای انتقال فایل در مدل **TCP/IP** است که اغلب یک برنامهٔ مستقل است. این پروتکل به کاربران اجازه می‌دهد تا از راه دور (مثلاً اینترنت) به فایل‌های یک سرور دسترسی پیدا کنند و از آن فایل دریافت کرده یا به آن فایل منتقل کنند یا فایلها را حذف و ویرایش کنند. این سرویس دو نوع است، یکی به صورت رایگان که همه کاربران اجازه استفاده از آن را دارند (مانند **ftp://ftp.Microsoft.com**) و دیگری که فقط مدیر سایت اجازه استفاده از آن را دارد. برای انتقال صحیح فایل‌ها مقررات و قواعدی وجود دارد که به پروتکل انتقال فایل (**File Transfer Protocol (FTP)**) موسوم است.

- **Simple Mail Transfer Protocol (SMTP)**

این پروتکل برای ارسال پیام الکترونیکی از یک رایانه به رایانهٔ دیگر استفاده می‌شود. امروزه در اینترنت از این پروتکل برای مبادلهٔ نامه‌های الکترونیکی توسط سرورهای پست الکترونیکی (**Mail Server**) استفاده می‌شود.

- **Simple Network Management Protocol (SNMP)**

پروتکل مدیریت شبکه است که طبق آن عوامل مختلف شبکه مانند سخت‌افزارها و نرم‌افزارها می‌توانند بر فعالیت وسایل شبکه نظارت کرده و آن را به کنسول شبکه گزارش کنند.

Telnet

از قدیمی‌ترین سرویس‌های اینترنتی است. افراد می‌توانند به وسیله **Telnet** به یک رایانه متصل به اینترنت (رایانه میزبان (**Host**)) دسترسی پیدا کنند و برنامه مورد نظر خود را بر روی آن رایانه اجرا کنند. در این صورت رایانه شخصی خودشان مبدل به یک پایانه راه دور (**Terminal**) می‌شود و تنها نقش ورود داده‌ها و دستورات به رایانه میزبان و دریافت اطلاعات از آن را ایفا می‌کند. از این طریق افراد می‌توانند برنامه‌های دلخواه خود را بر روی یک رایانه دیگر که ممکن است در گوشه دیگری از دنیا قرار داشته باشد اجرا کنند. امروزه این سرویس کمتر مورد استفاده قرار می‌گیرد.

Network News Transfer Protocol (NNTP)

یک پروتکل غیر رسمی استاندارد در اینترنت است که برای توزیع مقالات خبری و پرس و جو از سرویس دهنده‌های خبری مورد استفاده قرار می‌گیرد این سرویس از دو قسمت تشکیل شده است :

الف) **NNTP Client** یا **News Client**

ب) **NNTP Server** یا **News Server**

وقتی کاربری در یک گروه خبری است عضو می‌شود، رایانهٔ کاربر به عنوان **News Client** است و کاربر می‌تواند توسط این پروتکل آخرین اخبار ارسال شده به **News Server** را دریافت کرده و توسط همین پروتکل نظرات و مقالات خود را برای **News Server** ارسال کند تا به اعضاء دیگر گروه خبری ارسال شود.

Simple Network Time Protocol (SNTP)

ساعت دقیق در شبکه‌هایی که اطلاعات مالی، پرسنلی، مدیریت پروژه و غیره در آنها وارد می‌شود بسیار مهم است به همین منظور از پروتکل**SNTP** برای یکسان کردن دقیق زمان سرویس گیرنده با زمان سرویس دهنده استفاده می‌شود. **SNTP** از دو قسمت **NTP Client** و **NTP Server** تشکیل شده است. **NTP Client** در زمان‌های مشخص با **NTP Server** ارتباط برقرار کرده و ساعت خود را با سرور تنظیم می‌کند. بدین ترتیب ساعت همهٔ رایانه‌های شبکه با ساعت سرور یکی شده و دیگر نیازی نیست که ساعت همه رایانه‌های شبکه را تنظیم کنیم و فقط کافیست ساعت سرور تنظیم شود.

Remote Desktop Protocol (RDP)

مشابه **Telnet** است با این تفاوت که **RDP** گرافیکی است. در ویندوز نرم‌افزاری به نام **Remote Desktop** وجود دارد که متصل شدن به رایانهٔ دیگر را در شبکه ممکن می‌سازد. هنگامی که با این نرم افزار به یک رایانه دیگر متصل می‌شویم صفحه **Desktop** رایانه راه دور

بر روی رایانه ما ظاهر می‌شود و به راحتی می‌توانیم همانند رایانه خود با آن به صورت کاملا گرافیکی کار کنیم نرم افزار **Remote Desktop** از پروتکل **RDP** استفاده می‌کند.

۹-۵ خواندن و درک متون انگلیسی

متن زیر را مطالعه کرده و سپس به سئوالات پاسخ دهید.

Internet tools

TCP/IP provides File Transfer Protocol (FTP) and Telnet. FTP is a character-based utility that permits you to connect to FTP servers and transfer files. Telnet is graphical application that lets you log in to remote computers and issue commands as if you were at the keyboard of the computer. Multiple variations of FTP, Telnet, and other programs based on earlier Internet standards are also available on the Internet or commercially.

۱- دو پروتکل که TCP/IP ارائه می‌کند نام ببرید.

۲- پروتکل انتقال فایل را توضیح دهید.

۳- کاربرد پروتکل Telnet چیست؟

آزمون تشریحی

۱ -مفهوم پشتهٔ پروتکل را توضیح دهید و نمونه‌هایی از آن را در شبکهٔ مورد استفاده در آموزشگاه خود بیان کنید.

۲ - مهم‌ترین پروتکلهای لایهٔ شبکه را نام ببرید و کاربرد هر کدام را توضیح دهید. سپس بررسی کنید در شبکهٔ آموزشگاه شما از کدامیک از این پروتکلها استفاده می‌شود ؟ چرا ؟

۳ - تحقیق کنید در شبکهٔ آموزشگاه شما از کدام پروتکلهای لایهٔ انتقال استفاده می‌شود؟ چرا؟

۴ - مدل مرجع OSI چیست؟ توضیح دهید.

۵ - وظایف اصلی لایه‌های هفت گانهٔ مدل OSI را بیان نمایید.

۶ -کاربرد مدل TCP/IP را توضیح دهید. سپس تحقیق کنید یک برنامهٔ کاربردی نمونه برای استفاده در شبکه اینترنت از چه پروتکلهایی در لایه‌های مختلف این مدل استفاده می‌کند.

۷ - ویژگی‌های پروتکلهای اتصال‌گرا و بی‌اتصال را توضیح دهید و مثالهایی از برنامه‌های کاربردی که با هریک از پروتکلهای مذکور در شبکه کار می‌کنند ذکر کنید.

۸ - معماری شبکه چیست ؟ و در طراحی و پیاده‌سازی شبکه چه نقشی دارد ؟

۹ -سرویس‌های لایهٔ کاربردی TCP/IP را نام برده و کاربرد هریک را شرح دهید. بررسی کنید از کدام یک از سرویس‌های فوق در آموزشگاه شما استفاده می‌شود.

آزمون چهارگزینه‌ای

۱ -مدل هفت لایه‌ای مرجع برای بررسی شبکه ... نام دارد.

الف - TCP/IP　　ب - OSI　　ج - SNA　　د - Apple Talk

۲ -تعیین ماهیت و مشخصات سخت افزارهای شبکه در کدام لایه صورت می‌گیرد ؟

الف - شبکه　　ب - انتقال　　ج - جلسه　　د - فیزیکی

۳ -تعیین پروتکل لایهٔ شبکه که داده‌ها را تولید نموده است از وظایف لایهٔ ... است.

الف - شبکه　　ب - انتقال　　ج - پیوند داده　　د - فیزیکی

۴ -به بسته‌های تولید شده در لایهٔ شبکه ... می‌گویند.

الف - Datagram　　ب - Frame　　ج - Packet　　د - Token

۵ -پروتکل‌های کدام لایه، انتقال سالم اطلاعات را تضمین می‌کند ؟

الف - شبکه　　ب - انتقال　　ج - پیوند داده　　د - فیزیکی

۶ -تعیین نوع محموله و برقراری محموله از وظایف لایهٔ ... است

الف - شبکه ب - انتقال ج - پیوند داده د - جلسه

۷ -توافق در زمینهٔ استفاده از یک زبان مشترک بین رایانه فرستنده و گیرنده از وظایف لایهٔ ... است

الف - نمایش ب - انتقال ج - پیوند داده د - جلسه

۸ -به ساختار درونی یک شبکه رایانه‌ای که ویژگی‌های شبکه را مشخص می‌کند ... گفته می‌شود

الف - توپولوژی شبکه ب - معماری شبکه ج- ترمینولوژی شبکه د - پروتکل شبکه

۹ -کدام پروتکل اتصال‌گرا (Connection Oriented) است ؟

الف - TCP ب - IP ج - IPX د - UDP

۱۰ -در ویندوزهای XP از کدام پروتکل در لایه شبکه استفاده می‌شود؟

الف - TCP ب - IP ج - IPX د - SPX

۱۱ - Router در کدام لایه کار می‌کند ؟

الف -فیزیکی ب - پیوند داده ج - شبکه د - انتقال

۱۲ -کدام گروه از پروتکلهای لایه شبکه هستند ؟

الف- IPX –TCP ب- UDP -TCP

ج- SPX-UDP د- IPX- IP

۱۳ -در ویندوزهای ۹۸ و NT از کدام پروتکل لایه شبکه استفاده می‌شود؟

الف - TCP ب - IP ج - IPX د - NetBEUI

۱۴ -سرویس‌های TCP/IP در کدام لایهٔ شبکه خدمات ارائه می‌کند؟

الف - نمایش ب - کاربردی ج - پیوند داده د - جلسه

۱۵ -کدام پروتکل برای ارسال پیامهای الکترونیکی از یک کامپیوتر به کامپیوتر دیگر استفاده می‌شود ؟

الف - SNMP ب - HTTP ج - Telnet د - SMTP

۱۶ -کدام گروه از پروتکل‌های لایه کاربردی هستند ؟

الف- IPX-TCP-FTP ب- IPX-SMTP-NNTP

ج- SNTP-RDP-NNTP د- HTTP-IP-NetBEUI

فصل ششم

امنیت شبکه

هدفهای رفتاری :

پس از مطالعه این فصل از فراگیر انتظار می رود که :

- امنیت شبکه را توضیح دهد.
- با تدوین سیاستهای امنیتی برای یک سازمان آشنا باشد.
- دلیل محافظت با استفاده از کلمهٔ عبور را توضیح دهد.
- تنظیمات کلمهٔ عبور کاربران را انجام دهد.
- تنظیمات نحوهٔ دسترسی کاربران را بشناسد.
- مدل‌های امنیتی مناسب را بشناسد.
- کاربرد دیوارهٔ آتش(Firewall) را توضیح دهد.
- دیوارهٔ آتش ویندوز را فعال/غیرفعال کند.
- توانایی خواندن و درک متون انگلیسی مرتبط را داشته باشد

زمان نظری : ۱ ساعت

زمان عملی : ۲ ساعت

۴-۱ آشنایی با مفهوم امنیت

مفهوم امنیت در دنیای واقعی برای بسیاری از ما حیاتی است در دوران ماقبل تاریخ امنیت عبارت بود از اصول حفظ بقاء، نظیر امنیت در برابر حملهٔ دیگران یا حیوانات. امروزه با گسترش شبکه‌های رایانه‌ای و دسترسی همگانی به شبکه اینترنت، ایمن نگاه داشتن محل ذخیرهٔ اطلاعات و مبادلهٔ امن اطلاعات الزامی است. اینترنت بخودی خود رسانه‌ای نیست که نسبت به رفتار تبهکارانه ایمنی داشته باشد. هزینه عدم توجه به امنیت می‌تواند از دست دادن اطلاعات گران قیمت و مهم یک سازمان بزرگ باشد. همچون محیط زندگی واقعی در محیط شبکه نیز امنیت مطلق غیرممکن است ولی امنیتی به اندازهٔ کافی مناسب، تقریباً در تمامی شرایط محیطی دست یافتنی است. در متون رایانه‌ای برای امنیت تعاریف مختلفی ارائه شده است. فرهنگ اصطلاحات رایانه‌ای مایکروسافت امنیت را فنآوریهای مورد استفاده برای مقاوم کردن یک سرویس در مقابل دستیابی غیرمجاز به داده‌ها تعریف می‌کند مسئله اصلی در خصوص امنیت رایانه‌ها، به ویژه سیستمهایی که اشخاص زیادی به آنها دسترسی دارند یا از طریق خطوط ارتباط به آن دستیابی پیدا می‌کنند جلوگیری از دستیابی اشخاص غیر مسؤول است. به عبارت دیگر هنگامی در فضای مجازی امن هستید که دسترسی به منابع اطلاعاتی شما تحت کنترل خودتان باشد یعنی هیچ‌کس بدون کسب اجازه از شما قادر به دسترسی به این منابع اطلاعاتی نباشد.

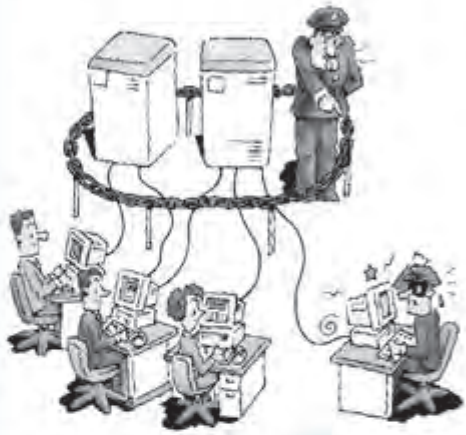
۴-۲ آشنایی با سیاستهای تدوین شده سازمان

امروزه سازمانها و موؤسسات بزرگ و متوسط با توجه به حساسیت و نوع اطلاعات خود برای حفظ اطلاعات، نگهداری فرایندها و دانش سازمانی اقدام به تدوین سیستم مدیریت امنیت اطلاعات می‌کنند و در این برنامه سیاستهای امنیتی، سطوح دسترسی و اقدامات امنیتی و غیره را برای حفظ اطلاعات، گردش اطلاعات و دسترسی کاربران مختلف به منابع اطلاعاتی سازمان تدوین می‌کنند. سیاستهای امنیتی سازمانها با توجه به نوع و حساسیت منابع اطلاعاتی در سازمانهای مختلف متفاوت است نمونه‌هایی از سیاستهای امنیتی منابع اطلاعاتی سازمانها عبارتند از :

- طبقه‌بندی منابع اطلاعاتی و دسترسی کاربران مختلف به این منابع با توجه به سطح اختیارات آنها (مانند: دسترسی کاربرانی خاص به چاپگر یا گزارشات خاصی از برنامه‌های کاربردی)
- دسترسی کاربران به منابع اطلاعاتی در شبکه یا اینترنت از طریق کلمهٔ عبور
- عدم استفاده از حافظه‌های جانبی قابل حمل در شبکه (مانند: دیسک نوری یا فلش دیسک)
- محدودیت دسترسی به شبکه از راه دور (مانند عدم دسترسی از طریق مودم)
- بستن پورتهایی خاصی در شبکه (مانند بستن پورت ۲۱ و ۱۱۰ برای عدم استفاده از پروتکلهای پست الکترونیکی)

۶-۳ آشنایی با امنیت شبکه

یکی از مهمترین وظایف مدیران شبکه برقراری امنیت اطلاعات شبکه است. منظور از امنیت شبکه، حفظ منابع و اطلاعات مختلف موجود در شبکه از دسترسی افراد غیر مجاز و حفاظت از این اطلاعات در مقابل دست کاری غیرمجاز است. مکانیزم‌های امنیتی مختلفی برای برقراری امنیت شبکه و حفظ منابع آن وجود دارد.



مهمترین روش‌های حفاظت از منابع شبکه عبارتند از :

- محافظت با کلمهٔ عبور
- استفاده از مدل‌های امنیتی مناسب
- استفاده از دیوارهٔ آتش(Firewall)
- استفاده از پروتکل‌های امنیتی

۶-۴ محافظت با استفاده از کلمهٔ عبور

برای جلوگیری از ورود افراد غیر مجاز به شبکه و استفاده از منابع موجود در آن روش‌های مختلفی وجود دارد. در برخی از شبکه‌ها که از امنیت بسیار بالایی برخوردارند افراد را مجبور به استفاده از کارتهای هوشمند یا اثر انگشت می‌کنند. اما در اغلب شبکه‌های رایج، کاربران را به گروه‌های کاری مختلف دسته بندی کرده و پس از تعیین سطح دسترسی آنها به منابع مختلف موجود در شبکه، برای هر کاربر یک **Username** و **Password** ویژه و محرمانه تعریف می‌کنند تا کاربر فوق در هنگام ورود به شبکه با آن تعیین هویت شده و صرفاً به منابعی که دسترسی آن برایش از قبل توسط مدیر شبکه تعیین شده است دسترسی پیدا نماید. اگر **Username** و **Password** کاربران در شبکه طوری برنامه‌ریزی شده باشد که هر کاربر با یکمرتبه واردکردن **Username** و **Password** بتواند به تمام منابع و برنامه‌های کاربردی مجاز خود دسترسی پیدا کند در این صورت اصطلاحاً به آن **Single Sign On (SSO)** گفته می‌شود و در حالتی که کاربر شبکه برای دسترسی به هریک از منابع مجاز در شبکه باید **Username** و **Password** خود را جداگانه وارد کند اصطلاحاً **Single Sign Off** گفته می‌شود. به عنوان مثال اگر دسترسی به یک چاپگر، برنامهٔ کاربردی اتوماسیون و اشتراک اینترنت در یک شبکه برای کاربری خاص مجاز باشد این کاربر در حالت

Single Sign On (SSO) با یک بار واردکردن **Username** و **Password** خود می‌تواند از تمام موارد مذکور استفاده کند.

گرچه سیستم عامل‌های شبکهٔ مختلف، کاربران را با توجه به سطح اختیارات آنها به گروه‌های مختلفی تقسیم می‌کنند اما تقریباً همه سیستم عامل‌های شبکه، کاربران را به سه گروه اصلی تقسیم می‌کنند :

- مدیر (Administrator یا Supervisor)
- عضو (Member)
- میهمان (Guest)

کاربر مدیر یا کاربرانی که در این گروه قرار داده می‌شوند می‌توانند تمام منابع شبکه را مدیریت نمایند، کاربر و اختیارات وی را تعریف نمایند، برنامه‌ها و سخت افزارها را در شبکه نصب نمایند، اطلاعات شبکه را جابجا کرده یا از آنها نسخهٔ کپی (پشتیبان) تهیه نمایند و خلاصه هر آنچه بخواهند می‌توانند در شبکه انجام دهند.

کاربر میهمان معمولاً می‌تواند بدون کلمه رمز عبور یا با یک کلمهٔ رمز عبور غیر محرمانه که در اختیار همگان است وارد شبکه شود و از منابع محدودی که استفاده از آنها برای عموم آزاد است استفاده نماید. در سیستم عامل شبکه ویندوز ۲۰۰۰ سرور، گروهی به نام **Everyone** با اختیارات پیش فرض وجود دارد که تمام کاربران پس از تعریف در این گروه عضو می‌شوند. و این گروه به هر منبعی از شبکه دسترسی داشته باشد، تمام کاربران به آن منبع دسترسی پیدا می‌کنند.

کاربران عضو یک شبکه ممکن است با توجه به دامنهٔ فعالیتشان به گروه‌های کاری مختلفی دسته بندی شوند. دسته بندی کاربران به گروه‌های کاری باعث می‌شود که مدیریت آنها برای مدیر شبکه آسان تر شود. مثلاً کاربرانی که از سیستم حقوق در شبکه استفاده می‌کنند را در گروهی به نام **Salary** قرار می‌دهیم و اختیارات و دسترسی این گروه کاری را تعیین می‌کنیم. حال تمام کاربران عضو این گروه می‌توانند از این اختیارات در شبکه بهره‌مند شوند.

کارایی استفاده از کلمهٔ عبور برای تامین امنیت منابع شبکه بستگی به تدابیر اتخاذ شده از سوی مدیر شبکه دارد. اگر مدیر شبکه بدلیل امنیت بیشتر برای کاربران خود کلمه‌های عبوری طولانی و مرکب از حروف و اعداد انتخاب نماید، ممکن است کاربران برای عدم فراموش کردن، آن را بر روی کاغذ یا حتی صفحهٔ مانیتور بنویسند و این به معنی از بین رفتن امنیت شبکه است. چنانچه مدیر شبکه‌ای کاربران خود را در تعیین کلمهٔ عبور آزاد بگذارد ممکن است کاربران کلمه‌های عبور بسیار ساده‌ای که امکان شناسایی آن راحت است انتخاب نمایند و باز هم امنیت شبکه به خطر بیافتد برای حل این مشکل اکثر سیستم عامل‌های شبکه راه حلی متشکل از هر دو روش فوق ارائه می‌کنند.

۶-۲-۱ تنظیمات کلمهٔ عبور کاربران

در سیستم عامل شبکه ویندوز ۲۰۰۰ سرور، در زمان ایجاد یک کاربر جدید توسط مدیر شبکه، گزینه‌های مختلفی را برای کنترل مسائل امنیتی کلمهٔ عبور کاربران در اختیار می‌گذارد که برخی از آنها عبارتند از :

- **User Must Change Password at Next Logon**
  کاربر باید اولین مرتبه که وارد شبکه می‌شود کلمهٔ عبور خود را تغییر دهد.
- **User Cannot Change Password**
  کاربر نمی‌تواند کلمهٔ عبور خود را تغییر دهد.
- **Password Never Expire**
  کلمهٔ عبور هرگز غیر فعال نشود (بصورت پیش فرض در سیستم عامل ویندوز ۲۰۰۰ سرور، کلمهٔ عبور کاربری که جدید تعریف می‌شود پس از چند روز غیر فعال می‌شود.)
- **Account Is Disabled**
  دسترسی کاربر فوق غیرفعال است.

علاوه بر موارد فوق مدیر شبکه می‌تواند تدابیر امنیتی شدیدتری را برای کلمهٔ عبور کاربران اتخاذ نماید که برخی از آنها عبارتند از :

- **مشخص کردن طول کلمهٔ عبور**
- **تعیین مدت اعتبار کلمهٔ عبور**
- **الزام به استفاده از کلمات عبور پیچیده**
- **رمز گزاری کلمه‌های عبور**

۶-۲-۲ تنظیمات نحوهٔ دسترسی کاربران

در سیستم عامل شبکه ویندوز ۲۰۰۰ سرور، امکاناتی را برای مدیر شبکه فراهم کرده است که به کمک آنها می‌تواند نحوهٔ دسترسی کاربران را معین کند. برخی از این امکانات عبارتند از :

- **کاربر مورد نظر فقط توسط رایانه مشخص شده توسط مدیر شبکه می‌تواند وارد شبکه شود.**
- **کاربر مورد نظر بطور هم زمان فقط از یک ایستگاه حق اتصال به شبکه را دارد.**
- **کاربر مورد نظر فقط زمان‌های خاصی بتواند از شبکه استفاده نماید. (طبق برنامهٔ زمان بندی که توسط مدیر شبکه مشخص می‌شود.)**
- **کاربر مورد نظر فقط تا تاریخ مشخصی حق استفاده از شبکه را داشته باشد.**

۴-۵ استفاده از مدل‌های امنیتی مناسب

در فصل‌های قبل با دو نوع شبکه **Peer to Peer** و **Client-Server** آشنا شدیم. در هریک از شبکه‌ها مدل امنیتی متفاوتی استفاده می‌شود.

دو مدل امنیتی در سیستم عامل‌های ویندوز، به شرح زیر وجود دارد :

- **سطح مشترک (Share Level)**
- **سطح کاربر (User Level)**

در شبکه‌های **Peer to Peer** هر رایانه اطلاعات امنیتی کاربران و منابع خود را بطور مستقل در خود ذخیره می‌کند. در این شبکه‌ها برای دسترسی سایر کاربران به منابع یک رایانه، لازم است آن رایانه فایل، پوشه یا منبع فوق را به اشتراک گذاشته و برای دسترسی به آن کلمهٔ رمز تعیین کند و آن را در اختیار کاربران شبکه قرار دهد به این روش سطح امنیتی مشترک گفته می‌شود زیرا همهٔ کاربران شبکه برای استفاده از یک منبع، از یک کلمهٔ عبور مشترک استفاده می‌کنند که امنیت آن پایین است.

در روش **Peer to Peer**، دو نوع دسترسی برای منابع می‌توان تعیین کرد:

- **Read Only**
  منبع یا فایل به اشتراک گذاشته شده فقط قابل خواندن است.
- **Full**
  دسترسی کامل به منبع یا فایل به اشتراک گذاشته شده است که شامل خواندن، نوشتن حذف کردن و .... است.

ویندوزهای ۹۵، ۹۸ و **ME** فقط می‌توانند از سطح امنیتی مشترک استفاده کنند.

در مدل امنیتی سطح کاربر، برای استفادهٔ سایر کاربران از منابع یک رایانه، برای هر یک از کاربران یک حساب جداگانه باز می‌شود و اطلاعات کاربری و دسترسی آنان را تعیین می‌کند. بنابراین در شبکه‌های **Peer to Peer** برای استفادهٔ یک کاربر از منابع سایر رایانه‌ها لازم است مشخصات و دسترسی وی بر روی تمام رایانه‌ها تعریف شود که امری دشوار است.

سیستم عامل	مجوز	عملکرد
Windows	Read	بازکردن، مشاهده و خواندن فایل
	Write	بازکردن، خواندن و نوشتن در فایل
	Create	ایجاد فایل جدید
	File Scan	مشاهدهٔ فهرست فایل‌های یک دایرکتوری
	Erase	حذف فایل
	Modify	تغییر نام یا مشخصات فایل
Windows Server 2003	Read	خواندن و کپی کردن فایل
	Execute	اجرای فایل
	Write	ایجاد فایل جدید
	Delete	حذف فایل
	Full Control	تمام اختیارات بالا
	No Access	عدم دسترسی به منابع

جدول ۱۱ـ۶ مجوزهای دسترسی شبکه

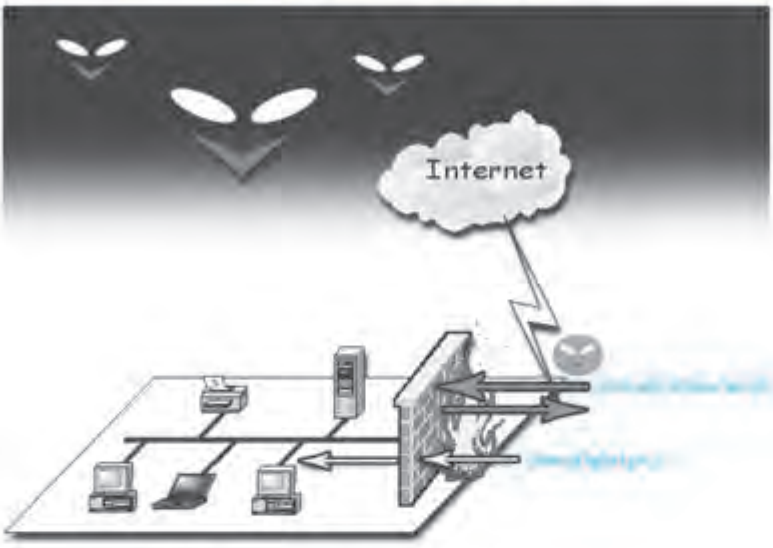
در شبکه‌های **Client-Server** اطلاعات تمام کاربران بصورت متمرکز در یک رایانه نگهداری می‌شود و مدیر شبکه می‌تواند بصورت متمرکز دسترسی کاربران مختلف را به منابع مختلف موجود در شبکه از طریق سطح امنیتی کاربر تعیین کند **(Single Sign On)**.

نسخه‌های مختلف ویندوزهای **NT**، **2000**، **XP** و **2003** اگر در شبکه‌های **Server Base** استفاده شوند از سطح امنیتی کاربر استفاده می‌کنند.

سیستم عامل‌های مختلف شبکه، سطوح دسترسی کاربران و گروه‌ها را با ویژگی‌های مختلفی تعیین می‌کنند. درجدول (۱-۶) انواع مجوزهای دسترسی در برخی از سیستم عاملهای شبکه ارائه شده است.

۶ـ۶ استفاده از دیوارهٔ آتش (Firewall)

در شبکه‌هایی که به شبکه‌های اینترنت یا سایر شبکه‌های بزرگ متصل می‌شوند، امنیت شبکه در مقابل کاربران خارجی اهمیت پیدا می‌کند. در این موارد برای تامین امنیت شبکه از دیوارهٔ آتش **(Firewall)** سخت افزاری یا نرم افزاری در نقطهٔ اتصال شبکه به خارج استفاده می‌شود.



[illegible]

سیستم امنیتی را که برای محافظت از شبکه داخلی در مقابل نفوذ افراد از خارج شبکه طراحی شده است، اصطلاحاً دیوار آتش می‌گویند. دیوار آتش مجموعه‌ای از نرم‌افزارها و سخت‌افزارهایی است که برای محافظت از شبکه داخلی و محافظت از اطلاعات کاربران شبکه نصب می‌شود. دیوار آتش از ارتباط مستقیم بین کاربران شبکه محلی و کاربران اینترنتی دیگر جلوگیری کرده و خود به عنوان یک حایل این ارتباط را برقرار می‌نماید. دیوار آتش کلیه اطلاعاتی را که وارد شبکه می‌شود مورد بررسی قرار داده و مشابه شکل (۲-۶) فقط درخواستهای مجاز و بی‌خطر را به داخل شبکه هدایت می‌کند و با این روش شبکه را در مقابل نفوذ هکرها، ویروس‌ها و دیگر خطرات احتمالی محافظت می‌نماید. معمولاً شما به عنوان یک کاربر اینترنت از وجود دیوار آتش اطلاعی ندارید ولی گاهی اوقات ممکن است که در استفاده از بعضی از نرم‌افزارهای اینترنتی دچار مشکل شوید و آن نرم‌افزار به شما اعلام می‌کند که احتمالاً شما پشت یک دیوار آتش هستید. در اینگونه مواقع شاید نتوانید از خدمات آن نرم‌افزار اینترنتی استفاده کنید زیرا دیوار آتش تشخیص داده است که استفاده از این نرم‌افزار برای شبکه محلی خطرناک است. در اینگونه مواقع باید با قسمت پشتیبانی شبکه خود تماس بگیرید تا برای رفع مشکل شما را راهنمایی کنند.

۶-۷ فعال و غیرفعال کردن دیوار آتش ویندوز XP

ویندوز **XP** برای حفاظت بیشتر رایانه در مقابل خطرات و تهدیدهای نرم‌افزارها و افراد غیرمجاز، دیوار آتش پیش بینی شده است که اغلب به صورت پیش فرض فعال است و توصیه می‌شود که این قابلیت همواره فعال باشد. برای فعال کردن یا غیر فعال کردن دیوار آتش ویندوز با کاربر مدیر سیستم وارد رایانه شده و مراحل زیر را دنبال می‌کنیم :

- از پنجرهٔ **Control panel** برنامه **Windows Firewall** را اجرا می‌کنیم و سربرگ **General** را انتخاب می‌کنیم.
- مشابه شکل (۳-۶) برای فعال کردن دیوار آتش گزینهٔ **On (recommended)** را انتخاب می‌کنیم و برای غیرفعال‌کردن دیوار آتش گزینهٔ **Off (not recommended)** را انتخاب می‌کنیم و دکمهٔ OK را کلیک می‌کنیم.

۸-۶ استفاده از پروتکل‌های امنیتی

در شبکه‌های بزرگ مانند شبکهٔ جهانی اینترنت، امنیت اطلاعات در حال عبور اهمیت پیدا می‌کند. زیرا در این شبکه‌ها افراد مختلف می‌توانند اطلاعات ارسالی از یک رایانه را به رایانه‌ای دیگر در بین راه دریافت کرده و استفاده کنند. برای حل این مشکل از پروتکل‌های امنیتی استانداردی برای رمز گزاری اطلاعات ارسال شده استفاده می‌شود. برخی از پروتکلهای امنیتی عبارتند از :

- **IPSec**
  برای رمز گزاری اطلاعات در شبکه‌های محلی استفاده می‌شود.
- **SSL**
  برای رمز گزاری اطلاعات ارسال شده از طریق وب استفاده می‌شود.
- **Kerberos**
  برای رمز گزاری اطلاعات هویتی کاربران در ویندوز استفاده می‌شود.

علاوه بر تدابیر امنیتی گفته شده در این فصل، در شبکه‌های مهم و حساس مسائل دیگری نیز از اهمیت بالایی برخوردارند. مانند امنیت در مقابل نفوذ ویروس‌ها و هکرها، تهیهٔ نسخهٔ پشتیبان از اطلاعات و امنیت فیزیکی شبکه و اطلاعات موجود در آن. در شبکه‌های حساس و مهم، مدیر شبکه و مدیران ارشد موسسات تدابیر امنیتی شدید و خاص خود را اعمال می‌کنند. علاقه‌مندان می‌توانند برای اطلاعات بیشتر به مراجع معتبر رجوع کنند و از مراکز شبکهٔ سازمانهای مختلف بازدید بعمل آورند.

۶-۹ خواندن و درک متون انگلیسی

متن زیر را که بخشی از راهنمای ویندوز **XP** در بارهٔ برنامهٔ **Security Center** واقع در **Control Panel** است مطالعه کرده و سپس به سئوالات پاسخ دهید.

The Security Center

Use the Security Center to check your security settings and learn more about how to improve the security of your computer with Windows Firewall, Automatic Updates, and antivirus software.

Windows Firewall
Windows Firewall is on by default and helps protect your computer against viruses and other security threats, such as intruders who might try to access your computer over the Internet.

Automatic Updates
With Automatic Updates, Windows can routinely check for the latest important updates for your computer and install them automatically

۱- با توجه به متن کاربرد Security Center را توضیح داده و سپس این برنامه را اجرا کنید و دربارهٔ توضیحات داده شده در متن تحقیق کنید.
۲- کاربرد Automatic Updates را توضیح دهید، بهروزرسانی خودکار ویندوز را فعال کنید.
۳- برای کاهش خطر دسترسی افراد و برنامه‌های غیر مجاز به رایانه چه کاری باید انجام داد؟

آزمون تشریحی

۱- مفهوم و لزوم امنیت شبکه را توضیح دهید.
۲- تحقیق کنید سیاستهای امنیتی شبکه آموزشگاه شما چیست؟
۳- روشهای اصلی امنیت شبکه را نام ببرید سپس تحقیق کنید کدام یک در آموزشگاه شما مورد استفاده قرار می‌گیرد؟
۴- ویروس محافظت را کلمهٔ مرور چگونه امنیت شبکه را برقرار می‌کند؟
۵- ویندوز از چه مدل‌های امنیتی برای شبکه استفاده می‌کند؟ توضیح دهید.
۶- فایروال‌های امنیتی چگونه امنیت شبکه را تضمین می‌کند؟

۷- طرز کار دیوارهٔ آتش را توضیح دهید و نقش آن را در برقراری امنیت شبکه بیان کنید.

۸- بررسی کنید در آموزشگاه محل تحصیل شما از چه دیوارهٔ آتش و تنظیمات امنیتی دیگر استفاده می‌شود چرا؟

آزمون چهارگزینه‌ای

۱- کدام گزینه باعث کاهش امنیت شبکه می‌شود؟

الف - الزام کاربران به استفاده از کلمهٔ عبور پیچیده

ب - تعیین مدت اعتبار کلمهٔ عبور و اجبار کاربر به تغییر آن

ج - اعطای اختیارات کامل به کاربر برای تعیین آزادانه کلمهٔ عبور دلخواه

د - سلب اختیار تغییر کلمهٔ عبور از کاربر

۲- برای غیر فعال کردن موقتی یک کاربر در شبکه از کدام گزینه استفاده می‌شود؟

الف - **Password Never Expire**　　ب - **Account is Disable**

ج - **Account is Enable**　　د - **User Cannot Change Password**

۳- مدل امنیتی سیستم عامل ویندوز سرور ۲۰۰۳ ..... است.

الف- در شبکه‌های **Server Base** مدل **Share Level**

ب- در شبکه‌های **Server Base** مدل **User Level**

ج- همیشه **User Level**

د- همیشه **Share Level**

۴- مدل امنیتی مورد استفاده در ویندوز **XP** کدام است؟

الف - **Share Level**　　ب - **User Level**

ج - **Share Level** و **User Level** باهم　　د - هیچکدام

۵- کدام مدل امنیتی مورد استفاده در سیستم عامل های ویندوز برای شبکه از امنیت بالاتری برخوردار است؟

الف - **Share Level**　　ب - **User Level**

ج - **Share Level** و **User Level** باهم　　د - هیچکدام

۶- برای تعیین هویت کاربران شبکه، کدام پروتکل امنیتی در سیستم عامل شبکه ویندوز ۲۰۰۰ سرور مورد استفاده قرار می‌گیرد؟

الف - **IPSec**　　ب - **SSL**　　ج - **Kerberos**　　د - **User Level**

فصل هفتم

توانایی کار با اینترنت

هدفهای رفتاری :

پس از مطالعه این فصل از فراگیر انتظار می رود که :

- ☑ مفاهیم شبکه جهانی وب ، فرایپوند ، فوق متن ، فوق رسانه ، صفحه وب ، وب سایت ، Home Page را تعریف کند.
- ☑ نحوه آدرس دهی صفحات وب را بیان کند.
- ☑ تنظیمات اتصال به اینترنت را انجام دهد.
- ☑ نرم افزار IE را برای استفاده از اینترنت بکار گیرد.
- ☑ تنظیمات نرم افزار IE را انجام دهد.
- ☑ سایتهای مورد علاقه خود را در Favorites ذخیره کند.
- ☑ صفحات وب مشاهده شده را از History مشاهده کند.
- ☑ تصاویر و صفحات وب را بر روی دیسک ذخیره کند.
- ☑ فایل های مورد نظر را از اینترنت دریافت کند.
- ☑ عملیات جستجو در وب را انجام دهد.

زمان نظری : ۲ ساعت

زمان عملی : ۱۰ ساعت

۷-۱ آشنایی با مفاهیم مقدماتی اینترنت

برای اینکه بتوانیم به نحو بهتری از شبکه جهانی اینترنت استفاده نماییم لازم است ابتدا با مفاهیم اولیه‌ای مانند شبکه اینترنت، شبکه جهانی وب، پروتکل‌های اینترنتی، **URL**، **ISP**، اشتراک اینترنت و غیره آشنا شویم و سپس با نحوه تنظیم و ایجاد ارتباط با اینترنت و کار با نرم‌افزار **Internet Explorer** آشنا شویم.

۷-۱-۱ شبکه اینترنت (Internet)

اینترنت بزرگترین شبکه رایانه‌ای جهان است که از میلیونها رایانه شخصی، مسیریاب (**Router**) و تجهیزات مخابراتی تشکیل شده‌است. سابقه ایجاد شبکه اینترنت به سال ۱۹۶۸ باز می‌گردد. در این سال برای اولین بار شبکه‌ای با نام آرپانت (**ARPANET**) بین مراکز نظامی ایجاد شد. به تدریج مراکز تحقیقاتی و دانشگاهها به این شبکه متصل شدند و کم‌کم سازمانها و افراد دیگر در سراسر دنیا شبکه‌های محلی خود را به این شبکه بین‌المللی متصل کردند تا شبکه اینترنت که در حقیقت شبکه‌ای از شبکه‌ها محسوب می‌شود، ایجاد شود. اینترنت ارتباط بین مراکز مهم دانشگاهی و تحقیقاتی، موسسات دولتی، مراکز تجاری و تمامی کاربران را در سراسر جهان فراهم می‌کند و در حقیقت امکان اتصال همگانی را میسر می‌سازد و متعلق به فرد یا گروه خاصی نمی‌باشد.

شکل ۷-۱ شبکه اینترنت

۷-۱-۲ سرویس‌های شبکه اینترنت

شبکه اینترنت در واقع بستری ارتباطی است که می‌توان انواع خدمات و سرویس‌ها را بر روی آن ارائه کرد. از زمان ایجاد این شبکه تاکنون سرویس‌های متنوعی بر روی این شبکه ارائه شده است که برخی از آنها پر استفاده‌تر و مشهورتر هستند و برخی از آنها کمتر استفاده می‌شوند.

برخی از مهمترین خدمات و سرویس‌های شبکه اینترنت عبارتند از :

- شبکه جهانی وب (WWW)
- پست الکترونیک (Email)
- انتقال فایل (FTP)
- گروه‌های خبری (USENET)
- کار با رایانه از راه دور (Telnet)

حقیقت این است که امروزه علاوه بر خدمات فوق، خدمات متنوع دیگری نیز در شبکه اینترنت ارائه می‌شود که برخی از آنها عبارتند از : انتقال صوت از طریق اینترنت (VOIP) یا همان تلفن اینترنتی، پیام‌رسان (Messenger) ، مشاهده تصاویر دوربین‌های زنده، رادیو و تلویزیون اینترنتی، ارسال SMS از طریق اینترنت ، شبکه‌های به اشتراک گذاری فایل بین رایانه‌ها و ده‌ها ایده دیگر که ممکن است در آینده از طریق شبکه اینترنت به عنوان خدمات جدید در اختیار کاربران قرار گیرد.

۳-۱-۷ شبکه جهانی وب

تور جهان گستر (World Wide Web) که معمولاً بصورت مختصر WWW نمایش داده می‌شود، به مجموعه اسنادی گفته می‌شود که به صورت صفحات مخصوصی به نام صفحه وب بر روی شبکه اینترنت قرار دارند که به آن شبکه جهانی وب نیز می‌گویند.

هر صفحه وب می‌تواند ترکیبی از متن، تصویر، صدا، فیلم و ... باشد. صفحات وب به یکدیگر مرتبط هستند که این ارتباط از طریق فراپیوند (Hyperlink) انجام می‌شود.

فراپیوند : Hyperlink

ارتباط بین یکی از اجزای یک صفحه وب با بخشی از همان صفحه یا صفحه وب دیگر را فراپیوند می‌گویند

یک فوق‌پیوند یک قطعه از متن یا تصویر روی صفحه وب است که وقتی روی آن کلیک می‌کنیم معمولاً یکی از موارد زیر اتفاق خواهد افتاد:

- ما را به قسمت دیگری از همان صفحه منتقل می‌کند.
- ما را به صفحه دیگری از آن سایت منتقل می‌کند.
- ما را به صفحه‌ای از سایتی دیگر منتقل می‌کند.
- یک فایل را دریافت می‌کند.
- یک فایل را اجرا می‌کند.

فرایوند ممکن است به صورت فوق‌متن (Hypertext) یا فوق رسانه (Hypermedia) باشد.

فوق متن یک متن متمایز شده است که معمولاً بصورت زیر خط دار و با یک رنگ متمایز در صفحه وب مشخص می‌شود. فوق متن امکان اتصال یک صفحه وب به صفحه وب دیگر را فراهم می‌کند. حتی یک فوق متن می‌تواند به عنصری از همان صفحه وبی که در آن قرار دارد ، ارتباط برقرار کند.

هر صفحه وب ممکن است توسط پیوندهای فوق متنی و یا پیوندهای فوق رسانه‌ای به چندین صفحه وب دیگر متصل باشد که هر کدام از این صفحات وب ممکن است بر روی یک رایانه در گوشه‌ای از دنیا باشند.

مثال ۱ در شکل (۲-۷) صفحه وبی را مشاهده می‌کنیم که کشور ایران را معرفی می‌کند. در این صفحه تصاویری از نقاط دیدنی کشور ایران قرار داده شده است. در قسمتی از متن آمده است :

پایتخت کشور ایران شهر تهران است.

و عبارت شهر تهران با رنگ متمایز و به صورت زیر خط دار مشخص شده است. یعنی عبارت شهر تهران یک پیوند فوق متن (Hypertext) است به این معنی که از طریق آن می‌توانیم به صفحه وبی مراجعه کنیم که حاوی اطلاعاتی در مورد شهر تهران است.

در صفحه وب شکل (۲-۷)، تصاویری از آثار تاریخی ایران را مشاهده می‌کنیم که هر تصویر به صفحهٔ وب دیگری متصل است که آن صفحه وب در مورد این اثر تاریخی توضیحات بیشتری را ارائه می‌کند. بنابراین تصاویر مذکور، پیوند فوق رسانه‌ای (Hypermedia) محسوب می‌شوند.

نکته جالب این است که هر صفحه وب ممکن است در رایانه‌ای از کشوری بسیار دور باشد که ما با یک کلیک ماوس می‌توانیم آن صفحه را دریافت و مشاهده کنیم. باید توجه کرد که وب به معنی کل اینترنت نیست و همانطور که گفته شد در شبکه جهانی اینترنت، سرویس‌ها و امکانات مختلفی وجود دارد که یکی از پرکاربردترین آنها سرویس وب است.

۷-۱-۴ نرم‌افزار مرورگر وب (Web Browser)

با ساختار و مفهوم شبکه جهانی وب آشنا شدیم. در این قسمت با نرم‌افزار مرورگر وب آشنا می‌شویم.

مرورگر وب (Web Browser)

به نرم‌افزاری که امکان نمایش و حرکت بین صفحات وب را میسر می‌کند، مرورگر وب می‌گویند.

نرم‌افزارهای مرورگر امکان نمایش صفحات وب و حرکت بین صفحات از طریق فوق‌پیوندها را می‌دهند. از معروفترین نرم‌افزارهای مرورگر می‌توان نرم‌افزار **Internet Explorer** محصول شرکت مایکروسافت و نرم‌افزار **FireFox** محصول شرکت **Mozilla** را نام برد.

۷-۱-۵ پروتکل‌های انتقال اطلاعات

در شبکه جهانی وب ، برای انتقال اطلاعات بین رایانه‌ها از قراردادهای استانداردی که پروتکل نامیده می‌شوند، استفاده می‌شود مهمترین پروتکل‌های انتقال اطلاعات عبارتند از : **HTTP** و **FTP**.

۷-۱-۵-۱ پروتکل HTTP

پروتکل HTTP مخفف عبارت Hypertext Transfer Protocol (پروتکل انتقال فوق‌متن) است.

فرض کنید که مرورگر وب شما می‌خواهد از یکی از سایتهای اینترنتی یک صفحه وب را دریافت کند. مرورگر وب یک درخواست HTTP به رایانه سرویس‌دهنده وب می‌فرستد. رایانه سرویس‌گیرنده این درخواست را دریافت کرده و فایل‌های درخواستی را مطابق پروتکل HTTP به رایانه شما می‌فرستد.

پروتکل HTTP

HTTP مجموعه‌ای از قوانین است که برای انتقال فایل در شبکه جهانی وب استفاده می‌شود. فایل‌های قابل انتقال با پروتکل HTTP عبارتند از: فایل‌های متنی، گرافیکی، صوتی، ویدیویی و یا هر نوع فایل چند رسانه‌ای دیگر.

۷-۱-۵-۲ پروتکل FTP

پروتکل FTP مخفف عبارت File Transfer Protocol (پروتکل انتقال فایل) است.

FTP معمولاً برای انتقال فایل‌های صفحات وب از روی رایانه طراح صفحات وب به روی رایانه سرویس‌دهنده (Server) استفاده می‌شود. این سرویس همچنین برای دریافت فایل (Download) از روی سرویس‌دهنده‌ها مورد استفاده قرار می‌گیرد.

پروتکل FTP

FTP مجموعه‌ای از قوانین است که برای انتقال فایل در شبکه جهانی وب استفاده می‌شود. از این پروتکل برای دریافت فایل (Download) در شبکه اینترنت استفاده می‌شود.

۷-۱-۶ آشنایی با صفحه وب (Web Page)

صفحات وب فایل‌های متنی هستند که اغلب توسط زبان استاندارد HTML (Hypertext Markup Language) ایجاد می‌شوند.[1] فایل‌های HTML معمولاً از یکسری دستورالعمل تشکیل شده‌اند که این دستورالعمل‌ها نحوه نمایش متن و تصویر را در صفحه وب مشخص می‌کنند و تعیین می‌کنند که چه کلماتی به صورت فوق‌متن هستند و پیوند آنها را با صفحات دیگر

---

[1]- امروزه تکنولوژی صفحات وب بسیار پیشرفت کرده است. صفحات وب امروزی ترکیبی از HTML، DHTML، JavaScript، VBScript و تکنولوژی‌های ASP، PHP، CGI، Aetivex، Applet، Flash و... است که صفحات وب را بسیار زیباتر، قدرتمندتر و کاربردی‌تر نموده است. برای کسب اطلاعات بیشتر می‌توانید به کتابهای طراحی صفحات وب مراجعه کنید.

مشخص می‌سازند. در شکل (۳-۷) و شکل (۴-۷) نمونه‌ای از یک صفحه وب و دستورالعمل‌های تشکیل دهنده آن را مشاهده می‌کنید.

شکل (۳-۷) یک صفحه وب

شکل (۴-۷) بخشی از کدهای تشکیل دهنده صفحه وب

۷-۱-۷ آشنایی با وب سایت (Web Site)

مجموعه‌ای از صفحات وب مرتبط به هم را که بر روی یک رایانه سرویس دهنده وب (Web Server) در شبکه اینترنت قرار داده شده است ، **وب سایت** می‌گویند. هر شخصی که به اینترنت دسترسی داشته باشد می‌تواند صفحات وب سایت را مشاهده نماید. معمولاً هر وب سایت متعلق به یک شخص ، گروه ، شرکت یا موسسه است. صفحات وب یک وب سایت از طریق فوق‌پیوند به یکدیگر متصل هستند.

۷-۱-۸ آشنایی با Home Page مرورگر

هنگامی که یک نرم‌افزار مرورگر را اجرا می‌کنیم، این نرم‌افزار بصورت پیش‌فرض به یک وب سایت متصل می‌شود که اصطلاحاً به آن صفحه اصلی (**Home Page**) مرورگر می‌گویند. هر کاربر می‌تواند وب سایت مورد نظر خود را به عنوان **Home Page** در نرم‌افزار مرورگر تعریف نماید. معمولاً کاربران وب سایتی را به عنوان **Home Page** تعریف می‌کنند که به آن سایت علاقه داشته و نیاز داشته باشند هر روز آن سایت را مشاهده نمایند.

۷-۱-۹ آشنایی با URL و نحوه آدرس دهی صفحات وب

امروزه اکثر شرکتها ، موسسات و حتی اشخاص در اینترنت ، وب سایت اختصاصی خود را دارند که در هرکدام از این سایتها تعداد زیادی صفحه وب وجود دارد. اگر یک کاربر بخواهد به یک وب سایت یا صفحه خاصی از یک وب سایت مراجعه کند، باید آدرس آن صفحه وب را داشته باشد. به همین منظور از (**U**niform **R**esource **L**ocator (**URL**) برای آدرس‌دهی هر منبع در اینترنت استفاده می‌شود که این منبع می‌تواند یک صفحه وب ، یک تصویر و ... باشد.

URL

به آدرس منحصر به فرد هر منبع در اینترنت ، **URL** می‌گویند.

مثال : URL زیر ، آدرس یک صفحه وب در سایت سازمان آموزش فنی و حرفه‌ای کشور است :

http://www.irantvto.com/index.htm

پروتکل — نام دامنه — صفحه وب

این آدرس URL از سه قسمت زیر تشکیل شده است:

- قسمت اول - پروتکل (http://)

عبارت **http://** مشخص می‌کند که پروتکل انتقال فایل‌ها در این سایت **Http** است.

- قسمت دوم - نام دامنه سایت (www.irantvto.com)

نام رایانه سرور میزبان سایت سازمان آموزشی فنی و حرفه‌ای کشور است که به قسمت **irantvto.com** آن حوزه یا دامنه (**Domain**) گفته می‌شود. هر شخص، شرکت یا سازمان می‌تواند نام حوزه مورد نظر خود را در اینترنت به ثبت برساند و برای خود سایت اینترنتی ایجاد نماید.

- قسمت سوم - نام منبع (صفحه وب index.htm)

index.htm نام صفحه اصلی وب سایت سازمان آموزش فنی و حرفه‌ای کشور است.

مکانیزم آدرس‌دهی فایلها در اینترنت مشابه مکانیزم آدرس‌دهی فایلها و پوشه‌ها در سیستم عامل ویندوز است. با این تفاوت که در آدرس‌دهی یک فایل در اینترنت از علامت / و در سیستم عامل ویندوز از علامت \ استفاده می‌شود.

وب نیز مانند دیگر سرویس‌های اینترنت بر اساس مدل سرویس گیرنده - سرویس دهنده کار می‌کند. سرویس دهنده، رایانه‌ای است در اینترنت که در آن صفحات وب ذخیره شده است و سرویس‌گیرنده همان نرم افزاری است که صفحات وب را دریافت کرده و نمایش می‌دهد.

۷-۱-۱۰ موتور جستجو (Search Engine)

شبکه اینترنت شامل میلیونها سایت و میلیاردها صفحه وب است. حال اگر بخواهیم در مورد یک موضوع خاص اطلاعاتی را بدست آوریم چگونه در این دریای اطلاعات مطالب مورد نظر خود را پیدا کنیم؟ موتورهای جستجو به کاربران شبکه اینترنت کمک می‌کنند تا سریعتر و بهتر مطالب مورد نظر خود را جستجو نمایند. موتورهای جستجو برای اینکه بتوانند اطلاعات کاملی در مورد همه سایتهای موجود در اینترنت داشته باشند، به صورت خودکار تمام سایتهای اینترنتی را مورد بررسی قرار می‌دهند و کلمات و عبارات موجود در این سایتها را در یک بانک اطلاعاتی عظیم نگهداری می‌کنند تا وقتی یک کاربر در مورد یک یا چند کلمه جستجو می‌نماید ، لیستی از صفحات وبی که این کلمات در آن قرار دارند را در اختیار کاربر قرار دهد. البته این سایتها بسیار هوشمند عمل می‌کنند و سعی می‌کنند از میان هزاران یا میلیونها صفحه‌ای که این کلمات در آن قرار دارند، بهترین و نزدیکترین صفحات را انتخاب کنند و آنها را به شما معرفی نمایند.

از آنجایی که سایتهای اینترنتی مرتباً تغییر می‌کنند و ممکن است صفحاتی از آنها حذف شود و یا صفحات جدیدی به آنها اضافه شود، موتورهای جستجو موظفند مرتباً خود را بروز رسانی کنند. البته موتورهای جستجو، اطلاعات همهٔ سایتهای وب را در اختیار ندارند ، به همین علت است که نتایج جستجو در سایتهای مختلف معمولاً متفاوت است. موتورهای جستجو معمولاً این امکان را به شما می‌دهند که وب سایت شخصی خود و یا وب سایت شرکت خود را به این موتورها معرفی کنید تا در آینده اگر کسی در موضوعات مربوط به شرکت شما جستجویی را انجام داد، موتور جستجو سایت شما را به عنوان یکی از سایتها معرفی نماید. به علت اینکه اطلاعات موجود در اینترنت روز به روز افزایش می‌یابد ، جستجو در آنها نیز سخت‌تر می‌شود به همین علت مهارت جستجو در اینترنت نیز به عنوان یک تخصص جدید مطرح است.

از معروفترین موتورهای جستجو می‌توان به سایتهای زیر اشاره کرد :

AltaVista	www.altavista.com	Excite	www.excite.com
Google	www.google.com	Hotbot	www.hotbot.com
MSN	www.msn.com	Yahoo	www.yahoo.com

۷-۱-۱۱ آشنایی با ISP

از آنجا که هزینه‌ها و تجهیزات ارتباطی اینترنت برای مصارف خانگی مقرون به صرفه نمی‌باشد لذا شرکت‌های خاصی با تدارک تجهیزات ماهواره‌ای نسبت به برقراری ارتباط با اینترنت اقدام می‌کنند.

این شرکت‌ها حق استفاده از اینترنت را در ساعات معینی تقسیم بندی کرده و بین مشتریان خود از طریق خطوط تلفن توزیع می‌کنند. به اینگونه شرکتها، ارائه کنندهٔ خدمات اینترنتی (**ISP**) (**Internet Service Provider**) گفته می‌شود. در شکل (۶-۷) نحوه عملکرد و استفاده از **ISP** را مشاهده می‌کنید.

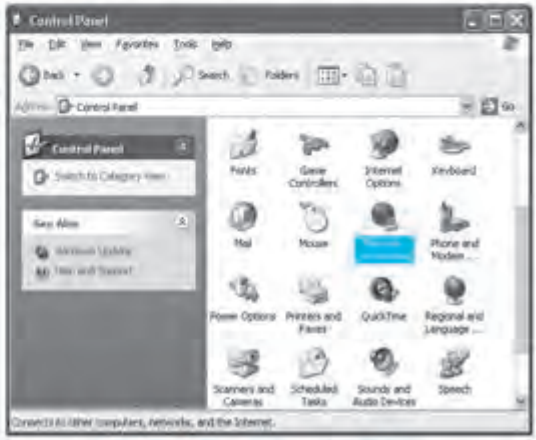
۷-۱-۲ آشنایی با اشتراک اینترنت (Account)

در کشور ما کاربران خانگی اغلب از طریق خط تلفن که اصطلاحاً **Dial-Up** گفته می‌شود به اینترنت وصل می‌شوند. برای این منظور می‌توانیم با خریداری کارتهای اعتباری مخصوص (کارت اینترنت) متعلق به یک شرکت ارائه دهنده خدمات اینترنتی (**ISP**)، نام کاربر (**Username**) و کلمهٔ عبور (**Password**) مخصوص خود را دریافت کنیم تا به کمک آن بتوانیم از طریق سایت شرکت مذکور به اینترنت متصل شویم. برای اتصال به سایت شرکت مذکور باید شمارهٔ تلفنهای ویژهٔ اینترنت آن شرکت را داشته‌باشیم (بر روی کارت این شماره درج شده است) کاربر پس از برقراری ارتباط تلفنی از طریق مودم رایانه خود با سایت شرکت و اعلام نام کاربر و کلمه عبور خود می‌تواند وارد اینترنت شده و از امکانات متنوع آن نظیر مشاهدهٔ سایت‌های گوناگون، پست الکترونیکی، گفتگوی زنده و ... استفاده کند.

۷-۲ تنظیمات اتصال به اینترنت

برای ایجاد یک ارتباط با اینترنت مراحل زیر را انجام می‌دهیم :

- در منوی start بر روی آیکن Control Panel کلیک می‌کنیم تا پنجره ***Control Panel*** باز شود.
- اگر این پنجره در حالت کلاسیک نیست در قسمت سمت چپ پنجره بر روی عبارت Switch to Classic View کلیک می‌کنیم.
- بر روی آیکن Network Connections دوبار کلیک می‌کنیم تا پنجره ***Network Connections*** ظاهر شود.



شکل ۷-۶ پنجره Control Panel

شکل (۷-۸) پنجره Network Connections

در این پنجره لیست ارتباطات ایجاد شده قبلی وجود دارد. برای ایجاد یک ارتباط جدید بر روی دستور Create a new connection کلیک می‌کنیم.

شکل (۷-۹) پنجره New Connection Wizard

پنجره ویزارد ایجاد ارتباط جدید، مطابق شکل ظاهر می‌شود. دکمه Next > را برای ادامه کار کلیک می‌کنیم.

شکل (۷-۱۰) پنجره New Connection Wizard

در پنجره بعدی امکان ایجاد ارتباط به اینترنت با شبکه محلی وجود دارد. گزینه Connect to the Internet را انتخاب کرده و دکمه Next > را کلیک می‌کنیم.

شکل (۷-۱۱) پنجره Make New Connection – قسمت سوم

در پنجره بعد گزینه *Setup my connection manually* را انتخاب کرده و دکمه Next > را برای ادامه کار کلیک می‌کنیم.

شکل (۷-۱۲) پنجره Make New Connection – قسمت چهارم

در پنجره بعد نحوه اتصال به اینترنت را مشخص می‌کنیم. از آنجایی که در کشور ما معمولاً اتصال به شبکه اینترنت از طریق شماره‌گیری **(Dial-up)** صورت می‌گیرد، گزینه *Connect Using a dial-up modem* را انتخاب کرده و دکمه Next > را کلیک می‌کنیم.

شکل (۷-۱۳) پنجره Make New Connection – قسمت پنجم

در این پنجره نام ارتباط را در محل مشخص شده وارد می‌کنیم. نام ارتباط هر نامی می‌تواند باشد و معمولاً نام **ISP** را که از آن برای ارتباط استفاده می‌کنیم ، وارد می‌نماییم. سپس دکمه Next > را کلیک می‌کنیم.

در پنجره بعدی شماره تلفن اتصال به شبکه (شماره تلفن **ISP**)را وارد می‌کنیم. پس از وارد کردن شماره تلفن، دکمه Next را کلیک می‌کنیم.

شکل (۲-۱۲۱) پنجره Make New Connection

در پنجره بعدی نام کاربری و کلمه عبور (درج شده روی کارت اینترنت) را در محل های مشخص شده وارد می‌کنیم. اگر در این پنجره نام کاربری و کلمه عبور را وارد نکنیم، هرگاه که بخواهیم به اینترنت متصل شویم، نام کاربری و کلمه عبور از ما پرسیده می‌شود. در این پنجره تنظیمات دیگری نیز وجود دارد که در شکل توضیح داده شده است. برای ادامه کار دکمه Next را کلیک می‌کنیم.

شکل (۲-۱۲۲) پنجره Make New Connection

در پنجره اتمام ایجاد ارتباط ، روی دکمه Finish برای اتمام کار کلیک می‌کنیم. (تنظیمات بیشتری را می‌توان روی ارتباط ایجاد شده انجام داد که این تنظیمات را در ادامه همین فصل فرا خواهیم گرفت)

شکل (۲-۱۲۳) پنجره Make New Connection

۷-۳ کار با مرورگر Internet Explorer

پس از آنکه یک ارتباط با اینترنت ایجاد کردیم درصورتیکه مرورگر **Internet Explorer** را اجرا نماییم، این مرورگر به کمک ارتباط ایجاد شده ، به اینترنت متصل می‌شود.

مرورگر Internet Explorer را از چند طریق می‌توان اجرا نمایید

- روی ایکن Internet Explorer در میز کار ویندوز دوبار کلیک می‌کنیم.
- در منوی Start روی ایکن Internet Explorer کلیک می‌کنیم.
- در نوار کار ویندوز و در قسمت **Quick Launch** که در کنار دکمهٔ Start قرار دارد، بر روی ایکن Internet Explorer کلیک می‌کنیم.

شکل (۷-۱۷) روشهای مختلف اجرای برنامهٔ IE

- بعد از اجرای مرورگر **IE** ، پنجرهٔ **Dial-Up Connection** برای اتصال به اینترنت ظاهر می‌شود. در این پنجره در قسمت **Connect to** نام ارتباطهایی که در پنجره **Network Connections** ایجاد کرده‌ایم، نشان داده می‌شود. **Connection** مورد نظر را از لیست انتخاب کرده و نام کاربری و کلمهٔ عبور به **ISP** که حق اشتراک را از آن تهیه کرده‌ایم، وارد می‌کنیم. دکمهٔ Connect را برای برقراری ارتباط با اینترنت کلیک می‌کنیم.

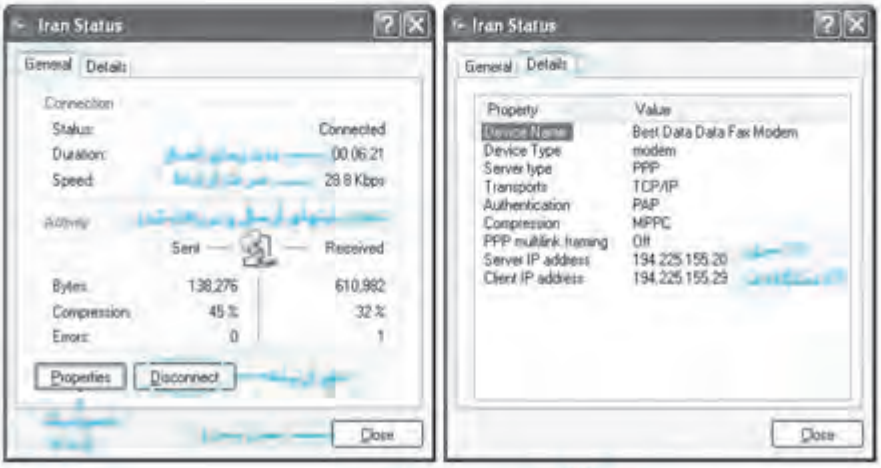
شکل (۷-۱۸) پنجرهٔ Dial-up Connection

- اگر در پنجرهٔ **Dial-Up Connection** گزینهٔ **Save Password** (ذخیرهٔ کلمه عبور) را فعال کنیم، در دفعات بعدی نیازی به وارد کردن کلمهٔ عبور نخواهیم داشت.
- اگر در پنجرهٔ **Dial-Up Connection** ، گزینهٔ **Connect automatically** (اتصال اتوماتیک) را انتخاب کنیم، در دفعات بعدی نیاز به کلیک کردن دکمهٔ Connect نبوده و عملیات اتصال بصورت اتوماتیک انجام می‌شود.

برای آنکه بتوانیم گزینه ***Connect automatically*** *را انتخاب کنیم، باید کلمه عبور را وارد کرده و سپس گزینه* ***Save Password*** *را انتخاب کنیم.*

پس از کلیک‌کردن دکمهٔ Connect، ابتدا شماره‌گیری انجام شده و سپس ارتباط با سرویس دهنده اینترنت برقرار می‌شود. سپس نام کاربری و کلمهٔ عبور توسط سرویس دهنده بررسی شده و در صورت داشتن مجوز عبور، امکان ارتباط با اینترنت از طریق **ISP** برقرار می‌شود. پس از برقراری ارتباط با اینترنت، مرورگر **IE** به صورت اتوماتیک به صفحه آغازین (**Home Page**) پیش فرض متصل می‌شود که معمولاً این صفحه آغازین سایت **Microsoft** است. نحوهٔ تعریف **Home Page** را در ادامه همین فصل خواهیم دید.

پس از اتصال به اینترنت آیکن در قسمت سمت راست نوار کار (ناحیه **System Tray**) ظاهر می‌شود که آیکن دو رایانه کوچک را نمایش می‌دهد. این آیکن نمایانگر برقراری ارتباط با اینترنت است. هنگامی که این آیکن روشن و خاموش می‌شود نمایانگر آنست که اطلاعات در حال ارسال و دریافت است. (روشن شدن رایانه پایین یعنی ارسال اطلاعات و روشن شدن رایانه بالایی یعنی دریافت اطلاعات) اگر روی این آیکن دو بار کلیک کنیم پنجرهٔ وضعیت ارتباط ظاهر می‌شود که در آن سرعت اتصال، مدت زمان اتصال و تعداد بایتهای ارسال شده و دریافت شده را نمایش می‌دهد. هرگاه بخواهیم ارتباط با اینترنت را قطع کنیم، دکمهٔ Disconnect را از این پنجره کلیک می‌کنیم. سربرگ **Details** توضیحات بیشتری را در مورد اتصال به اینترنت نمایش می‌دهد و دکمهٔ Close باعث پنهان شدن این پنجره می‌گردد.



نکته: روش دیگری برای اتصال به اینترنت وجود دارد. این روش به صورت زیر است :

- در منوی Start روی آیکن Connect To کلیک می‌کنیم.
- لیستی از ارتباطات ایجاد شده برای اتصال به اینترنت نمایش داده می‌شود. بر روی ارتباط مورد نظر کلیک می‌کنیم.
- پنجره *Dial-up Connection* مطابق شکل (۱۹-۷) ظاهر می‌شود.
- ادامه عملیات اتصال به اینترنت مشابه روش قبلی است.
- پس از اتصال به اینترنت مرورگر **IE** را اجرا می کنیم.

۷-۳-۱ آشنایی با پنجره اصلی Internet Explorer

نرم‌افزار **Internet Explorer** از قسمت های زیر تشکیل شده است:

شکل (۷-۳۰) پنجره اصلی IE

۷-۳-۱-۱ نوار عنوان (Title bar)

همانند اکثر برنامه‌های ویندوز، پنجره **IE** نیز نوار عنوان استاندارد ویندوز را دارد. در قسمت سمت چپ نوار عنوان، عنوان صفحه‌ای که هم اکنون در پنجره نمایش داده می‌شود، نوشته شده است. به عنوان مثال اگر سایت **Google** را مشاهده کنیم، نوار عنوان به صورت **Google - Microsoft Internet Explorer** نشان داده می‌شود. (عبارت **Microsoft Internet Explorer** در انتهای همهٔ عنوان‌ها می‌آید.)

۷-۳-۱-۲ نوار منو (Menu bar)

این نوار شامل منوهای **File** (پرونده)، **Edit** (ویرایش)، **View** (نمایش)، **Favorites** (مطلوب)، **Tools** (ابزار) و **Help** (راهنما) می‌باشد که با کاربرد آنها در ادامه همین فصل آشنا خواهیم شد.

شکل (۷-۲۱) نوار منو

۷-۳-۱-۳ نوار ابزارها (Toolbars)

سه نوار ابزار زیر در پنجرهٔ **IE** مشاهده می‌شود:

- نوار ابزار دکمه‌های استاندارد (Standard Buttons)
- نوار ابزار آدرس (Address)
- نوار ابزار پیوندها (Links)

در ادامه با عملکرد دکمه‌های این نوار ابزارها آشنا می‌شویم.

۷-۳-۱-۳-۱ نوار ابزار دکمه‌های استاندارد (Standard Buttons)

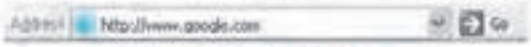
در شکل (۷-۲۲) نوار ابزار دکمه‌های استاندارد را مشاهده می‌کنید. این نوار ابزار بصورت پیش‌فرض در پنجره **IE** نمایش داده می‌شود.

شکل (۷-۲۲) نوار ابزار دکمه‌های استاندارد

در جدول (۷-۱) عملکرد هر یک از دکمه‌های نوار ابزار استاندارد را مشاهده می‌کنید. در ادامه همین فصل با نحوه کار این دکمه‌ها بیشتر آشنا می‌شویم.

۷-۳-۱-۳-۲ نوار ابزار Address

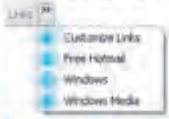
محل ورود آدرس **URL** صفحات وب است. با واردکردن آدرس صفحهٔ وب در این قسمت و فشردن کلید **Enter** یا کلیک‌کردن روی دکمه Go که در کنار آن قرار دارد، می‌توانیم صفحهٔ وب مورد نظر را دریافت کرده و آن را در پنجره **IE** مشاهده کنیم.



شکل (۷-۲۳) نوار ابزار Address

۷-۳-۹-۳-۳ نوار ابزار Links (پیوندها)

لیستی از خدمات و امکانات و سایتهای مربوط به مایکروسافت، به صورت یک نوار ابزار بنام **Links** در مرورگر **IE** قرار داده شده است. با کلیک‌کردن علامتی که در کنار نوار ابزار **Links** قرار دارد لیست **Link** ها باز می‌شود و با کلیک‌کردن روی هر آیتم به صفحهٔ وب مربوط به آن متصل می‌شویم.



شکل ۷-۳۴ منوی Links

دکمه	نام	عملکرد
Back	عقب	برای مراجعه به صفحات وب مشاهده شده قبلی استفاده می‌شود. اگر دکمهٔ **Back** غیرفعال باشد، یعنی صفحهٔ مشاهده شده قبلی در پنجره فعلی وجود ندارد.
Forward	جلو	عملکرد دکمهٔ **Forward** مشابه دکمهٔ **Back** است با این تفاوت که با دکمهٔ **Forward** حرکت به سوی جلو داریم. اگر دکمهٔ **Forward** غیرفعال باشد، یعنی این صفحه آخرین صفحه است و صفحه بعدی وجود ندارد.
Stop	توقف	برای توقف عملیات دریافت یک صفحهٔ وب ، از این دکمه استفاده می‌کنیم.
Refresh	فراخوانی مجدد	صفحه‌ای که هم اکنون در پنجره **IE** نمایش داده شده است را مجدداً فراخوانی می‌کند.
Home	صفحه آغازین	صفحهٔ وب سایت پیش فرض را در پنجره **IE** نمایش می‌دهد.
Search	جستجو	امکان انواع جستجو را در اینترنت می‌دهد و می‌توان یک صفحهٔ وب، آدرس شخص یا هر موضوع دیگری را توسط این دکمه جستجو کرد.
Favorites	سایتهای مورد علاقه	آدرس سایتهای مورد علاقه در پوشه‌ای به نام **Favorites** نگهداری می‌شود. برای مشاهدهٔ این پوشه و اتصال به سایتهای مطلوب از دکمهٔ **Favorites** استفاده می‌شود.
History	تاریخچه	همه صفحات وبی که در مرورگر **IE** مشاهده می‌کنیم بر روی دیسک سخت ذخیره می‌گردد تا کاربر بتواند صفحات و سایتهایی را که قبلاً مشاهده کرده است ، مجدداً مشاهده نماید. مشاهده این صفحات به کمک دکمه **History** انجام می‌شود.
Print	چاپ	صفحه وبی را که در پنجرهٔ فعلی نمایش داده می‌شود، چاپ می‌کند.

جدول ۷-۱۶ دکمه‌های نوار ابزار استاندارد

۲-۳-۱-۴ پنجره نمایش صفحه وب

در پایین نوار منو و نوار ابزارها، پنجره نمایش محتویات صفحات وب قرار دارد. در این قسمت صفحهٔ وبی که آدرس آن در قسمت نوار آدرس تایپ شده است، نمایش داده می‌شود. اگر صفحهٔ وب نمایش داده شده، بیش از یک صفحه باشد، نوار پیمایش **(Scroll bar)** در کنار این پنجره نمایش داده می‌شود که با بالا و پایین بردن این نوار توسط ماوس یا توسط کلیدهای جهت دار صفحه کلید، می‌توان کل صفحهٔ وب را مشاهده کرد.

۲-۳-۱-۵ نوار وضعیت (Status Bar)

نوار وضعیت در پایین‌ترین قسمت از پنجره **IE** قرار دارد. نوار وضعیت، در حالتهای مختلف، متن‌های مختلفی را نمایش می‌دهد. اما مهمترین کاربرد نوار وضعیت آن است که می‌توان آدرس پیوند یک فوق متن یا یک تصویر را در آن مشاهده کرد. هنگامی که اشاره‌گر ماوس را روی یک فوق متن می‌بریم، در نوار وضعیت آدرس پیوند صفحهٔ وبی که با کلیک کردن روی این فوق متن به آن متصل می‌شویم، نمایش داده می‌شود. این امکان به ما کمک می‌کند قبل از آنکه به یک پیوند مراجعه نماییم اطلاع پیدا کنیم که آن پیوند در کدام سایت است و از چه نوعی است مثلاً متوجه شویم که این پیوند ما را به یک صفحه وب متصل می‌کند یا به یک فیلم و یا یک تصویر.

در نوار وضعیت قسمتی برای نمایش وضعیت ارتباط با اینترنت در نظر گرفته شده است که اگر ارتباط با اینترنت قطع باشد یا اصطلاحاً در حالت **Offline** باشیم آیکن نمایش داده می‌شود.

شکل ۲-۳-۱-۴ نوار وضعیت

۲-۳-۲ شناسایی اصول دسترسی به یک آدرس وب

پس از اتصال به اینترنت، برای دسترسی به یک وب سایت به صورت زیر عمل می‌کنیم :

- روی آیکن Internet Explorer در محیط کار ویندوز دوبار کلیک می‌کنیم.
- آدرس *URL* سایت را در قسمت Address Go تایپ می‌کنیم.
- کلید *Enter* را می‌زنیم یا بر روی Go کلیک می‌کنیم تا پس از مدت کوتاهی وب سایت بر روی صفحه ظاهر شود.