وظایف اصلی 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.

ویژگی‌های اصلی پروتکل **NetBEUI** عبارتند از :

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

۵-۶-۴ 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.

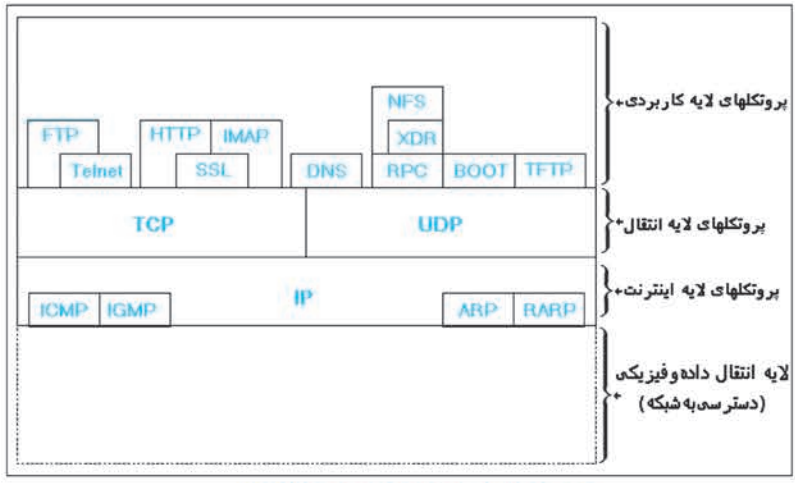
NWLink نمی‌تواند مستقیماً به رایانه‌هایی که با ویندوز کار می‌کنند اجازهٔ دسترسی به سرویس‌های به اشتراک گذاشتن فایل و چاپگر را بدهد. بلکه برای این منظور باید از سرویس‌هایی مانند **CSNW** و **GSNW** به ترتیب در ویندوزهای **Professional** و **Server** استفاده کرد.

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

۸-۵ 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.

مهم ترین سرویس‌های **TCP/IP** 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 بـه وسـیله **Telnet** بـه یـک رایانـه متصل به اینترنت (رایانه میزبان (**Host**)) دسترسی پیدا کنند و برنامه مورد نظـر خـود را بـر روی آن رایانه اجرا کنند. در این صورت رایانه شخصی خودشان مبدل بـه یـک پایانـه 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 یـک رایانـه 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 محاوره و برقراری محاوره 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 می‌کنند؟

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

۶-۱ 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.

۶-۲ 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 :

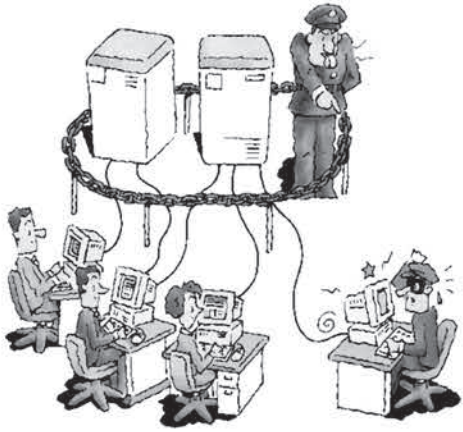
- طبقه‌بندی منابع اطلاعاتی و دسترسی کاربران مختلف به این منابع با توجه به سطح اختیارات آنها (مانند: دسترسی کاربرانی خاص به چاپگر یا گزارشات خاصی از برنامه‌های کاربردی)
- دسترسی کاربران به منابع اطلاعاتی در شبکه یا اینترنت از طریق کلمهٔ عبور
- عدم استفاده از حافظه‌های جانبی قابل حمل در شبکه (مانند: دیسک 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.

مهم ترین 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**



شکل (۱-۶) امنیت شبکه

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.

۶-۴-۱ 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**

۶-۴-۲ 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.**

۶-۵ 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
Netware	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 2000	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 (۱-۶)مجوزهای دسترسی شبکه

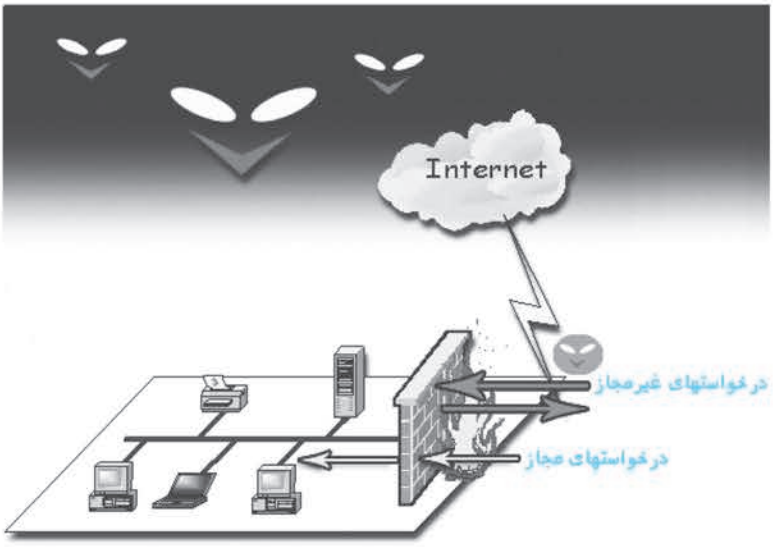
در شبکه‌های **Client-Server** اطلاعات تمام کاربران بصورت متمرکز در یک رایانه نگهداری می‌شود و مدیر شبکه می‌تواند بصورت متمرکز دسترسی کاربران مختلف را به منابع مختلف موجود در شبکه از طریق سطح امنیتی کاربر تعیین کند **(Single Sign On)**.

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.

۶-۶ 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.



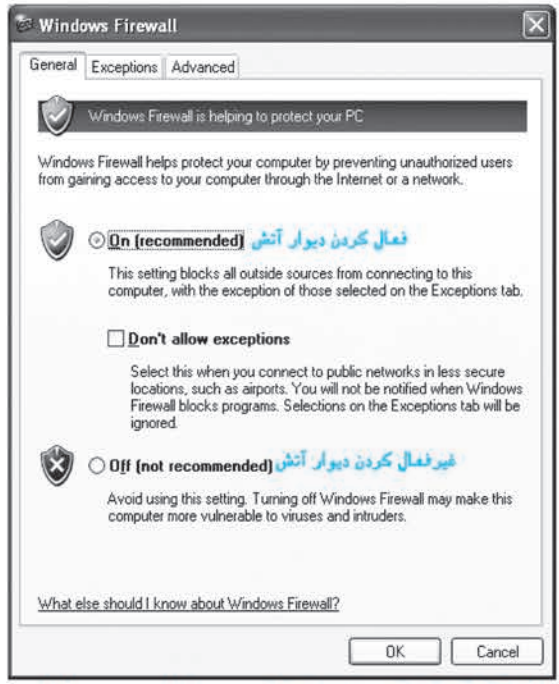
شکل (۲-۶) دیوار آتش درخواستهای مجاز را عبور می‌دهد و درخواستهای غیر مجاز را بازمی‌گرداند.

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.*



شکل (۳-۶) فعال کردن یا غیرفعال کردن دیوار آتش ویندوز XP

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 -روش محافظت با کلمهٔ عبور چگونه امنیت شبکه را برقرار می‌کند ؟
۵ -ویندوز از چه مدل‌های امنیتی برای شبکه استفاده می‌کند ؟ توضیح دهید.
۶ -استفاده از پروتکل‌های 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 تمهیدات 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 عامل‌های 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 ، فراپیوند ، 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 شبکهٔ 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 (۱-۷) شبکهٔ 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 عنصری از همان صفحه یا صفحه وب دیگر را فراپیوند می‌گوییم.

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 می‌کنیم.**
- **یک فایل را اجرا می‌کند.**

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

فوق متن (Hypertext)

اگر پیوند دو صفحه وب از طریق متن باشد ، به این پیوند ، فوق متن می‌گوییم.

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.

فوق رسانه (Hypermedia)

اگر پیوند دو صفحه وب از طریق تصویر، صدا و یا انیمیشن باشد ، به این پیوند ، فوق رسانه می‌گوییم.

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) 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.

شکل (۲-۷) نمونهٔ صفحه وب (معرفی کشور ایران)

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 در خواست **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**، **VBScript**، **JavaScript** و تکنولوژی‌های **ASP**، **PHP** ، **CGI**، **Activex**، **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.