



پودمان ۲

راه اندازی شبکه

حجم زیاد مبادله داده‌های تحت شبکه در شرکت‌ها و سازمان‌ها، مدیریت، نگهداری و پشتیبانی آنها را دشوار می‌کند. بنابراین باید برای امنیت و کاهش هزینه‌های دسترسی به داده‌ها راهکارهای مناسب صورت بگیرد. برای این منظور از روش‌های استاندارد مدیریت ارتباطات رایانه‌ای برای تبادل و پردازش داده‌ها استفاده می‌شود و با نظارت بر روش اتصال رایانه‌ها به یکدیگر و برقراری ارتباط امن بین آنها می‌توان علاوه بر مدیریت داده‌ها، دسترسی کاربران مختلف را مدیریت کرد. در سیستم عامل ویندوز امکانات عمومی برای اشتراک داده‌ها و مجوز دسترسی تعبیه شده است و مدیران شبکه با انجام تنظیمات در محیط این سیستم عامل ارتباط بین رایانه‌هایی را که به وسیله سخت‌افزار شبکه به یکدیگر متصل شده‌اند، نظارت می‌کنند و با استفاده از ویژگی‌های نرم‌افزاری مانند اشتراک گذاری داده‌ها و تنظیم مجوزها، داده‌ها را با حفظ امنیت آنها در اختیار کاربران قرار می‌دهند. در این پودمان در دو واحد یادگیری هنرجو با اتکا به دانش و مهارت قادر خواهد بود تنظیمات و پیکربندی شبکه، مدیریت اشتراک گذاری داده‌ها و نحوه دسترسی و اعمال مجوز روی داده‌ها را در سیستم عامل ویندوز انجام دهد و سرویس‌های DHCP و DNS را در سیستم عامل سرور راه اندازی کند.

واحد یادگیری ۲

شایستگی راه‌اندازی شبکه گروه کاری

آیا تا به حال پی برده‌اید

- چگونه کاربران یک شبکه رایانه‌ای می‌توانند با یکدیگر در ارتباط باشند؟
- برای در اختیار قراردادن همه بخش‌نامه‌ها و اسناد به کارمندان در یک اداره، چه باید کرد؟
- چگونه می‌توان برای بخش‌های مختلف یک سازمان شبکه‌های مستقل ایجاد کرد؟
- چرا دسترسی کاربران مختلف در شبکه باید متفاوت باشد؟

هدف از این واحد شایستگی ایجاد شبکه گروه کاری و مدیریت منابع در آن است.

استاندارد عملکرد

راه‌اندازی شبکه‌های p2p و ایجاد زیرشبکه و اشتراک‌گذاری منابع در سیستم‌عامل

پروتکل



تصور کنید شما در میدان اصلی شهر با یک مسافر خارجی برخورد کرده‌اید و می‌خواهید با یکدیگر صحبت کنید، چه اتفاقی خواهد افتاد؟ قطعاً از صحبت‌های هم چیزی نخواهید فهمید؛ زیرا زبان هر کشور الفبا، مفاهیم و دستور زبان خاص خود را دارد. بنابراین برای گفتگو باید هر دو طرف مکالمه، قوانین یکسانی داشته باشند، در غیر این صورت امکان برقراری ارتباط وجود نخواهد داشت.

این مشکل دقیقاً درباره رایانه‌های یک شبکه هم وجود دارد. رایانه‌ها برای ارتباط با یکدیگر احتیاج به یک زبان مشترک دارند. همانند هر روش ارتباطی دیگر، رایانه‌های شبکه براساس مجموعه‌ای از قوانین عمل می‌کنند تا ارسال، دریافت و ترجمه پیام‌ها امکان‌پذیر باشد. به مجموعه قوانین و قراردادهای که تعیین می‌کنند چگونه رایانه‌های درون یک شبکه با هم ارتباط برقرار کنند پروتکل (Protocol) گفته می‌شود.

برای انتقال داده‌ها در شبکه، داده‌ها به بسته‌های کوچکی به نام Packet تقسیم می‌شوند. شیوه تقسیم‌بندی، ارسال، جمع‌بندی مجدد بسته‌های ارسالی در مقصد، کنترل زمان تبادل اطلاعات، تعیین قالب انتقال داده‌ها، بررسی خطاهایی که هنگام نقل و انتقال در داده‌ها پیش می‌آید، تصحیح خطا و فشرده‌سازی داده‌ها از وظایف پروتکل است. برای ارتباط در شبکه پروتکل‌های متعددی وجود دارند که از نظر سرعت، قابلیت اطمینان، سادگی و ... با یکدیگر تفاوت دارند؛ اما مسئله مهم این است که دو طرف ارتباط، از پروتکل یکسان استفاده کنند و زبان هم را بفهمند. یکی از مهم‌ترین و مشهورترین پروتکل‌های مورد استفاده در شبکه‌های امروزی پروتکل TCP/IP است که نه تنها روی اینترنت و شبکه‌های گسترده گوناگون کاربرد دارد، بلکه در شبکه‌های محلی نیز مورد استفاده قرار می‌گیرد.

پروتکل اینترنت (Internet Protocol)

پروتکل اینترنت، ترتیب و تحویل بسته‌ها در شبکه را کنترل می‌کند. در هر بسته، آدرس مبدأ (source address) و آدرس مقصد (destination address) وجود دارد. این پروتکل باید به وسیله سیستم‌عامل پشتیبانی شود.

به کمک کتاب همراه هنرجو، فهرست سیستم‌عامل‌هایی را بنویسید که از پروتکل TCP/IP پشتیبانی می‌کنند.

در کارگاه رایانه هنرستان، نوع و نسخه سیستم‌عامل رایانه‌ها را به وسیله دستور winver بررسی کنید.

گره (Node)، میزبان (Host) و آدرس IP از اصطلاحات شبکه هستند.

گره (Node): دستگاهی که روی آن می‌توان آدرس شبکه را به صورت منحصر به فرد تنظیم کرد. مانند مسیریاب

میزبان (Host): گره‌ای که در ارتباطات شبکه به عنوان مبدأ یا مقصد تعیین می‌شود. مانند رایانه

برای تعیین آدرس رایانه‌ها از دو ویژگی آدرس IP و نام رایانه استفاده می‌شود.

آدرس (IP): یک شناسه عددی است که به هر دستگاهی در شبکه اختصاص داده می‌شود. همان طور که کدپستی شما مشخص می‌کند که خانه شما کجا قرار دارد، آدرس IP موقعیت دستگاه را در شبکه مشخص

کنجکاوی



فعالیت گروهی



می‌کند. برای مثال آدرس IP تارنمای یاهو 98.138.219.232 و اداره کل نظارت بر نشر و توزیع مواد آموزشی 37.228.138.195 است.

کارگاه ۱ مشاهده اطلاعات پیکربندی اتصالات شبکه

به وسیلهٔ واسط گرافیکی یا دستورات خط فرمان می‌توان اطلاعات پیکربندی شبکه را مشاهده کرد.

● مشاهده اطلاعات پیکربندی اتصالات شبکه به وسیلهٔ واسط گرافیکی

۱ پنجره تنظیمات شبکه را باز کنید.

در منوی شروع روی گزینه Settings و سپس Network & Internet کلیک کنید. در این پنجره گزینه‌های مختلفی وجود دارد که امکان مشاهده پیکربندی اتصالات شبکه را فراهم می‌کند.

۲ اطلاعات پیکربندی شبکه‌ای که به آن متصل هستید

را بررسی کنید.

گزینه View your network properties را انتخاب کنید

(شکل ۱).

فهرست مشخصاتی که برای هر یک از اتصالات شبکه نمایش داده می‌شود را یادداشت کنید.



شکل ۱- پنجره تنظیمات Network & Internet

سایر روش‌ها و گزینه‌های مربوط به پیکربندی اتصالات شبکه در پنجره Network & Internet را بررسی کرده، به صورت گروهی برای هم‌کلاسی‌های خود ارائه دهید.

فعالیت گروهی



● مشاهده اطلاعات پیکربندی اتصالات شبکه به وسیله خط فرمان

یکی از دستورات مهم در نمایش اطلاعات شبکه و عیب‌یابی، دستور ipconfig است. این دستور اطلاعاتی در مورد پیکربندی اتصالات شبکه رایانه نمایش می‌دهد.

۳ پنجره خط فرمان را باز کنید.

در کادر Run، cmd را تایپ کرده، با کلیک دکمه OK به محیط دستوری ویندوز وارد شوید. کادر Run را با کلید ترکیبی win+R نیز می‌توانید باز کنید.

۴ دستور ipconfig را اجرا کنید.

فهرست مشخصات نمایش داده شده برای هر یک از اتصالات شبکه را یادداشت کرده (شکل ۲)، با فهرست روش واسط گرافیکی مقایسه کنید.

۵ دستور ipconfig/all را اجرا کنید و نتیجه را با

مرحله ۴ مقایسه کنید.



شکل ۲- اجرای دستور ipconfig بدون پارامتر

با استفاده از پارامتر /all در دستور ipconfig اطلاعات کامل پیکربندی مربوط به همه اتصالات شبکه رایانه نمایش داده می‌شود. فهرست مشخصات نمایش داده شده برای هر یک از اتصالات شبکه را یادداشت کرده، با فهرست روش واسط گرافیکی مقایسه کنید.

نام رایانه

کاربران به‌جای آدرس IP بیشتر از نام رایانه برای برقراری ارتباط در شبکه استفاده می‌کنند تا به راحتی به رایانه‌ها و منابع شبکه دسترسی داشته باشند. سیستم‌عامل ویندوز ۱۰ از دو نوع نام استفاده می‌کند:

● **NetBIOS Name**: هنگام نصب سیستم‌عامل یک نام حداکثر ۱۵ نویسه‌ای به رایانه داده می‌شود که باید در شبکه داخلی منحصر به فرد بوده، تکراری نباشد به این نام، Computer name یا NetBIOS Name می‌گویند. از این نام امروزه کمتر استفاده می‌شود.

● **میزبان (Host name)**: رشته‌ای به طول حداکثر ۲۵۵ نویسه است که می‌تواند شامل حروف الفبا، ارقام ۰ تا ۹، نقطه و خط تیره (hyphen) باشد.

در رایانه‌های شبکه گروه کاری (Workgroup) این نام با NetBIOS Name که هنگام نصب سیستم‌عامل به رایانه اختصاص می‌یابد، یکی است. این نام را می‌توان از طریق پنجره ویژگی‌های سیستم (System Properties) مشاهده کرد و در صورت نیاز تغییر داد.

نام رایانه باید در شبکه یکتا باشد در غیر این صورت هنگام مدیریت و کنترل رایانه‌ها دچار مشکل می‌شوید.

یادداشت



کارگاه ۲ نمایش و تغییر نام رایانه

در این کارگاه قصد داریم با استفاده از واسط گرافیکی ویندوز و به کمک دستور در خط فرمان، نام رایانه را مشاهده کنیم. **۱ پنجره ویژگی‌های رایانه را باز کنید.**

روی نماد This PC راست کلیک کنید و گزینه Properties را انتخاب کنید. کلید میانبر این پنجره را در کتاب همراه هنرجو جست‌وجو کنید.

۲ نام رایانه را مشاهده کنید.

گزینه Change Setting را کلیک کنید. نام رایانه در شکل ۳ قابل مشاهده است.

۳ نام رایانه را تغییر دهید.

دکمه Change را انتخاب کنید. در کادر Computer name، نام جدید را وارد کرده، دکمه OK را کلیک کنید (شکل ۳). برای اعمال تغییر نام، رایانه را راه‌اندازی مجدد کنید.

۴ نام میزبان را با استفاده از دستور hostname مشاهده کنید.

دستور hostname را در محیط دستوری ویندوز تایپ کنید (شکل ۴).



شکل ۳- تغییر نام رایانه



شکل ۴- نتیجه اجرای دستور hostname

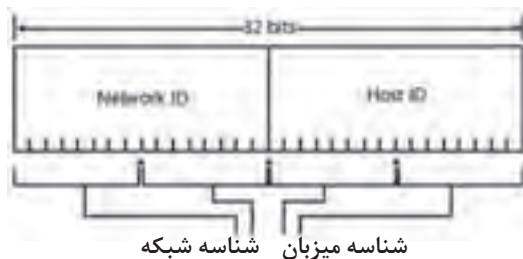
انواع IP

پروتکل اینترنت دارای دو نسخه ۴ (IPv4) و نسخه ۶ (IPv6) است. IPv4 نسخه اولیه برای استفاده در شبکه‌ها و اینترنت است که به وسیله سیستم‌عامل‌های مختلف پشتیبانی می‌شود و هنوز به دلیل گستردگی و سادگی کاربرد دارد. IPv6 از ویندوز Vista و server2008 به بعد به وسیله سیستم‌عامل‌های مایکروسافت پشتیبانی می‌شود و نسبت به IPv4 نیاز به تنظیمات کمتری دارد و پیکربندی آن ساده‌تر است.

پروتکل اینترنت نسخه ۴ (IPv4)

آدرس IPv4 یک عدد ۳۲ بیتی است که به بخش‌های ۸ بیتی تقسیم می‌شود. به هر بخش یک Byte یا Octet می‌گویند. هر بایت به صورت یک عدد دهدهی بین صفر تا ۲۵۵ نمایش داده می‌شود و با نقطه از یکدیگر جدا می‌شوند. مانند 192.168.100.138

روش آدرس دهی بیش از آنکه فقط یک روش برای شناسایی میزبان باشد، روشی برای پیدا کردن آن است. فرض کنید می‌خواهید برای دوستان نام‌های ارسال کنید، برای این کار نیاز به کدپستی دارید. کدپستی یک عدد ۱۰ رقمی است که شامل دو بخش است: ۵ رقم اول نشانگر کد رهسپاری (مشخصه شهر مقصد) و ۵ رقم دوم بیانگر کد توزیع (مشخصه مکانی مقصد) است. بدین ترتیب به وسیله کدپستی نامه شما به دست دوستان خواهد رسید. اگر آدرس IP را به کدپستی تشبیه کنیم، باید این آدرس هم شبکه و هم رایانه را مشخص کند تا بتوانیم به کمک آن رایانه مورد نظر را در شبکه پیدا کنیم و اطلاعات خود را برای آن بفرستیم.



آدرس IP به دو بخش تقسیم می‌شود: شناسه شبکه (Network ID) و شناسه میزبان (Host ID).

شناسه شبکه: بخش اول آدرس IP است که آدرس شبکه را مشخص می‌کند، به صورتی که بتوان یک شبکه را در بین سایر شبکه‌ها شناسایی کرد.

شناسه میزبان: بخش دوم آدرس IP است که مشخص کننده میزبان در شبکه است (شکل ۵).

شکل ۵- شناسه شبکه و شناسه میزبان در آدرس IP

همان‌طور که هر شهر کد رهسپاری مخصوص به خود دارد که در کدپستی خانه‌های آن شهر استفاده می‌شود، هر شبکه نیز شناسه مخصوص به خود دارد؛ بنابراین همه میزبان‌های یک شبکه، شناسه شبکه یکسانی دارند. شناسه میزبان، شناسه منحصر به فرد هر میزبان در یک شبکه است.

دو رایانه در دو شبکه مختلف می‌توانند شناسه میزبان یکسان داشته باشند.

یادداشت



سؤال این است که بخش شبکه و میزبان در آدرس IPv4 چگونه شناسایی و از یکدیگر جدا می‌شوند؟

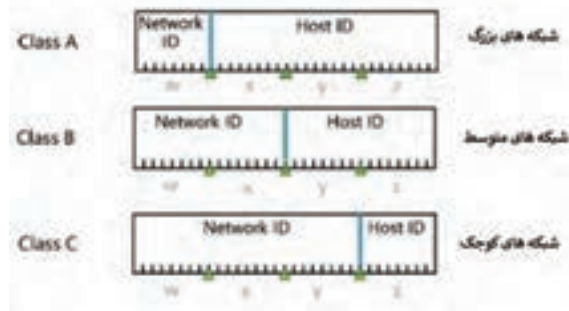
برای پاسخ به این سؤال باید با مفاهیم کلاس‌های آدرس IP و Subnet Mask آشنا شویم.

یکی از مشکلات طراحی اینترنت، تنوع شبکه‌ها و تعداد رایانه‌های هر شبکه بود. بنابراین باید به شکلی آدرس IP را طراحی می‌کردند که بتواند شبکه‌هایی با اندازه‌های مختلف را پشتیبانی کند؛ به این ترتیب دسته‌بندی آدرس‌های IP (Classful IP Addressing) شکل گرفت که به وسیله سازمان غیرانتفاعی IANA (Internet Assigned Numbers Authority) تعریف و پشتیبانی می‌شود. کلاس‌ها تعداد شبکه‌های قابل تعریف و تعداد دستگاه‌های عضو هر شبکه را با تقسیم‌بندی بایت‌های آدرس IP بین شناسه شبکه و شناسه میزبان مشخص می‌کنند.

اگر آدرس IP را به صورت w.x.y.z در نظر بگیریم، این دسته‌بندی براساس بایت اول (w) به ۳ کلاس تقسیم می‌شود. جدول ۱ تعداد بیت‌های شناسه شبکه و شناسه میزبان، تعداد شبکه‌ها و میزبان‌های هر کلاس را نشان می‌دهد.

جدول ۱- کلاس‌های آدرس IP

کلاس	عدد بایت اول (دهدهی) (w)	تعداد بیت‌های شناسه شبکه	تعداد شبکه‌ها	تعداد بیت‌های شناسه میزبان	تعداد میزبان در هر شبکه
A	1-126	8	126	24	$(2^{24} - 2)$ 16,777,214
B	128-191	16	16,384	16	$(2^{16} - 2)$ 65,534
C	192-223	24	2,097,152	8	$(2^8 - 2)$ 254



شکل ۶- شناسه شبکه و میزبان در کلاس‌های آدرس IP

بیت‌های شناسه میزبان نمی‌توانند همگی صفر یا همگی ۱ باشند؛ بنابراین در جدول ۱ از تعداد میزبان‌ها مقدار ۲ کم شده است.

یادداشت



- برای هر یک از شبکه‌های شکل ۷ کلاس IP و شناسه شبکه را تعیین کنید. برای تشخیص کلاس آدرس IP کافی است عدد بایت اول آن را با جدول کلاس‌ها مقایسه کنید.
- شناسه میزبان را در آدرس IP میزبان‌ها تعیین کنید.
- آدرس IP میزبان‌ها را کامل کنید.

فعالیت کارگاهی



شکل ۷- چند شبکه با آدرس‌دهی IP در کلاس‌های متفاوت

آدرس های IP خاص

- آدرس 127.0.0.1 (loopback address): به عنوان آدرس داخلی رایانه تعریف شده است و از آن برای بررسی درستی پیکربندی پروتکل TCP/IP استفاده می شود.
 - آدرس شبکه: از این آدرس برای شناسایی شبکه استفاده می شود. بیت های شناسه میزبان در این آدرس همگی صفر هستند.
- مثال:

آدرس شبکه	شناسه میزبان	شناسه شبکه	کلاس	آدرس IP
164.31.0.0	54.10	164.31	B	164.31.54.10

- برای به دست آوردن آدرس شبکه بر اساس کلاس آدرس IP بیت های مربوط به شناسه شبکه و شناسه میزبان را مشخص می کنیم و سپس بیت های شناسه میزبان را صفر می کنیم.
- آدرس Broadcast: از این آدرس برای ارسال اطلاعات به همه رایانه ها در یک شبکه استفاده می شود. بیت های شناسه میزبان در این آدرس همگی ۱ هستند.

آدرس Broadcast	شناسه میزبان	شناسه شبکه	کلاس	آدرس IP
164.31.255.255	54.10	164.31	B	164.31.54.10

- برای به دست آوردن آدرس Broadcast یک شبکه بر اساس کلاس آدرس IP بیت های مربوط به شناسه شبکه و شناسه میزبان را مشخص کرده، سپس بیت های شناسه میزبان را ۱ قرار می دهیم.

آدرس IP رایانه ای در شبکه هنرستان 192.168.100.7 است. جدول زیر را تکمیل کنید.

آدرس Broadcast	آدرس شبکه	شناسه میزبان	شناسه شبکه	کلاس	آدرس IP
					192.168.100.7

علاوه بر کلاس های A، B و C دو کلاس D و E نیز تعریف شده است. مقدار w در کلاس D عددی در محدوده ۲۳۹-۲۴۴ و در کلاس E عددی در محدوده ۲۵۵-۲۴۰ است. کلاس D برای شناسایی گروهی (multicast) دستگاه ها در شبکه تعریف شده است بطوری که رایانه ها و برنامه ها بتوانند اطلاعات خود را به تمام دستگاه هایی ارسال کنند که وظایف خاصی انجام می دهند مانند ویدیو کنفرانس. همچنین کلاس E برای کارهای آزمایشگاهی تعریف شده است.

Subnet Mask

یک رشته دودویی ۳۲ بیتی است که به صورت ۴ عدد ده دهی تعریف می شود و برای جدا کردن شناسه شبکه از شناسه میزبان در آدرس IP به کار می رود. از بیت صفر برای بخش شناسه میزبان و بیت یک برای بخش

فعالیت
کارگاهی



شناسه شبکه استفاده می‌شود. جدول ۲ برای کلاس‌های IP مقدار Subnet Mask و تعداد بیت‌های تعیین کننده زیرشبکه (Subnet) را نشان می‌دهد.

جدول ۲- Subnet Mask کلاس‌های IP

کلاس	شناسه میزبان شناسه شبکه	Subnet Mask	Subnet Value
A	W.X.Y.Z	255.0.0.0	/۸
B	W.X.Y.Z	255.255.0.0	/۱۶
C	W.X.Y.Z	255.255.255.0	/۲۴

انواع آدرس IPv4

هر دستگاهی که بخواهد مستقیم به اینترنت وصل شود، نیاز به یک آدرس IP ثابت شده و منحصر به فرد دارد که به آن Public IPv4 Addressing می‌گویند. از آنجایی که IPv4 محدودیت آدرس دهی (۲^{۳۲}) دارد، امکان اختصاص آدرس Public برای همه کاربران و دستگاه‌های سازمان‌ها وجود ندارد. برای رفع این مشکل از آدرس دیگری به نام Private IPv4 Addressing استفاده می‌شود. از این آدرس برای رایانه‌های شبکه‌های خانگی و داخلی سازمان‌ها استفاده می‌شود که به شبکه متصل هستند؛ اما نیاز به اتصال به شبکه‌های عمومی مثل اینترنت ندارند. شبکه‌های داخلی می‌توانند از آدرس‌های Private استفاده کنند بدون اینکه نگران اختصاص آنها به شبکه‌های دیگر باشند. IANA مرجع اصلی برای معرفی و کنترل آدرس‌های Private و Public است (جدول ۳).

جدول ۳- آدرس‌های Private

کلاس	آدرس شروع	آدرس پایان
A	10.0.0.0	10.255.255.255
B	172.16.0.0	172.31.255.255
C	192.168.0.0	192.168.255.255

روش‌های اختصاص IP

برای اختصاص آدرس IPv4 به گره‌های شبکه از دو روش زیر استفاده می‌کنیم:

● Manual Configuration

در این روش اختصاص آدرس IP به صورت دستی انجام می‌گیرد. این آدرس ثابت است و به آن Static Address می‌گویند. یکی از کاربردهای آدرس‌های استاتیک تخصیص آدرس IP به رایانه‌های سرور است. اصلی‌ترین مشکل این روش نبودن آن است که باعث می‌شود زمان زیادی صرف تنظیم آدرس برای رایانه‌های شبکه شود، ضمن اینکه امکان درج آدرس اشتباه یا تکراری وجود دارد که ممکن است سبب تداخل و عدم اتصال به شبکه شود.

● (Dynamic Host Configuration Protocol) DHCP

سرورسی در سیستم‌عامل‌های سرورسی‌دهنده است که اختصاص آدرس IP و تنظیمات آن را به صورت خودکار روی

میزبان‌های شبکه خود انجام می‌دهد. به آدرس IP که به این روش اختصاص داده می‌شود Dynamic Address می‌گویند.

کارگاه ۳ تنظیم آدرس IP به صورت استاتیک

۱ پنجره Network And Sharing Center را باز کنید.

روی نماد شبکه در ناحیه اطلاع‌رسانی راست کلیک کنید و گزینه Open Network And Sharing Center را انتخاب کنید.

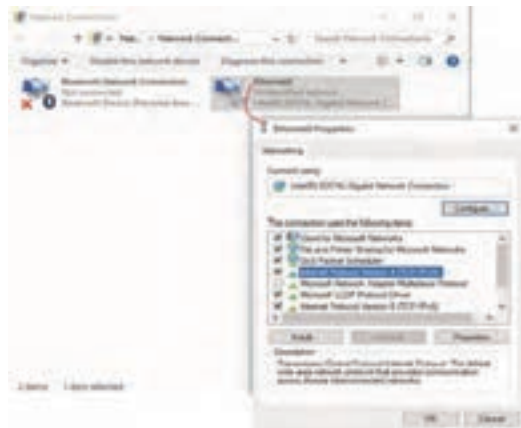


۲ پنجره تنظیمات کارت‌های شبکه را باز کنید.

روی گزینه Change Adapter Settings کلیک کنید، در پنجره باز شده همه اتصالات شبکه نمایش داده می‌شود.

۳ پنجره ویژگی اتصال موردنظر را باز کنید.

روی کارت شبکه راست کلیک کنید و گزینه Properties را انتخاب کنید.



۴ آدرس IP رایانه را تنظیم کنید.

روی Internet Protocol Version 4 (TCP/IPv4)

دابل کلیک کنید (شکل ۸).

شکل ۸- کادر مشخصات کارت شبکه



۵ تنظیم آدرس IP را در وضعیت static قرار دهید.

به‌طور پیش‌فرض کارت شبکه برای دریافت تنظیمات آدرس از حالت خودکار استفاده می‌کند. برای تنظیم آدرس IP به صورت استاتیک گزینه Use the following IP address را انتخاب کنید (شکل ۹).

۶ آدرس 192.168.100.Z را برای کارت شبکه تنظیم کنید.

Z را براساس شماره رایانه خود انتخاب کنید. با کلیک در کادر Subnet mask عدد 255.255.255.0 به‌صورت خودکار تنظیم می‌شود (شکل ۹).

شکل ۹- تنظیمات IP address و Subnet mask

۷ صحت عملکرد آدرس IP را بررسی کنید.

دستور `ping Ip-address` را تایپ کنید. به جای `Ip-address` آدرس یکی از رایانه‌های شبکه مانند 192.168.100.2 را درج کنید. دستور `ping`، برای عیب‌یابی و بررسی صحت ارتباط در شبکه به کار می‌رود.

پروتکل اینترنت نسخه ۶ (IPv6)

امروزه یکی از مهم‌ترین وظایف مدیران، آماده کردن شبکه سازمان برای استفاده از پروتکل اینترنت نسخه ۶ (IPv6) است. دلیل این امر رشد روزافزون اینترنت، نیاز به اتصال تلفن همراه به شبکه و کمبود فضای آدرس‌دهی IPv4 است. IPv6 نسبت به IPv4 مسیریابی مؤثرتر، پیاده‌سازی راحت‌تر و امنیت بیشتری دارد؛ اما بدون شک افزایش فضای آدرس‌دهی، مهم‌ترین ویژگی آن به حساب می‌آید. به‌همین منظور اکثر کشورهای دنیا در حال پیاده‌سازی IPv6 هستند به طوری که تا چند سال دیگر پروتکل IPv6 بستر اصلی اینترنت خواهد بود.

شکل ظاهری IPv6 و IPv6 نسبت به هم تفاوت دارد. آدرس‌های IPv4 به طول ۳۲ بیت هستند که از این جهت می‌توان حداکثر در حدود ۴ میلیارد آدرس در اختیار داشت. اما آدرس‌های IPv6 به طول ۱۲۸ بیت است که حداکثر 2^{128} (۳/۴ × ۱۰^{۳۸}) عدد آدرس در اختیار ما قرار می‌دهد که عدد بسیار بزرگی است. اگر هر آدرس را یک دانه شن در نظر بگیریم برای ذخیره آن به زمینی به وسعت خورشید نیاز داریم. این محدوده بسیار زیاد، این امکان را به ما می‌دهد که بتوانیم به هر کدام از دستگاه‌های واقع در شبکه، آدرس منحصر به فرد و **Public** اختصاص دهیم. آدرس‌های IPv6 به ۸ بخش ۱۶ بیتی تقسیم می‌شوند و هر بخش به‌وسیله علامت ":" از بخش دیگر جدا می‌شود. بر خلاف IPv4 که در مبنای ۱۰ نوشته می‌شود، IPv6 در مبنای ۱۶ نوشته می‌شود. IPv6 به صورت `XX:XX:XX:XX:XX:XX:XX:XX` است که هر X نشان‌دهنده یک بایت و به صورت دو رقم مبنای ۱۶ نمایش داده می‌شود. بنابراین هر بخش شامل ۴ رقم مبنای ۱۶ است.

به این مثال توجه کنید:
`21cd:0054:0000:0000:06dd:006e:af38:8d63`
 می‌توان آدرس IPv6 را با حذف صفرهای ابتدایی هر بخش، ساده کرد. با این شرط که حداقل یک رقم در آن بخش نوشته شود. بنابراین خواهیم داشت:

`21cd:0054:0000:0000:06dd:006e:af38:8d63` → `21cd:54:0:0:6dd:6e:af38:8d63`

همچنین در صورت وجود یک یا چند بخش با مقدار صفر مجاور هم، می‌توان آنها را حذف کرد و از علامت "::" به جای آنها استفاده کرد. مثال قبلی را بازنویسی می‌کنیم:

`21cd:54:0:0:6dd:6e:af38:8d63` → `21cd:54::6dd:6e:af38:8d63`

در هر آدرس IPv6 فقط یک بار می‌توان از علامت "::" استفاده کرد.

با استفاده از خط فرمان آدرس IPv6 رایانه خود را نمایش دهید و با دیگر رایانه‌های شبکه مقایسه کنید.

اگر سیستم‌عامل هر دو آدرس IPv6 و IPv4 را داشته باشد، ابتدا در برقراری ارتباط با میزبان راه دور از آدرس IPv6 استفاده می‌کند و در صورتی که پاسخی دریافت نکند از IPv4 استفاده می‌کند.

یادداشت



فعالیت گروهی



جدول ارزشیابی شایستگی های غیر فنی، ایمنی، بهداشت و توجهات زیست محیطی



شایستگی ها	شرایط عملکرد (ابزار، مواد، تجهیزات، زمان، مکان و...)	نتایج ممکن	استاندارد (شاخص ها/داوری /نمره دهی)	نمره
شایستگی های غیر فنی	مسئولیت پذیری، توجه به جزئیات کار - زبان فنی	قابل قبول	توجه به مسئولیت کاربر برای عضویت او در گروه ها و تعیین مجوزها - بازگرداندن تنظیمات به حالت اولیه پس از انجام عملیات	۲
ایمنی و بهداشت	توجه به سطح دسترسی مورد نیاز کاربران و گروه ها	غیر قابل قبول	توجه به ایمنی و بهداشت محیط کارگاه	۱
توجهات زیست محیطی	کاهش مصرف کاغذ با اشتراک گذاری منابع			
نگرش	دقت در اختصاص مجوزها و تنظیم IP رایانه			

* این شایستگی ها در ارزشیابی پایانی واحد یادگیری باید مورد توجه قرار گیرند.

ارزشیابی مرحله ۱



مراحل کار	شرایط عملکرد (ابزار، مواد، تجهیزات، زمان، مکان و...)	نتایج ممکن	استاندارد (شاخص ها/داوری /نمره دهی)	نمره
تعیین ویژگی های رایانه در شبکه	مکان: کارگاه استاندارد رایانه تجهیزات: رایانه متصل به شبکه زمان: ۱۰ دقیقه	بالاتر از حد انتظار	تعیین نام رایانه و تغییر آن - تعیین IP رایانه و نوع آن - اختصاص IP static به رایانه های شبکه - بررسی اتصال رایانه ها - تعیین Subnet mask و Network Address و Broadcast address بر اساس IP رایانه	۳
		در حد انتظار	تعیین نام رایانه و تغییر آن - تعیین IP رایانه و نوع آن - اختصاص IP static به رایانه های شبکه - بررسی اتصال رایانه ها	۲
		پایین تر از حد انتظار	تعیین نام رایانه و تغییر آن - تعیین IP رایانه و نوع آن	۱

زیر شبکه (Subnet)

در سازمان‌های کوچک که تعداد رایانه‌ها کم است و معمولاً در یک محل قرار دارند، استفاده از آدرس‌های classful ایده خوبی است؛ اما برای سازمان‌های بزرگ که تعداد رایانه‌ها زیاد و بیش از ۱۰۰ دستگاه است یا رایانه‌های آنها به دلیل وسعت جغرافیایی پراکنده هستند، بهتر است شبکه را به شبکه‌های کوچک‌تری به نام subnet تقسیم کنیم و با مسیریاب آنها را به هم متصل کنیم (شکل ۱۰).



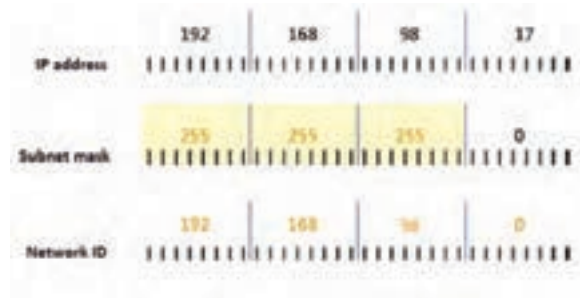
شکل ۱۰- اتصال subnetها با مسیریاب

Subnet یک زیر شبکه از شبکه اصلی است که برای مشخص کردن بخش‌های مختلف یک شبکه تعریف می‌شود و سپس به وسیله یک یا چند مسیریاب به بخش‌های دیگر متصل می‌شود. تقسیم شبکه به بخش‌های کوچک‌تر علاوه بر اینکه اجازه می‌دهد بتوانیم ترافیک داخلی شبکه را از ترافیک خارجی آن جدا کنیم باعث کاهش ترافیک در شبکه می‌شود و در نتیجه مدیریت شبکه را آسان‌تر می‌کند. به این عمل subnetting می‌گویند.

برای ایجاد زیر شبکه باید تعداد بیت‌های Subnet mask را تغییر دهیم تا آدرس IP انعطاف‌پذیری بیشتری برای افزایش یا کاهش تعداد میزبان‌ها و شبکه‌ها داشته باشد. هر چه تعداد بیت بیشتری به شناسه شبکه اختصاص دهیم، بیت کمتری برای بخش شناسه میزبان باقی می‌ماند. در نتیجه تعداد شبکه‌ها افزایش می‌یابد؛ اما تعداد میزبان‌ها برای هر شبکه کم می‌شود.

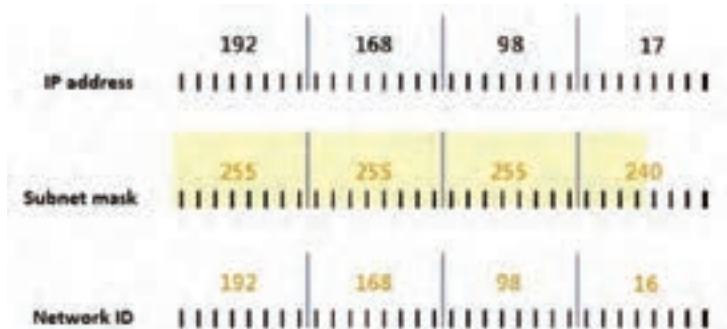
به مثال زیر توجه کنید:

آدرس 192.168.98.17 یک آدرس در کلاس C است که تعداد بیت Subnet mask آن ۲۴ بیت است و می‌تواند حداکثر ۲۵۴ آدرس برای میزبان‌های شبکه خود با شناسه شبکه 192.168.98.0 تولید کند (شکل ۱۱).



شکل ۱۱- Subnet mask در حالت classful

اکنون اگر تعداد بیت Subnet mask آن را از ۲۴ بیت به ۲۸ بیت افزایش دهیم برای بخش شناسه میزبان ۴ بیت باقی می ماند؛ بنابراین تعداد آدرس های IP از $2^8 - 2$ به $2^4 - 2$ (۱۴) کاهش می یابد (شکل ۱۲).



شکل ۱۲- Subnet mask برای ایجاد زیرشبکه

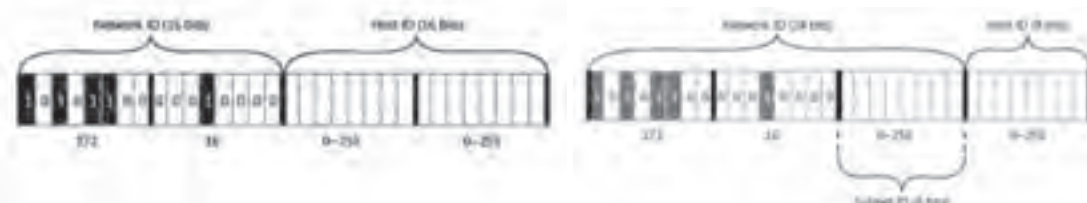
Subnet mask مثال مذکور 255.255.255.240 است. نحوه محاسبه عدد ۲۴۰ را بررسی کنید.

کنجکاو



پیاده سازی subnetting

وقتی آدرسی از ISP یا مدیر شبکه خود دریافت می کنید، آن آدرس شامل یک شناسه شبکه است که نمی توان آن را تغییر داد. مثلاً اگر آدرس کلاس B باشد ۱۶ بیت اول آن شناسه شبکه است که باید ثابت بماند و شما از ۱۶ بیت دوم که مربوط به شناسه میزبان است می توانید برای زیرشبکه ها استفاده کنید.



شکل ۱۳- استفاده از بیت های شناسه میزبان برای ایجاد زیرشبکه

شکل ۱۳ کلاس آدرس B است. دو بایت اول مشخص کننده شناسه شبکه است که باید برای همه دستگاه های شبکه یکسان باشد. بنابراین از دو بایت دوم که مربوط به شناسه میزبان است، یک بایت (بایت سوم) به شناسه subnet اختصاص یافته است و بایت دیگر (بایت چهارم) شناسه یکتا برای هر میزبان در داخل هر زیر شبکه است. به رشته ای از بیت ها که از شناسه میزبان جدا می شود و به شناسه شبکه برای توسعه شبکه سازمان اضافه می شود Subnet ID می گویند. بدین ترتیب می توانید شبکه سازمان خود را به بخش های کوچک تر تقسیم کرده، بدون اینکه در شناسه شبکه اصلی خود تغییر ایجاد کرده باشید، آدرس هر بخش را تعریف کنید. برای subnetting باید بر اساس تعداد شبکه های مورد نیاز و تعداد میزبان های هر شبکه شامل رایانه، چاپگر و... موارد زیر را مشخص کنیم.

الف) یک Subnet mask برای کل شبکه

ب) یک Subnet ID یکتا برای هر زیرشبکه

ج) محدوده IP برای میزبان های هر زیرشبکه

کارگاه ۴ تعیین محدوده آدرس برای subnetting با استفاده از نرم افزار

آدرس IP یکی از رایانه‌های شبکه 192.168.100.10 است. برای این شبکه می‌خواهیم ۶ زیر شبکه (Subnet) ایجاد کنیم. برای تعیین Subnet ID ، Subnet mask و محدوده آدرس IP میزبان‌ها می‌توانیم از نرم افزارهای Subnet Calculator استفاده کنیم.



۱ نرم افزار Advanced IP Address Calculator

را نصب کرده، اجرا کنید.

۲ آدرس IP و حداکثر تعداد زیر شبکه‌ها را در

نرم افزار وارد کنید.

آدرس IP را در کادر IP تایپ کنید و در کادر Max subnets عدد ۶ را برای تعریف حداکثر تعداد زیر شبکه‌ها انتخاب کنید (شکل ۱۴).

۳ اطلاعات خواسته شده در جدول را براساس

خروجی نرم افزار در بخش Subnets تکمیل کنید.

شکل ۱۴- نرم افزار Advanced IP Address Calculator

Class	Subnet Mask	Subnet Value	Subnet ID	محدوده آدرس IP برای میزبان	حداکثر تعداد میزبان
		۱۲۷			۳۰

- آدرس 142.9.26.1 در شبکه‌ای که نیاز به ۱۴ زیر شبکه دارد مفروض است. Subnet mask ، Subnet ID و محدوده IP را برای آن شبکه به دست آورید.
- واژه Subnet Calculator را در اینترنت جست‌وجو کنید و به کمک یکی از نرم افزارهایی که پیدا می‌کنید برای ایجاد ۴ زیر شبکه در کارگاه رایانه خود Subnet mask ، Subnet ID و محدوده IP را تعیین کنید.

فعالیت
گروهی



ارزشیابی مرحله ۲

مرحله کار	شرایط عملکرد (ابزار، مواد، تجهیزات، زمان، مکان و ...)	نتایج ممکن	استاندارد (شاخص‌ها/داوری/نمره دهی)	نمره
ایجاد زیر شبکه	مکان: کارگاه استاندارد رایانه تجهیزات: شبکه‌ای از رایانه‌ها زمان: ۱۵ دقیقه	بالاتر از حد انتظار	تعیین شناسه شبکه و شناسه میزبان - تعیین Subnet ID ، subnet mask و محدوده IP	۳
		در حد انتظار	تعیین شناسه شبکه و شناسه میزبان - تعیین Subnet mask و محدوده IP	۲
		پایین تر از حد انتظار	تعیین شناسه شبکه و شناسه میزبان	۱



شبکه‌های گروه‌کاری (Workgroup)

برای ایجاد و مدیریت شبکه چند راه وجود دارد که باید براساس نیاز کاربران و شرایط سازمان انتخاب شوند. در محیط‌های کوچک استفاده از شبکه‌های گروه‌کاری آسان است و معمولاً روشی مناسب برای چنین محیط‌هایی به‌شمار می‌رود؛ اما در سازمان‌های بزرگ به‌دلیل مسائل امنیتی و حجم زیاد اطلاعات، استفاده از شبکه‌های Domain انتخاب منطقی‌تری است.

به مجموعه کوچکی از رایانه‌های شبکه که می‌توانند منابع خود مانند پرونده و چاپگر را به اشتراک بگذارند Workgroup گفته می‌شود.

نام دیگر این نوع شبکه‌ها نظیر به نظیر (peer to peer) است که به اختصار p2p می‌گویند.

یادداشت



برای ایجاد یک شبکه گروه‌کاری ابتدا آدرس IP رایانه‌ها و سپس یک نام برای شبکه گروه‌کاری تعریف می‌کنیم. پس از آن همه رایانه‌هایی که می‌خواهیم عضو این شبکه باشند، با این نام تنظیم می‌شوند.

کارگاه ۵ ایجاد شبکه گروه‌کاری

۱ وارد تنظیمات سیستم شوید.

از Control Panel وارد تنظیمات سیستم شده، روی گزینه System And Security کلیک کرده، گزینه System را انتخاب کرده، سپس گزینه Change Setting را انتخاب کنید.

۲ رایانه را عضو گروه‌کاری با نام Site1-Work کنید.

در برگه Computer Name دکمه Change را انتخاب کرده، در کادر Workgroup نام جدید را وارد کنید (شکل ۱۵).



۲ تنظیمات را ذخیره کرده، رایانه را راه‌اندازی مجدد کنید.

شکل ۱۵- عضویت در شبکه گروه‌کاری

هر سه رایانه کارگاه را عضو یک گروه‌کاری کنید.

فعالیت
کارگاهی



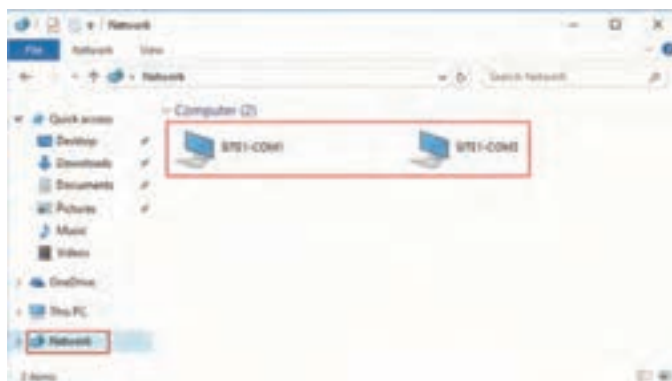
هر رایانه می تواند فقط عضو یک شبکه گروه کاری باشد.



۴ فهرست رایانه های شبکه را مشاهده کنید.

بعد از تنظیم نام شبکه گروه کاری روی همه رایانه های شبکه، می توانیم فهرست رایانه های موجود در شبکه را به همراه منابع شان مشاهده کنیم.

روی نماد This PC کلیک کنید. گزینه Network را انتخاب کنید. در پنجره ای که باز می شود فهرست رایانه های موجود در شبکه نمایش داده می شود (شکل ۱۶). آیا همه رایانه های موجود در کارگاه قابل مشاهده است؟ پیشنهاد شما برای مشاهده تمام رایانه های کارگاه چیست؟



شکل ۱۶- فهرست رایانه های شبکه

۵ منابع اشتراکی رایانه مورد نظر را مشاهده کنید.

با کلیک روی نام هر رایانه می توانید منابع اشتراکی آن را مشاهده کنید.

کاربر (User)

کاربران برای ورود به رایانه از نام کاربری و گذرواژه خود به عنوان حساب کاربری محلی (Local user account) استفاده می کنند. حساب کاربری محلی فقط اجازه ورود کاربر به رایانه ای را می دهد که در آن تعریف شده است. ویندوز دو ابزار برای ایجاد، تغییر و حذف حساب های کاربری معرفی می کند:

● ابزار User Accounts در Control Panel

● ابزار Computer Management

ابزار Computer Management نسبت به ابزار User Accounts توانمندی های بیشتر و قدرتمندتری دارد که علاوه بر حساب کاربری می تواند گروه های محلی را نیز مدیریت کند. فقط کاربران عضو گروه های مدیریتی می توانند به این ابزار دسترسی داشته باشند.

از حساب کاربری محلی در شبکه های گروه کاری استفاده می شود.

حساب کاربری administrator و guest را حساب های کاربری پیش ساخته (built-in) می گویند. این حساب ها قابل حذف کردن نیستند. اما می توانید نام آنها را تغییر دهید یا آنها را غیرفعال کنید.





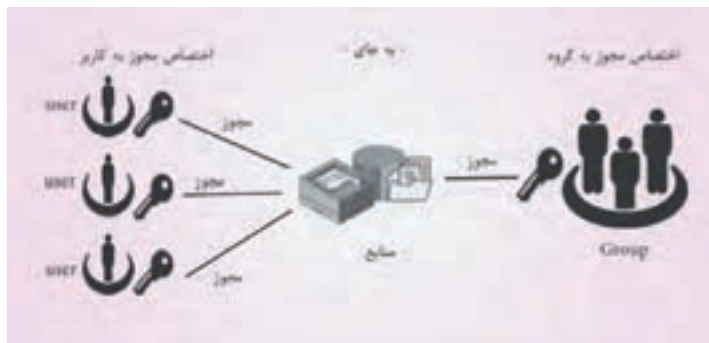
فیلم شماره ۱۲۱۰۷: ایجاد حساب کاربری محلی

پس از مشاهده فیلم فعالیت کارگاهی را انجام دهید.

- حساب کاربری به نام خود ایجاد کنید و خود را به عنوان هنرجوی رشته شبکه و نرم افزار رایانه معرفی کنید.
- تنظیم کنید که در هنگام وارد شدن به محیط ویندوز مجبور به تغییر گذرواژه خود شوید.

گروه (Group)

با گروه بندی کاربران می توانید آنها را به راحتی مدیریت کنید و به جای تعیین مجوزها و سیاست های امنیتی برای هر کاربر به صورت جداگانه، آنها را برای گروه تعیین کنید.



شکل ۱۷- تعیین مجوز برای گروه

کارگاه ۶ ایجاد گروه

۱ کادر محاوره ای ایجاد گروه را باز کنید.

پنجره Computer Management را باز کنید. روی گزینه Local Users And Groups دابل کلیک کنید. سپس روی گزینه Groups راست کلیک کرده و گزینه New Group را انتخاب کنید (شکل ۱۸).



شکل ۱۸- مسیر باز کردن کادر محاوره ای ایجاد گروه



شکل ۱۹- ایجاد گروه

۲ نام گروه را تعیین کنید.

در کادر Group Name نام class12 را وارد کنید.

۳ در کادر Description توضیحی دلخواه درمورد هدف گروه بنویسید.

۴ حساب کاربری خود را به فهرست اعضای گروه اضافه کنید (شکل ۱۹).

از دکمه Add استفاده کنید.

۵ گروه را ایجاد کنید.

بعد از تعیین نام و اعضای گروه روی دکمه Create برای ایجاد گروه کلیک کنید.

۶ گروه را حذف کنید.

برای حذف گروه نیز از ابزار Computer Management استفاده می‌کنیم. روی نام گروه class12 راست کلیک کرده، گزینه Delete را انتخاب کنید. در صورت حذف یک گروه، تمامی مجوزهای اختصاص داده شده به آن به همراه دیگر تنظیماتش از بین می‌رود.

کاربران می‌توانند عضو چندین گروه باشند. در صورتی که بخواهید کاربر را در چندین گروه عضو کنید باید از برگه Member Of پنجره Properties مربوط به کاربر استفاده کنید.

یادداشت



فعالیت گروهی

یک حساب کاربری برای خود و یکی از دوستان خود ایجاد کنید. سپس دو گروه ایجاد کرده، هر دو حساب کاربری را عضو گروه‌ها کنید.



گروه‌های پیش ساخته (built-in)

گروه‌هایی که با نصب ویندوز ایجاد می‌شوند، گروه‌های پیش ساخته هستند. ویندوز دو گروه پیش ساخته دارد:

- **گروه‌های محلی (Local groups):** اعضای این گروه می‌توانند وظایف سیستمی همچون پشتیبان‌گیری، تغییر زبان سیستم و مدیریت منابع سیستمی را انجام دهند (جدول ۴).

جدول ۴- برخی گروه‌های محلی

نام گروه	توضیح
Administrators	اعضای این گروه می‌توانند همه وظایف مدیریتی را روی رایانه انجام دهند. به طور پیش فرض حساب کاربری Administrator عضو این گروه است.
Backup Operators	اعضای این گروه می‌توانند از اطلاعات رایانه پشتیبان بگیرند و آنها را بازیابی کنند.
Guests	به طور پیش فرض حساب کاربری Guest عضو این گروه است.
Users	اعضای این گروه فقط وظایفی که به آنها مجوز داده می‌شود را می‌توانند انجام دهند. به طور پیش فرض هر حساب کاربری که ایجاد می‌شود عضو این گروه قرار می‌گیرد.

- گروه‌های سیستمی (System groups): این گروه‌ها اعضای مشخصی ندارند که بتوانیم آنها را تغییر دهیم. اعضای این گروه‌ها به‌وسیله سیستم‌عامل اضافه یا حذف می‌شوند (جدول ۵).
- جدول ۵ - برخی گروه‌های سیستمی

نام گروه	توضیح
Everyone	همه کاربرانی که به رایانه دسترسی دارند عضو این گروه هستند.
Creator Owner	هر کاربری که منبعی را ایجاد کند عضو این گروه می‌شود.
Network	کاربرانی که از طریق شبکه به منابع اشتراکی رایانه متصل می‌شوند در این گروه قرار دارند.
Interactive	کاربری که در حال استفاده از رایانه است، عضو این گروه قرار می‌گیرد.

ارزشیابی مرحله ۳



مرحله کار	شرایط عملکرد (ابزار، مواد، تجهیزات، زمان، مکان و ...)	نتایج ممکن	استاندارد (شاخص‌ها/داوری/نمره دهی)	نمره
عضویت در شبکه workgroup و ایجاد کاربر و گروه	مکان: کارگاه استاندارد رایانه تجهیزات: شبکه‌ای از رایانه‌ها زمان: ۱۵ دقیقه	بالاتر از حد انتظار	عضویت در workgroup - مشاهده منابع اشتراکی رایانه‌ها ایجاد کاربر و گروه - عضو کردن کاربر در گروه - تعیین گروه‌های اصلی سیستم‌عامل	۳
		در حد انتظار	عضویت در workgroup - مشاهده منابع اشتراکی رایانه‌ها - ایجاد کاربر و گروه - عضو کردن کاربر در گروه	۲
		پایین تر از حد انتظار	عضویت در workgroup - ایجاد کاربر	۱

اشتراک گذاری منابع

یکی از کاربردهای مهم شبکه به اشتراک گذاشتن منابع است. سازمان‌ها به دلایل مختلف نیازمند اشتراک داده‌ها و منابع هستند به‌همین دلیل از شبکه استفاده می‌کنند.

اشتراک گذاری پوشه

برای اشتراک گذاری پوشه‌ها از دو روش زیر می‌توان استفاده کرد:

- ابزار Shared Folders: این ابزار علاوه بر امکان اشتراک گذاری، اجازه مدیریت منابع اشتراکی موجود را نیز فراهم می‌کند.
- File Explorer

فیلم شماره ۸:۲۱۰۸: اشتراک گذاری منابع با Shared Folders

فیلم



فعالیت
کارگاهی



پس از مشاهده فیلم فعالیت را انجام دهید.

- در درایو D پوشه‌ای به نام workshop ایجاد کنید و پوشه‌ای با نام folder-test داخل آن بسازید.
- پوشه folder-test را به گونه‌ای به اشتراک بگذارید که هیچ کاربری به جز administrator نتواند به آن دسترسی داشته باشد.
- پوشه folder-test را از حالت اشتراک خارج کنید.

کارگاه ۷ | اشتراک گذاری پوشه به وسیله File Explorer

1 پوشه مورد نظر را برای اشتراک گذاری آماده کنید.

در پوشه workshop پوشه‌ای با نام myfolder ایجاد کنید و سپس یک پرونده متنی با نام letter1 ایجاد کرده، مشخصات خود و هم گروهی تان را در آن بنویسید.

2 پوشه را به اشتراک بگذارید.

روی پوشه myfolder راست کلیک کرده، گزینه properties را انتخاب کنید. در برگه sharing (1) روی دکمه Advanced sharing کلیک کرده (2)، گزینه Share this folder را انتخاب کنید (3).

3 نام منبع اشتراکی را تعیین کنید.

در کادر Share name عبارت net-letter را تایپ کنید (4). از نظر امنیتی بهتر است نام منابع اشتراکی را تغییر دهیم تا نام اصلی آنها از دید کاربران شبکه مخفی بماند.

4 مجوزها را تعیین کنید.

دکمه Permissions را کلیک کنید (5) و مجوز Change را انتخاب کرده (6)، دکمه OK پنجره‌ها را انتخاب کنید (شکل ۲۰).



مجوزهای پوشه‌های اشتراکی تنظیم شده روی منابع، سطح دسترسی کاربران شبکه را به منبع مشخص می‌کنند. این مجوزها عبارت‌اند از:

- Read: کاربران و گروه‌ها می‌توانند محتویات پرونده‌ها را ببینند؛ اما نمی‌توانند آنها را تغییر دهند یا حذف کنند.
- Change: کاربران و گروه‌ها می‌توانند علاوه بر دیدن محتویات پرونده‌ها آنها را تغییر دهند، حذف کنند و یا پرونده جدید ایجاد کنند؛ اما اجازه تغییر مجوزها را ندارند.
- Full Control: کاربران و گروه‌ها می‌توانند علاوه بر انجام کارهای قبلی، مجوزها را نیز تغییر دهند.

شکل ۲۰- اشتراک گذاری پوشه در کادر محاوره‌ای Properties

دسترسی به منابع اشتراکی

علاوه بر استفاده از گزینه Network در پنجره This PC می‌توانید به‌طور مستقیم از آدرس UNC (Universal Naming Convention) برای دسترسی به منابع اشتراکی به‌صورت زیر استفاده کنید:

\\computer name\share name

یا

\\Ip address\share name

برای مشاهده همه پوشه‌های اشتراکی فقط از نام رایانه یا آدرس IP به همراه \\ استفاده می‌کنیم.

کارگاه ۸ دسترسی به منابع اشتراکی به وسیله آدرس UNC



شکل ۲۱- دسترسی به منبع اشتراکی با آدرس UNC

می‌خواهیم به پوشه اشتراک گذاشته شده در کارگاه ۷ دسترسی پیدا کنیم.

۱ آدرس رایانه‌های شبکه کارگاه خود را با آدرس 192.168.100.z تنظیم کنید.

z را بر اساس شماره رایانه‌ها تعیین کنید.

۲ در پنجره Run آدرس دسترسی به پوشه اشتراکی را وارد کنید.

آدرس 192.168.100.1\net-letter را تایپ کنید و دکمه OK را کلیک کنید (شکل ۲۱).

۳ بعد از دسترسی به پرونده به اشتراک گذاشته شده، آن را تغییر دهید.

پرونده letter1 را باز کنید و جمله‌ای به آن اضافه کنید. آیا تغییرات در پرونده ذخیره می‌شوند؟ در مورد پاسخ با دوستان خود بحث کنید.

۴ پوشه را از حالت اشتراک خارج کنید.

گزینه Share this folder را از حالت انتخاب خارج کنید.

۵ تعداد کاربرانی که هم‌زمان به پوشه اشتراکی دسترسی پیدا خواهند کرد را محدود کنید.

گزینه Limit the number of simultaneous users to در پنجره Advanced sharing تعداد نفراتی که به‌صورت هم‌زمان به پوشه اشتراکی دسترسی پیدا می‌کنند را مشخص می‌کند. دوباره پوشه myfolder را به اشتراک بگذارید. نام آن را net-limit و عدد ۳ را برای گزینه Limit the number of simultaneous users to تنظیم کنید. از دوستان خود بخواهید یکی یکی به این پوشه دسترسی پیدا کنند. در مورد نتیجه کار با دوستان خود بحث کنید.

اشتراک گذاری پوشه به صورت مخفی

در صورتی که بخواهیم پوشه‌ای را به اشتراک بگذاریم ولی کاربران شبکه نتوانند آن را در فهرست منابع اشتراکی رایانه ما مشاهده کنند، در انتهای نام اشتراکی پوشه از علامت "\$" استفاده می‌کنیم. برای دسترسی به پوشه‌های اشتراکی مخفی باید از آدرس UNC آنها استفاده کنیم.

\\Ip address\share name\$

اختصاص نام درایو به مسیر دسترسی پوشه اشتراکی (Map Network Drive)

برای دسترسی به پوشه‌های اشتراکی پرکاربرد، کاربر مجبور است در طول روز چندین بار آدرس UNC آنها را تایپ کند. راهکاری پیشنهاد دهید که نیاز به تایپ این آدرس‌ها برای هر بار دسترسی نداشته باشد.

کارگاه ۹ ایجاد Map Network Drive

ویژگی Map Network Drive سبب می‌شود در پنجره File Explorer یک نام درایو به آدرس UNC مورد نظر اختصاص یابد، تا کاربر مجبور نباشد برای هر بار دسترسی، آدرس UNC آن را تایپ کرده و یا پنجره‌های متعددی را باز کند.

۱ پوشه Myfolder را با نام net-letter-full به اشتراک بگذارید.

۲ کادر Map Network Drive را باز کنید.

روی File Explorer راست کلیک کرده، گزینه Map Network Drive را انتخاب کنید.

۳ نام درایو را انتخاب کنید.

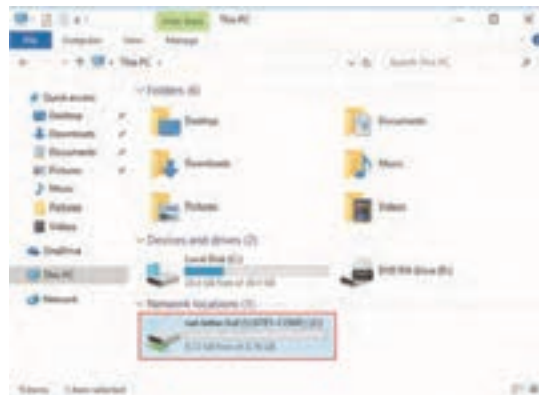
از کادر Drive نویسه Z را انتخاب کنید.

۴ آدرس UNC پوشه اشتراکی را تعیین کنید.

در کادر Folder آدرس \\192.168.100.1\net-letter-Full را تایپ کنید. می‌توانید از دکمه Browse نیز برای مشخص کردن آدرس پوشه اشتراکی استفاده کنید. دکمه Finish را کلیک کنید.

۵ از طریق درایو ایجاد شده به پوشه دسترسی پیدا کنید.

درایوی با نام Z به فهرست درایوها در File Explorer اضافه شده است که با کلیک روی آن پوشه اشتراکی net-letter باز می‌شود (شکل ۲۲).



شکل ۲۲- map drive پوشه اشتراکی

مجوزهای دسترسی به پرونده و پوشه

وقتی چند نفر از یک رایانه استفاده می‌کنند و پرونده‌های خود را روی آن ذخیره می‌کنند، لازم است تا از عدم امکان دسترسی بدون اجازه کاربران دیگر به پرونده‌های آنها مطمئن شوند. ویندوز این امنیت را به‌وسیله مجوزهای NTFS مدیریت می‌کند. درایوهایی که با سیستم‌فایل NTFS قالب‌بندی شده‌اند، به شما امکان پیکربندی مجوزها روی پرونده‌ها و پوشه‌ها را می‌دهند. بدین ترتیب می‌توانید کاربران یا گروه‌های مختلف را برای دسترسی به پرونده یا پوشه مدیریت کنید.

مجوزها به‌دو صورت قابل تنظیم هستند: تنظیم خودکار و تنظیم دستی

تنظیم خودکار مجوزها

تنظیم مجوز به صورت دستی برای صدها پرونده و پوشه بسیار وقت‌گیر و دشوار است. به‌همین دلیل مجوزها به صورت پیش‌فرض به‌وسیله ویژگی ارث‌بری روی پرونده‌ها و پوشه‌ها تنظیم می‌شوند تا علاوه بر کاهش زمان، مدیریت آنها را نیز ساده‌تر کنند. به این مجوزها، مجوزهای ارث‌برده شده (NTFS inheritance) می‌گویند.

کارگاه ۱۰ مشاهده مجوزهای NTFS

۱ یک پوشه ایجاد کنید.

در پوشه workshop پوشه‌ای با نام folder-inher ایجاد کنید.

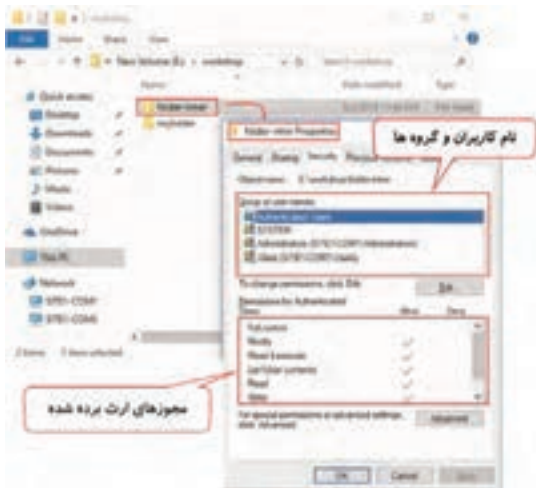
۲ مجوزهای پوشه جدید را بررسی کنید.

با راست کلیک روی پوشه folder-inher گزینه properties را انتخاب کرده، سربرگ Security را انتخاب کنید (شکل ۲۳).

مجوزهایی برای کاربران و گروه‌های مختلف تعریف شده است که از پوشه والد آن پوشه workshop در شکل ۲۳ به ارث برده شده‌اند. مجوزهای ارث برده شده به صورت کمرنگ نمایش داده می‌شوند.

روی دکمه Edit کلیک کنید و سپس دکمه Remove را انتخاب کنید. پیام نمایش داده شده را ترجمه کنید. در این مورد با هم کلاسی‌های خود بحث و گفتگو کنید.

۳ ویژگی ارث بری را غیرفعال کنید.



شکل ۲۳- مجوزهای ارث برده شده

فیلم شماره ۱۲۱۰۹: غیر فعال کردن ارث بری

فیلم



فیلم را مشاهده کنید و فعالیت زیر را انجام دهید.

- همه مجوزهای ارث برده شده پوشه folder-inher را پاک کنید. آیا می‌توانید پوشه را باز کنید؟
- پوشه‌ای ایجاد کنید و مجوزهای ارث برده شده آن را تبدیل به مجوز مستقیم کنید. آیا می‌توانید مجوزها را به وسیله دکمه Edit در برگه Security یکی یکی حذف کنید؟
پاسخ را با دوستانتان در میان بگذارید و نتیجه آن را به طور مختصر بنویسید.

فعالیت کارگاهی



تنظیم دستی مجوزها

هرچند ارث بری مجوزها مدیریت پرونده‌ها و پوشه‌ها را آسان تر می‌کند؛ اما در برخی از موارد نیاز به تعریف مجوز جدید برای پرونده یا پوشه داریم. مجوزهایی که به صورت دستی تنظیم می‌شوند را مجوز مستقیم می‌نامند.

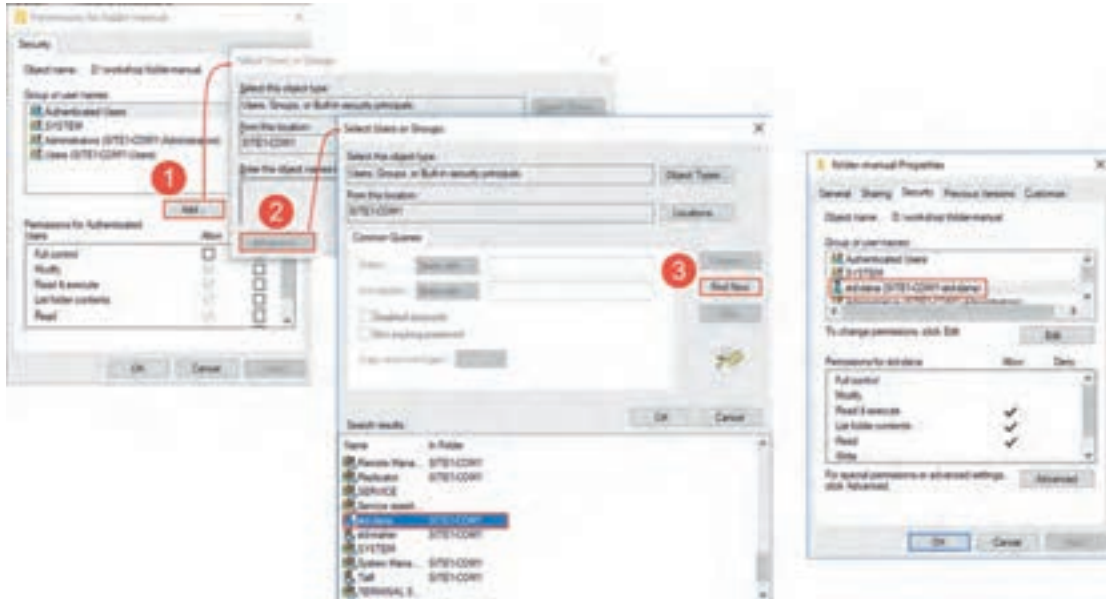
کارگاه ۱۱ تنظیم مجوز برای کاربران و گروه‌های دلخواه

۱ حساب کاربری با نام std-dana ایجاد کنید.

۲ در پوشه workshop، پوشه‌ای با نام folder-manual ایجاد کنید.

۳ با استفاده از فهرست کاربران و گروه‌های تعریف شده در رایانه، کاربران و گروه‌های موردنظر را انتخاب کنید.

روی پوشه folder-manual راست کلیک کنید و گزینه properties را انتخاب کرده، سربرگ Security را انتخاب کنید. روی دکمه Edit کلیک کرده، سپس دکمه Add را انتخاب کنید (۱). روی دکمه Advanced (۲) و سپس دکمه Find Now کلیک کنید (۳). فهرست نام کاربران و گروه‌های پیش فرض و تعریف شده نمایش داده می‌شود. حساب کاربری std-dana را انتخاب کنید. با کلیک دکمه OK پنجره‌های باز را تأیید کنید. حساب کاربری std-dana به فهرست برگه Security اضافه می‌شود (شکل ۲۴).



شکل ۲۴- انتخاب حساب کاربری

انواع مجوزهای NTFS

مجوزهای NTFS دو نوع هستند:

- **مجوزهای اصلی (Basic Permissions):** کار کردن با مجوزهای اصلی آسان است به همین دلیل برای بیشتر کارهای معمول از آنها استفاده می‌شود. مجوزهای اصلی شامل ۶ مجوز هستند (جدول ۶).

جدول ۶- عملکرد مجوزهای اصلی

عملکرد	مجوزهای اصلی
اجازه خواندن، نوشتن، تغییر و حذف پرونده‌ها و زیرپوشه‌ها را می‌دهد. ضمن آنکه تغییر مجوزها و مالکیت پرونده یا پوشه را برای کاربر فراهم می‌کند.	Full Control
اجازه خواندن، نوشتن، تغییر و حذف پرونده‌ها و زیرپوشه‌ها را می‌دهد اما اجازه تغییر مجوز و مالکیت را به کاربر نمی‌دهد.	Modify
اجازه دسترسی به محتوای پوشه، خواندن و اجرای پرونده‌ها را می‌دهد.	Read & Execute
فقط روی پوشه‌ها قابل اعمال است و اجازه دیدن محتویات پوشه را به کاربر می‌دهد.	List folder contents
اجازه دسترسی به محتوای پوشه و خواندن پرونده را می‌دهد.	Read
اجازه ایجاد و تغییر محتویات پرونده‌ها و پوشه‌ها را می‌دهد اما اجازه حذف نمی‌دهد.	Write

گروه مدیران (Administrators)، مالک پرونده یا پوشه (Owner) و کاربرانی که مجوز کامل (Full Control) روی پرونده یا پوشه دارند، می‌توانند روی آن پرونده یا پوشه برای کاربران و گروه‌های دیگر مجوز دسترسی تعریف کنند. وقتی کاربری پرونده یا پوشه‌ای ایجاد می‌کند به صورت خودکار مالک (Owner) آن پرونده یا پوشه می‌شود.

فیلم شماره ۱۲۱۱۰: مجوزهای اصلی

فیلم



فعالیت گروهی



پس از مشاهده فیلم، یک پرونده متنی به نام basic.txt در پوشه‌ای به نام folder-document ایجاد کنید. گروهی به نام teacher تعریف کنید و سپس مجوزهای زیر را پیاده‌سازی کنید:

(الف) مجوزهای ارث برده شده پوشه folder-document را حذف کنید و سپس برای حساب کاربری خودتان مجوز کامل تعریف کنید.

(ب) گروه teacher بتوانند پرونده‌های اجرایی موجود در پوشه folder-document را اجرا کند.

(ج) کاربر std-dana بتواند به محتوای پرونده basic دسترسی داشته باشد اما نتواند آن را تغییر دهد.

(د) گروه teacher بتوانند نام پرونده را تغییر دهند.

● **مجوزهای پیشرفته (Advanced Permissions):** در فعالیت گروهی قبل مجوزی برای کاربر std-dana تنظیم کردید که فقط بتواند پرونده basic را باز کند؛ اما نتواند محتوای آن را تغییر دهد. اکنون اگر بخواهیم به کاربر std-dana علاوه بر امکان خواندن، اجازه حذف پرونده را بدهیم باید مجوز Modify را برای آن تنظیم کنیم: $\text{Modify} = \text{Delete} + \text{Execute} + \text{Read} + \text{Write}$

در این صورت به کاربر مجوز Write هم اختصاص می‌یابد یعنی می‌تواند محتوای پرونده را تغییر دهد که خلاف خواسته ما است. مجوزهای اصلی در واقع مجموعه‌ای از مجوزهای پیشرفته هستند. در مثال ذکر شده مجوز Modify شامل مجوزهای پیشرفته خواندن، نوشتن، اجرا و حذف است. مجوزهای پیشرفته به شما امکان کنترل پرونده‌ها و پوشه‌ها را به صورت دقیق می‌دهند.

کارگاه ۱۲ تنظیم مجوزهای پیشرفته

- ۱ با حساب کاربری administrator وارد ویندوز شوید.
- ۲ کادر محاوره‌ای Properties پوشه folder-document را باز کنید.
- ۳ حساب کاربری دلخواه را برای تعیین مجوزهای پیشرفته اضافه کنید.

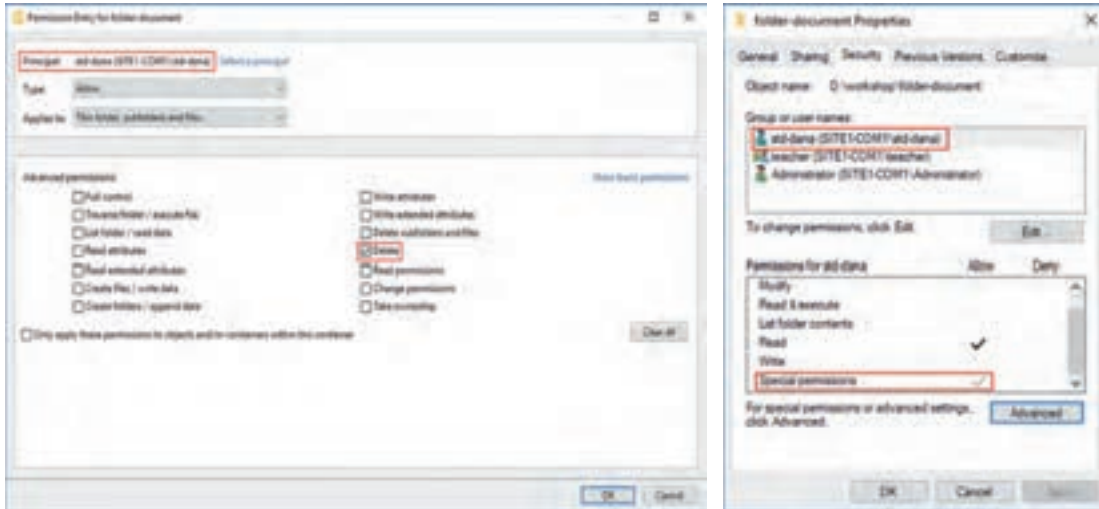


در برگه Security دکمه Advanced را انتخاب کنید. دکمه Add را انتخاب کرده، به کمک گزینه Select a principal حساب کاربری std-dana را انتخاب کنید (شکل ۲۵).

شکل ۲۵- تعیین مجوز پیشرفته برای کاربر دلخواه

۴ مجوزهای پیشرفته را برای حساب کاربری تعیین کنید.

گزینه Show advanced permissions را کلیک کرده، از فهرست مجوزها فقط گزینه Delete را انتخاب کنید (شکل ۲۶). با کلیک دکمه OK پنجره‌های باز را تأیید کنید. حساب کاربری std-dana به فهرست برگه Security اضافه شده، مجوز Special permissions آن علامت دار می‌شود (شکل ۲۷).



شکل ۲۶- تعیین مجوزهای پیشرفته

شکل ۲۷- برگه Security

۵ میزان دسترسی حساب کاربری به پوشه را بررسی کنید.

با حساب کاربری std-dana وارد شوید. پرونده basic را باز کنید. آیا می‌توانید محتوای آن را تغییر دهید؟ آیا می‌توانید پرونده را حذف کنید؟

مجوز مؤثر (Effective Permissions)

در برخی موارد امکان دارد که روی یک پرونده یا پوشه چندین مجوز برای کاربر و گروه‌هایی که کاربر عضو آن است تنظیم شده باشد. برای مثال ممکن است کاربر عضو دو گروه باشد که هر کدام مجوز متفاوتی برای دسترسی به پرونده یا پوشه داشته باشند. به مجموع مجوزهای کاربر روی یک منبع، مجوز مؤثر گفته می‌شود. مجوزها دارای دو وضعیت Allow و Deny هستند. اگر مجوزی برای کاربر یا گروهی Deny شود، تأکید می‌کند که آن کاربر یا گروه هرگز آن مجوز را نخواهند داشت؛ حتی اگر عضو گروهی باشند که این مجوز را دارد. مجوز مؤثر کاربر، از مجموع مجوزهای اعطا شده به کاربر و گروه‌هایی که کاربر عضو آنها است به دست می‌آید مگر آنکه مجوزی Deny شده باشد که در این صورت آن مجوز از مجموع مجوزها حذف می‌شود.

قوانین محاسبه مجوز مؤثر عبارت‌اند از:

- ۱ همه مجوزهای Allow را با یکدیگر ترکیب می‌کنیم.
- ۲ مجوز Deny بر مجوز Allow اولویت دارد؛ بنابراین مجوزهای Deny را اعمال می‌کنیم مگر آنکه مجوز Deny به ارث برده شده باشد که در این صورت مجوز Allow اعمال می‌شود. در واقع مجوز مستقیم بر مجوز ارث اولویت دارد.

کارگاه ۱۳ مجوز مؤثر

۱ یک حساب کاربری ایجاد کنید.

با حساب کاربری Administrator وارد ویندوز شوید و حساب کاربری با نام std-mobina ایجاد کنید.

۲ دو گروه ایجاد کرده، حساب کاربری را عضو آنها کنید.

نام گروه ها را g-programmer و g-database قرار دهید.

۳ در پوشه workshop پوشه‌ای با نام folder-rule1 ایجاد کنید.

۴ پرونده‌های مورد نیاز را درون پوشه قرار دهید.

در پوشه folder-rule1 یک پرونده متنی ایجاد کنید. یک نسخه مشابه از پرونده اجرایی CMD موجود در پوشه Windows\System32 را در پوشه folder-rule1 قرار دهید.

۵ مجوزهای ارث برده شده پوشه folder-rule1 را حذف کنید.

۶ بر اساس جدول زیر مجوز جدید تنظیم کنید.

نام کاربر یا گروه	مجوز	Allow	Deny
Administrator	Full Control	✓	
std-mobina	Read	✓	
g-programmer	Write		✓
g-database	Write	✓	

۷ با حساب کاربری std-mobina وارد ویندوز شوید و پوشه folder-rule1 را باز کنید.

چه عملیاتی قابل انجام است؟

۸ مجدداً با حساب کاربری Administrator وارد ویندوز شوید.

۹ در پوشه folder-rule1 پوشه‌ای با نام child ایجاد کنید و یک پرونده متنی در آن ایجاد کنید.

۱۰ مجوزهای پوشه child را تغییر دهید.

سربرگ Security پوشه child را انتخاب کنید و بر اساس جدول زیر مجوز جدید اضافه کنید. این مجوز مستقیم است و بر مجوز ارث برده شده اولویت دارد.

نام کاربر	مجوز	Allow	Deny
std-mobina	Write	✓	

۱۱ با حساب کاربری std-mobina وارد ویندوز شوید و پوشه child را باز کنید.

چه عملیاتی قابل انجام است؟

با توجه به اولویت مجوز مستقیم بر مجوز Deny می‌توانید پرونده متنی را تغییر دهید و پرونده یا پوشه جدید بسازید.

۱۲ حساب کاربری را برای مشاهده مجوز مؤثر انتخاب کنید.

در صورتی که بخواهید مجوز مؤثر کاربر یا گروهی را مشاهده کنید، می‌توانید از برگه Effective Access استفاده کنید.

روی پوشه folder-rule1 راست کلیک کرده، گزینه properties را انتخاب کنید. سربرگ Security را انتخاب کنید. روی دکمه Advanced و سپس سربرگ Effective Access کلیک کنید. به وسیله گزینه Select a user حساب کاربری std-mobina را انتخاب کنید (شکل ۲۸).



شکل ۲۸- انتخاب حساب کاربری برای مشاهده مجوز مؤثر

۱۳ مجوز مؤثر را مشاهده کنید.

دکمه View effective access را کلیک کنید (شکل ۲۹).



شکل ۲۹- مشاهده مجوز مؤثر

در صورتی که برای پرونده یا پوشه‌ای مجوز تعریف کنیم و کاربر آن را نسخه‌برداری کرده یا انتقال دهد، آیا مجوزها تغییر می‌کنند؟

فعالیت کارگاهی





نمره	استاندارد (شاخص‌ها/داوری / نمره دهی)	نتایج ممکن	شرایط عملکرد (ابزار، مواد، تجهیزات، زمان، مکان و ...)	مراحل کار
۳	به اشتراک گذاشتن منابع - ایجاد map drive - تعیین مجوزهای اشتراک و مجوزهای NTFS برای کاربران و گروه‌ها براساس نیاز - تعیین مجوز مؤثر	بالاتر از حد انتظار	مکان : کارگاه استاندارد رایانه تجهیزات: شبکه‌ای از رایانه‌ها زمان: ۳۰ دقیقه	اشتراک گذاری منابع در شبکه workgroup
۲	به اشتراک گذاشتن منابع - ایجاد map drive - تعیین مجوزهای اشتراک و مجوزهای NTFS برای کاربران و گروه‌ها براساس نیاز	در حد انتظار		
۱	به اشتراک گذاشتن منابع	پایین تر از حد انتظار		
<p>معیار شایستگی انجام کار:</p> <p>کسب حداقل نمره ۲ از مراحل عضویت در شبکه workgroup و ایجاد کاربر و گروه و اشتراک گذاری منابع در شبکه workgroup</p> <p>کسب حداقل نمره ۲ از بخش شایستگی‌های غیرفنی، ایمنی، بهداشت، توجهات زیست‌محیطی و نگرش</p> <p>کسب حداقل میانگین ۲ از مراحل کار</p>				

جدول ارزشیابی پایانی

<p>شرح کار: ۱- تعیین ویژگی‌های رایانه در شبکه ۲- ایجاد زیر شبکه ۳- عضویت در شبکه workgroup و ایجاد کاربر و گروه ۴- اشتراک گذاری منابع در شبکه workgroup</p>			
<p>استاندارد عملکرد: راه اندازی شبکه‌های p2p و ایجاد زیر شبکه و اشتراک گذاری منابع شاخص‌ها:</p>			
شماره مرحله کار	شاخص‌های مرحله کار		
۱	تعیین مشخصات اتصالات شبکه سیستم - تنظیم IP و سایر تنظیمات آن براساس نوع شبکه		
۲	تقسیم یک شبکه به چندین زیر شبکه		
۳	بررسی ارتباط رایانه‌های شبکه با یکدیگر - ایجاد کاربر و تنظیم پارامترهای آن - ایجاد گروه و عضو کردن کاربر در آن		
۴	اشتراک گذاری منابع مطابق نظر کارفرما - دسترسی به منابع اشتراکی - ایجاد درایو مجازی برای منبع اشتراکی		
<p>شرایط انجام کار و ابزار و تجهیزات: مکان: کارگاه رایانه مطابق استاندارد تجهیزات هنرستان‌ها تجهیزات: شبکه‌ای از رایانه‌ها زمان: ۷۰ دقیقه (تعیین ویژگی‌های رایانه در شبکه ۱۰ دقیقه - ایجاد زیر شبکه ۱۵ دقیقه - عضویت در شبکه workgroup ایجاد کاربر و گروه ۱۵ دقیقه - اشتراک گذاری منابع در شبکه workgroup ۳۰ دقیقه)</p>			
<p>معیار شایستگی:</p>			
ردیف	مرحله کار	حداقل نمره قبولی از ۳	نمره هنرجو
۱	تعیین ویژگی‌های رایانه در شبکه	۱	
۲	ایجاد زیر شبکه	۱	
۳	عضویت در شبکه workgroup و ایجاد کاربر و گروه	۲	
۴	اشتراک گذاری منابع در شبکه workgroup	۲	
	<p>شایستگی‌های غیر فنی، ایمنی، بهداشت، توجهات زیست محیطی و نگرش: مسئولیت پذیری، توجه به جزئیات کار - زبان فنی توجه به سطح دسترسی مورد نیاز کاربران و گروه‌ها کاهش مصرف کاغذ با اشتراک گذاری منابع دقت در اختصاص مجوزها و تنظیم IP رایانه</p>		۲
	<p>میانگین نمرات</p>		*
<p>* حداقل میانگین نمرات هنرجو برای قبولی و کسب شایستگی، ۲ است.</p>			

واحد یادگیری ۳

شایستگی کار با سیستم عامل سرویس دهنده شبکه

آیا تا به حال پی برده‌اید

- در فرودگاه‌ها چگونه تنظیمات شبکه به گوشی تلفن همراه ارسال می‌شود؟
- چگونه به وسیله نام تارنما به سرور آن دسترسی پیدا می‌کنیم؟
- چگونه می‌توان از تکراری شدن آدرس IP رایانه‌ها در شبکه جلوگیری کرد؟

هدف از این واحد شایستگی، استفاده از سرویس‌های DNS و DHCP در شبکه است.

استاندارد عملکرد

نصب سرویس‌های DNS و DHCP و استفاده از آنها در سیستم عامل سرویس دهنده

سیستم‌عامل ویندوز سرور

سیستم‌عامل ویندوز سرور یکی از سیستم‌عامل‌های خانواده ویندوز شرکت مایکروسافت است. این سیستم‌عامل ابزارهای متعددی برای راه‌اندازی سرویس و کنترل شبکه در اختیار مدیران شبکه قرار می‌دهد. مایکروسافت هر چند سال یک بار نسخه جدید ویندوز سرور خود را به همراه نسخه سرویس‌گیرنده آن عرضه می‌کند. در این کتاب نسخه ۲۰۱۲ معرفی می‌شود.

- با استفاده از کتاب همراه هنرجو بررسی کنید که چه سیستم‌عامل‌های سرور دیگری در بازار کار مورد استفاده قرار می‌گیرند؟
- با استفاده از کتاب همراه هنرجو نسخه‌های مختلف ویندوز سرور ۲۰۱۲ و سخت‌افزار موردنیاز برای نصب آن را در جدولی تهیه کرده، در کلاس ارائه کنید.
- چرا ویندوز سرور ۲۰۱۲ از پردازنده‌های ۳۲ بیتی پشتیبانی نمی‌کند؟

کنجکاو



سرویس DHCP

در تمام شهرهای کشورمان به منظور آدرس‌دهی صحیح به هر مکان یک کدپستی منحصر به فرد اختصاص داده می‌شود. به منظور جلوگیری از تداخل آدرس‌ها بهتر است این آدرس‌ها به صورت خودکار مثلاً به وسیله یک نرم‌افزار مناسب تولید شوند. در شبکه نیز به منظور ایجاد ارتباط بین گره‌ها نیاز به آدرس IP داریم که مانند همان کدپستی عمل می‌کند. اگر تعداد آدرس‌های IP مورد نیاز زیاد باشد، بهتر است به جای اختصاص آدرس IP به صورت استاتیک از روش‌های دینامیک استفاده شود. در روش دینامیک از سرویس نرم‌افزاری DHCP (Dynamic Host Configuration Protocol) برای تخصیص آدرس IP به سرویس‌گیرنده‌ها استفاده می‌شود. وظیفه تخصیص آدرس IP و دیگر موارد مرتبط با آن مانند Subnet mask با مدیر شبکه است. مدیر شبکه می‌تواند با توجه به تعداد آدرس‌های IP مورد نیاز تصمیم بگیرد که آیا از سرویس DHCP در شبکه استفاده کند یا خیر؟

DHCP یک پروتکل سرویس‌دهنده/سرویس‌گیرنده (client/server) است که به صورت خودکار به سرویس‌گیرنده‌ها آدرس IP و دیگر تنظیمات مرتبط را اختصاص می‌دهد (شکل ۳۰). با وجود سرویس‌دهنده DHCP در شبکه دیگر نیازی به تنظیم آدرس IP به صورت دستی روی سرویس‌گیرنده‌ها نیست.



شکل ۳۰- اختصاص خودکار آدرس به سرویس‌گیرنده به وسیله سرور DHCP

مزایای استفاده از سرویس DHCP

مدت زمان لازم برای انجام دستی تنظیمات شبکه برای ۱۰۰ گره شبکه چقدر است؟ چگونه می‌توان این زمان را کوتاه‌تر کرد؟

چند پیشنهاد برای جلوگیری از خطاهای احتمالی در آدرس‌دهی بنویسید.

کنجکاوی



استفاده از سرویس‌دهنده DHCP مزایای زیر را فراهم می‌کند:

- از اختصاص یک آدرس IP به ۲ یا چند گره و همچنین بروز اشتباهات تایپی جلوگیری می‌کند. خطای تداخل (conflict) زمانی بروز می‌کند که یک آدرس IP به بیش از یک گره تخصیص داده شود.
- به تنظیم دستی تک تک گره‌های شبکه نیازی نیست و در نتیجه صرفه‌جویی در زمان صورت می‌گیرد.
- در صورت جابه‌جایی یک سرویس‌گیرنده از یک شبکه به شبکه دیگر، نیاز به انجام تنظیمات مجدد برای آدرس IP نیست.
- در صورت خارج شدن یک سرویس‌گیرنده از شبکه، آدرس آن به سرویس‌گیرنده جدید اختصاص می‌یابد.
- مدیریت متمرکز آدرس‌دهی صورت می‌گیرد.

فیلم شماره ۱۲۱۱۱: نصب سرویس DHCP

فیلم



پس از مشاهده فیلم، سرویس DHCP را روی ویندوز سرور نصب کنید.

فعالیت کارگاهی



IP سرور باید به صورت استاتیک تعیین شود.

یادداشت



کارگاه ۱ ایجاد scope

پیش از اینکه سرویس‌دهنده DHCP بتواند به سرویس‌گیرنده‌ها آدرس IP اختصاص دهد، باید محدوده آدرس‌ها را مشخص کرد، به این محدوده Scope می‌گویند. فرض کنید می‌خواهیم تعداد ۱۰۰ آدرس IP به منظور اختصاص به سرویس‌گیرنده‌ها در نظر بگیریم. ابتدا باید محدوده مورد نظر را انتخاب کنیم. برای مثال در اینجا محدوده 192.168.20.x را در نظر می‌گیریم. با توجه به اینکه به ۱۰۰ آدرس نیاز داریم، آدرس ابتدا را 192.168.20.1 و آدرس انتها را 192.168.20.100 در نظر می‌گیریم.

محدوده تعریف شده در scope باید در محدوده آدرس IP سرویس‌دهنده باشد.

یادداشت

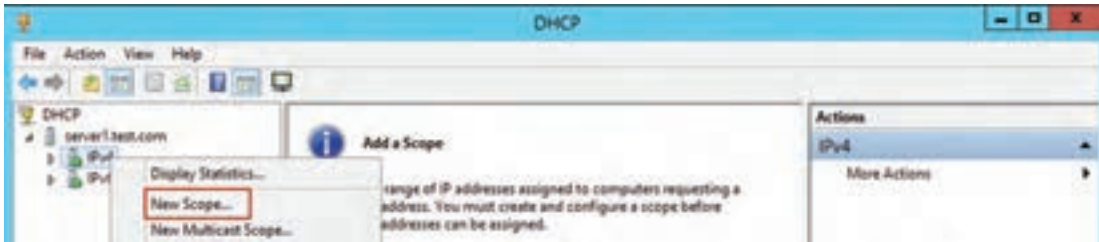


۱ وارد کنسول مدیریت DHCP شوید.

در کنترل پنل Administrative tools را انتخاب کرده، روی DHCP دابل کلیک کنید.

۲ یک Scope ایجاد کنید.

روی IPV4 راست کلیک کرده، گزینه New Scope را انتخاب کنید (شکل ۳۱).



شکل ۳۱- ایجاد Scope

۳ نام Scope را تعیین کنید.

در پنجره باز شده دکمه Next را انتخاب کرده، در پنجره بعدی یک نام برای Scope انتخاب کنید.

۴ محدوده آدرس دهی را مشخص کنید.

اولین و آخرین آدرس محدوده را وارد کنید. سیستم Subnet Mask مناسب را به صورت خودکار تشخیص می دهد. در صورت نیاز می توانید آن را تغییر دهید (شکل ۳۲).



شکل ۳۲- تعیین محدوده آدرس دهی

۵ محدوده Exclusions را مشخص کنید.

اگر بخواهیم از ۱۰۰ آدرس IP تعریف شده در بالا یک یا چند مورد را به هر دلیل به هیچ سرویس گیرنده ای اختصاص ندهیم آنها را در قسمت Exclusions مشخص می کنیم.

محدوده 192.168.20.1 تا 192.168.20.10 را در بخش Exclusions وارد کرده، گزینه Add را انتخاب و در نهایت روی Next کلیک کنید (شکل ۳۳).



شکل ۳۳- تعیین Address Exclusion

در صورتی که آدرس ها در یک محدوده نباشند چگونه باید آنها را مشخص کنیم؟

کنجکاوی



۶ مدت زمان اختصاص IP به سرویس گیرنده را مشخص کنید.

مدت زمانی که IP در اختیار سرویس گیرنده قرار می گیرد را Leased Duration می گویند. مدت زمان اختصاص IP به سرویس گیرنده را مشخص کرده، روی Next کلیک کنید.

۷ از انجام تنظیمات اختیاری صرف نظر کنید.

سرویس دهنده DHCP می تواند تنظیمات اختیاری دیگری مانند آدرس مسیریاب، آدرس سرویس دهنده DNS و... را نیز به سرویس گیرنده اختصاص دهد.

در پنجره Configure DHCP Option گزینه No, I will configure these options later را انتخاب کرده، روی Next کلیک کرده، دکمه Finish را کلیک کنید.

۸ Scope جدید را فعال کنید.

در این روش نصب باید قبل از استفاده از Scope آن را فعال (Active) کنیم. روی نام Scope راست کلیک کرده، گزینه Active را انتخاب کنید.

تنظیمات پیشرفته Scope

آدرس های اختصاص داده شده به یک سرویس گیرنده به وسیله سرویس دهنده DHCP در بازه های زمانی مختلف ممکن است متفاوت باشد. فرض کنید آدرس اختصاص داده شده به یک سرویس گیرنده امروز 192.168.20.55 باشد. اگر همین سیستم فردا مجدداً از سرویس دهنده درخواست IP کند، ممکن است آدرس دیگری به آن اختصاص داده شود. اگر بخواهیم به یک سیستم خاص برای مثال مدیر سازمان، یک آدرس IP ثابت اختصاص دهیم، باید آدرس IP را در قسمت Reservations وارد کنیم.

MAC Filtering: این امکان را به کاربر می دهد که با استفاده از مک آدرس سرویس گیرنده ها، مانع دسترسی یک یا چند سرویس گیرنده به سرویس DHCP شود.

فیلم شماره ۱۲۱۱۲: تنظیمات پیشرفته و فیلترینگ در Scope

فیلم



فیلم را مشاهده کرده، سپس فعالیت زیر را انجام دهید.

- روی DHCP سروری که نصب کرده اید، یک Scope با شرایط زیر ایجاد کنید:
- بتواند به ۱۰ سیستم آدرس IP اختصاص دهد.
- سومین آدرس IP به هیچ یک از سرویس گیرنده ها داده نشود.
- هر آدرس IP برای مدت ۱ ساعت در اختیار سرویس گیرنده ها قرار گیرد.
- یک آدرس را برای یک سرویس گیرنده رزرو کنید.
- تنظیمی انجام دهید که یکی از سرویس گیرنده ها نتواند از DHCP آدرس بگیرد.

فعالیت کارگاهی





شکل ۳۴- تنظیم سرویس‌گیرنده برای دریافت آدرس از سرویس دهنده DHCP

تنظیم سرویس‌گیرنده برای دریافت آدرس IP از سرویس‌دهنده DHCP

پس از اینکه سرویس‌دهنده DHCP راه‌اندازی شد باید سرویس‌گیرنده برای دریافت آدرس IP به صورت خودکار تنظیم شود تا بتواند سرویس‌دهنده DHCP را شناسایی کرده، تنظیمات لازم را از آن دریافت کند. این تنظیم به طور پیش فرض پس از نصب ویندوز وجود دارد.

کارت شبکه یک سرویس‌گیرنده را به صورتی تنظیم کنید که از DHCP آدرس IP دریافت کند.

فعالیت کارگاهی



حذف آدرس سرویس‌گیرنده

اگر رایانه‌ای در شبکه آدرس IP خود را از سرویس‌دهنده DHCP دریافت کرده باشد، می‌توان با استفاده از دستور `ipconfig/release` آدرس IP را حذف کرد. بعد از اجرای این دستور رایانه دیگر آدرس IP ندارد. سرویس‌دهنده DHCP جدولی از آدرس‌های IP اختصاص داده شده، رزرو شده و مسدود (blocked) دارد. پس از اجرای این دستور آدرس IP رایانه به صورت آماده نشان‌گذاری می‌شود. به این معنا که اگر سرویس‌گیرنده جدیدی درخواست IP کند، سرویس‌دهنده می‌تواند این آدرس را به سرویس‌گیرنده اختصاص دهد.

دریافت آدرس جدید

اگر قصد دریافت یک IP آدرس جدید از سرور DHCP را دارید، بایستی از دستور `ipconfig/renew` استفاده کنید.

سرویس‌گیرنده را به شکلی تنظیم کنید که بتواند از DHCP سرور آدرس IP بگیرد. سپس به وسیله دستورات خط فرمان آدرس IP دریافتی را حذف کنید و دوباره از سرور درخواست اختصاص IP کنید.

فعالیت کارگاهی



بعد از اجرای دستور `ipconfig/release` آدرس IP سیستم شما به چه آدرسی تغییر می‌کند؟ چرا؟

کنجکاوی



برای آدرس‌های IPv6 به جای پارامترهای /release و /renew باید از چه پارامتری استفاده کنیم؟



```
Wireless LAN adapter Wireless Network Connection:
Connection-specific DNS Suffix . : 
Description . . . . . : Intel(R) Wireless-N 7260
Physical Address. . . . . : 0C-8B-FD-7C-C7-C5
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::a4fc:4af8:13eb:d357%13(Preferred)
IPv4 Address. . . . . : 192.168.1.4(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : Thursday, April 05, 2018 11:11:49 AM
Lease Expires . . . . . : Sunday, April 08, 2018 12:56:03 PM
Default Gateway . . . . . : 192.168.1.1
DHCP Server . . . . . : 192.168.1.1
```

شکل ۳۵ - خروجی دستور ipconfig /all

دستور ipconfig /all را در رایانه خود اجرا کرده، سپس مفهوم مواردی که در شکل ۳۵ دور آنها کادر کشیده شده را بنویسید.



کارگاه ۲ سرویس APIPA

۱ تنظیم آدرس را روی حالت خودکار قرار دهید.

۲ در محیط دستوری ویندوز اطلاعات کامل پیکربندی شبکه را مشاهده کنید.

دستور ipconfig /all را اجرا کنید. از اطلاعات نمایش داده شده برای تکمیل ستون دوم جدول ۷ استفاده کنید (شکل ۳۶).

```
Command Prompt
C:\Users\Talif>ipconfig /all

Windows IP Configuration

Host Name . . . . . : server1
Primary Dns Suffix . . . . . : test.com
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
DNS Suffix Search List. . . . . : myzone.com

Ethernet adapter Ethernet:

Connection-specific DNS Suffix . : 
Description . . . . . : Intel(R) 82574L Gigabit Network Connection
Physical Address. . . . . : 00-0C-29-B4-87-99
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::b981:28da:ef99:95ad%12(Preferred)
Autoconfiguration IPv4 Address. . . : 169.254.149.173(Preferred)
Subnet Mask . . . . . : 255.255.0.0
Default Gateway . . . . . : 
DHCPv6 IAID . . . . . : 301993001
DHCPv6 Client DUID. . . . . : 00-01-00-01-21-F8-76-B6-00-0C-29-B4-87-99

DNS Servers . . . . . : fec0:0:0:ffff::1%1
                       fec0:0:0:ffff::2%1
                       fec0:0:0:ffff::3%1
NetBIOS over Tcpip. . . . . : Enabled
```

شکل ۳۶ - نتیجه اجرای دستور ipconfig /all

جدول ۷- اطلاعات پیکربندی شبکه

تنظیمات کارت شبکه	مقدار ۱	مقدار ۲
Physical address		
DHCP enabled		
Autoconfiguration enabled		
IPv4 address		
Subnet mask		

در حالت پیش فرض همه کارت‌های شبکه روی حالت خودکار تنظیم شده‌اند تا تنظیمات آدرس خود را از سرور DHCP دریافت کنند؛ اما اگر سرور DHCP در دسترس نباشد چه اتفاقی می‌افتد؟ آیا کارت شبکه می‌تواند بدون آدرس باشد؟

از آنجایی که کارت شبکه نمی‌تواند بدون آدرس باشد ویندوز از سرویس دیگری به نام APIPA (Automatic Private IP Addressing) برای تنظیم خودکار آدرس IP روی کارت شبکه استفاده می‌کند تا به صورت موقت مشکل آدرس کارت شبکه حل شود و رایانه بتواند به کار خود در شبکه ادامه دهد. در شکل ۳۶ سرویس DHCP فعال است اما چون سرور آن در دسترس نیست، رایانه شما یک آدرس IP در محدوده 169.254.y.z از سرویس APIPA دریافت کرده است. این سرویس به طور پیش فرض روی همه کارت‌های شبکه فعال است.

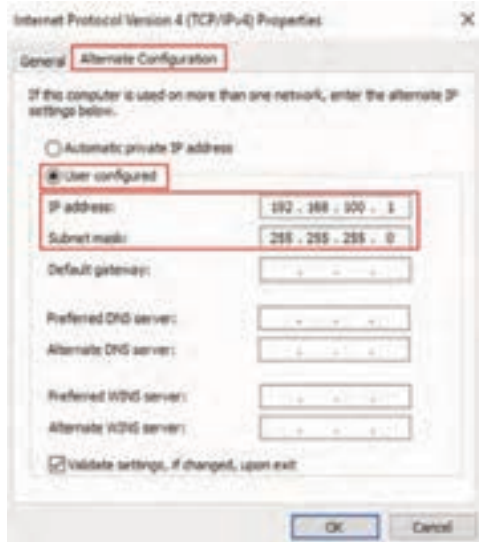
۳ آدرس 192.168.100.Z را به عنوان Alternate Configuration تنظیم کنید.

آدرسی که سرویس APIPA به رایانه اختصاص می‌دهد موقتی است و سرویس APIPA به صورت دوره‌ای و در بازه‌های زمانی پنج دقیقه، حضور سرویس دهنده DHCP را بررسی می‌کند و در صورتی که سرویس دهنده DHCP را در شبکه شناسایی کند، سرویس APIPA متوقف می‌شود و سرویس دهنده DHCP آدرس جدیدی را به سرویس گیرنده اختصاص می‌دهد. این عملیات ترافیک شبکه را افزایش می‌دهد.

برای جلوگیری از تخصیص آدرس موقتی، در برگه Alternate Configuration تنظیمات آدرس را انجام دهید که اگر سرویس دهنده DHCP در دسترس نبود، از این آدرس استفاده شود (شکل ۳۷). z را براساس شماره رایانه خود انتخاب کنید.

۴ دستور `ipconfig /all` را تایپ کنید و تغییرات را در ستون سوم جدول ۷ بنویسید.

نتیجه را با مرحله ۲ مقایسه کنید.



شکل ۳۷- برگه Alternate Configuration

جدول ارزشیابی شایستگی های غیر فنی، بهداشت و توجهات زیست محیطی



شایستگی ها	شرایط عملکرد (ابزار، مواد، تجهیزات، زمان، مکان و...)	نتایج ممکن	استاندارد (شاخص ها/داوری /نمره دهی)	نمره
شایستگی های غیر فنی	مسئولیت پذیری، توجه به جزئیات کار - زبان فنی	قابل قبول	توجه به محدوده مجاز IP آدرس و IP سرورها هنگام ایجاد Scope - بازگرداندن تنظیمات به حالت اولیه پس از انجام عملیات	۲
ایمنی و بهداشت	جلوگیری از ایجاد conflict در IP Address نودها			
توجهات زیست محیطی	دقت در انتخاب محدود IP	غیر قابل قبول	توجه به ایمنی و بهداشت محیط کارگاه	۱
نگرش				

* این شایستگی ها در ارزشیابی پایانی واحد یادگیری باید مورد توجه قرار گیرند.

ارزشیابی مرحله ۱



مراحل کار	شرایط عملکرد (ابزار، مواد، تجهیزات، زمان، مکان و...)	نتایج ممکن	استاندارد (شاخص ها/داوری /نمره دهی)	نمره
ایجاد Scope در DHCP	مکان: کارگاه استاندارد رایانه تجهیزات: شبکه ای از رایانه ها که حداقل یکی از آنها سیستم عامل سرور داشته باشد. زمان: ۲۰ دقیقه	بالاتر از حد انتظار	نصب سرویس DHCP در سیستم عامل سرور - ایجاد Scope و تنظیم پارامترهای Address Pool، Address Reservations و Exclusions - Lease Duration - انجام MAC Filtering و تنظیم client برای دریافت IP	۳
		در حد انتظار	نصب سرویس DHCP در سیستم عامل سرور - ایجاد Scope و تنظیم پارامترهای Address Pool، Address Reservations و Exclusions - Lease Duration - تنظیم client برای دریافت IP	۲
		پایین تر از حد انتظار	نصب سرویس DHCP در سیستم عامل سرور	۱

کارگاه ۳ پشتیبان‌گیری و بازیابی اطلاعات DHCP

آیا تاکنون برای شما اتفاق افتاده است که بخشی از اطلاعاتتان مانند اطلاعات مربوط به نرم‌افزارها و تلفن همراه از بین برود و همیشه افسوس از دست دادن آنها را بخورید؟ برای جبران این اتفاق چه کاری باید انجام داد؟

تهیه نسخه پشتیبان از سرویس مهمی مانند DHCP به خاطر نوع اطلاعاتی که ذخیره می‌کند همیشه حائز اهمیت است. ممکن است بنا به دلایل مختلف مانند مشکلات سخت‌افزاری، مشکلات نرم‌افزاری و غیره دسترسی شما

به سرویس مورد نظر قطع شود. در صورت داشتن نسخه پشتیبان می‌توان با نصب مجدد سرویس و بازگردانی اطلاعاتی که قبلاً پشتیبان‌گیری کرده‌اید بدون از دست دادن اطلاعات کلیدی، مجدداً سرویس را راه‌اندازی کنید.

۱ از اطلاعات DHCP پشتیبان بگیرید.

در کنسول DHCP روی نام سرویس‌دهنده راست کلیک کرده، گزینه Backup را انتخاب کنید.

۲ مسیر ذخیره پرونده پشتیبان را تعیین کنید.

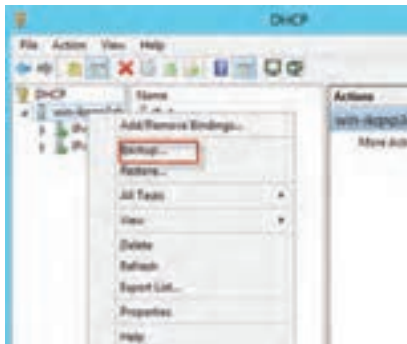
۳ پرونده پشتیبان DHCP را بازیابی کنید.

در صورتی که نیاز به بازیابی اطلاعات داشتید، در کنسول DHCP روی نام سرویس‌دهنده راست کلیک کرده، گزینه Restore را انتخاب کنید.

۴ محل ذخیره پرونده بازیابی شده را تعیین کنید.

۵ راه‌اندازی مجدد سرویس DHCP را تأیید کنید.

پس از تعیین محل ذخیره پرونده بازیابی شده، باید سرویس DHCP راه‌اندازی مجدد شود.



شکل ۳۸- تهیه پشتیبان از DHCP

ارزشیابی مرحله ۲

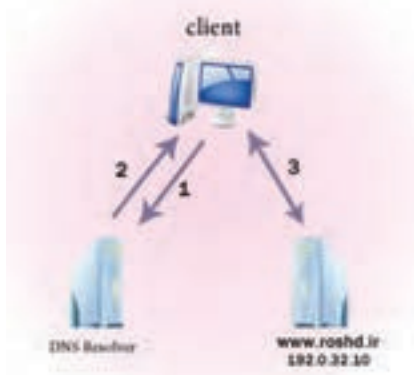


مرحل کار	شرایط عملکرد (ابزار، مواد، تجهیزات، زمان، مکان و ...)	نتایج ممکن	استاندارد (شاخص‌ها/داوری/نمره دهی)	نمره
پشتیبان‌گیری از DHCP و بازیابی آن	مکان: کارگاه استاندارد رایانه تجهیزات: شبکه‌ای از رایانه‌ها که حداقل یکی از آنها سیستم‌عامل سرور داشته باشد. زمان: ۵ دقیقه	بالاتر از حد انتظار	تهیه نسخه پشتیبان و ذخیره آن در مسیر مناسب و بازیابی آن	۳
		در حد انتظار	تهیه نسخه پشتیبان و بازیابی آن	۲
		پایین تر از حد انتظار	تهیه نسخه پشتیبان	۱

آیا تاکنون نیاز به تماس با یک شماره تلفن ثابت متعلق به یک مکان عمومی داشته‌اید که شماره آن را نداشته باشید؟ در این موقعیت چه کاری انجام می‌دهید؟ با راهنمای مشترکین ۱۱۸ مخابرات تماس می‌گیرید و با دادن نام محل مورد نظر شماره تماس آن را از اپراتور دریافت می‌کنید. زمانی که ما قصد اتصال به یک تارنما را داشته باشیم نام آن را در قسمت نشانی مرورگر اینترنت تایپ می‌کنیم. هر تارنما دارای یک آدرس IP است که با همین آدرس IP می‌توان به آن دسترسی داشت. به خاطر سپردن این آدرس‌ها برای کاربران سخت است، بنابراین متخصصان سرویسی را ارائه کردند که کاربران بتوانند از نام برای دسترسی به این تارنماها استفاده کنند. سرویسی که قادر است نام را به آدرس IP تبدیل کند، سرویس DNS می‌نامند. وظیفه DNS تبدیل نام به آدرس IP و برعکس است، مانند تبدیل نام میزبان‌های شبکه و آدرس تارنماها به آدرس IP. عملکرد این سرویس شبیه راهنمای مشترکین ۱۱۸ مخابرات است که با دادن نام تارنما، آدرس IP تارنما را برای کاربر ارسال می‌کند.



سرویس DNS هم در شبکه‌های LAN و هم در شبکه‌های WAN مانند اینترنت کاربرد دارد. **Name resolution** به عمل تبدیل نام به IP گفته می‌شود. ارسال کننده پیام ابتدا نام میزبان یا تارنمای مقصد را به DNS ارسال می‌کند و عمل Name resolution به وسیله سرویس دهنده DNS انجام شده، آدرس IP برای درخواست کننده ارسال خواهد شد.



در شکل ۳۹ سرویس گیرنده ابتدا نام میزبان درخواستی خود را برای سرویس دهنده DNS ارسال کرده، سپس در مرحله ۲ سرویس دهنده، آدرس IP میزبان را برای سرویس گیرنده ارسال می‌کند و در نهایت در مرحله ۳ سرویس گیرنده به وسیله آدرس IP به میزبان مورد نظر دسترسی پیدا می‌کند. البته این عمل در شبکه اینترنت پیچیدگی بیشتری دارد.

شکل ۳۹- مراحل Name Resolution

پویانمایی شماره ۱۲۱۱۳: ساختار DNS

فیلم



فعالیت
کارگاهی



- پس از مشاهده فیلم پاسخ دهید هر کدام از TLDهای ذکر شده در فهرست چه کاربردی دارند؟

- | | |
|-------------------------|---------------------|
| • .com (commercial) | • .net (network) |
| • .org (organization) | • .edu (education) |
| • .mil (military) | • .gov (government) |
| • .co (company) | • .biz (business) |
| • .info (informational) | • .me (personal) |

- بخش های مختلف آدرس های زیر را مانند نمونه در جدول ۸ به تفکیک بنویسید.

1 -media.roshd.ir

2 -www.archive.books.org.ir

3 -www.bing.com.uk

جدول ۸- اجزای آدرس تارنما

Host name	Sub Domain	SLD	TLD	
			gTLD	ccTLD
Server1	Sales.south	microsoft	com	_____

FQDN شامل همه اجزای آدرس از نام میزبان تا ریشه فضای نام ساختار سلسله مراتبی DNS است که نام آنها به وسیله نقطه از هم جدا شده است.

ساختار آدرس [HTTP://fa.wikipedia.org/wiki](http://fa.wikipedia.org/wiki) را بررسی کنید.

پژوهش



نصب سرویس DNS مشابه نصب سرویس DHCP است. سرویس DNS را نصب کنید.

فعالیت
گروهی





مرحله کار	شرایط عملکرد (ابزار، مواد، تجهیزات، زمان، مکان و ...)	نتایج ممکن	استاندارد (شاخص‌ها/دآوری/نمره دهی)	نمره
نصب DNS	مکان: کارگاه استاندارد رایانه تجهیزات: شبکه‌ای از رایانه‌ها که حداقل یکی از آنها سیستم‌عامل سرور داشته باشد. زمان: ۱۵ دقیقه	بالاتر از حد انتظار	نصب سرویس DNS در سیستم‌عامل سرور - تعیین اجزای FQDN طبق ساختار سلسله مراتبی - رسم ساختار درختی سلسله مراتبی و تعیین نام FQDN طبق این ساختار	۳
		در حد انتظار	نصب سرویس DNS در سیستم‌عامل سرور - تعیین اجزای FQDN طبق ساختار سلسله مراتبی	۲
		پایین‌تر از حد انتظار	نصب سرویس DNS در سیستم‌عامل سرور	۱

کارگاه ۴ ایجاد Zone

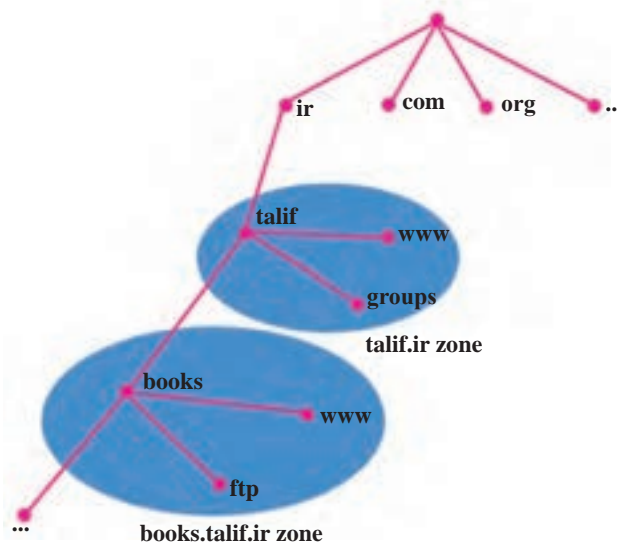
یک Zone می‌تواند فضای نام دامنه را به چند بخش تقسیم کند تا مدیریت هر بخش ساده‌تر شود. در هر Zone آدرس‌های IP و نام میزبان‌های موردنظر برای جست‌وجو وجود دارد که این اطلاعات به صورت رکورد (Resource Record) در بانک اطلاعاتی مربوط به Zone ذخیره می‌شود.

۱ پنجره مدیریت DNS را باز کنید.

گزینه Administrative tools را از Control Panel انتخاب و روی DNS کلیک کنید.

۲ یک Zone جدید از نوع Forward Lookup Zone ایجاد کنید.

به صورت کلی دو نوع Zone وجود دارد:



شکل ۴۰- ساختار سلسله مراتبی DNS و نمایش Zone

● **Forward Lookup Zone**: نام دامنه خواسته شده را به آدرس IP تبدیل می‌کند.

● **Reverse Lookup Zone**: آدرس IP را به نام دامنه تبدیل می‌کند.

برای ایجاد Zone از نوع Forward روی پوشه Forward Lookup Zone راست کلیک کرده، گزینه New Zone را انتخاب کنید (شکل ۴۱).



شکل ۴۱ - ایجاد یک Forward Lookup Zone

۲ نوع Zone را تعیین کند.

در پنجره بعدی Primary Zone را به عنوان نوع Zone انتخاب کرده، روی Next کلیک کنید.

۴ نام Zone را تعیین کنید.

در پنجره باز شده در قسمت Zone name یک نام برای Zone انتخاب کرده، روی Next کلیک کنید. نام Zone معمولاً یک نام چند بخشی مانند Microsoft.com است.

۵ نام پرونده Zone را وارد کنید.

در کادر محاوره‌ای Zone File نام پرونده و تنظیمات پیش فرض را پذیرفته، روی Next کلیک کنید.

۶ نوع به‌روزرسانی اطلاعات رکوردها را تعیین کنید.

در پنجره Dynamic Update تنظیم پیش فرض را پذیرفته، روی Next کلیک کنید.

۷ مشخصات تنظیم شده برای Zone را تأیید کنید.

مشخصات تنظیم شده برای Zone در کادر محاوره‌ای آخر نمایش داده می‌شود. روی دکمه Finish کلیک کنید. Zone موردنظر ایجاد می‌شود.

کارگاه ۵ ایجاد Resource Record

اطلاعات در بانک اطلاعاتی یک Zone به صورت رکوردهایی با نام Resource Record ذخیره می‌شوند. Resource Recordها با توجه به عملکردشان انواع مختلفی دارند که دو نوع پر کاربرد آنها Host و Pointer است.

● **رکورد Host (A)**: این نوع رکورد نام دامنه را به یک آدرس IPv4 مرتبط می‌کند و پرکاربردترین نوع رکورد است.

● **رکورد Pointer (PTR)**: رکورد PTR یا رکورد اشاره‌گر، آدرس IP را به دامنه مورد نظر شما مرتبط می‌کند و برعکس رکورد Host عمل می‌کند.

در این کارگاه قصد داریم، رکورد Host ایجاد کنیم.

۱ پنجره مدیریت DNS را باز کنید.

۲ Zone مورد نظر برای ایجاد رکورد را انتخاب کنید.

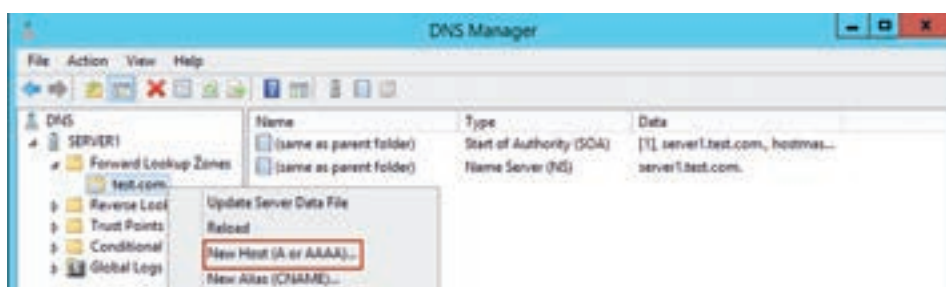
روی Zone ایجاد شده در مرحله قبل دابل کلیک کنید.

۳ رکورد Host ایجاد کنید.

روی نام Zone ایجاد شده راست کلیک کرده، گزینه New Host (A or AAAA)... را انتخاب کنید (شکل ۴۲).

۴ مشخصات رکورد جدید را تعیین کنید.

در پنجره باز شده در بخش Name نام رکورد و در بخش IP address، آدرس IP رکورد مورد نظر را درج کنید.



شکل ۴۲- ایجاد رکورد Host

آیا می‌توان برای IPv6 هم رکورد ایجاد کرد؟

پژوهش



تنظیم آدرس سرویس دهنده DNS در سرویس گیرنده

سرویس گیرنده‌ها برای دسترسی به سرویس دهنده DNS ابتدا باید آدرس سرویس دهنده DNS را داشته باشند. برای مثال ما ابتدا باید شماره راهنمای مشترکین ۱۱۸ در ایران را داشته باشیم تا بتوانیم با آن ارتباط برقرار کرده، درخواست خود را ارائه دهیم. به همین دلیل در سیستم عامل امکان تنظیم آدرس سرویس دهنده DNS وجود دارد. برای این منظور در بخش پایین کادرمحاوره‌ای تنظیم آدرس IP، آدرس سرویس دهنده DNS وارد می‌شود (شکل ۴۳).



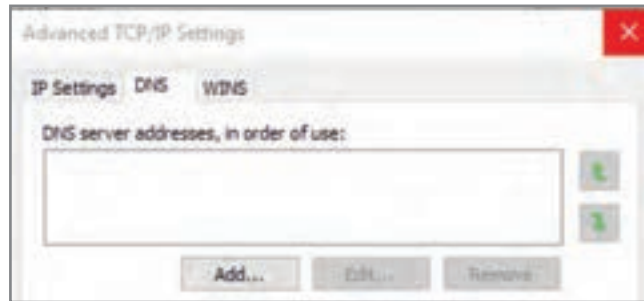
شکل ۴۳- تنظیم آدرس سرور DNS برای سرویس گیرنده

برای دسترسی به سرویس دهنده DNS می‌توان دو آدرس را مشخص کرد:

● Preferred DNS server: آدرس سرویس دهنده DNS که سرویس گیرنده ابتدا سعی می‌کند درخواست‌های خود را به آن ارسال کند.

- Alternate DNS server: در صورتی که Preferred DNS server به هر دلیلی به سرویس گیرنده پاسخ ندهد، سرویس گیرنده درخواست خود را به این سرویس دهنده ارسال می کند.

کاربرد دکمه Add در برگه DNS در بخش Advanced چیست (شکل ۴۴)؟



شکل ۴۴- برگه DNS تنظیمات آدرس IP

فعالیت
کارگاهی



کارگاه ۶ تست سرویس دهنده DNS

بعد از نصب سرویس DNS و تنظیم آدرس IP سرویس دهنده DNS روی سرویس گیرنده، بهتر است از صحت عملکرد این سرویس اطمینان حاصل کرد. برای این کار از دو دستور ping و nslookup می توان استفاده کرد.

۱ پنجره Cmd را باز کنید.

۲ با استفاده از دستور ping صحت عملکرد سرویس دهنده DNS را بررسی کنید.

بعد از تایپ واژه ping نام کامل رکوردی را بنویسید که ایجاد کرده اید. در صورتی که پیام Reply دریافت کنید. به معنی عملکرد صحیح سرویس DNS است (شکل ۴۵).

```
Administrator: Command Prompt

C:\>ping www.test.com

Pinging www.test.com [192.168.20.1] with 32 bytes of data:
Reply from 192.168.20.1: bytes=32 time=8ms TTL=128
Reply from 192.168.20.1: bytes=32 time<1ms TTL=128
Reply from 192.168.20.1: bytes=32 time<1ms TTL=128
Reply from 192.168.20.1: bytes=32 time<1ms TTL=128

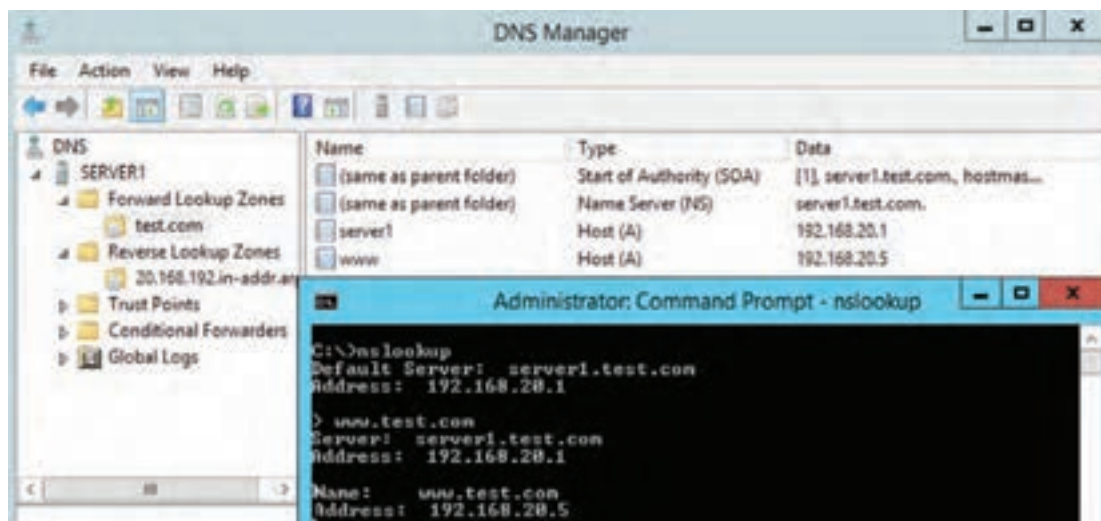
Ping statistics for 192.168.20.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 8ms, Average = 2ms

C:\>
```

شکل ۴۵- تست سرور DNS با دستور ping

۳ با دستور nslookup سرویس دهنده DNS را تست کنید.

در پنجره cmd عبارت nslookup را تایپ کنید. در خط فرمان دستور nslookup نام کامل رکورد ساخته شده در سرویس دهنده DNS را تایپ کرده، کلید Enter را بفشارید (شکل ۴۶).



شکل ۴۶- تست سرویس دهنده DNS با دستور nslookup

در صورتی که نام و آدرس IP صحیح نمایش داده شود، به معنی صحت عملکرد سرویس DNS است.

ارزیابی مرحله ۴



نمره	استاندارد (شاخص‌ها/داوری / نمره دهی)	نتایج ممکن	شرایط عملکرد (ابزار، مواد، تجهیزات، زمان، مکان و ...)	مراحل کار
۳	ایجاد Forward lookup Zone و رکوردهای مورد نیاز - تنظیم IP سرور DNS روی سرویس گیرنده - تست DNS	بالتر از حد انتظار	مکان: کارگاه استاندارد رایانه تجهیزات: شبکه‌ای از رایانه‌ها که حداقل یکی از آنها سیستم عامل سرور داشته باشد. زمان: ۲۰ دقیقه	ایجاد Zone و Resource Record
۲	ایجاد Forward lookup Zone و رکوردهای مورد نیاز - تنظیم IP سرور DNS روی سرویس گیرنده	در حد انتظار		
۱	ایجاد Forward lookup Zone	پایین تر از حد انتظار		

معیار شایستگی انجام کار:

کسب حداقل نمره ۲ از مراحل ایجاد Scope در DHCP و ایجاد Zone و Resource Record
کسب حداقل نمره ۲ از بخش شایستگی‌های غیرفنی، ایمنی، بهداشت، توجهات زیست محیطی و نگرش
کسب حداقل میانگین ۲ از مراحل کار

جدول ارزشیابی پایانی

<p>شرح کار:</p> <p>۱- ایجاد Scope در DHCP</p> <p>۲- پشتیبان‌گیری از DHCP و بازیابی آن</p> <p>۳- نصب DNS</p> <p>۴- ایجاد Zone و Resource Record</p>			
<p>استاندارد عملکرد:</p> <p>نصب سرویس‌های DNS و DHCP و استفاده از آنها در سیستم عامل سرور</p> <p>شاخص‌ها:</p>			
شماره مرحله کار	شاخص‌های مرحله کار		
۱	نصب سرویس DHCP در سیستم عامل سرور - ایجاد یک Scope و تنظیم پارامترهای آن - انجام MAC Filtering و Reservation - انجام تنظیمات لازم روی client		
۲	گرفتن نسخه پشتیبان از DHCP و بازیابی آن		
۳	نصب سرویس DNS در سیستم عامل سرور		
۴	ایجاد یک Forward lookup Zone - ساخت رکوردهایی از نوع Host - تست DNS - تنظیم IP سرور DNS روی سرویس گیرنده		
<p>شرایط انجام کار و ابزار و تجهیزات:</p> <p>مکان: کارگاه رایانه مطابق استاندارد تجهیزات هنرستان‌ها</p> <p>تجهیزات: شبکه‌ای از رایانه‌ها که حداقل یکی از آنها سیستم عامل سرور داشته باشد.</p> <p>زمان: ۶۰ دقیقه (ایجاد Scope در DHCP ۲۰ دقیقه - پشتیبان‌گیری از DHCP و بازیابی آن ۵ دقیقه - نصب DNS ۱۵ دقیقه - ایجاد Zone و Resource Record ۲۰ دقیقه)</p>			
<p>معیار شایستگی:</p>			
ردیف	مرحله کار	حداقل نمره قبولی از ۳	نمره هنرجو
۱	ایجاد Scope در DHCP	۲	
۲	پشتیبان‌گیری از DHCP و بازیابی آن	۱	
۳	نصب DNS	۱	
۴	ایجاد Zone و Resource Record	۲	
	شایستگی‌های غیر فنی، ایمنی، بهداشت، توجهات زیست محیطی و نگرش:	۲	
	مسئولیت‌پذیری - توجه به جزئیات کار - زبان فنی جلوگیری از ایجاد conflict در IP Address نودها دقت در انتخاب محدود IP		
	میانگین نمرات		*
* حداقل میانگین نمرات هنرجو برای قبولی و کسب شایستگی، ۲ است.			

