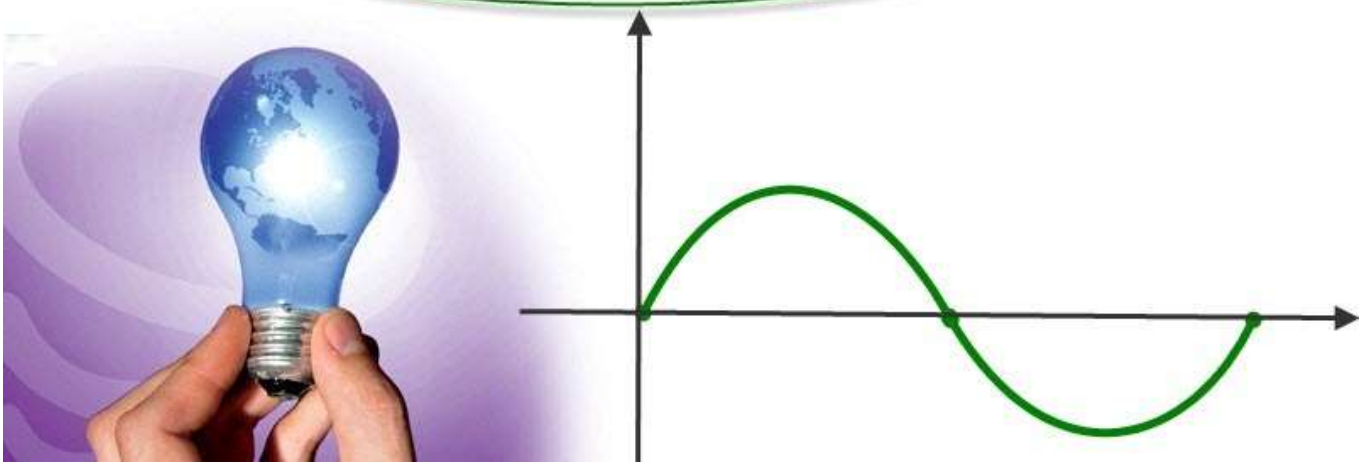

موضوع پروژه:

ویندوز سرور ۲۰۰۳

فهرست :

فصل اول : معرفی ویندوز سِرور ۲۰۰۳

ویندوز سرور ۲۰۰۳ نسبت به ویندوز ۲۰۰۰ گام بزرگی به جلو محسوب می‌شود. برای مدیران شبکه‌های ویندوز NT هم این نگارش جدید سیستم‌عامل مایکروسافت آن قدر ابزار و کنترل‌های مدیریتی زیادی را به ارمغان آورده است که آنها را از ادامه کار با NT منصرف می کند.

ویرایش‌های ویندوز سرور ۲۰۰۳

* ویندوز سرور ۲۰۰۳ ویرایش standard
* ویندوز سرور ۲۰۰۳ ویرایش enterprise (نگارش‌های ۳۲ و ۶۴ بیتی)
* ویندوز سرور ۲۰۰۳ ویرایش datacenter
* ویندوز سرور ۲۰۰۳ ویرایش web server

ویرایش standard

ویرایش standard ویندوز سرور ۲۰۰۳ برای اغلب شبکه‌ها مناسب است. این ویرایش، چندپردازشی متقارن (SMP) چهارراهه و ۴ گیگابابت RAM را پشتیبانی می‌کند. از ویرایش استاندارد می‌توان برای میزبانی network load balancing (ولی نه cluster services) و terminal server استفاده کرد.

ویرایش enterprise

ویرایش enterprise چنان طراحی شده است که همه نیازهای شرکت‌هایی با هر اندازه را برآورده می‌سازد. این ویرایش SMP هشت‌راهه، ۳۲ گیگابایت RAM در نگارش سی و دو بیتی، ۶۴ گیگابایت RAM در نگارش ۶۴ بیتی، و همچنین خوشه‌بندی سرویس‌دهنده‌ها تا هشت گره را پشتیبانی می کند.

ویرایش enterprise جایگزین ویرایش advanced server ویندوز ۲۰۰۰ شده است.

ویرایش datacenter

ویرایش datacenter که قدرتمندترین ویندوز به شمار می‌آید در نگارش سی و دو بیتی، SMPی ۳۲ راهه و در نگارش ۶۴ بیتی، SMPی ۶۴ راهه را پشتیبانی می کند. این ویرایش در نگارش سی و دو بیتی ۶۴ بیتی ۵۱۲ گیگابایت RAM را پشتیبانی می کند.

ویرایش web

این محصول جدید ویندوز برای ایجاد و راه‌اندازی سایت وب ساخته شده است. این ویرایش شامل IIS نگارش ۰/۶ و اجزای دیگری است که امکان میزبانی برنامه‌ها و صفحات وب و سرویس‌های وب XML را فراهم می‌کنند. از ویرایش web نمی‌توان برای راه‌اندازی مزرعهٔ سرویس‌دهندهٔ وب که به خوشه‌بندی نیاز دارد استفاده کرد، و در آن نمی‌توان هیچ گونه سرویس مدیریت شبکه مثل اکتیودایرکتوری، سرویس‌های DNS ، یا سرویس‌های DHCP را نصب نمود.

خدمات نصب راه دور (RIS) در سِرور

قبلاً RIS فقط برای نگارش‌های سرویس‌گیرنده / ایستگاه کاری ویندوز موجود بود، اما اکنون توابع جدید NET RIS را در همه نگارش‌های ویندوز سرور ۲۰۰۳ غیر از datacenter می‌توان به کار گرفت.

Remote desktop در ابتدا در ویندوز ۲۰۰۰ معرفی شد.

نرم‌افزار سرویس‌گیرنده (با نام Remote Desktop Connection) در ویندوز XP (عضو سرویس‌گیرندهٔ خانوادهٔ ویندوز سرور ۲۰۰۳) قرار داده شده است. برای نگارش‌های ویندوز پیش از XP ، می‌توان نرم‌افزار سمت سرویس‌گیرنده را از سی‌دی ویندوز سرور ۲۰۰۳ ، یا از یک نقطه اشتراکی شبکه که حاوی فایل‌های نصب ویندوز سرور ۲۰۰۳ باشد نصب نمود.

فقط با چند کلیک ماوس می‌توان سرویس‌دهنده را برای دستیابی راه دور پیکربندی کرد. همهٔ سرویس‌دهنده‌های ویندوز سرور ۲۰۰۳ یک گروه محلی به نام Remote Desktop Users Group دارند، که می‌توان به آن کاربر اضافه کرد و امنیت آن را پیکربندی نمود.

Remote Assistance

کسانی که در کار کمک‌رسانی به کاربران هستند می‌دانند که معمولا بهترین راه کمک کردن به یک کاربر، رفتن به سراغ ایستگاه کاری اوست. گاهی مشکل آن قدر پیچیده است که نمی‌توان راه‌حل را برای کاربر تشریح کرد، و گاهی کاربر به کمک‌رسانی دقیقی نیاز دارد که اگر بخواهیم صبر کنیم تا او خودش منو یا کادر مکالمه‌های مربوطه را پیدا کند مدت‌ها وقت می‌برد. Remote

Assistance امکان کار بر روی کامپیوتر کاربر از راه دور، بدون این که میز خود را ترک کند را فراهم می‌سازد. Remote Assistance کار خود را به این روش‌ها انجام می‌دهد:

* کمک‌خواهی یک کاربر مبتدی از یک کاربر باتجربه.

*کمک‌رسانی کاربر باتجربه به کاربر مبتدی، بدون این که کاربر مبتدی تقاضای کمک کرده باشد.

استفاده از Remote Assistance در صورتی ممکن است که:

* روی کامپیوترها ویندوز سرور ۲۰۰۳ یا ویندوز XP در حال اجرا باشد.

* کامپیوترها از طریق یک LAN یا اینترنت به هم وصل شده باشند.

تقاضای کمک

کاربر کامپیوتری که ویندوز سرور ۲۰۰۳ یا ویندوز XP روی آن در حال اجراست می‌تواند از کاربر دیگری که پشت کامپیوتر ویندوز ۲۰۰۰ یا ویندوز XP نشسته است تقاضای کمک کند. تقاضاهای Remote Assistance به صورت پیش‌فرض در ویندوز XP فعال هستند، بنابراین کاربر ویندوز XP می‌تواند از هر کاربر باتجربه‌ای که پشت کامپیوتر ویندوز سرور ۲۰۰۳ یا ویندوز XP نشسته است تقاضای کمک کند. اما در کامپیوترهای ویندوز سرور ۲۰۰۳ باید ویژگی Remote Assistance را فعال نمود تا بتوان تقاضای کمک کرد.

کمک‌رسانی بدون دعوت

کاربر مجبور نیست برای تقاضای کمک این همه مراحل را در GUI طی کند؛ او می‌تواند با تلفن (یا راحت‌تر از آن، با صدای بلند) از جایگاه کمک‌رسانی تقاضای کمک کند. در این صورت

فرد پشتیبان می‌تواند با استفاده از ویژگی Remote Assistance مستقیماً به کامپیوتر کاربر وصل شود. در واقع حتی اگر تقاضای کمک (از طریق پُست الکترونیکی یا به صورت شفاهی) هم صورت نگرفته باشد فرد پشتیبان می‌تواند با استفاده از این ویژگی اتصال مستقیم به کامپیوتر وصل شود. اما از آنجا که دستیابی به یک کامپیوتر دیگر، بالقوه خطرآفرین است، اگر این ویژگی با یک سیاست گروه فعال نشده باشد، فرایند با شکست مواجه می‌شود.

فصل دوم : نصب و روش‌های آن

مدل‌های نصب

ویندوز سرور ۲۰۰۳ را در شرایط بسیار مختلفی می‌توان نصب کرد. از نصب یک کپی از سیستم‌عامل بر روی کامپیوتری با یک درایو سخت پارتیشن‌بندی نشدهٔ نو گرفته تا ارتقای یک نگارش قبلی یک سیستم‌عامل ویندوز.

ارتقا

با ارتقای درجا، تنظیمات فعلی، از جمله اکانت کاربران و گروه‌ها، پروفایل‌ها، درایوهای اشتراکی، سرویس‌ها و جوازها حفظ می‌شوند. فایل‌ها و برنامه‌های نصب شده بر روی سیستم، از جمله تنظیمات رجیستری، آیکون‌های میز کار و پوشه‌ها نیز حفظ می‌شوند، اما این بدان معنی نیست که این برنامه‌ها الزاماً با ویندوز سرور ۲۰۰۳ سازگارند.

نصب کامل

در نصب کامل، هیچ چیزی، از جمله تنظیمات رجیستری، سرویس‌ها، پوشه‌ها و فایل‌های غیرمربوط، از سیستم‌عامل قبلی باقی نمی‌ماند. نصب کامل تضمین می‌کند که همه کامپیوترهای ویندوز سرور ۲۰۰۳ در خط پایهٔ خاصی قرار می‌گیرند.

Winnt.exe در مقابل Winnt32.exe

Winnt.exe و Winnt32.exe اسامی رسمی نصب‌کننده‌های شانزده بیتی و سی و دو بیتی هستندت که در همه پلت فرم‌های ویندوز به کار می‌روند. این دو برنامه خدماتی یک مجموعه غنی از انتخاب‌های خط فرمانی برای صب و ارتقای کامپیوترها را در اختیار می‌گذارند، از جمله نصب غیرحضوری، پشتیبانی پویا از به‌روزرسانی، گزارش‌گیری کامل از نصب، و پشتیبانی از Emergency Management Services . بسته به روش مورد نظر برای نصب ویندوز سرور ۲۰۰۳ ، جهت نصب سیستم‌عامل روی کامپیوتر از یکی از این دو می‌توان استفاده کرد:

* Winnt.exe یک برنامه شانزده بیتی است و فقط برای نصب کامل ویندوز سرور ۲۰۰۳ به‌کار می‌رود.
* Winnt325.exe یک برنامه سی و دو بیتی است و آن را می‌توان برای نصب کامل یا ارتقا از یک نگارش سازگار ویندوز به‌کار برد.

استفاده از ***Winnt.exe***

Winnt.exe یک باینری شانزده بیتی است و روی سیستم‌عامل‌های سی و دو بیتی اجرا نمی‌شود. این برنامه را می‌توان روی کامپیوتری که یک نگارش قدیمی‌تر ویندوز را دارد، برای نصب کامل (نه ارتقا) اجرا کرد.

استفاده از ***Winnt32.exe***

Winnt32.exe برنامه سِتاپ باینری سی و دو بیتی است که می‌توان از آن برای نصب کامل، یا ارتقای ویندوز ۹۵ یا نگارش‌های بعدی ویندوز استفاده کرد. هر چند Winnt32.exe می‌تواند روی یک نگارش قدیمی ویندوز اجرا شود، ولی همه نگارش‌ها را نمی‌تواند ارتقا دهد. از Winnt32.exe فقط برای ارتقای نگارش‌های سطح پایین خاصی از سیستم‌عامل‌های سرویس‌دهنده مایکروسافت می‌توان استفاده کرد. اما Winnt32.exe را می‌توان از یک پلت‌فرم غیر قابل ارتقا (مثل ویندوز ۹۸) به منظور بازنویسی کامل سیستم‌عامل جاری، یا اجرای نصبی با بوت دوگانه اجرا نمود.

نصب از روی سی‌دی

احتمالا ساده‌ترین راه نصب استفاده از سی‌دی ویندوز سرور ۲۰۰۳ است، زیرا به هیچ سخت‌افزار اضافی یا به پشتیبانی شبکه نیازی ندارد. علاوه بر این، نصب از روی سی‌دی‌رام معمولا سریع‌تر از هر روش نصب دیگری است، زیرا برای انتقالات I/O ، به پاس پُرسرعت بین سی‌دی‌رام و CPU متکی است نه به اتصالات کُندتر شبکه که در سایر روش‌های نصب مورد استفاده قرار می‌گیرد.

بوت از روی سی‌دی ویندوز سرور ۲۰۰۳

سالهاست که پلت فرم ویندوز رسانه سی‌دی‌رام قابل بوت را پشتیبانی می‌کند و ویندوز سرور ۲۰۰۳ هم این روش نصب ساده و مفید را در اختیار می‌گذارد. به منظور بوت از روی سی‌دی، باید درایو سی‌دی‌ای داشته باشید که ISO 9660 EI Torito برای رسانه قابل بوت را پشتیبانی کند و

بایوس کامپیوتر باید تنظیم شده باشد تا به عنوان اولین وسیلهٔ قابل بوت، از درایو سی‌دی استفاده کند.

از این روش تنها برای نصب ویندوز سرور ۲۰۰۳ می‌توان استفاده کرد و آن را نمی‌توان برای ارتقای یک نگارش قبلی ویندوز به کار برد.

نصب اتوماتیک

نصب اتوماتیک ویندوز سرور ۲۰۰۳ مدیران شبکه را قادر می‌سازد سیستم‌عامل را به آسانی و به سرعت در سرتاسر شبکه نصب کنند. مهم‌تر از آن این که این نصب‌ها بسیار همگون هستند، زیرا در طی فرایند نصب اتوماتیک تمام کامپیوترها از اطلاعات سِتاپ و پیکربندی و از فایل‌های نصب واحدی استفاده می‌کنند.

ویندوز سرور ۲۰۰۳ نصب اتوماتیک را با این سه روش پشتیبانی می‌کند:

* نصب غیرحضوری
* نصب SYSPREP
* Remote Installation Services (RIS)

نصب بر اساس تصویر

یک کامپیوتر اصلی کاملا پیکربندی شدهٔ ویندوز سرور ۲۰۰۳ را در یک یا چند سیستم دیگر کپی می‌کند. SYSPREP یک روش نصب بر اساس تصویر است و RIS می‌تواند نصب بر اساس تصویر نیز انجام دهد.

نصب بر اساس فایل جواب

برای پیکربندی کامپیوترهای ویندوز سرور ۲۰۰۳ از یک فایل متنی استفاده می‌کند. فایل متنی حاوی جواب سوال‌هایی است که برنامه سِتاپ از کاربری که ممکن بود نصب را انجام دهد می‌پرسید، ازجمله اسم کامپیوتر، مُد جواز، و تنظیمات شبکه. سِتاپ غیرحضوری یک روش نصب بر اساس فایل جواب است و RIS می‌تواند یک روش نصب بر اساس فایل جواب نیز باشد.

نصب غیر حضوری

نصب غیرحضوری (یا ستاپ غیرحضوری) به عنوان یک روش نصب بر اساس فایل جواب، به این صورت کار می‌کند که اطلاعات لازم برای نصب را در قالب یک فایل جواب در اختیار برنامه ستاپ ویندوز سرور ۲۰۰۳ قرار می‌دهد. علاوه بر این، ستاپ غیرحضوری می‌تواند هر درایور سخت‌افزار سفارشی مورد نیازی را در اختیار قرار دهد و حتی پس از اتمام ستاپ سیستم‌عامل، بدون دخالت کاربر به نصب برنامه بپردازد. نصب غیرحضوری با استفاده از برنامه‌های ستاپ Winnt.exe و Winnt32.exe آغاز می‌شود:

* از Winnt.exe برای نصب سیستم عامل استفاده می‌شود.
* از Winnt32.exe برای ارتقای یک سیستم عامل موجود استفاده می‌شود.

ایجاد فایل ***UNATTEND.TET*** (ستاپ اتوماتیک)

UNATTEND.TET نام فایل جوابی است که در طی ستاپ غیرحضوری مورد استفاده قرار می‌گیرد. فایل جواب اطلاعاتی را در اختیار می‌گذارد که اگر کاربری به نصب سیستم عامل از طریق

GUI می‌پرداخت وارد می‌کرد. فایل UNATTEND.TXT اطلاعات کلیدیی همچون مالکیت، تنظیمات منطقه‌ای، درایورهای سازندگان دیگر و سایر داده‌هایی را که برای نصب سیستم عامل لازم هستند در اختیار می‌گذارد. با ارائه اطلاعات در فایل UNATTEND.TXT می‌توان ستاپ غیرحضوری را به طور جزئی یا کلی اتوماتیک کرد.

اجرای نصب غیرحضوری

برای شروع نصب غیرحضوری می‌توان از Winnt.exe یا Winnt32.exe استفاده کرد. در اینجا چند نمونهٔ به‌راه‌اندازی نصب غیرحضوری را نشان داده‌ایم تا ببینید که چقدر می‌تواند انعطاف‌پذیر باشد.

Winnnt32.exe / unattend:5:unattend.txt / s:\\installsrv\dist

با استفاده از فایل UNATTEND.TXT که در درایو اشتراکی شبکه تحت عنوان \\installsrv\dist واقع است، ستاپ غیرحضوری را به راه می‌اندازد، و پس از کپی شدن فایل‌ها پنج ثانیه صبر می‌کند و آنگاه کامپیوتر را راه‌اندازی مجدد می‌کند.

winnt / u:unattened.txt / s:d:\i386\e:c:\dcpromo

با استفاده از فایل UNATTEND.TXT که در پوشهٔ i386\ درایو سی‌دی‌رام محلی قرار دارد، ستاپ غیرحضوری را به منظور نصب سیستم‌عامل به راه می‌اندازد، در طی ستاپ ویژگی‌های دسترس‌پذیری را فعال می‌کند و برنامه DCPROMO.EXE را به راه می‌اندازد.

SYSPREP

سالهاست که مدیران سیستم از فرایند تکثیر یک کامپیوتر – یک کپی بایتری از سیستم عامل، رجیستری و برنامه‌ها و همه فایل‌ها و ساختارهای روی درایو سخت کامپیوتر – به منظور ایجاد یک کپی از یک کامپیوتر روی کامپیوتر دیگر استفاده می‌کنند. این فرایند بسیار مفید است زیرا امکان پیکربندی یک یا چند کامپیوتر را در مدت خیلی‌کم فراهم می‌سازد، بدون این که نیازی به وارد کردن اطلاعات جواز باشد.

متأسفانه تکثیر دیسک یک عیب بزرگ هم دارد. این واقعیت که در این روش همه چیزِ روی دیسک کپی می‌شود بدین معنی است که اندک اطلاعاتی که باید در هر کامپیوتری منحصر به فرد باشند، مثل آدرس TCP/IP ، شناسه‌های امنیتی (SID)، و سایر مقادیر نیز کپی می‌شوند. هر چند این مسئله در سیستم‌عامل‌های قدیمی‌تر مایکروسافت مثل ویندوز ۹۵ مشکل بزرگی نبود، ولی در سیستم‌عامل پیچیده‌ای مثل ویندوز سرور ۲۰۰۳ یک مشکل جدی محسوب می‌شود. اگرچه ابزاری مثل NewSIDی (www.sysinternals.com) SysInternals' وجود دارند که برخی از این مقادیر را که باید منحصر به فرد باشند به خوبی تصحیح می‌کنند، اما هیچ یک واقعاً راهی را بری سفارشی کردن تصویر تکثیر شده در اختیار نمی‌گذارند.

SYSPREP نه تنها تخصیص اطلاعات منحصر به فرد به تصاویر تکثیر شده را اتوماتیک می‌کند بلکه برای هر نصبی که از روی یک تصویر تکثیر شده انجام می‌شود اطلاعات سفارشی را در اختیار می‌گذارد. با استفاده از SYSPREP می‌توان به آسانی اطلاعات ساخت سفارشی همچون نام

کامپیوتر، نام دامنه، جواز محصول و حتی اطلاعات فعالیت محصول را در یک ویندوز سرور ۲۰۰۳ی تکثیر شده ادغام نمود.

برنامه SYSPREP و ابزار پشتیبان آن (ازجمله برنامه Setup Manager) در فایل \SUPPORT\TOOLS\DEPLOY.CAB سی‌دی ویندوز سرور ۲۰۰۳ قرار دارند.

ایجاد ***Sysprep.inf***

به منظور استفاده از SYSPREP ایجاد فایل Sysprep.inf الزامی نیست، ولی با ایجاد این فایل می‌توان تعامل با کاربر در طی نصب را به شدت کاهش داد یا حتی حذف کرد. وقتی کامپیوتر مقصد، اولین بار پس از نصب تصویر کامپیوتر اصلی، راه‌اندازی مجدد می‌شود، مرحله‌ای با ورودی کاهش یافته تحت عنوان مینی‌ستاپ آغاز به کار می‌کند که لازم است طی آن شخصی که به نصب کامپیوتر مقصد مشغول است به سوال‌هایی درباره اطلاعات سفارشی کامپیوتر، از جمله تنظیمات شبکه، تنظیمات منطقه‌ای، و عضویت در دامنه یا گروه کاری پاسخ دهد. اما اگر فایل Sysprep.inf در پوشه %SystemDrive%\SYSPREP وجود داشته باشد، مینی‌ستاپ از مقادیر داخل آن فایل استفاده می‌کند.

Sysprep.inf یک فایل متنی است، و از نظر گرامر و ساختار بسیار شبیه فایل UNATTEND.TET که در روش نصب غیرحضوری به کار می‌رود می‌باشد. این فایل دارای بخش‌هایی است که هر کدام مجموعه‌ای از پارامترها و مقادیر را که در هنگام نصب تصویر اصلی روی کامپیوتر مقصد به کار می‌روند در اختیار می‌گذارند. انواع اقلامی که می‌توانند در فایل

Sysprep.inf قرار بگیرند خیلی زیاد هستند و بسیاری از آنها مشابه اقلام فایل UNATTEND.TXT می‌باشند.

اجرای برنامه‌ها پس از اتمام کار ***SYSPREP***

معمولا از SYSPREP به عنوان یک روش نصب تنها وقتی استفاده می‌شود که کامپیوتر تصویر اصلی و همه کامپیوترهای مقصد از سخت‌افزار یکسان یا خیلی مشابهی استفاده کنند.

تکثیر تصویر اصلی در یک فایل

از آنجا که مایکروسافت (هنوز) نرم‌افزاری که این مرحله را انجام بدهد عرضه نکرده یا نفروخته است، برای تکثیر تصویر اصلی به یک قطعه نرم‌افزار سازندگان دیگر نیاز است. محصولات تکثیر بسیارخوبی در بازار وجود دارند، از جمله Ghost متعلق به Symantec Software ، Drive Image متعلق به PowerQuest و NavaDISK متعلق به NovaSTOR . اغلب نرم‌افزارهای تکثیر تجاری سازندگان دیگر، امکان تکثیر تصویر اصلی در انواع رسانه، از جمله یک پارتیشن دیگر دیسک، درایوهای اشتراکی شبکه، CD-R/CD-RW یا یکی از استانداردهای قابل نوشتن DVD را فراهم می‌سازند.

مرحله مینی‌ستاپ

وقتی کامپیوتری که با یک تصویر SYSPREP بازیابی شده است برای اولین بار بوت می‌شود، مراحل زیر اجرا می‌شوند، مگر این که اطلاعات مربوط به آنها در یک فایل Sysprep.inf ارائه شده باشد:

۱- اتصال و اجرا همه سخت‌افزارهای سیستم سازگار را شناسایی می‌کند. معمولا این فرایند حدود سه تا پنج دقیقه طول می‌کشد؛ اما اگر بخش [SysprepMassStorage] فایل Sysprep.inf کاملا پر باشد، این فرایند ممکن است خیلی بیشتر طول بکشد (تا ۴۵ دقیقه!)

۲- از کاربر خواسته می‌شود که End-User License Agreement (EULA) ویندوز سرور ۲۰۰۳ را قبول کند.

۳- از کاربر خواسته می‌شود که نام و سازمان خود را مشخص کند.

۴- از کاربر خواسته می‌شود که به یک گروه کاری یا دامنه بپیوندد.

۵- از کاربر خواسته می‌شود تنظیمات منطقه‌ای سرویس‌دهنده، مانند زبان، نوع واحد پول و منطقه زمانی را مشخص کند.

۶- از کاربر خواسته می‌شود اطلاعات Telephony API (TAPI) ، همچون کُد ناحیه را مشخص کند.

۷- از کاربر خواسته می‌شود پروتکل‌ها، سرویس‌ها و آدرس‌دهی شبکه را مشخص کند.

۸- پوشه SYSPREP به صورت اتوماتیک حذف می‌شود.

۹- کامپیوتر دوباره به راه می‌افتد، و کادر مکالمه ورود ظاهر می‌شود.

Remote Installation Services (RIS)

ویندوز سرور ۲۰۰۳ روش نصب اتوماتیک سومی را هم پشتیبانی می‌کند. RIS چیزی است بین ستاپ اتوماتیک با استفاده از فایل UNATTEND.TXT و SYSPREP .

RIS در کار خود از پارتیشنی روی یک کامپیوتر میزبان ویندوز سرور ۲۰۰۳ استفاده می‌کند که به صورت یک سرویس‌دهندهٔ RIS تنظیم می‌شود. پارتیشن RIS روی این سرویس‌دهنده حاوی یک یا چند تصویر ویندوز سرور ۲۰۰۳ و فایل‌های اختیاری است که این تصویرها را در طی فرایند نصب تغییر می‌دهند.

پس از این که تصویرها روی یک سرویس‌دهندهٔ RIS ایجاد شدند، کامپیوترهای مقصد (سرویس‌گیرنده‌ها) به سرویس‌دهندهٔ RIS وصل می‌شوند و تصویر را از شبکه می‌گیرند و در درایو سخت محلی خود نصب می‌کنند.لازم نیست سرویس‌گیرنده‌ها یک کپی محلی از رسانه نصب یا تصویر داشته باشند، و بر خلاف SYSPREP ، برای ایجاد یا نصب تصویر روی کامپیوترها مقصد به نرم‌افزار تصویربرداری سازندگان دیگر نیازی نیست (البته RIS قادر به استفاده از تصویرهای تولید شده توسط نرم‌افزار تکثیر سازندگان دیگر می‌باشد).

ملزومات ***RIS***

هر چند RIS روش بسیار انعطاف‌پذیری برای نصب ویندوز سرور ۲۰۰۳ است، اما برای استفاده از آن ملزومات سختی هم وجود دارند که عبارتند از:

* RIS برای وصل شدن به سرویس‌دهندهٔ اختصاصی RIS ، به سرویس‌گیرنده‌ها وابسته است. اما بدین منظور سرویس‌گیرنده‌ها باید آداپتور شبکه‌ای داشته باشند که استاندارد بوت از راه دور Pre-Boot Execution (PXE) اینتل را پشتیبانی می‌کند.

* RIS به یک پارتیشن دیسک روی سرویس‌دهندهٔ RIS نیاز دارد تا تصویرهای RIS را نگه دارد، و این پارتیشن باید از سیستم فایل NTFS استفاده کند.

* TCP/IP باید روی سرویس‌دهندهٔ RIS در حال اجرا باشد.

* DHCP ، DNS و اکتیودایرکتوری باید برای شبکه و دامنه‌ای که سرویس‌دهنده و سرویس‌گیرنده‌های RIS روی آن قرار دارند موجود باشند.

* از RIS تنها در ویرایش‌های استاندارد، Enterprise و Datacenter ویندوز سرور ۲۰۰۳ می‌توان استفاده کرد.

نصب سرویس‌دهندهٔ ***RIS***

نصب یک سرویس‌دهندهٔ RIS اولین قدم برای فعال‌سازی RIS است. اگر RIS روی سرویس‌دهندهٔ RIS شما نصب نشده است، این سرویس را می‌توانید با استفاده از بخش Windows Components آپلت Add or Remover Programs پانل کنترل نصب نمایید. پس از نصب، ویزارد ستاپ RIS ، شما را برای طی کردن مراحل پیکربندی سرویس‌دهندهٔ RIS راهنمایی می‌کند.

وقتی ویزارد ستاپ به پایان می‌رسد، با فرض این که کادر انتخاب Respond to Client Computers Requesting علامت خورده باشد، سرویس‌دهندهٔ RIS قادر خواهد بود که تصویر ویندوز سرور ۲۰۰۳ را در اختیار سرویس‌گیرنده‌ها قرار دهد.

استفاده از تصاویر ***RIPrep RIS***

RIS هم مثل SYSPREP کاربر را قادر می‌سازد که تصویر کامپیوتریی که از پیش با برنامه‌ها و درایوهای سفارشی پیکربندی و نصب شده است را ایجاد کند. برنامه خدماتی‌ای که در RIS بدین منظور به کار می‌رود RIPrep نام دارد (Rprep.exe). RIPrep نسبت به SYSPREP چند مزیت دارد، که مهم‌ترین آنها این است که لازم نیست کامپیوترهایی که از یک تصویر واحد استفاده می‌کنند مشابه باشند، یا حتی از کنترل‌کننده ذخیره انبوه یکسانی استفاده کنند (البته لازم است که آنها یک HAL سازگار اشتراکی داشته باشند).

برای این که شخص بتواند تصویری را با RIPrep ایجاد کند، باید روی کامپیوتری که برای ایجاد تصویر به کار خواهد رفت عضو گروه Administators محلی باشد، و باید جواز نوشتن در پوشه‌های (\RemoteInstall) RIS روی سرویس‌دهندهٔ RIS را داشته باشد.

اجرای ویزارد ***Remote Installation Preparation***

پس از این که تصویر ایجاد شد، Riprep.exe را اجرا کنید، که تصویر را در سرویس‌دهندهٔ RIS کپی می‌کند و آن را برای نصب روی کامپیوترهای مقصد آماده می‌سازد.

ویزارد از شما می‌خواهد که اطلاعات سفارشی تصویر را وارد کنید، ازجمله: اسم سرویس‌دهندهٔ RIS (که به صورت پیش‌فرض سرویس‌دهندهٔ RIS ای است که Riprep.exe از آن اجرا می‌شود)، نام پوشه‌ای روی سرویس‌دهندهٔ RIS که می‌خواهید این تصویر را روی آن نصب کنید، و یک توضیح و متن کمکی دوستانه.

فصل سوم : سرویس مسیریابی و دستیابی از راه دور *(RRAS)*

سرویس مسیریابی و دستیابی از راه دور (RRAS) همیشه برای بسیاری از مدیران یک فناوری جذاب و در عین حال پیچیده بوده است. RRAS سرویس‌گیرنده‌های راه دور را قادر می‌سازد تا به منابع شبکهٔ شما وصل شوند و از آنها استفاده کنند، و به این ترتیب مرزهای فیزیکی محیط شبکه را پشت سر می‌گذارد. RRAS همچنین راهی را برای وصل کردن منابع شبکه در اختیار می‌گذارد تا کاربران بتوانند به منابع شبکه‌ها که در غیر این صورت نامتصل می‌بودند دست یابند.

RRAS یک سرویس پُربار است که شامل پشتیبانی برای به‌اشتراک‌گذاری یک اتصال اینترنت، شماره‌گیری سرویس‌دهنده، مسیردهی اطلاعات از یک شبکه به شبکهٔ دیگر، محافظت از داده‌ها از طریق استفاده از یک شبکهٔ خصوصی مجازی (VPN)، و بسیاری چیزهای دیگر می‌باشد. در این فصل مروری خواهیم داشت بر فناوری‌هایی که RRAS در اختیار می‌گذارد و توضیح خواهیم داد که چگونه می‌توانید راه‌حل‌های مناسبی را برای محیط شبکه ویندوز سرور ۲۰۰۳ خود بیابید و مدیریت کنید.

امن کردن RRAS

امن کردن اتصالات دستیابی راه دور دور لازمهٔ پیاده‌سازی موفقیت‌آمیز روش‌های دستیابی راه دور است. اگر اتصالات راه دور را به طور مناسب امن نکنید، این خطر ایجاد می‌شود که محیط شبکه ویندوز سرور ۲۰۰۳ شما به طور گسترده‌ای باز می‌ماند. RRAS ویندوز سرور ۲۰۰۳، امکانات امنیتی

زیادی را در اختیار می‌گذارد، ازجمله رمزگذاری، تأیید اعتبار، تماس مجدد، و کُد شناسایی (ID) شخصی تماس‌گیرنده، که اتصالات راه دور و در نتیجه شبکه شما را استحکام می‌بخشند.

روش‌های تأیید اعتبار

چندین روش تأیید اعتبار وجود دارد که می‌توان آنها را با اتصالات راه دور به کار گرفت. RRAS به طور پیش‌فرض از تأیید اعتبار MS-CHAP و MS-CHAPv2 استفاده می‌کند.

۱- Extensible Authentication Protocol (EAP)

۲- Microsoft Challenge Handshake Authentication Protocol version 2 (MS-CHAPv2)

۳- Microsoft Challenge Handshake Authentication Protocol (MS-CHAP)

۴- Challenge Handshake Authentication Protocol (CHAP)

۵- Shiva Password Authentication Protocol (SPAP)

۶- Password Authentication Protocol (PAP)

این روش‌های تأیید اعتبار را می‌توان در کنسول مدیریت RRAS یافت. برای این کار باید بعد از انتخاب سرویس‌دهندهٔ مورد نظر در کنسول، Properties را برگزینید. آنگاه در برگهٔ Security باید دکمهٔ Authentication Methods را انتخاب کنید. برای استفاده از هر یک از روش‌های تأیید اعتبار، کافی است کادر انتخاب کنار آنها را علامت (✓) بزنید.

تماس مجدد

تمام مجدد دقیقاً همان چیزی است که از نام آن برمی‌آید. یک سرویس‌گیرندهٔ راه دور، سرویس‌دهندهٔ RRAS را شماره‌گیری می‌کند، و اطلاعات اساسی سرویس‌گیرنده (اسم کاربر و کلمهٔ عبور) بررسی می‌شوند. پس از این که اطلاعات بررسی شدند، اتصال قطع می‌شود تا سرویس‌دهندهٔ RRAS بتواند سرویس‌گیرندهٔ راه دور را شماره‌گیری کند. شماره‌ای که سرویس‌دهندهٔ RRAS می‌گیرند می‌تواند طی تماس اول مشخص شود، یا این که از RRAS درخواست می‌شود که یک شمارهٔ خاص را بگیرد. روش دوم، امن‌ترین روش است زیرا محل‌های اتصال راه دور را محدود می‌کند، مزیت دیگر تماس مجدد آن است که در هزینهٔ اتصال سرویس‌گیرندهٔ راه دور صرفه‌جویی می‌شود.

ID تماس‌گیرنده

اغلب شما ID تماس‌گیرنده که در سیستم‌های تلفن به نمایش درمی‌آید و می‌تواند به عنوان مزاحم‌یاب به کار رود را دیده‌اید: کسی که با شما تماس می‌گیرد، و شماره تلفن او روی صفحه نمایش گوشی تلفن شما نشان داده می‌شود. همین کار می‌تواند به منظور امنیت بیشتر در دستیابی‌های راه دور انجام شود.

ID تماس‌گیرنده می‌تواند برای بررسی این که آیا سرویس‌گرندهٔ راه دوری که RRAS را شماره‌گیری کرده است از یک شمارهٔ خاص این کار را انجام داده است یا خیر، به کار رود (یعنی برای تأیید تماس سرویس‌گیرندهٔ راه دور از طریق شمارهٔ تعیین شده). اگر سرویس‌گیرنده، از آن

شماره تماس نگرفته باشد، اتصال قبول نمی‌شود و قطع می‌شود. گاهی ممکن است به دلیل این که قسمتی از POST برای کار با ID تماس‌گیرنده تجهیز نشده، یا این که تماس‌گیرنده مانع به نمایش درآمدن شماره شده است، شرکت تلفن نتواند شمارهٔ تماس گیرنده را در اختیار بگذارد. اگر به هر دلیلی شماره نتواند به نمایش درآید، اتصال برقرار نخواهد شد.

شبکه‌های خصوصی مجازی

شبکه خصوصی مجازی مفهومی است که خیلی دربارهٔ آن صحبت شده است، ولی در کمال تعجب از همهٔ مفاهیم مربوط به اینترنت و دستیابی راه دور کمتر فهمیده شده است. سالهاست که VPNها وجود دارند، ولی تا به حال توجه زیادی به آنها نشده است. VPNها از زمان پیاده‌سازی RRAS در ویندوز NT نگارش ۴ ، توسط مایکروسافت پشتیبانی می‌شدند و همچنان در RRAS ویندوز سرور ۲۰۰۳ نیز پشتیبانی می‌شوند.

بخشی از این سردرگمی‌ها مربوط به این است که کلمهٔ «خصوصی» چه معنی می‌دهد، چرا که مدتهاست که مثلا شرکت‌ها از طریق خطوط استیجاری اختصاصی، اتصالات سایت‌های خود (ازجمله شعب خود) را برقرار کرده‌اند. چنین شبکهٔ خصوصی‌ای در واقع شبکه‌ای است که توسعه یافته است تا به نواحی دور برسد. این را VPN بر اساس حامل نیز می‌خوانند. ISP (یا شرکت تلفن) مدارات مجازی را بین سایت‌ها بر پا می‌کند. برای ایجاد اتصال خصوصی، دو نوع مدار مجازی وجود دارد، مدار مجازی دائمی (PVC) و مدار مجازی سوئیچی (SVC)، که PVC رایج‌تر است.

در ادامه این بحث به VPNهای بر اساس حامل نخواهیم پرداخت، بلکه VPN اینترنت را مورد بررسی قرار می‌دهیم که RRAS آن را پشتیبانی می کند. به وسیلهٔ VPN اینترنت، دو کامپیوتر یا شبکه می‌توانند از طریق شبکه‌ای مثل اینترنت که در حالت معمول اشتراکی یا عمومی است، ارتباط خصوصی برقرار کنند. به این ترتیب هر یک از شبکه‌های خصوصی نیز توسعه می‌یابد، بدون این که لازم باشد یک ISP یا شرکت تلفن یک پیوند مجزای اضافی را بر پا کند تا اتصال را برقرار سازد. به این ترتیب در هزینه‌های شما خیلی صرفه‌جویی می‌شود. VPNها به اتصالات سایت به سایت محدود نمی‌شوند، آنها سرویس گیرنده‌های راه دور همچون کسانی که در خانه یا در سفر هستند را نیز قادر می‌سازد که به صورتی امن به شبکهٔ شرکت خود وصل شوند. به عنوان مثال، یک سرویس گیرندهٔ راه دور (به منظور صرفه‌جویی در هزینهٔ تلفن) ISP محلی خود را شماره‌گیری می کند و سپس VPN ای را از طریق اینترنت به شبکهٔ شرکت خود برقرار می‌سازد.

VPN ها امنیت و قابل اطمینان بودن را به اتصالی می‌افزایند که در حالت عادی یک اتصال ناامن در میان یک شبکه عمومی است. VPN اساساً از سه فناوری تشکیل می‌شود که وقتی با هم به‌کار می‌روند، اتصال امن را تشکیل می‌دهند. این سه فناوری عبارتند از: تأیید اعتبار، تونل زدن، و رمزگذاری.

نصب RRAS

وقتی Server ویندوز سرور ۲۰۰۳ را نصب می کنید، RRAS نیز به صورت اتوماتیک برای شما نصب می‌شود، ولی به صورت غیر فعال. این بدان معنی است که اگر آن را فعال نکنید، از منابع با

ارزش استفاده نخواهد کرد. به منظور استفاده از RRAS ، چه برای دستیابی راه دور، چه برای مسیریابی، و چه برای راه‌اندازی یک VPN بین سایت‌ها، لازم است که اول RRAS را فعال کنید.

فعال کردن RRAS

فعال‌کردن RRAS نیز به همان راحتی نصب کردن آن انجام می‌شود. از آنجا که پس از نصب Server ویندوز سرور ۲۰۰۳ ، سرویس RRAS به طور پیش‌فرض غیرفعال خواهد بود، ابتدا باید آن را فعال کنید. برای فعال کردن این سرویس لازم است جوازهای مدیریتی داشته باشید، یا این که عضوی از گروه امنیتی RAS and IAS Servers دامنه باشد. برای فعال کردن RRAS ، دستورالعمل زیر را دنبال کنید:

۱- در منوی Start/Programs/Administrative Tools ، گزینهٔ Routing and Remote Access را انتخاب کنید تا مدیر افزار Routing and Remote Access باز شود.

۲- در قاب سمت راست، نام سرویس‌دهنده‌ای را برگزینید که می‌خواهید فعال کنید و سپس در منوی Action ، بر روی Configure and Enable Routing and Remote Access کلیک کنید. با انجام چنین کاری ویزاردی با عنوان Routing and Remote Access Server Setup باز می‌شود و شما می‌توانید شروع به پیکربندی RRAS کنید.

قدم بعد آن است که نوع استفادهٔ خود از RRAS را پیکربندی نمایید.

ویزارد Routing and Remote Access Server Setup چهار انتخاب را برای پیکربندی‌های عمومی، و انتخاب پنجمی را برای پیکربندی سفارشی (Custom) در اختیار می‌گذارد. این ویزارد

فقط برای پیکربندی اولیهٔ RRAS روی یک سرویس‌دهنده موجود است. پس از این که گزینه‌های پیکربندی اولیه که ویزارد در اختیار می‌گذارد را شناختید، گزینه‌ای که از همه بیشتر به پیکربندی نهایی مورد نظر شما شبیه است را انتخاب کنید. ویزارد یک پیکربندی پیش‌فرض را ایجاد می‌کند که می‌توانید آن را بر اساس نیازهای خود اصلاح کنید.

پیکربندی دستیابی راه دور (شماره‌گیری یا VPN)

این انتخاب سرویس‌دهندهٔ ویندوز سرور ۲۰۰۳ را پیکربندی می‌کند تا اتصالات شماره‌گیری ورودی را از سرویس‌گیرنده‌های راه دور قبول کند. راه دیگر آن است که سرویس‌گیرنده‌ها با استفاده از یک اتصال VPN وصل شوند. با پیکربندی RRAS به صورت یک سرویس‌دهندهٔ VPN، سرویس‌گیرنده‌های راه دور اجازه می‌یابند تا از میان یک شبکه عمومی همچون اینترنت و از طریق یک تونل رمزگذاری شده، به محیط شبکه ویندوز سرور ۲۰۰۳ شما دست یابند.

به منظور پیکربندی این انتخاب، چنین کنید:

۱- Routing and Remote Access را از طریق منوی Start/Administrative Tools باز کنید.

۲- در منوی Action، گزینهٔ Configure and Enable Routing and Remote Access را انتخاب کنید. وقتی پنجرهٔ ویزارد Routing and Remote Access Server Setup باز شد، Next را کلیک کنید تا کار ادامه یابد.

۳- Remote access (Dial-up or VPN) را انتخاب کرده و Next را کلیک کنید.

۴- پنجرهٔ بعدی که می‌بینید دو انتخاب را در اختیار می‌گذارد: VPN و Dial-up . بسته به این که می‌خواهید کاربران راه دور چگونه به شبکه شما وصل شوند، یکی یا هر دوی این انتخاب‌ها را برگزیده و Next را کلیک کنید.

۵- اگر هر دو انتخاب را برگزیده باشید، پنجرهٔ اتصال VPN به نمایش درمی‌آید. این پنجره، واسطهای شبکه‌ای که در سرویس‌دهنده نصب هستند را نشان می‌دهند. واسطی را که کاربران راه دور به آن وصل خواهند شد را انتخاب کنید، یعنی واسطی که دارای آدرس IP یا اسم DNS ای است که سرویس‌گیرندهٔ VPN کاربران به آن وصل خواهد شد. اگر واسط شبکه‌ای که انتخاب کرده‌اید به دستیابی VPN اختصاص داده شده است (یعنی هیچ‌کس از طریق این واسط به سرویس‌دهنده وصل نمی‌شود مگر با استفاده از یک اتصال VPN)، می‌توانید انتخاب Enable security on the selected interface by setting packet filters را برگزینید. در این صورت فقط به بسته‌هایی اجازهٔ عبور داده می‌شود که توسط درگاه‌های TCP و UDP ای فرستاده می‌شوند که در پیکربندی VPN سرویس‌دهنده مشخص شده‌اند، و همهٔ بسته‌های دیگر حذف می‌شوند. پس از این که انتخاب‌های خود را به عمل آورید Next را کلیک کنید.

۶- اکنون باید انتخاب کنید که می‌خواهید آدرس‌های IP چگونه به سرویس‌گیرنده‌های راه دور اختصاص داده شوند. اگر شبکه شما برای تخصیص آدرس به سرویس‌گیرنده‌ها، از یک سرویس‌دهندهٔ DHCP استفاده می‌کند، این انتخاب را توصیه می‌کنیم. در غیر این

صورت محدوده‌ای از آدرس‌های IP را مشخص کنید تا RRAS بتواند آنها را اختصاص بدهد و انتخاب From a specified rang of addresses را برگزینید. اگر این انتخاب را برگزیده‌اید Next را کلیک کنید و محدودهٔ مورد نظر را در صفحه بعد مشخص نمایید. Next را کلیک کنید تا کار ادامه یابد.

۷- انتخاب کنید که آیا می‌خواهید همین حالا یک سرویس‌دهندهٔ RADIUS را پیکربندی کنید یا خیر (پیش‌فرض خیر است). اگر قرار نیست که سرویس‌گیرنده‌های راه دور برای وصل شدن از یک VPN استفاده کنند، حفظ حالت پیش‌فرض توصیه می‌شود.

۸- اگر انتخاب کرده باشید که یک سرویس‌دهندهٔ RADIUS را پیکربندی کنید، پنجرهٔ RADIUS Server Selection به نمایش درمی‌آید. اسم یا آدرس سرویس‌دهنده(های) RADIUS خود و کلمهٔ عبور را وارد کرده و Next را کلیک کنید.

۹- Finish را کلیک کنید تا کار خاتمه یابد.

پیکربندی NAT در مسیریاب

مسیریابی که NAT در آن فعال شده باشد، امنیت ارتباطات سرویس‌گیرنده به اینترنت را افزایش می‌دهد. به طور معمول همهٔ بسته‌های IP ، آدرس IP کامپیوتری که بسته را تولید کرده است را در خود دارند، یعنی آدرس IP مبدأ و شمارهٔ درگاه را. مسیریابی که NAT در آن فعال شده است، آدرس IP و شماره درگاه بسته را ذخیره می‌کند، و آنها را با یک آدرس IP عمومی ثابت و یک شمارهٔ درگاه که فقط بدین منظور در مسیریاب استفاده می‌شود تعویض می‌کند. وقتی مسیریاب

بسته‌ای با آن آدرس IP عمومی را دریافت می‌کند، از شمارهٔ درگاه (که اکنون در فیلد درگاه مقصد بسته است) استفاده می‌کند تا فیلد آدرس IP مقصد و درگاه بسته را دوباره با آدرس IP و درگاه واقعی سرویس‌گیرنده جایگزین نماید. NAT اساساً آدرس IP واقعی سرویس‌گیرنده را برای همهٔ ارتباطات خارجی مخفی می‌کند، و فقط بسته‌هایی را به شبکهٔ داخلی می‌فرستد که پاسخی به یک تقاضای برنامهٔ یک سرویس‌گیرندهٔ فعال باشد، یا به نظر برسد که این طور است.

انتخاب دوم مربوط به پیکربندی ویندوز سرور ۲۰۰۳ به عنوان یک مسیریاب Internet Connection Server با استفاده از NAT و از طریق وصل شدن به یک NIC است. این انتخاب، موارد زیر را پشتیبانی می‌کند:

* چند آدرس IP عمومی
* چند واسط SOHO
* محدودهٔ قابل پیکربندی آدرس‌های IP برای سرویس‌گیرنده‌های شبکه

برای پیکربندی یک سرویس‌دهندهٔ ویندوز سرور ۲۰۰۳ به صورت مسیریابی که از NAT استفاده می‌کند، به این صورت عمل کنید:

۱- Routing and Remote Access را از منوی Start/Programs/Administrative Tool باز کنید.

۲- از منوی Action ، گزینه Configure and Enable Routing and Remote Access را انتخاب کنید. وقتی پنجرهٔ ویزارد Routing and Remote Access Server Setup باز شد، Next را کلیک کنید.

۳- Network Address Translation (NAT) را انتخاب کرده و Next را کلیک کنید.

۴- Use this public interface to connect to the Internet را انتخاب کرده، سپس بر روی واسط مورد نظر کلیک کنید، Next را کلیک کنید.

۵- اگر ویزارد نتواند سرویس‌دهنده‌های DNS و DHCP شبکه را پیدا کند، پنجره‌ای به نمایش درمی‌آید که پیشنهاد می‌کند آنها را روی این سرویس‌دهنده بر پا کنید، یا این که بعداً آنها را پیکربندی نمایید. توصیه ما این است که انتخاب وجود DNS و DHCP در شبکه اطمینان حاصل نمایید. Next را کلیک کنید.

۶- در این مرحله کار پیکربندی مسیریاب NAT به پایان می‌رسد. Finish را کلیک کنید.

۷- گزینهٔ آخر، ویزارد Demand-Dial Interface را به کار می‌اندازد.

پیکربندی VPN و NAT

ویزارد RRAS Setup انتخابی را در اختیار می‌گذارد برای این که بتوان یک سرویس‌دهنده ویندوز سرور ۲۰۰۳ را به آسانی به صورت یک سرویس‌دهندهٔ VPN و همچنین یک مسیریاب با NAT پیکربندی کرد. در این انتخاب، عناصر فرایند ستاپ برای دستیابی راه دور از طریق VPN و

پیکربندی مسیریاب با استفاده از NAT ترکیب شده‌اند. هر دوی این فرایندها را قبلا در این فصل توضیح داده‌ایم، لذا در اینجا دوباره به جزئیات اشاره نمی‌کنیم. به منظور انجام این کار:

۱- Routing and Remote Access را از منوی Start/Program/Administrative Tools باز کنید.

۲- در منوی Action ، گزینه Configure and Enable Routing and Remote Access را انتخاب کنید. وقتی پنجرهٔ ویزارد Routing and Remote Access Server Setup باز شد، Next را کلیک کنید.

۳- Virtual Private Network (VPN) Access and NAT را انتخاب کرده و سپس Next را کلیک کنید. مراحل بعدی مشابه مراحلی هستند که در بخش‌های قبلی، یعنی «پیکربندی دستیابی راه دور (شماره‌گیری با VPN)» و «پیکربندی NAT در مسیریاب» توضیح داده‌ایم.

پیکربندی یک اتصال امن بین دو شبکه خصوصی

ویزارد RRAS Setup برای پیکربندی یک اتصال امن از یک سرویس‌دهندهٔ ویندوز سرور ۲۰۰۳ به یک سرویس‌دهندهٔ ویندوز سرور ۲۰۰۳ دیگر در یک شبکه راه دور که RRAS روی آن در حال اجراست انتخابی را در اختیار می‌گذارد. این انتخاب، از طریق اینترنت یا از طریق یکی از اتصالات شماره‌گیری در صورت تقاضا، یک اتصال VPN را به شبکهٔ راه دور پشتیبانی می‌کند. قسمتی از فرایند ستاپ که در ویزارد RRAS Setup وجود دارد صرفاً مقدمات کار را انجام می‌دهد، یعنی RRAS را با پشتیبان VPN نصب می‌کند، و اگر انتخاب کرده باشید، ویزارد Demand-Dial

Interface را به کار می‌اندازد. اما پس از این که کار ویزارد تمام شد، شما باید سایر خصوصیات پیوند را پیکربندی کنید.

به منظور فعال کردن RRAS برای این که یک پیوند امن را به دو شبکهٔ خصوصی برقرار کند چنین کنید:

۱- در منوی Start/Program/Administrative Tools گزینهٔ Routing and Remote Access را انتخاب کنید.

۲- در منوی Action ، گزینه Configure and Enable Routing and Remote Access را انتخاب کنید. وقتی ویزارد Routing and Remote Access Server Setup باز شد، Next را کلیک کنید.

۳- Secure connection between two private networks را انتخاب کرده و سپس Next را کلیک کنید.

۴- انتخاب کنید که آیا می‌خواهید از یک اتصال واسط شماره‌گیری در صورت تقاضا به منظور وصل شدن به شبکه راه دور استفاده کنید یا خیر، و سپس Next را کلیک کنید.

۵- اگر استفاده از اتصال واسط شماره‌گیری در صورت تقاضا را انتخاب کرده باشید، پنجرهٔ IP Address Assignment به نمایش درمی‌آید که از شما می‌خواهد بین استفاده از یک آدرس IPای به صورت اتوماتیک اختصاص داده شده (DHCP) برای اتصال راه دور، یا آدرسی که از محدودهٔ خاصی از آدرس‌ها انتخاب می‌شود، یکی را انتخاب کنید. اگر

سرویس‌دهندهٔ DHCPای وجود داشته باشد، DHCP انتخاب ارجح است. پس از این که انتخاب خود را کردید، Next را کلیک کنید. اکنون Finish را کلیک کنید تا ویزارد RRAS Setup به پایان برسد.

۶- اگر استفاده از یک اتصال واسط شماره‌گیری در صورت تقاضا را انتخاب کرده باشید، در این هنگام ویزارد Demand-Dial Interface به نمایش درمی‌آید.

پیکربندی RRAS به صورت سفارشی

آخرین انتخابی که در ابتدای ویزارد RRAS Setup عرضه می‌شود، امکان ایجاد یک پیکربندی سفارشی (با استفاده از هر یک از امکانات موجود RRAS) را فراهم می‌سازد. اگر این انتخاب، یعنی Custom Configuration را برگزینید، ویزارد، اجزای RRAS لازم برای پشتیبانی از انواع اتصالاتی که شما تقاضا می‌کنید را نصب می‌کند، ولی از شما هیچ اطلاعاتی برای پیکربندی اتصالات خاص نمی‌خواهد. این کار به شمار واگذار می‌شود، تا پس از پایان ویزارد، آن را انجام دهید.

به منظور پیکربندی RRAS به صورت سفارشی، دستورالعمل زیر را دنبال کنید:

۱- از منوی Start/Program/Administrative Tools گزینهٔ Routing and Remote Access را انتخاب کنید.

۲- در منوی Action ، گزینهٔ Configure and Enable Routing and Remote Access را انتخاب کنید. هنگامی که ویزارد Routing and Remote Access Server Setup باز شد، Next را کلیک کنید.

۳- Custom Configuration را انتخاب کرده و Next را کلیک کنید.

۴- پنجرهٔ Custom Configuration باز می‌شود و به شما امکان انتخاب هر یک از این موارد را می‌دهد:

* دستیابی از طریق VPN
* دستیابی به صورت شماره‌گیری
* اتصالات شماره‌گیری در صورت تقاضا
* NAT و فایروال ساده
* مسیریابی در LAN

۵- یک یا همهٔ انتخاب‌های مورد نظر را برگزیده، Next را کلیک کنید. با این کار پنجره‌ای باز می‌شود که نشان‌دهندهٔ اتمام کار است. پس از ملاحظهٔ اطلاعات ارائه شده در آن، Finish را کلیک کنید.

پیکربندی سرویس‌گیرنده‌های RRAS

پیکربندی سرویس‌گیرنده‌ها به منظور این که از راه دور وصل شوند در ویندوز سرور ۲۰۰۳ کار نسبتاً ساده‌ای است. RRAS سایر سیستم‌عامل‌های سرویس‌گیرنده، از جمله ویندوز NT ، ویندوز

9X ، انواع یونیکس، مکینتاش، و... را برای وصل شدن از راه دور پشتیبانی می‌کند، ولی ما در این بخش به سرویس‌گیرنده‌های ویندوز ۲۰۰۰ و ویندوز XP می‌پردازیم.

پس از این که مودم را روی سرویس‌گیرنده نصب کردید، می‌توانید اتصال به سرویس‌دهندهٔ RRAS را پیکربندی نمایید. بدین منظور باید مراحل زیر را دنبال کنید.

از سرویس‌گیرنده ویندوز ***XP***

۱- در منوی Start/Settings پوشهٔ Network Connections را باز کنید.

۲- آیکون New Connection Wizard را دابل کلیک کنید تا ویزارد New Connection به کار بیفتد. در اولین پنجرهٔ ویزارد، Next را کلیک کنید.

۳- انتخاب Connect to the network at my workplace مربوط به وصل شدن به سرویس‌دهندهٔ RRAS است که ایجاد اتصالات شماره‌گیری و VPN را پشتیبانی می‌کند. Next را کلیک کنید.

۴- پنجرهٔ Network Connection از شما می‌خواهد که بین اتصال شماره‌گیری و VPN ، یکی را انتخاب کنید. پس از انتخاب Next را کلیک کنید.

۵- پنجرهٔ بعدی از شما می‌خواهد که اسمی را برای اتصال مشخص نمایید. پس از انجام این کار Next را کلیک کنید.

۶- اگر در حال پیکربندی اتصال VPN هستید، ممکن است پنجرهٔ Public Network ظاهر شود، که از شما می‌پرسد که آیا می‌خواهید پیش از تلاش برای ایجاد اتصال مجازی VPN

، شبکه را شماره‌گیری کنید. اگر انتخاب کنید که ابتدا شبکه شماره‌گیری شود، می‌توانید یک اتصال شماره‌گیری موجود را انتخاب کرده یا شماره‌گیری دستی را برگزینید. Next را کلیک کنید.

۷- پنجرهٔ بعدی از شما می‌خواهد که یک شماره تلفن را برای شماره‌گیری، یا یک اسم میزبان (یا آدرس) را برای یک اتصال VPN مشخص کنید.اگر می‌خواهید شماره تلفن را وارد کنید، آن را به همان صورتی که از تلفن خود شماره‌گیری می‌کنید وارد نمایید، Next را کلیک کنید.

۸- انتخاب کنید که آیا می‌خواهید این اتصال را همه استفاده کنند یا فقط خودتان استفاده کنید. Next را کلیک کنید.

۹- در پنجرهٔ نشان‌دهندهٔ اتمام کار، پس از مطالعهٔ اطلاعات ارائه شده، Finish را کلیک کنید.

مدیریت و عیب‌یابی RRAS

همانند بسیاری از سرویس‌های ویندوز سرور ۲۰۰۳ ، پس از نصب و پیکربندی RRAS ممکن است لازم باشد بارها آن را مدیریت کرده و عیب‌یابی نمایید. به عنوان مثال، ممکن است بخواهید تنظیمات RRAS را تغییر دهید، منابعی را اضافه نمایید، بر اتصالات نظارت کنید یا کارهای دیگری را انجام دهید. مدیریت RRAS این امکان را فراهم می‌سازد که عملکرد آن را برای محیط خود سفارشی کرده و پیاده‌سازی آن را به‌روزرسانی نگه دارید.

مدیریت چند سرویس‌دهندهٔ RRAS

مدیریت محیط شبکهٔ ویندوز سرور ۲۰۰۳ ای که بیش از یک سرویس‌دهندهٔ RRAS دارد فوق‌العاده سخت خواهد بود اگر مجبور باشید که برای مدیریت تک تک دستگاه‌ها به سراغ آنها بروید. افزار Routing and Remote Access به طور پیش‌فرض فقط کامپیوتر محلی را در فهرست سرویس‌دهنده‌های خود به نمایش درمی‌آورد. اما به منظور راحتی کار می‌توان سایر سرویس‌دهنده‌های RRAS را هم به این افزار اضافه کرد تا امکان مدیریت آنها از یک محل مرکزی فراهم شود.

به منظور اضافه کردن یک سرویس‌دهندهٔ دیگر به افزار Routing and Remote Access چنین کنید:

۱- در قاب راست افزار Routing and Remote Access ، بر روی Server Status کلیک‌راست کرده و Add Server را انتخاب نمایید.

۲- در کادر مکالمهٔ Add Server ، یکی از چهار انتخابی که برای پیدا کردن و اضافه کردن یک سرویس‌دهندهٔ RRAS دیگر ارائه می‌شود را برگزینید:

* This Computer : کامپیوتر محلی.

* The following computer : این امکان را فراهم می‌سازد که اسم کامپیوتری را که می‌خواهید اضافه کنید را مشخص نمایید.

* All Routing and Remote Access Computers : در صورت برگزیدن این انتخاب باید اسم دامنه‌ای که می‌خواهید همهٔ سرویس‌های RRAS آن اضافه شوند را مشخص کنید. این انتخاب وقتی مفید است که سرویس‌دهنده‌های RRAS زیادی داشته باشید و بخواهید همهٔ آنها را از یک محل مرکزی مدیریت نمایید، یا وقتی که اسم سرویس‌دهندهٔ RRAS را ندانید.

* Browse Active Directory (AD) : اگر می‌خواهید سرویس دایرکتوری را مرور کنید تا یک یا چند سرویس‌دهندهٔ RRAS را در دامنه یا درخت پیدا کنید، باید این انتخاب را برگزینید.

توصیهٔ ما استفاده از واسط RRAS است، به خصوص اگر با فرمان route آشنا نباشید. علاوه بر این در صورت استفاده از این واسط کمتر احتمال دارد که دچار خطای گرامری، یا بدتر از آن، اشتباه در پیکربندی بشوید.

به منظور اضافه کردن یک مسیر ایستا با استفاده از افزار RRAS چنین کنید:

۱- از منوی Start/Programs/Administrative Tools ، پوشهٔ Routing and Remote Access را باز کنید.

۲- از قاب چپ پنجرهٔ کنسول، درخت کنسول را بسط دهید تا فقرهٔ Static Routes در زیر درخت IP Routing نمایان شود.

۳- اگر می‌خواهید یک مسیر ایستا را برای مسیریابی IP اضافه کنید، New Static Route را انتخاب کنید تا پنجرهٔ Static Route به نمایش درآید.

۴- اطلاعات لازم مربوط به موارد زیر (برای یک مسیر IP ایستا) را وارد نمایید:

* Interface : واسط شبکه‌ای که برای پیکربندی مسیر ایستا مورد استفاده قرار می‌گیرد.

* Destination : کامپیوتر یا مسیریابی که مسیردهی به اطلاعات در آن صورت می‌گیرد.

* Network mask : آدرس شبکه‌ای که از مسیر استفاده خواهد کرد.

* Gateway : آدرس IP ای که بسته‌ها باید به منظور مسیردهی شدن به آن فرستاده شوند؛ این معمولا دروازهٔ پیش‌فرض است.

* Metric : تعداد هاپ‌هایی که تا مقصد وجود دارند.

۵- OK را کلیک کنید.

فصل چهارم : معرفی دایرکتوری فعال

مفهوم دایرکتوری فعال

خدمات دایرکتوری پایگاه داده‌ای است که اطلاعات آن در یک هرم و با سلسله مراتب مشخص منظم شده‌اند و دایرکتوری فعال، خدمات دایرکتوری شبکه ویندوز است که ساختار سلسله مراتبی (hierarchical) برای پیاده‌سازی و مدیریت ناحیه به وجود می‌آورد. دیرکتوری فعال فضای نام

(name space) دارد که کاربران کاتالوگ‌ها و دامنه‌ها، گروه‌های کاربر، کامپیوترها، چاپگرها و خط‌مشی‌های امنیتی در یک پایگاه داده در آن قرار می‌گیرند. هر آیتم، مانند یک کاربر یا گروه را *شیء دایرکتوری فعال* می‌نامند.

ساختار سلسله مراتبی و درخت مانند دایرکتوری فعال باعث می‌شود اشتراک‌گذاری منابع در ساختار ناحیه آسان‌تر شود. همچنین اضافه کردن ناحیه جدید به درخت کار ساده‌ای است که مقیاس دایرکتوری فعال را انعطاف‌پذیر می‌کند.

نصب دایرکتوری فعال و ایجاد ناحیه ریشه

پس از باز شدن پنجره Configure your Server Wizard روی Next کلیک کنید تا از پنجره معرفی عبور کنید. در پنجره بعدی به شما یادآور می‌شود که از اتصال مودم‌ها، کارت‌های

شبکه و دیگر وسایل به سرور اطمینان حاصل کنید. پس از کسب اطمینان از اتصال آنها به سرور روی Next کلیک کنید.

ویزارد تنظیمات اتصال محلی را شناسایی می‌کند و صفحه Configuration Options را باز می‌کند. در این صفحه با دو گزینه روبرو هستید:

* **پیکربندی معمولی برای سرور ابتدایی**: با استفاده از این گزینه می‌توانید سرور را به صورت کنترل‌کننده ناحیه پیکربندی کنید. نصب شامل دایرکتوری فعال، DNS و DHCP خواهد بود. استفاده از این گزینه در مواردی که سرور ابتدایی را دارد ناحیه می‌کنید مفید خواهد بود.

* **پیکربندی سفارشی (Custom Configuration)** : با استفاده از این گزینه می‌توانید نقش‌های مختلف سرور مانند دایرکتوری فعال، سرور فعال و سرور WINS را انتخاب کنید. استفاده از این گزینه در مواردی مفید است که قصد دارید نقش‌های سرور را افزایش یا کاهش دهید.

فرض کنیم قصد دارید کنترل‌کننده ناحیه ابتدایی را روی ناحیه وارد کنید. گزینه اول (پیکربندی معمولی مبرای سرور ابتدایی) را انتخاب کنید و روی Next کلیک کنید.

همان طوری که در شکل بعد ملاحظه می‌کنید در این صفحه نام کامل DNS ناحیه را وارد می‌کنید (قواعد نامگذاری DNS را در فصل پنجم بررسی می‌کنیم). اگر درخت دایرکتوری فعال

آینه درخت DNS است، نام ناحیه را که (در حکم درخت شبکه ویندوز است) وارد کنید. مثلا در مثال قبل نام Spinach.Com را وارد کنید.

اگر درخت دایرکتوری فعال آینه درخت DNS نمی‌باشد و شبکه از ناحیه Internet / DNS مجزاست از Local پسوند استفاده کنید و به جای پسوند نامی قرار دهید. پس از وارد کردن نام ناحیه روی Next کلیک کنید.

در صفحه بعد نام ناحیه DNS که انتخاب کرده‌اید به همراه نسخه‌های NetBIOS نام نمایش داده می‌شود. شما می‌توانید نام NetBIOS را تغییر دهید یا از نام پیش‌فرض (نام NDS اختصاری) تبعیت کنید. جهت ادامه نصب روی Next کلیک کنید.

از آنجا که سرور را به صورت کنترل‌کننده ناحیه ابتدایی پیکربندی می‌کنید در صفحه بعد از شما سوال می‌شود که سرور DNS را طوری پیکربندی کنید که درخواست‌های DNS که قابل پاسخ‌دهی نمی‌باشند را به محل دیگری ارجاع دهد (Forwarding).

برای فعال سازی ارجاع جستجوی DNS (DNS query forwarding) آدرس IP و سرور DNS دیگری از شبکه را وارد کنید.

اگر قصد ندارید این درخواست‌ها را ارجاع کنید گزینه No را انتخاب کنید. پس از انتخاب گزینه مورد نظر روی Next کلیک کنید.

پنجره خلاصه ظاهر می‌شود که در آن فهرست اجزاء سرور که نصب می‌شوند قرار داده شده است. این فهرست DHCP ، DNS و دایرکتوری فعال را شامل می‌شود. روی Next کلیک کنید تا آخرین قدم در نصب دایرکتوری فعال را بردارید.

دایرکتوری فعال و اجزای سرور نصب می‌شوند و در حل فرایند نصب کامپیوتر مجدداً راه‌اندازی (reboot) می‌شود. پس از ورود به سیستم خلاصه‌ای از اجزای نصب شده را ملاحظه می‌کنید.

برای اتمام فرایند نصب دایرکتوری فعال و اجزای سرور روی Next و سپس Finish کلیک کنید.

افزودن ناحیه فرزند

پس از ایجاد ناحیه ریشه می‌توانید تعدادی ناحیه فرزند به درخت ناحیه اضافه کنید. برای انجام این کار از Configure your server wizard استفاده کنید. مراحل ایجاد ناحیه فرزند همانند مراحل ایجاد ناحیه ریشه است:

۱- Configure your server wizard را باز کنید. پس از عبور از صفحات معرفی و یادآوری‌کننده اتصال و قطعات به سرور روی Next کلیک کنید. پس از شناسایی اتصالات شبکه صفحه Server Role باز می‌شود.

۲- روی صفحه Server Role گزینه کنترل ناحیه (Domain Controller) را انتخاب و روی Next کلیک کنید. در صفحه بعد نوع کنترل‌کننده ناحیه را انتخاب کنید. قصد ایجاد

کنترل‌کننده در ناحیه جدیدی دارید یا کنترل‌کننده ناحیه را در ناحیه‌ای موجود قرار می‌دهید.

۳- برای ایجاد ناحیه فرزند گزینه Domain Controller for a New Domain را انتخاب و روی Next کلیک کنید.

۴- پنجره بعدی دارای سه گزینه است که نوع جدید را مشخص می‌کنند:

* **ناحیه در جنگل جدید** : این گزینه جنگل جدیدی احداث می‌کند و کنترل‌کننده ناحیه جدید به عنوان ریشه اولین درخت جنگل عمل می‌کند.

* **ناحیه فرزند در درخت ناحیه موجود** : این گزینه ناحیه فرزند را درختی که از قبل وجود داشته است قرار می‌دهد (این همان گزینه‌ای است که برای ایجاد ناحیه فرزند از آن استفاده می‌کنیم).

* **درخت ناحیه در جنگل موجود** : این گزینه ناحیه‌ای را در جنگل موجود ایجاد می‌کند.

۵- گزینه Child Domain in an Existing Domain Tree را انتخاب و روی Next کلیک کنید.

۶- در این صفحه نام کاربر و رمز عبور مربط به شناسه‌ای که حق سرپرستی نصب دایرکتوری فعال را دارد وارد کنید. معمولا نام شناسه سرپرست و رمز عبور آن به صورت پیش‌فرض ارائه می‌شود.

۷- روی Next کلیک کنید. در این صفحه نام فرزند را وارد کنید و روی Next کلیک کنید.

۸- در این صفحه نام NetBIOS مربوط به ناحیه فرزند جدید ظاهر می‌شود. در اغلب موارد نیازی به تغییر نام پیش‌فرض NetBIOS نیست مگر آن که مطمئن باشید این نام با نام کامپیوتر دیگری که روی شبکه قرار دارد تداخل دارد. روی Next کلیک کنید.

۹- در این صفحه به شما اعلام می‌گردد که پایگاه داده دایرکتوری فعال پوشه log روی کنترل‌کننده ناحیه ایجاد می‌شود. از نام‌های فایل پیش‌فرض استفاده کرده و روی Next کلیک کنید.

۱۰- در این صفحه محلی برای ذخیره‌سازی پوشه SYSVOL درخواست می‌شود. این پوشه حاوی اطلاعاتی است که میان کنترل‌کننده‌های ناحیه در فضای نام رونوشت‌برداری می‌شود. بهتر است محل پیش‌فرض را انتخاب و روی Next کلیک کنید.

۱۱- در این صفحه شناسایی خدمات DNS بر روی شبکه اعلام می‌شود. همان طور که می‌دانید وجود DNS روی شبکه برای نصب دایرکتوری فعال الزامی است. فرایند را کلیک روی Next ادامه دهید.

۱۲- در این صفحه سطوح مجوز مورد استفاده در ناحیه را انتخاب می‌کنید. اگر از ویندوز سرور ۲۰۰۳ یا ویندوز ۲۰۰۰ سرور استفاده می‌کنید گزینه دوم را انتخاب کنید. این گزینه دارای امنیت بیشتری است. اگر از ویندوز سرور NT ۲۰۰۳ سرور استفاده می‌کنید گزینه اول را انتخاب کنید. پس از انتخاب، روی Next کلیک کنید.

۱۳- در این صفحه رمز عبور حالت بازیابی را وارد می‌کنید. از این رمز عبور هنگامی استفاده می‌شود که سرور در حالت بازیابی خدمات دایرکتوری عمل کند. پس از وارد کردن رمز عبور (ضرورتی ندارد این رمز عبور همان رمز عبور سرپرستی باشد) روی Next کلیک کنید.

۱۴- در صفحه خلاصه، فهرست گزینه‌های انتخاب شده برای کنترل‌کننده ناحیه جدید را مشاهده می‌کنید. روی Next کلیک کنید تا پیکربندی دایرکتوری فعال برای کنترل‌کننده ناحیه جدید انجام شود.

۱۵- هنگامی که پنجره نهایی باز شد روی Finish کلیک کنید و سپس گزینه Restart Now را انتخاب کنید تا سرور مجدداً راه‌اندازی شود.

پس از راه‌اندازی مجدد سرور، اعلام می‌شود سرور به کنترل‌کننده ناحیه تبدیل شده است. روی Finish کلیک کنید.

ابزار مدیریت دایرکتوری فعال

پس از نصب دایرکتوری فعال روی کنترل‌کننده ناحیه می‌توانید از ابزار آن استفاده کنید. این ابزار کاربران و کامپیوتر را به ناحیه اضافه می‌کنند، توافق‌های مختلف موجود در ناحیه را مدیریت می‌کنند و با سایت‌های وسیع شبکه در تعاملند.

ابزار مدیریت دایرکتوری فعال در نماهای فوری کنسول مدیریت میکروسافت دیده می‌شوند. در ادامه این فصل نگاهی گذرا به این ابزار می‌اندازیم.

کامپیوترها و کاربران دایرکتوری فعال

نمای فوری Active Directory Users and Computers مدیریت کامپیوترها، کاربران، گروه‌ها و واحدهای سازمانی را بر عهده دارد. از این نمای فوری به دفعات استفاده خواهید کرد. تمام اشیاء دایرکتوری فعال را مدیریت می‌کند.

توافق‌ها و ناحیه‌های دایرکتوری فعال

نمای فوری Active Directory Domains and Trusts مدیریت توافق‌های (Trusts) میان ناحیه‌ها را بر عهده دارد. توافق‌های انتقالی میان دامنه‌های یک درخت برقرار می‌شود و از نمای فوری شکل ۸-۹ اغلب برای مدیریت توافق‌های میان جنگل‌های ناحیه مختلف استفاده می‌شود.

نمای فوری توافق‌ها و ناحیه‌های دایرکتوری فعال از جنبه دیگری هم حائز اهمیت است. این نمای فوری اجازه می‌دهد سطح عملکرد ناحیه را افزایش دهید. سطح عملکرد ناحیه، نوع کنترل‌کننده ناحیه که توسط ناحیه شما پشتیبانی می‌شود را تعیین می‌کند. سطح عملکرد ناحیه به صورت پیش‌فرض Windows 2000 Mixed انتخاب شده است که کنترل‌کننده‌های ناحیه ویندوز NT ۴ ، ویندوز ۲۰۰۰ و ویندوز سرور ۲۰۰۳ را پشتیبانی می‌کند.

سایت‌ها و خدمات دایرکتوری فعال

نمای فوری Active Directory Sites and Service ساختار فیزیکی و مختلفی ویندوز سرور ۲۰۰۳ را مدیریت می‌کند. سایت محلی فیزیکی است که می‌تواند زیر شبکه‌ها یا مجموعه‌ای از آنها را

در خود جای می‌دهد. با این نمای فوری می‌توانید سایت‌های چندگانه‌ای ایجاد کنید که محل‌های فیزیکی مختلفی را شامل شوند. این محل‌های فیزیکی توسط اتصالات WAN با هم ارتباط دارند. با ایجاد سایت‌ها می‌توانید میزان رونوشت‌برداری میان اجزای شبکه‌های با اتصالات WAN و LAN داخل را کنترل کنید.

افزودن کاربر به ناحیه

شناسه‌های کاربر توسط نمای فوری Active Directory users and Computers به ناحیه اضافه می‌شوند. جهت افزودن کاربر به ناحیه از مراحل زیر استفاده کنید:

۱- نمای فوری Active Directory Users and Computers را باز کنید.

۲- در درخت نمای فوری گره ناحیه را باز کنید و پوشه user را انتخاب کنید. در صفحه جزییات فهرستی از کاربران و گروه‌های پیش‌فرض را مشاهده می‌کنید.

۳- برای ایجاد کار جدید، روی نوار ابزار دایرکتوری فعال دکمه Current Container و گزینه Create a New User را انتخاب کنید. جعبه محاوره‌ای New Object – User باز می‌شود.

۴- نام و نام‌خانوادگی کاربر را وارد کنید. این نام در دایرکتوری فعال ظاهر خواهد شد.

۵- در جعبه User Login Name ، نام کاربر برای ورود به ناحیه را وارد کنید.

۶- پس از وارد کردن اطلاعات درخواستی روی Next کلیک کنید.

۷- در این صفحه، رمز عبور کاربر درخواست می‌شود. پس از وارد کردن رمز و تأیید آن می‌توانید خصوصیات رمز عبور را تعیین کنید. شما با چهار گزینه روبرو هستید:

* **کاربر در ورود به شبکه بعدی باید رمز عبور را تغییر دهد** : اگر می‌خواهید کاربران روی رمز عبور خود کنترل داشته باشند این گزینه را انتخاب کنید.

* **کاربر نمی‌تواند رمز عبور را تغییر دهد** : اگر قصد دارید کاربران را محدود کرده و حق انتخاب رمز عبور را از آنها سلب کنید، این گزینه را انتخاب کنید.

* **رمز عبور محدودیت زمانی ندارد** : با انتخاب این گزینه تا زمانی که ناحیه وجود دارد رمز عبورتان قابل استفاده است.

* **شناسه غیر فعال است** : با انتخاب این گزینه شناسه را غیرفعال می کنید بدون این که آن را حذف کنید.

۸- پس از تنظیم خصوصیات رمز عبور روی Next کلیک کرده، پنجره خلاصه را مشاهده و Finish را انتخاب کنید. شناسه کاربر جدید در صفحه جزییات نمای فوری ظاهر می‌شود.

تنظیمات زمان ورود به شبکه و کامپیوترهای شبکه

کادر Account زمان ورود به شبکه و کامپیوترهایی که کاربر می‌تواند وارد آنها شود را تنظیم می کند. برای تنظیم زمان ورود کاربر به شبکه از مراحل زیر استفاده کنید:

۱- در صفحه جزییات از نمای فوری Active Directory users computers روی شناسه کاربر کلیک راست کرده و از منوی ظاهر شده گزینه Properties را انتخاب کنید. سپس کادر Account را انتخاب کنید.

۲- در کادر Account دکمه Logon Hours را انتخاب کنید تا جعبه محاوره‌ای آن باز شود.

۳- به صورت پیش‌فرض همه ساعت‌ها انتخاب شده‌اند (رنگ آبی دارند). برای این که کاربر نتواند در روز شنبه وارد شبکه شود با کلیک کردن و کیدن (Click-Drag) محدود زمانی روز شنبه را انتخاب کرده و روی دکمه Logon Demed کلیک کنید. چارچوب زمانی انتخاب شده سفید می‌شود و کاربر در این چارچوب زمانی حق ورود به شبکه را ندارد. پس از تعیین ساعات مجاز و غیرمجاز برای ورود به شبکه روی Ok کلیک کنید.

۴- برای تعیین کامپیوترهایی که کاربر حق ورود به آنها را دارد در کارد Tab روی دکمه Log on To کلیک کنید. جعبه محاوره‌ای Logon Workstations باز می‌شود.

۵- گزینه The following Computers را انتخاب کنید. برای وارد کردن یک کامپیوتر در فهرست، نام NetBIOS آن را در جعبه Computer name وارد کنید (نام NetBIOS ، ۱۵ کاراکتر اول نام کامپیوتر است و پسوند نام ناحیه را شامل نمی‌شود).

۶- پس از وارد کردن نام کامپیوتر روی دکمه Add کلیک کنید. نام هر تعداد کامپیوتر که کاربر حق ورود به آنها را دارد وارد کنید و روی Ok کلیک کنید.

تغییر نام کاربر

برای تغییر شناسه کاربر ناحیه از صفحه جزییات Active Directory users and Computers استفاده کنید. روی نام کاربر کلیک راست کرده و گزینه Rename را انتخاب کنید. پس از ویرایش نام کاربر روی نقطه‌ای دلخواه از پنجره دایرکتوری کلیک کنید. جعبه محاوره‌ای Rename User ظاهر می‌شود و تغییرات اعمال شده در نام کاربر را نشان می‌دهد.

توجه داشته باشید که با تغییر نام کاربر، عضویت کاربر در گروه‌ها و مجوزهای وی تغییر نمی‌کنند. در صورت لزوم تغییرات دیگری در جعبه محاوره‌ای Rename User اعمال کنید و روی Ok کلیک کنید تا نام جدید در دایرکتوری فعال نمایان شود.

فصل پنجم : خدمات نام ناحیه *(DNS)*

مروری بر سرورهای DNS

خدمات نام ناحیه (DNS) یک ساختار سلسله مراتبی (هرمی شکل) پدید می‌آورد که توسط آن نام‌های کامل ناحیه (FQDN)، نام‌های میزبان و نام‌های دیگری را به آدرس‌های IP نسبت می‌دهد. نامگذاری در DNS ممکن است به صورت نام‌های آشنا و روزمره یا آدرس‌های منطقی (آدرس‌های IP) باشد. مثلا هنگامی که در پنجره آدرس مرورگر وب عبارت Microsoft.com را تایپ کنید، یکی از سرورهای DNS که روی شبکه اینترنت قرار دارد یک نام FQDN (نام Microsoft.com) را به آدرس IP سایت Microsoft web نسبت می‌دهد.

بنابراین در شبکه‌های TCP/IP ، به طور خاص شبکه اینترنت، هر سازمان و موسسه‌ای از سرورهای DNS برخوردار است که FQDN را به آدرس‌های IP نسبت می‌دهد. در واقع هر سازمان، موسسه یا شرکت دارای وظایف نامگذاری قسمت‌های مختلف اینترنت است. در واقع هنگامی که یک شرکت نام ناحیه‌ای را در Inter NIC ثبت می‌کند، باید آدرس‌های IP دو سرور DNS که وظایف نامگذاری را بر عهده دارند را به Inter NIC ارائه کند. کاربران می‌توانند پیاده‌سازی DNS را خودشان بکار گیرند یا آن را بر عهده ISPهایی بگذارند که این خدمات را ارائه می‌دهند.

سرورهایی که توسط Inter NIC اداره می‌شوند به یکی از سرورهای DNS محلی اجازه می‌دهند تا FQDN را به آدرس IP اختصاص دهد. سرورهای Inter NIC پایگاه داده‌ای دارند که در

آن فهرست همه سرورهای DNS ناحیه و آدرس‌های IP آنها قرار دارد. بنابراین سرور DNS محلی درون سرور Inter NIC به جستجو پرداخته و آدرس IP مربوط به سرور DNS که به ناحیه خاصی خدمات ارائه می‌کند را پیدا می‌کنند. هنگامی که سرور محلی آدرس‌های IP مربوط به یک سرور DNS راه دور را دریافت می‌کند سرور محلی می‌تواند به صورت مستقیم به جستجو پرداخته و FQDN راه دور را به یک آدرس IP نسبت دهد.

ویندوز سرور ۲۰۰۳ از استاندارد سرور DNS پویا (DDNS) استفاده می‌کند که کارهای سرپرستی مربوط به نگهداری پایگاه داده DNS را به شدت کاهش داده است (در مقایسه با سرورهای DNS). سرور و مشتری‌های DNS پایگاه داده DDNS را به صورت پویا می‌سازند.

فضای نام DNS

برای درک نحوه تعیین DNS یا FQDN باید با فضای نام ناحیه آشنا شوید. فضای نام ناحیه (Domain namespace) طرحی است که برای نامگذاری ناحیه‌ها به کار می‌رود. این ناحیه‌ها در سطوح مختلف درخت سلسله مراتبی ناحیه DNS قرار دارند. فضای نام ناحیه، همچنین، نام‌های کامپیوتر منفرد و دیگر وسایل موجود روی شبکه را در بر می‌گیرد.

ابتدا باید رابطه بین ناحیه و DNS را مشخص کنیم. هر بخش روی DNS به عنوان یک درخت در نظر گرفته می‌شود.

پایه درخت DNS را ریشه ناحیه تشکیل می‌دهد. ناحیه ریشه اینترنت با نقطه (.) نمایش داده می‌شوند. پایین ناحیه ریشه، ناحیه‌های سطح بالا قرار دارند. ناحیه‌های سطح بالا شامل پسوندهایی مانند com و edu است. فهرست نام‌های ناحیه سطح بالا عبارتست از:

* Com : توسط موسسات بازرگانی استفاده می‌شود. مثلا Samspublishing.com نام ناحیه انتشارات SAMS است.
* edu : توسط موسسات آموزشی استفاده می‌شود. مثلا une.edu نام ناحیه دانشگاه England New است.
* org : توسط موسسات غیر بازرگانی استفاده می‌شود. مثلا Sanjesh.org نام ناحیه سازمان سنجش است.
* gov : توسط سازمان‌های دولتی ایالات متحده استفاده می‌شوند. Senate.gov نام ناحیه سنایی آمریکاست.
* net : توسط شرکت‌های اینترنتی مانند ISP ها استفاده می‌شوند.
* Country names : مثلا ir برای ایران و us برای آمریکا.
* biz : یک ناحیه سطح بالای جدید است که برای موسسات تجاری به کار می‌رود.
* info : ناحیه سطح بالای جدیدی دیگری که برای سایت‌های وب خبری به کار می‌رود.

پایین ناحیه‌های سطح بالا، ناحیه سطح سوم قرار دارد. ناحیه‌های ثانویه شرکت‌ها و موسساتی را شامل می‌شوند که برای دسترسی به سایت وب نام آنها را وارد می‌کنیم مانند SAMS و Une . پایین

ناحیه‌های سطح دوم زیر ناحیه‌ها قرار دارند. زیرا ناحیه‌ها یک ناحیه ثانویه بزرگتر را به واحدهای جغرافیایی یا کاری تقسیم می‌کنند. مثلا اگر نام ناحیه ثانویه شرکت شما Habraken.com باشد و شرکت دارای دو بخش فروش (Salc 5) و مشاهده (Consulting) باشد دو زیرناحیه . Consulting Habraken . com و Sales . Habraken . com را می‌توان ایجاد کرد.

ناحیه‌های سطح دوم و زیر دامنه‌ها، میزبان‌ها را هم در بر می‌گیرند. میزبان‌ها کامپیوترها یا وسایل دیگری هستند که درون فضای نام زیر ناحیه یا ناحیه سطح سوم قرار دارند. مثلا اگر کامپیوتری با نام joe1 داشته باشید که در بخش فروش شرکت قرار دارد، نام آن به صورت . joe1 sales . Harbaken . com خواهد بود.

نحوه کار DNS

حالا که با سلسله مراتب نامگذاری DNS آشنا شده‌اید، روی این موضوع متمرکز می‌شویم که DNS چگونه FQDNها را به آدرس‌های IP (و بر عکس آن) نسبت می‌دهد. خدمات DNS دارای دو بخش است: سرور و اختصاص‌دهنده (resolver). اختصاص‌دهنده نرم‌افزاری است که درون Winsock قرار دارد (مانند یک مرورگر وب) هنگامی که FQDN یک میزبان به آدرس IP نیاز دارد، اختصاص‌دهنده در سرور به جستجو می‌پردازد. جزء DNS سرور توسط سرور DNS اداره می‌شود.

هنگامی که یک کامپیوتر مشتری بخواهد یک FQDN را به آدرس IP اختصاص دهد، اختصاص‌دهنده یک کاشه محلی (local Cache) را چک می‌کند تا ببیند که آیا اطلاعات اختصاص

داده FQDN به آدرس IP در این کاشه وجود دارد یا نه. اگر اطلاعات در کاشه موجود باشد فرایند خاتمه می‌یابد و کامپیوتر مشتری FQDN را به آدرس IP اختصاص می‌دهد.

اگر اطلاعات در کاشه وجود نداشته باشد، نرم‌افزار اختصاص دهنده آدرس IP سرور DNS ملحی را از تنظیمات TCP/IP کامپیوتر مشتری به دست می‌آورد. یک سرور DNS خاص توسط سرور DHCP یا به صورت ایستا، سرورها و مشتری‌های ویندوز را پیکربندی می‌کند. مفهوم سرور DHCP در فصل ششم بررسی خواهد شد. در شکل بعد خصوصیات TCP/IP مربوط به یک سرور عضو دارای ویندوز سرور ۲۰۰۳ نشان داده است. این سرور به عنوان سرور DNS خاص در نظر گرفته شده است.

مشتری درخواستی را برای DNS خاص می‌فرستد. فرض کنید FQDN ای که باید اختصاص داده شود مربوط به یک کامپیوتر میزبان باشد که در ناحیه DNS محلی قرار گرفته است. در این صورت سرور DNS در پایگاه داده به دنبال این نام می‌گردد و آدرس IP مناسب را به کامپیوتر درخواست‌دهنده برمی‌گرداند. اما اگر نام به کامپیوتری که روی ناحیه محلی قرار ندارد مربوط باشد دو حالت ممکن است اتفاق بیفتد : اگر اطلاعات در کاشه سرور DNS موجود باشد، سرور DNS آن را به مشتری درخواست‌دهنده ارائه می‌کند. اما اگر اطلاعات در کاشه سرور DNS وجود نداشته باشد، سرور DNS به سرور ریشه تماس می‌گیرد تا ناحیه سطح بالای نام میزبان را دریافت کند. سرور ریشه از طریق نام میزبان آدرس IP سرور DNS مجاز ناحیه را بدست می‌آورد. هنگامی که سرور DNS آدرس IP دورمین سرور DNS ناحیه را در اختیار گرفت، در سرور دوم جستجو می‌کند تا

اطلاعات لازم برای اختصاص آدرس IP به FQDN را پیدا کند. در نهایت سرور DNS محلی این اطلاعات را به میزبان درخواست‌کننده می‌فرستد.

نصب خدمات نام ناحیه

ویندوز سرور ۲۰۰۳ نسخه پیاده‌سازی جدیدی از DNS را ارائه داده است که به کاربران اجازه می‌دهد منابع خود را پایگاه داده DNS را به صورت خودکار به روز (update) کنند. DDNS با دایرکتوری فعال یکپارچه می‌شود. بدین معنا که پایگاه داده DNS در تمامی کنترل‌کننده‌های ناحیه (موجود در ناحیه) رونوشت‌برداری (replicate) می‌شود. همچنین DDNS با DHCP در تعامل است. سرور DNS به همراه DHCP نگاشت‌های نام میزبان به آدرس‌های IP را هماهنگ‌سازی می کند.

برای نصب DNS روی ویندوز سرور ۲۰۰۳ روش‌های مختلفی وجود دارد:

۱- در هنگام نصب ویندوز سرور ۲۰۰۳ با انتخاب گزینه‌های مربوط به additional Network Services می‌توانید DNS را نصب کنید.

۲- اگر روی کنترل ناحیه‌تان دایرکتوری فعال را نصب کنید و هیچ سرور DNS ای روی شبکه وجود نداشته باشد DNS و DHCP در هنگام نصب دایرکتوری فعال نصب خواهد شد.

۳- می‌توانید DNS را از طریق Configure your server wizard اضافه کنید.

پیکربندی سرور DNS

در صفحه بعد با ویزارد DNS با قابلیت‌های پیکربندی سرور DNS روبرو می‌شود. این قابلیت‌ها عبارتند از:

* Create a forward lookup zone : با استفاده از این گزینه می‌توانید یک منطقه جستجوی مستقیم ایجاد کنید. در بخش بعدی کتاب با منطقه جستجوی مستقیم آشنا می‌شوید. استفاده از این گزینه برای شبکه‌های کوچک‌تر توصیه می‌شود.
* Create forward and reverse lookup zones : با استفاده از این گزینه می‌توانید مناطق جستجوی مستقیم و معکوس ایجاد کنید. استفاده از گزینه برای شبکه‌های بزرگ توصیه می‌شود.
* Configure root hists only : استفاده از این گزینه برای کاربران حرفه‌ای توصیه می‌شود و سرور را طوری پیکربندی می‌کند که درخواست‌ها را به درخت DNS ارجاع دهد.

هدف ما ارائه توضیحات بیشتر درباره منطقه جستجوی مستقیم و معکوس است. بنابراین گزینه دوم را انتخاب کنید و روی Next کلیک کنید.

ایجاد منطقه جستجوی مستقیم

در صفحه بعد با گزینه‌های ایجاد منطقه جستجوی مستقیم مواجه هستید. منطقه جستجوی مستقیم (forward lookup zone) به میزبان اجازه می‌دهد تا با استفاده از نام میزبان یک وسیله یا کامپیوتر خاص به جستجوی آدرس IP بپردازد. میزبان آدرسی را به این علت پیدا می‌کند که DNS

به درخواست کامپیوتر میزبان پاسخ می‌دهد. برای این که DNS بتواند کار کند باید حداقل یک منطقه جستجوی مستقیم داشته باشد.

گزینه پیش‌فرض یعنی ایجاد منطقه جستجوی مستقیم را انتخاب کرده و روی Next کلیک کنید.

در صفحه بعد با سه نوع منطقه جستجوی مستقیم روبرو می‌شوید:

* Primary zone : منطقه اولی کپی اصلی پایگاه داده DNS است. منطقه اولیه روی سروری که در آن ایجاد شده است سرپرستی می‌شود. بنابراین آن سرور به عنوان سرور DNS مجاز برای منطقه شناخته می‌شود.
* Secondary zone : منطقه ثانویه از یک فایل پایگاه داده استفاده می‌کند. این فایل، یک همسان فقط خواندی از منطقه موجود است. سرور DNS که توسط منطقه ثانویه استاندارد پیکربندی شده است به سرور DNS اولیه کمک می‌کند که تخصیص نام در شبکه را انجام دهد.
* Stub zone : این گزینه تنها ثبت‌هایی (record) را در بر می‌گیرد که برای تعیین سرور DNS مجاز مربوط به یک منطقه خاص به آنها احتیاج دارد. با انتخاب این گزینه تنها به سرورهایی که منطقه اولیه را اداره می‌کنند در کانون توجه قرار می‌گیرند.

چون این سرور DNS شبکه را نصب می‌کند گزینه Primary zone را انتخاب کنید تا با بقیه صفحات ویزارد آشنا شوید. سپس روی Next کلیک کنید.

رونوشت‌برداری منطقه

در صفحه بعد گزینه‌های مربوط به رونوشت‌برداری منطقه را مشاهده می‌کنید. رونوشت‌برداری پایگاه داده DNS و ثبت‌های منطقی باعث می‌شود سرورهای DNS از ثبت‌های DNS اشتراک استفاده کنند. این بدان معناست که هر یک از سرورهای DNS روی شبکه می‌توانند به درخواست یک میزبان برای اختصاص آدرس IP به نام میزبان پاسخ مناسب و یکسان دهند.

نحوه رونوشت‌برداری پایگاه داده DNS در گزینه‌های موجود در این صفحه ویزارد تعیین می‌شود:

* To all DNS Servers in the Active Directory forest : با استفاده از این گزینه همه سرورهای DNS موجود در جنگل پایگاه‌های داده خود را رونوشت‌برداری کرده و به اشتراک می‌گذارند.
* To all DNS Servers in the Active Directory Domain : با استفاده از این گزینه همه سرورهای DNS ناحیه منطقه و ثبت‌هایشان را از طریق رونوشت‌برداری به اشتراک می‌گذارند.
* To all domain Controllers in the Active Directory Domain : از این گزینه هنگام استفاده می‌شود که DNS را روی کنترل‌کننده‌های ناحیه اجرا می‌کنید. پایگاه داده DNS به عنوان بخشی از دایرکتوری فعال ذخیره می‌شود و میان سرورهای DNS و کنترل‌کننده‌های

ناحیه به اشتراک گذاشته می‌شود. این گزینه به صورت پیش‌فرض انتخاب شده و بهترین زمینه در بکارگیری DNS است.

گزینهٔ مورد نظرتان را انتخاب کرده و روی Next کلیک کنید.

نام منطقه و به روز کردن پویا (Dynamic Update)

در صفحه بعد نام منطقه جستجوی مستقیم جدید را وارد می‌کنید. نام منطقه بر اساس نام ناحیه DNS تعیین می‌شود. مثلا اگر ناحیه DNS شبکه Spincah.com نام دارد نام منطقه هم Spinach.com است.

نام منطقه را بر اساس نام ناحیه DNS وارد کرده و روی Next کلیک کنید.

در صفحه بعد گزینه‌هایی برای به روز کردن پویا (Dynamic Update) کامپیوترهای میزبان در نظر گرفته شده است. گزینه پیش‌فرض به روز رسانی بی‌خطری است و امنیت بالایی دارد. گزینه دوم امنیت پایینی دارد و گزینه سوم به روز رسانی پویا را غیر فعال می‌کند.

در به روز رسانی رکوردهای کامپیوتر میزبان DNS سرور قرار می‌گیرند و به روز می‌شوند. گزینه اول را انتخاب کرده و روی Next کلیک کنید. توجه داشته باشید که گزینه اول امنیت بالایی دارد اما سرورهای DNS باید دارای دایرکتوری فعال باشند.

ایجاد یک منطقه جستجوی معکوس

در صفحه بعد از شما سوال می‌شود که آیا می‌خواهید منطقه جستجوی معکوس ایجاد کنید یا نه. منطقه جستجوی معکوس اجازه می‌دهد که آدرس‌های IP را به نام میزبان (hostnames)

اختصاص دهید. اگر سرور DNS را با منطقه جستجوی معکوس پیکربندی نکنید عملکرد سرور DNS دچار اختلال نمی‌شود، اما منطقه جستجوی معکوس فواید خاص خود را دارد و بهتر است سرور DNS را با آن پیکربندی کنید. مثلا اگر بخواهید Internet Information را طوری فعال کنید که هم‌نام‌های میزبان و هم‌آدرس‌های IP را در فایل گزارش ثبت کند، باید سرور DNS را به منطقه جستجوی معکوس پیکربندی کنید.

گزینه پیش‌فرض (Create a reverse lookup Zone) را انتخاب و روی Next کلیک کنید. در صفحه بعد منطقه را تعیین کنید. بهتر است گزینه Primary را انتخاب کرده و روی Next کلیک کنید.

در صفحه بعد نوع رونوشت‌برداری منطقه جستجوی معکوس جدید را مشخص کنید. گزینه‌های این صفحه همانند گزینه‌هایی هستند که در ایجاد منطقه جستجوی مستقیم آنها را مشاهده کردید. گزینه آخر (پیش‌فرض) بهترین گزینه است. این گزینه را انتخاب کرده و روی Next کلیک کنید.

نامگذاری منطقه جستجوی معکوس

در صفحه بعد، ID شبکه را وارد کنید. از این ID برای ایجاد نام منطقه جستجوی معکوس استفاده می‌شود. ID شبکه بخشی از آدرس IP است که به آدرس میزبان اشاره نمی‌کند. مثلا در آدرس IP کلاس C 1 . 5 . 168 . 192 فقط اوکتت چهارم شامل اطلاعات آدرس میزبان است

(ماسک زیرشبکه کلاس C ، 0 . 255 . 255 . 255 است). بنابراین ID شبکه برابر 5 . 168 . 192 است.

ID شبکه را وارد کرده و روی Next کلیک کنید.

در صفحه بعد نوع به روز رسانی پویا را تعیین کنید. در مورد این صفحه در ایجاد منطقه جستجوی مستقیم صحبت کردیم. گزینه پیش‌فرض بهترین گزینه است، آن را انتخاب کرده و روی Next کلیک نمایید. در صفحه بعدی ویزارد می‌توانید یک ارجاع‌دهنده (forwarder) انتخاب کنید. ارجاع‌دهنده‌ها سرورهای DNS ای هستند که از آنها برای پاسخ دادن به درخواست‌های DNS فعلی استفاده می‌شود. در واقع اگر DNS فعلی نتواند پاسخ درخواست‌های موجود را بدهد آنها را به سرورهای DNS دیگر (ارجاع‌دهنده‌ها) ارجاع می کند.

مدیریت DNS

DNS توسط نمای فوری DNSMGMT مدیریت می‌شود. برای باز کردن این نمای فوری Start / Administrative Tools / DNS را انتخاب کنید. نمای فوری باز می‌شود.

توسط نمای فوری DNSMGMT می‌توانید رکوردهای موجود در مناطق DNS را مشاهده کرده و مناطق را به سرور DNS اضافه کنید. از آنجا که رکوردها به صورت پویا ایجاد می‌شوند، در نمای فوری با باز کردن یک منطقه می‌توانید رکوردهای مربوط به آن را مشاهده کنید.

مثلا برای مشاهده رکوردهای منابع در منطقه جستجوی مستقیم گروه Forward Lookup Zone را باز کرده و یکی از مناطق جستجوی مستقیم را انتخاب کنید. رکوردهای موجود در منطقه در صفحه نمای فوری ظاهر می‌شوند.

در محیط DNS رکوردهای منبع مختلفی وجود دارند. یکی از انواع رکورد، رکورد میزبان است. رکورد میزبان در محیط DNS به صورت رکورد A طراحی شده است. رکوردهای A در مناطق جستجوی مستقیم دیده می‌شوند. در جدول بعد انواع رکوردهای منبع DNS را مشاهده می کنید.

نوع رکورد	نام در نمای فوری DNS و توصیف
SOA	Start of Autority نام سرور مجاز در ناحیه را شناسایی می کند و اولین رکورد در فایل پایگاه داده منطقه است. هنگامی که سرور نام اولیه را به شبکه متصل می کنید، این رکورد به صورت خودکار ایجاد می‌شود.
NS	Name Server ، برای هر سرور نام در ناحیه یک رکورد ایجاد می‌شود.
A	Host ، در یک منطقه جستجوی مستقیم، نام‌های میزبان را به آدرس‌های IP نگاشت می کند.
TR	Pointer ، عملکرد این نوع رکورد بر عکس در رکورد A است. این رکورد در منطقه جستجوی معکوس وجود دارد و آدرس‌های IP را به نام‌های میزبان نگاشت می کند.
SRV	Service ، خدماتی که روی یک کامپیوتر خاص وجود دارد را نشان می‌دهد، مثلا رکوردهای SRV می‌توانند کنترل‌کننده ناحیه را شناسایی کنند.
MX	Mail Exchanger ، سرورهای پستی (mail) موجود روی شبکه را شناسایی کرده و ترتیب اتصال آنها را مشخص می‌نماید.
CNAME	Canonical Name of Alias ، برای هر رکورد موجود یک لقب (alias) ایجاد می کند تا بتوانید در یک آدرس IP به چندین نام مختلف اشاره کنید.
HINFO	Host information ، اطلاعات مربوط به CPU ، سیستم عامل و سخت‌افزارها و نرم‌افزارها را ارائه می کند.
WINS	WINS ، به DOS اجازه می‌دهد برای اختصاص نام میزبان از WINS استفاده کند.

برخی از انواع رکورد به صورت خودکار ایجاد می‌شوند (مانند A ، NS ، SOA) و بقیه رکوردها توسط نمای فوری DNSMGMT به وجود می‌آیند.

عیب‌یابی خدمات سرور DNS

نمای فوری DNSMGMT روشی برای بررسی و تست سرور DNS را ارائه می‌کند. دو تست مختلف به صورت درخواست وجود دارد: تست درخواست ساده و تست درخواست بازگشتی.

ساده (Simple)

تست درخواست ساده نگاشت میزبان به آدرس IP را تست می‌کند. در این تست، مشتری DNS که روی سرور DNS قرار دارد به سرور نام درخواستی می‌فرستد. در این تست قابلیت‌های سرور DNS در مدیریت جستجوهای مستقیم بررسی می‌شود.

بازگشتی (recursive)

تست درخواست بازگشتی نگاشت آدرس IP به نام میزبان را تست می‌کند. در این تست قابلیت‌های سرور DNS در مدیریت جستجوهای معکوس آزمایش می‌شود.

برای به کار گیری این تست‌ها از گام‌های زیر استفاده کنید:

۱- در نمای فوری DNSMGMT روی سرور نام DNS کلیک راست کنید و Properties را انتخاب نمایید.

۲- روی کادر Monitoring کلیک کنید. با دو جعبه چک انواع تست مواجه می‌شوید.

۳- جعبه چک مناسب را انتخاب کرده (می‌توانید هر دو جعبه چک را انتخاب کنید) و روی دکمه Test Now کلیک کنید.

همچنین می‌توانید عملیات تست را به صورت خودکار و در بازه‌های زمانی که تعیین می‌کنید انجام دهید. برای انجام تست خودکار جعبه چک سوم را انتخاب و بازه زمانی مورد نظرتان را در Test interval وارد کنید. اگر در یکی از این تست‌ها، سرور معیوب تشخیص داده شود سرور توسط علامت هشدار (مثلثی که در آن علامت عجب قرار دارد) نمایش داده می‌شود.

فصل ششم : پروتکل پیکربندی پویای میزبان *(DHCP)*

آشنایی با DHCP

پروتکل پیکربندی پویای میزبان (DHCP) به شما اجازه می‌دهد آدرس‌های IP را به صورت پویا به کامپیوترها وسایل جانبی روی شبکه اختصاص دهید. آدرس‌های IP از مخزنی از آدرس‌های تهیه شده و به کامپیوترها اختصاص داده می‌شوند. اختصاص آدرس IP به صورت دائم یا موقت خواهد بود. وقتی این مساله را در نظر بگیرید که باید به هر کامپیوتر مشتری، آدرس IP ماسک زیر شبکه و آدرس دروازه اختصاص دهید، درمی‌یابید که احتمال خطا در اختصاص آدرس‌ها بسیار بالا است.

DHCP یک محیط پویا ایجاد می‌کند که آدرس‌های IP را به کامپیوترها و وسایل جانبی موجود در شبکه اختصاص می‌دهد. با این روش با دردسرهای اختصاص آدرس IP به صورت دستی روبرو نمی‌شوید و اختصاص آدرس‌های IP به کامپیوترها با دقت بالایی انجام می‌گیرد.

سرور DHCP (ویندوز سرور ۲۰۰۳ که با خدمات DHCP پیکربندی شده است) وظیفه دارد آدرس IP ، ماسک زیرشبکه، دروازه پیش‌ساخته، آدرس سرور DNS و آدرس سرور WINS را به مشتری DHCP ارائه دهد. مشتری DHCP هر کامپیوتر یا وسیله‌ای روی شبکه است که برای کسب پویای آدرس IP پیکربندی شده است. هنگامی که یک مشتری DHCP برای اولین بار راه‌اندازی می‌شود به دنبال آدرس IP می‌گردد. مشتری یک پیغام DHCP DISCOVER را نشان می‌دهند که

قرارداد IP فرستاده شده به همه سرورهای DHCP را درخواست می‌کند. پیام نمایش داده شده نام میزبان مشتری و آدرس سخت‌افزاری MAC مشتری را ارائه می‌کند.

در مرحله بعد، یک سرور DHCP که روی زیرشبکه قرار دارد توسط پیام DHCP OFFER آدرس IP پیشنهادی به همراه ماسک زیرشبکه و قرارداد IP را ارائه می‌کند. این پیام آدرس IP سرور DHCP را نیز شامل می‌شود.

هنگامی که مشتری اولین پیام DHCP POFFER را دریافت می‌کند یک پیام DHCP REQUEST به همه سرورهای DHCP شبکه می‌فرستد و پذیرش پیشنهاد ارائه شده را اعلام می‌کند. این پیام آدرس IP سرور DHCP ای را در بر می‌گیرد که مشتری با آن موافقت نموده است. بقیه سرورهای DHCP منتظر می‌مانند تا هنگامی که مشتری دیگری درخواست آدرس IP داشت به آن درخواست پاسخ دهند.

در نهایت، سرور DHCP که با پیشنهادش موافقت شده یک پیام تدیید برای مشتری می‌فرستد. پیام DHCP PACK یک قرارداد IP معتبر و اطلاعات پیکربندی TCP/IP را شامل می‌شود. مشتری این اطلاعات را در رجیستری ویندوز ذخیره می‌کند.

نصب خدمات DHCP

برای نصب خدمات DHCP دو روش وجود دارد: استفاده از ویزارد پیکربندی سرور یا Add or Remove Programs . قبل از نصب DHCP روی سرور باید سرور را توسط آدرس IP ثابت پیکربندی کنید.

برای اضافه کردن DHCP به شبکه با استفاده از ویزارد پیکربندی سرور:

۱- Configure your server wizard را باز کنید.

۲- روی Next کلیک کنید تا از صفحه معرفی عبور کنید. در صفحه بعد، فهرستی از سخت‌افزارهای قابل اتصال به شبکه (مانند کارت‌های شبکه و مودم) را مشاهده کنید. در صفحه بعد ویزارد به دنبال اتصالات شبکه موجود روی سرور ویندوز می‌گردد.

۳- در صفحه بعد فهرست نقش‌های سرور را مشاهده می‌کنید. خدماتی که به سرور اضافه کرده‌اید با yes مشخص شده‌اند و خدماتی را که روی سرور نصب کرده‌اید با کلمه No دیده می‌شوند.

۴- در فهرست Server Role گزینه DHCP Server را انتخاب و روی Next کلیک کنید. صفحه خلاصه‌ای را مشاهده می‌کنید.

۵- روی Next کلک کنید تا خدمات DHCP به سرور اضافه شود و ویزارد میدان دید جدید به صورت خودکار باز شود. در بخش بعدی با میدان دید (Scope) آشنا می‌شوید.

پیکربندی خدمات DHCP توسط میدان دید

مرحله بعدی در پیکربندی سرور DHCP استفاده از میدان دیدی است که از آدرس‌های IP تشکیل شده است. میدان دید (Scope) محدوده‌ای از آدرس‌های IP را مشخص می‌کند که سرور می‌تواند آنها را به مشتری‌های DHCP متقاضی ارائه دهد.

برای ایجاد میدان دید از Scope Wizard استفاده می‌شود. در این ویزارد پارامترهای مربوط به DHCP مانند محدوده استثناء (exclusion range) دیده می‌شوند. محدود استثناء زیرشبکه‌ای از آدرس‌های IP موجود در ناحیه دید است که به مشتری‌های DHCP ارائه نمی‌شود.

معیار دیگری که در پیکربندی توسط ناحیه دید در نظر گرفته می‌شود مدت زمانی است که آدرس‌های IP به مشتری ارائه می‌شوند و به اصطلاح با آن «قرارداد دارند». قرارداد مدت زمان استفاده مشتری از آدرس IP یکی از معیارهای مهم پیکربندی است که در حوزه دیگری مانند امنیت شبکه تأثیر فراوانی دارد.

در بخش قبلی و در هنگام نصب DHCP روی سرور تا مرحله‌ای پیش رفتیم که New Scope Wizard باز شد. اگر خدمات DHCP را توسط Add or Remove Programs نصب کرده‌اید DHCP نصب می‌شود اما این ویزارد را مشاهده نخواهید کرد.

مباحث مربوط به قرارداد DHCP

مدت زمان قرارداد DHCP با آدرس‌های IP تأثیر مهمی در کارایی شبکه دارد. اگر تعدادی کامپیوتر دارید که کاربران آنها به زیرشبکه‌های متفاوت متصل می‌شوند و شبکه نسبتاً سیاری دارید (شبکه دارای Laptop است) استفاده از قراردادهای با مدت زمان کمتر، دسترسی کاربران به منابع شبکه را آسانتر می‌کند.

تعداد آدرس‌های IP می‌تواند کمتر از تعداد کامپیوترهای شبکه باشد. مثلا می‌توانید شیفت‌های مختلفی داشته باشید، و در حالی که تعداد کاربران ثابت است، افراد مختلفی در شیفت‌های روز و شب به کامپیوترهای مختلفی وارد شوند.

از آنجا که از همه کامپیوترهای شبکه به صورت همزمان استفاده نمی‌شود با قراردادهای کوتاه‌مدت می‌توانید مخزنی از آدرس‌های IP را میان کامپیوترهای مختلف تقسیم کنید.

اگر شبکه نسبتا ثابتی دارید و وسایل در این شبکه جابه‌جایی زیادی ندارند از قراردادهای طولانی‌تر استفاده کنید. قراردادهای طولانی مدت تعداد نمایش‌های DHCP (DHCP broadcast) را کاهش می‌دهند زیرا کامپیوترها، قراردادها را تجدید نمی‌کنند. تعداد نمایش کمتر باعث می‌شود پهنای باند کمتری به ترافیک نمایش‌ها اختصاص یابد. بنابراین اگر مسئله پهنای باند برایتان مهم است قراردادهای طولانی مدت ارجعیت دارند.

تنظیم مدت زمان قرارداد در صفحه Lease Duration انجام می‌شود. پس از تنظیم مدت زمان قرارداد روی Next کلیک کنید. مدت زمان قرارداد پیش‌فرض ۸ ساعت است.

ایجاد میدان دید فوق‌العاده (Superscope)

قبل از پایان دادن به بحث درباره میدان دید با مفهوم منیدان دید فوق‌العاده آشنا می‌شوید. هنگام ایجاد میدان دید روی سرور DHCP فرض بر این است که محدوده آدرس‌های IP تنها زیرشبکه‌های منطقی را در بر می‌گیرد.

فرض کنید در یکی از زیرشبکه‌هایی که ایجاد کرده‌اید به تعداد بیشتری آدرس IP نیاز دارید بنابراین باید میدان دیدی ایجاد کنید که آدرس‌هایی بیشتر از آدرس‌های یک زیرشبکه داشته باشد. برای ایجاد یک میدان دید فوق‌العاده، یک میدان دید معمولی ایجاد کرده و آدرس‌های IP چندین زیرشبکه را به آن اختصاص می‌دهید. برای ایجاد یک میدان دید فوق‌العاده از گام‌های زیر استفاده کنید:

۱- در نمای فوری DHCP روی آیکون سرور DHCP کلیک راست کرده و از منوی ظاهر شده New Scope را انتخاب کنید.

۲- پس از عبور از صفحه اول ویزارد، در صفحه IP Address Range ، آدرس‌های ابتدایی و انتهایی میدان دید IP را وارد کنید و ماسک زیرشبکه را مشخص کنید. آدرس‌های IP باید به بیش از یک زیرشبکه تعلق داشته باشد.

۳- در صفحه بعد به شما اعلام می‌شود که آدرس‌های IP به بیش از یک زیرشبکه تعلق دارند و میدان دیدی که ایجاد می‌شود یک میدان دید فوق‌العاده (Superscope) است.

۴- گزینه yes را انتخاب و روی Next کلیک کنید.

۵- در صفحه بعد مدت زمان قرارداد میدان دید فوق‌العاده را تنظیم کنید و روی Next کلیک کنید.

همان طور که در ایجاد میدان دید معمولی گفته شد در مرحله بعدی ویزارد گزینه‌های مربوط به ارائه اطلاعات اضافی را نمایش می‌دهد. این اطلاعات به دروازه پیش‌فرض، سرور DNS و سرور

WINS مربوط می‌شوند. پس از وارد کردن اطلاعات لازم به فرایند ایجاد میدان دید فوق‌العاده خاتمه دهید.

ایجاد ذخیره‌ها

اگر بخواهید وسایل خاصی روی شبکه مانند چاپگرها همواره آدرس IP یکسانی دریافت کنند و این آدرس‌دهی توسط سرور DHCP به صورت پویا انجام شود آدرس IP را ذخیره کرده‌اید و به این آدرس، ذخیره (reservation) گویند.

برای ایجاد یک ذخیره از مراحل زیر استفاده کنید:

۱- در نمای فوری DHCP روی یکی از میدان‌های دید دوباره کلیک کنید.

۲- در صفحه جزییات روی آیکون Reservation کلیک راست کرده و گزینه New Reservation را انتخاب کنید.

۳- نام ذخیره و آدرس سخت‌افزاری MAC مربوط به وسیله‌ای که آدرس IP برای آن ذخیره می‌شود را وارد کنید. سپس آدرس IP واقعی را وارد کرده و روی Ok کلیک کنید.

فعال‌سازی میدان دید

برای این که مشتری‌های DHCP بتوانند از میدان دید استفاده کنند باید آن را فعال کنید. روی آیکون Scope کلیک راست کرده و گزینه Activate را انتخاب کنید. اگر گزینه Activate را در منو نمی‌بینید و گزینه Deactivate را مشاهده می‌کنید میدان دید از قبل فعال شده است.

تأیید سرور DHCP در دایرکتوری فعال

همه سرورهای DHCP که ناحیه ویندوز سرور ۲۰۰۳ قرار دارند باید توسط دایرکتور فعال تأیید شوند تا بتوانند روی شبکه کار کنند. با این کار اختصاص آدرس‌های IP نادرست به مشتری‌های DHCP جلوگیری می‌کند و امنیت شبکه بالاتر می‌رود.

اگر سرور توسط دایرکتوری فعال تأیید نشده باشد در نمای DHCP در کنار آن یک پیکان رو به پایین قرمز رنگ دیده می‌شود. اگر این سرور انتخاب کنید وضعیت آن در صفحه جزییات به صورت Autorize the DHCP Server نمایش داده می‌شود.

برای تأیید سرور DHCP برای کار در شبکه و دادن مجوز فعالت به آن از نمای فوری DHCP استفاده می‌شود. روی آیکون سرور کلیک کنید و در منوی Action گزینه Refresh را انتخاب نمایید. سرور با پیکان سبز رنگ دیده می‌شود که به معنای این است که مجوز کار در شبکه و اختصاص آدرس IP را دارد.

اگر سرور DHCP یک از سرورهای عضو ناحیه باشد یا کنترل‌کننده یک ناحیه فرزند است و بخواهید توسط یک سرور DHCP دیگر اجازه فعالیت آن را تأیید کنید، نمای فوری DNS را باز کرده و روی آیکون DHCP کلیک کنید. در منوی Action گزینه Manage Authorized Servers را انتخاب کنید تا جعبه محاوره آن باز شود.

روی دکمه Authorize کلیک کنید. نام یا آدرس IP سرور DHCP که می‌خواهید اجازه فعالیتش را تأیید کنید وارد کرده و روی Ok کلیک کنید.

به شما اجازه داده می‌شود تا سرور DHCP را به فهرست سروهای DHCP مجاز اضافه کنید.

اگر آدرس IP در فهرست قرار گرفته است روی yes کلیک کنید و جعبه محاوره را ببندید.

یکپارچه‌سازی DHCP و DNS

در ویندوز سرور ۲۰۰۳ ، DHCP و DNS با هم یکپارچه می‌شوند. اگر DHCP و DNS برای به روز رسانی پویا (Dynamic Update) پیکربندی شده باشند، هر گاه DHCP یک آدرس IP را به مشتری متقاضی اختصاص دهد، نام میزبان مشتری و آدرس IP در پایگاه داده DNS ثبت می‌شوند.

برای پیکربندی DHCP به روز سازی پویا از گام‌های زیر استفاده کنید:

۱- در نمای فوری DHCP روی آیکون سرور DHCP کلیک راست کرده و گزینه Properties را انتخاب کنید.

۲- روی کادر DNS کلیک کنید. در کادر DNS با چندین گزینه مواجه می‌شوید:

* Enable DNS Dynamic Updates according to the Settings below : این جعبه چک به صورت پیش‌فرض فعال است و در صورت انتخاب آن می‌توانید از میان دو گزینه که در پایین آن قرار دارند یکی را انتخاب کنید.

* Dynamically update DNS A and PTR records only if requested by the DHCP Clients : این گزینه نیاز به صورت پیش‌فرض انتخاب شده است و به این معناست که سرور DNS اطلاعات به روز رسانی را فقط هنگامی دریافت می‌کند که مشتری یک آدرس IP را از سرور DHCP تقاضا کند.

* Always dynamically update DNS A and PTR records : با انتخاب این گزینه رکوردهای DNS مربوط به هر مشتری DHCP که تقاضای تجدید آدرس IPرا دارد، به‌روز می‌شوند.

* Discard A and PTR records when lease id deleted : این گزینه پیش‌فرض، سرور DHCP موظف می‌کند تا پیامی را به سرور DNS بفرستد تا در صورت اتمام قرارداد آدرس IP رکوردهای مربوط به میزبان حذف شوند.

* Dynamically update DNS A and PTR records for DNS Clients that do not request Update : اگر یک از کامپیوترهای مشتری از به روز رسانی پویا پشتیبانی بکنند اما دارای قرارداد آدرس IP باشد، انتخاب این گزینه باعث می‌شود که DHCP اطلاعات به روز شده را به سرور DNS بفرستد.

۳- بعد از انتخاب گزینه مناسب (اگر از مشتری‌های با ویندوز قبل از ویندوز ۲۰۰۰ استفاده می‌کنید ممکن است تغییراتی نیاز باشد و در غیر این صورت گزینه‌های پیش‌فرض را انتخاب کنید). روی دکمه Ok کلیک کنید تا به نمای فوری DHCP برگردید.

ویرایش گزینه‌ای سرور DHCP

تنظیمات مربوط به سرور DHCP مانند دروازه پیش‌فرض (default gateway) ، سرور DNS و سرور WINS را می‌توانید تغییر دهید. ویرایش این گزینه‌ها در جعبه محاوره Server Option Properties انجام می‌شود.

روی درخت نمای فوری، گروه سرور DHCP را باز کنید. روی آیکون Server Options کلیک راست کرده و Configure Options را انتخاب کنید تا جعبه محاوره مربوط به آن باز شود.

وارد کادر General شوید، هر یک از گزینه‌های موجود در این کادر دارای شمارهٔ مخصوص به فرد است مثلا شمارهٔ مسیریاب ۰۰۳ یا شماره سرور DNS معادل ۰۰۶ است. مثلا برای این که مسیریاب مربوط به مشتری‌های DHCP بتوانند اطلاعات را از سرور DHCP به دست آورند در جعبهٔ چک ۰۰۳ کلیک کرده و سپس آدرس IP مسریاب را وارد نمایید. پیکربندی سرور DNS و WINS به همین صورت است. پس از انجام تغییرات در اطلاعات پیکربندی روی Ok کلیک کنید تا جعبهٔ محاوره بسته شود.

بررسی قراردادهای DHCP

از آنجا که هدف اصلی DHCP ارائه قراردادهایی IP به مشتریانش است باید به بررسی این قراردادها پرداخت. قراردادهای جاری در نمای فوری DHCP مشاهده می‌شود. برای دیدن آنها از گام‌های زیر استفاده کنید:

۱- در نمای فوری DHCP گره سرور DHCP را باز کنید. پوشهٔ Scope را ملاحظه می‌نمایید.

۲- این پوشه را باز کرده و روی ایکون Address Leases کلیک نمایید.

۳- همهٔ قراردادهای جاری در صفحه جزئیات نمای فوری دیده می‌شود.

همچنین می‌توانید سرورهای دیگری را به نمای فوری اضافه کنید. با این کار می‌توانید به طور همزمان چندین سرور DHCP را بررسی نمایید. در نمای فوری DHCP روی آیکون DHCP کلیک کرده و سپس در منوی Action گزینهٔ Monage Authorized Server را انتخاب کنید.

برای افزودن یک سرور به نمای فوری روی سرور کلیک کرده و Ok را انتخاب کنید.

سرور به نمای فوری DHCP اضافه می‌شود. حالا می‌توانید میدان دید آدرس IP و قراردادهای موجود را بررسی کنید.

سرور به نمای فوری DHCP اضافه می‌شود. حالا می‌توانید میدان دید آدرس IP و قراردادهای موجود را بررسی کنید.

بارگذاری پشتیبان پایگاه داده DHCP

یکی دیگر از مسایل مدیریتی DHCP بر روی شبکه کار با پشتیبان (back up) پایگاه داده DHCP است. به طور پیش‌فرض در هر ساعت از پایگاه داده، پشتیبانی تهیه می‌شود. اگر مشتری‌ها در استفاده از آدرس‌های IP دچار مشکل هستند احتمالا پایگاه دادهٔ DHCP دچار نقص است.

برای بارگذاری یک کپی پشتیبانی از مراحل زیر استفاده کنید:

۱- روی گره سرور DHCP کلیک راست کرده و گزینه Restore را انتخاب کنید. جعبهٔ محاوره‌ای باز می‌شود که در آن پوشهٔ عمومی پشتیبان DHCP را تعیین می‌کنید. معمولا این پوشه به صورت پیش‌فرض انتخاب شده است.

۲- روی Ok کلیک کنید. به شما اعلام می‌شود که سرور باید مجدداً راه‌اندازی شود تا پشتیبان پایگاه داده بارگذاری شود (Load).

عیب‌یابی DHCP

دو فرمان مفید در عیب‌یابی DHCP عبارتند از ping و ipcofig . فرمان ping اتصال بین سرور DHCP و مشتری را چک می‌کند. ipconfig پیکربندی IP مربوط به مشتری را نشان می‌دهد. اگر با اجرای این فرمان آدرس IP و ماسک زیرشبکه را مشاهده نکنید مشتری اطلاعات را از سرور DHCP دریافت نمی‌کند.