« فصل ۵ »

مدیریت پروتکل DHCP

Managing DHCP Protocol

TCP/IP یکی از پروتکل‌های پراهمیت در ویندوز سرور 2008 و 2008R2 می‌باشد. این پروتکل جهت برقراری ارتباط میان کاربران با استفاده از آدرس‌های IP مورد استفاده قرار می‌گیرد. جهت برخورداری کاربران و سرورها از آدرس‌های IP دو روش وجود دارد. روش اول وارد کردن آدرس‌ها به صورت دستی، و روش دوم دریافت آدرس به صورت خودکار می‌باشد. وارد کردن دستی آدرس‌های IP کار نسبتاً ساده‌ای است، مدیر شبکه به تنظیمات TCP/IP هریک از ماشین‌های متصل به شبکه رفته و یک آدرس به آن اختصاص می‌دهد. مشکل این روش زمانی آشکار می‌شود که تعداد ماشین‌ها در شبکه زیاد می‌شوند. تصور کنید که مدیر شبکه قرار است به ۵۰۰۰ ماشین در شبکه آدرس IP، Default Gateway، Subnet mask و آدرس‌های DNS را اختصاص دهد. در این مورد وارد کردن دستی آنها کار چندان ساده‌ای نخواهد بود.

به کمک سرویس DHCP[1] می‌توانید محدوده‌ای از آدرس‌ها و اطلاعات مورد نیاز مثل Default Gateway، Subnet mask و تنظیمات DNS را فراهم نموده و به راحتی آنها را به ماشین‌ها اختصاص دهید. در این فصل قصد داریم نحوه راه‌اندازی این سرویس و مدیریت آنرا مورد بررسی قرار دهیم. بطور کلی مهمترین مباحثی که در این فصل به آنها پرداخته خواهد شد عبارتند از:

- نصب و راه‌اندازی سرویس DHCP
- پیکربندی سرورریس DHCP
- ایجاد و مدیریت Scopeها
- DHCP در اکتیو دایرکتوری

۵-۱ معرفی پردازش DORA

ساده ترین راه جهت آشنایی با طرز کار DHCP، آگاهی از فرایندی به نام DORA می‌باشد. DORA برگرفته از لغات Discover (کشف)، Offer (پیشنهاد)، Request (درخواست) و Acknowledge (تصدیق) می‌باشد. بطور خلاصه، فرایند DORA در DHCP به صورت زیر می‌باشد:

۱. **Discover**: در شبکه‌های مبتنی بر IP، زمانی‌که کاربران قصد دارند از سرویس DHCP استفاده کنند، ابتدا ماشین آنها یک پیغام خاص که DHCPDISCOVER (کشف DHCP) نامیده می‌شود، به داخل شبکه ارسال می‌کند.

۲. **Offer**: کلیه سرورهای DHCP که در حال گوش دادن به درخواست‌های کاربران هستند، پس از دریافت این پیغام، پایگاه‌داده داخلی خود را بررسی نموده و با یک پیغام که DHCPOFFER نامیده می‌شود و حاوی آدرس IP است به کاربر پاسخ می‌دهند. محتویات این پیغام بستگی به این دارد

1. Dynamic Host Configuration Protocol

که سرور DHCP چگونه پیکربندی شده باشد. در ویندوز سرور 2008 و 2008R2 علاوه بر آدرس IP، Optiinهای دیگری نیز جهت اختصاص به کاربران وجود دارد (مثل Default Gateway و ...).

۳. **Request**: پس از اینکه درخواست کاربر توسط سرورهای DHCP پاسخ داده شد، کاربر یک یا تعدادی از پیام‌های DHCPOFFER را بسته به تعداد سرورهای DHCP که در زیرشبکه قرار دارد دریافت می‌کند، سپس یکی از آدرس‌ها را از میان OFFERها انتخاب نموده و پیغام DHCPREQUEST را به سرور انتخاب شده به منظور اعلام پذیرش سیگنال DHCPOFFER ارسال می‌کند. این پیغام‌ها ممکن است پارامترهای پیکربندی اضافه‌تری را درخواست کنند.

٤. **Acknowledge**: زمانی که سرور DHCP یک DHCPREQUEST دریافت می‌کند، یک آدرس IP را به عنوان آدرس درحال استفاده علامت‌گذاری نموده، سپس یک DHCPACK[1] (تصدیق DHCP) به کاربر ارسال می‌کند. پیغام تصدیق شامل پارامترهای درخواست شده در پیکربندی می‌باشد.
اگر سرور به هر دلیلی قادر به پذیرفتن DHCPREQUEST نباشد، یک پیغام DHCPNAK[2](عدم تصدیق DHCP) ارسال می‌کند. اگر کاربر این پیغام را دریافت کند، فرایند درخواست آدرس را مجدداً آغاز می‌کند.

٥. زمانی که کاربر آدرس IP پیشنهاد شده (OFFER) را می‌پذیرد، این آدرس برای مدت زمانی محدود به او اختصاص پیدا می‌کند که این عمل Lease (اجاره) نامیده می‌شود. پس از دریافت DHCPACK، کاربر یک بررسی نهایی پیرامون پارامترهای پیکربندی انجام داده و از مدت زمان Lease آگاه می‌شود. پس از آن، ماشین کاربر با تنظیمات دریافت‌شده از سوی سرور DHCP پیکربندی می‌گردد.

اگر کاربر متوجه شود که آدرس پیشنهاد شده ار طرف سرور قبلاً به ماشین دیگری اختصاص داده شده است، یک پیغام DHCPDECLINE (عدم پذیرش DHCP) برای سرور ارسال می‌کند. درصورتی که سرور DHCP با توجه به تعداد آدرس‌های موجود در پایگاه خود آدرس دیگری جهت اختصاص به کاربر دراختیار نداشته باشد قادر به ایجاد OFFER نمی‌باشد. اگر سایر سرورها نیز هیچ OFFERای ایجاد نکنند، اختصاص آدرس IP به کاربر با شکست مواجه می‌شود.

۵-۲ مزایا و معایب DHCP

DHCP جهت ساده کردن مدیریت شبکه ایجاد شده است. این پروتکل از مزایای قابل توجهی برخوردار است اما اشکالاتی نیز در آن دیده می‌شود. در ادامه، این مزایا و معایب را مورد بررسی قرار می‌دهیم.

1. DHCP Acknowledgment
2. DHCP Negative Acknowledgment

۵-۲-۱ مزایای DHCP

مهمترین مزایای DHCP به شرح زیر می‌باشد:

- پیکربندی آدرس‌های IP برای شبکه‌های بسیار بزرگ را ساده می‌کند. به عنوان مثال اگر قرار باشد آدرس سرور DNS برای کاربران شبکه تغییر کند، مدیر شبکه لازم نیست این تغییر را در تک تک ماشین‌ها و بطور فیزیکی اعمال کند، بلکه کافی است آنرا از طریق سرور DHCP تغییر دهد.
- زمانی که تنظیمات پیکربندی را در یک محل (که همان سرور است) انجام می‌دهید، این تنظیمات به صورت خودکار میان کاربران شبکه توزیع شده و مشکلات ناشی از انجام تنظیمات اشتباه بر روی ماشین‌های کاربران و نیاز به رفع این اشتباهات حذف می‌گردد.
- به دلیل وجود مدیریت مرکزی، از هدر رفتن آدرس‌هایIP جلوگیری می‌شود، زیرا این آدرس‌ها فقط در زمان درخواست کاربران به آنها اختصاص داده می‌شوند.
- پیکربندی IP در شبکه کاملاً خودکار انجام می‌شود. می‌توانید بدون نگرانی در رابطه با انتخاب آدرس IP، یک ماشین را به شبکه اضافه نموده و یا آنرا حذف کنید. به عنوان مثال زمانی که یک سرور DNS را در شبکه پیکربندی می‌کنید کافی است آدرس آنرا در تنظیمات سرور DHCP وارد کنید. پس از آن مشاهده خواهید نمود که این سرور برروی کلیه کاربران پیکربندی می‌شود.
- به ماشین‌های کاربران اجازه می‌دهد که در محیطی به نام PXE[1] اجرا شده و بتوانند آدرس‌های TCP/IP را از سرور DHCP دریافت کنند. کاربران PXE که کاربران "سرویس‌های نصب از راه دور ماکروسافت[2]" یا RIS نیز نامیده می‌شوند، می‌توانند بدون نیاز به داشتن سیستم عامل بر روی کامپیوتر خود، آدرس‌های IP را دریافت کنند (به شبکه متصل شوند). این کار به کاربران RIS امکان می‌دهد تا از طریق پروتکل TCP/IP به سرور RIS متصل شده و به صورت Remote بتوانند سیستم عامل را دریافت کنند.

۵-۲-۲ معایب DHCP

متأسفانه، تعدادی مشکل نیز در DHCP وجود دارد که عبارتند از:

- سرور DHCP می‌تواند به یک مرکز شکست برای شبکه تبدیل شود. اگر در شبکه تنها یک سرور DHCP داشته باشید و این سرور در دسترس نباشد، کاربران نمی‌توانند از آن آدرس IP درخواست کنند.

1. Preboot Execution Environment
2. Microsoft Remote Installation Services

- اگر سرور DHCP حاوی اطلاعات اشتباه باشد، این اطلاعات بطور خودکار برروی همه کاربران آن اعمال می‌شود.
- اگر بخواهید سرور DHCP را در یک شبکه چندقسمتی[1] استفاده کنید، باید برای هر قسمت یک سرور DHCP راه‌اندازی کنید؛ همچنین در صورتی که از مسیریاب[2] بین دو قسمت از شبکه استفاده می‌کنید باید مطمئن شوید که مسیریاب شما قابلیت انتقال پیام‌ها از یک قسمت به قسمت دیگر را دارا می‌باشد.

۵-۳ فرایند DHCP Lease

فرایند DHCP Lease مراحلی است که از زمان درخواست آدرس IP توسط یک کاربر تا زمان تحویل این آدرس توسط سرور DHCP باید طی شوند. این مراحل عبارتند از:

۱. DHCP discovery
۲. DHCP lease offer
۳. DHCP lease Selection
٤. DHCP lease acknowledgment

پس از پایان این مراحل، کاربر قادر خواهد بود آدرس IP و سایر تنظیمات پیکربندی که در سروریس DHCP تعریف شده است را از آن دریافت کند. در ادامه این مراحل را شرح خواهیم داد.

۵-۳-۱ مرحله ۱: DHCP discovery

اولین مرحله در فرایند DHCP Lease، پیدا کردن سرور DHCP می‌باشد. این مرحله زمانی اتفاق می‌افتد که کاربر DHCP برای اولین بار به شبکه متصل شده و درخواست پیکربندی آدرس IP می‌کند، و یا زمانی که یک آدرس IP درخواست می‌شود ولی در دسترس نیست.

در زمان درخواست Lease، کاربر از آدرس IP خود و آدرس سرور آگاهی ندارد بنابراین از آدرس 0.0.0.0 برای خود و 255.255.255.255 برای سرور استفاده می‌کند. پس از آن یک پیغام DHCPDISCOVER را در قالب بسته‌های UDP[3] و از طریق پورت شماره ٦٨ (در مبدأ) به پورت شماره ٦٧ از مقصد می‌فرستد. این پیغام حاوی آدرس سخت افزار (MAC)[4] کاربر می‌باشد. اگر این پیغام توسط سرور DHCP پاسخ داده نشود، درخواست مجدداً برای پنج بار و در فواصل زمانی ۰، ٤، ۸، ١٦ و ۳۲ ثانیه تکرار می‌شود. اگر کاربر هنوز پاسخی دریافت نکرده باشد، از مکانیسمی به نام APIPA[5] و یا از تنظیمات پیکربندی ثانویه برای ارسال پیغام‌های DHCPDISCOVER به سرور استفاده

1. Multisegment
2. Router
3. User Datagram Protocol
4. Media Access Control Address
5. Automatic Private IP Addressing

می‌کند. این پیغام‌ها هر پنج دقیقه یک بار فرستاده می‌شوند.

با استفاده از APIPA، کاربر بجای انتظار برای دریافت پاسخ، آدرسی که فکر می‌کند مورد استفاده قرار نگرفته است را انتخاب می‌کند (این آدرس به صورت 169.254 x x می‌باشد). با وجود اینکه پس از آن کاربر دارای آدرس IP می‌باشد، اما بازهم هر پنج دقیقه یک بار، به درخواست خود جهت اتصال به سرور DHCP ادامه می‌دهد. زمانی که سرور DHCP در دسترس قرار گرفت، کاربر آدرس خود را از آن دریافت خواهد نمود.

۵-۳-۲ مرحله ۲: DHCP lease offer

در مرحله دوم از فرایند DHCP Lease، هر سرور DHCP که در شبکه پیغام DHCPDISCOVER را دریافت کند، در صورت دارا بودن یک آدرس معتبر درخواست کاربر را با استفاده از یک پیغام OFFER پاسخ می‌دهد (این ویژگی به شما امکان می‌دهد که چندین سرور DHCP را در شبکه پیکربندی نموده و درصورتی که یک سرور قادر به پاسخگویی نباشد، سایر سرورها بتوانند به درخواست‌ها پاسخ دهند).

پیغام OFFER از سمت سرور به کاربر پیشنهاد می‌شود و حاوی اطلاعاتی مانند آدرس IP و معمولاً سایر اطلاعات مثل آدرس قاب زیرشبکه[1]، مدت زمان Lease (به روز) و Default Gateway می‌باشد. هر پیغام OFFER فقط به یک کاربر فرستاده می‌شود و در واقع برای آن کاربر رزرو[2] می‌شود، بنابراین امکان اختصاص یک آدرس به چندین کاربر وجود ندارد. این پیغام‌ها مستقیماً به آدرس سخت افزار کاربر (MAC) فرستاده می‌شوند.

۵-۳-۳ مرحله ۳: DHCP lease Selection

سومین مرحله از فرایند DHCP Lease زمانی آغاز می‌شود که کاربر حداقل یک OFFER دریافت می‌کند. در این مرحله، ماشین کاربر یکی از OFFERها را که معمولاً اولین OFFER دریافت شده است انتخاب می‌کند. پس از انتخاب، کاربر پیغام پذیرش (ACCEPT) که حاوی آدرس IP سرورِ انتخاب شده می‌باشد در شبکه ارسال (پخش) می‌کند. پخش این پیام در شبکه باعث می‌شود که سایر سرورها، OFFERهای فرستاده شده به کاربر را برای او رزرو نکنند.

۵-۳-۴ مرحله ۴: DHCP lease Acknowledgment

زمانی که سرور DHCP پیغام پذیرش را از طرف کاربر دریافت می‌کند، یک آدرس IP را به عنوان Lease علامت‌گذاری نموده و یک پیغام تصدیق که DHCPACK نامیده می‌شود برای کاربر ارسال می‌کند.

1. Subnet mask
2. Reserve

اگر مشکلی وجود داشته باشد، سرور یک پیغام تصدیق منفی یا DHCPNACK به کاربر ارسال می‌کند. این پیغام‌ها بیشتر به دلایل زیر ایجاد می‌شوند:

- یک کاربر در حال تلاش جهت تمدید یک Lease برای آدرس IP سابق خود می‌باشد در حالی که آن آدرس به کاربر دیگری اختصاص داده شده است.
- کاربر دارای آدرس IP نادرستی می‌باشد زیرا مکان خود را بطور فیزیکی در شبکه تغییر داده است.

پیغام DHCPACK شامل همه تنظیمات مشخص شده توسط سرور DHCP به همراه آدرس IP و آدرس قاب زیرشبکه می‌باشد. زمانی که یک کاربر این پیغام را دریافت می‌کند، همه این پارامترها را در پشته IP ماشین خود یکپارچه می‌کند، درست مثل اینکه این پارامترها را به صورت دستی پیکربندی کرده باشد.

مراحل بالا اگرچه ممکن است کمی پیچیده به نظر برسند ولی وجود همگی آنها ضروری است. نتیجه فرایند DHCP Lease این است که دقیقاً یک سرور، یک آدرس IP را به یک کاربر اختصاص می‌دهد. اگر هریک از سرورهایی که پیغام‌های OFFERرا ارسال می‌کنند عملکرد صحیحی نداشته باشند، به عنوان مثال سریعاً پس از درخواست یک کاربر آدرس را به او اختصاص دهند، طولی نمی‌کشد که دیگر آدرسی برای کاربران جدید وجود نداشته باشد. همچنین زمانی که یک کاربر درحال تصمیم گیری برای پذیرش و یا رد یک Lease می‌باشد، کاربران کُند می‌توانند باعث شوند که سرور یک آدرس را به عنوان آدرس اختصاص داده نشده علامت‌گذاری نموده و سپس آنرا در جایی دیگر اختصاص دهد. این امر باعث می‌شود که به دو کاربر یک آدرس IP اختصاص داده شود.

۵-۳-۵ تمدید[1] DHCP Lease

زمانی که یک Lease منقضی[2] می‌شود و یا نیاز به تمدید دارد چه اتفاقی می‌افتد؟ هرگاه مدت Lease به بیش از نصف زمان تعریف شده می‌رسد (این زمان T1 نامیده می‌شود)، کاربر یک درخواست تمدید جدید به سرور DHCP ارسال می‌کند. اگر سرور به پیغام درخواست کاربر گوش دهد و دلیلی برای ردکردن آن وجود نداشته باشد، یک پیغام DHCPACK به کاربر ارسال می‌کند که مدت زمان Lease را Reset (بازنشانی) می‌کند. این کار مثل این است که یک راننده درخواست اجاره یک ماشین را تمدید نموده، و اجاره‌دهنده این درخواست را امضا کند.

اگر سرور DHCP در دسترس نباشد، کاربر متوجه می‌شود که امکان تمدید Lease وجود ندارد بنابراین از همان آدرس فعلی استفاده می‌کند. زمانی‌که ۸۷.۵ درصد از زمان Lease سپری شد (این

1. DHCP Lease Renewal
2. Expires

زمان T2 نامیده می‌شود)، کاربر درخواست تمدید دیگری به سرور ارسال می‌کند. در این نقطه زمانی، هر سرور DHCP که به پیغام درخواست گوش دهد، می‌تواند با استفاده از یک DHCPACK به کاربر پاسخ داده و Lease را تمدید کند. اگر در هر لحظه طی این پردازش، کاربر یک پیغام DHCPNACK دریافت کند باید سریعاً استفاده از آدرس IP را متوقف نموده و فرایند درخواست Lease را از ابتدا آغاز کند.

زمانی که کاربر با یک آدرس IP مقداردهی شد، در زمان‌های تعیین شده برای تمدید Lease تلاش می‌کند. در صورتی که پس از اتمام زمان Lease قصد نداشته باشد از آن استفاده کند، دیگر درخواستی جهت تمدید آن ارسال نمی‌کند. اگر کاربر قصد تمدید Lease را داشته باشد ولی قادر به انجام آن نباشد، کلیه عملکردهای مبتنی بر IP تا زمانی که یک آدرس معتبر بدست آورد متوقف خواهند شد.

۵-۳-۶ آزاد سازی DHCP Lease

اگرچه ممکن است درخواست تمدید Lease بارها تکرار شود اما گاهی پیش می‌آید که دیگر نیازی به استفاده از Lease نمی‌باشد و باید آدرس اختصاص داده شده به کاربر آزاد گردد. آزاد شدن Lease می‌تواند به دلیل لغو کردن آن توسط کاربر و یا سرور انجام شود. به عنوان مثال زمانی که کاربر قبل از منقضی شدن زمان Lease موفق به تمدید آن نشود، این فرایند را رها نموده و به APIPA مراجعه می‌کند. فرایند آزادسازی Lease از اهمیت زیادی برخوردار می‌باشد زیرا آدرس اشغال شده توسط سیستم را پس گرفته و به سرور تحویل می‌دهد.

۵-۴ آشنایی با Scopeها

اکنون که با فرایند Lease آشنا شدید، لازم است قبل از وارد شدن به بحث پیکربندی سرور DHCP، با مفاهیمی همچون Scope، Superscope، Exclusion، Reservation، Address Pool و Relay Agent آشنا شوید. در ادامه هریک از این مفاهیم را مورد بررسی قرار خواهیم داد.

۵-۴-۱ Scope

Scope، محدوده‌ای پیوسته از آدرس‌های IP است. معمولاً برای هر زیرشبکه فیزیکی یک Scope وجود دارد که می‌تواند با آدرس‌های کلاس A، B، C از IPv4 و یا آدرس‌های IPv6 مقداردهی شود. سرور DHCP از این Scopeها جهت مدیریت و اختصاص آدرس‌های IP به کاربران استفاده می‌کند.

هر Scope شامل مجموعه‌ای از پارامترها است که Scope option نامیده می‌شوند و می‌توانید آنها را برروی ماشین‌های کاربران پیکربندی کنید. Scope optionها در واقع داده‌هایی که پس از اتمام فرایند درخواست آدرس، به کاربران DHCP تحویل داده می‌شوند را کنترل می‌کنند. به عنوان مثال

پارامترهایی مانند آدرس سرور DNS و آدرس Default Gateway گزینه‌هایی هستند که می‌توانند به صورت جداگانه در Scope تعریف شده و به کاربران اختصاص داده شوند.

۵-۴-۲ Superscope

Superscopeها به سرور DHCP اجازه می‌دهند که آدرس‌های موجود در بیش از یک Scope را برای کاربران یک زیرشبکه فیزیکی فراهم کنند. این کار زمانی مفید است که کاربرانِ یک زیرشبکه، به بیش از یک شبکه مبتنی بر IP متصل هستند؛ بنابراین باید آدرس‌های IP خود را از بیش از یک Address Pool (حوض آدرس) بدست آورند. در کنسول مدیریت DHCP می‌توانید آدرس‌های اختصاص داده شده در Superscope را مدیریت کنید.

۵-۴-۳ Exclusions و Reservations

Scopeها تعیین می‌کنند که چه آدرس‌های IP می‌توانند به کاربران اختصاص داده شوند. دو روش دیگر جهت تعیین آدرس‌های اختصاص داده شده به کاربران، Exclusion و Reservation می‌باشد.

- **Exclusion**: محدوده‌ای از آدرس‌های IP است که قصد ندارید بطور خودکار به کاربران اختصاص داده شوند. این آدرس‌ها خارج از محدوده DHCP می‌باشند، بنابراین زمانی که نمی‌خواهید آدرس‌های IP مشخصی به کاربران اختصاص داده شوند می‌توانید آنها را در محدوده Exclusions تعریف کنید. آدرس‌هایی که در این محدوده تعریف می‌شوند معمولاً برای سرورها و کاربردهای ضروری در شبکه مورد استفاده قرار می‌گیرند.
- **Reservation**: محدوده‌ای از آدرس‌های IP است که می‌توانید بطور دائمی به فرایند DHCP Lease اختصاص دهید. این آدرس‌ها اساساً محدوده‌ای از آدرس‌های IP هستند که می‌توان آنها را برای تعدادی دستگاه مخصوص در شبکه رزرو کرد. اگر این دستگاه‌ها با اجرای فرایند DHCP Release (آزادسازی DHCP Lease) آدرس IP خود را به سرور تحویل دهند، پس از درخواست مجدد، همان آدرس قبلی را دریافت خواهند نمود.

آدرس‌های Exclusion زمانی استفاده می‌شوند که نخواهید یک محدوده از آدرس‌های IP در سرور DHCP استفاده شوند. آدرس‌های Reservation نیز زمانی استفاده می‌شوند که قصد داشته باشید محدوده‌ای از آدرس‌های IP را برای کاربران مشخصی اختصاص دهید تا این کاربران همیشه از آدرس‌های یکسانی استفاده کنند.

۵-۴-۴ Address Pool

محدوده‌ای از آدرس‌های IP است که می‌تواند در سرور DHCP مورد استفاده قرارگرفته و به کاربران یا سرورها اختصاص داده شود. فرض کنید که در یک سرور DHCP، یک Scope جدید ایجاد نموده که آدرس زیرشبکه در آن 192.168.1 می‌باشد. این Scope تعداد ۲۵۵ آدرس (از 192.168.1.1 تا 192.168.1.255) در اختیار شما قرار می‌دهد که این آدرس‌ها، Address Pool این Scope را تشکیل می‌دهند. پس از اضافه کردن این Address Pool می‌توانید به عنوان مثال آدرس‌های 192.168.1.240 تا 192.168.1.255 را به عنوان محدوده Exclusion تعریف کنید تا به کاربران اختصاص داده نشوند.

۵-۴-۵ DHCP Relay Agent

سرویس DHCP، جهت برقراری ارتباط میان کاربران و سرورها در یک شبکه مبتنی بر IP طراحی شده است، اما در استانداردهای تعریف شده برای شبکه‌ها (RFC 1542) راهکارهایی جهت برقراری ارتباط میان کاربران و سرورها در شبکه‌های جداگانه که مبتنی بر IP می‌باشند ایجاد شده است. زمانی که هیچ سرور DHCP در شبکه قابل دسترسی نباشد، می‌توان با استفاده از DHCP Relay Agent (عامل تقویت‌کننده DHCP) پیغام‌های کاربرانِ یک شبکه را دریافت نموده و آنرا به سرور DHCP منتقل نمود. Relay Agent به عنوان یک تقویت‌کننده عمل می‌کند یعنی اینکه به درخواست‌های کاربران DHCP در یک شبکه گوش داده و این درخواست‌ها را از طریق مسیریاب به سرور DHCP تحویل می‌دهد.

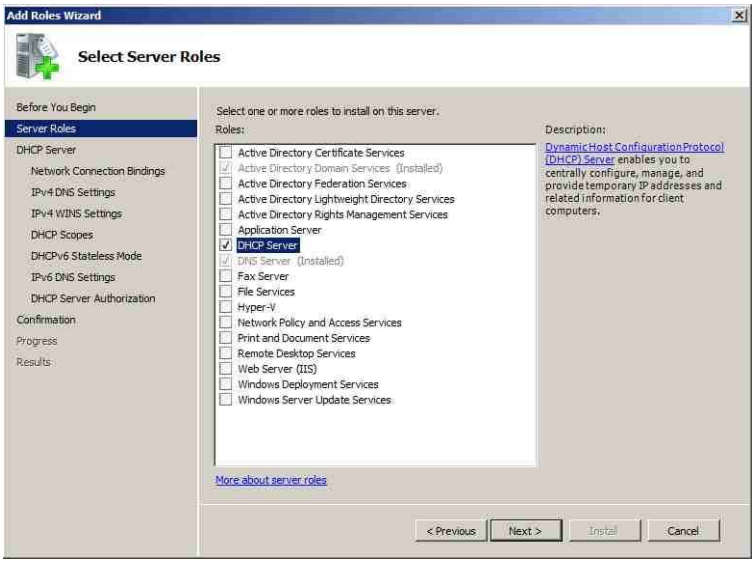
۵-۵ نصب DHCP Role

نصب DHCP با استفاده از ابزارهای جدید در ویندوز سرور 2008 و 2008R2 بسیار ساده شده است. کافی است قبل از شروع عملیات نصب، یک آدرس IP تهیه نموده و آنرا در تنظیمات TCP/IP سرور وارد کنید (آدرسی که فراهم کرده‌اید را باید به صورت دستی وارد کنید. چنانچه کارت شبکه آدرس را به صورت خودکار دریافت کند، قبل از نصب DHCP هشداری به شما داده خواهد شد). پس از وارد کردن آدرس IP می‌توانید مراحل زیر را دنبال کنید:

۱. کنسول Server Manager را از مسیر Start » Administrative Tools » Server Manager اجرا کنید.

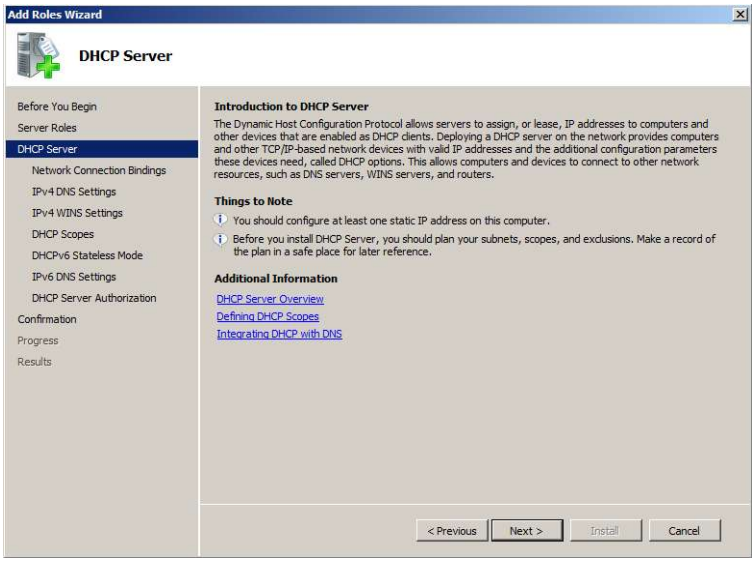
۲. در قسمت Roles Summary، گزینه Add Roles را انتخاب نموده تا ویزارد "Add Roles Wizard" اجرا شود.

۳. در صفحه "Select Server Roles" گزینه DHCP Server را انتخاب نموده و برروی Next کلیک کنید.



شکل ۵-۱

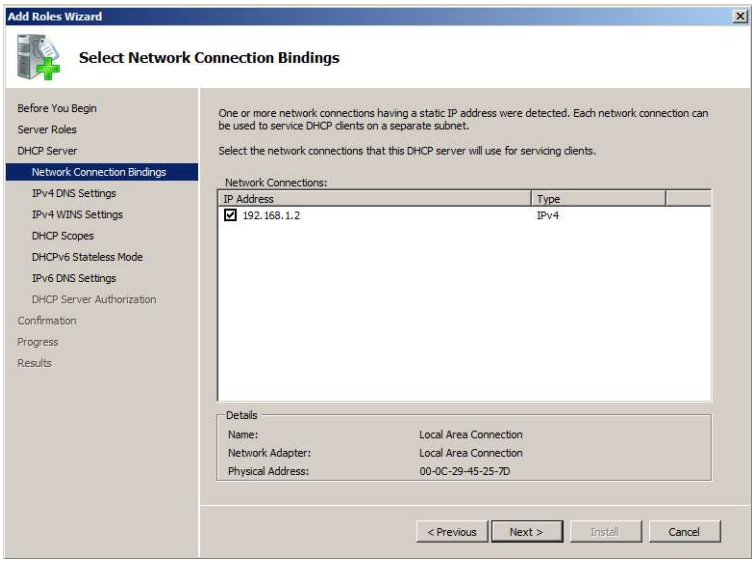
٤. در صفحه "DHCP Server"، توضیحاتی راجع به سرویس DHCP و عملکرد آن ارائه شده است. پس از مشاهده اطلاعات ارائه شده برروی Next کلیک کنید.



شکل ۵-۲

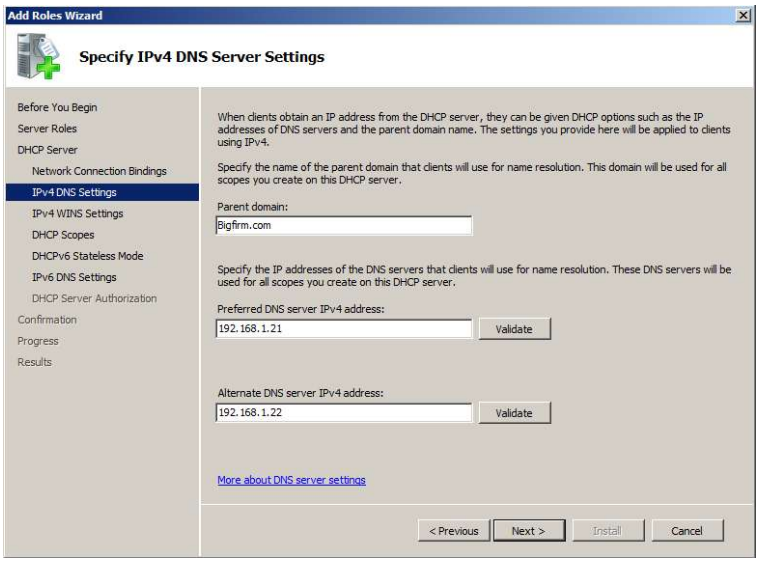
۵. در صفحه "Select Network Connection Bindings"، Connection های مورد استفاده در سرویس DHCP را انتخاب کنید. با کلیک برروی هر Connection، می‌توانید مشخصات آن از جمله نام و

MAC Address آنرا مشاهده کنید. پس از انتخاب Connection برروی Next کلیک کنید.



شکل ۵-۳

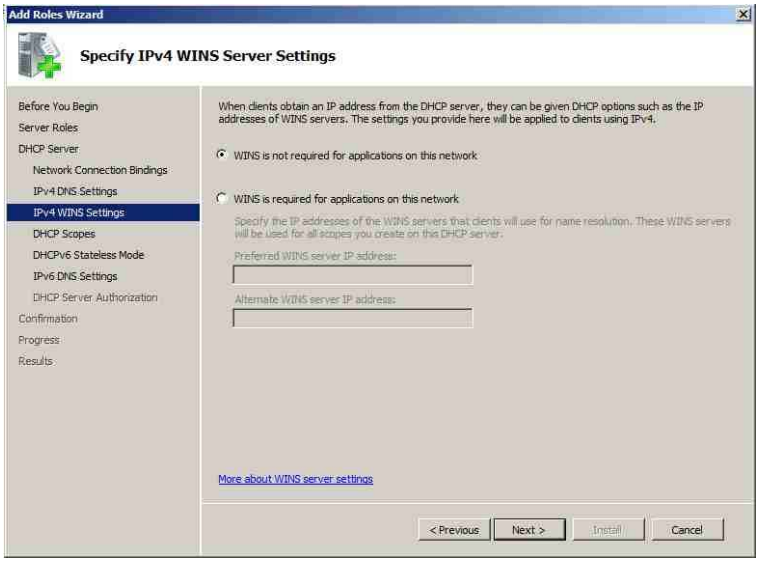
۶. در صفحه "Specify IPv4 DNS Server Settings" باید نام دامنه، آدرس سرور DNS اصلی و در صورت وجود، آدرس سرور DNS ثانویه را وارد کنید. پس از آن برروی Next کلیک کنید.



شکل ۵-۴

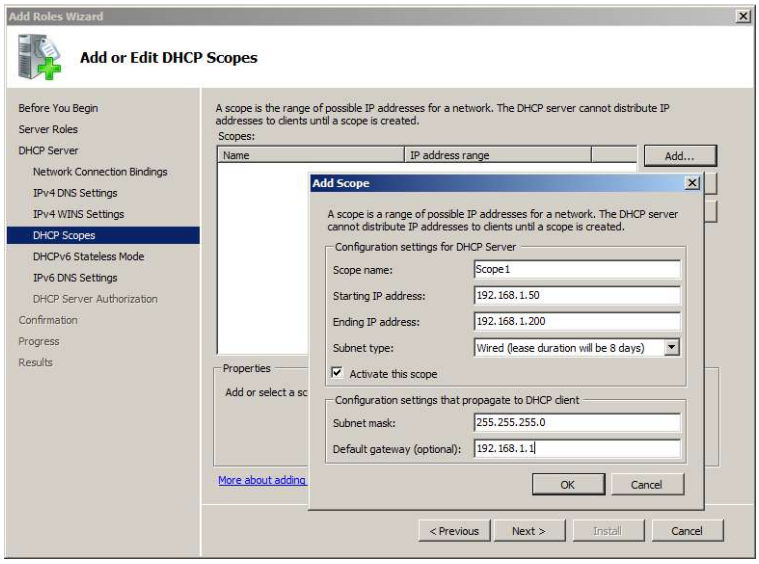
۷. در صفحه "Specify IPv4 WINS Server Settings" چنانچه از سرور WINS در شبکه استفاده

می‌کنید، با انتخاب گزینه دوم آدرس آنرا وارد نموده و در غیر اینصورت برروی Next کلیک کنید.



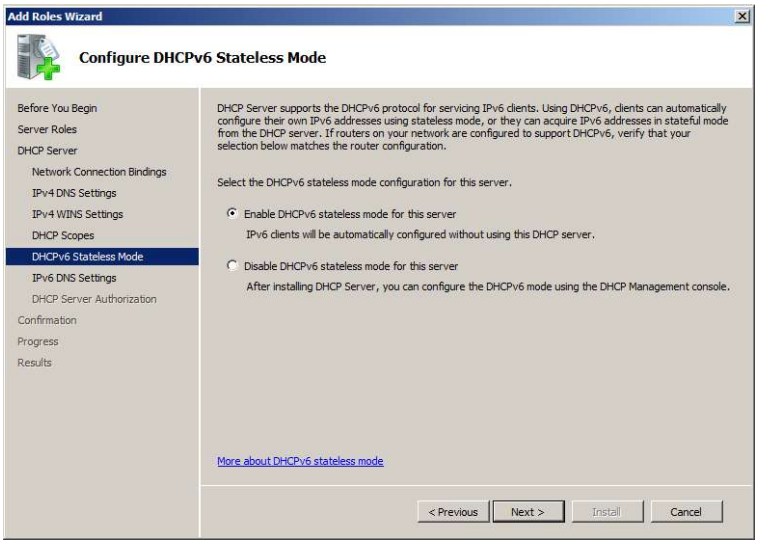
شکل ۵-۵

۸. در صفحه "Add or Edit DHCP Scopes" می‌توانید Scope های مورد نظر را ایجاد یا ویرایش کنید. جهت اضافه کردن Scope برروی Add کلیک کنید نموده و در پنجره "Add Scope" مشخصات Scope را وارد کنید. (نام Scope، آدرس شروع و پایان، بستر ارتباطی شبکه (کابل یا بی‌سیم)، قاب زیرشبکه و Default Gateway). پس از تکمیل فیلدها برروی OK و سپس برروی Next کلیک کنید.



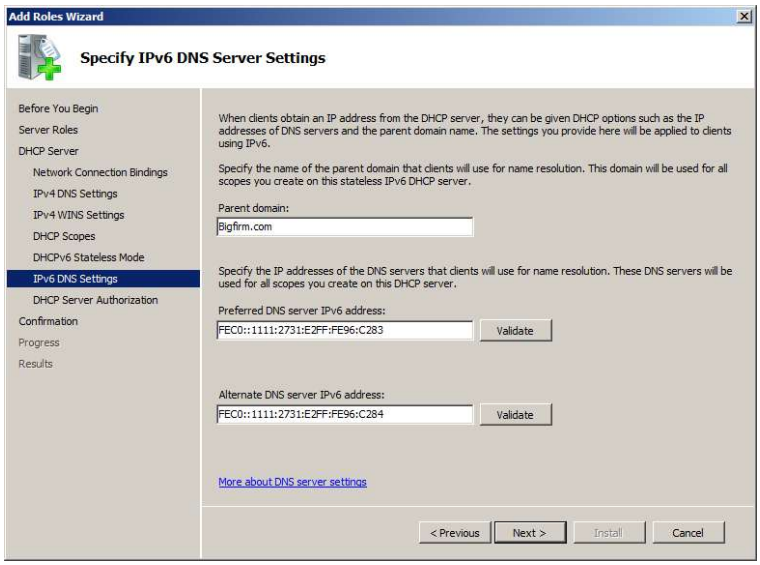
شکل ۵-۶

۹. در صفحه"Configure DHCPv6 Stateless Mode " می‌توانید تعیین کنید که امکان استفاده از آدرس‌های IPv6 وجود داشته باشد یا خیر. چنانچه قصد استفاده از IPv6 دارید گزینه "Enable DHCPv6 stateless mode" را انتخاب نموده و برروی Next کلیک کنید.



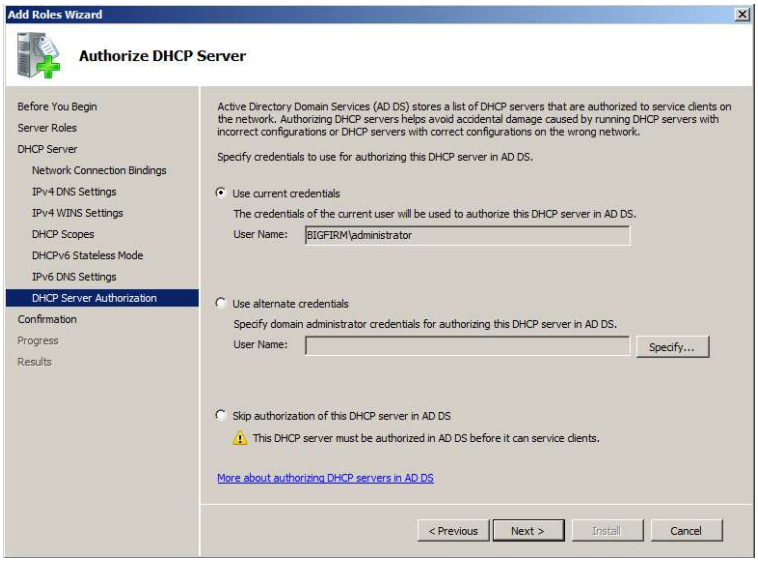
شکل ۵-۷

۱۰. در صفحه "Specify IPv6 DNS Server Settings" تنظیمات مربوط به آدرس IPv6 برای سرور DNS انجام می‌شود. آدرس IPv6 مربوط به سرور DNS را وارد نموده و برروی Next کلیک کنید. (چنانچه آدرس IPv6 برای سرور DNS در اختیار ندارید در مرحله قبل گزینه دوم را انتخاب کنید)



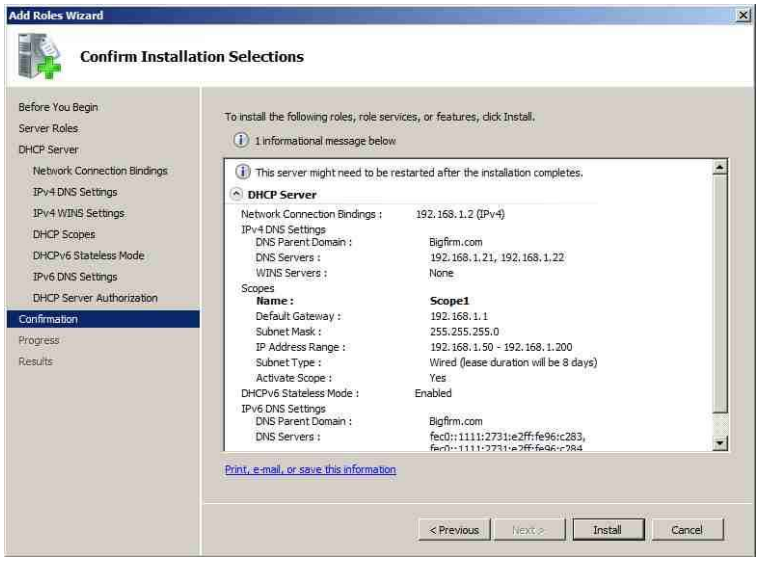
شکل ۵-۸

۱۱. در صفحه "Authorize DHCP Server" باید مدیر سرور را تعیین کنید. گزینه Use Current Credentials را انتخاب نموده و برروی Next کلیک کنید (این گزینه کاربر فعلی که همان مدیر اصلی سرور است را به عنوان مدیر DHCP تعیین می‌کند).



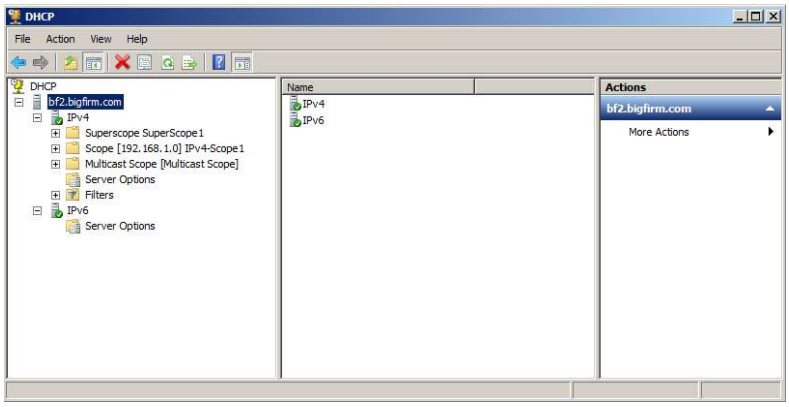
شکل ۵-۹

۱۲. در صفحه "Confirm Installation Selections" خلاصه‌ای از تنظیمات نشان داده می‌شود. پس از مشاهده این تنظیمات برروی Install کلیک نموده و منتظر بمانید تا عملیات نصب به پایان برسد.



شکل ۵-۱۰

۱۳. پس از اتمام مراحل نصب، می‌توانید از مسیر Start « Administrative Tools « DHCP به کنسول مدیریت DHCP دسترسی پیدا کنید.



شکل ۵-۱۱

همانطور که در شکل ۵-۱۱ مشاهده می‌کنید، در پنل سمت چپ به ازای هر سرور DHCP دو قسمت IPv4 و IPv6 وجود دارد. با کلیک برروی علامت "+" در هر قسمت، گزینه‌هایی جهت ایجاد و مدیریت Scopeها وجود دارد. کلیه مفاهیمی که در ابتدای فصل معرفی کردیم، از این قسمت قابل دسترسی می‌باشند. در قسمت‌های بعد این موارد را مورد بررسی قرار خواهیم داد.

۵-۵-۱ DHCP Authorizing برای اکتیو دایرکتوری

DHCP Authorizing (تصویب DHCP) باعث می‌شود که این سرور در فهرست سرورهای مجاز در اکتیو دایرکتوری قرار گیرد و به کمک آن بتوانید شبکه را از دسترسی سرورهای بدون مجوز حفظ کنید. سرورهای بدون مجوز معمولاً دو مشکل در روند کار DHCP ایجاد می‌کنند: اول اینکه Leaseهای جعلی ایجاد نموده و آنرا به داخل شبکه می‌فرستند بنابراین ترافیک شبکه را افزایش می‌دهند. دوم اینکه ممکن است درخواست تمدید Lease که از طرف کاربران مجاز صادر می‌شود را باطل جلوه داده و آنها را رد کنند.

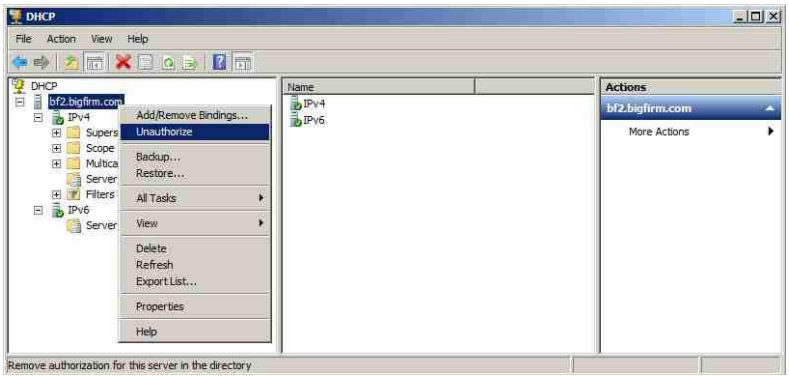
DHCP تا زمانی که برای اکتیو دایرکتوری مجاز نشده باشد نمی‌تواند به کاربران سرویس‌دهی کند. به عبارت دیگر، آدرس IP سرور DHCP باید در فهرست آدرس اشیاء مجاز در اکتیو دایرکتوری قرار داشته باشد. قبل از اینکه سرویس DHCP اجرا شود آدرس خود را در فهرست IPهای مجاز در اکتیو دایرکتوری جستجو می‌کند، در صورتی که آدرس را پیدا نکند اجرای آن با شکست مواجه خواهد شد.

تصویب یا عدم تصویب DHCP در اکتیو دایرکتوری به سادگی و با چند کلیک امکان‌پذیر می‌باشد. ابتدا با فرض اینکه سرور برای اکتیو دایرکتوری مجاز است، آنرا به حالت غیرمجاز انتقال می‌دهیم.

مراحل زیر را دنبال کنید:

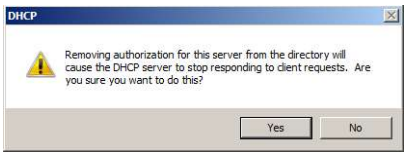
۱. از مسیر Start » Administrative Tools » DHCP، کنسول مدیریت DHCP را اجرا کنید.

۲. برروی نام سرور کلیک‌راست نموده و گزینه Unauthorize را انتخاب کنید.



شکل ۵-۱۲

۳. هشداری مبنی‌بر متوقف شدن پاسخگویی به درخواست‌های کاربران ظاهر می‌شود. بـرروی Yes کلیک کنید.



شکل ۵-۱۳

٤. کمی منتظر بمانید تا عملیات انجام شود. جهت اطمینان از اجرای صحیح عملیات بار دیگر بـرروی نام سرور کلیک‌راست کنید. این بار باید بجای گزینه Unauthorize، گزینه authorize ظاهر شود.

٥. جهت Authorizing سرور نیز کافی است برروی نام سرور کلیک‌راست نموده و گزینه authorize را انتخاب کنید.

۵-۶ ایجاد و مدیریت Scopeها در DHCP

همانطور که قبلاً اشاره کردیم، Scope محدوده‌ای از آدرس‌های IP اسـت کـه بـرای سـرور DHCP تعریف می‌شود. در یک شـبکه مـی‌تـوان چنـدین سـرور DHCP قـرار داده و بـرای هـر کـدام از آنهـا Scopeهایی با تنظیمات و اطلاعات متفاوت ایجاد نمود. با این کار می‌تـوان شـبکه را طـوری پیکربنـدی کرد که کاربران بتوانند از سرورها و تجهیزات جداگانه‌ای استفاده کنند.

اقدامات مدیریتی زیر برروی Scopeها قابل انجام است:

- ایجاد Scope
- پیکربندی مشخصات Scope
- پیکربندی Reservations و Exclusions
- تنظیم Scope options
- فعال و غیرفعال کردن Scope
- ایجاد Superscope
- ایجاد Multicast Scope (Scopeهای چندپخشی)
- یکپارچه سازی Dynamic DNS با DHCP

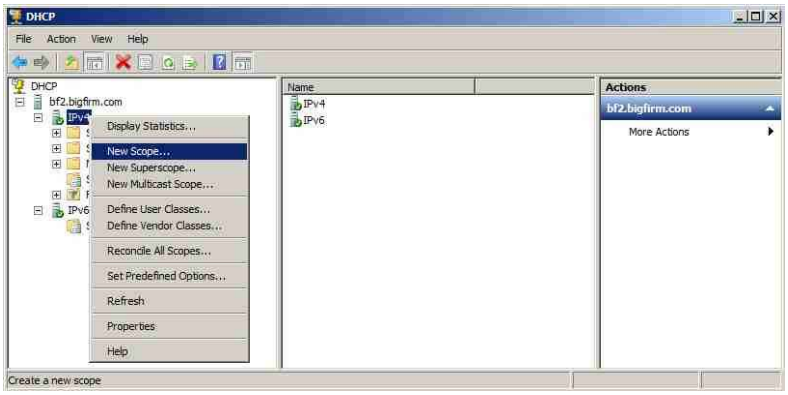
۵-۶-۱ ایجاد Scope در IPv4

ایجاد Scope با استفاده از ویزاردی به نام "New Scope Wizard" انجام می‌شود. اگرچه ممکن است در هنگام نصب DHCP یک Scope نیز ایجاد کرده باشید، اما گاهی اوقات داشتن یک Scope پاسخگو به نیازهای کاربران نخواهد بود. بنابراین لازم است که با توجه به شرایط بتوان Scopeهای جدیدی برروی سرور ایجاد نمود. قبل از شروع کار، داشتن اطلاعاتی اضافی راجع به Scope می‌تواند کار را برایتان ساده‌تر کند. این اطلاعات عبارتند از:

- آدرس‌هایی که از لیست Address Pool مستثنی می‌کنید.
- آدرس‌هایی که برای اهداف خاصی رزرو می‌کنید.
- مقادیری که باید به همراه Scope تنظیم کنید، مثل آدرس DNS، Default Gateway و ...

در اختیار داشتن این آیتم‌ها برای ایجاد Scope ضروری نیست ولی با داشتن آنها می‌توان یک Scope کامل و کارآمد ایجاد نمود. جهت ایجاد Scope مراحل زیر را دنبال کنید:

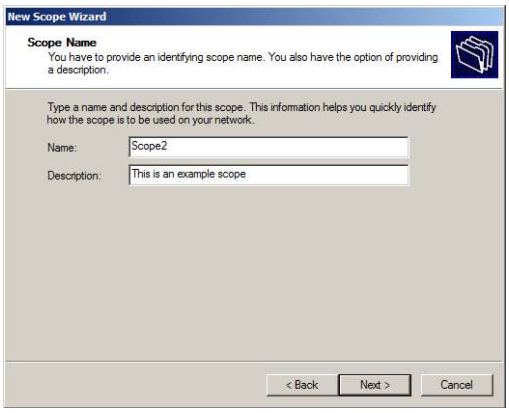
۱. در زیر نام سرور برروی IPv4 کلیک‌راست نموده و گزینه New Scope را انتخاب کنید.



شکل ۵-۱۴

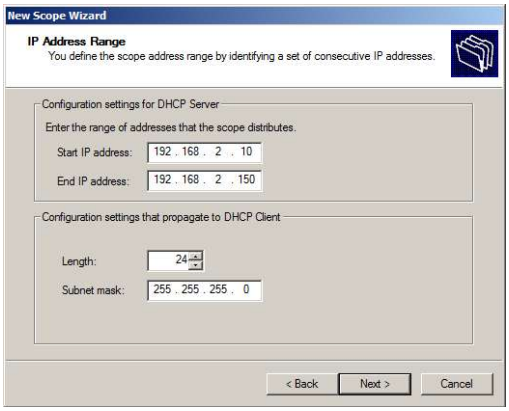
۲. در صفحه "Welcom to the New Scope Wizard" برروی Next کلیک کنید.

۳. در صفحه "Scope Name"، نام Scope و توضیحی مختصر پیرامون آن وارد کنید.



شکل ۵-۱۵

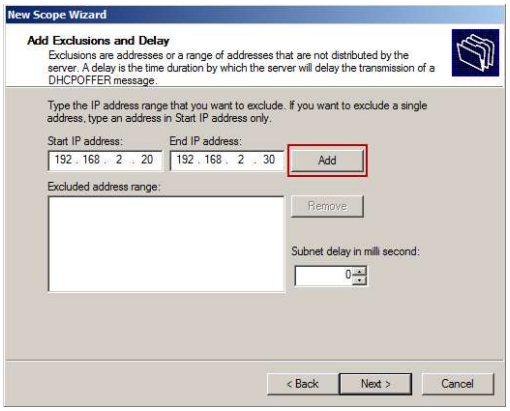
٤. در صفحه "IP Address Range"، آدرس شروع و پایان Scope را وارد کنید. پس از وارد کردن آدرس‌ها، Subnet mask بطور خودکار محاسبه می‌شود. برای تغییر آن می‌توانید از قسمت Length تعداد بیت‌های آنرا تغییر داده تا mask مورد نظر ایجاد شود (جهت کسب اطلاعات بیشتر در مورد محاسبه Subnet nmask به فصل اول مراجعه کنید).



شکل ۵-۱۶

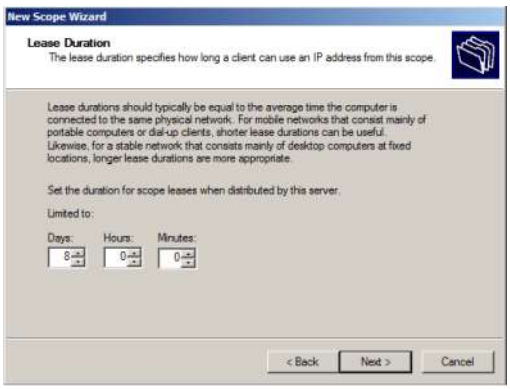
۵. در صفحه "Add Exclusions and Delay" می‌توانید از بین آدرس‌هایی که در مرحله قبل تعریف کرده‌اید، محدوده‌هایی را مستثنی نموده تا (با استفاده از سرویس DHCP) به کاربران و سرورها اختصاص داده نشوند. پس از وارد کردن آدرس شروع و پایان این محدوده‌ها، برروی Add کلیک

کنید تا به فهرست اضافه شوند. در این صفحه علاوه بر تعیین این محدوده‌ها می‌توانید مدت زمان تأخیر برای ارسال پیغام‌های DHCPOFFER به زیرشبکه را مشخص کنید. پس از انجام تنظیمات برروی Next کلیک کنید.



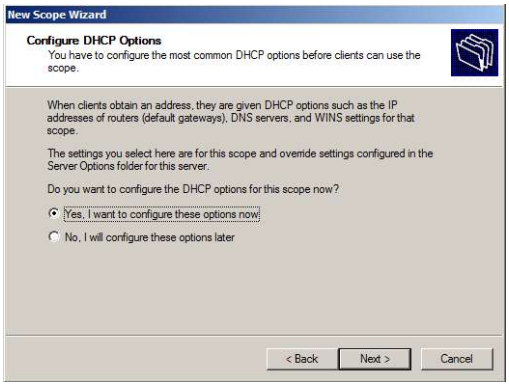
شکل ۵-۱۷

۶. در صفحه "Lease Duration" می‌توانید مدت زمان Lease (اجاره) را مشخص کنید. این زمان تعیین می‌کند که یک کاربر تا چه مدتی می‌تواند از آدرس IP استفاده کند. مقدار پیش‌فرض این زمان هشت روز است و می‌توانید آنرا برحسب روز، ساعت و دقیقه تنظیم کنید.



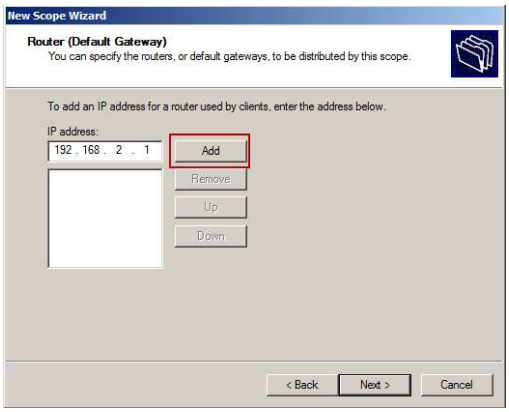
شکل ۵-۱۸

۷. در صفحه "Configure DHCP Options" جهت انجام پیکربندی DHCP Optionها در ادامه مراحل این ویزارد، گزینه اول (Yes, I want to configure this option now) را انتخاب نموده و برروی Next کلیک کنید (با انتخاب گزینه دوم این تنظیمات را بعد از ایجاد Scope می‌توانید انجام دهید).



شکل ۵-۱۹

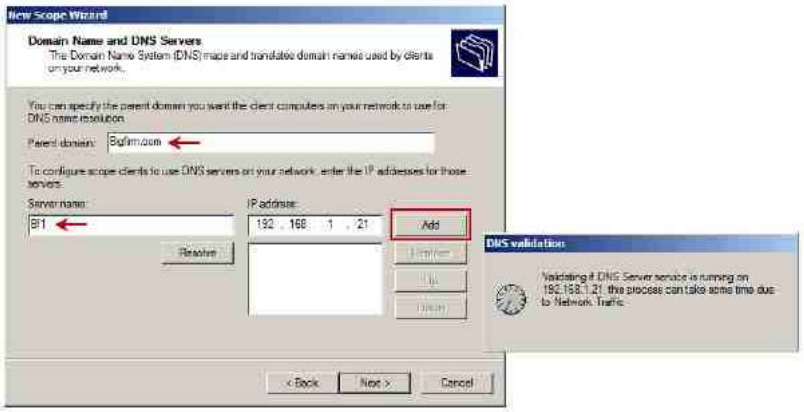
۸. در صفحه Router (Default Gateway)، آدرس Router یا Default Gateway هایی که در این Scope مورد استفاده قرار می‌گیرند را وارد کنید. پس از وارد کردن آدرس برروی Add کلیک کنید تا به فهرست اضافه شود. با استفاده از دکمه‌های Up و Down نیز می‌توانید ترتیب و اولویت آنها را تعیین کنید. پس از انجام عملیات برروی Next کلیک کنید.



شکل ۵-۲۰

۹. در صفحه "Domain Name and DNS Servers" باید تنظیمات مربوط به نام دامنه و سرور DNS را انجام دهید. در قسمت Parent domain نام دامنه‌ای که کاربران از سرور DNS آن استفاده می‌کنند (در اینجا Bigfirm.com) را وارد کنید. در قسمت Server name و IP address نیز نام و آدرس IP سرور DNS را وارد نموده و برروی Add کلیک کنید. پس از کلیک برروی Add، سرور اعتبارسنجی شده و درصورت وجود به فهرست اضافه می‌گردد. چنانچه سروری با آن آدرس وجود نداشته باشد، پیغامی ظاهر شده و اعلام می‌کند که سرور وجود ندارد. با کلیک برروی Yes

می‌توانید آنرا به فهرست اضافه کنید. پس از انجام تنظیمات برروی Next کلیک کنید.



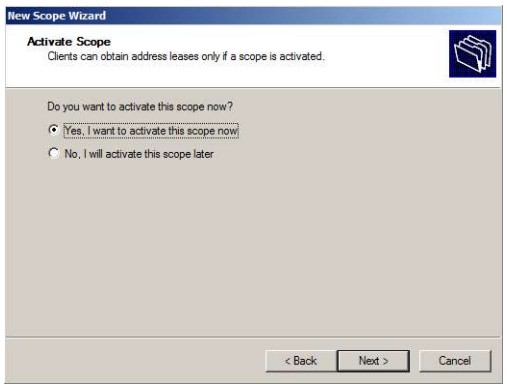
شکل ۵-۲۱

۱۰. چنانچه در شبکه از سرور WINS استفاده می‌کنید، در صفحه "WINS Servers" نام و آدرس IP آنرا وارد نموده و برروی Add کلیک کنید (چنانچه چنین سروری ندارید برروی Next کلیک کنید).

شکل ۵-۲۲

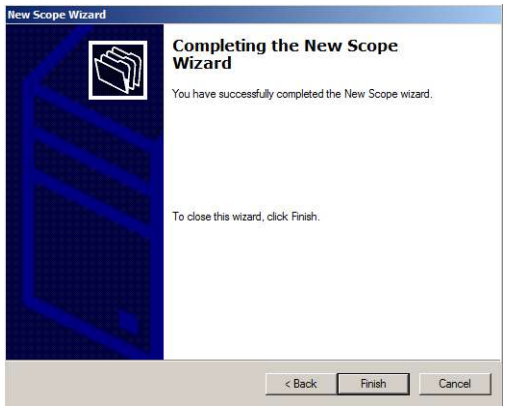
سرویس WINS (Windows Internet Name Service)، یک سرویس مبتنی بر پروتکل NetBIOS است که در ویندوزهای قبل از 2000 به کار گرفته می‌شود و تقریباً دارای عملکردی مشابه با DNS می‌باشد. در شبکه‌های مبتنی بر DNS، نام کامپیوترها در یک دامنه باید منحصر بفرد باشد ولی در کل شبکه می‌توان دو کامپیوتر با نام یکسان در اختیار داشت. به عنوان مثال، نام Ec1 می‌تواند در دو دامنه Bigfirm.com و Littlefirm.com یکسان باشد در حالی که در سرویس WINS تنها یک کاربر با نام Ec1 می‌تواند وجود داشته باشد. این سرویس برای شبکه‌های کوچک ممکن است مناسب باشد اما در شبکه‌های بزرگ و مخصوصاً اینترنت، استفاده از آن پیشنهاد نمی‌گردد.

۱۱. پس از پایان تنظیمات، در صفحه Active Scopes می‌توانید فعال یا غیرفعال بودن Scope را تعیین نمایید. گزینه اول را انتخاب نموده و برروی Next کلیک کنید.



شکل ۵-۲۳

۱۲. در صفحه "Completing the New Scope Wizard" برروی Finish کلیک کنید.

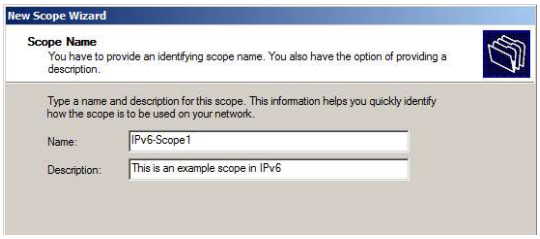


شکل ۵-۲۴

۵-۶-۲ ایجاد Scope در IPv6

اکنون که با نحوه ایجاد Scope در IPv4 آشنا شدید، قصد داریم نحوه ایجاد آنرا در IPv6 نشان دهیم. جهت ایجاد Scope مراحل زیر را دنبال کنید:

۱. در زیر نام سرور برروی IPv6 کلیک‌راست نموده و گزینه New Scope را انتخاب کنید.
۲. در صفحه "Welcom to the New Scope Wizard" برروی Next کلیک کنید.
۳. در صفحه "Scope Name"، نام Scope و توضیحی مختصر پیرامون آن وارد نموده و برروی Next کلیک کنید.

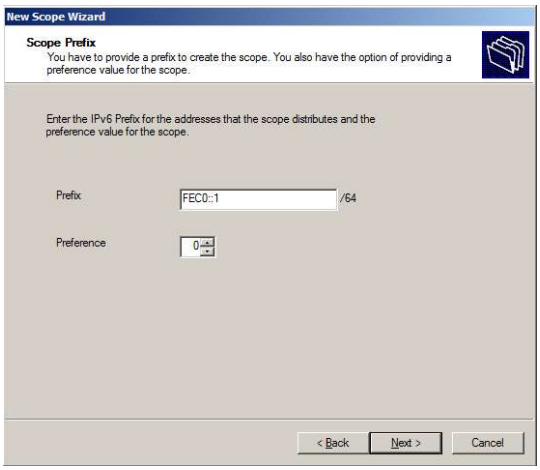


شکل ۵-۲۵

٤. در صفحه "Scope Prefix" باید پیشوند آدرس‌های IPv6 را وارد کنید. در فصل اول گفتیم که آدرس‌های IPv6 به چند نوع تقسیم شده و هر نوع با پیشوند خاصی شروع می‌شود. تعدادی از این پیشوندها عبارتند از:

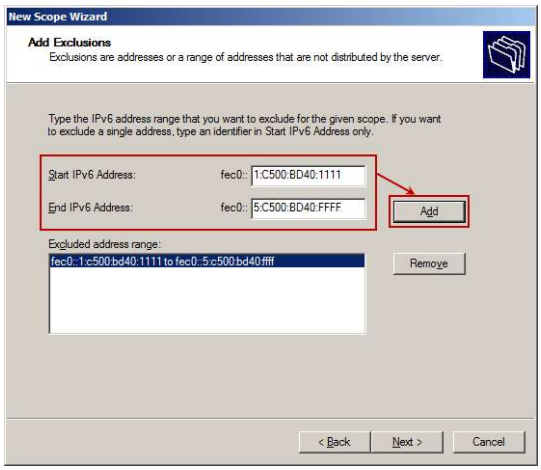
- 2000::/3 برای آدرس‌های global unicast (قابل استفاده در اینترنت)
- FE80::/64 برای آدرس‌های Link-local unicast (استفاده در ارتباطات نقطه به نقطه)
- FEC0::/64 برای آدرس‌های Site-local unicast (قابل استفاده در محدوده یک سایت-معادل با آدرس‌های خصوصی در IPv4)
- FF00 تا FFFF برای آدرس‌های Multicast (استفاده در چندپخشی)

در اینجا از پیشوند FEC0::1 یا FEC0:0:0:1 استفاده شده است (چون آدرس‌های IPv6 از هشت قسمت ١٦ بیتی تشکیل شده‌اند و در این پیشوند چهار قسمت مقداردهی شده است، چهار قسمت بعدی برای تعیین آدرس‌های ماشین‌ها تغییر می‌کند). دقت داشته باشید که از قسمت Preference نیز می‌توانید اولویت این Scope را تعیین کنید.



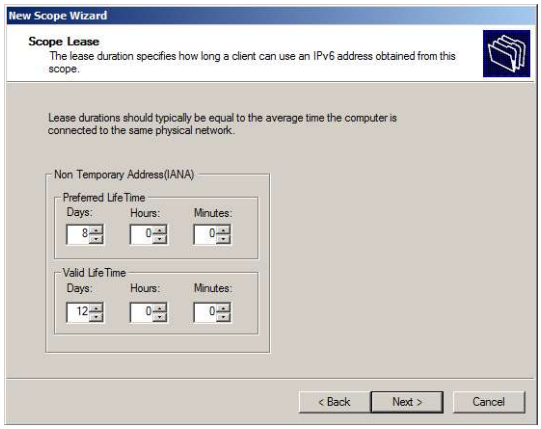
شکل ۵-۲۶

۵. در صفحه "Add Exclusions" می‌توانید محدوده‌ای از آدرس‌های IP را که نمی‌خواهید در سرویس DHCP استفاده شود، تعیین نمایید. آدرس شروع (در اینجا FEC0::1:C500:BD40:1111) و پایان (در اینجا FEC0::1:C500:BD40:FFFF) را وارد نموده و برروی Add کلیک کنید تا به فهرست اضافه شوند. پس از آن برروی Next کلیک کنید (دقت داشته باشید که در شکل ۵-۲۷ سه قسمت اول آدرس‌ها _FEC0::_ بطور پیش‌فرض در نظر گرفته شده‌اند و شما باید قسمت‌های بعدی را وارد کنید)



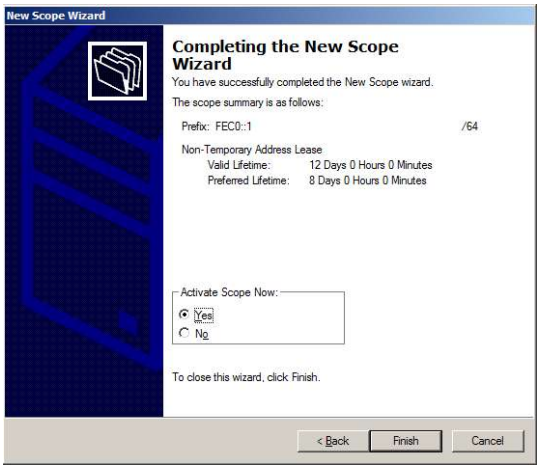
شکل ۵-۲۷

۶. در صفحه "Scope Lease" باید مدت زمان Lease (مدت زمان استفاده از آدرس IP توسط ماشین‌ها) را تعیین کنید. تنظیمات لازم را انجام داده و برروی Next کلیک کنید.



شکل ۵-۲۸

۷. در صفحه "Completing the New Scope Wizard" پس از مشاهده خلاصه‌ای از تنظیمات می‌توانید فعال یا غیرفعال بودن Scope را تعیین کنید. در قسمت Active Scope Now گزینه Yes را انتخاب نموده و برروی Finish کلیک کنید.



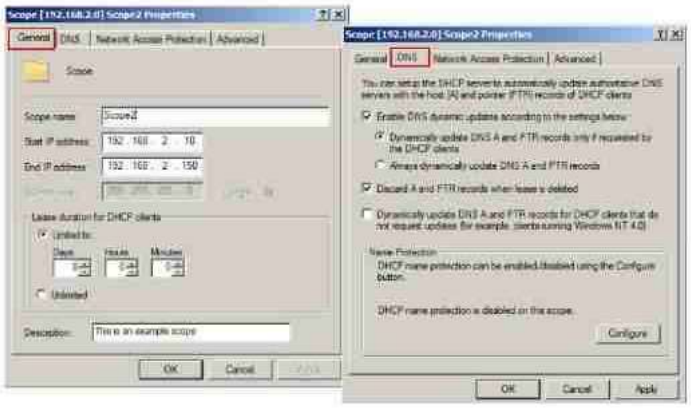
شکل ۵-۲۹

۵-۶-۳ تغییر مشخصات Scopeها

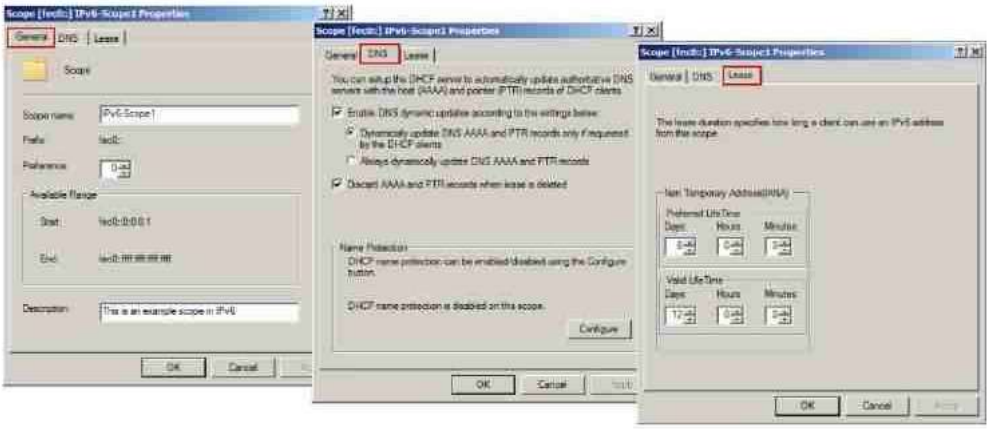
هر Scope شامل مجموعه‌ای از مشخصات است که با آن همراه شده‌اند. جهت دسترسی به مشخصات هر Scope می‌توانید برروی نام آن کلیک راست نموده و Properties را انتخاب کنید. پنجره Scope Properties (بسته به نوع Scope) شامل تب‌هایی مانند General، DNS، Lease است که با استفاده از آنها می‌توانید تنظیمات Scopeها را تغییر دهید. تعدادی از مهمترین این تنظیمات در ادامه معرفی شده است:

- Scope name: نام Scope را مشخص می‌کند.
- Start IP Address و End IP Address: آدرس‌های شروع و پایان Scope هستند که در حین ایجاد Scope آنها را تعیین کرده‌اید. می‌توانید ادرس‌های جدیدی در این فیلدها وارد نموده و محدوده آدرس‌ها را تغییر دهید.
- Lease duration for DHCP client: در Scopeهای IPv4، تنظیمات این قسمت مشخص می‌کنند که یک Lease چه مدت دارای ارزش می‌باشد. در Scopeهای IPv6 تب جداگانه‌ای جهت انجام تنظیمات Lease وجود دارد.
- Enable DNS dynamic update: با استفاده از این گزینه و آپشن‌های آن امکان انجام تنظیماتی پیرامون فعال‌سازی Dynamic DNS و رکوردهای Host و PTR فراهم گردیده است.

در شکل‌های ۵-۳۰ و ۵-۳۱ پنجره Scope Properties برای IPv4 و IPv6 نشان داده شده است.



شکل ۵-۳۰: IPv4 Scope Properties



شکل ۵-۳۱: IPv6 Scope Properties

زمانی‌که مشخصات یک Scope را تغییر می‌دهید، این تغییرات برروی Lease که در حال اجرا می‌باشد تاثیری نمی‌گذارد. به عنوان مثال فرض کنید که یک Scope از آدرس 172.30.1.1 تا آدرس 172.30.1.199 در اختیار دارید و کاربران در حال استفاده از آن هستند. پس از انجام تغییرات، محدوده آدرس‌های این Scope را به 172.30.1.1 تا 172.30.1.150 تغییر می‌دهید. حال اگر کاربری از آدرس 172.30.1.180 که جزئی از Scope، قبل از تغییر می‌باشد استفاده کند، کاربر این آدرس را تا زمانی که اعتبار Lease به پایان نرسیده باشد استفاده خواهد کرد ولی قادر به تمدید آن نمی‌باشد.

۵-۷ مدیریت Reservation و Exclusion

پس از تعریف Address Pool برای Scope، ممکن است نیاز به ایجاد آدرس‌های Reservation (رزرو) و Exclusion (مثتثنی) داشته باشید. درنظر گرفتن این آدرس‌ها موجب کاهش تعداد کل آدرس‌های مورد استفاده توسط سرویس DHCP می‌گردد. در ادامه، نحوه افزودن و یا حذف‌کردن آدرس‌های Reservation و Exclusion را شرح خواهیم داد.

۵-۷-۱ افزودن و حذف‌کردن Exclusions

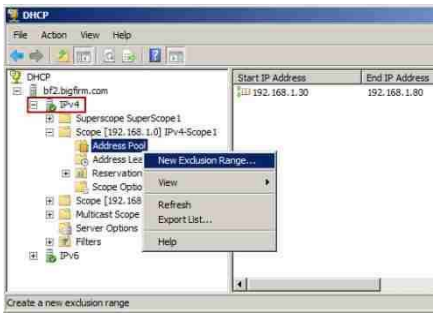
زمانی که قصد دارید محدوده‌ای از آدرس‌ها را از سرویس DHCP حذف کنید، باید آنها را به لیست آدرس‌های Exclusion اضافه کنید. بهتر است این کار قبل از فعال‌کردن یک Scope انجام شود مانع از اختصاص این آدرس‌ها به کاربران شده و بنابراین در زمان تمدید Lease با مشکلی مواجه نخواهند بود.

افزودن Exclusions

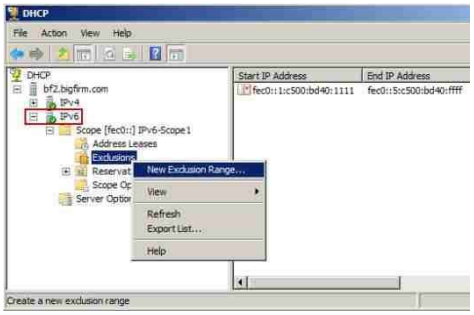
جهت افزودن آدرس‌ها به لیست Exclusions مراحل زیر را دنبال کنید:

۱. در کنسول مدیریت DHCP، نوع Scope مورد نظر جهت تعیین Exclusions را انتخاب کنید (IPv4 یا IPv6).

۲. برای Scopeهای IPv4، برروی Address Pool کلیک‌راست نموده و گزینه New Exclusion Range را انتخاب کنید. برای IPv6 این گزینه با کلیک‌راست برروی Exclusions قابل دسترسی می‌باشد.



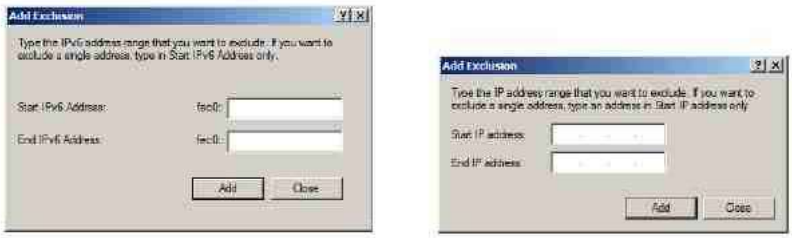
IPv4



IPv6

شکل ۵-۳۲

۳. با مشاهده پنجره "Add Exclusion"، آدرس‌های شروع و پایان Exclusion را وارد نموده و برروی Add کلیک کنید.



IPv6 IPv4

شکل ۵-۳۳

٤. پس از اتمام کار می‌توانید با کلیک برروی قسمت Exclusion در IPv4 یا IPv6، این آدرس‌ها را مشاهده کنید.

حذف Exclusions

جهت حذف یک Exclusion کافی است برروی آن کلیک‌راست نموده و Delete را انتخاب کنید. پس از حذف، آدرس‌هایی که در این دامنه قرار دارند بلافاصله به آدرس‌های قابل دسترسی افزوده می‌شوند.

۵-۷-۲ افزودن و حذف کردن Reservation

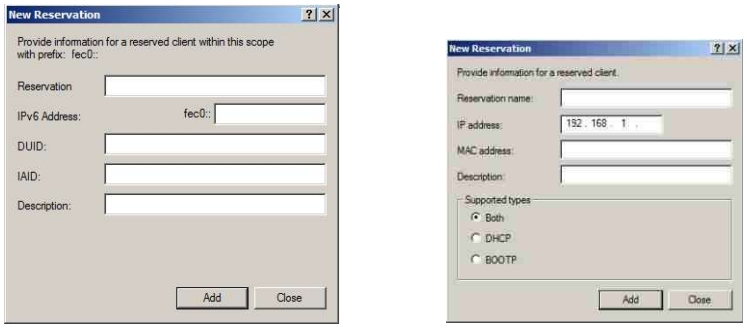
زمانی که قصد دارید یک دستگاه همیشه از آدرس IP یکسانی استفاده کند می‌توانید آنرا به فهرست Reservation اضافه کنید. این روش جهت سهولت دسترسی به ماشین‌های پرکاربرد و مهم در شبکه استفاده شده و بیشتر جهت اختصاص آدرس IP به دستگاه‌هایی مانند سرورها، پرینتر و ... به کار می‌رود.

افزودن Reservation

اضافه کردن Reservation بسیار ساده است. کافی است آدرس سخت افزار یک دستگاه (MAC Address) و یا شناسه آن را در اختیار داشته و مطابق مراحل زیر اقدام کنید:

۱. Scope مورد نظر را انتخاب کنید.
۲. برروی Reservations کلیک‌راست نموده و گزینه NewReservation را انتخاب کنید.
۳. در پنجره "New Reservation" آدرس سخت افزار (MAC) یا شناسه آنرا به همراه آدرس IP که قصد دارید به آن اختصاص دهید وارد کنید (شکل ٥-٣٤).

برای پیدا کردن آدرس MAC می‌توانید از دستور `ipconfig` در خط فرمان استفاده کنید. چنانچه قصد دارید آدرس MAC را برای یک ماشین Remote (راه دور) پیدا کنید، می‌توانید از دستور `nbtstat -a computername` استفاده کنید (بجای computername نام ماشین مورد نظر را وارد نمایید).



IPv6 IPv4

شکل ۵-۳۴

٤. در صورت تمایل می‌توانید نام و توضیحی نیز راجع به Reservations وارد کنید.

٥. برای IPv4 می‌توانید از قسمت Supported Types تعیین‌کنید که انجام رزرو برای DHCP، BOOTP (قابل استفاده برای دستگاه‌های Remote) و یا هر دو باشد.

حذف Reservation

جهت **حذف** یک Reservation کافی است برروی آن کلیک‌راست نموده و گزینه Delete را انتخاب کنید. دقت داشته باشید که حذف Reservation تاثیری بر ماشین کاربر نخواهد داشت.

۵-۸ تنظیمات Scope Options برای IPv4

پس از راه اندازی سرور DHCP، تصویب[1] آن در اکتیو دایرکتوری، و ایجاد Scope، نوبت به انجام تنظیمات Scope Options می‌رسد. تنظیمات مربوط به Optionها، امکاناتی جهت دسترسی کاربران به یکدیگر و یا به سرورها فراهم می‌کنند. این تنظیمات شامل مواردی مانند تنظیم Default Gateway، DNS و ... می‌باشند. تنظیمات Scope Option باید قبل از فعال‌سازی یک Scope پیکربندی شوند زیرا ثبت کاربران در Scope بدون استفاده از این Optionها عملاً کاری بی‌فایده می‌باشد. Scope Options به همراه آدرس IP و قاب زیرشبکه که در قسمت‌های قبل پیکربندی نمودید، تنظیمات TCP/IP را برای کاربران تکمیل خواهند نمود. در ادامه نحوه پیکربندی Optionها برروی سرور DHCP را شرح خواهیم داد.

۵-۸-۱ آشنایی با سطوح تخصیص Optionها

Optionهای DHCP در پنج سطح قابل اختصاص به میزبان‌های شبکه می‌باشند:

1. Authorizing

Predefined Options

Predefined Options، الگوهایی[1] هستند که بطور پیش‌فرض در پنجره‌های مربوط به Optionهای Scope، Server و Client تنظیم شده‌اند.

Server Options

این Optionها به کلیه Scopeها و کاربران یک سرور اختصاص داده می‌شوند. این بدان معناست که بهترین روش برای اختصاص یک Option به همه کاربران (یک سرور)، بدون توجه به Scopeها استفاده از تنظیمات سطح سرور می‌باشد.

Scope Options

اگر قصد دارید Optionهایی را به کاربران یک زیرشبکه اختصاص دهید، بهترین گزینه استفاده از تنظیمات سطح Scope می‌باشد. به عنوان مثال یکی از کارهای رایج در شبکه‌ها این است که تعدادی مسیریاب را برای زیرشبکه‌های فیزیکی متفاوت مشخص می‌کنند. حال اگر شما به ازای یک زیرشبکه دو Scope داشته باشید می‌توانید به هرکدام از Scopeها آدرس یکی از مسیریاب‌ها را اختصاص دهید، بنابراین کاربران زیرشبکه می‌توانند از هر دو مسیریاب استفاده کنند.

Class Options

Optionهای سطح Class می‌توانند به کاربران متفاوتی در شبکه اختصاص داده شوند. همیشه کاربران شبکه از سیستم‌های مشابهی استفاده نمی‌کنند، به عنوان مثال ممکن است کاربران از ویندوزهای 2000، XP، Vista، Server 2003، Server 2008 و 2008R2 استفاده نمایند که Optionهای تحت پوشش این سیستم‌عامل‌ها (در DHCP)، برای سیستم‌عامل‌های Windows98، Windows NT و Mac OS ناشناخته هستند(و برعکس). با تعریف کلاس‌های نوع Windows 2000 یا Windows 98 می‌توانید این Optionها را دسته‌بندی نموده و با توجه به نوع کاربران به آنها اختصاص دهید.

Client Options

این optionها می‌توانند در سطح کاربر اختصاص داده شوند. به عنوان مثال زمانی که کاربران از آدرس‌های رزرو شده استفاده می‌کنند، می‌توانید Optionهایی را به این آدرس‌ها پیوست نموده و به کاربران اختصاص دهید. تنظیمات سطح کاربر، کلیه تنظیمات سطح Server، Class و Scope را لغو می‌کنند.

Optionهای سطح پایین (مثل سطح کاربر) می‌توانند Optionهای سطوح بالاتر را لغو کنند. به عبارت دیگر اگر کاربران را با استفاده از Optionهای سطوح بالا تنظیم نموده، سپس برروی تعدادی از آنها Optionهای سطح پایین را پیکربندی کنید، تنظیمات قبلی لغو خواهند شد. ترتیب لغو شدن Optionها بصورت روبرو می‌باشد: Client Options « Class Options « Scope Options « Server Options

1. Templates

۵-۸-۲ اختصاص Optionها

با استفاده از کنسول مدیریت DHCP می‌توانید Optionها را به Scope، سرور، آدرس‌های رزرو شده و یا کلاس‌ها اختصاص دهید. روش انجام کار در همه سطوح یکسان است و تنها تفاوت آن در محلی است که Option اختصاص داده می‌شود.

زمانی که یک Option را اختصاص می‌دهید بخاطر داشته باشید که این Option به همه کاربران در آن سرور یا Scope اختصاص داده می‌شود. این Optionها قابل انتقال از یک Scope و یا سرور به دیگری نمی‌باشند.

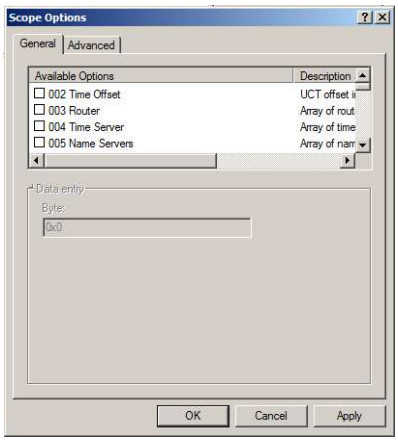
ایجاد و اختصاص یک Option جدید

جهت ایجاد و اختصاص یک Option مراحل زیر را دنبال کنید:

۱. ابتدا سطح اختصاص Option را تعیین کنید:

- جهت اختصاص Option به سرور، برروی آن کلیک کنید تا زیرشاخه‌های آن نمایش داده شوند. در فهرست زیرشاخه‌ها، برروی آیتم Server Options کلیک‌راست نموده و گزینه Configure Options را انتخاب کنید.
- جهت اختصاص Option به Scope، برروی آن کلیک نموده و از بین آیتم‌های موجود، Scope Options را انتخاب کنید. برروی Scope Options کلیک‌راست نموده و گزینه Configure Options را انتخاب کنید.
- جهت اختصاص Option به آدرس‌های Reservation نیز برروی Reservation کلیک‌راست نموده گزینه Configure Options را انتخاب کنید.

۲. پس از انتخاب گزینه موردنظر، پنجره Server/Scope/Reservation Options نمایش‌داده می‌شود. در این پنجره تمام Optionهای قابل اختصاص فهرست شده است.



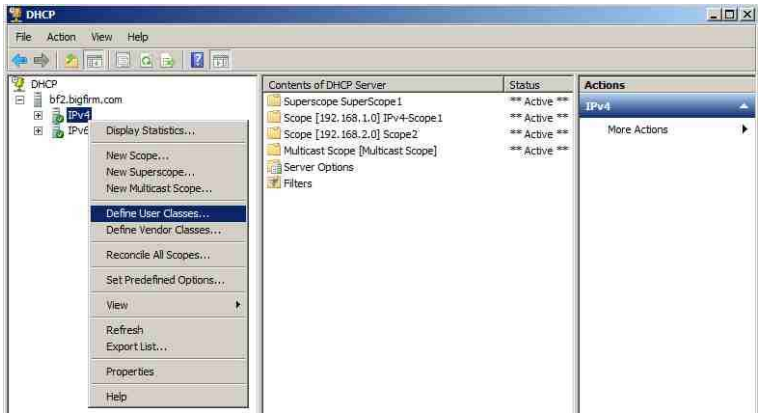
شکل ۵-۳۵

۳. جهت انتخاب یک Option، تیک مربوط به آن را فعال نموده و از قسمت پایین پنجـره (Data Entry) مقادیر مورد نظر را اختصاص دهید. در نهایت برروی OK کلیک کنید.

۵-۸-۳ پیکربندی سرور DHCP برای کلاس‌ها

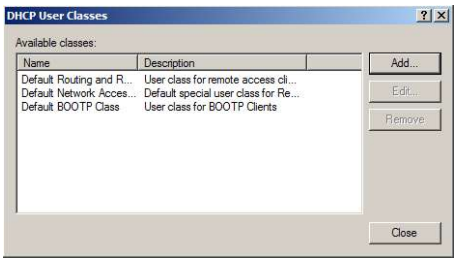
با استفاده از Class، مدیر شبکه می‌تواند کاربران را گروه‌بندی نموده و Optionهـای یکسـانی روی کامپیوترهای هر گروه اعمال کند. در این قسمت قصد داریـم نحـوه ایجـاد کـلاس در سـرور DHCP و همچنین اختصاص Optionها به آنرا شرح دهیم. برای انجام این کار مراحل زیر را دنبال کنید:

۱. از مسیر Start» Administrative Tools» DHCP، کنسول مدیریت DHCP را اجرا کنید.
۲. برروی آیتم IPv4 کلیک‌راست نموده و گزینه Define User Classes را انتخاب کنید.



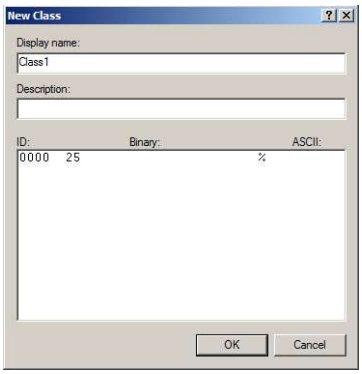
شکل ۵-۳۶

۳. در پنجره "DHCP User Classes"، برروی دکمه Add کلیک کنید.



شکل ۵-۳۷

٤. در پنجره New Class، از قسمت Display Name و ID، نام و شناسه کلاس را وارد نموده و برروی OK کلیک کنید. همچنین می‌توانید از قسمت Description توضیحاتی نیز راجع به آن ارائه دهید.

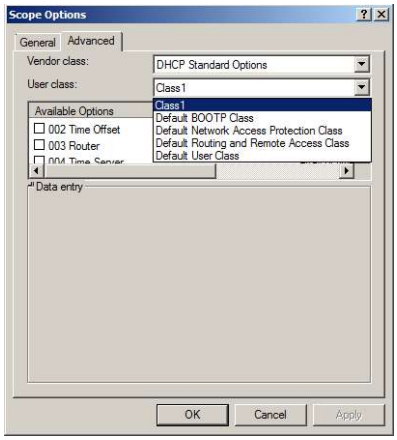


شکل ۵-۳۸

۵. پس از کلیک برروی OK، کلاسی که ایجاد نموده‌اید در پنجره "DHCP User Classes" نشان داده می‌شود. برروی Close کلیک کنید.

۶. در کنسول مدیریت DHCP، برروی Scope Options کلیک‌راست نموده و گزینه Configure Options را انتخاب کنید.

۷. در تب Advanced و از قسمت User Class، کلاسی که تعریف نمودید را انتخاب کنید.



شکل ۵-۳۹

۸. Optionهای مورد نظر را به کلاس اختصاص داده و در نهایت برروی OK کلیک کنید.

جهت اختصاص شناسه کلاس به کاربران می‌توانید از دستور `ipconfig` به همراه پارامتر `/setclassid` استفاده کنید. این دستور به صورت زیر می‌باشد:

```
Ipconfig /setclassid <adapter name> <Class ID>
```

چنانچه برروی یک کامپیوتر از چندین کارت شبکه استفاده می‌کنید، جهت اختصاص ID یکسان به آنها می‌توانید از دستور زیر استفاده کنید:

```
Ipconfig /setclassid * <Class ID>
```

همچنین درصورتی که قصد دارید به کارت‌های شبکه‌ای که نام آنها با عبارت خاصی آغاز می‌شود ID اختصاص دهید، آن عبارت را به همراه یک ستاره (*)، و چنانچه شامل عبارت خاصی می‌باشد آن عبارت را بین دو ستاره به صورت زیر وارد کنید:

```
rem start name with "Local"
Ipconfig /setclassid Local*  <Class ID>

rem name Include "Con"
Ipconfig /setclassid *Con*  <Class ID>
```

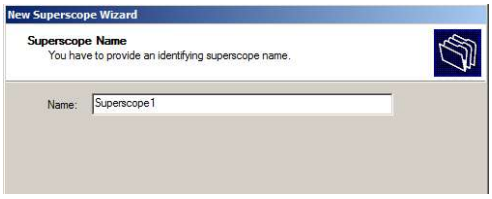
۵-۹ ایجاد و حذف Superscope در IPv4

Superscope، به سرور DHCP اجازه می‌دهد که آدرس‌های چندین زیرشبکه منطقی را در اختیار کاربران یک شبکه فیزیکی قرار دهد. ایجاد Superscope با استفاده از گزینه New Superscope در کنسول مدیریت DHCP انجام می‌شود.

۵-۹-۱ ایجاد یک Superscope

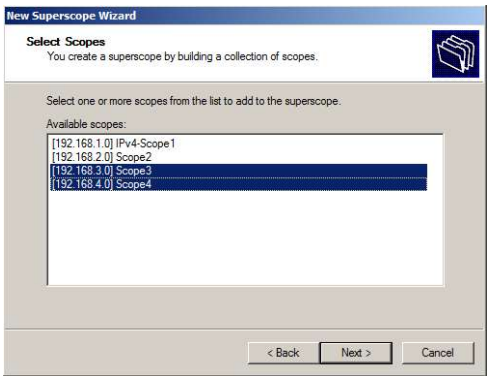
جهت ایجاد Superscope مراحل زیر را دنبال کنید:

۱. کنسول مدیریت DHCP را از مسیر «Start» «Administrative Tools» DHCP اجرا کنید.
۲. با استفاده از گزینه New Scope (قسمت ۵-٦-۱) دو Scope با محدوده‌های 192.168.3.2 تا 192.168.3.127 و 192.168.4.2 تا 192.168.4.127 ایجاد کنید.
۳. برروی IPv4 کلیک‌راست نموده و گزینه New Superscope را انتخاب کنید.
٤. در صفحه "Welcom to the New Superscope Wizard" برروی Next کلیک کنید.
۵. در صفحه "Superscope Name" نام Superscope را وارد نموده و برروی Next کلیک کنید.



شکل ۵-۴۰

۶. در صفحه Select Scopes لیست Scopeهـای موجـود نشـان داده شـده اسـت. دو Scope کـه ایجـاد کردید را انتخاب نموده و برروی Next کلیک کنید.

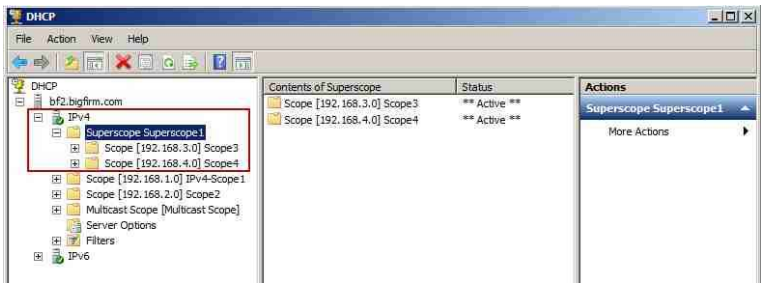


شکل ۵-۴۱

۷. در صفحه "Completing the New Super Scope Wizard" خلاصه ای از تنظیمات انجام شـده نشـان داده می‌شود. برروی Finish کلیک کنید.

شکل ۵-۴۲

۸. در کنسول مدیریت DHCP می‌توانید Superscope که ایجاد نموده‌اید را مشاهده کنید.



شکل ۵-۴۳

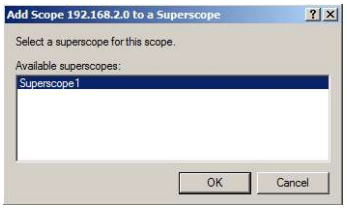
حذف Superscope

جهت حذف یک Superscope، برروی آن کلیک‌راست نموده و گزینه Delete را انتخاب کنید. دقت داشته باشید که حذف یک Superscope تأثیری بر Scopeهای اصلی ندارد.

۵-۹-۲ افزودن Scope به Superscope

جهت افزودن Scope به یک Superscope مراحل زیر را دنبال کنید:

۱. برروی Scope مورد نظر کلیک‌راست نموده و گزینه Add to Superscope را انتخاب کنید.
۲. لیست تمام Superscopeهای شناخته شده برای سرور نشان داده می‌شود. Superscope موردنظر را انتخاب نموده و برروی OK کلیک کنید.



شکل ۵-۴۴

حذف Scope از Superscope

جهت حذف Scope از یک Superscope، در زیرمجموعه Superscope برروی Scope مورد نظر کلیک‌راست نموده و گزینه Remove From Superscope را انتخاب کنید.

۵-۹-۳ فعال و غیرفعال کردن Superscope

جهت فعال‌سازی یا غیرفعال کردن یک Scope و یا Superscope، برروی آن کلیک‌راست نموده و گزینه Active یا Deactive را انتخاب کنید. توجه داشته باشید که با غیرفعال کردن Scope یا Superscope، کاربران Leaseهای فعلی خود را از دست خواهند داد و باید مجدداً درخواست Lease نمایند.

۵-۱۰ ایجاد Scopeهای Multicast برای IPv4

Multicasting (چند پخشی) زمانی اتفاق می‌افتد که یک ماشین بجای برقراری ارتباط با تک تک کامپیوترها در شبکه، با شبکه‌ای از کامپیوترها ارتباط برقرار نماید. این کار بیشتر زمانی مفید است که بخواهید یک ویدئو یا صدا را به تعدادی از کاربران در شبکه ارسال کنید. در ادامه با پروتکلی به نام MADCAP که انجام Multicasting را کنترل می‌کند آشنا خواهید شد و سپس نحوه ایجاد و

پیکربندی یک Scope از نوع Multicast را شرح خواهیم داد.

۵-۱۰-۱ آشنایی با پروتکل MADCAP[1]

سرویس DHCP معمولاً برای اختصاص آدرس‌های IP و سایر اطلاعات پیکربندی در ارتباطات شبکه‌ای تک‌پخشی[2] (یک به یک) استفاده می‌شود. با استفاده از Multicasting چندین نوع فضای آدرس‌دهی جداگانه از آدرس 224.0.0.0 تا 239.255.255.255 وجود دارد. آدرس‌هایی که در این دامنه قرار می‌گیرند، آدرس‌های کلاس D (Class D) یا آدرس‌های Multicast شناخته می‌شوند. کاربران تنها با دانستن و استفاده از این آدرس‌ها می‌توانند (جهت دریافت محتوا) در یک Multicast شرکت کنند، اگرچه به آدرس‌های IP معمولی نیز نیاز دارند.

اما کاربران چگونه می‌توانند از آدرسی که باید استفاده کنند مطلع شوند؟ DHCP در این زمینه کمکی نخواهد کرد زیرا این سرویس جهت اختصاص آدرس‌های IP و سایر اطلاعات به یک کاربر در هر لحظه طراحی شده است. برای تحقق بخشیدن به این موضوع، گروه مهندسین اینترنت (IETF)[3] پروتکلی به نام MADCAP را طراحی کرده‌اند. این پروتکل در کاربردهای Multicast مورد استفاده قرار می‌گیرد و شبیه پروتکل DHCP می‌باشد. با استفاده از این پروتکل، کاربران MADCAP زمانی که قصد مشارکت در یک Multicast داشته باشند می‌توانند Leaseهایی از نوع Multicast را از سرور درخواست نمایند.

DHCP و MADCAP دارای چندین تفاوت مهم هستند: این دو پروتکل کاملاً از یکدیگر جدا هستند. یک سرور می‌تواند به عنوان سرور DHCP یا سرور MADCAP و یا هردو به کار گرفته شود، اما هیچ رابطه ضمنی و یا واقعی میان این دو وجود ندارد. علاوه بر این، کاربران می‌توانند بطور همزمان از DHCP و/یا MADCAP استفاده کنند، کافی است کاربران MADCAP یک آدرس Unicast را از جایی دریافت کنند.

توجه داشته باشید که DHCP می‌تواند طی فرایند Lease، اطلاعات Optionها را به کاربران اختصاص دهد، در حالی که MADCAP قادر به انجام چنین کاری نیست و فقط می‌تواند آدرس‌های Multicast را به صورت پویا به کاربران اختصاص دهد.

۵-۱۰-۲ ایجاد Multicast Scopes

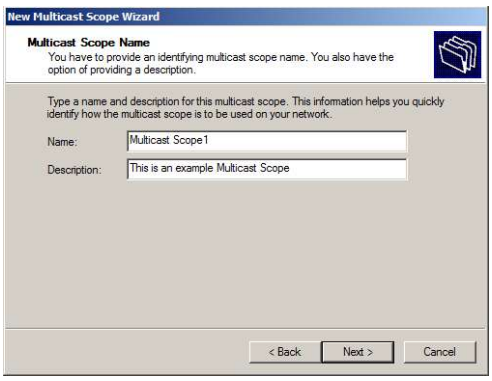
جهت ایجاد Multicast Scopes مراحل زیر را دنبال کنید:

1. Multicast Address Dynamic Client Allocation Protocol
2. Unicast
3. Internet Engineering Task Force

۱. در کنسول مدیریت DHCP برروی IPv4 کلیک‌راست نموده و گزینه New Multicast Scope را انتخاب کنید.

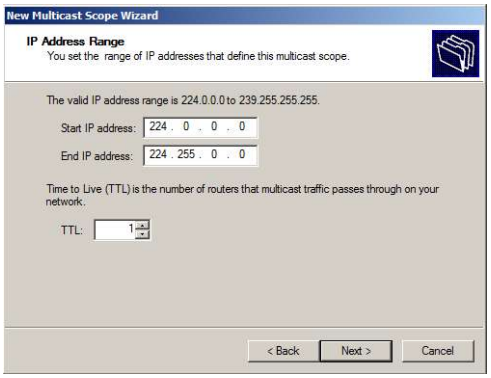
۲. در صفحه "Welcom to the New Multicast Scope Wizard" برروی Next کلیک کنید.

۳. در صفحه "Multicast Scope Name"، نام و توضیحی راجع به Scope وارد نموده و برروی Next کلیک کنید.



شکل ۵-۴۵

٤. صفحه "IP Address Range" نشان داده می‌شود. در قسمت Start IP address، آدرس 224.0.0.0 و در قسمت End IP address آدرس 224.255.0.0 را وارد کنید. در قسمت TTL[1] نیز عدد ۱ را وارد نموده تا مطمئن شوید که هیچ پاکتِ Multicast از شبکه خارج نمی‌گردد (در واقع این عدد تعداد مسیریاب‌هایی که در فرایند Multicast مورد استفاده قرار می‌گیرند را مشخص می‌نماید).



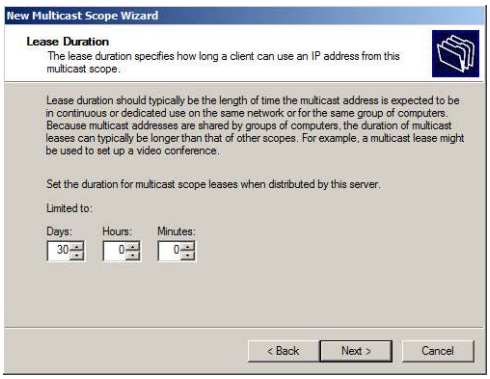
شکل ۵-۴۶

۵. در صفحه "Add Exclusions" می‌توانید محدوده آدرس‌های Exclusions را تعیین نمایید. برروی Next کلیک کنید.

1. Time to Live

شکل ۵-۴۷

٦. در صفحه "Lease Duration" می‌توانید مدت زمان Lease را تعیین کنید. این زمان بطور پیش‌فرض ۳۰ روز می‌باشد. پس از تنظیم مدت زمان، برروی Next کلیک کنید.



شکل ۵-۴۸

۷. در صفحه "Active Multicast Address" می‌توانید فعال یا غیرفعال بودن Scope را تعیین کنید. گزینه No را انتخاب نموده و برروی Next کلیک کنید.

شکل ۵-۴۹

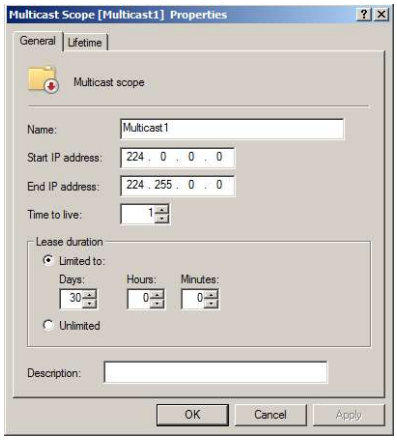
۸. در صفحه "Completing the New Multicast Scope Wizard" برروی Finish کلیک کنید.

۵-۱۰-۳ تنظیم مشخصات Multicast Scopes

همانند سایر Scopeها، می‌توانید مشخصات Scopeهای Multicast را تغییر داده و یا تنظیم نمایید. برای انجام این کار مراحل زیر را دنبال کنید:

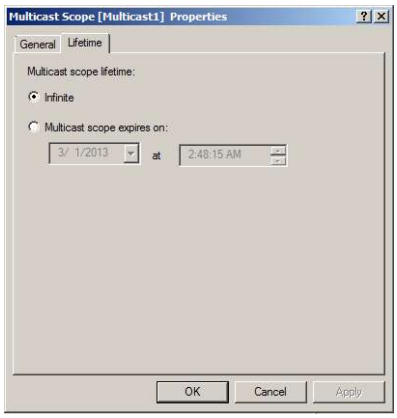
۱. برروی Multicast Scope مورد نظر کلیک‌راست نموده و Properties را انتخاب کنید.

۲. پنجره "Multicast Scope [Scope name] Properties" نشان داده می‌شود. در تب General از این پنجره می‌توانید تنظیماتی مانند نام Scope، آدرس‌های شروع و پایان Scope، مدت زمان عمر بسته‌ها (TTL)، مدت زمان Lease و توضیحاتی راجع به Scope را انجام دهید.



شکل ۵-۵۰

۳. در تب lifetime نیز می‌توانید مدت زمان فعال بودن Scope را تعیین کنید. بطور پیش‌فرض، Scope برای همیشه فعال است اما چون این Scopeها برای رویدادهای خاصی ایجاد می‌شوند می‌توانید مدت زمان فعال بودن آنها را به صورت دلخواه تنظیم کنید. جهت انجام این کار باید گزینه Multicast scope expires on را انتخاب نموده و تاریخ و ساعت غیرفعال شدن آنرا تعیین نمایید.



شکل ۵-۵۱

۵-۱۱ یکپارچه سازی DDNS با DHCP

اطلاعات سرورDNS به دو روش می‌تواند بروز رسانی شود. روش اول زمانی است که کاربران DHCP آدرس خود را به سرورDNS اعلام می‌کنند، و روش دوم زمانی است که سرور DHCP در هنگام ثبت یک کاربر جدید، آدرس آنرا به سرور DNS اعلام می‌کند. هیچکدام از این بروز رسانی‌ها تا وقتی که سرورDNS را برای استفاده از DNS پویا[1] (DDNS) پیکربندی نکنید انجام نخواهد شد.

پیکربندی DDNS در دو سطح قابل انجام است:

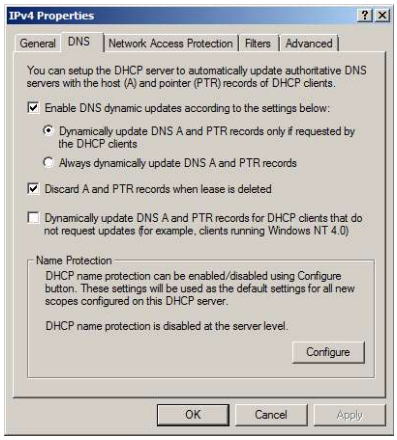
- **سطح Scope**: اگر پیکربندی در سطح یک Scope انجام شود، تنظیمات آن تنها برروی کاربران همان Scope اعمال خواهند شد.
- **سطح Server**: پیکربندی سطح سرور، تنظیمات را برروی کلیه Scopeها و Superscopeها اعمال می‌کند.

انتخاب سطح پیکربندی بستگی به محدوده‌ای دارد که قرار است از DDNS پشتیبانی کند. به عنوان مثال بیشتر وب‌سایت‌هایی که برروی اینترنت مشاهده می‌کنید، بروزرسانی DNS را در سطح سرور انجام می‌دهند.

۵-۱۱-۱ بروز رسانی اطلاعات DNS در DHCP

برای بروز رسانی تنظیمات چه در سطح Scope و یا سطح سرور، مراحل زیر را دنبال کنید:

۱. برروی Scope یا سرور مورد نظر کلیک‌راست نموده و properties را انتخاب کنید.
۲. در پنجره IPv4 Properties/Scope Properties، تب DNS را انتخاب کنید.



شکل ۵-۵۲

1. Dynamic DNS

همانطور که در شکل ۵-۵۲ مشاهده می‌کنید تب DNS شامل موارد زیر می‌باشد:

- **Enable DNS Dynamic Updates According To The Settings Below**: این گزینه فعال یا غیرفعال کردن توانایی سرور DHCP جهت ثبت اطلاعات Lease به همراه سرور DNS را کنترل می‌کند. جهت فعال‌سازی DDNS این گزینه باید تیک خورده باشد.
- **Dynamically Update DNS A And PTR Records Only If Requested By The DHCP Clients**: این گزینه به سرور DHCP اعلام می‌کند که فقط در صورت درخواست کاربران برای ثبت نام در DNS، بروز رسانی را انجام دهد. زمانی که این گزینه فعال باشد، کاربران DHCP که به DDNS متصل نباشند نمی‌توانند بروز رسانی رکوردهای DNS را در اختیار داشته باشند. با این حال، کاربران ویندوزهای 2000، XP، Vista، Server 2003، Server 2008 و Server 2008R2 به اندازه‌ای هوشمند هستند که برای این بروز رسانی درخواست دهند.
- **Always Dynamically Update DNS A And PTR Records**: این گزینه سرور DHCP را مجبور می‌کند که بروز رسانی را برای تمام کاربران انجام دهد. اگرچه این ویژگی باعث می‌شود که اطلاعات بروز رسانی برای دستگاه‌هایی که DHCP برروی آنها فعال بوده ولی نیاز به این اطلاعات ندارند (مثل Print Server) ارسال شود، اما به سایر کاربران (کاربران ماشین‌های Mac OS، Windows NT و Linux) اجازه می‌دهد که بروز رسانی خودکار اطلاعات DNS را در اختیار داشته باشند.
- **Discard A And PTR Records When Lease Is Deleted**: این گزینه اتفاقی که برای اطلاعات DNS مرتبط با یک Lease در زمان اتمام آن رخ می‌دهد را مشخص می‌نماید. چنانچه این گزینه فعال باشد (تیک خورده باشد) اطلاعات DNS در زمان اتمام Lease حذف خواهند شد ولی در صورتی که این گزینه غیرفعال باشد، پس از اتمام اعتبار Lease نیز اطلاعات DNS برای آن نگهداری خواهد شد.
- **Dynamically Update DNS A And PTR Records For DHCP Clients That Do Not Request Updates**: این گزینه باعث فراهم شدن اطلاعات بروز رسانی DNS برای کاربرانی می‌شود که آن اطلاعات را درخواست نکرده‌اند (البته فعال‌سازی این ویژگی لطفی است که در حق این کاربران انجام می‌شود!)

۵-۱۱-۲ یکپارچه سازی DNS با DHCP

جهت یکپارچه سازی DNS با DHCP مراحل زیر را دنبال کنید:

۱. در کنسول مدیریت DHCP برروی IPv4 کلیک‌راست نموده و Properties را انتخاب کنید.

۲. در پنجره "IPv4 Properties" تب DNS را انتخاب کنید.
۳. گزینه Enable DNS Dynamic Updates According To The Settings Below را فعال نموده و سپس گزینه Dynamically Update DNS A And PTR Records Only If Requested By The DHCP Clients را انتخاب کنید.
٤. مطمئن شوید که گزینه Discard A And PTR Records When Lease Is Deleted نیز فعال است (در غیر اینصورت آنرا فعال کنید).
٥. برروی OK کلیک کنید تا تنظیمات اعمال گردد.
٦. پنجره "IPv4 Properties" را ببندید.

۵-۱۲ نظارت و عیب‌یابی DHCP

DHCP به مراقبت زیاد و مداوم نیاز ندارد، با این حال دانستن نحوه نظارت[1] و عیب‌یابی[2] آن در مواردی که کارهای نادرستی انجام می‌شود، می‌تواند مفید واقع گردد. در ادامه به مباحثی مثل نظارت بر Leaseهای DHCP، ثبت[3] فعالیت‌های DHCP، کارکردن با فایل‌های ثبت وقایع و پایگاه‌داده‌های DHCP و تطبیق‌دادن[4] Scopeها در DHCP خواهیم پرداخت.

۵-۱۲-۱ نظارت بر Leaseهای DHCP

با استفاده از کنسول مدیریت DHCP، امکان مدیرت و نظارت بر Leaseها بسیار ساده شده است. جهت مشاهده Leaseها می‌توانید از زیرشاخه هر Scope، برروی Address Leases کلیک نموده و لیست Leaseها را مشاهده کنید.

چنانچه قصد داشته باشید Lease مرتبط با یک کاربر را حذف کنید، کافی است در قسمت Address Leases برروی Lease کلیک‌راست نموده و Delete را انتخاب کنید. این کار باعث لغو شدن و حذف Lease می‌گردد. معمولاً بهترین کار این است که بجای حذف دستی Lease، اجازه دهید مدت زمان آن به پایان برسد، اما گاهی اوقات و با توجه به شرایط، حذف دستی آنها لازم است.

در ادامه قصد داریم نحوه بررسی Leaseها را با ذخیره کردن آنها به صورت یک فایل متنی شرح دهیم. قبل از این کار لازم است حداقل یک یا دو Lease در حال اجرا باشند. جهت انجام این کار مراحل زیر را دنبال کنید:

۱. در کنسول مدیریت DHCP برروی IPv4 کلیک کنید تا آیتم‌های زیرشاخه آن نشان داده شوند.

1. Monitoring
2. Troubleshooting
3. Log
4. Reconcile

۲. Scope مورد نظر را انتخاب کنید.

۳. برروی Scope کلیک‌راست نموده و گزینه Export List را انتخاب کنید.

٤. در پنجره"Save As " محل ذخیره و نام فایل Export را مشخص نموده و برروی Save کلیک کنید.

٥. فایل را در یکی از برنامه‌های Notepad، WordPad، Word، Excel و یا ... باز کنید. توجه داشته باشید که محتویات این فایل همان چیزی است که در کنسول DHCP مشاهده نمودید. چنانچه هیچ Leaseای اختصاص داده نشده باشد، شما تنها یک سطر حاوی عنوان هر ستون مشاهده خواهید نمود.

۵-۱۲-۲ ثبت فعالیت‌های DHCP

سرور DHCP به طور خودکار تمام فعالیت‌های DHCP را در یک فایل ثبت وقایع (log) به صورت روزانه ثبت می‌کند. این فایل در پوشه C:\Windows\System32\dhcp و با نام DhcpSrvLog-Day قرار دارد که Day یک مخفف سه حرفی و نمایانگر روزهای هفته می‌باشد.

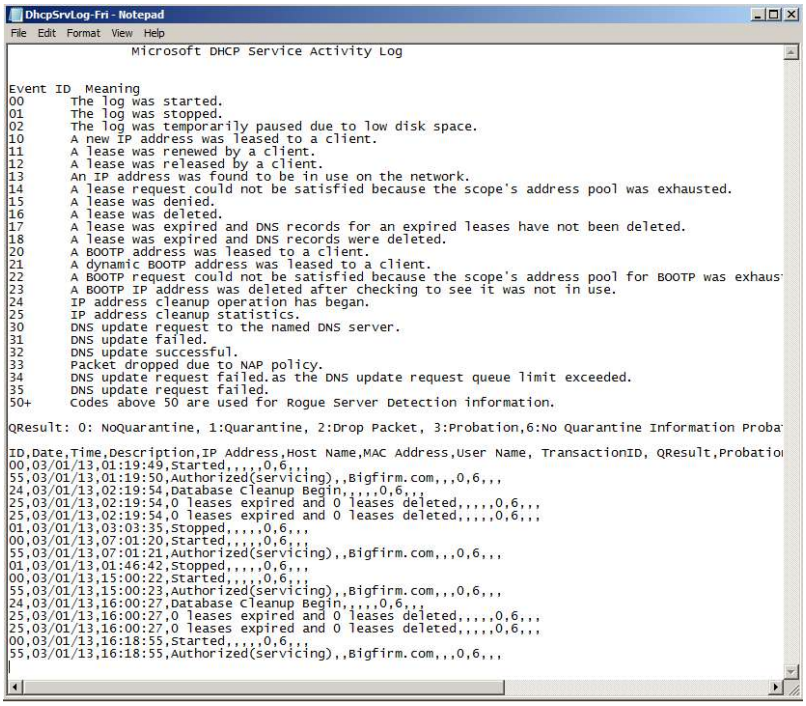
فایل‌های Log در DHCP، یک سری از فایل‌های متنی هستند که در آن هر مدخل[1] (ورودی) در یک سطر جداگانه آورده می‌شود. تعدادی از فیلدهایی که برای مدخل‌های این فایل‌ها وجود دارد، در جدول ۵-۱ شرح داده شده است

جدول ۵-۱ : فیلدهای موجود در فایل‌های Log در سرور DHCP

نام فیلد	شرح
ID	شناسه مربوط به رویداد در سرور DHCP (00، 01 و ...)
Date	تاریخی که یک رویداد در سرور DHCP اتفاق می‌افتد
Time	زمانی که یک رویداد در سرور DHCP اتفاق می‌افتد
Description	نوع رویدادی که در سرور DHCP رخ می‌دهد
IP Address	آدرس IP کاربر DHCP
Host Name	نام میزبان (نام ماشین) کاربر DHCP
MAC Address	آدرس سخت افزار کاربر که همان آدرس فیزیکی کارت شبکه می‌باشد
User Name	نام کاربر DHCP

در شکل ۵-۵۳ می‌توانید محتویات یکی از فایل‌های Log را مشاهده کنید.

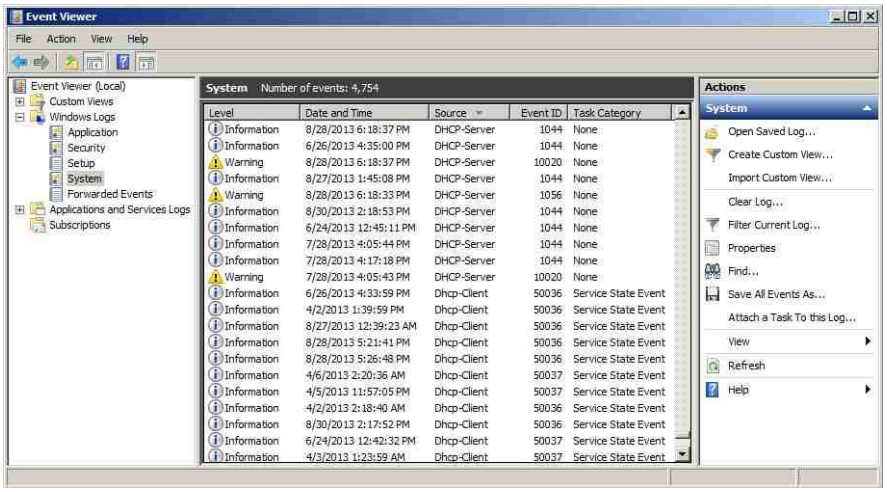
1. Entry



```
DhcpSrvLog-Fri - Notepad
File  Edit  Format  View  Help
                Microsoft DHCP Service Activity Log


Event ID  Meaning
00        The log was started.
01        The log was stopped.
02        The log was temporarily paused due to low disk space.
10        A new IP address was leased to a client.
11        A lease was renewed by a client.
12        A lease was released by a client.
13        An IP address was found to be in use on the network.
14        A lease request could not be satisfied because the scope's address pool was exhausted.
15        A lease was denied.
16        A lease was deleted.
17        A lease was expired and DNS records for an expired leases have not been deleted.
18        A lease was expired and DNS records were deleted.
20        A BOOTP address was leased to a client.
21        A dynamic BOOTP address was leased to a client.
22        A BOOTP request could not be satisfied because the scope's address pool for BOOTP was exhaus
23        A BOOTP IP address was deleted after checking to see it was not in use.
24        IP address cleanup operation has began.
25        IP address cleanup statistics.
30        DNS update request to the named DNS server.
31        DNS update failed.
32        DNS update successful.
33        Packet dropped due to NAP policy.
34        DNS update request failed.as the DNS update request queue limit exceeded.
35        DNS update request failed.
50+       Codes above 50 are used for Rogue Server Detection information.

QResult: 0: NoQuarantine, 1:Quarantine, 2:Drop Packet, 3:Probation,6:No Quarantine Information Proba

ID,Date,Time,Description,IP Address,Host Name,MAC Address,User Name, TransactionID, QResult,Probatio
00,03/01/13,01:19:49,Started,,,,0,6,,,
55,03/01/13,01:19:50,Authorized(servicing),,Bigfirm.com,,,0,6,,,
24,03/01/13,02:19:54,Database Cleanup Begin,,,,0,6,,,
25,03/01/13,02:19:54,0 leases expired and 0 leases deleted,,,,0,6,,,
25,03/01/13,02:19:54,0 leases expired and 0 leases deleted,,,,0,6,,,
01,03/01/13,03:03:35,Stopped,,,,0,6,,,
00,03/01/13,07:01:20,Started,,,,0,6,,,
55,03/01/13,07:01:21,Authorized(servicing),,Bigfirm.com,,,0,6,,,
01,03/01/13,01:46:42,Stopped,,,,0,6,,,
00,03/01/13,15:00:22,Started,,,,0,6,,,
55,03/01/13,15:00:23,Authorized(servicing),,Bigfirm.com,,,0,6,,,
24,03/01/13,16:00:27,Database Cleanup Begin,,,,0,6,,,
25,03/01/13,16:00:27,0 leases expired and 0 leases deleted,,,,0,6,,,
25,03/01/13,16:00:27,0 leases expired and 0 leases deleted,,,,0,6,,,
00,03/01/13,16:18:55,Started,,,,0,6,,,
55,03/01/13,16:18:55,Authorized(servicing),,Bigfirm.com,,,0,6,,,
```

شکل ۵-۵۳

دقت داشته باشید که این رویدادها را می‌توان از ابزار Event Viewer نیز مشاهده نمود. این ابزار از مسیر Start» Administrative Tools» Event Viewer قابل دسترسی می‌باشد. در Logهای این ابـزار بایـد به دنبال مدخل‌های مرتبط با DHCP بگردید (شکل ۵-۵٤).



شکل ۵-۵۴

۵-۱۲-۳ کار با پایگاه‌داده‌های DHCP

DHCP جهت نگهداری اطلاعات مربوط به Scopeها، Superscopeها و Leaseهای کاربران، از چند پایگاه‌داده استفاده می‌کند. این فایل‌ها در مسیر C:\Windows\System32\dhcp قرار دارند و در زمان اجرای سرویس DHCP مورد استفاده قرار می‌گیرند. مشاهده محتویات و ایجاد تغییرات در این فایل‌ها تا زمانی‌که سرویس DHCP در حال اجرا می‌باشد امکان‌پذیر نیست، بنابراین قبل از ایجاد تغییرات باید این سرویس را متوقف کنید.

فایل اصلی مربوط به پایگاه‌داده DHCP با نام dhcp mdb و در مسیر ذکر شده قرار دارد و حاوی اطلاعات تمام Scopeها می‌باشد. تعدادی دیگر از فایل‌های مرتبط با پایگاه‌داده DHCP که در این مسیر قرار دارند عبارتند از:

- **Dhcp.tmp**: این فایل یک کپی از فایل Backup پایگاه‌داده DHCP می‌باشد که در زمان شاخص‌دهی مجدد[1] پایگاه‌داده ایجاد می‌شود.
- **J50 log** (به اضافه تعدادی از فایل‌ها با نام J50xxxxx.log که xxxxx مقادیر 00001 و 00002 و 00003 و مشابه آن می‌باشند): این فایل هرگونه تغییری را قبل از نوشته شدن برروی پایگاه‌داده ذخیره می‌کند. موتور[2] پایگاه‌داده DHCP، در هنگام راه‌اندازی سرور از این فایل‌ها جهت بازیابی تعدادی از تغییرات استفاده می‌کند.
- **J50.chk**: یک فایل Chekpoint (نقطه بررسی) می‌باشد و به موتور DHCP اعلام می‌کند که کدامیک از فایل‌های Log نیازمند بازیابی می‌باشند.

حذف فایل‌های پایگاه‌داده

گاهی اوقات ممکن است در هنگام کار با پایگاه‌داده متوجه شوید که اطلاعات مربوط به Leaseها با آنچه که در شبکه باید وجود داشته باشد ناسازگار است. یکی از راه حل‌هایی که جهت برطرف کردن این مشکل به کار گرفته می‌شود، حذف فایل پایگاه‌داده و راه‌اندازی سرور با استفاده از یک فایل بدون محتوا می‌باشد. برای انجام این کار مراحل زیر را دنبال کنید:

۱. سرویس DHCP را با استفاده از دستور `net stop dhcpserver` و یا با کلیک‌راست برروی نام سرور در کنسول مدیریت DHCP و انتخاب All Tasks» Stop متوقف کنید.
۲. کلیه فایل‌های موجود در پوشه C:\Windows\System32\dhcp را حذف کنید.
۳. سرور را Restart کنید.
٤. Scope (ها) را با سرور تطبیق دهید تا محتویات پایگاه‌داده مجدداً ایجاد شوند.

1. Reindexing
2. Engine

تغییر بازه زمانی Backup گیری از پایگاه‌داده

بطور پیش‌فرض، DHCP هر ٦٠ دقیقه یکبار از پایگاه‌داده خود Backup گیری می‌کند. می‌توانید این زمان را با استفاده از مقدار Backup Interval در رجیستری تغییر دهید. این مقدار از مسیر زیر قابل دسترسی می‌باشد:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\DHCPServer\Parameter

جابجایی فایل‌های پایگاه‌داده DHCP

گاهی اوقات لازم است که سرور DHCP و عملکردهای مرتبط با آنرا به کامپیوتر دیگری انتقال دهید. در این مواقع بهترین کار این است که فایل‌های پایگاه‌داده DHCP را کپی نموده و آنرا مستقیماً به کامپیوتر جدید منتقل کنید. با این روش دیگر نیازی به ایجاد مجدد فایل‌ها و همچنین برطرف کردن خطاهایی که در هنگام ایجاد آنها ممکن است رخ دهد نخواهید داشت.

در این قسمت قصد داریم نحوه انتقال فایل پایگاه‌داده DHCP از یک ویندوز 2000، سرور 2003 و سرور 2008 را به دیگری نشان دهیم. جهت جابجایی پایگاه‌داده مراحل زیر را دنبال کنید:

١. سرور DHCP را با دستور `net stop dhcpserver` در خط فرمان متوقف کنید.
٢. پوشه C:\Windows\System32\dhcp را به یک پوشه موقت در سرور مقصد کپی کنید.
٣. با نوشتن دستور `Regedit.exe` در Cmd، رجیستری را اجرا نموده و کلید Configuration را از مسیر HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\DhcpServer پیدا کنید. آنرا انتخاب نموده و از منوی بالای پنجره رجیستری، گزینه File » Export را انتخاب کنید.
٤. سرویس DHCP را برروی سرور مقصد نصب نموده با دستور `net stop dhcpserver` آنرا متوقف کنید.
٥. فایل System.mdb را از پوشه موقت انتخاب نموده و نام آنرا به System.src تغییر دهید.
٦. تمام محتویات پوشه C:\Windows\System32\dhcp را در کامپیوتر مقصد حذف کنید.
٧. رجیستری را در کامپیوتر مقصد اجرا نموده و مجدداً کلید Configuration را از مسیر HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\DhcpServer پیدا کنید. این کلید را انتخاب نموده و از منوی بالای پنجره رجیستری، گزینه File » Import را انتخاب کنید.
٨. فایلی که اخیراً ذخیره نموده‌اید را انتخاب نموده و برروی Yes کلیک کنید تا جایگزین تنظیمات فعلی گردد.
٩. سرویس DHCP را در کامپیوتر مقصد با دستور `net start dhcpserver` در خط فرمان راه‌اندازی کنید.
١٠. در آخرین مرحله نیز باید سرور را در اکتیودایرکتوری مجاز کنید. جهت انجام این کار برروی

نام سرور کلیک‌راست نموده و گزینه Authority را انتخاب کنید.

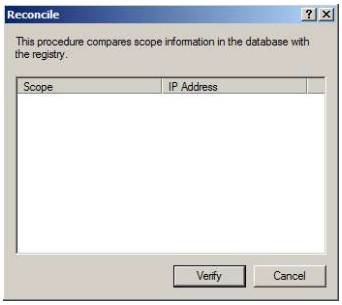
۵-۱۲-۴ تطبیق دادن Scopeهای DHCP در IPv4

با گذشت زمان ممکن است متوجه شوید که اطلاعات پایگاه‌داده DHCP با اطلاعات اصلی در شبکه سازگار نمی‌باشد و بنابراین دیگر از کارایی لازم برخوردار نخواهند بود. راه‌حل این مشکل، حذف پایگاه‌داده و ایجاد مجدد آن می‌باشد. برای انجام این کار باید Scopeهای خود را با پایگاه‌داده تطبیق دهید.

تطبیق دادن یک Scope

جهت تطبیق‌دادن یک Scope مراحل زیر را دنبال کنید:

۱. کنسول مدیریت DHCP را اجرا کنید.
۲. برروی IPv4 کلیک کنید تا آیتم‌های زیرشاخه آن نشان داده شود.
۳. برروی Scope موردنظر کلیک‌راست نموده و گزینه Reconcile را انتخاب کنید.
٤. در پنجره "Reconcile" برروی دکمه Verify کلیک کنید تا عمل تطبیق آغاز شود.



شکل ۵-۵۵

۵. اگر پایگاه‌داده با Scope سازگار بود، پنجره‌ای ظاهرشده و سازگاری آنرا اعلام می‌نماید. در صورتی که هرگونه ناسازگاری وجود داشته باشد، پنجره‌ای حاوی فهرست آنها نشان داده می‌شود و به شما اجازه می‌دهد تا این ناسازگاری‌ها را برطرف کنید.

تطبیق دادن همه Scopeها

برای تطبیق دادن همه Scopeها با پایگاه‌داده نیز فرایند مشابهی اجرا می‌گردد:

۱. پنجره مدیریت DHCP را اجرا کنید.
۲. برروی IPv4 کلیک‌راست نموده و گزینه Reconcile All Scopes را انتخاب کنید.
۳. برروی دکمه Verify کلیک کنید.

بازگردانی یک سرور ناموفق

روش پیشنهادی برای بازگردانی یک سرور ناموفق به صورت زیر می‌باشد:

۱. حذف فایل پایگاه‌داده
۲. Reconcile کردن همه Scopeها در سرور برای بازسازی پایگاه‌داده.