باسمه تعالی

مرکز تحقیقات مخابرات ایران

پژوهشکده شبکه – گروه دیتا

پروژه مشاوره با دیتا

عنوان گزارش:

IPv6

تهیه کنندگان:

مجتبی یعقوبی

سیما اسدآبادی

لادن امینی

عباس ایروانی

مدیر پروژه

علیرضا دهستانی

پاییز ۱۳۸۳

فهرست

پیشگفتار

رشد روزافزون اینترنت و پایان یافتن قریب الوقوع آدرس‌های **IPv4** لزوم ایجاد یک پروتکل آدرس‌دهی جدید برای حل این معضل را نشان می‌دهد چرا که راه حل‌هایی که به صورت موقتی برای حل معضل آدرس‌دهی **IPv4** پیشنهاد شده بودند نظیر **CIDR** و **NAT** موجب حل کامل این مشکل نشده‌اند و بعضا خود نیز مشکلاتی جدید به وجود آورده‌اند. از این رو پروتکل آدرس‌دهی نسل جدید با نام **IPv6** یا **IPv6** به وجود آمد. این تغییرات تنها در سطح لایه شبکه پروتکل **TCP/IP** اعمال خواهد شد و با افزایش فضای آدرس‌دهی به نظر می‌رسد که این مشکل را برای همیشه مرتفع کند.. در این نوشته نحوه آدرس‌دهی **IPv6** و چگونگی برخورد **DNS** با این آدرس‌دهی شرح داده‌شده است.

چگونگی آدرس‌دهی در IPv6

۱–۱ مقدمه

در حقیقت مهمترین تفاوت بین پروتکل اینترنت نسخه ۴ یا **IPv4** و پروتکل اینترنت نسخه ۶ یا **IPv6** را می‌توان در پیکربندی و نحوه آدرس‌دهی آن‌ها دانست. **IPv6** با بسط فضای آدرس مهمترین مشکل **IPv4** که همانا پایان یافتن آدرس‌های معتبر آن بود را حل نمود. در حالی که **IPv4** با تخصیص ۳۲ بیت برای آدرس‌دهی به اندازه 2^{32} یعنی **4,294,967,296** تعداد آدرس را پشتیبانی می‌نماید که مقدار زیادی از آن نیز به دلایل گوناگون به هدر می‌رود، **IPv6** با اختصاص فضای چهار برابر یعنی ۱۲۸ بیت برای آدرس‌دهی 2^{128} آدرس یا به عبارتی **340,282,366,920,938,463,463,374,607,431,768,211,456** **(3.4×10^{38})** تعداد آدرس را پشتیبانی می‌نماید که به نظر نمی‌رسد هیچگاه به پایان برسد.

در اواخر دهه ۷۰ هنگامی که آدرس‌های **IPv4** طراحی شد هرگز به ذهن طراحان آن خطور نمی‌کرد که روزی این آدرس‌ها به پایان برسد. اما رشد روزافزون اینترنت و انفجار یکباره مشترکین اینترنت پایانی بر آدرس‌دهی **IPv4** پیش‌بینی نمود و در سال ۱۹۹۲ ایجاد یک پروتکل جدید آدرس‌دهی را اجتناب ناپذیر می نمود.

اما امروزه با طراحی آدرس‌دهی **IPv6** به هیچ وجه نمی‌توان متصور شد که این میزان آدرس روزی به پایان برسد! همان تصوری که روزگاری طراحان **IPv4** در ذهن خود داشتند! برای درک بهتر تعداد آدرس‌های **IPv6** اجازه بدهید تا مساله را روشنتر نماییم. با تعداد آدرس‌های موجود **IPv6** در حال حاضر می‌توان به هر متر مربع از کره زمین تعداد **655,570,793,348,866,943,898,599 (6.5×10^{23})** آدرس اختصاص داد! بنابراین تصور طراحان **IPv6** مبنی بر پایان نیافتن **IPv6** تصور باطلی نخواهد بود و حتی به فکرمان نیز خطور نخواهد کرد که چگونه ممکن است این تعداد آدرس روزی به پایان برسد. البته باید توجه داشت که به هیچ وجه اساس طراحی **IPv6** این نبوده است که به هر متر مربع از کره زمین این تعداد آدرس اختصاص یابد و این مثال تنها برای تصور بهتر از میزان زیاد آدرس‌های **IPv6** آورده شده است.

در حقیقت تعداد بیتهای زیاد آدرس‌دهی در **IPv6** نیاز این پروتکل به تقسیم‌بندی سلسله مراتبی و اختصاص آن به نواحی جغرافیایی مختلف بوده است که در قسمتهای آینده در مورد آن بیشتر خواهیم نوشت. تعداد ۱۲۸ بیت آدرس موجب راحتی در تخصیص سلسله مراتبی آدرس‌ها و مدیریت آسانتر آن می‌شود. برای مطالعه دقیقتر ساختار آدرس‌دهی **IPv6** می‌توانید به **RFC3513** مراجعه نمایید.

۱–۲ نحوه نمایش آدرس‌های IPv6

همانطور که می‌دانیم **IPv4** به صورت اعداد دهدهی که با استفاده از نقطه از هم جدا می‌شوند نمایش داده می‌شوند. به طور مثال **192.168.1.1** یک نمونه از آدرس‌های **IPv4** می‌باشد. در این نمایش تعداد ۳۲ بیت آدرس به چهار قسمت هشت بیتی که توسط نقطه از هم جدا می‌شوند تقسیم و هر بخش به صورت اعداد دهدهی که بین صفر و ۲۵۵ قرار دارند نمایش داده می‌شوند.

در **IPv6** برای نمایش آدرس‌ها کل بیتها را به هشت بخش ۱۶ بیتی تقسیم‌بندی می‌کنیم و هر بخش را با استفاده از دو نقطه (:) از بخش دیگر جدا می‌کنیم. بخش‌های ۱۶ بیتی را نیز به صورت اعداد مبنای ۱۶ که بین **0000** و **FFFF** واقع می‌شوند نشان می‌دهیم. عدد دودویی ۱۲۸ بیتی زیر را در نظر بگیرید:

```
00100001110110100000000011010011000000000000000000010111100111011
00000010101010100000000011111111111111110001010001001110001011010
```

این اعداد نمایانگر یک آدرس **IPv6** هستند. برای نمایش آدرس معادل ابتدا آنرا به ۸ بخش ۱۶ بیتی تقسیم‌بندی می‌کنیم:

```
0010000111011010   0000000011010011   0000000000000000   0010111100111011
0000001010101010   0000000011111111   1111111000101000   1001110001011010
```

حال با نمایش این بخش‌ها در مبنای ۱۶ و جداسازی آن‌ها به کمک دونقطه به آدرس **IPv6** زیر می‌رسیم:

21DA:00D3:0000:2F3B:02AA:00FF:FE28:9C5A

همانطور که در آدرس‌دهی **IPv4** می‌توان به جای آدرس **080.123.001.025** از آدرس **80.123.1.25** استفاده نمود و از صفرهای بی‌ارزش صرف‌نظر کرد در آدرس‌دهی **IPv6** نیز می‌توان این صفرها را در نظر نگرفت. بنابراین آدرس مثال بالا را می‌توان به صورت زیر نمایش داد:

21DA:D3:0:2F3B:2AA:FF:FE28:9C5A

۱–۳ فشرده‌سازی صفرها[1]

همانطور که مشاهده شد نمایش آدرس‌های **IPv6** بسیار طولانی و به خاطر سپردن آن دشوار است. از طرفی در بسیاری از آدرس‌های **IPv6** که مورد استفاده قرار می‌گیرند تعداد زیادی از بخش‌های ۱۶ بیتی

[1] **Zero Compression**

را صفرها تشکیل می‌دهند. از اینرو جهت ساده‌سازی نمایش آدرس‌های **IPv6** مقرر شد که بتوان بجای صفرهای پشت سر هم از علامت **::** استفاده شود. به این روش نمایش فشرده‌سازی صفر گفته می‌شود. از آنجاییکه تعداد بخش‌های ۱۶ بیتی یک آدرس **IPv6** مشخص و به تعداد ۸ تا می‌باشد به راحتی می‌توان تعداد بخش‌هایی که معادل صفر بوده و با علامت **::** نشان داده شده است را مشخص نمود. به طور مثال آدرس **FE80:0:0:0:2AA:FF:FE9A:4CA2** را می‌توان به صورت **FE80::2AA:FF:FE9A:4CA2** نمایش داد یا آدرس **0:0:0:0:0:0:0:1** را می‌توان به صورت **::1** نمایش‌داد. بدیهی است که استفاده از این علامت در یک نمایش آدرس تنها یکبار مجاز است و بنابراین آدرس‌های **IPv6** را تنها یکبار می‌توان فشرده نمود. لذا نمایش آدرس مثالی **FFFE:0:0:30:0:0:0:803** به صورت **FFFE::30::803** نامعتبر است. تنها صورتهای درست نمایش این آدرس به صورت **FFFE::30:0:0:0:803** یا **FFFE:0:0:30::803** می‌باشد. در صورت اول با توجه به اینکه ۶ بخش ۱۶بیتی در آدرس وجود دارد نشان‌دهنده آن است که تعداد دو بخش معادل صفر فشرده شده است و در صورت دوم با توجه به وجود ۵ بخش ۱۶بیتی یقینا ۳ بخش معادل صفر فشرده‌سازی شده‌اند اما در صورت نامعتبر نشان‌داده شده نمی‌توان مشخص کرد که چه تعداد از صفرها مربوط به **::** اول و چه تعداد مربوط به **::** دوم می‌باشند.

۱-۴ پیشوندهای IPv6

همانطور که می‌دانیم در **IPv4** از ماسک زیرشبکه[1] برای مشخص نمودن بخش شبکه آدرس و بخش مربوط به میزبان آدرس استفاده می‌شود. با معرفی **CIDR** در **IPv4** استفاده از طول بیتهای مساوی یک در ماسک زیر شبکه نیز به عنوان پیشوند برای جداسازی بخش شبکه و میزبان یک آدرس مورد پذیرش قرار گرفت. به طور مثال می‌توان آدرس شبکه **192.168.1.0** با ماسک **255.255.255.0** را به صورت پیشوندی **192.168.1.0/24** نشان داد.

در **IPv6** برای نشان‌دادن بخش شبکه‌ای آدرس تنها می‌توان از پیشوندها استفاده نمود. پیشوند نشان‌دهنده تعداد بیتی از آدرس است که همواره در شبکه اختصاص داده‌شده ثابت است. به طور مثال آدرس **2001:4188::/32** یعنی اینکه ۳۲ بیت اول این آدرس برای مصرف‌کننده غیرقابل تغییر بوده و تنها

[1] **Subnet Mask**

می‌توان ۹۶ بیت باقیمانده را بین شبکه‌های مختلف و میزبآن‌های گوناگون تغییر داد. توجه داشته باشید که در **IPv6** استفاده از ماسک زیر شبکه معنایی نخواهد داشت.

۱–۵ انواع آدرس‌های IPv6

آدرس‌های **IPv6** را به صورت کلی می‌توان به سه دسته مختلف تقسیم‌بندی نمود. به عبارت دیگر **IPv6** از سه نوع آدرس‌دهی پشتیبانی می‌کند:

۱–۵–۱ آدرس‌های *unicast*

آدرس‌های **unicast** تنها به یک واسط شبکه‌ای اختصاص داده می‌شوند و به عبارت دیگر آدرس‌های **unicast** در یک محدوده تنها نمایانگر یک واسط شبکه‌ای می‌باشند. درخواستهایی که به آدرس‌های **unicast** ارسال می‌شوند بعد از مسیریابی موفق تنها به وسیله یک آدرس مشخص دریافت می‌شوند.

۱–۵–۲ آدرس‌های *multicast*

آدرس‌های **multicast** در آن واحد، نمایانگر چند واسط شبکه‌ای می‌باشند. بسته‌هایی که به آدرس **multicast** ارسال می‌شوند بعد از طی مسیرهای مسیریابی شده توسط تمامی واسطهای شبکه‌ای که آدرس **multicast** مورد نظر به آن‌ها اختصاص یافته است دریافت می‌شوند. از آدرس‌های **multicast** برای ارتباطات یک به چند استفاده می‌شود.

۱–۵–۳ آدرس‌های *anycast*

آدرس‌های **anycast** همانند آدرس‌های **multicast** به چند واسط شبکه به صورت همزمان اختصاص داده می‌شوند؛ اما بسته‌هایی که به اینگونه آدرس‌ها ارسال می‌شوند تنها توسط یک واسط شبکه دریافت می‌شوند که این واسط نزدیکترین واسط شبکه نسبت به فرستنده می‌باشد. نزدیکترین واسط نیز با توجه به الگوریتم‌های مسیریابی تعیین می‌شود. در حقیقت آدرس‌های **anycast** جهت دسترسی یک به یکی از چند واسط استفاده می‌شود.

در تمامی حالتهای آدرس‌دهی باید توجه داشته باشیم که آدرس‌ها به واسطهای شبکه‌ای اختصاص داده می‌شوند، نه به نقاط شبکه. به عبارت دیگر هر نقطه شبکه ممکن است چند واسط شبکه داشته باشد که هریک آدرس مجزای خود را داشته باشند.

در **IPv6** آدرس‌های موسوم به **broadcast** که در **IPv4** تعریف می‌شوند وجود ندارند. بجای آدرس‌های **broadcast** در **IPv6** از آدرس‌های **multicast** استفاده می‌شود. مثلا می‌توان از **multicast** به همه بجای **broadcast** استفاده نمود.

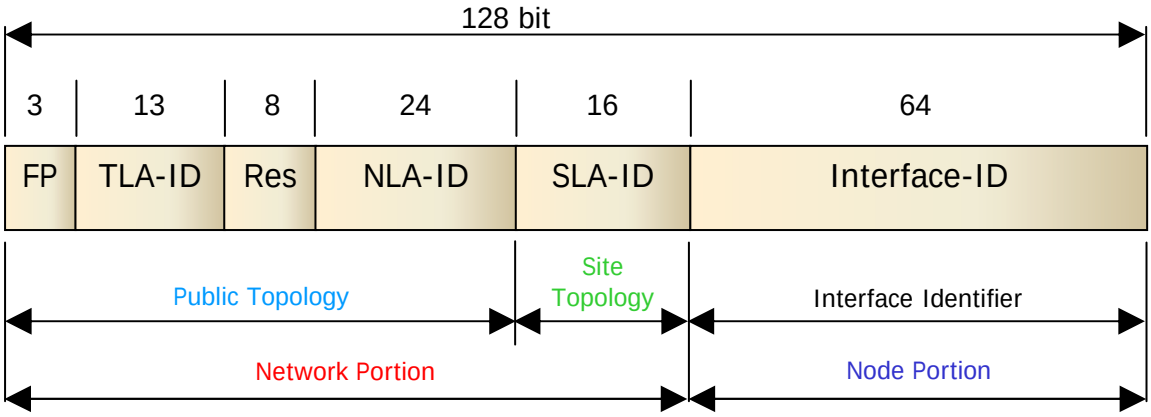
۱–۶ انواع آدرس‌های unicast

آدرس‌های **unicast** خود به چهار دسته کلی تقسیم‌بندی می‌شوند که عبارتند از :

- آدرس‌های **global unicast** یا آدرس‌های **unicast** عمومی
- آدرس‌های **link-local** یا آدرس‌های اتصال محلی
- آدرس‌های **site-local** یا آدرس‌های سایت محلی
- آدرس‌های مخصوص

۱–۶–۱ آدرس‌های unicast عمومی

آدرس‌های **unicast** عمومی که به آدرس‌های **unicast** عمومی **aggregateable** نیز موسومند در حقیقت همان معادل‌های آدرس‌های معتبر در **IPv4** می باشند. این آدرس‌ها در شبکه اینترنت مسیریابی می‌شوند و معادل یک واسط شبکه معتبر و یکتا در جهان هستند. همانطور که می‌دانیم هرچند آدرس‌های **IPv4** از یک ساختار سلسله مراتبی پیروی می‌کنند اما اختصاص این آدرس‌ها به نقاط جغرافیایی دارای نظم مشخصی نیست. از این رو ممکن است مثلا بخشی از آدرس **80.0.0.0/8** که به زیرشبکه‌های مختلف تقسیم شده است به یک قاره جهان و بخش دیگر به قاره‌ای دیگر اختصاص یابد. این امر موجب به وجود آمدن جدول‌های مسیریابی بسیار بزرگی در مسیریاب‌های هسته اصلی اینترنت می‌شود که به یکی از معضلات پیچیده و بسیار بزرگ **IPv4** در دنیای امروز تبدیل شده است. از این رو کارشناسان تقسیم آدرس در اینترنت تصمیم گرفتند که در مورد **IPv6** اختصاص آدرس‌ها به مناطق جغرافیایی نیز از یک ساختار سلسله مراتبی پیروی نماید. لذا بخشی از پیشوندهای مربوط به آدرس **IPv6** به مناطق جغرافیایی برای تعیین درست مسیر اختصاص یافته است. شکل ۱–۱ نمایی از ساختاربندی اینگونه آدرس‌ها را نشان می‌دهد.



شکل ۱-۱: نمایی از ساختاربندی آدرس **unicast** عمومی

همانطور که در شکل دیده می‌شود این ساختار از چند بخش تشکیل شده است:

FP: شکل پیشوند که تعیین کننده نوع آدرس می‌باشد. به عنوان مثال اگر پیشوند **001** باشد حتما این آدرس از نوع **unicast** عمومی می‌باشد. طول این قسمت سه بیت می‌باشد. بنابراین آدرس‌های **unicast** عمومی حتما با عدد ۲ یا ۳ در مبنای ۱۶ آغاز می‌شوند.

TLA-ID: شناسه مربوط به **Aggregation** در بالاترین سطح. این قسمت توسط سازمان بین‌المللی تخصیص آدرس‌های اینترنتی **(IANA)** به حوزه‌های ثبت آدرس‌های اینترنتی اختصاص داده می‌شود. از اینرو از روی یک آدرس می‌توان مکان جغرافیایی یک آدرس را در سطح قاره‌ها پیدا کرد.

Res: این قسمت برای استفاده‌های بعدی کنار گذاشته شده است. و می‌توان با کم کردن بیتهای اختصاص داده شده آن به بخش‌های قبل و بعد از آن فضای قسمتهای دیگر را افزایش داد.

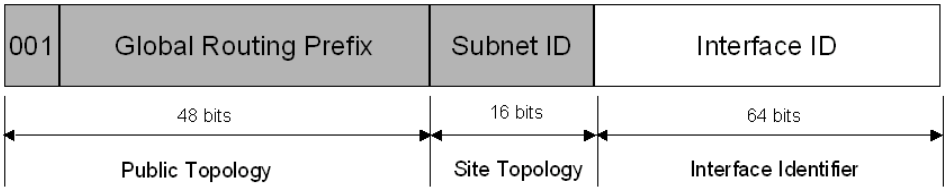
NLA-ID: شناسه مربوط به **Aggregation** سطح بعدی. از این شناسه برای مشخص نمودن کشورها، حوزه‌های ثبت محلی[1] و بخش‌های جغرافیایی کوچکتر استفاده می‌شود. در حال حاضر حوزه‌های ثبت آدرس‌های اینترنتی بخشی از این قسمت را به مشخص کردن حوزه‌های ثبت محلی اختصاص می‌دهند و بخش دیگر را جهت تقسیم به نواحی کوچکتر در اختیار حوزه‌های ثبت محلی می‌گذارند. در حال حاضر آدرس‌هایی با طول پیشوند ۳۲ بیت به درخواست‌کننده‌ها اختصاص می‌یابند.

SLA-ID: شناسه مربوط به **Aggregation** سطح سایت. از این شناسه برای مشخص نمودن ادارات و سازمان‌های وابسته به یک حوزه ثبت محلی استفاده می‌شود.

[1] **Local Registries**

Interface ID: از این شناسه برای مشخص نمودن آدرس منحصر به فرد هر واسط شبکه استفاده می‌شود. طول اختصاص داده‌شده به این بخش ثابت و ۶۴ بیت می‌باشد.

به طور کلی در یک صورت خلاصه‌شده می‌توان آدرس **IPv6** عمومی را به صورت شکل ۱-۲ در نظر گرفت.



شکل ۱-۲: ساختار سه سطحی آدرس‌های **Unicast** عمومی

این ساختار از سه سطح کلی تشکیل شده است که نشان می‌دهد بیتهای سمت چپ از اهمیت بیشتری برخوردارند. ۴۸ بیت اول به عنوان توپولوژی عمومی اینترنت، ۱۶ بیت بعدی به عنوان شناسه‌ای برای مناطق ناحیه‌ای و ۶۴ بیت آخر نیز مشخص کننده واسط شبکه می‌باشد.

۱-۷ استفاده‌های محلی از آدرس‌های Unicast

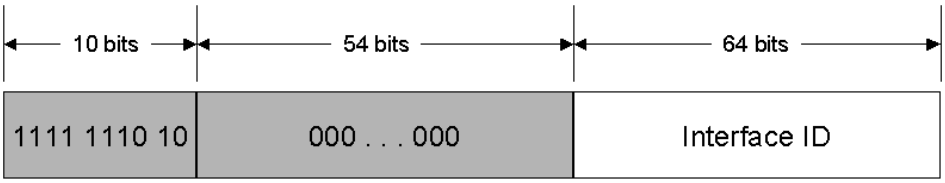
دو نوع استفاده محلی برای آدرس‌های **Unicast** محلی وجود دارد. آدرس‌های محلی مربوط به اتصال و آدرس‌های محلی مربوط به ناحیه که به ترتیب آدرس‌های **Link-Local** و آدرس‌های **Site-Local** نامیده می‌شوند.

۱-۷-۱ آدرس‌های *link-local*

این آدرس‌ها برای برقراری ارتباط بین نقاطی که در یک اتصال موجودند استفاده می‌شوند. این آدرس‌ها عموما برای تعیین وضعیت شبکه توسط پروتکل **Neighbor Discovery** مورد استفاده قرار می‌گیرند. همچنین می‌توان از این آدرس‌ها برای ارتباطات محلی در یک شبکه هنگامی که هیچ مسیریابی در شبکه موجود نیست استفاده نمود. معادل این آدرس‌ها در **IPv4** همان آدرس‌های **APIPA**[1] یا آدرس‌های خودکار خصوصی می‌باشند که از نوع آدرس‌های کلاس **B** بوده، معادل آدرس **169.254.0.0/16** در **IPv4** می‌باشند. این آدرس‌ها هنگامی که هیچ آدرسی برای پروتکل **IPv4** قابل

[1] **Automatic Private IP Address**

دستیابی نباشد به صورت خودکار تنظیم می‌شوند. در **IPv6** نیز چنین آدرس‌هایی موجودند که به آن‌ها آدرس‌های **Link-Local** گفته می‌شود. شکل ۱-۳ نمایی از ساختار آدرس‌دهی **Link-Local** را نشان می‌دهد.

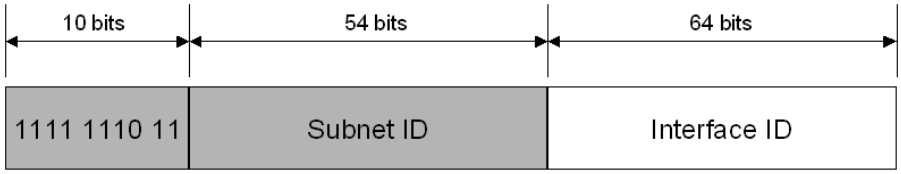


شکل ۱-۳: نحوه آدرس‌دهی **Link-Local**

همانطور که مشاهده می‌شود آدرس‌های **Link-Local** دارای ۱۰ بیت ثابت و ۵۴ بیت صفر هستند. بنابراین می‌توان آن‌ها را به صورت **FE80::/64** نشان داد. تنها ۶۴ بیت آخر این آدرس‌ها به **Interface ID** اختصاص دارد که نحوه به دست آمدن **Interface ID** را در بخش‌های بعدی توضیح خواهیم داد.

۱-۷-۲ آدرس‌های *Site-Local*

آدرس‌های **Site-Local** در **IPv6** معادل آدرس‌های خصوصی در **IPv4** هستند. همانطور که می‌دانیم آدرس‌های **192.168.0.0/16** ، **172.16.0.0/12** و **10.0.0.0/8** به عنوان آدرس‌های خصوصی برای استفاده محلی در **IPv4** پیش‌بینی شده‌اند. معادل این آدرس‌ها در **IPv6** آدرس‌های **Site-Local** نامیده می‌شوند. این آدرس‌ها برای استفاده‌های درون ناحیه‌ای و داخل شرکتها و سازمان‌ها در نظر گرفته شده‌اند و تنها مسیریاب‌های داخلی امکان مسیریابی آن‌ها را خواهند داشت. این آدرس‌ها در مسیریاب‌های اینترنت به هیچ وجه مسیریابی نخواهند شد. برعکس آدرس‌های **Link-Local** این آدرس‌ها به صورت خودکار تخصیص داده نمی‌شوند و باید به صورت دستی آن‌ها را تنظیم نمود یا از طریق مسیریاب آن‌ها را به شبکه معرفی نمود. شکل ۱-۴ نمایی از آدرس‌دهی **Site-Local** را نشان می‌دهد.



شکل ۱-۴: نمایی از نحوه آدرس‌دهی **Site-Local**

همانطور که در شکل دیده می‌شود این آدرس‌ها نیز از ۱۰ بیت ثابت به همراه ۵۴ بیت که مربوط به شناسه زیرشبکه می‌باشند، تشکیل شده است. بنابراین آدرس‌های **Site-Local** را می‌توان به صورت

FEC0::/10 نشان داد. از ۵۴ بیت مربوط به شناسه زیر شبکه می‌توان جهت ایجاد یک ساختار سلسله مراتبی در سازمان‌ها بهره جست. ۶۴ بیت انتهایی نیز همانند گذشته به آدرس واسط شبکه تعلق دارد.

۱–۸ آدرس‌های IPv6 مخصوص

بعضی از آدرس‌های **IPv6** برای استفاده خاص استفاده می‌شوند و نباید جهت تنظیم آدرس مورد استفاده قرار گیرد. این آدرس‌ها عبارتند از :

– **آدرس نامعین**: آدرس **IPv6** معادل **0:0:0:0:0:0:0:0** یا به عبارت ساده‌تر **::** نمایانگر عدم وجود آدرس برای یک واسط شبکه بوده و به هیچ عنوان استفاده خارجی ندارد. معادل این آدرس در **IPv4** آدرس **0.0.0.0** می‌باشد که برای شروع کار **TCP/IP** و تعیین آدرس مورد استفاده قرار می‌گیرد.

– **آدرس Loopback**: این آدرس برای مشخص نمودن آدرس شبکه‌ای **loopback** مورد استفاده قرار می‌گیرد. معادل این آدرس در **IPv4** همان آدرس **127.0.0.1** می‌باشد که برای آزمایش کارکرد داخلی **TCP/IP** استفاده می‌شود. در **IPv6** این آدرس را به صورت **0:0:0:0:0:0:0:1** یا به صورت خلاصه شده **1::** نشان می‌دهند. این آدرس نباید برای هیچ واسط شبکه‌ای تنظیم شود و یا برای ارتباط بین چند واسط مورد استفاده قرار گیرد.

۱–۹ آدرس‌های سازگار با بستر IPv4

برای راحتی گذر از بستر **IPv4** به بستر **IPv6** چند نوع آدرس سازگار با **IPv4** برای **IPv6** تعریف شده است که این لزوم وجود این آدرس‌ها برای این مرحله گذر و استفاده همزمان از هر دو نوع آدرس‌دهی اجتناب ناپذیر می‌باشند. این آدرس‌ها را در کل می‌توان به سه دسته تقسیم نمود:

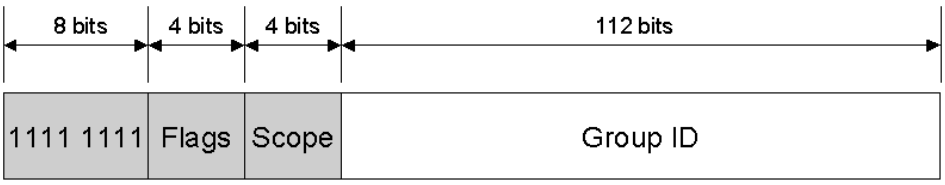
- **آدرس‌های سازگار با IPv4** : این آدرس‌های به صورت **0:0:0:0:0:0:w.x.y.z** یا به صورت خلاصه آن آدرس‌های **::w.x.y.z** آدرس‌های سازگار با **IPv4** نامیده می‌شوند که در آن‌ها **w.x.y.z** نمایانگر صورت نسخه ۴ آدرس‌های اینترنتی یا همان **IPv4** در شکل دهدهی که با نقطه از هم جدا شده‌اند، می‌باشد. این آدرس‌ها توسط نقطه‌های **IPv4/IPv6** که می‌خواهند از بستر **IPv6** برای برقراری ارتباط با **IPv4** بهره ببرند، استفاده می‌شوند. نقطه‌های **IPv4/IPv6** نقاطی هستند که به صورت همزمان هر دو پروتکل **IPv4** و **IPv6** را

پشتیبانی می‌کنند. هنگامی که یک آدرس **IPv6** سازگار با **IPv4** به عنوان گیرنده در یک بسته استفاده می‌شود به صورت خودکار این بسته با سرآیندهای نسخه ۴ بسته‌بندی شده و با ساختار **IPv4** به مقصد فرستاده می‌شود.

- **آدرس‌های نگاشت به IPv4** : این آدرس‌ها که به صورت **0:0:0:0:0:FFFF:w.x.y.z** یا **::FFFF:w.x.y.z** نمایش داده می‌شوند نمایانگر یک نقطه که تنها **IPv4** را پشتیبانی می‌کند می‌باشند. این آدرس‌ها فقط برای استفاده داخلی **TCP/IP** استفاده می‌شوند و به هیچ عنوان به عنوان آدرس‌های مبدا یا مقصد **IPv6** تنظیم نمی‌شوند.
- **آدرس‌های 6to4** : این آدرس‌ها برای برقراری ارتباط بین دو نقطه که هر دو هم **IPv4** و هم **IPv6** را پشتیبانی می‌کنند و می‌خواهند از یک بستر مسیریابی **IPv4** برای برقراری ارتباط استفاده کنند مورد استفاده قرار می‌گیرند. آدرس‌های **6to4** از پیشوند **2002::/16** و اضافه کردن ۳۲ بیت مربوط به **IPv4** به ادامه آن برای ساخت یک آدرس با پیشوند ۴۸تایی بهره می‌گیرند. **6to4** در حقیقت یک راهکار تونل‌زنی می‌باشد که برای برقراری ارتباط بین جزیره‌های **IPv6** موجود در سرتاسر جهان روی بستر موجود **IPv4** مورد استفاده قرار می‌گیرد. برای توضیحات تکمیلی این مبحث می‌توانید به **RFC3065** مراجعه نمایید.

۱–۱۰ آدرس‌های Multicast IPv6

عملکرد **multicast** در **IPv6** همانند عملکرد **multicast** در ارتباطات **IPv4** می‌باشد. همانطور که می‌دانیم از آدرس‌های **Multicast** برای ارتباطات یک به چند استفاده می‌شود. هر نقطه شبکه می‌تواند به صورت همزمان به چندین آدرس **multicast** گوش دهد. آدرس‌های **multicast** مربوط به **IPv6** دارای ۸ بیت یک در ابتدا می‌باشند. بنابراین تشخیص اینکه یک آدرس از نوع **multicast** می‌باشد یا نه بسیار آسان است زیرا آدرس‌های **multicast** با **FF** شروع می‌شوند. از آدرس‌های **multicast** نمی‌توان به عنوان آدرس مبدا و یا آدرس مقصد مسیریابی‌ها استفاده نمود. بعد از ۸ بیت اول آدرس‌های **multicast** از بیتهای بعدی آدرس برای ساختاربندی نواحی و گروههای **multicast**ا استفاده می‌شود. شکل ۱–۵ نمایی از نحوه ساختار بندی آدرس‌های **multicast** را نشان می‌دهد.



شکل ۱-۵: نحوه ساختار بندی آدرس‌های **multicast**

بخش‌های تشکیل‌دهنده آدرس‌های **multicast** علاوه بر ۸ بیت اول عبارتند از :

بخش پرچم‌ها[۱]: اندازه این بخش ۴ بیت می‌باشد. طبق تعریف **RFC3513** تنها پرچم تعریف شده تا کنون پرچم "گذرا[۲]" می‌باشد. برای تنظیم این پرچم از کم ارزش‌ترین بیت این بخش استفاده می‌شود. در صورتی که بیت مربوطه صفر باشد، نشان‌دهنده آن است که آدرس **multicast** اختصاص داده‌شده دایمی بوده و به وسیله **IANA**[۳] اختصاص داده شده است. اگر این پرچم یک باشد یعنی اینکه آدرس مذکور گذرا بوده و دایمی نمی‌باشد. برای مشاهده آدرس‌های دایمی اختصاص داده‌شده تاکنون توسط **IANA** می‌توانید به آدرس اینترنتی **http://www.iana.org/assignments/ipv6-multicast-addresses** مراجعه نمایید.

بخش ناحیه[۴]: این بخش نشان‌دهنده ناحیه‌ای است که آدرس **multicast** در ارتباطات بین شبکه‌ای **IPv6** مورد استفاده قرار می‌گیرد. اندازه این بخش ۴ بیت می‌باشد. مسیریاب‌ها علاوه بر استفاده از پروتکل‌های مسیریابی مربوط به **multicast** از اطلاعات این بخش برای تعیین این‌که آیا بسته **multicast** بایستی به مقصد بعدی فرستاده شود یا نه استفاده می‌کنند. رایج‌ترین مقادیر برای این بخش مقادیر ۱، ۲ و ۵ می‌باشند که به ترتیب نشان‌دهنده ناحیه واسط شبکه محلی[۵]، ناحیه اتصال شبکه محلی[۶] و ناحیه سایت شبکه محلی[۷] می‌باشند. به طور مثال آدرس **multicast** برابر **FF02::2** مربوط به اتصال محلی می‌باشد و توسط مسیریاب‌ها به بیرون از اتصال هدایت نخواهد شد.

[1] **Flags**
[2] **Transit**
[3] **Internet Assigned Number Authority**
[4] **Scope**
[5] **Interface Local Scope**
[6] **Link Local Scope**
[7] **Site Local Scope**

بخش شناسه گروه[1]: این بخش مشخص‌کننده گروه **multicast** بوده، در هر ناحیه نیز منحصر به فرد می‌باشد. اندازه این بخش ۱۱۲ بیت می‌باشد. آدرس‌هایی که از نوع دایمی باشند شناسه گروهی آن‌ها با شناسه ناحیه‌شان مرتبط نخواهد بود. برای آدرس‌های غیردایمی نیز شناسه گروهی تنها در ناحیه خودشان معتبر است. آدرس‌های **multicast** بین **FF01::** و **FF0F::** برای آدرس‌های مشهور کنارگذاشته‌شده است و به جایی اختصاص داده نمی‌شود که در ادامه به برخی از آن‌ها اشاره خواهیم کرد.

برای مشخص کردن تمامی نقاط در یک واسط شبکه یا در یک اتصال شبکه از آدرس‌های **multicast** زیر استفاده می‌شود:

- **FF01::1** این آدرس نمایانگر تمامی نقاط در یک واسط محلی می‌باشد.
- **FF02::1** این آدرس نمایانگر تمامی نقاط در یک اتصال محلی می‌باشد.

برای مشخص نمودن تمامی مسیریاب‌ها در یک واسط یا یک اتصال و یا یک سایت از آدرس‌های زیر استفاده می‌شود:

- **FF01::2** نشان‌دهنده تمامی مسیریاب‌هایی است که در ناحیه واسط محلی قرار دارند.
- **FF02::2** نشان‌دهنده تمامی مسیریاب‌هایی است که در ناحیه اتصال محلی قرار دارند.
- **FF05::2** نشان‌دهنده تمامی مسیریاب‌هایی است که در ناحیه یک سایت قرار دارند.

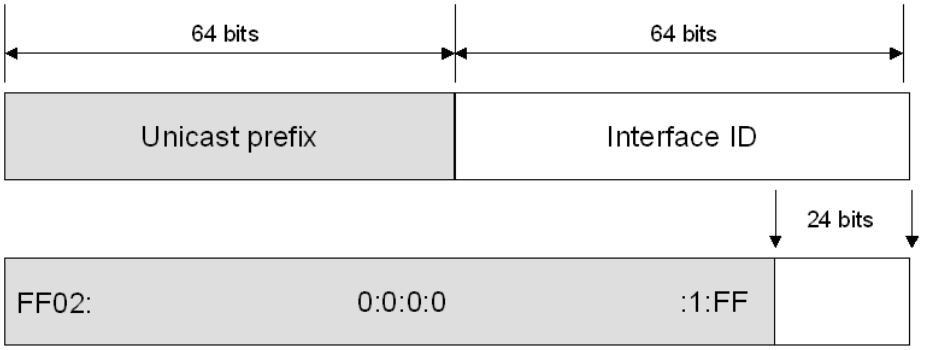
با استفاده از ۱۱۲ بیت اختصاص داده‌شده به شناسه گروه امکان تعریف 2^{112} گروه مختلف تعریف کرد. با توجه به نحوه نگاشت آدرس‌های **multicast** به آدرس‌های **multicast** اترنت **MAC** در **RFC 3513** پیشنهاد شده است که از ۳۲ بیت کم‌ارزش به عنوان شناسه گروه استفاده و بقیه بیتها صفر در نظر گرفته شوند. شکل ۱-۶ این ساختار پیشنهادی را نشان می‌دهد.

شکل ۱-۶: ساختار پیشنهادی **RFC 3513** برای مشخص نمودن شناسه گروهها

[1] **Group ID**

۱–۱۱ آدرس نقطه درخواستی[1]

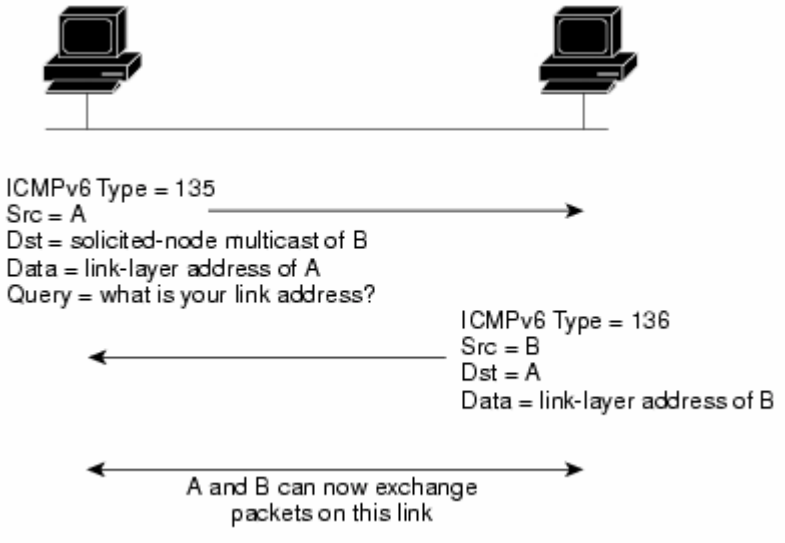
استفاده از آدرس نقطه درخواستی به دست آوردن آدرس‌های سخت‌افزاری سیستم و مشخصات مورد نیاز را آسانتر می‌کند. در **IPv4** درخواستهای **ARP** چنین کاری را انجام می‌دهند. درخواستهای **ARP** به صورت **broadcast** به همه نقطه‌ها ارسال می‌شوند و تمامی نقاط آن را دریافت می‌کنند. این نکته باعث شلوغی شبکه خواهد شد. در **IPv6** به جای استفاده از **ARP** از پیغام تقاضای اطلاعات همسایه[2] استفاده می‌شود. در این پیغام به جای اینکه پیغام به آدرس **multicast** تمامی نقاط اتصال شبکه محلی ارسال شود پیغام به آدرس نقطه درخواستی که یک آدرس **multicast** است ارسال می‌شود. آدرس **multicast** نقطه درخواستی از پیشوند ۱۰۴ تایی **FF02::1:FF00:0/104** و ۲۴ بیت آخر آدرس **IPv6** درخواستی تشکیل می‌شود. شکل ۱–۷ نمایی از ساختار چنین آدرسی را نشان می‌دهد.



شکل ۱–۷: ساختار آدرس **multicast** نقطه درخواستی

به طور مثال یک نقطه دسترسی به نام **A** با آدرس **FE80::2AA:FF:FE28:9C5A** موجود است. این نقطه در عین حال بایستی به آدرس **multicast** معادل **FF02::1:FF28:9C5A** نیز گوش فرا دهد (بخشی از آدرس که با خط زیر مشخص شده است نشان‌دهنده ۲۴ بیت آخر آدرس می‌باشد.). حال اگر نقطه **B** بخواهد با **A** ارتباط برقرار کند بجای فرستادن درخواست به همه یک درخواست به آدرس **multicast** ذکرشده می‌فرستد و **A** در جواب یک پیغام تبلیغ شبکه برای آگاه‌سازی **B** از وضعیت خود خواهد فرستاد. با اندکی تعمق مشاهده می‌شود که در این حالت کارایی بیشتری نسبت به حالتهای قبل در شبکه به وجود می‌آید. شکل ۱–۸ نمایی از فرآیند تقاضای اطلاعات همسایه مشاهده می‌شود.

[1] **Solicited-Node Address**
[2] **Network Solicitation Message**



شکل ۱–۸: نحوه درخواست اطلاعات همسایه در **IPv6**

۱–۱۲ آدرس‌های Anycast

آدرس‌های **Anycast** به صورت همزمان به چند واسط شبکه اختصاص داده می‌شوند. بسته‌هایی که به مقصد **anycast** ارسال می‌شوند از طریق ساختارهای مسیریابی مربوط به **anycast** به نزدیکترین مقصد فرستاده می‌شوند. برای بهبود ساختار مسیریابی مسیریاب‌ها بایستی از مکان آدرس‌های **anycast** و فاصله آن‌ها بر حسب معیارهای مسیریابی[1] مطلع باشند. در حال حاضر آدرس‌های **anycast** تنها به عنوان آدرس مقصد آنهم برای مسیریاب‌ها مورد استفاده قرار می‌گیرند. آدرس‌های **anycast** از روی آدرس‌های **unicast** به دست می‌آیند و محدوده کاری آن‌ها نیز بستگی به محدوده کاری آدرس‌های **unicast** مرجع دارد.

آدرس **anycast** مربوط به مسیریاب زیر شبکه یک آدرس از قبل تعریف شده است. این آدرس از روی پیشوند زیرشبکه موجود ساخته می‌شود. برای ساختن این آدرس بخش شبکه‌ای آدرس را ثابت در نظر گرفته و بقیه بیتها را صفر می‌کنند؛ بنابراین تمامی مسیریاب‌های موجود در یک زیرشبکه دارای آدرس **anycast** یکسانی خواهند بود. به طور مثال برای شبکه **2001:4188:1:1::/64** آدرس **anycast** برابر **2001:4188:1:1:0:0:0:0** یا به عبارتی **2001:4188:1:1::** خواهد بود. این آدرس برای دسترسی نقاط موجود در یک شبکه از یکی از مسیریاب‌های موجود مورد استفاده قرار می‌گیرد.

[1] **Routing Metrics**

۱–۱۳ آدرس‌های IPv6 مربوط به میزبان[1]

یک میزبان **IPv4** در حالت عادی معمولا یک آدرس **IPv4** به خود اختصاص می‌دهد؛ ولی در مورد میزبآن‌های **IPv6** قضیه فرق می‌کند. یک میزبان **IPv6** معمولا چند آدرس **IPv6** دارد. به یک میزبان **IPv6** آدرس‌های زیر اختصاص می‌یابد:

- یک آدرس اتصال محلی برای هر واسط شبکه
- آدرس **unicast** برای هر واسط شبکه که می‌تواند از یک آدرس سایت محلی و یک یا چند آدرس **unicast** عمومی تشکیل شود.
- آدرس **loopback** که همان آدرس **::1** می‌باشد.

در حقیقت میزبآن‌های **IPv6** از نوع چند شبکه‌ای می‌باشند؛ زیرا هم یک آدرس از نوع اتصال محلی برای ارتباطات داخل شبکه‌ای دارند و هم یک یا چند آدرس مسیریابی‌شونده برای ارتباطات بین شبکه‌ای را دارا هستند.

علاوه بر آدرس‌های مذکور میزبآن‌های **IPv6** بایستی به آدرس‌های **multicast** زیر نیز گوش دهند:

- آدرس **multicast** تمام نقاط موجود در ناحیه واسط محلی **(FF01::1)**
- آدرس **multicast** تمام نقاط موجود در ناحیه اتصال محلی **(FF02::1)**
- آدرس نقطه درخواستی برای هر آدرس **unicast** روی هر واسط شبکه
- آدرس‌های **multicast** گروههای **multicast** که آن میزبان عضو آن باشد.

۱–۱۴ آدرس‌های IPv6 مربوط به مسیریاب‌ها

آدرس‌های زیر را می‌توان برای یک مسیریاب **IPv6** در نظر گرفت:

- یک آدرس اتصال محلی برای هر واسط شبکه

[1] **Host**

- آدرس **unicast** برای هر واسط شبکه که می‌تواند از یک آدرس سایت محلی و یک یا چند آدرس **unicast** عمومی تشکیل شود.
- آدرس **anycast** مربوط به مسیریاب زیرشبکه
- آدرس‌های دیگر **anycast** که در مواقع لزوم تنظیم می‌شوند
- آدرس **loopback** که **::1** می‌باشد

همچنین یک مسیریاب **IPv6** بایستی به آدرس‌های **multicast** زیر گوش دهد:

- آدرس **multicast** تمام نقاط موجود در ناحیه واسط محلی **(FF01::1)**
- آدرس **multicast** تمام مسیریاب‌های موجود در ناحیه واسط محلی **(FF01::2)**
- آدرس **multicast** تمام نقاط موجود در ناحیه اتصال محلی **(FF02::1)**
- آدرس **multicast** تمام مسیریاب‌های موجود در ناحیه اتصال محلی **(FF02::2)**
- آدرس **multicast** تمام مسیریاب‌های موجود در ناحیه سایت محلی **(FF05::2)**
- آدرس نقطه درخواستی برای هر آدرس **unicast** روی هر واسط شبکه
- آدرس‌های **multicast** گروههای **multicast** که آن مسیریاب عضو آن باشد.

۱–۱۵ شناسه واسط در IPv6 [1]

۶۴ بیت آخر آدرس‌های **IPv6** مربوط به شناسه واسط شبکه می‌باشد که باید در یک زیرشبکه **IPv6** منحصر به فرد باشد. راههایی که برای ایجاد این شناسه ۶۴ بیتی وجود دارد تا یکتایی آن تضمین شود به شرح زیر است:

- یک آدرس واسط شبکه که از روی شناسه منحصربه‌فرد توسعه یافته[2] معروف به **EUI-64** به دست آمده باشد.
- یک شناسه واسط که به صورت تصادفی ایجاد می‌شود و در بسترهای گوناگون تغییر می‌کند.

[1] **IPv6 Interface Identifier**
[2] **Extended Unique Identifier (EUI)**

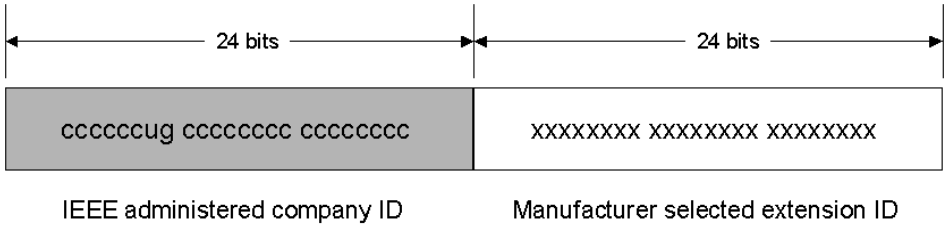
- یک شناسه منحصر به فرد که به صورت اتوماتیک توسط ابزارهایی نظیر **DHCPv6** اختصاص داده می‌شود. در حال حاضر **DHCPv6** معرفی و اجرا شده است.

۱–۱۶ شناسه واسط مبتنی بر EUI-64

در **RFC 3513** خاطرنشان شده است که تمامی آدرس‌های **unicast** عمومی که سه بیت اول آن‌ها **001** می‌باشد بایستی حتما از یک شناسه واسط ۶۴ بیتی مبتنی بر **EUI-64** استفاده نمایند. شناسه **EUI-64** توسط انجمن مهندسان برق و الکترونیک **(IEEE)** معرفی شده است. آدرس‌های **EUI-64** یا از ابتدا بر روی واسطهای شبکه تنظیم‌شده‌اند و یا از روی آدرس‌های سخت‌افزاری موجود معروف به آدرس‌های **IEEE 802** که طول آن‌ها ۴۸ بیت است ساخته می‌شوند.

۱–۱۷ آدرس IEEE 802

شناسه‌های سنتی واسطهای کارت شبکه از یک آدرس ۴۸ بیتی برای شناساندن خود استفاده می‌کنند. این آدرس از دو بخش چهار بیتی تشکیل شده است که ۲۴ بیت نخست آن مربوط به شرکت سازنده بوده و ۲۴ بیت سمت راست آن مربوط به شناسه محصول به خصوص می‌باشد. به ۲۴ بیت اول در اصطلاح **Company ID** یا **Manufacture ID** و به ۲۴ بیت دوم در اصطلاح **Extension ID** یا **Board ID** گفته می‌شود. ترکیب بخش **Company ID** که به صورت یکتا به هر کارخانه سازنده کارت شبکه اختصاص می‌یابد و بخش **Board ID** که به صورت یکتا به هر کارت شبکه تولید شرکت اختصاص می‌یابد، یک آدرس منحصر به فرد ۴۸ بیتی در جهان تولید می‌کند. آدرس تولید شده به آدرس فیزیکی یا آدرس سخت‌افزاری و یا آدرس **MAC**[1] موسوم است. شکل ۱–۹ نمایی از ساختار **MAC** را نشان می‌دهد.



شکل ۱–۹: ساختار آدرسی **MAC**

[1] **Medium Access Control**

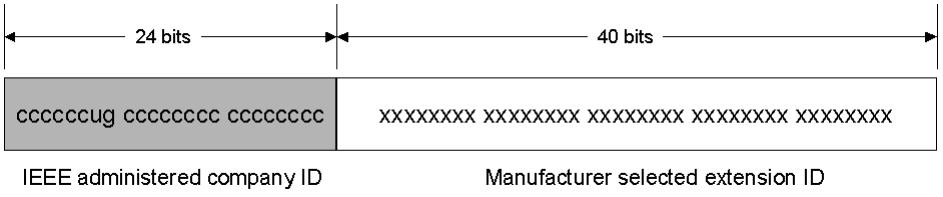
دو بیت از ۴۸ بیت مربوط به آدرس **MAC** از پیش تعریف شده می‌باشند که عبارتند از:

- بیت عمومی/محلی (بیت **U/L**): هفتمین بیت از سمت چپ آدرس‌های **MAC** مربوط به مشخص نمودن نوع آدرس از نظر محلی یا عمومی بودن آن است. این بیت که **U/L** نام دارد اگر صفر باشد نشان‌دهنده آن است که آدرس تولید شده توسط **IEEE** کنترل می‌شود و یک آدرس عمومی است و اگر یک باشد یعنی اینکه آدرس تولیدشده به صورت محلی مدیریت می‌شود. این بیت با علامت **u** در شکل ۱-۹ نشان داده شده است.
- بیت فردی/گروهی (بیت **I/G**): هشتمین بیت از سمت چپ در ۴۸ بیت آدرس **MAC** بیت فردی/گروهی نام دارد که مشخص کننده نوع آدرس از نظر فردی **(unicast)** یا گروهی بودن **(multicast)** می‌باشد. اگر این بیت صفر باشد آدرس مذکور یک آدرس **unicast** می‌باشد و در غیر این صورت آدرس مذکور متعلق به یک گروه **multicast** است. این بیت در شکل ۱-۹ با علامت **g** نشان داده شده است.

در حالت عادی هر دو بیت مذکور در آدرس‌های **MAC** صفر می‌باشند که مشخص‌کننده یک آدرس عمومی و **unicast** می‌باشند.

۱-۱۸ آدرس IEEE EUI-64

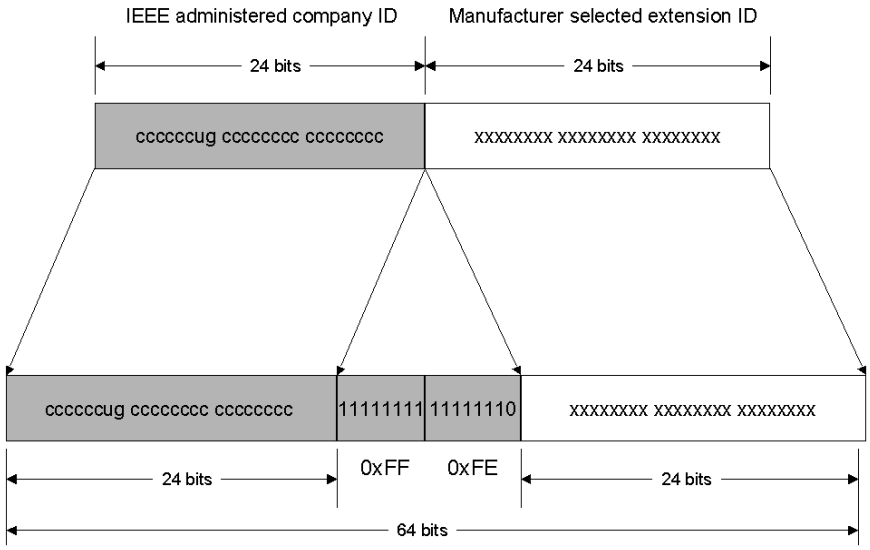
IEEE EUI-64 یک ساختار جدید برای آدرس‌دهی واسطهای شبکه معرفی می‌کند. در این ساختار جدید بخش **Company ID** همچنان ۲۴ بیت باقی می‌ماند اما بخش **Extension ID** به ۴۰ بیت افزایش می‌یابد که باعث به وجود آمدن آدرس‌های بیشتر برای محصولات کارخانه‌ها می‌شود. ساختار بیتهای **U/L** و **I/G** همچنان همانند ساختار این بیتها در **MAC** می‌باشد. شکل ۱-۱۰ چگونگی ساختار آدرس **IEEE EUI-64** را نشان می‌دهد.



شکل ۱-۱۰: ساختار آدرس‌دهی **IEEE EUI-64**

۱–۱۹ نگاشت آدرس MAC به آدرس EUI-64

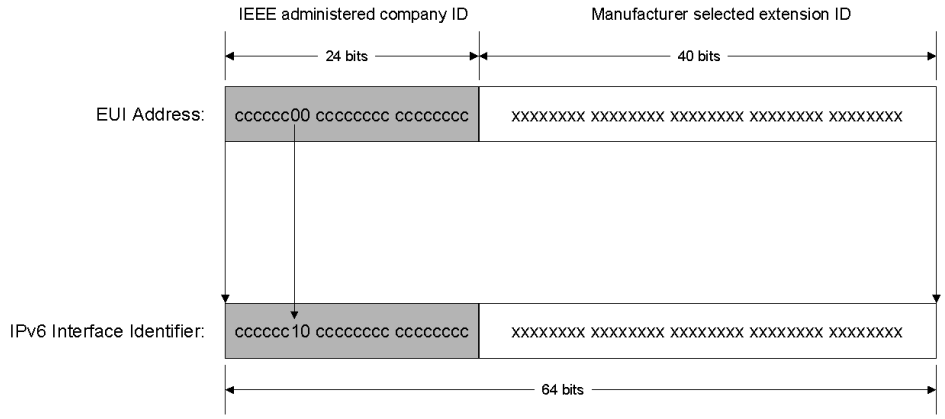
برای ساختن آدرس **EUI-64** از روی آدرس **MAC**، مطابق شکل ۱–۱۱، شانزده بیت **11111111 11111110 (0xFFFE)** بین بخش‌های **Company ID** و **Board ID** اضافه می‌شود.



شکل ۱–۱۱: ساختن آدرس **EUI-64** از روی آدرس **MAC**

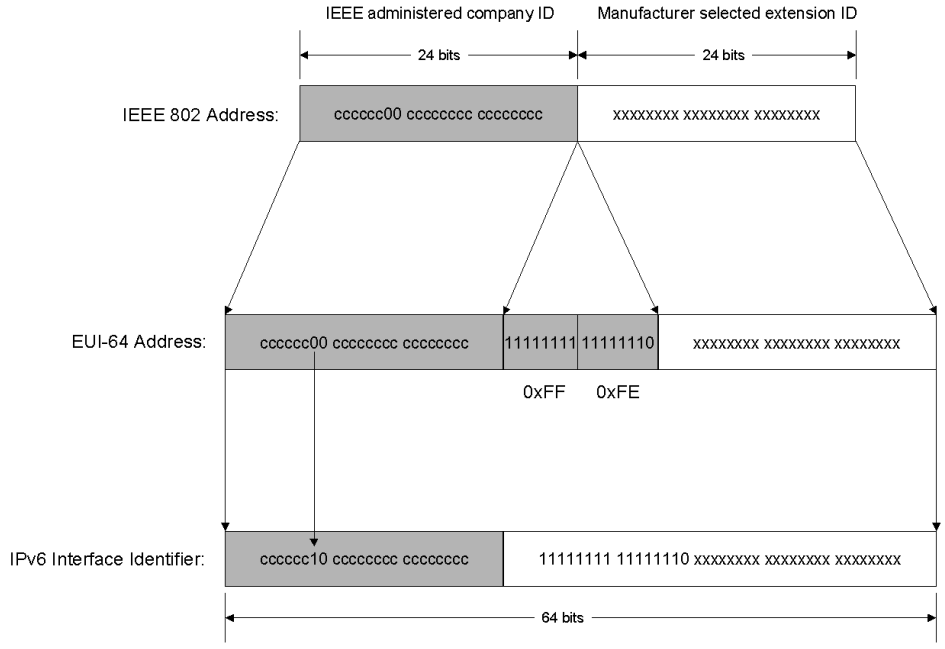
۱–۲۰ نگاشت آدرس EUI-64 به بخش شناسه واسط در IPv6

برای اینکه شناسه واسط **IPv6** را به دست بیاوریم بیت مربوط به **U/L** را در **EUI-64** معکوس می‌کنیم به گونه‌ای که بیت صفر به یک و بیت یک به صفر تبدیل شود. شکل ۱–۱۲ چگونگی این امر را نشان می‌دهد.



شکل ۱–۱۲: تبدیل **EUI-64** به شناسه واسط **IPv6**

برای تبدیل یک آدرس **IEEE 802** یا همان **MAC** به یک شناسه واسط شبکه **IPv6** ابتدا این آدرس را به صورت **EUI-64** تبدیل کرده و سپس آنرا به شناسه واسط شبکه نگاشت می‌نماییم. توضیح بهتر این نکته را می‌توان در شکل ۱–۱۳ مشاهده کرد.



شکل ۱–۱۳: تبدیل آدرس **MAC** به شناسه واسط **IPv6**

۱–۲۱ مثالی برای تبدیل آدرس

فرض کنید میزبان **A** دارای آدرس فیزیکی یا همان **MAC** معادل **00-AA-00-3F-2A-1C** می‌باشد. برای ساخت شناسه واسط **IPv6** ابتدا آنرا به صورت **EUI-64** در می‌آوریم. یعنی **FFFE** را بین بایتهای سوم و چهارم آن اضافه می‌کنیم تا آدرس **00-AA-00-FF-FE-3F-2A-1C** به دست آید. حال بیت **U/L** را که هفتمین بیت از سمت چپ می‌باشد را معکوس می‌کنیم. در این مثال بایت اول بهصورت بیتی برابر **00000000** می‌باشد که با معکوس کردن بیت هفتم به **00000010 (0x02)** خواهیم رسید. بنابراین نتیجه نهایی تبدیل آدرس به صورت **02-AA-00-FF-FE-3F-2A-1C** خواهد بود که اگر به شکل اعداد مبنای ۱۶ و جداسازی دونقطه نمایش داده شوند نتیجه به صورت **2AA:FF:FE3F:2A1C** می‌شود. بنابراین به طور مثال آدرس اتصال محلی برای یک آدرس **MAC** معادل **00-AA-00-3F-2A-1C** برابر **FE80::2AA:FF:FE3F:2A1C** می‌شود.

۱–۲۲ آدرس شناسه واسط موقتی

در دنیای امروز کاربران اینترنت عموما از طریق پروتکل‌هایی نظیر پروتکل نقطه به نقطه **(PPP)** و پروتکل کنترل پروتکل اینترنت **(IPCP)** به ارایه‌دهندگان خدمات اینترنتی **(ISP)** متصل می‌شوند. هر زمان که کاربری به یک **ISP** متصل می‌شود ممکن است آدرس **IPv4** جدیدی دریافت کند. از این رو پیگیری ارتباطات کاربران از طریق آدرس‌های مبدا کاری دشوار خواهد بود.

در **IPv6** هنگامی که یک کاربر به **ISP** متصل می‌شود یک پیشوند ۶۴تایی شبکه از مسیریاب یا مکانیزم‌هایی نظیر **DHCPv6** دریافت می‌کند. حال اگر شناسه واسط شبکه همواره از **EUI-64** و آدرس فیزیکی واسط شبکه به دست آید در این صورت امکان پیگیری ارتباط کاربران با توجه به منحصر به فرد بودن آدرس **EUI-64** فراهم می‌شود. برای رفع این مشکل و برای اینکه همانند گذشته کاربران به صورت نامشخص از ارتباطات بهره بگیرند مطابق **RFC 3041** یک آدرس جایگزین شناسه واسط **IPv6** به صورت تصادفی که همواره در طول زمان تغییر می‌کند ایجاد می‌شود و مورد استفاده قرار می‌گیرد.

آدرس شناسه واسط اولیه به صورت تصادفی ایجاد می‌شود. برای دستگاههایی که امکان نگهداری آدرس‌های قبلی تولیدشده را ندارند این آدرس در هر شروع مجدد **IPv6** دوباره به صورت تصادفی

ایجاد می‌شود. برای دستگاههایی که امکان ذخیره و نگه‌داری این آدرس را دارا باشند در هر شروع مجدد **IPv6** مراحل زیر برای ساخت آدرس جدید اعمال می‌شود:

- ابتدا آدرس قبلی موجود در حافظه فراخوانی شده، آدرس **EUI-64** آن مشخص می‌شود.
- روی مقدار به دست آمده یک عمل کد کردن **MD5** که یک طرفه می‌باشد انجام می‌پذیرد.
- ۶۴ بیت انتهایی عدد به دست آمده برای ذخیره در حافظه برای ساخت آدرس بعدی در نظر گرفته می‌شود.
- ۴۶ بیت ابتدایی نیز به عنوان آدرس **EUI-64** جدید استفاده می‌شود و هفتمین بیت سمت چپ آن صفر می‌شود تا به عنوان یک آدرس عمومی **unicast** مورد استفاده قرار گیرد.

آدرس‌های **EUI-64** به دست آمده از این روش، آدرس‌های شناسه واسط موقتی نامیده می‌شوند. اینگونه آدرس‌ها برای پیشوندهای عمومی **IPv6** که توسط مسیریاب‌ها یا ابزار دیگر به صورت **stateless** به شبکه معرفی می‌شوند مورد استفاده قرار می‌گیرند. زمان اعتبار این آدرس نیز از روی کمترین مقدار بین دو مورد زیر به دست می‌آید:

- زمان تنظیم شده در معرفی کننده شبکه که پیشوند عمومی آدرس را معرفی نموده است.
- زمان پیش فرض یک هفته برای **valid lifetime** و یک روز برای **preferred lifetime**

در صورتی که هر یک از زمان‌های مذکور به پایان برسد آدرس **IPv6** جدید از نو ساخته می‌شود.

۱–۲۳ نگاشت آدرس‌های IPv6 multicast به آدرس‌های اترنت

هنگامی که یک بسته به آدرس **multicast** فرستاده می‌شود آدرس **MAC** مقصد به صورت **33-33-mm-mm-mm-mm** تنظیم می‌شود که در آن **mm-mm-mm-mm** مطابق شکل ۱–۱۴ نشان‌دهنده ۳۲ بیت انتهایی آدرس **multicast** می‌باشد.

شکل ۱-۱۴: نگاشت آدرس‌های **IPv6 multicast** به آدرس‌های اترنت

برای اینکه کارت شبکه‌های موجود در یک اتصال یا همان واسطهای موجود در یک اتصال بتوانند بسته‌های **multicast** را دریافت نمایند می‌توان آدرس‌های **MAC** مورد نظر را در جدول **MAC** مربوط به کارت شبکه ذخیره نمود. هنگامی که یک بسته اترنت توسط کارت شبکه دریافت شود درصورت وجود همخوانی بین آدرس **MAC** مقصد و آدرس **MAC** موجود در جدول این بسته به لایه‌های بالاتر ارسال خواهد شد.

به طور مثال یک میزبان با آدرس فیزیکی **00-AA-00-3F-2A-1C** که دارای آدرس اتصال محلی **FE80::2AA:FF:FE3F:2A1C** است، آدرس‌های زیر را در جدول **MAC** خود ذخیره می‌کند:

- آدرس **33-33-00-00-00-01** که معادل آدرس تمامی نقطه‌ها در اتصال محلی می‌باشد (یعنی همان آدرس **FF02::1**).
- آدرس **33-33-FF-3F-2A-1C** که منطبق بر آدرس **multicast** نقطه درخواستی یا همان **FF02::1:FF3F:2A1C** می‌باشد.

آدرس‌های **multicast** دیگر نیز بسته به مورد در جدول اضافه یا کم می‌شوند.

۱-۲۴ معادل‌های IPv4 در IPv6

جدول ۱-۱ معادل‌های **IPv4** مرتبط با **IPv6** را نشان می‌دهد.

جدول ۱-۱: معادل‌های **IPv4** در **IPv6**

IPv4 Address	**IPv6 Address**
Internet address classes	Not applicable in IPv6
Multicast addresses (224.0.0.0/4)	IPv6 multicast addresses (FF00::/8)
Broadcast addresses	Not applicable in IPv6
Unspecified address is 0.0.0.0	Unspecified address is ::
Loopback address is 127.0.0.1	Loopback address is ::1
Public IP addresses	Global unicast addresses
Private IP addresses (10.0.0.0/8, 172.16.0.0/12, and 192.168.0.0/16)	Site-local addresses (FEC0::/10)
Autoconfigured addresses (169.254.0.0/16)	Link-local addresses (FE80::/64)
Text representation: Dotted decimal notation	Text representation: Colon hexadecimal format with suppression of leading zeros and zero compression. IPv4-compatible addresses are expressed in dotted decimal notation.
Network bits representation: Subnet mask in dotted decimal notation or prefix length	Network bits representation: Prefix length notation only

فصل دوم:

سرویس دهندهٔ DNS و IPv6

۲–۱ مقدمه

آدرس‌های طولانی **IPv6** وجود سیستمی برای نگاشت نام‌های دامنه به آدرس‌های اینچنینی را بیش از پیش لازم می‌سازد. انسآن‌ها به خاطر ساختار ذهنیشان امکان به خاطر سپردن اعداد آدرس **IPv6** را در سطح وسیع ندارند و این در حالی است که نام‌ها و دامنه‌ها را باتوجه به قراین ذهنی و محیطی به سادگی به خاطر می‌سپرند و در موقع لزوم آن را به یاد می‌آورند. چنین سرویسی در دنیای اینترنت و شبکه‌های کامپیوتری **DNS** [1] نام دارد. در این نوشتار درمی‌یابیم که **DNS** چگونه برای تشخیص[2] نام یک رایانه در یک شبکه محلی (**LAN**) و یا یک سرویس دهنده[3] در شبکه سراسری اینترنت به کار می رود. همچنین تعریف دامنه و **Zone** و دامنه های متداول و اصلی موجود در محیط اینترنت و ثبت منابع توضیح داده خواهد شد. این فصل مقدمه ای برای فصل های بعدی که چگونگی نصب و راه اندازی یک سرویس دهنده **DNS** را در سیستم عامل ویندوز ۲۰۰۳ نشان می‌دهد می‌باشد. ویندوزهای ۲۰۰۳ دارای یک بخش اضافه برای نصب **DNS** می‌باشد. در این بخش آشنایی با **DNS** و چگونگی پیاده سازی آن را بر روی ویندوز ۲۰۰۳ ملاحظه می فرمایید. تا پایان فصل توانایی تشخیص اجزا **DNS**، نصب و شکل دادن **DNS** و رفع عیب **DNS** بر روی ویندوز ۲۰۰۳ ارایه می‌شود.

۲–۲ معرفی DNS

DNS شبیه به یک دفترچه تلفن می‌باشد. هر رایانه بر روی اینترنت هم نام‌میزبان[4] و هم آدرس **IP** را دارا می‌باشد. بصورت نوعی، وقتیکه شما می‌خواهید با کامپیوتر دیگری ارتباط برقرار نمایید، شما باید نام‌میزبان را وارد نمایید. کامپیوتر شما با سرویس دهنده **DNS** ارتباط برقرار نموده و برای آن اسم میزبان شما یک شماره **IP** واقعی ارایه می‌دهد. که این شماره **IP** برای اتصال از دور به آن کامپیوتر میزبان استفاده می‌شود. در این بخش معماری و ساختار **DNS** تشریح می‌شود.

۲–۲–۱ دلیل وجود *DNS*

قبل از پیاده‌سازی **DNS**، می‌باید فایل‌هایی که شامل لیستی از نام‌های کامپیوترها و آدرس **IP** متناظرشان می باشد، آماده شود. بر روی اینترنت این فایل‌ها به صورت مرکزی مدیریت می‌شوند و برای هر ناحیه

[1] **Domain Name Service**
[2] **Resolve**
[3] **Server**
[4] **Host Name**

یک نسخه از این فایل‌ها می‌باید به صورت متناوب دریافت شود. در مواردی که تعداد کامپیوترها افزایش یابند، مدیریت این امر غیر ممکن شده و مشکل ساز می‌شود. بر اساس یک نتیجه، **DNS** برای جایگزینی منحصر به فرد فایل مدیریت شده میزبآن‌ها طراحی شده است. **DNS** خدماتی است برای ترجمه کردن نام‌های اینترنتی به آدرس‌های **IP**. به طور مثال **www.microsoft.com** به شماره **207.46.130.149** ترجمه می‌شود. **DNS** همانند یک دفترچه تلفن می‌باشد. همانگونه که در یک دفترچه تلفن با مراجعه به اسم افراد یا اسم شرکتها شماره تلفن مربوطه را بدست می‌آورید در یک **DNS** نیز با رجوع به اسم کامپیوتر ویا سرویس دهنده می‌توان آدرس **IP** آن کامپیوتر و یا سرویس دهنده را جهت ایجاد ارتباط با آن بدست آورید.

پیاده سازی سرویس دهنده **DNS** برای سیستم‌های **Microsoft** در سیستم عامل‌های **Windows NT** ویا **Windows 2000** و یا **Windows 2003** امکان پذیر می‌باشد.

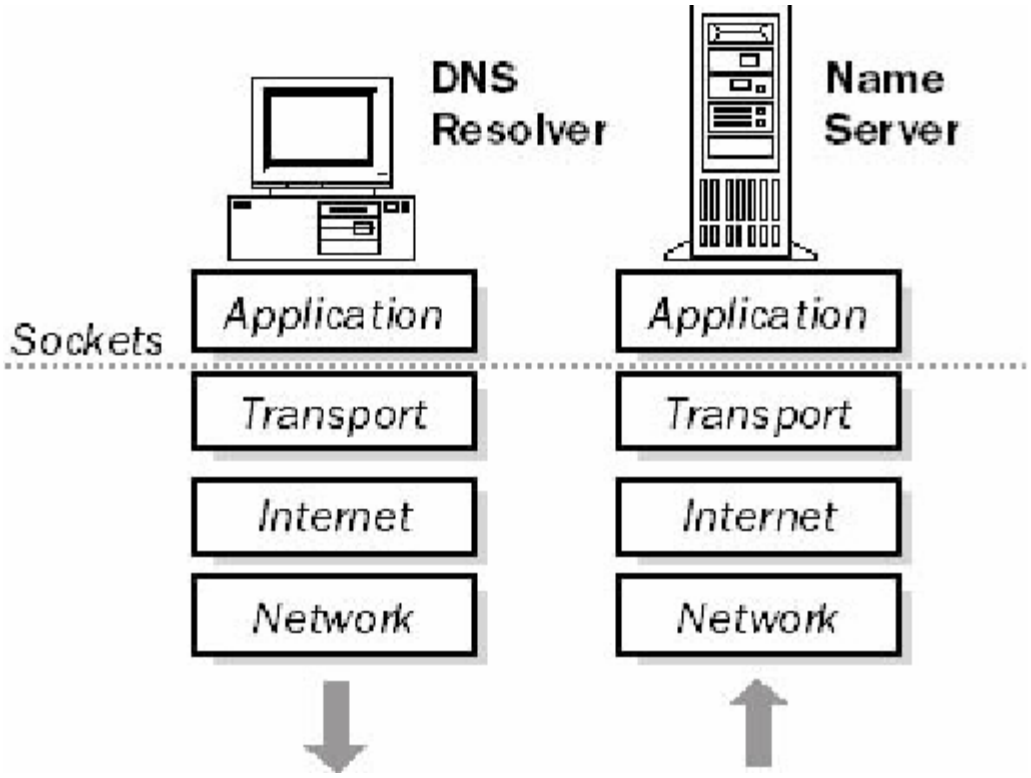
۲-۲-۲ *DNS و Windows*

علاوه بر تحلیل نام‌های اینترنتی، **DNS** سرویس اولیه ویندوز ۲۰۰۳ می باشد. این سیستم عامل بسیار قابل اطمینان، سلسله مراتبی، توزیع یافته و دارای پایگاه داده‌ای قابل گسترش می‌باشد. مشتریان[1] ویندوز۲۰۰۳ برای تشخیص نام‌ها و دریافت خدمات محلی از **DNS** استفاده می‌نمایند. در ویندوز۲۰۰۳ یک سرویس دهنده **DNS** پیاده سازی شده که توانایی تبادل اطلاعات با سایر سرویس دهنده‌های **DNS** استاندارد موجود در شبکه دارد.

۲-۲-۳ *عملکرد DNS*

هدف پایگاه داده‌های **DNS** ترجمه نام‌های کامپیوترها به آدرس **IP**ها می‌باشد بطوریکه در شکل ۲-۱ نشان داده شده است. در **DNS** مشتریان تحلیلگرها و سرویس دهنده‌ها سرویس دهنده‌های اسامی نامیده می‌شوند.

[1] **Clients**



شکل۲-۱ تحلیلگرها و سرویس دهنده های نام

DNS از سه جز تشخیص‌دهنده، سرویس دهنده اسامی و فضای حوزه اسامی[1] کار می‌نماید. در ارتباط ساده با یک سرویس دهنده **DNS**، درخواست تشخیص یک نام به سرویس دهنده ارسال می‌شود. سرویس دهنده اسامی در صورت وجود اطلاعات مناسب در سرویس دهنده، به درخواست پاسخ می‌دهد ویا یک اشاره‌گر به سرویس دهنده اسامی بعدی می‌فرستد و یا اگر نتواند پاسخ مناسبی برای درخواست پیدا نماید، پیغام خطا را ارسال می‌نماید. **DNS** بر روی لایه کاربردی[2] (لایه پنجم از استاندارد **TCP/IP** که لایه ایجاد ارتباط با کاربر شبکه می‌باشد و در این لایه سیستم عامل و نرم افزارهای کاربردی واقع است، بنابراین سیستم عامل نقش اصلی را در قدرت و توانمندی سرویس دهنده **DNS** ایفا می‌نماید) نگاشت می‌شود و از **UDP**[3] و **TCP**[4] بعنوان لایه‌های زیرین استفاده می‌نماید. برای افزایش بازدهی، تشخیص دهنده‌ها جستجو را با پروتکل **UDP** به سرویس دهنده‌های

[1] **Domain Name**
[2] **Application Layer**
[3] **User Datagram Protocol**
[4] **Transmission Control Protocol**

اول می فرستند، سپس چنانچه برش[1] داده‌های برگشتی نیاز باشد برای دسته بندی مجدد از **TCP** استفاده می‌نماید.

۲-۲-۴ تشخیص دهنده‌ها[2]

تشخیص‌دهنده‌ها، اطلاعات آدرسی یکی از مشتریان را برای سایر کامپیوترهای شبکه آماده می‌نمایند. وظیفه تشخیص‌دهنده‌ها ردکردن اسامی درخواستی بین لایه‌های کاربردی[3] و سرویس‌دهنده‌های اسامی می باشد. درخواست نام شامل یک روال همچون آدرس **IP** در **Web** می‌باشد. تشخیص‌دهنده در لایه کاربردی ساخته می‌شود و یا بر روی کامپیوتر میزبان به صورت یک روال کتابخآن‌های عمل می‌نماید. تشخیص‌دهنده‌ها برای افزایش کارایی ابتدا درخواستها را بر روی **UDP** ارسال نموده و سپس اگر برش داده‌های بازگشتی رخ دهد، دسته بندی مجدد توسط **TCP** انجام می‌پذیرد.

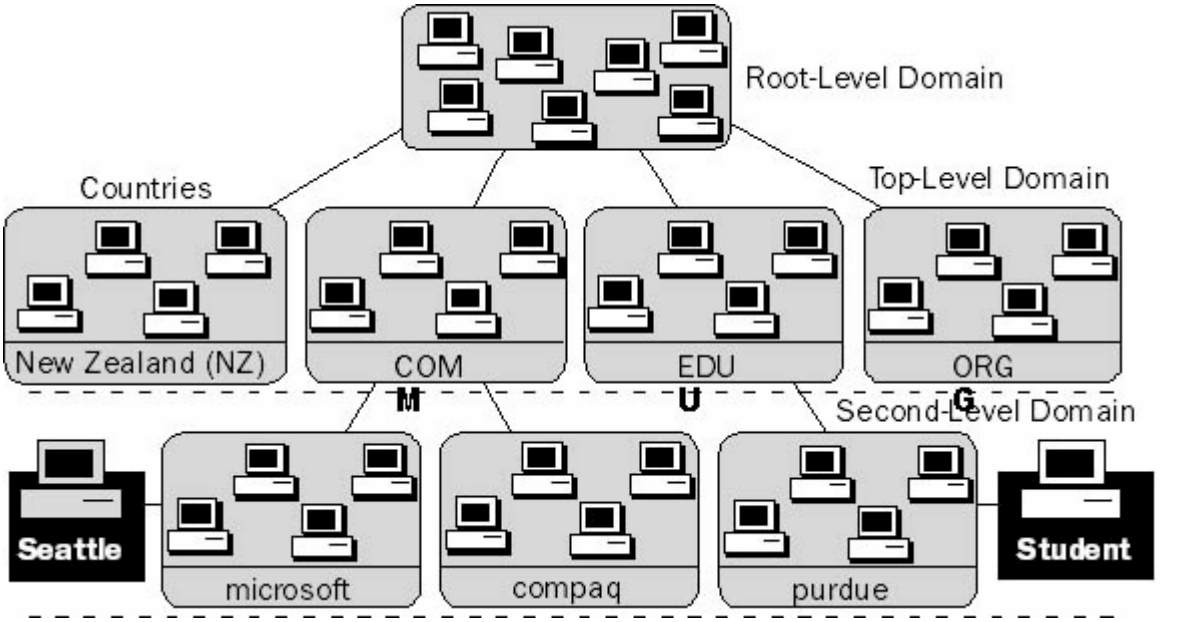
۲-۲-۵ سرویس‌دهنده‌های نام[4]

یک سرویس‌دهنده اسم شامل اطلاعات آدرس در مورد سایر کامپیوترهای شبکه می‌باشد. این اطلاعات می‌تواند به کامپیوترهای مشتری داده شود تا یک درخواست برای سرویس دهنده نام بسازد. اگر سرویس‌دهنده نتواند نام درخواستی را تشخیص دهد، می‌تواند درخواست را به سرویس‌دهنده دیگری ارسال نماید. سرویس‌دهنده‌های اسامی در سطوح مختلف گروه گروه می‌شوند که نام هر گروه را دامنه یا حوزه[5] می‌نامند. یک حوزه یک گروه منطقی[6] از کامپیوترها در داخل یک شبکه بزرگ می‌باشد. دسترسی به هر کامپیوتر در یک گروه توسط یک سرویس دهنده همان مجموعه کنترل می‌شود.

۲-۲-۶ ساختار *DNS*

فضای دامنه اسامی یک گروه‌بندی سلسله مراتبی مطابق شکل ۲-۲ دارد.

[1] **Truncation**
[2] **Resolvers**
[3] **Application Layer**
[4] **Name Servers**
[5] **Domain**
[6] **Logical**



شکل ۲-۲ تفکیک سطوح در فضای دامنه اسامی

۲-۲-۷ دامنه‌های سطح ریشه

دامنه‌ها سطوح متفاوتی از اختیارات و توانایی‌ها را در یک ساختار سلسله مراتبی معین می‌نمایند. راس این ساختار سلسله مراتبی ریشه دامنه نام دارد. ارجاعها به ریشه دامنه توسط یک علامت "." جدا می‌شود. در حال حاضر در دنیا سرویس‌دهنده نام دامنه‌ای که در بستر **IPv6** و در سطح ریشه ارایه خدمات نماید وجود ندارد.

۲-۲-۸ دامنه‌های سطح بالا

در نام‌گذاری سایتهای موجود، برای راحتی شناسایی واحدها و سازمان‌ها از یکدیگر (از لحاظ نوع عملکرد و ساختار اداری و اهداف تجاری) نام‌های دامنه سطوح بالای متفاوتی برگزیده شده است. این امر موجب تفکیک و تمیز سازمان‌های دولتی، غیر انتفاعی، تجاری، تحقیقاتی و دانشگاهی و ... از یکدیگر می‌شود و موجب راحتی جستجوی سایتها و یا انتخاب صحیح در ارایه اعتبار و یا تبادل اطلاعات دانشگاهی و فنی می‌شود.

در زیر، نام‌های دامنه‌های سطح بالای متداول و ارگآن‌ها یا سازمان‌های مربوطه آمده است:

- ارگآن‌های تجاری **com**
- انستیتوهای تحصیلی و دانشگاهی **edu**
- سازمان‌های غیر انتفاعی **org**

- شبکه‌ها (فقرات اینترنت) **net**
- ارگآن‌های غیرنظامی دولتی **gov**
- ارگآن‌های نظامی دولتی **mil**
- شماره‌های تلفن **num**
- معکوس **arpa**
- کد دوحرفی کشوری **xx**

سطح بالایی دامنه‌ها می‌تواند شامل سطح دومی از دامنه‌ها و میزبآن‌ها باشد.

۲-۲-۹ سطح دوم دامنه‌ها

سطح دوم دامنه‌ها می‌تواند هم شامل میزبآن‌ها و هم شامل سایر دامنه‌های دیگر (که زیرناحیه نام دارد) باشد. به عنوان مثال حوزه مایکروسافت، **Microsoft.com**، می‌تواند شامل کامپیوترهایی نظیر **ftp.microsoft.com** و زیرناحیه‌هایی همچون **dev.microsoft.com** باشد. زیرناحیه **dev.microsoft.com** می‌تواند شامل میزبآن‌هایی همچون **netserver.dev.microsoft.com** می‌باشد.

۲-۲-۱۰ اسامی میزبان

اسم دامنه با اسم میزبان برای خلق یک نام ناحیه کاملا مناسب برای کامپیوتر[1] مورد استفاده قرار می‌گیرد. **FQDN** نام میزبان می‌باشد که در ادامه **(.)** قرار گرفته و در ادامه نامه دامنه میآید. برای مثال در جاییکه **fileserver1** نام میزبان می‌باشد و **Microsoft.com** نام دامنه می‌باشد، **FQDN** می‌تواند **fileserver1.microsoft.com** باشد.

۲-۲-۱۱ Zoneها

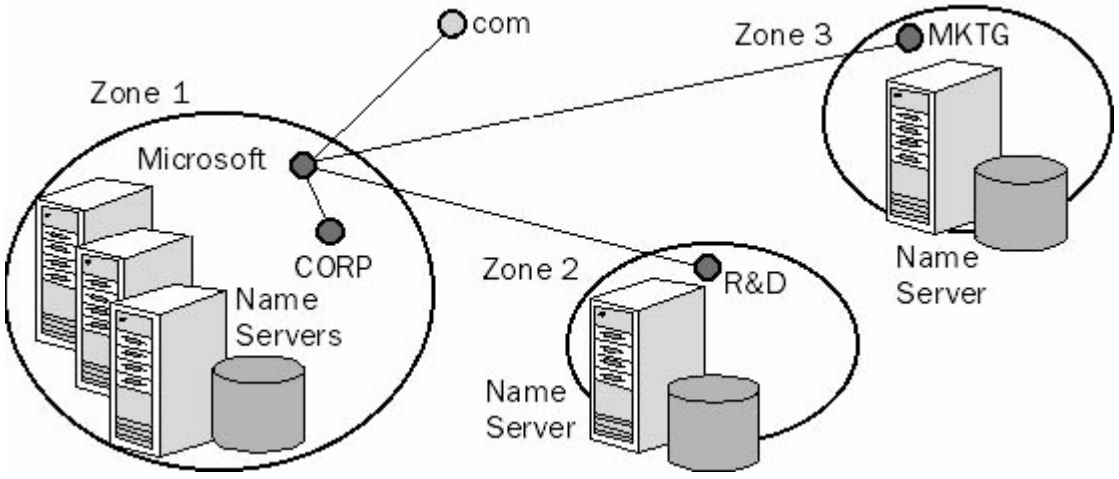
واحد مدیریت برای **DNS**، **Zone** می‌باشد. یک **Zone** یک زیر شاخه برای پایگاه داده‌های **DNS** می‌باشد که تنها راه مدیریت تفکیک شده برای آن می‌باشد. این می‌تواند شامل یک دامنه واحد یا یک دامنه با زیردامنه‌هایش باشد. در سطوح پایین‌تر زیر دامنهٔ یک **Zone**، می‌توان **Zone**های تفکیک شده و مجزای دیگری داشت.

[1] **Fully Qualified Domain name (FQDN)**

۲-۲-۱۲ سرپرستی Zone

Zone سرپرستی بخشی از فضای ناحیه اسم می‌باشد که سرویس دهنده نام می‌تواند برای آن زیر شاخه تعریف نماید. سرویس دهنده نام تمامی آدرس‌های نگاشت شده بر روی فضای ناحیه اسمی که داخل **Zone** قرار دارد و پاسخهای مشتریان برای آن نام‌ها را در خود ذخیره می‌نماید. سرویس دهنده نام سرپرست **Zone** حداقل یک دامنه را پوشش می‌دهد. این دامنه به دامنه اصلی **Zone** ارجاع می‌دهد. همچنین برای سرپرستی بیش از یک **Zone** می‌توان سرویس دهنده دومی در شبکه وجود داشته باشد که اطلاعات سرویس دهنده **DNS** اولیه را در خود ذخیره نماید. این **Zone** را **Zone** انتقال می‌نامند.

همانطوریکه در شکل ۲-۳ ملاحظه می‌شود، **Microsoft.com** یک دامنه می‌باشد ولیکن کل دامنه توسط یک **Zone File** کنترل نمی‌شود. بخش از دامنه در یک **Zone** دیگر و با نام **dev.microsoft.com** تعریف شده است. خرد کردن یک دامنه به چندین **Zone files** امکان دارد برای توزیع مدیریت دامنهٔ بخش‌های مختلف یک سازمان یا برای بهبود تکرارگرایی داده‌های ضروری باشد.



شکل۲-۳ دامنه به چندین **Zone** تقسیم شده‌است

۲-۲-۱۳ نقش سرویس دهنده نام

سرویس دهنده‌های اسامی برای چگونگی ذخیره و پشتیبانی از پایگاه داده‌های اسامی می‌توانند با نقش‌های متفاوتی تنظیم شوند. یک سرویس دهنده **DNS** مایکروسافت می‌تواند سرویس دهنده **DNS** اولیه و یا ثانویه برای سرویس دهنده **DNS** دیگر مایکروسافت باشد و یا سرویس دهنده **DNS** تحت یک سیستم عامل دیگری همچون **UNIX** راه‌اندازی شود. حداقل تعداد سرویس دهنده **DNS** که در هر

Zone نیاز می‌باشد دو سرویس دهنده، یکی اولیه و دیگری ثانویه می‌باشد. هم سرویس دهنده اولیه و هم ثانویه نیاز به افزونگی[1] پایگاه داده‌ها و یک درجه از دامنه خطا[2] دارند.

۲-۲-۱۴ سرویس دهنده‌های نام اولیه

یک سرویس دهنده اسم اولیه یک سرویس دهنده **DNS** می‌باشد که به **Zone**هایش از فایل‌های پایگاه داده‌های **DNS** محلی، داده ارایه می‌دهد. وقتیکه یک تغییر در داده **Zone** رخ می‌دهد، همچون وکالت دادن[3] یک بخش از **Zone** به سرویس دهنده**DNS** دیگر یا اضافه کردن میزبان به **Zone**، تغییرات باید در سرویس دهنده **DNS** اولیه با ورود اطلاعات به فایل **Zone** محلی، اعمال شود.

۲-۲-۱۵ سرویس دهنده‌های نام ثانویه

یک سرویس دهنده اسم ثانویه برای آن **Zone** که دارای اختیارات می‌باشد، فایل داده‌های **Zone** را از سرویس دهنده **DNS** اولیه می‌گیرد. در روال ذکر شده، سرویس دهنده **DNS** اولیه یک نسخه از فایل **Zone** را برای سرویس دهنده **DNS** ثانویه ارسال می‌نماید.

سه دلیل برای وجود سرویس دهنده‌های اسم ثانویه وجود دارد:

- **افزونگی**: برای هر **Zone** نیاز به یک سرویس دهنده نام اولیه و یک سرویس دهنده نام ثانویه می‌باشد. کامپیوترها می‌باید تا حد ممکن مستقل از هم باشند. بطورکلی طرح استفاده از سرویس دهنده‌های اولیه و ثانویه در دو زیرشبکه[4] متفاوت بدین دلیل می‌باشد که در صورت بروز مشکل در یکی از زیرشبکه‌ها، پشتیبانی از درخواستهای **DNS** ادامه داشته باشد.
- **دسترسی سریعتر برای محل‌های دور**: اگر شما یک سری مشتری در محلی دور داشته باشید، داشتن سرویس دهنده نام ثانویه (یا سرویس دهنده ثانویه دیگری برای زیردامنه‌ها) مانع از آن می‌شود که تشخیص نام برای این مشتریان با سرعت پایین صورت پذیرد.
- **کاهش بار شبکه**: سرویس دهنده نام ثانویه بار بر روی سرویس دهنده اولیه را کم می‌نماید.

از آنجاییکه اطلاعات هر **Zone** در فایل‌هایی مجزا ذخیره می‌شود، طراحی این سرویس دهنده‌های اولیه و ثانویه در یک سطح **Zone** انجام می‌پذیرد. این بدین معنی است که یک سرویس دهنده نام خاص می‌تواند برای یک **Zone** معین سرویس دهنده اولیه و برای **Zone** دیگر سرویس دهنده ثانویه باشد.

---

[1] **Redundancy**
[2] **Fault Tolerance**
[3] **Delegating**
[4] **Subnet**

۲-۲-۱۶ سرویس دهنده‌های نام اصلی[1]

وقتیکه شما یک **Zone** را برای یک سرویس دهنده نام بعنوان یک **Zone** ثانویه تعریف می‌نمایید، باید یک سرویس دهنده نام دیگری را برای بدست آوردن اطلاعات **Zone** طراحی نمایید. منبع اطلاعات **Zone** برای یک سرویس دهنده نام ثانویه در یک **DNS** سلسله مراتبی در یک سرویس دهنده نام اصلی قرار دارد. یک سرویس دهنده نام اصلی برای **Zone** متقاضی می‌تواند هم نقش سرویس دهنده نام اولیه و هم سرویس دهنده نام ثانویه را ایفا نماید. وقتیکه یک سرویس دهنده نام ثانویه راه‌اندازی می‌شود، با سرویس دهنده نام اصلی ارتباط برقرار کرده و اطلاعات ابتدایی برای شناسایی **Zone** به آن سرویس دهنده منتقل می‌شود.

۲-۲-۱۷ سرویس دهنده‌های ذخیره[2]

اگرچه سرویس دهنده‌های نام **DNS** درخواستهای تشخیص داده شده را در حافظه ذخیره می‌نمایند ولیکن سرویس دهنده‌های صرفا ذخیره تنها وظیفه ذخیره درخواستها و پاسخهای بازگشتی را دارند. به عبارت دیگر آن‌ها اعتباری در دامنه جز ذخیره کردن درخواستها و تشخیصهای انجام شده ندارند.

وقتیکه یک سرویس دهنده راه اندازی می‌شود، در ابتدا هیچگونه اطلاعاتی در داخل سرویس دهنده‌های صرفا ذخیره وجود ندارد و با گذشت زمان و تبادل درخواستها و تشخیصها در داخل **Zone** اطلاعات در داخل سرویس دهنده ذخیره می‌شود. با عملکرد این سرویس دهنده‌ها ترافیک کمتری بین سرویس دهنده‌ها حاکم می‌شود، چراکه بین سرویس دهنده‌ها **Zone Transfer** رخ نمی‌دهد. اینکه بین اتصال بین سایتها سرعت بالا باشد بسیار مهم است.

۲-۳ پشتیبانی از IPv6 در DNSهای جدید

طول زیاد آدرس‌های اینترنتی نسخه ششم یا همان **IPv6** لزوم استفاده از **DNS**ها هرچه بیشتر نمایان می‌سازد. بر این اساس چند پیشنهاد برای ارتقا استانداردهای موجود تعریف‌شده برای **DNS** مطرح و از آن میان دو پیشنهاد به صورت استاندارد تعریف و در **RFC**های شماره **1886** و **2874** منتشر شد.

[1] **Master Name Server**
[2] **Caching-Only Servers**

۲-۳-۱ *RFC 1886*

برای توسعه **DNS**های موجود دو نوع رکورد جدید بایستی در **DNS** تعریف شود تا علاوه بر خواسته‌های قبلی بتواند **IPv6** را به نام‌های اینترنتی و بالعکس نگاشت نماید.

۲-۳-۱-۱ رکورد AAAA

رکورد معرفی شده در **RFC 1886** که شماره نوع آن در استانداردهای مربوط به **DNS**، ۲۸ می‌باشد، رکورد **AAAA** می‌باشد که هر رکورد آن ۱۲۸ بیت آدرس می‌باشد. این رکورد اولین پیشنهاد موجود برای نگاشت نام‌های اینترنتی به آدرس‌های **IPv6** بود. برای وارد نمودن آدرس **IPv6** نیز باید از روش استاندارد نمایش **IPv6** با جداسازی دونقطه استفاده نمود.

۲-۳-۱-۲ دامنه IP6.INT

برای **IPv4** یک مکانیزم معکوس برای نگاشت آدرس‌های **IPv4** به آدرس اینترنتی وجود دارد. در این صورت مثلا می‌توان مشخص نمود که آدرس **100.101.102.103** معادل چه نام اینترنتی می‌باشد. برای این منظور مثلا در **DNS** یک دامنه معکوس **x.102.101.100** تعریف شده و مقادیر **x** برحسب مورد وارد می‌شود. برای **IPv6** نیز در **RFC** مذکور چنین مکانیزمی پیشنهاد شده است. بدین ترتیب که یک دامنه معکوس که شامل تمامی ارقام دامنه **IPv6** در شکل مبنای ۱۶ باشد و از کم‌ارزشترین تا پرارزشترین رقم مرتب شده باشد معرفی می‌شود. این ارقام با نقطه از هم جدا می‌شوند. به طور مثال آدرس **4321:0:1:2:3:4:567:89ab** به صورت

b.a.9.8.7.6.5.0.4.0.0.0.3.0.0.0.2.0.0.0.1.0.0.0.0.0.0.0.1.2.3.4.IP6.INT تعریف می‌شود.

۲-۳-۲ *RFC 2874*

در **RFC2874** جایگزینی برای روش معرفی‌شده در **RFC 1886** پیشنهاد شده است. این روش جایگزین در هنگام تعویض آدرس‌های **IPv6** و همچنین سرویس‌دهنده‌هایی که به چندین شبکه متفاوت متصل می‌باشند بهتر عمل می‌کند. به نظر می‌آید روش پیشنهادی در صورت پیاده‌سازی صحیح به صورت کامل جایگزین روش قبلی شود.

۲-۳-۲-۱ رکورد A6

در این روش به جای استفاده از رکورد **AAAA** رکورد جدید **A6** پیشنهاد شده است. مزیت این روش بیشتر برای برنامه‌نویسان و توسعه‌دهندگان **DNS** اشکار خواهد بود. در این روش نیز هر نام اینترنتی به یک آدرس از نوع **A6** که دارای معادل **IPv6** می‌باشد نگاشت می‌شود. همچنین می‌توان در این روش بجای نگاشت یک آدرس اینترنتی به یک آدرس **IPv6**، یک دامنه اینترنتی را به یک آدرس شبکه **IPv6** نگاشت نمود که در مورد قبل این امکان وجود نداشت.

۲-۳-۲-۲ دامنه IP6.arpa

در این روش بجای استفاده از **IP6.INT** از نام دامنه جدید **IP6.arpa** استفاده می‌شود. این روش در نمایش و نگاشت آدرس‌های **IPv6** به نام‌های اینترنتی بسیار کاراتر عمل می‌کند.

RFC 2874 یک منبع جامع و کامل برای معرفی روش پیشنهادی می‌باشد که برای درک بهتر موضوع و همچنین روش‌های بهبود روش‌های قبلی و چگونگی گذر از رکوردهای **AAAA** به **A6** می‌توانید آن را مطالعه نمایید.

۲-۴ ثبت انواع منابع[1]

یک پایگاه داده‌های **DNS** شامل یک یا چندین فایل‌های **Zone** مورد استفاده توسط سرویس دهنده **DNS** می‌باشد. هر **Zone** یک مجموعه از ثبتهای منابع ساختاریافته را حفظ می‌نماید بطوریکه این منابع توسط سرویسهای سرویس دهنده **DNS** حمایت می‌شوند. رکوردها یا همان ثبتهای زیادی بسته به مورد در **DNS** تعریف شده‌اند که در ادامه معروفترین آن‌ها ذکر خواهد شد.

۲-۴-۱ شکل ثبتهای منابع *DNS*

تمامی ثبت‌های منابع بر اساس فیلدهای زیر تعریف می‌شوند:

صاحب[2]: به دامنه نام **DNS** اتلاق می‌شود. این نام همان نامی می‌باشد که ثبت منابع در آن ناحیه قرار دارد.

زمان زنده ماندن[1] (TTL): تعداد شبکه‌هایی که یک **Packet** در شبکه اینترنتی طی می‌نماید و در نهایت این **Packet** در صورت نرسیدن به مقصد دور انداخته می‌شود.

[1] **Resource Records**
[2] **Owner**

کلاس: شامل متن معرف معین کننده کلاس ثبت منابع می‌باشد. برای مثال یک ردیف از **"IN"** معین می‌نماید که ثبت منابع متعلق است به کلاس اینترنت که تنها کلاسی است که توسط ویندوز ۲۰۰۳ پشتیبانی می‌شود.

نوع: شامل متن معرف معین کننده نوع ثبت منابع می‌باشد. بعنوان مثال یک **"A"** معرف ثبت منابعی است که اطلاعات آدرس میزبان را ذخیره می‌نماید.

داده‌های ثبت تعیین شده[۲]: یک فیلد متغیر شامل اطلاعات توصیف منابع می‌باشد. شکل این اطلاعات بر اساس نوع و کلاس ثبت منابع تغییر می‌نماید.

A

نگاشت آدرس میزبان ثبت منابع می‌باشد. یک دامنه نام **DNS** را بر روی آدرس ۳۲ بیتی یک پروتکل اینترنت نسخه ۴ (**IPv4**) را نشان می‌دهد.

Syntax:
owner class ttl A ***IP_v4_address***
Example:
host1.example.microsoft.com. ***IN*** *A* ***127.0.0.1***

AAAA

آدرس میزبان ثبت منابع برای **IPv6** و مطابق با **RFC 1886** می‌باشد. نگاشت‌های یک دامنه نام **DNS** را بر روی آدرس ۱۲۸ بیتی یک پروتکل اینترنت نسخه ۶ (**IPv6**) نشان می‌دهد.

Syntax:
owner class ttl *AAAA* ***IP_v6_address***
Example:
ipv6_host1.example.microsoft.com. ***IN*** *AAAA* ***4321:0:1:2:3:4:567:8bb***

CNAME[3]

نگاشت‌های یک نام دامنه **DNS** جایگزین را در بخش **صاحب دامنه**، به یک نام دامنه **DNS** اولیه (که در فیلد **Canonical_Name** تعیین شده است) را نشان می‌دهد. در داده‌های مورد نیازی که باید به یک نام دامنه **DNS** در فضای نام تشخیص داده شوند، استفاده می‌شود.

Syntax:
owner ttl class *CNAME* ***canonical_name***

---

[1] **Time to Live**
[2] **Record-specific data**
[3] **Canonical Name**

Example:
aliasname.example.microsoft.com. *CNAME* ***truename.example.microsoft.com***

NS[1]

نگاشت یک دامنه نام **DNS** در یک **صاحب دامنه** به نام سرویس دهنده‌های **DNS** میزبان معین شده (که در فیلد **name_server_domain_name** تعیین شده است) را نشان می‌دهد.

Syntax: ***owner ttl*** **IN** NS ***name_server_domain_name***
Example:
example.microsoft.com. IN NS nameserver1.example.microsoft.com

PTR[2]

نگاشت‌های **PTR** در داخل یک **Reverse Lookup Zone** مسوولیت نگاشت آدرس به نام را برعهده دارند. برای تولید نگاشت **PTR** ارقام آدرس **IP** به صورت معکوس نوشته می‌شوند و سپس **"in_addr.arpa"** به انتهای این ارقم افزوده می‌شود. برای مثال، برای جستجوی نام مربوطه به **IP** با شمارهٔ **157.55.200.51** یک سؤال از نوع **PTR** برای نام **51.200.55.157.in_addr.arpa** مورد نیاز می‌باشد.

Syntax:
owner ttl class *PTR* ***targeted_domain_name***
Example:
51.200.55.157.in-addr.arpa. *PTR* ***host.example.microsoft.com***

SOA[3]

اولین نگاشت در هر فایل پایگاه داده بایستی نگاشت **SOA** باشد. **SOA** مشخصه‌های کلی مربوط به هر **Zone** موجود در **DNS** را تعریف می‌کند. این نگاشت منابع یک سرویس دهنده **DNS** اولیه را برای **Zone** به عنوان بهترین منبع اطلاعات برای داده‌های داخل آن **Zone** و نیز نهاد بروز رساننده اطلاعات برای **Zone** مشخص می‌کند. همچنین سایر خواص اولیه **Zone** را نشان می‌دهد. **SOA** معمولا در هر **Zone** می‌باشد.

نکته: در مثال پایین، صاحب (سرویس دهنده اولیه **DNS**) با علامت **"@"** تعیین شده است، چراکه نام دامنه همان نام اصلی تمام داده‌ها در **Zone** می‌باشد (**example.microsoft.com**). این یک علامت استاندارد برای ثبت منابع می‌باشد که اغلب در ثبت **SOA** استفاده می‌شود.

[1] **Name Server**
[2] **Pointer (PTR)**
[3] **Start of Authority**

Syntax:
owner class SOA ***name_server responsible_person (serial_number refresh_interval retry_interval expiration minimum_time_to_live）***

Example:
```
@  IN  SOA    nameserver.example.microsoft.com.  postmaster.example.microsoft.com. (
                1          ; serial number
                3600       ; refresh   [1h]
                600        ; retry     [10m]
                86400      ; expire    [1d]
                3600 )     ; min TTL   [1h]
```

ثبت منابع دیگری نیز در ویندوز ۲۰۰۳ وجود دارد که بدلیل عدم اهمیت زیاد در این گزارش ذکری از آن‌ها آورده نشده است. در صورتیکه خواننده علاقمند به مطالعه این ثبت منابع باشد می‌تواند به مراجع آخر گزارش مراجعه نماید.

۲-۵ پیکربندی DNS در IPv4

Microsoft DNS، سرویس‌دهنده های منطبق بر استانداردهای **RFC** است. در نتیجه فایل‌های **zone** ای که ایجاد میکند و از آن‌ها استفاده میکند، از همه انواع نگاشت‌های منابع[1] منطبق بر استانداردهای **RFC** پشتیبانی میکنند. این سرویس دهنده همچنین قابلیت کار با انواع سرویس‌دهنده‌های **DNS** را دارد و نیز دارای خاصیت تشخیص **NSLOOKUP** می باشد. **Microsoft DNS** با **Windows Internet Naming Service (WINS)** نیز یکپارچه است و قابل مدیریت با ابزار گرافیکی مدیریت که **DNS Manager** خوانده میشوند، می باشد. در این قسمت نحوه نصب یک سرویس **DNS** را بر روی ویندوز۲۰۰۳ داده می‌شود.

قبل از هر چیز باید پروتکل **TCP/IP** به درستی پیکر بندی شود. سرویس دهنده **DNS** به طور پیش فرض، نگاشت های **SOA**، میزبان و سایر نگاشت های **DNS** را بر اساس نام دامنه و نام میزبان مشخصی تعیین میکند و اگر نام میزبان و دامنه مشخص نباشند فقط رکوردهای **SOA** را بوجود می آورد.

قبل از پیکر بندی **DNS** باید صحت تنظیمات مشتری های **DNS** را مورد بازبینی قرار داد. برای بازبینی تنظیمات مشتری‌های **DNS** در ویندوز بایستی مراحل زیر را اجرا نمود.

۱- ابتدا باید روی **My Network Places** کلیک راست کرد.

---

[1] **Resorce record**

۲- قسمت **Properties** را انتخاب کرده، به این ترتیب صفحه مشخصات باز می‌شود.

۳- روی اتصال اینترنت دستگاه (که **DNS** برای آن اتصال پیکر بندی می شود) کلیک راست کرده و به همان ترتیب بالا صفحه مشخصات آنرا باز می‌کنیم.

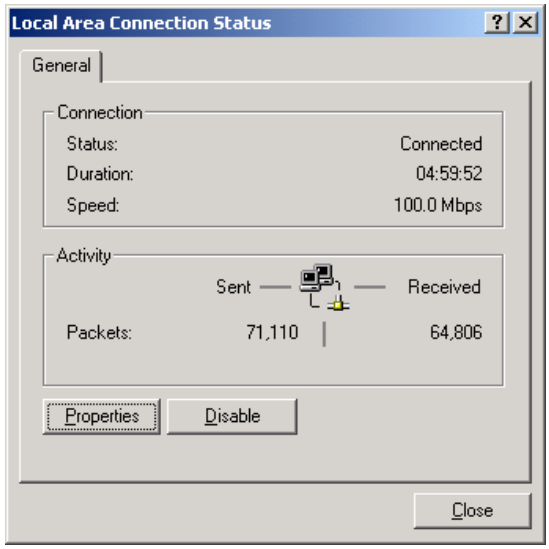
۴- پروتکل **TCP/IP** را انتخاب کرده، صفحه مشخصات آنرا هم باز می‌کنیم.

۵- آدرس **IP** و **DNS** موجود را وارد می‌کنیم.

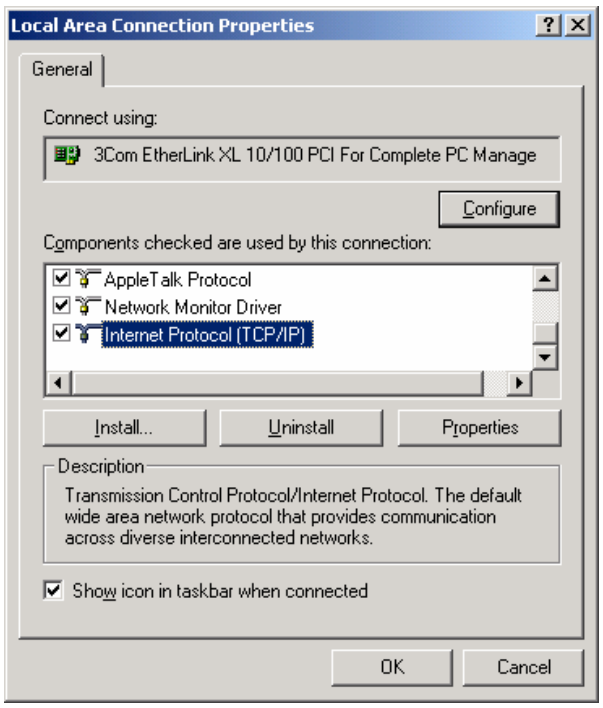
۶- اگر لازم بود که بیش از یک **DNS** وارد شود باید به قسمت **Advanced** و سپس **DNS** وارد شویم.

۷- برای بسته شدن پنجره **TCP/IP Properties**، **Ok** را فشار می‌دهیم.

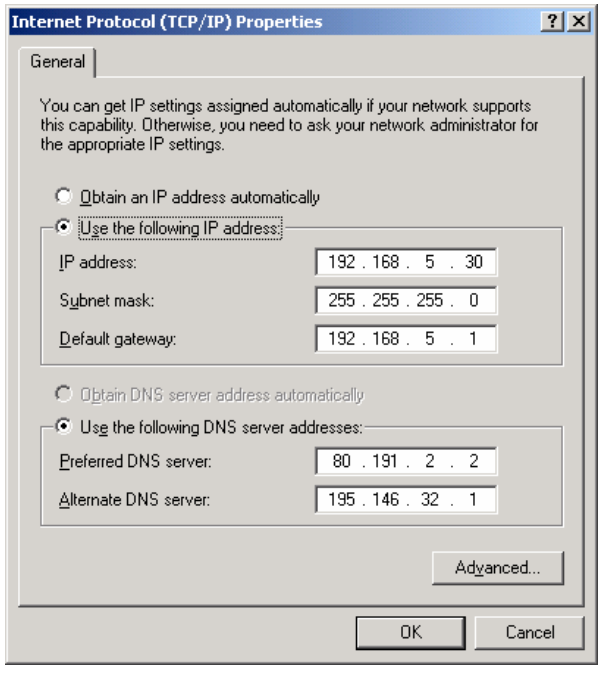
۸- برای بسته شدن پنجره **Connection Properties** ، **Ok** را فشار می‌دهیم.



شکل ۲-۴: صفحه مشخصات اتصال اینترنت دستگاه



شکل ۲-۵: صفحه انتخاب پروتکل **TCP/IP**



شکل ۲-۶: صفحه مربوط به تنظیم مشخصات پروتکل **TCP/IP**

۲– ۶ نصب سرویس‌دهنده DNS

برای نصب سرویس‌دهنده **DNS** همانند سایر سرویسهای شبکه‌ای ویندوز لازم است آن را از طریق پنجره **Add/Remove Programs** به سرویسهای ویندوز اضافه نمود. مراحل نصب این سرویس‌دهنده در ادامه آمده است.

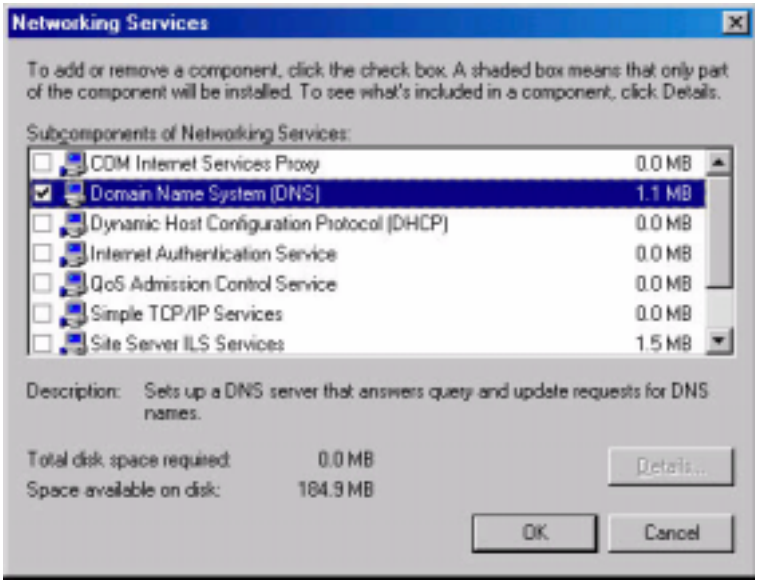
۱– در **Control Panel** ، **Add/Remove Programs** را باز کرده، سپس بر روی **Add/Remove Windows Components** کلیک دوتایی میکنیم.

۲– صفحه ای ظاهر میشود که در آن با کلیک بر روی **Networking Services** و سپس **Details**، جعبه گفتگوی **Networking Service** ظاهر میشود.

۳– باید دقت داشت که قسمت **Domain Name System(DNS)** اگر که انتخاب نشده بود علامت زده شود، پس از انجام این تنظیمات بر روی **OK** کلیک میکنیم.

۴– با کلیک کردن بر روی **Next**، ویندوز، **DNS** را نصب میکند.

۵– **Finish** به این مرحله پایان میدهد.



شکل ۲–۷: چگونگی نصب سرویس دهنده **DNS** بر روی کامپیوتر

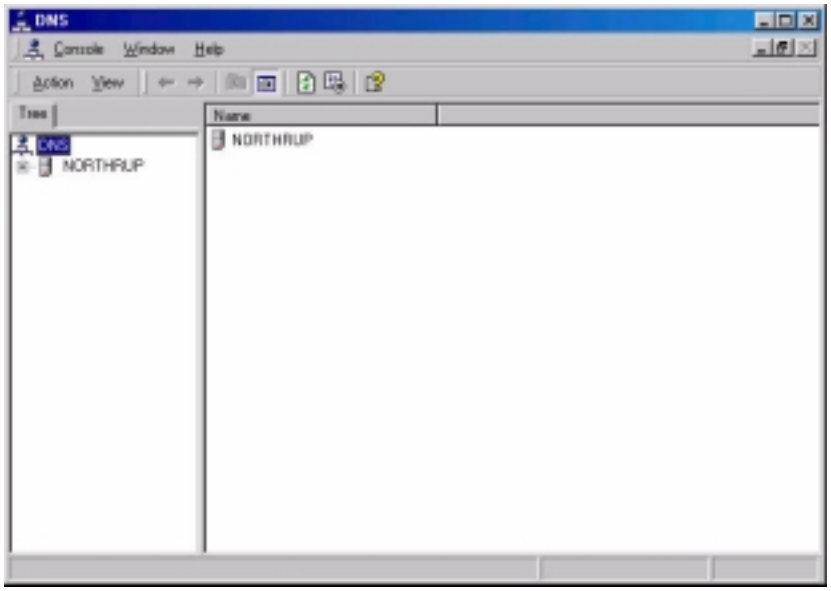
۲–۷ پیکربندی سرویس دهنده DNS

برای مدیریت سرویس دهنده های **DNS** در مایکروسافت دو راه وجود دارد. برای راه یافتن به قسمت مدیریت **DNS** و استفاده از آن یا ویرایش دستی فایل‌های پیکربندی **DNS**. مراحل زیر بایستی اجرا شوند:

۱- در قسمت **Start** مسیر **All programs ->Administrator Tools** را طی کرده سپس به قسمت **DNS** وارد میشویم.

۲- با کلیک راست روی نام سرویس دهنده گزینه Configure a DNS Server را انتخاب می کنیم.

۳- در پنجره باز شده روی **Next** کلیک میکنیم. باید توجه داشت در این قسمت گزینه **DNS Checklist** اطلاعات خوبی راجع به تنظیمات **DNS** به ما میدهد.



شکل ۲–۸: چگونگی انجام تنظیمات **DNS** در **Microsoft management console**

اولین ابزاری که برای پیکربندی سرویس دهنده های **DNS** مایکروسافت به کار میرود، **DNS console** است که در شکل نشان داده شده است. از آنجایی‌که سرویس دهنده **DNS** در ابتدا هیچگونه اطلاعات اولیه ای در مورد شبکه های کاربران ندارد به عنوان یک سرویس دهنده **caching-only** برای اینترنت نصب می شود. به این معنی که سرویس دهنده**DNS** فقط شامل اطلاعات سرویس دهنده های ریشه

اینترنت میباشد. برای اغلب پیکر بندی‌های سرویس دهنده**DNS** برای عملکرد بهتر باید اطلاعات اضافه ای فراهم شود.

در این قسمت نحوه پیکربندی یک سرویس دهنده **DNS** با اضافه کردن یک **zone** اولیه، توضیح داده می‌شود.

برای اضافه کردن یک**zone** به یک سرویس دهنده **DNS** بایستی مراحل زیر را اجرا کرد:

۱- با کلیک راست در درخت **Consol** بر روی نام کامپیوتر و سپس انتخاب گزینه **New Zone** صفحه **New Zone Wizard** ظاهر میشود.

۲- در این صفحه**Next** راکلیک میکنیم، در صفحه **Zone Type** به صورت پیش فرض **Zone Primary** انتخاب شده است که ما هم همان‌را انتخاب میکنیم.

۳- بر روی **Next** کلیک میکنیم. در قسمت **Forward or Reverse Lookup Zone**، **Forward lookup zone** را انتخاب میکنیم که البته به طور پیش فرض انتخاب شده است.

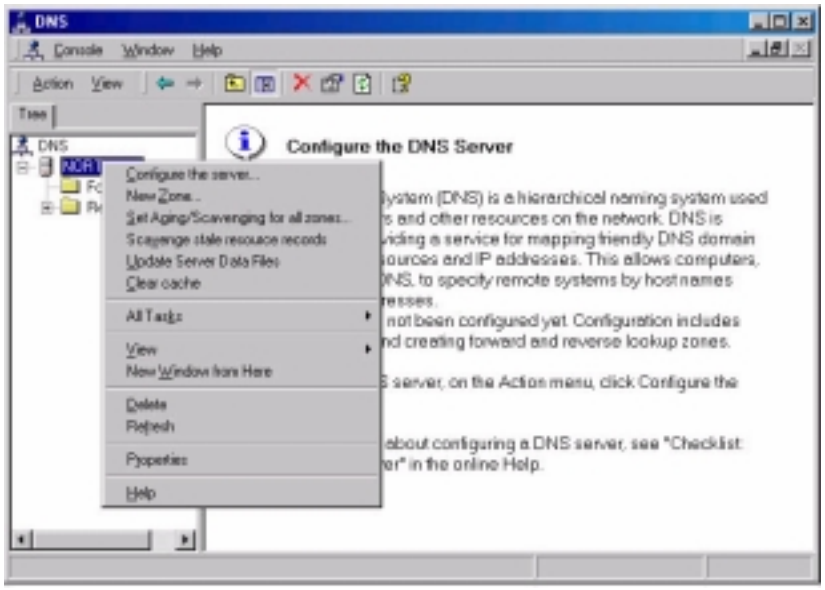
۴- در قسمت **Name box** بایستی نام **Zone** را وارد کنیم. (در اینجا نام **Zone** را **Zone1.org** انتخاب می‌کنیم).

۵- اگر بر روی **Create A New File** کلیک کنیم و سپس **Next** را فشار دهیم نام فایل **Zone1.org.dns** خواهد شد.(که **Zone1.org** نام **Zone** هست).

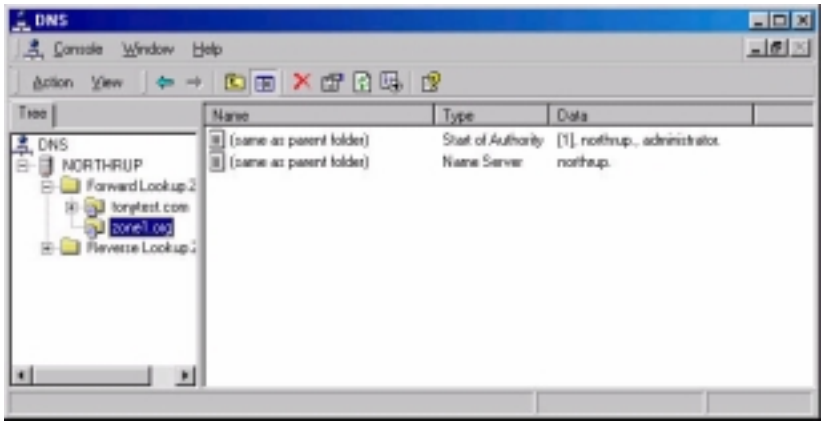
۶- در این مرحله بر روی **Next** کلیک می‌کنیم و در صفحه **Dynamic Update**، قسمت **Allow bouth nonesecure and secure dynamic update** را انتخاب میکنیم ودوباره بر روی **Next** کلیک می‌کنیم.

۷- در انتها برای ساخته شدن یک **Zone** جدید بر روی **Finish** کلیک میکنیم.

پس از انجام این مراحل، همان‌طور که در شکل نشان داده شده است پرونده **Forward Lookup Zone** در بردارنده **Zone** جدید است.



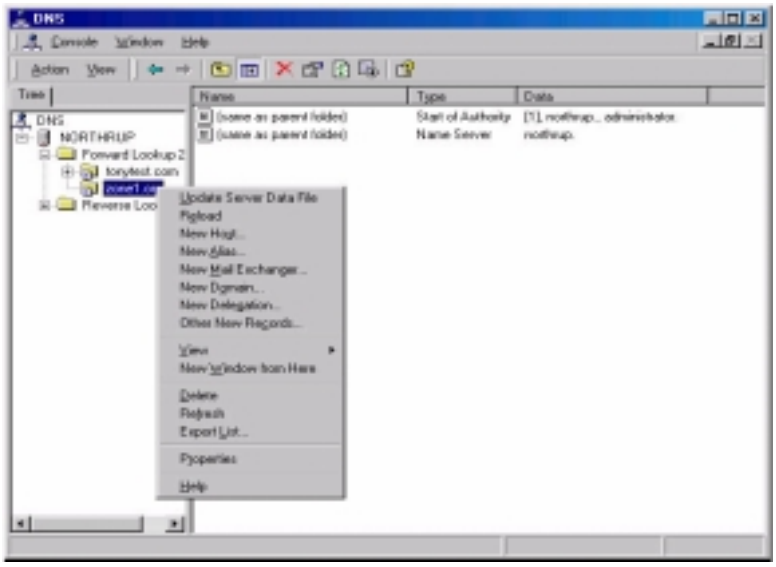
شکل ۲–۹: ایجاد یک **Zone** جدید در **DNS Console**



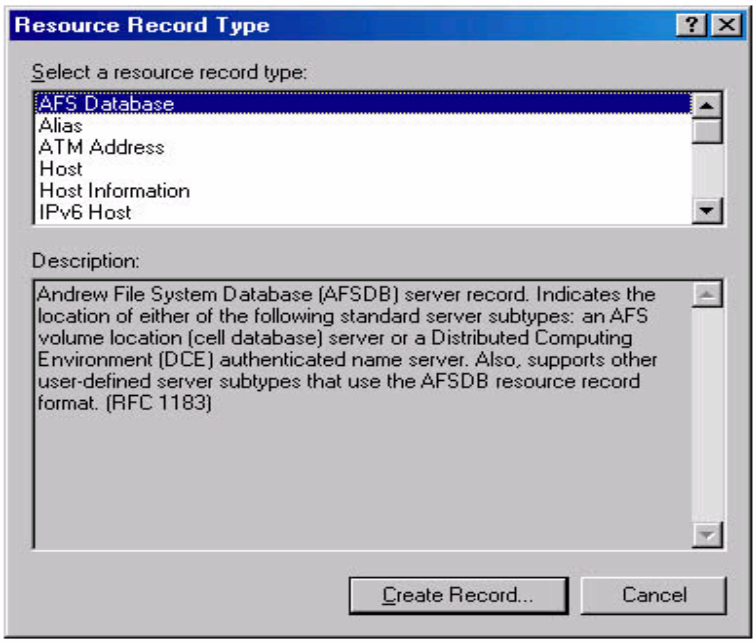
شکل ۲–۱۰: صفحه مربوط به افزوده شدن **Zone** جدید به پوشه **Forward Lookup Zone**

۲–۸ اضافه کردن نگاشت های منابع در داخل Zone

وقتی که **Zone**ها و زیر دامنه ها ساخته شدند، نگاشت های منابع میتوانند در داخل آن‌ها اضافه شوند. همانطور که در شکل نشان داده شده است برای ساختن یک میزبان جدید، بایستی بر روی **Zone** یا زیر دامنه کلیک راست کرد و سپس گزینه **New Host** را انتخاب کرد. پس از آن باید نام میزبان را وارد کرد و سپس روی **Add Host** کلیک نمود. به این ترتیب نگاشت میزبان به وجود می آید.



شکل ۲-۱۱:چگونگی اضافه کردن یک میزبان جدید در داخل **Zone**



شکل ۲-۱۲:نمایی از پنجره مربوط به انتخاب انواع مختلف نگاشت

برای ساختن انواع نگاشت های دیگر در داخل **Zone** بایستی بر روی آن و یا زیر دامنه کلیک شود و سپس گزینه **Other New Records** انتخاب شود. بعد از آن باید گزینه

which resource record type to create انتخاب شود. همانطور که در شکل نشان داده شده است یک جعبه گفتگو ظاهر میشود که گزینه های مختلفی برای مشخص کردن نوع نگاشت ها دارد.

۲–۹ یافتن مشکلات به وجود آمده در DNS توسط دستور NSLOOKUP

NSLOOKUP ابزار مفیدی برای یافتن مشکلات پیش آمده در **DNS** میباشد. وقتی که این ابزار شروع به کار میکند، اسم میزبان وآدرس **IP** مربوط به سرویس دهنده **DNS** ی را که برای سیستم محلی پیکر بندی شده است را نشان میدهد، بعد از آن خط، دستور آماده گرفتن درخواستهای بعدی می شود. اگر یک علامت سوال وارد کنید، **NSLOOKUP** همه دستورات موجود را نشان میدهد. برای خارج شدن از **NSLOOKUP** بایستی دستور **exit** را وارد کرد. برای دیدن آدرس **IP** میزبآن‌ها در محیط **NSLOOKUP** با استفاده از **DNS**، اسم میزبان را باید وارد کرد و سپس بر روی **Enter** کلیک نمود. به صورت پیش فرض **NSLOOKUP** برای سرویس دهنده های**DNS**ی که بر روی آن‌ها اجرا میشود به کار میرود ولی با تایپ**server <name>** (که منظور از **<name>** نام یک میزبان از سرویس‌دهنده‌ای است که **NSLOOKUP** بر روی آن اجرا می‌شود) میتوان بقیه میزبآن‌ها را نیز دید.

۲–۱۰ راه اندازیDNS در IPv6

برای فعال سازی **IPv6** در ویندوز ۲۰۰۳ ابتدا بایستی پروتکل **TCP/IP IPv6** را به ترتیب زیر فعال کرد:

- با کلیک دوتایی بر روی اتصال اینترنت دستگاه میتوان صفحه مشخصات آنرا باز کرد.
- برای فعال کردن **IPv6** باید گزینه **IPv6** از پروتکل **Microsoft TCP/IP** را فعال کرد.

پس از آن باید این پروتکل را روی دستگاه نصب کرد. اینکار به کمک دستورات خط فرمان و به صورت زیر انجام می‌شود. در خط فرمان بایستی دستور زیر را وارد کرد:

netsh interface ipv6 install

۲–۱۱ پیکر بندی سرویس دهنده DNS برای گوش دادن به IPv6

وقتی که روی سرویس دهنده **DNS** شما هم **IPv4** و هم **IPv6** تنظیم شده باشد، می‌توان سرویس دهنده **DNS** را برای گوش دادن به نام‌های **DNS**ی ثبت شده و درخواستهای **IPv6** آن پیکر بندی کرد.

- دستگاههایی که روی آن‌ها **IPv6** هست ولی **IPv4** نیست با این **DNS** به خوبی کار می کنند.
- کامپیوترها و سایر دستگاههایی که هم **IPv4** و هم **IPv6** به صورت پیش فرض **IPv6** را به کار میبرند.

برای اینکار باید در خط فرمان، دستور زیر نوشته شود:

Dnscmd/config/enable IPv6 1

۲–۱۲ پیکر بندی سرویس گیرنده ها با آدرس سرویس دهنده های DNS

برای برقراری ارتباط مابین سرویس گیرنده ها و سرویس دهنده های **DNS**، می‌توان سرویس گیرنده ها را با آدرس **IPv6** سرویس دهنده **DNS** پیکر بندی کرد، یا اینکه می توان بر روی سرویس دهنده **DNS** یکی از سه آدرس پیش فرض **IPv6** را تنظیم کرد که به طور خودکار بر روی همه سرویس گیرنده های آن سرویس دهنده پیکربندی شود. تنظیم آدرس سرویس دهنده **DNS** بر روی سرویس گیرنده ها با دستور زیر بر روی هر سرویس گیرنده انجام میشود:

netsh interface ipv6 add dns [interface=]*String* [address=]*IPAddress* [[index=]*Integer*]

که در آن **interface** نام اتصال شبکه سرویس گیرنده است.

برای پیکر بندی سرویس دهنده **DNS** با یکی از سه آدرس **IP** پیش فرض میتوان دستور زیر را به کار برد:

netsh interface ipv6 add address[interface=]*String* [address=]*IPAddress* [[index=]*Integer*]

که در آن **interface** نام اتصال شبکه سرویس دهنده است و **addres**، آدرس **IP** سرویس دهنده **DNS** است.

سه آدرس **IPv6**ذکر شده عبارتند از:

- **FEC0:0:0:FFFF::1**
- **FEC0:0:0:FFFF::2**
- **FEC0:0:0:FFFF::3**

اگر سرویس دهنده **DNS**ِ در زیردامنه‌ای غیر از آن زیر دامنه ای که سرویس گیرنده **DNS** در آن قرار دارد، باشد باید روی هر روتر **IPv6** ی که از زیر گروه سرویس دهنده **DNS** قابل دسترسی است یک**static route** به سرویس دهنده **DNS** تعریف شود.

۱۳-۲ پیکربندی Reverse Lookup

برای پیدا کردن نام میزبان با دادن شماره **IP** آن بایستی برای هر میزبانی که در پایگاه داده **DNS** موجود است درهر شبکه یک **Reverse lookup zone** ساخته شود. مراحل اضافه کردن یک **reverse lookup zone** عینا مانند اضافه کردن هر نوع **zone** دیگری است، اما نحوه نامگذاری **zone** متفاوت است. برای مثال اگر **IP** میزبان **198.231.25.89** باشد در دامنه **in-addr.arpa** به صورت **89.25.231.198.in.addr.arpa.** نمایش داده میشود. برای فعال کردن میزبان، برای پاسخ دادن به سرویس گیرنده یک **zone** بایستی به **DNS** **25.231.198.in-addr.arpa** اضافه شود. همچنین همه رکوردهای **PTR** شبکه **192.231.25.0** باید به این **server lookup zone** اضافه شوند.

http://www.microsoft.com/resources/documentation/WindowsServ/2003/standard/proddocs/en-us/Default.asp?url=/resources/documentation/WindowsServ/2003/standard/proddocs/en-us/sag_IP_v6_imp_config_items.asp

۱۴-۲ بررسی Delegation در سرویس‌دهنده‌های DNS

پایگاه داده‌های[1] **DNS** می‌تواند به بخش‌های متعددی که **Zone** نام دارند تقسیم بندی شود. یک **Zone** بخشی از پایگاه داده‌های **DNS** می‌باشد که دربردارنده نگاشت‌های منابع[2] است. فایل‌های مربوط به هر **Zone** بر روی سرویس‌دهنده‌های **DNS** وجود دارند. یک سرویس‌دهنده **DNS** می‌تواند به گونه‌ای ساختاردهی شود که دارای یک یا چندین **Zone** باشد و یا هیچ‌گونه **Zone** ای

[1] - **Database**
[2] - **Resource Records (RR)**

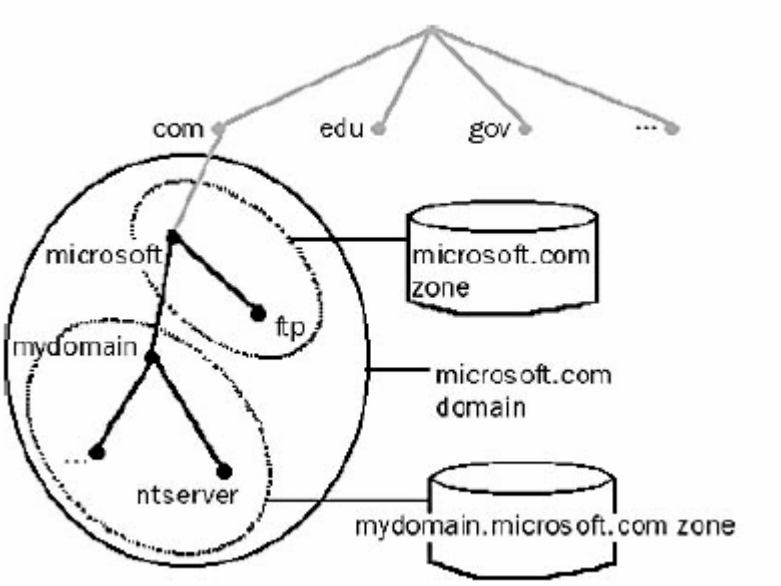
نداشته باشد. به هر **Zone** یک نام دامنه‌ای ویژه که دامنه ریشه **Zone** [1] نام دارد تعلق می‌گیرد. یک **Zone**، اطلاعات مربوط به کلیه نام‌هایی که با نام دامنه ریشه **Zone** ختم می‌شوند را دربردارد. یک سرویس‌دهنده **DNS** در صورتی که دارای یک **Zone** باشد که حاوی اطلاعات مربوط به یک نام است برای آن نام اعتبار دارد. اولین نگاشت[2] در هر فایل **Zone**، یک نگاشت منابع تحت عنوان آغاز اعتبار[3] یا **SOA** است. این نگاشت منابع یک سرویس‌دهنده **DNS** اولیه را برای **Zone** به عنوان بهترین منبع اطلاعات برای داده‌های داخل آن **Zone** و نیز نهاد به روز رساننده اطلاعات برای **Zone** مشخص می‌کند. نام‌هایی که در داخل یک **Zone** وجود دارند به **Zone** های دیگر نیز می‌توانند محول شوند. محول‌سازی[4] یا همان **Delegation** یک فرآیند تخصیص مسوولیت برای بخشی از دامنه اسمی **DNS** به یک نهاد مجزا است. این نهاد مجزا می‌تواند سازمان، ساختمان و یا گروه کاری دیگری در داخل شرکت باشد. به عبارت فنی‌تر، محول‌سازی به معنی تخصیص اعتبار بخش‌هایی از دامنه اسمی **DNS** به **Zone** های دیگر است. نگاشت سرویس‌دهنده اسمی که **Zone** محول شده را مشخص می‌کند و نام سرویس‌دهنده **DNS** معتبر برای آن **Zone**، بیان‌کننده محول‌سازی است. استفاده از قابلیت محول‌سازی در میان **Zone** های متعدد، بخشی اصلی هدف طراحی **DNS** بود. در زیر دلایلی که برای استفاده از محول‌سازی در فضای اسمی **DNS** وجود دارند آورده شده‌اند:

- نیاز برای محول ساختن مدیریت یک دامنه **DNS** به یک تعداد از سازمان‌ها یا ساختمآن‌های داخل یک سازمان.
- نیاز برای توزیع بار نگهداری از یک پایگاه داده بزرگ **DNS** به کمک سرویس‌دهنده‌های متعدد برای بهبود بخشیدن به عملکرد تشخیص نام[5] علاوه بر تولید یک محیط **DNS**با قابلیت تحمل خرابی[6].
- نیاز برای برقراری پیوندهای سازمانی مابین میزبآن‌ها[7] با قرار گرفتن آن‌ها در دامنه‌های مناسب.

نگاشت‌های منابع سرویس‌دهنده‌های نام با مشخص ساختن سرویس‌دهنده‌های **DNS** برای هر **Zone** امر محول‌سازی را تسهیل می‌کنند. این نگاشت‌ها در همه **Lookup Zone** های **Reverse** و **Forward**

[1] - Zone's Root Domain
[2] - Record
[3] - Start of Authority
[4] - Delegation
[5] - Name Resolution
[6] - Fault Tolerant
[7] - Host

ظاهر می‌شوند. در هر زمان که یک سرویس دهنده **DNS** نیاز به استفاده از یک محول‌سازی دارد به نگاشت‌های منابع سرویس‌دهنده برای سرویس‌دهنده‌های **DNS** مورد نظر رجوع می‌کند. در شکل () مدیریت دامنه **Microsoft.com** به دو **Zone** با عنوان‌های **micrisoft.com** و **mydomain.microsoft.com** محول شده است.



شکل۲-۱۳: بررسی مفاهیم **Zone** و **Domain** با استفاده از مثال

اگر نگاشت‌های متعدد سرویس‌دهنده **DNS** برای یک **Zone** محول شده وجود داشته باشند که معرفی‌کننده سرویس‌دهنده‌های **DNS** متعدد قابل‌دسترس برای پاسخگویی می‌باشند، سرویس‌دهنده **DNS** در **windows 2000** قادر به انتخاب نزدیکترین **DNS** سرویس‌دهنده بر اساس فاصله‌های زمانی رفت و برگشت برای هر سرویس‌دهنده **DNS** خواهد بود.

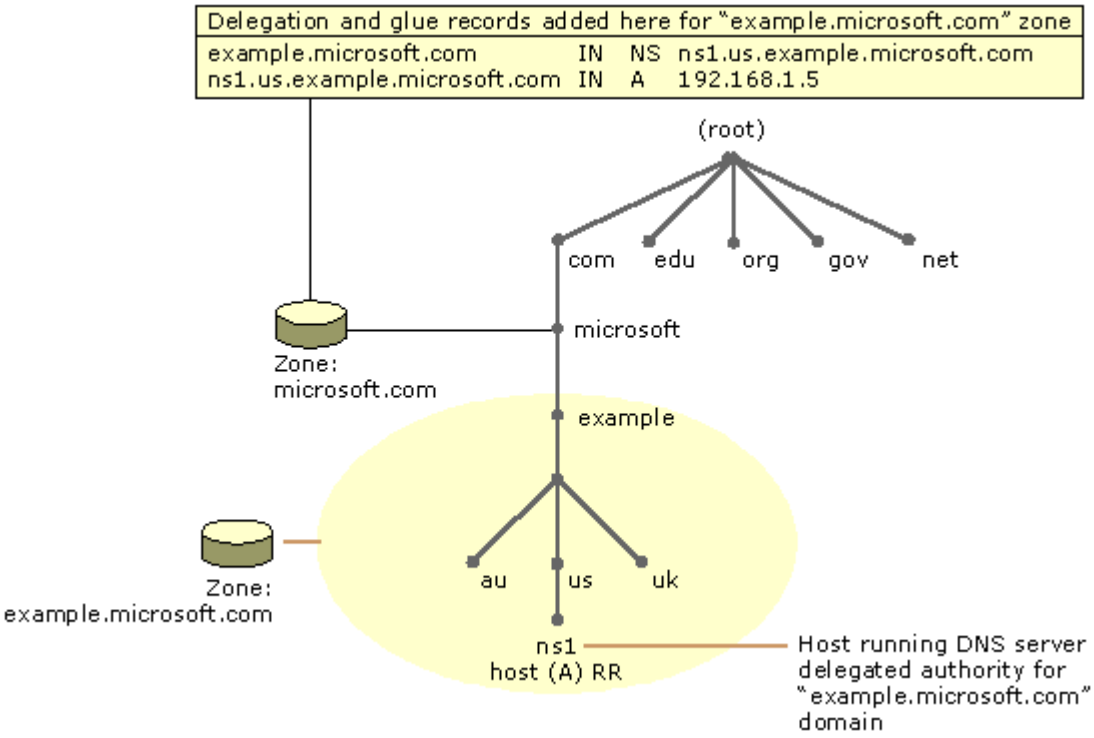
۲-۱۵ بررسی Zone ها و دامنه‌های DNS

DNS ها اطلاعات مربوط به بخشی از فضای اسمی دامنه را که **Zone** نامیده می‌شود ذخیره می‌کنند. یک سرویس‌دهنده **DNS** منحصر به فرد می‌تواند برای تعداد زیادی از **Zone** ها معتبر باشد. فهم و درک تفاوت مابین یک **Zone** و یک دامنه، کمی پیچیده است. می‌توان گفت که یک **Zone** بخشی از یک دامنه است. برای مثال، دامنه **Microsoft.com** شامل همه داده‌های مربوط به **microsoft.com**، **marketing.microsoft.com** و **development.microsoft.com** می‌باشد. هر چند **Zone** مربوط به **Microsoft.com** تنها شامل اطلاعات **Microsoft.com** و اطلاعات

سرویس‌دهنده‌های نام معتبر برای زیردامنه‌ها است. اگر این زیردامنه‌ها به سرویس‌دهنده دیگری محول نشده باشند این **Zone** می‌تواند اطلاعات زیردامنه‌های **Microsoft.com** را نیز دربربگیرد. اگر زیردامنه‌ها وجود نداشته باشند **Zone** و دامنه در اصل یکی خواهند بود. در این حالت **Zone** شامل همه اطلاعات مربوط به دامنه است.

مثال: محول ساختن یک زیردامنه به یک Zone **جدید**

همان طور که در شکل زیر نشان داده شده است زمانی که یک **Zone** جدید برای یک زیردامنه **(example.microsoft.com)** ایجاد می‌شود، محول‌سازی از **Zone** اصلی **(Microsoft.com)** مورد نیاز است.



شکل ۲-۱۴: محول ساختن یک زیردامنه به یک **Zone** جدید

در این مثال، یک کامپیوتر سرویس‌دهنده **DNS** معتبر برای زیردامنه محول شده اخیر **(example.microsoft.com)** بر اساس یک زیردامنه که در **Zone** جدید قرار دارد **(ns1.us.example.microsoft.com)** نام‌گذاری می‌شود. برای شناساندن این سرویس‌دهنده به دیگرانی که در خارج **Zone** محول شده جدید وجود دارند، دو نگاشت منابع **(RR)**

در **Microsoft.com zone** و در جهت تکمیل محول‌سازی به **Zone** جدید، مورد نیاز است. این نگاشت‌های منابع عبارتند از:

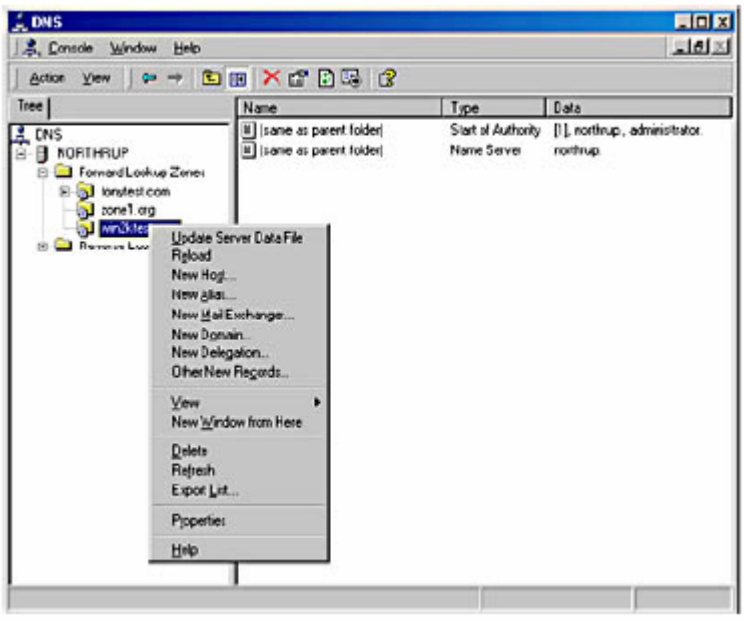
- یک **NS RR** برای اجرای محول‌سازی. این **RR** برای انتشار نام **ns1.us.example.microsoft.com** به عنوان سرویس‌دهنده معتبر برای زیردامنه محول شده، مورد استفاده قرار می‌گیرد.
- یک **A RR** برای نگاشت اسم سرویس‌دهنده تعیین شده در **NS RR** به آدرس **IP** آن مورد نیاز است.

۲-۱۶ مراحل ایجاد یک Zone Delegation

۲-۱۶-۱ تنظیمات در Windows

۱- بر روی **start** کلیک می‌کنیم، مسیر **Programs** و **Administrative Tools** را طی می‌کنیم و سپس بر روی **DNS** کلیک می‌کنیم.

۲- در **console tree** بر روی زیردامنه مورد نظر راست کلیک می‌کنیم و سپس بر روی **New Delegation** کلیک می‌کنیم (مطابق شکل زیر).

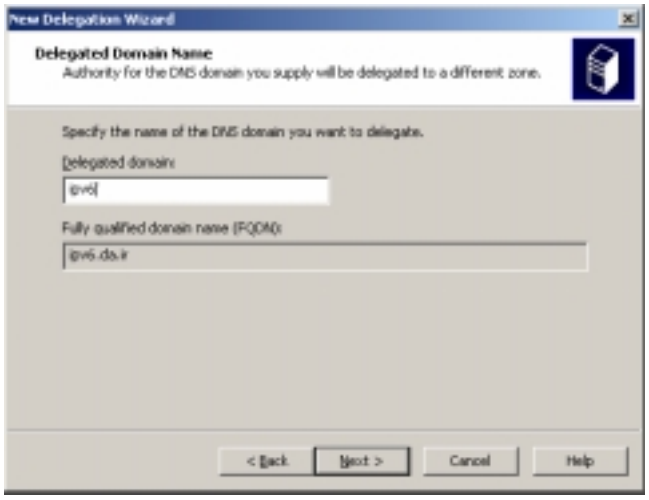


شکل۲-۱۵: نمایی از چگونگی ایجاد یک **Zone Delegation**

در این مرحله **New Delegation Wizard** ظاهر می‌شود.

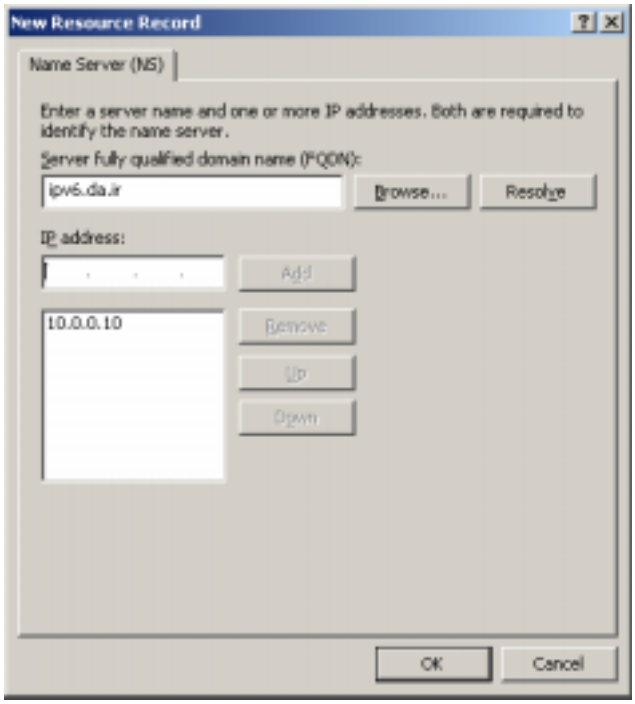
۳- بر روی **Next** کلیک می‌کنیم.

۴- در **Delegated Domain Name dialog box** نام دامنه محول شده را می‌نویسیم و سپس بر روی **Next** کلیک می‌کنیم.



شکل ۲-۱۶: مشخص کردن دامنه **Delegation**

۵- در **Name Servers dialog box** برای تعیین اسامی و آدرس‌های **IP** سرویس‌دهنده‌های **DNS** که می‌خواهیم میزبان **Zone** محول شده باشند، بر روی **Add** کلیک می‌کنیم.



شکل ۲-۱۷: مشخص کردن سرویس‌دهنده نام **Delegation**

در این مرحله، **New Resource Record dialog box** ظاهر می‌شود و به ما اجازه تعیین سرویس‌دهنده‌های **DNS** را می‌دهد.

۶- نام سرویس‌دهنده **DNS** را می‌نویسیم، بر روی **Add** و سپس **OK** کلیک می‌کنیم.

۷- در **Name Servers dialog box** بر روی **Next** کلیک می‌کنیم.

برای بسته شدن **New Delegation Wizard** بر روی **Finish** کلیک می‌کنیم.

۲-۱۶-۲ تنظیمات با استفاده از خط فرمان[1] (برای IPv4 و IPv6)

۱- صفحه **Command Prompt** را باز می‌کنیم.

۲- دستور را به شکل زیر وارد می‌کنیم:

dnscmd ***ServerName*** /RecordAdd ***ZoneName*** ***NodeName*** **[**/Aging**]** **[**/OpenAcl**]** **[*Ttl*]** NS **{*HostName*|*FQDN*}**

به طور مثال برای همان مساله بالا دستور را به شکل زیر وارد می‌نماییم:

dnscmd da.ir /recordadd da.ir ipv6 NS ipv6.da.ir

همچنین توجه داریم که حتما بایستی قبلا منبع **ipv6.da.ir** را به لیست میزبآن‌های **da.ir** اضافه کرده‌باشیم. توضیحات بیشتر مربوط به دستور، در جدول آورده شده است.

متاسفانه در **Microsoft Windows Server 2003** که برای اولین بار پشتیبانی از **IPv6** در **DNS** مد نظر قرار گرفته است امکان پیاده‌سازی **Delegation** در یک بستر **IPv6** تنها و بدون استفاده از **IPv4** امکان‌پذیر نیست. به عبارت دیگر برای محول نمودن بخشی از اختیارات به یک سرویس‌دهنده دیگر نام دامنه نیازمند یک بستر **IPv4** و برقراری ارتباط بین سرویس‌دهنده اصلی و سرویس‌دهنده دارای اختیارات با استفاده از **IPv4** خواهیم بود.

[1] **- Command Line**

Value	Description
dnscmd	Specifies the name of the command-line tool.
ServerName	Required. Specifies the DNS host name of the DNS server. You can also type the IP address of the DNS server. To specify the DNS server on the local computer, you can also type a period (.)
/RecordAdd	Required. Specifies the command to add a resource record.
ZoneName	Required. Specifies the fully qualified domain name (FQDN) of the zone.
NodeName	Required. Specifies the FQDN of the node in the DNS namespace for which the SOA record is added. You can also type the node name relative to the *ZoneName* or @, which specifies the zone's root node.
/Aging	If this command is used, this resource record is able to be aged and scavenged. If this command is not used, the resource record remains in the DNS database unless it is manually updated or removed.
/OpenAcl	Specifies that new records are open to modification by any user. Without this parameter, only administrators may modify the new record.
Ttl	Specifies the Time-To-Live (TTL) setting for the resource record. (The default TTL is defined in SOA resource record).
NS	Required. Specifies that you are adding a name server (NS) resource record to the zone specified in *ZoneName*.
HostName|FQDN	Required. Specifies the host name or FQDN of the new authoritative server.

جدول ۲-۱

۲-۱۷ بررسی فرآیند به روز رسانی پویا[1] در سرویس‌دهنده‌های DNS

در آغاز **DNS** به گونه‌ای طراحی شد که تنها می‌توانست ایجاد تغییرات استاتیک در پایگاه داده **Zone** را پشتیبانی کند. به دلیل محدودیت‌های موجود در طراحی **DNS** استاتیک، قابلیت اضافه کردن، حذف یا اصلاح منابع نگاشت تنها می‌توانست به صورت دستی و توسط یک مجری آشنا به سیستم **DNS** صورت بگیرد. برای مثال، یک مجری بایستی نگاشت‌های موجود در **Zone** یک سرویس‌دهنده اولیه را ویرایش کند و سپس باید پایگاه داده اصلاح شده **Zone** از طریق انتقال[2] **Zone** به سرویس‌دهنده‌های ثانویه منتقل شود. این طرح، زمانی که تعداد تغییرات موجود، کم است و به روز رساندن پایگاه داده‌ها به ندرت رخ می‌دهد، قابل استفاده است اما در غیر این صورت نمی‌توان آن را مدیریت کرد.

windows 2003 از مشتری و سرویس‌دهنده برای استفاده از فرآیند به روز رسانی پویا پشتیبانی می‌کند. به روز رسانی‌های پویا کامپیوترهای مشتری **DNS** را قادر می‌سازند که به صورت پویا نگاشت‌های منابع مربوط به خود را که در سرویس‌دهنده‌های **DNS** آن‌ها موجود است در هر زمان که

[1] - **Dynamic Update**
[2] -**Transfer**

تغییری در آن‌ها رخ می‌دهد به روز برسانند. این قابلیت، نیاز به عملیات اجرایی دستی در نگاشت‌های **Zone** را کاهش می‌دهد، به خصوص برای مشتری‌هایی که دایما مکان آن‌ها تغییر می‌کند و از **DHCP** برای به دست آوردن آدرس **IP** استفاده می‌کنند.

به صورت پیش‌فرض، کامپیوترهایی که **windows 2003** را اجرا می‌کنند و تنظیم استاتیک آن‌ها برای **TCP/IP** انجام شده است، به صورت پویا نگاشت‌های منابع میزبان **(A)** و اشاره‌کننده **(PTR)** به آدرس‌های **IP** تنظیم شده که توسط اتصالات نصب شده شبکه آن‌ها استفاده می‌شود را به سرویس‌دهنده **DNS** معرفی می‌کنند. به روز رسانی‌های پویا با وقوع هر یک از حوادث زیر فرستاده می‌شوند:

- یک آدرس **IP** در قسمت تنظیم خصوصیات **TCP/IP** برای هر یک از اتصالات نصب شده شبکه، اضافه، حذف و یا اصلاح می‌شود.
- یک **IP address lease** تغییر می‌کند و یا توسط سرویس‌دهنده **DHCP** هر یک از اتصالات نصب شده شبکه تجدید می‌شود. برای مثال، زمانی که کامپیوتر راه‌اندازی می‌شود یا زمانی که فرمان **ipconfig /renew** استفاده می‌شود.
- فرمان **ipconfig /registerdns** استفاده می‌شود و بدین وسیله به صورت دستی ثبت نام مشتری در **DNS** اجباری می‌شود.
- زمانی که کامپیوتر روشن می‌شود.

زمانی که به دلیل وقوع هر یک از این حوادث، به روز رسانی پویا به‌کارمی‌افتد سرویس **DHCP Client** (نه سرویس مشتری **DNS**) اطلاعات به روز رسانده شده را می‌فرستد. این روند به گونه‌ای طراحی شده است که اگر تغییری در اطلاعات مربوط به آدرس **IP** به دلیل **DHCP** رخ دهد، مراحلی که برای به روز رساندن این اطلاعات در **DNS** لازم است، طی می‌شوند. سرویس مشتری **DHCP** این عمل را برای همه اتصالات شبکه استفاده شده روی سیستم که برای استفاده از **DHCP** تنظیم نشده‌اند، انجام می‌دهد.

سرویس دهنده **DNS** اجازه می‌دهد که به روز رسانی پویا بر مبنای **Zone** در هر سرویس‌دهنده‌ای که برای یک **Zone** استاندارد اولیه یا **directory-integrated zone** تنظیم شده است، فعال یا غیر فعال شود. زمانی که **Zone** های **DNS** در شاخه فعال[1] ذخیره می‌شوند، **DNS** به صورت پیش‌فرض برای

[1] - **Active Directory**

پذیرفتن به روز رسانی‌های پویا تنظیم می‌شود. علاوه بر این باید دانست که مساله امنیت در به روز رساندن **DNS** تنها برای **Zone** هایی قابل دسترس است که در شاخه فعال قرار دارند.

حال این سوال پیش می‌آید که چگونه کامپیوترهای سرویس‌دهنده و مشتری، اسم‌های **DNS** ای خود را به روز می‌رسانند. همان طور که گفته شد به صورت پیش‌فرض، کامپیوترهایی که **windows 2003** را اجرا می‌کنند و تنظیم استاتیک آن‌ها برای **TCP/IP** انجام شده است، به صورت پویا نگاشت‌های منابع میزبان **(A)** و اشاره کننده **(PTR)** به آدرس‌های **IP** تنظیم شده که توسط اتصالات نصب شده شبکه آن‌ها استفاده می‌شود را به سرویس‌دهنده **DNS** معرفی می‌کنند. اما برای این تنظیمات حتما به بستر **IPv4** نیاز داریم. به عبارت دیگر این تنظیمات را نمی‌توان تنها برای **IPv6** انجام داد. به صورت پیش-فرض همه کامپیوترها نگاشت‌های خود را بر اساس **FQDN** [1] خود ثبت می‌کنند. نام اولیه کامل یک کامپیوتر، یک **FQDN**، بر مبنای الحاق یک پیشوند **DNS** اولیه کامپیوتر[2] به نام کامپیوتر است. هر دو تنظیم ذکر شده در جدول نام کامپیوتر[3] واقع در خصوصیات سیستم[4]، قابل اجرا است. فرآیند به روز رسانی پویا در کامپیوترهایی که سیستم‌عامل‌های **Windows 2000**، **Windows XP** یا **Windows Server 2003** را اجرا می‌کنند و از سرویس‌دهنده‌های **DHCP** برای به دست آوردن آدرس‌های **IP** خود استفاده می‌کنند، متفاوت از توضیحاتی است که در این بخش آورده خواهد شد. در این قسمت به بررسی یک مثال برای روشن‌تر شدن چگونگی نحوه کار فرآیند به روز رسانی پویا پرداخته می‌شود.

به روز رسانی‌های پویا زمانی که یک تغییر در نام **DNS** ای و یا آدرس **IP** یک کامپیوتر رخ می‌دهد، مورد استفاده قرار می‌گیرند. برای مثال، فرض کنید که مطابق شکل زیر در ابتدا نام یک مشتری در پنجره خصوصیات سیستم، **oldhost** تنظیم شده باشد.

Computer name	oldhost
DNS domain name of computer	example.microsoft.com
Full computer name	oldhost.example.microsoft.com

شکل ۲–۱۸: تشکیل نام کامل کامپیوتر با استفاده از نام کامپیوتر و نام دامنه ای **DNS** آن

در این مثال، نام‌های دامنه **DNS** از نوع **connection-specific** برای کامپیوتر تنظیم نشده‌اند. بعد از مدتی نام کامپیوتر از **oldhost** به **newhost** تغییر می‌کند که باعث وقوع تغییرات نشان داده شده در شکل زیر می‌شود.

[1] - **Fully Qualified Domain Name**
[2] - **Primary DNS Suffix of a Computer**
[3] - **Computer Name**
[4] - **System properties**

Computer name	newhost
DNS domain name of computer	example.microsoft.com
Full computer name	newhost.example.microsoft.com

شکل ۲-۱۹: تغییر نام کامل کامپیوتر بعد از تغییر نام آن

زمانی که تغییر نام در پنجره خصوصیات سیستم، اعمال می‌شود کامپیوتر بایستی از نو شروع به کار کند[1]. همان‌طور که در شکل () نشان داده شده است زمانی که کامپیوتر از نو شروع به کار می‌کند سرویس **DHCP Client** مراحل زیر را برای به روز رساندن **DNS** انجام می‌دهد:

۱- سرویس **DHCP Client** یک سوال از نوع **SOA** با استفاده از نام دامنه **DNS** کامپیوتر می‌فرستد. به عبارت دیگر، کامپیوتر مشتری از **FQDN** تنظیم شده متداول کامپیوتر (مانند **newhost.example.microsoft.com**) به عنوان نام مشخص شده در این سوال استفاده می‌کند.

۲- سرویس دهنده **DNS** ای که برای **Zone** دربردارنده **FQDN** مشتری، معتبر است به سوال نوع **SOA** پاسخ می‌دهد. برای **Zone** های اولیه استاندارد، سرویس‌دهنده اولیه برگشت داده شده در پاسخ به سوال **SOA** ثابت و ایستا می‌شود. این پاسخ با نام دقیق **DNS** همان‌طور که توسط **Zone** در **SOA RR** ذخیره شده است مطابقت دارد. حتی اگر **Zone** به روز رسانده شده، **directory-integrated** باشد هر سرویس‌دهنده **DNS** که **Zone** را بار می‌کند می‌تواند پاسخ دهد و به صورت پویا نام خود را به عنوان سرویس‌دهنده اولیه **Zone** در سوال **SOA** پاسخ دهد.

۳- سرویس **DHCP Client** سپس برای برقراری ارتباط با سرویس‌دهنده **DNS** اولیه تلاش می‌کند. مشتری، پاسخ داده شده به سوال **SOA** را برای نام خود برای مشخص کردن آدرس **IP** سرویس‌دهنده معتبر به عنوان سرویس‌دهنده اولیه برای پذیرش نام خود، تجزیه و تحلیل می‌کند. مشتری سپس برای انجام مراحل زیر که برای اتصال به سرویس‌دهنده اولیه و به روز رساندن پویای اطلاعات آن لازم است، پیش می‌رود:

a. یک تقاضای به روز رساندن پویا را به سرویس‌دهنده اولیه که در پاسخ سوال **SOA** مشخص شد، می‌فرستد. اگر عملیات به روز رساندن، موفق شود عملیات دیگری رخ نمی‌دهد.

[1] **-Restart**

b. اگر مرحله قبل به موفقیت نرسد، مشتری یک سوال از نوع **NS** برای نام **Zone** ای که در نگاشت **SOA** مشخص است می‌فرستد.

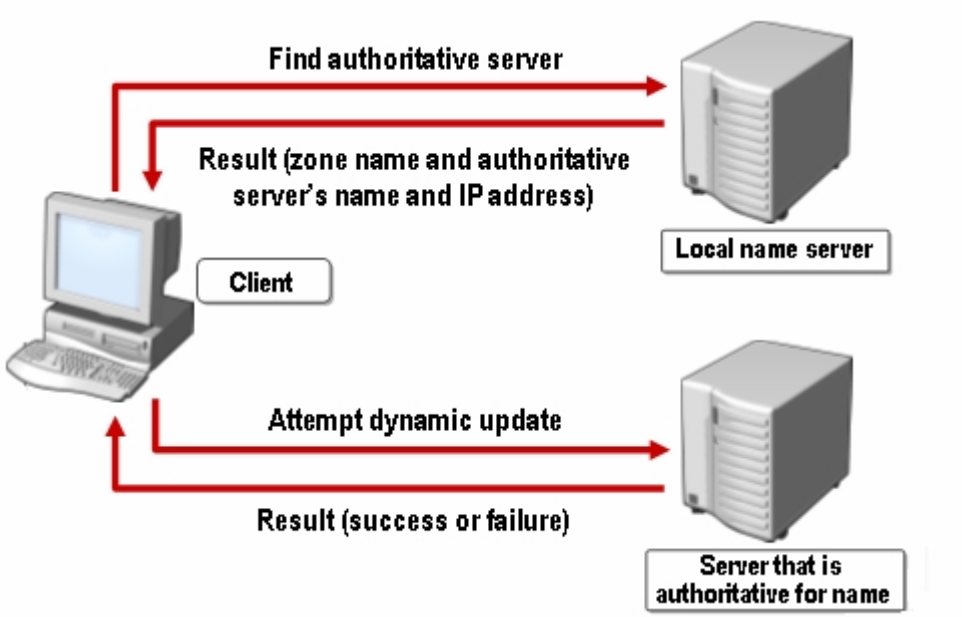
c. زمانی که پاسخ به این سوال را دریافت می‌کند، یک سوال **SOA** به اولین سرویس‌دهنده **DNS** ای که در پاسخ لیست شده است می‌فرستد.

d. بعد از اینکه سوال **SOA** تشخیص داده شد، مشتری فرآیند به روز رسانی را برای سرویس‌دهنده مشخص شده در نگاشت **SOA** ی برگشت داده شده، انجام می‌دهد. اگر عملیات به روز رساندن، موفق شود عملیات دیگری رخ نمی‌دهد.

e. اگر مرحله قبل نیز به موفقیت نرسد، مشتری فرآیند سوال **SOA** را با فرستادن به سرویس‌دهنده **DNS** بعدی که در پاسخ لیست شده است تکرار می‌کند.

۴- زمانی که اتصال با سرویس‌دهنده اولیه ای که می‌تواند عملیات به روز رسانی را انجام دهد برقرار می‌شود، تقاضای به روز رسانی از سوی مشتری فرستاده می‌شود و سرویس‌دهنده، آن را تجزیه و تحلیل می‌کند. محتویات تقاضای به روز رسانی شامل دستورالعمل‌هایی برای افزودن نگاشت‌های منابع **A** (و احتمالا **PTR**) برای **newhost.example.microsoft.com** و حذف نگاشت‌های منابع مشابه برای نام قبلی ثبت نام شده یعنی **oldhost.example.microsoft.com** می‌باشد.

قابل ذکر است که سرویس‌دهنده بررسی می‌کند که آیا عملیات به روز رسانی برای تقاضای مشتری انجام می‌شود یا خیر. برای **Zone** های اولیه استاندارد، فرآیند به روز رسانی های پویا امن نیستند بنابراین هر مشتری سعی می‌کند که عملیات به روز رسانی موفقی داشته باشد. برای **Zone** های **Active Directory-integrated** عملیات به روز رسانی، امن می‌باشد و با استفاده از تنظیمات امنیتی **directory-based** انجام می‌شود. به روز رسانی‌های پویا به طور متناوب فرستاده و تجدید می‌شوند. به صورت پیش‌فرض، کامپیوترها هر هفت روز یک بار عملیات به روز رسانی را تکرار می‌کنند. اگر عملیات به روز رسانی باعث ایجاد هیچ‌گونه تغییری در اطلاعات **Zone** نشود، **Zone** در همان حالت قبلی خود باقی خواهد ماند و چیزی در آن نوشته نخواهد شد.



شکل ۲-۲۰: مراحل فرآیند به روزرسانی پویای اطلاعات در سرویس‌دهنده **DNS**

۲-۱۸ فعال کردن به روز رسانی های پویا بر روی سرویس‌دهنده‌های DNS

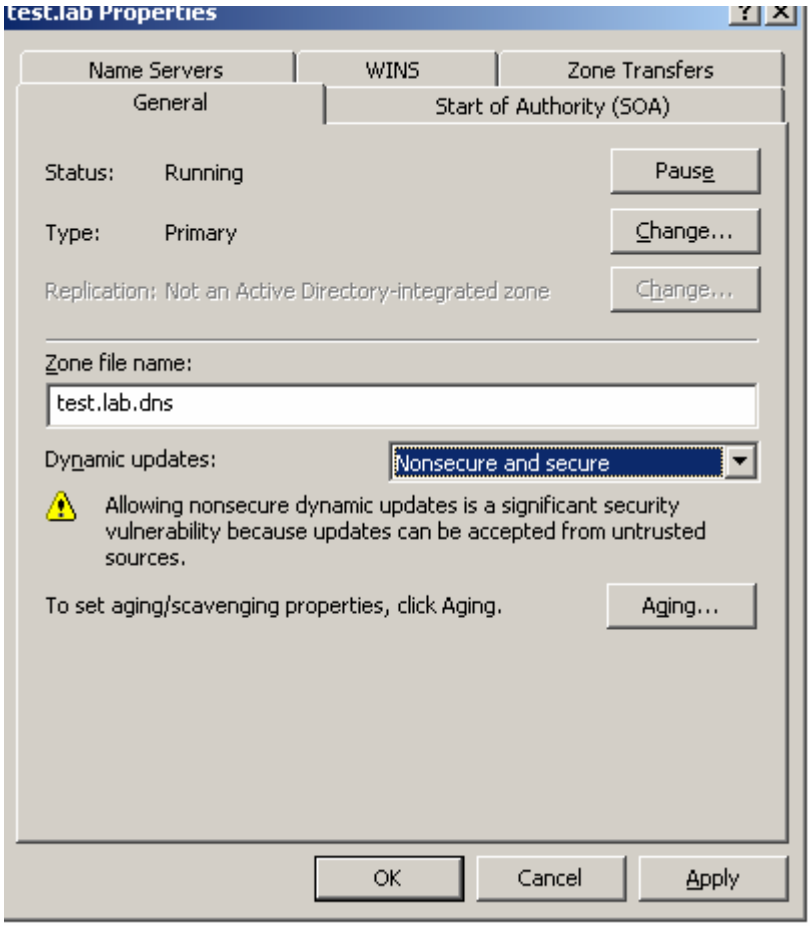
۱- بر روی **start** کلیک می‌کنیم، مسیر **Programs** و **Administration Tools** را طی می‌کنیم و سپس بر روی **DNS** کلیک می‌کنیم.

۲- در **console tree** بر روی **Zone** راست کلیک می‌کنیم، سپس بر روی **Properties** کلیک می‌کنیم.

در اینجا پنجره صحبت **Zone Properties** همان‌طور که در شکل زیر نشان داده شده است باز می‌شود.

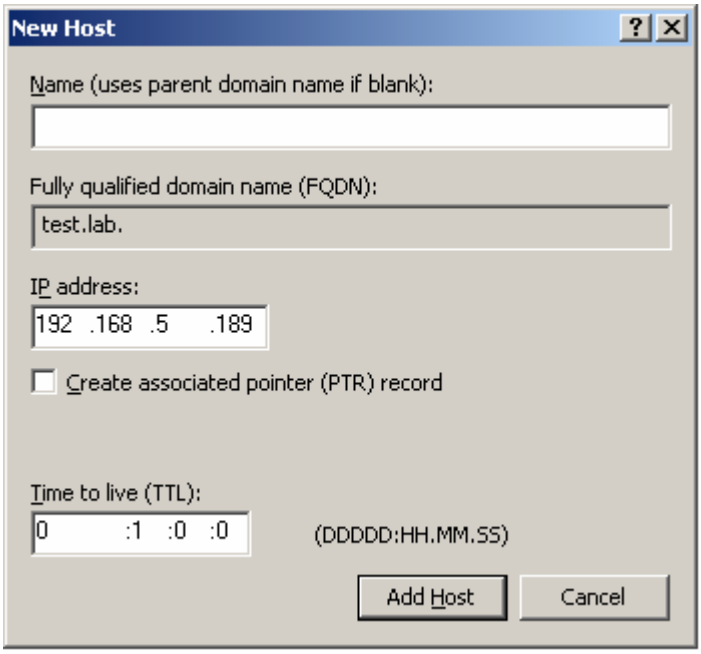
۳- در این پنجره می‌توانیم **Dynamic Update** را فعال کنیم.

۴- بر روی **OK** کلیک می‌کنیم و به این وسیله پنجره صحبت **Zone Properties** را می‌بندیم.



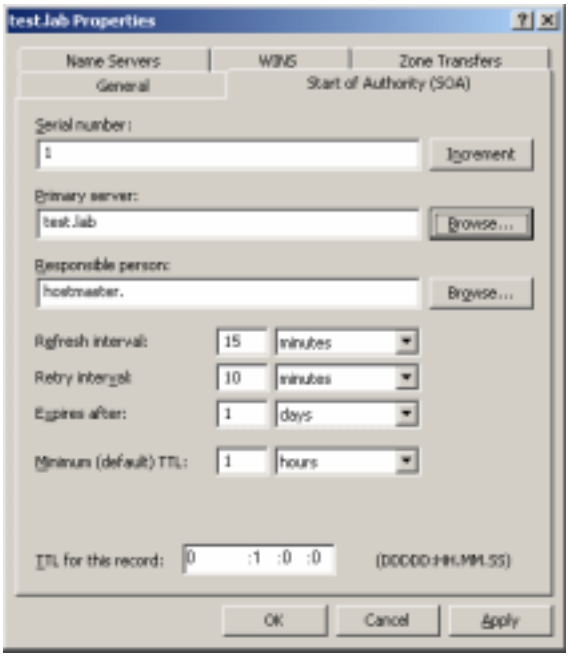
شکل ۲-۲۱: فعال کردن به روز رسانی‌های پویا بر روی سرویس‌دهنده‌های **DNS**

یکی از مشکلاتی که در هنگام پیاده‌سازی به روز رسانی پویا مشاهده می‌شود این است که پس از فعال کردن قابلیت به روز رسانی پویا برای یک **Zone** حتما بایستی نگاشت‌های منابع **NS** و **SOA** در آن **Zone** به صورت دستی تنظیم شوند. به عنوان مثال، یک **Zone** با نام **test.lab** را در نظر بگیرید. برای انجام تنظیمات مورد نظر ابتدا بایستی مطابق شکل زیر یک نگاشت میزبان **A** را بدون وارد کردن نام و با نوشتن **IP** سرویس‌دهنده **DNS**، در آن **Zone** ایجاد کرد (فرض کنید **IP** سرویس‌دهنده **DNS**، **192.168.5.189** باشد).

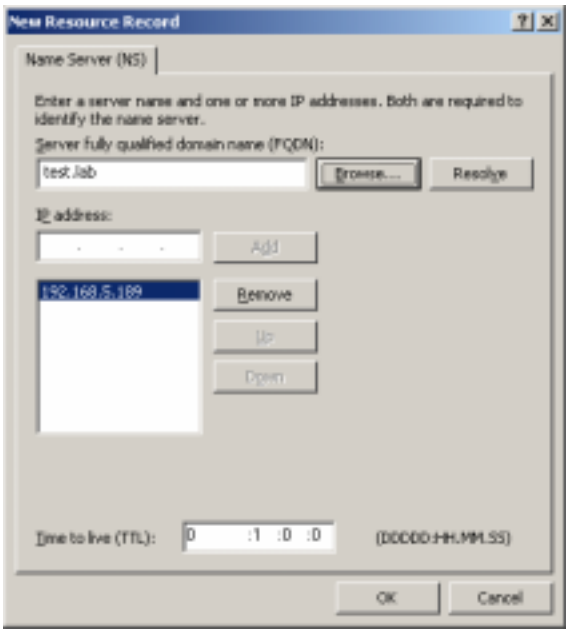


شکل ۲-۲۲: ساخت یک نگاشت میزبان **A** برای معرفی سرویس‌دهنده **DNS**

پس از این، همان‌طور که در شکل زیر نشان داده شده است باید در قسمت تنظیمات **NS** نام و آدرس سرویس‌دهنده را که به کمک مراحل بالا در **Zone** معرفی شده است را وارد کرد و در قسمت تنظیمات **SOA** نیز این سرویس‌دهنده **DNS** را به عنوان سرویس‌دهنده اولیه معرفی کرد.

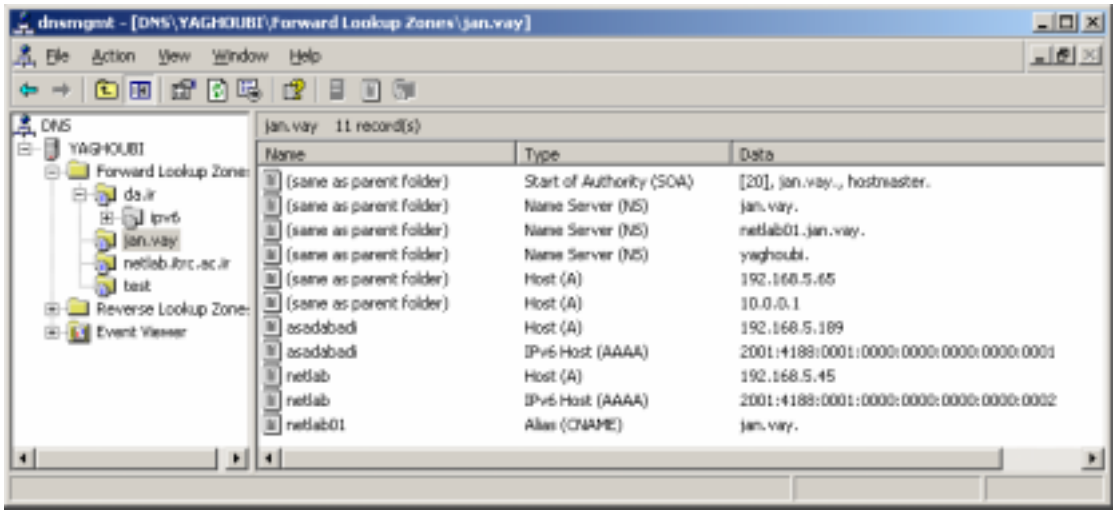


شکل ۲-۲۳: صفحه تنظیمات **SOA**



شکل ۲-۲۴: نحوه انجام تنظیمات **NS** و **SOA**

به روز رسانی پویا در **DNS** پیاده‌سازی‌شده در ویندوز ۲۰۰۳ در هر دو بستر **IPv4** و **IPv6** کار می‌کند. یعنی هم آدرس‌های **IPv6** هم آدرس‌های **IPv6** یک مشتری به صورت خودکار به سرویس‌دهنده نام دامنه فرستاده می‌شوند. در شکل چند رکورد که به صورت خودکار در **DNS** ثبت شده‌اند نشان داده شده است.

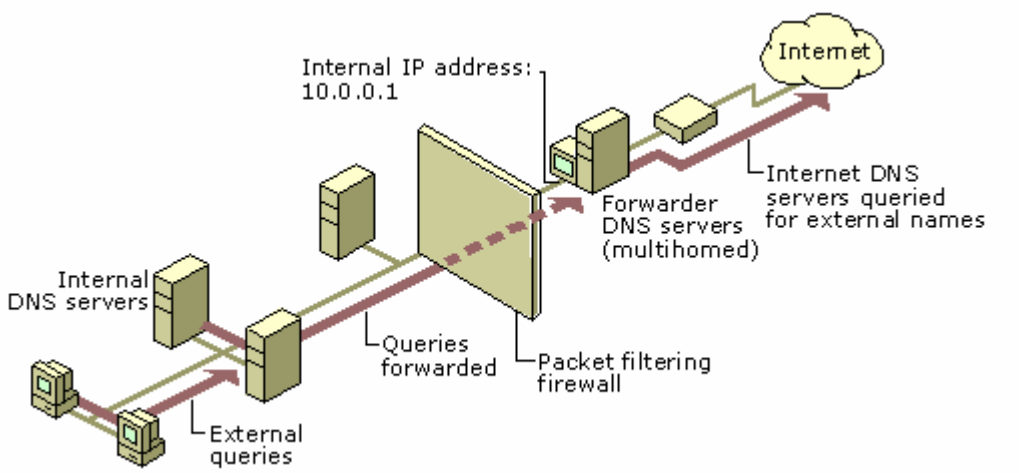


شکل ۲–۲۵: انواع رکوردهای **DNS**

۲–۱۹ بررسی Forwarder ها

Forwarder یک سرویس‌دهنده **DNS** بر روی یک شبکه است که برای ارسال سوالات **DNS** ای مربوط به نام‌های **DNS** ای خارجی به سرویس‌دهنده‌های **DNS** واقع در خارج آن شبکه مورد استفاده قرار می‌گیرند. همچنین با استفاده از **Forwarder** های شرطی[1] می‌توان سوالات را مطابق با نام‌های دامنه‌ای ویژه ارسال کرد. یک سرویس‌دهنده **DNS** بر روی یک شبکه تحت عنوان **Forwarder** طراحی می‌شود و به این ترتیب سرویس‌دهنده‌های **DNS** موجود در شبکه زمانی که قادر به تشخیص اسامی به صورت محلی نباشند، سوالات را به **Forwarder** می‌فرستند. با استفاده از یک **Forwarder** می‌توان فرآیند تشخیص اسم را برای نام‌هایی که در خارج شبکه قرار دارند، مانند نام‌های اینترنتی، مدیریت کرد و میزان بهره‌وری از فرآیند تشخیص اسم را برای کامپیوترهای موجود در شبکه بالا برد. در شکل زیر چگونگی نظارت بر سوالات مربوط به نام‌های خارجی که توسط **Forwarder** ها صورت می‌گیرد نشان داده شده است.

[1] - **Conditional Forwarders**



شکل ۲-۲۶: چگونگی نظارت بر سوالات مربوط به نام‌های خارجی به کمک **Forwarder**

بدون داشتن یک سرویس‌دهنده **DNS** که به عنوان **Forwarder** طراحی شده باشد، همه سرویس‌دهنده‌های **DNS** می‌توانند سوالات خارجی را با استفاده از **root hint** ها به خارج از یک شبکه بفرستند. در نتیجه، بسیاری از اطلاعات داخلی و احتمالا مهم مربوط به **DNS** در اینترنت قابل دسترسی خواهند شد. علاوه بر این آسیب امنیتی، این روش تشخیص می‌تواند باعث ایجاد ترافیک خارجی بزرگی شود و این مساله برای شبکه‌ای که سرعت اینترنت در آن بالا و یا پایین است، باعث بالا رفتن هزینه‌ها و کم شدن کارایی می‌شود. زمانی که یک سرویس‌دهنده **DNS** به عنوان **Forwarder** طراحی می‌شود، مسوول تماس با ترافیک خارجی خواهد شد بنابراین سرویس‌دهنده **DNS** که در داخل شبکه است در معرض اینترنت قرار نخواهد گرفت. یک **Forwarder** یک مخزن[1] بزرگ از اطلاعات **DNS** خارجی خواهد ساخت. زیرا از طریق آن همه سوالات خارجی **DNS** در شبکه تشخیص داده می‌شوند. در مدت زمان کمی یک **Forwarder** بخش مناسبی از سوالات خارجی **DNS** را با استفاده از اطلاعات ذخیره شده، تشخیص خواهد داد و به همین دلیل بار ترافیکی شبکه و در نتیجه مدت زمان پاسخگویی به مشتری‌های **DNS** کاهش خواهد یافت.

عملکرد یک سرویس‌دهنده **DNS** که برای استفاده از یک **Forwarder** تنظیم شده است متفاوت از سرویس‌دهنده **DNS** ای که برای این منظور تنظیم نشده است می‌باشد. عملکرد سرویس‌دهنده **DNS** که تنظیمات **Forwarder** بر روی آن انجام شده است به صورت زیر است:

[1]- **Cache**

۱- زمانی که سرویس‌دهنده **DNS** یک سوال را دریافت می‌کند، برای تشخیص و حل آن سوال از **Zone** های اولیه و ثانویه و نیز مخزن خود استفاده می‌کند.
۲- اگر سرویس‌دهنده **DNS** به کمک اطلاعات محلی نتواند سوال را تشخیص دهد و حل کند، آن سوال را به **Forwarder** خواهد فرستاد.
۳- سرویس‌دهنده **DNS** قبل از تلاش برای اتصال به سرویس‌دهنده‌های **DNS** که در **root hint** آن مشخص شده‌اند کمی برای دریافت پاسخ از سوی **Forwarder** صبر می‌کند.

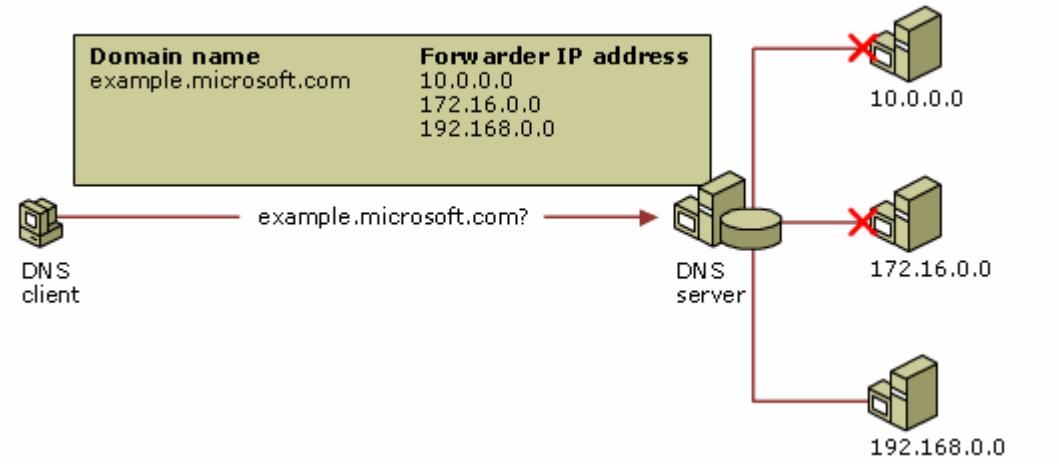
زمانی که یک سرویس‌دهنده **DNS** سوالی را به **Forwarder** می‌فرستد در واقع یک سوال بازگشتی[1] را به آن می‌فرستد. این نوع سوال با سوال تکراری[2] که سرویس‌دهنده **DNS** به دیگر سرویس‌دهنده‌های **DNS** در حالت تشخیص نام استاندارد می‌فرستد (در حالتی که از **Forwarder** استفاده نمی‌شود) متفاوت است.

۲-۲۰ بررسی مراحل Forwarding

ترتیب **IP** آدرس‌های لیست شده به عنوان **Forwarder** ها بر روی یک سرویس‌دهنده **DNS**، مشخص‌کننده ترتیب استفاده از آن‌ها است. بعد از آنکه سرویس‌دهنده **DNS** به کمک اولین **IP** آدرس، سوال را به **Forwarder** می‌فرستد قبل از آنکه عملیات فرستادن سوال را با **IP** آدرس بعدی ادامه دهد مدت زمان کوتاهی (مطابق با تنظیمات انجام شده در سرویس‌دهنده **DNS**) را برای پاسخ گرفتن از اولین **Forwarder** صبر می‌کند. این فرآیند تا زمانی ادامه می‌یابد که سرویس‌دهنده **DNS** پاسخ مثبت از یک **Forwarder** بگیرد.

به عنوان مثال، در شکل پایین **Forwarder** های اول و دوم که دارای **IP** آدرس‌های اول و دوم هستند نمی‌توانند به سرویس‌دهنده **DNS** پاسخ دهند. اما **Forwarder** با **IP** آدرس سوم، پاسخ می‌دهد و سوال به آن **Forwarder** فرستاده می‌شود.

[1] - **Recursive Query**
[2] - **Iterative Query**



شکل ۲-۲۷: ارسال سوالات به **Forwarder** ها برمبنای ترتیب آدرس‌های لیست شده در **DNS**

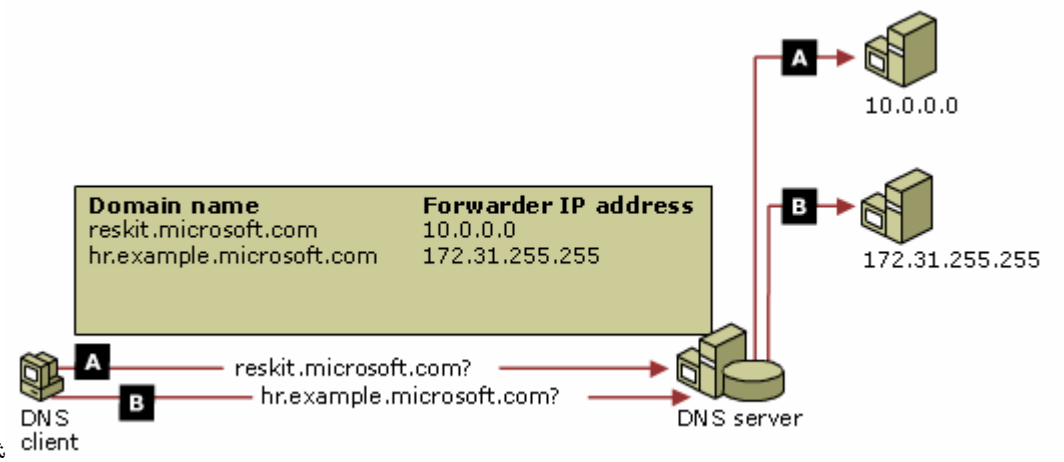
۲-۲۱ Forwarder های شرطی

Forwarder شرطی، یک سرویس‌دهنده **DNS** بر روی یک شبکه است که برای فرستادن سوالات **DNS** ای مطابق با نام دامنه **DNS** در سوال، استفاده می‌شود. به عبارت دیگر، زمانی که یک سرویس‌دهنده **DNS** نمی‌تواند سوالات خارجی را تشخیص دهد به جای فرستادن همه این سوالات به یک **Forwarder** می‌تواند به گونه‌ای تنظیم شود که مطابق با نام‌های دامنه‌ای ویژه که در هر سوال وجود دارند، سوالات را به **Forwarder** های متفاوت بفرستد. برای مثال، یک سرویس‌دهنده **DNS** می‌تواند به گونه‌ای تنظیم شود که همه سوالاتی را که نام آن‌ها به **widgets.example.com** ختم می‌شود را به آدرس **IP** یک سرویس‌دهنده **DNS** ویژه و یا آدرس‌های **IP** چندین سرویس‌دهنده **DNS** بفرستد.

تنظیمات **Forwarder** شرطی برای یک سرویس‌دهنده **DNS**، شامل موارد زیر است:

- نام دامنه‌ها که هر سرویس‌دهنده **DNS** سوالات مربوط به آن‌ها را به **Forwarder** ها خواهد فرستاد.
- آدرس‌های **IP** مربوط به **Forwarder** هایی که برای هر دامنه اسمی ویژه، مورد استفاده قرار می‌گیرند.

به عنوان مثال در شکل زیر هر یک از سوالات، با توجه به نام‌های دامنه‌ای خود به سرویس‌دهنده **DNS** مربوطه فرستاده می‌شوند.



شکل ۲۸:

شکل ۲-۲۸: چگونگی عملکرد **Forwarder** های شرطی

Forwarder های شرطی می‌توانند باعث بهبود بخشیدن فرآیند تشخیص نام، مابین فضاهای اسمی داخلی **DNS** که بخشی از فضای اسمی **DNS** در اینترنت نیستند، شوند. با تنظیم سرویس‌دهنده‌های **DNS** در یک فضای اسمی داخلی به گونه‌ای که همه سوالات را به سرویس‌دهنده‌های **DNS** معتبر در یک فضای اسمی داخلی دوم بفرستد، **Forwarder** های شرطی فرآیند تشخیص نام مابین دو فضای اسمی را بدون انجام مراحل بازگشت[1] در فضای اسمی **DNS** اینترنت، فعال می‌سازند.

مساله‌ای که در هنگام استفاده از **Forwarder** ها بایستی به آن توجه کرد این است که یک سرویس‌دهنده **DNS** نمی‌تواند سوالاتی را که مربوط به نام‌های دامنه‌ای موجود در **Zone** های آن است را به **Forwarder** بفرستد. برای مثال، سرویس‌دهنده **DNS** معتبر برای **Zone** ای با عنوان **widgets.example.com** نمی‌تواند سوالاتی را که مطابق با نام دامنه‌ای **widgets.example.com** هستند را به **Forwarder** بفرستد. در صورتی که **hr.widgets.example.com** به سرویس‌دهنده **DNS** دیگری محول شده باشد، سرویس‌دهنده **DNS** معتبر برای **widgets.examole.com** می‌تواند سوالات مربوط به نام‌هایی را که به **hr.widgets.example.com** ختم می‌شوند را به **Forwarder** بفرستد.

[1] - **Recursion**

۲-۲۲ تشخیص نام در شبکه اینترنت داخلی[1]

استفاده از یک **Forwarder** شرطی می‌تواند تشخیص نام برای دامنه‌ها را در شبکه اینترنت داخلی بهبود بخشد. تشخیص نام در شبکه اینترنت داخلی با تنظیم سرویس‌دهنده‌های **DNS** برای استفاده **Forwarder** هایی برای نام‌های دامنه‌ای داخلی ویژه، بهبود می‌یابد. برای مثال، همه سرویس‌دهنده‌های **DNS** در دامنه **widgets.example.com** می‌توانند برای فرستادن سوالات مربوط به نام‌های ختم‌شونده با **test.example.com** به سرویس‌دهنده‌های معتبر برای **merged.widgets.examole.com**، تنظیم شوند. بنابراین مرحله سوال از **root server** های **example.com** و یا مرحله تنظیم سرویس‌دهنده‌های **DNS** در **widgets.example.com zone** با **Zone** های ثانویه برای **test.example.com** حذف می‌شوند.

۲-۲۳ تشخیص نام در شبکه اینترنت

سرویس‌دهنده‌های **DNS** می‌توانند از **Forwarder** های شرطی برای تشخیص سوالات مابین نام‌های دامنه‌ای **DNS** شرکت‌هایی که اطلاعات را پخش می‌کنند، استفاده کنند. برای مثال، شرکت‌های **Widgets Toys** و **Tailspin Toys** سعی در بهبود چگونگی تشخیص نام‌های مشتریان **DNS** در **Tailspin Toys** توسط مشتری‌های **DNS** در **Widgets Toys** دارند. مجریان اجرایی **Tailspin Toys** مجریان اجرایی **Widgets Toys** را درباره مجموعه سرویس‌دهنده‌های **DNS** در شبکه **Tailspin Toys** که **Widgets** می‌تواند سوالات مربوط به دامنه **dolls.tailspintoys.com** را به آنجا بفرستد، مطلع می‌سازند. سرویس‌دهنده‌های **DNS** در داخل شبکه **Widgets Toys** به گونه‌ای تنظیم می‌شوند که همه سوالات مربوط به نام‌های ختم‌شونده با **dolls.tailspintoys.com** را به سرویس‌دهنده‌های **DNS** در شبکه **Tailspin Toys** بفرستند. در نتیجه، سرویس‌دهنده‌های **DNS** در شبکه **Widgets Toys** برای تشخیص سوالات مربوط به نام‌های ختم‌شونده با **dolls.tailspintoys** نیاز به سوال از **root server** های داخلی خود و یا **root server** های اینترنتی ندارند.

[1] - **Intranet**

۲-۲۴ تنظیمات سرویس دهنده DNS برای استفاده از Forwarder ها

۲-۲۴-۱ تنظیمات در windows

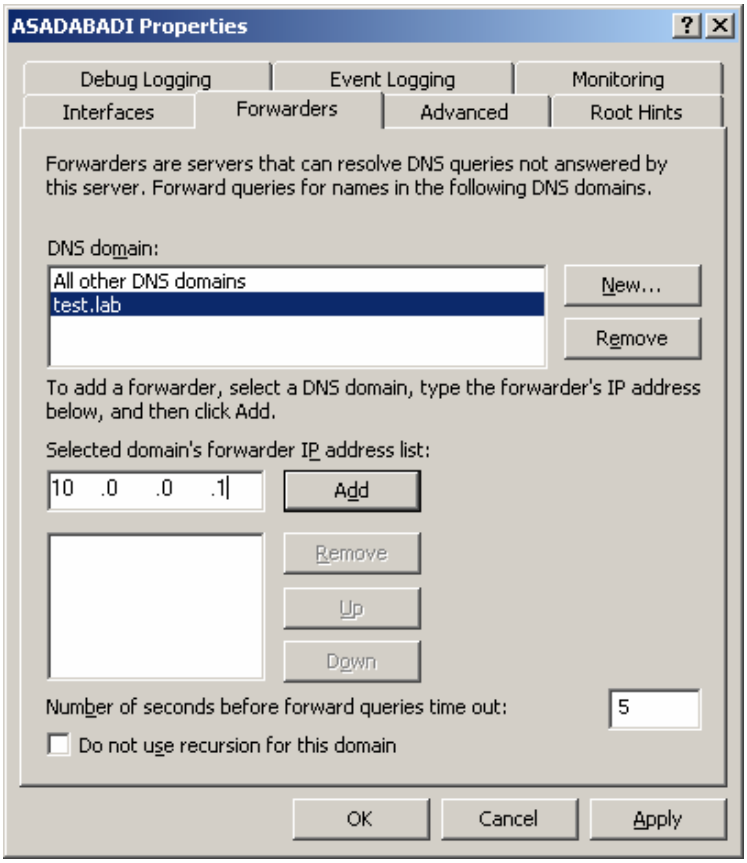
۱- ابتدا پنجره اصلی **DNS** را باز می‌کنیم.

۲- در **console tree** بر روی سرویس‌دهنده **DNS** کلیک می‌کنیم.

۳- در منوی **Action** در روی **Properties** کلیک می‌کنیم.

۴- بر روی قسمت **Forwarders**، زیر **DNS domain** یک نام دامنه‌ای وارد می‌کنیم.

۵- همان‌طور که در شکل زیر نشان داده شده است زیر **Selected domain's forwarder IP address list**، آدرس **IP** یک **Forwarder** را می‌نویسیم و سپس بر روی **Add** کلیک می‌کنیم.



شکل ۲-۲۹: چگونگی تنظیمات سرویس‌دهنده **DNS** برای استفاده از **Forwarder** ها در **windows**

۲-۲۴-۲ تنظیمات با استفاده از خط فرمان

۱- صفحه **Command Prompt** را باز می‌کنیم.

۲- دستور زیر را می‌نویسیم.

dnscmd **ServerName** /ZoneAdd **ZoneName** /Forwarder **MasterIPaddress …[**/TimeOut **Time] [**/Slave**]**

توضیحات مربوط به دستور در جدول ۲ آورده شده است.

Value	Description
dnscmd	Specifies the name of the command-line tool.
ServerName	Required. Specifies the DNS host name of the DNS server. You can also type the IP address of the DNS server. To specify the DNS server on the local computer, you can also type a period (.).
/ZoneAdd	Required. Adds a zone.
ZoneName	Required. Specifies the fully qualified domain name (FQDN) of the zone.
/Forwarder	Required. Specifies the command to configure a forwarder. When configuring forwarders on DNS servers running on Active Directory domai controllers, you must use **/DsForwarder** in place of **/Forwarder**. **/DsForwarder** will replicate the forwarder setting to all DNS servers running on domain controllers in an Active Directory domain.
MasterIPaddress...	Required. Specifies a space-separated list of one or more IP addresses of the DNS servers where queries for *ZoneName* are forwarded. You may specify a list of space-separated IP addresses.
/TimeOut	Specifies the timeout setting. The timeout setting is the number of second before unsuccessful forward queries time out.
Time	Specifies the value for the **/TimeOut** parameter. The value is in seconds. The default timeout is 5 seconds.
/Slave	Determines whether or not the DNS server uses recursion when querying for the domain name specified by *ZoneName*.

جدول ۲

در تنظیم **Forwarder**ها نیز همانند تنظیم **Delegation** به یک بستر **IPv4** نیازمندیم. به عبارت دیگر **DNS** ارایه شده در **Windows Server 2003** از پیاده‌سازی **Forwarder**ها در بستر **IPv6** به تنهایی پشتیبانی نمی‌کند.

۲-۲۵ طول نام دامنه‌ای Forwarder های شرطی

زمانی که یک سرویس‌دهنده **DNS** با یک **Forwarder** شرطی برای یک دامنه اسمی، تنظیم می‌شود، آن نام دامنه‌ای را با تمامی وضعیت‌های نام دامنه‌ای موجود در لیست خود مقایسه می‌کند و از طولانی‌ترین وضعیت نام دامنه‌ای که مربوط به نام دامنه‌ای سوال است استفاده می‌کند. برای مثال، در

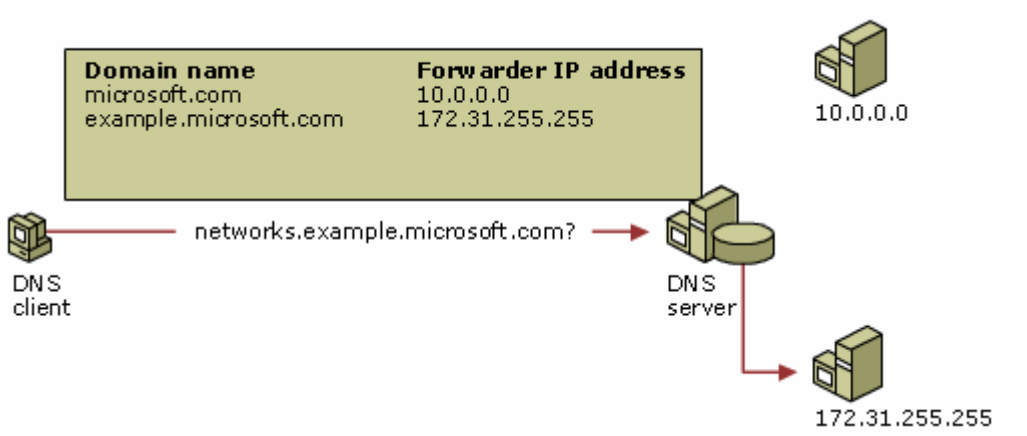
شکل زیر، سرویس‌دهنده **DNS** منطق زیر را برای مشخص کردن نحوه فرستادن یک سوال برای یک نام دامنه‌ای انجام می‌دهد:

۱- سرویس‌دهنده **DNS** سوالی را برای **toys.widgets.example.com.** می‌فرستد.

۲- سرویس‌دهنده **DNS**، آن نام دامنه‌ای را با **example.com** و **widgets.example.com** مقایسه می‌کند.

۳- سرویس‌دهنده **DNS** مشخص می‌کند که **widgets.example.com** نام دامنه‌ای است که نزدیکترین تطابق را با دامنه اسمی سوال دارد.

۴- سرویس‌دهنده **DNS** سوال را به سرویس‌دهنده **DNS** با آدرس **172.31.255.255** که مربوط به **widgets.example.com** است می‌فرستد.



شکل ۲-۳۰: ارسال سوال به **Forwarder** با استفاده از طولانی‌ترین وضعیت نام دامنه‌ای مربوط به سوال

منابع و مراجع

[1] Microsoft IPv6 Technical Resource, Available at: http://www.microsoft.com/ipv6

[2] Microsoft Windows Server 2003 Technical Resource, Available at: http://www.microsoft.com/windowsserver2003/techinfo/default.mspx

[3] www.cisco.com

[4] Introduction to IP Version 6, Microsoft Corporation, Published: September 2003, Updated: March 2004

[5] Jeff Madden, MCSE Training Kit--Microsoft Windows 2000 Server, Microsoft Press, A Division of Microsoft Corporation, Washington 2000