

DNS و روش‌های تبدیل اسم به IP

هدف‌های رفتاری: هنرجو پس از پایان این فصل می‌تواند:

- کاربردهای DNS را بیان کند.
- اسامی اینترنتی و Host Name را شناسایی کند.
- اجزای DNS را توضیح دهد.
- مراحل تبدیل اسم به IP را در اینترنت شرح دهد.
- یک سرویس DNS را نصب و راه اندازی کند.
- سرویس DNS را برای انجام عمل Name Resolution آزمایش کند.

۱۳-۱- کاربردهای DNS

سرویس Domain Name System یا سیستم نام دامنه، به اختصار DNS نامیده می‌شود. همانطور که قبلاً اشاره شد، برای دسترسی به یک رایانه در یک شبکه محلی هم می‌توان از نام رایانه استفاده نمود و هم امکان استفاده از آدرس IP آن رایانه وجود دارد. برای ورود به وب سایت‌های اینترنتی هم این شرایط صادق است، یعنی هم می‌توان آدرس سایت (نام سایت) را در مرورگر وب^۱ وارد کرد و هم می‌توان با دانستن آدرس IP وب سرور، به سایت مورد نظر دسترسی پیدا نمود، ولی اکثر کاربرها ترجیح می‌دهند به جای استفاده از اعداد و ارقام آدرس IP، از نام آن سایت استفاده کنند، چرا که به خاطر سپردن نام به مراتب راحت‌تر از آدرس IP می‌باشد. (توجه داشته باشید که به خاطر سپردن IPv6 به مراتب سخت‌تر خواهد شد)

به عنوان مثال با استفاده از آدرس IPv4 مربوط به سازمان سنجش آموزش کشور (که برابر

^۱ - Web Browser

1. 92.242.195 (می‌باشد) و وارد کردن این عدد IP در مرورگر وب، می‌توان وب سایت سازمان سنجش را مشاهده نمود، ولی با استفاده از آدرس www.sanjesh.org هم می‌توان به آن دسترسی پیدا کرد. با توجه به مطالب فوق باید مکانیزمی برای تطبیق نام و آدرس IP وجود داشته باشد تا از بروز خطا جلوگیری شود که به آن مکانیم در شبکه‌های رایانه ای سرویس DNS می‌گویند. بنابراین سرویس DNS عمل تطبیق نام با آدرس IP را انجام می‌دهد (در حقیقت DNS، یک سیستم پایگاه داده ای است که نام FQDN را به آدرس IP ترجمه می‌کند)

سرویس Domain Name System (DNS) در اینترنت و بسیاری از شبکه‌های خصوصی استفاده می‌شود و نقش کلیدی در ویندوز ۲۰۰۸ سرور دارد و یکی از کارهای اصلی آن تبدیل اسم به IP و بالعکس می‌باشد. لازم به ذکر است که اکتیو دایرکتوری (AD) به کمک DNS تحلیل نام رایانه و پیدا کردن آن‌ها در شبکه را انجام می‌دهد.

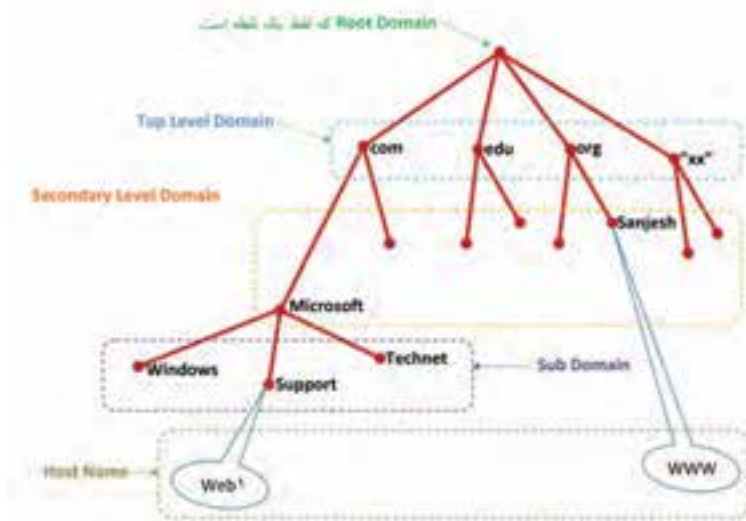
می‌توان گفت که استفاده از DNS شبیه برقراری یک تماس تلفنی با گوشی تلفن همراه می‌باشد، وقتی که شما نام مخاطب را تعیین می‌کنید، به طور خودکار شماره مخاطب مورد نظر در دسترس قرار خواهد گرفت.

نکته: قبل از DNS، تطبیق نام با آدرس IP با استفاده از پرونده‌های متنی به نام پرونده میزبان (Host File) که به صورت محلی بر روی هر رایانه ذخیره شده بود انجام می‌گرفت. پرونده میزبان حاوی اسامی و آدرس‌های IP متناظر با آن اسامی می‌باشد. هر گاه یک میزبان جدید به شبکه اضافه می‌شد، مدیر شبکه به صورت دستی نام میزبان جدید و آدرس IP آن را به پرونده میزبان اضافه و آن را به روز رسانی می‌کرد.

۲-۱۳- انواع اسامی دامنه DNS

سرویس DNS از نام گذاری سلسله مراتبی پشتیبانی می‌کند و به عنوان یک پایگاه داده سلسله مراتبی و توزیع شده می‌باشد که حاوی انواع داده‌ها، اسامی دامنه و اسامی میزبان می‌باشد. اسامی در DNS از ساختار درختی سلسله مراتبی به نام فضای نام دامنه یا Domain Namespace تشکیل شده است و از پنج مجموعه برای تشریح فضای نام دامنه (Domain Namespace) استفاده می‌شود.

الف) Root Domain : در بالاترین محل ساختار درختی دامنه ریشه (Root Domain) قرار دارد و به صورت یک نقطه "." می باشد یعنی تمام اسامی اینترنتی به یک نقطه ختم می شوند البته در موقع درج یک آدرس استفاده از نقطه الزامی نیست و معمولاً در معرفی یک آدرس اینترنتی آن را نمی نویسند، ولی باید توجه داشته باشید که این نقطه بخشی از نام آدرس اینترنتی می باشد (برخلاف نقطه های دیگر آدرس که به عنوان جدا کننده استفاده می شود).



شکل ۱-۱۳- ساختار درختی آدرس اینترنتی

با توجه ساختار درختی ۱-۱۳ می توان FQDN های زیر را نوشت

Web1.support.Microsoft.com.

www.sanjesh.org.

ب) Top Level Domain یا TDL : دومین بخش از ساختار درختی یک آدرس می باشد که تعیین کننده حوزه فعالیت می باشد و به دو بخش تجزیه می شود :

● **Generic TDL یا gTDL :** به مفهوم حوزه عمومی فعالیت و تعیین کننده نوع سازمان بوده و شامل پسوندهایی نظیر com, edu, net, org, sch و ac می باشد.

● **ccTDL یا Country Code :** از یک استاندارد دو حرفی برای تعیین کشور (حوزه جغرافیایی) استفاده می شود مانند ir, tw, ip, uk, us و که به ترتیب مشخص کننده کشورهای ایران، تایوان، عراق، ژاپن، انگلیس و آمریکا و ... می باشد.

به عنوان مثال آدرس www.bmi.ir، آدرس اینترنتی بانک ملی جمهوری اسلامی ایران می باشد.

در بعضی از مواقع gTDL و ccTDL به صورت ترکیبی مورد استفاده قرار می گیرند به طوری که ابتدا gTDL و سپس ccTDL قرار می گیرد

gTDL.ccTDL

به عنوان مثال در ایران gov.ir برای وزارتخانه ها و فرمانداری ها و سایر مؤسسات دولتی استفاده می شود.

www.refah.gov.ir (وزارت رفاه)، www.mfa.gov.ir (وزارت امور خارجه) و www.kashan.gov.ir (فرمانداری کاشان) و www.gilan.mim.gov.ir (سازمان صنایع و معادن استان گیلان) و www.oil.gov.iq (وزارت نفت عراق)

به عنوان نمونه دیگر برای مدارس و سازمان های وابسته به آن در کشور ما، از sch.ir استفاده می شود.

مانند www.chap.sch.ir (پایگاه کتاب های درسی)، www.talif.sch.ir (دفتر برنامه ریزی و تألیف کتب درسی) و www.jafari.sch.ir (هنرستان علامه جعفری)

همچنین برای دانشگاه های ایران از پسوند ac.ir استفاده می شود :

مانند www.tvu.ac.ir (دانشگاه فنی و حرفه ای کشور)، www.pnu.ac.ir (دانشگاه

پیام نور) و www.nit.ac.ir (دانشگاه صنعتی نوشیروانی بابل)

ج) Secondary Level Domain یا SLD : دومین سطح دامنه می باشد که به صورت منحصر به فرد بوده و می توان آن را به صورت حقیقی^۱ یا حقوقی^۲ به ثبت رساند.

مطالعه آژواه

مدیریت Domain Root در اختیار شرکت بین المللی غیر انتفاعی ICANN^۳ می باشد (آدرس سایت شرکت www.icann.org می باشد) که ابتدا این مدیریت قبل از سال ۱۹۹۸ در اختیار دولت آمریکا بود. ضمناً gTLD نیز توسط ICANN

۲- ثبت به نام شرکت یا مؤسسه

۱- ثبت به نام شخص

۳- Internet Corporation for Assigned Numbers and Names

مدیریت می‌شود و به یک سری از ثبات‌های معتبر واگذار شده است. اینترنتیک InterNIC^۱ (زیرمجموع ICANN است) سازمانی است که domain name ها را صادر می‌کند، ولی مدیریت ccTLD به کشورهای مربوطه واگذار شده است (مانند ir که به ایران واگذار شده است). در ایران امتیاز و مسئولیت دامنه‌ها برعهده پژوهشگاه دانش‌های بنیادی است. لازم به ذکر است شرکت ICANN محتوای اینترنت را کنترل نمی‌کند، بلکه فقط آدرس‌های اینترنتی را کنترل می‌نماید.

د) Sub Domain : زیر دامنه که به شرکت‌های مربوطه واگذار می‌شود (در واقع به SLD واگذار می‌شود) برای مثال شرکت Microsoft می‌تواند زیر دامنه Support یا هر زیر دامنه دلخواه دیگر را ایجاد نماید و کنترل نام زیر دامنه برعهده شرکت Microsoft خواهد بود.

ه) Host Name : می‌توان نام میزبان را مانند برگ در درخت دانست که برای شناسایی یک منبع خاص استفاده می‌شود.

با توجه به ساختار درختی فوق می‌توان آدرس کامل یک سایت یا FQDN یک سایت را به صورت زیر نوشت :

www.support.microsoft.com

FQDN^۲ یک نام منحصر به فرد برای شناسایی موقعیت میزبان درون درخت سلسله مراتبی DNS می‌باشد. به عبارت دیگر FQDN، محل دقیق قرارگیری یک کامپیوتر در دامنه را توصیف می‌کند. حال با توجه به مطالب فوق می‌توان فرم کلی اسامی اینترنتی را به صورت زیر نوشت :

Host.subdomain.SLD.TLD

۱۳-۳-۲ اجزای DNS

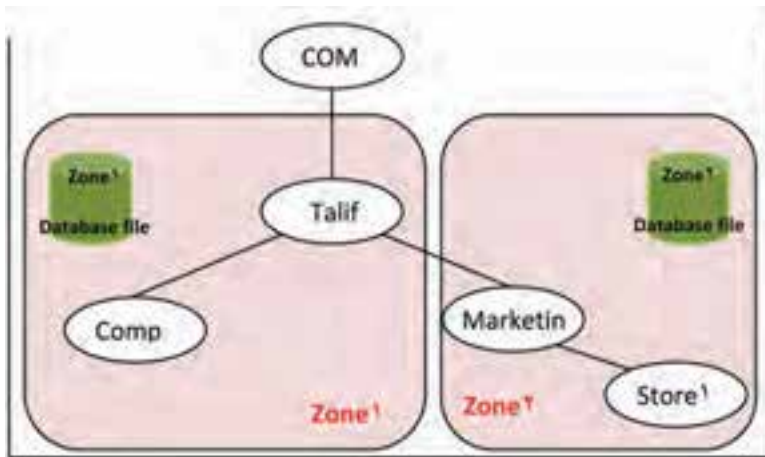
۱-۱۳-۳ Zone : بخشی از فضای نام دامنه (Domain namespace) در DNS می‌باشد. یک Zone فضای نام دامنه را به چند بخش تقسیم می‌کند تا مدیریت آنها برای مدیران راحت‌تر شود. باید توجه داشت که Zone معادل Domain نیست بلکه از یک یا چند Domain مجاور هم تشکیل شده است. (چند Domain غیر مجاور نمی‌توانند یک Zone را تشکیل دهند) بنابراین Zone ها

^۱ - Internet Network Information Center

^۲ - Fully Qualified Domain Name

شامل رکوردهای منابع برای اسامی یک منطقه خاص می‌باشد. در یک سرور DNS، پرونده‌های Zone شامل رکوردهای بانک اطلاعاتی DNS Server می‌باشد ولی زمانی که AD با DNS به صورت مجتمع نصب می‌شوند داده‌های DNS داخل AD ذخیره خواهند شد.

به عنوان مثال، در شکل ۱۳-۲، قلمروی Talif.com به دو Zone تقسیم شده است. این Zone ها به یک مدیر اجازه می‌دهند قلمروی Talif و sales را مدیریت کند و به مدیر دیگر، مدیریت قلمرو marketing و Stroe1 را واگذار می‌کند.



شکل ۱۳-۲

هر Zone شامل یک بانک اطلاعاتی مخصوص به خود است که تمامی اطلاعات مربوط به زیر دامنه‌های خود را در آن نگهداری می‌کند.

۱۳-۳-۲ Name Server: به کامپیوتری گفته می‌شود که سرویس DNS بر روی آن نصب

شده باشد و داده‌های مربوط به یک Zone یا چندین Zone را در خود نگهداری کند. در واقع Name Server دارای یک فایل بانک اطلاعاتی اصلی است که به بانک اطلاعاتی Zone ها اشاره دارد.

۱۳-۳-۳ Name Resolution: فرآیندی است که توسط Name Server جهت پیدا

کردن کامپیوتر در یک دامنه، با تبدیل اسم به IP و یا بالعکس، انجام می‌گیرد.

DNS دو نوع درخواست را بررسی می‌کند:

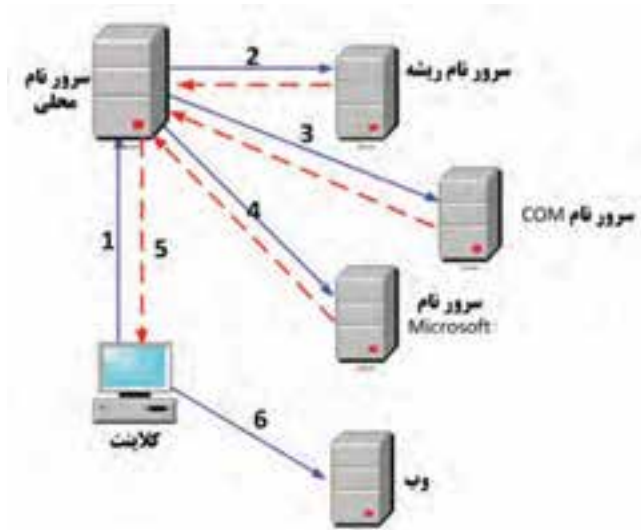
● **Forward Lookup Query:** درخواست‌های Forward، نام را به IP تبدیل می‌کنند.

Client درخواست خود را به Name Server محلی خود ارسال می‌کند. Name Server

اگر پاسخ در خواست را داشته باشد به Client جواب می‌دهد، در غیر این صورت در خواست Client

را به یک Name Server دیگر می‌فرستد.

مراحل تحلیل این درخواست، در شکل ۳-۱۳ برای پیدا کردن IP آدرس www.microsoft.com نشان داده شده است.



شکل ۳-۱۳

مراحل شکل ۳-۱۳، عملیات زیر را به تصویر کشیده‌اند:

۱- کلیانت (Client) درخواست forward برای www.microsoft.com را به سرور محلی خود ارسال می‌کند.

۲- سرور محلی، درخواست را با بانک اطلاعاتی خود مقایسه می‌کند در صورتی که این درخواست قبلاً ثبت شده باشد و IP آن را یک بار جستجو کرده باشد، IP را به کلیانت بازمی‌گرداند اما اگر قبلاً این آدرس درخواست نشده باشد برای شناسایی قلمروی Top-level آن، درخواست را برای سرور ریشه (Root Server) ارسال می‌کند. بعد از بازگشت مشخص می‌کند قلمروی آن www.microsoft.com است.

۳- سرور محلی، درخواست را به سرور com می‌فرستد. آدرس تحلیل و در پاسخ، Second-level، microsoft را برمی‌گرداند.

۴- سرور محلی این بار درخواست را به سرور microsoft ارسال می‌کند. با توجه به این که این آدرس در سرور microsoft ثبت گردیده، این سرور IP آن را برای سرور محلی برمی‌گرداند.

۵- سرور محلی، IP را به کلیانت می‌فرستد.

۶- Client، IP را دریافت کرده و در اختیار مرورگر خود قرار می‌دهد تا کاربر توسط آن به سایت مورد درخواست خود دسترسی پیدا کند.

نکته: Name Server Caching : وقتی که Name Server فرآیند جست‌وجو را انجام می‌دهد برای گرفتن پاسخ به چندین پرس و جو نیاز دارد به همین دلیل برای کاهش بار ترافیک شبکه، نتایج آنها را Cache می‌کند. این نتایج برای مدت زمان معینی با عنوان TTL (Time To live) نگهداری می‌شوند.

● **Reverse lookup Query :** درخواست‌های Reverse، IP را به نام تبدیل می‌کنند. معمولاً ابزارهای عیب‌یابی مانند دستور NSlookup از این سرویس برای برگشت گزارش به Client استفاده می‌کنند که در ادامه تشریح خواهد شد.

۳-۱۳- **Resource Records :** بانک اطلاعاتی Zone، اطلاعات خود را به صورت رکورد ذخیره می‌کند. این رکوردها به صورت‌های متفاوتی، اطلاعاتی را نگه‌داری می‌کنند که مهمترین آنها عبارتند از :

● **رکورد (Host (A or AAAA) :** رکورد نوع A بیشترین نوع رکوردی است که در DNS و برای اختصاص نام دامنه یک کامپیوتر به آدرس IPv4 استفاده می‌شود. AAAA (خوانده شود quad-A) جهت تعریف رکورد برای کامپیوتر دارای آدرس IPv6 به کار می‌رود.

● **رکورد (Alias (CNAME) :** به شما امکان می‌دهد که چندین نام را برای یک کامپیوتر خاص استفاده کنید. برای مثال سرورهای معروفی که به نام www نام‌گذاری شده‌اند اغلب از نوع CNAME هستند.

● **رکورد (Pointer (PTR) :** رکورد نوع PTR در بخش Reverse استفاده می‌شود و به منظور اختصاص IP به نام دامنه یک کامپیوتر به کار می‌رود.

● **رکورد (Service location (SRV) :** رکوردهای SRV برای پیدا کردن محل یک سرویس مشخص در دامنه مورد استفاده قرار می‌گیرد. برنامه‌های کاربردی مثل AD، توسط این نوع رکورد آدرس سرورهای مرتبط با خود را پیدا می‌کنند.

● **رکورد NS :** از این رکورد برای معرفی Name Server استفاده می‌شود. این رکورد قابل ایجاد به صورت دستی نمی‌باشد.

۱۳-۴- نصب و راه اندازی سرویس DNS

۱-۴-۱۳- نصب سرویس DNS : این سرویس به طور پیش فرض هنگام نصب AD، بر روی سرور نصب می شود این سرویس مخصوص AD نیست و برای DHCP و WINS نیز استفاده می شود و همچنین می توان آن را بر روی سرویس دهنده های Stand alone نیز نصب کرد. برای نصب مجزای این سرویس از ابزار Server Manager استفاده می شود. با انتخاب گزینه Add Roles دربخش Roles این برنامه، پنجره ای مطابق با شکل ۱۳-۴ ظاهر می شود.



شکل ۱۳-۴

گزینه DNS Server را فعال و دکمه Next را انتخاب کنید.



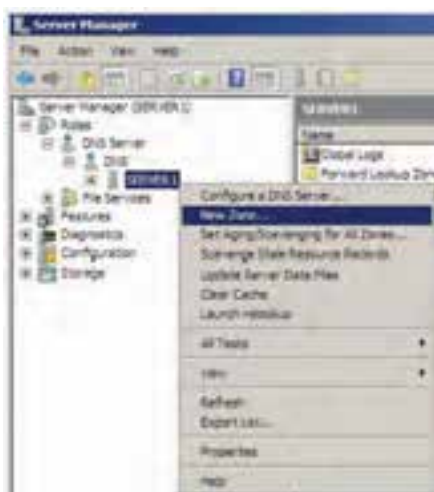
شکل ۱۳-۵

در پنجره بعدی توضیحاتی در مورد DNS و مفاهیم آن نمایش داده می شود. دکمه Next را کلیک کنید.

در پنجره بعدی (شکل ۱۳-۵) با انتخاب دکمه Install، فرآیند نصب DNS شروع می شود.

پس از پایان این فرآیند، ابزار DNS در مسیر Start → Administrative Tools قرار می‌گیرد. به این ترتیب سرور شما تبدیل به یک DNS Server (Name Server) شده است و می‌تواند به سرویس گیرنده‌ها برای اتصال به اینترنت و شبکه‌های دیگر سرویس دهی کند.

نکته: برای حذف DNS Server در پنجره Server Manager از منوی Action گزینه Remove Roles را انتخاب نموده و در وینارد نمایش داده شده سرویس DNS را برای حذف انتخاب نمایید.



۲-۴-۱۳- ایجاد کردن

Zone: می‌خواهیم یک Zone به نام test.com ایجاد کنیم. مطابق با شکل ۶-۱۳، بر روی گزینه Forward Lookup zones کلیک راست کرده و گزینه New Zone را انتخاب کنید.

شکل ۶-۱۳

پنجره welcome ظاهر می‌شود دکمه Next را کلیک کنید.



شکل ۷-۱۳

پنجره شکل ۸-۱۳ به نمایش درمی آید.



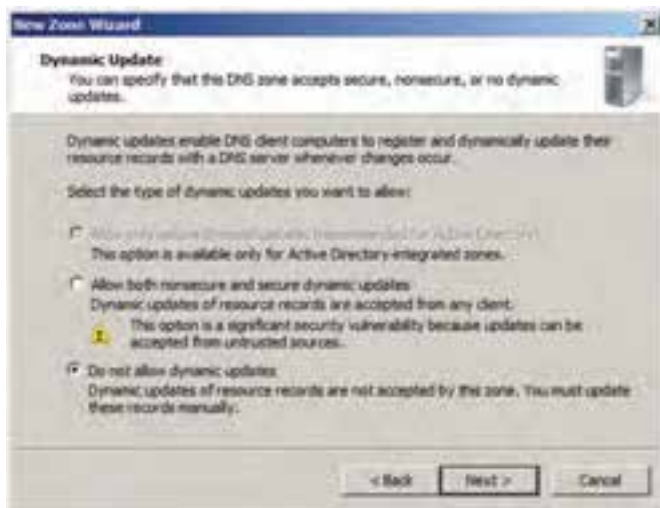
شکل ۸-۱۳

در این پنجره نوع Zone و نحوه ارتباط Zone با AD از ما سؤال می شود و چون از بحث این کتاب خارج است، حالت پیش فرض را انتخاب و گزینه ... Store the zone را غیر فعال کنید. سپس روی Next کلیک کنید. در پنجره بعد نام Zone از شما سؤال می شود، test.com را در کادر Zone name وارد کنید و روی دکمه Next کلیک کنید. (شکل ۹-۱۳)



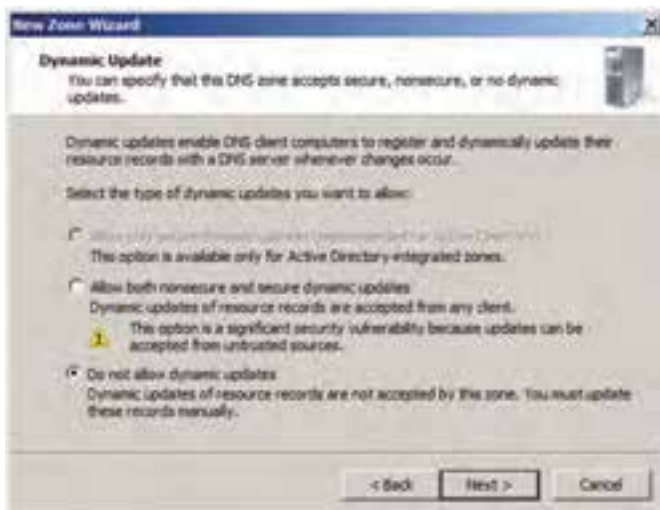
شکل ۹-۱۳

پنجره شکل ۱۰-۱۳ ظاهر می‌شود. در این پنجره نام پرونده Zone، جهت ذخیره اطلاعات مربوط به آن از شما سؤال می‌شود. نام پیش فرض را قبول کرده و روی گزینه Next کلیک کنید.



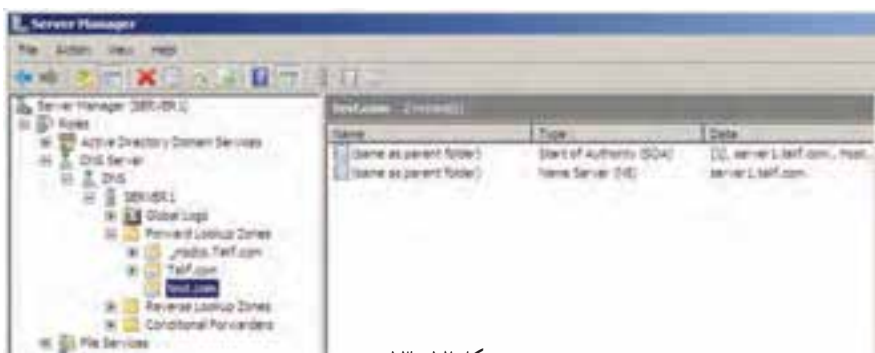
شکل ۱۰-۱۳

در پنجره بعدی نوع به روز رسانی اطلاعات مربوط به رکوردها سؤال می‌شود. حالت پیش فرض را تأیید کنید. (شکل ۱۱-۱۳)



شکل ۱۱-۱۳

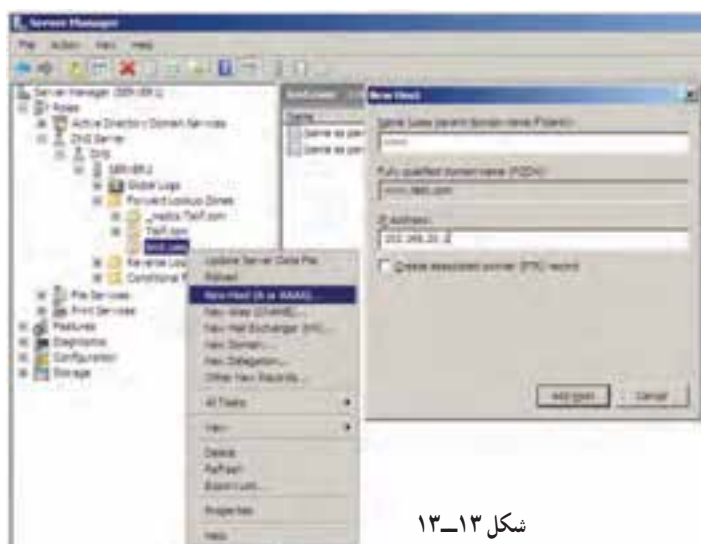
در پنجره آخر، خلاصه‌ای از مشخصات Zone تعریف شده نمایش می‌یابد. با تأیید آن، Zone به لیست بخش Forward Lookup Zones اضافه می‌شود. (شکل ۱۲-۱۳)



شکل ۱۲-۱۳

۳-۴-۱۳- ایجاد کردن **Resource Record**: برای ایجاد رکورد، بر روی Zone، test.com، کلیک راست کرده و از منویی که ظاهر می‌شود گزینه New Host (A or AAAA) را انتخاب کنید.

در پنجره‌ای که باز می‌شود در قسمت Name، www و در قسمت IP address، IP سرویس دهنده مورد نظر را وارد کنید. اگر می‌خواهید که برای این رکورد، یک PTR نیز به طور خودکار ایجاد شود گزینه Create associated pointer (PTR) record را فعال کنید. سپس دکمه Add Host را انتخاب کنید (شکل ۱۳-۱۳).



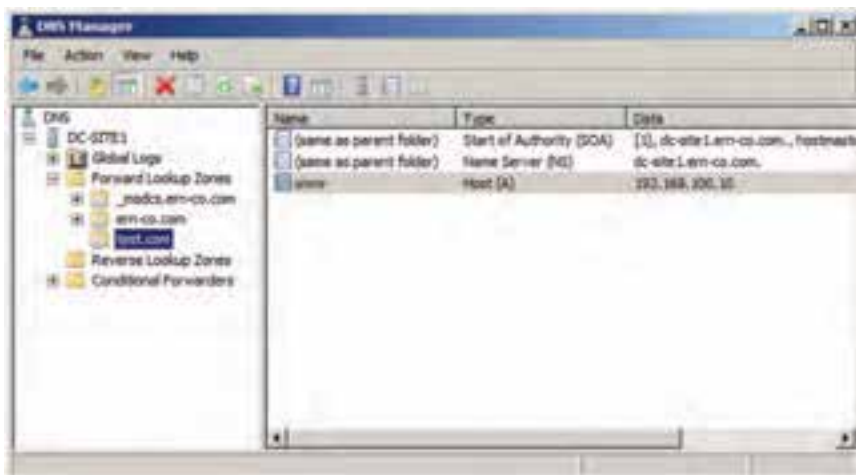
شکل ۱۳-۱۳

بعد از کلیک بر روی Add Host کادر تأیید شکل ۱۴-۱۳ ظاهر می‌گردد.



شکل ۱۴-۱۳

همان‌طور که در شکل ۱۵-۱۳ مشاهده می‌کنید، یک رکورد از نوع Host(A) با نام www در Zone، test.com ایجاد شده است.



شکل ۱۵-۱۳

۴-۱۳-۴- تست کردن DNS برای انجام عمل Name Resolution :

می‌خواهیم یک درخواست (Query) به سرور DNS ارسال کنیم تا IP رکوردهای تعریف شده در بانک اطلاعاتی Zone ها را ببینیم. برای انجام این کار می‌توان از یکی از دو دستور زیر استفاده کرد :

□ دستور ping : با اجرای دستور ping www.test.com مطابق با شکل

۱۶-۱۳، مشاهده خواهید کرد که IP نام رکورد درخواست شده به شما نشان داده می‌شود.

```

Administrator: C:\Windows\system32\cmd.exe

C:\Users\Administrator>ping www.test.com

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

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

C:\Users\Administrator>_

```

شکل ۱۶-۱۳

بعد از اجرای فرمان Ping اگر ارتباط برقرار نباشد، پیغام خطای Ping request could not find host ظاهر می‌گردد.

□ دستور nslookup : فرمان nslookup را به دو صورت می‌توانید مورد استفاده قرار دهید.

● *nslookup SiteName* : مانند nslookup www.tci.ir

(البته زمانی می‌توانید IP سایت‌های اینترنتی را پیدا کنید که به اینترنت متصل

باشید.)

```

Administrator: C:\Windows\system32\cmd.exe

C:\Users\Administrator>nslookup www.tci.ir
DNS request timed out.
    timeout was 2 seconds.
Server: Unknown
Address: 192.168.1.1

Non-authoritative answer:
Name:   www.tci.ir
Address: 217.218.25.215

C:\Users\Administrator>

```

```

Administrator: C:\Windows\system32\cmd.exe

C:\Users\Administrator>nslookup www.test.com
DNS request timed out.
    timeout was 2 seconds.
Server: Unknown
Address: ::1

Name:   www.test.com
Address: 192.168.20.1

C:\Users\Administrator>

```

شکل ۱۷-۱۳

اجرای nslookup بدون پارامتر: پس از اجرای دستور nslookup اعلان فرمان به > تغییر می‌یابد. در این قسمت هر نامی را که وارد می‌کنید به سرور DNS پیش فرض ارسال می‌شود و IP آن را درخواست می‌کند. در صورت پیدا کردن رکورد معادل آن، IP آن را نمایش می‌دهد (شکل ۱۸-۱۳).



شکل ۱۸-۱۳

خودآزمایی و پژوهش

- ۱- کاربرد سرویس DNS در شبکه را توضیح دهید.
- ۲- مفهوم هر یک از اجزای آدرس اینترنتی <http://www.tvoccd.sch.ir> را بنویسید.
- ۳- انواع Zone را نام برده و وظیفه هر یک را توضیح دهید.
- ۴- زمانی که سرویس دهنده Local IP با درخواست شده سرویس گیرنده را پیدا کرد به چه دلیل آن اسم و IP را در Cache کپی می‌کند؟
- ۵- DNS سرور به طور پیش فرض چند Root Name Server را شناسایی می‌کند و IP آن‌ها را چگونه می‌توان دید.
- ۶- فرمانی بنویسید که به وسیله آن بتوان Host, IP با نام <http://www.tvoccd.sch.ir> به دست آورد.