Managing DNS Update

The DNS Update protocol (RFC 2136) integrates DNS with DHCP. The latter two protocols are complementary; DHCP centralizes and automates IP address allocation, while DNS automatically records the association between assigned addresses and hostnames. When you use DHCP with DNS update, this configures a host automatically for network access whenever it attaches to the IP network. You can locate and reach the host using its unique DNS hostname. Mobile hosts, for example, can move freely without user or administrator intervention.

This chapter explains how to use DNS update with Cisco Prime IP Express servers, and its special relevance to Windows client systems.

DNS Update Process

To configure DNS updates, you must:

1. Create a DNS update configuration for a forward or reverse zone or both. See Creating DNS Update Configurations, on page 12.
2. Use this DNS update configuration in either of two ways:
    - Specify the DNS update configuration on a named, embedded, or default DHCP policy. See Creating and Applying DHCP Policies.

- Define a DNS update map to autoconfigure a single DNS update relationship between a Cisco Prime IP Express DHCP server or failover pair and a DNS server or High-Availability (HA) pair. Specify the update configuration in the DNS update map. See Creating DNS Update Maps, on page 18

3. Optionally define access control lists (ACLs) or transaction signatures (TSIGs) for the DNS update. See Configuring Access Control Lists and Transaction Security, on page 5.
4. Optionally create one or more DNS update policies based on these ACLs or TSIGs and apply them to the zones. See Configuring DNS Update Policies, on page 14.
5. Optionally configure the DNS update to transition from TXT RR to DHCID RR for DHCPv4. See Transitioning to DHCID RR for DHCPv4, on page 22.
6. Adjust the DNS update configuration for Windows clients, if necessary; for example, for dual zone updates. See Configuring DNS Update for Windows Clients, on page 23.
7. Configure DHCP clients to supply hostnames or request that Cisco Prime IP Express generate them.
8. Reload the DHCP and DNS servers, if necessary based on the edit mode.

Special DNS Update Considerations

Consider these two issues when configuring DNS updates:

- For security purposes, the Cisco Prime IP Express DNS update process does not modify or delete a name an administrator manually enters in the DNS database.
- If you enable DNS update for large deployments, and you are not using HA DNS (see the *"Deploying High Availability DNS Pair" chapter in Cisco Prime IP Express 9.0 Authoritative and Caching DNS User Guide*), divide primary DNS and DHCP servers across multiple clusters. DNS update generates an additional load on the servers.

DNS Updates for DHCPv6

Cisco Prime IP Express currently supports DHCPv6 DNS update over IPv4 and IPv6. For DHCPv6, DNS update applies to nontemporary stateful addresses and delegated prefixes.

DNS Updates for Non-Temporary Stateful Addresses

DNS Updates for DHCPv6 involves AAAA and PTR RR mappings for leases. Cisco Prime IP Express supports server- or extension-synthesizing fully qualified domain names and the DHCPv6 *client-fqdn* option (39).

Because Cisco Prime IP Express is compliant with RFCs 4701, 4703, and 4704, it supports the DHCID resource record (RR). All RFC-4703-compliant updaters can generate DHCID RRs and result in data that is a hash of the client identifier (DUID) and the FQDN (per RFC 4701). Nevertheless, you can use AAAA and DHCID RRs in update policy rules.

DNS update processing for DHCPv6 is similar to that for DHCPv4 except that a single FQDN can have more than one lease, resulting in multiple AAAA and PTR RRs for a single client. The multiple AAAA RRs can be under the same name or a different name; however, PTR RRs are always under a different name, based on the lease address. RFC-4703-compliant updaters use the DHCID RR to avoid collisions among multiple clients.

Note If the DNS server is down and the DHCP server can not complete the DNS updates to remove RRs added for a DHCPv6 lease, the lease continues to exist in the AVAILABLE state. Only the same client reuses the lease.

DNS Updates for Delegated Prefixes

DNS Updates for delegated prefixes can be enabled to update AAAA and/or PTR mappings for delegated prefix leases. However, this only updates DNS for the all 0's address for the delegated prefix. For example, if a prefix of 2001:db8:3333:3333::/64 is delegated, only the PTR and/or AAAA for 2001:db8:3333:3333::0 is updated in DNS. This feature does not provide a means for doing DNS delegations for delegated prefix.

Updates for delegated prefixes are only enabled if the DNS Update Configuration has the *prefix-delegation-updates* attribute enabled. This attribute is disabled by default. Updates for delegated prefixes most likely occur to different zones than the address updates, and therefore you may need to create new DNS update configurations and associate them with the corresponding prefixes.

Since the standard name generation rules apply, a client that includes an FQDN option with a hint can impact the resulting name (if the configuration allows this). Clients are never returned the name used for prefix delegation updates if they request the FQDN option.

Note If using this feature, you MUST assure that both the failover partners are running a version which supports this feature. Otherwise, updates will only be done when serviced by the server that has been upgraded. Therefore, do not enable this feature until both partners have been upgraded.

Related Topics

DHCPv6 Upgrade Considerations, on page 3

Generating Synthetic Names in DHCPv4 and DHCPv6, on page 4

Determining Reverse Zones for DNS Updates, on page 4

Using the Client FQDN, on page 5

DHCPv6 Upgrade Considerations

If you use any policy configured prior to Cisco Prime IP Express that references a DNS update object for DHCPv6 processing (see DHCPv6 Policy Hierarchy), after the upgrade, the server begins queuing DNS updates to the specified DNS server or servers. This means that DNS updates might automatically (and unexpectedly) start for DHCPv6 leases.

Caution If you use earlier versions of Cisco Prime IP Express or other DNS servers, you might experience interoperability issues for zone transfers and DNS updates, because of recent DHCID RR standards changes. You might need to upgrade DNS servers to support DHCPv6 DNS updates.

Generating Synthetic Names in DHCPv4 and DHCPv6

If clients do not supply hostnames, DHCPv4 and DHCPv6 includes a synthetic name generator. The *v6-synthetic-name-generator* attribute for the DNS update configuration allows appending a generated name to the *synthetic-name-stem* based on the:

- Hash of the client DHCP Unique Identifier (DUID) value (the preset value).
- Raw client DUID value (as a hex string with no separators).
- CableLabs *cablelabs-17* option *device-id* suboption value (as a hex string with no separators, or the hash of the client DUID if not found).
- CableLabs *cablelabs-17* option *cm-mac-address* suboption value (as a hex string with no separators, or the hash of the client DUID if not found).

Caution Some generation methods might cause privacy issues if the domain is accessible from the Internet.

The *v4-synthetic-name-generator* attribute for the DNS update configuration allows appending a generated name to the synthetic-name-stem based on the:

- **address**—Identifies the v4 address of client.
- **client-id**—Client-id or DUID given by DHCPv4 client in its request (Option 61).
- **hashed-client-id**—The hashed client-id which is a 13-character base 32 encoded string formed of the right part 64-bits of the SHA-256 hash appended with the forward zone name.

See Creating DNS Update Configurations, on page 12 for how to create a DNS update configuration with synthetic name generation.

In the CLI, an example of this setting is:

```
nrcmd> dhcp-dns-update example-update-config set v6-synthetic-name-generator=hashed-duid

nrcmd> dhcp-dns-update example-update-config set v4-synthetic-name-generator=client-id
```

Determining Reverse Zones for DNS Updates

The DNS update configuration uses the prefix length value in the specified *reverse-zone-prefix-length* attribute to generate a reverse zone in the ip6.arpa domain. You do not need to specify the full reverse zone, because you can synthesize it by using the ip6.arpa domain. You set this attribute for the reverse DNS update configuration (see Creating DNS Update Configurations, on page 12). Here are some rules for *reverse-zone-prefix-length*:

- Use a multiple of 4 for the value, because ip6.arpa zones are on 4-bit boundaries. If not a multiple of 4, the value is rounded up to the next multiple of 4.
- The maximum value is 124, because specifying 128 would create a zone name without any possible hostnames contained therein.
- A value of 0 means none of the bits are used for the zone name, hence ip6.arpa is used.
- If you omit the value from the DNS update configuration, the server uses the value from the prefix or, as a last resort, the prefix length derived from the *address* value of the prefix (see Configuring Prefixes and Links).

Note that to synthesize the reverse zone name, the *synthesize-reverse-zone* attribute must remain enabled for the DHCP server. Thus, the order in which a reverse zone name is synthesized for DHCPv6 is:

1. Use the full *reverse-zone-name* in the reverse DNS update configuration.
2. Base it on the ip6.arpa zone from the *reverse-zone-prefix-length* in the reverse DNS update configuration.
3. Base it on the ip6.arpa zone from the *reverse-zone-prefix-length* in the prefix definition.
4. Base it on the ip6.arpa zone from the prefix length for the *address* in the prefix definition.

In the CLI, an example of setting the reverse zone prefix length is:

```
nrcmd> dhcp-dns-update example-update-config set reverse-zone-prefix-length=32
```

To create a reverse zone for a prefix in the web UI, the List/Add Prefixes page includes a **Create Reverse Zone** button for each prefix. (See Creating and Editing Prefixes.)

The CLI also provides the **prefix** *name* **createReverseZone** [**–range**] command to create a reverse zone for a prefix (from its address or range value). Delete the reverse zone by using **prefix** *name* **deleteReverseZone** [**–range**].

You can also create a reverse zone from a DHCPv4 subnet or DHCPv6 prefix by entering the subnet or prefix value when directly configuring the reverse zone. See the *"Configuring Primary Reverse Zones" section in Cisco Prime IP Express 9.0 Authoritative and Caching DNS User Guide* for details.

Using the Client FQDN

The existing DHCP server *use-client-fqdn* attribute controls whether the server pays attention to the DHCPv6 client FQDN option in the request. The rules that the server uses to determine which name to return when multiple names exist for a client are in the following order of preference:

1. The server FQDN that uses the client requested FQDN if it is in use for any lease (even if not considered to be in DNS).
2. The FQDN with the longest valid lifetime considered to be in DNS.
3. The FQDN with the longest valid lifetime that is not yet considered to be in DNS.

Configuring Access Control Lists and Transaction Security

ACLs are authorization lists, while transaction signatures (TSIG) is an authentication mechanism:

- ACLs enable the server to allow or disallow the request or action defined in a packet.
- TSIG ensures that DNS messages come from a trusted source and are not tampered with.

For each DNS query, update, or zone transfer that is to be secured, you must set up an ACL to provide permission control. TSIG processing is performed only on messages that contain TSIG information. A message that does not contain, or is stripped of, this information bypasses the authentication process.

For a totally secure solution, messages should be authorized by the same authentication key. For example, if the DHCP server is configured to use TSIG for DNS updates and the same TSIG key is included in the ACL for the zones to be updated, then any packet that does not contain TSIG information fails the authorization step. This secures the update transactions and ensures that messages are both authenticated and authorized before making zone changes.

ACLs and TSIG play a role in setting up DNS update policies for the server or zones, as described in Configuring DNS Update Policies, on page 14.

Related Topics

Assigning ACLs on DNS Caching Servers or Zones , on page 6

Configuring Zones for ACLs, on page 7

Transaction Security, on page 7

Assigning ACLs on DNS Caching Servers or Zones

You assign ACLs on the DNS Caching server or zone level. ACLs can include one or more of these elements:

- **IP address**—In dotted decimal notation; for example, 192.168.1.2.
- **Network address**—In dotted decimal and slash notation; for example, 192.168.0.0/24. In this example, only hosts on that network can update the DNS server.
- **Another ACL**—Must be predefined. You cannot delete an ACL that is embedded in another one until you remove the embedded relationship. You should not delete an ACL until all references to that ACL are deleted.
- **Transaction Signature (TSIG) key**—The value must be in the form **key** *value*, with the keyword **key** followed by the secret value. To accommodate space characters, the entire list must be enclosed in double quotes. For TSIG keys, see Transaction Security, on page 7.

You assign each ACL a unique name. However, the following ACL names have special meanings and you cannot use them for regular ACL names:

- **any**—Anyone can perform a certain action
- **none**—No one can perform a certain action
- **localhost**—Any of the local host addresses can perform a certain action
- **localnets**—Any of the local networks can perform a certain action

Note the following:

- If an ACL is not configured, **any** is assumed.
- If an ACL is configured, at least one clause must allow traffic.
- The negation operator (**!**) disallows traffic for the object it precedes, but it does not intrinsically allow anything else unless you also explicitly specify it. For example, to disallow traffic for the IP address 192.168.50.0 only, use **!192.168.50.0, any**.

Local Advanced Web UI

From the **Design** menu, choose **ACLs** under the **Security** submenu to open the List/Add Access Control Lists page. Click the **Add ACLs** icon in the ACLs pane and enter an ACL name and match list and click Add ACL. Note that a **key** *value* pair should not be in quotes. At the regional level, you can additionally pull replica ACLs or push ACLs to local clusters.

CLI Commands

Use **acl** *name* **create** *match-list*, which takes a name and one or more ACL elements. The ACL list is comma-separated, with double quotes surrounding it if there is a space character. The CLI does not provide the pull/push function.

For example, the following commands create three ACLs. The first is a key with a value, the second is for a network, and the third points to the first ACL. Including an exclamation point (**!**) before a value negates that value, so that you can exclude it in a series of values:

```
nrcmd> acl sec-acl create "key h-a.h-b.example.com."

nrcmd> acl dyn-update-acl create "!192.168.2.13,192.168.2.0/24"

nrcmd> acl main-acl create sec-acl
```

Configuring Zones for ACLs

To configure ACLs for the DNS server or zones, set up a DNS update policy, then define this update policy for the zone (see Configuring DNS Update Policies, on page 14).

Transaction Security

Transaction Signature (TSIG) RRs enable the DNS server to authenticate each message that it receives, containing a TSIG. Communication between servers is not encrypted but it becomes authenticated, which allows validation of the authenticity of the data and the source of the packet.

When you configure the Cisco Prime IP Express DHCP server to use TSIG for DNS updates, the server appends a TSIG RR to the messages. Part of the TSIG record is a message authentication code.

When the DNS server receives a message, it looks for the TSIG record. If it finds one, it first verifies that the key name in it is one of the keys it recognizes. It then verifies that the time stamp in the update is reasonable (to help fight against traffic replay attacks). Finally, the server looks up the key shared secret that was sent in the packet and calculates its own authentication code. If the resulting calculated authentication code matches the one included in the packet, then the contents are considered to be authentic.

Related Topics

Creating TSIG Keys, on page 7

Generating Keys, on page 8

Considerations for Managing Keys, on page 9

Adding Supporting TSIG Attributes, on page 9

Creating TSIG Keys

Note If you want to enable key authentication for Address-to-User Lookup (ATUL) support, you must also define a key identifier (*id* attribute value). See Setting DHCP Forwarding.

Local Advanced Web UI

From the **Design** menu, choose **Keys** under the **Security** submenu to open the List/Add Encryption Keys page.

For a description of the Algorithm, Security Type, Time Skew, Key ID, and Secret values, see Table 1: Options for the cnr_keygen Utility . See also Considerations for Managing Keys, on page 9.

To edit a TSIG key, click its name on the List/Add Encryption Keys page to open the Edit Encryption Key page.

At the regional level, you can additionally pull replica keys, or push keys to local clusters.

CLI Commands

Use **key** *name* **create** *secret*. Provide a name for the key (in domain name format; for example, hosta-hostb-example.com.) and a minimum of the shared secret as a base-64 encoded string (see Table 1: Options for the cnr_keygen Utility for a description of the optional time skew attribute). An example in the CLI would be:

```
nrcmd> key hosta-hostb-example.com.create secret-string
```

Generating Keys

It is recommended that you use the Cisco Prime IP Express **cnr_keygen** utility to generate TSIG keys so that you add them or import them using **import keys**.

Execute the **cnr_keygen** key generator utility from a DOS prompt, or a Linux shell:

- On Windows, the utility is in the *install-path* \bin folder.
- On Linux, the utility is in the *install-path* /usrbin directory.

An example of its usage (on Linux) is:

```
> /opt/nwreg2/local/usrbin/cnr_keygen -n a.b.example.com. -a hmac-md5 -t TSIG -b 16
-s 300

key "a.b.example.com." {
algorithm hmac-md5;
secret "xGVCsFZ0/6e0N97HGF50eg==";
# cnr-time-skew 300;
# cnr-security-type TSIG;
};
```

The only required input is the key name. The options are described in the table below.

Table 1: Options for the cnr_keygen Utility

Option	Description
–a hmac-md5	Algorithm. Optional. Only hmac-md5 is currently supported.
–b *secret-size*	Byte size of the secret. Optional. The preset value is 16 bytes. The valid range is 1 through 64 bytes.
–s *time-skew*	Time skew for the key, in seconds. This is the maximum difference between the time stamp in packets signed with this key and the local system time. Optional. The preset value is 5 minutes. The range is one second through one hour.
–n *name*	Key name. Required. The maximum length is 255 bytes.
–t TSIG	Type of security used. Optional. Only TSIG is currently supported.
–h	Help. Optional. Displays the syntax and options of the utility.

Option	Description
–v	Version. Optional. Displays the version of the utility.

The resulting secret is base64-encoded as a random string.

You can also redirect the output to a file if you use the right-arrow (>) or double-right-arrow (>>) indicators at the end of the command line. The > writes or overwrites a given file, while the >> appends to an existing file. For example:

```
> /opt/nwreg2/local/usrbin/cnr_keygen -n example.com > keyfile.txt
```

```
> /opt/nwreg2/local/usrbin/cnr_keygen -n example.com >> addtokeyfile.txt
```

You can then import the key file into Cisco Prime IP Express using the CLI to generate the keys in the file. The key import can generate as many keys as it finds in the import file. The path to the file should be fully qualified. For example:

```
nrcmd> import keys keydir/keyfile.txt
```

Considerations for Managing Keys

If you generate your own keys, you must enter them as a base64-encoded string (See RFC 4648 for more information on base64 encoding). This means that the only characters allowed are those in the base64 alphabet and the equals sign (=) as pad character. Entering a nonbase64-encoded string results in an error message.

Here are some other suggestions:

- Do not add or modify keys using batch commands.
- Change shared secrets frequently; every two months is recommended. Note that Cisco Prime IP Express does not explicitly enforce this.
- The shared secret length should be at least as long as the keyed message digest (HMAC-MD5 is 16 bytes). Note that Cisco Prime IP Express does not explicitly enforce this and only checks that the shared secret is a valid base64-encoded string, but it is the policy recommended by RFC 2845.

Adding Supporting TSIG Attributes

To add TSIG support for a DNS update configuration (see Creating DNS Update Configurations, on page 12), set these attributes:

- *server-key*
- *backup-server-key*

To use GSS-TSIG security algorithm in TSIG, enable the below attribute:

- *use-gss-tsig*

GSS-TSIG

RFC 3645 proposed extending TSIG to allow the Generic Security Service (GSS) method of secure key exchange, eliminating the need for manually distributing keys to all GSS clients. It defines an algorithm to use with TSIG, which is based on the Generic Security Service Application Program Interface(GSS API), as specified in RFC2743.

GSS-TSIG provides the secure DDNS updates and secure Zone Transfers utilizing the Kerberos security mechanism.

Client and Server use GSS API calls to establish a limited lifetime security context for authentication, integrity and confidentiality. Establishing a security context involves the passing of opaque tokens between the client and server until the negotiation is complete. The TKEY resource record [RFC2930] is used as the vehicle to transfer tokens between client and server. Once the security context is established it is used to generate and verify signatures using GSS API calls. These signatures are exchanged by the Client and Server as a part of the TSIG records exchanged in DNS messages sent between the Client and Server, as described in [RFC2845].

Client and Server MUST be locally authenticated with Kerberos server before using this protocol. Generally the initial TGT(ticket to get ticket) ticket is available in cache through system logon or obtained using utility like kinit. DHCP/DNS Client will request Kerberos server for the service ticket using the principal name(DNS/<hostname>). Client provides the service ticket to prove authentication when interacting, securely, with DNS server. The service ticket will be encrypted by the Kerberos server using service key, which can be decrypted only by the application server using the same service key.

For more information, see the Configuring GSS-TSIG, on page 35 for the configuration required on the DHCP Server and DNS Server.

Note By default, Cisco Prime IP Express will support HMAC-MD5 based secure TSIG updates. To enable the GSS based secure updates, user has to disable-all HMAC-MD5 configuration in the DNS server by selecting none option in tsig-processing attribute.

DHCP Server and Secondary DNS Server Configuration in Linux

Configure the KDC Server information in /etc/krb5.conf. Use kinit utility to get the initial ticket from KDC.

DHCP Server and Secondary DNS Server Configuration in Windows

The server machine should be under the AD domain and not workgroup.

Note To enable GSS-TSIG in DHCP server/Secondary DNS server, ensure that use-gss-tsig(Boolean) attribute is configured in DNS Update Config/Secondary Zone page respectively.

Troubleshooting DHCP Server and Secondary DNS Server Configuration

- Client-related errors that can occur while getting the initial credentials:
- CLOCK SKEW ERROR - Ensure the Kerberos client and server and synchronized in time if not synchronize with ntp.
- KDC not reachable - Ensure AD hostname is resolvable.
- kinit - Client not found in Kerberos database while getting initial credentials - Verify whether the user exists in AD.
- kinit - Cannot resolve servers for KDC in realm "DOMAIN.com" while getting the initial credentials - Verify whether the REALM exists in AD.

- kinit - Preauthentication failed while getting the initial credentials - Verify whether the password entered to get the ticket is same as the password associated to the user in AD.

Note Generally the initial TGT (ticket to get ticket) ticket is available in cache through system logon in Windows.

Creating GSS-TSIG Configuration

DNS/DHCP maintains non-persistent table for key management.

Note You have the option to change the default TKEY management values used by DHCP and DNS server. You must create a GSS- TSIG configuration and provide reference in the DHCP/DNS server page.

Local Basic or Advanced Web UI

From the **Design** menu, choose **GSS-TSIG** under the **Security** submenu to open the List/Add GSS-TSIG Configuration page.

GSS-TSIG attributes

- *tkey-max-exchanges* - Per recommendation from RFC 3645 to prevent endless looping, the DNS server shall impose a maximum number of TKEY exchanges (i.e. number TKEY queries received from a particular client) in the attempt to negotiate a particular key. This attribute shall specify this limit. A TKEY table record maintains the exchange-count. If exchange-count exceeds tkey-max-exchanges during key negotiation, the DNS server shall abort the key negotiation.
- *tkey-table-max-size* - This attribute bounds the size of the TKEY table.
- *tkey-table-purge-interval* - The time interval at which purging of expired keys from TKEY table should happen.
- *tkey-session-time* - Specifies the user configurable maximum lifetime of a key. Lifetime of a key is controlled by the Kerberos server expiry time obtained during the initial key negotiation and through this attribute. If set to 0, this attribute is disabled and the key lifetime is controlled only by the Kerberos given expiry time. When this attribute is configured with a value > 0, the minimum of Kerberos expiry time and this value is taken as the maximum lifetime of the key.

To edit a GSS-TSIG configuration, click its name on the List/Add GSS-TSIG Configuration page to open the Edit GSS-TSIG Configuration page.

At the regional level, you can additionally pull or push GSS-TSIG configuration to local clusters.

CLI Commands

Use **gss-tsig** *name* **create** [*attribute=value ...*]. Provide a name for the GSS-TSIG configuration object. For example:

```
nrcmd> gss-tsig gss create tkey-max-exchanges=6 tkey-table-max-size=500
tkey-table-purge-interval=90
```

Creating DNS Update Configurations

A DNS update configuration defines the DHCP server framework for DNS updates to a DNS server or HA DNS server pair. It determines if you want to generate forward or reverse zone DNS updates (or both). It optionally sets TSIG keys for the transaction, attributes to control the style of autogenerated hostnames, and the specific forward or reverse zone to be updated. You must specify a DNS update configuration for each unique server relationship.

For example, if all updates from the DHCP server are directed to a single DNS server, you can create a single DNS update configuration that is set on the server default policy. To assign each group of clients in a client-class to a corresponding forward zone, set the forward zone name for each in a more specific client-class policy.

Local Advanced and Regional Web UI

Step 1 From the **Deploy** menu, choose **DNS Update Configs** under the **DNS Updates** submenu to open the List/Add DNS Update Configurations page.

Step 2 Click the **Add DNS Update Configs** icon in the **DNS Update Configs** pane to open the **Add DnsUpdateConfig** dialog box.

Step 3 Enter a name for the update configuration in the *Name* attribute field.

Step 4 Click **Add DnsUpdateConfig** to add the DNS update configuration.

Step 5 Select the name of update configuration to open the Edit DNS Update Configuration page.

Step 6 Click the appropriate *dynamic-dns* setting under the Update Settings block:

- **update-none**—Do not update forward or reverse zones.
- **update-all**—Update forward and reverse zones (the default value).
- **update-fwd-only**—Update forward zones only.
- **update-reverse-only**—Update reverse zones only.

Step 7 Click the appropriate *dns-client-identity* setting under the Update Settings block:

- **txt**—The server uses TXT RR for DHCPv4 DNS updates and DHCID RR for DHCPv6 DNS updates.
- **dhcid**—The server uses DHCID RR for both DHCPv4 and DHCPv6 DNS updates.
- **transition-to-dhcid**—The server uses DHCID RR for new records in the DNS server and updates existing entries to use the DHCID RR when the next DNS update is done.
- **regress-to-txt**—The server uses the TXT RR for new entries in the DNS server and upgrades existing entries to use the TXT RR when the next DNS update is done.

Note The *dns-client-identity* attribute is also available as part of the DHCP server-wide settings which will be taken into consideration if the attribute of the individual DNS update config was not configured.

Step 8 Set the other attributes appropriately:

- If necessary, enable *synthesize-name* and set the *synthetic-name-stem* value.

  You can set the stem of the default hostname to use if clients do not supply hostnames, by using *synthetic-name-stem*. For DHCPv4, enable the *synthesize-name* attribute to trigger the DHCP server to synthesize unique names for clients based on the value of the *synthetic-name-stem*. The resulting name is the name stem appended with the

hyphenated IP address. For example, if you specify a *synthetic-name-stem* of **host** for address 192.168.50.1 in the example.com domain, and enable the *synthesize-name* attribute, the resulting hostname is host-192-168-50-1.example.com. The preset value for the synthetic name stem is **dhcp**

The *synthetic-name-stem* must:

- Be a relative name without a trailing dot.
- Include alphanumeric values and hyphens (–) only. Space characters and underscores become hyphens and other characters are removed.
- Include no leading or trailing hyphen characters.
- Have DNS hostnames of no more than 63 characters per label and 255 characters in their entirety. The algorithm uses the configured forward zone name to determine the number of available characters for the hostname, and truncates the end of the last label if necessary.

For DHCPv6, see Generating Synthetic Names in DHCPv4 and DHCPv6, on page 4.

- Set *forward-zone-name* to the forward zone, if updating forward zones. Note that the policy *forward-zone-name* takes precedence over the one set in the DNS update configuration.

  For DHCPv6, the server ignores the client and client-class policies when searching for a *forward-zone-name* value in the policy hierarchy. The search for a forward zone name begins with the prefix embedded policy.

- For DHCPv4, set *reverse-zone-name* to the reverse (in.addr.arpa) zone to be updated with PTR and TXT records. If unset and the DHCP server *synthesize-reverse-zone* attribute is enabled, the server synthesizes a reverse zone name based on the address of each lease, scope subnet number, and DNS update configuration (or scope) *dns-host-bytes* attribute value.

  The *dns-host-bytes* value controls the split between the host and zone parts of the reverse zone name. The value sets the number of bytes from the lease IP address to use for the hostname; the remaining bytes are used for the in-addr.arpa zone name. A value of 1 means use just one byte for the host part of the domain and the other three from the domain name (reversed). A value of 4 means use all four bytes for the host part of the address, thus using just the in-addr.arpa part of the domain. If unset, the server synthesizes an appropriate value based on the scope subnet size, or if the *reverse-zone-name* is defined, calculates the host bytes from this name.

  The one-a-rr-per-dns-name controls the DHCPv4 DNS updates to allow either one or multiple A RRs per name. The introduction of the DUID support and DHCID RR, multi-connection clients will have multiple A RRs.

  For DHCPv6, see Determining Reverse Zones for DNS Updates, on page 4.

- Set *server-addr/server-ipv6addr* to the IPv4/IPv6 address of the primary DNS server for the forward zone (or reverse zone if updating reverse zones only.

Set *server-key* and *backup-server-key* if you are using a TSIG key to process all DNS updates (see Transaction Security, on page 7).

Set *use-gss-tsig* to true, if you are using the Generic Security Service (GSS) method of the secure key exchange (see Configuring GSS-TSIG

- Set *backup-server-addr/backup-server-ipv6addr* to the IPv4/IPv6 address of the backup DNS server, if HA DNS is configured.
- If necessary, enable or disable *update-dns-first* (preset value disabled) or *update-dns-for-bootp* (preset value enabled). The *update-dns-first* setting controls whether DHCP updates DNS before granting a lease. Enabling this attribute is not recommended.

Step 9 At the regional level, you can also push update configurations to the local clusters, or pull them from the replica database on the List/Add DNS Update Configurations page.

Step 10 Click **Save**.

Step 11 To specify this DNS update configuration on a policy, see Creating and Applying DHCP Policies.

CLI Commands

Use **dhcp-dns-update** *name* **create** [*attribute=value* ...]. For example:

```
dhcp-dns-update example-update-config create
```

Set the *dynamic-dns* attribute to its appropriate value (update-none, update-all, update-fwd-only, or update-reverse-only). For example:

```
nrcmd> dhcp-dns-update example-update-config set dynamic-dns=update-all
```

Related Topics

DNS Update Process, on page 1
Special DNS Update Considerations, on page 2
DNS Updates for DHCPv6, on page 2

Configuring DNS Update Policies

DNS update policies provide a mechanism for managing update authorization at the RR level. Using update policies, you can grant or deny DNS updates based on rules that are based on ACLs as well as RR names and types. ACLs are described in Assigning ACLs on DNS Caching Servers or Zones , on page 6.

Related Topics

Compatibility with Cisco IP Express Releases, on page 14
Creating and Editing Update Policies, on page 15
Defining and Applying Rules for Update Policies, on page 15

Compatibility with Cisco IP Express Releases

Cisco Prime IP Express releases used static RRs that administrators entered, but that DNS updates could not modify. This distinction between static and dynamic RRs no longer exists. RRs can now be marked as protected or unprotected (see the *"Protecting Resource Record Sets" section in Cisco Prime IP Express 9.0 Authoritative and Caching DNS User Guide*). Administrators creating or modifying RRs can now specify whether RRs should be protected. A DNS update cannot modify a protected RR set, even if an RR of the given type does not yet exist in the set.

Note Previous releases allowed DNS updates only to A, TXT, PTR, CNAME and SRV records. This was changed to allow updates to all but SOA and NS records in unprotected name sets. To remain compatible with a previous release, use an update policy to limit RR updates.

Creating and Editing Update Policies

Creating an update policy initially involves creating a name for it.

Local Advanced Web UI

Step 1 From the **Design** menu, choose **Update Policies** under the **Security** submenu to open the List/Add DNS Update Policies page. The option is available if the server is configured with authoritative service.

Step 2 Click the **Add Update Policies** icon in the Update Policies pane to open the **Add DNS Update Policy** dialog box.

Step 3 Enter a name for the update policy.

Step 4 Click **Add DNS Update Policy**.

Step 5 Proceed to Defining and Applying Rules for Update Policies, on page 15.

CLI Commands

Use **update-policy** *name* **create**. For example:

```
nrcmd> update-policy policy1 create
```

Defining and Applying Rules for Update Policies

DNS update policies are effective only if you define rules for each that grant or deny updates for certain RRs based on an ACL. If no rule is satisfied, the default (last implicit) rule is to deny all updates (**"deny any wildcard * *"**).

Related Topics

Defining Rules for Named Update Policies, on page 15

Applying Update Policies to Zones, on page 18

Defining Rules for Named Update Policies

Defining rules for named update policies involves a series of Grant and Deny statements.

Local Advanced Web UI

Step 1 Create an update policy, as described in Creating and Editing Update Policies, on page 15, or edit it.

Step 2 On the List/Add DNS Update Policies or Edit DNS Update Policy page:

a) Enter an optional value in the Index field.
b) Click Grant to grant the rule, or Deny to deny the rule.
c) Enter an access control list in the ACL List field.
d) Choose a keyword from the Keyword drop-down list.
e) Enter a value based on the keyword in the Value field. This can be a RR or subdomain name, or, if the **wildcard** keyword is used, it can contain wildcards (see the table below).

As networks make the transition from the IPv4 to IPv6 addressing, a lot of network devices will use both IPv4 and IPv6 addresses. These devices may be using multiple interfaces on the same host, using different networks, or using different DHCP versions. These devices need to be identified consistently with respect to DHCP server and accordingly the DHCP server will update the DNS server.

In Cisco Prime IP Express 8.2 and later, DHCPv4 uses TXT RRs and DHCPv6 uses DHCID RRs to make the DNS updates. To avoid conflicts in the client-requested names the dual-stack clients cannot use a single forward FQDN. These conflicts are primarily applied to the client-requested names and not to the generated names, which are generally unique. To avoid these conflicts, different zones were used for the DHCPv4 and DHCPv6 names.

In Cisco Prime IP Express 8.2 and later, DHCPv4 uses TXT RR or DHCID RR and DHCPv6 uses DHCID RR for DNS updates. The default value of DHCP server-wide settings attribute dns-client-identity is txt and the attribute is not configured for individual DNS update config objects. You can configure the DNS updates in one of the following ways:

- TXT RR for DHCPv4 and DHCID for DHCPv6—To enable this configuration set the dns-client-identity to txt. The server will use the TXT RR in DHCPv4 DNS updates and DHCID RR for DHCPv6 DNS updates.
- DHCID RR for both DHCPv4 and DHCPv6—To enable this configuration set the dns-client-identity to dhcid. The server will use the DHCID RR for both DHCPv4 and DHCPv6 DNS updates. This setting should be used to support dual stack clients and can only be used if all DHCP servers doing DNS updates to the zones for this configuration support and are configured to use the DHCID RR.
- Transition to DHCID RR—To enable this configuration set the dns-client-identity to transition-to-dhcid. Set the force-dns-update attribute to true. Reload the server. For the zones that need to be upgraded, set the dns-client-identity attribute to dhcid and restore the force-dns-update attribute to its earlier value, after the longest lease time configured in the server.

Note You must set the transition-to-dhcid attribute until all the DHCPv4 resource records are updated to DHCID RR. For more information, see Transitioning to DHCID RR for DHCPv4, on page 22.

- Regress to TXT RR—To enable this configuration set the dns-client-identity to regress-to-txt. Set the force-dns-update attribute to true. Reload the server. For the zones that need to be upgraded, set the dns-client-identity attribute to txt and restore the force-dns-update attribute to its earlier value, after the longest lease time configured in the server.

Note The CCM server will not allow the failover synchronization if one of the failover servers runs on Cisco Prime IP Express 8.1 or earlier and the dns-client-identity attribute, in the DHCP server or a DNS Update Configuration, is set to anything other than txt.

Table 2: Wildcard Values for Update Policy Rules

Wildcard	Description
*	Matches zero or more characters. For example, the pattern **example*** matches all strings starting with *example*, including **example–**.
?	Matches a single character only. For example, the pattern **example?.com** matches **example1.com** and **example2.com**, but not **example.com**.
/[/]	Matches any characters in the (escaped) brackets; for example, **/[abc/]**. Each square bracket must be escaped using a slash (/). The characters can also be in a range; for example, **/[0–9/]** and **/[a–z/]**. If a pattern should include a hyphen, make the hyphen the first character; for example, **example/[–a–z/]**.

f) Enter one or more RR types, separated by commas, in the RR Types field, or use ***** for "all RRs." You can use negated values, which are values prefixed by an exclamation point; for example, **!PTR**.

g) Click **Save**.

Step 3 At the regional level, you can also push update policies to the local clusters, or pull them from the replica database on the List/Add DNS Update Policies page.

Step 4 To edit an update policy, click the name of the update policy on the List/Add DNS Update Policies page to open the Edit DNS Update Policy page, make changes to the fields, then click **Save**.

CLI Commands

Create or edit an update policy (see Creating and Editing Update Policies, on page 15, then use **update-policy** *name* **rules add** *rule*, with *rule* being the rule. (See the table above for the rule wildcard values.) For example:

```
nrcmd> update-policy policy1 rules add "grant 192.168.50.101 name host1 A,TXT" 0
```

The rule is enclosed in quotes. To parse the rule syntax for the example:

- **grant**—Action that the server should take, either **grant** or **deny**.
- **192.168.50.101**—The ACL, in this case an IP address. The ACL can be one of the following:
  - Name—ACL created by name, as described in Assigning ACLs on DNS Caching Servers or Zones , on page 6.
  - IP address, as in the example.
  - Network address, including mask; for example, **192.168.50.0/24**.
  - TSIG key—Transaction signature key, in the form **key=***key*, (as described in Transaction Security, on page 7.
  - One of the reserved words:

    any—Any ACL

    none—No ACL

    localhost—Any local host addresses

    localnets—Any local network address

You can negate the ACL value by preceding it with an exclamation point (**!**).

- **name**—Keyword, or type of check to perform on the RR, which can be one of the following:
  - **name**—Name of the RR, requiring a name value.
  - **subdomain**—Name of the RR or the subdomain with any of its RRs, requiring a name or subdomain value.
  - **wildcard**—Name of the RR, using a wildcard value (see the table above).
- **host1**—Value based on the keyword, in this case the RR named host1. This can also be a subdomain name or, if the **wildcard** keyword is used, can contain wildcards (see the table above).
- **A,TXT**—RR types, each separated by a comma. This can be a list of any of the RR types described in the *"Resource Records" section in Cisco Prime IP Express 9.0 Authoritative and Caching DNS User Guide* You can negate each record type value by preceding it with an exclamation point (**!**).
- Note that if this or any assigned rule is not satisfied, the default is to deny all RR updates.

Tacked onto the end of the rule, outside the quotes, is an index number, in the example, **0**. The index numbers start at 0. If there are multiple rules for an update policy, the index serves to add the rule in a specific order, such that lower numbered indexes have priority in the list. If a rule does not include an index, it is placed at

the end of the list. Thus, a rule always has an index, whether or not it is explicitly defined. You also specify the index number in case you need to remove the rule.

To replace a rule, use **update-policy** *name* **delete**, then recreate the update policy. To edit a rule, use **update-policy** *name* **rules remove** *index*, where *index* is the explicitly defined or system-defined index number (remembering that the index numbering starts at 0), then recreate the rule. To remove the second rule in the previous example, enter:

```
nrcmd> update-policy policy1 rules remove 1
```

Applying Update Policies to Zones

After creating an update policy, you can apply it to a zone (forward and reverse) or zone template if you have configured the DNS server with authoritative services.

Local Advanced Web UI

Step 1 From the **Design** menu, choose **Forward Zones** under the **Auth DNS** submenu to open the List/Add Forward Zones page.

Step 2 Click the name of the of zone to open the Edit Zone page.

Tip You can also perform this function for zone templates on the Edit Zone Template page, and primary reverse zones on the Edit Primary Reverse Zone page (see the *"Managing Zones" chapter in Cisco Prime IP Express 9.0 Authoritative and Caching DNS User Guide*).

Step 3 Enter the name or (comma-separated) names of one or more of the existing named update policies in the *update-policy-list* attribute field.

Note The server processes the update-acl before it processes the *update-policy-list*.

Step 4 Click **Save.**

CLI Commands

Use **zone** *name* **set update-policy-list**, equating the *update-policy-list* attribute with a quoted list of comma-separated update policies, as defined in Creating and Editing Update Policies, on page 15. For example:

```
nrcmd> zone example.com set update-policy-list="policy1,policy2"
```

Creating DNS Update Maps

A DNS update map facilitates configuring DNS updates so that the update properties are synchronized between HA DNS server pairs or DHCP failover server pairs, based on an update configuration, so as to reduce redundant data entry. The update map applies to all the primary zones that the DNS pairs service, or all the scopes that the DHCP pairs service. You must specify a policy for the update map. To use this function, you must be an administrator assigned the server-management subrole of the dns-management or central-dns-management role, and the dhcp-management role (for update configurations).

Local and Regional Web UI

Step 1 From the **Deploy** menu, choose **Update Maps** under the **DNS Updates** submenu to open the List/Add DNS Update Maps page. The option is available if the server is configured with authoritative service.

Step 2 Click the **Add DNS Update Map** icon in the Update Maps pane to open the Add DNS Update Map dialog box.

Step 3 Enter a name for the update map in the Name field.

Step 4 Choose the The DNS server or HA pair associated with this configuration.

Step 5 Choose the DHCP server or DHCP failover pair associated with this configuration.

Step 6 Enter the DNS update configuration from the previous section in the *dns-config* field.

Step 7 Set the kind of policy selection you want for the *dhcp-policy-selector* attribute. The choices are:

- **use-named-policy**—Use the named policy set for the *dhcp-named-policy* attribute (the preset value).
- **use-client-class-embedded-policy**—Use the embedded policy from the client-class set for the *dhcp-client-class* attribute.
- **use-scope-embedded-policy**—Use the embedded policy from the scope.

Step 8 If using update ACLs (see Configuring Access Control Lists and Transaction Security, on page 5) or DNS update policies (see Configuring DNS Update Policies, on page 14), set either the *dns-update-acl* or *dns-update-policy-list* attribute. Either value can be one or more addresses separated by commas. The *dns-update-acl* takes precedence over the *dns-update-policy-list*.

If you omit both values, a simple update ACL is constructed whereby only the specified DHCP servers or failover pair can perform updates, along with any *server-key* value set in the update configuration specified for the *dns-config* attribute.

Step 9 Click **Add DNS Update Map**.

Step 10 At the regional level, you can also push update maps to the local clusters, or pull them from the replica database on the List/Add DNS Update Maps page.

CLI Commands

Specify the name, cluster of the DHCP and DNS servers (or DHCP failover or HA DNS server pair), and the DNS update configuration when you create the update map, using **dns-update-map** *name* **create** *dhcp-cluster dns-cluster dns-config*. For example:

```
nrcmd> dns-update-map example-update-map create Example-cluster Boston-cluster
example-update-config
```

Set the *dhcp-policy-selector* attribute value to use-named-policy, use-client-class-embedded-policy, or use-scope-embedded-policy. If using the use-named-policy value, also set the *dhcp-named-policy* attribute value. For example:

```
nrcmd> dns-update-map example-update-map set dhcp-policy-selector=use-named-policy

nrcmd> dns-update-map example-update-map set dhcp-named-policy=example-policy
```

Confirming Dynamic Records

The Cisco Prime IP Express DHCP server stores all pending DNS update data on disk. If the DHCP server cannot communicate with a DNS server, it periodically tests for re-established communication and submits all pending updates. This test typically occurs every 40 seconds.

Local Advanced Web UI

From the **Design** menu, choose **Forward Zones** under the **Auth DNS** submenu. Click the **Resource Records** tab to open the Edit Zone page.

CLI Commands

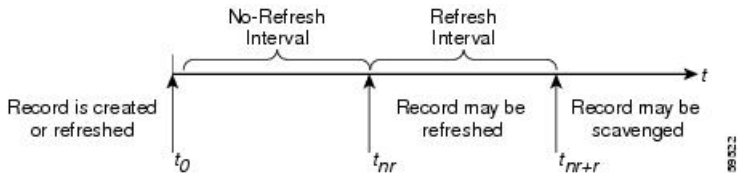
Use **zone** *name* **listRR dns**.

Scavenging Dynamic Records

Microsoft Windows DNS clients that get DHCP leases can update (refresh) their Address (A) records directly with the DNS server. Because many of these clients are mobile laptops that are not permanently connected, some A records may become obsolete over time. The Windows DNS server scavenges and purges these primary zone records periodically. Cisco Prime IP Express provides a similar feature that you can use to periodically purge stale records.

Scavenging is normally disabled by default, but you should enable it for zones that exclusively contain Windows clients. Zones are configured with *no-refresh* and *refresh* intervals. A record expires once it ages past its initial creation date plus these two intervals. The image below shows the intervals in the scavenging time line.

Figure 1: Address Record Scavenging Time Line Intervals



The Cisco Prime IP Express process is:

1. When the client updates the DNS server with a new A record, this record gets a timestamp, or if the client refreshes its A record, this may update the timestamp ("Record is created or refreshed").
2. During a no-refresh interval (a default value of seven days), if the client keeps sending the same record without an address change, this does not update the record timestamp.
3. Once the record ages past the no-refresh interval, it enters the refresh interval (also a default value of seven days), during which time DNS updates refresh the timestamp and put the record back into the no-refresh interval.
4. A record that ages past the refresh interval is available for scavenging when it reaches the scavenge interval.

Note Only unprotected RRs are scavenged. To keep RRs from being scavenged, set them to protected. However, top-of-zone (@) RRs, even if unprotected, are not scavenged.

The following DNS server attributes affect scavenging:

- ***scvg-interval***—Period during which the DNS server checks for stale records in a zone. The value can range from one hour to 365 days. You can also set this for the server (the default value is one week), although the zone setting overrides it.
- ***scvg-no-refresh-interval***—Interval during which actions, such as dynamic or prerequisite-only DNS updates, do not update the record timestamp. The value can range from one hour to 365 days. The zone setting overrides the server setting (the default value is one week).
- ***scvg-refresh-interval***—Interval during which DNS updates increment the record timestamp. After both the no-refresh and refresh intervals expire, the record is a candidate for scavenging. The value can range from one hour to 365 days. The zone setting overrides the server setting (the default value is one week).
- ***scvg-ignore-restart-interval***—Ensures that the server does not reset the scavenging time with every server restart. Within this interval, Cisco Prime IP Express ignores the duration between a server down instance and a restart, which is usually fairly short.

  The value can range from two hours to one day. With any value longer than that set, Cisco Prime IP Express recalculates the scavenging period to allow for record updates that cannot take place while the server is stopped. The zone setting overrides the server setting (the default value is 2 hours.

Enable scavenging only for zones where a Cisco Prime IP Express DNS server receives updates exclusively from Windows clients (or those known to do automatic periodic DNS updates). Set the attributes listed above. The Cisco Prime IP Express scavenging manager starts at server startup. It reports records purged through scavenging to the changeset database. Cisco Prime IP Express also notifies secondary zones by way of zone transfers of any records scavenged from the primary zone. In cases where you create a zone that has scavenging disabled (the records do not have a timestamp) and then subsequently enable it, Cisco Prime IP Express uses a proxy timestamp as a default timestamp for each record.

You can monitor scavenging activity using one or more of the log settings scavenge, scavenge-details, ddns-refreshes, and ddns-refreshes-details.

Local Advanced Web UI

On the Manage DNS Server page, click the **Commands** button to open the DNS Commands dialog box. Click the **Run** icon next to Scavenge all zones.

To scavenge a particular forward or reverse zone only, go to the Zone Commands for Zone page, which is available by clicking the **Commands** button on the List/Add Forward Zones page or List/Add Reverse Zones page. Click the **Run** icon next to Scavenge zone on the Zone Commands for Zone page. To find out the next time scavenging is scheduled for the zone, click the **Run** icon next to Get scavenge start time.

CLI Commands

Use **dns scavenge** for all zones that have scavenging enabled. Use the **getScavengeStartTime** action on a zone to find out the next time scavenging is scheduled to start.

Transitioning to DHCID RR for DHCPv4

As networks make the transition from the IPv4 to IPv6 addressing, a lot of network devices will use both IPv4 and IPv6 addresses. These devices may be using multiple interfaces on the same host, using different networks, or using different DHCP versions. These devices need to be identified consistently with respect to DHCP server and accordingly the DHCP server will update the DNS server.

In Cisco Prime IP Express 8.2 and later, DHCPv4 uses TXT RR or DHCID RR and DHCPv6 uses DHCID RR for DNS updates. The default value of DHCP server-wide settings attribute dns-client-identity is txt and the attribute is not configured for individual DNS update config objects. You can configure the DNS updates in one of the following ways:

- **TXT RR for DHCPv4 and DHCID for DHCPv6**—To enable this configuration set the dns-client-identity to txt. The server will use the TXT RR in DHCPv4 DNS updates and DHCID RR for DHCPv6 DNS updates.
- **DHCID RR for both DHCPv4 and DHCPv6**—To enable this configuration set the dns-client-identity to dhcid. The server will use the DHCID RR for both DHCPv4 and DHCPv6 DNS updates. This setting should be used to support dual stack clients and can only be used if all DHCP servers doing DNS updates to the zones for this configuration support and are configured to use the DHCID RR.
- **Transition to DHCID RR**—To enable this configuration set the dns-client-identity to transition-to-dhcid. Set the force-dns-update attribute to true. Reload the server. For the zones that need to be upgraded, set the dns-client-identity attribute to dhcid and restore the force-dns-update attribute to its earlier value, after the longest lease time configured in the server.

Note You must set the transition-to-dhcid attribute until all the DHCPv4 resource records are updated to DHCID RR. For more information, see Transitioning to DHCID RR for DHCPv4, on page 22.

- **Regress to TXT RR**—To enable this configuration set the dns-client-identity to regress-to-txt. Set the force-dns-update attribute to true. Reload the server. For the zones that need to be upgraded, set the dns-client-identity attribute to txt and restore the force-dns-update attribute to its earlier value, after the longest lease time configured in the server.

Note The CCM server will not allow the failover synchronization if one of the failover servers runs on Cisco Prime IP Express 8.1 or earlier and the dns-client-identity attribute, in the DHCP server or a DNS Update Configuration, is set to anything other than txt.

Local Advanced and Regional Web UI

Step 1 From the **Deploy** menu, choose **DNS Update Configs** under the **DNS Updates** submenu to open the List/Add DNS Update Configurations page.

Step 2 Select the name of the update configuration to open the **Edit DNS Update Configuration** page.

Step 3 In the DNS update settings, set *transition-to-dhcid as dns-client-identity* in DNS update settings.

Step 4 Optionally set *force-dns-update* to true. Using this setting will expedite the process of transitioning from TXT RR to DHCID RR.

Step 5 Set scavenging settings attributes in forward or reverse zones to the following values:

- Set scvg-enabled to true.

Step 6 Set scavenging settings attributes in DNS server to the following values:

- Set *scvg-interval* to longest lease time.
- Set *scvg-refresh-interval* to longest lease time.
- Set *scvg-no-refresh-interval* to 0.

Step 7 Verify that all TXT RRs are converted to DHCID RRs in the RRs for the zones. You must set the transition-to-dhcid attribute until all the DHCPv4 resource records are updated to DHCID RR. If some TXT RRs entries do not transition to DHCID RR, you may need to remove these DNS entries manually by using the Cisco Prime IP Express single-record dynamic RR removal feature.

Step 8 Click **Save**.

Configuring DNS Update for Windows Clients

The Windows operating system rely heavily on DNS and, to a lesser extent, DHCP. This reliance requires careful preparation on the part of network administrators prior to wide-scale Windows deployments. Windows clients can add entries for themselves into DNS by directly updating forward zones with their address (A) record. They cannot update reverse zones with their pointer (PTR) records.

Related Topics

Client DNS Updates, on page 23

Dual Zone Updates for Windows Clients, on page 25

DNS Update Settings in Windows Clients, on page 26

Windows Client Settings in DHCP Servers, on page 26

SRV Records and DNS Updates, on page 27

Issues Related to Windows Environments, on page 28

Frequently Asked Questions About Windows Integration, on page 32

Client DNS Updates

It is not recommended that clients be allowed to update DNS directly.

For a Windows client to send address record updates to the DNS server, two conditions must apply:

- The Windows client must have the **Register this connection's addresses in DNS** box checked on the **DNS** tab of its TCP/IP control panel settings.
- The DHCP policy must enable direct updating (Cisco Prime IP Express policies do so by default).

The Windows client notifies the DHCP server of its intention to update the A record to the DNS server by sending the *client-fqdn* DHCP option (81) in a DHCPREQUEST packet. By indicating the fully qualified

domain name (FQDN), the option states unambiguously the client location in the domain namespace. Along with the FQDN itself, the client or server can send one of these possible flags in the *client-fqdn* option:

- **0**—Client should register its A record directly with the DNS server, and the DHCP server registers the PTR record (done through the policy *allow-client-a-record-update* attribute being enabled).
- **1**—Client wants the DHCP server to register its A and PTR records with the DNS server.
- **3**—DHCP server registers the A and PTR records with the DNS server regardless of the client request (done through the policy *allow-client-a-record-update* attribute being disabled, which is the default value). Only the DHCP server can set this flag.

The DHCP server returns its own *client-fqdn* response to the client in a DHCPACK based on whether DNS update is enabled. However, if the 0 flag is set (the *allow-client-a-record-update* attribute is enabled for the policy), enabling or disabling DNS update is irrelevant, because the client can still send its updates to DNS servers. See the table below for the actions taken based on how various properties are set.

Table 3: Windows Client DNS Update Options

DHCP Client Action	DNS Update	DHCP Server Action
Checks **Register this connection's addresses in DNS** and sends *client-fqdn* ; DHCP server enables *allow-client-a-record-update*	Enabled or disabled	Responds with *client-fqdn* that it allows the client to update its A records (sets flag 0), but the DHCP server still updates the PTR records.
Checks **Register**... and sends *client-fqdn* ; DHCP disables *allow-client-a-record-update*	Enabled	Responds with *client-fqdn* that it does not allow the client to update the DNS server directly (sets flag 3), and updates the A and PTR records.
	Disabled	Does not respond with *client-fqdn* and does not update the DNS server.
Unchecks **Register**... and sends *client-fqdn*	Enabled	Responds with *client-fqdn* that it is updating the A and PTR records.
	Disabled	Does not respond with *client-fqdn* and does not update the DNS server.
Does not send *client-fqdn*	Enabled	Does not respond with *client-fqdn*, but updates the A and PTR records.
	Disabled	Does not respond with *client-fqdn* and does not update the DNS server.

A Windows DHCP server can set the *client-fqdn* option to ignore the client request. To enable this behavior in Cisco Prime IP Express, create a policy for Windows clients and disable the *allow-client-a-record-update* attribute for this policy.

The following attributes are enabled by default in Cisco Prime IP Express:

- **Server use-client-fqdn**—The server uses the *client-fqdn* value on incoming packets and does not examine the *host-name*. The DHCP server ignores all characters after the first dot in the domain name value, because it determines the domain from the defined scope for that client. Disable *use-client-fqdn* only if you do not want the server to determine hostnames from *client-fqdn*, possibly because the client is sending unexpected characters.

- **Server use-client-fqdn-first**—The server examines *client-fqdn* on incoming packets from the client before examining the *host-name* option (12). If *client-fqdn* contains a hostname, the server uses it. If the server does not find the option, it uses the *host-name* value. If *use-client-fqdn-first* is disabled, the server prefers the *host-name* value over *client-fqdn*.
- **Server use-client-fqdn-if-asked**—The server returns the *client-fqdn* value in the outgoing packets if the client requests it. For example, the client might want to know the status of DNS activity, and hence request that the DHCP server should present the *client-fqdn* value.
- **Policy allow-client-a-record-update**—The client can update its A record directly with the DNS server, as long as the client sets the *client-fqdn* flag to 0 (requesting direct updating). Otherwise, the server updates the A record based on other configuration properties.

The hostnames returned to client requests vary depending on these settings (see the table below).

Table 4: Hostnames Returned Based on Client Request Parameters

Client Request	With Server/Policy Settings	Resulting Hostname
Includes *host-name* (option 12)	*use-host-name* =true *use-client-fqdn* =false (or *use-client-fqdn-first* =false) *trim-host-name* =true	*host-name* trimmed at first dot. Example: *host-name* host1.bob is returned host1.
	(same except:) *trim-host-name* =false	*host-name*. Example: *host-name* host1.bob is returned host1.bob.
Includes *client-fqdn* (option 81)	*use-client-fqdn* =true *use-host-name* =false (or *use-client-fqdn-first* =true)	*client-fqdn* trimmed at first dot. Example: *client-fqdn* host1.bob is returned host1.
Omits *host-name* (option 12) and *client-fqdn* (option 81)	Or: *use-host-name* =false *use-client-fqdn* =false	Set by client/policy hierarchy.
	(same as the previous except:) hostname is undefined in the client/policy hierarchy, with *synthesize-name* =true	Synthesized following the synthesizing rule, which is to append the hyphenated IP address of the host after the specified *synthetic-name-stem*.
	(same as the previous except:) *synthesize-name* =false	Undefined.

Dual Zone Updates for Windows Clients

Windows DHCP clients might be part of a DHCP deployment where they have A records in two DNS zones. In this case, the DHCP server returns the *client-fqdn* so that the client can request a dual zone update. To enable a dual zone update, enable the policy attribute *allow-dual-zone-dns-update*.

The DHCP client sends the 0 flag in *client-fqdn* and the DHCP server returns the 0 flag so that the client can update the DNS server with the A record in its main zone. However, the DHCP server also directly sends an A record update based on the client secondary zone in the behalf of the client. If both *allow-client-a-record-update* and the *allow-dual-zone-dns-update* are enabled, allowing the dual zone update takes precedence so that the server can update the secondary zone A record.

DNS Update Settings in Windows Clients

The Windows client can set advanced properties to enable sending the *client-fqdn* option.

Step 1 On the Windows client, go to the Control Panel and open the TCP/IP Settings dialog box.

Step 2 Click the **Advanced** tab.

Step 3 Click the **DNS** tab.

Step 4 To have the client send the *client-fqdn* option in its request, leave the **Register this connection's addresses in DNS** box checked. This indicates that the client wants to do the A record update.

Windows Client Settings in DHCP Servers

You can apply a relevant policy to a scope that includes the Windows clients, and enable DNS updates for the scope.

Step 1 Create a policy for the scope that includes the Windows clients. For example:

a) Create a policywin2k. You have to specify the forward or reverse zone name, main and backup server IP addresses when you create a policy.

b) Create a win2k scope with the subnet 192.168.1.0/24 and policywin2k as the policy. Add an address range of 192.168.1.10 through 192.168.1.100.

Step 2 Set the zone name, server address (for A records), reverse zone name, and reverse server address (for PTR records), as described in Creating DNS Update Configurations, on page 12.

Step 3 If you want the client to update its A records at the DNS server, enable the policy attribute *allow-client-a-record-update* (this is the preset value). There are a few caveats to this:

- If *allow-client-a-record-update* is enabled and the client sends the *client-fqdn* with the update bit enabled, the *host-name* and *client-fqdn* returned to the client match the client *client-fqdn*. (However, if the *override-client-fqdn* is also enabled on the server, the hostname and FQDN returned to the client are generated by the configured hostname and policy domain name.)
- If, instead, the client does not send the *client-fqdn* with the update bit enabled, the server does the A record update, and the *host-name* and *client-fqdn* (if requested) returned to the client match the name used for the DNS update.
- If *allow-client-a-record-update* is disabled, the server does the A record updates, and the *host-name* and *client-fqdn* (with the update bit disabled) values returned to the client match the name used for the DNS update.
- If *allow-dual-zone-dns-update* is enabled, the DHCP server always does the A record updates. (See Dual Zone Updates for Windows Clients, on page 25.)
- If *use-dns-update-prereqs* is enabled (the preset value) for the DHCP server or DNS update configuration and *update-dns-first* is disabled (the preset value) for the update configuration, the hostname and *client-fqdn* returned to the client are not guaranteed to match the DNS update, because of delayed name disambiguation. However, the lease data will be updated with the new names.

  According to RFC 2136, update prerequisites determine the action the primary master DNS server takes based on whether an RR set or name record should or should not exist. Disable *use-dns-update-prereqs* only under rare circumstances.

Step 4 Reload the DHCP server.

SRV Records and DNS Updates

Windows relies heavily on the DNS protocol for advertising services to the network. The table below describes how Windows handles service location (SRV) DNS RRs and DNS updates.

You can configure the Cisco Prime IP Express DNS server so that Windows domain controllers can dynamically register their services in DNS and, thereby, advertise themselves to the network. Because this process occurs through RFC-compliant DNS updates, you do not need to do anything out of the ordinary in Cisco Prime IP Express.

Table 5: Windows SRV Records and DNS Updates

Feature	Description

SRV records	Windows domain controllers use the SRV RR to advertise services to the network. This RR is defined in the RFC 2782, "A DNS RR for specifying the location of services (DNS SRV)." The RFC defines the format of the SRV record (DNS type code 33) as:
	`_ service ._ protocol . name ttl class SRV priority weight port target`
	There should always be an A record associated with target of the SRV record, so that the client can resolve the service back to a host. In the Windows implementation of SRV records, the records might look like this:
	`myserver.example.com A 10.100.200.11`
	`_ldap._tcp.example.com SRV 0 0 389 myserver.example.com`
	`_kdc._tcp.example.com SRV 0 0 88 myserver.example.com`
	`_ldap._tcp.dc_msdcs.example.com SRV 0 0 88 myserver.example.com`

	An underscore always precedes the service and protocol names. In the example, _kdc is the Key Distribution Center. The priority and weight help you choose between target servers providing the same service (the weight differentiating those with equal priorities). With zero priority and weight, the listed order determines the priority. Windows domain controllers automatically place these SRV records in DNS.
How SRV records are used	When a Windows client boots up, it tries to initiate the network login process to authenticate against its Windows domain controller. The client must first discover where the domain controller is, and they do so using the dynamically generated SRV records. Before launching the net-login process, the client queries DNS with a service name; for example, _ldap._tcp.dc_msdcs.example.com. The DNS server SRV record target, for example, is my-domain-controller.example.com. The Windows client then queries DNS with the hostname my-domain-controller.example.com. DNS returns the host address and the client uses this address to find the domain controller. The net-login process fails without these SRV records.

DNS updates	When a Windows server is configured as a domain controller, you statically configure the name of the domain it manages through the Active Directory management console. This Windows domain should have a corresponding DNS zone associated with it. The domain controller should also have a series of DNS resolvers configured in its TCP/IP properties control panel.
	When the Windows domain controller boots up, it performs these steps to register itself in DNS and advertise its services to the network: **1.** Queries DNS asking for the start of authority (SOA) record for the DNS domain that mostly closely encapsulates its Windows domain. **2.** Identifies the primary DNS server for the DNS zone (from the SOA record) that mostly closely encapsulates its Windows domain name. **3.** Creates a series of SRV records in this zone using the RFC 2136 DNS Update protocol.

Server boot process log file examples	Under normal operating conditions, the Cisco Prime IP Express primary DNS server writes these log entries when a Windows domain controller boots up and creates its SRV records:
	`data time name/dns/1 Activity Protocol 0 Added type 33 record to name "_ldap._tcp.w2k.example.com", zone "w2k.example.com"`
	`data time name/dns/1 Activity Protocol 0 Update of zone "w2k.example.com" from address [10.100.200.2] succeeded.`
	This log shows only one DNS update for a single SRV record. A Windows domain controller typically registers 17 of these SRV records when it boots up.

Issues Related to Windows Environments

The table below describes the issues concerning interoperability between Windows and Cisco Prime IP Express, The information in this table is intended to inform you of possible problems before you encounter them in the field. For some frequently asked questions about Windows interoperability, see Frequently Asked Questions About Windows Integration, on page 32.

Table 6: Issues Concerning Windows and Cisco Prime IP Express Interoperability

Issue	Description
Invisible dynamically created RRs	Cisco Prime IP Express, when properly configured, accepts DNS updates from both DHCP and Windows servers. You can use the CLI to access the dynamic portion of the DNS zone for viewing and deleting records. Enter this command to view all DNS RRs in a given zone: `nrcmd> zone myzone listRR dynamic myfile`

	This redirects the output to the myfile file (see the following *Example: Output Showing Invisible Dynamically Created RRs* section). You can delete dynamically generated records by entering this command: `nrcmd> zone myzone removeDynRR myname [ type ]` You can also use **nslookup** to verify their existence, and you can use version 5. *x* (shipped with Windows) to view dynamic SRV records. In this version, use **set type=SRV** to enable viewing SRV records.
Domain controller registration	A Windows domain controller has to register itself in DNS using DNS updates. The DNS RFCs dictate that only a primary DNS server for a particular zone can accept edits to the zone data. Hence, the Windows domain controller has to discover which DNS server is the primary for the zone that includes its Windows domain name. The domain controller discovers this by querying the first DNS server in its resolver list (configured in the TCP/IP properties control panel). The initial query is for the SOA record of the zone that includes the Windows domain of the domain controller. The SOA record includes the name of the primary server for the zone. If no zone exists for the domain name, the domain controller keeps removing the left-most label of the domain name and sends queries until it finds an SOA record with a primary server included in that domain. Once the domain controller has the name of the primary DNS server for its domain, it sends it DNS updates to create the necessary SRV records. Ensure that the name of the zone primary DNS server is in its SOA record.

Failure of A record DNS updates	When a Windows domain controller tries to advertise itself to the network, it sends several DNS update requests to the DNS server of record for its domain. Most of these update requests are for SRV records. However, the domain controller also requests an update for a single A record of the same name as the Windows domain.
	
	If the Cisco Prime IP Express DNS server is also authoritative for a zone identical to this Windows domain, it rejects registering its A record, because the DNS A record update conflicts with the static SOA and NS records. This is to prevent possible security infractions, such as a dynamic host registering itself and spoofing Web traffic to a site.
	
	For example, the domain controller might control the w2k.example.com Windows zone. If a zone with the same name exists on the Cisco Prime IP Express DNS server, these RRs could be part of that zone. (Example follows.)
	
	`w2k.example.com. 43200 SOA nameserver.example.com.`
	`hostmaster.example.com.`
	`(`
	`98011312 ;serial`
	`3600 ;refresh`
	`3600 ;retry`
	`3600000 ;expire`
	`43200 ) ;minim`
	`w2k.example.com.86400 NS nameserver.example.com`
	
	The domain controller would try to add an additional record; for example:
	
	`w2k.example.com. 86400 A 192.168.2.1`
	
	Cisco Prime IP Express does not allow a DNS update to conflict with any statically configured name in the zone, even if the record type associated with that name is different. In the above example, an attempt to add an A record associated with the name w2k.example.com collides with the SOA and NS records.
	
	When the domain controller boots up, a DNS log file entry such as this appears:
	
	`0 8/10/2000 16:35:33 name/dns/1 Info Protocol 0 Error - REFUSED -`
	
	`Update of static name "w2k.example.com", from address [10.100.200.2]`
	
	This is how Cisco Prime IP Express responds to DNS updates of static DNS data. Additionally, you can ignore this DNS update failure. Windows clients do not use this A record. Allocation of domain controllers happens through SRV records. Microsoft added the A record to accommodate legacy NT clients that do not support SRV records.
	
	Note that failing to register the controller A record slows down the domain controller bootup process, affecting the overall login of worker clients. As mentioned earlier, the workaround is to define the Windows domain as a subdomain of the authoritative zone, or enable the DNS server*simulate-zone-top-dynupdate* attribute. If this is not possible, contact the Cisco Technical Assistance Center for help.

Windows RC1 DHCP clients	Microsoft released Windows build 2072 (known as RC1) with a broken DHCP client. This client sends a misformed packet that Cisco Prime IP Express cannot parse. Cisco Prime IP Express drops the packet and cannot serve the client, logging this error:
	`08/10/2000 14:56:23 name/dhcp/1 Activity Protocol 0 10.0.0.15 Lease offered to Host:'My-Computer' CID: 01:00:a0:24:1a:b0:d8 packet'R15' until True, 10 Aug 2000 14:58:23 -0400. 301 ms.`
	`08/10/2000 14:56:23 name/dhcp/1 Warning Protocol 0 Unable to find necessary Client information in packet from MAC address:'1,6,00:d0:ba:d3:bd:3b'. Packet dropped!`
	Cisco Prime IP Express includes error checking specifically designed to deal with errors such as this improperly built FQDN option. However, if you encounter this problem, install the Microsoft patch to the RC1 client on the DHCP client. You must obtain this patch from Microsoft.

Windows plug-and-play network interface card (NIC) configuration	If configured to use DHCP, a Windows system tries to obtain a DHCP lease on startup. If no DHCP server is available, Windows may automatically configure the computer interface with a plug-and-play IP address. This address is not one that the network administrator or DHCP server configured or selected. These plug-and-play addresses are in the range 169.254.0.0/16. If you see devices in this address range on a network, it means that Windows autoconfigured the interfaces because it could not obtain a lease from a DHCP server. This can cause significant network and troubleshooting problems. The Windows system no longer informs the user that the DHCP client could not obtain a lease. Everything appears to function normally, but the client cannot route packets off its local subnet. Additionally, you may see the DHCP client trying to operate on the network with an address from the 169.254.0.0/16 network. This may lead you to think that the Cisco Prime IP Express DHCP server is broken and handing out the wrong addresses.
	If this problem occurs, perform these steps: **1.** Ensure that the DHCP client has an active network port and a properly configured NIC. **2.** Ensure that the network between the client and the DHCP server(s) are properly configured. Ensure that all router interfaces are configured with the correct IPHelper address. **3.** Reboot the DHCP client. **4.** If necessary, look at the DHCP log file. If the DHCP client can successfully route packets to the server, this logs a DHCPDISCOVER, even if Cisco Prime IP Express does not answer the packet. If the network is correctly configured, and if the DHCP client is not broken, Cisco Prime IP Express should receive the packet and log it. If there is no log entry for a packet receipt, there is a problem somewhere else in the network.

Scavenging Windows client address records	Windows clients do not clean up after themselves, potentially causing their dynamic record registration to remain indefinitely. This leaves stale address records on the DNS server. To ensure that these stale records are periodically removed, you must enable scavenging for the zone (see Scavenging Dynamic Records, on page 20).

Example: Output Showing Invisible Dynamically Created RRs

```
 Dynamic Resource Records _ldap._tcp.test-lab._sites 600 IN SRV 0
100 389 CNR-MKT-1.w2k.example.com. _ldap._tcp.test-lab._sites.gc._msdcs 600 IN
SRV 0 100 3268 CNR-MKT-1.w2k.example.com.
_kerberos._tcp.test-lab._sites.dc._msdcs 600 IN SRV 0 100 88
CNR-MKT-1.w2k.example.com. _ldap._tcp.test-lab._sites.dc._msdcs 600 IN SRV 0
100 389 CNR-MKT-1.w2k.example.com. _ldap._tcp 600 IN SRV 0 100 389
CNR-MKT-1.w2k.example.com. _kerberos._tcp.test-lab._sites 600 IN SRV 0 100 88
CNR-MKT-1.w2k.example.com. _ldap._tcp.pdc._msdcs 600 IN SRV 0 100 389
CNR-MKT-1.w2k.example.com. _ldap._tcp.gc._msdcs 600 IN SRV 0 100 3268
CNR-MKT-1.w2k.example.com.
_ldap._tcp.1ca176bc-86bf-46f1-8a0f-235ab891bcd2.domains._msdcs 600 IN SRV 0 100
389 CNR-MKT-1.w2k.example.com. e5b0e667-27c8-44f7-bd76-6b8385c74bd7._msdcs 600
IN CNAME CNR-MKT-1.w2k.example.com. _kerberos._tcp.dc._msdcs 600 IN SRV 0 100
88 CNR-MKT-1.w2k.example.com. _ldap._tcp.dc._msdcs 600 IN SRV 0 100 389
CNR-MKT-1.w2k.example.com. _kerberos._tcp 600 IN SRV 0 100 88
CNR-MKT-1.w2k.example.com. _gc._tcp 600 IN SRV 0 100 3268
CNR-MKT-1.w2k.example.com. _kerberos._udp 600 IN SRV 0 100 88
CNR-MKT-1.w2k.example.com. _kpasswd._tcp 600 IN SRV 0 100 464
CNR-MKT-1.w2k.example.com. _kpasswd._udp 600 IN SRV 0 100 464
CNR-MKT-1.w2k.example.com. gc._msdcs 600 IN A 10.100.200.2
_gc._tcp.test-lab._sites 600 IN SRV 0 100 3268 CNR-MKT-1.w2k.example.com.
```

Frequently Asked Questions About Windows Integration

These questions are frequently asked about integrating Cisco Prime IP Express DNS services with Windows:

What happens if both Windows clients and the DHCP server are allowed to update the same zone? Can this create the potential for stale DNS records being left in a zone? If so, what can be done about it?

The recommendation is not to allow Windows clients to update their zones. Instead, the DHCP server should manage all the client dynamic RR records. When configured to perform DNS updates, the DHCP server accurately manages all the RRs associated with the clients that it served leases to. In contrast, Windows client machines blindly send a daily DNS update to the server, and when removed from the network, leave a stale DNS entry behind.

Any zone being updated by DNS update clients should have DNS scavenging enabled to shorten the longevity of stale RRs left by transient Windows clients. If the DHCP server and Windows clients are both updating the same zone, three things are required in Cisco Prime IP Express:

1. Enable scavenging for the zone.
2. Configure the DHCP server to refresh its DNS update entries as each client renews its lease. By default, Cisco Prime IP Express does not update the DNS record again between its creation and its final deletion. A DNS update record that Cisco Prime IP Express creates lives from the start of the lease until the lease expires. You can change this behavior using a DHCP server (or DNS update configuration) attribute, *force-dns-updates*. For example:

   ```
   nrcmd> dhcp enable force-dns-updates
   ```

```
100 Ok
force-dns-updates=true
```

3. If scavenging is enabled on a particular zone, then the lease time associated with clients that the DHCP server updates that zone on behalf of must be less than the sum of the *no-refresh-interval* and *refresh-interval* scavenging settings. Both of these settings default to seven days. You can set the lease time to 14 days or less if you do not change these default values.

What needs to be done to integrate a Windows domain with a pre-existing DNS domain naming structure if it was decided not to have overlapping DNS and Windows domains? For example, if there is a pre-existing DNS domain called example.com and a Windows domain is created that is called w2k.example.com, what needs to be done to integrate the Windows domain with the DNS domain?

In the example, a tree in the Windows domain forest would have a root of w2k.example.com. There would be a DNS domain named example.com. This DNS domain would be represented by a zone named example.com. There may be additional DNS subdomains represented in this zone, but no subdomains are ever delegated out of this zone into their own zones. All the subdomains will always reside in the example.com. zone.

In this case, how are DNS updates from the domain controllers dealt with?

To deal with the SRV record updates from the Windows domain controllers, limit DNS updates to the example.com. zone to the domain controllers by IP address only. (Later, you will also add the IP address of the DHCP server to the list.) Enable scavenging on the zone. The controllers will update SRV and A records for the w2k.example.com subdomain in the example.com zone. There is no special configuration required to deal with the A record update from each domain controller, because an A record for w2k.example.com does not conflict with the SOA, NS, or any other static record in the example.com zone.

The example.com zone then might include these records:

```
example.com. 43200 SOA ns.example.com. hostmaster.example.com. (
98011312 ;serial
3600 ;refresh
3600 ;retry
3600000 ;expire
43200 ) ;minimum
example.com.86400 NS ns.example.com
ns.example.com. 86400 A 10.0.0.10
_ldap._tcp.w2k.example.com. IN SRV 0 0 389 dc1.w2k.example.com
w2k.example.com 86400 A 10.0.0.25
...
```

In this case, how are zone updates from individual Windows client machines dealt with?

In this scenario, the clients could potentially try to update the example.com. zone with updates to the w2k.example.com domain. The way to avoid this is to close down the zone to updates except from trusted sources. For Cisco Prime IP Express, you can use transaction signatures (TSIG) between the DHCP server and the primary DNS server for the example.com zone.

Configure the DHCP server to do DNS updates to the example.com zone and the appropriate reverse zone for each client, and use option 81 to prevent the clients from doing DNS updates themselves.

Has security been addressed in this case?

By configuring the forward and reverse zone to accept only updates from trusted IP addresses, you close the zone to updates from any other device on the network. Security by IP is not the most ideal solution, as it would not prevent a malicious attack from a spoofed IP address source. You can secure updates from the DHCP server by configuring TSIG between the DHCP server and the DNS server.

Is scavenging required in this case?

No. Updates are only accepted from the domain controllers and the DHCP server. The DHCP server accurately maintains the life cycle of the records that they add and do not require scavenging. You can manage the domain controller dynamic entries manually by using the Cisco Prime IP Express single-record dynamic RR removal feature.

What needs to be done to integrate a Windows domain that shares its namespace with a DNS domain? For example, if there is a pre-existing DNS zone called example.com and a Windows Active Directory domain called example.com needs to be deployed, how can it be done?

In this example, a tree in the Windows domain forest would have a root of example.com. There is a pre-existing domain that is also named example.com that is represented by a zone named example.com.

In this case, how are DNS updates from individual Windows client machines dealt with?

To deal with the SRV record updates, create subzones for:

```
_tcp.example.com.
_sites.example.com.
_msdcs.example.com.
_msdcs.example.com.
_udp.example.com.
```

Limit DNS updates to those zones to the domain controllers by IP address only. Enable scavenging on these zones.

To deal with the A record update from each domain controller, enable a DNS server attribute, *simulate-zone-top-dynupdate*.

```
nrcmd> dns enable simulate-zone-top-dynupdate
```

It is not required, but if desired, manually add an A record for the domain controllers to the example.com zone.

In this case, how are zone updates from individual Windows client machines dealt with?

In this scenario, the clients could potentially try to update the example.com zone. The way to avoid this is to close down the zone to updates except from trusted sources. For Cisco Prime IP Express, you can use transaction signatures (TSIG) between the DHCP server and the primary DNS server for the example.com zone.

Configure the DHCP server to do DNS updates to the example.com zone and the appropriate reverse zone for each client, and use option 81 to prevent the clients from doing DNS updates themselves.

Has security been addressed in this case?

By configuring the forward and reverse zone to accept only updates from trusted IP addresses, you close the zone to updates from other devices on the network. Security by IP is not the most ideal solution, as it would not prevent a malicious attack from a spoofed source. Updates from the DHCP server are more secure when TSIG is configured between the DHCP server and the DNS server.

Has scavenging been addressed in this case?

Yes. The subzones _tcp.example.com, _sites.example.com, _msdcs.example.com, _msdcs.example.com, and _udp.example.com zones accept updates only from the domain controllers, and scavenging was turned on for these zones. The example.com zone accepts DNS updates only from the DHCP server.

Configuring GSS-TSIG

Cisco Prime IP Express DNS Configuration to integrate with AD

To integrate AD with Cisco Prime IP Express DNS configuration, follow these steps:

Step 1 Install Cisco Prime IP Express DNS on a Workgroup machine.

Step 2 Create a zone (same as the domain of AD).

Install AD on a windows server using dcpromo.exe and integrate with Cisco Prime IP Express DNS.

Step 3 Ensure the SRV records are added in Cisco Prime IP Express DNS

```
DCHOSTNAME. DOMAIN.COM A AD-IP-ADDRESS
_ldap._tcp.DOMAIN.COM. SRV 0 0 389 DCHOSTNAME.DOMAIN.COM.
_kerberos._tcp.DOMAIN.COM. SRV 0 0 88 DCHOSTNAME.DOMAIN.COM.
_ldap._tcp.dc._msdcs.DOMAIN.COM. SRV 0 0 389 DCHOSTNAME.DOMAIN.COM.
_kerberos._tcp.dc._msdcs.DOMAIN.COM. SRV 0 0 88 DCHOSTNAME.DOMAIN.COM.
```

Note **DCHOSTNAME** refers to AD host name and **DOMAIN.COM** is the domain that exists in AD.

Bring Cisco Prime IP Express DNS and AD under the same domain in the windows environment:

Step 1 Change the domain, **Computer > Properties > Computer Name >** change the member of domain (same as the domain of AD).

Step 2 Control Panel > Network and Internet > Network and Sharing Center > Local Area Connection > Properties > TCP/IPV4 > Preferred DNS (Cisco Prime IP Express DNS running IP).

Step 3 Restart the computer, and login with the User that exists in AD.

Step 4 Login to AD and do the following:

- check the DNS active Hostname is added into, **AD Server Manager > Computers**

```
setspn -s DNS/ <hostname of the DNS server> <Computer Name>
```

Integrating the DNS server to AD-KDC

In Linux, the primary DNS server is integrated to AD-KDC:

Step 1 Ensure the /etc/krb5.conf or DNS server with SRV record is configured to reach the required AD.

```
krb5.conf cofiguration
[libdefaults]
ticket_lifetime = 24h
default_realm = <AD REALM>
default_tkt_enctypes = rc4-hmac
default_tgs_enctypes = rc4-hmac
dns_lookup_realm = true
dns_lookup_kdc = false
forwardable = true
<AD REALM> = {
  kdc =< AD-HOSTNAME>:88
  admin_server = =< AD-HOSTNAME:749
  default_domain = <AD REALM>
}
```

Note Ensure that the AD-HOSTNAME is resolvable.

Step 2 Create a service account in the Windows Server Active Directory:

1. Use the Active Directory Users and Computers Administrative Tool to create a new user account.
   - Assign a user name to the account without any space.
   - Assign a password to the account

   Note Whenever the password expires/changed, the **keytab** file needs to be generated with a new associated *kvno*.

2. Assign a Service Principal Name (SPN) to the account utilizing the SETSPN.EXE. An SPN is the service-name/hostname/domain depending on the deployment. There can be multiple SPNs assigned to a single account.

   For example, specify a <service-name> and a <hostname> where the service-name is DNS and the hostname is the fully qualified domain name of the machine on which the DNS server will be running.

   ```
   setspn -s DNS/<DNS running Computer Name> <Service Name>
   ```

3. Get the *kvno* details:

   ```
   ldifde -f <Filename> -d "DC=<DOMAIN>,DC=com" -l *,msDS-KeyVersionNumber -r
   "(serviceprincipalname=<service-principal name>)" -p subtree OR kvno.exe <service-principal
   name>@<REALM>
   ```

4. Genetare the Keytab file using the ktpass.exe command:

   ```
   ktpass -out<filename>  -princ <Principal name> -pass <password associated with the user> -crypto
    all -ptype KRB5_NT_PRINCIPAL -kvno <Kvno details>
   ```

   Transfer the keytab file to the Linux machine and run Kutil to add the Keytab entry to the existing Keytab file:

   ```
   > ktutil
    ktutil:  rkt <keytab file name>
    ktutil:  wkt /etc/krb5.keytab
    ktutil:  q
   ```

Step 3 Display the keytab entry using:

```
klist -k -t -e /etc/krb5.keytab
```

Primary DNS Server on Linux Integrated to MIT-KDC

To associate the service-principal name to MIT KDC:

Step 1 Login to the Linux DNS server and use kadmin utility to add the principal name to the MIT-KDC:

```
>kadmin
Authenticating as principal <MIT-KDC USER@REALM> with password.
Password for <MIT-KDC USER@REALM.COM > : <Enter the associated Password>
kadmin:  addprinc -randkey DNS/<hostname of the DNS server>
WARNING: no policy specified for DNS/<hostname of the DNS server>@REALM; defaulting to no policy
add_principal: Principal or policy already exists while creating " DNS/<hostname of the DNS
server>@REALM".
kadmin:  ktadd -randkey DNS/<hostname of the DNS server>
kadmin: Principal -randkey does not exist.
Entry for principal DNS/<hostname of the DNS server> with kvno x, encryption type AES-256 CTS mode
with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5.keytab.
Entry for principal DNS/<hostname of the DNS server>with kvno x, encryption type AES-128 CTS mode
with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5.keytab.
Entry for principal DNS/<hostname of the DNS server>with kvno x, encryption type Triple DES cbc mode
 with HMAC/sha1 added to keytab WRFILE:/etc/krb5.keytab.
Entry for principal DNS/<hostname of the DNS server>with kvno x, encryption type ArcFour with HMAC/md5
 added to keytab WRFILE:/etc/krb5.keytab.
kadmin:  quit
```

Step 2 Display the keytab entry using:

```
klist -k -t -e /etc/krb5.keytab
```

Step 3 Login to the MIT-KDC running LINUX server and check the added principal name has the same kvno associated as above using the command:

```
Kvno DNS/<hostname of the DNS server>
```

Troubleshooting GSS-TSIG Configuration

To get the details of GSS/SSPI failure and major/minor status, enable the DEBUG options in the DNS server and set the value of g=3.

- "The key version number for the principal in the key table is incorrect."

  The Kvno returned by, klist -k -t -e /etc/krb5.keytab in the DNS running machine should be the same kvno in KDC.

  Verification of knvo in AD-KDC:

  ```
  ldifde -f c:\spn1_out.txt -d "DC=TIG,DC=com" -l *,msDS-KeyVersionNumber -r
  "(serviceprincipalname=DNS/WIN-CPNUV*)" -p subtree
  ```

  Verification of kvno is MIT- KDC:

  ```
  Kvno <principal name>
  ```

- "Wrong Principal Name"

  Ensure that the GSS Client and the server are using the same service-key that is used to encrypt/decrypt the service ticket.

Troubleshooting DNS Update

You can use a standard DNS tool such as **dig** and **nslookup** to query the server for RRs. The tool can be valuable in determining whether dynamically generated RRs are present. For example:

```
$ nslookup

default Server: server2.example.com
Address: 192.168.1.2
> leasehost1.example.com

Server: server2.example.com
Address: 192.168.1.100
> set type=ptr

> 192.168.1.100

Server: server2.example.com
Address: 192.168.1.100
100.40.168.192.in-addr.arpa name = leasehost1.example.com
40.168,192.in-addr.arpa nameserver = server2.example.com
```

You can monitor DNS updates on the DNS server by setting the *log-settings* attribute to *ddns*, or show even more details by setting it to *ddns-details*.