Chapter 21 Configuring DDNS Updates

DDNS (Dynamic DNS) is a method to update DNS data (A, TXT, and PTR records) from sources such as DHCP servers and other systems that support DDNS updates, such as Microsoft Windows servers 2000, 2003, 2008, 2008 R2, 2012, 2012 R2, and 2016. This chapter provides conceptual information about DDNS and explains how to configure NIOS appliances running DHCP, DHCPv6 and DNS to support DDNS updates. It contains the following main sections:

- bookmark1915
  - Configuring DHCP for DDNS
    - Enabling DDNS for IPv4 and IPv6 DHCP Clients
    - Sending Updates to DNS Servers
  - Configuring DDNS Features
    - Resending DDNS Updates
    - Generating Host Names for DDNS Updates
    - Configuring DDNS Features
    - Replacing Host Names for DDNS Updates
  - About the Client FQDN Option
    - Enabling FQDN Option Support
    - Sending Updates for DHCP Clients Using the FQDN Option
  - Configuring DDNS Update Verification
  - Configuring DNS Servers for DDNS
    - Enabling DNS Servers to Accept DDNS Updates
    - Forwarding Updates
  - Supporting Active Directory
    - Sending DDNS Updates to a DNS Server
  - About GSS-TSIG
    - Sending Secure DDNS Updates to a DNS Server in the Same Domain
    - Configuring DHCP to Send GSS-TSIG Updates in the Same Domain
    - Sending Secure DDNS Updates to a DNS Server in Another Domain
    - Configuring DHCP to Send GSS-TSIG Updates to Another Domain
    - Sending GSS-TSIG Updates to a DNS Server in Another Forest
  - Configuring GSS-TSIG keys
    - Limitations when Using Multiple GSS-TSIG keys
    - Scheduled Upgrade
    - Admin Permissions for Configuring GSS-TSIG keys
    - Enabling GSS-TSIG Authentication for DHCP
    - Deleting GSS-TSIG keys associated with DHCP Objects
    - Enabling GSS-TSIG Authentication for DNS
    - Deleting GSS-TSIG keys associated with the DNS Objects
    - Logging Messages
    - Managing GSS-TSIG keys
    - Selecting Keys in the GSS-TSIG Key Selector
  - Accepting DDNS Updates from DHCP Clients
  - Supporting Active Directory and Unauthenticated DDNS Updates
  - Accepting GSS-TSIG-Authenticated Updates
  - Configuring DNS to Receive GSS-TSIG Updates
  - Secure Dynamic Updates
    - Restricting Updates to Static Records
    - Restricting Updates to Protected Records
    - Restricting Updates Based on GSS-TSIG Principal Authentication
    - Restricting Updates Based on FQDN Patterns

Understanding DDNS Updates from DHCP

DHCP supports several DNS-related options (such as options 12, 15, and 81 for IPv4, and options 23, 24, and 39 for IPv6). With DDNS (Dynamic DNS) updates, a DHCP server or client can use the information in these options to inform a DNS server of dynamic domain name-to-IP address assignments.

Note: DDNS updates is not supported by IPv6-only appliances.

To set up one or more NIOS appliances for DDNS updates originating from DHCP, you must configure at least one DHCP server and one DNS server. These servers might be on the same appliance or on separate appliances. Three possible arrangements for a DHCP server to update a DNS server are shown in Figure 21.1.
Figure 21.1 Relationship of DHCP and DNS Servers for DDNS Updates

**Scenario 1:**
- DDNS when the DHCP server and primary DNS server are on the same NIOS appliance.
- DDNS Update
- Zone Transfer

**Scenario 2:**
- DDNS when the DHCP server and primary DNS server are on different NIOS appliances and the DHCP server updates the primary DNS server.
- DDNS Update
- Zone Transfer

**Scenario 3:**
- DDNS when the DHCP server and primary DNS server are on different appliances and the DHCP server updates a secondary DNS server.
- DDNS Update
- Forwarded DDNS Update
- Zone Transfer
Here is a closer look at one setup for performing DDNS updates from a DHCP server (the steps relate to Figure 21.2).

1. When an IPv4 DHCP client requests an IP address, the client sends its host name (DHCP option 12). The client also includes its MAC address in the ethernet frame header.
2. a. When the DHCP server responds with an IP address, it usually provides a domain name (DHCP option 15). The combined host name (from the client) and domain name (from the server) form an FQDN (fully qualified domain name), which the NIOS appliance associates with the IP address in the DHCP lease.
b. The DHCP server sends the A, TXT, and PTR records of the DHCP client to the primary DNS server to update its resource records with the dynamically associated FQDN + IP address.
3. The primary DNS server notifies its secondary servers of a change. The secondary servers confirm the need for a zone transfer, and the primary server sends the updated zone data to the secondary server, completing the update.

**Note:** For information about zone transfers, see *Enabling Zone Transfers.*

*Figure 21.2 DDNS Update from a DHCP Server*

To enable a DHCP server to send DDNS updates to a DNS server, you must configure both servers to support the updates. First, configure the DHCP server to do the following:

- Provide what is needed to create an FQDN: add a server-generated host name to a server-provided domain name, add a server-provided domain name to a client-supplied host name, or permit the client to provide its own FQDN
- Send updates to a DNS server
Then, configure the following on the DNS server:

- Accept updates from the DHCP server, a secondary DNS server, or a DHCP client
- If the DHCP server sends updates to a secondary DNS server, configure the secondary server to forward updates to the primary DNS server
When setting up DDNS, you can determine the amount of information that DHCP clients provide to a DHCP server — and vice versa — and where the DDNS updates originate. A summary of these options for IPv4 is shown in Figure 21.3. It is similar for IPv6, except that the DHCP client and server exchange Request and Reply messages, AAAA records are updated instead of A records, and the FQDN option is option 39.

Figure 21.3 DHCP Clients and Server Providing DNS Information and Updates

You can configure the DHCP and DNS settings for DDNS at the Grid level, member level, and network and zone level. By applying the inheritance model in the NIOS appliance, settings made at the Grid level apply to all members in the Grid. Settings you make at the member level apply to all networks and zones configured on that member. Settings made at the network and zone level apply specifically to just that network and zone. When configuring independent appliances (that is, appliances that are not in a Grid), do not use the member-level settings. Instead, configure DDNS updates at the Grid level to apply to all zones and, if necessary, override the Grid-level settings on a per zone basis.