12

Domain Name System (DNS) Services

Contents

Overview

Domain Name System (DNS) is the Internet protocol for translating domain names or hostnames into IP addresses. The hostname is the familiar, alpha-numeric name for a host on the Internet (for example, www.hp.com), and the IP address is the 32-bit address that machines use to reach each other. DNS allows users to enter more readily memorable and intuitive hostnames rather than IP addresses. It also allows a host to keep the same hostname even if it changes its IP address.

Host and Domain Names

The domain name of a single host is also called a hostname. A hostname is typically made up of at least three domain levels. For example, the top-level domain of www.hp.com is "com." The Internet is divided into hundreds of top-level domains. The most common include com, gov, org, and two-letter codes for every country.

There are millions of first-level domains (hp, in our example), each designating an organization. When you want to reserve a domain name, you work through the proper channel for your top-level domain. The top-level organization ensures that every first-level domain in the top-level domain is unique.

The second (or third or fourth) domain level refers to the specific machine. For example, *www* often identifies a domain's Web server. An organization can subdivide its domain, so a hostname might include four or more levels.

Host Tables

In the very early days of the Internet, Stanford Research Institute's Network Information Center (SRI-NIC) maintained a single host table mapping all hostnames in the Internet to their IP addresses. Individual network adminis-trators would download new entries to their name servers. However, as the Internet exploded with new domains, SRI-NIC simply could not manage all the new entries, nor could name servers hold them all.

DNS distributes host tables throughout many DNS servers or name servers. The host table is divided into many zones, and each name server only holds the information for a few zones. Every organization maintains the host table for its own domain on its name server or servers. It is up to the organization to keep its own information accurate and up to date.

This system diffuses domain records throughout the Internet. Hosts anywhere on the Internet can still reach each other because name servers can query each other for the hostnames they cannot translate.

Authoritative and Caching Name Servers

Most name servers function as an authoritative server for one or several zones and as a caching server for all other zones. A name server's host table includes entries for all hosts in the zones on which it is authoritative. When a client requests the IP address for one of these hosts, the authoritative server can immediately provide it. The server caches the most recently requested entries for hosts in other zones. It has received these entries from other servers through a query process.

DNS Queries

When a server receives a request to translate a hostname that is not in its host table or cache, it runs its resolver and queries its root server. Root servers know the addresses for the top-level name servers, which in turn know the addresses for the name servers of their first-level domains. These servers provide IP addresses for hosts in their domain. (See Figure 12-1 for an example of a DNS query.)

Caching addresses speeds up the query process. Clients are constantly requesting .com addresses. A name server will hold the top-level name server's address in its cache, instead of having to query its root server for it each time a client requests an address ending in .com.
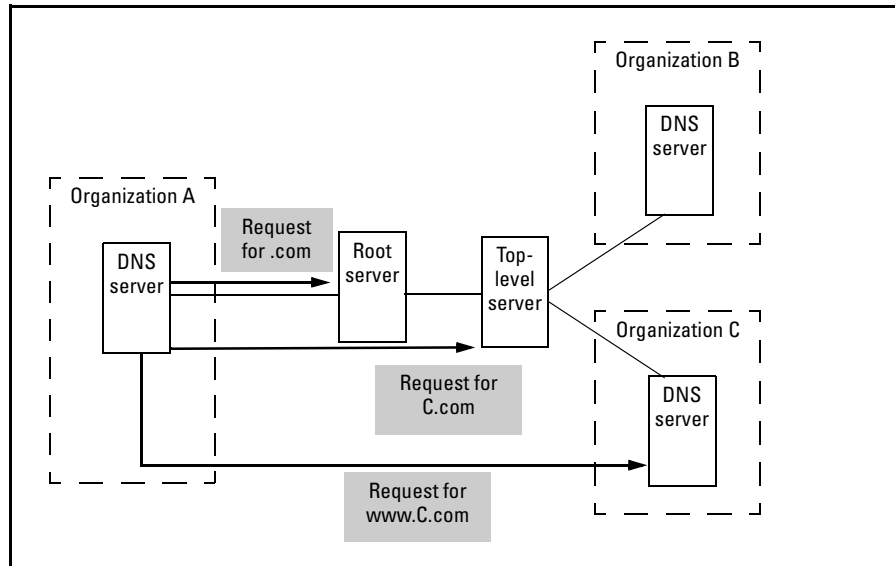
Figure 12-1. DNS Queries

Similarly, when a client accesses several hosts in the same first-level domain, the DNS server caches the IP address for the first-level domain server.

ProCurve Secure Router DNS Support

The ProCurve Secure Router can function as an authoritative name server for hosts in your domain. The router stores a host table with the entries for local hosts. It can also act as a caching server. When the ProCurve Secure Router runs DNS proxy, it can ask another server to resolve clients' queries for hostnames not in its own table.

In addition, the ProCurve Secure Router can run a DNS client for itself. The DNS client lets you enter hostnames instead of IP addresses for ping, traceroute, and other troubleshooting commands. When the router acts as a client, it can look up names for itself in its host table. It can also send DNS requests to its external DNS servers.

Dynamic DNS

Your device's IP address may change, and such changes are not always under your control. For example, your router may receive a dynamic address from your Internet service provider (ISP). When a device's address changes, DNS servers will no longer be able to resolve its hostname, and customers will not be able to access the device.

In order to map a dynamic IP address with a static hostname, you should register with an organization that provides dynamic DNS services.

The ProCurve Secure Router supports a client that is compatible with Dynamic Networking Services, Inc. (**www.dyndns.org**), or DynDNS. The client runs on a router interface. It automatically notifies DynDNS whenever the interface's IP address changes, and DynDNS propagates the change throughout its system of DNS servers.

DynDNS provides several types of services:

- Dynamic DNS^{SM}
- Static DNS^{SM}
- Custom DNS^{SM}

Depending on the service you select, you can register a hostname in one of the domains provided by DynDNS or in your own domain.

Dynamic DNS

Dynamic DNS is a free service that allows you to map dynamic addresses to up to five hostnames. You must register hostnames in one of 68 set domains. (See **http://www.dyndns.org/services/dns/dyndns/domains.html** for a list of available domains.)

The client running on the ProCurve Secure Router interface automatically updates DynDNS when the interface's IP address changes. (If DynDNS does not receive at least one update every 35 days, it deletes the hostname.) DynDNS provides five globally redundant DNS servers to ensure that your hostname will always resolve.

Dynamic DNS is primarily designed for private users. For commercial applications, you should probably purchase an account upgrade or Custom DNS.

Static DNS

You can use Static DNS to register a device with a free hostname in one of the domains used with Dynamic DNS. Static DNS provides many of the same services as Dynamic DNS, but it is tailored for devices whose IP addresses rarely change. When you use Static DNS, new information takes longer to propagate; however, DynDNS maintains a device's hostname even when the device does not send an update within 35 days.

Static DNS may be a good solution for you when:

■ your device's IP address rarely changes

■ you want to assign the device a static, easy-to-remember hostname, but you do not want to purchase a domain name

Custom DNS

You can use Custom DNS with both static and dynamic IP addresses. Custom DNS provides all the features of Dynamic DNS, with several additions.

With Custom DNS, you can map a dynamic IP address to a hostname in nearly any domain. (Exceptions include domains in alternate roots; see **http://www.dyndns.org/services/dns/custom/supported-domains.html** for more information.) You can also use your own domain, over which you have complete control. You can purchase the domain name from another organization or from DynDNS.

You can configure various hostnames in the domain. You can also specify various subdomains, which can point to the same IP address or different IP addresses.

You can configure Custom DNS using DynDNS's standard or expert interface. The standard interface automatically provides services such as having **www.yourdomain.com** point to the same address as **yourdomain.com**.

Configuring DNS

The extent to which you enable DNS functions on the ProCurve Secure Router depends on whether you want the router to simply be able to run the DNS client or to act as a name server for your organization.

If you only want the router to act as a DNS client, you must:

■ enable DNS (which is enabled by default)

■ specify at least one external DNS server

You can also:

■ add entries for local hosts to the router's host table

If you want the router to act as a name server for hosts in your network, you must:

■ enable DNS (which is enabled by default)

■ specify at least one external DNS server

■ add entries for local hosts to the router's host table

■ enable DNS proxy

Enabling DNS

The ProCurve Secure Router automatically supports DNS. You can turn DNS on and off with the following global configuration mode command:

Syntax: [no] ip domain-lookup

This command enables the DNS client on the router. You can input Web addresses instead of IP addresses for applications such as ping, Telnet, and traceroute, and the router will either translate the names itself using its host table or query its primary DNS server.

In order for the router to translate hostnames for itself, you must add entries for hosts in its domain to its host table.

In order for the router to resolve the names of hosts outside its domain, you must specify the IP address of the DNS server it should query.

The router will only act as a name server for connected hosts if you enable DNS proxy. (See "Enabling the Router to Act as a Name Server" on page 12-10.)

Adding an Entry to the Router's Host Table

DNS distributes the now overwhelmingly vast host table throughout many name servers. Network administrators maintain entries for their own domains, which keeps the table accurate and under control. You manage only the small section of the table on which you are an expert. You should configure the host table on your ProCurve Secure Router only with entries for hosts on its own network.

If the router is acting as a Dynamic Host Configuration Protocol (DHCP) server, the Secure Router OS automatically adds the router's clients to the host table. If the router is acting as an authoritative server for its own network, you should also manually add entries for any devices with a static address that users may need to access such as your organization's Web and email servers. Do not add entries for external hosts or any other host for which the router can get information from other servers.

To add a hostname to the table, enter:

Syntax: ip host *<hostname>* *<A.B.C.D>*

For example:

ProCurve(config)# ip host www 192.168.1.25

A hostname can be any combination of numbers and letters under 256 characters. However, the hostname cannot constitute a valid IP address. Use the **no** form of this command to remove names from the hostname table.

Do not include the domain name for hostnames. Instead, you should specify your organization's domain name as the default name the router uses to resolve hostnames. Enter:

Syntax: ip domain-name *<domain name>*

Do not include the initial period that separates an unresolved name from the domain name. For example:

ProCurve(config)# ip domain-name procurve.com

If you enable DNS proxy, the router can also use the default domain name when forwarding requests. If the external name server cannot resolve a query, the router appends the default domain name to the original query and resends the request.

Specifying DNS Server Addresses

No single DNS server contains the entire host table for every host on the Internet. In order for the Internet to do its job—to allow a host in one location to access a host in any other location—name servers must be able to query each other about the many hosts not in their own tables.

You must specify at least one external name server for the router. This can be a root server, or it can be a DNS server in your organization's WAN that knows how to reach the root server. The router will contact this server:

■ to resolve hostnames for the router (when the router is acting as a DNS client)

■ to resolve hostnames for connected hosts (when the router is running DNS proxy)

To configure the address for the router's DNS server, enter:

Syntax: ip name-server <A.B.C.D> <secondary server A.B.C.D>

You may enter addresses for up to six servers (separate each with a space). The ProCurve Secure Router will first send DNS requests to the first address listed. For example, enter three:

ProCurve(config)# ip name-server 10.1.1.1 10.2.2.2 10.3.3.3

Use the **no** form of the command to remove a server from the list.

Enabling the Router to Act as a Name Server

The router will automatically act as a server for itself (for example, when you ping a device by its hostname) as long as DNS lookup is enabled. To enable the ProCurve Secure Router to act as a name server for connected hosts, enter:

ProCurve(config)# ip domain-proxy

When the ProCurve Secure Router receives a request from a client to translate a hostname, it follows this process:

1. It checks its local host table for a matching entry. (See "Adding an Entry to the Router's Host Table" on page 12-9 to learn how to create this table.) If it finds a match, it sends the IP address stored for the host to the client.

2. If it does not find a match, it forwards the request to an external DNS server. (See "Specifying DNS Server Addresses" on page 12-10.) When the router receives a reply, it forwards it to the client.

3. If the external server cannot resolve the name, the router appends the default domain name (if configured) and resends the request.

Troubleshooting DNS

When the ProCurve Secure Router cannot correctly resolve domain names, you can monitor DNS error messages to pinpoint the source of the problem.

You should be able to interpret DNS messages well enough to track the DNS process and determine where problems arise.

C a u t i o n   Enabling DNS debug messages can seriously compromise the network as the router is forced to debug the many DNS requests arriving from clients.

Before enabling debug messages, you can check for some of the most common problems described in the next section.

You should also determine that all connections are up and that hosts can ping each other. In other words, you should be certain that basic connectivity is not the root of the problem.

Process

First, determine whether the router is acting as a DNS client or a DNS server. Then activate the corresponding debug messages.

The ProCurve Secure Router acts as a DNS server when it:

- receives DNS requests from hosts on its network
- checks its host table for a matching entry
- forwards queries to an external DNS server
- forwards the IP address for a hostname to a DNS client

The ProCurve Secure Router acts as a DNS client when it:

- sends a query to an external name server on its own behalf

Debugging DNS Server Activity

To monitor the router's activity as it receives, forwards, and responds to DNS requests, enter the following enable mode context command:

ProCurve# debug ip dns-proxy

N o t e	You can also start displaying the debug messages from any mode context with the **do** command.

Then, have the DNS client again attempt to access the host. Track the router's activity. It should pass through the steps shown in Table 12-1. Determine where the process breaks down and troubleshoot the problem accordingly.

Table 12-1. DNS Proxy Process

Step	IP.DNS PROXY Messages	Likely Problem If The Message Does Not Appear	Likely Problem If The Message Repeats
1. The router receives a request to translate a hostname.	**Received request from <DNS client>**	DNS proxy is not enabled.	The router cannot resolve the hostname. (See Steps 2, 3, and 5 for possible causes.)
2. If the hostname is in the local host table, the router sends its IP address to the client.	**Serving reply for "<hostname>" from host database: <host A.B.C.D>**	The host table does not include the hostname.	——
3. If the hostname is not in the table, the router queries its own DNS server.	**Forwarding query for "<hostname>" to <DNS A.B.C.D>**	You have not specified at least one external DNS server.	• The external server cannot translate the hostname. • The router cannot reach the external server.
4. If the server can translate the name, the router forwards the response to the client.	• **Received response from server** • **Transmitting response to <DNS client>**	• The external server cannot translate the hostname. • The router cannot reach the external server.	——
5. If the server cannot translate the name, the router appends the default domain name to the request and resends it.	**Forwarding query for "<hostname>.<default domain name>" to <DNS server A.B.C.D>**	You have not configured a default domain name.	• The external server cannot translate the hostname. • The router cannot reach the external server.
6. If the server can translate the name, the router forwards the response to the client.	• **Received response from server** • **Transmitting response to <DNS client>**	• The external server cannot translate the hostname. • The router cannot reach the external server.	——

Host Table Does Not Include a Hostname. If necessary, add an entry to the host table. You can view the current entries in the running-config. Look for a miskeyed entry. Delete the faulty entry from the host table before adding the correct entry. (It is very easy to edit an entry in the Web browser interface; see *Chapter 14: Using the Web Browser Interface for Basic Configuration Tasks.*)

Often, however, the local host table does not contain the entry for a host because it *should* not. The router only should have local hostnames in its host table. The router should be able to communicate with external name servers to receive IP addresses for hosts outside its own domain.

No External DNS Server. If the debug messages indicate that the router is not forwarding queries, you should specify an IP address for at least one DNS server. (See "Specifying DNS Server Addresses" on page 12-10.)

Forwarding Debug Message Repeats. If, on the other hand, you continually receive the **Forwarding query...** message, the router either cannot reach the DNS server or the server cannot translate the hostname.

If the server cannot translate the name, there is little you can do beyond adding another DNS server in hopes that it will provide better service. It is also quite possible that the hostname is invalid.

If the server consistently fails to translate hostnames, you should remove it from the system by entering **no ip name-server** *<server A.B.C.D>*. (Find the address in the running-config.)

However, before writing hostnames and servers off, you should determine that the router is actually reaching the server. Verify that the connection is up and attempt to ping the server. (Tips for bringing up an interface can be found in *Chapter 3: Configuring Ethernet Interfaces*, *Chapter 4: Configuring E1 and T1 Interfaces*, *Chapter 5: Configuring Serial Interfaces for E1- and T1-Carrier Lines*, *Chapter 6: Configuring the Data Link Layer Protocol for E1, T1, and Serial Interfaces*, and *Chapter 7: ADSL WAN Connections*.) If the router cannot reach the server, verify that it knows a route to the server's subnet (enter **show ip route**). You can learn how to add a static route and troubleshoot routing protocols in *Chapter 11: IP Routing—Configuring Static Routes*.

No Default Domain Name. Also, check that the router is appending a default domain name to resent queries and that this domain name is correct. See "Adding an Entry to the Router's Host Table" on page 12-9 to learn how to configure the default domain name.

Debugging DNS Client Activity

DNS client activity deals only with the DNS requests the router makes on its own behalf. (The router always checks its own host table first. If it finds a match, no debug messages appear.)

To monitor DNS client messages, move to the enable mode context and enter:

ProCurve# debug ip dns-client

Real-time debug messages tracking the ProCurve Secure Router's DNS client activity will display. For example, if you try to ping a hostname that the ProCurve Secure Router cannot find in its hostname table, the following message appears:

DNS: CLIENT Transmitting query packet for <*hostname*>

If this message does not appear, then you have not specified an IP address for the external server and should do so. (See "Specifying DNS Server Addresses" on page 12-10.)

The command line interface (CLI) should next display this message:

DNS: CLIENT Received query response

If you do not receive this message, the external DNS server cannot resolve the hostname. It is possible that the hostname is not valid. It is also possible that the DNS server address has been miskeyed and is not that of a valid name server. Find the address the router is contacting in the running-config (enter **show running-config** and look for **ip name-server <A.B.C.D>**).

Before deleting the address and entering a new one, ping the server and verify that the router can reach it. If the server does not reply, the server may be down or the router's connection to the server may be down. The Stat LED for the interface through which the router reaches the DNS server should be green. See *Chapter 3: Configuring Ethernet Interfaces*, *Chapter 4: Configuring E1 and T1 Interfaces*, *Chapter 5: Configuring Serial Interfaces for E1- and T1-Carrier Lines*, *Chapter 6: Configuring the Data Link Layer Protocol for E1, T1, and Serial Interfaces*, and *Chapter 7: ADSL WAN Connections* for tips on troubleshooting a connection.

Also verify that the route table includes a route to the server's subnet. See *Chapter 11: IP Routing—Configuring Static Routes* for more information about the route table.

If the interface can reach the server, but the server consistently fails to translate hostnames, you should remove the server. If necessary, specify a new one. You can specify up to six DNS servers.

Configuring Dynamic DNS

When an interface has a dynamic IP address—for example, when your ISP provides its address—you should register its hostname with a dynamic DNS service provider. Dynamic DNS keeps track of the static hostname and ensures that, even when the associated device's IP address changes, the hostname resolves to the correct address.

The ProCurve Secure Router supports a client that is compatible with Dynamic Networking Services, Inc., or DynDNS.

The dynamic DNS client on the ProCurve Secure Router can request one of these three levels of service:

- Dynamic DNS^{SM}
- Static DNS^{SM}
- Custom DNS^{SM}

Dynamic DNS and Static DNS are currently free services. Dynamic DNS allows you to map a dynamic address to a static hostname in one of 68 domains. Static DNS provides much the same services, but for devices whose IP addresses rarely change. DynDNS provides both these services for up to five hostnames.

You can purchase Custom DNS for a complete DNS solution. Custom DNS grants you control over an entire domain name: either one that you purchase from DynDNS or one that you have already purchased from another organization. You can also configure subdomains and map them to the same IP address or different IP addresses.

You should visit **www.dyndns.org** for more information about these services.

The following router interfaces can register for dynamic DNS services:

- Ethernet interfaces
- Ethernet subinterfaces (VLAN interfaces)
- Point-to-Point Protocol (PPP) interfaces
- High-level Data Link Control (HDLC) interfaces
- Frame Relay subinterfaces
- Asynchronous Transfer Mode (ATM) subinterfaces

You must complete three steps to configure a DynDNS service for a router interface:

1. Open an account with DynDNS.

2. Configure the logical interface's IP address.

3. Activate the dynamic DNS client.

Opening an Account with DynDNS

You should first register with DynDNS for a hostname. Visit the Web site at **www.dyndns.org** and create an account. Select either the **static** or **dynamic** option. DynDNS will guide you through the process of selecting a domain from the 68 that it supports.

If you select the custom service, you can lease your own domain name.

Note	DynDNS allows you to map a wildcard hostname to the address. You should use this option, for example, to allow users to access the same device by entering **yourdomain.com** or **www.yourdomain.com**.

Configuring the Interface's IP Address

On the ProCurve Secure Router, move to the configuration mode context for the interface whose IP address you want to map to the static hostname.

The interface must have an IP address to run the dynamic DNS client. If you have not already done so, configure the IP address.

Setting a Dynamic Address

When using Dynamic DNS, this address is generally a dynamic address—for example, one obtained using DHCP. Interfaces using Custom DNS can also have a dynamic address.

Enter:

Syntax: ip address dhcp [hostname <word> | no-default-route | no-domain-name | no-nameservers]

When you activate the DHCP client on an interface, you can optionally enter a hostname for the interface, which your ISP may advertise to its DNS servers. You can request that your ISP accept the hostname that you will register with DynDNS. You would then enter that hostname for the **hostname** option. See *Chapter 13: Dynamic Host Configuration Protocol (DHCP)* for more information on configuring a DHCP client.

You can configure a PPP interface to take a dynamic address from a service provider with this interface configuration mode command:

Syntax: ip address negotiated [no-default]

See *Chapter 6: Configuring the Data Link Layer Protocol for E1, T1, and Serial Interfaces* for more information on configuring IP addresses for logical interfaces.

Specifying a Static Address

If you selected the Static DNS service, you should assign the interface a static address. An interface that uses Custom DNS can also have a static address, if you so choose.

From the Ethernet or logical interface configuration mode context, enter:

Syntax: ip address <*A.B.C.D*> <*subnet mask | /prefix length*>

See *Chapter 6: Configuring the Data Link Layer Protocol for E1, T1, and Serial Interfaces* for more information on configuring IP addresses for logical interfaces.

Activating the Dynamic DNS Client

You should now activate the client that automatically updates DynDNS when the interface's dynamic IP address changes. Use this command, entered from the interface configuration mode context:

Syntax: dynamic-dns [dyndns | dyndns-custom | dyndns-static] <*hostname*> <*username*> <*password*>

Select the **dyndns** option for the Dynamic DNS service, the **dyndns-static** option for the Static DNS service, and the **dyndns-custom** option for Custom DNS. Enter the hostname you have selected for the router interface. Then enter the username and password that you established when creating your DynDNS account.

For example:

ProCurve(config-atm 1.1)# dynamic-dns dyndns procurve admin secret

Special Considerations for Configuring Custom DNS

Custom DNS expands the services provided by Dynamic and Static DNS. For example:

■ You control your own domain name, which you may already possess or which you may purchase from DynDNS.

■ You can turn your hostname into a subdomain, which is handled by your own DNS servers.

■ You can customize the TTL for hostnames, depending on whether the device has a static, pseudo-static, or dynamic IP address.

When you open your account, the DynDNS standard interface will guide you through setting up these services. (Experienced users can use the expert interface.)

N o t e   If you purchased your domain name from a different organization, you must tell that organization to use DynDNS's DNS servers to resolve hostnames in your domain. DynDNS will instruct you how to do so.

Quick Start

This section provides the commands you must enter to quickly configure the ProCurve Secure Router to act as:

■ a DNS client

■ a proxy name server

It also shows you how to configure a router interface to run a client that updates a dynamic DNS service when the interface's IP address changes.

Only minimal explanation is provided. If you need additional information about any of these options, check "Contents" on page 12-1 to locate the section that contains the explanation you need.

Configuring the ProCurve Secure Router as a DNS Client

1. The router automatically acts as a DNS client. If this function has been turned off, you can re-enable it from the global configuration mode context.

    Syntax: ip domain-lookup

2. Specify IP address(es) for the router's name server(s) from the global configuration mode context.

    Syntax: ip name-server <*A.B.C.D*> <*secondary A.B.C.D*>

    You can enter up to six name servers.

3. If so desired, add entries for devices on the network to the local host table. Enter this command from the global configuration mode context:

    Syntax: ip host <*hostname*> <*A.B.C.D*>

    For example:

    ProCurve(config)# ip host www 192.168.3.25

4. Configure a default domain name for the router.

    Syntax: ip domain-name <*domain name*>

    For example:

    ProCurve(config)# ip domain-name procurve.com

Configuring the ProCurve Secure Router as a Name Server

1. Enable DNS proxy from the global configuration mode context:

    Syntax: ip domain-proxy

2. Add entries for static devices on the network to the local host table.

    Syntax: ip host <*hostname*> <*A.B.C.D*>

    For example:

    ProCurve(config)# ip host www 192.168.3.25

3. Configure a default domain name for the router.

    Syntax: ip domain-name <*domain name*>

    For example:

    ProCurve(config)# ip domain-name procurve.com

4. Specify IP address(es) for the DNS server(s) to which the router should forward requests it cannot translate.

    Syntax: ip name-server <*A.B.C.D*> <*secondary A.B.C.D*>

    You can specify up to six DNS servers.

Configuring a Dynamic DNS Client on a ProCurve Secure Router Interface

These interfaces can run the Dynamic DNS client:

■   Ethernet interfaces

■   Ethernet subinterfaces (VLAN interfaces)

■   PPP interfaces

■   HDLC interfaces

■   Frame Relay subinterfaces

■   ATM subinterfaces

1. From the global configuration mode context, move to the correct interface configuration mode context.

    Syntax: interface <*interface ID*>

    For example:

    ProCurve(config)# interface atm 1.1

2. If you have not already done so, configure the interface's IP address:

   a. To configure a dynamic IP address for an Ethernet interface, Frame Relay subinterface, or ATM subinterface, enter:

      Syntax: ip address dhcp [hostname <*word*> | no-default-route | no-domain-name | no-nameservers]

   b. To configure a dynamic IP address for a PPP interface, enter:

      Syntax: ip address negotiated [no-default]

   c. To configure a static address, enter:

      Syntax: ip address <*A.B.C.D*> <*subnet mask* | /*prefix length*>

3. Activate the dynamic DNS client.

   Syntax: dynamic-dns [dyndns | dyndns-custom | dyndns-static] <*hostname*> <*username*> <*password*>

   Select **dyndns** if you have registered for Dynamic DNS, **dyndns-custom** if you have registered for Custom DNS, and **dyndns-static** if you have registered for Static DNS.

   Enter the interface's hostname. Enter the username and password for your account with DynDNS.

   For example:

   ProCurve(config-atm 1.1)# dynamic-dns dyndns-custom procurve admin secret