8 IP Control

Introduction

This chapter describes the technologies used by the IP Control feature to manage IP (Internet Protocol) address allocations through the OmniSwitch, OmniS/R and OmniStack. Setup and configuration instructions required to implement the switch-enabled IP Control feature are also provided in this chapter, in addition to the required User Interface switch settings. The following is a brief overview of IP Control.

IP addresses can be easily managed with IP Control through the combined use of three integrated technologies:

LDAP (Lightweight Directory Access Protocol) client software

DHCP (Dynamic Host Configuration Protocol) server

DNS (Domain Name System) server

Embedding DHCP and DNS servers allows IP address management functions to be provided on the same platforms used to provide network connectivity. This lowers the cost of being able to deploy and manage these services in the network. The use of an LDAP-enabled directory server to store configuration information, DHCP leases, and DNS records allows network information to be stored on the directory servers being used to manage other aspects of the user population and network. Directory servers can function as a single point of administration for the enterprise.

The server and host configuration data stored on directory servers is initially retrieved by the DHCP and DNS servers via the LDAP client when the switch is booted. The LDAP client is also used by DHCP servers to create or update DHCP and DNS records on directory servers, and by DNS servers to retrieve current host records. Host computers can obtain their configurations from DHCP servers upon request providing the configuration data delivered to the servers is accurate.

LDAP uses TCP/IP as its transport protocol (as does most of the internet) which broadens its usability, while allowing it to quickly and reliably deliver the necessary data to the servers. See *LDAP (Lightweight Directory Access Protocol)* on page 8-16 for a detailed discussion of LDAP operations.

The IP Control feature includes a web-based IP Control management application that runs on HTTP (Hypertext Transport Protocol) web servers. Standard web browsers can be used remotely from anywhere in the network to configure DHCP and DNS servers, enable LDAP operations, and manage the allocation of network IP addresses.

How IP Control Works

When the DHCP server on the switch is initialized, it retrieves its configuration data from the directory server using the LDAP client in the switch software. This data contains the range of addresses in which the server is assigning addresses, the time length of the leases, host configuration information (templates), and any static address mappings. The DHCP server is now ready to begin processing DHCP requests from client stations on the network.

When the DHCP server receives a request for an address assignment from a host computer on the network it first determines the subnet of the requesting host. If the server is providing addresses for the host along with specific configuration information for the host subnet, it finds an available address and offers it to the host along with specific information for the host such as subnet mask, router address, and DNS server address.

If the address offer is accepted by the host, the DHCP server connects to the directory server to create (or update) the lease record stored there. This information is also retained locally in the switch. The DHCP server also updates the DNS record associated with the computer's host name.

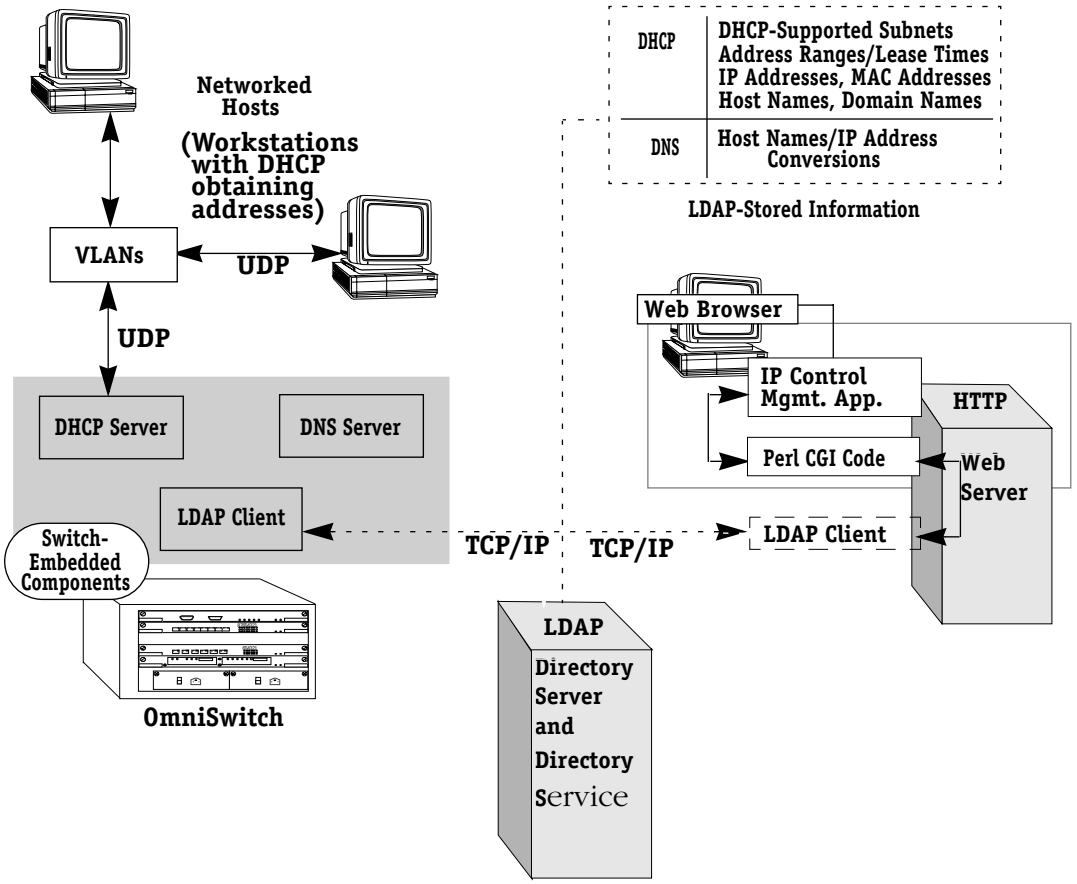
Once it receives the configuration information, the DHCP server does not need to contact the directory server each time in order to assign addresses; however, if the DHCP server is unable to update the information on the directory server, the management application may display an inaccurate view of the lease records (see *System Time Configuration for IP Control* on page 8-14.)

When the DNS server is initialized it reads its configuration information from the directory server. The configuration information defines the network domain zones, or portions of the domain name space the server is supporting, and whether it is the primary or secondary server. The records for the Domain Name server, which translates domain names, remain on the directory server. When the DNS server receives a name resolution query from a host on the network, the DNS server first determines if the request is for the domain for which the DNS server is responsible.

If so, it contacts an accessible LDAP–enabled directory server and retrieves the current records for the associated host name and sends a response to the host. If the request is for another domain, the Name server begins the work to determine the correct server of the domain. Once the correct server from the domain has been determined, the DNS server obtains the necessary information, and returns the result to the host. The information is cached in local memory of the switch so the DNS server can respond directly if another host computer or workstation in its domain requests the IP address of the same host.

The IP Control management application can be used at anytime to reconfigure the components of the IP Control feature as needed.

The general manner in which DHCP, DNS, and LDAP communicate is shown below. (For a more detailed illustration on LDAP, see *LDAP Operations* on page 8-20).



How DHCP, DNS and Directory Servers Communicate

What is Communicated

Information that is processed exclusively by the DHCP server, but stored in the directory server, is described below. This is the configuration data obtained by the DHCP server when it initializes or updates its configuration.

- Subnets supported by the DHCP server.
- Address ranges and lease times (grants and expirations) used by DHCP when assigning addresses to hosts.
- IP Addresses (static and dynamic) assigned by DHCP in the correct VLAN.
- Information to be returned in DHCP messages by DHCP servers (subnet mask, IP router address, DNS server address, domain name).

The information that is processed exclusively by the DNS server, but stored in the directory server is described below. This is the configuration data obtained by the DNS server when it initializes or updates its configuration.

- Domain information
- Location of primary or secondary DNS server.
- Name Server Records
- DNS Options

Components of the IP Control Feature

The IP Control feature requires the following standard and third–party components:

Components of the IP Control Feature

Components	Description
IP Control Components	•Embedded DHCP Server •Embedded DNS/DDNS Server To support Dynamic DNS (DDNS), the DHCP and DNS servers must be enabled and use the same directory server. The DHCP, DNS/DDNS software is part of the dynamically loadable IP Control Software module (**ipcntrl.img**). The DHCP and DNS servers must be able to contact LDAP–enabled directory servers using the switch-enabled LDAP client, or they will not operate; however, the DHCP and DNS servers can operate independent of each other. **• IP Control Management Application** This program is supported on Solaris (UNIX) and Windows NT 4.0. The application install package includes the Apache web server, the necessary PERL code, and the LDAP v3 client software. Note: Apache is a web server that is part of an ongoing group effort to develop and maintain an open source HTTP server that is secure, extensible and complies with current HTTP standards. To find out more about the Apache project, go to http://www.apache.org. Perl (Practical Extension and Report Language), a text-processing programming language by Larry Wall (lwall@netlabs.com), is also part of an integration project with Apache. Perl is frequently used for writing CGI (Common Gateway Interface) scripts that transfer information between HTTP servers and CGI programs.
Third–party Components	•**LDAP–enabled Directory Server** *(primary and secondary servers recommended)* Servers must be networked, fully operational, and have necessary schema extensions installed before using the IP Control feature. •Web Browser Web browsers used to access IP Control management application must be frames–capable, e.g., Netscape Navigator 3.0 (or higher). (Internet Explorer not recommended). •Web Server An HTTP server with Perl 5.004 (or higher) is required. The distribution package contains Apache web server (see above), but other web servers may be used.

IP Control Component Setup

Components required to implement the IP Control feature as described above, must be set up and configured in addition to setting the UI commands for the DHCP and DNS servers that enable LDAP operations through the switch (see *User Interface (UI) Commands* on page 8-12). For more details on IP Control components, see *Component Descriptions* on page 8-15.

The distribution CD for IP Control contains the following:

- IP Control web management install package for Windows NT 4.0 and Solaris (UNIX) which includes the Apache Web server (with Perl libraries), web server installation notes, and IP Control install considerations relating to other products. IP Control can be used with various directory servers.
- Schema extension files for directory servers. (For the University of Michigan slapd server and many other servers these are the configuration (**.conf**) files containing the object classes and attributes and the **.ldif** file used to populate the directory server database, as referenced in the steps below.

IP Control and the switch image file (**ipcntrl.img**) may be purchased with the switch or sold separately.

Pre-Installation Hardware Considerations

IP Control can be used with other directory and web servers, but the most common configurations are likely to use the components provided in the install package. As a result, instructions for installing IP Control on a single machine have been provided below, and are somewhat general to be representative of other installations. Before installing IP Control on an any machine, the following hardware considerations should be taken into account.

- IP Control and the directory server may be installed together on one machine, or separately on two machines. If the plan is to use IP Control on a single machine, it must be installed on an NT 4.0 server with at least Service Pack 3, or Solaris 2.5 (or later), as a prerequisite for the IP Control web management application.

IP Control Installation

These instructions address the minimum installation requirements to render the IP Control feature operational in most configurations, **and are geared toward setting up the switch to use IP Control on an NT 4.0 server using Netscape directory server 4.0, as an example**. Please note that this does not imply in any way an endorsement of Netscape's directory server or Microsoft Windows NT. The instructions should be modified accordingly to match the server operating system, web server, and directory server being used to support IP Control. The following procedures should be performed in the order presented.

- Configure the switch for IP Control and set the switch time.
- Install the directory server on the machine running NT 4.0 server.
- Install the IP Control web management application (which optionally installs the Apache web server) from the distribution CD to the NT 4.0 server.
- Copy the contents of IP Control schema extension (.conf) files from the distribution CD to the directory server.
- Copy the IP Control DHCP and DNS database file (.ldif) from the distribution CD to the directory server, then modify and import the file to the directory server.
- Configure the embedded DHCP and DNS servers using the IP Control web management application after the application is installed on the NT 4.0 server.

Configure the Switch for IP Control and Set the Switch Time

1. Confirm the **ipcntrl.img** file for IP Control is on the FLASH directory (use the **ls** command at the switch prompt to get a list of files on the switch) If the **ipcntrl.img** file is not in the list that displays, contact sales to place an order for IP Control.

Note

The DHCP and DNS servers load automatically if the **ipcntrl.img** file is on the FLASH directory. Do not enable servers until IP Control installation is complete.

2. Set the *User Interface (UI) Commands* on page 8-12 to enable LDAP operations through the switch for the DHCP and DNS servers, and to set the system time in the switch for IP Control.

   Switch settings must be entered in addition to enabling LDAP operations for the DHCP and DNS servers in the IP Control management application.

Note

Some settings between the switch, the directory server, and the IP Control management application must match for IP Control to work. Keep the settings readily available for reference purposes as each IP Control component is installed.

Install the Directory Server

1. Set up an NT 4.0 server (NTFS partition) with at least Service Pack 3 using the vendor-supplied instructions.

2. Install a frames-capable web browser on the NT 4.0 server, such as Netscape Navigator 3.0. (Internet Explorer not recommended.)

3. Load the Netcape Directory server software (for LDAP operations) onto the NT server, and then create the directory server using the vendor-supplied instructions (4.0 or higher recommended). During the installation, take special consideration of the following:

   - The same port number, e.g., 389 (the default for TCP/IP LDAP), must be used in the switch UI (item 3 of the **ipcntrl** menu), the directory server and the web server.
   - The same password (recommended), e.g., secret88, should be used in the switch UI (item 5 of the **ipcntrl** menu) for the directory server, IP Control web management application, and the associated .ldif file in use.
   - The same bind name, e.g., **cn=manager**, must be used in the switch UI (item 4 of the **ipcntrl** menu), the **xylan.ldif** file, the directory server, and IP Control web management application.
   - The same base suffix, .e.g, **o=company**, must be used in the switch UI (item 6 of the **ipcntrl** menu), the **xylan.ldif** file, the directory server, and the IP Control web management application.

Note

Important! Do not use the default setting "enabled" for Schema Checking when installing the directory server. The Schema Checking setting must be changed to "disabled."

Install the IP Control Management Application and Web Server

1. Load the IP Control management application and web server from the distribution CD onto the NT 4.0 server.
   - Before installing the web server, review the Install notes in the IP Control directory (or folder) created by the IP Control management application when loading the software.
   - During the installation of the IP Control management application, select the option to install the Apache web server when prompted.
2. Test the IP Control management application and web server by entering the following information in the URL command line of the web browser:

   http://nnn.nnn.nnn.nnn:80/ipcontrol/index.html

   where nnn... is the IP address of the web server,

   80 is the port number of the web server,

   ipcontrol is the discretionary name of the home directory specified when the web management application is installed,

   and index.html is the home page of the IP Control management application on the web server.

   If the IP Control management application and web server were installed properly, the IP Control management application will display on the screen.

Copy IP Control Schema Extension (.conf) Files to the Directory Server

Extend the directory server schema on the directory server as follows:

Copy the contents of the IP Control object class and attribute schema extension configuration (**.conf**) files from the IP Control distribution CD to the directory server directory (or folder) ***netscape/server4/slapd-server (name identifier)/config*** to replace the same files installed by the directory server:

Object class configuration file: **slapd_user_oc.conf**

Attribute configuration file: **slapd_user_at.conf**

Note

Do not replace the LDAP configuration files currently residing on the directory server if the files have been modified and need to be retained in that form. Instead, using a text editor, cut and paste the IP Control **.conf** files and add them into the existing files.

The object class and attribute configuration files are crucial to the operation of the IP Control feature, and are used either to replace or modify the existing configuration files on the directory server.

Copy and Modify IP Control Database File (Xylan.ldif) to the Directory Server

Copy and then modify the **Xylan.ldif** database file containing DHCP and DNS database information to the directory server as follows:

1. Copy the **Xylan.ldif** file from the IP Control distribution CD to the directory server directory (or folder) ***netscape/server4/slapd-server (name identifier)/ldif*** to replace the same files installed by the directory server, and then modify the file on the server as follows:
   - Using a text editor, modify the **xylan.ldif** file to meet your business needs, making certain that information such as the search base is changed from **o=Alcatel, c=US,** to something that applies to your organization. (These values must be changed to the values entered for the base suffix when the directory server was created.)
   - Save the modified file on the directory server using the same name.
2. Start or restart the directory server.

Configure the Embedded Servers Using the IP Control Management Application

Once the switch-embedded servers are enabled, the switch time and UI commands are set for IP Control, the IP Control management application, web server, and the directory server have been installed on the NT 4.0 server, set up and configure the DHCP and DNS servers using the IP Control management application.

For information exclusive to the servers, see *DHCP Configuration* on page 8-24 and *DNS Configuration* on page 8-26.

IP Control setup procedures are performed through the DHCP and DNS menus in the IP Control management application. For a general guideline as to the use and contents of these options, especially for setup purposes, see *IP Control Menu Options* on page 8-10.

1. Start the IP Control web management application by entering the IP Control URL in the command line of the web browser (described above in Step 2 of installing the IP Control web management application). When the application displays, click the **HELP** button in the main menu.
2. Click on S*etup Instructions for DHCP and DDNS/DNS Services* or scroll through the online help file to locate the setup instructions, and then follow the instructions for setup.
   - *As a minimum for DHCP, this will require defining the DHCP service in the DHCP Service Manager, creating Templates, Subnets and Scopes (in that order) as described in the online instructions.*
   - Begin by selecting DHCP from the main menu, and then selecting the Service Manager.

Note

Be sure to select the service and then click the Update button once after all of the required settings for Subnets, Templates, etc., have been entered, and every time thereafter when *any* changes to the service are made, for the changes to take effect.

While configuring the DHCP service in the switch, also refer to the special instructions concerning these particular screen parameters.

DHCP Service Manager (Define)

(*) Address:Enter the IP address of the switch containing the DHCP server.

(*) Identifier:Enter the fully qualified domain name for the directory server storing the DHCP and DNS server records.

(*) DHCP Server Group:Make sure the DHCP server group matches line 7 of the **ipcntrl** UI menu.

(*) LDAP Search Base:Enter the search base that reflects your organizational entry (referenced above in Step 3 for installing the directory server).

(*) LDAP Bind Name:Enter the bind name (referenced above in Step 3 for installing the directory server).

(*) LDAP Server Password:This password must also match the password specified in the **Xylan.ldif** file for the user allowed to modify the DHCP and DNS entries.

DHCP Templates (New)

(*) Subnet Mask:Enter a Subnet Mask to use in the scope.

(*) Router(s):Enter a default router IP address.

Once the minimum Template parameters are entered, click the Create button at the bottom of the screen.

Subnets (No special instructions)

Scopes (New)

Test the DHCP lease assignments by connecting a workstation to an appropriate port in the switch.

Create a scope in the Create Scope window. Select the Subnet and Template created previously and then input the following:

Protocol: Select DHCP

Lease Time: Select Limited to:

As a test, set the leases to last five minutes, and then click the Create button (change these settings later when IP Control is operational; three months is the default setting).

Select the Service from the DHCP Service Manager and then click the Update button.

Once a lease has been obtained, disconnect the workstation from the switch, and click the DHCP View Active Leases screen. Click the View All button and check to see if the lease for the workstation has expired, and that the times shown correspond with the current time on the switch.

If the lease is expired and the times correspond with the switch time, the IP Control feature is functioning properly.

Click on the DHCP Service Manager to confirm the service is running (there are no UI switch commands to indicate this in the **ipcntrl** menu).

IP Control Menu Options

The following information is a general guideline concerning the use and contents of the options contained in the IP Control management application. It is not intended to replace the online help file included with the IP Control management application that provides detailed instructions.

Accessing IP Control Menu Options

To access the menu options in the IP Control management application, click on either the **DHCP** or **DNS** main menu option, and then click on an associated menu option such as *Server Manager*. Click the **New** button in the various windows that display for the options to setup the servers. The exception to this procedure is to click the **Define** button in the DHCP Server Manager option when setting up DHCP servers.

DHCP Menu Options

The DHCP menu consists of these options: *Service Manager, Templates*, *Subnets*, *Scopes* and *Static Addresses*. The options are used to identify and define operational parameters for DHCP servers, and to enable operations with LDAP-enabled directory servers.

Server Manager — Use this option to designate DHCP server IP addresses, enter LDAP settings, and to set functions like Ping Delay, e.g., set Ping Delay to 300 ms. for the default setting, or 0 ms. to disable pinging. This option is also used to start and stop DHCP servers, and to reload (update) their configurations from the directory servers.

Note

LDAP configuration data must match the data entered via the switch UI and the data in the LDIF file used to configure the directory server.

Templates — Use this option to define the configuration data that is returned to DHCP hosts (along with IP address assignments), and to enter parameters for IP Host and Link Layers, TCP, Application and Service parameters, and to extend DHCP functions.

Note

Templates must be created before entering values for subnets, scopes and static addresses, because those elements are attached to the templates.

All subnets must be defined before the scopes and static addresses as those settings apply to all objects defined in the subnet.

Subnets — Use this option to define subnets where the DHCP server is providing addresses.

Scopes — Use this option to designate the range of IP addresses in a particular subnet the DHCP server is authorized to assign, including their associated lease times, host configuration data (templates), and the transmission protocol (DHCP or BootP) to be used.

Static Addresses — Use this option to associate an IP address with a MAC address for static or reserved use, to designate a transmission protocol, subnet, template, and TFTP (Trivial File Transport Protocol) Server Name and Bootfile Name for host configuration file downloads.

DNS Menu Options

The DNS menu consists of these options: *Service Manager, Primary Domains, Delegated Domains, Secondary Domains,* and *Objects.* The options are used to identify and define operational parameters for DNS servers, and to enable operations with LDAP–enabled directory servers.

Server Manager — Use this option to identify DNS servers, and to enter LDAP settings. This option is also used to start and stop DNS servers, and to reload (update) their configurations from directory servers.

Primary Domains — Use this option to define the primary DNS server (the server that actually stores domain records), and its domain zones, the portions of the DNS Name server database for which it is responsible.

Delegated Domains — Use this option to define the delegated DNS server (the server that is delegated responsibility to other DNS servers), and its domain zones.

Secondary Domains — Use this option to define the secondary DNS server (the server used as a backup to the primary DNS server), and its domain zones.

Objects — Use this option to define an object name record (host name to IP address mapping) in the DNS server, and to designate its operating conditions.

DNS Server Options

The DNS server can be configured to support a number of functions. This is done by creating entries in the named.conf.corp file that resides in the /$IPCONTROLhome/WWW/ldap directory.

The entries in the named.conf.corp file are combined with the definitions created by the web management application to form a named.conf file that defines the behavior of the DNS server. For more information, see Appendix B in the IP Control management application online help file.

User Interface (UI) Commands

UI commands must be set through the switch to enable the IP Control feature as follows:

DHCP and DNS Server Configuration for LDAP

System Time Configuration for IP Control

DHCP and DNS Server Configuration

User Interface commands for configuring the DHCP and DNS servers are located in the Networking/IP/ipcntrl configuration menu.

To view the DHCP configuration menu, type **ipcntrl** at any prompt, and then enter the appropriate values. Values shown here are not necessarily the correct values. Items preceded by an asterisk (*) are required. Items 2 through 10 must match similar information entered for DHCP and DNS server configuration through the IP Control management application.

```
DHCP and DNS Server Configuration for LDAP

1.      DHCP Enabled: Yes
       10.*Update Sec. DNS: Yes
       11.*DDNS Enabled: Yes
2.      *Primary LDAP Server: 208.19.33.4
3.      *Primary LDAP Server Port: 389
4.      *LDAP Server Username: cn=manager
5.      *LDAP Server Password: secret88
6.      *LDAP Base Identifier: o=xylan, c=US
7.      *IP Control Group Name: dhcp_group
8.      Secondary LDAP Server: UNSET
9.      Secondary LDAP Server Port: UNSET
```

Note

At initial configuration the UI commands for DHCP, items 1 and 11 will be set to NO; items 2-9 will be set to UNSET.

The menu items (above) are defined as follows:

DHCP Enabled

Enables DHCP server. The default is NO. See *DHCP Server* on page 8-24 for more information. (UDP transports use the default DHCP server port 67.)

*Primary LDAP Server

IP address of primary LDAP–enabled directory server. See *LDAP–Enabled Directory Server* on page 8-16.

*Primary LDAP Server Port

TCP/IP Port number used by DHCP and DNS servers to connect to Primary directory server. Default port number is 389, but server may use other port as defined when directory server was created. (The default SSL port number is 636, although this is not yet supported by the IP Control LDAP client).

*LDAP Server Username

Username used for accessing the DHCP and DNS entries on the LDAP–enabled directory server. This name must be preceded by cn=. The Username is defined with the LDIF file used to create the database in the directory server. The Username must also match the name defined in the directory server **.ldif** file, and the name entered on the switch. See *Directory Entries* on page 8-18 for more information.

*LDAP Server Password

Password for the Username used to access the directory server. It is used when the DHCP and DNS servers bind to the directory server. The Password is originally defined with the LDIF file used to create the database in the directory server.

*LDAP Base Identifier

DN of the DHCP and DNS entries on the directory server established during its configuration to indicate where DHCP and DNS data is stored, where **o=organization**, and **c=country**.

This was defined in the LDIF file used to populate the directory server.

*IP Control Group Name

Name used to identify the specific DHCP and DNS entries on the directory server where information is stored. Group name is used for the **ou= portion** of the DN.

Secondary LDAP Server

IP address of Secondary directory server.

Secondary LDAP Server Port

TCP/IP port number used by DHCP client-server to connect to Secondary server. This number is user–specific.

Update Secondary DNS Server

Enables automated updates from Secondary DNS/DDNS servers to DNS server in the switch.

DDNS Enabled

Determines whether dynamic updates of DNS server are operational. The default is NO.

DNS uses port 53 to allow access to the DNS server. If using Check Point firewall service this port setting should be entered in Check Point to allow access to the DNS server across the firewall. See Chapter 1, *"Authentication Services"*.

System Time Configuration for IP Control

The system time for the switch must be set correctly or the IP Control management application will not display the correct values allotted for lease grants and expirations.

The User Interface command used to configure the system time for the switch is located in the **System** menu.

To view the **System** menu, type **System** at any prompt, and then type **dt**.

Note

All switches running DHCP/DNS servers for IP Control, must set the system time on the switch to **utc** (Universal Time Coordinate) using the **dt** command.

The time should be set to the correct local time and the time zone value should be set to indicate the offset of local time from UTC. Daylight Savings Time (DST) is automatically set with the time zone, but it can be changed manually.

When the time is not set correctly, it will be noticeable in the View Active Leases screen of the IP Control management application, whereby even valid and recently issued leases might appear to be expired.

Please refer to the chapter "Configuring Switch-Wide Parameters" in the switch manual for more information on time configuration using the **System** menu, including commands and valid parameters for the time zone, offset, and DST.

Component Descriptions

The main components of the IP Control feature, namely the IP Control management application, the LDAP client, and the DHCP and DNS servers are described below. For information concerning specific operation of any required third-party components used, please refer to the appropriate vendor-specific documentation.

IP Control Management Application

The IP Control management application resides on the HTTP server, and is used to manage and configure the DHCP and DNS servers used with IP Control, and to enable operations with LDAP–enabled directory servers. Information handled by the IP Control management application is stored on the directory servers. It is recommended that one installation of the IP Control management application support 10,000 or less networked hosts.

The management application can be accessed from a web browser anywhere in the network. The screens are used to set up, modify, delete, and view DHCP and DNS client-server information including the IP and MAC Addresses, Lease Grants and Expirations assigned by DHCP, and the Domain and Object Name IP address associations maintained by DNS. Reports listing Domain Objects and Active Leases can also be generated from this application.

Note

The system time for the DHCP and DNS servers must be set correctly or the IP Control management application will not display the correct values allotted for lease grants and expirations. See *System Time Configuration for IP Control* on page 8-14.

An online help file for the IP Control management application provides specific instructions on using the program to manage and automatically control the allocation and use of IP addresses. The file goes into considerable detail concerning the description, setup, modification, and monitoring of the DHCP and DNS servers as a whole. A brief overview of the program's menus and functions, particularly for set up, is located in the *IP Control Menu Options* on page 8-10.

LDAP (Lightweight Directory Access Protocol)

The following information describes the LDAP Protocol, LDAP client and LDAP–enabled directory servers, and how they enable LDAP to search for, retrieve, and disperse IP address and host information to DHCP and DNS Servers. LDIF (LDAP Data Interchange Format) files and directory entries are also discussed. The LDAP client used in the switch has been developed in accordance with the following RFCs:

RFC2251, Lightweight Directory Access Protocol, v3

RFC2252, Lightweight Directory Access Protocol, v3, Attribute Syntax Definitions

RFC2253, Lightweight Directory Access Protocol, v3, UTF-8 String Representation of Distinguished Names

RFC2254, The String Representation of LDAP Search Filters

RFC2255, The LDAP URL Format

RFC2256, A Summary of the X.500 User Schema for use with LDAPv3.

RFCs (Requests for Comments) are generally available to all on the internet.

LDAP Protocol Description

The LDAP protocol was originally developed by IETF (Internet Engineering Task Force) to define a way to use directory services over TCP/IP, and to simplify the directory access protocol (DAP) defined as part of the OSI (Open Systems Interconnection) effort. Originally, it was a front–end for the X.500 DAP developed under ISO OSI, and has grown into a full–fledged directory protocol. The IETF continues to define enhancements to the LDAP protocol.

The LDAP protocol synchronizes and governs the communications between the LDAP client and the LDAP–enabled directory servers. The protocol also dictates how its databases of information, which are normally stored in hierarchical form, are searched, from the root directory down to distinct entries.

LDAP is a database query application designed to satisfy huge demands for efficient data storage administration by providing effortless retrieval of and fast updates to enterprise–wide, IP–related information held by the directory servers.

In addition, LDAP has its own format that permits LDAP–enabled web browsers to perform directory searches over TCP/IP using this syntax: **ldap//**. See *The LDAP URL* on page 8-22 for more details.

LDAP Client

The LDAP client switch software is included in the MPM image (mpm.img), and its configuration information is stored in the system configuration file (mpm.cnf). It uses the standard LDAP functions, although not all available capabilities are used. The LDAP client contains the synchronous and asynchronous interfaces that permit IP Control servers to connect to and access LDAP-enabled directory servers.

LDAP–Enabled Directory Server

LDAP–enabled directory servers function as online repositories of information for switch features such as IP Control, LDAP Authentication and the Policy Manager. (See Chapter 3, *"LDAP Authentication,"* and Chapter 6 "Policy Manager" for more information on using LDAP specifically with these features.) With IP Control DHCP and DNS servers, for example, active lease information and host name to IP address mappings are stored on the directory servers. These servers allow access to directories of information, and rely on IP addresses and Domain Names to reference and retrieve related information like someone's name and organization, and available company resources in a given enterprise. LDAP–enabled directory services

should provide controls for setting permissions, access, and rights to any content-sensitive data stored in the directories.

LDAP Server Configuration

LDAP–enabled directory servers can be configured to support Replication and Referral services.

- The directory Replication service automatically copies directory data from one directory server to another, i.e., from the Primary (Active or Supplier) server, to the Secondary (Standby or Consumer) server. Only the Supplier server is used to make modifications to the directory.
- The Referral service distributes directory data among different directory servers, whereby a directory server would return a Referral address to the LDAP client, indicating which server to search next if requested information could not be located on that server.

LDAP–enabled directory servers must be configured with the properly defined LDAP schema and correct database suffix, including well–populated data. The LDAP schema is extensible, permitting entry of user–defined schema as needed.

LDAP–enabled directory servers are also able to import and export directory databases using LDIF (LDAP Data Interchange Format).

LDIF (LDAP Data Interchange Format)

LDIF is a data interchange format exclusive to LDAP. It is used mainly to transfer bulk amounts of data to LDAP–enabled directory servers in order to build directories of information, or to modify segments of existing LDAP Directory Information Databases (DIBs). LDIF was initially developed by the University of Michigan to describe directory entries, and was later expanded to show changes to directory entries.

LDIF files consist of records containing a sequence of lines used either to specify multiple directory entries, or changes to multiple entries, but not both. LDIF presents directory entries in a simple text format. As a result, most text editors can be used to create or modify entries in LDIF files. Directory entries can also be added or modified individually using third-party LDAP software and/or server Command Line utilities.

In addition, LDIF files import and export binary data encoded according to the base 64 convention used with MIME (Multipurpose Internet Mail Extensions) to send various media file types, such as jpeg graphics, through Internet electronic mail.

The general structure of information contained in LDIF files is shown in the examples below.

An LDIF file entry used to define an organizational unit would look like this:

```
dn: <distinguished name>
objectClass: top
objectClass: organizationalUnit
ou: <organizational unit name>
<list of optional attributes>
. . .
```

Below are definitions of some LDIF file entries.

dn: <distinguished name>

Defines entry DN (required).

objectClass: top

Defines top object class (at least one is required).

objectClass: organizationalUnit

Defines organizationalUnit object.

(objectClass defines the list of attributes required and allowed in directory server entries.)

ou: <organizationalUnit name>

Defines attribute of organizational unit's name.

<list of attributes>

Defines list of optional entry attributes.

Common Entries

The most common entries included in directories describe people in companies and organizations. The LDIF used to define a person in an organization would appear as such:

```
dn: <distinguished name>
objectClass: top
objectClass: person
objectClass: organizational Person
cn: <common name>
sn: <surname>
<list of optional attributes>
. . .
```

This is how the file would appear with actual data in it.

```
dn: uid=yname, ou=people, o=yourcompany
objectClass: top
objectClass: person
objectClass: organizational Person
cn: your name
sn: last name
givenname: first name
uid: yname
ou:people
description:
<list of optional attributes>
. . .
```

Directory Entries

Directory entries are used to store data in directory servers. LDAP–enabled directory entries contain information about an object (person, place, or thing) in the form of a Distinguished Name (DN) that should be created in compliance with the LDAP protocol naming conventions.

Distinguished names are constructed from Relative Distinguished Names (RDNs), related entries that share no more than one attribute value with a DN. RDNs are the components of DNs, and DNs are string representations of entry names in directory servers.

Distinguished names typically consist of descriptive information about the entries they name, and frequently include the full names of individuals in a network, their email addresses, TCP/IP addresses, with related attributes such as a department name, used to further distinguish the DN. Entries include one or more object classes, and often a number of attributes that are defined by values.

Object classes define all required and optional attributes (a set of object classes is referred to as a "schema"). As a minimum, every entry must include the DN and one defined object class, like the name of an organization. Attributes required by a particular object class must also be defined. Some commonly used attributes that comprise a DN include the following:

Country (c), State or Province (st), Locality (l),
Organization (o), Organization Unit (ou),
and Common Name (cn)

Although each attribute would necessarily have its own values, the attributes syntax determines what kind of values are allowed for a particular attribute, e.g., **(c=US)**, where country is the attribute and **US** is the value. Extra consideration for attribute language codes will be necessary if entries are made in more than one language.

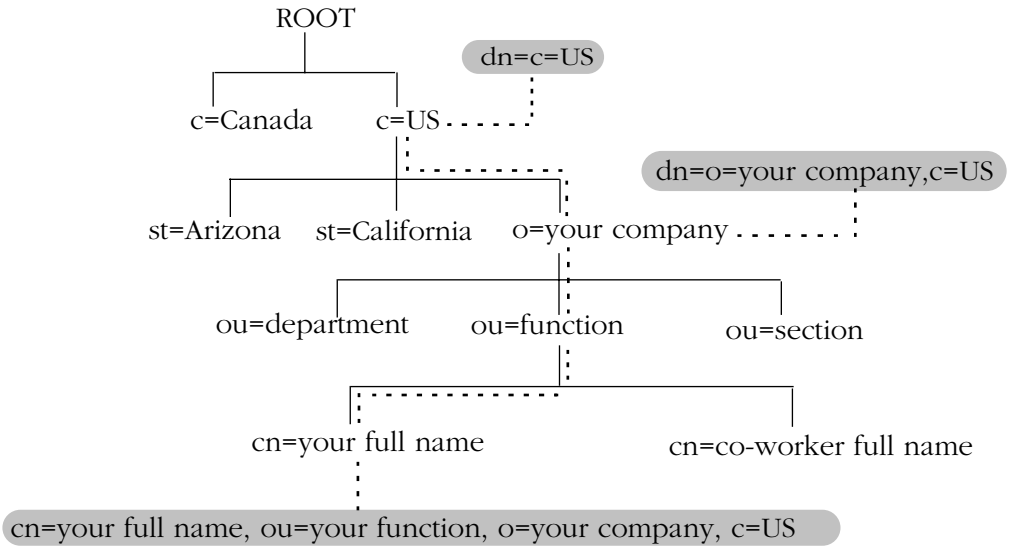
Entries are usually based on physical locations and established policies in a Directory Information Tree (DIT); the DN locates an entry in the hierarchy of the tree. Alias entries pointing to other entries can also be used to circumvent the hierarchy during searches for entries.

Once a directory is set up, DN attributes should thereafter be specified in the same order to keep the directory paths consistent. DN attributes are separated by commas as shown in this example:

cn=your name, ou=your function, o= your company, c=US

As there are other conventions used, please refer to the appropriate RFC specification for further details.

In addition to managing attributes in directory entries, LDAP makes the descriptive information stored in the entries accessible to other applications. The general structure of entries in a directory tree is shown in the following illustration. It also includes example entries at various branches in the tree.

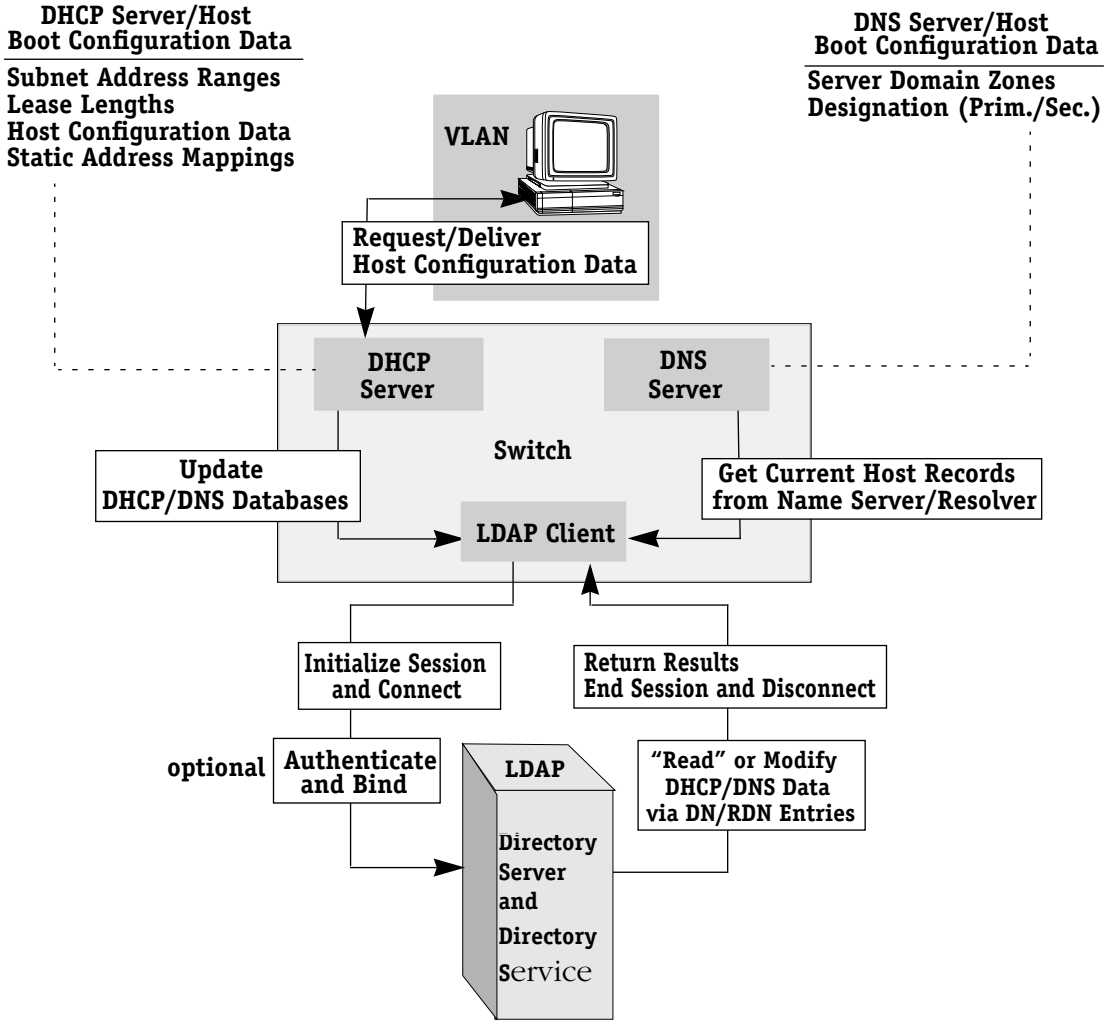


Directory Information Tree

LDAP Operations

The LDAP client library integrated in the switch software contains the routines and function calls that allow LDAP to access directory entries, and to perform most of its operations. LDAP operations include: Bind and Unbind, Search and Modify (includes Add, Delete, Modify RDN), and Abandon.

LDAP's basic operations and interactions with the DHCP and DNS servers in the IP Control feature are shown in the next illustration. The overall process for LDAP sessions begins with requests from the DHCP server to update the DHCP and DNS databases.



How IP Control Uses LDAP

LDAP Sessions

Before the LDAP client in the switch can access and retrieve directory information (which is the object of a search), it must initialize a session, connect and then bind to a directory server as described below, typically via either a simple password–based or Kerberos method of authentication.

Note

The LDAP v3 protocol does not require a bind to the LDAP–enabled directory server before performing any operations unless authentication to the server is desired for directory modification purposes, or a connection is being made to a v2 server. Anonymous binds are also permitted in this version for general directory searches.

Getting the Connection

LDAP client operations are initialized with a directory server when the IP control functions become operational, and the port number is passed to the client (the default port parameter is 389). If successful, a connection handle is returned that points to information about the directory server connection. When any API functions are called to interact with the directory server, connection handles are passed as parameters to the functions to provide context for the connection.

After a session with a directory server is initialized, API functions can be called to set the session handle options to control aspects of the sessions, such as search time limits, and the maximum number of entries that can be returned for a search, or default settings will be used.

The Bind

At this point, the bind and authentication process begins, whereby the LDAP client sends a request to bind to the server. Bind requests must include the LDAP version number being used to accept the request, as well as the session name, and the authentication name and password. The server then issues a Bind response to acknowledge its bind with the client. The LDAP client can then forward the details of the needed service to the directory server, which in turn, will execute the service and provide the needed response.

Error Checking

The error and status checking functions of the application are also called into play to verify proper operation of the service. The LDAP client prints standard LDAP errors messages which list the error code and meaning of the last error that occurred.

Ending the Connection

When no further services are needed, the session is terminated, but can be re-established at anytime if additional requests to bind are issued by the client. To end an LDAP session, the session handler is returned, at which time the LDAP client must unbind and close the connection to the directory server. Memory allocated for the session is then freed.

Once a directory server session has been initialized, and if desired, authenticated, operations such as directory searches, and adding or modifying entries can then be performed; however, this is permissible only when the server controls allow access to these operations.

LDAP–Enabled Directory Searches

LDAP uses the Search function to search directories for specific information, and uses DNs (Distinguished Names) to find the directory entries containing the desired information. DNs are always the starting point for searches unless indicated otherwise in the directory schema.

Searches involve the use of various criteria including scopes and filters which must be predefined, and utility routines, such as Sort. Searches should be limited in scope to specific durations and areas of the directory. Some other parameters used to control LDAP searches include the size of the search, and whether to include attributes associated with name

searches.

Base objects and scopes are specified in the searches, and indicate where to search in the directory. Filters are used to specify entries to select in a given scope. The filters are used to test the existence of object class attributes, and enable LDAP to emulate a “read” of entry listings during the searches. All search preferences are implemented by means of a filter in the search. Filtered searches are based on some component of the DN.

Retrieving Directory Search Results

Results of directory searches are individually delivered to the LDAP client. LDAP referrals to other servers are not returned to the LDAP client, only results or errors. If referrals are issued the server is responsible for them, although the LDAP client will retrieve results of asynchronous operations.

LDAP–Enabled Directory Modifications

Modifications to directory entries contain changes to DN entry attribute values, and are submitted to the server by an LDAP client application. The LDAP–enabled directory server uses the DNs to find the entries to either add or modify their attribute values.

Attributes are automatically created for requests to add values if the attributes are not already contained in the entries.

All attributes are automatically deleted when requests to delete the last value of an attribute are submitted. Attributes can also be deleted by specifying delete value operations without attaching any values.

Modified attribute values are replaced with other given values by submitting replace requests to the server, which then translates and performs the requests.

Directory Compare and Sort

LDAP will compare directory entries with given attribute values to find the information it needs. The Compare function in LDAP uses a DN as the identity of an entry, and searches the directory with the type and value of an attribute. Compare is similar to the Search function, but simpler.

LDAP will also sort entries by their types and attributes. For the Sort function, there are essentially two methods of sorting through directory entries. One is to sort by entries where the DN (Distinguished Name) is the sort key. The other is to sort by attributes with multiple values.

The LDAP URL

LDAP URLs are used to send search requests to directory servers over TCP/IP on the internet, using the protocol prefix: **ldap://**. (Searches over SSL would use the same prefix with an s at the end, i.e., **ldaps://**.)

LDAP URLs are entered in the command line of any web browser, just as HTTP or FTP URLs are entered. When LDAP searches are initiated LDAP checks the validity of the LDAP URLs, parsing the various components contained within the URLs to process the searches. LDAP URLs can specify and implement complex or simple searches of a directory depending on what is submitted in the URLs. Searches performed directly with LDAP URLs are affected by the LDAP session parameters described above.

In the case of multiple directory servers, LDAP URLS are also used for referrals to other directory servers when a particular directory server does not contain any portion of requested IP address information. Search requests generated through LDAP URLs are not authenticated.

Searches are based on entries for attribute data pairs.

The syntax for TCP/IP LDAP URLs is as follows:

ldap://<hostname>:<port>/<base_dn>?attributes>?<scope>?<filter>

e.g., **ldap://ldap.company name.xxx/o=company name%inc./,c=US>** (base search including all attributes/object classes in scope).

LDAP URLs use the percent symbol to represent commas in the DN. The following table shows the basic components of LDAP URLs.

Components of the LDAP URL (Uniform Resource Locator)

Components	Description
<ldap>	Specifies TCP/IP connection for LDAP protocol. (The **<ldaps>** prefix specifies SSL connection for LDAP protocol.)
<hostname>	Host name of directory server or computer, or its IP address (in dotted decimal format.)
<port>	TCP/IP port number for directory server. If using TCP/IP and default port number (389), port number need not be specified in URL. SSL port number for directory server (default no. is 636).
<base_dn>	DN of directory entry where search is initiated.
<attributes>	Attributes to be returned for entry search results. All attributes are returned if search attributes not specified.
<scope>	Different results are retrieved depending on the scopes associated with entry searches: "base" search: retrieves information about distinguished name as specified in URL. This is a **<base_dn>** search. Base searches are assumed when scope not designated. "one" (one-level) search: retrieves information about all entries one level under distinguished name (**<base_dn>**) as specified in URL, excluding base entry. "sub" (subtree) search: retrieves information about entries from all levels under distinguished name (**<base_dn>**) as specified in URL, including base entry.
<filter>	Search filters are applied to entries within specified search scopes. Default filter **objectClass=*** is used when filters are not designated. (Automatic Search Filtering not yet available).

DHCP (Dynamic Host Configuration Protocol) and LDAP

The following information describes the DHCP protocol and DHCP server, and how they work in the IP Control feature. The switch-integrated DHCP server has been developed in accordance with RFCs 2131 and 2132, and is based on technology developed by Quadritek.

DHCP Protocol Description

The DHCP protocol is an extension of the older Bootstrap protocol (BootP) and is used to configure host computers with IP addresses and other configuration parameters upon request, usually at startup (boot-time), through the network.

DHCP differs mainly from BootP in that DHCP allocates IP addresses automatically and temporarily. Addresses assigned using BootP are static and used indefinitely, although BootP can be used to automatically allocate an IP address if an individual MAC address is unknown. Static addresses are typically used for devices such as servers.

The manner in which DHCP and the BootP relay enable host computers to obtain this information is discussed extensively in the "IP Routing" chapter in the switch manual. In the IP Control feature either transmission protocol can be used by selecting it in the IP Control management application in the DHCP Scopes and Static Address menus. See *IP Control Component Setup* on page 8-5 for more details.

Furthermore, through the use of the DNS protocol, the DHCP servers can automatically pass IP address lease assignment information to DNS servers. This allows the networked hosts that are assigned dynamic addresses by DHCP client-servers to be tracked by DNS servers, which can then be located by a name (URL). Dynamic DNS enables DHCP servers to inform DNS servers of dynamically assigned IP addresses and their corresponding computer names.

When the LDAP protocol is added to this DHCP/DDNS pairing, an efficient means of storing and organizing this information is afforded, providing a way to quickly retrieve and update this information from one location.

DHCP Server

The switch-integrated DHCP server is part of the MPM software on the switch. The DHCP protocol runs over UDP.

In the IP Control feature, host computers on IP networks extract their configurations from DHCP servers by issuing requests. DHCP servers then follow through by assigning the hosts either dynamic or static IP addresses. In most cases, dynamic IP addresses will be issued. The DHCP server then updates the LDAP database used by the DNS server with the IP addresses assigned to the hosts. Approximately 20 host leases per second can be assigned by DHCP servers.

All of this configuration information is stored on the directory server in a location specified during server setup. A single DHCP server supports 1000 or less clients. The server operates with DHCP port rules and DHCP/BootP relay functions already in the software.

DHCP Configuration

The IP Control management application enables embedded DHCP servers to be configured and managed from a web browser at any location in the network. Please refer to the online help to obtain information on configuring DHCP client-servers through the IP Control management application.

Note

When hosts are issued IP address leases from DHCP, the address will belong to the first subnet group a host request encounters in the network.

DHCP server configuration requirements for allocating automatic, dynamic or static IP addresses can be set in the IP Control web management application as follows.

Automatic and Dynamic IP address assignments are designated in the DHCP [Edit} Scopes menu option using the Lease Time and Protocol fields:

- Automatic BootP — Allocates address using BootP if the individual MAC address is unknown.

  Lease Time: Unlimited
  Protocol: BootP

- Automatic DHCP — Allocates addresses to a DHCP template with an infinite lease time.

  Lease Time: Unlimited
  Protocol: DHCP

- Dynamic DHCP — Allocates addresses to a DHCP template for a specific lease time.

  Lease Time: Limited to: ...
  Protocol: DHCP

Static IP Address Assignments are designated in the DHCP [Edit} Static Address menu option using the Protocol field:

- Manual DHCP— Allocates addresses using DHCP if the MAC address is defined.

  Protocol: DHCP

- Manual BootP— Allocates addresses using BootP if the MAC address is defined.

  Protocol: BootP

In the standard DHCP configuration, IP address assignments obtained from a pool of addresses (which includes lease information), are by default set to Automatic.

DNS (Domain Name System) and LDAP

The following information describes the DNS Protocol and DNS server, and how they work in the IP Control feature. The switch-integrated DNS/DDNS server has been developed in accordance with RFCs 1034, 1035, 2136, and BIND 8.1.2.

DNS Protocol Description

DNS is a Network Service that provides the mapping between text–based host names and the IP addresses assigned to the hosts. It is a global network of servers that translate host names into numerical IP addresses in dotted decimal format (and the reverse).

DNS is a distributed database that exists on servers throughout the world. DNS is an extension to the BIND (Berkley Internet Name Domain) protocol. DNS BIND 8.1.2 is the implementation component of DNS that allows dynamic DNS updates and IP address–based access control for queries, domain zone transfers and updates. The IP Control feature provides a full function DNS server.

DDNS (Dynamic Domain Name System) allows the dynamic update of a network of DNS servers with DHCP–assigned IP addresses for host computers. As host computers are authenticated and assigned IP addresses, the DNS server in the switch helps ensure hosts remain reachable over the network. To permit dynamic DNS updates, DNS and DHCP servers be enabled simultaneously, and use the same directory server. The DHCP server must also be set to Dynamic through the IP Control management application via the DHCP [Edit] Scopes screen.

DNS Server

The switch-integrated DNS server runs on the MPM in the switch over UDP. DNS servers function as Name servers and Resolvers. When a Name server cannot convert a name into an IP address, the Resolver tries another Name server. For information on configuring Name resolvers in the switch, see the “Network Management” chapter in the switch manual.

The DNS server can be configured as a primary or secondary server. The primary DNS server is the authoritative server for the zone. The secondary server obtains and stores data from the primary DNS server (which it must periodically update via zone transfers), enabling it to function if the primary DNS server fails.

Note

If the general public will be accessing the primary DNS server, it is recommended that an external DNS server be configured as the primary server, and the DNS server in the switch be configured as the secondary server.

DNS Configuration

The IP Control management application enables the embedded DNS server to be configured and managed from a web browser at any location in the network. Please refer to the online help to obtain information on configuring the DNS client-server in the switch through the IP Control management application.

DNS server resource records contain configuration information used by the DNS server to respond to DNS name queries. DNS resource records are stored in LDAP–enabled directory servers in a location specified during server setup.