DHCP Overview

Last Updated: December 3, 2012

The Dynamic Host Configuration Protocol (DHCP) is based on the Bootstrap Protocol (BOOTP), which provides the framework for passing configuration information to hosts on a TCP/IP network. DHCP adds the capability to automatically allocate reusable network addresses and configuration options to Internet hosts. DHCP consists of two components: a protocol for delivering host-specific configuration parameters from a DHCP server to a host and a mechanism for allocating network addresses to hosts. DHCP is built on a client/server model, where designated DHCP server hosts allocate network addresses and deliver configuration parameters to dynamically configured hosts.

This module describes the concepts needed to understand Cisco IOS DHCP.

Information About DHCP

DHCP Overview

Cisco routers running Cisco IOS software include DHCP server and relay agent software. The Cisco IOS DHCP server is a full DHCP server implementation that assigns and manages IP addresses from specified address pools within the router to DHCP clients. These address pools can also be configured to supply additional information to the requesting client such as the IP address of the DNS server, the default router, and other configuration parameters. If the Cisco IOS DHCP server cannot satisfy a DHCP request from its

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

own database, it can forward the request to one or more secondary DHCP servers defined by the network administrator.

DHCP supports three mechanisms for IP address allocation:

- Automatic allocation--DHCP assigns a permanent IP address to a client.
- Dynamic allocation--DHCP assigns an IP address to a client for a limited period of time, which is called a lease (or until the client explicitly relinquishes the address). DHCP also supports on-demand address pools (ODAPs), which is a feature in which pools of IP addresses can be dynamically increased or reduced in size depending on the address utilization level. ODAPs support address assignment for customers using private addresses.
- Manual allocation--The network administrator assigns an IP address to a client and DHCP is used simply to convey the assigned address to the client.

The format of DHCP messages is based on the format of BOOTP messages, which ensures support for BOOTP relay agent functionality and interoperability between BOOTP clients and DHCP servers. BOOTP relay agents eliminate the need for deploying a DHCP server on each physical network segment. BOOTP is explained in RFC 951, Bootstrap Protocol (BOOTP), and RFC 1542, Clarifications and Extensions for the Bootstrap Protocol.

The main advantage of DHCP compared to BOOTP is that DHCP does not require that the DHCP server be configured with all MAC addresses of all clients. DHCP defines a process by which the DHCP server knows the IP subnet in which the DHCP client resides, and it can assign an IP address from a pool of valid IP addresses in that subnet. Most of the other information that DHCP might supply, such as the default router IP address, is the same for all hosts in the subnet, so DHCP servers can usually configure information per subnet rather than per host. This functionality reduces network administration tasks compared to BOOTP.

Benefits of Using Cisco IOS DHCP

The Cisco IOS DHCP implementation offers the following benefits:

- Reduced Internet access costs

Using automatic IP address assignment at each remote site substantially reduces Internet access costs. Static IP addresses are considerably more expensive to purchase than are automatically allocated IP addresses.

- Reduced client configuration tasks and costs

Because DHCP is easy to configure, it minimizes operational overhead and costs associated with device configuration tasks and eases deployment by nontechnical users.

- Centralized management

Because the DHCP server maintains configurations for several subnets, an administrator only needs to update a single, central server when configuration parameters change.

# DHCP Server Relay Agent and Client Operation

DHCP provides a framework for passing configuration information dynamically to hosts on a TCP/IP network. A DHCP client is an Internet host that uses DHCP to obtain configuration parameters such as an IP address.

A DHCP relay agent is any host that forwards DHCP packets between clients and servers. Relay agents are used to forward requests and replies between clients and servers when they are not on the same physical subnet. Relay agent forwarding is distinct from the normal forwarding of an IP router, where IP datagrams

are switched between networks, somewhat transparently. In contrast, relay agents receive DHCP messages and then generate a new DHCP message to send on another interface.

The figure below shows the basic steps that occur when a DHCP client requests an IP address from a DHCP server. The client, Host A, sends a DHCPDISCOVER broadcast message to locate a DHCP server. A relay agent forwards the packets between the DHCP client and server. A DHCP server offers configuration parameters (such as an IP address, a MAC address, a domain name, and a lease for the IP address) to the client in a DHCPOFFER unicast message.

Figure 1   ***DHCP Request for an IP Address from a DHCP Server***
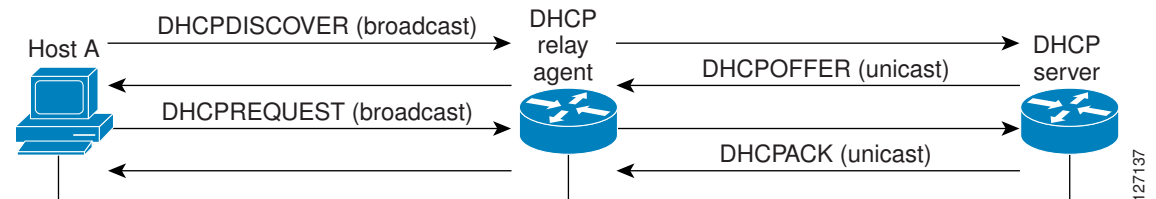
A DHCP client may receive offers from multiple DHCP servers and can accept any one of the offers; however, the client usually accepts the first offer it receives. Additionally, the offer from the DHCP server is not a guarantee that the IP address will be allocated to the client; however, the server usually reserves the address until the client has had a chance to formally request the address.

The client returns a formal request for the offered IP address to the DHCP server in a DHCPREQUEST broadcast message. The DHCP server confirms that the IP address has been allocated to the client by returning a DHCPACK unicast message to the client.

The formal request for the offered IP address (the DHCPREQUEST message) that is sent by the client is broadcast so that all other DHCP servers that received the DHCPDISCOVER broadcast message from the client can reclaim the IP addresses that they offered to the client.

If the configuration parameters sent to the client in the DHCPOFFER unicast message by the DHCP server are invalid (a misconfiguration error exists), the client returns a DHCPDECLINE broadcast message to the DHCP server.

The DHCP server will send a DHCPNAK denial broadcast message to the client, which means that the offered configuration parameters have not been assigned, if an error has occurred during the negotiation of the parameters or the client has been slow in responding to the DHCPOFFER message (the DHCP server assigned the parameters to another client) of the DHCP server.

DHCP Database

DHCP address pools are stored in nonvolatile RAM (NVRAM). There is no limit on the number of address pools. An address binding is the mapping between the client's IP and hardware addresses. The client's IP address can be configured by the administrator (manual address allocation) or assigned from a pool by the DHCP server.

Manual bindings are stored in NVRAM. Manual bindings are just special address pools configured by a network administrator. There is no limit on the number of manual bindings.

Automatic bindings are IP addresses that have been automatically mapped to the MAC addresses of hosts that are found in the DHCP database. Automatic bindings are stored on a remote host called the database agent. A DHCP database agent is any host--for example, an FTP, TFTP, or RCP server--that stores the DHCP bindings database.The bindings are saved as text records for easy maintenance.

You can configure multiple DHCP database agents and the interval between database updates and transfers for each agent.

DHCP Attribute Inheritance

The DHCP server database is organized as a tree. The root of the tree is the address pool for natural networks, branches are subnetwork address pools, and leaves are manual bindings to clients. Subnetworks inherit network parameters and clients inherit subnetwork parameters. Therefore, common parameters, for example the domain name, should be configured at the highest (network or subnetwork) level of the tree.

Inherited parameters can be overridden. For example, if a parameter is defined in both the natural network and a subnetwork, the definition of the subnetwork is used.

Address leases are not inherited. If a lease is not specified for an IP address, by default, the DHCP server assigns a one-day lease for the address.

DHCP Options and Suboptions

Configuration parameters and other control information are carried in tagged data items that are stored in the options field of the DHCP message. Options provide a method of appending additional information. Vendors that want to provide additional information to their client not designed into the protocol can use options.

The Cisco IOS DHCP implementation also allows most DHCP server options to be customized. For example, the TFTP server, which stores the Cisco IOS image, can be customized with option 150 to support intelligent IP phones.

VPNs allow the possibility that two pools in separate networks can have the same address space, with private network addresses, served by the same DHCP server. Cisco IOS software supports VPN-related options and suboptions such as the relay agent information option and VPN identification suboption. A relay agent can recognize these VPN-related options and suboptions and forward the client-originated DHCP packets to a DHCP server. The DHCP server can use this information to assign IP addresses and other parameters, distinguished by a VPN identifier, to help select the VPN to which the client belongs.

For more information on DHCP options and suboptions, see the "DHCP Options" appendix in the *Network Registrar User's Guide* , Release 6.2.

During lease negotiation, the DHCP server sends the options shown in the table below to the client.

Table 1   *Default DHCP Server Options*

DHCP Option Name	DHCP Option Code	Description
Subnet mask option	1	Specifies the client's subnet mask per RFC 950.
Router option	3	Specifies a list of IP addresses for routers on the client's subnet, usually listed in order of preference.
Domain name server option	6	Specifies a list of DNS name servers available to the client, usually listed in order of preference.

DHCP Option Name	DHCP Option Code	Description
Hostname option	12	Specifies the name of the client. The name may or may not be qualified with the local domain name.
Domain name option	15	Specifies the domain name that the client should use when resolving hostnames via the Domain Name System.
NetBIOS over TCP/IP name server option	44	Specifies a list of RFC 1001/1002 NetBIOS name servers listed in order of preference.
NetBIOS over TCP/IP node type option	46	Enables NetBIOS over TCP/IP clients that are configurable to be configured as described in RFC 1001/1002.
IP address lease time option	51	Allows the client to request a lease for the IP address.
DHCP message type option	53	Conveys the type of the DHCP message.
Server identifier option	54	Identifies the IP address of the selected DHCP server.
Renewal (T1) time option	58	Specifies the time interval from address assignment until the client transitions to the renewing state.
Rebinding (T2) time option	59	Specifies the time interval from address assignment until the client transitions to the rebinding state.

The table below lists the option codes that are not used for DHCP pool configuration:

Table 2   *DHCP Server Options--Not Used for DHCP Pool Configuration*

Macro Name	DHCP Option Code
DHCPOPT_PAD	0
DHCPOPT_SUBNET_MASK	1
DHCPOPT_DEFAULT_ROUTER	3
DHCPOPT_DOMAIN_NAME_SERVER	6
DHCPOPT_HOST_NAME	12
DHCPOPT_DOMAIN_NAME	15
DHCPOPT_NETBIOS_NAME_SERVER	44
DHCPOPT_NETBIOS_NODE_TYPE	46

Macro Name	DHCP Option Code
DHCPOPT_REQUESTED_ADDRESS	50
DHCPOPT_LEASE_TIME	51
DHCPOPT_OPTION_OVERLOAD	52
DHCPOPT_MESSAGE_TYPE	53
DHCPOPT_SERVER_IDENTIFIER	54
DHCPOPT_RENEWAL_TIME	58
DHCPOPT_REBINDING_TIME	59
DHCPOPT_CLIENT_IDENTIFIER	61
DHCPOPT_RELAY_INFORMATION	82
DHCPOPT_END	255

DHCP Server On-Demand Address Pool Management Overview

The Cisco IOS DHCP server on-demand address pool (ODAP) manager is used to centralize the management of large pools of addresses and simplify the configuration of large networks. ODAP provides a central management point for the allocation and assignment of IP addresses. When a Cisco IOS router is configured as an ODAP manager, pools of IP addresses are dynamically increased or reduced in size depending on the address utilization level.

ODAPs support address assignment using DHCP for customers using private addresses. Each ODAP is configured and associated with a particular Multiprotocol Label Switching (MPLS) VPN. Cisco IOS software also provides ODAP support for non-MPLS VPN address pools by adding pool name support to the **peer default ip address dhcp-pool** *pool name*command.

DHCP server subnet allocation is a way of offering entire subnets (ranges of addresses) to relay agents so that remote access devices can provision IP addresses to DHCP clients. This functionality can occur along with or instead of managing individual client addresses. Subnet allocation can improve IP address provisioning, aggregation, characterization, and distribution by relying on the DHCP infrastructure to dynamically manage subnets.

This capability allows the DHCP server to be configured with a pool of subnets for lease to ODAP clients. Subnet pools can be configured for global ODAP clients or MPLS VPN ODAP clients on a per-client basis. The DHCP subnet allocation server creates bindings for the subnet leases and stores these leases in the DHCP database.

DHCP Services for Accounting and Security Overview

Cisco IOS software supports several new capabilities that enhance DHCP accounting, reliability, and security in Public Wireless LANs (PWLANs). This functionality can also be used in other network implementations.

DHCP accounting provides authentication, authorization, and accounting (AAA) and Remote Authentication Dial-In User Service (RADIUS) support for DHCP. The AAA and RADIUS support improves security by sending secure START and STOP accounting messages. The configuration of DHCP

accounting adds a layer of security that allows DHCP lease assignment and termination to be triggered for the appropriate RADIUS START and STOP accounting records so that the session state is properly maintained by upstream devices such as a Service Selection Gateway (SSG). This additional security can help to prevent unauthorized clients or hackers from gaining illegal entry to the network by spoofing authorized DHCP leases.

Three other features have been designed and implemented to address the security concerns in PWLANs. The first feature secures ARP table entries to DHCP leases in the DHCP database. The secure ARP functionality prevents IP spoofing by synchronizing the database of the DHCP server with the ARP table to avoid address hijacking. Secure ARP adds an entry to the ARP table for a client when an address is allocated that can be deleted by the DHCP server only when a binding expires.

The second feature is DHCP authorized ARP. This functionality provides a complete solution by addressing the need for DHCP to explicitly know when a user logs out. Before the introduction of DHCP authorized ARP, there was no mechanism to inform the DHCP server if a user had left the system ungracefully, which could result in excessive billing for a customer that had logged out but the system had not detected the log out. To prevent this problem, DHCP authorized ARP sends periodic ARP messages on a per-minute basis to determine if a user is still logged in. Only authorized users can respond to the ARP request. ARP responses from unauthorized users are blocked at the DHCP server providing an extra level of security.

In addition, DHCP authorized ARP disables dynamic ARP learning on an interface. The address mapping can be installed only by the authorized component specified by the **arp authorized** interface configuration command. DHCP is the only authorized component currently allowed to install ARP entries.

The third feature is ARP autologoff, which adds finer control for probing when authorized users log out. The **arp probe interval** command specifies when to start a probe (the timeout), how frequent a peer is probed (the interval), and the maximum number of retries (the count).

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
DHCP commands: complete command syntax, command mode, command history, defaults, usage guidelines, and examples	*Cisco IOS IP Addressing Services Command Reference*
DHCP server configuration	"Configuring the Cisco IOS DHCP Server" module
DHCP relay agent configuration	"Configuring the Cisco IOS DHCP Relay Agent" module
DHCP client configuration	"Configuring the Cisco IOS DHCP Client" module
DHCP server on-demand address pools	"Configuring the DHCP Server On-Demand Address Pool Manager" module
DHCP advanced features	"Configuring DHCP Services for Accounting and Security" module

Related Topic	Document Title
DHCP enhancements for edge-session management	"Configuring DHCP Enhancements for Edge-Session Management" module
DHCP options	"DHCP Options" appendix in the *Network Registrar User's Guide* , Release 6.1.1

Standards

Standard	Title
No new or modified standards are supported.	--

MIBs

MIB	MIBs Link
No new or modified MIBs are supported.	To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
RFC 951	*Bootstrap Protocol (BOOTP)*
RFC 1542	*Clarifications and Extensions for the Bootstrap Protocol*
RFC 2131	*Dynamic Host Configuration Protocol*
RFC 2132	*DHCP Options and BOOTP Vendor Extensions*

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Glossary

address binding --A mapping between the client's IP and hardware (MAC) addresses. The client's IP address may be configured by the administrator (manual address allocation) or assigned from a pool by the DHCP server (automatic address allocation). The binding also contains a lease expiration date. The default for the lease expiration date is one day.

address conflict --A duplication of use of the same IP address by two hosts. During address assignment, DHCP checks for conflicts using ping and gratuitous (ARP). If a conflict is detected, the address is removed from the pool. The address will not be assigned until the administrator resolves the conflict.

address pool --The range of IP addresses assigned by the DHCP server. Address pools are indexed by subnet number.

automatic address allocation --An address assignment method where a network administrator obtains an IP address for a client for a finite period of time or until the client explicitly relinquishes the address. Automatic allocation is particularly useful for assigning an address to a client that will be connected to the network only temporarily or for sharing a limited pool of IP addresses among a group of clients that do not need permanent IP addresses. Automatic allocation may also be a good choice for assigning an IP address to a new client being permanently connected to a network where IP addresses are sufficiently scarce that it is important to reclaim them when old clients are retired.

BOOTP --Bootstrap Protocol. A protocol that provides a method for a booting computer to find out its IP address and the location of the boot file with the rest of its parameters.

client --Any host requesting configuration parameters.

database--A collection of address pools and bindings.

database agent --Any host storing the DHCP bindings database, for example, a Trivial File Transfer Protocol (TFTP) server.

DHCP --Dynamic Host Configuration Protocol. A protocol that provides a mechanism for allocating IP addresses dynamically so that addresses can be reused when hosts no longer need them.

DNS --Domain Name System. A system used in the Internet for translating names of network nodes into addresses.

manual address allocation --An address assignment method that allocates an administratively assigned IP address to a host. Manual allocation allows DHCP to be used to eliminate the error-prone process of manually configuring hosts with IP addresses.

PWLAN --Public Wireless Local Area Network. A type of wireless LAN, often referred to as a hotspot, that anyone having a properly configured computer device can access.

relay agent --A router that forwards DHCP and BOOTP messages between a server and a client on different subnets.

server --Any host providing configuration parameters.

SSG --Service Selection Gateway. The Cisco IOS feature set that provides on-demand service enforcement within the Cisco network.

Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.