6

DHCP APPLICATIONS

The most fundamental application for DHCP is automated address assignment. We take DHCP for granted when we connect to an IP network. This basic function renders IP applications easier to use by automating initialization of the IP layer. End users need not call the help desk to obtain and enter IP addresses into their devices. DHCP not only automates IP address assignments but also enables network administrators to retain control of what IP addresses may be assigned to certain clients, even up to denying access as we'll discuss in Chapter 8. In this chapter, we'll discuss technology applications that rely on DHCP, beyond basic address assignment services. Of course, these applications that rely on DHCP therefore also rely on the DHCP configuration being consistent with the IP address plan!

This chapter highlights those applications requiring special purpose DHCP configurations, including device-specific configuration and broadband provisioning. DHCP-based access control could also be grouped within this topic, but we'll cover that in the context of security in Chapter 8 instead.

The cornerstone in supporting various applications with DHCP is the ability of the DHCP server to classify a device requesting an address and to supply an appropriate IP address and additional configuration information. This classification of clients into *client classes* enables the DHCP administrator to identify a parameter value within a particular

IP Address Management: Principles and Practice, by Timothy Rooney

DHCP packet field or option to match on a per-DHCP transaction basis. When a client is classified, the DHCP server may then determine

- from which IP address pool to assign an address to the client (if any)
- what additional or alternative option parameter values to provide to the client.

Leading DHCP reference implementations from the Internet Systems Consortium (ISC) and Microsoft support both the vendor class identifier (option 60 for IPv4 and 16 for IPv6) and the user class identifier (option 77 for IPv4 and 15 for IPv6) options as class parameters. When these options are included in the Discover or Solicit packet, the server can use this information to identify the type of device that is requesting its configuration.

6.1 MULTIMEDIA DEVICE TYPE SPECIFIC CONFIGURATION

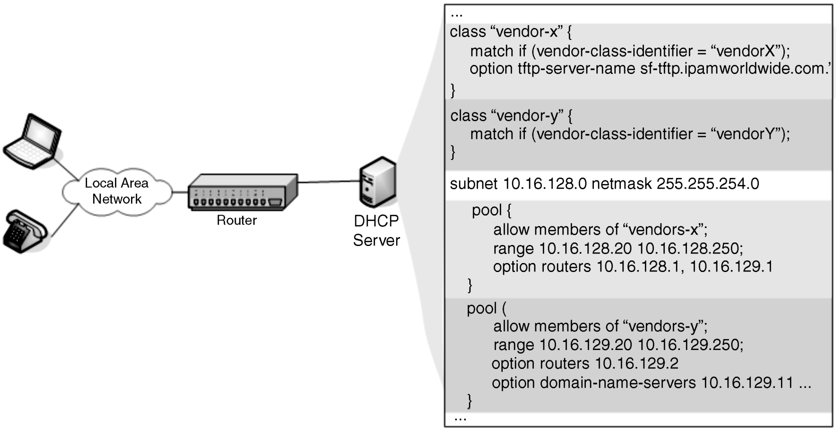
The most common example application we've used so far is that of multimedia device initialization, such as voice over IP (VoIP) devices. In many cases, the multimedia vendor manufacturer encodes a given vendor class identifier option value. Most vendors supply a model number and/or manufacturer name within the vendor class identifier option field. Configuring the DHCP server to recognize this particular value enables the server to supply certain DHCP options required by the client and to assign an IP address from a specific address pool. Other application-specific DHCP clients requiring particular configuration parameters may likewise be identified and configured on the basis of the value of the corresponding vendor class option.

The user class identifier option is another candidate for determining client configuration. However, since user class identifier is typically end-user settable, it is considered less reliable. Should a user outside of the user class group discover the value or setting, he or she could program his or her device accordingly. For example, using Microsoft's ipconfig utility with the/setclassid argument, it's quite easy to set the value of the user class identifier option.

In Chapter 4, we introduced an example VoIP application configuration when discussing the setting up of client classes for IPAM Worldwide's San Francisco office to differentiate VoIP devices by vendor class. Figure 4.5b, reproduced here as Figure 6.1, illustrates a simple example of configuring an ISC DHCP server to identify clients of class "vendor-y" if a DHCP packet contains a vendor class identifier option value of "vendorY." Once classified as a vendor-y device, the client would be issued an address from the 10.16.129.20–10.16.129.250 pool on the subnet with corresponding routers and DNS server options. These option values are specified along with the allowed members of "vendor-y" statement within this pool declaration.

Similarly, devices of class "vendor-x" will be identified by clients supplying a vendor class identifier option value of "vendorX." Such devices will be assigned from the 10.16.128.20–10.16.128.250 pool on the 10.16.128/23 subnet with the routers (and tftp-server-name) option values.

The ISC DHCP server supports filtering on additional class parameters, in fact, up to any packet parameter from MAC address, a subset of the MAC address, or any option



```
...
class “vendor-x” {
    match if (vendor-class-identifier = “vendorX”);
    option tftp-server-name sf-tftp.ipamworldwide.com.’
}
class “vendor-y” {
    match if (vendor-class-identifier = “vendorY”);
}
subnet 10.16.128.0 netmask 255.255.254.0
    pool {
        allow members of “vendors-x”;
        range 10.16.128.20 10.16.128.250;
        option routers 10.16.128.1, 10.16.129.1
    }
   pool (
        allow members of “vendors-y”;
        range 10.16.129.20 10.16.129.250;
        option routers 10.16.129.2
        option domain-name-servers 10.16.129.11 ...
    }
...
```

Figure 6.1. Specifying configuration information for DHCP clients by class (syntax based on Ref. 35).

value. This is convenient if a given MAC address (interface card) or MAC prefix (manufacturer) needs to be filtered and assigned certain parameters.

6.2 BROADBAND SUBSCRIBER PROVISIONING

The cable industry defined a standard for data transmission over cable, referred to as Data Over Cable Service Interface Specifications (DOCSIS®). The DOCSIS specifications, authored by CableLabs, require the use of DHCP for provisioning of customer premises equipment (CPE), such as cable modems and telephony devices. A cable operator that offers cable data or broadband Internet services must deploy DHCP servers to support the CPE provisioning process. Other broadband technologies such as digital subscriber line (DSL) and fiber may also use DHCP or Bootp, though other techniques such as PPP (Point-to-Point Protocol) are also used by these broadband technologies.

The incorporation of DHCP into the provisioning process affords the broadband operator control over IP address assignments and capacity, as well as additional configuration parameters used by CPE for initialization. DHCP can also be used to assign IP addresses from address pools corresponding to various service levels based upon the customer’s subscription. Assigning an address from a given pool requires the network routing infrastructure be configured to route IP packets with such addresses only to certain networks, permit access to certain destinations, and treat packets with corresponding levels of priority and queuing.

Let’s consider an example to illustrate these concepts. In Figure 6.2, three subscribers are connected to a common broadband gateway via the broadband access network. The figure depicts each subscriber with various levels of service as indicated by different shading, connected to individual ports on the broadband gateway. Depending on the broadband access technology, these may be physical ports or logical ports for shared network access.

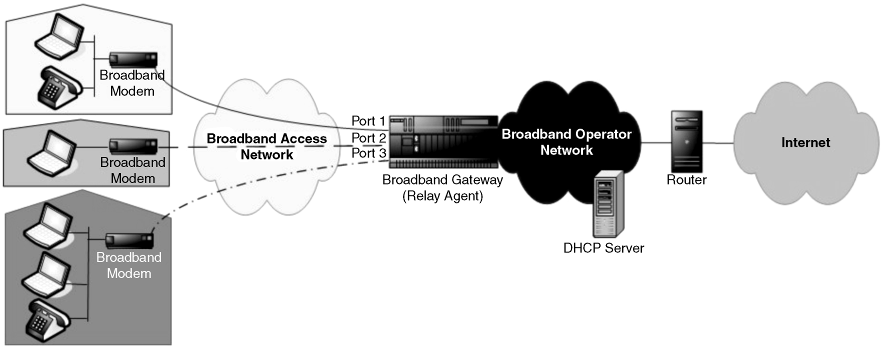


Figure 6.2. Broadband access scenario (11).

Regardless of the broadband access technology, service providers using DHCP need to base address and parameter assignment on known or trusted information. Instead of relying on the client hardware address field of the DHCP packet, which can be spoofed, service providers rely on information from the broadband gateway, which resides in the service provider's network and is considered trustworthy.

The broadband gateway, acting as a DHCP Relay agent, unicasts the DHCP packet to the appropriate DHCP server(s), inserting the GIAddr field within the DHCP packet header. The gateway also inserts the relay agent information option parameter as the last option before the null option terminator. The relay agent information option provides information such as the subscriber device hardware address or subscriber virtual circuit identifier to help the DHCP server identify the subscriber client that issued the DHCPDISCOVER packet.

This enables the DHCP server to provide, on the basis of its configuration, an appropriate number of IP addresses and/or option parameters for a given subscriber. The relay agent information option in IPv4 (option 82) is comprised of one or more suboptions, the following of which have been defined:

Suboption Code	Name	Description	RFC Ref.
1	Circuit ID	Encodes information about the connection to the subscriber. This consists of a virtual circuit identifier corresponding to the subscriber, typically corresponding to a layer 2 identifier such as an ATM virtual circuit ID, frame relay data link connection identifier (DLCI), or remote access server or switch port number	3046 (42)
2	Remote ID	Encodes information about the remote client device such as its Ethernet address, modem identifier, or caller ID for a dial-up connection	3046 (42)

(*Continued*)

Suboption Code	Name	Description	RFC Ref.
3	Reserved	Not used	—
4	DOCSIS device class	Encodes the DOCSIS device class of the cable CPE. This option is applicable to DOCSIS cable access networks and the CMTS (cable edge device) may include this suboption on the basis of this information gathered during the DOCSIS registration process	3256(82)
5	Link selection	Encodes an IP address to be used in lieu of the GIAddr field by the DHCP server when selecting a subnet address for address assignment to the client. This would apply when shared subnets* are in use	3527(83)
6	Subscriber ID	Encodes a subscriber identifier string to associate the DHCPDICSCOVER with the given subscriber's client. This is useful if the subscriber can access the network over various media where use of the circuit identifier or remote identifier would only indicate the underlying access mechanism and not the subscriber association	3993(84)
7	RADIUS attributes	Encodes RADIUS attributes per the RADIUS protocol (RFC 2865) to use by the DHCP server in making parameter assignments. These attributes are encoded as a type length value octet stream and can include the user name, passwords, access server IP/port, and others	4014 (85)
8	Authentication	Encodes authentication information as a means to provide message integrity checking on relay agent information. This encoding is similar to that used for DHCP authentication, which is discussed in Chapter 8	4030 (86)
9	Vendor-specific information	Encoded as one or more sets of vendor-specific information each consisting of a 3-tuple: IANA-registered enterprise number, length, and data	4243 (87)

(*continued*)

(*Continued*)

Suboption Code	Name	Description	RFC Ref.
10	Relay Agent Flags	Extensible suboption to flag conditions; one flag is defined to indicate that the relay agent received the DHCP packet via unicast (1) or broadcast (0)	5010 (88)
11	Server Identifier Override	Instructs the DHCP server to use this specified value in its Server Identifier field in its response to the client; this enables the relay agent to receive DHCPRENEW packets that it may not otherwise have visibility to, enabling the relay agent to insert other relay agent suboption values associated with the client when forwarding the DHCPRENEW packet to the server	5107 (89)

*Shared subnets refers to the provisioning of multiple logical subnets on a single physical subnet (router interface).

Within DHCPv6, two analogous options have been defined:

- Code 37 = Option_remote_id
- Code 38 = Option_subscriber_id

Let's consider an example DHCP server configuration using ISC DHCP syntax (35) to illustrate relay agent processing. This statement declares the class "broadband" that is based on matching the circuit ID suboption of the relay agent identification option. Here, we define a single client class but provision subclasses to identify specific instances of the broadband class. In this case, we simply define two subclasses for two corresponding values of the circuit ID suboption.

```
class "broadband" {

 match option agent.circuit-id;

}

subclass "modem" "45023" {

  [ declarations and parameters for modem devices ]

}

subclass "phone" "67032" {

  [ declarations and parameters for phone devices ]

}
```

A more scalable approach would be to utilize the class-spawning feature of the ISC DHCP implementation. We'll illustrate this along with the ability to limit the number of leases or IP addresses assignable to a subscriber. A basic level of service may promise a single IP address, while a higher level of service (and perhaps price) may include two or more. The `lease limit` statement enables this feature control within the ISC DHCP configuration file. This statement can be associated with a client class definition to specify the maximum number of leases that can be provided to clients matching this class.

Class spawning enables dynamic creation or spawning of client subclasses on the fly based on information in the DHCP packet. The `spawn with` declaration defines a spawning class with the parameter on which to base the spawn. For example, the DHCP server can be configured to spawn client classes based on each unique circuit ID relay agent suboption value. Thus, when a DHCPDISCOVER is received by the DHCP server, it analyzes the circuit ID suboption. If a class exists (was previously spawned) for the given value, the corresponding parameters and declarations are analyzed for processing; if a class with that circuit ID does not exist, the DHCP server spawns a new subclass for the given value. The example below illustrates the definition of a broadband client class with a spawning subclass based on the circuit ID that limits outstanding subscriber leases to a maximum of six using ISC DHCP syntax (35).

```
class "broadband" {

  spawn with option agent.circuit-id;

  lease limit 6;

}
```

6.3 RELATED LEASE ASSIGNMENT OR LIMITATION APPLICATIONS

The use of lease limiting and parameter setting based on relay agent information is not exclusive to broadband environments. Other applications may use the same technique assuming relay agents support the population of the relay agent information option. In such cases, using the ISC DHCP server enables address and parameter assignment as well as lease limiting based on defined classes and relay agent information parameters. This technique may be employed to throttle address assignments on certain subnets or to provide configuration parameters to devices in factory or similar applications.

6.4 PREBOOT EXECUTION ENVIRONMENT CLIENTS

Preboot Execution Environment (PXE or "Pixie") clients are devices that boot up relying on network servers instead of a co-resident hard disk. Such diskless servers and other such devices typically use DHCP to obtain an IP address and boot parameters including boot server addresses and boot file names. DHCP provides a convenient mechanism to initialize these devices without manual intervention. Historically, DHCP servers had to be configured with the MAC address of each PXE client to provide configuration information specific to the device, even if multiple PXE clients of the same "type" could leverage exactly the same boot information.

RFC 4578 (49) is an informational RFC defining a means whereby a PXE client can identify its type or architecture to the server. This information can be used by the DHCP server to identify and provide appropriate device initialization parameters. The DHCP server would need to be configured to match on particular client-provided PXE option values, then map these results to a corresponding set of configuration parameters or options to return to the client. Naturally, this is accomplished using client class processing.

Options to be included between PXE clients and the DHCP server are as follows:

- Option 93—client system architecture type—specifies the architecture type of the PXE device and must be included in all DHCP packets during the transaction
    - Intel x86PC
    - NEC/PC98
    - EFI Itanium
    - DEC Alpha
    - Arc x86
    - Intel Lean Client
    - EFI IA32
    - EFI BC
    - EFI Xscale
    - EFI x86-64
- Option 94—client network interface identifier—identifies the network interface type and version and must be included in all DHCP packets in the transaction. The only defined interface type is for universal network device interface (UNDI).
- Option 97—client machine identifier—identifies the type of machine booting. This option is encoded with a type and identifier. The only defined type, 0, indicates the identifier is encoded as a 16-octet globally unique identifier (GUID).
- Options 128–135—these options are to be requested by PXE clients and are intended for use by downloaded bootstrap programs, if needed, though they are not officially assigned for PXE use.

Be aware that PXE clients using options 128–135 may conflict with the alternative assigned meaning of these options as summarized in Chapter 4.

6.4.1 PPP/RADIUS Environments

The RADIUS (Remote Access Dial In User Service) protocol provides a means to authenticate end users attempting to connect to a network. RADIUS is a vital component of 802.1X, a popular layer 2 media access control protocol proposed within leading network admission control (NAC) offerings. RADIUS also plays a role at layer 3, especially when used in conjunction with PPP connections, commonly used with dial-up or DSL connections.

When operating at layer 3, some RADIUS servers can be configured to assign IP addresses to each client at the other end of the PPP connection. This address assignment process can be performed by configuring an address pool directly on the server or by configuring the RADIUS server to obtain an address via a DHCP server. In the latter scenario, the RADIUS server functions as a DHCP proxy on behalf of the client. The RADIUS server initiates the DHCP D-O-R-A process, issuing a DHCPDISCOVER packet. One caveat with this approach is that the RADIUS server must generate a hardware address or client identifier on behalf of each client to uniquely identify each. Otherwise, by using the RADIUS server's hardware address, the DHCP server would assume that the same client is continually rebooting and assigns the same IP address on all requests! The RADIUS server can spoof the client's hardware address using an internal mechanism but needs to map the derived address to the end client to process subsequent lease transactions like Renews and Releases. An alternative approach is to leverage the RADIUS attributes suboption of the Relay Agent Information option described earlier in order to uniquely identify each client.

6.4.2 Mobile IP

Mobile IP provides a mechanism for an IP device to retain network connectivity while moving about a local or remote IP network. This movement may occur during a communication session, not only when conducting and then terminating a session, for example, from a headquarters meeting to opening a new session at a branch office. The mobile device has a home address, corresponding to its home network, as well as a care-of address, which is obtained on serving network depending on where the mobile device is presently connected. For example, if I power up my personal digital assistant (PDA) device while out of town, I may obtain wireless service from a different service provider from the one I normally use when "at home." As long as my home provider has a service agreement with the provider I'm visiting, I should be able to obtain an address manually, via DHCP, or via autoconfiguration.

IP mobility support differs somewhat between IPv4 and IPv6, but both protocols leverage the concept of a mobile node possessing a home address, the node's address on the "home" network, and a care-of address, its address on the visited network. While not strictly a DHCP "application," we mention it here as an area for consideration with respect to address allocation and assignment strategies, not to mention access security for visiting nodes on your network.