LABORATORY WORK NO. 6

EASY IP: DHCP, NAT

1. Objectives

The aims of this laboratory are: understanding the DHCP lease process, lease renewal and release, understanding DHCP scopes, including address ranges, exclusions, reservations, superscopes, commonly used options, relay agent, understanding NAT, PAT, installing and configuring a DHCP server, configuring a DHCP client to obtain an IP address from a DHCP server and testing the configuration.

2. Theoretical considerations

2.1 DHCP – Dynamic Host Configuration Protocol

2.1.1 Introduction

DHCP is an open and standard-based, as defined by IETF RFCs 2131 and 2132. DHCP can automatically configure a host while it is booting on a TCP/IP network, as well as change settings while the host is attached. This lets all available IP addresses to be stored in a central database along with associated configuration information, such as the subnet mask, gateways and address of DNS Servers.

Together with Domain Name System (DNS), the DHCP serves as a basic foundation for a network infrastructure. In all but the smallest networks, DHCP provides hosts with an IP configuration needed to communicate with other computers on the network. This configuration includes – at a minimum – an IP address and a subnet mask, but it typically also includes a primary domain suffix, a default gateway, preferred and alternate DNS servers, WINS servers (on Windows-based systems), and several other options.

2.1.2 The DHCP Lease Process

The DHCP Service allocates IP addressing information to client computers. The allocation of IP addressing is called a DHCP release. The DHCP lease process occurs when one of the following events occurs:

- TCP/IP is initialized for the first time on a DHCP client;
- a client request specific IP address and is denied;
- a client previously leased an IP address but released the IP address and requires a new one.

DHCP uses a four phase process to lease IP addressing information to a DHCP client for a specific period.

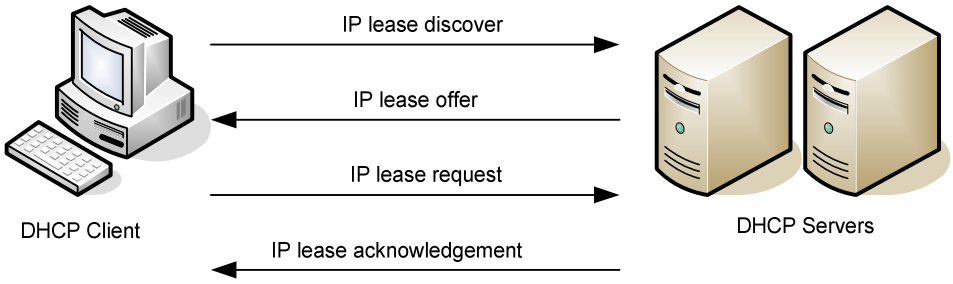

Figure 6.1 *DHCP lease process*

1. IP Lease Discover

During the boot process of a client, it requests to lease an IP address by broadcasting a request to all DHCP servers. Because the client does not know the IP address of a DHCP server, or do not have an IP address, it uses 0.0.0.0 as the source address and 255.255.255.255 as the destination address. The DHCPDiscover message contains client's hardware address and computer name so that DHCP servers can determine which client sent the request.

2. IP Lease Offer

All DHCP servers that receive the IP lease request and have a valid configuration for the client broadcast a DHCPOffer message that includes the following information:

- the client's hardware address;
- an offered IP address;
- a subnet mask;
- the length of the lease;
- a server identifier (the IP address of the offering DHCP server).

The DHCP server sends a broadcast message because the client does not yet have an IP address. The DHCP client selects the IP address from the first offer that it receives.

3. IP Lease Request

After the client receives an offer from at least one DHCP server, it broadcasts a DHCPRequest message to all DHCP servers, indicating that it has accepted an offer. The DHCPRequest message includes the server identifier (IP address) of the server whose offer it accepted. All other DHCP servers then retract their offers and retain their IP addresses for the next IP lease request.

4. IP Lease Acknowledgement

4.1 Successful

The DHCP server with the accepted offer broadcasts a successful acknowledgment to the client in the form of a DHCPACK message. This message contains a valid lease for an IP address and possibly other configuration information. When the DHCP client receives the acknowledgment, TCP/IP is completely initialized and the client is considered a bound DHCP client. Once bound, the client can use TCP/IP to communicate on the network.

4.2 Unsuccessful

If the DHCPRequest is not successful, the DHCP server broadcasts a negative acknowledgment (DHCPNACK) if one of the following conditions is met:

- the client is trying to lease its previous IP address and that IP address is no longer available;
- the IP address is invalid because the client has been physically moved to a different subnet.

When the client receives an unsuccessful acknowledgment it returns to the process of requesting an IP lease.

2.1.3 IP Lease Renewal and Release

All DHCP clients attempt to renew their lease when 50 percent of the lease time has expired. To renew its lease, a DHCP client sends a DHCPRequest message directly to the DHCP server from which it obtained the lease. If the DHCP server is available, it renews the lease and sends the client a DHCPACK message with the new lease time and any updated configuration parameters. The client updates its configuration when it receives the acknowledgment.

Each time a DHCP client restarts, it attempts to lease the same IP address from the original DHCP server. If the lease request is unsuccessful and lease time is still available, the DHCP client continues to use the same IP address until the next attempt to renew the lease.

If a DHCP client cannot renew its lease with the original DHCP server at the 50 percent interval, the client broadcasts a DHCPRequest to contact any available DHCP server when 87.5 percent of the lease time has expired. Any DHCP server can respond with a DHCPACK message (renewing the lease) or a DHCPNACK message (forcing the DHCP client to reinitialize and obtain a lease for a different IP address).

If the lease expires or a DHCPNACK message is received, the DHCP client must immediately discontinue using that IP address. The DHCP client then begins the DHCP lease process to lease a new IP address.

2.1.3.1 Using Ipconfig to Renew a Lease

Use the `ipconfig` command with the `/renew` switch to send a DHCPRequest message to the DHCP server to receive updated options and lease time. If the DHCP server is unavailable, the client continues using the current DHCP-supplied configuration options.

2.1.3.2 Using Ipconfig to Release a Lease

You can use the `ipconfig` command with the `/release` switch to cause a DHCP client to send a DHCPRelease message to the DHCP server and to release its lease. This is useful when you are moving a client to a different network and the client will not require its previous lease. TCP/IP communications with the client stops after you issue this command.
Note: Microsoft DHCP clients do not initiate DHCPRelease messages when shutting down. If a client remains shut down for the length of its lease (and the lease is not renewed), the DHCP server might assign that client's IP address to a different client after the lease expires. A client has a better chance of receiving the same IP address during initialization if it does not send a DHCPRelease message.

2.1.4. Understanding DHCP scopes, address ranges, reservations, exclusions, and relay agent

2.1.4.1 DHCP scopes

A DHCP scope is a pool of IP addresses within a logical subnet, which the DHCP server can assign to client. Scopes provide the essential means for the server to manage distribution and assignment of IP addresses and of any related configuration parameters to clients on the network. An IP address within a defined scope that is offered to a DHCP client is known as a lease. When a lease is made to a client, the lease is active. Each lease has a specified duration, and the client must periodically renew the lease if the client is going to continue to use the address. The default lease duration is 8 days.

2.1.4.2 IP Address Range

When defining the IP address range of a scope, you should use the consecutive addresses that make up the subnet for which you are enabling the DHCP service. However, you should also be sure to exclude from this defined range any addresses of statically configured computers already existing on your network. To exclude predefined addresses, you can simply choose to limit the scope range so that it does not include any statically assigned addresses. Alternatively, you can configure a scope that makes up entire subnet ad then immediately define exclusion ranges.

2.1.4.3 Exclusion ranges

An exclusion range is a set of one or more IP addresses, included within the range of the defined scope that you do not want to lease to DHCP clients. Exclusion ranges assures that the server does not offer to DHCP clients on your network any addresses in these ranges. After you define a DHCP scope and apply ranges, the remaining addresses form the available address pool within the scope. Pooled addresses are eligible for dynamic assignment by the server to DHCP clients on your network.

2.1.4.4 Using the 80/20 rule for servers and scopes

To provide fault tolerance for the DHCP device within a given subnet, you might want to configure two DHCP servers to assign addresses for the same subnet. With two DHCP servers deployed, of one server is unavailable, the other server can take its place and continue to lease new addresses or renew existing clients. For balancing DHCP server use In this case, a good practice is to use the 80/20 rule to divide the scope addresses between the two DHCP servers. If Server 1 is configured to make available most (approximately 80 percent) of the addresses, Server 2 can be configured to make the other addresses available to clients.

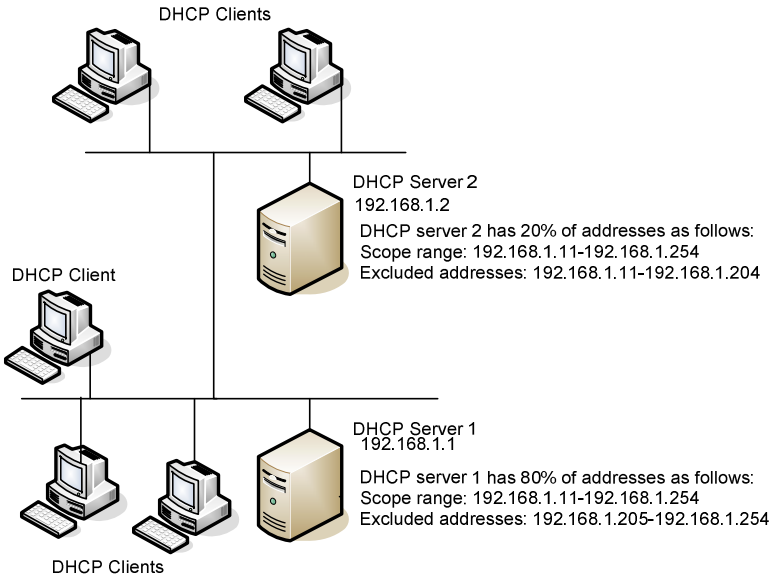

Figure 6.2 *80/20 rule for DHCP subnets*

2.1.4.5 Reservations

You use a reservation to create a permanent address lease assignment by the DHCP server. Reservations assure that a specified hardware device on the subnet can always use the same IP address. Reservations cannot be used interchangeably with manual (static) configuration.

You can use a reservation when you want to assign a specific address to a non-essential computer. Through this method, you can dedicate an address while still enjoying the other benefits of DHCP, including centralized management, address conflict prevention, and scope option assignment.

2.1.4.6 DHCP Options

DHCP options provide clients with additional configuration data, such as specific server addresses, along with an address lease. You can configure options at the reservation level, scope level, or server level. More than 60 standard DHCP options are available; the most common of these include the following: 006 DNS Servers – the IP addresses for the DNS name servers that DHCP clients can contact and use to solve a domain host name query, 015 DNS Domain Name – an option that specified the domain name that DHCP clients should use when resolving unqualified names during DNS domain name resolution, this option also allows clients to perform dynamic DNS updates, 044 WINS/NBNS servers – the IP addresses of primary and secondary WINS servers for the DHCP client to use.

2.1.4.7 Using superscopes

A superscope is an administrative grouping of scopes that is used to support multinets, or multiple logical subnets on a single network segment. Multinetting commonly occurs when the number of hosts on a physical segment grows beyond the capacity of the original address space. By creating a logically second scope to add to an original scope, and then grouping these two scopes into a single superscope, you can double your physical segment’s capacity for addresses. In this way, the DHCP server can provide clients on a single physical network with leases from more than one scope.

2.1.4.8 Understanding DHCP Relay Agent

DHCP Relay Agent is a routing protocol that allows client computers to obtain an address from a DHCP server on a remote subnet. Typically, DHCP clients broadcast DHCPDiscover packets that are received and answered by a DHCP server on the same subnet. Because routers block broadcasts, DHCP clients and servers must normally be located on the same physical subnet. However, two methods can help you work around this limitation. First, if the routers separating the DHCP server and clients are RFC 1542-compliant, the routers can be configured for Boot Protocol forwarding. Through BOOTP forwarding, routers forward DHCP broadcasts between clients and servers and inform servers of the originating subnet of the DHCP requests. This process allows DHCP servers to assign addresses to the remote clients from the appropriate scope. The second way to allow remote communication between DHCP servers and clients is to configure a DHCP relay agent on the subnet containing the remote clients. DHCP relay agents intercept DHPCDiscover packets and forward them to a remote DHCP server whose address has been preconfigured. Although DHCP Relay Agent is configured through Routing and Remote Access, the computer hosting the agent does not need to be functioning as an actual router between subnets.

2.2 NAT – Network Address Translation

Network Address Translation is a mechanism for translating the IP addresses of hosts on a private network into IP addresses belonging to a different (public) network. NAT is usually used at the boundary of two networks, especially where a private network such as a corporate network meets a public network such as the Internet.

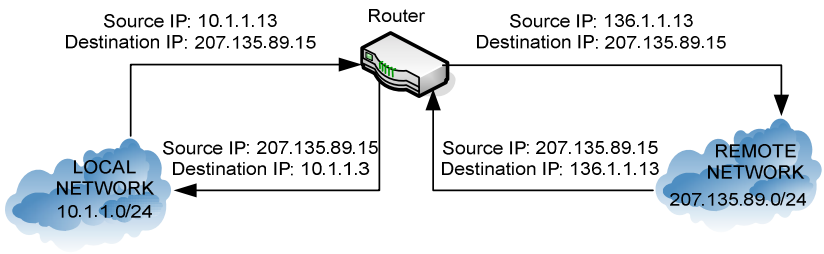

Figure 6.3 *Network Address Translation*

The motivation behind the creation of NAT is that the number of available global (public) registered IP addresses on the Internet is rapidly being depleted. NAT works around this problem by:

- address reuse: NAT allows multiple private networks to use the same network IDs (same range of IP addresses). Private networks can use any range of IP addresses but usually employ those address specially reserved by the IANA (Internet Assigned Numbers Authority) for private network usage, such as 10/8, 172.16/12, 192.168/16. Addresses in this rage are assigned by IANA as nonroutable addresses, and network using these addresses cannot directly connect to Internet using a router. Instead, they need a router or access device that supports NAT so that these nonroutable addresses can be translated into public addresses for routing over the Internet;
- address multiplexing: NAT allows IP addresses of multiple hosts on a private network to be exposed to the Internet as a single public IP address. This allows the addresses of the hosts on a private network to be hidden from the outside world, improving security on the network. Address multiplexing is sometimes referred to as a network address port translation (NAPT).

In a typical scenario, a NAT-enabled router connects an internal corporate network with the Internet. The internal network has multiple IP hosts using private network addresses, while the router has a similar private IP address on its near-side (internal) interface and a public (global) address on its fair-side (external) interface. NAT operates by examining traffic that passes through the router and building a table that maps the connections between hosts inside the network and hosts outside on the Internet. For each connection the table contains:

- original IP address and port number of source address;
- original and port number of destination address;
- translated IP address and port number of source address;
- translated IP address and port number of destination address;
- Transmission Control Protocol (TCP) and ICMP sequence numbers.

Implementing NAT on a router or firewall thus involves creating and configuring a NAT table containing these private/public IP address mappings. These address mappings can either be:

- manually created: a static NAT table essentially consists of a series of manually created NAT rules that specify how IP addresses will be

translated. Static NAT mappings are always one-to-one mappings between actual and translated addresses. This approach can be used, when corporate networks with conflicting addresses need to be merged into one network. Static mappings are not very useful, however, for connections between private networks and the Internet due to the large number of possible connections to the Internet hosts, which can make the NAT table grow excessively large thus degrading router performance;

- dynamically created: Nat-enabled routers can often dynamically allocate IP addresses to hosts on the private network by selecting addresses drawn from a specific pool. Dynamic NAT mappings are also one-to-one mappings between actual and translated addresses. This process is similar to DHCP and can be done either randomly or, more usually, on a round-robin basis. Each time a connection is formed between the external and internal networks, NAT assigns a different IP address from the pool to the internal host being connected to and address information in packets is modified accordingly.

Another form of dynamic NAT is called address overloading (masquerading, port address translation - PAT) or network address port translation (NAPT). In this situation all the IP addresses of the internal private network are hidden to outsiders, who can access only the single IP address of the interface exposed to the public network. Address overloading thus employs many-to-many mappings of IP addresses and is used when the number of internal addresses is greater than the available number of global addresses. Address overloading differs from standard NAT in that port numbers are also translated, not just IP addresses. For example, it is possible to multiplex many TCP connections through a single global IP address by assigning each connection a different port number. PAT is often used by firewalls and sometimes for load balancing Web servers.

Disadvantages: NAT’s main disadvantage is that some protocols simply do not work when IP addresses are translated. This particularly applies to protocols that involve: encryption and embedded addresses (protocols embed address and port information within the data portion of packets in a nonpredictable fashion). Another disadvantage of NAT is that end-to-end connectivity is effectively lost, which makes it difficult to troubleshoot routing issues.

3. Lab activity

3.1 Installing the DHCP Server Service

Implementing a basic DHCP server requires installing the server, authorizing the server; configuring scopes, exclusions, reservations and options; activating the scopes; and finally, verifying the configuration. To implement DHCP, you must install the DHCP Service on at least one computer running Windows 2000 Server within the TCP/IP network. Before you install the DHCP Server, you should specify a static IP address, subnet mask, and default gateway for the network adapter in the computer designed as the DHCP Server.

1. Select Start, Settings, Control Panel, Add or Remove Programs.
2. On the Add or Remove Programs page, click Add/Remove Windows Components to open the Windows Component Wizard.
3. Select Networking Services.
4. Click the Details button to open the Networking Services window.
5. Select Dynamic Host Configuration Protocol (DHCP) and click OK.
6. Back in the Windows Components Wizard page, click Next to begin the installation.
7. If you are prompted to supply the location of your Windows Server 2000 CD-ROM or installation files, provide the correct location. Windows installs the DHCP service files on your computer.

After the installation has completed, you can verify that the DHCP Server service has been installed on your computer by opening the DHCP console administrative tool. To access the DHCP console, click Start, select the Administrative Tools, and then select DHCP. The DHCP console is the interface from which you can configure and manage virtually all features related to your DHCP server, including scopes, exclusions, reservations and option.

Note: DHCP servers must be authorized if they are to be integrated in Active Directory networks. Only domain controllers and domain member servers participate in Active Directory, and only these server types can become authorized. When your network includes Active Directory domains,

the first DHCP server you install on the network must be an authorized DHCP server. When the DHCP server service is installed on a domain controller, you can perform the authorizing procedure by simply right-clicking the server node in the DHCP console and selecting Authorized.

3.2 Configuring scopes

1. Open the DHCP console and select New Scope from the context menu.
2. Name the scope Test Scope.
3. In the IP Address Range page, in In the Start IP Address text box, type 192.168.0.1, in the End IP Address text box, type 192.160.0.10. Verify that the subnet mask value reads 255.255.255.0.
4. In the Excluded Address Range window, exclude the address 192.168.0.1 and the range 192.168.0.3 – 192.168.0.5.

Note: The Lease Duration: you can configure the amount of time for which a DHCP lease is valid. The default setting is 8 days and can be changed to any value between 1 minute and almost 1,000 days (999 days, 23 hours, 59 seconds, to be exact). For the average network, the default setting of 8 days is sufficient. Set the lease duration to 10 minutes.

5. On the next pages of the wizard, the Configure DHCP Options pages, you are given the choice to configure additional options for your scope now or later. Configure the Default Gateway page, the DNS Server page, the WINS Server page with the information given from the instructor.
6. On the next page of the wizard, the Activate Scope page, you are given the option to active the configured scope now or later. In most cases you want to activate the scope right away. Select Yes, I Want to Activate This Scope Now and click Next to activate the configured scope.

3.3 Configuring the client

1. Open the Local Area Connection Properties dialog box, and then open the Internet Protocol (TCP/IP) Properties dialog box.
2. On the General tab, select the Obtain An IP Address Automatically option.
3. Select the Obtain DNS Server Address Automatically option.
4. In the Local Area Connection Properties dialog box, click Close.

3.4 Testing the configuration

1. Open a command prompt.
2. At the command prompt type ipconfig /all, and then press Enter.

The new IP address configuration obtained through DHCP is displayed, including the address. The Default Gateway, the DHCP Server, and DNS Server parameters are all set.

3.5 Testing the configuration with more examples

1. Stop the DHCP server.
2. Test on client ipconfig/all. What is the IP address of the client?
3. Wait until lease expires (10 minutes). Test `ipconfig/all`. What is now the IP address of the client?
4. Restart the DHCP server. Test on client `ipconfig/all`. What is the IP address of the client?
5. On the DHCP server, make a reservation for the address 192.168.0.2.

Note: You can configure an address reservation by right-clicking Reservations and selecting New Reservation from the context menu. You can configure a reservation for any device that you want to have a DHCP -assigned IP address that never expires. Configure the reservation for a MAC address from your lab and after you've configured a reservation, you can see it in the Reservations node of the DHCP console.

6. On the client type `ipconfig/release` then `ipconfig/renew`. Which is the new address of your client computer?

Notes