DHCP Server

Heng Sovannarith
heng_sovannarith@yahoo.com

Introduction

- Dynamic Host Configuration Protocol (DHCP) automatically assigns IP addresses and other network configuration information to computers on a network.
- Setting up a DHCP server enables you to centrally manage the addresses and other network information for client computers on your private network.

Introduction (cont.)

- DHCP reduces the human error in manual network configuration and the amount of time required to configure clients and allows one to move a computer to various networks and be configured with the appropriate IP address, gateway and subnet mask.

Features

1 - Provides automatic network configuration to the client:

a - IP Address

b - Subnet mask

c - Default gateway

d - DNS Servers (Domain Name Services)

e - NTP Servers (Network time protocol (NTP).

f - WINS Servers (**Windows Internet Name Service**)

DHCP Terminology

- ***DHCP client*** - A computer that obtains its configuration information from DHCP.
- ***DHCP server*** - A computer that provides DHCP configuration information to multiple clients.
  - The IP addresses and configuration information that the DHCP server makes available to the client are defined by the DHCP administrator.

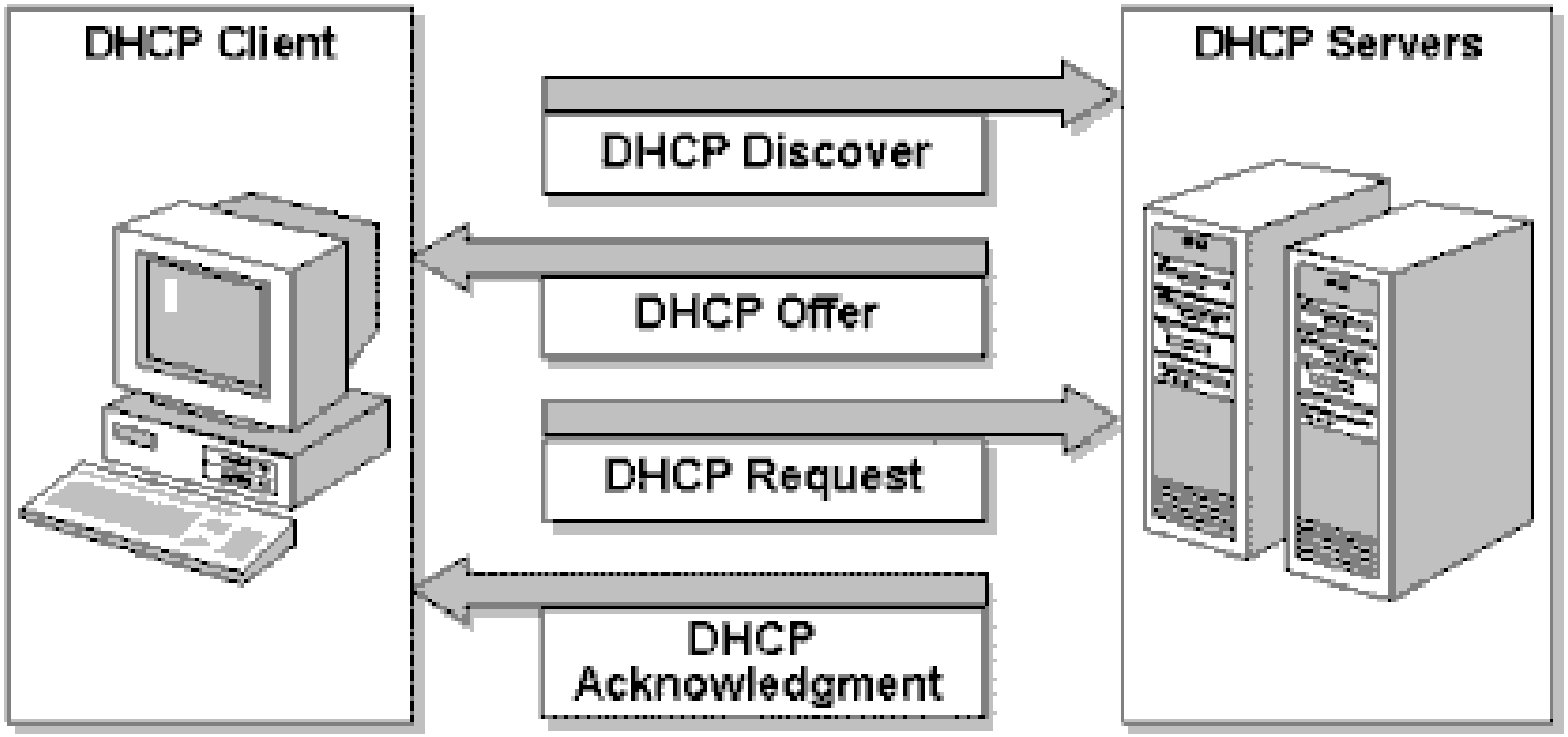
DHCP Terminology (cont.)

- ***DHCP lease*** - This defines the duration for which a DHCP server assigns an IP address to a DHCP client.
  - The lease duration can be any amount of time between 1 minute and 999 days, or it can be unlimited.
  - The default lease duration is eight days.

DHCP Message

- All DHCP messages are carried in ***User Datagram Protocol (UDP)*** datagrams using the well-known port numbers 67 (from the server) and 68 (to the client).
- UDP operates at the Transport Layer of the OSI model and is a low-overhead protocol because it does not use any type of packet acknowledgement.
- The firewall on your DHCP server must be configured to allow access to UDP ports 67 and 68.

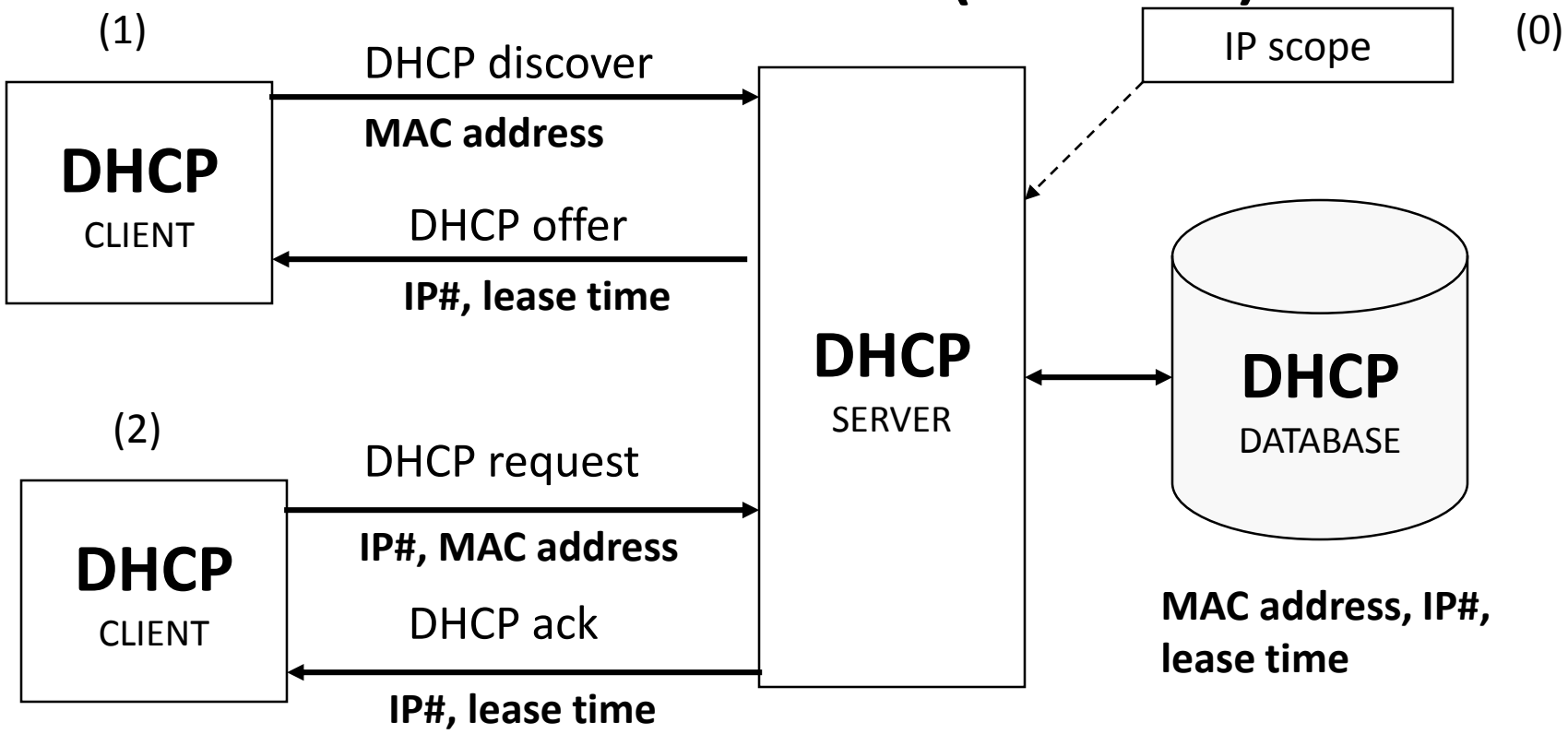
DHCP Process (DORA)



DHCP Process (DORA)

- The initial DHCP lease process is accomplished using four messages:
  - DHCPDISCOVER — client sends a broadcast, source=0.0.0.0 destination=255.255.255.255(think of the client saying “I need an IP address”)
  - DHCPOFFER — DHCP server responds with a broadcast, it includes its own IP address and the MAC address of the client(think or a response saying “this is 10.10.10.5 and this is what I got”)
  - DHCPREQUEST — client send a broadcast back that includes the IP of the chosen DHCP server(think of client saying “10.10.10.5 I accept your offer”)
  - DHCPACK — The DHCP server sends final ACK that include lease duration for the client’s IP address
  - Lease Renewal: When half of the lease time has expired, the client will issue a new request to the DHCP server.

DHCP Process (DORA)



- a range of IP addresses
- the IP# is assigned temporarily
- servers are assigned fixed IP addresses

Pron and Con

- **Pros**
  - **simplifies the task of assigning IP numbers to each machine in the network**
  - **makes easy to add, remove or move a host**
  - **can assign defaults: default gateway, domain name, DNS server, WINS server (if any) .**
  - **ability to have fewer IP# than hosts**
- **Cons**

  if DHCP server is down, all hosts are down

  hard to keep information on free and used IP #

Install and Configure DHCP

- Install DHCP

  # yum -y install dhcp

- Edit the DHCP configuration file

  #vim /etc/dhcpd.conf

- Take note of the location of the sample configuration file.

- Copy the sample configuration file to the actual file

  #cp /usr/share/doc/dhcp-3.05/dhcpd.conf.sample /etc/dhcpd.conf

- When asked to confirm whether you want to overwrite the configuration file type y then press enter.

- The elements that can be used in a configuration file are: (global) parameters, shared networks, subnets, groups and hosts.
  - Global Parameter: The value of a global parameter can be overridden by assigning the parameter another value in subsequent sections.
  - A shared-network declaration is used if there are multiple subnets on the same physical network.
  - A subnet-declaration is used to define a network segment. Parameters that only apply to the subnet in question are defined within the subnet-declaration.
  - A group-declaration is used to group other declarations, including group-declarations.
  - A host declaration is used to set properties for a specific client.

```
ddns-update-style interim;
authoritative;

subnet 192.168.0.0 netmask 255.255.255.0 {
   #global parameters for the subnet
   option routers                  192.168.0.1;
   option subnet-mask              255.255.255.0;
   option domain-name              "example.com";
   option domain-name-servers      192.168.1.1;
   range dynamic-bootp 192.168.0.128 192.168.0.254;
   default-lease-time 21600;
   max-lease-time 43200;

   # fixed address example
   host jadefox {
      next-server ns.example.com;
      hardware ethernet 12:34:56:78:AB:CD;
      fixed-address 192.168.0.4;
   }
}
```

Shared-Network

```
shared-network third-floor {
   #global parameters for the shared network
   option routers                    192.168.0.1;
   option subnet-mask                255.255.255.0;
   option nis-domain                 "example.com";
   option domain-name                "example.com";
   option domain-name-servers        192.168.1.1;
   default-lease-time 21600;
   max-lease-time 43200;

   subnet 192.168.10.0 netmask 255.255.255.0 {
      range dynamic-bootp 192.168.10.1 192.168.10.254;
   }

   subnet 192.168.20.0 netmask 255.255.255.0 {
      range dynamic-bootp 192.168.20.1 192.168.20.254;
   }
}
```

Group Declaration

```
group {
   #common parameters for both host declarations
   option routers                  192.168.10.254;
   option subnet-mask              255.255.255.0;
   option domain-name              "example.com";
   option domain-name-servers       192.168.10.24;
   default-lease-time 21600;
   max-lease-time 43200;

   host printer {
      option host-name "printer.example.com";
      hardware ethernet 01:BE:BB:5E:1A:CC;
      fixed-address 192.168.10.7;
   }

   host payroll {
      option host-name "payroll.example.com";
      hardware ethernet 02:B4:7C:43:DD:FF;
      fixed-address 192.168.10.10;
   }
}
```

Network Interface for DHCP

- Edit the system configuration file for dhcpd
  - vim /etc/sysconfig/dhcpd
- Set the name of the network interface to use for dhcp configuration (generally eth0).

```
# Command line options here
DHCPDARGS=eth0
~
~
```

Services

- To restart the dhcp server type:

  #service dhcpd restart

Service (cont.)

- To make the dhcp server restart at boot time, issue the commands:

  #chkconfig dhcpd on

DHCP Database

- All leases granted by the DHCP Service are stored in a file called dhcpd.leases.
- In CentOS Linux, the dhcpd.leases file are stored in the /var/lib/dhcpd/dhcpd.leases

  #vim /var/lib/dhcpd/dhcpd.leases

Check whether DHCP Server is Working or Not!

- There are a few ways you can verify that your DHCP server is working:
  - Check the /var/log/messages file. If the DHCP service has trouble starting, you will see messages in this file indicating what the problem is.
  - Check the /var/lib/dhcpd/dhcpd.leases file. If a client has been assigned addresses successfully from the DHCP server, a lease line should appear in that file.

```
lease 10.0.0.225 {
        starts 2 2009/05/04 03:48:12;
        ends 2 2009/05/04 15:48:12;
        hardware ethernet 00:50:ba:d8:03:9e;
        client-hostname "zarkov";
}
```

Class and Subclass

- Create a Class name “MyHosts”

```
class "MyHosts" {
    match hardware;
}
subclass "MyHosts" 1:10:bf:48:xx:xx:xx;  # host2
subclass "MyHosts" 1:10:bf:48:xx:xx:xx;  # host3
```

- For ethernet clients, the hardware type is 1, thus the 1: prefix in the data string of the subclass statements.

Class and Subclass (cont.)

```
subnet 192.168.1.0 netmask 255.255.255.0 {
    ...
    pool {
        range 192.168.1.101 192.168.1.250;
        ...
        deny members of "MyHosts";
        ...
    }
    pool {
        range 192.168.1.1 192.168.1.20;
        ...
        allow members of "MyHosts";
        ...
    }
}
```

Class and Subclass (cont.)

- Pool-Level Allow/Deny Declarations
  - **known-clients**
    - a known client is one that has a host declaration within the configuration file.
    - The allow known-clients declaration allows the assignment of an address within a pool to a client if it has a host declaration; deny known-clients will disallow assignment of an address to a client with a host declaration from the pool.

```
allow known-clients;

deny known-clients;
```

Class and Subclass (cont.)

- **unknown-clients**
  - – an unknown client does not have a host declaration within the configuration file. The allow unknown-clients declaration allows the assignment of an address within a pool to a client if it does not have a host declaration;
  - deny unknown-clients will disallow assignment of an address to a client that does not have a host declaration from the pool.

```
allow unknown-clients;

deny unknown-clients;
```

Class and Subclass (cont.)

- **`members of "class"`** – this declaration is used to define whether addresses within this pool can be assigned to members matching the specified class definition (allow) or not (deny).

```
allow members of "class";
deny members of "class";
```

Where *class* is the class name of a class declaration defining its members via match statements.

Class and Subclass (cont.)

- **`all clients`** – this declaration allow or denies address allocation from this pool for all (any) clients. Denying all clients can be used to define a pool that is not yet turned up in production. Flipping the definition to allow then brings it online in the server.

```
allow all clients;
deny all clients;
```

- **`after time`** – this declaration with allow or deny keywords enables or disables respectively address allocation from this pool at or after a specified point in time. This declaration is useful for moving clients from one pool to another. The `deny after time` could be used on the pool from which clients are being moved; the DHCP server will modify the lease time to be the *`time`* specified plus the min-lease-time option value.

  The `allow after time` declaration would be defined on the pool to which the clients are being moved, configuring the DHCP server to service clients with leases only after *`time`*. The *`time`* parameter is formatted as a UTC (coordinated universal time) time string; e.g., `2008-03-17 08:27:32 -0500`.

```
allow after time;
deny after time;
```

Release and Renew IP Address

- `ifconfig` to release and renew an IP address

```
#ifconfig eth0 down          (disable eth0)
#ifconfig eth0 up            (enable eth0)
#dhclient eth0       (Renew the IP Address)
```

Release and Renew IP Address (cont.)

- **IPCONFIG /ALL**

  FQDN, servers (DNS, WINS), node type, etc

  NIC description, MAC address, IP address, gateway, subnet mask

- **To handle leases**

  IP CONFIG/RENEW [adapter]

  IP CONFIG/RELEASE [adapter]

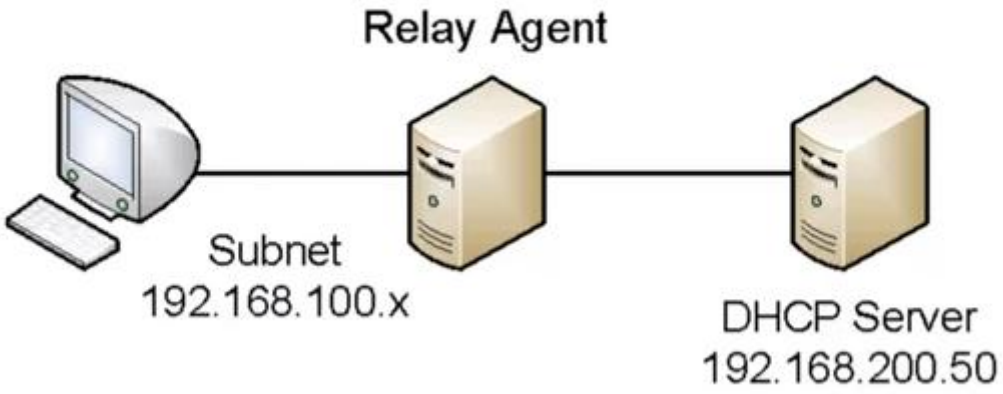
  if no adapter name is specified, then the IP leases for all adapters bound to TCP/IP will be released or renewed.

DHCP Relay Agent

- DHCP relies heavily on broadcast messages.
- Broadcast messages are generally limited to the subnet in which they originate and are not forwarded to other subnets.
- A *DHCP relay agent* is either a host or an IP router that listens for DHCP (and BOOTP) client messages being broadcast on a subnet and then forwards those DHCP messages to a DHCP server.
- The DHCP server sends DHCP response messages back to the relay agent, which then broadcasts them onto the subnet for the DHCP client.
- Using DHCP relay agents eliminates the need to have a DHCP server on every subnet.

DHCP Relay Agent (cont.)

- What is a DHCP Relay Agent?
  - The DHCP Relay Agent relays Dynamic Host Configuration Protocol (DHCP) messages between DHCP clients and DHCP server on different IP networks.



DHCP Relay Agent (cont.)

- Some DHCP messages are broadcast packets
  - Discover, Offer, Request, Ack
- Routers do not pass broadcast packets
- The Relay Agent coverts broadcast into unicast packets.

DHCP Relay Agent (cont.)

- We can use either the server or the router to act as DHCP Relay Agent.
- Install the DHCP Relay Agent on Server:
  - Acting as DHCP Relay Agent, we also install dhcp service.

    ```
    #yum –y install dhcp
    ```
  - After installation is complete, configure the DHCP Relay Agent in dhcrelay file.

    ```
    #vim vi /etc/sysconfig/dhcrelay
    ```

DHCP Relay Agent (cont.)

- In the configuration, add the following content:

```
INTERFACES="eth0 eth1 eth2"
DHCPSERVERS="172.16.1.1"
```

DHCP Relay Agent (cont.)

- Enable IP forwarding (Routing)
  - Check if routing is enabled:

```
#cat /proc/sys/net/ipv4/ip_forward
```

    - 0 = disabled
    - 1 = enabled

```
# For binary values, 0 is disabled, 1 is enabled.  See
# sysctl.conf(5) for more details.

# Controls IP packet forwarding
net.ipv4.ip_forward = 1

# Controls source route verification
net.ipv4.conf.default.rp_filter = 1

# Do not accept source routing
net.ipv4.conf.default.accept source route = 0
```

DHCP Relay Agent (cont.)

- Start DHCP Relay service (dhcrelay)

```
#chkconfig dhcrelay on
#service dhcrelay start
```