Understanding DHCP, DNS & NTP Services

ine.com

VOD-3490

Keith Bogart

CCIE #4923

✉ kbogart@ine.com
🐦 @keithbogart1
in linkedin.com/in/keith-bogart-2a75042

CCIE Routing & Switching

- General understanding of the Internet Protocol
- Familiarity with IP addresses

Course Prerequisites

Course Objectives

+ To introduce you to the Dynamic Host Configuration Protocol (DHCP)
+ To explain how the Domain Name Service (DNS) is used in computer networks
+ To provide an introduction to the Network Time Protocol (NTP)

The Dynamic Host Configuration Protocol (DHCP)

ine.com

Topic Overview

+ How IP Information Is Obtained
+ Introduction To DHCP
+ DORA
+ Other Types Of DHCP Packets

The Necessity Of IP
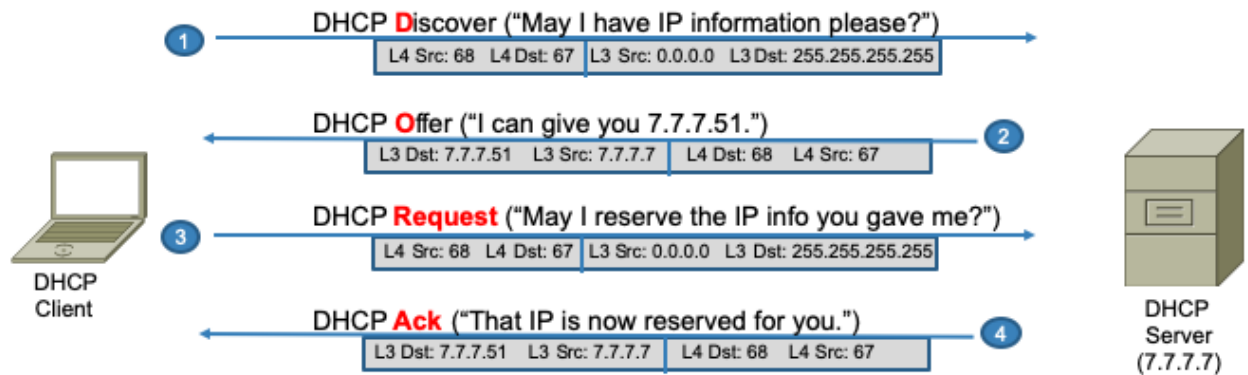
+ Hosts require IP information in order to utilize the services of an IP-based network
+ What is the minimum necessary information?
    + IP address
    + Subnet mask
    + Lease time
    + Default gateway address
    + DNS server address
+ Where can devices obtain these addresses?
    + Statically
    + Dynamically

Introduction To DHCP

+ Dynamic Host Configuration Protocol
+ Operates in application layer
+ Provides dynamic method of leasing an IP address to a host
+ IPv4 DHCP uses UDP ports 67 and 68
+ DHCPv6 uses UDP ports 546 and 547
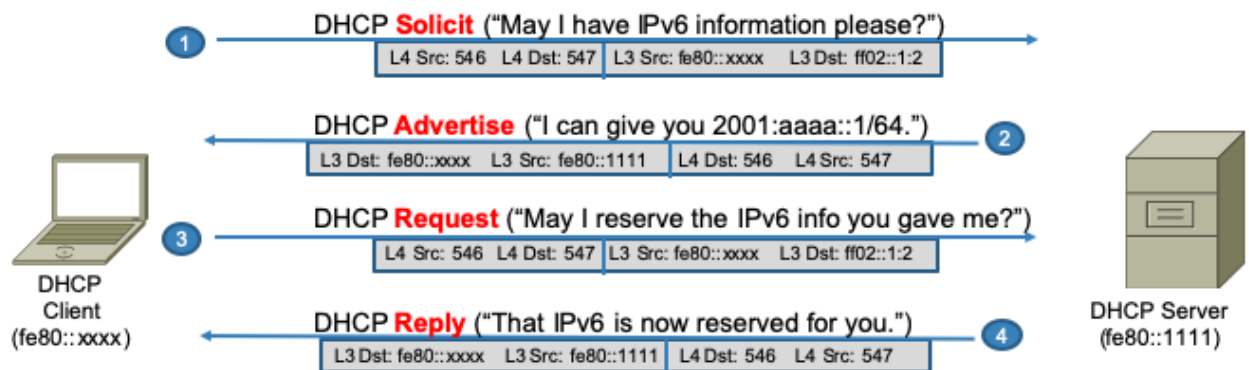+ Enhancement to an older protocol, BootP

IPv4 DORA

+ Four discreet steps are used between a DHCP Client and DHCP Server
+ These steps can be remembered using the acronym D.O.R.A.

DHCP **D**iscover ("May I have IP information please?")

| L4 Src: 68 | L4 Dst: 67 | L3 Src: 0.0.0.0 | L3 Dst: 255.255.255.255 |

DHCP **O**ffer ("I can give you 7.7.7.51.")

| L3 Dst: 7.7.7.51 | L3 Src: 7.7.7.7 | L4 Dst: 68 | L4 Src: 67 |

DHCP **Request** ("May I reserve the IP info you gave me?")

| L4 Src: 68 | L4 Dst: 67 | L3 Src: 0.0.0.0 | L3 Dst: 255.255.255.255 |

DHCP **Ack** ("That IP is now reserved for you.")

| L3 Dst: 7.7.7.51 | L3 Src: 7.7.7.7 | L4 Dst: 68 | L4 Src: 67 |

DHCP Client

DHCP Server (7.7.7.7)

Notice that UDP port 68 is used to address (send things to) the DHCP Client…and UDP Port 67 is used to address (send things to) the DHCP Server.

IPv6 SARR

+ Four discreet steps are used between a DHCPv6 Client and DHCPv6 Server

+ These steps can be remembered using the acronym S.A.R.R.

DHCP **Solicit** ("May I have IPv6 information please?")

| L4 Src: 546 | L4 Dst: 547 | L3 Src: fe80::xxxx | L3 Dst: ff02::1:2 |

DHCP **Advertise** ("I can give you 2001:aaaa::1/64.")

| L3 Dst: fe80::xxxx | L3 Src: fe80::1111 | L4 Dst: 546 | L4 Src: 547 |

DHCP **Request** ("May I reserve the IPv6 info you gave me?")

| L4 Src: 546 | L4 Dst: 547 | L3 Src: fe80::xxxx | L3 Dst: ff02::1:2 |

DHCP **Reply** ("That IPv6 is now reserved for you.")

| L3 Dst: fe80::xxxx | L3 Src: fe80::1111 | L4 Dst: 546 | L4 Src: 547 |

DHCP Client (fe80::xxxx)

DHCP Server (fe80::1111)

Other Types Of DHCP Messages

+ ## DHCP Release
    + Used by Client to inform Server that IP address is no longer needed and may be placed back into the DHCP Pool
+ ## DHCP NACK
    + A DHCP Client may request an address that was previously used by that same client
    + If the address has subsequently been allocated to a different client, DHCP Server sends a DHCP NACK

Other Types Of DHCP Messages

+ DHCP Inform
    + Used by Client who already has an IP address but requests additional parameters from DHCP Server
+ DHCP Decline
    + Used by a Client to inform Server that parameters contained in the DHCP Offer were unacceptable to the Client
    + DHCP Process must start over

On a Mac, you can get it to transmit a DHCP Inform message by selecting the option (under System – Network) of "Use DHCP With Manual Address". The Mac will then transmit a DHCP Inform message requesting everything else but the IP address…such as a subnet mask, default gateway, etc.

Configuring Cisco IOS As A DHCP Server Or Relay Agent

Topic Overview

+ DHCP Broadcast Handling
+ DHCP Relay Agents
+ Cisco IOS DHCP Server

DHCP Broadcast Handling Options

+ DHCP Client messages are broadcast
+ Broadcasts are not routable
+ A router (or Layer-3 switch) can deal with a DHCP broadcast in one of three ways:
    + Drop it (default behavior)
    + Relay it to a known DHCP Server
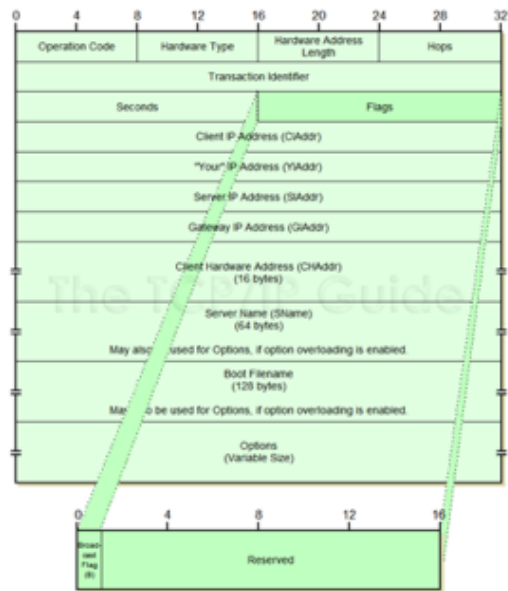   + Respond to it as a configured DHCP Server

DHCP Relay Agents

+ Device which receives a DHCP Client broadcast and unicasts the packet to a known DHCP Server
+ Relay Agents populate their own IP address into the GiAddr field of DHCP Packets
    + Also known as "Relay Agent IP Address" field

Src: 0.0.0.0 Dst: 255.255.255.255   Src: 1.1.1.1 Dst: 7.7.7.7

Gig0/0

1.1.1.1   R1   2.2.2.1   2.2.2.2   R2   7.7.7.2

DHCP Relay Agent
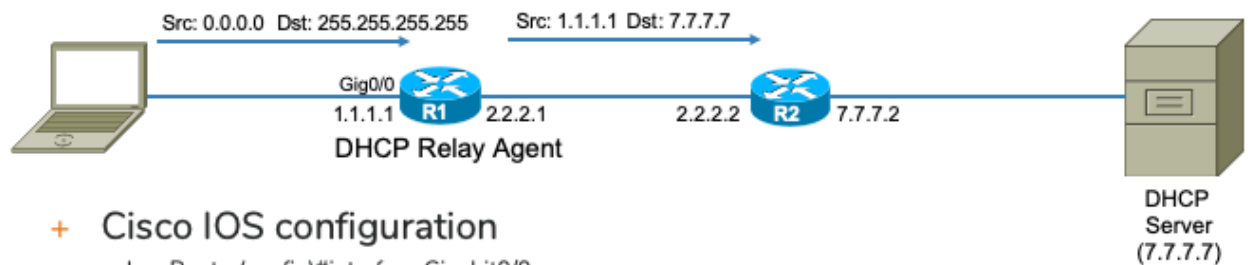
DHCP Server (7.7.7.7)

+ Cisco IOS configuration
    + Router(config)#interface Gigabit0/0
    + Router(config-if)#ip helper-address 7.7.7.7

DHCP Packet Format

0	4	8	12	16	20	24	28	32

Operation Code	Hardware Type	Hardware Address Length	Hops

Transaction Identifier

Seconds	Flags

Client IP Address (CIAddr)

"Your" IP Address (YIAddr)

Server IP Address (SIAddr)

Gateway IP Address (GIAddr)

Client Hardware Address (CHAddr)
(16 bytes)

Server Name (SName)
(64 bytes)

May also be used for Options, if option overloading is enabled.

Boot Filename
(128 bytes)

May also be used for Options, if option overloading is enabled.

Options
(Variable Size)

0	4	8	12	16

Broadcast Flag (B)	Reserved

Cisco IOS DHCP Server

+ In smaller networks, a router or switch can be configured as a DHCP Server

```
Router(config)# service dhcp
Router(config)# ip dhcp pool <pool-name>
Router(config-dhcp)# network < network-id>
Router(config-dhcp)# default-router <default gateway>
Router(config-dhcp)# dns-server <dns-server address>
Router(config-dhcp)# lease <duration>
Router(config-dhcp)# end
```

+ Devices with static IP's should be excluded from the DHCP Pool

```
Router(config)# ip dhcp excluded-address <start-ip> <end-ip>
```

Cisco IOS devices have a default Lease time of 1-day (86,400 seconds) if you don't configure that value.

Methods Of Verification

+ Verification commands

Router# **show ip dhcp binding**

```
R3#sho ip dhcp binding
Bindings from all pools not associated with VRF:
IP address          Client-ID/             Lease expiration       Type
                    Hardware address/
                    User name
10.1.1.1            0063.6973.636f.2d30.   Sep 24 2019 02:23 PM   Automatic
                    6363.392e.3962.3666.
                    2e65.3630.302d.4769.
                    302f.30
10.1.1.3            0063.6973.636f.2d30.   Sep 24 2019 02:25 PM   Automatic
                    6363.392e.3962.6665.
                    2e34.6230.302d.4769.
                    302f.30
```

The client identifier is an ASCII value in the form cisco-mac-name where mac is the MAC address of the interface and name is the short form of the interface name.

Thanks for Watching!

Configuring DHCP Clients

ine.com

Topic Overview

+ Configuring & Verifying DHCP For Windows Clients
+ Configuring & Verifying DHCP For MAC Clients

Thanks for Watching!

The Domain Name Service (DNS)

Topic Overview

+ What Problem Is Solved By DNS?
+ Overview Of DNS Operation
+ Example Of DNS Operation

DNS, What Problem is Solved?

+ Remembering IPv4/IPv6 addresses for devices, websites, services, etc is cumbersome
+ Easier to remember human-readable names
+ These names must be resolved to IP addresses for network connectivity
+ DNS is designed to do just that
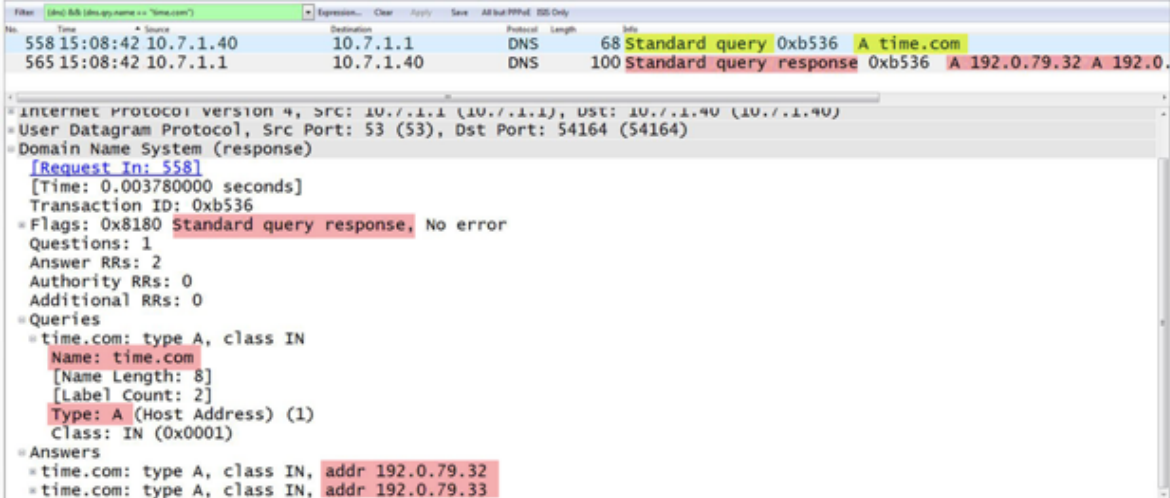
Another benefit is that if a device is known by its name, its IP address can be moved. As long as that name-to-address mapping is updated in a DNS server any endpoint can find it without everyone NEEDING to know that the IP address has been changed.

DNS Operation

+ DNS Server IP typically learned via DHCP
+ Client-Server Operation
+ DNS Queries and Replies
  + Use UDP Port 53
  + "A" Record Lookup = IPv4
  + "AAAA" Record Lookup = IPv6
+ DNS Updates (copying of name-resolution tables between DNS Servers)
  + Uses TCP Port 53

DNS For URL lookups

+ Most common application of DNS is to resolve websites to IP addresses

For more detailed information about DNS I'd recommend watching my course titled, "Understanding Common Network Applications" as well as the video titled, "The DNS Protocol" from the larger course titled, "**Cisco IOS Infrastructure Services**"

The Network Time Protocol (NTP)

ine.com

Topic Overview

+ Why Keep Track Of Time?
+ Where Do We Get The Clock?
+ Sources Of Network Time
+ NTP Overview
+ NTP Clients & Servers
+ Cisco IOS NTP Configuration

Why Do We Need To Keep Track Of Time?

+ Cisco devices (routers and switches) can utilize time for several purposes:
    + Logging output
    + Debugging output
    + User "show" commands
    + Network Management/Reporting tools
+ Having an accurate timestamp on the above features can be critical

Where Do We Get The Clock?

+ All routers/switches have an internal "system clock"
+ Most are battery-driven and maintain the time/date across reloads
+ Devices with battery-driven system clocks can also distribute this information to remote devices via NTP

Sources Of Time

+ The System Clock can obtain its information via:
    + Manual Configuration
    + NTP (network time protocol)
    + SNTP (simple network time protocol)
    + VINES Time Service (Virtual Integrated Network Service)
+ In this section we'll be concentrating on NTP

SNTP is a simplified version of NTP that provides client-only services (can receive time, but not propagate it to other devices). No authentication capability.

CCNA doesn't expect you to know anything about SNTP or VINES.

NTP

+ Network Time Protocol
+ IETF Standard: RFC 1305 (version-3) and RFC 5905 (version-4)
+ Uses UDP port 123 (source and destination)
+ NTP Nodes obtain time from an authoritative source:
    + Atomic Clock
    + GPS
    + Radio Clock
    + Other network devices

NTP Device Roles

+ NTP Client = Device that periodically polls a server for time/calendar information
+ NTP Server = Provides that information to Client
+ NTP Server also considered an "authoritative source" of time based on its Stratum Level
  + Stratum 1 = Device directly connected to a radio or atomic clock source
  + Stratum 2 = Time Server that is one hop away from Stratum-1 device

NTP Master/Client Configuration

+ NTP Server Configuration
  + Router#clock set 07:01:30 28 Feb 2015
  + Router(config)#ntp master [stratum]

+ NTP Client Configuration:
  + Router(config)#ntp server x.x.x.x

Default stratum level assigned if not configured is "stratum 8".

NTP Verification

+ ## Show ntp status

```
Switch-1#sho ntp status
Clock is synchronized  stratum 9, reference is 11.11.11.1
```

+ ## Show ntp associations

```
Switch-1#sho ntp associations

        address            ref clock        st  
*~11.11.11.1          127.127.1.1          8
 * master (synced), # master (unsynced),
```

For some unknown reason, it often takes several minutes for NTP to synchronize when both the NTP Client and NTP Server are Cisco IOS devices. So if trying this out for yourself in a lab, be very patient.

Thanks for Watching!