Common Hub and Switch Network Connectivity Devices

by Sophia

WHAT'S COVERED

In this lesson, you will continue to learn about some commonly used networking devices and three of the protocols that they use.

Specifically, this lesson will cover the following:

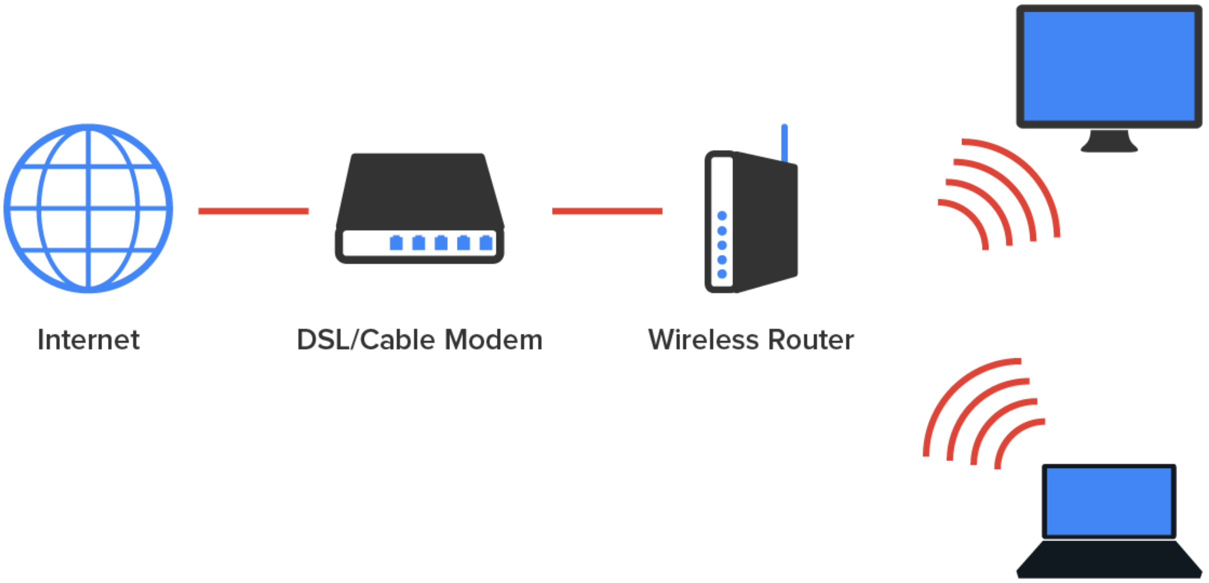
1. WLAN Devices

Wireless local area networks (WLANs) are widely popular in both SOHO and enterprise environments, because they provide end users with mobility, which is the freedom to move around an area while maintaining a connection to a network. This section will focus on two common components of wireless networks: access points and wireless range extenders.

1a. Access Points

Access points (APs), like wireless networks, help users access a network. APs could be computers or mobile devices, and soon home appliances will have IP addresses and be able to communicate wirelessly. The ease of communicating on a network using a wireless access point (WAP) instead of having to use an Ethernet cable enables end-user mobility.

The diagram below shows how an AP would look in a small network, such as a home.



An AP is a device that permits wireless devices to connect to a network. The wireless client **modulates** a digital signal to an analog signal, which the AP can read and demodulate back to a digital signal. A WAP is the wireless equivalent of a switch or router, and it provides the same services to the network. An AP may operate at half-duplex, but some wireless standards provide full-duplex-type connectivity. Currently, a wireless host typically operates at a lower speed, and with less security, than a wired Ethernet network connection.

TERMS TO KNOW

Access Point
A device that permits wireless devices to connect to a network.

Modulate
To vary the amplitude, frequency, or phase of a carrier wave in proportion to a source wave.

1b. Wireless Range Extenders

Wireless range extenders are used to extend wireless signals far from the AP. These are radios with antennas that receive the wireless signal from an AP and then transmit it to an area not covered by the AP. These devices should be placed so there is at least a 15% overlap of the coverage areas of the AP and the extender.

2. Media Access Control Protocols

In both wireless and wired environments that are shared media, frames from multiple devices could collide and destroy the data. Both wired and wireless environments use a **media access control protocol** to arbitrate access to the medium to help prevent collisions or, at the least, recover from them when they occur. A media access control protocol is a set of rules that enables multiple devices to share the physical medium of a network. In the following sections, we will look at the method used in each environment.

TERM TO KNOW

Media Access Control Protocol

A set of rules that enables multiple devices to share the physical medium of a network.

2a. CSMA/CA

When the device transmits the frame onto a wireless network, carrier-sense multiple access with collision avoidance (CSMA/CA) or the contention method is used. The method starts with a check of the medium (in this case, a check of the radio frequency) for activity called physical carrier sense. If the medium is not clear, the station will implement an internal countdown mechanism called the random back-off algorithm. This counter will have started counting down after the last time this station was allowed to transmit. All stations will begin the countdown on their own individual timers. When a station’s timer expires, it is allowed to send the information. If the physical carrier is clear and the countdown timer is at zero, the station will send.

The frame will go to the AP. The AP will acknowledge the reception of the frame. If the frame is destined for another wireless station located on this WLAN, the AP will forward the frame to it. When this occurs, the AP will follow the same CSMA/CA contention method to get the frame onto the wireless medium. Because it is impossible for wireless stations to detect collisions, another contention method is required to arbitrate access to the network. The method is called **carrier-sense multiple access with collision avoidance (CSMA/CA)**.

Describing CSMA/CA Operation

CSMA/CA operation requires a more involved process of checking for existing wireless traffic before a frame can be transmitted wirelessly. The stations (including the AP) must also acknowledge all frames.

STEP BY STEP

The steps in the process are as follows:

1. Laptop A has a frame to send to Laptop B. Before sending the frame, Laptop A must check for traffic in two ways. First, it performs carrier sense, which means it listens to determine whether any radio waves are being received on its transmitter.
2. If the channel is *not* clear (the traffic is being transmitted), Laptop A will decrement an internal countdown mechanism called the random back-off algorithm. This counter will have started counting down after the last time this station was allowed to transmit. All stations will begin the countdown on their own individual timers at randomly set values. When a station’s timer expires, it is allowed to send the frame.
3. If Laptop A checks for carrier sense, and there is no traffic and its timer hits zero, it will send the frame.
4. The frame goes to the AP.
5. The AP sends an acknowledgment back to Laptop A. Until that acknowledgment is received by Laptop A, all other stations must remain silent. The AP will cache the frame, where it already may have other cached frames that need to be relayed to other stations. Each frame that the AP needs to relay must wait its turn to be sent using the same mechanism as the station’s.

6. When the frame's turn comes up in the cache queue, the frame from Laptop A is relayed to Laptop B.
7. Laptop B sends an acknowledgment back to the AP. Until that acknowledgment is received by the AP, all other stations must remain silent.

When you consider that this process has to occur for every single frame and that there are many other frame types used by the AP to manage the other functions of the network that also compete for air time, it is no wonder that the actual **throughput** on a wireless LAN is typically about half the advertised rate.

TERMS TO KNOW

Carrier-Sense Multiple Access with Collision Avoidance (CSMA/CA)
A media access control protocol for Wi-Fi networks.

Throughput
The rate at which data are transferred through a system.

2b. CSMA/CD

When the device transmits the frame onto a wired network, the CSMA/CD contention method is used. This method is more efficient, because it is possible for wired computers to detect collisions, whereas wireless stations cannot. When a host's or router's interface needs to send a frame, it checks the wire; if no traffic is detected, it sends the frame without checking a random back-off timer.

However, it continues to listen, and if it detects that a collision has occurred, it sends out a jam signal that requires all stations to stop transmitting. Then, the two computers that were involved in the collision will both wait a random amount of time (that each will arrive at independently) and will resend the frame. So, instead of using a random back-off algorithm every time a transmission occurs, Ethernet uses its ability to detect collisions and uses this timer only when required, which makes the process more efficient.

Describing CSMA/CD Operation

The contention method used in wired Ethernet networks is called **carrier-sense multiple access with collision detection (CSMA/CD)**. It has mechanisms that help minimize but not eliminate collisions.

STEP BY STEP

Its operation is as follows:

1. When a device needs to transmit, it checks the wire. If a transmission is already underway, the device can tell.
2. If the wire is clear, the device will transmit. Even as it is transmitting, it is performing carrier sense.
3. If another host is sending information simultaneously, there will be a collision. The collision will be detected by both devices through carrier sense.
4. Both devices will issue a jam signal to all the other devices, which indicates to them to not transmit.
5. Then, both devices will increment a retransmission counter. This is a cumulative total of the number of times this frame has been transmitted and a collision has occurred. There is a maximum number at which the device aborts the transmission of the frame.

6. Both devices will calculate a random amount of time and will wait that amount of time before transmitting again. This calculation is called a random back-off.
7. In most cases, because both devices choose random amounts of time to wait, another collision will not occur.

TERM TO KNOW

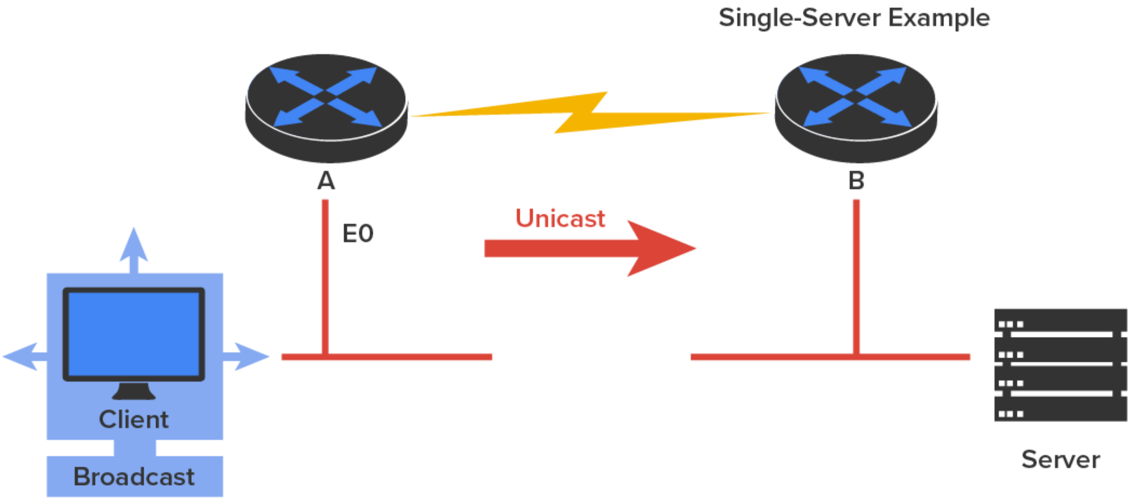
Carrier-Sense Multiple Access with Collision Detection (CSMA/CD)
A media access control protocol for Ethernet networks.

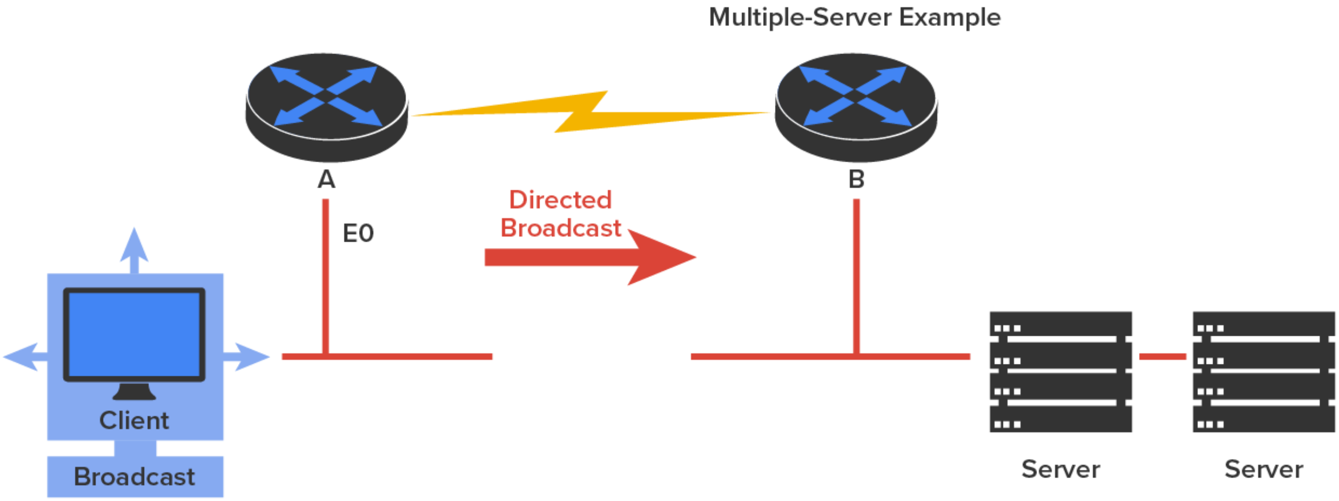
3. Dynamic Host Configuration Protocol Server (DHCP)

Even though we are going to get into the finer points of **Dynamic Host Configuration Protocol (DHCP)** later in the course, it may be helpful to get some basic insight into this server service here. DHCP servers automatically assign IP addresses and other information to a host computer. An alternative method known as static IP addressing requires each host to be configured manually. DHCP works well in any network environment and allows all types of hardware to be employed as a DHCP server, including switches, hubs, bridges, repeaters, and routers.

DHCP works like this: A DHCP server receives a request for IP information from a DHCP client using a broadcast. The administrator configures the DHCP server with a pool of addresses that it uses for this purpose.

If the DHCP server is not on the same segment as the DHCP client, the server will not receive the broadcast, because by default, routers will not forward broadcasts, as shown in the diagram below.

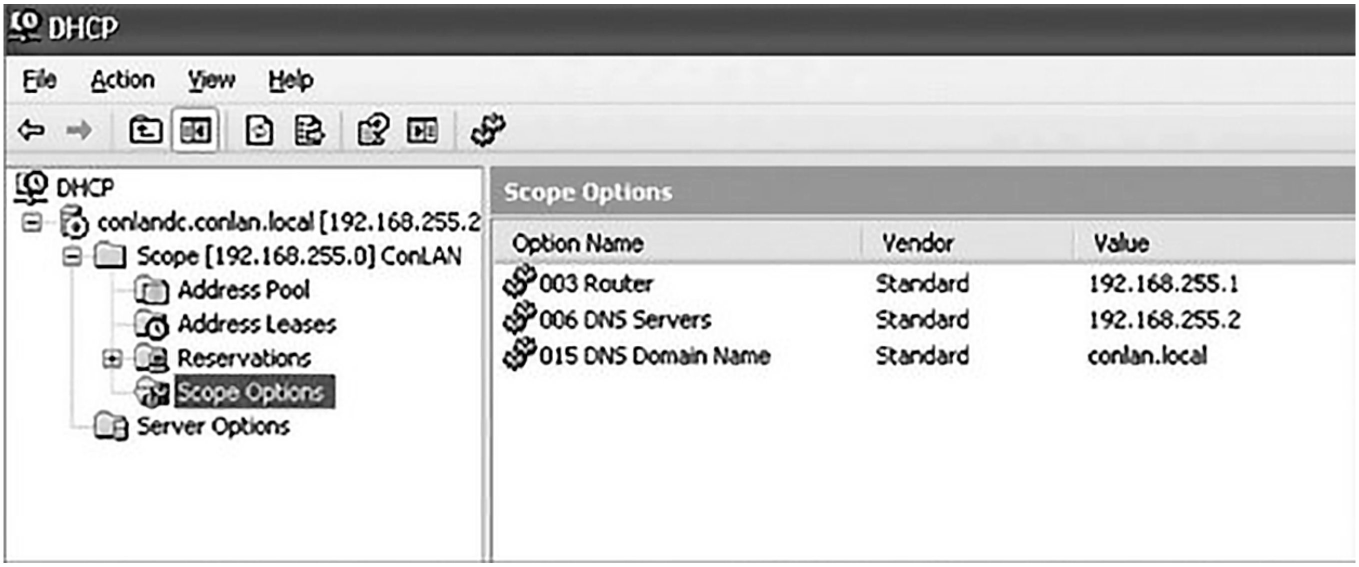




There's a way around this problem, however. In the diagram above, Router A is configured with the IP helper address command on Interface E0 of the router. Whenever Interface E0 receives a broadcast request, Router A will forward that request as a unicast (which means that instead of a broadcast, the packet now has the destination IP address of the DHCP server).

So, as shown in the diagram, you can configure Router A to forward these requests and even use multiple DHCP servers for redundancy. This works because the router has been configured to forward the request to a single server using a unicast or by sending the request to multiple servers via a directed broadcast.

The following screenshot shows a Windows server's DHCP configuration utility, where you can configure Scope Options.

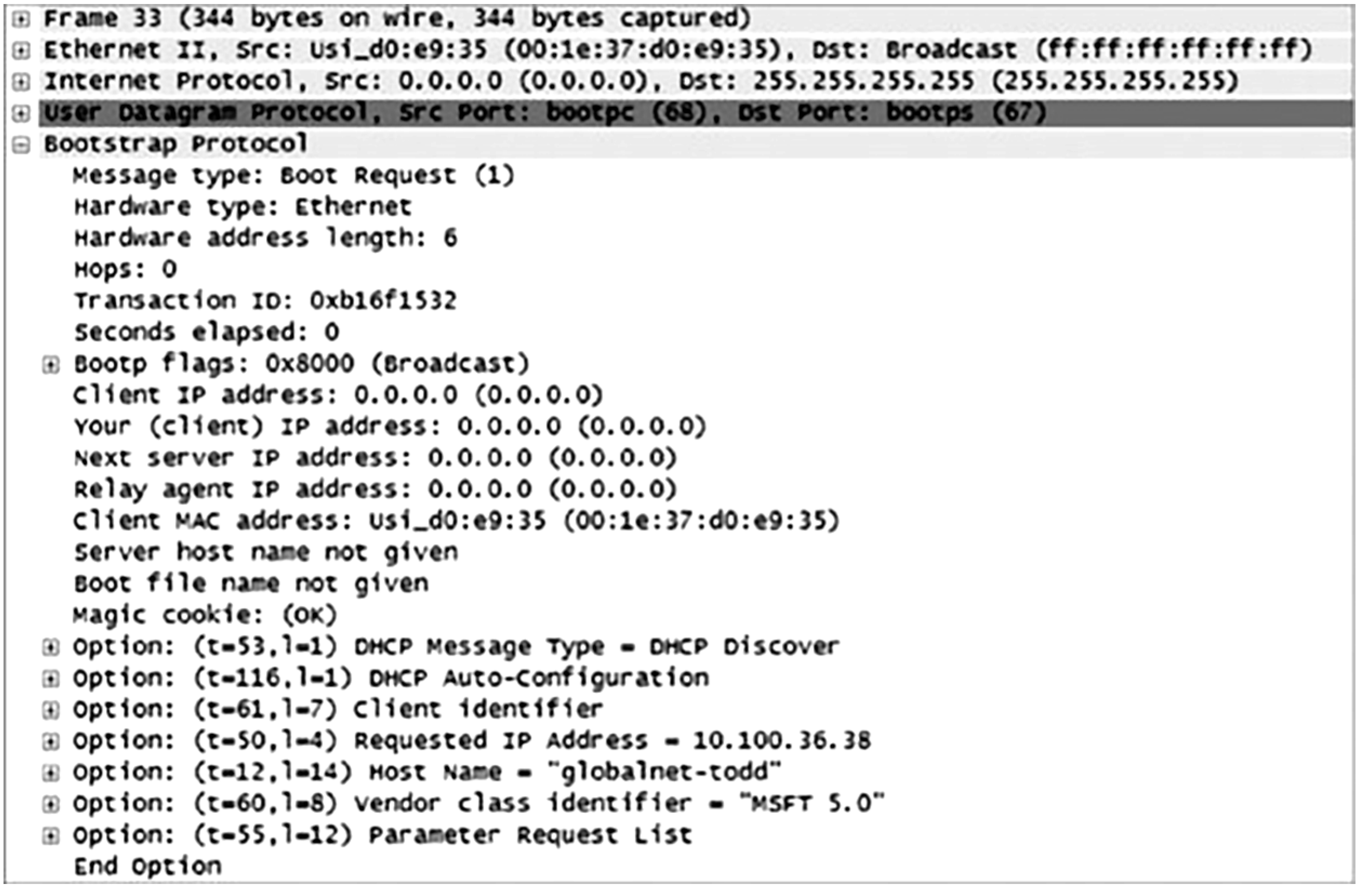


Option Name	Vendor	Value
003 Router	Standard	192.168.255.1
006 DNS Servers	Standard	192.168.255.2
015 DNS Domain Name	Standard	conlan.local

A **scope** is a range of IP addresses. Scope Options provide IP configuration for hosts on a specific subnet. Below Scope Options, you will find Server Options; these options provide IP information for all scopes configured on the server.

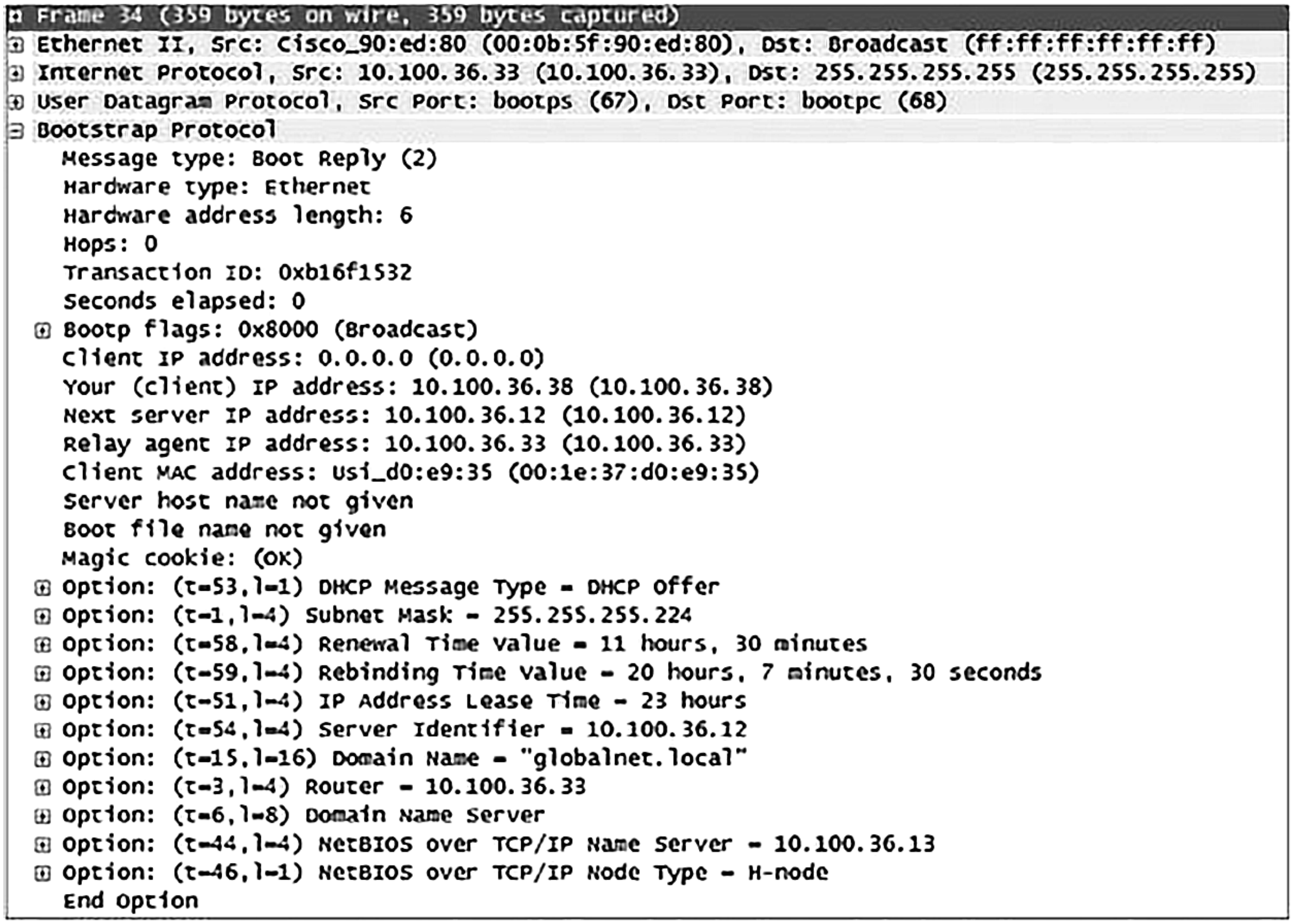
A DHCP client requests an IP address, a subnet mask, and a default gateway, and the DHCP server responds to the client request. You will learn about IP addressing later in the course. DHCP may also supply a lot of other information to the client as well.

Let us take a look at a DHCP client request on an analyzer. The screenshot below shows the options that the client is requesting from the DHCP server.



```
⊞ Frame 33 (344 bytes on wire, 344 bytes captured)
⊞ Ethernet II, Src: Usi_d0:e9:35 (00:1e:37:d0:e9:35), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
⊞ Internet Protocol, Src: 0.0.0.0 (0.0.0.0), Dst: 255.255.255.255 (255.255.255.255)
⊞ User Datagram Protocol, Src Port: bootpc (68), Dst Port: bootps (67)
⊟ Bootstrap Protocol
    Message type: Boot Request (1)
    Hardware type: Ethernet
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0xb16f1532
    Seconds elapsed: 0
  ⊞ Bootp flags: 0x8000 (Broadcast)
    Client IP address: 0.0.0.0 (0.0.0.0)
    Your (client) IP address: 0.0.0.0 (0.0.0.0)
    Next server IP address: 0.0.0.0 (0.0.0.0)
    Relay agent IP address: 0.0.0.0 (0.0.0.0)
    Client MAC address: Usi_d0:e9:35 (00:1e:37:d0:e9:35)
    Server host name not given
    Boot file name not given
    Magic cookie: (OK)
  ⊞ Option: (t=53,l=1) DHCP Message Type = DHCP Discover
  ⊞ Option: (t=116,l=1) DHCP Auto-Configuration
  ⊞ Option: (t=61,l=7) Client identifier
  ⊞ Option: (t=50,l=4) Requested IP Address = 10.100.36.38
  ⊞ Option: (t=12,l=14) Host Name = "globalnet-todd"
  ⊞ Option: (t=60,l=8) Vendor class identifier = "MSFT 5.0"
  ⊞ Option: (t=55,l=12) Parameter Request List
    End Option
```

First, you can see that the client is “requesting” a certain IP address, because this is the IP address it received from the server the last time it requested an IP address. Take a look at what the server’s response is. The screenshot below shows the DHCP server response.



```
⊞ Frame 34 (359 bytes on wire, 359 bytes captured)
⊞ Ethernet II, Src: Cisco_90:ed:80 (00:0b:5f:90:ed:80), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
⊞ Internet Protocol, Src: 10.100.36.33 (10.100.36.33), Dst: 255.255.255.255 (255.255.255.255)
⊞ User Datagram Protocol, Src Port: bootps (67), Dst Port: bootpc (68)
⊟ Bootstrap Protocol
    Message type: Boot Reply (2)
    Hardware type: Ethernet
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0xb16f1532
    Seconds elapsed: 0
  ⊞ Bootp flags: 0x8000 (Broadcast)
    Client IP address: 0.0.0.0 (0.0.0.0)
    Your (client) IP address: 10.100.36.38 (10.100.36.38)
    Next server IP address: 10.100.36.12 (10.100.36.12)
    Relay agent IP address: 10.100.36.33 (10.100.36.33)
    Client MAC address: Usi_d0:e9:35 (00:1e:37:d0:e9:35)
    Server host name not given
    Boot file name not given
    Magic cookie: (OK)
  ⊞ Option: (t=53,l=1) DHCP Message Type = DHCP Offer
  ⊞ Option: (t=1,l=4) Subnet Mask = 255.255.255.224
  ⊞ Option: (t=58,l=4) Renewal Time Value = 11 hours, 30 minutes
  ⊞ Option: (t=59,l=4) Rebinding Time Value = 20 hours, 7 minutes, 30 seconds
  ⊞ Option: (t=51,l=4) IP Address Lease Time = 23 hours
  ⊞ Option: (t=54,l=4) Server Identifier = 10.100.36.12
  ⊞ Option: (t=15,l=16) Domain Name = "globalnet.local"
  ⊞ Option: (t=3,l=4) Router = 10.100.36.33
  ⊞ Option: (t=6,l=8) Domain Name Server
  ⊞ Option: (t=44,l=4) NetBIOS over TCP/IP Name Server = 10.100.36.13
  ⊞ Option: (t=46,l=1) NetBIOS over TCP/IP Node Type = H-node
    End Option
```

The client is going to get the IP address that it asked for (10.100.36.38), a subnet mask of 255.255.255.224, a lease time of 23 hr (the amount of time before the IP address and other DHCP information expire on the client), the IP address of the DHCP server, the default gateway (router), the **Domain Name Service (DNS)** server IP address (it gets two), the domain name used by DNS, and some network basic input/output system (NetBIOS) information (used by Windows for name resolution).

KEY CONCEPT

The lease time is important and can even be used to tell you if you have a DHCP problem or, more specifically, if the DHCP server is no longer handing out IP addresses to hosts. If hosts start failing to get onto the network one at a time as they try to get a new IP address while their lease time expires, you need to check your server settings.

TERMS TO KNOW

Dynamic Host Configuration Protocol (DHCP)

A protocol that computers use to decide on one IP address to use for dynamic IP addressing.

Scope

A range of IP addresses.

Domain Name Service (DNS)

A server that resolves host names into IP addresses.

SUMMARY

In this lesson, you learned about **WLAN devices**, particularly APs; two **media access control protocols**, CSMA/CA for wireless networks and CSMA/CD for wired Ethernet networks; and **Dynamic Host Configuration Protocol** (DHCP), which enables automatic IP address assignments for devices on a network.

Source: This content and supplemental material has been adapted from CompTIA Network+ Study Guide: Exam N10-007, 4th Edition. Source **Lammle: CompTIA Network+ Study Guide: Exam N10-007, 4th Edition - Instructor Companion Site (wiley.com)**

TERMS TO KNOW

Access Point
A device that permits wireless devices to connect to a network.

Carrier-Sense Multiple Access with Collision Avoidance (CSMA/CA)
A media access control protocol for Wi-Fi networks.

Carrier-Sense Multiple Access with Collision Detection (CSMA/CD)
A media access control protocol for Ethernet networks.

Domain Name Service (DNS)
A server that resolves host names into IP addresses.

Dynamic Host Configuration Protocol (DHCP)
A protocol that computers use to decide on one IP address to use for dynamic IP addressing.

Media Access Control Protocol
A set of rules that enables multiple devices to share the physical medium of a network.

Modulate
To vary the amplitude, frequency, or phase of a carrier wave in proportion to a source wave.

Scope
A range of IP addresses.

Throughput
The rate at which data are transferred through a system.