Todd Lammle’s CompTIA Network+
Chapter 5: Networking Devices

Instructor: Mansour Rousta Zadeh

Chapter 5 Objectives

The Following CompTIA Network+ Exam Objectives Are Covered in This Chapter:

- **3.1 Install, configure and differentiate between common network devices**
  - **Hub**
  - **Repeater**
  - **Modem**
  - **NIC**
  - **Media converters**
  - **Basic switch**
  - **Bridge**
  - **Wireless access point**
  - **Basic router**
  - **Basic firewall**
  - **Basic DHCP server**

Chapter 5 Objectives (cont.)

- **3.2 Identify the functions of specialized network devices**
  - **Multilayer switch**
  - **Content switch**
  - **IDS/IPS**
  - **Load balancer**
  - **Multifunction network devices**
  - **DNS server**
  - **Bandwidth shaper**
  - **Proxy server**
  - **CSU/DSU**

Common Network Devices

Here's a list of the devices we'll be covering in this chapter:

- Hub
- Repeater
- Modem
- Network Interface Card (NIC)
- Transceiver (media converter)
- Bridge
- Basic switch
- Wireless access point (AP)
- Basic router
- Basic firewall
- Basic Dynamic Host Configuration Protocol (DHCP) server
- Other specialized devices

A Basic Hub

As you learned earlier, a *hub* is the device that connects all the segments of the network together in a star topology Ethernet network. Every device in the network connects directly to the hub through a single cable and is used to connect multiple devices without segmenting a network.

Ethernet Repeater

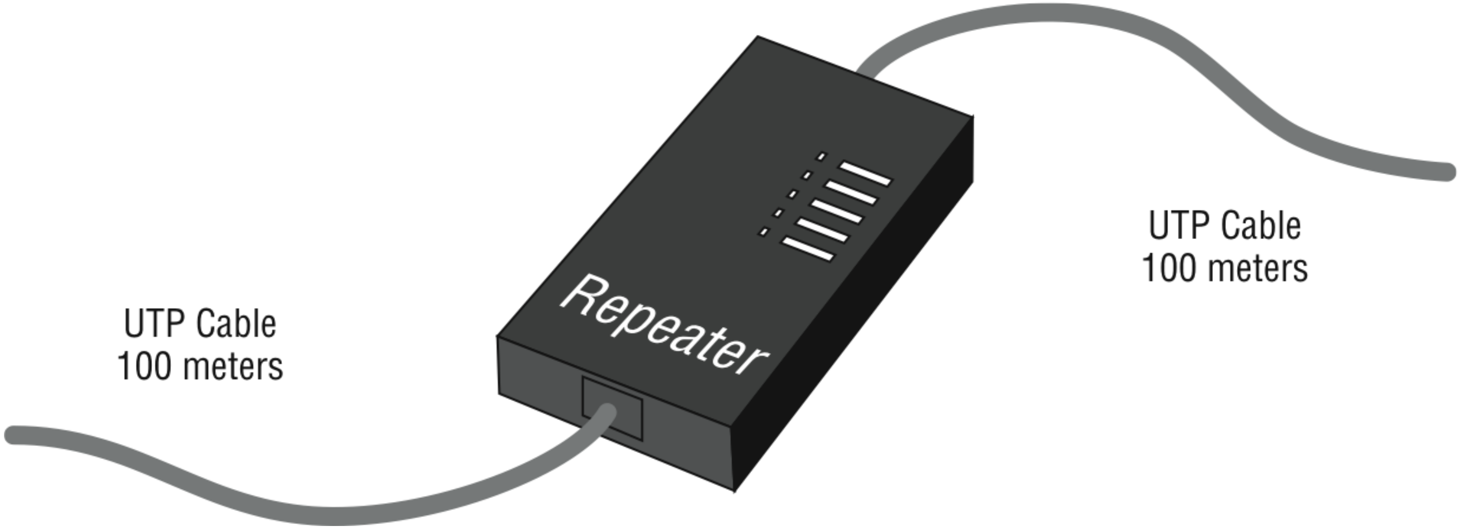


Figure 5.2 shows a repeater being used to connect two unshielded twisted-pair (UTP) connectors. This configuration will provide an extension to your Ethernet segment and give you a gain of another 100 meters (328 feet).

Modem

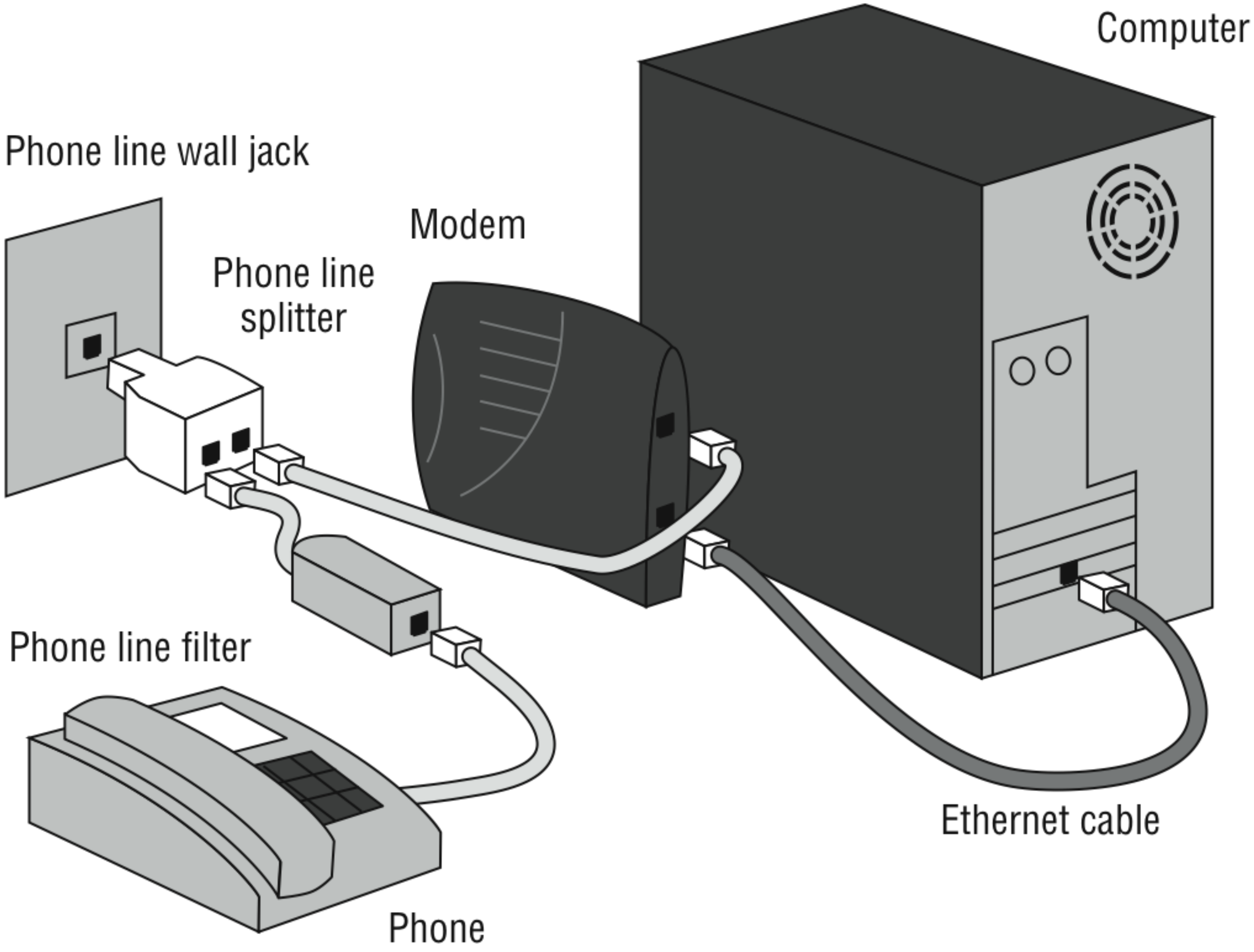
- A *modem* is a device that modulates digital data onto an analog carrier for transmission over an analog medium and then demodulates from the analog carrier to a digital signal again at the receiving end. A mouthful, yes, but the term *modem* is actually an acronym that stands for MOdulator/DEModulator. When you hear the term *modem,* three different types should come to mind:
  - Traditional (plain old telephone service [POTS])
  - DSL
  - Cable
- **Traditional (POTS)**

Most modems you find in computers today fall into the category of traditional modems. These modems convert the signals from your computer into those that travel over plain old telephone service (POTS) lines. The majority of modems that exist today are POTS modems, mainly because PC manufacturers include one with the computer, built right into the motherboard.

DSL

- Digital subscriber line (DSL) has replaced traditional modem access because it offers higher data throughput rates for a reasonable cost.
- Plus, you get to make regular, land-line phone calls while online.
- DSL uses higher frequencies (above 3200Hz) than regular voice phone calls use, which provides greater bandwidth than regular POTS modems—up to several megabits per second.

DSL


Computer
Phone line wall jack
Modem
Phone line splitter
Phone line filter
Ethernet cable
Phone

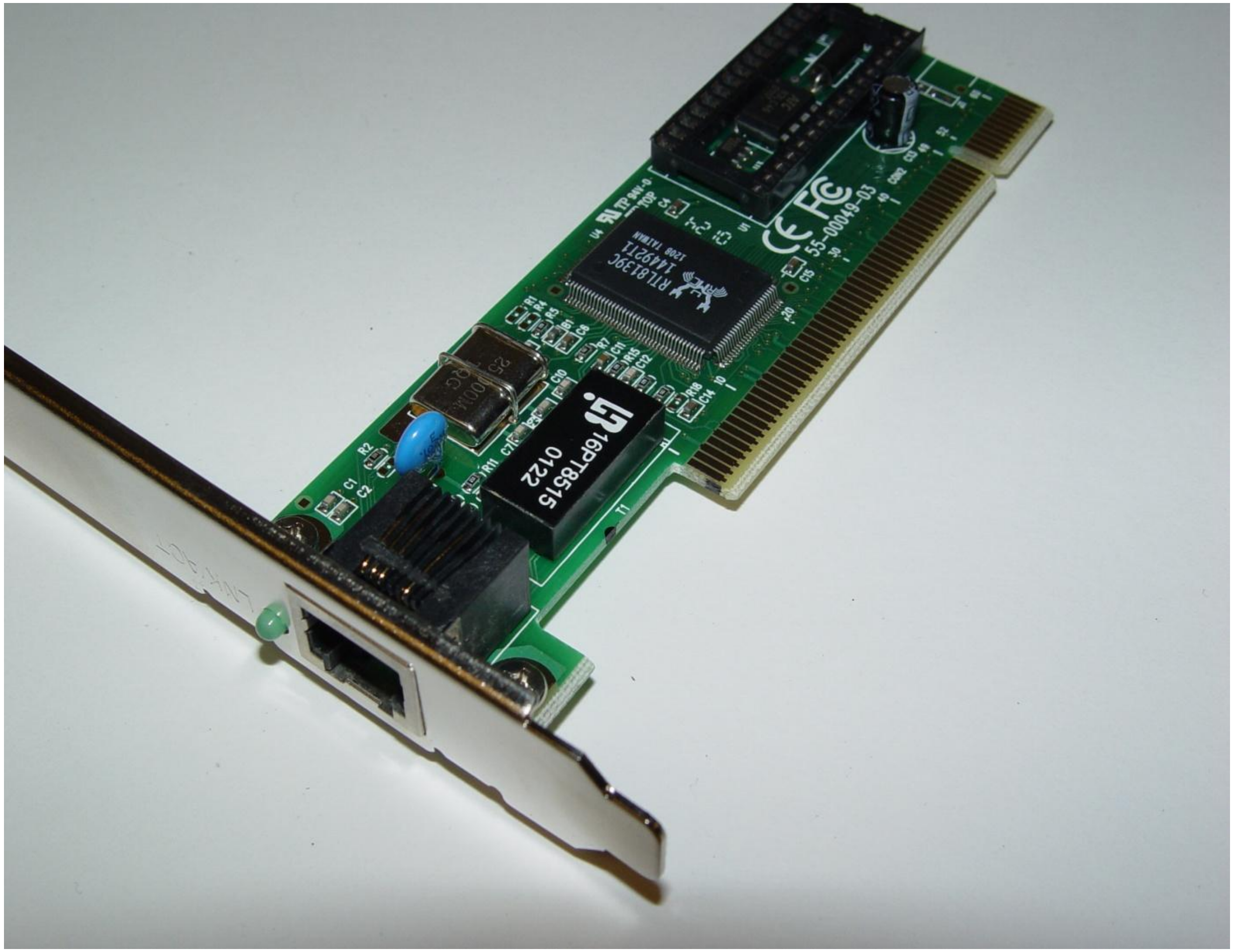
Cable

- Another popular high-speed Internet-access technology is cable-modem access. Cable modems connect an individual PC or network to the Internet using your television cable.
- The cable TV companies use their existing cable infrastructure to deliver data services on unused frequency bands.
- The cable modem itself is a fairly simple device. It has a standard coax connector on the back as well as an Ethernet port.

Network Interface Card (NIC)

- Those of you who aren't familiar with NICs probably want to be, at this point, so here goes: a *Network Interface Card* (NIC) is installed in your computer to connect, or interface, your computer to the network.
- It provides the physical, electrical, and electronic connections to the network media.
- A NIC either is an expansion card or is built right into the computer's motherboard.
- The NIC usually connects to the computer through *expansion slots* located on the motherboard that allow peripherals to be plugged in directly.
- In some notebook computers, NIC adapters can be connected to the printer port or through a PC card slot.

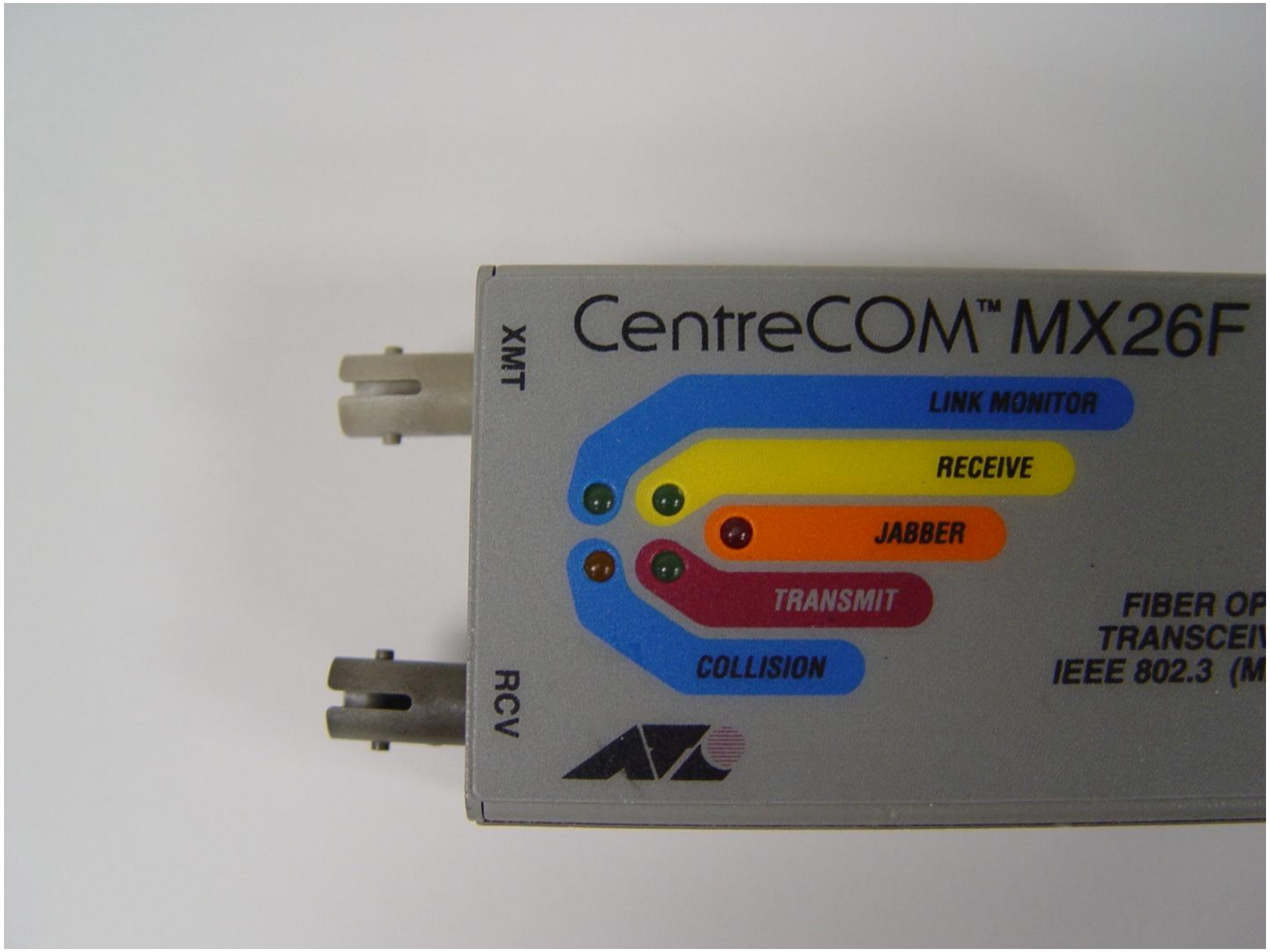
Network Interface Card (NIC)



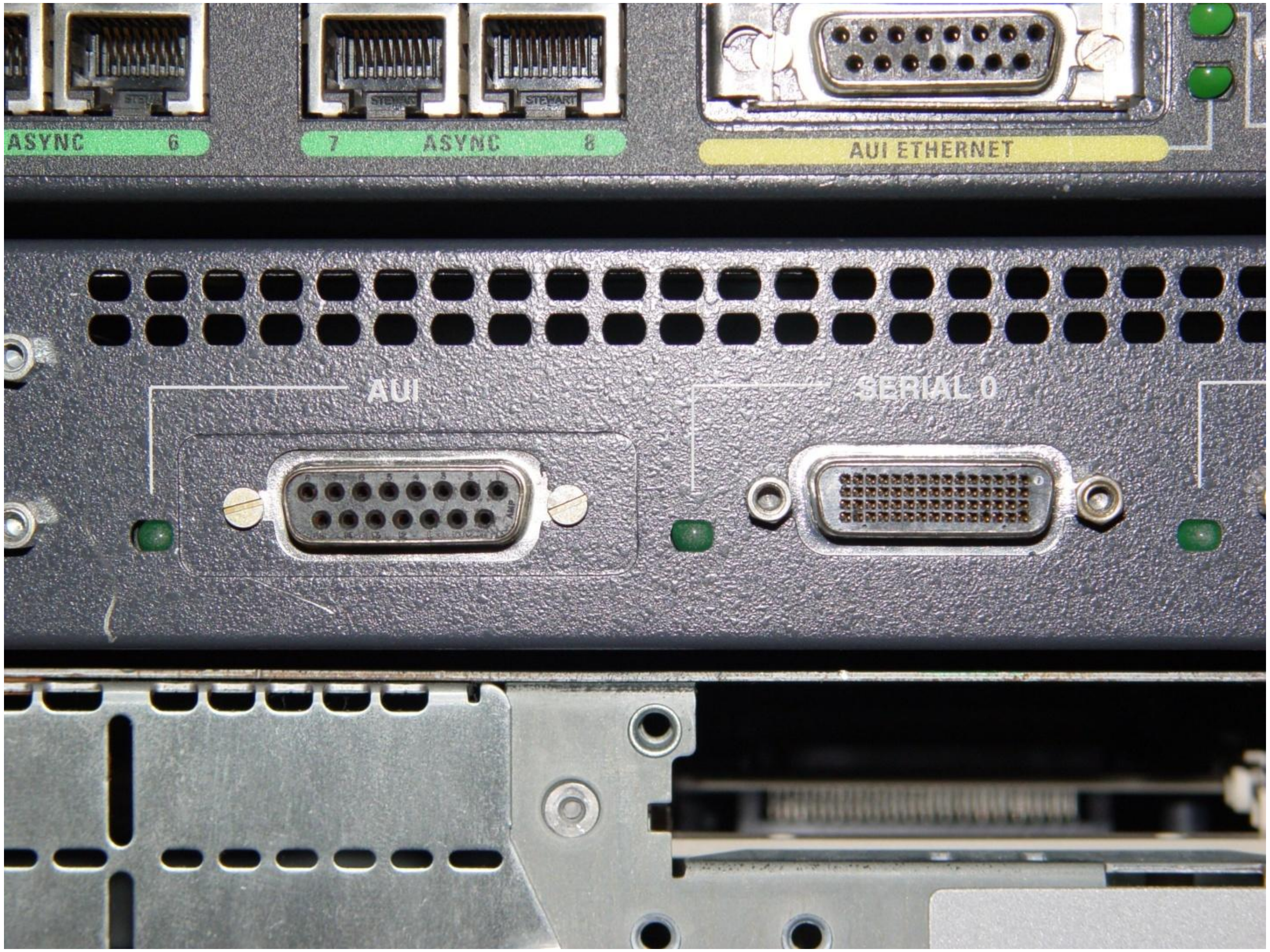
Transceiver

- Another small device that you might come across on a network is an external transceiver, otherwise known as a media converter.
- These simple devices allow a NIC or other networking device to connect to a different type of media than it was designed to connect to.
- Many hubs, switches, and NICs have special connectors that allow for this.

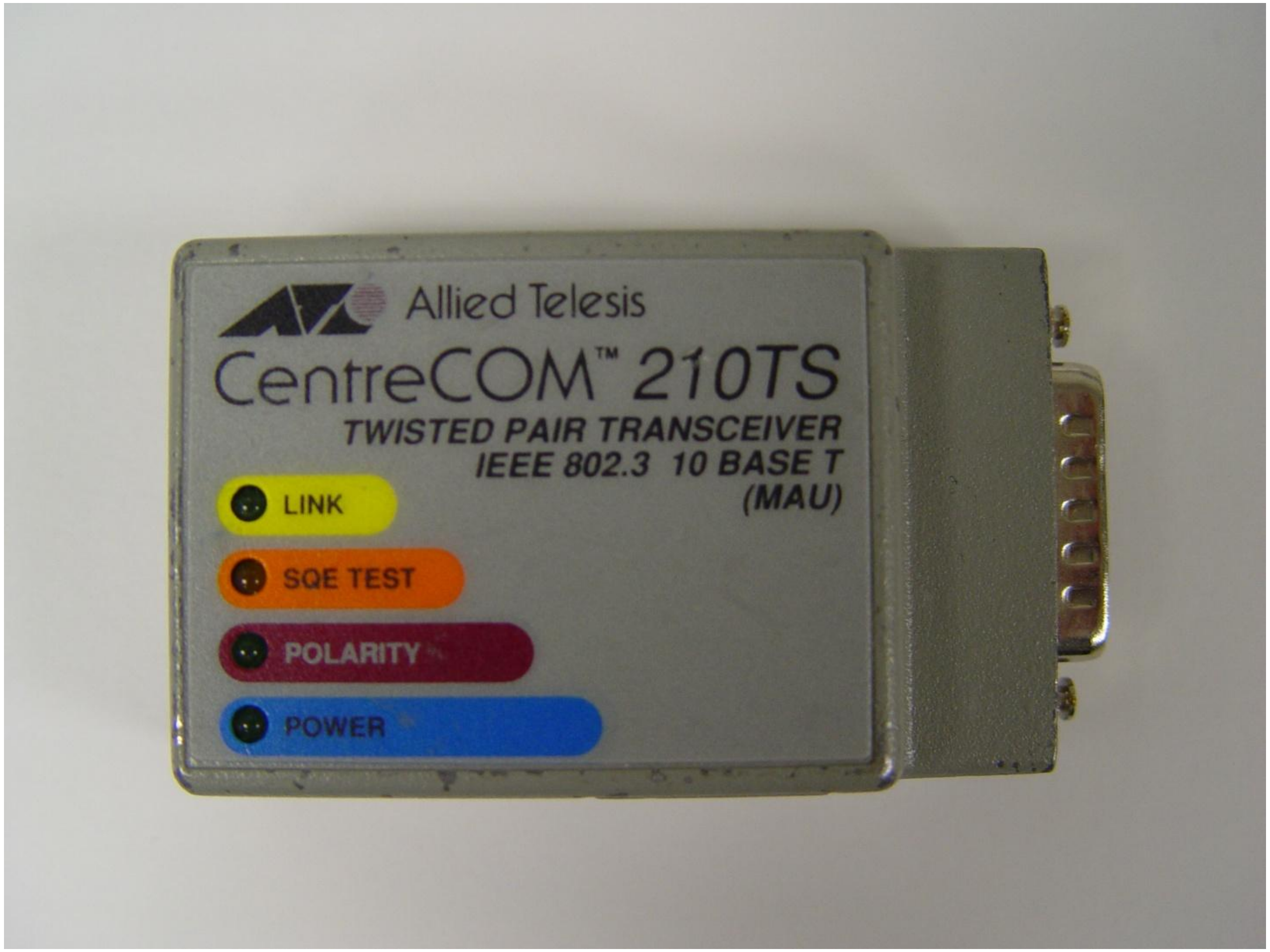
Transceiver Example



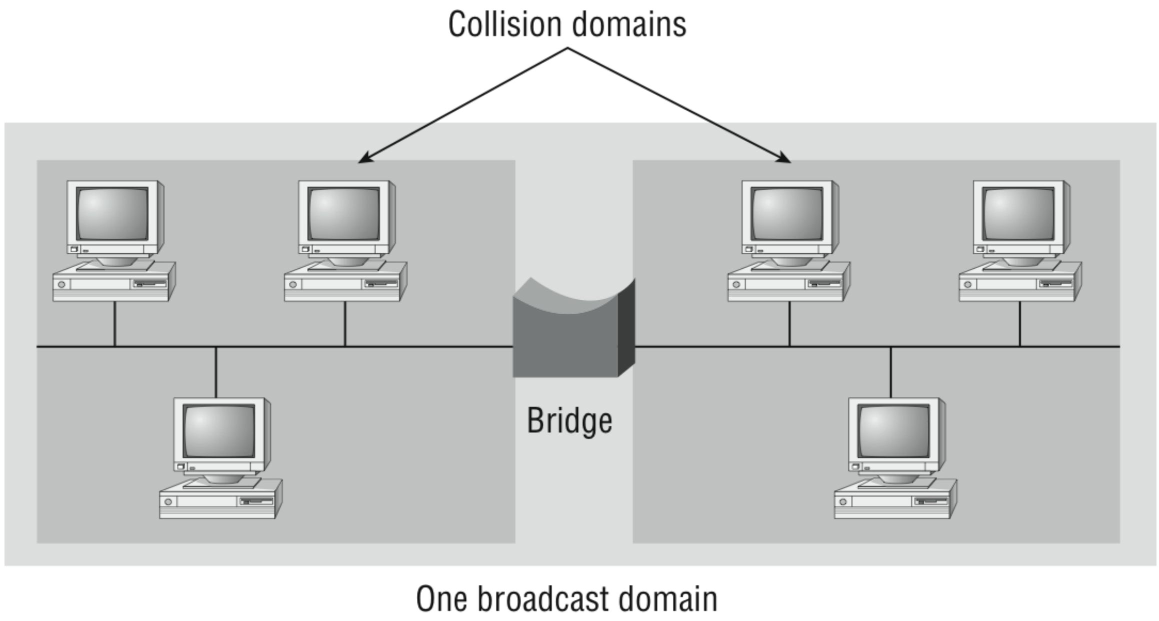
Router with AUI Connector



DIX Transceiver



Bridge



A *bridge*—specifically, a transparent bridge—is a network device that connects two similar network segments together. Its primary function is to keep traffic separated on either side of the bridge, breaking up collision domains.

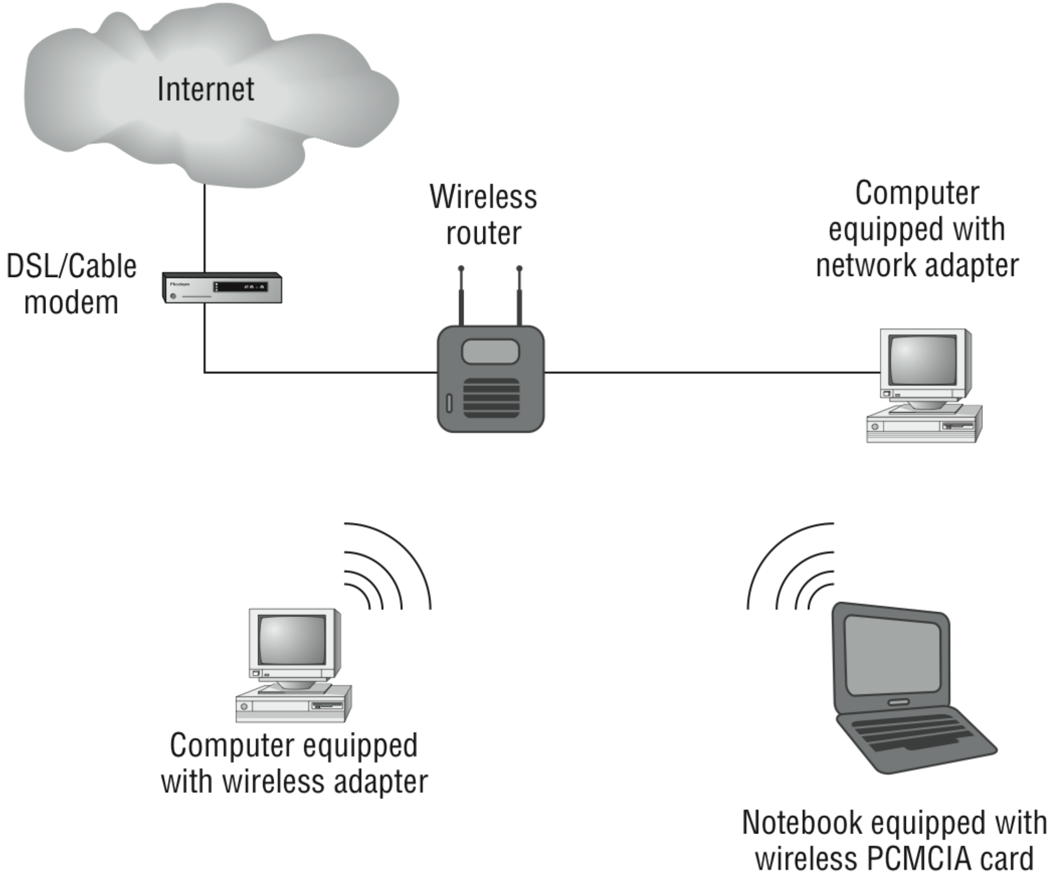
Switch

Switches connect multiple segments of a network together much like hubs do, but with three significant differences—a switch recognizes frames and pays attention to the source and destination MAC address of the incoming frame as well as the port on which it was received.

Access Point (P)

An *AP* allows mobile users to connect to a wired network wirelessly via radio frequency technologies. Using wireless technologies, APs also allow wired networks to connect to each other and are basically the wireless equivalent of hubs or switches because they can connect multiple wireless (and often wired) devices together to form a network.

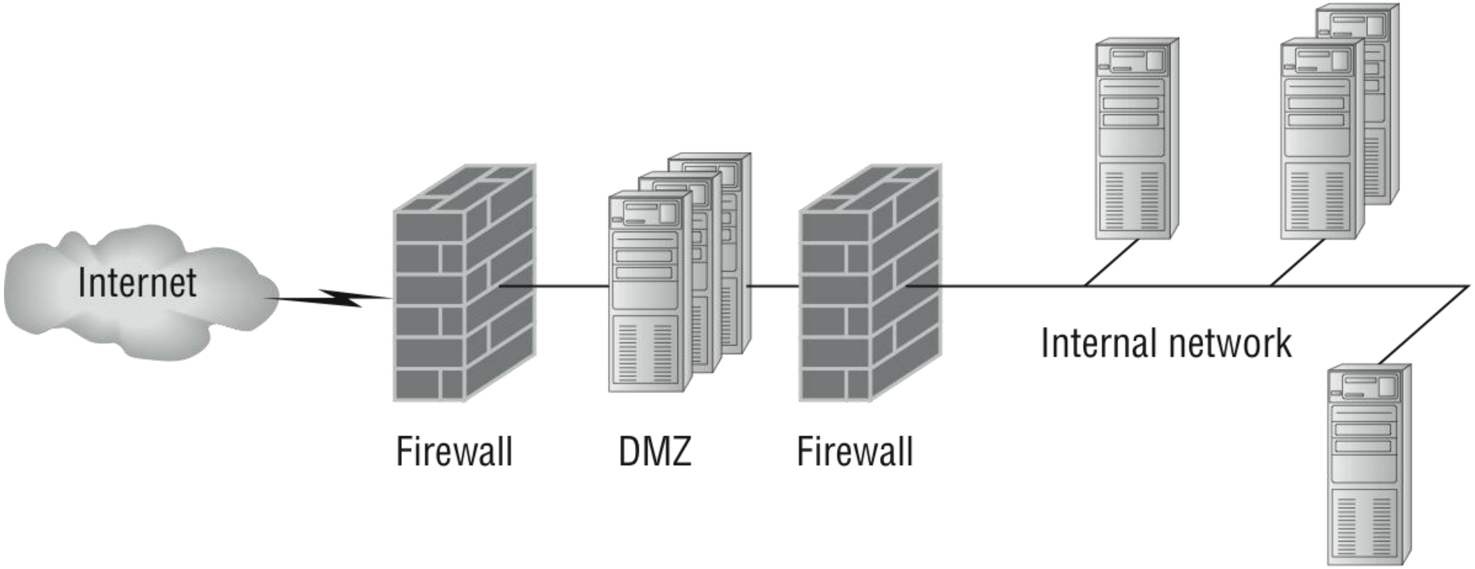
A Router Wired and Wireless


Internet
DSL/Cable modem
Wireless router
Computer equipped with network adapter
Computer equipped with wireless adapter
Notebook equipped with wireless PCMCIA card

Firewall

- Basically, firewalls are your network's security guards; and to be real, they're probably the most important thing to implement on your network.
- That's because today's networks are almost always connected to the Internet—a situation that makes security crucial!
- A firewall protects your LAN resources from invaders that prowl the Internet for unprotected networks, while simultaneously preventing all or some of your LAN's computers from accessing certain services on the Internet.
- You can employ them to filter packets based on rules that you or the network administrator create and configure to strictly delimit the type of information allowed to flow in and out of the network's Internet connection.

Firewall



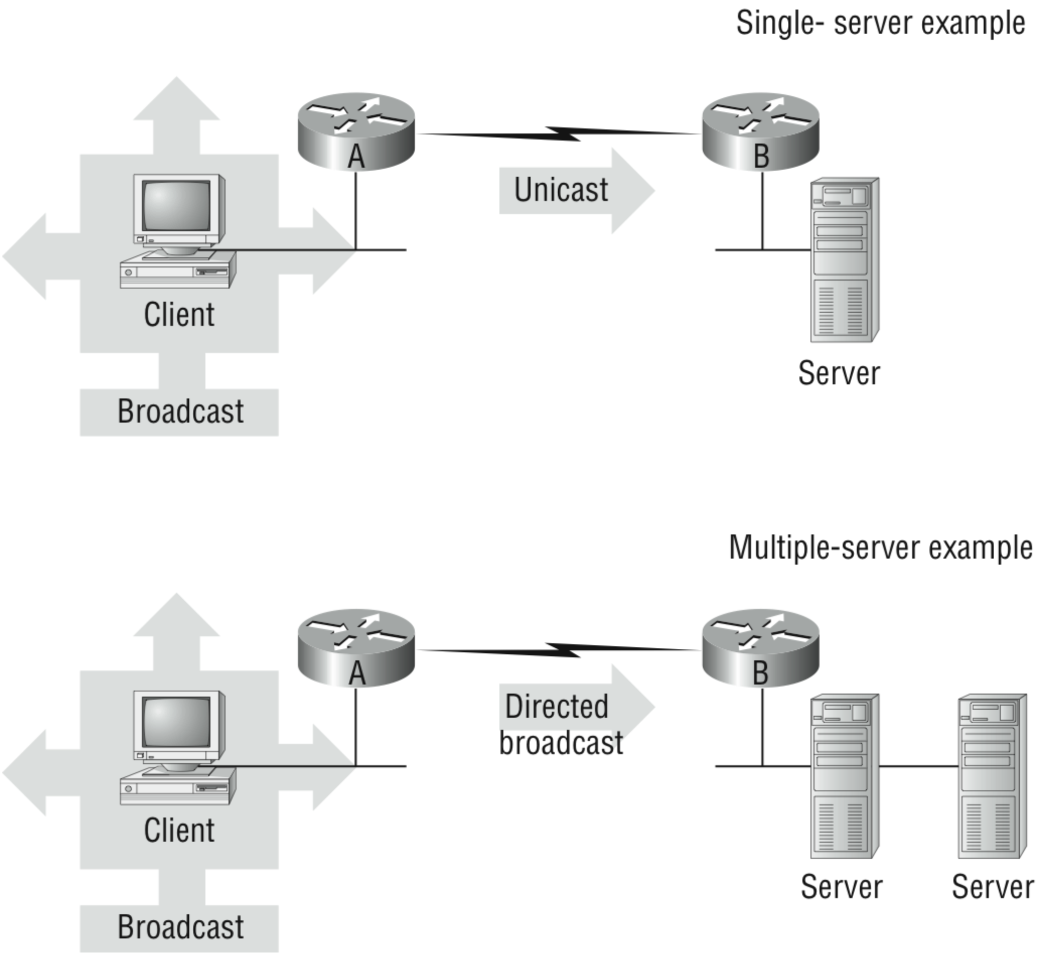
DHCP

- In essence, DHCP servers assign IP addresses to hosts. This protocol gives us a much easier way to administrate—by automatically providing IP information—than the alternative and tedious method known as static IP addressing, where we have to address each host manually.
- It works well in any network environment, from tiny to huge, and allows all types of hardware to be employed as a DHCP server, including routers.
- A DHCP server receives request for IP information from a DHCP client using a broadcast. The only hitch is that if the DHCP server isn't on the same segment as the DHCP client, the broadcast won't be received by the server because by default, routers won't forward broadcasts.

DHCP Client

- Shown in the figure on the next slide, 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 those requests as a unicast (meaning instead of a broadcast, the packet now has the destination IP address of the DHCP server).
- You can configure Router A to forward these requests and even use multiple DHCP servers for redundancy, if needed. 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.

DHCP Client

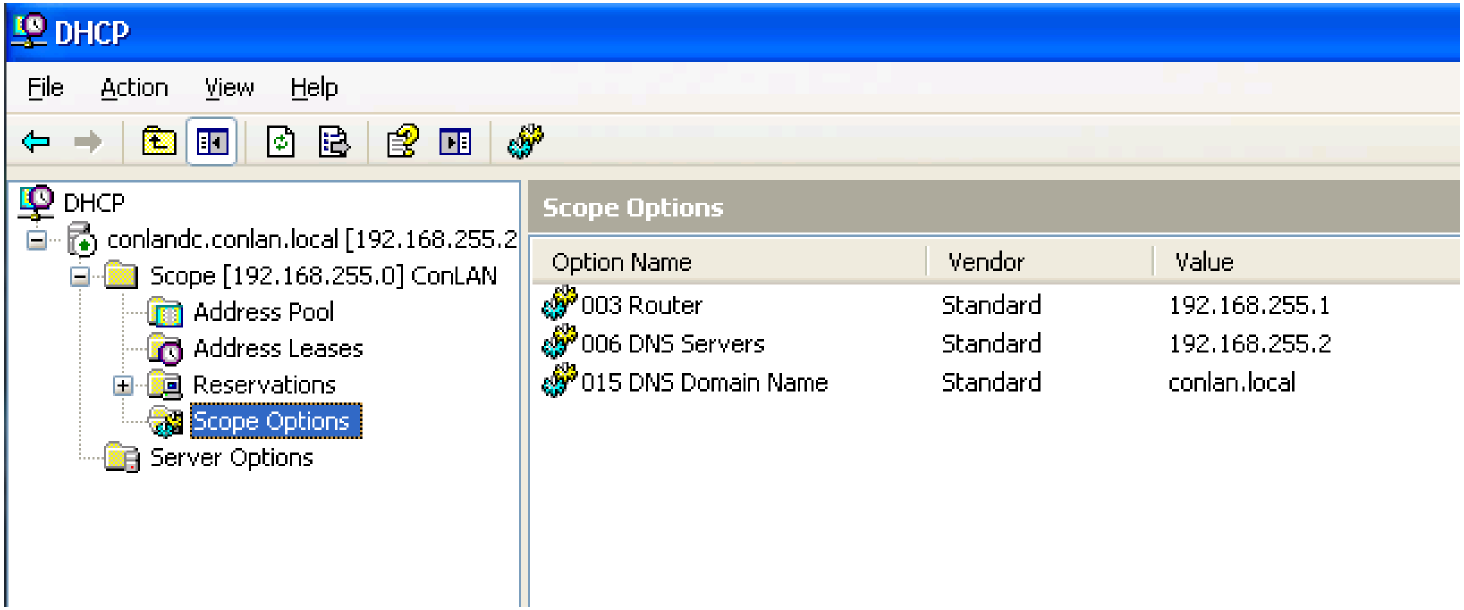


Single- server example
A
B
Unicast
Client
Broadcast
Server
Multiple-server example
A
B
Directed broadcast
Client
Broadcast
Server
Server

DHCP Server Options

- Scope Options provide IP configuration for hosts on a specific subnet. Below the Scope Options, you’ll find Server Options, which provide IP information for all scopes configured on the server.
- If I had just one Domain Name Service (DNS) server for the entire network, I’d configure the Server Options with my DNS server information; that DNS server information would then show up automatically in all scopes configured on my sever.

DHCP Server Options

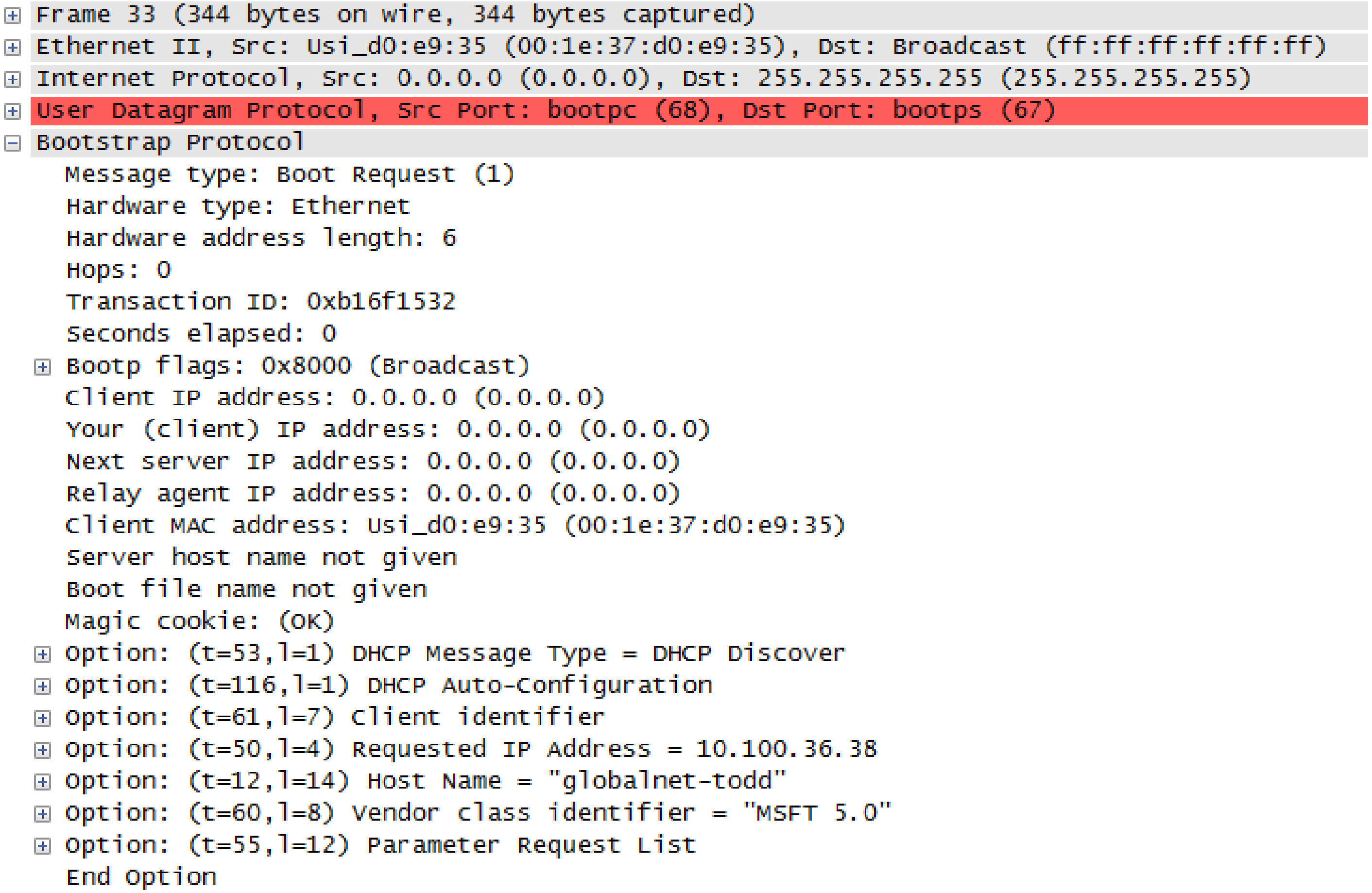


Option Name	Vendor	Value
003 Router	Standard	192.168.255.1
006 DNS Servers	Standard	192.168.255.2
015 DNS Domain Name	Standard	conlan.local

DHCP Client Request

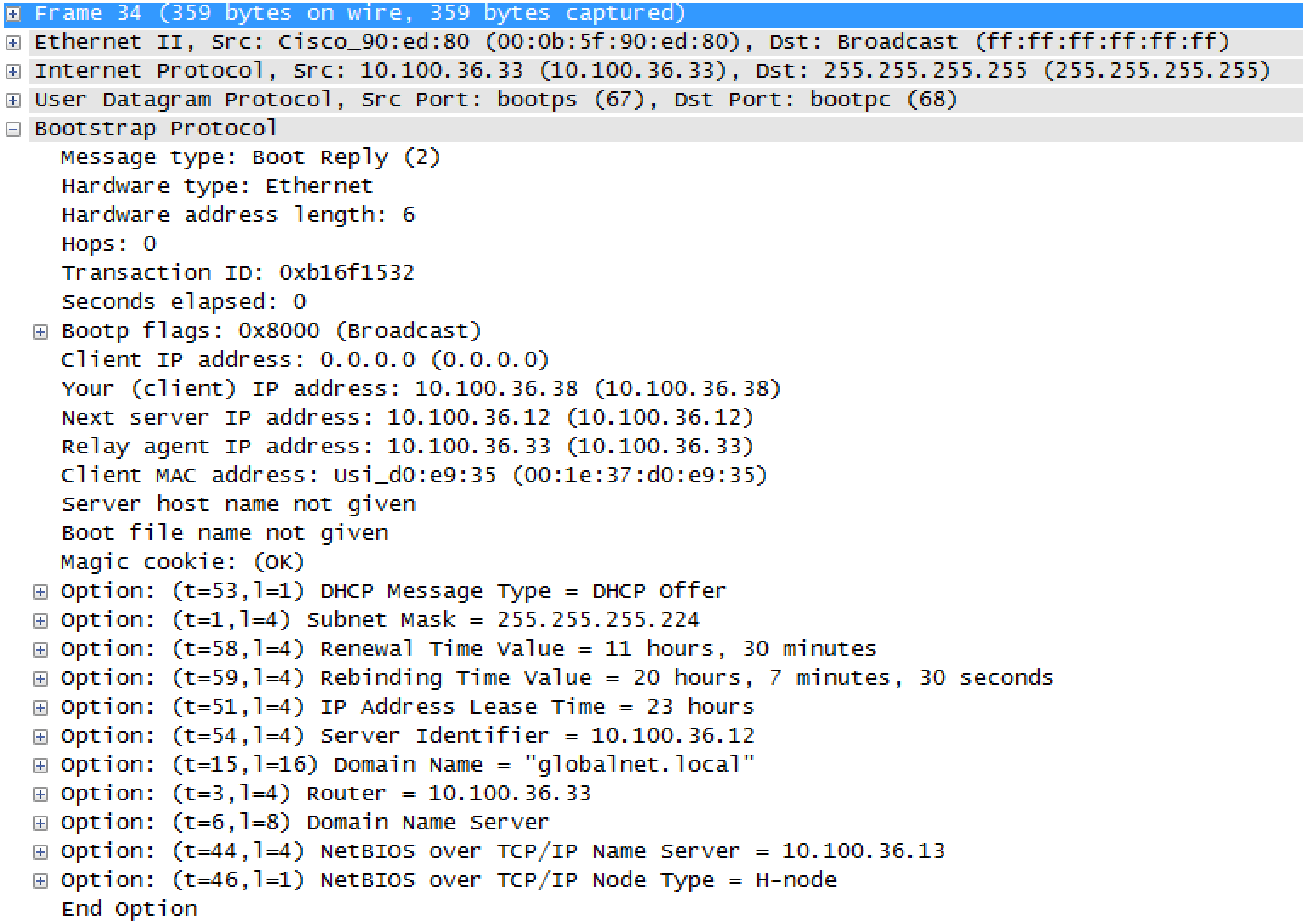
- So, what exactly does a DHCP client ask for, and what does a DHCP server provide? Is it just an IP address, a mask, and a default gateway? Let’s take a look at a DHCP client request on an analyzer on the next slide.

DHCP Client Request



```
⊞ 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
```

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
```

Specialized Devices

- Multilayer switch
- Content switch
- Intrusion Detection or Prevention System (IDS/IPS)
- Load balancer
- Multifunction network devices
- DNS server
- Bandwidth shaper
- Proxy server
- Channel Service Unit/Data Service Unit (CSU/DSU)

Multilayer Switch

- A *multilayer switch* (MLS) is a computer networking device that switches on Open Systems Interconnection (OSI) Layer 2 like an ordinary network switch but provides extra functions on higher OSI Layers, like Layer 3, for routing.
- A layer 3 switch (multilayer switch) can also be called a router, and vice versa.

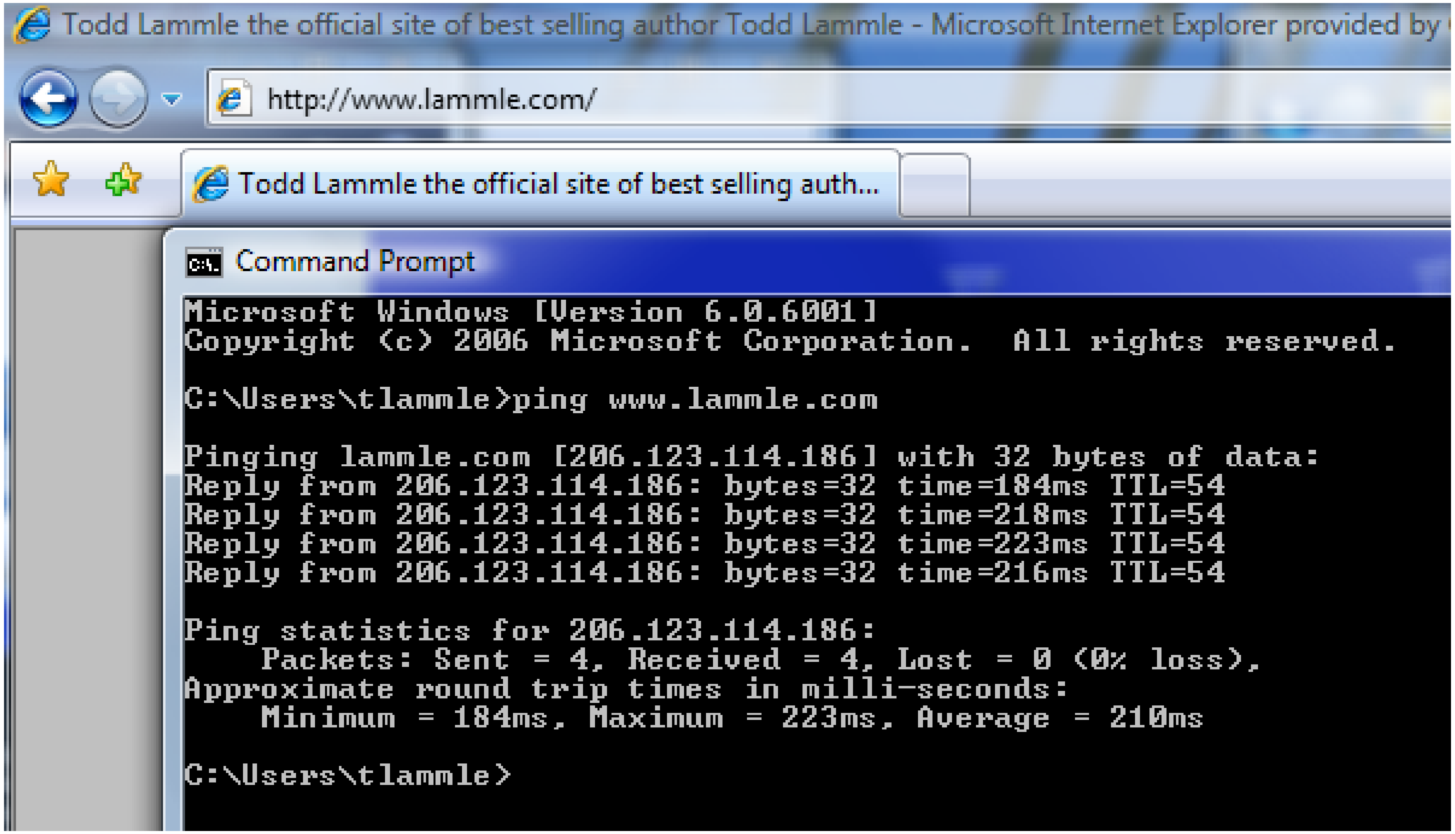
IDS/IPS

- *Intrusion Detection System (IDS)* is exactly what it sounds like—a powerful security tool that detects a plethora of nasty tactics that bad guys use to exploit systems, including unauthorized logins and privilege increases that can give them access to your sensitive data and files.
- An *Intrusion Prevention System (IPS)* provides computers with security by vigilantly watching for any suspicious and potentially malicious tactics. It works in real time and, as its name suggests, prevents these evil activities.

Domain Name Service (DNS)

- A *Domain Name Service (DNS) server* is one of the most important servers in your network and on the Internet as well.
- A host name is typically the name of a device that has a specific IP address; on the Internet, it is part of what is known as a fully qualified domain name (FQDN). An FQDN consists of a host name and a domain name.
- Your local ISP is probably a member of the .net domain, and your company is probably part of the .com domain. The .gov and .mil domains are reserved strictly for use by the government and the military within the United States.

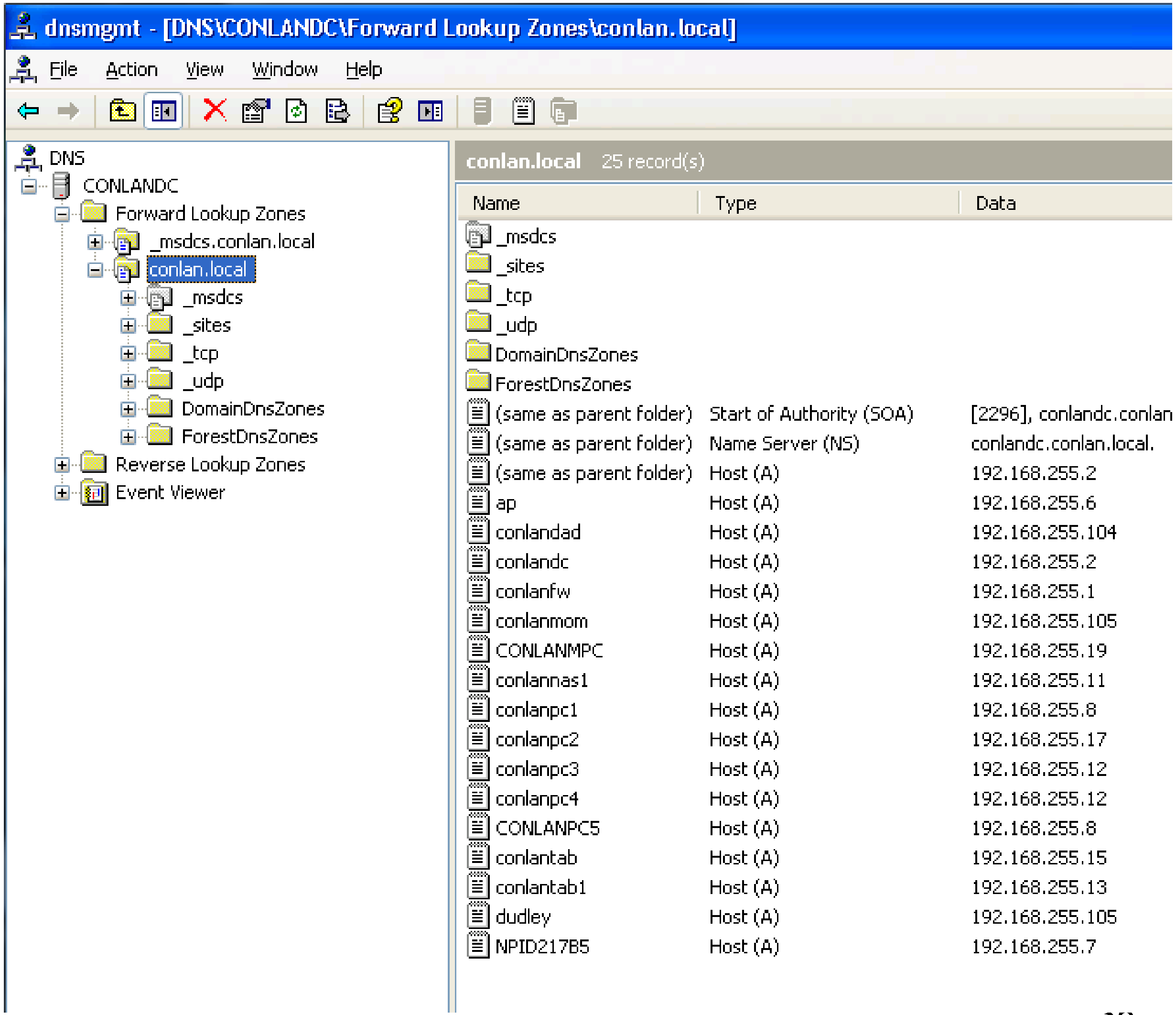
DNS Resolution Example



Todd Lammle the official site of best selling author Todd Lammle - Microsoft Internet Explorer provided by
http://www.lammle.com/
Todd Lammle the official site of best selling auth...
Command Prompt

```
Microsoft Windows [Version 6.0.6001]
Copyright (c) 2006 Microsoft Corporation.  All rights reserved.

C:\Users\tlammle>ping www.lammle.com

Pinging lammle.com [206.123.114.186] with 32 bytes of data:
Reply from 206.123.114.186: bytes=32 time=184ms TTL=54
Reply from 206.123.114.186: bytes=32 time=218ms TTL=54
Reply from 206.123.114.186: bytes=32 time=223ms TTL=54
Reply from 206.123.114.186: bytes=32 time=216ms TTL=54

Ping statistics for 206.123.114.186:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 184ms, Maximum = 223ms, Average = 210ms

C:\Users\tlammle>
```

DNS Server Config



- DNS
  - CONLANDC
    - Forward Lookup Zones
      - _msdcs.conlan.local
      - conlan.local
        - _msdcs
        - _sites
        - _tcp
        - _udp
        - DomainDnsZones
        - ForestDnsZones
    - Reverse Lookup Zones
    - Event Viewer

conlan.local 25 record(s)

Name	Type	Data
_msdcs		
_sites		
_tcp		
_udp		
DomainDnsZones		
ForestDnsZones		
(same as parent folder)	Start of Authority (SOA)	[2296], conlandc.conlan
(same as parent folder)	Name Server (NS)	conlandc.conlan.local.
(same as parent folder)	Host (A)	192.168.255.2
ap	Host (A)	192.168.255.6
conlandad	Host (A)	192.168.255.104
conlandc	Host (A)	192.168.255.2
conlanfw	Host (A)	192.168.255.1
conlanmom	Host (A)	192.168.255.105
CONLANMPC	Host (A)	192.168.255.19
conlannas1	Host (A)	192.168.255.11
conlanpc1	Host (A)	192.168.255.8
conlanpc2	Host (A)	192.168.255.17
conlanpc3	Host (A)	192.168.255.12
conlanpc4	Host (A)	192.168.255.12
CONLANPC5	Host (A)	192.168.255.8
conlantab	Host (A)	192.168.255.15
conlantab1	Host (A)	192.168.255.13
dudley	Host (A)	192.168.255.105
NPID217B5	Host (A)	192.168.255.7

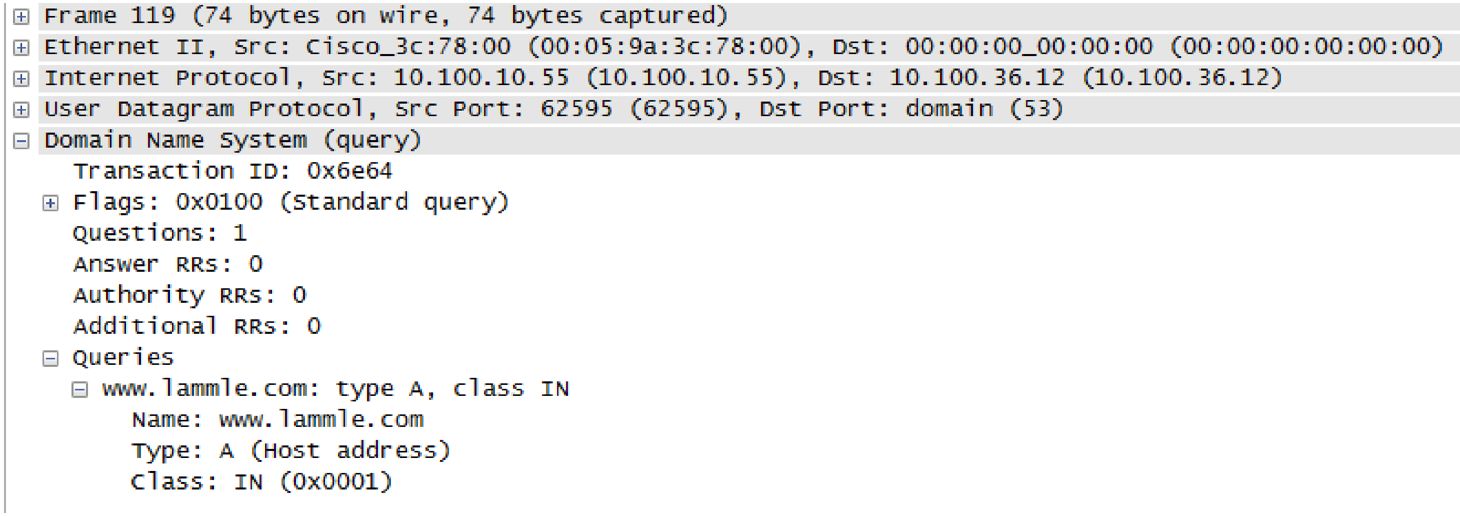
Mail Exchanger (MX)

- Here are some sample mail-exchange records:

```
hostname.company.com.  IN   MX   10 mail.company.com
hostname.company.com.  IN   MX   20 mail2.company.com
hostname.company.com.  IN   MX   30 mail3.company.com
```

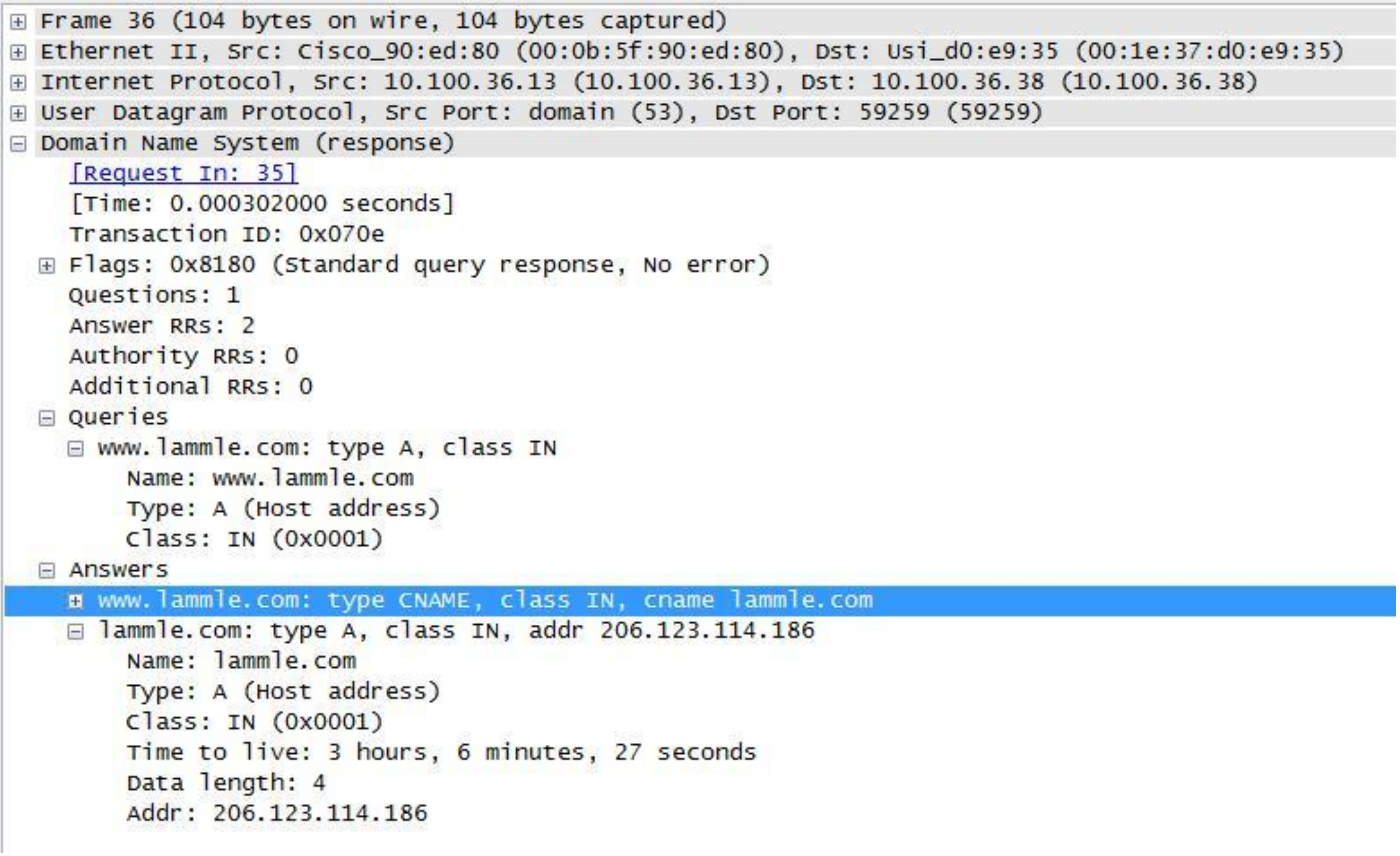
- In this example, if the first mail exchanger, mail.company.com, does not respond, the second one, mail2.company.com, is tried, and so on.

DNS Query



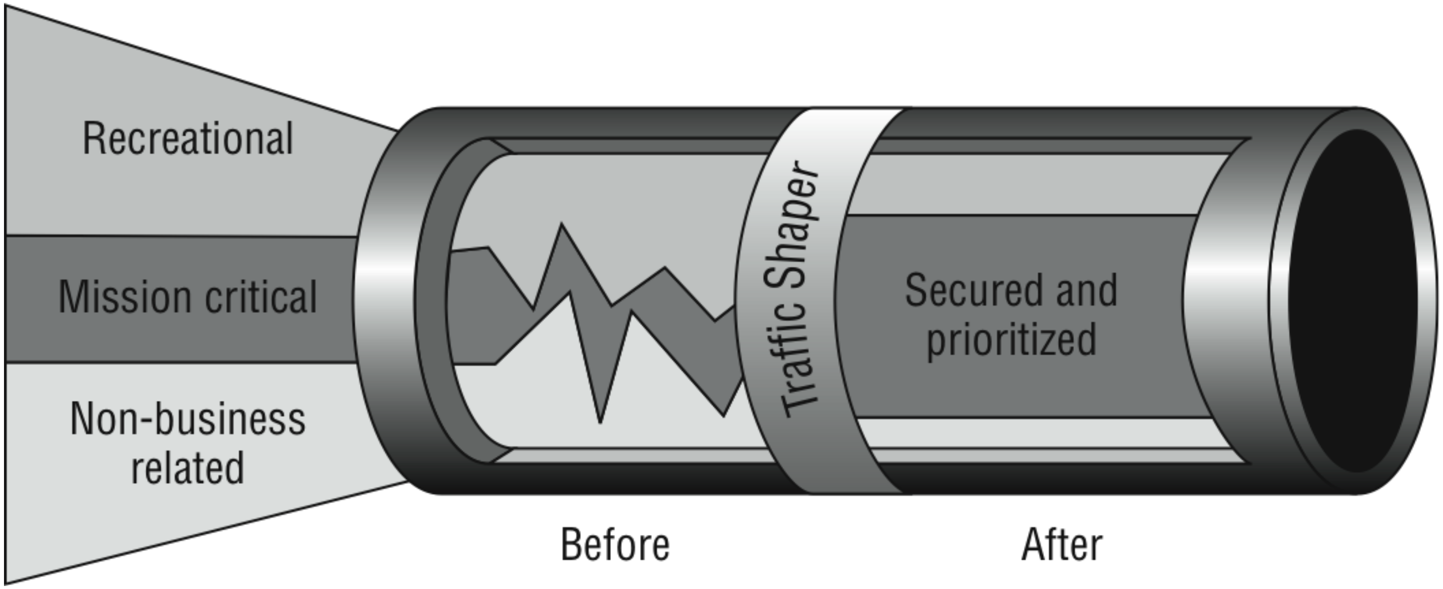
```
⊞ Frame 119 (74 bytes on wire, 74 bytes captured)
⊞ Ethernet II, Src: Cisco_3c:78:00 (00:05:9a:3c:78:00), Dst: 00:00:00_00:00:00 (00:00:00:00:00:00)
⊞ Internet Protocol, Src: 10.100.10.55 (10.100.10.55), Dst: 10.100.36.12 (10.100.36.12)
⊞ User Datagram Protocol, Src Port: 62595 (62595), Dst Port: domain (53)
⊟ Domain Name System (query)
    Transaction ID: 0x6e64
  ⊞ Flags: 0x0100 (Standard query)
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  ⊟ Queries
    ⊟ www.lammle.com: type A, class IN
        Name: www.lammle.com
        Type: A (Host address)
        Class: IN (0x0001)
```

DNS Answer

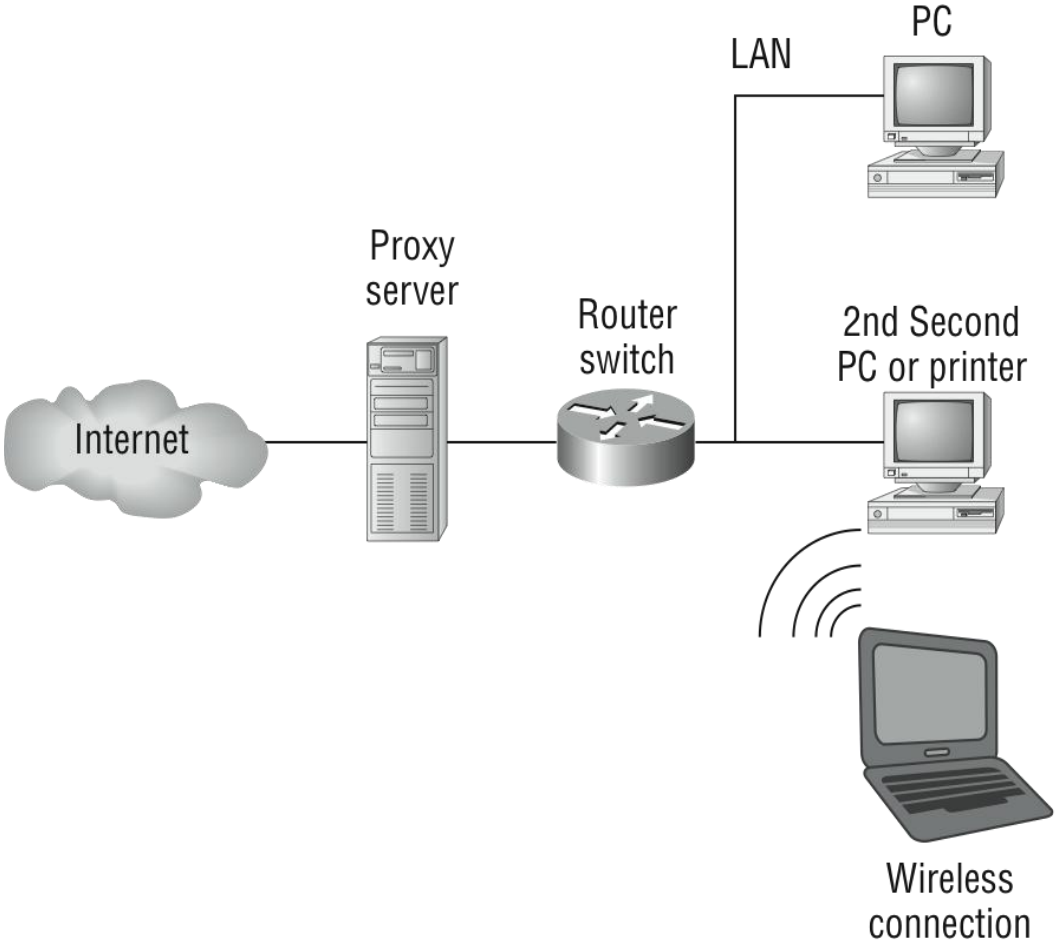


```
⊞ Frame 36 (104 bytes on wire, 104 bytes captured)
⊞ Ethernet II, Src: Cisco_90:ed:80 (00:0b:5f:90:ed:80), Dst: Usi_d0:e9:35 (00:1e:37:d0:e9:35)
⊞ Internet Protocol, Src: 10.100.36.13 (10.100.36.13), Dst: 10.100.36.38 (10.100.36.38)
⊞ User Datagram Protocol, Src Port: domain (53), Dst Port: 59259 (59259)
⊟ Domain Name System (response)
    [Request In: 35]
    [Time: 0.000302000 seconds]
    Transaction ID: 0x070e
  ⊞ Flags: 0x8180 (Standard query response, No error)
    Questions: 1
    Answer RRs: 2
    Authority RRs: 0
    Additional RRs: 0
  ⊟ Queries
    ⊟ www.lammle.com: type A, class IN
        Name: www.lammle.com
        Type: A (Host address)
        Class: IN (0x0001)
  ⊟ Answers
    ⊞ www.lammle.com: type CNAME, class IN, cname lammle.com
    ⊟ lammle.com: type A, class IN, addr 206.123.114.186
        Name: lammle.com
        Type: A (Host address)
        Class: IN (0x0001)
        Time to live: 3 hours, 6 minutes, 27 seconds
        Data length: 4
        Addr: 206.123.114.186
```

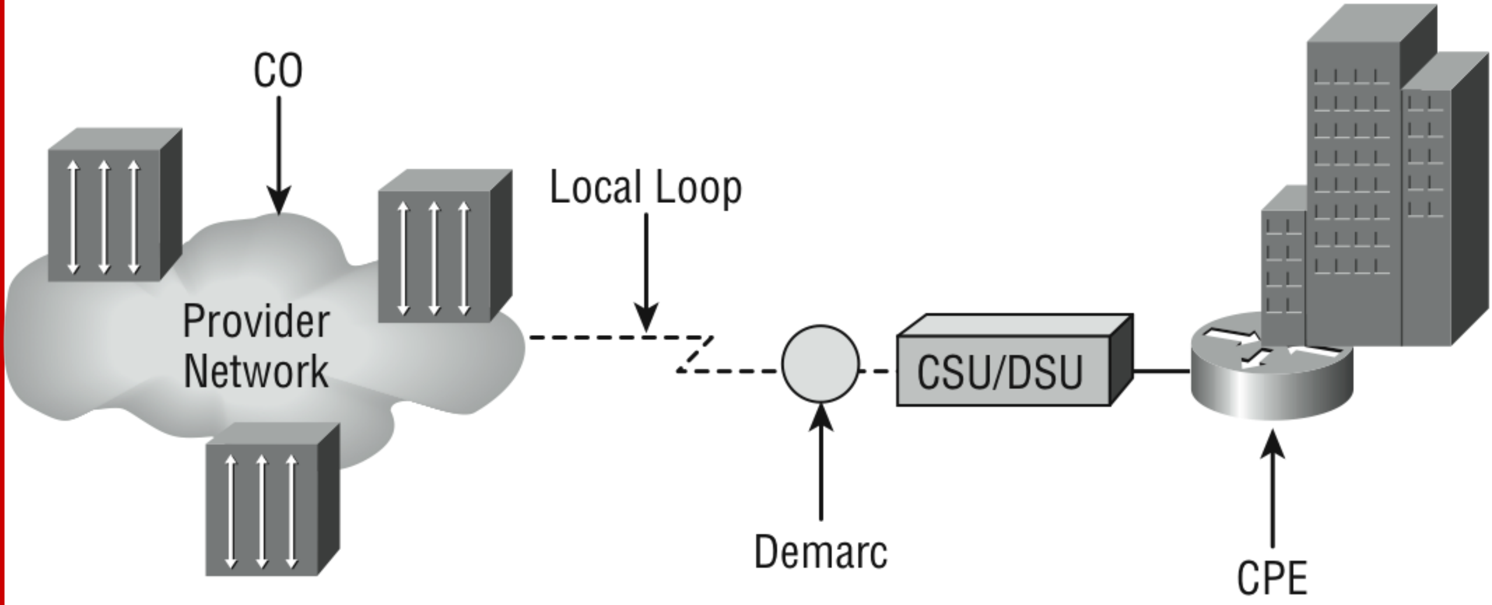
Bandwidth Shaper



Proxy Server



CSU/DSU



Summary

- Summary
- Exam Essentials Section
- Written Labs
- Review Questions