Chapter 4

The Network Layer & Internetworking

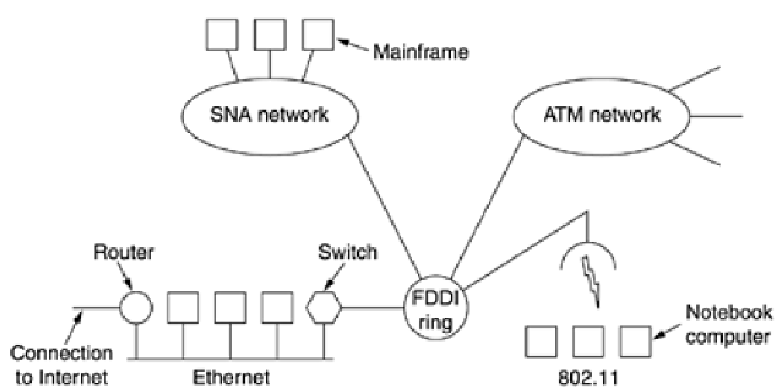
Content

- Internetworking
- The Network Layer in the Internet
- Network Layer Design Issues
- Routing Algorithms
- Congestion Control Algorithms

Internetworking

- Overview
- How Networks Differ ?
- How Networks Can Be Connected ?
- Concatenated Virtual Circuits
- Connectionless Internetworking
- Tunneling
- Internetwork Routing
- Fragmentation

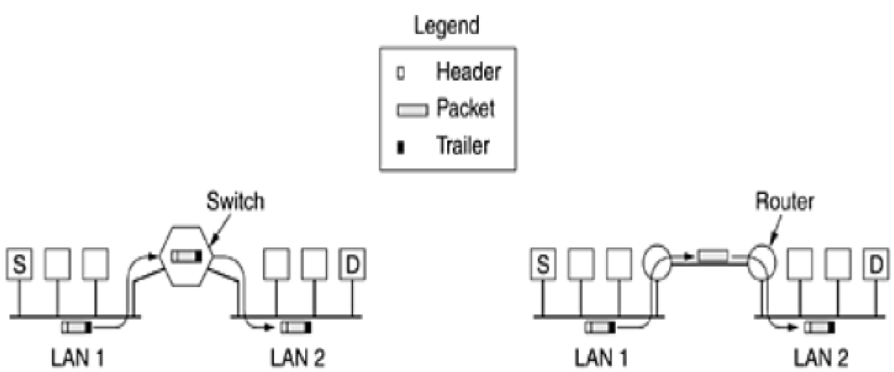
Overview



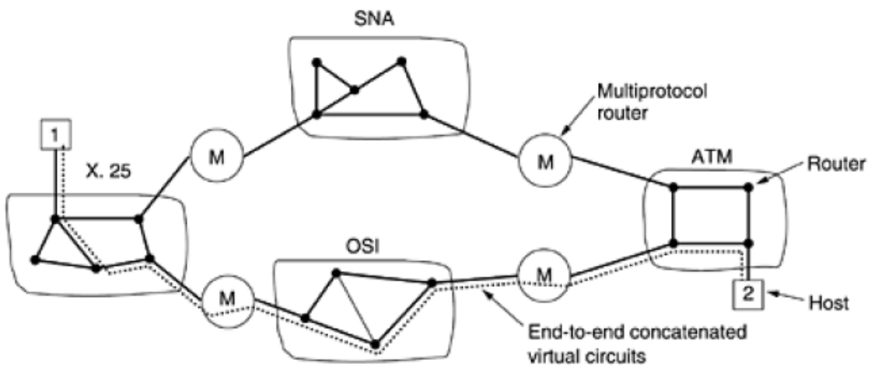
How Networks Differ ?

Item	Some Possibilities
Service offered	Connection oriented versus connectionless
Protocols	IP, IPX, SNA, ATM, MPLS, AppleTalk, etc.
Addressing	Flat (802) versus hierarchical (IP)
Multicasting	Present or absent (also broadcasting)
Packet size	Every network has its own maximum
Quality of service	Present or absent; many different kinds
Error handling	Reliable, ordered, and unordered delivery
Flow control	Sliding window, rate control, other, or none
Congestion control	Leaky bucket, token bucket, RED, choke packets, etc.
Security	Privacy rules, encryption, etc.
Parameters	Different timeouts, flow specifications, etc.
Accounting	By connect time, by packet, by byte, or not at all

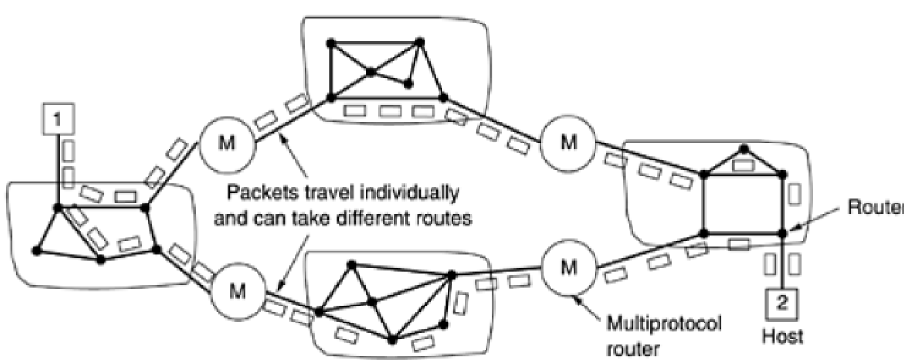
How Networks Can Be Connected ?



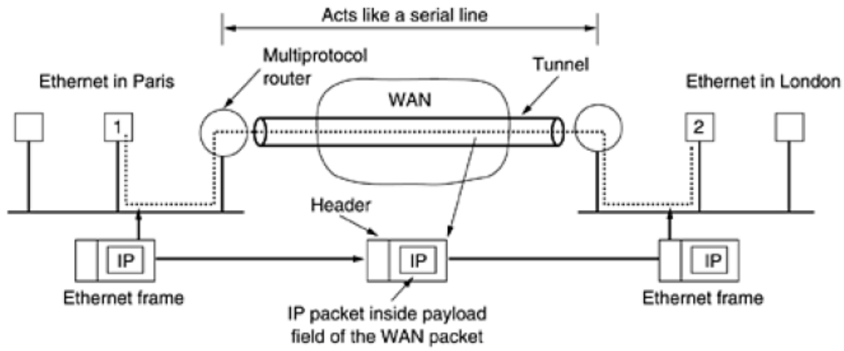
Concatenated Virtual Circuits



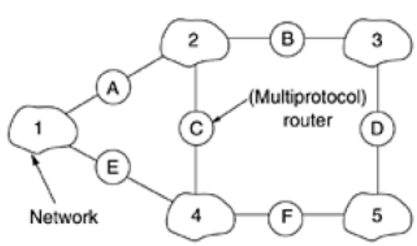
Connectionless Internetworking

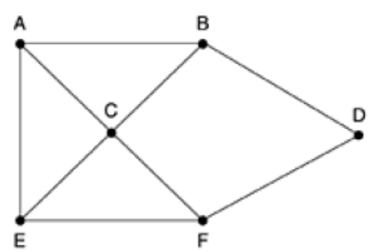


Tunneling

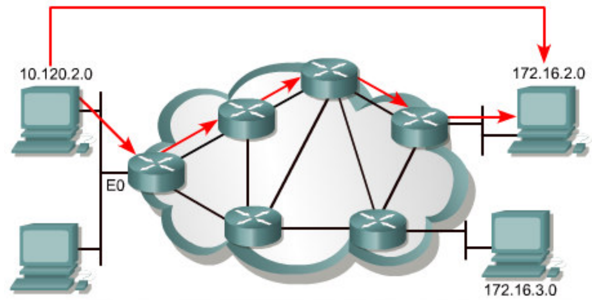


Internetwork Routing





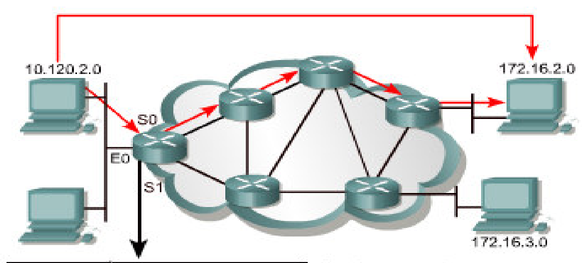
Routed versus Routing



Routed protocol transport data from one end-station to another.

- Routed protocol: used at the network layer that transfer data from one host to another across a router
- Routing protocols: allow routers to choose the best path for data from source to destination
- Examples: Internet Protocol (IP); Novell's Internetwork Packet Exchange (IPX); DECnet, AppleTalk, Banyan VINES, and Xerox Network Systems (XNS).

Routing protocol



Network Protocol	Destination Network	Exit Interface
Connected	10.120.2.0	E0
RIP	172.16.2.0	S0
IGRP	172.16.3.0	S1

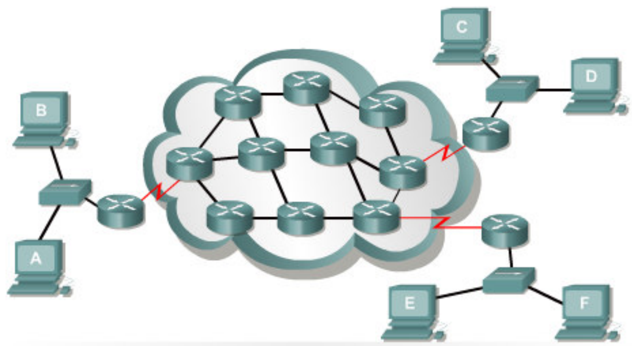
Routing protocols are used between routers to determine paths and maintaining routing tables

After the path is determined a router can route a routed protocol

Routing protocol = RIP, IGRP

- Provides processes for sharing route information
- Allows routers to communicate with other routers to update and maintain the routing tables
- Examples: Routing Information Protocol (RIP), Interior Gateway Routing Protocol (IGRP), Open Shortest Path First (OSPF), Border Gateway Protocol (BGP), and Enhanced IGRP (EIGRP)

Path Determination



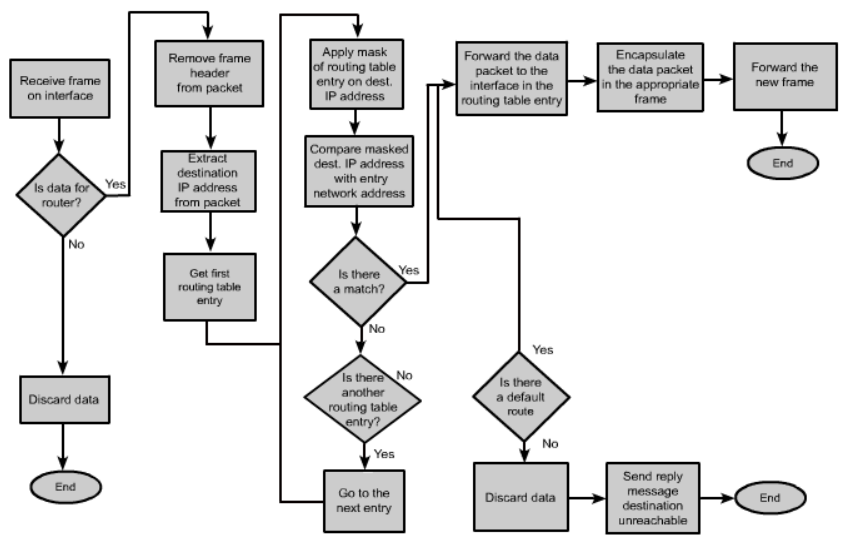
If computer A was sending data to computer F, what path would the data take? That is determined by the information in the routing table.

- Path determination enables a router to compare the destination address to the available routes in its routing table, and to select the best path
- Static or Dynamic routing

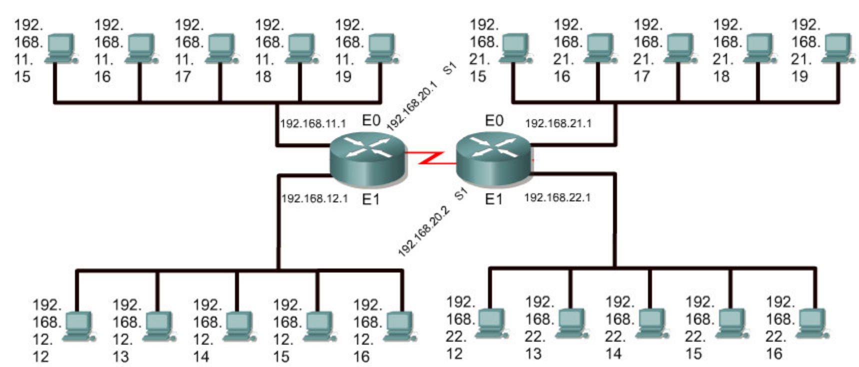
Transportation Analogy

Which is the best route from the house to the university? There are many possible choices, but which is the fastest, the safest, the shortest, and the most reliable? The same questions are asked and answered when routing data.

The Routing Process



Routing Table



Routing Table

Learned	Network Address	Hop	Interface
C -	192.168.11.0	0	E0
C -	192.168.12.0	0	E1
C -	192.168.20.0	0	S0
R -	192.168.21.0	1	S0
R -	192.168.22.0	1	S0

Routing Table

Learned	Network Address	Hop	Interface
C -	192.168.21.0	0	E0
C -	192.168.22.0	0	E1
C -	192.168.20.0	0	S1
R -	192.168.11.0	1	S1
R -	192.168.12.0	1	S1

Information in Routing Table

- **Protocol type** – The type of routing protocol that created the routing table entry
- **Destination/next-hop associations** – These associations tell a router that a particular destination is either directly connected to the router, or that it can be reached using another router called the "next-hop" on the way to the final destination
- **Routing metric** – Different routing protocols use different routing metrics.
- **Outbound interfaces** – The interface that the data must be sent out on

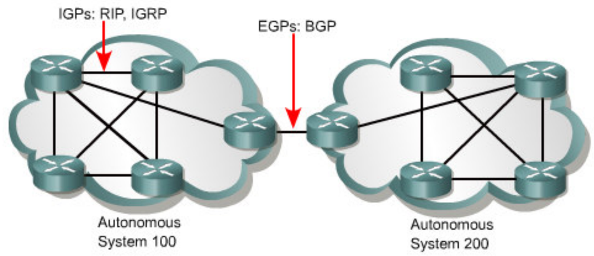
Routing Algorithms & Metrics

Protocol	Metric	Maximum number of routers	Origins
RIP	Hop count	15	Xerox
IGRP	• Bandwidth • Load • Delay • Reliability	255	Cisco

Routing metrics are the values used to determine the best path to the next hop.

- Design goals of Routing Protocols
  - Optimization
  - Simplicity & Low Overhead
  - Robustness & stability
  - Flexibility
  - Rapid Convegence
- Some metrics used by Routing Protocols:
  - Bandwidth
  - Delay
  - Load
  - Reliability
  - Hop count
  - Ticks, cost

IGP and EGP



An autonomous system is a collection of networks under a common administrative domain. IGPs operate within an autonomous system. EGPs connect different autonomous system.

- Autonomous system is a network or set of networks under common administrative control. An autonomous system consists of routers that present a consistent view of routing to the external world.
- Interior Gateway Protocols (IGP): route data within an autonomous system. Eg: RIP and RIPv2; IGRP; EIGRP; OSPF; IS-IS;
- Exterior Gateway Protocols (EGP): route data between autonomous systems. Eg: BGP

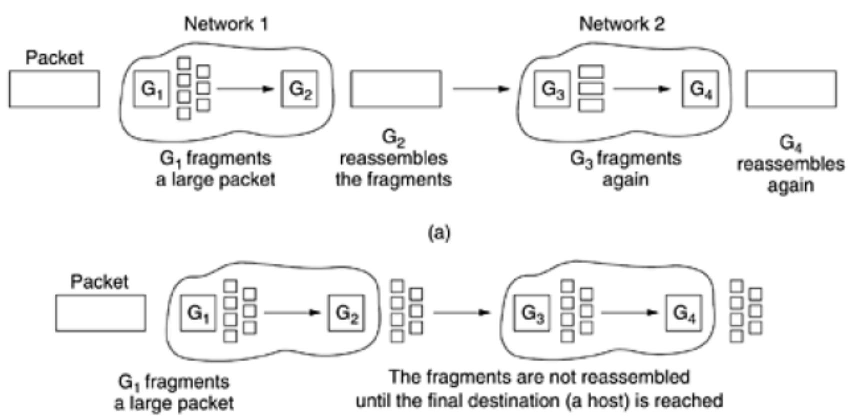
Link state and Distance Vector

- The distance-vector routing approach determines the distance and direction, vector, to any link in the internetwork. Routers using distance-vector algorithms send all or part of their routing table entries to adjacent routers on a periodic basis. This happens even if there are no changes in the network. Eg: RIP, IGRP, EIRP
- Link state routing protocols send periodic update at longer time interval (30'), Flood update only when there is a change in topology. Link state use their database to creat routing table. Eg: OSPF, IS-IS

Routing Protocols

- RIP:distance vector; uses hop count as its metric; RIP cannot route a packet beyond 15 hops. RIPv1 requires all devices in the network use the same subnet mask. RIPv2 supports VLSM.
- IGRP:distance-vector; routing protocol developed by Cisco. IGRP can select the fastest path based on delay, bandwidth, load, and reliability. It also has a much higher maximum hop count limit than RIP.
- OSPF
- IS-IS
- EIGRP
- BGP

Fragmentation

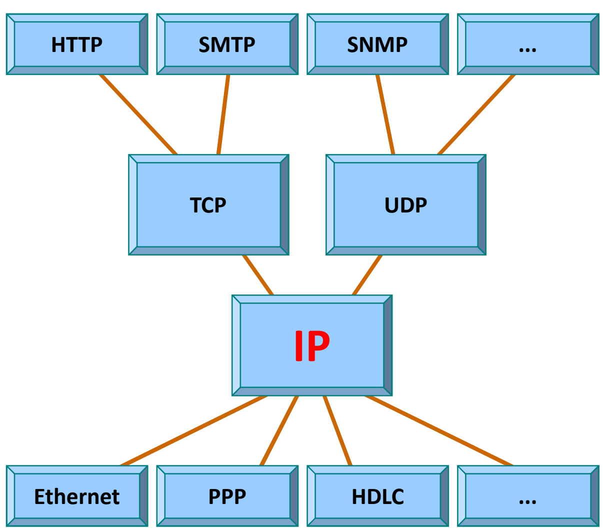


Transparent and Non-Transparent Fragmentation

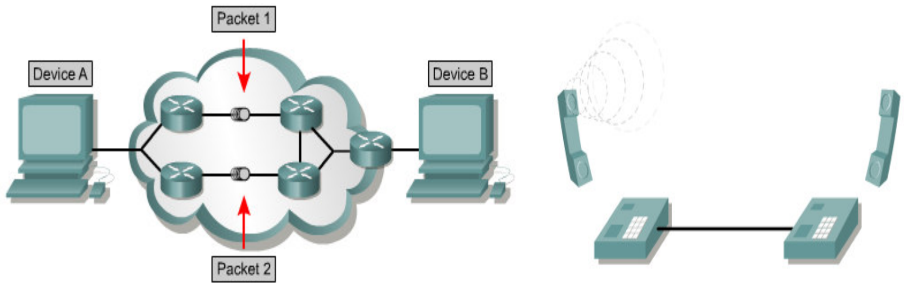
The Network Layer in the Internet

- TCP/IP model
- Internet Protocol (IP)
- Addressing
- IP Address
- Internet Control Protocols
  - Internet Control Message Protocol
  - ARP - Address Resolution Protocol
  - RARP, BOOTP, and DHCP
- OSPF - Interior Gateway Routing Protocol
- BGP - Exterior Gateway Routing Protocol
- Internet Multicasting
- Mobile IP
- IPv6

TCP/IP



Internet Protocol (IP)



○ **Connectionless**: Different packets may take different paths to get through the network; reassembled at the destination, the destination is not contacted before a packet is sent.

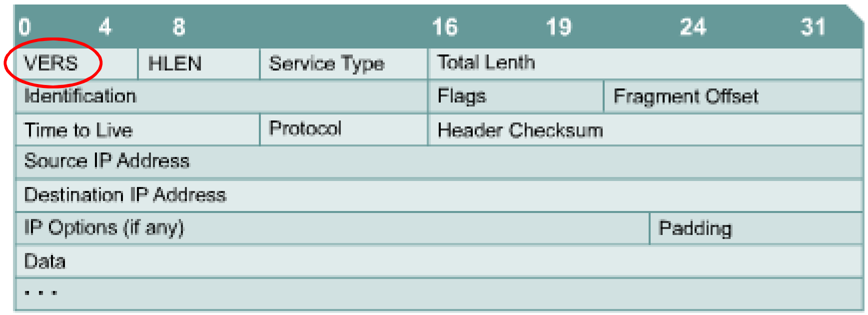
○ **Connection-oriented**: A connection is established between the sender and the recipient before any *data is* transferred.

The IPv4 header

0	4	8	16	19	24	31
VERS	HLEN	Service Type	Total Lenth			
Identification			Flags	Fragment Offset		
Time to Live		Protocol	Header Checksum			
Source IP Address						
Destination IP Address						
IP Options (if any)					Padding	
Data						
. . .						

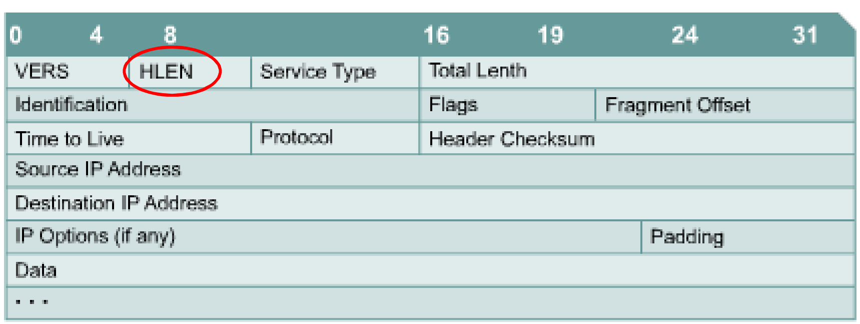
These are the header fields in an IP packet header. All field lengths are fixed except for IP options and the padding fields

The IPv4 header



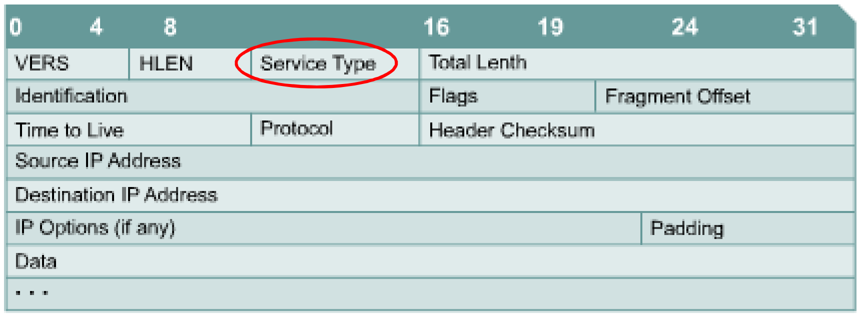
- 4 bits
- Indicates version of IP used
- IPv4: 0100; IPv6: 0110

The IPv4 header



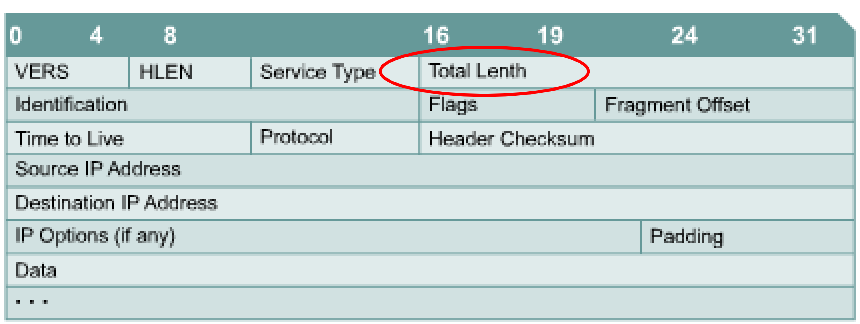
- 4 bits
- Indicates datagram header length in 32 bit words

The IPv4 header



- 8 bits
- Specifies the level of importance that has been assigned by upper-layer protocol

The IPv4 header



- 16 bits
- Specifies the length of the entire packet in bytes, including data and header

The IPv4 header

0	4	8	16	19	24	31
VERS	HLEN	Service Type	Total Lenth			
Identification			Flags	Fragment Offset		
Time to Live		Protocol	Header Checksum			
Source IP Address						
Destination IP Address						
IP Options (if any)					Padding	
Data						
. . .						

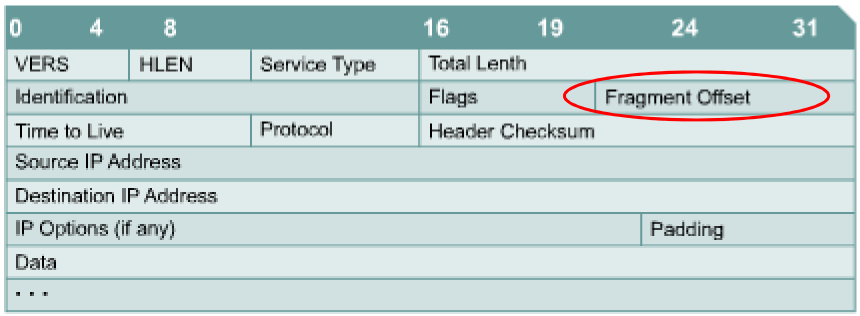
- 16 bits
- Identifies the current datagram

The IPv4 header

0	4	8	16	19	24	31
VERS	HLEN	Service Type	Total Lenth			
Identification			Flags	Fragment Offset		
Time to Live		Protocol	Header Checksum			
Source IP Address						
Destination IP Address						
IP Options (if any)					Padding	
Data						
. . .						

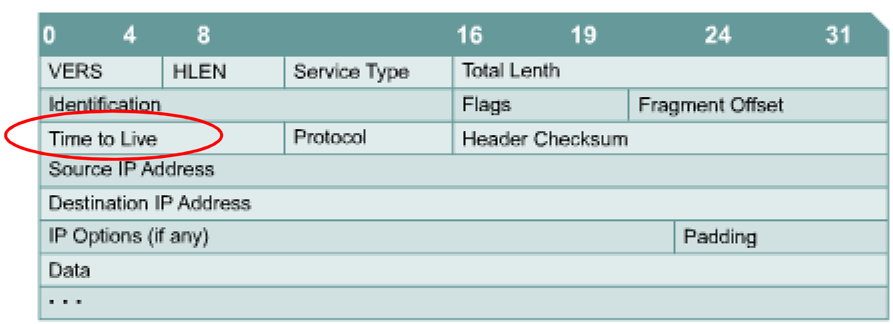
- 3 bits
- The second bit specifies if the packet can be fragmented; the last bit specifying whether the packet is the last fragment in a series of fragmented packets.

The IPv4 header



- 13 bits
- Used to help piece together datagram fragments

The IPv4 header



- 8 bits
- Specifies the number of hops a packet may travel. This number is decreased by one as the packet travels through a router

The IPv4 header

0	4	8	16	19	24	31
VERS	HLEN	Service Type	Total Lenth			
Identification			Flags	Fragment Offset		
Time to Live		Protocol	Header Checksum			
Source IP Address						
Destination IP Address						
IP Options (if any)					Padding	
Data						
. . .						

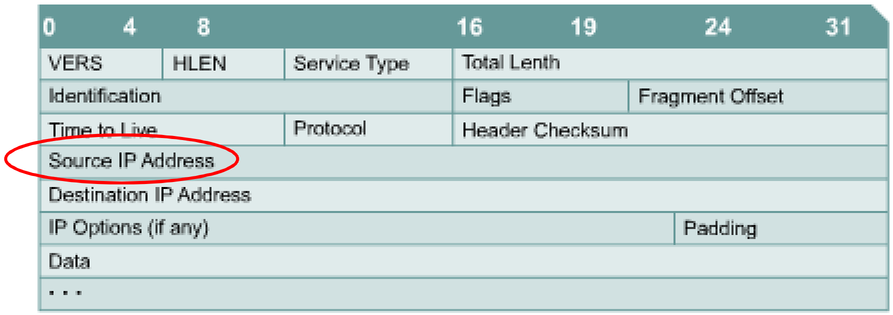
- 8 bits
- Indicates which upper-layer protocol, such as TCP(6) or UDP(17), receives incoming packets after IP processing has been completed

The IPv4 header

0	4	8	16	19	24	31
VERS	HLEN	Service Type	Total Lenth			
Identification			Flags	Fragment Offset		
Time to Live		Protocol	Header Checksum			
Source IP Address						
Destination IP Address						
IP Options (if any)					Padding	
Data						
. . .						

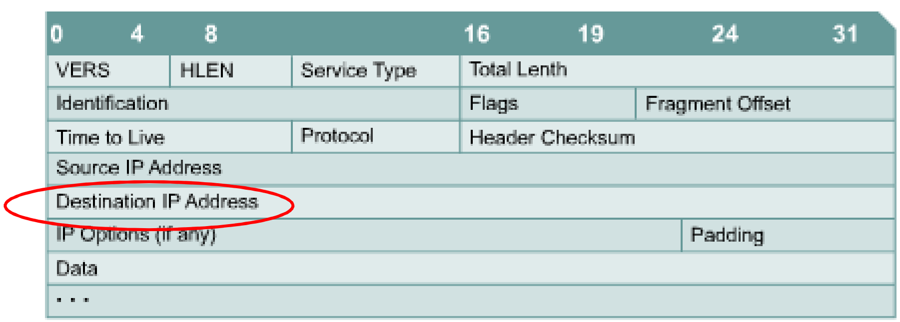
- 16 bits
- Helps ensure IP header integrity
- Not caculated for the encapsulation data

The IPv4 header



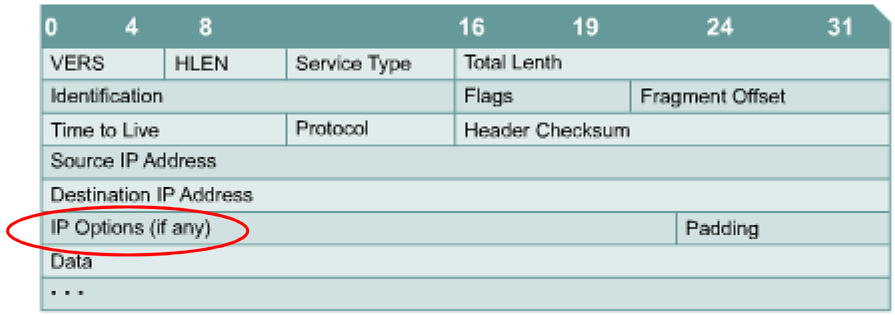
- 32 bits
- Specifies the sending node IP address

The IPv4 header



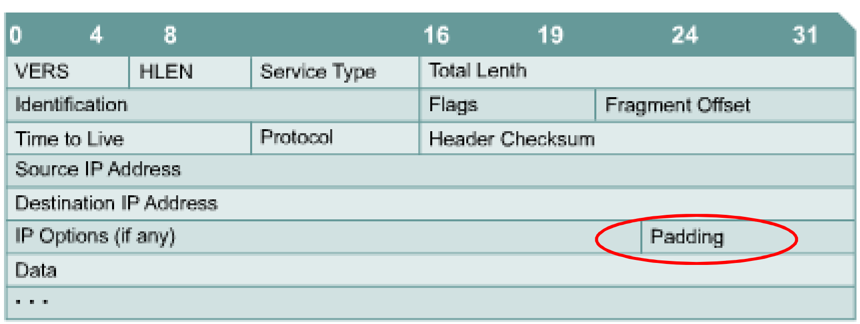
- 32 bits
- Specifies the receiving node IP address

The IPv4 header



- Variable length
- Allows IP to support various options, such as security

The IPv4 header



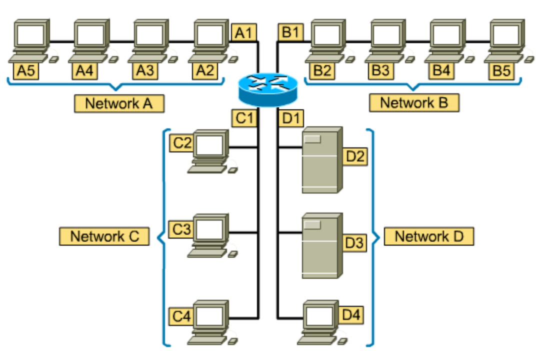
- Variable length
- Extra zeros are added to this field to ensure that the IP header is always a multiple of 32 bits.

The IPv4 header

0	4	8	16	19	24	31
VERS	HLEN	Service Type	Total Lenth			
Identification			Flags	Fragment Offset		
Time to Live		Protocol	Header Checksum			
Source IP Address						
Destination IP Address						
IP Options (if any)					Padding	
Data						
. . .						

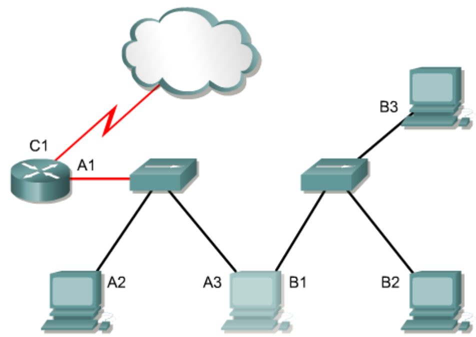
- Variable length up to 64 Kb
- Contains upper-layer information

Addressing



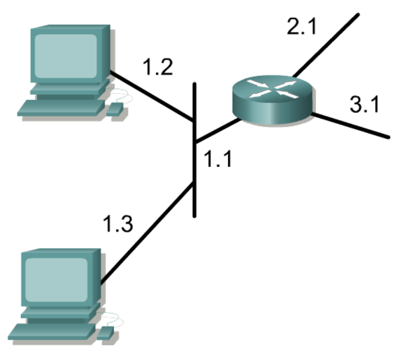
- For any two systems to communicate, they must be able to identify and locate each other. We call it “**addressing**”.
- The **hosts** are “grouped” into **networks**. In the illustration, we use the A or B to identify the network and the number sequence to identify the individual host.
- The combination of letter (**network address**) and the number (**host address**) create a **unique address** for each device on the network.

Addressing



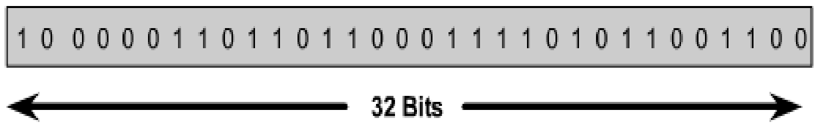
- An address generally represents the connection to the network. A device that have two connection points may need two addresses beloging to two networks.
- Each connection points (espcially in LAN technologies) also has its ID (example: **MAC** address) which is called **physical address**. There is also the need to map between physical adresses (layer 2) and logical addresses (layer 3).

Addressing Rule



- Every IP address has two parts. One part identifies the network where the system is connected, and a second part identifies that particular system on the network.
- Two different networks must have different network address (**net-id**), and two different hosts in the same network must have different host address (**host-id**). Of cause, hosts in the same network have the same network address.

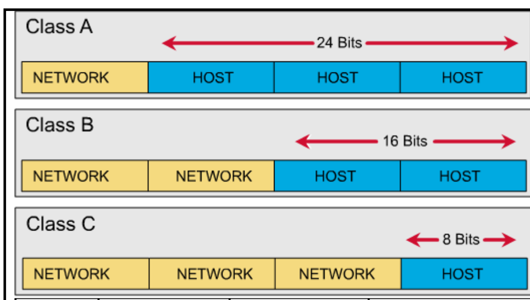
IP Address (IPv4)



Binary : 11000000.10101000.000000001.00001000 and 11000000.10101000.00000001.00001001

Decimal : 192.168.1.8 and 192.168.1.9

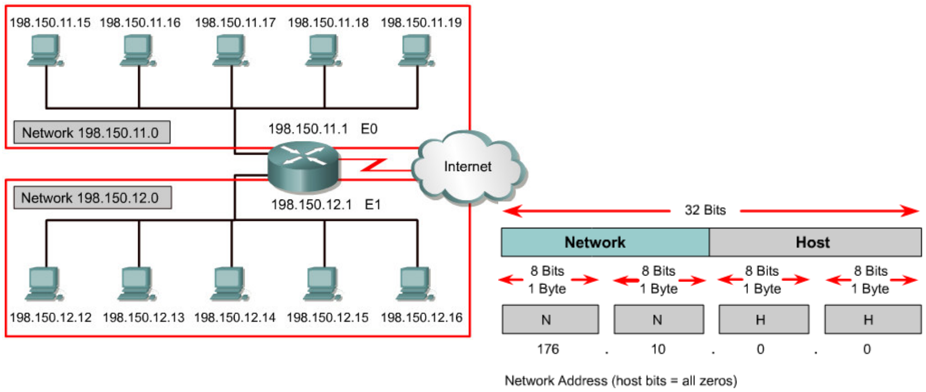
2^{15}	2^{14}	2^{13}	2^{12}	2^{11}	2^{10}	2^9	2^8	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
32768	16384	8192	4096	2048	1024	512	256	128	64	32	16	8	4	2	1



IP address class	IP address range (First Octet Decimal Value)
Class A	1-126 (00000001-01111110) *
Class B	128-191 (10000000-10111111)
Class C	192-223 (11000000-11011111)
Class D	224-239 (11100000-11101111)
Class E	240-255 (11110000-11111111)

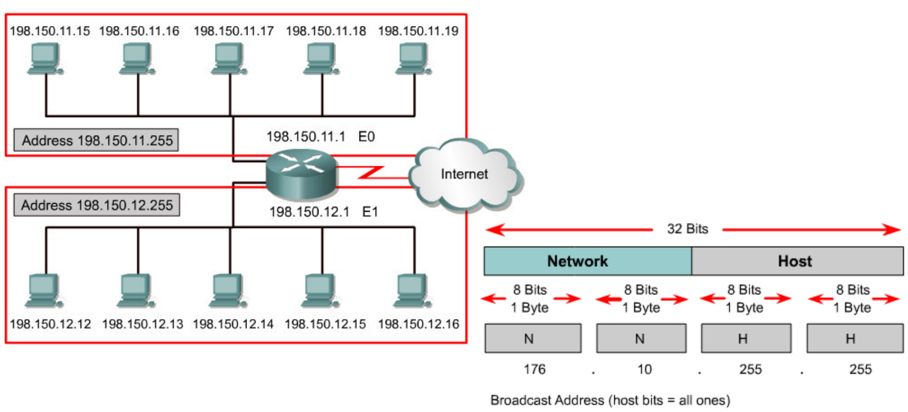
Class	1^{st} Octet Decimal Range	1^{st} Octet High Order Bits	Network/Host ID (N=Network, H=Host)	Default Subnet Mask	Number of Networks	Hosts per Network (Usable Addresses)
A	1 – 126 *	0	N.H.H.H	255.0.0.0	126 ($2^7 – 2$)	16,777,214 ($2^{24} – 2$)
B	128 – 191	10	N.N.H.H	255.255.0.0	16,382 ($2^{14} – 2$)	65,534 ($2^{16} – 2$)
C	192 – 223	110	N.N.N.H	255.255.255.0	2,097,150 ($2^{21} – 2$)	254 ($2^8 – 2$)
D	224 – 239	1110	Reserved for Multicasting			
E	240 – 254	11110	Experimental; used for research			

Network Address



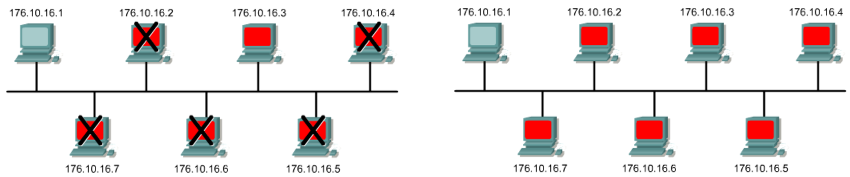
When all **host-bits** are zeros, we have a number that represents **network address**. This address is reserved, namely it cannot be assigned to any host.

Broadcast Address



- When **host-bits** are all one, we have a number that represents **broadcast address**. This address is also reserved, namely it cannot be assigned to any host.
- Example where Broadcast addresses are used: a host need to locate a specific service.

Unicast and Broadcast Transmission

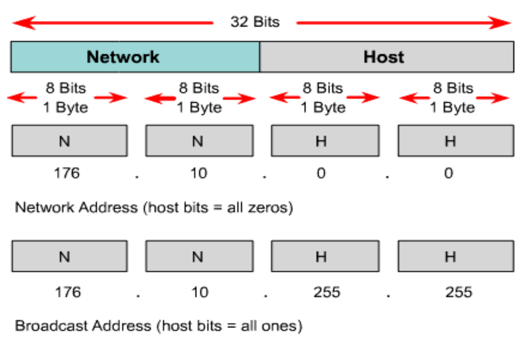


Unicast transmission

Broadcast transmission

The concept of unicast and broadcast transmission exist in both layer 2 and layer 3 protocols. There are refelections in the addressing scheme

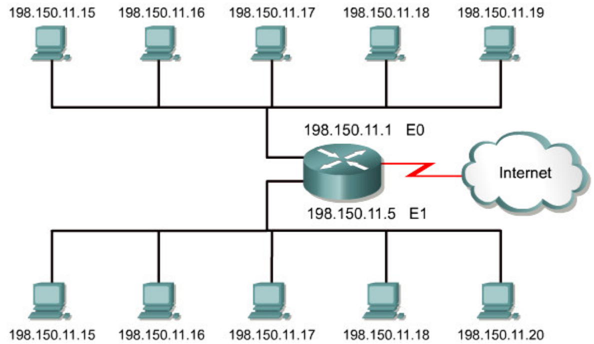
Reserved IP Address



Certain host addresses are reserved and cannot be assigned to devices on a network. These reserved host addresses include the following:

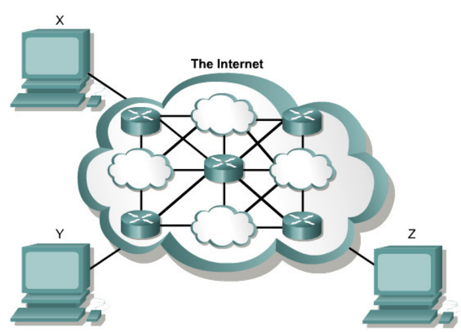
- Host-bits = all zeros (network address);
- Host-bits = all ones (broadcast address);
- Network-bits = all ones;
- Network-bits = all zeros;
- **127**.x.x.x (loopback address = **127.0.0.1**).

Required Unique Address



- The stability of the Internet depends directly on the uniqueness of publicly used network addresses.
- In the figure, there is an “IP conflict” issue.
- A procedure was needed to make sure that addresses were in fact unique. Originally, an organization known as the Internet Network Information Center (**InterNIC**) handled this procedure. InterNIC no longer exists and has been succeeded by the Internet Assigned Numbers Authority (**IANA**).

Public IP Addresses



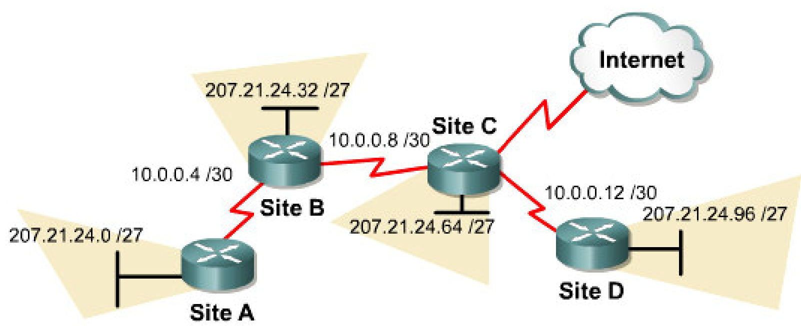
- **Public IP addresses** are unique. No two machines that connect to a public network can have the same IP address.
- Public IP addresses must be obtained from an Internet service provider (**ISP**) or a registry **at some expense**.
- With the rapid growth of the Internet, public IP addresses were beginning to run out (**IP address depletion**).
- New addressing schemes, such as classless interdomain routing (**CIDR**) and **IPv6** were developed to help solve the problem. **Private IP addresses** are another solution.

Private IP Addresses

Class	RFC 1918 internal address range
A	10.0.0.0 to 10.255.255.255
B	172.16.0.0 to 172.31.255.255
C	192.168.0.0 to 192.168.255.255

- **RFC 1918** sets aside three blocks of IP addresses for **private**, internal use. These three blocks consist of one Class A, a range of Class B addresses, and a range of Class C addresses.
- Addresses that fall within these ranges are **not** routed on the Internet backbone. Internet routers immediately discard private addresses.

Using Private Addresses



- When addressing a nonpublic intranet, a test lab, or a home network, we normally use private addresses instead of globally unique addresses.
- Private addresses can be used to address point-to-point serial links without wasting real IP addresses.
- Connecting a network using private addresses to the Internet requires translation of the private addresses to public addresses. This translation process is referred to as Network Address Translation (**NAT**).

Introduction to Subnetting

Class C network address 192.168.10.0

11000000.10101000.00001010.00000000
N . N . N . H

11000000.10101000.00001010.00000000
N . N . N . sN H
In this example three bits have been assigned to designate the subnet.

Class B network address 147.10.0.0

10010011.00001010.00000000.00000000
N . N . H . H

10010011.00001010.00000000.00000000
N . N . sN H. H
In this example five bits have been assigned to designate the subnet.

Class A network adress 28.0.0.0

00011100.00000000.00000000.00000000
N . H . H . H

00011100.00000000.00000000.00000000
N . sN . sN H . H
In this example twelve bits have been assigned to designate the subnet.

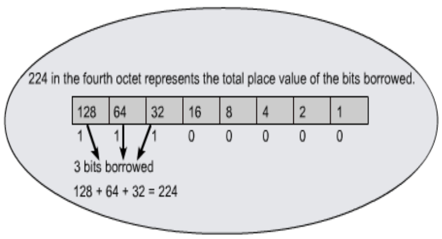
Reason for Subnetting

Decimal notation for first Host octet	Number of Subnets	Number of Class A Hosts per Subnet	Number of Class B Hosts per Subnet	Number of Class C Hosts per Subnet
.192	2	4,194,302	16,382	62
.224	6	2,097,150	8,190	30
.240	14	1,048,574	4,094	14
.248	30	524,286	2,046	6
.252	62	262,142	1,022	2
.254	126	131,070	510	-
.255	254	65,534	254	-

- **Subnetting** is another method of managing IP addresses. This method of **dividing** full network address classes **into smaller pieces** has prevented complete IP address exhaustion.
- The network is no longer limited to the **default Class A, B, or C** network masks and there is more flexibility in the network design.
- Analogy: telephone.
- Subnet addresses include the **network** portion, plus a **subnet** field and a **host** field.
- To create a subnet address, a network administrator **borrows bits from the host field** and designates them as the subnet field.

Establishing SM address

Slash format	/25	/26	/27	/28	/29	/30	N/A	N/A
Mask	128	192	224	240	248	252	254	255
Bits borrowed	1	2	3	4	5	6	7	8
Value	128	64	32	16	8	4	2	1
Total Subnets		4	8	16	32	64		
Usable Subnets		2	6	14	30	62		
Total Hosts		64	32	16	8	4		
Usable Hosts		62	30	14	6	2		



The number of bits in the subnet will depend on the maximum number of hosts required per subnet.

The subnet mask: using binary ones in the host octet(s)

($2^{\text{power of borrowed bits}}$) – 2 = usable subnets

($2^{\text{power of remaining host bits}}$) –2= usable hosts

Applying the Subnet Mask

Subnetwork #	Subnetwork ID	Host Range	Broadcast ID
0	192.168.10.0	.1--.30	192.168.10.31
1	192.168.10.32	.33--.62	192.168.10.63
2	192.168.10.64	.65--.94	192.168.10.95
3	192.168.10.96	.97--.126	192.168.10.127
4	192.168.10.128	.129--.158	192.168.10.159
5	192.168.10.160	.161--.190	192.168.10.191
6	192.168.10.192	.193--.222	192.168.10.223
7	192.168.10.224	.225--.254	192.168.10.255

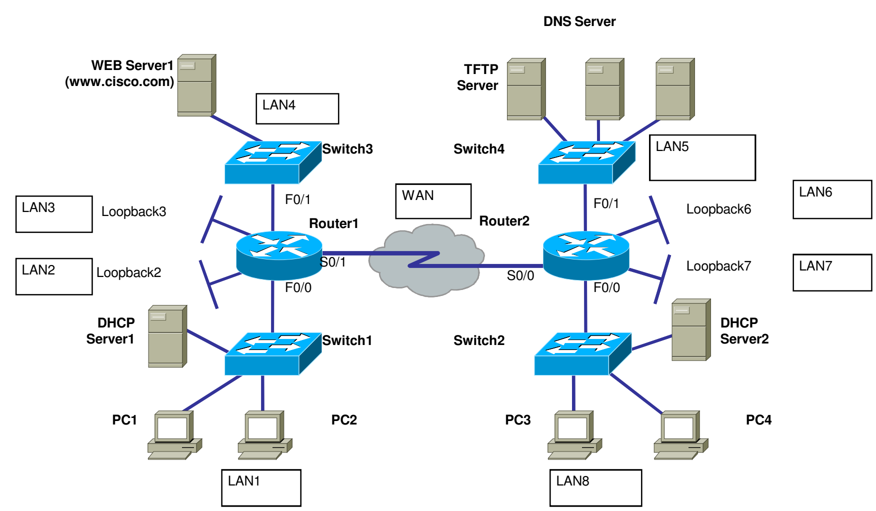
The Logical ANDing process

0	AND	0	=	0
0	AND	1	=	0
1	AND	0	=	0
1	AND	1	=	1

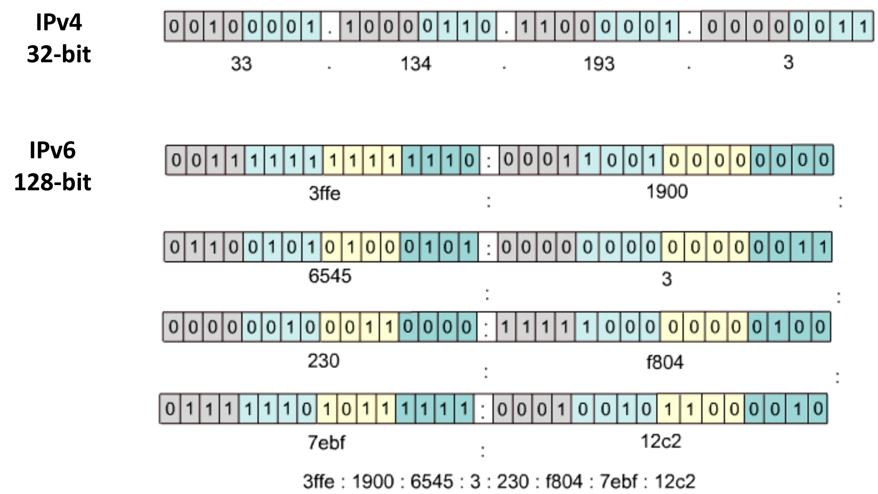
Packet address	201.10.11.65	11001001.00001010.00001011.01000001
AND		
Mask	255.255.255.224	11111111.11111111.11111111.11100000
Subnetwork ID	201.10.11.64	11001001.00001010.00001011.01000000

- ANDing is a binary process by which the router calculates the subnetwork ID for an incoming packet
- ANDding process is handled at the binary level
- (IP address) AND (subnetmask address) = subnetwork ID (router uses that information to forward the packet across the correct interface)

Practice



IPv4 and IPv6 Addresses



IPv4 and IPv6

Internet Protocol Version 4 (IPv4)	4 octets
11010001.11011100.11001001.01110001	
209.156.201.113	
4,294,467,295 IP addresses	

4.3 e 9 IP addresses

Internet Protocol Version 6 (IPv6)	16 octets
11010001.11011100.11001001.01110001.11010001.11011100.	
110011001.01110001.11010001.11011100.11001001.	
01110001.11010001.11011100.11001001.01110001	
A524:72D3:2C80:DD02:0029:EC7A:002B:EA73	
3.4 x 10^{38} IP addresses	

3.4 e 38 IP addresses

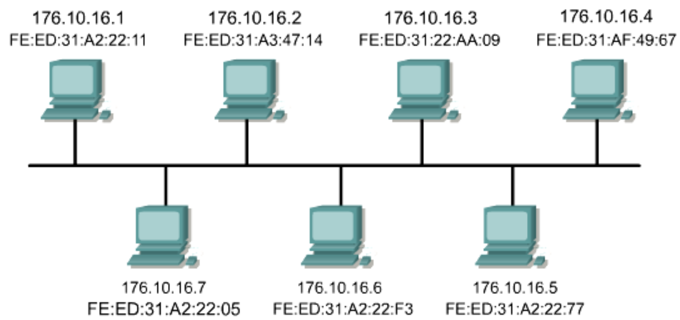
Internet Control Protocols

- ICMP - Internet Control Message Protocol
- ARP - Address Resolution Protocol
- RARP, BOOTP, and DHCP

ICMP - Internet Control Message Protocol

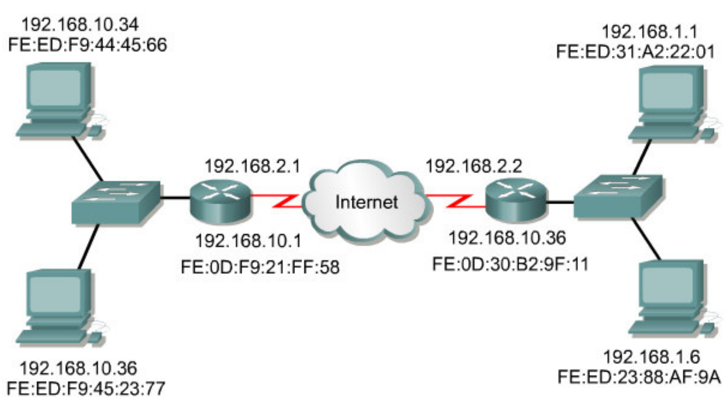
Message type	Description
Destination unreachable	Packet could not be delivered
Time exceeded	Time to live field hit 0
Parameter problem	Invalid header field
Source quench	Choke packet
Redirect	Teach a router about geography
Echo	Ask a machine if it is alive
Echo reply	Yes, I am alive
Timestamp request	Same as Echo request, but with timestamp
Timestamp reply	Same as Echo reply, but with timestamp

ARP



The issue of address mapping between level-2 and level-3 addresses are quite relevent. In TCP/IP communication, a host needs to know both IP address and MAC address of the destination host in order to send packet to it. So there comes Address Resolution Protocol (ARP) which helps hosts in the same LAN segments to find each other MAC addresses.

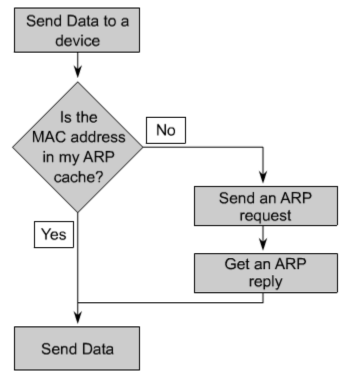
Proxy ARP



Communications among LAN segments have an additional task. TCP/IP has a variation on ARP called Proxy ARP that will provide the MAC address of an intermediate device (example *router*) for transmission outside the LAN to another network segment.

ARP

- Some devices keep the IP-MAC mapping in a so-called **ARP table** which is stored in RAM.
- Example: **arp -a**, **arp -d ***.
- When a devices needs to send data to a host --whose IP is known but MAC is unknown-- it send an **ARP request** as a **broadcast** frame. Then the destination reply with **ARP reply**.
- Another way to build ARP table is to **monitor** the traffic.
- Router generally do not forward such the broadcast. If this feature is turned on, a router performs a **Proxy ARP**.
- However, in reality, we apply the **default gateway** feature. When the destination host is of the different network, then the IP packet is sent to the default gateway (MAC) while IP address is set to the final destination.
- If there is **neither default gateway nor Proxy ARP**, no traffic can leave the local network.

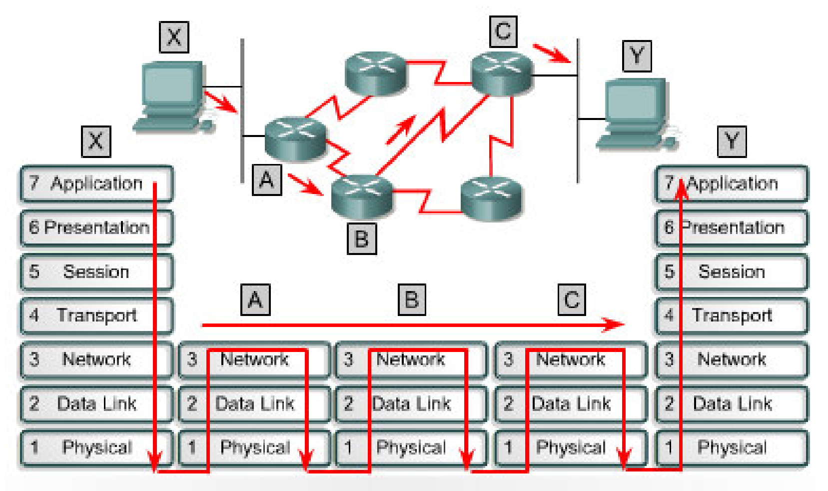


Please remember that both ARP and RARP use the same message structure.

Arp Table 198.150.11.36

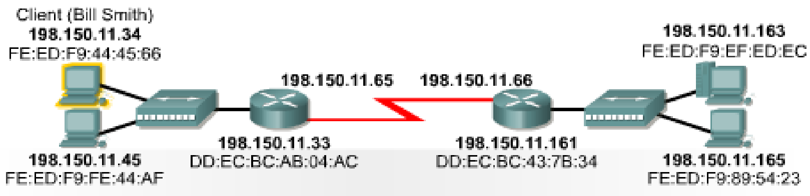
MAC	IP
FE:ED:F9:44:45:66	198.150.11.34
DD:EC:BC:00:04:AC	198.150.11.33
DD:EC:BC:00:94:D4	198.150.11.35
FE:ED:F9:23:44:EF	198.150.11.36

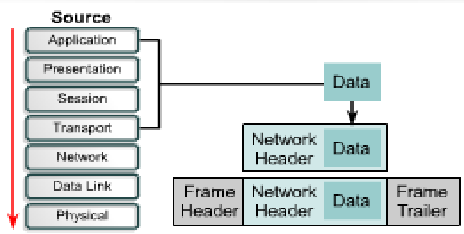
Packet Propagation and Switching



Each router provides its services to support upper-layer functions.

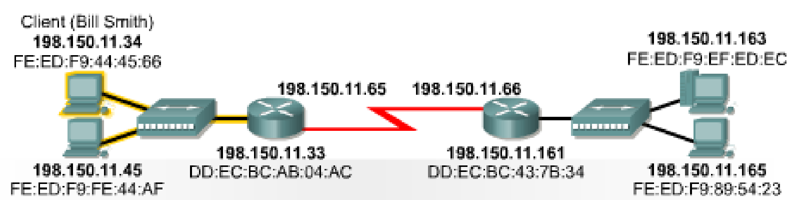
Router Protocol Stripping





The transport layer again segments, sequences and adds error checking to the email message. The network layer source and destination addresses are added to the datagram. The ARP cache provides the MAC address for the destination IP address, so the Ethernet frame is added with the source and destination addresses.

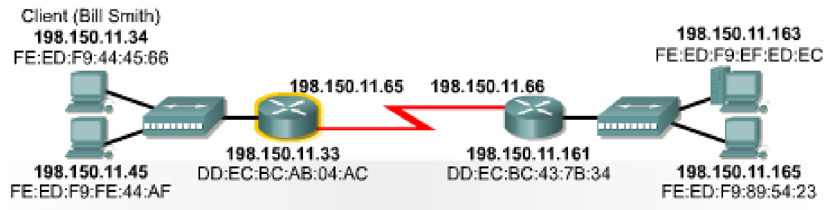
Router Protocol Stripping

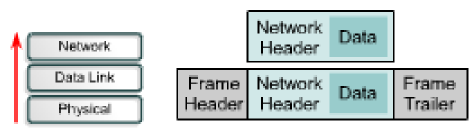


Frame Header		Network Header		Data	Frame Trailer
Destination	Source	Source	Destination		
DD:EC:BC:AB:04:AC	FE:ED:F9:44:45:66	198.150.11.34	198.150.11.163	Email Data	CRC-32

The data frames are then transmitted on the Ethernet segment. All stations pick up the packet and check to see if the packet is for them. All devices except for the Router discard the packet.

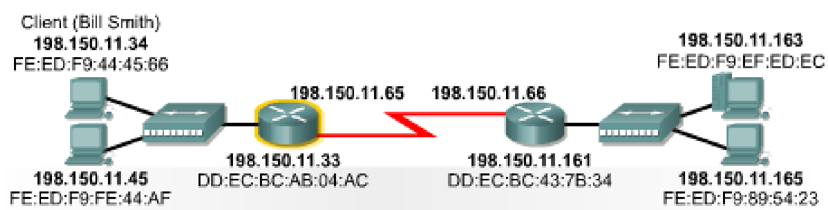
Router Protocol Stripping





The router picks up the frame which was addressed to its MAC address and strips off the Ethernet frame.

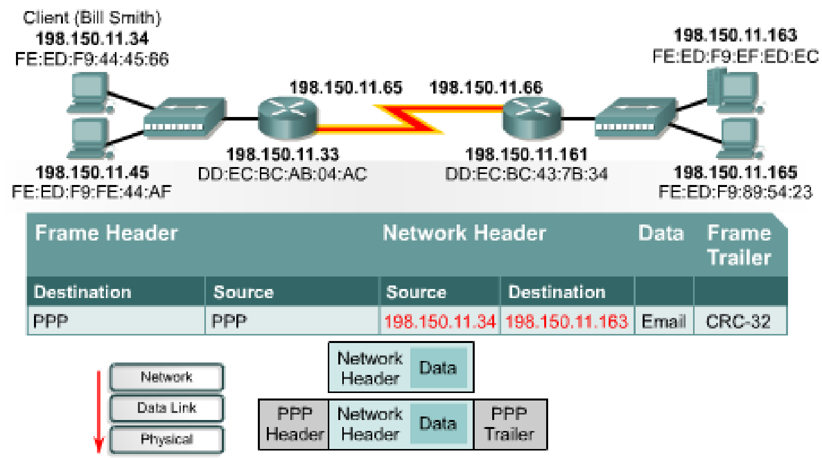
Router Protocol Stripping



198.150. 11.163	**IP Address**
255.255.255.224	**Subnet mask**
198.150. 11.160	**Result**

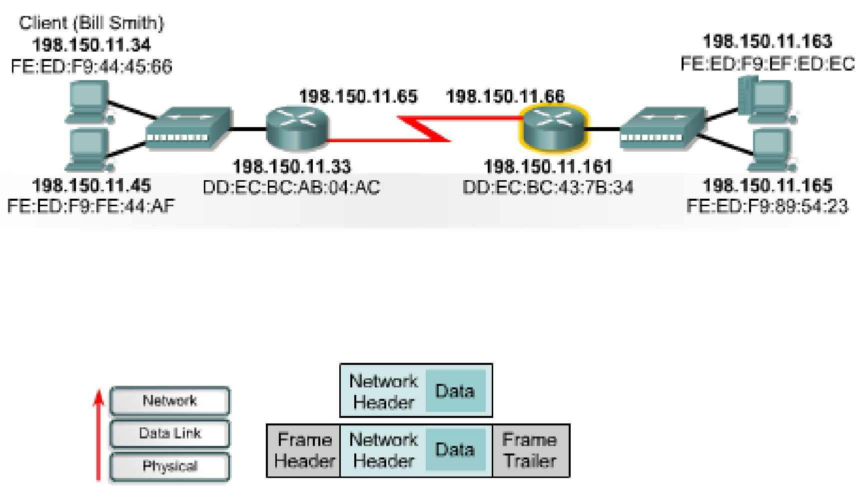
The router applies the subnet mask to the destination address. The router then compares the result to its router table. The table shows that to get to network 198.150.11.160 the packet must be forwarded out the serial (198.150.11.65) port on the router.

Router Protocol Stripping



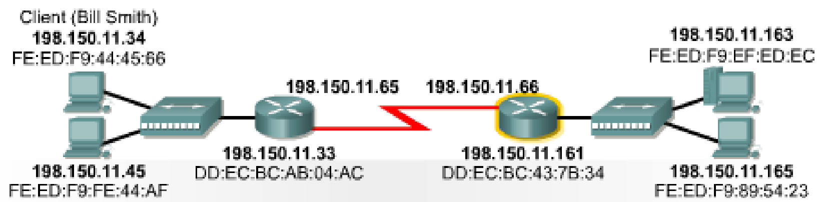
The request is encapsulated for serial transmission and sent to the next router.

Router Protocol Stripping



The router picks up the frame, strips off the PPP frame.

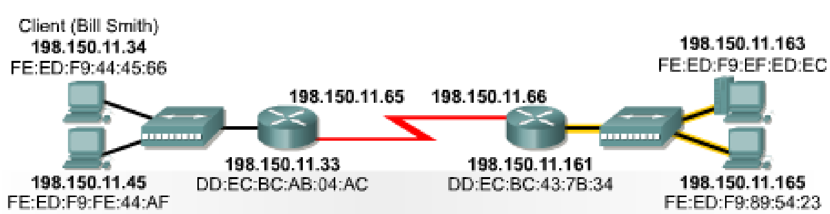
Router Protocol Stripping



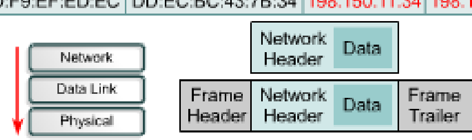
198.150. 11.163	**IP Address**
255.255.255.224	**Subnet mask**
198.150. 11.160	**Result**

The router applies the subnet mask to the destination address. The router then compares the result to its router table. The table shows that to get to network 198.150.11.160 the packet must be forwarded out the Ethernet (198.150.11.161) port on the router.

Router Protocol Stripping

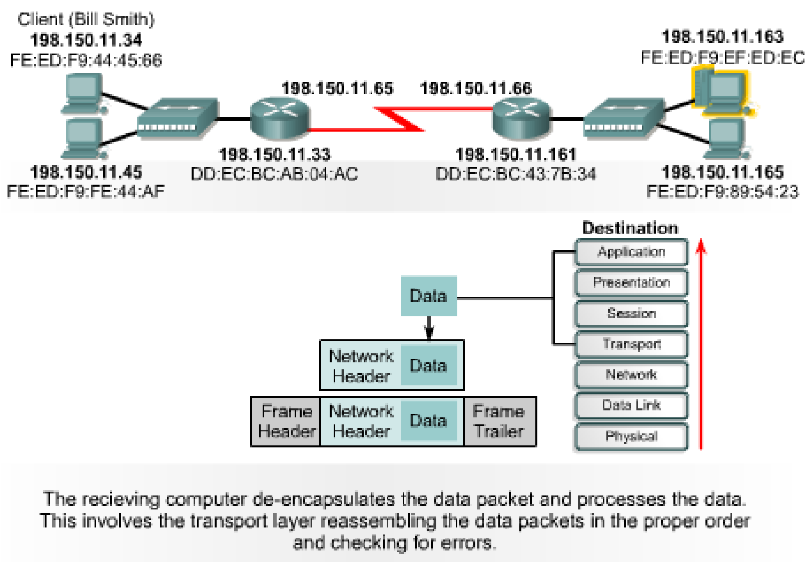


Frame Header		Network Header		Data	Frame Trailer
Destination	Source	Source	Destination		
FE:ED:F9:EF:ED:EC	DD:EC:BC:43:7B:34	198.150.11.34	198.150.11.163	Email	CRC-32

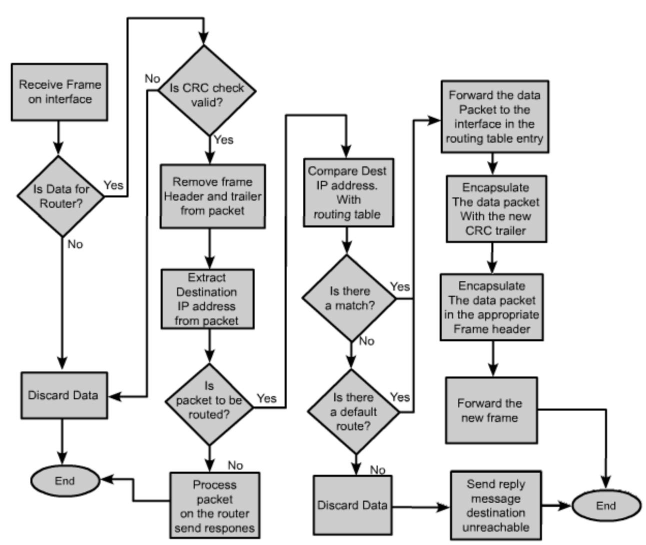


The request is encapsulated for Ethernet transmission and then transmitted on the Ethernet segment. All stations pick up the packet check to see if packet is for them. All devices except for the computer with the IP address 198.150.11.163 discard the packet.

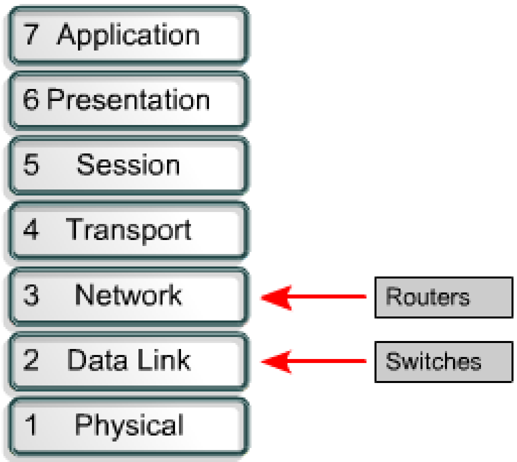
Router Protocol Stripping



Encapsulation changes in a Router

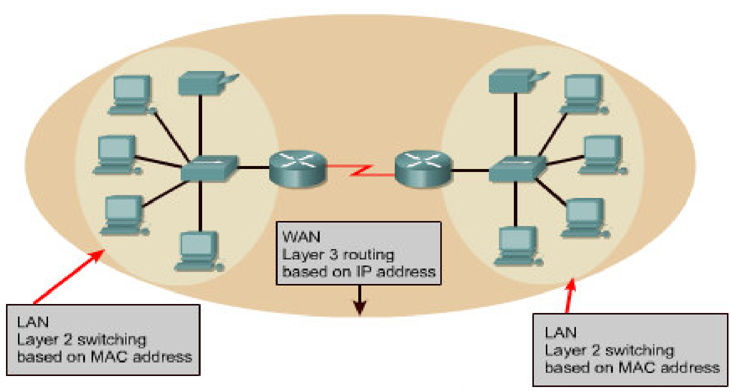


Routing vs. Switching



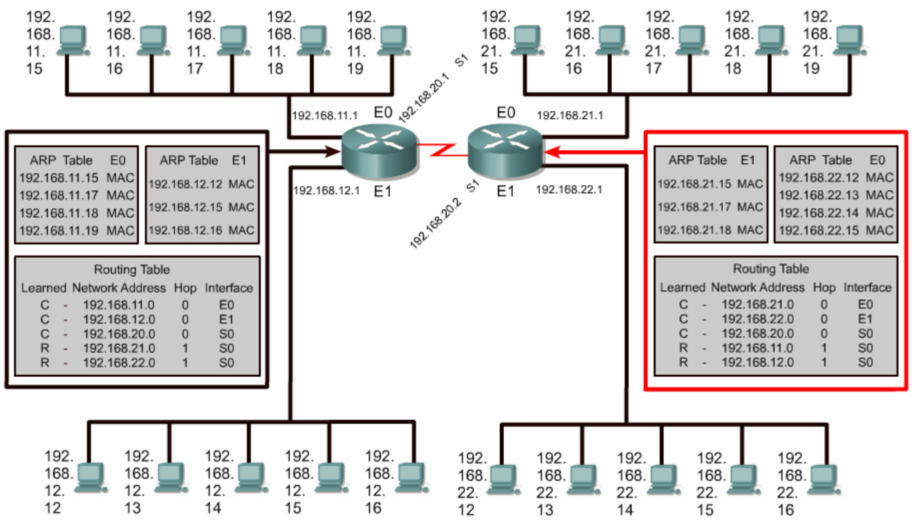
Switching occurs at Layer 2, routing occurs at Layer 3. Routing and switching use different information in the process of moving data from source to destination

Switching and Layer 2 Routing



Layer 2 switching takes place within the LAN. Layer 3 routing moves traffic between broadcast domains. This requires the hierarchical addressing format that a Layer 3 addressing scheme like IP provides.

ARP table and Routing table



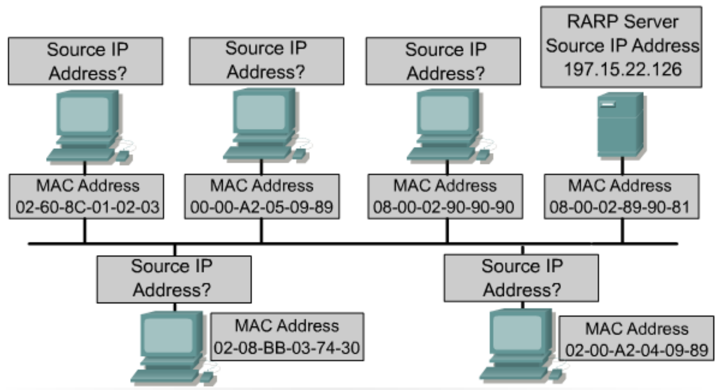
Router and Switch

Features	Router	Switch
Speed	Slower	Faster
OSI Layer	Layer 3	Layer 2
Addressing used	IP	MAC
Broadcasts	Blocks	Forwards
Security	Higher	Lower

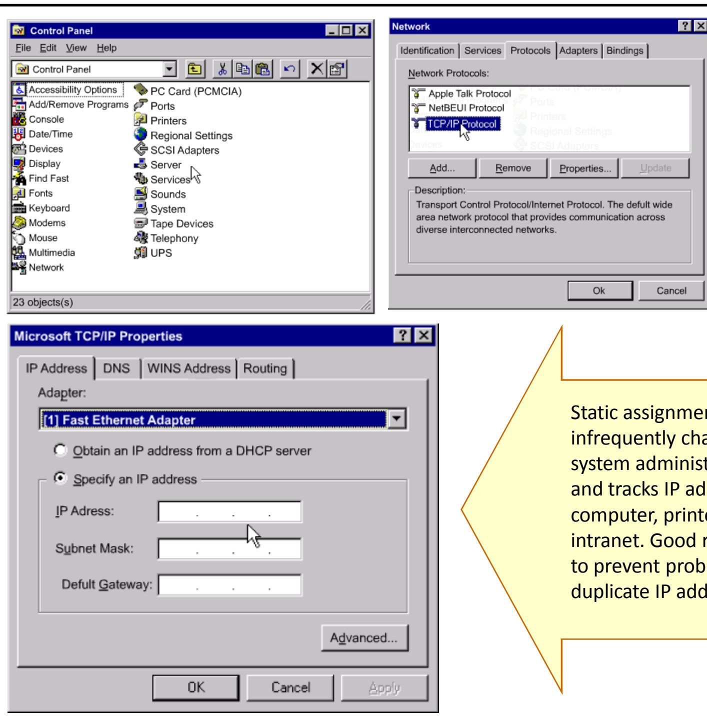
The speed and security are relative comparisons, and depend on the configurations of the device.

- Each computer and router interface maintains an ARP table for Layer 2 communication. The ARP table is only effective for the broadcast domain (or LAN) that it is connected to
- MAC addresses are not logically organized, but IP addresses are organized in a hierarchical manner

Obtaining IP Addresses



Devices come with MAC addresses (layer-2). However, IP addresses (layer-3) require proper configuration. There are basically two ways to obtain IP addresses: static and dynamic.



Static assignment works best on small, infrequently changing networks. The system administrator manually assigns and tracks IP addresses for each computer, printer, or server on the intranet. Good recordkeeping is critical to prevent problems which occur with duplicate IP addresses.

RARP

0 - 15 bits		16 - 31 bits
Hardware Type		Protocol Type
HLen (1 byte)	PLen (1 byte)	Operation
Sender HA (bytes 1 - 4)		
Sender HA (byte 5- 6)		Sender PA (byte 1 - 2)
Sender PA (byte 3 - 4)		Target HA (byte 1 -2)
Target HA (bytes 3 - 6)		
Target PA (bytes 1 - 4)		

RARP *header structure*

Reverse Address Resolution Protocol (RARP) associates a known MAC addresses with an IP addresses. This association allows network devices to encapsulate data before sending the data out on the network. A network device, such as a diskless workstation, might know its MAC address but not its IP address. RARP allows the device to make a request to learn its IP address.

RARP

0 - 15 bits		16 - 31 bits
Hardware Type		Protocol Type
HLen (1 byte)	PLen (1 byte)	Operation
Sender HA (bytes 1 - 4)		
Sender HA (byte 5- 6)		Sender PA (byte 1 - 2)
Sender PA (byte 3 - 4)		Target HA (byte 1 -2)
Target HA (bytes 3 - 6)		
Target PA (bytes 1 - 4)		

RARP *header structure*

ARP and RARP share the same packet format, which is encapsulated on layer-2 frames. They differentiate themselves by the "operation" field.

Operation:
1: ARP request
2: ARP response
3: RARP request
4: RARP response
5: Dynamic RARP request
6: Dynamic RARP response
7: Dynamic RARP error
8: InARP request
9: InARP response

RARP

0 - 15 bits		16 - 31 bits
Hardware Type		Protocol Type
HLen (1 byte)	PLen (1 byte)	Operation
Sender HA (bytes 1 - 4)		
Sender HA (byte 5- 6)		Sender PA (byte 1 - 2)
Sender PA (byte 3 - 4)		Target HA (byte 1 -2)
Target HA (bytes 3 - 6)		
Target PA (bytes 1 - 4)		
RARP *header structure*		

- Hardware Type specifies a hardware interface type for which the sender requires a response (ie. ~layer 2).
- Protocol Type specifies the type of high level protocol address the sender has supplied (ie. ~layer 3).

RARP

0 - 15 bits		16 - 31 bits
Hardware Type		Protocol Type
HLen (1 byte)	PLen (1 byte)	Operation
Sender HA (bytes 1 - 4)		
Sender HA (byte 5- 6)		Sender PA (byte 1 - 2)
Sender PA (byte 3 - 4)		Target HA (byte 1 -2)
Target HA (bytes 3 - 6)		
Target PA (bytes 1 - 4)		
RARP *header structure*		

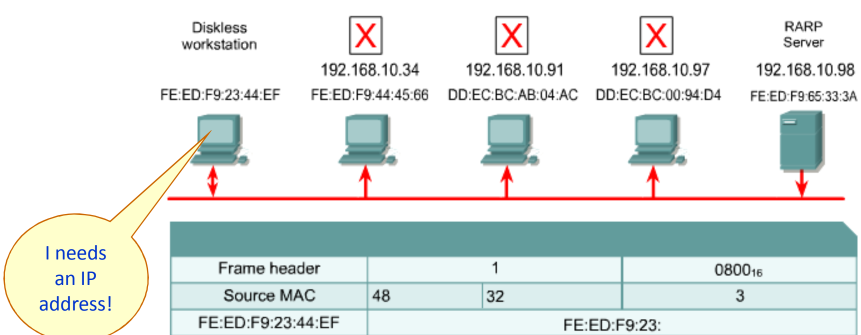
- HLen: Hardware address length.
- PLen: Protocol address length.

RARP

0 - 15 bits		16 - 31 bits
Hardware Type		Protocol Type
HLen (1 byte)	PLen (1 byte)	Operation
Sender HA (bytes 1 - 4)		
Sender HA (byte 5- 6)		Sender PA (byte 1 - 2)
Sender PA (byte 3 - 4)		Target HA (byte 1 -2)
Target HA (bytes 3 - 6)		
Target PA (bytes 1 - 4)		
RARP *header structure*		

- Sender Hardware Address: Hardware address of the sender.
- Sender Protocol Address: Protocol address of the sender.
- Target Hardware Address: Hardware address of the targer.
- Target Protocol Address: Protocol address of the target.

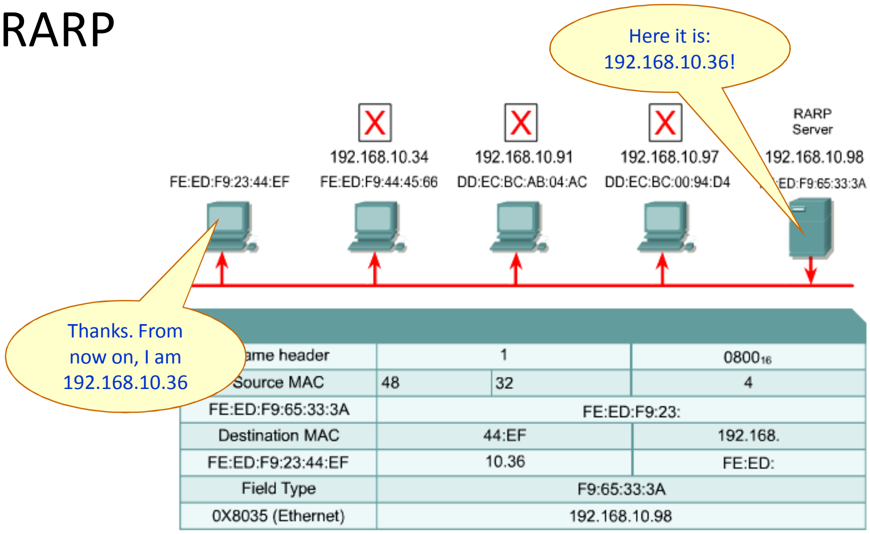
RARP



Frame header	1		0800_{16}
Source MAC	48	32	3
FE:ED:F9:23:44:EF	FE:ED:F9:23:		
Destination MAC	44:EF		undefined
FF:FF:FF:FF:FF:FF	undefined		FF:FF:
Field Type	FF:FF:FF:FF		
0X8035 (Ethernet)	undefined		

- The workstation boots, and then generates an RARP request.
- It broadcasts the request to all hosts (using layer-2 broadcast address).
- All other host discard the request, except the RARP server, who accepts it.

RARP



- The RARP server generates the RARP response which contain its' answer.
- It broadcasts the response to all the hosts.
- The workstation receives the answer and set its IP address.

BOOTP

0 -7 bits	8 -15 bits	16 - 23 bits	24 - 31 bits
Op (1)	Htype (1)	HLen (1)	Hops (1)
Xid (4bytes)			
Seconds (2 bytes)		Unused	
Ciadder (4 bytes)			
Yiadder (4 bytes)			
Siadder (4 bytes)			
Giadder (4bytes)			
Chadder (16 bytes)			
Server Host Name (32 bytes)			
Boot File Name (64 bytes)			
Vendor Specific Area (32 bytes)			
BOOTP *message structure*			

The bootstrap protocol (BOOTP) operates in a client-server environment and only requires a single packet exchange to obtain IP information. However, unlike RARP, BOOTP packets can include the IP address, as well as the address of a router, the address of a server, and vendor-specific information, etc. BOOTP is encapsulated on UDP datagram.

BOOTP

0 -7 bits	8 -15 bits	16 - 23 bits	24 - 31 bits
Op (1)	Htype (1)	HLen (1)	Hops (1)
Xid (4bytes)			
Seconds (2 bytes)		Unused	
Ciadder (4 bytes)			
Yiadder (4 bytes)			
Siadder (4 bytes)			
Giadder (4bytes)			
Chadder (16 bytes)			
Server Host Name (32 bytes)			
Boot File Name (64 bytes)			
Vendor Specific Area (32 bytes)			

BOOTP *message structure*

- Op: Message operation code; can be BOOTREQUEST or BOOTREPLY.
- Htype: Hardware address type.
- HLen: Hardware address length.
- Hops: Clients place zero, this field is used by BOOTP server to send request to another network.

BOOTP

0 -7 bits	8 -15 bits	16 - 23 bits	24 - 31 bits
Op (1)	Htype (1)	HLen (1)	Hops (1)
Xid (4bytes)			
Seconds (2 bytes)		Unused	
Ciadder (4 bytes)			
Yiadder (4 bytes)			
Siadder (4 bytes)			
Giadder (4bytes)			
Chadder (16 bytes)			
Server Host Name (32 bytes)			
Boot File Name (64 bytes)			
Vendor Specific Area (32 bytes)			

BOOTP *message structure*

- Xid: Transaction ID
- Seconds: Seconds elapsed since the client began the address acquisition or renewal process.

BOOTP

0 -7 bits	8 -15 bits	16 - 23 bits	24 - 31 bits
Op (1)	Htype (1)	HLen (1)	Hops (1)
Xid (4bytes)			
Seconds (2 bytes)		Unused	
Ciadder (4 bytes)			
Yiadder (4 bytes)			
Siadder (4 bytes)			
Giadder (4bytes)			
Chadder (16 bytes)			
Server Host Name (32 bytes)			
Boot File Name (64 bytes)			
Vendor Specific Area (32 bytes)			
BOOTP *message structure*			

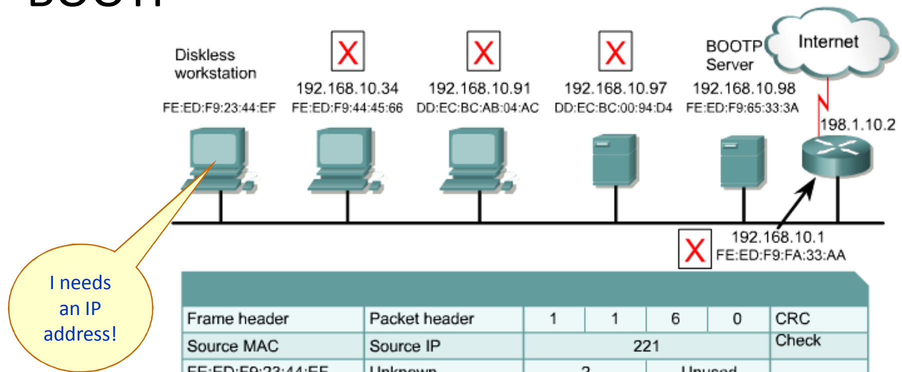
- Ciadder: Client IP address.
- Yiadder: “Your” (client) IP address.
- Siadder: IP address of the next server to use in bootstrap.
- Giadder: Relay agent IP address used in booting via a relay agent.
- Chadder: Client hardware address.

BOOTP

0 -7 bits	8 -15 bits	16 - 23 bits	24 - 31 bits
Op (1)	Htype (1)	HLen (1)	Hops (1)
Xid (4bytes)			
Seconds (2 bytes)		Unused	
Ciadder (4 bytes)			
Yiadder (4 bytes)			
Siadder (4 bytes)			
Giadder (4bytes)			
Chadder (16 bytes)			
Server Host Name (32 bytes)			
Boot File Name (64 bytes)			
Vendor Specific Area (32 bytes)			
BOOTP *message structure*			

- Server Host Name: Specifies particular server to get BOOTP information from.
- Boot File Name:Alow multiple boot files (example: for different OSes).
- Vendor Specific Area: Optional vendor information that can be passed to the host.

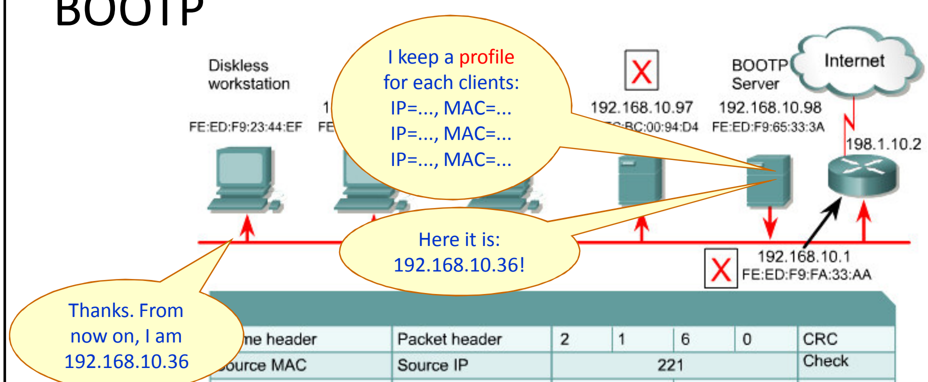
BOOTP



Frame header	Packet header	1	1	6	0	CRC
Source MAC	Source IP	221				Check
FE:ED:F9:23:44:EF	Unknown	2		Unused		
Destination MAC	Destination IP	0				
FE:FF:FF:FF:FF:FF	225.225.225.225	0				
Field Type		0				
0X8035 (Ethernet)		0				
		FE:ED:F9:23:44:EF				

- The workstation boots, and then generates an BOOTP request.
- It broadcasts the request to all hosts (IP source address = unknown).
- All other host discard the request, except the BOOTP server, who accepts it.

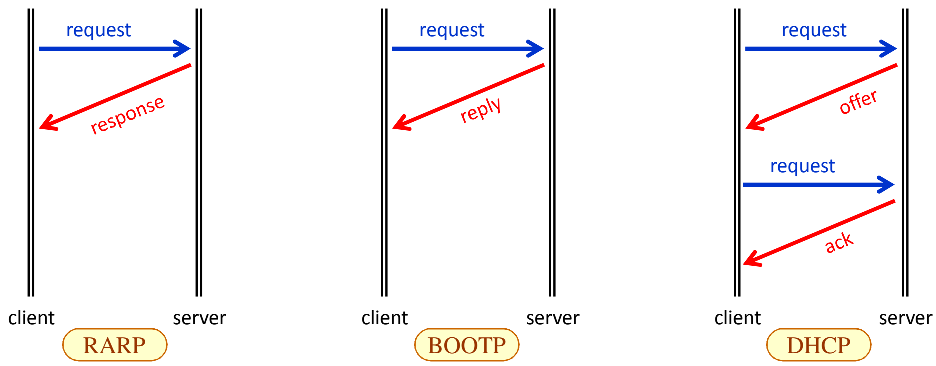
BOOTP



ne header	Packet header	2	1	6	0	CRC
ource MAC	Source IP	221				Check
FE:ED:F9:65:33:3A	192.168.10.98	2		Unused		
Destination MAC	Destination IP	0				
FE:ED:F9:23:44:EF	225.225.225.225	192.168.10.36				
Field Type		192.168.10.97				
0X8035 (Ethernet)		192.168.10.97				
		FE:ED:F9:23:44:EF				

- The BOOTP server generates the BOOTP reply which contain its' answer.
- It broadcasts the response to all the hosts.
- The workstation receives the answer and set its IP address.

DHCP



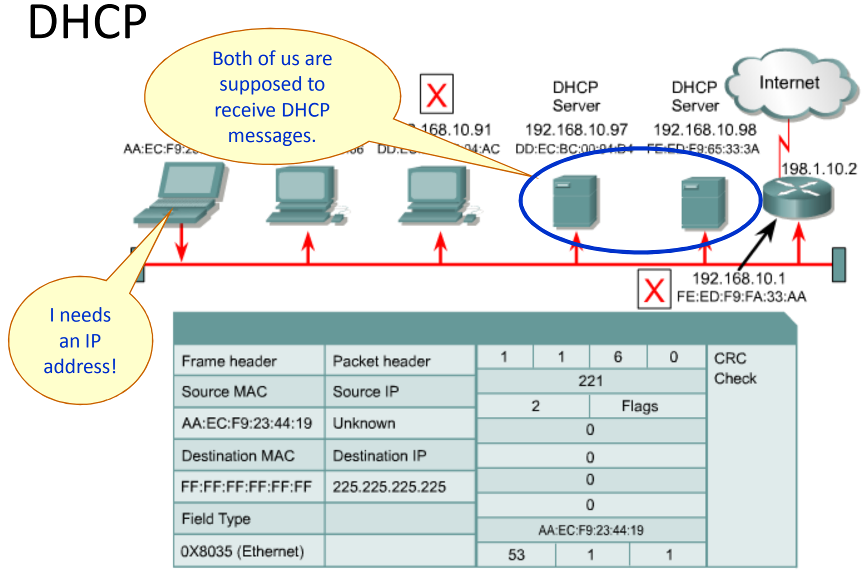
Dynamic host configuration protocol (DHCP) is the successor to BOOTP. Unlike BOOTP, DHCP allows a host to obtain an IP address dynamically without individual profile that the network administrator having to set up for each device. All that is required when using DHCP is a defined range of IP addresses on a DHCP server. The major advantage that DHCP has over BOOTP is that it allows users to be mobile. DHCP offers a one to many ratio of IP addresses and that an address is available to anyone who connects to the network.

DHCP

0 -7 bits	8 -15 bits	16 - 23 bits	24 - 31 bits
Op (1)	Htype (1)	HLen (1)	Hops (1)
Xid (4bytes)			
Seconds (2 bytes)		Flags(2 bytes)	
Ciaddr (4 bytes)			
Yiaddr (4 bytes)			
Siaddr (4 bytes)			
Giaddr (4bytes)			
Chaddr (16 bytes)			
Server Host Name (32 bytes)			
Boot File Name (64 bytes)			
Vendor Specific Area (variable)			
DHCP *message structure*			

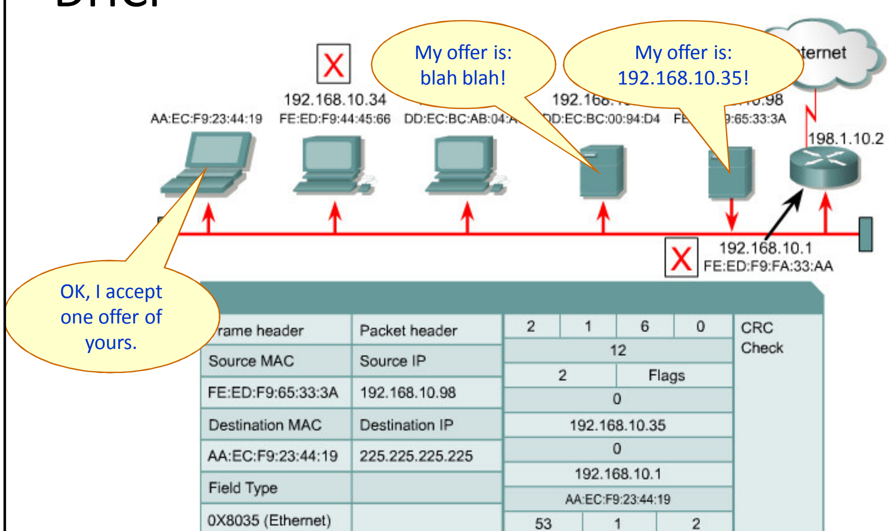
DHCP uses the same message structure of BOOTP, with some extentions (subnet masks, etc.) The idea is that the entire network configuration of a computer can be obtained in one message.

DHCP



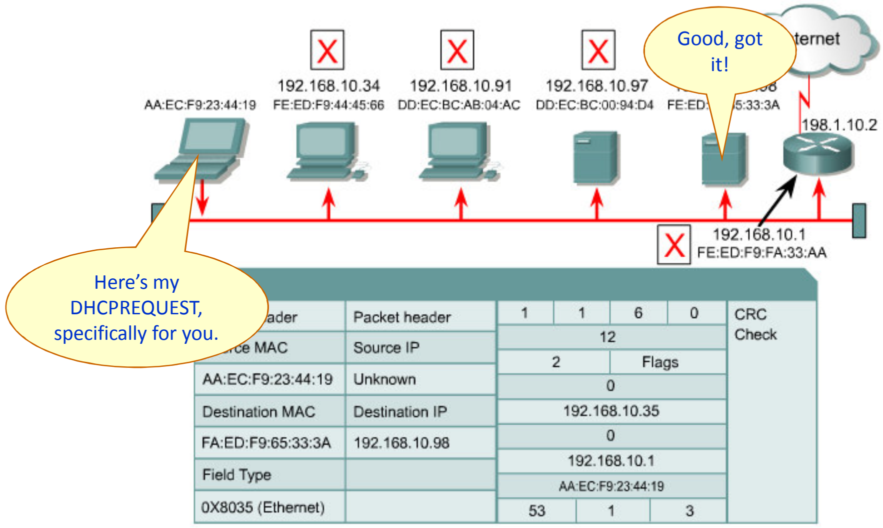
- The laptop boots, and then generates an DHCP request.
- It broadcasts the request to all hosts (to discover who is the server).
- All other host discard the request, except the DHCP servers, who accept it.

DHCP



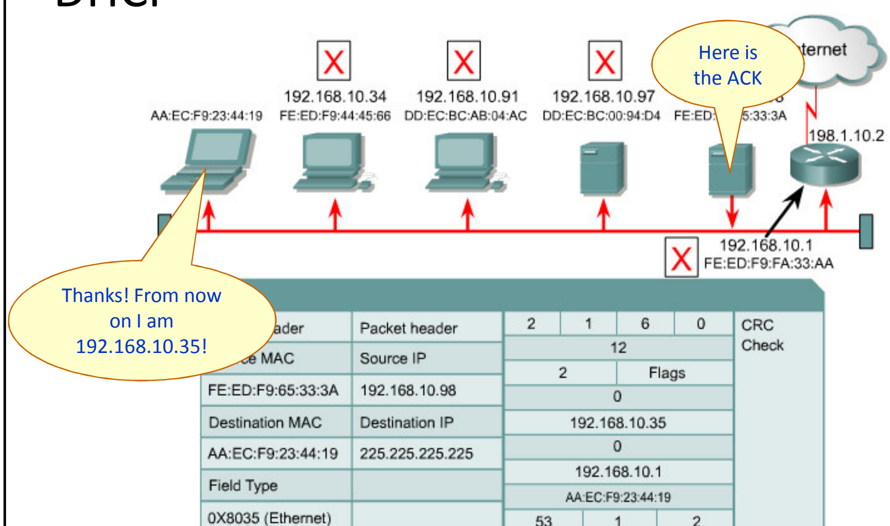
- The DHCP servers generates the DHCP offers which contain its' answer.
- It broadcasts the response to all the hosts.
- The laptop receives the answers, select one of them (the first one).

DHCP



- The laptop sends DCHPREQUEST addressed to the specific DHCP server that has sent the accepted offer.

DHCP



- The DHCP server sends the DHCPACK
- And the laptop sets the IP address accordingly.