Principles of Modern Communications Internetworks

based on 2011 lecture series by Dr. S. Waharte.
Department of Computer Science and Technology,
University of Bedfordshire.

17^{th} January 2013

Outline

TCP/IP concepts

Perspective

- Single switched and wireless networks
  - Operate at Layers 1 and 2 (physical and data link)
  - Standards come almost entirely from OSI
- Internets
  - Operate at layers 3 and 4 (internet and transport)
  - Standards come predominantly from the Internet Engineering Task Force (IETF)
  - Called TCP/IP standards
  - Publications are requests for comments (RFCs)

Major TCP/IP Standards

5 Application	User Applications			Supervisory Applications		
	HTTP	SMTP	Many Others	DNS	Dynamic Routing Protocols	Many Others
4 Transport	TCP				UDP	
3 Internet	IP			ICMP		ARP
2 Data Link	None: Use OSI Standards					
1 Physical	None: Use OSI Standards					

- TCP/IP has core internet and transport standards: IP, TCP, and UDP.

Major TCP/IP Standards

5 Application	User Applications			Supervisory Applications		
	HTTP	SMTP	Many Others	DNS	Dynamic Routing Protocols	Many Others
4 Transport	TCP				UDP	
3 Internet	IP			ICMP		ARP
2 Data Link	None: Use OSI Standards					
1 Physical	None: Use OSI Standards					

- TCP/IP also has many application standards.

Major TCP/IP Standards

Layer						
5 Application	User Applications			Supervisory Applications		
	HTTP	SMTP	Many Others	DNS	Dynamic Routing Protocols	Many Others
4 Transport	TCP				UDP	
3 Internet	IP			ICMP		ARP
2 Data Link	None: Use OSI Standards					
1 Physical	None: Use OSI Standards					

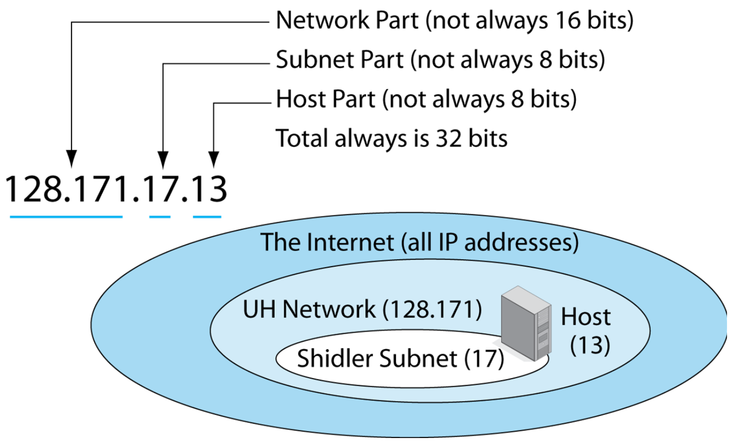
- TCP/IP also has many supervisory standards at the internet, transport, and application layers.

IP, TCP, and UDP

Protocol	Layer	Connection-Oriented/ Connectionless	Reliable/ Unreliable	Lightweight/ Heavyweight
TCP	4 (Transport)	Connection-oriented	Reliable	Heavyweight
UDP	4 (Transport)	Connectionless	Unreliable	Lightweight
IP	3 (Internet)	Connectionless	Unreliable	Lightweight

Hierarchical IP addresses

Hierarchical IP Address



- An IP address usually has three parts.

Hierarchical IP Address

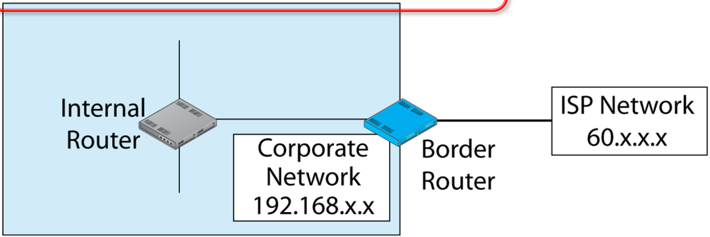
- The network part is given to a firm, ISP, or other entity by a registered number provider.
  - The firm divides its address space into subnets.
    - On each subnet, the host part indicates a particular host.

Hierarchical IP Address

- In an IP address, how long are the network, subnet, and host parts?

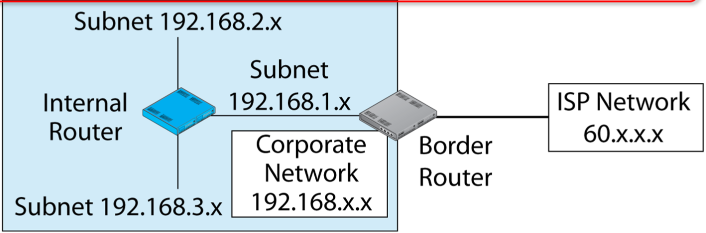
Border Router, Internal Router, Networks, and Subnets

Border routers connect different networks (192.168.x.x & 60.x.x.x)



Border Router, Internal Router, Networks, and Subnets

Internal routers connect different subnets within a network



IP Network and Subnet Masks

- The Problem
  - There is no way to tell by looking at an IP address the sizes of the network, subnet, and host parts individually—only that their total is 32 bits.
  - The solution: masks.

IP Network and Subnet Masks

- Masks
  - In spray painting, you often use a mask.
  - The mask allows part of the paint through but stops the rest from going through.
  - Network and subnet masks do something similar.

IP Network and Subnet Masks

- The solution: masks
  - A mask is a series of initial ones followed by series of final zeros, for a total of 32 bits.
  - Example 1: Sixteen 1s followed by Sixteen 0s
    - 11111111 11111111 00000000 00000000
    - Eight 1s is 255 in dotted decimal notation.
    - Eight 0s is 0 in dotted decimal notation.
    - In dotted decimal notation, 255.255.0.0.
    - In prefix notation, /16.

IP Network and Subnet Masks

- The solution: masks
  - A mask is a series of initial ones followed by series of final zeros, for a total of 32 bits.
  - Example 2: Twenty-four 1s followed by eight 0s
    - 11111111 11111111 11111111 00000000
    - Eight 1s is 255 in dotted decimal notation.
    - Eight 0s is 0 in dotted decimal notation.
    - In dotted decimal notation, 255.255.255.0.
    - In prefix notation, /24.

IP Network and Subnet Masks

- The solution: masks
  - Your turn.
  - Draw the 32 bits of the mask /14. Do not do it in dotted decimal notation. Write the bits in groups of eight. Here's a start:
  - 11111111 11

IP Network and Subnet Masks

- Masks are applied to 32-bit IP addresses.

IP Address bit	1	0	1	0
Mask bit	1	1	0	0
Result bit	1	0	0	0

If the mask bit = 0, the result is always 0.

If the mask bit = 1, the result is always the IP address bit in that position.

IP Network and Subnet Masks

Network Mask	Dotted Decimal Notation			
Destination IP Address	128	171	17	13
Network Mask	255	255	0	0
Bits in network part, followed by zeros	128	171	0	0

IP Network and Subnet Masks

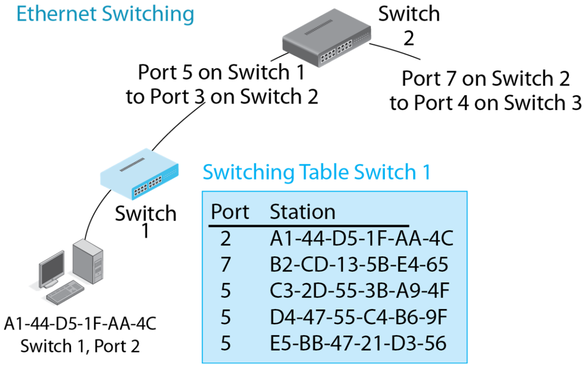
Subnet Mask	Dotted Decimal Notation			
Destination IP Address	128	171	17	13
Subnet Mask	255	255	255	0
Bits in network part, followed by zeros	128	171	17	0

Router operation

Router Operation

- We have talked about routers since Lecture 1.
- Now we will finally see what they do.
- We will see what happens after a packet addressed to a particular IP address arrives.
- But we will first recap how Ethernet switches handle arriving frames.

Ethernet Switching versus IP Routing

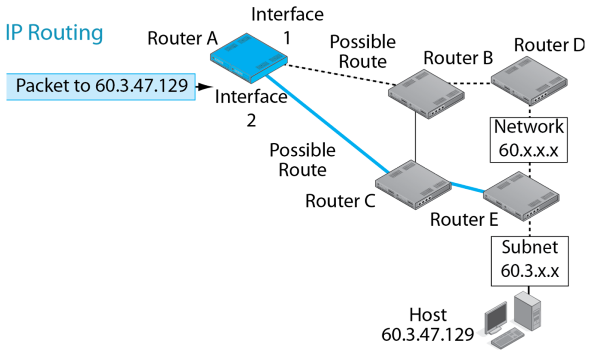


Switching Table Switch 1

Port	Station
2	A1-44-D5-1F-AA-4C
7	B2-CD-13-5B-E4-65
5	C3-2D-55-3B-A9-4F
5	D4-47-55-C4-B6-9F
5	E5-BB-47-21-D3-56

- Ethernet switches are organized in a hierarchy, so there is only one possible port to send a frame out and so only one row per address.

Ethernet Switching versus IP Routing



- Routers are arranged in meshes with multiple alternative routes between hosts.
- So a router may send a packet out more than one interface (port) and still get the packet to its destination host.

Ethernet Switching versus IP Routing

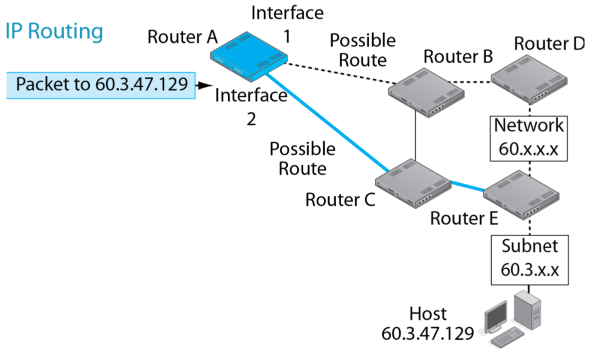
Routing Table for Router A

Route	IP Address Range	Interface	Next-Hop Router
1	60.3.x.x	1	B
2	128.171.x.x	1	B
3	60.3.47.x	2	C
4	10.5.3.x	4	Q
5	128.171.17.x	3	Local
6	10.4.3.x	2	C

- So in routing tables, multiple rows may give conflicting information about what to do with a packet.

The Routing Process

- Routing
  - Processing an individual packet and passing it on its way is called routing.



The Routing Process

- The Routing Table
  - Each router has a routing table that it uses to make routing decisions.
  - Routing Table Rows
    - Each row represents a route for a range of IP addresses—often packets going to the same network or subnet.

Route	IP Address Range	Interface
1	60.3.x.x	1
2	128.171.x.x	1
3	60.3.47.x	2
4	10.5.3.x	4
5	128.171.17.x	3
6	10.4.3.x	2

The Routing Process

- Ethernet switching table rows are rules for handling individual Ethernet MAC addresses.
- Router routing table rows are rules for handling ranges of IP addresses.

Routing Table Columns

Column	Meaning
Row Number	Designates the row in the routing table
Destination	Range of IP addresses governed by the row
Mask	Mask for the row
Metric	Quality of the route listed in this row
Interface	The interface (port) to use to send the packet out
Next–Hop Router	The device (router or destination host) on the interface subnet to receive the packet

The Routing Process

- A Routing Decision
  - Whenever a packet arrives, the router looks at its IP address, then. . .
  - Step 1: Finds All Row Matches
  - Step 2: Finds the Best-Match Row
  - Step 3: Sends the Packet Back out According to Directions in the Best-Match Row

The Routing Process

- Step 1: Finding All Row Matches
  - The router looks at the destination IP address in an arriving packet.
  - It matches this IP address against each row.
    - It begins with the first row.
    - It looks at every subsequent row.
    - It stops only after it looks at the last row.

The Routing Process

- Step 1: Finding All Row Matches
  - Each row is a rule for routing packets within a range of IP addresses. The IP address range is indicated by a destination and a mask.

Row	Destination Network or Subnet	Mask
1	128.171.0.0	/16
2	172.30.33.0	/24
3	60.168.6.0	/24

The Routing Process

- Step 1: Finding All Row Matches
  - Each row is a rule for routing packets within a range of IP addresses.
  - The router has the IP address of an arriving packet.
  - It applies the mask in a row to the arriving IP address.
  - If the result is equal to the value in the destination column, then the IP address of the packet is in the row's range. The row is a match.

The Routing Process

- Example 1: A Destination IP Address that Is NOT in the Range of the Row
  - Dest. IP Address of Packet 60. 43. 7. 8
  - Apply the (Network) Mask 255.255. 0. 0
  - Result of Masking 60. 43. 0. 0
  - Destination Column Value 128.171. 0. 0
  - Does Destination Match the Masking Result? No
  - Conclusion: Not a Match

The Routing Process

- Example 2: A Destination IP Address that IS in the Range of the Row
  - Dest. IP Address of Packet 128.171. 17. 13
  - Apply the (Network) Mask 255.255. 0. 0
  - Result of Masking 128.171. 0. 0
  - Destination Column Value 128.171. 0. 0
  - Does Destination Match the Masking Result? Yes
  - Conclusion: Is a Match

The Routing Process

- Step 1: Finding All Row Matches
  - The router does this to ALL rows because there may be multiple matches.
  - Question 1: If there are 127,976 rows and the only rows that match are the second and seventh rows, what row will the router examine first?
  - Question 2: If there are 127,976 rows and the only rows that match are the second and seventh rows, how many rows will the router have to check to see if they match?

The Routing Process

- A Routing Decision
  - Whenever a packet arrives, the router looks at its IP address, then. . .
  - Step 1: Finds All Row Matches
  - Step 2: Finds the Best-Match Row
  - Step 3: Sends the Packet Back out According to Directions in the Best-Match Row

The Routing Process

- To find the best-match row, the router uses the mask column and perhaps the metric column.

Row	Mask	Metric (Cost)
1	/16	47
2	/24	0
3	/24	12

The Routing Process

- Step 2: Find the Best-Match Row
  - The router examines the matching rows it found in Step 1 to find the best-match row.
  - Basic Rule: it selects the row with the longest match (Initial 1s in the row mask).
    - Row 99 matches, mask is /16 (255.255.0.0)
    - Row 78 matches, mask is /24 (255.255.255.0)
    - Select Row 78 as the best-match row.

The Routing Process

- Step 2: Find the Best-Match Row
  - Basic Rule: it selects the row with the longest match (Initial 1s in the row mask).
  - Tie Breaker: if there is a tie for longest match, select among the tie rows based on metric.
    - There is a tie for longest length of match.
    - Row 668 has match length /16, cost metric = 20.
    - Row 790 has match length /16, cost metric = 16.
    - Router selects 790, which has the best cost.

The Routing Process

- Step 2: Find the Best-Match Row
  - Basic Rule: it selects the row with the longest match (Initial 1s in the row mask).
  - Tie Breaker: if there is a tie on longest match, select among the tie rows based on metric.
    - There is a tie for longest length of match.
    - Row 668 has match /16, speed metric = 20.
    - Row 790 has a match /16, speed metric = 16.
    - Router selects 668, which has the best speed.

The Routing Process

- Step 2: Find the Best-Match Row
  - The following rows are matches.
    - Row / Mask / Metric
    - 220 /24 / speed metric = 40
    - 345 /18 / speed metric = 50
    - 682 /8 /speed metric = 40
  - Question: What is the best-match row? Why?

The Routing Process

- Step 2: Find the Best-Match Row
  - The following rows match.
    - 107 / 12 / speed metric = 30
    - 220 / 14 / speed metric = 100
    - 345 / 18 / speed metric = 50
    - 682 / 18 / speed metric = 40
  - Question: What is the best-match row? Why?

The Routing Process

- A Routing Decision
  - Whenever a packet arrives, the router looks at its IP address, then...
  - Step 1: Finds All Row Matches
  - Step 2: Finds the Best-Match Row
  - Step 3: Sends the Packet Back out According to Directions in the Best-Match Row

The Routing Process

- Step 3: Send the Packet Back out
    - Send the packet out the router interface (port) designated in the best-match row.
    - Send the packet to the router in the next-hop router column.
- **Router Port = Interface**

Row	Interface	Next-Hop Router
1	2	G
2	1	Local
3	2	H

The Routing Process

- Step 3: Send the Packet Back out
  - If the address says Local, the destination host is out that interface.
    - Sends the packet to the destination IP address in a frame.

Row	Interface	Next-Hop Router
1	2	G
2	1	Local
3	2	H

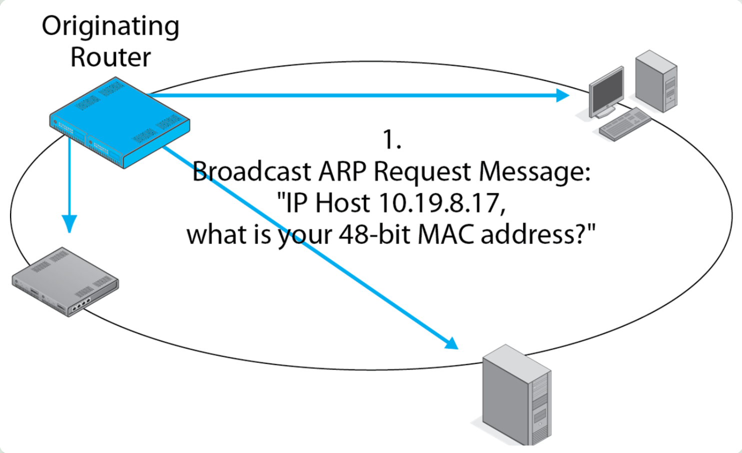
The Routing Process

- A Routing Decision
  - Whenever a packet arrives, the router looks at its IP address, then. . .
  - Step 1: Finds All Row Matches
  - Step 2: Finds the Best-Match Row
  - Step 3: Sends the Packet Back out According to Directions in the Best-Match Row

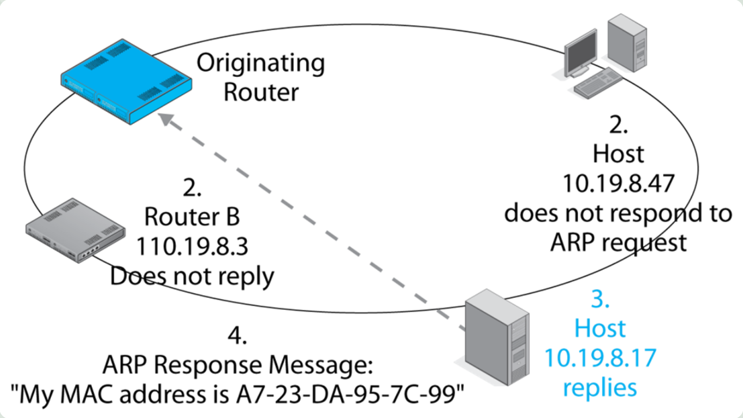
Address Resolution Protocol (ARP)

- The Problem
  - The router wants to send the packet to a next-hop router or to the destination host.
  - The router knows the destination IP address of the NHR or destination host.
  - But it must send the packet in a frame suitable for that subnet.
  - The router does not know the destination device's data link layer address.
  - It must learn it using the address resolution protocol (ARP).

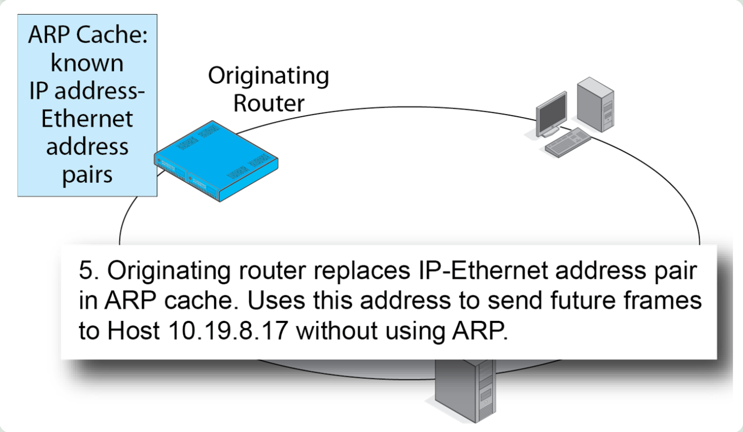
Address Resolution Protocol (ARP)



Address Resolution Protocol (ARP)



Address Resolution Protocol (ARP)



IPv4 and IPv6

IPv4 and IPv6 Packets

<table>
<tr><td>Bit 0</td><td colspan="3">IP Version 4 Packet</td><td colspan="2">Bit 31</td></tr>
<tr><td>Version
(4 bits)
Value is 4 (0100)</td><td>Header Length
(4 bits)</td><td>Diff-Serv
(8 bits)</td><td colspan="3">Total Length
(16 bits)
Length in octets</td></tr>
<tr><td colspan="3">Identification (16 bits)
Unique value in each original IP packet</td><td>Flags
(3 bits)</td><td colspan="2">Fragment Offset (13 bits)
Octets from start of original IP fragment’ s data field</td></tr>
<tr><td colspan="2">Time to Live
(8 bits)</td><td>Protocol (8 bits)
1=ICMP, 6=TCP, 17=UDP</td><td colspan="3">Header Checksum
(16 bits)</td></tr>
</table>

- IPv4 is the dominant version of IP today. The version number in its header is 4 (0100).
- The header length and total length field tell the size of the packet.
- The Diff-Serv field can be used for quality of service labeling.

IPv4 and IPv6 Packets

Bit 0 **IP Version 4 Packet** Bit 31

<table>
<tr><td>Version
(4 bits)
Value is 4 (0100)</td><td>Header Length
(4 bits)</td><td>Diff–Serv
(8 bits)</td><td colspan="2">Total Length
(16 bits)
Length in octets</td></tr>
<tr><td colspan="3">Identification (16 bits)
Unique value in each original IP packet</td><td>Flags
(3 bits)</td><td>Fragment Offset (13 bits)
Octets from start of original IP fragment's data field</td></tr>
<tr><td colspan="2">Time to Live
(8 bits)</td><td>Protocol (8 bits)
1=ICMP, 6=TCP, 17=UDP</td><td colspan="2">Header Checksum
(16 bits)</td></tr>
</table>

- The second row is used for reassembling fragmented IP packets, but IP fragmentation is quite rare, so we will not look at these fields.

IPv4 and IPv6 Packets

Bit 0 — **IP Version 4 Packet** — Bit 31

Version (4 bits) Value is 4 (0100)	Header Length (4 bits)	Diff–Serv (8 bits)	Total Length (16 bits) Length in octets	
Identification (16 bits) Unique value in each original IP packet			Flags (3 bits)	Fragment Offset (13 bits) Octets from start of original IP fragment’s data field
Time to Live (8 bits)		Protocol (8 bits) 1=ICMP, 6=TCP, 17=UDP	Header Checksum (16 bits)	

- The sender sets the time-to-live value (usually 64 to 128). Each router along the way decreases the value by one. A router decreasing the value to zero discards the packet. It may send an ICMP error message.

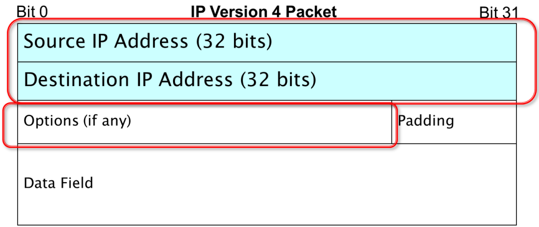
IPv4 and IPv6 Packets

Bit 0 — **IP Version 4 Packet** — Bit 31

Version (4 bits) Value is 4 (0100)	Header Length (4 bits)	Diff-Serv (8 bits)	Total Length (16 bits) Length in octets	
Identification (16 bits) Unique value in each original IP packet			Flags (3 bits)	Fragment Offset (13 bits) Octets from start of original IP fragment' s data field
Time to Live (8 bits)		Protocol (8 bits) 1=ICMP, 6=TCP, 17=UDP	Header Checksum (16 bits)	

- The protocol field describes the message in the data field (1=ICMP, 6=TCP, 17=UDP, etc).
- The header checksum is used to find errors in the header. If a packet has an error, the router drops it.
- There is no retransmission at the internet layer, so the internet layer is still unreliable.

IPv4 and IPv6 Packets



- The source and destination IP addresses are 32 bits long, as you would expect.
- Options can be added, but these are rare.

IPv4 and IPv6 Packets

Bit 0 **IP Version 6 Packet** Bit 31

Version (4 bits) Value is 6 (0110)	Diff–Serv (8 bits)	Flow Label (20 bits) Marks a packet as part of a specific flow	
Payload Length (16 bits)		Next Header (8 bits) Name of next header	Hop Limit (8 bits)
Source IP Address (128 bits)			
Destination IP Address (128 bits)			
Next Header or Payload (Data Field)			

- IP Version 6 is the emerging version of the Internet protocol.
- Has 128-bit addresses for an almost unlimited number of IP addresses.
- Needed because of rapid growth in Asia. Also needed because of the exploding number of mobile devices.

IPv4 and IPv6 Packets

- IP Version 4
  - 32-bit addresses
  - 232 possible addresses
  - 4,294,967,296 (about 4 billion)
  - Running out of these
- IP Version 6
  - 128-bit addresses
  - 2128 possible addresses
  - 340,282,366,920,938,000,000,000,000,000,000,000,000 addresses

TCP and UDP

UDP

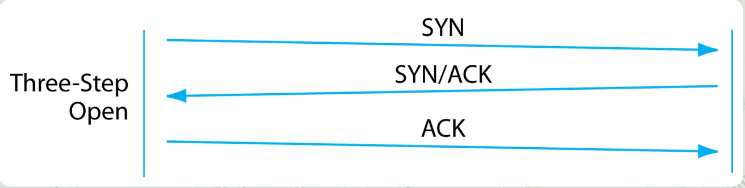
Source Port	Destination Port
Length	UDP Checksum
Data Field	

- UDP does error detection but not error correction. It is not reliable.

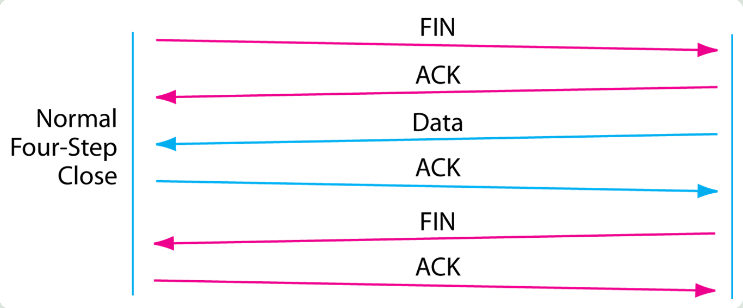
UDP

- Length field gives the length of the data field in octets.
  - The length field is 16 bits long.
  - So the maximum size of the data field is 65,536 octets.
- UDP does not do fragmentation like TCP.
  - So the entire application message must fit in a single UDP datagram (message).

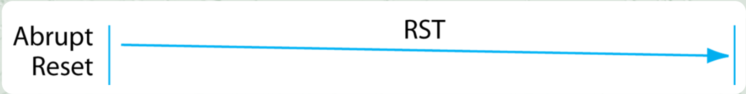
TCP Session Openings and Closings



TCP Session Openings and Closings



TCP Session Openings and Closings



- Abrupt TCP Close closes the connection immediately. Other side does not reply.

Use of TCP (and UDP) Port Numbers

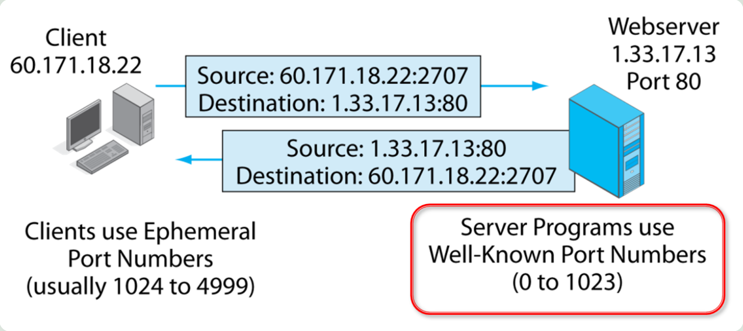
Source Port	Destination Port
Length	UDP Checksum
Data Field	

- TCP and UDP have port numbers.

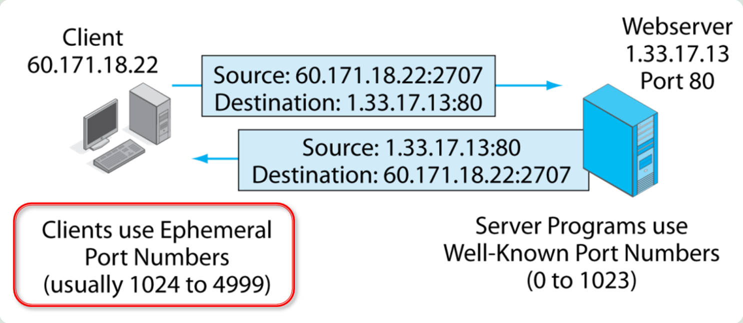
Use of TCP (and UDP) Port Numbers

- Sockets
  - IP address, colon, port number
  - 128.171.17.13:80
  - Designates a particular application or connection (port number) on a particular host (IP address).

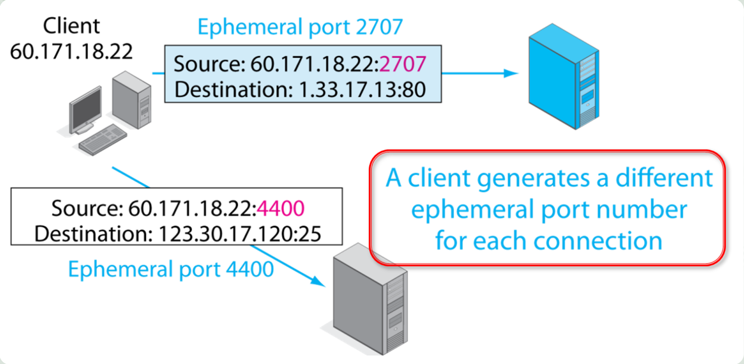
Use of TCP (and UDP) Port Numbers



Use of TCP (and UDP) Port Numbers



Use of TCP (and UDP) Port Numbers



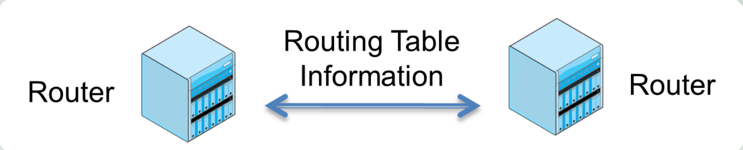
TCP/IP SUPERVISORY STANDARDS

TCP/IP Supervisory Protocols

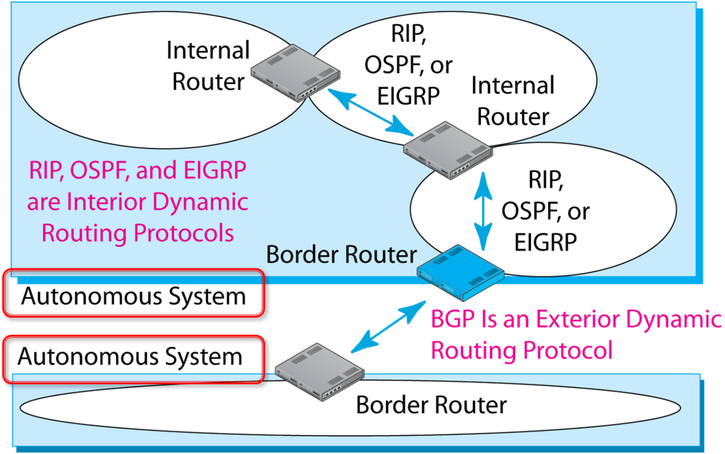
- In addition to IP, TCP, UDP, and user application protocols, TCP/IP has many supervisory protocols to help manage internets.

TCP/IP Supervisory Protocols

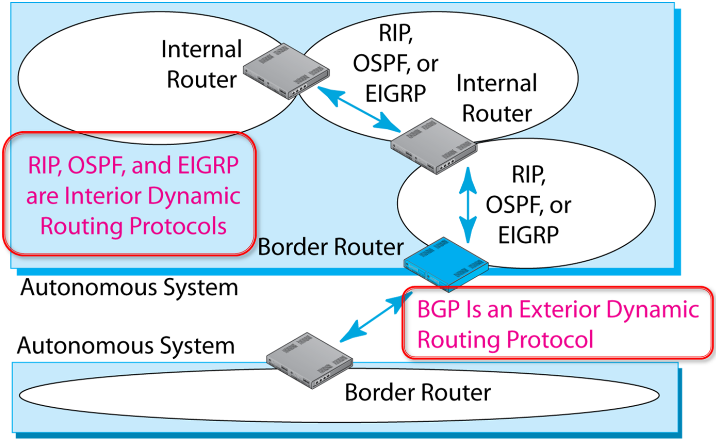
- Dynamic routing protocols allow routers to share routing table information. Dynamic routing protocols are the ways routers normally get the information in their routing tables.



Dynamic Routing Protocols



Dynamic Routing Protocols



Dynamic Routing Protocols

Dynamic Routing Protocol	Interior or Exterior Routing Protocol?	Remarks
RIP (Routing Information Protocol)	Interior	Only for small autonomous systems with low needs for security
OSPF (Open Shortest Path First)	Interior	For large autonomous systems that only use TCP/IP
EIGRP (Enhanced Interior Gateway Routing Protocol)	Interior	Proprietary Cisco Systems protocol. Not limited to TCP/IP routing. Also handles IPX/SPX, SNA, and so forth.

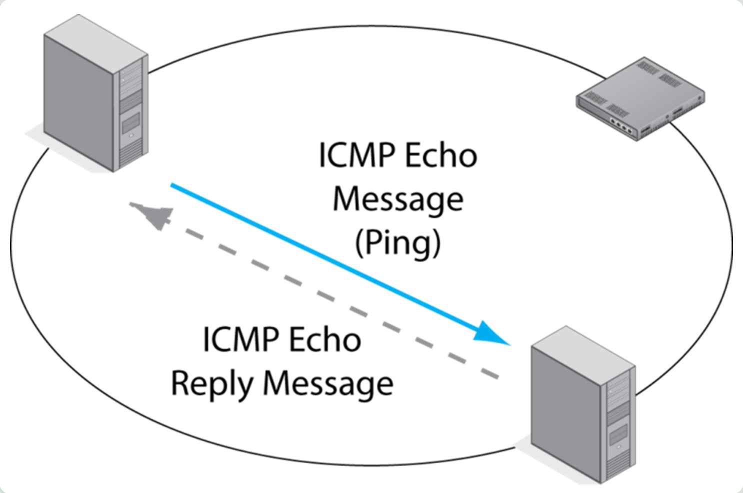
Dynamic Routing Protocols

Dynamic Routing Protocol	Interior or Exterior Routing Protocol?	Remarks
BGP (Border Gateway Protocol)	Exterior	Organization cannot choose what exterior routing protocol it will use

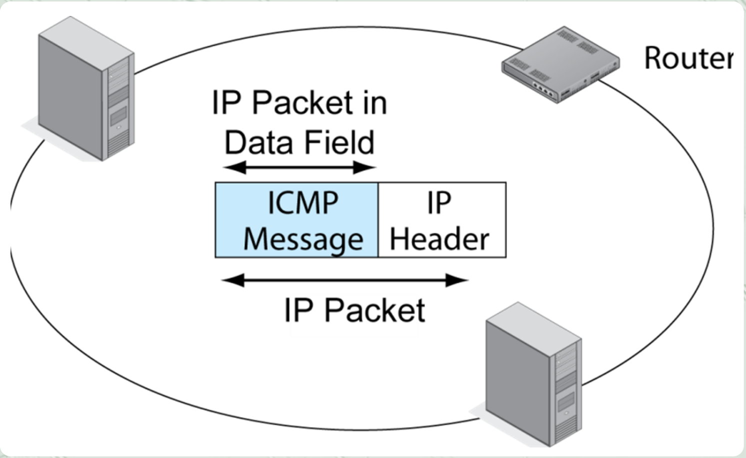
TCP/IP Supervisory Protocols

- Internet Control Message Protocol (ICMP)
  - A general protocol for sending control information between routers and hosts
    - Error messages
    - Pings (Echo messages)
    - And so on
    - Supplements IP packet forwarding with supervisory information
    - IP is RFC 791; ICMP is RFC 792

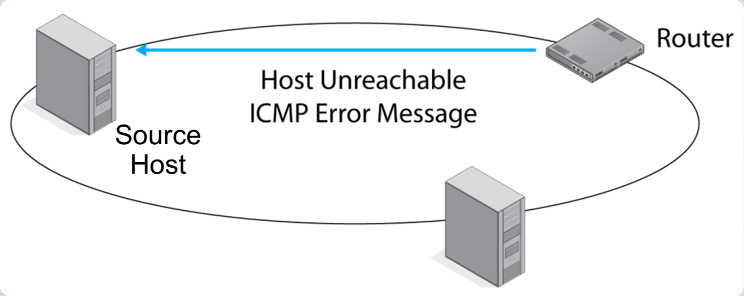
Internet Control Message Protocol (ICMP)



Internet Control Message Protocol (ICMP)



Internet Control Message Protocol (ICMP)

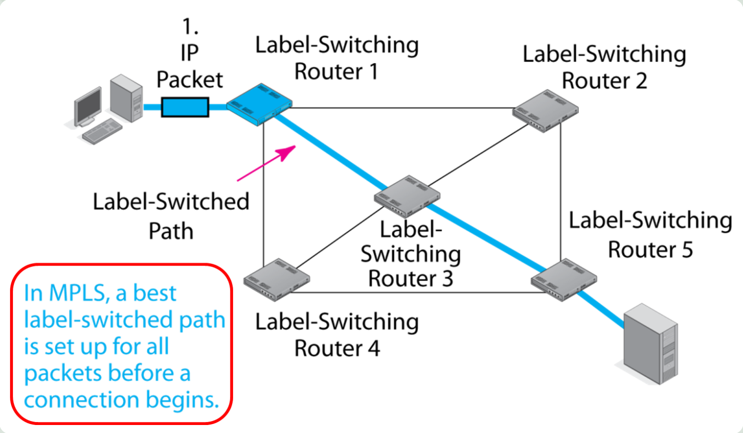


Multiprotocol Label Switching (MPLS)

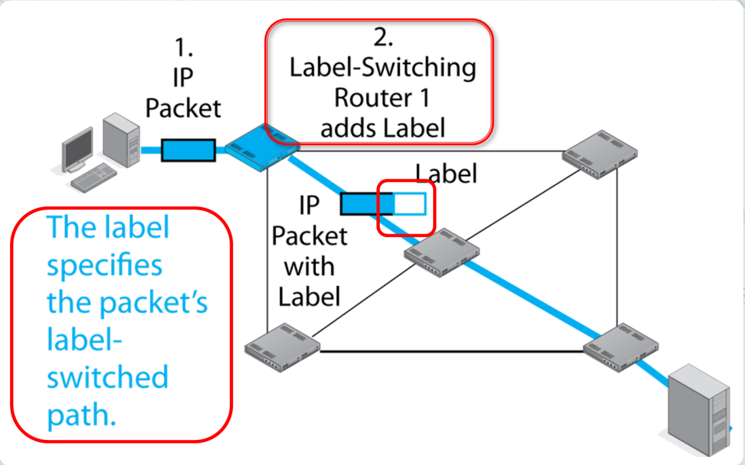
Multiprotocol Label Switching

- The issue
  - Routers traditionally look at packets in isolation, going through the three steps we saw earlier.
  - Even if the next packet is going to the same destination IP address, the router will go through all three steps.
  - This is expensive.
- MPLS addresses this issue.
  - The best route for a range of IP addresses is identified before sending data.

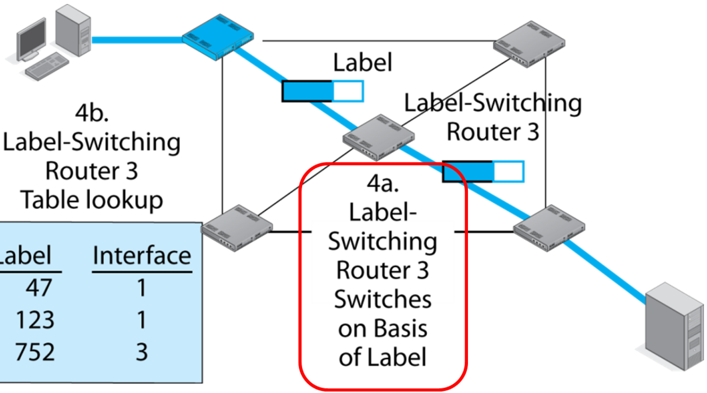
Multiprotocol Label Switching (MPLS)



Multiprotocol Label Switching (MPLS)

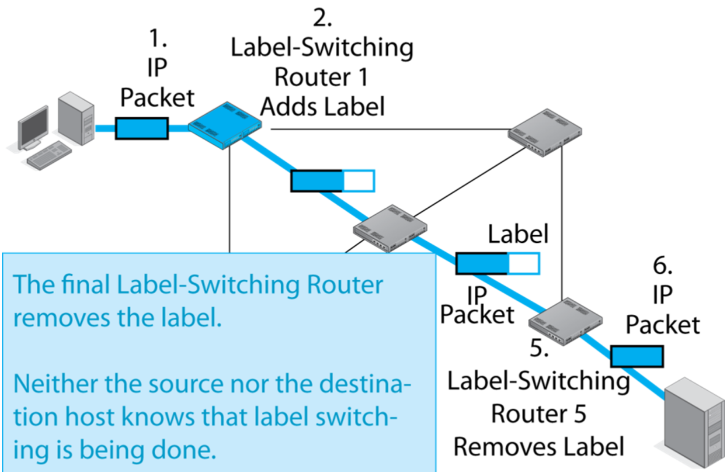


Multiprotocol Label Switching (MPLS)



Label	Interface
47	1
123	1
752	3

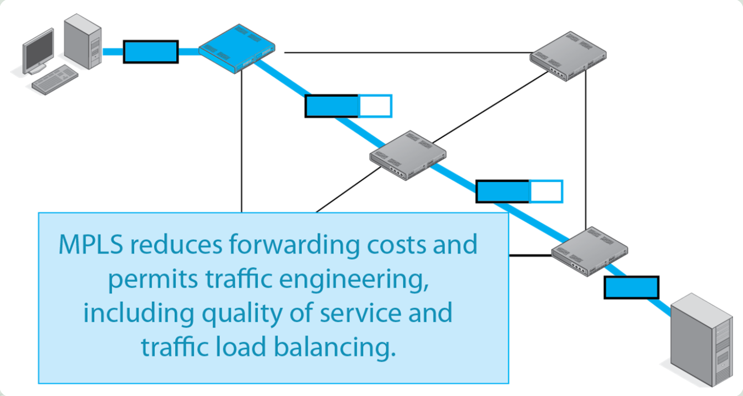
Multiprotocol Label Switching (MPLS)



The final Label-Switching Router removes the label.

Neither the source nor the destination host knows that label switching is being done.

Multiprotocol Label Switching (MPLS)



Multiprotocol Label Switching (MPLS)

- Implementing MPLS is difficult.
- Many individual ISPs and corporations to it.
- Some individual ISPs have "peering" arrangements with other individual ISPs to do it.
- There is no general way to move MPLS out to all ISPs and organizations.