CprE 530

Lecture 10

Topics

- 1. Addressing
- 2. Routing
- 3. Packet Formats
- 4. ICMP   Internet Control Message Protocol

Routing

- All hosts and gateways store routing tables
- Each row in the route table contains:
  - Destination address or address range
  - Next hop for that destination address range
  - The physical interface to use for that address range. (i.e.: which Ethernet card to use)

Example:

Destination	Next	Interface
129.186.4.0	129.186.5.254	en0

Routing

In order to route a packet:

1. IP layer finds the route table entry where the destination address matches the range given in the table.
2. If the next hop falls within the local network, the packet is sent directly to the destination. Otherwise the packet is sent to the next hop.

Next Hop Routing

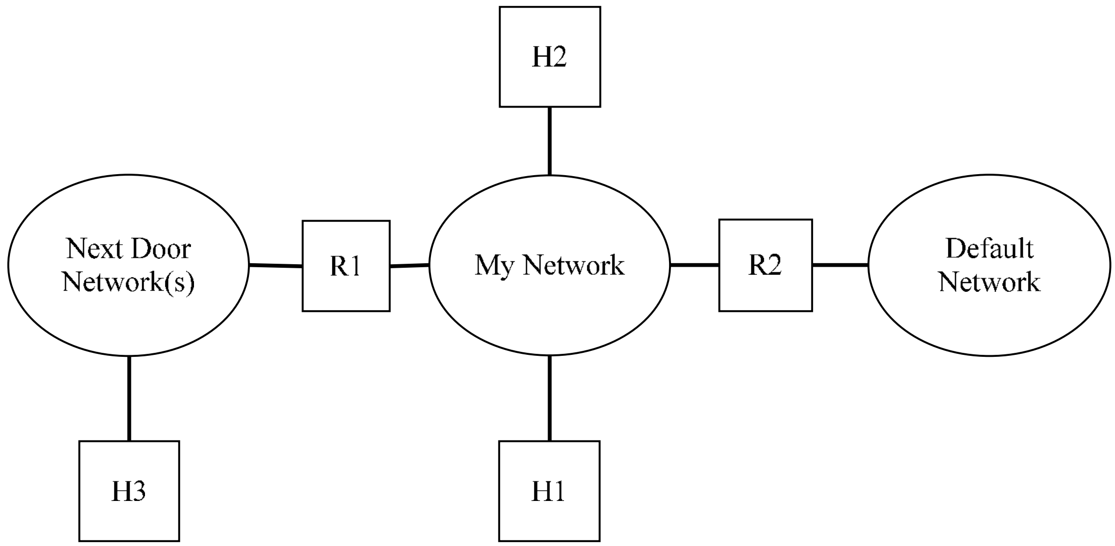


Figure 6.6 IP Next Hop Routing

Routing

Netmask

– Determines which part of the IP address is network and which part is host
– Allows for the ability to create subnetworks
– Example: a netmask of 255.255.255.0 indicates that the first 3 bytes of the IP address is the network, and the last 8 bytes is the host.
– The above netmask allows for 254 subnetworks each with up to 254 attached hosts.
– The following are examples of subnetworks:
  • 129.186.5.0   129.186.15.0   129.186.55.0

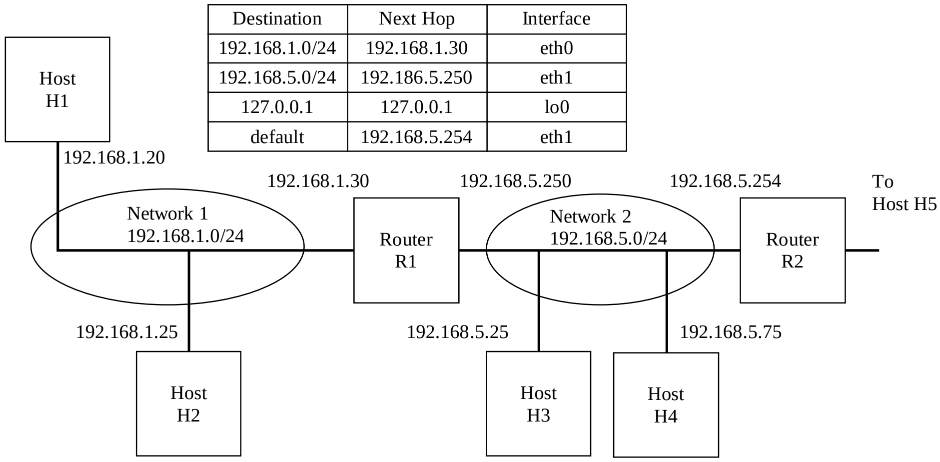
Routing

We will study routing using three scenarios:

1. A simple network with only one router
2. A network with multiple routers
3. A single network with multiple IP's

Route Table Router R1

Destination	Next Hop	Interface
192.168.1.0/24	192.168.1.30	eth0
192.168.5.0/24	192.186.5.250	eth1
127.0.0.1	127.0.0.1	lo0
default	192.168.5.254	eth1



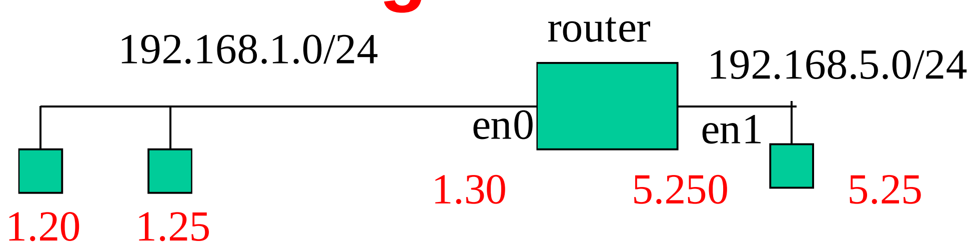
Route Table Host H1

Destination	Next Hop	Interface
192.168.1.0/24	192.168.1.20	eth0
127.0.0.1	127.0.0.1	lo0
default	192.168.1.30	eth0

Route Table Host H3

Destination	Next Hop	Interface
192.168.5.0/24	192.168.5.25	eth0
192.168.1.0/24	192.186.5.250	eth0
127.0.0.1	127.0.0.1	lo0
default	192.168.5.254	eth0

Routing Scenario 1



Packet from H1 to H2 (same network)

IP Address		Hardware Address	
SRC	DEST	SRC	DEST
H1	H2	H1	H2

Packet from H1 to H3 (Next door network)

IP Address		Hardware Address	
SRC	DEST	SRC	DEST
H1	H2	H1	R1 (EN0)
H1	H2	R1 (EN1)	H3

Routing Scenario 1

Steps involved in sending a packet from H1 to H2:

Destination	**Next Hop**
192.168.1.0/24	192.168.1.20
Default	192.168.1.30

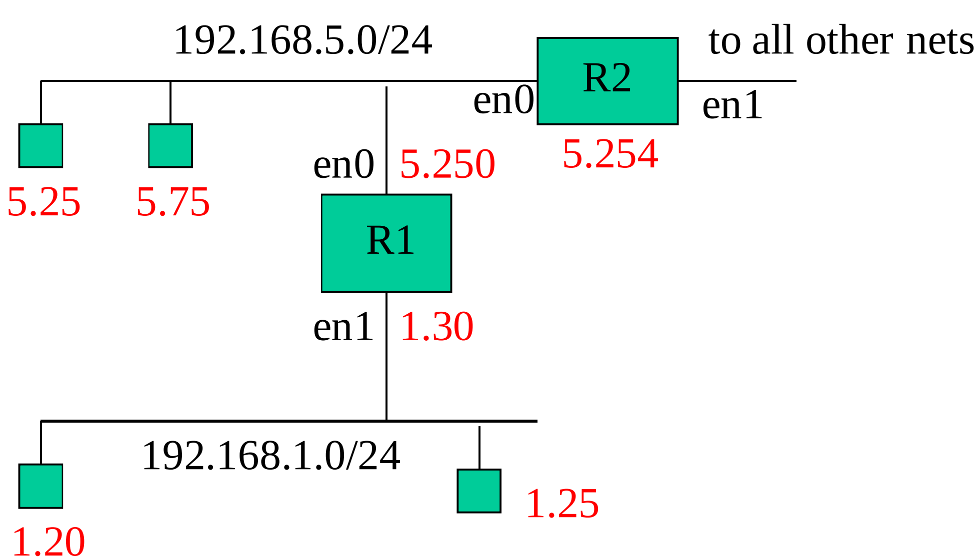
1. Route table is checked.
   192.168.1.25/24 matches the 192.168.1.0 entry
2. The next hop is the host itself (192.168.1.20). This means the destination is on the local network.
3. H1 then sends an ARP packet to find the data link address of the destination
4. Once the data link address is found, the packet is sent

Routing Scenario 1

Steps involved in sending a packet from H1 to an address that is on another network:

1. Route table is checked. The destination address matches the default entry in the table.
2. The next hop is 192.168.1.30. This means the destination is on the other side of a router.
3. H1 sends an ARP packet to determine the data link address of the gateway.
4. The packet is sent to the router
5. The router's route table is checked and the packet is sent to the next hop
6. This continues until the packet reaches the final destination

Routing Scenario 2



Routing Scenario 2

Packet from H3 to H4 (same network)

IP Address		Hardware Address	
SRC	DEST	SRC	DEST
H3	H4	H3	H4

Packet from H3 to H1 (Next door network)

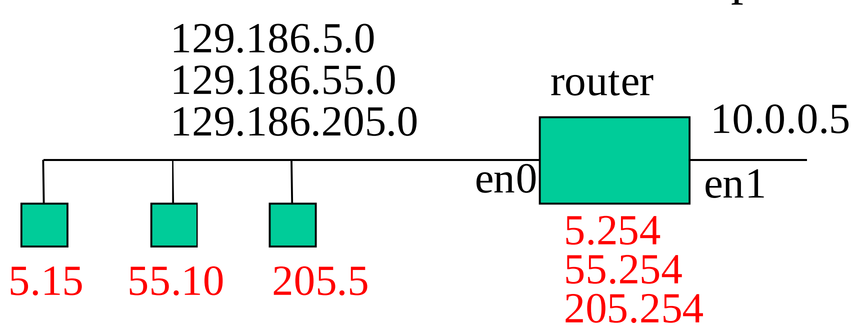
IP Address		Hardware Address	
SRC	DEST	SRC	DEST
H3	H1	H3	R1 (EN1)
H3	H1	R1 (EN0)	H1

Packet from H3 to H5 (default network)

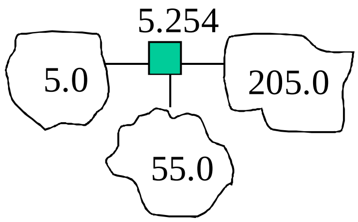
IP Address		Hardware Address	
SRC	DEST	SRC	DEST
H3	H5	H3	R2 (EN0)

Routing Example 3

Sometimes a network can have multiple IP's:



Logically, the network is viewed like this for host 5.15:



Destination	**Next**
129.186.5.0	129.186.5.15
Default	129.186.5.254

IP Packet Format

<table>
<tr><td>VER=4</td><td>IHL</td><td>TYPE</td><td colspan="2">TOTAL LENGTH (bytes)</td></tr>
<tr><td colspan="3">ID</td><td>FLAG</td><td>OFFSET</td></tr>
<tr><td colspan="2">TTL</td><td>PROTOCOL</td><td colspan="2">CHECKSUM</td></tr>
<tr><td colspan="5">SOURCE IP</td></tr>
<tr><td colspan="5">DESTINATION IP</td></tr>
<tr><td colspan="5">OPTION</td></tr>
<tr><td colspan="5">DATA ….</td></tr>
</table>

IP Packet Format

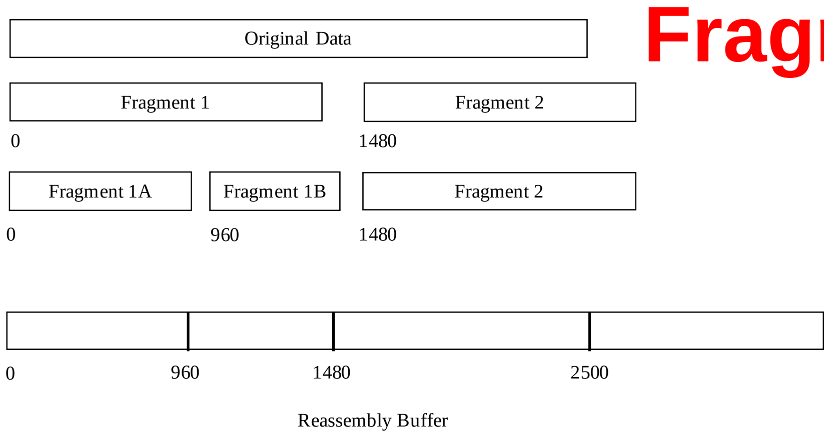
- IHL: header length in words
- Type of service: almost always 0
- Total length (bytes) includes header length.
  Max packet size = 2^{11} bytes
- ID: used in fragmentation
- Flag: 0: not used
  D=1: don't fragment
  M=:1 more data. M=0: last packet of fragment
- Offset: #8 bytes
- TTL (time to live): starts at 255 then decrements after each hop
- Checksum: worthless because it must be recalculated after every router due to the TTL decrement

IP Protocol Field

1	Internet Control Message Protocol (ICMP)
3	Gateway-to-Gateway protocol
5	Stream
6	Transport Control Protocol (TCP)
8	Exterior Gateway Protocol
9	Any private interior gateway protocol
11	Network voice protocol
17	User datagram protocol (UDP)
20	Host Monitoring Protocol
22	Xerox Network System Internet Datagram Protocol
27	Reliable Datagram Protocol
28	Internet Reliable Transaction Protocol
30	Bulk Data Transfer Protocol
61	Any Host Internet Protocol

Fields	Original Packet	Fragment 1	Fragment 2	Fragment 1a	Fragment 1b
Ver/HLEN	4/5	4/5	4/5	4/5	4/5
Type	0	0	0	0	0
Length	2540	1500	1060	1000	560
ID	2356	2356	2356	2356	2356
Flags	0	0 0 1	0 0 0	0 0 1	0 0 1
Offset	0	0	185	0	120
TTL	150	computed	computed	computed	computed
Protocol	TCP	TCP	TCP	TCP	TCP
Checksum	computed	computed	computed	computed	computed
Source IP	IP1	IP1	IP1	IP1	IP1
Dest IP	IP2	IP2	IP2	IP2	IP2
Data Len	2500	1480	1020	960	520

Fragmentation



Machine Address Resolution

- We now have the IP address for the destination, but we need to find the datalink address of the destination.
- There is no assigned relationship between the datalink address and the IP address.
- We need a protocol to query the network to find the data link address of a host with a given IP address.
- This protocol is called Address Resolution Protocol (ARP). The ARP protocol uses the datalink broadcast address to query all hosts on the network. The host whose IP address matches the requested address will respond with a packet that contains its data link address.

ARP Packet Format

<table>
<tr><td colspan="2">HW type</td><td colspan="2">Protocol type</td></tr>
<tr><td>HLEN</td><td>PLEN</td><td colspan="2">Operation</td></tr>
<tr><td colspan="4">Sender HA (bytes 0-3)</td></tr>
<tr><td colspan="2">Sender HA (4-5)</td><td colspan="2">Sender IP (bytes 0-1)</td></tr>
<tr><td colspan="2">Sender IP (bytes 2-3)</td><td colspan="2">Target HA (bytes 0-1)</td></tr>
<tr><td colspan="4">Target HA (bytes 2-5)</td></tr>
<tr><td colspan="4">Target IP (bytes 0-3)</td></tr>
</table>

ARP Packet Format

- Hardware type 1 = Ethernet
- Protocol Type 0x800 = IP
- HLEN = 6
- PLEN = 4
- Operation
  - 1 = ARP Request
  - 2 = ARP Response
  - 3 = RARP Request
  - 4 = RARP Reply

ARP Protocol

- A station that needs to find a datalink address will create an ARP packet and will fill in the sender IP and HA fields with its IP address and Hardware address. It will place the IP address of the target machine in the target IP field. The station will also fill in the first 5 fields. The ARP packet is then used as the data field in an Ethernet packet. This Ethernet packet has the broadcast address in the destination field.

ARP

- The packet is then sent out on the network. Since it is a broadcast packet all stations will receive the packet. The station whose IP address matches the target IP address will create a new ARP packet to send back to the sender. The target machine will put his address into the sender fields and will put the requestors address into the target fields. The ARP packet will then be sent as data in an Ethernet packet whose destination address is the requesting station.

ARP

- The help cut down on the traffic stations on the network can use an internal ARP table to cache ARP responses and also to cache information from ARP requests. For example when a station receives an ARP request, even if the target IP address does not match the station can store the IP address and Ethernet address found in the sender fields.

ARP

- The entries in the table have a short life. This enables changes in the mapping between IP address and Hardware address without clearing the table.
- The RARP protocol is used by diskless workstations to find their IP address from a server. They only know their own Ethernet address.

ICMP

Internet Control Message Protocol

- Designed as error control
- Provides a means for transferring messages between hosts
- Examples for use:
  - When a datagram cannot reach its destination
  - When a gateway can direct the host to send traffic on a shorter route
  - Ping

ICMP Packet Format

VER=4	IHL	TYPE	TOTAL LENGTH (bytes)		
ID			FLAG	OFFSET	
TTL		PROTOCOL	CHECKSUM		
SOURCE IP					
DESTINATION IP					
Type		Code	Checksum		
Parameter					
Information					

ICMP Packet Format

- ICMP packets are carried within the data of an IP packet
- Fields:
  - Type (8 bits): message type
  - Code (8 bits): message sub-type
  - Checksum (16 bits)
  - Parameter (32 bits)
  - Information (variable)

ICMP Message Types

0	Echo Reply
3	Destination Unreachable
4	Source Quench
5	Redirect
8	Echo
12	Parameter Problem
13	Timestamp
14	Timestamp Reply
15	Information Request
16	Information Reply
17	Address Mask Request
18	Address Mask Reply

ICMP Echo (Ping)

- Type = 8 (echo)
  Type = 0 (reply)
- Code = 0
- Parameter
  - ID number (2 bytes)
  - Sequence number (2 bytes)
- Optional Data

Note: the optional data field of ping has been used in the past for tunneling information through a firewall

ICMP Destination Unreachable

- Type = 3
- Code:
  - 0 Network Unreachable
  - 1 Host Unreachable
  - 2 Protocol Unreachable
  - 3 Port Unreachable
  - 4 Fragmentation needed and DF set
  - 5 Source Route Failed
- Parameter = 0
- Data = IP header + first 8 bytes of datagram

ICMP Source Quench

- Type = 4
- Code = 0
- Parameter = 0
- Data = IP header + first 8 bytes of datagram
- Sent when a packet arrives too quickly for a host to process. The packet is discarded.
- A host receiving a source quench message will slow down its rate of transmission until it no longer receives source quench messages. Then it will slowly increase its rate as long as no more source quench messages are received.

ICMP Redirect

- Type = 5
  Code:
  - 0 Redirect for the NET
  - 1 Redirect for the Host
  - 2 Redirect for type of service and net
  - 3 Redirect for type of service and host

  Parameter = gateway IP address
  Data = IP header + first 8 bytes of datagram
- Sent when a gateway detects a host using a non-optimum route
- Original packet is not dropped
- If the host does not update its route table and continues using the non-optimum route, an ICMP redirect storm can occur

ICMP Time Exceeded

- Type = 11
- Code:
  - 0 TTL (time to live) count exceeded
  - 1 Fragment reassembly time exceeded
- Parameter = 0
- Data = IP header + first 8 bytes of datagram

ICMP Parameter Problem

- Type = 12
- Code = 0
- Parameter (8 bits) = pointer to error
- Data = IP header + first 8 bytes of datagram
- Sent when a gateway or host finds a problem with the IP header.
- The pointer identifies the octed in the header that caused the problem

ICMP Timestamp

- Type = 13 (echo)
  Type = 14 (reply)
- Code = 0
- Parameter:
  - ID number (2 bytes)
  - Sequence number (2 bytes)
- Originate timestamp
- Receive timestamp (reply only)
- Transmit timestamp (reply only)