The Address Resolution Protocol (ARP)

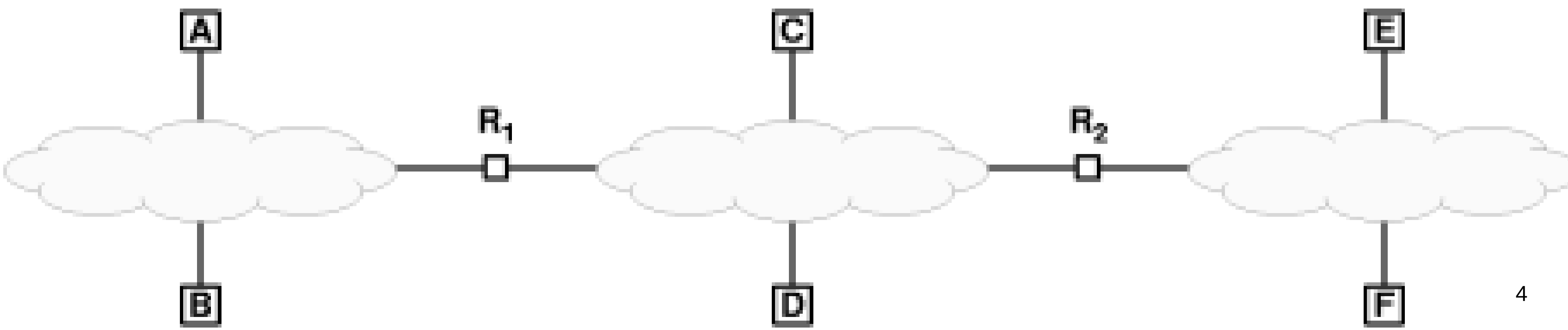
Binding Protocol Addresses (ARP)

- A frame transmitted across a physical network must contain the hardware address of the destination.
- Before protocol software can send a packet across a physical network, the software must translate the IP address of the destination computer into an equivalent hardware address
- Protocol addresses are abstractions provided by software; physical network hardware does not know how to locate a computer from its protocol address.
- The protocol address of the next hop must be translated to an equivalent hardware address before a packet can be sent

Address Resolution

- Translation (mapping) of a computer's protocol address (eg. IP) to an equivalent hardware address (eg. Ethernet address)
  - protocol address is said to be resolved (mapped or translated) to the correct hardware address
- Address resolution is local to a network.
  - One computer can resolve the address of another computer only if both computers attach to the same physical network
  - a computer never resolves the address of a computer on a remote network

- In the figure, hosts A and B attach to the same physical network. If an application on host A sends data to an application on host B, the application uses B’s IP address as the destination. Protocol software on A resolves B’s IP address to B’s hardware address, and uses the hardware address to send the frame directly.
- If A sends message to F?



Forwarding Packets to Remote Networks

- If the destination computer is on a different network, the source computer resolves the IP address of the next-hop router to its hardware address and sends the packet to the router
- The router determines whether to forward the packet to another router or whether the destination is attached directly to one of its network.

Address Resolution Techniques

- Table lookup
  - bindings are stored in a table in memory, which the software searches when it needs to resolve an address.
  - Each entry in the table contains a pair (P,H), where P is a protocol address and H is the equivalent hardware address.
  - An example binding table:

IP Address	Hardware Address
197.15.3.2	0A:07:4B:12:82:36
197.15.3.3	0A:9C:28:71:32:8D
197.15.3.4	0A:11:C3:68:01:99
197.15.3.5	0A:74:59:32:CC:1F
197.15.3.6	0A:04:BC:00:03:28
197.15.3.7	0A:77:81:0E:52:FA

Address Resolution Techniques
Table lookup

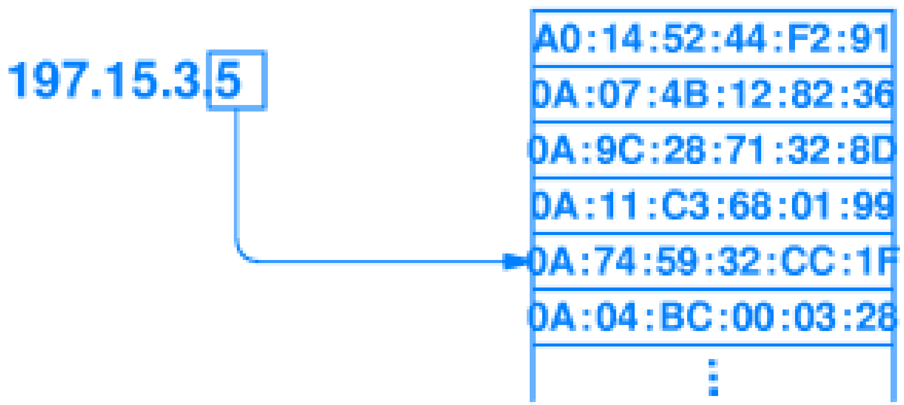
- The chief advantage of table lookup approach is generality, a table can store the address bindings for an arbitrary set of computers on a given network. The table lookup algorithm for address resolution is straightforward and among the easiest to program.

- For small networks sequential search is sufficient.
- Two other standard implementations are used:
  - Hashing is well-known by most programmers.
  - Direct Indexing is slightly more efficient, but less general technique. It can be used in cases where protocol address are assigned from a compact range (in sequential address).

Address Resolution Techniques

Table lookup

- To use direct indexing, the software maintains one-dimentional array of hardware addresses, and uses the host suffix from an IP addressas an index into the array.
- In the figure, the software extracts the host suffix 5, and uses it as an index into the array to obtain the hardware address of host.



Address Resolution Techniques

Closed-form Computation

- A resolver that uses a closed-form method computes a mathematical function, using basic Boolean and arithmetic operations, that maps an IP address to a hardware address.
- Hardware and IP addresses can be changed, so this can be efficient for a network.

Address Resolution Techniques
Message Exchange

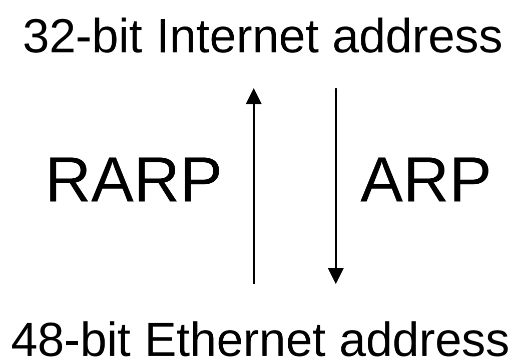
- Address resolution server(s)
- Computers exchange messages across a network to resolve an address (eg. ARP). When a computer broadcasts a request for address resolution, another computer whose protocol address matches that of the request sends a reply that contains the requested information (physical address).

Address Resolution Protocol (ARP)

- TCP/IP can use 3 address resolution methods; the method chosen for a particular network depends on the addressing scheme used by underlying hardware.
- Table lookup is usually employed to resolve IP address across a WAN, closed-form computation is used with configurable networks, message exchange is used on LAN hardware that has static addressing.
- To guarantee that all computers agree on the exact format and meaning of messages used to resolve addresses, the TCP/IP protocol suite includes ARP.
- The ARP used to resolve IP address to hardware address.

Address Resolution Protocol (ARP)

- Address resolution provides a mapping between the two different forms of address.
  - 32-bit Internet address
  - 48-bit Ethernet address



ARP and RARP

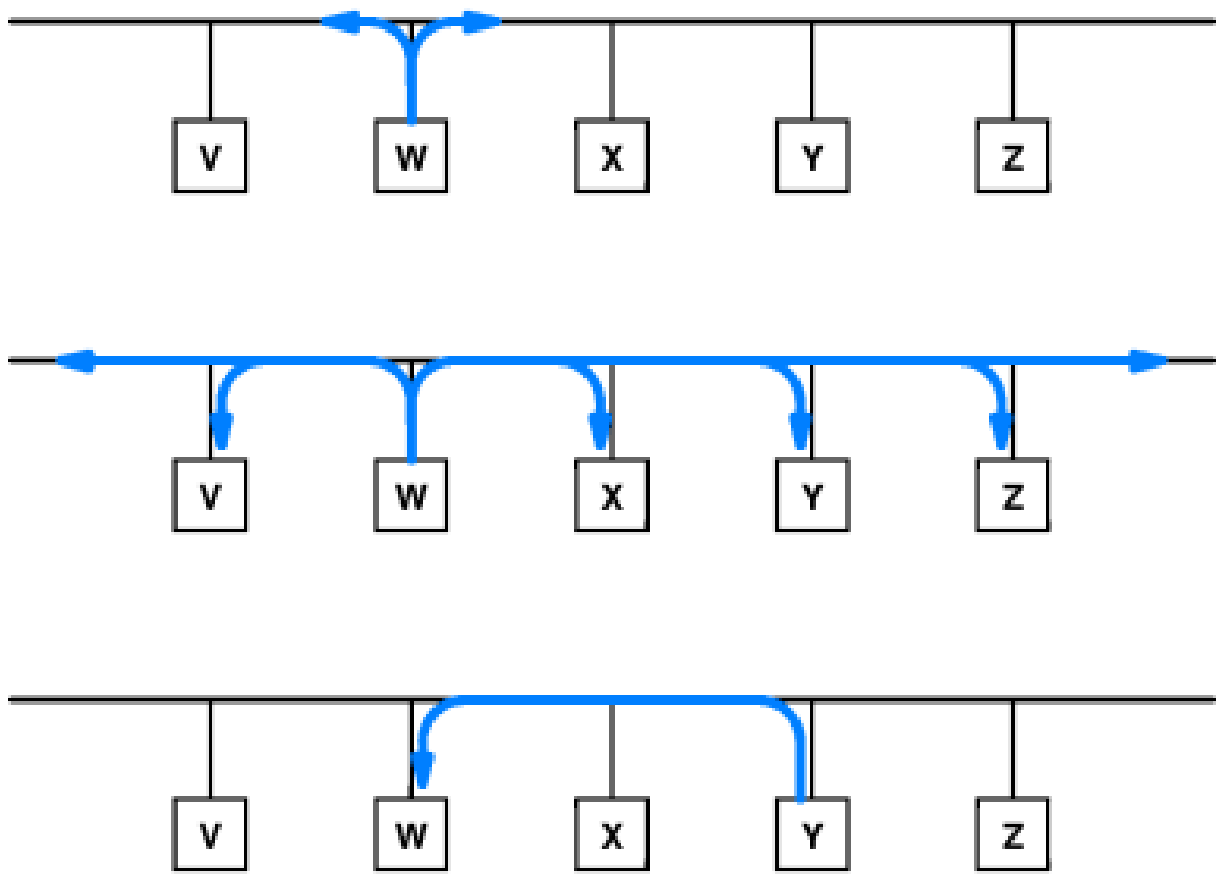
- ARP
  - ARP provides a dynamic mapping from an IP address to the corresponding hardware address.
  - We use the term dynamic since it happens automatically and is normally not a concern of either the application user or the system administrator.
- RARP (Reverse Address Resolution Protocol)
  - RARP is used by systems without a disk drive but requires manual configuration by the system administrator.

Address Resolution Protocol (ARP)

- Has two basic message types:
  - ARP request message
    - broadcasted to all computers on the local network
    - contains an IP address and request the corresponding hardware address
    - each computer receives this request and examines the IP address.
  - ARP reply message
    - The computer mentioned in the ARP request sends a reply containing both the IP address sent in the request and the hardware address
    - All other computers process and discard the request with no response

Address Resolution Protocol (ARP)

Message Delivery

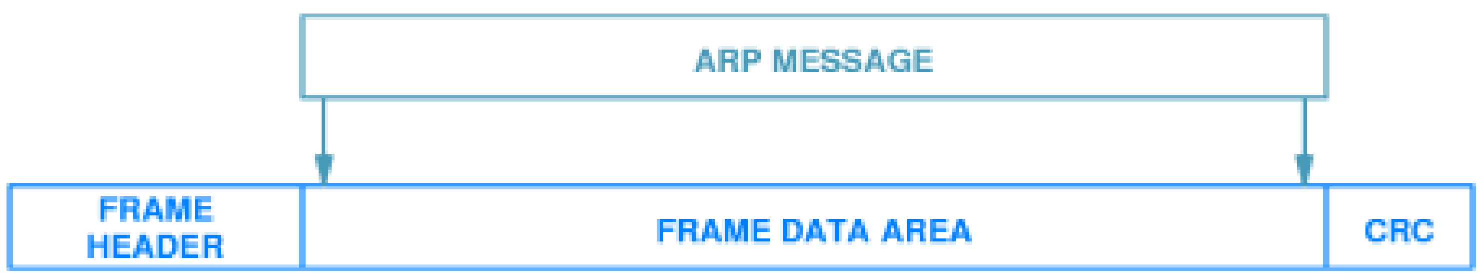


ARP Message Format

<table>
<tr><td>0</td><td>8</td><td>16</td><td>31</td></tr>
<tr><td colspan="2">Hardware type = 1</td><td colspan="2">ProtocolType = 0x0800</td></tr>
<tr><td>HLEN = 48</td><td>PLEN = 32</td><td colspan="2">Operation</td></tr>
<tr><td colspan="4">SourceHardwareAddr (bytes 0 – 3)</td></tr>
<tr><td colspan="2">SourceHardwareAddr (bytes 4 – 5)</td><td colspan="2">SourceProtocolAddr (bytes 0 – 1)</td></tr>
<tr><td colspan="2">SourceProtocolAddr (bytes 2 – 3)</td><td colspan="2">TargetHardwareAddr (bytes 0 – 1)</td></tr>
<tr><td colspan="4">TargetHardwareAddr (bytes 2 – 5)</td></tr>
<tr><td colspan="4">TargetProtocolAddr (bytes 0 – 3)</td></tr>
</table>

Sending an ARP Message

- The ARP message is treated as data being transported, the network hardware does not know about the ARP message format and does not examine the contents of individual fields.
- Placing a message inside a frame for transport is called **encapsulation**; ARP is encapsulated directly in a hardware frame.



IP Datagrams and Datagram Forwarding

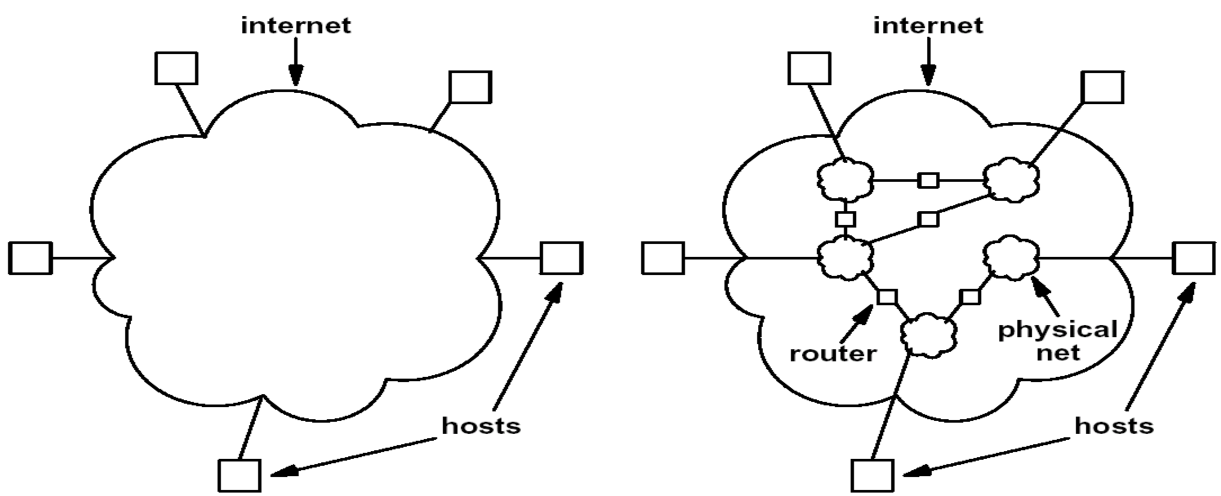
Routing

- ***Routing***: The process of choosing a path over which to send packets.
- ***Router***: A machine making this choice.

- Routing occurs at several levels:
  - From node to node in a simple LAN
  - From LAN to LAN in a WAN

Internet, Router, Host

- ***Internet*** is composed of multiple physical networks interconnected by computers called *routers*.
- *Routers* have direct connections to two or more networks.
- A ***Host*** usually connects directly to one physical network.



Universal, Virtual Packets

- A router cannot transmit a copy of a frame that arrives on one network across another, if it can connect heterogeneous networks, in which frame formats are different.
- To accommodate heterogeneity, an internet must define a hardware-independent packet format, **universal, virtual packet**.

IP Datagram

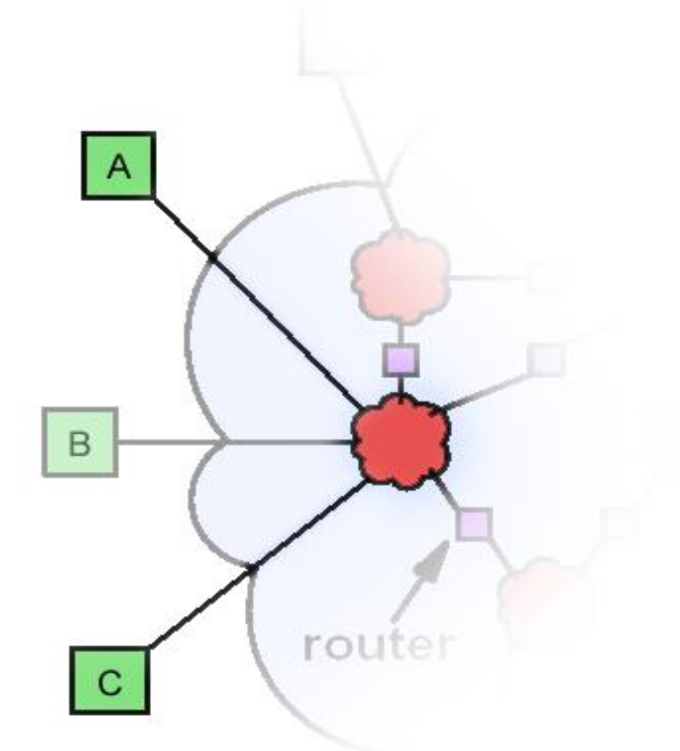
- IP datagram = IP packet
- Payload (data) is not a fixed size
  - One octet to 64K octets
- Header
  - Source IP address
  - Destination IP address
  - Payload size
  - CRC
  - And some other stuff…

Direct / Indirect Delivery

- Routing can be divided into two forms:
  - *Direct Delivery*
    - When two machines are both attached to the same underlying physical transmission system (i.e. a single Ethernet)
  - *Indirect Delivery*
    - When two machines are not directly attached to the same network and packets must go through at least one router for delivery.

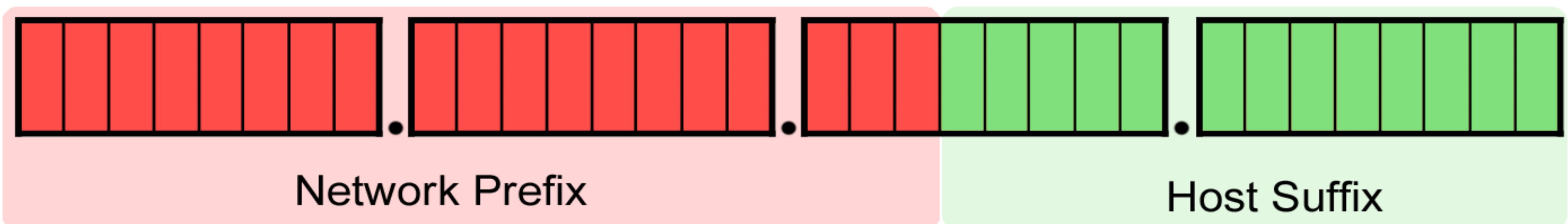
Direct Delivery

- Delivery from **A** to **C**:
  - **A** encapsulates the datagram in a physical frame
  - Maps the destination IP address to a physical address (MAC address)
  - Uses the network hardware to deliver it
- How does **A** know whether **C** is in the same network?



Network Prefix

- IP addresses are divided into a Network Prefix and a Host Suffix
- By checking the network prefix of the destination IP address, sender will know if it is directly connected to the destination machine or not.



Indirect Delivery

- **B** wants to deliver a datagram to **D**
  - **B** checks the network prefix and realizes that D is outside of **L1.**
  - In an internet, every host can reach a router directly.
  - **B** sends the packet to **R1** *directly* and lets **R1** handle the delivery.

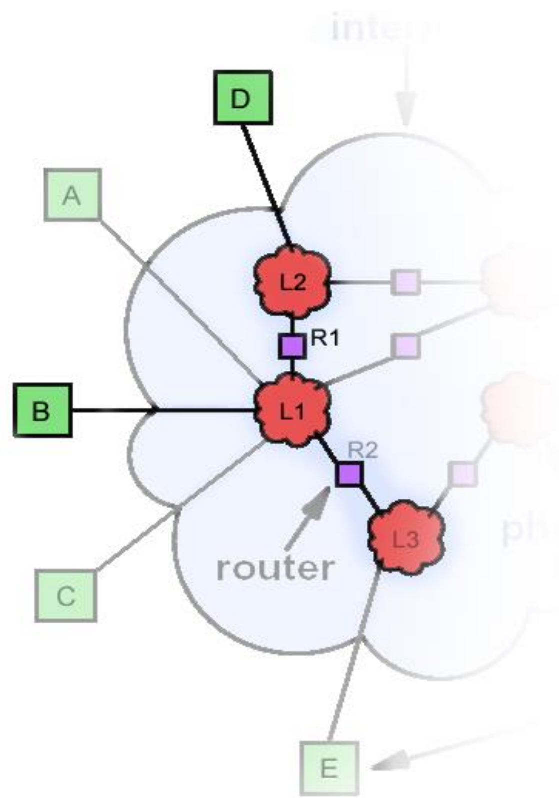


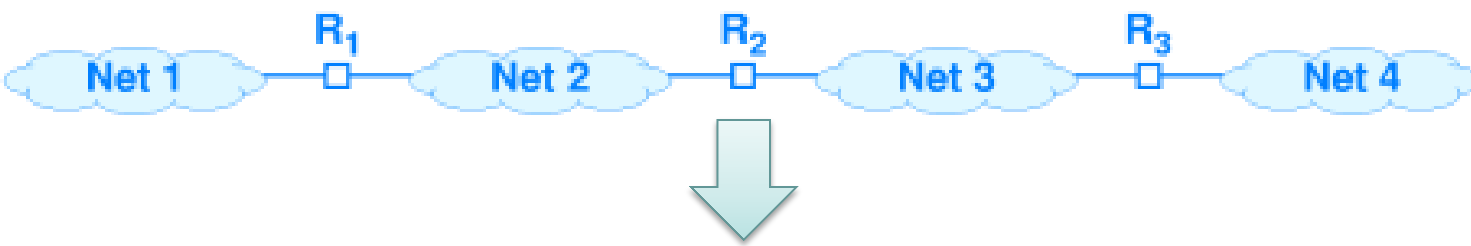
Table-Driven Routing

- How does **B** decide to send the datagram to **R1** and not to **R2**?
- How does **R1** know where to send the datagram?

- The usual IP routing algorithm employs an *Internet Routing Table* or *IP Routing Table*.
- Both hosts and routers have IP routing tables.

- IP routing tables, based on the destination address, tell the router where to send a datagram.

Table-Driven Routing

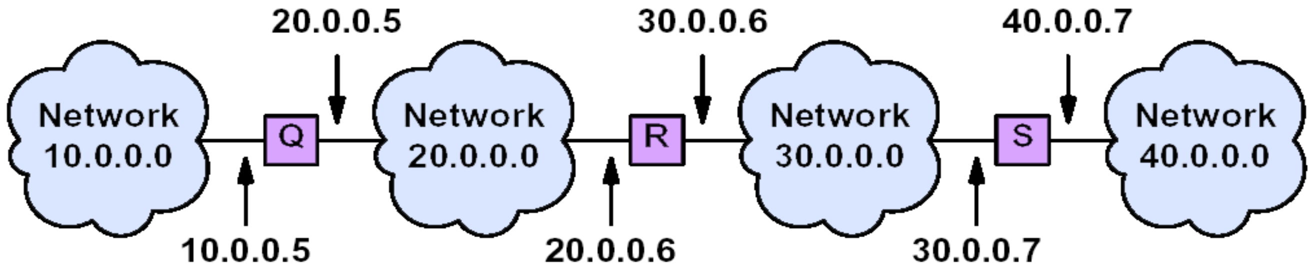


Destination	Next Hop
net 1	R_1
net 2	deliver direct
net 3	deliver direct
net 4	R_3

Next-Hop

- Do we need to keep the whole path to a destination address?
- Every router only needs to know what is the next router in the path.
- This next router is called the ***next hop***.

Next-Hop Routing

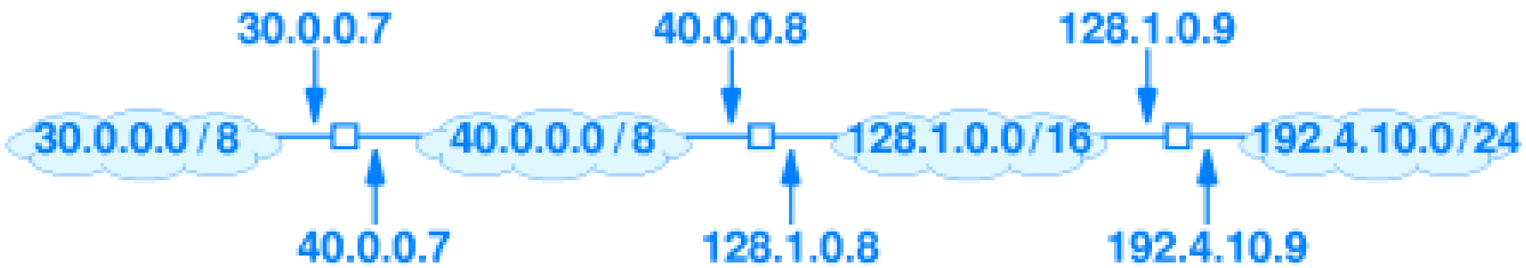


Destination Network	Next Hop
20.0.0.0	DELIVER DIRECTLY
30.0.0.0	DELIVER DIRECTLY
10.0.0.0	20.0.0.5
40.0.0.0	30.0.0.7

Routing Table for router **R**

- Each router in a routing table can be reached via a direct connection.

IP Addresses and Routing Table Entries



(a)

Destination	Mask	Next Hop
30.0.0.0	255.0.0.0	40.0.0.7
40.0.0.0	255.0.0.0	deliver direct
128.1.0.0	255.255.0.0	deliver direct
192.4.10.0	255.255.255.0	128.1.0.9

(b)

The Mask Field and Datagram Forwarding

- Routing/Forwarding: The process of using a routing table to select a next hop for a given datagram.
- Mask field: Used to extract the network part of an address during lookup.
- If a datagram contains IP address D,

  if ((Mask[i] & D) == Destination[i]) forward to NextHop[i];

Consider a datagram destined for address 192.4.10.3; the entries in routing table are tried:

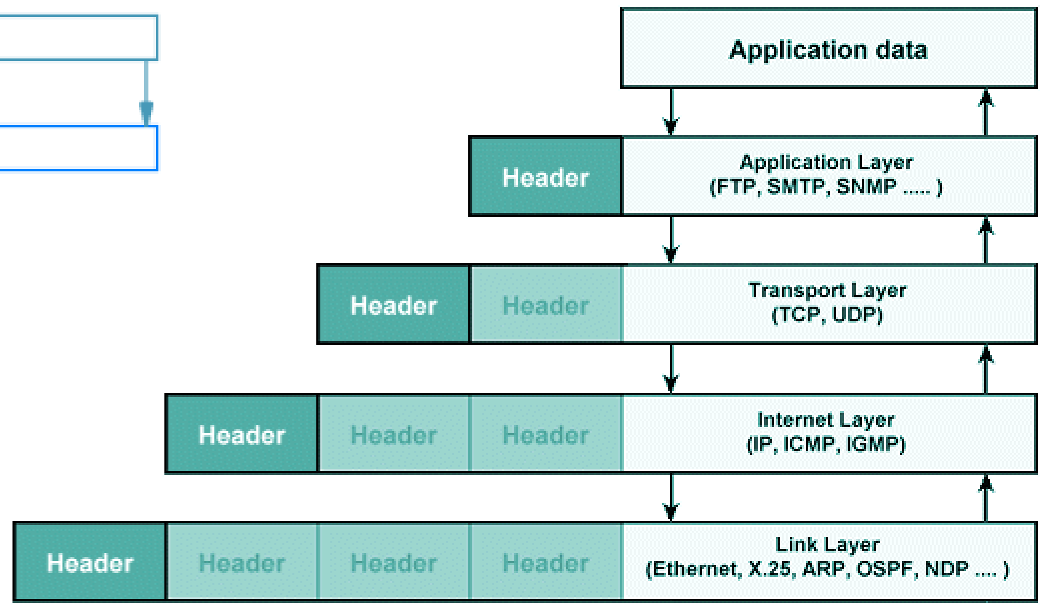
255.255.255.0 & 192.4.10.3 == 192.4.10.0

Best-Effort Delivery

- In addition to defining the format of internet datagrams, the IP defines the semantics of communication, and uses the term **best-effort** to describe the service it offers.
- **Best effort delivery** describes a network service in which the network does not provide any guarantees that data is delivered or that a user is given a guaranteed quality of service level or a certain priority.
- The standard specifies that although IP makes a best-effort attempt to deliver each datagram, IP does not guarantee that it will handle the problems of:
  - Datagram duplication,
  - Delayed or out-of-order delivery,
  - Corruption of data,
  - Datagram loss.
- Higher layers of protocol software are required to handle each of these errors.

Encapsulation

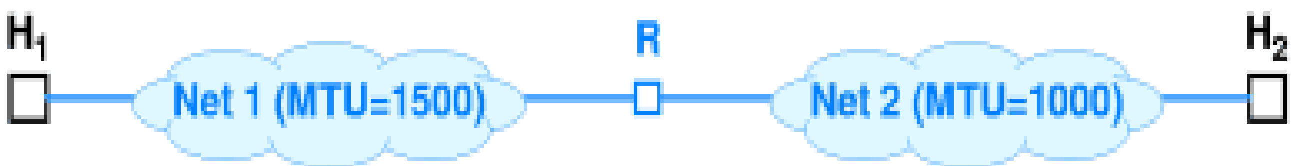
- How can a datagram be transmitted across a network that does not understand the datagram format? *Encapsulation*
- When an IP datagram is encapsulated in a frame, the entire datagram is placed in the data area of a frame.



Encapsulation of data in the TCP/IP protocol stack

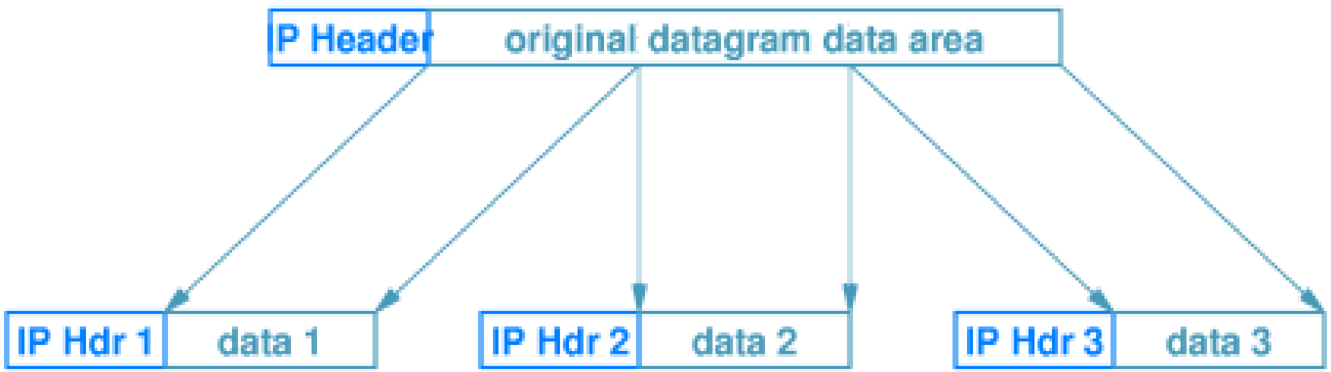
MTU, Datagram Size, and Encapsulation

- MTU is the **Maximum Transmission Unit** – the maximum amount of data that a frame can carry.
- In an Internet that connects heterogeneous networks, MTU restrictions can cause a problem.



- An IP router uses a technique known as *fragmentation* to solve the problem of heterogeneous MTUs.
- When a datagram is larger than the MTU, the router divides the datagram into smaller pieces called fragments.
- Each fragment is sent separately.

MTU, Datagram Size, and Encapsulation



An IP datagram divided into three fragments. Each fragment carries some data from the original datagram, and has an IP header similar to the original datagram.

Reassembly

- The process of creating a copy of the original datagram from fragments is called ***reassembly***.
- All fragments have the same destination address as the original datagram.
- The fragment that carries the final piece of data has an additional bit set in the header.
- A receiver performing reassembly can tell whether all fragments have arrived successfully.

Identifying A Datagram

- Since IP does not guarantee delivery, some fragments can be lost or arrive out of order.
- How does IP reassemble fragments that arrive out of order?

  IDENTIFICATION field: a unique ID number of each outgoing datagram.
- When a router fragments the datagram, the router copies the ID number into each fragment.

  The FRAGMENT OFFSET field tells a receiver how to order fragments within a given datagram

Fragment Loss

- Recall that <u>IP does not guarantee datagram delivery</u>
- Some fragments may be delayed or lost
- Datagrams with lost fragments cannot be reassembled
- Fragments may be saved temporarily.
- IP specifies a maximum time to hold fragments.
- After a timer expires, saved fragments are discarded.

Summary

- An IP datagram is encapsulated in a network frame for transmission across a hardware network.
- To encapsulate a datagram, the sender places the entire datagram in the data area of a network frame.
- Each network technology defines **the maximum amount of data (MTU)** accepted.

Summary

- When a router receives a datagram that is larger than the network MTU, the router divides the datagram into fragments.
- Each fragment travels to the ultimate destination, which is responsible for reassembling fragments into the original datagram.