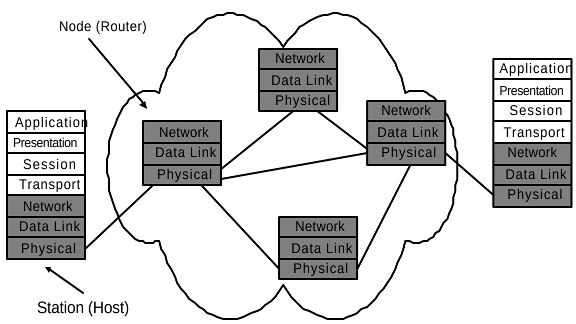
Network Layer

Introduction
Datagrams and Virtual Circuits
Routing
Traffic Control

Main Objective

- Data delivery from source to destination



Issues at the Network Layer

- Addressing
  - IP addresses on the Internet
- Switching
  - Datagram packet switching
  - Virtual circuit packet switching
- Routing
  - How to calculate a path from source to destination?

Models of the Network Service

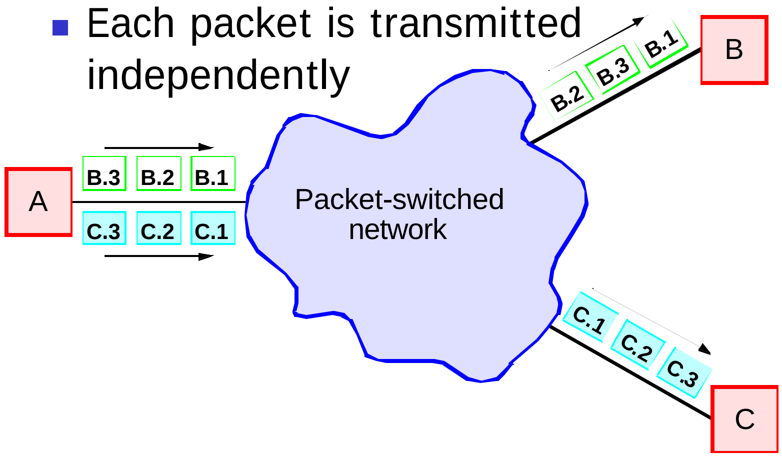
- The “post office” model (IP)
  - Simple, unreliable, unordered delivery service
  - Different letters between the same parties are handled independently (connectionless model)
  - Stateless (no record of who’s corresponding with whom)
  - Intelligent end-user
- The “phone service” model (ATM)
  - Concept of “connections” between conversing users
  - Reliable delivery (of voice)
  - State is maintained regarding active connections
  - Dumb end-device (phone)

Connectionless vs. Connection-Oriented Service

- Network Layer Solutions
  - Connection-Oriented Service (ATM)
  - Connectionless Service (IP)
- Transport Layer Solutions (assume a connectionless network)
  - Connection-Oriented Service (TCP)
  - Connectionless Service (UDP)

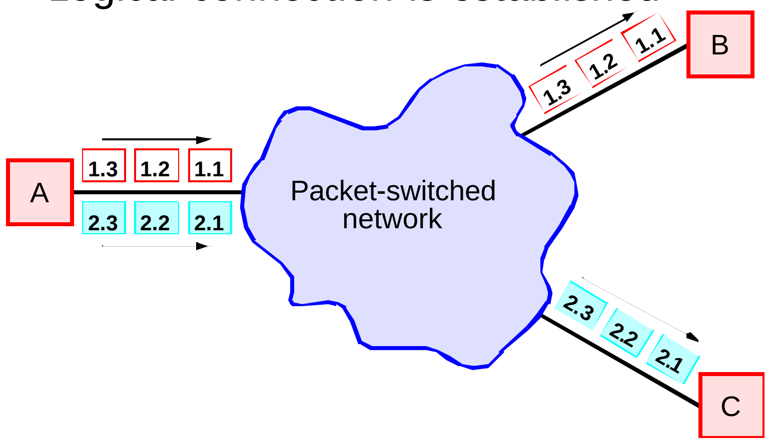
Connectionless Service

- Each packet is transmitted independently



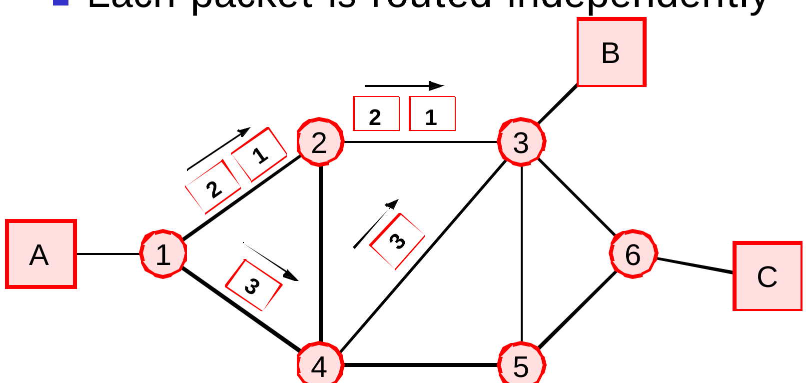
Connection-oriented Service

- Logical connection is established



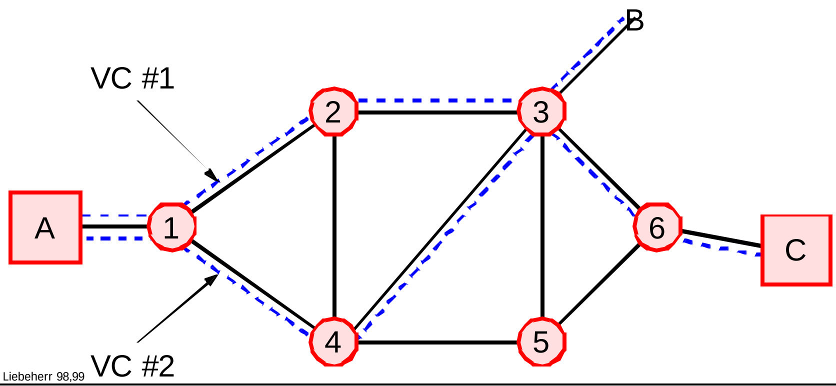
Datagram Packet-Switching

- Unreliable, connectionless service
- Each packet is routed independently



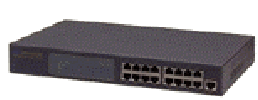
Virtual-Circuit Packet Switching

- Connection-oriented service
- All packets of a VC follow the same route



Network Switches

- A network switch (or router) is a device that forwards data in the direction of the destination



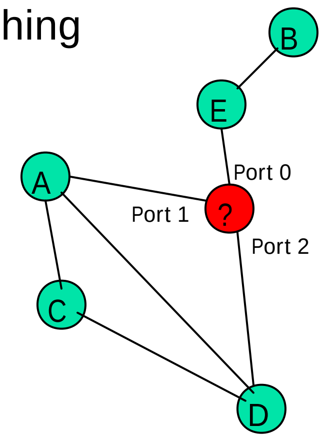
Ethernet Switch
(Link layer device)

Cisco Router
(Network layer device)

Forwarding Tables

- Datagram packet switching

Destination	Next hop (port)
A	
B	
C	
D	
E	



Packet Forwarding of Datagrams

- When a packet with destination node arrives at an incoming link, ...
  1. The router looks up the routing table
  2. The routing table lookup yields the address of the next node (next hop)
  3. The packet is transmitted onto the outgoing link that goes to the next hop

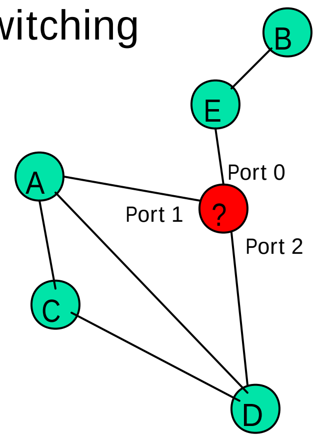
Good: The router does not need to know about flows

Bad: Size of the routing table can grow very large

Forwarding Tables

- Virtual circuit packet switching

In Port	In VCI	Out Port	Out VCI



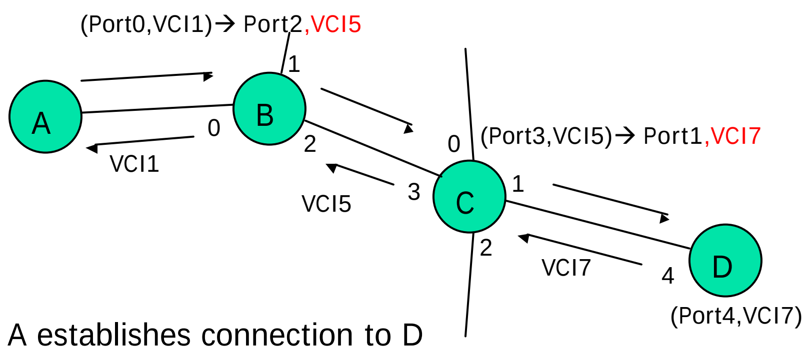
Packet Forwarding of Virtual Circuits

- When a packet with VC_{in} in header arrives from router n_{in}, ...
  1. The router looks up the routing table for an entry with (VC_{in}, n_{in})
  2. The routing table lookup yields (VC_{out}, n_{out})
  3. The router updates the VC# of the header to VC_{out} and transmits the packet to n_{out}

Good: Routing table is small (how small?)

Bad: Changing the route is complicated.
Routing table changes for each virtual circuit

VCI Establishment in Virtual Circuit Packet Switching



A establishes connection to D

Source Routing

- Source determines the entire route of the packet
- Packet header carries complete route information
- Switches follow directions in packet header
- Problems?

Comparison

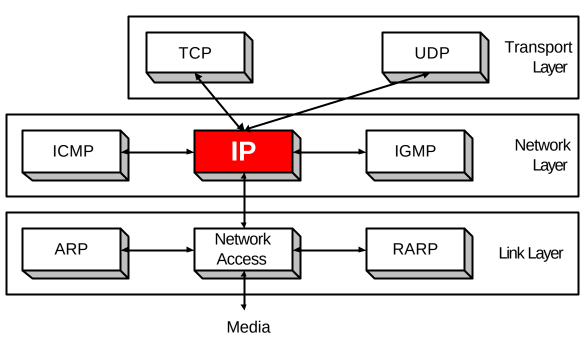
IP Model (connectionless, unreliable)	ATM Model (connection-oriented, reliable)

■ No connection establishment
  ■ favors small transactions
	■ Signalling delay
	  ■ favors large data transfers

■ Complex transport layer	■ Complex network layer
■ Stateless network core	■ Per-connection state
■ Scalable	■ Scalability is a tough issue
■ Robust	■ Vulnerable to router failure
■ No reservation mechanism	■ Easy reservation
■ No QoS guarantees	■ QoS

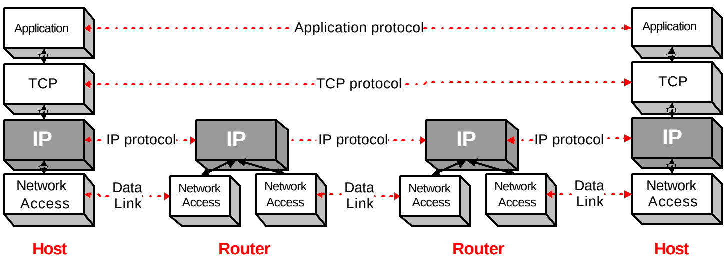
IP Protocol Stack

- IP (Internet Protocol) is a Network Layer Protocol



IP Overview

- IP is the highest layer protocol that is implemented at both routers and hosts
- Offers unreliable connectionless service (send and deliver primitives)



IP Addresses

- Each router or host on the Internet has a unique global address, called the IP address
- An IP address
  - is 32 bits long.
  - encodes a network number and a host number
- IP addresses are written in a dotted decimal notation:
  - **128.238.42.112** means

10000000	in 1st Byte
11101110	in 2nd Byte
00101010	in 3rd Byte
01110000	in 4th Byte

IP Datagrams

- IP breaks data up into Datagrams limited to 64K bytes each
- Datagrams prevent long flows from monopolizing the network for a long time
- In future gigabit networks the 64K limit can be increased
  - Example: For how long will a 1M byte datagram tie up a T1 line (1.5Mbps)?
  - How about a 1 Gbps optical fiber?
- Datagrams can further be fragmented depending on packet size of the data link layer (e.g., Ethernet)

IP Datagram Format

<table>
<tr><td>version (4 bits)</td><td>header length</td><td>Type of Service/TOS (8 bits)</td><td colspan="2">Total Length (in bytes) (16 bits)</td></tr>
<tr><td colspan="3">Identification (16 bits)</td><td>flags (3 bits)</td><td>Fragment Offset (13 bits)</td></tr>
<tr><td colspan="2">TTL Time-to-Live (8 bits)</td><td>Protocol (8 bits)</td><td colspan="2">Header Checksum (16 bits)</td></tr>
<tr><td colspan="5">Source IP address (32 bits)</td></tr>
<tr><td colspan="5">Destination IP address (32 bits)</td></tr>
<tr><td colspan="5">Options (if any, <40 bytes)</td></tr>
<tr><td colspan="5">DATA</td></tr>
</table>

>= five 32-bit words

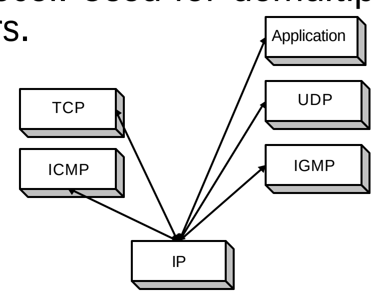
0 — 32-bit word — 31

IP Header

- **Version:**
  - Coexistence of multiple versions (smooth transition)
- **Identification, Fragment offset:**
  - 64K datagrams, fragmentation
- **ToS:**
  - Allows prioritized or differentiated services
- **TTL:**
  - Loop suppression

IP Header (Continued)

- **Protocol:** Specifies the higher-layer protocol. Used for demultiplexing to higher layers.



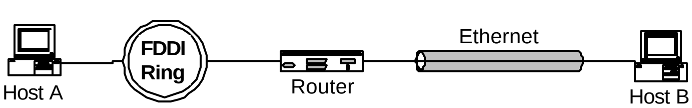
- **Header checksum:** verifies correctness of header.

IP Header (Continued)

- **Options:**
  - Security restrictions
  - Record Route: each router that processes the packet adds its IP address to the header.
  - Timestamp: each router that processes the packet adds its IP address and time to the header.
  - (loose) Source Routing: specifies a list of routers that must be traversed.
  - (strict) Source Routing: specifies a list of the only routers that can be traversed.
- **Padding:** ensures that header ends on a 4-byte boundary

IP Fragmentation

- Host A sends large IP datagram to host B
- Datagram traverses multiple networks with different MTUs
  - Problem?



MTUs: FDDI: 4352 Ethernet: 1500

- IP Router performs fragmentation

What's involved in Fragmentation?

- The following fields in the IP header are involved:

version (4 bits)	header length	Type of Service/TO	Total Length (in bytes)	
Identification			flags	Fragment Offset
TTL Time-to-Live (8 bits)		Protocol (8 bits)	Header Checksum (16 bits)	
......				

Identification is the same in all fragments.
Flags contains a "more fragments" bit

(There is also a "don't fragment bit" that can be set)

Fragment offset contains the offset of current fragment in the original datagram

Total length is changed by fragmentation