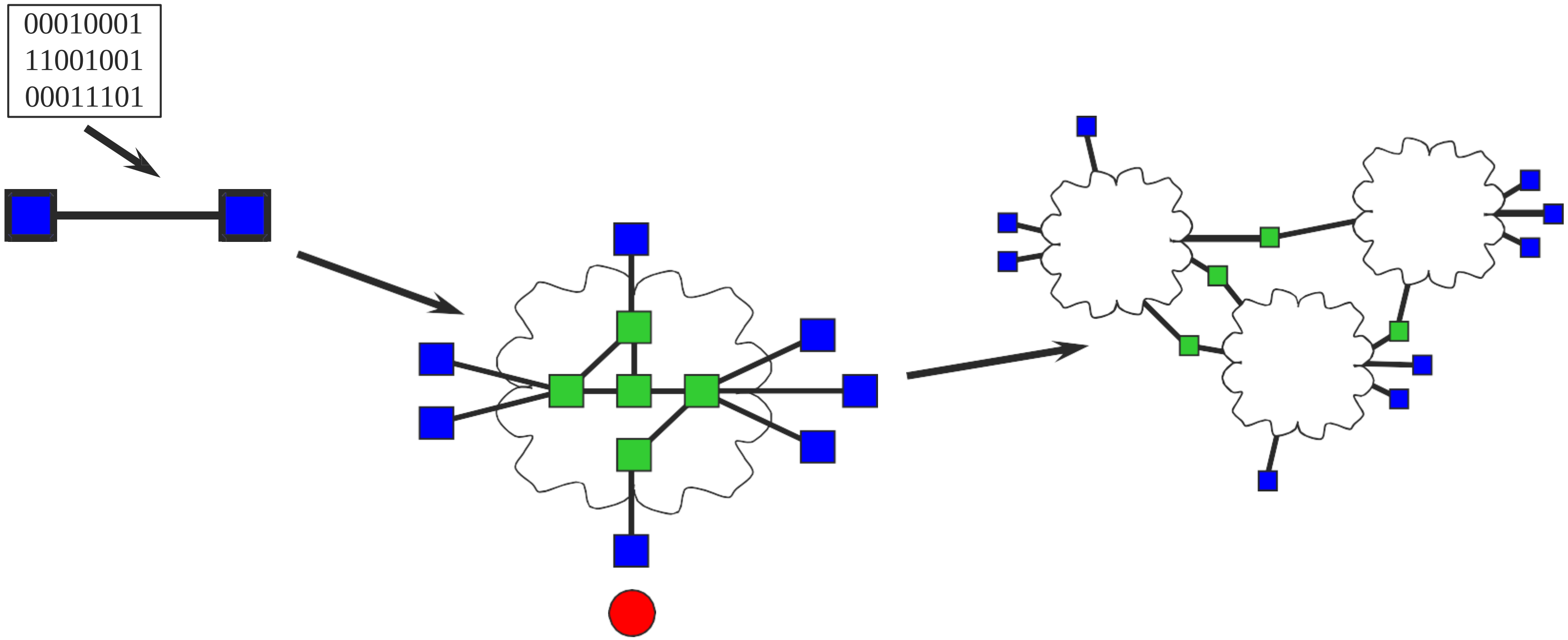
Internetworking
Chapter 3.3.1 – 3.3.7

The Big Picture



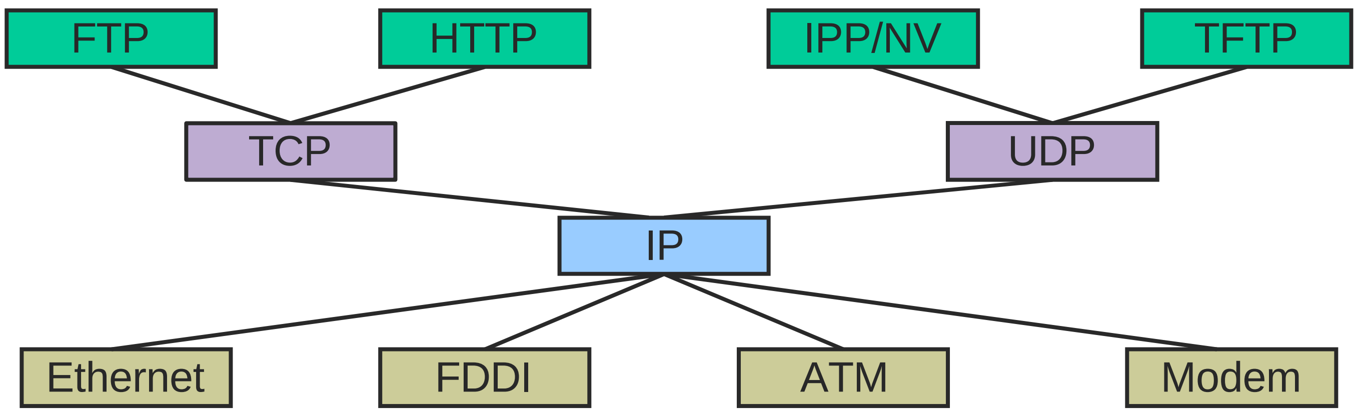
We are here

Internetworking

- Challenges
  - Heterogeneity of networks
  - Rapid growth of Internet (scalability issues)

Internet Protocol (IP)

- Network-level protocol for the Internet
- Operates on all hosts and routers
  - Routers are nodes connecting distinct networks to the Internet

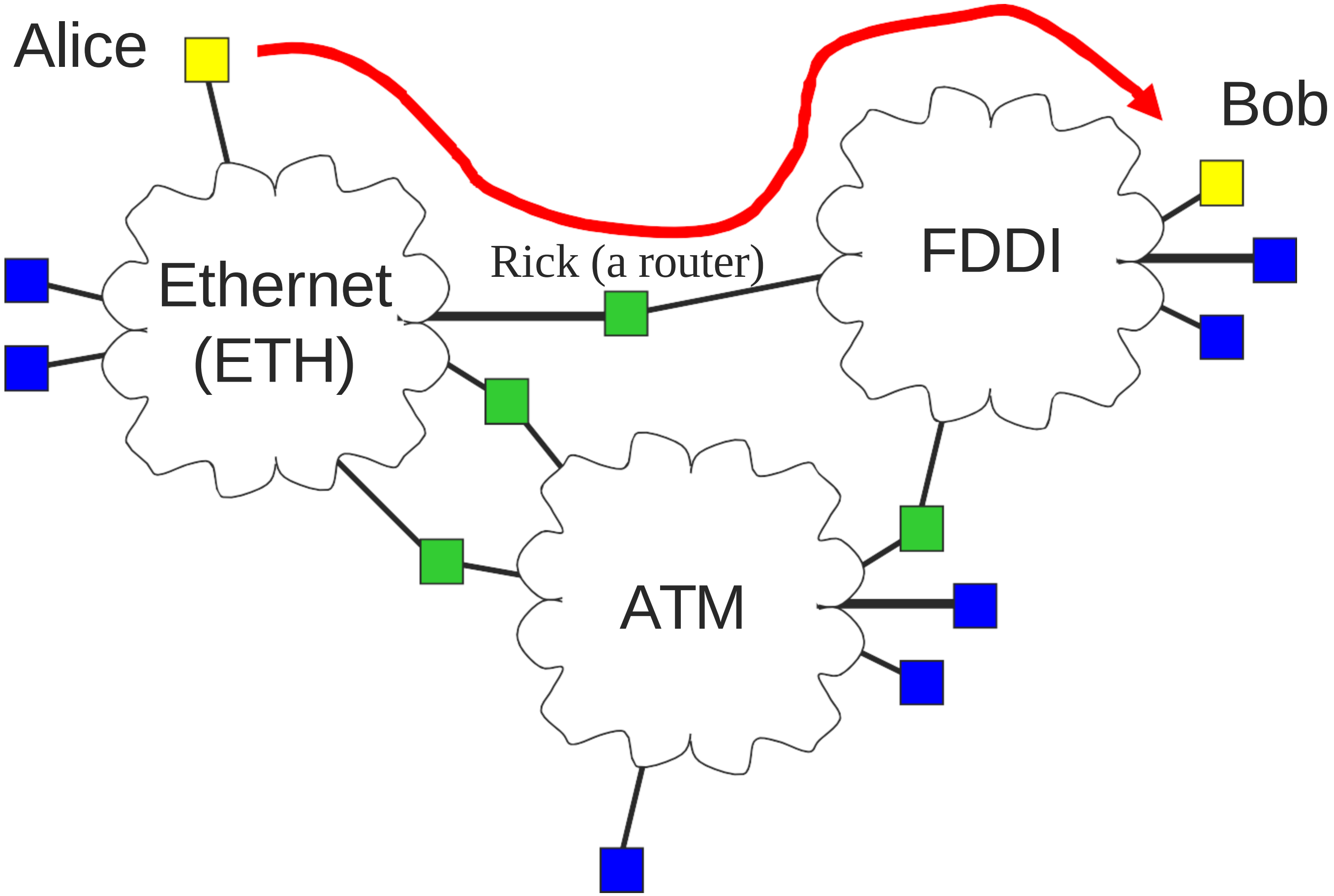


Outline of Internetworking with IP

- Overview of message transmission
- Fragmentation and reassembly
- Host addressing and address translation
- Error reporting/control messages
- Dynamic configuration

Overview of message transmission

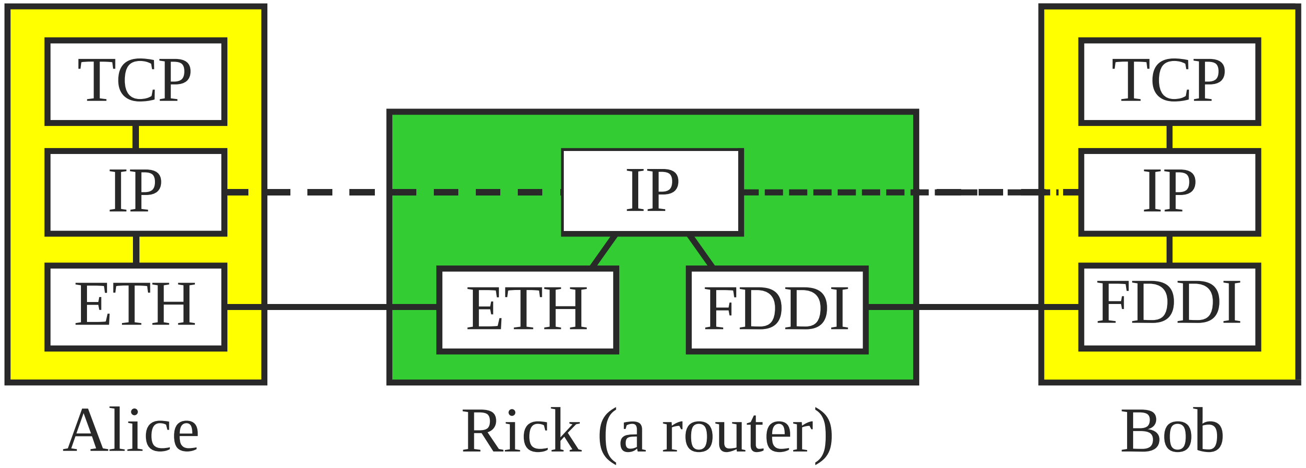
Message Transmission



Message Transmission

Alice's IP datagram:
Alice's IP, Bob's IP

Alice's Ethernet Frame
Alice' MAC address, Rick's MAC address, Alice's IP datagram



Rick's Ethernet Frame
Rick's MAC address, Bob's MAC address, Alice's IP datagram

1. Alice/application finds Bob's IP address, sends packet
2. Alice/IP forwards packet to Rick
3. Alice/IP looks up Rick's Ethernet address and sends it to Rick's Ethernet interface.
4. Rick/IP forwards packet to Bob
5. Rick/IP looks up Bob's FDDI address and sends it to Bob's FDDI interface.

IP service model

- Undemanding - operability with any underlaying network technology that might turn up in the internetwork.
- Two fundamental parts:
  - Datagram delivery – connectionless data delivery model
    - Best effort model → unreliable services.
  - Addressing Model – identify the hosts in the internetwork.

Fragmentation and reassembly

IP Packet Size

- Problem
  - Different physical layers provide different limits on frame length
    - Maximum transmission unit (MTU)
    - which is the largest IP datagram that it can carry in a frame
  - Source host does not know minimum value
    - Especially along dynamic routes

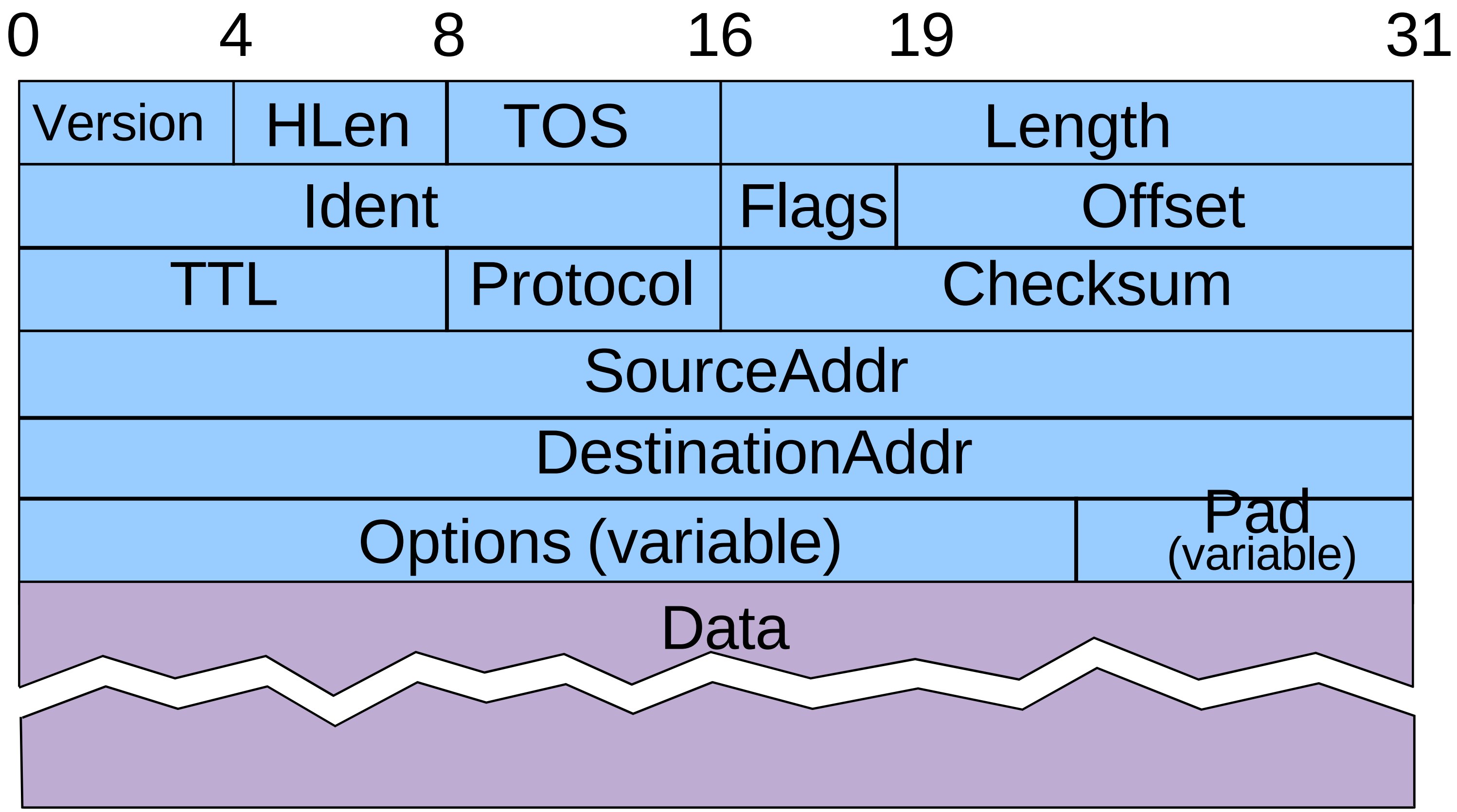
IP Fragmentation and Reassembly

- Solution
  - When necessary, split IP packet into acceptably sized packets prior to sending over physical link
  - Questions
    - Where should reassembly occur?
    - What happens when a fragment is damaged/lost?

IP Fragmentation and Reassembly

- Fragments are self-contained IP datagrams
- Reassemble at destination to minimize refragmentation
- Drop all fragments in a packet if one or more fragments are lost

IP Packet Format

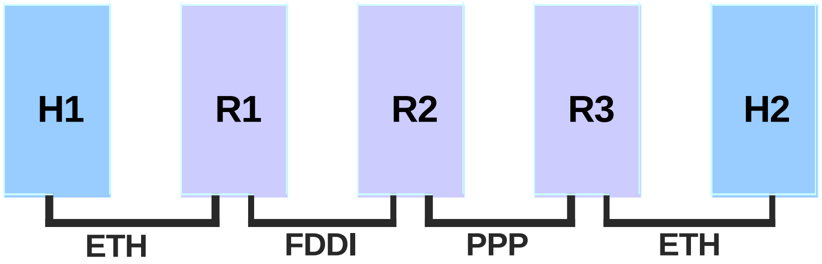


IP Packet Format

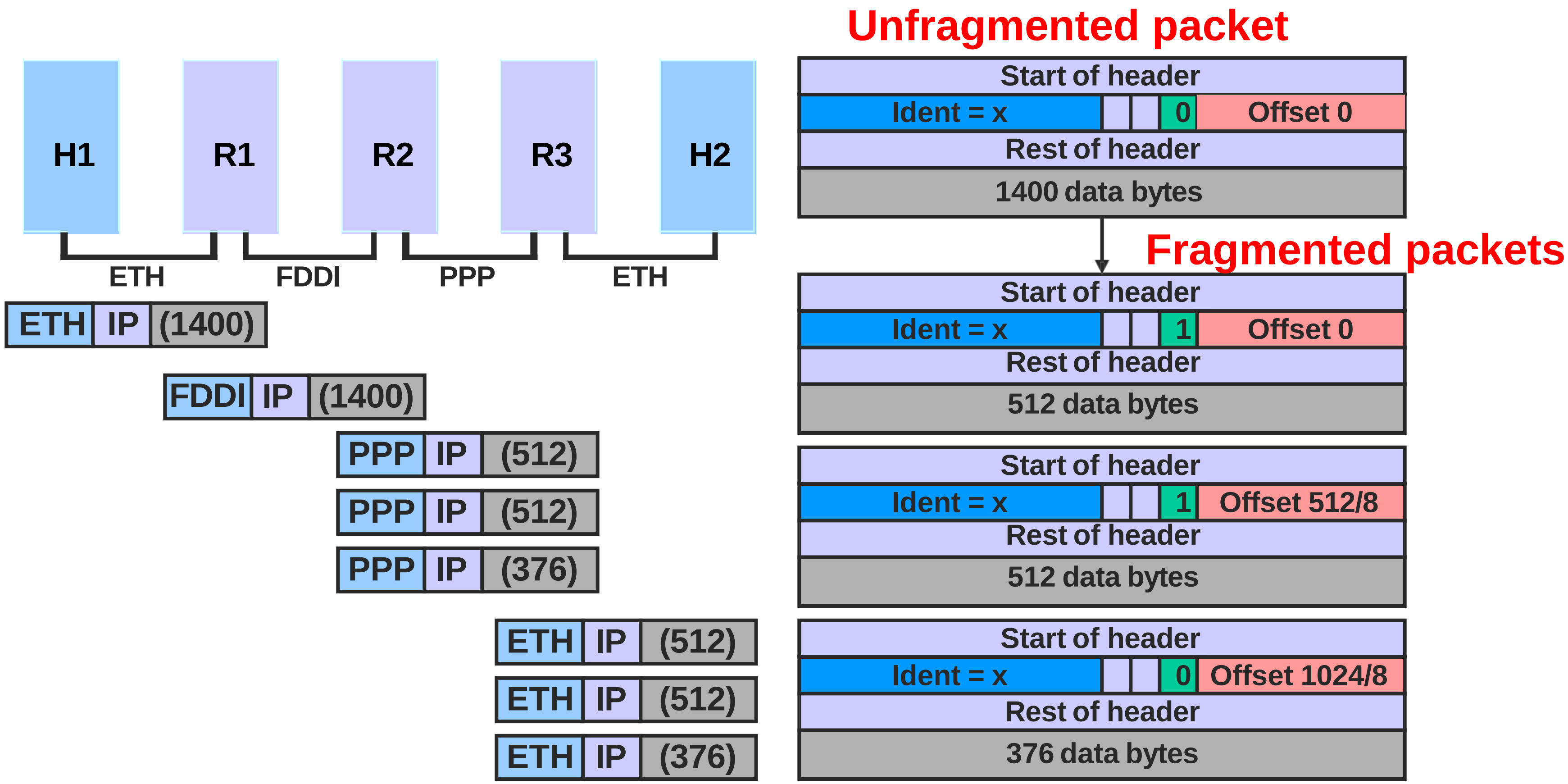
- Fragmentation support
  - 16-bit packet ID
    - All fragments from the same packet have the same ID
  - 3-bit flags
    - 1-bit to mark last fragment
  - 13-bit fragment offset into packet
    - Counted in 8-byte words
- 8-bit time-to-live field (TTL)
  - Hop count decremented at each router
  - Packet is discard if TTL = 0

Example:

- H1-> H2, through R1 (Ethernet), R2 (FDDI), R3 (Point2Point, PPP)=>H2 (Ethernet)
- Assume: MTUs are 1500 for Ethernet, FDDI, and 532 for PPP
- IP datagram is 1420B (20B IP header + 1400 B data)
- At PPP: 512, 512 , 376 (total 1400)
- The fragmentation process is by looking at the header fields of each datagram
- Offset: 8 B chunks, so 512/8, 1024/8



IP Fragmentation and Reassembly



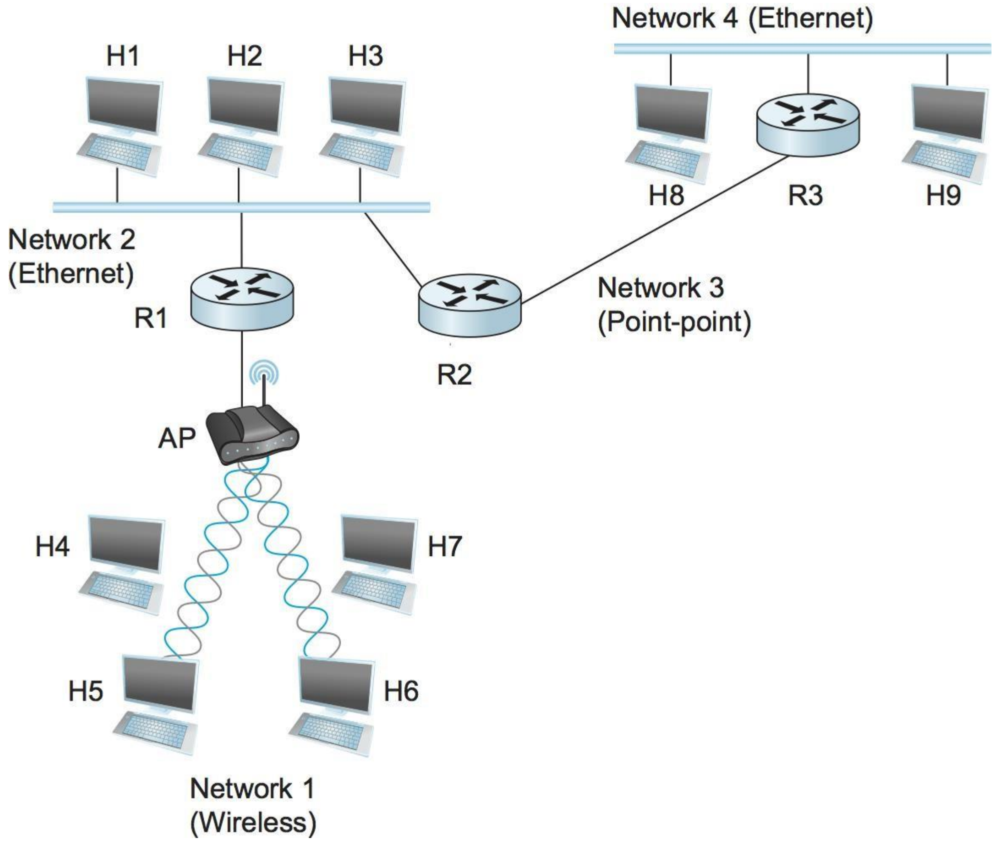
IP Addressing Model

IP addressing: introduction

IP address: 32-bit identifier associated with each host or router *interface*

interface: connection between host/router and physical link

- router's typically have multiple interfaces
- host typically has one or two interfaces.

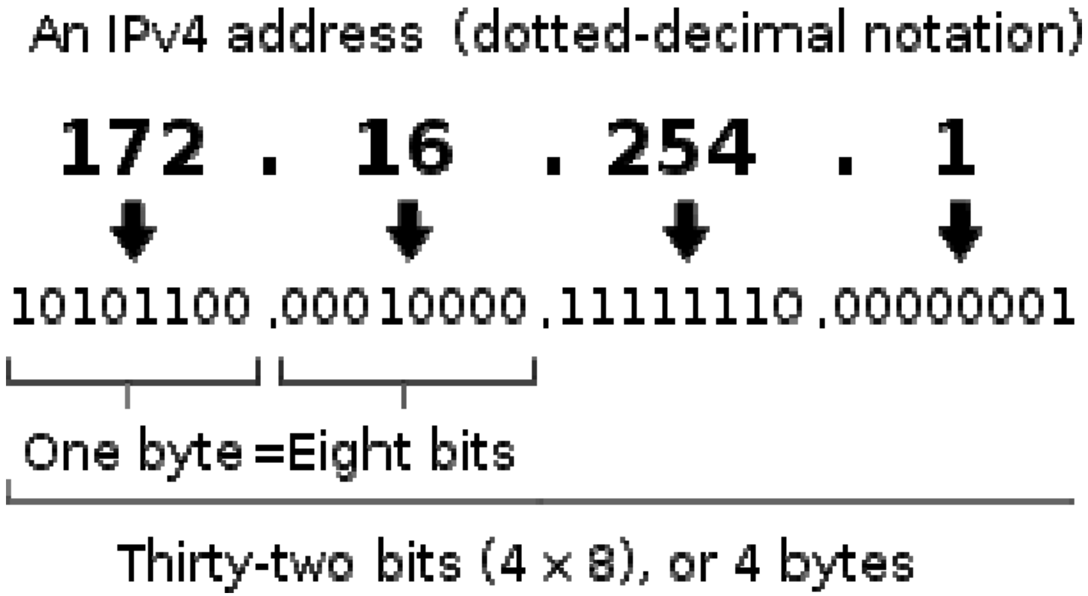


IPv4 Address Model

- Properties
  - 32-bit address
  - Hierarchical
    - Network, subnet, host hierarchy
  - Maps to logically unique network adaptor
- Three Class Model

Class A:	0	Network (7 bits)			Host (24 bits)
Class B:	1	0	Network (14 bits)		Host (16 bits)
Class C:	1	1	0	Network (21 bits)	Host (8 bits)

IP Address Model



IPv4 Address Model

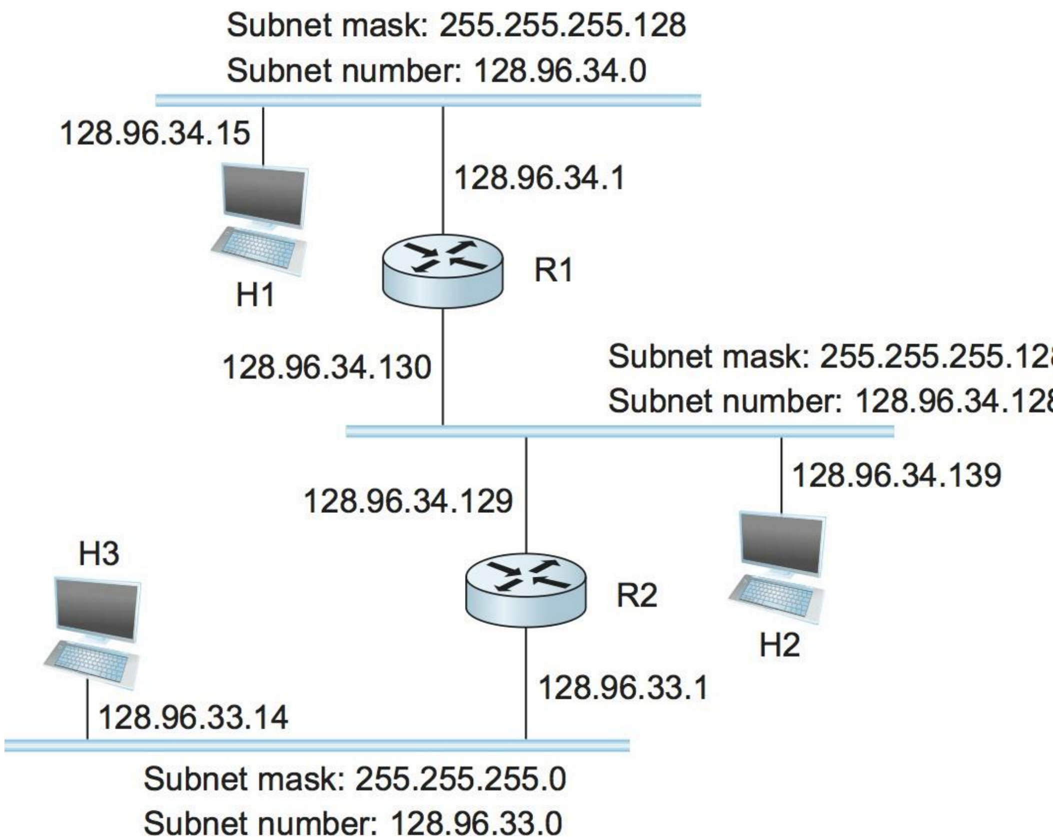
Class	Network ID	Host ID	# of Addresses	# of Networks
A	"0" + 7 bit	24 bit	2^{24}-2	126
B	"10" + 14 bit	16 bit	65,536 - 2	2^{14}
C	"110" + 21 bit	8 bit	256 - 2	2^{21}
D	1110 + Multicast Address		IP Multicast	
E	Future Use			

IPv4 Address Model

- Address Classes
  - 0 to 127: Class A address "prefix 0" (0 and 127 are reserved) → 0|0000001 – 0|1111110
    - Class "A" addresses range from 1.x.x.x to 126.x.x.x only.
  - 128 to 191: Class B address "prefix 10" → 10|000000 – 10|111111
    - Class "B" IP Addresses range from 128.0.x.x to 191.255.x.x.
  - 192 to 223: Class "C" address "prefix 110"→ 110|00000 – 110|11111
    - Class C IP addresses range from 192.0.0.x to 223.255.255.x.
  - 224 to 239: Class "D" or multicast "prefix 1110" → 1110|0000 – 1110|1111
    - Multicast IP address range from 224.0.0.0 to 239.255.255.255
  - 224 to 239: Class "E" IP addresses range from 240.0.0.0 to 255.255.255.254
- Example:
  - Host in class A network
    - 104.93.164.21 → www.canada.ca
  - Host in class B network
    - 132.216.177.160 → www.mcgill.ca

Subnetting addresses

- *What's a subnet ?*
  - device interfaces that can physically reach each other without passing through an intervening router (i.e., L3)
- IP addresses have structure:
  - subnet part: devices in same subnet have common high order bits
  - host part: remaining low order bits



Subnetting addresses

```
D = destination IP address
for each forwarding table entry (SubnetNumber, SubnetMask, NextHop)
    D1 = SubnetMask & D
    if D1 = SubnetNumber
        if NextHop is an interface
            deliver datagram directly to destination
        else
            deliver datagram to NextHop (a router)
```

Network number	Host number

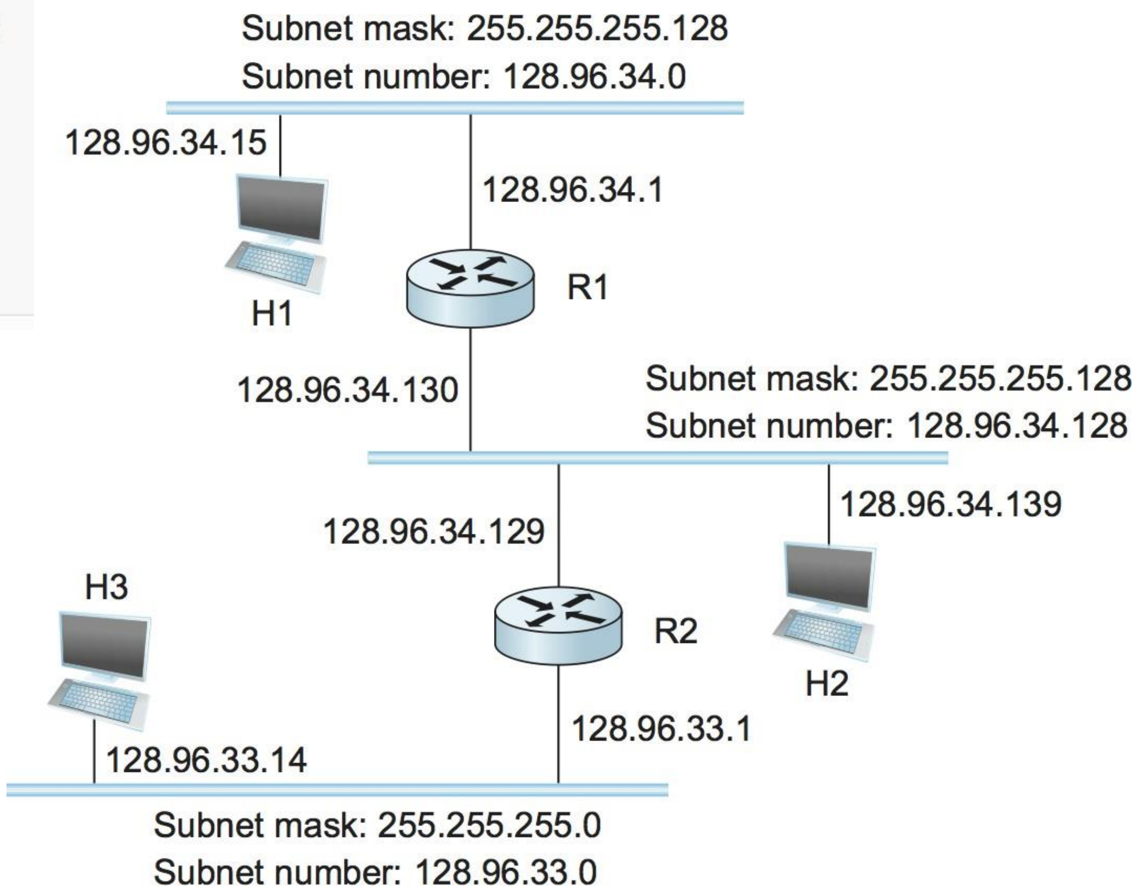
Class B address

111111111111111111111111	00000000

Subnet mask (255.255.255.0)

Network number	Subnet ID	Host ID

Subnetted address



One network Number to the rest of Internet Routers which is 128.96

IP address classes revisited

- Class A default subnet mask: 255.0.0.0/8
- Class B default subnet mask: 255.255.0.0/16
- Class C default sub netmask: 255.255.255.0/24
- No sub netmask for Class D (Multicast) or E (future use)

IP addressing: CIDR

CIDR: Classless InterDomain Routing (pronounced "cider")

- subnet portion of address of arbitrary length
- address format: a.b.c.d/x, where x is # bits in subnet portion of address

subnet part — host part

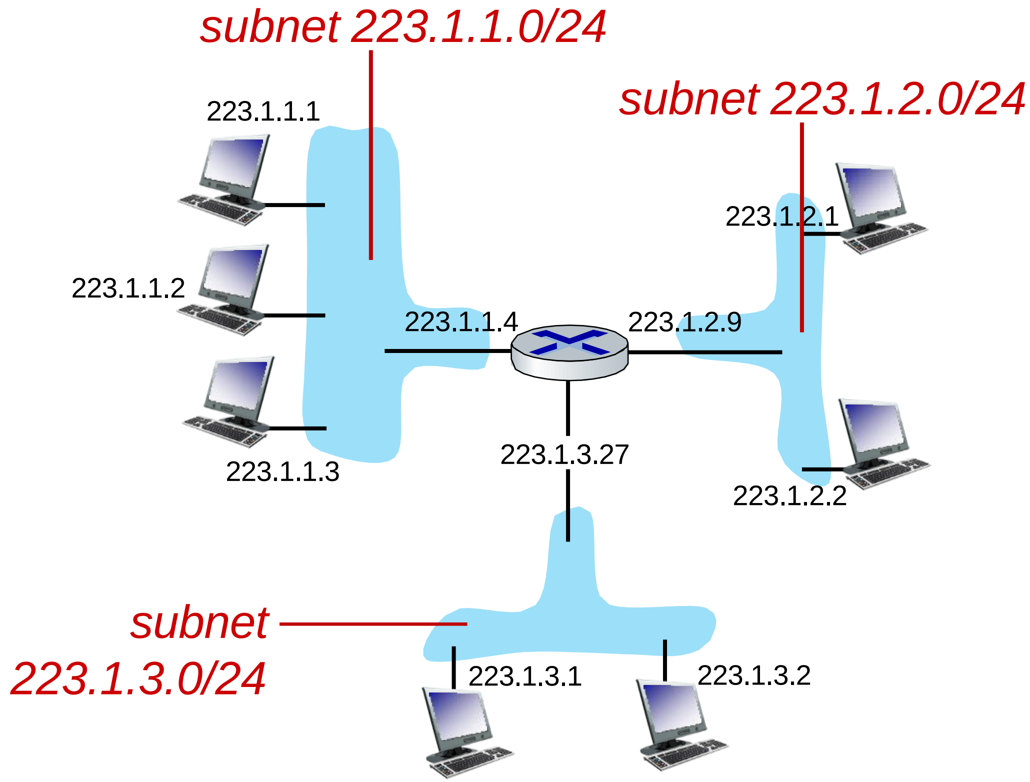
11001000 00010111 00010000 00000000

200.23.16.0/23

Subnets

Recipe for defining subnets:

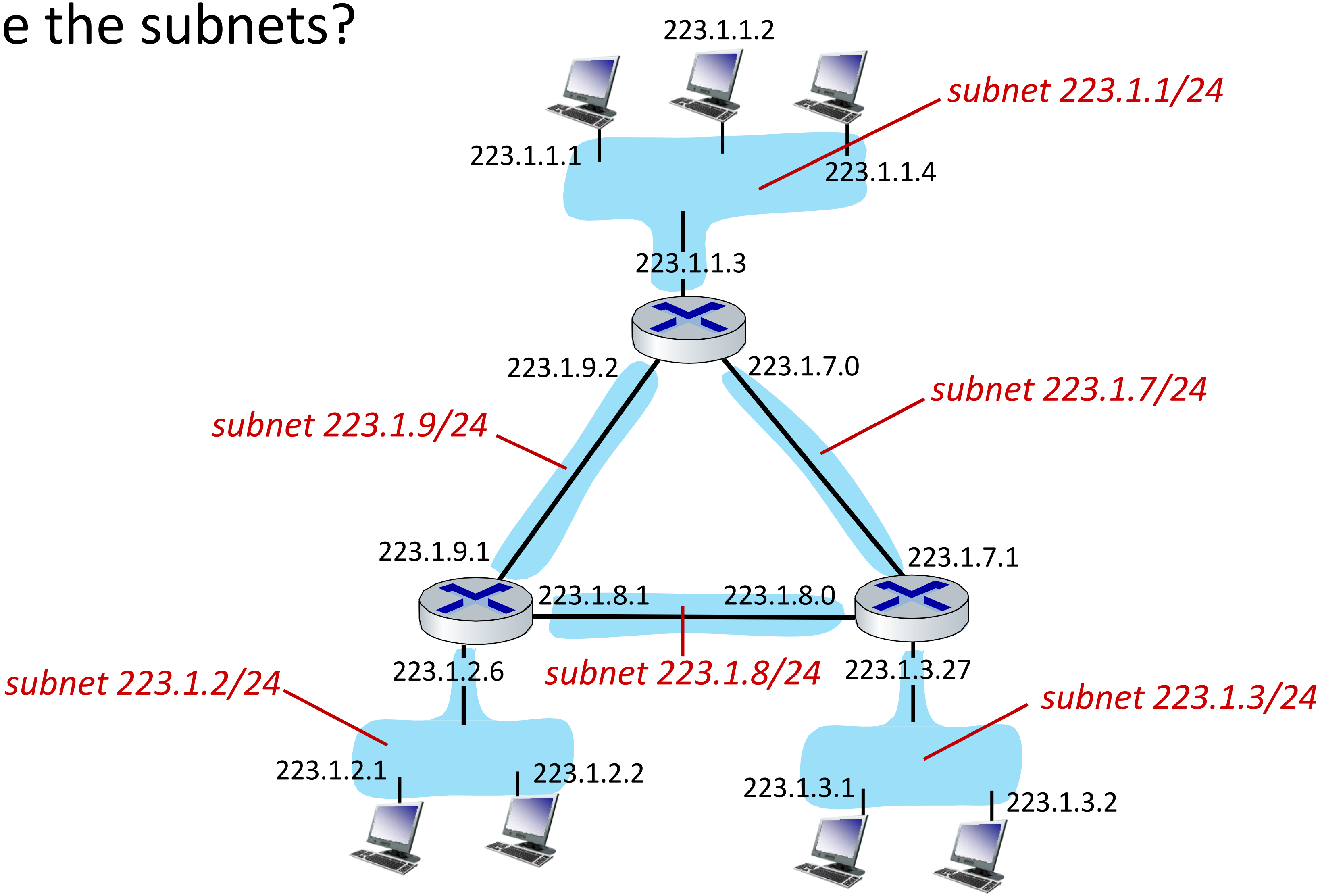
- detach each interface from its host or router, creating "islands" of isolated networks
- each isolated network is called a *subnet*



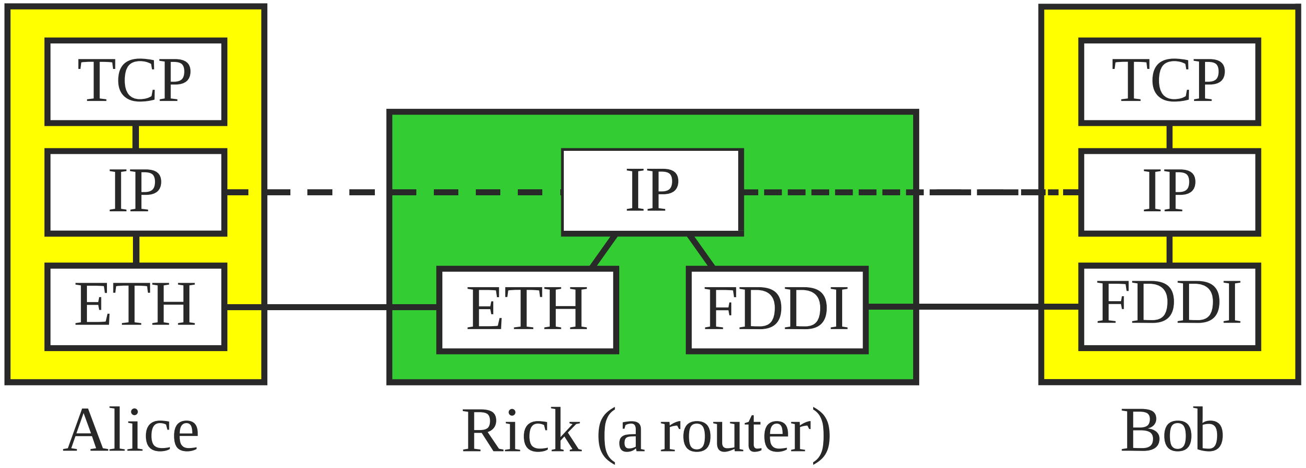
subnet mask: /24
(high-order 24 bits: subnet part of IP address)

Subnets

- where are the subnets?



Host addressing and address translation



IPv4 Address Translation Support

- IP addresses to LAN physical addresses

- Problem
  - An IP route can pass through many physical networks
  - Data must be delivered to destination's physical network
  - Hosts only listen for packets marked with physical interface names

IP to Physical Address Translation

- Hard-coded
  - Encode physical address in IP address
    - Not always possible
- Fixed table
  - Maintain a central repository and distribute to hosts
    - Bottleneck for queries and updates
- Build a table using ARP
  - Each host has a table
  - Use timeouts to clean up table

ARP (Address Resolution Protocol)

- Check table for physical address (IP-> Physical address)
- If address not present
  - Broadcast a query, include target's IP
  - Hope there is a match from one of the host
  - Wait for a response (with physical address)
- Upon receipt of ARP query/response
  - Targeted host responds with address translation
  - If address already present
    - Refresh entry and reset timeout
  - If address not present
    - Add entry for requesting host
- Timeout and discard entries after O(10) minutes

ARP Packet

0	8	16	31
Hardware type = 1		ProtocolType = 0x0800	
HLEN = 48	PLEN = 32	Operation	
SourceHardwareAddr (bytes 0 – 3)			
SourceHardwareAddr (bytes 4 – 5)		SourceProtocolAddr (bytes 0 – 1)	
SourceProtocolAddr (bytes 2 – 3)		TargetHardwareAddr (bytes 0 – 1)	
TargetHardwareAddr (bytes 2 – 5)			
TargetProtocolAddr (bytes 0 – 3)			

Datagram forwarding with IP

- Hosts and routers maintain forwarding tables
  - List of <network/host, next hop> pairs
- Packet forwarding
  - Compare network portion of address with <network/host, next hop> pairs in table
  - Send directly to a host on same network
  - Send indirectly (via router on same network) to a host on different network
  - Use ARP to get hardware address of host/router

Dynamic configuration

Host Configuration

- Plug new host into network
  - How much information must be known?
  - What new information must be assigned?
  - How can the process be automated?
- Some answers
  - Host needs an IP address (must know it)
  - Host must also
    - Send packets out of physical (direct) network
    - Thus needs physical address of router

Dynamic Host Configuration Protocol (DHCP)

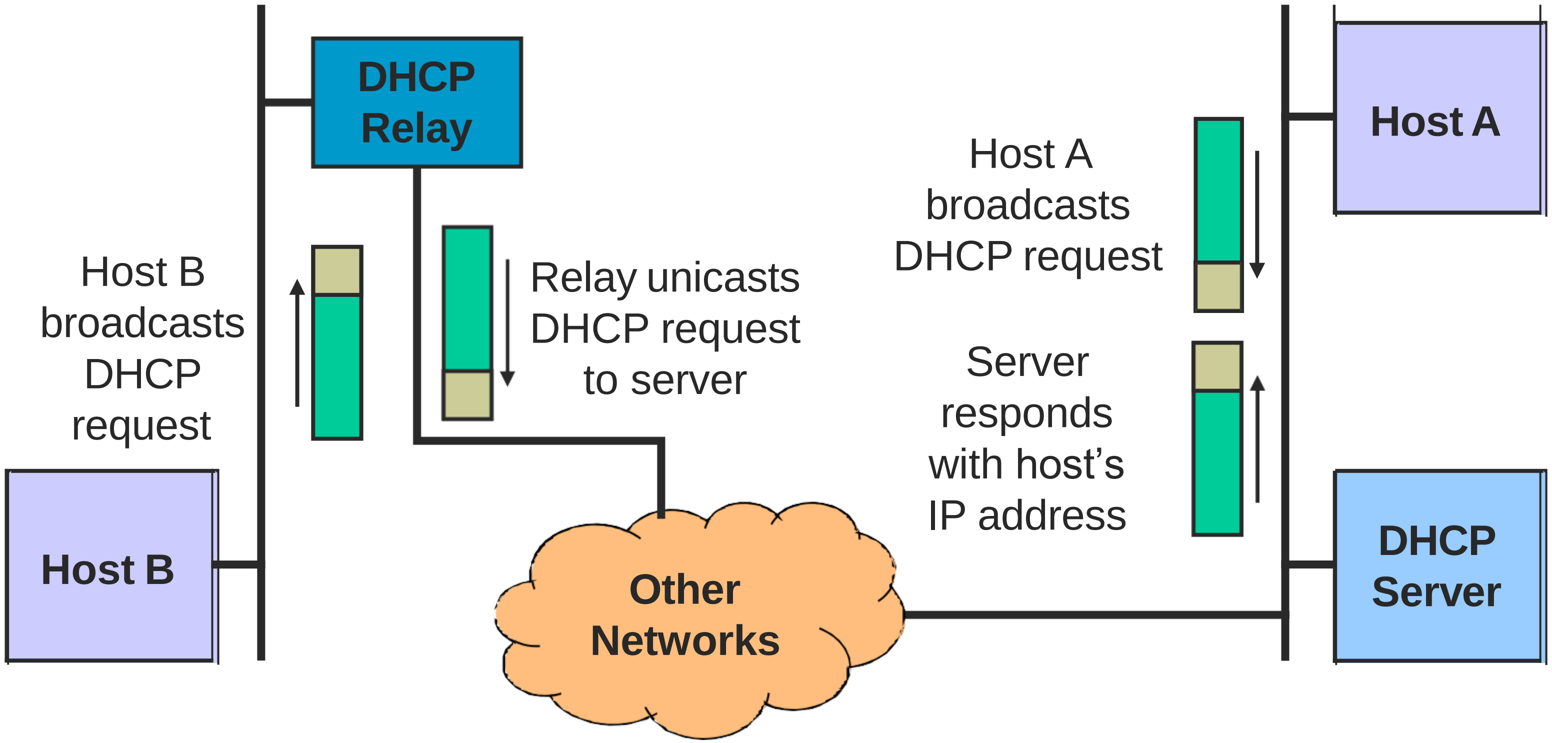
- A simple way to automate configuration information
  - Network administrator does not need to enter host IP address by hand
  - Good for large and/or dynamic networks

Dynamic Host Configuration Protocol (DHCP)

- New machine sends request to DHCP server for assignment and information
- Server assigns IP address and may provides other info
- DHCP server can maintain a list of (Ethernet address->IP address)
- There is at least one DHCP server for an administrative domain.

DHCP

Dynamic configuration



A DHCP relay agent receives a broadcast DHCPDISCOVER message from a host and sends a unicast DHCPDISCOVER to the DHCP server.

Extra Exercises in Textbook

- Chapter 3
  - 33, 34, 36, and 38.

TCP/IP	OSI Model	Protocols
Application Layer	Application Layer	DNS, DHCP, FTP, HTTPS, IMAP, LDAP, NTP,POP3, RTP, RTSP, SSH, SIP, SMTP, SNMP, Telnet, TFTP
	Presentation Layer	JPEG, MIDI, MPEG, PICT, TIFF
	Session Layer	NetBIOS, NFS, PAP, SCP, SQL, ZIP
Transport Layer	Transport Layer	TCP, UDP
Internet Layer	Network Layer	ICMP, IGMP, IPsec, IPv4, IPv6, IPX, RIP
Link Layer	Data Link Layer	ARP, ATM, CDP, FDDI, Frame Relay, HDLC, MPLS, PPP, STP, Token Ring
	Physical Layer	Bluetooth, Ethernet, DSL, ISDN, 802.11 Wi-Fi