CPE348: Introduction to Computer Networks

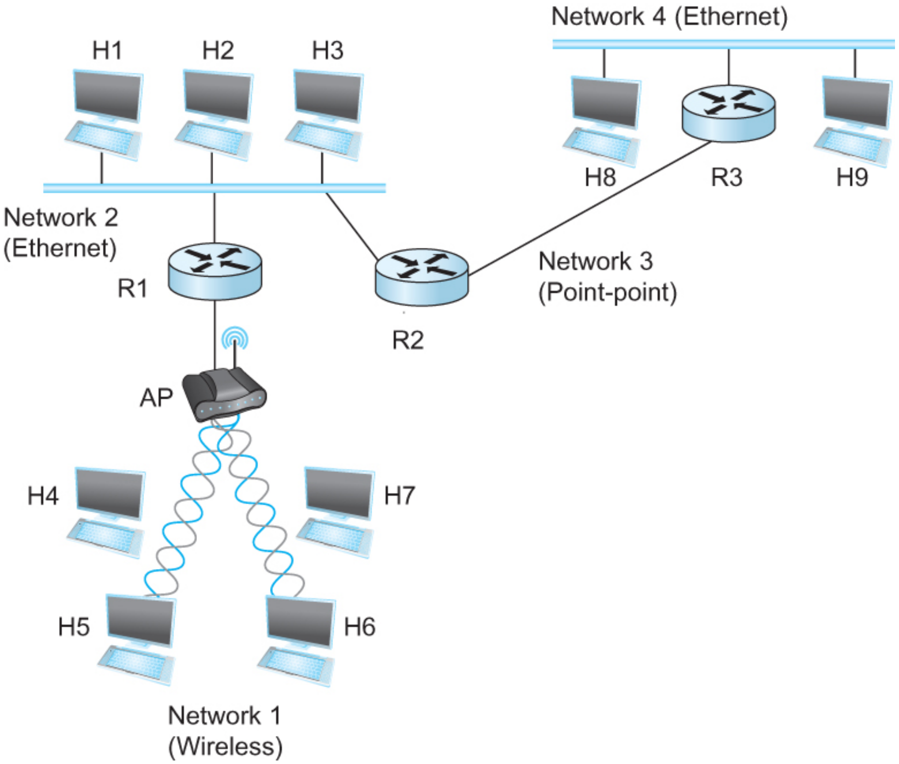
Lecture #11: Chapter 3.4

Jianqing Liu
Assistant Professor of Electrical and Computer Engineering, University of Alabama in Huntsville

jianqing.liu@uah.edu
http://jianqingliu.net

Internetworking

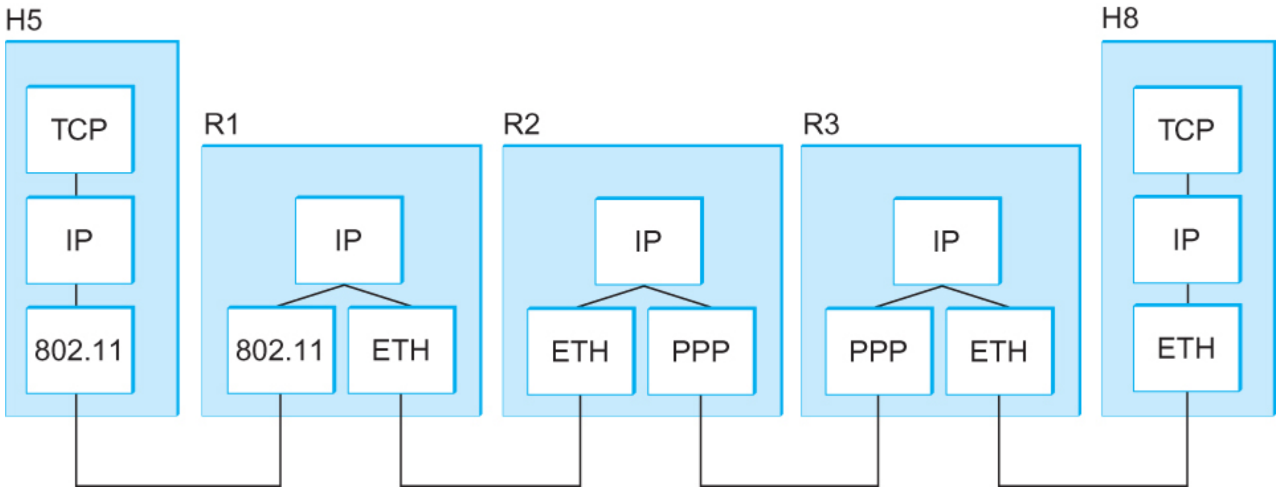
- What is internetwork
  - An arbitrary collection of networks interconnected to provide host-host packet delivery service



A simple internetwork where H represents hosts and R represents routers

Internetworking

- What is IP
  - IP stands for Internet Protocol
  - Key tool used today to build scalable, heterogeneous internetworks
  - It runs on all the nodes in a collection of networks and defines the infrastructure that allows these nodes and networks to function as a single logical internetwork



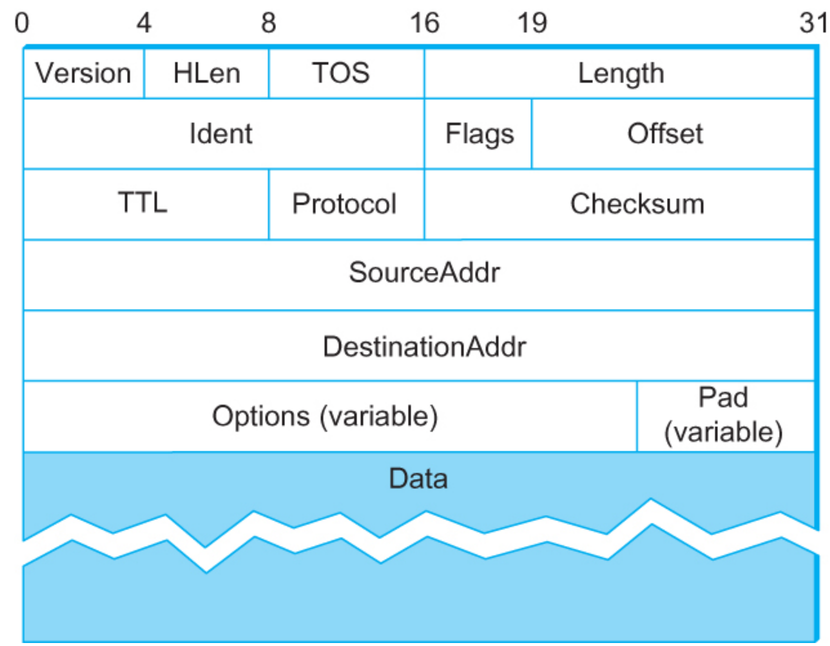
A simple internetwork showing the protocol layers

IP Service Model

- Packet Delivery Model
  - Connectionless model for data delivery
  - Best-effort delivery (unreliable service)
    - packets are lost
    - packets are delivered out of order
    - duplicate copies of a packet are delivered
    - packets can be delayed for a long time
- Global Addressing Scheme
  - Provides a way to identify all hosts in the network

Packet Format (IPv4)

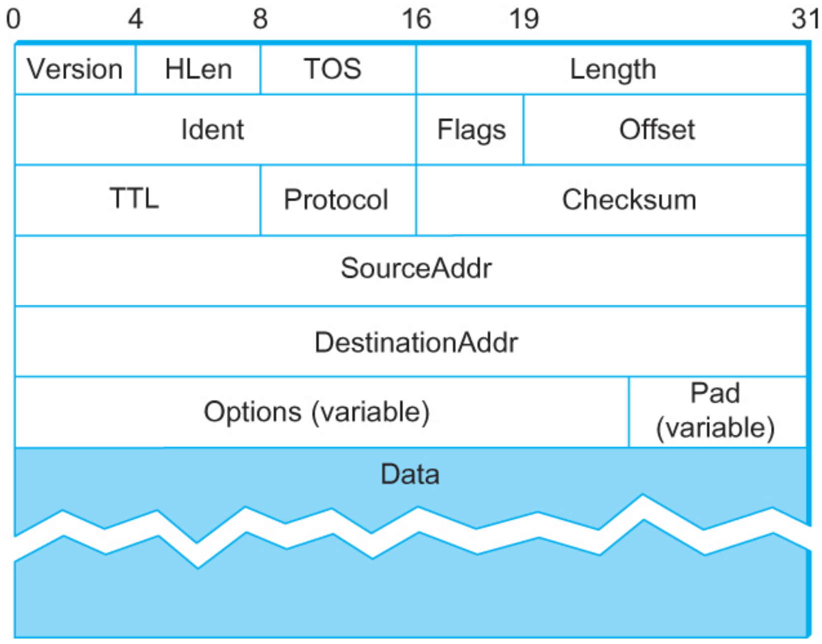
- Version (4 bits): IPv4/6
- Hlen (4 bits): number of 32-bit words in header. 5 words typically without Options
- TOS (8 bits): type of service (not widely used)
- Length (16 bits): number of bytes in this datagram – maximum datagram size is 65535 Bytes
- Ident (16 bits): used by fragmentation
- Flags/Offset (16 bits): used by fragmentation



<Return>

Packet Format (IPv4)

- TTL (8 bits): number of hops this datagram has traveled – typically it is a countdown timer
- Protocol (8): demux key (TCP=6, UDP=17)-higher level protocol using the packet info
- Checksum (16 bits): of the header only (IP checksum algorithm)
- DestAddr & SrcAddr (32 bits each, IPv6 has 128)
- Options/Pad (32 bits) – rarely used

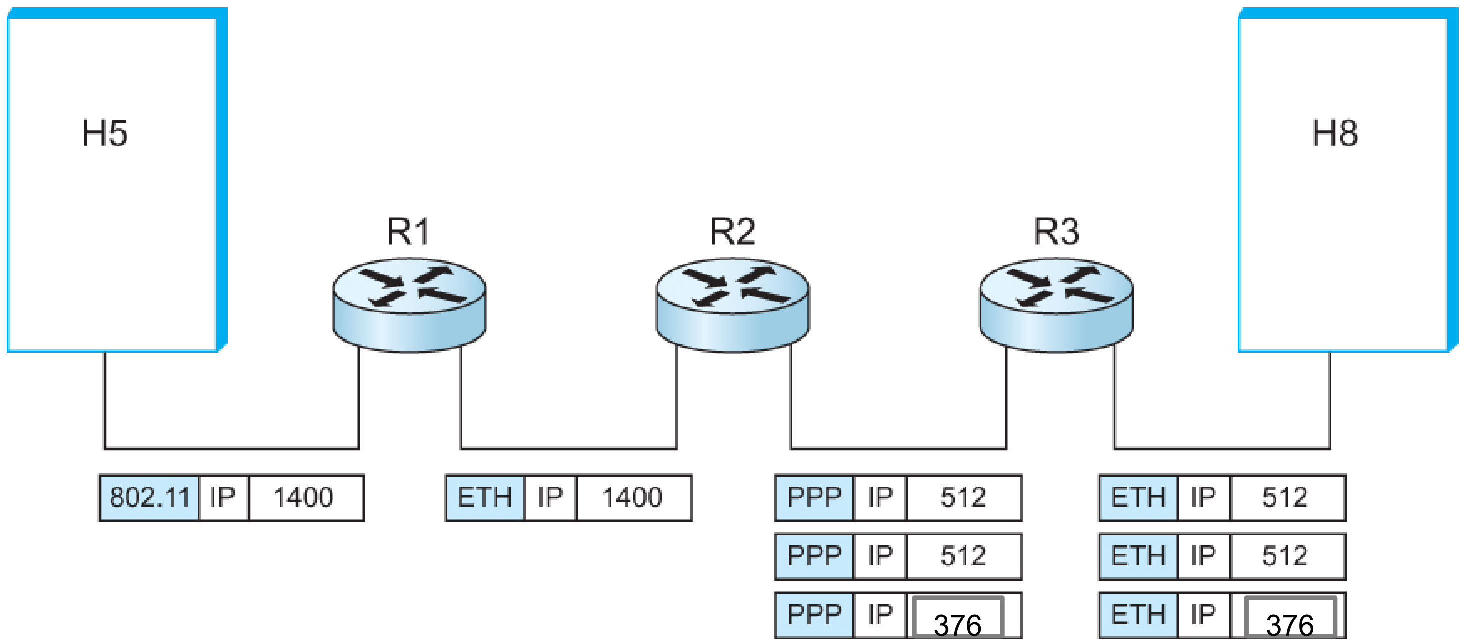


IP Fragmentation and Reassembly

- Each network has some MTU (Maximum Transmission Unit)
  - Ethernet (1500 bytes)

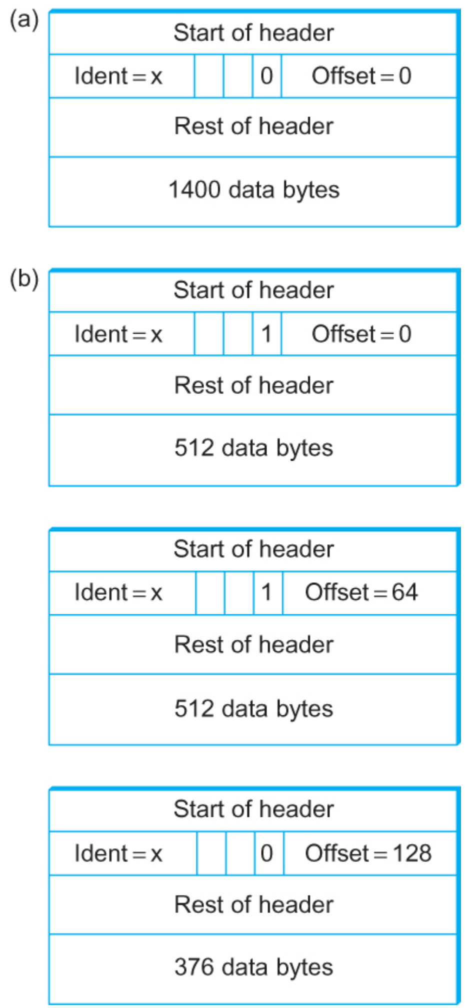
- Strategy
  - Fragmentation occurs in a router when it receives a datagram
  - Reassembly is done at the receiving host
  - All the fragments carry the same identifier in the *Ident* field
  - Fragments are self-contained datagrams
  - Fragments re-encapsulate each IP datagram
  - IP does not recover from missing fragments

IP Fragmentation and Reassembly



IP datagrams traversing the sequence of physical networks

IP Fragmentation and Reassembly



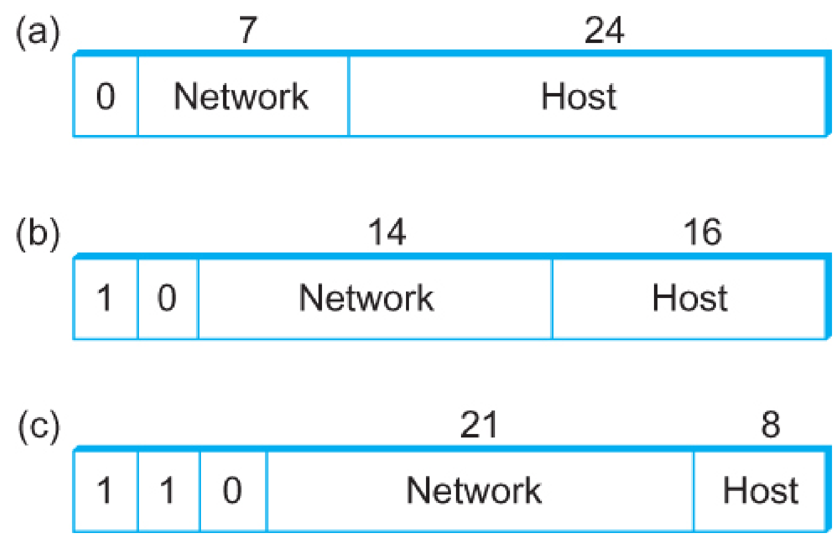
(a) Total packet size = 1420 bytes
(20 bytes for header, 1400 for data)

(b) Total size of packets = 20*3 + 1400 = 1460 Bytes
(3 headers @ 20 bytes each plus data)

Header fields used in IP fragmentation. (a) Unfragmented packet; (b) fragmented packets.

Global Addresses

- Properties
  - globally unique
  - hierarchical: network + host
  - 4 Billion IP address, half are A type, ¼ is B type, and 1/8 is C type
- Format



(a) Class A, (b) Class B, (c) Class C

- Dot notation
  - 10.3.2.4
  - 128.96.33.81
  - 192.12.69.77

Global Addresses

Class	1st Octet Decimal Range	1st Octet High Order Bits	Network/ Host ID (N=Network, H=Host)	Default Subnet Mask	Number of Networks	Hosts per Network (Usable Addresses)**
A	1 – 126*	0	N.H.H.H	255.0.0.0	126 ($2^7 - 2$)	16,777,214 ($2^{24} - 2$)
B	128 – 191	10	N.N.H.H	255.255.0.0	16,382 ($2^{14} - 2$)	65,534 ($2^{16} - 2$)
C	192 – 223	110	N.N.N.H	255.255.255.0	2,097,150 ($2^{21} - 2$)	254 ($2^8 - 2$)
D	224 – 239	1110	Reserved for Multicasting			
E	240 – 254	1111	Experimental; used for research			

Note: *Class A addresses 127.0.0.0 to 127.255.255.255 cannot be used and are reserved for loopback and diagnostic functions.

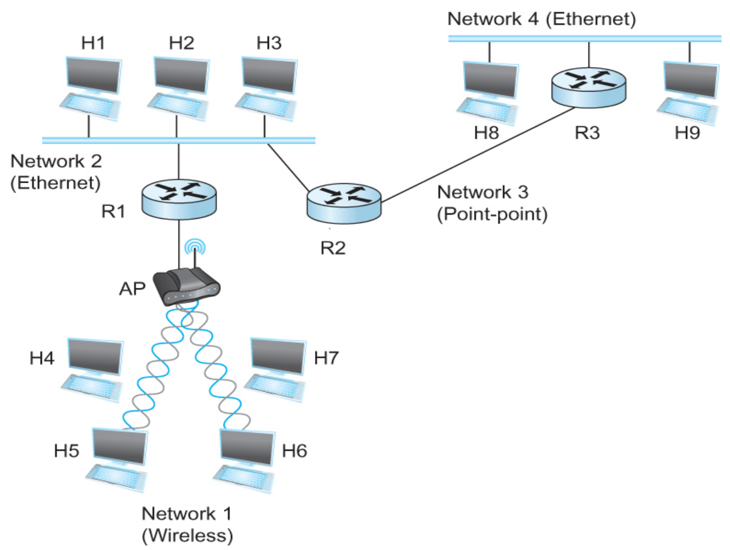
** host 255 is for broadcast, host 0 is not a valid host – identifies the network

IP Datagram Forwarding

- Strategy
  - every datagram contains destination's address
  - if directly connected to destination network, then forward to host
  - if not, then forward to some router
  - forwarding table maps network number into next hop
  - each host has a default router
  - each router maintains a forwarding table

- Example (router R2)

NetworkNum	NextHop
1	R1
2	Interface 1
3	Interface 0
4	R3



Subnetting

- Take one IP network number and break it up into subnets
- Adds another level to address hierarchy: *subnet*
- *Subnet masks* define variable partition of host part of class A and B addresses
- Subnets visible only within site of base IP network

- Reason: Allows for smaller number of hosts to be handled more efficiently
  - If a network is to connect 300 hosts
    - Need 2 class C networks – requires 2 Network addresses in tables
    - 1 class B network – requires one network address, but wastes over 65,000 hosts

Subnetting

- Assign a Class B network to a group that creates a subnet

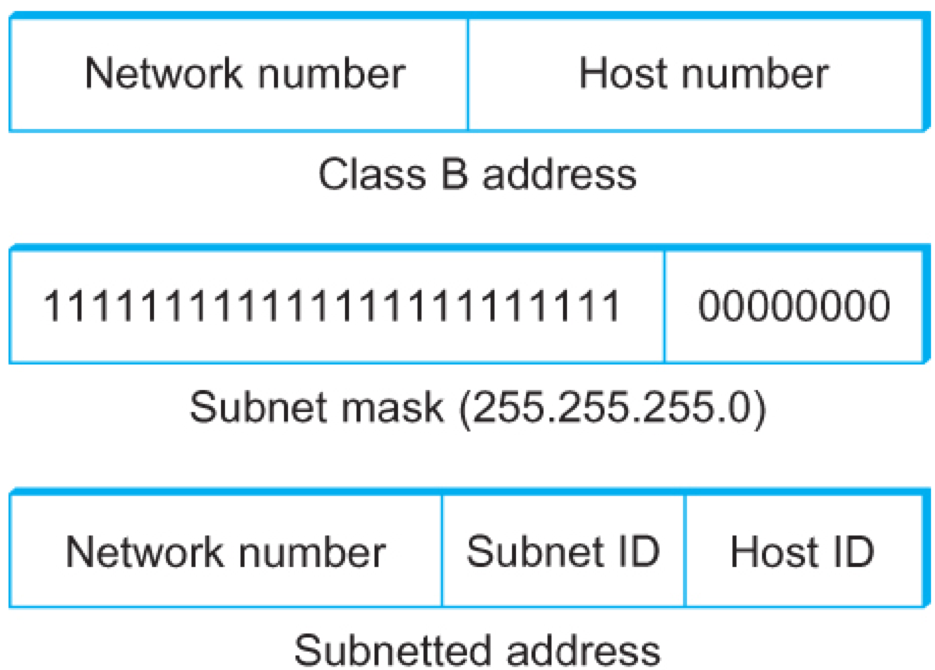
  192.11.0.0 to 192.11.255.255

- Router advertises network address192.11.0.0/16 (/16 indicates first 16 bits as the network address)
  - Subnet mask is 255.255.XXX.0
  - The third octet of mask determines how the Class B network is subnetted

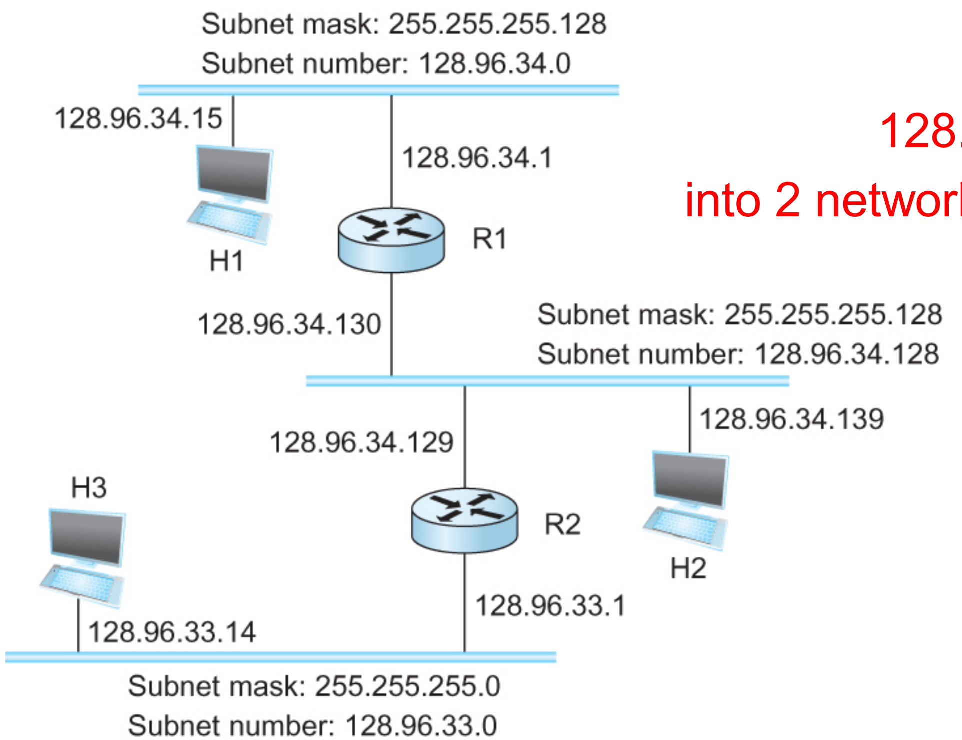
Start Address	End Address	Subnet Mask	Subnet IP
192.11.128.0	192.11.255.255	255.255.128.0	192.11.128.0
192.11.64.0	192.11.127.255	255.255.192.0	192.11.64.0
192.11.16.0	192.11.31.255	255.255.240.0	192.11.16.0
192.11.48.0	192.11.63.255	255.255.240.0	192.11.48.0

Subnetting

- Subnets visible only within site.
- Subnetted address is calculated by bit-wise AND operation between IP address and subnet mask.



Subnetting



128.96.34 is split

into 2 networks with 126 hosts each

- Forwarding Table at Router R1

SubnetNumber	SubnetMask	NextHop
128.96.34.0	255.255.255.128	Interface 0
128.96.34.128	255.255.255.128	Interface 1
128.96.33.0	255.255.255.0	R2

Subnetting

Forwarding Algorithm

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

Subnetting

Notes

- Would use a default router if nothing matches
- Subnets not visible from the rest of the Internet

Classless Addressing

- Classless Inter-Domain Routing (CIDR)
  - A technique that addresses two scaling concerns in the Internet
    - The growth of backbone routing table
    - Potential exhaustion of the 32-bit address space
  - Addresses assignment efficiency
    - IP address structure forces us to hand out network address space in fixed-size chunks
      - A network with two hosts needs a class C address
        - Address assignment efficiency = 2/255 = 0.78e-2
      - A network with 256 hosts needs a class B address
        - Address assignment efficiency = 256/65535 = 0.39e-2

Classless Addressing

Example:

- If a company has, say 16 class C network numbers assigned to it (4064 hosts),
  - Every Internet backbone router needs 16 entries in its routing tables for them
  - Even if the path to every one of class C networks is the same

- If we had assigned a class B address to them
  - The same routing information can be stored in one entry
  - But Efficiency(% used) = 16 × 256 / 65, 536 = 6.25%

Classless Addressing

- CIDR tries to balance the desire to minimize the number of routes that a router needs to know against the need to hand out addresses efficiently.

- CIDR uses aggregate routes
  - Uses a single entry in the forwarding table to tell the router how to reach a lot of different networks

Classless Addressing

- Consider a company with 16 class C network numbers.
- Instead of handing out 16 addresses at random, hand out a block of contiguous class C addresses
- Suppose we assign the class C network numbers from 192.4.16 through 192.4.31
- Observe that top 20 bits of all the addresses in this range are the same (11000000 00000100 0001)

Classless Addressing

- The convention is to place a /X after the prefix where X is the prefix length in bits
- In this example, the 20-bit prefix for all the networks 192.4.16 through 192.4.31 is represented as 192.4.16/20

Subnetting

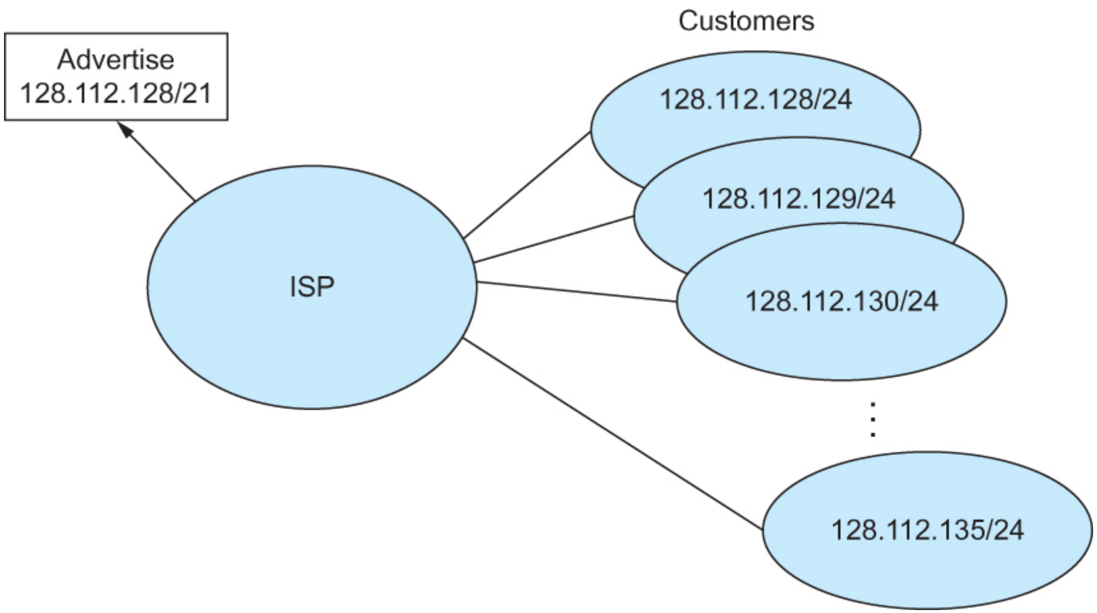
- Want a network router to handle 8 class C networks

  192.11.64.XXX to 192.11.71.XXX

- Router advertises network address192.11.64/21
  - Subnet mask is 255.255.248.0
  - The third octet of IP addresses are masked with 11111000 (248)

Third Octet	3^{rd} Octet Binary	Masked	Subnet IP
63	00111111	00111000	192.11.56.0
64	01000000	01000000	192.11.64.0
71	01000111	01000000	192.11.64.0
72	01001000	01001000	192.11.72.0

Classless Addressing



Route aggregation with CIDR

Classless Addressing

- It is also possible to have prefixes in the forwarding tables that overlap
- For example, we might find both 171.69 (a 16 bit prefix) and 171.69.10 (a 24 bit prefix) in the forwarding table of a single router
- A packet destined to 171.69.10.5 clearly matches both prefixes - The rule is based on the "longest match"!

Address Translation Protocol (ARP)

- Map IP addresses into physical (MAC) addresses
- ARP (Address Resolution Protocol)
  - table of IP to physical address bindings
  - broadcast request if IP address not in table
  - target machine responds with its physical address
  - table entries are discarded if not refreshed

ARP Packet Format

<table>
<tr><th>0</th><th>8</th><th colspan="2">16   31</th></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>

- HardwareType: type of physical network (e.g., Ethernet)
- ProtocolType: type of higher layer protocol (e.g., IP)
- HLEN & PLEN: length of physical(MAC) and protocol(IP) addresses
- Operation: ARP request or ARP response
- Source/Target Physical(Ethernet)/Protocol(IP) addresses

Host Configurations

- When a computer is firstly connected to the Internet,
  - A unique IP address is assigned
    1. Either automatically,
    2. Or, its OS manually configures it

- Drawbacks of manual configuration
  - A lot of work to configure all the hosts in a large network
  - Configuration process is error-prone

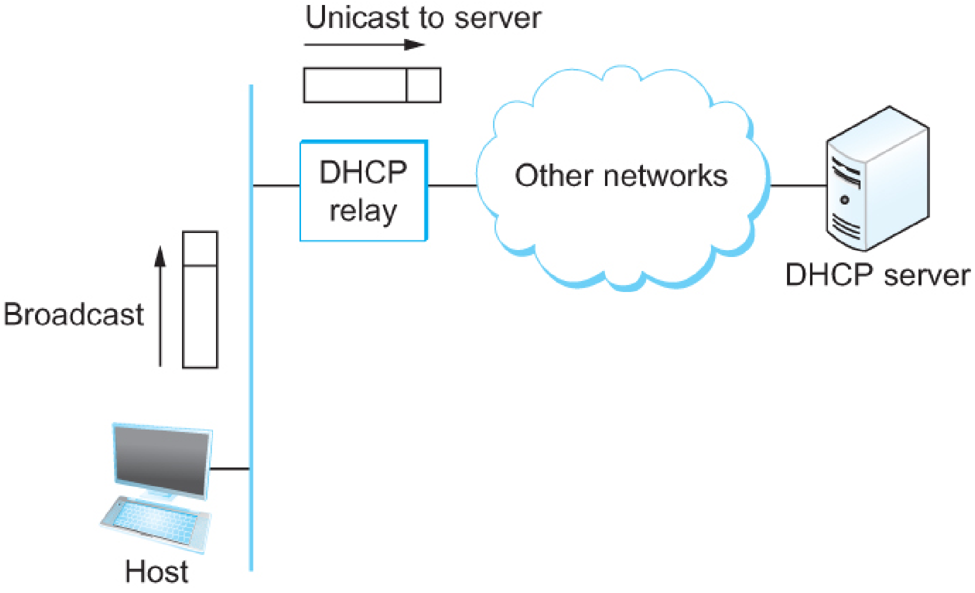
Dynamic Host Configuration Protocol (DHCP)

- DHCP server is responsible for providing automatic IP configuration to hosts
  - There is at least one DHCP server for an administrative domain
  - DHCP server maintains a pool of available addresses
  - DHCP leases an address to a host. Host must renew the lease periodically, in case of disconnected.

DHCP

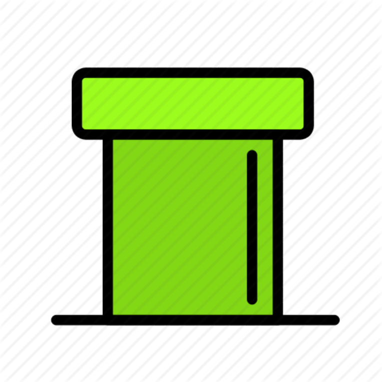
- New host sends DHCPDISCOVER message to a special IP address (255.255.255.255)

- DHCP relay agent unicasts the message to DHCP server and waits for the response

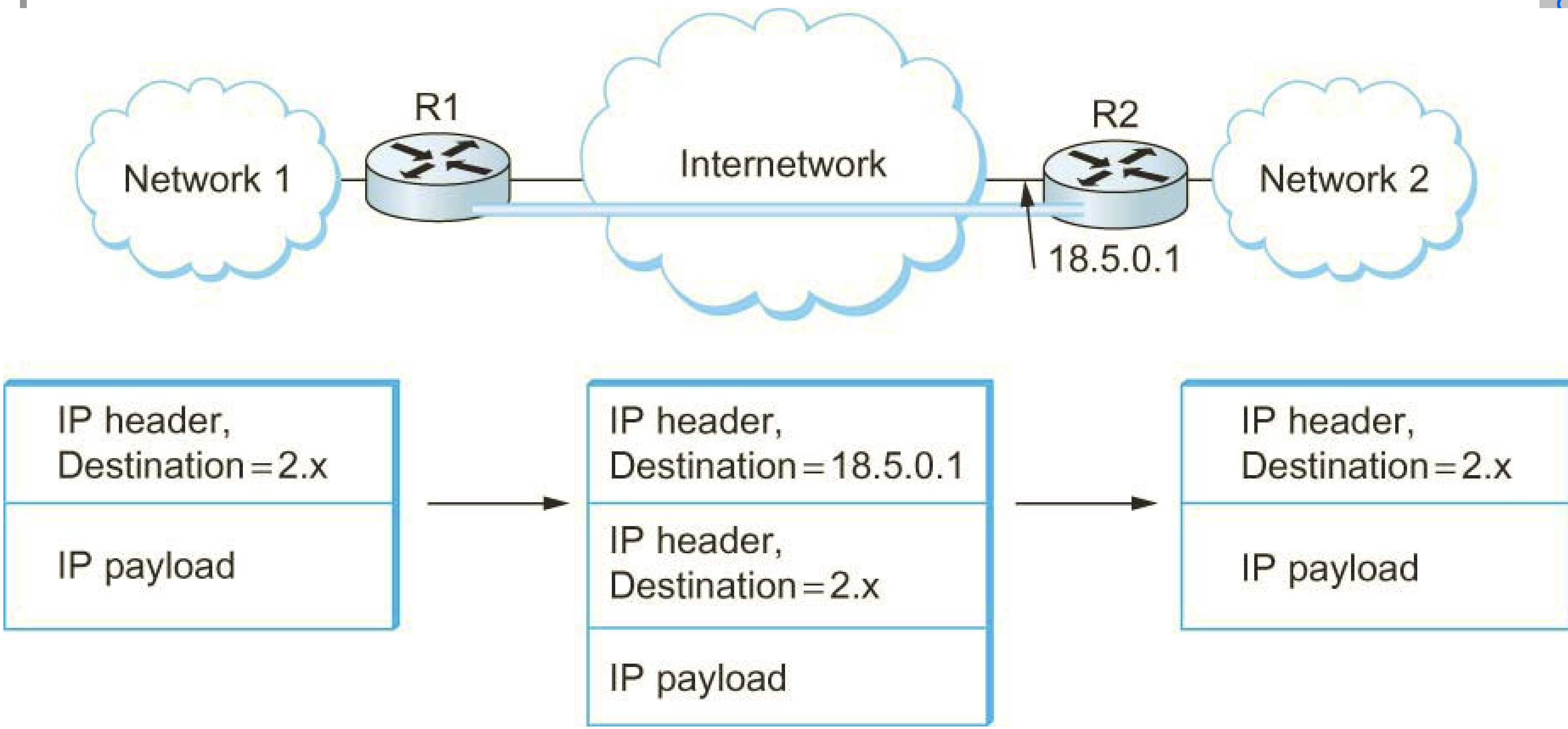


Virtual Networks and Tunnels

- VPN – virtual Private Network
  - Use Virtual point-to-point links on a shared network
  - For IP, use a concept called tunneling
- IP Tunnel
  - Router to Router transmission of an IP Packet
  - It encapsulates the entire IP packet from source to destination.



Virtual Networks and Tunnels



IP Tunnels

- IP Tunnel Advantages
  - Provides security of transmissions
  - Can carry packets from protocols different from IP
  - Can force a packet to be delivered to a particular destination – used with mobile hosts

- IP Tunnel Disadvantages
  - Longer packets are created
  - More work is required at the edge router