

COMS3200

## COMS3200 - Week 8 Network Layer Internet Protocol (IP)

School of Information Technology and Electrical Engineering  
The University of Queensland

COMS3200

## Outline

- Internet Protocol (IP)
  - Packet format
  - Fragmentation
  - Addressing (Covered in COMP2303)
    - Subnets
    - NAT
- Internet Control Message Protocol (ICMP)
- Address Resolution Protocol (ARP)
- Dynamic Host Configuration Protocol (DHCP)
- IPv6
- Mobile IP

2

COMS3200

## Learning objectives

After this week you should:

- Understand aspects of IP (Internet Protocol)
  - Addressing
  - Fragmentation
  - IP header
  - NAT
  - Subnets
- Understand the purposes of the Internet Control Message Protocol
- Understand relationship between Link addresses and IP addresses and the purpose of the Address Resolution Protocol (ARP)

3

COMS3200

## Internetwork

- Definition:
  - Arbitrary collection of networks, interconnected to provide some sort of packet delivery service
- Also called: internet (lowercase i)
- The Internet (uppercase I)
  - Specific example of an internet

4

COMS3200

## Internetworking at network layer

- Three possible ways
  - Concatenation of connections (used for connection-oriented protocols like ATM, frame relay, WiMax)
  - Connectionless internetworking (used in Internet)
  - Tunnelling (if source and destination on same type of network, but there are different networks in between)
- We will concentrate on connectionless internetworking

5

COMS3200

## Internet Structure: Network of Networks

- roughly hierarchical
- at center: "tier-1" ISPs
  - "Backbone" of the Internet
  - international coverage
  - treat each other as equals (peering agreement)
  - Link speeds: 622Mbps - 10Gbps
  - Tier-1 ISPs are typically connected to all other Tier-1 ISPs

6

### History of Peering

- In the early days of the Internet, a **backbone network** existed in the form of first ARPANET and later NSFNET. All other networks connected with one another via the Internet backbone, and routing information was exchanged between the backbone and the other networks via the Exterior Gateway Protocol (EGP).
- The modern Internet no longer has a backbone in the traditional meaning, rather it consists entirely of the various commercial ISPs and private networks. They are all connected at their peering points and supported by the Border Gateway Protocol (BGP)

7

### Tier 1 ISPs

- Qwest
- Telecom Italia Sparkle (Seabone)
- Verizon Business UUNet
- Sprint
- TeliaSonera International Carrier
- NTT Communications
- Tinet
- Deutsche Telekom AG (DTAG)
- Level 3 Communications Global Crossing
- Savvis
- Tata Communications
- AT&T

For up to date Internet map look at [http://www.caida.org/research/topology/as\\_core\\_network/](http://www.caida.org/research/topology/as_core_network/)

8

### Tier-1 ISP: e.g., Sprint

Sprint US backbone network

Sprint

### Internet structure: network of networks

- Tier-2 ISPs: smaller (often regional) ISPs**
  - Connect to one or more tier-1 ISPs, possibly other tier-2 ISPs

Tier-2 ISP pays tier-1 ISP for connectivity to rest of Internet  
 tier-2 ISP is customer of tier-1 provider

Tier-2 ISPs also peer with each other, interconnect at NAP

10

### Internet structure: network of networks

- Tier-3 ISPs and local ISPs**
  - last hop ("access") network (closest to end systems)

Local and tier-3 ISPs are customers of higher tier ISPs connecting them to rest of Internet

11

### Internet structure: network of networks

- a packet passes through many networks!

12

## Traceroute Example

www.traceroute.org

Traceroute originating from telstra server: <http://tcruskit.telstra.net/cgi-bin/trace>

traceroute to www.slashdot.org (66.35.250.151), 30 hops max, 40 byte packets

```

1 FastEthernet6-0.civservice1.Canberra.telstra.net (203.50.1.65) 0.268 ms 0.178 ms 0.164 ms
2 GigabitEthernet3-0.civ-core2.Canberra.telstra.net (203.50.10.129) 0.723 ms 0.652 ms 0.777 ms
3 GigabitEthernet2-2.dkn-core1.Canberra.telstra.net (203.50.6.126) 1.055 ms 1.009 ms 0.613 ms
4 Pos4-1.ken-core4.Sydney.telstra.net (203.50.6.69) 4.329 ms 3.965 ms 4.257 ms
5 10GigabitEthernet3-0.pad-core4.Sydney.telstra.net (203.50.6.86) 4.618 ms 4.656 ms 4.669 ms
6 GigabitEthernet0-2.syd-core01.Sydney.net.reach.com (203.50.13.226) 4.33 ms 4.461 ms 4.424 ms
7 12-1.wil-core02.net.reach.com (202.84.144.65) 161.724 ms 161.804 ms 161.373 ms
8 202.84.251.166 (202.84.251.166) 161.933 ms 162.539 ms 162.346 ms
9 sl-gw28-ana-10-0.sprintlink.net (144.232.58.221) 210.376 ms 210.727 ms 210.797 ms
10 sl-bb24-ana-5-0.sprintlink.net (144.232.1.49) 210.416 ms 210.571 ms 210.346 ms
11 sl-st21-la-13-0.sprintlink.net (144.232.20.69) 212.179 ms 212.825 ms 212.598 ms
12 bpr2-so-3-0-0.LosAngelesEquinix.savvis.net (208.174.196.73) 199.974 ms 198.933 ms 199.003 ms
13 dhr1-pos-5-0.Elsegundola1.savvis.net (208.174.196.98) 198.295 ms 198.618 ms 198.306 ms
14 dhr2-ge-6-0.Elsegundola1.savvis.net (208.172.35.42) 198.132 ms 197.954 ms 198.059 ms
15 dcr2-loopback.LosAngeles.savvis.net (208.172.35.65) 199.565 ms 199.687 ms 199.651 ms
16 dcr2-loopback.SanFranciscofo.savvis.net (206.24.210.100) 210.293 ms 210.556 ms 210.628 ms
17 bhr1-pos-0-0.SantaClaras8.savvis.net (208.172.156.198) 210.09 ms 210.115 ms 209.445 ms
18 csr1-ve240.SantaClaras8.savvis.net (66.35.194.34) 210.252 ms 210.134 ms 438.87 ms
19 66.35.212.174 (66.35.212.174) 212.343 ms 213.872 ms 212.474 ms
20 star.slashdot.org (66.35.250.151) 209.889 ms 210.047 ms 209.481 ms
    
```

13

## The Internet

- Collection of sub-networks
  - Autonomous Systems (AS) is a collection of Networks (i.e. routers) with:
    - A single administrative authority
    - Using common (external) Routing Policy
    - Each AS has a unique AS number
  - Autonomous Systems exchange routing information via BGP protocol
- Quasi-hierarchical
  - Tier-1,2,3 ISPs
- Held together by Internet Protocol (IP)
  - Designed for internetworking
  - Delivers packets from source to destination without regard to networks between

14

## The Internet Network layer

Host, router network layer functions:

15

## Internet Engineering Task Force (IETF)

- Governing body for Internet standards (IP, TCP, UDP, HTTP, SMTP, POP, IMAP, SSL...)
- Credo: "We reject kings, presidents and voting. We believe in rough consensus and running code." Dave Clark
- Organised in Working Groups
  - Routing, security, applications etc.
- Standards are published as Request for Comments (RFC)
- RFCs are numbered in order of publication starting from 1 to the currently highest of RFC5997
- All RFCs are publicly available for free from [www.ietf.org](http://www.ietf.org)
  - E.g. RFC2616 (HTTP 1.1)

16

## Internet Protocol (IP)

- IP's service model
  - "Best effort"
    - No guarantee
      - That packets are delivered
      - Order in which packets are delivered
      - Delay of packets (variation of delay "jitter")
- Addressing scheme – identifies all hosts
  - Each network **interface** has a unique IP address (32bit)
    - Hosts with multiple interfaces (routers) have multiple IP addresses

17

## Internet Network Layer Design Principles

- Outlined in RFC1958
- Keep network simple (datagram forwarding), put complexity at end hosts
  - Deployment of services and upgrades are much easier at end hosts
- Much quoted "End-to-end principle",
  - Saltzer, Reed, and Clark, 1984, "End-to-End Arguments in System Design"

"The function in question can completely and correctly be implemented only with the knowledge and help of the application standing at the endpoints of the communication system. Therefore, providing that questioned function as a feature of the communication system itself is not possible. (Sometimes an incomplete version of the function provided by the communication system may be useful as a performance enhancement.)"

"This principle has important consequences if we require applications to survive partial network failures. An end-to-end protocol design should not rely on the maintenance of state (i.e. information about the state of the end-to-end communication) inside the network. Such state should be maintained only in the endpoints, in such a way that the state can only be destroyed when the endpoint itself breaks (known as fate-sharing). An immediate consequence of this is that datagrams are better than classical virtual circuits. The network's job is to transmit datagrams as efficiently and flexibly as possible."

18

### IP Datagram Format

total datagram length (max  $2^{16}-1=65535$  bytes)

header length 4 bits (in words of 32 bits)

\*"type" of data

max number remaining hops (decremented at each router)

upper layer protocol to deliver payload to E.g. TCP, UDP, ICMP (RFC1700)

how much overhead with TCP?

- 20 bytes of TCP
- 20 bytes of IP
- = 40 bytes + app layer overhead

19

### IP Datagram Format Options

header length 4 bits (in words of 32 bits)

Min=5 (no options)

Max  $2^{16}-1$  words =  $15 \times 32 \text{ bits} = 60$  bytes

(20 bytes IP header + 40 bytes options)

Options:

- Source route:** specify routers along the way that packet needs to go through
- Record Route:** record all routers visited along the path (40 bytes not enough!!)
- Timestamp:** Each router appends timestamp
- Security:** How "secret" is information (useless, never used)

Options are hardly ever used! (Size is too limited to be useful!)

20

### Questions to Reinforce Understanding

- What's the most data you can send in an IP packet?
- How much application layer data can you send in an IP packet
  - Using TCP?
  - Using UDP?
- What use is the TTL (Time-to-live) field?
- Why discard all packets which fail checksum? Why not try to fix the problem?

21

### IP Fragmentation & Reassembly

fragmentation:

in: one large datagram

out: 3 smaller datagrams

- network links have MTU (max transfer size) - largest possible link-level frame.
  - different link types, different MTUs
    - Ethernet: 1500 bytes
    - FDDI: 4500 bytes
- large IP datagram divided ("fragmented") within net
  - one datagram becomes several datagrams
  - "reassembled" only at final destination (put complexity at end-host)
  - IP header bits used to identify, order related fragments
- IP requires all machines/networks to accept fragments of 576 bytes or less

22

### IP fragmentation

- 16-bit ID identifies all fragments belonging to the same packet
- Flags:
  - 1 bit unused
  - DF (don't fragment)
    - Sender can ask routers not to fragment
  - MF (More Fragments)
    - More fragments for this packet to come
- Fragment offset (13 bits)
  - Position (offset) of start of this fragment in entire packet
  - Expressed in multiple of 8 bytes (all fragments except last one must be multiple of 8 bytes)
  - $(2^{13}) \times 8 \text{ bytes} = 65536 \text{ bytes}$  (one byte more than max size of IP datagram)

23

### Example Network

3 Routers

PD-249

24

### Fragmentation Example

- Example MTUs
  - Ethernet: 1500
  - FDDI: 4500
  - PPP: 532
- What happens if 1420 byte datagram is sent from H1 to H8?

25

### Fragmentation Example (cont.)

26

### Example Header Fields

- For earlier fragmentation example, what will the header fields look like?

27

### Think...

- Why does the size of the last fragment not have to be a multiple of 8?
- What's wrong with sending lots of small packets instead of fewer bigger packets?

28

### IP Addressing

- **IP address:** 32-bit identifier for host, router *interface*
- **interface:** connection between host/router and physical link
  - Routers have multiple interfaces
  - host may have multiple interfaces
  - IP addresses associated with **each interface**
- Dotted decimal notation: 223.1.1.1 =  $\underbrace{11011111}_{223} \underbrace{00000001}_{1} \underbrace{00000001}_{1} \underbrace{00000001}_{1} \underbrace{00000001}_{29}$

29

### IP Addresses – classful addressing

- Hierarchical format (2-level hierarchy):
  - network
  - hosts

Class	Network	Host	Range of host addresses
A	0		1.0.0.0 to 127.255.255.255
B	10		128.0.0.0 to 191.255.255.255
C	110		192.0.0.0 to 223.255.255.255
D	1110		224.0.0.0 to 239.255.255.255
E	11110		240.0.0.0 to 247.255.255.255

T-449



## Subnets (covered in COMP2303)

- Sub-netting is done within an organisation and is transparent to the rest of the Internet
- Routing/forwarding steps
  1. Routers only need to know how to reach the organisation's network, i.e. its router
  2. The network's router then knows how to find the right subnet, i.e. its router
  3. The router of the subnet then finds the destination host
- Routers in step 1 only need to know all networks
- Organisation's main routers (step 2) only need to know all sub-nets
- Sub-net router only needs to know hosts on subnet and Organisation's main router
- Routers in (in step 2 and 3) need to know sub-net mask (not implicitly determined through class)
- Sub-Netmask must be specifically added to routing tables of routers within organisation

37

## Subnet masks

- Mask that removes host-id when ANDed with address
  - Same as Netmask but is extended to mask out sub-net bits as well
  - Notation: 11111111 11111111 11111111 11000000 → /26
- Example address: 130.50.15.6  
Subnet mask: 255.255.252.0
- Destination subnet: \_\_\_\_ . \_\_\_\_ . \_\_\_\_ . \_\_\_\_
- Subnet address is looked up in routing table

38

## Addressing - Subnets

```
marius@mango:~$ ifconfig -a
lo0: flags=1000849<UP,LOOPBACK,RUNNING,MULTICAST,IPv4> mtu 8232 index 1
    inet 127.0.0.1 netmask ff000000
hme0: flags=1000843<UP,BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index 2
    inet 130.102.66.4 netmask ffff0000 broadcast 130.102.67.255
marius@mango:~$
```

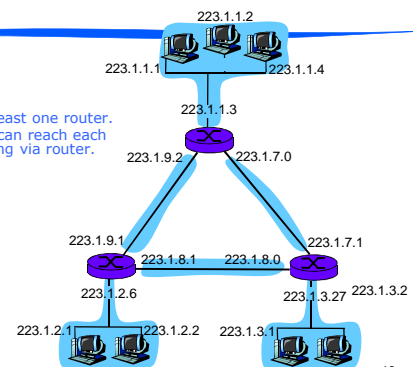
- What class is a loopback address?
- What class is 130.102.66.4 address?
- What's the size of its subnet?
- How many sub-nets can we have?

39

## Subnets

How many?

Each subnet has at least one router.  
Hosts within subnet can reach each other without going via router.



40

## Weaknesses in IP Addressing

- Move host between networks
  - IP address must change
- If class C network grows > 254 hosts
  - Must change to class B address
- Address space is not used effectively
  - Class B networks – too big
  - Class C networks – too small
  - → Shortage of IP addresses

41

## CIDR Classless InterDomain Routing

- CIDR helps do deal with shortage of IP addresses
- Idea: Allocate remaining IP addresses in variable size blocks, without regard to the class
- If a company needs 2000 addresses, it is given a block of 2048 (instead of 64k of a class B network)
- Basically same idea as sub-netting, applied to the whole IP address
- Every routing table entry needs netmask to indicate network part and host part
- This makes forwarding more complicated

42

## CIDR

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

200.23.16.0/23

43

## IP addresses: how to get one?

- Example:
  - ISP has block of addresses: 200.23.16.0/20
    - One network with  $(2^{12} - 2 = 4094)$  hosts
  - ISP divides block into 8 equal sized, contiguous blocks to give to its customers (Organisation 1 - 7)
    - Each block has  $(2^9 - 2 = 510)$  hosts
  - Process is the same as in Sub-netting, but here "subnets" and corresponding netmasks are visible to all Internet routers
  - (Subnet part is underlined, host part is not)

ISP's block	11001000 00010111 00010000 00000000	200.23.16.0/20
Organization 0	11001000 00010111 <u>00010000</u> 00000000	200.23.16.0/23
Organization 1	11001000 00010111 <u>00010010</u> 00000000	200.23.18.0/23
Organization 2	11001000 00010111 <u>00010100</u> 00000000	200.23.20.0/23
...	.....	.....
Organization 7	11001000 00010111 <u>00011110</u> 00000000	200.23.30.0/23

44

## Hierarchical addressing: route aggregation

- Hierarchical addressing allows efficient advertisement of routing information:
- Ability to use a single prefix to advertise multiple networks is called *route aggregation*

45

## Hierarchical addressing: more specific routes

- What happens if addresses are not allocated in contiguous blocks?
- Scenario: Organisation 1 moves to ISPs-R-Us and takes its 200.23.18.0/23 address block to avoid renumbering
- Now ISPs-R-Us advertises two blocks of addresses
- Every Internet router now has 200.23.18.0/23 and 200.23.18./23 advertisement

46

## Longest Prefix Matching

- Based on example in previous Slide, Routing Table Entries in each Internet router:

```

Fly-By-Night ISP
200.23.16.0/20  11001000 00010111 00010000 00000000  Interface 4

ISPs-R-Us: Org 1
200.23.18.0/23  11001000 00010111 00010010 00000000  Interface 3
    
```

The IP packets with the following dest. IP address arrive, where do they get forwarded to?

```

Packet A  11001000 00010111 00010010 00010101
(matches both entries, choose longest match → Interface 3

Packet B  11001000 00010111 00011110 11010101
(matches only first entry → Interface 4)
    
```

47

## IP addresses: how to get one?

**Q:** How does *host* get IP address?

- hard-coded by system admin in a file
  - Wintel: control-panel->network->configuration->tcp/ip->properties
  - UNIX: /etc/rc.config
- **DHCP:** Dynamic Host Configuration Protocol: dynamically get address from as server
  - "plug-and-play"

48

### DHCP

- **Functionality**
  - DHCP server assigns IP addresses
  - Both manual and automatic assignment
  - Each LAN has a DHCP relay agent
- **Operation**
  - Host broadcasts "DHCP DISCOVER" packet
  - DHCP relay agent relays it to DHCP server
  - As IP addresses are usually assigned for fixed time ("leasing") – host has to ask for renewal

49

### IP addressing: the last word...

**Q:** How does an ISP get block of addresses?

**A:** **ICANN**: Internet Corporation for Assigned Names and Numbers

- allocates addresses
- manages DNS
- assigns domain names, resolves disputes

50

### NAT - Network Address Translation

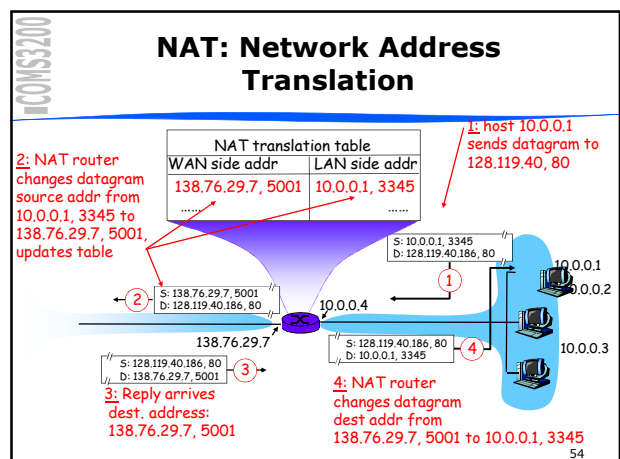
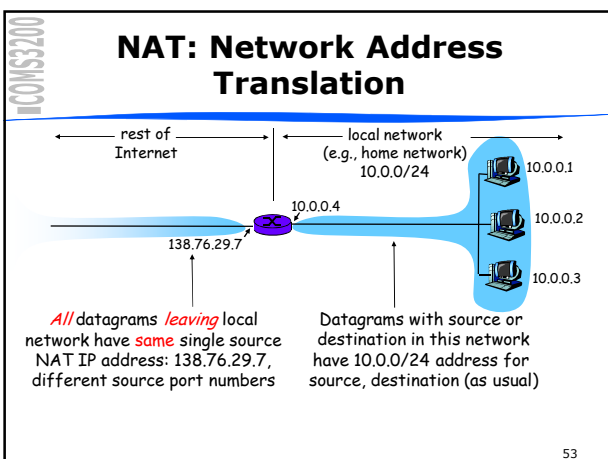
- Another approach to deal with shortage of IP addresses
- Basic idea
  - Assign each company or (home user) a single **public** IP address
  - Use unique, **private** IP addresses within company
  - Change private IP address into company's IP address when packet leaves network
- Three ranges of private IP addresses exist
  - 10.0.0.0/8, 172.16.0.0/12, and 192.168.0.0/16
- Private IP addresses must not appear on Internet

51

### NAT: Network Address Translation

- **Motivation:** local network uses just one IP address as far as outside world is concerned:
  - no need to be allocated range of addresses from ISP: - just one IP address is used for all devices
  - can change addresses of devices in local network without notifying outside world
  - can change ISP without changing addresses of devices in local network
  - devices inside local net not explicitly addressable, visible by outside world (a security plus).

52



### NAT: Network Address Translation (RFC3022)

- 16-bit port-number field:
  - 60,000 simultaneous connections with a single LAN-side address!
- NAT is controversial:
  - routers should only process up to layer 3
  - violates end-to-end argument (e2e significance of IP addresses)
    - NAT possibility must be taken into account by app designers, eg, P2P applications
    - Some applications and protocols assume that all hosts have public IP addresses (e.g. Voice over IP, SIP) → incompatibility with NAT
  - address shortage should instead be solved by IPv6
- With NAT, we can only create outgoing connections/sessions. External host cannot connect to host behind NAT, since there is no NAT entry for this session.
  - Problem for P2P applications, VoIP etc.

55

### ICMP: Internet Control Message Protocol

- used by hosts & routers to communicate network-level information
  - error reporting:
    - unreachable host, network, port, protocol
    - echo request/reply (used by ping)
  - network-layer "above" IP:
    - ICMP msgs carried in IP datagrams
- ICMP message: type, code plus first 8 bytes of IP datagram causing error

Type	Code	description
0	0	echo reply (ping)
3	0	dest. network unreachable
3	1	dest host unreachable
3	2	dest protocol unreachable
3	3	dest port unreachable
3	6	dest network unknown
3	7	dest host unknown
4	0	source quench (congestion control - not used)
8	0	echo request (ping)
9	0	route advertisement
10	0	router discovery
11	0	TTL expired
12	0	bad IP header

56

### Traceroute and ICMP

- Source sends series of UDP segments to dest
  - First has TTL = 1
  - Second has TTL = 2, etc.
  - Unlikely port number
- When nth datagram arrives to nth router:
  - Router discards datagram
  - And sends to source an ICMP message (type 11, code 0)
  - Message includes name of router & IP address
- When ICMP message arrives, source calculates RTT
- Traceroute does this 3 times
- Stopping criterion**
  - UDP segment eventually arrives at destination host
  - Destination returns ICMP "port unreachable" packet (type 3, code 3)
  - When source gets this ICMP, stops.

57

### ICMP – Internet Control Message Protocol

- Used
  - by routers – to report the unexpected
  - for testing the Internet
- More important messages:
  - Destination unreachable – packet undeliverable
  - Time exceeded – TTL field hit 0
    - Used in **traceroute**
  - Parameter problem – invalid header field
  - Source quench – Slow down!
  - Redirect – teach a router geography
  - Echo request – are you alive?
    - Used in **ping**
  - Echo reply – yes I am!

58

### ICMP

- ICMP messages encapsulated in IP datagrams
  - Typical size: 56 bytes
    - 20 bytes IP header
    - 8 bytes ICMP header
    - 28 bytes payload
      - 20 bytes original IP datagram header
      - first 8 bytes of original IP datagram data
  - Why is this payload included?
- Protocol number 1

59

### Addresses on the Network

- Data link layer doesn't understand IP addresses
- Actually need to send info with LAN address
  - e.g. every Ethernet card in the world has unique address (48 bit MAC address)
- How do we map IP addresses to LAN addresses?
  - Static – have a configuration file or table
  - Dynamic – ask over the network

Bytes	7	1	2 or 6	2 or 6	2	0-1500	0-46	4
	Preamble	↑	Destination address	Source address	↑	Data	Pad	Checksum
		Start of frame delimiter			Length of data field			(Figure shown in Lecture 6)

60

## ARP: Address Resolution Protocol

- Example: Host needs to send to 192.31.65.5
  - Sends broadcast packet:
    - "Who owns IP address 192.31.65.5?"
  - ONE reply should come back
- Variations
  - Cache
    - Entries should expire every few minutes
  - Supply own details when make request
  - Broadcast on boot
    - "Who owns my IP address?"

61

## Example

The diagram shows a central Campus FDDI ring with IP 192.31.60.0. It is connected to three Ethernet networks: CS Ethernet (192.31.65.0), EE Ethernet (192.31.63.0), and a WAN. Hosts 1-4 are on the CS and EE networks. Routers F1, F2, and F3 connect these networks to the central ring. Router F2 has two IP addresses: 192.31.60.4 and 192.31.65.1. Router F3 has two IP addresses: 192.31.60.7 and 192.31.63.3.

- Several class C networks (how do we know this?)
- How does an IP packet get from
  - host 1 to 2? host 1 to 4?

62

## IPv6

- **Initial motivation:** 32-bit address space soon to be completely allocated.
- Additional motivation:
  - header format helps speed processing/forwarding
  - header changes to facilitate QoS

**IPv6 datagram format:**

- fixed-length 40 byte main header
- no fragmentation allowed
- Extension headers

63

## IPv6 Main Header

*Priority:* identify priority among datagrams in flow  
*Flow Label:* identify datagrams in same "flow."  
 (concept of "flow" not well defined).  
*Next header:* identify upper layer protocol for data, or optional headers

ver	pri	flow label	
payload len		next hdr	hop limit
source address (128 bits)			
destination address (128 bits)			
data			

← 32 bits →

64

## Extension Headers

Extension header	Description
Hop-by-hop options	Miscellaneous information for routers
Destination options	Additional information for the destination
Routing	Loose list of routers to visit
Fragmentation	Management of datagram fragments
Authentication	Verification of the sender's identity
Encrypted security payload	Information about the encrypted contents

65

## Extension Headers (2)

Next header	0	194	4
-------------	---	-----	---

Jumbo payload length

The hop-by-hop extension header for large datagrams (jumbograms)

Next header	Header extension length	Routing type	Segments left
-------------	-------------------------	--------------	---------------

Type-specific data

The extension header for routing

66

## Other Changes from IPv4

- **Checksum:** removed entirely to reduce processing time at each hop
- **Options:** allowed, but outside of header, indicated by "Next Header" field
- **ICMPv6:** new version of ICMP
  - additional message types, e.g. "Packet Too Big"
  - multicast group management functions

67

## Transition From IPv4 To IPv6

- Not all routers can be upgraded simultaneously
  - no "flag days"
  - How will the network operate with mixed IPv4 and IPv6 routers?
- **Tunneling:** IPv6 carried as payload in IPv4 datagram among IPv4 routers
- It has been more than 10 years since IPv6 has been defined, what happened?
- NAT and CIDR eased IP address shortage
- IPv6 existed as "IPv6 islands"
- However last year many Internet service providers started allocating IPv6 addresses to users

68

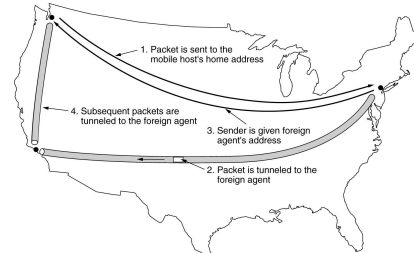
## Mobile IP Protocol

- IP delivers packets between source and destination IP addresses
  - IP address includes network identifier
  - Problem:
    - Mobile computers move between networks – how can packets be delivered to mobile computers?
  - Solution: Mobile IP – mobile computer has two IP addresses
    - Home address,
    - Care-of address
- We will return to Mobile IP next week ...

69

## Mobile IP

### Packet routing in Mobile IP



70

## Summary

- Internet Protocol (IP)
  - Packet formats
  - Fragmentation
  - Addressing
    - Subnets
    - NAT
  - ARP
  - ICMP
  - IPv6
  - Mobile IP

71

## Readings

- Tanenbaum: 5.5, 5.6 (5.6.1, 5.6.2, 5.6.3, 5.6.4), 5.6.9
- (4<sup>th</sup> ed: 5.5, 5.6.1, 5.6.2, 5.6.3 (section on ICMP), 5.6.8)
- Next week: Routing
  - Tanenbaum: pp 362-392 (Routing)
  - pp 474-484 (OSPF, BGP) ← *less important*
- (4<sup>th</sup> ed: pp 350-380 (Routing) 454-461)
  - IGRP: [http://docwiki.cisco.com/wiki/Interior\\_Gateway\\_Routing\\_Protocol](http://docwiki.cisco.com/wiki/Interior_Gateway_Routing_Protocol)

72