CS118 Discussion 1B, Week 6

Zhehui Zhang
HAINES A2 / Friday / 12:00pm-1:50pm

Outline

- Network Layer
  - Overview: data v.s. control plane
  - IPv4/IPv6, DHCP, NAT
- Midterm review

Network layer: overview

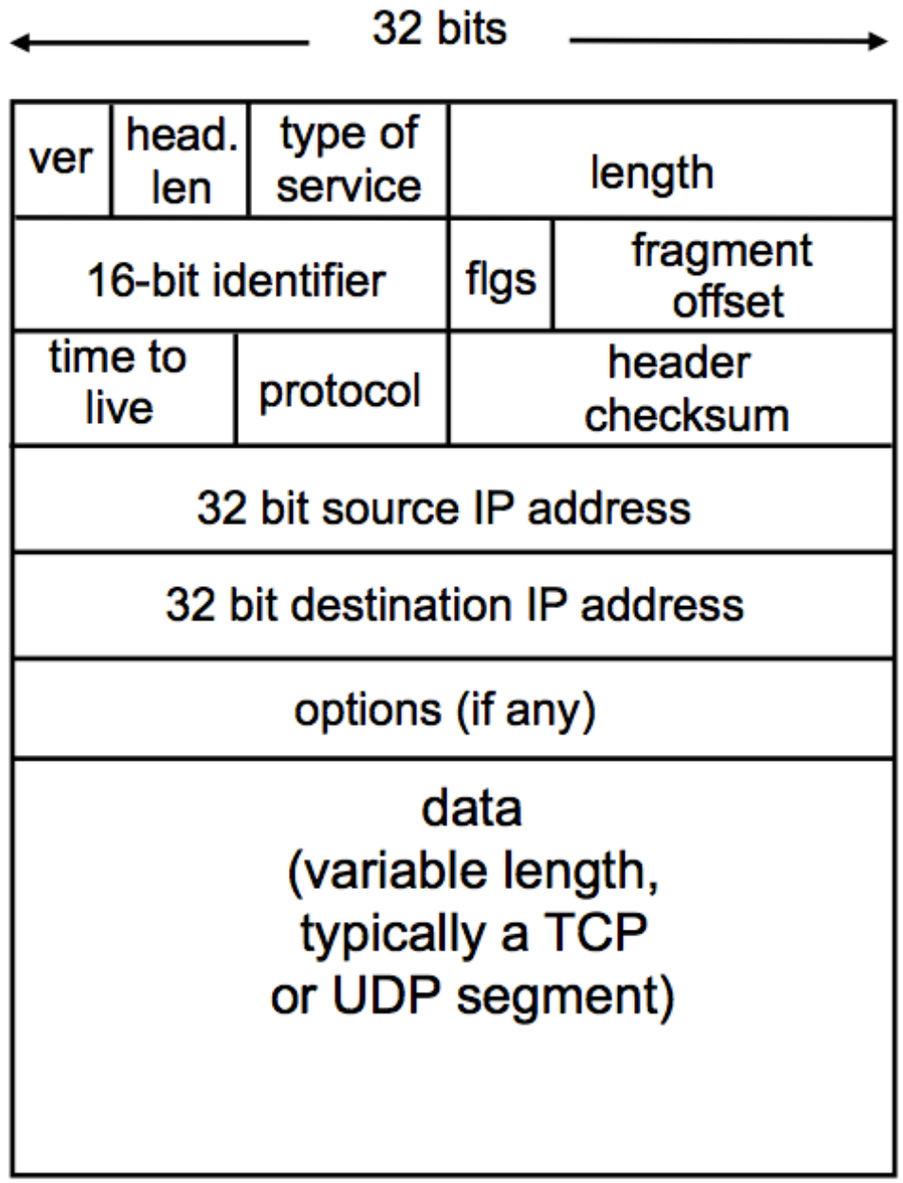
- Basic functions for network layer
  - Forwarding/Routing
- Network service model
  - Guaranteed delivery
  - Guaranteed delivery w/ bounded delay
  - In-order packet delivery
  - Guaranteed minimal bandwidth

Network layer: overview

- Connection v.s. connection-less delivery
  - circuit switch/packet switch
- Network layer protocols
  - Addressing and fragmentation: IPv4, IPv6
  - Routing: RIP, OSPF, BGP, DVMRP, PIM
  - Others: DHCP, ICMP, NAT

IPv4 Header

- **Header length**: 4-byte unit
- **Length**: 1-byte unit
- **Fragmentation**: id + MF/DF + offset (8-byte unit)
- **TTL**: time to live
- **Checksum**
  - Is it redundant?
  - Why is it just checksum for header?
- **Protocol**: identifies the upper layer protocol
- **Source and destination IP addresses**



IP address

- Globally recognizable identifier
- IPv4: 0.0.0.0~255.255.255.255
  - Most IP addresses are globally unique
    - Exception — why?
- Network id, host id
- CIDR address

IP address classes

- http://www.vlsm-calc.net/ipclasses.php

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			

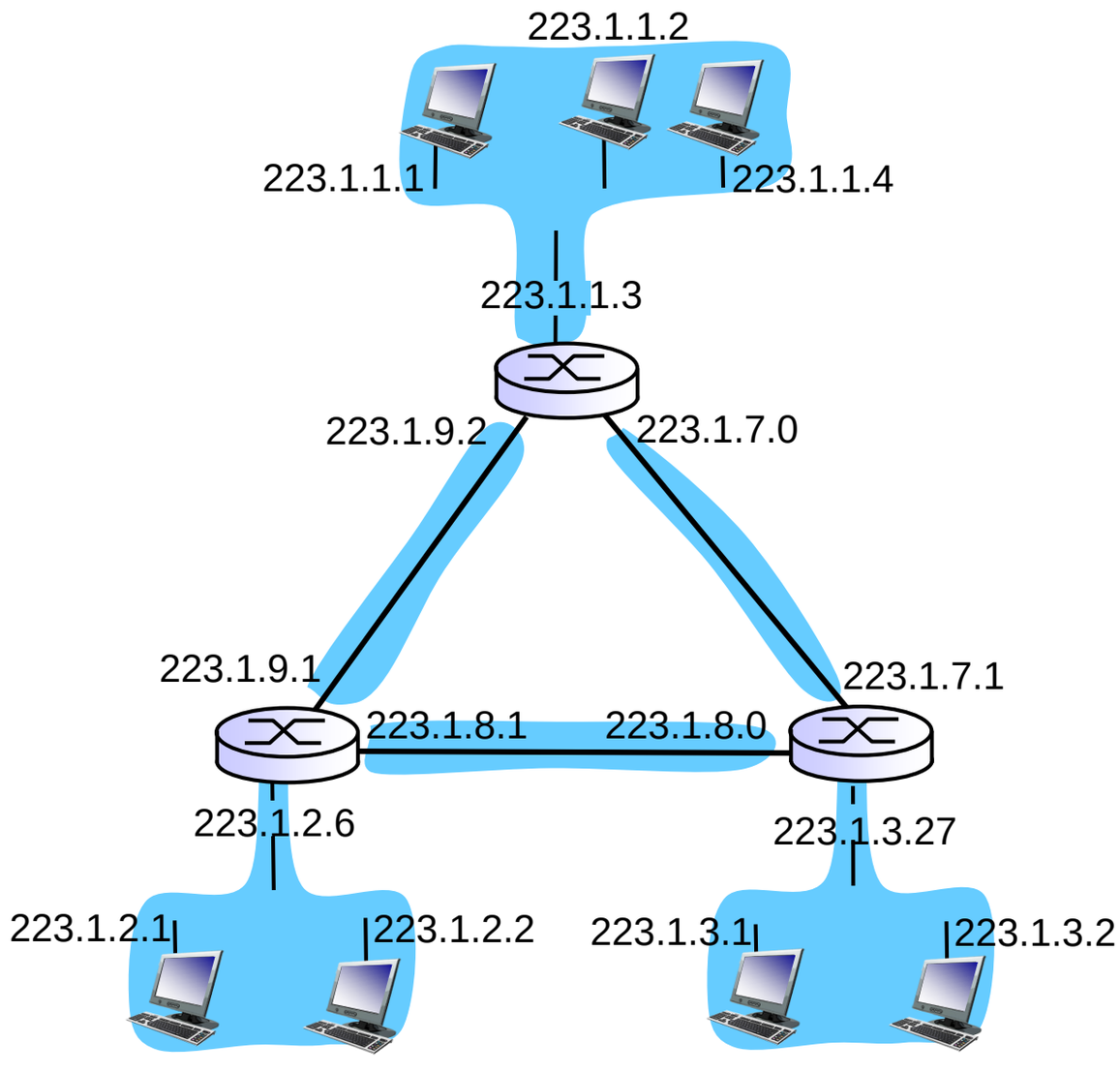
Class	Private Networks	Subnet Mask	Address Range
A	10.0.0.0	255.0.0.0	10.0.0.0 - 10.255.255.255
B	172.16.0.0 - 172.31.0.0	255.240.0.0	172.16.0.0 - 172.31.255.255
C	192.168.0.0	255.255.0.0	192.168.0.0 - 192.168.255.255

Hierarchical addressing

- subnet: a portion of addressing space
  - extend bits from the network id
  - <network address>/<subnet mask>
- route aggregation

Quick question

- How many subnets



CIDR address

- a.b.c.d/x
  - x: # bits in network ID portion of the address
  - address: a.b.c.d, network mask: 2^32 — 2^(32-x)

CIDR 11001000 00010111 00010000 00000000

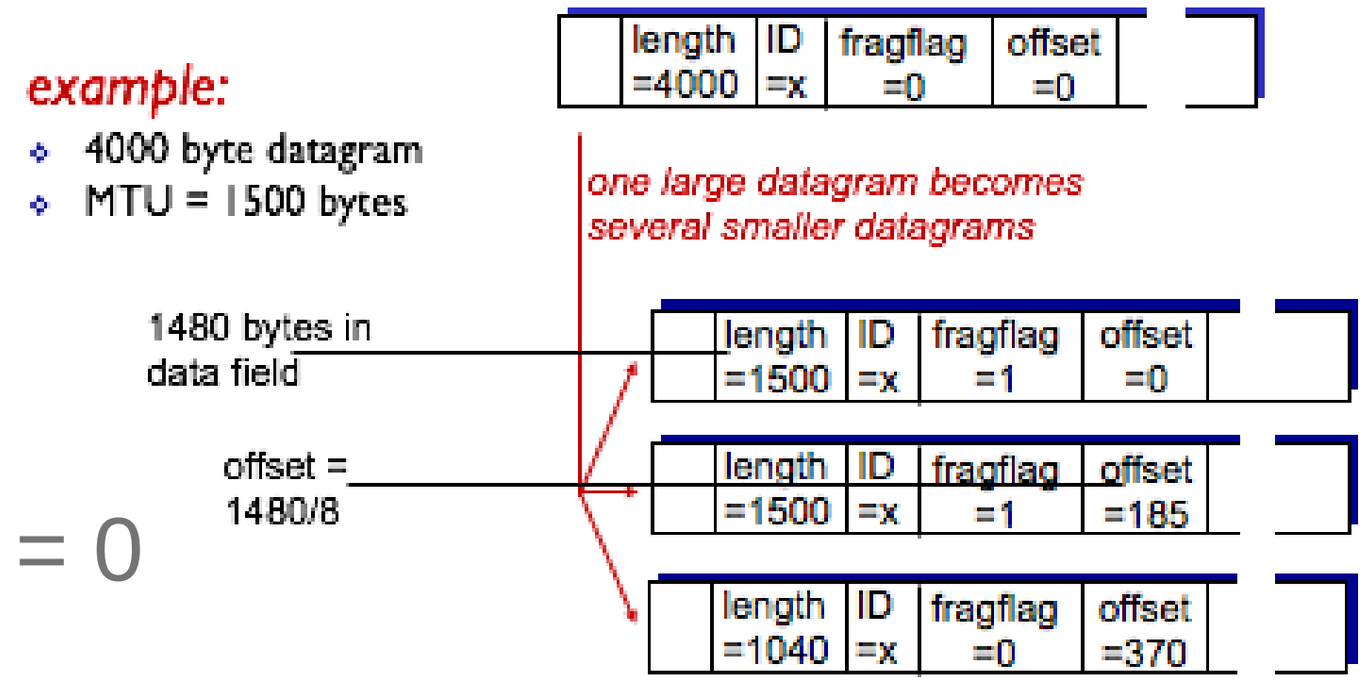
IP prefix 200.23.16.0/23

netmask 11111111 11111111 11111110 00000000

255.255.254.0

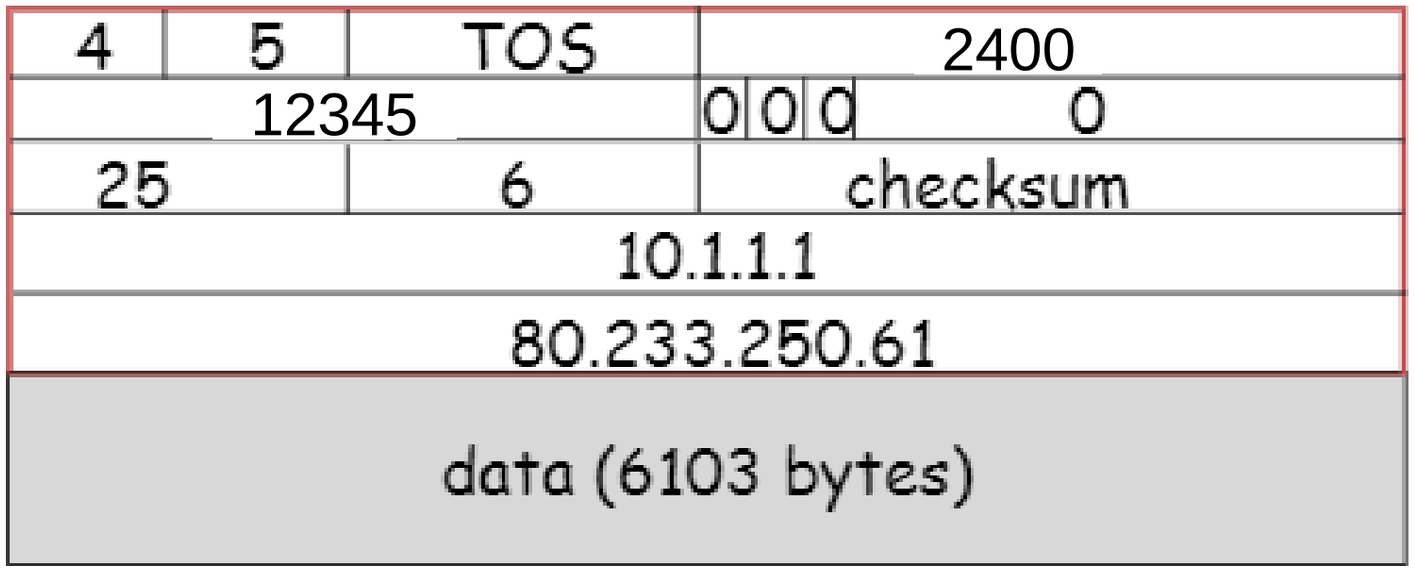
IP fragmentation and reassembly

- MTU: maximum transmission unit
- identifier
- flag bit: three bit
  - DF (Do not Fragment) = 0
  - MF (More Fragments) = 0?
- offset



Quick question

- Consider following IP packet



- Assume MTU = 1450 Bytes. Show the header length, total length, identification, flags, fragment offset, TTL, and IP payload size.

Quick question

- Consider following IP packet

4	5	TOS	2400
12345			0 0 0 0
25		6	checksum
10.1.1.1			
80.233.250.61			

- Assume MTU = 1450 Bytes. Show the header length, total length, identification, flags, fragment offset, TTL, and IP payload size.

For the first packet: 20 bytes, 1444 bytes, ID = 12345, 01, Offset = 0, TTL = 25, 1424 bytes.
For the second packet: 20 bytes, 976 bytes, ID = 12345, 00, Offset = 178, TTL = 25, 956 bytes.

Switching

- Longest prefix matching

Destination Address Range	Link interface
11001000 00010111 00011000 *********	0
11001000 00010111 00010*** *********	1
11001000 00010111 0001**** *********	2
******** ******** ******** ********	3

- Linear lookup

DHCP: Dynamic Host Configuration Protocol

- Dynamically allocates the following info to a host
  - IP address for the host
  - IP address for default router
  - Subnet mask
  - IP address for DNS caching resolver
- Allows address reuse

DHCP: operations

- Host broadcasts “DHCP discovery” msg [optional]
- DHCP server responds with “DHCP offer” msg [optional]
- Host requests IP address: “DHCP request” msg
- DHCP server sends address: “DHCP ack” msg

Important example on Chapter 4 slides 45—46!

NAT (network address translation)

- Depletion of IPv4 addresses — short-term solution
  - IP tunneling?
- Use private IP addresses
- Side-benefit: security
- How to achieve?
  - <public IP:port> — <private IP:port> mapping

NAT: detail

- outgoing packets:
  - replace (source IP address, source port #) of every outgoing packet to (NAT IP address, new port #)
- remote clients/servers will respond using (NAT IP address, new port #) as destination address
- remember (in NAT translation table) every (source IP address, port #) to (NAT IP address, new port #) translation pair
- incoming packets:
  - replace (destination NAT IP address, destination port #) of every incoming packet with corresponding (source IP address, port #) stored in NAT table

NAT: downside

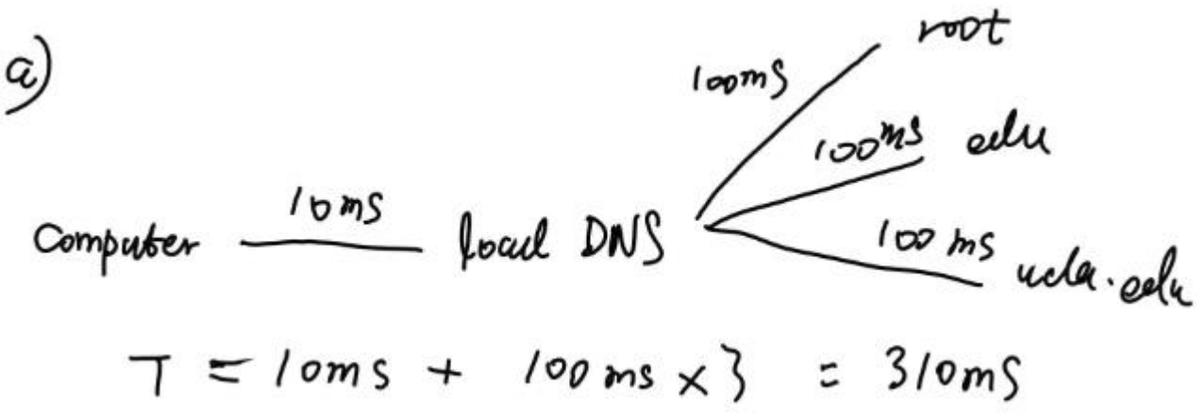
- Increased complexity
- Single point of failure
- Cannot run services inside a NAT box

Midterm tips

- Show intermediate steps
- Explain your answers
- Use diagrams

(a) 10 + 100 + 100 = 210ms

a)



T = 10ms + 100 ms × 3 = 310ms