The Network Layer: IP Addressing

Smith College, CSC 249
March 6, 2008

slides mostly from J.F Kurose and K.W. Ross, copyright 1996-2007

Chapter 4: Network Layer

Chapter goals:

- Understand principles behind network layer services:
  - network layer service models
  - forwarding versus routing
  - how a router works
  - routing (path selection)
- Implementation in the Internet

Key Network-Layer Functions

- 1. *routing:* determine route taken by packets from source to destination
  - *Routing algorithms*
- 2. *forwarding:* move packets from router's input to appropriate router output

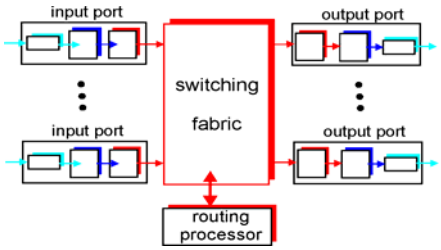
analogy:

- routing: process of planning a car trip from source to destination
- forwarding: process of driving through a single intersection

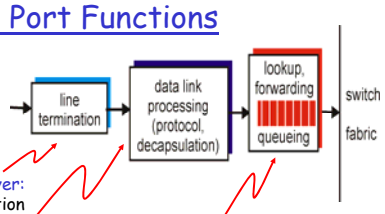
Router Architecture Overview

Two key router functions:

- 1. *run routing algorithms*/protocol
- 2. *forwarding* datagrams from incoming to outgoing link



Input Port Functions



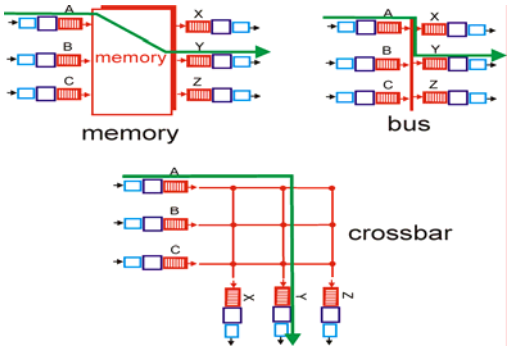
Physical layer:
bit-level reception

Data link layer:
e.g., Ethernet
see chapter 5

Decentralized switching:

- given datagram dest., lookup output port using forwarding table in input port memory
- goal: complete input port processing at 'line speed'
- queuing: if datagrams arrive faster than forwarding rate into switch fabric

Three types of switching fabrics

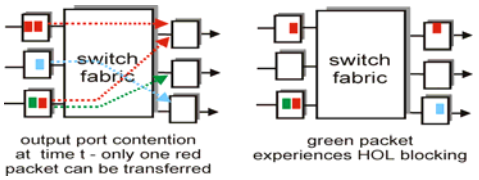


Queuing in Routers

- Where can queuing occur?
- Why does it occur?

Input Port Queuing

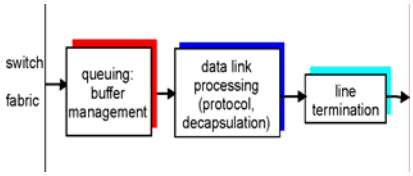
- Switching fabric slower than input ports combined -> queueing may occur at input queues
- Head-of-the-Line (HOL) blocking: queued datagram at front of queue prevents others in queue from moving forward
- *queuing delay and loss due to input buffer overflow*



Queuing in Routers

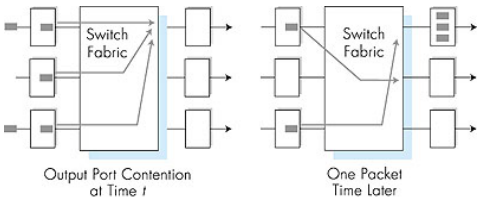
- Where can queuing occur?
- Why does it occur?
- Packet scheduler at the output port
  - Select one queued packet for transmission
    - FCFS
    - Weighted-fair-queuing – share the outgoing link "fairly" among connections

Output Ports



- *Buffering* required when datagrams arrive from fabric faster than the transmission rate
- *Scheduling discipline* chooses among queued datagrams for transmission

Output port queueing

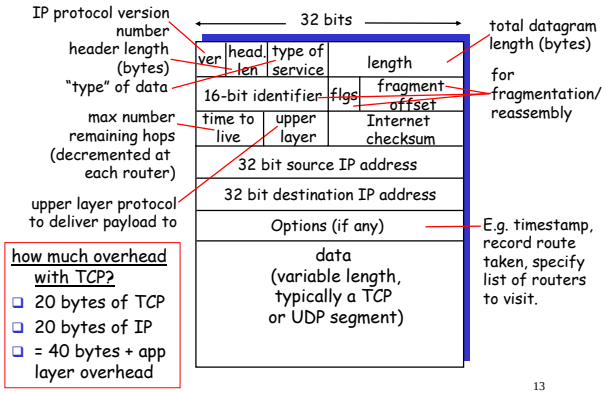


- *queuing (delay) and loss due to output port buffer overflow*

Chapter 4: Network Layer

- 4. 1 Introduction
- 4.2 Virtual circuit and datagram networks
- 4.3 What's inside a router
- 4.4 IP: Internet Protocol
  - Datagram format
  - IPv4 addressing
  - ICMP
  - IPv6
- 4.5 Routing algorithms
  - Link state
  - Distance Vector
  - Hierarchical routing
- 4.6 Routing in the Internet
  - RIP
  - OSPF
  - BGP
- 4.7 Broadcast and multicast routing

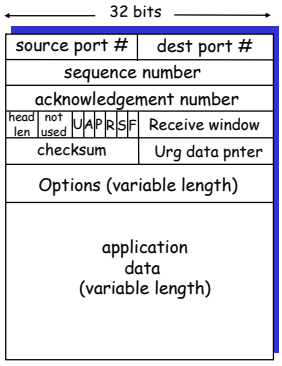
IP datagram format



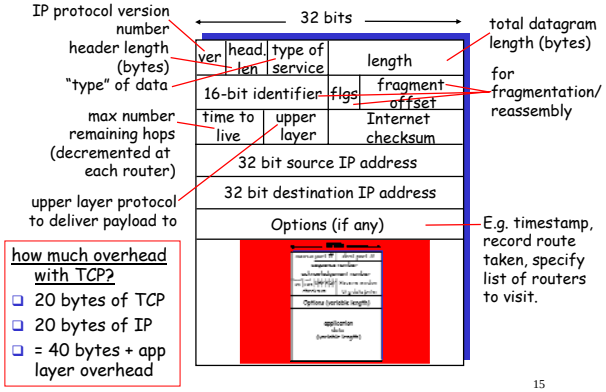
how much overhead with TCP?

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

TCP segment structure



IP datagram format

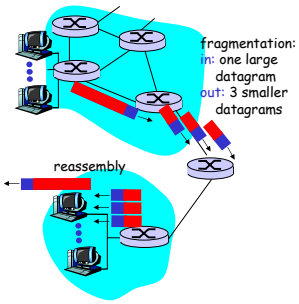


how much overhead with TCP?

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

IP Fragmentation & Reassembly

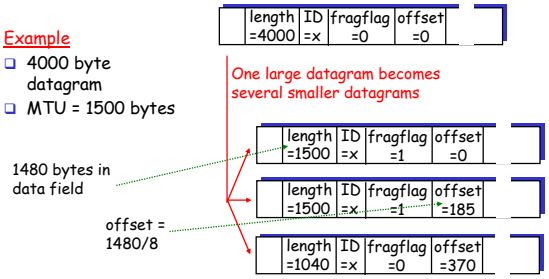
- network links have MTU (max.transfer size) - largest possible link-level frame
  - different link types have different MTUs
- large IP datagram is divided ("fragmented")
  - "reassembled" only at final destination
  - IP header bits used to identify, order related fragments



IP Fragmentation and Reassembly

Example

- 4000 byte datagram
- MTU = 1500 bytes

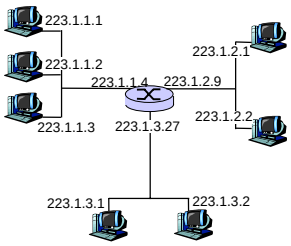


Chapter 4: Network Layer

- 4. 1 Introduction
- 4.2 Virtual circuit and datagram networks
- 4.3 What's inside a router
- 4.4 IP: Internet Protocol
  - Datagram format
  - IPv4 addressing
  - ICMP
  - IPv6
- 4.5 Routing algorithms
  - Link state
  - Distance Vector
  - Hierarchical routing
- 4.6 Routing in the Internet
  - RIP
  - OSPF
  - BGP
- 4.7 Broadcast and multicast routing

IP Addressing: introduction

- IP address: 32-bit identifier for host, router *interface*
- *interface:* connection between host/router and physical link
  - router's typically have multiple interfaces
  - host typically has one interface
  - IP addresses associated with each interface

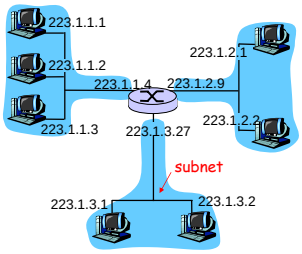


223.1.1.1 = 11011111 00000001 00000001 00000001

223 1 1 1

Subnets

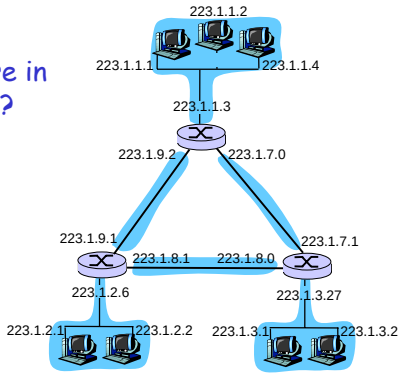
- *What is a subnet ?*
  - Devices that can physically reach each other without an intervening router
- IP address:
  - subnet portion (high order bits)
  - host portion (low order bits)



network consisting of 3 subnets

Subnets

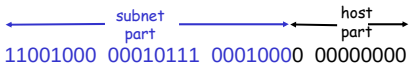
How many are in this figure?



IP addressing: CIDR

CIDR: Classless InterDomain Routing

- 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

IP addresses: how to get one?

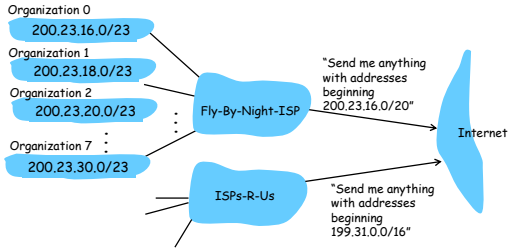
Q: How does *host* get IP address?

- hard-coded by system admin in a file
- DHCP: Dynamic Host Configuration Protocol: dynamically get address from as server
  - "plug-and-play"

Q: How does *network* get subnet part of IP addr?

A: gets allocated portion of its provider ISP's address space

Hierarchical addressing: route aggregation



DHCP: Dynamic Host Configuration Protocol

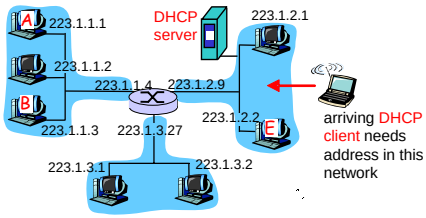
Goal: allow host to *dynamically* obtain its IP address from network server when it joins network

- Can renew its lease on address in use
- Allows reuse of addresses (only hold address while connected an "on")
- Support for mobile users who want to join network (more shortly)

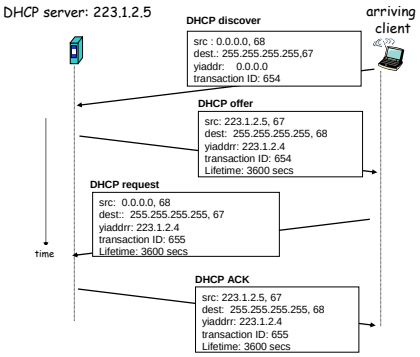
DHCP overview:

- host broadcasts "DHCP discover" msg
- DHCP server responds with "DHCP offer" msg
- host requests IP address: "DHCP request" msg
- DHCP server sends address: "DHCP ack" msg

DHCP client-server scenario



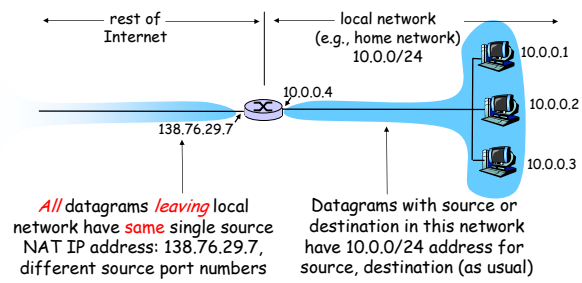
DHCP client-server scenario



NAT: Network Address Translation

- Motivation: local network uses just one IP address as far as outside world view:
  - range of addresses not needed from ISP: just one IP address 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)

NAT: Network Address Translation



Summary Section 4.4

- IP Addressing
  - Class A, B…
  - Subnets
- DHCP – dynamic addressing
- NAT – network address translation
- ICMP – internet control message protocol
  - Ping and Traceroute
- IPv6
  - Overcomes IPv4 flaws, but is hard to compel transition