IP address (continue)

Lecture 14:

Operating Systems and Networks

Behzad Bordbar

recap

- IP address: two parts
- IP address classes

A: 1- 126,B: 128-191, C: 192-223,D: 224- 239
E:240-254 (127, broadcast, network address)

- Mask (both used for identifying Network/host id and telling if destination is on network without intermediate router)
- private IP addresses and NAT
- more than two level of hierarchy (subnet)
- what is the IP address of the subnet?

How to calculate subnet address?

- Given an IP address and a subnet mask calculate the subnet addresses:

Rules:

- if mask 255 corresponding part of the IP address repeated
- if mask 0 corresponding part of the IP address is set to zero
- otherwise bitwise “and” operation
- Example 156.72.56.5 with mask 255.255.200.0
- IP 181 92 56 5
- mask 255 255 200 0

subnet 181 72 8 0

Why 8?

- 56= (0011 1000)
- 200= (1100 1000)
- 0000 1000 which is 8

Classless Inter domain Address (CIDR)

- suppose a company with 1000 machines (say SoCS), what type of IP address should I buy? see slide on classes
- purchase 5 class C address >> must manage multiple address!
- buy a class B address >> 64000 addresses go to waste!
- Solution Classless Interdomain Routing (CIDR) with Variable Length Subnet Masks (VLSM)

CIDR (Continue)

- address form are xy.xyz.xyz/N, when N is the offset (in binary) showing network address
- How many address are there in the CIDR address 192.168.100.0/22 ?
- 192= (1100 0000)
- 168= (1010 1000)
- 100 = (0110 0100)

so the ip address is

1100 0000.1010 1000.0110 0100.0000 0000

^ 22nd digit

- Range is between 00 0000 0000 and 11 1111 1111, which gives total number of 11 1111 1111 +1 = 100 0000 0000 which is 1024 numbers.
- solved the problem of 1000 machine with one address!
- routing table (CIDR routers) modified to have the mask.

how to assign IP address to devices?

- Static: manually add the ip address, network mask and default router (router that this machine is connected to)
- dynamic DHCP A server that has a pool of IP addresses and assigns them to users
- Automated Private IP Addressing APIPA [to produce network stack for applications that fail to work without a network stack]
  - A temporary IP address in the range
    169.254.0.1 to 169.254.255.254
  - if your DHCP server is down or your static ip address is not set correctly.
  - Not publically available addresses.
  - Randomly pick one address.
  - Computers on the same range can speak to each other.
  - But your device can not work with outside world.

IPv6

- permanent solution to shortage of IP address
- 128 bits in hex
- the number that
- 7X10^23 ip addresses per square meter of the earth....
- What is ipv6 google? How about pinging?

$ping6 ipv6.google.com or $host www.go...

Not only larger addresses?

- no fragmentation or checksum to increase routing speed, TCP takes are of this

IPv6 (continue)

- provision for real-time traffic. To ensure QoS (not having jitter throughput…) some packets are marked as *flow* and will be processed faster.
- IPv6 supports anycast
- Security in IPv4 is by authentication and encryption at higher layers. IPV6 pushes the security down to IP. For authentication and payload encryption, header is extended.

For further discussion on IPv6 see Tanenbaum.

router, gateway and all that

- Repeater:
  - extends the physical length of network. Signals can travel fixed distance.
  - don’t change the functionality.
  - produce a refreshed copy of the signal before it becomes too weak.
  - only operate at physical layer.
- Bridge:
  - Divide a large network into smaller segments.
  - used to relay frames between two separate LAN.
  - can have logic to filter network traffic for each segment separate.
  - also do the job of repeaters by regenerating packets and send them to the right segment.
  - can be single port connecting only two segment or multiports… .
  - have a table for directly of packets.
  - can be transparent, they learn and build the table as they dirct the packets.
  - operates both at physical and datalink layer of the OSI model.
  - (due to cheapness of switches bridges are not popular any more)
- Switch: provides bridges functionality with greater efficiency. They act like multiport bridges connecting segments in LAN.

router, gateway and all that

Bridges and repeaters are simple devices

Router:

- relay packets among multiple interconnected networks.
- operate across physical and datalink layer and networklayer.

Gateways:

- operate across all seven OSI layers.
- A router by itself transfers, accepts, and relays packets only across networks using similar protoocls.
- A gateway is a protocol converter. [packets in AppleTalk can be turned into TCP/IP packets before forwarding]
- Gateways are a software installed within a router
- It understands the protocols and adjust the header, datarate, size and format.
- Default gateway is the IP address of a router that a computer uses to go outside its network.
- Draw a picture!

Now that you have learnt

Experiment with your network.

- learn about ping, tcpdump, traceroute, netstat,
- **explore** you IP configuration and your network: ifconfig, iwconfig, iwlist,… what are these?

Knowing your shell programming you can do lots of cool things!

Review of some Protocols

- IP: transfer datagram from one host to another
  - Unreliable best effort
  - only header checksum
- TCP and UDP
  - main transport level protocols used by IP
- MobileIP
  - connectivity for mobile devices, even in transit
  - device retains single IP address
  - re-routing by Home (HA) and Foreign Agents (FA)
  - transparent
- Wireless LAN (IEEE 802.11)
  - radio or infra-red communications
  - CSMA/CA based

IP

- Internet Protocol is unreliable and connectionless
- Best effort (no error checking or Ack)
- Packets called Datagram have Header
  - IP address of source and destination
  - Containing version, Header Length (HLEN), length (Header +data) …
  - higher level protocol ?? (info encapsulated UDP, TCP, RIP2, …)
  - header checksum
  - Fragmentation
  - Timestamp (IP address of the router + Universal time)
- …
- Not all exploited by all higher level protocols

Transport layer protocols

- UDP (basic, used for some IP functions)
  - uses IP address + port number
  - no guarantee of delivery, optional checksum
  - messages up to 64KB
- TCP (more sophisticated, most IP functions)
  - data stream abstraction, reliable delivery of all data
  - messages divided into segments, sequence numbers
  - sliding window, acknowledgement+retransmission
  - buffering (with timeout for interactive applications)
  - checksum (if no match segment dropped)

Both are process-to-process communication

Draw packets!

Communication service types

- Connectionless: UDP
  - 'send and pray' unreliable delivery
  - efficient and easy to implement
- Connection-oriented: TCP
  - with basic reliability guarantees
  - less efficient, memory and time overhead for error correction

Connectionless service

- UDP (User Datagram Protocol)
  - messages possibly lost, duplicated, delivered out of order, without telling the user
  - maintains no state information, so cannot detect lost, duplicate or out-of-order messages
  - each message contains source and destination address
  - may discard corrupted messages due to no error correction (simple checksum) or congestion
- Used e.g. for DNS (Domain Name System) or RIP.

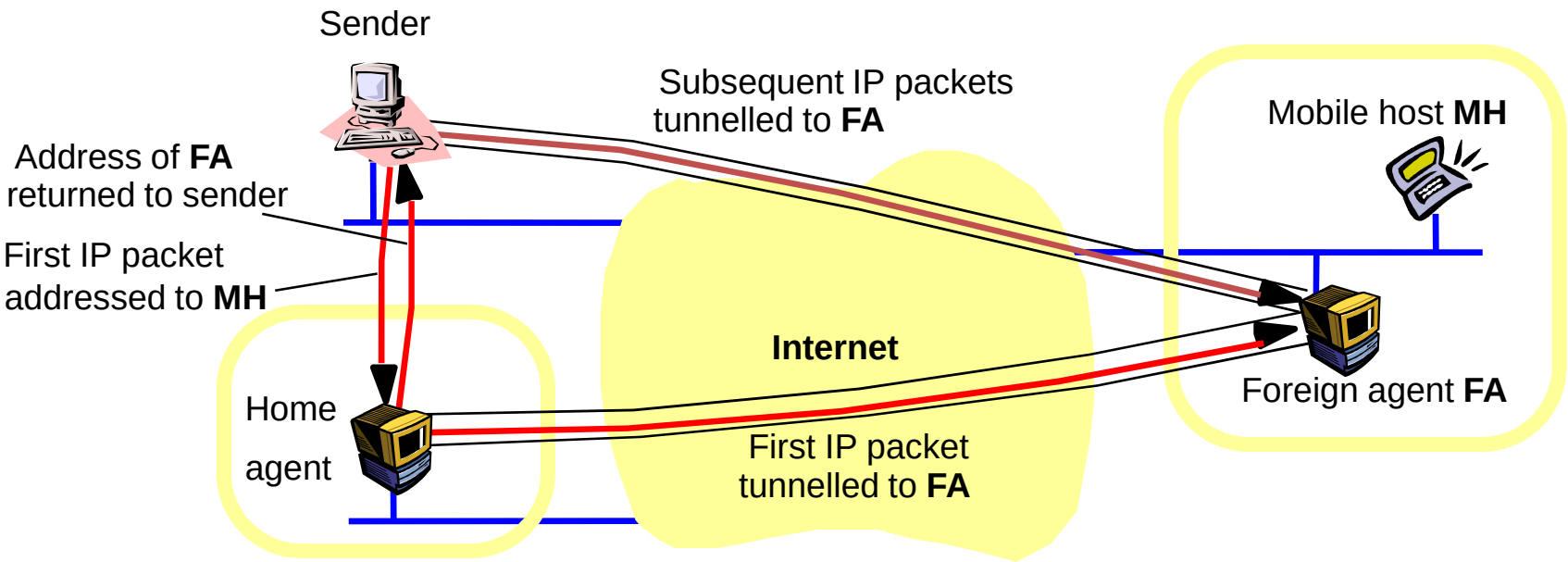
Connection-oriented service

- TCP (Transmission Control Protocol)
  - establishes data stream connection to ensure reliable, in-sequence delivery
  - error checking and reporting to both ends
  - attempts to match speeds (timeouts, buffering)
  - sliding window: state information includes
    - unacknowledged messages
    - message sequence numbers
    - flow control information (matching the speeds)
- Used e.g. for HTTP, FTP, SMTP on Internet.

MobileIP

- At home normal, when elsewhere mobile host:
  - notifies HA before leaving
  - informs FA, who allocates temporary care-of IP address & tells HA
- Packets for mobile host:
  - first packet routed to HA, encapsulated in MobileIP packet and sent to FA (tunnelling)
  - FA unpacks MobileIP packet and sends to mobile host
  - sender notified of the care-of address for future communications which can be direct via FA
- Problems
  - efficiency low, need to notify HA

MobileIP routing



Wireless LAN (802.11)

- Radio broadcast (fading strength, obstruction)
- Collision avoidance by
  - slot reservation mechanism by Request to Send (RTS) and Clear to Send (CTS)
  - stations in range pick up RTS/CTS and avoid transmission at the reserved times
  - collisions less likely than Ethernet since RTS/CTS short
  - random back off period
- Problems
  - security (eavesdropping), use shared-key authentication