CS 456 Hao Pan
Salahuddin, Mohammad
Spring 2018

Chapter 4.3 IP: Internet Protocol

4.3.1 IP Fragmentation and Reassembly

- Network links have a *max transfer size (MTU)*, the largest possible link-level frame that can be sent.
- Large IP datagrams are divided within the let such that one datagram becomes several. IP header bits are used to identify and order these fragments. They are only reassembled at the final destination.

4.3.2 IP Addressing

4.3.2.1 Introduction

- An **IP address** is a 32-bit identifier for host and router interface.
- The **interface** is a connection between the host/router and a physical link. Routers tend to have multiple interfaces while a host only has one or two.
- The IP address is associated with each interface.

4.3.2.2 Subnets

- The IP address consists of:
  - **Subnet part** - high order bits
  - **Host part** - low order bits
- Device interfaces with the same **subnet** part of their IP address can physically reach each other without an intervening router.

4.3.2.3 Classless InterDomain Routing (CIDR)

- The subnet portion of an address has arbitrary length.
- In the address with format: $a.b.c.d/x$, x is the number of bits in the subnet portion of an address.

4.3.2.4 How to get an IP Address

- The IP address is usually hard-coded by system admins in a file.
  - In Windows, the IP address is in: control panel→network→configuration→tcp/ip→properties
  - In UNIX, it is in /etc/rc.config
- **Dynamic Host Configuration Protocol (DHCP)** is used to dynamically get the address from an as server.
- The network gets the subnet part of an IP address from the ISP. The ISP allocates a portion of its address space for the network.
- The ISP can get a block of addresses from *I*nternet Corporation for Assigned Names and Numbers (ICANN). ICANN is responsible for allocating addresses, managing DNS, assigning domain names, and resolving disputes.

4.3.3 Dynamic Host Configuration Protocol (DHCP)

- The *goal* is to allow hosts to dynamically obtain its IP address from a network server when it joins the network.
- The host can renew its lease on the address it's using, or it can reuse its address (only hold the address while connected).
-
- Overview:
  - Host optionally broadcasts a *"DHCP discover"* message.
  - DHCP server optionally responds with a *"DHCP offer"* message.
  - Host requests an IP address by sending a *"DHCP request"* message.
  - DHCP server sends address using a *"DHCP ack"* message.
- DHCP can return more than just the allocated IP address. It can also return:
  - The address of the first-hop router for client.
  - The name and IP address of the DNS server.
  - The network mask, which indicates the network vs. host portion of the address.

4.3.4 Hierarchial Addressing

- Hierarchial addressing allows efficient advertising of routing information. A visual can be seen on **slide 4-42**.
- Some ISPs may use more specific routes to organizations, as shown on **slide 4-43**.

4.3.5 Network Address Translation (NAT)

- All datagrams leaving local networks have the same source NAT IP address, but different source port numbers.
- A local network uses only one IP address, as seen from the outside word. A range of IP addresses is not needed from the ISP. One IP address can be used for all devices.
- The address of local devices can be changed without notifying the outside world.
- The ISP can be changed without changing the addresses of devices in the local network.
- Devices in side the local net are not explicitly addressable by the outside world. This is an extra security feature.
- A NAT router must:
  - Replace (source IP address, port number) of every outgoing datagram to (NAT IP address, new port number).
  - Remember every source (IP address, port number) to (NAT IP address, new port number) translation pair.
  - Replace (NAT IP address, new port number) in destination fields of every incoming datagram with corresponding (source IP address, port number) stored in the NAT table.
- See example process of NAT router on **slide 4-48**.
- NAT is controversial because:
  - Routers should only process up to layer 3.
  - Address shortage should be solved by IPv6.
  - Violates end-to-end argument, since NAT possibility must be taken into account by app designers.
  - NAT traversial becomes more compicated if the client wants to connect to the server behind NAT.

4.3.6 IPv6

4.3.6.1 Motivation

- 32-bit address space will soon be completely allocated.
- In addition, using a header format helps to speed up processing an forwarding, as well as helping to facilitate QoS.

4.3.6.2 Datagram Format

- **Priority**: Identified among datagrams in flow.
- **Flow label**: Identify datagrams in the same ”flow”.
- **Next header**: Identify upper layer protocol for data.

4.3.6.3 Changes from IPv4

- **Checksum** has been removed to reduce processing time at each hop.
- **Options** are allowed, but are outside of the header. They are indicated by a ”Next Header” field.
- **ICMPv6**, a new version of ICMP, which supports new message types (ex. *”Packet Too Big”*), and multicast group management functions.

4.3.6.4 Transition from IPv4 to IPv6

- Not all routers can be upgraded simultaneously. Thus, the network must learn to operate with mixed IPv4 and IPv6 routers.
- **Tunneling** IPv6 datagrams can be carried as **payload** in IPv4 datagram among IPv4 routers.