Lecture 14: NAT and Routing
Lecture 14 Overview

- What to do when you run out of names
- Introduction to routing
Private Address Space

- Sometimes you can’t get/don’t want IP addresses
  - An organization wants to change service providers without having to renumber its entire network
  - A network may be unable obtain (or cannot afford) enough IP addresses for all of its hosts

- IP provides **private address space** anyone can use
  - 10/8, 192.168/16, 172.16.0/20
  - These addresses are not routable—Internet routers should drop packets destined to these so-called **bogons**

- What good are they if can’t use them on the Internet?
Gateway router can rewrite IP addresses as packets leave or enter a given network

- I.e., replace private addresses with public ones
- Router needs to see and update every packet

Maintains a mapping of private-to-public addresses

- Simple case is a one-to-one mapping
- Anytime you change provider, just update mapping table
- In more clever scenarios, can map a larger set of private addresses to a smaller set of public addresses
- In the extreme map the entire private network to one public IP!
A.K.A. Network Address [and port] Translation (NAT), Port Address Translation (PAT), or, colloquially, just NAT.

Entire local network uses just one IP address as far as outside world is concerned:
- 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).
A NAT’d Network

All packets leaving local network have same single source NAT IP address: 138.76.29.7

Packets with source or destination in this network have 10.0.0.0/8 address for source, destination (as usual)

rest of Internet

local network (e.g., home network) 10.0.0.0/8

138.76.29.7

10.0.0.1

10.0.0.2

10.0.0.3

10.0.0.4

How do you figure out what traffic is for each host behind the NAT?
NAT’s hack: use port numbers!

2: NAT router changes packet source addr from 10.0.0.1:3345 to 138.76.29.7:5001, updates table

NAT translation table

<table>
<thead>
<tr>
<th>WAN side addr</th>
<th>LAN side addr</th>
</tr>
</thead>
<tbody>
<tr>
<td>138.76.29.7:5001</td>
<td>10.0.0.4:3345</td>
</tr>
<tr>
<td>......</td>
<td>......</td>
</tr>
</tbody>
</table>

1: host 10.0.0.4 sends packet to 132.239.8.45:80

3: Reply arrives dest. address: 138.76.29.7:5001

4: NAT router changes packet dest addr from 138.76.29.7:5001 to 10.0.0.4:3345
NAT Challenges

- End hosts may not be aware of external IP address
  - Some applications include IP addresses in application data
  - Packets will contain private IP addresses inside payload
  - Many NATs will inspect/rewrite certain protocols, e.g., FTP

- NAT’d end hosts are not reachable from the Internet
  - All connections must be initiated from within private network
  - Alternative is to configure fixed forwarding in NAT
  - Many protocols for NAT traversal to get around this
Introduction to Routing

- **Forwarding**
  - Move packet from input link to the appropriate output link
  - Purely local computation
  - Must go be very fast (executed for every packet)

- **Routing**
  - Make sure that the next hop actually leads to the destination
  - Global decisions; distributed computation and communication
  - Can go slower (only important when topology changes)
Forwarding Options

- **Source routing**
  - Complete path listed in packet

- **Virtual circuits**
  - Set up path out-of-band and store path identifier in routers
  - Local path identifier in packet

- **Destination-based forwarding**
  - Router looks up address in forwarding table
  - Forwarding table contains (address, next-hop) tuples
Routing

- Host computes path
  - Must know global topology and detect failures
- Packet contains complete ordered path information
  - I.e. node A then D then X then J...
- Requires variable length path header

Forwarding

- Router looks up next hop in packet header, strips it off and forwards remaining packet
  - Very quick forwarding, no lookup required

In practice

- ad hoc networks (DSR), some HPC networks (Myrinet), and for debugging on the Internet (LSR, SSR)
Virtual Circuits

- **Routing**
  - Hosts sets up path out-of-band, requires connection setup
  - Write (input id, output id, next hop) into each router on path
  - Flexible (one path per flow)

- **Forwarding**
  - Send packet with path id
  - Router looks up input, swaps for output, forwards on next hop
  - Repeat until reach destination
  - Table lookup for forwarding (why faster than IP lookup?)

- **In practice**
  - ATM: fixed VC identifiers and separate signaling code
  - MPLS: ATM meets the IP world (why? traffic engineering)
For next time…

- Project 2 due tonight at midnight pacific time

- Study for the Midterm
  - **Midterm will by async:** 1 hour to complete after you start, and available online for 24 hours
  - Exam covers everything up to Monday’s lecture
  - Homework 1 and 2 solutions posted on Piazza and website

- Read Chapter 3.4 in P&D