Lecture 13: NAT and Routing

CSE 123: Computer Networks
Aaron Schulman

UCSD CSE
Lecture 13 Overview

- Wrap up discussion of naming
- Overview of routing
- Intra vs. Inter-domain routing
- Link-state routing protocols
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?
Network Address Translation

- 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 network changes provider, just update mapping table
  - In more clever scenarios, can map a set of private addresses to a smaller set of public addresses
  - In the extreme map the entire private network to one public IP!
IP Masquerading

- A.K.A. Network Address and port Translation (NAP), 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, different source port numbers

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

1: host 10.0.0.4 sends packet to 132.239.8.45:80

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

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 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>

CSE 123 – Lecture 12: Naming
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
Router Tasks

- **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*)
Destination-based Forwarding

- **Routing**
  - All addresses are globally known
    - No connection setup
  - Host sends packet with destination address in header
    - No path state; only routers need to worry about failure
  - Distributed routing protocol used to routing tables

- **Forwarding**
  - Router looks up destination in table
    - Must keep state proportional to destinations rather than connections
  - Lookup address, send packet to next-hop link
    - All packets follow same path to destination

- In Practice: IP routing
The routing table at A, lists – at a minimum – the next hops for the different destinations

<table>
<thead>
<tr>
<th>Dest</th>
<th>Next Hop</th>
</tr>
</thead>
<tbody>
<tr>
<td>B</td>
<td>B</td>
</tr>
<tr>
<td>C</td>
<td>C</td>
</tr>
<tr>
<td>D</td>
<td>C</td>
</tr>
<tr>
<td>E</td>
<td>E</td>
</tr>
<tr>
<td>F</td>
<td>F</td>
</tr>
<tr>
<td>G</td>
<td>F</td>
</tr>
</tbody>
</table>
Routing on a Graph

- Essentially a graph theory problem
  - Network is a directed graph; routers are vertices
- Find “best” path between every pair of vertices
  - In the simplest case, best path is the shortest path
Routing Challenges

- How to choose best path?
  - Defining “best” can be slippery

- How to scale to millions of users?
  - Minimize control messages and routing table size

- How to adapt to failures or changes?
  - Node and link failures, plus message loss
Routing within a network/organization
- A single administrative domain
- The administrator can set edge costs

Overall goals
- Provide intra-network connectivity
- Adapt quickly to failures or topology changes
- Optimize use of network resources

Non-goals
- Extreme scalability
- Lying, and/or disagreements about edge costs
For next time…

• Read Chapter 3.3.2 in P&D