Lecture 13
More IP

Peter Steenkiste
School of Computer Science
Carnegie Mellon University

15-441 Networking, Spring 2006
http://www.cs.cmu.edu/~prs/15-441

Coming Attractions

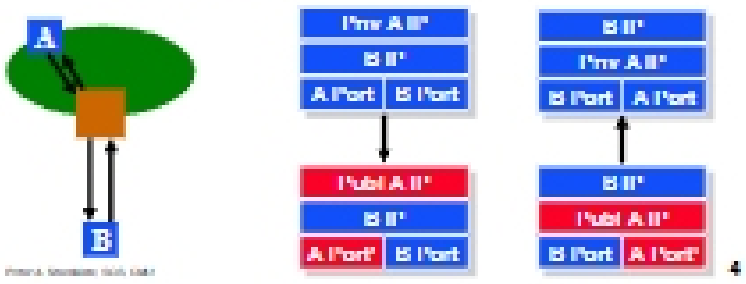
- Project 2 is due Thursday evening ...
- Mid-semester grades will be based on the two homeworks, project 1, and the midterm
- Project 3 will be handed out the 2nd week after Spring break and will be due the 6th week after Spring break, i.e. one week before the last day of classes.
- We will also have ~3 more homeworks.
  - At least one will be hands-on lab

Outline

- NAT.
- Tunnelling.
- IPv6.
- SNMP.
- IP multicast.

Network Address Translation
NAT

- NAT maps (private source IP, source port) onto (public source IP, unique source port)
  - reverse mapping on the way back
  - destination host does not know that this process is happening
- Very simple working solution.
  - NAT functionality fits well with firewalls



NAT Considerations

- NAT translation must be consistent during a session.
  - Set up mapping at the beginning of a session and maintain it during the session
  - Recycle the mapping that the end of the session
- Must determine the end of "sessions" so entries can be retired.
  - Relatively easy for TCP (but be careful about retransmissions)
  - Harder for UDP since NAT does not "understand" protocol
  - Typically uses a timer based mechanism
- NAT has to be consistent with other protocols.
  - ICMP, routing, ...
- Many flavors of NAT exist.
  - Basic, network address port translation (NAPT), bi-directional,..

NAT Challenges

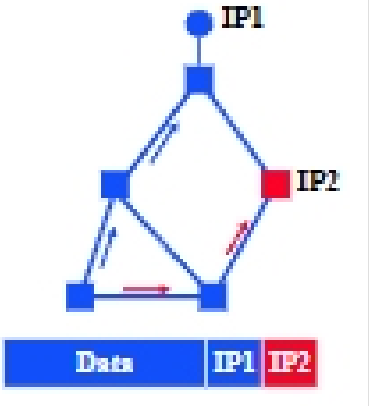
- NAT breaks the basic IP-based connection model used in the Internet.
- NAT creates problems for certain classes of applications.
  - E.g., applications that pass IP information in payload
- Solution is to make NAT aware of these protocols.
  - Unfortunately this only works for standard protocols, e.g. special support for FTP in NATs
- NATs continue to be a problem for some applications, e.g. peer-to-peer applications.
  - Has results in the development of lots of tricks to punch holes through NATs

Outline

- NAT.
- Tunnelling.
- IPv6.
- SNMP.
- IP multicast.

Tunneling

- Force a packet to go to a specific point in the network.
  - Path taken is different from the regular routing
- Achieved by adding an extra IP header to the packet with a new destination address.
  - Similar to putting a letter in another envelop
  - preferable to using IP source routing option
- Used increasingly to deal with special routing requirements or new features.
  - Mobile IP,..
  - Multicast, IPv6, research, ..

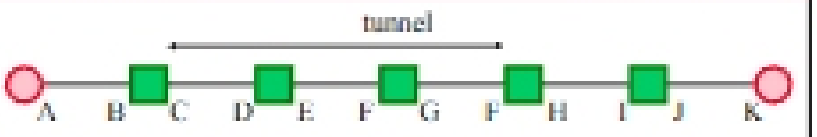


IP-in-IP Tunneling

- Described in RFC 1853.
- IP source and destination address identify tunnel endpoints.
- Protocol Id = 4.
  - IP
- Several fields are copies of the inner-IP header.
  - TOS, some flags, ..
- Inner header is not modified, except for decrementing TTL.

VIHL	TOS	Length
ID		Flags/Offset
TTL	4	H. Checksum
Tunnel Entry IP		
Tunnel Exit IP		
VIHL	TOS	Length
ID		Flags/Offset
TTL	Prot.	H. Checksum
Source IP address		
Destination IP address		
Payload		

Tunneling Example



Tunneling Considerations

- Tunnels are currently standardized.
  - Some diversity in initial implementations
  - Early versions sometimes merged with multicast code
- Performance.
  - Tunneling adds (of course) processing overhead
  - Tunneling increases the packet length, which may cause fragmentation
    - Big hit in performance in most systems
    - Tunneling in effect reduces the MTU of the path, but end-points may not know this
- Security issues.
  - Should verify both inner and outer header
  - Tunneling often used with "IP sec" – see Security lectures

Tunneling Applications

- Virtual private networks.
  - Connect subnets of a corporation using IP tunnels
  - Often combined with IP Sec
- Support for new or unusual protocols.
  - Routers that support the protocols use tunnels to "bypass" routers that do not support it
  - E.g. multicast
- Force packets to follow non-standard routes.
  - Routing is based on outer-header
  - E.g. mobile IP

Outline

- NAT.
- Tunnelling.
- IPv6.
- SNMP.
- IP multicast.

IP v6

- "Next generation" IP.
- Most urgent issue: increasing address space.
  - 128 bit addresses
- Simplified header for faster processing.
- Many other changes.
- Support for guaranteed services: priority and flow id
- Options handled as "next header"
  - reduces overhead of handling options

IPv6 Addressing

- 128 bit addresses with complex structure.
- Examples: format for local configuration, IPv4 backwards compatible, ..
- Provider-based unicast addressing extends the format used in IPv4 with CIDR.
  - Eventually supposed to be the primary addressing model

Migration from IPv4 to IPv6

- Interoperability with IP v4 is necessary for gradual deployment.
- Two complementary mechanisms:
  - dual stack operation: IP v6 nodes support both address types
  - tunneling: tunnel IP v6 packets through IP v4 clouds
- Alternative is to create IPv6 islands, e.g. corporate networks, ...
  - Use of form of NAT to connect to the outside world
  - NAT must not only translate addresses but also translate between IPv4 and IPv6 protocols

IPv6 Discussion

- Unfortunately there is little motivation for any one organization to move to IP v6.
  - the challenge is the existing hosts (using IPv4 addresses)
  - little benefit unless one can consistently use IPv6
    - can no longer talk to IPv4 nodes directly
- People have continued to improve the IPv4 infrastructure.
  - stretching address space through address translation seems to work reasonably well
  - New standards, e.g. IP Sec, diff serv, ..
- Networking increasingly supports IPsec.

Outline

- NAT.
- Tunnelling.
- IPv6.
- SNMP.
- IP multicast.