CPSC 317 COMPUTER NETWORKING

Module 6: Network Address Translation (NAT)

READING

- Reading: 4.3.4

OUR WORST NETWORK NASTY TRICK

- We should have run out of IP addresses
  - Last addresses allocated by IANA on 31 January 2011
  - Regional Internet Registries allocated their last addresses on:

RIR	Date
APNIC	15 April 2011
LACNIC	10 June 2014
ARIN	24 September 2015
AFRINIC	21 April 2017
RIPE NCC	25 November 2019

TWO CHOICES

- Actually switch to IPv6
- Play games with IPv4 addresses pretending that we have more than we actually have
  - Increasing complexity
  - Ignoring layering
  - Breaking abstraction
  - Providing partial functionality

WHICH ONE DID WE CHOOSE?

- Actually switch to IPv6
- Play games with IPv4 addresses pretending that we have more than we actually have
  - Increasing complexity
  - Ignoring layering
  - Breaking abstraction
  - Providing partial functionality

HERE'S THE ARGUMENT

- We have run out of IPv4 addresses
- Do you actually need a globally unique address?
- What would other hosts need your address for?
  - Do other hosts initiate a connection to your host?
    - Rarely
  - Most connections target servers "out there" in the Internet
- Maybe several hosts could share an IP address!

REMEMBER THOSE NON-ROUTABLE IP ADDRESSES?

- Some addresses can never be advertised publically
  - Initially used only for local communication (no Internet connection)
- Networks:
  - 10.0.0.0/8 (16 million addresses)
  - 172.16.0.0/12 (1 million addresses)
  - 192.168.0.0/16 (65,536 addresses)
  - Carrier-grade NAT: 100.64.0.0/10 (4 million addresses)

HERE'S THE IDEA

- All the hosts in a network (your house) share a single IP address
  - The address is "owned" by the edge router (cable modem, etc.)
    - The one that attaches to your ISP
  - All other hosts in the network (your house) get a private network address
- We play games with IP addresses as datagrams pass through your edge router

NETWORK ADDRESS TRANSLATION (NAT)

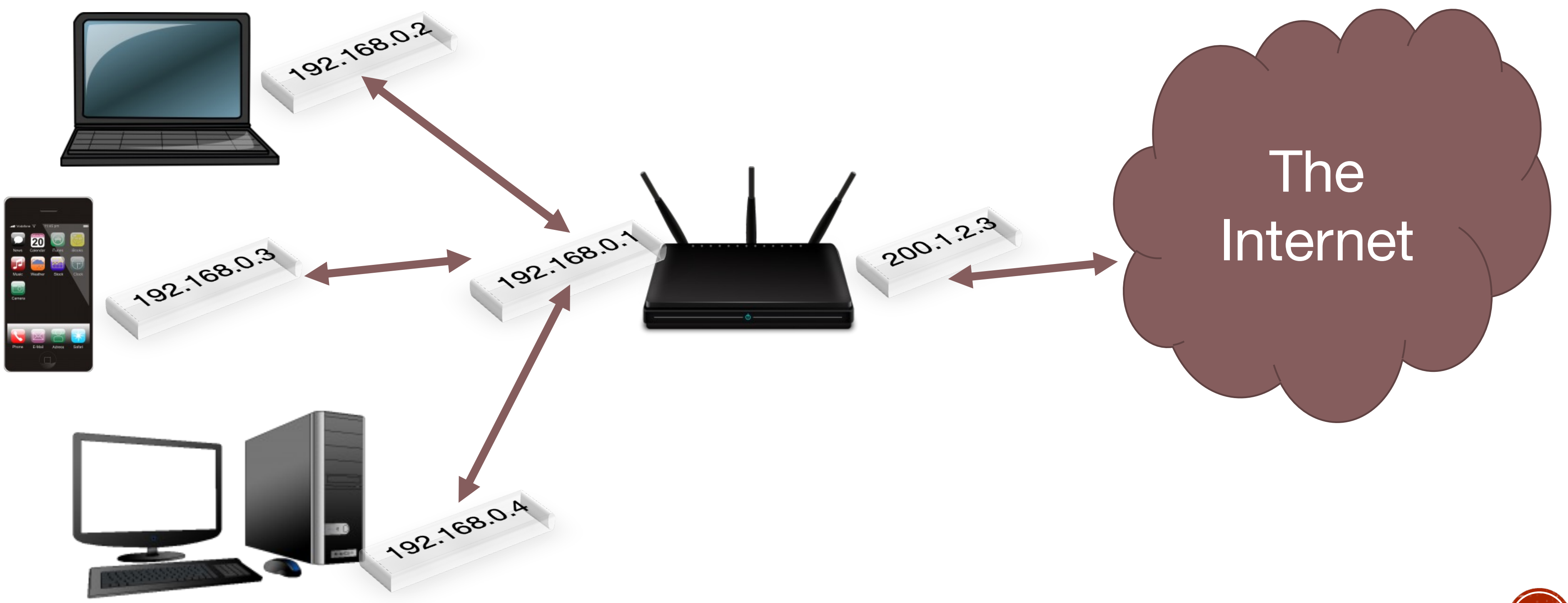
From now on, we'll call that edge router in your house a NAT router

LEARNING GOALS

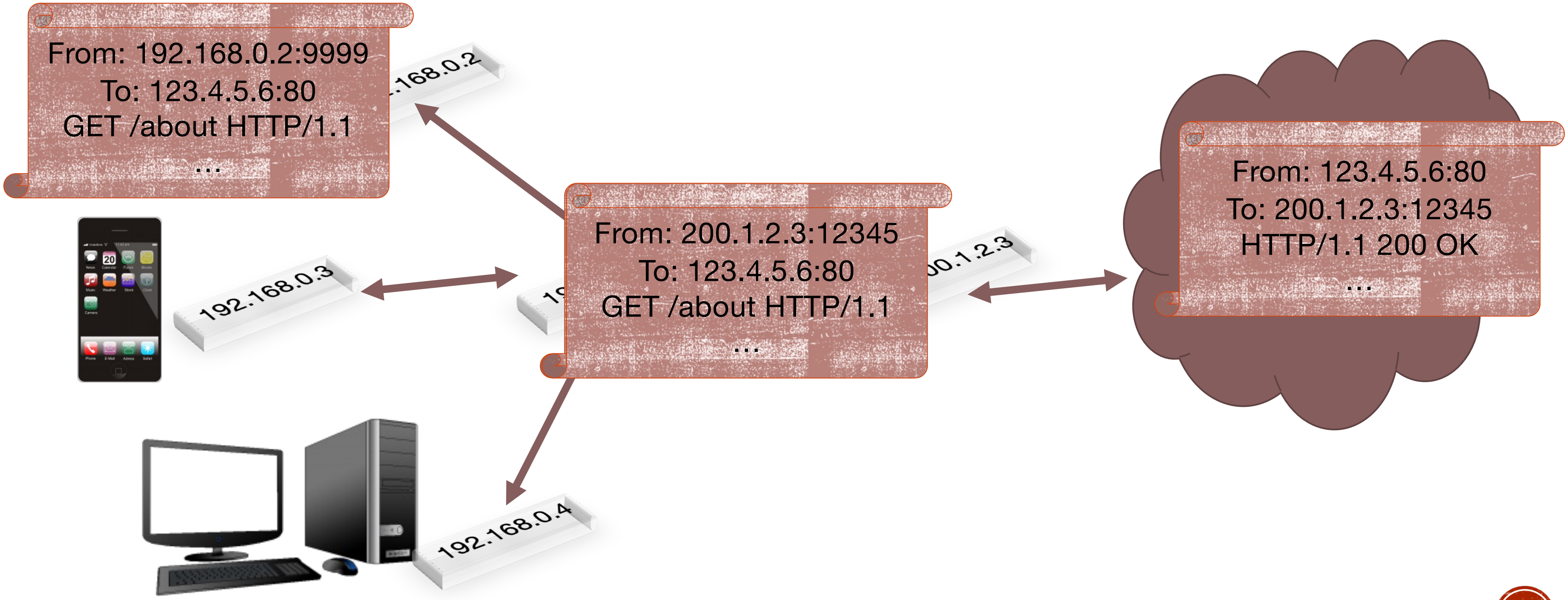
Network Address Translation (NAT)

- Given an IP header, explain its role in NAT
- Given transport and network headers for an IP network, trace how they are used and changed when in an NAT environment
- Trace what happens when a remote machine wants to connect to a server behind a NATing router
- Identify the short comings of NAT for certain classes of application protocols
- Explain why the application layer of applications behind a home router gets involved in NAT (i.e., ftp: passive versus active mode)

NAT ROUTER CONFIGURATION



MESSAGE TRANSFER PROCESS



From: 192.168.0.2:9999
To: 123.4.5.6:80
GET /about HTTP/1.1
...

From: 200.1.2.3:12345
To: 123.4.5.6:80
GET /about HTTP/1.1
...

From: 123.4.5.6:80
To: 200.1.2.3:12345
HTTP/1.1 200 OK
...

IDENTIFYING A CONNECTION

- <source IP, source port, destination IP, destination port, protocol>
- Protocol: transport, typically TCP or UDP
- Local (internal) and remote
  - For incoming messages at a router, local is receiver, remote is sender
  - For outgoing messages from a router, local is sender, remote is receiver
  - e.g., local and remote IP, local and remote port

HANDLING OF MESSAGES THROUGH NAT

- When an internal client sends a message to an external server
  - Router converts source IP to router's public IP
  - Router converts source port to some available port
  - Router adds entry to NAT table describing this mapping
    - source IP, source port, destination IP, destination port, protocol, NAT IP, NAT port
- When the response comes from an external server
  - Router finds NAT table entry for (source IP, source port, destination port, protocol)
  - Router changes destination IP/port to value in the table entry

CLICKER QUESTION

Does NAT work at the network layer or at the transport layer?

A. Network layer only
B. Transport layer only
C. Both network and transport layer
D. Neither network nor transport layer

NAT FORWARDING TABLE EXAMPLE

Internal IP	Internal Port	Remote IP	Remote Port	Protocol	NAT IP	NAT Port
192.168.0.2	9999	123.4.5.6	80	TCP	200.1.2.3	12345
192.168.0.1	6445	12.34.5.6	53	TCP	200.1.2.3	12346
192.168.0.1	6553	1.23.45.6	2628	UDP	200.1.2.3	12347
…	…	…	…		…	…

MULTIPLE INTERNAL DEVICES CONNECTING TO THE SAME SERVER

Internal IP	Internal Port	Remote IP	Remote Port	Protocol	NAT IP	NAT Port
192.168.0.2	9999	123.4.5.6	80	TCP	200.1.2.3	12345
192.168.0.3	9999	123.4.5.6	80	TCP	200.1.2.3	12348
192.168.0.3	9998	123.4.5.6	80	TCP	200.1.2.3	12349
192.168.0.1	6445	12.34.5.6	53	TCP	200.1.2.3	12346
192.168.0.1	6553	1.23.45.6	2628	UDP	200.1.2.3	12347
…	…	…	…		…	…

MULTIPLE INTERNAL DEVICES CONNECTING TO THE SAME SERVER

Internal IP	Internal Port	Remote IP	Remote Port	Protocol	NAT IP	NAT Port
192.168.0.2	9999	123.4.5.6	80	TCP	200.1.2.3	12345
192.168.0.3	9999	123.4.5.6	80	TCP	200.1.2.3	12348
192.168.0.3	9998	123.4.5.6	80	TCP	200.1.2.3	12349
192.168.0.1	6445	12.34.5.6	53	TCP	200.1.2.3	12346
192.168.0.1	6553	1.23.45.6	2628	UDP	200.1.2.3	12347
…	…	…	…		…	…

SERVER ON THE INSIDE

- What if the initial connection comes from outside?
  - Example: server is inside the NAT
  - Example: connection where both hosts are inside NATs
- NAT translation will not find an entry in the table

SERVER ON THE INSIDE

- Option 1: Manually add a fixed rule
  - Example: add a rule that if a connection comes to port 200.1.2.3:8080, it should be forwarded to 192.168.0.2:80
- Option 2: UPnP (Universal Plug and Play)
  - Protocol that runs on the router and internal host
  - Host asks router to enter a forwarding rule (like the manual rule)

Internal IP	Internal Port	Remote IP	Remote Port	Protocol	NAT IP	NAT Port
192.168.0.2	9999	123.4.5.6	80	TCP	200.1.2.3	12345
192.168.0.2	80	Any (manual/UPnP entry)		TCP	200.1.2.3	8080
…	…	…	…		…	…

SERVER ON THE INSIDE

- A client at 123.4.5.6:12345 connects to 200.1.2.3:8080, which is forwarded to 192.168.0.2:80

Internal IP	Internal Port	Remote IP	Remote Port	Protocol	NAT IP	NAT Port
192.168.0.2	9999	123.4.5.6	80	TCP	200.1.2.3	12345
192.168.0.2	80	Any (manual/UPnP entry)		TCP	200.1.2.3	8080
…	…	…	…		…	…

SERVER ON THE INSIDE

- A client at 123.4.5.6:12345 connects to 200.1.2.3:8080, which is forwarded to 192.168.0.2:80

Internal IP	Internal Port	Remote IP	Remote Port	Protocol	NAT IP	NAT Port
192.168.0.2	9999	123.4.5.6	80	TCP	200.1.2.3	12345
192.168.0.2	80	123.4.5.6	12345	TCP	200.1.2.3	8080
192.168.0.2	80	Any (manual/UPnP entry)		TCP	200.1.2.3	8080
…	…	…	…		…	…

SERVER ON THE INSIDE

- A client at 123.4.5.6:12345 connects to 200.1.2.3:8080, which is forwarded to 192.168.0.2:80
- Another client at 123.4.5.6:12346 connects to 200.1.2.3:8080, which is forwarded to 192.168.0.2:80

Internal IP	Internal Port	Remote IP	Remote Port	Protocol	NAT IP	NAT Port
192.168.0.2	9999	123.4.5.6	80	TCP	200.1.2.3	12345
192.168.0.2	80	123.4.5.6	12345	TCP	200.1.2.3	8080
192.168.0.2	80	Any (manual/UPnP entry)		TCP	200.1.2.3	8080
…	…	…	…		…	…

SERVER ON THE INSIDE

- A client at 123.4.5.6:12345 connects to 200.1.2.3:8080, which is forwarded to 192.168.0.2:80
- Another client at 123.4.5.6:12346 connects to 200.1.2.3:8080, which is forwarded to 192.168.0.2:80

Internal IP	Internal Port	Remote IP	Remote Port	Protocol	NAT IP	NAT Port
192.168.0.2	9999	123.4.5.6	80	TCP	200.1.2.3	12345
192.168.0.2	80	123.4.5.6	12345	TCP	200.1.2.3	8080
192.168.0.2	80	123.4.5.6	12346	TCP	200.1.2.3	8080
192.168.0.2	80	Any (manual/UPnP entry)		TCP	200.1.2.3	8080
…	…	…	…		…	…

PROBLEMS WITH NAT?

- Design-level concerns
  - Breaks layering
  - Routers aren’t supposed to be modifying IP addresses, much less ports!
- Security concerns
  - Port forwarding/UPnP opens ports for anybody to connect to your device
  - Expose to viruses and other attacks
- Some applications don’t work well

APPLICATIONS AND NAT

- In some application-level protocols, clients advertise their IP address in their messages
  - Internal host advertises address to be used for connection
  - Example: FTP active mode
  - Example: P2P applications
- If behind NAT, how does client know which IP to use?
- Solution: depends on the application
  - FTP: use passive mode
  - P2P: typically require manual set up or UPnP

IN-CLASS ACTIVITY

- ICA61