Computer Network Security

COMP 178 | Spring 2020 | University of the Pacific | Jeff Shafer

NAT

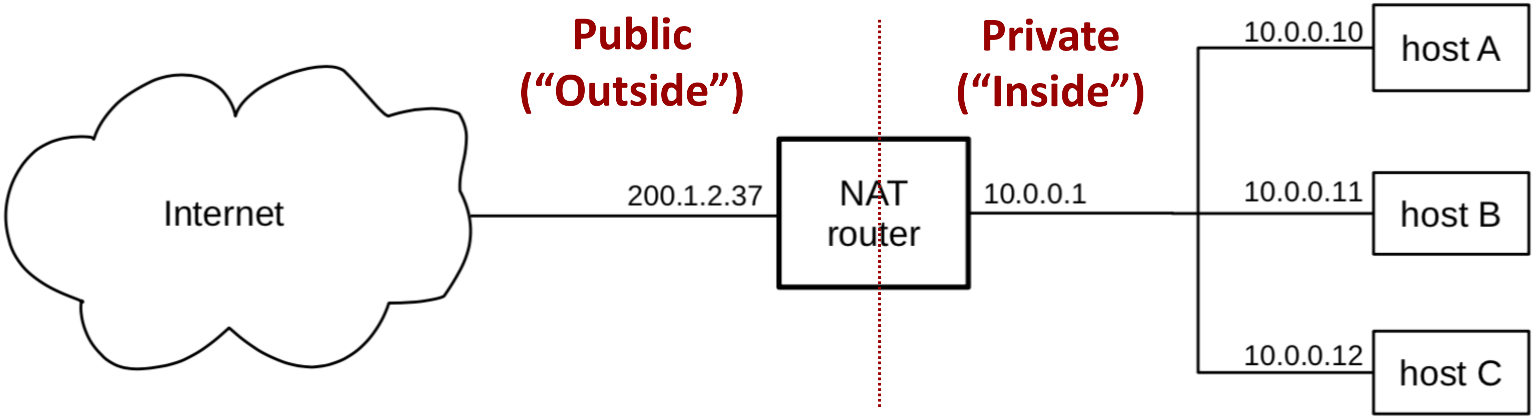
Network Address Translation

Network Address Translation (NAT)

- Suppose you have multiple devices that need to be connected to the Internet
- For the sake of economy the ISP assigns a *single* public IP address to you as a customer
  - How multiple devices can use the only provided valid IP address?
  - Answer: You need *network address translation (NAT)*
- NAT is a capability of routers (*software* or *hardware*) that enables multiplexing large number of individual hosts behind a single IPv4 public address
- Benefits of NAT
  - Conserves *limited address space of IPv4*
  - Enables a form of *firewall-based security* in LANs

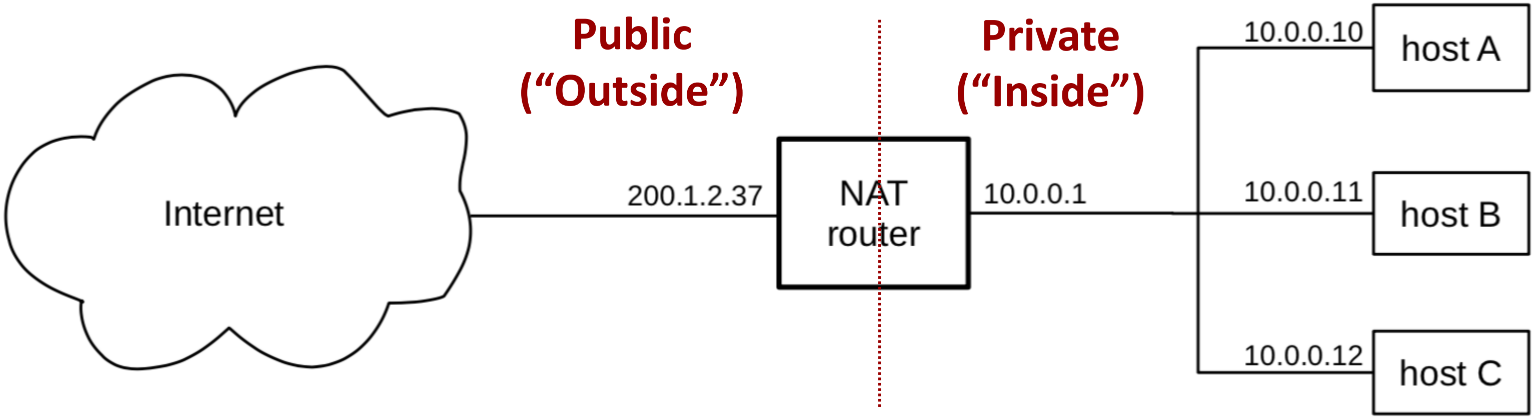
NAT Configuration

- Assign each interface a private IPv4 address
- Assign the interface of NAT router *within the LAN* a **private** IPv4 address
- Assign the publicly facing interface of NAT router the single **public** IPv4 address



NAT Configuration

- The NAT router blocks all connections originating from outside
  - Blocks *inbound* initial SYN packet in TCP 3-way handshake
  - Blocks *inbound* UDP packets that are not in response to earlier outbound requests

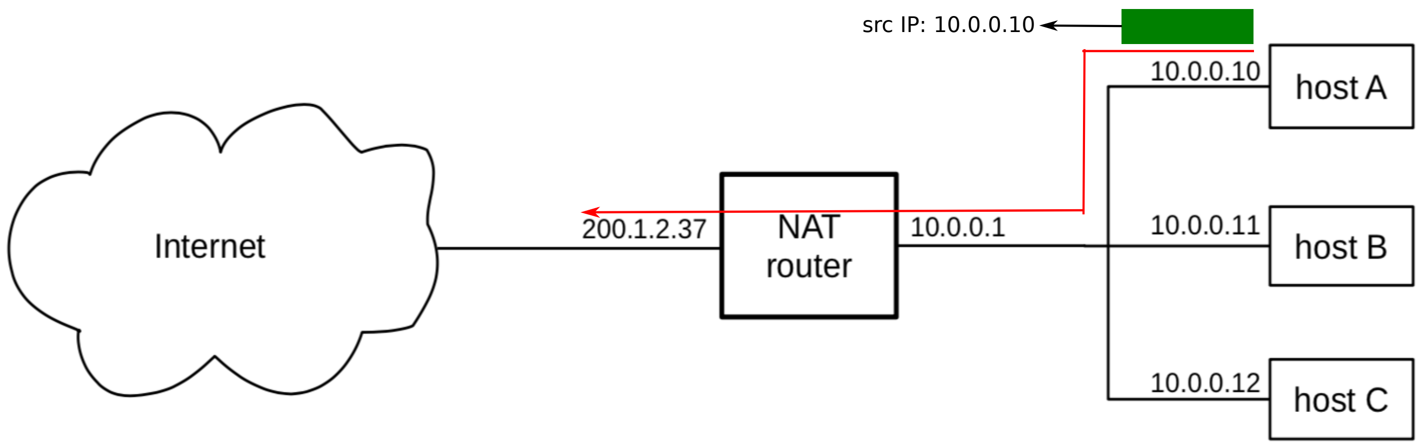


How NAT Works

- The NAT router manipulates *IPv4 addresses* and potentially *TCP/UDP port numbers* within the packet when routing them toward the next hop
  - Both inbound and outbound packets are modified!
- For an *outbound* packet, the NAT router modifies
  - The *source IP* address in IPv4 header
    - Replaced with the publicly visible IP address of its interface
    - (Potentially) the *source port* number in TCP/UDP header
- For an *inbound* packet, the NAT router modifies
  - The *destination* IP address in IPv4 header
    - Replaced with the private IP address that this packet should be forwarded to
    - (Potentially) the *destination port* number in TCP/UDP header

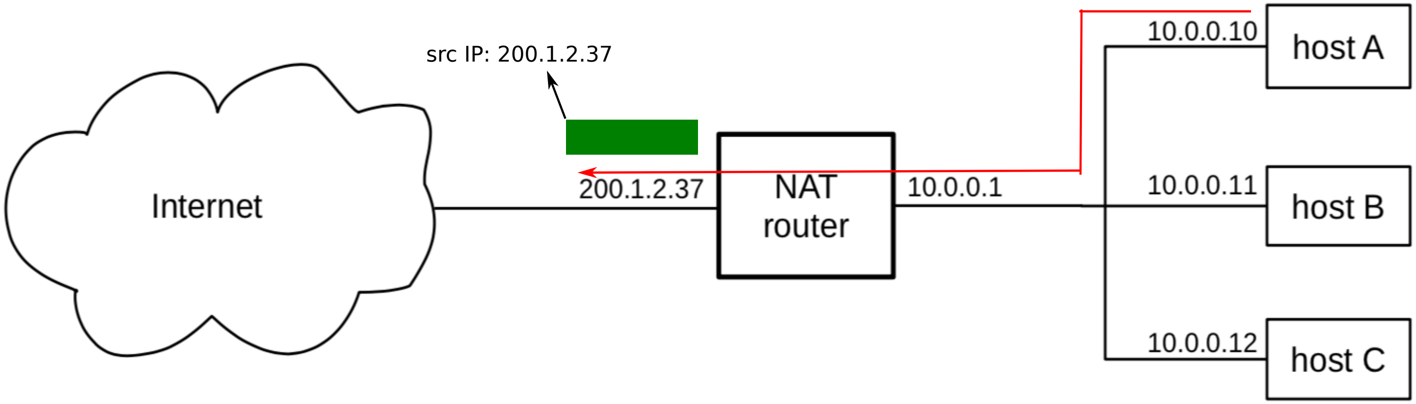
NAT Example

- Assume that host A wants to send a packet to some destination H outside the LAN
  - Source IP address would be 10.0.0.10



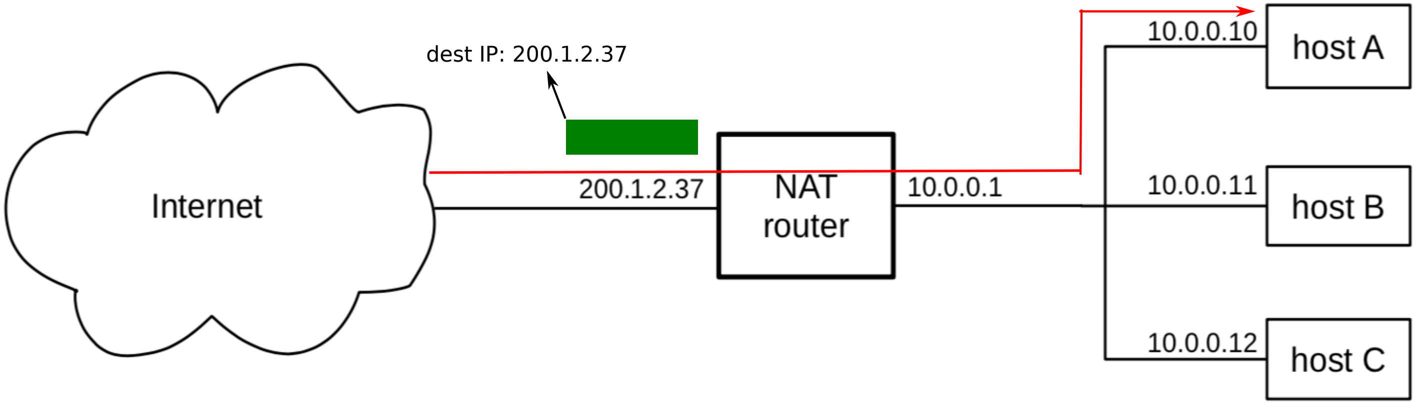
NAT Example

- Assume that host A wants to send a packet to some destination H outside the LAN
  - Source IP address would be 10.0.0.10
- When the NAT router receives this packet, it modifies the *source IP address* from `10.0.0.10` to `200.1.2.37`



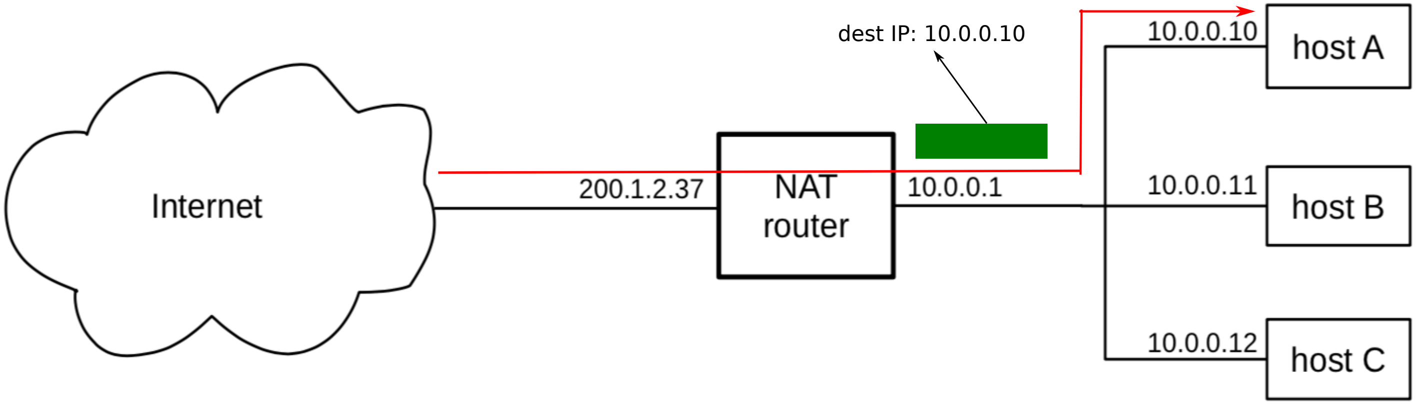
NAT Example

- The response packet comes to the NAT router from the outside node H. The destination address is `200.1.2.37`



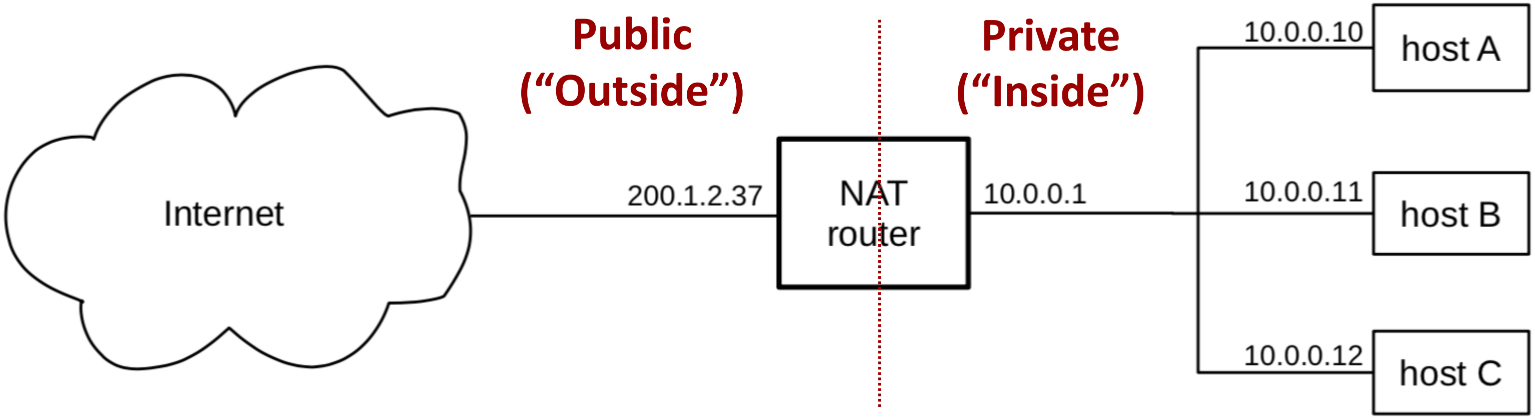
NAT Example

- The response packet comes to the NAT router from the outside node H. The destination address is `200.1.2.37`
- The NAT router changes the destination address to host A’s address, and forwards it to A



Visibility

- In the outsider's view, **only the NAT router is visible**
- The response packets destined to the private LAN are routed to the publicly visible interface of that LAN's NAT router
- All internal addresses (private addresses) are invisible and **non-routable**



NAT Operation

- ***How does NAT router keep track of inbound responses to earlier outbound requests?***

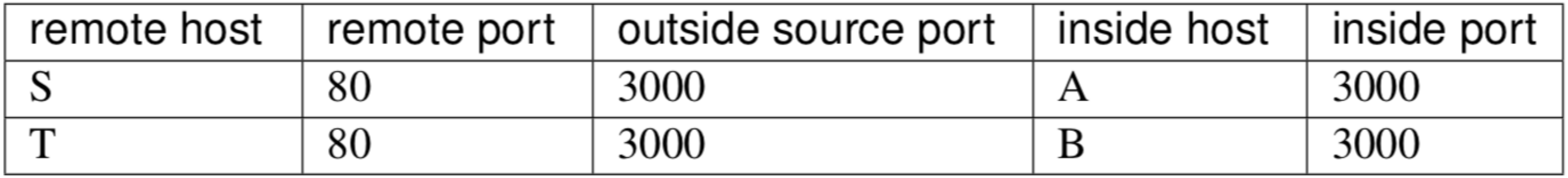
- NAT router stores the state of the connections made between internal (LAN-side) machines and remote (WAN-side) machines
  - This information is stored in the NAT table

- NAT table consists of different information for each connection made between a LAN-side machine and a WAN-side machine, including
  - Remote host IP address and port number
  - Internal host IP address and port number
  - External port number (of NAT router)

- Since port numbers are included, a NAT router maps between internal processes and their external representations

NAT Operation: Remote Host Address

- The remote host address is used to distinguish between two connections from different hosts that use the same (internal) port numbers



remote host	remote port	outside source port	inside host	inside port
S	80	3000	A	3000
T	80	3000	B	3000

- If NAT router receives an inbound packet:
  - … And the source IP is S and source port is 80
    - The destination IP should be changed to A
    - Destination port is unchanged as inside port and outside port are the same
  - … And the source IP is T and source port is 80
    - The destination IP should be changed to B
    - Destination port is unchanged as inside port and outside port are the same

NAT Operation: External Port Number

- External port number is usually the same as the internal port number, but not always!

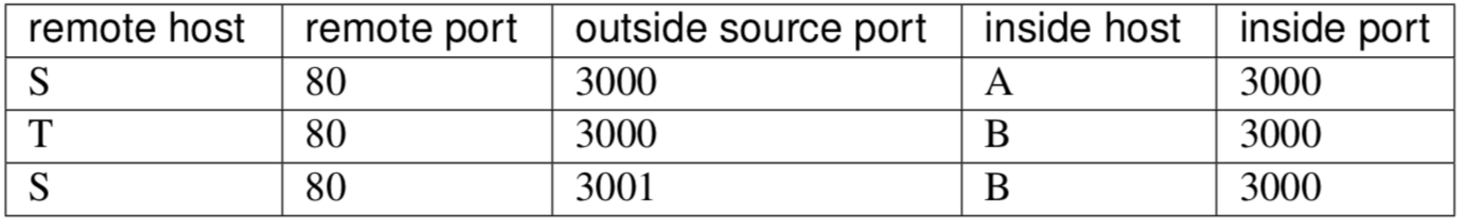
- It can be used to distinguish connections

- Suppose there are two connections from different internal machines (with different IP addresses) and the same port numbers to the same remote process (same IP and port number)

- Then NAT router can use the internal port number in the external port number field for only one of two connections ☹
  - For the other connection, the external port number should be some other value – randomly select!

NAT Operation: External Port Number

- Scenario
  - Internal host A on port 3000 sends a packet to remote host S on port 80
  - Internal host B on port 3000 sends a packet to remote host S on port 80
  - NAT router assigns external port number 3000 to one of the connections (only!)
  - For the other connection, external port number 3001 is assigned

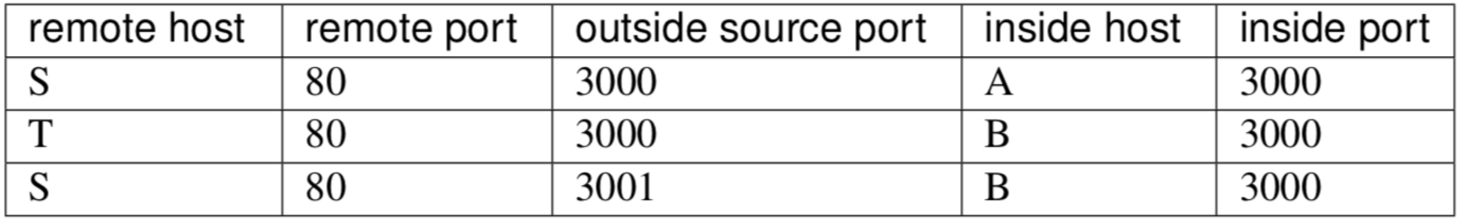


remote host	remote port	outside source port	inside host	inside port
S	80	3000	A	3000
T	80	3000	B	3000
S	80	3001	B	3000

- If A on port 3000 sends a packet to S on port 80, NAT router modifies source IP to its own public IP, and does not change the source port

- If B on port 3000 sends a packet to S on port 80, NAT router modifies source IP to its own public IP, and changes the source port to 3001

NAT Operation: External Port Number



remote host	remote port	outside source port	inside host	inside port
S	80	3000	A	3000
T	80	3000	B	3000
S	80	3001	B	3000

- When the NAT router receives a packet on public interface: checks the source IP, source port number and destination port number
  - If source IP is S, source port is 80, and destination port is 3000, then this packet should be forwarded to A
    - Destination IP is changed to A, but destination port is not changed as both internal and external port numbers are the same
  - If source IP is S, source port is 80, and destination port is 3001, then this packet should be forwarded to B
    - Destination IP is changed to B, and destination port is changed to 3000, as indicated by internal port number

NAT Routers vs TCP

- A NAT router does not establish TCP connections between itself and remote hosts. **It's not a proxy!**
    - It only rewrites the source/destination IP addresses, and potentially source/destination port numbers, along with forwarding the packet
    - NAT router is a Layer-3 device that inspects (and potentially modifies) transport layer port numbers
- NAT routers monitor TCP connections:
    - Whenever NAT router receives an outbound SYN packet (in TCP 3-way handshake), it adds an entry to the NAT table for the connection
    - Whenever NAT router receives an inbound SYN packet (in TCP 3-way handshake), it blocks the packet
    - Upon TCP closing between the internal and remote hosts, NAT router removes the corresponding connection entry from its NAT table

NAT Routers vs UDP

- NAT routers monitor UDP connections to some extent
  - Whenever NAT router receives an outbound UDP packet, it adds an entry to the NAT table for that connection,
  - Whenever NAT router receives an inbound UDP packet, it checks its NAT table. If an entry already refers to such connection the packet should be forwarded
    - Otherwise, packet is blocked
  - NAT routers remove UDP entries after period of inactivity

- NAT routers also work for some non-transport layer traffic, e.g., ICMP messages.
  - Ping messages or ICMP error messages can be forwarded through NAT routers
  - In this case, port numbers in NAT table become irrelevant

Problems with NAT: Architecture

- Generally, NAT works well for applications with
  - Client-server architecture, where
  - Client is behind NAT router, but server is publicly visible
- In other configurations of client-server communication, and in peer-to-peer applications, NAT does not work well and needs special treatment
  - For example, setting manual entries in the NAT router that maps an external port to a fixed internal IP and port ("Port forwarding")

Closing Thoughts

Recap

- Today we discussed
  - Network Address translation
  - NAT tables
  - Problems with NAT

Next Class

- Tuesday: Project work day
- Thursday: Parallel Network Programming

Class Activity

CA.14 – NAT & Wireshark

Due tonight at 11:59pm