Routing METHODS(NAT/PAT and port fowarding)

Presented by
Omid Panahi

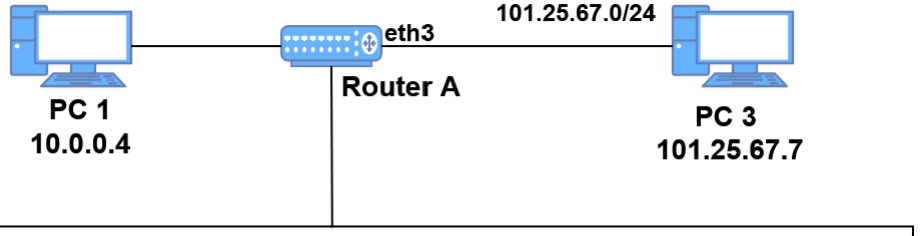
Champlain
COLLEGESAINT-LAMBERT

Review:
Components of Routing Table Entries

- **Destination address:** this refers to the IP address of the destination network.
- **Subnet mask/Netmask:** this refers to the class or range of the destination address. It's used to map the destination address to the right network.
- **Gateway/Next Hop:** this refers to the next IP address to which the packet is forwarded.
- **Interface:** this refers to the outgoing interface that connects to the destination.
- **Metric:** this assigns a value to each route to ensure that optimal routes are chosen for sending packets. In some instances, the metric is the number of hops or number of routers to be crossed to get to the destination network. If multiple routes exist, the route with the lowest metric is usually chosen.

Review:
A Routing Table Entry Example

- Looking at the first entry below, suppose PC1 would like to send a packet to PC3 on the destination at 101.25.67.0. However, PC3 is not on PC1's network, so PC1 forwards this packet to Router A. Upon arrival at Router A, the router checks its routing table for a path to destination 101.25.67.0:

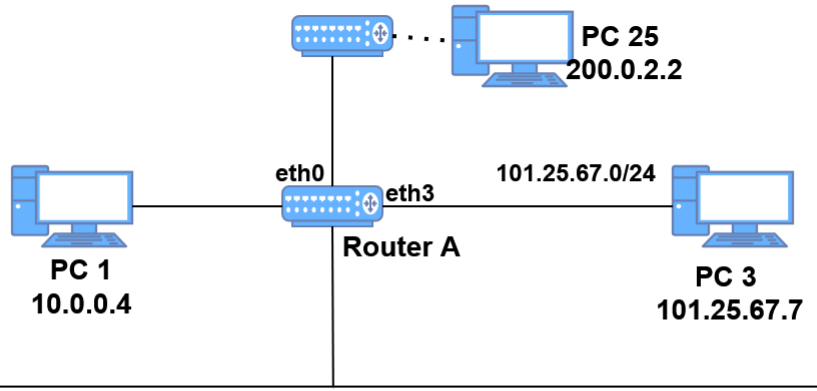


Network Destination	Netmask	Gateway	Interface	Metric
101.25.67.0	255.255.255.0	10.0.0.2	eth3	1
default	0.0.0.0	10.0.0.1	eth0	0
192.25.67.0	255.255.255.0	10.0.0.3	eth5	10

Since a path exists, the packet will be forwarded to the gateway at 10.0.0.2 through interface eth3 on Router A.

Review:
A Routing Table Entry Example (2)

- Suppose a user on PC1 wants to send a packet to PC25 on the network 200.0.2.0. Router A will check its routing table for an entry to the address on which PC25 is located. Since there is no recorded entry, Router A forwards this packet to the default gateway at 10.0.0.1 through the interface eth0 to other networks connected to it.
- The default gateway route is always present in any routing table. It's used when there is no entry for a specific network on the routing table. The default gateway usually connects to other remote networks. For example, in a home environment, the default gateway is connected to the Internet.



Network Destination	Netmask	Gateway	Interface	Metric
101.25.67.0	255.255.255.0	10.0.0.2	eth3	1
default	0.0.0.0	10.0.0.1	eth0	0
192.25.67.0	255.255.255.0	10.0.0.3	eth5	10

Routing METHODS

Dynamic DNS Service

- A dynamic DNS (DDNS) service automatically updates a domain name to point to a changing public IP address.
- This service is useful for home users and businesses because most internet service providers assign dynamic IP addresses that can change without notice.
- Without DDNS, it would be difficult to consistently access hosted websites, as you wouldn't know the correct IP address to connect to.

How Dynamic DNS Works

1. IP address changes: Your Internet Service Provider (ISP) can change your IP address periodically.
2. DNS record is outdated: A standard Domain Name System (DNS) record would become outdated, and you wouldn't be able to connect to your devices.
3. Automatic update: A DDNS client, which can be on your router or a program on your computer, detects the IP address change.
4. DDNS service updates: The client then notifies the DDNS service provider, which automatically updates the DNS record for your domain name to reflect the new IP address.

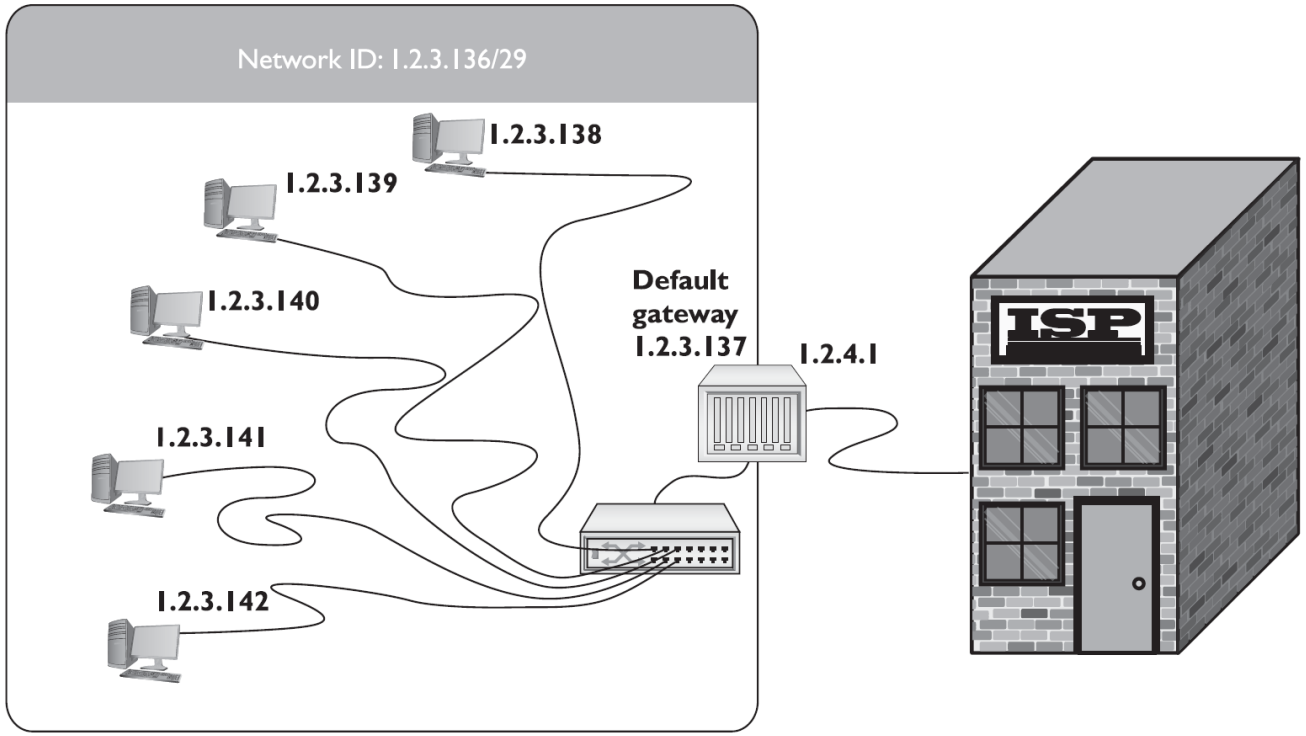
Limitations

- IPv4 has a limited number of public addresses (about 4.3 billion).
- Private IPs (e.g., 192.168.x.x) are **not routable on the internet**.
- How **change internal IP addressing** without affecting external connectivity ?
- How ISPs or organizations can reorganize internal subnets freely?

Static addresses assigned by ISP

Notice:

- Network ID/29 (6 IP's)
- Shared between LAN and WAN.



NAT (Network Address Translation)

- NAT is a simple concept: the router replaces the source IP address of a computer with its outside interface address on outgoing packets.
- *Basic NAT*, does exactly that, translating the private or internal IP address to a global IP address on a one-to-one basis.

Routing Methods

Port Forwarding

Port Forwarding

- We can “share” a public IP address by sending received Internet messages to different computers/servers depending on the PORT it is sent to.
- Example:
  - Port 80 : Send to web server at 172.20.20.150
  - Port 443: Send to same web server 172.20.20.150
  - Port 22: Send to a Linux server 172.20.20.175
  - Port 3389: Send to your personal windows computer (remote desktop) at 172.20.20.200
- Remote Port Forwarding is a way to route incoming requests from the Internet to machines in your LAN.
- Router rules apply to incoming PORTS.
- We can change the destination port (from the Internet) to a specific port such as 1.2.3.4:8080 (1.2.3.4 is the ip of your wan connection).

Scenarios

- Forward port 80 to your main web server.
- Forward port 8080 to your second web server.
- Forward port 8000 to your third server.

- Suppose your public IP is 200.10.20.33, here is how you access your servers from the Internet:
- http://200.10.20.33 (server 1 - No need to specify 80)
- http://200.10.20.33:8080 (server 2)
- http://200.10.20.33:8000 (server 3)

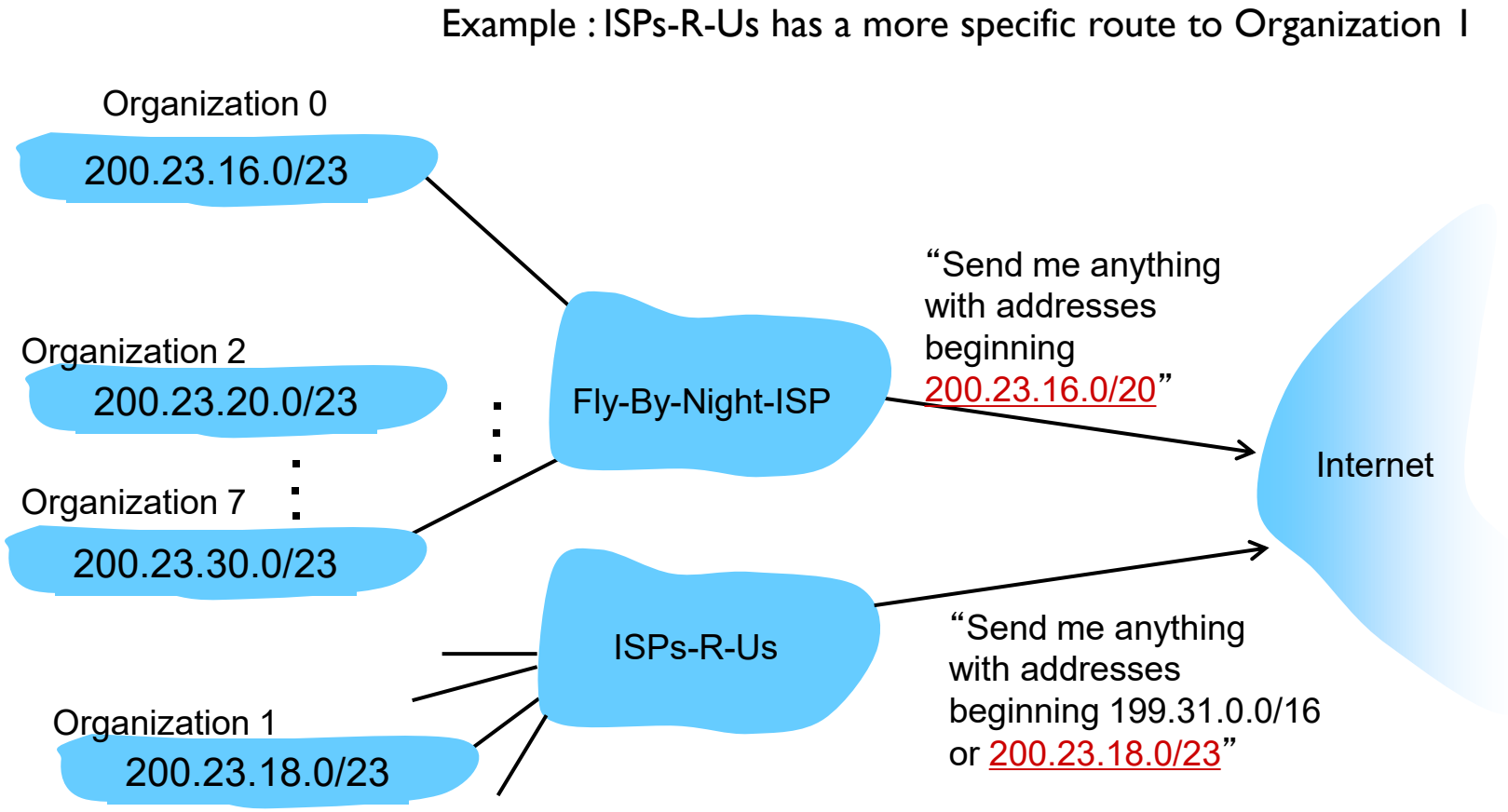
One to Many NAT

- Called PAT (Port Address Translation)
- It's a mapping between PORTS of internal PC's and Ports on the external interface.

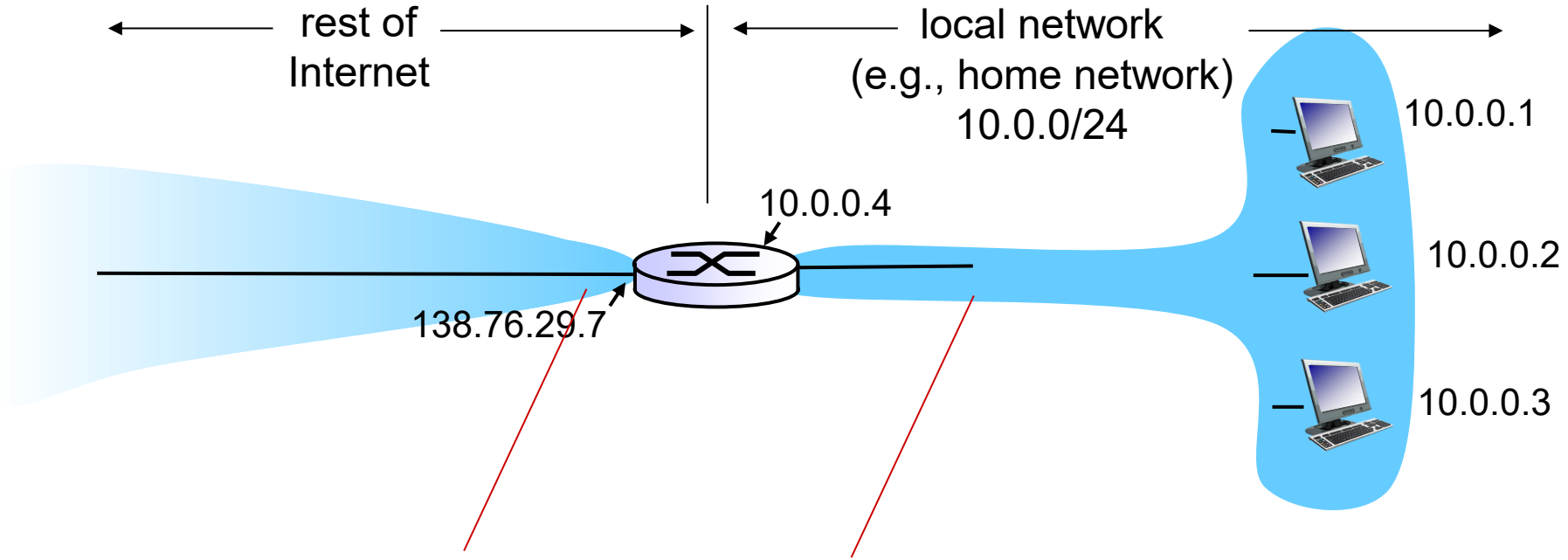
Source	Translated Source	Destination
192.168.1.12:7000	208.190.121.12:7500	
192.168.1.24:13245	208.190.121.12:15000	17.5.85.11:80

Hierarchical addressing: more specific routes

hierarchical addressing allows efficient advertisement of routing information



NAT: network address translation



all datagrams *leaving* local network have *same* single source NAT IP address: 138.76.29.7,different source port numbers

datagrams with source or destination in this network have 10.0.0/24 address for source, destination (as usual)

NAT: network address translation

motivation: local network uses just one IP address as far as outside world is concerned:

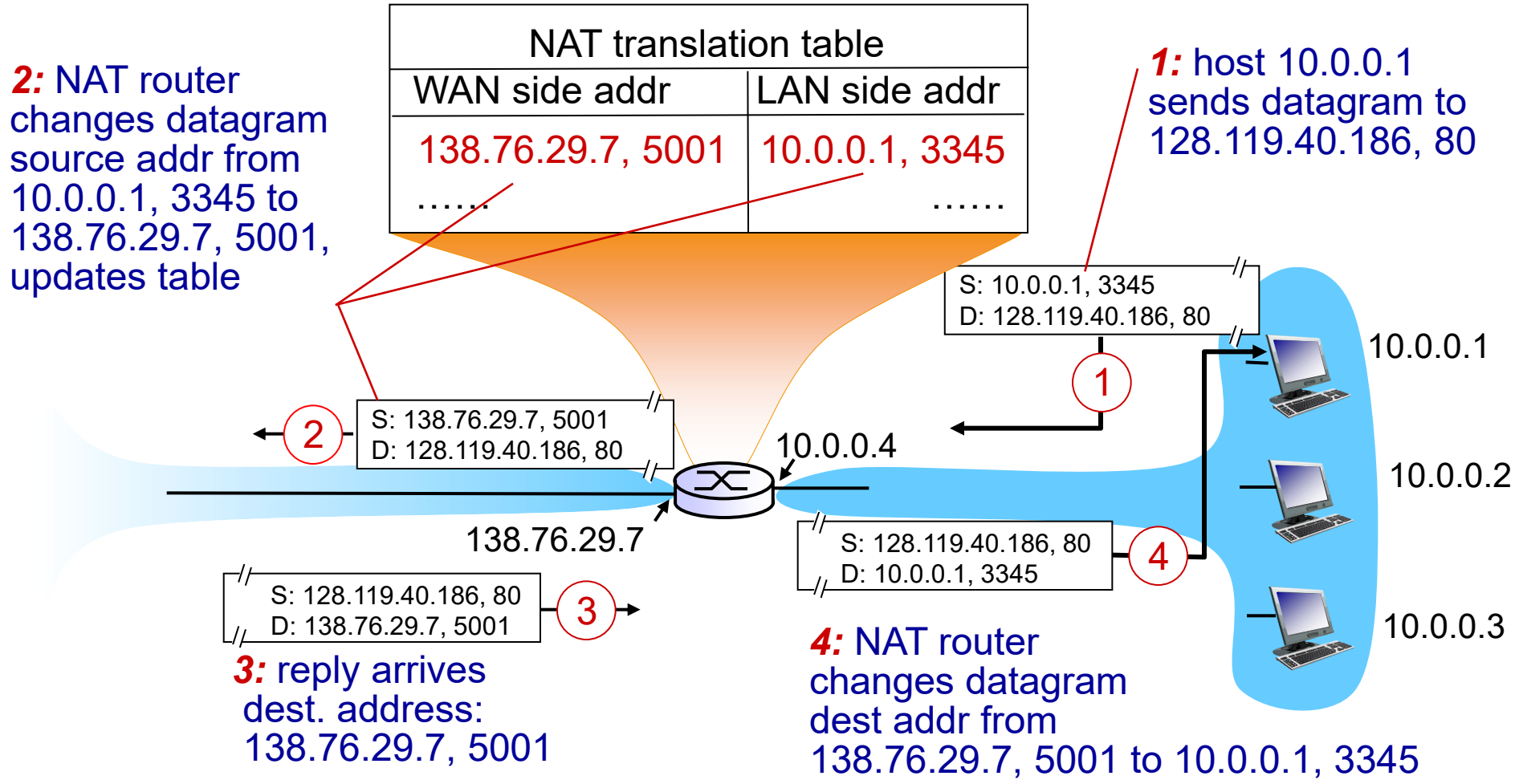
- range of addresses not needed from ISP: just one IP address for all devices
- can change addresses of devices in local network without notifying outside world
- can change ISP without changing addresses of devices in local network
- devices inside local Network not explicitly addressable, visible by outside world (a security plus)

NAT: network address translation

implementation: NAT router must:

- *outgoing datagrams: replace* (source IP address, port #) of every outgoing datagram to (NAT IP address, new port #)
  - . . . remote clients/servers will respond using (NAT IP address, new port #) as destination addr
- *remember (in NAT translation table)* every (source IP address, port #) to (NAT IP address, new port #) translation pair
- *incoming datagrams: replace* (NAT IP address, new port #) in dest fields of every incoming datagram with corresponding (source IP address, port #) stored in NAT table

NAT: network address translation



* Check out the online interactive exercises for more examples: http://gaia.cs.umass.edu/kurose_ross/interactive/

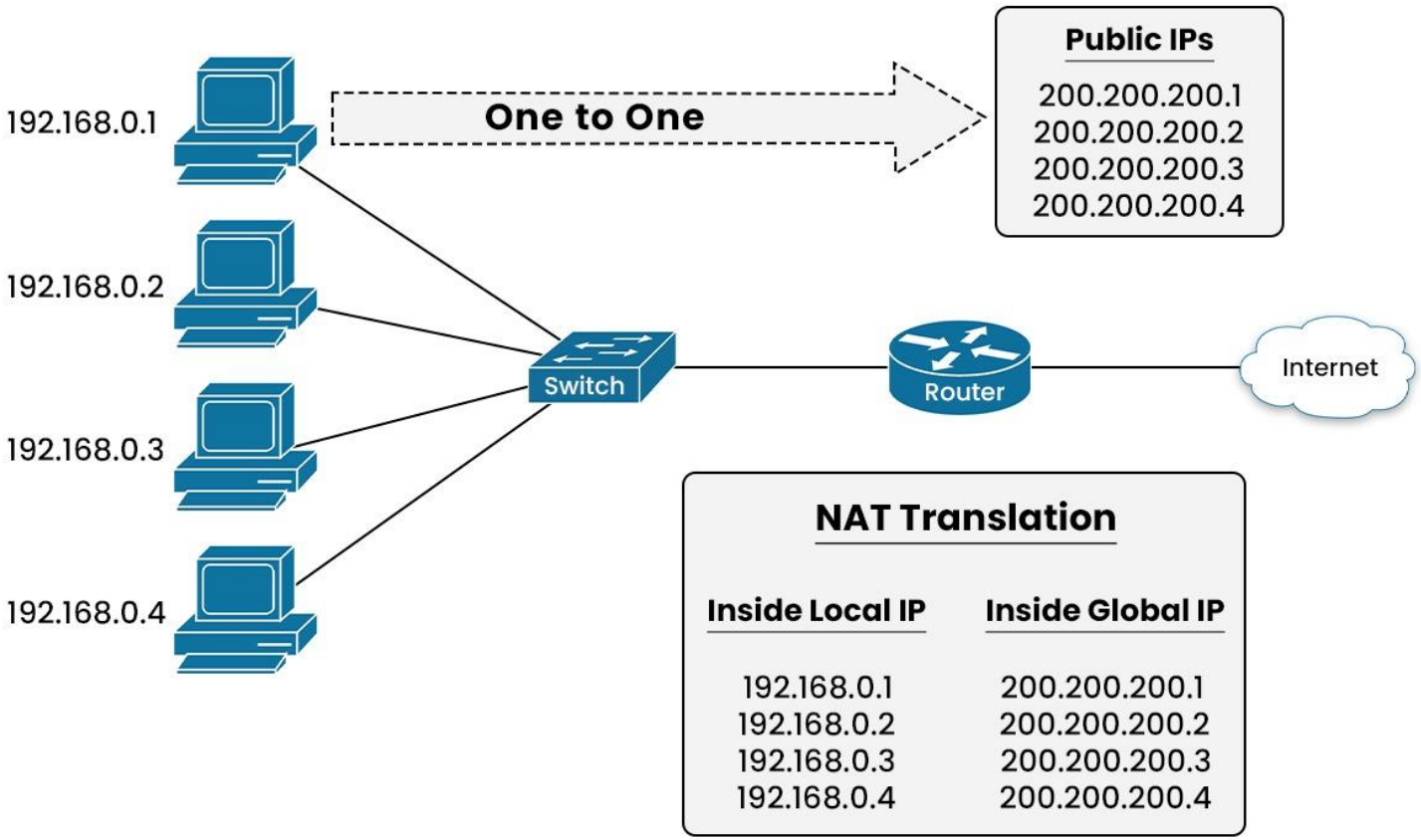
NAT: network address translation

- 16-bit port-number field:
  - 60,000 simultaneous connections with a single LAN-side address!
- NAT is controversial:
  - routers should only process up to layer 3
  - address shortage should be solved by IPv6
  - violates end-to-end argument
    - NAT possibility must be taken into account by app designers, e.g., P2P applications
  - NAT traversal: what if client wants to connect to server behind NAT?

Static NAT

- The simplest NAT implementation comes through Static NAT. A unique public IP address from the external network is mapped to every private IP address from the internal network when using static NAT. The mapping stays fixed since each communication between internal devices and external networks maintains identical public IP addresses.
- Maps a public IP directly to an internal IP
- Creates a 1:1 direct link

STATIC NAT


192.168.0.1
192.168.0.2
192.168.0.3
192.168.0.4
One to One
Public IPs
200.200.200.1
200.200.200.2
200.200.200.3
200.200.200.4
Switch
Router
Internet
NAT Translation
Inside Local IP
Inside Global IP
192.168.0.1
192.168.0.2
192.168.0.3
192.168.0.4
200.200.200.1
200.200.200.2
200.200.200.3
200.200.200.4

Use Cases for Static NAT

Static NAT is mainly used to provide outside-world access to a particular device located on your internal network. For example:

- **Web Servers:** Static NAT allows web server access from the internet by connecting server private IP addresses to public IP addresses.
- **VPN Servers:** The external accessibility of your VPN server depends on static NAT because this translation system assigns the desired public IP for server reachability.
- **VoIP Servers:** The use of static NAT in VoIP Server environments supports continuous communication operations.

Advantages of Static NAT

- **Simplicity:** You can implement Static NAT because its configuration methods and management are straightforward.
- **Predictable Communication:** Static NAT allows reliable communication management through its predictable mapping, which remains static.
- **No Overhead:** The translating process creates minimal processing overhead because the translation is done once and remains static.

Disadvantages of Static NAT

- **Limited Address Conservation:** The use of static NAT provides no benefits for conserving IP addresses because each internal IP requires its own individual public IP address.
- **Costly:** Static NAT becomes expensive to employ because public IP addresses are limited and costly for managing multiple devices.

Routing Methods

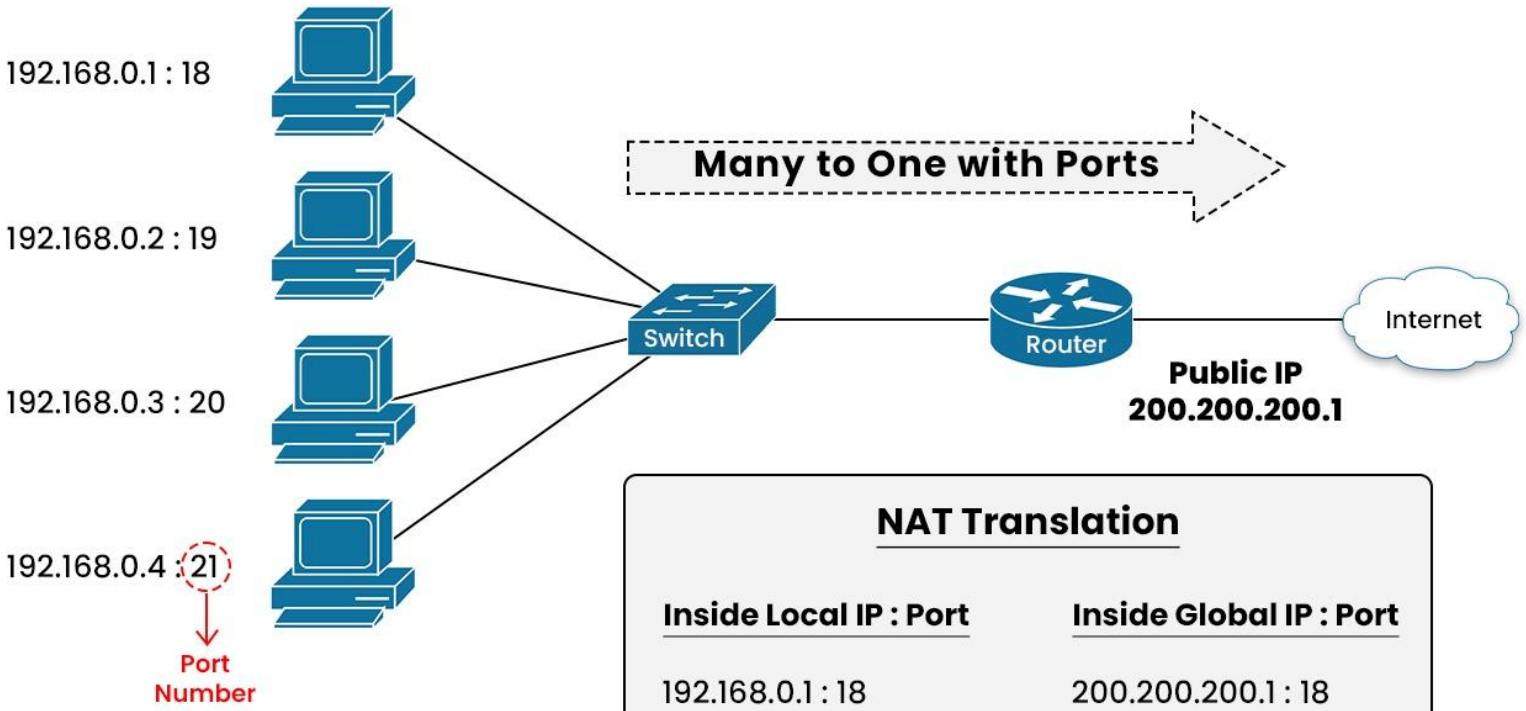
PAT (Port Address Translation)

Port Address Translation (PAT)

- It's a mapping between PORTS of internal PC's and Ports on the external interface.

Source	Translated Source	Destination
192.168.1.12:7000	208.190.121.12:7500	
192.168.1.24:13245	208.190.121.12:15000	17.5.85.11:80

PAT (NAT Overload)



NAT Translation

Inside Local IP : Port	Inside Global IP : Port
192.168.0.1 : 18	200.200.200.1 : 18
192.168.0.2 : 19	200.200.200.1 : 19
192.168.0.3 : 20	200.200.200.1 : 20
192.168.0.4 : 21	200.200.200.1 : 21

PAT

- When the receiving system sends the packet back, it reverses the IP addresses and ports. The router compares the incoming destination port and source IP address to the entry in the **NAT translation table** to determine which IP address to put back on the packet. It then sends the packet to the correct computer on the network.
- IP Ports used for outgoing PAT: 49152 to 65535

Use Cases for PAT

PAT is widely used in scenarios where many devices need to connect through one public IP address. Some common use cases include:

- **Residential Networks:** Home routers implement PAT to allow their users to connect multiple devices with a single public Internet Protocol address.
- **Large Enterprise Networks:** In large enterprise networks, PAT functions to maintain public IP address conservation as it allows multiple devices to access the internet.
- **Mobile Networks:** Mobile networks implement PAT to allow a large number of devices to utilize a limited number of public IP addresses.

Advantages of PAT

- **Maximal IP Address Conservation:** IP Address Conservation reaches its maximum potential through PAT when devices can use a single public IP address to create connections for hundreds or thousands of devices.
- **Efficiency:** The PAT makes use of available port numbers effectively so multiple connections remain free of interference.
- **Scalability:** The PAT offers excellent scalability because it works effectively with large networks that contain many devices.

Disadvantages of PAT

- **Complexity:** Configuration and management of PAT becomes challenging because PAT performs both IP address and port translation.
- **Security Considerations:** Security threats arise from PAT because the protocol hides internal devices' actual IP addresses, which makes tracking malicious activities more difficult.
- **Port conflict avoidance:**

  If an internal device attempts to use a port that is already in use, the router will select an alternative port from the available pool.

PAT – Steps (1,2)

1. **Private host sends a packet:** A device on the internal network (e.g., 192.168.1.10) sends a packet to an external server (e.g., 8.8.8.8) using its private IP address and a source port (e.g., port 50000).
2. **Router translates the address and port:** The NAT-enabled router replaces the private IP address with its public IP address (e.g., 203.0.113.5).It also assigns a unique source port number (e.g., 40001) to keep track of this connection in its NAT table.

PAT – Steps (3)

3. **Packet goes to the Internet:** The translated packet now has:
   - Source IP: 203.0.113.5
   - Source Port: 40001
   - Destination IP: 8.8.8.8
   - Destination Port: 53

PAT – Steps (4)

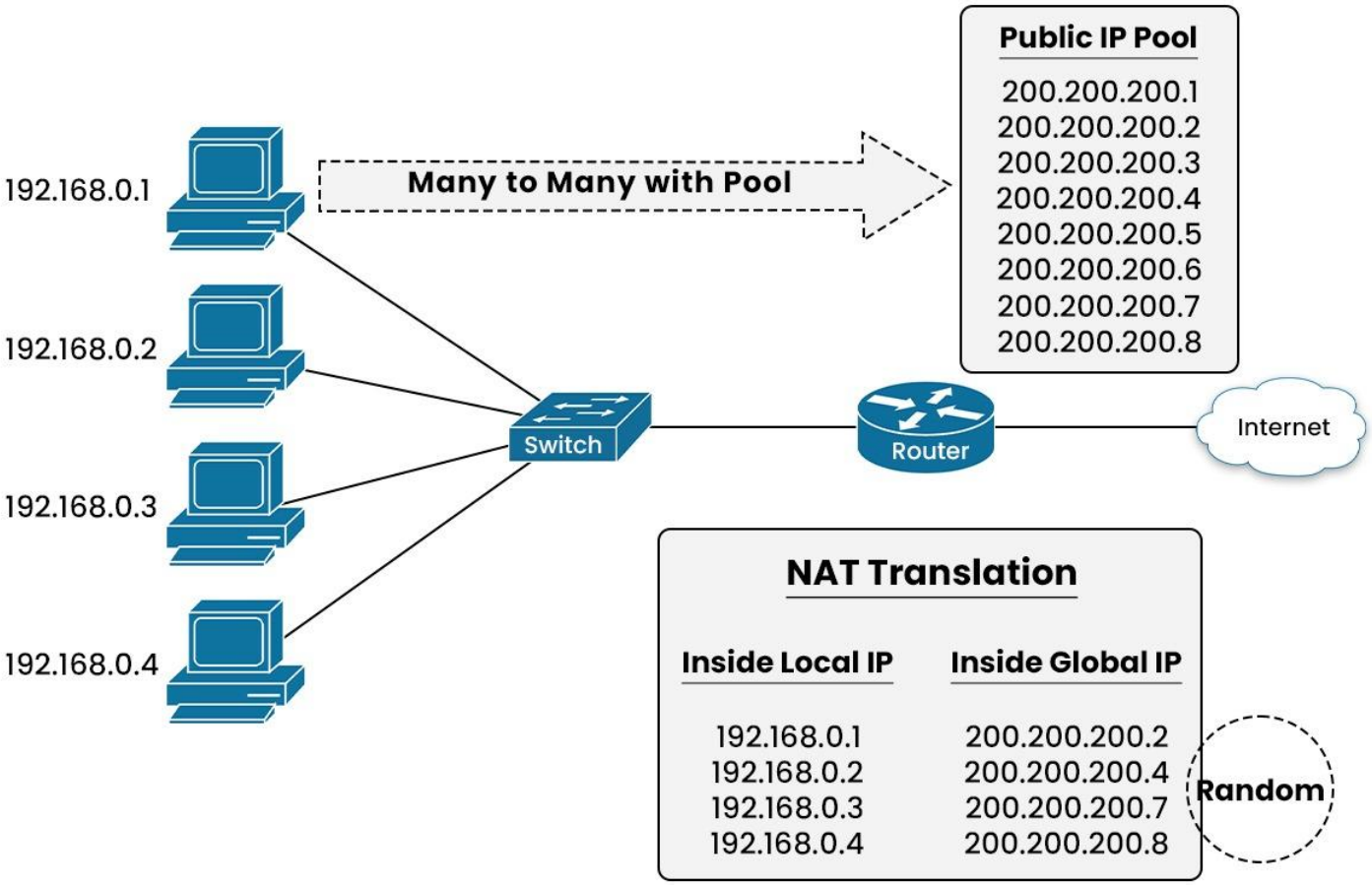
4. **Response comes back:** The external server (8.8.8.8) sends a response to 203.0.113.5:40001.Router looks up the NAT table:The router checks its translation table and finds which internal device and port correspond to 203.0.113.5:40001 → 192.168.1.10:50000.
5. **Router translates back and forwards to the host:** The router changes the destination address/port back to the internal host (192.168.1.10:50000) and sends the packet inside the LAN.

Dynamic NAT

Dynamic NAT

- Sharing a pool of routable IP addresses (usually less than the # of computers)
- When a computer needs to contact a resource on the Internet, it gets assigned an IP from the pool.
- Also called "pooled nat"

DYNAMIC NAT


Public IP Pool
200.200.200.1
200.200.200.2
200.200.200.3
200.200.200.4
200.200.200.5
200.200.200.6
200.200.200.7
200.200.200.8
192.168.0.1
Many to Many with Pool
192.168.0.2
Switch
Router
Internet
192.168.0.3
192.168.0.4
NAT Translation
Inside Local IP
Inside Global IP
192.168.0.1
192.168.0.2
192.168.0.3
192.168.0.4
200.200.200.2
200.200.200.4
200.200.200.7
200.200.200.8
Random

Use Cases for Dynamic NAT

The deployment of Dynamic NAT provides an appropriate solution for multiple devices that access a limited set of public IP addresses. Examples include:

- **Home Networks:** Most home routers implement dynamic NAT for multiple devices to share one public IP address.
- **Small Office Networks:** Small businesses with numerous devices can benefit from dynamic NAT for conserving public IP address usage.
- **Temporary Connections:** Dynamic NAT provides an excellent solution for short-term connection requirements like VPNs and remote access because devices utilize public IP addresses in a temporary manner.

Advantages of Dynamic NAT

- **IP Address Conservation:** Dynamic NAT allows multiple devices to share a few public IP addresses, which directly conserves the available IPv4 address space.
- **Flexibility:** Devices that use dynamic NAT benefit from flexible translations because they require no predefined rules for device connection and disconnection.
- **Cost-Effective:** Dynamic NAT allows shared public IP addresses, which lowers expenses for obtaining numerous public IP addresses.

Disadvantages of Dynamic NAT

- **Complexity:** The implementation of dynamic NAT needs a more intricate setup and management compared to how static NAT operates.
- **Overhead:** The translation process involves the operation of a translation table, which results in processing overhead.

Key Differences of PAT versus Dynamic NAT

Feature	Dynamic NAT	PAT (Port Address Translation)
Mapping	One-to-one (private to public IP)	Many-to-one (private IPs to a single public IP)
IP Address	Requires multiple public IPs	Uses a single public IP
Key Component	IP address translation only	IP address and port number translation
Scalability	Limited	High
Complexity	Simpler to configure	More complex due to port management

Complete Routing Methods LAB with Packet Tracer

Champlain

COLLEGE SAINT-LAMBERT