Network Address Translation and Port Forwarding

Prof. Chien-Chao Tseng

曾 建 超 教授

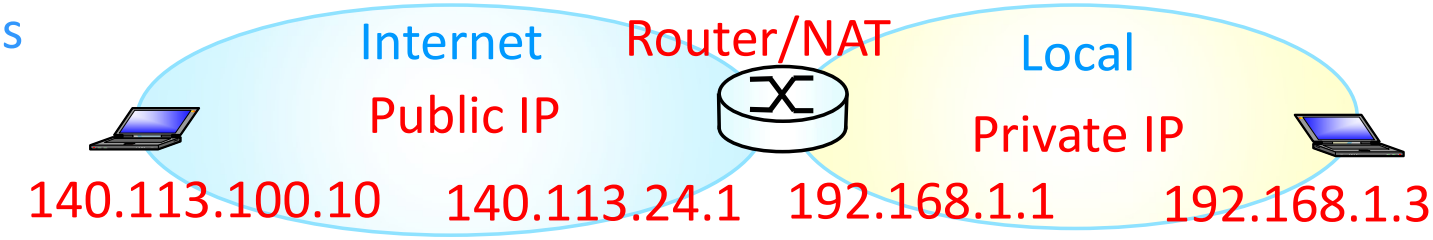
Department of Computer Science
National Yang Ming Chiao Tung University

cctseng@cs.nctu.edu.tw

Reference: J. F. Kurose and K. W. Ross, Computer Networking: A Top Down Approach

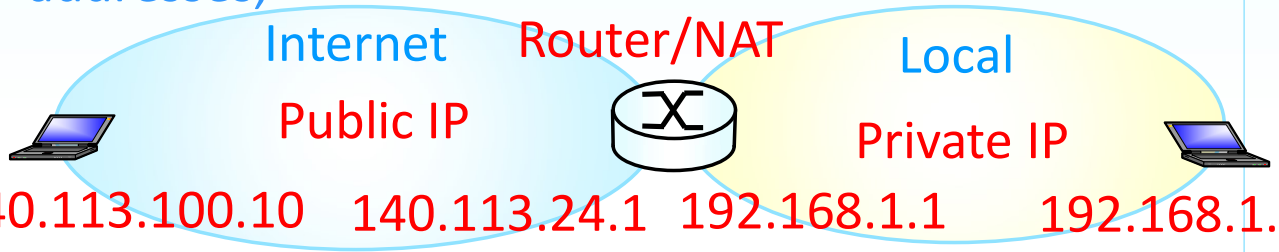
Depletion of IP Addresses

- Internet Protocol (IP) Address: Host ID on Internet
  - IPv4 addresses: 32-bits long
    - Numbers of IPs: $0 \sim 2^{32} - 1 = 4{,}294{,}967{,}295$.
- Machine connects directly into Internet must have a **globally unique** IP address
- Public IPs: Globally unique, registered IP addresses
  - Administered by Internet Assigned Numbers Authority (IANA)
- Depletion of IP address
- Solutions
  - Short term
    - Classless Inter-Domain Routing (CIDR) with subnetting
    - Private IP addresses with Network Address Translation (NAT)
  - Long term
    - IPv6 (with 128 bits address space)



Public and Private IP Addresses

- Public IPs: Administered by Internet Assigned Numbers Authority (IANA)
  - Globally unique, registered IP addresses,
  - Globally Routable
- Private IP Addresses
  - Not Globally Delegated
  - Used for intranets (private networks),



- **Three blocks of IP address space** for **private networks** (RFC 1918)

172.11110000.255.255

Block Size`	CIDR Prefix	Mask	Private Address Space	Classful
24 bits	10.0.0.0/8	255.0.0.0	10.0.0.0 – 10.255.255.255	1 A
20-bits	172.16.0.0/12	255.240.0.0	172.16.0.0 – 172.31.255.255	16 B
16 bits	192.168.0.0/16	255.255.0.0	192.168.0.0 – 192.168.255.255	256 C

  - Cannot be transmitted onto the public Internet

172.00010000.255.255

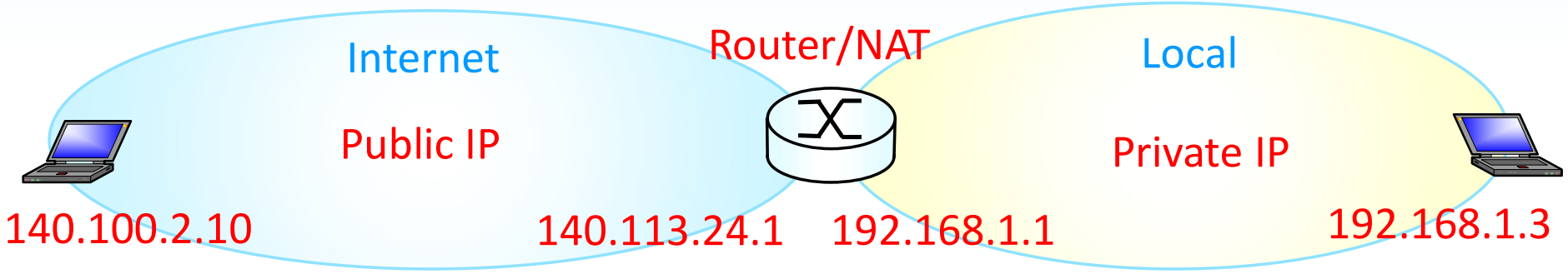
172.00011111.255.255

➢ Need **Network Address Translation** (NAT)

What is Network Address Translation (NAT)?

- Network Address Translation

  A method that maps IP addresses from one address realm to another



- NAT maps private addresses into globally routable ones and vice versus
  - Allows organization to use **private IP addresses** and yet **connect to the Internet**

✓ With NAT, **internal network** of an organization ***appear,*** from the outside, to be using a **different IP address space** (than what it is actually using.)

Transport Multiplexing

- Access to multiple services
- Not mixing up sessions
  - Host OS can identify distinct sessions
- Unique Flow IDs:
  - Five-tuples
    - Destination IP, Port
    - Source IP, Port
    - Protocol

Example: Multiple Co-existing Session Identification

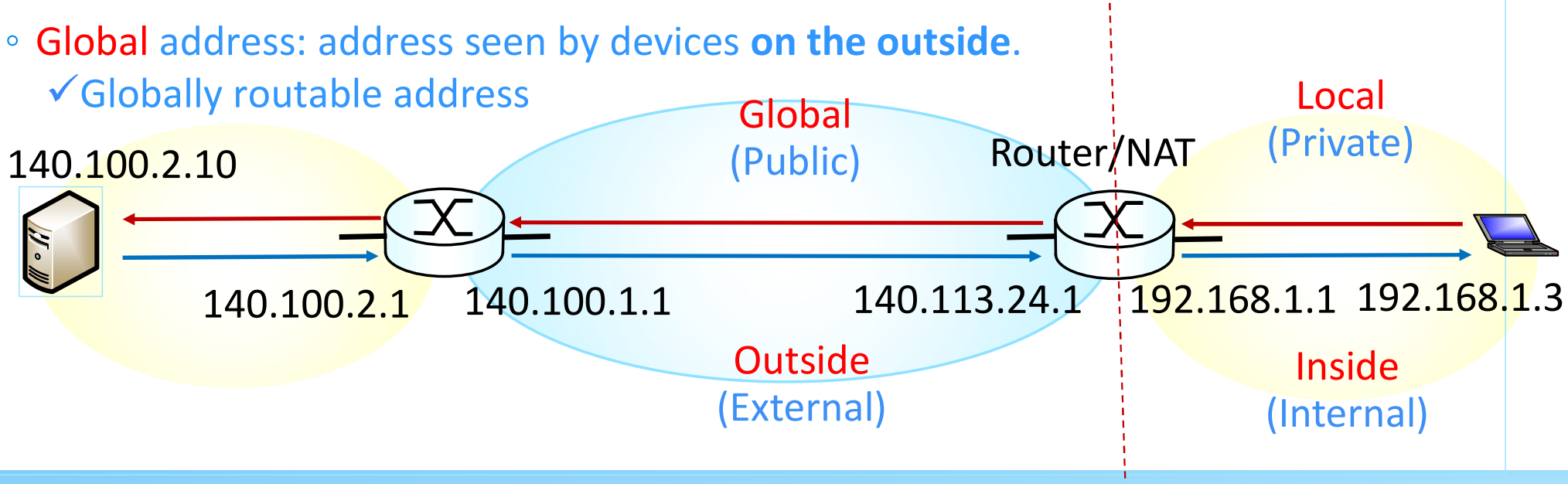
- **TCP** is connection-oriented
  - TCP Sessions identified by **Five Tuples**

Protocol	Source IP	Source Port	Destination IP	Destination Port
TCP	192.168.0.193	53375	140.113.43.18	443
TCP	192.168.0.193	53509	140.113.43.18	443
TCP	192.168.0.193	55466	180.222.102.158	443
UDP	…	…	…	

  - Application (Browser) provides Destination IP and Port
  - OS provides Source IP and a unique Source Port
- UDP is connectionless,
  - UDP Sessions identified by Protocol and (Dest IP, Dest port) (on receiving host)

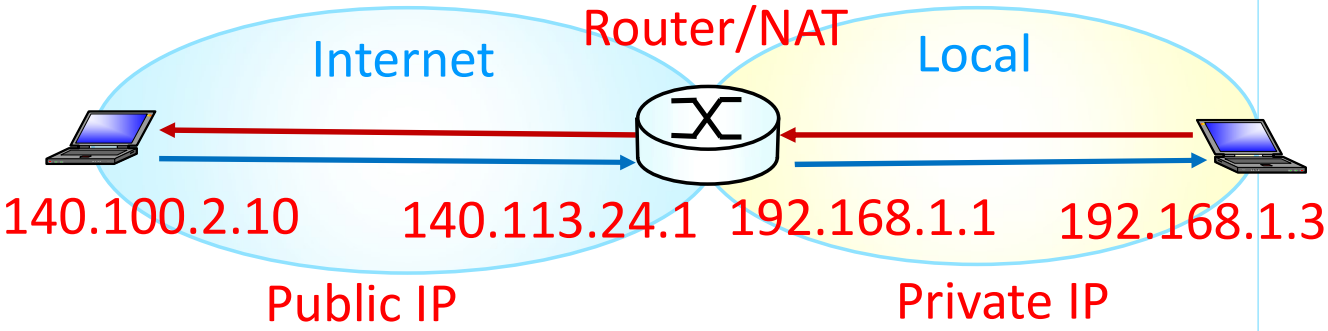
Anatomy of IP Addresses

- **NAT device** divides its universe into
  - Inside: Private network and devices connected to the network
  - Outside: Public Internet and devices reachable over Internet.
- IP addresses could be classified as ***local*** or ***global***.
  - Local address: address seen by devices **on the inside**
  - Global address: address seen by devices **on the outside**.
    - ✓Globally routable address



Overview of NAT

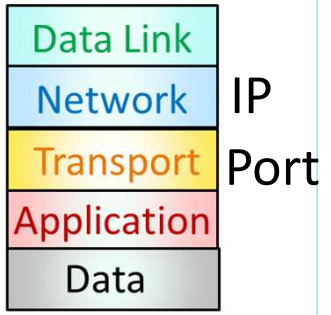
- What does NAT do?
  - Re-write the source and/or destination addresses of IP packets when they pass through a router or firewall
  - What can be re-written?
    - Source/Destination IPs
    - Source/Destination Ports
- What can NAT do?
  - Solve the IPv4 address shortage . (Most common purpose)
  - Firewall (Security)
  - Load balancing (Scalability)
  - Fail over (High Availability)



NAT Overloading (Port Address Translation)

- Dynamic NAT: Dynamically map private IP addresses to public IP addresses
- **Overloading: Many-to-one** mapping between **private** and **public** addresses
  - ➢ Mapping multiple **private IP** addresses to a single **registered public IP** address.
- **Network Address Port Translation** (NAPT)/**Port Address Translation** (PAT)
  - Track **IP addresses**, **Protocol** and **Ports**
  - ➢ Translating both **IP** address and **Port** number of packets

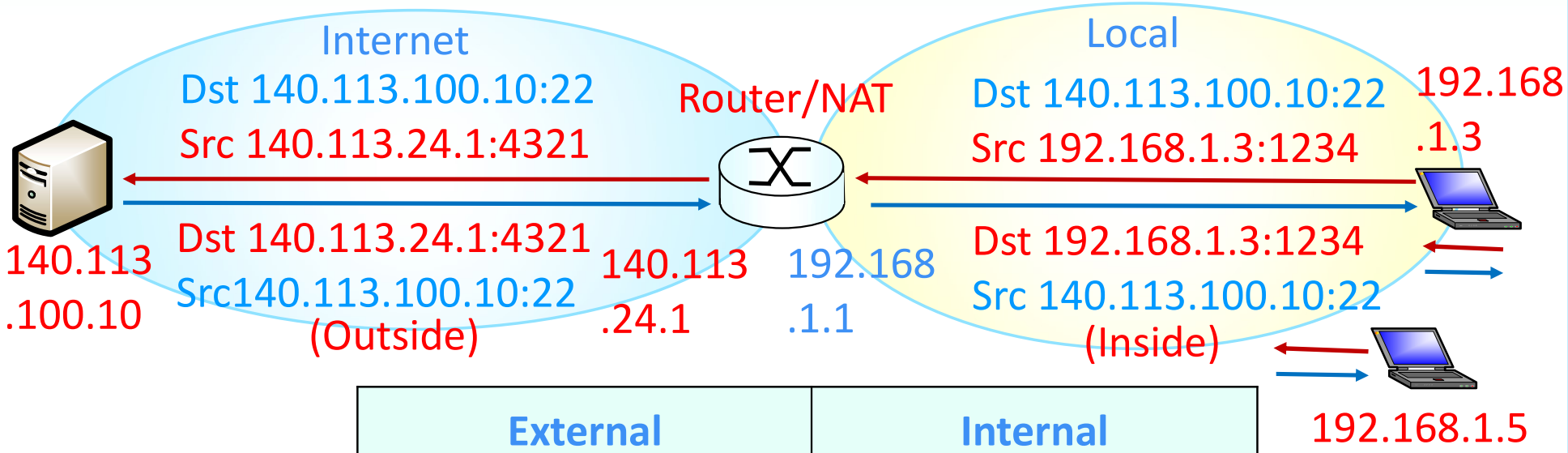
External	Internal
140.113.24.1:**4321**	192.168.1.3:**1234**
140.113.24.1:8765	192.168.1.5:5678
. . .	. . .



  - A single **global address** can map up to 65535 **local** addresses
- ➢ Many hosts can simultaneously connect to Internet using a single global IP address
- ✓ Helps with the issue of IP depletion problem.

NAT Port Address Translation

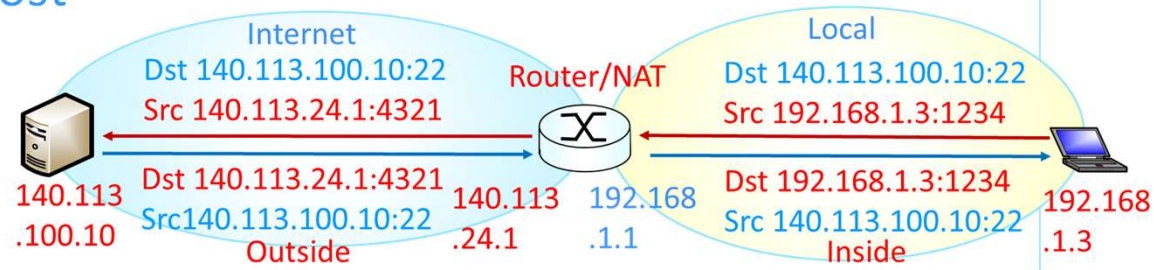
- Assigns transport identifiers (ports) for connections
- Maps internal transport addresses (IP and port) to external transport addresses
- Records mapping and re-write transport addresses in IP headers



External	Internal
140.113.24.1:4321	192.168.1.3:1234
140.113.24.1:8765	192.168.1.3:5678
140.113.24.1:9999	192.168.1.5:1234

How NAT/NAPT Works

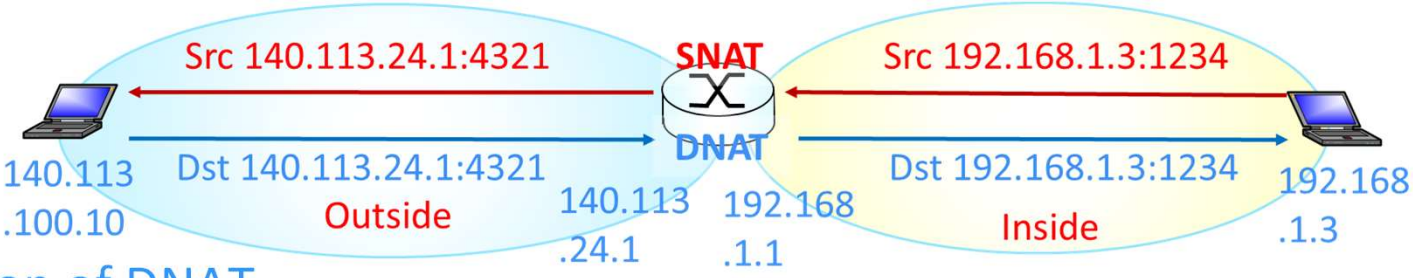
- **For outgoing datagrams:**
  - *Replaces* (IP address, Port #) in **Source Fields** with (NAT IP address, NAT Port #),
  - *Sends* replaced datagram to remote host
    - ➢Remote host responds using (NAT IP address, NAT Port #) as **Destination Transport address**
  - *Remember (in NAT translation table)* every (IP address, Port #) to (NAT IP address, NAT port #) translation pair



- **For incoming datagrams:**
  - *Replace* (NAT IP address, NAT Port #) in **Destination Fields** with corresponding (IP address, Port #) stored in NAT table

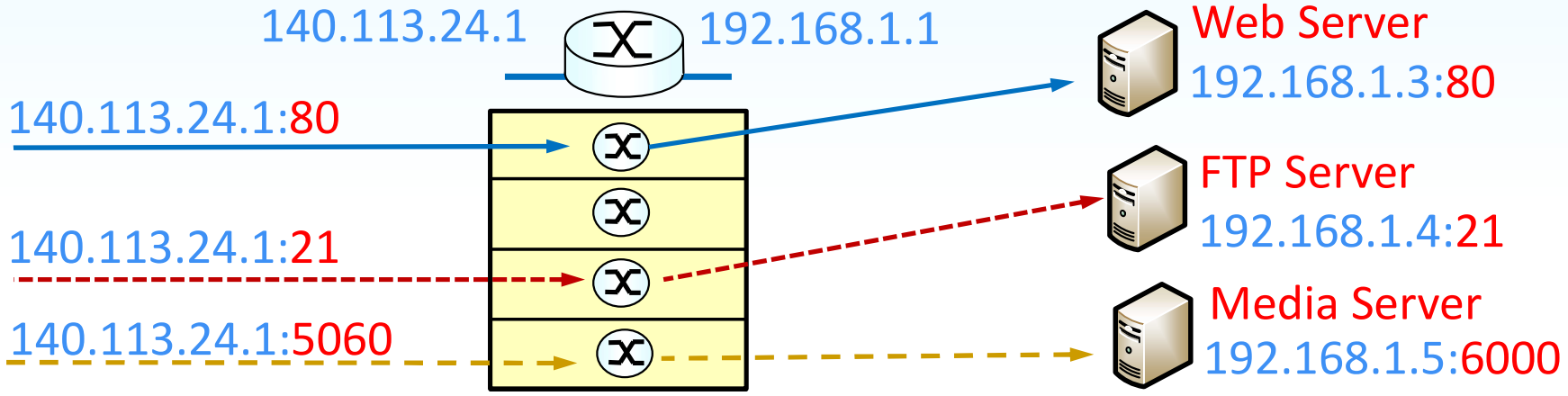
SNATs and DNATs

- **Source NAT (SNAT)**
  - Change source IP address, retain destination IP address.
  - Allows a host on "**inside**" with a private IP address to initiate a connection to a host on "**outside**".
- **Destination NAT (DNAT):**
  - Retain source IP address, change destination address.
  - Allows a host on "**outside**" with a public IP to connect to a host on the "**inside**" with a private IP.



- **Port forwarding**
  - A common application of DNAT
  - Redirects a packet from one destination transport address to another.
  - Commonly used to **publish** a service located in **a private network**

Illustration of Port Forwarding



- NAT Translation Table:

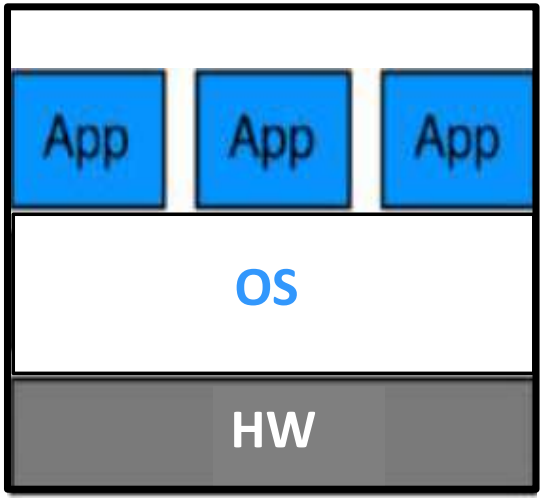
External	Internal
140.113.24.1:80	192.168.1.3:80
○ ○ ○	○ ○ ○
140.113.24.1:21	192.168.1.3:21
140.113.24.1:5060	192.168.1.5:6000

- **Recall:** IP is destination-based routing
  - **SNAT** is performed after routing decision.
  - **DNAT** is performed before routing decision

Virtual Machine

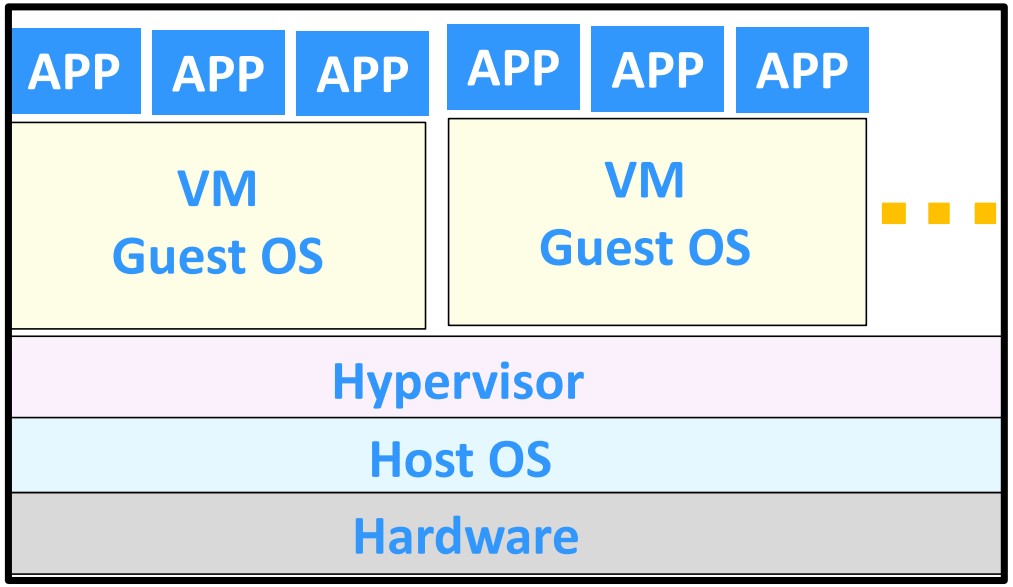
- A virtual machine is a software computer that, like a physical computer, runs an **operating system** and **applications**.

- **Physical Machine**



Virtualization

- **Virtual Machines**



VirtualBox and Networking Modes

- By Oracle
- Networking Modes:
  - Not attached.
  - Network Address Translation (NAT)
    - Default Mode
  - NAT Network.
  - Bridged networking.
  - Internal networking.
  - Host-only networking.
  - Cloud networking.
  - Generic networking.