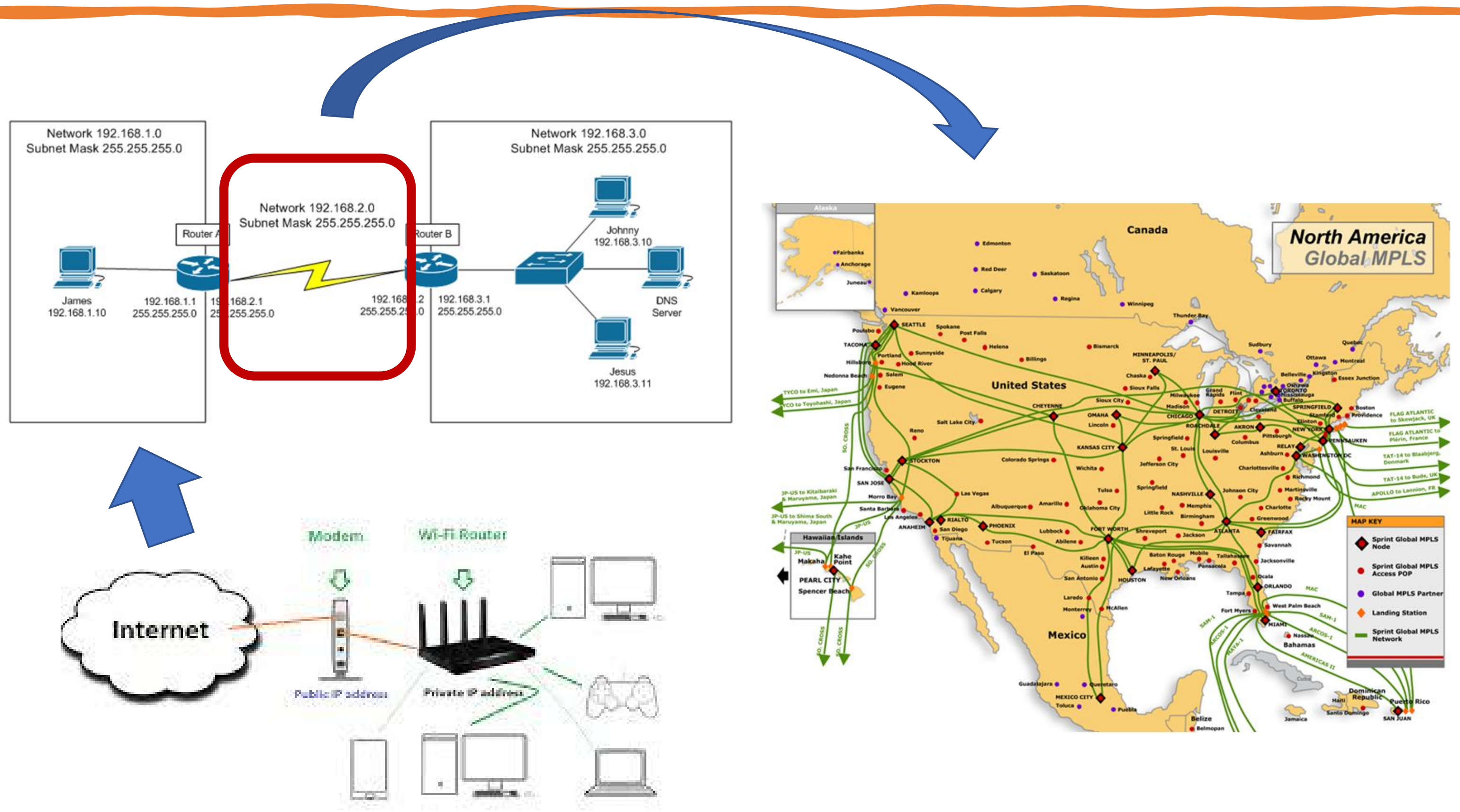
Chapter 01
Setting up your virtual lab

How Network Works



Protocols

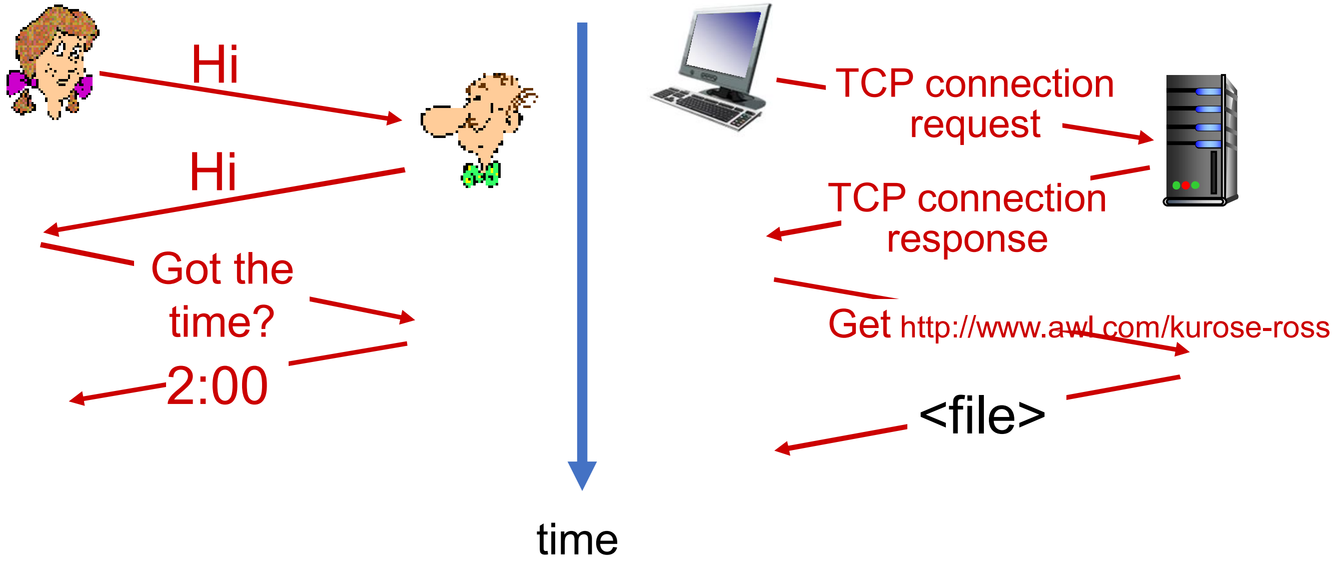
- A **protocol** defines the rules for communication between computers

- **Connectionless protocol**
  - Sends data out as soon as there is enough data to be transmitted
  - E.g., user datagram protocol (**UDP**)

- **Connection-oriented protocol**
  - Provides a **reliable connection** stream between two nodes
  - Consists of **set up, transmission, and tear down** phases
  - Creates virtual circuit-switched network
  - E.g., transmission control protocol (**TCP**)

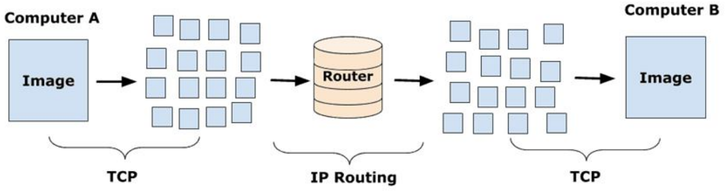
Protocols

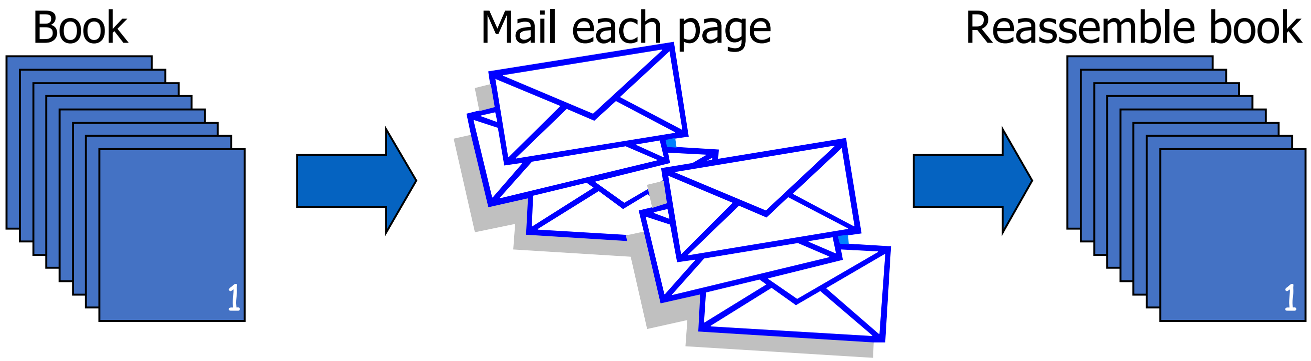
- **Few Concepts**



TCP: Transmission Control Protocol

- **Connection-oriented**, preserves order
  - Sender
    - Break data into packets
    - Attach packet numbers
  - Receiver
    - Acknowledge receipt; lost packets are resent
    - Reassemble packets in correct order

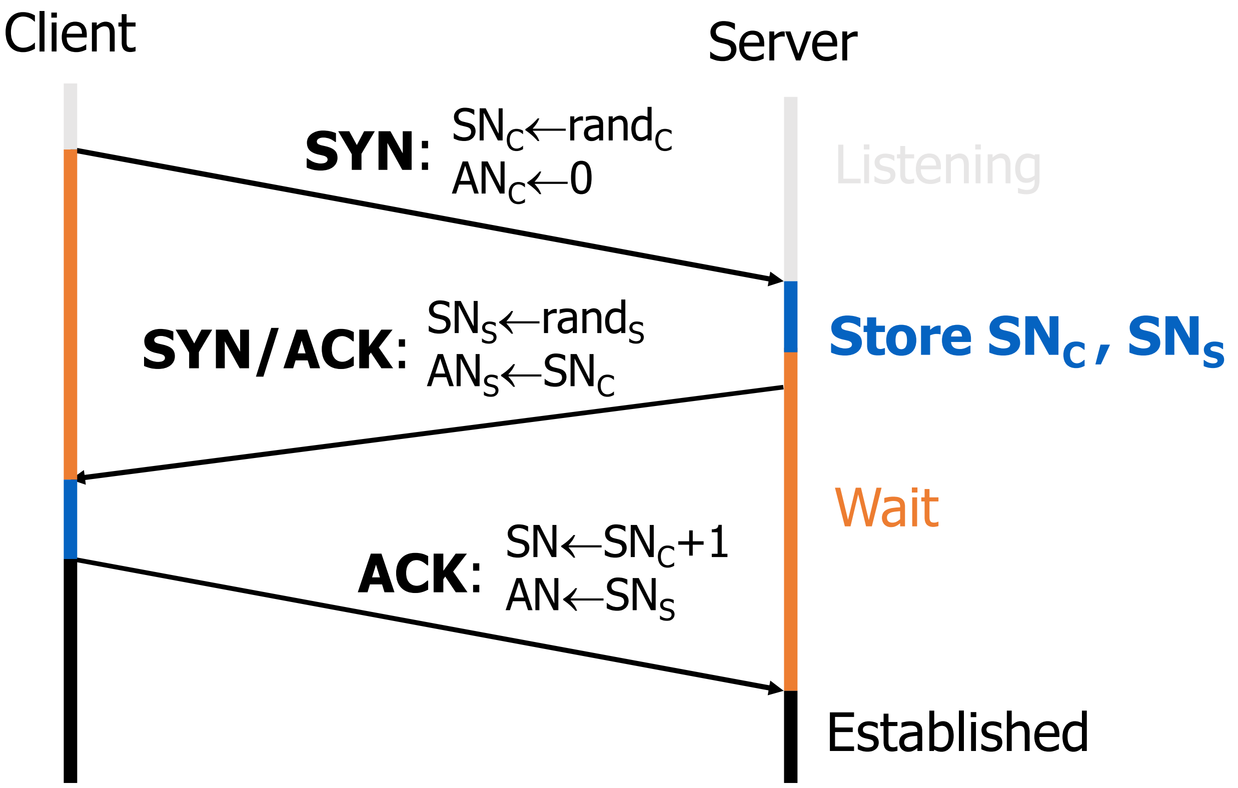



Book

Mail each page

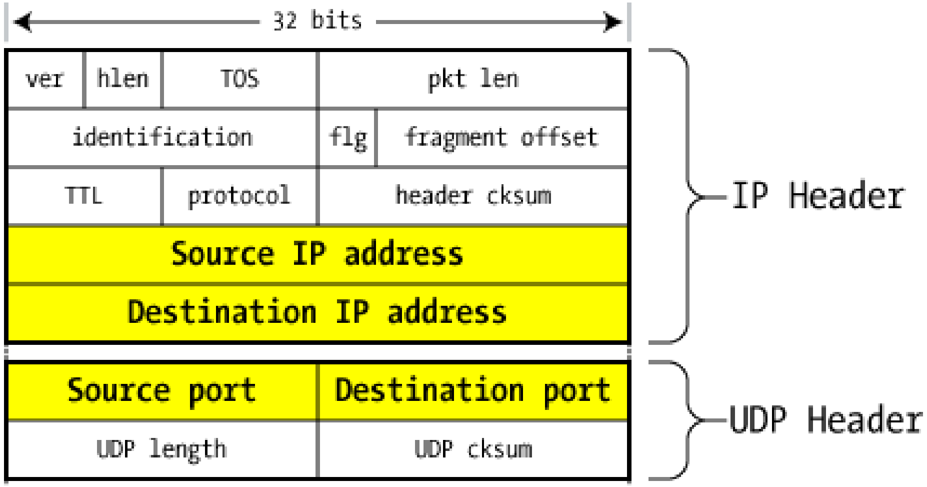
Reassemble book

Review: TCP Handshake


Client
Server
SYN: $SN_C \leftarrow rand_C$ $AN_C \leftarrow 0$
Listening
SYN/ACK: $SN_S \leftarrow rand_S$ $AN_S \leftarrow SN_C$
Store SN_C, SN_S
Wait
ACK: $SN \leftarrow SN_C+1$ $AN \leftarrow SN_S$
Established

UDP: User Datagram Protocol

- **Unreliable** transport on top of IP:
  - No acknowledgment
  - No congestion control
  - No message continuation



32 bits

ver | hlen | TOS | pkt len

identification | flg | fragment offset

TTL | protocol | header cksum

Source IP address

Destination IP address

Source port | Destination port

UDP length | UDP cksum

IP Header

UDP Header

UDP …

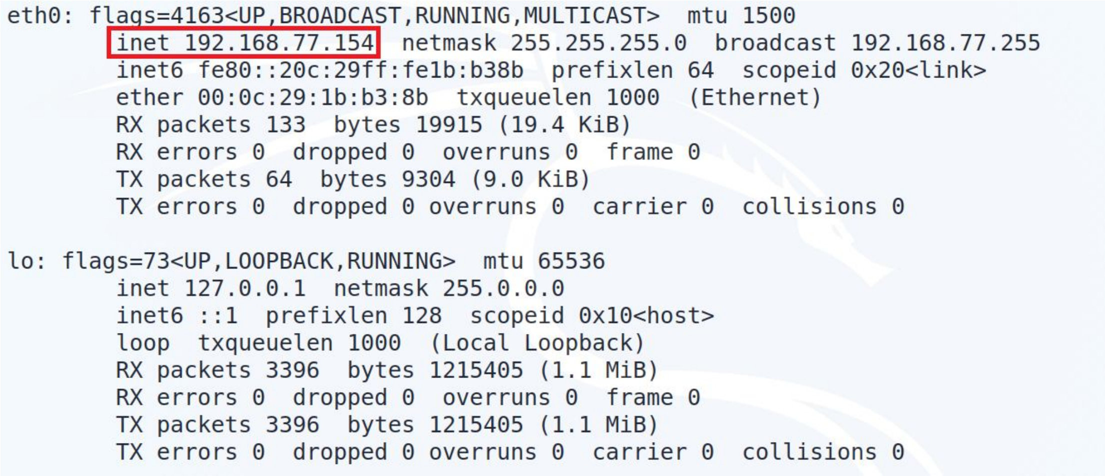
Want to hear a funny UDP joke?
Um, okay?
You may not get it, and I really won't care.
…………
www.NeweggBusiness.com
Design: Dana Choi

ICMP

- **Internet Control Message Protocol** (ICMP)
  - Used for network **testing** and **debugging**
  - Simple messages encapsulated in single IP packets
  - Considered a network layer protocol
- Tools based on ICMP
  - **Ping**: sends series of echo request messages and provides statistics on roundtrip times and packet loss
  - **Traceroute**: sends series ICMP packets with increasing TTL value to discover routes

IP Addressing

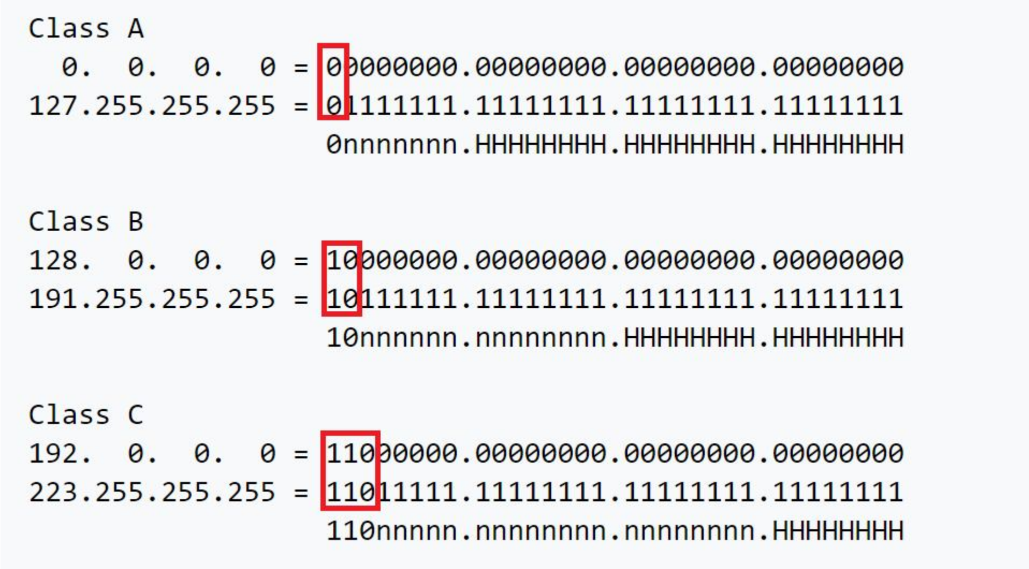
- IP address: 32-bit identifier for host, router interface
- Interface: connection between host/router and physical link
  - router's typically have multiple interfaces
  - host typically has one or two interfaces (e.g., wired Ethernet, wireless 802.11)
- IP addresses associated with each interface



```
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.77.154  netmask 255.255.255.0  broadcast 192.168.77.255
        inet6 fe80::20c:29ff:fe1b:b38b  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:1b:b3:8b  txqueuelen 1000  (Ethernet)
        RX packets 133  bytes 19915 (19.4 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 64  bytes 9304 (9.0 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 3396  bytes 1215405 (1.1 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 3396  bytes 1215405 (1.1 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Classful Addressing Definition

- Class A: 0.0.0.0 - 127.255.255.255
- Class B: 128.0.0.0 - 191.255.255.255
- Class C: 192.0.0.0 - 223.255.255.255



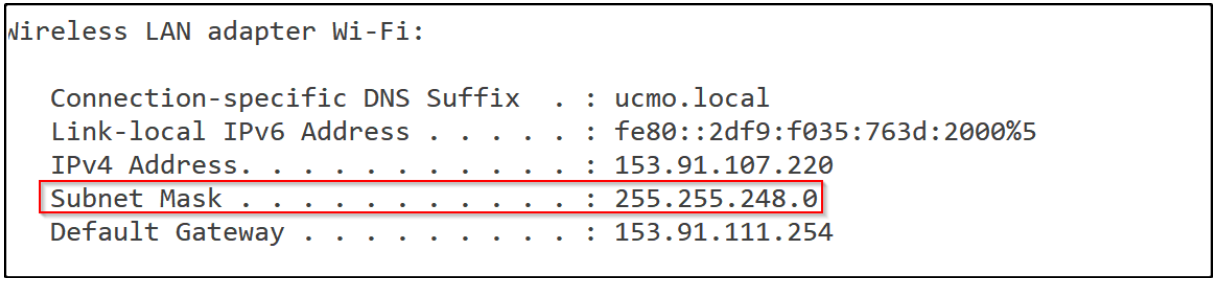
```
Class A
  0.   0.   0.   0 = 00000000.00000000.00000000.00000000
127.255.255.255 = 01111111.11111111.11111111.11111111
                  0nnnnnnn.HHHHHHHH.HHHHHHHH.HHHHHHHH

Class B
128.   0.   0.   0 = 10000000.00000000.00000000.00000000
191.255.255.255 = 10111111.11111111.11111111.11111111
                  10nnnnnn.nnnnnnnn.HHHHHHHH.HHHHHHHH

Class C
192.   0.   0.   0 = 11000000.00000000.00000000.00000000
223.255.255.255 = 11011111.11111111.11111111.11111111
                  110nnnnn.nnnnnnnn.nnnnnnnn.HHHHHHHH
```

Special IP Addresses

- Private IP Addresses
  - 10.0.0.0/8, 10.0.0.0 – 10.255.255.255
  - 172.16.0.0/12, 172.16.0.0 – 172.31.255.255
  - 192.168.0.0/16, 192.168.0.0 – 192.168.255.255

- Loopback Address (localhost)
  - 127.0.0.1

An Example



```
Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . : ucmo.local
   Link-local IPv6 Address . . . . . : fe80::2df9:f035:763d:2000%5
   IPv4 Address. . . . . . . . . . . : 153.91.107.220
   Subnet Mask . . . . . . . . . . . : 255.255.248.0
   Default Gateway . . . . . . . . . : 153.91.111.254
```

- 255.255.248.0 - 11111111.11111111.11111000.00000000
- 153.91.107.220 -10010111.01011011.01101011.11011100

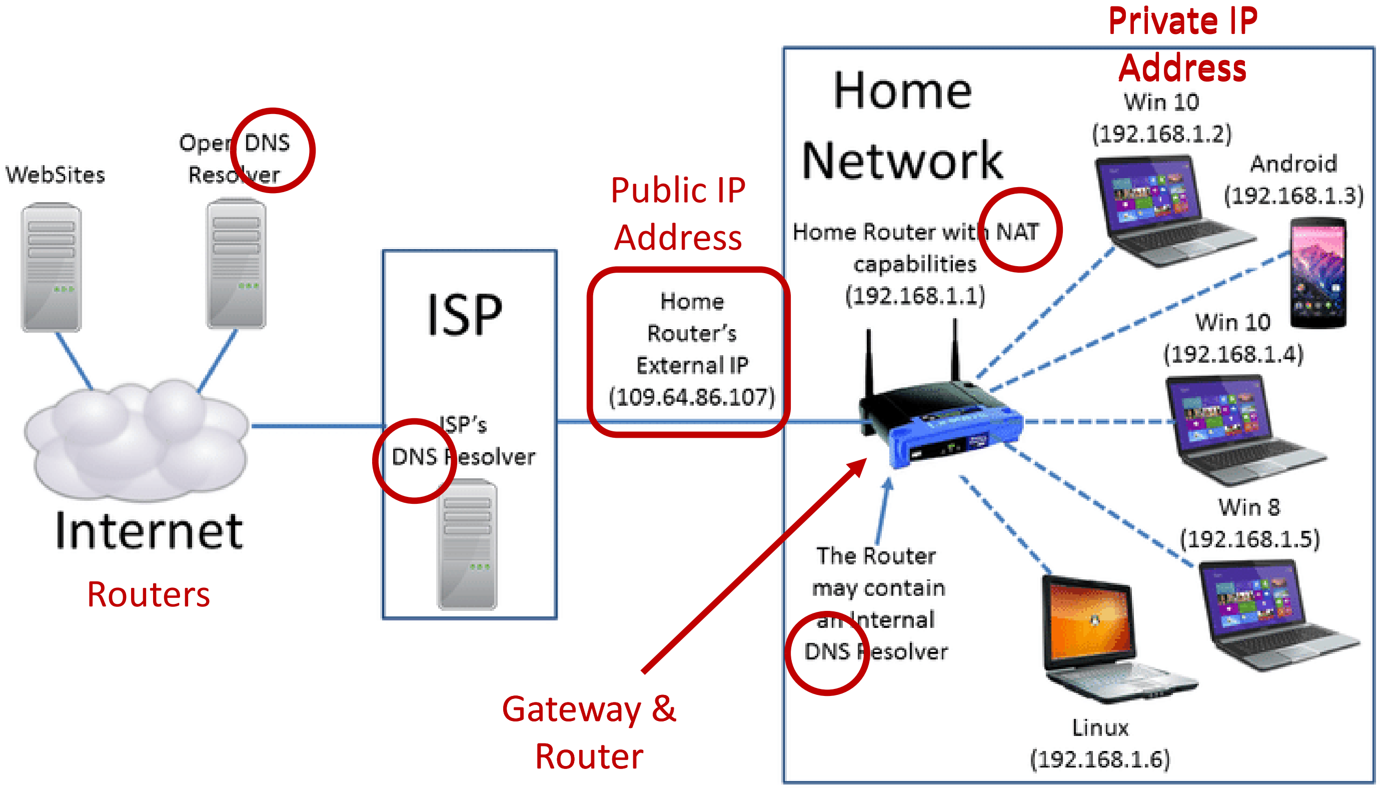
- Address range
- 10010111.01011011.01101000.00000000 - 153.91.104.0
- 10010111.01011011.01101111.11111111 - 153.91.111.255

How Hosts Get IP Addresses

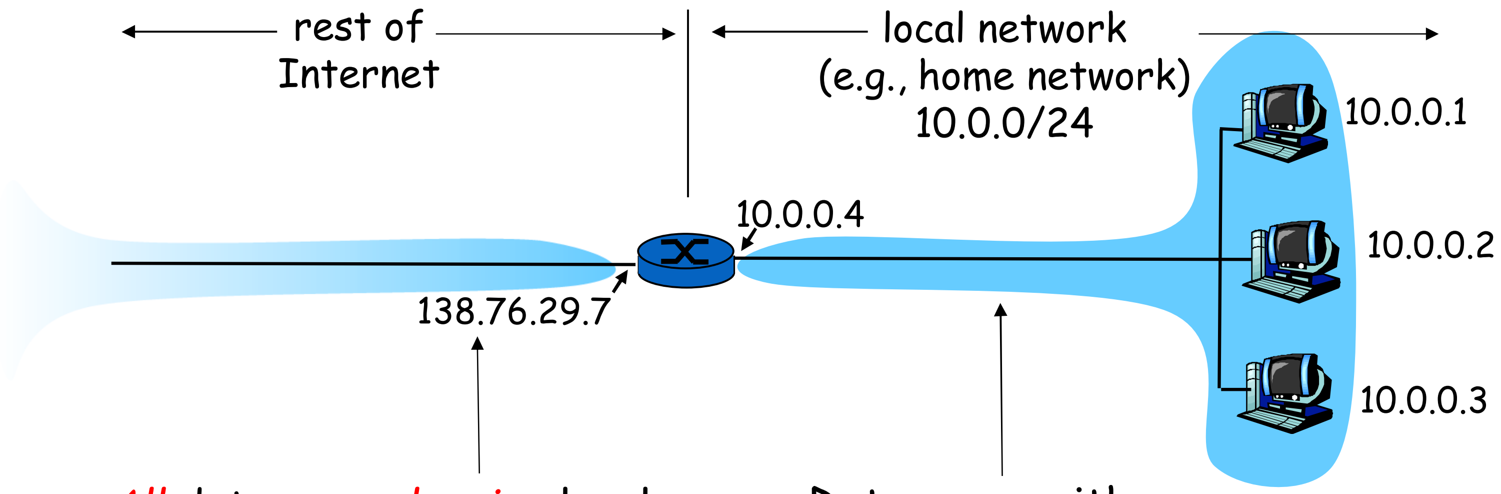
- Manually assign IP address to host
  - **$ sudo ip addr add 10.10.10.10/24 dev eth0**
  - **$ sudo ifconfig eth0 192.168.60.3/24 up**

- Automatically assign IP address to host
  - DHCP – Dynamic Host Configuration protocol

Private IP Address & NAT



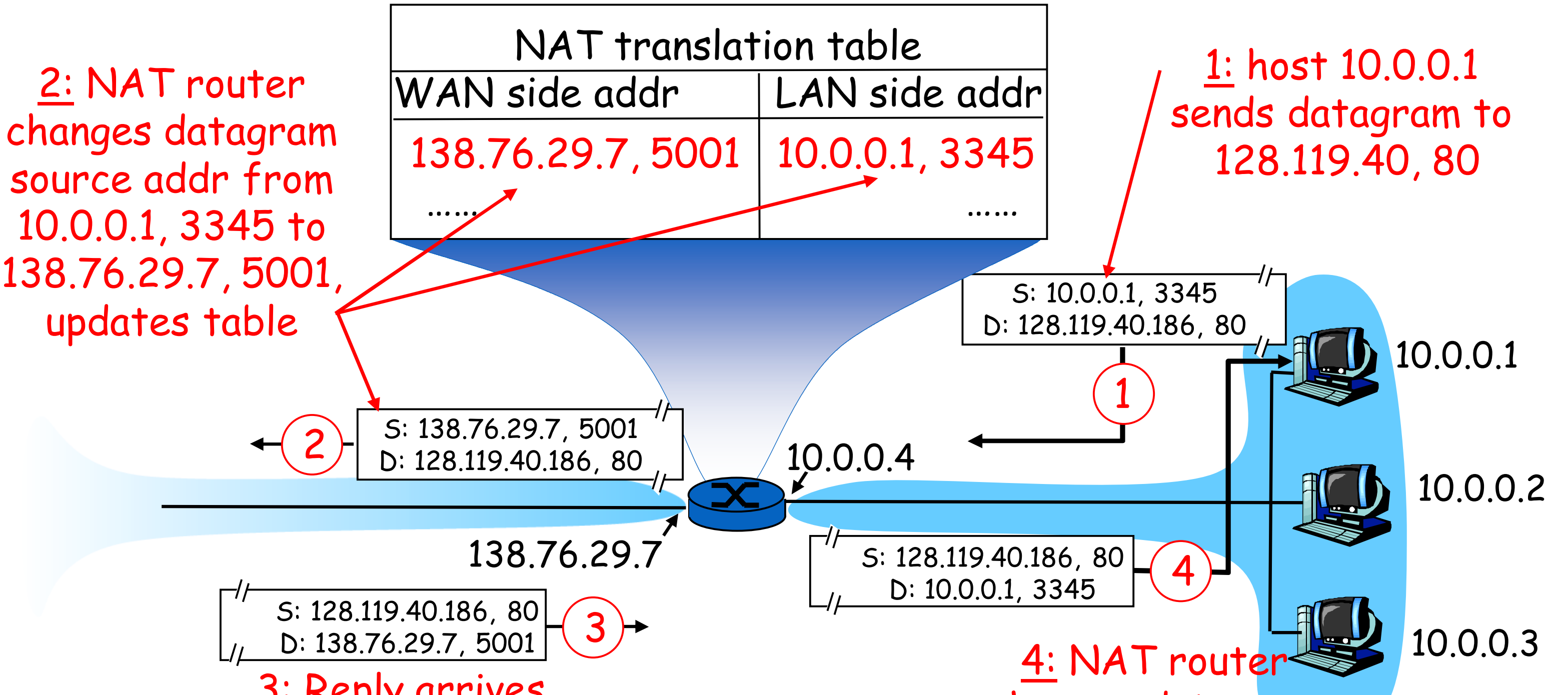
NAT: Network Address Translation



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



NAT translation table

WAN side addr	LAN side addr
138.76.29.7, 5001	10.0.0.1, 3345
……	……

1: host 10.0.0.1 sends datagram to 128.119.40, 80

2: NAT router changes datagram source addr from 10.0.0.1, 3345 to 138.76.29.7, 5001, updates table

3: Reply arrives dest. address: 138.76.29.7, 5001

4: NAT router changes datagram dest addr from 138.76.29.7, 5001 to 10.0.0.1, 3345

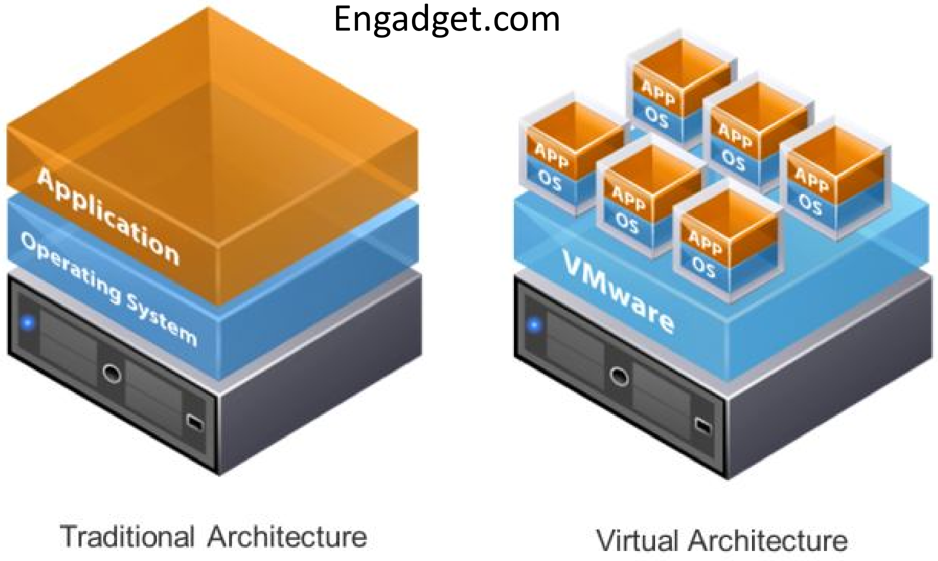
Installing VMware

- VMware Workstation 17 Pro download link
  - ❖ https://e5.onthehub.com/WebStore/ProductsByMajorVersionList.aspx?ws=ac2dddd5-d02e-de11-a497-0030485a8df0&vsro=8&JSEnabled=1
  - ❖ You will receive your login id and password through your UCM email （next week）
  - ❖ If you use MacOS, please download VMware Fusion 13 Pro

What is VMware

- A virtual machine environment
- Emulates CPU and various PC hardware components such as memory, network adapters, hard drives all in software
- Single host operating system
- One or more guest operating systems

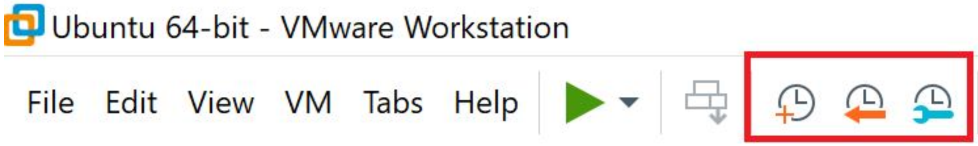
Engadget.com



VMware Machines

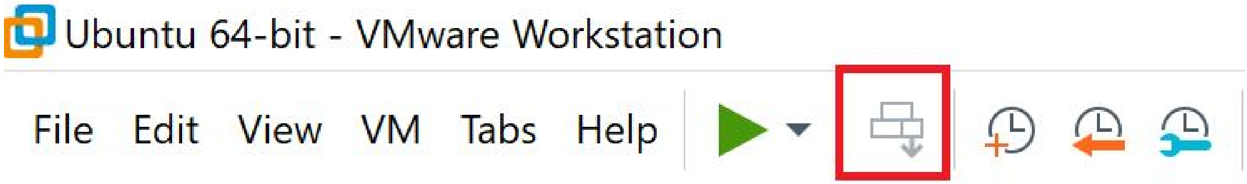
- VMware machines consist of files in the host operating system, typically grouped into a single directory for each virtual machine

- **.vmx**: virtual machine's configuration
- **.nvram**: store the state of virtual machines BIOS
- **.vmdk**: stores virtual disk files, the hard drive image of the virtual machine
- **.vmss**: suspended state file, for a paused virtual machine
- **.vmsn**: snapshot file, taking a snapshot of the system state for restoring it later


Ubuntu 64-bit - VMware Workstation

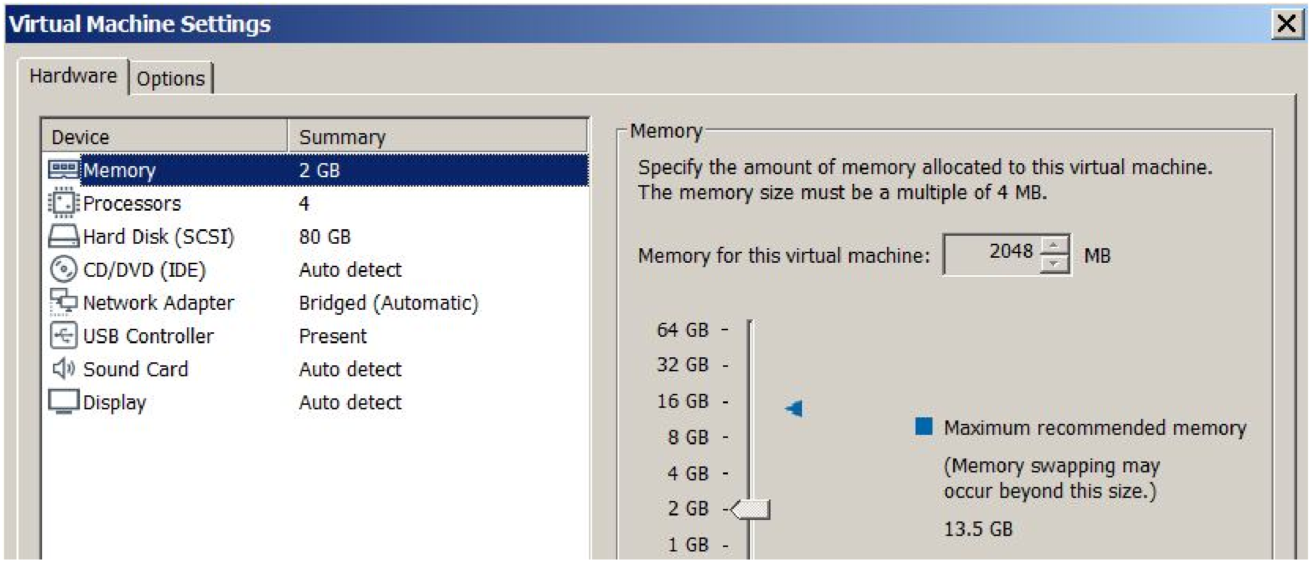
Shortcut Keys

- You can hit CTRL+ALT to jump out of virtual machine back into the host
- If a certain VMware is stuck, stop and replay it.
- To send virtual machine a CTRL+ALT+DEL, you need to go to the VMware window and select VM → Send CTRL+ALT+DEL



VMware Configuration Options

- To adjust any of the virtual hardware settings of a guest operating system, go to **VM → Settings**



Virtual Machine Settings

Hardware | Options

Device	Summary
Memory	2 GB
Processors	4
Hard Disk (SCSI)	80 GB
CD/DVD (IDE)	Auto detect
Network Adapter	Bridged (Automatic)
USB Controller	Present
Sound Card	Auto detect
Display	Auto detect

Memory

Specify the amount of memory allocated to this virtual machine. The memory size must be a multiple of 4 MB.

Memory for this virtual machine: 2048 MB

■ Maximum recommended memory

(Memory swapping may occur beyond this size.)

13.5 GB

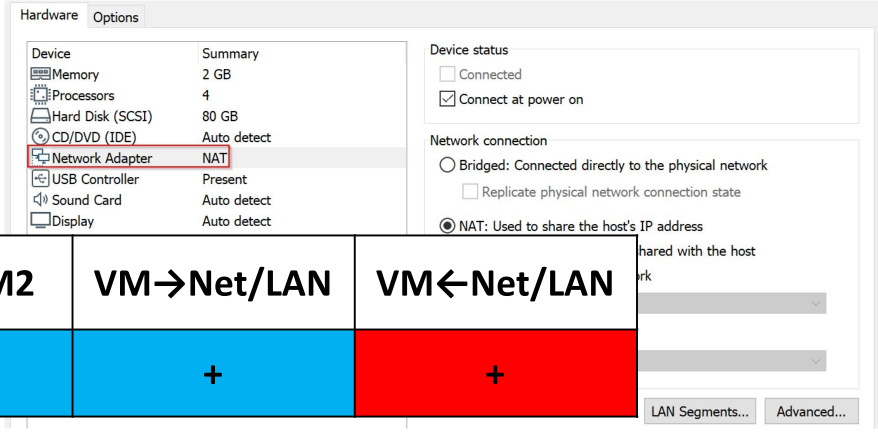
VMware Network Options

- Virtual machine can use one of the three network options
- **Host-only network:** the virtual machine will be able to communicate with other virtual machines in the host-only network as well as the host machine itself. It will not be able to send or receive any traffic with the local network or internet
- **NAT:** the host acts as a NAT device, which the virtual machines sit behind. All packets get their source IP translated so that they appear to have come from the host instead of the guest OS

Mode	**VM→Host**	**VM←Host**	**VM1↔VM2**	**VM→Net/LAN**	**VM←Net/LAN**
Host-only	**+**	**+**	**+**	–	–
NAT	**+**	Port forward	**+**	**+**	Port forward

VMware Network Options

- **Bridged network:** the host and virtual machines behave as though they are sitting next to each other on a switch
  - ❖Introduce virtual machine MAC address on the LAN
  - ❖Put host network interface in promiscuous mode (to capture traffic destined for the virtual machines)



Hardware | Options

Device	Summary
Memory	2 GB
Processors	4
Hard Disk (SCSI)	80 GB
CD/DVD (IDE)	Auto detect
Network Adapter	NAT
USB Controller	Present
Sound Card	Auto detect
Display	Auto detect

Device status

□ Connected

☑ Connect at power on

Network connection

○ Bridged: Connected directly to the physical network

□ Replicate physical network connection state

● NAT: Used to share the host's IP address

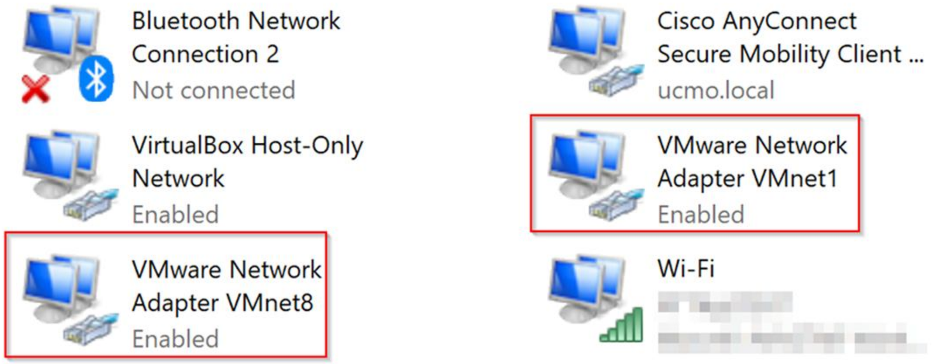
hared with the host

rk

Mode	VM→Host	VM←Host	VM1↔VM2	VM→Net/LAN	VM←Net/LAN
Bridged	+	+	+	+	+

VMware Networking

- In your **host OS**, do not alter virtual adapters unless you really know what you are doing.
  - ❖VMnet0: is used for bridged networking
  - ❖VMnet1: is used for **host-only** networking
  - ❖VMnet8: is used for **NAT**
- Do not configure them for DHCP or hard coded IP addresses



Bluetooth Network Connection 2
Not connected

Cisco AnyConnect Secure Mobility Client ...
ucmo.local

VirtualBox Host-Only Network
Enabled

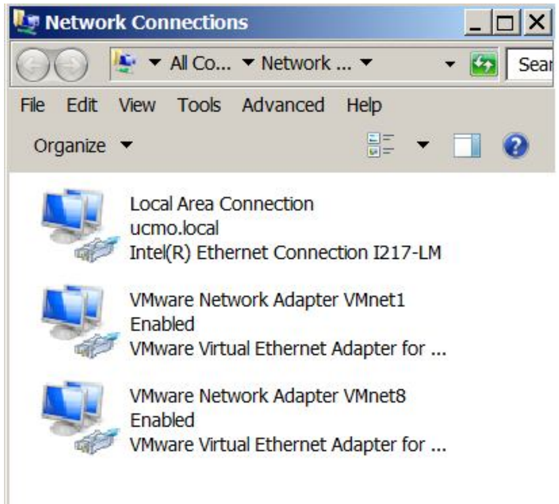
VMware Network Adapter VMnet1
Enabled

VMware Network Adapter VMnet8
Enabled

Wi-Fi
[redacted]

Setting Windows Host for Host-only Communication

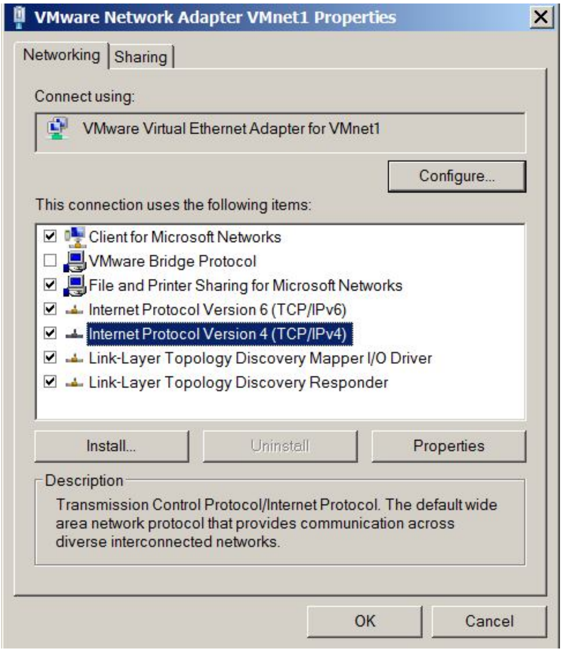
- In the Windows host OS, run the following command as an admin (an elevated shell) to bring up the network adapters
- **C:\> ncpa.cpl**



Local Area Connection
ucmo.local
Intel(R) Ethernet Connection I217-LM

VMware Network Adapter VMnet1
Enabled
VMware Virtual Ethernet Adapter for ...

VMware Network Adapter VMnet8
Enabled
VMware Virtual Ethernet Adapter for ...

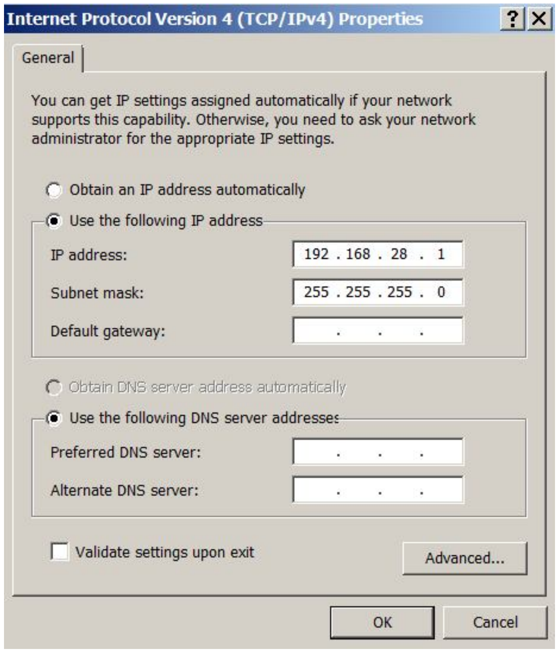


Connect using:
VMware Virtual Ethernet Adapter for VMnet1

This connection uses the following items:

- ☑ Client for Microsoft Networks
- ☐ VMware Bridge Protocol
- ☑ File and Printer Sharing for Microsoft Networks
- ☑ Internet Protocol Version 6 (TCP/IPv6)
- ☑ Internet Protocol Version 4 (TCP/IPv4)
- ☑ Link-Layer Topology Discovery Mapper I/O Driver
- ☑ Link-Layer Topology Discovery Responder

Description
Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.



You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically
● Use the following IP address:

IP address:	192 . 168 . 28 . 1
Subnet mask:	255 . 255 . 255 . 0
Default gateway:	. . .

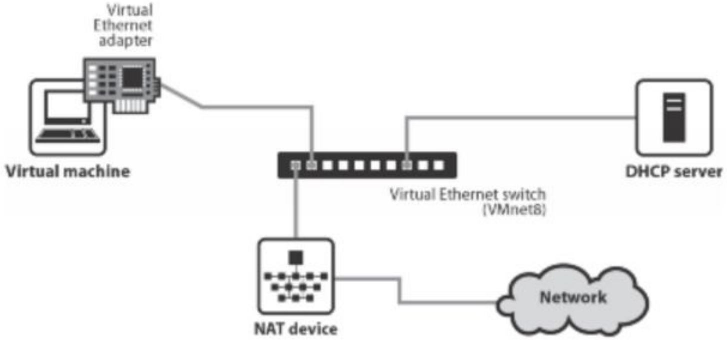
○ Obtain DNS server address automatically
● Use the following DNS server addresses:

Preferred DNS server:	. . .
Alternate DNS server:	. . .

☐ Validate settings upon exit

VMware NAT Device

- A DHCP server is automatically installed when you install VMware Workstation. The virtual DHCP server serves NAT and host-only networks
- The DHCP server dynamically allocates IP addresses in the range of <net>.128 through <net>.254
- IP addresses <net>.3 through <net>.127 can be used for static IP addresses
- IP address <net>.1 is reserved for the **host adapter**; <net>.2 is reserved for the **NAT device**
- VMware Workstation always uses a Class C address for NAT networks
  - Class C: 192.0.0.0 - 223.255.255.255
- In the default configuration, computers on the external network **cannot** initiate connections to the virtual machine on the NAT network (basic-level firewall protection)



DNS on the NAT Network

- DNS (Domain Name Service) is a system which maintains a relationship between Internet Protocol (IP) addresses and domain names
  - E.g.) 153.91.1.10 => www.ucmo.edu
- The NAT device acts as a DNS server for the virtual machines on the VMware NAT network
- In the DHCP response, the NAT device instructs the virtual machine to use the IP address <net>.2 as the default gateway and DNS server
- However, the virtual machines can be statically configured to use another DNS server other than the NAT device

Kali Linux

- Download Kali Linux
    - https://www.kali.org/get-kali/#kali-virtual-machines

- Download the 64bit image not the Torrent

- If your OS is 32 bit, download the 32 bit image

- **Default username:** kali
- **Default password:** kali

- Change your password immediately. You do not want your classmates to hack into your Kali box

Ubuntu 8.10 Target

- Download the VMware image from the Google Drive

Windows XP Target

- Our best friend in this course
- Download the VMware image from the Google Drive

Creating the Windows 7 Target

- Windows 7 image download
  - ❖Download from Google Drive

Windows 10 Target

- Download the VMware image from the Google Drive

Note on Nomenclature

- **Testing machines:** Systems used by the penetration tester or ethical hacker to evaluate the security of other machines. We also call them **attack machines**

- **Target machines:** Systems whose security stance is being evaluated. We also call them **victim machines**

Commands Prompts

- Thought this course, we work with numerous different shells
  - ❖ And frequently change between them
  - ❖ On different systems (Windows vs Linux)
  - ❖ On the same system (within OS and with Metasploit)

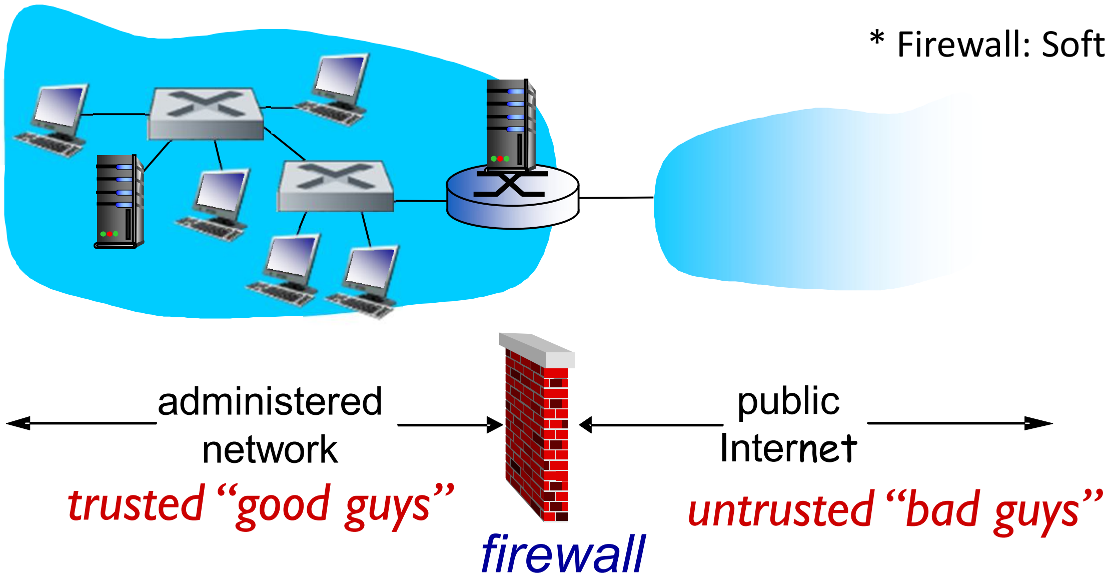
- Please make sure you enter commands at the right prompt
  - ❖ **Windows cmd.exe:** C:\>
  - ❖ **Windows PowerShell:** PS C:\>
  - ❖ **Linux:** # or $
  - ❖ **Msfconsole:** msf >
  - ❖ **Meterpreter:** meterpreter >
  - ❖ **Python: >>>**
  - ❖ **Empire: (Empire) >**
  - ❖ ***And more*** …

Firewall

firewall

isolates organization's internal net from larger Internet, allowing some packets to pass, blocking others

* Firewall: Software or Hardware



administered network

trusted "good guys"

firewall

public Internet

untrusted "bad guys"

* NAT can act as a firewall

Firewall Types

- Packet filtering
  - ❖firewall looks at the header information of the packets to determine legitimate traffic
  - ❖Looks at a single packet to make a filtering decision
  - ❖Packets are forwarded through the device

- Stateful packet filtering
  - ❖Determine the legitimacy of traffic based on the state of the connection from which the traffic originated
  - ❖Looks at a packet in relationship to other packets
  - ❖Packets are forwarded through the device

Firewall Concerns

- If your testing machines are firewalled from the internet, your attack might be blocked or neutered
  - ❖NAT or PAT
    - Scan could fill up tables, dropping packets
    - Attempts at reverse shell connections from target to attack system will not be carried back in
  - ❖HTTP proxy
    - Exploit encoding could be altered, breaking exploit
  - ❖Application-level inspections
    - May drop packets that don't conform to app-level protocol
    - Or try to clear up protocol

Firewall Concerns Continued

- Not using a network firewall and even a personal firewall on the testing network and testing machines

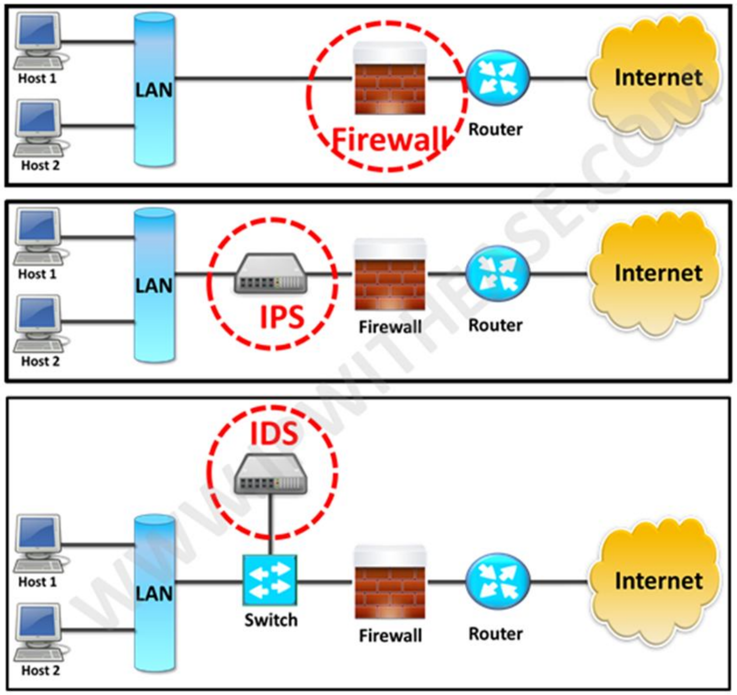
- Make sure to thoroughly harden the testing machines

- Shut off unneeded services

- Increase security settings but not to the point that you inhibit the functionality of your testing tools
  - ❖LM Challenge-Response, NTLMv1 and NTLMv2

IDS and IPS

- **Intrusion Detections Systems (IDS)**
  - ❖ Passive in nature. It senses a questionable activity occurring and passively reacts by sending notification to an admin signifying something is wrong
- **Intrusion Prevention Systems (IPS)**
  - ❖ Proactive and preventive. Senses potential malicious activity on the network and takes steps to prevent further damage and thwart further attacks



Iptables Firewall in Linux (Access Control)

- Rules are arranged in hierarchical structure as shown in the table.

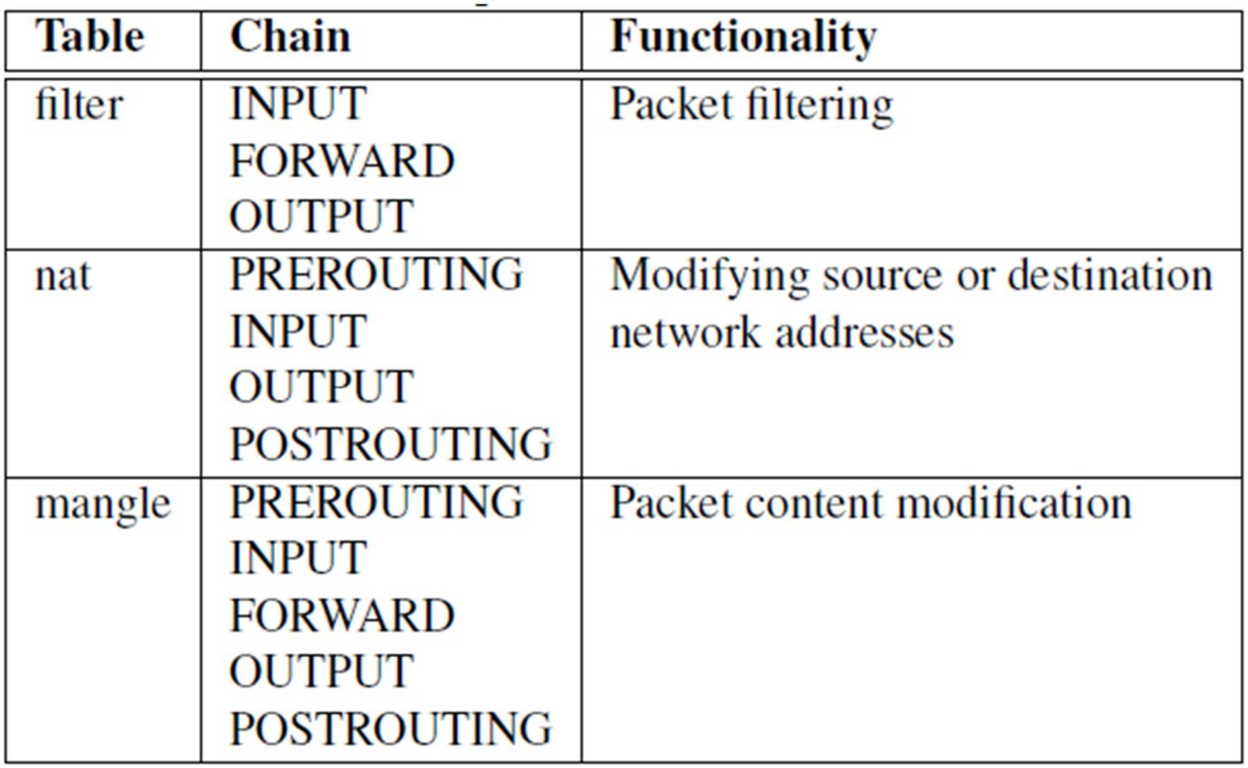


Table	Chain	Functionality
filter	INPUT FORWARD OUTPUT	Packet filtering
nat	PREROUTING INPUT OUTPUT POSTROUTING	Modifying source or destination network addresses
mangle	PREROUTING INPUT FORWARD OUTPUT POSTROUTING	Packet content modification

Tables and Chains

- Filter
  - The Filter table is the most frequently used one. It decides who gets in and out of your network
- Network Address Translation (NAT)
  - This table contains NAT (Network Address Translation) rules for routing packets to networks that cannot be accessed directly. When the destination or source of the packet has to be altered, the NAT table is used
- Mangle (Modification of the IP Packet)
  - The Mangle table adjusts the IP header properties of packets

Packet Filtering: Using **iptables**

- General format
  $ iptables [-t filter] –A INPUT <rule> -j <target>

- Specifying rules
  - -i interface (incoming)
  - -o interface (outgoing)
  - -s source IP (/mask)
  - -d destination IP (/mask)
  - -p protocol (protocol specific rule)
    - -p tcp --dport 21:23
    - -p icmp --icmp-type echo-request

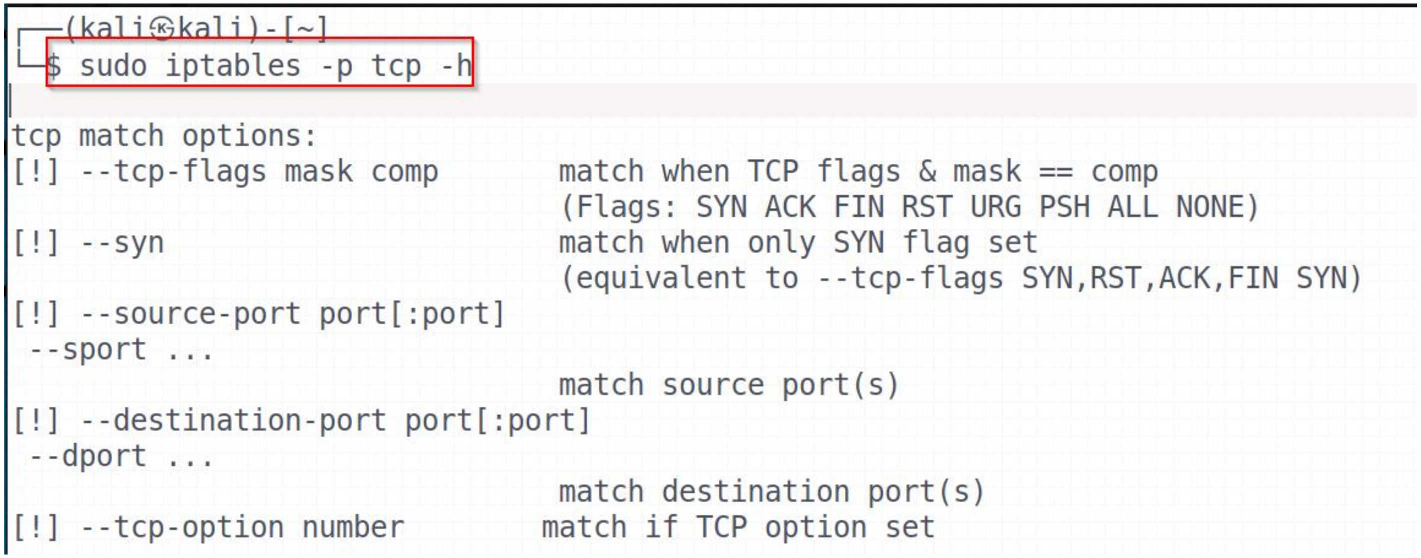
- Ex) $ iptables -A INPUT -p icmp --icmp-type echo-request –j ACCEPT

Targets

- A target is what happens after a packet matches a rule criteria
- With terminating targets, a packet is evaluated immediately and is not matched against another chain. The terminating targets in Linux iptables are
  - **Accept** – this rule accepts the packets to come through the iptables firewall
  - **Drop** – the dropped package is not matched against any further chain. When Linux iptables drop an incoming connection to your server, the person trying to connect does not receive an error. It appears as if they are trying to connect to a non-existing machine
  - **Reject** – the iptables firewall rejects a packet and sends an error to the connecting device

Getting Help

- $ sudo iptables -h
- To get help on a particular item



```
┌──(kali㉿kali)-[~]
└─$ sudo iptables -p tcp -h

tcp match options:
[!] --tcp-flags mask comp        match when TCP flags & mask == comp
                                 (Flags: SYN ACK FIN RST URG PSH ALL NONE)
[!] --syn                        match when only SYN flag set
                                 (equivalent to --tcp-flags SYN,RST,ACK,FIN SYN)
[!] --source-port port[:port]
 --sport ...
                                 match source port(s)
[!] --destination-port port[:port]
 --dport ...
                                 match destination port(s)
[!] --tcp-option number         match if TCP option set
```

Other iptables Commands

- $ iptables [-t table] -[ALF] chain
- $ iptables [-t table] -I chain [rulenum]
- $ iptables [-t table] -P chain target
- **-A:** Append one or more rules **to the end** of the selected chain
- **-I :** Insert one or more rules in the selected chain as the given rule number. If the rule number is 1, the rule or rules are inserted at the head of the chain. This is also the default if no rule number is specified
- **-L:** List all rules in the selected chain. If no chain is selected, all chains in the table are listed
- **-F:** Flush the selected chain (all the chains in the table if none is given)
- **-P:** Set the policy for the chain to the given target
- Example - allow incoming traffic on multiple TCP ports
  - $ iptables -A INPUT -p tcp -m multiport --dports 110,143,993,995 -j ACCEPT

Exercises

- Block in-coming ICMP echo requests (ping)
- Block in-coming SSH request
- Block out-going web traffic

Scrub Test Machines between Tests

- Don't leave results on your testing machines for longer than necessary

- Merely deleting the files isn't enough

- At test completion, thoroughly scrub test machines
  - ❖ The Linux shred commands overwrite 3 times by default. Use –n [N] to force overwrite N times
  - ❖ The Windows cipher /w:[file] command overwrite 3 times