

# CSCI369 Ethical Hacking

## Lecture 3-1 ARP and ARP Poisoning

A/Prof Joonsang Baek

School of Computing and Information Technology



This slide is copyrighted. It must not be distributed without permission from UOW

# ARP (Address Resolution Protocol)

- ARP

➤ ARP is a Data Link protocol (Layer 2).

OSI (Open Source Interconnection) 7 Layer Model

Layer	Application/Example	Central Device/Protocols	DOD4 Model
<b>Application (7)</b> Serves as the window for users and application processes to access the network services.	<b>End User layer</b> Program that opens what was sent or creates what is to be sent Resource sharing • Remote file access • Remote printer access • Directory services • Network management	<b>User Applications</b> SMTP	<b>G A T E W A Y</b> Process
<b>Presentation (6)</b> Formals the data to be presented to the Application layer. It can be viewed as the "Translator" for the network.	<b>Syntax layer</b> encrypt & decrypt (if needed) Character code translation • Data conversion • Data compression • Data encryption • Character Set Translation	JPEG/ASCII EBDIC/TIFF/GIF PICT	
<b>Session (5)</b> Allows session establishment between processes running on different stations.	<b>Synch &amp; send to ports</b> (logical ports) Session establishment, maintenance and termination • Session support - perform security, name recognition, logging, etc.	<b>Logical Ports</b> RPC/SQL/NFS NetBIOS names	
<b>Transport (4)</b> Ensures that messages are delivered error-free, in sequence, and with no losses or duplications.	<b>TCP</b> Host to Host, Flow Control Message segmentation • Message acknowledgement • Message traffic control • Session multiplexing	<b>Routers</b> TCP/SPX/UDP IP/IPX/ICMP	Host to Host
<b>Network (3)</b> Controls the operations of the subnet, deciding which physical path the data takes.	<b>Packets</b> ("letter", contains IP address) Routing • Subnet traffic control • Frame fragmentation • Logical-physical address mapping • Subnet usage accounting		Internet
<b>Data Link (2)</b> Provides error-free transfer of data frames from one node to another over the Physical layer.	<b>Frames</b> ("envelopes", contains MAC address) [NIC card — Switch — NIC card] (end to end) Establishes & terminates the logical link between nodes • Frame traffic control • Frame sequencing • Frame acknowledgment • Frame delimiting • Frame error checking • Media access control	<b>Switch Bridge WAP</b> PPP/SLIP	Can be used on all layers
<b>Physical (1)</b> Concerned with the transmission and reception of the unstructured raw bit stream over the physical medium.	<b>Physical structure</b> Cables, hubs, etc. Data Encoding • Physical medium attachment • Transmission technique - Baseband or Broadband • Physical medium transmission Bits & Volts	<b>Hub</b> Land Based Layers	Network

ARP



UNIVERSITY  
OF WOLLONGONG  
AUSTRALIA

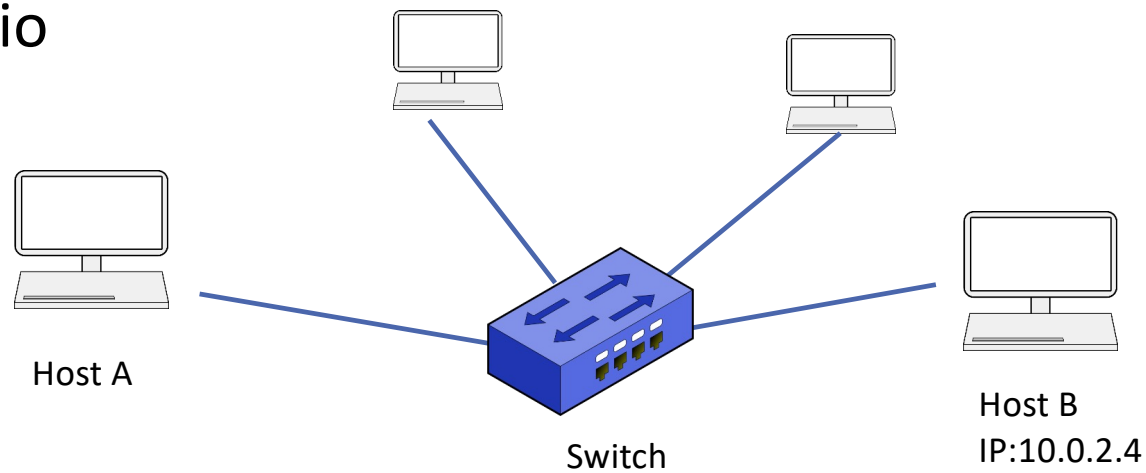
This slide is copyrighted. It must not be distributed without permission from UOW

# ARP Basics

- ARP (Address Resolution Protocol)
  - A network protocol used to discover the hardware (**MAC**) address of a host from an IP address.
  - ARP is used on Ethernet LANs when hosts want to communicate with each other and they should know each other's MAC address.
  - It is a simple request-reply protocol; ARP request messages are used to request the MAC address, while ARP reply messages are used to send the requested MAC address.

# ARP Basics

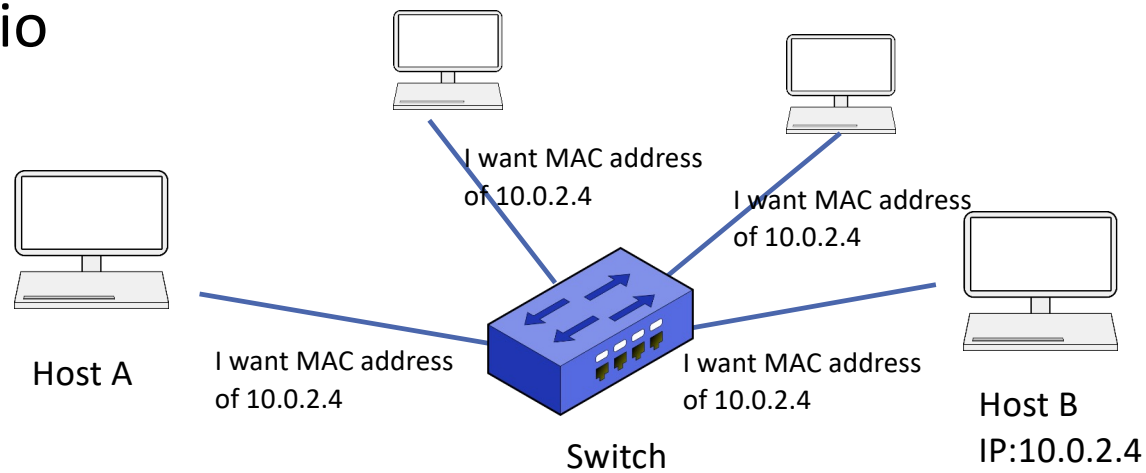
- Scenario



Host A wants to communicate with Host B with IP 10.0.2.4.  
Host A does not know Host B's MAC address.

# ARP Basics

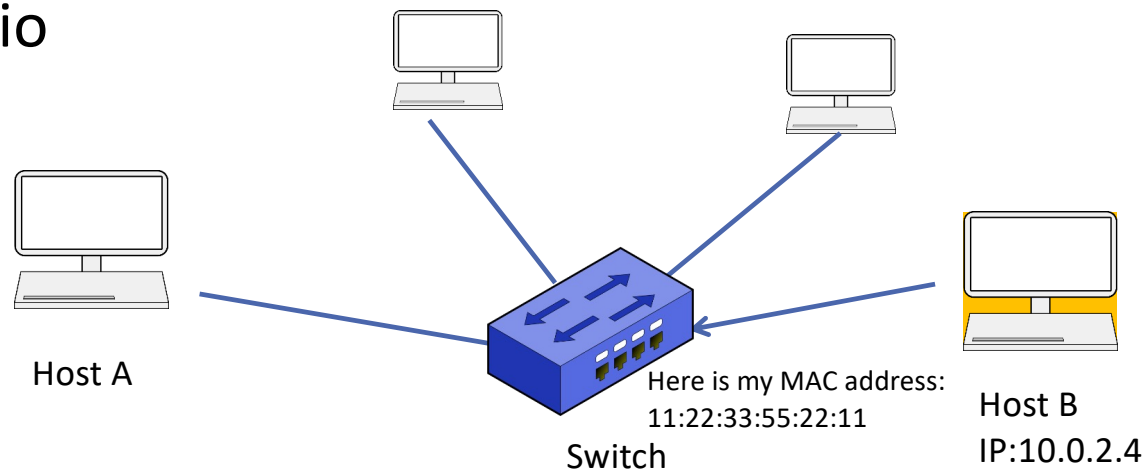
- Scenario



Host A sends **ARP request** to broadcast address. Switch will flood this request to all interfaces.

# ARP Basics

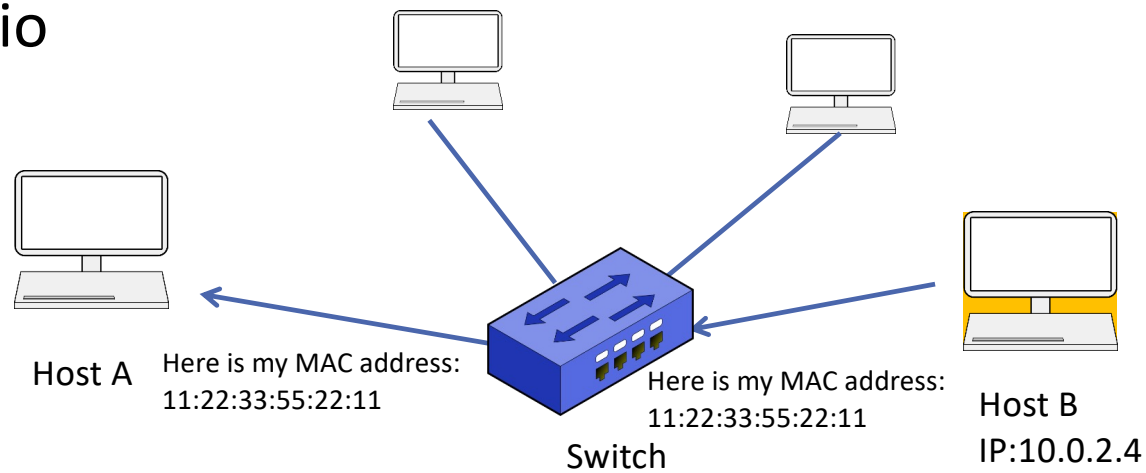
- Scenario



Once Host B receives this request, it processes the request and prepares **ARP reply containing MAC address of Host B.**

# ARP Basics

- Scenario



ARP reply will be relayed to Host A.

# ARP Poisoning – Preparation

- Features of ARP packet
  - ICMP can be filtered by a host's local firewall, while ARP requests cannot be blocked because ARP requests are not routed on a TCP/IP network. → ARP can be used to discover hosts that are directly connected to the same network hub or switch.
- Assumption
  - We assume that an attacker has obtained access to a target's internal network
    - ✓ For example, a hacker has gained access to our university network having obtained username/password of some student/staff



# ARP Basics

- `arp` command
  - This command is to display and modify a current **ARP cache**.
  - Each host will use the ARP cache first to resolve the address of the neighbor.
  - **-a** option will display the device name, IP address, **HW address (MAC address)**, HW type and network interface.
  - If the cache does not contain the information required to resolve the address then a request is sent to every device (machine) on the network.

# ARP Basics

- `netdiscover`

- A tool used to discover the connected clients to the current network interface.
- Shows basic information about the clients: IP and MAC address and the hardware manufacturers of the clients' network card.
- Passive mode: This mode does not generate any packet on the network, it just sniffs arp request on the network.
  - ✓ `netdiscover -i [INTERFACE] -p`
- Active mode: This mode allows to find nodes by sending arp requests
  - ✓ Command structure: `netdiscover -i [INTERFACE] -r [RANGE]`
- Note that RANGE should be given as CIDR notations like 10.0.2.1/24.

# ARP Scanning

- ARP host recovery
  - The Address Resolution Protocol (ARP) maps system's MAC address (hardware address) to its IP address.
  - An ARP can send ARP request to every host on a subnet: If an ARP reply is received, that host is considered "live".
  - As it operates **below** the layers of ICMP/TCP/UDP, it can bypass firewall, **the attacker needs to be located on the same local network.**
  - Ex) `arp-scan 192.169.8.2 - 192.169.8.10`

# ARP Scanning Example

- ARP Scanning can be visualized through Wireshark.

- ARP scan with Scapy

✓ `ans, unans = srp(Ether(dst="ff:ff:ff:ff:ff:ff") / ARP(pdst = ips), timeout = 2, iface = interface, inter = 0.1)`  
where `ips` is ip addresses such as “10.0.2.0/30” and `iface` is the network interface name such as “eth0”.

Source	Destination	Protocol	Length	Info
PcsCompu_22:...	Broadcast	ARP	42	Who has 10.0.2.0? Tell 10.0.2.6
PcsCompu_22:...	Broadcast	ARP	42	Who has 10.0.2.1? Tell 10.0.2.6
RealtekU_12:...	PcsCompu_22:a4:...	ARP	60	10.0.2.1 is at 52:54:00:12:35:00
PcsCompu_22:...	Broadcast	ARP	42	Who has 10.0.2.2? Tell 10.0.2.6
RealtekU_12:...	PcsCompu_22:a4:...	ARP	60	10.0.2.2 is at 52:54:00:12:35:00
PcsCompu_22:...	Broadcast	ARP	42	Who has 10.0.2.3? Tell 10.0.2.6
PcsCompu_7f:...	PcsCompu_22:a4:...	ARP	60	10.0.2.3 is at 08:00:27:7f:9f:d0



# ARP Scanning Example

- ARP addresses is cached in the OS. The `arp -a` command to view and modify the ARP table entries on the local computer.
- The command can be used to display all the known connected hosts on the target's local network segment (if they have been active and in the cache).

```
$ arp -a
Net to Media Table: IPv4
Device    IP Address                Mask      Flags      Phys Addr
-----
aggr557001 pan-SharedCompute-557-router.its.uow.edu.au 255.255.255.255
00:1b:17:00:01:26
igb0      scylla.cs.uow.edu.au 255.255.255.255 SPLA      00:21:28:f1:a2:dc
igb0      pan-VirtualInfra-553-router.its.uow.edu.au 255.255.255.255      00:1b
:17:00:01:26
```



# Man-In-the-Middle (MITM)

- MITM

- An attack where the attacker secretly relays and possibly modifies the communication between two parties, who believe they are directly communicating with each other.
- The attacker must be able to intercept all relevant messages passing between the two victims and inject new ones.

Alice  $\leftrightarrow$  Bob: Normal communication

Alice  $\leftrightarrow$  Charlie (attacker)  $\leftrightarrow$  Bob: MITM

# ARP Poisoning

- **ARP Poisoning (Sometimes called ARP Spoofing)**
  - An attacker can exploit the fact that
    - 1) ARP request/reply is trusted
    - 2) Clients can accept any responses even if they did not send a request

# ARP Poisoning

- Preliminary: Default gateway

- In general, a gateway is a network node that serves as an access point to another network.

- **The default gateway** is a device, such as a DSL router or cable router, that connects the local network to the public network (the Internet).

- In a home or small office environment:

- ✓ The default gateway router directly connects the local network to the public network.

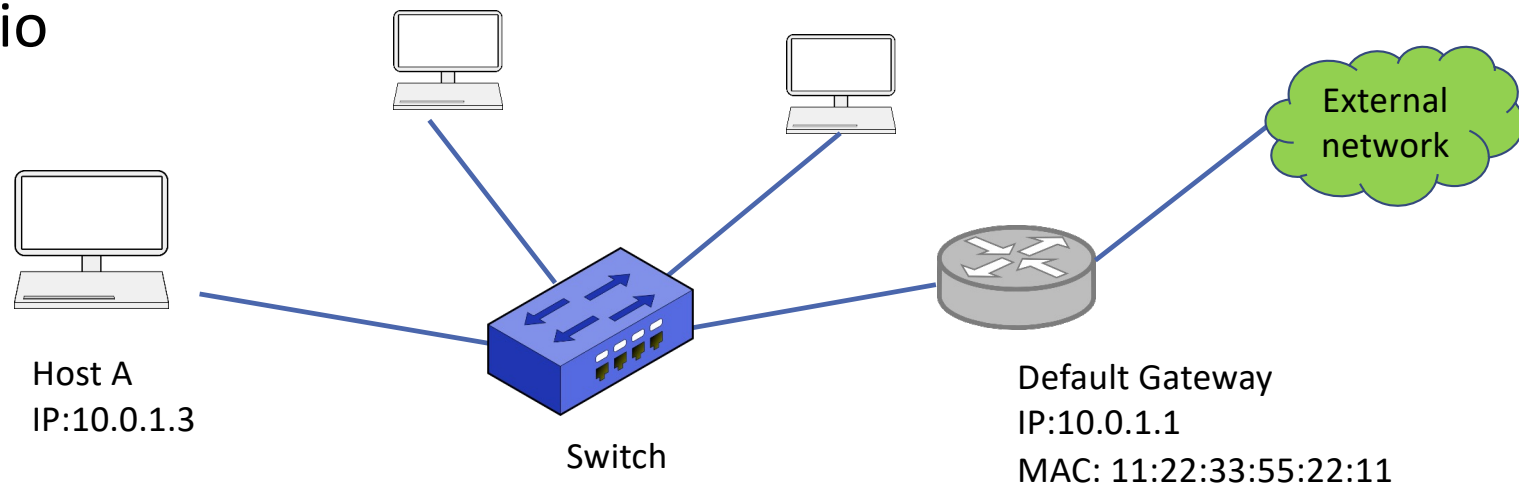
- In enterprise network environment:

- ✓ The default gateway router connects the local network to adjacent network, one hop closer to the public network.



# ARP Poisoning

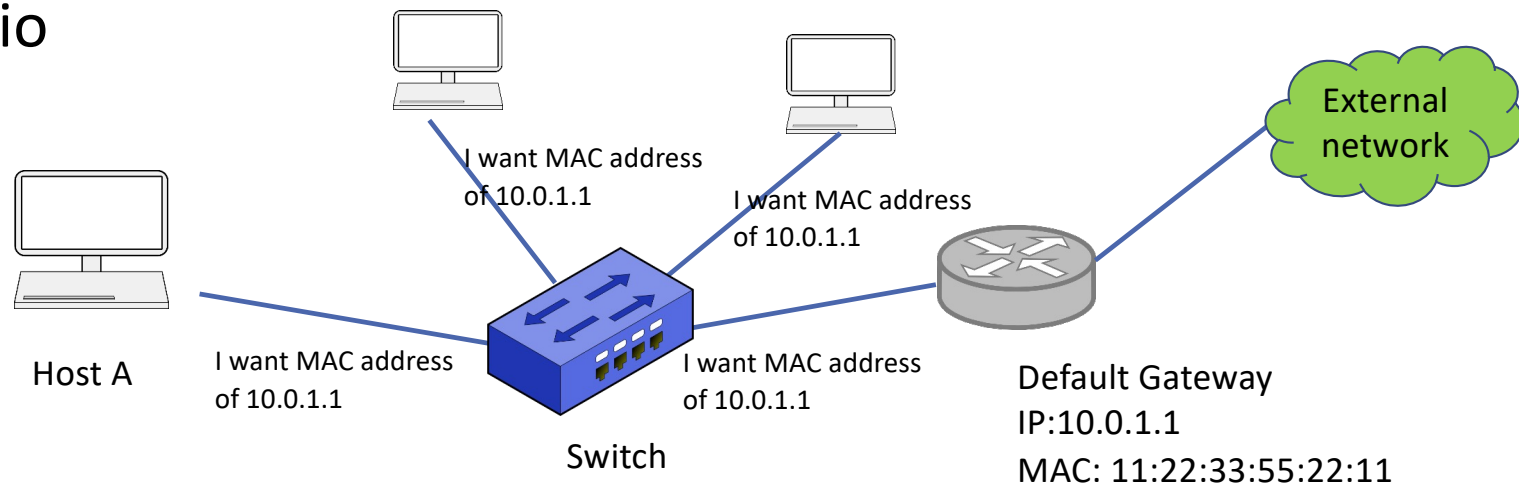
- Scenario



Host A wants to communicate with the external network through Default Gateway with IP 10.0.1.1. Host A does not know Default Gateway's MAC address.

# ARP Basics

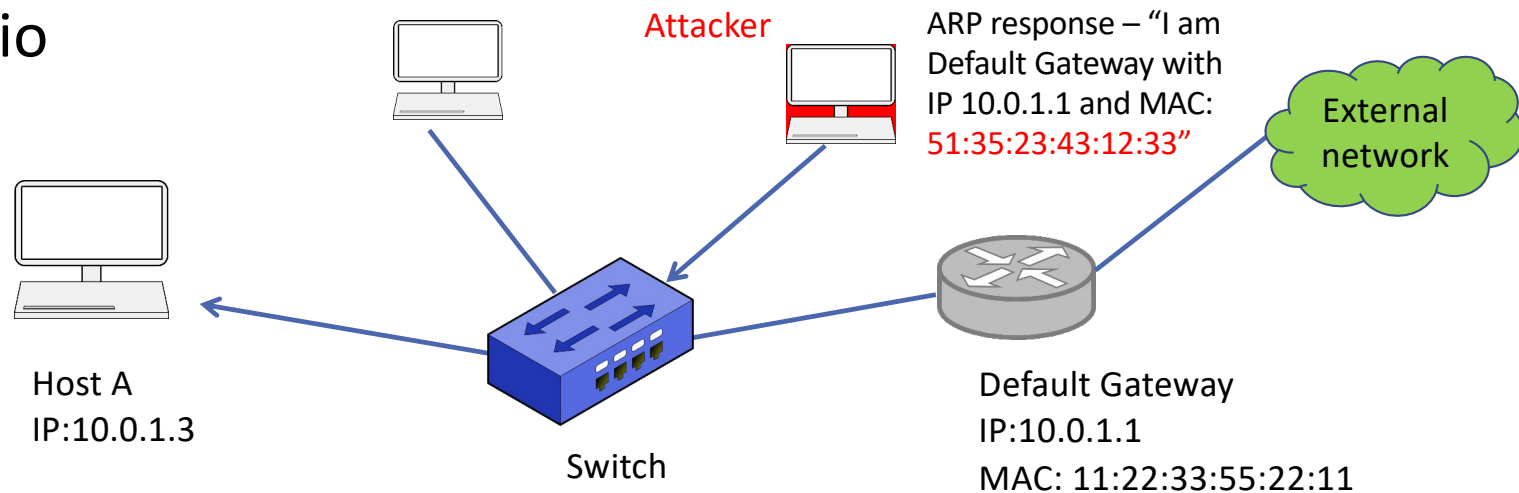
- Scenario



Host A sends **ARP request** to broadcast address. Switch will flood this request to all interfaces.

# ARP Poisoning

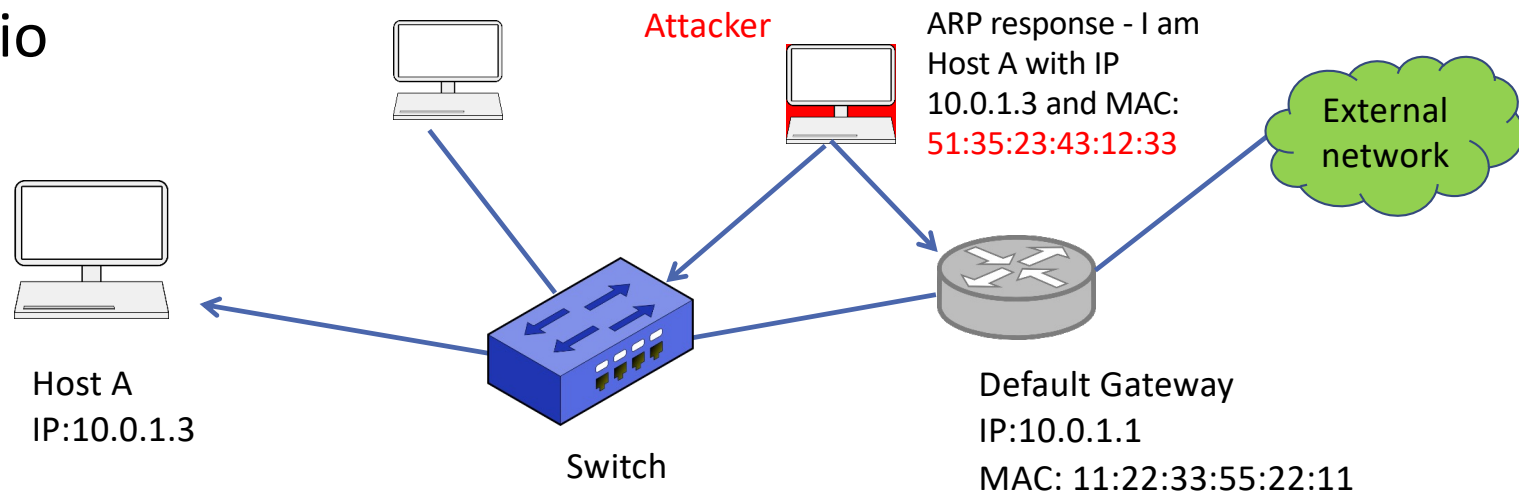
- Scenario



The attacker sends ARP response to Host A (through switch) claiming that it is a Default Gateway with the IP address 10.0.1.1 and **its own MAC**.

# ARP Poisoning

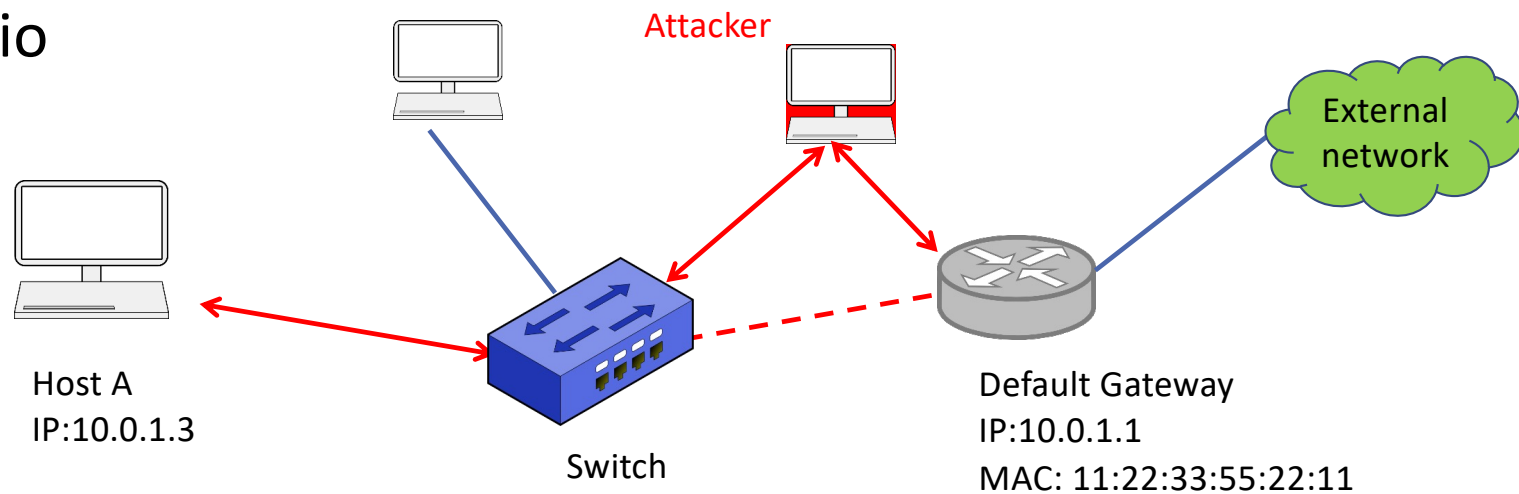
- Scenario



The attacker now sends ARP response to Default Gateway claiming that it is Host A with the (real) Host A IP address and **its own MAC**.

# ARP Poisoning

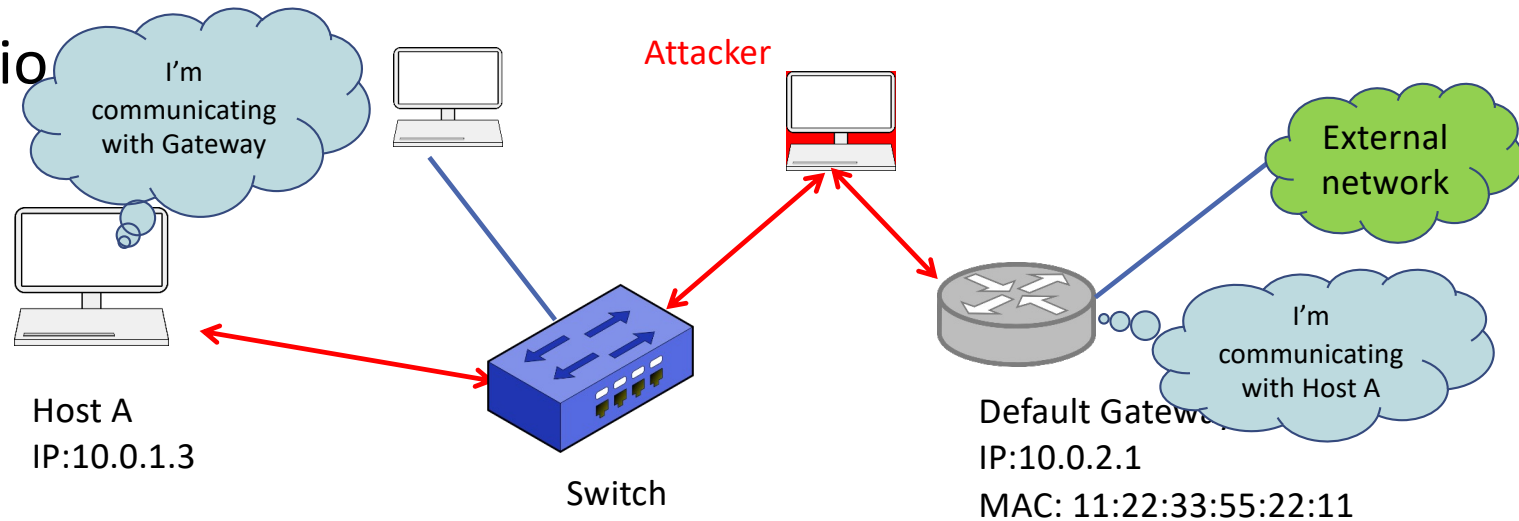
- Scenario



Host A sends its packets to the external network **via the attacker.**

# ARP Poisoning

- Scenario



Host A and Default Gateway believe that they are communicating each other, which is not true.

# ARP Poisoning

- After the ARP poisoning happens:
  - *The real gateway thinks that the attacker is Host A while Host A thinks that the attacker is the gateway.*
  - So the attacker's device is in the middle of the connection between Host A and the gateway → Every packet that is going to/from the client will have to go through the attacker's device first.

# Danger of ARP Poisoning

- ARP poisoning will redirect traffic to and from any client to the attacker's device
  - The attacker can read/modify/drop these packets in the traffic.
  - This allows the attacker to conduct more powerful attacks.
- It is very effective and dangerous, but it is difficult to protect against it.



# ARP Poisoning with Arpspoof

- How to perform ARP poisoning attack on Kali

- **Arpspoof** is a tool for performing ARP Poisoning attack

- ```
arpspoof -i [interface] -t [Target A] [Target B]
```

- Step 1: Tell the target that the attacker is the default gateway

- ```
arpspoof -i eth0 -t 10.0.1.3 10.0.1.1
```

- Step 2: Tell the default gateway that the attacker is the target

- ```
arpspoof -i eth0 -t 10.0.1.1 10.0.1.3
```

- Step 3: Enable IP forward to make packets go through the attacker's device.

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

# ARP Poisoning with Arpspoof

- How to check the attack has been successful
  - Run `arp -a` (on the target's machine) to check whether the MAC address of the default gateway has been changed
  - In the scenario above, Host A will see **51:35:23:43:12:33** as the **MAC address of Default Gateway**, whose real MAC address is **11:22:33:55:22:11**

# ARP Poisoning with Bettercap

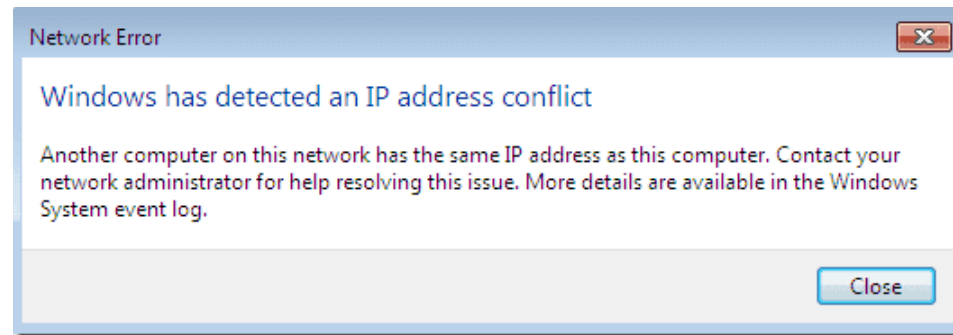
- Another method to perform ARP poisoning attack on Kali
  - Bettercap provides a nicer user interface to perform ARP poisoning (spoofing).
  - Bettercap Scripting called “caplet” can be used to automate command executions.
  - Can be combined with other attacks.

# Protection against ARP Poisoning

- It is very difficult to prevent ARP poisoning itself **as it exploits the insecure way that ARP works.**
- Using static ARP tables can protect against MITM attacks but it does not scale well → It is not practical in large networks (Note that even in small networks, ARP tables have to be configured every time a new device is connected to the network)
- In fact ARP poisoning can easily be discovered by looking at the current ARP table (`arp -a`)
  - If the MAC address of the gateway (router) changes then poisoning has happened; but we do not check the ARP table all the time

# Protection against ARP Poisoning

- There are tools that monitor the ARP table automatically and send a user a notification if anything suspicious happens.



- By using Wireshark, one can detect ARP poisoning (and other suspicious activities) in the network. → Next slide

# Protection against ARP Poisoning

arp.src.hw\_mac == de:ad:be:ef:de:ad

No.	Time	Source	Destination	Protocol	Length	Info
13	7.371348	de:ad:be:ef:de:ad	00:00:00_00:00:00	ARP	42	192.168.112.1 is at de:ad:be:ef:de:ad (duplicate use of 192.168.112.1 detected!)
14	7.371358	de:ad:be:ef:de:ad	00:00:00_00:00:00	ARP	42	192.168.112.1 is at de:ad:be:ef:de:ad (duplicate use of 192.168.112.1 detected!)
15	7.371474	de:ad:be:ef:de:ad	Routerbo_bd:1e:63	ARP	42	192.168.112.11 is at de:ad:be:ef:de:ad
16	7.371480	de:ad:be:ef:de:ad	Routerbo_bd:1e:63	ARP	42	192.168.112.11 is at de:ad:be:ef:de:ad
40	22.372398	de:ad:be:ef:de:ad	00:00:00_00:00:00	ARP	42	192.168.112.1 is at de:ad:be:ef:de:ad (duplicate use of 192.168.112.1 detected!)
41	22.372411	de:ad:be:ef:de:ad	00:00:00_00:00:00	ARP	42	192.168.112.1 is at de:ad:be:ef:de:ad (duplicate use of 192.168.112.1 detected!)
42	22.372582	de:ad:be:ef:de:ad	Routerbo_bd:1e:63	ARP	42	192.168.112.11 is at de:ad:be:ef:de:ad
43	22.372592	de:ad:be:ef:de:ad	Routerbo_bd:1e:63	ARP	42	192.168.112.11 is at de:ad:be:ef:de:ad

Frame 13: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0

Ethernet II, Src: de:ad:be:ef:de:ad (de:ad:be:ef:de:ad), Dst: 00:00:00\_00:00:00 (00:00:00:00:00:00)

[Duplicate IP address detected for 192.168.112.1 (de:ad:be:ef:de:ad) - also in use by e4:8d:8c:bd:1e:63 (frame 4)]

[Frame showing earlier use of IP address: 4]

[Expert Info (Warning/Sequence): Duplicate IP address configured (192.168.112.1)]

[Duplicate IP address configured (192.168.112.1)]

[Severity level: Warning]

[Group: Sequence]

[Seconds since earlier frame seen: 4]

Address Resolution Protocol (arp):

