Network Security

S. R. Shinde

Definitions

- **Computer Security** - generic name for the collection of tools designed to protect data from hackers

- **Network Security** - measures to protect data during their transmission

- **Internet Security** - measures to protect data during their transmission over a collection of interconnected networks

Attack Goals

- **Theft of sensitive information** (example, credit card information)
- **Disruption of service** (rendering a service inaccessible or unavailable)
- **Illegal access to or use of resources** (gain control so as to get unauthorized access)

Types of Attacks

- DOS/DDOS
- IP Spoofing
- ARP Spoofing
- DNS Spoofing
- Session Hijacking
- SQL injection
- Phishing
- Man in the Middle attack

Malware Attacks

- **Worms** and **viruses** are malware that replicate themselves.
- A **virus** typically infects a file and spreads from one file to another.
- A **worm** is usually a **stand-alone program** that infects a computer, so a worm spreads from one computer to another.
- Worms and viruses use various spreading techniques.

  E-mail, internet messages, web pages, Bluetooth and MMS are some of the propagation vectors.

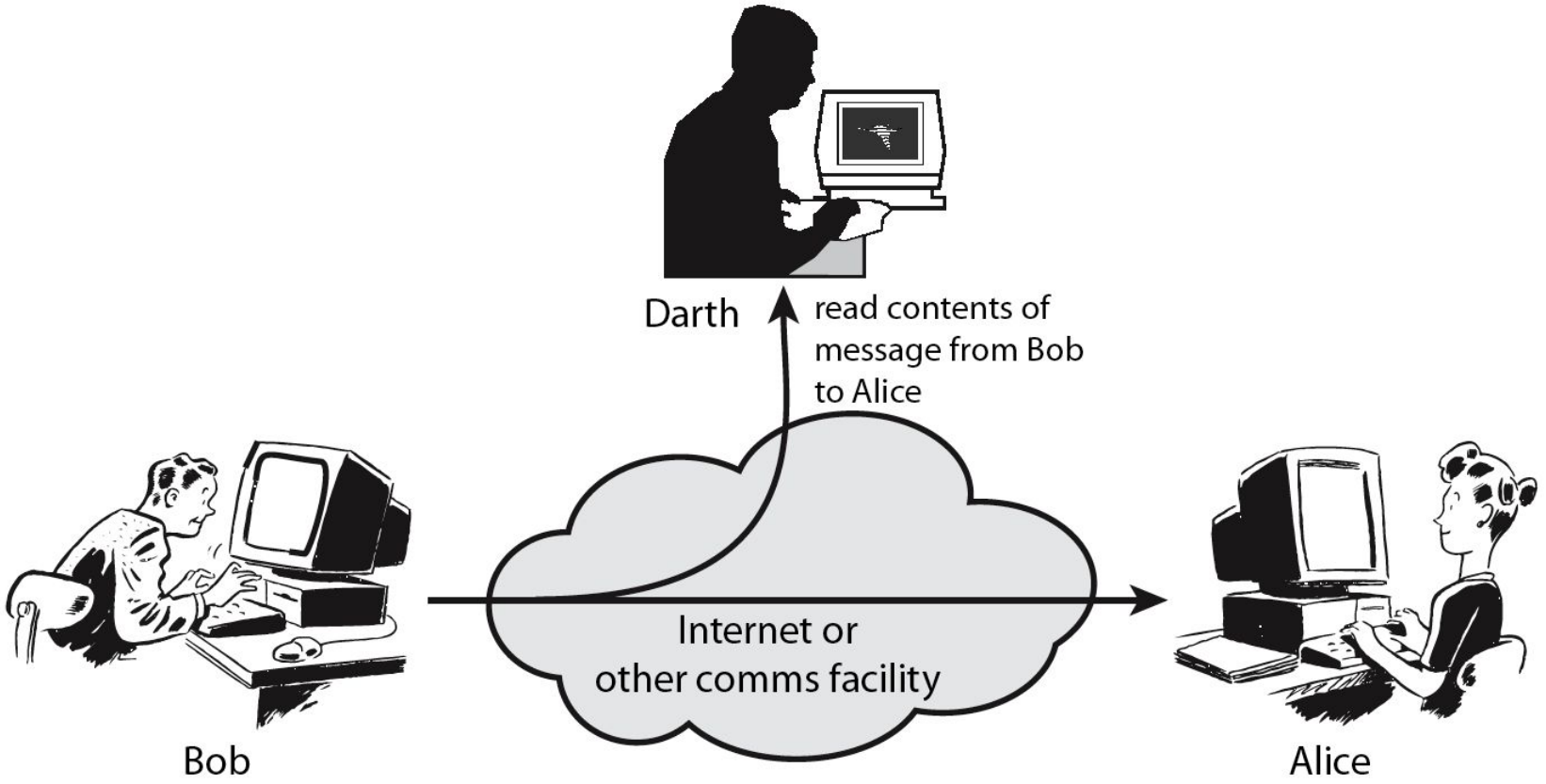
Malware Attacks (contd.)

- A **Trojan** is a kind of malware that masquerades(false outward show) as a utility but has other insidious(spreading harmfully) goals such as the modification of files, data theft, etc.

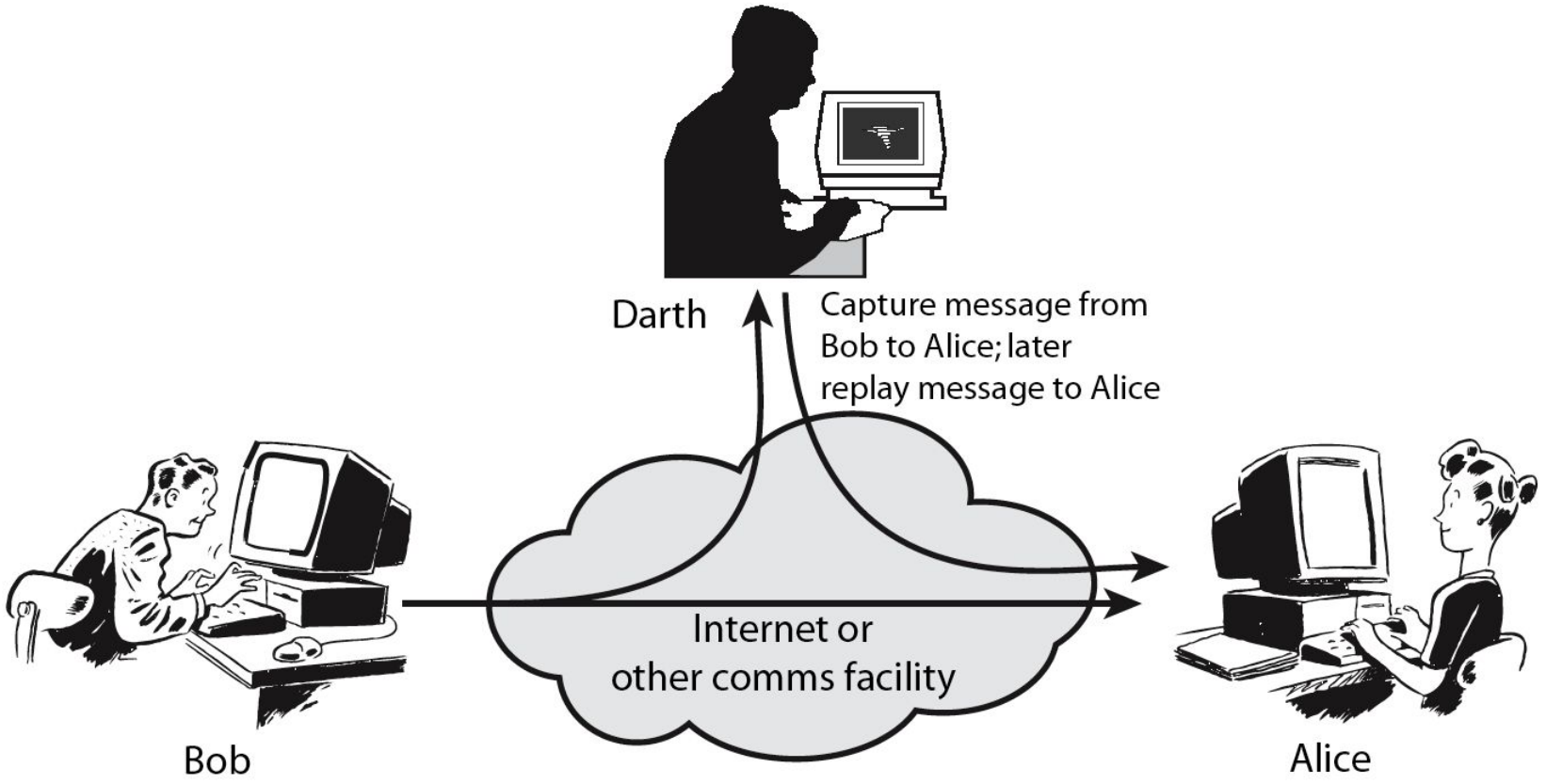
- **Spyware**, installed on a machine, can be used to monitor user activity and as a key logger to recover valuable information such as passwords from user keystrokes.

- **Bots** are malware hosted by a compromised machine connected to the internet and **remotely controlled** by a “botmaster”.

Passive Attacks



Active Attacks



Vulnerabilities

- A vulnerability is a **weakness** or lacuna in a policy, procedure, protocol, hardware or software within an organization that has the potential to cause it damage or loss.

Vulnerability Types

- Human Vulnerabilities
  - Induced by careless/unthinking human behaviour
  - Ex. clicking on a link in an e-mail message from a questionable source
  - Related to phishing

Vulnerability Types (contd.)

- Protocol Vulnerabilities
  - Attacks on commonly used networking protocols such as TCP, IP, ARP, ICMP and DNS
  - Ex. Session hijacking Attacks (DoS) which exploit the 3-way TCP handshake
  - Pharming attacks exploit vulnerabilities in DNS

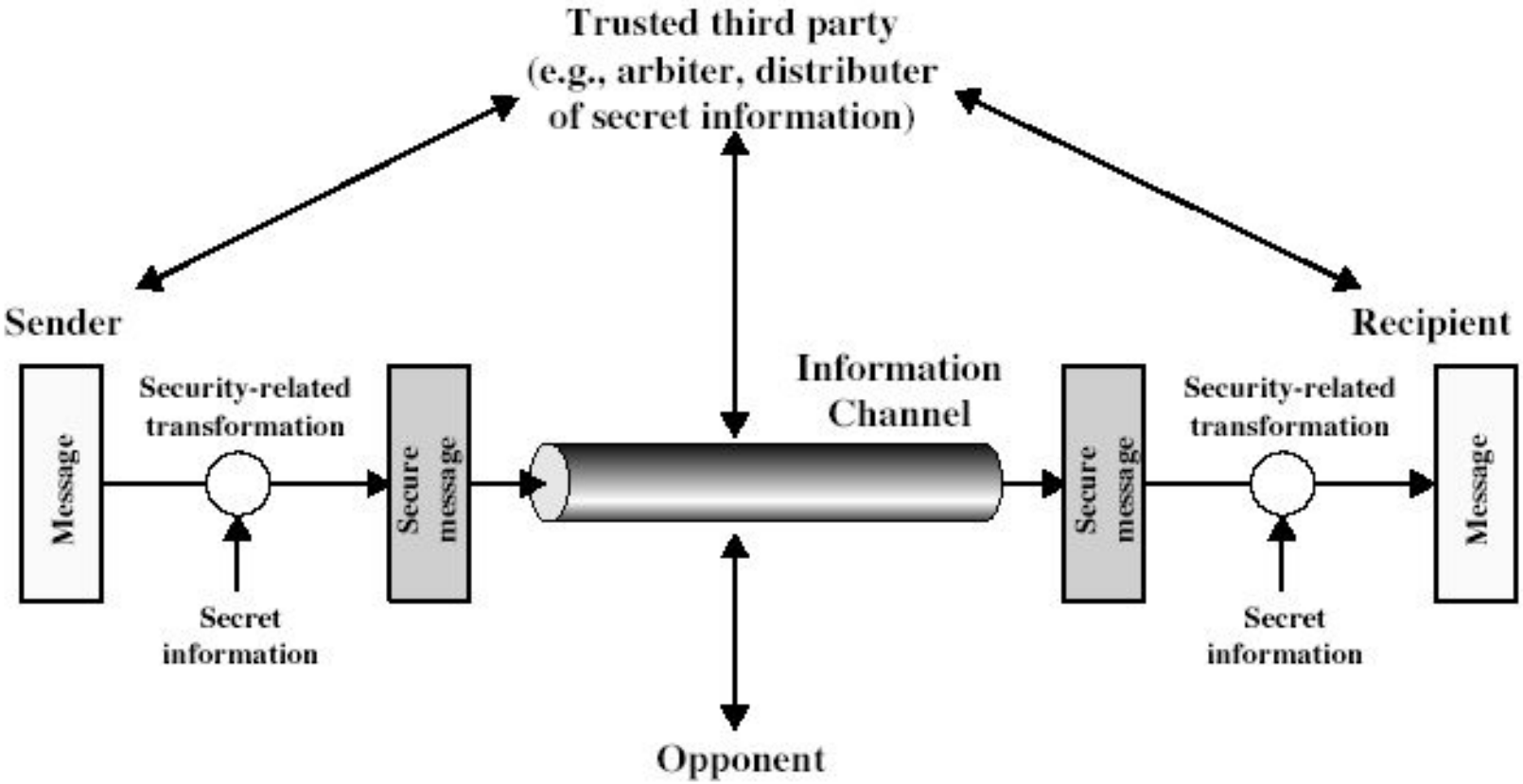
Vulnerability Types (contd.)

- Software Vulnerabilities
  - Caused by sloppy(careless) software
  - Software may perform as expected under normal conditions but when provided with a specific input, it turns malicious
  - Examples include cross-site scripting (XSS) vulnerability and SQL injection vulnerability

Vulnerability Types (contd.)

- Configuration Vulnerabilities
  - related to settings on system/application software, on files, etc.
  - Read-write-execute (and other) permissions on files (and other objects) may be too generous and susceptible to abuse.
  - Privilege level assigned to a process may be higher than what it should be to carry out a task.
  - Often lead to "**privilege escalation**" attacks.

Model for Network Security



Model for Network Security

- using this model requires us to:

1. Design a suitable algorithm for the security transformation
2. Generate the secret information (keys) for the algorithm
3. Develop methods to distribute and share the secret information
4. Specify a protocol enabling the principals to use the transformation and secret information for a security service

Commonly used terms in security

- **Security Policy** is the set of rules and practices that regulate how an organization manages and protects its computing and communication resources from unauthorized use or misuse.

- A **security mechanism** is a technique or device used to implement a security policy.

- **Entity Authentication** is the process of verifying that the entity being communicated with is indeed the entity it claims to be.

- **Message Authentication** is the process of verifying the source or origin of the message.

Commonly used terms in security (contd.)

- **Access Control** - prevention of the unauthorized use of a resource
- **Data Confidentiality** –protection of data from unauthorized disclosure
- **Data Integrity** - assurance that data received is as sent by an authorized entity
- **Non-Repudiation** - protection against denial by one of the parties in a communication

Security Practice – Principle 1

- **Security is as much (or more) a human problem rather than a technological problem and must be addressed at different levels.**

  Besides processes and technology, security is also a people problem and should involve a security team, system administrators and all members of an organization through awareness programs

Security Practice – Principle 2

- **Security should be factored in at inception, not as an afterthought**

Security should be factored in early on during the design phase of a new product and then carried forward right through implementation and testing.

Security Practice – Principle 3

- **Security by obscurity or by complexity is often bogus**

Let the security community scrutinize a crypto algorithm or protocol before standardizing it. This will help identify and eliminate bugs prior to actual deployment. In this context, openness rather than obscurity wins.

Security Practice – Principle 4

- **Always consider the "Default Deny" policy for adoption in access control**

The "Default Deny" policy is the conservative approach in which the subject's request is denied unless it is on a **whitelist**.

The "Default Permit" policy grants the subject's request unless the subject is on a **blacklist** or it has certain blacklisted attributes.

Security Practice – Principle 5

- **An entity should be given the least amount/level of permissions/privileges to accomplish a given task**

Conferring higher privilege to an individual than what is warranted by his/her current role could compromise the system through one of the many types of privilege escalation attacks.

Security Practice – Principle 6

- **Defense in depth could help frustrate carefully laid out attack plans**

A good example of this principle is the use of at least two packet filtering appliances (such as a firewall) from different vendors and possibly configured by two different system administrators. What escapes Firewall 1 may be caught by Firewall 2 and vice versa.

Security Practice – Principle 7

- **Identify vulnerabilities and respond appropriately**

  For each identifiable vulnerability, identify the risk involved and act accordingly.

Security Practice – Principle 8

- **Carefully study the tradeoffs involving security before making any**

Security almost always comes with a price tag - the most clear-cut tradeoffs are

- security versus performance,
- security versus cost and
- security versus convenience/flexibility

TCP Session Hijacking

- **TCP** session hijacking is when a hacker takes over a **TCP** session between two machines.

- Since most authentication only occurs at the start of a **TCP** session, this allows the hacker to gain access to a machine.

Categories of **TCP** Session Hijacking

- Based on the anticipation of ***sequence numbers*** there are two types of **TCP** hijacking:
  - Man-in-the-middle (**MITM**)
  - Blind Hijack

Man-in-the-middle

- A hacker can also be "inline" between **B** and **C** using a ***sniffing program*** to watch the sequence numbers and acknowledge numbers in the **IP** packets transmitted between **B** and **C**. And then hijack the connection.
- This is known as a "***man-in-the-middle attack***".

Man in the Middle Attack Using Packet Sniffers

- This technique involves using a ***packet sniffer*** to intercept the communication between client and the server.
- Packet sniffer comes in two categories:
  - Active sniffers
  - Passive sniffers.

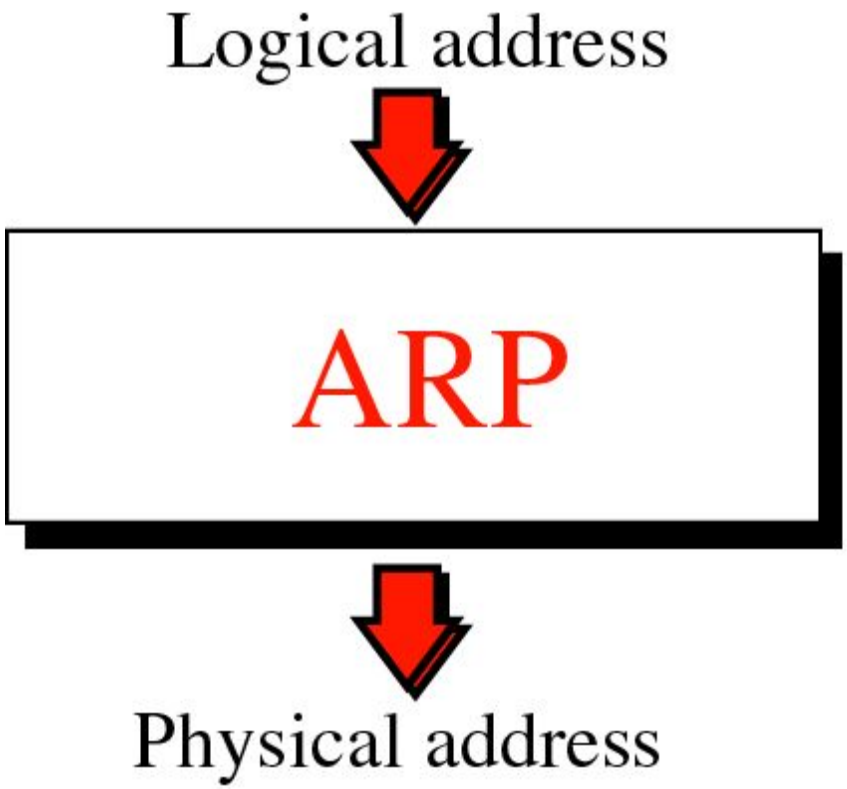
Packet Sniffers

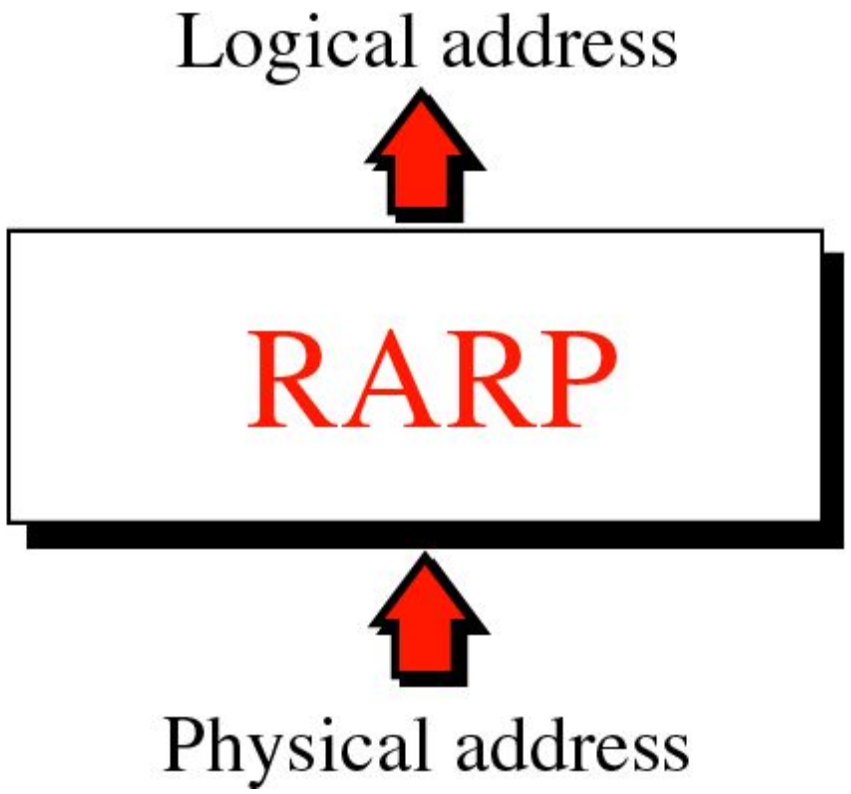
- ***Passive sniffers*** monitors and sniffs **IP** packets from a network having same collision domain (i.e. network with a hub, as all packets are broadcasted on each port of hub.)
- ***Active Sniffers*** One way of doing so is to change the default gateway of the client's machine so that it will route its packets via the hijacker's machine.
- This can be done by **ARP *spoofing*** (i.e. by sending malicious **ARP** packets mapping its **MAC** address to the default gateways **IP** address so as to update the **ARP** cache on the client, to redirect the traffic to hijacker).

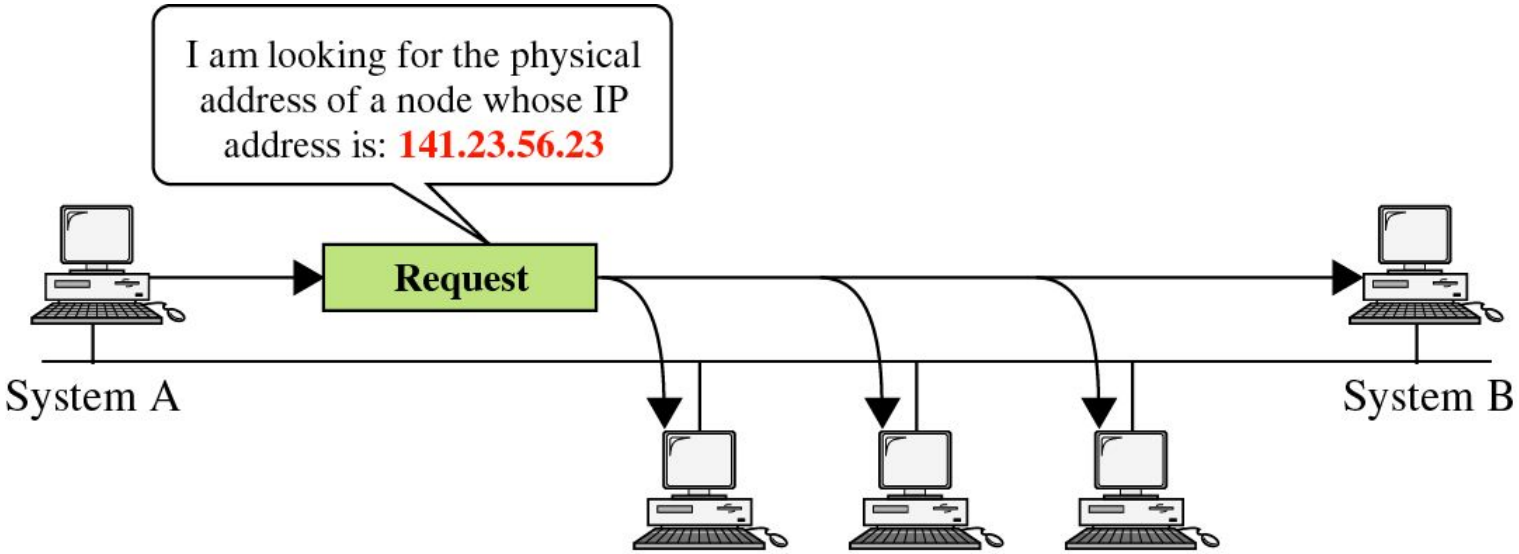
Blind Hijacking

- If you are **NOT** able to sniff the packets and guess the correct sequence number expected by server, you have to implement "***Blind Session Hijacking***.''
- You have to brute force 4 billion combinations of sequence number which will be an unreliable task.

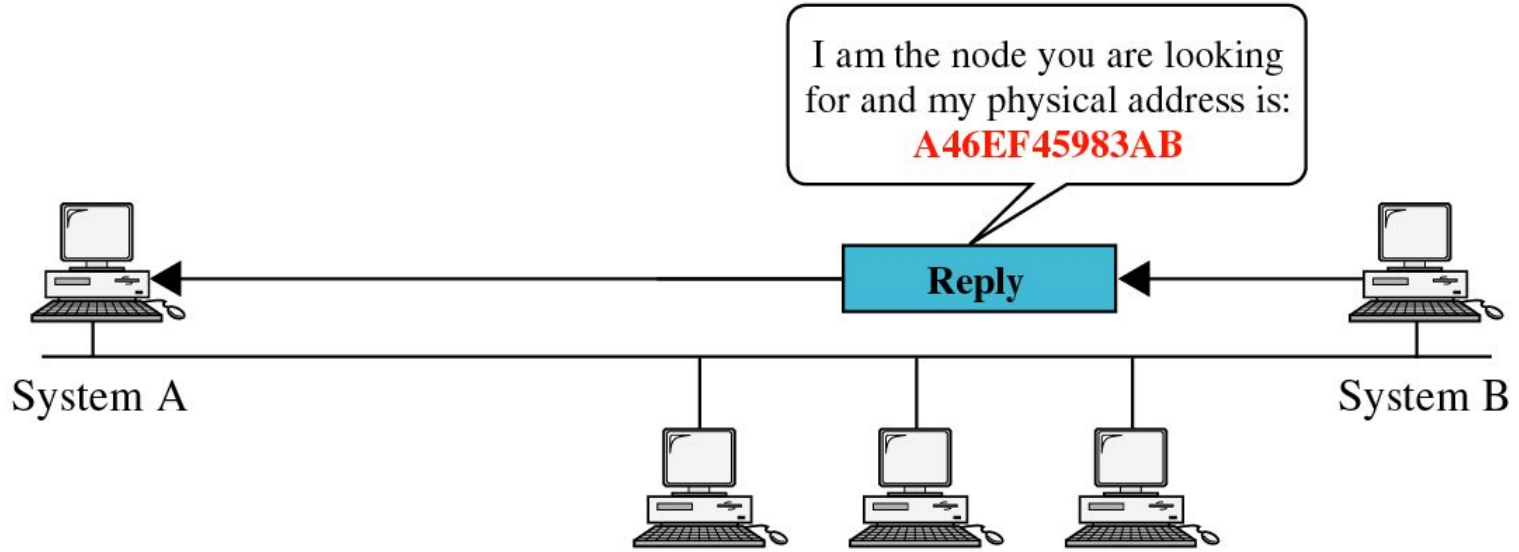
Address resolution and Reverse address resolution





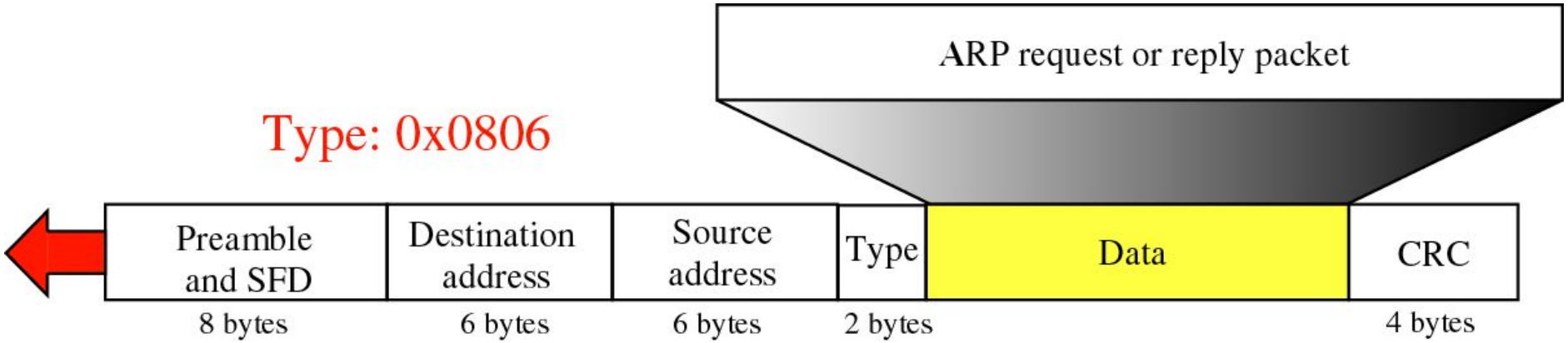


a. ARP request is broadcast



b. ARP reply is unicast

<table>
<tr><td colspan="2">Hardware Type</td><td>Protocol Type</td></tr>
<tr><td>Hardware
length</td><td>Protocol
length</td><td>Operation
Request 1, Reply 2</td></tr>
<tr><td colspan="3">Sender hardware address
(For example, 6 bytes for Ethernet)</td></tr>
<tr><td colspan="3">Sender protocol address
(For example, 4 bytes for IP)</td></tr>
<tr><td colspan="3">Target hardware address
(For example, 6 bytes for Ethernet)
(It is not filled in a request)</td></tr>
<tr><td colspan="3">Target protocol address
(For example, 4 bytes for IP)</td></tr>
</table>

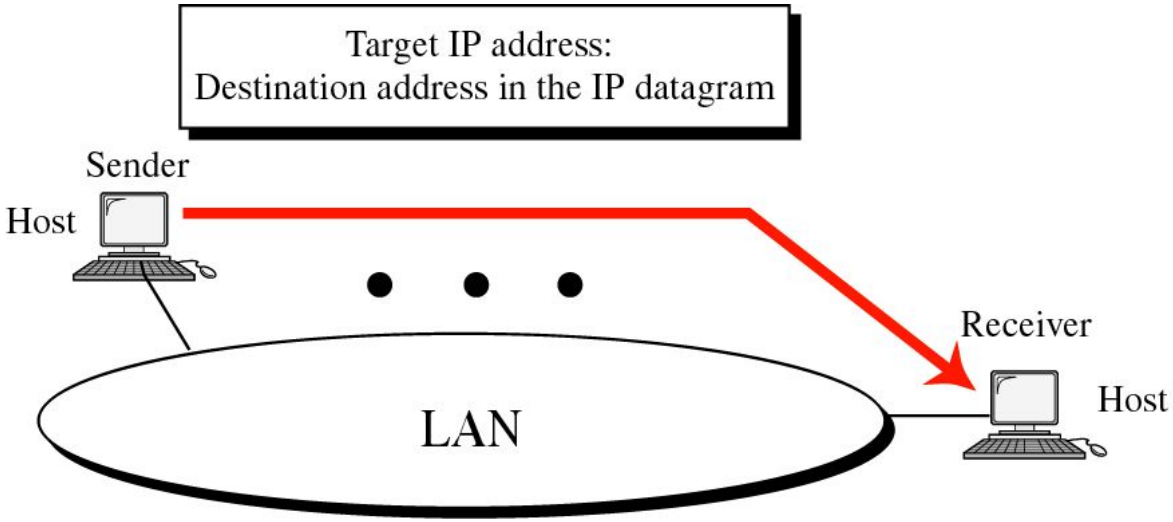


Encapsulation of ARP

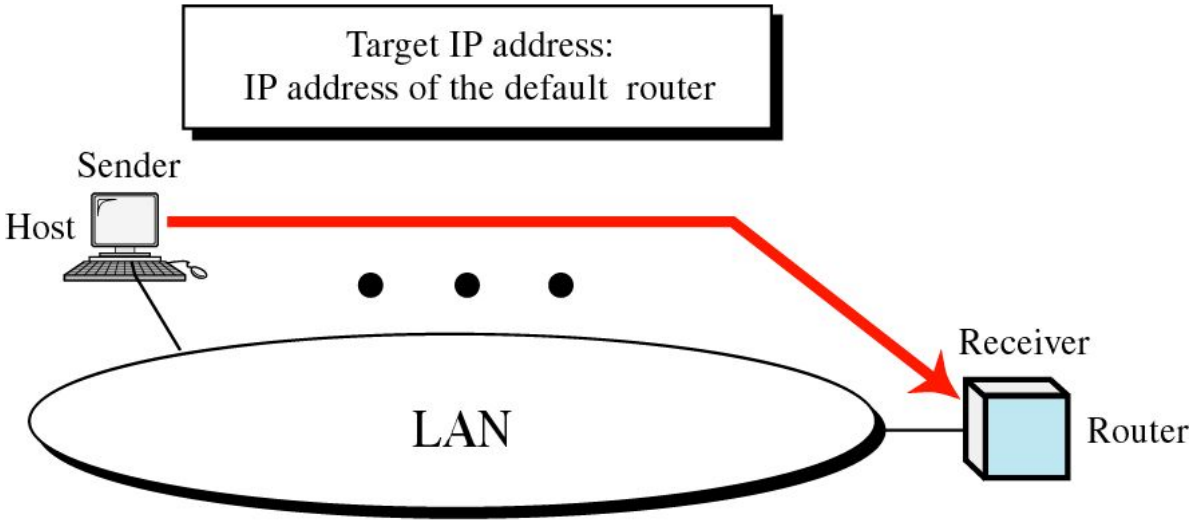
- How ARP functions:

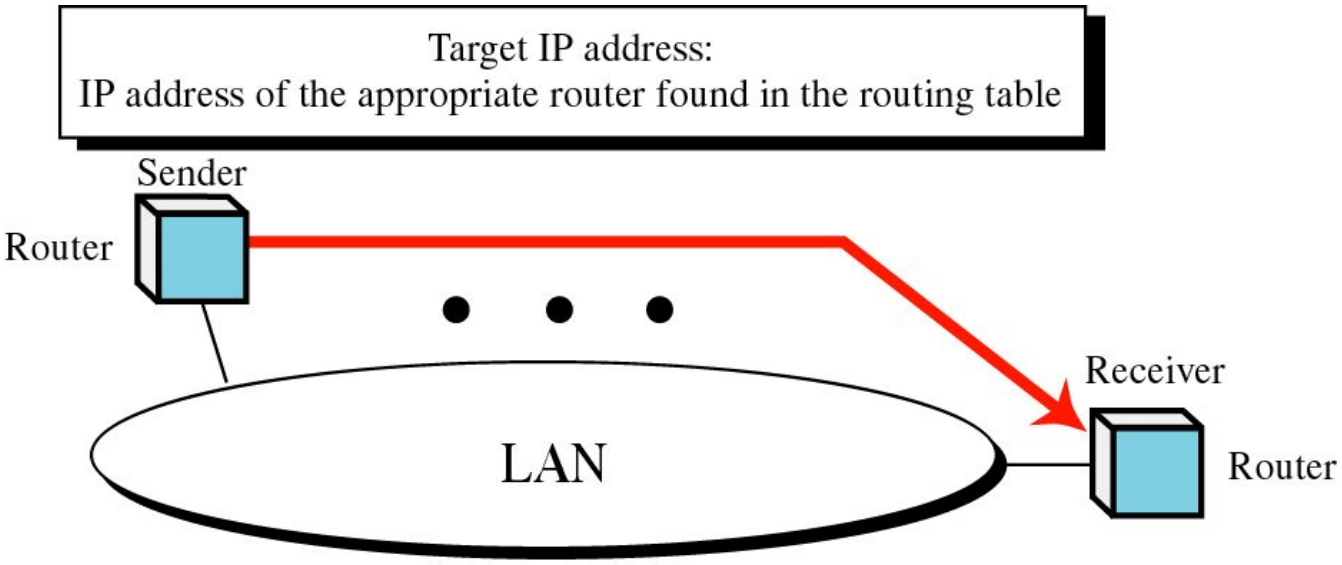
1. Get IP address of target.
2. Create a request ARP message
   - Fill sender physical address
   - Fill sender IP address
   - Fill target IP address
   - Target physical address is filled with 0
3. The message is passed to the data link layer where it is encapsulated in a frame.
   - Source address: physical address of the sender.
   - Destination address: broadcast address.

4. Every host or router on the LAN receives the frame.
   - All stations pass it to ARP.
   - All machines except the one targeted drop the packet.
5. The target machine replies with an ARP message that contains its physical address.
   - A unicast message.
6. The sender receives the reply message and knows the physical address of the target machine.

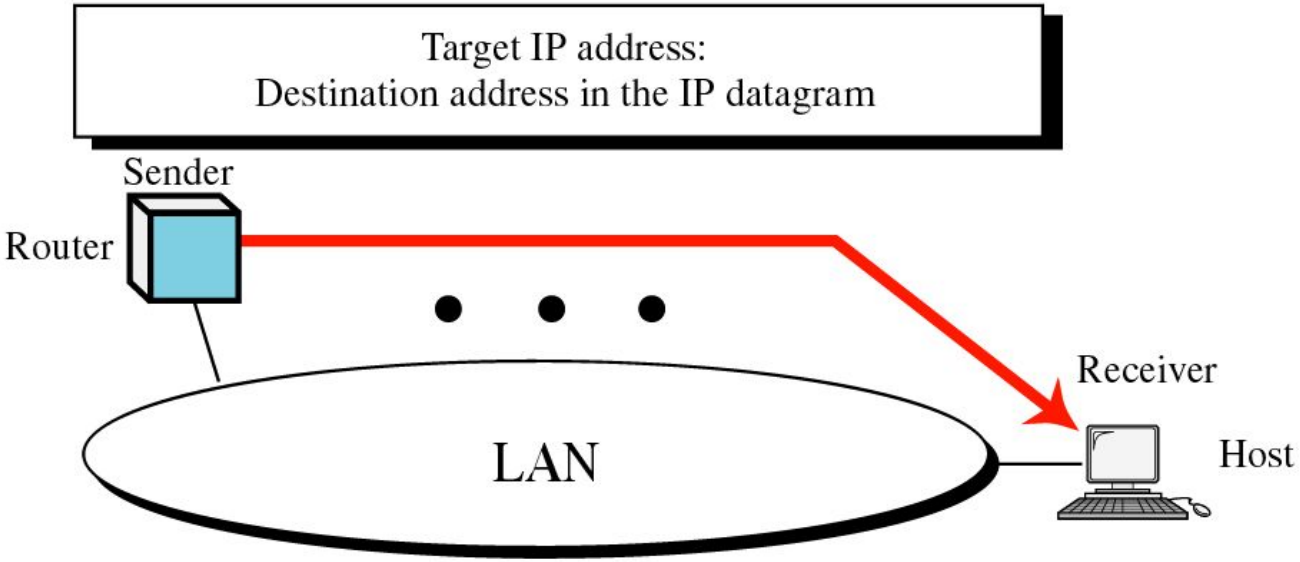


Case 1. A host has a packet to send to another host on the same network.

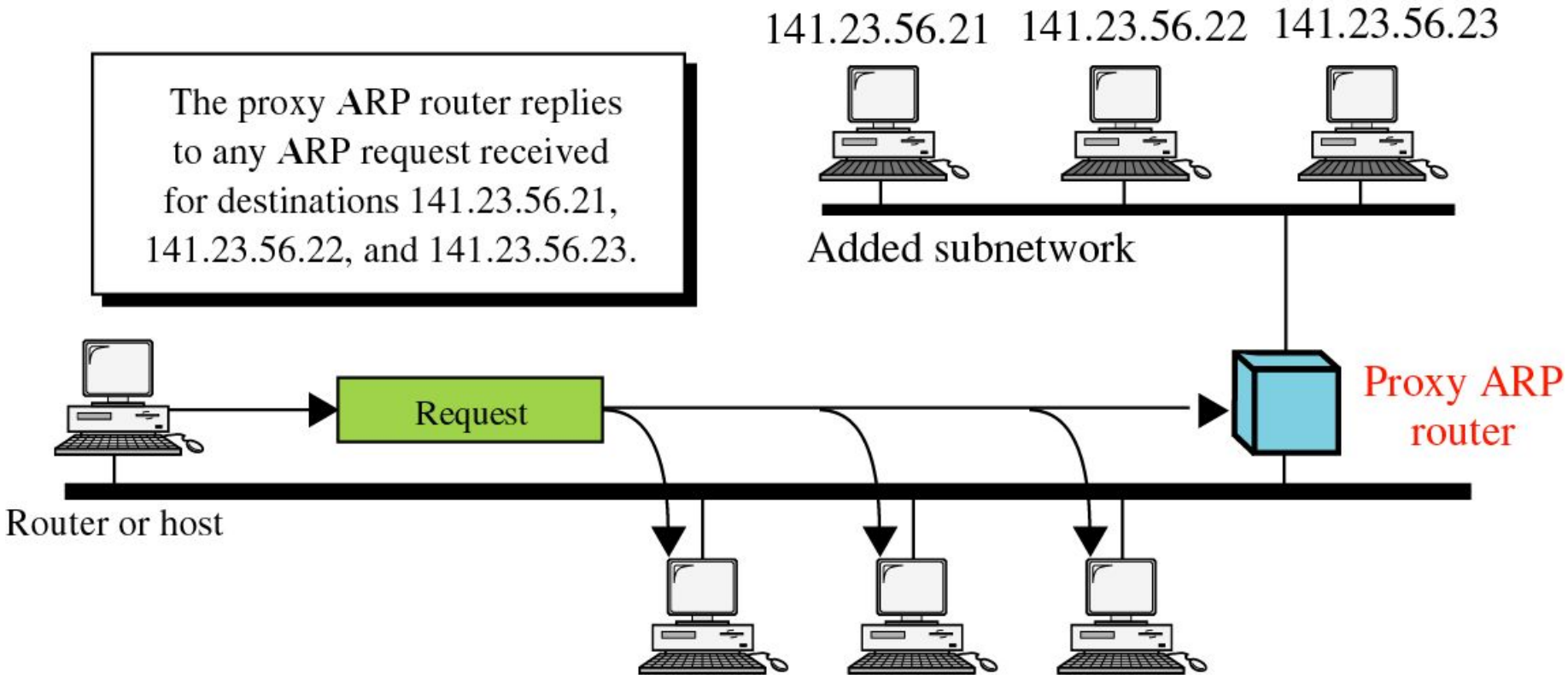


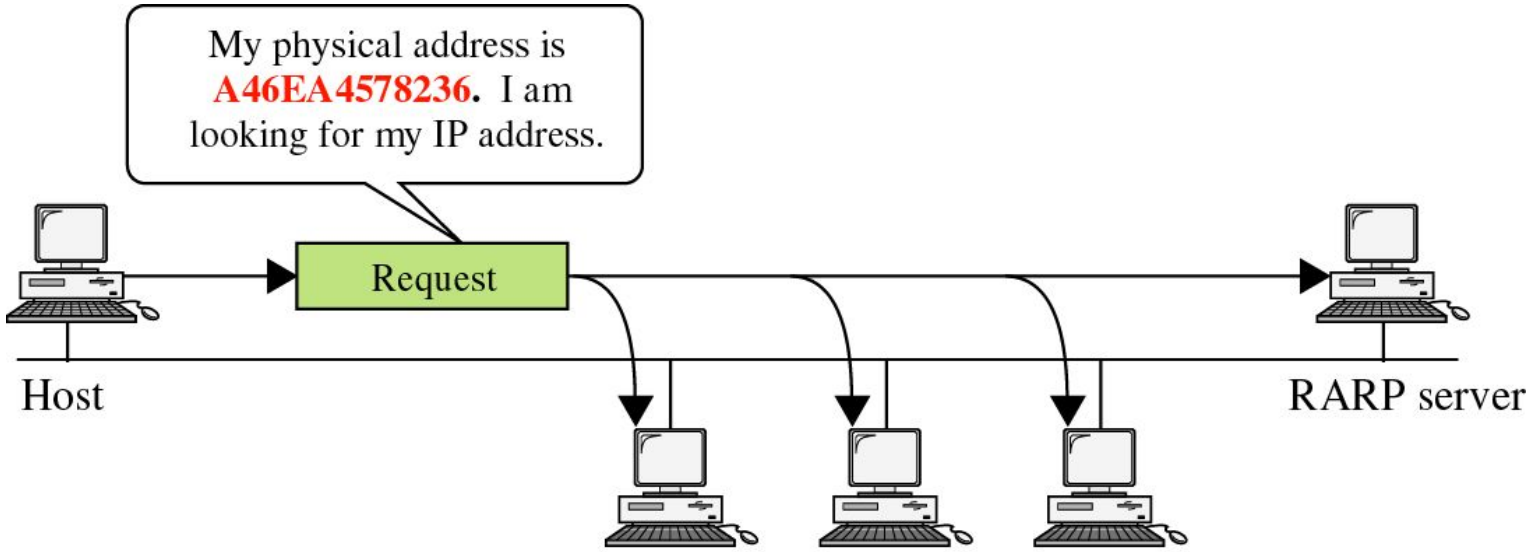


Case 3. A router receives a packet to be sent to a host on another network. It must first be delivered to the appropriate router.

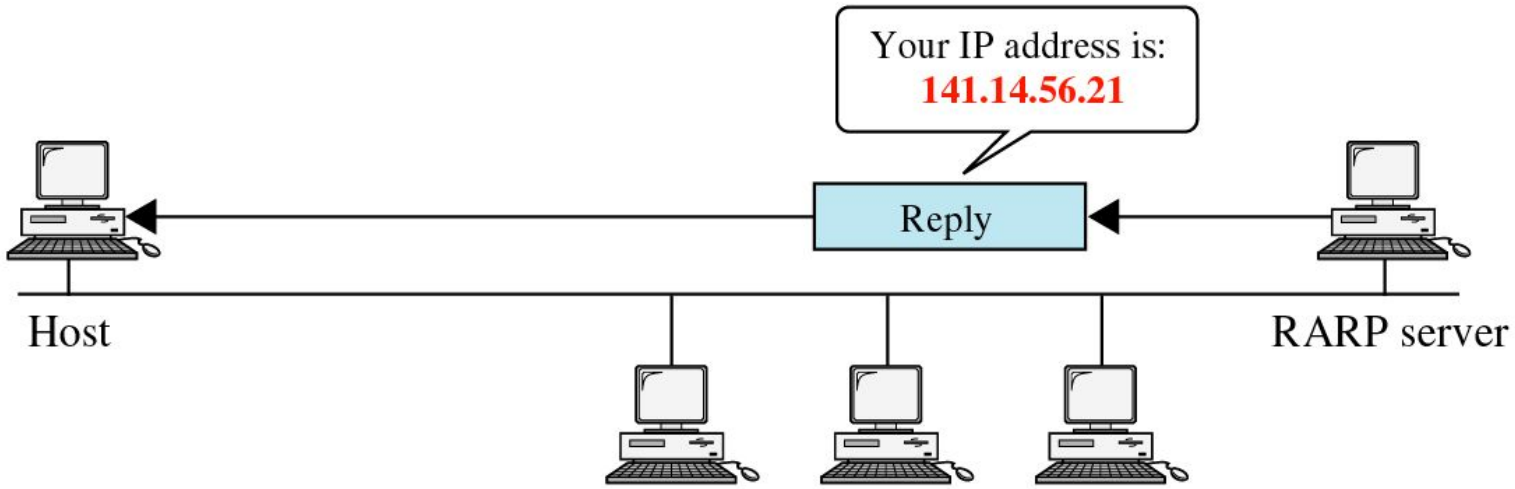


Case 4. A router receives a packet to be sent to a host on the same network.


141.23.56.21
141.23.56.22
141.23.56.23
The proxy ARP router replies to any ARP request received for destinations 141.23.56.21, 141.23.56.22, and 141.23.56.23.
Added subnetwork
Request
Proxy ARP router
Router or host

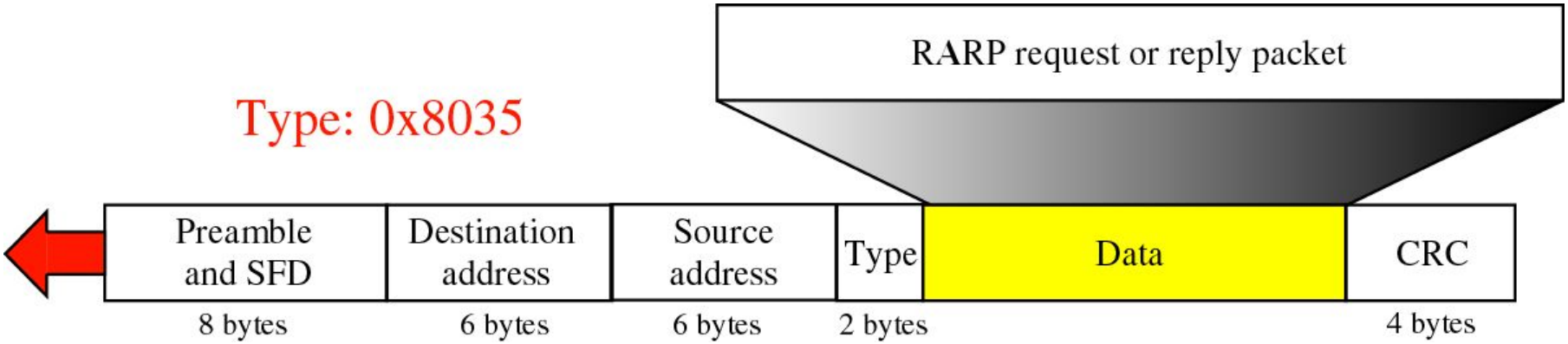


a. RARP request is broadcast



b. RARP reply is unicast

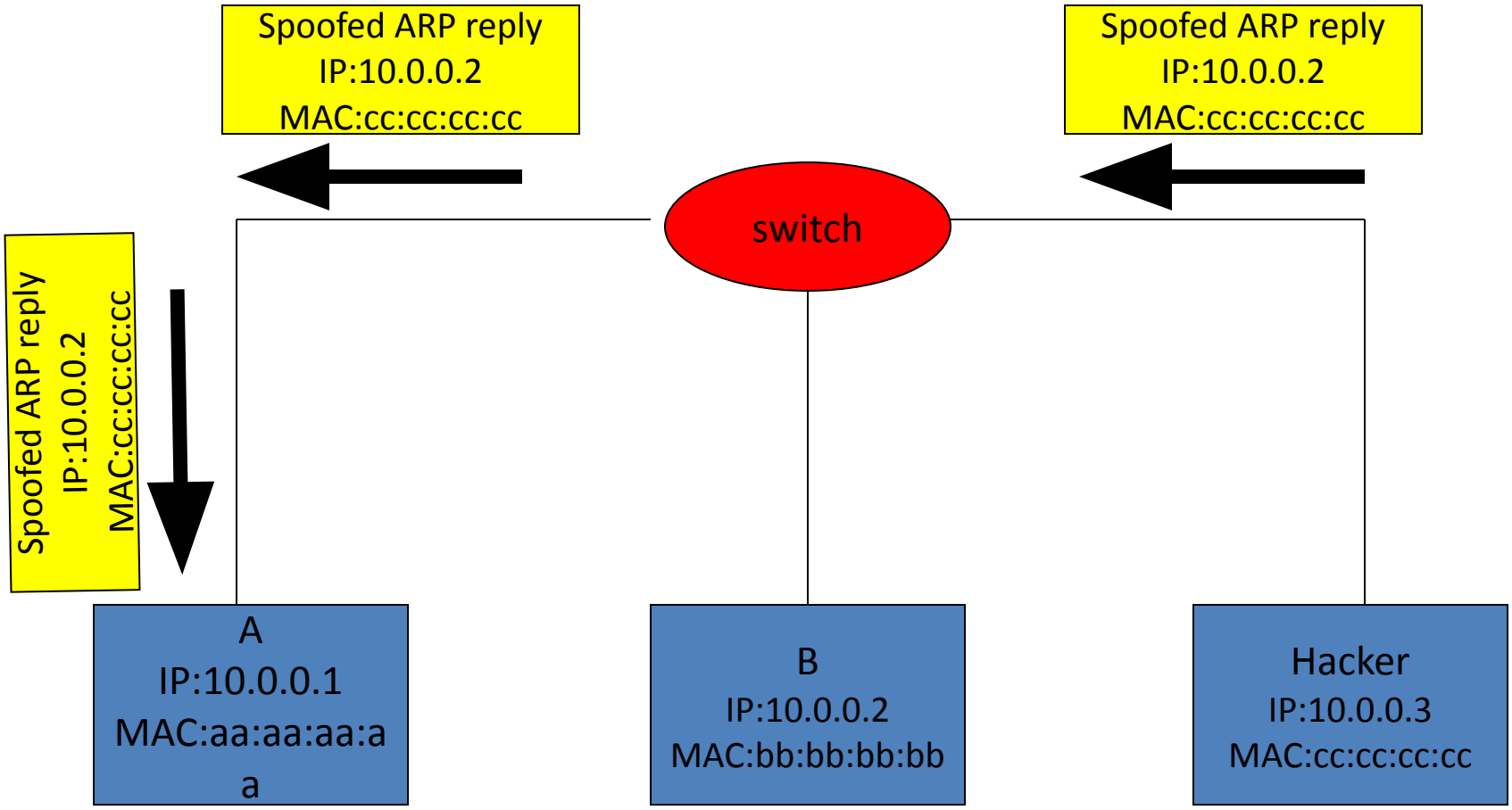
<table>
<tr><td colspan="2">Hardware type</td><td>Protocol type</td></tr>
<tr><td>Hardware
length</td><td>Protocol
length</td><td>Operation
Request 3, Reply 4</td></tr>
<tr><td colspan="3">Sender hardware address
(For example, 6 bytes for Ethernet)</td></tr>
<tr><td colspan="3">Sender protocol address
(For example, 4 bytes for IP)
(It is not filled for request)</td></tr>
<tr><td colspan="3">Target hardware address
(For example, 6 bytes for Ethernet)
(It is not filled for request)</td></tr>
<tr><td colspan="3">Target protocol address
(For example, 4 bytes for IP)
(It is not filled for request)</td></tr>
</table>


RARP request or reply packet
Type: 0x8035
Preamble and SFD
Destination address
Source address
Type
Data
CRC
8 bytes
6 bytes
6 bytes
2 bytes
4 bytes

- To avoid having to send an ARP request packet each time, a host can cache the IP and the corresponding host addresses in its ARP table (ARP cache).
- Each entry in the ARP table is usually “aged” so that the contents are erased if no activity occurs within a certain period.
- When a computer receives an ARP reply, it will update its ARP cache.
- ARP is a stateless protocol, most operating systems will update their cache if a reply is received, regardless of whether they have sent out an actual request.

ARP Spoofing

- Construct spoofed ARP replies.
- A target computer could be convinced to send frames destined for computer A to instead go to computer B.
- Computer A will have no idea that this redirection took place.
- This process of updating a target computer's ARP cache is referred to as "ARP poisoning".

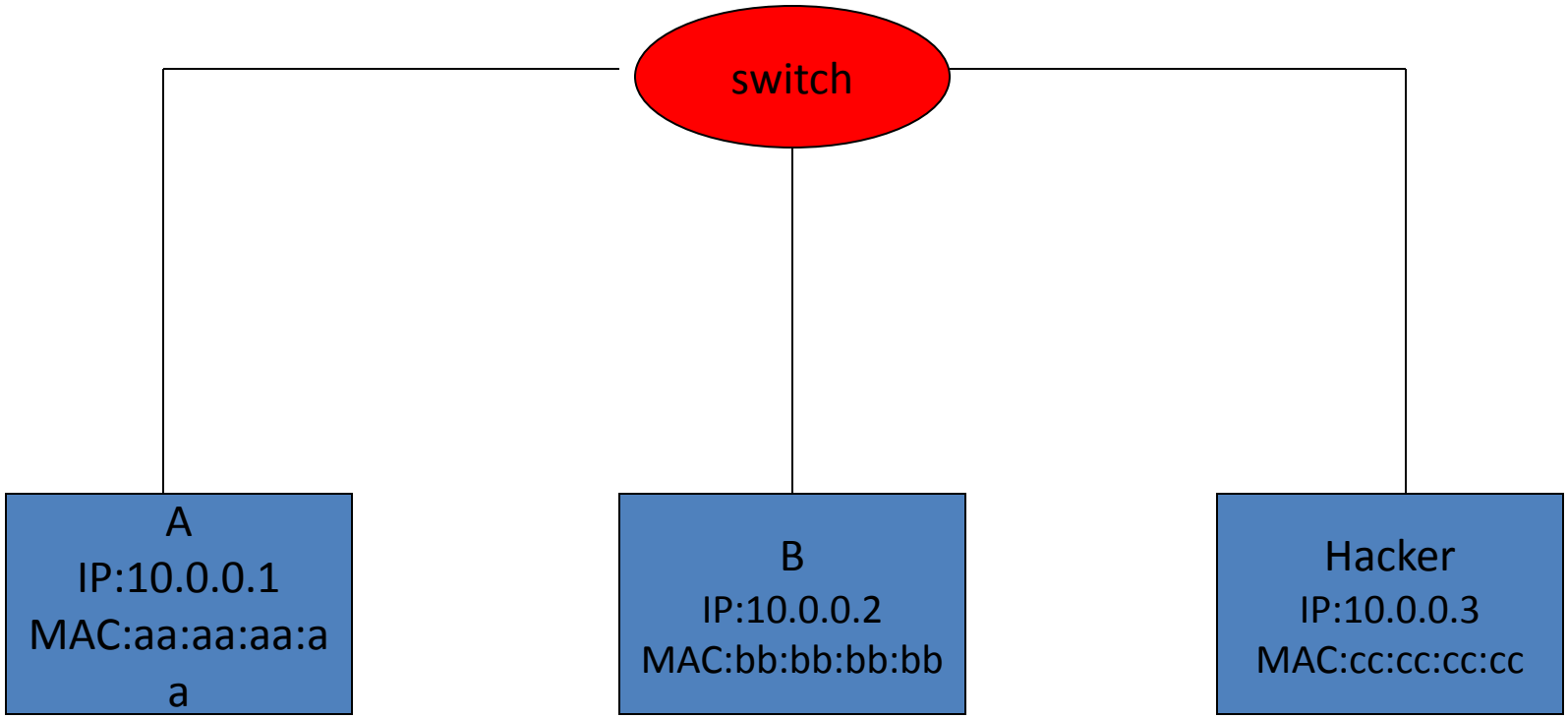


ARP cache

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	cc:cc:cc:cc

ARP cache

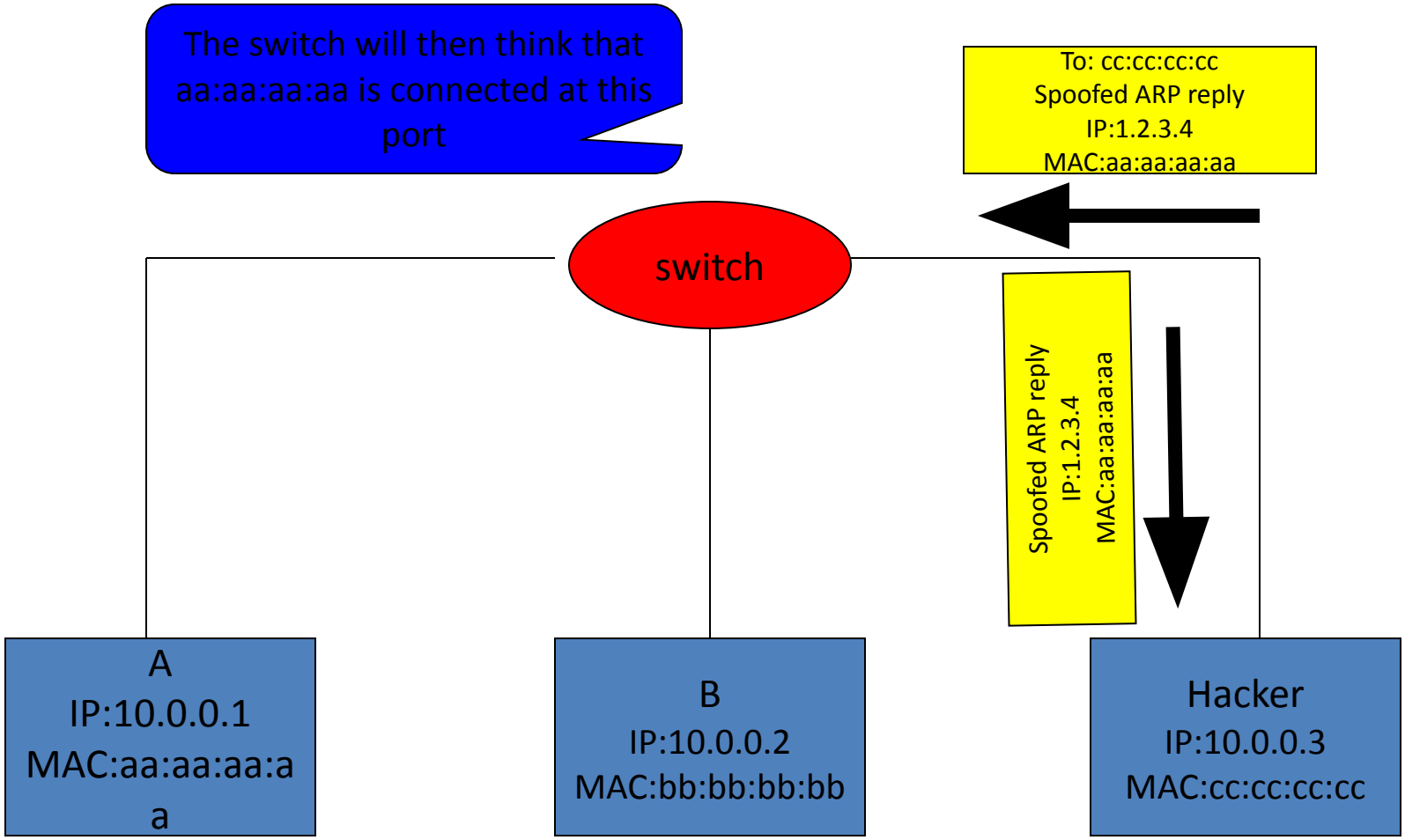
IP	MAC
10.0.0.1	aa:aa:aa:aa

A's cache is poisoned

- Now all the packets that A intends to send to B will go to the hacker's machine.
- Cache entry would expire, so it needs to be updated by sending the ARP reply again.
  - How often?
  - depends on the particular system.
  - Usually every 40s should be sufficient.
- In addition the hacker may not want his Ethernet driver talk too much
  - Accomplish with ifconfig -arp

- Complication
  - Some systems would try to update their cache entries by sending a unicast ARP request.
    - Like your wife calling you just to make sure you are there. ☺️
  - Such a request can screw things up, because it could change victim's ARP entry that the hacker just faked.
    - A computer will also cache the MAC address appeared in the ARP request.

- Prevention is better than cure
  - Accomplished by feeding the "wife" system with replies so that it never has to ask for it.
  - A real packet from B to A will be sent by the hacker's machine.
  - How often?
    - Again every 40s is usually OK.


The switch will then think that aa:aa:aa:aa is connected at this port
To: cc:cc:cc:cc
Spoofed ARP reply
IP:1.2.3.4
MAC:aa:aa:aa:aa
switch
Spoofed ARP reply
IP:1.2.3.4
MAC:aa:aa:aa:aa
A
IP:10.0.0.1
MAC:aa:aa:aa:a
a
B
IP:10.0.0.2
MAC:bb:bb:bb:bb
Hacker
IP:10.0.0.3
MAC:cc:cc:cc:cc

Demonstration

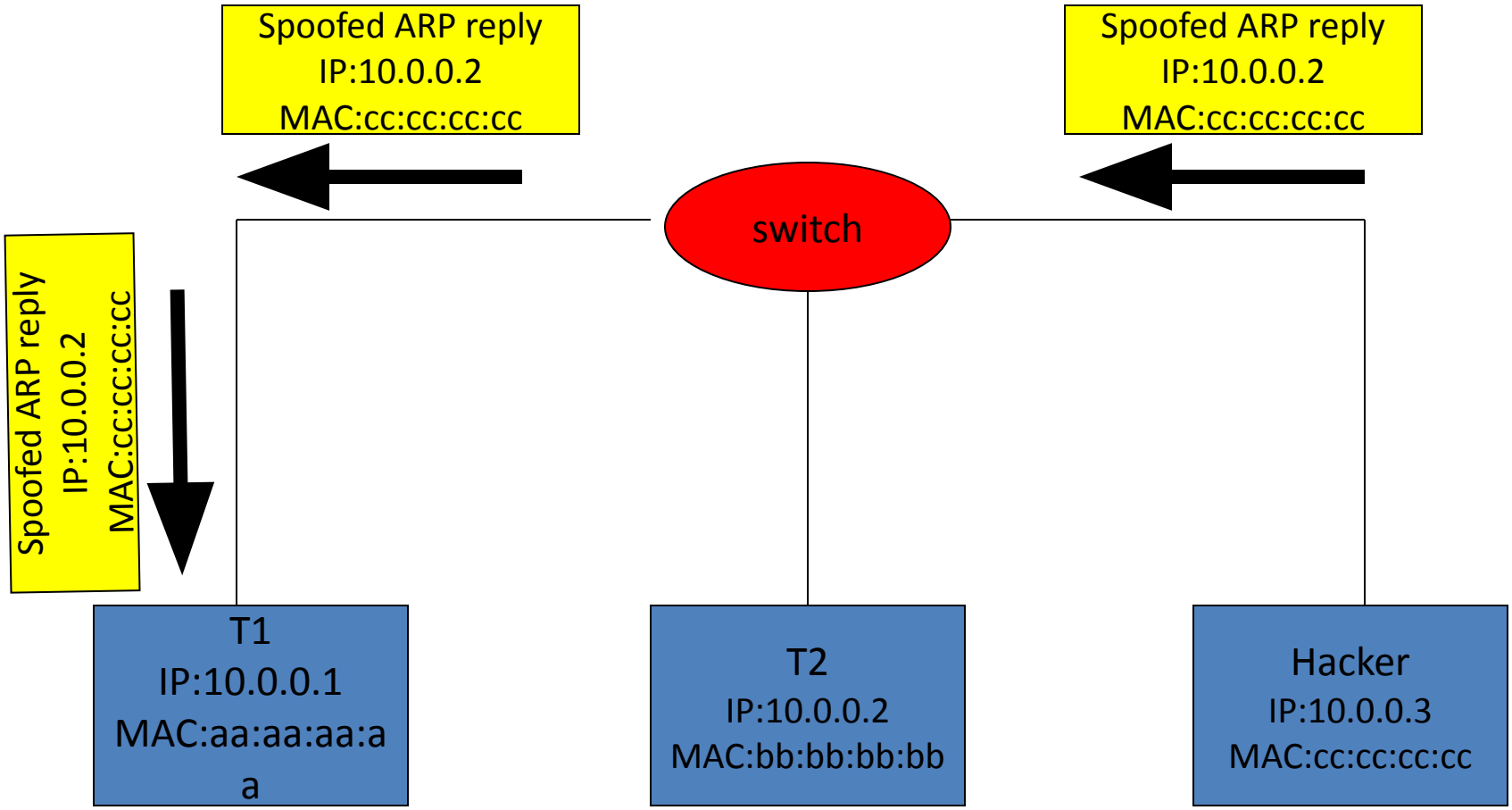
- Experiment
  - Use Ethereal to capture the forged ARP reply.
  - Use the command “arp –a” to show that the target machine will accept the reply and updates its ARP cache.
  - We can also show that the table in the switch can be changed.
- We can also modify the program, so that it can forge ARP request.
  - Show that some machines will also accept the MAC address appeared in the ARP request.

Man-in-the-Middle Attack

- A hacker inserts his computer between the communications path of two target computers.
- The hacker will forward frames between the two target computers so communications are not interrupted.
- E.g., Hunt, Ettercap etc.
  - Can be obtained easily in many web archives.

- The attack is performed as follows:
  - Suppose X is the hacker's computer
  - T1 and T2 are the targets

1. X poisons the ARP cache of T1 and T2.
2. T1 associates T2's IP with X's MAC.
3. T2 associates T1's IP with X's MAC.
4. All of T1 and T2's traffic will then go to X first, instead of directly to each other.

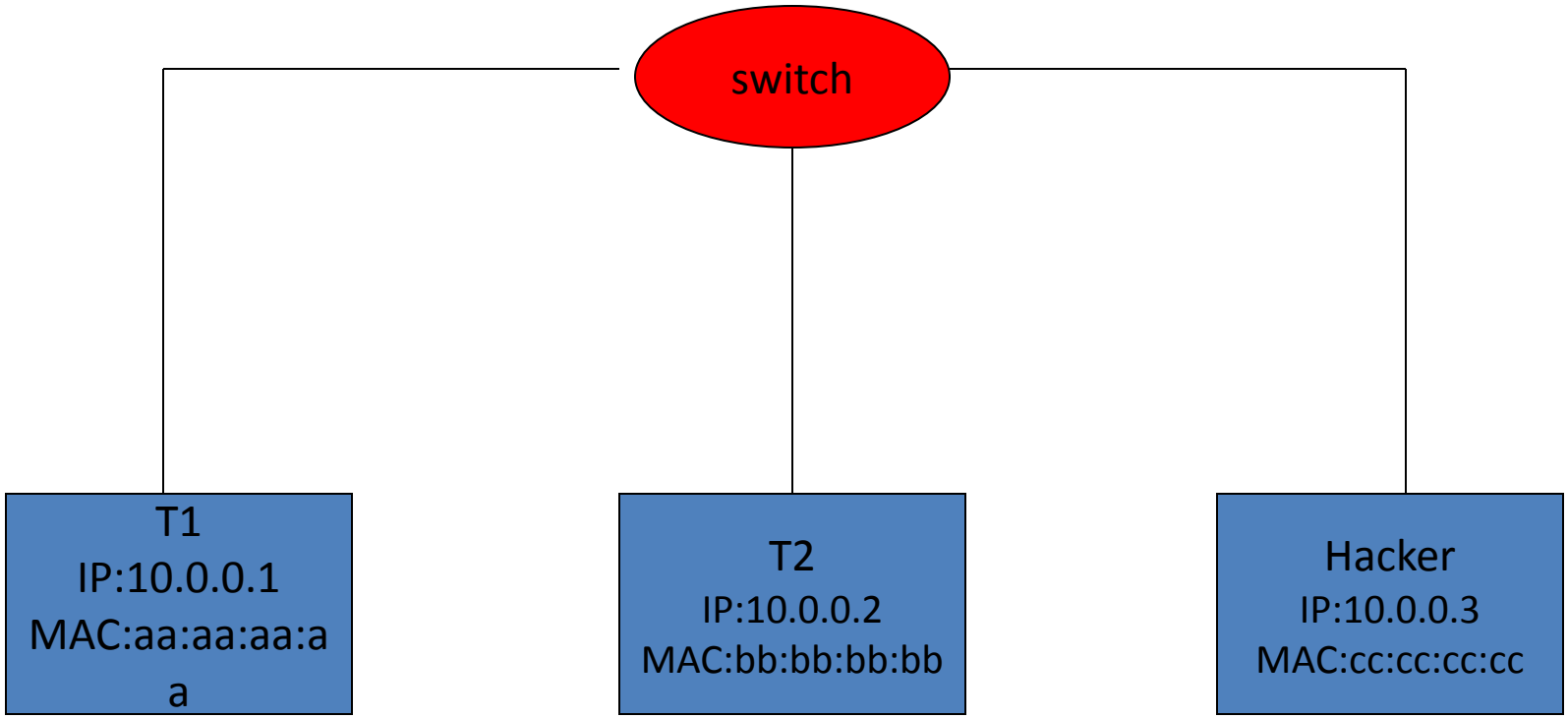


ARP cache

IP	MAC
10.0.0.2	bb:bb:bb:bb

ARP cache

IP	MAC
10.0.0.1	aa:aa:aa:aa



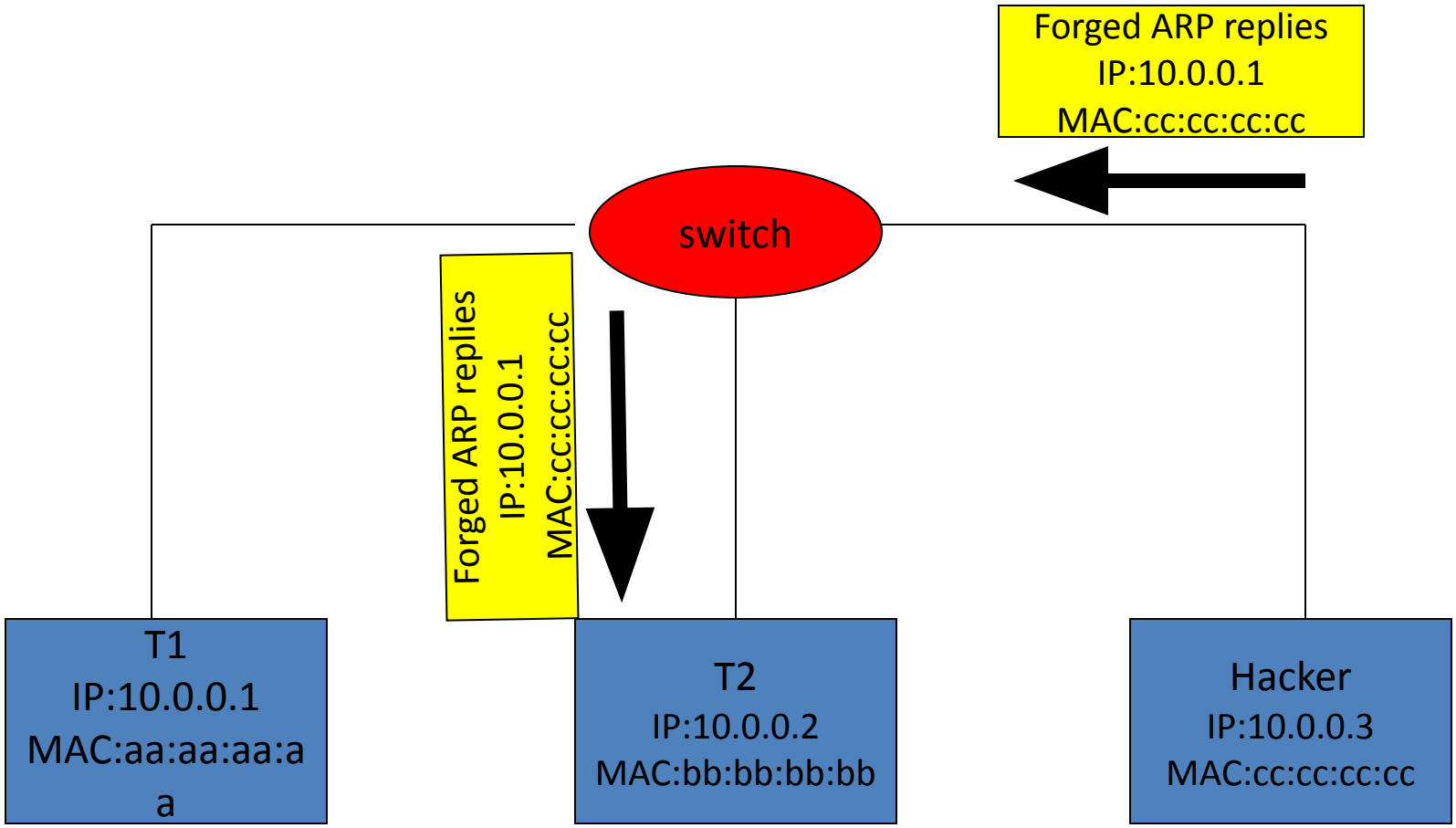
ARP cache

IP	MAC
10.0.0.2	cc:cc:cc:cc

ARP cache

IP	MAC
10.0.0.1	aa:aa:aa:aa

T1's cache is poisoned

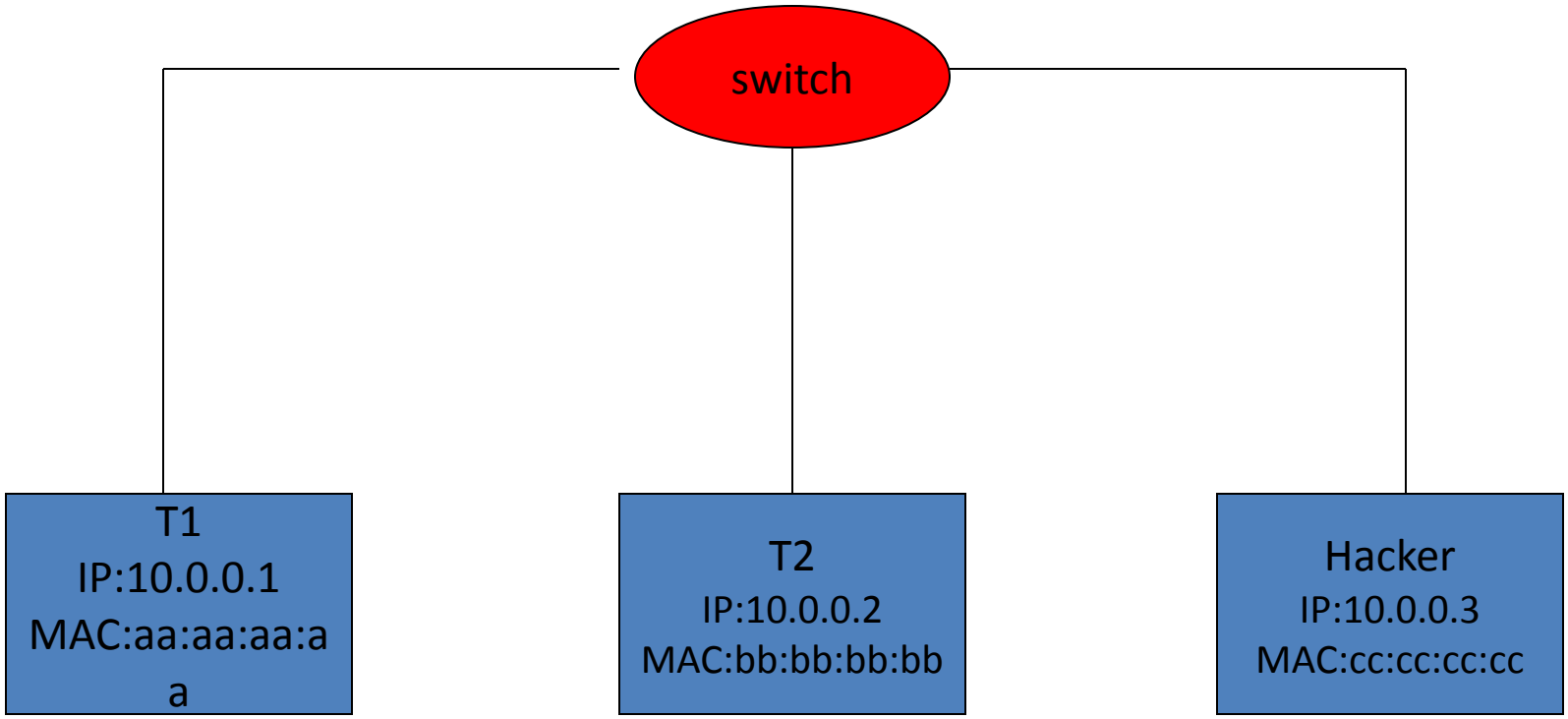


ARP cache

IP	MAC
10.0.0.2	cc:cc:cc:cc

ARP cache

IP	MAC
10.0.0.1	aa:aa:aa:aa



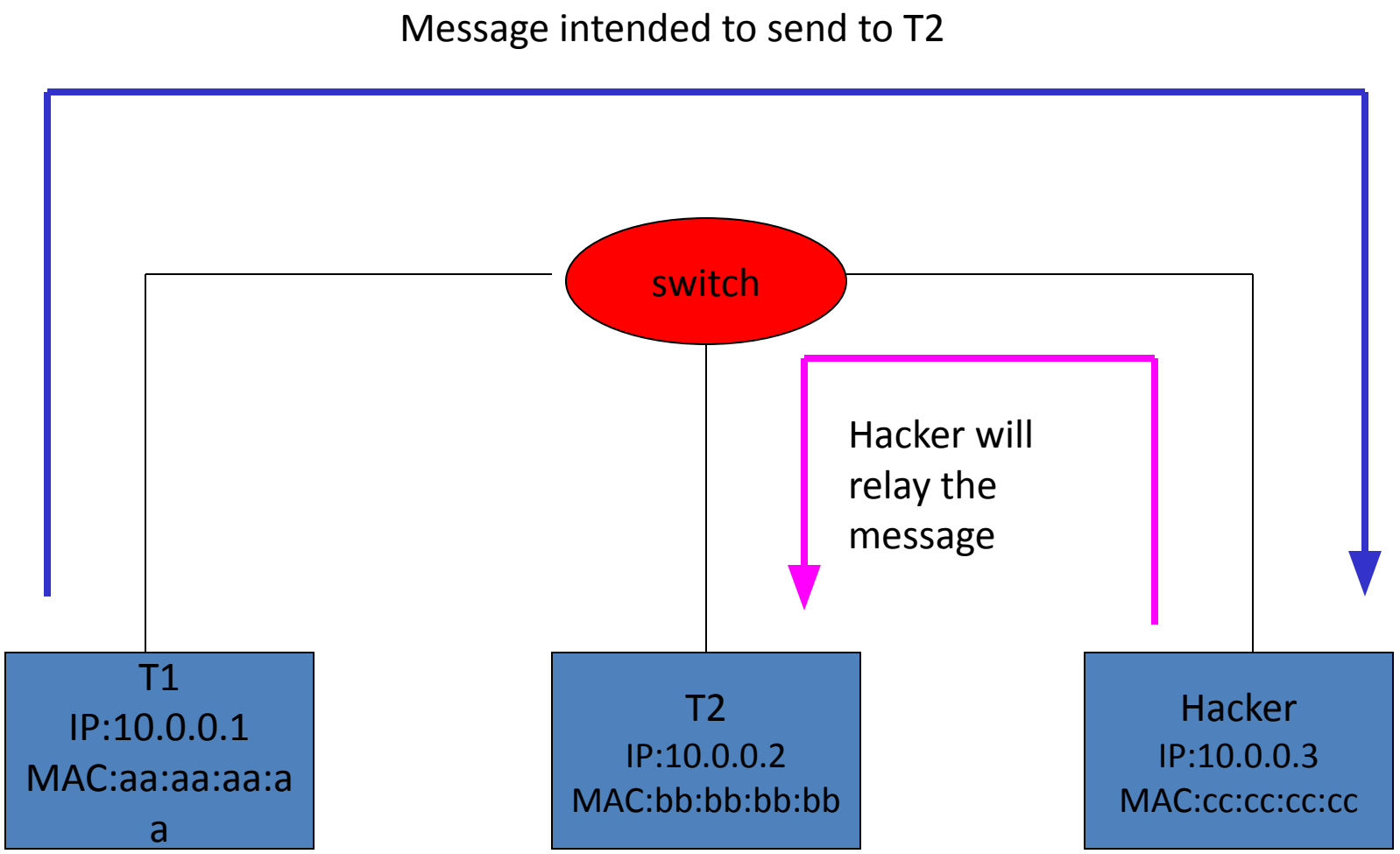
ARP cache

IP	MAC
10.0.0.2	cc:cc:cc:cc

ARP cache

IP	MAC
10.0.0.1	cc:cc:cc:cc

T2's cache is poisoned



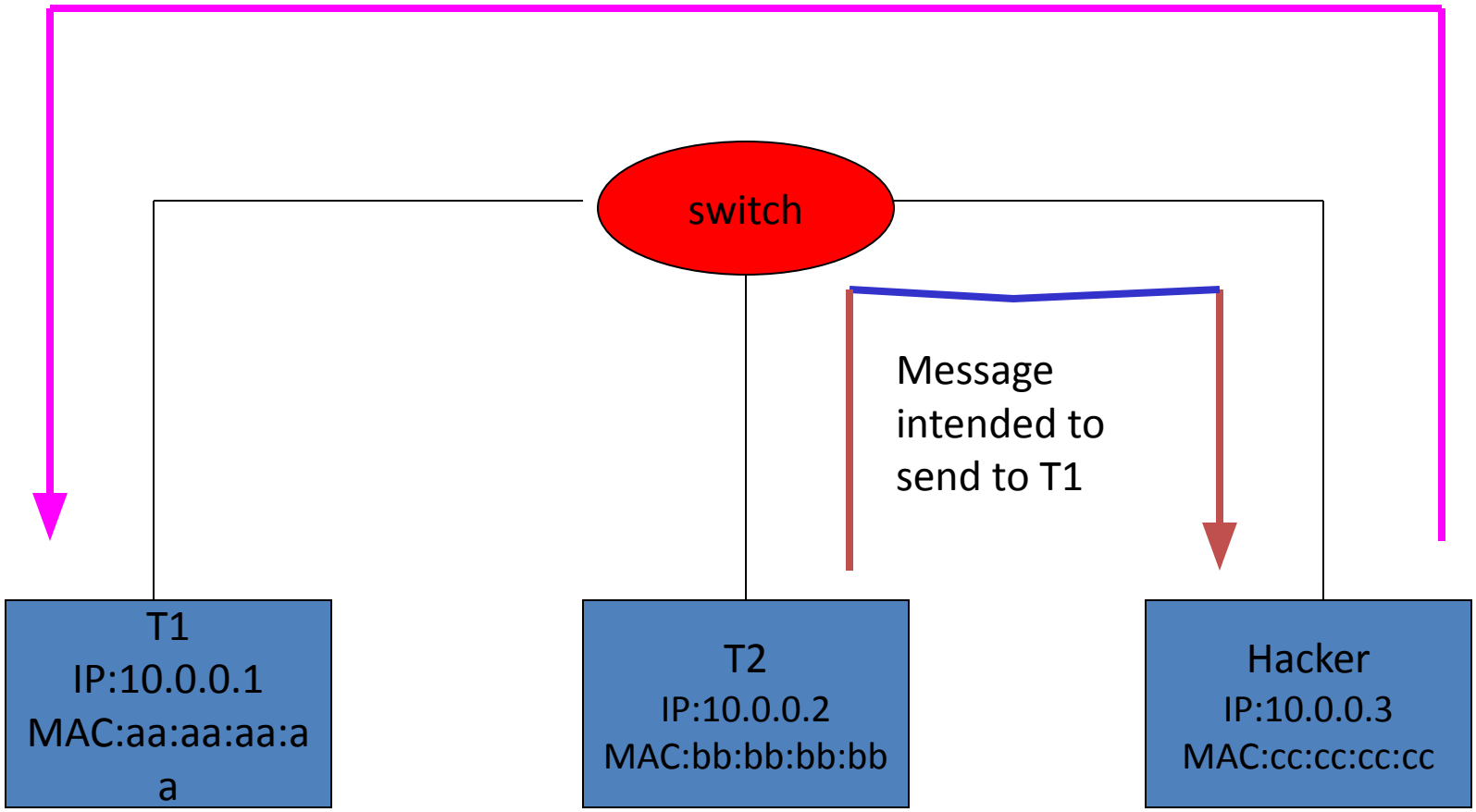
ARP cache

IP	MAC
10.0.0.2	cc:cc:cc:cc

ARP cache

IP	MAC
10.0.0.1	cc:cc:cc:cc

Hacker will relay the message



ARP cache

IP	MAC
10.0.0.2	cc:cc:cc:cc

ARP cache

IP	MAC
10.0.0.1	cc:cc:cc:cc

- Possible types of attacks
  - Sniffing
    - By using ARP spoofing, all the traffic can be directed to the hackers.
    - It is possible to perform sniffing on a switched network now.
  - DoS
    - Updating ARP caches with non-existent MAC addresses will cause frames to be dropped.
    - These could be sent out in a sweeping fashion to all clients on the network in order to cause a Denial of Service attack (DoS).

- This could also be a post-MiM attacks: target computers will continue to send frames to the attacker's MAC address even after they remove themselves from the communication path.
- In order the perform a clean MiM attack, the hacker will restore the ARP entries.

– Hijacking
  - By using MiM attack, all the traffic of a TCP connection will go through the hacker.
  - Now it is much easier to hijack the session as compared to the method we discussed earlier in TCP exploits.

- Broadcasting
  - Frames can be broadcast to the entire network by setting the destination address to FF:FF:FF:FF:FF:FF (broadcast MAC).
  - By sweeping a network with spoofed ARP replies which set the MAC of the network gateway to the broadcast address, all external-bound data will be broadcast, thus enabling sniffing.
  - If a hacker listen for ARP requests and generate reply with broadcast address, large amounts of data could be broadcast on the networks.

- Cloning
  - A MAC address is supposed to be unique.
  - It is possible to change the MAC address of a network card (burn into the ROM).
  - It is also possible to change the MAC on the OS level in some OS.
    - ifconfig
  - An attacker can DoS a target computer, then assign themselves the IP and MAC of the target computer, thus he can receive all frames intended for the target.

Defenses against ARP Spoofing

- No Universal defense.
- Use static ARP entries
  - Cannot be updated
  - Spoofed ARP replies are ignored.
  - ARP table needs a static entry for each machine on the network.
  - Large overhead
    - Deploying these tables
    - Keep the table up-to-date

- Someone point out
  Windows still accepts spoofed ARP replies and updates the static entry with the forged MAC.
  - Sabotaging the purpose of static routes.

- Port Security
  - Also known as port binding or MAC Binding.
  - A feature on some high-end switches.
  - Prevents changes to the MAC tables of a switch.
    - Unless manually performed by a network administrator.
  - Not suitable for large networks and networks using DHCP.

- Arpwatch
  - A free UNIX program which listens for ARP replies on a network.
  - Build a table of IP/MAC associations and store it in a file.
  - When a MAC/IP pair changes (flip-flop), an email is sent to an administrator.
  - Some programs, such as Ettercap, cause only a few flip flops is difficult to be detected on a DHCP-enabled network, where flip flops occur at regular intervals.