KF School of Computing and Information Sciences
Florida International University

CNT 4403
Computing and Network Security

Network Security – Network Attacks

Dr. Kemal Akkaya

E-mail: *kakkaya@fiu.edu*

Internet

❑ The Internet is untrusted

- ➢ Have to guard against attacks
  - ✓ Passive intercepts
  - ✓ Man in the middle
  - ✓ Denial of service

❑ Attacks on Different Layers

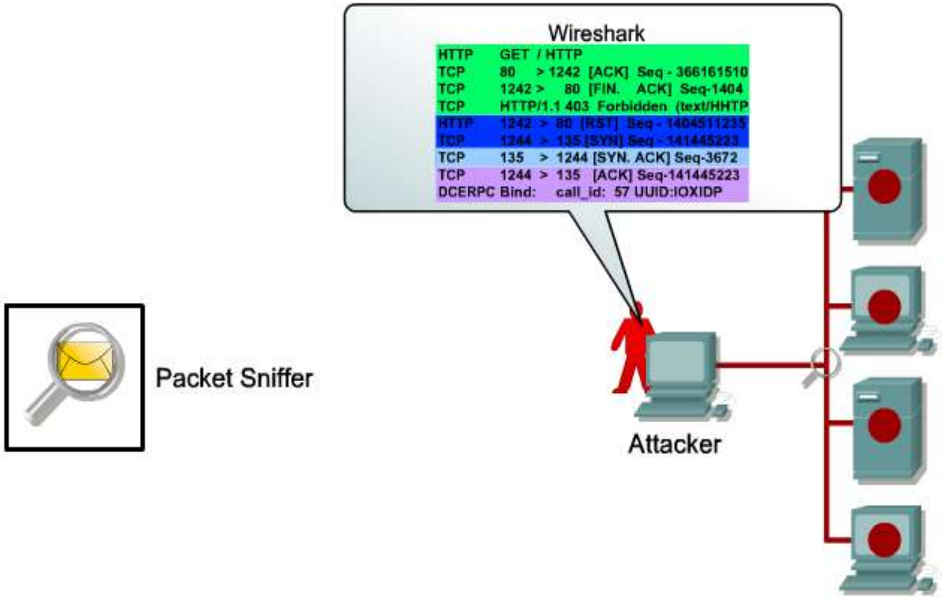
- ➢ MAC (Data Link) Layer attacks
- ➢ IP Layer Attacks
- ➢ Transport Layer Attacks
- ➢ Application Layer Attacks

❑ Security Approaches

- ➢ End-to-end : Treat Internet as big untrusted “cloud”
- ➢ Link-level: Implement protection between each router

MAC - Packet Sniffing Attacks

- **On Ethernet-based networks, any machine on the network can see the traffic for every machine on that network**



Wireshark

```
HTTP    GET  / HTTP
TCP     80    > 1242  [ACK]  Seq - 366161510
TCP     1242 >    80  [FIN.   ACK]  Seq-1404
TCP     HTTP/1.1 403  Forbidden  (text/HHTP
HTTP    1242  >  80  [RST]  Seq - 1404511235
TCP     1244  >  135 [SYN] Seq - 141445223
TCP     135   >  1244 [SYN. ACK] Seq-3672
TCP     1244  >  135   [ACK] Seq-141445223
DCERPC Bind:    call_id:  57 UUID:IOXIDP
```

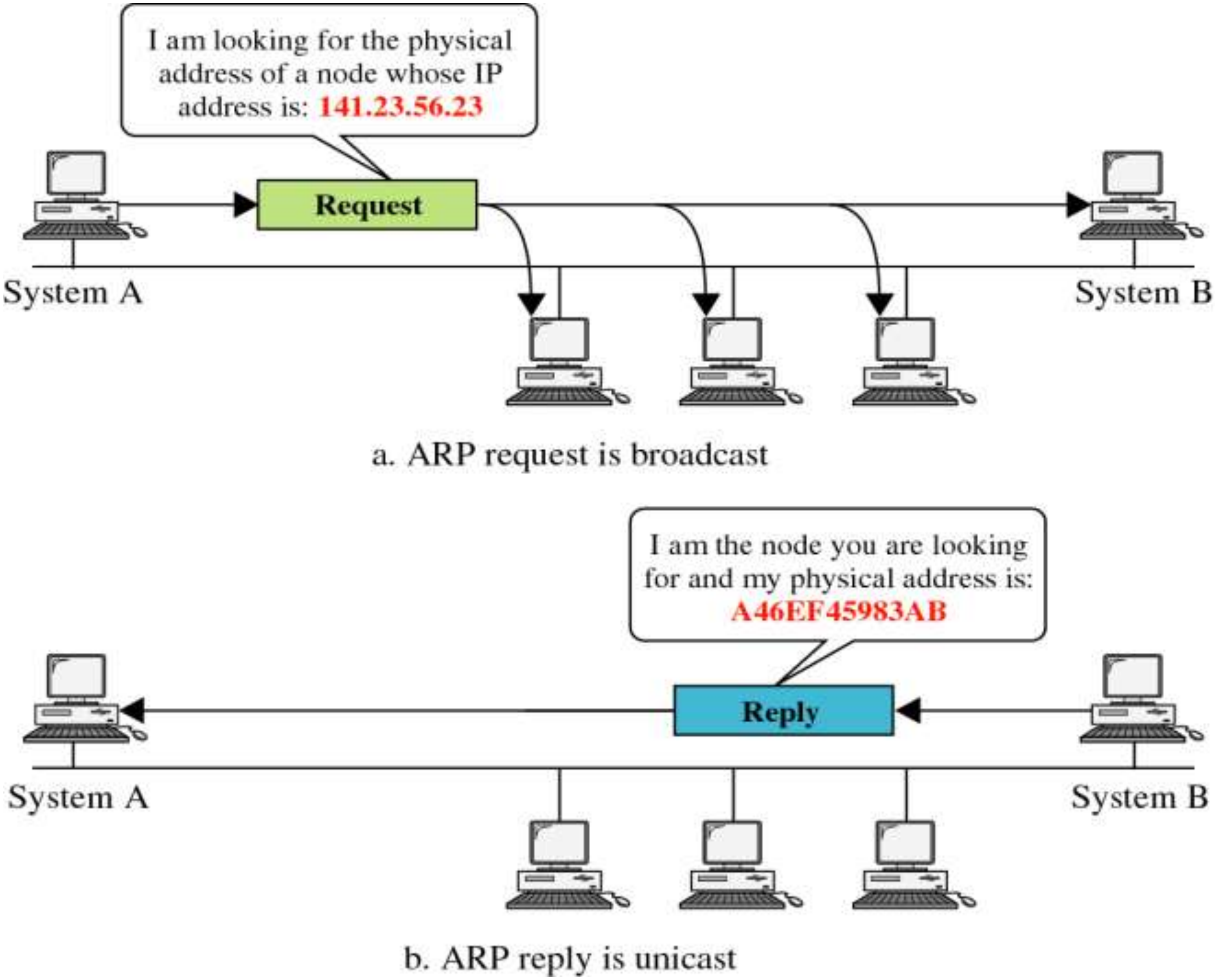
- **Network interface cards (NICs) work in non-promiscuous mode listening to only frames destined to them**
  - A packet sniffer works with promiscuous mode to listen all the traffic
  - Sniffer programs monitor all traffic and capturing the first 128 bytes or so of every unencrypted FTP or Telnet session (the part that contains user passwords)
- **Solutions:**
  - Use encryption to encrypt traffic (ssh, ssl, etc.)
  - Do not use hubs

Replay Attacks via Sniffing

- Via sniffing replay attacks possible.
- Replay involves capturing traffic while in transit and use that to gain access to systems.
- Example:
  - Hacker sniffs login information of a valid user
  - Even if the information is encrypted, the hacker replays the login information to fool the system and gains access
- Countermeasure
  - Session tokens
  - Timestamping

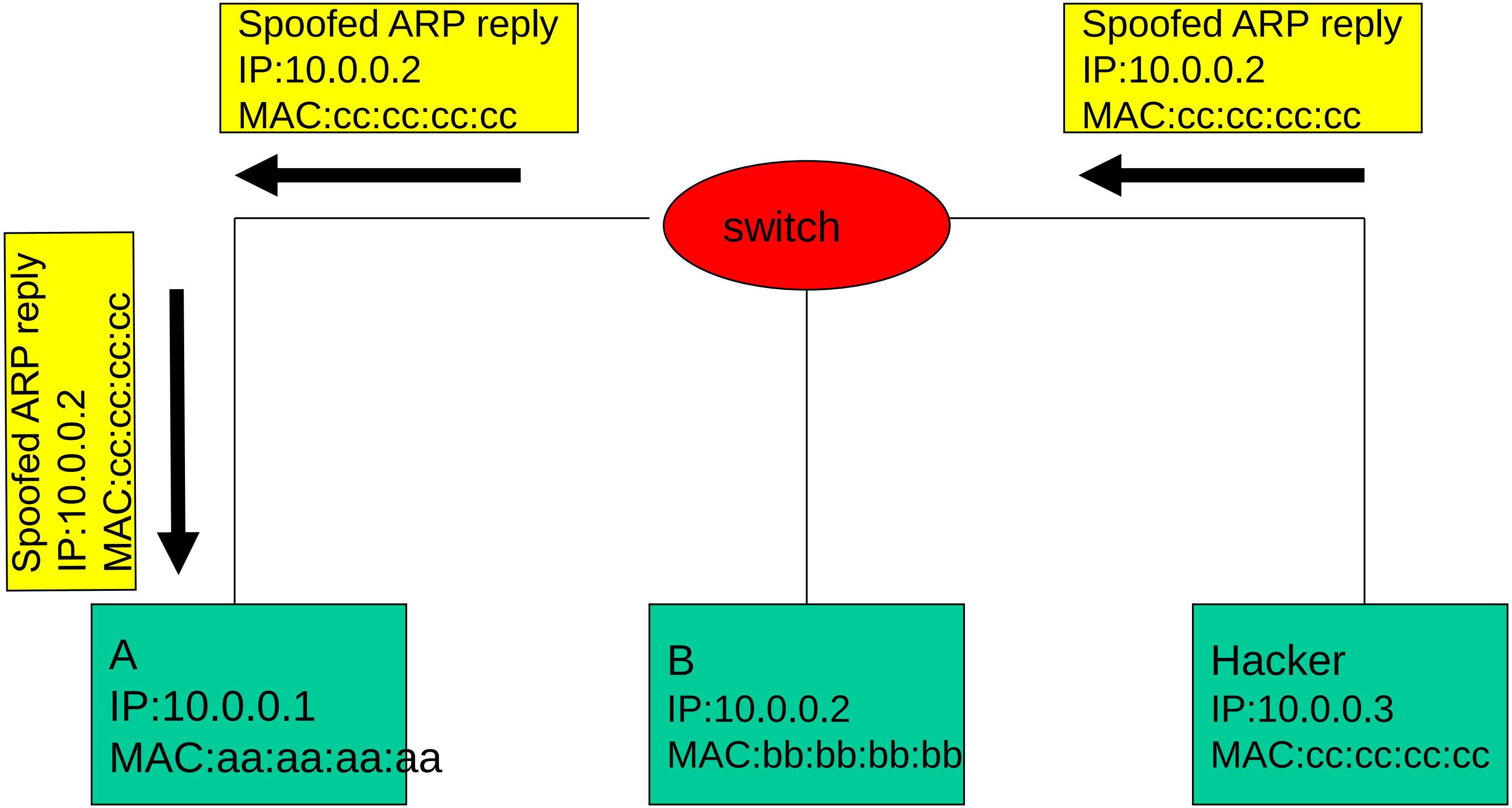
MAC - Address Resolution Protocol

- ARP is used by routers extensively to find the destination node's MAC address
- To deliver the packet to the destination node, the router broadcasts the IP address of the destination
- In response, it receives the MAC address (48-bits) via unicast.


I am looking for the physical address of a node whose IP address is: 141.23.56.23
Request
System A
System B
a. ARP request is broadcast
I am the node you are looking for and my physical address is: A46EF45983AB
Reply
System A
System B
b. ARP reply is unicast

ARP Poisoning Attacks

- ❑ **Construct spoofed ARP replies.**
  - ➢ Reply is destined for a particular address
  - ➢ Changes the MAC address of an IP address
- ❑ **A target computer could be convinced to send frames destined for computer A.**
- ❑ **Computer A will have no idea that this the ARP reply is a fake/spoofed one sent from an attacker computer.**
- ❑ **This process of updating a target computer's ARP cache is referred to as "ARP poisoning".**



Spoofed ARP reply
IP:10.0.0.2
MAC:cc:cc:cc:cc

Spoofed ARP reply
IP:10.0.0.2
MAC:cc:cc:cc:cc

switch

Spoofed ARP reply
IP:10.0.0.2
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

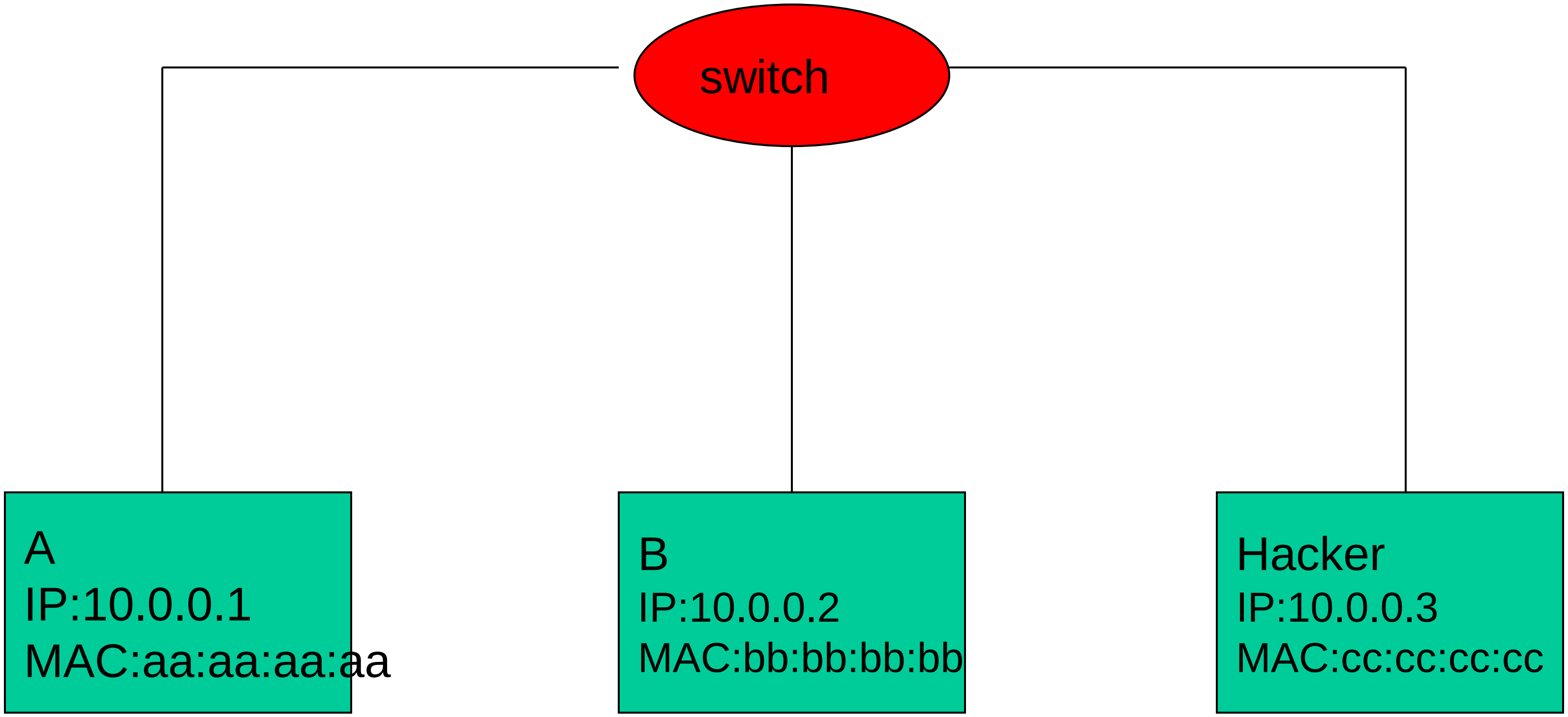
Hacker
IP:10.0.0.3
MAC:cc:cc:cc:cc

ARP cache

IP	MAC
10.0.0.2	bb:bb:bb:bb

ARP cache

IP	MAC
10.0.0.1	aa:aa:aa:aa



switch

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

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

Hacker
IP:10.0.0.3
MAC:cc:cc:cc:cc

ARP cache

IP	MAC
10.0.0.2	cc:cc:cc:cc

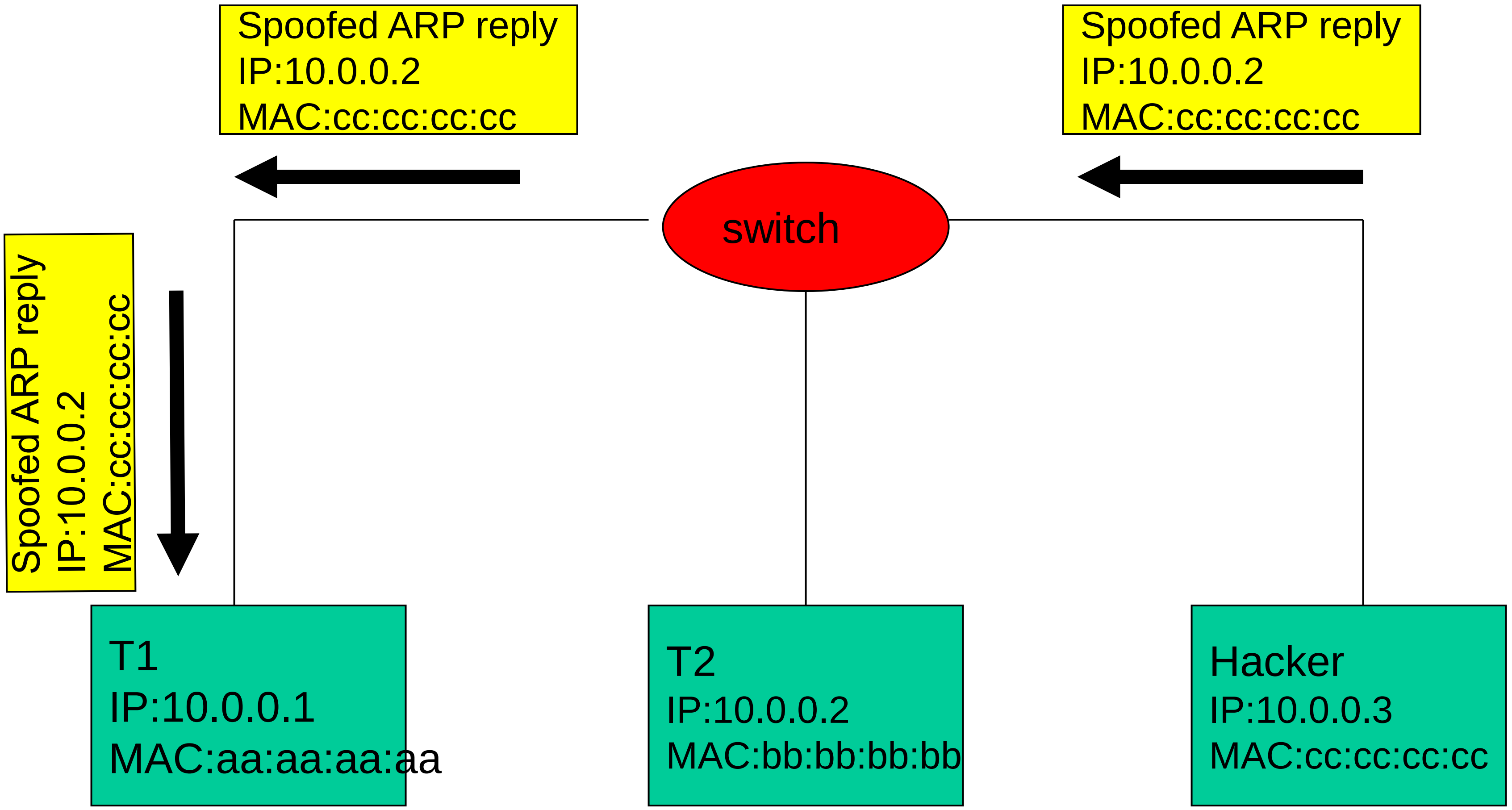
ARP cache

IP	MAC
10.0.0.1	aa:aa:aa:aa

Man in the Middle Attacks via ARP Spoofing/Poisoning

- ❑ **A hacker inserts his computer between the communications path of two target computers (MitM).**
  - ➢ 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.



Spoofed ARP reply
IP:10.0.0.2
MAC:cc:cc:cc:cc

Spoofed ARP reply
IP:10.0.0.2
MAC:cc:cc:cc:cc

switch

Spoofed ARP reply
IP:10.0.0.2
MAC:cc:cc:cc:cc

T1
IP:10.0.0.1
MAC:aa:aa:aa:aa

T2
IP:10.0.0.2
MAC:bb:bb:bb:bb

Hacker
IP:10.0.0.3
MAC:cc:cc:cc:cc

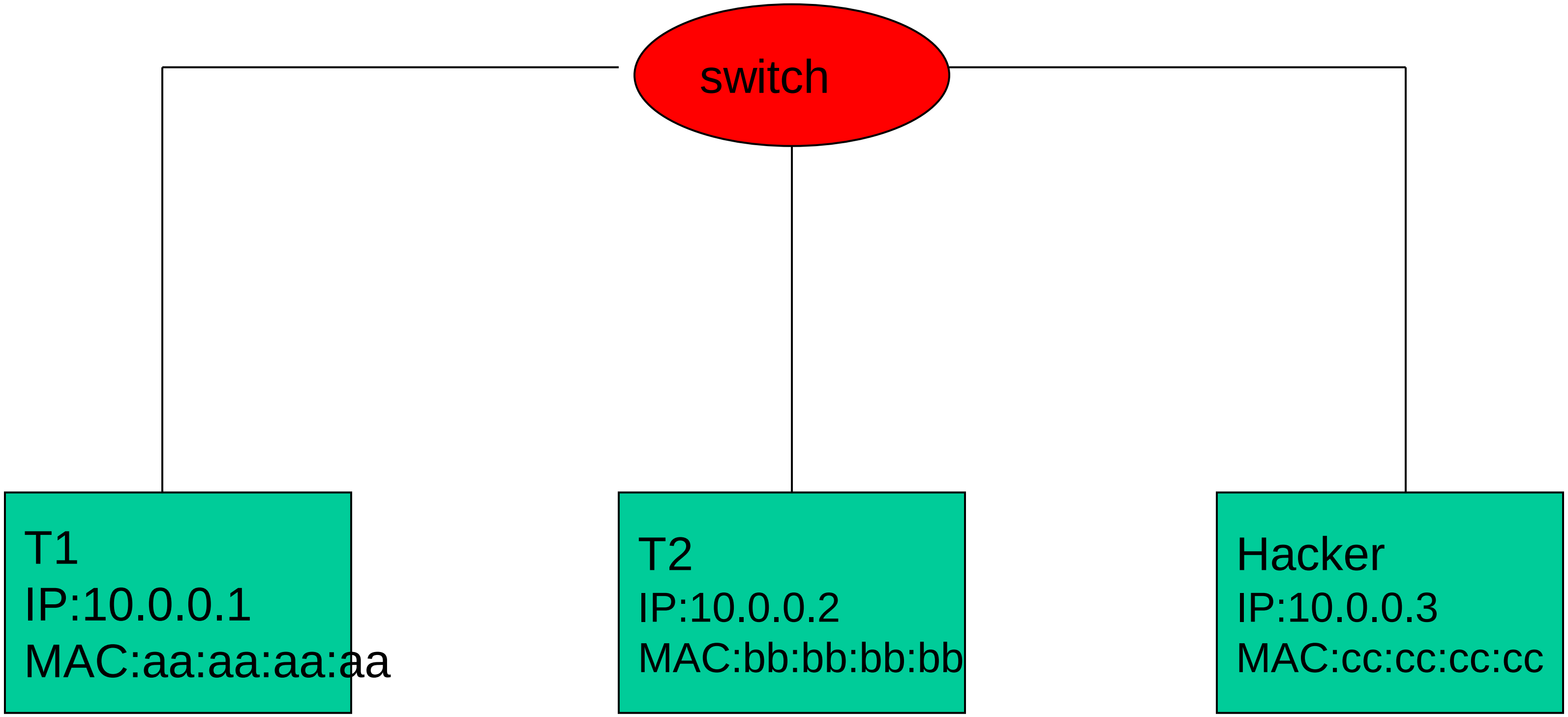
ARP cache

IP	MAC
10.0.0.2	bb:bb:bb:bb

ARP cache

IP	MAC
10.0.0.1	aa:aa:aa:aa

T1’s cache is poisoned



switch

T1
IP:10.0.0.1
MAC:aa:aa:aa:aa

T2
IP:10.0.0.2
MAC:bb:bb:bb:bb

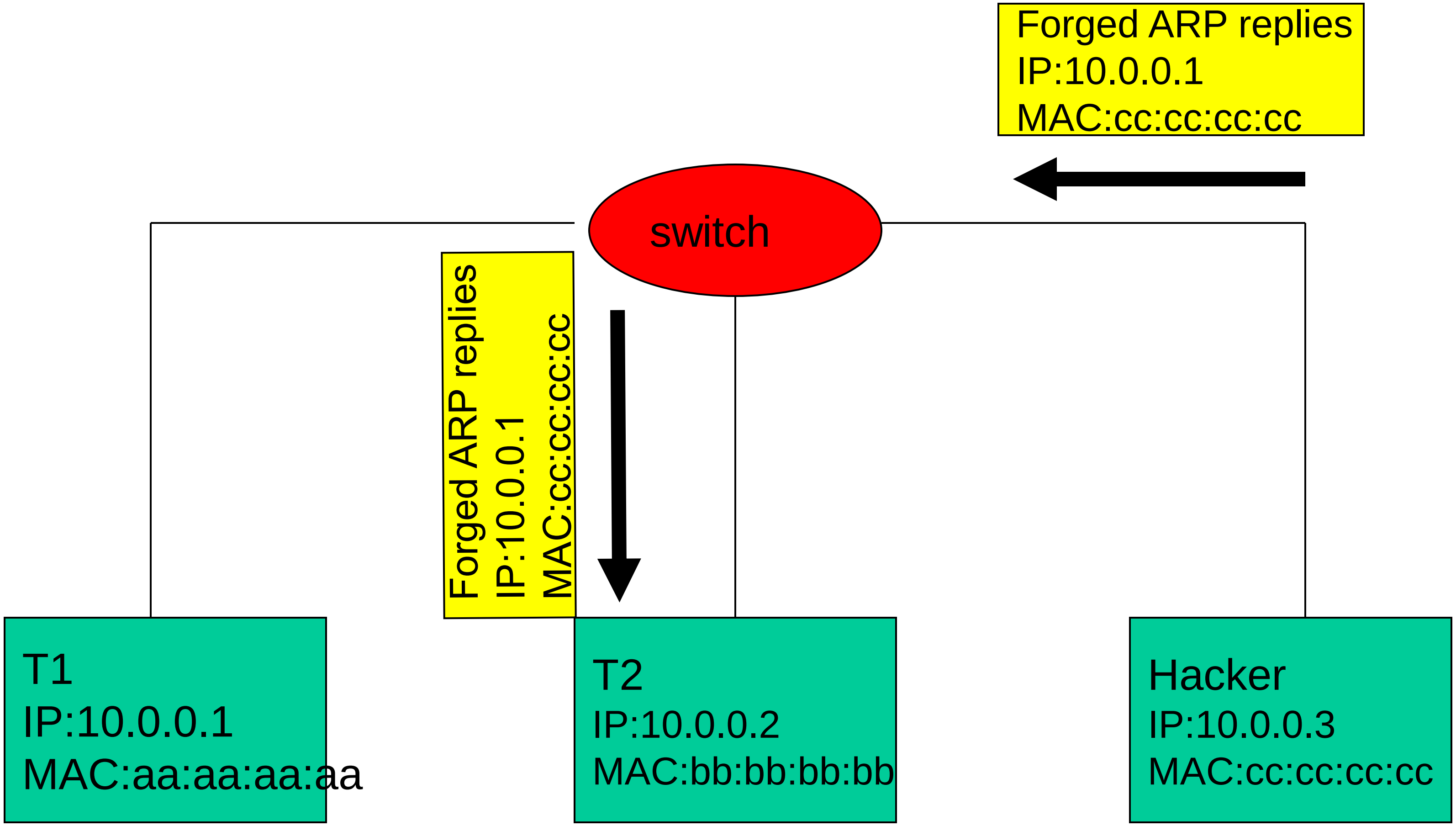
Hacker
IP:10.0.0.3
MAC:cc:cc:cc:cc

ARP cache

IP	MAC
10.0.0.2	cc:cc:cc:cc

ARP cache

IP	MAC
10.0.0.1	aa:aa:aa:aa



Forged ARP replies
IP:10.0.0.1
MAC:cc:cc:cc:cc

switch

Forged ARP replies
IP:10.0.0.1
MAC:cc:cc:cc:cc

T1
IP:10.0.0.1
MAC:aa:aa:aa:aa

T2
IP:10.0.0.2
MAC:bb:bb:bb:bb

Hacker
IP:10.0.0.3
MAC:cc:cc:cc:cc

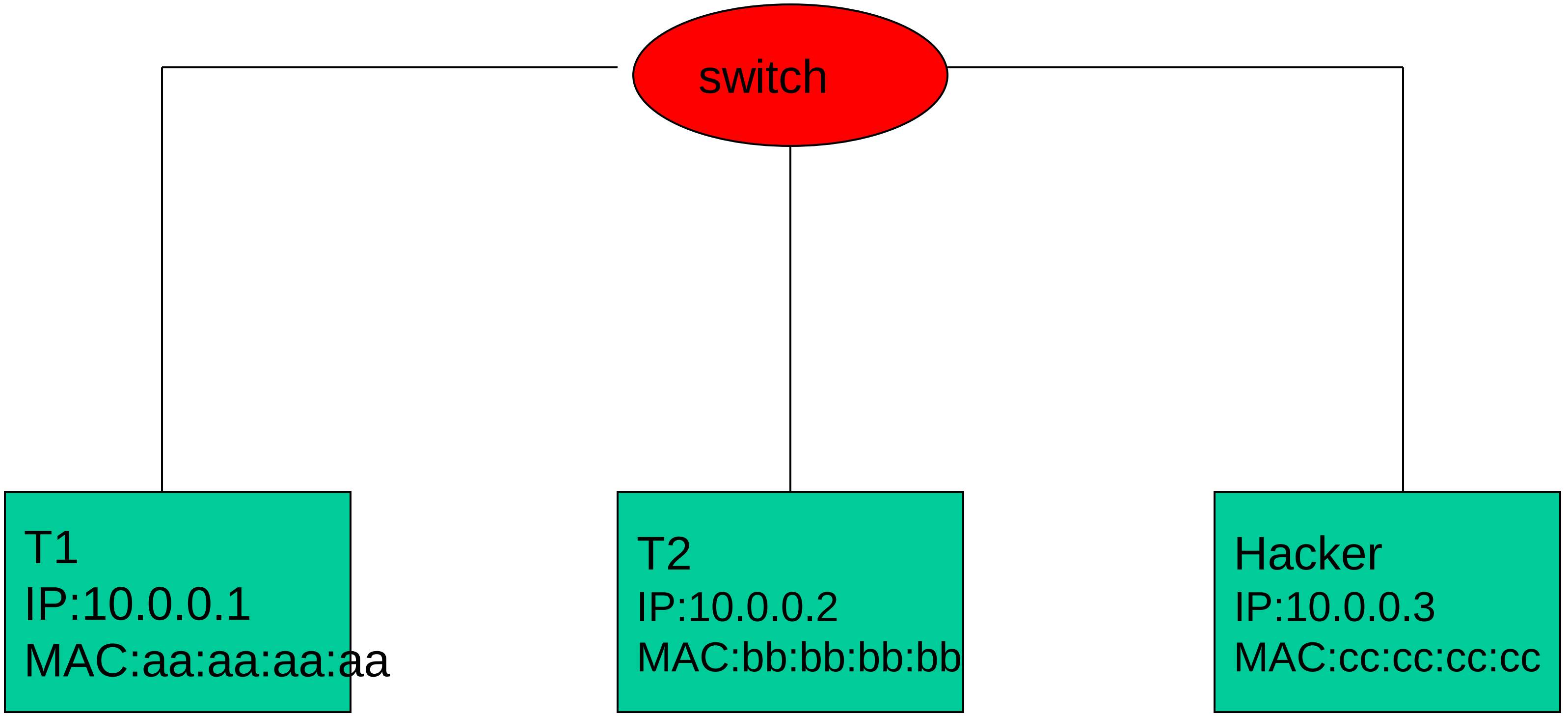
ARP cache

IP	MAC
10.0.0.2	cc:cc:cc:cc

ARP cache

IP	MAC
10.0.0.1	aa:aa:aa:aa

T2’s cache is poisoned



switch

T1
IP:10.0.0.1
MAC:aa:aa:aa:aa

T2
IP:10.0.0.2
MAC:bb:bb:bb:bb

Hacker
IP:10.0.0.3
MAC:cc:cc:cc:cc

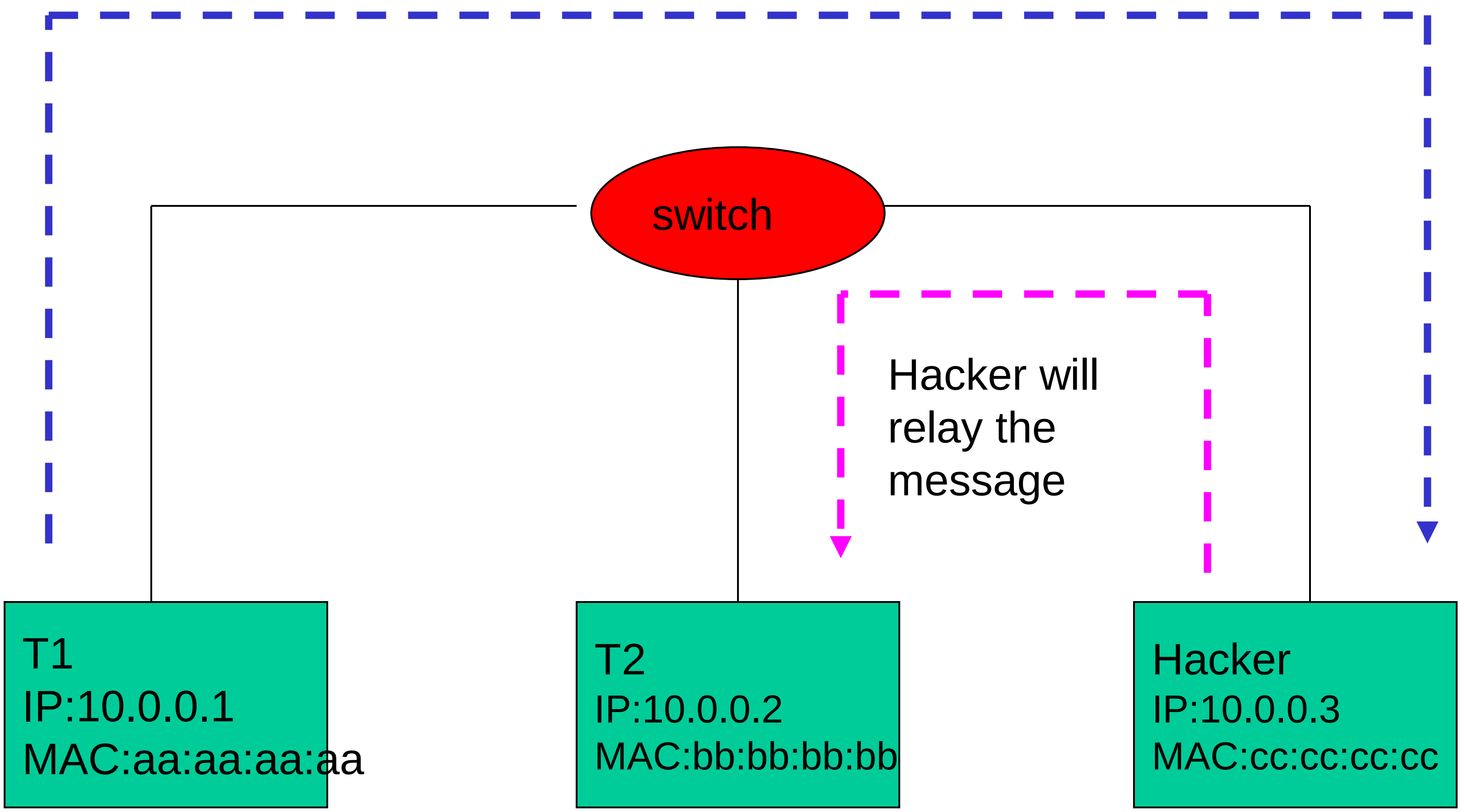
ARP cache

IP	MAC
10.0.0.2	cc:cc:cc:cc

ARP cache

IP	MAC
10.0.0.1	cc:cc:cc:cc

Message intended to send to T2



switch

Hacker will relay the message

T1
IP:10.0.0.1
MAC:aa:aa:aa:aa

T2
IP:10.0.0.2
MAC:bb:bb:bb:bb

Hacker
IP:10.0.0.3
MAC:cc:cc:cc:cc

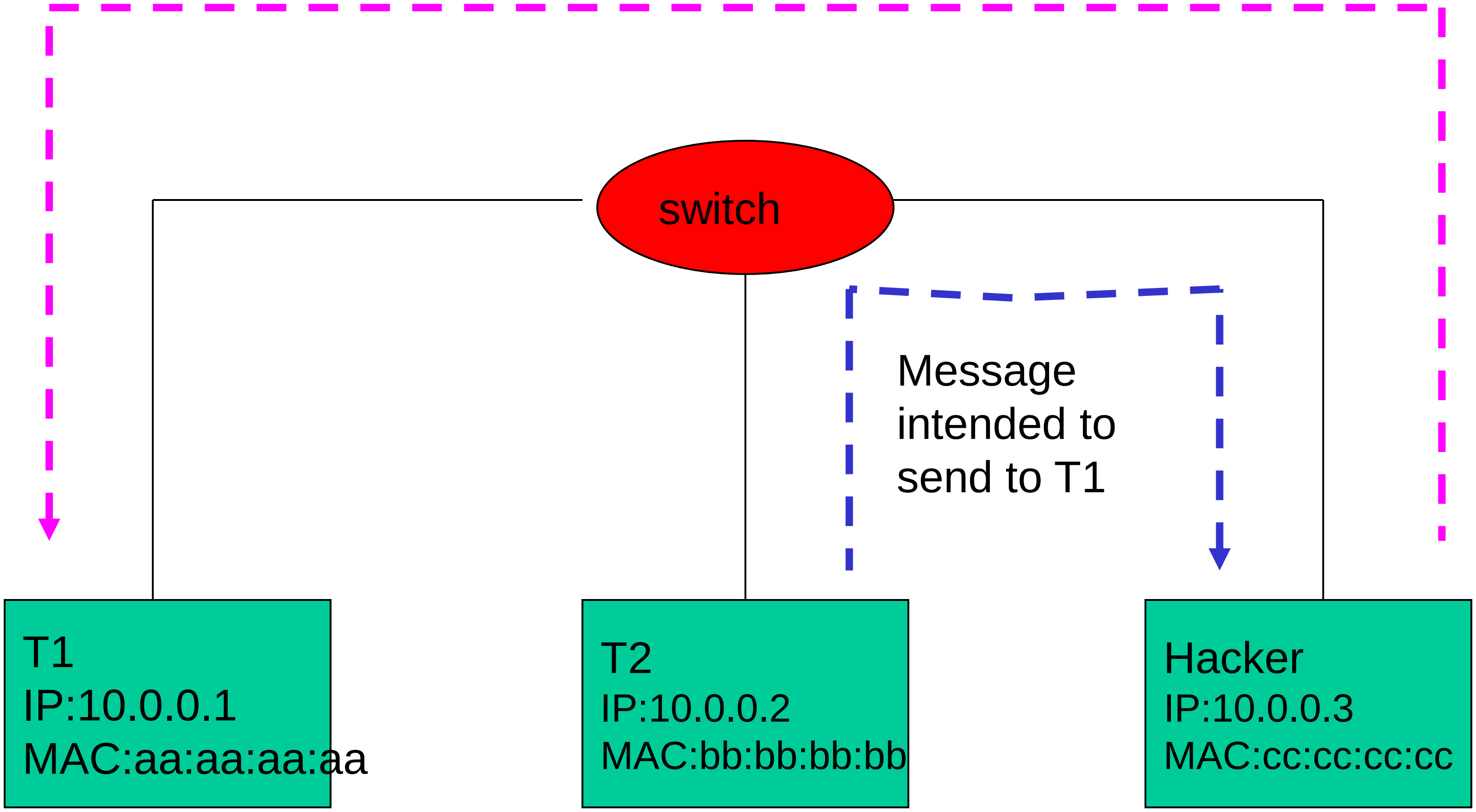
ARP cache

IP	MAC
10.0.0.2	cc:cc:cc:cc

ARP cache

IP	MAC
10.0.0.1	cc:cc:cc:cc

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

Other possible types of attacks with ARP Poisoning

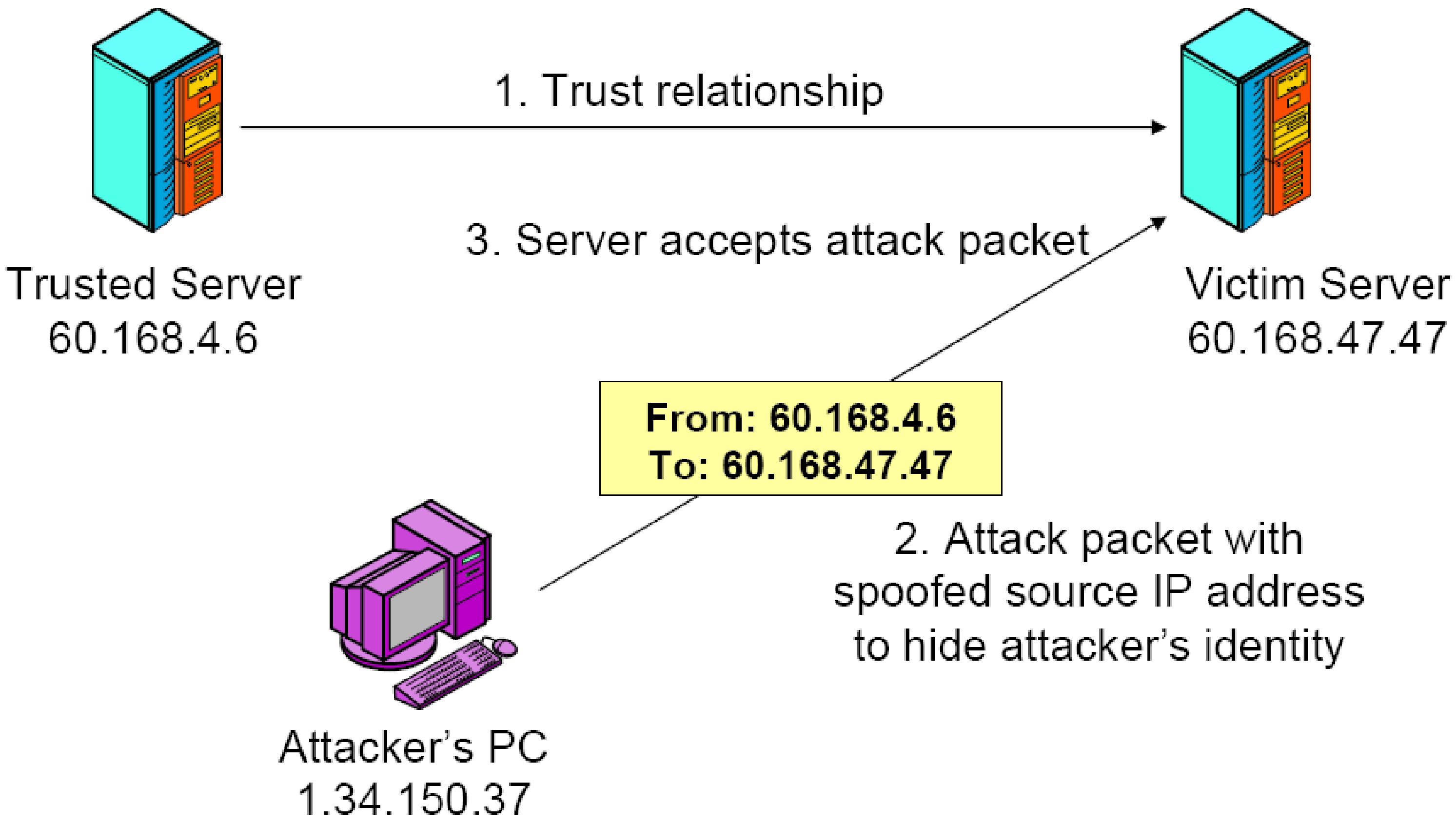
- ❑ **Denial of Service (DoS)**
  - ➢ Updating ARP caches with non-existent MAC addresses will cause frames to be dropped.
  - ➢ These could be sent out in a sweeping fashion to all clients on the network in order to cause a DoS attack.
- ❑ **Broadcasting**
  - ➢ Frames can be broadcast to the entire network by setting the destination address to FF:FF:FF:FF:FF:FF (broadcast MAC).
  - ➢ 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.
- ❑ **Hijacking**
  - ➢ By using this attack, all the traffic of a TCP connection will go through the hacker.
  - ➢ It is much easier to hijack the session (TCP hijacking)

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 the tables & keeping them up-to-date
- ❑ **Port Security**
  - ➢ 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, an email is sent to an administrator.

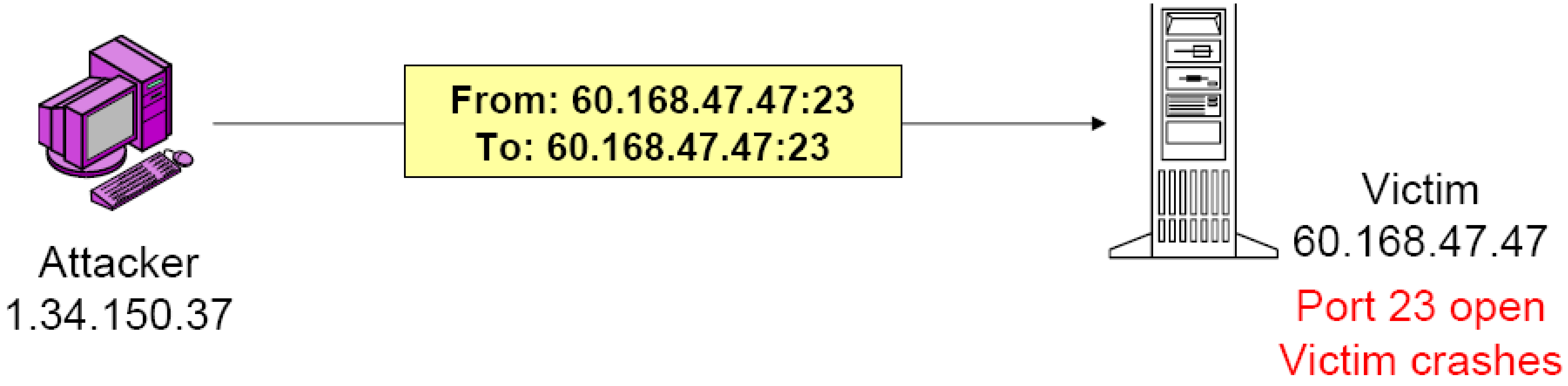
IP Layer – IP Spoofing

- Exploits trust relationships between routers



IP Layer - Land Attack

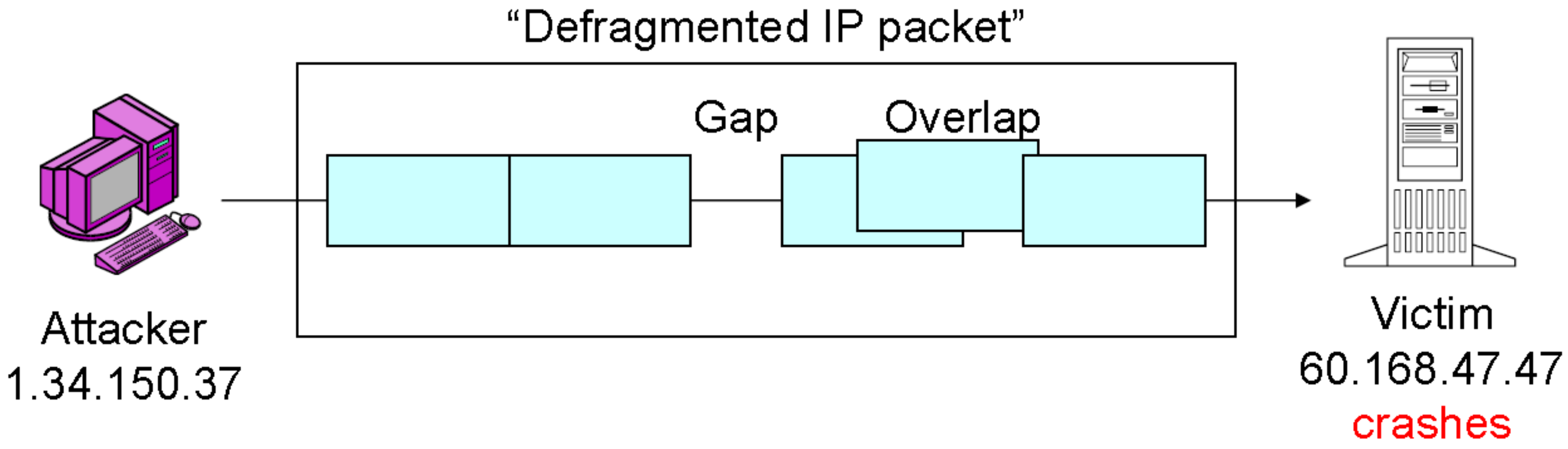
- ❑ **A denial of service (DoS) attack**
- ❑ **Exploits IP Spoofing**
  - ➢ The attacker sends an IP packet with the same source and destination address
  - ➢ Source and destination port numbers are also same in the TCP header
  - ➢ May cause crashing with faulty implementations



From: 60.168.47.47:23
To: 60.168.47.47:23

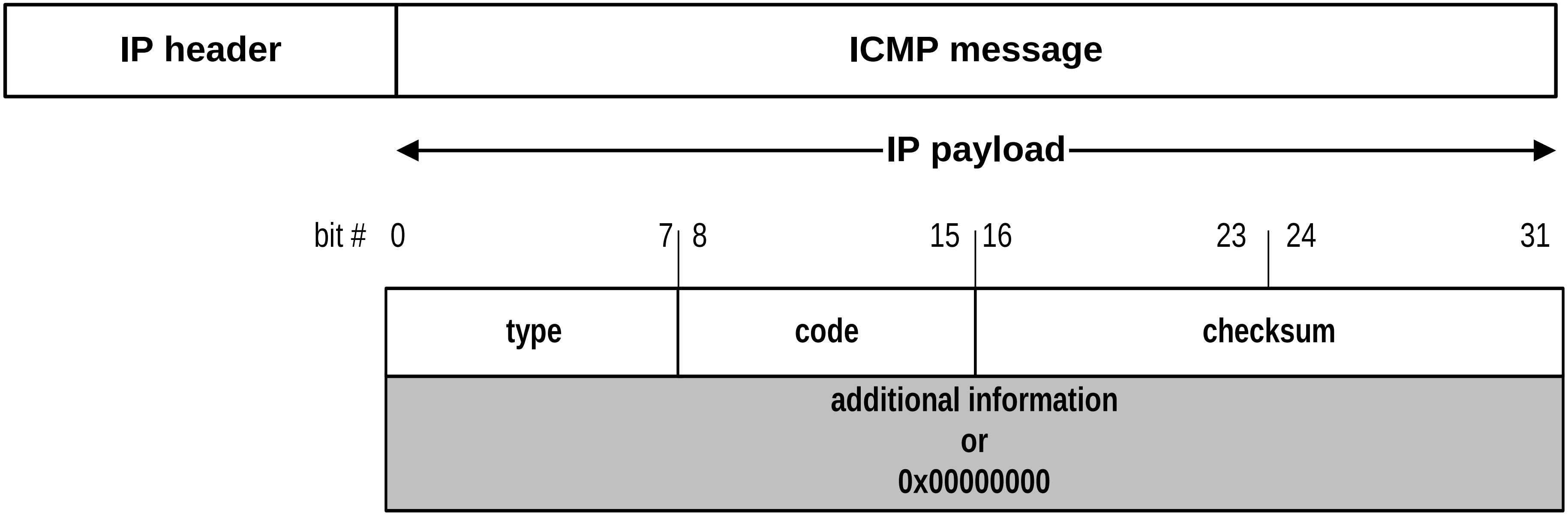
IP Layer – Teardrop Attack

- **DoS type of attack**
  - Works by altering the offset field in every other TCP/IP packet header
  - Causes overlapping IP fragments
    - ✓ Called a “fragment attack” because of this property
    - ✓ server cannot reassemble the fragments correctly
    - ✓ Usually causes loss of network connection or the blue screen of death for clients who are connected to the target
      - May cause damage if a client has unsaved data in an open application



IP Layer - ICMP

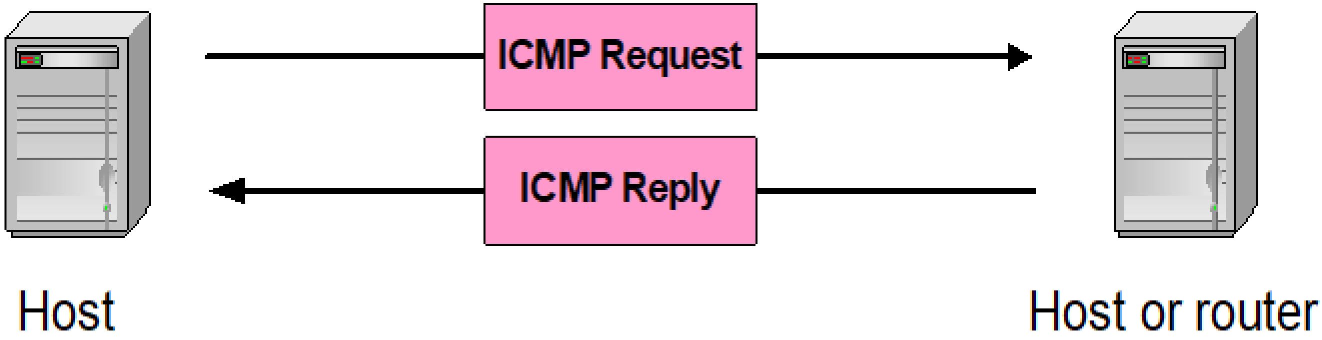
- **The Internet Control Message Protocol (ICMP) is a helper protocol that supports IP with facility for**
  - Error reporting
  - Simple queries
- **ICMP messages are encapsulated as IP datagrams:**



How ICMP works?

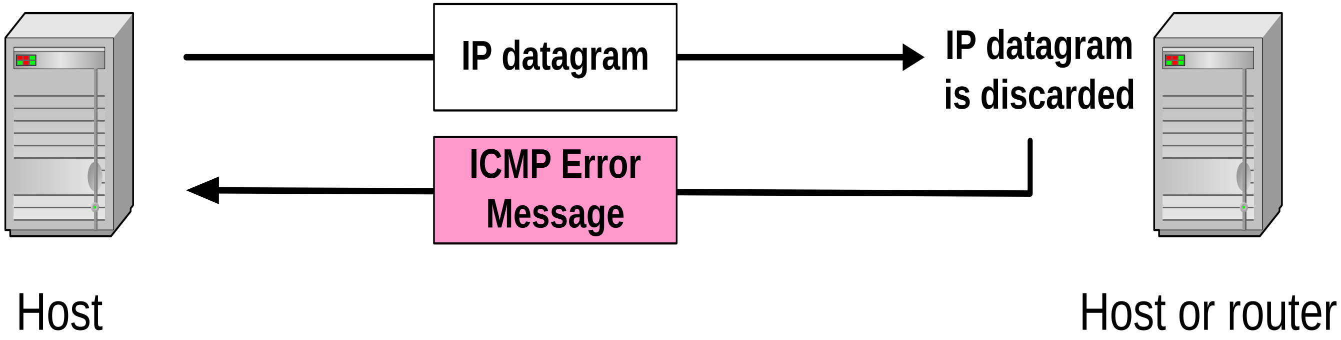
❑ Queries

- ➢ Each Ping is translated into an *ICMP Echo Request*
- ➢ The Ping'ed host responds with an *ICMP Echo Reply*



❑ Error Messages

- ➢ Sent by the routers (different message codes exist)



ICMP Sample Message Codes

Code	Description	Reason for Sending
0	Network Unreachable	No routing table entry is available for the destination network.
1	Host Unreachable	Destination host should be directly reachable, but does not respond to ARP Requests.
2	Protocol Unreachable	The protocol in the protocol field of the IP header is not supported at the destination.
3	Port Unreachable	The transport protocol at the destination host cannot pass the datagram to an application.
4	Fragmentation Needed and DF Bit Set	IP datagram must be fragmented, but the DF bit in the IP header is set.

ICMP Attack - Ping of Death

- ❑ **ICMP echo requests are a maximum of 65,525 bytes (counting the header)**
  - ➢ Sending a packet larger than 65,525 bytes can cause buffer overflows and OS failure
- ❑ **Packet fragments use offsets to determine the next packet**
  - ❑ By manipulating the offsets/packets you can create a packet of size > 65,525 bytes
- ❑ **When the victim combines the fragments the OS can shut down, restart or freeze**
- ❑ **How to prevent it:**
  - ➢ Block ping at firewall
  - ➢ Have OS check the packet size as it combines fragments
  - ➢ Overflow protection by the OS

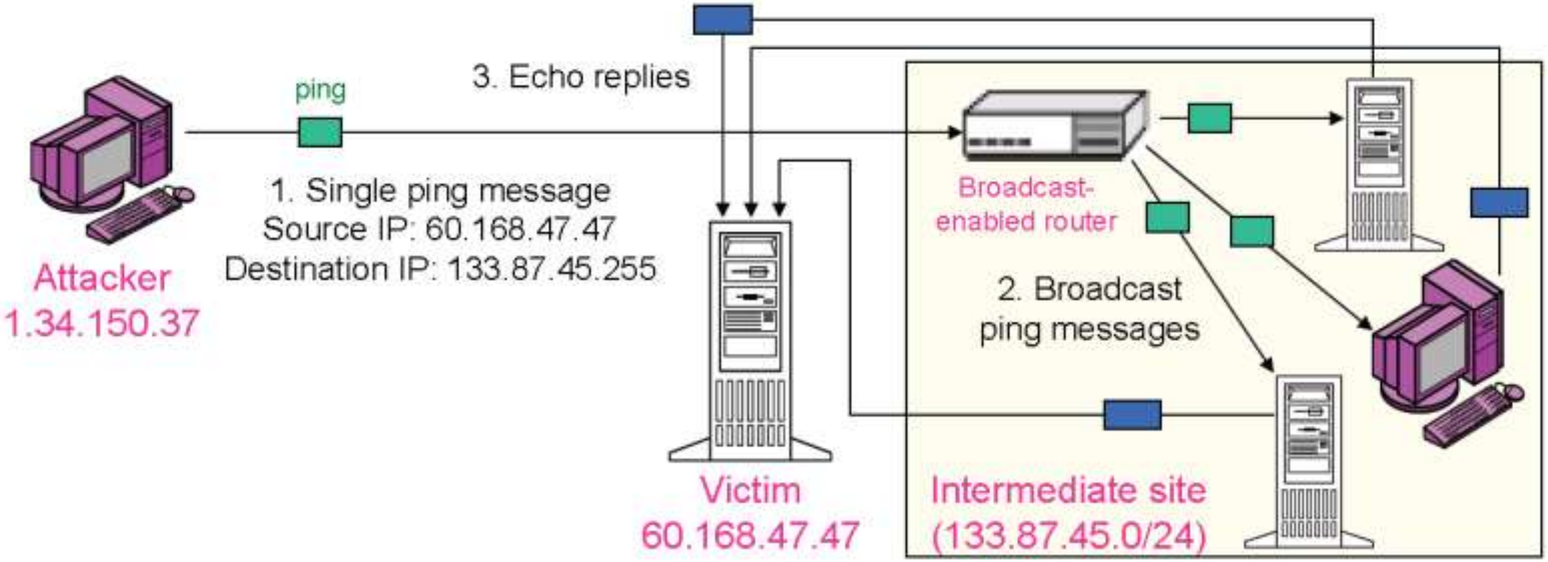
ICMP Smurf Attack

❑ DoS type of attack exploiting IP spoofing

- ➢ Spoof your IP
- ➢ Broadcast an ICMP ping request
- ➢ Most machines will reply with an echo to the victim machine
  - ✓ High impact to the victim's machine, with low impact to the attacker's machine

❑ Countermeasure

- ➢ Do not allow IP broadcast at the routers



Transmission Control Protocol (TCP)

- **Provides end-to-end control which does not exist for UDP**
  - 3-way handshake to initiate TCP
  - Sequence numbers
  - Window size for flow/congestion control

TCP Header

← **32 bits** →

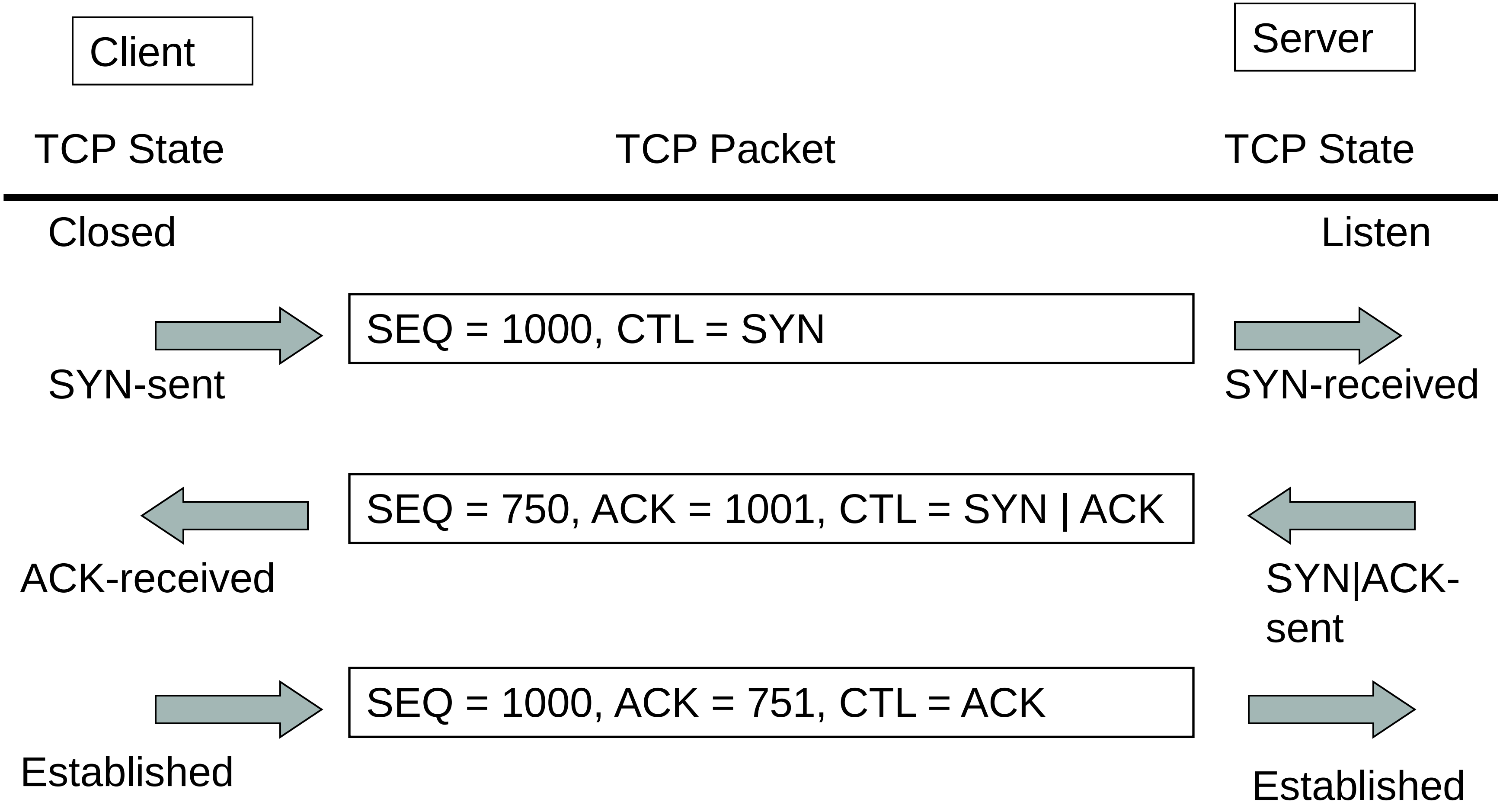
<table>
<tr><td colspan="3">Source Port</td><td colspan="2">Destination Port</td></tr>
<tr><td colspan="5">Sequence Number</td></tr>
<tr><td colspan="5">Acknowledgement Number</td></tr>
<tr><td>Data Offset</td><td>Reserved</td><td>Flags</td><td colspan="2">Window (sliding window)</td></tr>
<tr><td colspan="3">Checksum</td><td colspan="2">Urgent Pointer</td></tr>
<tr><td colspan="4">Options</td><td>Padding</td></tr>
<tr><td colspan="5">Data</td></tr>
</table>

UDP Header

← **32 bits** →

Source Port	Destination Port
Length	Checksum

TCP 3-way Handshake for Connection Establishment

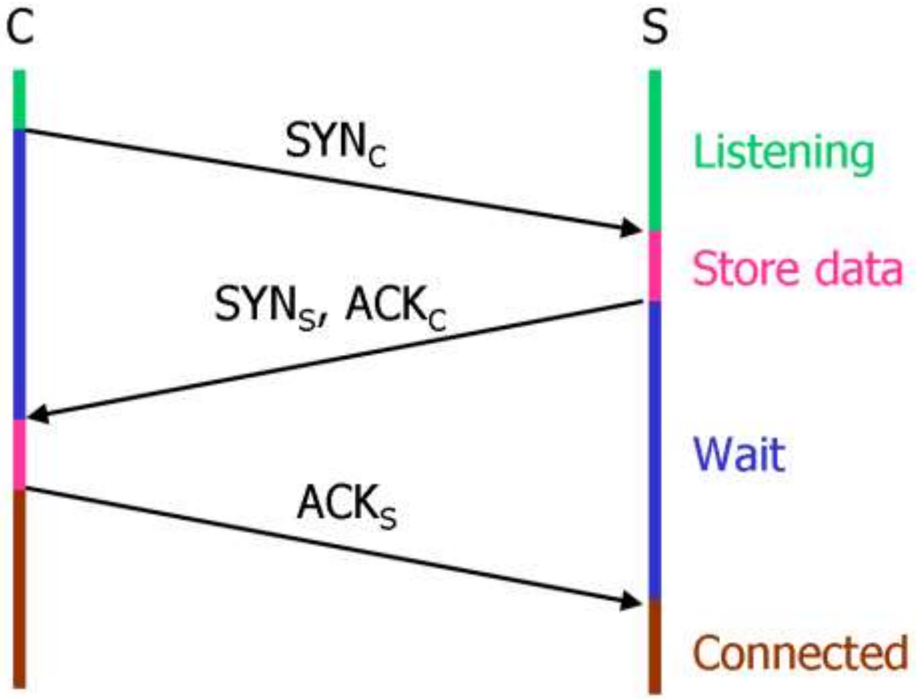


Client		Server
TCP State	TCP Packet	TCP State
Closed		Listen
SYN-sent	SEQ = 1000, CTL = SYN	SYN-received
ACK-received	SEQ = 750, ACK = 1001, CTL = SYN | ACK	SYN|ACK-sent
Established	SEQ = 1000, ACK = 751, CTL = ACK	Established

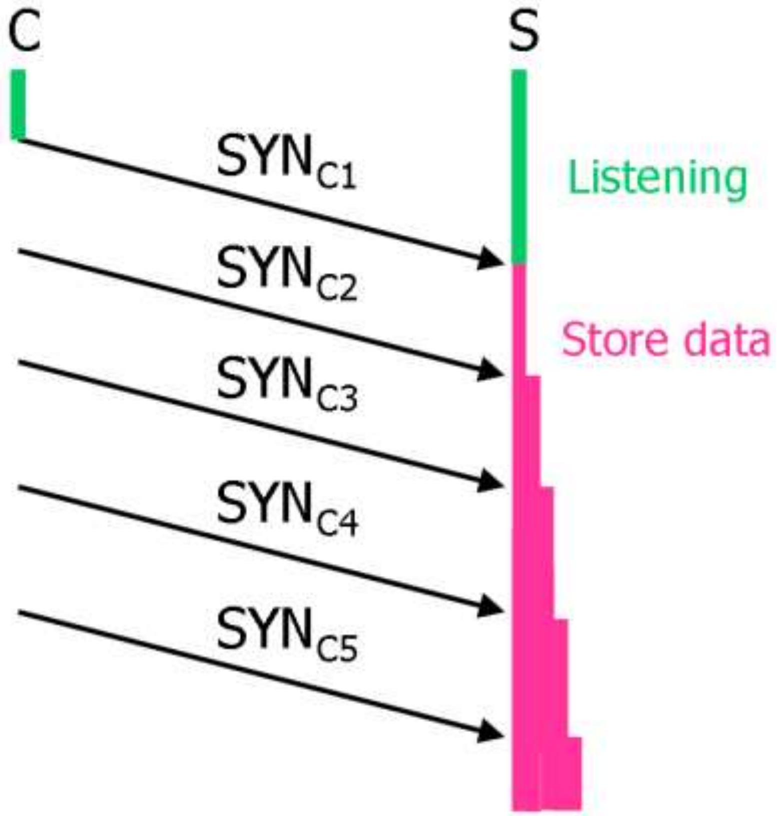
TCP Layer - SYN Flooding Attack

- ❑ **This exploits how the 3-way handshake of TCP services for opening a session works.**
- ❑ **SYN packets are sent to the target node with incomplete, spoofed or non-existent source IP addresses**
- ❑ **The node under attack sends an ACK packet and waits for response**
  - ➢ will wait for 511 seconds for ACK
  - ➢ Finite queue size for incomplete connections (1024)
- ❑ **Since the request has not been processed, it takes up memory**
- ❑ **Many such SYN packets clog the system and take up memory**
- ❑ **Eventually the attacked node is unable to process any requests as it runs out of memory space**

SYN Flooding Attack



Normal Operation

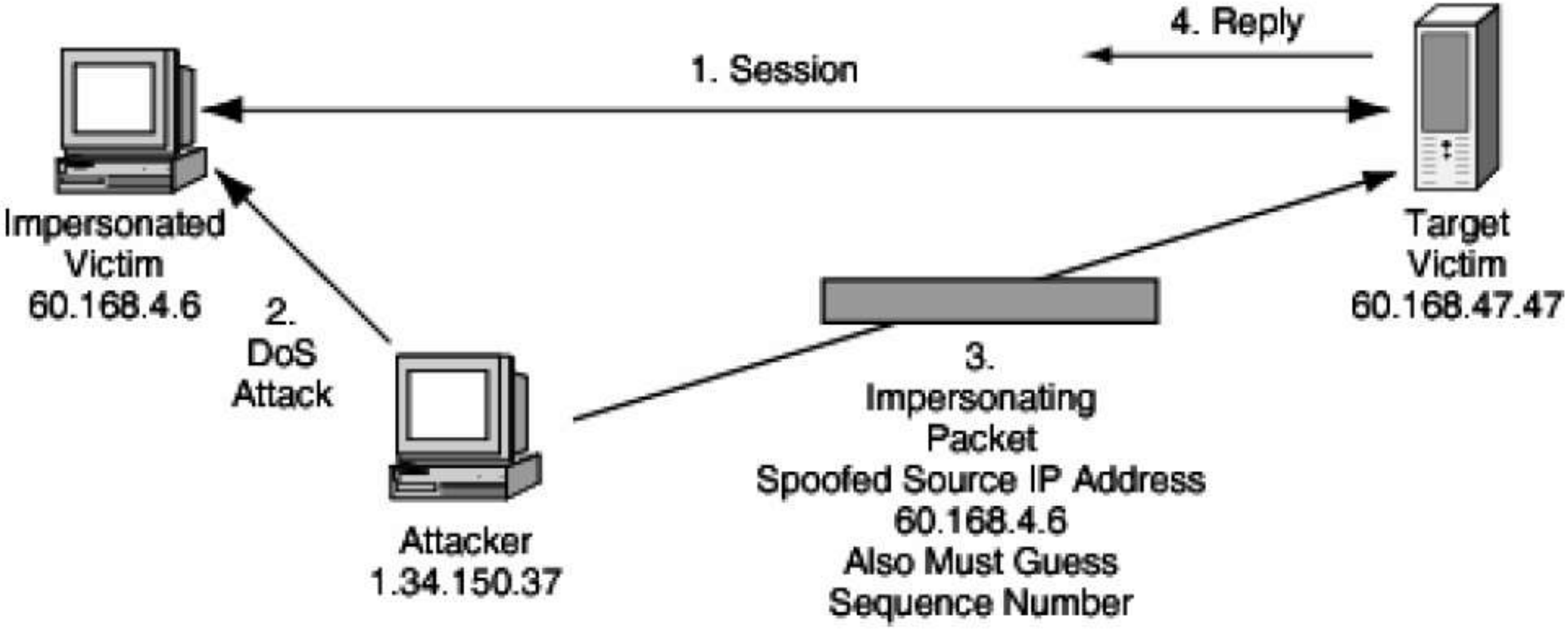


Attack

TCP Layer - Session Hijacking

- ❑ **TCP connections have associated state**
  - ➢ Starting sequence numbers, port numbers
- ❑ **Problem – what if an attacker learns these values?**
- ❑ **If an attacker learns the associated TCP state for the connection, then the connection can be hijacked!**
  - ➢ Sniff traffic
  - ➢ Guess it: Many earlier systems had predictable sequence numbers
- ❑ **Attacker can insert malicious data into the TCP stream, and the recipient will believe it came from the original source**
  - ➢ Ex. Instead of downloading and running new program, you download a virus and execute it

Session Hijacking Example


4. Reply
1. Session
Impersonated Victim 60.168.4.6
2. DoS Attack
Target Victim 60.168.47.47
Attacker 1.34.150.37
3. Impersonating Packet
Spoofed Source IP Address 60.168.4.6
Also Must Guess Sequence Number

TCP Layer - Port Scanning

- **The first step of attacker is to determine the services running on a target host.**
  - Some of these services can have known vulnerabilities
- **Port Scanner is a program that reports which ports in an individual machine are open**
- **Simplest port scanning technique:**
  - Send a SYN request with a different port number
  - Any port which sends a SYN+ACK segment is open
  - Instead of completing the handshake, send a reset (RST) segment to close the connection
    - ✓ A RST message causes the receiver to close the connection

Fingerprinting

- ❑ **Once a victim host is determined, the next step is to learn the OS and services running on this host**
  - ➢ Referred to as Fingerprinting
- ❑ **Common techniques:**
  - ➢ To send specially crafted or invalid IP, ICMP or TCP messages
  - ➢ Different OSes will respond differently (some even do not respond)
  - ➢ OS Finger printing example
    - ✓ Step 1. Attacker sends an UDP packet with DF bit set to a target host whose UDP port is closed.
    - ✓ Step 2. An ICMP "Destination unreachable port" message will be returned to the attacker.
    - ✓ Step 3. Due to the fact that different hosts will send a slightly different ICMP packet back, OS can be determined by examining several bits in the return packet.
      - – e.g., If the precedence bits field of the packet has 0xc0, the underlying operating system can most likely be deduced to be a Linux kernel based machine or a Cisco based router etc.

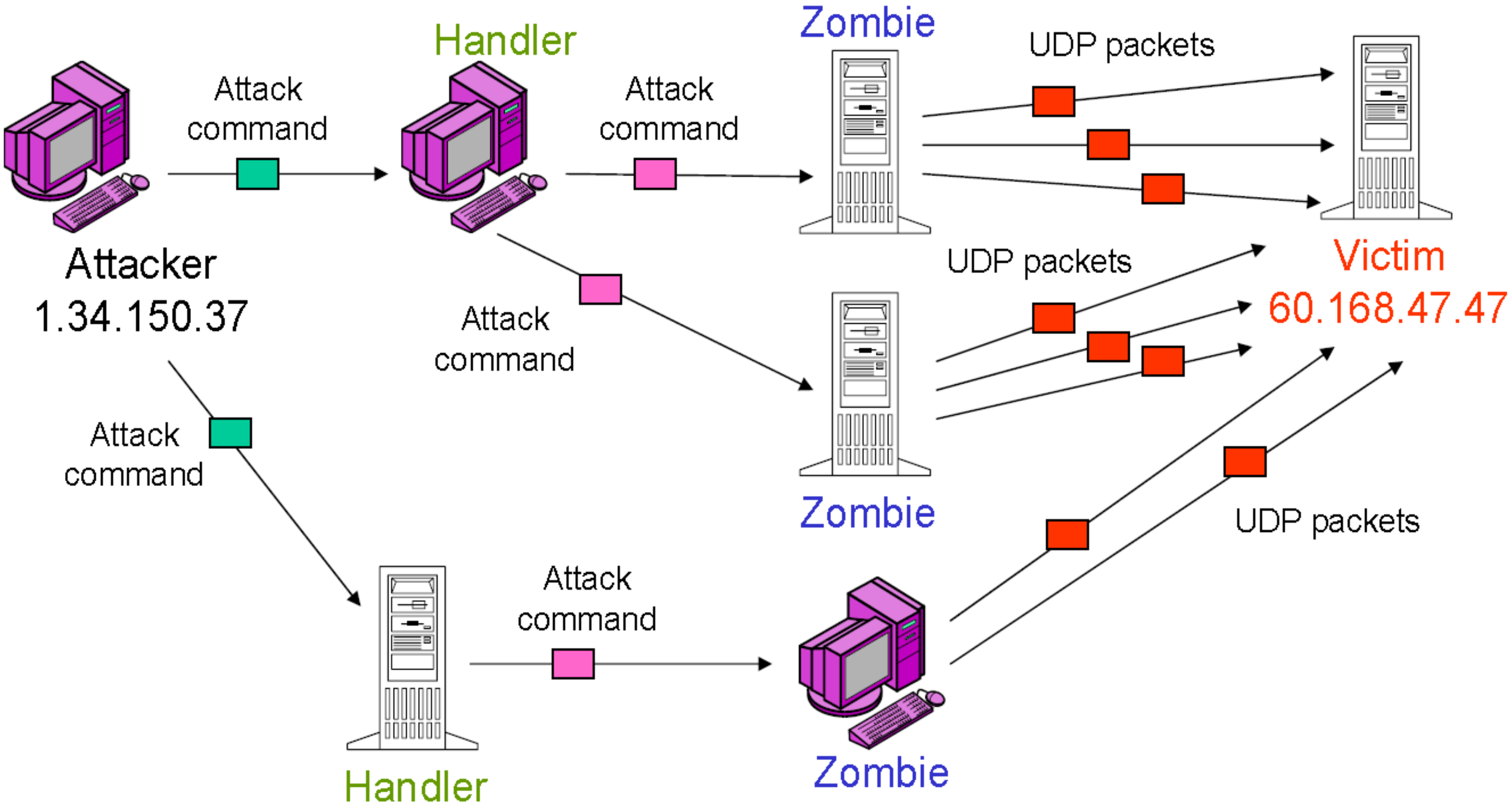
UDP Layer- Flood Attack

- ❑ **Exploiting UDP is not as straightforward as TCP to start attacks**
- ❑ **DoS type attacks are still possible**
- ❑ **Send a large number of UDP packets to random ports on the victim’s machine**
  - ➢ IP address of the packets can be spoofed
- ❑ **The host will return Destination Unreachable packet**
  - ➢ The attacker will never get them due to spoofed IP
  - ➢ Given the large number of UDP requests, the victim will be unreachable by other clients
- ❑ **Countermeasure: Deploying Firewalls**

UDP Layer - Distributed Denial of Service (DDoS)

- ❑ In DDoS, the hacker identifies computers with weak security as handlers.
- ❑ The software in the handlers scan for hosts to be used as agents or zombies.
- ❑ Hundreds of thousands of zombies simultaneously launch the DoS attack in a distributed manner.
- ❑ Difficult to identify the attacker and filter our messages
  - ➢ Come from several different sources
- ❑ Trinoo is such an attack

Trinoo


Attacker
1.34.150.37
Attack command
Handler
Attack command
Attack command
Attack command
Handler
Attack command
Zombie
Zombie
Zombie
UDP packets
UDP packets
UDP packets
Victim
60.168.47.47

Application Layer - Web Spoofing

- ❑ In this attack the malicious site pretends to be authentic
- ❑ It is a form of man-in-the-middle attack
- ❑ This is accomplished by compromising and accessing the victim website and putting a link to a malicious site.
- ❑ For example, www.nytimes.com could be linked to www.hackersite.com but the user would not be aware of this unless they pay attention to the actual site linked.

DNS Spoofing

- This is similar to web spoofing
- DNS server could be a simple machine placed behind a firewall
- Usually it is isolated from the rest of the nodes in functionality
- Hacker gets access to the DNS server and changes in the lookup table the mapping.
- For example, www.nytimes.com is supposed to point to 199.239.136.200.
  - The hacker could redirect it to his web server instead.