Network Security
(6CCS3NSE - 7CCSMNSE)

Diego Sempreboni
Department of Informatics
King's College London, UK

Second term 2019/20

Lecture 3

Objectives and learning outcomes

- To understand Spoofing and Jamming vulnerabilities in and exploits of
  - Link and network layer and a bit of transport layer (Lecture 3)
  - Routing, other transport and DNS (Lecture 4)

Some of these actively enable Sniffing

Objectives and learning outcomes

- List of attacks:
  - Power and ease of jamming
  - ARP spoofing and ARP cache poisoning
  - MAC flooding
  - DHCP starvation and Rogue Server
  - Smurfing attacks
  - Amplification and NTP DoS attacks
  - SYN flooding
  - Botnets

Jamming

- Affecting availability for legitimate packets by talking too much

Jamming at the link layer

- The link layer typically broadcast-based
- Users must be polite: one user talks at a time
- Jamming: hogging broadcast medium so no one can talk. Works easily on ethernet, WIFI...

Very easy to jam, e.g., Ethernet

- **Throughput**: a performance measure of how many frames of data are successfully delivered per unit of time

- **Contention**: sharing the broadcast medium across a number of devices

- **Throughput** of randomised multiple-access drop drastically as **contention** increases

Portable jammer…

- WIFI
- 3G/4G
  - 5-20 meters
- £ 100-200

Jamming at network layer = DoS

- Denial of Service (DoS) attack: send too many packets and overwhelm server or network link

- This can have huge impact:
  - Amazon makes an estimated $450K every minute. Downtime costs a lot!
  - Paypal was attacked by Anonymous and lost nearly 3.5 millions £ (according to court case)

- Many different forms of DoS exists: several involve **spoofing!**


Support The Guardian
Available for everyone, funded by readers
Contribute → Subscribe →
Search jobs Dating Sign in Search The Guardian UK edition
News Opinion Sport Culture Lifestyle More
UK World Business Football Environment UK politics Education Society Science Tech Global development Cities Obituaries
Anonymous
This article is more than 6 years old
Anonymous cyber-attacks cost PayPal £3.5m, court told
Student on trial accused of playing a leading role in revenge campaign against several sites after backlash against WikiLeaks
Sandra Laville, crime correspondent
Thu 22 Nov 2012 17.14 GMT

Mr. Robot: DDoS

Spoofing

Spoofing attacks

- Pretending to be somebody you are not (masquerading), BUT
- What is a “somebody” on the Internet?
  - An IP address
- What is “somebody” on the LAN?
  - A MAC address
- Spoofing forms the basis of a lot of attacks
  - Why? Because it is very easy to change your address

Spoofing attack 1: ARP Spoofing

- Each layer has its own address:
  - **IP address** at network layer (logical address):

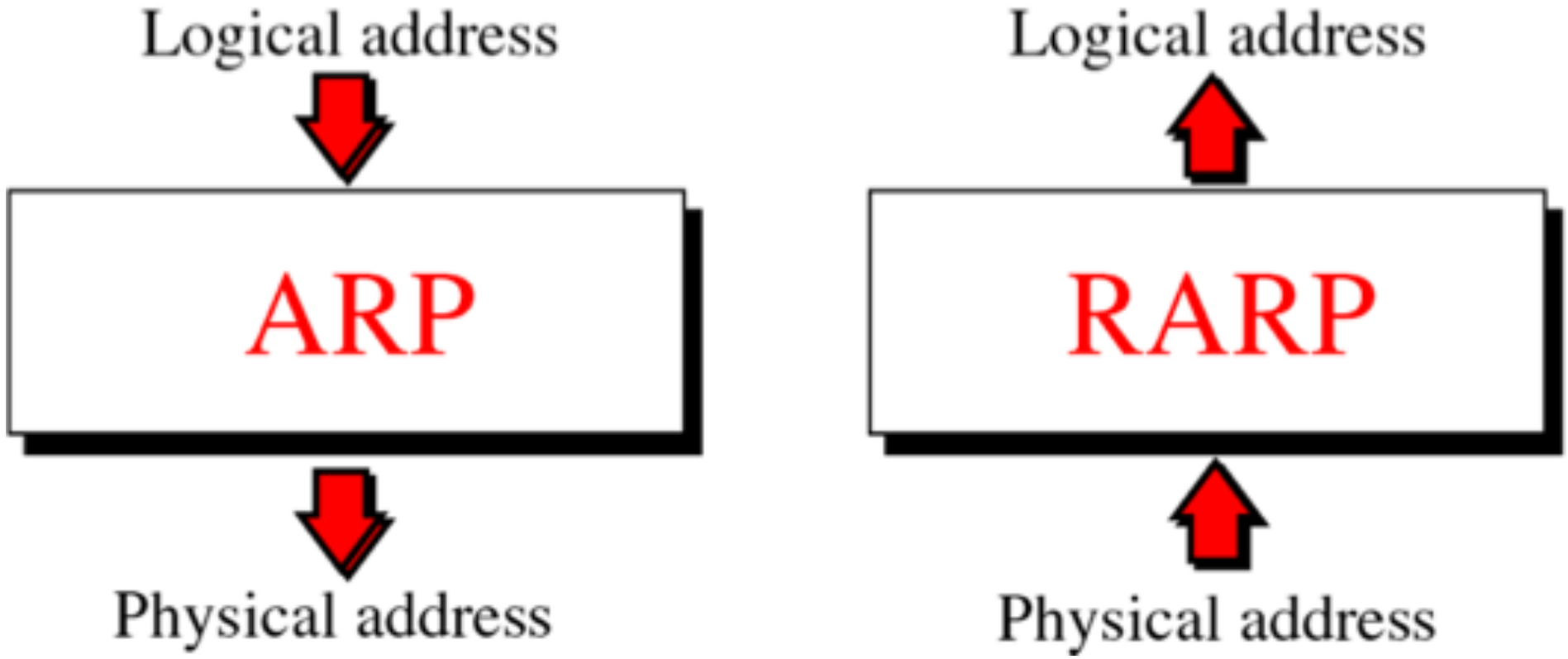
    Used by applications and the socket interface
  - **MAC address** at link layer (physical address):

    Ethernet header contains the MAC address of the source and the destination computer. Used for link local communications, i.e on each IP hop

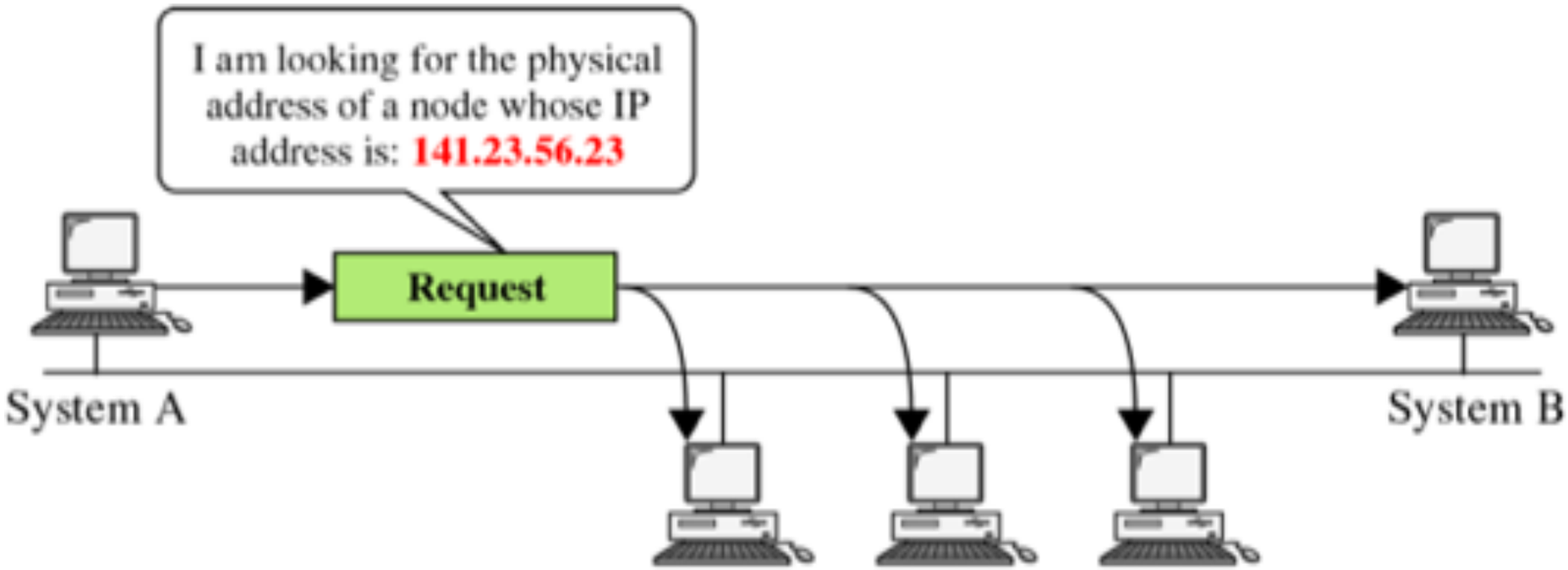
Spoofing attack 1: ARP Spoofing

- At the link layer, IP is encapsulated in an ethernet frame

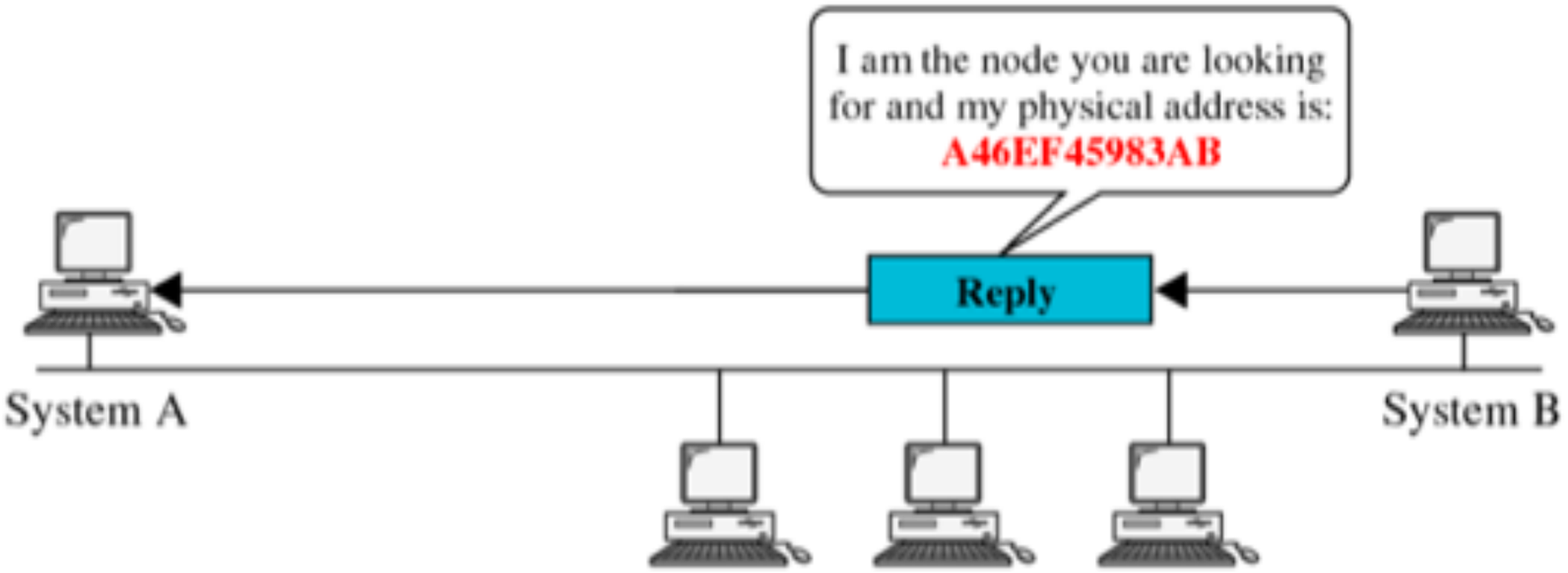
  But what ethernet destination address to use for a given IP address?



Spoofing attack 1: ARP operation

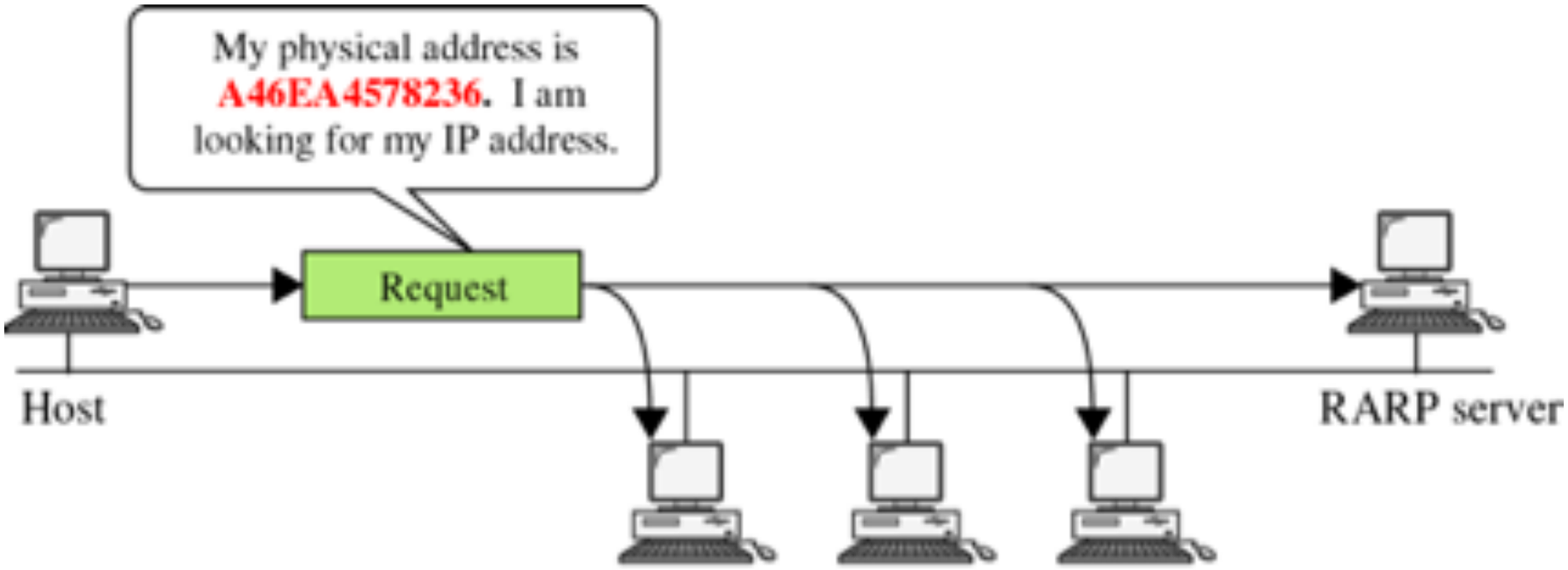


a. ARP request is broadcast



b. ARP reply is unicast

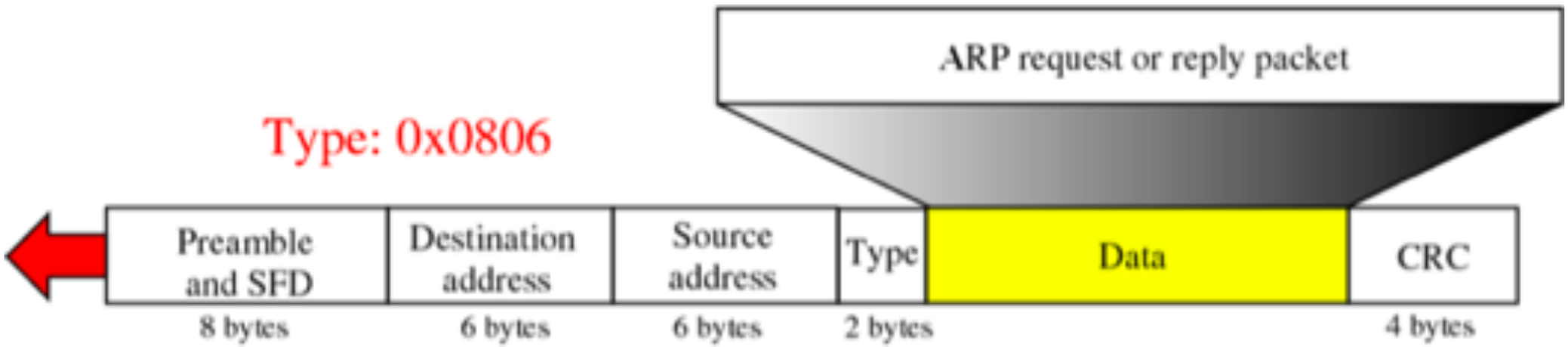
Spoofing attack 1: RARP operation (reverse of ARP)

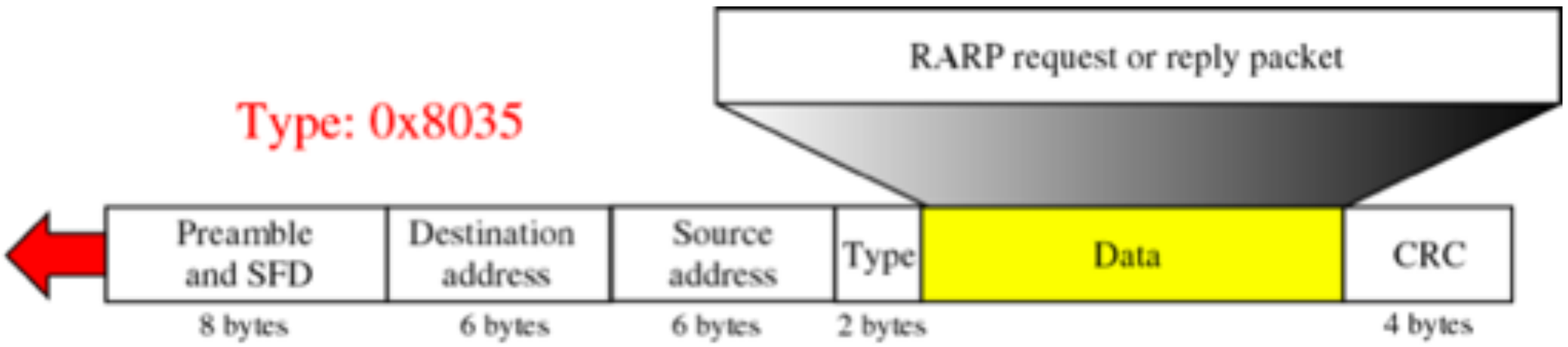


a. RARP request is broadcast

b. RARP reply is unicast

ARP and RARP are ethernet msgs





How ARP functions

1. Get IP address of the 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 data link layer where it is encapsulated in a frame

- Source address: physical address of the sender
- **Destination address**: broadcast address

How ARP functions

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. Target machines replies with ARP message that contains its physical address
   - **A unicast message**

6. Sender receives the reply message and knows physical address of the target

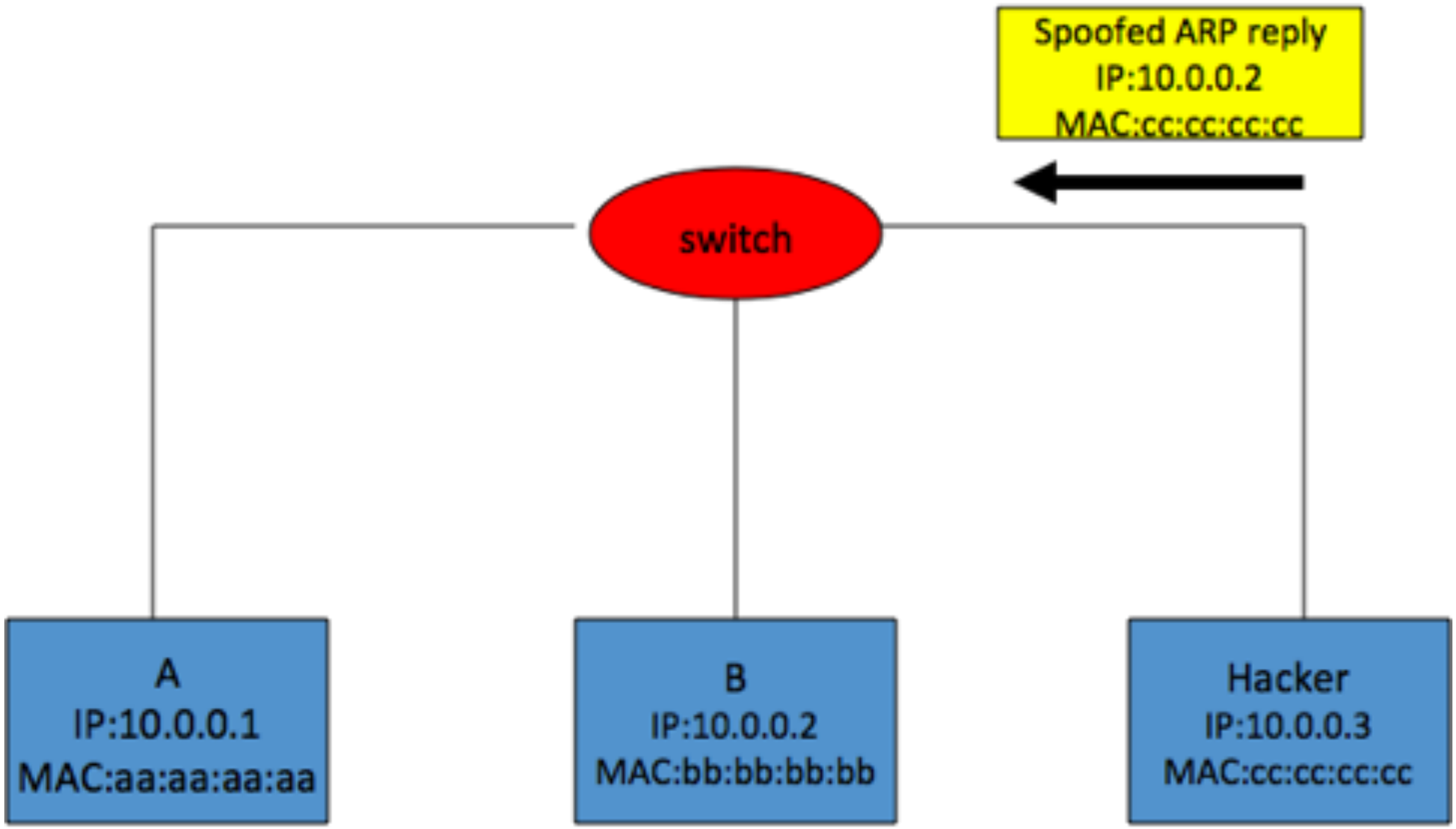
ARP cache

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

ARP cache poisoning by spoofing

- Construct spoofed ARP replies
- A target computer could be convinced to send frames destined for compute **A** to instead go to computer **B**
- **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 spoofing/ARP poison routing/ ARP cache poisoning."**

ARP spoofing attack

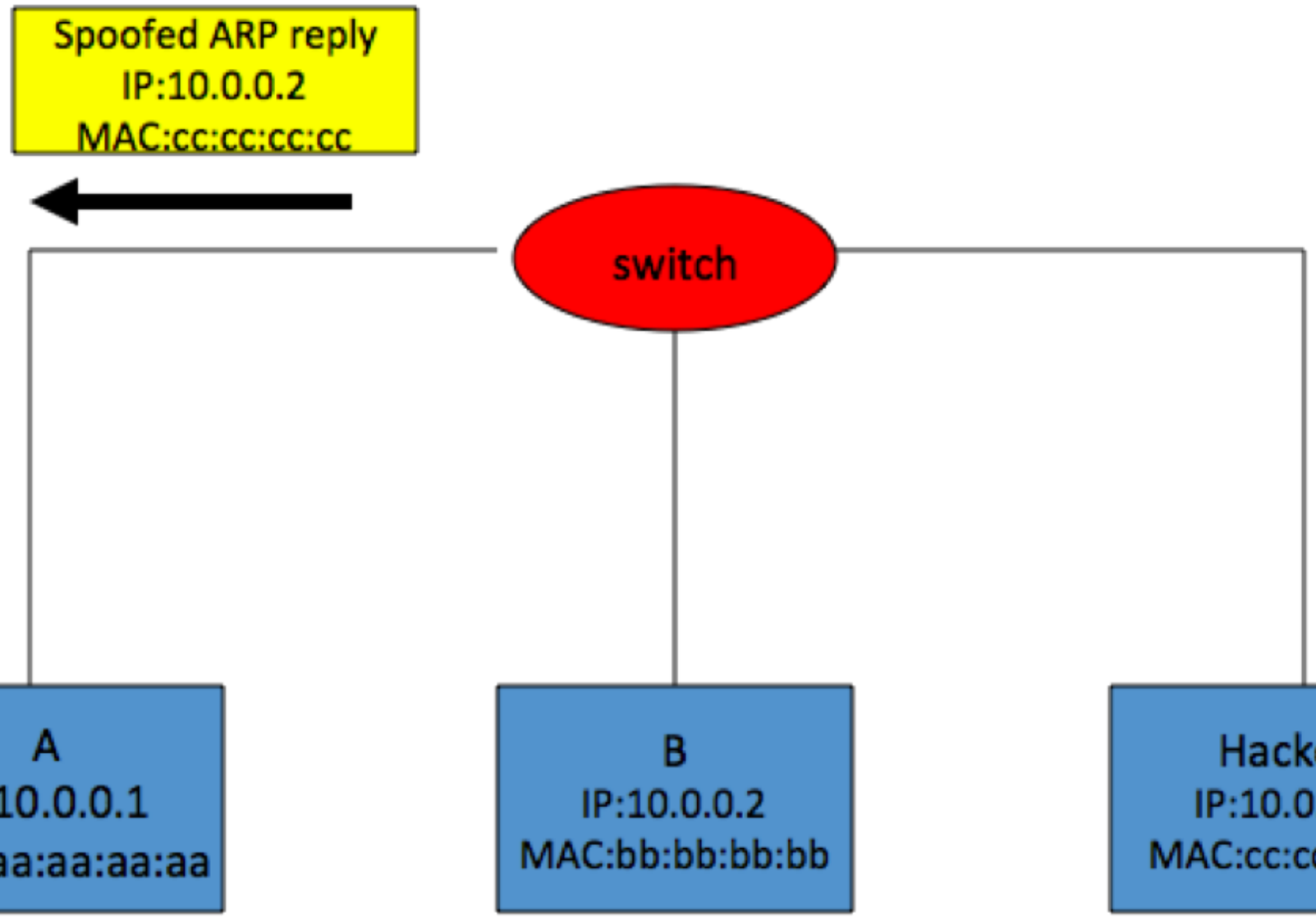


ARP cache

ARP cache

IP	MAC
10.0.0.1	aa:aa:aa:aa

ARP spoofing attack



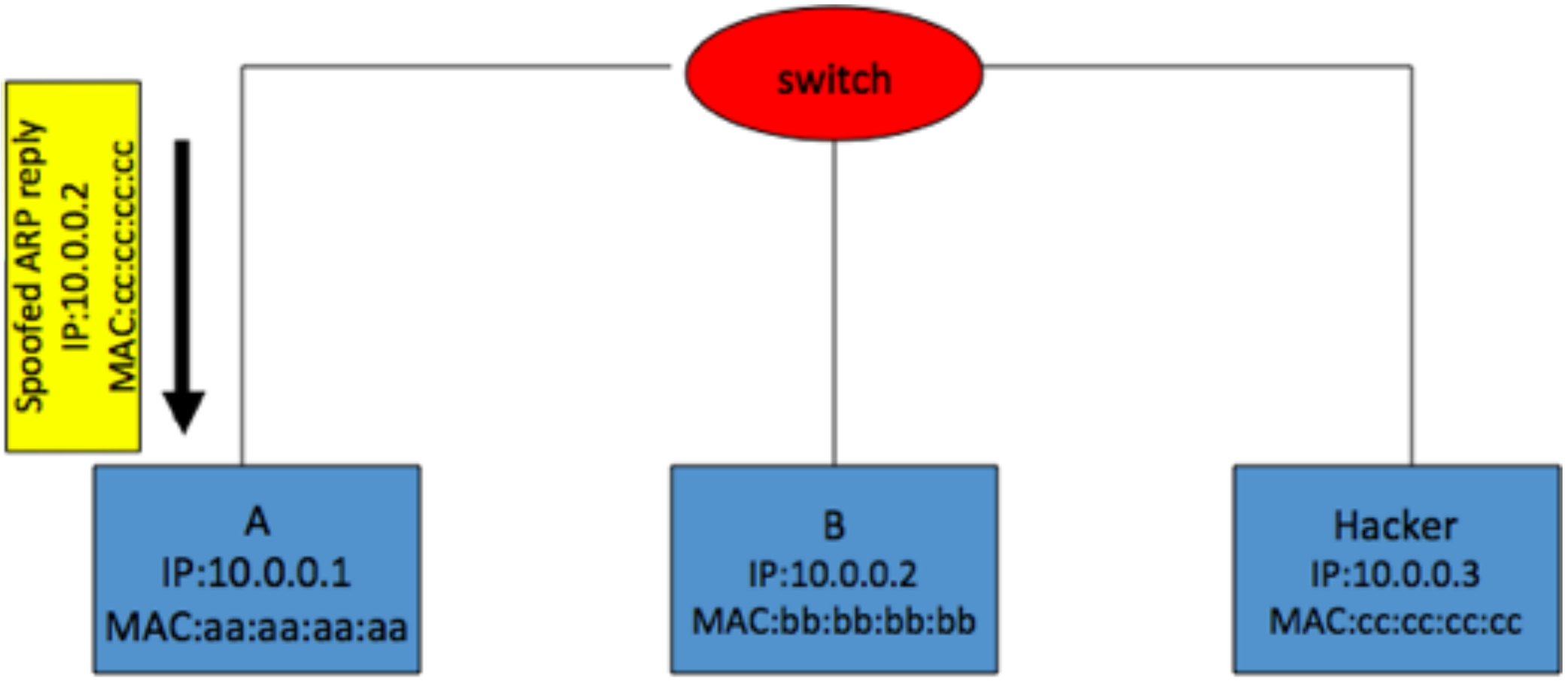
ARP cache

IP	MAC
10.0.0.2	bb:bb:bb:bb

ARP cache

IP	MAC
10.0.0.1	aa:aa:aa:aa

ARP spoofing attack



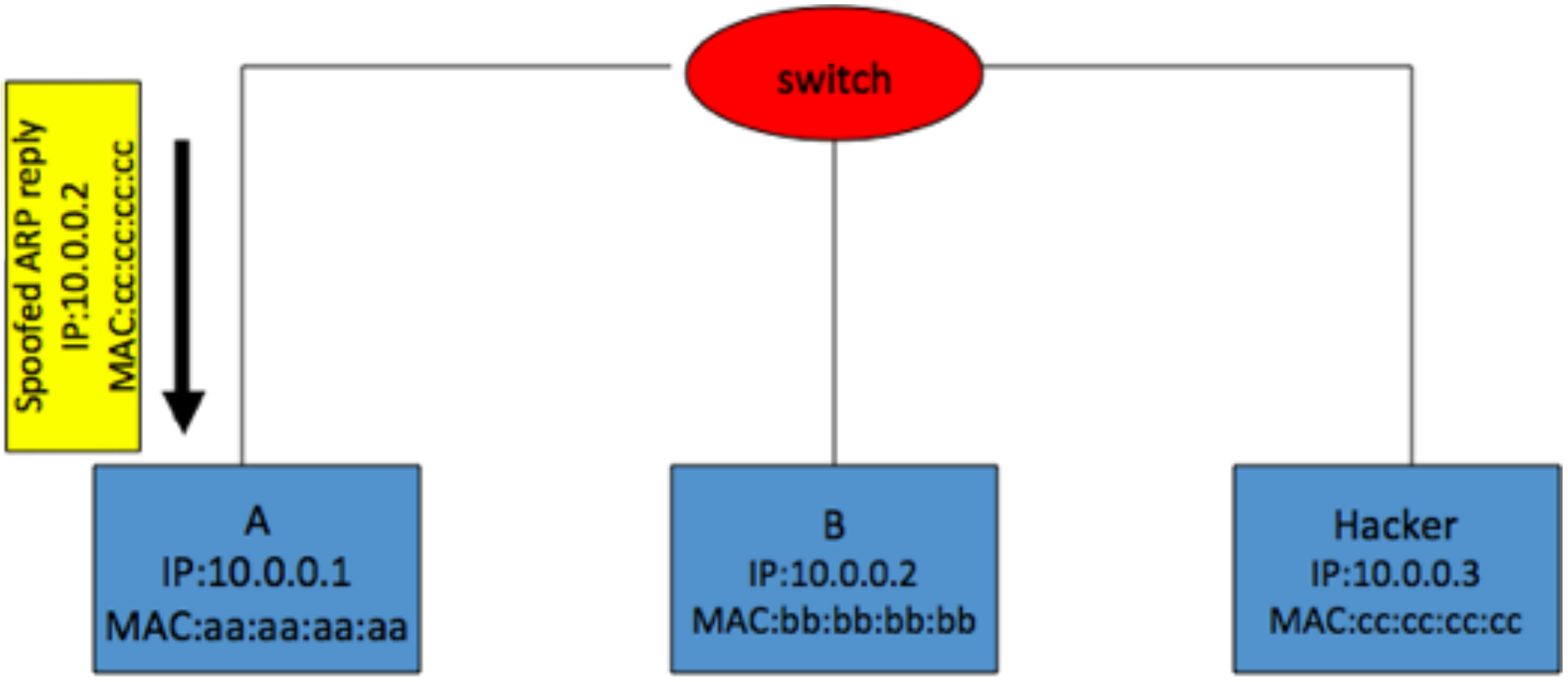
ARP cache

IP	MAC
10.0.0.2	bb:bb:bb:bb

ARP cache

IP	MAC
10.0.0.1	aa:aa:aa:aa

ARP spoofing attack



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 now poisoned

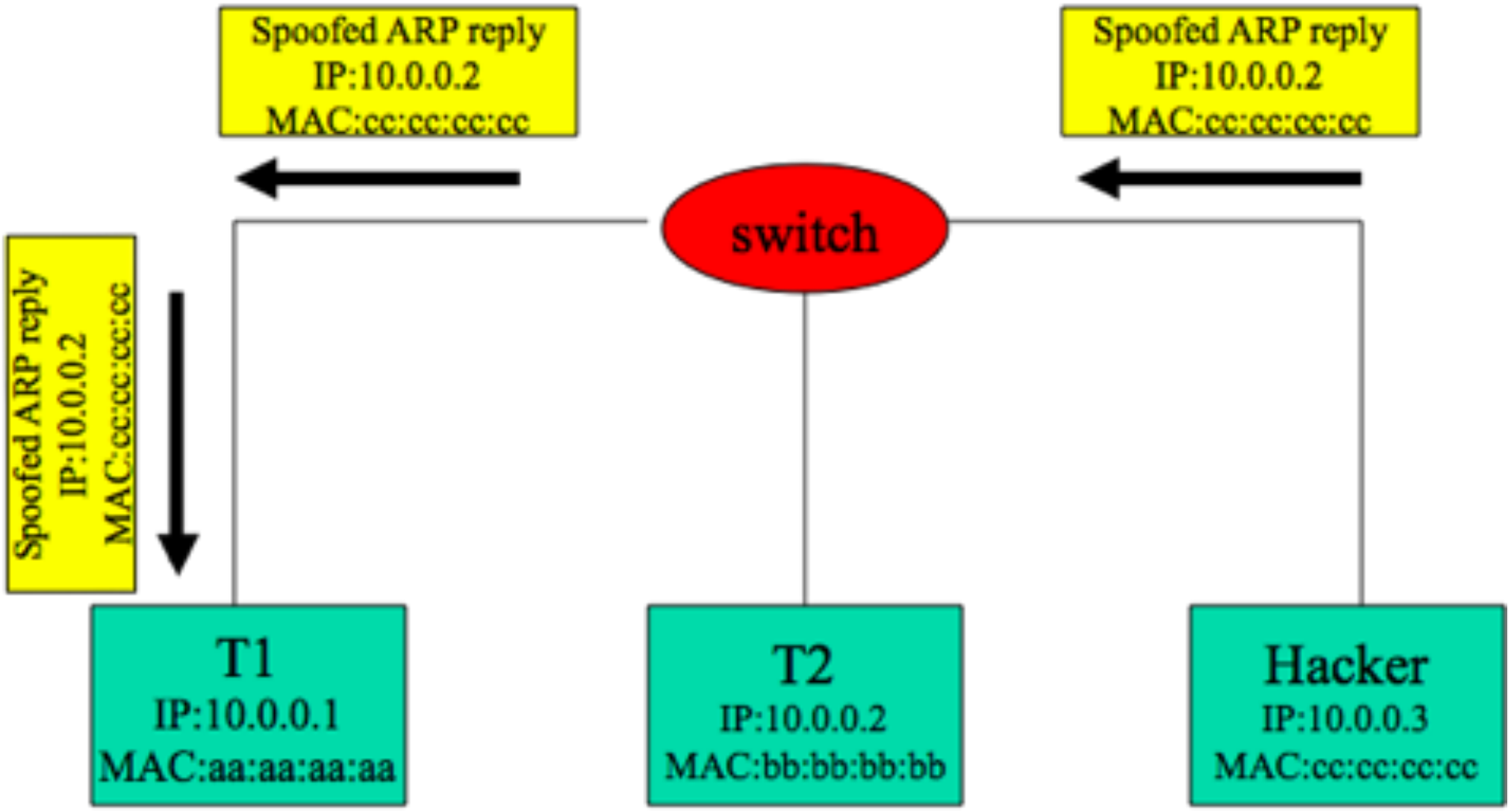
Managing spoofed ARP entry

- After poisoning, all packets that A intends for B get sent to hacker!
- Complications:
  - Cache entries expire
  - Some systems may try to send unicast ARP to confirm or update cache
  - In both cases, re-send ARP spoof packet (once every ~40s is sufficient usually)

Man-in-the-Middle (MITM) attack with ARP spoofing

- GOAL: insert hacker's computer H in between conversation of A and B. A and B should continue conversation but H has complete access to all their packets.

Man-in-the-Middle (MITM) attack with ARP spoofing



ARP cache

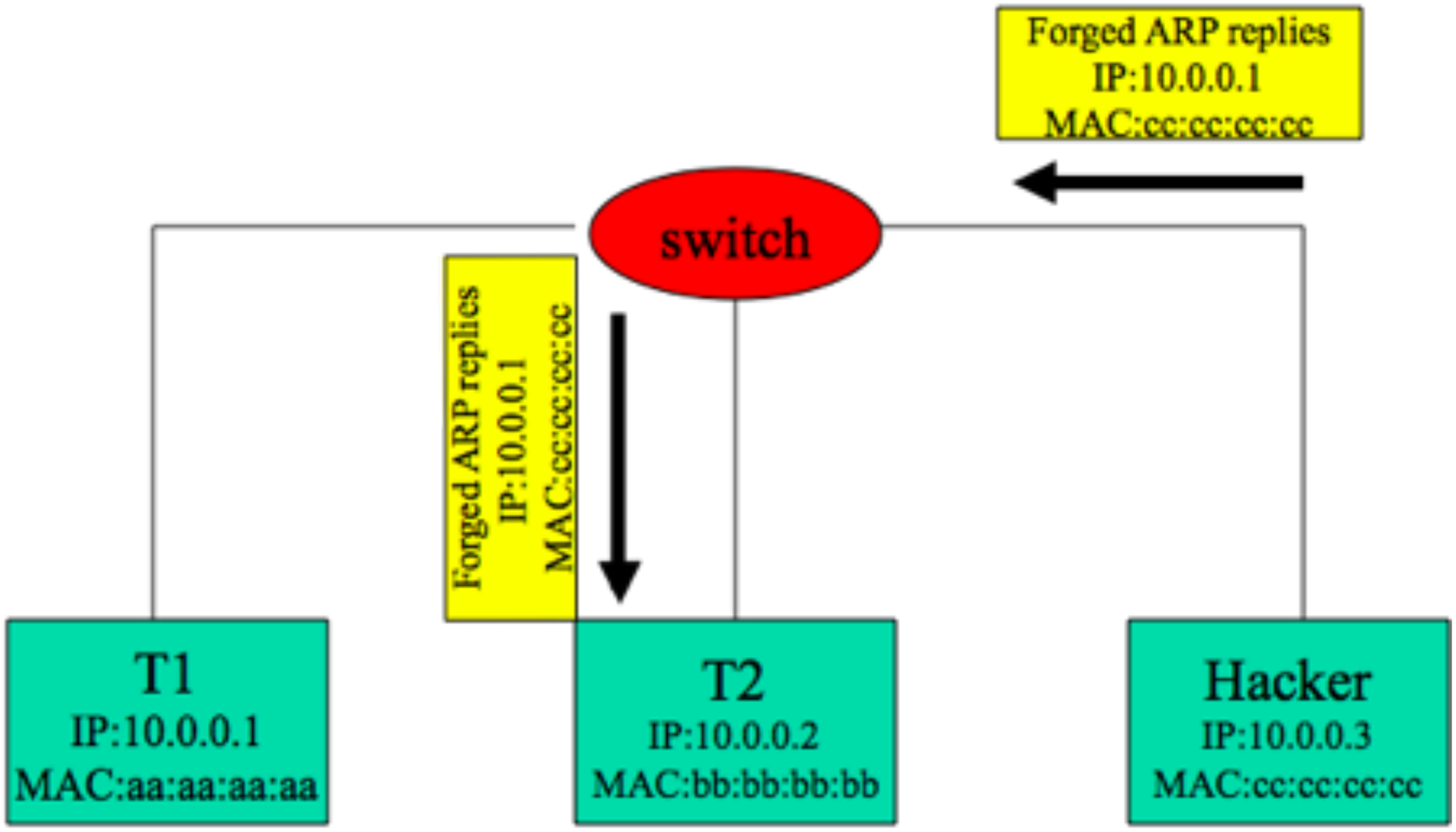
IP	MAC
10.0.0.2	CC:CC:CC:CC

ARP cache

IP	MAC
10.0.0.1	aa:aa:aa:aa

T1's cache is poisoned

Man-in-the-Middle (MITM) attack with ARP spoofing



ARP cache

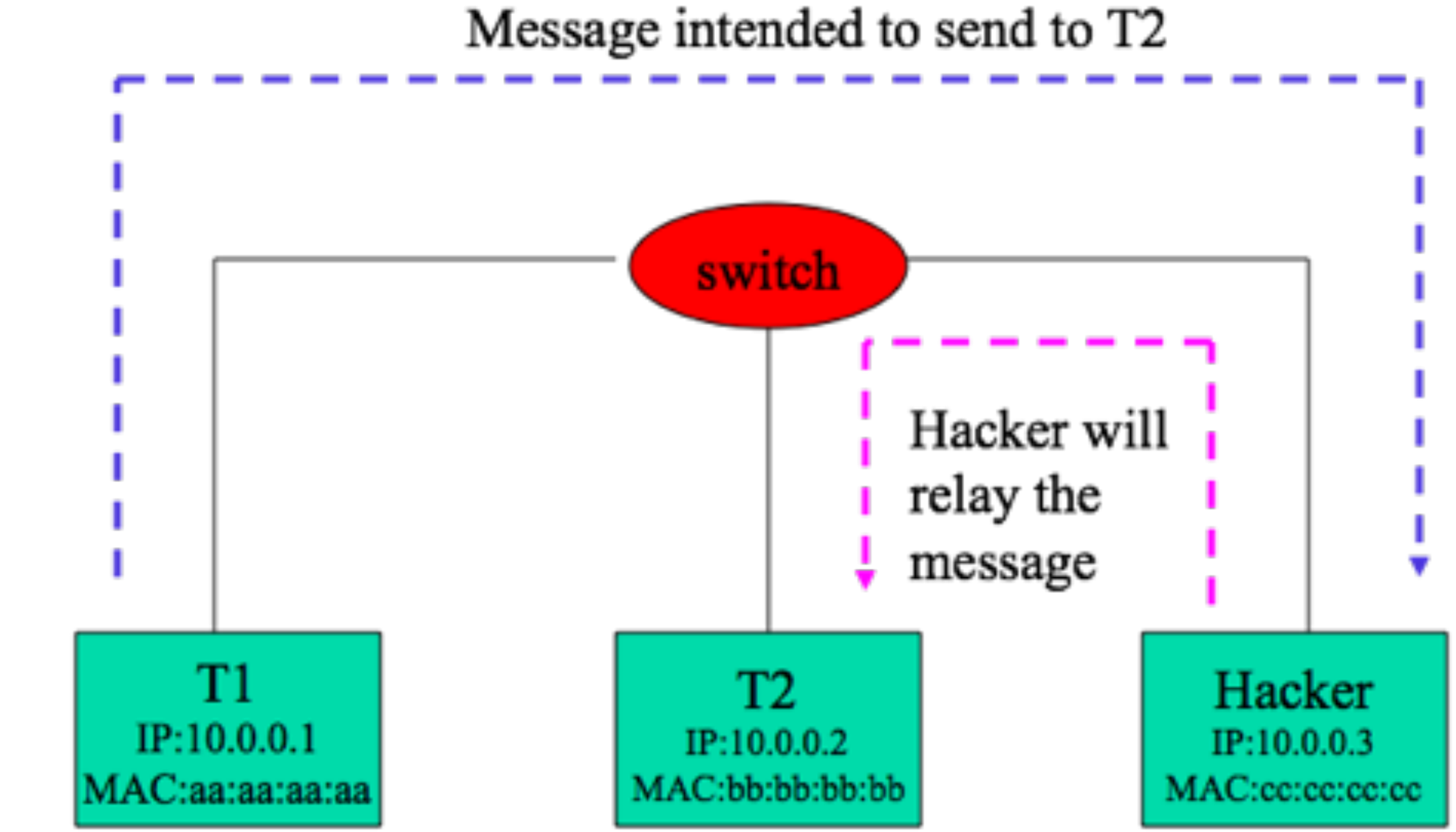
IP	MAC
10.0.0.2	cc:cc:cc:cc

ARP cache

IP	MAC
10.0.0.1	CC:CC:CC:CC

T2's cache is poisoned

Man-in-the-Middle (MITM) attack with ARP spoofing



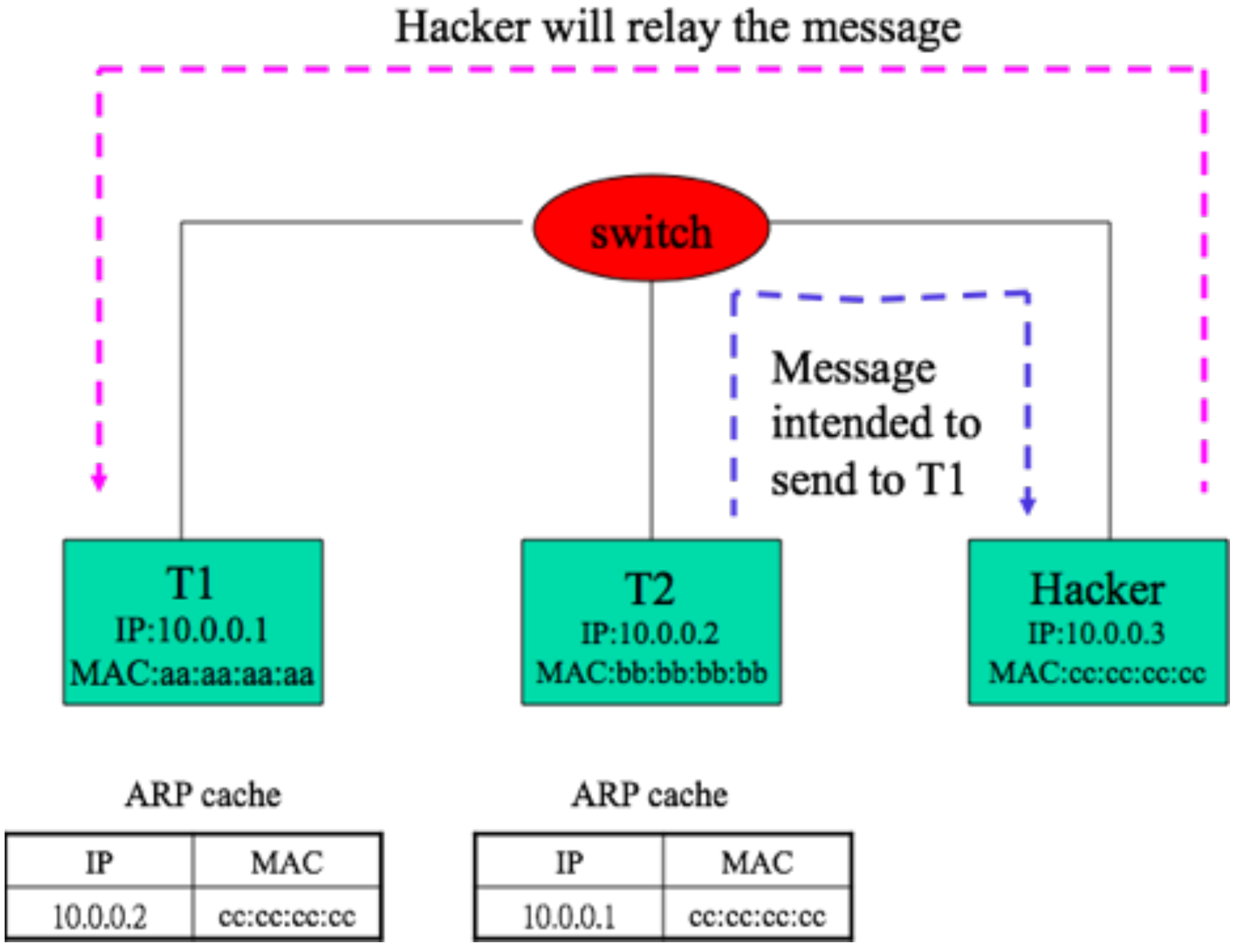
ARP cache

IP	MAC
10.0.0.2	cc:cc:cc:cc

ARP cache

IP	MAC
10.0.0.1	cc:cc:cc:cc

Man-in-the-Middle (MITM) attack with ARP spoofing



MAC flooding with ARP Spoofing

- Switches have an internal table which maps switch ports to MAC addresses

```
2960-1#show mac address-table
Mac Address Table
-------------------------------------------
Vlan Mac Address   Type   Ports
---- ----------- -------- -----
1    00ld.70ab.5d60 DYNAMIC  2
1    00le.f724.al60 DYNAMIC  3
```

- In a MAC flooding attack, a switch is fed many Ethernet frames, each containing different spoofed source MAC addresses to consume the limited memory in the switch and force significant quantities of incoming frames to be flooded out on all ports

Active interception for Sniffing!

DHCP

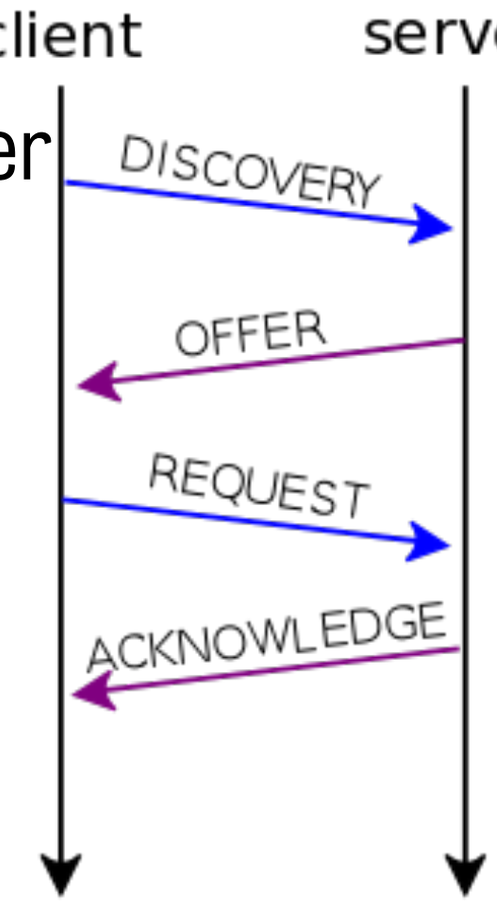
- **D**ynamic **H**ost **C**onfiguration **P**rotocol (DHCP) is a protocol that automatically provides clients with IP addresses and other related configuration (e.g., default gateway)

- Discovery: broadcast message to discover the server

- Offer: unicast message of server offering IP

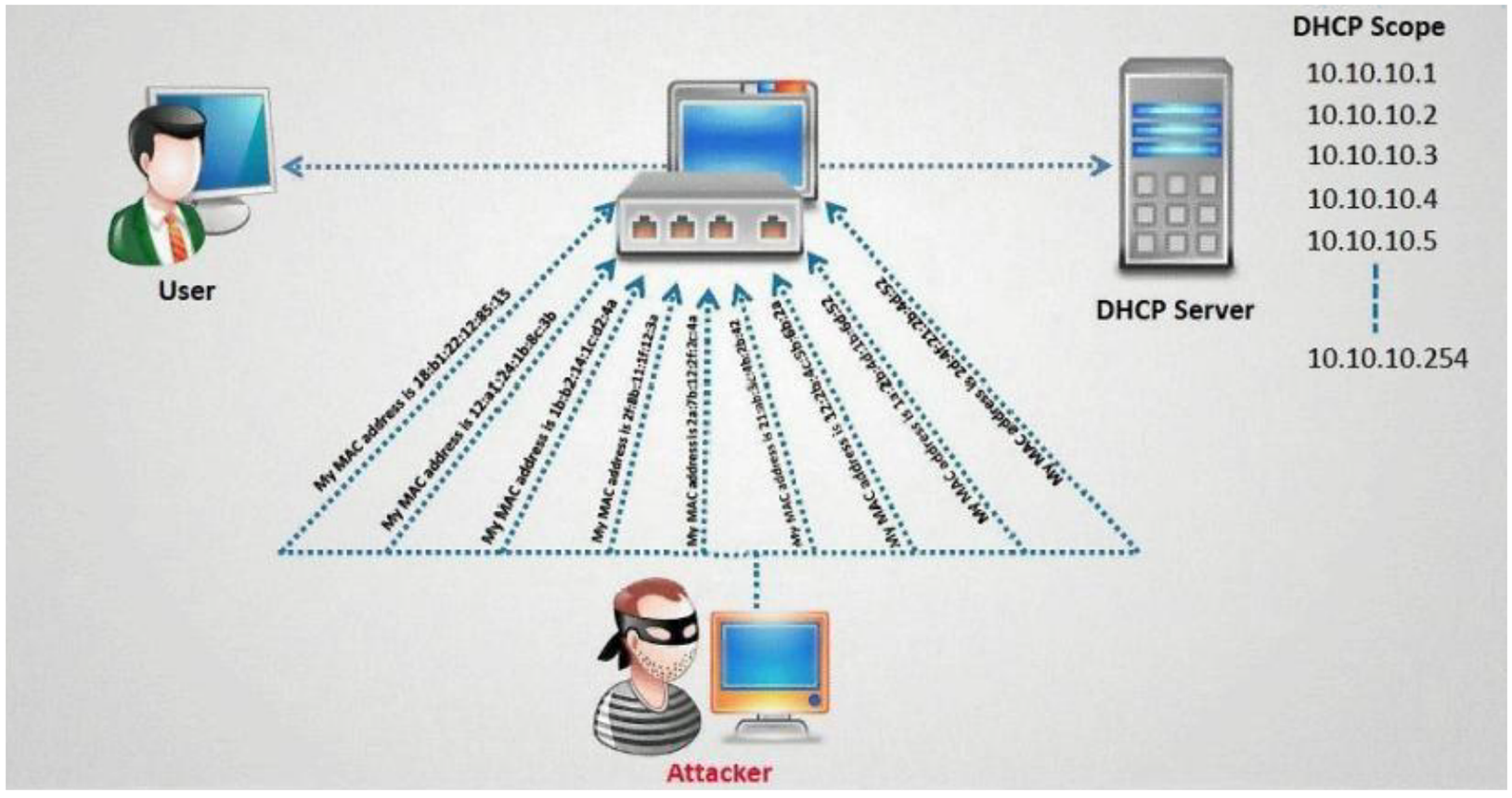
- Request: client accepting the IP offered

- Acknowledge: server acknowledges the IP and sends other related configuration.



DHCP Starvation

- In a DHCP starvation attack, an attacker broadcasts large number of DHCP_REQUEST messages with spoofed source MAC addresses
- If the legitimate DHCP server in the network start responding to all these bogus DHCP_REQUEST messages, available IP addresses in the DHCP server scope will be depleted within a very short span of time



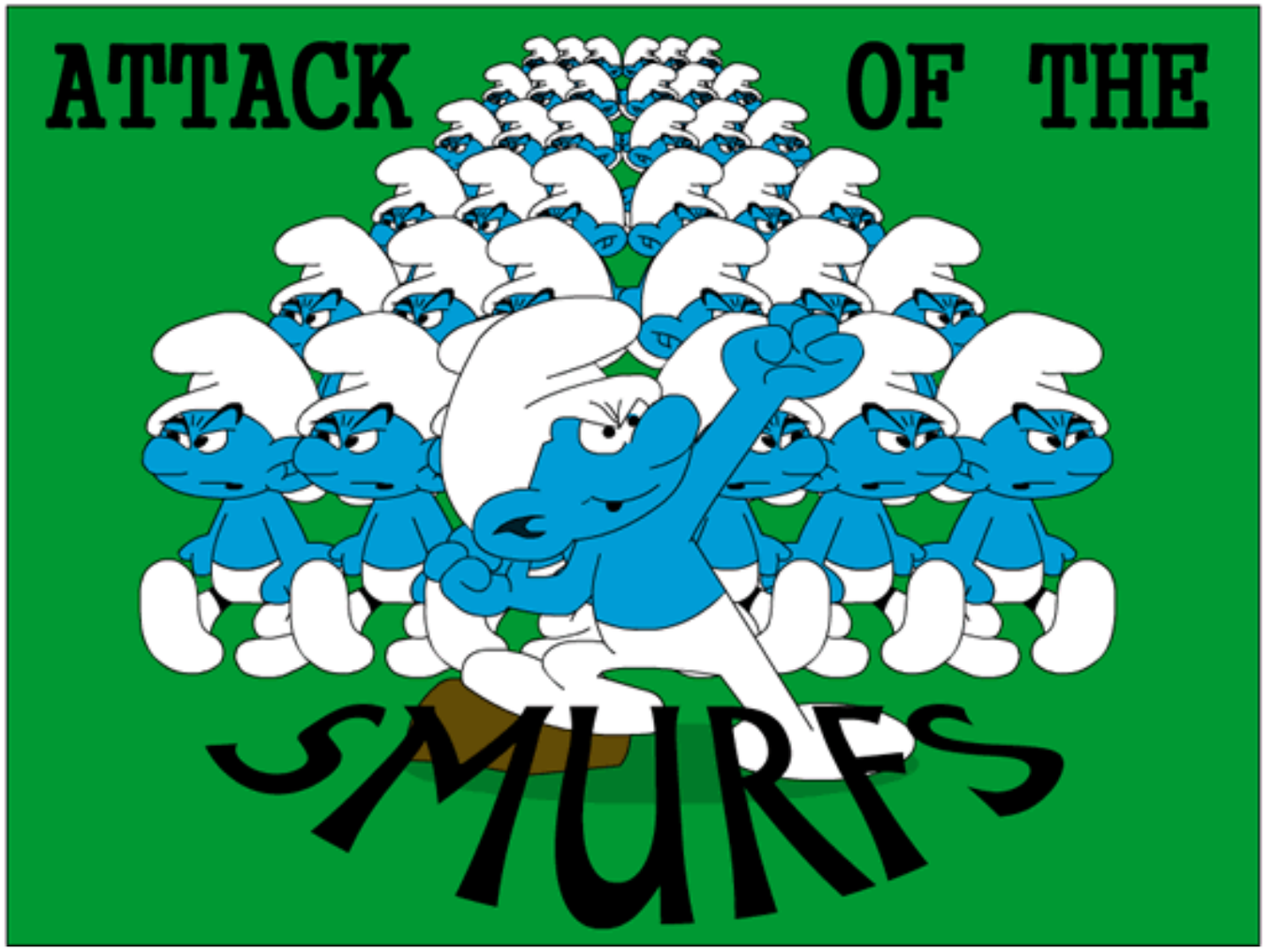
DHCP Rogue Server

- Once the available number of IP addresses in the DHCP server is depleted, network attackers could set up a rogue DHCP server and respond to new DHCP requests from network DHCP clients

- **DHCP spoofing attack**
  - The rogue server starts distributing IP addresses and other TCP/IP configuration settings including default Gateway and DNS server IP addresses, which can now point to an IP address controller by the attacker.
  - Facilitates MITM and Sniffing attacks

Spoofing attack: SMURFING

- Broadcast a ping to your LAN
- Spoof the source address
- What happens?
  - **Denial of service (DoS)**



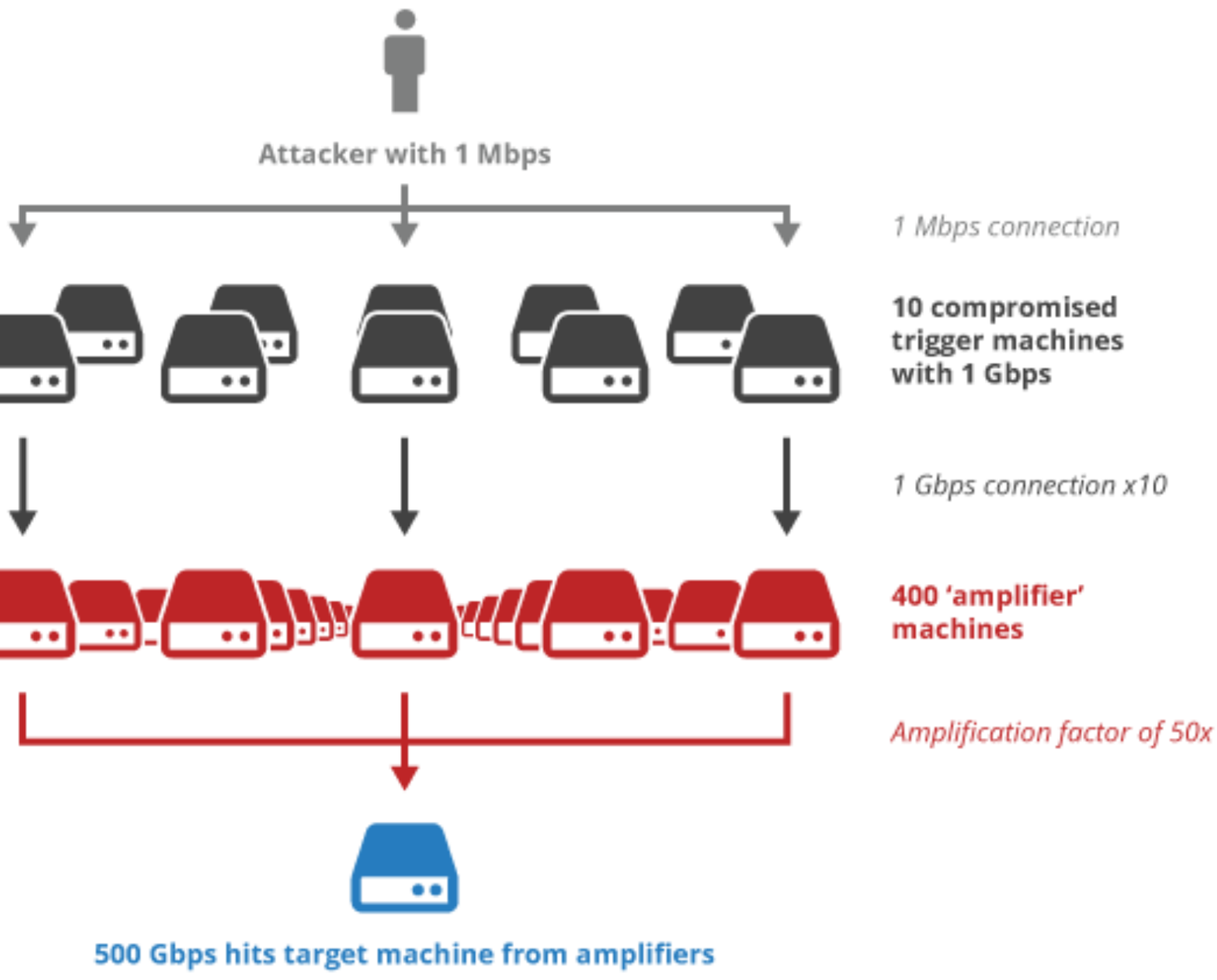
How does smurfing work?

- A smurf attack scenario can be broken down as follows:

1. Smurf malware is used to generate a fake Echo request containing a spoofed source IP, which is actually the target server address
2. The request is sent to an intermediate IP broadcast network
3. The request is transmitted to all of the network hosts on the network
4. Each host sends an ICMP (ping) response to the spoofed source address
5. With enough ICMP (ping) responses forwarded, the target server is brought down

How does smurfing work?

- **Amplification:** small amounts of traffic are converted into large amounts of traffic.



Spoofing attack: NTP DoS

- **N**etwork **T**ime **P**rotocol (NTP) allows computers to synchronise their clock (UDP based protocol)

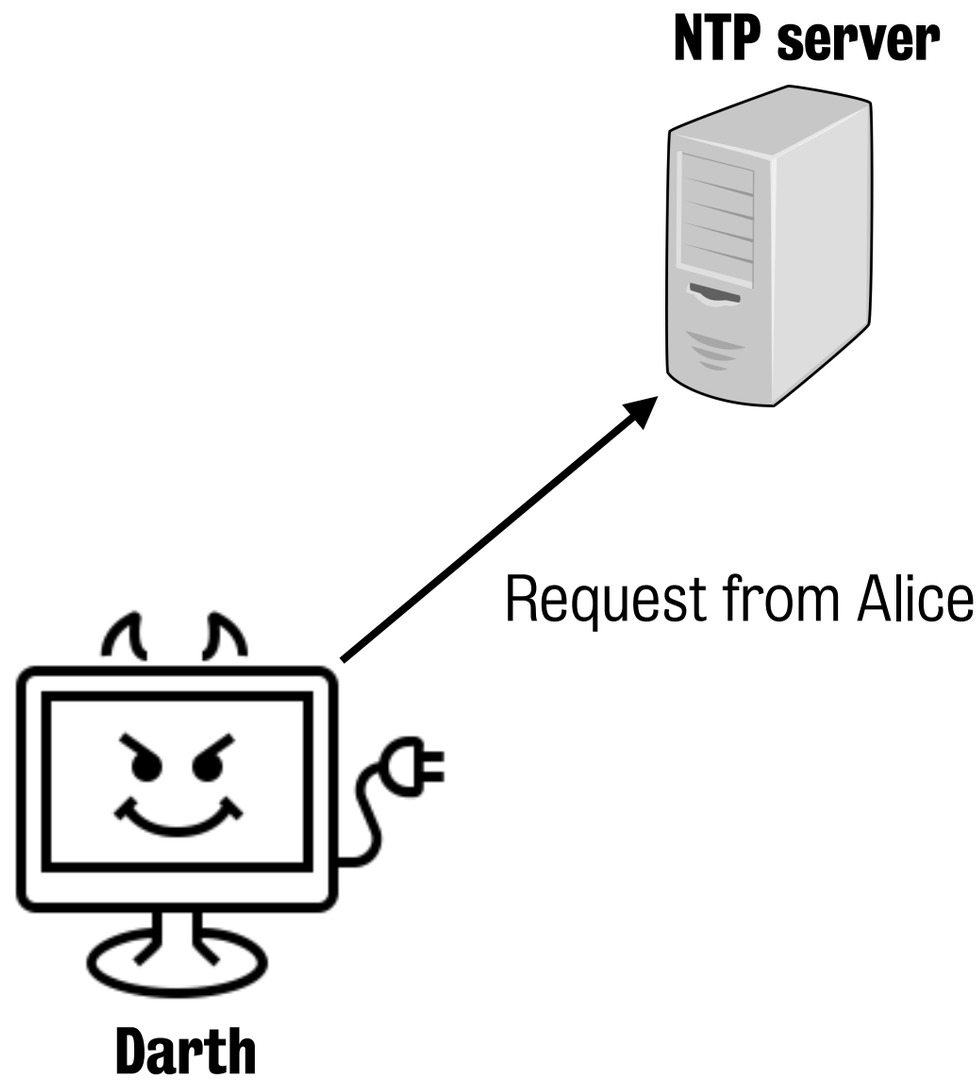
- How could NTP be used for an amplification attack?

- Spoof the IP address to send response to victim
- monlist command returns last 600 hosts
- ntpd prior to 4.2.7 is vulnerable

Spoofing attack: NTP DoS

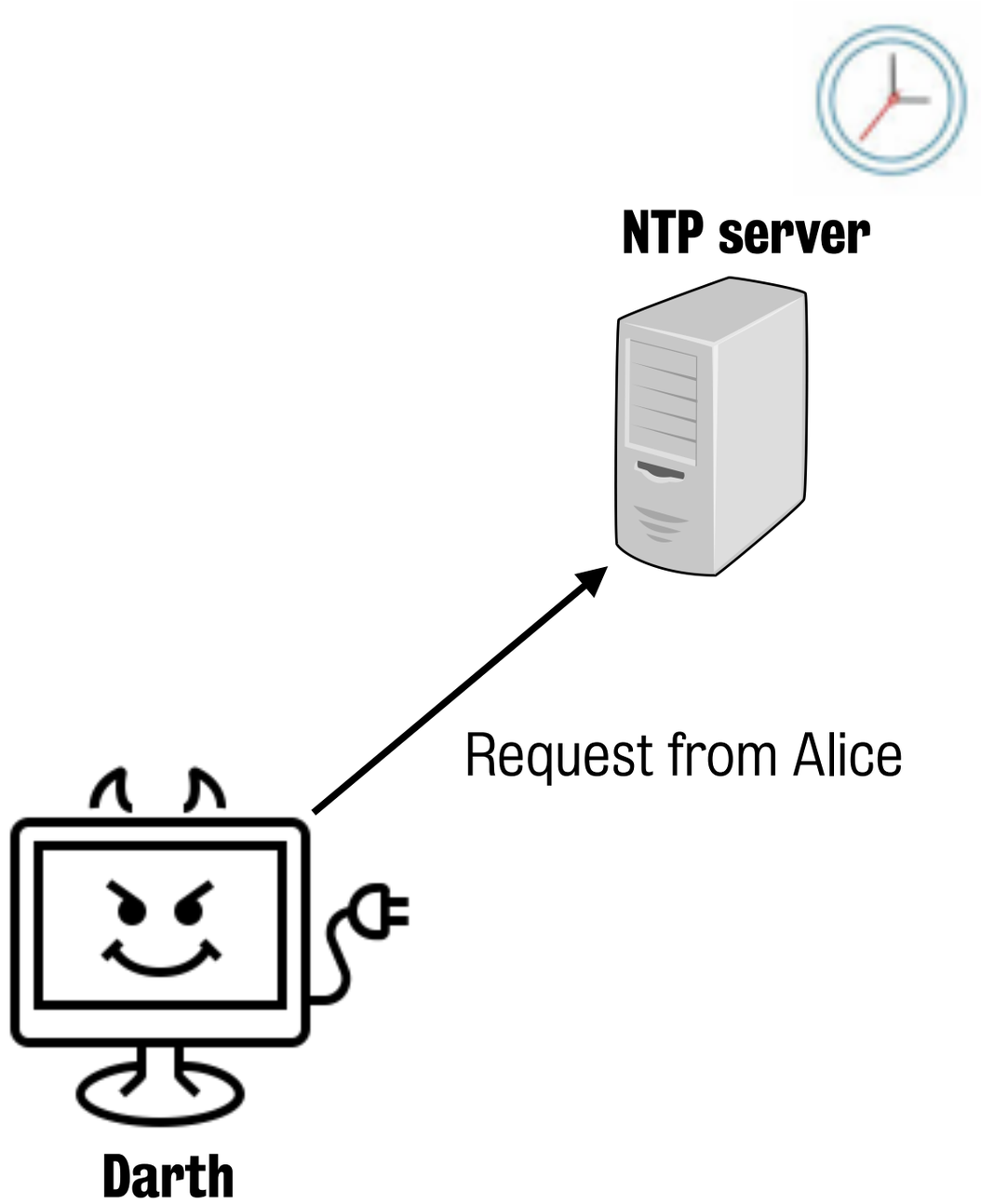
- An NTP amplification attack can be broken down as follows:

  1. The attacker uses a botnet to send UDP packets with **spoofed IP** addresses to a NTP server which has its monlist command enabled. The spoofed IP address on each packet points to the real IP address of the victim.



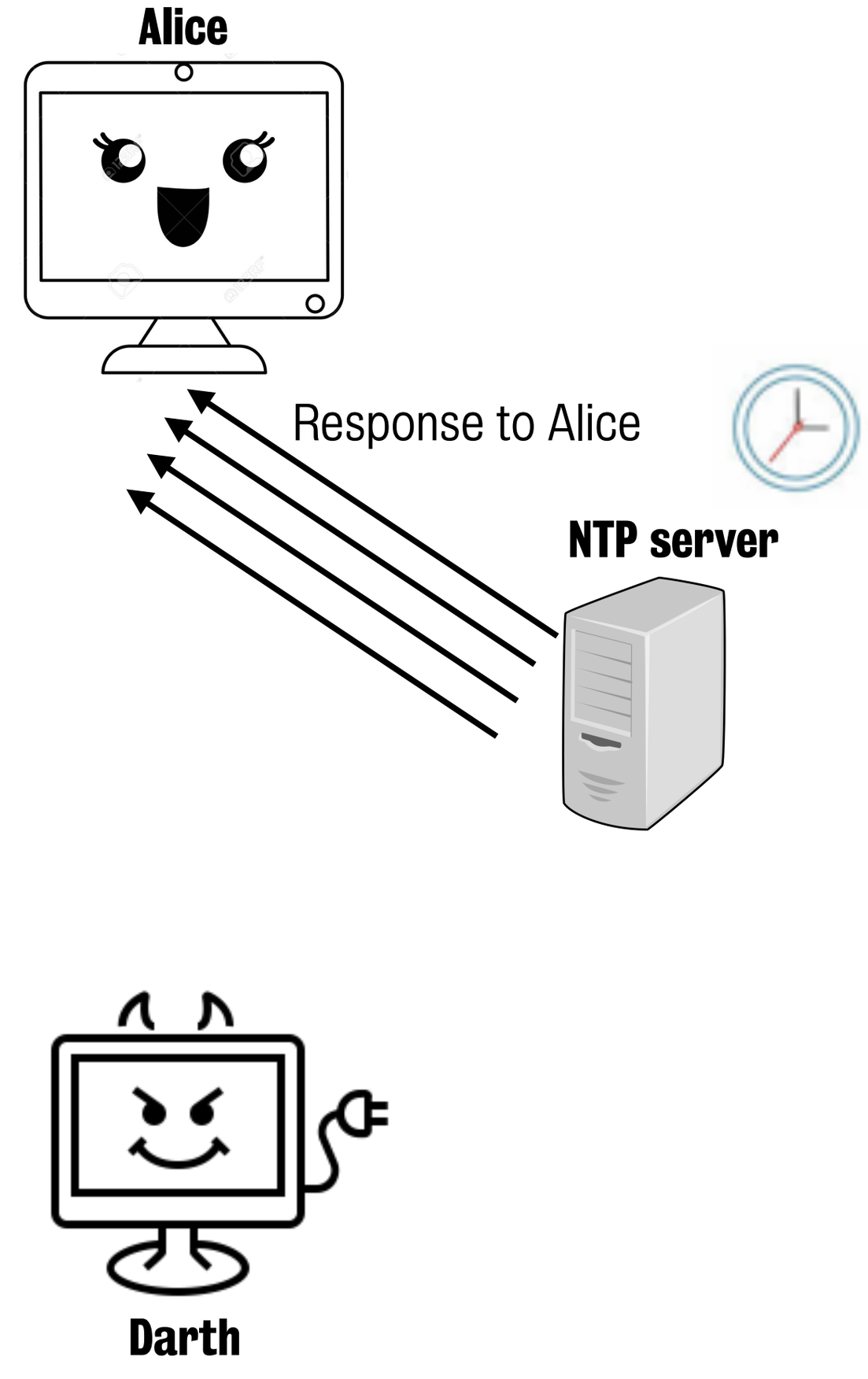
Spoofing attack: NTP DoS

2. Each UDP packet makes a request to the NTP server using its monlist command, resulting in a large response



Spoofing attack: NTP DoS

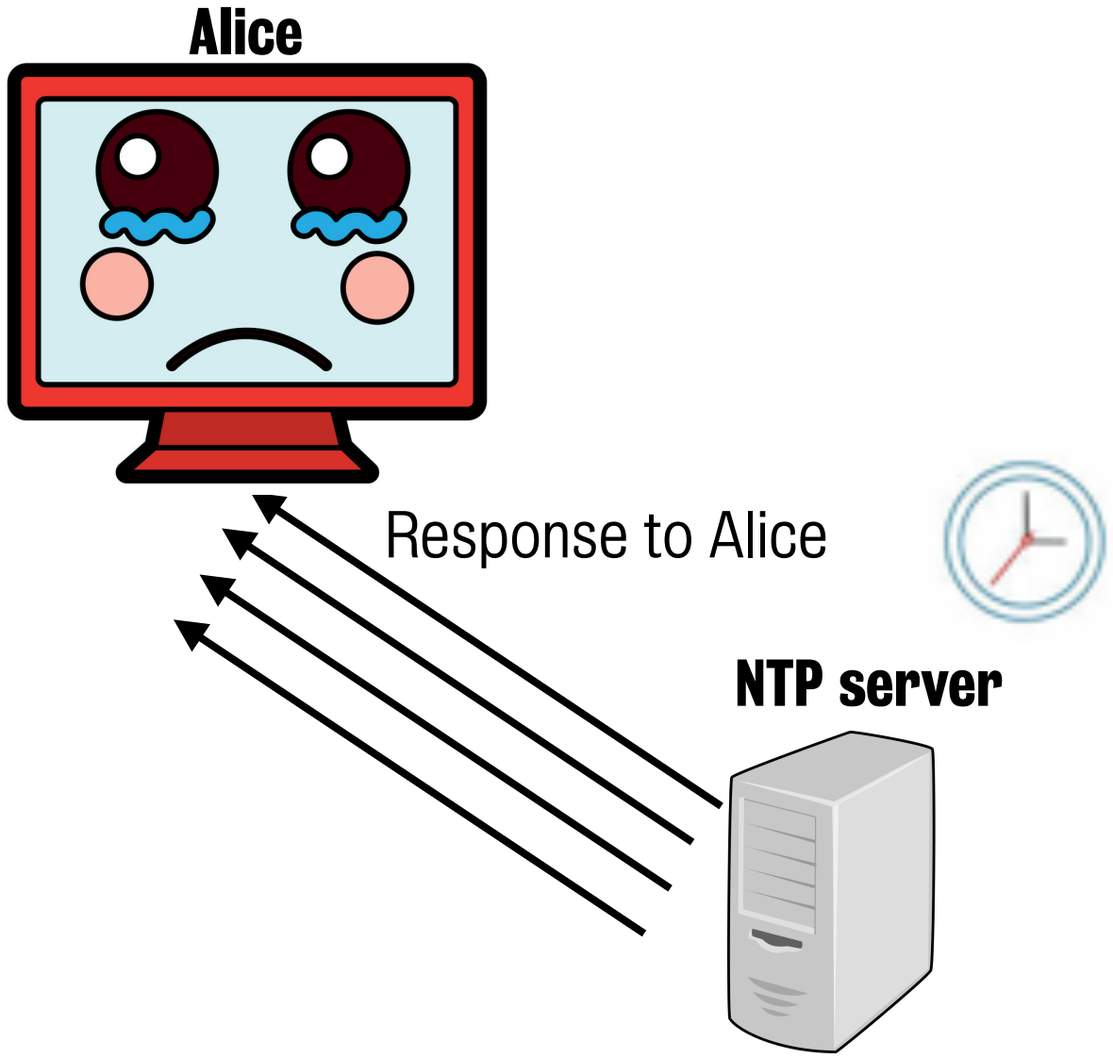
3. The server then responds to the spoofed address with the resulting data

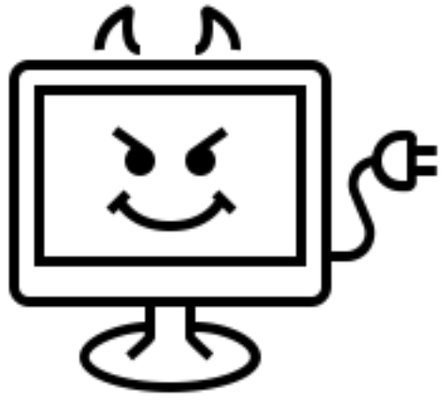


Spoofing attack: NTP DoS

4. The IP address of the target receives the response and the surrounding network infrastructure becomes overwhelmed with the deluge of traffic, resulting in a **D**enial **o**f **S**ervice **(DoS)**

A response can be up to 206 time larger than the request

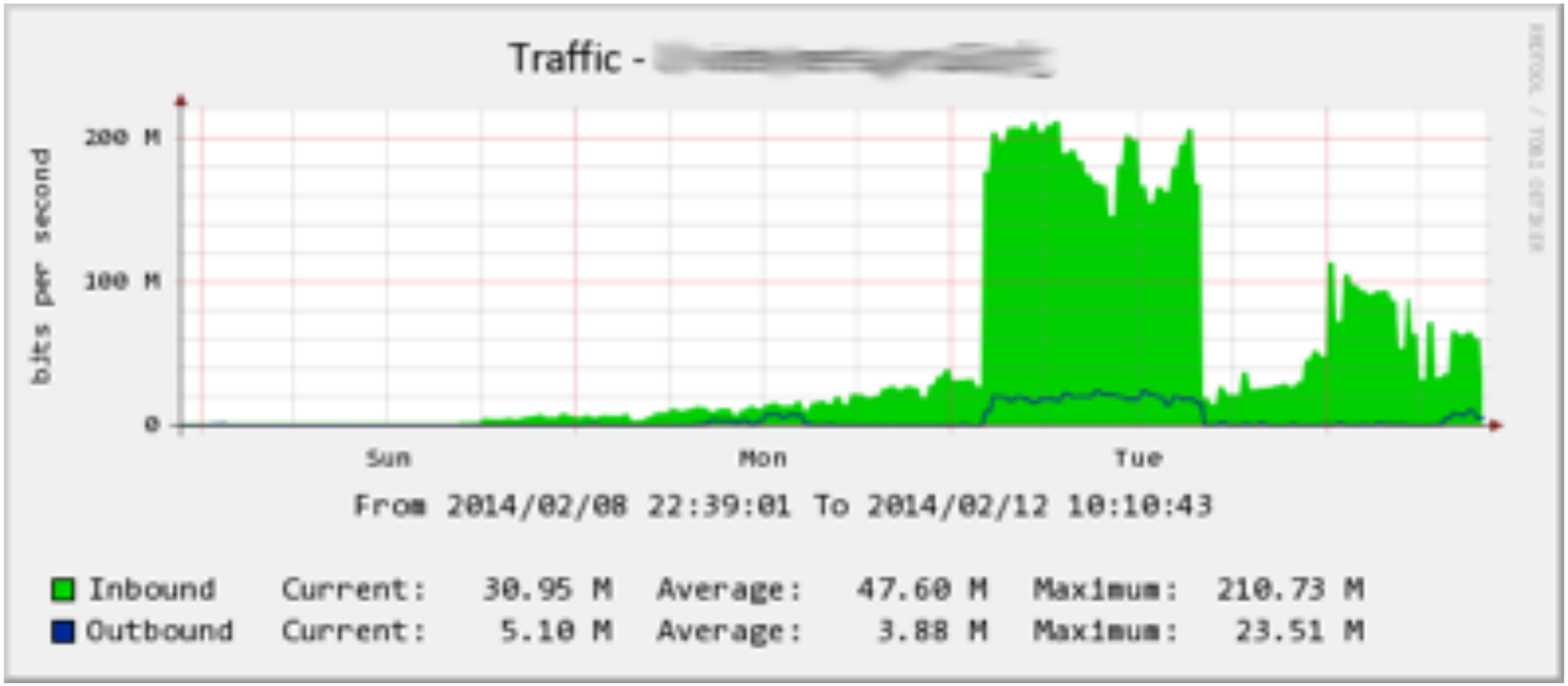




Darth

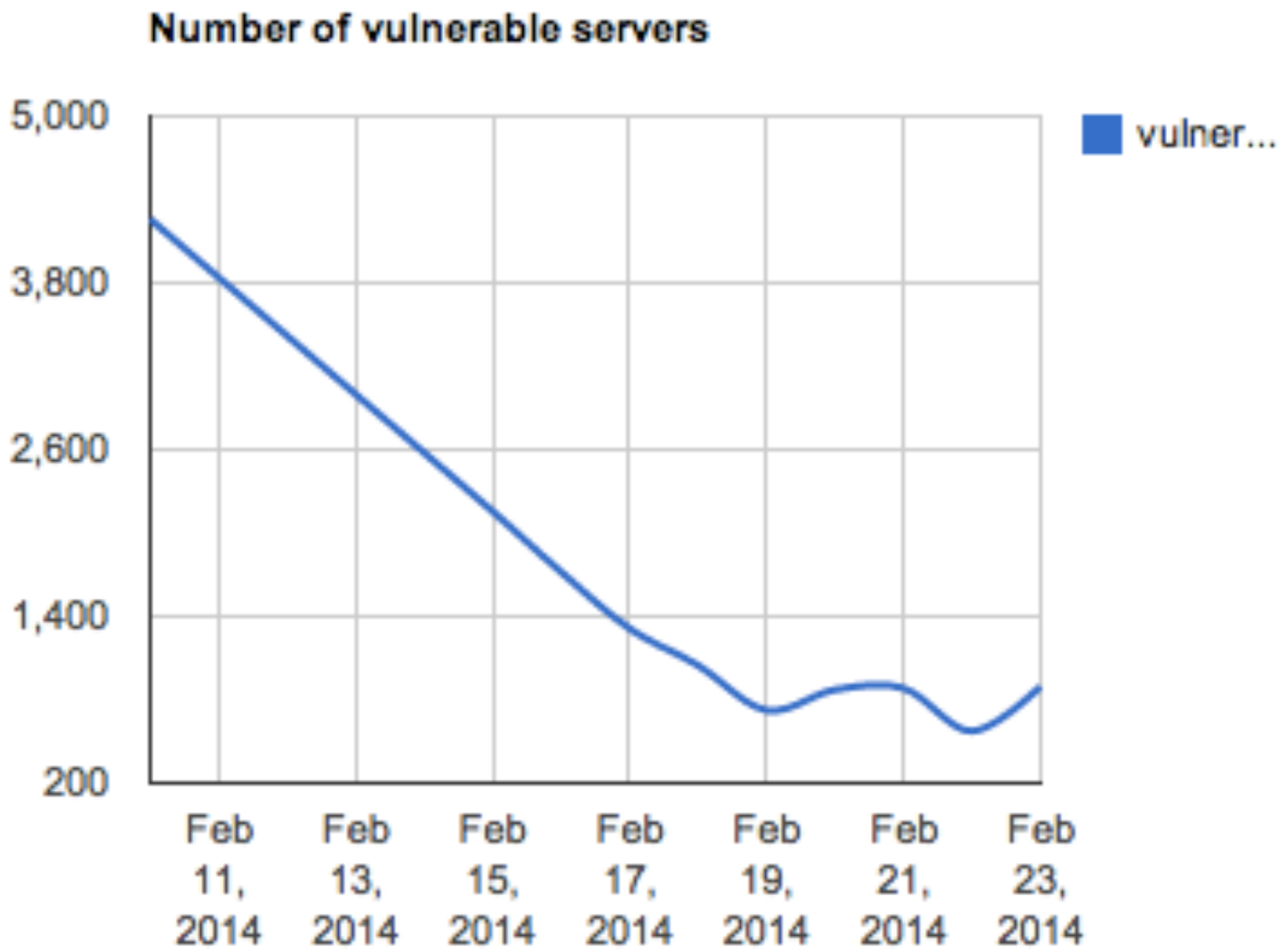
Spoofing attack: NTP DoS

- In February 2014 Cloudflare witnessed a 400 Gbps NTP attack
- Used 4529 NTP servers



Spoofing attack: NTP DoS

- In February 2014 Cloudflare witnessed a 400 Gbps NTP attack
- Used 4529 NTP servers



Botnets

Botnets

- A botnet is a logical collection of Internet-connected devices (computers, smartphones or IoT devices) that have been infected and are controlled by a third party

- A controller software (known as “command & control”) is able to direct the activities of each compromised device (known as a “bot”) using network protocols like HTTP

- Botnets are used for **D**istributet **D**enial **o**f **S**ervice (DDoS) attacks and other types of attacks (spam, data theft, etc...)

engadget

Login

Reviews Gear Gaming Entertainment Tomorrow Audio Video Buyer's Guide

B@d P@sswOrd

Bad Password is a monthly hacking and security column examining infosec and our ever-eroding "privacy".

See all articles

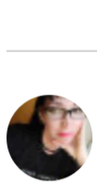
Latest in Gear

Amazon says it'll roll out a new grocery store format next year

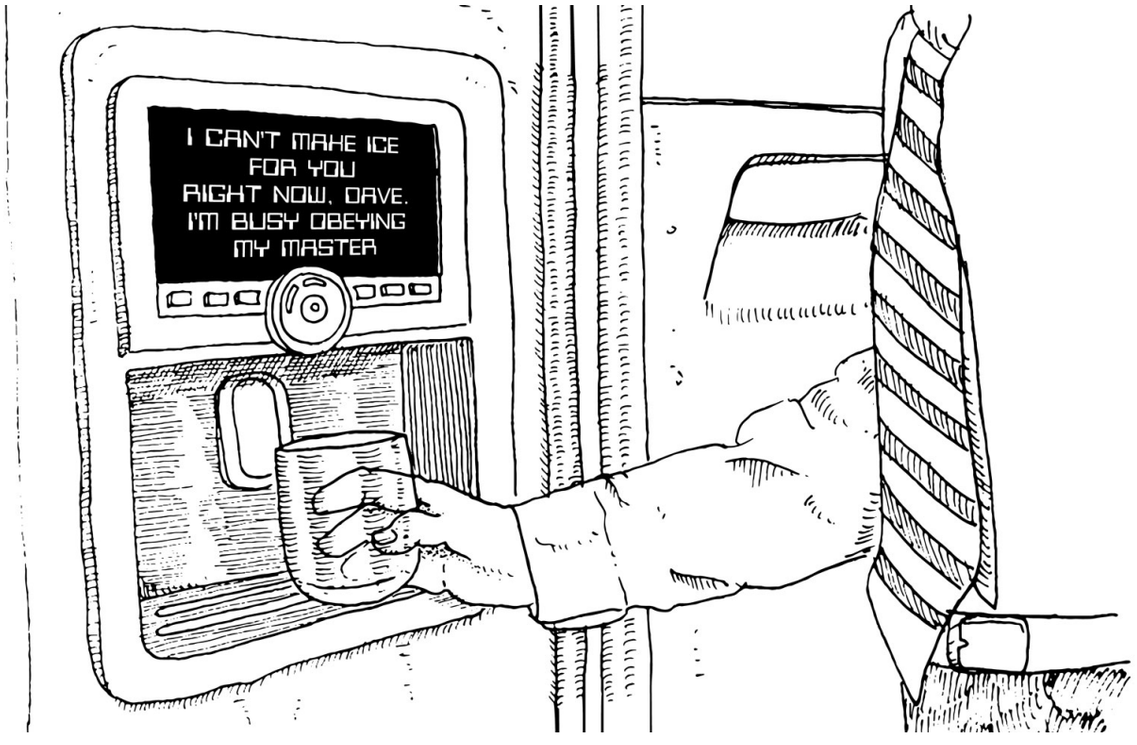
15m ago

That time your smart toaster broke the internet

Did anyone try turning it off and on again?



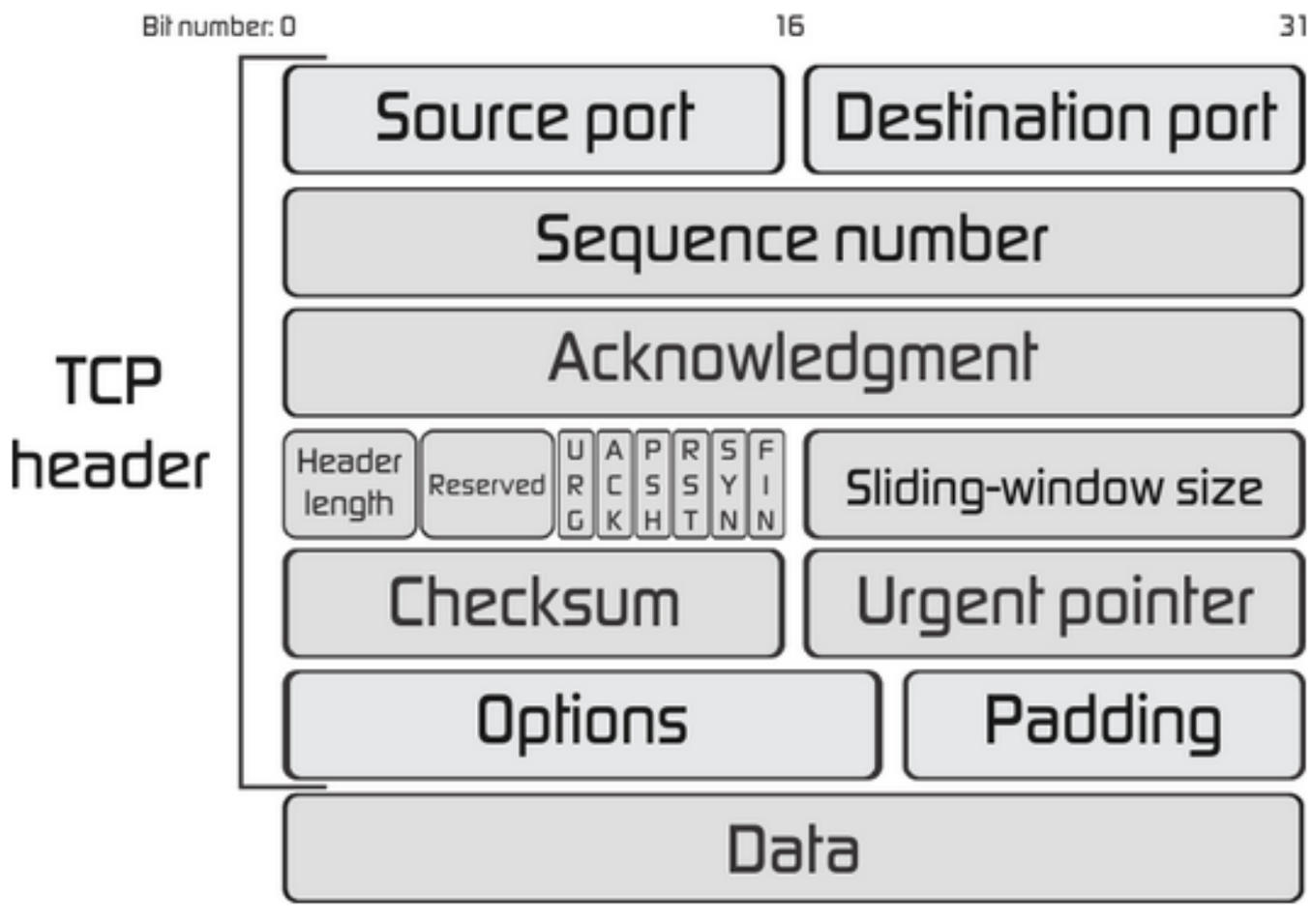
Violet Blue, @violetblue
10.28.16 in Security



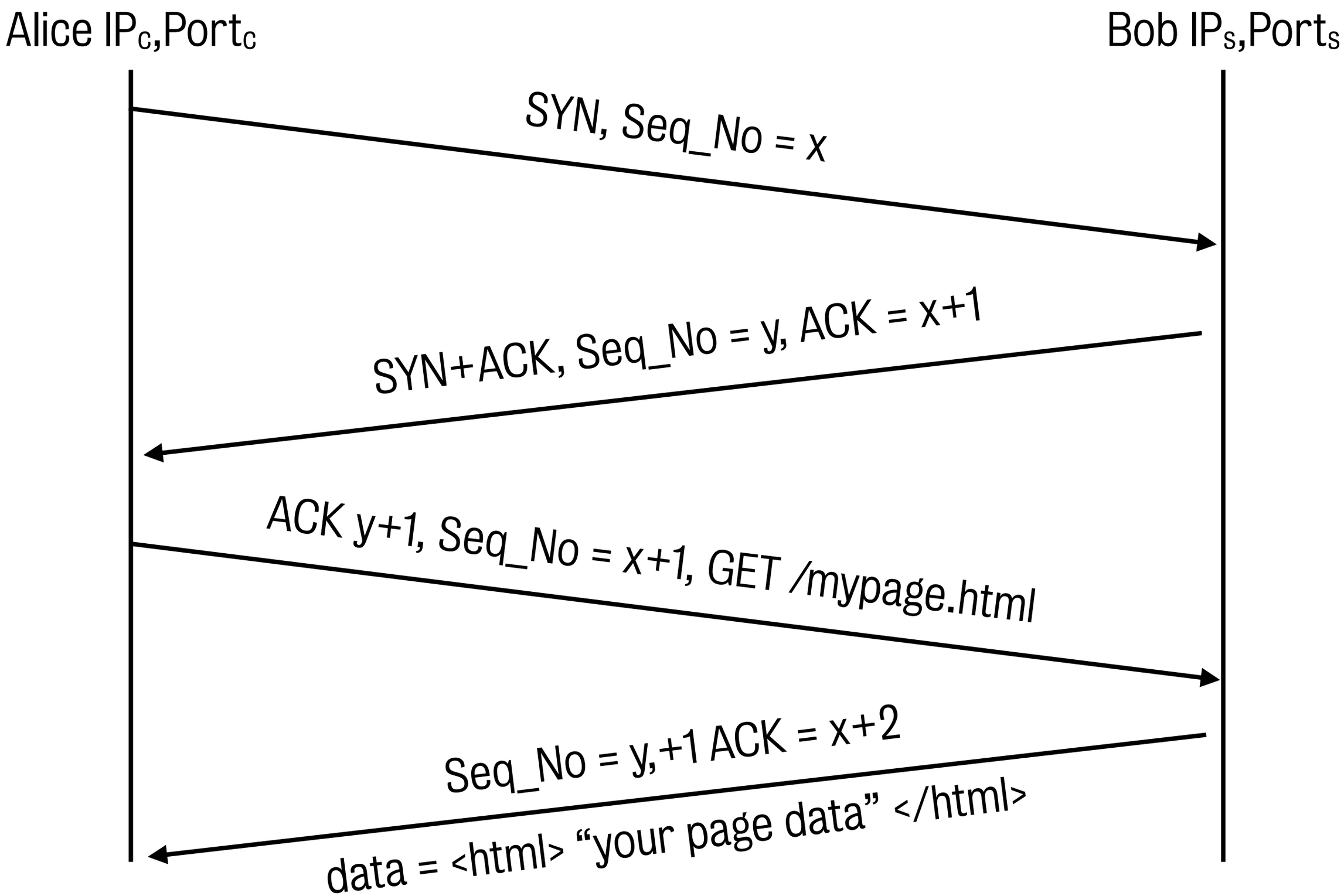
Spoofing attack: SYN flooding

- **T**ransmission **C**ontrol **P**rotocol (TCP) defines a connection of ordered sequence of bytes, over unordered IP network

- IP address + port number defines connection



TCP connection set up: Three Way Handshake



SYN flooding

- A SYN flood attack works by not responding to server with the expected ACK code.

- The malicious client can either not send the expected ACK, or more effectively **spoof the source IP address** in the SYN, causing the server to send the SYN-ACK to a falsified IP address - which will not send an ACK because it “knows” that it never sent a SYN.

- The server will wait for the missing ACK for a bit. However, the resources bound on the server may eventually exceed the resources available and the server cannot connect to any client.

LAB time (EPISODE 2)

- Network Tools and Sniffing
- You will learn how to use:
  - Network commands -> ifconfig, netstat, arp, etc...
  - Sniffing tools: tcpdump, wireshark