Sniffing and Spoofing

Ethical Hacking

Alessandro Brighente
Eleonora Losiouk

October, 2022

Master Degree on Cybersecurity

Università degli Studi di Padova

SPRITZ
Security & Privacy
Research Group

What is Network Security?

- “Network security is the protection of the underlying networking infrastructure from unauthorized access, misuse, or theft. It involves creating a secure infrastructure for devices, applications, users, and applications to work in a secure manner.” **Cisco**

- “Network security is a category of practices and technologies that keep internal networks protected from attacks and data breaches. It encompasses access control, cyber attack prevention, malware detection, and other security measures.” **Cloudflare**

What do we Need?

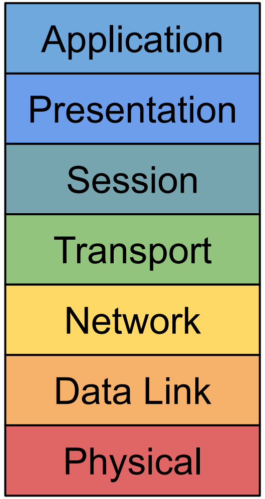
- Network security is based on the knowledge of both the network architecture and the protocols that manage the different aspects of the network
    - How are devices connected?
    - Who can access which part of the network?
    - Who can send and receive messages in the network?

How to Setup a Connection

What do devices need to communicate?

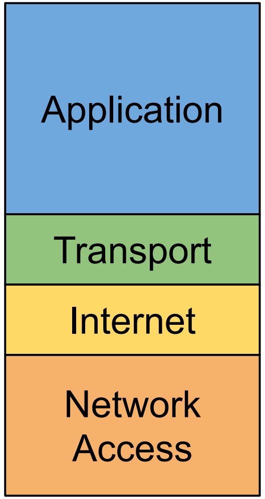
- Physical address
- Network address
- A common language

TCP/IP Model



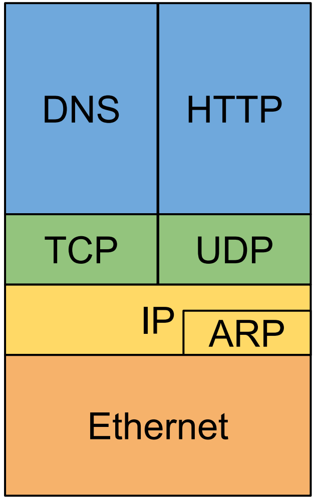
Application
Presentation
Session
Transport
Network
Data Link
Physical

ISO/OSI



Application
Transport
Internet
Network Access

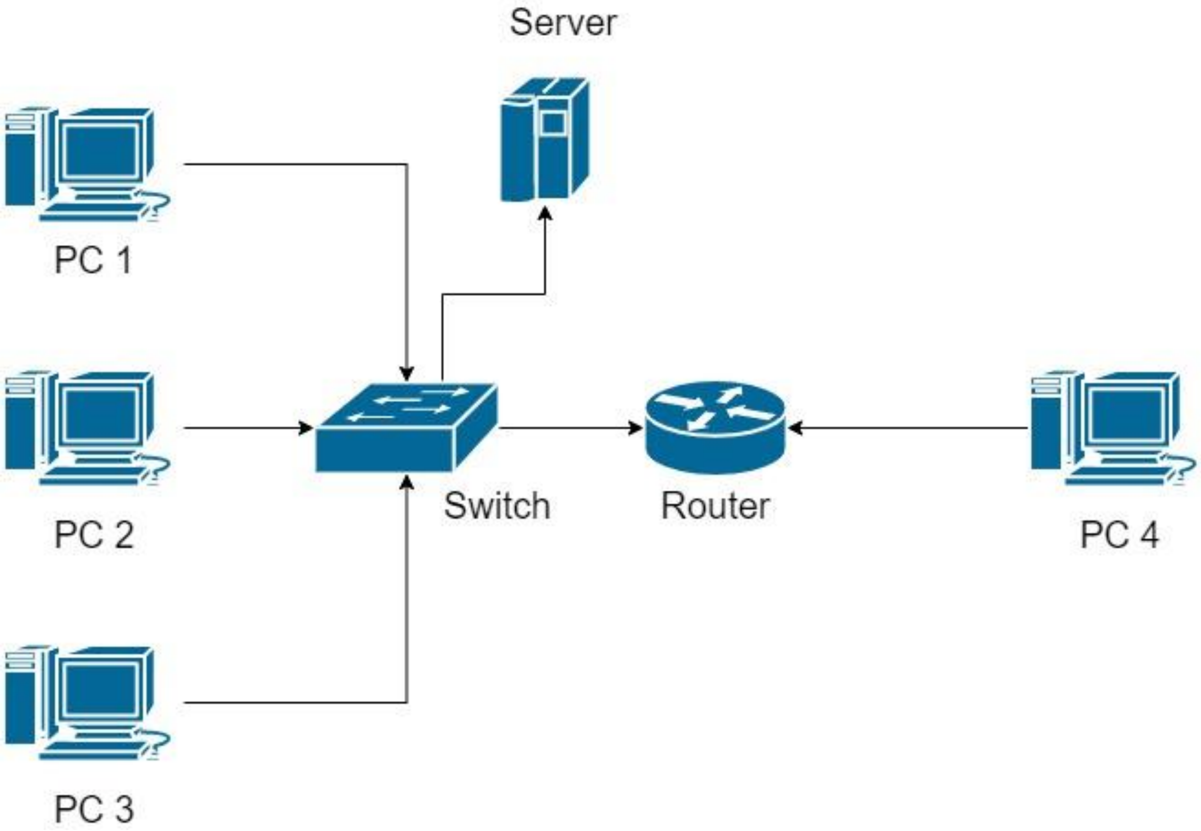
TCP/IP



DNS
HTTP
TCP
UDP
IP
ARP
Ethernet

Standard Protocols

A Basic Network



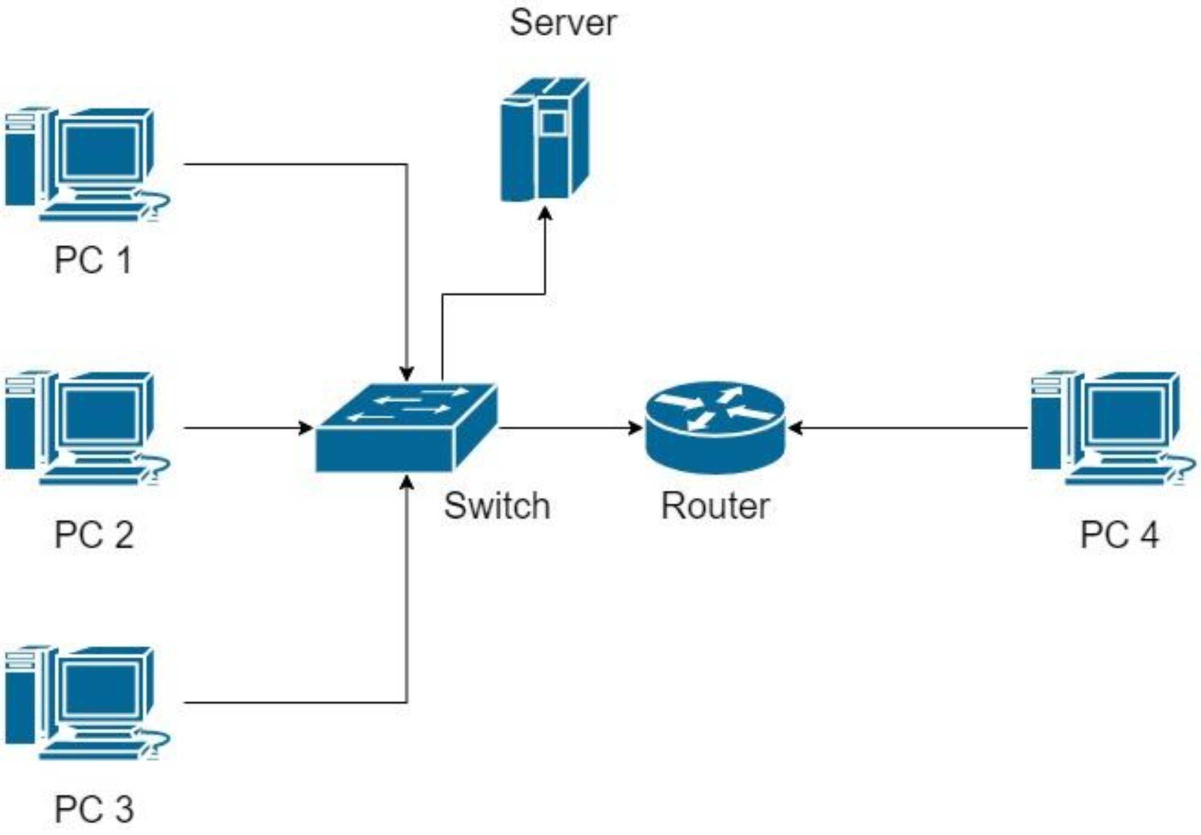
A Basic Network

Assigned in this network

IP: 192.168.2.1

MAC: 00:25:96:FF:FE:12:34:56

Device specific

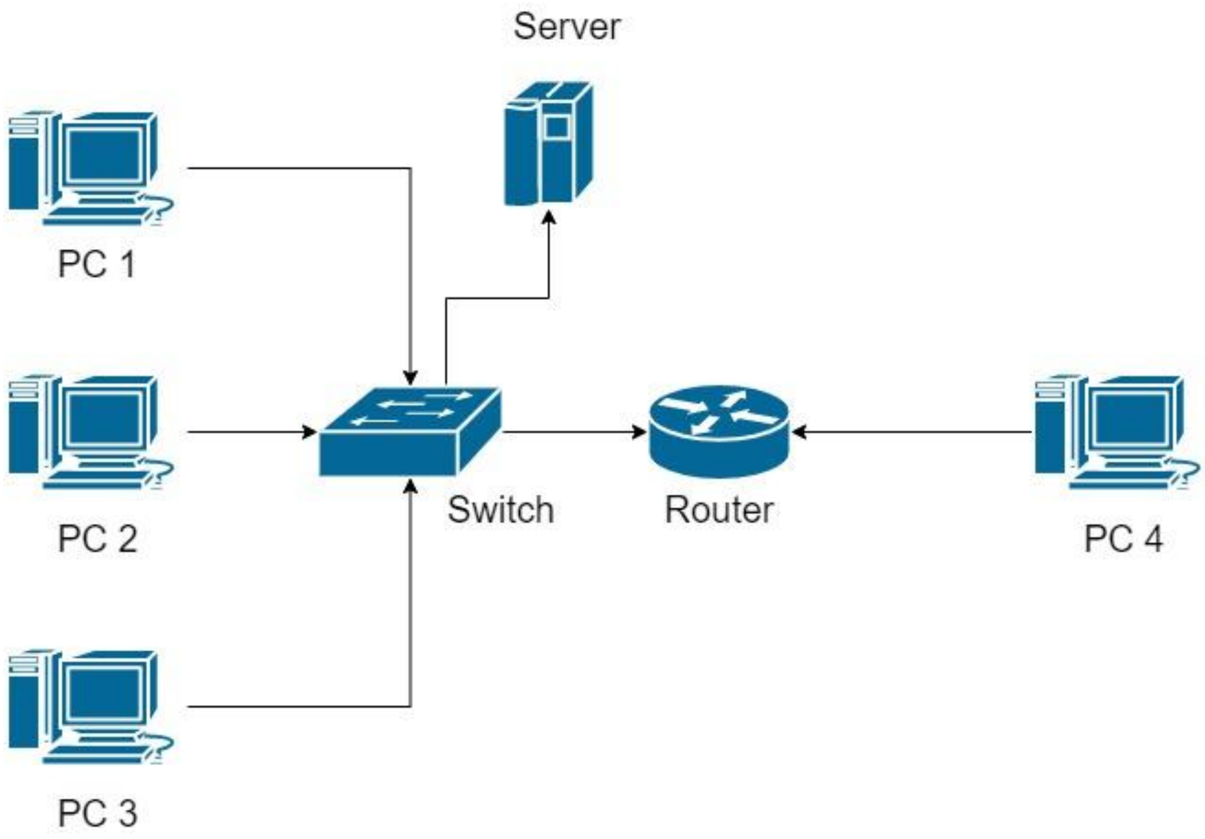


A Basic Network

IP: 192.168.2.1
MAC: 00:25:96:FF:FE:12:34:56

IP: 192.168.2.2
MAC: 00:45:96:FE:FE:24:04:56

IP: 192.168.2.3
MAC: 01:15:23:FF:FF:04:04:56

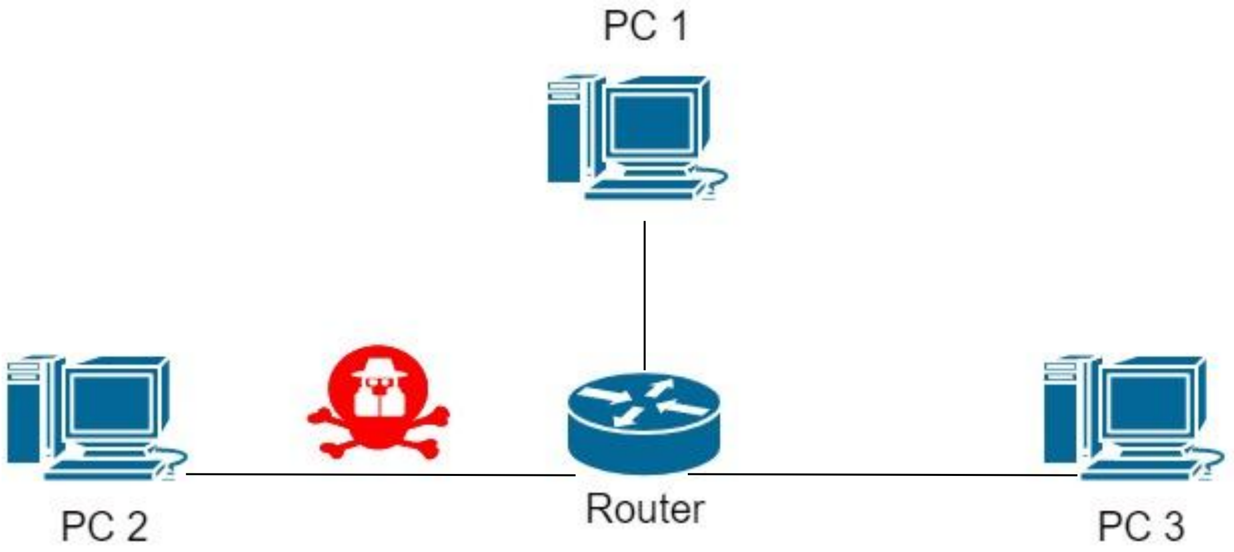


Packet Sniffing

- Sniffing attacks involves an attacker overhearing live communication between devices in the network
- Thanks to sniffing, the attacker might get useful information on the network devices, the running services, or possible sensitive users' information
- In order to sniff packets, the attacker shall be connected to the transmission medium

Sniffing

- The attacker captures the packets exchanged in the network
- Obtain information on connected devices, and information exchanged
- Hosts, routing table, addresses,...

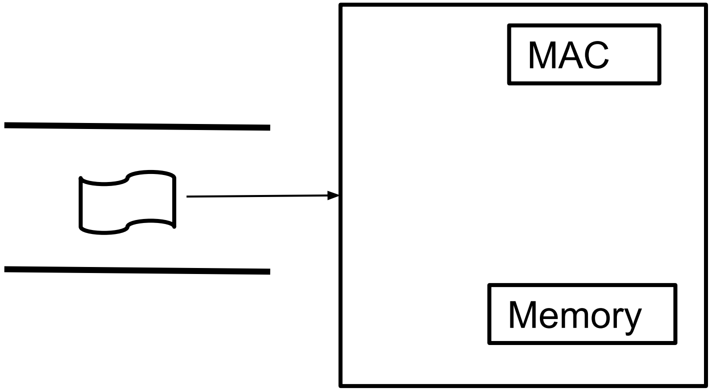


How are packets received

- Machines are connected to the network via a Network Interface Card (NIC)
- A NIC is a physical device associated with a MAC address
- Physical and logical interface from the machine to the network and viceversa

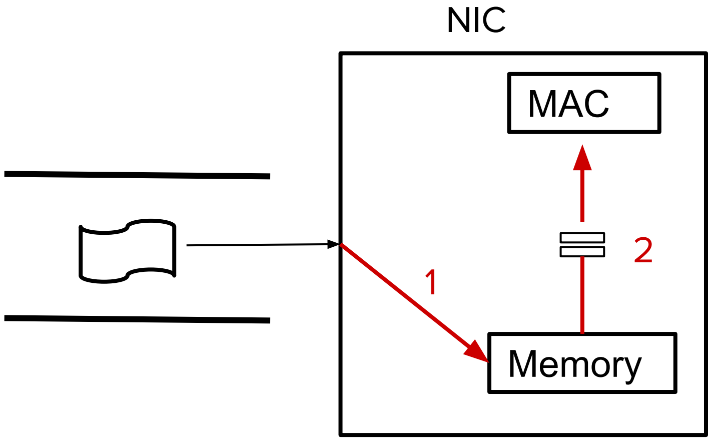
How are packets received

- Machines are connected to the network via a Network Interface Card (NIC)
- A NIC is a physical device associated with a MAC address



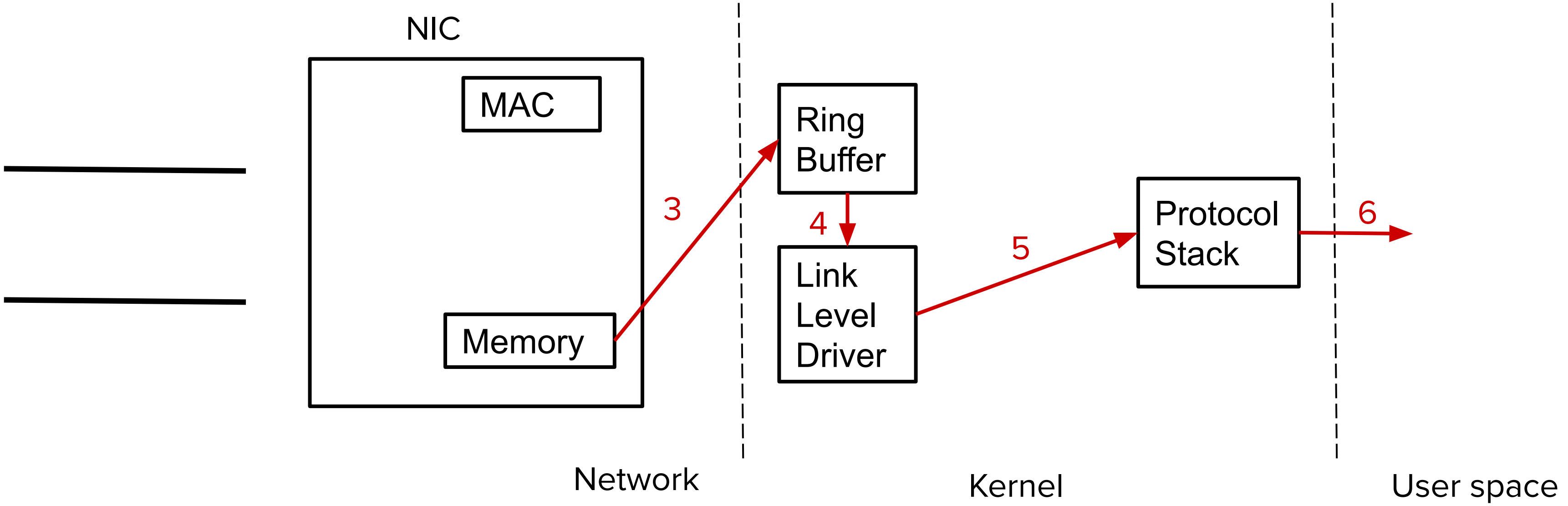
How are packets received

- Machines are connected to the network via a Network Interface Card (NIC)
- A NIC is a physical device associated with a MAC address



How are packets received

- Machines are connected to the network via a Network Interface Card (NIC)
- A NIC is a physical device associated with a MAC address



Promiscuous and Monitor Modes

- Generally a NIC discards packets for which it is not the intended destination
- However, if set in promiscuous mode, it forwards all the packets to the kernel and eventually to a sniffer program
- This allows an attacker to overhear communications among other machines
- Monitor mode is the equivalent for wireless networks

What after sniffing?

- Thanks to sniffing we can have a lot of useful information
- Network addresses, host addresses, running services, protocols..
- This may be generally used by network administrators to check the well being of the network
- However, an attacker may use this information for malicious purposes

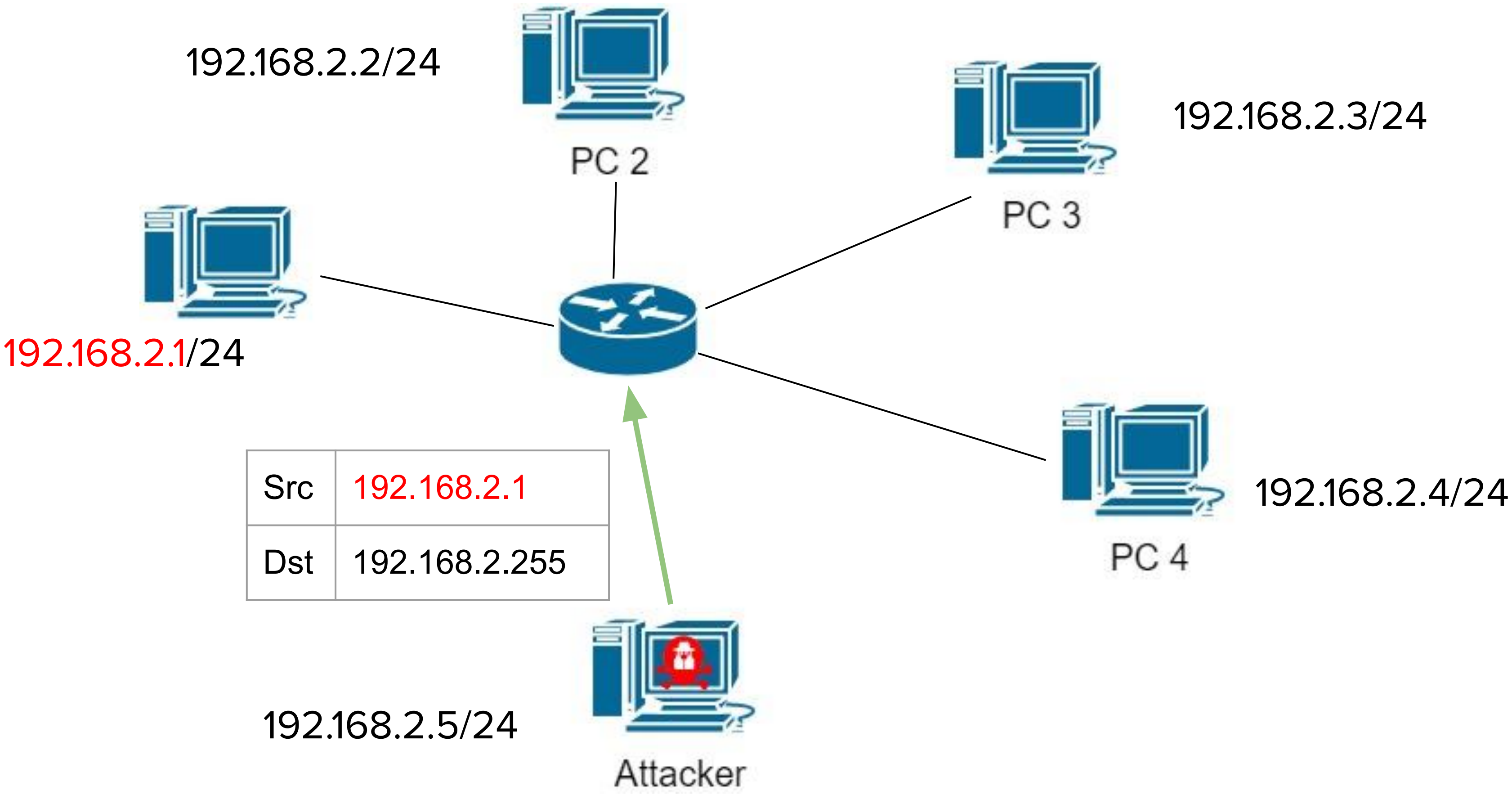
Spoofing

- When using socket programming to send packets we typically have control over few fields in the header
- For instance, when sending an IP packet, we can only select the destination address
- The source address is automatically filled in by the sending device
- However, an attacker may manipulate packets to include bogus and malicious information
- Spoofing: process when some critical information in the packet is forged

Smurf Attack

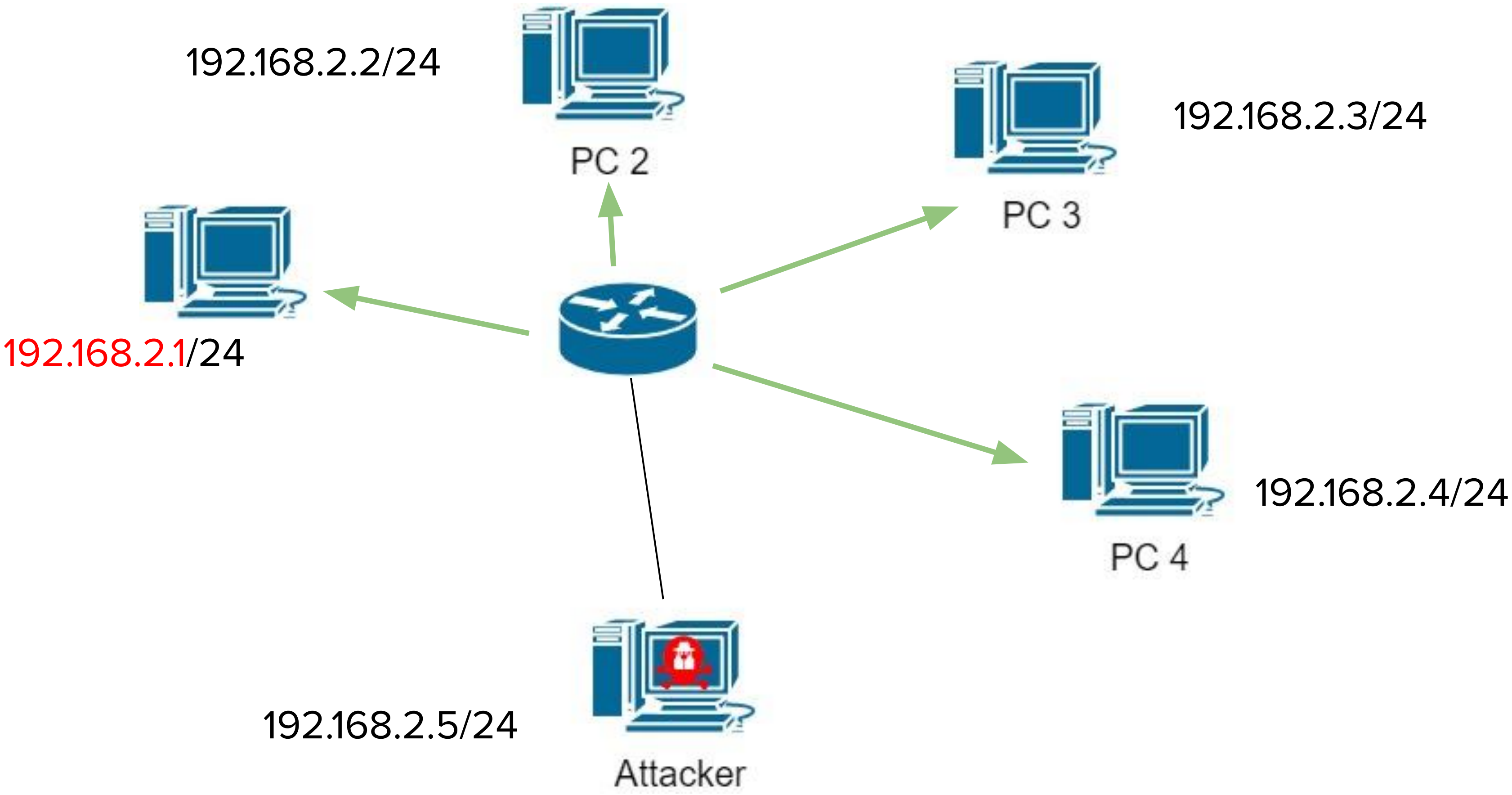
- Spoofing attack in Internet Control Message Protocol (ICMP)
- The attacker sends a spoofed ICMP packet using the victim’s address as sender’s address
- The attacker sends the ICMP request on a broadcast address
- Each node in the network replies to the ICMP request
- The victim node is overwhelmed by ICMP response packets

Smurf Attack

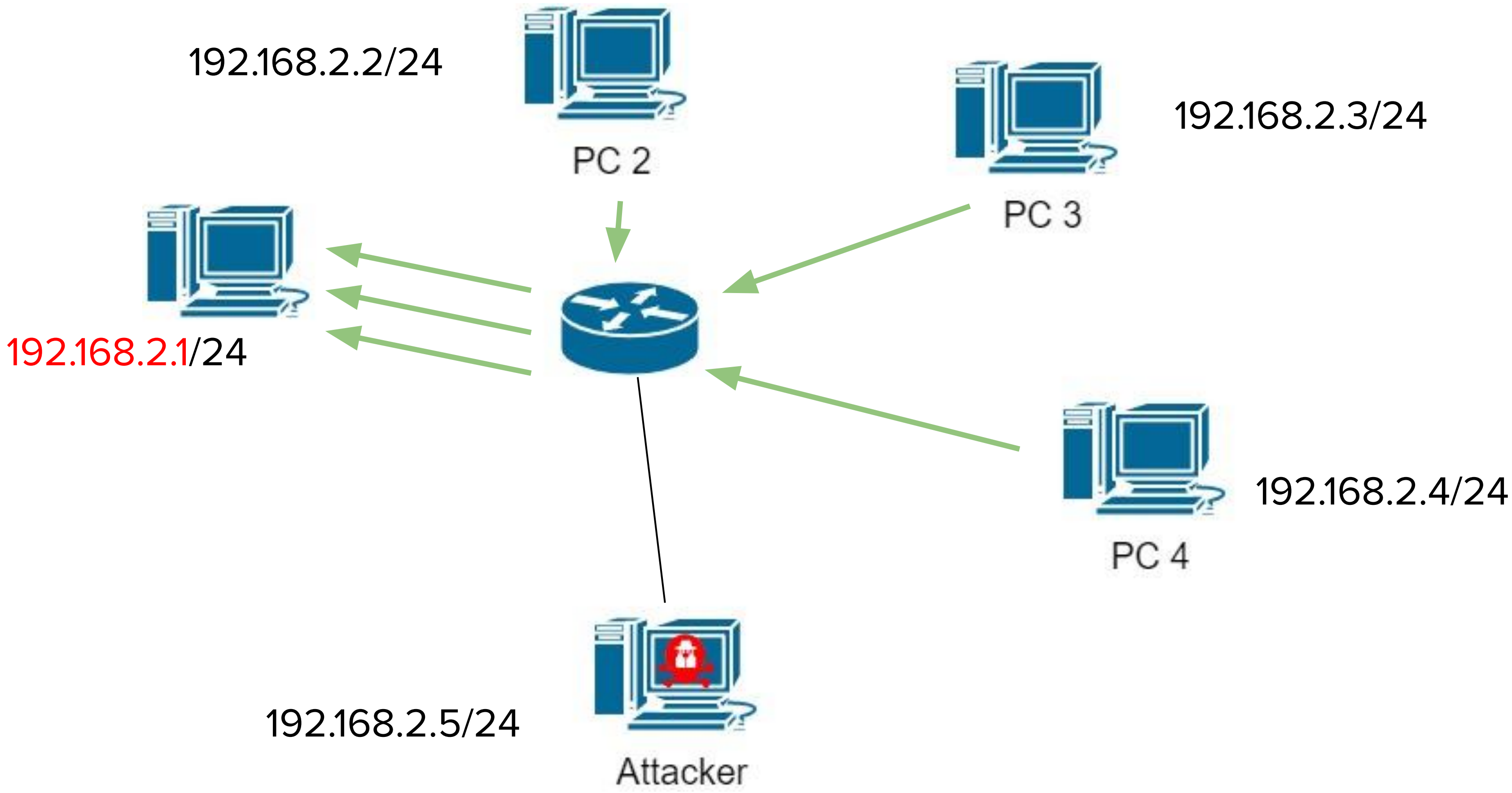


Src	192.168.2.1
Dst	192.168.2.255

Smurf Attack



Smurf Attack


192.168.2.2/24
PC 2
192.168.2.3/24
PC 3
192.168.2.1/24
192.168.2.4/24
PC 4
192.168.2.5/24
Attacker