Wrocław University of Technology

Network Attack and Defense

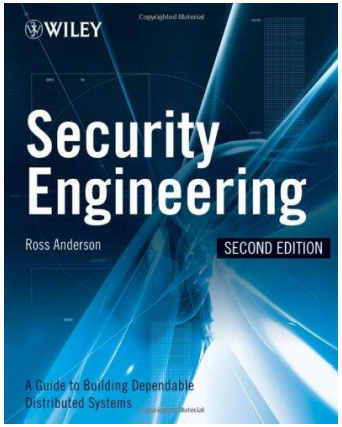
Piotr Giedziun

Agenda

- Book coverage
- Introduction
- Network vulnerabilities
  - Network protocols
  - Application layer
  - People
- Defense
- Summary

Book vs Slides

- Local Networks Attacks
  - ARP/DHCP Spoofing
- Internet Protocols Attacks
  - DoS/DDoS
  - SYN Flooding, Smurfing, Spam
- Application vulnerabilities
- Trojans, Viruses, Worms and Rootkits
- Firewalls, Spam Filters, Intrusion Detection
- Encryption

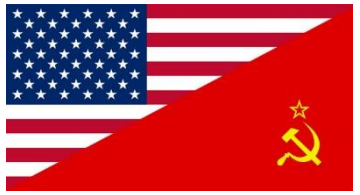


Chapter 21
"Security Engineering"
by Ross Anderson

BOOK PRESENTATION

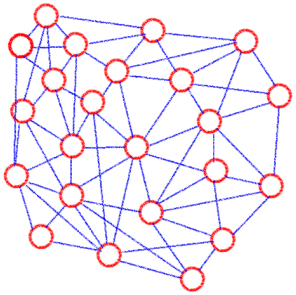
Introduction

- Project **ARPA**NET (1969)
  - Made to share information
  - 4-node network

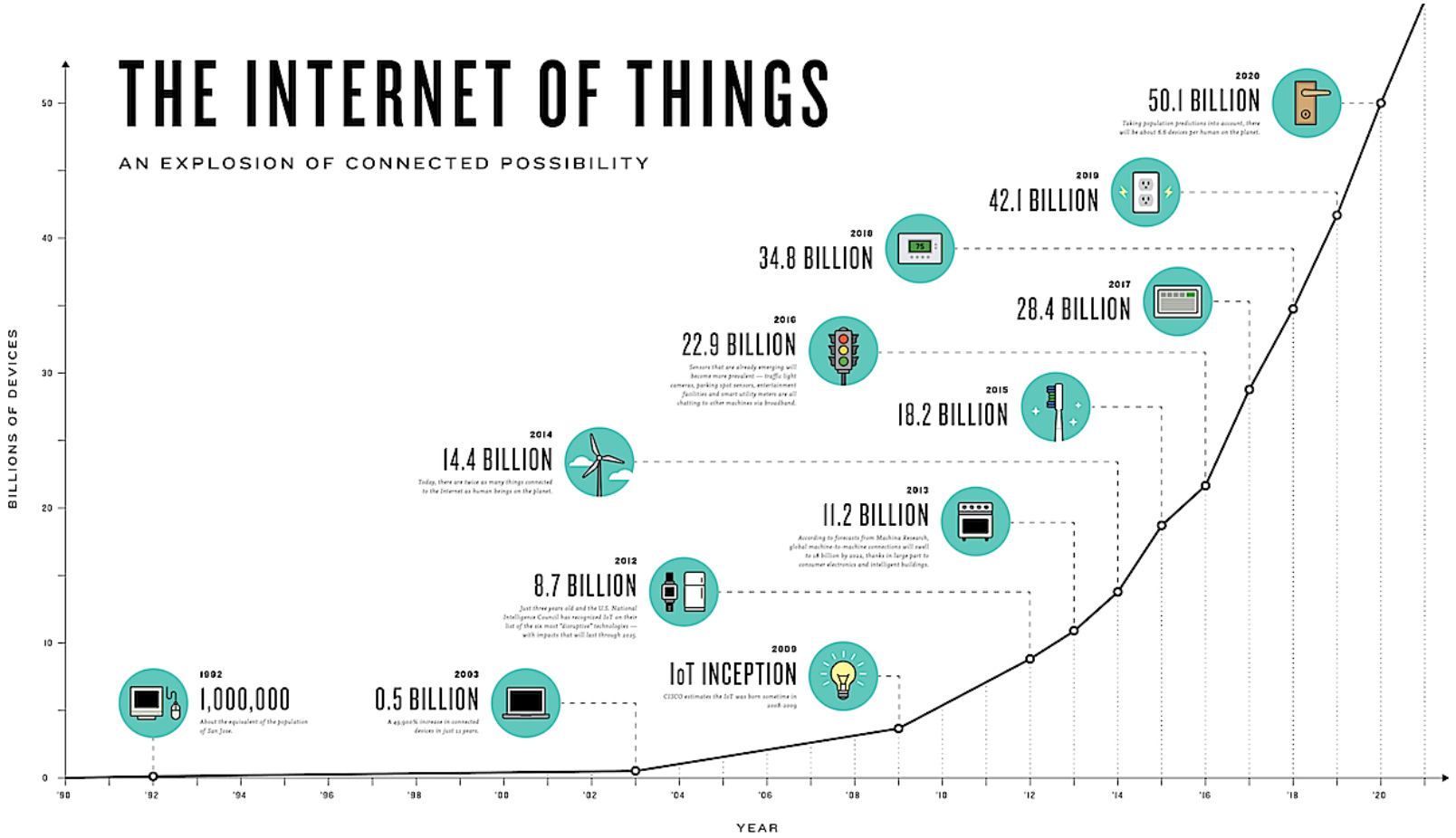


Sputnik 1

- ARPANET was replaced by NSFNet (1989)
  - 100,000 computers
  - Main goal to share research



Introduction #2



Source: www.theconnectivist.com

Introduction #3

- 41% of the world population has an internet connection

- 30,000 web sites are hacked every day
- Internet users send over 204 million emails **per minute**
  - 70% of them are spam

Source: www.factslides.com

Introduction #4

Yearly Cyber Crime Victim Count Estimate

Victims per year	556 million
Victims per day	Over 1.5 million

Countries Where Cyber Attacks Originate

1. Russia	2,402,722
2. Taiwan	907,102
13. Poland	**162,235**

Source: www.go-gulf.com

Introduction #4

Yearly Cyber Crime Victim Count Estimate

Victims per year	556 million
Victims per day	Over 1.5 million

Countries Where Cyber Attacks Originate

1. Russia	2,402,722
2. Taiwan	907,102
13. Poland	**162,235**

76 in FIFA Ranking 2013

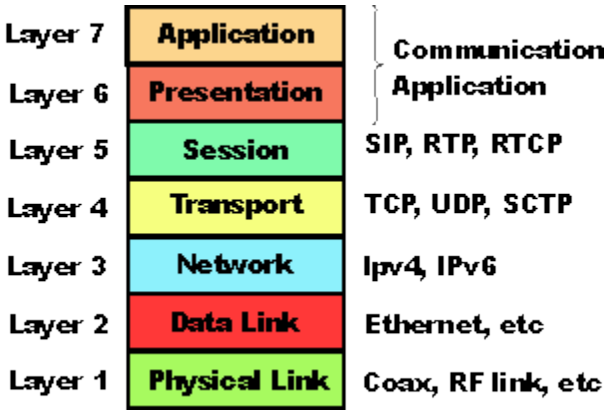
Source: www.go-gulf.com

Network Attacks - vulnerabilities

- Network Protocols flaws
- Application vulnerabilities
  - Software bugs
  - Implementation flaws
- People

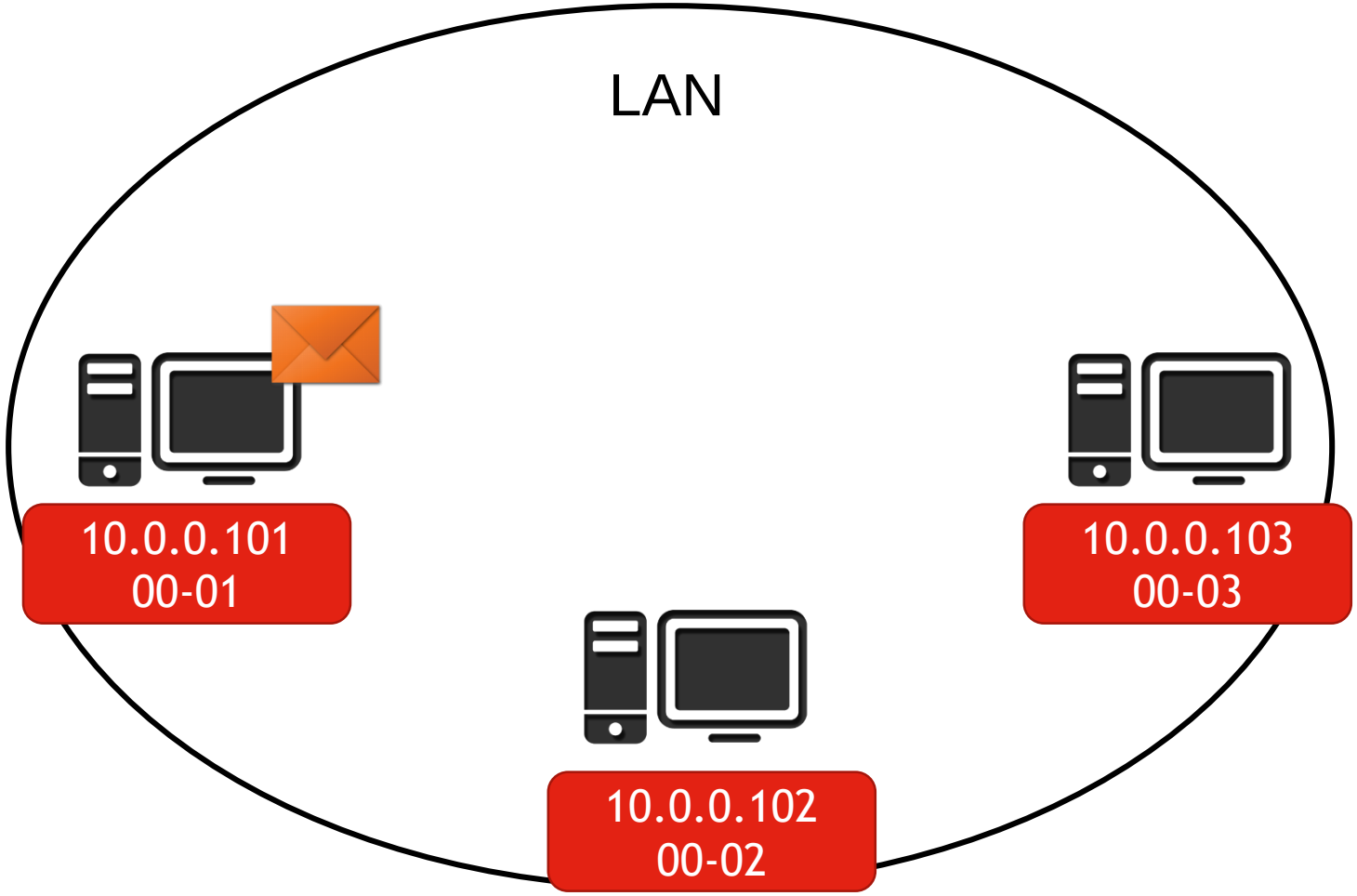
Network Protocols flaws

- ARP (layer 2/3)
  - Used for mapping network IP addresses to physical addresses (MAC) **without authentication**
  - Uses ARP cache for **maintain a correlation** between each MAC address and its corresponding IP address

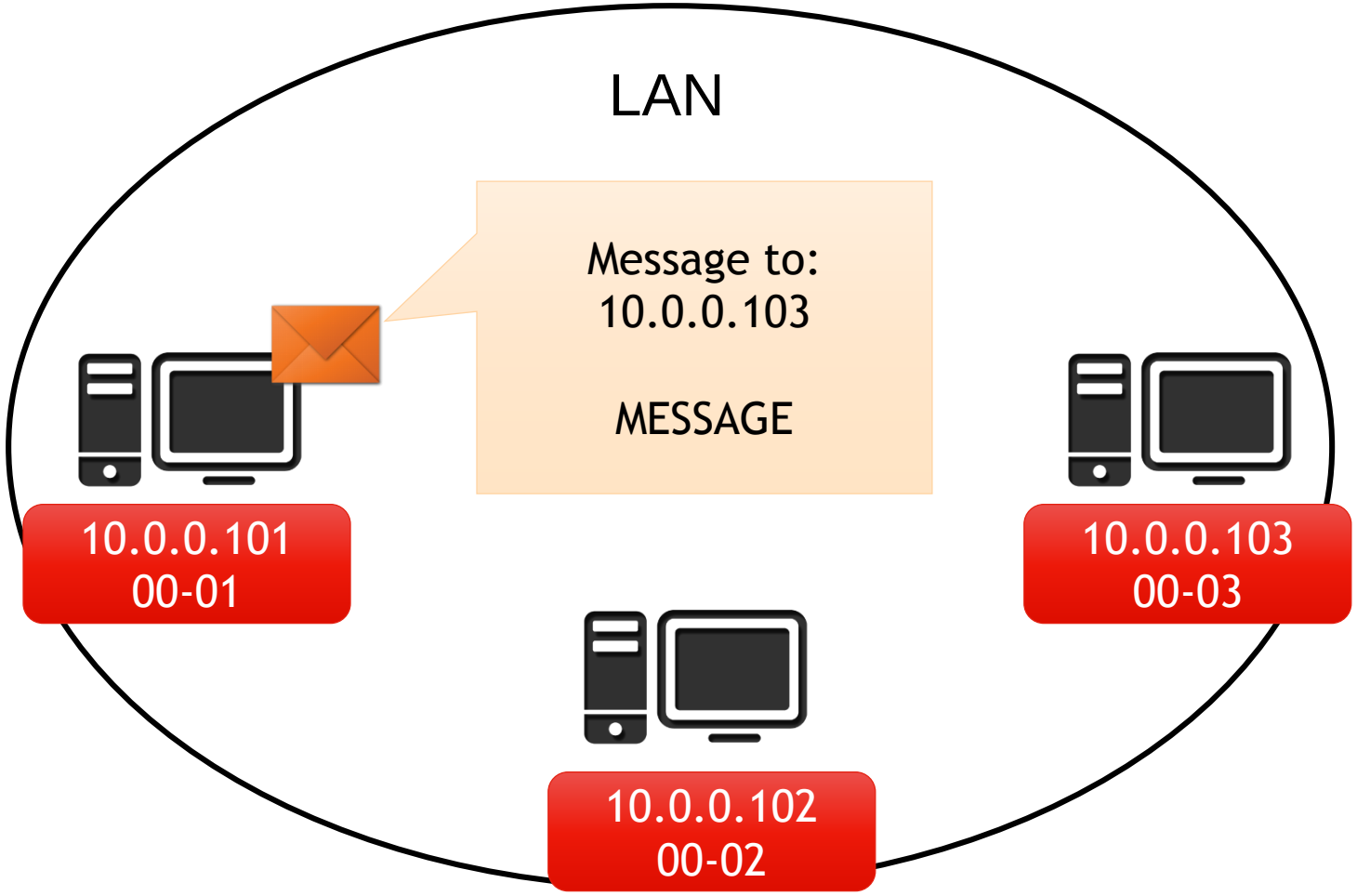


OSI Model

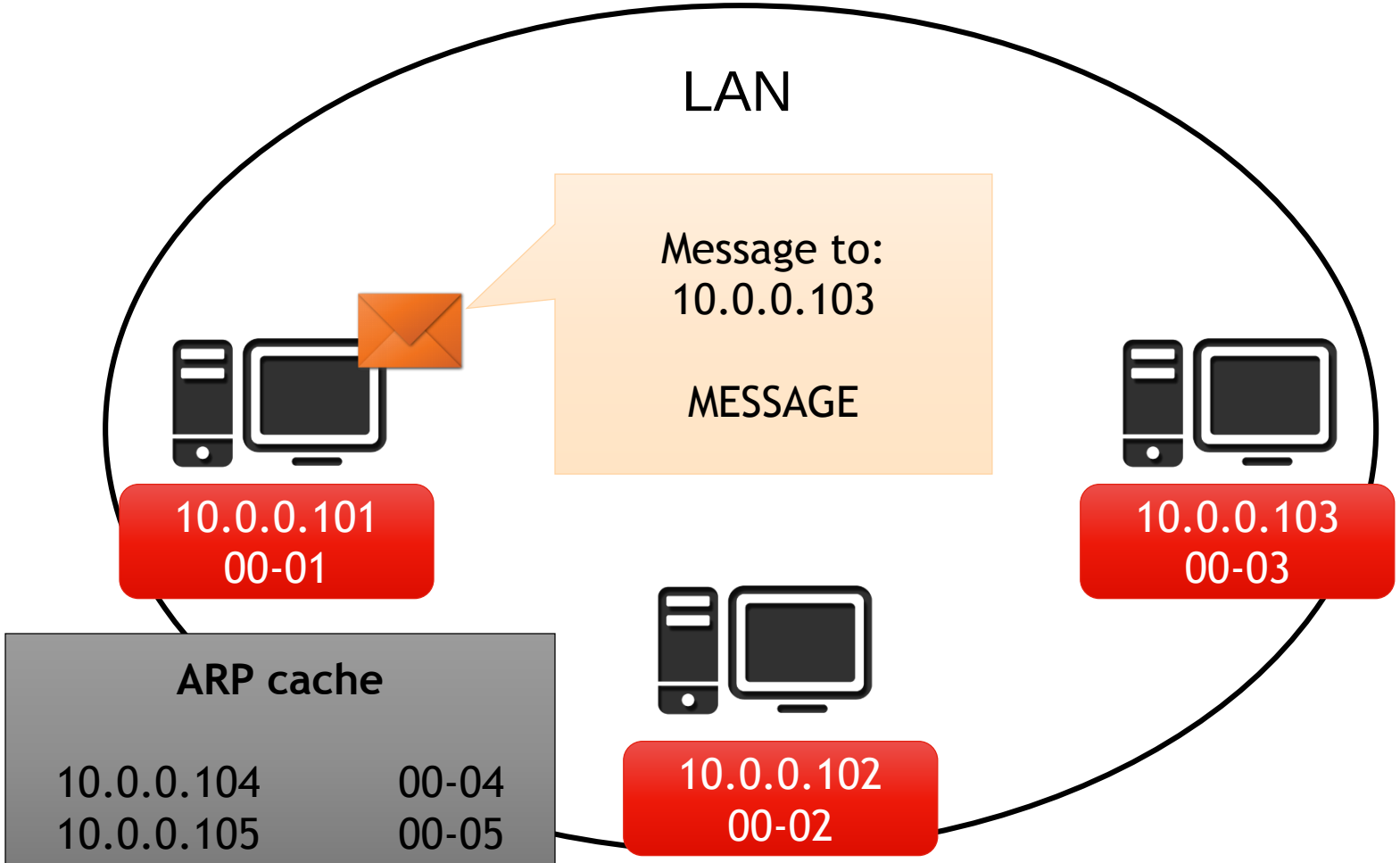
Address Resolution Protocol



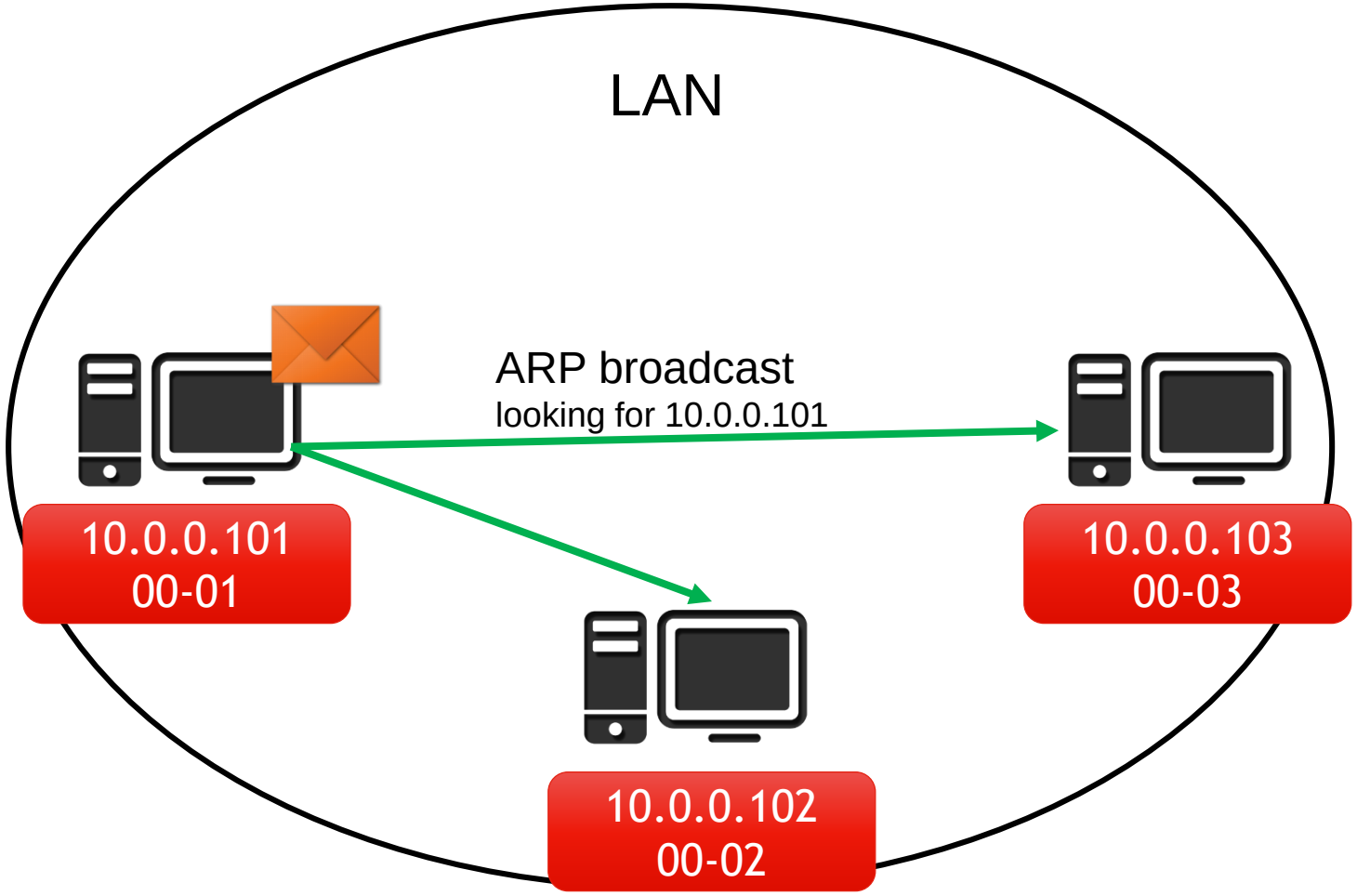
Address Resolution Protocol



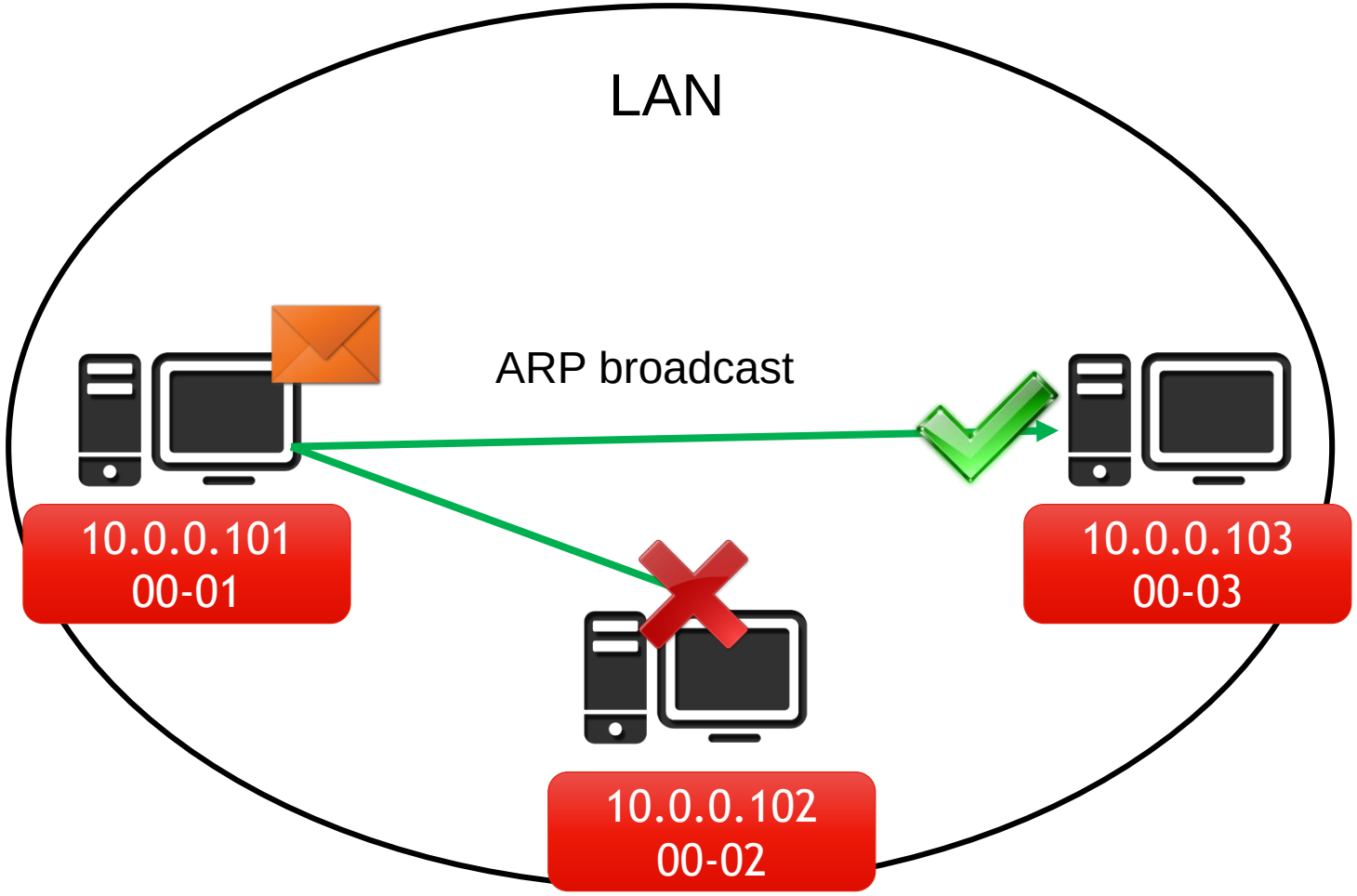
Address Resolution Protocol



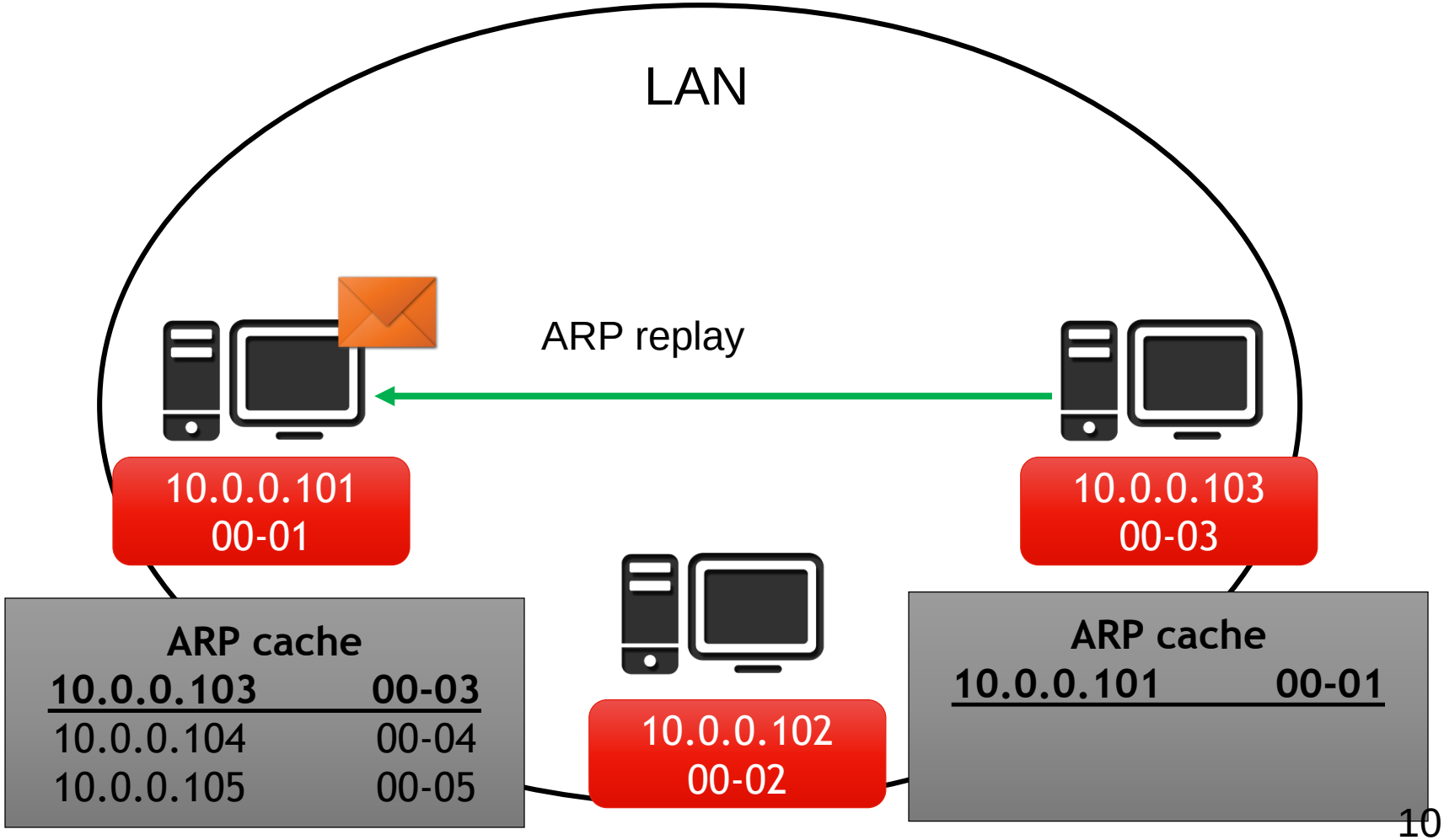
Address Resolution Protocol



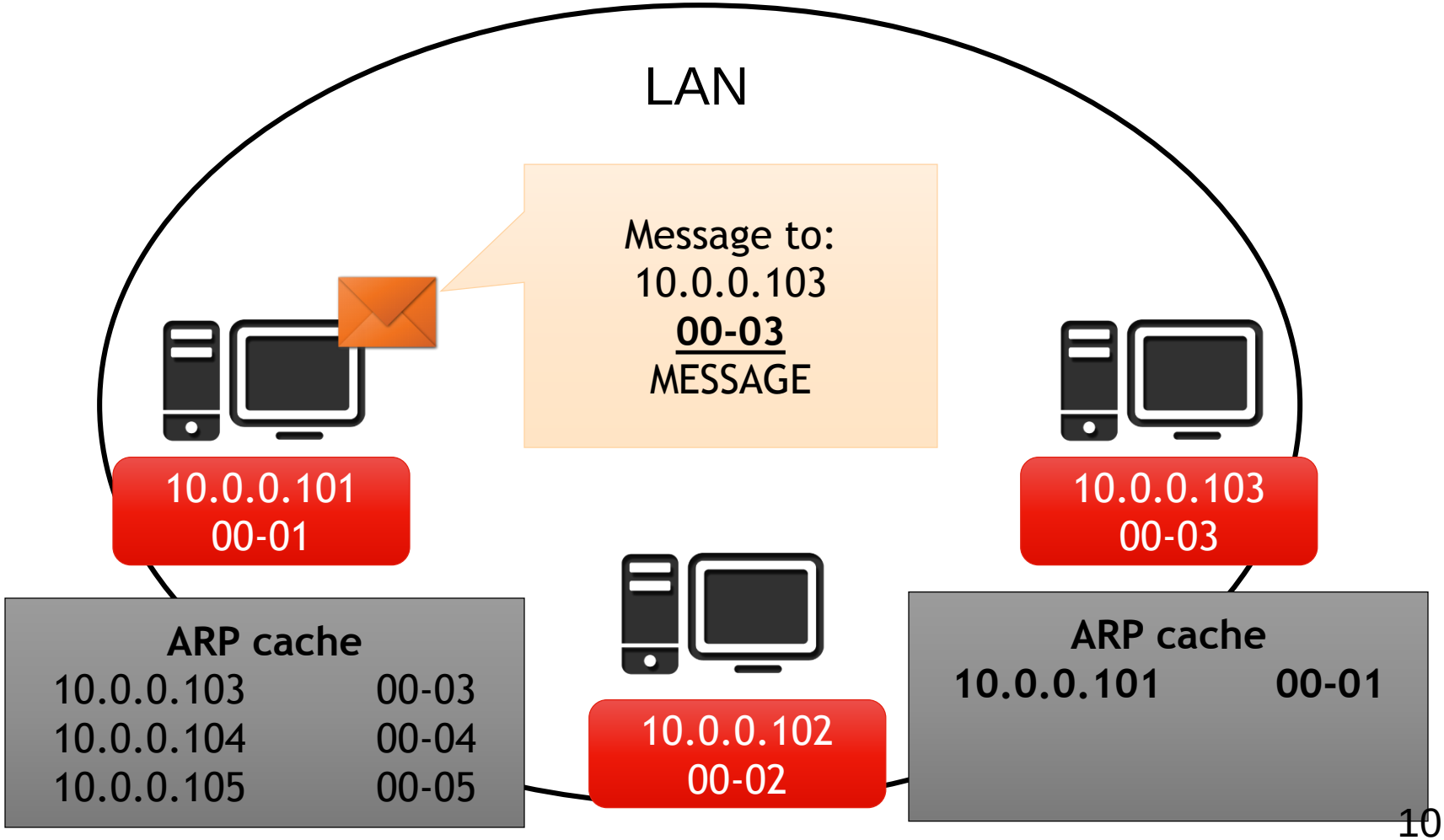
Address Resolution Protocol



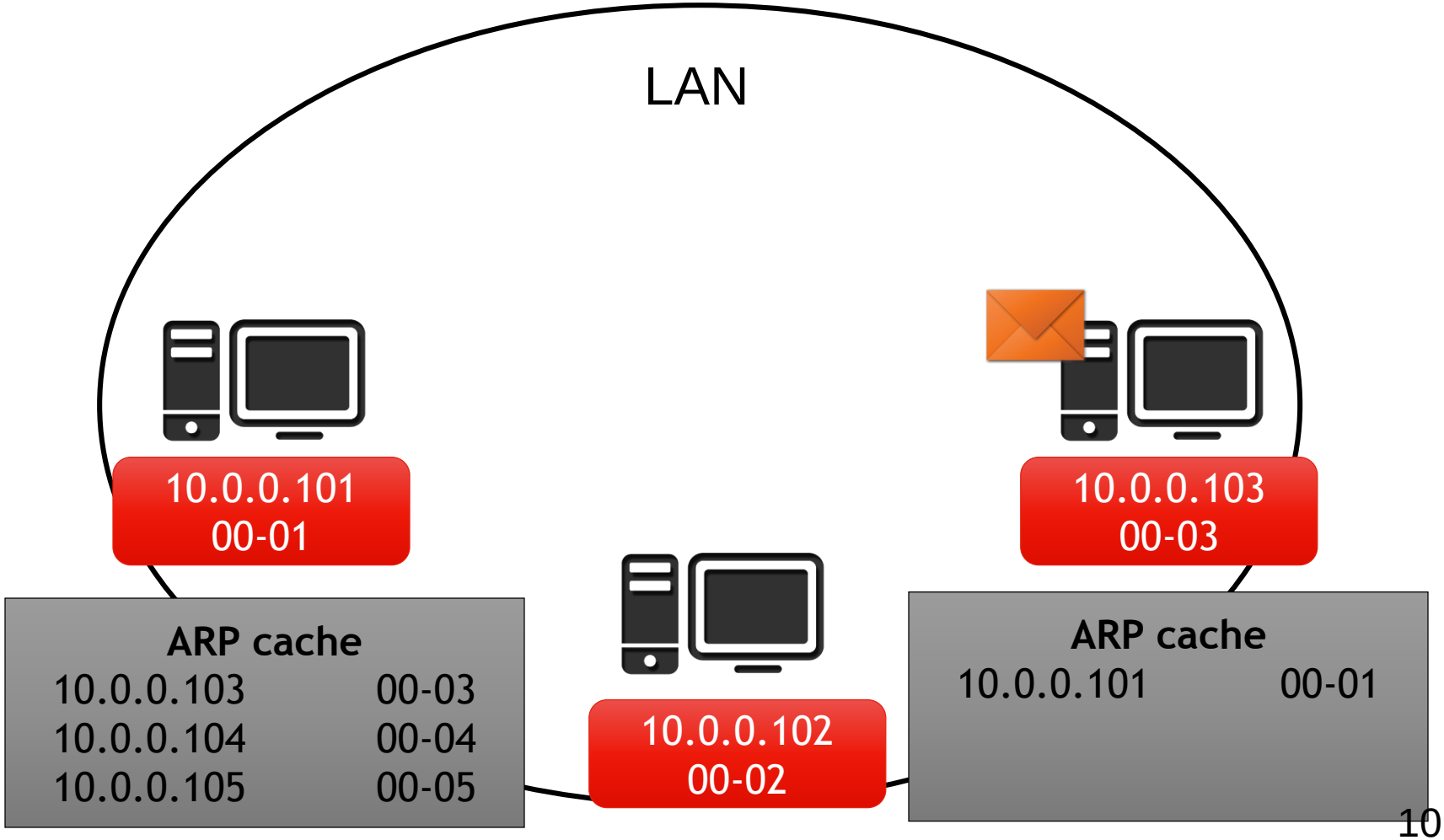
Address Resolution Protocol



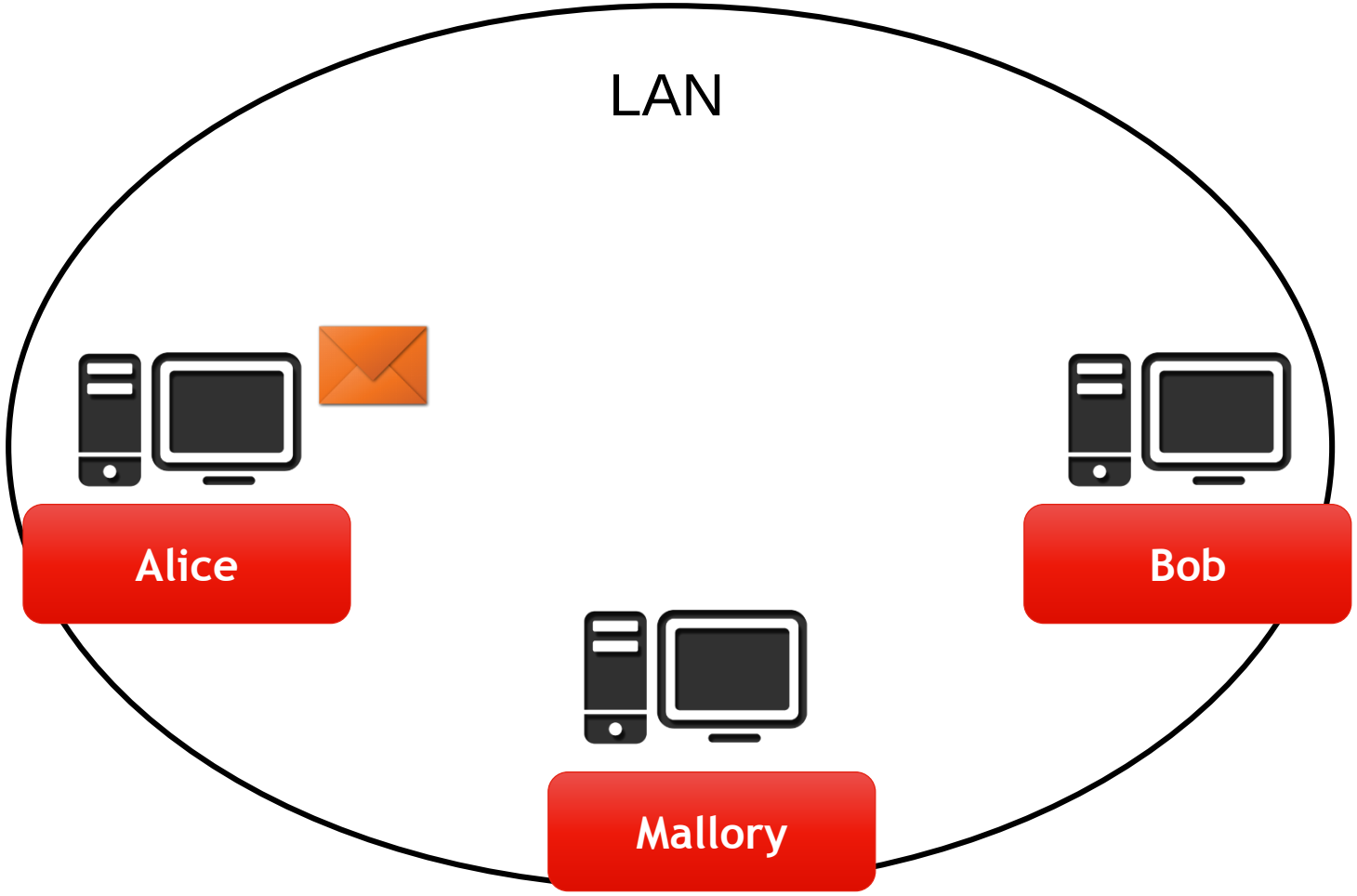
Address Resolution Protocol



Address Resolution Protocol

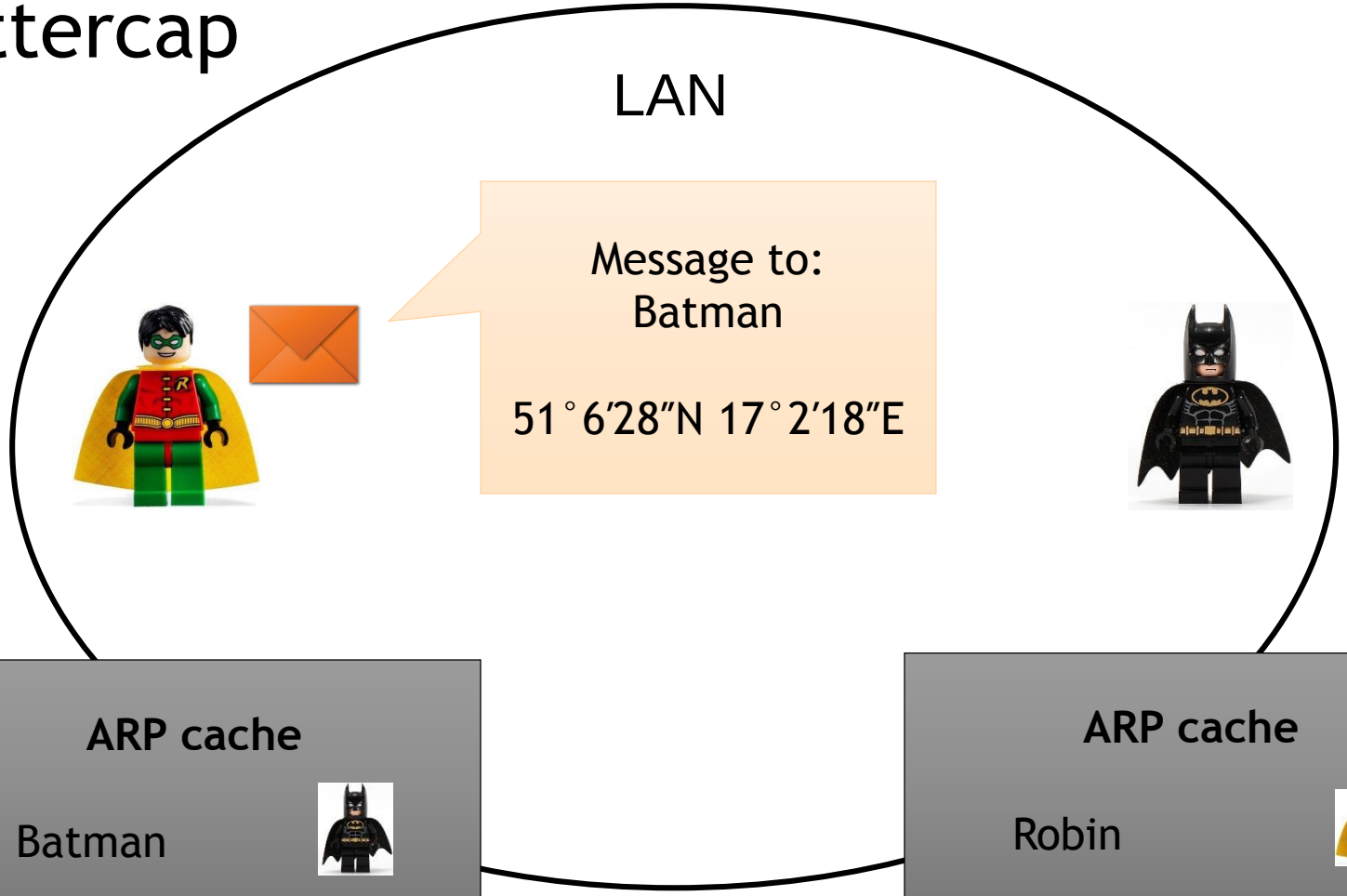


ARP Spoofing

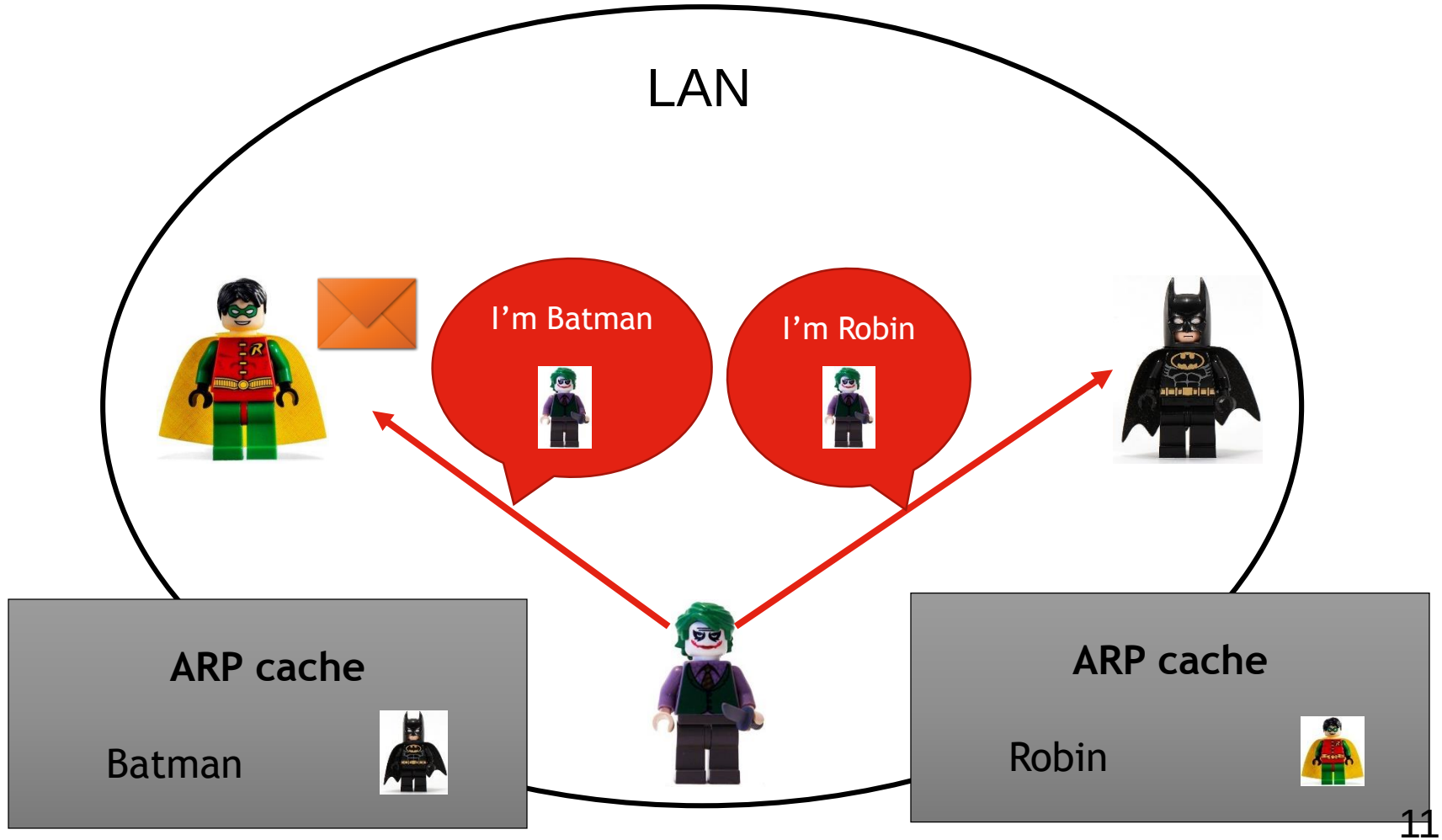


ARP Spoofing

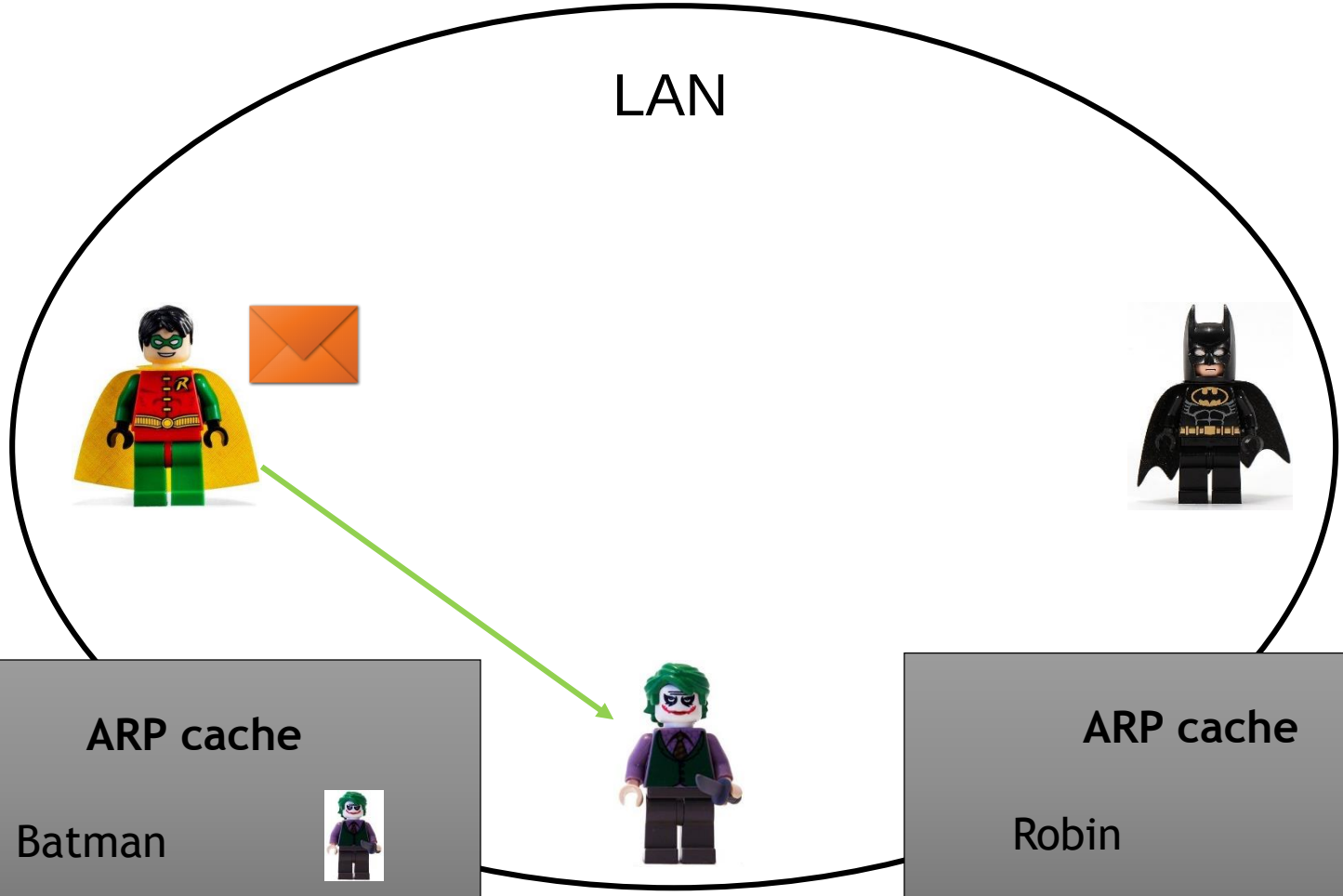
- ettercap



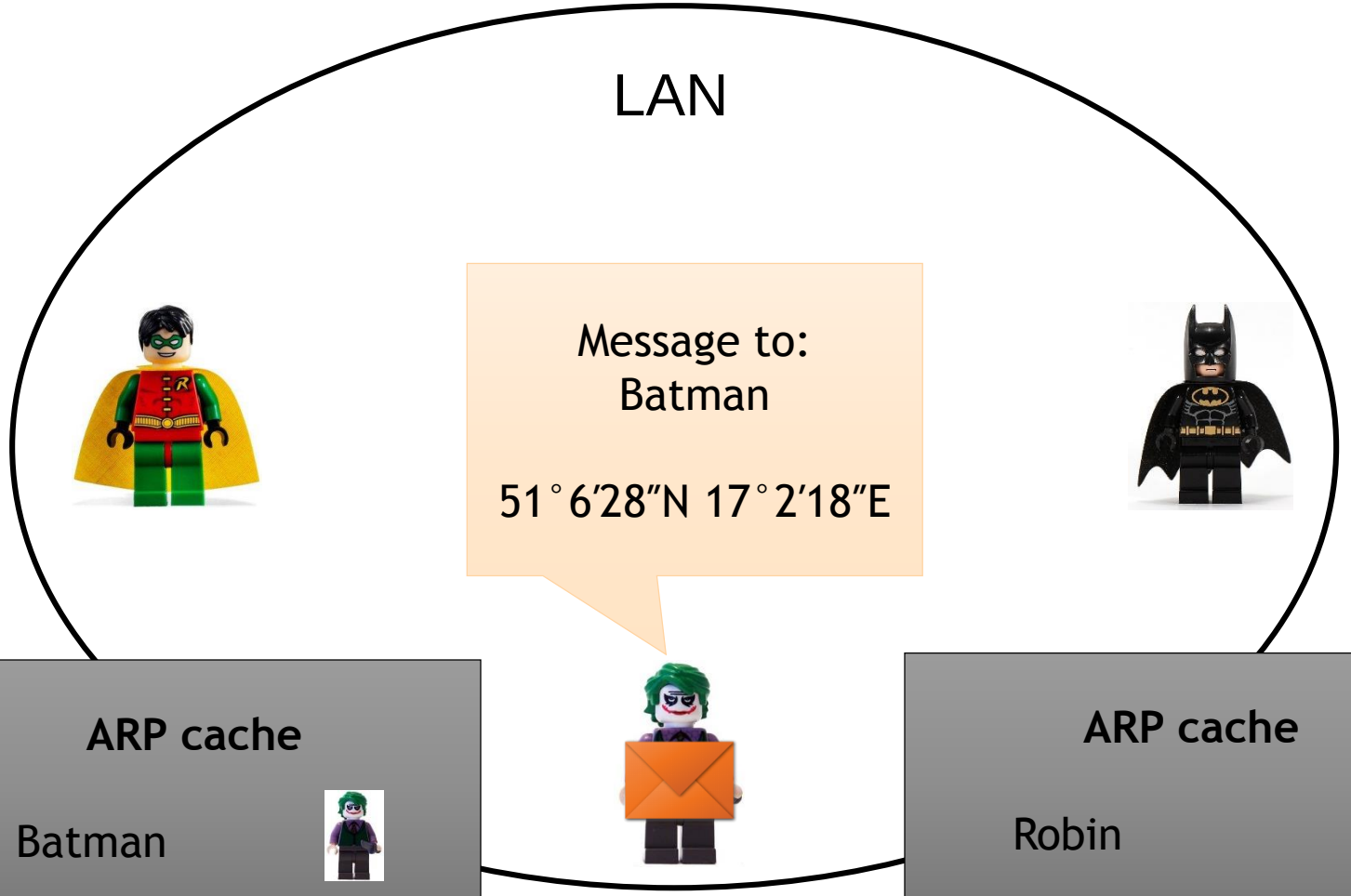
ARP Spoofing – Man in the middle



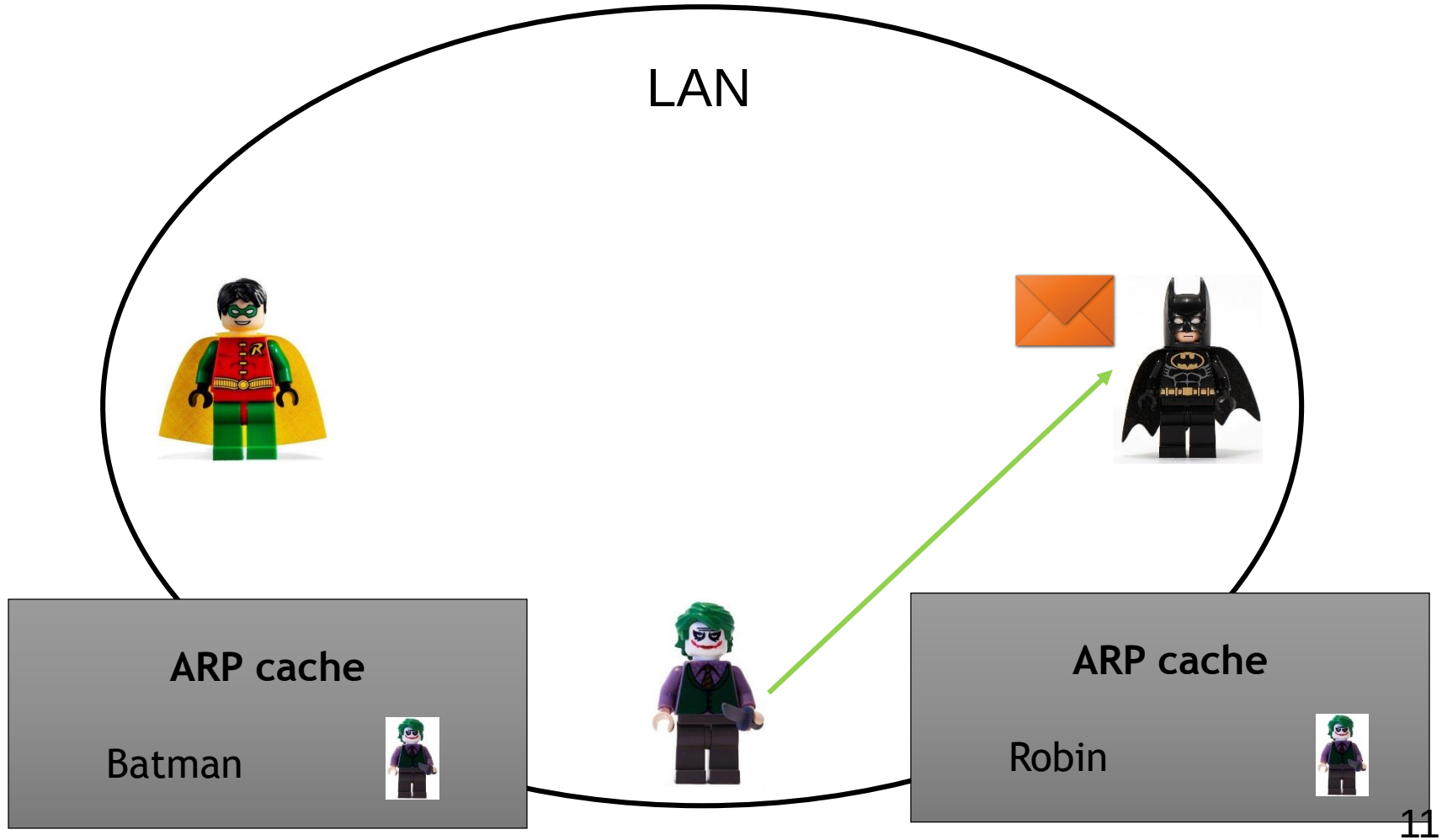
ARP Spoofing – Man in the middle



ARP Spoofing – Man in the middle



ARP Spoofing – Man in the middle

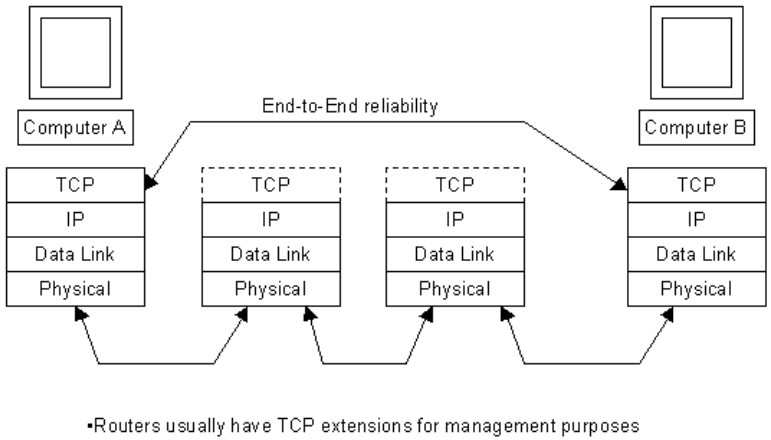


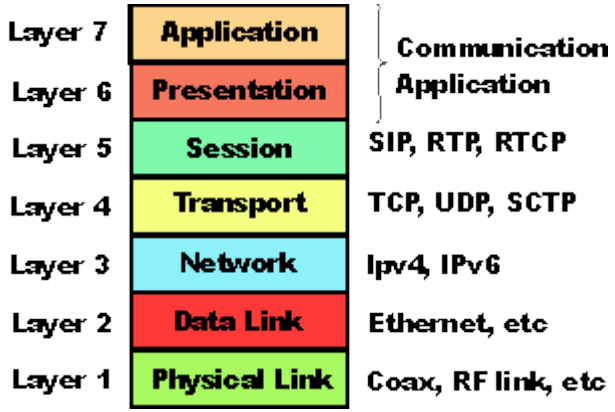
ARP Spoofing - Defenses

- Use cryptographic network protocols
- Static ARP entries
- OS security
- ARP spoofing detection software

Network Protocols flaws

- TCP/IP - widely used protocol (~UDP)

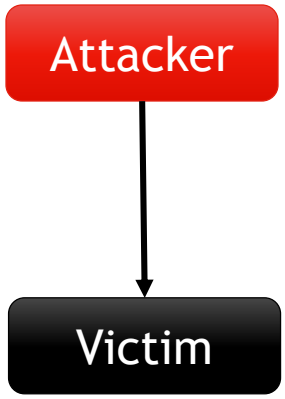




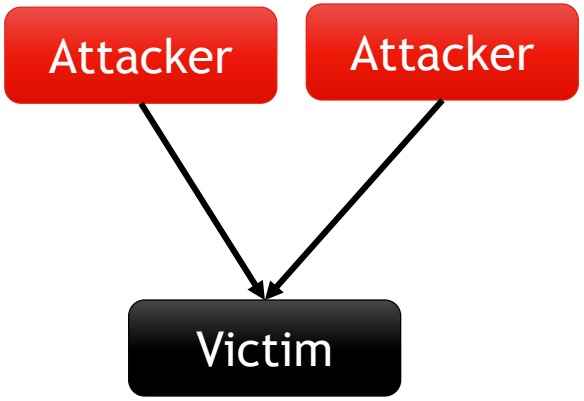
- Vulnerable to sniffing
  - Plaintext Authentication
    - TELNET, FTP, POP, IMAP, HTTP Basic Authentication
- Spoofing (i.e. IP address, email)

Network Protocols flaws

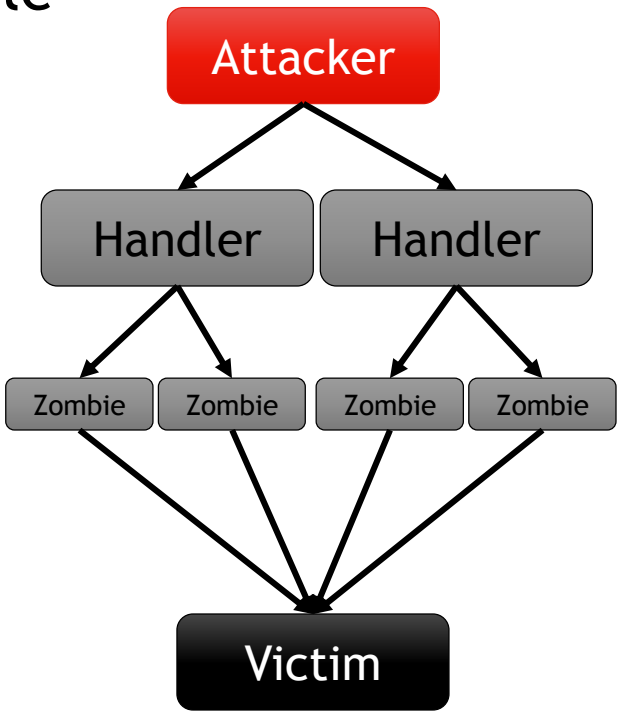
- DoS/DDoS
  - Objective: make a service unusable
  - Consume host resources
  - Consume bandwidth



DoS



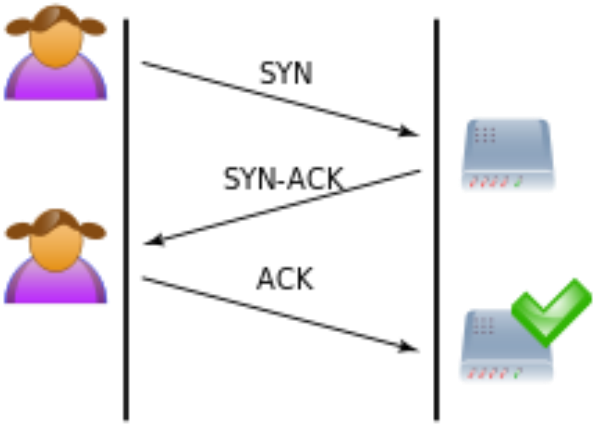
Coordinated DoS

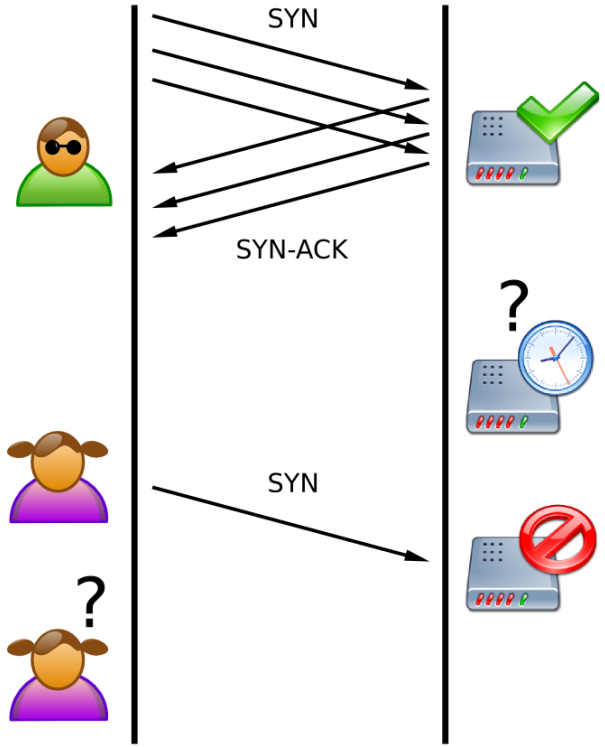


DDoS

Network Protocols flaws

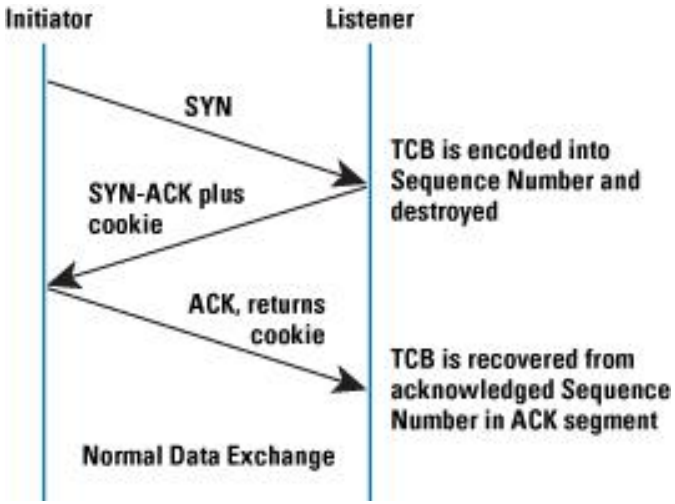
- DDoS - TCP SYN Flood





Network Protocols flaws

- DDoS - TCP SYN Flood – Defense
  - net.ipv4.tcp_syncookies = 1
  - Firewall rules



Connection Establishment with SYN Cookies

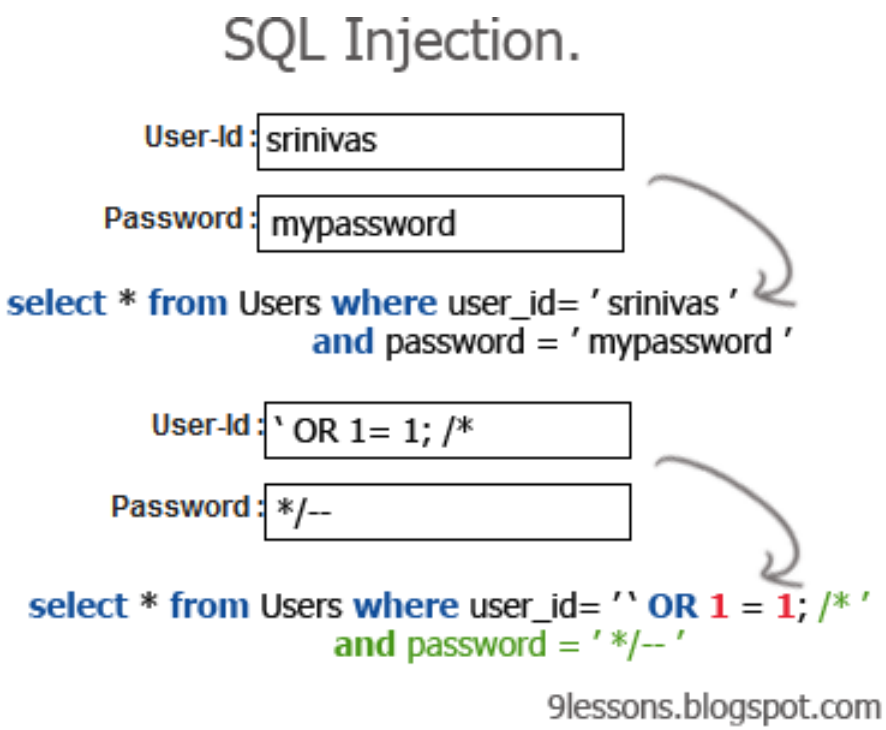
(Web) Application vulnerabilities

- Remote code execution
- Cross Site Scripting (XSS)
- SQL Inject

- Google hacking (link)
  - intitle:FRITZ!Box inurl:login.lua
  - inurl:.php? intext:CHARACTER_SETS,COLLATIONS, ?intitle:phpmyadmin

Application vulnerabilities

- SQL Inject



Application vulnerabilities

- SQL Inject

DEMO

People

- Phishing
- Not running the latest updates
- Pirating software (infected software)
- Operating system (i.e. Windows)

People often represent the weakest link in the security chain and are chronically responsible for the failure of security systems.

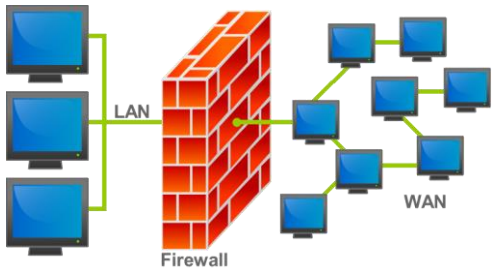
Bruce Schneier, Secrets and Lies 2000

People

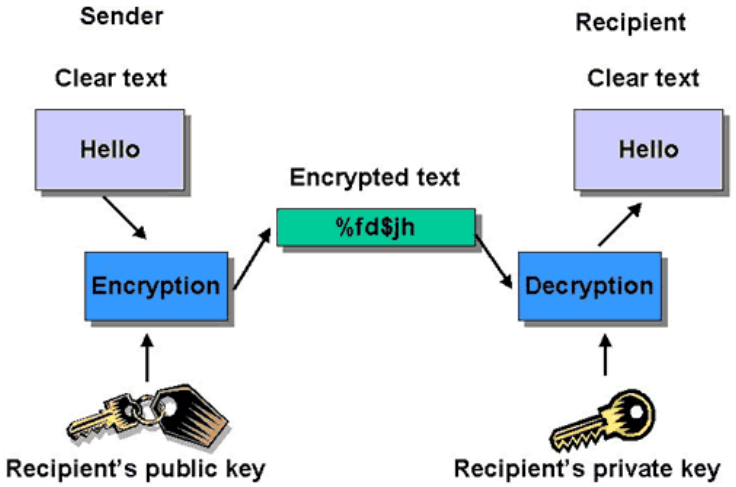
- Phishing
  - Mail Spoofing
  - Wi-Fi phishing
- Pharming Attack
  - DNS Cache Poisoning Attack Scenario
  - Hosts File Modification

Defense

- Firewalls
  - inspects traffic through it
  - Packet Filter
    - Allow/Deny



- Encryption
  - VPN
  - SSH tunneling



Summary

- **Don’t** accept without reading
- **Be cautious** when opening an email attachments
- **Keep** your operating system and its programs **current**
- Make sure you are downloading software from a **reliable source**

Wrocław University of Technology

Network Attack and Defense

Piotr Giedziun