SECURITY IN COMPUTING, FIFTH EDITION

Chapter 6: Networks

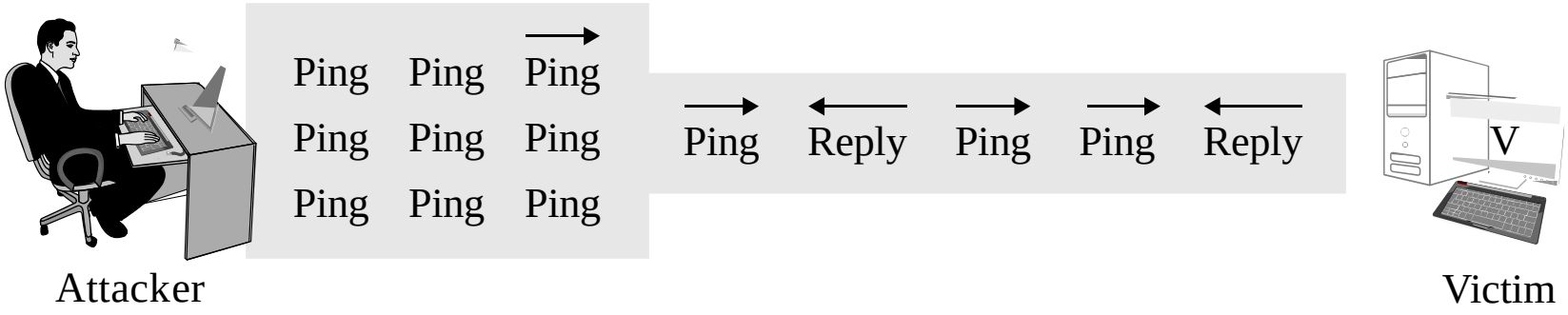
Objectives for Chapter 6

- Networking basics
- Network threats and vulnerabilities
- WiFi security
- Denial-of-service attacks
- Network encryption concepts and tools
- Types of firewalls and what they do
- Intrusion detection and prevention systems
- Security information and event management tools

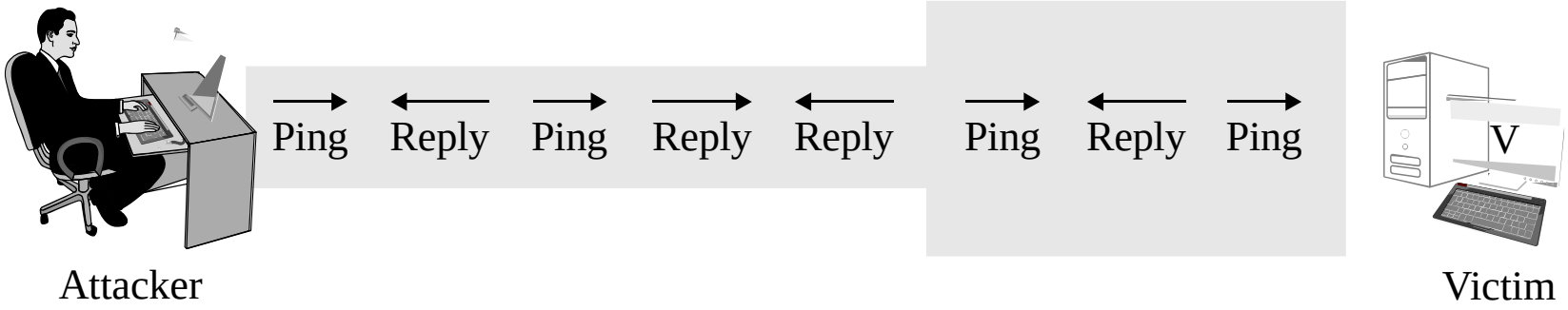
Denial of Service (DoS)

- DoS attacks are attempts to defeat a system's availability
- Volumetric attacks
- Application-based attacks
- Disabled communications
- Hardware or software failure

DoS Attack: Ping Flood

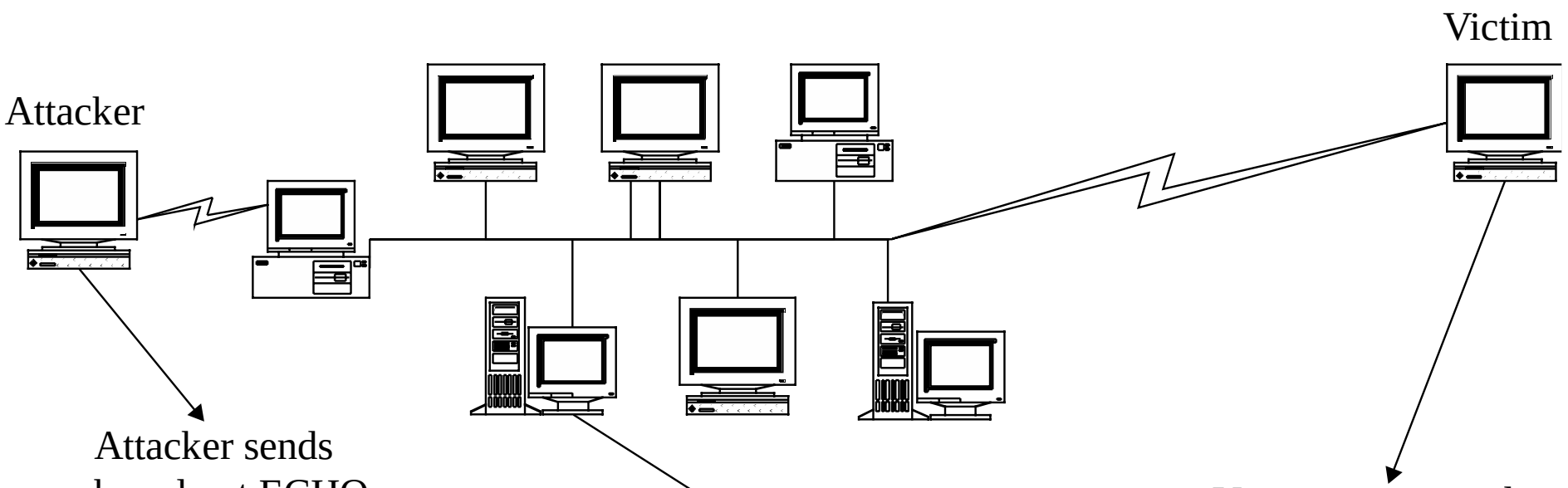


(a) Attacker has greater bandwidth



(b) Victim has greater bandwidth

DoS Attack: Smurf Attack



DoS Attack: Echo-Chargen

Victim A

Victim B

Chargen packet with echo bit on →

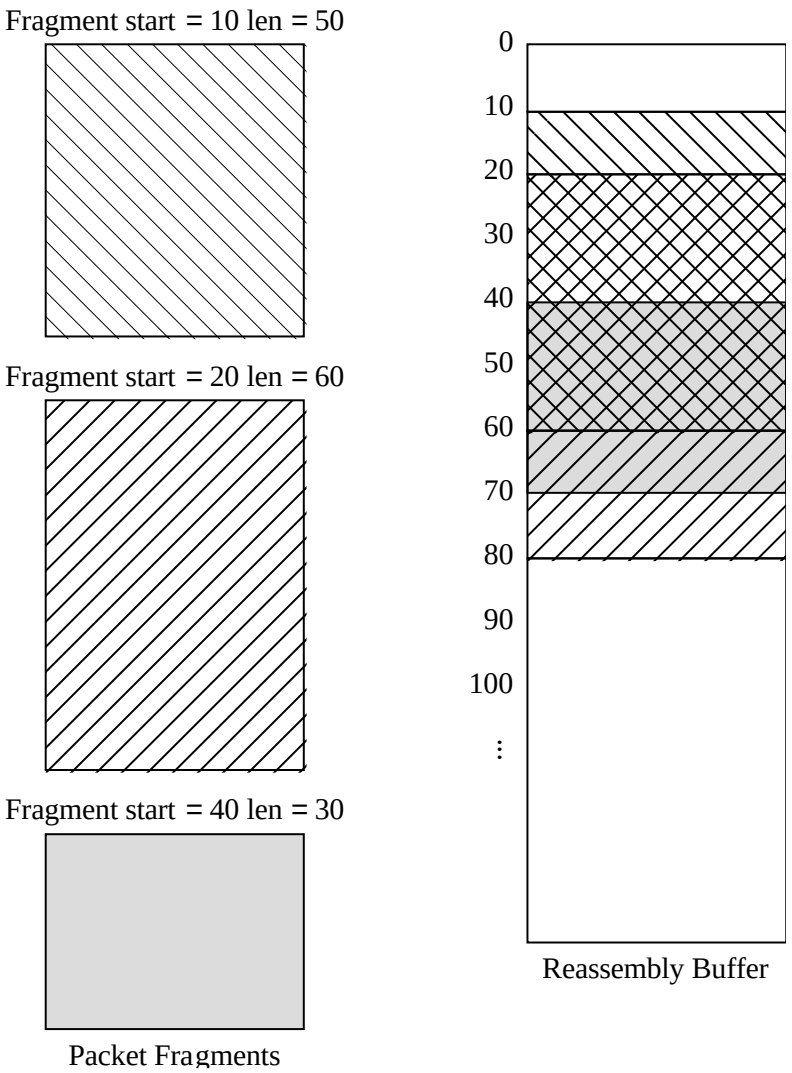
← Echoing what you just sent me

Chargen another packet with echo bit on →

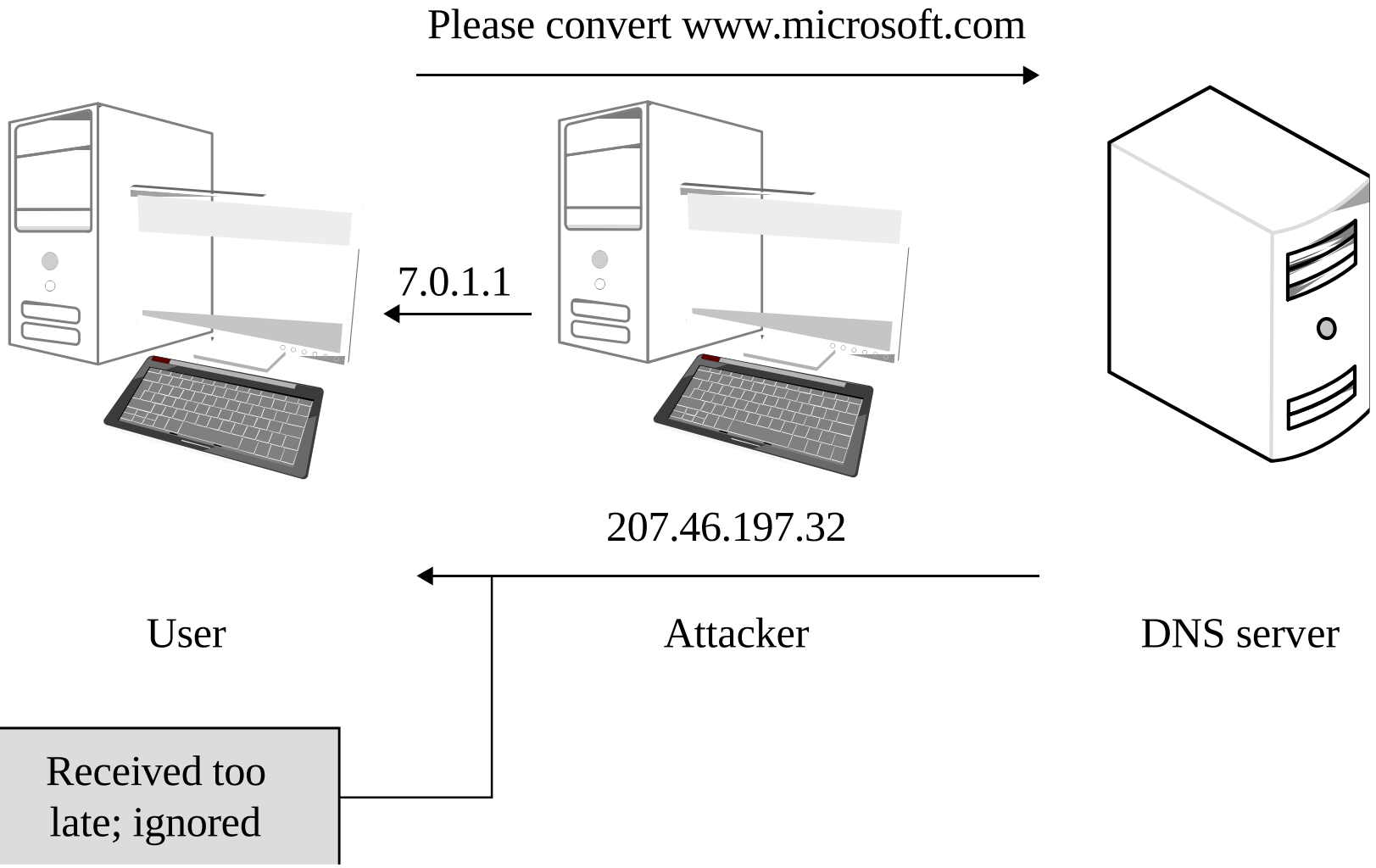
← Echoing that again

Chargen another packet with echo bit on →

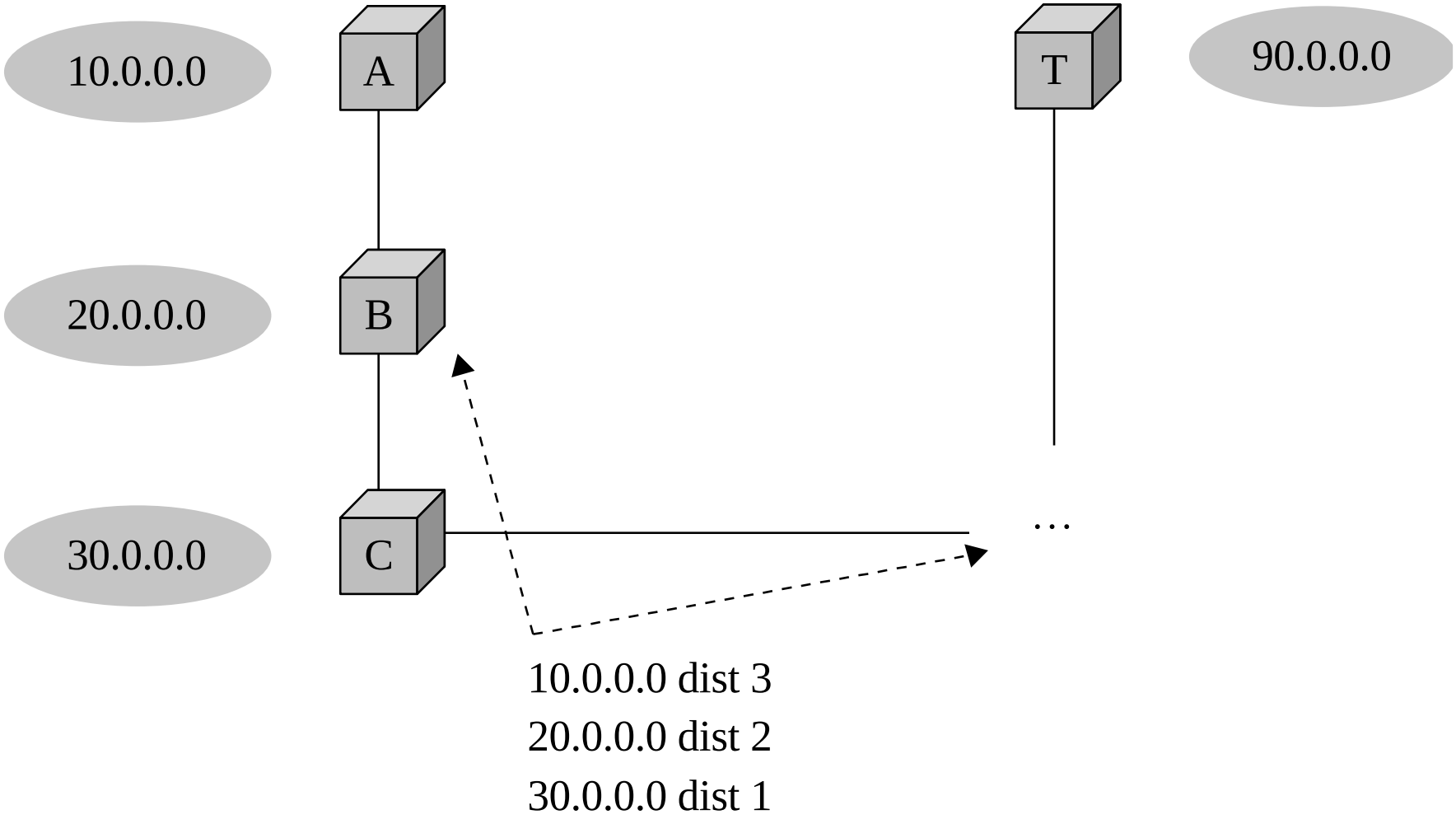
DoS Attack: Teardrop Attack



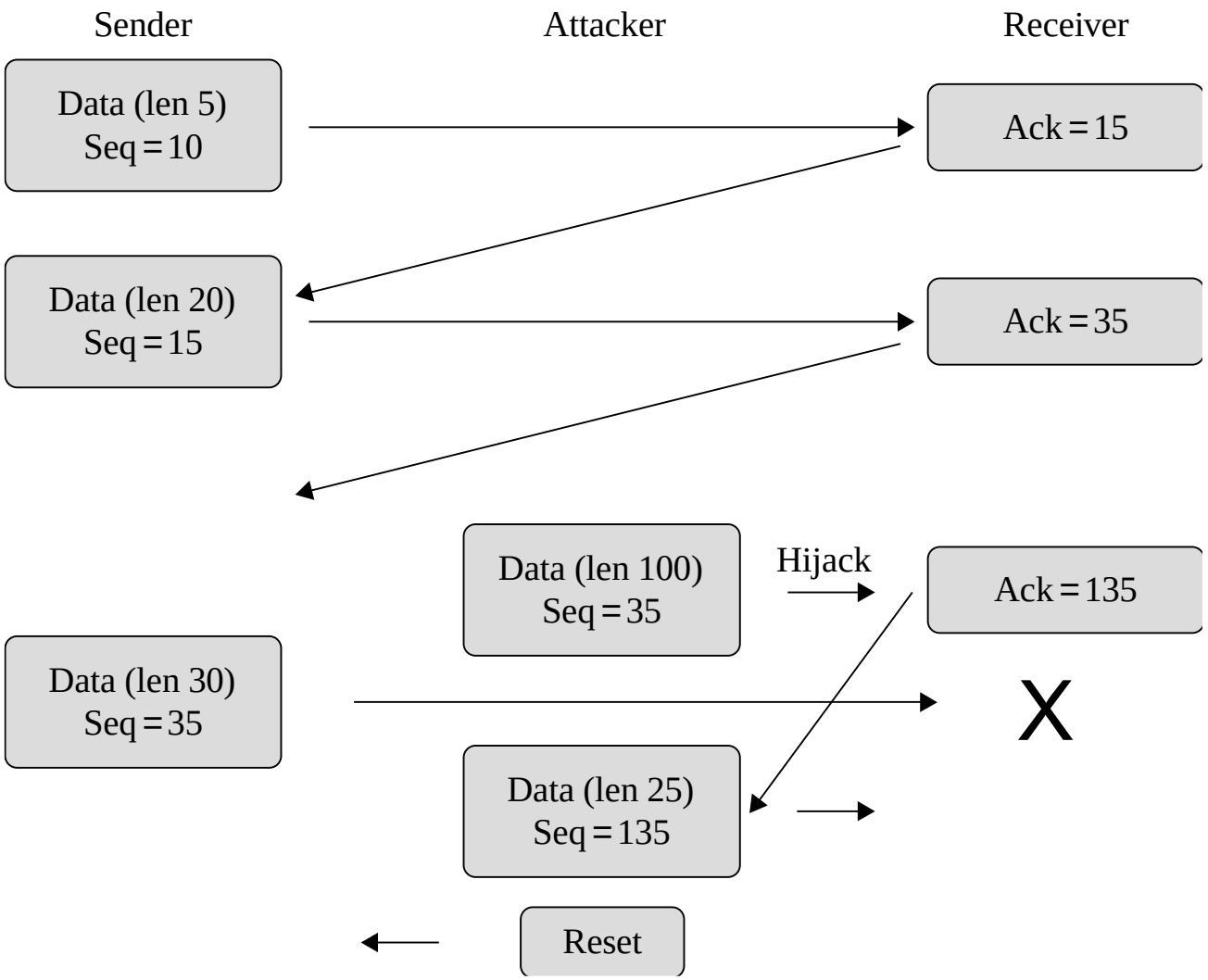
DoS Attack: DNS Spoofing



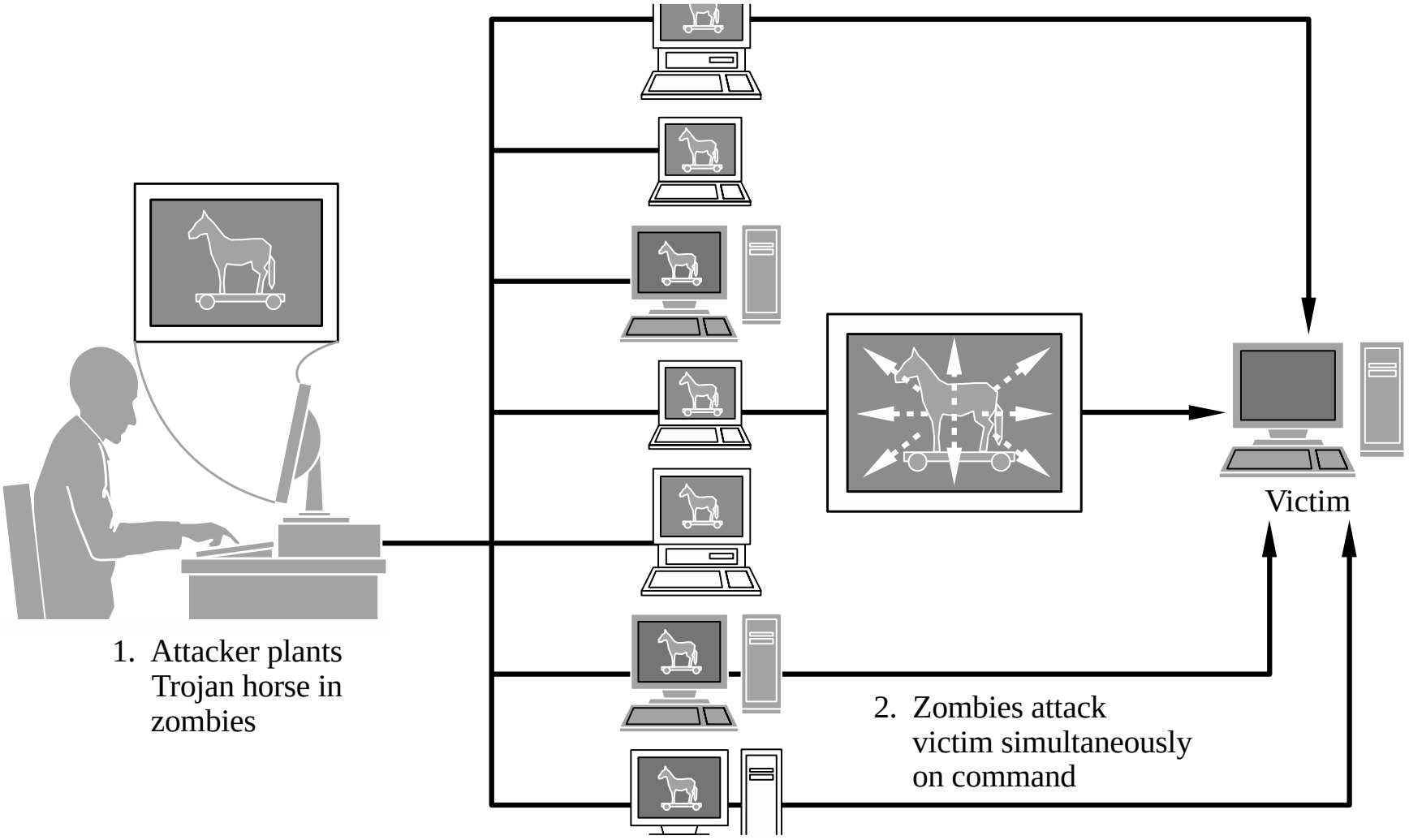
DoS Attack: Rerouting Routing



DoS Attack: Session Hijacking



Distributed Denial of Service (DDoS)



Summary

- Networks are threatened by attacks aimed at interception, modification, fabrication, and interruption
- WPA2 has many critical security advantages over WEP
- DoS attacks come in many flavors, but malicious ones are usually either volumetric in nature or exploit a bug
- Network encryption can be achieved using specialized tools—some for link encryption and some for end-to-end—such as VPNs, SSH, and the SSL/TLS protocols
- A wide variety of firewall types exist, ranging from very basic IP-based functionality to complex application-layer logic, and both on networks and hosts
- There are many flavors of IDS, each of which detects different kinds of attacks in very different parts of the network