SECURITY IN COMPUTING, FIFTH EDITION

Chapter 6: Networks

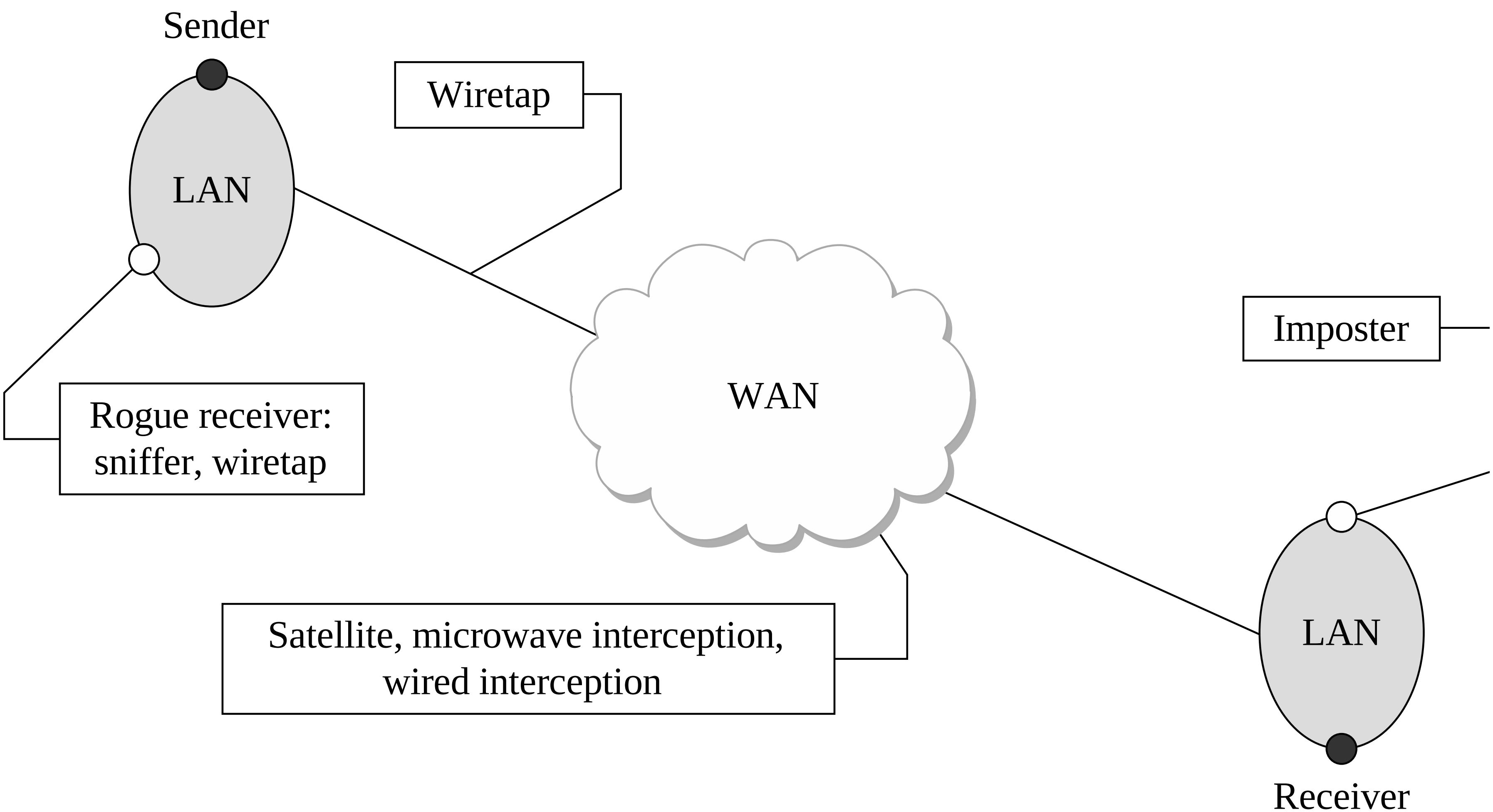
Objectives for Chapter 6

- 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

Network Transmission Media

- Cable
- Optical fiber
- Microwave
- WiFi
- Satellite communication

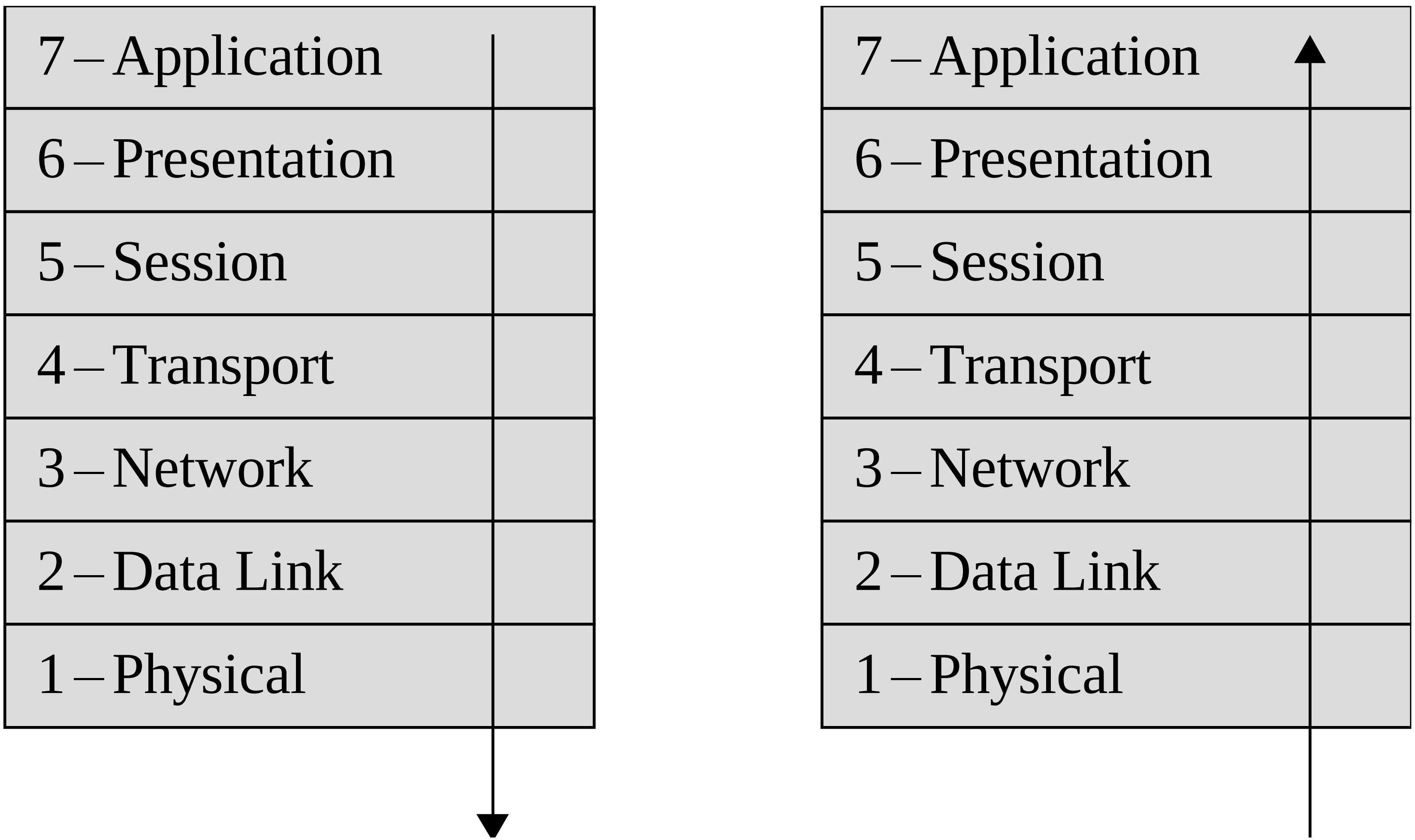
Communication Media Vulnerability



Communication Media Pros/Cons

Medium	Strengths	Weaknesses
Wire	• Widely used • Inexpensive to buy, install, maintain	• Susceptible to emanation • Susceptible to physical wiretapping
Optical fiber	• Immune to emanation • Difficult to wiretap	• Potentially exposed at connection points
Microwave	• Strong signal, not seriously affected by weather	• Exposed to interception along path of transmission • Requires line of sight location • Signal must be repeated approximately every 30 miles (50 kilometers)
Wireless (radio, WiFi)	• Widely available • Built into many computers	• Signal degrades over distance; suitable for short range • Signal interceptable in circular pattern around transmitter
Satellite	• Strong, fast signal	• Delay due to distance signal travels up and down • Signal exposed over wide area at receiving end

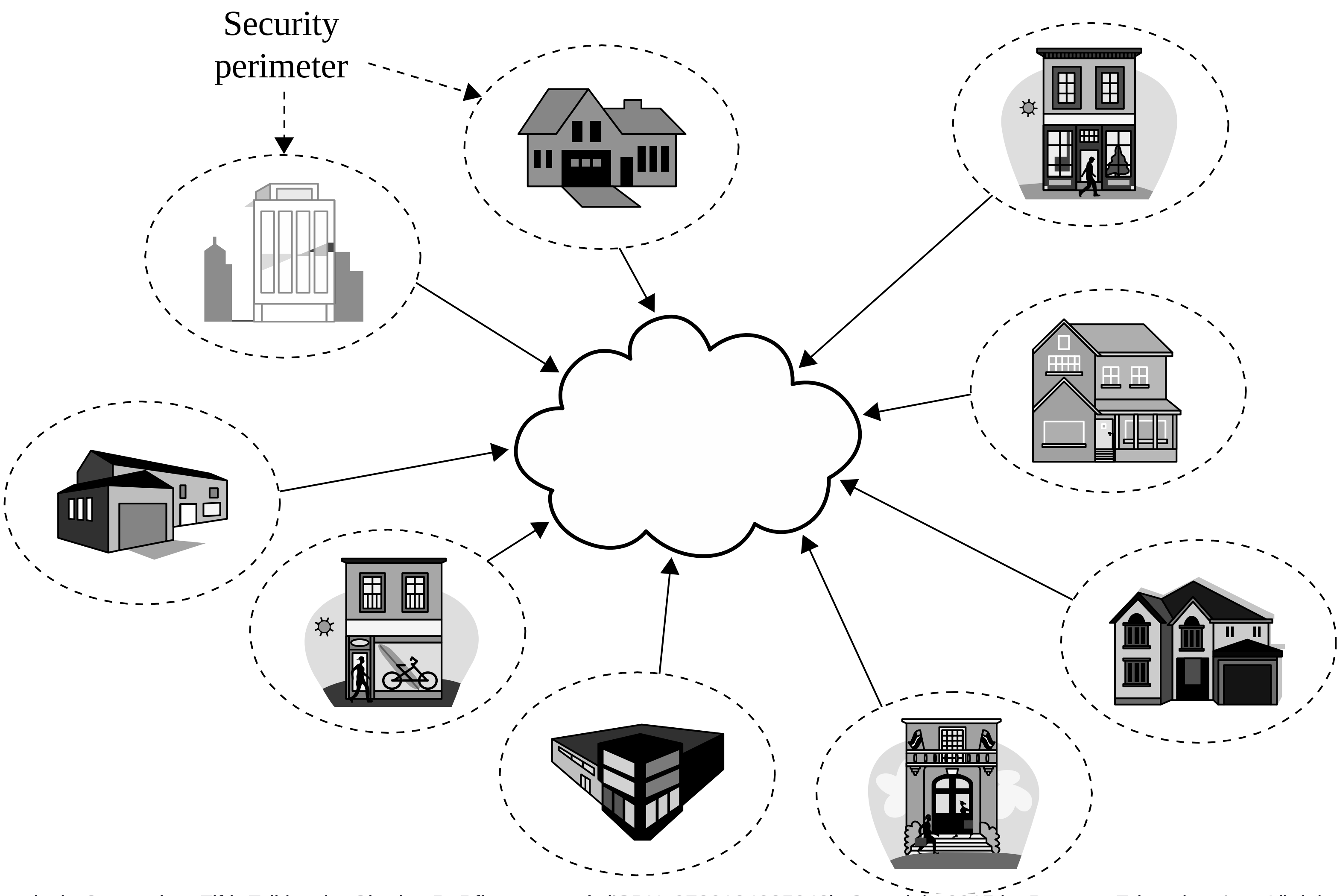
The OSI Model



Threats to Network Communications

- *Interception*, or unauthorized viewing
- *Modification*, or unauthorized change
- *Fabrication*, or unauthorized creation
- *Interruption*, or preventing authorized access

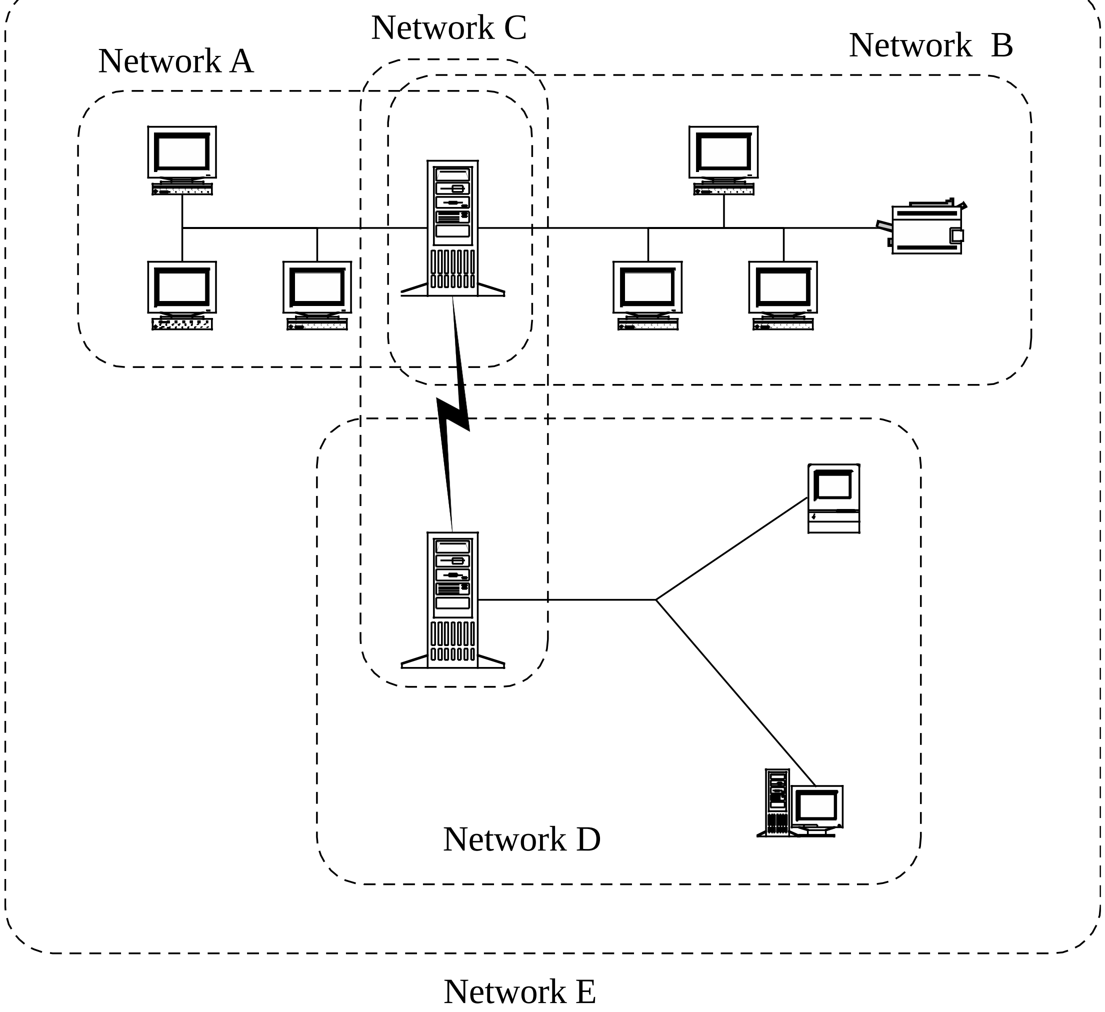
Security Perimeters



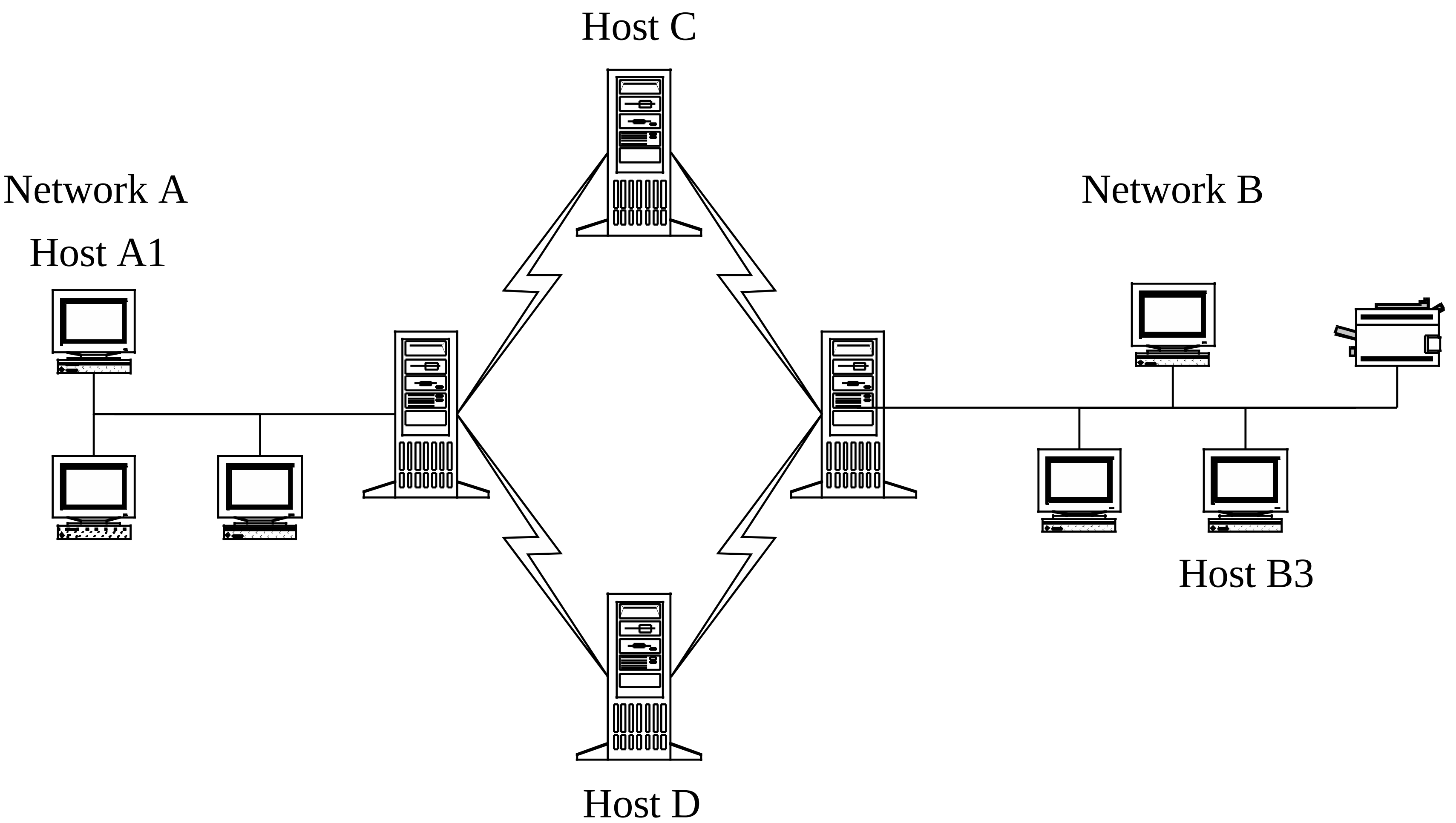
What Makes a Network Vulnerable to Interception?

- Anonymity
  - An attacker can attempt many attacks, anonymously, from thousands of miles away
- Many points of attack
  - Large networks mean many points of potential entry
- Sharing
  - Networked systems open up potential access to more users than do single computers
- System complexity
  - One system is very complex and hard to protect; networks of many different systems, with disparate OSs, vulnerabilities, and purposes are that much more complex
- Unknown perimeter
  - Networks, especially large ones, change all the time, so it can be hard to tell which systems belong and are behaving, and impossible to tell which systems bridge networks
- Unknown path
  - There may be many paths, including untrustworthy ones, from one host to another

Unknown Perimeter



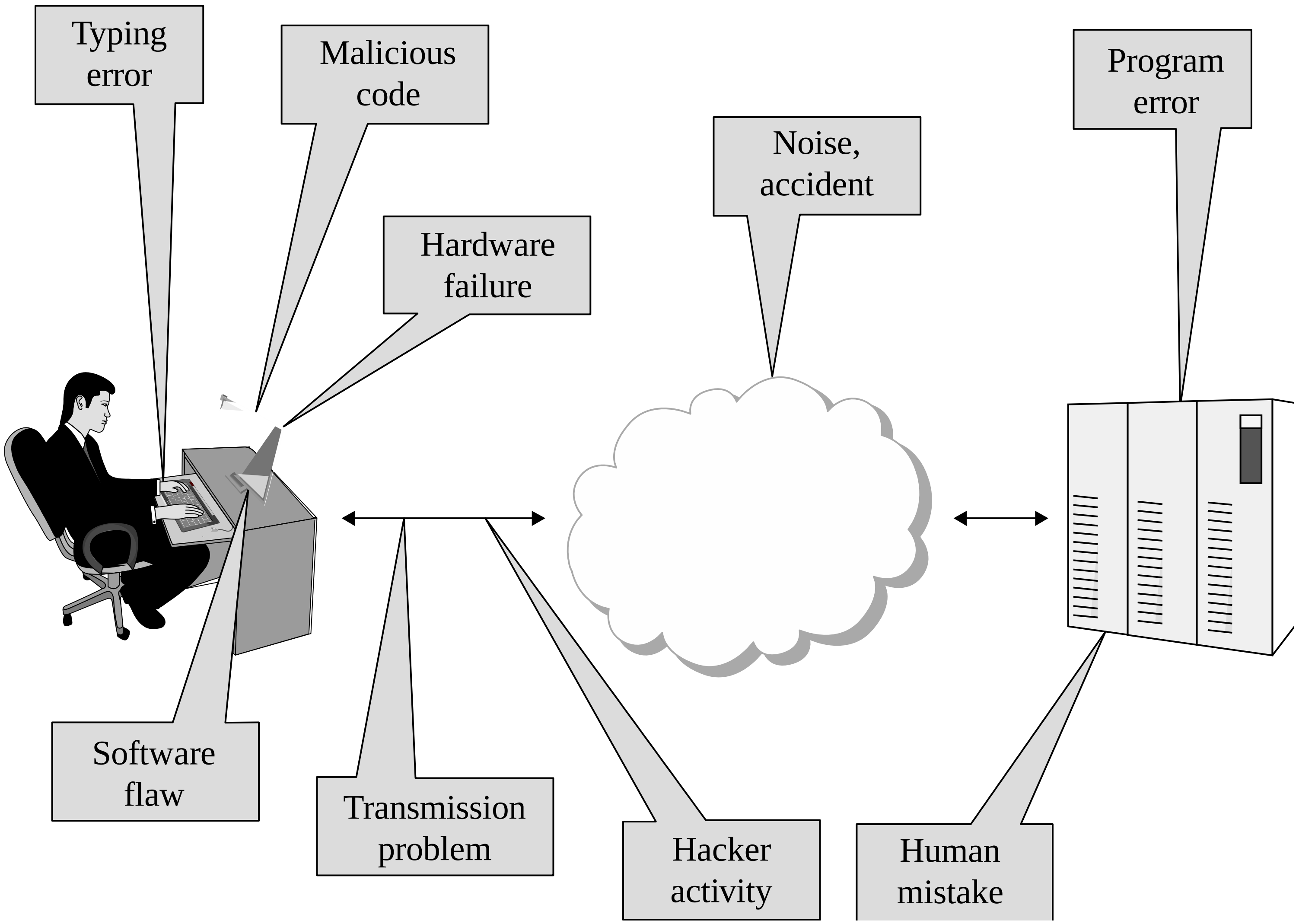
Unknown Path



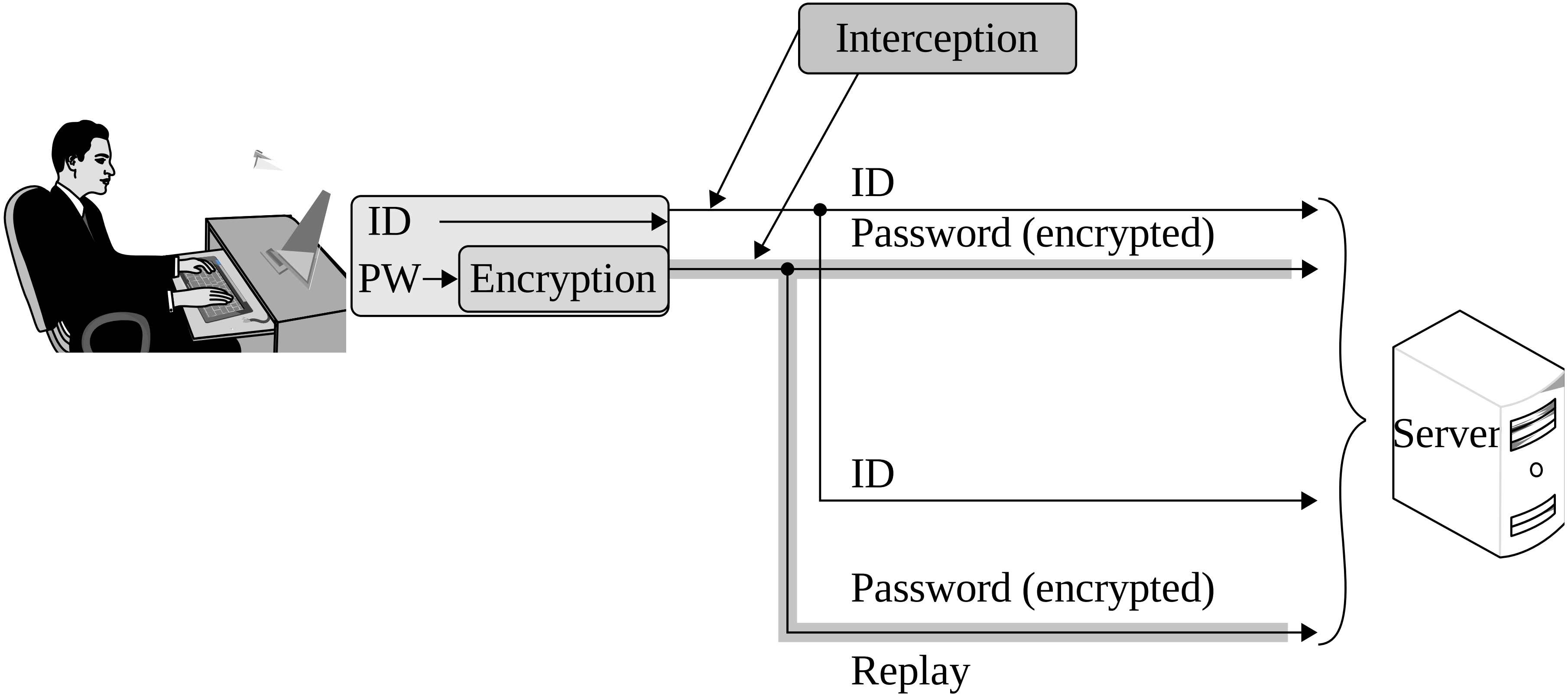
Modification and Fabrication

- Data corruption
  - May be intentional or unintentional, malicious or nonmalicious, directed or random
- Sequencing
  - Permuting the order of data, such as packets arriving in sequence
- Substitution
  - Replacement of one piece of a data stream with another
- Insertion
  - A form of substitution in which data values are inserted into a stream
- Replay
  - Legitimate data are intercepted and reused

Sources of Data Corruption



Simple Replay Attack



Interruption: Loss of Service

- Routing
  - Internet routing protocols are complicated, and one misconfiguration can poison the data of many routers
- Excessive demand
  - Network capacity is finite and can be exhausted; an attacker can generate enough demand to overwhelm a critical part of a network
- Component failure
  - Component failures tend to be sporadic and unpredictable, and will cause loss of service if not planned for

Port Scanning

```
Nmap scan report
192.168.1.1 / somehost.com (online) ping results
address: 192.168.1.1 (ipv4)
hostnames: somehost.com (user)
The 83 ports scanned but not shown below are in state: closed
Port        State     Service Reason      Product  Version  Extra info
21    tcp   open      ftp     syn-ack     ProFTPD  1.3.1
22    tcp   filtered  ssh     no-response
25    tcp   filtered  smtp    no-response
80    tcp   open      http    syn-ack     Apache   2.2.3    (CentOS)
106   tcp   open      pop3pw  syn-ack     poppassd
110   tcp   open      pop3    syn-ack     Courier pop3d
111   tcp   filtered  rpcbind no-response
113   tcp   filtered  auth    no-response
143   tcp   open       imap    syn-ack     Courier Imapd       released
2004
443   tcp   open      http    syn-ack     Apache  2.2.3      (CentOS)
465   tcp   open      unknown syn-ack
646   tcp   filtered  ldp     no-response
993   tcp   open      imap    syn-ack     Courier Imapd      released
2004
995   tcp   open              syn-ack
2049 tcp   filtered  nfs     no-response
3306 tcp   open      mysql   syn-ack     MySQL   5.0.45
8443 tcp   open      unknown syn-ack
34 sec. scanned
1 host(s) scanned
1 host(s) online
0 host(s) offline
```

Vulnerabilities in Wireless Networks

- Confidentiality
- Integrity
- Availability
- Unauthorized WiFi access
- WiFi protocol weaknesses
  - Picking up the beacon
  - SSID in all frames
  - Association issues

Failed Countermeasure: WEP

- Wired equivalent privacy, or WEP, was designed at the same time as the original 802.11 WiFi standards as the mechanism for securing those communications
- Weaknesses in WEP were first identified in 2001, four years after release
- More weaknesses were discovered over the course of years, until any WEP-encrypted communication could be cracked in a matter of minutes

How WEP Works

- Client and access point (AP) have a pre-shared key
- AP sends a random number to the client, which the client then encrypts using the key and returns to the AP
- The AP decrypts the number using the key and checks that it’s the same number to authenticate the client
- Once the client is authenticated, the AP and client communicate using messages encrypted with the key

WEP Weaknesses

- Weak encryption key
  - WEP allows to be either 64- or 128-bit, but 24 of those bits are reserved for initialization vectors (IV), thus reducing effective key size to 40 or 140 bits
  - Keys were either alphanumeric or hex phrases that users typed in and were therefore vulnerable to dictionary attacks
- Static key
  - Since the key was just a value the user typed in at the client and AP, and since users rarely changed those keys, one key would be used for many months of communications
- Weak encryption process
  - A 40-bit key can be brute forced easily. Flaws that were eventually discovered in the RC4 encryption algorithm WEP uses made the 104-bit keys easy to crack as well

WEP Weaknesses (cont.)

- Weak encryption algorithm
  - WEP used RC4 in a strange way (always a bad sign), which resulted in a flaw that allowed attackers to decrypt large portions of any WEP communication
- IV collisions
  - There were only 16 million possible values of IV, which, in practice, is not that many to cycle through for cracking. Also, they were not as randomly selected as they should have been, with some values being much more common than others
- Faulty integrity check
  - WEP messages included a checksum to identify transmission errors but did not use one that could address malicious modification
- No authentication
  - Any client that knows the AP's SSID and MAC address is assumed to be legitimate

WPA (WiFi Protected Access)

- WPA was designed in 2003 as a replacement for WEP and was quickly followed in 2004 by WPA2, the algorithm that remains the standard today
- Non-static encryption key
    - WPA uses a hierarchy of keys: New keys are generated for confidentiality and integrity of each session, and the encryption key is automatically changed on each packet
    - This way, the keys that are most important are used in very few places and indirect ways, protecting them from disclosure
- Authentication
    - WPA allows authentication by password, token, or certificate

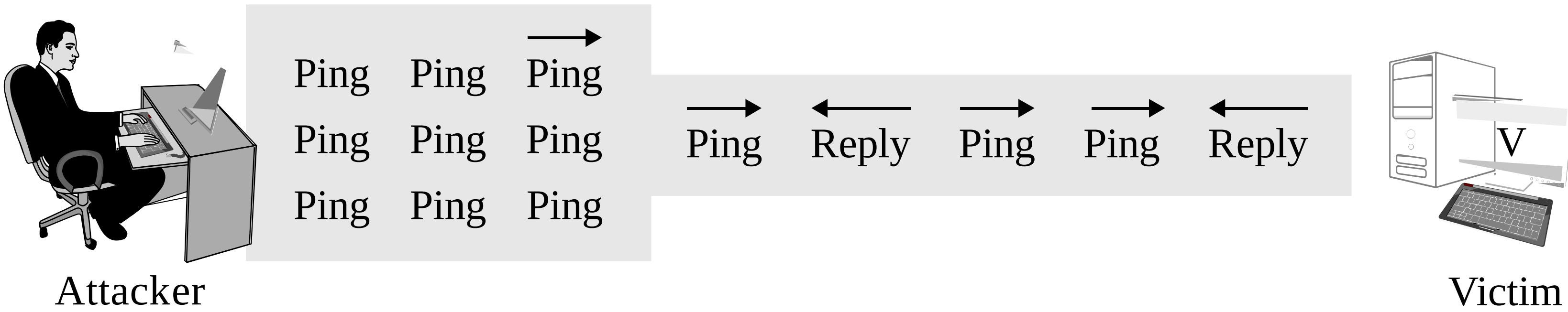
WPA (cont.)

- Strong encryption
  - WPA adds support for AES, a much more reliably strong encryption algorithm
- Integrity protection
  - WPA includes a 64-bit cryptographic integrity check
- Session initiation
  - WPA sessions begin with authentication and a four-way handshake that results in separate keys for encryption and integrity on both ends
- While there are some attacks against WPA, they are either of very limited effectiveness or require weak passwords

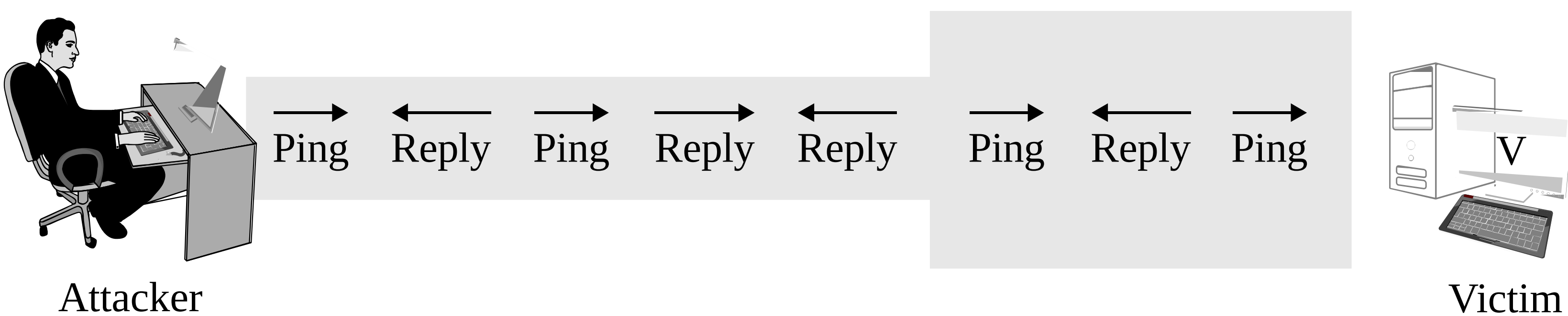
Denial of Service (DoS)

- 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

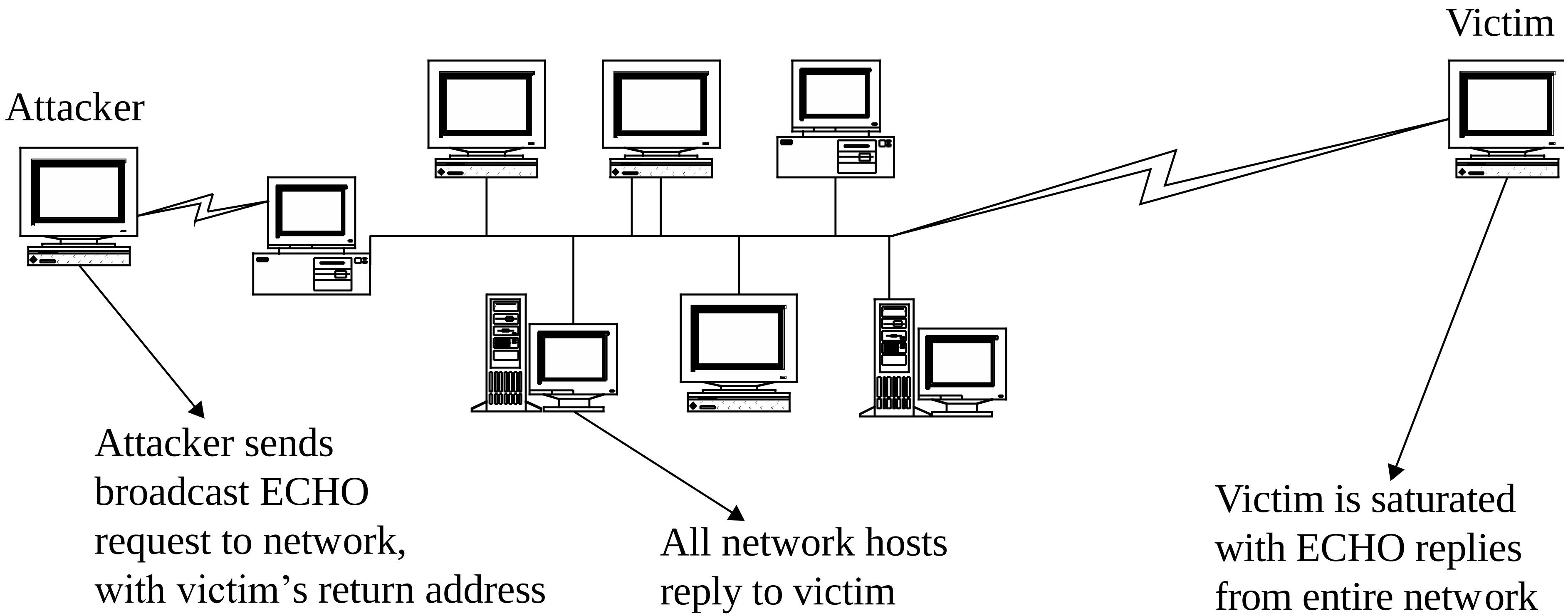


(a) Attacker has greater bandwidth



(b) Victim has greater bandwidth

DoS Attack: Smurf Attack



DoS Attack: Echo-Chargen

Victim A

Victim B

→ Chargen packet with echo bit on

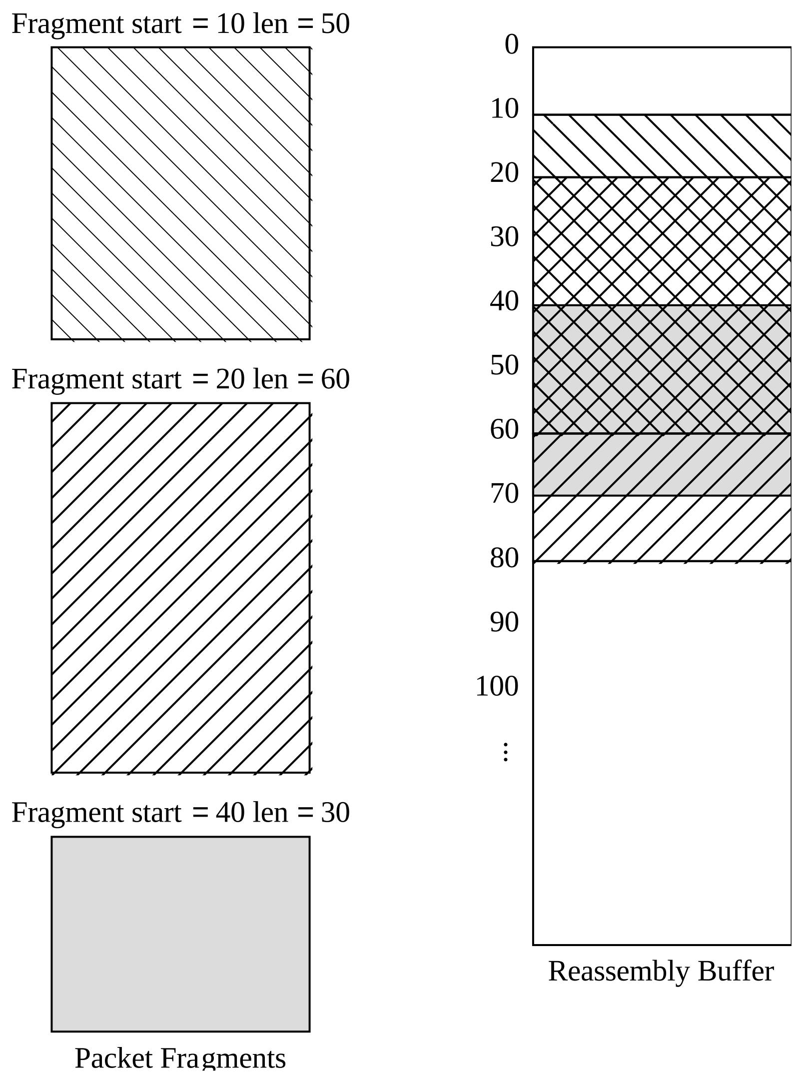
← Echoing what you just sent me

→ Chargen another packet with echo bit on

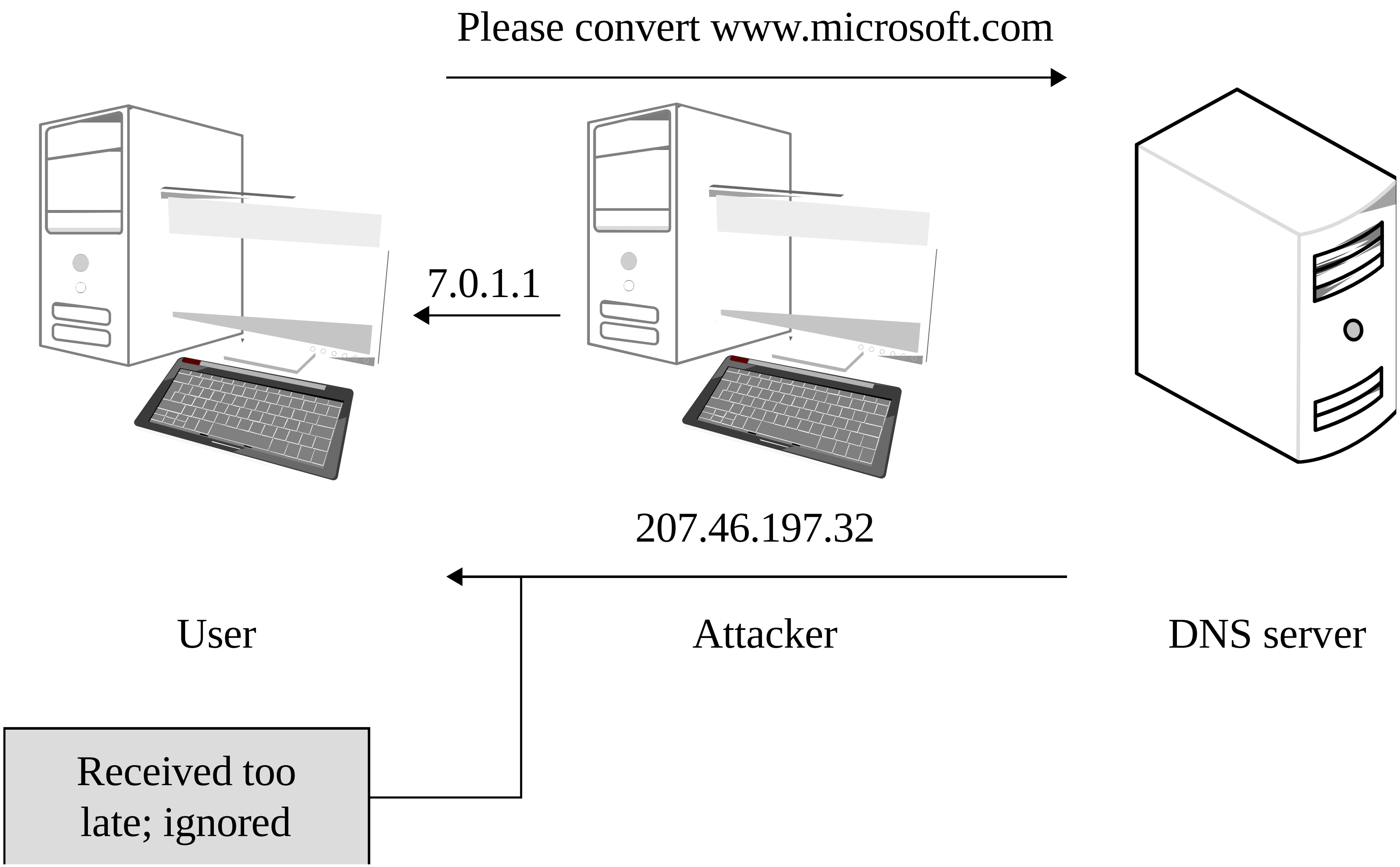
← Echoing that again

→ Chargen another packet with echo bit on

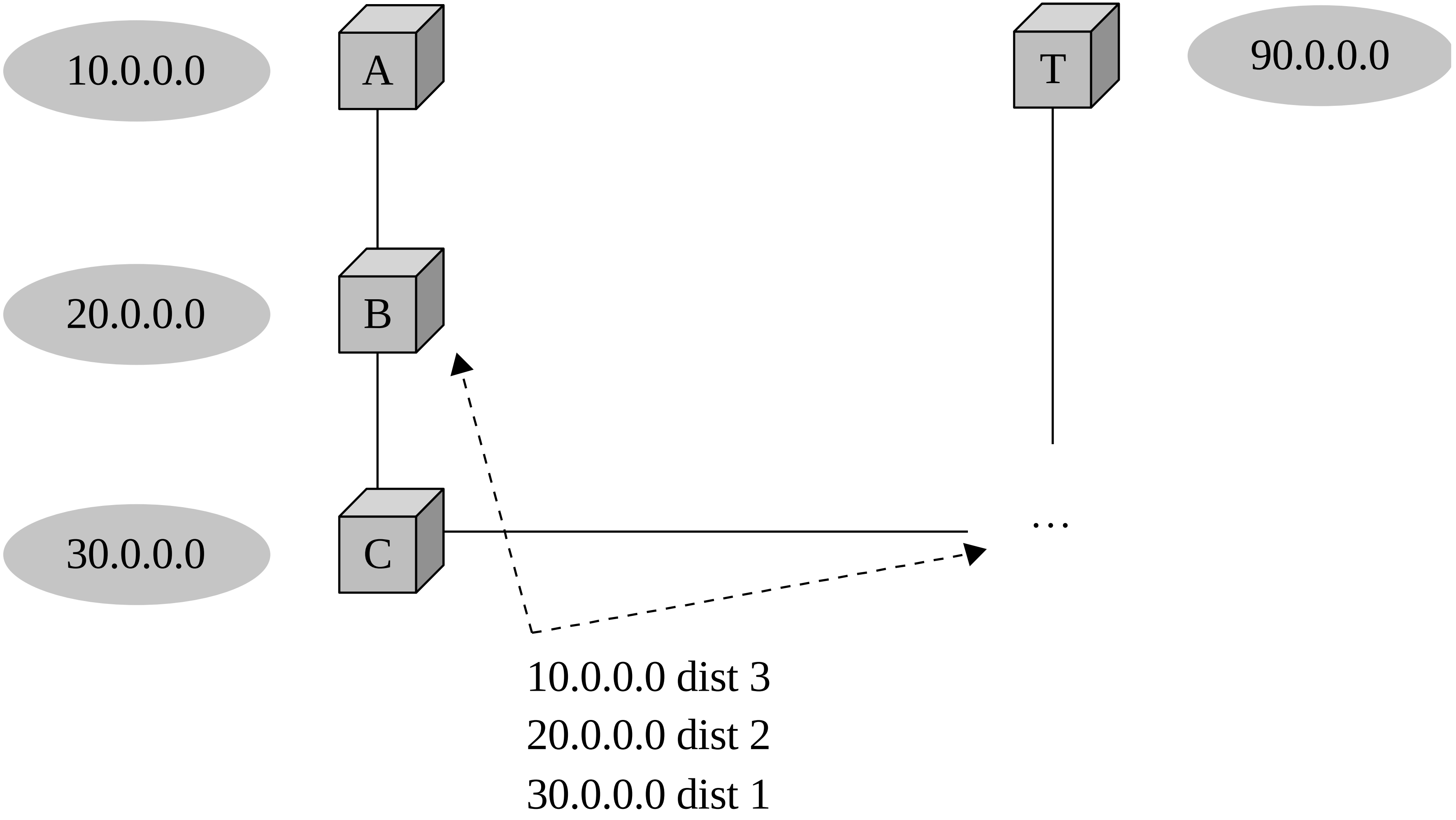
DoS Attack: Teardrop Attack



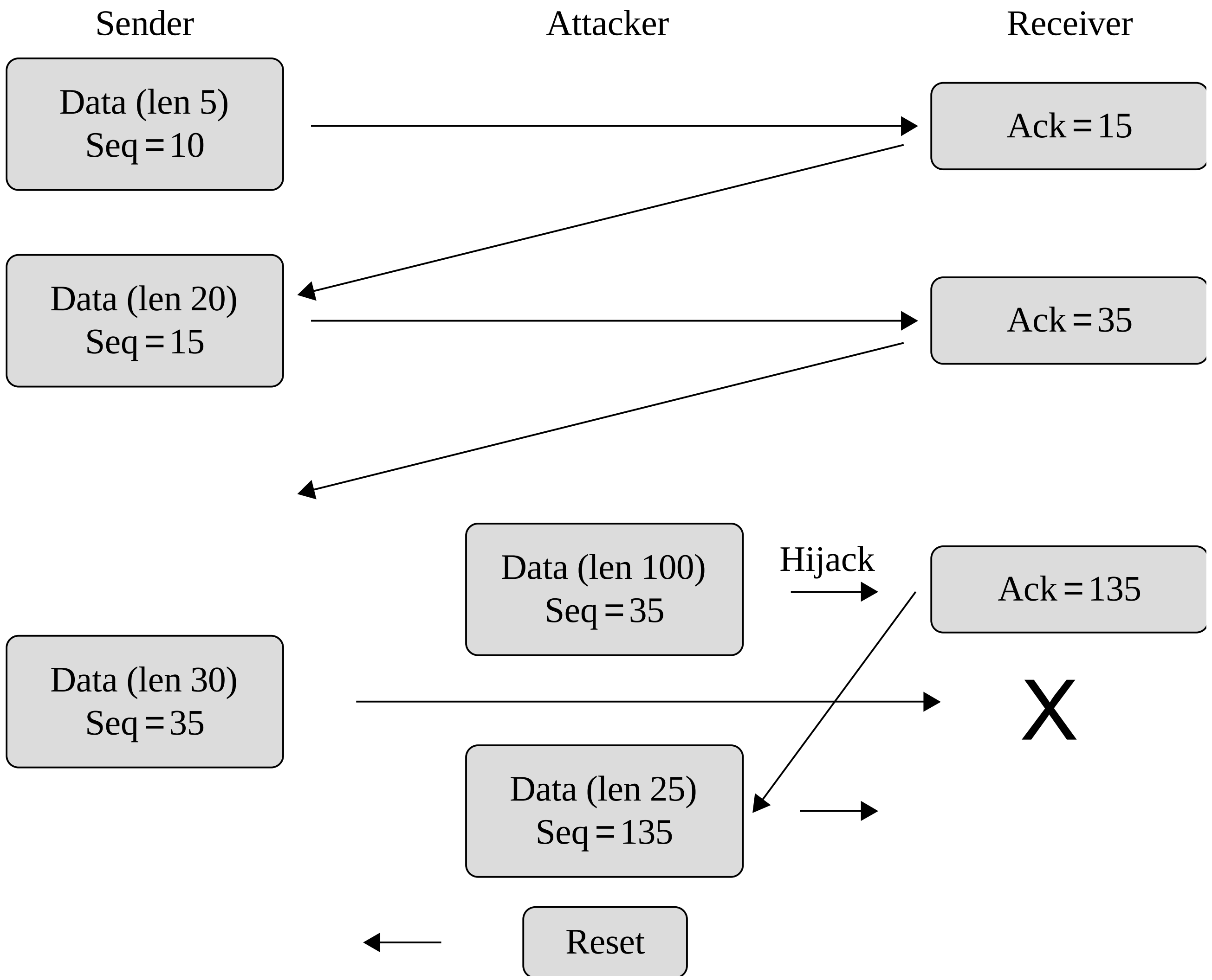
DoS Attack: DNS Spoofing



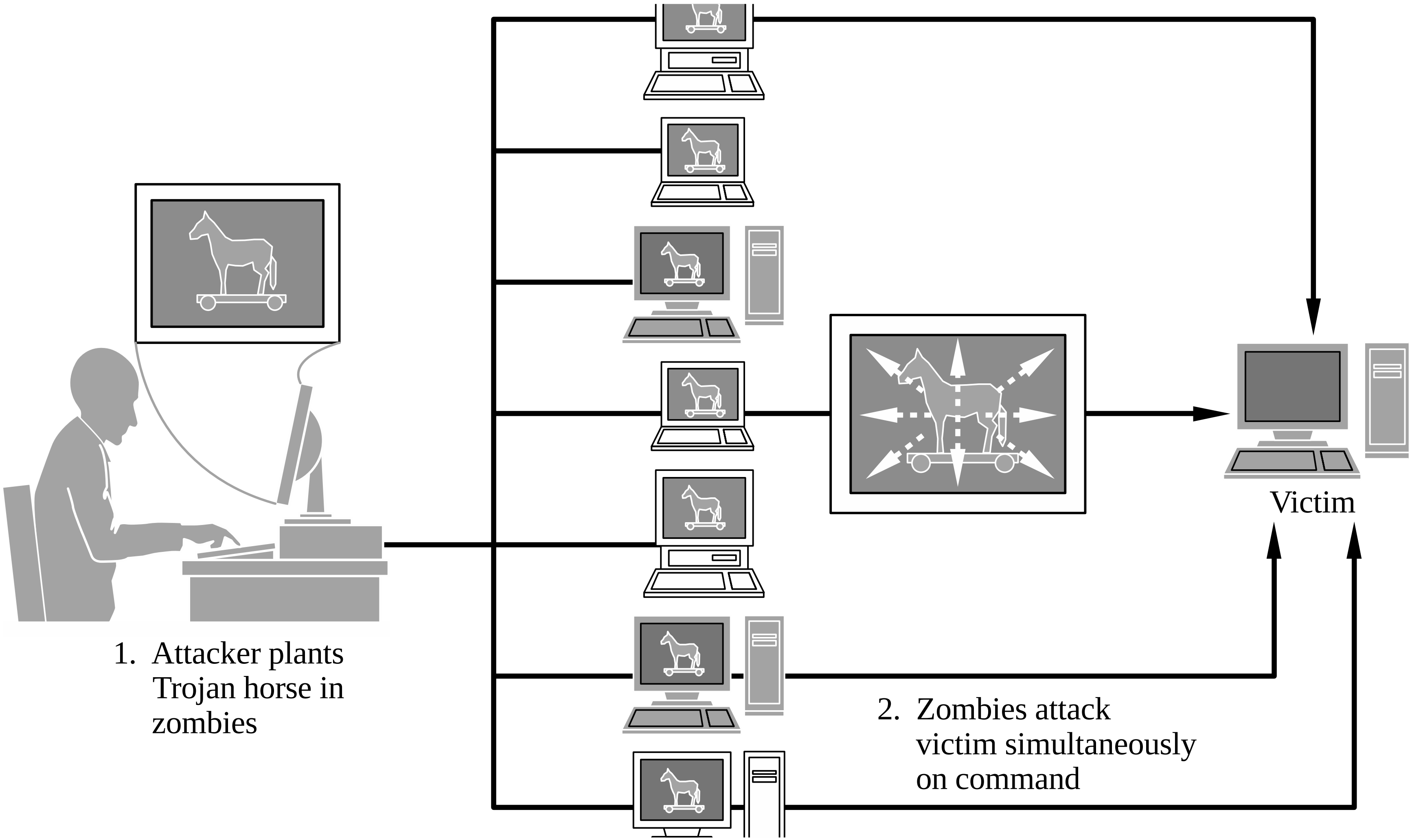
DoS Attack: Rerouting Routing



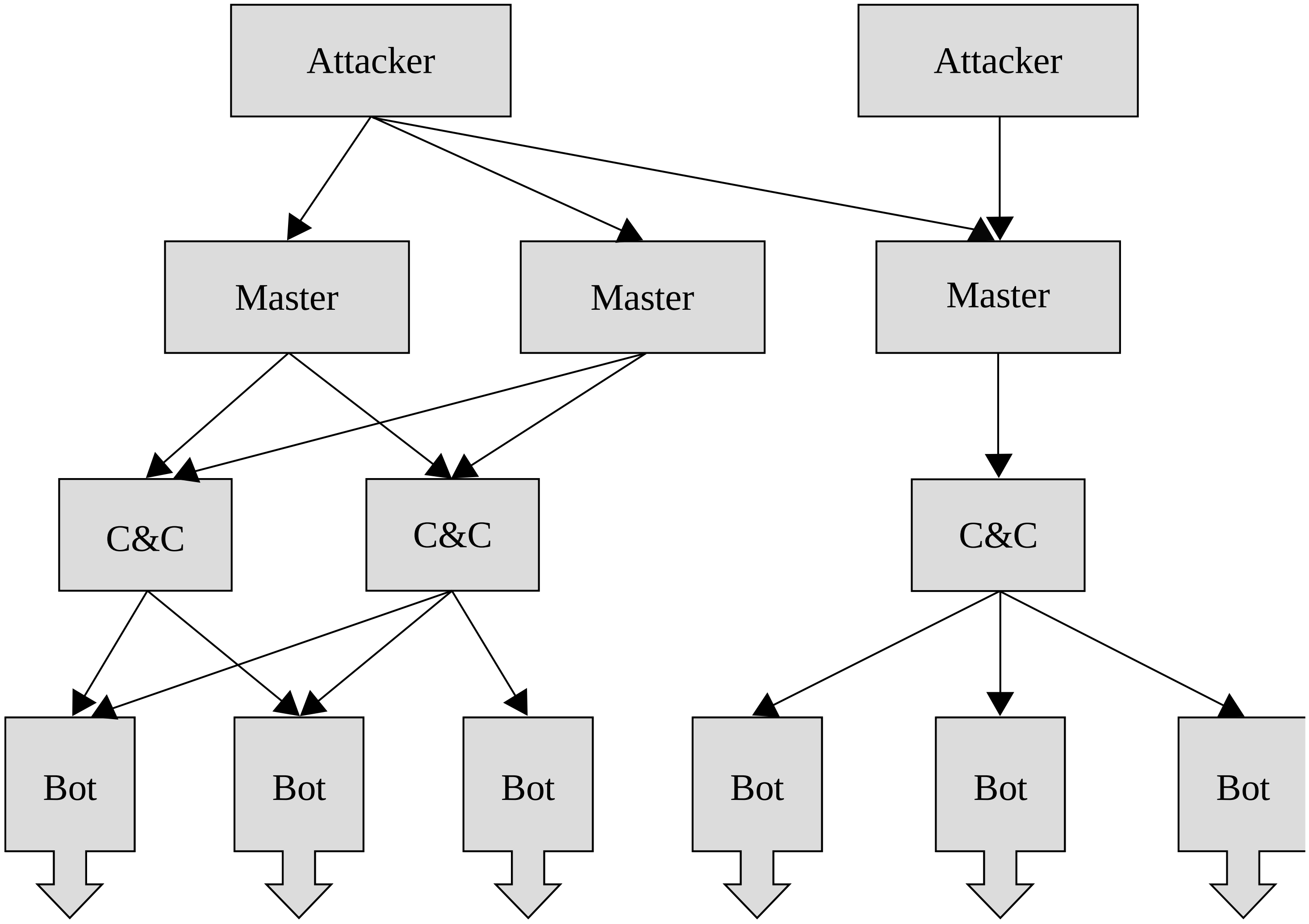
DoS Attack: Session Hijacking



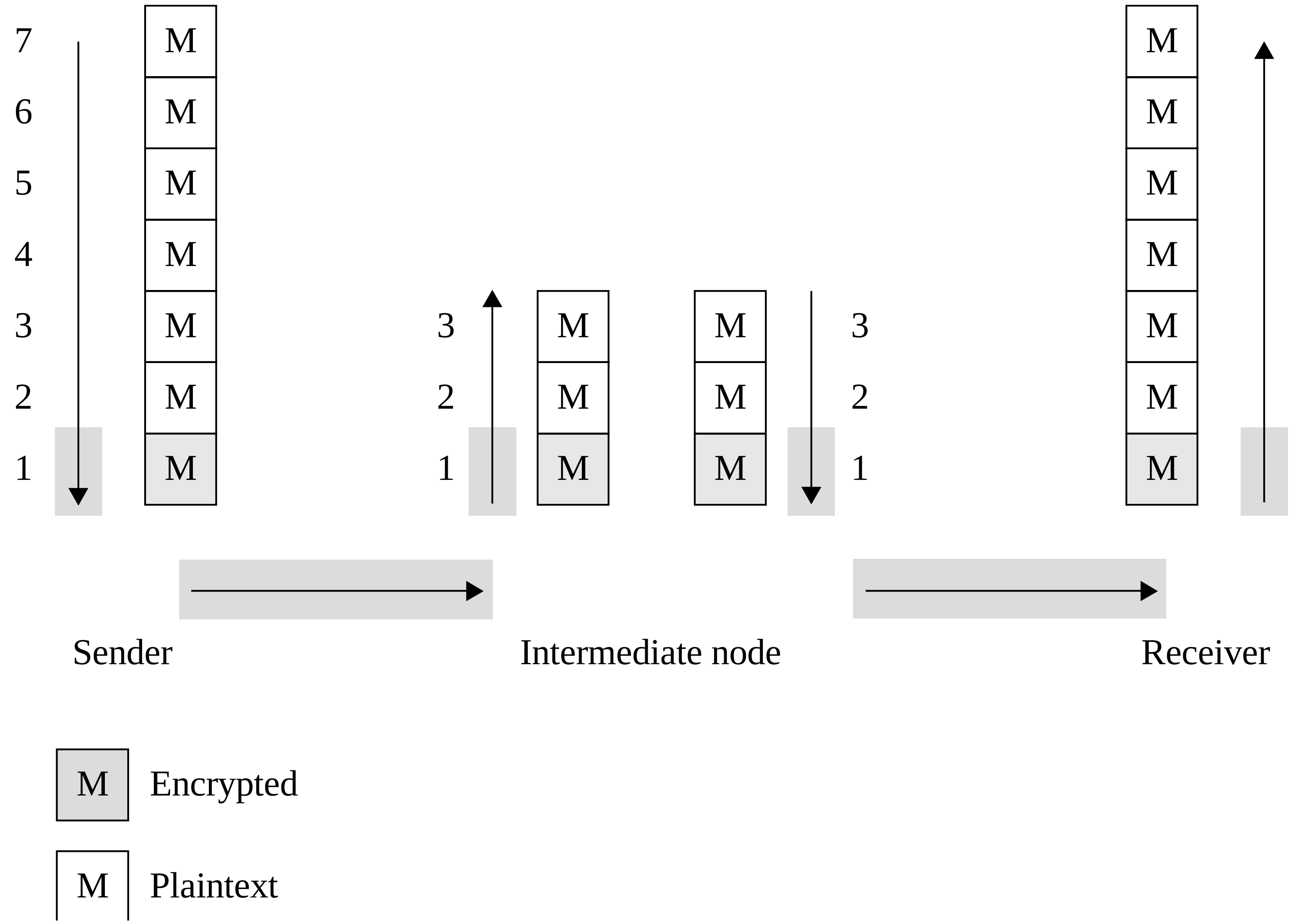
Distributed Denial of Service (DDoS)



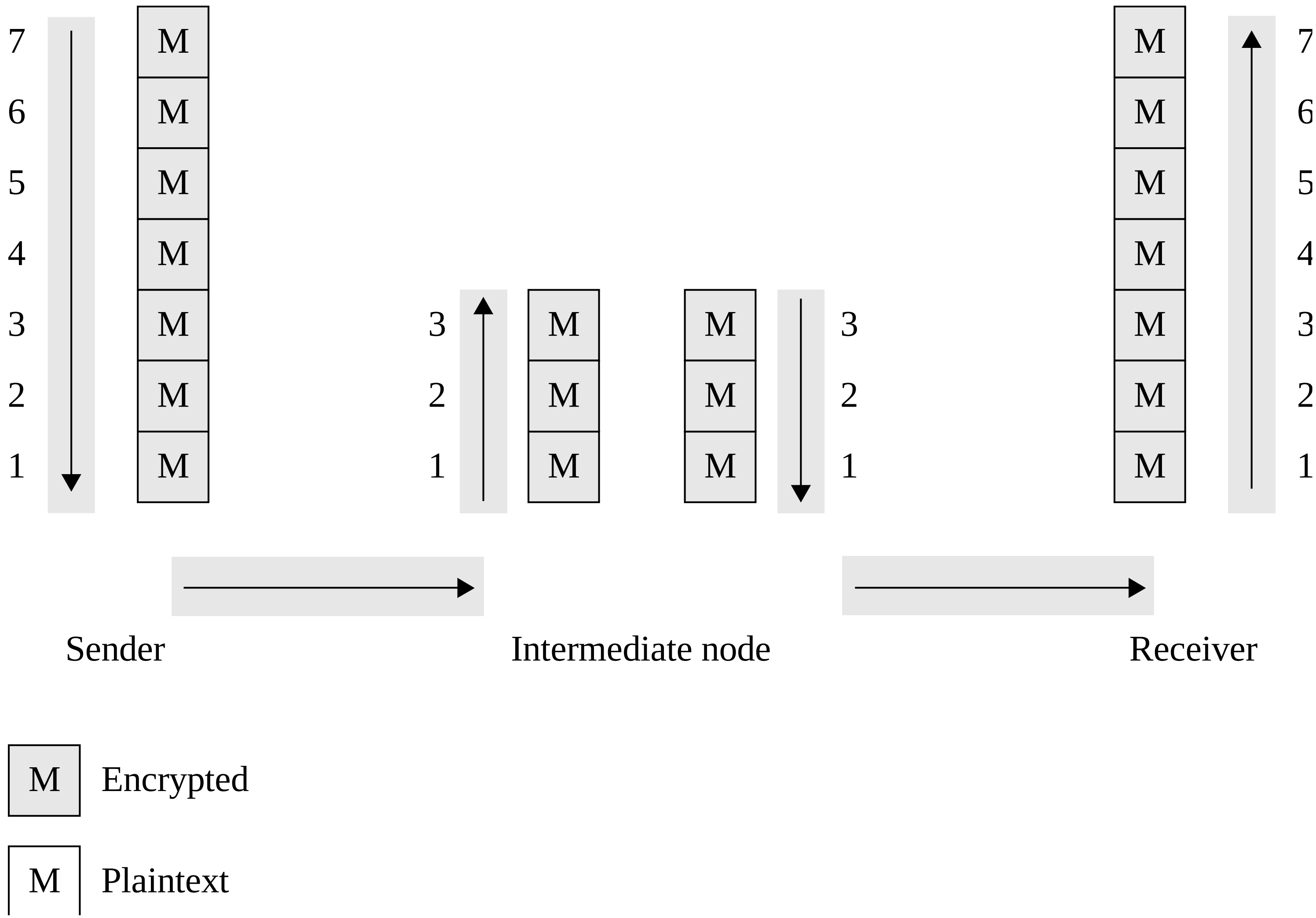
Botnets


Attacker
Attacker
Master
Master
Master
C&C
C&C
C&C
Bot
Bot
Bot
Bot
Bot
Bot

Link Encryption



End-to-End Encryption



Link vs. End-to-End

Link Encryption	End-to-End Encryption
Security within hosts	
Data partially exposed in sending host	Data protected in sending host
Data partially exposed in intermediate nodes	Data protected through intermediate nodes
Role of user	
Applied by sending host	Applied by user application
Invisible to user	User application encrypts
Host administrators select encryption	User selects algorithm
One facility for all users	Each user selects
Can be done in software or hardware	Usually software implementation; occasionally performed by user add-on hardware
All or no data encrypted	User can selectively encrypt individual data items
Implementation considerations	
Requires one key per pair of hosts	Requires one key per pair of users
Provides node authentication	Provides user authentication

Secure Shell (SSH)

- Originally developed for UNIX but now available on most OSs
- Provides an authenticated, encrypted path to the OS command line over the network
- Replacement for insecure utilities such as Telnet, rlogin, and rsh
- Protects against spoofing attacks and modification of data in communication

SSL and TLS

- Secure Sockets Layer (SSL) was designed in the 1990s to protect communication between a web browser and server
- In a 1999 upgrade to SSL, it was renamed Transport Layer Security (TLS)
- While the protocol is still commonly called SSL, TLS is the modern, and much more secure, protocol
- SSL is implemented at OSI layer 4 (transport) and provides
  - Server authentication
  - Client authentication (optional)
  - Encrypted communication

SSL Cipher Suites

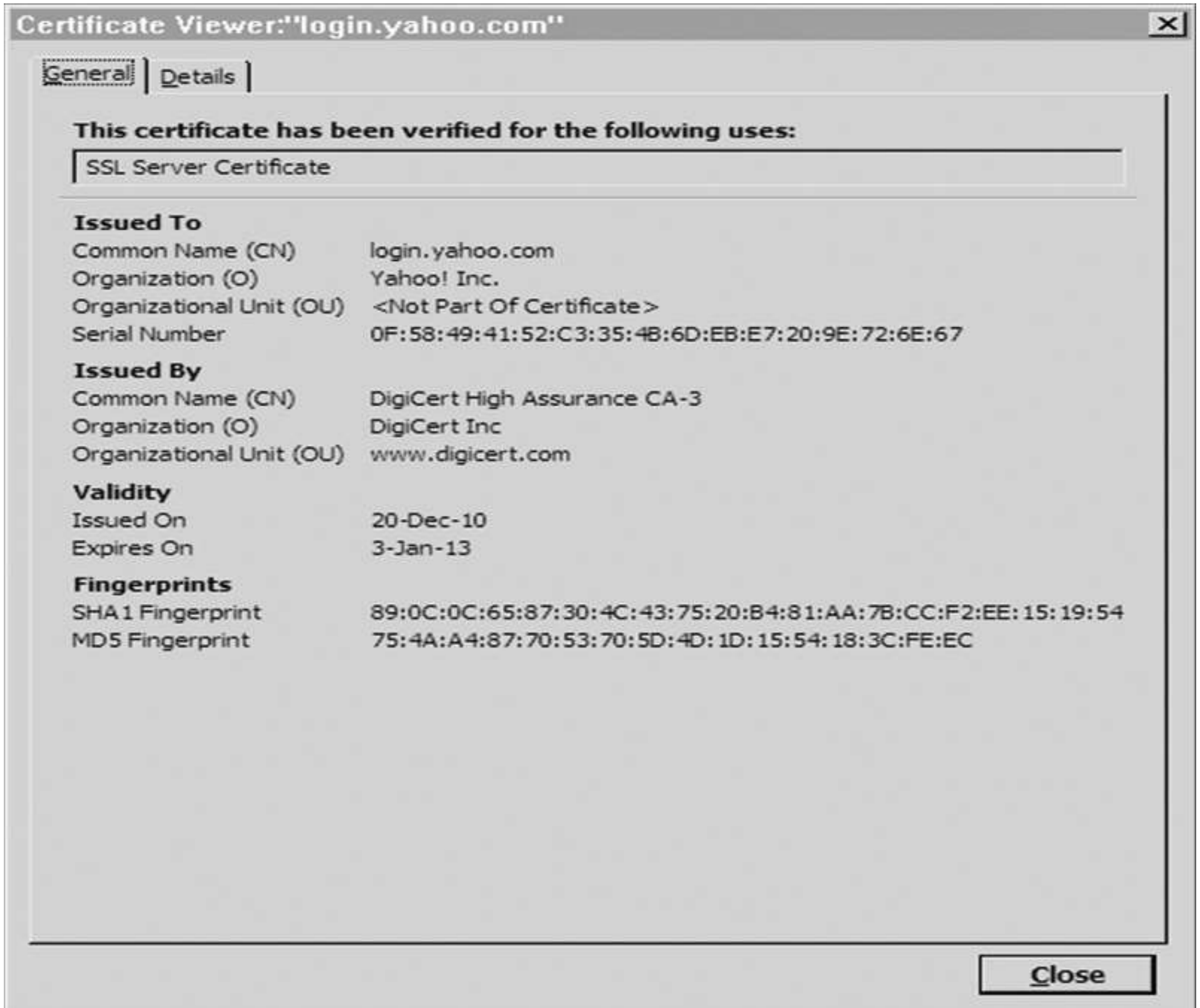
- At the start of an SSL session, the client and server negotiate encryption algorithms, known as the "cipher suite"
- The server sends a list of cipher suite options, and the client chooses an option from that list
- The cipher suite consists of
  - A digital signature algorithm for authentication
  - An encryption algorithm for confidentiality
  - A hash algorithm for integrity

SSL Cipher Suites (Partial List)

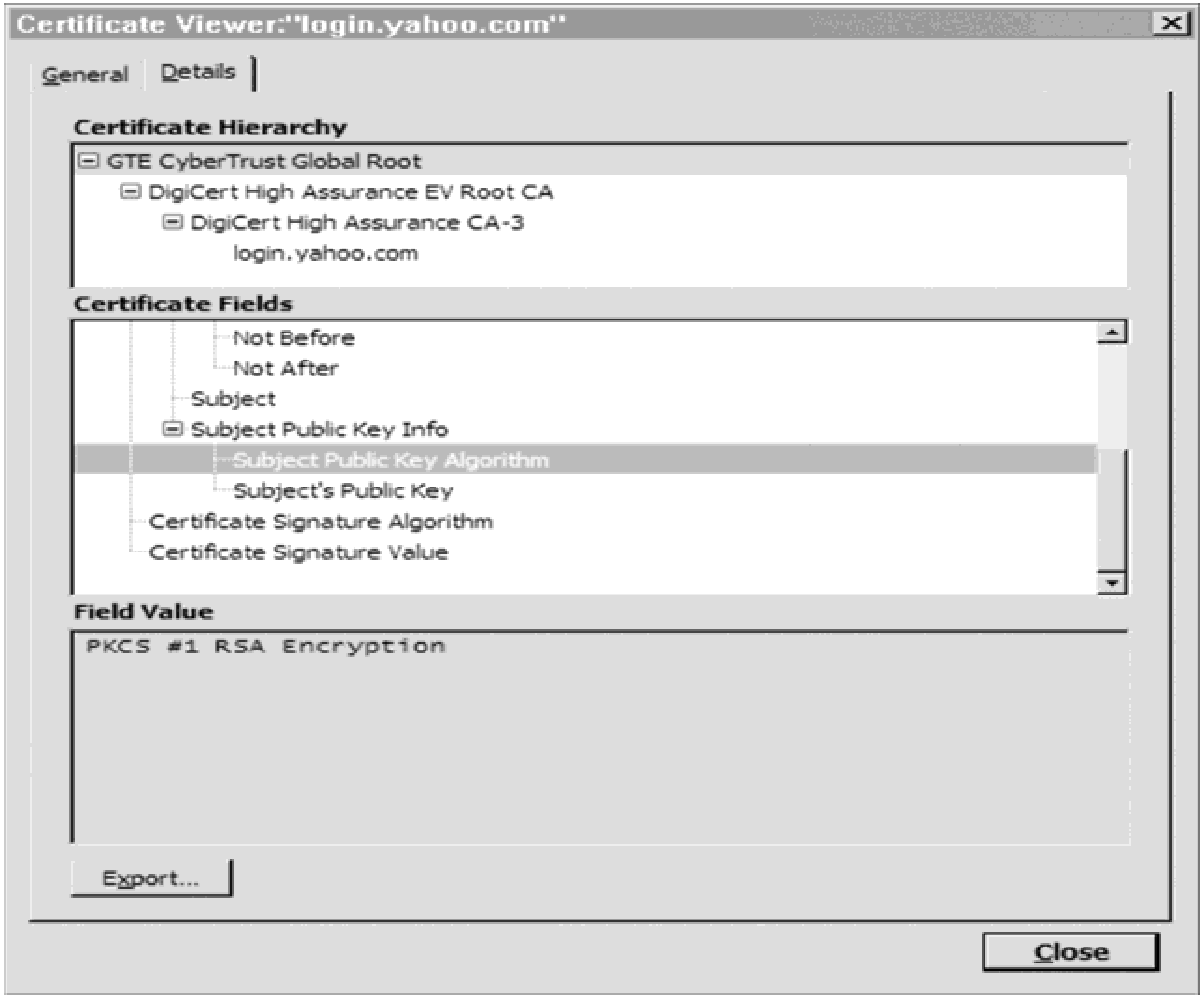
Cipher Suite Identifier	Algorithms Used
TLS_NULL_WITH_NULL_NULL	No authentication, no encryption, no hash function
TLS_RSA_WITH_NULL_MD5	RSA authentication, no encryption, MD5 hash function
TLS_RSA_EXPORT_WITH_RC4_40_MD5	RSA authentication with limited key length, RC4 encryption with a 40-bit key, MD5 hash function
TLS_RSA_WITH_3DES_EDE_CBC_SHA	RSA authentication, triple DES encryption, SHA-1 hash function
TLS_RSA_WITH_AES_128_CBC_SHA	RSA authentication, AES with a 128-bit key encryption, SHA-1 hash function
TLS_RSA_WITH_AES_256_CBC_SHA	RSA authentication, AES with a 256-bit key encryption, SHA-1 hash function
TLS_RSA_WITH_AES_128_CBC_SHA256	RSA authentication, AES with a 128-bit key encryption, SHA-256 hash function
TLS_RSA_WITH_AES_256_CBC_SHA256	RSA authentication, AES with a 256-bit key encryption, SHA-256 hash function
TLS_DH_DSS_WITH_3DES_EDE_CBC_SHA	Diffie-Hellman digital signature standard, triple DES encryption, SHA-1 hash function
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA http://www.iana.org/go/rfc5932	RSA digital signature, Camellia encryption with a 256-bit key, SHA-1 hash function
TLS_ECDHE_ECDSA_WITH_ARIA_256_CBC_SHA384	Elliptic curve cryptosystem digital signature algorithm, Aria encryption with a 256-bit key, SHA-384 hash function

SSL Session Established

SSL Certificate



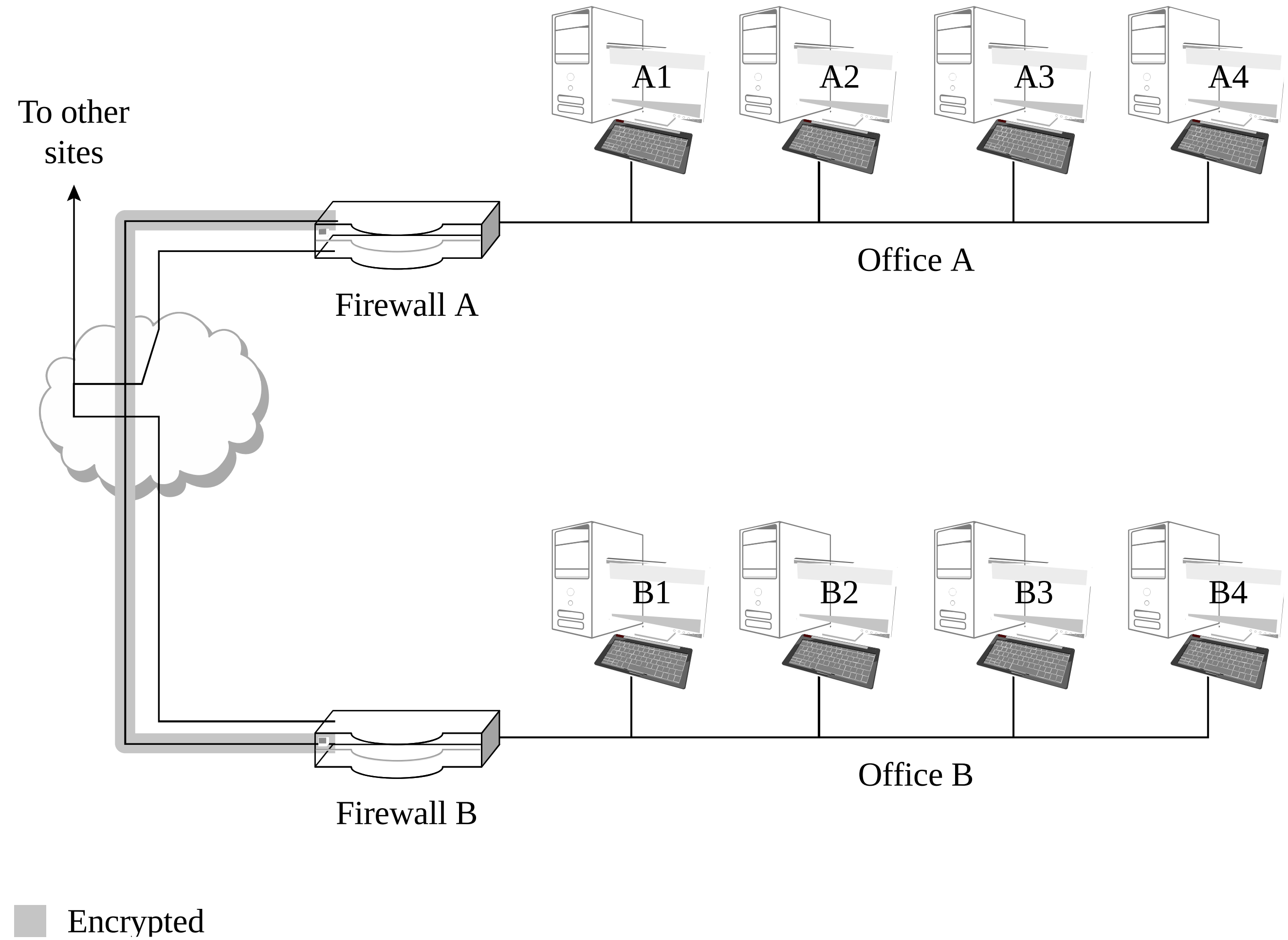
Chain of Certificates



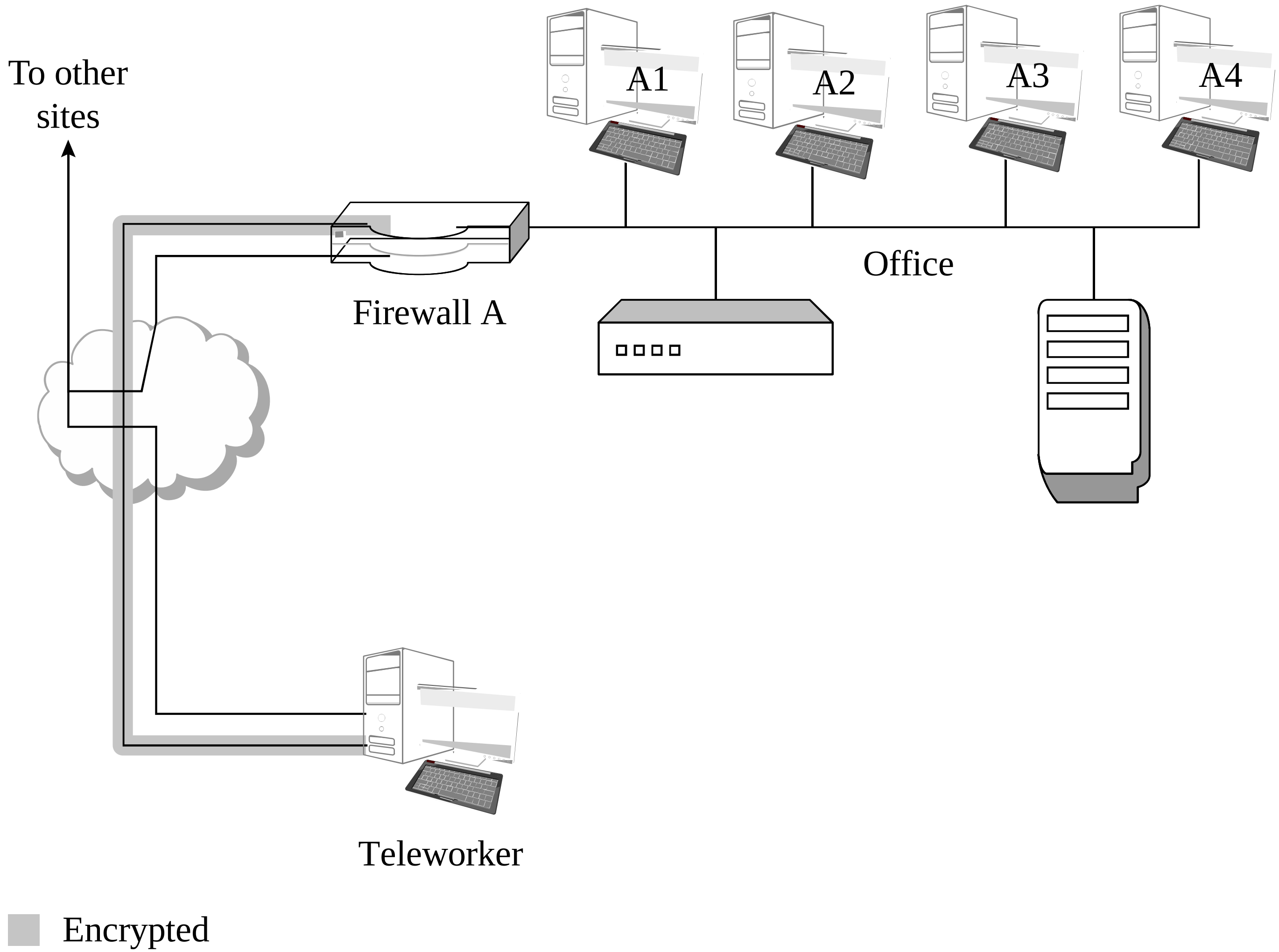
Onion Routing

- Onion routing prevents an eavesdropper from learning source, destination, or content of data in transit in a network
- This is particularly helpful for evading authorities, such as when users in oppressive countries want to communicate freely with the outside world
- Uses asymmetric cryptography, as well as layers of intermediate hosts, so that
  - The intermediate host that sends the message to the ultimate destination cannot determine the original sender, and
  - The host that received the message from the original sender cannot determine the ultimate destination

Virtual Private Networks (VPN)



VPN (cont.)


To other sites
A1
A2
A3
A4
Firewall A
Office
Teleworker
Encrypted

Firewalls

- A device that filters all traffic between a protected or “inside” network and less trustworthy or “outside” network
- Most firewalls run as dedicated devices
  - Easier to design correctly and inspect for bugs
  - Easier to optimize for performance
- Firewalls implement security policies, or set of rules that determine what traffic can or cannot pass through
- A firewall is an example of a reference monitor, which means it should have three characteristics:
  - Always invoked (cannot be circumvented)
  - Tamperproof
  - Small and simple enough for rigorous analysis

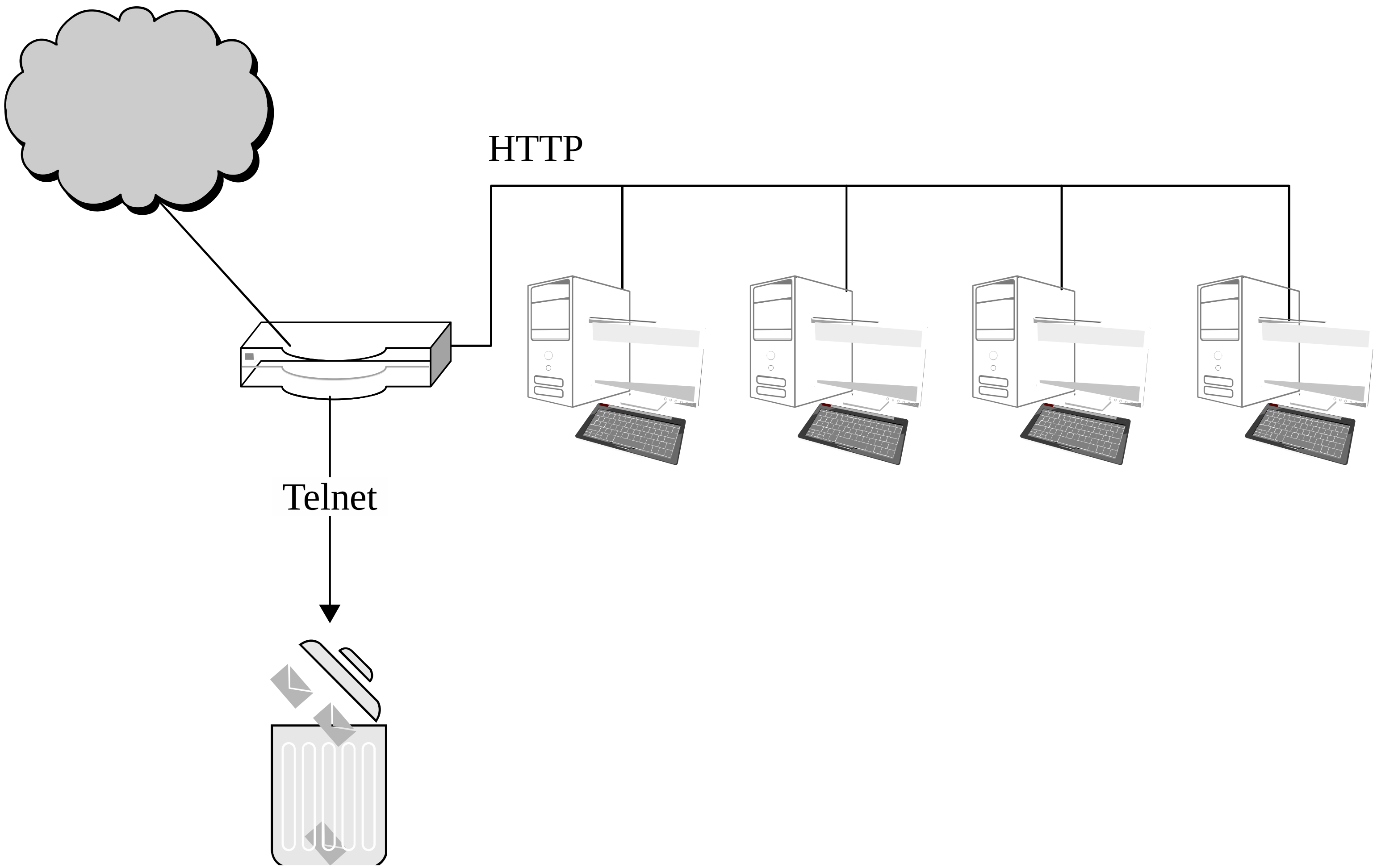
Firewall Security Policy

Rule	Type	Source Address	Destination Address	Destination Port	Action
1	TCP	*	192.168.1.*	25	Permit
2	UDP	*	192.168.1.*	69	Permit
3	TCP	192.168.1.*	*	80	Permit
4	TCP	*	192.168.1.18	80	Permit
5	TCP	*	192.168.1.*	*	Deny
6	UDP	*	192.168.1.*	*	Deny

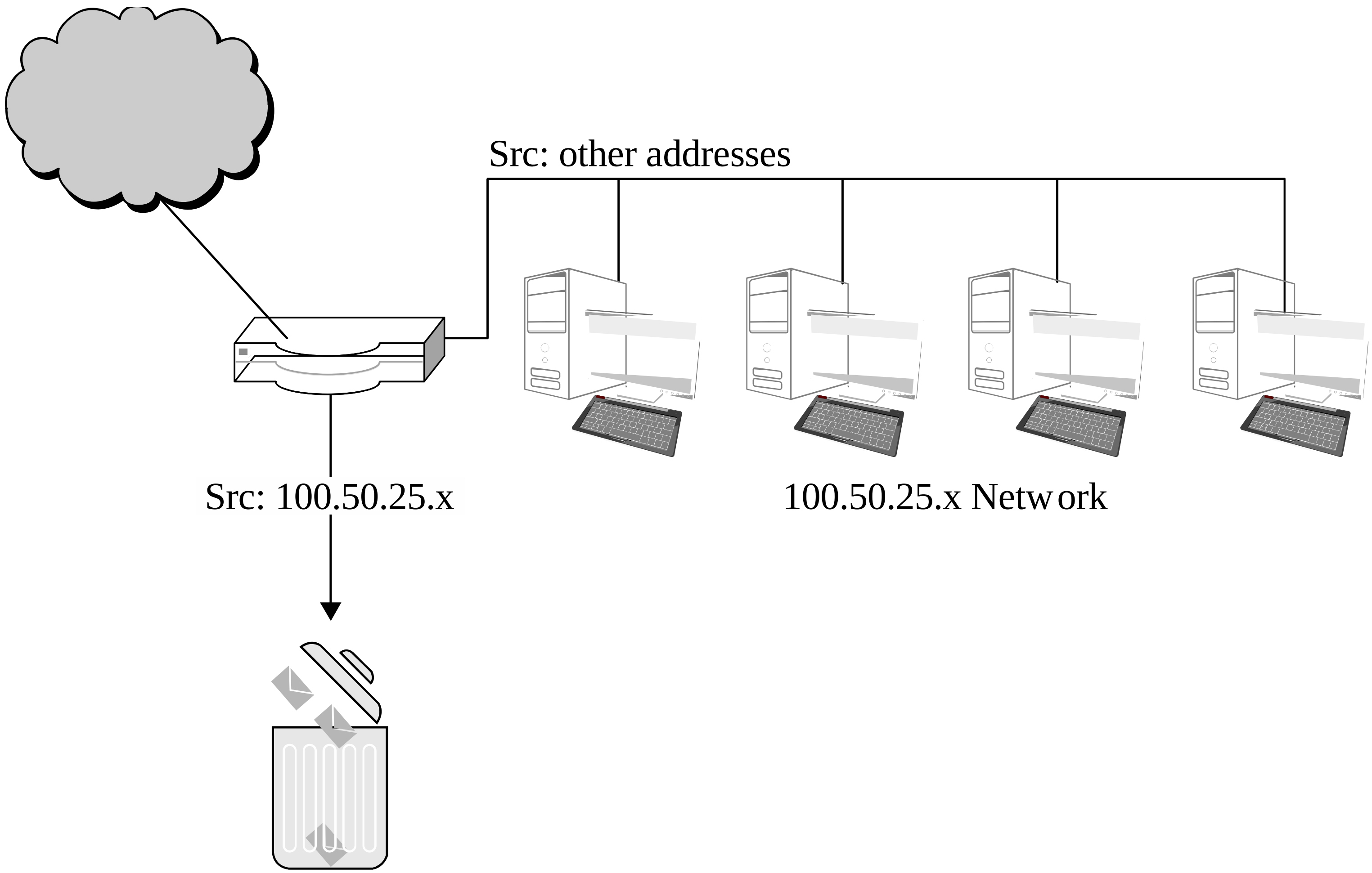
Types of Firewalls

- Packet filtering gateways or screening routers
- Stateful inspection firewalls
- Application-level gateways, also known as proxies
- Circuit-level gateways
- Guards
- Personal or host-based firewalls

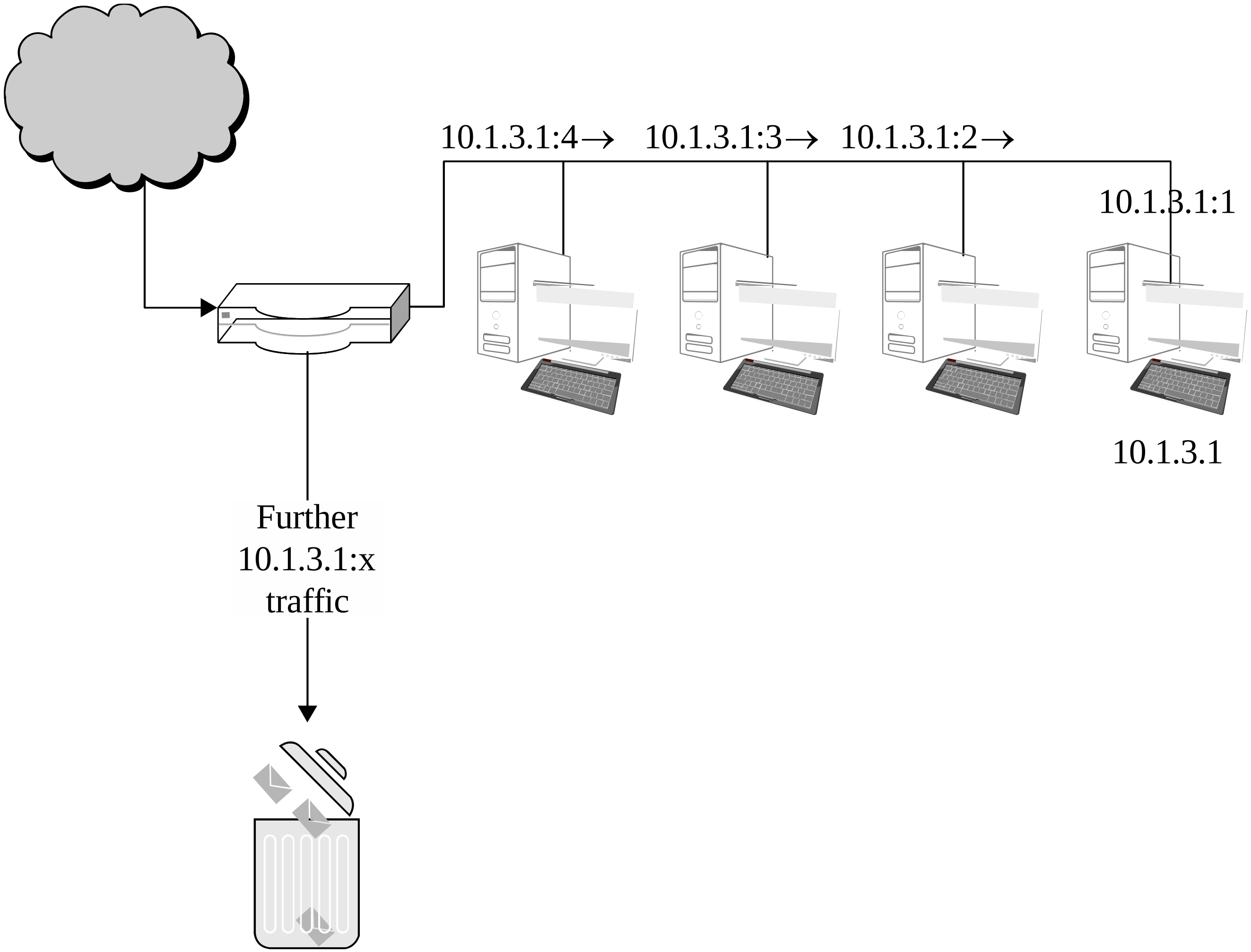
Packet-Filtering Gateways



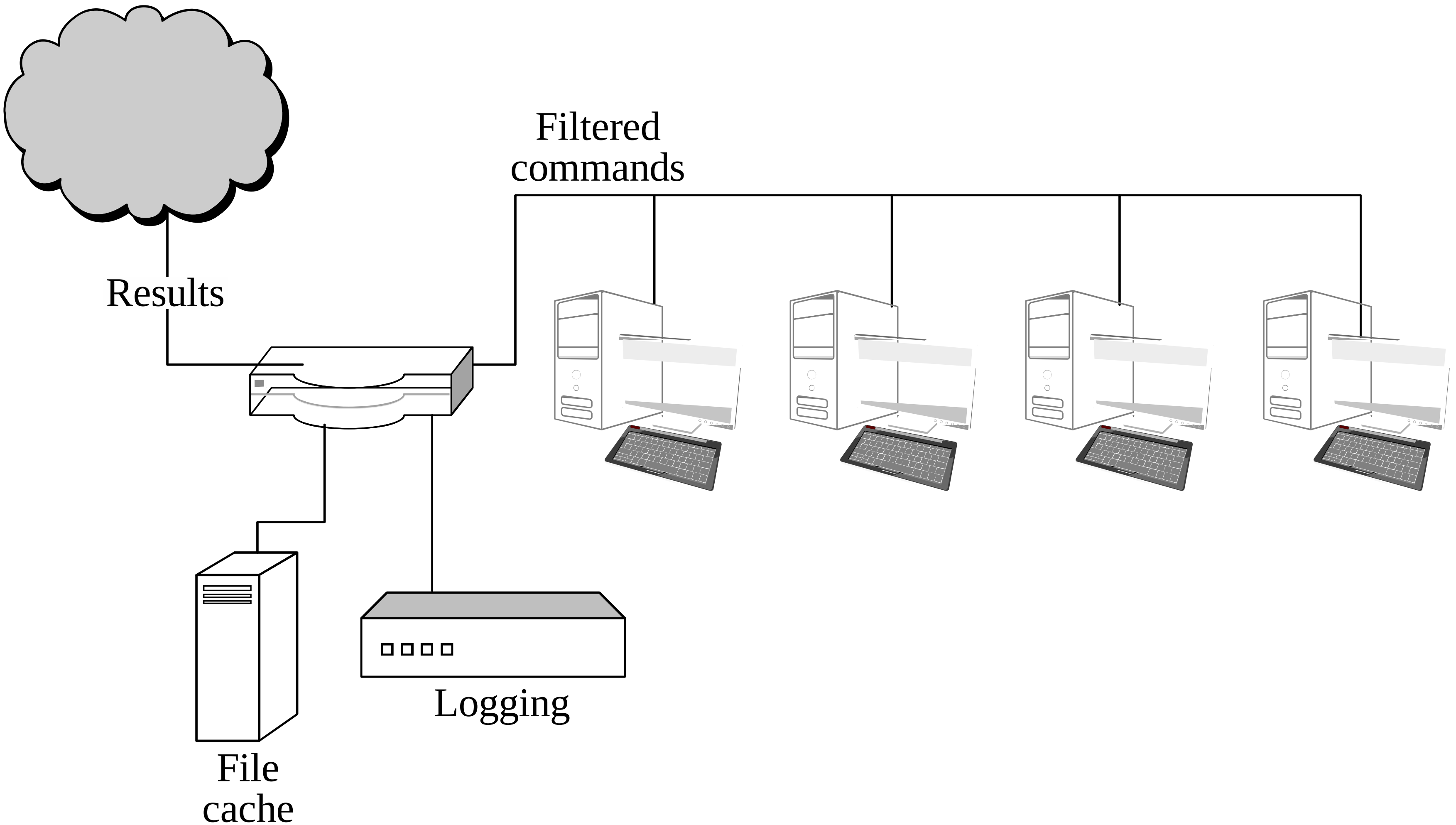
Packet-Filtering Gateways (cont.)



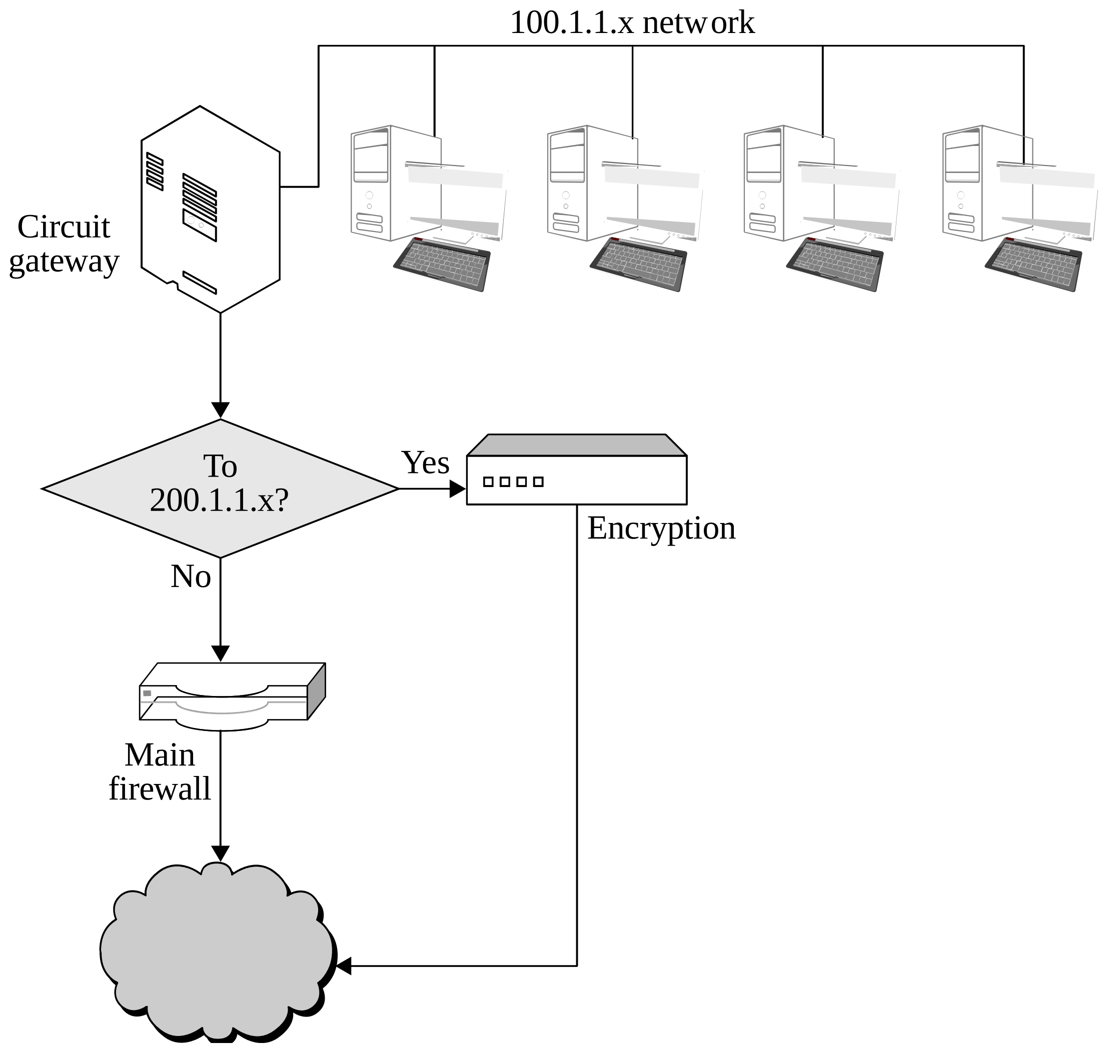
Stateful Inspection Firewall



Application Proxy



Circuit-Level Gateway



Guard

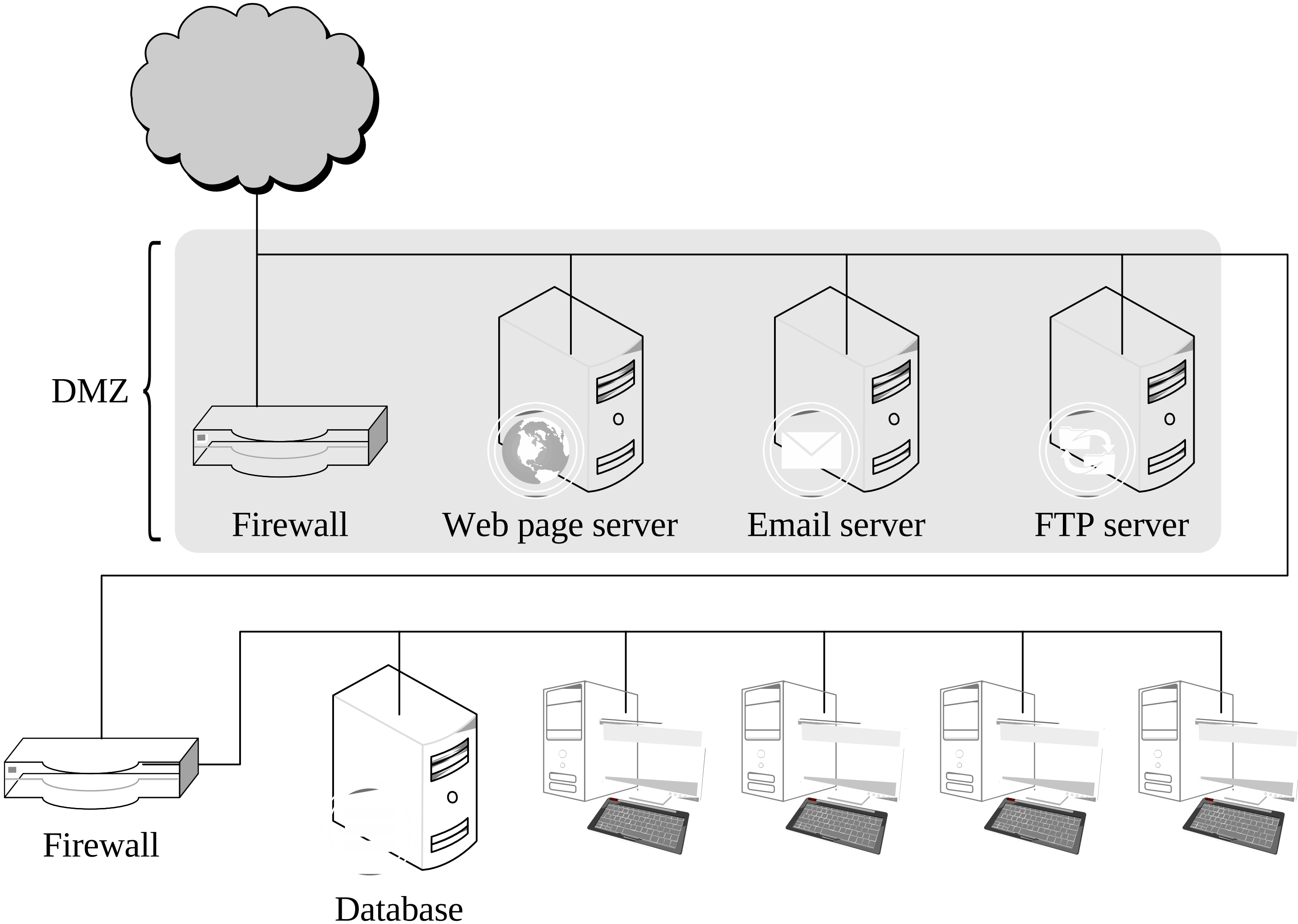
- A sophisticated firewall that, like an application proxy, can interpret data at the protocol level and respond
- The distinction between a guard and an application proxy can be fuzzy; the more protection features an application proxy implements, the more it becomes like a guard
- Guards may implement any programmable set of rules; for example:
  - Limit the number of email messages a user can receive
  - Limit users' web bandwidth
  - Filter documents containing the word "Secret"
  - Pass downloaded files through a virus scanner

Personal Firewalls

Comparison of Firewall Types

Packet Filter	Stateful Inspection	Application Proxy	Circuit Gateway	Guard	Personal Firewall
Simplest decision-making rules, packet by packet	Correlates data across packets	Simulates effect of an application program	Joins two subnetworks	Implements any conditions that can be programmed	Similar to packet filter, but getting more complex
Sees only addresses and service protocol type	Can see addresses and data	Sees and analyzes full data portion of pack	Sees addresses and data	Sees and analyzes full content of data	Can see full data portion
Auditing limited because of speed limitations	Auditing possible	Auditing likely	Auditing likely	Auditing likely	Auditing likely
Screens based on connection rules	Screens based on information across multiple packets—in either headers or data	Screens based on behavior of application	Screens based on address	Screens based on interpretation of content	Typically, screens based on content of each packet individually, based on address or content
Complex addressing rules can make configuration tricky	Usually preconfigured to detect certain attack signatures	Simple proxies can substitute for complex decision rules, but proxies must be aware of application's behavior	Relatively simple addressing rules; make configuration straightforward	Complex guard functionality; can be difficult to define and program accurately	Usually starts in mode to deny all inbound traffic; adds addresses and functions to trust as they arise

Demilitarized Zone (DMZ)



What Firewalls Can and Cannot Do

- Firewalls can protect an environment only if they control the entire perimeter
- Firewalls do not protect data outside the perimeter
- Firewalls are the most visible part of an installation to the outside, so they are an attractive target for attack
- Firewalls must be correctly configured, that configuration must be updated as the environment changes, and firewall activity reports must be reviewed periodically for evidence of attempted or successful intrusion
- Firewalls exercise only minor control over the content admitted to the inside, meaning that inaccurate or malicious code must be controlled by means inside the perimeter

Network Address Translation (NAT)

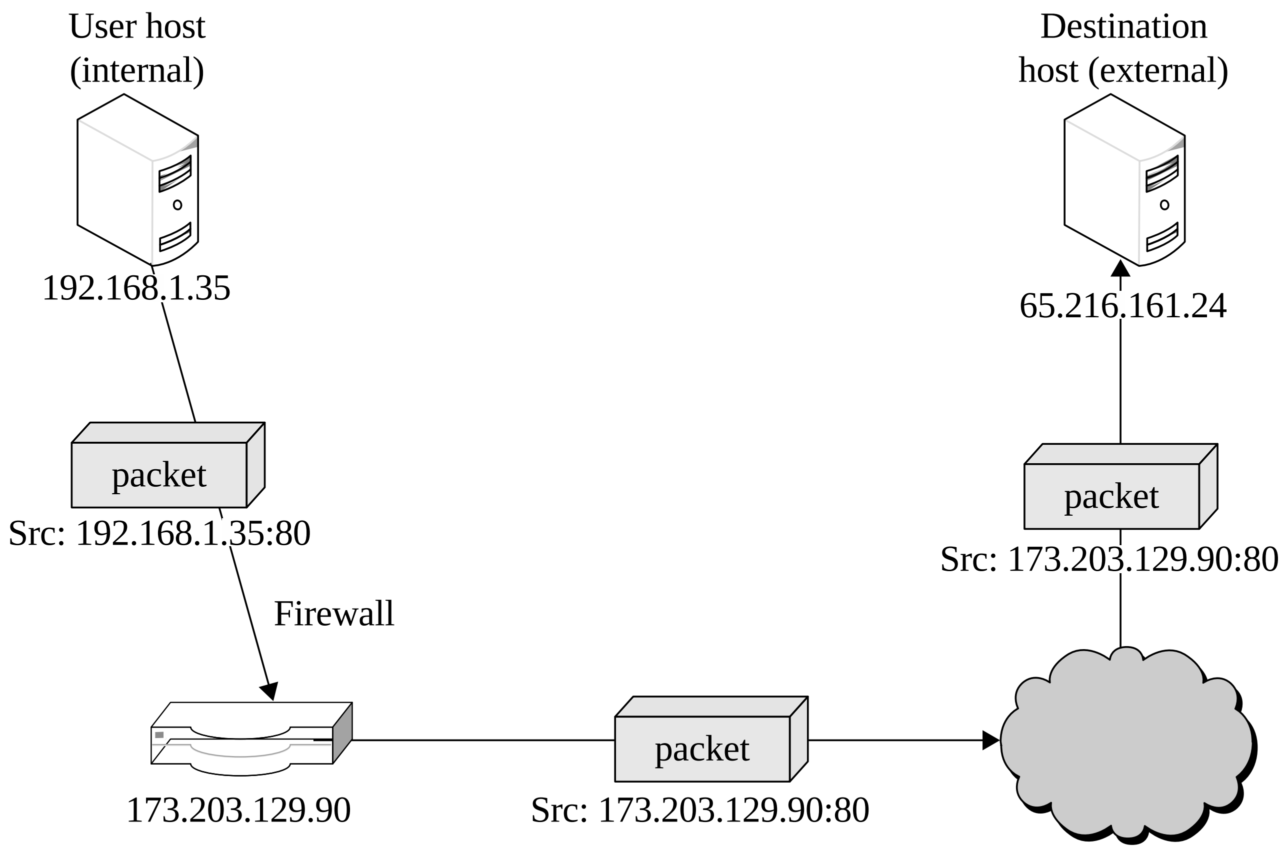


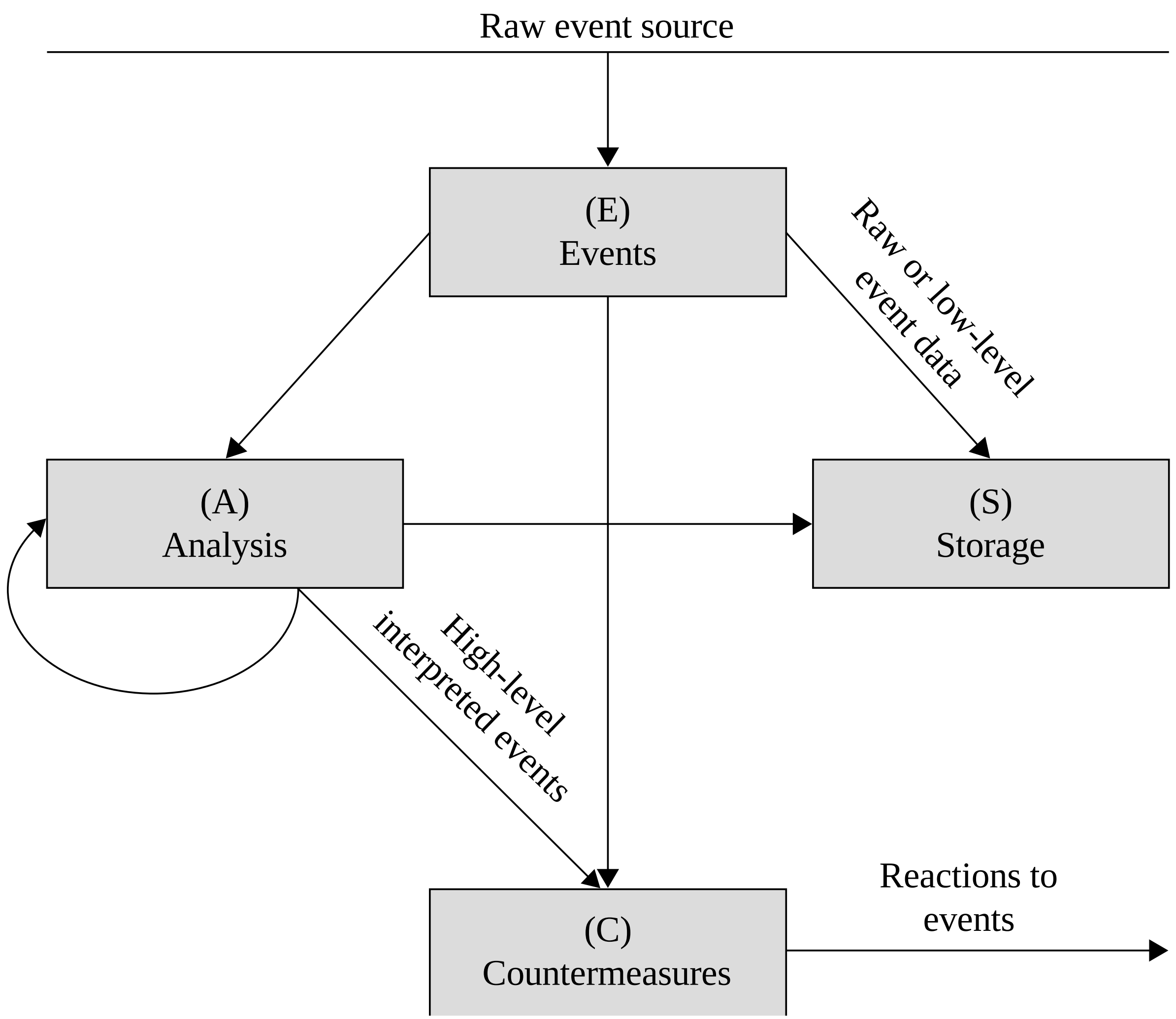
Table of translations performed

Source	Dest
192.168.1.35:80	65.216.161.24:80

Data Loss Prevention (DLP)

- DLP is a set of technologies that can detect and possibly prevent attempts to send sensitive data where it is not allowed to go
- Can be implemented as
  - Agent installed as an OS rootkit
  - Guard
- Indicators DLP looks for:
  - Keywords
  - Traffic patterns
  - Encoding/encryption
- DLP is best for preventing accidental incidents, as malicious users will often find ways to circumvent it

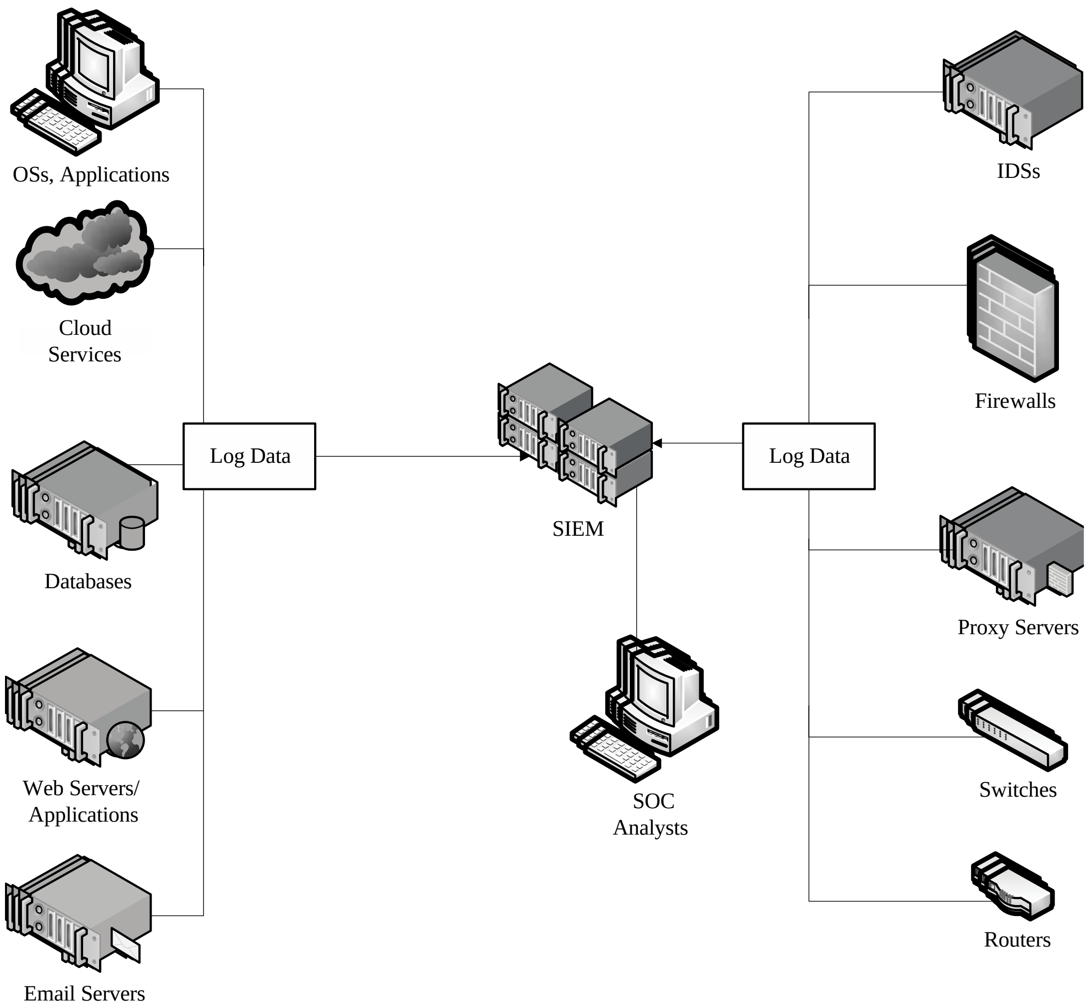
Intrusion Detection Systems (IDS)



Types of IDS

- Detection method
  - Signature-based
  - Heuristic
- Location
  - Front end
  - Internal
- Scope
  - Host-based IDS (HIDS)
  - Network-based IDS (NIDS)
- Capability
  - Passive
  - Active, also known as intrusion prevention systems (IPS)

Security Information and Event Management (SIEM)



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