CSCI-GA.3205 Applied Cryptography & Network Security

Department of Computer Science
New York University

PRESENTED BY DR. MAZDAK ZAMANI
mazdak.zamani@NYU.edu

Application, Data, and Host Security
Securing Network Devices
Network Security Hardware
Securing the operating system (OS)
Digital Signatures & Certificates
Pretty Good Privacy (PGP)
Security Through Network Design Elements

09

NYU

CompTIA Security+ Guide to Network Security Fundamentals, Fifth Edition

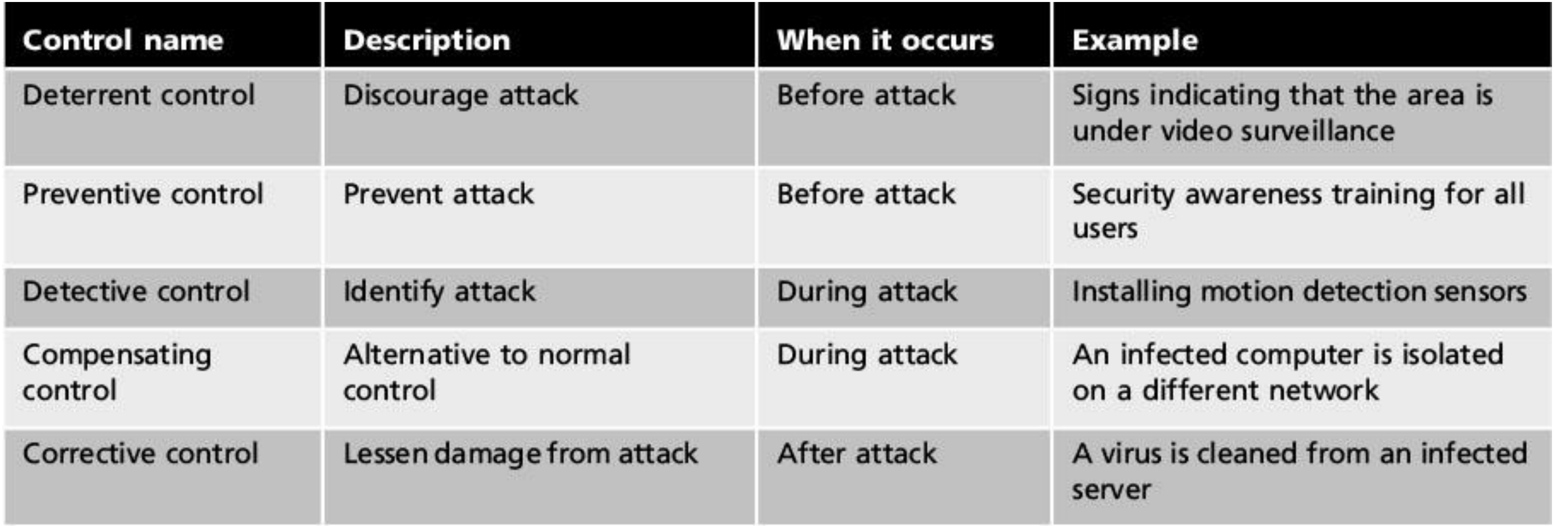
Chapter 4

Host, Application, and Data Security

Securing Devices

- Security control - any device or process that is used to reduce risk
- Two levels of security controls:
    - Administrative controls - processes for developing and ensuring that policies and procedures are carried out
    - Technical controls - controls that are carried out or managed by devices
- There are five subtypes of controls (sometimes called activity phase controls) described on the following slide

Securing Devices



Control name	Description	When it occurs	Example
Deterrent control	Discourage attack	Before attack	Signs indicating that the area is under video surveillance
Preventive control	Prevent attack	Before attack	Security awareness training for all users
Detective control	Identify attack	During attack	Installing motion detection sensors
Compensating control	Alternative to normal control	During attack	An infected computer is isolated on a different network
Corrective control	Lessen damage from attack	After attack	A virus is cleaned from an infected server

Table 4-1 Activity phase controls

External Perimeter Defenses

- External perimeter defenses are designed to restrict access to equipment areas. This type of defense includes:
- Barriers
  - Fencing - usually a tall, permanent structure
    - Modern perimeter fences are equipped with other deterrents such as proper lighting and signage
  - Barricade - large concrete ones should be used
- Guards
  - Human guards are considered active security elements
  - Video surveillance uses cameras to transmit a signal to a specific and limited set of receivers called closed circuit television (CCTV)
- Motion Detection
  - Determining an object’s change in position in relation to its surroundings
  - This movement usually generates an audible alarm

Internal Physical Access Security

- These protections include:
  - Hardware locks
  - Proximity readers
  - Access lists
  - Mantraps
  - Protected distribution systems for cabling

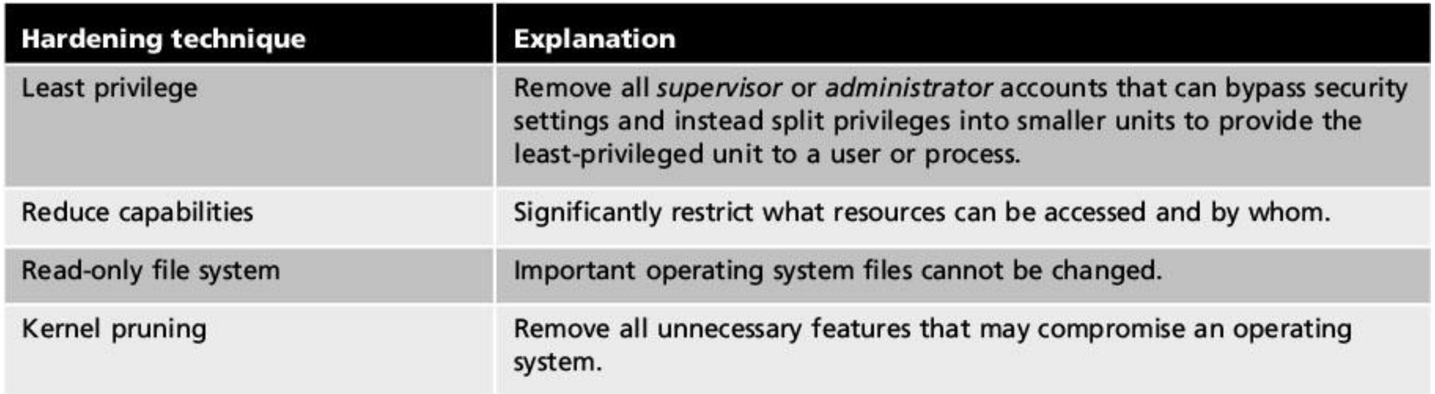
Securing the Operating System Software

Five-step process for protecting operating system

- Develop the security policy
  - Security policy - a document(s) that clearly define organization's defense mechanisms
- Perform host software baselining
  - Baseline - the standard or checklist against which systems can be evaluated
- Configure operating system security and settings
  - Eliminating unnecessary software, services, protocols
  - Enabling security features such as a firewall
- Deploy and Manage Security Settings
  - Group policy - Windows feature providing centralized computer management; a single configuration may be deployed to many users
- Implement Patch Management
  - New attack tools have made secure functions vulnerable
  - **Security patch** - software security update to repair discovered vulnerabilities

Securing the Operating System Software

- Security Through Design
  - **OS hardening** - tightening security during the design and coding of the OS
  - **Trusted OS** - an OS that has been designed through OS hardening



Hardening technique	Explanation
Least privilege	Remove all *supervisor* or *administrator* accounts that can bypass security settings and instead split privileges into smaller units to provide the least-privileged unit to a user or process.
Reduce capabilities	Significantly restrict what resources can be accessed and by whom.
Read-only file system	Important operating system files cannot be changed.
Kernel pruning	Remove all unnecessary features that may compromise an operating system.

Table 4-4 **OS hardening techniques**

Securing with Antimalware

- Third-party antimalware software packages can provide added security

- Antimalware software includes:
    - Antivirus
    - Antispam
    - Popup Blockers
    - Antispyware
    - Host-based firewalls

Application Security

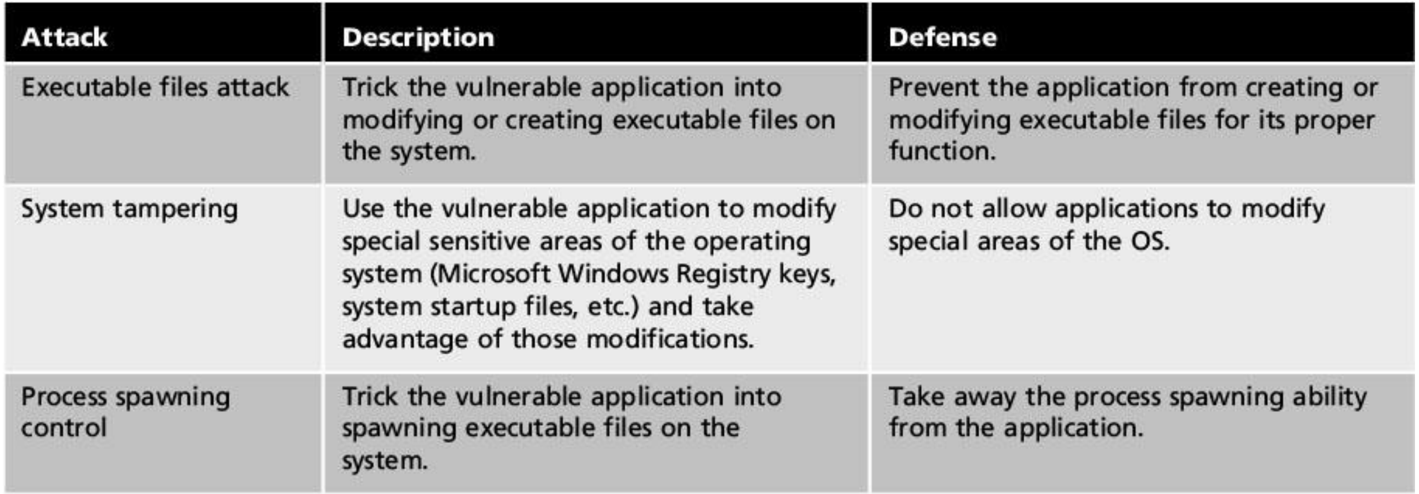
- Besides protecting OS software on hosts, there is a need to protect applications that run on these devices
- Aspects of application security:
  - Application development security
  - Application hardening and patch management

Application Development Security

- Security for applications must be considered through all phases of development cycle
- Errors and Exception Handling
    - Errors - faults that occur while application is running
    - Improper error handling in an application can lead to application failure
    - Fuzz testing (fuzzing) - a software testing technique that deliberately provides invalid, unexpected, or random data as inputs to a program
- Input Validation
    - A specific type of error handling is verifying responses that the user makes to the application
    - Improper verification is the cause for XSS, SQL, or XML injection attacks

Application Hardening and Patch Management

- Application hardening
  - Intended to prevent attackers from exploiting vulnerabilities in software applications



Attack	Description	Defense
Executable files attack	Trick the vulnerable application into modifying or creating executable files on the system.	Prevent the application from creating or modifying executable files for its proper function.
System tampering	Use the vulnerable application to modify special sensitive areas of the operating system (Microsoft Windows Registry keys, system startup files, etc.) and take advantage of those modifications.	Do not allow applications to modify special areas of the OS.
Process spawning control	Trick the vulnerable application into spawning executable files on the system.	Take away the process spawning ability from the application.

Table 4-6 Attacks based on application vulnerabilities

Securing Data

- **Data loss prevention (DLP)**
  - System of security tools used to recognize and identify critical data and ensure it is protected
  - Goal: protect data from unauthorized users
- DLP examines data as it resides in any of three states: *Data in use, Data in-transit, Data at rest*
- Most DLP systems use *content inspection*

- Three types of DLP sensors:
  - *DLP network sensors* - installed on the perimeter of the network to protect data in-transit by monitoring all network traffic
  - *DLP storage sensors* - designed to protect data at-rest
  - *DLP agent sensors* - installed on each host device and protect data in-use

CompTIA Security+ Guide to Network Security Fundamentals, Fifth Edition

Chapter 7

Network Security Fundamentals

Network Security

- Standard Network Devices
- Network Security Hardware
- Security Through Network Technologies
- Security Through Network Design Elements

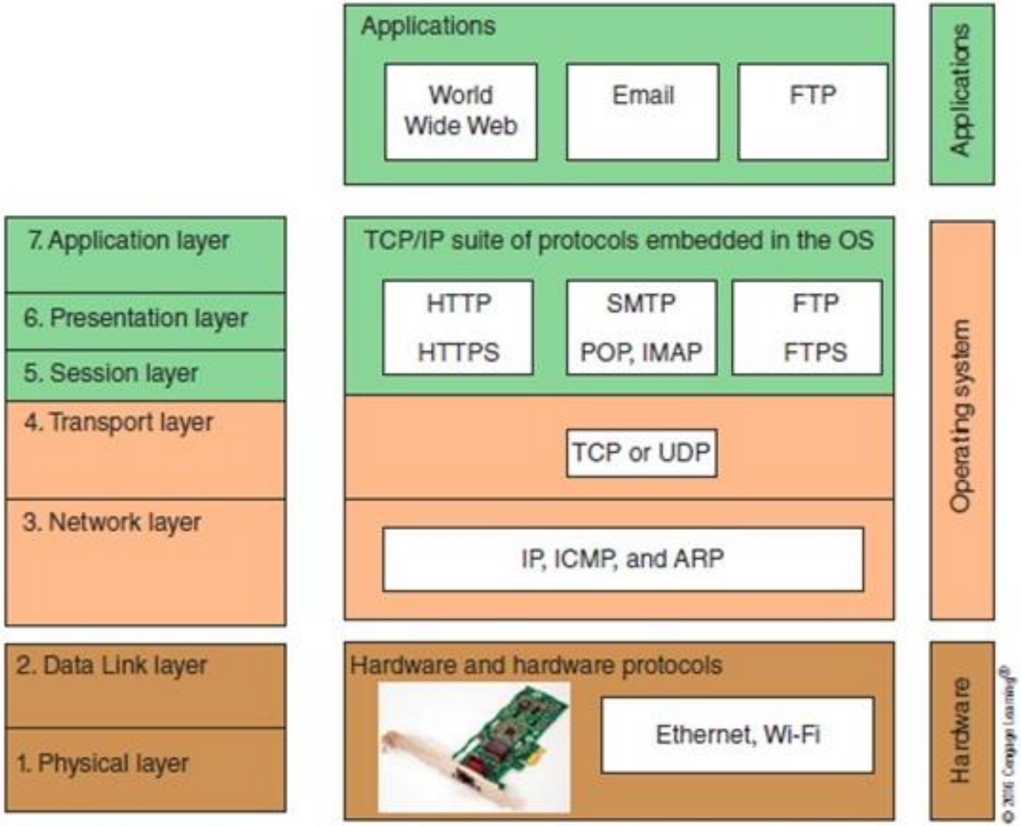
Security Through Network Devices

- **Layered security**
  - A defense that uses multiple types of security devices to protect a network
  - Also called *defense in depth*
- Layered network security can be achieved by using *networking devices* or *hardware designed for security*.

Standard Network Devices

- OSI model breaks networking steps into seven layers
- Standard network devices can be classified by the OSI layer at which they function. Some devices include:
  - Switches, routers, load balancers, and proxies
- Security features found in network hardware provide basic level of security.

OSI model - Review



7. Application layer

6. Presentation layer

5. Session layer

4. Transport layer

3. Network layer

2. Data Link layer

1. Physical layer

Applications

World Wide Web

Email

FTP

TCP/IP suite of protocols embedded in the OS

HTTP
HTTPS

SMTP
POP, IMAP

FTP
FTPS

TCP or UDP

IP, ICMP, and ARP

Hardware and hardware protocols

Ethernet, Wi-Fi

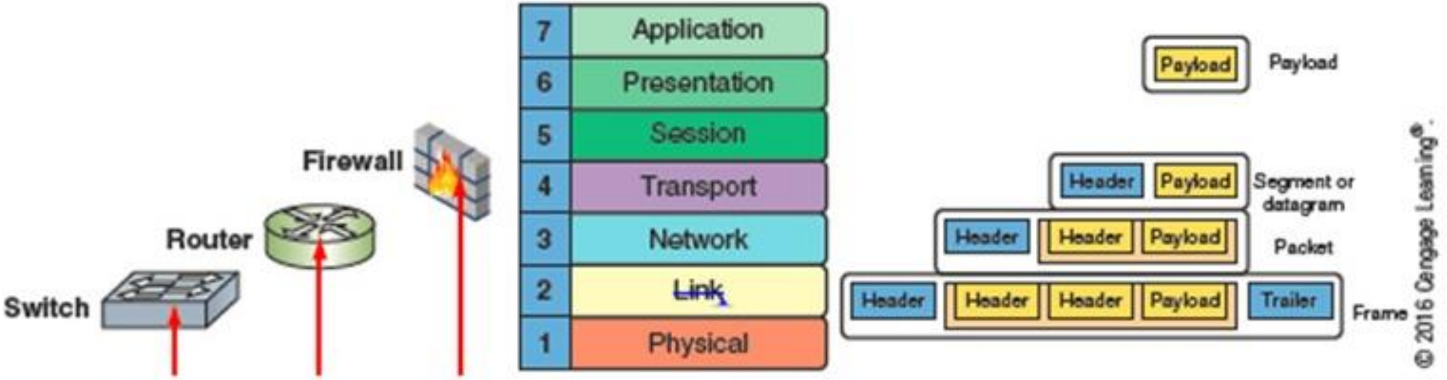
Applications

Operating system

Hardware

© 2016 Cengage Learning®

TCP-IP Protocol - Review

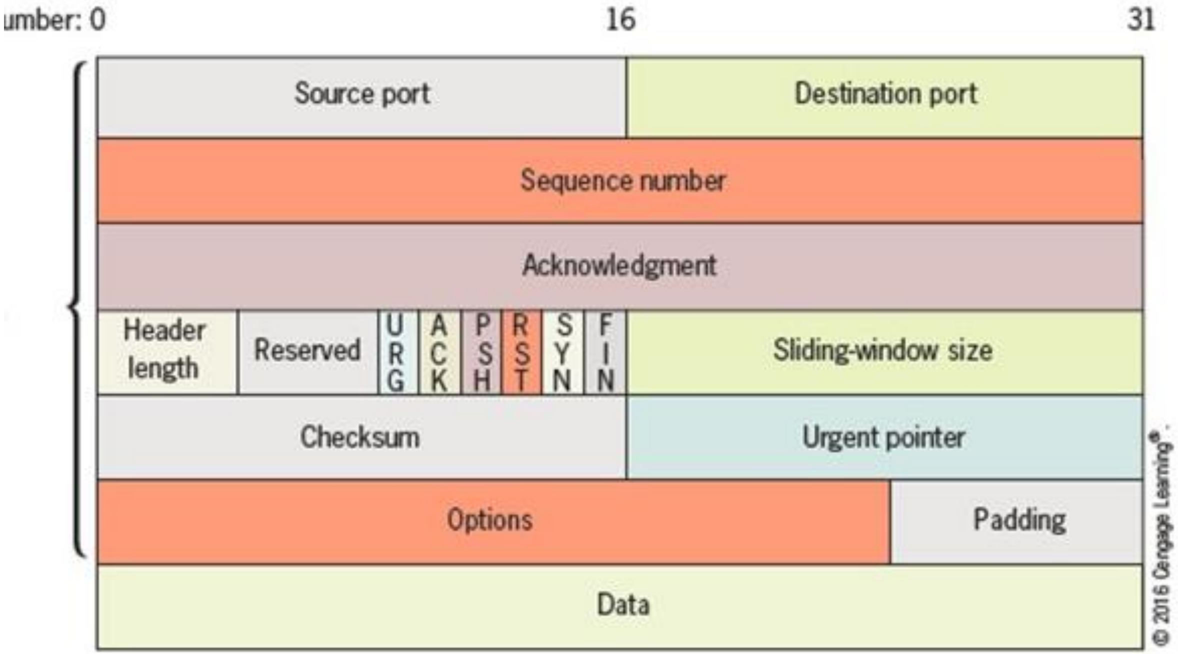


© 2016 Cengage Learning®.

Figure 3-2 Connectivity devices are known by the highest OSI layer they read and process

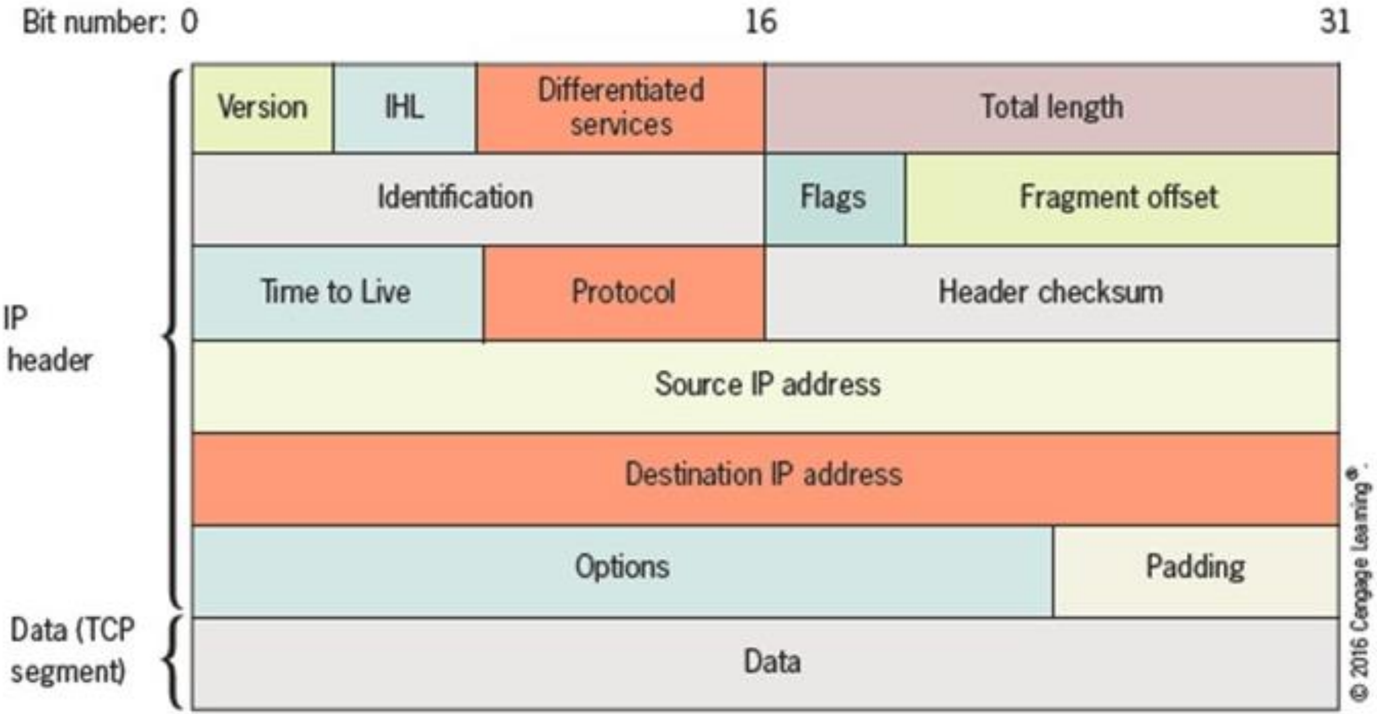
TCP Segment

TCP segment = TCP header + data from higher layer



Source port								Destination port
Sequence number								
Acknowledgment								
Header length	Reserved	URG	ACK	PSH	RST	SYN	FIN	Sliding-window size
Checksum								Urgent pointer
Options								Padding
Data								

IPv4-Packet



Bit number: 0 16 31

IP header

Version | IHL | Differentiated services | Total length

Identification | Flags | Fragment offset

Time to Live | Protocol | Header checksum

Source IP address

Destination IP address

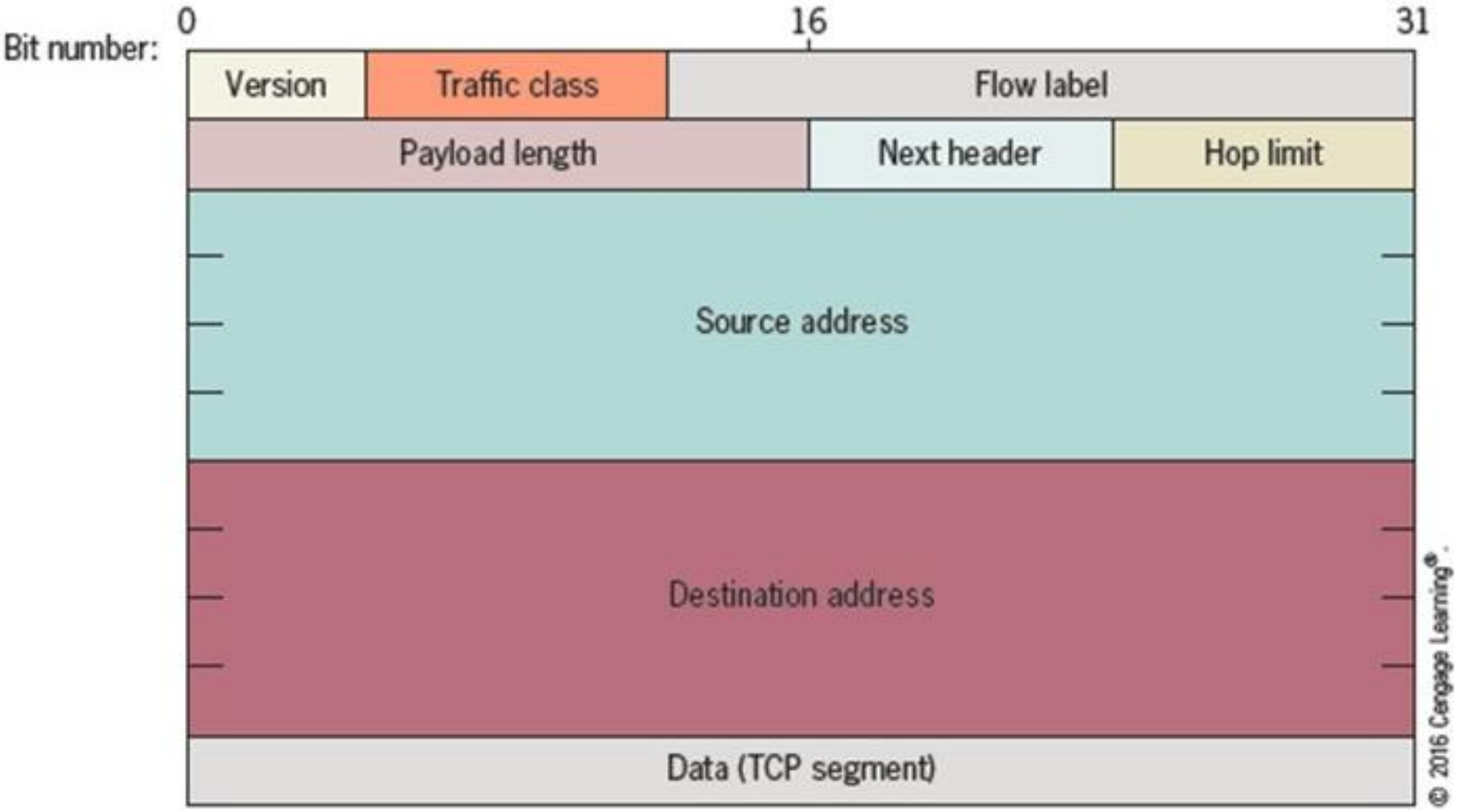
Options | Padding

Data (TCP segment)

Data

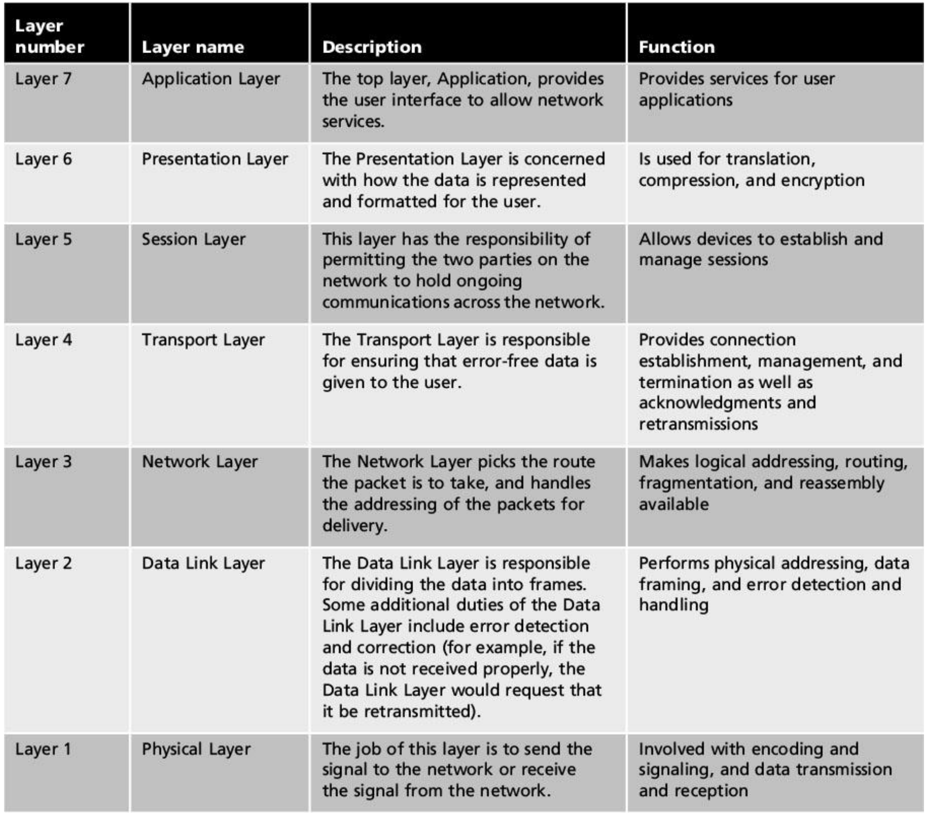
© 2016 Cengage Learning®.

IPv6-Packet



© 2016 Cengage Learning®.

Standard Network Devices



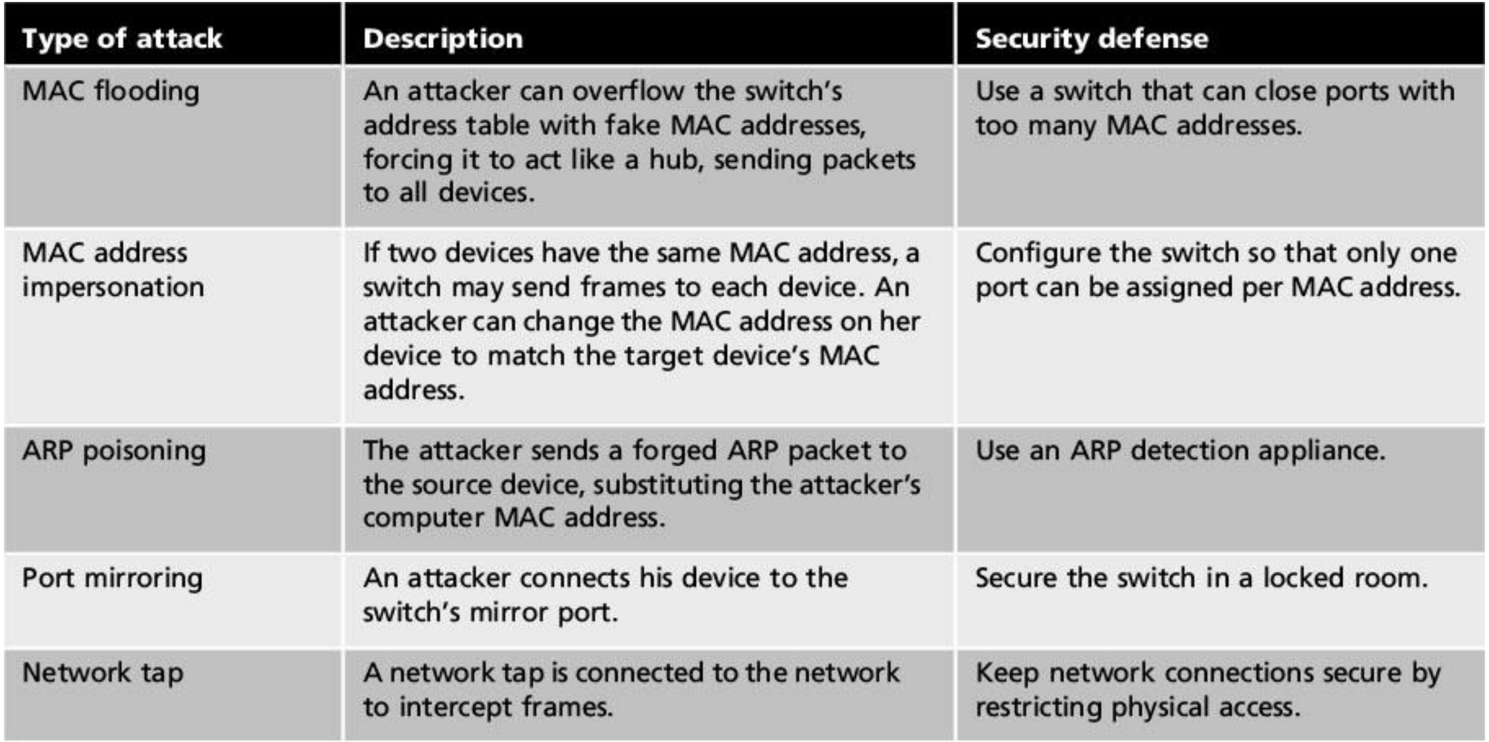
Layer number	Layer name	Description	Function
Layer 7	Application Layer	The top layer, Application, provides the user interface to allow network services.	Provides services for user applications
Layer 6	Presentation Layer	The Presentation Layer is concerned with how the data is represented and formatted for the user.	Is used for translation, compression, and encryption
Layer 5	Session Layer	This layer has the responsibility of permitting the two parties on the network to hold ongoing communications across the network.	Allows devices to establish and manage sessions
Layer 4	Transport Layer	The Transport Layer is responsible for ensuring that error-free data is given to the user.	Provides connection establishment, management, and termination as well as acknowledgments and retransmissions
Layer 3	Network Layer	The Network Layer picks the route the packet is to take, and handles the addressing of the packets for delivery.	Makes logical addressing, routing, fragmentation, and reassembly available
Layer 2	Data Link Layer	The Data Link Layer is responsible for dividing the data into frames. Some additional duties of the Data Link Layer include error detection and correction (for example, if the data is not received properly, the Data Link Layer would request that it be retransmitted).	Performs physical addressing, data framing, and error detection and handling
Layer 1	Physical Layer	The job of this layer is to send the signal to the network or receive the signal from the network.	Involved with encoding and signaling, and data transmission and reception

Table 7-1 **OSI reference model**

Switches

- A network switch is a device that connects network devices together
- Operates at Data Link Layer (Layer 2)
- Can determine which device is connected to each port
- Can forward frames sent to that specific device (unicast) or frames sent to all devices (broadcast)
- Uses MAC addresses to identify devices
- An attacker attached to a switch will see only frames that are directed to that device and not others
- Attackers could use a protocol analyzer to capture all packets
    - Protocol analyzers could decode and analyze packet contents

Protecting the switch



Type of attack	Description	Security defense
MAC flooding	An attacker can overflow the switch's address table with fake MAC addresses, forcing it to act like a hub, sending packets to all devices.	Use a switch that can close ports with too many MAC addresses.
MAC address impersonation	If two devices have the same MAC address, a switch may send frames to each device. An attacker can change the MAC address on her device to match the target device's MAC address.	Configure the switch so that only one port can be assigned per MAC address.
ARP poisoning	The attacker sends a forged ARP packet to the source device, substituting the attacker's computer MAC address.	Use an ARP detection appliance.
Port mirroring	An attacker connects his device to the switch's mirror port.	Secure the switch in a locked room.
Network tap	A network tap is connected to the network to intercept frames.	Keep network connections secure by restricting physical access.

Table 7-2 **Protecting the switch**

Routers & Load Balancers

- Routers
  - Forward packets across different computer networks
  - Operate at Network Layer (Layer 3)
  - Can be set to filter out specific types of network traffic
- Load balancers
  - Help evenly distribute work across a network
  - Can detect and stop attacks directed at a server or application
  - Can detect and prevent denial-of-service (DoS) and protocol attacks

Proxies

- Proxy server - a computer or an application program that intercepts user requests from the internal network and processes that request on behalf of the user.

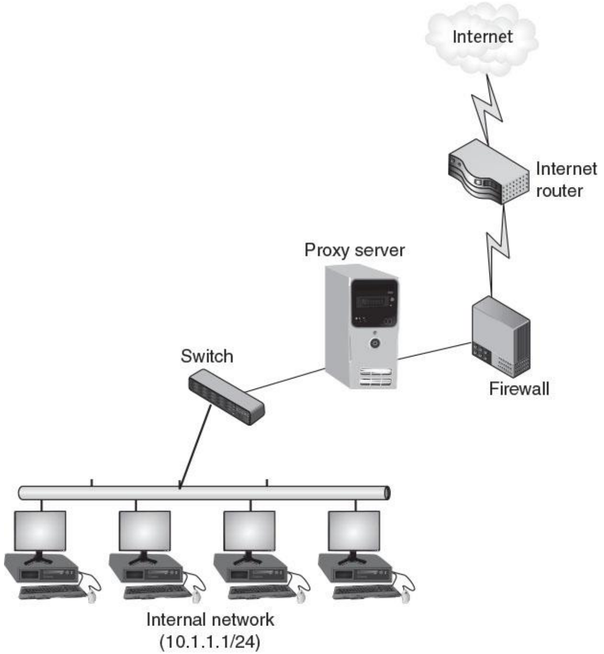


Figure 7-3 Proxy server

Network Security Hardware

- Specifically designed security hardware devices: Provide greater protection than standard networking devices
  - Network Firewalls
  - Spam filters
  - Virtual private network (VPN)
  - Intrusion detection system (IDS)
  - Intrusion Prevention System (IPS)
  - Unified Threat Management (UTM)

Network Security Hardware - Firewalls

- Network Firewalls: inspect packets and either accept or deny entry
  - Can be software-based or hardware-based
  - Hardware firewalls are usually located outside the network perimeter
- Methods of firewall packet filtering
  - *Stateless packet filtering*
    - Inspects incoming packet and permits or denies based on conditions set by administrator
  - *Stateful packet filtering*
    - Keeps a record of the state of a connection
    - Makes decisions based on the connection and conditions

Network Security Hardware - Firewalls

- Firewall actions on a packet
  - *Allow* (let packet pass through)
  - *Drop* (prevent the packet from passing into the network and send no response to sender)
  - *Reject* (prevent the packet from passing into the network but send a message to the sender)
- Rule-based firewalls
  - Use a set of individual instructions to control actions, called firewall rules
  - Each rule is a separate instruction processed in sequence telling the firewall what action to take
- Application-Aware Firewalls
  - Sometimes called a next-generation firewall (NGFW)
  - Operate at a higher level by identifying applications that send packets through the firewall and make decisions about actions to take
- Web application firewall
  - Special type of application-aware firewall that looks deeply into packets that carry HTTP traffic
  - Can block specific sites or specific types of HTTP traffic

Network Security Hardware - Spam filters

- Spam filters
  - Enterprise-wide spam filters block spam before it reaches the host
- Email systems use two protocols
  - Simple Mail Transfer Protocol (SMTP)
    - Handles outgoing mail
  - Post Office Protocol (POP)
    - Handles incoming mail

Network Security Hardware - Spam filters

- Spam filters installed on the POP3 server
  - All spam must first pass through SMTP server and be delivered to user's mailbox
  - Can result in increased costs
    - Storage, transmission, backup, deletion

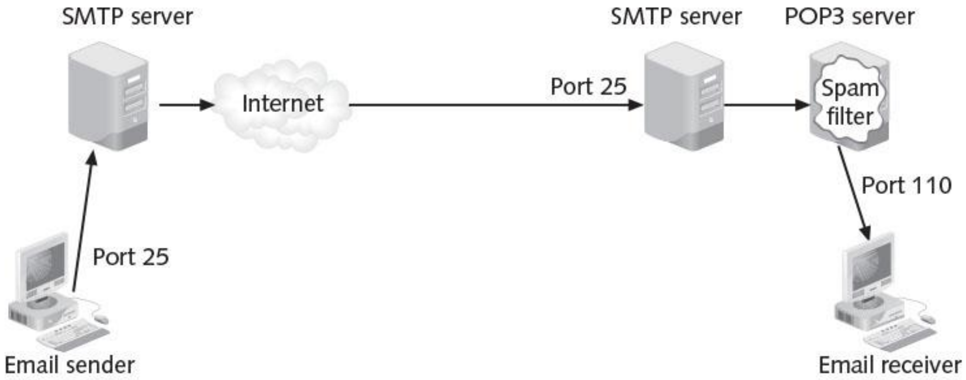


Figure 7-8 Spam filter on POP3 server

Network Security Hardware - VPN

- **Virtual private network (VPN)** - enables authorized users to use an unsecured public network as if it were a secure private network
  - All data transmitted between remote device and network is encrypted
- Endpoints
  - The end of the tunnel between VPN devices
- Tunneling protocols enclose a packet within another packet and are used for VPN transmissions
- A remote-access VPN generally uses either IPsec or the *Layer 2 Tunneling Protocol (L2TP)*

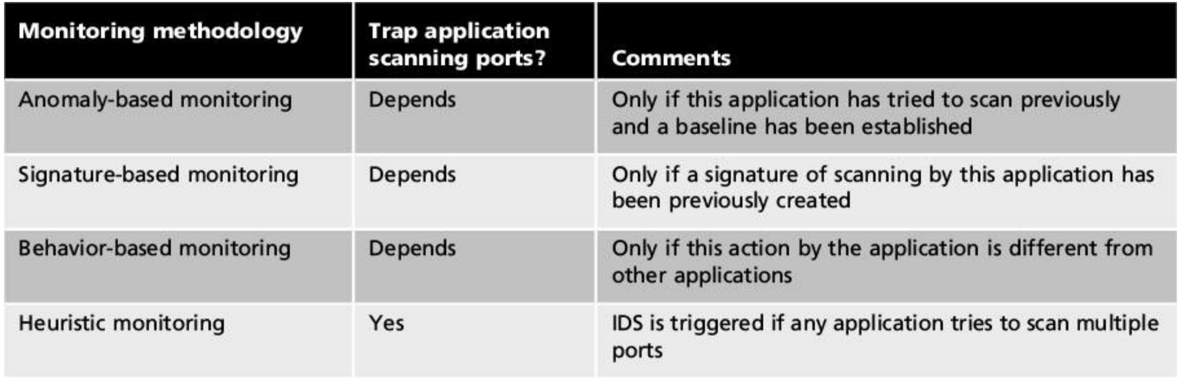
Network Security Hardware - IDS

- Intrusion detection system (IDS)
  - Can detect attack as it occurs
  - Can be installed on either local hosts or networks

- Intrusion Prevention System (IPS)
  - An extension of IDS is an intrusion prevention system (IPS)
  - Monitors network traffic to immediately block a malicious attack

Network Security Hardware

- Monitoring methodologies
  - Anomaly-based monitoring
    - Compares current detected behavior with baseline
  - Signature-based monitoring
    - Looks for well-known attack signature patterns
  - Behavior-based monitoring
    - Detects abnormal actions by processes or programs
    - Alerts user who decides whether to allow or block activity
  - Heuristic monitoring
    - Uses experience-based techniques



Monitoring methodology	Trap application scanning ports?	Comments
Anomaly-based monitoring	Depends	Only if this application has tried to scan previously and a baseline has been established
Signature-based monitoring	Depends	Only if a signature of scanning by this application has been previously created
Behavior-based monitoring	Depends	Only if this action by the application is different from other applications
Heuristic monitoring	Yes	IDS is triggered if any application tries to scan multiple ports

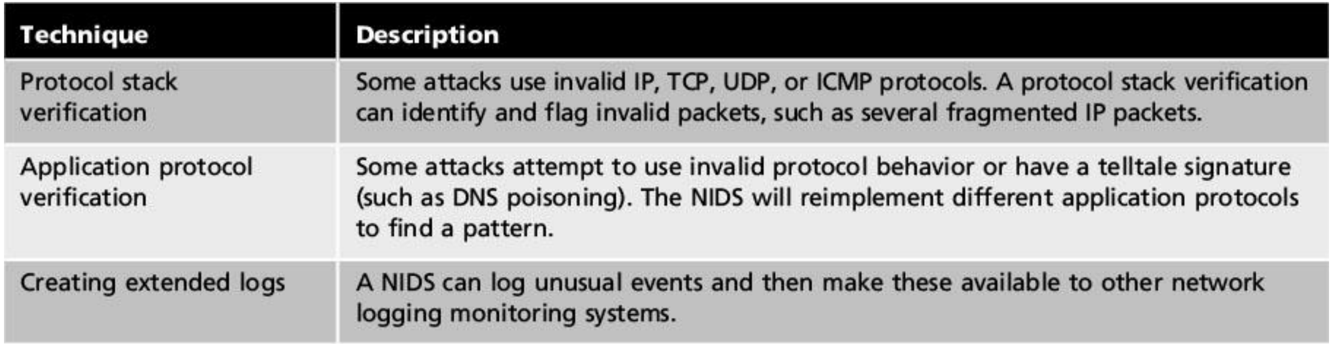
Table 7-4 Methodology comparisons to trap port scanning application

Network Security Hardware

- Types of IDS - two basic types if IDS exist
- Host intrusion detection system (HIDS)
  - A software-based application that can detect an attack as it occurs
  - Installed on each system needing protection
  - Monitors:
    - System calls and file system access
    - Can recognize unauthorized Registry modification
    - Host input and output communications
      - Detects anomalous activity
  - Disadvantages of HIDS
    - Cannot monitor network traffic that does not reach local system
    - All log data is stored locally
    - Resource-intensive and can slow system

Network Security Hardware - NIDS

- Network intrusion detection system (NIDS)
  - Watches for attacks on the network
  - NIDS sensors installed on firewalls and routers:
    - Gather information and report back to central device
  - Passive NIDS will sound an alarm
  - An NIDS may use one or more of the evaluation techniques listed in Table 7-5



Technique	Description
Protocol stack verification	Some attacks use invalid IP, TCP, UDP, or ICMP protocols. A protocol stack verification can identify and flag invalid packets, such as several fragmented IP packets.
Application protocol verification	Some attacks attempt to use invalid protocol behavior or have a telltale signature (such as DNS poisoning). The NIDS will reimplement different application protocols to find a pattern.
Creating extended logs	A NIDS can log unusual events and then make these available to other network logging monitoring systems.

Table 7-5 **NIDS evaluation techniques**

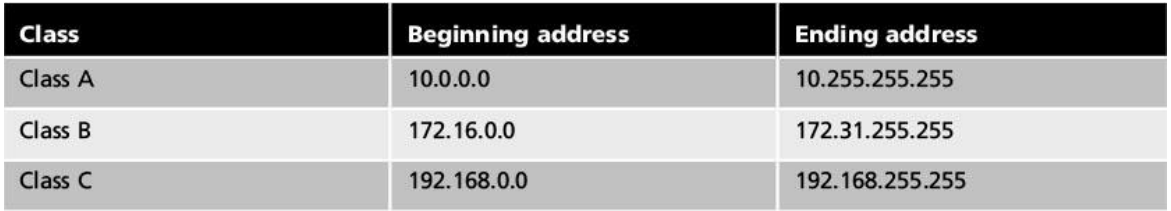
Network Security Hardware - Unified Threat Management

- Unified Threat Management (UTM) Security Appliances
  - Network hardware that provides multiple security functions, such as:
    - Antispam, antiphishing, antivirus, and antispyware
    - Bandwidth optimization
    - Content filtering
    - Encryption
    - Firewall
    - Instant messaging control and web filtering
    - Intrusion protection

Security Through Network Technologies

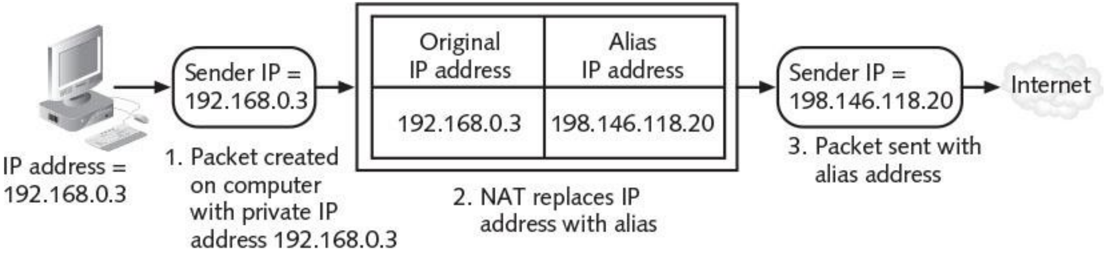
- Internet routers normally drop packet with a private address
- Network address translation (NAT)
  - Allows private IP addresses to be used on the public Internet
  - Replaces private IP address with public address
- Advantage of NAT
  - Masks IP addresses of internal devices
  - An attacker who captures the packet on the Internet cannot determine the actual IP address of sender
- Port address translation (PAT)
  - Variation of NAT
    - Outgoing packets given same IP address but different TCP port number

Security Through Network Technologies



Class	Beginning address	Ending address
Class A	10.0.0.0	10.255.255.255
Class B	172.16.0.0	172.31.255.255
Class C	192.168.0.0	192.168.255.255

Table 7-6 **Private IP addresses**



IP address = 192.168.0.3

Sender IP = 192.168.0.3

1. Packet created on computer with private IP address 192.168.0.3

Original IP address	Alias IP address
192.168.0.3	198.146.118.20

2. NAT replaces IP address with alias

Sender IP = 198.146.118.20

3. Packet sent with alias address

Figure 7-9 Network address translation (NAT)

Security Through Network Design Elements

- Elements of a secure network design
    - Demilitarized zones
    - Subnetting
    - Virtual LANs
    - Remote access

Demilitarized Zone (DMZ)

- DMZ - a separate network located outside secure network perimeter
- Untrusted outside users can access DMZ but not secure network

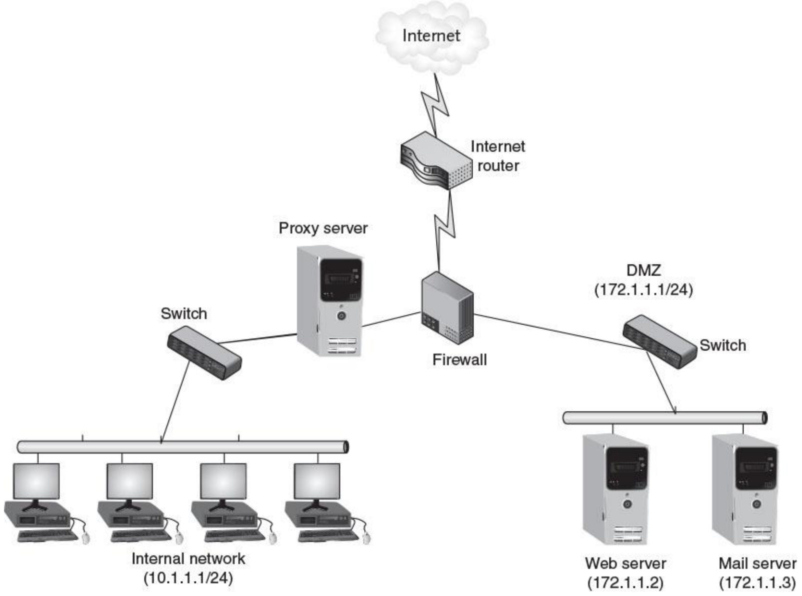
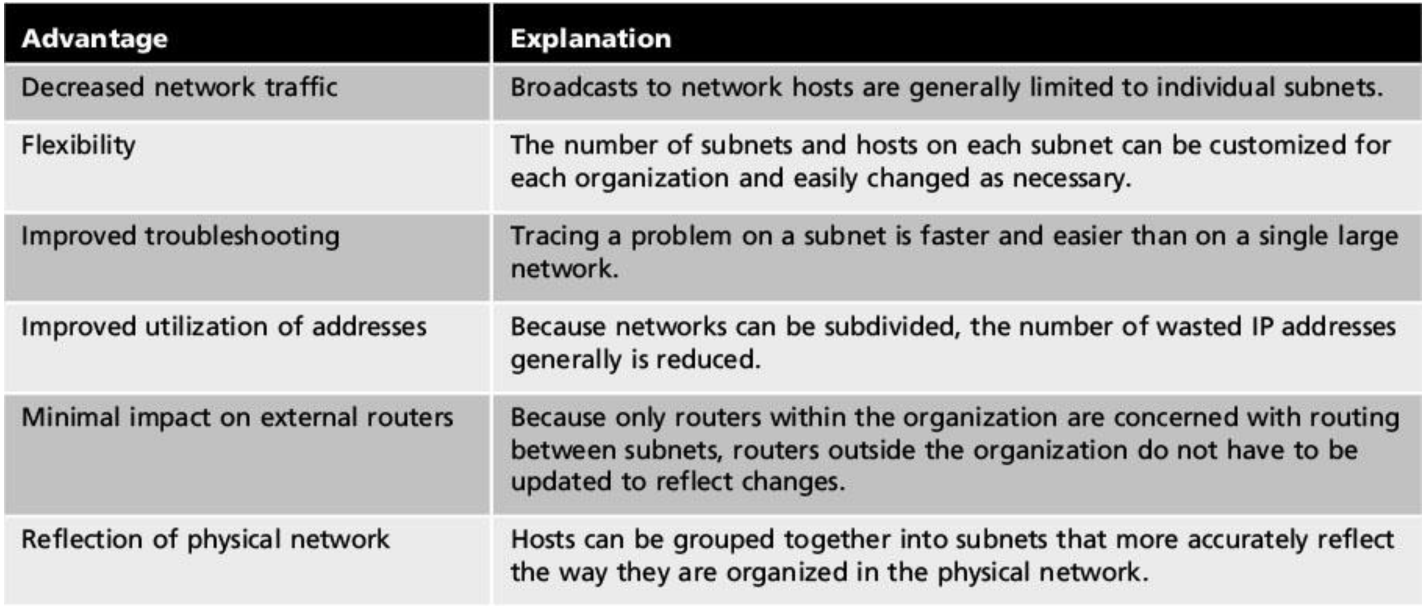


Figure 7-11 DMZ with one firewall

Subnetting

- An IP address is used to identify a network and a host on that network
    - One part is a network address and one part is a host address
- Subnetting allows a large network to be divided into smaller subnets
- Each network can contain several subnets
- Each subnet can contain multiple hosts
- Improves network security by isolating groups of hosts
- Administrators can utilize network security tools to make it easier to regulate who has access in and out of a particular subnetwork
- Allows network administrators to hide the internal network layout
    - Makes it more difficult for attackers to target their attacks

Subnetting



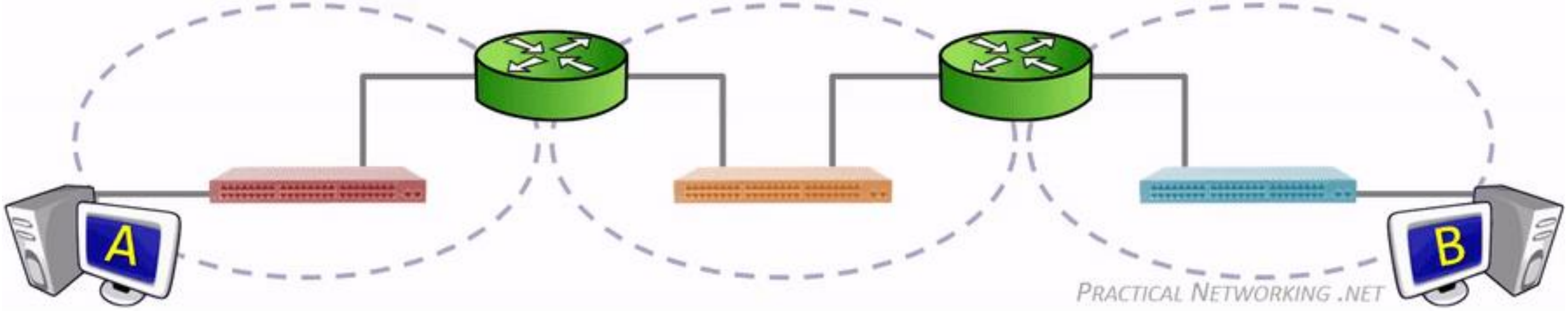
Advantage	Explanation
Decreased network traffic	Broadcasts to network hosts are generally limited to individual subnets.
Flexibility	The number of subnets and hosts on each subnet can be customized for each organization and easily changed as necessary.
Improved troubleshooting	Tracing a problem on a subnet is faster and easier than on a single large network.
Improved utilization of addresses	Because networks can be subdivided, the number of wasted IP addresses generally is reduced.
Minimal impact on external routers	Because only routers within the organization are concerned with routing between subnets, routers outside the organization do not have to be updated to reflect changes.
Reflection of physical network	Hosts can be grouped together into subnets that more accurately reflect the way they are organized in the physical network.

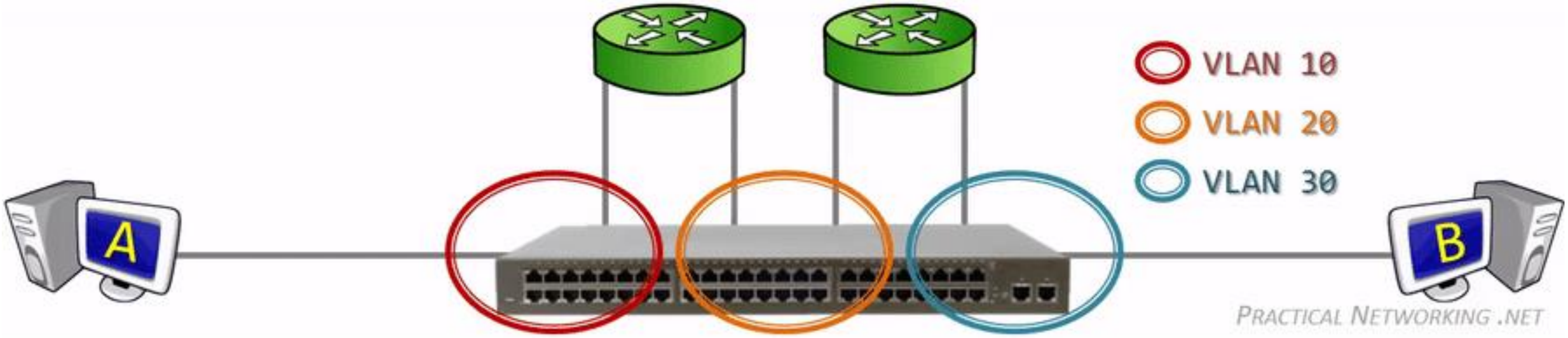
Table 7-7 **Advantages of subnetting**

Virtual LANs (VLAN)

- Allow scattered users to be logically grouped together
  - Even if attached to different switches
- Can isolate sensitive data to VLAN members
- Communication on a VLAN
  - If connected to same switch, switch handles packet transfer
  - A special “tagging” protocol is used for communicating between switches

Virtual LANs (VLAN)





Remote Access

- Remote Access
  - Any combination of hardware and software that enables remote users to access a local internal network
  - Provides same the functionality as local users through a VPN or dial-up connection