UNIVERSITI TEKNIKAL MALAYSIA MELAKA

Fakulti Teknologi Maklumat dan Komunikasi

Network Security Administration and Management

BITS 3353

Lecture 9: Administering a Secure Network

Objectives

- List and describe the functions of common network protocols
- Explain how network administration principles can be applied
- Define the new types of network applications and how they can be secured

Common Network Protocols

PROTOCOLS

- Rules of conduct and communication
- Essential for proper communication between network devices

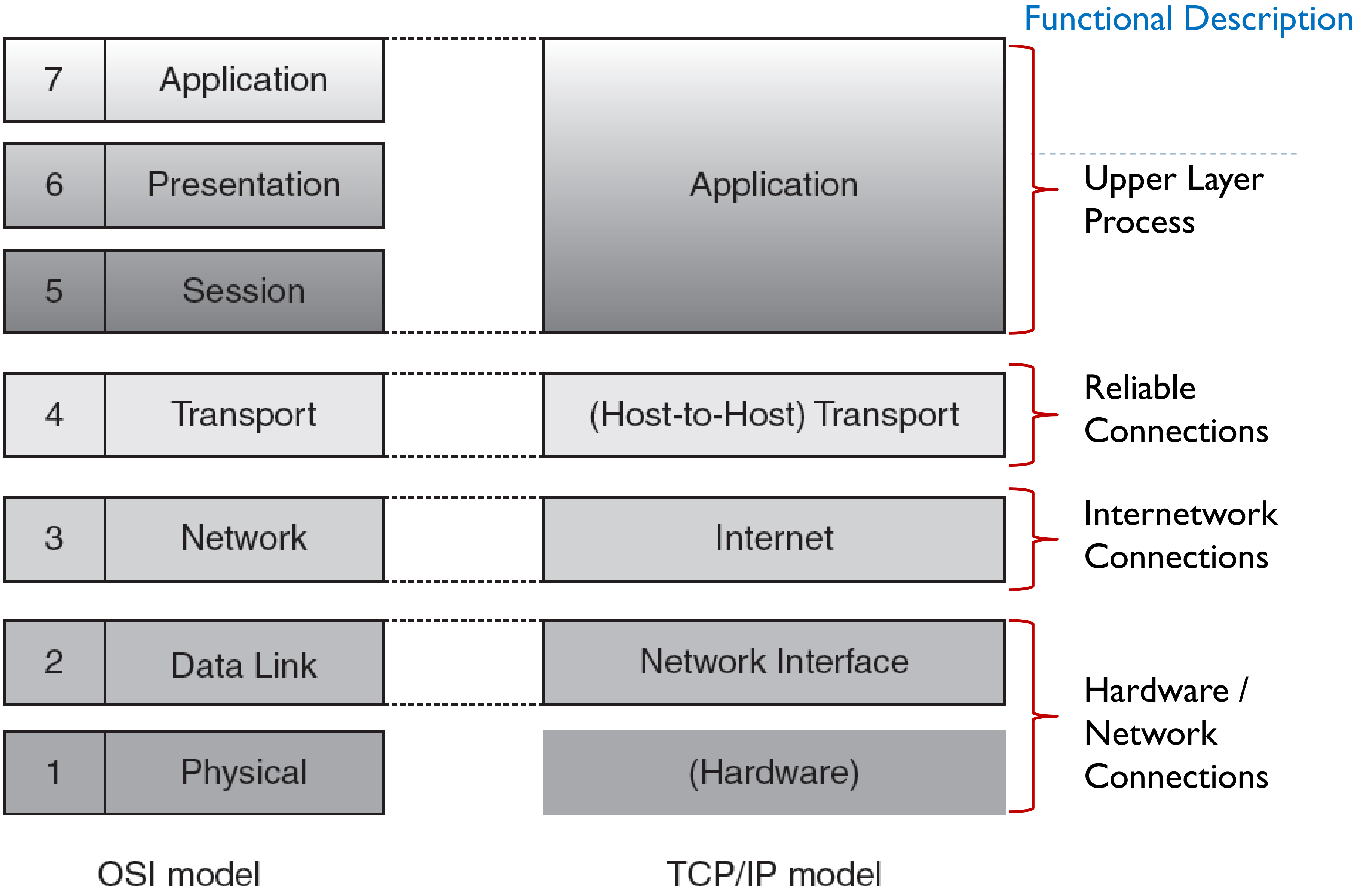
Most common protocol suite used for local area networks and the Internet

- Transport Layer (Layer 4) protocol
- Establishes connections and reliable data transport between devices

Transmission Control Protocol/Internet Protocol (TCP/IP)

- Protocol that functions primarily at Open Systems Interconnection (OSI) Network Layer (Layer 3)

TCP/IP uses a four layer architecture –Network Interface, Internet, Transport, Application



OSI model		TCP/IP model	Functional Description
7	Application	Application	Upper Layer Process
6	Presentation		
5	Session		
4	Transport	(Host-to-Host) Transport	Reliable Connections
3	Network	Internet	Internetwork Connections
2	Data Link	Network Interface	Hardware / Network Connections
1	Physical	(Hardware)	

OSI model vs. TCP/IP model

Internet Control Message Protocol (ICMP)

- One of the core protocols of TCP/IP
- communications between devices

Informational and query messages

- These messages are used for devices to exchange information and perform testing.
- Generated either by an application or simply on a regular basis by devices to provide information to other devices.

Error messages

- Provide feedback to another device about an error that has occurred. These messages can be sent as the result of basic errors (such as a requested service is not available or that a device cannot be reached) or more advanced situations (such as a web security gateway does not have sufficient buffering capacity to forward a packet).

Internet Control Message Protocol (ICMP)

ICMP message fields

–Type (8-bit)

•Identifies general message category

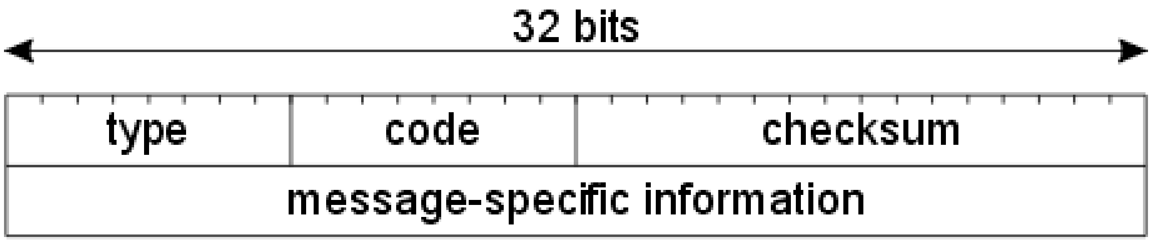
–Code (8-bit)

•Gives additional information about the Type field

–Checksum (16-bit)

•Verifies message integrity

ICMP packet format



32 bits

type	code	checksum
message-specific information		

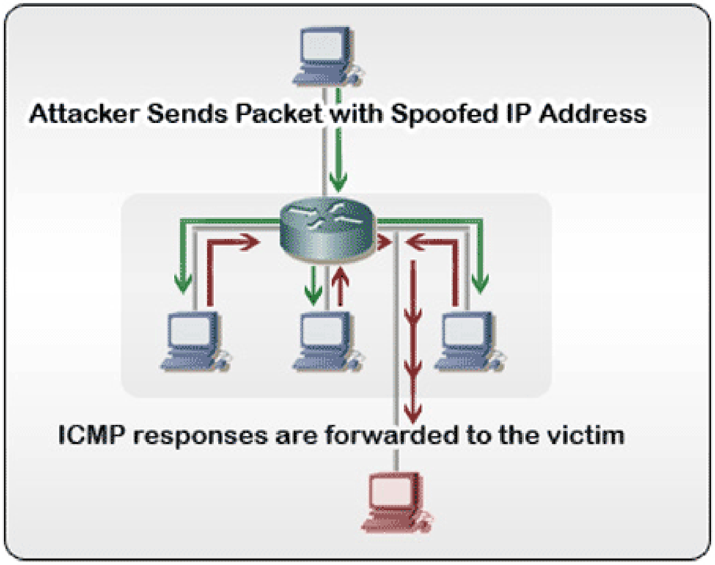
Internet Control Message Protocol (ICMP)

Attacks that are associated with ICMP:

•Network discovery - the attacker sends packets that request information about a network. Not an attack as much as information gathering for an attacker.

•Smurf attack - the attacker sends ping requests (ICMP echo requests) to as many devices as possible, coding the requests so that the replies will all hit and flood a target machine, typically a server

Smurf Attack

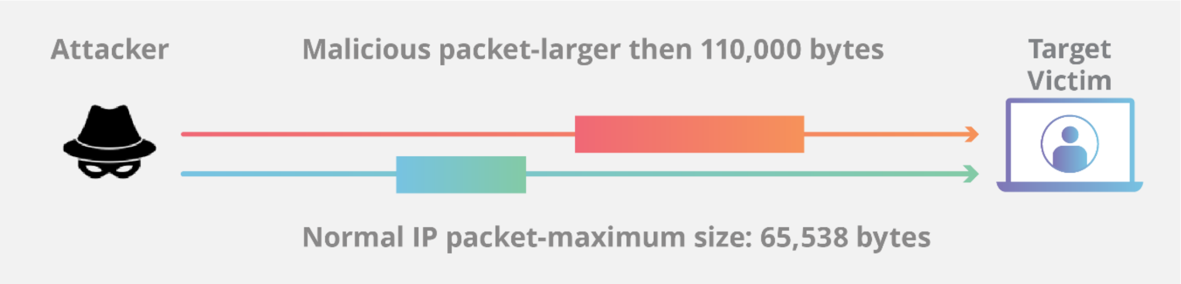

Attacker Sends Packet with Spoofed IP Address
ICMP responses are forwarded to the victim

Internet Control Message Protocol (ICMP)

Attacks that are associated with ICMP:

•ICMP redirect - the attacker sends a request to a device, asking it to send all traffic to a device of the attacker's choice

•Ping of death - the attacker sends an ICMP packet that is larger than the largest size allowed for packets on a given network; the target device might crash, or might just be knocked off the network; this kind of attack should not work any longer


Attacker
Malicious packet-larger then 110,000 bytes
Target Victim
Normal IP packet-maximum size: 65,538 bytes

Simple Network Management Protocol (SNMP)

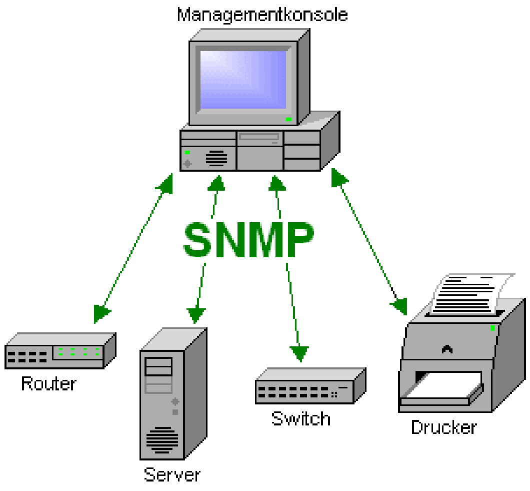
- First introduced in 1988
- Supported by most network equipment manufacturers
- Allows administrators to remotely monitor, manage, and configure network devices
- Functions by exchanging management information between network devices
- Each SNMP-managed device has an agent or service

  -Listens for and executes commands
- Agents are password protected

  -Password is known as community string
- Security vulnerabilities were present in SNMP versions 1 and 2

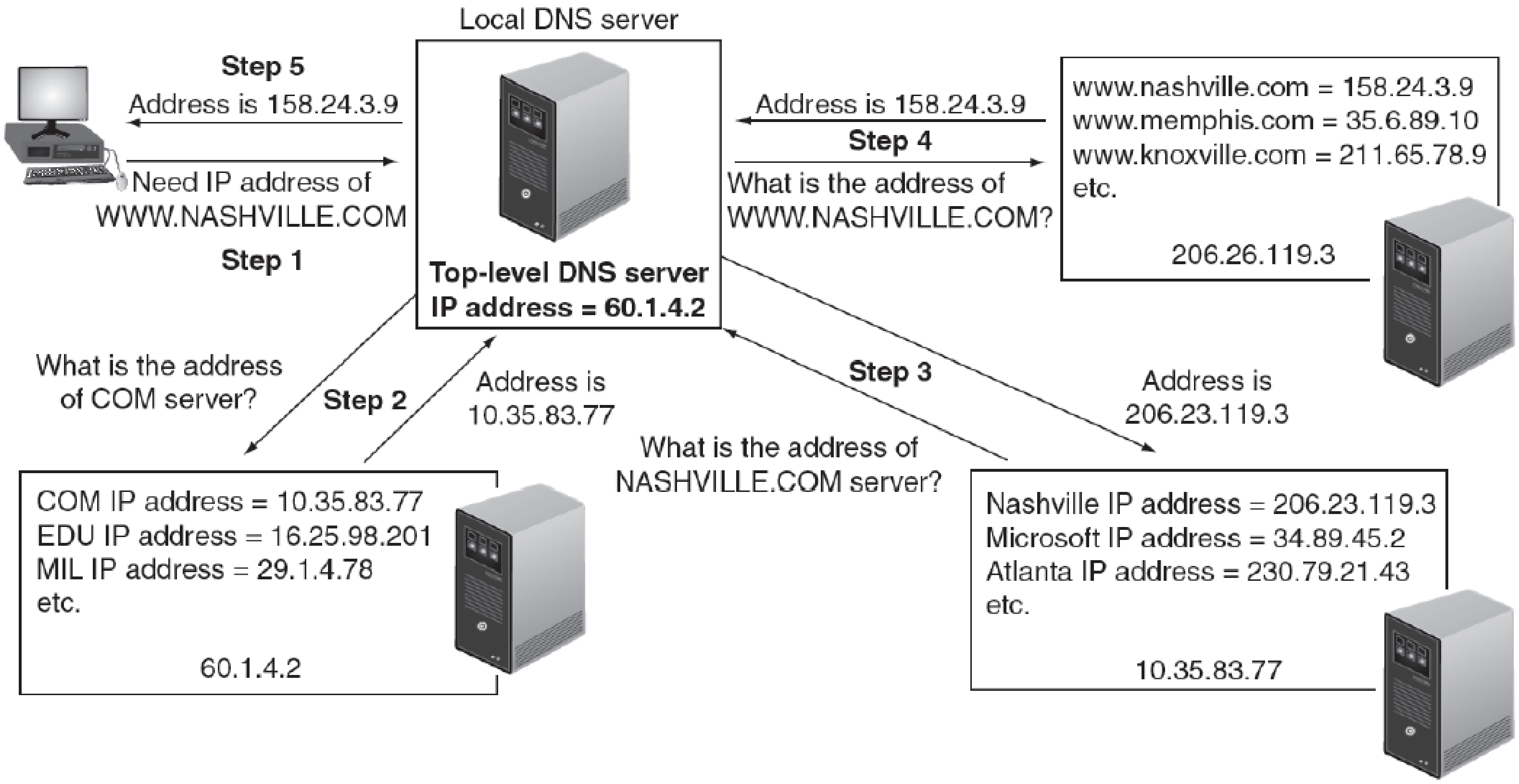
  -Version 3 introduced in 1998

  -Uses usernames and passwords along with encryption to address vulnerabilities



Domain Name System (DNS)

- A TCP/IP protocol that maps IP addresses to their symbolic name
- Database with name of each site and corresponding IP number
- Database is distributed to many different servers on the Internet



Domain Name System (DNS)

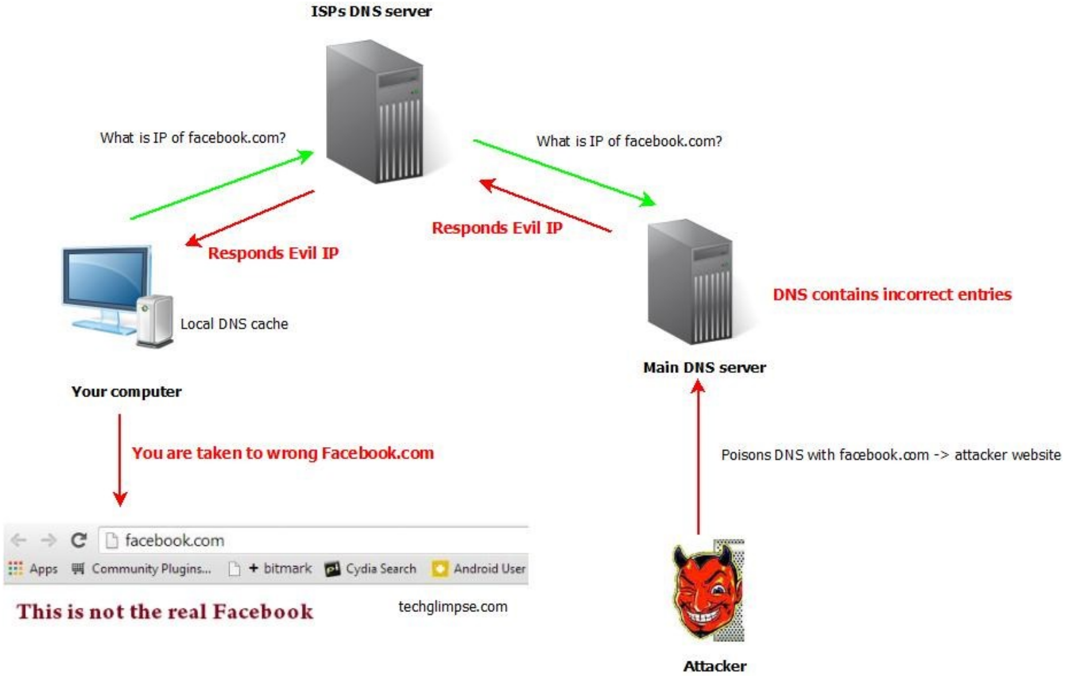
DNS can be the focus of attacks:

DNS poisoning

- substitutes fraudulent IP address

DNS transfer

- the attacker asks a DNS server for a copy of its database, which provides the attacker with information about the addresses, devices, and software used in the server's network


ISPs DNS server
What is IP of facebook.com?
What is IP of facebook.com?
Responds Evil IP
Responds Evil IP
DNS contains incorrect entries
Local DNS cache
Main DNS server
Your computer
You are taken to wrong Facebook.com
Poisons DNS with facebook.com -> attacker website
facebook.com
Apps
Community Plugins...
+ bitmark
Cydia Search
Android User
This is not the real Facebook
techglimpse.com
Attacker

File Transfer Protocols

TCP/IP protocols used for transferring files

- File transfer protocol (FTP)

  - standard protocol for transferring files between computing system; require user authentication but no encryption

  - unsecure protocol used to connect to an FTP server

Methods for using FTP on local host computer
–Command prompt
–Web browser
–FTP client

FTP vulnerabilities
–Does not use encryption
–Files transferred using FTP vulnerable to man-in-the-middle attacks

Secure transmission options over FTP

- Secure sockets layer **(FTPS)** encrypts commands
  - Uses SSL or TLS to encrypt commands sent over the control port (port 21); data port may not be encrypted
- Secure FTP **(SFTP)**
  - uses one single TCP port (typically port 22)
  - All commands and data are encrypted

Secure Copy Protocols (SCP)

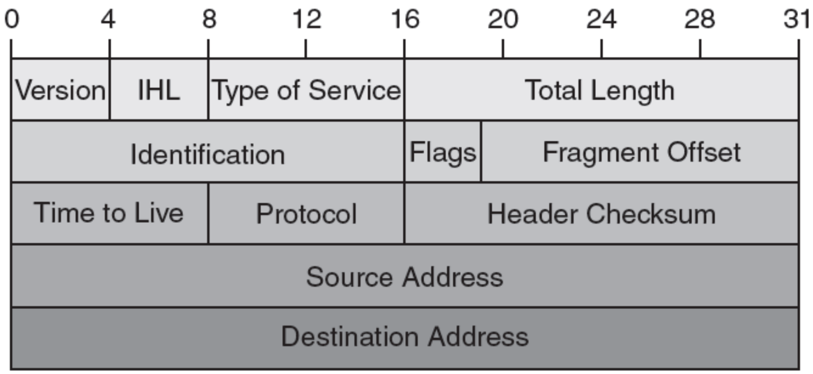
–Enhanced version of Remote Copy Protocol
–Encrypts files and commands
–File transfer cannot be interrupted and resumed
–Found mainly on Linux and UNIX platforms

IPv6

- Current version of IP protocol is version 4 (IPv4)
  - Developed in 1981
  - Number of available IP address is limited to 4.3 billion
    - Number of internet connected devices will grow beyond this number
  - Has security weaknesses
- Internet Protocol version 6 (IPv6)
  - Next generation of IP protocol
  - Addresses weaknesses of IPv4
  - Provides enhanced security features
    - Cryptographic protocols
    - New authentication headers prevent IP packets from being altered

IPv6

IPv4 Header



0 4 8 12 16 20 24 28 31

Version | IHL | Type of Service | Total Length

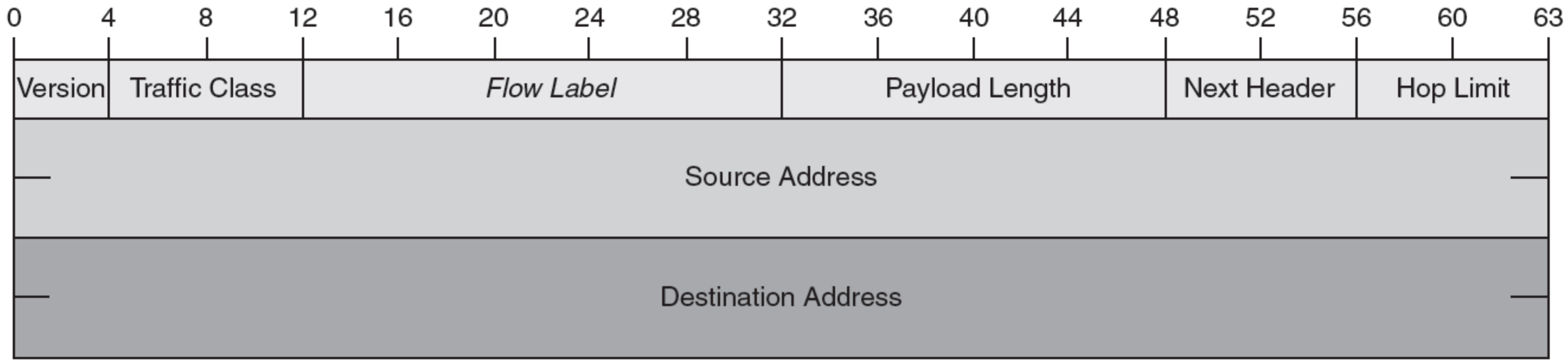
Identification | Flags | Fragment Offset

Time to Live | Protocol | Header Checksum

Source Address

Destination Address

IPv6 Header



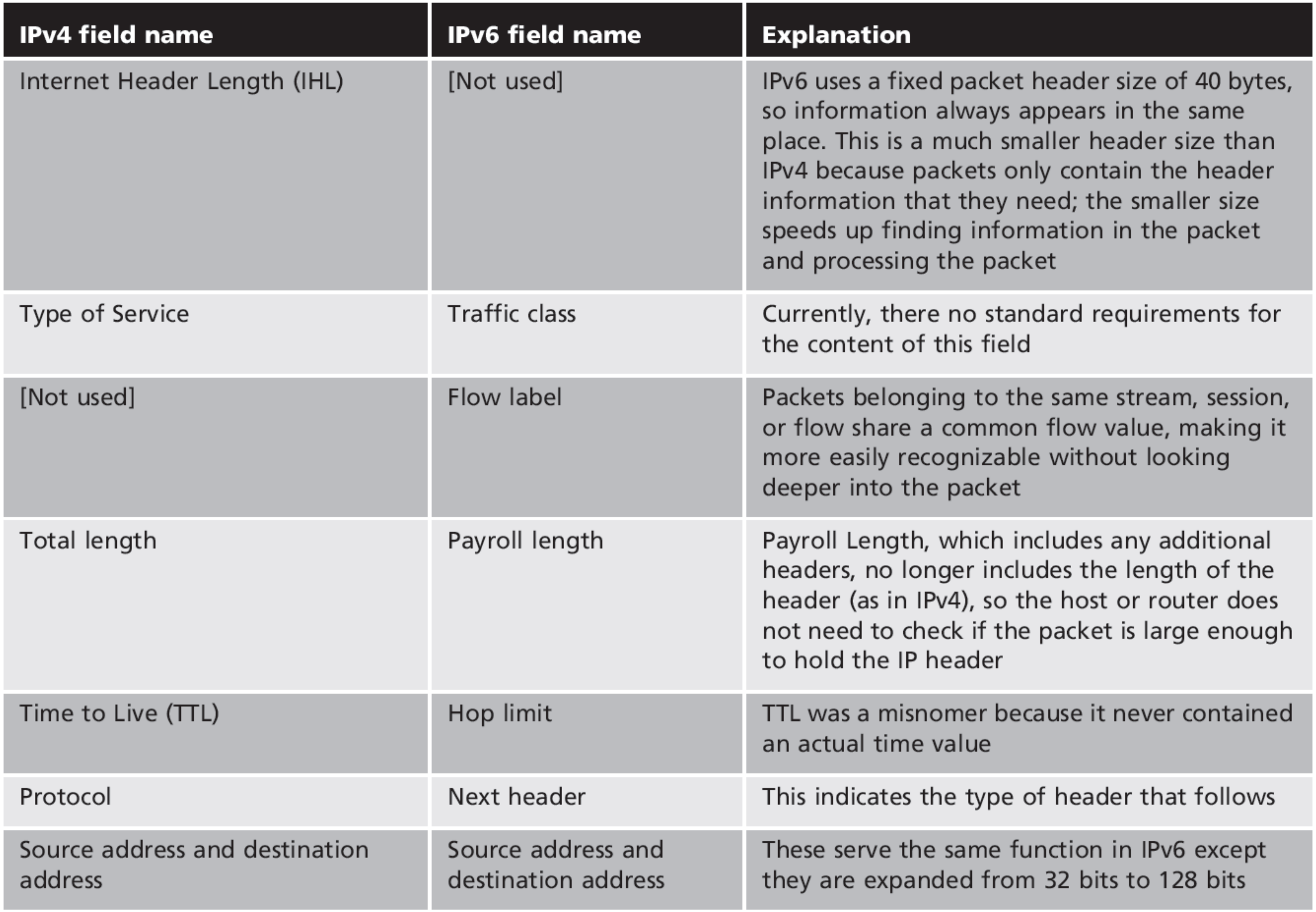
0 4 8 12 16 20 24 28 32 36 40 44 48 52 56 60 63

Version | Traffic Class | *Flow Label* | Payload Length | Next Header | Hop Limit

Source Address

Destination Address

IPv6



IPv4 field name	IPv6 field name	Explanation
Internet Header Length (IHL)	[Not used]	IPv6 uses a fixed packet header size of 40 bytes, so information always appears in the same place. This is a much smaller header size than IPv4 because packets only contain the header information that they need; the smaller size speeds up finding information in the packet and processing the packet
Type of Service	Traffic class	Currently, there no standard requirements for the content of this field
[Not used]	Flow label	Packets belonging to the same stream, session, or flow share a common flow value, making it more easily recognizable without looking deeper into the packet
Total length	Payroll length	Payroll Length, which includes any additional headers, no longer includes the length of the header (as in IPv4), so the host or router does not need to check if the packet is large enough to hold the IP header
Time to Live (TTL)	Hop limit	TTL was a misnomer because it never contained an actual time value
Protocol	Next header	This indicates the type of header that follows
Source address and destination address	Source address and destination address	These serve the same function in IPv6 except they are expanded from 32 bits to 128 bits

Network Administration Principles

- Administering a secure network can be challenging
- Successful management is often based on rules
- Rule-based management approach
- Relies on following procedures and rules

Procedural Rules

- Rules may be external (applicable laws) or internal
- Procedural rules dictate technical rules

Technical Rules

•Device security

•Network management and port security

•Example: configuring a firewall to conform to procedural rules

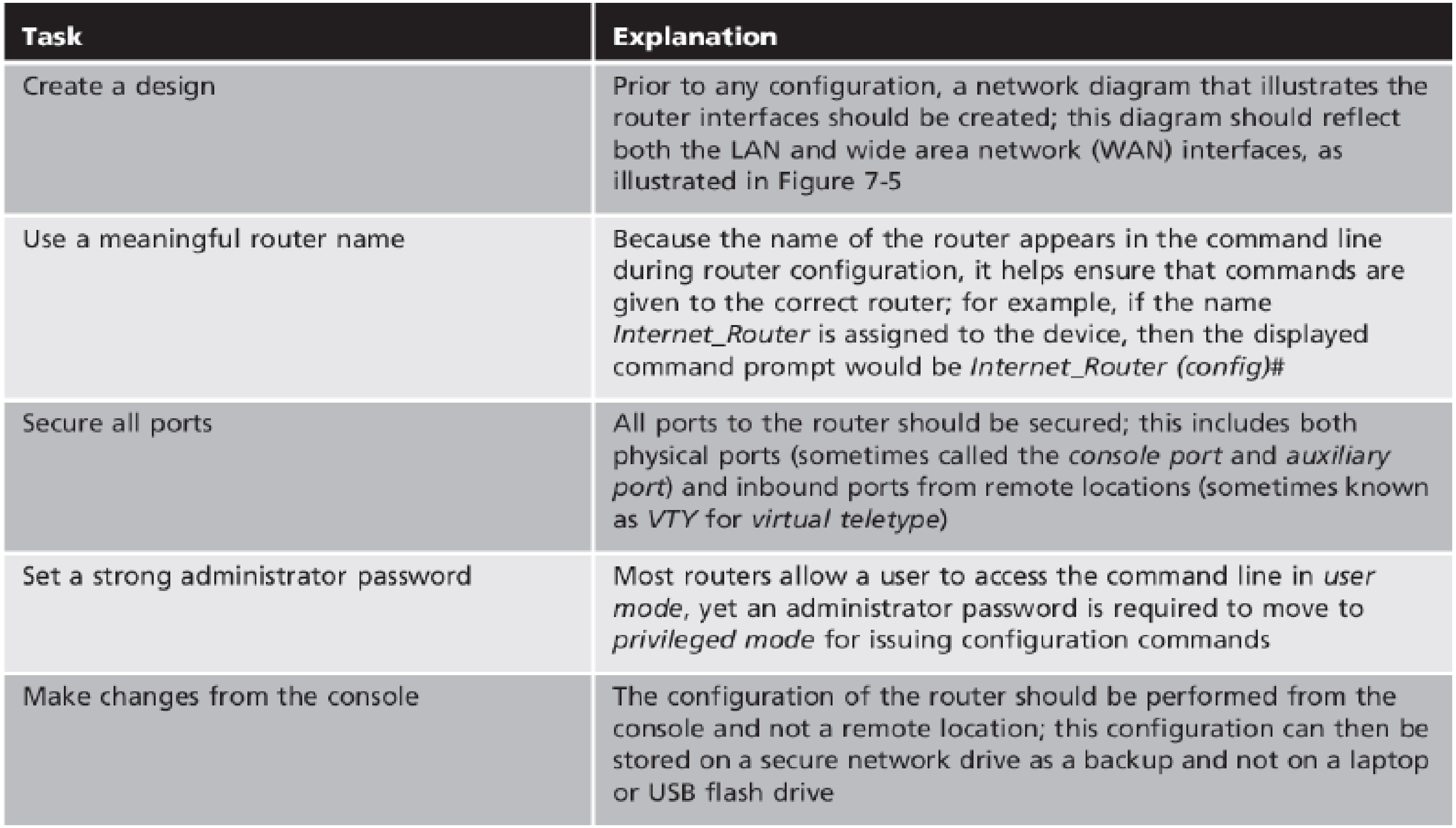
Device Security

1 Establishing a secure router configuration

2 Implementing flood guards

Device Security: Secure router configuration

- Router operates at Network Layer (Layer 3)
  - Forwards packets across computer networks
- Routers can perform a security function
  - Can be configured to filter out specific types of network traffic



Task	Explanation
Create a design	Prior to any configuration, a network diagram that illustrates the router interfaces should be created; this diagram should reflect both the LAN and wide area network (WAN) interfaces, as illustrated in Figure 7-5
Use a meaningful router name	Because the name of the router appears in the command line during router configuration, it helps ensure that commands are given to the correct router; for example, if the name *Internet_Router* is assigned to the device, then the displayed command prompt would be *Internet_Router (config)#*
Secure all ports	All ports to the router should be secured; this includes both physical ports (sometimes called the *console port* and *auxiliary port*) and inbound ports from remote locations (sometimes known as *VTY* for *virtual teletype*)
Set a strong administrator password	Most routers allow a user to access the command line in *user mode*, yet an administrator password is required to move to *privileged mode* for issuing configuration commands
Make changes from the console	The configuration of the router should be performed from the console and not a remote location; this configuration can then be stored on a secure network drive as a backup and not on a laptop or USB flash drive

Secure router configuration tasks

Device Security: Flood guard

- Preventive control against denial-of-service (DoS) or distributed denial-of-service (DDoS) attacks.
- Flood guards are available either as standalone devices or as firewall components.
- It is capable of monitoring network traffic to identify DoS attacks in progress generated through packet

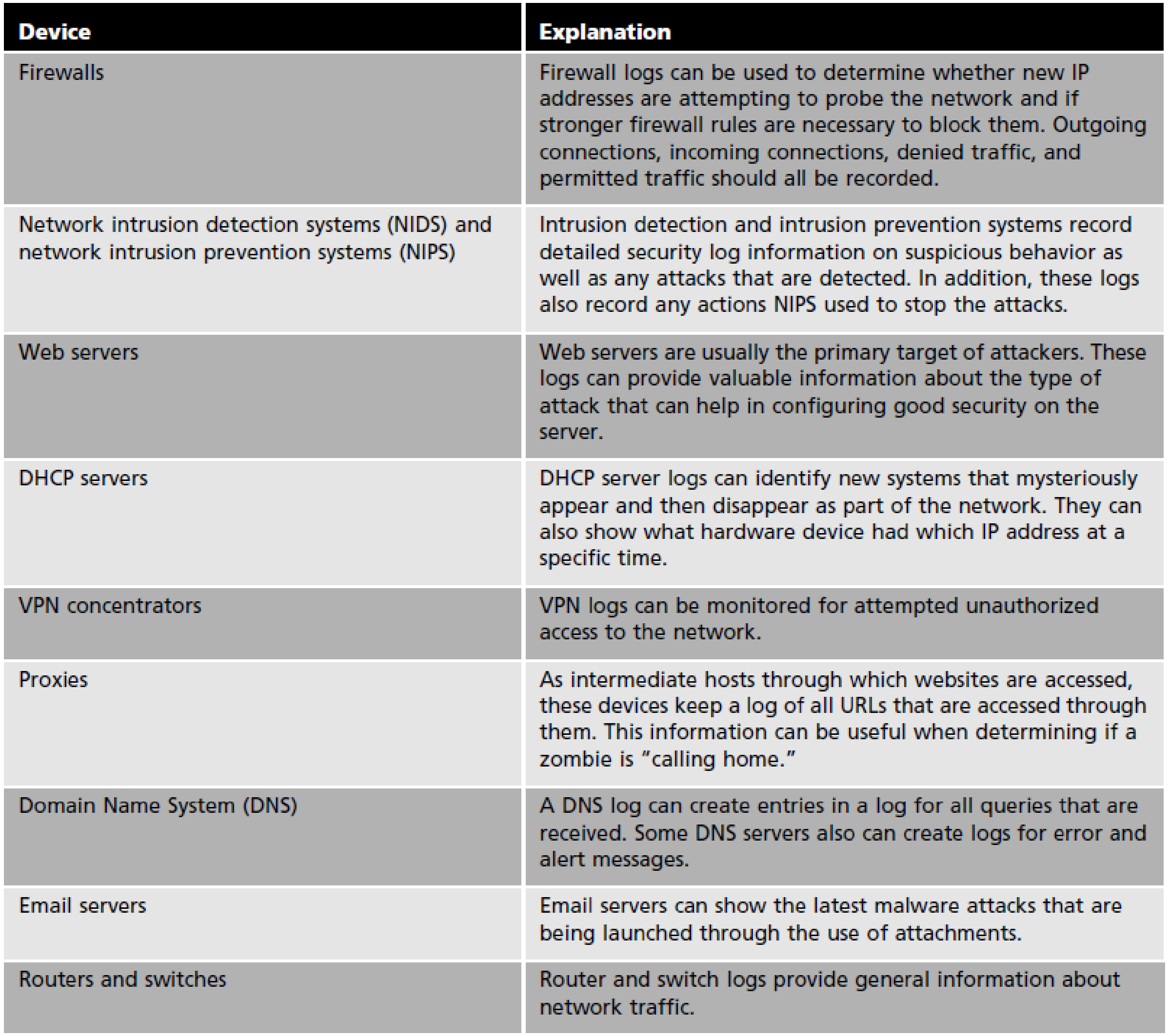
Monitoring and Analyzing Logs

- Log records events that occur
- Monitoring logs can be useful in determining how attack occurred
- A security **access lo**g can provide details regarding requests for specific files on a system
- **Audit log** is used to record which user performed an action and what that action was
- System **event logs** document any unsuccessful events and the most significant successful events
- Information that can be recorded might include the date and time of the event, a description of the event, its status, error codes, service name, and user or system that was responsible for launching the event.

Monitoring and Analyzing Logs

- Types of security hardware logs
  - –NIDS, NIPS, DNS, proxy servers, and firewalls
- Firewall log items to be examined
  - –IP addresses rejected and dropped
  - –Probes to ports that have no application servers on them
  - –Source-routed packets
  - –Suspicious outbound connections
  - –Unsuccessful logins

Monitoring and Analyzing Logs



Device	Explanation
Firewalls	Firewall logs can be used to determine whether new IP addresses are attempting to probe the network and if stronger firewall rules are necessary to block them. Outgoing connections, incoming connections, denied traffic, and permitted traffic should all be recorded.
Network intrusion detection systems (NIDS) and network intrusion prevention systems (NIPS)	Intrusion detection and intrusion prevention systems record detailed security log information on suspicious behavior as well as any attacks that are detected. In addition, these logs also record any actions NIPS used to stop the attacks.
Web servers	Web servers are usually the primary target of attackers. These logs can provide valuable information about the type of attack that can help in configuring good security on the server.
DHCP servers	DHCP server logs can identify new systems that mysteriously appear and then disappear as part of the network. They can also show what hardware device had which IP address at a specific time.
VPN concentrators	VPN logs can be monitored for attempted unauthorized access to the network.
Proxies	As intermediate hosts through which websites are accessed, these devices keep a log of all URLs that are accessed through them. This information can be useful when determining if a zombie is "calling home."
Domain Name System (DNS)	A DNS log can create entries in a log for all queries that are received. Some DNS servers also can create logs for error and alert messages.
Email servers	Email servers can show the latest malware attacks that are being launched through the use of attachments.
Routers and switches	Router and switch logs provide general information about network traffic.

Network Design Management

- To ensure that security and the viability of the network

Network Separation

- Provides separation between different parts of the network
  - –Example: order entry network segment cannot access human resources network

Network Design Management

VLAN Management

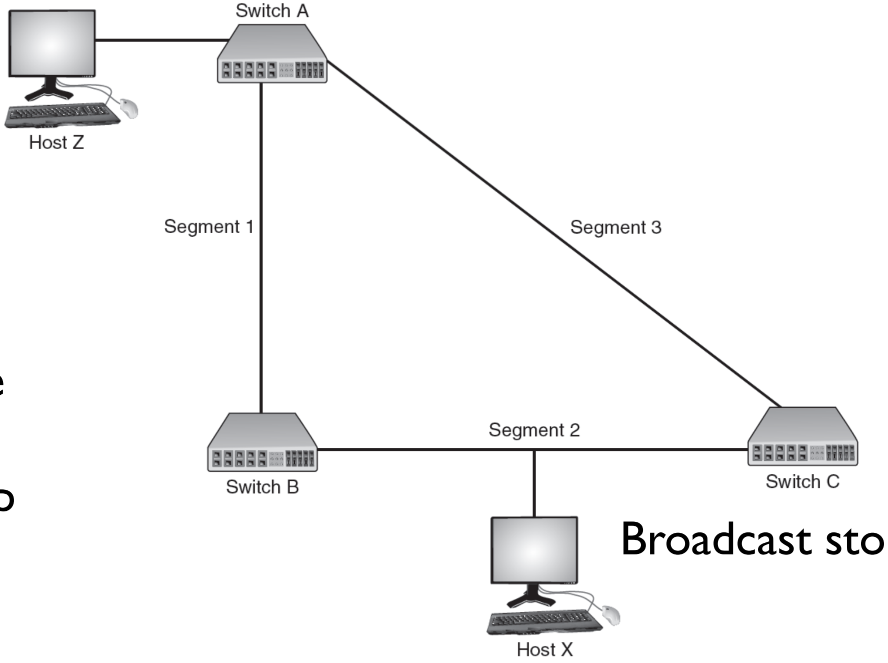
- Network may be segmented into logical groups of physical devices through VLAN
  - –Scattered users may be logically grouped together:
- Regardless of which switch they are attached to

General principles for managing VLANs
–A VLAN should not communicate with another VLAN unless they are both connected to a router
–Configure empty switch ports to connect to an unused VLAN
–Different VLANs should be connected to different switches
–Change any default VLAN names
–Configure switch ports that pass tagged VLAN packets to explicitly forward specific tags
–Configure VLANs so that public devices are not on a private VLAN

Network Design Management

Loop Protection

–Refer to Figure for description of broadcast storm
–Host Z wants to send frames to Host X
–Switch A floods network with the packet
–Packet travels down Segments 1 and 3 to the Switches B and C
–Switches B and C add Host Z to their lookup tables
–Both switches flood Segment 2 looking for Host X
•They receive each other's packets and flood them back out again



Broadcast storm

Broadcast storms can be prevented with loop protection, which uses the IEEE 802.1d standard spanning-tree algorithm (STA). STA can determine that a switch has multiple ways to communicate with a host and then determine the best path while blocking out other paths.

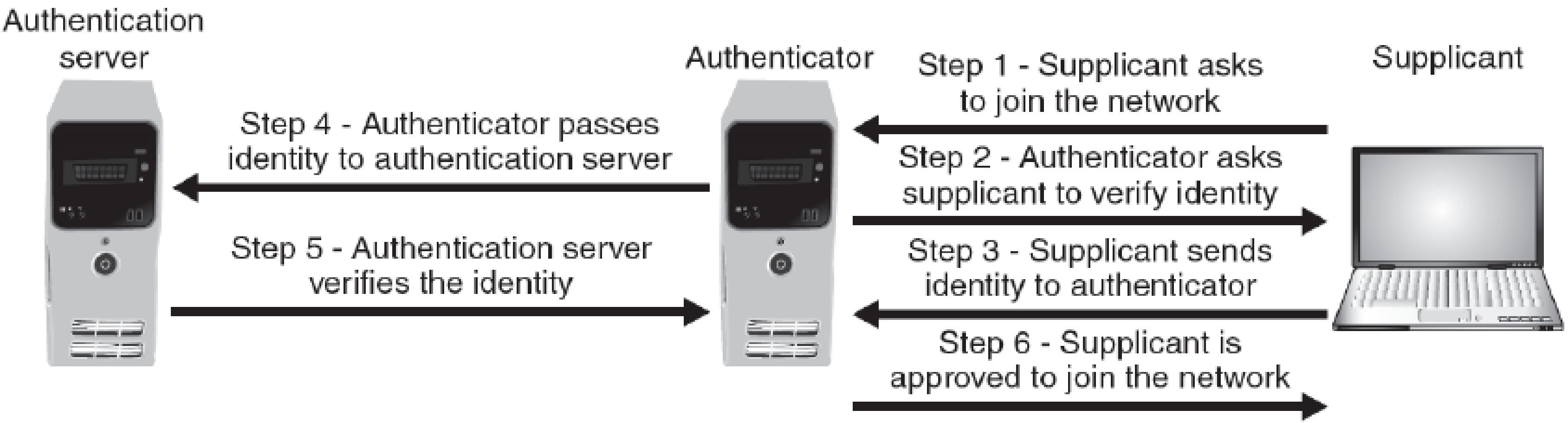
Port Security

- Disabling unused interfaces
  - –Turn off ports not required on a network
  - –Often overlooked security technique
  - –Switch without port security allows attackers to connect to unused ports and attack network
  - –All ports should be secured before switch is deployed
  - –Network administrator should issue shutdown command to each unused port

- MAC limiting and filtering
  - –Filters and limits number of media access control (MAC) addresses allowed on a port
  - –Port can be set to limit of 1
  - –Specific MAC address can be assigned to a port
    - •Enables only single authorized host to connect

Port Security

- IEEE 802.1x
  - –Standard that provides the highest degree of port security
  - –Implements port-based authentication
  - –Blocks all traffic on a port-by-port basis:
    - •Until client is authenticated


Authentication server
Authenticator
Supplicant
Step 1 - Supplicant asks to join the network
Step 2 - Authenticator asks supplicant to verify identity
Step 3 - Supplicant sends identity to authenticator
Step 4 - Authenticator passes identity to authentication server
Step 5 - Authentication server verifies the identity
Step 6 - Supplicant is approved to join the network

IEEE 802.1x process

Securing Network Applications

Some applications and platforms require special security considerations:

VIRTUALIZATION

IP TELEPHONY

CLOUD COMPUTING

Securing Network Applications:Virtualization

VIRTUALIZATION

managing and presenting computer resources without regard to physical layout or location

HOST VIRTUALIZATION

Virtual machine simulated as software environment on host system

ADVANTAGES

- Test latest patches by downloading on a virtual machine before installing on production computer
- Security control testing can be performed using simulated network environment
- Can be used for training purposes

Securing Network Applications: IP Telephony

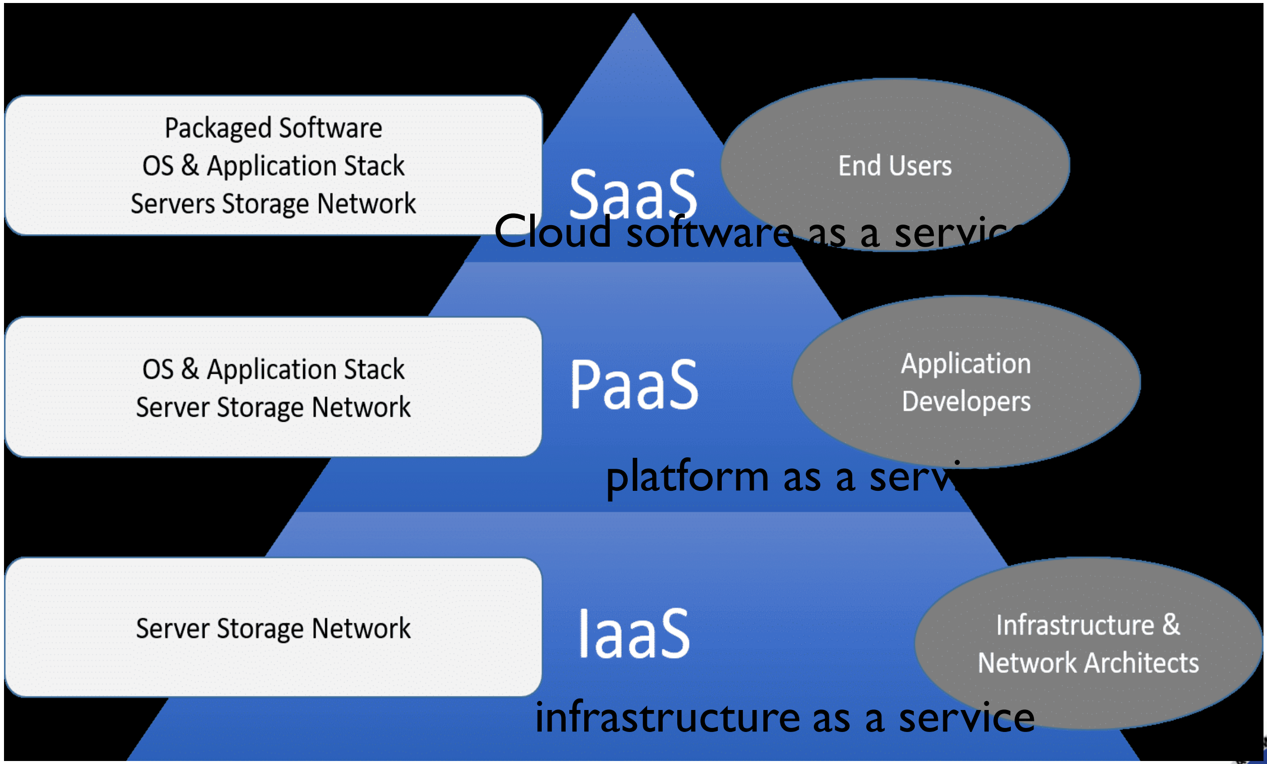
- Shift to all digital technology infrastructure is underway
  - –Converges voice and data traffic over single IP network
  - –IP telephony adds digital voice clients and new voice applications to a data based network
- IP telephony advantages
  - –Incoming calls can be selectively forwarded or blocked
  - –Cost savings
  - –Managing a single network for all applications
  - –Applications can be developed more quickly with fewer resources
  - –Reduced wired infrastructure requirements
  - –Reduced regulatory requirements

Securing Network Applications: Cloud Computing

CLOUD COMPUTING

- Pay-per-use computing model
  - –Customers pay for only the resources they need
  - –May revolutionize computing
  - –Unlike hosted services, does not require long-term contracts

Three service models of cloud computing



Securing Network Applications: Cloud Computing

Cloud computing security challenges

- Cloud provider must guarantee means to approve authorized users and deny imposters
- Transmissions from the cloud must be protected
- Customers’ data must be isolated from one another

Summary

- TCP/IP
  - –Most common protocol for LANs and the Internet
- Protocols for transferring files
  - –FTP, FTPS, SFTP, SCP
- Network Administration Principles can be applied through procedural rules and technical rules (device security, network management, port security)
- Router configuration must provide a secure network environment
- Networks can be configured to provide separation and increased security
- Securing ports is an important step in network management
  - –Unused ports should be disabled
- New network applications that have special security considerations
  - –Virtualization
  - –IP Telephony
  - –Cloud computing