C|SA™
Certified SOC Analyst

EC-Council

Fundamental Essential Concepts

MODULE OBJECTIVE

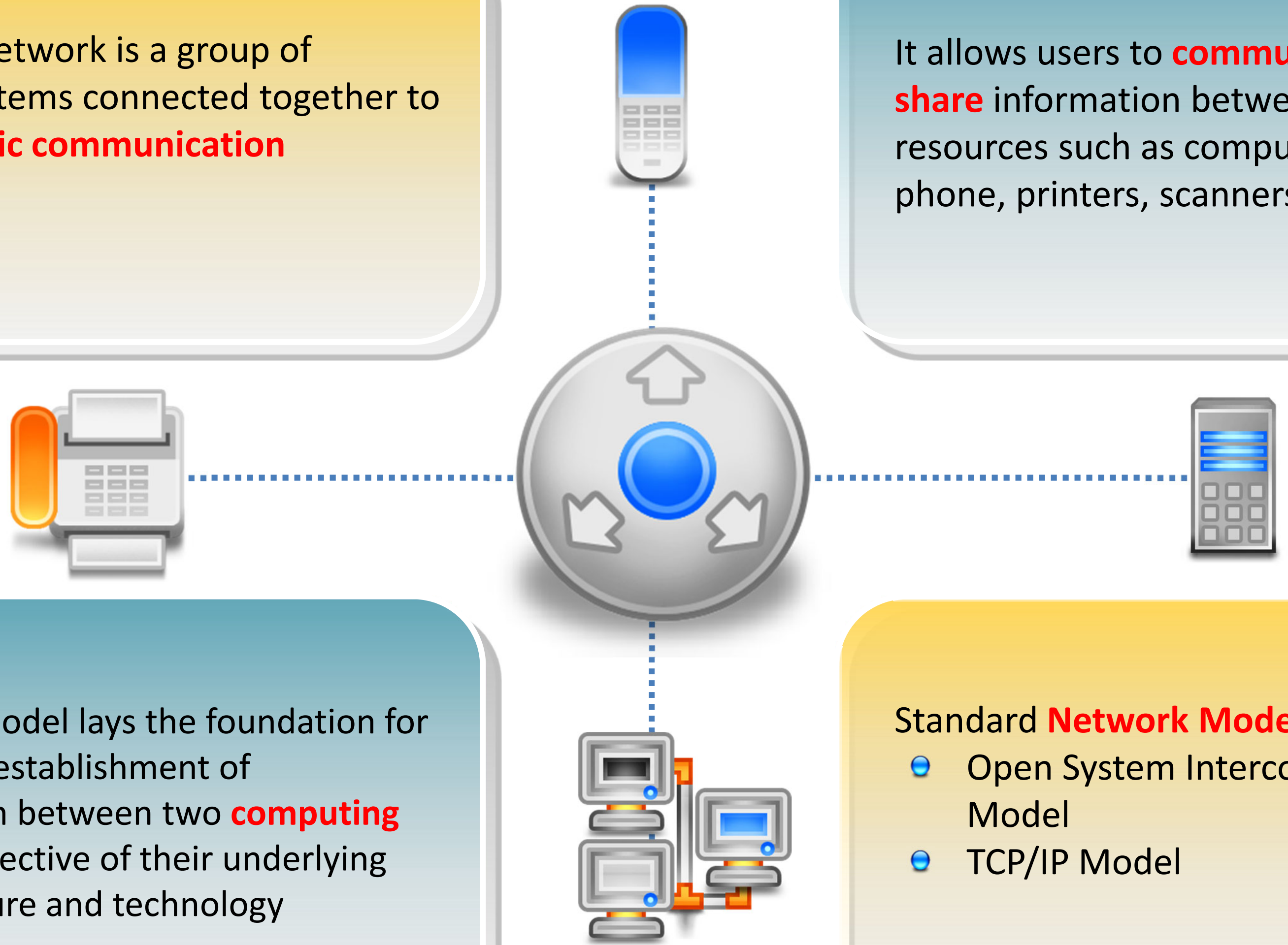
This is a self-study module for the students. The objective of this module is help in preparing for the SOC class. This modules delivers fundamental knowledge required for the course. The module basically deals the fundamental concepts of network, application and host level. The module presents concepts on networking including working of TCP/IP protocols, topologies, IP addressing, etc. The module presents application level concepts including protocols, communication, methods used for communication, architecture, etc. The module also presents host level concepts including Windows and Linux security. By studying this module student will quickly be able to understand concepts of working of network, application, host level incidents and also logic for the SIEM use cases for detecting incidents at network, application and host level.

Computer Network Fundamentals

Computer Network

A Computer Network is a group of computing systems connected together to allow **electronic communication**

It allows users to **communicate** and **share** information between various resources such as computer, mobile phone, printers, scanners, etc.



The network model lays the foundation for the successful establishment of communication between two **computing systems**, irrespective of their underlying internal structure and technology

Standard **Network Models**:

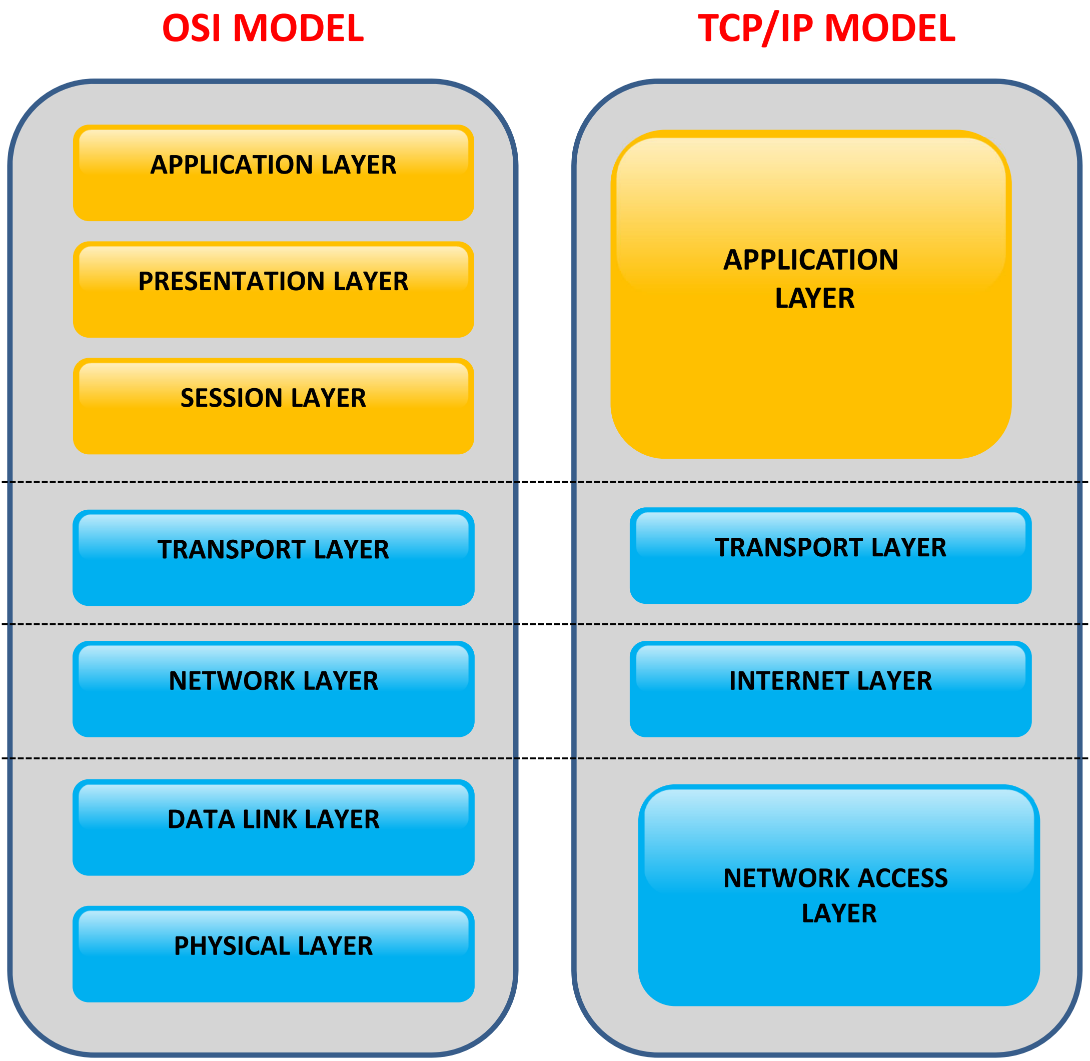
- Open System Interconnection (OSI) Model
- TCP/IP Model

TCP/IP Model

TCP/IP model is a framework for the Internet Protocol suite of computer network protocols that defines the communication in an IP-based network

Functions	Layers	Protocols
Handles high-level protocols, issues of representation, encoding, and dialog control	Application Layer	File Transfer (TFTP, FTP, NFS), Email (SMTP), Remote Login (Telnet, rlogin), Network Management (SNMP), Name Management (DNS)
Constitutes a logical connection between the endpoints and provides transport services from the source to the destination host	Transport Layer	Transmission Control Protocol (TCP) and User Datagram Protocol (UDP)
Selects the best path through the network for packets to travel	Internet Layer	Internet Protocol (IP), Internet Control Message Protocol (ICMP), Address Resolution Protocol (ARP), Reverse Address Resolution Protocol (RARP)
Defines how to transmit an IP datagram to the other devices on a directly attached network	Network Access Layer	Ethernet, Fast Ethernet, SLIP, PPP, FDDI, ATM, Frame Relay, SMDS, ARP, Proxy ARP, RARP

Comparing OSI and TCP/IP



TCP/IP model is based on the practical implementation of protocols around which the Internet has developed, whereas the OSI model, often referred to as a reference model, is a generic protocol-independent standard

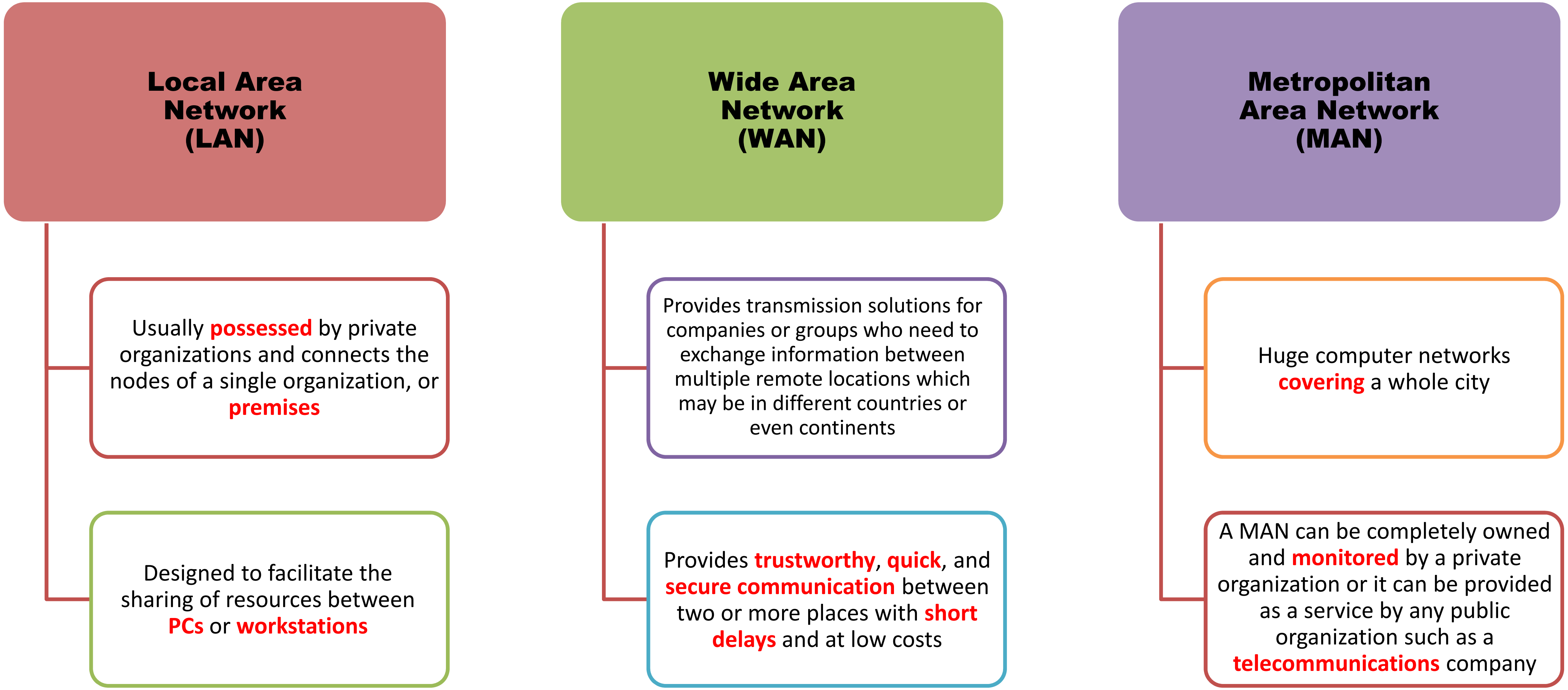
Only connection-oriented communication

Both connectionless and connection-oriented communication

OSI model defines services, intervals and protocols, whereas TCP/IP does not provide a clear distinction between these

Types of Networks

- **Classification of networks based on the physical location or the geographical boundaries**



Local Area Network (LAN)

- Usually **possessed** by private organizations and connects the nodes of a single organization, or **premises**
- Designed to facilitate the sharing of resources between **PCs** or **workstations**

Wide Area Network (WAN)

- Provides transmission solutions for companies or groups who need to exchange information between multiple remote locations which may be in different countries or even continents
- Provides **trustworthy**, **quick**, and **secure communication** between two or more places with **short delays** and at low costs

Metropolitan Area Network (MAN)

- Huge computer networks **covering** a whole city
- A MAN can be completely owned and **monitored** by a private organization or it can be provided as a service by any public organization such as a **telecommunications** company

Types of Networks (Cont'd)

04

Personal Area Network (PAN)

- Wireless communication that uses both **radio** and **optical** signals
- Covers individual's work area or work group and is also known as a **room-size network**

05

Campus Area Network (CAN)

- Covers only **limited geographical area**
- This kind of network is applicable for a **university** campus

06

Global Area Network (GAN)

- Combination of different **interconnected** computer networks
- Covers an unlimited geographical area
- The Internet is an example of a GAN

Types of Networks (Cont'd)

Wireless Networks (WLAN)

- Wireless networks use **Radio Frequency (RF) signals** to connect wireless-enabled devices in the network
- It uses IEEE standard of 802.11 and uses radio waves for communication

Advantages

- Installation is easy and **eliminates wiring**
- Access to the network can be from **anywhere** within the range of an access point
- Public places like airports, schools, etc. can offer **constant Internet connection** using Wireless LAN

Limitations

- Wi-Fi **Security** may not meet the expectations
- The **bandwidth** suffers with the number of users on the network
- Wi-Fi standard changes may require replacing wireless components
- Some electronic equipment can **interfere** with the Wi-Fi network

Network Topologies

- Network topology is a specification that **deals with a network's overall design and flow of data** in it

Types of Topology

- **Physical Topology** – Physical layout of nodes, workstations and cables in the network
- **Logical Topology** – The way information flows between different components

Physical Network Topologies

Bus Topology
Network devices are connected to the central cable, called a bus, by the help of interface connectors

Star Topology
Network devices are connected to a central computer called hub which functions as a router to send messages

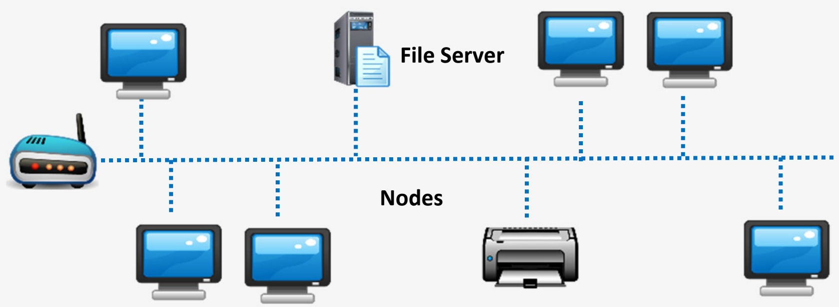
Ring Topology
Network devices are connected in a closed loop. Data travels from node to node, with each node along the way handling every packet

Mesh Topology
Network devices are connected in a way such that every device has a point-to-point link to every other device on the network

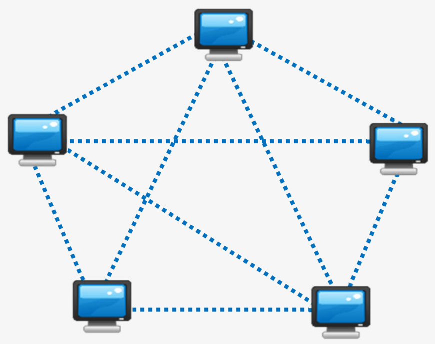
Tree Topology
It is a hybrid of bus and star topologies, in which groups of star-configured networks are connected to a linear bus backbone cable

Hybrid Topology
Combination of any two or more different topologies. Star-Bus or Star-Ring topologies are widely used

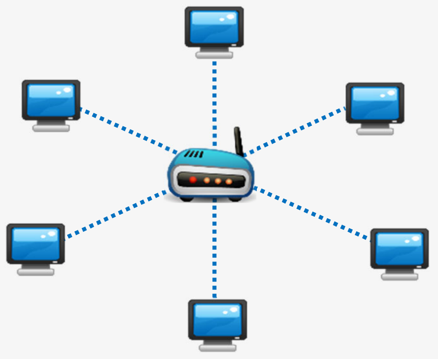
Network Topologies (Cont'd)



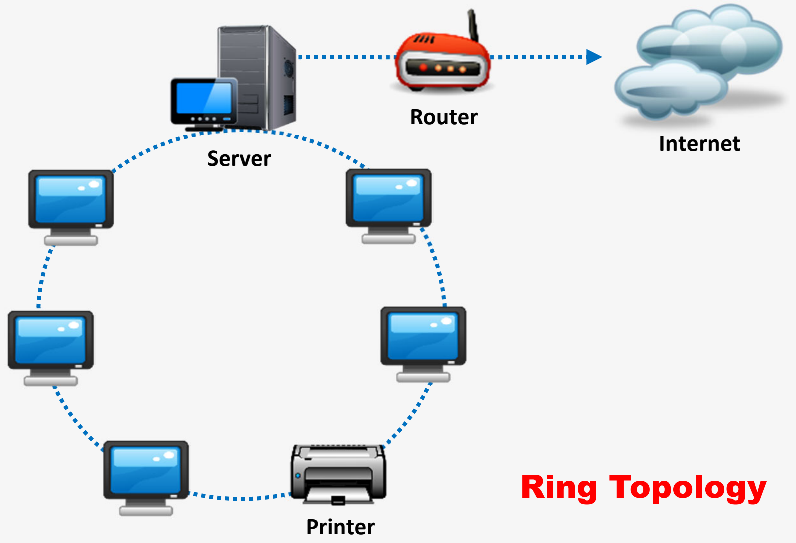
Linear Bus



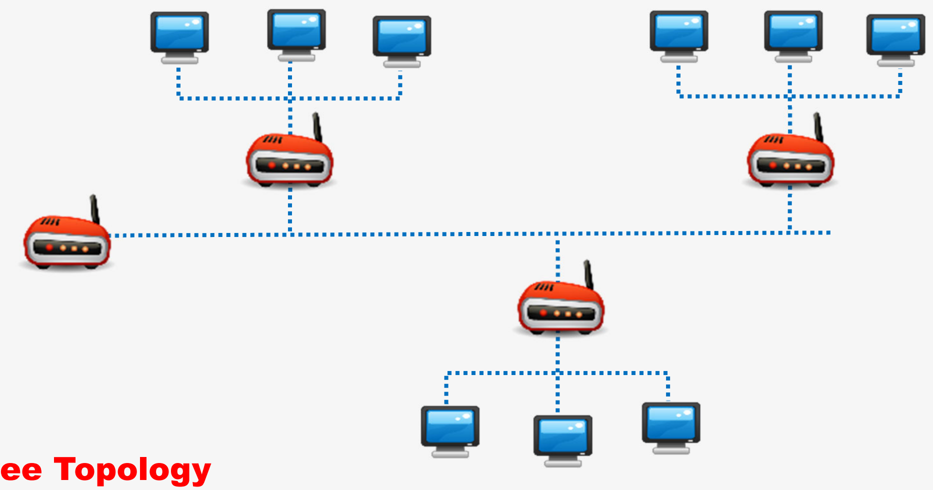
Mesh Topology



Star Topology



Ring Topology



Tree Topology

Network Hardware Components

Network Interface Card (NIC): It allows the computers to **connect** and **communicate** with the network

Repeater: It is used to **increase** the strength of an incoming signal in a network

Hub: It is used to connect segments of a **LAN**. All the LAN segments can see all the packets

Switch: It is similar to hub. However, no **equipment** in the LAN segment can see the packets except the target node

Router: It **receives** data packets from one network segment and **forwards** it to another

Bridges: It combines two network segments and manages **network traffic**

Gateways: It **enables** communication between different types of environments and protocols

Types of LAN Technology

Ethernet

- Ethernet is the physical layer of LAN technology. It maintains proper balance between the speed, cost and ease of installation
- It describes the number of conductors required for making the connection, the performance thresholds that are required, and offers the framework for data transmission
- A standard Ethernet network can send data at a rate of up to 10 Megabits per second (10 Mbps)
- Ethernet standard, IEEE standard 802.3, specifies configuration rules for an Ethernet network and also states the interaction of elements in a network

Fast Ethernet

- The Fast Ethernet standard, IEEE 802.3u, is a new version of ethernet that transmits data at a minimum speed rate of 100 Mbit/s
- Three types of Fast Ethernet are available in the market: **100BASE-TX** , to use with level 5 UTP cable; **100BASE-FX,** to use with fiber-optic cable; and 1**00BASE-T4**, for utilizing extra two wires with level 3 UTP cable.

Types of LAN Technology (Cont'd)

- **Gigabit Ethernet**
  - Gigabit ethernet was defined by the IEEE 802.3-2008 standard and conveys Ethernet frames at a speed rate of a gigabit per second
  - It is used on fast speed communication networks like multimedia and Voice over IP (VoIP)
  - It is also called as "gigabit-Ethernet-over-copper" or 1000Base-T, as it's speed is 10 times more than 100Base-T
- **10 Gigabit Ethernet**
  - 10 Gigabit Ethernet was first defined by IEEE 802.3ae-2002 standard
  - It conveys Ethernet frames at a speed rate of 10 gigabits per second. This makes it 10 times faster than Gigabit ~~e~~Ethernet
  - As compared to other Ethernet systems, 10 Gigabit Ethernet uses optical fiber connections
- **Asynchronous Transfer Mode (ATM)**
  - Asynchronous Transfer Mode (ATM) is a cell-based fast-packet communication standard developed for transmitting information of different types like voice, video or data, in small, fixed-sized cells, etc.
  - It operates on the data link layer through fiber or twisted-pair cable
  - It is mainly used on private long-distance networks, especially by the internet service providers

Types of LAN Technology (Cont'd)

- **Power over Ethernet (PoE)**
  - Power over Ethernet (PoE) is a networking feature defined by the IEEE 802.3af and 802.3at standards
  - It allows the Ethernet cables to supply power to network devices over the existing data connection
  - PoE-capable devices can be power sourcing equipment (PSE), powered devices (PDs), or sometimes both. PSE is the device that transmits power, whereas PD is the device that is powered

Types of LAN Technology (Cont'd)

Specifications of LAN Technology

Name	IEEE Standard	Data Rate	Media Type	Maximum Distance
Ethernet	802.3	10 Mbps	10Base-T	100 meters
Fast Ethernet/ 100Base-T	802.3u	100 Mbps	100Base-TX 100Base-FX	100 meters 2000 meters
Gigabit Ethernet/ GigE	802.3z	1000 Mbps	1000Base-T 1000Base-SX 1000Base-LX	100 meters 275/550 meters 550/5000 meters
10 Gigabit Ethernet	IEEE 802.3ae	10 Gbps	10GBase-SR 10GBase-LX4 10GBase-LR/ER 10GBase-SW/LW/EW	300 meters 300 m MMF/ 10 km SMF 10 km/40 km 300 m/10 km/40 km

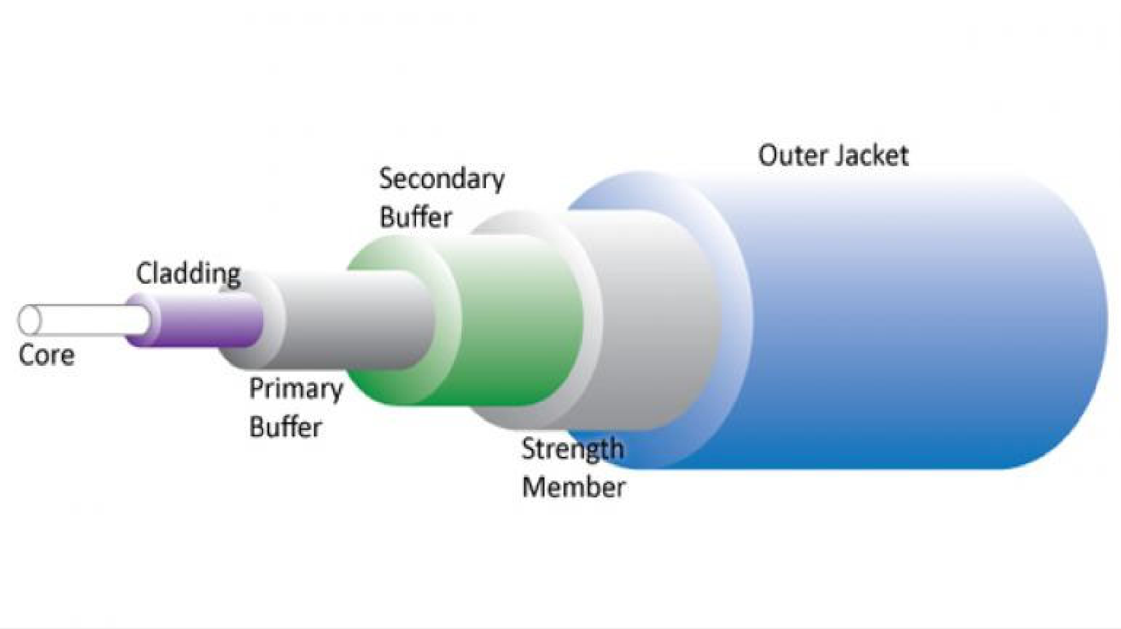
Types of Cables: Fiber Optic Cable

Fiber optic cable

- Optical fiber cable consists of Core, Cladding, Buffer and Jacket layers
- Core consists of glass or plastic with higher index of refraction than cladding, and it carries signal
- Cladding also consists of glass or plastic with lower refractive index compared to core
- Buffer protects the fiber from damage and moisture
- Jacket holds one or more fibers in a cable

Features:

- Lower cost
- Extremely wide bandwidth
- Lighter weight and small in size
- More secure
- Resist to corrosion
- Longer life and easy to maintain
- Elimination of the cross talk
- Immunity to electrostatic interference

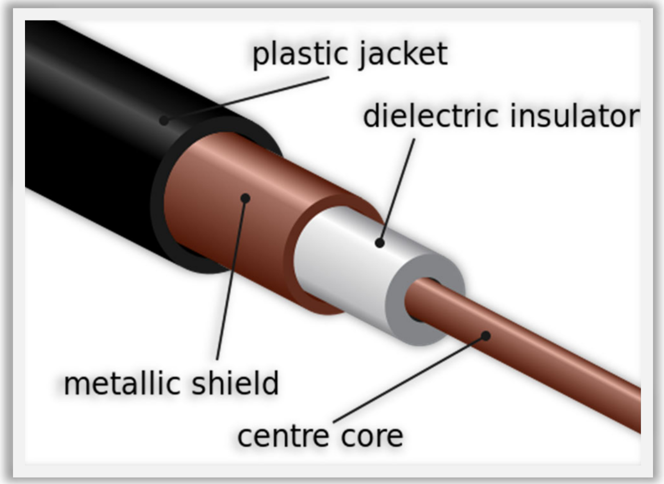


Types of Cables: Coaxial Cable

- Coaxial cable is a type of copper cable built with a metal shield and other components engineered to block signal interference
- It consists of two conductors separated by a dielectric material
- The center conductor and outer conductor are configured in such a way that they form concentric cylinder with a common axis
- 50 ohm and 75 ohm coaxial cables are widely used
- 50 ohm cable is used for digital transmission and 75 ohm cable is used for analog transmission
- It has large bandwidth and low losses
- It has a data rate of 10 Mbps, which can be increased with the increase in diameter of the inner conductor

Advantages:

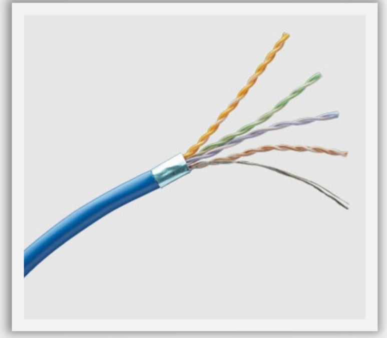
- Cheap to install
- Great channel capacity
- Good bandwidth
- Easy to modify
- Cheap to make



Types of Cables: CAT 3 and CAT 4

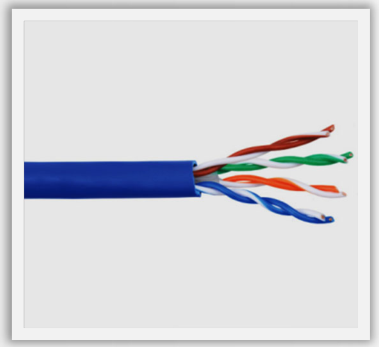
CAT 3

- Commonly known as category 3 or station wire
- Used in voice application and 10 BaseT (10Mbps) Ethernet
- Bandwidth 16 MHz
- Attenuation 11.5 dB
- Impedance 100 ohms



CAT 4

- Commonly known as category 4 cable and consists of four unshielded twisted pair copper wires
- Used in 10 BaseT (10Mbps) Ethernet
- Bandwidth 20 MHz
- Attenuation 7.5 dB
- Impedance 100 ohms



Types of Cables: CAT 5

CAT 5 (Category 5):

- It is an unshielded, twisted pair cable which is terminated with RJ 45 connectors
- It has a maximum length of 100 m and supports frequency up to 100 MHz
- It is suitable for 10BASE-T, 100BASE-TX and 1000BASE-T networking
- It carries the telephony and video signals
- Punch-down blocks and modular connectors are used to connect this cable

Features:

- It is applicable to most LAN topologies and also suitable for 4 and 16 Mbps UTP Token Ring Systems
- It has 100 MHz bandwidth, 24.0 dB attenuation, 100 Ohms impedance
- It is used for high speed data transmission

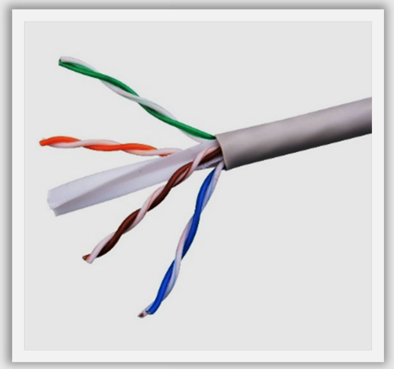
Types of Cables: CAT 5e and CAT 6

CAT 5e

- Commonly known as category 5 cable, which is used to transmit high speed data
- Used in fast ethernet (100 Mbps), Gigabit Ethernet (1000 Mbps) and 155 Mbps ATM
- Bandwidth 350 MHz
- Attenuation 24.0 dB
- Impedance 100 Ohms

CAT 6

- Commonly known as category 5 cable which transmits high speed data
- Used in Gigabit Ethernet (1000 Mbps) and 10 Gig Ethernet (10000 Mbps)
- Bandwidth 250 MHz
- Attenuation 19.8 dB
- Impedance 100 ohms



Types of Cables: 10/100/1000BaseT (UTP Ethernet)

- An ethernet connection method uses twisted pair cables and operates at 10, 100 or 1000 Mbps
- BASE denotes that baseband transmission and T stands for twisted pair cabling
- **10 Base-T:**
  - It has a transmission speed of 10 Mbps and a maximum cable length of 100 m
  - It uses 802.3i IEEE standard
  - Cat 3 and Cat 5 are suitable
  - It uses 4 wires (pins 1,2,3,6)
- **100 Base-T:**
  - It has a transmission speed of 100 Mbps
  - It uses 802.3u IEEE standard
  - Cat 5 is suitable
  - It uses 4 wires (pins 1,2,3,6)
- **1000 Base-T:**
  - It has a transmission speed of 1000 Mbps
  - It uses 802.3ab IEEE standard
  - Cat 5e is suitable cable
  - It uses 8 wires (pins 1,2,3,4,5,6,7,8)

TCP/IP Protocol Suite

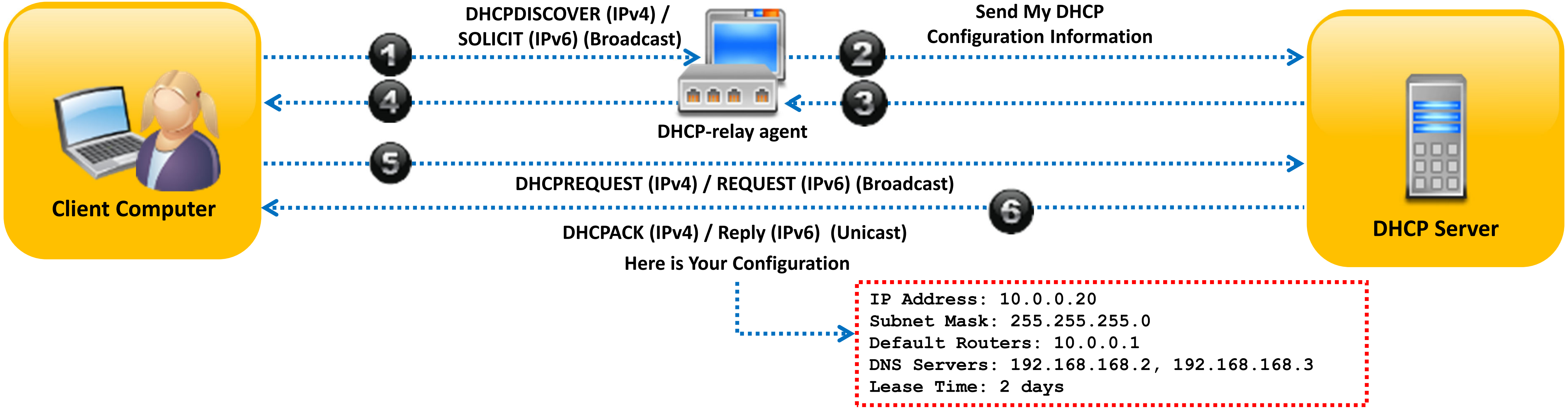
TCP/IP Protocol Suite

Application Layer	Transport Layer	Internet Layer	Link Layer
DHCP	TCP	IP	FDDI
DNS	UDP	IPv6	Token ring
DNSSEC	SSL	IPsec	WEP
HTTP	TLS	ICMP	WPA
S-HTTP		ARP	WPA2
HTTPS		IGRP	TKIP
FTP		EIGRP	EAP
SFTP			LEAP
TFTP			PEAP
SMTP			CDP
S/MIME			HSRP
PGP			VRRP
Telnet			VTP
SSH			STP
SOAP			
SNMP			
NTP			
RPC			
SMB			
SIP			
RADIUS			
TACACS+			
RIP			
OSPF			

Application Layer Protocols

Dynamic Host Configuration Protocol (DHCP)

- DHCP is used by DHCP servers to distribute TCP/IP configuration information to DHCP-enabled clients in the form of a lease offer



Client Computer

DHCP-relay agent

DHCP Server

1 DHCPDISCOVER (IPv4) / SOLICIT (IPv6) (Broadcast)

2 Send My DHCP Configuration Information

3

4

5 DHCPREQUEST (IPv4) / REQUEST (IPv6) (Broadcast)

6 DHCPACK (IPv4) / Reply (IPv6) (Unicast)

Here is Your Configuration

```
IP Address: 10.0.0.20
Subnet Mask: 255.255.255.0
Default Routers: 10.0.0.1
DNS Servers: 192.168.168.2, 192.168.168.3
Lease Time: 2 days
```

DHCP Packet Format

Byte 0	Byte 1	Byte 2	Byte 3
OP Code (1)	Hardware Type (1)	Hardware Addr. Len. (1)	Hops (1)
Transaction Identifier			
Seconds (2)		Flags (2)	
Client IP Address (CIADDR) – 4 bytes			
Your IP Address (YIADDR) – 4 bytes			
Server IP Address (SIADDR) – 4 bytes			
Gateway IP Address (GIADDR) – 4 bytes			
Client Hardware Address (CHADDR) –16 bytes			
Server Name (SNAME) – 64 bytes			
Filename – 128 bytes			
DHCP Options – variable			

- DHCP runs over **UDP port 67** (connections to server) and **68** (connections to client)

OP Code:

1 for request message

2 for reply message

Hardware Type:

1 = Ethernet

2 = Experimental Ethernet

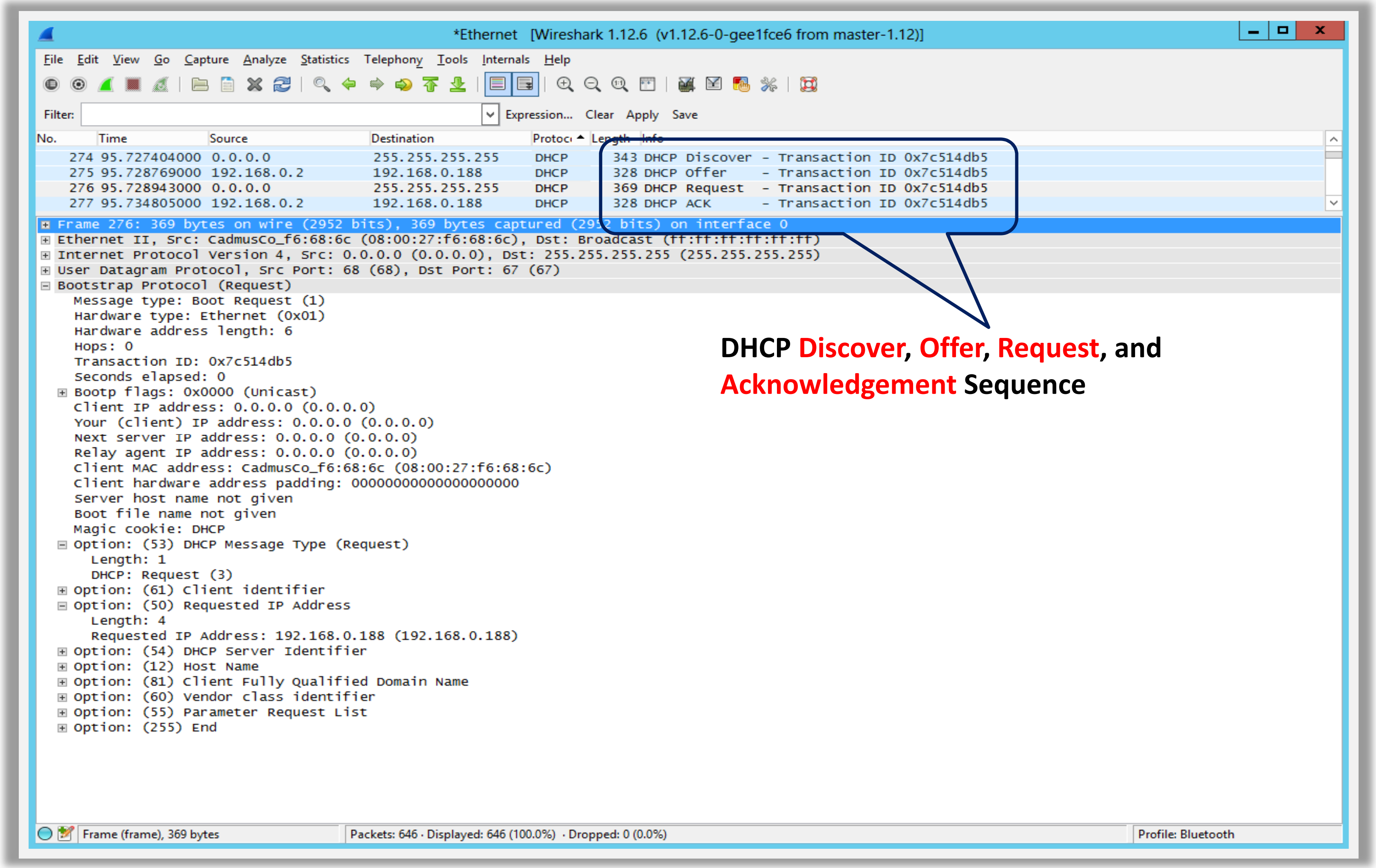
3 = Amateur Radio AX.25

4 = Proteon ProNET Token Ring

5 = Chaos

6 = IEEE 802 Networks, etc.

DHCP Packet Analysis



*Ethernet [Wireshark 1.12.6 (v1.12.6-0-gee1fce6 from master-1.12)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply Save

```
No.   Time           Source        Destination       Protocol Length Info
  274 95.727404000 0.0.0.0       255.255.255.255   DHCP     343 DHCP Discover  - Transaction ID 0x7c514db5
  275 95.728769000 192.168.0.2   192.168.0.188     DHCP     328 DHCP Offer     - Transaction ID 0x7c514db5
  276 95.728943000 0.0.0.0       255.255.255.255   DHCP     369 DHCP Request   - Transaction ID 0x7c514db5
  277 95.734805000 192.168.0.2   192.168.0.188     DHCP     328 DHCP ACK       - Transaction ID 0x7c514db5
```

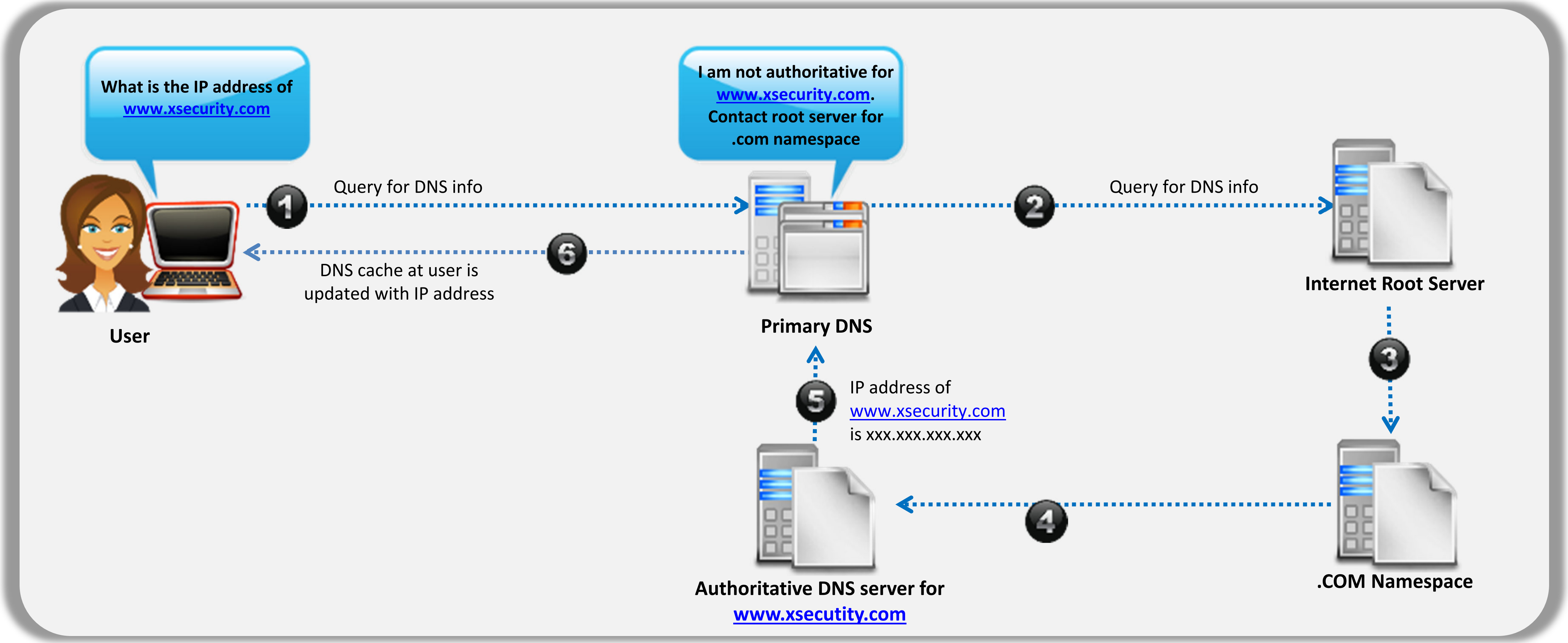
```
⊞ Frame 276: 369 bytes on wire (2952 bits), 369 bytes captured (2952 bits) on interface 0
⊞ Ethernet II, Src: CadmusCo_f6:68:6c (08:00:27:f6:68:6c), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
⊞ Internet Protocol Version 4, Src: 0.0.0.0 (0.0.0.0), Dst: 255.255.255.255 (255.255.255.255)
⊞ User Datagram Protocol, Src Port: 68 (68), Dst Port: 67 (67)
⊟ Bootstrap Protocol (Request)
    Message type: Boot Request (1)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0x7c514db5
    Seconds elapsed: 0
  ⊞ Bootp flags: 0x0000 (Unicast)
    Client IP address: 0.0.0.0 (0.0.0.0)
    Your (client) IP address: 0.0.0.0 (0.0.0.0)
    Next server IP address: 0.0.0.0 (0.0.0.0)
    Relay agent IP address: 0.0.0.0 (0.0.0.0)
    Client MAC address: CadmusCo_f6:68:6c (08:00:27:f6:68:6c)
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
  ⊟ Option: (53) DHCP Message Type (Request)
      Length: 1
      DHCP: Request (3)
  ⊞ Option: (61) Client identifier
  ⊟ Option: (50) Requested IP Address
      Length: 4
      Requested IP Address: 192.168.0.188 (192.168.0.188)
  ⊞ Option: (54) DHCP Server Identifier
  ⊞ Option: (12) Host Name
  ⊞ Option: (81) Client Fully Qualified Domain Name
  ⊞ Option: (60) Vendor class identifier
  ⊞ Option: (55) Parameter Request List
  ⊞ Option: (255) End
```

Frame (frame), 369 bytes | Packets: 646 · Displayed: 646 (100.0%) · Dropped: 0 (0.0%) | Profile: Bluetooth

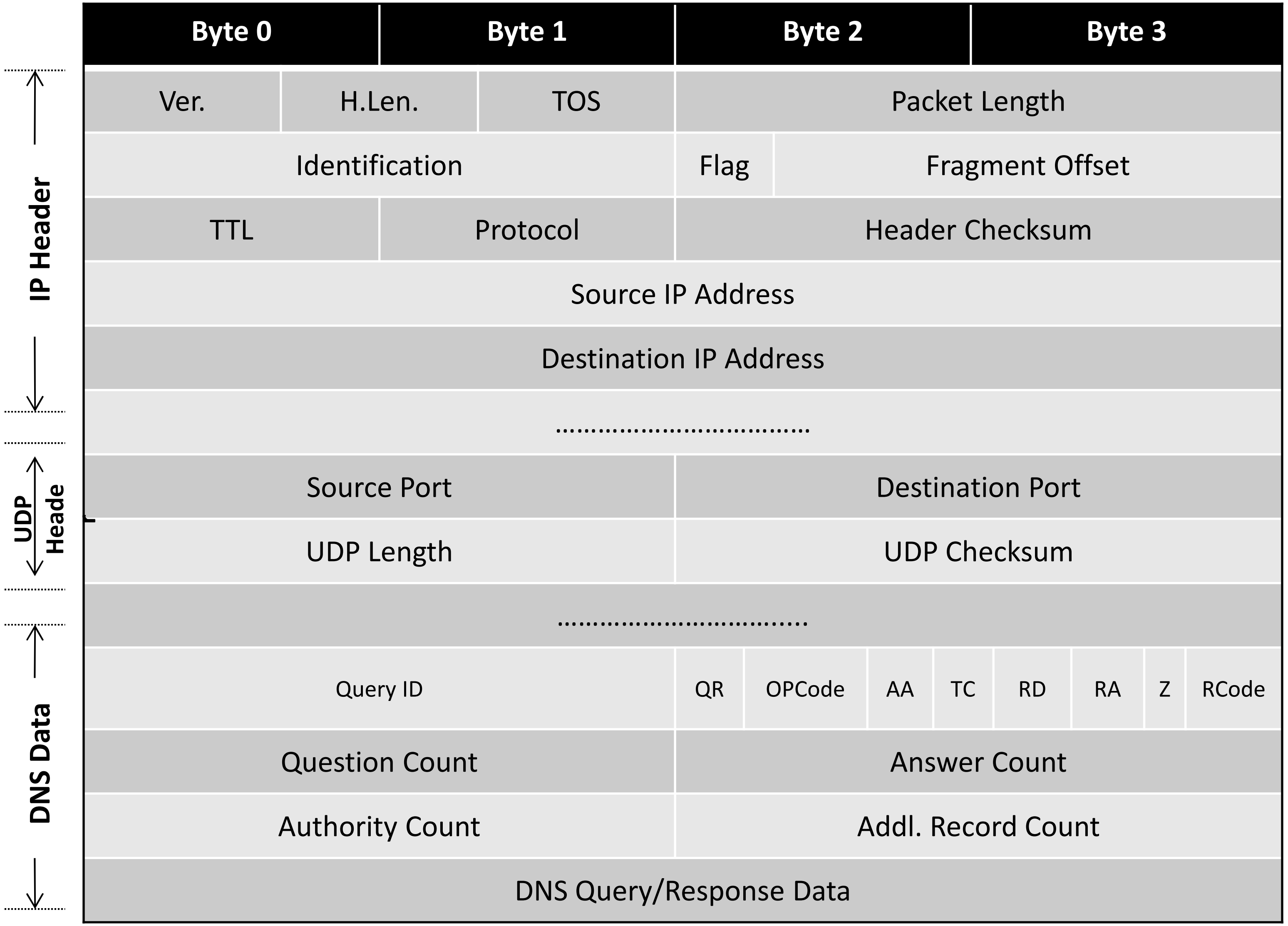
DHCP Discover, Offer, Request, and Acknowledgement Sequence

Domain Name System (DNS)

- DNS is a distributed hierarchic database that maps URLs to IP addresses


What is the IP address of www.xsecurity.com
I am not authoritative for www.xsecurity.com. Contact root server for .com namespace
1
Query for DNS info
2
Query for DNS info
6
DNS cache at user is updated with IP address
User
Primary DNS
Internet Root Server
3
5
IP address of www.xsecurity.com is xxx.xxx.xxx.xxx
4
Authoritative DNS server for www.xsecutity.com
.COM Namespace

DNS Packet Format



<table>
<tr><th></th><th colspan="6">Byte 0</th><th colspan="6">Byte 1</th><th colspan="6">Byte 2</th><th colspan="6">Byte 3</th></tr>
<tr><td rowspan="5">IP Header</td><td colspan="4">Ver.</td><td colspan="4">H.Len.</td><td colspan="4">TOS</td><td colspan="12">Packet Length</td></tr>
<tr><td colspan="12">Identification</td><td colspan="2">Flag</td><td colspan="10">Fragment Offset</td></tr>
<tr><td colspan="6">TTL</td><td colspan="6">Protocol</td><td colspan="12">Header Checksum</td></tr>
<tr><td colspan="24">Source IP Address</td></tr>
<tr><td colspan="24">Destination IP Address</td></tr>
<tr><td></td><td colspan="24">……………………………</td></tr>
<tr><td rowspan="2">UDP Heade</td><td colspan="12">Source Port</td><td colspan="12">Destination Port</td></tr>
<tr><td colspan="12">UDP Length</td><td colspan="12">UDP Checksum</td></tr>
<tr><td></td><td colspan="24">……………………………</td></tr>
<tr><td rowspan="4">DNS Data</td><td colspan="12">Query ID</td><td>QR</td><td colspan="3">OPCode</td><td>AA</td><td>TC</td><td colspan="2">RD</td><td colspan="2">RA</td><td>Z</td><td>RCode</td></tr>
<tr><td colspan="12">Question Count</td><td colspan="12">Answer Count</td></tr>
<tr><td colspan="12">Authority Count</td><td colspan="12">Addl. Record Count</td></tr>
<tr><td colspan="24">DNS Query/Response Data</td></tr>
</table>

QR

- 0 Query
- 1 Response

Opcode

- 0 Standard Query (QUERY)
- 1 Inverse Query (IQUERY)
- 2 Sever Status Request (STATUS)

AA 1 = Authoritative Answer

TC 1 = TrunCation

RD 1 = Recursion Desired

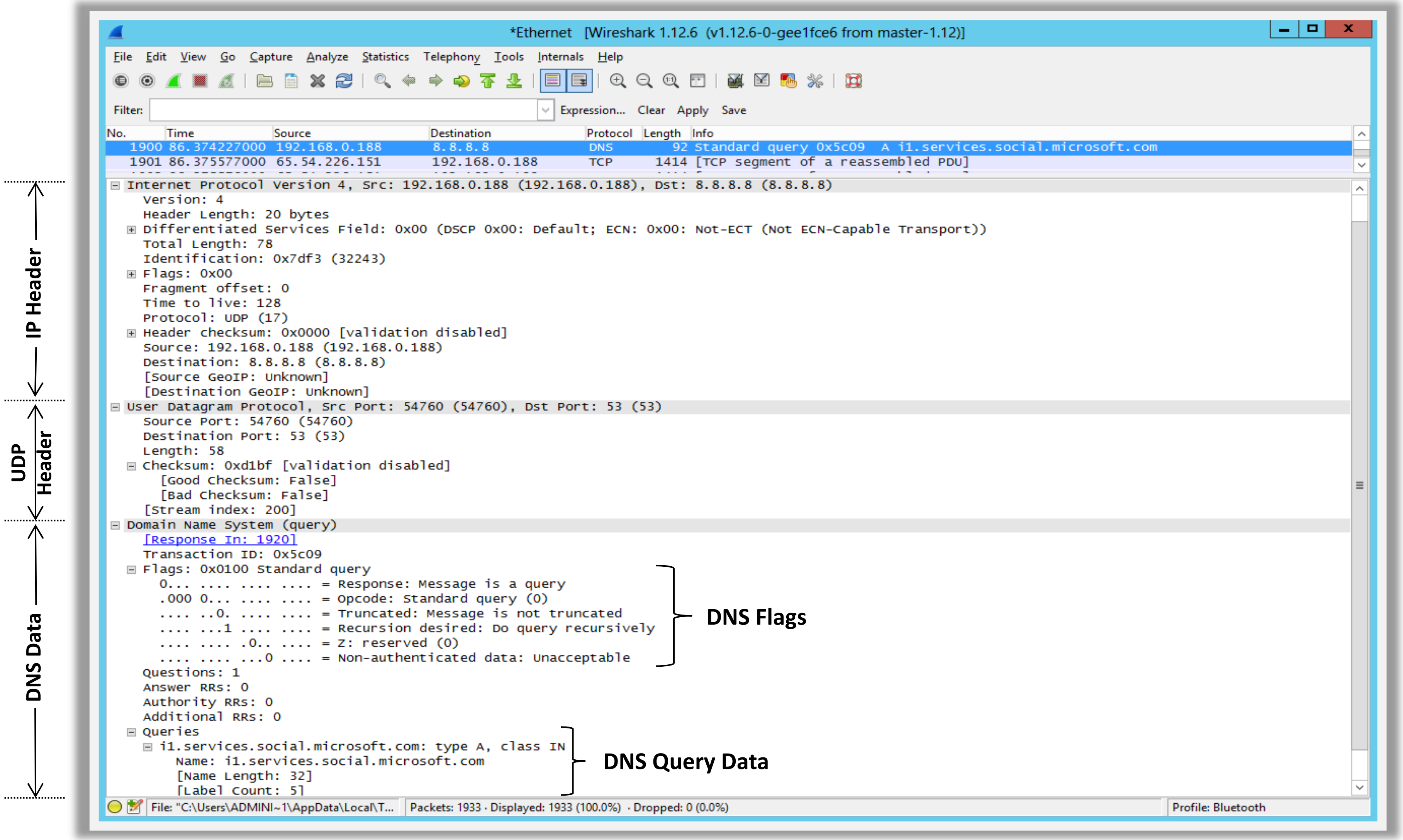
RA 1 = Recursion Available

Z = Reserved, set to 0

Response Code

- 0 No Error
- 1 Format Error
- 2 Server Failure
- 3 Non-existent Domain
- 4 Query Type Not Implemented
- 5 Query Refused

DNS Packet Analysis


*Ethernet [Wireshark 1.12.6 (v1.12.6-0-gee1fce6 from master-1.12)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply Save
IP Header
UDP Header
DNS Data
DNS Flags
DNS Query Data
File: "C:\Users\ADMINI~1\AppData\Local\T...
Packets: 1933 · Displayed: 1933 (100.0%) · Dropped: 0 (0.0%)
Profile: Bluetooth

```
No.    Time           Source          Destination     Protocol Length Info
  1900 86.374227000  192.168.0.188   8.8.8.8         DNS        92 Standard query 0x5c09  A i1.services.social.microsoft.com
  1901 86.375577000  65.54.226.151   192.168.0.188   TCP      1414 [TCP segment of a reassembled PDU]
```

```
⊟ Internet Protocol Version 4, Src: 192.168.0.188 (192.168.0.188), Dst: 8.8.8.8 (8.8.8.8)
    Version: 4
    Header Length: 20 bytes
  ⊞ Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
    Total Length: 78
    Identification: 0x7df3 (32243)
  ⊞ Flags: 0x00
    Fragment offset: 0
    Time to live: 128
    Protocol: UDP (17)
  ⊞ Header checksum: 0x0000 [validation disabled]
    Source: 192.168.0.188 (192.168.0.188)
    Destination: 8.8.8.8 (8.8.8.8)
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
⊟ User Datagram Protocol, Src Port: 54760 (54760), Dst Port: 53 (53)
    Source Port: 54760 (54760)
    Destination Port: 53 (53)
    Length: 58
  ⊟ Checksum: 0xd1bf [validation disabled]
      [Good Checksum: False]
      [Bad Checksum: False]
    [Stream index: 200]
⊟ Domain Name System (query)
    [Response In: 1920]
    Transaction ID: 0x5c09
  ⊟ Flags: 0x0100 Standard query
      0... .... .... .... = Response: Message is a query
      .000 0... .... .... = Opcode: Standard query (0)
      .... ..0. .... .... = Truncated: Message is not truncated
      .... ...1 .... .... = Recursion desired: Do query recursively
      .... .... .0.. .... = Z: reserved (0)
      .... .... ...0 .... = Non-authenticated data: Unacceptable
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  ⊟ Queries
    ⊟ i1.services.social.microsoft.com: type A, class IN
        Name: i1.services.social.microsoft.com
        [Name Length: 32]
        [Label Count: 5]
```

DNSSEC

- Domain Name System Security Extensions (DNSSEC) is a suite of Internet Engineering Task Force (IETF)
- It is used for securing certain kinds of information provided by DNS
- It works by digitally signing records for DNS lookup with the help of public-key cryptography

DNSSEC guarantees:

- Authenticity
- Integrity
- The non-existence of a domain name or type

DNSSEC does not guarantee:

- Confidentiality
- Protection against Denial of Service (DoS)

How DNSSEC Works?

1. DNSSEC works with the concept of asymmetric keys - Public key and private key
2. DNSSEC adds a digital signature to each piece of a domain name's DNS information
3. When a guest enters the domain name's URL in a web browser, the resolver verifies the digital signature
4. The digital signature must match the value on file at the registry, or the resolver rejects the response

Managing DNSSEC for your Domain Name

1

DNSSEC adds a layer of security to your domain names by adding digital signatures to their Domain Name System (DNS) information

2

Delegation Signing (DS) data contains the digital signature information for respective domain name's DNS

3

Following are the extensions that can be managed in DS records:

- .com; .net; .biz; .us; .org; .eu; .co.uk, .me.uk, and .org.uk; .co; .com.co, .net.co, and .nom.co

4

Depending upon the domain name's extension, you can work one or more DS records at one time

What is a DS Record?

- Allowing DNSSEC for your domain name involves this information to complete the setup of your signed domain name

- Delegation Signing (DS) records give complete information about a signed zone file

How does DNSSEC Protect Internet Users?

- DNSSEC is planned to shield Internet users from artificial DNS data, such as a deceptive or mischievous address instead of the genuine address that was requested
- Difference between non-aware and DNSSEC-aware lookups:

Non-DNSSEC-Aware Lookups

- URL request goes towards the Internet and accepts the first response it receives
- A mischievous Internet user can cut off the request and send back incorrect information
- The response received points to an undesired Internet site where personal data can be compromised

DNSSEC-Aware Lookups

- These DNS lookups travel toward the domain name's registry and get a duplicate of the digital signature that is being used by the URL
- The browser cannot display the site unless an address response also includes a matching digital signature
- This way, you can't be redirected to a bogus location that you didn't request

Operation of DNSSEC

Authenticity and integrity are provided by the signature of the RRSET created with a private key

The public key is used to verify the signature of an RRSET (RRSIG)

Authenticity of the non-existence of a name or type is provided by a chain of names (NSEC), in which each name points to the next in the zone, in a canonical order

Delegated zones (child) sign the RRSETs with a private key

The authenticity of the key is verified by the signature of the DS record, present in the parent zone (Hash of the public key – DNSKEY)

Hypertext Transfer Protocol (HTTP)

- HTTP lays the foundation for communication on world wide web (WWW)
- It is the standard application protocol on the top of TCP/IP, handling web browser requests and web server responses
- It is used to transfer data (like audio, video, images, hypertext, plain text, etc.) between client and server
- HTTP messages are exchanged between client and server during communication
- Client sends HTTP request messages to the server while the server sends a response with HTTP response messages

Weaknesses in HTTP:

- Vulnerable to Man-In-Middle attack
- It lacks in security as data sent via HTTP is not encrypted
- One can use HTTP without any encryption or digital certificates

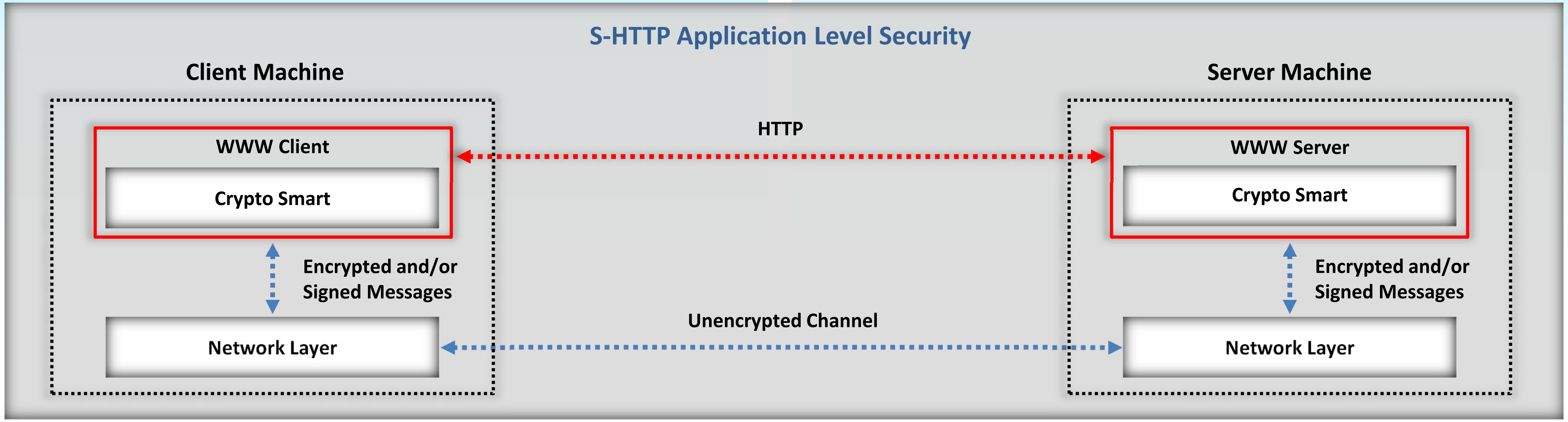
Secure HTTP

Secure HTTP is an application layer protocol used to **encrypt** the **web communications** carried over HTTP

It is an alternate for the **HTTPS** (SSL) protocol

It ensures **secure data transmission** of individual messages while SSL establishes a secure connection between two entities ensuring security of the entire communication

It is generally used in situations where the server requires **authentication** from the user

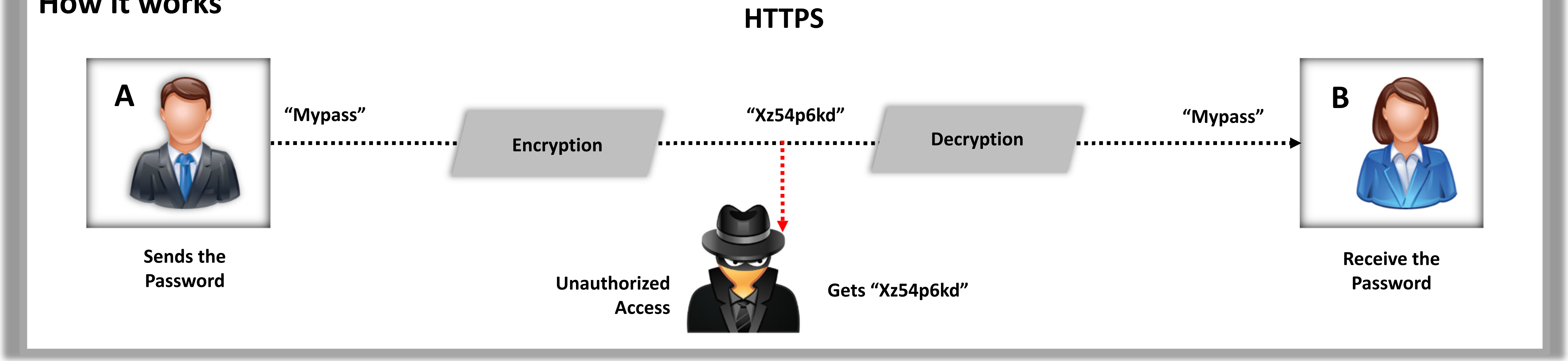


Note: Not all Web browsers and servers support S-HTTP

Hyper Text Transfer Protocol Secure (HTTPS)

- HTTPS ensures **secure communication** between two computers over HTTP
- The connection is **encrypted** using Transport Layer Security (TLS) or Secure Sockets Layer (SSL) protocol
- It is often used in **confidential online transactions**
- It protects against **man-in-the-middle attacks** as data is transmitted over encrypted channel
- However, it can be vulnerable to DROWN (Decrypting RSA with Obsolete and Weakened eNcryption) attack

How it works



File Transfer Protocol (FTP)

- File Transfer Protocol (FTP) is the standard networking protocol used for sharing files over the Internet's TCP/IP protocols
- Based on the client-server architecture, FTP uses SSL/TLS and SSH encryptions for data security
- FTP servers provide access to the users using a simple login mechanism

How FTP Works?

FTP uses two connections:

- **Control connection** – transmits commands and replies to those commands between the client and the server
- **Data connection** – for the transfer of data files

FTP supports two modes of operation

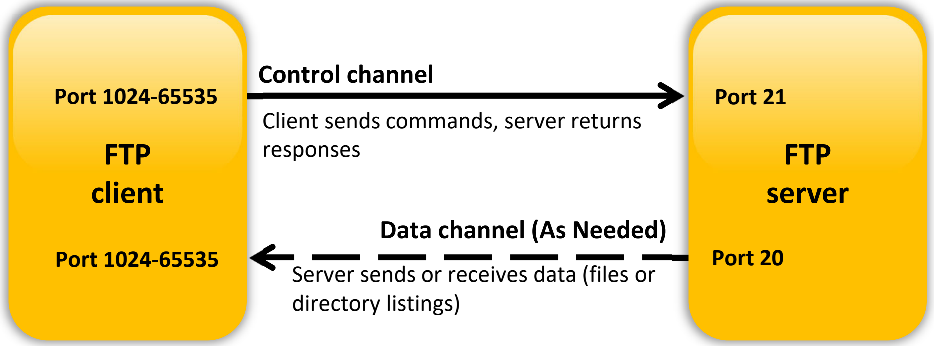
Active Mode

Control connection is made from the FTP client, and all data connections are made from the FTP server to FTP client

Passive Mode

Both control and data connections are made from the FTP client to the FTP server

Active FTP: control In, Data Out



Port 1024-65535

FTP client

Port 1024-65535

Control channel

Client sends commands, server returns responses

Data channel (As Needed)

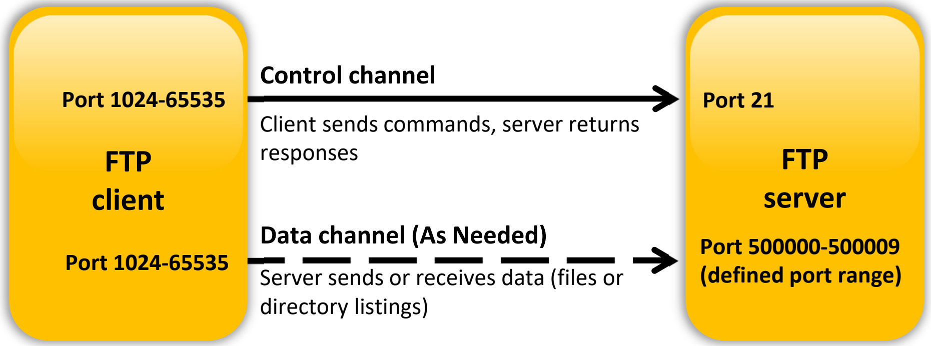
Server sends or receives data (files or directory listings)

Port 21

FTP server

Port 20

Passive FTP: Both connections Inbound



Port 1024-65535

FTP client

Port 1024-65535

Control channel

Client sends commands, server returns responses

Data channel (As Needed)

Server sends or receives data (files or directory listings)

Port 21

FTP server

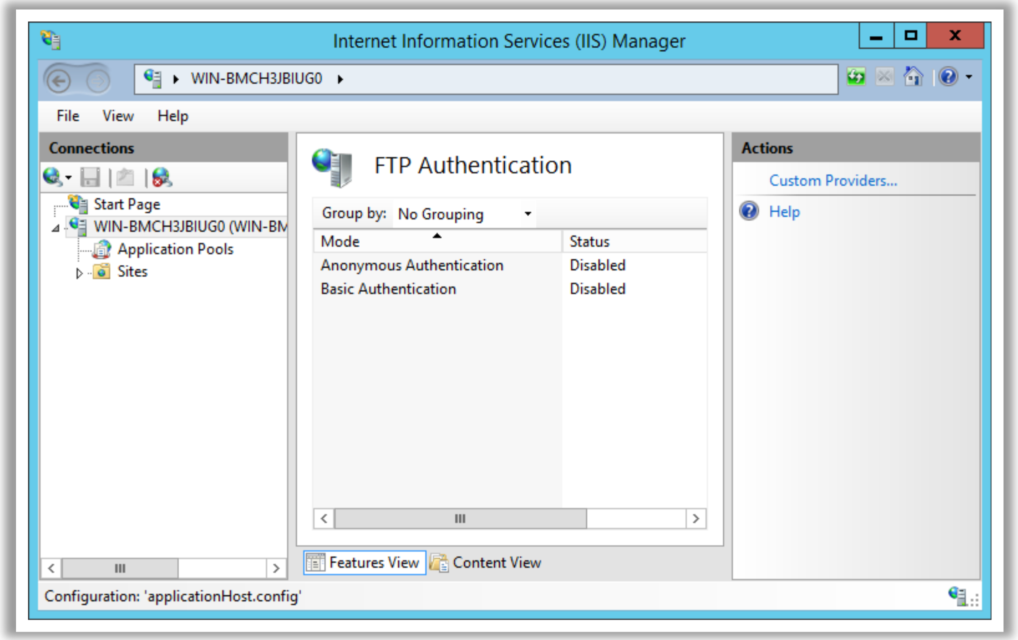
Port 500000-500009 (defined port range)

FTP Anonymous Access and its Risk

Anonymous access to FTP servers:

- Most FTP servers allow anonymous access to the services, wherein the users do not need to have an account on the server or domain
- Users can access FTP servers configured to allow anonymous access without any server credential or by providing any random credential
- Anonymous users can create and store arbitrary files with write permission on the FTP servers
- Attackers can exploit the FTP write access to distribute stolen copyrighted software, malware or other illicit data

Hardening FTP Servers



FTP Authentication

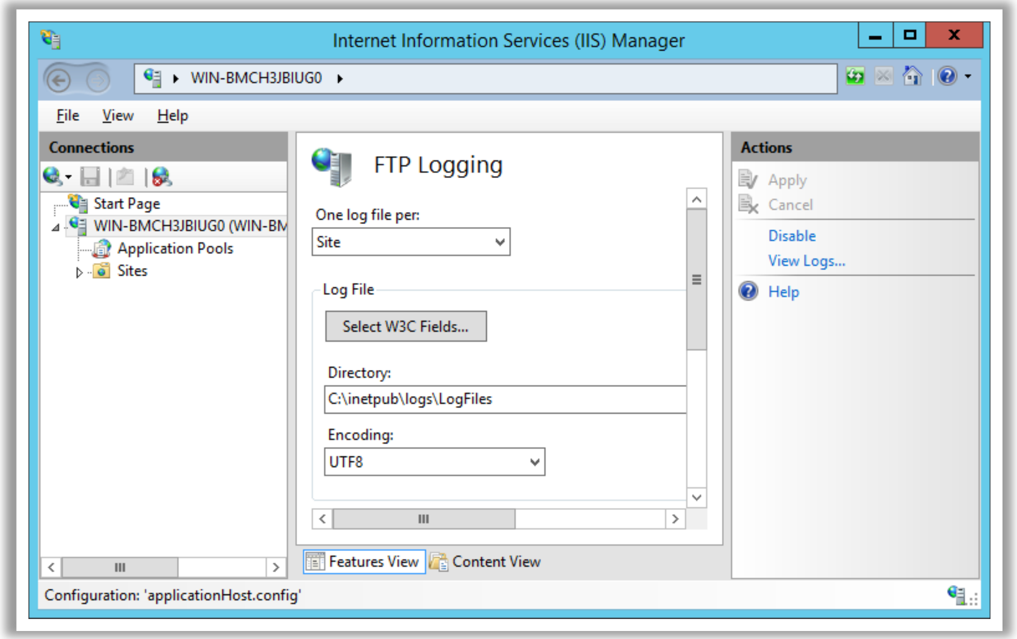
Group by: No Grouping

Mode	Status
Anonymous Authentication	Disabled
Basic Authentication	Disabled

Configuration: 'applicationHost.config'

Disable Anonymous FTP accounts. If not possible, monitor Anonymous FTP accounts regularly

Enable logging for your FTP site



FTP Logging

One log file per: Site

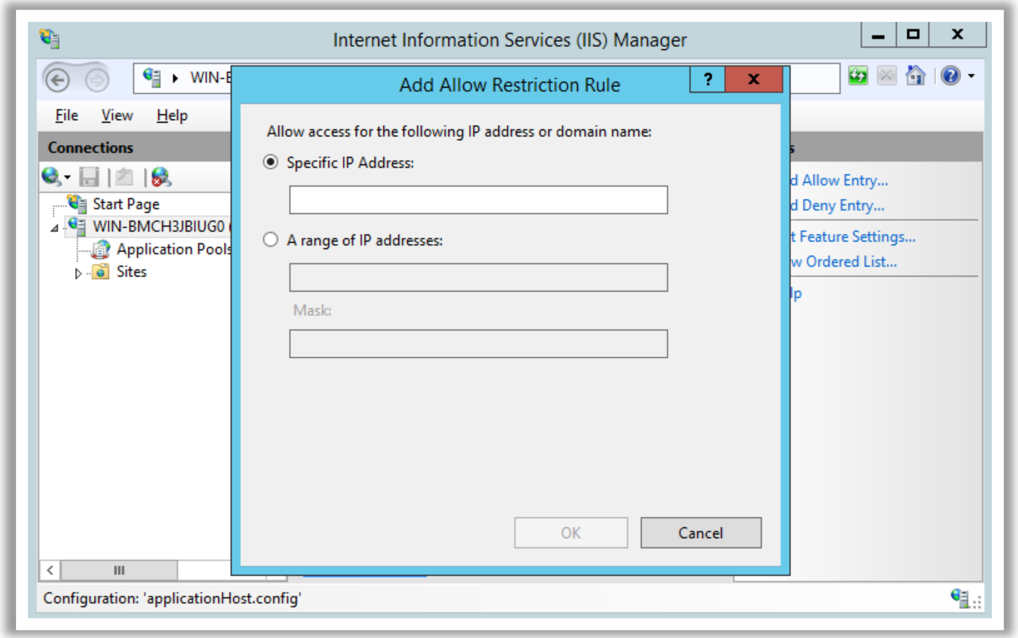
Log File

Directory: C:\inetpub\logs\LogFiles

Encoding: UTF8

Configuration: 'applicationHost.config'

Hardening FTP Servers (Cont'd)



Internet Information Services (IIS) Manager

Add Allow Restriction Rule

Allow access for the following IP address or domain name:

● Specific IP Address:

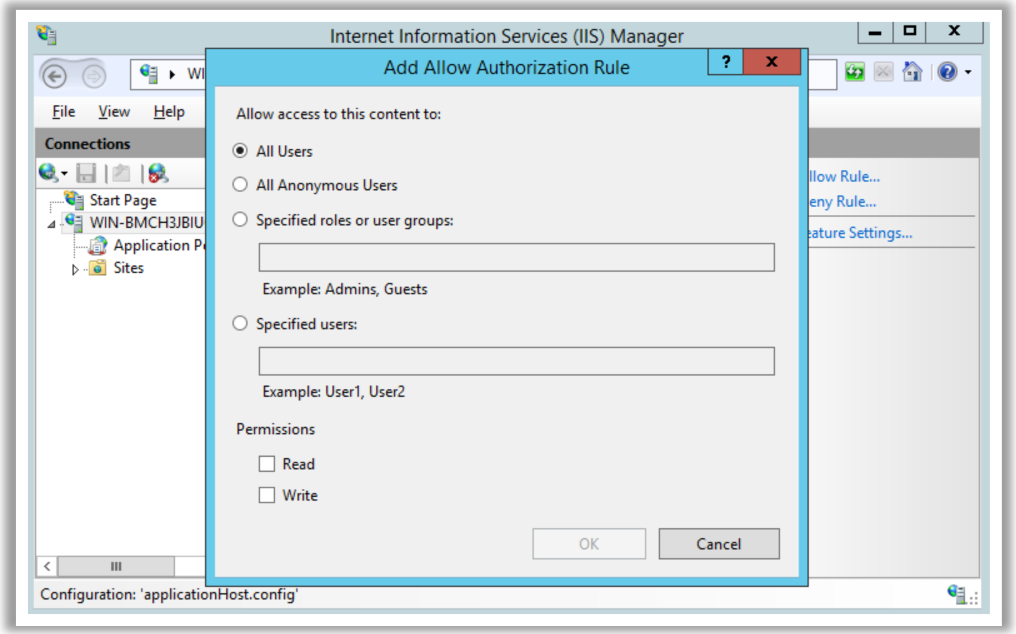
○ A range of IP addresses:

Mask:

Configuration: 'applicationHost.config'

Restrict Access by **IP** or **domain name**

Configure Access controls on authenticated **FTP** accounts with the help of ACLs



Internet Information Services (IIS) Manager

Add Allow Authorization Rule

Allow access to this content to:

● All Users

○ All Anonymous Users

○ Specified roles or user groups:

Example: Admins, Guests

○ Specified users:

Example: User1, User2

Permissions

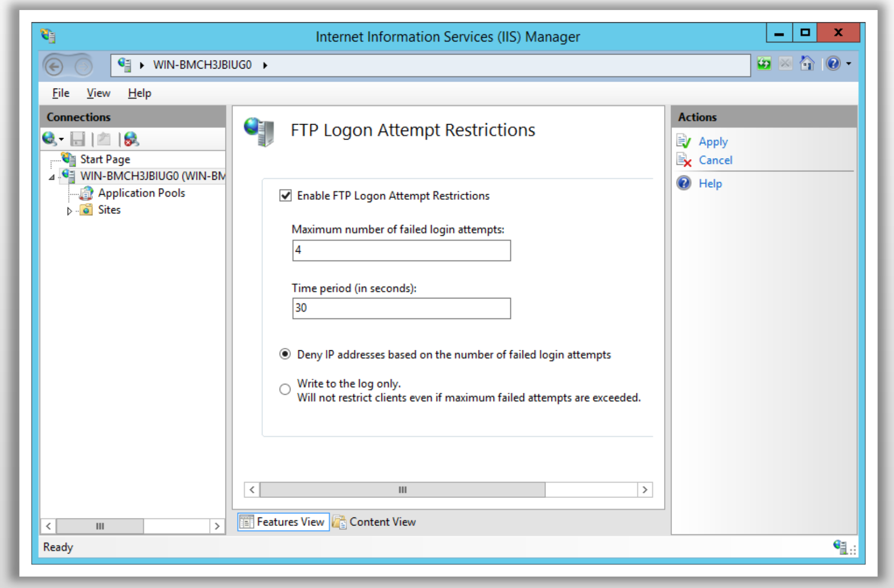
□ Read

□ Write

Configuration: 'applicationHost.config'

Hardening FTP Servers (Cont'd)

Restrict **Logon attempts** and time



FTP Logon Attempt Restrictions

☑ Enable FTP Logon Attempt Restrictions

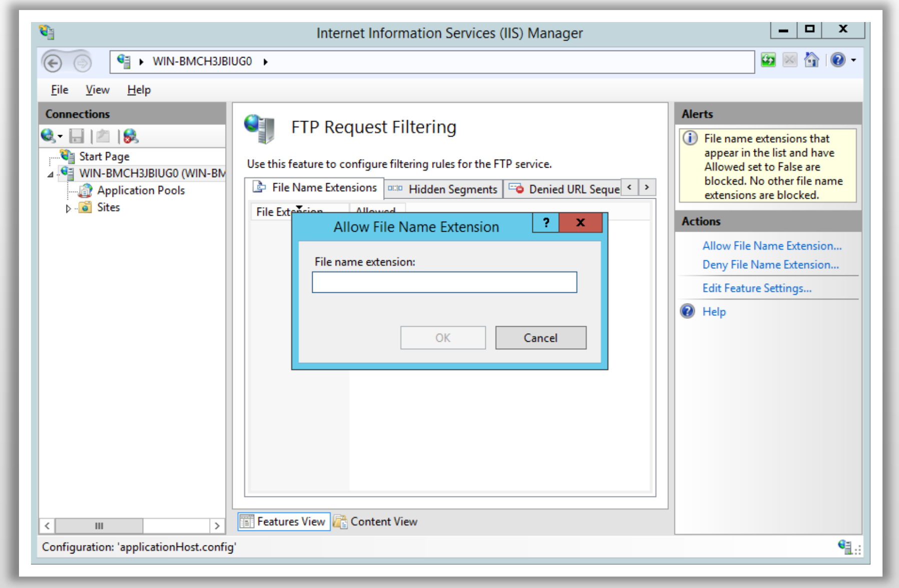
Maximum number of failed login attempts: 4

Time period (in seconds): 30

● Deny IP addresses based on the number of failed login attempts

○ Write to the log only.
Will not restrict clients even if maximum failed attempts are exceeded.

Configure **filtering rules** for your FTP service



FTP Request Filtering

Use this feature to configure filtering rules for the FTP service.

Allow File Name Extension

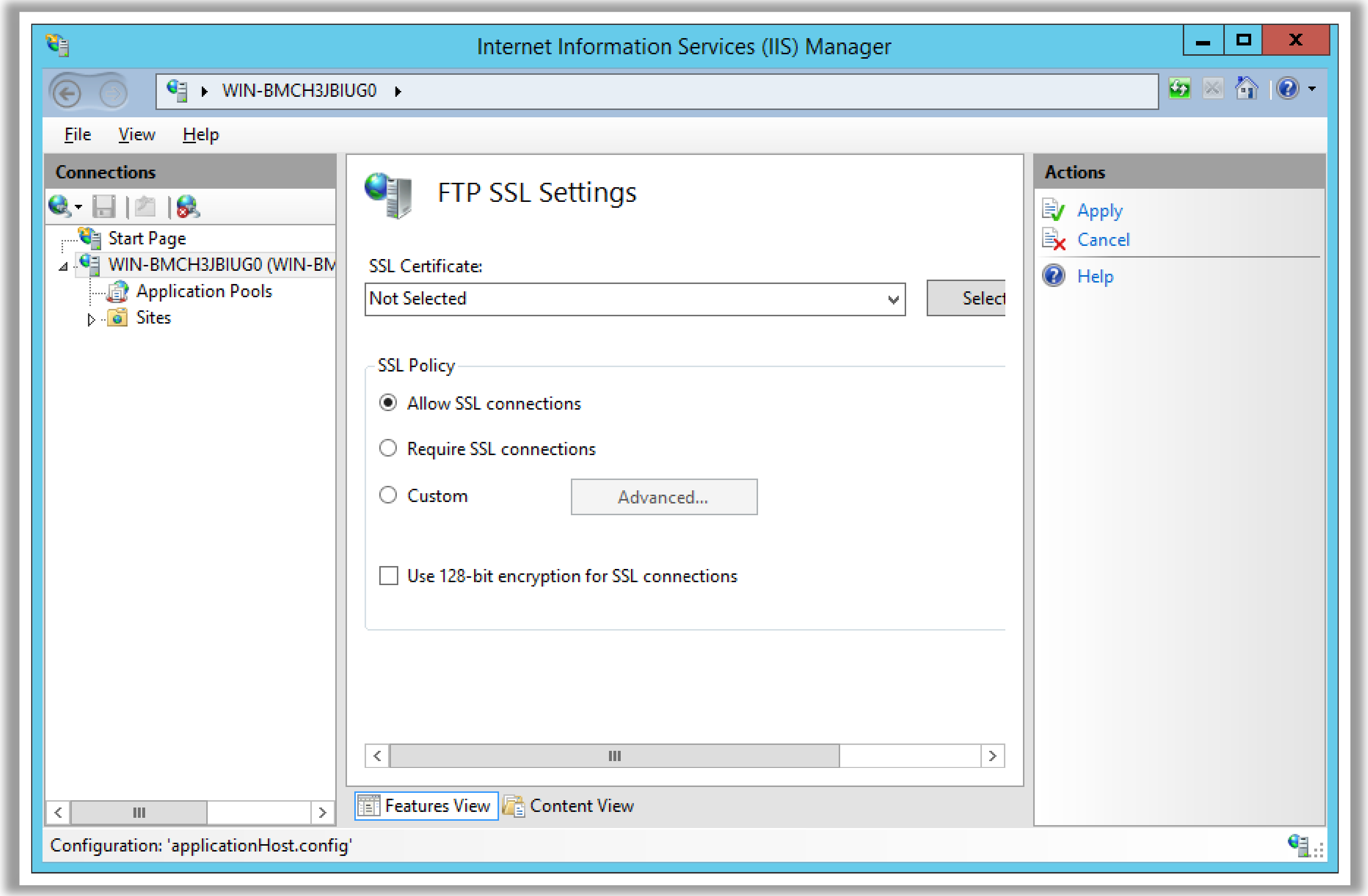
File name extension:

OK Cancel

File name extensions that appear in the list and have Allowed set to False are blocked. No other file name extensions are blocked.

Configuration: 'applicationHost.config'

Hardening FTP Servers (Cont’d)



FTP SSL Settings

SSL Certificate: Not Selected Select

SSL Policy

● Allow SSL connections

○ Require SSL connections

○ Custom Advanced...

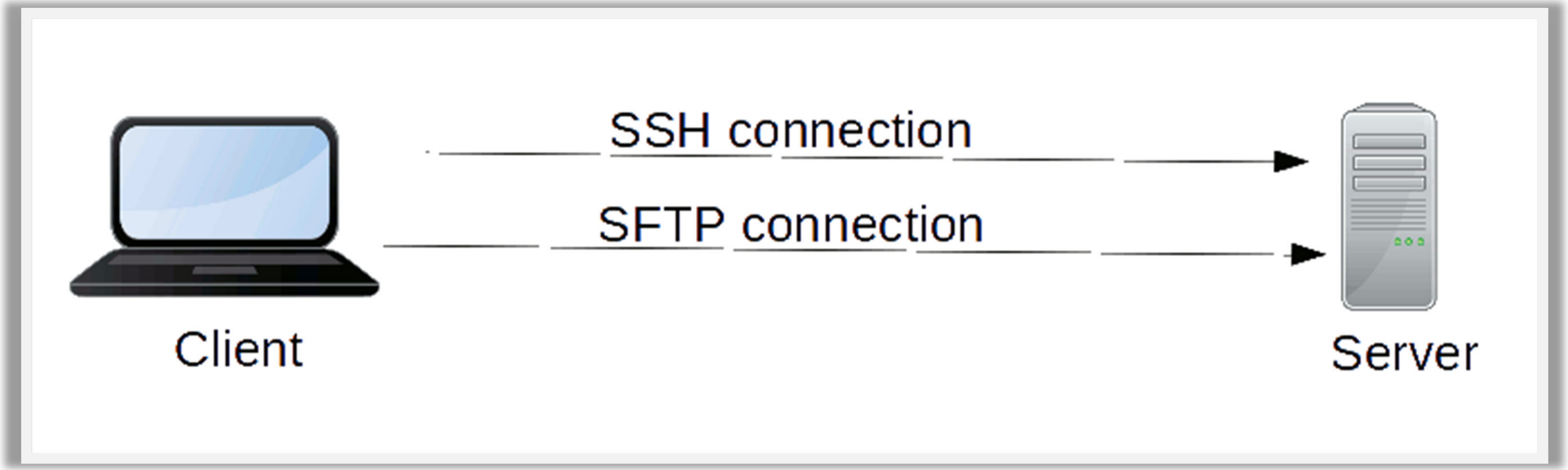
□ Use 128-bit encryption for SSL connections

Configuration: 'applicationHost.config'

Use **SSL / FTPS** for authenticated FTP accounts

Secure File Transfer Protocol (SFTP)

- SFTP is a secure version of FTP and an extension of SSH2 protocol
- It is used for secure file transmission and file access over reliable data stream
- It runs on TCP port 22



Trivial File Transfer Protocol (TFTP)

- TFTP is a lockstep communication protocol
- It transmits files in both directions of a client-server application
- It help in nodes booting on a local area network when the operating system or firmware images are stored on a file server
- TFTP only reads and writes files from or to a remote server. It cannot list, delete, or rename files or directories, and it has no provisions for user authentication
- TFTP is generally only used on local area networks (LAN)
- TFTP constitutes an independent exchange

Weaknesses :

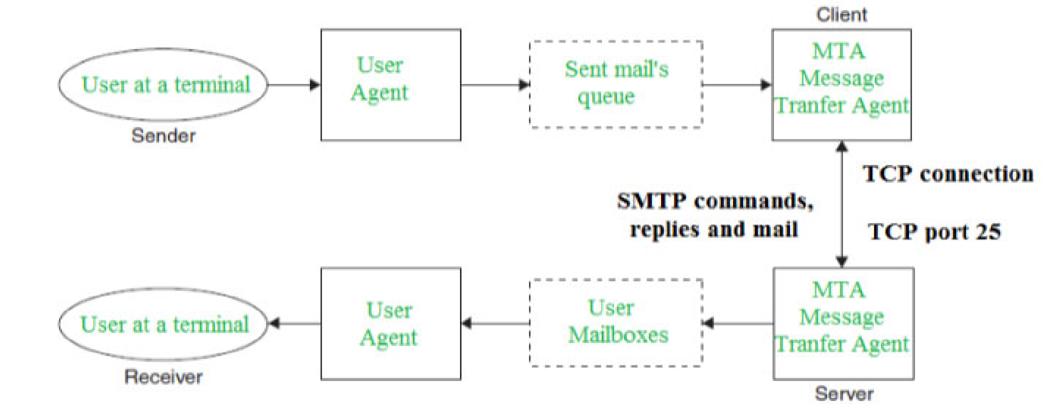
- It is vulnerable to denial of service (DoS) attack
- It is vulnerable to Directory traversal vulnerability

Simple Mail Transfer Protocol (SMTP)

- SMTP is an application layer protocol for electronic mail (email) transmission
- It is a relatively simple and text-based protocol that communicates with the mail server over TCP port 25
- There are two types of SMTP model
  - End to end: Used to communicate between different organization
  - Store and forward : Used to communicate within organization

Features:

- Mail forwarding
- Mail gatewaying
- Mail relaying
- Address debugging
- Mailing list expansion



Model of SMTP system

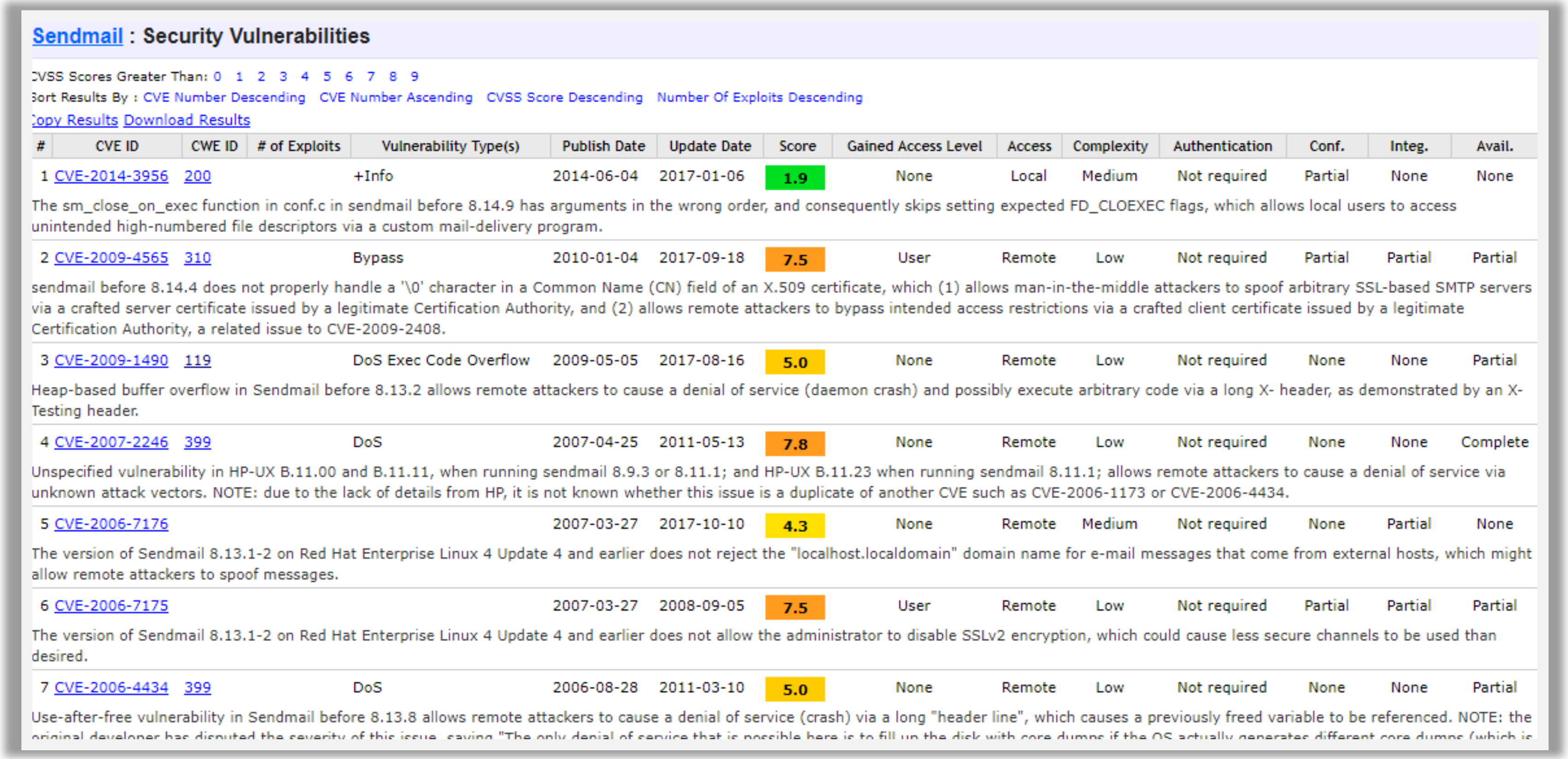
Simple Mail Transfer Protocol (SMTP) (Cont'd)

Advantages:

- SMTP provides the simplest form of communication through mail
- Quick email delivery
- It offers reliability in terms of outgoing email messages
- Easy to connect and can connect to any system having flexibility with existing applications
- Supported on many platform
- Low implementation and administration cost
- Security matters for SMTP are worst
- Limited to 7 bit ASCII characters
- SMTP lacks the security specified in X.400
- Its simplicity limits its usefulness

Sendmail

- Sendmail is the Unix-based implementation of SMTP protocol
- Sendmail has a number of security vulnerabilities in it
- The CVE databases shows the recent security vulnerabilities in Sendmail



Sendmail : Security Vulnerabilities

CVSS Scores Greater Than: 0 1 2 3 4 5 6 7 8 9

Sort Results By : CVE Number Descending CVE Number Ascending CVSS Score Descending Number Of Exploits Descending

Copy Results Download Results

<table>
<tr><th>#</th><th>CVE ID</th><th>CWE ID</th><th># of Exploits</th><th>Vulnerability Type(s)</th><th>Publish Date</th><th>Update Date</th><th>Score</th><th>Gained Access Level</th><th>Access</th><th>Complexity</th><th>Authentication</th><th>Conf.</th><th>Integ.</th><th>Avail.</th></tr>
<tr><td>1</td><td>CVE-2014-3956</td><td>200</td><td></td><td>+Info</td><td>2014-06-04</td><td>2017-01-06</td><td>1.9</td><td>None</td><td>Local</td><td>Medium</td><td>Not required</td><td>Partial</td><td>None</td><td>None</td></tr>
<tr><td colspan="15">The sm_close_on_exec function in conf.c in sendmail before 8.14.9 has arguments in the wrong order, and consequently skips setting expected FD_CLOEXEC flags, which allows local users to access unintended high-numbered file descriptors via a custom mail-delivery program.</td></tr>
<tr><td>2</td><td>CVE-2009-4565</td><td>310</td><td></td><td>Bypass</td><td>2010-01-04</td><td>2017-09-18</td><td>7.5</td><td>User</td><td>Remote</td><td>Low</td><td>Not required</td><td>Partial</td><td>Partial</td><td>Partial</td></tr>
<tr><td colspan="15">sendmail before 8.14.4 does not properly handle a '\0' character in a Common Name (CN) field of an X.509 certificate, which (1) allows man-in-the-middle attackers to spoof arbitrary SSL-based SMTP servers via a crafted server certificate issued by a legitimate Certification Authority, and (2) allows remote attackers to bypass intended access restrictions via a crafted client certificate issued by a legitimate Certification Authority, a related issue to CVE-2009-2408.</td></tr>
<tr><td>3</td><td>CVE-2009-1490</td><td>119</td><td></td><td>DoS Exec Code Overflow</td><td>2009-05-05</td><td>2017-08-16</td><td>5.0</td><td>None</td><td>Remote</td><td>Low</td><td>Not required</td><td>None</td><td>None</td><td>Partial</td></tr>
<tr><td colspan="15">Heap-based buffer overflow in Sendmail before 8.13.2 allows remote attackers to cause a denial of service (daemon crash) and possibly execute arbitrary code via a long X- header, as demonstrated by an X-Testing header.</td></tr>
<tr><td>4</td><td>CVE-2007-2246</td><td>399</td><td></td><td>DoS</td><td>2007-04-25</td><td>2011-05-13</td><td>7.8</td><td>None</td><td>Remote</td><td>Low</td><td>Not required</td><td>None</td><td>None</td><td>Complete</td></tr>
<tr><td colspan="15">Unspecified vulnerability in HP-UX B.11.00 and B.11.11, when running sendmail 8.9.3 or 8.11.1; and HP-UX B.11.23 when running sendmail 8.11.1; allows remote attackers to cause a denial of service via unknown attack vectors. NOTE: due to the lack of details from HP, it is not known whether this issue is a duplicate of another CVE such as CVE-2006-1173 or CVE-2006-4434.</td></tr>
<tr><td>5</td><td>CVE-2006-7176</td><td></td><td></td><td></td><td>2007-03-27</td><td>2017-10-10</td><td>4.3</td><td>None</td><td>Remote</td><td>Medium</td><td>Not required</td><td>None</td><td>Partial</td><td>None</td></tr>
<tr><td colspan="15">The version of Sendmail 8.13.1-2 on Red Hat Enterprise Linux 4 Update 4 and earlier does not reject the "localhost.localdomain" domain name for e-mail messages that come from external hosts, which might allow remote attackers to spoof messages.</td></tr>
<tr><td>6</td><td>CVE-2006-7175</td><td></td><td></td><td></td><td>2007-03-27</td><td>2008-09-05</td><td>7.5</td><td>User</td><td>Remote</td><td>Low</td><td>Not required</td><td>Partial</td><td>Partial</td><td>Partial</td></tr>
<tr><td colspan="15">The version of Sendmail 8.13.1-2 on Red Hat Enterprise Linux 4 Update 4 and earlier does not allow the administrator to disable SSLv2 encryption, which could cause less secure channels to be used than desired.</td></tr>
<tr><td>7</td><td>CVE-2006-4434</td><td>399</td><td></td><td>DoS</td><td>2006-08-28</td><td>2011-03-10</td><td>5.0</td><td>None</td><td>Remote</td><td>Low</td><td>Not required</td><td>None</td><td>None</td><td>Partial</td></tr>
<tr><td colspan="15">Use-after-free vulnerability in Sendmail before 8.13.8 allows remote attackers to cause a denial of service (crash) via a long "header line", which causes a previously freed variable to be referenced. NOTE: the original developer has disputed the severity of this issue, saying "The only denial of service that is possible here is to fill up the disk with core dumps if the OS actually generates different core dumps (which is</td></tr>
</table>

Mail Relaying

- **Mail Relay:**
  - Mail Relay is an email server used to destined an e-mail to the correct destination
- **Open Relay:**
  - An open relay is SMTP server that allows third party to relay of e-mail messages
  - It allows sending messages from anyone to anyone over the internet instead of it restricting for or from a local user
  - It is generally the default configuration for mail server
  - It is considered insecure way of mail relaying
- **Close Relay:**
  - The inbound and outbound emails are allowed from known users only
  - The restrictions are imposed by authentication or maintaining trusted list of Local IP addresses
  - It is typically used in local networks

S/MIME

1

S/MIME (Secure/Multipurpose Internet Mail Extensions) is an application layer protocol which is used to send **digitally signed** and **encrypted email messages**

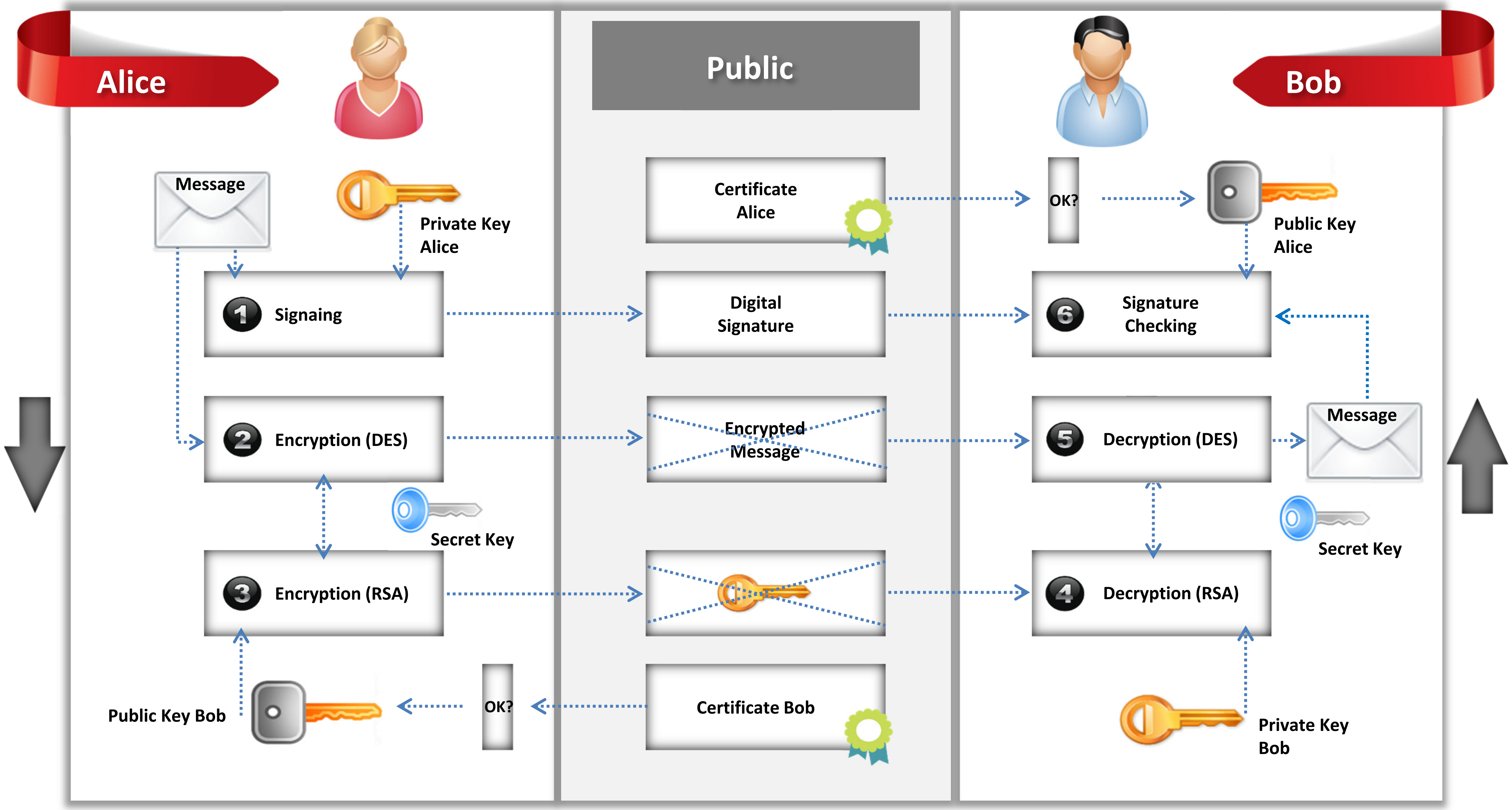
2

It uses **RSA** for digital signature and DES for message encryption

3

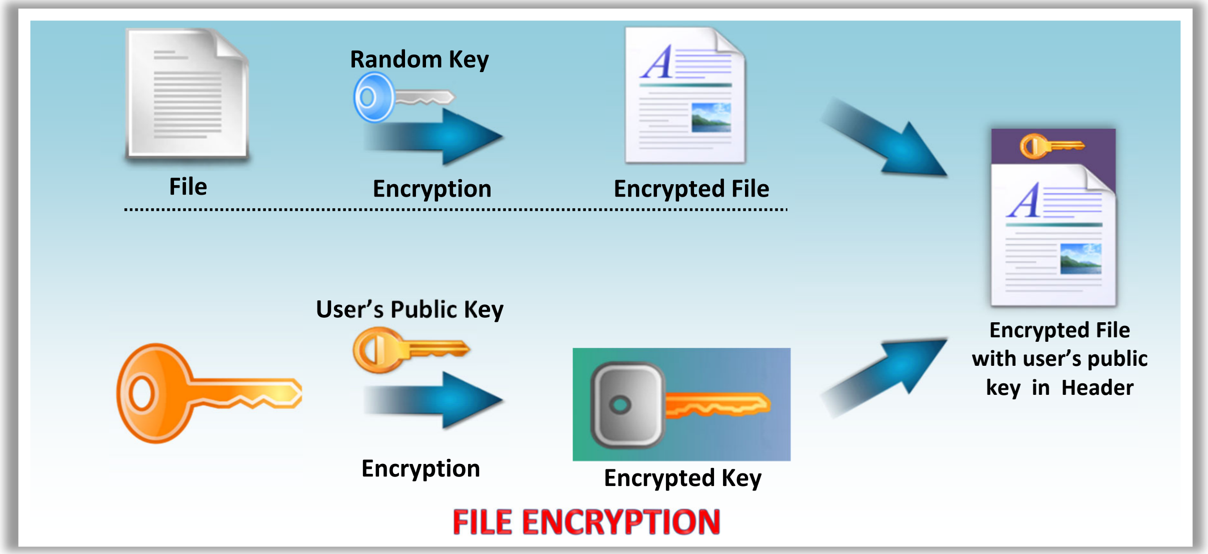
Administrators need to **enable** S/MIME-based security for mailboxes in their organizations

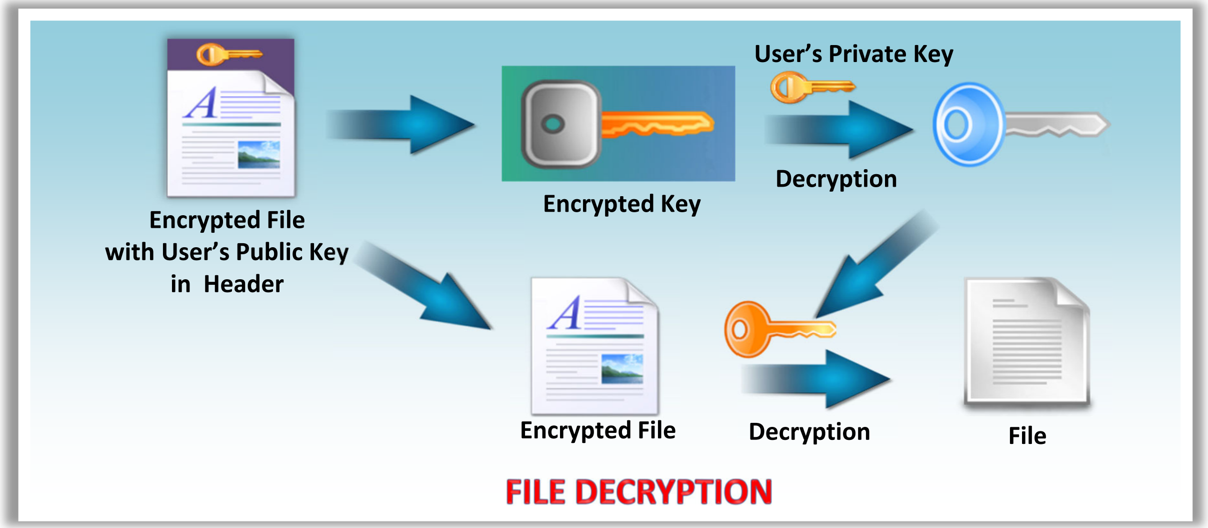
How it Works?


Alice
Public
Bob
Message
Private Key Alice
1 Signaing
2 Encryption (DES)
Secret Key
3 Encryption (RSA)
Public Key Bob
OK?
Certificate Alice
Digital Signature
Encrypted Message
Certificate Bob
OK?
Public Key Alice
6 Signature Checking
5 Decryption (DES)
Message
Secret Key
4 Decryption (RSA)
Private Key Bob

Pretty Good Privacy (PGP)

- PGP is an application layer protocol which provides **cryptographic privacy** and authentication for network communication
- It encrypts and decrypts email communication as well as authenticates messages with **digital signatures** and encrypts stored files





Difference between PGP and S/MIME

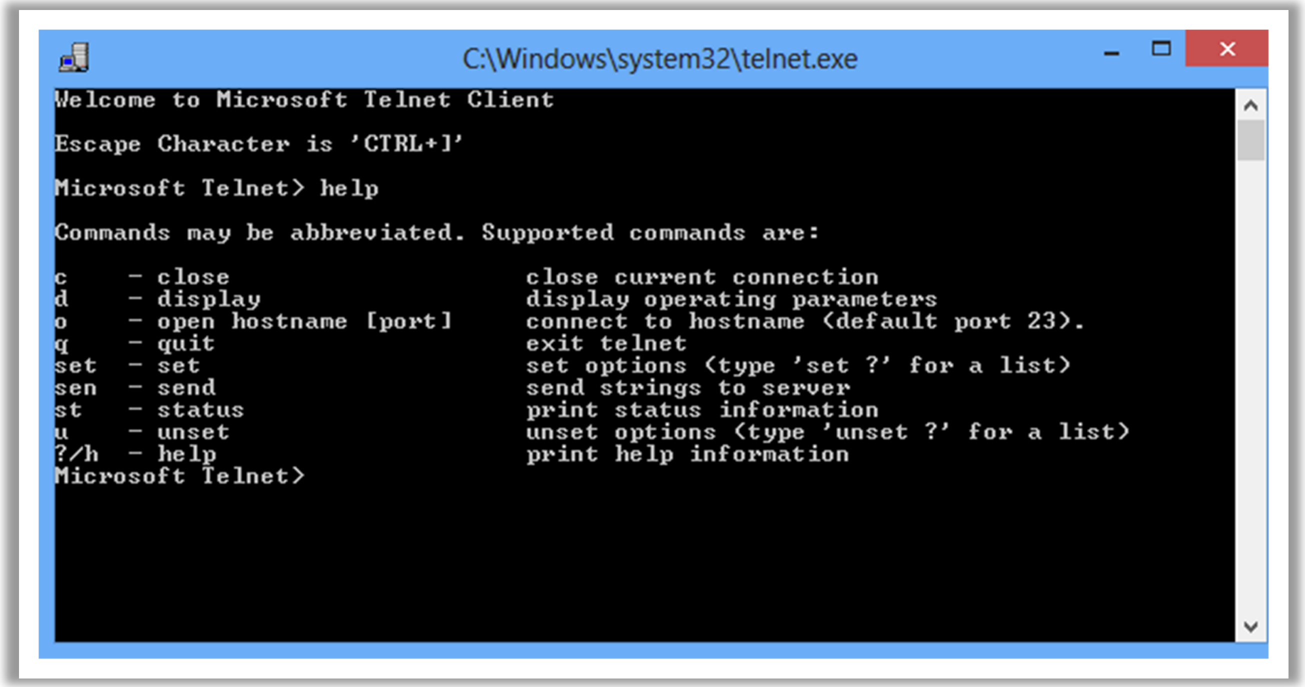
Mandatory Features	S/MIME v3	OpenPGP
Message Format	Binary, Based on CMS	Application/Pkcs 7-mime
Certificate Format	Binary, Based on X.509v3	Binary, Based on previous PGP
Symmetric Encryption Algorithm	Triple DES (DES, EDE3, CBC)	Triple DES (DES, EDE3, Eccentric CFB)
Signature Algorithm	Diffie-Hellman (X9.42) with DSS or RSA	ElGamal with DSS
Hash Algorithm	SHA- 1	SHA- 1
MIME Encapsulation of Signed Data	Choice of Multipart/signed or CMS Format	Multipart/signed ASCII armor
MIME Encapsulation of Encrypted Data	Application/Pkcs 7-mime	Multipart/Encrypted

Telnet

- Telnet (telecommunications network) is a **TCP/IP protocol** used on LAN, which helps a user/administrator to **access** remote computers over a network

Advantages

- Allows to log on to a remote computer and execute programs
- Allows to control Web servers remotely and enable communication with other servers on the network
- Fast and efficient even when the network and system loads are high



```
Welcome to Microsoft Telnet Client

Escape Character is 'CTRL+]'

Microsoft Telnet> help

Commands may be abbreviated. Supported commands are:

c    - close                    close current connection
d    - display                  display operating parameters
o    - open hostname [port]     connect to hostname (default port 23).
q    - quit                     exit telnet
set  - set                      set options (type 'set ?' for a list)
sen  - send                     send strings to server
st   - status                   print status information
u    - unset                    unset options (type 'unset ?' for a list)
?/h  - help                     print help information
Microsoft Telnet>
```

Weaknesses

- Vulnerable to denial of service attack
- Vulnerable to Packet sniffing attack
- Telnet is not secure as it passes all data in clear text
- Eavesdropping attack is also possible on the telnet network

Telnet (Cont'd)

Cisco Reverse Telnet

- In reverse telnet, instead of providing a command shell to the host devices, the server side of the connection reads and writes data to a computer terminal line
- Generally, it is implemented on the embedded devices which has Ethernet network interface and serial ports
- Use of reverse telnet is not only limited to modem connection or other asynchronous devices but can be used for connecting to the console part of the router, switch, etc.
- To connect using reverse telnet, one should know the IP address of the terminal server hardware interfaces

Weaknesses:

- Remote attacker could send extremely large amount packets to reverse telnet; this causes denial-of-service attack

SSH

- SSH, also known as Secure Shell, is another network management protocol primarily used in UNIX and Linux environments.
- It is mainly used for secure remote login
- It builds a secure, encrypted tunnel for exchanging information between the network management software and the devices
- Here, administrators have to provide a username, password, and port number combination for authentication

SSH Authentication Mechanism

1. Simple Authentication: Authentication is performed based on user's password

2. Key-based Authentication: SSH allows key pair-based authentication

- User needs to generate public and a private key.
- The keys are generated using ssh-keygen -t rsa or ssh-keygen -t dsa
- The private keys are used by the users next time when they try to establish a connection
- The public key has to be saved in ~/.ssh/authorized_keys

3. Host-based authentication: If the host-based authentication is enabled on the target machine, then users on a trusted host can log on to the target machine using the same username. To enable this feature, set setuid bit on /usr/lib/ssh/ssh-keysign (32-bit systems) or/usr/lib64/ssh/ssh-keysign (64-bit systems)

SSH (Cont'd)

Weaknesses :

- It is vulnerable to Man-In-the-Middle attack
- Lack of confidentiality, integrity, and authenticity in the access control files

Recommendation for Securing SSH

- Strong password and username should be used
- Root logins need to be disabled
- There should be limited user logins
- Protocol 1 should be disabled
- Non-Standard port should be used
- Authenticate using public or private keys

SOAP (Simple Object Access Protocol)

- It is an XML-Based messaging protocol used to transmit data between computers
- It provides data transport for Web services and is independent of both platform as well as language; SOAP can be used in any language
- It has three different characteristics: extensibility, neutrality and independence
- It is equivalent to RPC (Remote Procedure Calls), which is used in technologies like DCOM and COBRA

Weaknesses:

- Statelessness
- Too much reliance on HTTP
- Slower than CORBA or RMI or IIOP due to the lengthy XML format that it has to follow and the parsing of the envelop that is required
- It depends on WSDL and does not have any standardized mechanism for dynamic discovery of the services

Simple Network Management Protocol (SNMP)

- SNMP is an application layer protocol which manages TCP/IP based network based on client server architecture
- It can collect and manage the information about the devices on TCP/IP based networks
- Network devices that supports SNMP includes router, hub modem, printer, bridges, switches, servers, workstations, etc.

Common risks to Cisco IOS SNMP configurations

- DDoS attack
- SNMP Remote Code Execution

NTP (Network Time Protocol)

- NTP is used to synchronize the computer clock times in a network
- The NTP client initiates a time request exchange with the NTP server

Features:

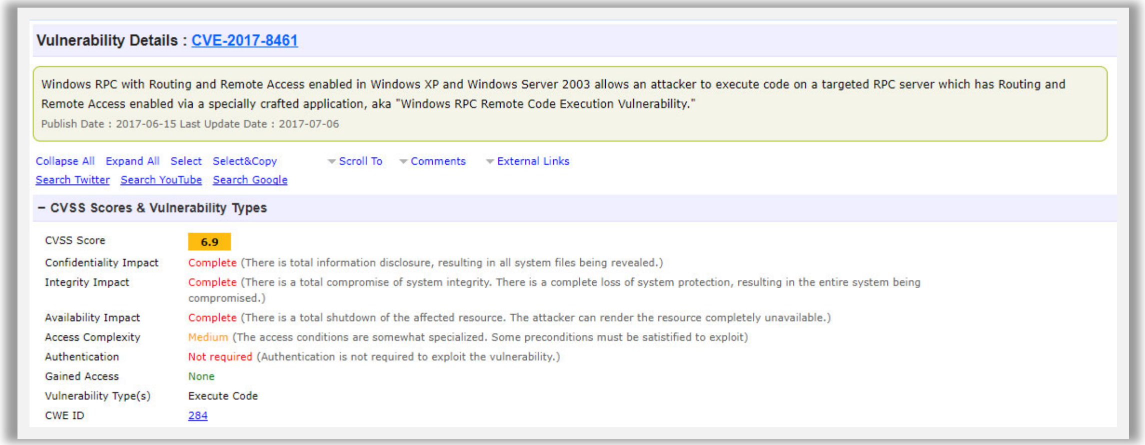
- Uses UTC as a reference time
- Highly scalable

Weaknesses :

- It is vulnerable to denial-of-service attack/DDoS amplification attack
- Intruder can intercept the packets between authentic client and server
- Intruder can replay on one or more packets

RPC (Remote Procedure Call)

- Remote Procedure Call (RPC) is a protocol that allows inter-process communication between two programs (client and server) without having to understand the network's details
- Some of the RPC services on Unix are Network Information Service, Network File System, and Common Desktop Environment,
- Some of the recent RPC vulnerabilities on Windows and Linux platform:
  - Microsoft Windows Remote Procedure Call Security Bypass Vulnerability
  - Microsoft RPC DCOM Interface Overflow
  - Microsoft Windows RPC CVE-2017-8461 Remote Code Execution Vulnerability
  - Multiple Linux Vendor rpc.statd Remote Format String Vulnerability
  - Port 111 rpcbind Vulnerability



Vulnerability Details : CVE-2017-8461

Windows RPC with Routing and Remote Access enabled in Windows XP and Windows Server 2003 allows an attacker to execute code on a targeted RPC server which has Routing and Remote Access enabled via a specially crafted application, aka "Windows RPC Remote Code Execution Vulnerability."

Publish Date : 2017-06-15 Last Update Date : 2017-07-06

– CVSS Scores & Vulnerability Types

CVSS Score	6.9
Confidentiality Impact	Complete (There is total information disclosure, resulting in all system files being revealed.)
Integrity Impact	Complete (There is a total compromise of system integrity. There is a complete loss of system protection, resulting in the entire system being compromised.)
Availability Impact	Complete (There is a total shutdown of the affected resource. The attacker can render the resource completely unavailable.)
Access Complexity	Medium (The access conditions are somewhat specialized. Some preconditions must be satistified to exploit)
Authentication	Not required (Authentication is not required to exploit the vulnerability.)
Gained Access	None
Vulnerability Type(s)	Execute Code
CWE ID	284

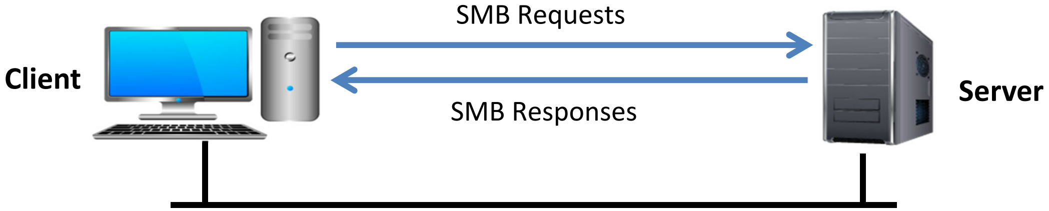
Server Message Block (SMB) Protocol

1. The Server Message Block (SMB) is an **application-layer** network protocol used to provide shared access to files, printers, serials ports, etc. between the **nodes** of a network

2. It provides an authenticated **inter-process communication** mechanism and is widely used by Microsoft Windows

3. SMB works through a client-server approach
   - Client makes specific **requests** to the server, and the server responds accordingly
   - Based on the request made, the server makes their **file systems** and other resources available to clients on the network

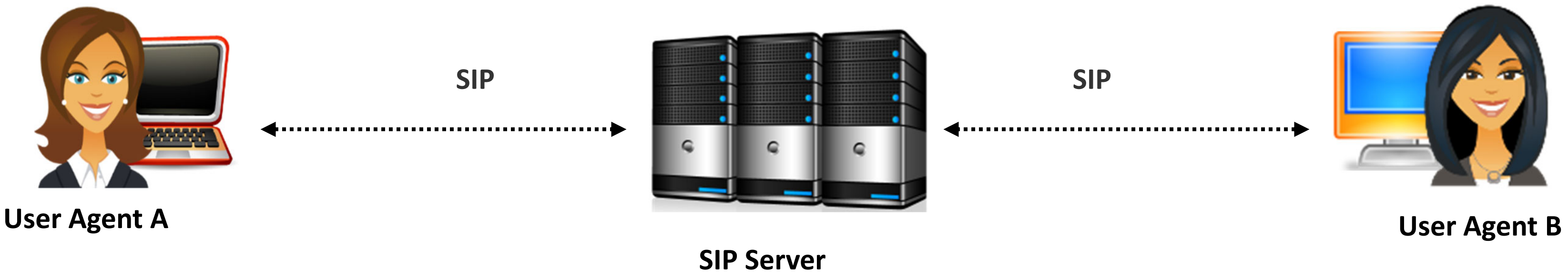
4. The transport layer protocol that **Microsoft SMB Protocol** is most often used with is NetBIOS over TCP/IP (NBT)



Note: The enhanced version of SMB called Common Internet File System (CIFS) was developed by Microsoft for open use on the Internet

Session Initiation Protocol (SIP)

- ❑ SIP is a communications protocol that is used for signaling and controlling real-time multimedia sessions that involve voice, video, instant messaging and other communication applications
- ❑ It works in conjunction with various other protocols like SDP, RTP, SRTP, TLS, etc.
- ❑ SIP determines user attributes like user location, user availability, user capability, session setup and session management

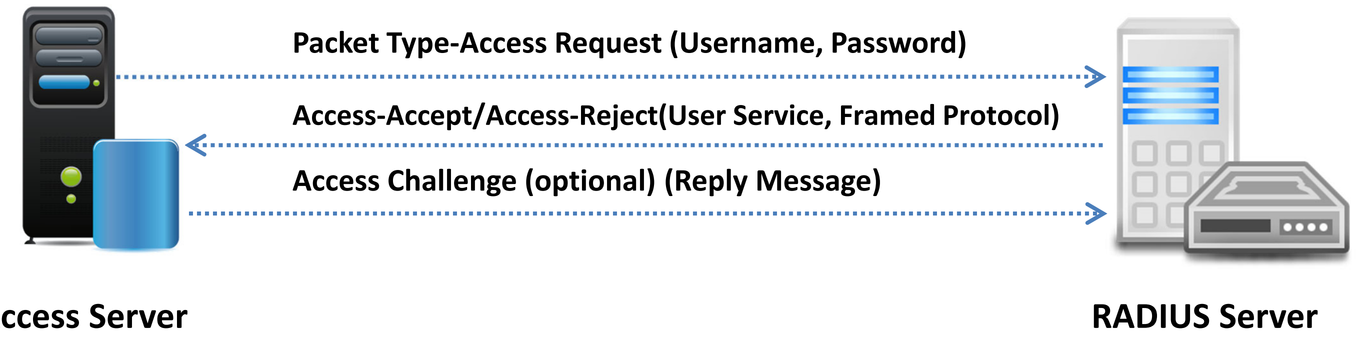


RADIUS

- Remote Authentication Dial-In User Service (RADIUS) is an **authentication protocol** which provides centralized authentication, authorization, and accounting (AAA) for the remote access servers to communicate with the central server

- **Radius Authentication Steps:**

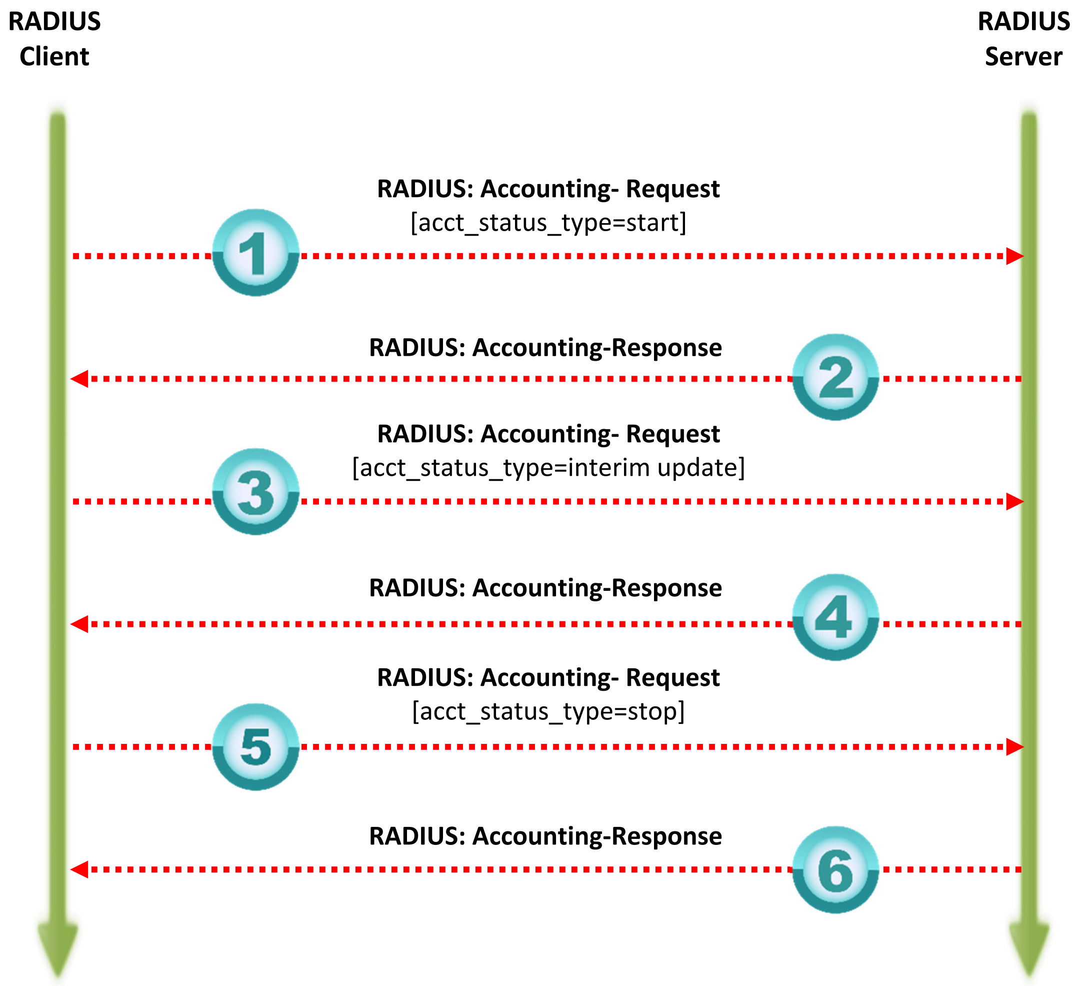
  1. The client initiates the connection by sending **Access-Request packet** to the server
  2. The server receives the access request from the client and compares the credentials with the ones stored in the database. If the provided information matches, then it sends the **Accept-Accept message** along with the **Access-Challenge** to the client for additional authentication, else it sends back Accept Reject message
  3. Client sends the **Accounting-Request** to the server to specify accounting information for a connection that was accepted


Packet Type-Access Request (Username, Password)
Access-Accept/Access-Reject(User Service, Framed Protocol)
Access Challenge (optional) (Reply Message)
Access Server
RADIUS Server

RADIUS (Cont'd)

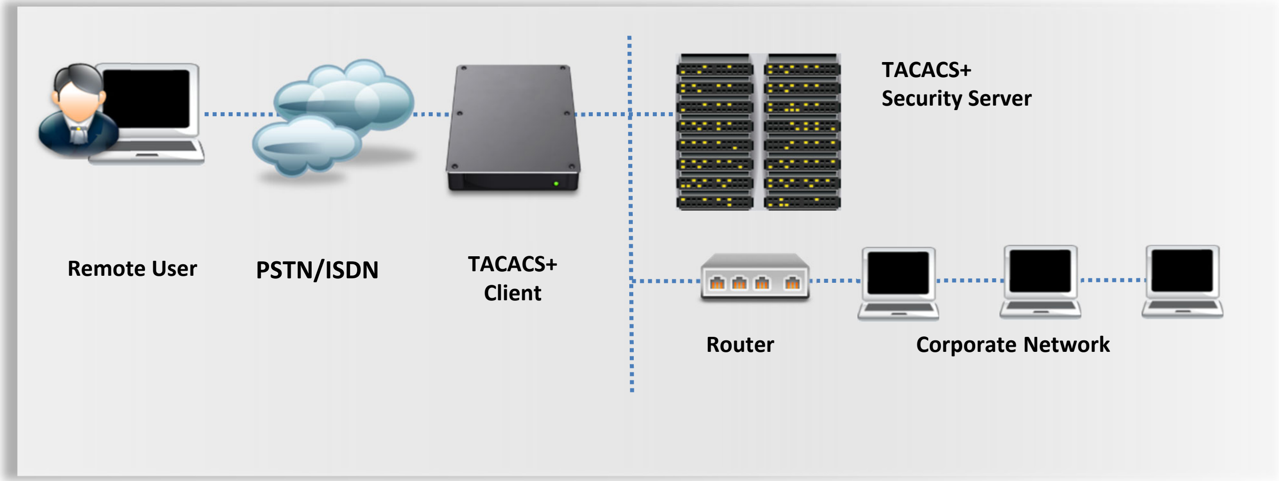
Radius Accounting Steps:

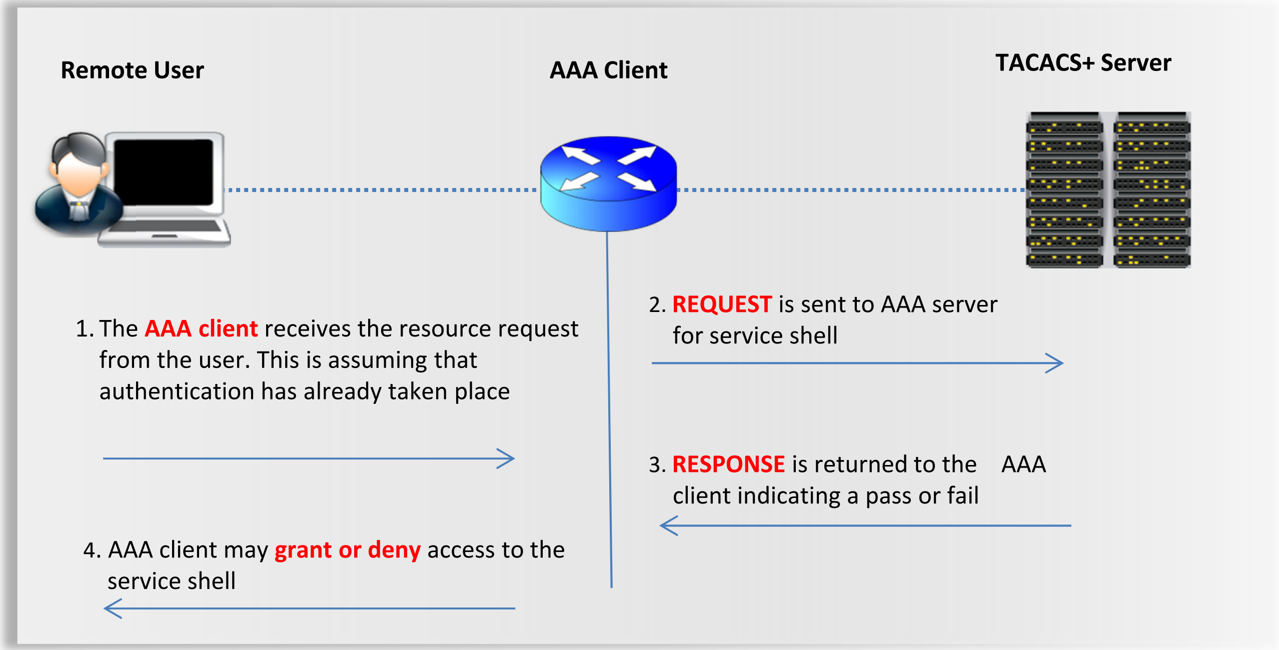
- Client sends the **Accounting-Request** to the server to specify accounting information for a connection that was accepted
- The server receives the Accounting-Request message and sends back the **Accounting-Response message** which states the successful establishment of network


RADIUS Client
RADIUS Server
1
RADIUS: Accounting- Request
[acct_status_type=start]
2
RADIUS: Accounting-Response
3
RADIUS: Accounting- Request
[acct_status_type=interim update]
4
RADIUS: Accounting-Response
5
RADIUS: Accounting- Request
[acct_status_type=stop]
6
RADIUS: Accounting-Response

TACACS+

- ❑ Terminal Access Controller Access-Control System Plus is a **network security protocol** used for authentication, authorization, and accounting for network devices like switches, routers and firewalls through one or more **centralized servers**
- ❑ TACACS+ **encrypts** the entire communication between the client and server including the user's password which protects from sniffing attacks
- ❑ It is a **client server model** approach where the client (user or network device) requests for connection to the server, then the server authenticates the user by examining the credentials
- ❑ Some of the Security Issues with TACACS+:
  - ▪ No integrity checking
  - ▪ Vulnerable to replay attacks
  - ▪ Accounting information is sent in clear text
  - ▪ Weak Encryption





1. The **AAA client** receives the resource request from the user. This is assuming that authentication has already taken place

2. **REQUEST** is sent to AAA server for service shell

3. **RESPONSE** is returned to the AAA client indicating a pass or fail

4. AAA client may **grant or deny** access to the service shell

Routing Information Protocol (RIP)

- It is a Distance Vector routing protocol, specially used for smaller networks
- It uses Internet Protocol (IP) to connect networks for exchanging routing information

RIP includes the following Distance Vector characteristics:

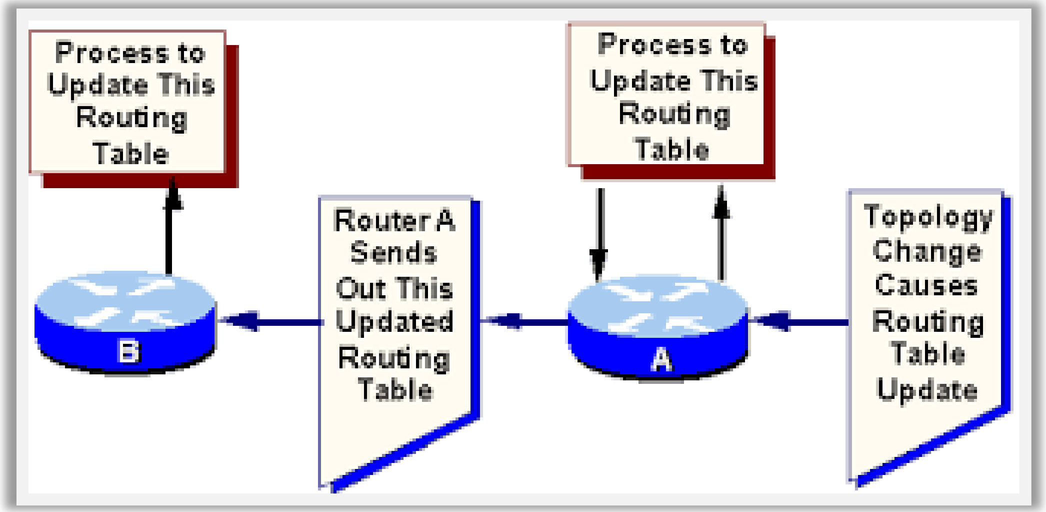
- Periodic routing updates after every 30 seconds
- Includes full routing table after every periodic update
- Broadcast updates
- Neighbors
- It defines the finest "path" to a specific destination through the Bellman-Ford Distance Vector algorithm

Features :

- RIP performs IP and IPX routing
- RIP makes use of UDP port 520
- An administrative distance of RIP routes is 120
- It has a maximum hopcount of 15 hops

RIP Request/Response Process

- Initially, a router sends request to the the full routing table
- Then, the RIP-enabled neighbors send back the response message
- Then, the start-up router sends out the triggered update regarding all RIP enabled interfaces


Process to Update This Routing Table
Process to Update This Routing Table
Router A Sends Out This Updated Routing Table
Topology Change Causes Routing Table Update
B
A

OSPF (Open Shortest Path First)

- It is an Interior Gateway Protocol (IGP) for the Internet, developed to distribute IP routing information throughout a single Autonomous System (AS) in an IP network
- It is also a link-state routing protocol. This means that the routers can exchange topology information with their nearest neighbors
- The OSPF process creates and maintains three different tables
    - A neighbor table : It includes a list of all neighboring routers
    - A topology table : It includes a list of all possible routes to all known networks within an area
    - A routing table : It includes the best route for each known network.

Features:

- It supports only IP routing
- The administrative distance of OSPF routes is 110
- It uses cost as its metric
- It has no hop-count limit

Transport Layer Protocols

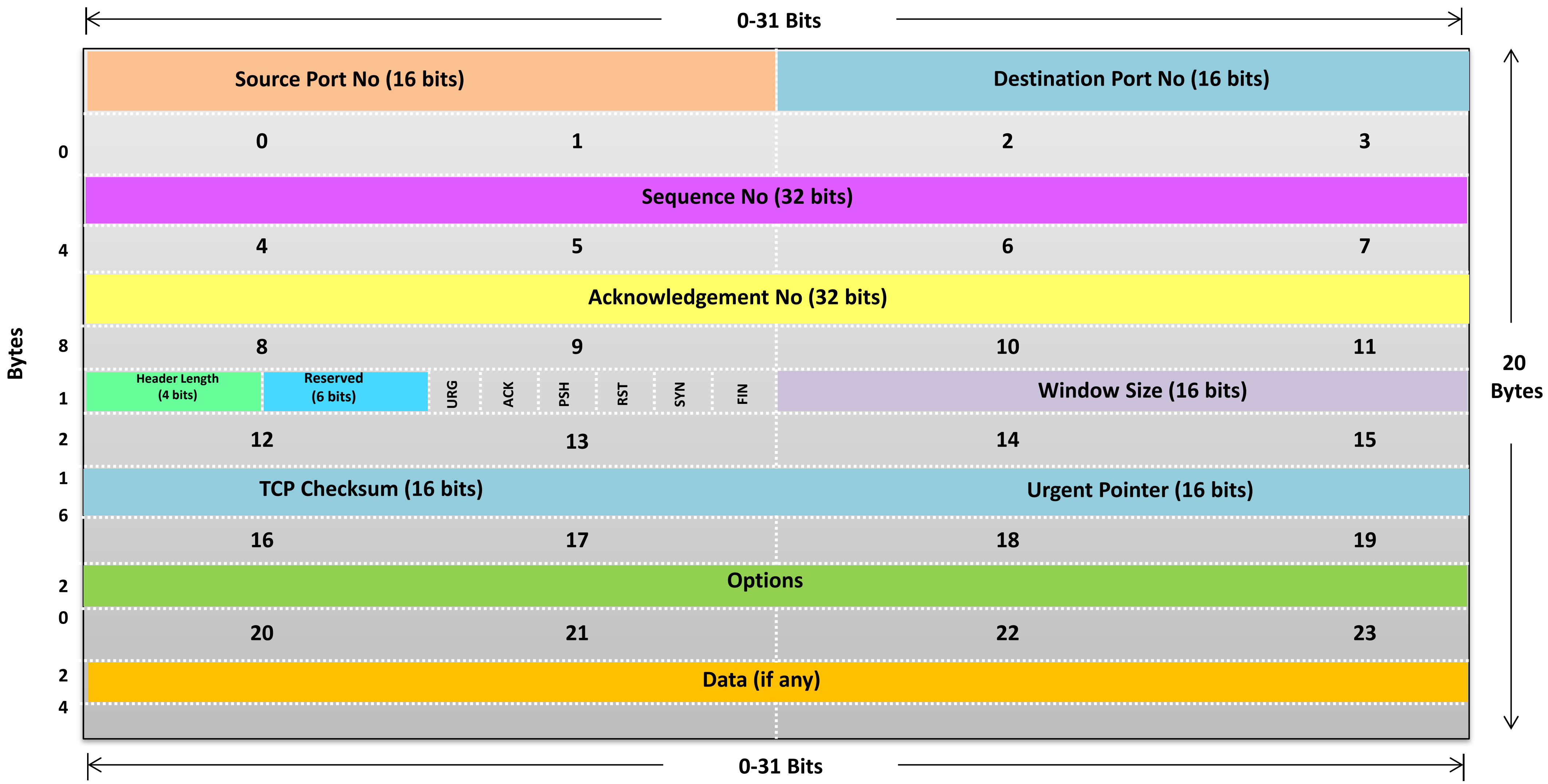
Transmission Control Protocol (TCP)

- TCP is a **connection-oriented** four-layer protocol
- TCP breaks the messages into **segments**, **reassembles** them at the **destination station**, and **resends** the packets that are not received at the destination

The protocols that use TCP include

HTTP (Hypertext Transfer Protocol)
FTP (File Transfer Protocol)
SMTP (Simple Mail Transfer Protocol)
Telnet

TCP Header Format



0-31 Bits

Source Port No (16 bits) | Destination Port No (16 bits)

0 1 2 3

Sequence No (32 bits)

4 5 6 7

Acknowledgement No (32 bits)

8 9 10 11

Header Length (4 bits) | Reserved (6 bits) | URG | ACK | PSH | RST | SYN | FIN | Window Size (16 bits)

12 13 14 15

TCP Checksum (16 bits) | Urgent Pointer (16 bits)

16 17 18 19

Options

20 21 22 23

Data (if any)

0-31 Bits

TCP Services

Simplex

- Each flow has its own window size, sequence numbers, and acknowledgment numbers

1

Half-duplex

- Half-duplex service allows sending information in both directions between two nodes, but only one direction or the other can be utilized at a time

2

Full-duplex

- TCP full-duplex service allows data flow in each direction, independent of the other direction
- Each flow has its own window size, sequence numbers, and acknowledgment numbers

3

User Datagram Protocol (UDP)

- UDP is a connectionless transport protocol that exchanges datagrams, without acknowledgments or guaranteed delivery
- It uses no windowing or acknowledgments, so reliability, if needed, is provided by application layer protocols

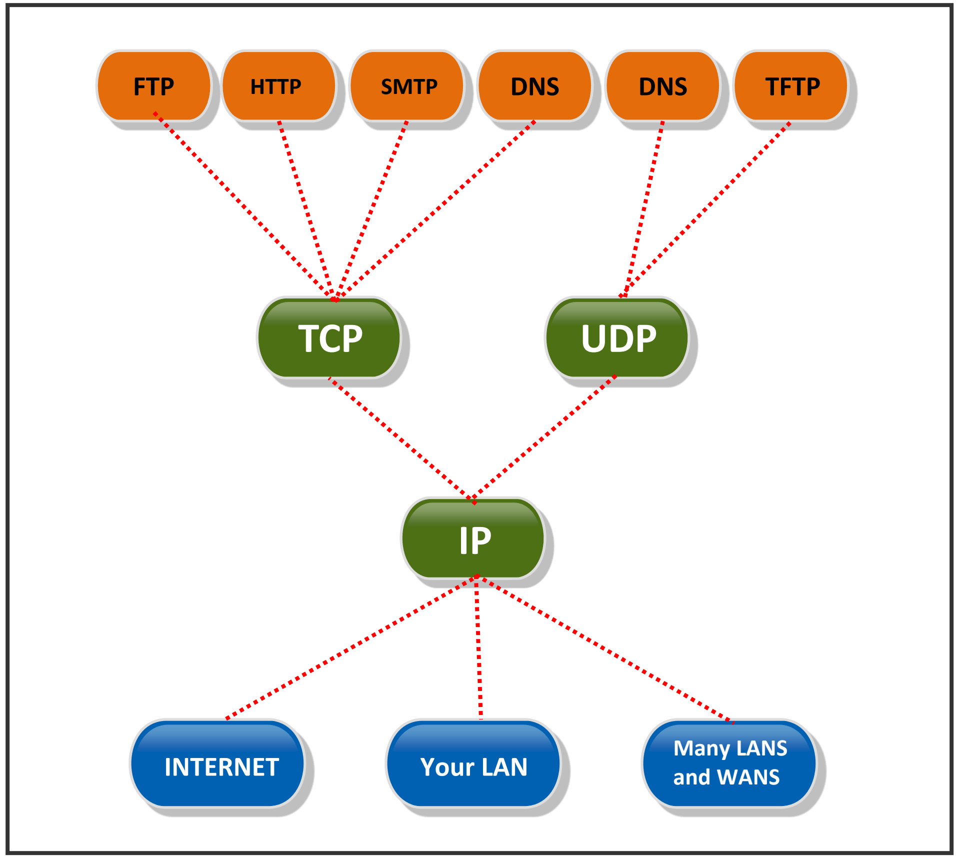
- The protocols that use UDP include:
  - TFTP (Trivial File Transfer Protocol)
  - SNMP (Simple Network Management Protocol)
  - DHCP (Dynamic Host Configuration Protocol)

UDP Segment Format

# of Bits	16	16	16	16	16
	Source Port	Destination Port	Length	Checksum	Data. . .

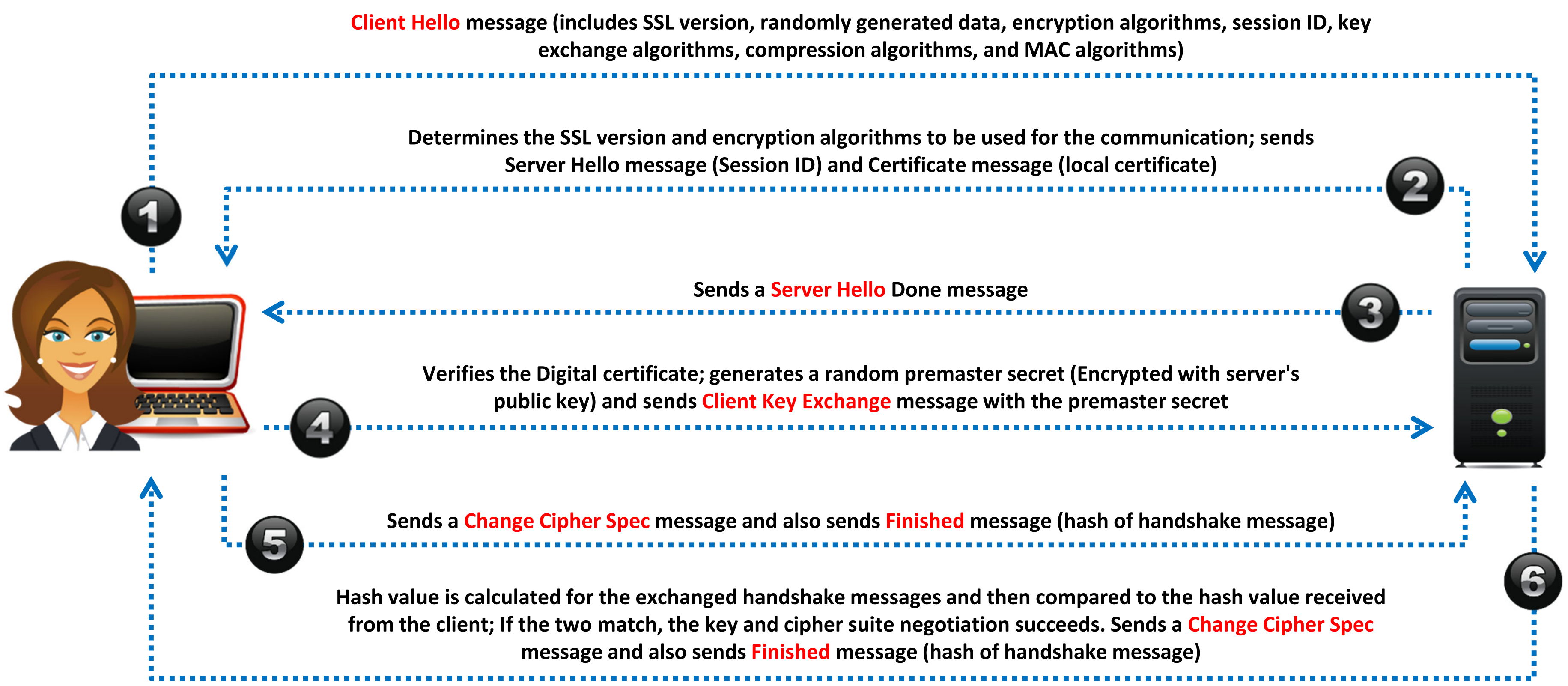
UDP Operation

- UDP does not use windowing or acknowledgments, so application layer protocols must provide error detection
- The Source Port field is an optional field used only if the information needs to return to the sending host
- When a destination router receives a routing update, the source router is not requesting anything~~,~~; so nothing needs to return to the source
- This is regarding only RIP updates:
  - BGP uses TCP; IGRP is sent directly over IP
  - EIGRP and OSPF are also sent directly over IP with their own way of handling reliability



Secure Sockets Layer (SSL)

- SSL is developed by Netscape for **managing the security** of a message transmission on the Internet
- It uses **RSA asymmetric (public key) encryption** to encrypt data transferred over SSL connections



Client Hello message (includes SSL version, randomly generated data, encryption algorithms, session ID, key exchange algorithms, compression algorithms, and MAC algorithms)

Determines the SSL version and encryption algorithms to be used for the communication; sends Server Hello message (Session ID) and Certificate message (local certificate)

Sends a Server Hello Done message

Verifies the Digital certificate; generates a random premaster secret (Encrypted with server's public key) and sends Client Key Exchange message with the premaster secret

Sends a Change Cipher Spec message and also sends Finished message (hash of handshake message)

Hash value is calculated for the exchanged handshake messages and then compared to the hash value received from the client; If the two match, the key and cipher suite negotiation succeeds. Sends a Change Cipher Spec message and also sends Finished message (hash of handshake message)

Secure Sockets Layer (SSL) (Cont'd)

- SSL was first developed by Netscape in 1995. However, SSL 1.0 was not released

- Later, SSL 2.0 was released, but due to a number of security flaws in this protocol, this did not last long, leading to the release of SSL 3.0

- SSL 3.0 has various improvements over SSL 2.0 like:
  - Separation of transport of data from message layer
  - Usage of 128-bit keying material on the existing export cipher
  - Implementation of key exchange protocols like Diffie-Hellman, Fortezza key exchanges as well as non-RSA certificates
  - A possibility of record compression and decompression, etc.

Transport Layer Security (TLS)

- TLS ensures **secure communication** between client-server applications over the internet
- It **prevents** the network communication from being eavesdropped or tampered

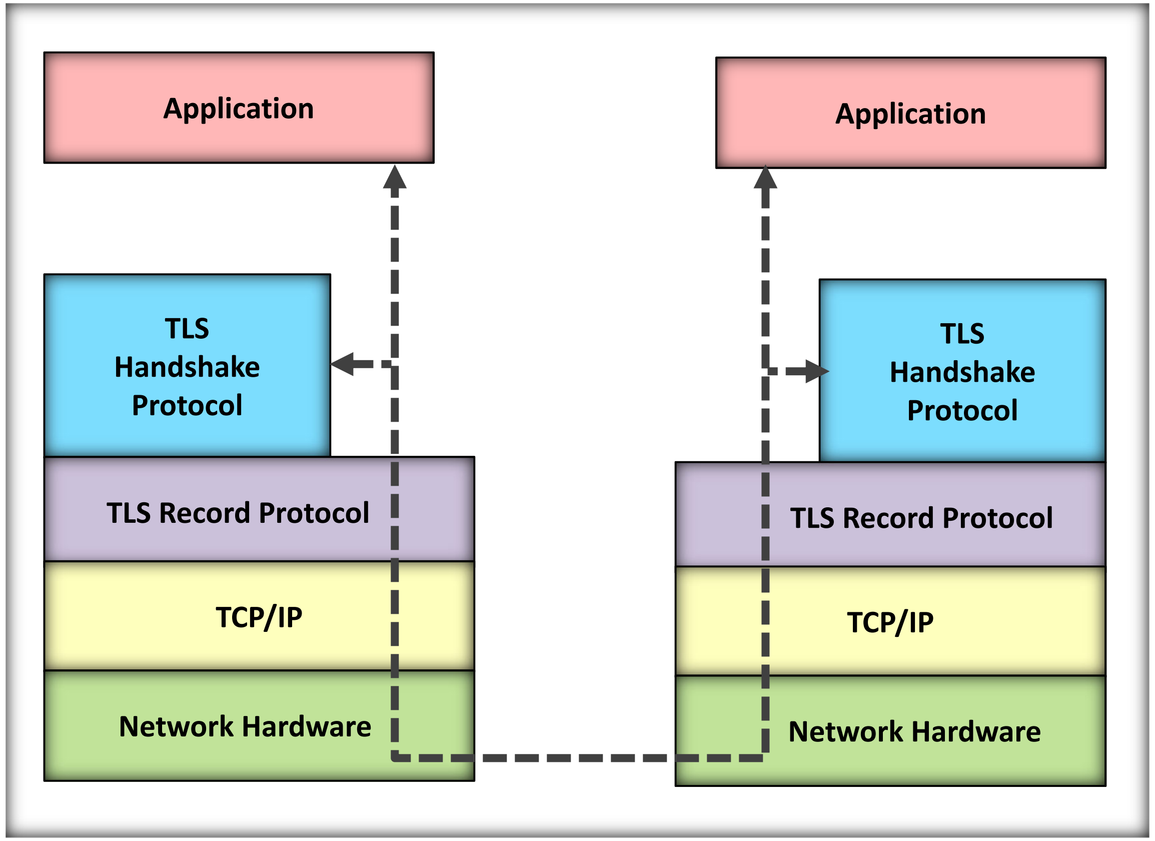
Layers of TLS Protocol

TLS Record Protocol

- It ensures **connection security** with encryption

TLS Handshake Protocol

- It ensures server and client **authentication**



Transport Layer Security (TLS) (Cont'd)

- TLS is the successor of SSL. TLS 1.0 is an upgraded version of SSL 3.0. However, the updates in TLS 1.0 are minor compared to SSL 3.0 like different key derivation functions, MACs are different, etc.

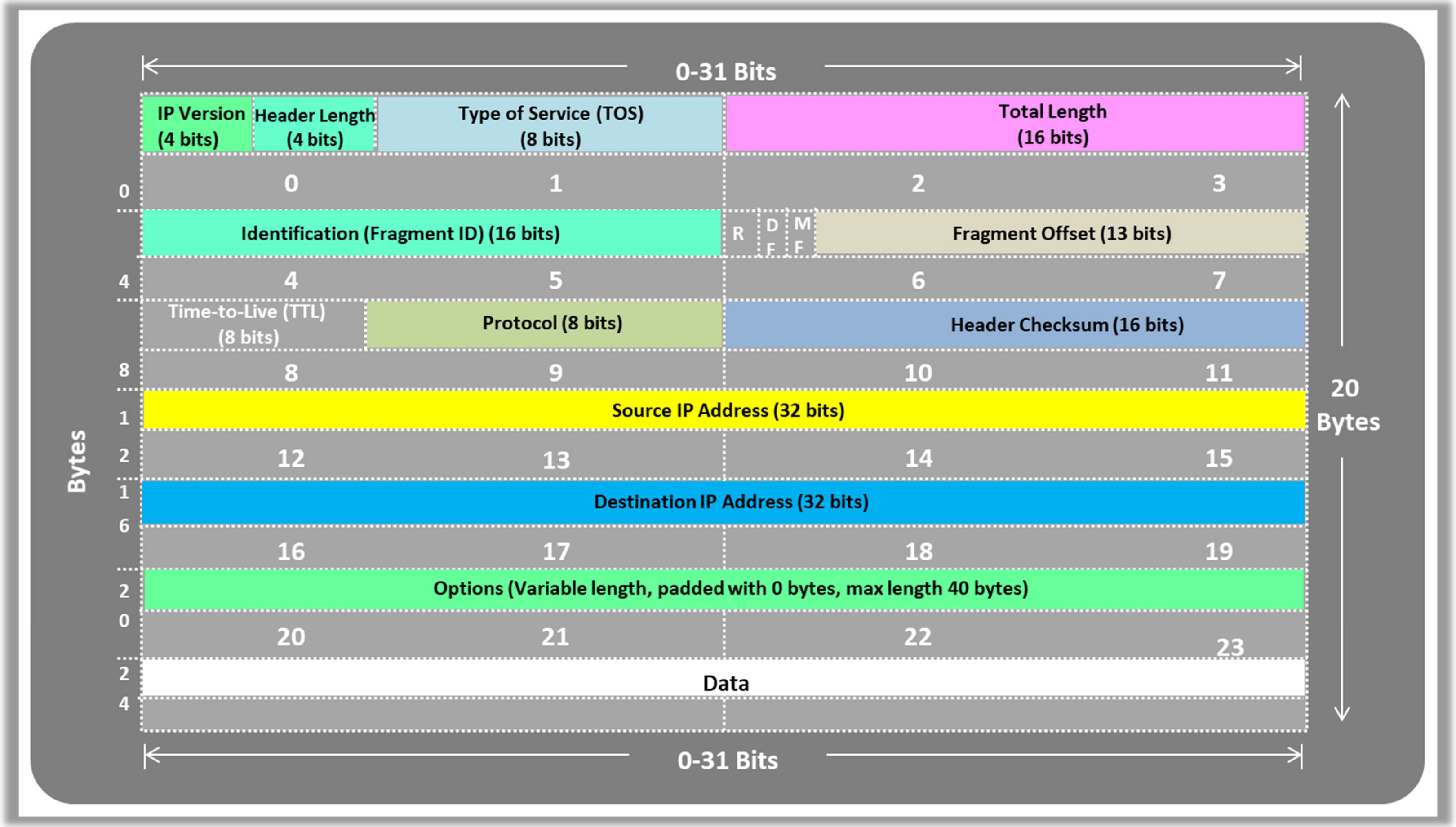
- TLS 1.1 was released to cover the gaps of TLS 1.0 like providing advanced protection against Cipher Block Chaining (CBC) attacks, defined IANA registers for protocols, etc.

- TLS 1.2 is the most advanced protocol and is considered to be more flexible compared to all the other protocols. In this version,
  - MD5/SHA-1 combination in the pseudorandom function (PRF) was replaced with cipher-suite-specified PRFs
  - MD5/SHA-1 combination in the digitally-signed element was replaced with a single hash
  - Flexibility provided for client's and server's ability to specify which hash and signature algorithms they will accept
  - TLS Extensions definition and AES Cipher Suites were merged
  - Enabled tighter checking of EncryptedPreMasterSecret version numbers

Internet Layer Protocols

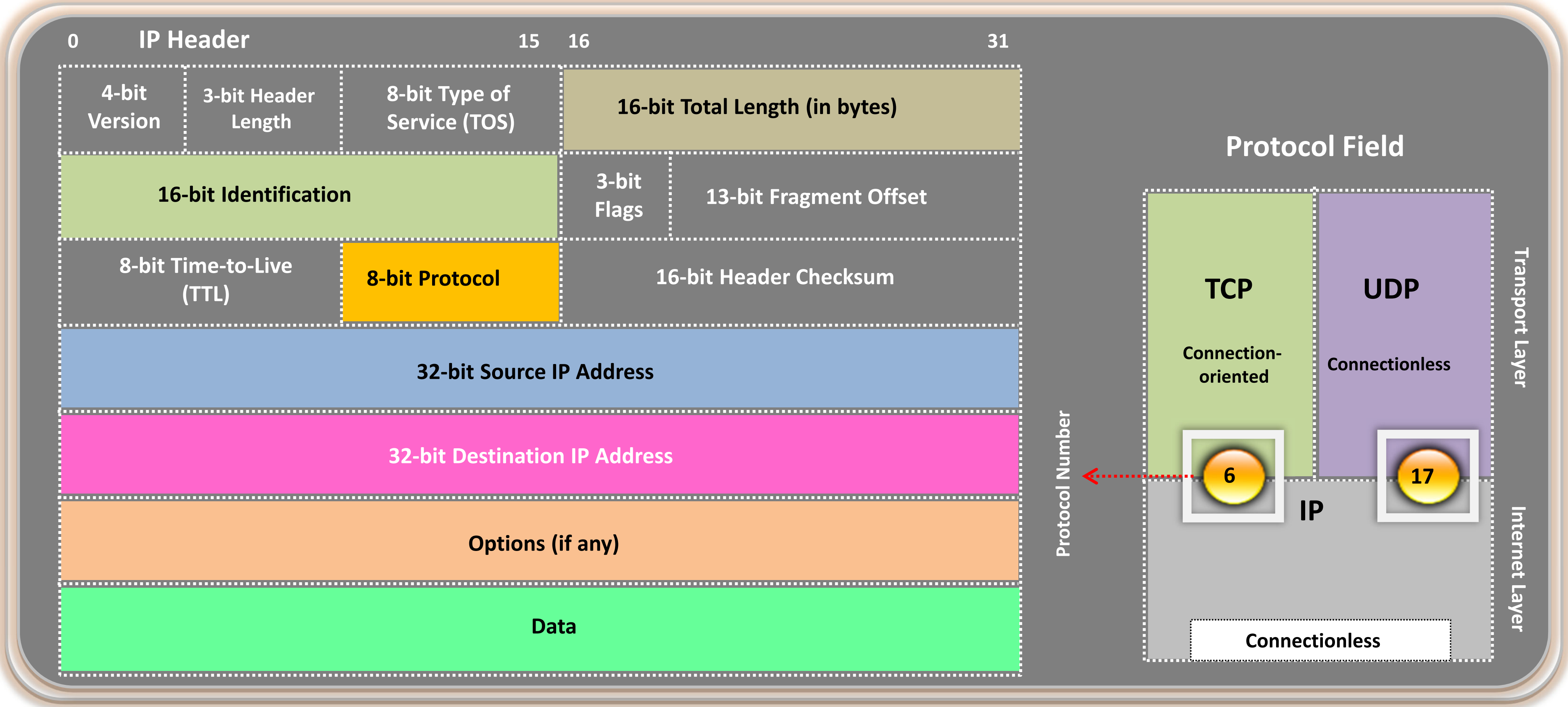
Internet Protocol (IP)

- Internet Protocol (IP) is a fundamental network layer protocol in the TCP/IP protocol suite as it is primarily responsible for sending datagrams across network boundaries


0-31 Bits
IP Version (4 bits)
Header Length (4 bits)
Type of Service (TOS) (8 bits)
Total Length (16 bits)
0
1
2
3
Identification (Fragment ID) (16 bits)
R
D F
M F
Fragment Offset (13 bits)
4
5
6
7
Time-to-Live (TTL) (8 bits)
Protocol (8 bits)
Header Checksum (16 bits)
8
9
10
11
Source IP Address (32 bits)
12
13
14
15
Destination IP Address (32 bits)
16
17
18
19
Options (Variable length, padded with 0 bytes, max length 40 bytes)
20
21
22
23
Data
0-31 Bits
Bytes
0
4
8
12
16
20
24
20 Bytes

IP Header: Protocol Field

- The IP packet has a protocol field that specifies whether the **segment** is **TCP** or **UDP**



IP Header

0 15 16 31

4-bit Version | 3-bit Header Length | 8-bit Type of Service (TOS) | 16-bit Total Length (in bytes)

16-bit Identification | 3-bit Flags | 13-bit Fragment Offset

8-bit Time-to-Live (TTL) | 8-bit Protocol | 16-bit Header Checksum

32-bit Source IP Address

32-bit Destination IP Address

Options (if any)

Data

Protocol Number

Protocol Field

TCP

Connection-oriented

6

UDP

Connectionless

17

IP

Connectionless

Transport Layer

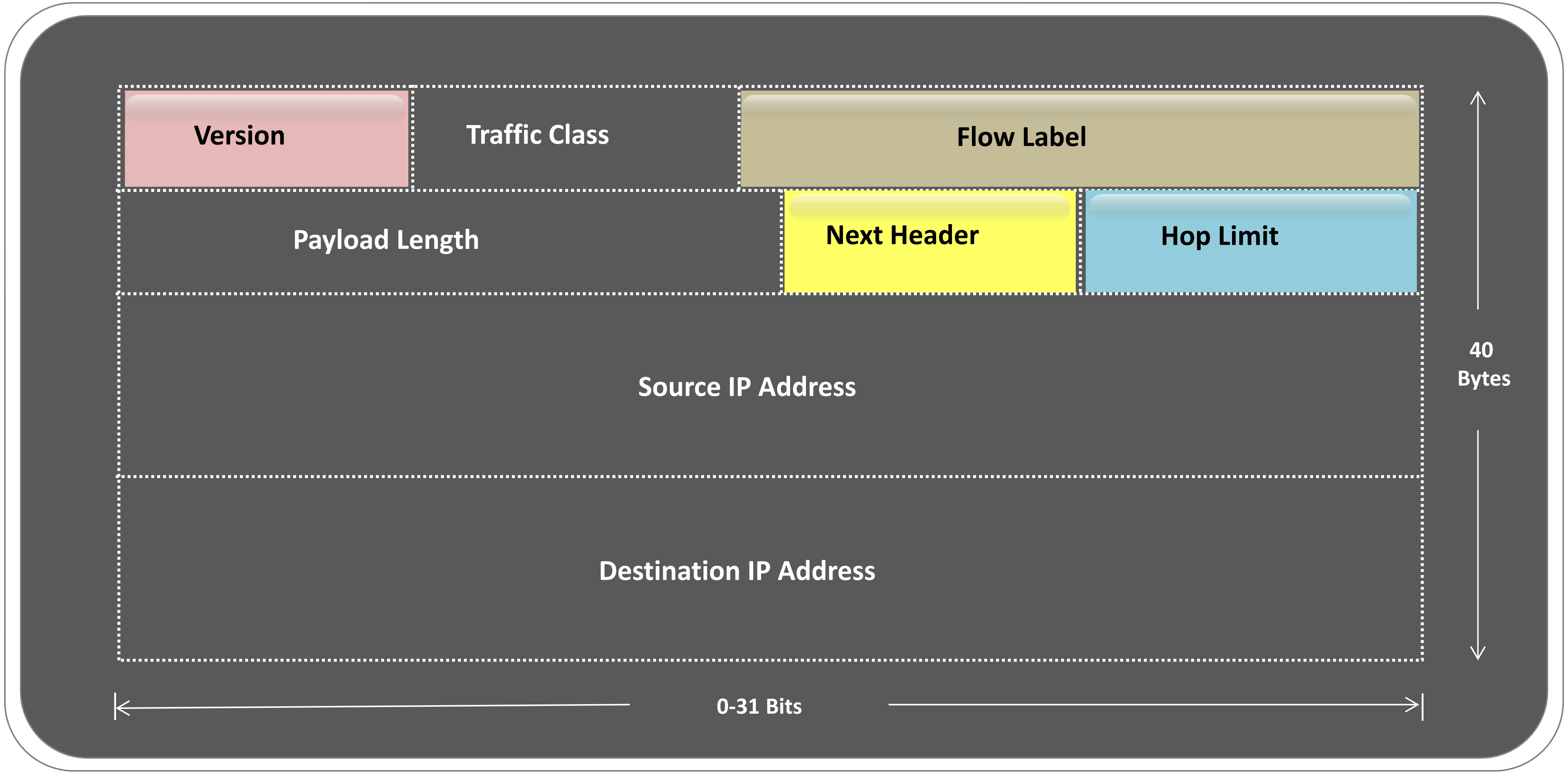
Internet Layer

What is Internet Protocol v6 (IPv6)?

- IPv6, also called IPng or next generation protocol, provides a base for enhanced Internet functionalities
- The most important feature of IPv6 is that it can store larger address space in comparison to IPv4
- IPv6 contains both addressing and controlling data or information to route packets for next-generation Internet
- IPv6 has security features built into its foundation than IPv4

- IPv6 features that provide a platform for growth of IT development:
  - Expandable **address space** (large and diverse) and routing capabilities
  - Scalable to new **users** and **services**
  - Auto **configuration** ability (plug-n-play)
  - Mobility (**improves** mobility model)
  - End-to-end security (high **comfort factor**)
  - Extension **headers** (offer enormous potential)
  - **Authentication** and **privacy**
  - Support for **source** demand **routing** protocol
  - **Quality** of **Service** (QoS)

IPv6 Header



Version

Traffic Class

Flow Label

Payload Length

Next Header

Hop Limit

Source IP Address

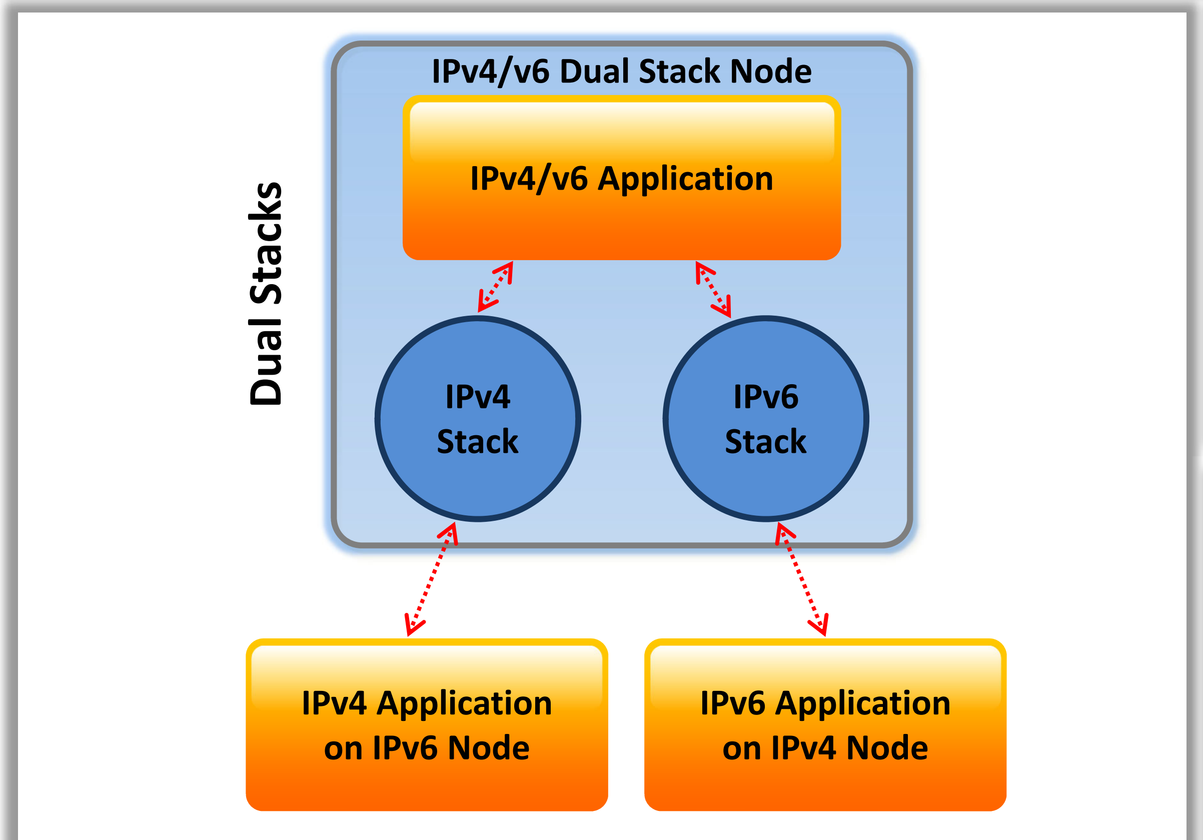
Destination IP Address

40 Bytes

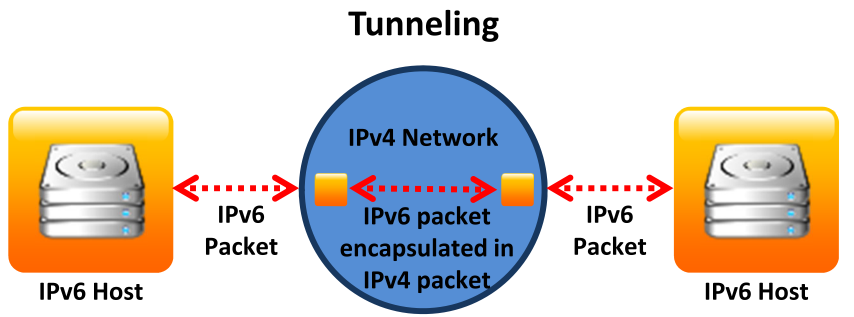
0-31 Bits

IPv4/IPv6 Transition Mechanisms

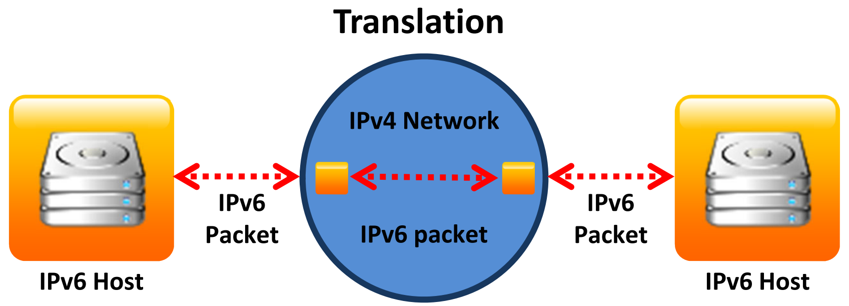
- There are three transition mechanisms available to deploy **IPv6** on the **IPv4** networks



Dual stacks: Based on the DNS value, node uses IPv4 or IPv6



Tunneling: It encapsulates IPv6 packets in IPv4 packets



Translation: NAT-PT and SIIT are used to enable the IPv6 host to communicate with an IPv4 host

Note: The transitions can be used in any combination

IPv6 Security Issues

- Dual-stack related issues: IPv6-IPv4 dual stacks increase the potential for security vulnerabilities
- Header manipulation issues: Using extension headers and IPsec can deter some header-manipulation-based attacks
- Flooding issues: Scanning in IPv6 networks for valid host addresses is difficult
- Trespassing: With the advanced network discovery of IPv6, it becomes easy for an attacker to get information from any remote networks
- Bypassing filtering devices: There are chances of attackers hiding traffic due to the variation in DMZ protection for IPv6 traffic
- Denial-of-Service (DoS): There are possibilities of DoS attacks while using the same links for sending and receiving IPv6 packets
- Anycast (no longer safe): The routing header 0 (zero) feature of IPv6 can single out all instances of anycast services that work with the same IP on the Internet

IPv6 Infrastructure Security Issues

DNS Issues

- Performance may be affected due to the IPv6's improper configuration and use
- IPv6 has less impact on DNS Security

Mobile IP

- Need for authenticated, dynamic registration
- Firewalls need to control the use of routing and home address headers

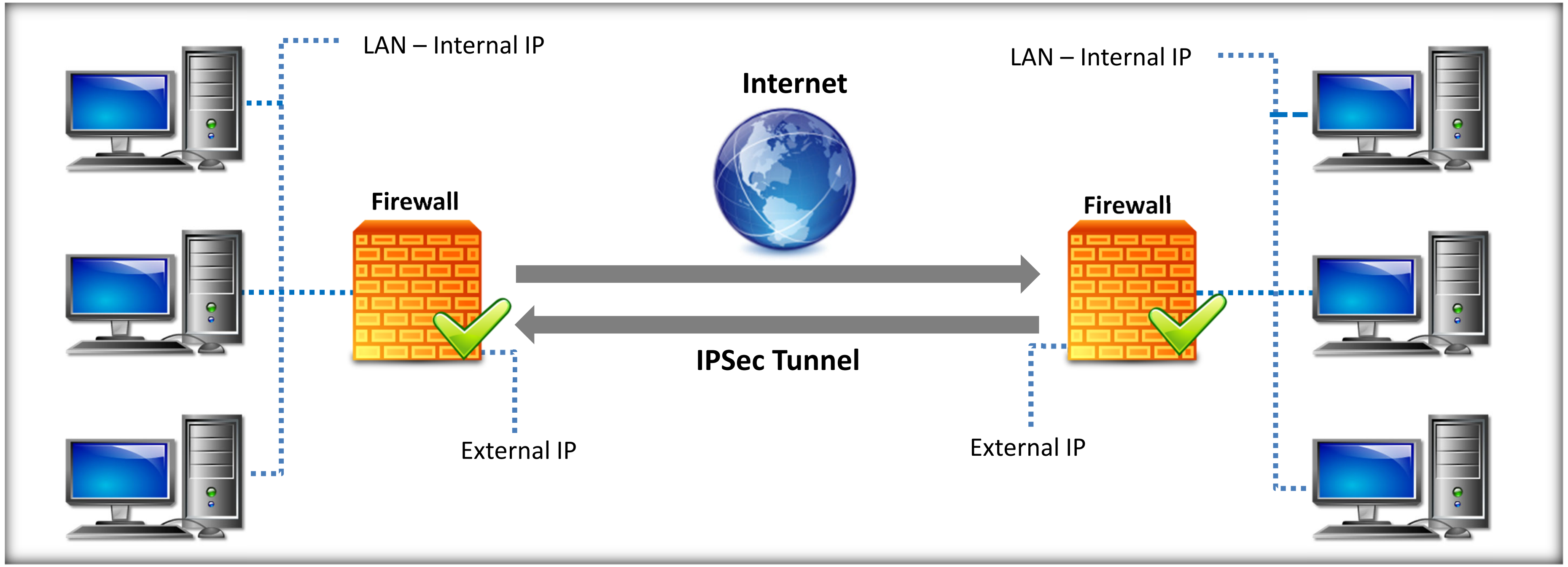
IPv4 vs. IPv6

IPv4	IPv6
Length of addresses is 32 bits (4 bytes)	Length of addresses is 128 bits (16 bytes)
Header consists of a checksum	Header does not consist of a checksum
Header consists of options	Extension headers support optional data
IPsec header support is optional	IPsec header support is required
Address can be organized physically or through DHCP	Stateless auto-organized link-local address will be obtained
ARP uses broadcast ARP request to solve IP to MAC/Hardware address	Multicast neighbor solicitation communication solves IP addresses to MAC addresses
Broadcast addresses are used to send traffic to all nodes on a subnet	IPv6 uses a link-local scope all-nodes multicast address

Internet Protocol Security (IPsec)

- IPsec is a network layer protocol that ensures **secure Internet Protocol** (IP) level communication
- It provides **end-to-end security** at the Internet Layer of the Internet Protocol Suite

- It **encrypts** and **authenticates** each IP packet in the communication
- It **supports** network-level peer authentication, data origin authentication, data integrity, data confidentiality (encryption), and replay protection



Internet Protocol Security (IPsec) (Cont’d)

Components of IPsec

- IPsec Driver
- Internet Key Exchange (IKE)
- Internet Security Association Key Management Protocol
- Oakley
- IPsec Policy Agent

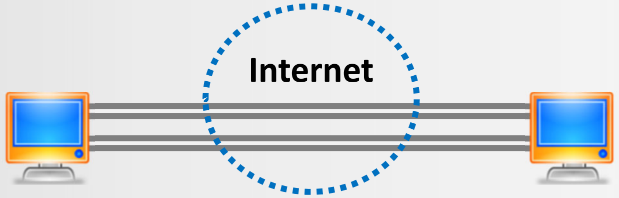
Benefits of IPSec

- Network-level peer authentication
- Data origin authentication
- Data integrity
- Data confidentiality (encryption)
- Replay protection

Internet Protocol Security (IPsec) (Cont'd)

Modes of IPsec

Transport Mode



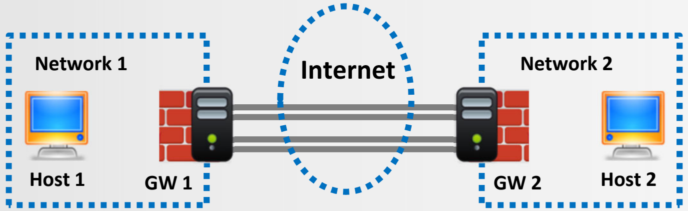
Transport – mode encapsulation

IP header	IPsec header	Transport data (TCP, UDP, etc.)	IPsec trailer (ESP only)

← encrypted →

← encrypted →

Tunnel Mode



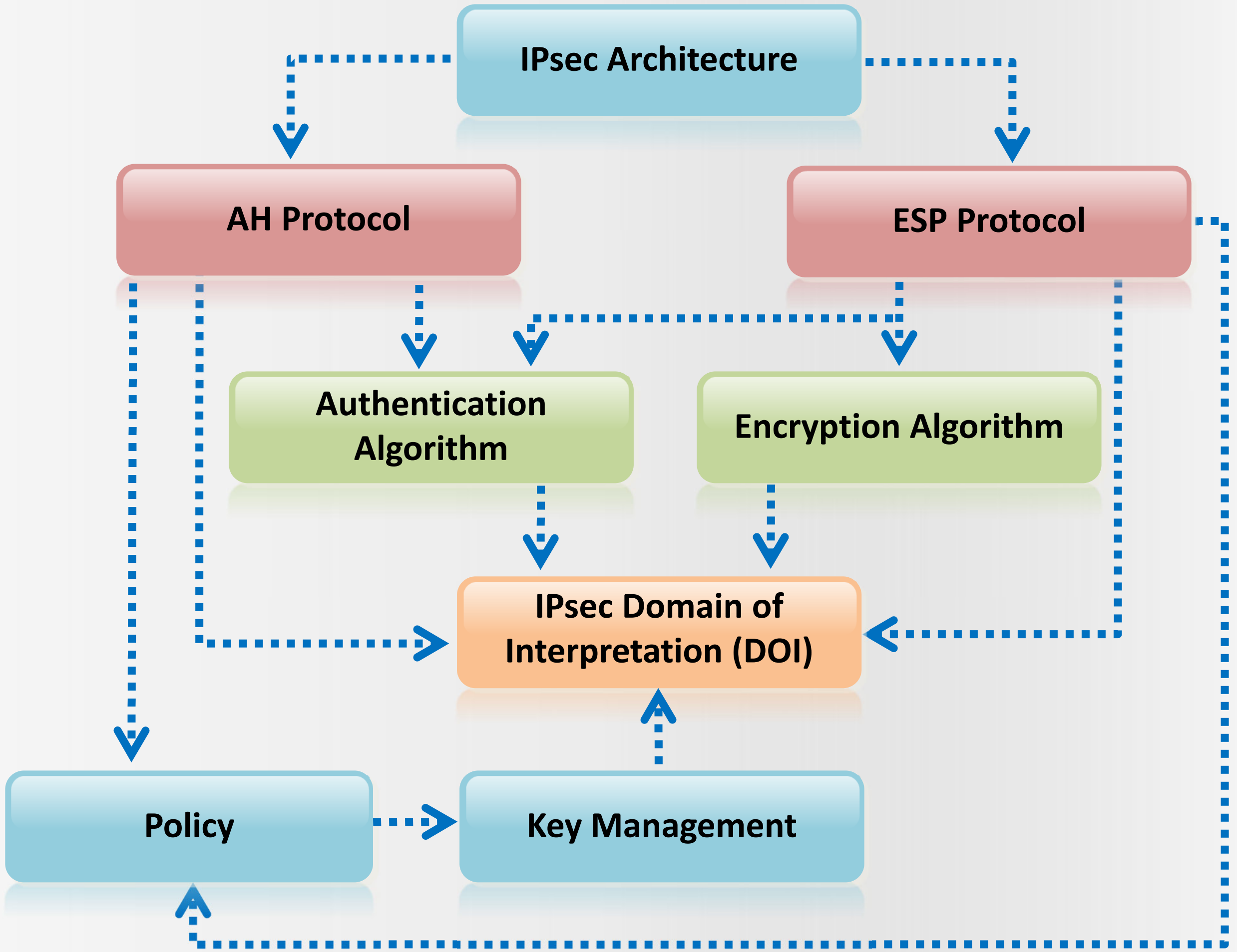
Tunnel – mode encapsulation

Outer IP header	IPsec header	Inner IP header	IP payload	IPsec trailer (ESP only)

← encrypted →

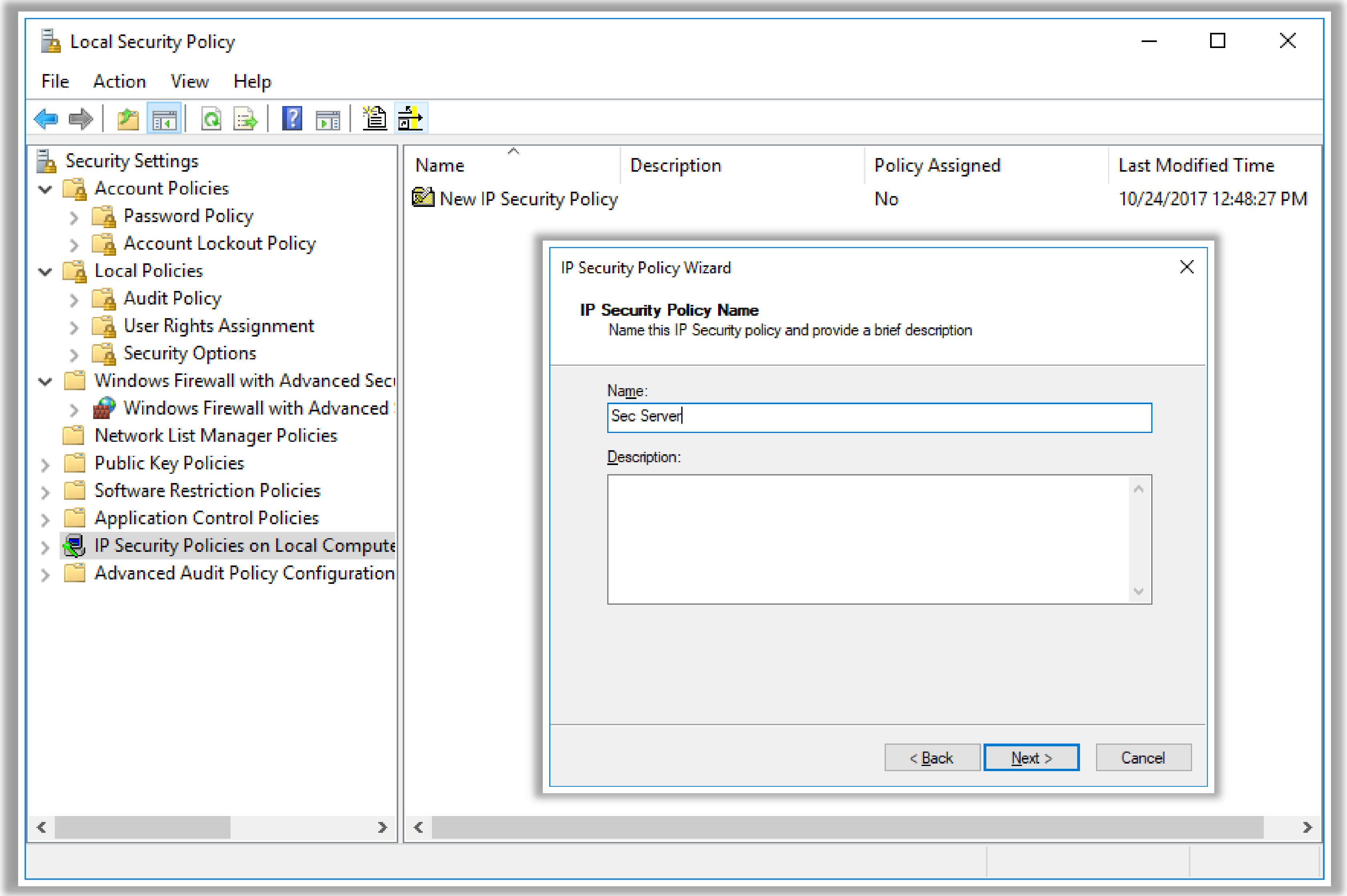
← encrypted →

IPsec Architecture



IPsec Authentication and Confidentiality

- IPsec uses two different security services for authentication and confidentiality
  - **Authentication Header (AH)**: Provides data authentication of the sender
  - **Encapsulation Security Payload (ESP)**: Provides both data authentication and encryption (confidentiality) of the sender


Local Security Policy
File
Action
View
Help
Security Settings
Account Policies
Password Policy
Account Lockout Policy
Local Policies
Audit Policy
User Rights Assignment
Security Options
Windows Firewall with Advanced Secu
Windows Firewall with Advanced
Network List Manager Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Local Compute
Advanced Audit Policy Configuration
IP Security Policy Wizard
< Back
Next >
Cancel

Name	Description	Policy Assigned	Last Modified Time
New IP Security Policy		No	10/24/2017 12:48:27 PM

IP Security Policy Name

Name this IP Security policy and provide a brief description

Name: Sec Server

Description:

Internet Control Message Protocol (ICMP)

IP is an unreliable method for the delivery of network data

It does not notify the sender of failed data transmission

Internet Control Message Protocol (ICMP) is the component of the TCP/IP protocol stack that addresses this basic limitation of IP

ICMP does not overcome the unreliability issues in IP

Reliability must be provided by upper-layer protocols (TCP or the application), if it is required

Error Reporting and Correction

When datagram delivery errors occur, ICMP reports the following errors back to the source of the datagram:

Workstation 1 sends a datagram to Workstation 6

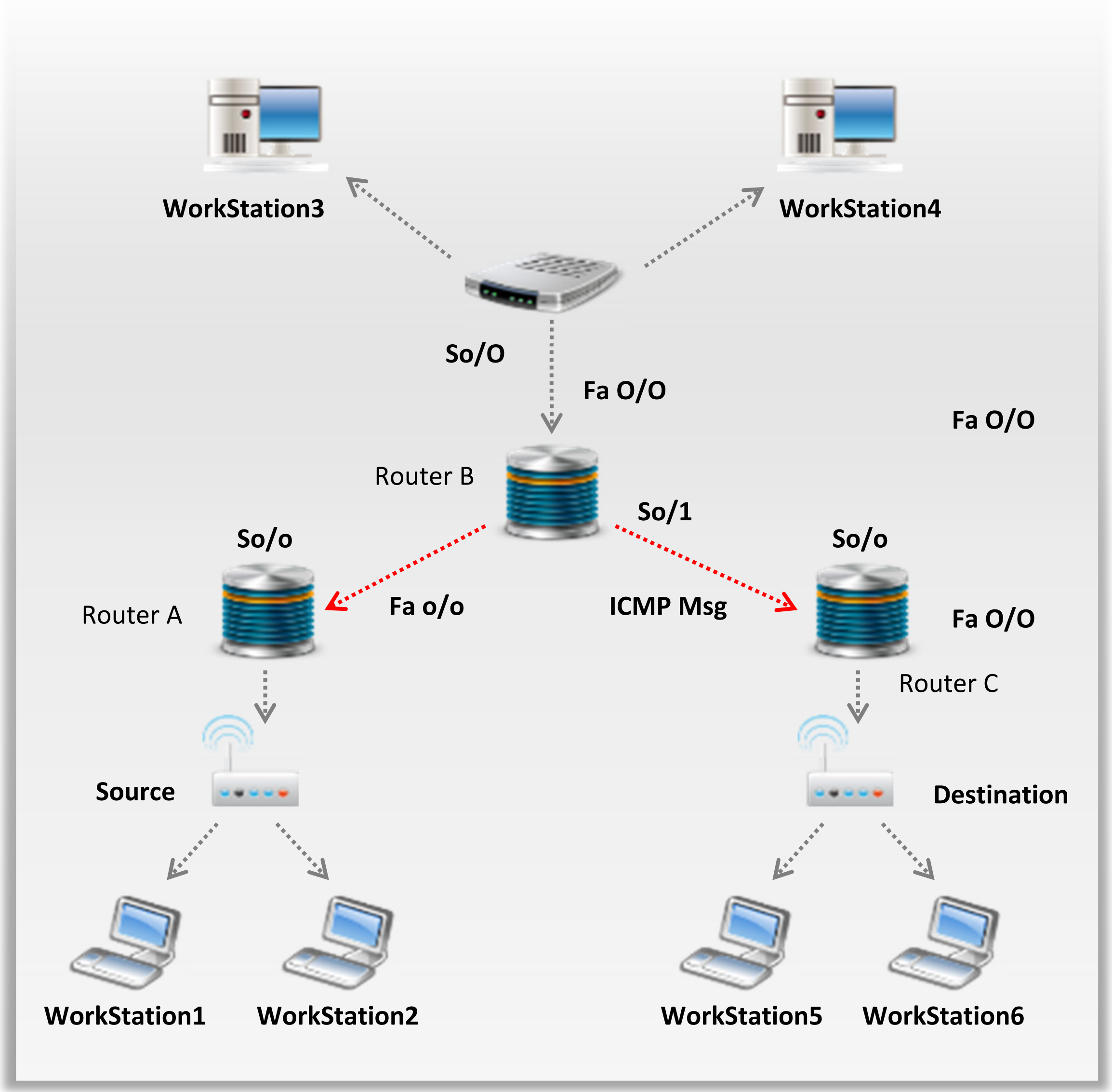
Fa0/0 on Router C goes down

Router C then utilizes ICMP to send a message back to Workstation 1 indicating that the datagram could not be delivered

ICMP does not correct the encountered network problem

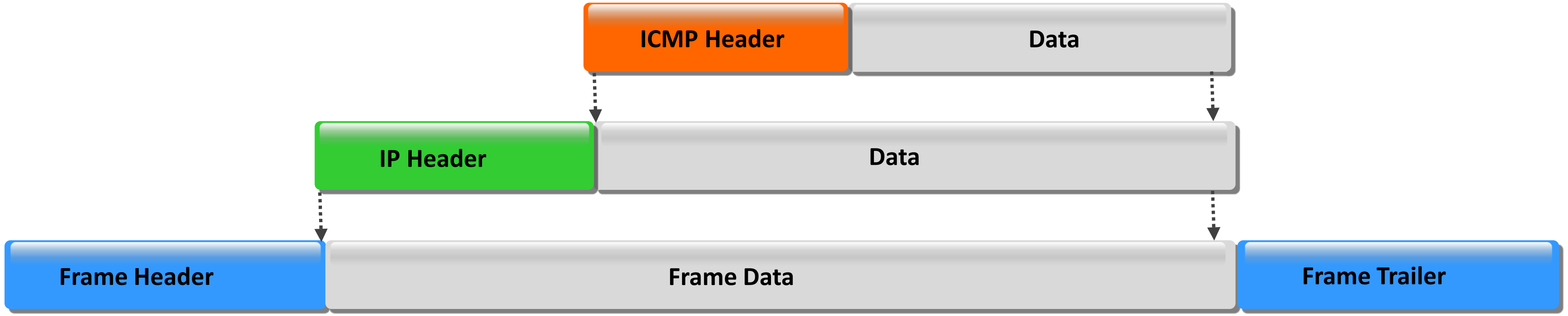
Router C knows only the source and destination IP addresses of the datagram

ICMP reports on the status of the delivered packet only to the source device



ICMP Message Delivery

- ICMP messages are encapsulated into the datagram
- Encapsulation follows the same technique used by IP to deliver data, subject to the same delivery failures as any IP packet
- This creates a scenario where error reports could generate more error reports
- This causes increased congestion on an already ailing network
- Errors created by ICMP messages do not generate their own ICMP messages
- Thus, it is possible to have a datagram delivery error that is never reported back to the sender of the data



Format of an ICMP Message

Type	Name
0	Echo Reply
1	Unassigned
2	Unassigned
3	Destination Unreachable
4	Source Quench
5	Redirect
6	Alternate Host Address
7	Unassigned
8	Echo
9	Router Advertisement
10	Router Solicitation
11	Time Exceeded
12	Parameter Problem
13	Timestamp
14	Timestamp Reply
15	Information Request
16	Information Reply
17	Address Mask Request
18	Address Mask Reply
19	Reserved (for Security)
20-29	Reserved (for Robustness Experiment)
30	Traceroute
31	Datagram Conversion Error
32	Mobile Host Redirect
33	IPv6 Where-Are-You
34	IPv6 I-Am-Here
35	Mobile Registration Request
36	Mobile Registration Reply
37	Domain Name Request
38	Domain Name Reply
39	SKIP
40	Photuris
41-255	Reserved

Code Field

Type 3: Destination Unreachable

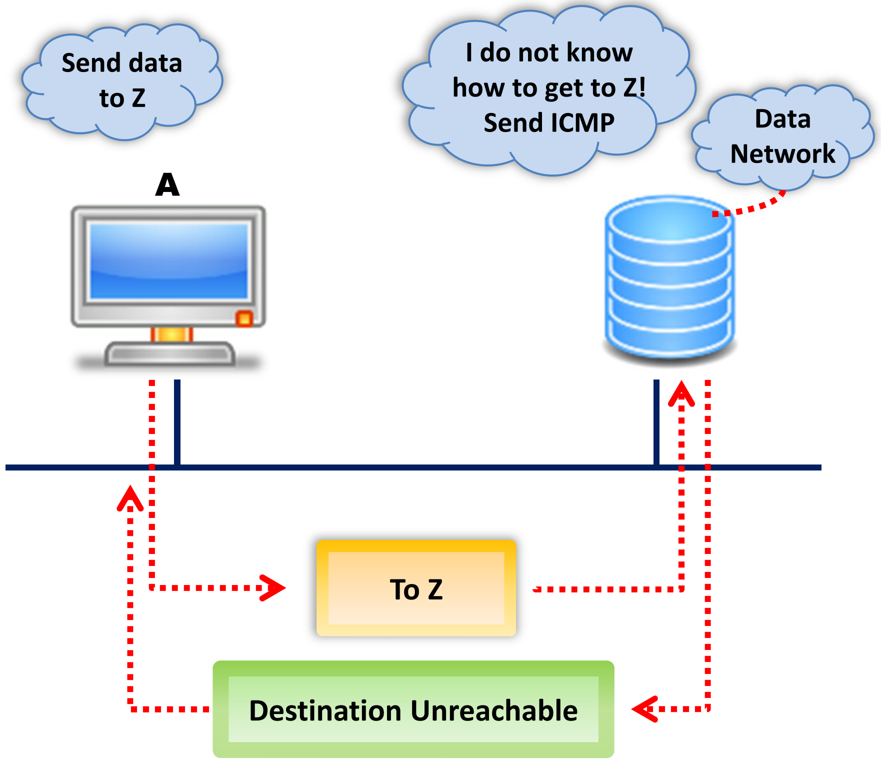
Codes

0	Net Unreachable
1	Host Unreachable
2	Protocol Unreachable
3	Port Unreachable
4	Fragmentation Needed and Don't Fragment was Set
5	Source Route Failed
6	Destination Network Unknown
7	Destination Host Unknown
8	Source Host Isolated
9	Communication with Destination Network is Administratively Prohibited
10	Communication with Destination Host is Administratively Prohibited
11	Destination Network Unreachable for Type of Service
12	Destination Host Unreachable for Type of Service
13	Communication Administratively Prohibited
14	Host Precedence Violation
15	Precedence cutoff in effect

Type (8 bits)	Code (8 bits)	Checksum (16 bits)
Parameters		
Data.....		

Unreachable Networks

- Network communication depends ~~up~~on certain basic conditions being met:
  - Sending and receiving devices must have the TCP/IP protocol stack properly configured:
    - Proper configuration of the IP address and subnet mask
    - A default gateway must also be configured, if datagrams are to travel outside of the local network
  - A router also must have the TCP/IP protocol properly configured on its interfaces, and it must use an appropriate routing protocol
  - If these conditions are not met, then network communication cannot take place
  - **Examples of problems:**
    - Sending device may address the datagram to a non-existent IP address
    - Destination device is not connected to its network
    - Router's connecting interface is down
    - Router does not have the information necessary to find the destination network



- An ICMP destination **unreachable message** is sent if:
  - Host or port is unreachable
  - Network is unreachable

Destination Unreachable Message

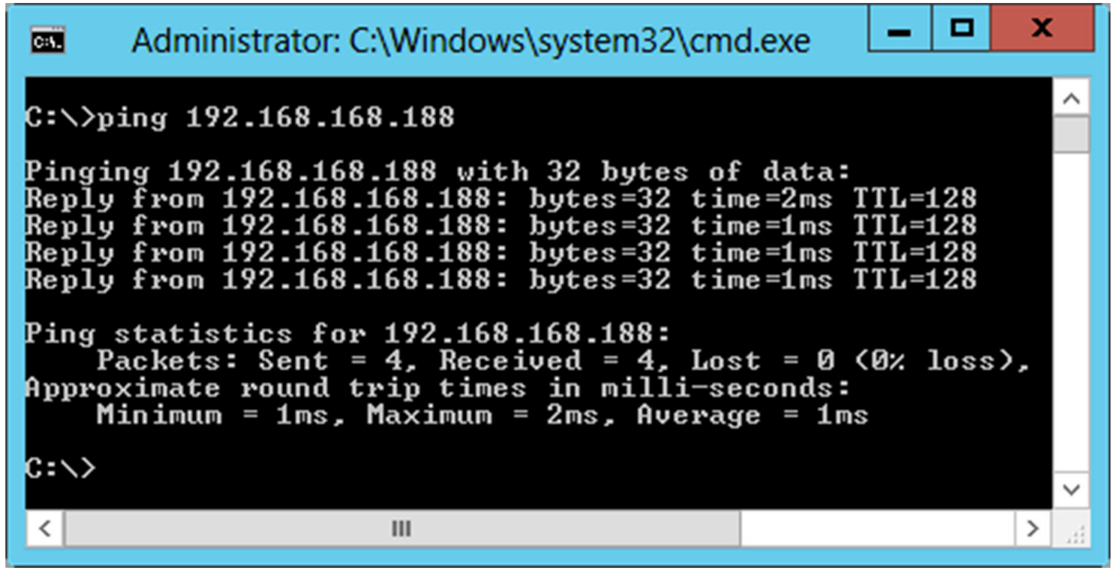
If datagrams cannot always be forwarded to their destinations, ICMP delivers back a destination unreachable message, indicating to the sender that the datagram could not be properly forwarded

A destination unreachable message may also be sent when packet fragmentation is required in order to forward a packet:

- Fragmentation is usually necessary when a datagram is forwarded from a token-ring network to an Ethernet network
- If the datagram does not allow fragmentation, the packet cannot be forwarded, so a destination unreachable message will be sent

Destination unreachable messages may also be generated if the IP-related services such as FTP or web services are unavailable

ICMP Echo (Request) and Echo Reply



```
C:\>ping 192.168.168.188

Pinging 192.168.168.188 with 32 bytes of data:
Reply from 192.168.168.188: bytes=32 time=2ms TTL=128
Reply from 192.168.168.188: bytes=32 time=1ms TTL=128
Reply from 192.168.168.188: bytes=32 time=1ms TTL=128
Reply from 192.168.168.188: bytes=32 time=1ms TTL=128

Ping statistics for 192.168.168.188:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 2ms, Average = 1ms

C:\>
```

Type (8 bits)	Code (8 bits)	Checksum (16 bits)
Parameters		
Data..........		

Echo = Type 8

Echo Reply = Type 0

Ethernet Header (Layer 2)			IP Header (Layer 3)	ICMP Message (Layer 3)						Ether. Tr.
Ethernet Destination Address (MAC)	Ethernet Source Address (MAC)	Frame Type	Source IP Add. Dest. IP Add. Protocol Field	Type 0 or 8	Code 0	Checksum	ID	Seq. Num.	Data	FCS

IP Protocol Field = 1
The echo request message is typically initiated using the ping command

Time Exceeded Message

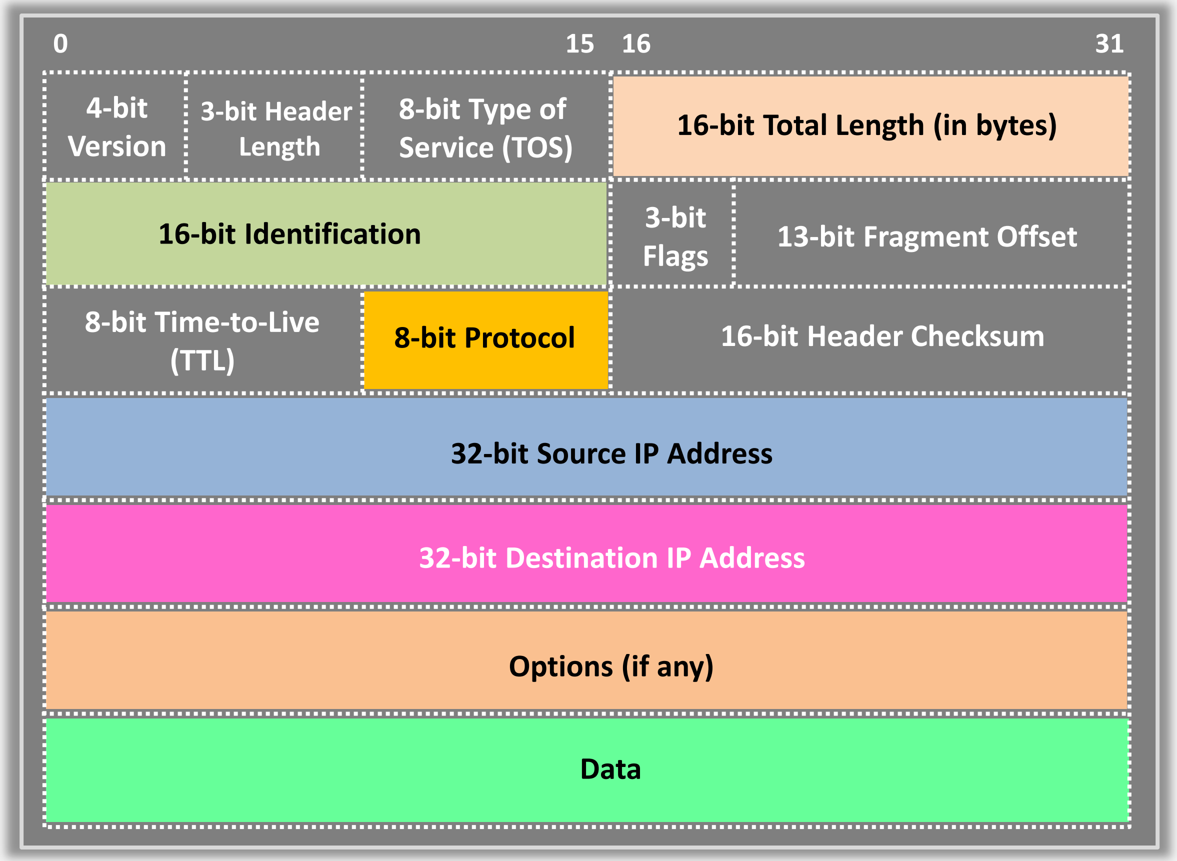
ICMP Time Exceeded

Type = 11

Type (8 bits)	Code (8 bits)	Checksum (16 bits)
Parameters		
Data..........		

- A TTL value is defined in each datagram (IP packet)
- As each router processes the datagram, it decreases the TTL value by one
- When the TTL of the datagram value reaches zero, the packet is discarded
- ICMP uses a time exceeded message to notify the source device that the TTL of the datagram has been exceeded

IP Header



0 15 16 31

4-bit Version | 3-bit Header Length | 8-bit Type of Service (TOS) | 16-bit Total Length (in bytes)

16-bit Identification | 3-bit Flags | 13-bit Fragment Offset

8-bit Time-to-Live (TTL) | 8-bit Protocol | 16-bit Header Checksum

32-bit Source IP Address

32-bit Destination IP Address

Options (if any)

Data

IP Parameter Problem

- Devices that **process** datagrams may not be able to forward a **datagram** due to some type of **error** in the header
- This error does not relate to the state of the destination **host** or network but still prevents the datagram from being **processed** and **delivered**
- An ICMP **type 12 parameter** problem message is sent to the **source** of the **datagram**

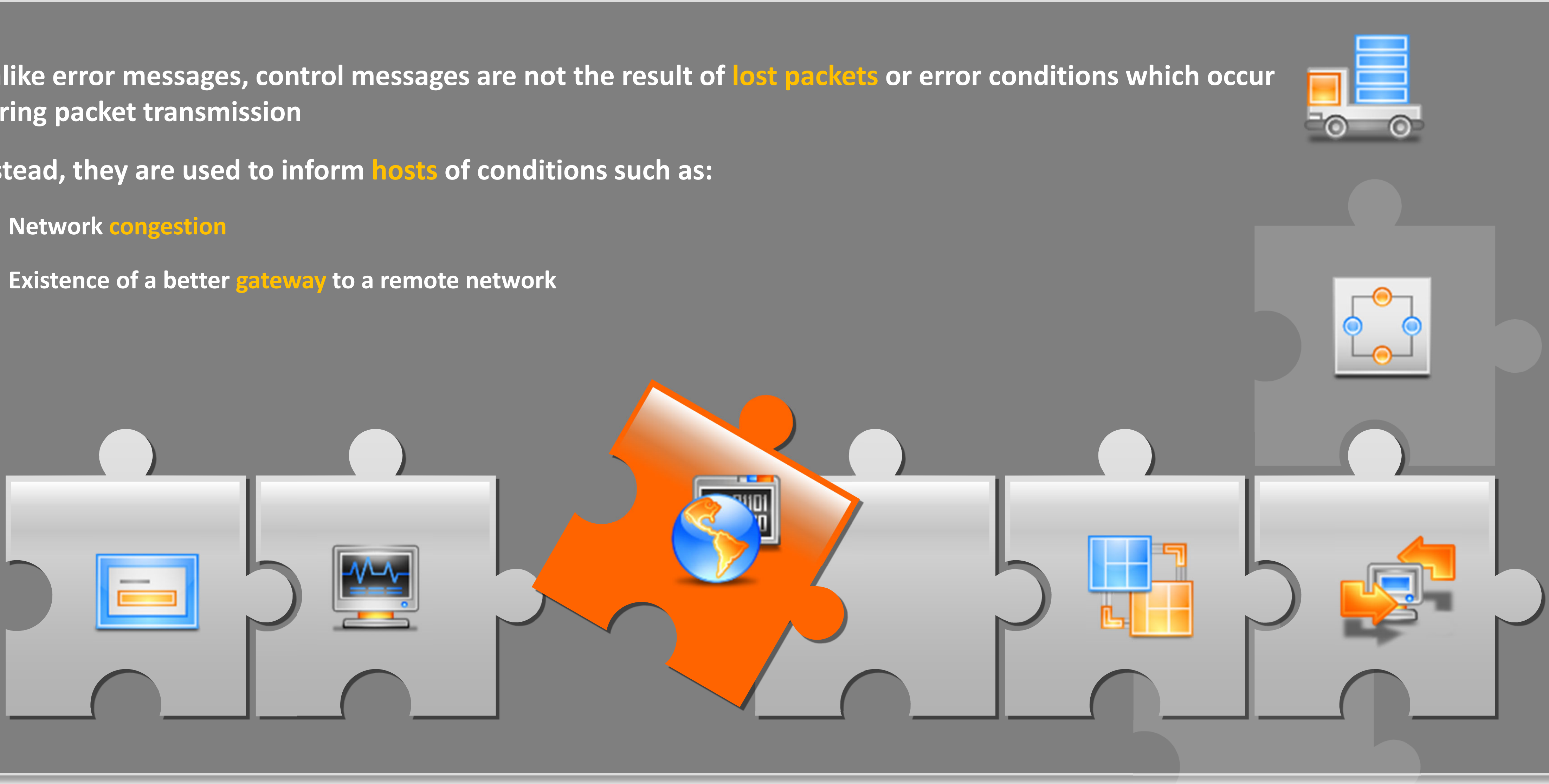
ICMP Parameter Problem

Type = 12

0	8	16	31
Type (3)	Code (0-12)	Checksum	
Unused (must be zero)			
Internet Header + First 64 Bits of Datagram			

ICMP Control Messages

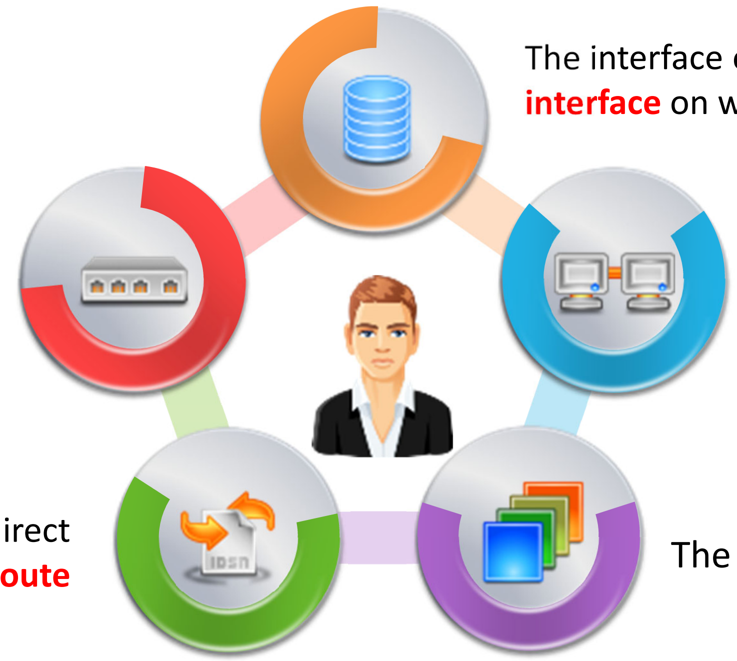
- Unlike error messages, control messages are not the result of lost packets or error conditions which occur during packet transmission
- Instead, they are used to inform hosts of conditions such as:
  - Network congestion
  - Existence of a better gateway to a remote network



ICMP Redirects

- **ICMP Redirects; Type = 5, Code = 0 to 3**
- Default gateway only sends the ICMP **redirect**/**change** request messages, if the following **conditions** are met:

Type (8 bits)	Code (8 bits)	Checksum (16 bits)
Parameters		
Data..........		



The interface on which the **packet** comes into the router is the same **interface** on which the packet gets routed out

The subnet/network of the **source IP address** is the same subnet/network of the next-hop IP address of the routed packet

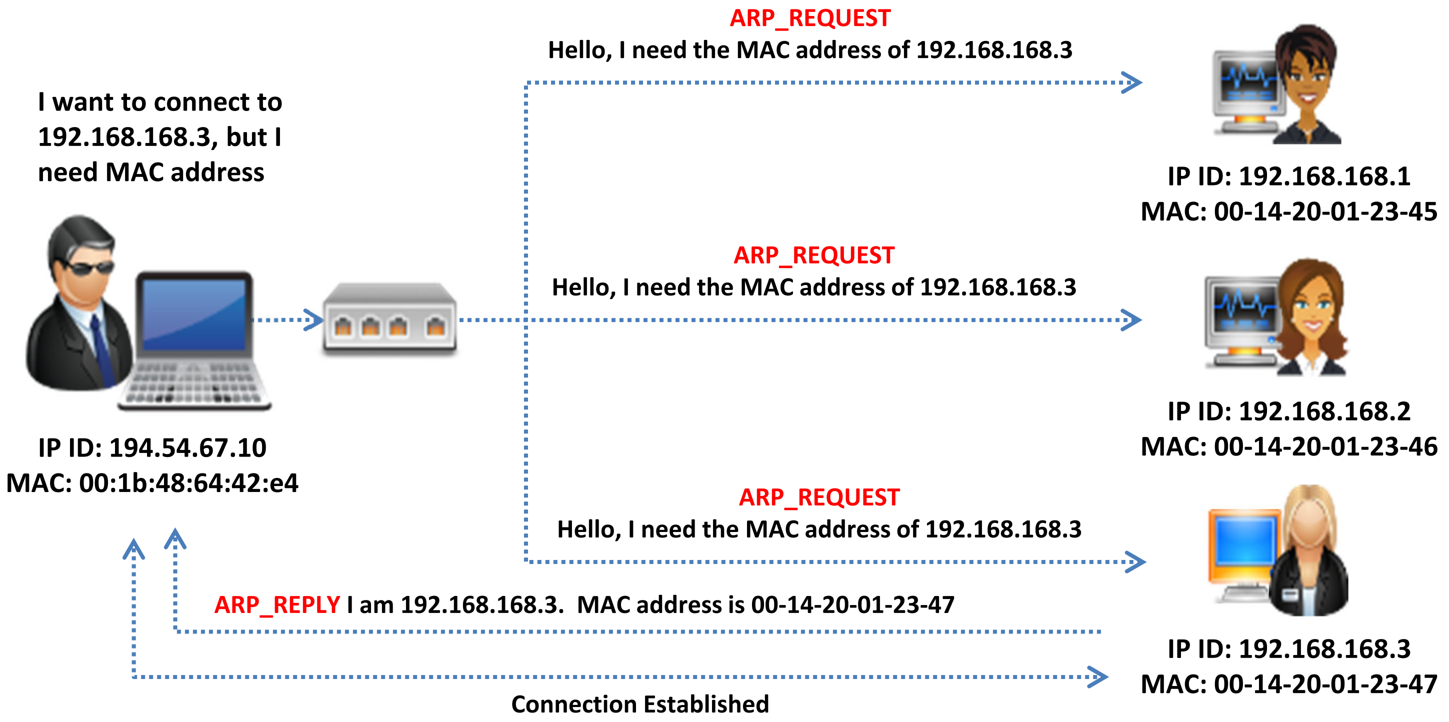
The datagram is not **source-routed**

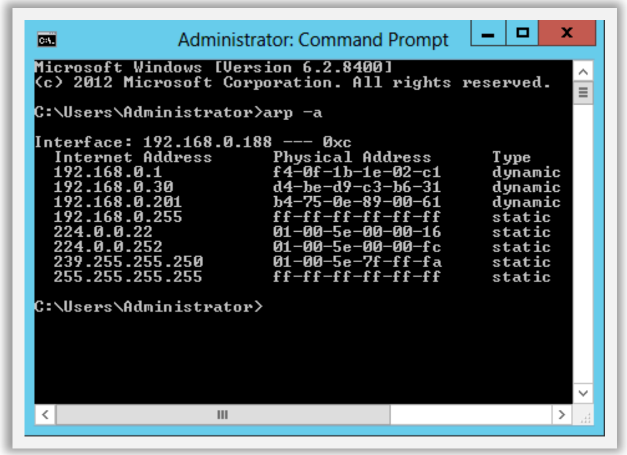
The route for the **redirect** is not another ICMP redirect or a **default route**

The router is **configured** to send redirects

Address Resolution Protocol (ARP)

- ARP is a stateless protocol used for **resolving IP addresses to machine** (MAC) addresses
- ARP request is **broadcast** over the network, whereas the response is a **unicast** message to the requester
- The IP address and MAC pair is stored in the system, switch, and/or router's **ARP cache**, through which the ARP reply passes


I want to connect to 192.168.168.3, but I need MAC address
IP ID: 194.54.67.10
MAC: 00:1b:48:64:42:e4
ARP_REQUEST
Hello, I need the MAC address of 192.168.168.3
IP ID: 192.168.168.1
MAC: 00-14-20-01-23-45
ARP_REQUEST
Hello, I need the MAC address of 192.168.168.3
IP ID: 192.168.168.2
MAC: 00-14-20-01-23-46
ARP_REQUEST
Hello, I need the MAC address of 192.168.168.3
IP ID: 192.168.168.3
MAC: 00-14-20-01-23-47
ARP_REPLY I am 192.168.168.3. MAC address is 00-14-20-01-23-47
Connection Established



```
Microsoft Windows [Version 6.2.8400]
(c) 2012 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>arp -a

Interface: 192.168.0.188 --- 0xc
  Internet Address      Physical Address      Type
  192.168.0.1           f4-0f-1b-1e-02-c1     dynamic
  192.168.0.30          d4-be-d9-c3-b6-31     dynamic
  192.168.0.201         b4-75-0e-89-00-61     dynamic
  192.168.0.255         ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static

C:\Users\Administrator>
```

ARP Cache Table

ARP Packet Format

Byte 0	Byte 1	Byte 2	Byte 3
Hardware Type		Protocol Type	
Hardware Length	Protocol Length	Operation (1 for Request, 2 for Reply)	
Sender’s Hardware Address (First 4 Bytes of Ethernet Address)			
Sender’s Hardware Address (Last 2 Bytes of Ethernet Address)		Sender’s Protocol Address (First 2 Bytes of IP Address)	
Sender’s Protocol Address (Last 2 Bytes of IP Address)		Target’s Hardware Address (2 Bytes of Ethernet Address, Null in ARP Request)	
Target’s Hardware Address (Last 4 Bytes of Ethernet Address, Null in ARP Request)			
Sender’s Protocol Address (4-byte IP Address)			

Hardware Type:

- 1 = Ethernet
- 2 = Experimental Ethernet
- 3 = Amateur Radio AX.25
- 4 = Proteon ProNET Token Ring
- 5 = Chaos
- 6 = IEEE 802 Networks, etc.

Protocol Type:

- IPv4 = 0x0800
- IPv6 = 0x86DD

Hardware Length:

- 6 for Ethernet

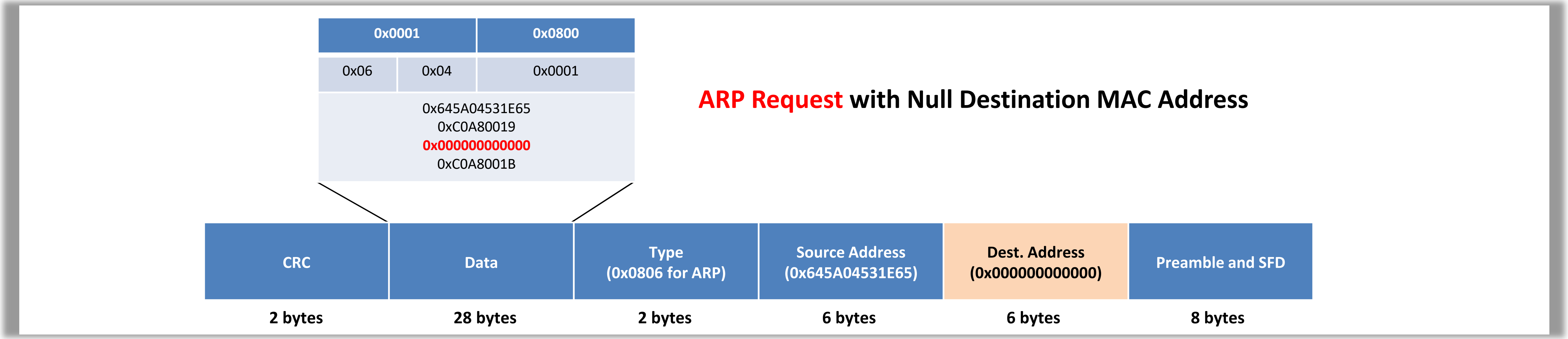
Protocol Length:

- 4 for IPv4

Operation Code:

- 1 For Request
- 2 For Reply

ARP Packet Encapsulation

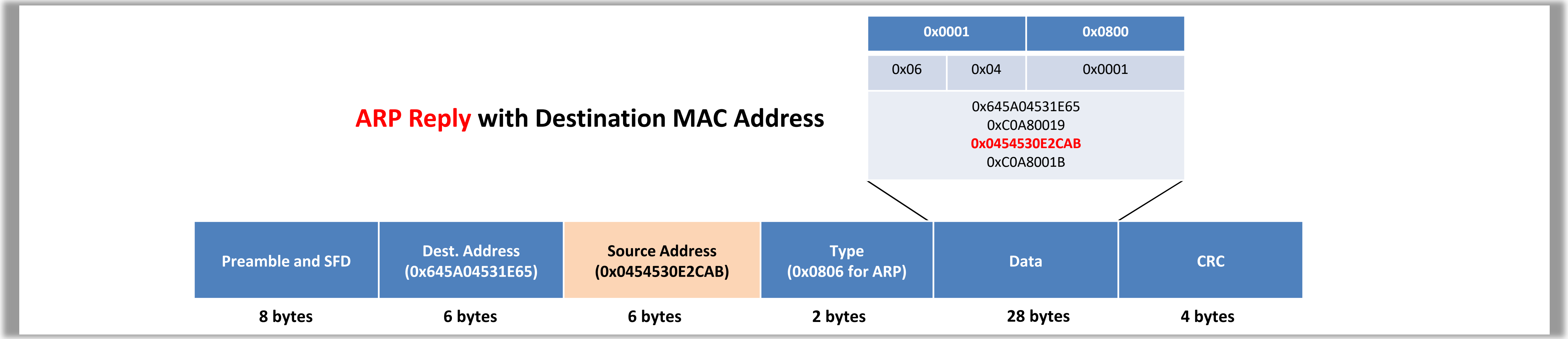


ARP Request with Null Destination MAC Address

0x0001		0x0800
0x06	0x04	0x0001

0x645A04531E65
0xC0A80019
0x000000000000
0xC0A8001B

CRC	Data	Type (0x0806 for ARP)	Source Address (0x645A04531E65)	Dest. Address (0x000000000000)	Preamble and SFD
2 bytes	28 bytes	2 bytes	6 bytes	6 bytes	8 bytes



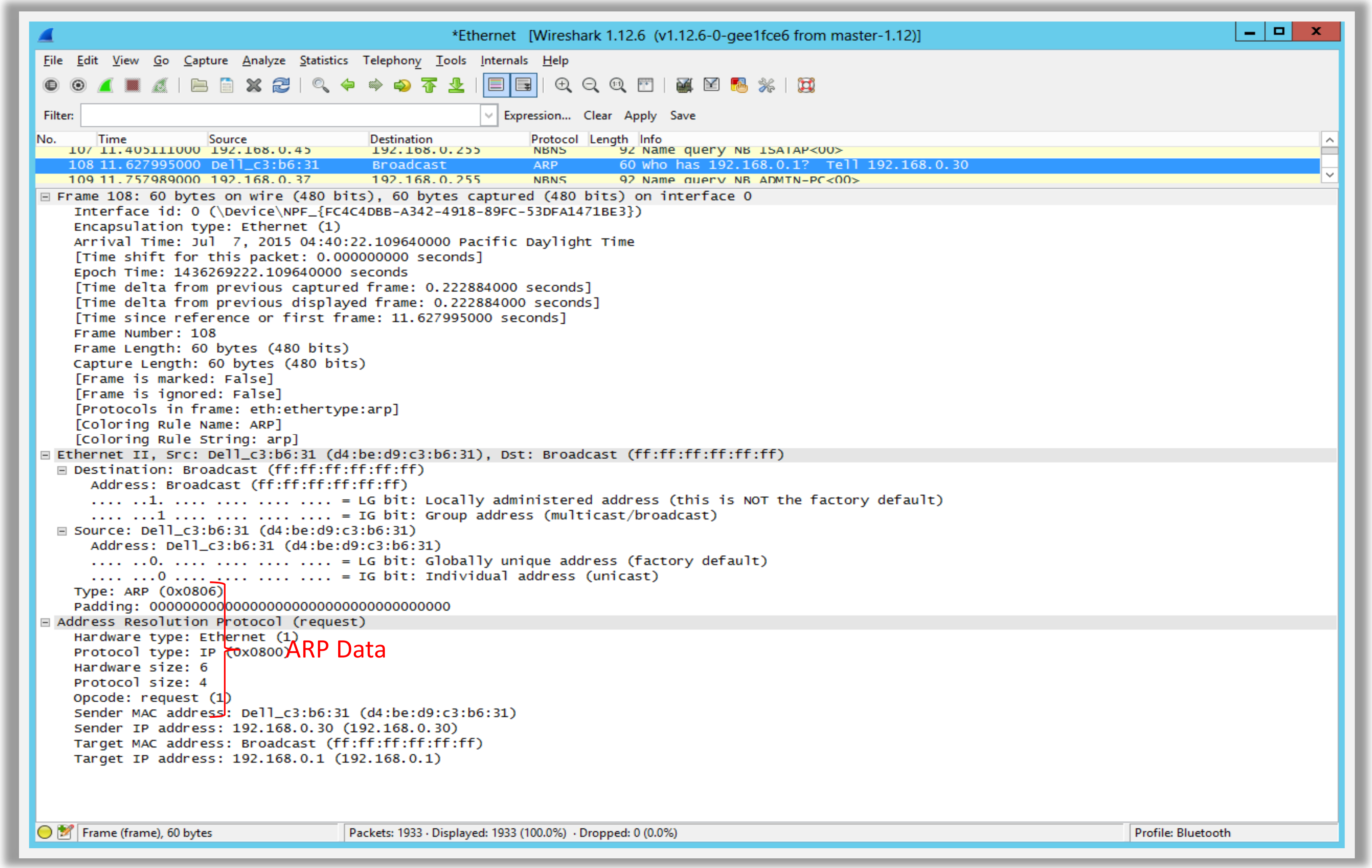
ARP Reply with Destination MAC Address

0x0001		0x0800
0x06	0x04	0x0001

0x645A04531E65
0xC0A80019
0x0454530E2CAB
0xC0A8001B

Preamble and SFD	Dest. Address (0x645A04531E65)	Source Address (0x0454530E2CAB)	Type (0x0806 for ARP)	Data	CRC
8 bytes	6 bytes	6 bytes	2 bytes	28 bytes	4 bytes

ARP Packet Analysis



*Ethernet [Wireshark 1.12.6 (v1.12.6-0-gee1fce6 from master-1.12)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply Save

```
No.   Time          Source          Destination     Protocol Length Info
  107 11.405111000  192.168.0.45    192.168.0.255   NBNS      92 Name query NB ISATAP<00>
  108 11.627995000  Dell_c3:b6:31   Broadcast       ARP       60 Who has 192.168.0.1?  Tell 192.168.0.30
  109 11.757989000  192.168.0.37    192.168.0.255   NBNS      92 Name query NB ADMIN-PC<00>
```

```
⊟ Frame 108: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
    Interface id: 0 (\Device\NPF_{FC4C4DBB-A342-4918-89FC-53DFA1471BE3})
    Encapsulation type: Ethernet (1)
    Arrival Time: Jul  7, 2015 04:40:22.109640000 Pacific Daylight Time
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1436269222.109640000 seconds
    [Time delta from previous captured frame: 0.222884000 seconds]
    [Time delta from previous displayed frame: 0.222884000 seconds]
    [Time since reference or first frame: 11.627995000 seconds]
    Frame Number: 108
    Frame Length: 60 bytes (480 bits)
    Capture Length: 60 bytes (480 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:arp]
    [Coloring Rule Name: ARP]
    [Coloring Rule String: arp]
⊟ Ethernet II, Src: Dell_c3:b6:31 (d4:be:d9:c3:b6:31), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
  ⊟ Destination: Broadcast (ff:ff:ff:ff:ff:ff)
      Address: Broadcast (ff:ff:ff:ff:ff:ff)
      .... ..1. .... .... .... .... = LG bit: Locally administered address (this is NOT the factory default)
      .... ...1 .... .... .... .... = IG bit: Group address (multicast/broadcast)
  ⊟ Source: Dell_c3:b6:31 (d4:be:d9:c3:b6:31)
      Address: Dell_c3:b6:31 (d4:be:d9:c3:b6:31)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: ARP (0x0806)
    Padding: 000000000000000000000000000000000000
⊟ Address Resolution Protocol (request)
    Hardware type: Ethernet (1)
    Protocol type: IP (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    Sender MAC address: Dell_c3:b6:31 (d4:be:d9:c3:b6:31)
    Sender IP address: 192.168.0.30 (192.168.0.30)
    Target MAC address: Broadcast (ff:ff:ff:ff:ff:ff)
    Target IP address: 192.168.0.1 (192.168.0.1)
```

ARP Data

Frame (frame), 60 bytes | Packets: 1933 · Displayed: 1933 (100.0%) · Dropped: 0 (0.0%) | Profile: Bluetooth

IGRP (Interior Gateway Routing Protocol)

- IGRP is also a Distance-Vector protocol, developed for transmitting routing data within the internet network
- It is unlike IP RIP and IPX RIP, which were developed for multi-vendor networks
- It calculates distance metric by using Bandwidth and Delay of the Line, by default. It can also use other attributes like Reliability, Load, and MTU, but these are optional.
- IGRP includes the following Distance-Vector characteristics:
  - Periodic routing updates after every 90 seconds
  - Includes full routing table after every periodic update
  - Broadcast updates
  - Neighbors
  - It defines the finest "path" to a specific destination through the Bellman-Ford Distance Vector algorithm

Features:

- It performs only IP routing
- It makes use of IP protocol 9
- An administrative distance of IGRP routes is 100
- It has a maximum of 100 hops, by default. It can be extended to 255 hops

EIGRP (Enhanced Interior Gateway Routing Protocol)

- It is a Hybrid routing protocol. It includes characteristics of both Distance-Vector and Link-State routing protocols
- It allows a router to share routes with other routers within the same network system

EIGRP adheres to the following Hybrid characteristics:

- It uses Diffusing Update Algorithm (DUAL) to define the best path among all "feasible" paths and ensure a loop-free routing environment
- It maintains neighbor relationships with adjacent routers in the same Autonomous System (AS)
- Its traffic is either sent as unicasts or as multicasts on address 224.0.0.10, based on the EIGRP packet type
- Reliable Transport Protocol (RTP) is used to ensure the delivery of most of the EIGRP packets
- EIGRP routers do not send periodic, full-table routing updates. Updates are sent when a change occurs and includes only the change
- It is a classless protocol; therefore, it supports VLSMs.

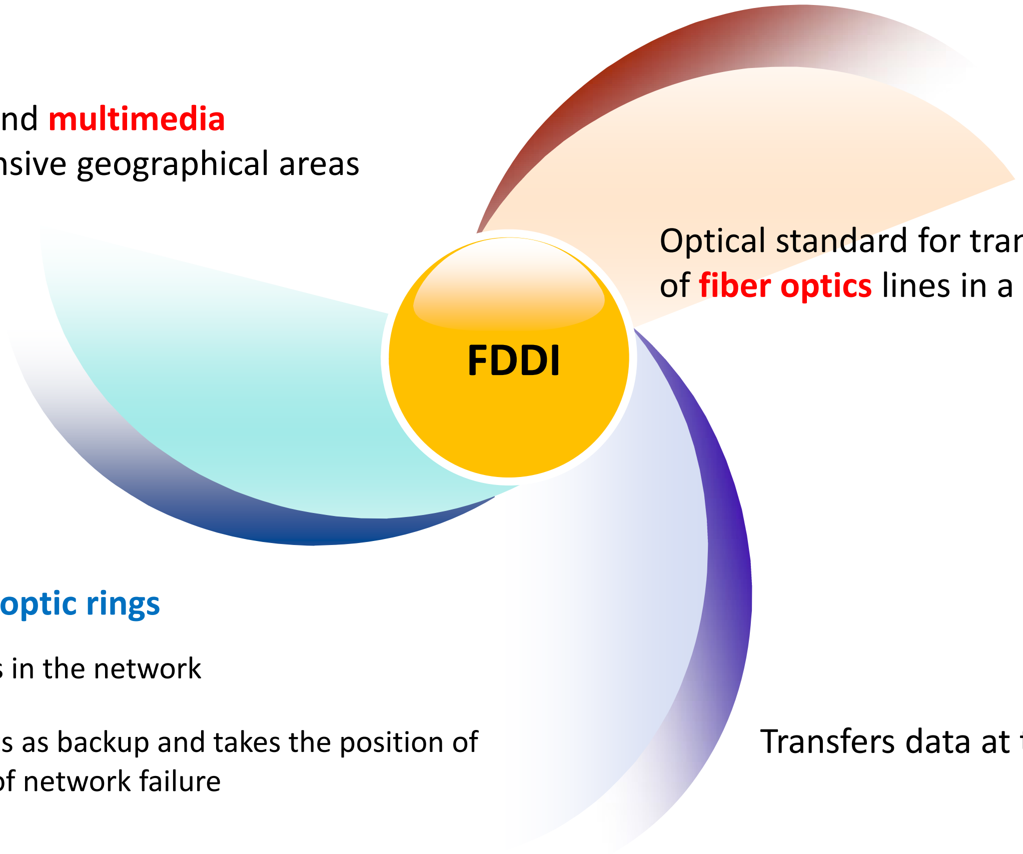
Features:

- It supports IP, IPX, and Appletalk routing
- It uses an Administrative Distance of 90 for routes originating within the local Autonomous System
- It uses an Administrative Distance of 170 for external routes coming from outside the local Autonomous System
- It calculates distance metric by using Bandwidth and Delay of the Line, by default. It can also use other attributes like Reliability, Load, and MTU, but these are optional.
- It has a maximum of 100 hops, by default. It can be extended to 255 hops

Link Layer Protocols

Fiber Distributed Data Interface (FDDI)

FDDI-2 supports **voice** and **multimedia** communication to extensive geographical areas



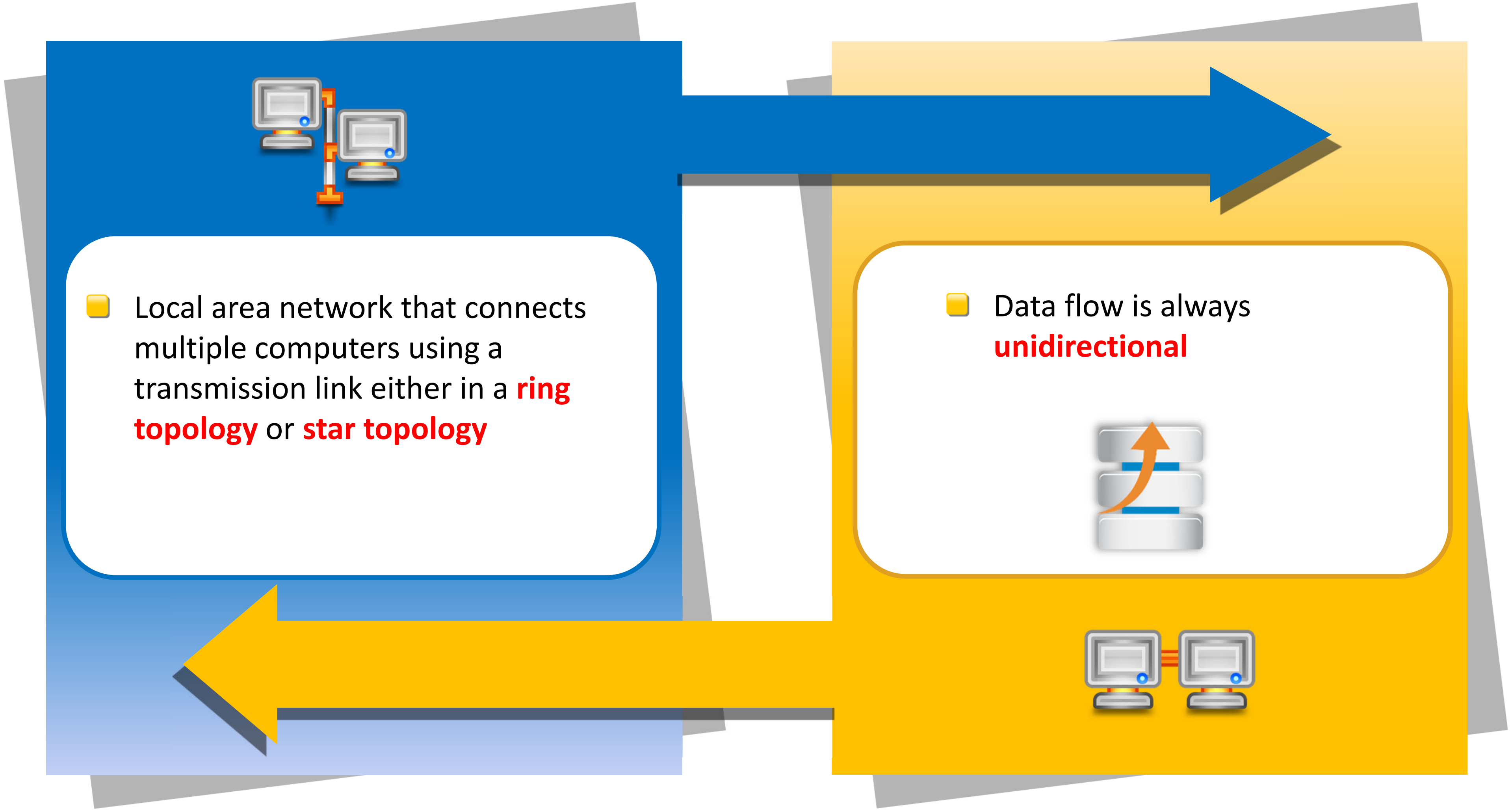
Optical standard for transferring data by means of **fiber optics** lines in a LAN up to 200 km

Comprises of two fiber optic rings

- **Primary ring:** Works in the network
- **Secondary ring:** Acts as backup and takes the position of primary ring in case of network failure

Transfers data at the rate of **100 Mbps**

Token Ring

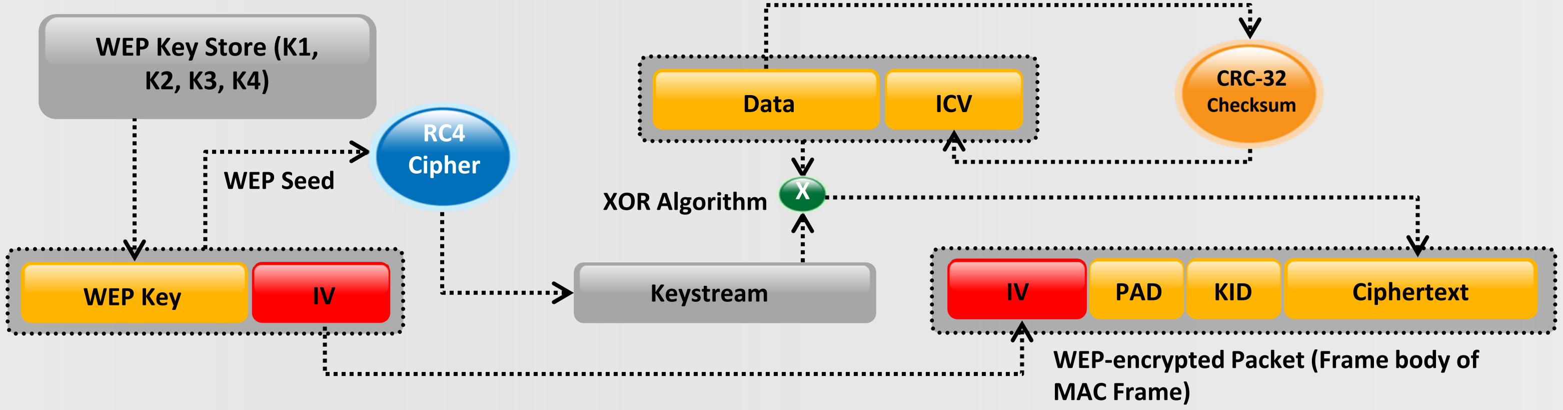


- Local area network that connects multiple computers using a transmission link either in a **ring topology** or **star topology**

- Data flow is always **unidirectional**

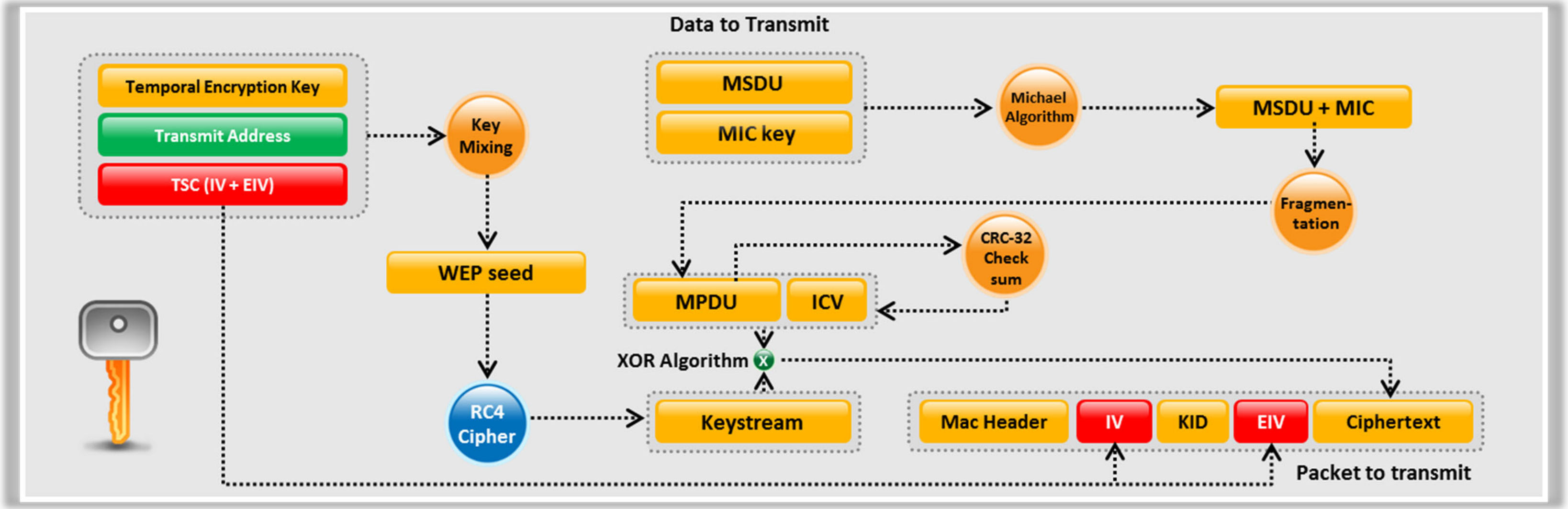
WEP (Wired Equivalent Privacy) Encryption

- WEP is a security protocol defined by the 802.11b standard; it was designed to provide ~~a~~ wireless LAN with a level of **security and privacy** comparable to a wired LAN
- A 24-bit arbitrary number known as Initialization Vector (IV) is added to the WEP key. The WEP key and the IV together are called as a **WEP seed**
- The 64, 128, and 256-bit WEP versions use 40, 104, and 232-bit keys, respectively
- The WEP seed is used as the input for the **RC4 algorithm** to generate a keystream (keystream is bit-wise XORed with the combination of data and ICV to produce the encrypted data)
- The **CRC-32 checksum** is used to calculate a 32-bit Integrity Check Value (ICV) for the data, which, in turn, is added to the data frame
- The IV field (IV+PAD+KID) is added to the **cipher text** to generate a MAC frame



WPA (Wi-Fi Protected Access) Encryption

- WPA is a security protocol defined by 802.11i standards; it uses a Temporal Key Integrity Protocol (TKIP) that utilizes **the RC4 stream cipher encryption** with 128-bit keys and 64-bit MIC integrity check to provide stronger encryption, and authentication
- The temporal encryption key, transmits address, and TKIP sequence counter (TSC) is used as an input for the RC4 algorithm to generate a **keystream**
- A MAC Service Data Unit (MSDU) and message integrity check (MIC) are combined using the **Michael algorithm**
- The combination of the **MSDU** and the **MIC** is fragmented to generate the MAC Protocol Data Unit (MPDU)
- A 32-bit ICV is calculated for the MPDU, and the combination of the MPDU and the ICV is then bitwise XORed with keystream to produce the **encrypted data**
- The IV is added to the encrypted data to generate the **MAC frame**



WPA2 Encryption

WPA2 is an **upgrade to WPA**. It includes mandatory support for Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP), **an AES-based encryption mode** with strong security

WPA2-Personal

- WPA2-Personal uses a set-up password (**Pre-shared Key**, PSK) to protect unauthorized network access
- In PSK mode, each wireless network device encrypts the network traffic using a **128-bit key** that is derived from a passphrase of 8 to 63 ASCII characters

WPA2-Enterprise

- It includes **EAP** or **RADIUS** for centralized client authentication using multiple authentication methods, such as token cards, Kerberos, certificates etc.
- Users are assigned **login credentials** by a centralized server which they must present when connecting to the network

WEP vs. WPA vs. WPA2

Encryption	Attributes			
	Encryption Algorithm	IV Size	Encryption Key Length	Integrity Check Mechanism
WEP	RC4	24-bits	40/104-bit	CRC-32
WPA	RC4, TKIP	48-bit	128-bit	Michael algorithm and CRC-32
WPA2	AES-CCMP	48-bit	128-bit	CBC-MAC

WEP ✗	Should be replaced with more secure WPA and WPA2
WPA, WPA2 ✓	Incorporates protection against forgery and replay attacks

TKIP

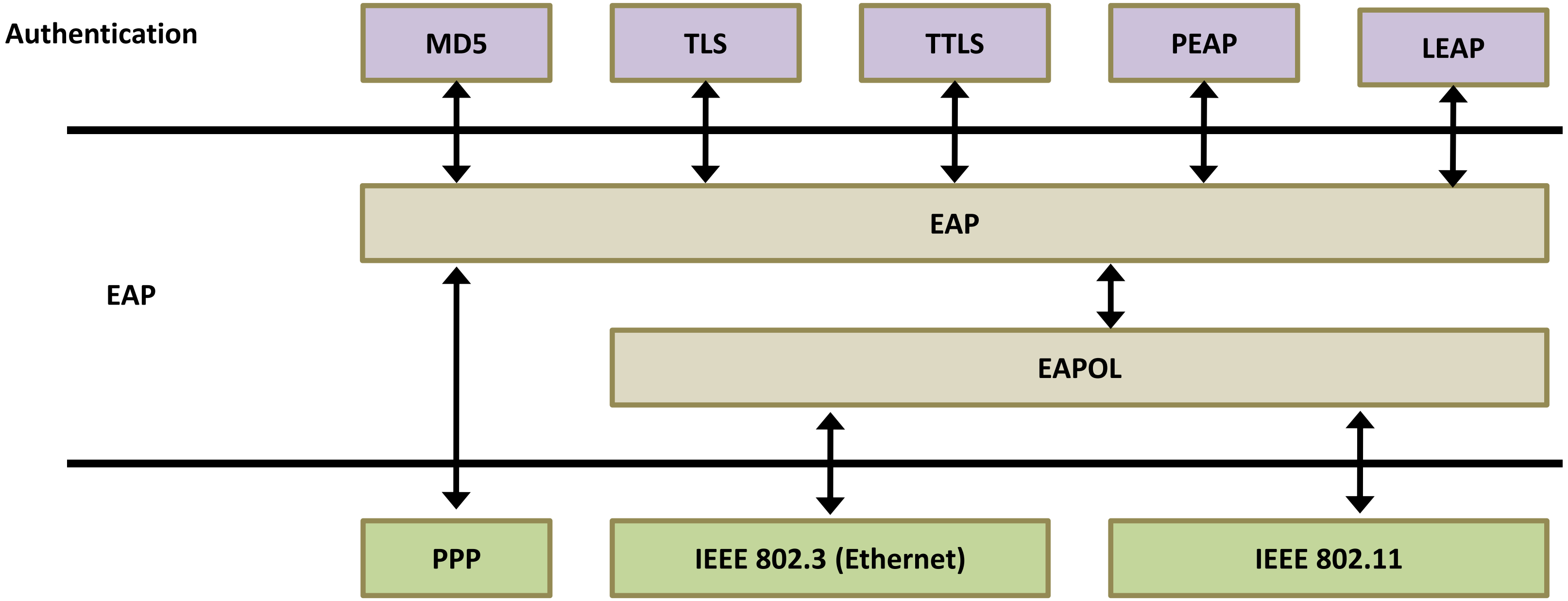
- TKIP (Temporal Key Integrity Protocol) is an encryption protocol used in IEEE 802.11 wireless network standard
- TKIP is the TaskGroupi’s solution for the security loop holes present in the already deployed 802.11 hardware

TKIP features:

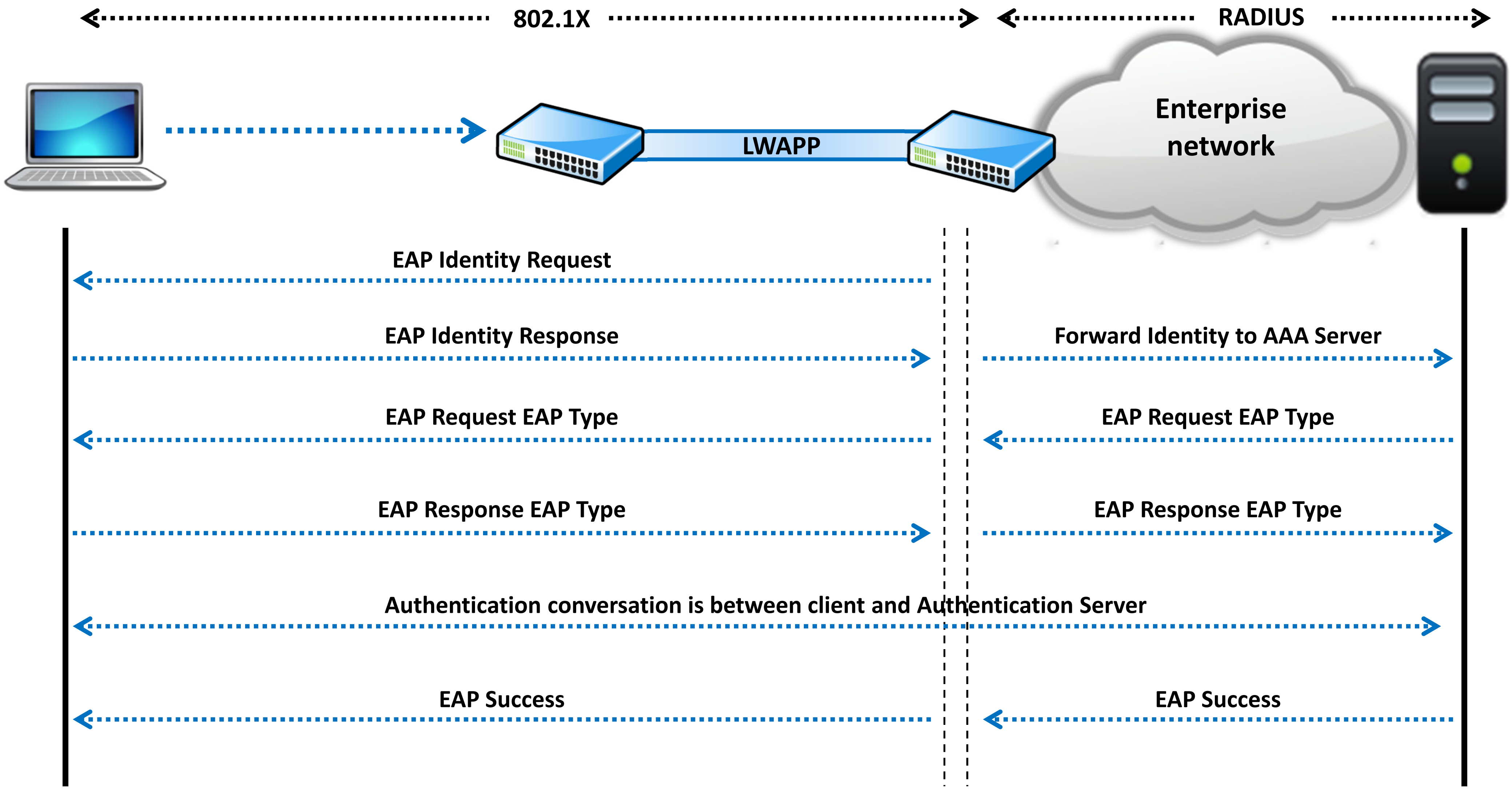
- Boosts encryption strength
- Prevents collision attacks without hardware replacement
- Serves as a WEP code wrapper and also adding per-packet mixing of media access control (MAC) base keys and serial numbers
- Assigns a unique 48-bit sequencing number to each packet
- Utilizes the RC4 stream cipher - 128-bit encryption keys and 64-bit authentication keys

EAP (Extensible Authentication Protocol)

- EAP (Extensible Authentication Protocol) is the most commonly used authentication framework for both Point-to-Point connections as well as wireless networks
- It is used as primary authentication method in most of the wireless security protocols like WPA and WPA2 in wireless networks
- Some of the more popular authentication methods in EAP protocol include MD5, TLS, TTLS, PEAP, LEAP, etc.



How EAP Works?



Understanding LEAP / PEAP

- LEAP (Lightweight Extensible Authentication Protocol) was created by Cisco Systems where you don't have to set up any digital certificates and PKI's. The major drawback of this protocol is that it uses modified version of MS-CHAP authentication protocol which does not ensure protection of user credentials. You can use tools like ASLEAP to compromise LEAP protocol

- PEAP (Protected Extensible Authentication Protocol) is a fully encapsulated EAP, which is intended to work within TLS tunnel. PEAP was developed to correct most of the deficiencies of EAP protocol. Initial version of PEAP, i.e., PEAPv0 was initially used in Windows XP, and PEAPv1 and PEAPv2 are used in the subsequent products

CDP (Cisco Discovery Protocol)

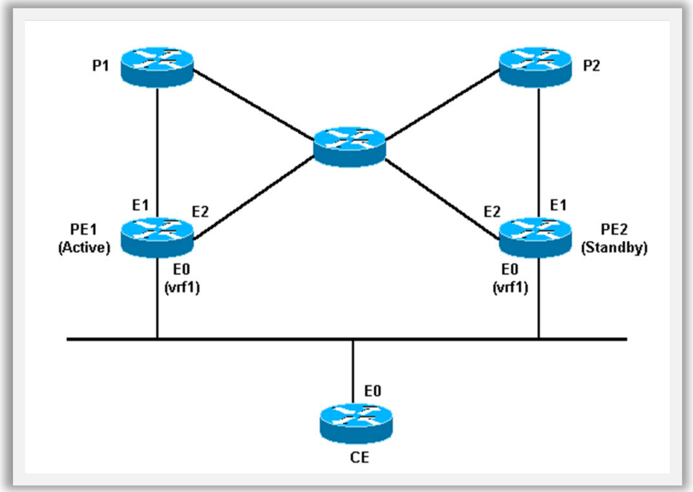
- It is a layer 2 (data link layer) Cisco proprietary protocol
- It shares the data between directly connected network devices
- It is media as well as network independent
- CDP uses a destination MAC address of 01.00.0c.cc.cc.cc
- It connects lower physical media and upper network layer protocols
- It runs between direct connected network entities
- It can also be used for On-Demand Routing
- CDP is used to obtain information about neighboring devices, such as:
  - Types of devices connected
  - Router interfaces they are connected to
  - Interfaces used to make the connections
  - Model numbers of the devices

Security issues:

- It can be vulnerable to Denial-of-Service (DoS) attack

HSRP (Hot Standby Router Protocol)

- It is a routing protocol used to establish a fault-tolerant default gateway and allows the host computer to use multiple routers that act as a single virtual router
- It is a Cisco-developed redundancy protocol
- Virtual IP and MAC address are shared between the two routers
- To verify HSRP state, use the show standby command
- It makes sure that only active router takes part in sending packets
- It is designed for multi access or broadcast LAN
- It get automatically self updated when MAC address is modified



Security issues:

- It can be vulnerable to DoS attack

Virtual Router Redundancy Protocol (VRRP)

- It is a computer networking protocol that provides for automatic assignment of available Internet Protocol (IP) routers to participating hosts
- It provides information on the state of a router. It does not provide information about routes processed and exchanged by the router
- If the physical router that is routing packets on behalf of the virtual router fails, another physical router is selected automatically to replace it

Security issues:

- It is vulnerable to DoS attack

VLAN Trunking Protocol (VTP)

- VTP is a messaging protocol developed by Cisco and is used to exchange VLAN information across trunk links
- It works on data link layer of OSI model
- It allows network manager to distribute VLAN configuration to all switches in the same domain
- It stores VLAN configuration in VLAN database
- It supports Plug-and-play configuration when adding new VLANs

Security issues:

- It is vulnerable to DoS attack
- There can be Integer wrap in VTP revision
- The Buffer Overflow vulnerability exists in VTP VLAN name

STP (Spanning Tree Protocol)

- STP (Spanning Tree Protocol) is a layer 2, network protocol that runs on bridges and switches
- Network control protocol is designed for use in entertainment and communications systems to control streaming media servers

Security issues:

STP can be vulnerable to:

- Man-in-the-middle Attack
- Attack on file and path name
- DNS Spoofing
- Denial-of-service
- Session hijacking
- Authentication mechanism

IP Addressing and Port Numbers

Internet Assigned Numbers Authority (IANA)

IANA is responsible for the global coordination of DNS Root, IP addressing, and other Internet protocol resources

The well-known ports are assigned by IANA and can only be used by the system (or root) processes or by programs executed by the privileged users on most systems

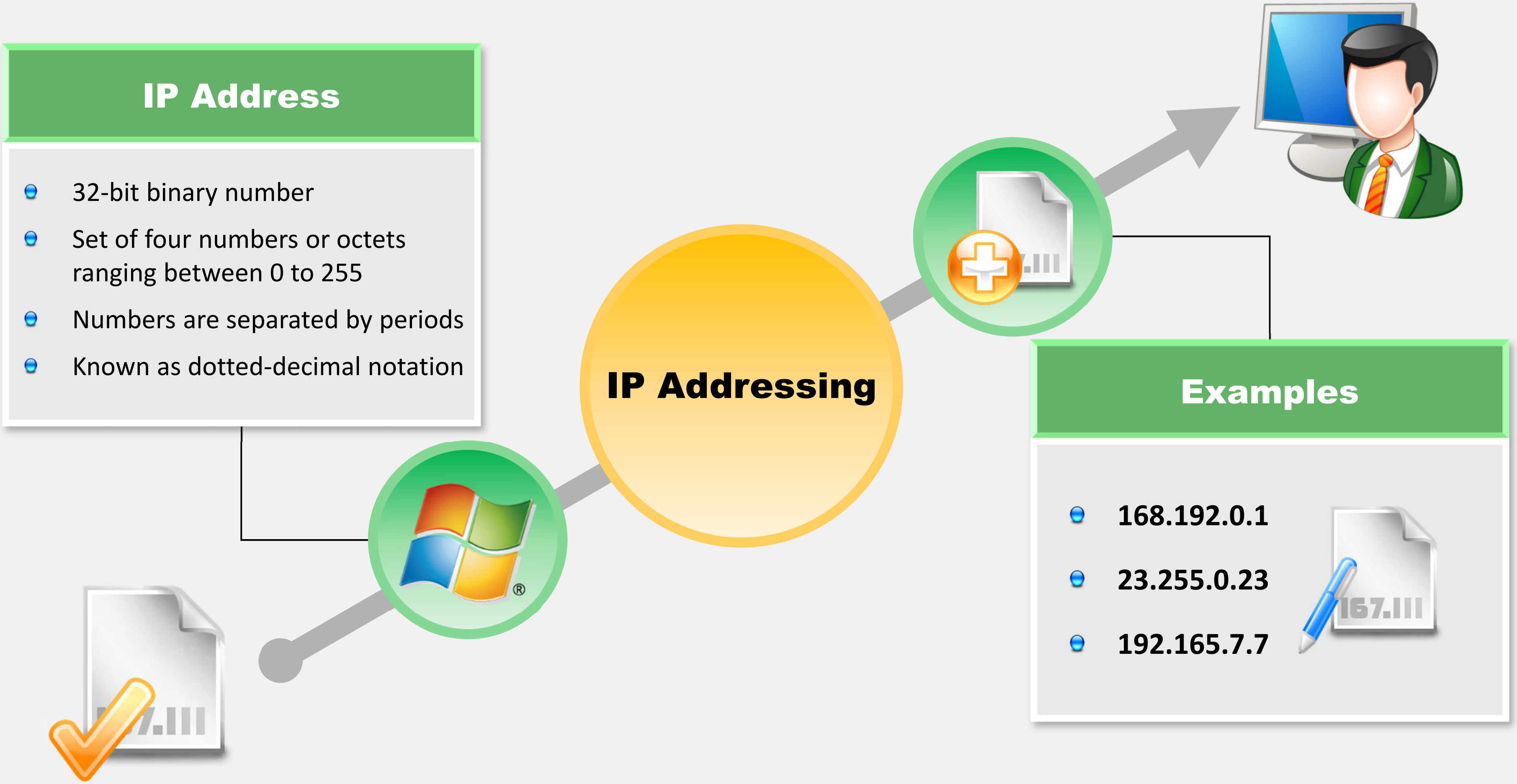
The registered ports are listed by the IANA and can be used by ordinary user processes or programs executed by the ordinary users on most systems

The IANA registers the uses of these ports as a convenience to the community

The range for assigned ports managed by the IANA is 0-1023

IP Addressing

IP Address is a unique numeric value assigned to a node or a network connection



IP Address

- 32-bit binary number
- Set of four numbers or octets ranging between 0 to 255
- Numbers are separated by periods
- Known as dotted-decimal notation

IP Addressing

Examples

- 168.192.0.1
- 23.255.0.23
- 192.165.7.7

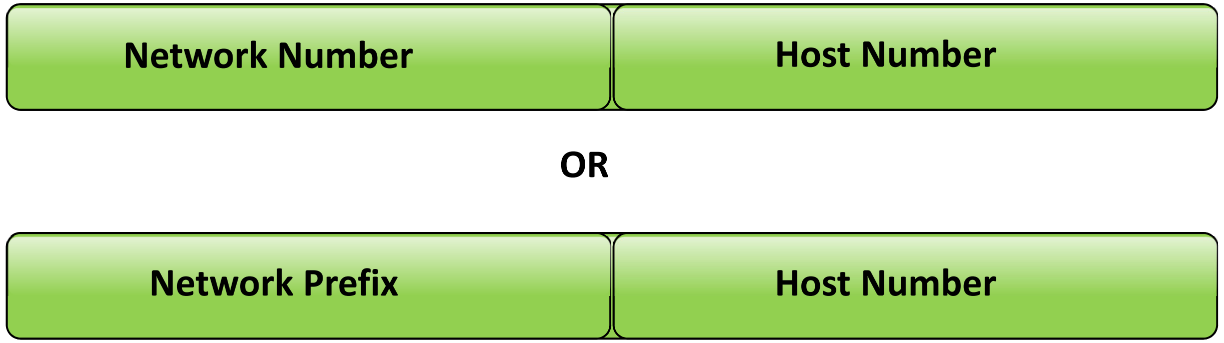
Classful IP Addressing

- IP addresses is divided into **5 major classes** in classful IP addressing scheme
- It was the first **addressing** scheme of Internet that managed addressing through classes **A**, **B**, **C**, **D**, and **E**
- An IP address can be broken down into two parts:
  - First part represents network
  - Second part represents a specific **host** on the network

NOTE:

- All the hosts residing on a network can **share the same network** prefix but should have a unique host number
- Hosts residing on different networks can have the same host number but should have **different** network **prefixes**

Two-Level Internet Address Structure:

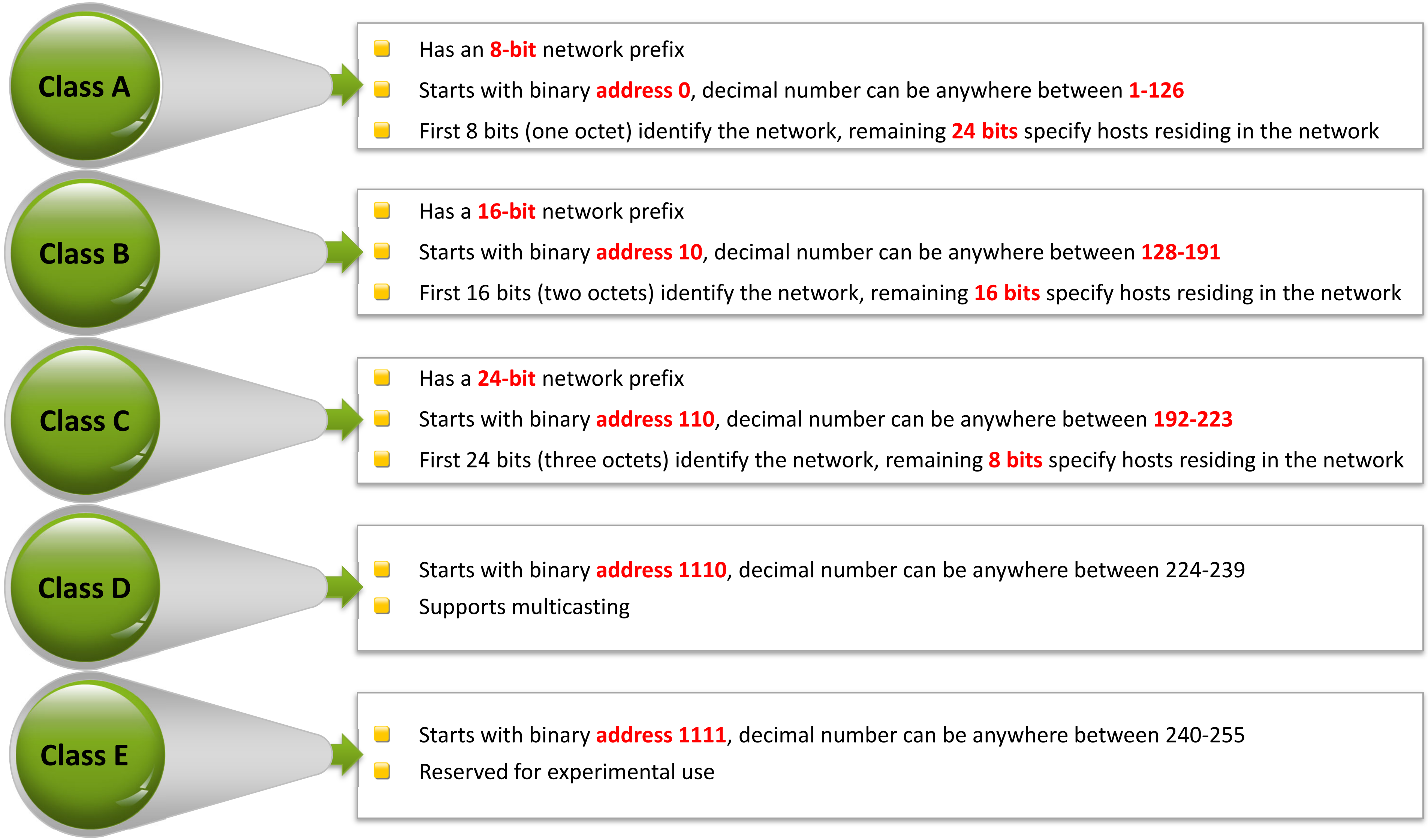


Network Number	Host Number

OR

Network Prefix	Host Number

Address Classes



Class A

- Has an **8-bit** network prefix
- Starts with binary **address 0**, decimal number can be anywhere between **1-126**
- First 8 bits (one octet) identify the network, remaining **24 bits** specify hosts residing in the network

Class B

- Has a **16-bit** network prefix
- Starts with binary **address 10**, decimal number can be anywhere between **128-191**
- First 16 bits (two octets) identify the network, remaining **16 bits** specify hosts residing in the network

Class C

- Has a **24-bit** network prefix
- Starts with binary **address 110**, decimal number can be anywhere between **192-223**
- First 24 bits (three octets) identify the network, remaining **8 bits** specify hosts residing in the network

Class D

- Starts with binary **address 1110**, decimal number can be anywhere between 224-239
- Supports multicasting

Class E

- Starts with binary **address 1111**, decimal number can be anywhere between 240-255
- Reserved for experimental use

Address Classes (Cont'd)

Table showing number of Networks and Hosts:

Class	Leading Bits	Size of Network Number Bit Field	Size of Host Number Bit Field	Number of Networks	Addresses Per Network
Class A	0	7	24	126	16,277,214
Class B	10	14	16	16,384	65,534
Class C	110	21	8	2,097,152	254
Class D (Multi cast)	1110	20	8	1,048,576	254
Class E (Reserved)	1111	20	8	1,048,576	254

IP Address Classes and class characteristics and uses

IP Address Class	Fraction of Total IP Address Space	Number of Network ID Bits	Number of Host ID Bits	Intended Use
Class A	1/2	8	24	Used for Unicast addressing for very large size organizations
Class B	1/4	16	16	Used for Unicast addressing for medium or large size organizations
Class C	1/8	24	8	Used for Unicast addressing for small size organizations
Class D	1/16	N/A	N/A	Used for IP multicasting
Class E	1/16	N/A	N/A	Reserved

Subnet Masking

1. Subnet Mask divides the IP address of the host into **network and host** number

2. Subnet allows division of Class A, B, and C network numbers into **smaller segments**

3. Variable length subnet mask (VLSM) allows two or more subnet masks in the **same network**

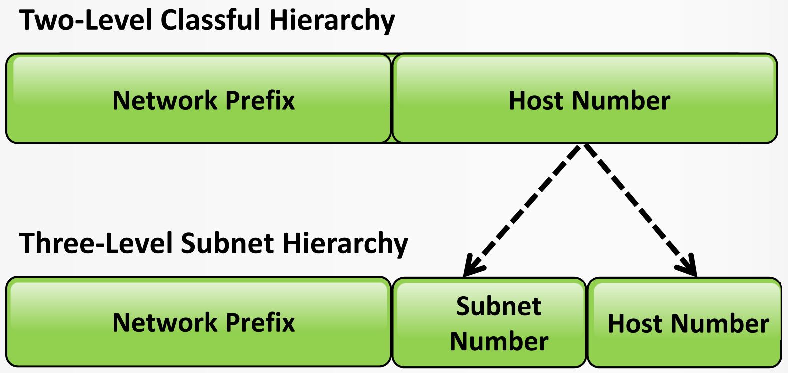
4. VLSM effectively uses **IP address** space in a network

Default Subnet Masks for Class A, Class B and Class C Networks

IP Address Class	Total # bits for Network ID/Host ID	Default Subnet Mask			
		First Octet	Second Octet	Third Octet	Fourth Octet
Class A	8/24	11111111	00000000	00000000	00000000
Class B	16/16	11111111	11111111	00000000	00000000
Class C	24/8	11111111	11111111	11111111	00000000

Subnetting

- Subnetting allows you to divide a Class A, B, or C network into different **logical subnets**
- To subnet a network, use some of the bits from the host ID portion, in order to **extend natural mask**



Subnet Address Hierarchy

- For example, Consider class C Address

IP Address : 192.168.1.12
11000000.10101000.00000001.00001010

Subnet mask: 255.255.255.0
11111111.11111111.11111111.00000000

Subnetting: 255.255.255.224
11111111.11111111.11111111.11100000

These three extra bits from host ID portion allows you to create eight subnets

Supernetting

Class A and B **addresses** are in depletion stage

Supernetting combines various Class C addresses and creates a **super network**

Also known as Classless **Inter-Domain** Routing (CIDR), it was invented to keep IP addresses from exhaustion

Class C provides only 256 **hosts** in a network out of which 254 are available for use

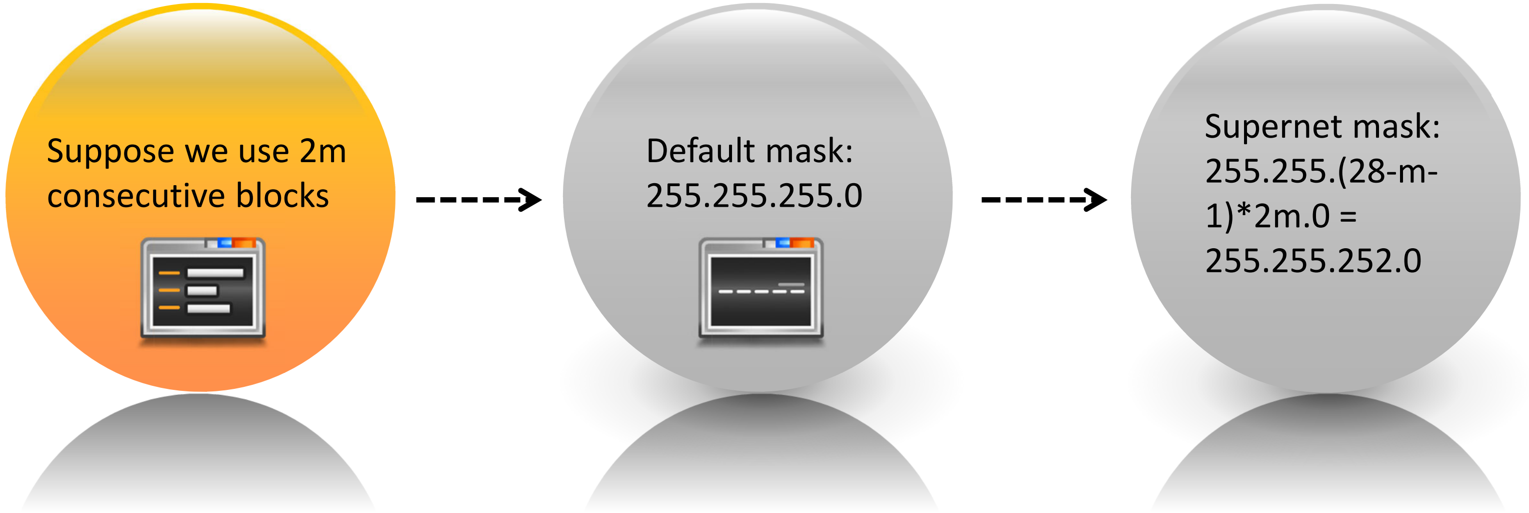
It applies to **Class C** addresses

Supernet mask is **reverse** of subnet mask

Subnet Mask	11111111 11111111 11111111 **111** 00000
Default Mask	11111111 11111111 11111111 000 00000
Supernet Mask	11111111 11111111 11111**000** 000 00000

Supernetting (Cont'd)

Supernetting Class C Example:

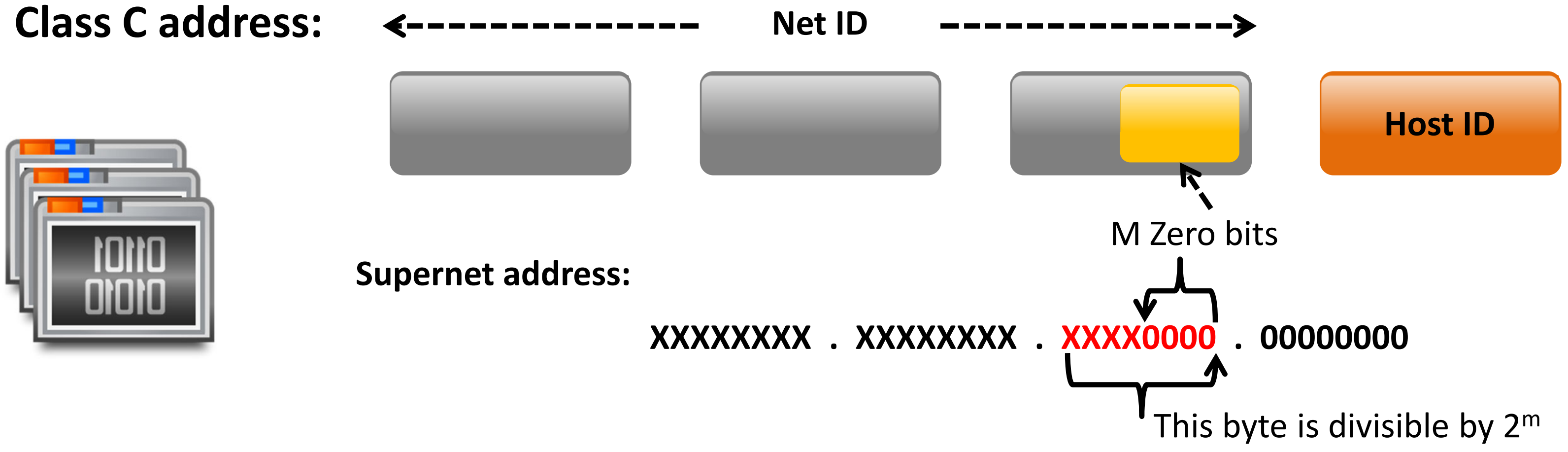


Suppose we use 2m consecutive blocks

Default mask: 255.255.255.0

Supernet mask: 255.255.(28-m-1)*2m.0 = 255.255.252.0

Class C address:



Supernet address:

XXXXXXXX . XXXXXXXX . XXXX0000 . 00000000

This byte is divisible by 2^m

IPv6 Addressing

- Based on the **standard** specified by the RFC 4291
- Allows **multilevel** subnetting
- Supports unicast, anycast, and multicast addresses
- IPv6 address space is organized in a **hierarchical** structure

IPv6: Format prefix allocation

Allocation	Format Prefix	Start of address range (hex)	Mask length (bits)	Fraction of address space
Reserved	0000 0000	0:: 8/	8	1/256
Reserved for Network Service Allocation Point (NSAP)	0000 001	200:: /7	7	1/128
Reserved for IPX	0000 010	400:: /7	7	1/128
Aggregatable global unicast addresses	001	2000:: /3	3	1/8
Link-local unicast	1111 1110 10	FE80:: /10	10	1/1024
Site-local unicast	1111 1110 11	FEC0:: /10	10	1/1024
Multicast	1111 1111	FF00:: /8	8	1/256

Difference between IPv4 and IPv6

	Internet Protocol version 4 (IPv4)	Internet Protocol version 6 (IPv6)
Deployed	In the year 1981	In the year 1999
Size	32-bit addresses	128-bit source and destination addresses
Format	Dotted-decimal notation (separated by periods)	Hexadecimal notation (separated by colon)
Example	192.168.0.77	3ffe:1900:4545:AB00: 0123:4567:8901:ABCD
Prefix Notation	192.168.0.7/74	3FFE:F200:0234::/77
Total Number of Addresses	2^32 = ~4,294,967,296	2^128 = ~340,282,366, 920,938,463,463,374, 607,431,768,211,456
Configuration	Manually perform static or dynamic configuration	Auto-configuration of addresses is available
Security	IPSec is optional	Inbuilt support for IPSec

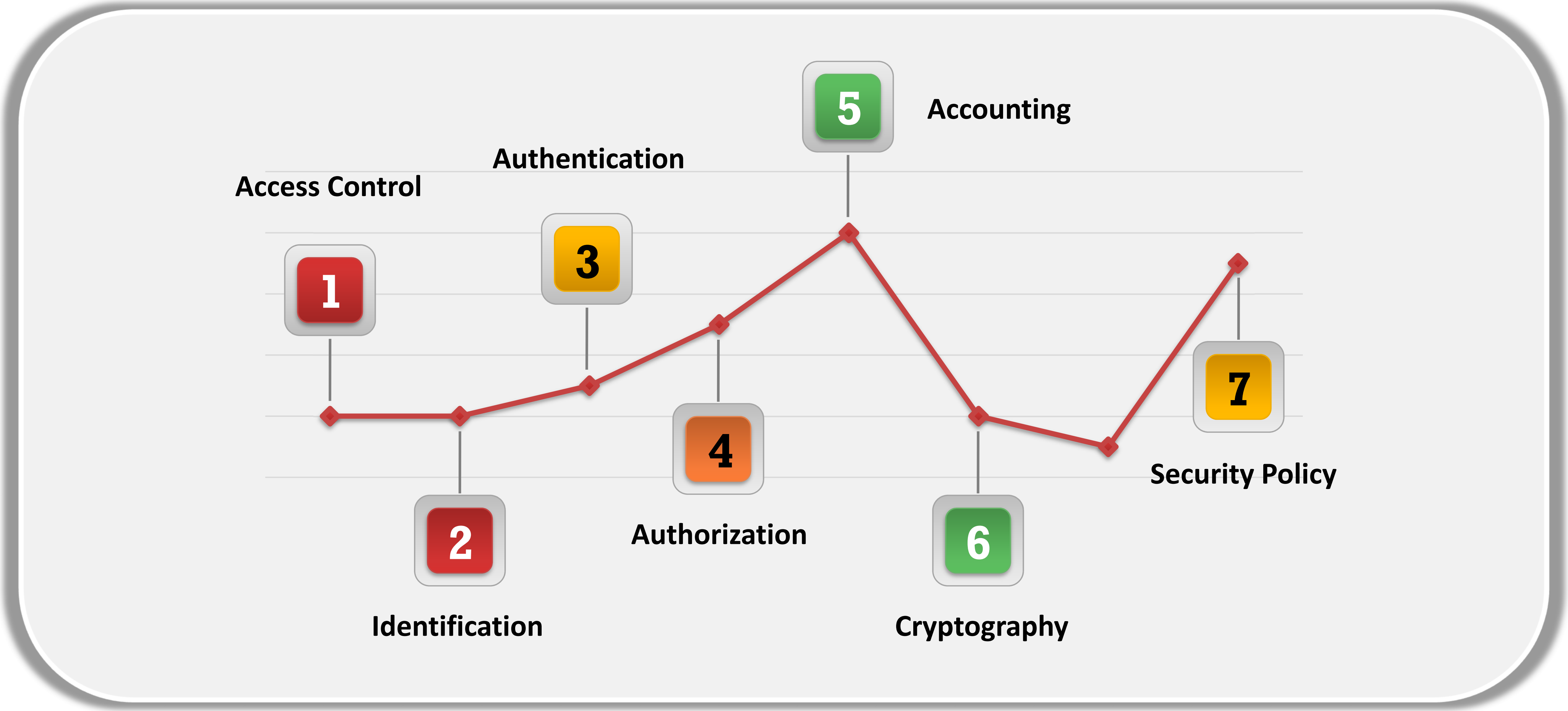
Port Numbers

- Both TCP and UDP use port (socket) numbers to pass information to the upper layers
- Port numbers are used to keep track of different conversations crossing the network at the same time
- Conversations that do not involve an application with a well-known port number are, instead, assigned port numbers that are randomly selected from within a specific range
- Some ports are reserved in both TCP and UDP, although applications might not be written to support them
- End systems use port numbers to select a proper application to handle the communication

- Port numbers have the following assigned ranges:
  - Numbers below 1024 are considered well-known port numbers
  - Numbers above 1024 are dynamically assigned port numbers
  - Registered port numbers are those registered for vendor-specific applications; most of these are above 1024

Network Security Controls

Network Security Controls



Access Control

Access control is the **selective restriction** of access to a place or other system/network resource

It **protects information assets** by determining who can and cannot access them

It **involves user identification**, authentication, authorization, and accountability

Access Control Terminology

Subject

It refers to a particular user or process which wants to access the resource

Object

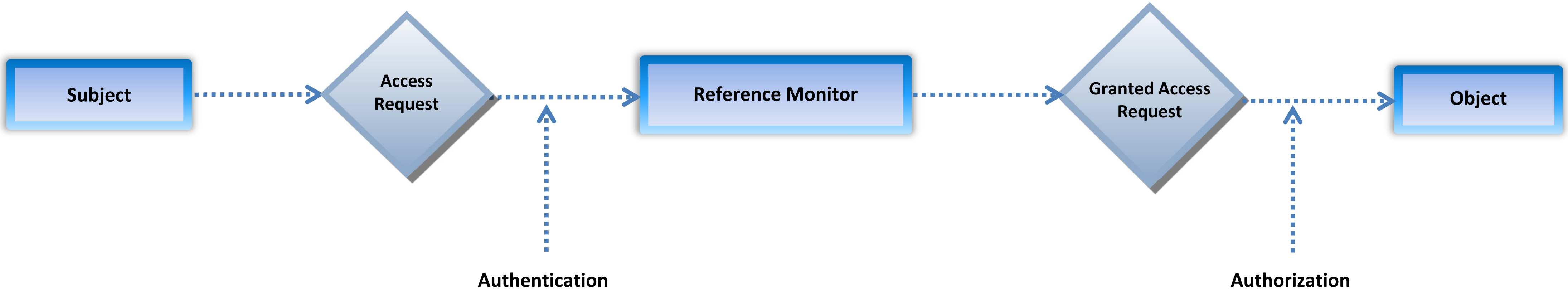
It refers to a specific resource that the user wants to access such as a file or any hardware device

Reference Monitor

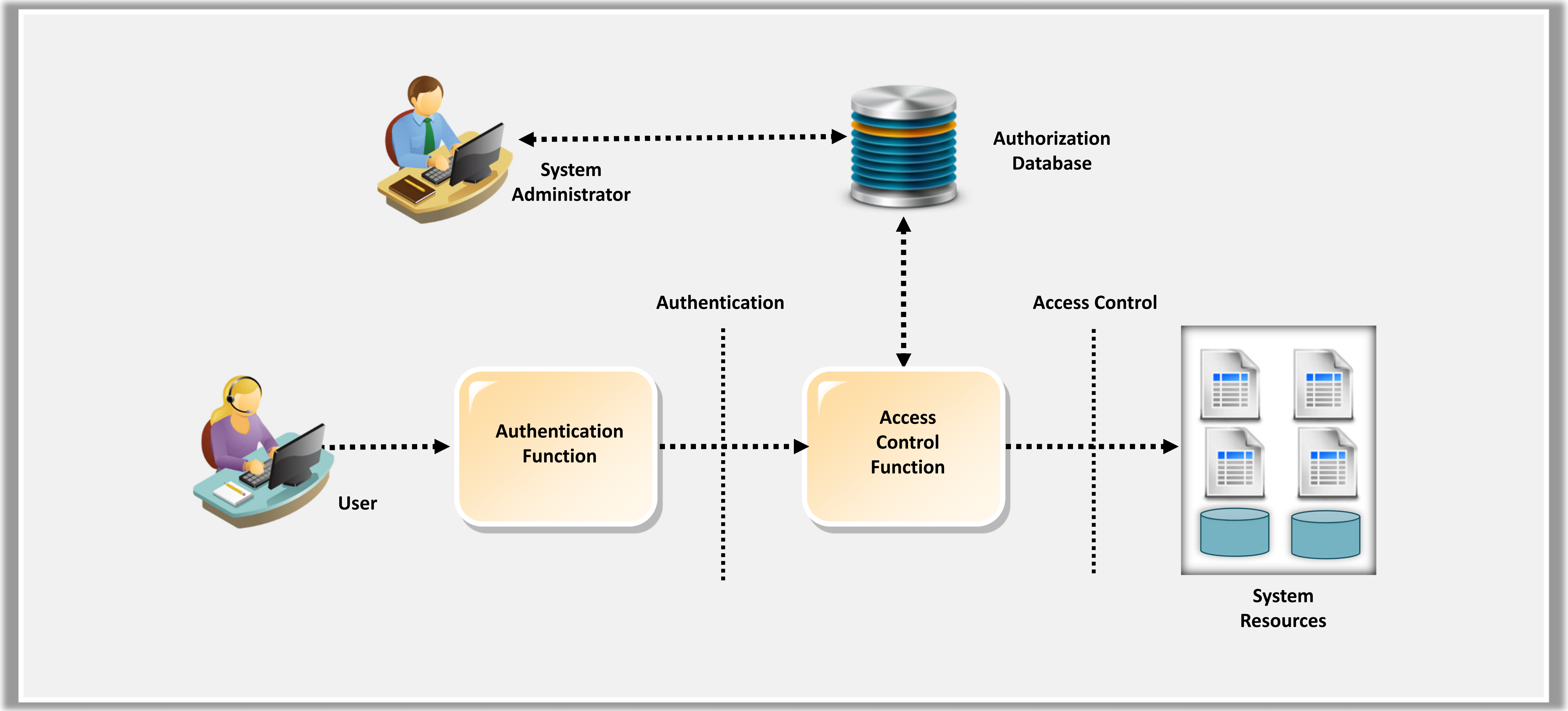
It checks the access control rule for specific restrictions

Operation

It represents the action taken by the object on the subject



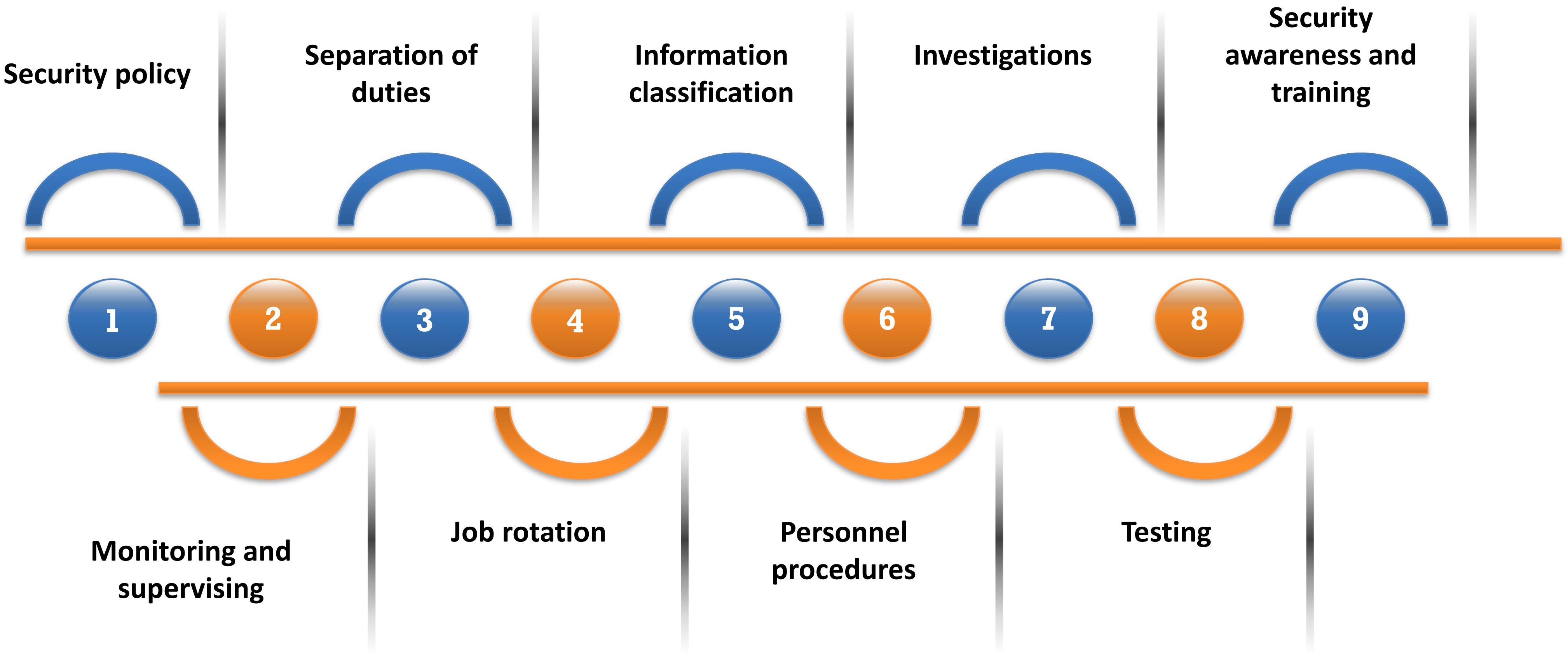
Access Control Principles



Access Control System: Administrative Access Control

- The management implements administrative access controls to **ensure** the **safety** of the organization

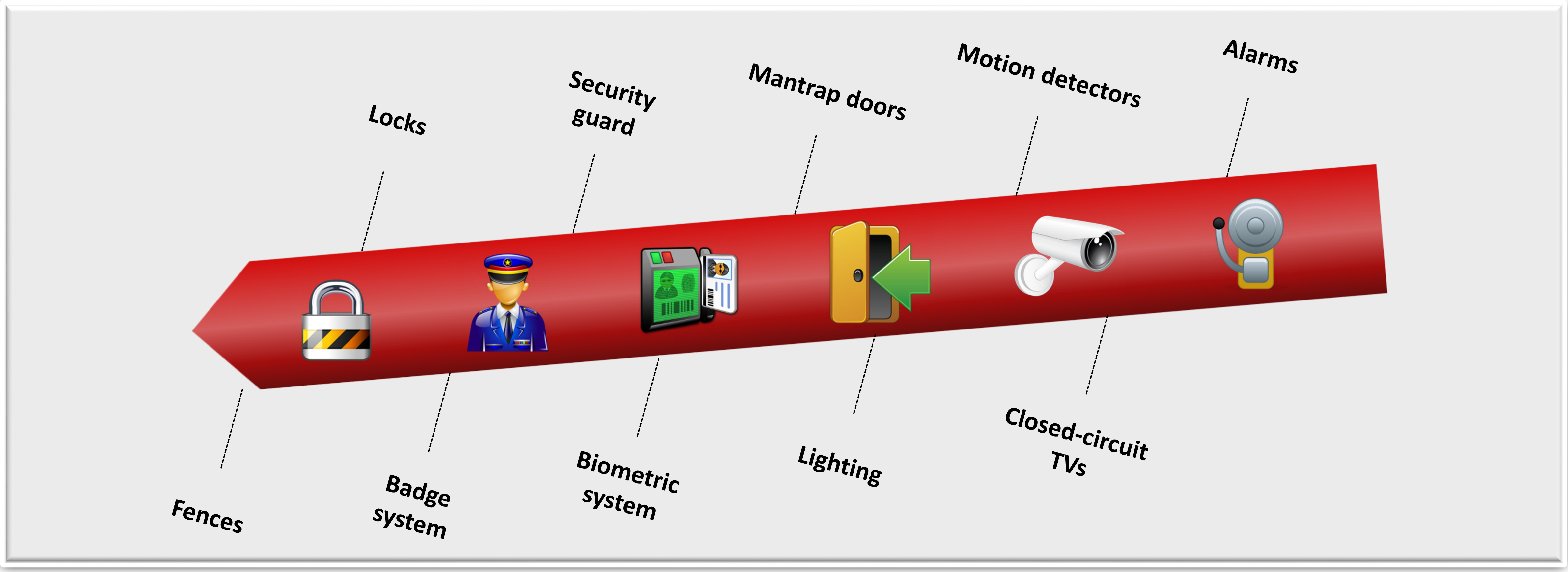
Administrative Access Controls



Access Control System: Physical Access Controls

- It is a set of security measures taken to **prevent unauthorized access** to physical devices

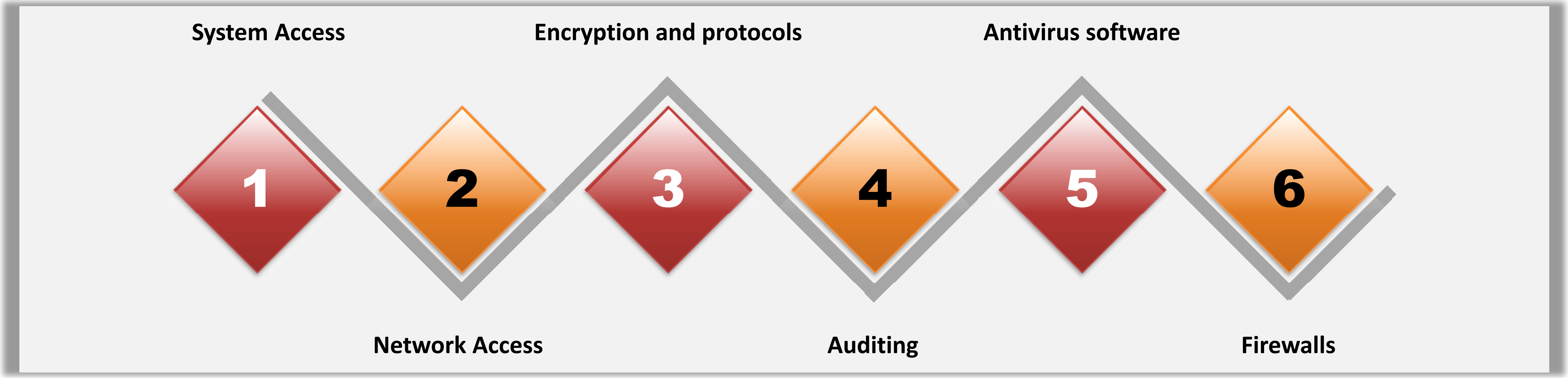
Physical Access Controls



Access Control System: Technical Access Controls

- It is a set of security measures taken to ensure confidentiality, integrity and availability of the resources

Technical Access Controls



1 System Access

2 Network Access

3 Encryption and protocols

4 Auditing

5 Antivirus software

6 Firewalls

Types of Access Control

Discretionary Access Control (DAC)

- It permits the user, who is granted access to information, to decide how **to protect the information** and the **level of sharing** desired
- Access to files is **restricted to users** and **groups** based upon their identity and the groups to which the users belong

Mandatory Access Control (MAC)

- It does not permit the end user **to decide who can access the information**
- It does not permit the user to **pass privileges** to other users, as the access could then be circumvented

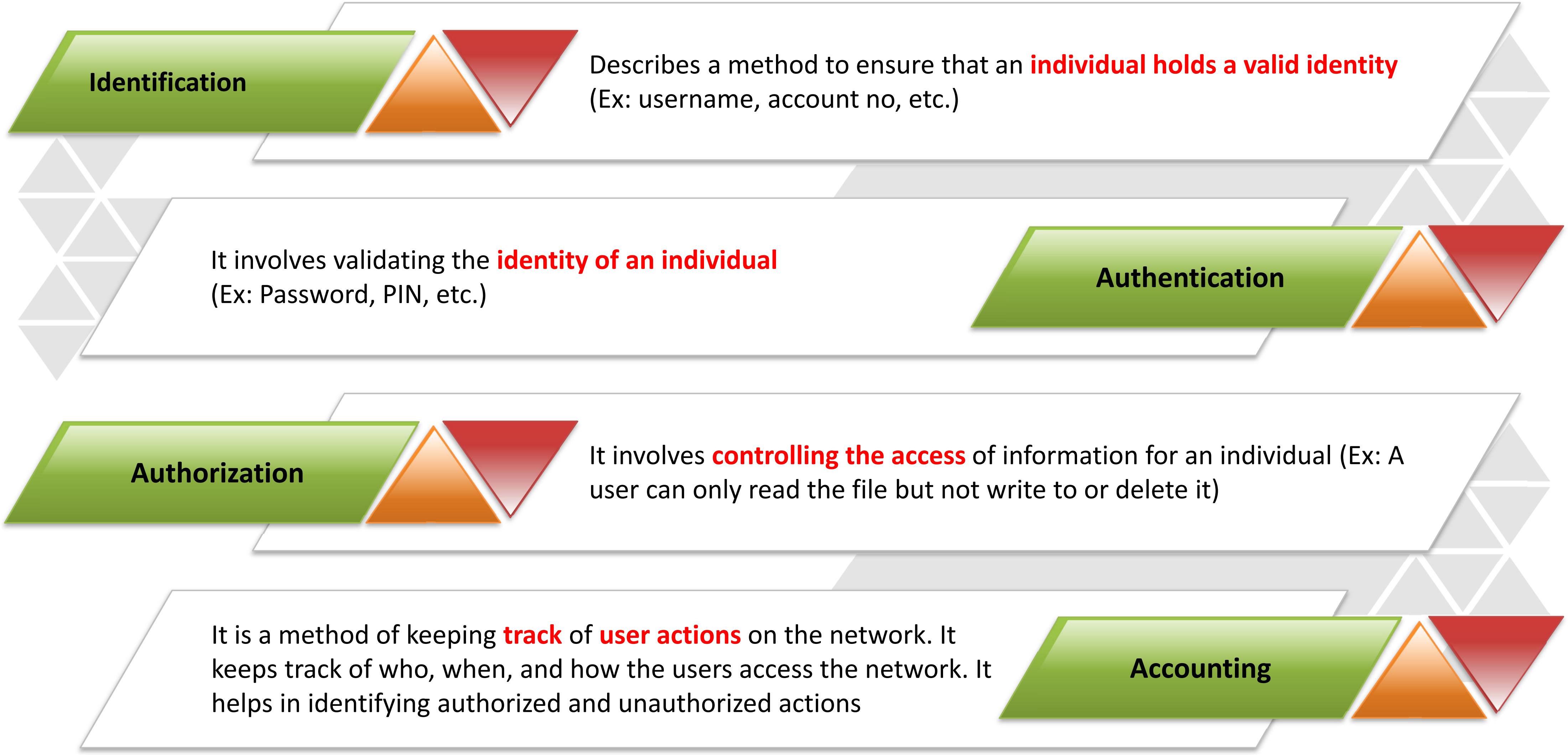
Role-based Access

- Users can be assigned **access to systems**, **files**, and **fields on a one-by-one basis** whereby access is granted to the user for a particular file or system
- It can simplify the **assignment of privileges** and ensure that individuals have all the privileges necessary to perform their duties

Network Access Control List

- Access control to an a specific object/operation is defined in terms of access control lists (ACL) or Access control rules
- Access control lists (ACL) is a list of permissions attached to a specific object/operation
- These permissions ~~states~~ that which user have access to specific object and the operations he/she is allowed to perform
- These ACLs are configured on network devices such as Firewall, routers, switches, etc.

User Identification, Authentication, Authorization and Accounting



Identification

Describes a method to ensure that an **individual holds a valid identity** (Ex: username, account no, etc.)

Authentication

It involves validating the **identity of an individual** (Ex: Password, PIN, etc.)

Authorization

It involves **controlling the access** of information for an individual (Ex: A user can only read the file but not write to or delete it)

Accounting

It is a method of keeping **track** of **user actions** on the network. It keeps track of who, when, and how the users access the network. It helps in identifying authorized and unauthorized actions

Types of Authentication: Password Authentication

1 Password Authentication uses a **combination** of username and password to authenticate network users

2 The password is checked against a **database** and allows access, if it matches

3 Password authentication can be vulnerable to **password cracking attacks** such as brute force, dictionary attacks

Types of Authentication: Two-factor Authentication

01

Two-factor authentication involves using two different authentication factors out of three (a knowledge factor, a possession factor, and an inherence factor) to verify the **identity of an individual** in order to enhance **security in authentication systems**

02

Combinations of two-factor authentication: password and smartcard/token, password and biometrics, password and OTP, smartcard/token and biometrics, etc.

03

Inherence factor (biometric authentication) is the best companion of two-factor authentication as it is considered as the **hardest to forge** or **spoof**

04

Most widely used physical or behavioral characteristics to establish or verify an identity: fingerprints, palm pattern, voice or face pattern, iris features, keyboard dynamics, signature dynamics, etc.

Types of Authentication: Biometrics

- Biometrics refers to the **identification of individuals** based on their physical characteristics

Biometric Identification Techniques

Fingerprinting

Ridges and **furrows** on the surface of a finger are used to identify a person, which are **unique**

Retinal Scanning

Identifies a person by **analyzing** the layer of blood vessels at the back of their eyes

Iris Scanning

Analyzes the colored part of the eye **suspended** behind the cornea

Vein Structure Recognition

Thickness and location of veins are **analyzed** to identify a person

Face Recognition

Type of **authentication** that uses facial **recognition** to identify or verify a person

Voice Recognition

Type of authentication that uses voice recognition to **identify** or **verify** a person

Types of Authentication: Smart Card Authentication

- Smartcard is a small **computer chip device** that holds a users' personal information required to authenticate them

- Users have to insert their Smartcards into readers and their **Personal Identification Number** (PIN) to authenticate themselves

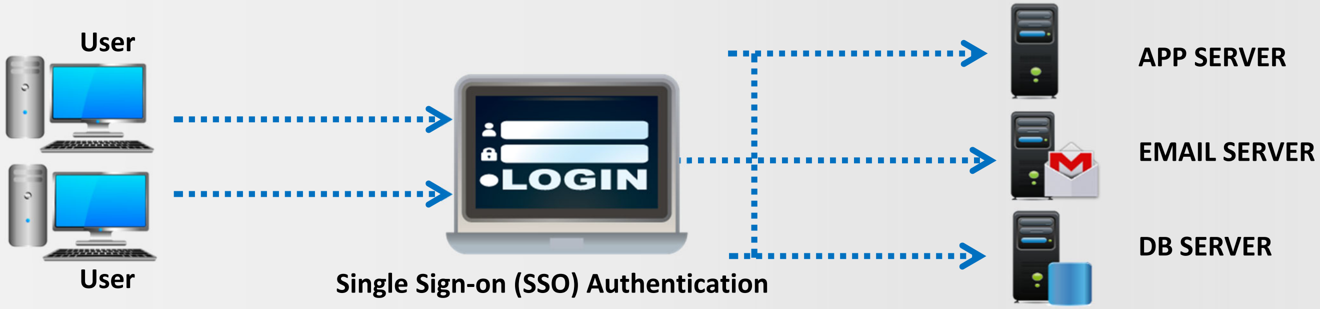
- Smartcard Authentication is a **cryptography-based authentication** and provides stronger security than password authentication

Types of Authentication: Single Sign-on (SSO)

- It allows a user to authenticate themselves to **multiple servers** on a network with **single password** without re-entering it every time

Advantages:

- Don't need to remember passwords of multiple applications or systems
- Reduces the time for entering a username and password
- Reduces the network traffic to the **centralized server**
- Users need to enter credentials only once for multiple applications



Single Sign-on (SSO) Authentication

Types of Authorization Systems

Centralized Authorization

- Authorization for network access is done through **single centralized** authorization unit
- It maintains a **single database** for authorizing all the network resources or applications
- It is an **easy and inexpensive** authorization approach

Implicit Authorization

- Users can access the requested resource **on behalf** of others
- The access request goes through a **primary resource** to access the requested resource

Decentralized Authorization

- Each network resource maintains its **authorization unit** and performs authorization locally
- It maintains its **own database** for authorization

Explicit Authorization

- Unlike Implicit Authorization, it requires **separate authorization** for each requested resource
- It explicitly maintains authorization for each **requested object**

Authorization Principles

Least privilege

- **Assigning** only **limited access** to users or groups for accessing resources of a computer like programs, processes or files to fulfill their job responsibilities
- System administrator is responsible for assigning privileges to **prevent** the **risks** of information security incidents and ~~to~~ achieve better system stability and system security

Separation of duties

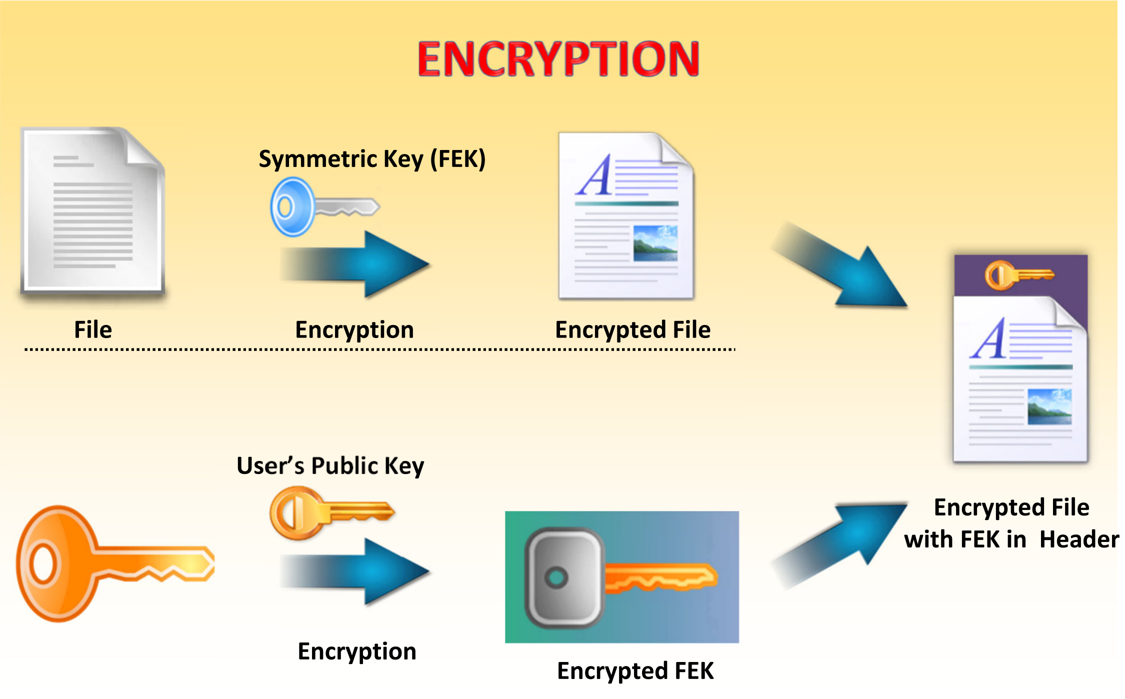
- **Restricting permissions** and privileges to the users by separating the administrator account and the user account
- Individuals or workgroups should not be in a position to control all parts of a **system application**
- Provides security and reduces the risk of loss of confidentiality, integrity, and availability of **enterprise information**

Encryption

- Encryption is a way of **protecting information** by transforming it in such a way that the resulting transformed form is unreadable to an unauthorized party
- To encrypt data, an encryption algorithm uses a **key** to perform a transformation on the data

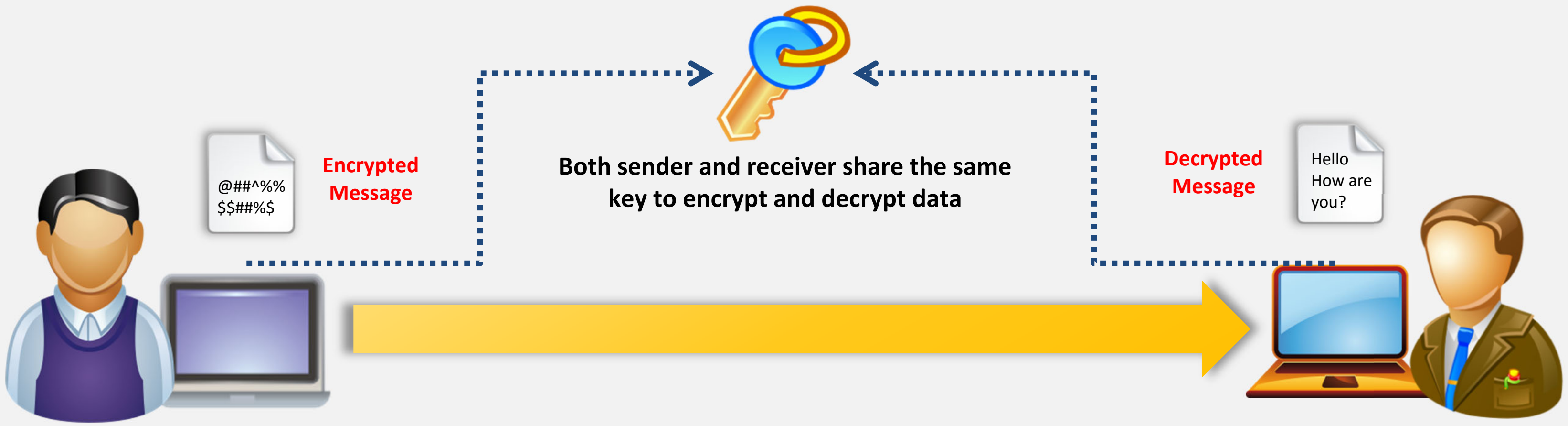
Types of Encryption

- **Symmetric Encryption**
- **Asymmetric Encryption**



Symmetric Encryption

- Symmetric encryption is the oldest cryptographic technique used to **encrypt digital data** in order to **ensure data confidentiality**
- It is called symmetric encryption as a **single key** is used for encrypting and decrypting the data
- It is used to encrypt **large amounts of data**


@##^%%
$$##%$
Encrypted Message
Both sender and receiver share the same key to encrypt and decrypt data
Decrypted Message
Hello
How are
you?

Sender

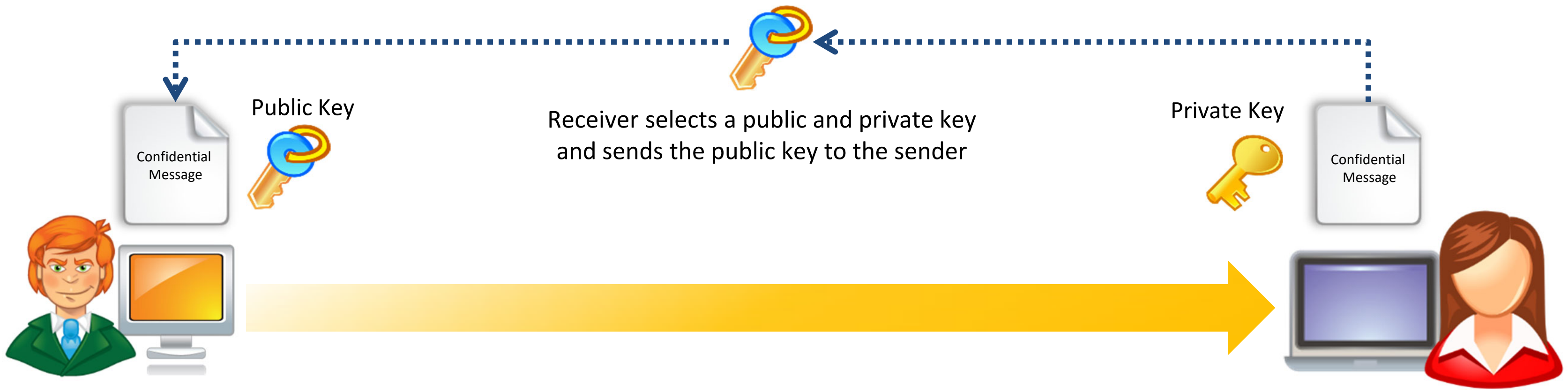
(Sender uses the secret key to encrypt the confidential message and sends it to the receiver)

Receiver

(Receiver decrypts the data using the secret key and reads the confidential message)

Asymmetric Encryption

- Asymmetric encryption, unlike symmetric encryption, **uses two separate keys** to carry out encryption and decryption; one key, called the **public key,** for encrypting messages, and the second key, called the **private key** for decrypting messages
- It is also called **public key encryption** and is used to **encrypt small amounts of data**



Receiver selects a public and private key and sends the public key to the sender

Sender

Sender uses the public key to encrypt the message and sends it to the receiver

Receiver

Receiver decrypts the data using the private key and reads the message

Encryption Algorithms: Data Encryption Standard (DES)

The algorithm is designed to **encipher** and **decipher** blocks of data consisting of **64 bits** under control of a 56-bit key

DES is the **archetypal block cipher** - an algorithm that takes a fixed-length string of plaintext bits and transforms it into a ciphertext bit string of the same length

Due to the **inherent weakness** of DES with today's technologies, some organizations repeat the process three times (3DES) for added strength until they can afford to update their equipment to AES capabilities

Encryption Algorithms: Advanced Encryption Standard (AES)

- AES is a **symmetric-key** algorithm for securing sensitive data but unclassified material by U.S. government agencies

- AES is an **iterated block cipher**, which works by repeating the same operation **multiple** times

- It has a **128-bit** block size, with key sizes of 128, 192, and 256 bits, respectively for AES-128, AES-192, and AES-256

AES Pseudocode

```
Cipher (byte in[4*Nb], byte out[4*Nb], word
w[Nb*(Nr+1)])
begin
  byte state[4,Nb]
  state = in
  AddRoundKey(state, w)
   for round = 1 step 1 to Nr-1
     SubBytes(state)
     ShiftRows(state)
     MixColumns(state)
     AddRoundKey(state, w+round*Nb)
   end for
  SubBytes(state)
  ShiftRows(state)
  AddRoundKey(state, w+Nr*Nb)
  out = state
end
```

Encryption Algorithms: RC4, RC5, RC6 Algorithms

RC4

- A variable key size **symmetric key stream cipher** with byte-oriented operations and is based on the use of a random permutation

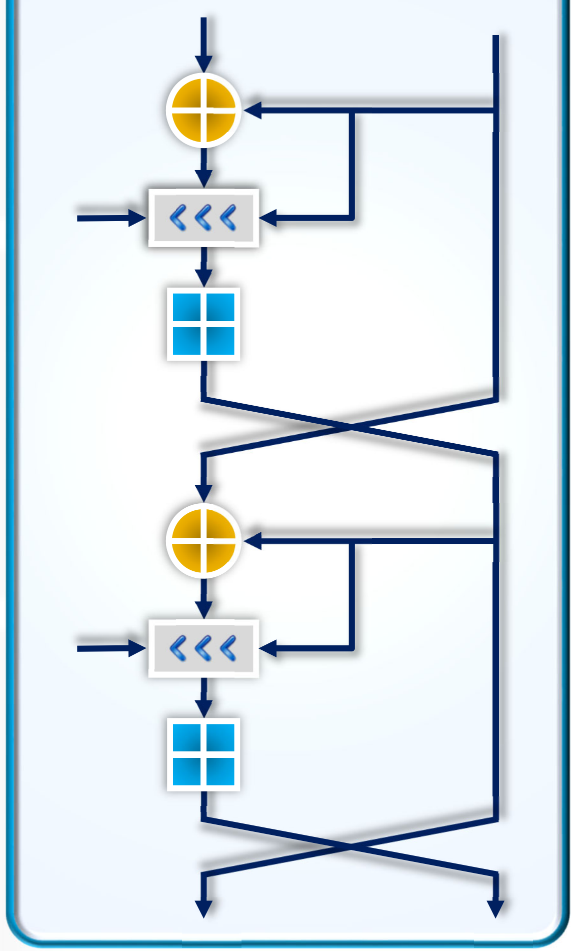
RC5

- It is a **parameterized algorithm** with a variable block size, a variable key size, and a variable number of rounds. The key size is **128-bits**

RC6

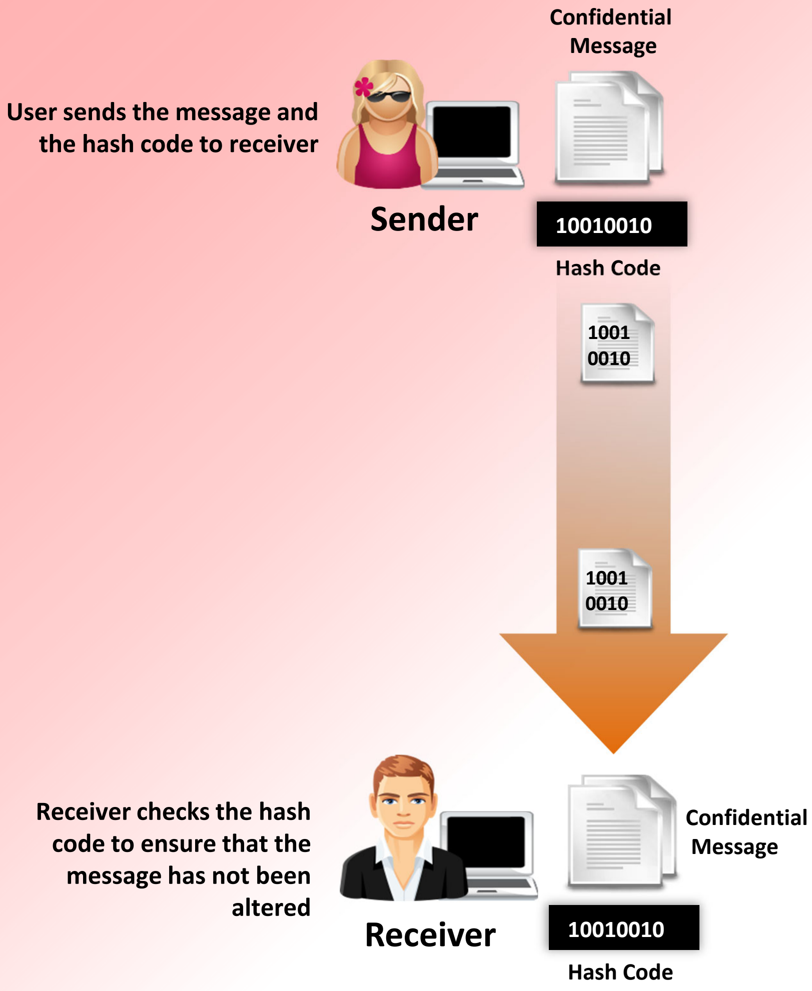
- RC6 is a **symmetric key block cipher** derived from RC5 with two additional features:
  - Uses **Integer multiplication**
  - Uses **four 4-bit working registers** (RC5 uses two 2-bit registers)

RC5 Algorithm



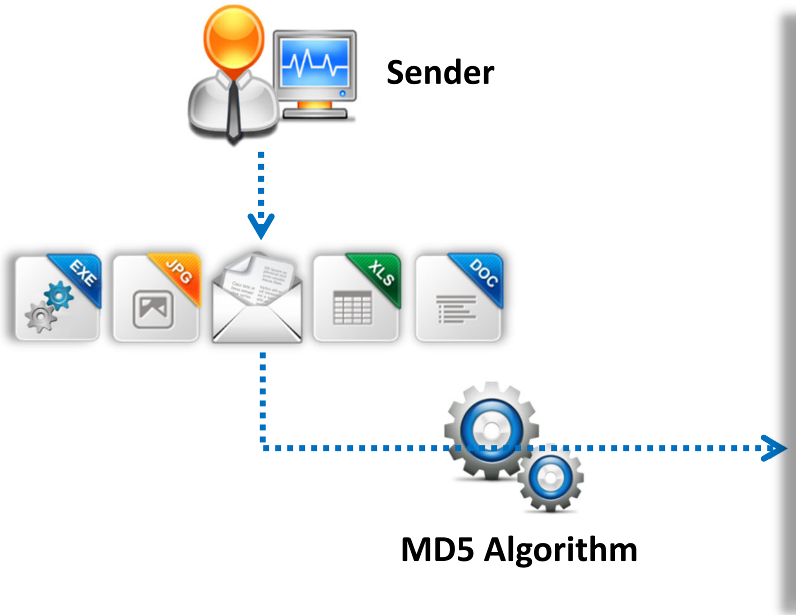
Hashing: Data Integrity

- Hashing is one of the forms of **cryptography** that transforms the information into a **fixed-length value** or key that represents the original information
- Hashing ensures the **security of information** by checking the **integrity of information** on both the sender and receiver sides
- Checking the integrity of information:
  - The sender of the message creates a **hash code** of it and sends the message to the **receiver** along with its **hash code**
  - The receiver again creates a **hash code** for the same messages at the **receiver side** and compares both the hash codes; if it is a match, then the message has not been tampered with

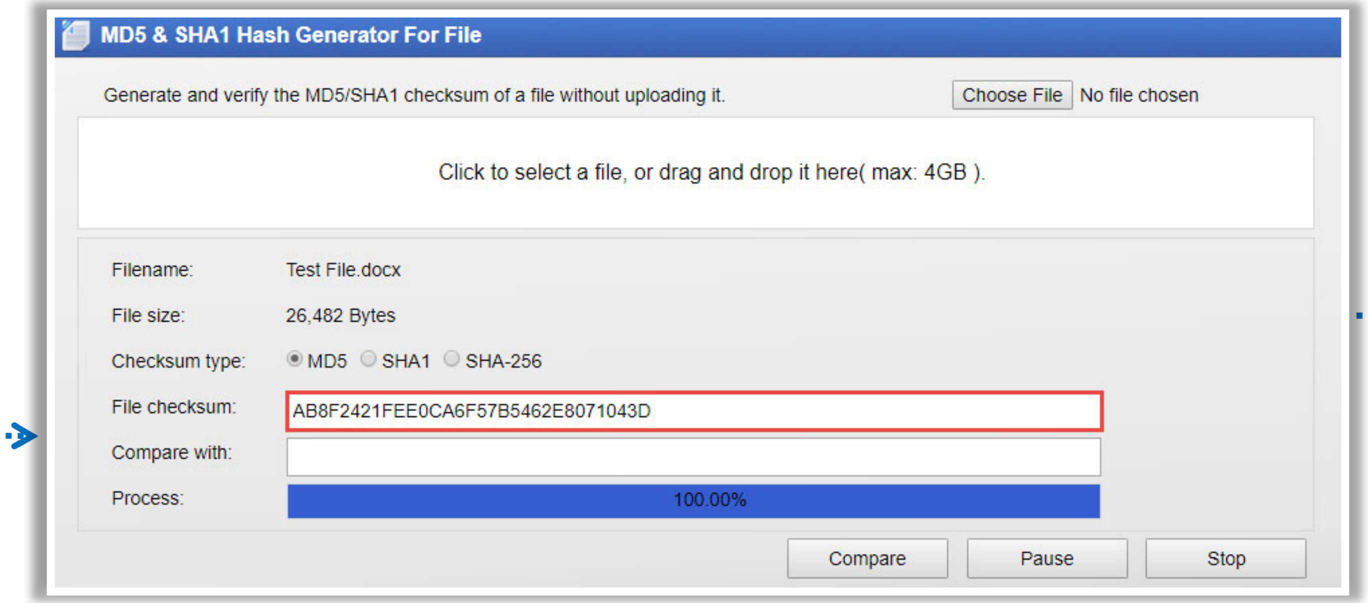

Confidential Message
User sends the message and the hash code to receiver
Sender
10010010
Hash Code
1001 0010
1001 0010
Receiver checks the hash code to ensure that the message has not been altered
Receiver
Confidential Message
10010010
Hash Code

Message Digest Function: MD5

- MD5 algorithm takes a message of **arbitrary length** as input and outputs a **128-bit fingerprint** or message digest of the input
- MD5 is not collision resistant; use of latest algorithms such as **SHA-2** and **SHA-3** is recommended
- It is still deployed for digital signature applications, file integrity checking and storing passwords



MD5 & SHA1 Hash Generator and Verifier



Generate and verify the MD5/SHA1 checksum of a file without uploading it.

No file chosen

Click to select a file, or drag and drop it here(max: 4GB).

Filename: Test File.docx

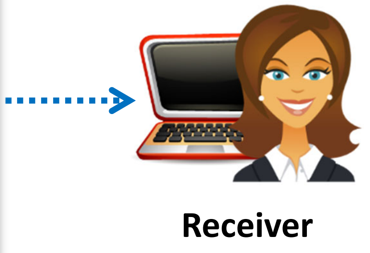
File size: 26,482 Bytes

Checksum type: ● MD5 ○ SHA1 ○ SHA-256

File checksum: AB8F2421FEE0CA6F57B5462E8071043D

Compare with:

Process: 100.00%



Source: *http://onlinemd5.com*

Message Digest Function: Secure Hashing Algorithm (SHA)

It is an algorithm for generating cryptographically secure one-way hash, published by the **National Institute of Standards and Technology** as a **U.S. Federal Information Processing Standard**

SHA1

It produces a **160-bit digest** from a message with a maximum length of **(264 – 1) bits** and resembles the MD5 algorithm

SHA2

It is a family of two similar hash functions, with different block sizes, namely **SHA-256** that uses **32-bit words** and **SHA-512** that uses **64-bit words**

SHA3

SHA-3 uses the **sponge construction** in which message blocks are **XORed** into the initial bits of the state, which is then invertibly permuted

Hash-based Message Authentication Code (HMAC)

1. HMAC is a type of **message authentication code** (MAC) that uses a **cryptographic key** with a combination of a cryptographic hash function

2. It is widely used to verify the **integrity of the data** and **authentication** of a message

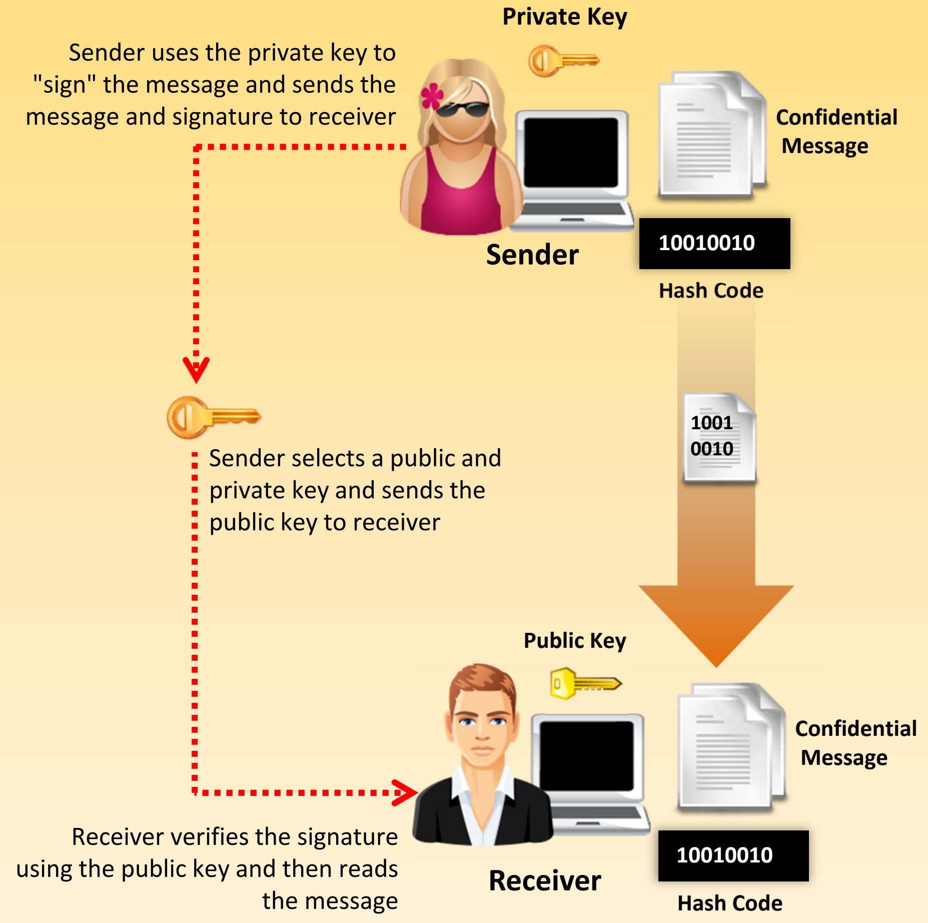
3. This algorithm includes an embedded hash function such as **SHA-1** or **MD5**

4. The strength of the HMAC depends on the **embedded hash function**, key size and the size of the hash output

5. As the HMAC executes the underlying hash function twice, it protects from various **length extension attacks**

Digital Signatures

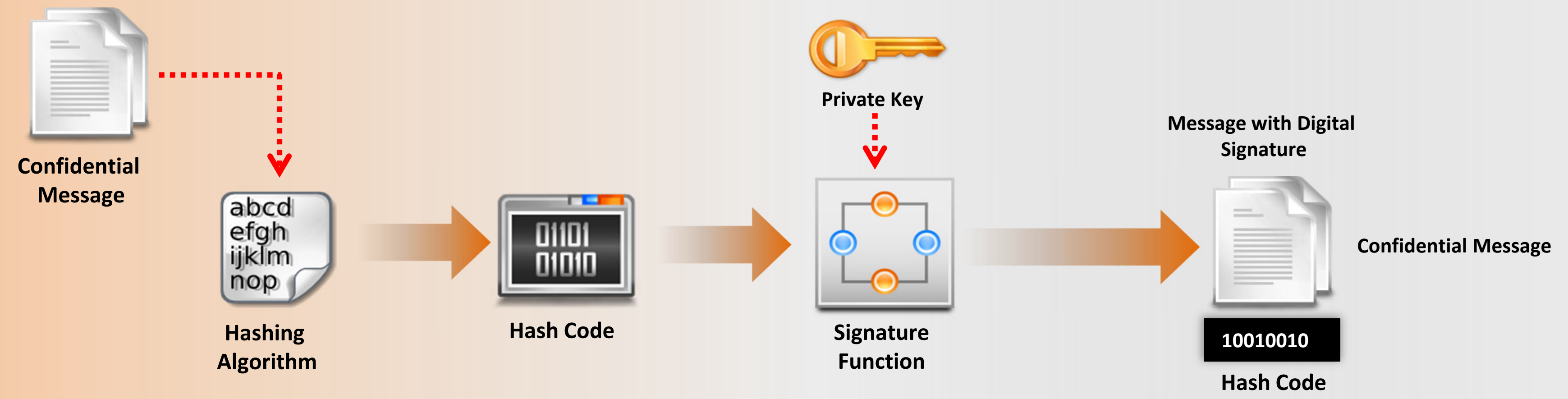
- Digital signatures use the **asymmetric key algorithms** to provide **data integrity**
- A specific signature function is added to the asymmetric algorithm at the sender's side to **digitally sign the message** and a specific **verification function** is added to verify the signature to ensure message integrity at the recipient side
- The asymmetric algorithms that support these two functions are called **digital signature algorithms**
- Digitally signing messages **slows performance**; the hash value of the message is used instead of the message itself for better performance
- A **digital signature** is created using the hash code of the message, the **private key** of the sender, and the signature function
- It is then verified using the hash code of message, the **public key** of sender, and the verification function



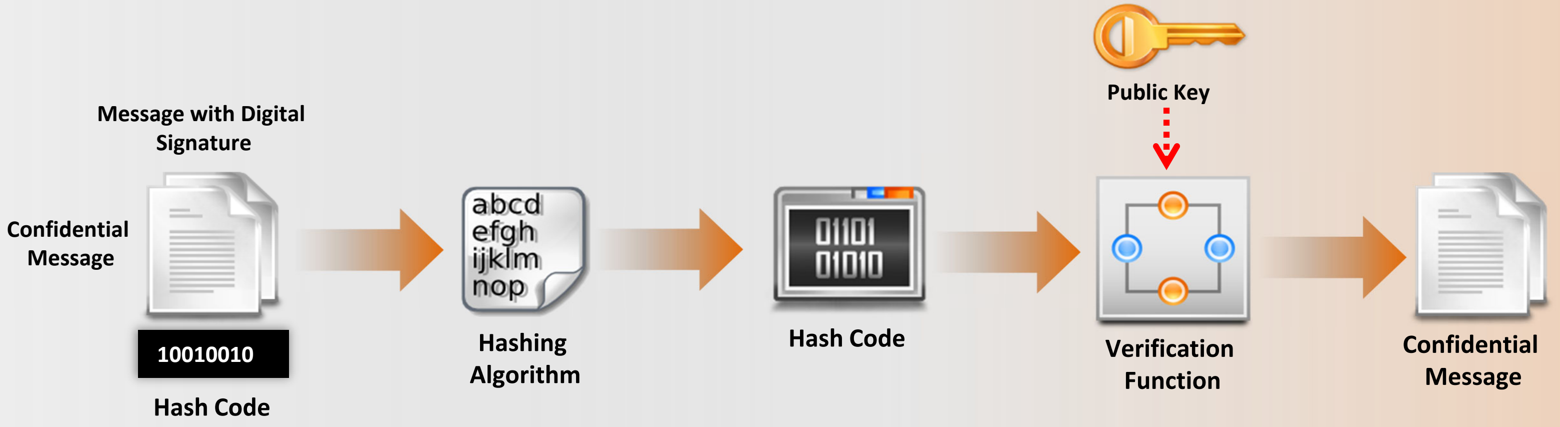
Private Key
Sender uses the private key to "sign" the message and sends the message and signature to receiver
Confidential Message
Sender
10010010
Hash Code
1001
0010
Sender selects a public and private key and sends the public key to receiver
Public Key
Confidential Message
Receiver verifies the signature using the public key and then reads the message
Receiver
10010010
Hash Code

Digital Signatures (Cont'd)

Creating a digital signature at sender side

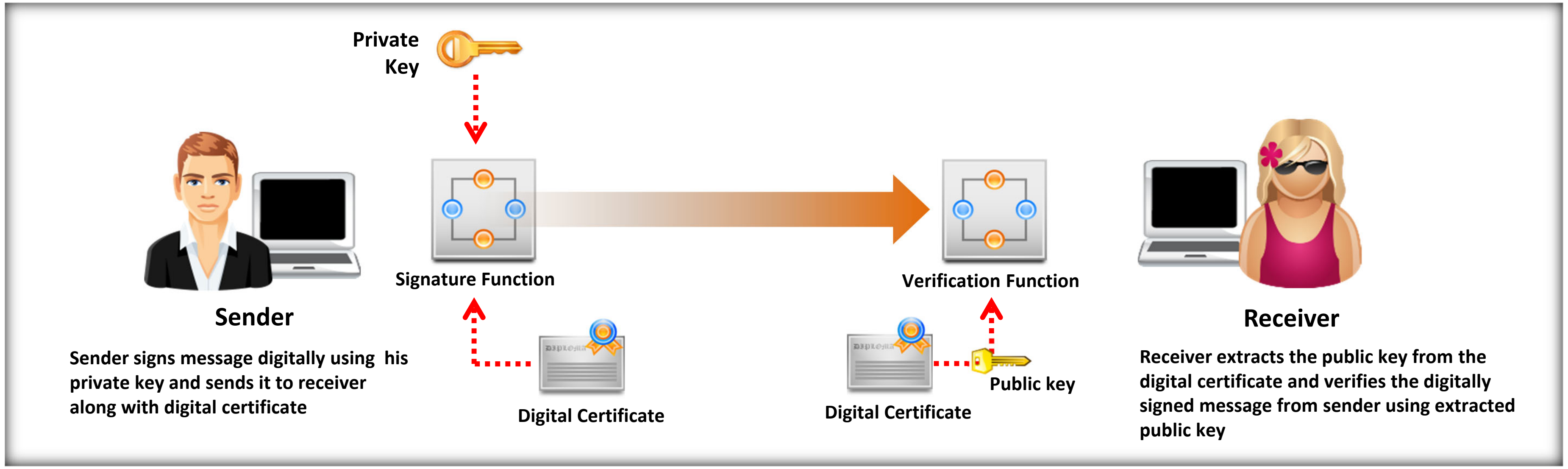


Verifying a digital signature at recipient side



Digital Certificates

- The public key in a digital signature can be transmitted securely by sending it over a **secured channel** like SSL. But if the sender wants to send his public key to **more users**, a number of these secured channels need to be created for each user communication; this process will become quite tedious and unmanageable
- The digital certificates are used to deal with security concerns about **transmitting public keys securely** to the receiver in the digital signature
- The **trusted intermediary solution** is used to secure public keys, where the public key is bound with the name of its owner
- Owners of the public key need to get their public keys certified from the intermediary; the intermediary then issues certificates called **digital certificates** to the owners which they can use to send the public key to a number of users



Sender signs message digitally using his private key and sends it to receiver along with digital certificate

Receiver extracts the public key from the digital certificate and verifies the digitally signed message from sender using extracted public key

Digital Certificates (Cont'd)

Digital Certificate Attributes

Serial number: Represents the unique certificate identity

Subject: Represents the owner of the certificate which may be a person or an organization

Signature algorithm: States the name of algorithm used for creating the signature

Key-usage: Specifies the purpose of the public key, whether it should be used for encryption, signature verification, or both

Public key: Used for encrypting the message or verifying the signature of the owner

Issuer: Provides the identity of the intermediary that issued the certificate

Valid from: Denotes the date from which the certificate is valid

Valid to: Denotes the date till which the certificate is valid

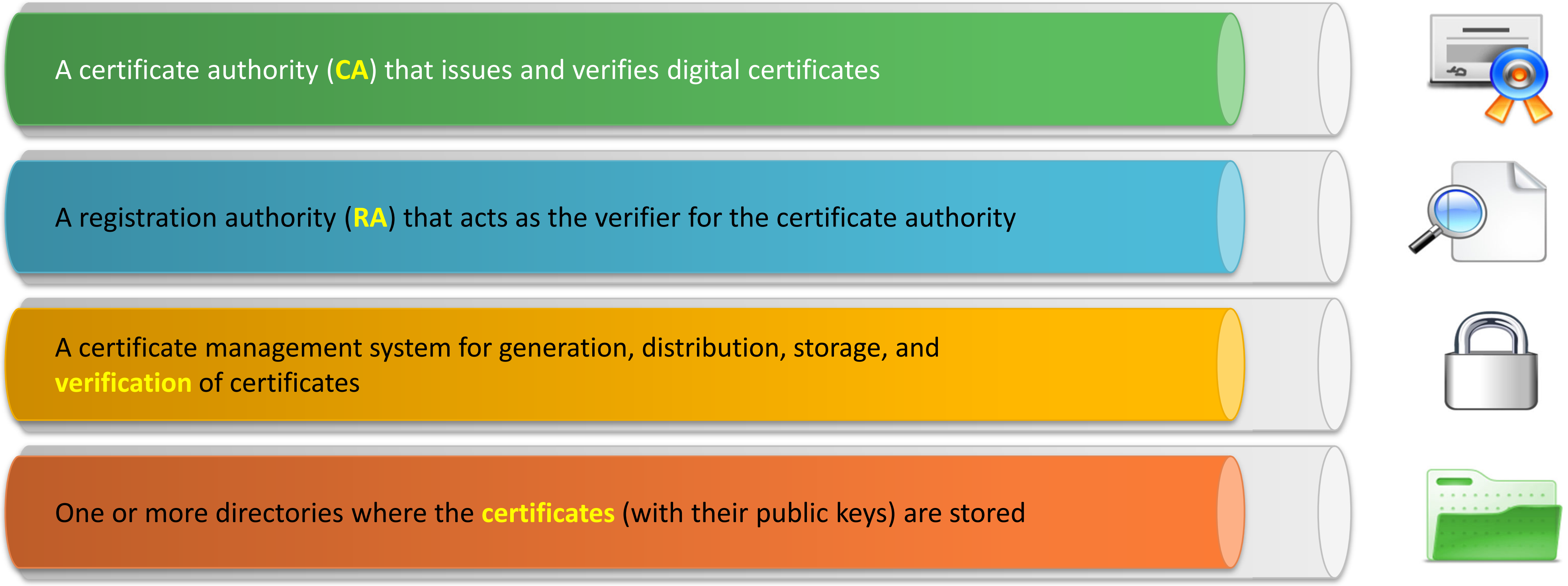
Thumbprint algorithm: Specifies the hashing algorithm used for digital signatures

Thumbprint: Specifies the hash value for the certificate, which is used for verifying the certificate's integrity

Public Key Infrastructure (PKI)

- Public Key Infrastructure (PKI) is a set of hardware, software, people, policies, and procedures required to create, manage, distribute, use, store, and revoke **digital certificates**

Components of PKI



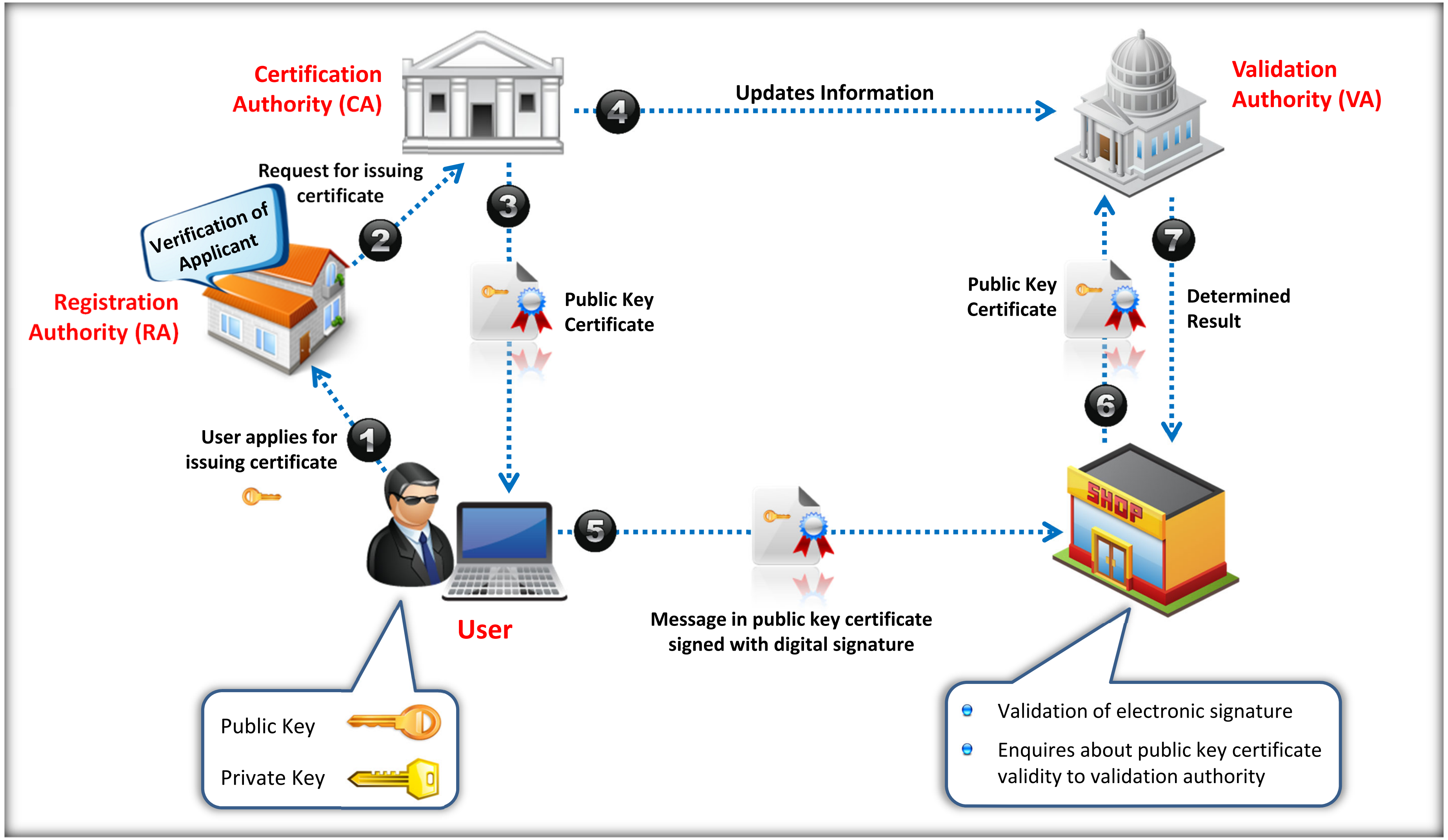
A certificate authority (**CA**) that issues and verifies digital certificates

A registration authority (**RA**) that acts as the verifier for the certificate authority

A certificate management system for generation, distribution, storage, and **verification** of certificates

One or more directories where the **certificates** (with their public keys) are stored

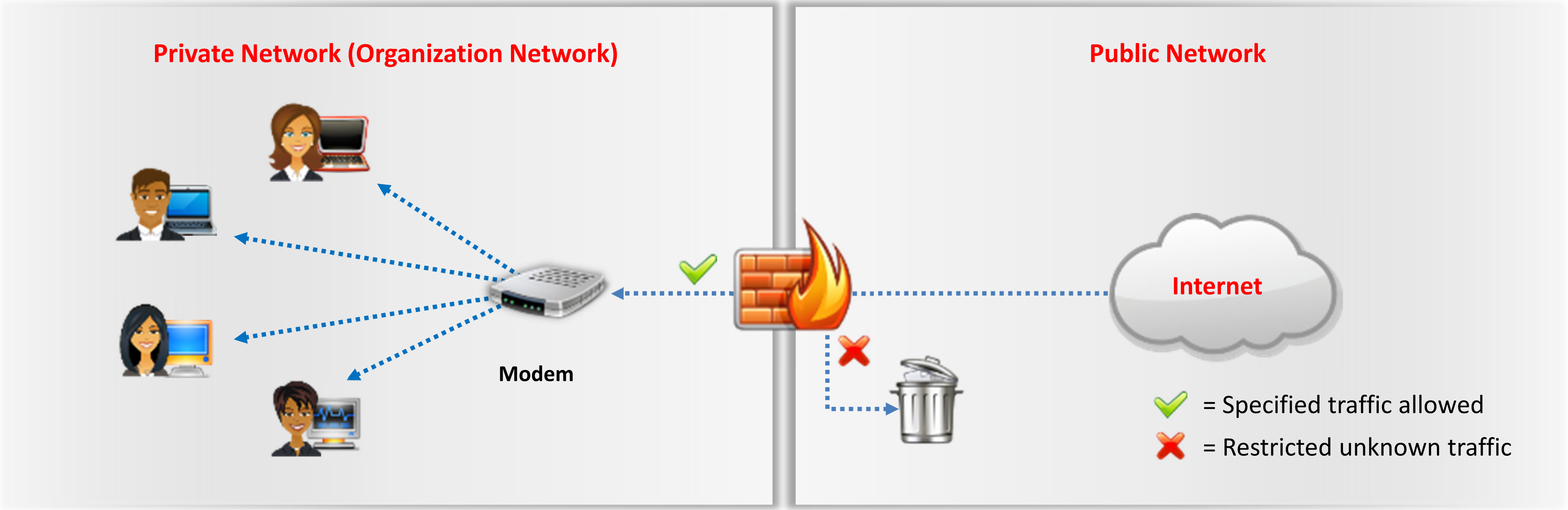
Public Key Infrastructure (PKI) (Cont'd)


Certification Authority (CA)
4
Updates Information
Validation Authority (VA)
Request for issuing certificate
2
Verification of Applicant
3
Registration Authority (RA)
Public Key Certificate
Public Key Certificate
7
Determined Result
6
User applies for issuing certificate
1
5
User
Message in public key certificate signed with digital signature
Public Key
Private Key
Validation of electronic signature
Enquires about public key certificate validity to validation authority

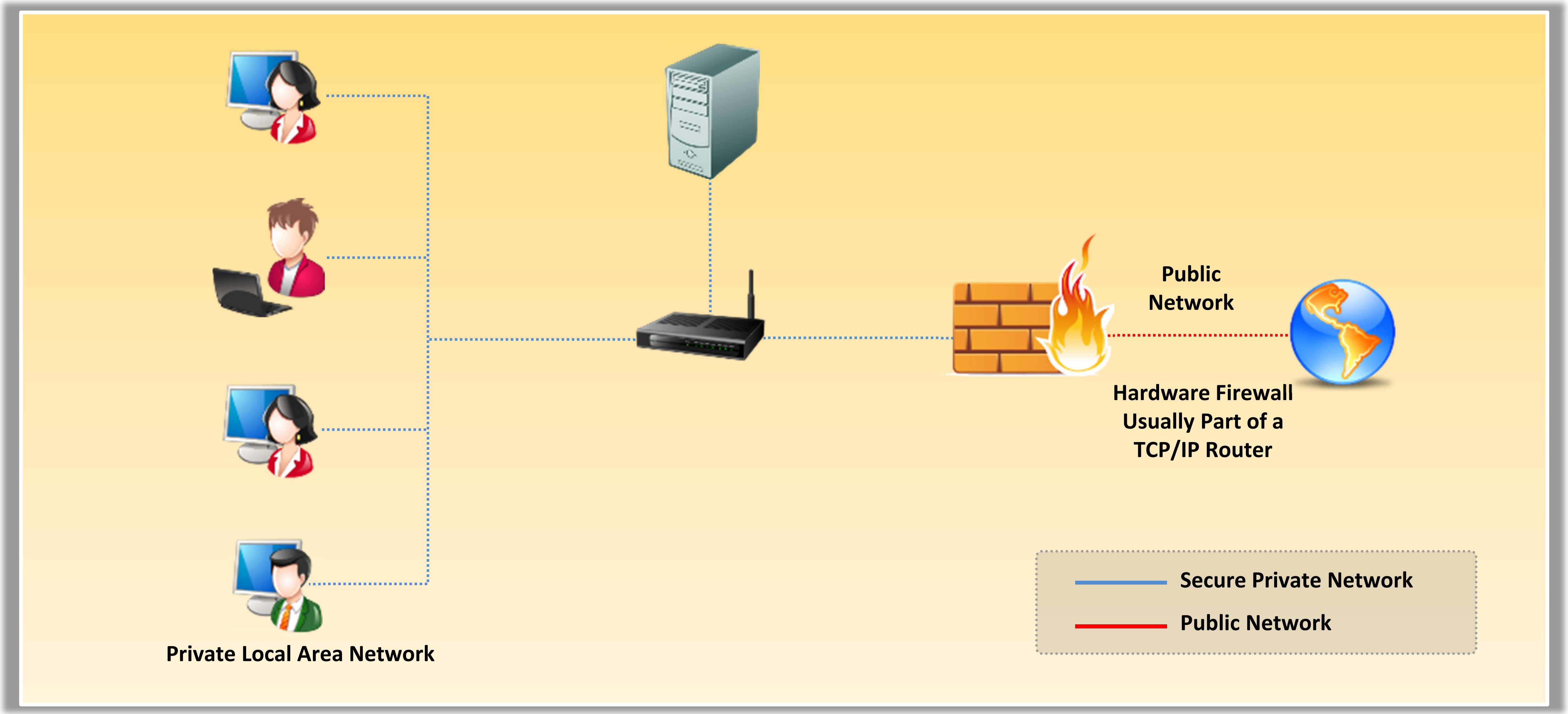
Network Security Devices

What is a Firewall?

- A firewall is a hardware device and/or software that prevents **unauthorized access** to or from a private network
- It is placed at the junction point or gateway between two networks, usually a private network and a public network, such as the Internet or an **untrusted corporate network**
- Firewalls mainly are concerned with the **type of traffic**, or with source or destination addresses and ports, and allow all traffic that meets certain criteria


Private Network (Organization Network)
Public Network
Modem
Internet
✓ = Specified traffic allowed
✗ = Restricted unknown traffic

Hardware Firewall



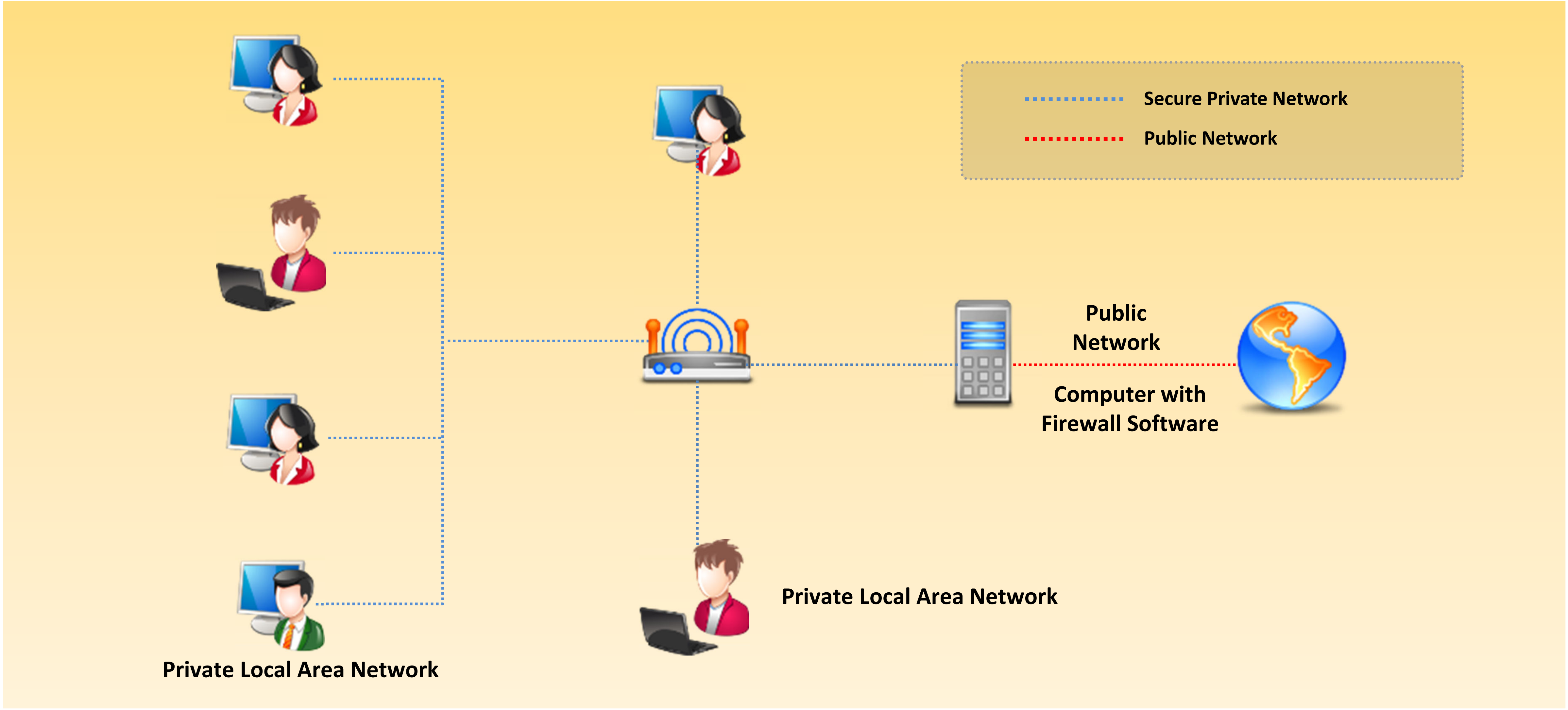
Public Network

Hardware Firewall Usually Part of a TCP/IP Router

Private Local Area Network

🟦	Secure Private Network
🟥	Public Network

Software Firewall


Secure Private Network
Public Network
Public Network
Computer with Firewall Software
Private Local Area Network
Private Local Area Network

What Does a Firewall Do?

1. Examines all traffic routed between two networks to see if it meets certain criteria
2. Routes packets between the networks
3. Filters both inbound and outbound traffic
4. Manages public access to private networked resources, such as host applications
5. Logs all attempts to enter the private network and triggers alarms when hostile or unauthorized entry is attempted

What Can't a Firewall Do?

A firewall cannot prevent individual users with modems from dialing into or out of the network, bypassing the firewall altogether

Employee misconduct or carelessness cannot be controlled by firewalls

Policies involving the use and misuse of passwords and user accounts must be strictly enforced

Types of Firewalls

Types of Firewalls

Packet Filtering Firewalls

- Packet filtering firewalls work at the network level of the OSI model (or the IP layer of TCP/IP)
- Each packet is compared to a set of criteria before it is forwarded
- The advantage of packet filtering firewalls is their low cost and low impact on network performance

Circuit Level Gateways

- Circuit level gateways work at the session layer of the OSI model or the TCP layer of TCP/IP
- They monitor TCP handshaking between packets to determine whether a requested session is legitimate
- Circuit level gateways are relatively inexpensive

Application Level Gateways

- Application level gateways (also called proxies) work at the **application layer** of the OSI model
- Incoming or outgoing packets cannot access **services** for which there is no proxy
- In plain terms, an application level gateway that is configured to be a **web proxy** will not allow through any FTP, gopher, Telnet, or other traffic

Stateful Multilayer Inspection Firewalls

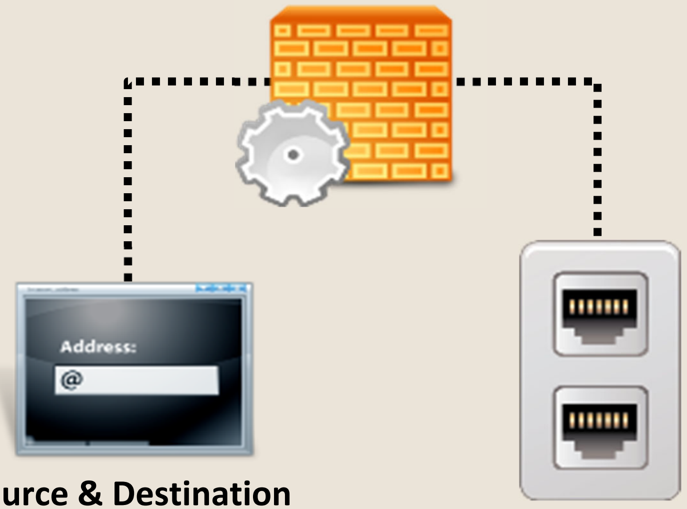
- Stateful multilayer inspection firewalls combine the aspects of the other **three types of firewalls**
- They filter packets at the network layer determine whether **session packets** are legitimate and evaluate the contents of packets at the application layer
- They are expensive and require **competent personnel** to administer them

Note: The type of criteria used to determine whether traffic should be allowed through varies from one type of firewall to another

Packet Filtering

Address Filtering

- Firewalls can filter packets based on their source and destination addresses and port numbers



Source & Destination Address

Ports

Network Filtering

- Firewalls can also filter specific types of network traffic
- The decision to forward or reject traffic is dependent upon the protocol used, e.g., HTTP, FTP, or Telnet
- Firewalls can also filter traffic by packet attribute or state

Firewall Policy

Build a firewall that handles **application traffic** like web, email, or Telnet

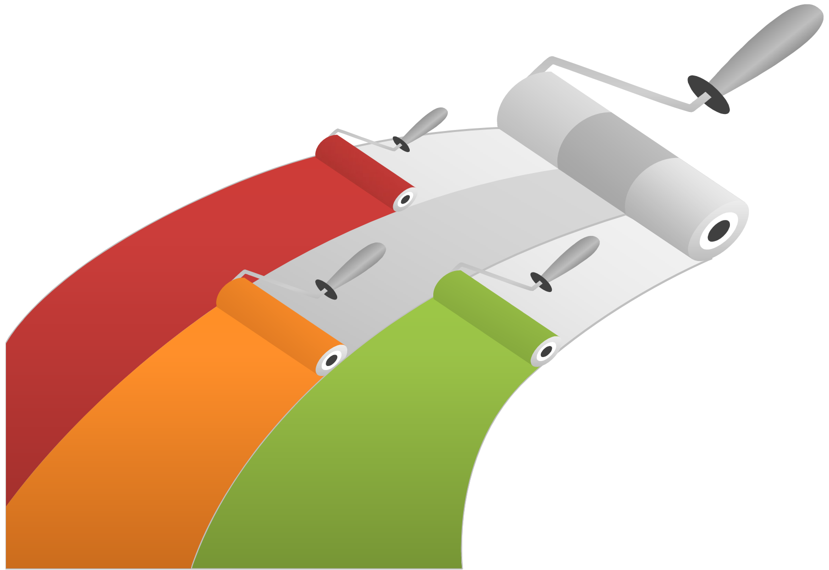
The policy should explain how the firewall is to be updated and managed

The steps involved in creating a **firewall policy** are as follows:

- **Step1**: Identify the **network applications** that are of utmost importance
- **Step2**: Identify the **vulnerabilities** that are related to the network applications
- **Step3**: Prepare a **cost-benefit analysis** to secure the network applications
- **Step4**: Create a **network application traffic matrix** to identify the protection method
- **Step5**: Create a **firewall ruleset** that depends on the application’s traffic matrix

Periodic Review of Information Security Policies

- Create periodic reviews for **information security policies** to achieve **accuracy** and **timeliness**
- Review and update information **security policies** every six months
- If a firewall's application is upgraded, then the firewall's ruleset must be formally changed
- Firewall installations, along with systems and other resources, should be **audited** on a **regular basis**



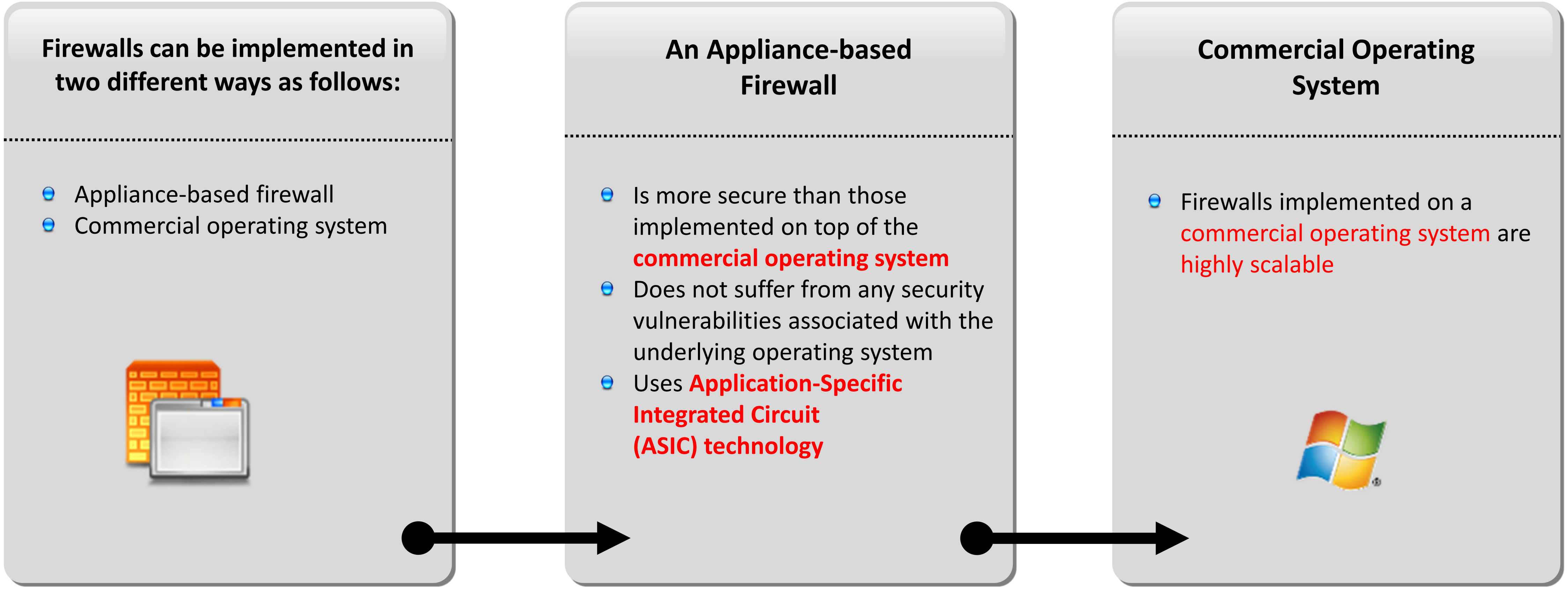
Periodic reviews should include:

I. Actual audits and vulnerability assessments of production

II. Backup infrastructure components

III. Computer systems

Firewall Implementation



Firewalls can be implemented in two different ways as follows:

- Appliance-based firewall
- Commercial operating system

An Appliance-based Firewall

- Is more secure than those implemented on top of the **commercial operating system**
- Does not suffer from any security vulnerabilities associated with the underlying operating system
- Uses **Application-Specific Integrated Circuit (ASIC) technology**

Commercial Operating System

- Firewalls implemented on a commercial operating system are highly scalable

Build a Firewall Ruleset

Most firewall platforms use **rulesets** as their common system for implementing **security controls**

The contents of the firewall ruleset establish the **functionality** of the firewall

- Based on the **firewall's platform architecture**, firewall rulesets contain the following information:
  - Source address of the packet
  - Destination address of the packet
  - Type of traffic

Egress Filtering and its Importance

Egress filtering:

- **Egress filtering** monitors and controls the flow of information transferred from one network to another
- Routers, firewall or similar edge device examines the TCP/IP packets that are being sent out of the internal network
- The packets are not permitted to leave if it can't fulfill the security rules. It means -they are denied "egress“

Importance of Egress Filtering:

- It does not allow the transfer of unwanted traffic out to the Internet
- It also prevents information leaks due to misconfiguration, as well as some network mapping attempts
- Moreover, it also restricts internal systems from performing outbound IP spoofing attacks

Risks associated with Outbound Connections:

- Loss of employee productivity
- Litigation
- Bandwidth abuse
- Data exfiltration

Ingress Filtering and its Importance

- Ingress filtering technique ensures that incoming packets are actually coming from the networks from which they are required to come
- It does not allow attack packets to enter into the protected network
- It applies the rules in order
- It rejects known fallacious source addresses
  - Private addresses
    - 10.*.*.*
    - 172.16.*.* to 172.31.*.*,
    - 192.168.*.*
  - Internal Address Ranges
  - Other obvious or known common addresses
    - 1.2.3.4, 0.0.0.0, 0.0.0.1, etc.

- It rejects known TCP vulnerabilities
  - Syn flood (TCP SYN=1 AND FIN=1)
  - FTP (TCP destination port = 20)
    - Supervisory control connection (TCP destination port = 21)
  - Telnet (TCP destination port = 23)
  - NetBIOS (TCP destination port = 135 through 139)
  - UNIX rlogin (TCP destination port = 513)
  - UNIX rsh launch shell without login (TCP port 514)

Firewall Rulebase Review

A firewall rulebase review consists of:

- Review rulebase for firewall rulebase standards documents
- Review rulebase against any permitted connections that do not follow the firewall policy
- Review rulebase for security practices
- Review rulebase against integrity
- Review rulebase for account logging
- Examine firewall objects that group several networks, hosts or ports
- Verify entries defining “ANY” as source, destination, port or protocol
- Review rulebase against undue complexity that disturbs the firewall and the performance of the firewall administrators
- Review rulebase against duplication~~,~~ that disturbs the firewall and the performance of the firewall administrators
- Review rulebase against conflicting rules that influence the firewall capacity to work appropriately

Maintenance and Management of Firewall

- The two mechanisms used by **commercial firewall platforms** for configuring and maintenance are:
  - Command Line Interface (**CLI**) configuration
  - Graphical User Interface (**GUI**) configuration

- For **web-based interfaces**, security is provided through Secure Socket Layer (**SSL**) encryption, along with user ID and password

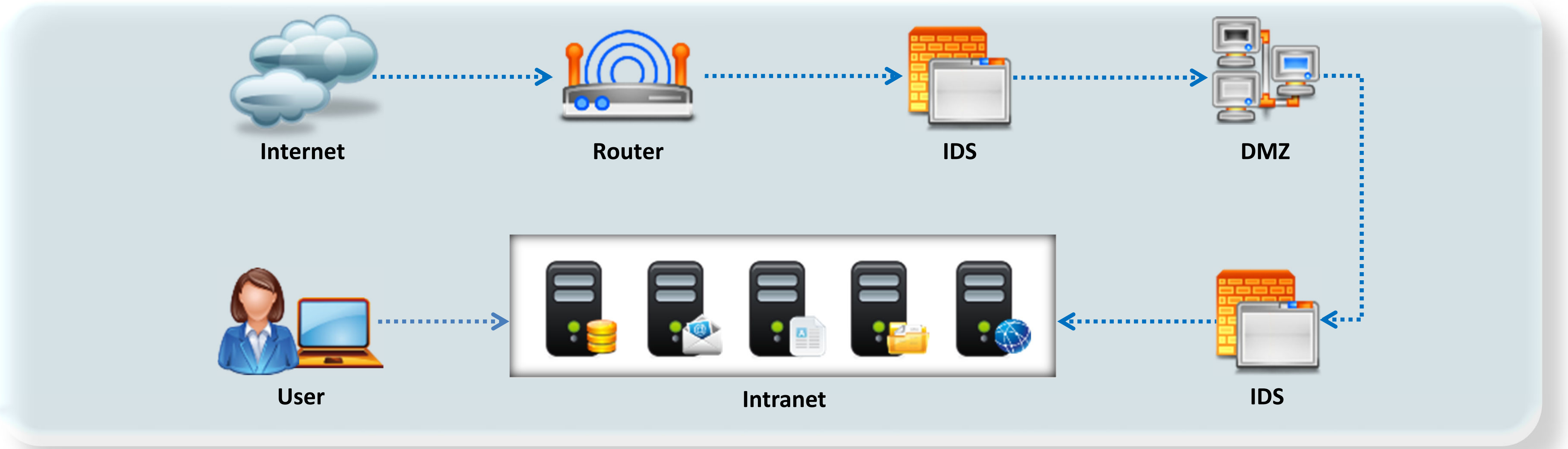
- For **non-web interfaces**, security is implemented through **custom transport encryption**

- In order to perform these monitoring mechanisms, organizations must establish effective **incident response procedures**

- **Maintenance** and **management** of firewall allows organization to:
  - Monitor the firewall for suspicious activities
  - Detect intrusion attempts

Introduction to Intrusion Detection System (IDS)

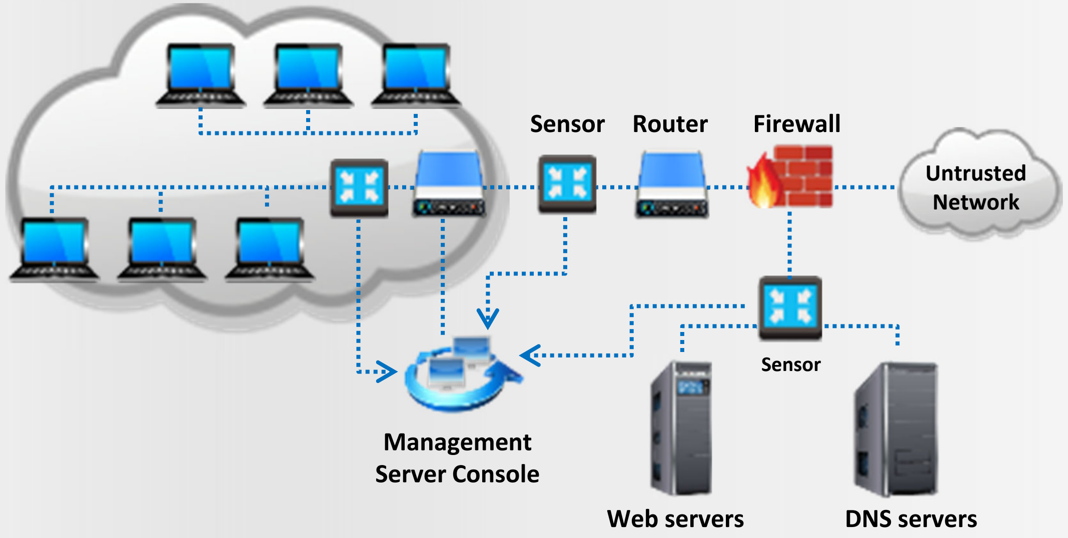
- An Intrusion Detection System (IDS) is **security software** or **hardware device** used to monitor, detect, and protect networks or system from malicious activities, and alerts the concern security personnel immediately upon detecting intrusions
- It inspects all inbound and outbound **network traffic** for **suspicious patterns** that may indicate a network or system security breach



Types of Intrusion Detection Systems

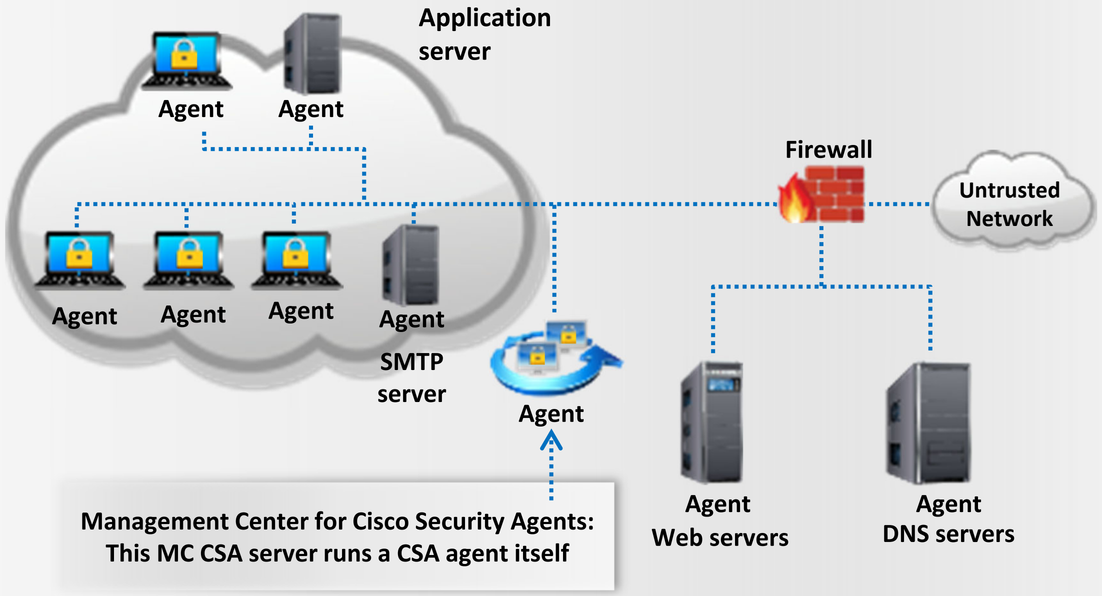
Network-Based Intrusion Detection Systems (NIDS)

- A network-based IDS detects malicious activity such as Denial-of-Service attacks, port scans, or even attempts to crack into computers by monitoring network traffic
- It consist of a black box that is placed on the network in promiscuous mode, listening for patterns indicative of an intrusion



Host-Based Intrusion Detection Systems (HIDS)

- A host-based IDS monitors individual hosts on the network for malicious activity (e.g. Cisco Security Agent)
- These mechanisms usually include auditing for events that occur on a specific host



Application-based IDS

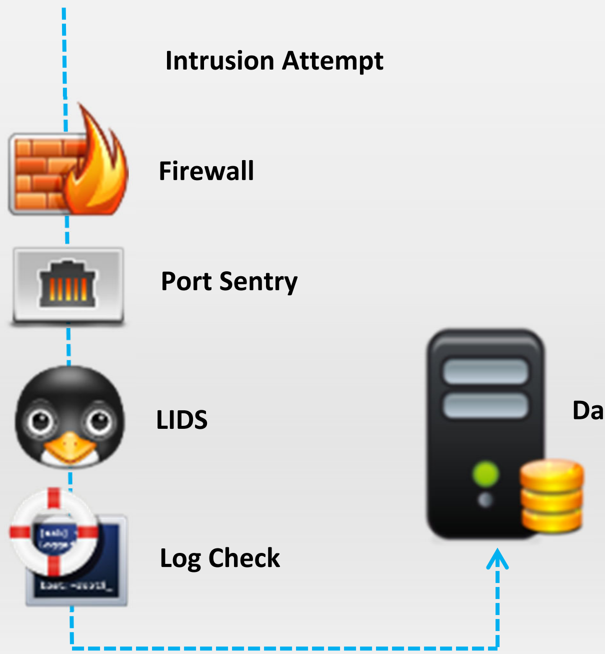
An application-based IDS is like a host-based IDS designed to monitor a specific application (similar to anti-virus software designed specifically to monitor your mail server)

An application-based IDS is extremely accurate in detecting malicious activity for the applications it protects

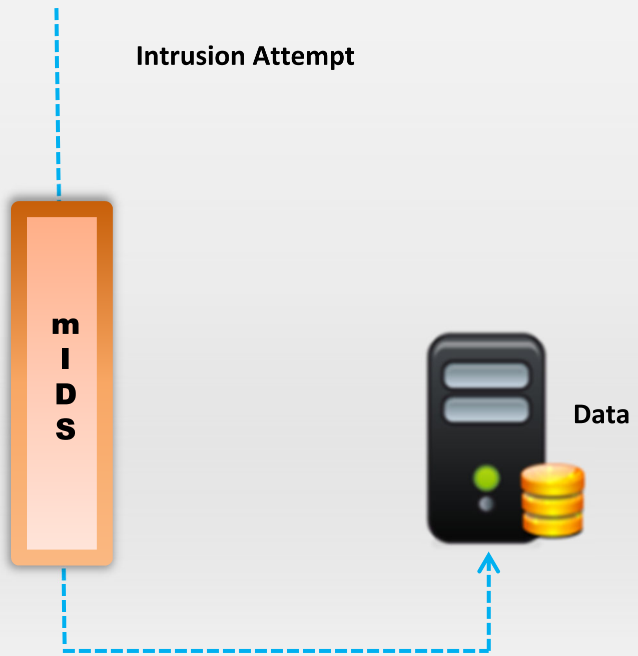
Multi-Layer Intrusion Detection Systems (mIDS)

- An mIDS integrates many layers of IDS technologies into a **single monitoring** and **analysis engine**
- It aggregates integrity monitoring software logs, **system logs**, IDS logs, and **firewall logs** into a single monitoring and analysis source

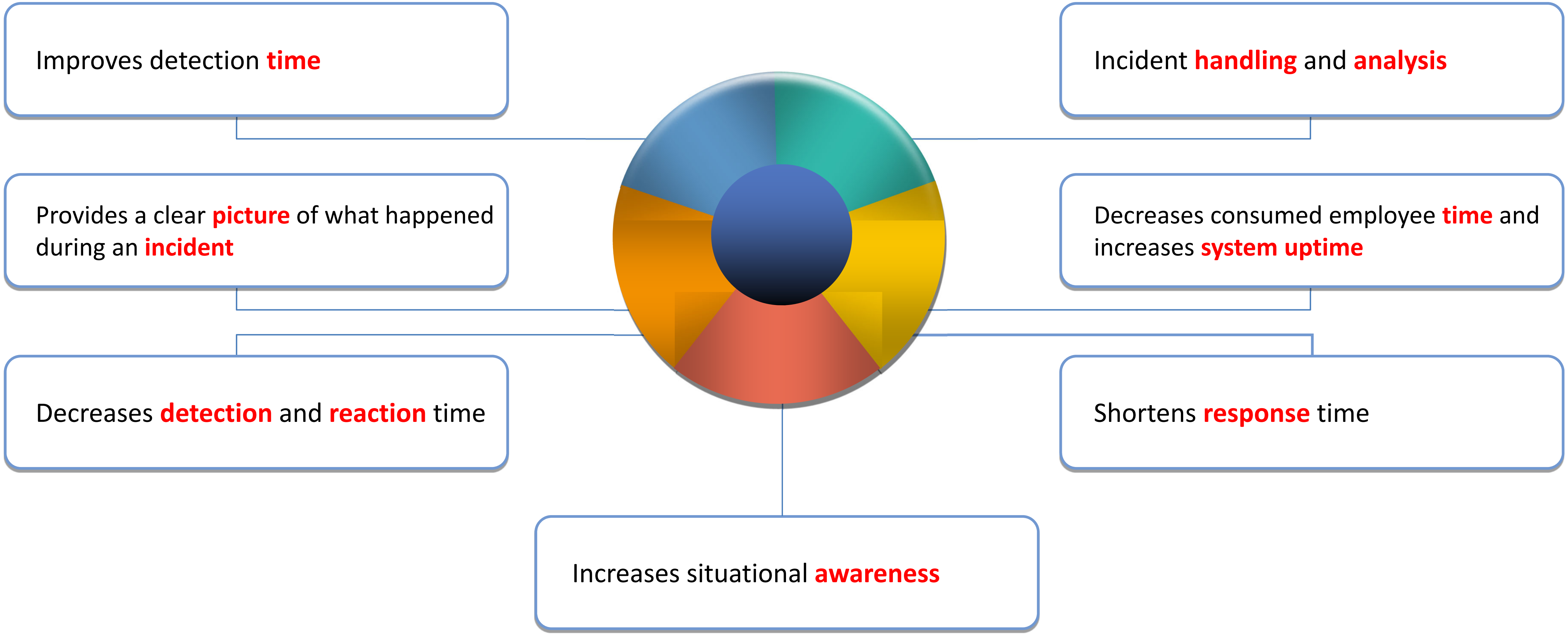
A Multi-Layer Approach to System Security



mIDS Security System



Multi-Layer Intrusion Detection System Benefits



Improves detection **time**

Provides a clear **picture** of what happened during an **incident**

Decreases **detection** and **reaction** time

Incident **handling** and **analysis**

Decreases consumed employee **time** and increases **system uptime**

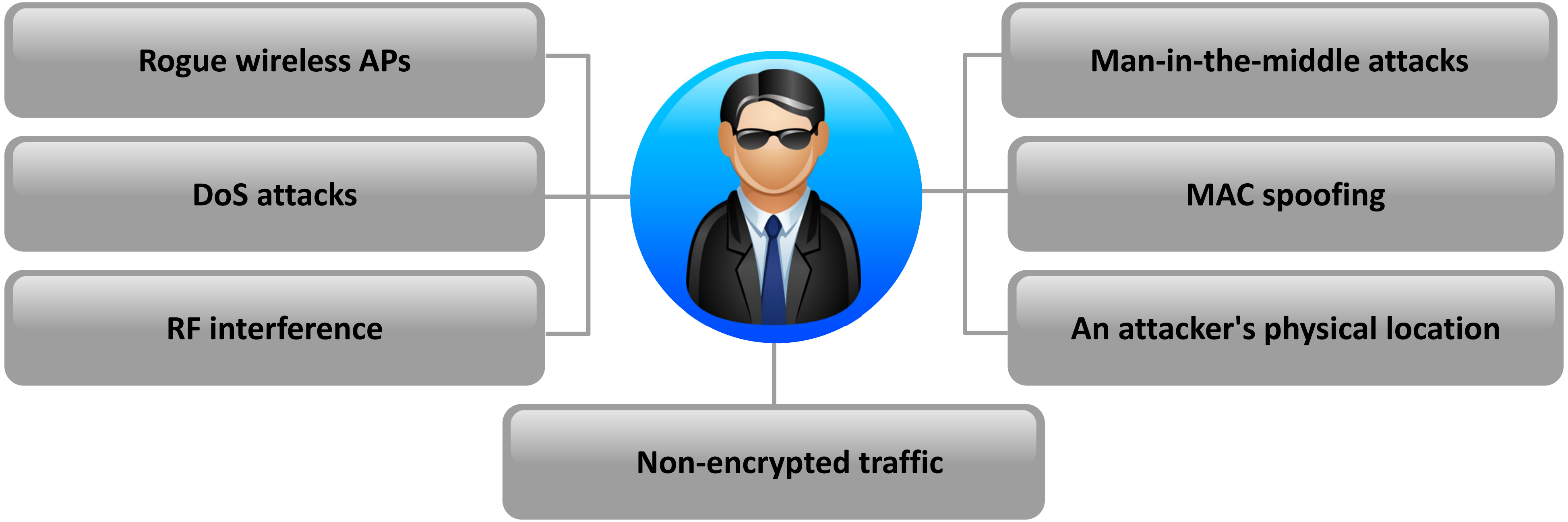
Shortens **response** time

Increases situational **awareness**

Wireless Intrusion Detection Systems (WIDSs)

- WIDSs monitor and evaluate user and **system activities**, identify known attacks, determine abnormal **network activity**, and detect **policy violations** for WLANs
- Check for potential **weaknesses** that damage the WLAN security

A WIDS detects:



Rogue wireless APs

DoS attacks

RF interference

Man-in-the-middle attacks

MAC spoofing

An attacker's physical location

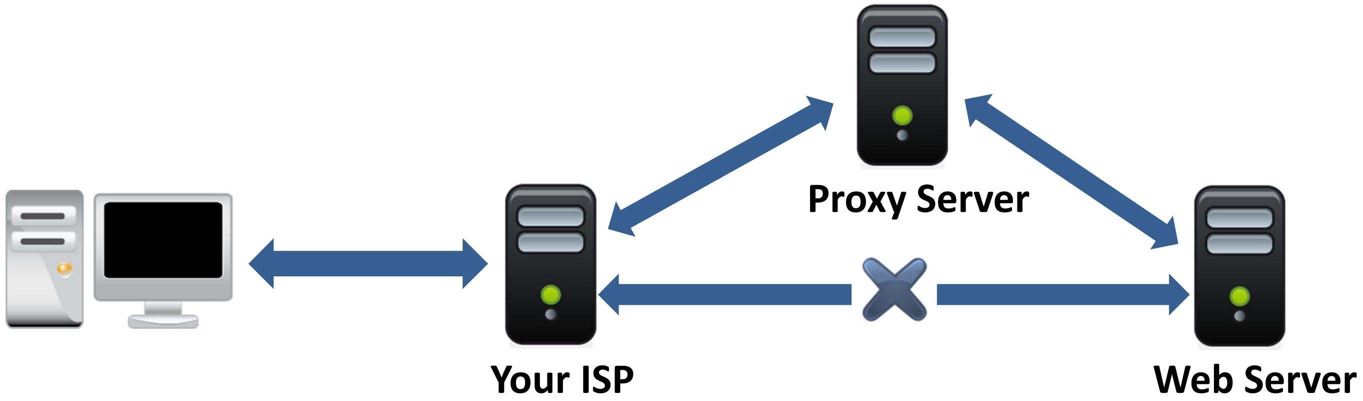
Non-encrypted traffic

Common Techniques Used to Evade IDS Systems

- Try the pattern matching approach to identify potential attacks within the exploit code
- Use the Unicode Evasion method, which allows for viewing files on the IIS server
- Search for the central log server's IP address and crash the system using a DoS attack
- Send specially crafted packets in order to trigger alerts and breed a large number of false reports
- Flood the network with noise traffic to exhaust its resources examining risk-free traffic

Proxy Server

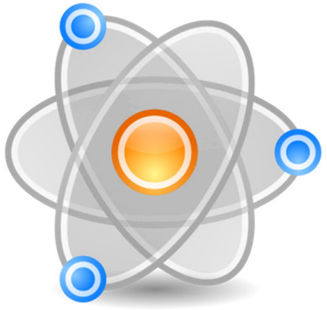
- Proxy are intermediary servers that sits between the client and the server
- It is used intercept incoming and outgoing requests from the client browser
- Attackers and Pen testers generally use proxies to inspect and modify the HTTP request and responses

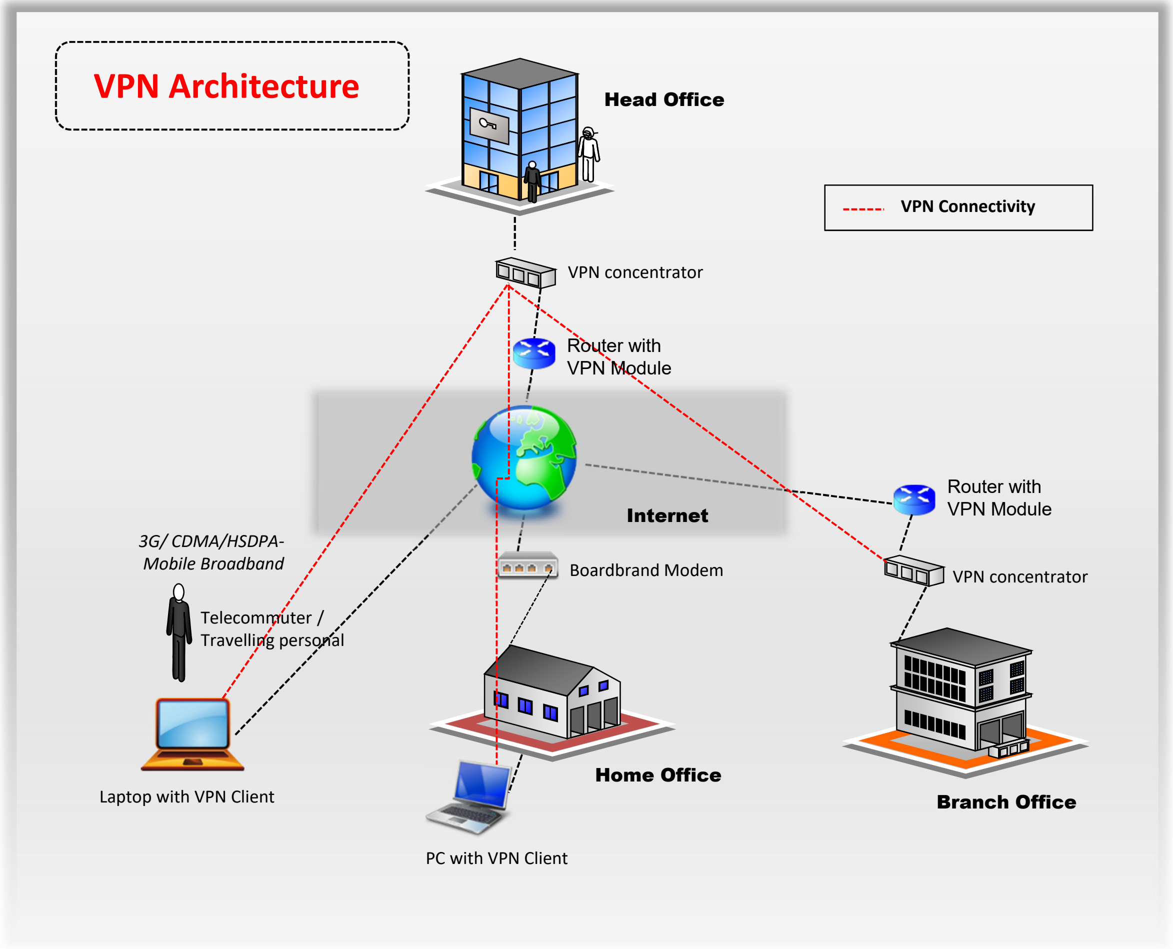


Virtual Private Network (VPN)

- A VPN is used to **securely communicate** with different computers over insecure channels

- A VPN uses the Internet and ensures secure communication to distant offices or users within their **enterprise's network**





VPN Security

- VPNs provide security by the use of **tunneling protocols** and through security procedures such as encryption

Encryption

- Encryption in VPN ensures data **integrity** and **privacy**
- It allows only **authorized** users to see the **confidential** information

Most Widely used VPN protocols:

IP security (IPSec)	**Group of various correlated protocols, present in network layer of the OSI model** **Used for encryption in correlation with L2TP tunneling protocol**
Layer 2 Tunneling Protocol (L2TP)/IPsec	**Chiefly employed in Cisco products, present in data link layer of the OSI model**
Secure Sockets Layer (SSL)	**SSL is a VPN accessible via https over web browser** **SSL VPNs restrict user access to specific applications**
Point-to-Point Tunneling Protocol (PPTP)	**Supports validation of the information and encryption of data**
Secure Shell (SSH)	**SSH creates both the VPN tunnel and the encryption that protects it**

VPN Security (Cont'd)

IPsec Server

- The IPsec server provides **advanced security** features such as better encryption algorithms and more comprehensive authentication
- **IPsec server contains two encryption modes:**
  - Tunnel mode encrypts the **header** and **payload** of each packet
  - Transport mode encrypts the only **payload**

AAA Server

- The AAA server is used in a **remote-access** VPN environment for more secure access
- When a request comes from a **dial-up client** to establish a session, then the request is proxied to the AAA server
- **This server checks the following:**
  - Who you are (authentication)
  - What you are allowed to do (authorization)
  - What you actually do (accounting)

Windows Security

Patch Management

Patch Management ensures that appropriate and **updated patches** are installed on the system

Patches are the small programs, which apply a fix to a specific type of vulnerability

It involves applying patches, Service Packs and/or **upgrading Windows** to a newer version

Service Packs can fix vulnerabilities along with some functionality improvements

Use Patch Management tools to identify the **missing patches** and install them on the system

Version upgrades fix vulnerabilities and come with improved security features

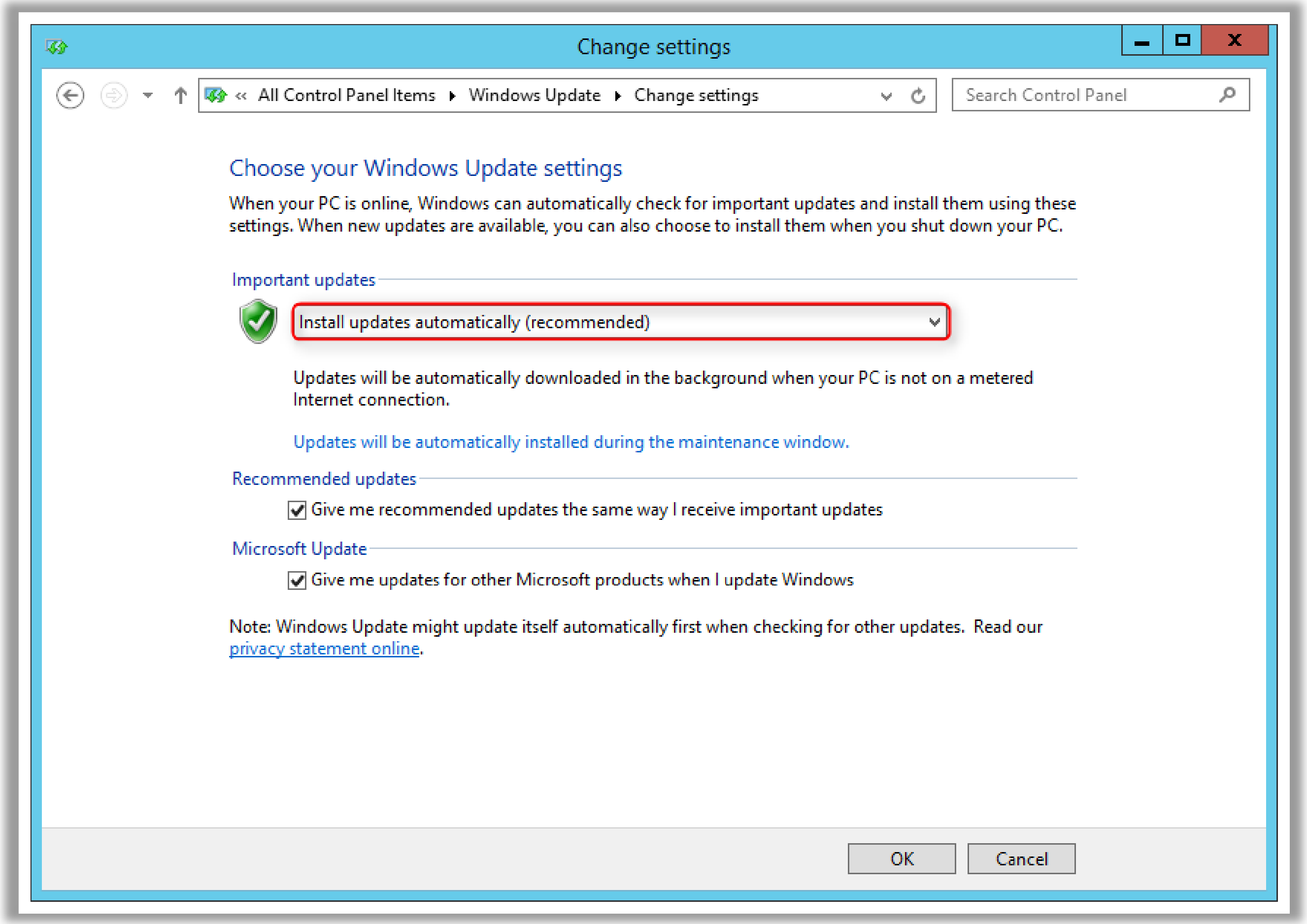
- **Patch Management Activities:**
  - Choosing, verifying, testing and applying patches
  - **Updating** previous version of patches to current ones
  - **Recording** repositories or depots of patches for easy selection
  - **Assigning** and deploying applied patches

Configuring an Update Method for Installing Patches

- Go to **Start** → **Control Panel** → **System** and click **Windows Updates** and select option **Install update automatically**
- You can also use a **third-party Windows update tool** for remote-desktop patch management

Advantages of automated patching

- You can **force updates** to install by specific date
- Computers not on the Internet can receive updates
- Users **cannot disable** or circumvent updates



Change settings
« All Control Panel Items ▸ Windows Update ▸ Change settings
Search Control Panel

Choose your Windows Update settings

When your PC is online, Windows can automatically check for important updates and install them using these settings. When new updates are available, you can also choose to install them when you shut down your PC.

Important updates

Install updates automatically (recommended)

Updates will be automatically downloaded in the background when your PC is not on a metered Internet connection.

Updates will be automatically installed during the maintenance window.

Recommended updates

☑ Give me recommended updates the same way I receive important updates

Microsoft Update

☑ Give me updates for other Microsoft products when I update Windows

Note: Windows Update might update itself automatically first when checking for other updates. Read our privacy statement online.

System Management Server : SMS

- SMS is managing and servicing solution to manage networked Windows XP Embedded-based devices alongside Windows desktop, Windows server, and other Windows Mobile systems
- SMS has its own database that stores Software and Hardware inventories

SMS Administration and System diagnostics:

SMS enables the N/w Administrator to handle H/w and S/w inventory stored in SMS Database

SMS also enables the N/w Administrator to handle software distribution and installation over network

Diagnostics tests for PCs over network are also enabled for the Administrator

Microsoft Software Update Services : SUS

- SUS provide Critical updates and security updates for windows such as Microsoft windows 2000 server, Windows 2000 Professional, and Windows XP and Windows Server 2003

SUS Functional work:

Critical updates for Server side

Critical updates for client side

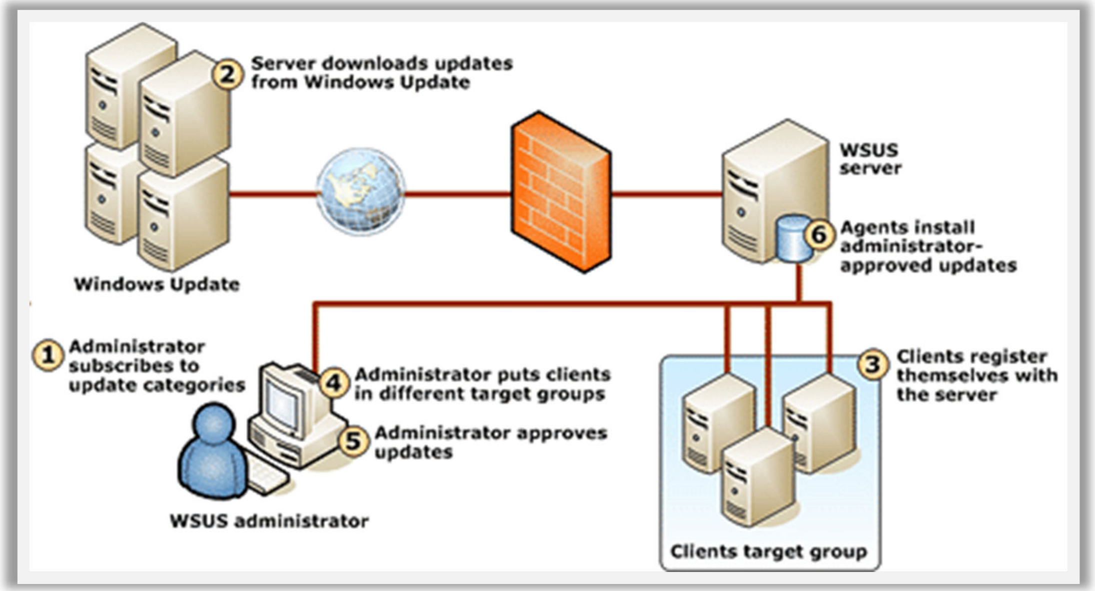
Deploy Security Patches

Dynamic Notification for Critical Updates.

Windows Software Update Services : WSUS

- WSUS Provide:
  - Automatic Download Updates
  - Hotfixes
  - Service packs
  - Device Drivers

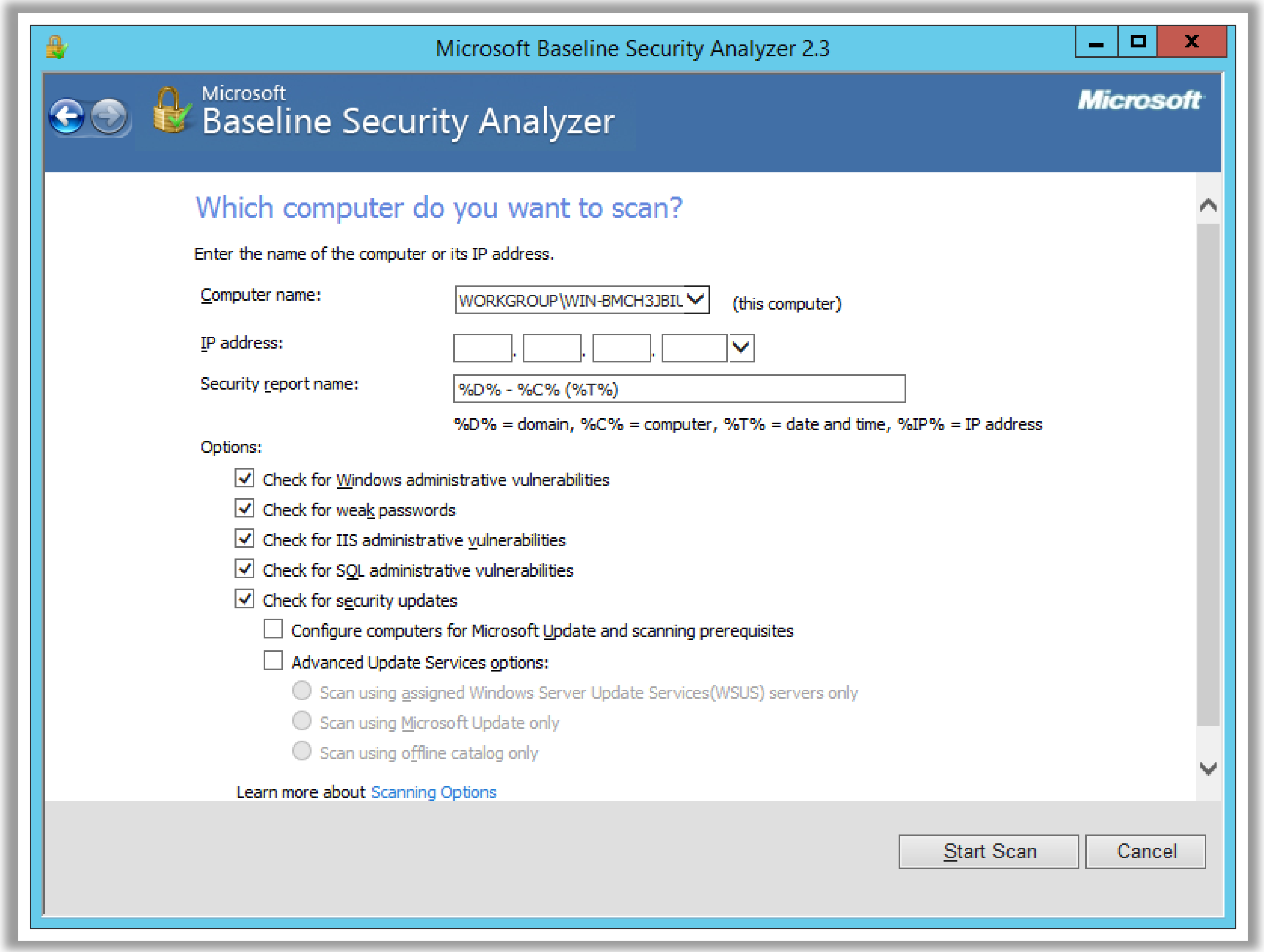
- WSUS Operations:
  - Update Packages from Microsoft Repository
  - Approve or Decline Updates before release
  - Enables the administrator to control for update, or install software, drivers by WSUS


2 Server downloads updates from Windows Update
Windows Update
WSUS server
6 Agents install administrator-approved updates
1 Administrator subscribes to update categories
4 Administrator puts clients in different target groups
5 Administrator approves updates
WSUS administrator
3 Clients register themselves with the server
Clients target group

Microsoft Baseline Security Analyzer (MBSA)

- The Microsoft Baseline Security Analyzer provides a **streamlined method** to identify the missing security updates and common security misconfigurations of a Windows OS

- It performs **local or remote scans** of Microsoft Windows systems



Microsoft Baseline Security Analyzer 2.3

Microsoft
Baseline Security Analyzer

Microsoft

Which computer do you want to scan?

Enter the name of the computer or its IP address.

Computer name: WORKGROUP\WIN-BMCH3JBIL (this computer)

IP address: . . .

Security report name: %D% - %C% (%T%)

%D% = domain, %C% = computer, %T% = date and time, %IP% = IP address

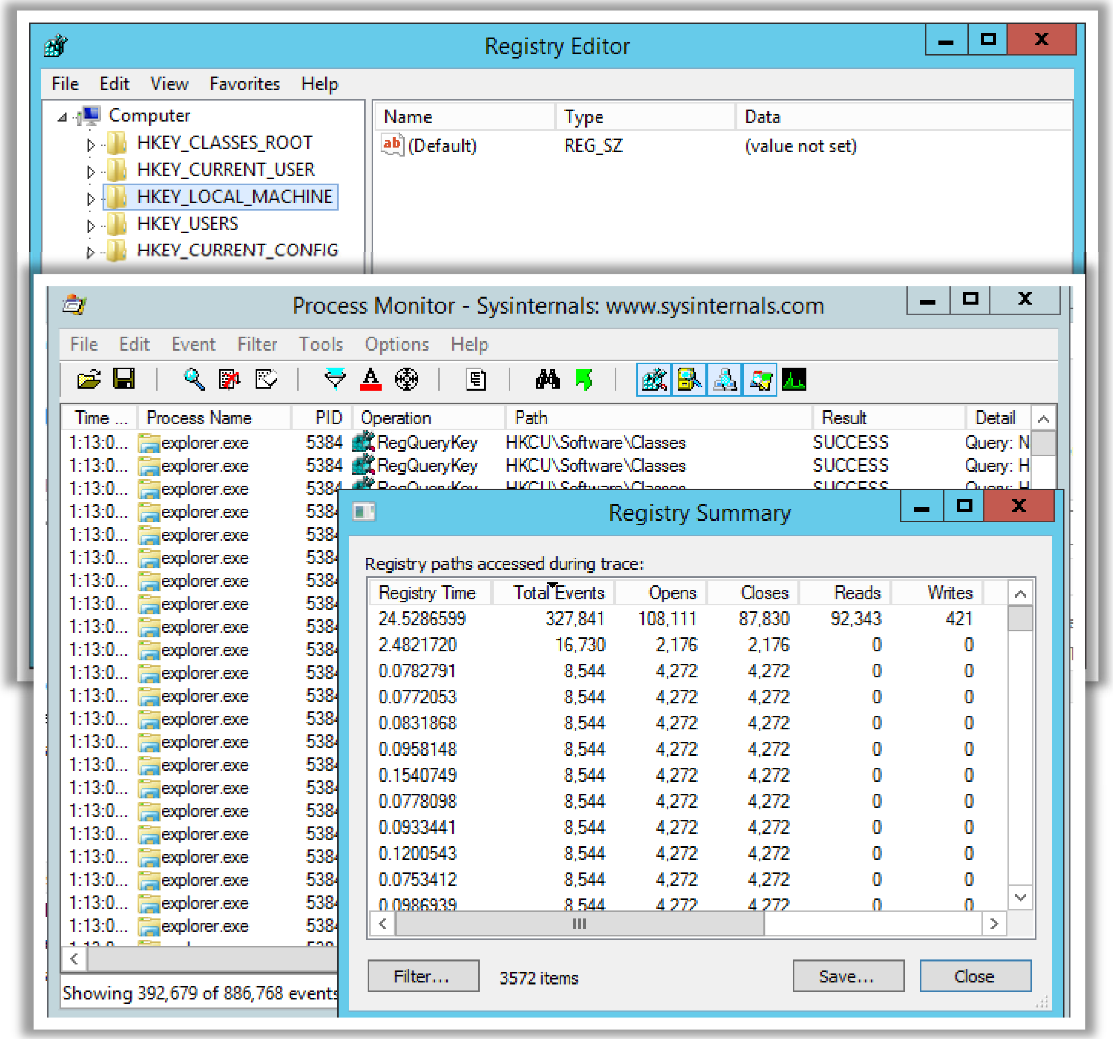
Options:

☑ Check for Windows administrative vulnerabilities
☑ Check for weak passwords
☑ Check for IIS administrative vulnerabilities
☑ Check for SQL administrative vulnerabilities
☑ Check for security updates
□ Configure computers for Microsoft Update and scanning prerequisites
□ Advanced Update Services options:
○ Scan using assigned Windows Server Update Services(WSUS) servers only
○ Scan using Microsoft Update only
○ Scan using offline catalog only

Learn more about Scanning Options

Source: *https://www.microsoft.com*

Windows Registry



Registry Editor
File Edit View Favorites Help
Computer
HKEY_CLASSES_ROOT
HKEY_CURRENT_USER
HKEY_LOCAL_MACHINE
HKEY_USERS
HKEY_CURRENT_CONFIG

Name	Type	Data
(Default)	REG_SZ	(value not set)

Process Monitor - Sysinternals: www.sysinternals.com
File Edit Event Filter Tools Options Help

Time ...	Process Name	PID	Operation	Path	Result	Detail
1:13:0...	explorer.exe	5384	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: N
1:13:0...	explorer.exe	5384	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: H
1:13:0...	explorer.exe	5384	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: H
1:13:0...	explorer.exe	538				
1:13:0...	explorer.exe	538				
1:13:0...	explorer.exe	538				
1:13:0...	explorer.exe	538				
1:13:0...	explorer.exe	538				
1:13:0...	explorer.exe	538				
1:13:0...	explorer.exe	538				
1:13:0...	explorer.exe	538				
1:13:0...	explorer.exe	538				
1:13:0...	explorer.exe	538				
1:13:0...	explorer.exe	538				
1:13:0...	explorer.exe	538				
1:13:0...	explorer.exe	538				
1:13:0...	explorer.exe	538				
1:13:0...	explorer.exe	538				
1:13:0...	explorer.exe	538				
1:13:0...	explorer.exe	538				
1:13:0...	explorer.exe	538				
1:13:0...	explorer.exe	538				

Showing 392,679 of 886,768 events

Registry paths accessed during trace:

Registry Time	Total Events	Opens	Closes	Reads	Writes
24.5286599	327,841	108,111	87,830	92,343	421
2.4821720	16,730	2,176	2,176	0	0
0.0782791	8,544	4,272	4,272	0	0
0.0772053	8,544	4,272	4,272	0	0
0.0831868	8,544	4,272	4,272	0	0
0.0958148	8,544	4,272	4,272	0	0
0.1540749	8,544	4,272	4,272	0	0
0.0778098	8,544	4,272	4,272	0	0
0.0933441	8,544	4,272	4,272	0	0
0.1200543	8,544	4,272	4,272	0	0
0.0753412	8,544	4,272	4,272	0	0
0.0986939	8,544	4,272	4,272	0	0

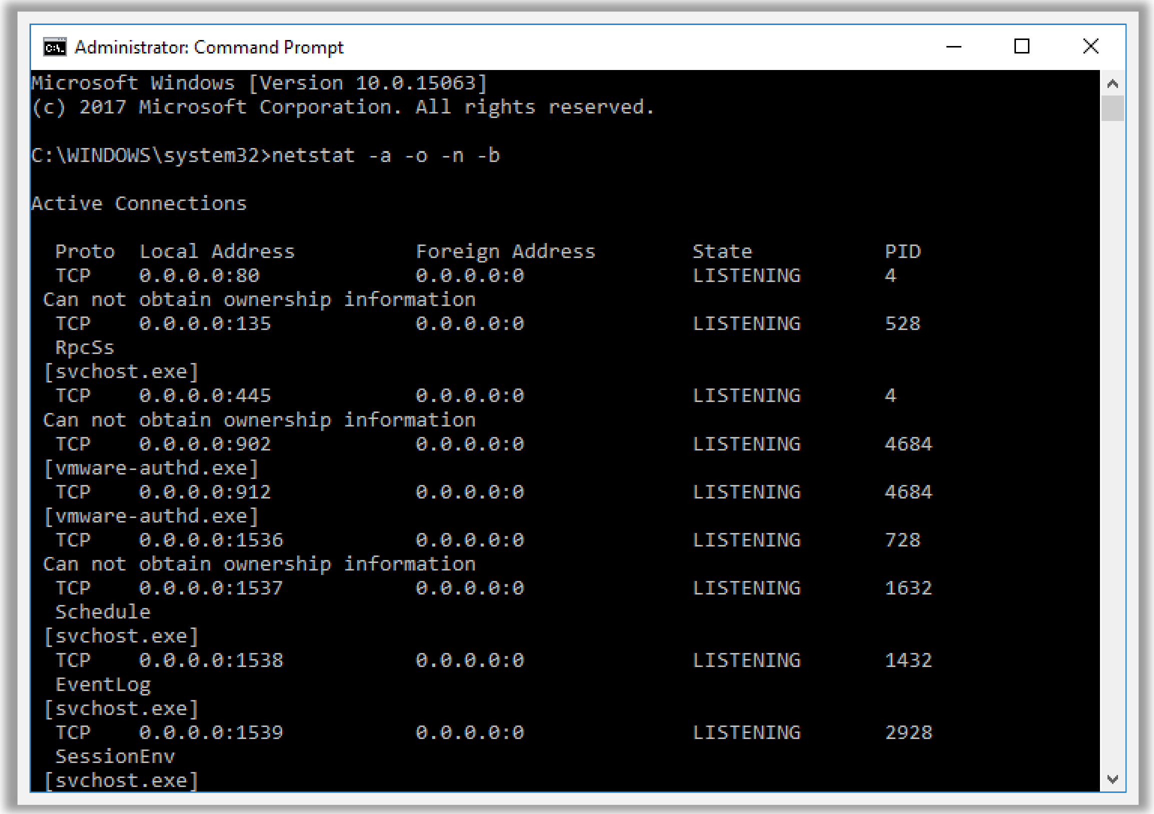
3572 items

Source: *https://technet.microsoft.com*

- Windows registry stores all the **configuration settings** of the applications and systems
- OS **records** every action taken by the user in the registry
- It maintains the **registry keys** for various user actions in terms of Log, Autorun Locations, MRU lists, UserAssist, etc.
- Organizations usually do not audit the registry of the workstations
- **Regular Monitoring and Auditing** of the registry can help you detect traces of malicious activity on the system
- Use the **Process Monitor** utility to monitor registry activity in real time

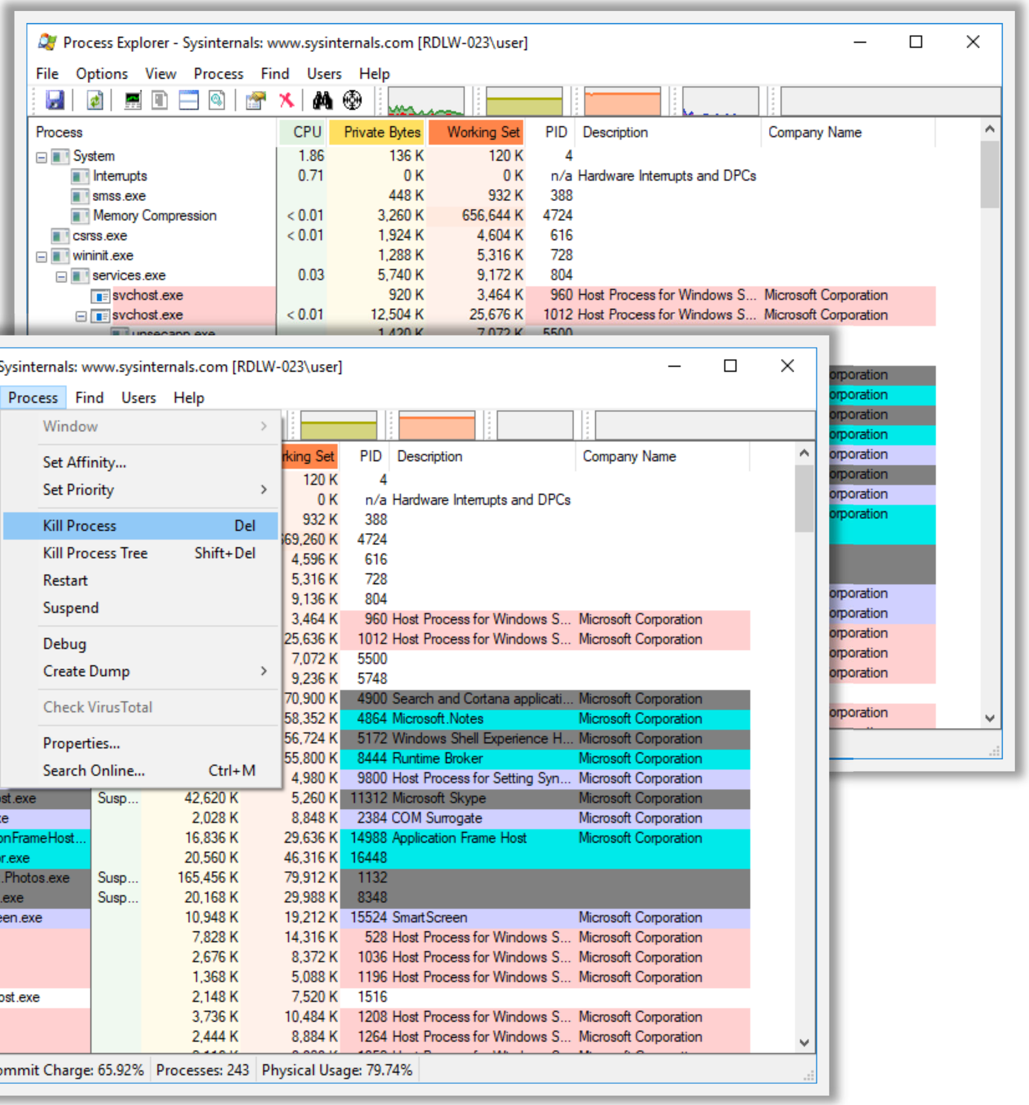
Identifying Running Process and its Associated Sockets

- ❑ Use tools such as Process Explorer, Process Monitor, etc. to identify processes running on Windows System
- ❑ You can also use netstat utility to identify the connection or listening port or sockets associated with the each running process



Administrator: Command Prompt

```
Microsoft Windows [Version 10.0.15063]
(c) 2017 Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>netstat -a -o -n -b

Active Connections

  Proto  Local Address          Foreign Address        State           PID
  TCP    0.0.0.0:80             0.0.0.0:0              LISTENING       4
 Can not obtain ownership information
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING       528
  RpcSs
 [svchost.exe]
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING       4
 Can not obtain ownership information
  TCP    0.0.0.0:902            0.0.0.0:0              LISTENING       4684
 [vmware-authd.exe]
  TCP    0.0.0.0:912            0.0.0.0:0              LISTENING       4684
 [vmware-authd.exe]
  TCP    0.0.0.0:1536           0.0.0.0:0              LISTENING       728
 Can not obtain ownership information
  TCP    0.0.0.0:1537           0.0.0.0:0              LISTENING       1632
  Schedule
 [svchost.exe]
  TCP    0.0.0.0:1538           0.0.0.0:0              LISTENING       1432
  EventLog
 [svchost.exe]
  TCP    0.0.0.0:1539           0.0.0.0:0              LISTENING       2928
  SessionEnv
 [svchost.exe]
```



Process Explorer - Sysinternals: www.sysinternals.com [RDLW-023\user]

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
System	1.86	136 K	120 K	4		
Interrupts	0.71	0 K	0 K	n/a	Hardware Interrupts and DPCs	
smss.exe		448 K	932 K	388		
Memory Compression	< 0.01	3,260 K	656,644 K	4724		
csrss.exe	< 0.01	1,924 K	4,604 K	616		
wininit.exe		1,288 K	5,316 K	728		
services.exe	0.03	5,740 K	9,172 K	804		
svchost.exe		920 K	3,464 K	960	Host Process for Windows S...	Microsoft Corporation
svchost.exe	< 0.01	12,504 K	25,676 K	1012	Host Process for Windows S...	Microsoft Corporation

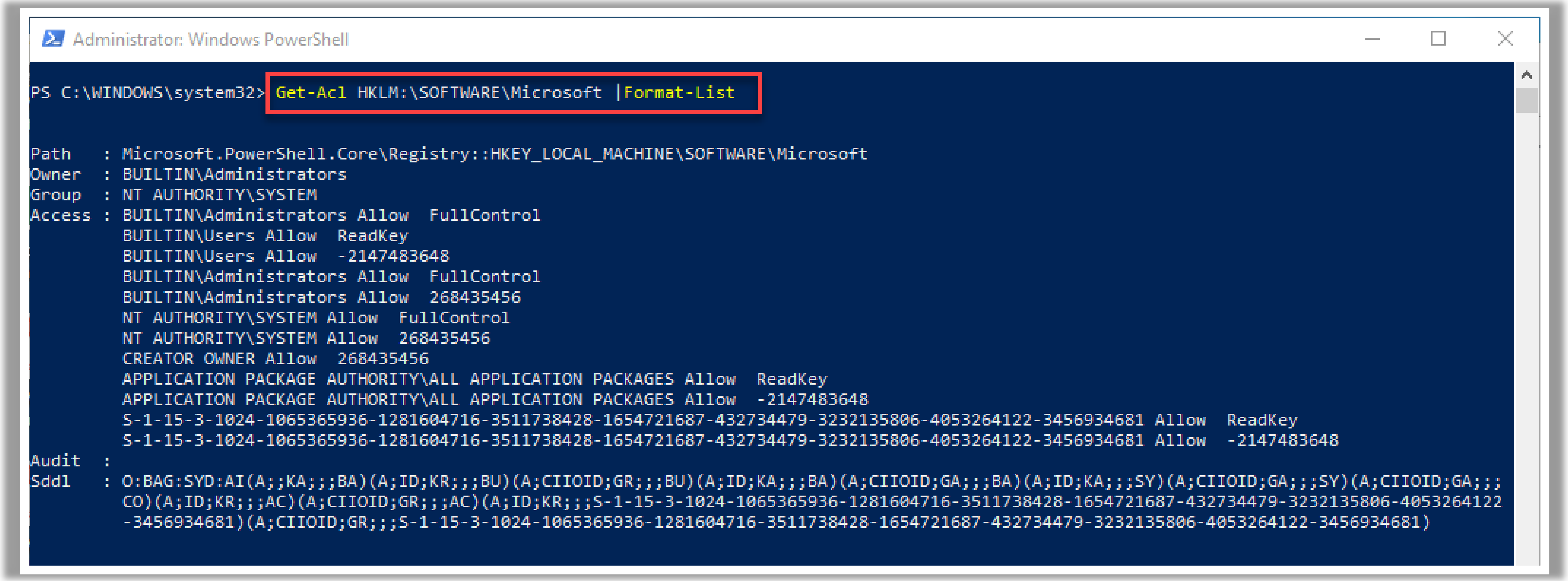
Process Explorer - Sysinternals: www.sysinternals.com [RDLW-023\user]

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
System			120 K	4		
Interrupts			0 K	n/a	Hardware Interrupts and DPCs	
smss.exe			932 K	388		
Memory Compre			69,260 K	4724		
csrss.exe			4,596 K	616		
wininit.exe			5,316 K	728		
services.exe			9,136 K	804		
svchost.exe			3,464 K	960	Host Process for Windows S...	Microsoft Corporation
svchost.exe			25,636 K	1012	Host Process for Windows S...	Microsoft Corporation
unsecap			7,072 K	5500		
WmiPrvS			9,236 K	5748		
SearchU			70,900 K	4900	Search and Cortana applicati...	Microsoft Corporation
Microsoft			58,352 K	4864	Microsoft.Notes	Microsoft Corporation
ShellExp			56,724 K	5172	Windows Shell Experience H...	Microsoft Corporation
RuntimeE			55,800 K	8444	Runtime Broker	Microsoft Corporation
SettingSy			4,980 K	9800	Host Process for Setting Syn...	Microsoft Corporation
SkypeHost.exe	Susp...	42,620 K	5,260 K	11312	Microsoft Skype	Microsoft Corporation
dllhost.exe		2,028 K	8,848 K	2384	COM Surrogate	Microsoft Corporation
ApplicationFrameHost...		16,836 K	29,636 K	14988	Application Frame Host	Microsoft Corporation
Calculator.exe		20,560 K	46,316 K	16448		
Microsoft.Photos.exe	Susp...	165,456 K	79,912 K	1132		
Music.UI.exe	Susp...	20,168 K	29,988 K	8348		
smartscreen.exe		10,948 K	19,212 K	15524	SmartScreen	Microsoft Corporation
svchost.exe		7,828 K	14,316 K	528	Host Process for Windows S...	Microsoft Corporation
svchost.exe		2,676 K	8,372 K	1036	Host Process for Windows S...	Microsoft Corporation
svchost.exe		1,368 K	5,088 K	1196	Host Process for Windows S...	Microsoft Corporation
WUDFHost.exe		2,148 K	7,520 K	1516		
svchost.exe		3,736 K	10,484 K	1208	Host Process for Windows S...	Microsoft Corporation
svchost.exe		2,444 K	8,884 K	1264	Host Process for Windows S...	Microsoft Corporation

CPU Usage: 12.03% | Commit Charge: 65.92% | Processes: 243 | Physical Usage: 79.74%

Analyzing Registry ACLs

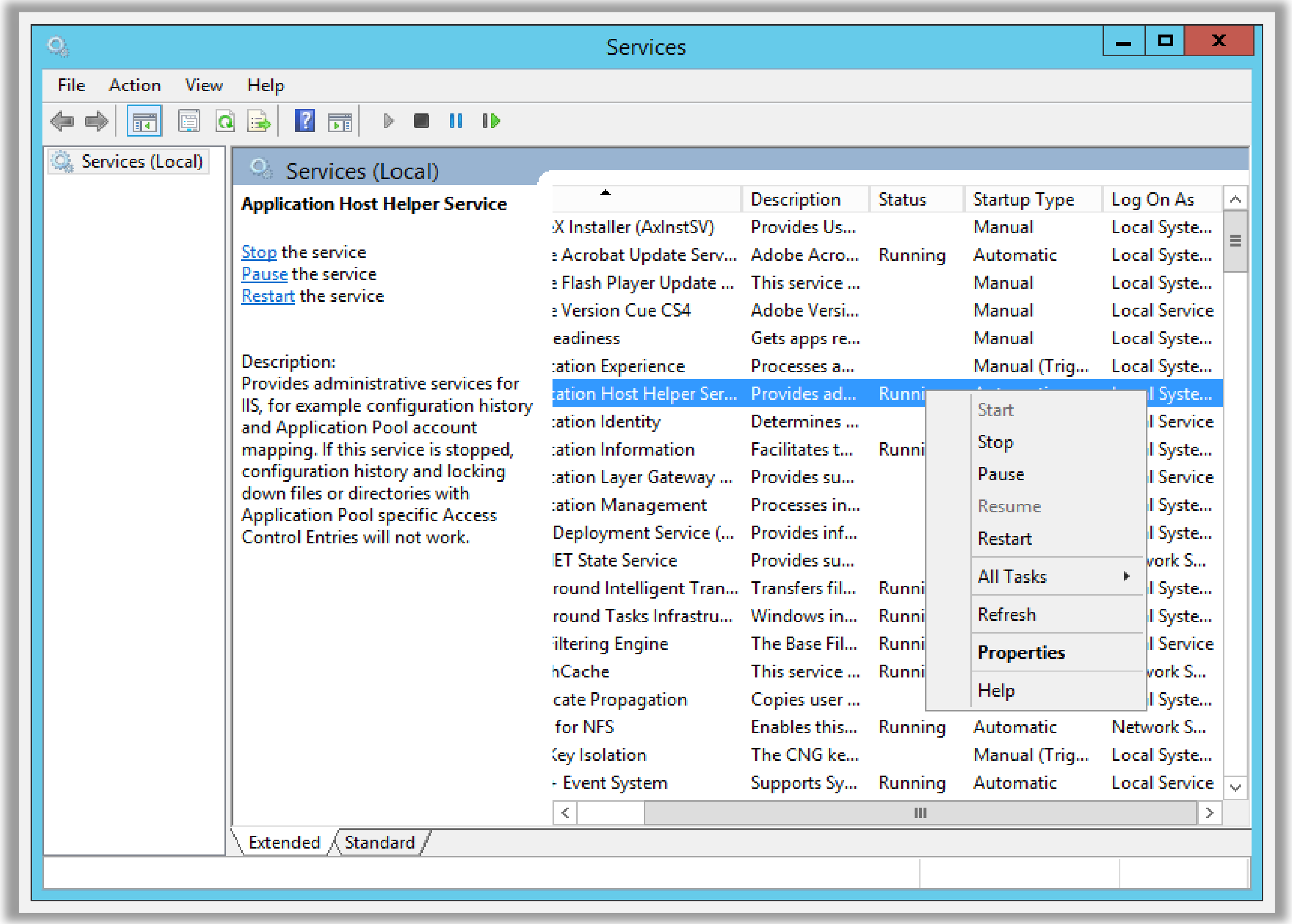
- With the Powershell, you can view the list of ACLs on a registry key
- Use **Get-Acl** command to view the existing ACL on a registry key
- Analyze and identify the list of users and their permissions on the registry key



```
PS C:\WINDOWS\system32> Get-Acl HKLM:\SOFTWARE\Microsoft |Format-List


Path   : Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft
Owner  : BUILTIN\Administrators
Group  : NT AUTHORITY\SYSTEM
Access : BUILTIN\Administrators Allow  FullControl
         BUILTIN\Users Allow  ReadKey
         BUILTIN\Users Allow  -2147483648
         BUILTIN\Administrators Allow  FullControl
         BUILTIN\Administrators Allow  268435456
         NT AUTHORITY\SYSTEM Allow  FullControl
         NT AUTHORITY\SYSTEM Allow  268435456
         CREATOR OWNER Allow  268435456
         APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES Allow  ReadKey
         APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES Allow  -2147483648
         S-1-15-3-1024-1065365936-1281604716-3511738428-1654721687-432734479-3232135806-4053264122-3456934681 Allow  ReadKey
         S-1-15-3-1024-1065365936-1281604716-3511738428-1654721687-432734479-3232135806-4053264122-3456934681 Allow  -2147483648
Audit  :
Sddl   : O:BAG:SYD:AI(A;;KA;;;BA)(A;ID;KR;;;BU)(A;CIIOID;GR;;;BU)(A;ID;KA;;;BA)(A;CIIOID;GA;;;BA)(A;ID;KA;;;SY)(A;CIIOID;GA;;;
         CO)(A;ID;KR;;;AC)(A;CIIOID;GR;;;AC)(A;ID;KR;;;S-1-15-3-1024-1065365936-1281604716-3511738428-1654721687-432734479-3232135806-4053264122
         -3456934681)(A;CIIOID;GR;;;S-1-15-3-1024-1065365936-1281604716-3511738428-1654721687-432734479-3232135806-4053264122-3456934681)
```

Disabling Unused System Services

- Go to **Control Panel → Administrative Tools → Services**
- **Disable** the following service on any machine other than a server
  - IIS
  - FTP
  - SQL Server
  - Proxy services
  - Telnet
  - Universal Plug And Play on any machine



Application Host Helper Service

Stop the service
Pause the service
Restart the service

Description:
Provides administrative services for IIS, for example configuration history and Application Pool account mapping. If this service is stopped, configuration history and locking down files or directories with Application Pool specific Access Control Entries will not work.

	Description	Status	Startup Type	Log On As
X Installer (AxInstSV)	Provides Us...		Manual	Local Syste...
Acrobat Update Serv...	Adobe Acro...	Running	Automatic	Local Syste...
Flash Player Update ...	This service ...		Manual	Local Syste...
Version Cue CS4	Adobe Versi...		Manual	Local Service
eadiness	Gets apps re...		Manual	Local Syste...
ation Experience	Processes a...		Manual (Trig...	Local Syste...
ation Host Helper Ser...	Provides ad...	Runni		l Syste...
ation Identity	Determines ...			l Service
ation Information	Facilitates t...	Runni		l Syste...
ation Layer Gateway ...	Provides su...			l Service
ation Management	Processes in...			l Syste...
Deployment Service (...	Provides inf...			l Syste...
ET State Service	Provides su...			vork S...
round Intelligent Tran...	Transfers fil...	Runni		l Syste...
round Tasks Infrastru...	Windows in...	Runni		l Syste...
iltering Engine	The Base Fil...	Runni		l Service
hCache	This service ...	Runni		vork S...
cate Propagation	Copies user ...			l Syste...
for NFS	Enables this...	Running	Automatic	Network S...
ey Isolation	The CNG ke...		Manual (Trig...	Local Syste...
Event System	Supports Sy...	Running	Automatic	Local Service

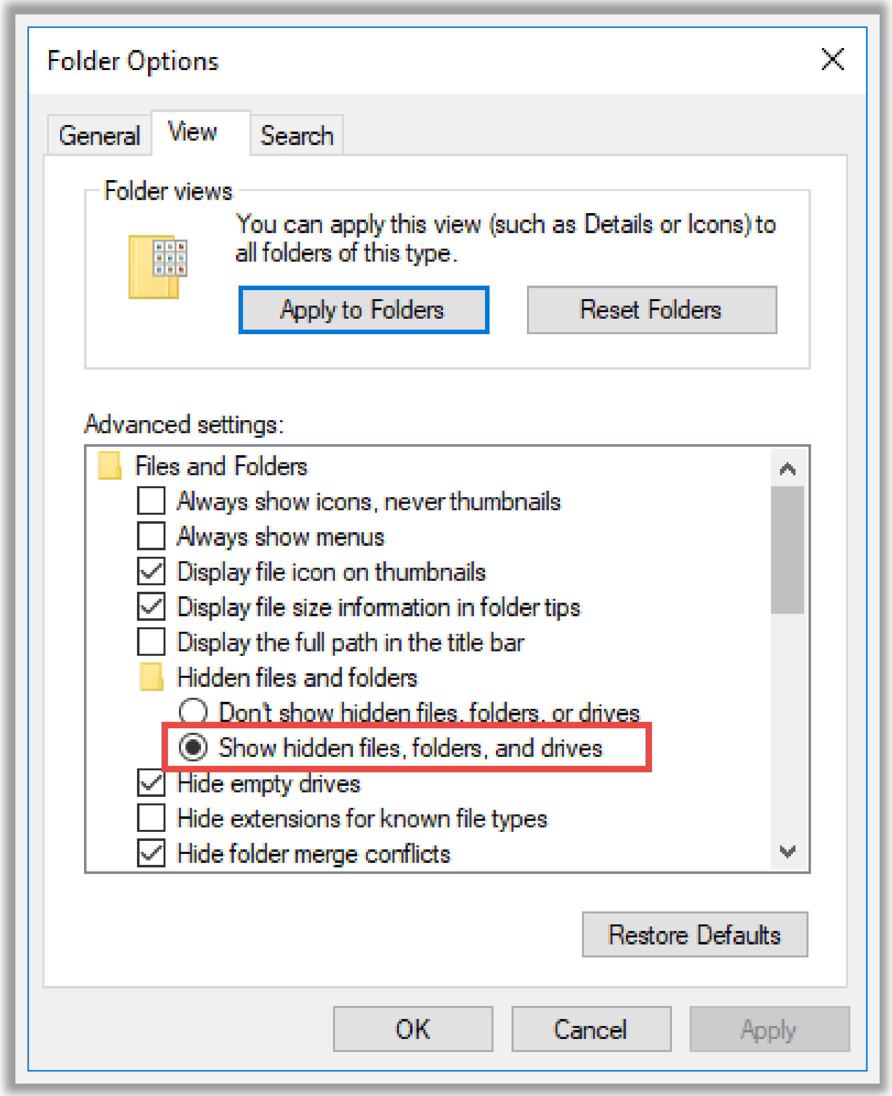
Finding Suspicious/Hidden/Interesting Files

Identify Hidden Files

- To protect data, the user uses a **hidden** attribute of file, which will be invisible from the normal user
- Windows by default does not display hidden files
- Sometimes, a hidden suspicious file can pose security risk to the system

Examples of Suspicious Hidden files

- Malicious Software malware
- Spyware
- Worms



Folder Options

General | View | Search

Folder views

You can apply this view (such as Details or Icons) to all folders of this type.

Advanced settings:

- Files and Folders
  - □ Always show icons, never thumbnails
  - □ Always show menus
  - ☑ Display file icon on thumbnails
  - ☑ Display file size information in folder tips
  - □ Display the full path in the title bar
  - Hidden files and folders
    - ○ Don't show hidden files, folders, or drives
    - ● Show hidden files, folders, and drives
  - ☑ Hide empty drives
  - □ Hide extensions for known file types
  - ☑ Hide folder merge conflicts

File System Security: Setting Access Controls and Permission

- Use **Access Control List (ACLs) and Permissions** to control access to Files and folders

Access Control Entry (ACE)

- **Allow/deny access** to file or directories for user or group of users

Access Control List (ACL)

- It is a **collection of ACEs** for accessing specific files or directories

Permissions

- Access control on specific file or folder is achieved by enforcing certain permissions on it
- Two types of permissions

  1. **NTFS permissions** (Security Permissions) 2. **Share permissions**

File System Security: Setting Access Controls and Permission to Files and Folders

Applying NTFS permissions

- Typical file permissions allowed on NTFS file system are:
  - Full Control
  - Modify
  - Read & Execute
  - Read
  - Write
- Each of these permissions includes a **logical group** of special permissions

Special permissions associated with each of **NTFS file permissions**:

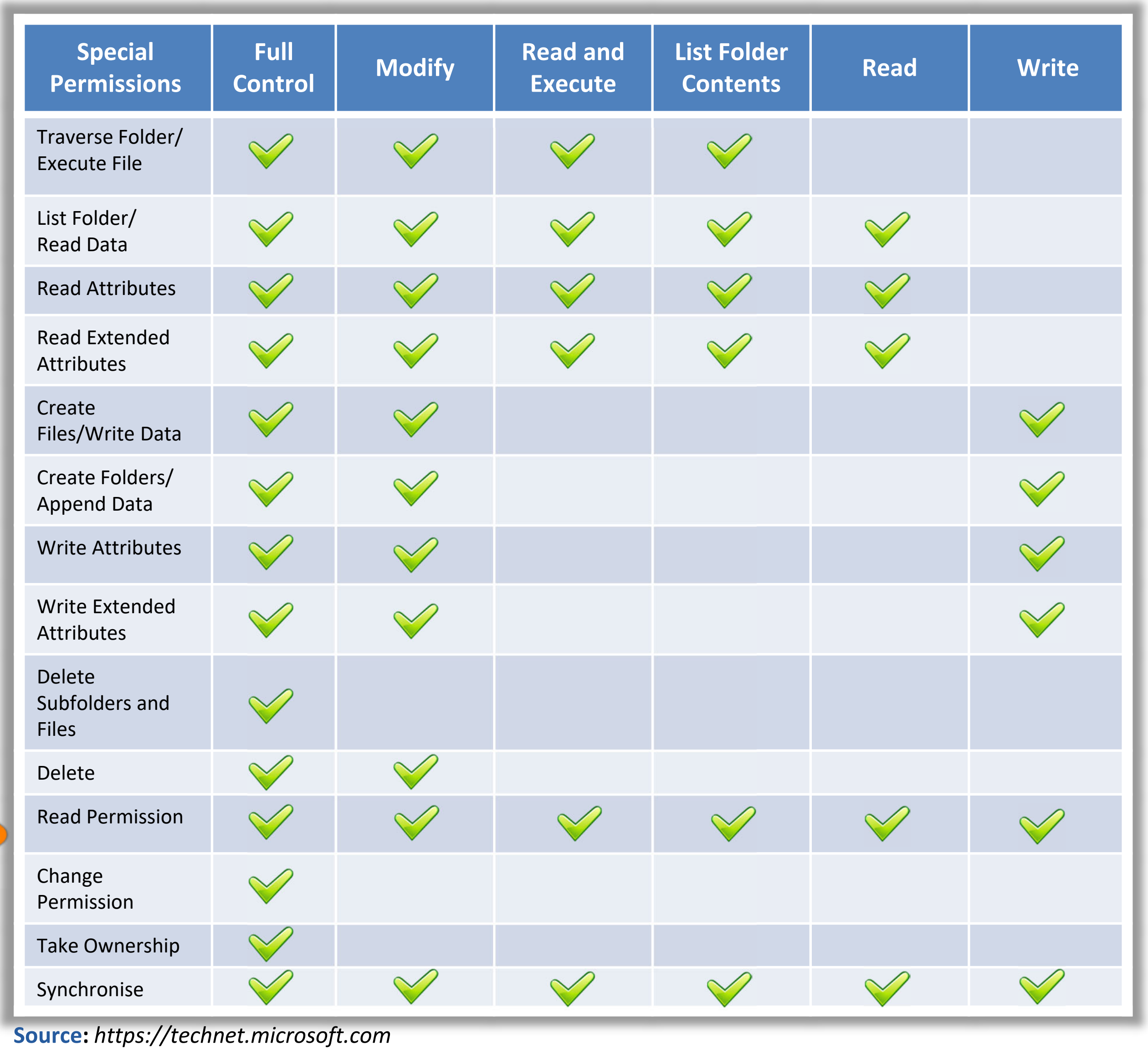
Special Permissions	Full Control	Modify	Read and Execute	Read	Write
Traverse Folder/ Execute File	✓	✓	✓		
List Folder/ Read Data	✓	✓	✓	✓	
Read Attributes	✓	✓	✓	✓	
Read Extended Attributes	✓	✓	✓	✓	
Create Files/Write Data	✓	✓			✓
Create Folders/ Append Data	✓	✓			✓
Write Attributes	✓	✓			✓
Write Extended Attributes	✓	✓			✓
Delete Subfolders and Files	✓				
Delete	✓	✓			
Read Permission	✓	✓	✓	✓	✓
Change Permission	✓				
Take Ownership	✓				
Synchronise	✓	✓	✓	✓	✓

Source: *https://technet.microsoft.com*

File System Security: Setting Access Controls and Permission to Files and Folders (Cont'd)

- Typical folder permissions allowed on NTFS file system are
  - Full Control
  - Modify
  - Read & Execute
  - List Folder Contents
  - Read
  - Write
- Each of these permissions include a **logical group** of special permissions

Special permissions associated with each of NTFS folder permissions

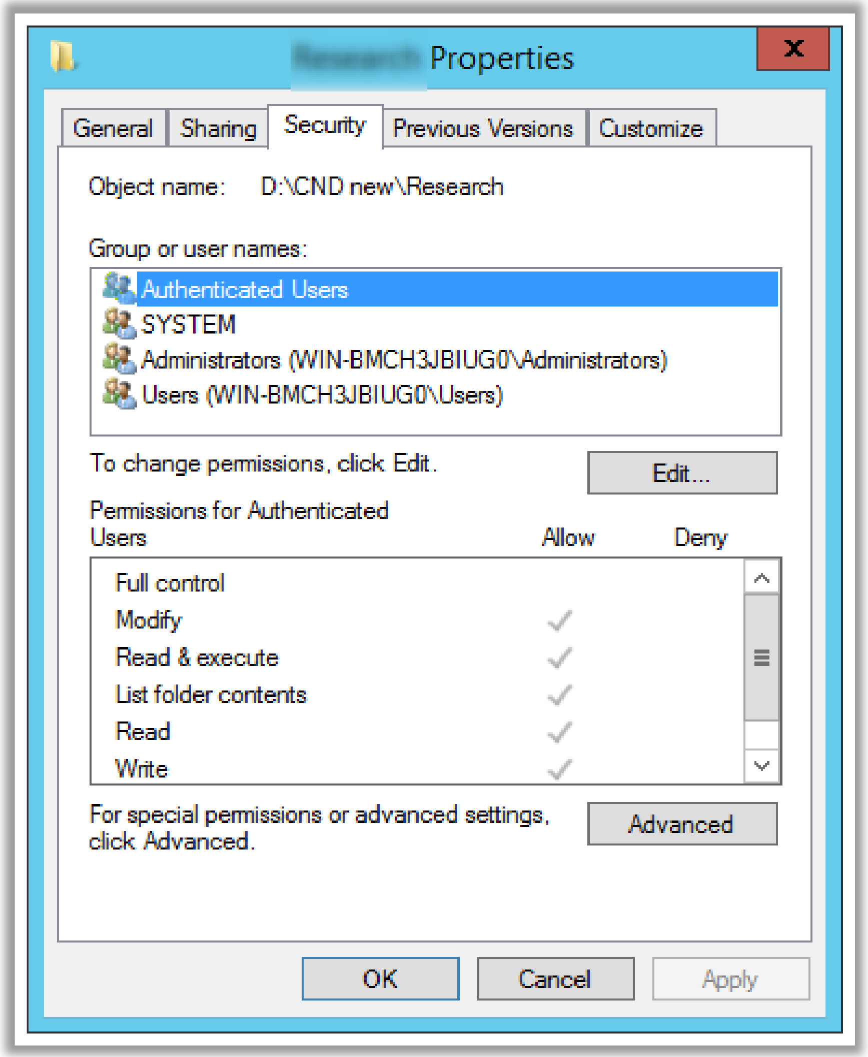


Special Permissions	Full Control	Modify	Read and Execute	List Folder Contents	Read	Write
Traverse Folder/ Execute File	✓	✓	✓	✓		
List Folder/ Read Data	✓	✓	✓	✓	✓	
Read Attributes	✓	✓	✓	✓	✓	
Read Extended Attributes	✓	✓	✓	✓	✓	
Create Files/Write Data	✓	✓				✓
Create Folders/ Append Data	✓	✓				✓
Write Attributes	✓	✓				✓
Write Extended Attributes	✓	✓				✓
Delete Subfolders and Files	✓					
Delete	✓	✓				
Read Permission	✓	✓	✓	✓	✓	✓
Change Permission	✓					
Take Ownership	✓					
Synchronise	✓	✓	✓	✓	✓	✓

Source: *https://technet.microsoft.com*

File System Security: Setting Access Controls and Permission to Files and Folders (Cont'd)

- To set, view, edit, or remove **special permissions**:
  - Go to specific file or folder on which you want to set special permission
  - Right-click the file or folder, click **Properties**, and then click the **Security** tab
  - Click **Advanced**
  - Click **Add** to set special permissions for a new group or user in Permission Entry Window



[redacted] Properties

Object name: D:\CND new\Research

Group or user names:

- Authenticated Users
- SYSTEM
- Administrators (WIN-BMCH3JBIUG0\Administrators)
- Users (WIN-BMCH3JBIUG0\Users)

To change permissions, click Edit.

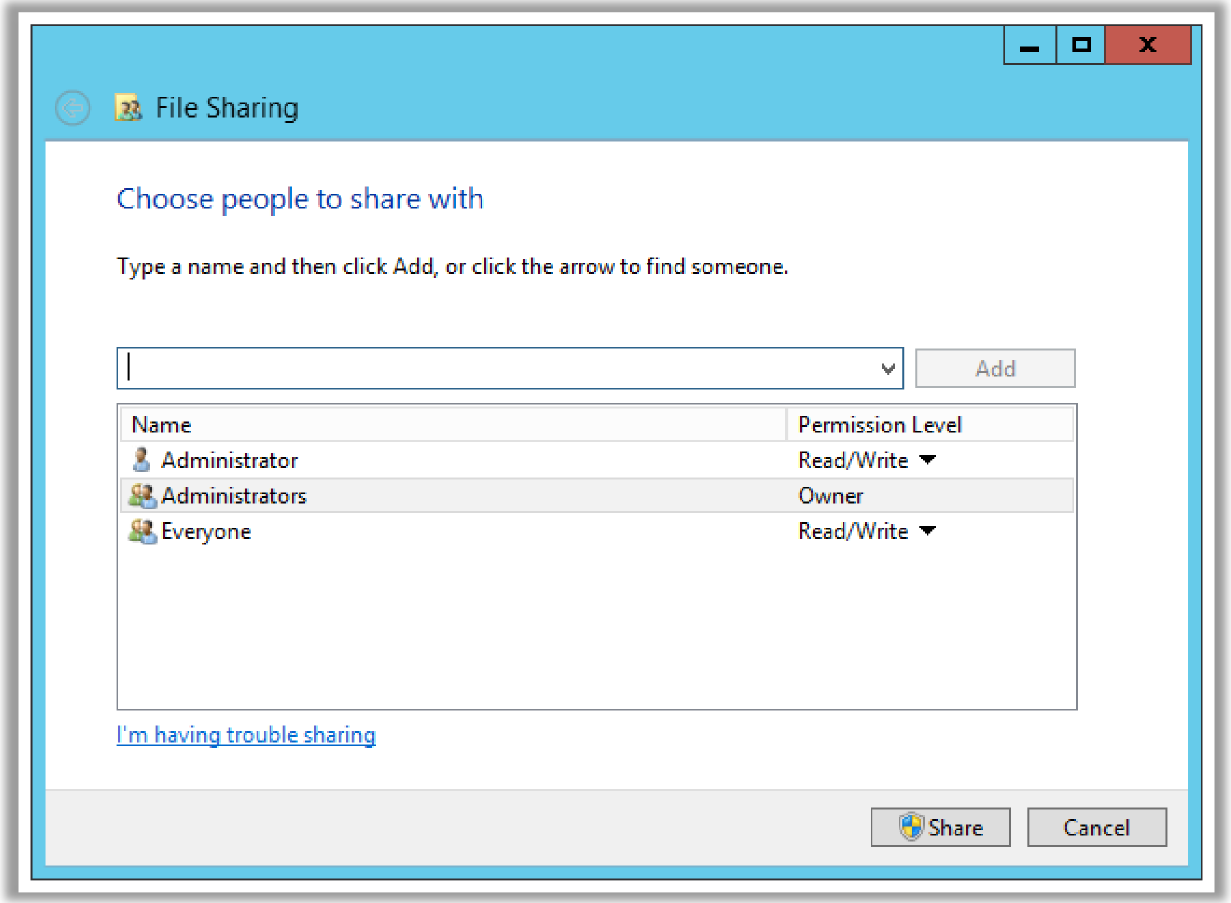
Permissions for Authenticated Users	Allow	Deny
Full control		
Modify	✓	
Read & execute	✓	
List folder contents	✓	
Read	✓	
Write	✓	

For special permissions or advanced settings, click Advanced.

File System Security: Setting Access Controls and Permission to Files and Folders (Cont'd)

Applying Share Permissions

- Share permissions are applied when you need to provide access to a **shared folder** over the network
- With Share permission, you can **restrict access** to share folders
  1. Go to the specific file or folder on which you want to set Share Permissions
  2. Right-click the folder and click Share with option
  3. Select specific user or group to whom you want to assign share permission such as Read, Read/Write



Choose people to share with

Type a name and then click Add, or click the arrow to find someone.

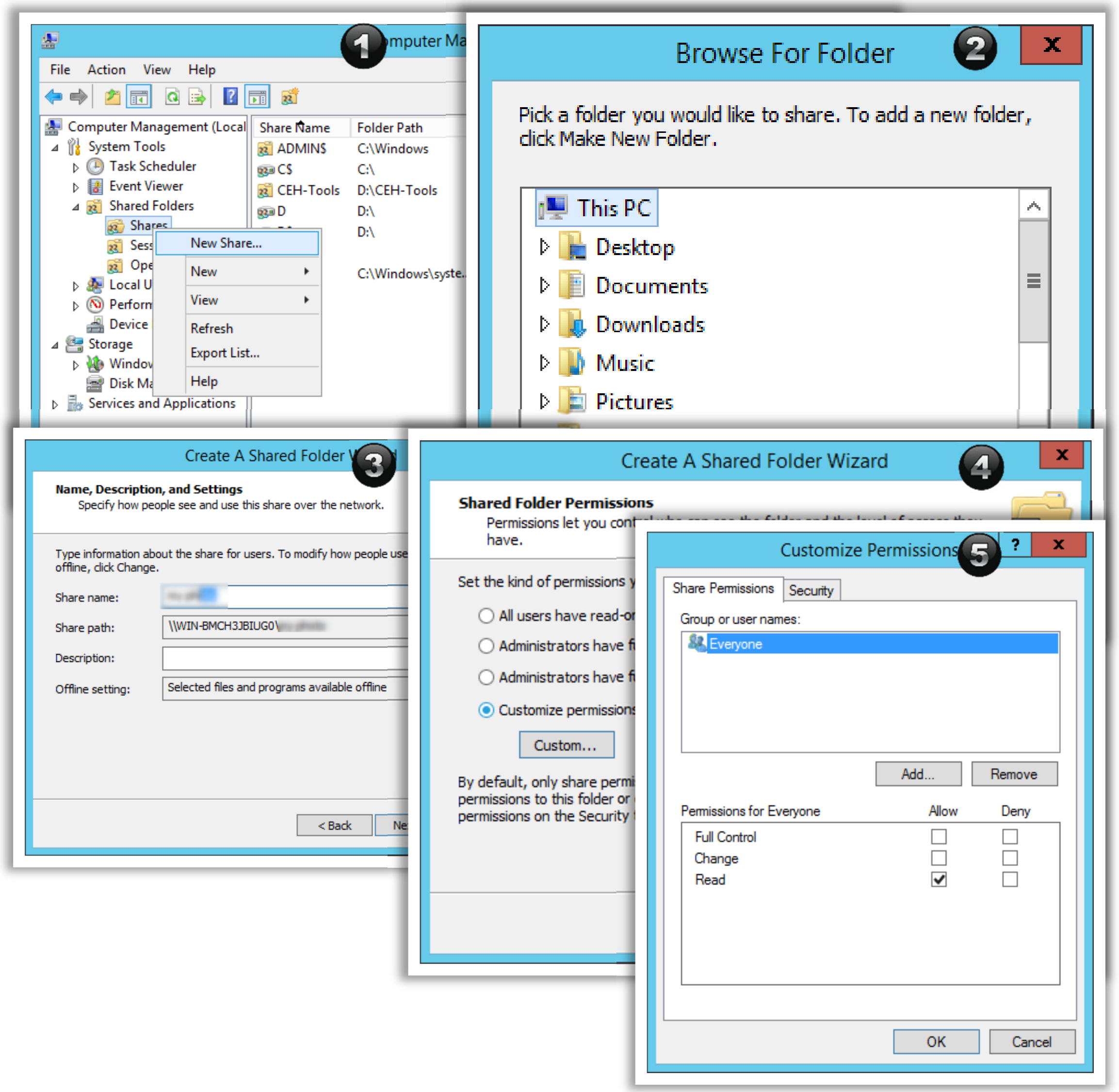
Name	Permission Level
Administrator	Read/Write ▼
Administrators	Owner
Everyone	Read/Write ▼

Note: Use NTFS Permission in addition to shared permissions to provide more restriction to shared folders

Creating and Securing a Windows File Share

Creating New File Share

- Go to **Computer Management**
  - Click **System Tools**, right-click **Shares** and click **New Share**
  - Browse the folder that you want to share
  - Enter the **[Share Name]**
  - Select **Customize permissions** and click **Custom to** customize the Share Folder Permissions
  - Add the correct **Active Directory User(s) &/or Group(s)**
    - The Share Permissions only allow Users and/or Group of users to access to a **specific shared Folder**
    - The User(s) and/or Group(s) must also have the appropriate **NTFS Permissions** to access the files



1 Computer Management

Share Name	Folder Path
ADMIN$	C:\Windows
C$	C:\
CEH-Tools	D:\CEH-Tools
D	D:\
	D:\
	C:\Windows\syste...

2 Browse For Folder

Pick a folder you would like to share. To add a new folder, click Make New Folder.

3 Create A Shared Folder Wizard

Name, Description, and Settings
Specify how people see and use this share over the network.

Type information about the share for users. To modify how people use offline, click Change.

Share name: [redacted]
Share path: \\WIN-BMCH3JBIUG0\[redacted]
Description:
Offline setting: Selected files and programs available offline

4 Create A Shared Folder Wizard

Shared Folder Permissions
Permissions let you cont... have.

Set the kind of permissions y...

○ All users have read-o...
○ Administrators have f...
○ Administrators have f...
● Customize permissions

By default, only share permi... permissions to this folder or ... permissions on the Security ...

5 Customize Permissions

Group or user names: Everyone

Permissions for Everyone	Allow	Deny
Full Control	☐	☐
Change	☐	☐
Read	☑	☐

Desktop Locked Down

- Desktop Lockdown refers to the process of preventing the users from accessing a desktop or making any changes to its configuration settings.

Desktop Locked down is required to:

- Maintain security
- Slow down an attackers' attempt
- Avoid unauthorized s/w and patch installation

Policies or Settings in locked down desktop

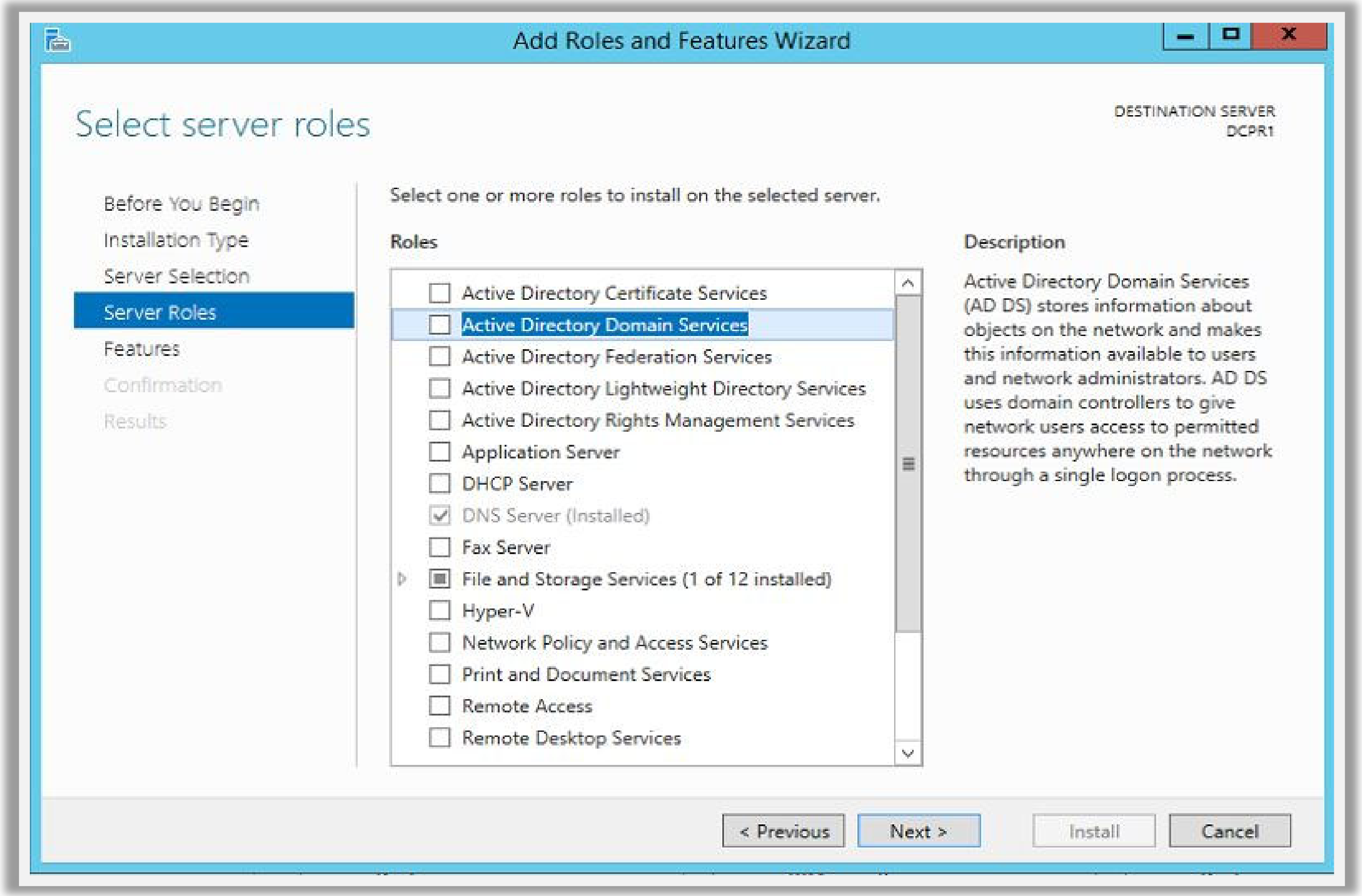
- Software Restriction
- User rights
- Security Templates
- Administrative
- Access Control List(ACLs)

Some Techniques to enforce Desktop Locked down :

- Enable User Group Policy loopback processing mode.
- Avoid viewing last Login user name on login screen
- Restriction for cd/floppy devices access to locally logged on user only
- Disable Windows installer
- Prevent access to Windows Shutdown command
- Restrict to user changing my Document Path
- Disable control panel
- Disable Registry editing tool

Active Directory(AD)

- Active Directory is a directory service for a Windows OS that facilitates and manages network components such as a user or service such as a users, services,, sites, systems, users, shares on Windows Network
- It is the central storehouse for all objects in an organization and their attributes
- Each component tracked by AD is an object, which is described by its attributes



Add Roles and Features Wizard

Select server roles

DESTINATION SERVER
DCPR1

Select one or more roles to install on the selected server.

Roles

- ☐ Active Directory Certificate Services
- ☐ Active Directory Domain Services
- ☐ Active Directory Federation Services
- ☐ Active Directory Lightweight Directory Services
- ☐ Active Directory Rights Management Services
- ☐ Application Server
- ☐ DHCP Server
- ☑ DNS Server (Installed)
- ☐ Fax Server
- ■ File and Storage Services (1 of 12 installed)
- ☐ Hyper-V
- ☐ Network Policy and Access Services
- ☐ Print and Document Services
- ☐ Remote Access
- ☐ Remote Desktop Services

Description

Active Directory Domain Services (AD DS) stores information about objects on the network and makes this information available to users and network administrators. AD DS uses domain controllers to give network users access to permitted resources anywhere on the network through a single logon process.

Active Directory Roles: Global Catalog (GC)

- Global Catalog (GC) is a single Lightweight Directory Access Protocol (LDAP) data repository containing partial representation of objects present in a multidomain Active Directory Domain Services (AD DS) forest
- GC server is a part of active directory and allows users to find objects to which they have been granted access
- The GC server stores and replicates information such as the domain forest schema data and configuration data
- It is stored in domain controllers and enables faster searching of objects by locating them in any domain without knowing the domain name
- Common global catalog usage scenarios include:
  - Forest-wide searches
  - User logon
  - Universal group membership caching
  - Exchange address book lookups

Active Directory Roles: Master Browser

Master Browser is a server or computer that gathers information about all the servers in its domain or workgroup and the list of all domains on the network

The list collected by a master browser is called as Browse list

When a user opens the available Network places, the network client requests the browse list and displays the list of available servers

Each domain in a TCP/IP-based subnet has its own master browser

If a domain extends more than one subnet, the master browser will maintain a separate browse list for the part of the domain on its subnet

Active Directory Roles: FSMO

- Flexible Single Master Operation (FSMO) role refers to the ability of an active directory to transfer roles to any domain controller (DC) in the enterprise

- Windows has five FSMO roles including:
  - **Schema master:** The DC holding this will be responsible for performing updates to the directory schema.
  - **Domain naming master:** The holder of this role will be responsible for making changes to the forest-wide domain name space of the directory. It can also add or remove cross references to domains in external directories.
  - **RID master:** This role allows the holder to process relative ID (RID) Pool requests from all DCs belonging to same domain. It enables moving of an object from one domain to another.
  - **PDC emulator:** Primary Domain Controller (PDC) emulator synchronizes time among all the domain controllers in an enterprise. It records the password changes performed by other DCs in the domain, authentication failures due to entering an incorrect password and processes account lockout.
  - **Infrastructure master:** This role ensures proper handling of the cross-domain object references. It works only in a multi-domain environment. It is responsible for managing updates when changes occur in the remote domain.

How AD Relies on DNS

- Active Directory uses DNS as its domain controller location mechanism
- Uses the namespace design of DNS in the design of Active Directory domain names
- DNS domain name supports in creating the Active Directory DNS objects
- DNS also helps in locating the objects stored within the Active Directory
- Active Directory clients can use DNS resolution to locate any number of services because Active Directory servers publish a list of addresses to DNS using the new features of dynamic update

How AD Relies on LDAP Group Policy

- Active Directory must comply with the LDAP standards and use them to understand and respond to a request
- LDAP helps AD to communicate queries
- AD supports authentication based on the LDAP 2 and 3 versions
- Active Directory allows a directory administrator to define group policy directory entries using LDAP

Windows Passwords: Password Policy

- Operating systems, such as Windows, use passwords as the most common method to authenticate users
- A password can be a secret passphrase or a string containing different characters
- Passwords prevent the unauthorized users from accessing the user accounts
- Windows has a well defined password policy that helps in creating strong passwords

Password policy

- Password policy refers to a set of rules that help in creating and implementing strong passwords
- It defines length, complexity, lifetime and methods of saving for a password
- Organizations can have different password policies based on their security requirements
- Users can configure the password policy settings in the following location: **Computer Configuration\Windows Settings\Security Settings\Account Policies\Password Policy**
- In windows, the password policy includes the following settings:
  - Enforce password history
  - Maximum password age
  - Minimum password age
  - Minimum password length
  - Password complexity
  - Store passwords using reversible encryption

Windows Passwords: Password Policy (Cont'd)

Enforce password history

- This policy determines the number of unique new passwords a user must set to a user account before reusing an old password
- The policy works together with the maximum password age to secure the passwords as longer use of the same password increases the chances of determining it through various attacks
- It helps in preventing password reuse or reuse a small number of passwords to increase the efficacy of a good password policy
- The user can specify the password history value between 0 and 24

Maximum and minimum password age:

- Also called as password lifetime, the policy determines the maximum and minimum age a password should have
- It defines the number of days for which users can use a password before the system requires them to change it
- The minimum age of the password must always be less than the maximum age
- Best practice is to set the maximum age value between 30 and 90 days and the minimum age value to 2 days

Windows Passwords: Password Policy (Cont'd)

1

Minimum password length:

- This policy limits the least number of characters a password must have for a user account
- Users can set a the length between 1 and 14 characters, while the best practice is to set the password length to at least eight characters

2

Password complexity:

- In windows, the complexity policy is a series of guidelines that helps in setting a strong password
- The policy guidelines include:
  - Password must not contain the user's account name value or entire display name in either upper or lower case
  - The password contains characters from three of the following categories:
    - Uppercase letters of European languages
    - Lowercase letters of European languages
    - Base 10 digits (0 through 9)
    - Non-alphanumeric characters (special characters): (~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/)
    - Any Unicode character that is categorized as an alphabetic character but is not uppercase or lowercase

Windows Passwords: Password Policy (Cont'd)

Store passwords using reversible encryption:

This policy setting determines if the users want to store their passwords on the systems using a reversible encryption

It supports the applications that require password for user authentication

Best practice is to disable this setting because the attackers can break the reversible encryption to compromise the account

Account Lockout Policy

1. Attackers can try to guess the passwords for a user account using trial and error methods leading to a numerous unsuccessful attempts

2. In Windows, the users can use account lockout to configure the domain controllers to prevent password guessing attacks by disabling the account for a predefined duration

3. Account Lockout Policy allows the users to configure the maximum number of times an user can fail to enter the correct password and the system response in case the number of attempts cross the threshold

4. Users can configure the Account Lockout Policy settings in Windows in the following location: **Computer Configuration\Windows Settings\Security Settings\Account Policies\Account Lockout Policy**

5. The account lockout policy has the following settings:
   - Account lockout duration
   - Account lockout threshold
   - Reset account lockout counter after

Account Lockout Policy (Cont'd)

Account lockout duration:

- This setting will allow the user to determine the number of minutes an account must remain locked out
- It has a range of 1 to 99,999 minutes and a setting zero minutes specifies that the system will never lockout the account
- The users must set Account lockout duration of approximately 30 minutes

Account lockout threshold:

- The option helps in setting the number of failed sign-in attempts it will offer before the system locks the user account
- It offers a range starting from 1 to 999 failed sign-in attempts, while providing a null value will specify that the account never locks
- Users can select the threshold that offers a balance between operational efficiency and security, depending on the organization's risk level
- A setting ranging between four and 10 is recommendable as it gives the users ample chances to enter correct password and protect the account from brute-force attacks as well

Reset account lockout counter after:

- The option helps users to limit the number of minutes a user must wait from the first failure attempt to make a new attempt before the failed logon attempt counter is reset
- It offers a range of 1 to 99,999 minutes
- Users need to select a value based on the organization's threat level and to balance the cost incurred in support for password resets

Microsoft Authentication

The Windows passwords are generated and stored either as an LM Hash or an NT Hash

- **LAN Manager hash (LANMAN or LM hash):** It is a encryption mechanism employed by Microsoft to encrypt the passwords stored on the system. These hashes are easy to crack using rainbow tables or brute force attacks. NTLM hashes replaced this encryption starting from Windows NT.

- **NTLM:** NTLM is an authentication protocol used by Windows to authenticate users and computers in a network based on a challenge/response mechanism. This protocol does not send the credentials but, enables the system requesting the authentication to make a calculation to prove that it has access to the credentials.

  - **NTLMv1:** The authentication uses an 8-byte challenge and returns 24 byte results

  - **NTLMv2:** V2 was developed to replace V1 and includes stronger algorithm, wherein the authentication uses two 8-byte challenges and returns 16-byte HMAC-MD5 hash results

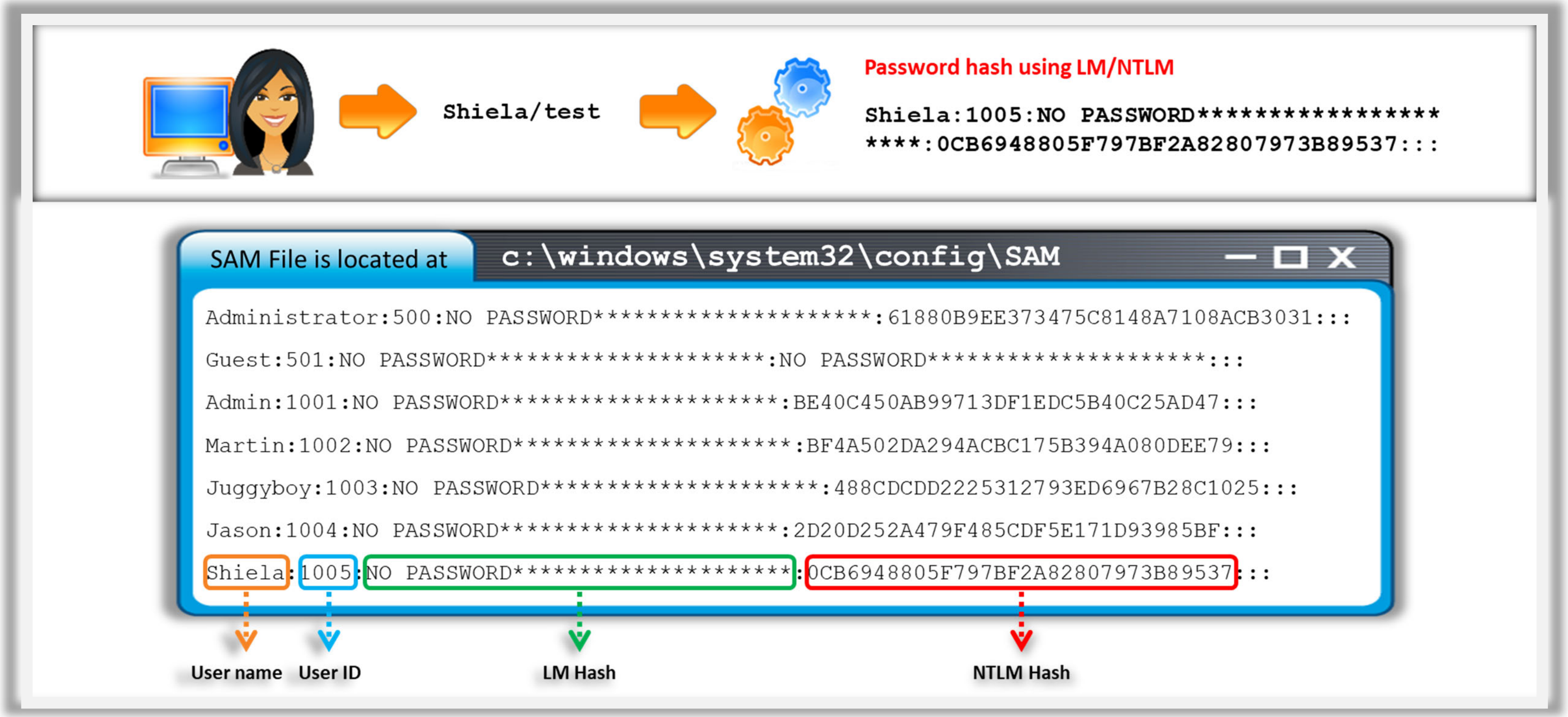
- Both LANMAN and NTLMv1 protocols are the same except that LANMAN uses LM Hash and NTLMv1 uses NT Hash to authenticate users

- Kerberos Authentication: Microsoft has upgraded its **default authentication protocol** to Kerberos which provides a stronger authentication for client/server applications than NTLM

Security Accounts Manager (SAM) Database

- Windows stores user passwords in SAM or in the **Active Directory database** in domains. Passwords are never stored in clear text; passwords are hashed, and the results are stored in the SAM

How Hash Passwords Are Stored in Windows SAM?



```
Shiela:1005:NO PASSWORD*****************
****:0CB6948805F797BF2A82807973B89537:::
```

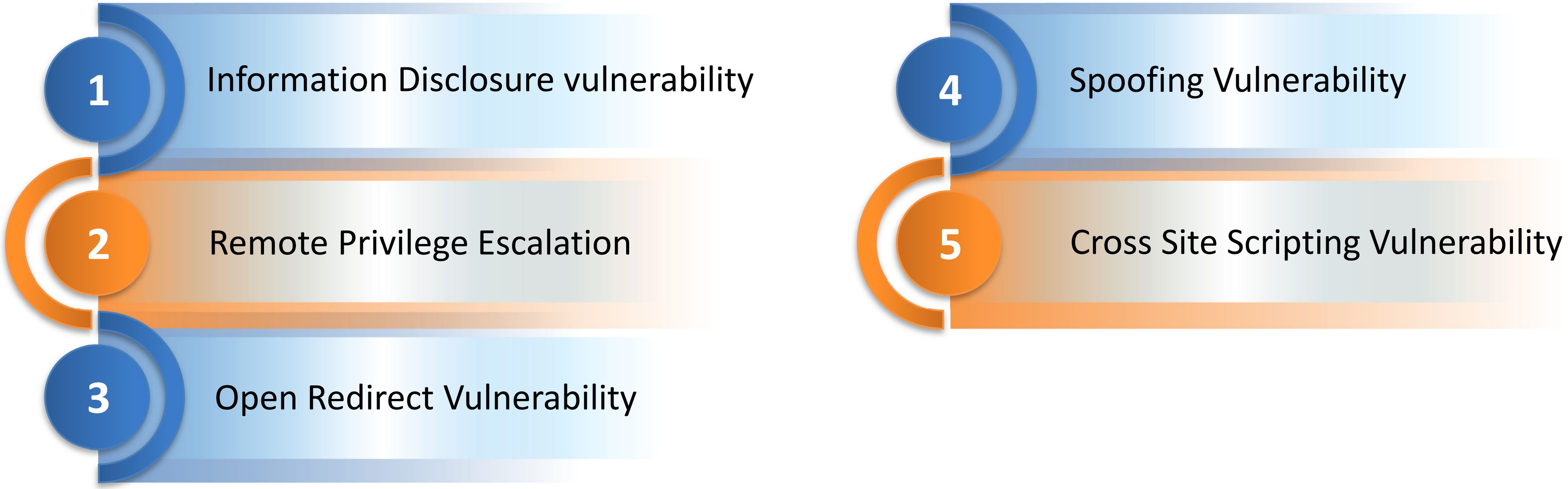
```
c:\windows\system32\config\SAM

Administrator:500:NO PASSWORD*********************:61880B9EE373475C8148A7108ACB3031:::
Guest:501:NO PASSWORD*********************:NO PASSWORD*********************:::
Admin:1001:NO PASSWORD*********************:BE40C450AB99713DF1EDC5B40C25AD47:::
Martin:1002:NO PASSWORD*********************:BF4A502DA294ACBC175B394A080DEE79:::
Juggyboy:1003:NO PASSWORD*********************:488CDCDD2225312793ED6967B28C1025:::
Jason:1004:NO PASSWORD*********************:2D20D252A479F485CDF5E171D93985BF:::
Shiela:1005:NO PASSWORD*********************:0CB6948805F797BF2A82807973B89537:::
```

"LM hashes have been disabled in **Windows Vista** and **later** Windows operating systems, LM will be **blank** in those systems"

Microsoft Exchange Server and its Concerns

Microsoft Exchange Server is a mail server designed to run on Windows Server operating systems

Some of the security Issues with Microsoft Exchange Server:

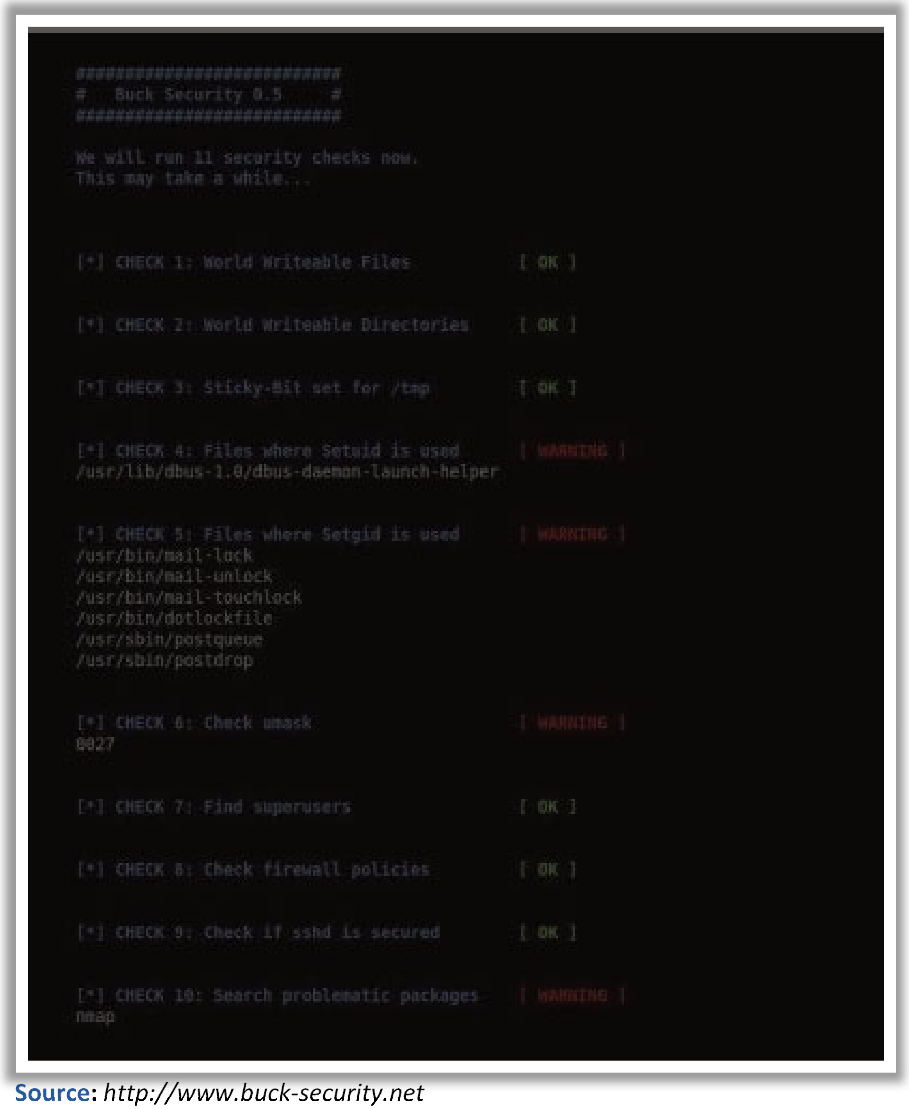


1. Information Disclosure vulnerability
2. Remote Privilege Escalation
3. Open Redirect Vulnerability
4. Spoofing Vulnerability
5. Cross Site Scripting Vulnerability

Unix/Linux Security

Linux Baseline Security Checker: buck-security

- **buck-security** allows you to get a quick overview of the security status of your system
- It conducts a **security check** against the baseline
  - Searching for worldwriteable files
  - Searching for worldwriteable directories
  - Searching for programs where the setuid is set
  - Searching for programs where the setgid is set
  - Checking your umask
  - Checking if the sticky-bit is set for /tmp
  - Searching for superusers
  - Checking firewall policies
  - Checking if sshd is secured
  - Searching for listening services
  - Creating and checking checksums of system programs
  - Searching for installed attack tool packages

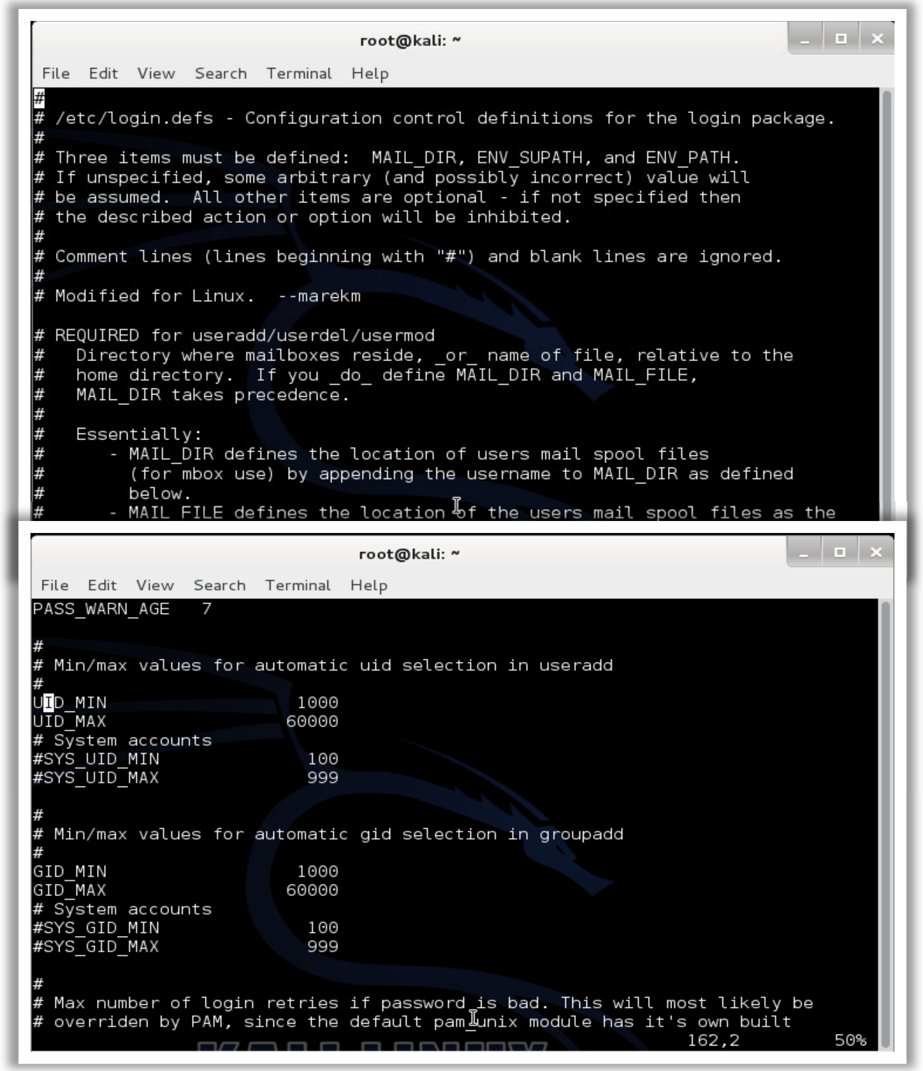


```
############################
#   Buck Security 0.5      #
############################

We will run 11 security checks now.
This may take a while...


[*] CHECK 1: World Writeable Files           [ OK ]


[*] CHECK 2: World Writeable Directories     [ OK ]


[*] CHECK 3: Sticky-Bit set for /tmp         [ OK ]


[*] CHECK 4: Files where Setuid is used      [ WARNING ]
/usr/lib/dbus-1.0/dbus-daemon-launch-helper


[*] CHECK 5: Files where Setgid is used      [ WARNING ]
/usr/bin/mail-lock
/usr/bin/mail-unlock
/usr/bin/mail-touchlock
/usr/bin/dotlockfile
/usr/sbin/postqueue
/usr/sbin/postdrop


[*] CHECK 6: Check umask                     [ WARNING ]
0027


[*] CHECK 7: Find superusers                 [ OK ]


[*] CHECK 8: Check firewall policies         [ OK ]


[*] CHECK 9: Check if sshd is secured        [ OK ]


[*] CHECK 10: Search problematic packages    [ WARNING ]
nmap
```

Source: *http://www.buck-security.net*

Password Management

- Use strong **"root"** passwords according to the organization's policy
- The **default system** password policy should match your organization's password policy
- Go to the **/etc/login.defs** file to view and change the default password policy settings per the organization's password policy
- Use following command to view and change the default password policy settings
  - `# sudo vi /etc/logins.defs`

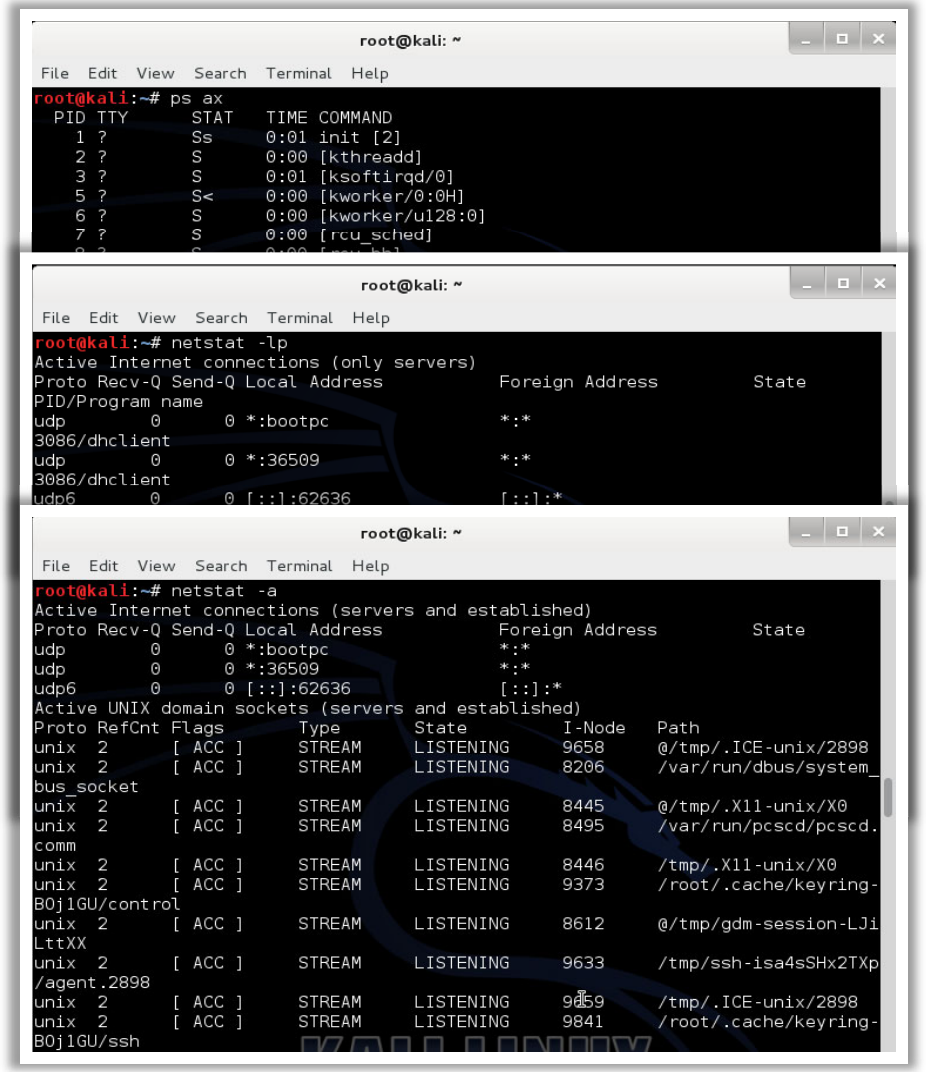


```
#
# /etc/login.defs - Configuration control definitions for the login package.
#
# Three items must be defined:  MAIL_DIR, ENV_SUPATH, and ENV_PATH.
# If unspecified, some arbitrary (and possibly incorrect) value will
# be assumed.  All other items are optional - if not specified then
# the described action or option will be inhibited.
#
# Comment lines (lines beginning with "#") and blank lines are ignored.
#
# Modified for Linux.  --marekm

# REQUIRED for useradd/userdel/usermod
#   Directory where mailboxes reside, _or_ name of file, relative to the
#   home directory.  If you _do_ define MAIL_DIR and MAIL_FILE,
#   MAIL_DIR takes precedence.
#
#   Essentially:
#      - MAIL_DIR defines the location of users mail spool files
#        (for mbox use) by appending the username to MAIL_DIR as defined
#        below.
#      - MAIL_FILE defines the location of the users mail spool files as the
```

```
PASS_WARN_AGE   7

#
# Min/max values for automatic uid selection in useradd
#
UID_MIN                  1000
UID_MAX                 60000
# System accounts
#SYS_UID_MIN              100
#SYS_UID_MAX              999

#
# Min/max values for automatic gid selection in groupadd
#
GID_MIN                  1000
GID_MAX                 60000
# System accounts
#SYS_GID_MIN              100
#SYS_GID_MAX              999

#
# Max number of login retries if password is bad. This will most likely be
# overriden by PAM, since the default pam_unix module has it's own built
                                                          162,2         50%
```

Disabling Unnecessary Services

- Know what **types of services** are running on your system
  - `#ps ax`
- Know the processes that are **accepting connections** and a list of open ports
  - `# netstat –lp`
  - `# netstat –a`
- Use the following commands to disable unwanted services on **Red Hat, Fedora, and Red Hat based Linux distributions**
  - `# chkconfig [service name]off`
  - `# chkconfig [service name] –del`
  - `# service [service name] stop`
- Use the following commands to disable unwanted services on **Debian, Ubuntu, and other Debian based Linux distributions**
  - `# update-rc.d -f [service name] remove`



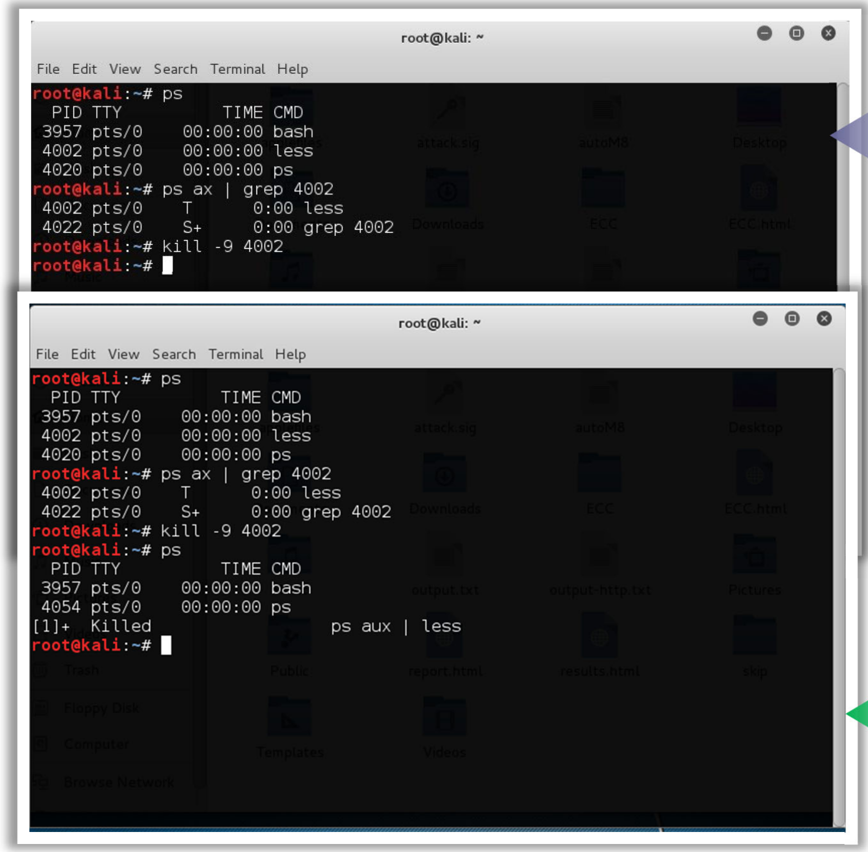
```
root@kali:~# ps ax
  PID TTY      STAT   TIME COMMAND
    1 ?        Ss     0:01 init [2]
    2 ?        S      0:00 [kthreadd]
    3 ?        S      0:01 [ksoftirqd/0]
    5 ?        S<     0:00 [kworker/0:0H]
    6 ?        S      0:00 [kworker/u128:0]
    7 ?        S      0:00 [rcu_sched]
```

```
root@kali:~# netstat -lp
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
PID/Program name
udp        0      0 *:bootpc                *:*
3086/dhclient
udp        0      0 *:36509                 *:*
3086/dhclient
udp6       0      0 [::]:62636              [::]:*
```

```
root@kali:~# netstat -a
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
udp        0      0 *:bootpc                *:*
udp        0      0 *:36509                 *:*
udp6       0      0 [::]:62636              [::]:*
Active UNIX domain sockets (servers and established)
Proto RefCnt Flags       Type       State         I-Node   Path
unix  2      [ ACC ]     STREAM     LISTENING     9658     @/tmp/.ICE-unix/2898
unix  2      [ ACC ]     STREAM     LISTENING     8206     /var/run/dbus/system_
bus_socket
unix  2      [ ACC ]     STREAM     LISTENING     8445     @/tmp/.X11-unix/X0
unix  2      [ ACC ]     STREAM     LISTENING     8495     /var/run/pcscd/pcscd.
comm
unix  2      [ ACC ]     STREAM     LISTENING     8446     /tmp/.X11-unix/X0
unix  2      [ ACC ]     STREAM     LISTENING     9373     /root/.cache/keyring-
BOj1GU/control
unix  2      [ ACC ]     STREAM     LISTENING     8612     @/tmp/gdm-session-LJi
LttXX
unix  2      [ ACC ]     STREAM     LISTENING     9633     /tmp/ssh-isa4sSHx2TXp
/agent.2898
unix  2      [ ACC ]     STREAM     LISTENING     9659     /tmp/.ICE-unix/2898
unix  2      [ ACC ]     STREAM     LISTENING     9841     /root/.cache/keyring-
BOj1GU/ssh
```

Killing Unnecessary Processes

Use the **‘Kill PID‘** command to kill unwanted processes



root@kali: ~

```
root@kali:~# ps
  PID TTY          TIME CMD
 3957 pts/0    00:00:00 bash
 4002 pts/0    00:00:00 less
 4020 pts/0    00:00:00 ps
root@kali:~# ps ax | grep 4002
 4002 pts/0    T      0:00 less
 4022 pts/0    S+     0:00 grep 4002
root@kali:~# kill -9 4002
root@kali:~# 
```

root@kali: ~

```
root@kali:~# ps
  PID TTY          TIME CMD
 3957 pts/0    00:00:00 bash
 4002 pts/0    00:00:00 less
 4020 pts/0    00:00:00 ps
root@kali:~# ps ax | grep 4002
 4002 pts/0    T      0:00 less
 4022 pts/0    S+     0:00 grep 4002
root@kali:~# kill -9 4002
root@kali:~# ps
  PID TTY          TIME CMD
 3957 pts/0    00:00:00 bash
 4054 pts/0    00:00:00 ps
[1]+  Killed                  ps aux | less
root@kali:~# 
```

1

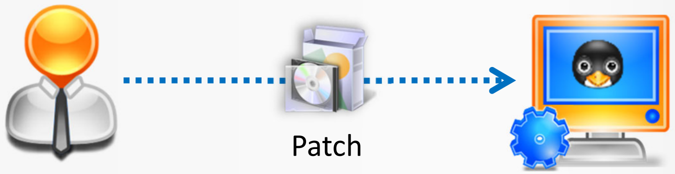
- Knowing **PID** of target process
  - ➢ `#ps ax | grep [Target Process]`

2

- **Killing** target process
  - ➢ `#kill -9 [PID]`

Linux Patch Management

- **Update or patch** your Linux system in one of the following ways:
  1. Download **updated packages** from a distribution's website and manually install it on your system
     - Check your **distribution's website** for the latest patch and update
  2. Download and install updates using third-party applications



- Most Linux distributions come with a command line or even graphic software to update your Linux system
  - Use the following tools to update your Linux system
    - Use **`up2date`** for Red Hat based Linux distributions
    - Use **`apt-get`** for Debian based Linux distributions
    - Use **`swaret`** for Slackware based Linux distributions
    - Use **`autoupdate`** for other RPM-based Linux distributions

File System Security: Unix/Linux

Components of Unix/Linux File System Security

- File Permission
- Account Permission
- File Permissions
- Access control List

Attributes of Setting File System Permission

- Owner Permission-
- Group Permission-
- Other permission-

File System Access Protection

- **Read-** Read File or Directory content
- **Write-** Write data to a file or change the content of directory
- **Execute-** Run Executable program or search content of folder or subdirectory

Setting Permission for File or Directory

- **Symbolic Mode** e.g. chmod g + rw here (g=group, +-=operation such as add, remove, set & rw read write)
- **Absolute Mode** e.g. chmod u=rwx,g=rx,o=r row* (it will apply to all rows current directory)

Understanding and Checking Linux File Permissions

- Type **ls -l** command to list out list of files and their permissions under home directory

Types of permissions

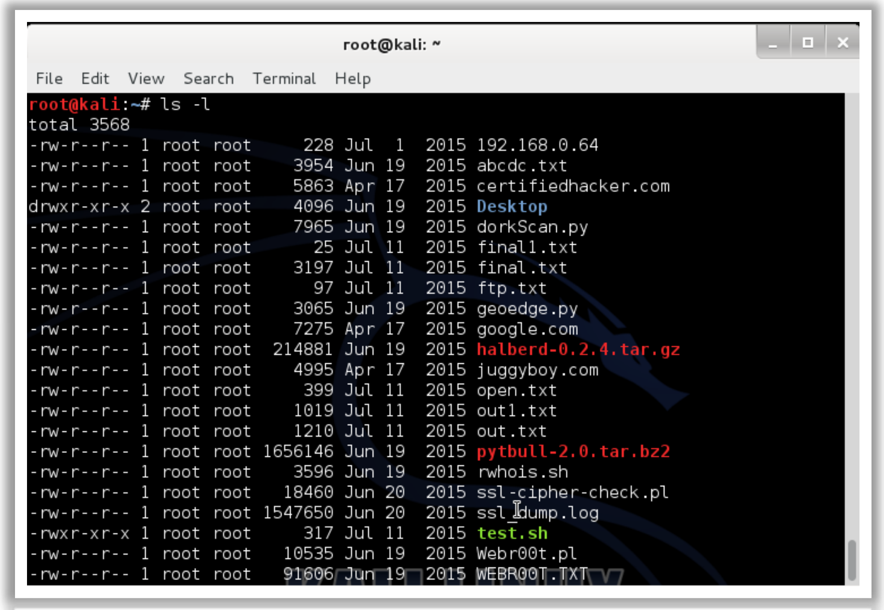
- r →denotes read permission
- w → denotes write permission
- x →denotes execute permission
- - refers to No permission.

Permission details::

- The first character in the directory list denotes file type(d, if directory)
- The next three characters denote user permissions.
- The next three characters denote group permissions.
- The final three characters denote other permissions

Permission Groups: Owner and group

- First name after number is Owner name
- Second name after number id group name



```
root@kali:~# ls -l
total 3568
-rw-r--r-- 1 root root     228 Jul  1  2015 192.168.0.64
-rw-r--r-- 1 root root    3954 Jun 19  2015 abcdc.txt
-rw-r--r-- 1 root root    5863 Apr 17  2015 certifiedhacker.com
drwxr-xr-x 2 root root    4096 Jun 19  2015 Desktop
-rw-r--r-- 1 root root    7965 Jun 19  2015 dorkScan.py
-rw-r--r-- 1 root root      25 Jul 11  2015 final1.txt
-rw-r--r-- 1 root root    3197 Jul 11  2015 final.txt
-rw-r--r-- 1 root root      97 Jul 11  2015 ftp.txt
-rw-r--r-- 1 root root    3065 Jun 19  2015 geoedge.py
-rw-r--r-- 1 root root    7275 Apr 17  2015 google.com
-rw-r--r-- 1 root root  214881 Jun 19  2015 halberd-0.2.4.tar.gz
-rw-r--r-- 1 root root    4995 Apr 17  2015 juggyboy.com
-rw-r--r-- 1 root root     399 Jul 11  2015 open.txt
-rw-r--r-- 1 root root    1019 Jul 11  2015 out1.txt
-rw-r--r-- 1 root root    1210 Jul 11  2015 out.txt
-rw-r--r-- 1 root root 1656146 Jun 19  2015 pytbull-2.0.tar.bz2
-rw-r--r-- 1 root root    3596 Jun 19  2015 rwhois.sh
-rw-r--r-- 1 root root   18460 Jun 20  2015 ssl-cipher-check.pl
-rw-r--r-- 1 root root 1547650 Jun 20  2015 ssl_dump.log
-rwxr-xr-x 1 root root     317 Jul 11  2015 test.sh
-rw-r--r-- 1 root root   10535 Jun 19  2015 Webr00t.pl
-rw-r--r-- 1 root root   91606 Jun 19  2015 WEBR00T.TXT
```

Changing File Permissions

- Check for permission on **sensitive files**
- Use **chmod** command to change the permissions of a file or directory
  - `chmod [permission Value] [File Name]`

Common Directory Permission Settings

Value	Meaning
777	(rwxrwxrwx) No restrctions on permissions. Anybody can list files, create new files in the directory, and delete files in the directory
755	(Rwxr-xr-x) The directory owner has full access. All others can list the directory but cannot read or delete it. This setting is useful for directories that you wish to share with other users
700	(Rwx------) The directory owner has full access. Nobody else has any rights. This setting is useful for directories that only the user can use and must be kept private from others

Common File Permission Settings

Value	Meaning
777	(Rwxrwxrwx) No restrcitions on anything. Anybody can do anything. Generally, not a desirable setting
755	(Rwxr-xr-x) The file owner may read, write, and execute the file. Others can read and execute the file. This setting is useful for all programs that are used by all users
700	(Rwx------)The file owner my read, write, and execute the file. Nobody else has any rights. This setting is useful for programs that only user may use and are kept private from others
666	(rw-rw-rw) All users can read and write the file
644	(rw-r—r--) The owner can read and write a file, while others may only read the file. A very common setting where everybody may read but only the owner can make changes
600	(rw-------) Owner can read and write a file. Others have no rights. A common setting for files that the owner wants to keep private

Check and Verify Permissions for Sensitive Files and Directories

Permission	File Pathname	Description
600	/boot/grub/menu.lst	GRUB boot loader menu file
400	/etc/cron.allow	List of users permitted to use cron to submit periodic jobs
400	/etc/cron.deny	List of users who can’t use cron to submit periodic jobs
644	/etc/crontab	System-wide periodic jobs
644	/etc/hosts.allow	List of hosts allowed to use internet services that are started using TCP wrappers
644	/etc/hosts.deny	List of hosts denied access to internet services that are started using TCP wrappers
644	/etc/logrotate.conf	File that controls how log files rotate
644	/etc/xinetd.conf	Configuration file for xinetd server
755	/etc/xinetd.d	Directory containing configuration files for specific
755	/var/log	Directory with all log files
644	/var/log/lastlog	Information about all previous logins
644	/var/log/messages	Main system message log file
664	/var/log/wtmp	Information about current logins
755	/etc/pam.d	Directory with configuration files for pluggable authentication modules (PAMs)

Source: *http://www.dummies.com*

Check and Verify Permissions for Sensitive Files and Directories (Cont'd)

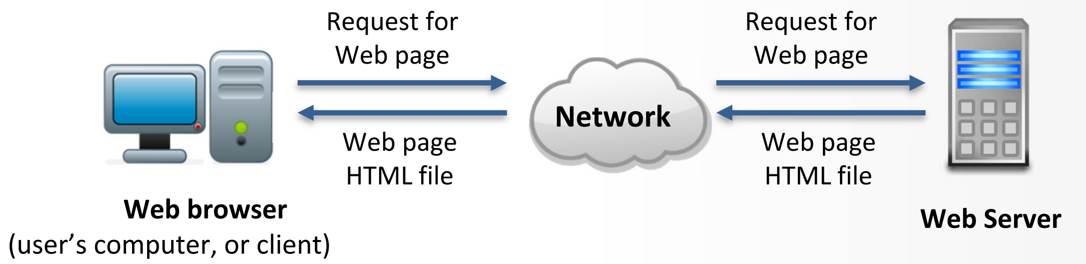
Permission	File Pathname	Description
644	/etc/passwd	Old-style password file with user account information but not the passwords
755	/etc/rc.d	Directory with system-startup scripts
600	/etc/securetty	TTY interfaces (terminals) from which root can log in
755	/etc/security	Policy files that control system access
400	/etc/shadow	Files with encrypted passwords and password expiration information
400	/etc/shutdown.allow	Users who can shut down or reboot by pressing Ctrl+Alt+Delete
755	/etc/ssh	Directory with configuration files for the Secure Shell (SSH)
755	/etc/sysconfig	System configuration files
644	/etc/sysct1.conf	Kernel configuration parameters
644	/etc/syslog.conf	Configuration file for the syslogd server that logs messages
644	/etc/udev/udev.conf	Configuration file for udev – the program that provides the capability to dynamically name hot-pluggable devices and create the device files in the /dev directory
600	/etc/vsftpd	Configuration file for the very secure FTP server
600	/etc/vsftpd.ftpusers	List of users who are not allowed to use FTP to transfer files

Source: *http://www.dummies.com*

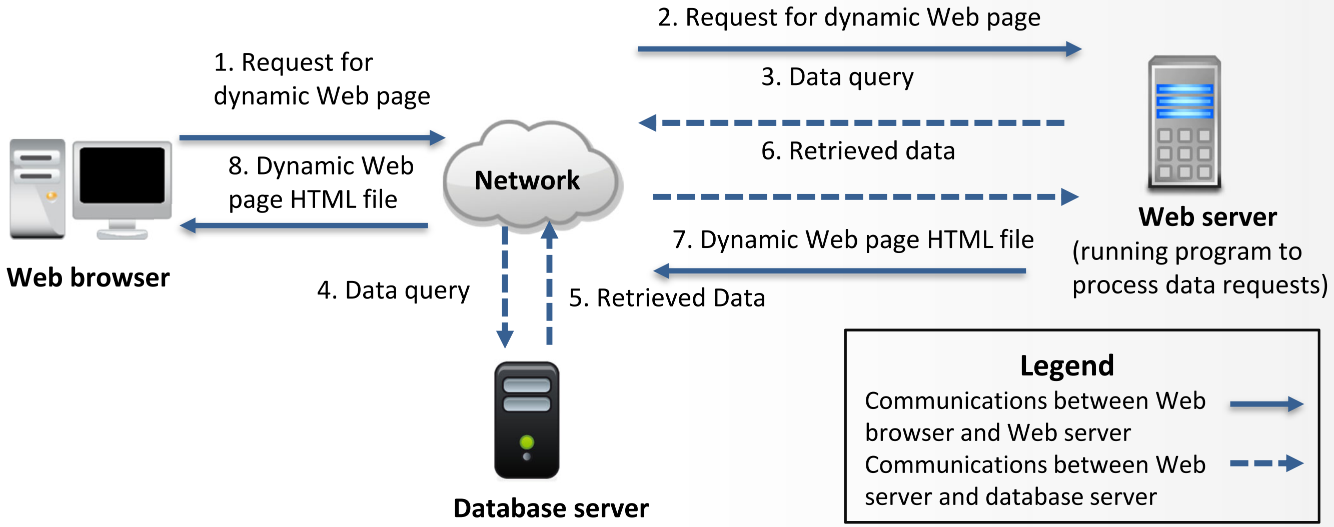
Web Application Fundamentals

Overview of Web Application Architecture

- A web application or web app is a client-server computer program where the client requests a web page and the server retrieves the requested page
- Web Browser running on the user's system represents the client
- The web server sits remotely on the internet and hosts the application
- The communication between client and server takes place using HTTP protocol
- Web browsers are the software program used to retrieve, transfer and present information on World Wide Web (WWW)
- Web servers is a computer program (hardware, software or both) which accepts request from the client and sends the response back to the client

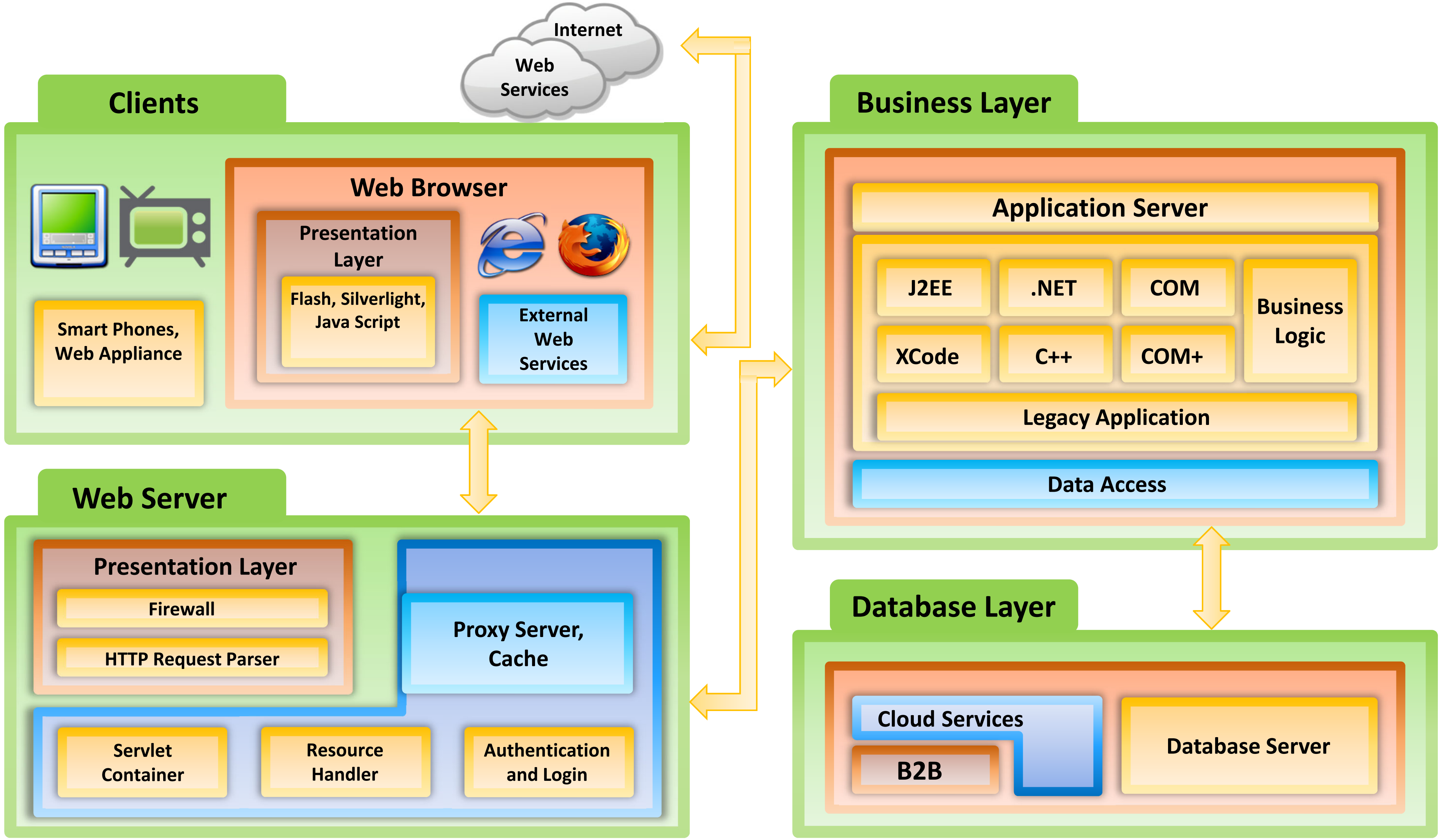


2-Tier Web Application Architecture


2. Request for dynamic Web page
1. Request for dynamic Web page
3. Data query
6. Retrieved data
8. Dynamic Web page HTML file
Network
Web server
(running program to process data requests)
7. Dynamic Web page HTML file
Web browser
4. Data query
5. Retrieved Data
Database server
Legend
Communications between Web browser and Web server
Communications between Web server and database server

3-Tier Web Application Architecture

Web Application Architecture

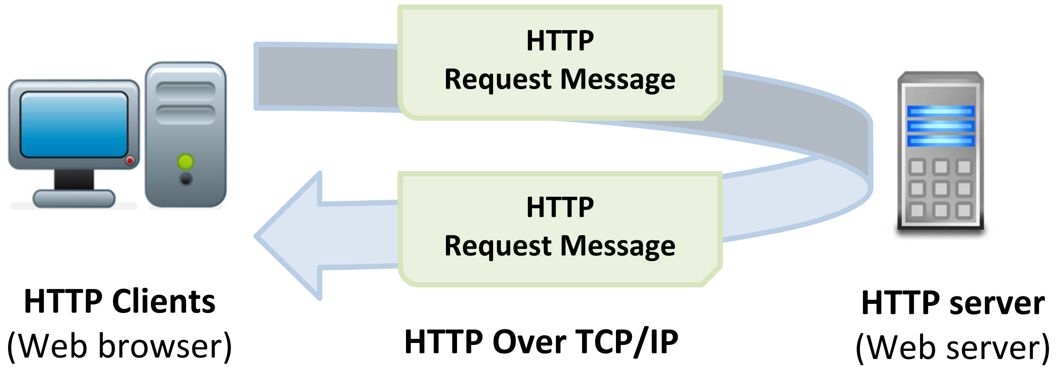


HTTP Communication

1. Hypertext Transfer Protocol (HTTP) lays the foundation for communication on World Wide Web(WWW)
2. It is the standard application protocol on the top of the TCP/IP stack, handling web browser requests and web server responses
3. It is used to transfer data (audio, video, images, hypertext, plain text, etc.) between the client and the server
4. HTTP messages are exchanged between the client and the server during communication
5. The client sends HTTP request messages to the server, and then the server sends HTTP response messages back to the client

Characteristics:

- It follows request response mechanism
- It is media independent
- It is connectionless
- It is stateless
- It uses TCP connection by default on TCP port 80



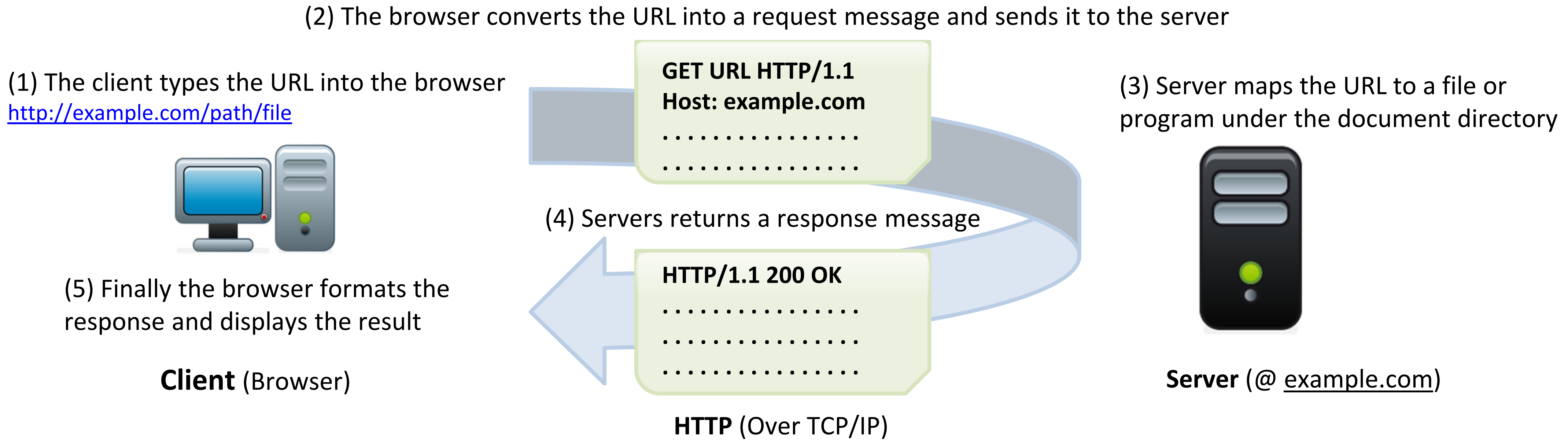
Exchange of HTTP Request and Response Messages

01 Client issue URL from the browser

02 Browser converts this URL into request message and sends it to server

03 The HTTP server reads the request message and returns the appropriate response message

04 Finally browser formats the response and displays the result



(2) The browser converts the URL into a request message and sends it to the server

(1) The client types the URL into the browser
http://example.com/path/file

```
GET URL HTTP/1.1
Host: example.com
. . . . . . . . . . . . . . . .
. . . . . . . . . . . . . . . .
```

(3) Server maps the URL to a file or program under the document directory

(4) Servers returns a response message

```
HTTP/1.1 200 OK
. . . . . . . . . . . . . . . .
. . . . . . . . . . . . . . . .
. . . . . . . . . . . . . . . .
```

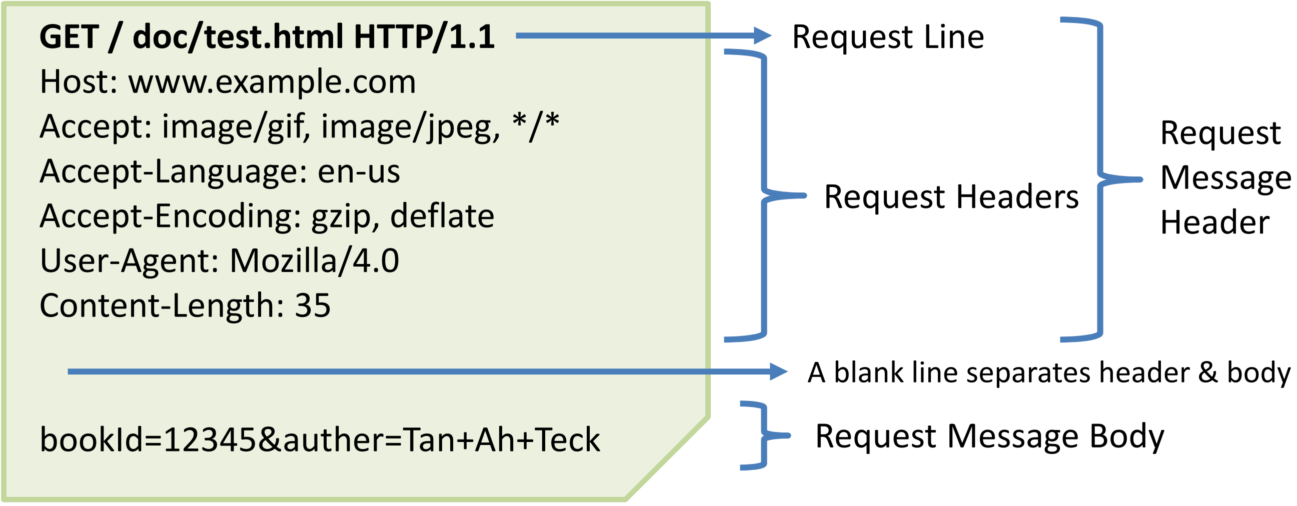
(5) Finally the browser formats the response and displays the result

Client (Browser)

HTTP (Over TCP/IP)

Server (@ example.com)

HTTP Request Message Format



```
GET / doc/test.html HTTP/1.1
Host: www.example.com
Accept: image/gif, image/jpeg, */*
Accept-Language: en-us
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0
Content-Length: 35

bookId=12345&auther=Tan+Ah+Teck
```

Request Line

Request Headers

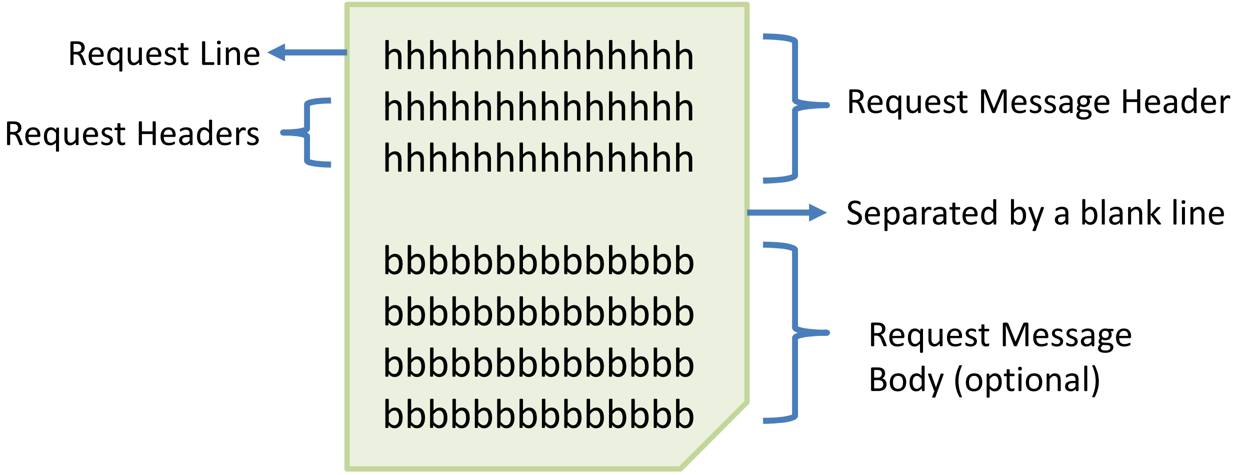
Request Message Header

A blank line separates header & body

Request Message Body

- The syntax of request line is ***request-method-name request-URI HTTP-version***
- *request-**method-name***: specifies the method used to send the request
- *request-**URI***: specifies the requested resource
- *HTTP-**version***: specifies the version of the HTTP in the session, generally HTTP/1.0 or HTTP/1.1

- The syntax of request header is in the name – value pair form
- *request-**header-name***: *request-header-value1, request-header-value2*



Request Line

Request Headers

```
hhhhhhhhhhhhh
hhhhhhhhhhhhh
hhhhhhhhhhhhh

bbbbbbbbbbbbb
bbbbbbbbbbbbb
bbbbbbbbbbbbb
bbbbbbbbbbbbb
```

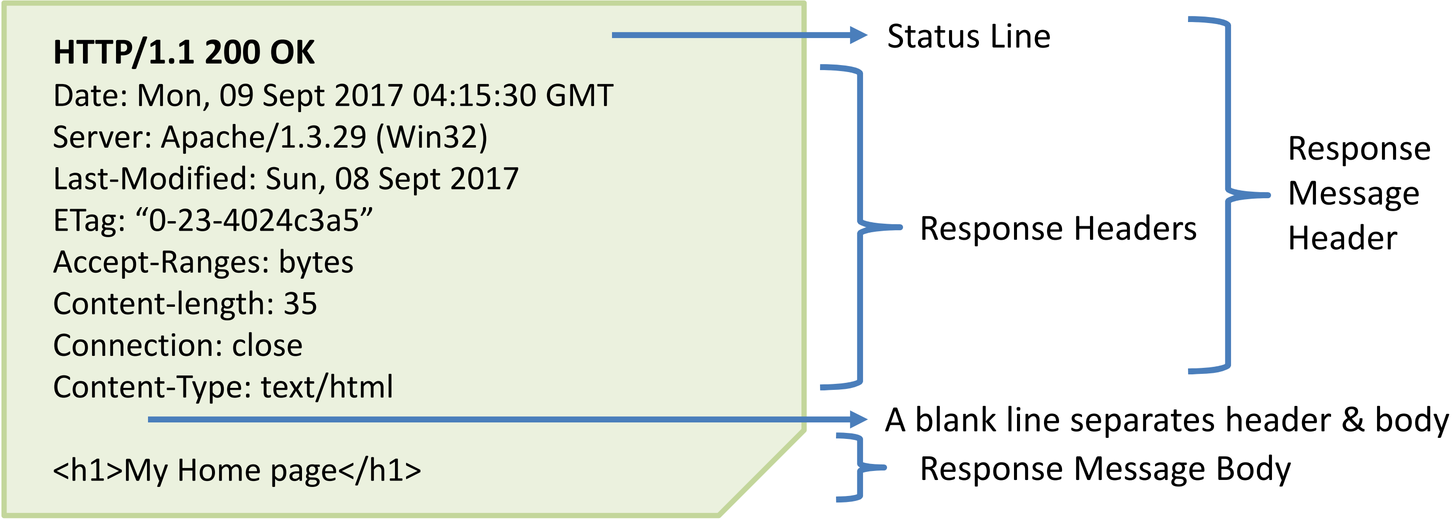
Request Message Header

Separated by a blank line

Request Message Body (optional)

HTTP Request Message

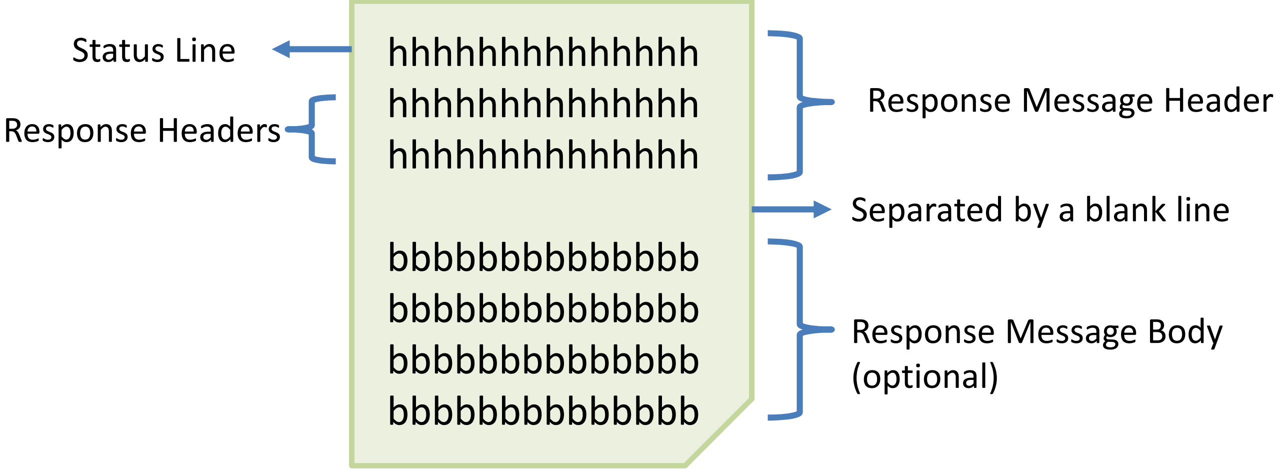
HTTP Response Message Format



```
HTTP/1.1 200 OK
Date: Mon, 09 Sept 2017 04:15:30 GMT
Server: Apache/1.3.29 (Win32)
Last-Modified: Sun, 08 Sept 2017
ETag: “0-23-4024c3a5”
Accept-Ranges: bytes
Content-length: 35
Connection: close
Content-Type: text/html

<h1>My Home page</h1>
```

- The syntax of status line is ***HTTP-version status-code reason-phrase***
- *HTTP-**version***: Specifies the version used in the session
- *status-**code***: 3 digit number specifies the result of the request
- *reason-**phrase***: provides a short explanation of status code

- The syntax of response header is in the name – value pair form
- *response-**header-name***: *response-header-value1, request-header-value2*



HTTP Response Message

HTTP Message Parameters

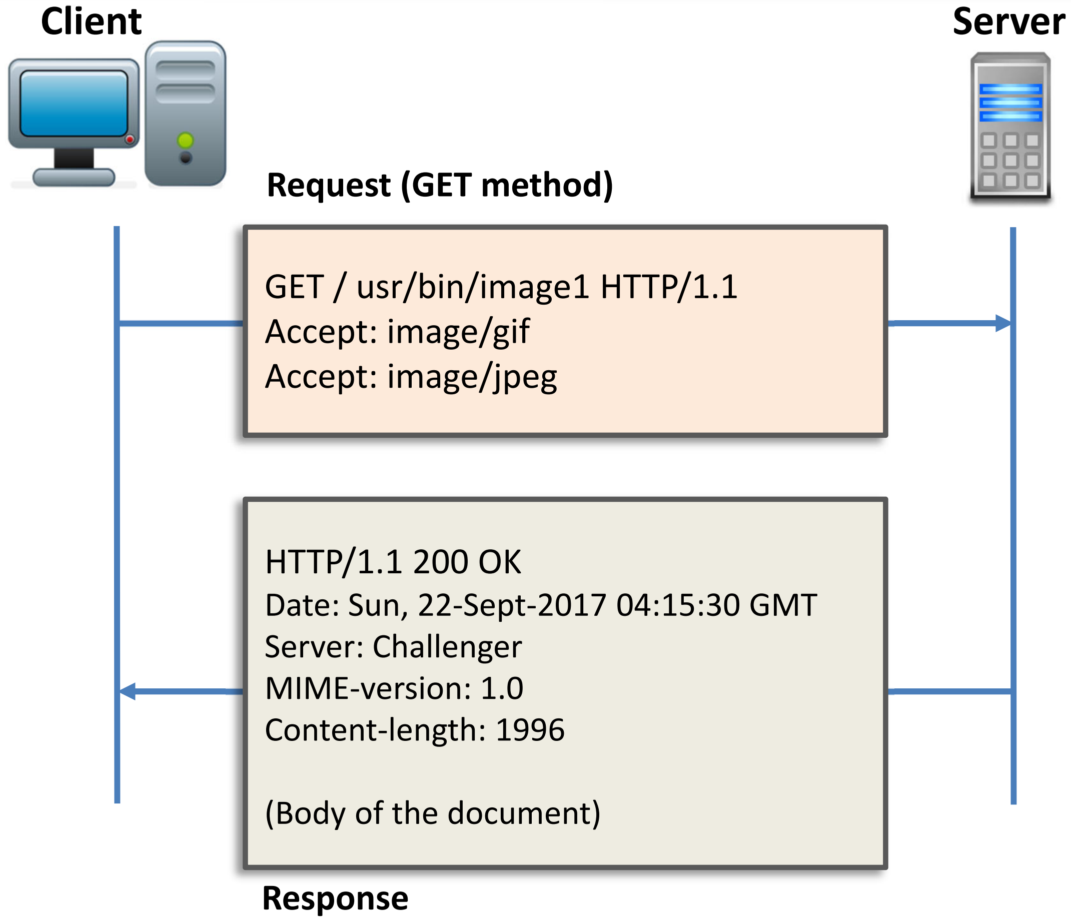
HTTP Parameters	Description	Syntax	Example
HTTP version	<major>.<minor> numbering scheme is used to indicate the version of HTTP protocol	HTTP-Version = “HTTP” “/” 1*DIGIT “.” 1*DIGIT	HTTP/1.0, HTTP/1.1
Uniform resource identifier (URI)	It is a string character containing name, location, etc. to identify resources	URI = “http:” “//” host [“:” port] [abs path [“?” query]]	http://XYZ.com/%9Ejohn/home.html
Date/time formats	Greenwich mean time (GMT) is used to represent the date/time format	Date = "Date" ":" HTTP-date	Sun, 09 Sept 1991 04:15:30 GMT ; RFC 822, updated by RFC 1123
Character sets	It is used to specify the character sets that the client prefers	—	US-ASCII, ISO-8859-1
Content encoding	It is used to encode the content before passing it on the network	—	Accept-Encoding : compress
Media types	It is used to provide open and extensible data typing and type negotiation	media-type = type “/” subtype *(“;” parameter)	Accept : image/gif
Language tags	HTTP uses language tags within Accept-Language and Content-Language fields	Language-tag = primary-tag *(“-” suntag)	en, en-US, en-cockney, i-cherokee

HTTP Request Methods

Request Methods	Action
GET	Requests a document from server
HEAD	Requests information about document
POST	Sends information from client to the server
PUT	Sends document from the server to the client
TRACE	Echoes the incoming request
CONNECT	Establishes connection to the server
OPTION	Inquires about available option
DELETE	Removes all existing representations

HTTP GET and POST Request Method

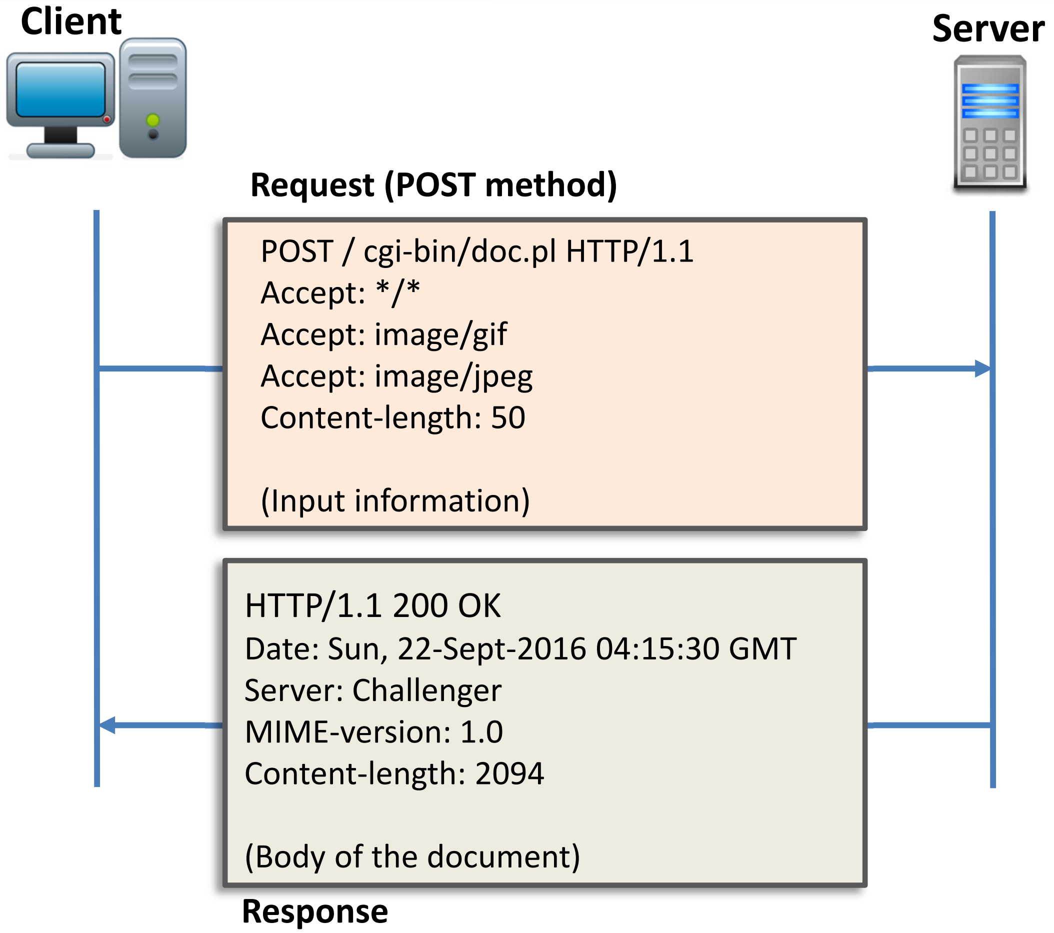
HTTP Request and Response messages, when client uses the GET method to send the data to the server.



```
GET / usr/bin/image1 HTTP/1.1
Accept: image/gif
Accept: image/jpeg
```

```
HTTP/1.1 200 OK
Date: Sun, 22-Sept-2017 04:15:30 GMT
Server: Challenger
MIME-version: 1.0
Content-length: 1996

(Body of the document)
```

HTTP Request and Response messages, when client uses the POST method to send the data to the server

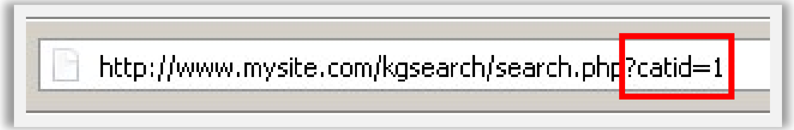


```
POST / cgi-bin/doc.pl HTTP/1.1
Accept: */*
Accept: image/gif
Accept: image/jpeg
Content-length: 50

(Input information)
```

```
HTTP/1.1 200 OK
Date: Sun, 22-Sept-2016 04:15:30 GMT
Server: Challenger
MIME-version: 1.0
Content-length: 2094

(Body of the document)
```

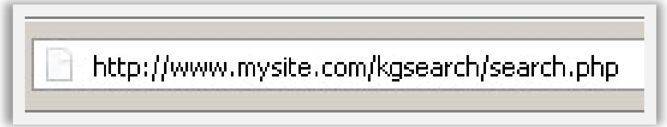
HTTP GET and POST Request Method (Cont'd)

When client uses the GET method for the request, the data is sent in the URL



http://www.mysite.com/kgsearch/search.php?catid=1

When client uses POST method for the request, the data is sent in the body of the request



http://www.mysite.com/kgsearch/search.php

Request Message

```
GET http://www.mysite.com/kgsearch/search.php?catid=1 HTTP/1.1
Host: www.mysite.com
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.8.1.13)
Gecko/20080311 Firefox/2.0.0.13
Accept:
text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q
=0.8,image/png,*/*;q=0.5
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 300
Connection: keep-alive
Referer: http://www.mysite.com/
```

```
POST http://www.mysite.com/kgsearch/search.php HTTP/1.1
Host: www.mysite.com
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.8.1.13)
Gecko/20080311 Firefox/2.0.0.13
Accept:
text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=
0.8,image/png,*/*;q=0.5
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 300
Connection: keep-alive
Referer: http://www.mysite.com/

catid=1
```

HTTP Response Status Codes and Phrases

Following are values for first digit integer of status code:

1. **1xx: Informational**: This indicates that request was received and the process is continuing
2. **2xx: Success**: This indicates action was received, understood, and accepted
3. **3xx: Redirection**: This indicates the next action needed to complete the request
4. **4xx: Client Error**: This indicates the request contains an incorrect syntax
5. **5xx: Server Error**: This indicates that the server failed to fulfill the request

1xx: Informational

Code	Message	Description
100	Continue	The initial part of the request has been received, and the client may continue with request.
101	Switching	The server is complying with a client request to switch protocols defined in upgrade header

HTTP Response Status Codes and Phrases (Cont'd)

Certified SOC Analyst

2xx: Success

Code	Message	Description
200	OK	The request is successful
201	Created	A new URL is created
202	Accepted	The request is accepted, but it is not immediately acted upon
203	Non authoritative information	Specifies that the request is completed but the enclosed payload has been changed from the origin server's 200 (OK) response by a transforming proxy.
204	No Comment	Indicates that there is no content in the body
205	Reset content	Instructs the client to reset the document view
206	Partial content	Instructs the client that the request has finished and the body includes the requested ranges of data Indicates that the requested URL is no longer used by the server

3xx: Redirection

Code	Message	Description
300	Multiple choices	Specifies that the request has more than one possible response
301	Moved permanently	Indicates that the requested URL is no longer used by the server
302	Found	Indicates that the requested URL has moved temporarily
303	See other	Notifies the client that the redirects have not linked to the newly uploaded resources but to another page
304	Not modified	The document has not been modified
307	Temporary redirect	Instructs the client that the resource requested has been temporarily moved to the URL given by the location headers.

HTTP Response Status Codes and Phrases (Cont'd)

4xx: Client Error

Code	Message	Code	Message
400	Bad request	**409**	Conflict
401	Unauthorized	**410**	Gone
402	Payment required	**411**	Length required
403	Forbidden	**412**	Precondition failed
404	Not found	**413**	Request entity too large
405	Method not allowed	**414**	Request URL too large
406	Not acceptable	**415**	Unsupported media type
407	Proxy authentication required	**416**	Requested range not satisfiable
408	Request timeout	**417**	Expectation failed

5xx: Server Error

Code	Message	Description
500	Internal error	There is an error such as crash~~,~~ on the server side
501	Not implemented	The action requested cannot be performed
502	Bad gateway	The request was not completed
503	Service unavailable	The service is temporarily unavailable, but may be requested in future
504	Gateway timeout	The gateway has timed out
505	HTTP version Not supported	The server is not supported on this version of HTTP protocol

HTTP Header Fields: General Header

- **These General headers** are used in both request and response messages

HTTP headers	Description
Cache-control	It specifies information about the web browser cache
connection	It shows whether connections are closed or not
Date	It shows the current date
pragma	It is used to include the implementation specific directives
Trailer	It shows a given set of header fields present in the trailer of the message encoded with chunk transfer coding
Transfer-Encoding	It shows the type of transformation applied to the message body for safe communication
Upgrade	It specifies the preferred communication protocol
Via	It is used to indicate the intermediate protocol and recipient by gateway
Warning	It is used to carry additional information about status

HTTP Header Fields: Request Header

Request Headers	Description	Request Headers	Description
Accept-Charset	Shows the character set that the client can handle	**If-None-Match**	Sends the document only if it does not match a given tag
Accept-Encoding	Shows the encoding scheme that the client can handle	**If-Range**	Sends only the portion of the document that is missing
Accept-Language	Shows the language that the client can accept	**If-Unmodified-Since**	Sends the document if it has not changed since specified date
Authorization	Shows what permission the client has	**If-Match**	Sends the document only if it matches given tag
Expect	It is used to indicate the behavior of a particular server	**If-Modifies-Since**	Sends the document if newer than specifies date
From	Shows the email address of the user	**Referrer**	Specifies the URL of the linked document
Host	Shows the host number and port number of the server	**User-Agent**	Identifies the client program

HTTP Header Fields: Response Header

Response headers	Description
Accept-Ranges	It shows the range request accepted by the server
Age	It shows the age of the document
ETag	It gives the entity tag
Location	It is used to redirect the recipient to the location
Proxy-Authenticate	It is included as a part of a 407 response
Retry-After	It states the date after which the server is available
Server	It shows the server name and version number
Vary	It states that the entity has multiple sources
WWW-Authenticate	It should be included in the 401 response message

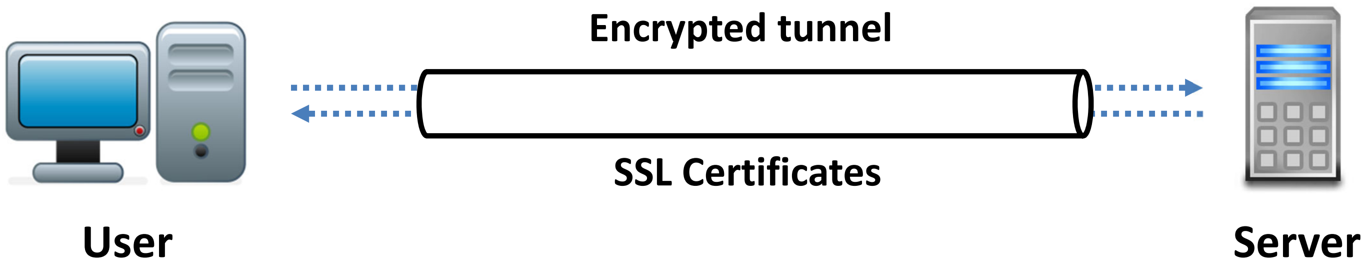
HTTP Header Fields: Entity Header

- **Entity header:** It defines meta information about entity-body

Entity header	Description
Allow	Lists valid methods that are used with the URL
Content-Encoding	It states the encoding scheme used
Content-Language	It states the language used
Content-Length	It states the length of the document
Content-Location	It states the document location
Content-MD5	It is used to supply the MD5 digest algorithms of the entity
Content-Range	It states the range of the document
Content-Type	It states the medium type
Expires	It gives the date and time of the content change
Last-modified	It gives the date and time of the last change

An Overview to HTTPS Protocol

- HTTPS (Hypertext Transfer Protocol over Secure Socket Layer) or HTTP over SSL is a secure version of HTTP
- It is a communication protocol used for secure communication over the internet
- It uses Transport Layer Security or its predecessor, Secure Socket Layer, in order to encrypt and decrypt the connection between the web browser and website
- HTTPS connections securely encrypt and decrypt all of the message in order to exchange sensitive information and ~~to~~ prevent unauthorized access



Encrypted tunnel

SSL Certificates

User

Server

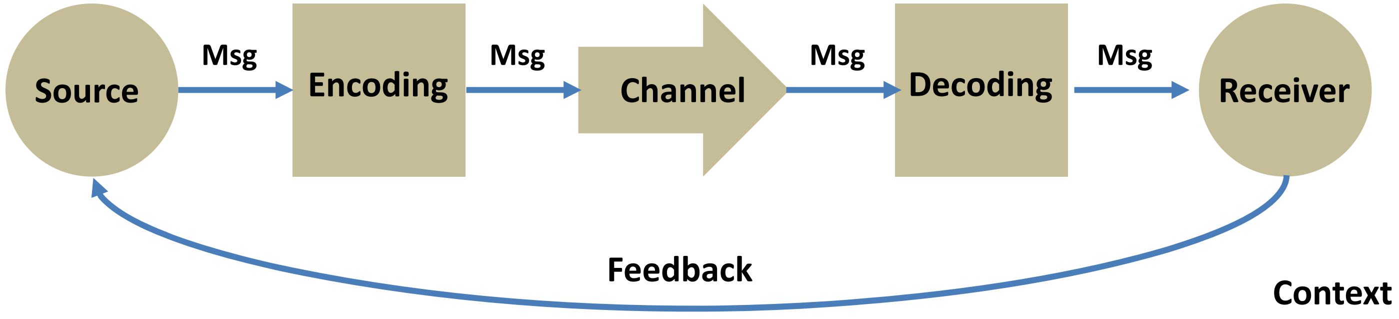
Encoding and Decoding

1. Encoding and decoding plays an important role in web communication

2. Encoding converts the body of message into a specialized format for secure transmission

3. URL encoding, ASCII encoding, HTML encoding, Unicode encoding, etc., are the different encoding techniques used to encode message transmitted between the client and the server

4. Decoding means converting an encoded message back into the unencrypted original message



Encoding Techniques

ASCII

- ASCII, which stands for American Standard Code for Information Interchange, is a fixed length code for the numerical representation of the alphabet, numeric and punctuation characters

Unicode

- Unicode encoding encodes a character from any language or writing system
- Unicode encoding includes various encoding schemes like:
  - UTF-8: It uses 1 byte to represent first 128 code points which are ASCII characters and up to 4 byte for other characters
  - UTF-16: It uses 2 bytes for each characters but can only encode the first 65,536 code points
  - UTF-32: It uses 4 bytes for each characters

Encoding Techniques (Cont'd)

HTML Encoding

- HTML encoding is used to represent different characters which can be used in HTML documents
- Characters like <, > are a part of HTML markup which can be used after HTML encoding
- There are two ways to HTML encode characters
  - HTML encoding provides different entities to represent characters that can be part of the markup

    Example: > - &gt;, < - &lt;
  - HTML encode any character using its ASCII code by prefixing it with &# and then using the ASCII decimal value, or prefixing it with &#x and using the ASCII hex value

    Example: < - &#60;, > - &#62;

Hex/ Base 16 Encoding

- In Hex encoding, the hex value of each character is used to represent the collection of all character
- In this encoding, each binary byte is represented with 2 character encoding
- Example: Hex Coding of "**Hello**" can be represented as "**68656C6C6F**"

Encoding Techniques (Cont'd)

URL Encoding

- URL/Percent encoding is a mechanism for encoding information in uniform resource identifier (URI) in specific situation
- URL encoding is performed when the URL contains some printable ASCII characters with special meaning or you want to use characters outside the printable ASCII range
- It is also used in submission of HTML form data in HTTP request
- To apply URL encoding on a character, prefix its hex value with a %. Example: % - %25 , space - %20, tab - %09, = - %3D

Base64

- Base 64 uses only printable characters to represent binary data
- It is not only used to encode user credentials but also to encode email attachments that are transmitted over SMTP
- It further encodes binary data by treating it numerically and translating it into a base 64 representation
- It takes data in blocks of 3 bytes (24 bits) and divides these 24 bits into 4 chunks of 6 bits
- Each chuck is then converted to its respective base 64 value

Differences between Encryption and Encoding

Encryption	Encoding
It is the process of transforming the information in a specific format using some algorithms so that an authorized person can access it	It is a process of changing the data into digitalized form for efficient transmission
It has the ability to maintain confidentiality and reverse the information for security purpose	It maintains data usability and uses which are publicly available
Original data can be retrieved if we know the key and algorithm used during encryption	Original data can be reverted using only encoding algorithm. No need of key
It is used for maintaining data confidentiality	It is used to maintain data usability
AES, Blowfish, RSA these algorithms are used during encryption	ASCII, Unicode, URL Encoding, Base64 these algorithms are used for encoding
Example: One can send the encrypted letter with some confidential information and its decryption key or password via email so the intended user can get that data	Example: Email containing binary data or with some special character

ASCII Control Characters Encoding

ASCII control characters or unprintable characters are mainly used for output control and its ranges from 00-1F hex (0-31 decimal) and 7F (127 decimal)

The complete ASCII Control Characters Encoding table is shown below:

Decimal	Hex Value	Character	URL Encode
0	00		%00
1	01		%01
2	02		%02
3	03		%03
4	04		%04
5	05		%05
6	06		%06
7	07		%07
8	08	backspace	%08

ASCII Control Characters Encoding (Cont'd)

Decimal	Hex Value	Character	URL Encode
9	09	tab	%09
10	0a	linefeed	%0a
11	0b		%0b
12	0c		%0c
13	0d	carriage return	%0d
14	0e		%0e
15	0f		%0f
16	10		%10
17	11		%11
18	12		%12
19	13		%13
20	14		%14
21	15		%15
22	16		%16
23	17		%17
24	18		%18
25	19		%19
26	1a		%1a
27	1b		%1b
28	1c		%1c
29	1d		%1d
30	1e		%1e
31	1f		%1f
127	7f		%7f

Non-ASCII Control Characters Encoding

- ❑ Non-ASCII control characters are outside the ASCII character set of 128 characters.
- ❑ It includes the complete "top half" of the ISO-Latin set 80-FF hex (128-255 decimal)

- ❑ The complete non-ASCII control characters encoding table is shown below:

Decimal	Hex Value	Character	URL Encode
128	80	€	%80
129	81		%81
130	82	‚	%82
131	83	ƒ	%83
132	84	„	%84
133	85	…	%85
134	86	†	%86
135	87	‡	%87
136	88	ˆ	%88
137	89	‰	%89
138	8a	Š	%8a
139	8b	‹	%8b
140	8c	Œ	%8c
141	8d		%8d

Non-ASCII Control Characters Encoding (Cont’d)

Decimal	Hex Value	Character	URL Encode
142	8e	Ž	%8e
143	8f		%8f
144	90		%90
145	91	‘	%91
146	92	’	%92
147	93	“	%93
148	94	”	%94
149	95	•	%95
150	96	–	%96
151	97	—	%97
152	98	˜	%98
153	99	™	%99
154	9a	š	%9a
155	9b	›	%9b
156	9c	œ	%9c
157	9d		%9d
158	9e	ž	%9e
159	9f	Ÿ	%9f
160	a0		%a0
161	a1	¡	%a1
162	a2	¢	%a2
163	a3	£	%a3

Non-ASCII Control Characters Encoding (Cont'd)

Decimal	Hex Value	Character	URL Encode
164	a4	¤	%a4
165	a5	¥	%a5
166	a6	¦	%a6
167	a7	§	%a7
168	a8	¨	%a8
169	a9	©	%a9
170	aa	ª	%aa
171	ab	«	%ab
172	ac	¬	%ac
173	ad		%ad
174	ae	®	%ae
175	af	¯	%af
176	b0	°	%b0
177	b1	±	%b1
178	b2	²	%b2
179	b3	³	%b3
180	b4	´	%b4
181	b5	µ	%b5
182	b6	¶	%b6
183	b7	·	%b7
184	b8	¸	%b8
185	b9	¹	%b9

Non-ASCII Control Characters Encoding (Cont'd)

Decimal	Hex Value	Character	URL Encode
186	ba	º	%ba
187	bb	»	%bb
188	bc	¼	%bc
189	bd	½	%bd
190	be	¾	%be
191	bf	¿	%bf
192	c0	À	%c0
193	c1	Á	%c1
194	c2	Â	%c2
195	c3	Ã	%c3
196	c4	Ä	%c4

Decimal	Hex Value	Character	URL Encode
197	c5	Å	%c5
198	c6	Æ	%v6
199	c7	Ç	%c7
200	c8	È	%c8
201	c9	É	%c9
202	ca	Ê	%ca
203	cb	Ë	%cb
204	cc	Ì	%cc
205	cd	Í	%cd
206	ce	Î	%ce
207	cf	Ï	%cf

Non-ASCII Control Characters Encoding (Cont'd)

Decimal	Hex Value	Character	URL Encode
208	d0	Ð	%d0
209	d1	Ñ	%d1
210	d2	Ò	%d2
211	d3	Ó	%d3
212	d4	Ô	%d4
213	d5	Õ	%d5
214	d6	Ö	%d6
215	d7	×	%d7
216	d8	Ø	%d8
217	d9	Ù	%d9
218	da	Ú	%da
219	db	Û	%db
220	dc	Ü	%dc
221	dd	Ý	%dd
222	de	Þ	%de
223	df	ß	%df
224	e0	à	%e0
225	e1	á	%e1
226	e2	â	%e2
227	e3	ã	%e3
228	e4	ä	%e4
229	e5	å	%e5
230	e6	æ	%e6
231	e7	ç	%e7

Non-ASCII Control Characters Encoding (Cont’d)

Decimal	Hex Value	Character	URL Encode
232	e8	è	%e8
233	e9	é	%e9
234	ea	ê	%ea
235	eb	ë	%eb
236	ec	ì	%ec
237	ed	í	%ed
238	ee	î	%ee
239	ef	ï	%ef
240	f0	ð	%f0
241	f1	ñ	%f1
242	f2	ò	%f2
243	f3	ó	%f3
244	f4	ô	%f4
245	f5	õ	%f5
246	f6	ö	%f6
247	f7	÷	%f7
248	f8	ø	%f8
249	f9	ù	%f9
250	fa	ú	%fa
251	fb	û	%fb
252	fc	ü	%fc
253	fd	ý	%fd
254	fe	þ	%fe
255	ff	ÿ	%ff

Reserved Characters Encoding

01

- Reserved characters are the special characters like the dollar sign, ampersand, plus, common, forward slash, colon, semi-colon, equals sign, question mark, and "at" symbol

02

- These characters have different meaning in the URL, so it is required to encode them

- The complete reserved characters encoding table is shown below:

Decimal	Hex Value	Char	URL Encode
36	24	$	%24
38	26	&	%26
43	2b	+	%2b
44	2c	,	%2c
47	2f	/	%2f

Decimal	Hex Value	Char	URL Encode
58	3a	:	%3a
59	3b	;	%3b
61	3d	=	%3d
63	3f	?	%3f
64	40	@	%40

Unsafe Characters Encoding

- ❑ Unsafe characters include space, quotation marks, less than symbol, greater than symbol, pound character, percent character, Left Curly Brace, Right Curly Brace, Pipe, Backslash, Caret, Tilde, Left Square Bracket, Right Square Bracket, Grave Accent
- ❑ It is always required to encode such types of characters
- ❑ The complete unsafe characters encoding table is shown below:

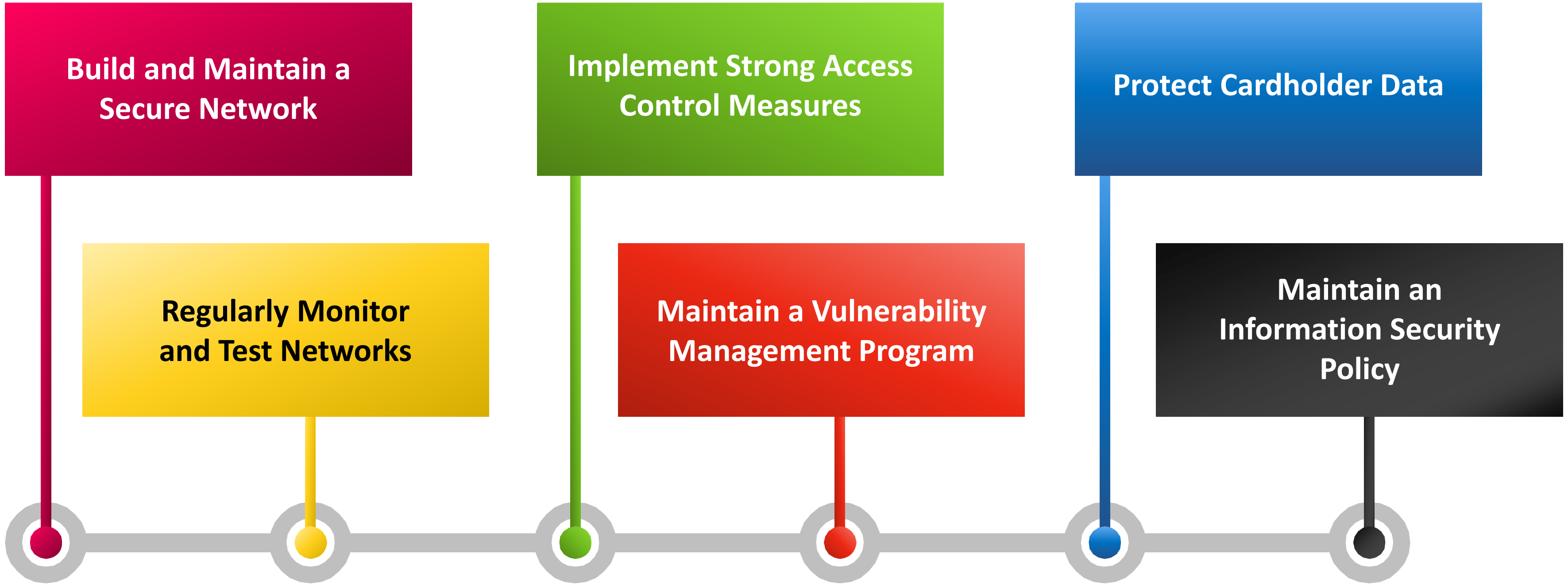
Decimal	Hex Value	Char	URL Encode
32	20	space	%20
34	22	"	%22
60	3c	<	%3c
62	3e	>	%3e
35	23	#	%23
37	25	%	%25
123	7b	{	%7b
125	7d	}	%7d
124	7c	|	%7c
92	5c	\	%5c
94	5e	^	%5e
126	7e	~	%7e
91	5b	[	%5b
93	5d	]	%5d
96	60	`	%60

Information Security Standards, Laws and Acts

Payment Card Industry Data Security Standard (PCI-DSS)

- The Payment Card Industry Data Security Standard (PCI DSS) is a proprietary **information security standard for organizations** that handle cardholder information for the major debit, credit, prepaid, e-purse, ATM, and POS cards
- PCI DSS **applies to all entities involved in payment card processing** – including merchants, processors, acquirers, issuers, and service providers, as well as all other entities that store, process or transmit cardholder data
- High level overview of the PCI DSS requirements developed and maintained by **Payment Card Industry (PCI) Security Standards Council**:

PCI Data Security Standard – High Level Overview



Build and Maintain a Secure Network

Regularly Monitor and Test Networks

Implement Strong Access Control Measures

Maintain a Vulnerability Management Program

Protect Cardholder Data

Maintain an Information Security Policy

Source: *https://www.pcisecuritystandards.org*

Failure to meet the PCI DSS requirements may result in fines or termination of payment card processing privileges

Health Insurance Portability and Accountability Act (HIPAA)

HIPAA's Administrative Simplification Statute and Rules

Electronic Transaction and Code Sets Standards

Requires every provider who does business electronically to **use the same health care transactions**, **code sets**, and **identifiers**

Privacy Rule

Provides **federal protections for personal health information** held by covered entities and gives patients an array of rights with respect to that information

Security Rule

Specifies a series of administrative, physical, and technical safeguards for covered entities to use and assure the **confidentiality**, **integrity**, and **availability of electronic protected health information**

National Identifier Requirements

Requires that health care providers, health plans, and employers have standard national numbers that identify them on **standard transactions**

Enforcement Rule

Provides standards for enforcing all the **Administration Simplification Rules**

Source: *http://www.hhs.gov*

Information Security Acts: Sarbanes Oxley Act (SOX)

- Sarbanes–Oxley is a United States federal law that sets new or enhanced standards for all US public company **boards**, **management,** and **accounting firms**
- The rules and enforcement policies outlined by the SOX Act amend or supplement existing legislation dealing with **security regulations**

Section 302

- A mandate that requires senior management to certify the accuracy of the reported financial statement
- CEOs and CFOs of accounting company's clients must sign statements verifying the completeness and accuracy of the financial reports

Section 404

- A requirement that management and auditors establish internal controls and reporting methods on the adequacy of those controls
- CEOs, CFOs, and auditors must report on, and attest to the effectiveness of internal controls for financial reporting

Information Security Acts: General Data Protection Regulation (GDPR)

The GDPR is a regulation in EU law on **data protection and privacy for all individuals within the European Union** and the European Economic Area. It also addresses the export of personal data outside the EU and EEA areas.

The EU General Data Protection Regulation (GDPR) replaces the Data Protection Directive 95/46/EC **and is designed to:**

- Harmonize data privacy laws across Europe,
- Protect and empower all EU citizens data privacy
- Reshape the way organizations across the region approach data privacy.

Source: https://eugdpr.org

Information Security Acts: Gramm-Leach-Bliley Act (GLBA)

- The objective of the **Gramm-Leach-Bliley Act** was to ease the transfer of **financial** information between **institutions** and **banks** while making the rights of the individual through **security** requirements more specific

Key Points Include:

- Protecting consumer's **personal financial information** held by financial institutions and their service providers
- The officers and directors of the financial institution shall be subject to, and personally liable for, a civil penalty of not more than **$10,000 for each violation**

Although the penalty is small, it is easy to see how it could impact a bank

Information Security Acts: The Digital Millennium Copyright Act (DMCA) and Federal Information Security Management Act (FISMA)

The Digital Millennium Copyright Act (DMCA)

- The DMCA is a United States copyright law that implements two 1996 treaties of the **World Intellectual Property Organization** (WIPO).
- It defines **legal prohibitions** against the circumvention of technological protection measures employed by copyright owners to protect their works, and against the **removal** or **alteration** of copyright management information.

Source: *http://www.copyright.gov*

Federal Information Security Management Act (FISMA)

- The FISMA provides a comprehensive framework for ensuring the **effectiveness of information security controls** over information resources that support Federal operations and assets.
- It includes
  - Standards for **categorizing** information and information systems by mission impact
  - Standards for minimum **security requirements** for information and information systems
  - Guidance for selecting appropriate **security controls** for information systems
  - Guidance for **assessing security controls** in information systems and determining security control effectiveness
  - Guidance for the security authorization of information systems

Source: *http://csrc.nist.gov*

Module Summary

- ❑ TCP/IP model is a framework for the Internet Protocol suite of computer network protocols that define the communication in an IP-based network
- ❑ A firewall is a hardware device and/or software that prevents unauthorized access to or from a private network
- ❑ Patch Management ensures appropriate and updated patches are installed on the system
- ❑ Desktop Lockdown refers to the process of preventing the users from accessing a desktop or making any changes to its configuration settings
- ❑ Active Directory is directory service for a Windows OS that facilitates and the manages network components such as a user or service such as a users, services, sites, systems, users, shares on Windows Network
- ❑ Hypertext Transfer Protocol (HTTP) lays the foundation for communication on World Wide Web (WWW)