Unit #5

MIS5214

Secure Networks

Agenda

- In The News
- Quick Review: Reasons to Use Cryptography
- Digital Certificates
- Public Key Infrastructure
- Types of Networks
- OSI Model
- Layer 1 Network Devices
- Layer 2 Network Devices
- Layer 3 Network Devices
- Layer 3 – 7 Network Devices

# In The News: Section 001 & Section 701

Quick Review: Symmetric versus Asymmetric algorithms

- Symmetric cryptography
  - Uses a copied pair of symmetric (identical) secret keys
  - The sender and the receive use the same key for encryption and decryption functions
  - Confidentiality achieved across the Internet at a high-speed
  - But, no provisions for: authentication, non-repudiation, nor integrity

- Asymmetric cryptography
  - Also know as "public key cryptography"
  - Use different ("asymmetric") keys for encryption and decryption
  - One is called the "private key" and the other is the "public key"
  - Confidentiality, authenticity, and non-repudiation achieved, no integrity
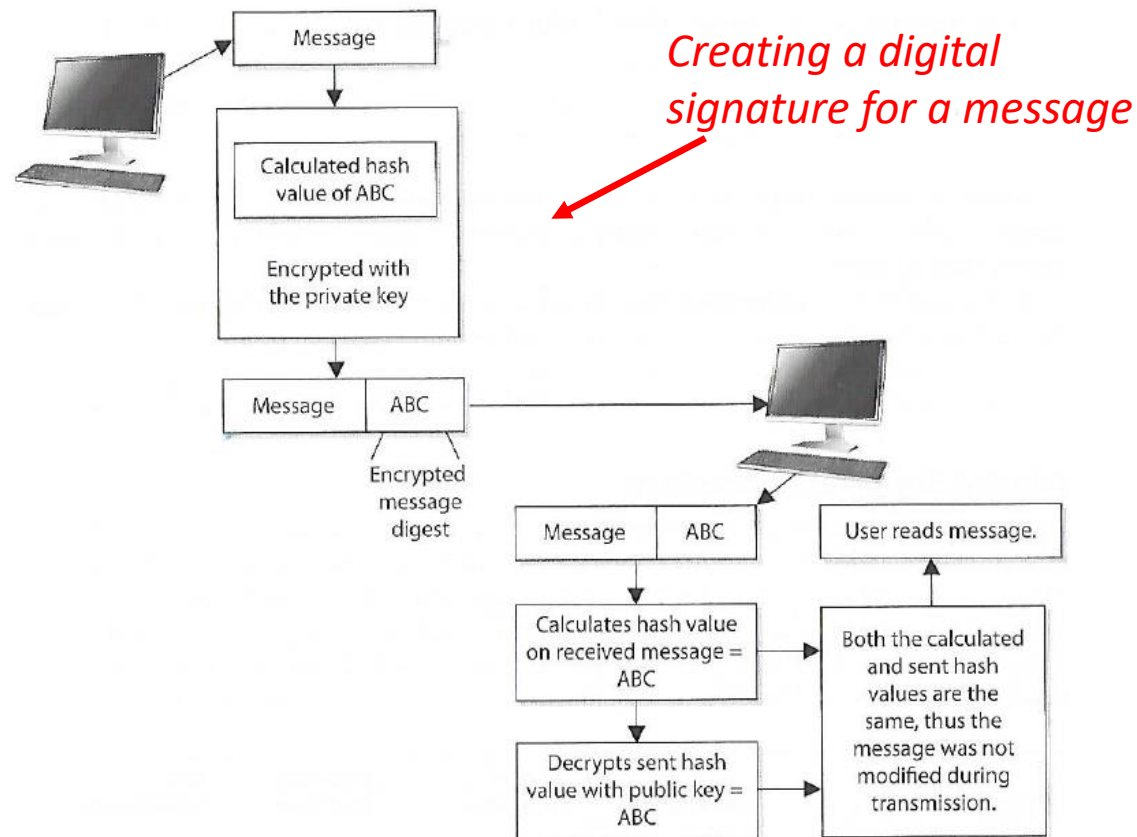
Quick Review: One-way Hash

- Assures message **integrity**

- A function that takes a variable-length string (i.e. message) and produces a fixed-length value called a hash value

- Does not use keys

1. Sender puts message through hashing function
2. Message digest generated
3. Message digest appended to the message
4. Sender sends message to receiver
5. Receiver puts message through hashing function
6. Receiver generates message digest value
7. Receiver compares the two message digests values. If they are the same, the message has not been altered

Hashing

5
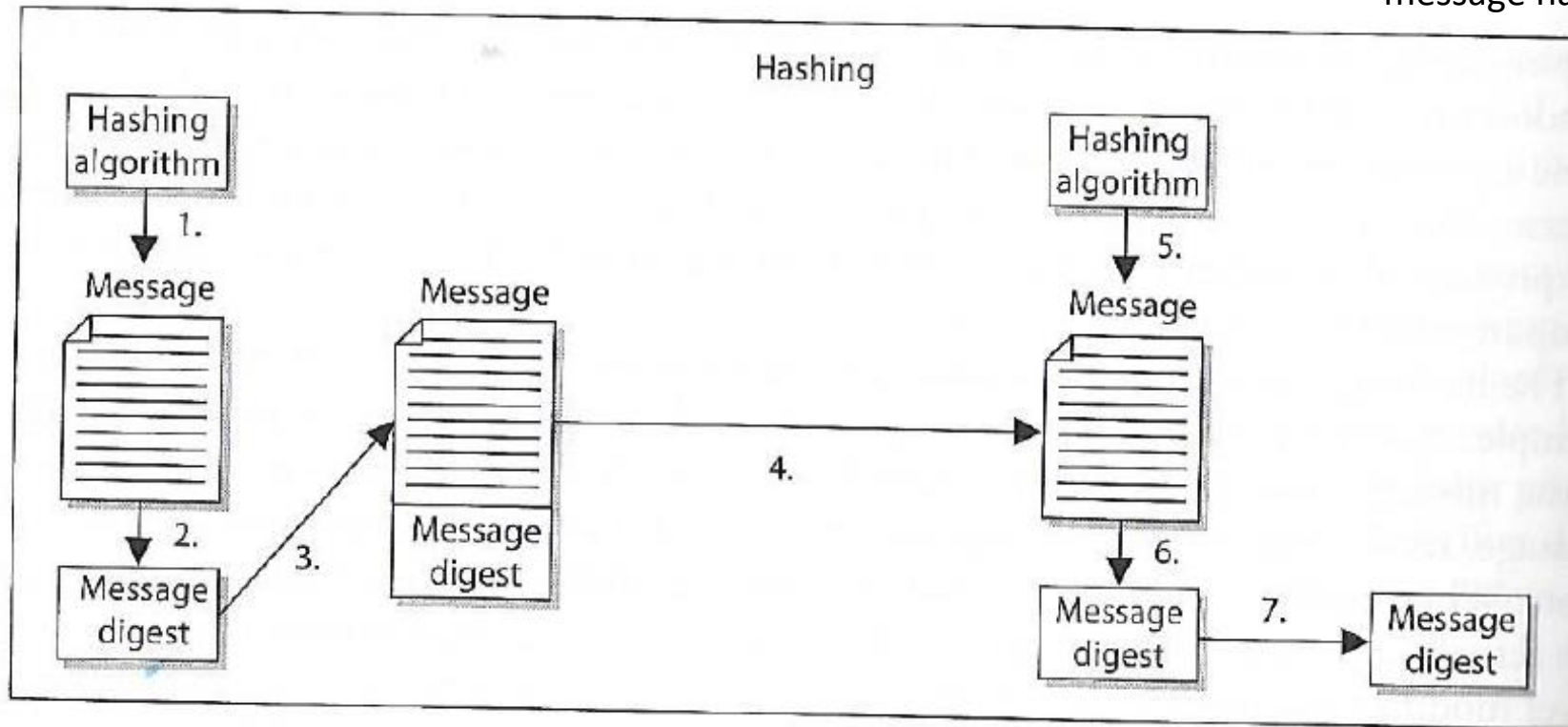
Quick Review: Digital Signature

- A hash value provides integrity and is encrypted with the sender's private key which provides authenticity and non-repudiation

- The act of signing means encrypting the message's hash value with the private key

Creating a digital signature for a message

Harris, S. and Maymi, F. (2016) <u>All-In-One CISSP Exam Guide</u>, McGraw Hill Education

Reasons to Use Cryptography

Reason	How achieved
Confidentiality	The message can be encrypted and decrypted by authorized users or processes
Integrity	The message can be hashed and/or digitally signed
Authentication	The encrypted message can be authenticated
Nonrepudiation	The encrypted message can be authenticated, and source of message can be identified

Agenda

- ✓In The News
- Quick Review – Reasons to Use Cryptography
- Digital Certificates
- Public Key Infrastructure
- Types of Networks
- OSI Model
- Layer 1 Network Devices
- Layer 2 Network Devices
- Layer 3 Network Devices
- Layer 3 – 7 Network Devices

Public Key Infrastructure (PKI)

Public key cryptography enables entities previously unknown to each other to verify the identity of each other, validate the information being transferred, and securely communicate on an insecure public network

- **Public key infrastructure**
  - Enables online activities requiring more trust and proof of identity than simple passwords
  - Provides a hierarchy of trust relationships that:
    - Enable knowing a public key really belongs to the person/system you want to communicate with
    - Are necessary for hybrid cryptography
    - Facilitate secure electronic transfer of information for a range of network activities such as e-commerce, internet banking and confidential email

Public Key Infrastructure (PKI)

Is a system for creating, storing, distributing, validating, revoking and managing **digital certificates** used to verify the identity the owner of a public key contained within the certificate

- Assumes
  - Receiver's and Sender's identities can be positively ensured through digital certificates
  - Asymmetric algorithm will automatically carry out the process of key exchange
- Contains components that
  - Identify users
  - Creates and distributes certificates
  - Maintains and revokes certificates
  - Distributes and maintains encryption keys
  - Enables information technologies to communicate and work together to achieve confidentiality, authentication, integrity, and non-repudiation
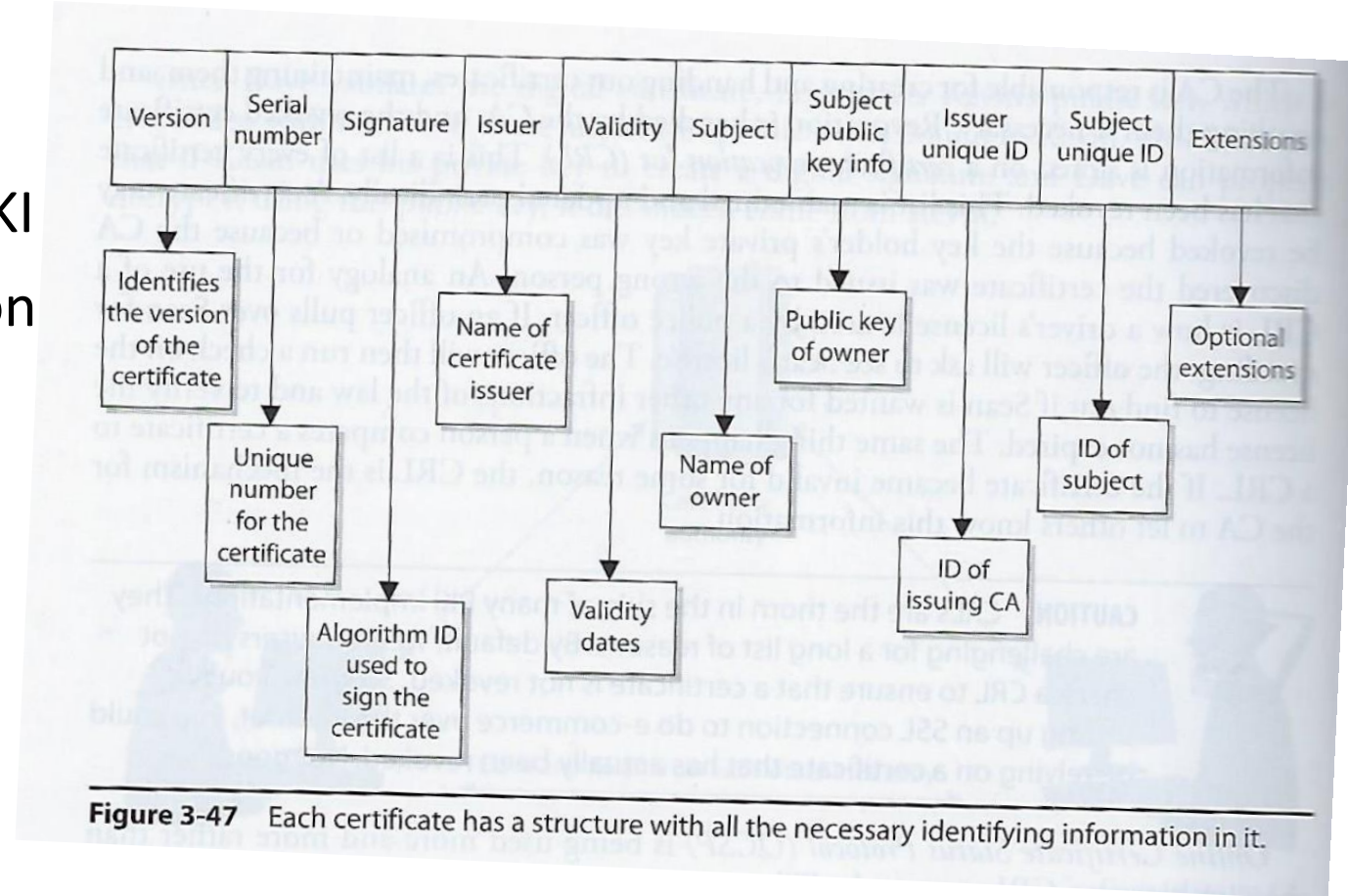
Public Key Infrastructure (PKI)

Consists of:

- **Public key certificates ("digital certificates")** are electronic documents used to prove the ownership of public keys
- *Roles*
    - *Certificate Authorities* (CA) store, issue and sign the digital certificates
    - *Registration Authorities* (RA) verify identities of entities requesting their digital certificates be stored at the CA
- *Technologies*
    - *Central directory* provides a secure location in which keys are stored and indexed
    - *Certificate management system*
        - Creates and delivers new certificates to be issued
        - Searches, retrieves and accesses to stored certificates
- *Certificate policy* states procedures for allowing outsiders to analyze the PKI's trustworthiness

Digital Certificate

One of the most important pieces of a PKI

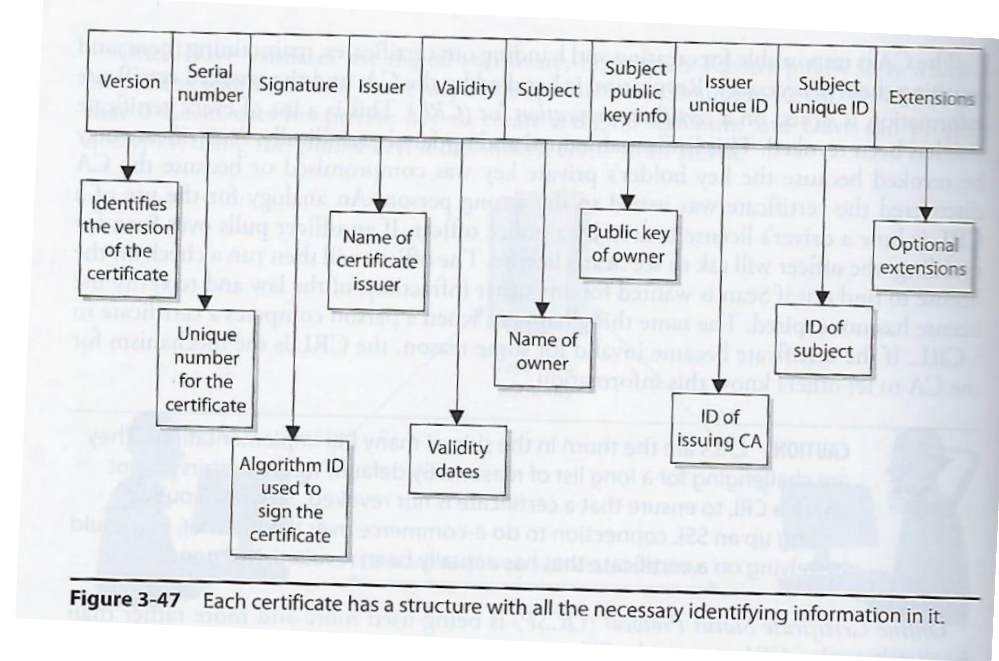- Associates a public key with information for uniquely identifying its owner

Version	Serial number	Signature	Issuer	Validity	Subject	Subject public key info	Issuer unique ID	Subject unique ID	Extensions
Identifies the version of the certificate	Unique number for the certificate	Algorithm ID used to sign the certificate	Name of certificate issuer	Validity dates	Name of owner	Public key of owner	ID of issuing CA	ID of subject	Optional extensions

Figure 3-47 Each certificate has a structure with all the necessary identifying information in it.

- X.509 standard defines the format of public key certificates used in many Internet cryptographic protocols for HTTPS for servers & clients, secure email, code signing, digital signatures…
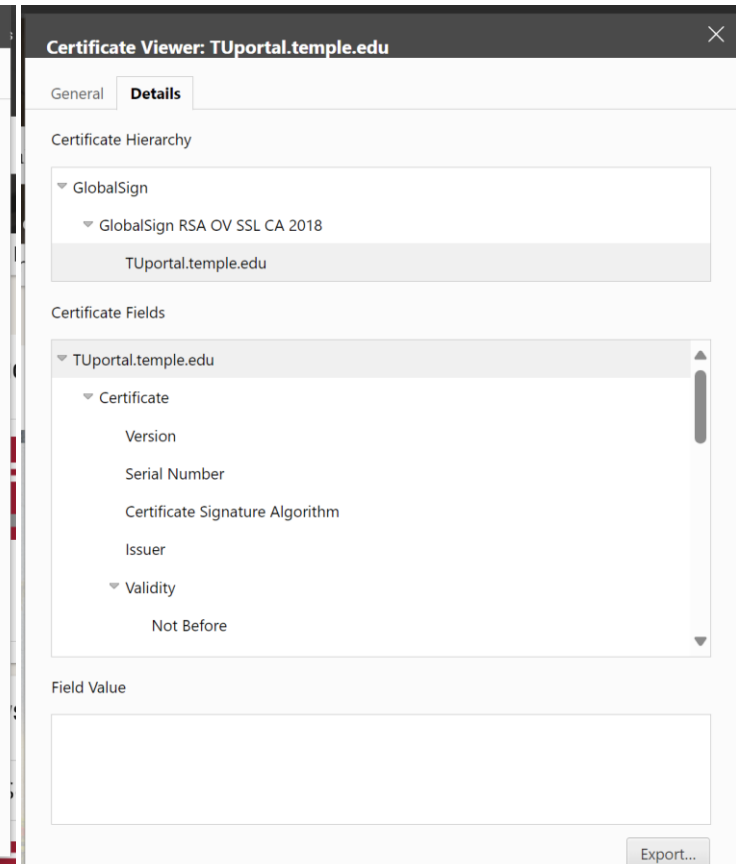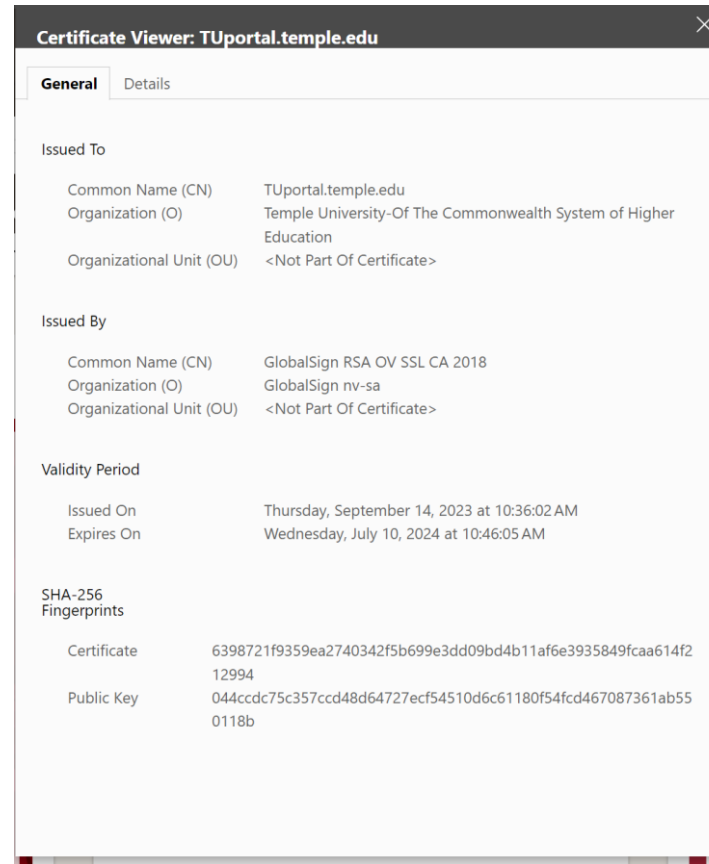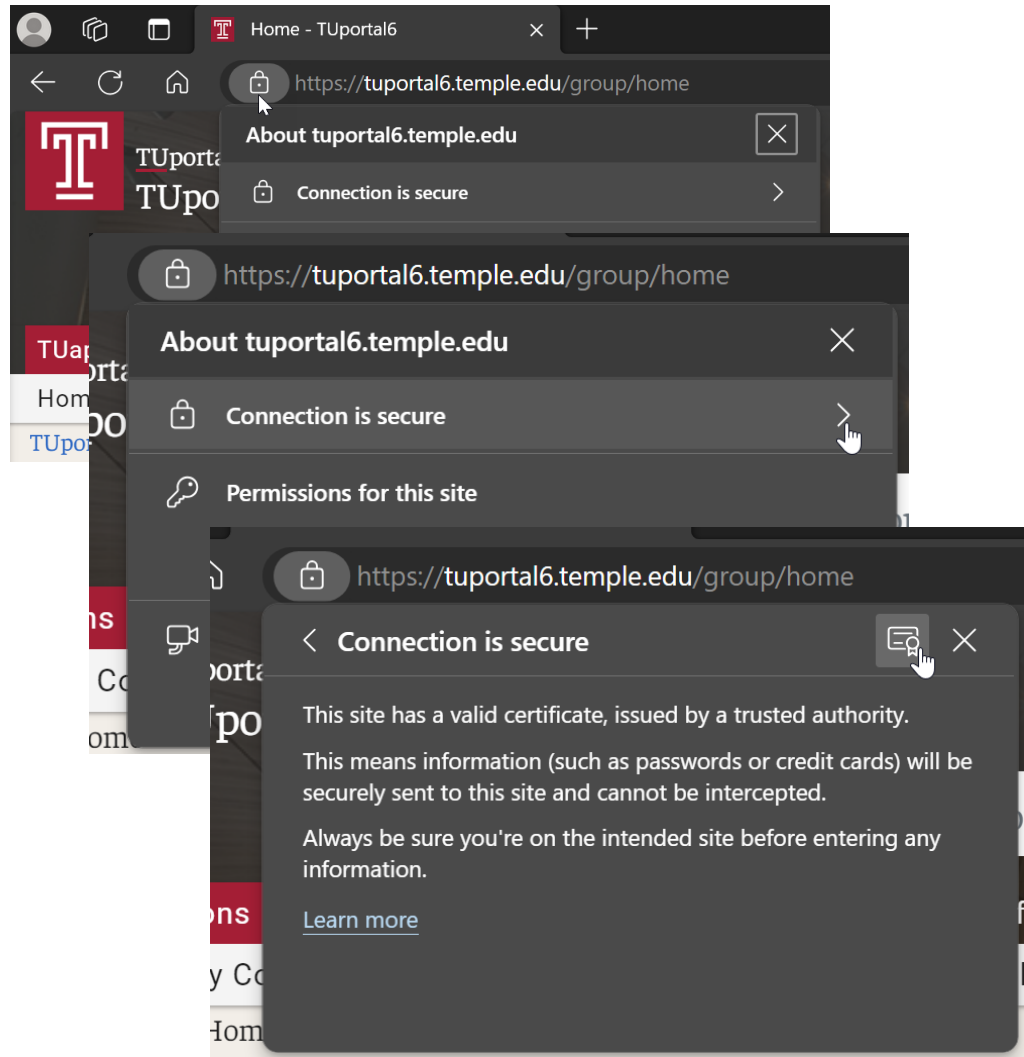
Public Key Certificate

Electronic documents used to prove ownership of a public key

Figure 3-47 Each certificate has a structure with all the necessary identifying information in it.

A certificate includes the following common fields:

- Information about the certificate
    - **Serial Number:** Used to uniquely identify the certificate
    - **Issuer:** Entity that verified the information and signed the certificate
    - **Signature Algorithm**: The algorithm used to sign the public key certificate
    - **Signature**: A signature of the certificate body by the issuer's private key

- Information about the public key
    - **Not Before**: Earliest time and date on which the certificate is valid.
    - **Not After**: Time and date past which the certificate is no longer valid
    - **Key Usage**: Valid cryptographic uses of the certificate's public key, e.g. digital signature validation, key encipherment, and certificate signing
    - **Extended Key Usage**: Applications the certificate may be used for, e.g. TLS server authentication, email protection, code signing, or electronic signature

- Information about the identity of its owner (called the subject)
    - **Subject: E**ntity a certificate belongs to, e.g. individual, machine, or organization

Certificate

Certificate Details

Certificate Details

Certificate Viewer: TUportal.temple.edu

General | **Details**

Certificate Hierarchy

- ▼ GlobalSign
  - ▼ GlobalSign RSA OV SSL CA 2018
    - TUportal.temple.edu

Certificate Fields

- Validity
  - Not Before
  - Not After
- Subject
- ▼ Subject Public Key Info
  - Subject Public Key Algorithm
  - **Subject's Public Key**
- ▼ Extensions
  - Certificate Key Usage

Field Value

```
Modulus (2048 bits):
  EF C0 9B 98 3F DA 05 CF BC 8D 2F 08 08 3A FC EB
41 AA 4F AE D2 59 42 B8 2A F5 BC 46 FF 54 06 D1
3C C3 70 E3 FD 83 94 21 59 66 43 D9 EB 05 1E 4F
4F CC 6E F7 1B FD FA 3E 2B 13 20 5E 02 A7 53 CD
```

Export...

MIS 5214

Certificate Viewer: TUportal.temple.edu

General | **Details**

Certificate Hierarchy

- ▼ GlobalSign
  - ▼ GlobalSign RSA OV SSL CA 2018
    - TUportal.temple.edu

Certificate Fields

- Validity
  - Not Before
  - Not After
- Subject
- ▼ Subject Public Key Info
  - Subject Public Key Algorithm
  - Subject's Public Key
- ▼ Extensions
  - Certificate Key Usage

Field Value

```
Modulus (2048 bits):
  EF C0 9B 98 3F DA 05 CF BC 8D 2F 08 08 3A FC EB
41 AA 4F AE D2 59 42 B8 2A F5 BC 46 FF 54 06 D1
3C C3 70 E3 FD 83 94 21 59 66 43 D9 EB 05 1E 4F
4F CC 6E F7 1B FD FA 3E 2B 13 20 5E 02 A7 53 CD
7D 83 FB 0C 7F 47 7A 93 61 F6 27 23 3C 92 1D 8D
61 62 DB B7 2D 9E E0 CD FC 8C 93 40 F2 F6 41 63
1D 18 81 0A 38 2B 31 79 6F 89 BF A8 CC 26 E8 D7
69 45 7B CE AE 1F EB 62 E9 31 56 3D B3 AB 0A 51
8F 5B 5A E6 3C 24 E9 3F 73 15 16 A4 AC 56 A5 06
BA 6D 41 D3 44 E0 A1 7D 97 A1 2C 96 2E 73 D9 86
39 AB 7F 26 EE 49 BF C4 92 00 5B EB 99 39 6D
2E DD C5 9C A3 AB 6A BB 86 BB 5E DB 54 F5 37 1D
8D 14 C1 BF 55 52 9E 09 6C 2B C1 78 09 BF EA CA
5A 73 86 47 8C AE 51 C4 72 86 31 71 D1 F0 DC 94
6B EE D6 C0 9B 49 97 33 2C FC 0C D3 44 A0 EB D2
30 DA 6B 73 15 40 52 69 C6 7E 91 24 FD 0D AA 8D

Public Exponent (17 bits):
01 00 01
```

Export...

🔒 https://cryptii.com

cryptii

VIEW

Text ⌄

```
 EF C0 9B 98 3F DA 05 CF BC 8D
2F 08 08 3A FC EB
41 AA 4F AE D2 59 42 B8 2A F5
BC 46 FF 54 06 D1
3C C3 70 E3 FD 83 94 21 59 66
43 D9 EB 05 1E 4F
4F CC 6E F7 1B FD FA 3E 2B 13
20 5E 02 A7 53 CD
7D 83 FB 0C 7F 47 7A 93 61 F6
27 23 3C 92 1D 8D
61 62 DB B7 2D 9E E0 CD FC 8C
93 40 F2 F6 41 63
1D 18 81 0A 38 2B 31 79 6F 89
BF A8 CC 26 E8 D7
69 45 7B CE AE 1F EB 62 E9 31
56 3D B3 AB 0A 51
8F 5B 5A E6 3C 24 E9 3F 73 15
16 A4 AC 56 A5 06
```

ENCODE DECODE

Numeral system ⌄

READ

- ○ Binary (2)
- ○ Octal (8)
- ○ Decimal (10)
- ● Hexadecimal (16)
- ○ Roman numerals

CONVERT TO

- ● Binary (2)
- ○ Octal (8)
- ○ Decimal (10)
- ○ Hexadecimal (16)
- ○ Roman numerals

→ Encoded 2061 chars

VIEW

Text ⌄

```
11101111 11000000 10011011
10011000 111111 11011010 101
11001111 10111100 10001101
101111 1000 1000 111010
11111100 11101011
1000001 10101010 1001111
101101110 11010010 1011001
1000010 10111000 101010
11110101 10111100 1000110
11111111 1010100 110 11010001
111100 11000011 1110000
11000011 11111101 10000011
10010100 100001 1011001 1100110
1000011 11011001 11101011 101
11110 1001111
1001111 11001100 1101110
11110111 11011 11111101
11111010 111110 101011 10011
```

https://cryptii.com/

Types of Certificates: Different cryptographic protocols ("applications")

X.509 is a standard of the International Telecommunications Union which defines the format of public key certificates used in many Internet cryptographic protocols, including:

1. **Transport Layer Security** (TLS/SSL) HTTPS protocol for securely browsing the web
   Certificate's subject is typically a computer or other device, but may also identify organizations or individuals
   - **Server certificate**
     - A server is required to present a certificate as part of the initial connection setup. A client connecting to that server will validate the certificate by checking that
       1. The certificate's subject matches the hostname (i.e. domain name) to which the client is trying to connect
       2. The certificate is signed by a trusted certificate authority
   - **Client certificate** (less common than server certificates)
     - Used to authenticate the client connecting to a TLS service (e.g. for access control)
     - Most client certificates contain an email address or personal name rather than a hostname

2. **Email encryption certificate**
   - A certificate's subject is typically a person or organization
   - For secure email, senders use an email certificate to discover which public key to use for any given recipient

3. **Code signing certificate**
   - A code signing certificate is used to validate signatures on programs to ensure they were not tampered with during delivery

4. **Qualified digital certificate**
   - A "Qualified digital certificate" identifies an individual for electronic signature purposes

Roles in PKI - Certificate Authority (CA)

Serves as a trusted third party responsible for verifying identities and signing digital certificates of identity ("digital signature") which are exchanged between two parties introducing themselves to each other

Each person wanting to participate in a PKI requires a digital certificate
- Digital certificate is a credential containing the public key for that individual along with other identifying information

A CA is a trusted organization (or server) responsible for:
- Issuing (creating and handing) out digital certificates
- Maintaining digital certificates
- Revoking digital certificates

Use of PKI and exchanging digital certificates is intended to block Man-in-the-Middle attacks where 2 users are not working in PKI environment do not truly know the identity of the owners of public keys

Roles in PKI - Certificate Authority (CA)

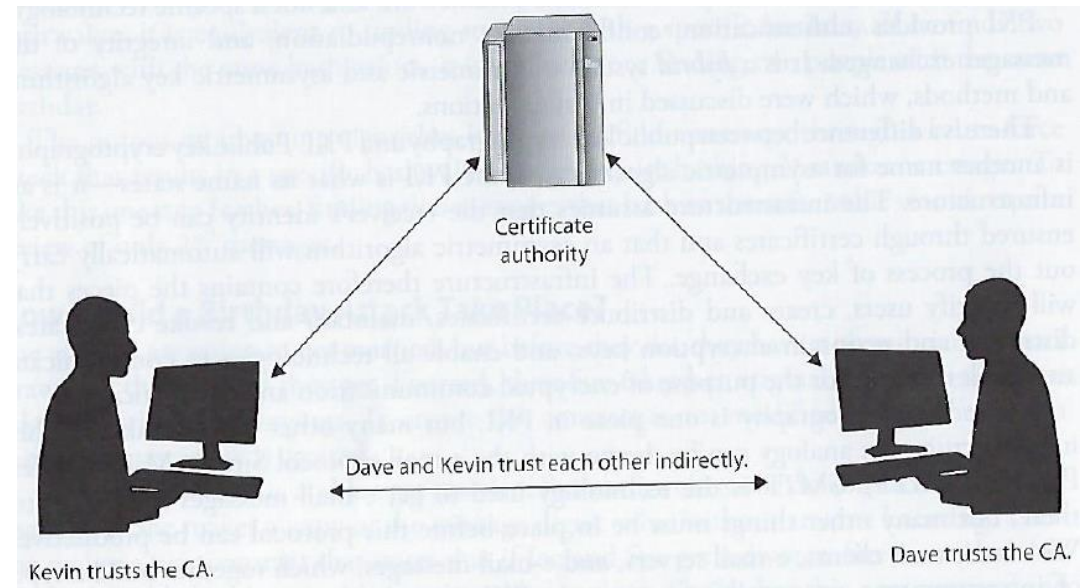Each person wanting to participate in a PKI requires a digital certificate

- Digital certificate is a credential containing the public key for that individual, computer or organization along with other identifying information

When a CA signs the certificate, it binds the individual's, computer's or organization' identity to the public key

- The CA takes liability for the authenticity of the identity
    - *Making a CA the "trusted 3rd party" that allows people who have never met to use their public keys to authenticate each other and communicate in a secure way*

Certificate Revocation Information

CA's are also responsible for maintaining up-to-date revocation information about certificates they have issued, indicating when certificates of identity are no longer valid
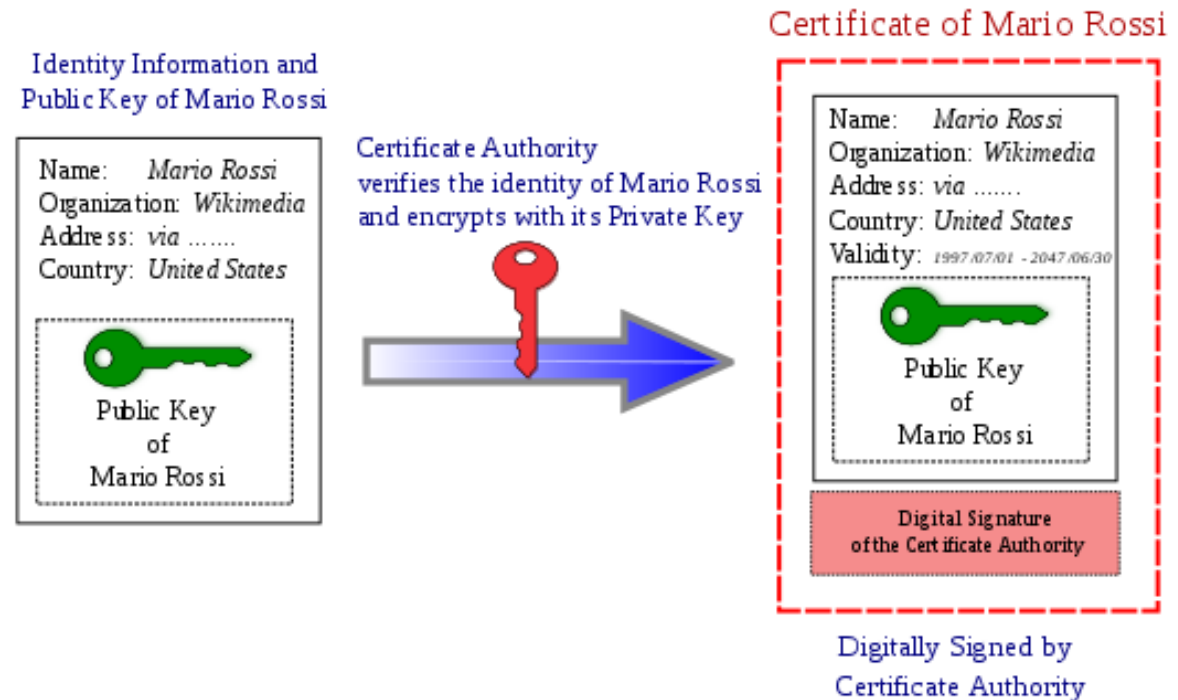

Certificate authority

Dave and Kevin trust each other indirectly.

Kevin trusts the CA.

Dave trusts the CA.

Roles in PKI – Certificate Authority (CA)

New Certificate Requests

A CA processes requests from people or organizations requesting certificates (called "subscribers")

1. Verifies the subscriber's information
2. Potentially signs an end-entity certificate based on the subscriber's information

Registration Authority (RA)

When a user needs a new certificate, the user makes a request to the RA

RA serves as a broker between the user and the CA, and performs certain certification registration tasks

- Performs the certificate life-cycle management functions
- Establishes and confirms the identity of the individual
  - The RA verifies all the necessary identification information before allowing a request to go to the CA
- Initiates the certification process with the CA for the end user

RA cannot issue certificates

PKI Steps

Suppose: John needs to obtain a digital certificate to participate in PKI

1. John requests a digital certificate from a RA

2. The RA requests John's identification information
   - E.g. driver's license, address, phone number, email, …

3. RA receives John's information, verifies it, and sends his certificate request to CA

4. CA creates a certificate with John's public key and embedded identity information
   - Private/Public key pair is generated on John's machine or by the CA (depends on system configuration)
     - Usually – user generates this pair and sends his public key in as part of registration process
     - If CA creates key pair, John's private key needs to be sent to him via secure means

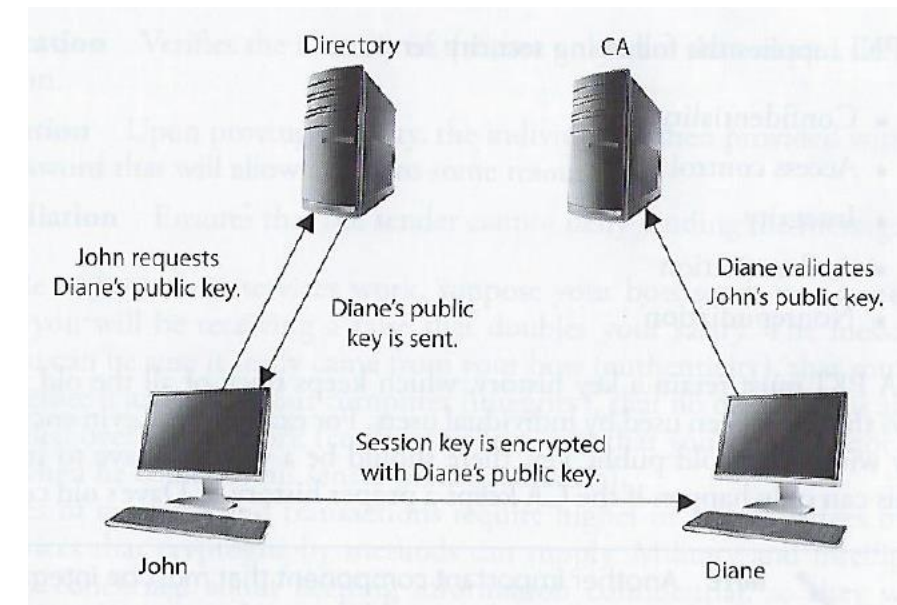Now John is registered and is able to participate in PKI
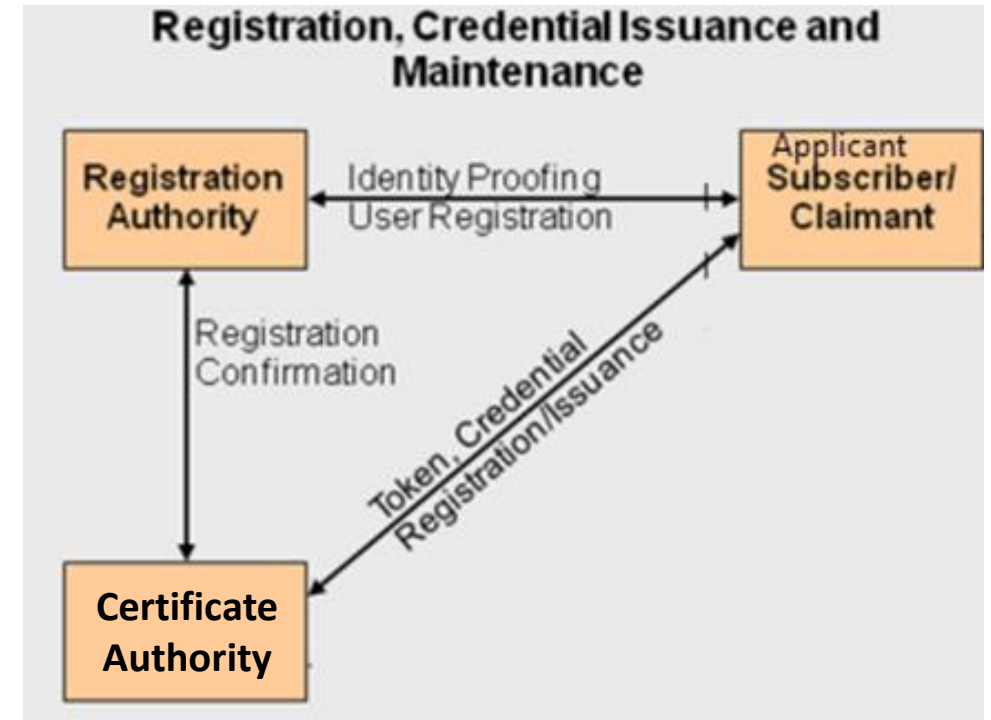
Token, Credential = Public Key

PKI Steps

John and Diane decide to communicate securely using PKI…

1. John requests Diane's public key form a public directory
2. The directory (a.k.a. repository) sends Diane's digital certificate
3. John verifies the digital certificate…
   - extracts her public key, uses the public key to encrypt a session key that will be used to encrypt their messages
   - John sends the encrypted session key to Diane
   - John also sends his certificate, containing his public key to Diane
4. Diane browser receives John's certificate, **looks to see if it trusts the CA** that digitally signed the certificate
   - Diane's browser trusts this CA
   - After verifying the certificate, both John and Diane can communicate using encryption

Types of certificates: Chain of trust

A PKI is often set up with multiple levels of CAs, for practical reasons:

- There is a top-level CA, called the root, which issues certificates on the keys of lower-level CAs, which in turn certify the user keys

- The system of identity validation still behaves in the same way, but now Diane has to check two certificates to verify John's key

- **Root certificate**
  - Self-signed certificate used to sign other certificates
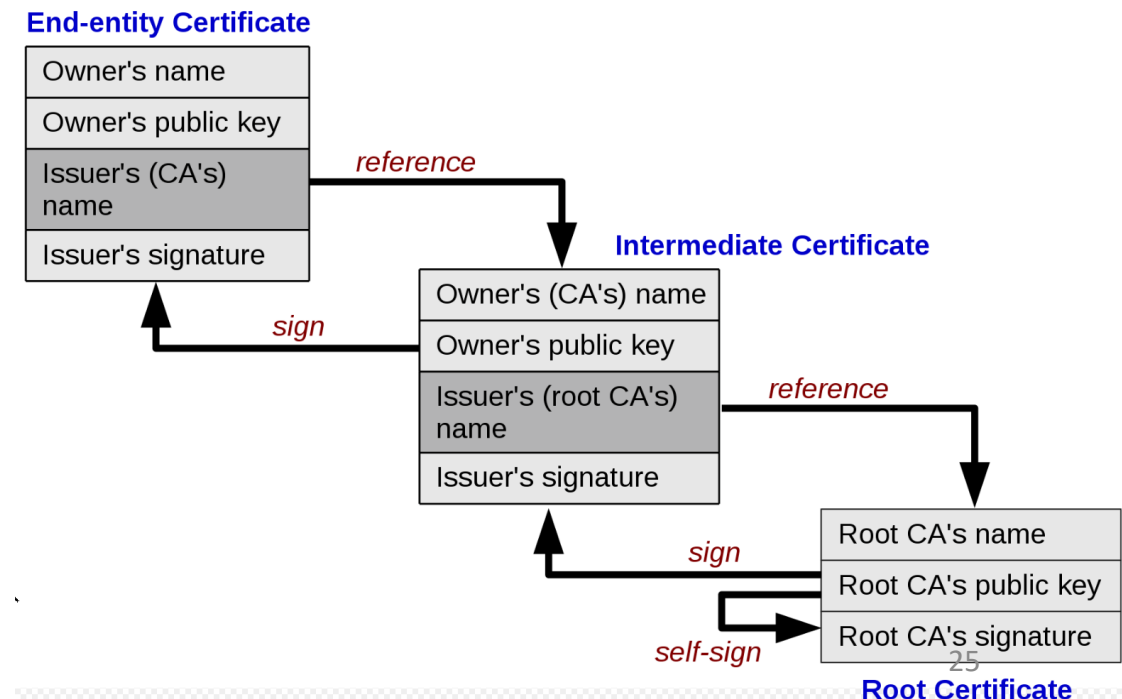
- **Intermediate certificate**
  - A certificate used to sign other certificates.
  - Must be signed by either a root certificate or another intermediate certificate
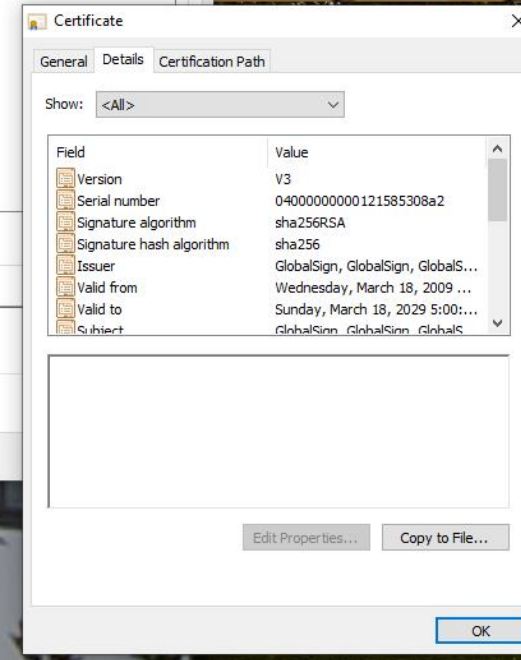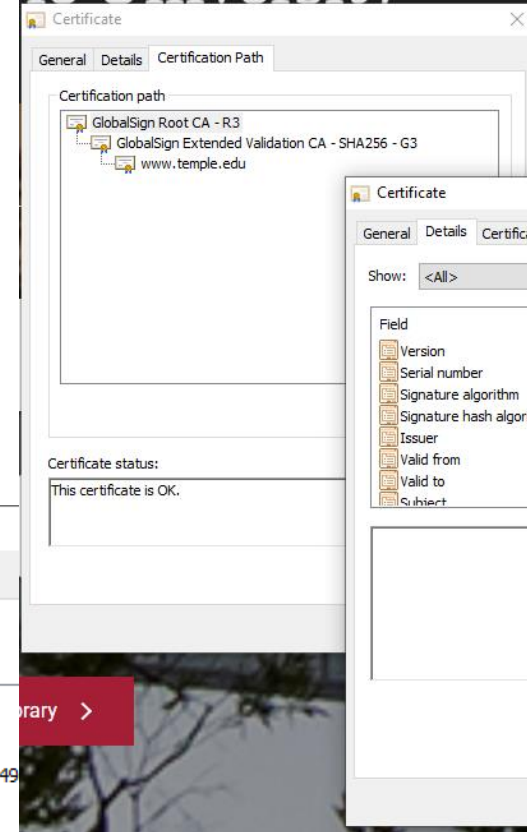
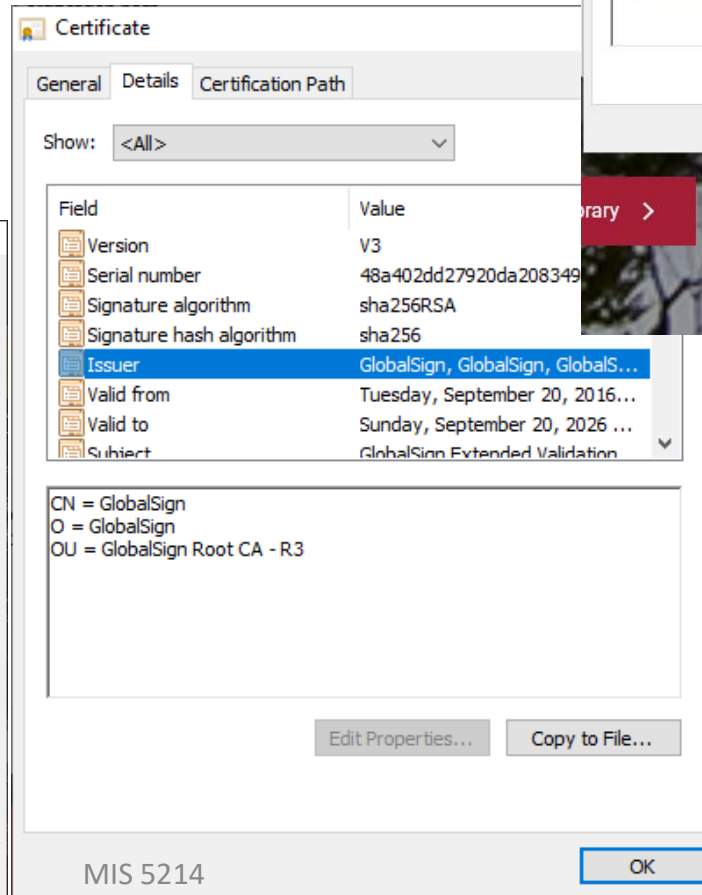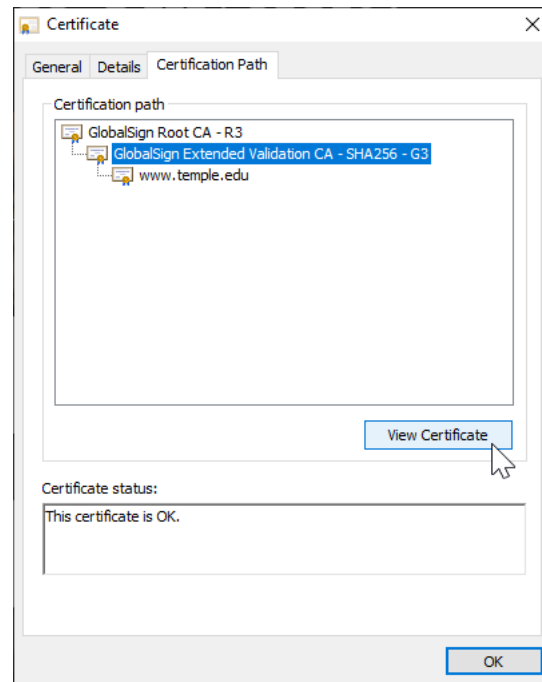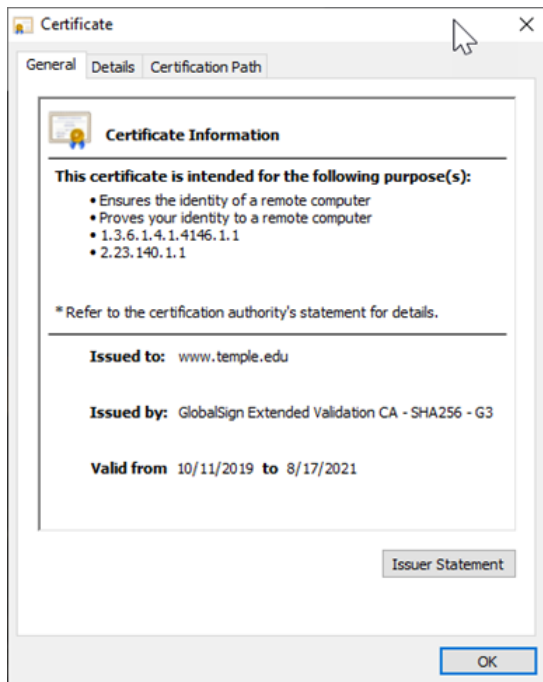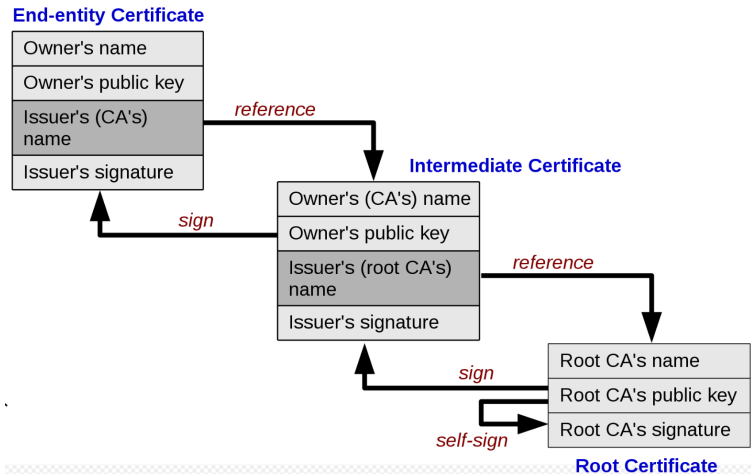- **End-entity ("leaf") certificate**
  - Cannot be used to sign other certificates
  - Include:
    - TLS/SSL server and client certificates
    - Email certificates
    - Code signing certificates
    - Qualified certificates

End-entity Certificate

| Owner's name |
| Owner's public key |
| Issuer's (CA's) name |
| Issuer's signature |

reference

sign

Intermediate Certificate

| Owner's (CA's) name |
| Owner's public key |
| Issuer's (root CA's) name |
| Issuer's signature |

reference

sign

| Root CA's name |
| Root CA's public key |
| Root CA's signature |

self-sign

Root Certificate

Types of certificates: Chain of trust

End-entity Certificate

Owner's name
Owner's public key
Issuer's (CA's) name
Issuer's signature

reference

sign

Intermediate Certificate

Owner's (CA's) name
Owner's public key
Issuer's (root CA's) name
Issuer's signature

reference

sign

Root Certificate

Root CA's name
Root CA's public key
Root CA's signature

self-sign

Certificate — Certification Path

Certification path
- GlobalSign Root CA - R3
  - GlobalSign Extended Validation CA - SHA256 - G3
    - www.temple.edu

Certificate status:
This certificate is OK.

Certificate — Details

Show: <All>

Field	Value
Version	V3
Serial number	04000000000121585308a2
Signature algorithm	sha256RSA
Signature hash algorithm	sha256
Issuer	GlobalSign, GlobalSign, GlobalS...
Valid from	Wednesday, March 18, 2009 ...
Valid to	Sunday, March 18, 2029 5:00:...
Subject	GlobalSign, GlobalSign, GlobalS...

Edit Properties...   Copy to File...

OK

About

Certificate — General

Certificate Information

This certificate is intended for the following purpose(s):
- Ensures the identity of a remote computer
- Proves your identity to a remote computer
- 1.3.6.1.4.1.4146.1.1
- 2.23.140.1.1

* Refer to the certification authority's statement for details.

Issued to: www.temple.edu

Issued by: GlobalSign Extended Validation CA - SHA256 - G3

Valid from 10/11/2019 to 8/17/2021

Issuer Statement

OK

Certificate — Certification Path

Certification path
- GlobalSign Root CA - R3
  - GlobalSign Extended Validation CA - SHA256 - G3
    - www.temple.edu

View Certificate

Certificate status:
This certificate is OK.

OK

Certificate — Details

Show: <All>

Field	Value
Version	V3
Serial number	48a402dd27920da208349
Signature algorithm	sha256RSA
Signature hash algorithm	sha256
Issuer	GlobalSign, GlobalSign, GlobalS...
Valid from	Tuesday, September 20, 2016...
Valid to	Sunday, September 20, 2026 ...
Subject	GlobalSign Extended Validation

CN = GlobalSign
O = GlobalSign
OU = GlobalSign Root CA - R3

Edit Properties...   Copy to File...

OK

MIS 5214

Types of certificates: Chain of trust

- **CN:** CommonName
- **OU:** OrganizationalUnit
- **O:** Organization
- **L:** Locality
- **S:** StateOrProvinceName
- **C:** CountryName

End-entity Certificate

Owner's name
Owner's public key
Issuer's (CA's) name
Issuer's signature

reference

sign

Intermediate Certificate

Owner's (CA's) name
Owner's public key
Issuer's (root CA's) name
Issuer's signature

reference

sign

Root CA's name
Root CA's public key
Root CA's signature

self-sign

Root Certificate

Certificate Viewer: TUportal.temple.edu ✕

General | **Details**

Certificate Hierarchy

- ▾ GlobalSign
  - ▾ GlobalSign RSA OV SSL CA 2018
    - TUportal.temple.edu

Certificate Fields

- ▾ TUportal.temple.edu
  - ▾ Certificate
    - Version
    - Serial Number
    - Certificate Signature Algorithm
    - **Issuer**
  - ▾ Validity
    - Not Before

Field Value

```
CN = GlobalSign RSA OV SSL CA 2018
O = GlobalSign nv-sa
C = BE
```

Export...

Certificate Viewer: TUportal.temple.edu ✕

General | **Details**

Certificate Hierarchy

- ▾ GlobalSign
  - ▾ GlobalSign RSA OV SSL CA 2018
    - TUportal.temple.edu

Certificate Fields

- ▾ GlobalSign RSA OV SSL CA 2018
  - ▾ Certificate
    - Version
    - Serial Number
    - Certificate Signature Algorithm
    - Issuer
  - ▾ Validity
    - Not Before

Field Value

```
CN = GlobalSign
O = GlobalSign
OU = GlobalSign Root CA - R3
```

Export...

Certificate Viewer: TUportal.temple.edu ✕

General | **Details**

Certificate Hierarchy

- ▾ GlobalSign
  - ▾ GlobalSign RSA OV SSL CA 2018
    - TUportal.temple.edu

Certificate Fields

- ▾ GlobalSign
  - ▾ Certificate
    - Version
    - Serial Number
    - Certificate Signature Algorithm
    - Issuer
  - ▾ Validity
    - Not Before

Field Value

```
CN = GlobalSign
O = GlobalSign
OU = GlobalSign Root CA - R3
```

Export...

Types of certificates: Chain of trust

End-entity Certificate

Owner's name
Owner's public key
Issuer's (CA's) name
Issuer's signature

reference

Intermediate Certificate

Owner's (CA's) name
Owner's public key
Issuer's (root CA's) name
Issuer's signature

sign

reference

Root Certificate

Root CA's name
Root CA's public key
Root CA's signature

sign

self-sign
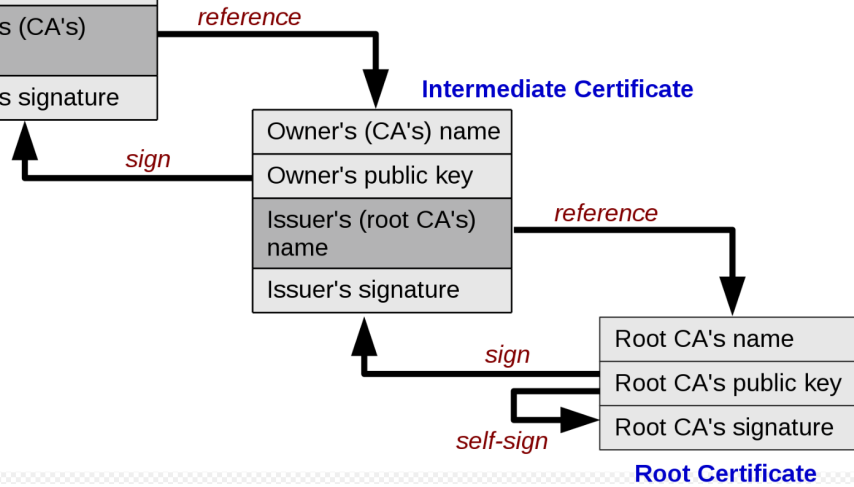
- CN: CommonName
- OU: OrganizationalUnit
- O: Organization
- L: Locality
- S: StateOrProvinceName
- C: CountryName

← ⟳ ⌂ 🔒 https://docs.oracle.com/cd/E24191_01/common/tutorials/authz_cert_attributes.html

Certificate Attributes

Certificate Viewer: www-ww.oracle.com ✕

General   **Details**

Certificate Hierarchy

Contents

- Overview
- Configuration

▼ DigiCert Global Root CA
    ▼ DigiCert TLS RSA SHA256 2020 CA1
       www-ww.oracle.com

Certificate Fields

Overview

The Enterprise Gateway can authorize access to a Web Servic
whose certificates have a Distinguished Name (DName) contai

An X.509 certificate consists of a number of fields. The Subje
to an X.500 directory object. It consists of a number of attribu

- CN: CommonName
- OU: OrganizationalUnit
- O: Organization
- L: Locality
- S: StateOrProvinceName
- C: CountryName

For example, the following is the DName of the *sample.p12* cli

CN=Sample Cert, OU=R&D, O=Company

Using the **Certificate Attributes** filter, it is possible to autho

▼ www-ww.oracle.com
   ▼ Certificate
     Version
     Serial Number
     Certificate Signature Algorithm
     Issuer
    ▼ Validity
      Not Before

Field Value

CN = DigiCert TLS RSA SHA256 2020 CA1
O = DigiCert Inc
C = US

Configuration

The **X.509 Attributes** table lists a number of attribute check
configured attribute values match those in the client certificate

For example, imagine the following is configured as an entry i

Export...

Types of certificates: Chain of trust

To perform its role effectively, a CA needs to have one or more broadly trusted <u>root certificates</u> or intermediate certificates and the corresponding private keys
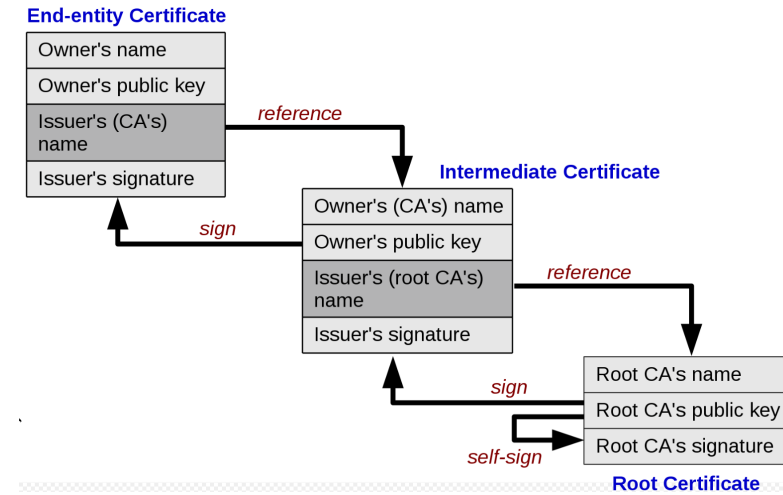
A CA may achieve broad trust by:
  Having its root certificates included in popular software
  Obtaining a cross-signature from another CA delegating trust

Or a CA may be trusted within a relatively small community, like a business
  In which its root certificates are distributed by other mechanisms like Windows Group Policy

Types of certificates: Chain of trust
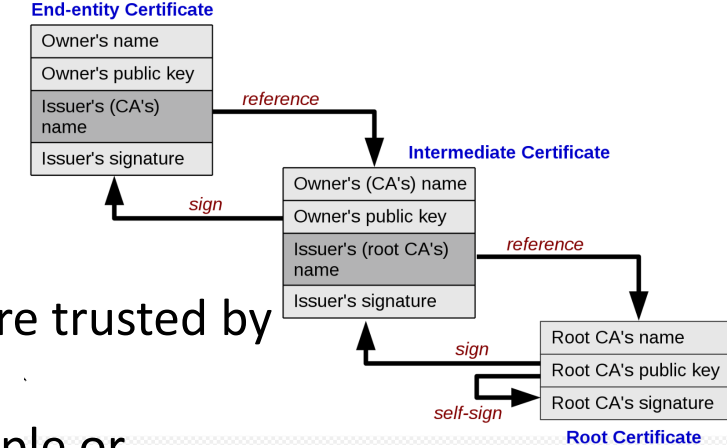
Root programs:
- Some major software products contain a list of certificate authorities that are trusted by default
- This makes it easier for end-users to validate certificates, and easier for people or organizations that request certificates to know which certificate authorities can issue a certificate that will be broadly trusted
- This is particularly important in HTTPS, where a web site operator generally wants to get a certificate that is trusted by nearly all potential visitors to their web site

  The most influential root programs are:
  - Microsoft Root Program
  - Apple Root Program
  - Mozilla Root Program
  - Oracle Java root program
  - Adobe Approved Trust List and EUTL root programs (used for document signing)

End-entity Certificate

Owner's name
Owner's public key
Issuer's (CA's) name
Issuer's signature

reference
sign

Intermediate Certificate

Owner's (CA's) name
Owner's public key
Issuer's (root CA's) name
Issuer's signature

reference
sign

Root CA's name
Root CA's public key
Root CA's signature

self-sign
Root Certificate

Types of certificates: Chain of trust

End-entity Certificate
- Owner's name
- Owner's public key
- Issuer's (CA's) name — *reference*
- Issuer's signature — *sign*

Intermediate Certificate
- Owner's (CA's) name
- Owner's public key
- Issuer's (root CA's) name — *reference*
- Issuer's signature — *sign*

Root Certificate
- Root CA's name
- Root CA's public key
- Root CA's signature — *self-sign*

Root programs:

Browsers generally use the operating system's facilities to decide which certificate authorities are trusted:

- Google Chrome on Windows trusts certificate authorities included in Microsoft Root Program
- Google Chrome on macOS or iOS trusts certificate authorities in Apple Root Program
- Edge and Safari use their respective operating system trust stores as well, but each is only available on a single OS.

- Firefox, in contrast, uses the Mozilla Root Program trust store on all platforms

Microsoft Windows Root Program's Trust Stores

1. Run **mmc.exe**

2. Select **File -> Add/Remove Snap-in**

3. Select **Certificates**, click **Add**

4. Select **Computer Account,** click **next,** click **Finish**

5. Expand the **Certificates** node -> **Trusted Root Certificate Authorities Store**

MIS 5214

Microsoft Windows Root Program's Trust Stores

Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name	S
AAA Certificate Services	AAA Certificate Services	12/31/2028	Client Authenticatio...	Sectigo (AAA)	
Baltimore CyberTrust Root	Baltimore CyberTrust Root	5/12/2025	Client Authenticatio...	DigiCert Baltimore R...	
Certum Trusted Network CA	Certum Trusted Network CA	12/31/2029	Client Authenticatio...	Certum Trusted Net...	
Class 3 Public Primary Certificati...	Class 3 Public Primary Certification ...	8/1/2028	Client Authenticatio...	VeriSign Class 3 Pub...	
COMODO RSA Certification Aut...	COMODO RSA Certification Autho...	1/18/2038	Client Authenticatio...	Sectigo (formerly Co...	
Copyright (c) 1997 Microsoft Corp.	Copyright (c) 1997 Microsoft Corp.	12/30/1999	Time Stamping	Microsoft Timestam...	
DigiCert Assured ID Root CA	DigiCert Assured ID Root CA	11/9/2031	<All>	<None>	
DigiCert Assured ID Root CA	DigiCert Assured ID Root CA	11/9/2031	Client Authenticatio...	DigiCert	
DigiCert Global Root CA	DigiCert Global Root CA	11/9/2031	Client Authenticatio...	DigiCert	
DigiCert Global Root G2	DigiCert Global Root G2	1/15/2038	Client Authenticatio...	DigiCert Global Roo...	
DigiCert Global Root G3	DigiCert Global Root G3	1/15/2038	Client Authenticatio...	DigiCert Global Roo...	
DigiCert High Assurance EV Roo...	DigiCert High Assurance EV Root CA	11/9/2031	Client Authenticatio...	DigiCert	
DigiCert Trusted Root G4	DigiCert Trusted Root G4	1/15/2038	Client Authenticatio...	DigiCert Trusted Ro...	
DST Root CA X3	DST Root CA X3	9/30/2021	Client Authenticatio...	DST Root CA X3	
Entrust Root Certification Autho...	Entrust Root Certification Authority	11/27/2026	Client Authenticatio...	Entrust	
Entrust Root Certification Autho...	Entrust Root Certification Authorit...	12/7/2030	Client Authenticatio...	Entrust.net	
Entrust.net Certification Authorit...	Entrust.net Certification Authority (...	7/24/2029	Client Authenticatio...	Entrust (2048)	
GlobalSign	GlobalSign	3/18/2029	<All>	<None>	
GlobalSign	GlobalSign	3/18/2029	Client Authenticatio...	GlobalSign Root CA ...	
GlobalSign Root CA	GlobalSign Root CA	1/28/2028	<All>	<None>	
GlobalSign Root CA	GlobalSign Root CA	1/28/2028	Client Authenticatio...	GlobalSign Root CA ...	
Go Daddy Class 2 Certification A...	Go Daddy Class 2 Certification Aut...	6/29/2034	Client Authenticatio...	Go Daddy Class 2 C...	
Go Daddy Root Certificate Auth...	Go Daddy Root Certificate Authori...	12/31/2037	<All>	<None>	
Go Daddy Root Certificate Auth...	Go Daddy Root Certificate Authori...	12/31/2037	Client Authenticatio...	Go Daddy Root Cert...	
ISRG Root X1	ISRG Root X1	6/4/2035	Client Authenticatio...	ISRG Root X1	
Logitech Inc	DigiCert Trusted G4 Code Signing ...	4/10/2025	Code Signing	<None>	
Microsoft Authenticode(tm) Roo...	Microsoft Authenticode(tm) Root ...	12/31/1999	Secure Email, Code ...	Microsoft Authentic...	
Microsoft ECC Product Root Cert...	Microsoft ECC Product Root Certifi...	2/27/2043	<All>	Microsoft ECC Prod...	
Microsoft ECC TS Root Certificat...	Microsoft ECC TS Root Certificate ...	2/27/2043	<All>	Microsoft ECC TS Ro...	
Microsoft Root Authority	Microsoft Root Authority	12/31/2020	<All>	Microsoft Root Aut...	
Microsoft Root Certificate Autho...	Microsoft Root Certificate Authority	5/9/2021	<All>	Microsoft Root Certi...	
Microsoft Root Certificate Autho...	Microsoft Root Certificate Authorit...	6/23/2035	<All>	Microsoft Root Certi...	
Microsoft Root Certificate Autho...	Microsoft Root Certificate Authorit...	3/22/2036	<All>	Microsoft Root Certi...	
Microsoft Time Stamp Root Cert...	Microsoft Time Stamp Root Certifi...	10/22/2039	<All>	Microsoft Time Sta...	
NO LIABILITY ACCEPTED, (c)97 Ve...	NO LIABILITY ACCEPTED, (c)97 VeriS...	1/7/2004	Time Stamping	VeriSign Time Stam...	
QuoVadis Root CA 2 G3	QuoVadis Root CA 2 G3	1/12/2042	Client Authenticatio...	QuoVadis Root CA 2...	
QuoVadis Root Certification Aut...	QuoVadis Root Certification Autho...	3/17/2021	Client Authenticatio...	QuoVadis Root Certi...	
SecureTrust CA	SecureTrust CA	12/31/2029	Client Authenticatio...	Trustwave	
Security Communication RootCA1	Security Communication RootCA1	9/29/2023	Client Authenticatio...	SECOM Trust Syste...	
Security Communication RootCA2	Security Communication RootCA2	5/29/2029	Client Authenticatio...	SECOM Trust Syste...	
SSL.com Root Certification Auth...	SSL.com Root Certification Authori...	2/12/2041	Client Authenticatio...	SSL.com Root Certifi...	
Starfield Class 2 Certification Aut...	Starfield Class 2 Certification Auth...	6/29/2034	Client Authenticatio...	Starfield Class 2 Cert...	
Starfield Root Certificate Authori...	Starfield Root Certificate Authority...	12/31/2037	Client Authenticatio...	Starfield Root Certifi...	
Symantec Enterprise Mobile Ro...	Symantec Enterprise Mobile Root f...	3/14/2032	Code Signing	<None>	
Thawte Timestamping CA	Thawte Timestamping CA	12/31/2020	Time Stamping	Thawte Timestampi...	
USERTrust ECC Certification Auth...	USERTrust ECC Certification Author...	1/18/2038	Client Authenticatio...	Sectigo ECC	
USERTrust RSA Certification Auth...	USERTrust RSA Certification Author...	1/18/2038	Client Authenticatio...	Sectigo	
VeriSign Class 3 Public Primary C...	VeriSign Class 3 Public Primary Cert...	7/16/2036	Client Authenticatio...	VeriSign	
VeriSign Universal Root Certifica...	VeriSign Universal Root Certificatio...	12/1/2037	<All>	<None>	

MIS 5214

Mac OS X

The root store is in the Keychain.app

1. Search Finder (Spotlight) for "keychain"
2. Double-click Keychain Access app
3. Select "System Roots" in the left-hand pane

Certificate Revocation List (CRL) – in principle

CRL is the mechanism for the CA to let others know that a certificate has become invalid for some reason

A certificate may be revoked because
- The key holder's private key was compromised
- CA discovered the Certificate was issued to the wrong person
- The certificate expired
- The certificate became invalid for other reasons…

The CA handles revocation by putting the revoked certificate's information on a *certificate revocation list* (CRL)
- The CRL is a list of every certificate that has been revoked
- The CRL is maintained and updated

Certificate Revocation List (CRL) – in practice

CRLs are problematic in many PKI implementations for many reasons
- Either user's browser must check a central CRL to find out if a certificate has been revoked
- …or the CA must continually push out CRL values to clients to ensure they have an updated CRL

By default, web browsers do not check a CRL to ensure that a certificate is not revoked
- So when you are setting up a SSL connection to do e-Commerce over the Internet, you may be relying on a revoked certificate and not know it

Online Certificate Status Protocol (OCSP) is increasingly being used…
- If OCSP is implemented, it works automatically
- OCSP does real-time certificate validation
  - Checks the CRL maintained by the CA
  - Notifies user if certificate is valid, invalid, or unknown

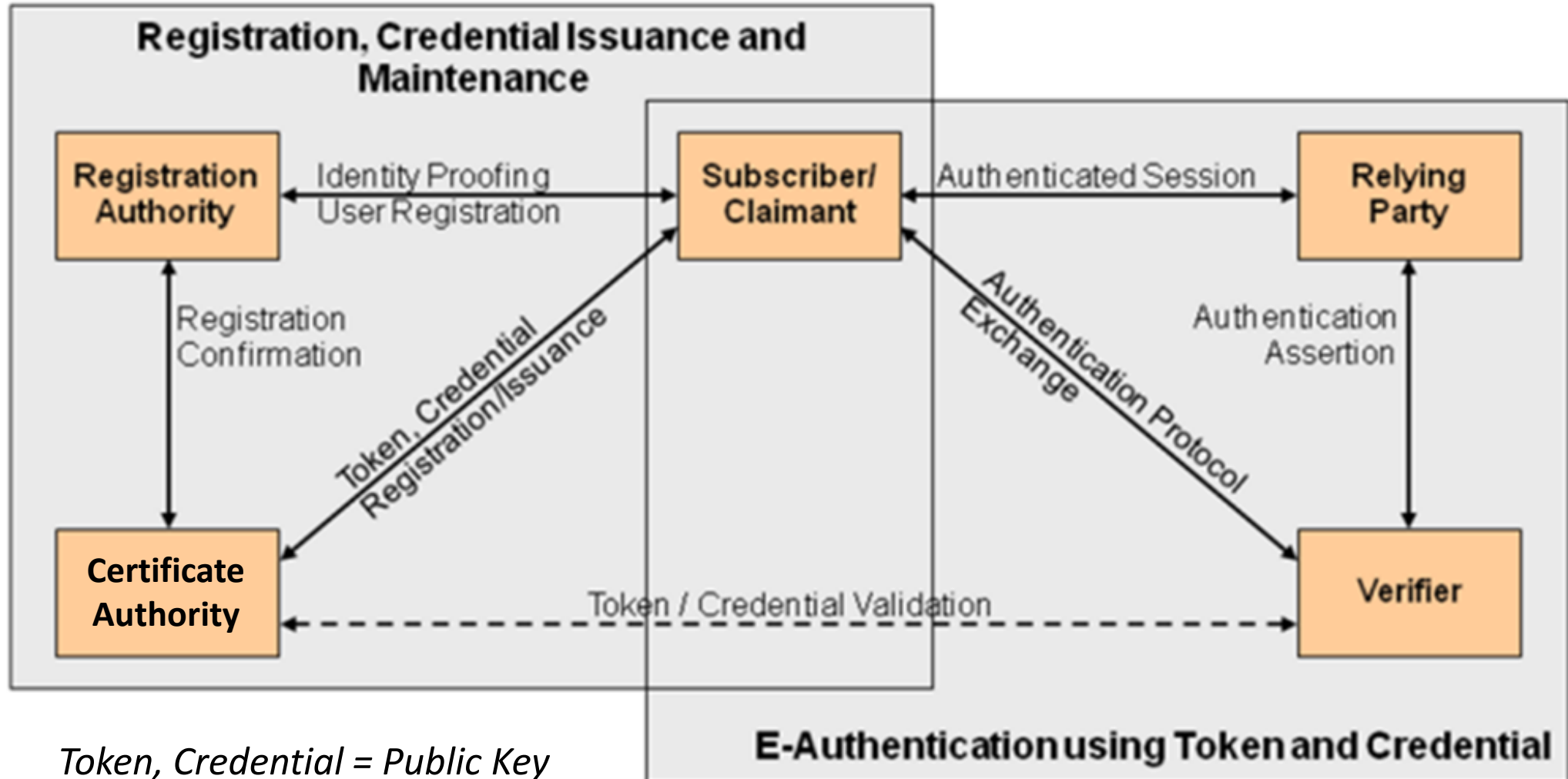# OCSP Stapling Solution *(Note: newly added after lecture)*

Servers include (or **staple**) the cached OCSP response in their HTTPS responses alongside the SSL certificate

- This enables browsers before the secure connection is established to verify the CAs signature on the OCSP response and be assured that the certificate has not been revoked
- OCSP stapling enables servers to retrieve cached OCSP responses in non-real-time and remove performance overhead imposed by CRLs and OCSP
- OCSP stapling does not completely solve OCSP's soft-fail security issue, since stapling is implemented in the server and browsers cannot know if a server actually supports Stapling or not

- OCSP Must-Staple (extension of SSL Certificates: [RFC 7633](#))
  - Mandates OCSP stapling for the certificate
  - If a browser encounters a certificate with this extension that is used without OCSP Stapling, then it will be rejected
  - Enabling OCSP stapling on servers improves security and performance for your web site at the same time

https://www.ssl.com/article/page-load-optimization-ocsp-stapling/

PKI Roles and Workflows

Token, Credential = Public Key

Where do you look for Security Controls for PKI Certificates ?

CNTL NO.	CONTROL NAME	PRIORITY	INITIAL CONTROL BASELINES		
			LOW	MOD	HIGH
System and Communications Protection					
SC-1	System and Communications Protection Policy and Procedures	P1	SC-1	SC-1	SC-1
SC-2	Application Partitioning	P1	Not Selected	SC-2	SC-2
SC-3	Security Function Isolation	P1	Not Selected	Not Selected	SC-3
SC-4	Information in Shared Resources	P1	Not Selected	SC-4	SC-4
SC-5	Denial of Service Protection	P1	SC-5	SC-5	SC-5
SC-6	Resource Availability	P0	Not Selected	Not Selected	Not Selected
SC-7	Boundary Protection	P1	SC-7	SC-7 (3) (4) (5) (7)	SC-7 (3) (4) (5) (7) (8) (18) (21)
SC-8	Transmission Confidentiality and Integrity	P1	Not Selected	SC-8 (1)	SC-8 (1)
SC-9	**Withdrawn**	---	---	---	---
SC-10	Network Disconnect	P2	Not Selected	SC-10	SC-10
SC-11	Trusted Path	P0	Not Selected	Not Selected	Not Selected
SC-12	Cryptographic Key Establishment and Management	P1	SC-12	SC-12	SC-12 (1)
SC-13	Cryptographic Protection	P1	SC-13	SC-13	SC-13
SC-14	**Withdrawn**	---	---	---	---
SC-15	Collaborative Computing Devices	P1	SC-15	SC-15	SC-15
SC-16	Transmission of Security Attributes	P0	Not Selected	Not Selected	Not Selected
SC-17	Public Key Infrastructure Certificates	P1	Not Selected	SC-17	SC-17
SC-18	Mobile Code	P2	Not Selected	SC-18	SC-18
SC-19	Voice Over Internet Protocol	P1	Not Selected	SC-19	SC-19
SC-20	Secure Name /Address Resolution Service (Authoritative Source)	P1	SC-20	SC-20	SC-20
SC-21	Secure Name /Address Resolution Service (Recursive or Caching Resolver)	P1	SC-21	SC-21	SC-21
SC-22	Architecture and Provisioning for Name/Address Resolution Service	P1	SC-22	SC-22	SC-22
SC-23	Session Authenticity	P1	Not Selected	SC-23	SC-23
SC-24	Fail in Known State	P1	Not Selected	Not Selected	SC-24

NIST Special Publication 800-53
Revision 5

Security and Privacy Controls for Information Systems and Organizations

JOINT TASK FORCE

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-53r5

Septpember 2020
INCLUDES UPDATES AS OF 12-10-2020; SEE PAGE XVII

U.S. Department of Commerce
Wilbur L. Ross, Jr., Secretary

National Institute of Standards and Technology
Walter Copan, NIST Director and Under Secretary of Commerce for Standards and Technology

Where else do you look for Security Controls based on the use of PKI Certificates ?

*…there are a number of controls that use certificates, including:*

certificate   2/56   ∧ ∨ ✕

CM-14 SIGNED COMPONENTS

Control: Prevent the installation of [*Assignment: organization-defined software and firmware components*] without verification that the component has been digitally signed using a certificate that is recognized and approved by the organization.

Discussion: Software and firmware components prevented from installation unless signed with recognized and approved certificates include software and firmware version updates, patches, service packs, device drivers, and basic input/output system updates. Organizations can identify applicable software and firmware components by type, by specific items, or a combination of both. Digital signatures and organizational verification of such signatures is a method of code authentication.

Related Controls: CM-7, SC-12, SC-13, SI-7.

References: [IR 8062].
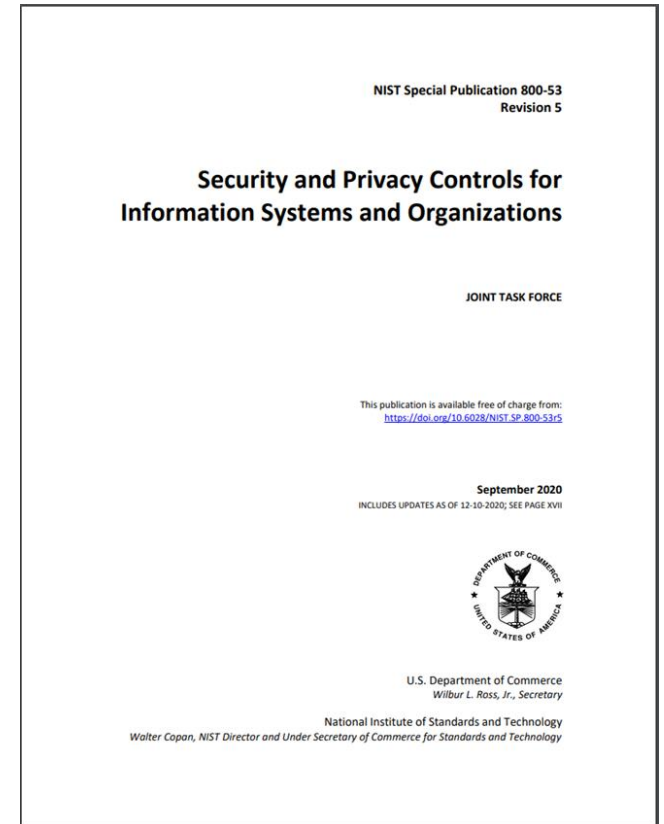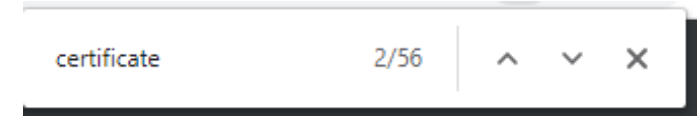
Agenda

- ✓ In The News
- ✓ Quick Review: Reasons to Use Cryptography
- ✓ Digital Certificates
- ✓ Public Key Infrastructure
- Types of Networks
- OSI Model
- Layer 1 Network Devices
- Layer 2 Network Devices
- Layer 3 Network Devices
- Layer 3 – 7 Network Devices
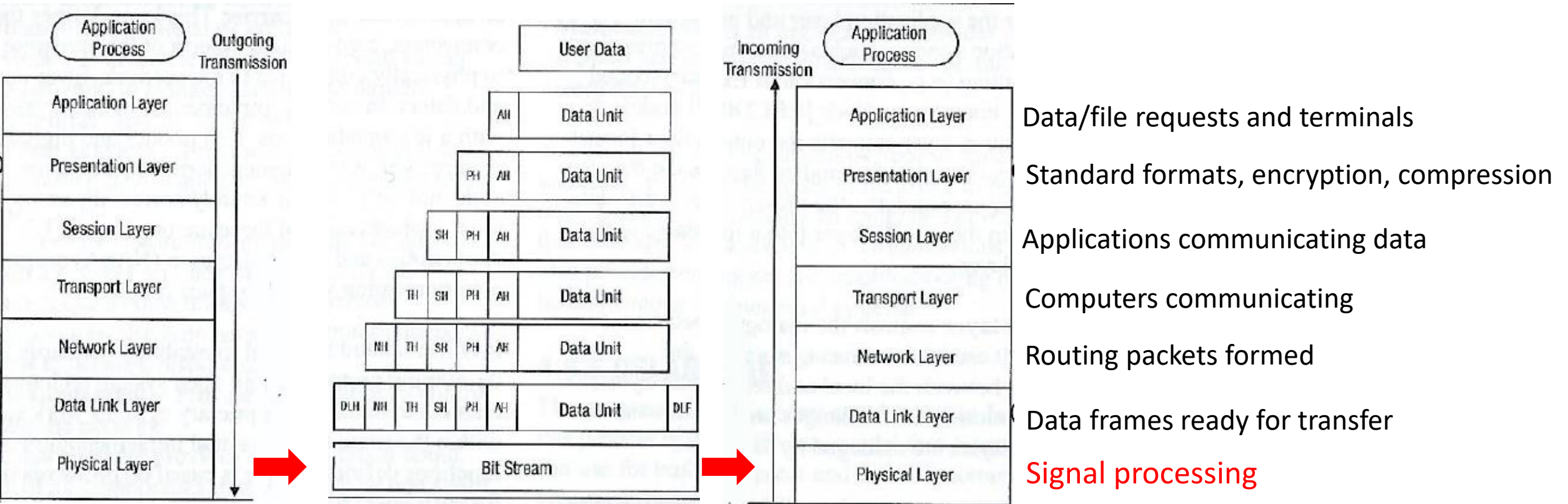
Types of networks

- Personal Area Network (PAN)
    - Generally, a microcomputer network used for communications among personal computer devices being used by an individual
        - Laptops, tablets, printers, scanners, cameras, telephones
    - May also be connected to a higher-level network and the Internet
    - Extent is typically within 10 meters (33 feet)
    - May be wired with computer buses such as Universal Serial Bus (USB)
    - A Wireless PAN (WPAN) can be set up using network technology such as infrared data association (IrDA) and Bluetooth (piconet)
        - A piconet can include up to 8 active devices in master-slave relationship can range from 10 meters to 100 meters

Types of networks

- Local Area Network (LAN)
  - Cover a limited area, such as home, office or campus
  - Characteristics: High data transfer rates, with smaller geographic range
  - Eithernet and Wi-Fi (WLANs) are the 2 most common technologies used

- Storage Area Network (SAN)
  - Centralize the process for the storage and administration of data
  - Variation of LAN dedicated to connecting storage devices to servers and other computing devices

- Wide Area Network (WAN)
  - Computer network that covers a broad area, such as a city, region, nation or an international link
  - Used to connect LANS and other types of networks together so that users and computers in one location can communicate with users and computers in other locations
    - May be private and built for 1 particular organization
    - May be built by Internet Service Providers (ISPs) to provide connections from an organization's LAN to the Internet
    - May be wireless (WWAN)
  - Internet is the largest example of a WAN

- Metropolitan Area Network (MAN)
  - A WAN that is limited to a city or a region
  - MANs are usually, characterized by higher data transfer rates than WANs

OSI Model

Data/file requests and terminals

Standard formats, encryption, compression

Applications communicating data

Computers communicating

Routing packets formed

Data frames ready for transfer

Signal processing

Layer 1: Physical Layer

Network Interface Card (NIC)

- Produces and interprets electromagnetic signals from the network to/from binary bits processed in the computer

- Converts bits into signals or voltages suitable for transmission across the Local Area Network (LAN) and/or Wide Area Network technology it is connected to

- Determines synchronization, data transfer rates, line noise and transmission techniques based on the physical connection to electrical, optical or mechanical equipment

E.g. A '1' bit transmitted via Ethernet would be translated by the NIC to +0.5-volt electric signal, and '0' bit would be transmitted as 0-volts

TIA – Telecommunications Industry Association
EIA – Electronic Industry Alliance
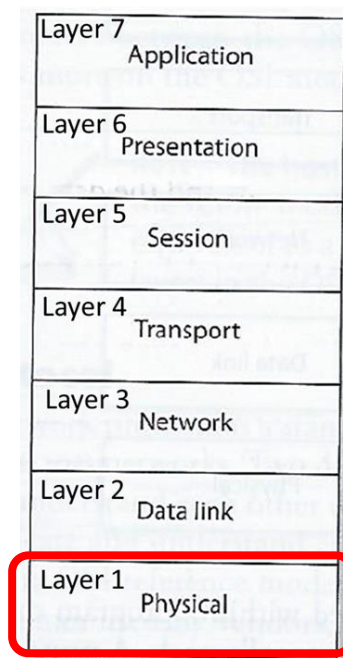
Standard interfaces at this layer include:

- RS/EIA/TIA-422, RS/EIA/TIA-423, RS/EIA/TIA-429, RS/EIA/TIA-449, RS/EIA/TIA-485
- 10Base-T, 10Base2, 10Base5, 100Base-TX, 100Base-FX, 100Base-T, 1000Base-T, 1000-Base-SX

Layer 1 Network Components – Repeaters & Hubs

- A <u>repeater</u> provides the simplest type of connectivity
  - ***Work at the physical layer (Layer 1) – looks at the electrical signal (not within the packets)***
  - Add-on devices for extending a network over a greater distance by repeating electrical signals between cable segments
  - Needed to amplify signals because signals are attenuated (reduced) the further they travel
- A <u>hub</u> is a multiport repeater
  - Often referred to as a "concentrator" physically connecting several computers and devices enabling them to communicate with each other
  - When one system sends a signal to go to another system, the hub broadcasts the signal to all ports and systems connected to the hub
- Does not understand nor work with IP or MAC addresses
- Can work as a line conditioner to clean up signals
  - Works much better when amplifying digital signals which are discrete units – making removal of background noise much easier
  - When amplifying analog signals, accompanying noise can be amplified too – further distorting the signal

Layer 1 Collision Domain – Hubs

- The term **collision domain** is used to describe a part of a network where packet collisions can occur
    - Packet collisions occur when two devices on a shared network segment send packets simultaneously
    - The colliding packets must be discarded and sent again, which reduces network efficiency

- Collisions occur often in a hub environment because all devices connected to the hub are in the same collision domain

Hub

Collision domain

- Total network bandwidth is shared among all devices
- Only one device may transmit at time, and all the other devices connected to the hub must listen to the network in order to avoid collisions
- This contention and resulting collisions causes traffic delays and uses up previous bandwidth
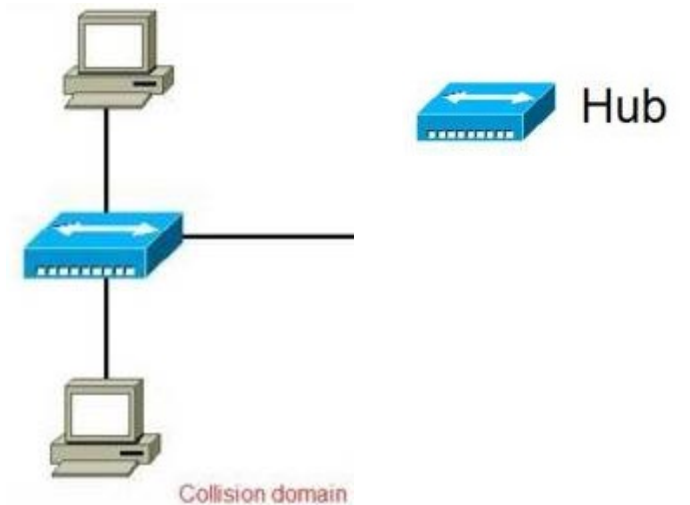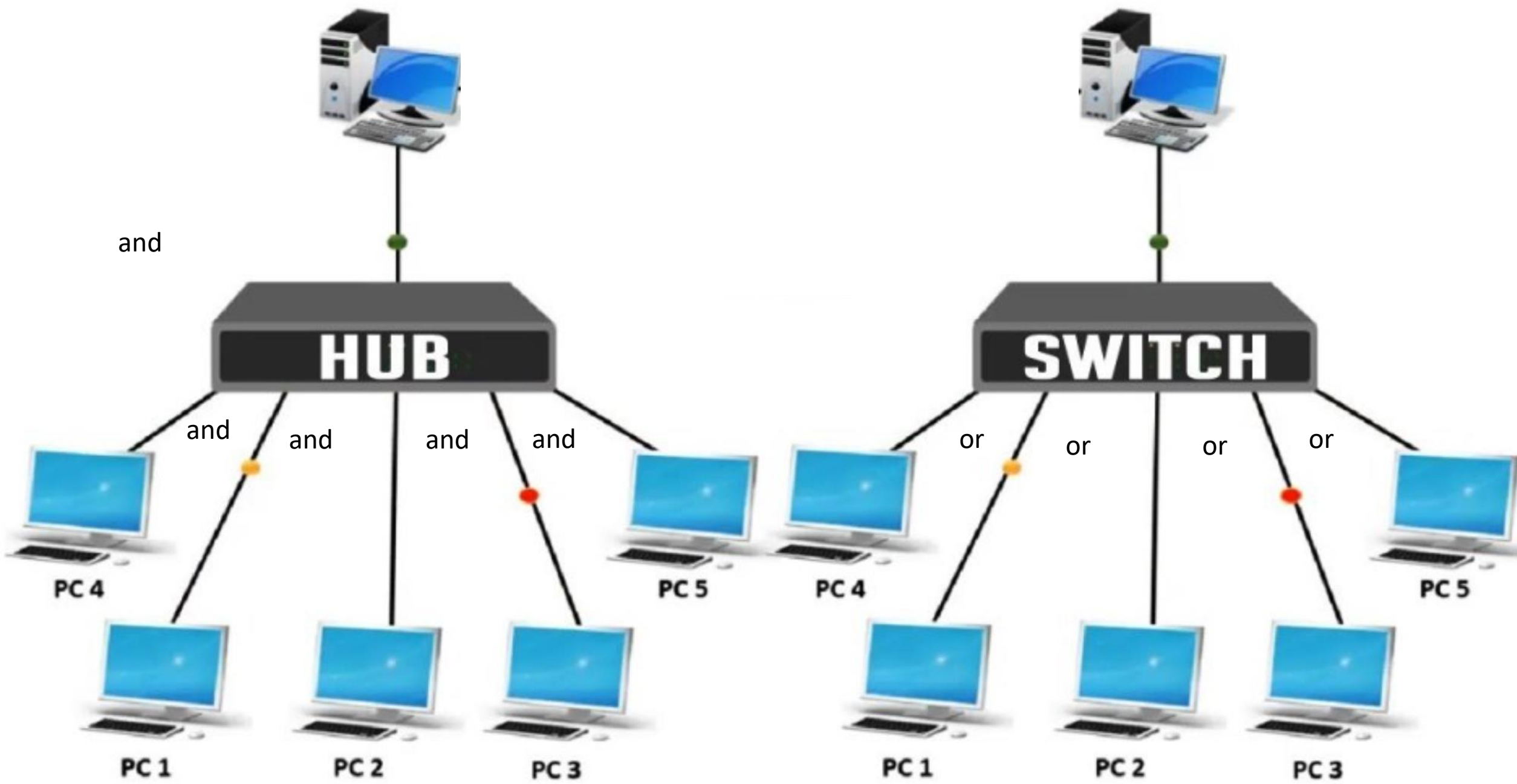
Layer 2 Network Components – Bridge

- Local Area Network (LAN) device used to connect LAN segments
  - ***Works at the data link layer (Layer 2) – looks at the MAC address within the header***
  - Used to segment larger overburdened networks into smaller segments to reduce collision domains and ensure better use of bandwidth and traffic control
  - Amplifies the electrical signal (like a repeater)
  - Has more intelligence than a repeater for filtering frames and controlling where they go
- Filters data frames based on MAC addresses at data link layer (not with IP addresses)
  - When data frame arrives the bridge determines if MAC address is on LAN segment, and if so it sends the data to the port which the network segment is connected
  - If MAC address is not on LAN segment, bridge forwards frame to correct network segment
- "Transparent bridging"
  - Enables bridges to dynamically learn and record MAC addresses and ports from computers sending data frames
- 3 types of bridges:
  1. Local bridge – connects 2+ LAN segments within a local area (e.g. building)
  2. Remote bridge – connects 2+ LAN segments over a Metropolitan Area Network (MAN) using telecommunication links (e.g. telephone or other transmission lines)
  3. Translation bridge – translates protocols as it connects 2+ different types of networks (e.g. Ethernet and fiberoptic)
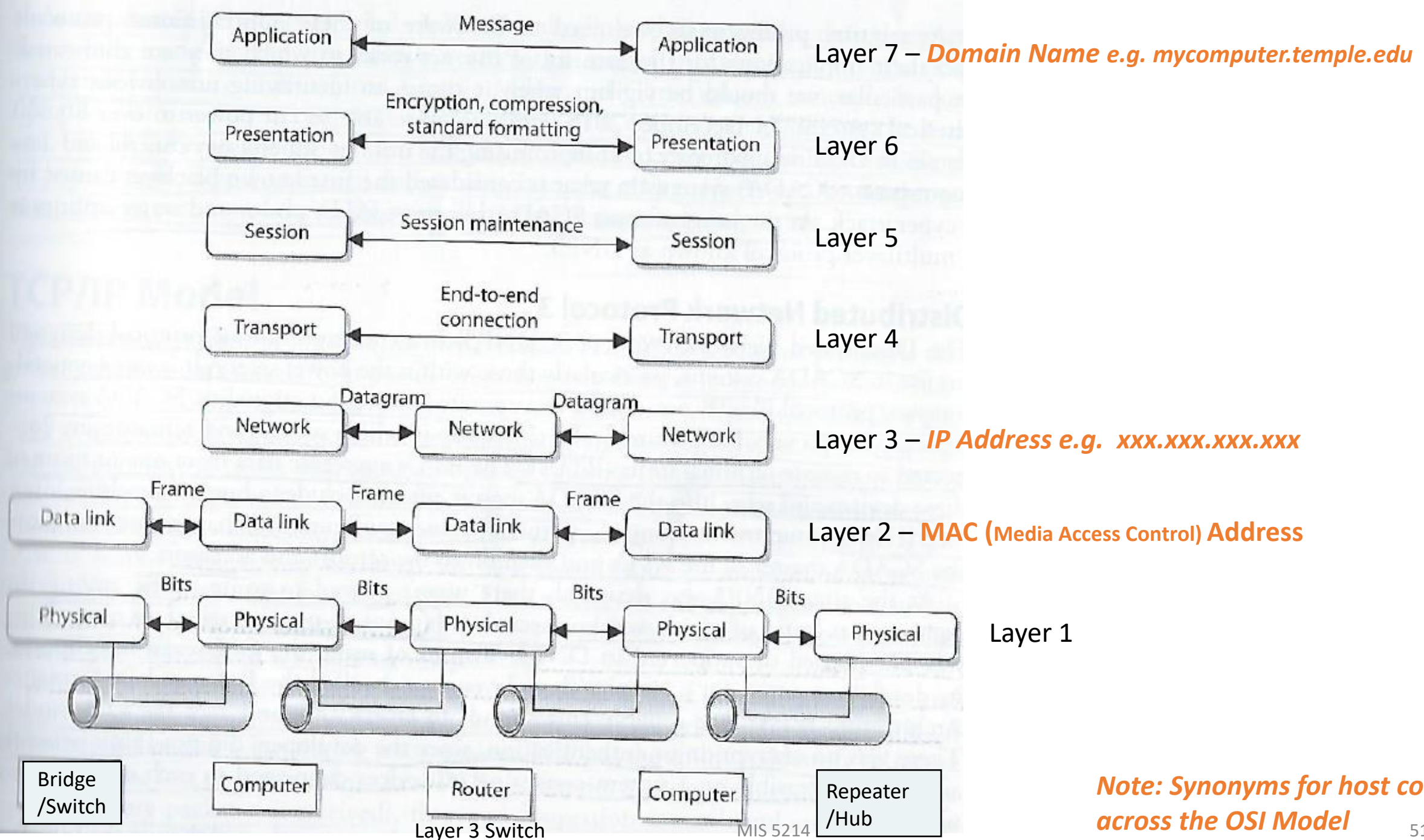
Layer 2 Network Components – Switch (basic)

Works at the data link layer (Layer 2), forwarding traffic based on MAC addresses

- Is a multiport bridging device, and each port provides dedicated bandwidth to each device attached to it
    - A port is bridged to another port so the 2 devices have an end-to-end private link
    - Employs full-duplex communication, ensures the 2 are not competing for the same bandwidth
        - 1 wire pair is used for sending, another pair used for receiving
- Reduces and removes the sharing of the network medium and problems that come with it
    - When the data frame comes to the switch, the switch sends the frame directly to the destination computer or network
        - Results in
            - A reduction of traffic
            - More efficient use of network bandwidth
            - Decreased latency
            - Increased security – each computer can only see traffic sent to it MAC address (blocks eavesdropping)
- Contention between computers using the network and collisions are not issues when switches are used

HUB

and

and · and · and · and

PC 4 · PC 1 · PC 2 · PC 3 · PC 5

SWITCH

or · or · or · or

PC 4 · PC 1 · PC 2 · PC 3 · PC 5

Application	Message	Application

Layer 7 – *Domain Name e.g. mycomputer.temple.edu*

Presentation — Encryption, compression, standard formatting — Presentation

Layer 6

Session — Session maintenance — Session

Layer 5

Transport — End-to-end connection — Transport

Layer 4

Network — Datagram — Network — Datagram — Network

Layer 3 – *IP Address e.g. xxx.xxx.xxx.xxx*

Data link — Frame — Data link — Frame — Data link — Frame — Data link

Layer 2 – **MAC (Media Access Control) Address**

Physical — Bits — Physical — Bits — Physical — Bits — Physical — Bits — Physical

Layer 1

Bridge /Switch

Computer

Layer 3 Switch

Router

Computer

MIS 5214

Repeater /Hub

Note: Synonyms for host computer across the OSI Model

51

Layer 3 Network Components - Routers

- ***Works at the network layer (Layer 3), looking farther into the frame at the IP address and other routing information***

- Used by administrator to divide network along the lines of departments, workgroups, or other business-oriented divisions

- Connecting 2 or more networks together
  - Can connect similar types of networks (e.g. 2 Ethernet LANS) or different types of networks (e.g. Ethernet LAN to a Token Ring LAN)

- Has 2+ interfaces, a routing table, and is able to calculate the shortest route between sending and receiving hosts
  - Changes header information in the packet so the packet can go to the next correct router, or if the destination computer is on the connecting network, the changes made enable the packet to go directly to the destination computer

- Has a 1st generation fire-wall i.e. Access Control List (ACL) built in
  - When packets arrive at one of the interfaces, the router compares the source and destination IP addresses, protocol type, and source and destination ports to the ACL
  - Decides which packets are allowed in and which are denied

ROUTER

HUB

SWITCH

PC 4

PC 1

PC 2

PC 3

PC 5

PC 4

PC 1

PC 2

PC 3

PC 5
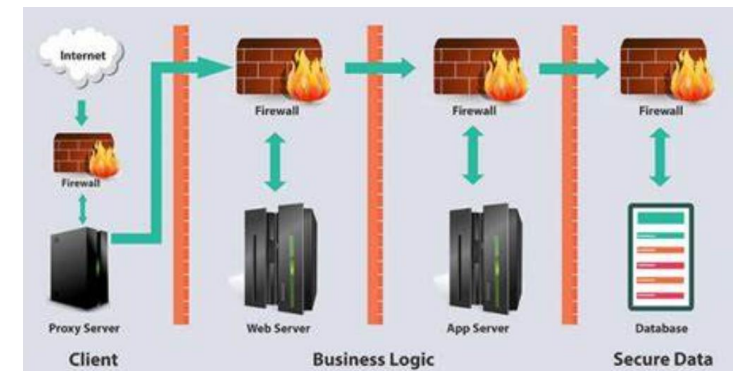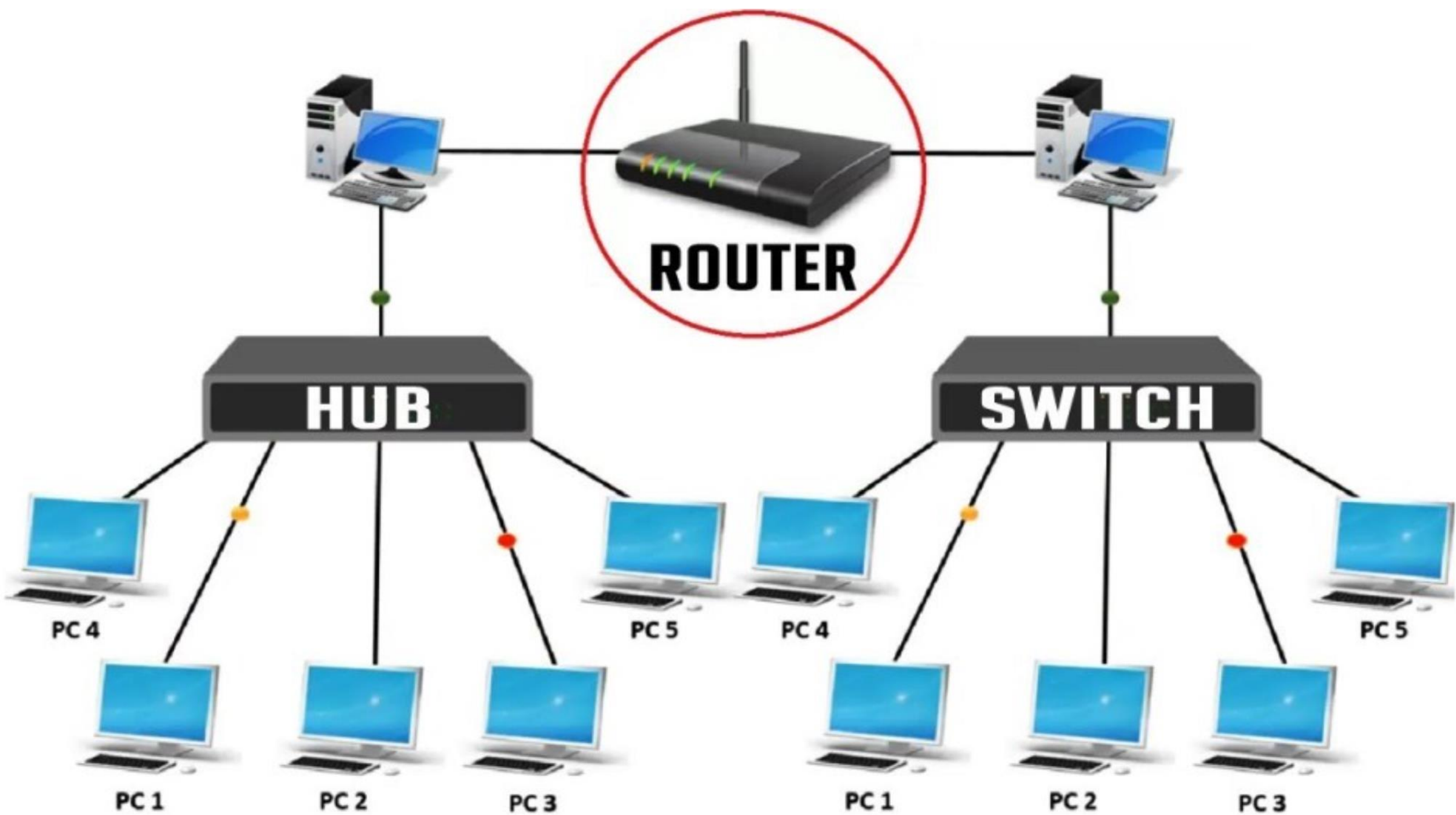
Collision Domains - Bridge, Switch, and Router

In contrast to hubs, every port on a bridge, switch, or a router is in a separate collision domain

- This eliminates the possibility of collisions and enables the devices to use the full-duplex mode of communication, which effectively doubles the maximum data capacity
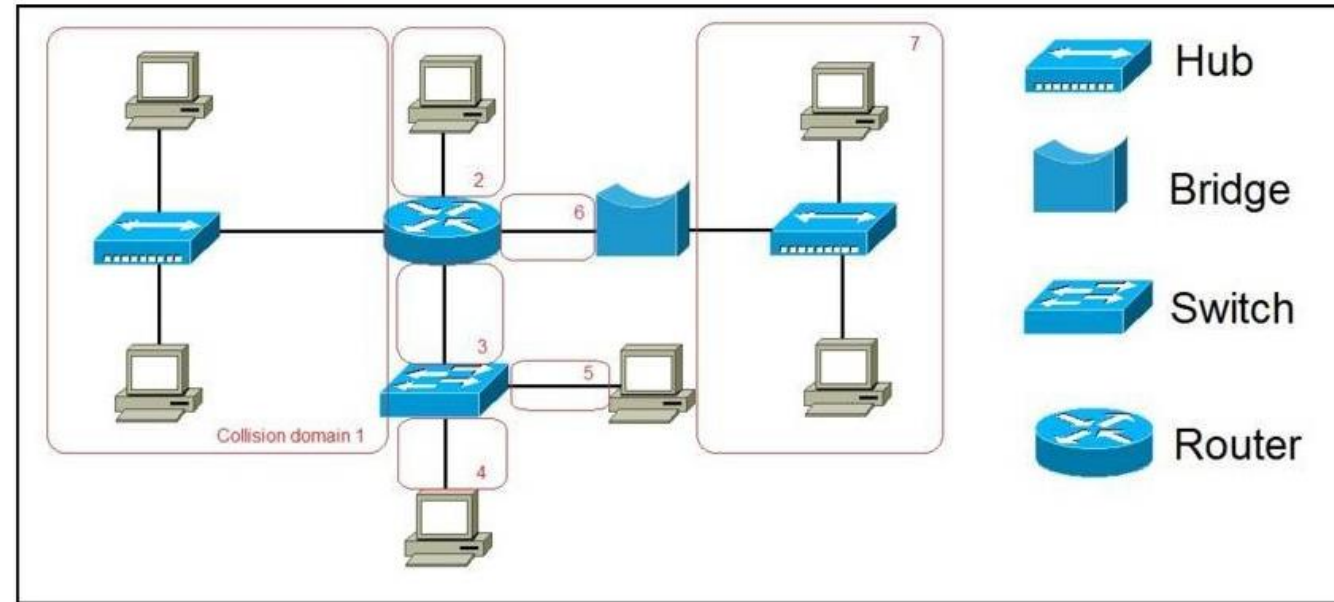
The picture depicts a network of:
- 7 computers, two hubs, a bridge, a switch, and a router
- 7 collision domains are created by these devices, marked in red
    - All devices connected to a hub are in the same collision domain
    - Each port on a bridge, a switch or router is in a separate collision domain

Network Components – Layer 3 Switches

Switches have evolved…

- They now can work at the Network Layer…

- Layer 3 switch is a "router on steroids"

  Has the intelligence of a router (MAC and IP addressing) but is much more efficient

  - While a router's functionality is implemented in software running on a microprocessor, a layer 3 switch's routing functionality is implemented directly in hardware

  - Layer 3 (& 4) switches use Multiprotocol Label Switching (MPLS) for

    - Faster more direct routing between sender and receiver

    - Addressing additional service and security requirements of different types of packets

      - Time-sensitive traffic has higher priority than less sensitive traffic

      - More granular access control

Layer 7 Application
Layer 6 Presentation
Layer 5 Session
Layer 4 Transport
Layer 3 Network
Layer 2 Data link
Layer 1 Physical
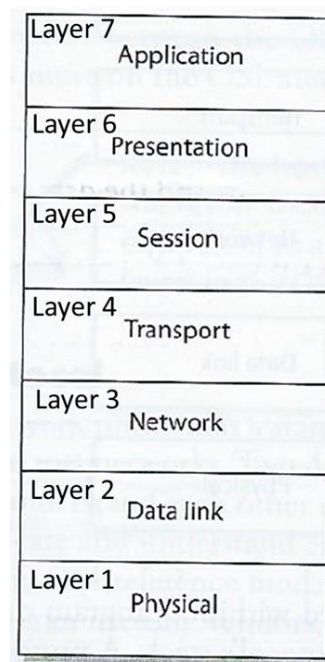
Layer 3+ VLANS

Modern layer 3+ switches enable administrators to create Virtual LANs (VLANs) to separate and group computers logically based on:

- Business needs, resource requirements, and security policies
- Rather than physical location of the systems (as is done with repeaters, bridges, and routers)
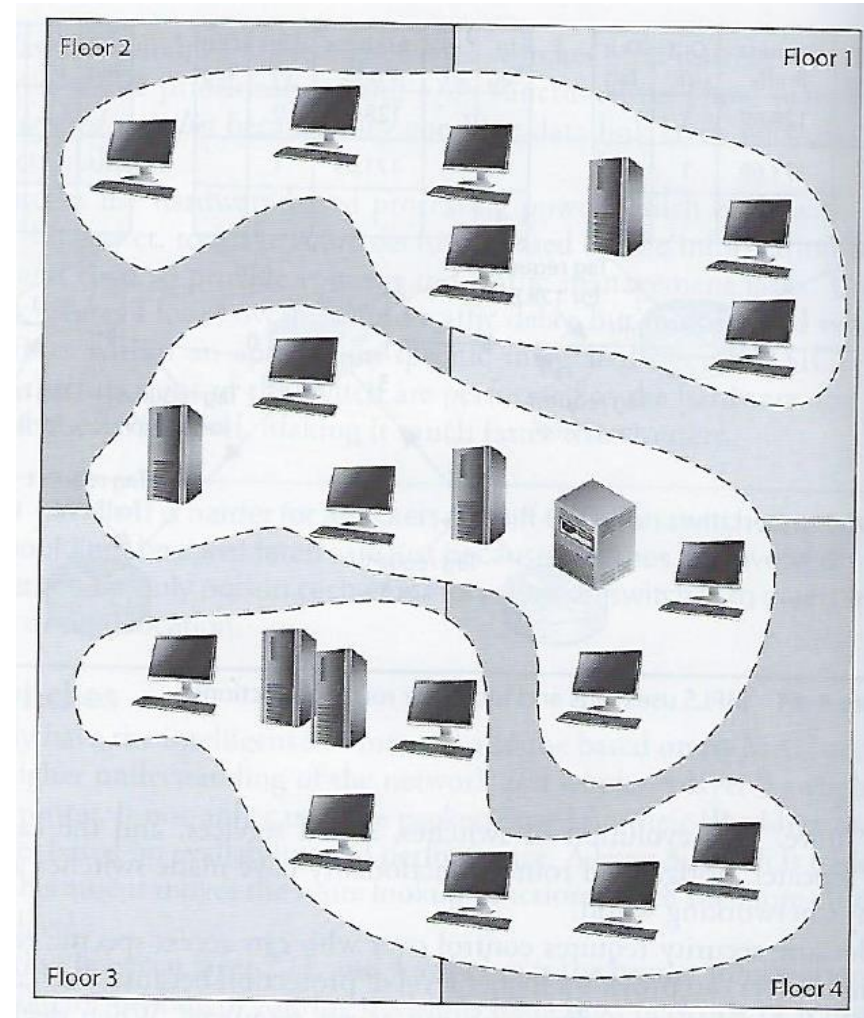
Harris and Maymi (2019) <u>All In One CISSP Exam Guide</u>, p. 604

Layer 3+ VLANS

Exist on a higher logical level than the physical network and are not bound by it

- If Workstation P1 wants to communicate with workstation D1,
  - The message has to be <u>routed</u> even though the workstations are physically next to each other, because they are on different logical networks
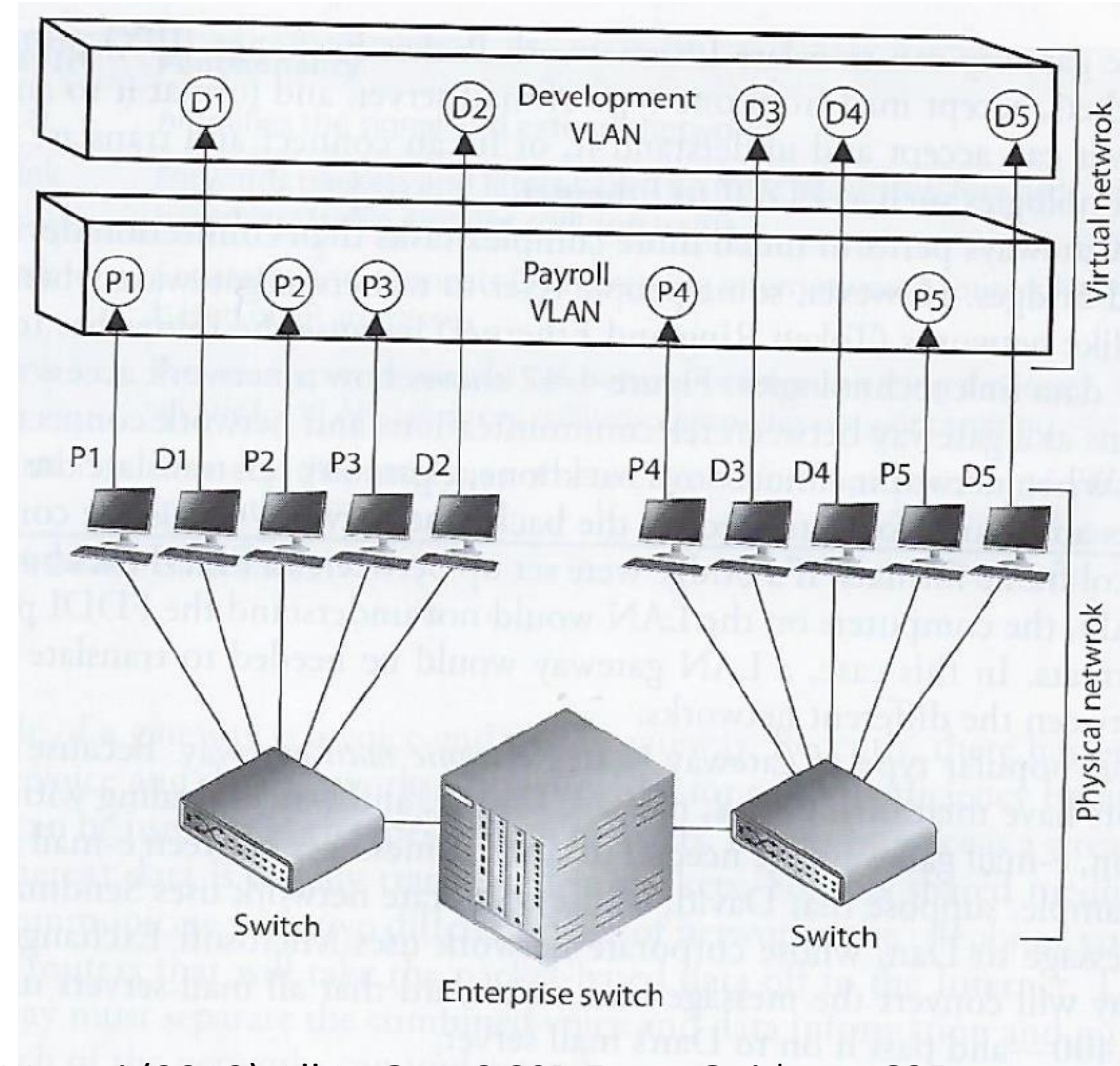
Harris and Maymi (2019) <u>All In One CISSP Exam Guide</u>, p. 605

Layer 3+ VLANS

VLANs enable the administrator the flexibility to apply different security policies to respective logical groups

- If tighter security is required for the payroll department, the administrator can develop policy, add all payroll systems to a specific VLAN, and apply the security policy only to the payroll VLAN

VLANS must be properly configured and managed for security

- VLAN hopping and switch spoofing attacks allow attackers to access traffic in various VLAN segments
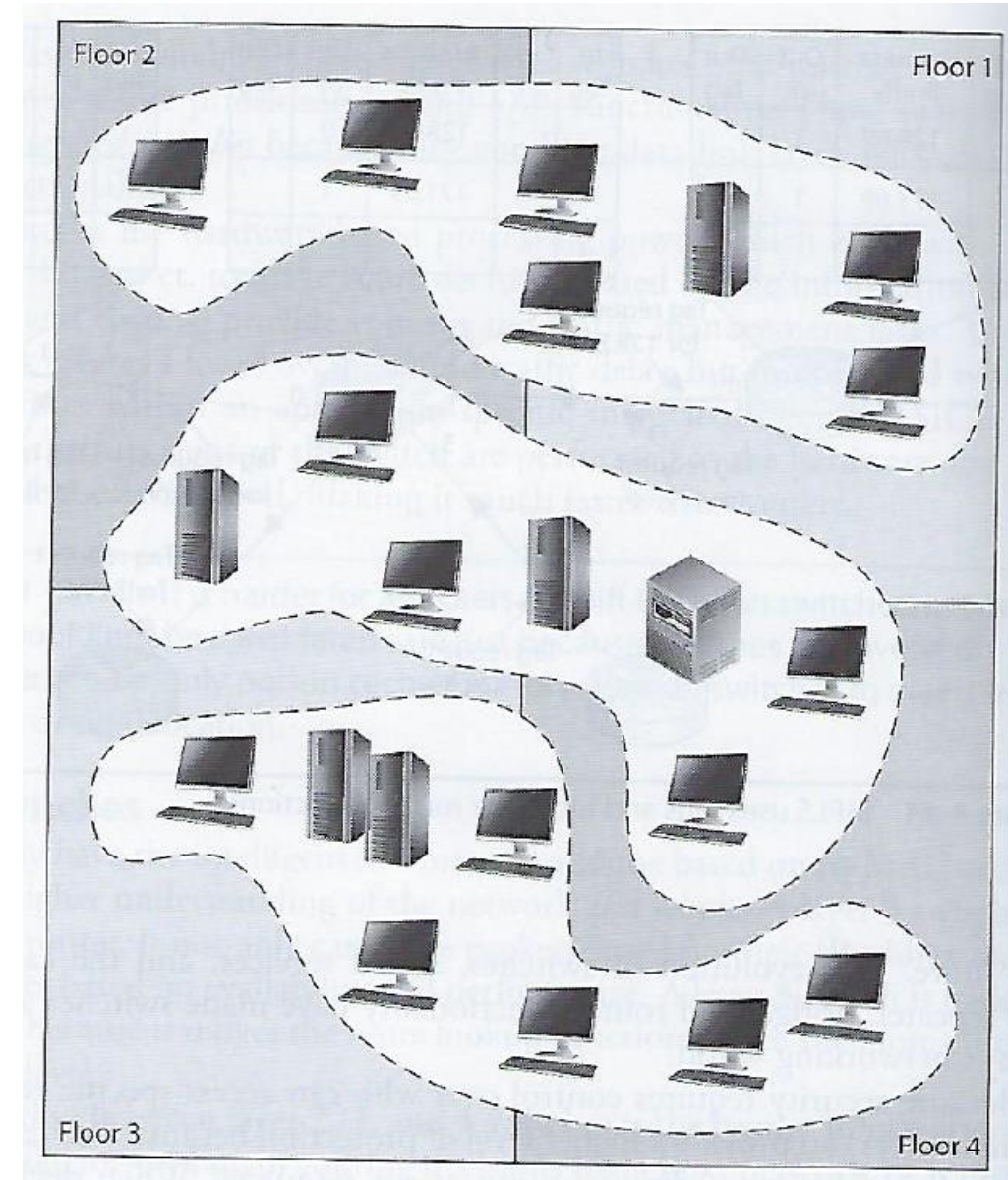
Network Components – Layer 4 through 7 Switches

- Layer 4 switch works at the transport layer, supporting TCP and UDP
  - More resource intensive
  - Able to perform policy-based switching to off-load a sever by balancing traffic across a cluster of servers based on individual session information and status
- Layer 4 – 7 switches are also known as
  - Content switches
  - Web-switches
  - Application-switches
- Used for load-balancing among groups of servers based on: HTTP, HTTPS, VPN, or for any application TCP/IP traffic using a specific port
- Can also be used for TLS encryption/decryption and to centralize the management of digital certificates
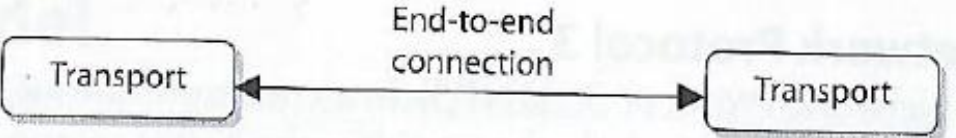
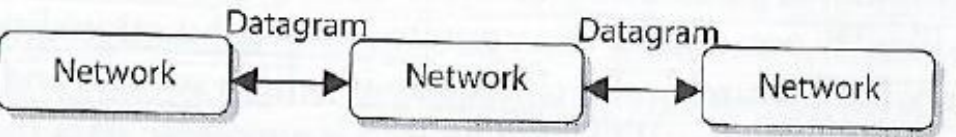| Layer 7 | Application |
Layer 6	Presentation
Layer 5	Session
Layer 4	Transport
Layer 3	Network
Layer 2	Data link
Layer 1	Physical
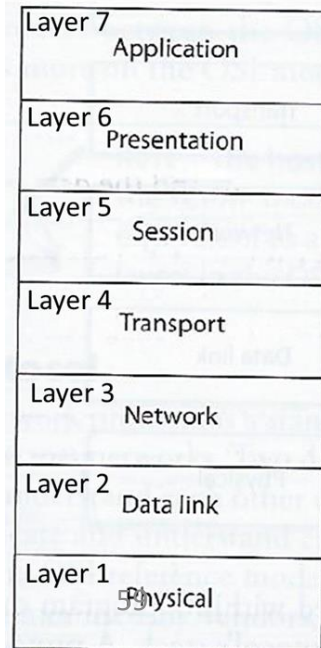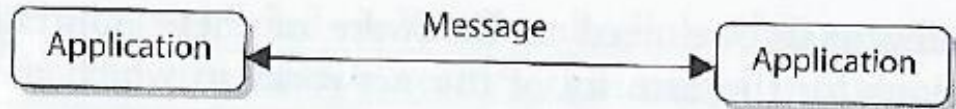
Layer 7 – *Domain Name e.g. mycomputer.temple.edu*
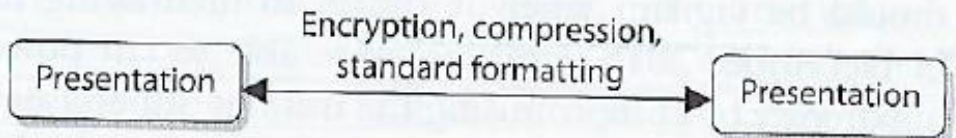
Layer 6
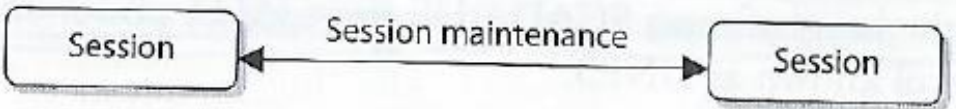
Layer 5

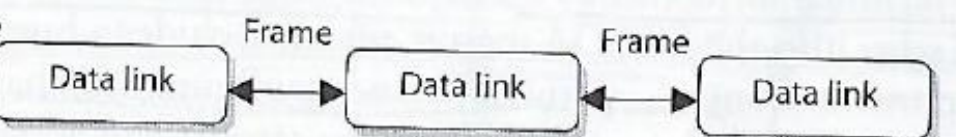Layer 4
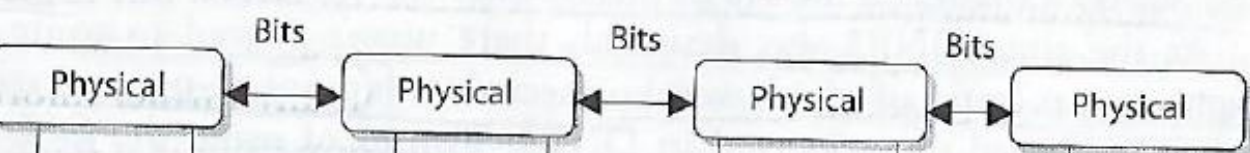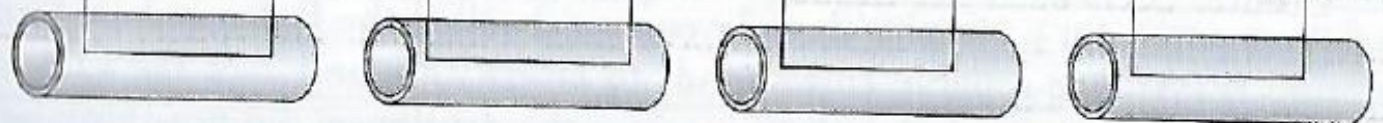
Layer 3 – *IP Address e.g. xxx.xxx.xxx.xxx*

Layer 2 – **MAC (Media Access Control) Address**

Layer 1

Note: Synonyms for host computer across the OSI Model

Bridge /Switch

Computer

Router
Layer 3 Switch

Computer

Repeater /Hub

MIS 5214

60

Layer 7 Network Components - Gateways

Gateway is a general term for software running on a device that connects 2 different environments

- Acts as a translator for their protocols

- Or, restricts their interactions

- …
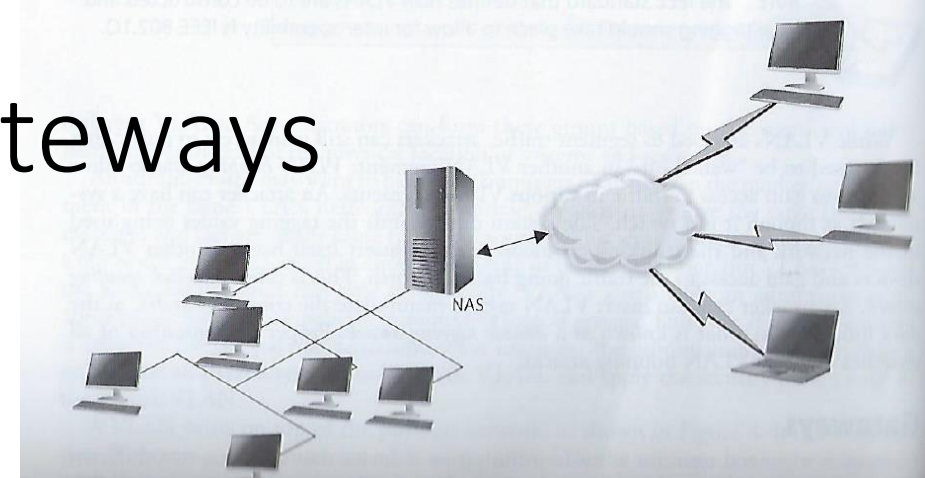
Because of the translation of protocols, many gateways work at Layer 7 Application Layer

- Network attached storage Gateway
- Electronic mail Gateway for "Sendmail" and Microsoft Exchange
- Voice and Media Gateway
- Voice and Data Gateway

Summary – Some differences of Network Devices

Device	OSI Layer	Functionality
Repeater	1 - Physical	Amplifies the signal and extends networks
Bridge	2 - Data link	Forwards packets and filters based on MAC addresses; Forwards broadcast traffic, but not collision traffic
Router	3 - Network	Separates and connects LANS creating internetworks; routers filter based on IP addresses
Switch	2 through 7 – Data link, Network, Transport, Session, Presentation, Application	Provides private virtual link between communicating devices; allows for VLANS; reduces collisions; impedes network sniffing
Gateway	Application	Connects different types of networks; performs protocol and format translations

Note: Router (layer 3) with Layer 4 Firewall protections

tp-link

HackerSploit

Status
Quick Setup
Network
Wireless
Guest Network
DHCP
Forwarding
Security
- Basic Security
- Advanced Security
- Local Management
- Remote Management
Parental Controls
Access Control
Advanced Routing
Bandwidth Control
IP & MAC Binding
Dynamic DNS
IPv6
System Tools
Logout

Advanced Security

DoS Protection: ○ Enable ● Disable

☐ Enable ICMP-Flood Attack Filtering
ICMP-Flood Packets Threshold (5~3600):   50   packets/second

☐ Enable UDP-Flood Attack Filtering
UDP-Flood Packets Threshold (5~3600) :   500   packets/second

☐ Enable TCP-SYN-Flood Attack Filtering
TCP-SYN-Flood Packets Threshold (5~3600) :   50   packets/second

☑ Forbid Ping Packet From WAN Port
☐ Forbid Ping Packet From LAN Port

Save   Blocked DOS Host List

Advanced Security Help

Using the **Advanced Settings** page, you can protect the Router from being attacked by TCP-SYN Flood, UDP Flood and ICMP-Flood.

Note: FLOOD Filtering will take effect only when the **Statistics** in **System Tools** is enabled.

- **DoS Protection** - Enable or Disable the DoS protection function. Only when it is enabled, will the flood filters be enabled.
- **Enable ICMP-FLOOD Attack Filtering** - Enable or Disable the ICMP-FLOOD Attack Filtering.
- **ICMP-FLOOD Packets Threshold (5~3600)** - The default value is 50. Enter a value between 5 ~ 3600. When the current ICMP-FLOOD Packets number is beyond the set value, the Router will startup the blocking
- **Enable UDP-FLOOD Filtering** - Enable or Disable the UDP-FLOOD Filtering.
- **UDP-FLOOD Packets Threshold (5~3600)** - The default value is 500. Enter a value between 5 ~ 3600. When the current UPD-FLOOD Packets number is beyond the set value, the Router will startup the blocking function immediately.
- **Enable TCP-SYN-FLOOD Attack Filtering** - Enable or Disable the TCP-SYN-FLOOD Attack Filtering.
- **TCP-SYN-FLOOD Packets Threshold (5~3600)** - The default value is 50. Enter a value between 5 ~ 3600. When the current TCP-SYN-FLOOD Packets numbers is beyond the set value, the Router will startup the blocking function immediately.
- **Forbid Ping Packet From WAN Port** - Enable or Disable Forbid Ping Packet From WAN Port. The default setting is enabled. The ping packet from WAN cannot access the Router. (Defends against some viruses).
- **Forbid Ping Packet From LAN Port** - Enable or Disable Forbid Ping Packet From LAN Port. The default setting is disabled. If enabled, the ping packet from LAN cannot access the Router. (Defends against some viruses).

Click the **Save** button to save the settings.

Click the **Blocked DoS Host List** button to display the DoS host table by blocking.
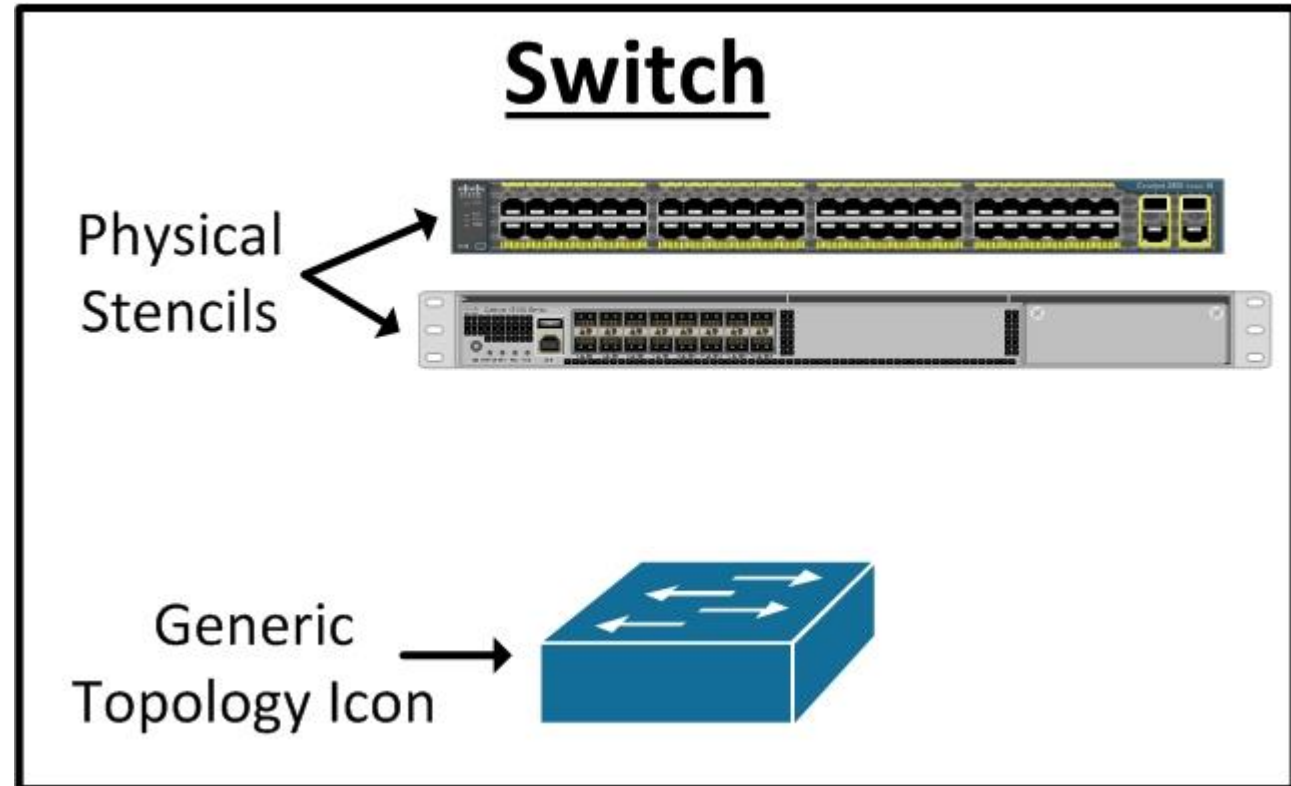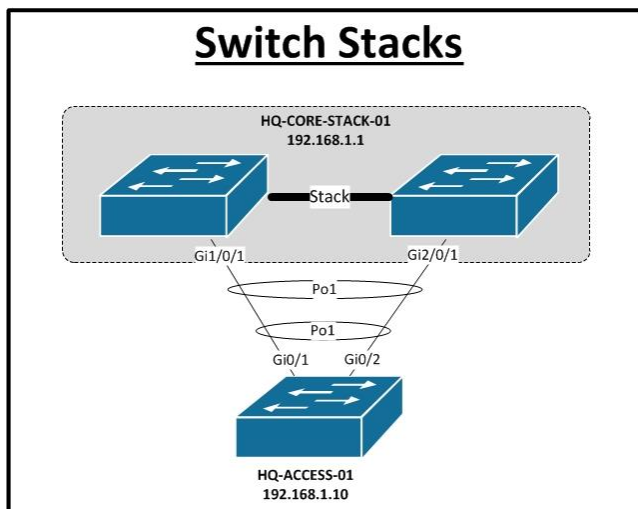
MORE VIDEOS

Agenda

- ✓ In The News
- ✓ Quick Review: Reasons to Use Cryptography
- ✓ Digital Certificates
- ✓ Public Key Infrastructure
- ✓ Types of Networks
- ✓ OSI Model
- ✓ Layer 1 Network Devices
- ✓ Layer 2 Network Devices
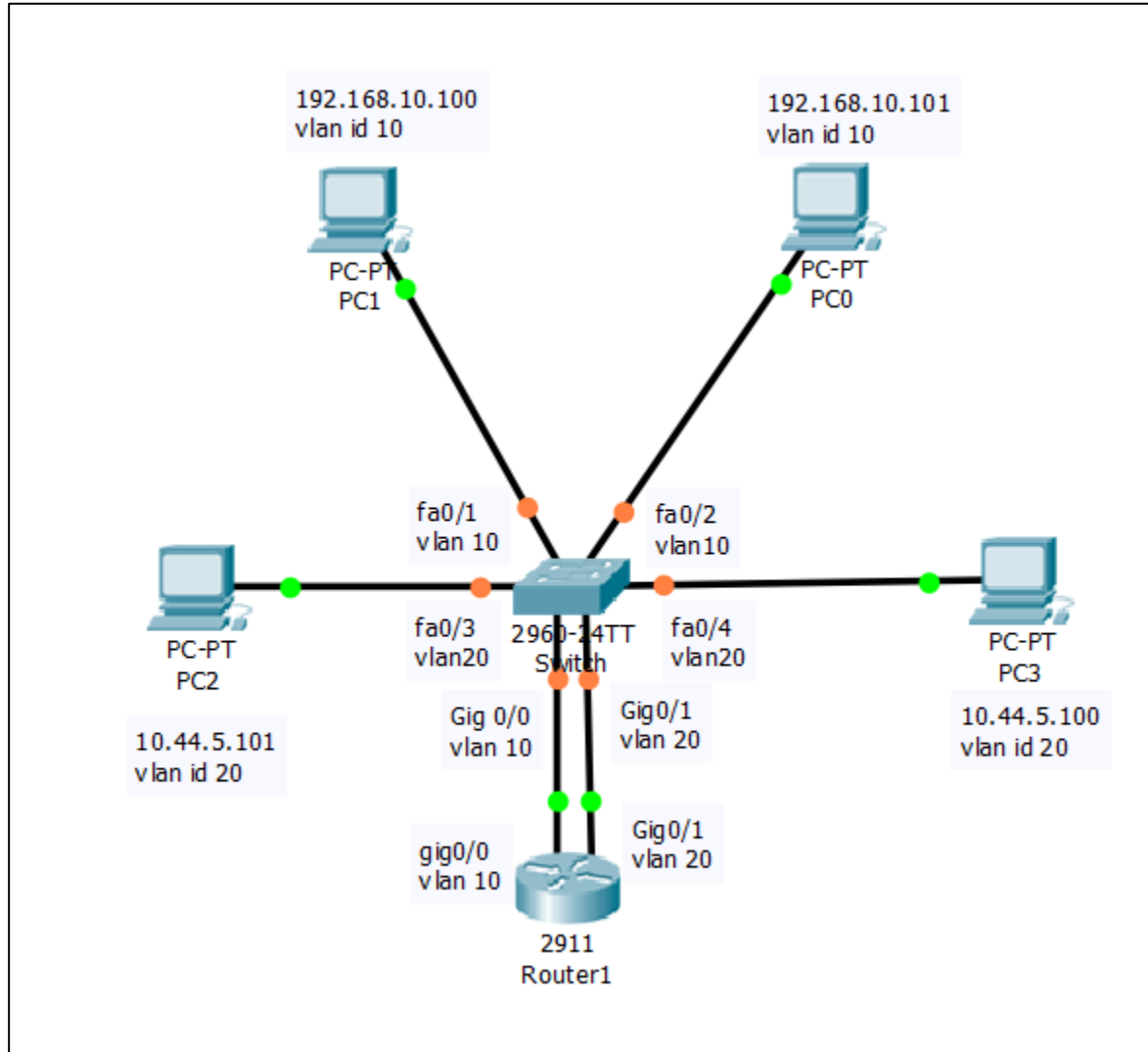- ✓ Layer 3 Network Devices
- ✓ Layer 3 – 7 Network Devices
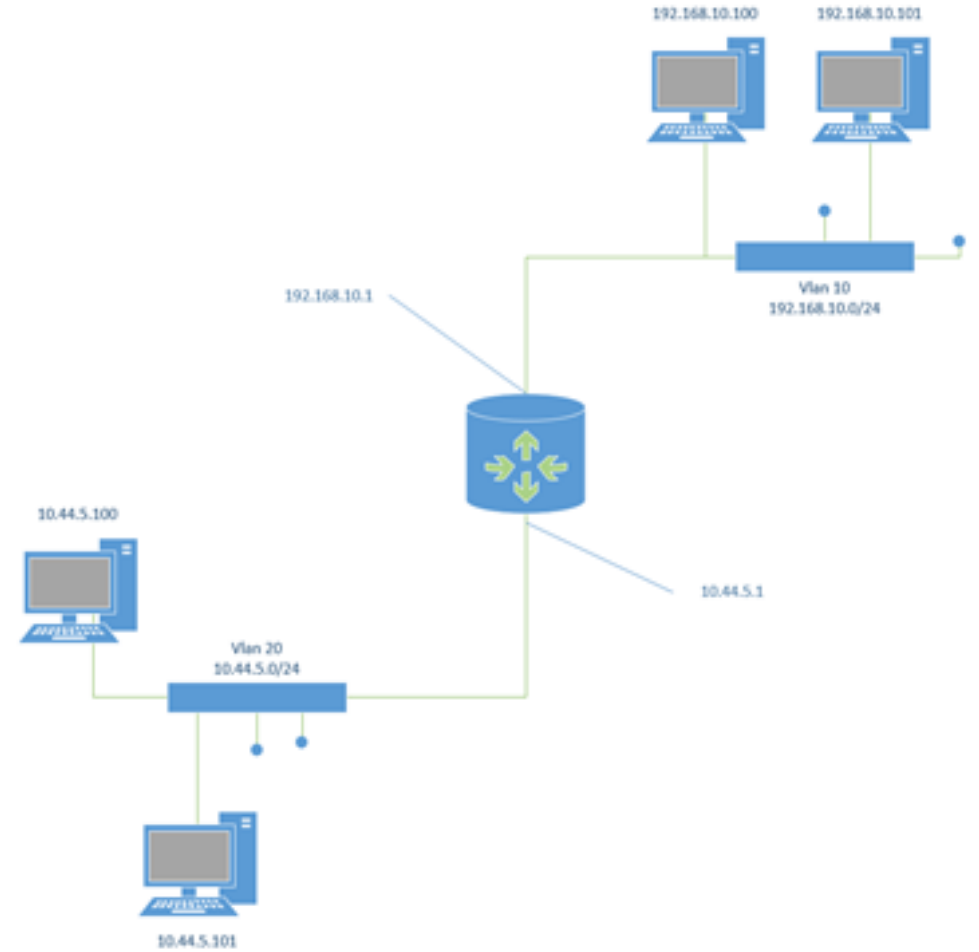
Extra diagrams…

Physical vs. Logical perspectives

- A **<u>physical</u>** network diagram shows the physical connections of network components.

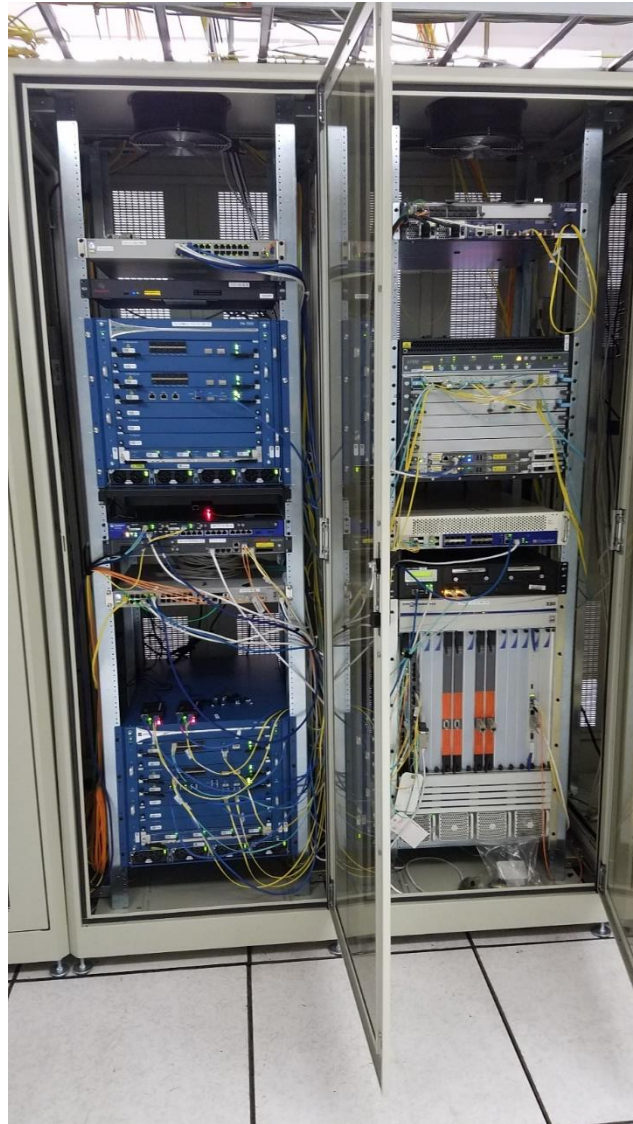- A **<u>logical</u>** diagram shows relationships and flow.

Switch Stacks

HQ-CORE-STACK-01
192.168.1.1

Stack

Gi1/0/1   Gi2/0/1

Po1

Po1

Gi0/1   Gi0/2

HQ-ACCESS-01
192.168.1.10

Switch

Physical Stencils

Generic Topology Icon

Physical Connectivity

Logical diagram version

192.168.10.100
vlan id 10

192.168.10.101
vlan id 10

PC-PT
PC1

PC-PT
PC0

fa0/1
vlan 10

fa0/2
vlan10

PC-PT
PC2

fa0/3
vlan20

2960-24TT
Switch

fa0/4
vlan20

PC-PT
PC3

10.44.5.101
vlan id 20

Gig 0/0
vlan 10

Gig0/1
vlan 20

10.44.5.100
vlan id 20

gig0/0
vlan 10

Gig0/1
vlan 20

2911
Router1

192.168.10.100   192.168.10.101

192.168.10.1

Vlan 10
192.168.10.0/24

10.44.5.100

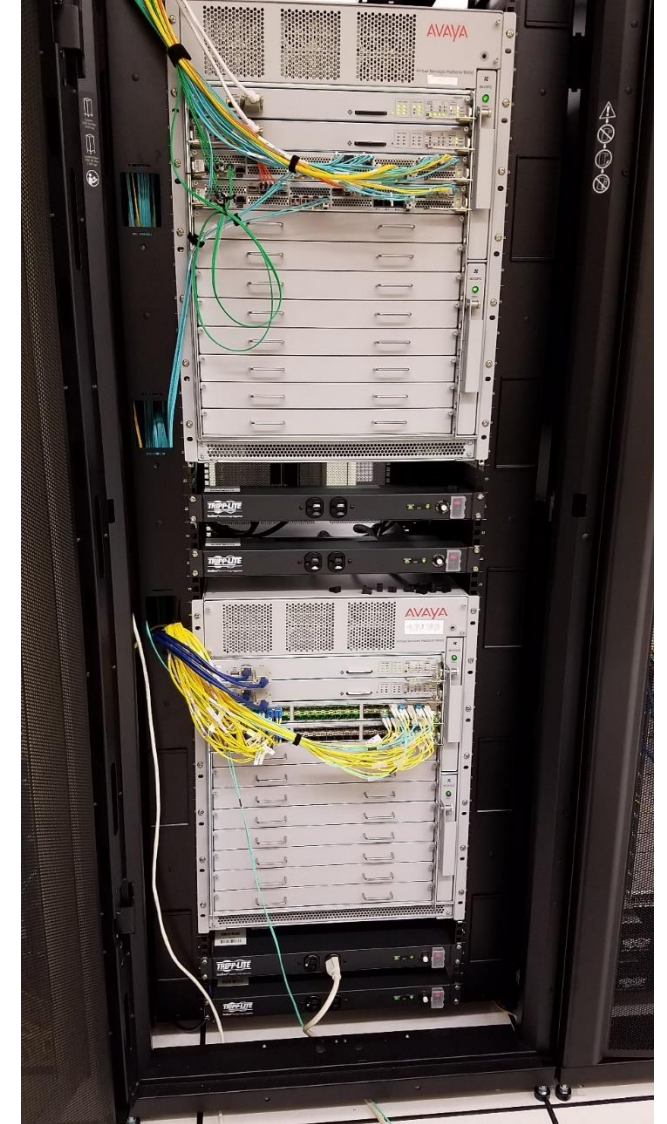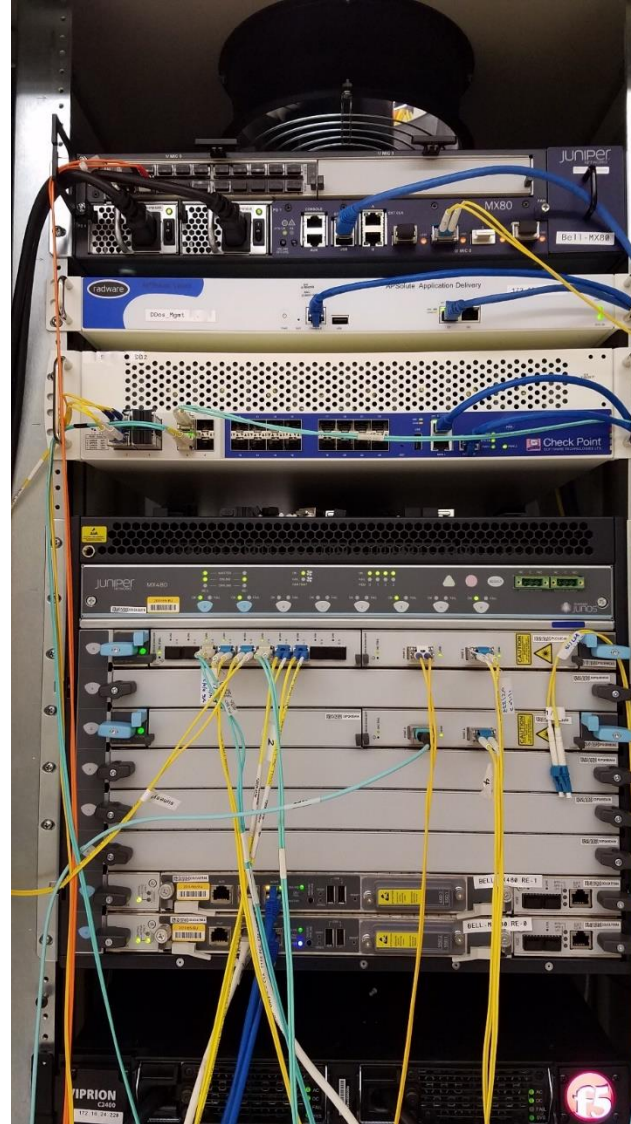10.44.5.1

Vlan 20
10.44.5.0/24
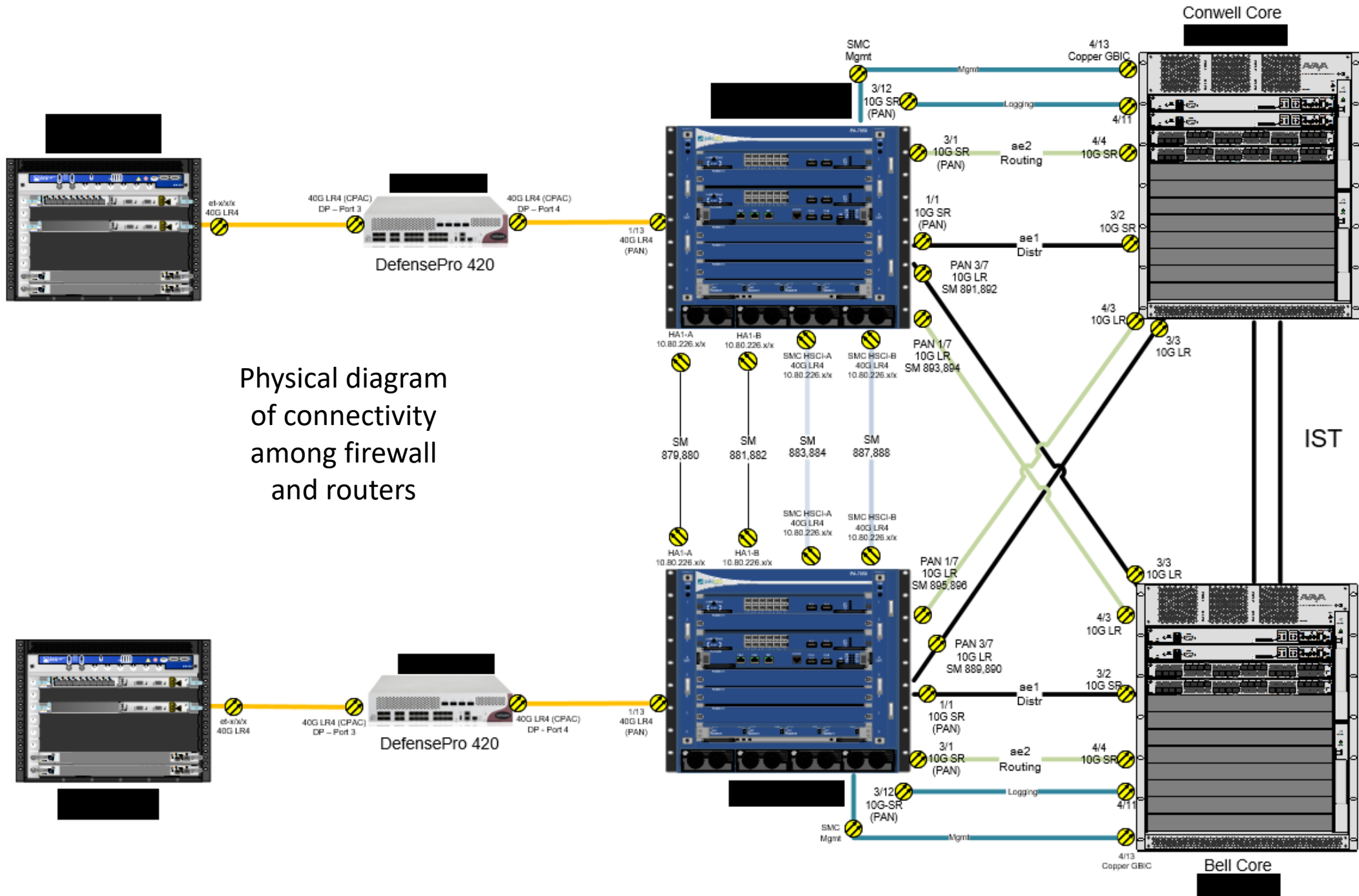
10.44.5.101

The Physical Hardware – Chassis Based

Firewalls

Routers

Physical diagram of connectivity among firewall and routers