Network Troubleshooting and Security

Valiant Voora
Center of Excellence in Digital Forensics
CoEDF

E.R. Ramesh, M.C.A., M.Sc., M.B.A.,

Unit - 1

Introduction

Seven layers in action
Troubleshooting Layer 3 Problems
Network security model
Classical Encryption techniques
(Symmetric cipher model, substitution techniques, transposition Techniques, steganography)
Topology
Cabling
Networking Industry Standards IEEE
Ethernet topology

Unit - 1

Introduction

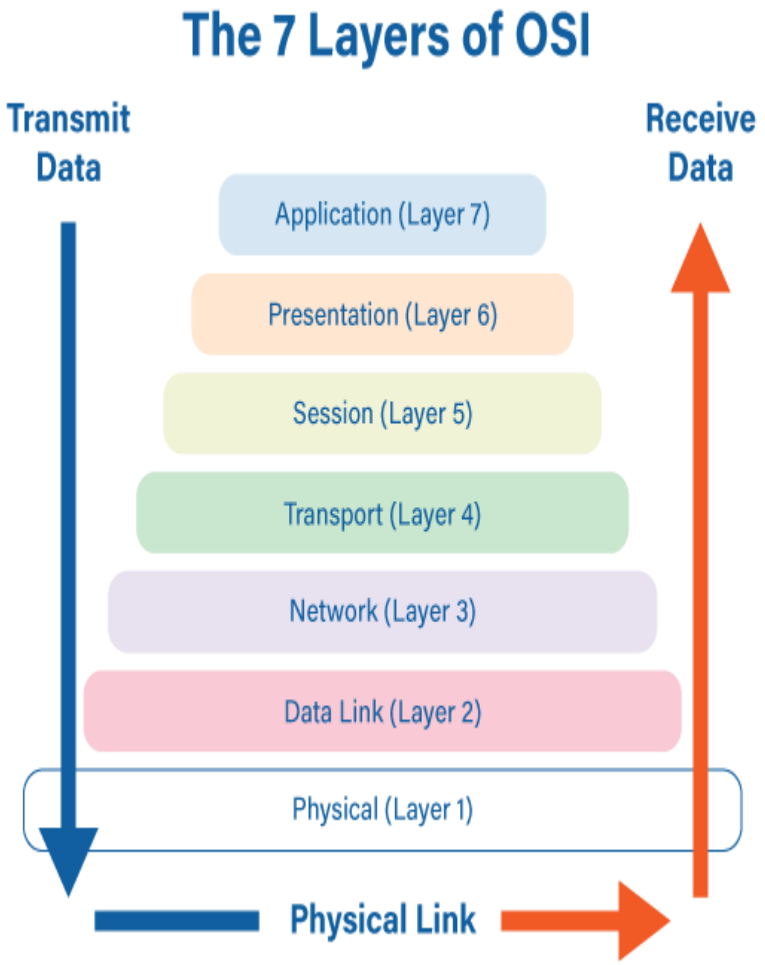
Troubleshooting Network Performance Issues
Baseline Network Performance
Collect Network Device Performance Metrics
Switch/Router CPU Utilization
Switch/Router Memory Utilization
Interface/Bandwidth Utilization.

Seven Layers in action

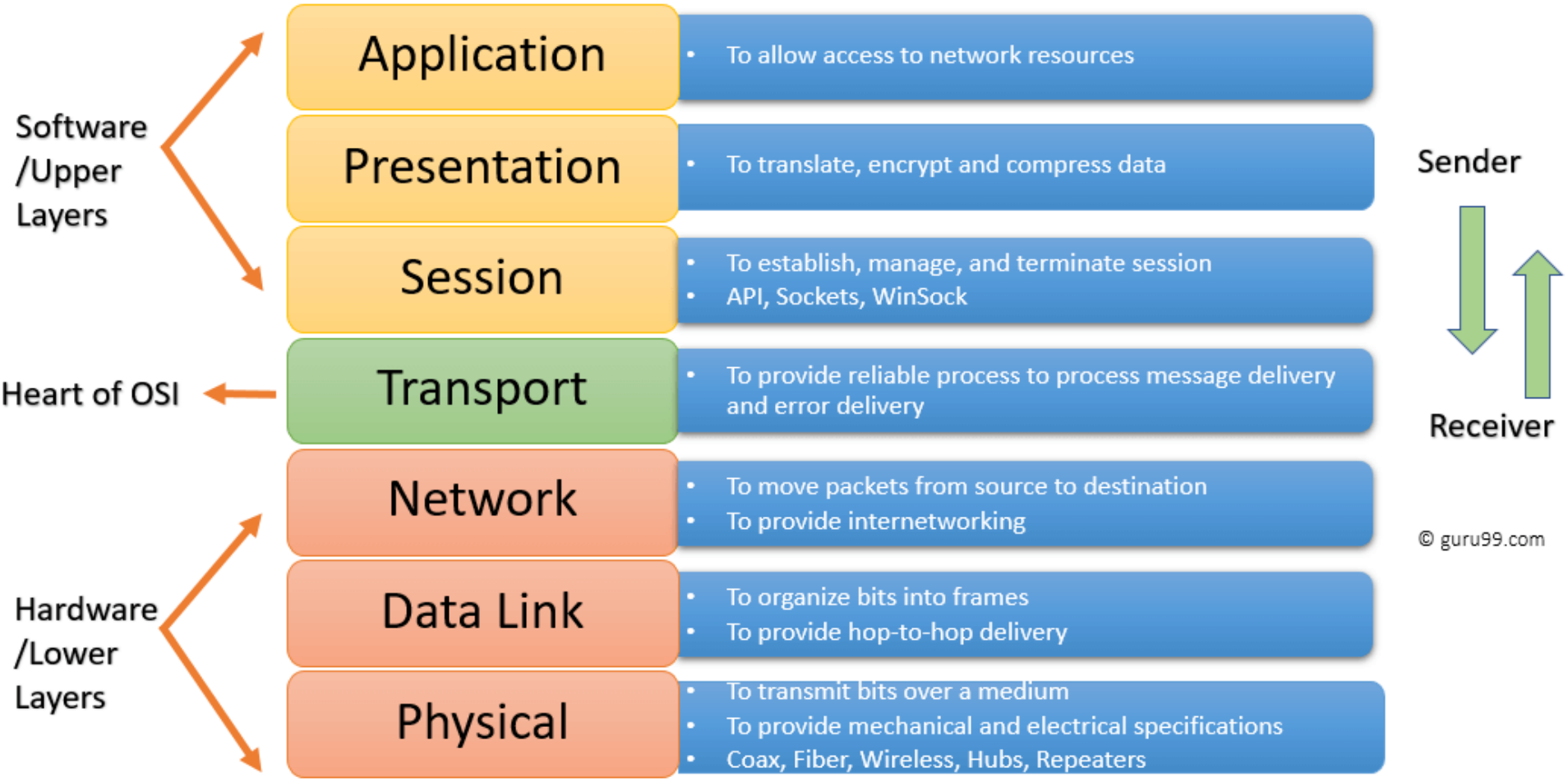
7 Layers of OSI Model

- The **OSI model is broken up into seven layers**. Each layer fulfills an important role within the networking stack and **communicates with other layers** by exchanging protocol data units (PDUs).

- The layers in the OSI model are commonly referred to by name or number (1-7). From lowest-level to highest-level they are:



Seven Layers in action



Seven Layers in action

#1. The Physical Layer

- The physical layer is where the raw bitstream is physically transmitted over a physical medium. The Layer 1 PDU is the “symbol”. This includes translating bits to electricity, light, or radio signals and controlling the rates at which they are sent over the chosen medium.

#2. The Data Link Layer

- The data link layer breaks data to be transmitted into frames for transmission at the physical layer. It also manages connections between two different nodes, including setting up the connection, identifying and correcting any bit errors that occur at the physical layer, and terminating the connection once the session is complete.

Seven Layers in action

#3. The Network Layer

- At the network layer, the focus expands from a point-to-point link to include many interconnected nodes within a network. Network-layer devices operate on packets and are responsible for routing traffic to its destination based on IP addresses.

#4. The Transport Layer

- The transport layer is the first of four “host” layers with the rest referred to as “media” layers. The transport layer PDU is the “segment” or “datagram”. This layer manages the transmission of data between nodes, including ensuring that data arrives in the correct sequence and that any errors are corrected. The Transmission Control Protocol (TCP) operates at Layer 4.

Seven Layers in action

#5. The Session Layer

- The session layer manages sessions between nodes and acts on the “data” PDU. Session management includes setup, authentication, termination, and reconnections.

#6. The Presentation Layer

- The presentation layer is primarily responsible for translating data from network data to the formats expected by an application. For example, data encodings and encryption are managed at Layer 6.

#7. The Application Layer

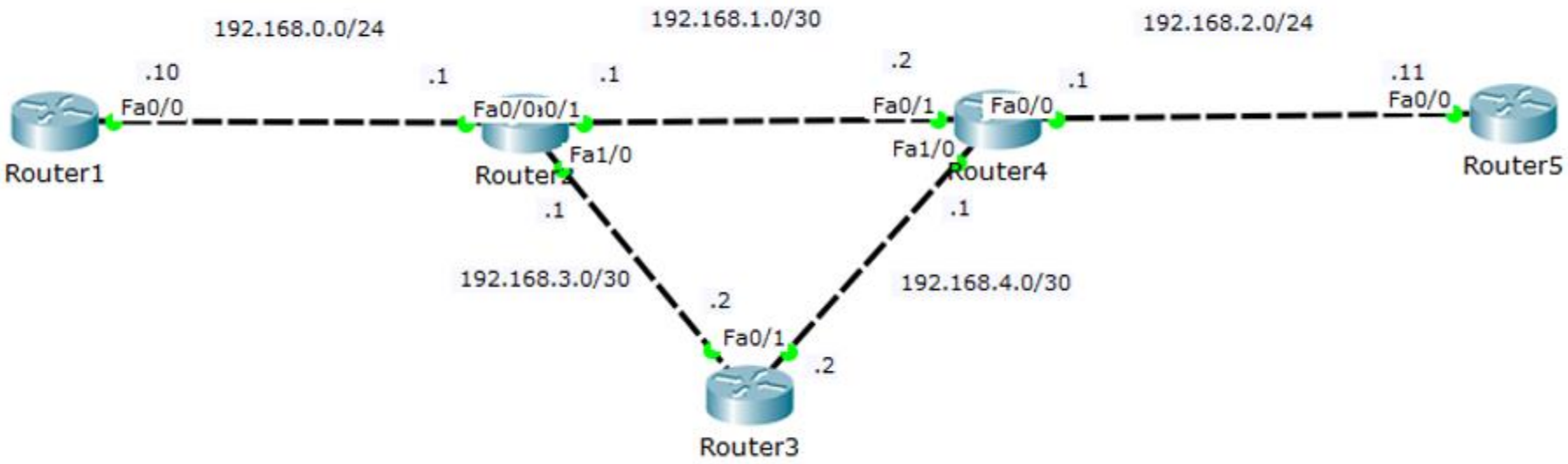
- The application layer includes protocols designed for end-users. For example, HTTP is a Layer 7 protocol designed to transmit data between a web server and a client.

Troubleshooting Layer 3 problems

Layer 3 network layer issues

- Physical and Data link layers are working properly
- Network connectivity issues
- Possibly cannot ping
- Incorrect IP or subnet mask settings
- No gateway configured
- Misconfigurations
- Connectivity issues
- Neighbor issues
- Topology database incorrect or incomplete
- Routing table incorrect or incomplete
- Commands use to troubleshoot layer 3 connectivity issues include ping, traceroute and show

Troubleshooting Layer 3 problems



Troubleshooting Layer 3 problems

Describe Troubleshooting Methodologies and Troubleshooting Tools

- There are three main methods for troubleshooting:
- Bottom-Up Troubleshooting Method

  In bottom-up troubleshooting you start with the physical components of the network and move up through the layers.

  Bottom-up troubleshooting is a good approach to use when the problem is suspected to be a physical one.

- Top-Down Troubleshooting Method

  In top-down troubleshooting your start with the end-user applications and move down the layers of the OSI model.

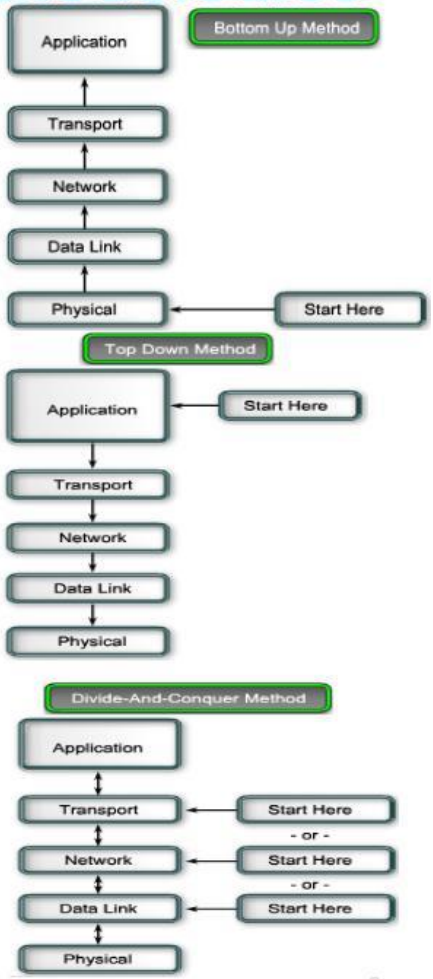
  Use this approach for simpler problems or when you think the problem is with a piece of software.

- Divide-and-Conquer Troubleshooting Method

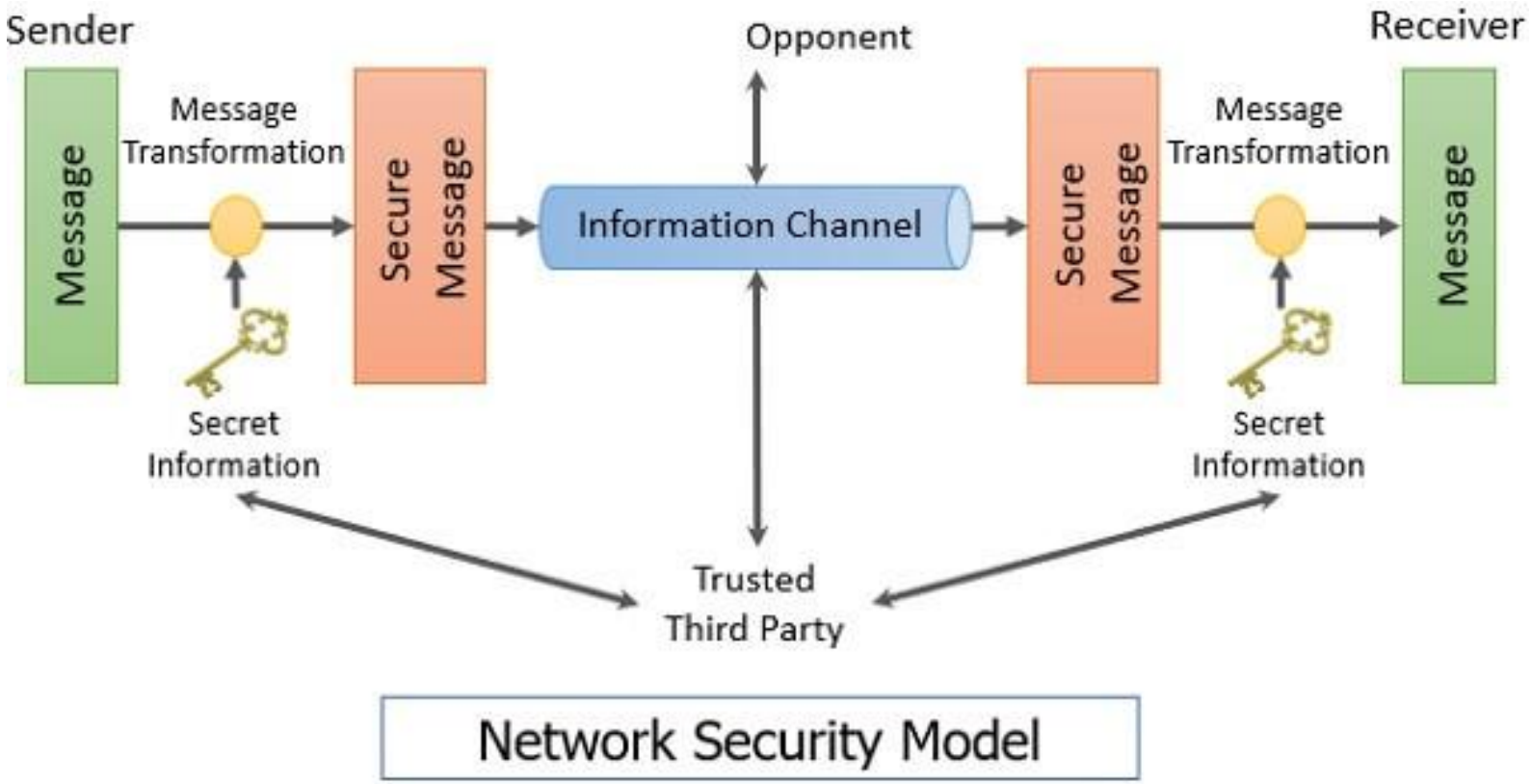
  In divide-and-conquer troubleshooting you start by collecting user experience of the problem, document the symptoms and then, using that information, make an informed guess as to which OSI layer to start your investigation.

  For example, if users can't access the web server and you can ping the server, then you know that the problem is above Layer 3.

  If you can't ping the server, then you know the problem is likely at a lower OSI layer.



Network Security Model



A Network Security Model exhibits how the security service has been designed over the network to prevent the opponent from causing a threat to the **confidentiality** or **authenticity** of the information that is being transmitted through the network.

Network Security Model

- For a message to be sent or receive there must be a sender and a receiver. Both the sender and receiver must also be mutually agreeing to the sharing of the message. Now, the transmission of a message from sender to receiver needs a medium i.e., **Information channel** which is an **Internet** service.

- A logical route is defined through the network (Internet), from sender to the receiver and using the **communication protocols** both the sender and the receiver established communication.

- Well, we are concerned about the security of the message over the network when the message has some confidential or authentic information which has a threat from an opponent present at the information channel. Any security service would have the **three components** discussed below:

Network Security Model

1. Transformation of the information which has to be sent to the receiver. So, that any opponent present at the information channel is unable to read the message. This indicates the **encryption** of the message.

It also includes the addition of code during the transformation of the information which will be used in verifying the identity of the authentic receiver.

2. Sharing of the **secret information** between sender and receiver of which the opponent must not any clue. Yes, we are talking of the **encryption key** which is used during the encryption of the message at the sender's end and also during the decryption of message at receiver's end.

3. There must be a **trusted third party** which should take the responsibility of **distributing the secret information** (key) to both the communicating parties and also prevent it from any opponent.

Network Security Model

- The network security model presents the two communicating parties **sender** and **receiver** who mutually agrees to exchange the information. The sender has information to share with the receiver.

- But sender cannot send the message on the information channel in the readable form as it will have a threat of being attacked by the opponent. So, before sending the message through the information channel, it should be **transformed** into an unreadable format.

- **Secret information** is used while transforming the message which will also be required when the message will be retransformed at the recipient side. That's why a trusted third party is required which would take the responsibility of distributing this secret information to both the parties involved in communication.

Network Security Model

So, considering this general model of network security, one must consider the following four tasks while designing the security model.

1. To **transform** a readable message at the sender side into an unreadable format, an appropriate algorithm should be designed such that it should be difficult for an opponent to crack that security algorithm.

2. Next, the network security model designer is concerned about the **generation of the secret information** which is known as a **key**. This secret information is used in conjunction with the security algorithm in order to transform the message.

3. Now, the secret information is required at both the ends, sender's end and receiver's end. At sender's end, it is used to encrypt or transform the message into unreadable form and at the receiver's end, it is used to decrypt or retransform the message into readable form.

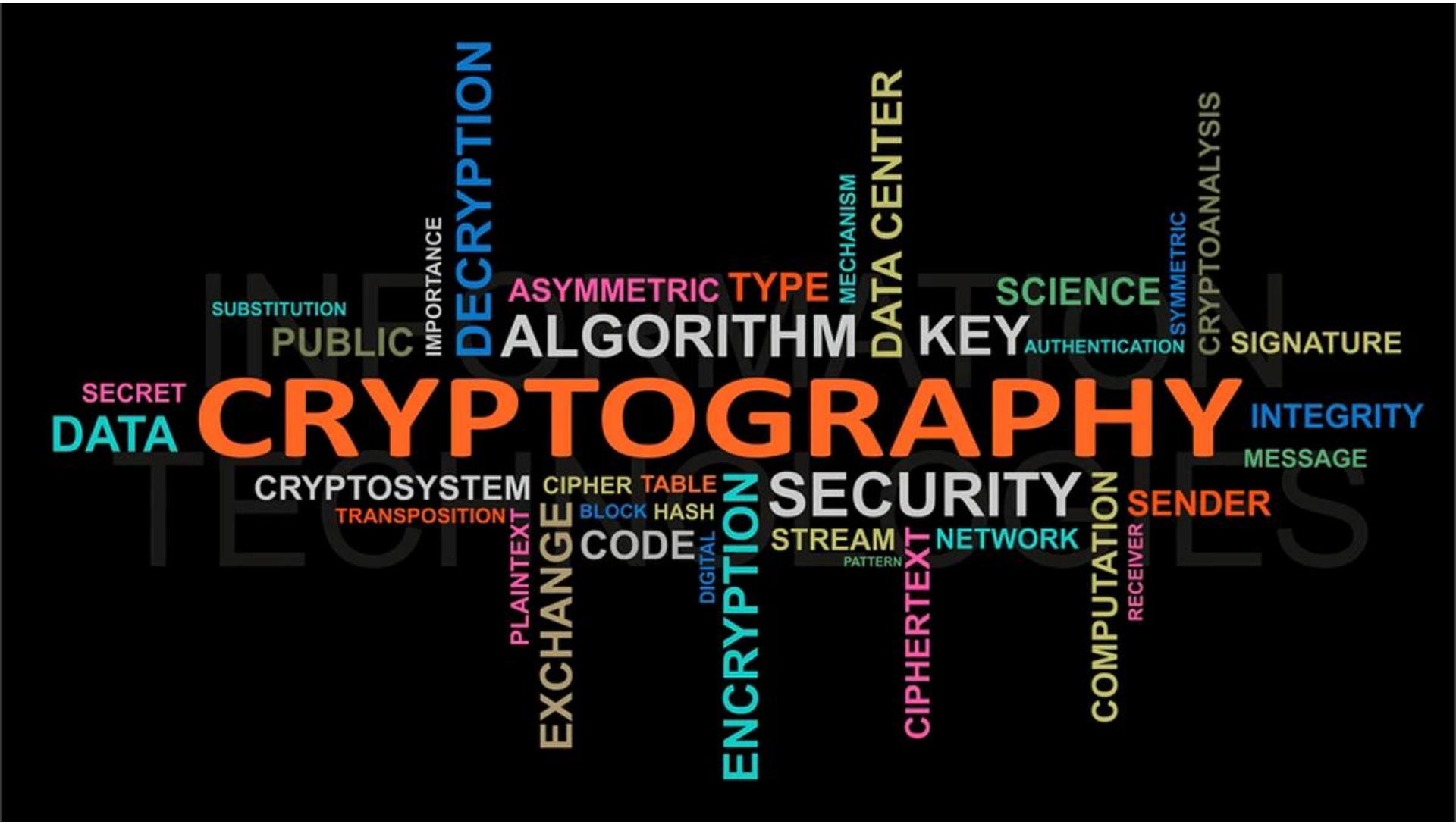
Network Security Model

- So, there must be a **trusted third party** which will distribute the secret information to both sender and receiver. While designing the network security model designer must also concentrate on **developing the methods** to distribute the key to the sender and receiver.

- An appropriate methodology must be used to deliver the secret information to the communicating parties without the interference of the opponent.

- It is also taken care that the **communication protocols** that are used by the communicating parties should be supporting the security algorithm and the secret key in order to achieve the security service.

Cryptography

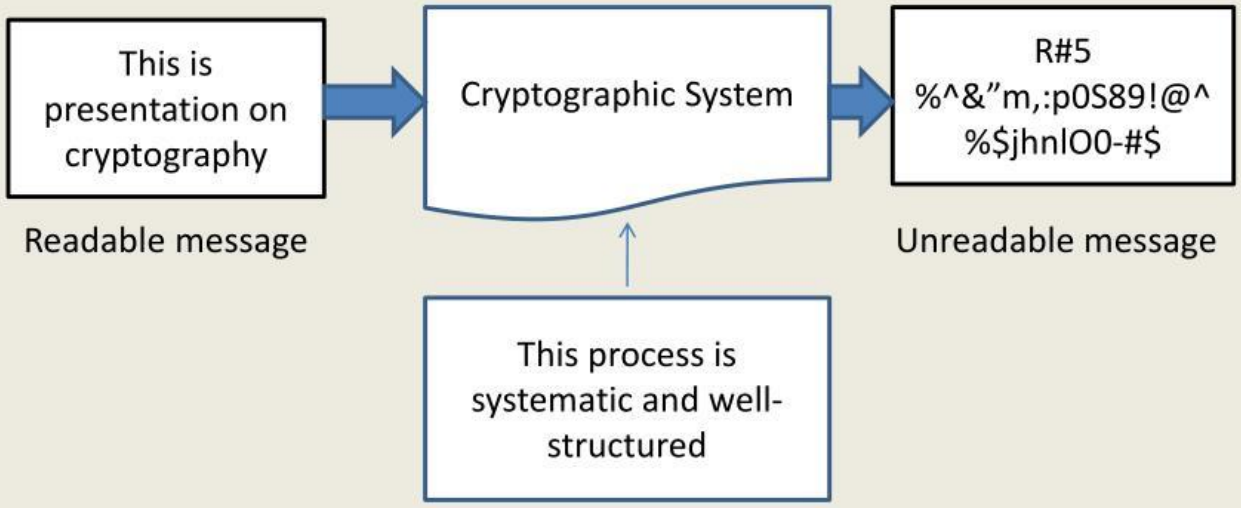


Cryptography

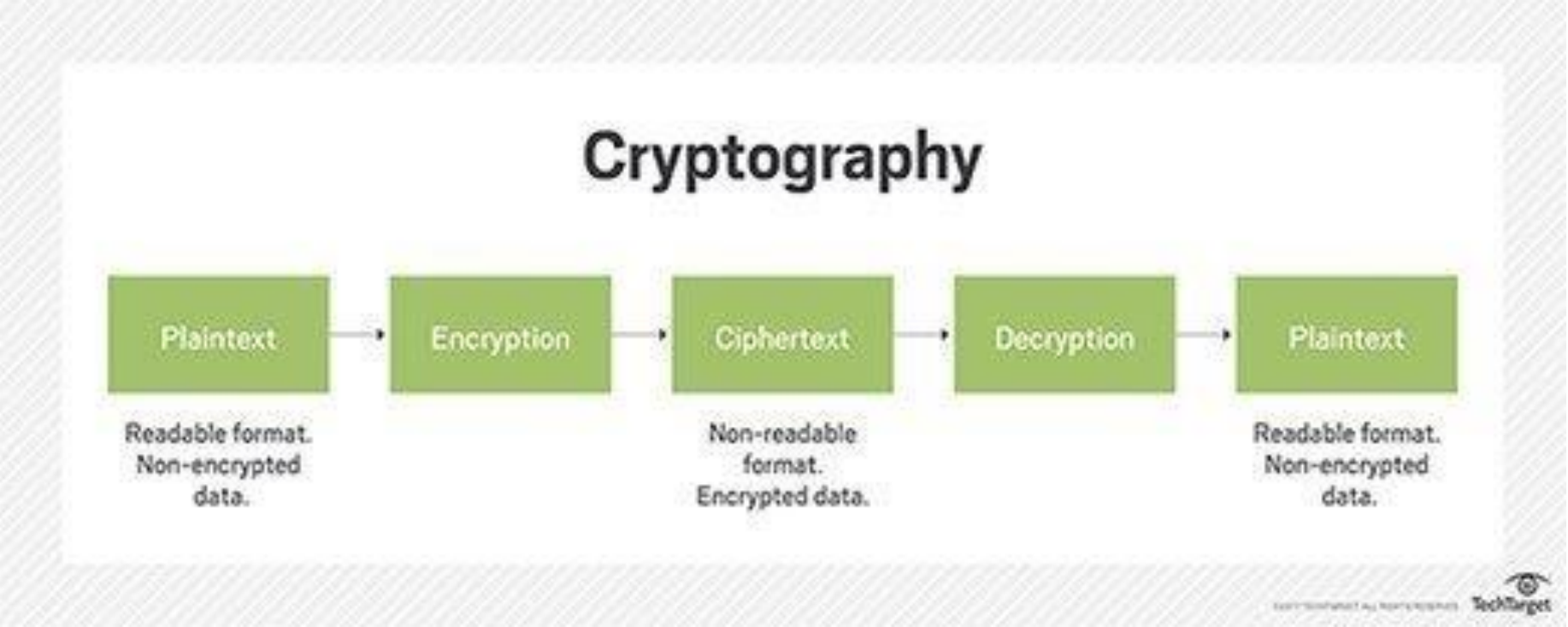
Cryptography

What is cryptography?

- **Definition :** Cryptography is the art and science of achieving security by encoding message to make them non-readable.



Cryptography



Terminologies

What is cryptology?

- Greek: “krypto” = hide
- Cryptology – science of hiding
  = cryptography + cryptanalysis + steganography
- Cryptography – secret writing
- Cryptanalysis – analyzing (breaking) secrets
  Cryptanalysis is what attacker does
  Decipher or *Decryption* is what legitimate receiver does

Terminologies

Cryptographic basics

- Cryptology is divided into cryptography and steganography.
- **Cryptography** means ciphering and deciphering text. The goal is not to hide that test is encrypted. It is only difficult to decrypt it.
- **Steganography** is a collection of techniques, which hide the text that should be kept secret (like hiding microfilms to a pin point, hiding text into images and so on). Steganography is not necessarily difficult to break, once you know where is the hidden text.
- It is possible to combine the two techniques and e.g. hide encrypted text into images using steganography.
- **Cryptoanalysis** is the art of decrypting cipher text without a key.

Terminologies

Cryptography

- **Cryptography**: art or science of keeping messages secret
- **Cryptology**: branch of mathematics that studies the mathematical foundations of cryptographic methods.
- **Plaintext P** = the original message.
- **Encryption E_k :** Encoding the contents of the message to hides its contents from outsiders.
- **Ciphertext C:** The encrypted message.
- **Decryption D_k :** The process of retrieving the plaintext from the ciphertext.
- **Key K:** Encryption and decryption usually make use of a **key**, and the coding method is such that decryption can be performed only by knowing the proper key.
- **Cryptosystem=** finite set of **plaintexts P +** finite set of **ciphertexts C +** set of **keys K+** set of **encryption** functions E_k and corresponding **decryption** functions D_k for each key **k** from **K,** such that $D_k[E_k(x)] = x$.
- **Cryptanalysis**: is the art of breaking ciphers without knowing the proper key.
- **Cryptographers:** People who do cryptography.
- **Cryptanalysts:** practitioners of cryptanalysis.

Terminologies

Question: What is cryptology?
Answer: Cryptology is the science of making information secure. It includes both cryptography, the discipline of communicating secretly through ciphers, and cryptanalysis, the practice of attempting to find weaknesses in a cipher.

Question: How does cryptology protect information?
Answer: Cryptology relies on encryption. Encryption uses algorithms or other processes called ciphers to make a plaintext message unrecognizable to humans. Ciphers work like a key, allowing messages to be encrypted or decrypted.

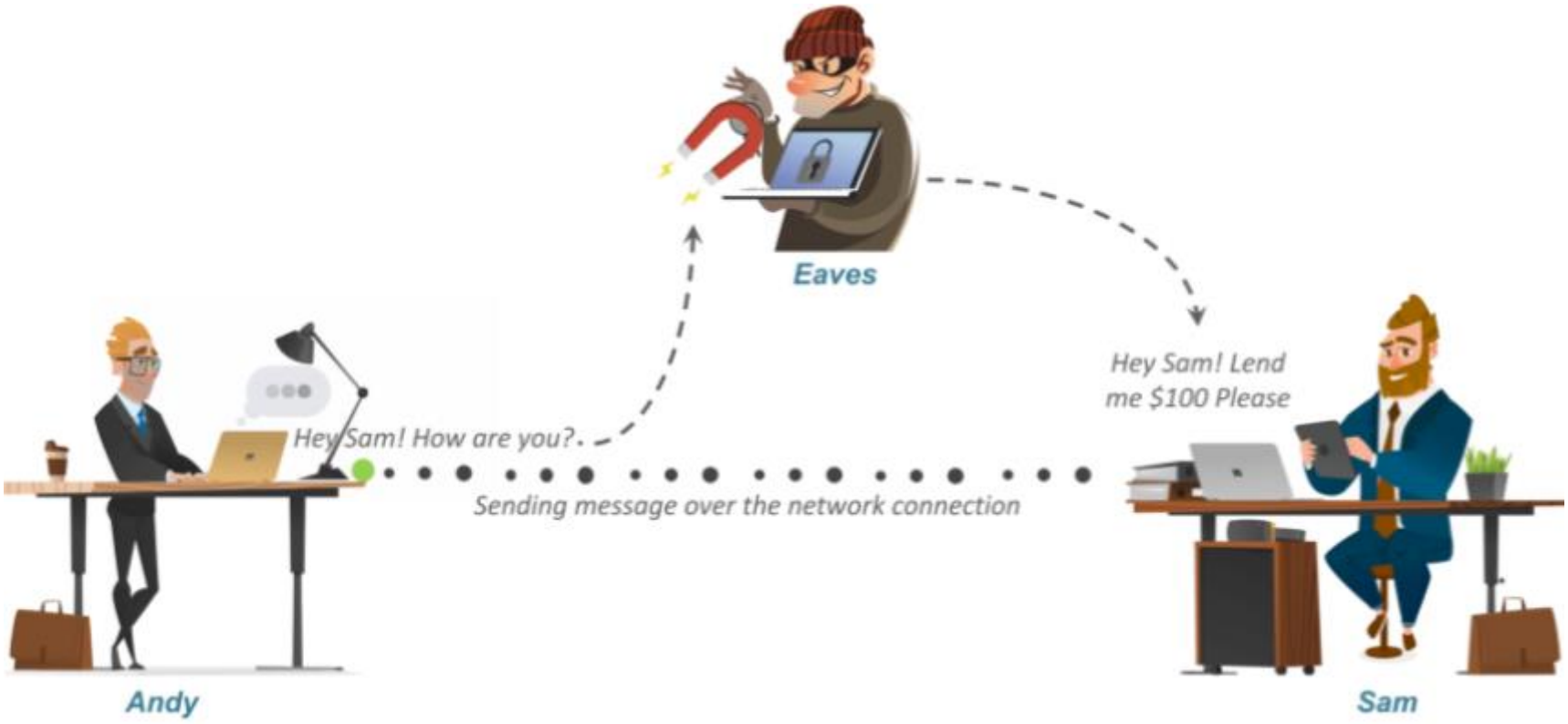
Introduction to Cryptography

- Cryptography is the science of keeping secrets secret. Assume a sender referred to here and in what follows as Alice (as is commonly used) wants to send a message m to a receiver referred to as Bob.

- She uses an insecure communication channel. For example, the channel could be a computer network or a telephone line.

- There is a problem if the message contains confidential information.

Introduction to Cryptography



- The message could be intercepted and read by an eavesdropper.

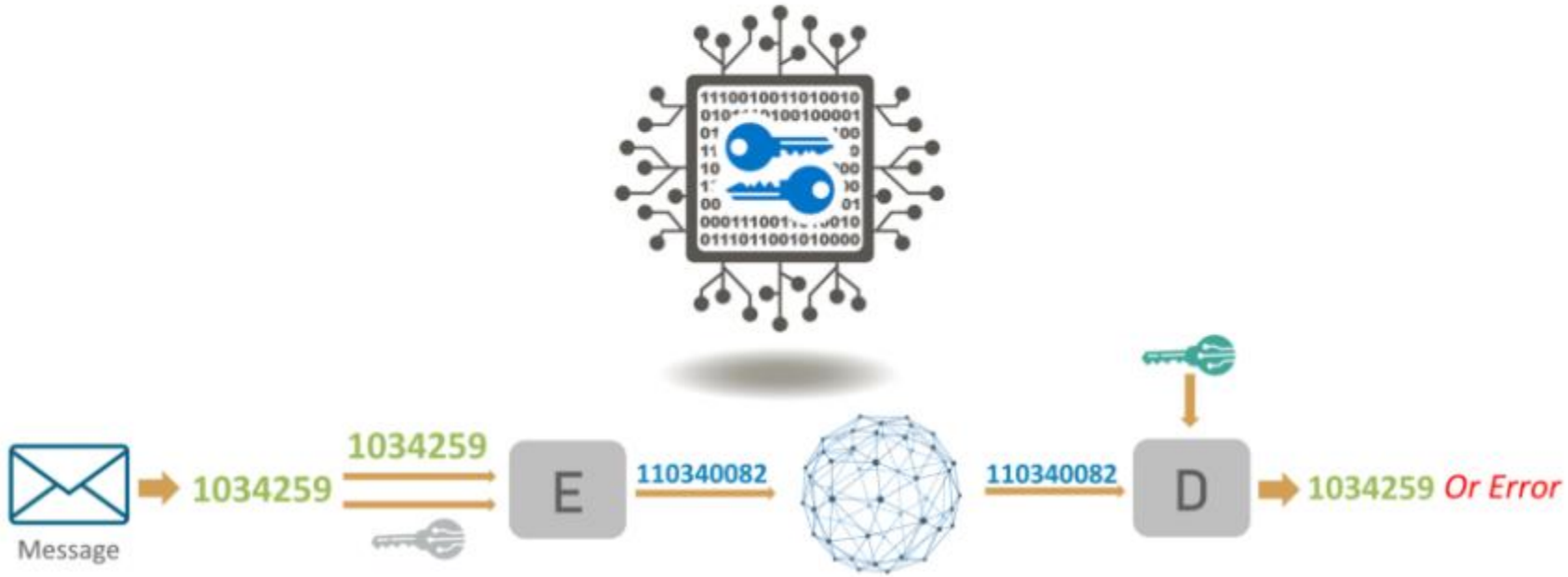
Introduction to Cryptography

- Or, even worse, the adversary, as usual referred to here as Eve, **might be able to modify the message during transmission** in such a way that the **legitimate recipient Bob does not detect the manipulation.**

Introduction to Cryptography

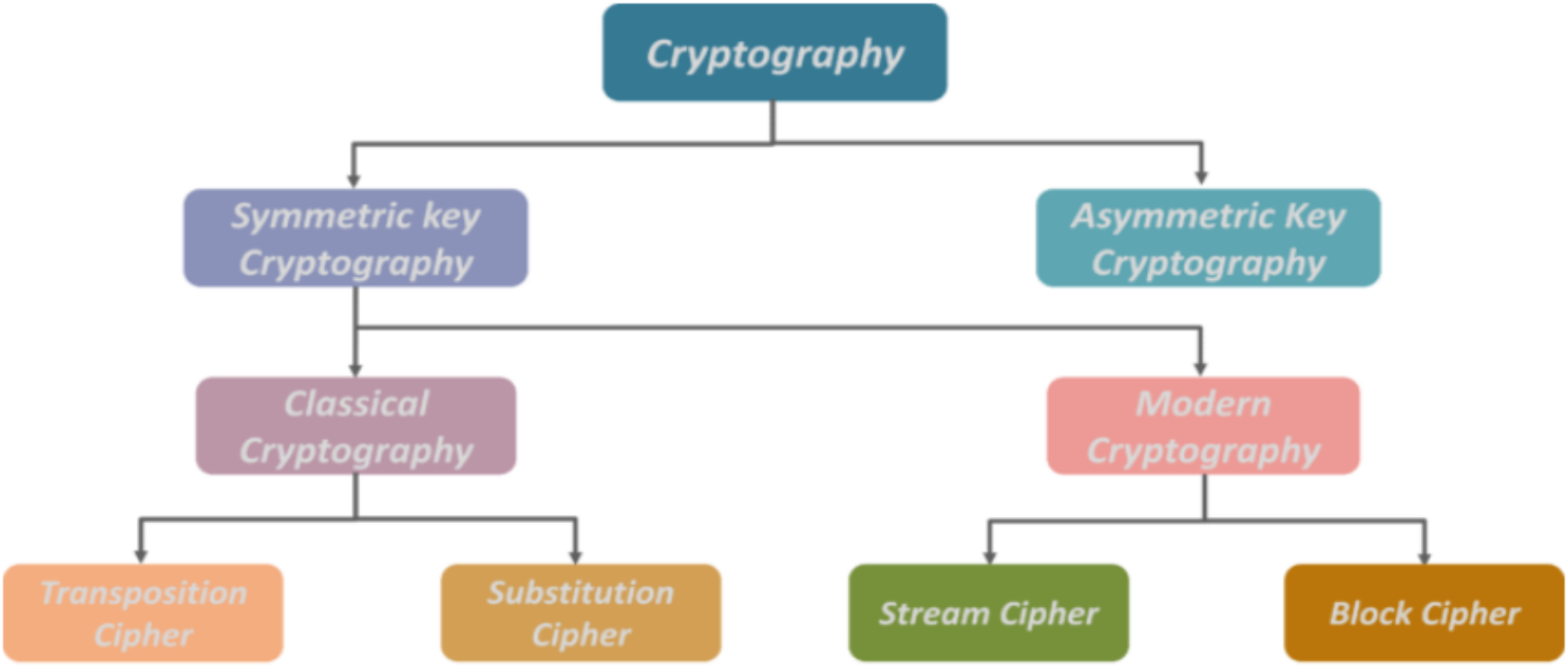
What Is Cryptography?

> *Cryptography is the practice and study of techniques for securing communication and data in the presence of adversaries.*



Encryption Algorithms

Cryptography is broadly classified into two categories: ***Symmetric key Cryptography*** and ***Asymmetric key Cryptography*** (popularly known as public key cryptography).

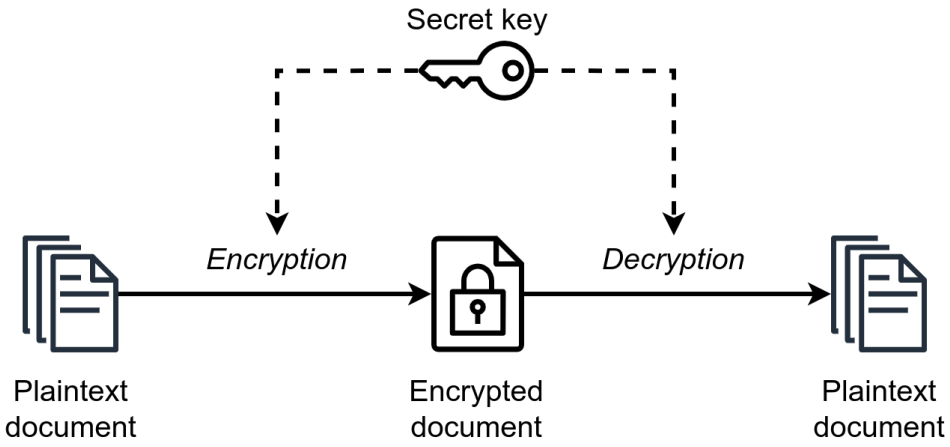


Symmetric cipher model

- **Symmetric-key algorithms** are algorithms for cryptography that use the **same cryptographic keys for both the encryption of plaintext and the decryption of ciphertext**. The keys may be **identical**, or there may be a simple transformation to go between the two keys.

- The keys, in practice, represent a **shared secret between two or more parties** that can be used to maintain a private information link. The requirement that **both parties have access to the secret key** is one of the main drawbacks of symmetric-key encryption, in comparison to public-key encryption (also known as asymmetric-key encryption).

Symmetric cipher model

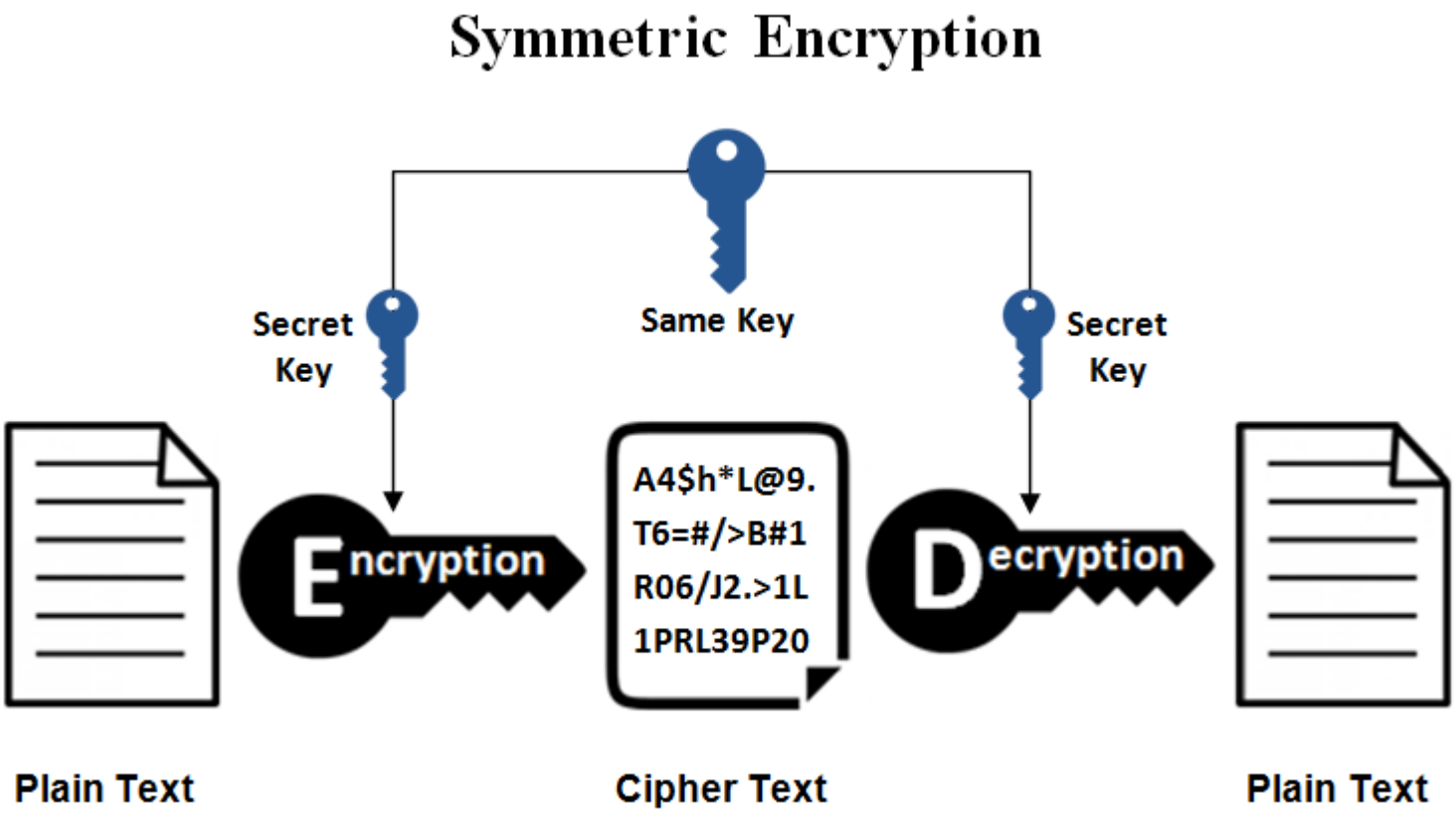


- However, **symmetric-key encryption algorithms are usually better for bulk encryption**. With exception of the one-time pad, they have a smaller key size, which means less storage space and faster transmission.

- Due to this, asymmetric-key encryption is often used to exchange the secret key for symmetric-key encryption.

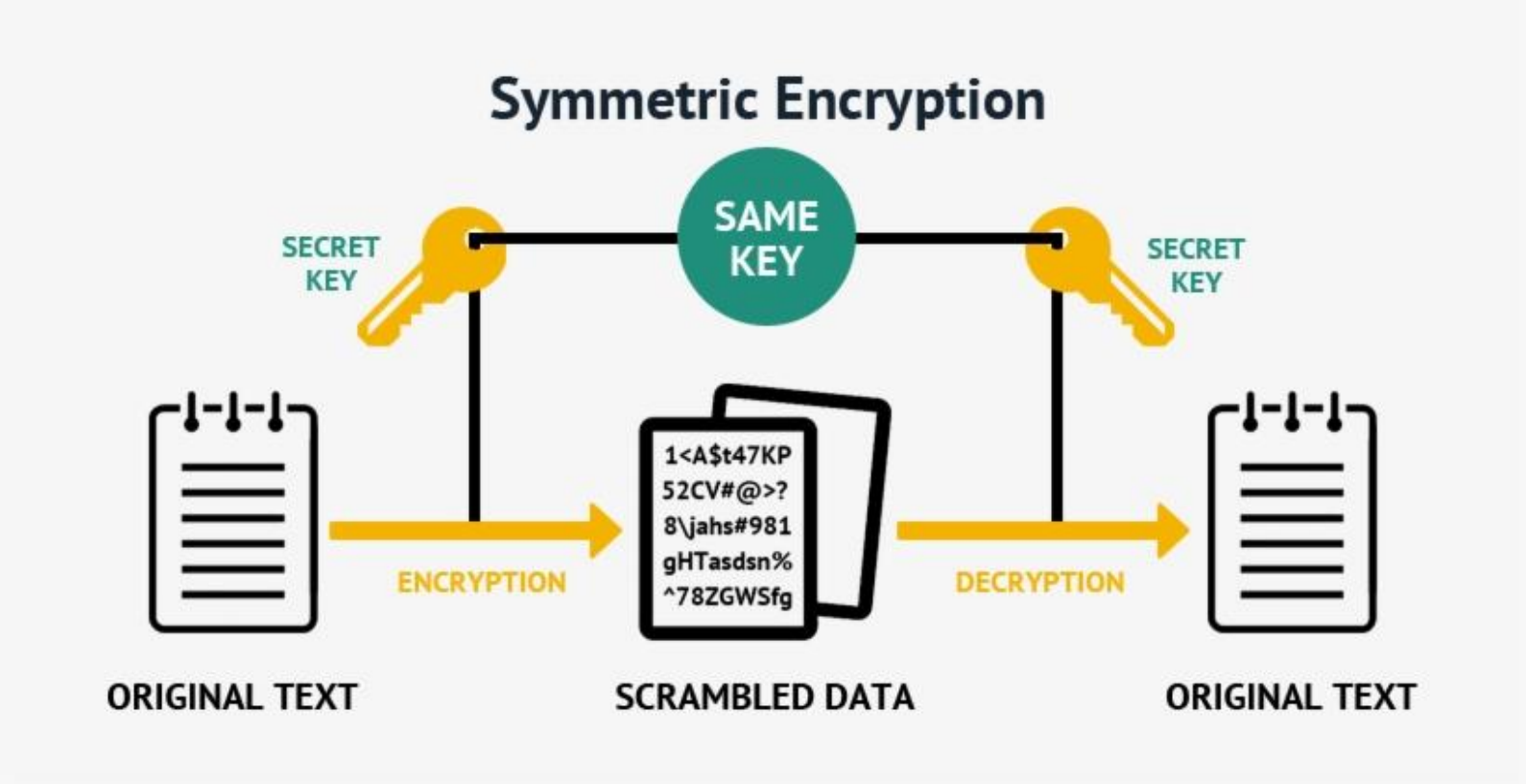
Symmetric-Key Cryptography

- Now Symmetric key Cryptography is further categorized as **Classical Cryptography** and **Modern Cryptography**.



Symmetric-Key Cryptography

- Further drilling down, **Classical Cryptography** is divided into **Transposition Cipher** and **Substitution Cipher**.



Discuss: Challenge?

Classical Cryptography

- In **cryptography**, a **transposition cipher** is a method of **encryption** by which the positions held by units of plaintext (which are **commonly characters** or **groups of characters**) are **shifted according to a regular system**, so that the **ciphertext** constitutes a permutation of the plaintext.

Transposition Cipher

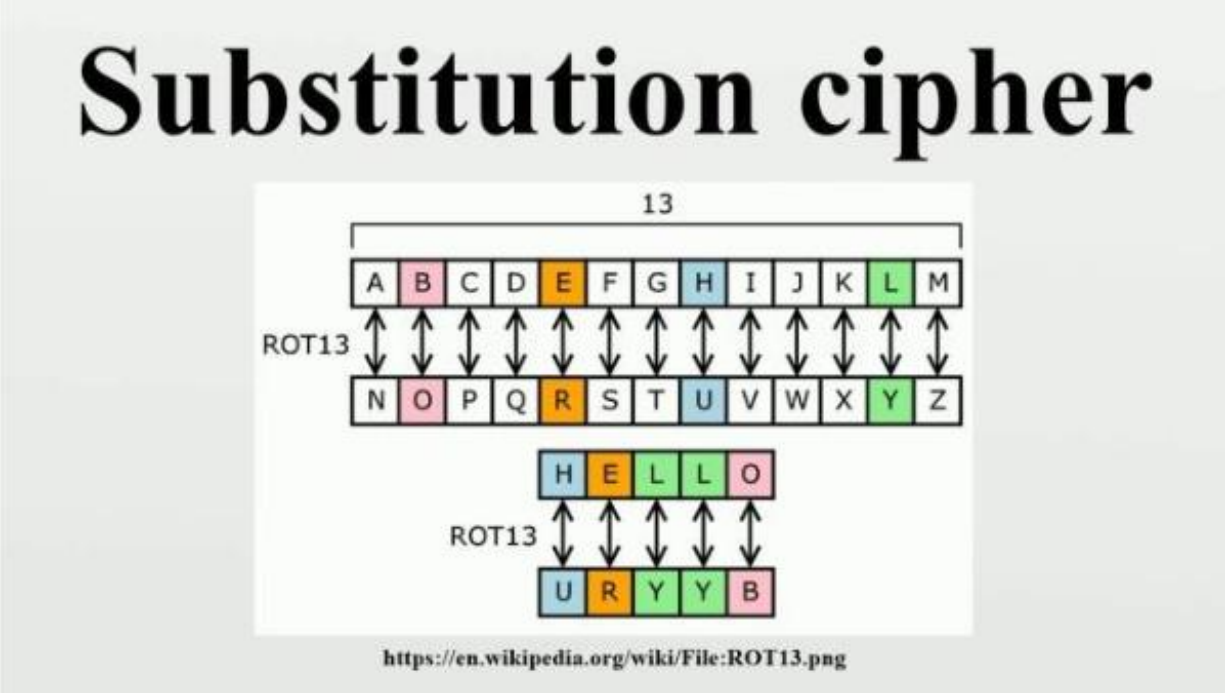
- Definition: A Transposition Cipher is a cipher in which the plaintext message is rearranged by some means agreed upon by the sender and receiver.
  - In transposition ciphers, no new alphabet is created. The letters of the plaintext are just rearranged in some fashion…

TABLE I. EXAMPLE OF TRANSPOSITION CIPHER

Plaintext	A	L	G	O	R	I	T	H	M	S
Position	1	2	3	4	5	1	2	3	4	5
Key	3	5	2	1	4	3	5	2	1	4
Ciphertext	G	R	L	A	O	H	S	T	I	M

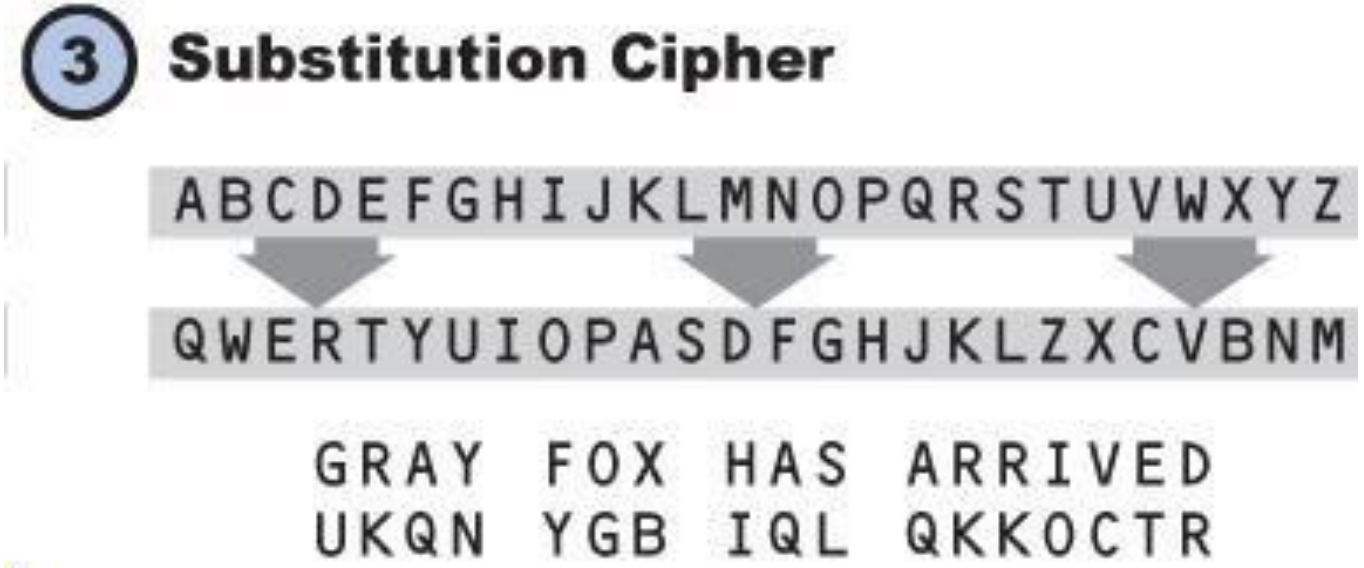
Substitution Cipher

- In **cryptography**, a **substitution cipher** is a method of encrypting in which units of plaintext are replaced with **ciphertext**, according to a fixed system; the "units" may be single letters (the most common), pairs of letters, triplets of letters, mixtures of the above, and so forth.



Substitution Cipher

- **Substitution ciphers** encrypt the plaintext by swapping each letter or symbol in the plaintext by a different symbol as directed by the key. Spaces in the **ciphertext** are just added for readability; they would be removed in a real application of the **cipher** to make attacking the **ciphertext** more difficult.



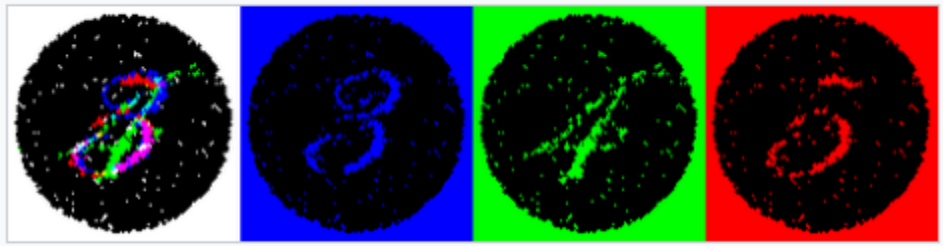
Steganography

- **Steganography** is the **practice of representing information within another message or physical object**, in such a manner that the **presence of the information is not evident to human inspection**.

- In computing/electronic contexts, a computer file, message, image, or video is concealed within another file, message, image, or video.

- The word *steganography* comes from Greek *steganographia*, which combines the words *steganós*, meaning "covered or concealed", and *-graphia* meaning "writing".

Steganography



The same image viewed by white, blue, green, and red lights reveals different hidden numbers.

- The **advantage of steganography over cryptography alone is that the intended secret message does not attract attention to itself as an object of scrutiny**. Plainly visible encrypted messages, no matter how unbreakable they are, arouse interest and may in themselves be incriminating in countries in which encryption is illegal.

Steganography

- Steganography includes the concealment of information within computer files. In digital steganography, electronic communications may include steganographic coding inside of a transport layer, such as a document file, image file, program, or protocol.

- Media files are ideal for steganographic transmission because of their large size. For example, a sender might start with an innocuous image file and adjust the color of every hundredth pixel to correspond to a letter in the alphabet.

- The change is so subtle that someone who is not specifically looking for it is unlikely to notice the change.

Topology

- **Network topology** is the arrangement of the various elements (links, nodes, etc.) of a computer network. Essentially, it is the topological structure of a network and may be depicted physically or logically.

- *Physical topology* is the placement of the various components of a network, including device location and cable installation, while *logical topology* illustrates how data flows within a network, regardless of its physical design.

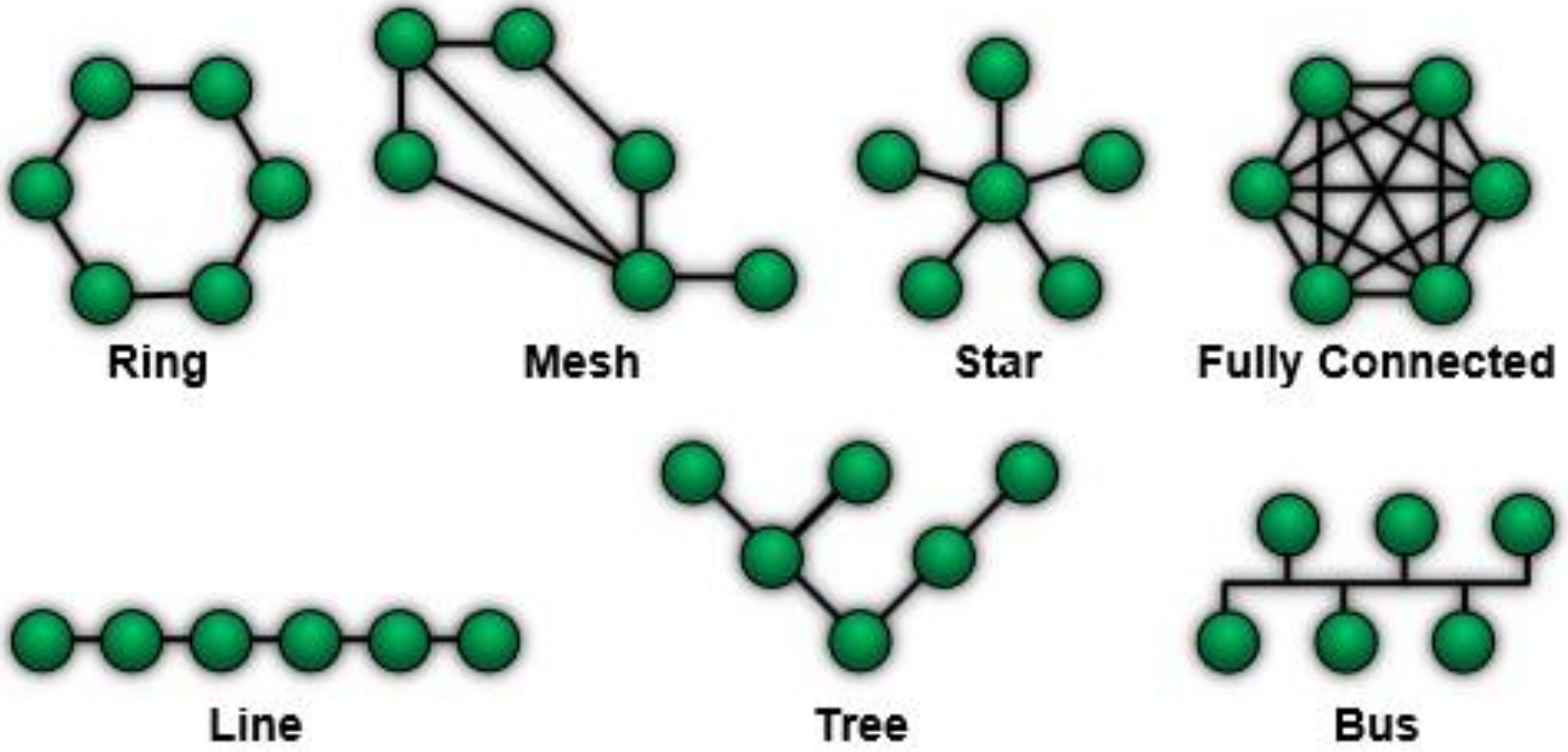
- Distances between nodes, physical interconnections, transmission rates, or signal types may differ between two networks, yet their topologies may be identical.

Topology

- An example is a local area network (LAN). Any given node in the LAN has one or more physical links to other devices in the network; graphically mapping these links results in a geometric shape that can be used to describe the physical topology of the network.

- Conversely, mapping the data flow between the components determines the logical topology of the network.

Topology



Cabling

- **Networking cable** is a piece of networking hardware used to connect one network device to other network devices or to connect two or more computers to share devices such as printers or scanners.

- Different types of network cables, such as coaxial cable, optical fiber cable, and twisted pair cables, are used depending on the network's topology, protocol, and size.

- The devices can be separated by a few meters (e.g., via Ethernet) or nearly unlimited distances (e.g., via the interconnections of the Internet).

Cabling

- There are several technologies used for network connections. Patch cables are used for short distances in offices and wiring closets.

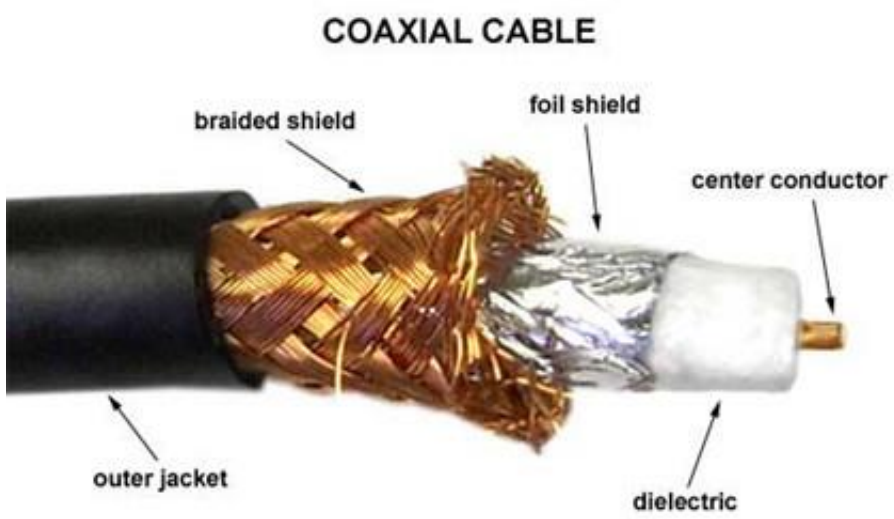
- Electrical connections using twisted pair or coaxial cable are used within a building. Optical fiber cable is used for long distances or for applications requiring high bandwidth or electrical isolation.

- Many installations use structured cabling practices to improve reliability and maintainability. In some home and industrial applications power lines are used as network cabling.

Wired technologies

- The orders of the following wired technologies are, roughly, from slowest to fastest transmission speed.

Coaxial cable is widely used for cable television systems, office buildings, and other work-sites for local area networks. The cables consist of copper or aluminum wire surrounded by an insulating layer (typically a flexible material with a high dielectric constant), which itself is surrounded by a conductive layer.



Wired technologies

- The insulation helps minimize interference and distortion. Transmission speed ranges from 200 million bits per second to more than 500 million bits per second.

- ITU-T G.hn technology uses existing home wiring (coaxial cable, phone lines and power lines) to create a high-speed (up to 1 Gigabit/s) local area network.

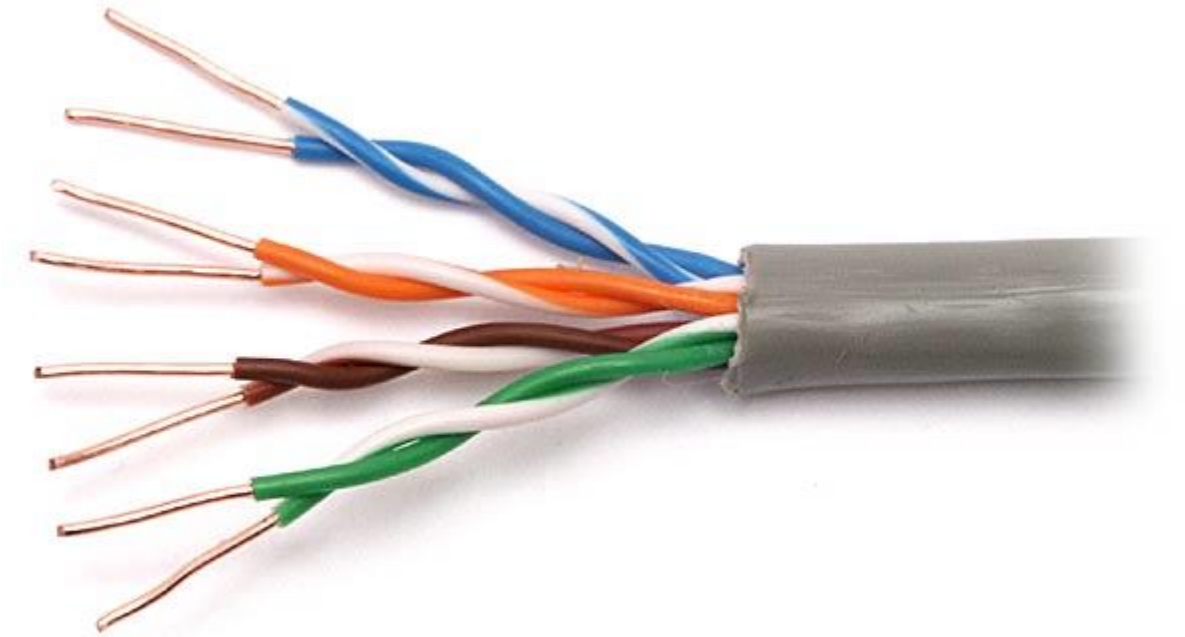
Wired technologies

- *Twisted pair wire* is the most widely used medium for all telecommunication. Twisted-pair cabling consist of copper wires that are twisted into pairs. Ordinary telephone wires consist of two insulated copper wires twisted into pairs.

- Computer network cabling (wired Ethernet as defined by IEEE 802.3) consists of 4 pairs of copper cabling that can be utilized for both voice and data transmission.

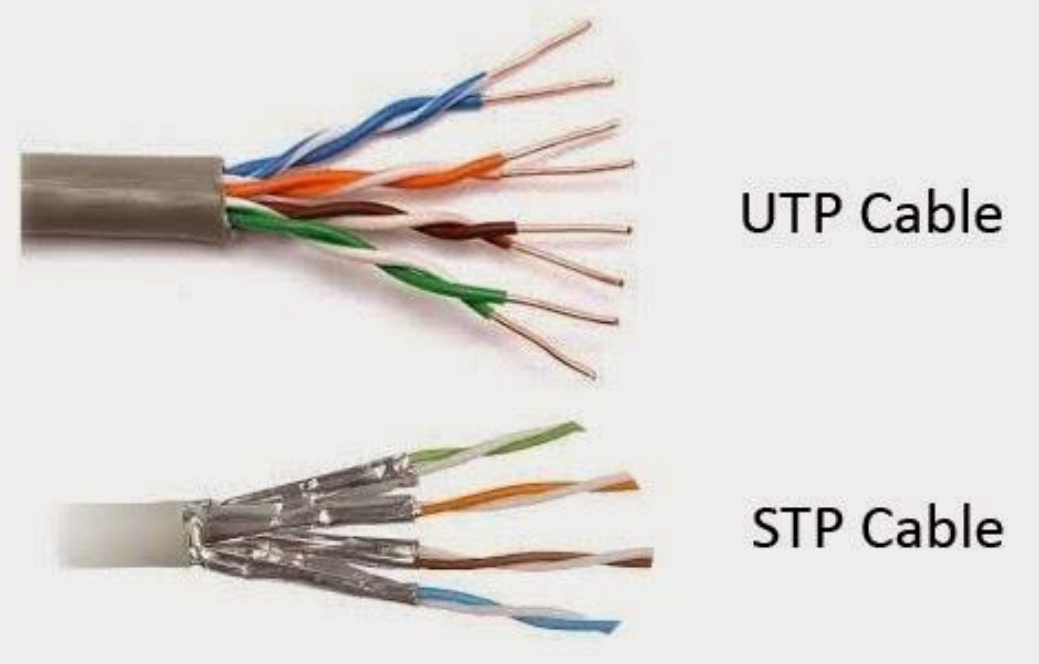
Wired technologies

- The use of two wires twisted together helps to reduce crosstalk and electromagnetic induction. The transmission speed ranges from 2 million bits per second to 10 billion bits per second.



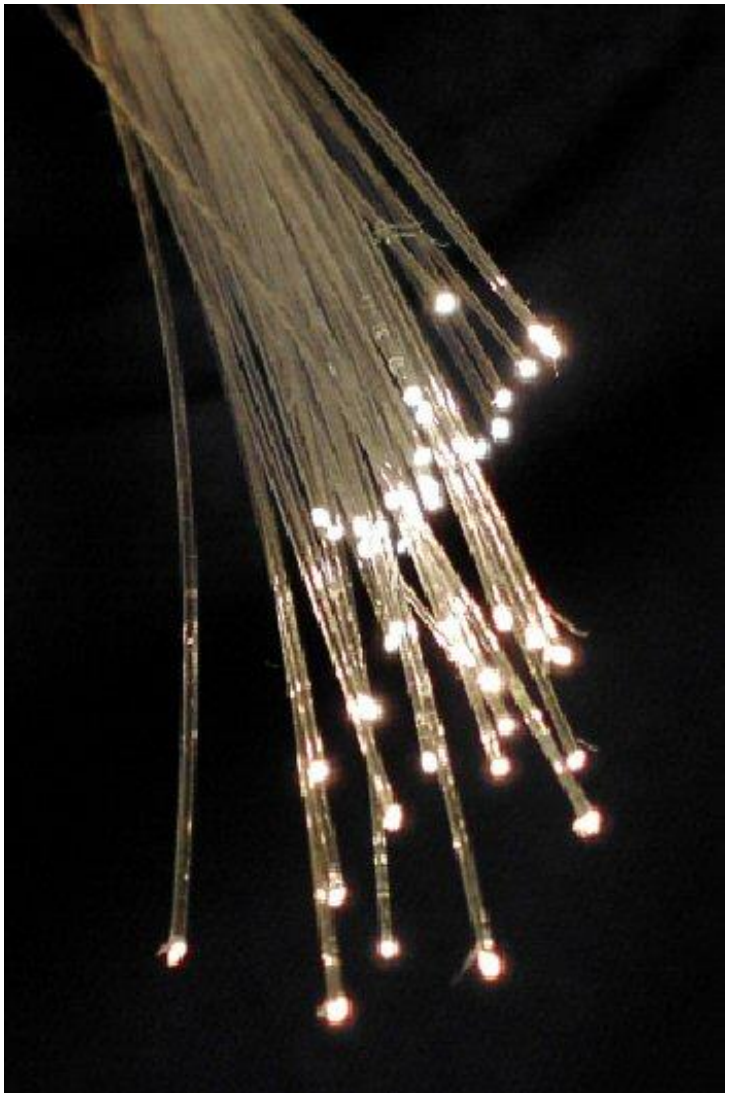
Wired technologies

- Twisted pair cabling comes in two forms: unshielded twisted pair (UTP) and shielded twisted-pair (STP). Each form comes in several category ratings, designed for use in various scenarios.



Wired technologies

- An ***optical fiber*** is a glass fiber. It carries pulses of light that represent data. Some advantages of optical fibers over metal wires are very low transmission loss and immunity from electrical interference.



Wired technologies

- Optical fibers can simultaneously carry multiple wavelengths of light, which greatly increases the rate that data can be sent, and helps enable data rates of up to trillions of bits per second.

- Optic fibers can be used for long runs of cable carrying very high data rates, and are used for undersea cables to interconnect continents.

Wired technologies

- Price is a main factor distinguishing wired- and wireless-technology options in a business. Wireless options command a price premium that can make purchasing wired computers, printers and other devices a financial benefit.

- Before making the decision to purchase hard-wired technology products, a review of the restrictions and limitations of the selections is necessary. Business and employee needs may override any cost considerations.

Networking Industry Standards IEEE

- IEEE stands for Institute of Electrical and Electronics Engineers. The main AIM of IEEE is to foster technological innovation and excellence for the benefit of humanity.

- The IEEE standards in computer networks ensure communication between various devices; it also helps to make sure that the network service, i.e., the Internet and its related technologies, must follow a set of guidelines and practices so that all the networking devices can communicate and work smoothly.

Networking Industry Standards IEEE

- Since there are various types of computer system manufacturers, the IEEE's Computer Society started a project in 1985 called project 802 to enable standard communication between various devices.

- The standards that deal with computer networking are called the IEEE 802 wireless standards.

Networking Industry Standards IEEE

1. **IEEE 802**: The IEEE 802 deals with the standards of LAN and MAN, i.e., Local Area Network and Metropolitan Area Network.
2. **IEEE 802.1**: The IEEE 802.1 deals with the standards of LAN and MAN. Along with that, it also deals with the MAC (Media Access Control) bridging.
3. **IEEE 802.2**: The IEEE 802.2 deals with the LLC (Logical Link Control).

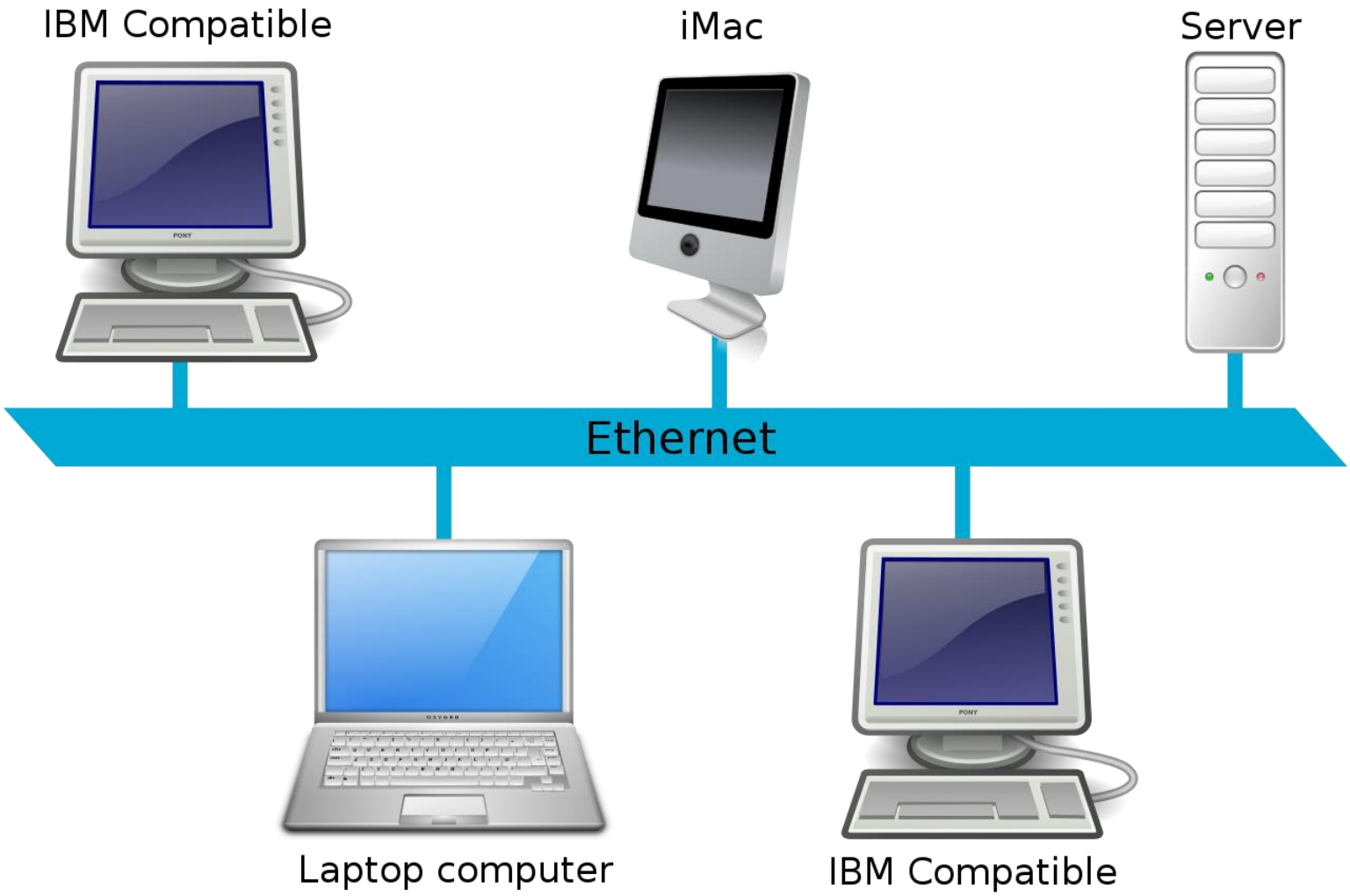
Networking Industry Standards IEEE

IEEE 802.3	It is used in Ethernet (CSMA/CD access method).
IEEE 802.3ae	It is used for 10 Gigabit Ethernet.
IEEE 802.4	It is used for token passing bus access methods and the physical layer specifications.
IEEE 802.5	It is used for token ring access methods and the physical layer specifications.

Networking Industry Standards IEEE

IEEE 802.7	It is used in broadband LAN.
IEEE 802.8	It is used in fiber optics.
IEEE 802.9	It is used in isochronous LANs.
IEEE 802.10	It is used in interoperable LAN/MAN security.
IEEE 802.11	It is used in wireless LAN, MAC, and Physical layer specifications.
IEEE 802.12	It is used in the demand-priority access method, in the physical layer, and in repeater specifications.

Ethernet topology



Ethernet topology

- A **local area network** (**LAN**) is a computer network that interconnects computers within a limited area such as a residence, school, laboratory, university campus or office building.

- **Ethernet** and Wi-Fi are the two **most common technologies** in use for local area networks. Historical network technologies include ARCNET, Token Ring and AppleTalk.

- Ethernet generally uses a **bus topology**. Ethernet operates in two layers of the OSI model, the physical layer and the data link layer. For Ethernet, the protocol data unit is a frame since we mainly deal with DLLs.

- In order to handle collisions, the Access control mechanism used in Ethernet is **CSMA/CD**.

Ethernet topology

- A **bus network** is a network topology in which nodes are directly connected to a common **half-duplex** link called a bus.

- A host on a bus network is called a *station*. In a bus network, every station will receive all network traffic, and the traffic generated by each station has equal transmission priority.

- A bus network forms a single network segment and collision domain. In order for nodes to share the bus, they use a medium access control technology such as carrier-sense multiple access (CSMA) or a bus master.

Troubleshooting Network Performance Issues

What Is Troubleshooting a Network?

- The **term troubleshooting refers to the process of identifying problems with a network** through a **rigorous and repeatable process and then solving those problems using testable methods**.

- Troubleshooting is more effective than trying things at random until the network functions because it **allows you to target individual network components**, **testing each for function**, and encourages you to document your process.

Troubleshooting Network Performance Issues

Basic Network Troubleshooting Steps

- Network troubleshooting is a repeatable process, which means that you can break it down into clear steps that anyone can follow.

1. **Identify the Problem**

- The first step in troubleshooting a network is to identify the problem. As a part of this step, you should do the following:
- **Gather information** about the current state of the network using the network troubleshooting tools that you have available to you.

Troubleshooting Network Performance Issues

- **Duplicate the problem** on a test piece of hardware or software, if possible. This can help you to confirm where your problem lies.

- **Question users** on the network to learn about the errors or difficulties they have encountered.

- **Identify the symptoms** of the network outage. For example, do they include complete loss of network connection? Slow behavior on the network? Is there a network-wide problem, or are the issues only being experienced by one user?

Troubleshooting Network Performance Issues

- **Determine if anything has changed** in the network before the issues appeared. Is there a new piece of hardware that's in use? Has the network taken on new users? Has there been a software update or change somewhere in the network?

- **Define individual problems clearly**. Sometimes a network can have multiple problems. This is the time to identify each individual issue so that your solutions to one aren't bogged down by other unsolved problems.

Troubleshooting Network Performance Issues

2. **Develop a Theory**

- Once you have finished gathering all the information that you can about the network issue or issues, it's time to develop a working theory. While you're producing your theory about the causes of the network issue, don't be afraid to question the obvious, but remain on the lookout for more serious issues.

- Sometimes a network outage occurs because someone tripped on a wire or some other simple problem. However, at other times the problems might be related more complicated causes, like a breach in network security.

Troubleshooting Network Performance Issues

3. **Test the Theory**

- Using the tools at your disposal, it's time to test your theory. If your theory is that the network router is defective, try replacing it with another router to see if that fixes the issue. At this stage, it's important to remember that proving your own theories wrong doesn't mean that you've failed.

- Instead, it means that it's time to return to step two, develop a new theory, and then find a way to test that one. Sometimes your first theory may be right, but it's also common to go through several theories before arriving at the true cause of your network's issues.

Troubleshooting Network Performance Issues

4. Plan of Action

- Once you've confirmed your theory about the causes of the network issues, you're in a position to solve them. Come up with a plan of action to address the problem. Sometimes your plan will include just one step.

- For example, restart the router. In other cases, your plan will be more complex and take longer, such as when you need to order a new part or roll a piece of software back to a previous version on multiple users' computers.

Troubleshooting Network Performance Issues

5. Implement the Solution

- Now that you have a plan for fixing the network, it's time to implement it. There are some solutions that you may be able to do by yourself, while others may require cooperation from other network administrators or users.

Troubleshooting Network Performance Issues

6. Verify System Functionality

- Once you've implemented your solution, be sure to test the network. Make sure that the issue in question has been resolved, but also be on the lookout for other issues that may have arisen from the changes that you made to the network.

- As part of your verification process, make sure to consult both the network tools at your disposal as well as individual user accounts of their experiences on the network.

Troubleshooting Network Performance Issues

7. Document the Issue

- If you are a network professional or an enthusiast who is around networks often, then it's safe to say that this won't be the last time you encounter this particular issue.

- Make sure to document each stage of troubleshooting the problem, including the symptoms that appeared on the network, the theory you developed, your strategy for testing the theory and the solution that you came up with to solve the issue.

Baseline Network Performance

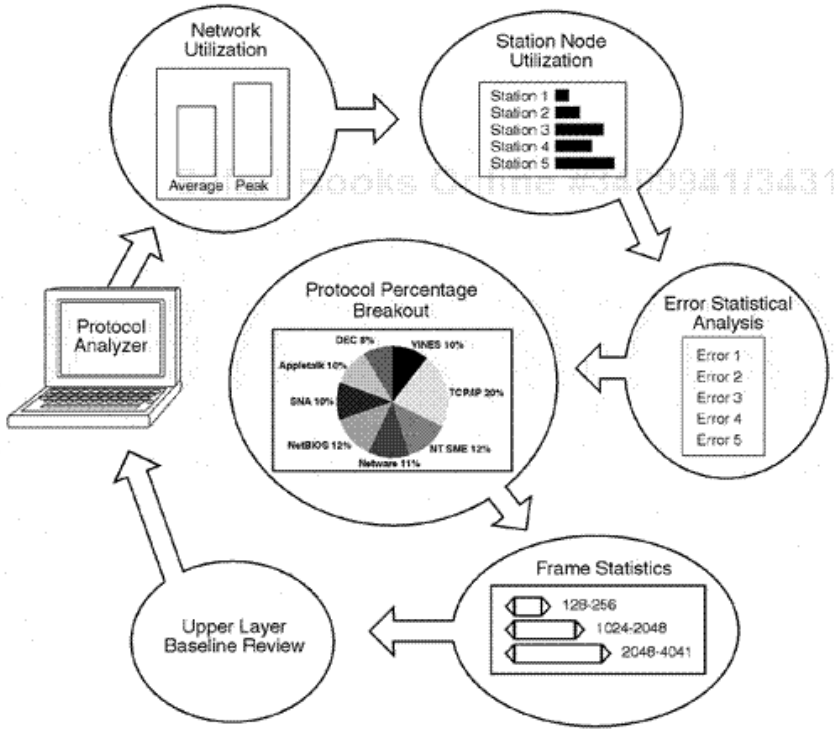
- Network performance baseline is a set of metrics used in network performance monitoring to define the normal working conditions of an enterprise network infrastructure.

- Engineers use network performance baselines for comparison to catch changes in traffic that could indicate a problem.

Baseline Network Performance

Why is baseline important in network?

- You need an accurate network baseline to work from. It stands to reason that you can't identify problems and anomalies unless you know what 'normal' looks like for your network.



Collect Network Device Performance Metrics

- Different methods and tools can be used to collect network performance metrics, depending on the type and level of measurement. SNMP (Simple Network Management Protocol) is a standard protocol for collecting and managing information from network devices, such as routers, switches, servers, or printers.

Collect Network Device Performance Metrics

Network Performance Monitoring Metrics

- Network performance monitoring (NPM) refers to the process of measuring, diagnosing, and optimizing the service quality of a network as experienced by users. NPM is complementary to application performance management (APM).

- Network performance monitoring (NPM) is critical to managing and maintaining a network's overall health, stability, and efficiency. It involves the continuous measurement, analysis, and optimization of various network parameters to ensure that users experience seamless connectivity and optimal performance.

Collect Network Device Performance Metrics

- By employing NPM strategies and leveraging key metrics, network administrators can proactively identify bottlenecks, troubleshoot performance issues, and optimize resources to deliver a high-quality user experience across the entire network ecosystem.

Collect Network Device Performance Metrics

Typical NPM Metrics

- Network performance monitoring addresses the network and the internet's role in the end-user experience. Typical NPM metrics include:

- **Latency**: How much time it takes to get a response to a packet. This is measured bi-directionally. One direction of measurement looks at when a local host, such as an application or load-balancing server (like HAProxy or NGINX), sends a packet to a remote host and times how long it takes to get a response back.

Collect Network Device Performance Metrics

- The other direction looks at when a packet is received from a remote host and measures how long it takes for the application (server) to send a response.

- **Number and percent of out-of-order packets**: This is an important measure because TCP can't pass data up to applications until bytes are in the right order. Small numbers of out-of-order packets typically don't affect things much, but when they get too high, they will impact application performance.

Collect Network Device Performance Metrics

- **TCP retransmits**: When a portion of a network path is overloaded or has performance problems, it may drop packets. TCP ensures the delivery of data by using ACKs to signal that data has been received.

- If a sender doesn't get a timely ACK from the receiver, it will resend a packet with the unacknowledged TCP segment.

- When TCP retransmits go over very low single-digit percentage levels, application performance starts to degrade.

Collect Network Device Performance Metrics

Network Device Metrics including:

- **CPU Utilization:** The percentage of CPU utilization for a specific component within a device.

- **Memory Total, Used, Free, and Utilization:** These metrics provide insight into a device component's memory allocation, usage, and availability.

Switch/Router CPU Utilization

- To determine switch CPU utilization, enter the show processes cpu sorted privileged EXEC command. The output shows how busy the CPU has been in the past 5 seconds, the past 1 minute, and the past 5 minutes.

- The output also shows the utilization percentage that each system process has used in these periods.

Switch/Router CPU Utilization

- High CPU usage on your Cisco router can be caused by a number of things, Its your job to find out why and fix the issue.

- First of all, there are several show commands you can use, the most important command of all is the "**show log**". Look for unusual entries like link flapping, arp messages, HSRP messages, routing topology changes etc.

- "**show processes cpu history**" this will give you a nice little visual of the last 60 seconds, 60 minutes and 72 hours so you can see how long this problem has been going on for, you might also be able to use this to trace back to certain times of the day and correlate this with your log messages.

Switch/Router CPU Utilization


```
rtr-wan01#sh processes cpu history
rtr-wan01   01:39:56 PM Monday Sep 24 2012 CDT


                                      2222222222222211111
    333444445555577777888886666644444000000000099999222223333344
100
 90
 80
 70
 60
 50
 40
 30
 20                                  **********
 10          ****************************************
   0....5....1....1....2....2....3....3....4....4....5....5....6
             0    5    0    5    0    5    0    5    0    5    0
              CPU% per second (last 60 seconds)


      1 2   2 1   2 1   2 2   2 2   2 1   2 1   1 2   2 1   2 1   111   2 2
    658405406964349464839415064269461595695144049441394588946043
100
 90
 80
 70
 60
 50
 40
 30
 20    * *   * *   * *   * *   * *   * *   * *   * *   * *   * *   ***   * *
 10 **# ##* ##*#* # # ##### #*#* #*# *##*#*#*#*   # #   # #  *##*#  *# #
   0....5....1....1....2....2....3....3....4....4....5....5....6
             0    5    0    5    0    5    0    5    0    5    0
              CPU% per minute (last 60 minutes)
             * = maximum CPU%   # = average CPU%


    222222211212121111111111111111111142112111111111112112212221122112122222
    465556099086948899889887999888888308938898899998918801900099068968103554
100
 90
 80
 70
 60
 50
 40                                    *
 30  *****     *                       *                                 *   *    **
 20 ************************************************************************************
 10 ######################################################################*****###
   0....5....1....1....2....2....3....3....4....4....5....5....6....6....7..
             0    5    0    5    0    5    0    5    0    5    0    5    0
                  CPU% per hour (last 72 hours)
                 * = maximum CPU%   # = average CPU%
```

Switch/Router CPU Utilization

- The next show command you should be using is the "**sh processes cpu sorted**" this command will show you a list of processes and the cpu percentage they are using for the last 5 seconds, 1 minute and 5 minutes.

- See next slide as an example, in this example highlighted is an important part of the output and this shows us the CPU interrupt percentage, typically this should not be over 10%

Switch/Router CPU Utilization


```
rtr-  -wan01#  sh processes cpu sorted
CPU utilization for five seconds: 4%/1%; one minute: 6%; five minutes: 5%
 PID Runtime(ms)     Invoked      uSecs   5Sec   1Min   5Min TTY Process
 300    18210576  1007945806         18  0.79%  2.05%  2.00%   0 IP SLAs XOS Even
   5     3882528      462691       8391  0.79%  0.14%  0.11%   0 Check heaps
 268         540         292       1849  0.39%  0.15%  0.07% 514 Virtual Exec
 301     3479872    18592255        187  0.23%  0.10%  0.10%   0 IP SNMP
 303     3395860     9292863        365  0.23%  0.11%  0.10%   0 SNMP ENGINE
 101       25076   385908749          0  0.23%  0.24%  0.23%   0 Ethernet Msec Ti
 128    25957780   124093852        209  0.15%  0.54%  0.49%   0 IP Input
  65       11324     3038780          3  0.15%  0.11%  0.10%   0 Per-Second Jobs
   2        4100      607724          6  0.07%  0.02%  0.01%   0 Load Meter
 267        5564     3035556          1  0.07%  0.00%  0.00%   0 BGP Router
  30        1020     3168874          0  0.07%  0.00%  0.00%   0 ARP Background
 124        8656    94885762          0  0.07%  0.05%  0.07%   0 IPAM Manager
 165        1016     3091557          0  0.07%  0.00%  0.00%   0 TCP Timer
 100        1172    18513496          0  0.07%  0.00%  0.00%   0 Ethernet Timer C
  85        7204      142004         50  0.07%  0.00%  0.00%   0 BGP I/O
```

Switch/Router CPU Utilization

- High processor use on “arp input” an arp message is sent as a broadcast and are limited to one request every 2 secs for the same IP, so if you do a “**show arp**” and see lots of incomplete entries chances are your default route is specified as an interface or someone is scanning your subnet for hosts.

- Spanning-tree misconfiguration can be a cause of high CPU usage if for example there is a layer 2 loop this will cause high CPU usage, but if you have the correct precautions like, “BPDU Guard” and “port-security” on your access ports you should be ok.

- Link Flapping, commonly associated with a BGP flap causes high CPU usage this may only spike your CPU but if it’s happening every few seconds or minutes then you need to investigate why the link is flapping.

Switch/Router CPU Utilization

- Routing protocol changes, a topology change can sometimes spike your CPU, have a look at the size of your routing table are the updates too big? even a route-map can be the cause of high CPU having to process too many.

- Someone else is running a debug command on another session, use the "**show users**" to see who else is logged in and find out if they have any debugs running if not then use the "**undebug all**" command to kill any debugs then check your CPU usage.

Switch/Router CPU Utilization

Host Learning

- The Catalyst 4500 learns the MAC addresses of various hosts, if the MAC address is not already in the MAC address table. The switching engine forwards a copy of the packet with the new MAC address to the CPU.

- All the VLAN interfaces (layer 3) use the chassis base hardware address as their MAC address. As a result, there is not an entry in the MAC address table, and the packets destined to these VLAN interfaces are not sent to the CPU for processing.

If there is an excessive number of new MAC addresses for the switch to learn, high CPU utilization can result.

Switch/Router CPU Utilization

Step 1: Check for the Cisco IOS Process with the show processes cpu Command.

Issue the **show processes cpu**command in order to check which Cisco IOS process consumes the CPU. In this command output, notice that the top process is the**Cat4k Mgmt LoPri**:

```
Switch#show processes cpu
CPU utilization for five seconds: 89%/1%; one minute: 74%; five minutes: 71%
 PID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min TTY Process
   1           4        53         75  0.00%  0.00%  0.00%   0 Chunk Manager

!--- Output suppressed.

  25        8008   1329154          6  0.00%  0.00%  0.00%   0 Per-Second Jobs
  26      413128     38493      10732  0.00%  0.02%  0.00%   0 Per-minute Jobs
  27   148288424 354390017        418 26.47% 10.28% 10.11%   0 Cat4k Mgmt HiPri
  28   285796820 720618753        396 52.71% 56.79% 55.70%   0 Cat4k Mgmt LoPri
```

Switch/Router CPU Utilization

Step 2: Check for the Catalyst 4500-specific process with the show platform health command.

The output of the **show platform health** command confirms the use of the CPU in order to process CPU-bound packets.

```
Switch#show platform health
                     %CPU   %CPU    RunTimeMax   Priority  Average %CPU  Total
                     Target Actual Target Actual   Fg   Bg 5Sec Min Hour  CPU

!--- Output suppressed.

TagMan-RecreateMtegR   1.00   0.00     10      4  100  500    0   0    0  0:00
K2CpuMan Review       30.00  46.88     30     47  100  500   30  29   21  265:01
K2AccelPacketMan: Tx  10.00   8.03     20      0  100  500   21  29   26  270:4
```

Switch/Router CPU Utilization

Step 3: Check the CPU queue that receives traffic in order to identify the type of CPU-bound traffic.

In order to determine the type of traffic that hits the CPU, issue the **show platform cpu packet statistics** command.

```
Switch#show platform cpu packet statistics

!--- Output suppressed.

Packets Received by Packet Queue
```

Queue	Total	5 sec avg	1 min avg	5 min avg	1 hour avg
Esmp	48613268	38	39	38	39
Control	142166648	74	74	73	73
Host Learning	**1845568**	**1328**	**1808**	**1393**	**1309**
L3 Fwd High	17	0	0	0	0
L3 Fwd Medium	2626	0	0	0	0
L3 Fwd Low	1582414	1	1	1	1
L2 Fwd Medium	1	0	0	0	0
L2 Fwd Low	576905398	37	7	8	5
L3 Rx High	257147	0	0	0	0
L3 Rx Low	5325772	10	19	13	7
RPF Failure	155	0	0	0	0
ACL fwd(snooping)	65604591	53	54	54	53
ACL log, unreach	11013420	9	8	8	8

Switch/Router CPU Utilization

Step 4: Identify the Root Cause.

- The output of the **show platform health** command shows you that the CPU sees a lot of new MAC addresses. This situation is often the result of network topology instability. For example, if the spanning-tree topology changes, the switch generates Topology Change Notifications (TCNs). The issue of TCNs reduces the aging time to 15 seconds in PVST+ mode. MAC address entries are flushed if the addresses are not learned back within the time period. In the case of Rapid STP (RSTP) (IEEE 802.1w) or MST (IEEE 802.1s), the entries immediately age out if the TCN comes from another switch.

- This age out causes MAC addresses to be learned anew. This is not a major issue if the topology changes are rare. But there can be an excessive number of topology changes because of a flapping link, faulty switch, or host ports that are not enabled for PortFast.

Switch/Router CPU Utilization

- A large number of MAC table flushes and subsequent relearning can result. The next step in root cause identification is to troubleshoot the network. The switch works as expected and sends the packets to the CPU for host address learning. **Identify and fix the faulty device that results in excessive TCNs.**

- Your network can have a lot of devices that send traffic in bursts, which causes MAC addresses to be aged out and subsequently relearned on the switch. In this case, increase the MAC address table aging time in order to provide some relief.

- With a longer aging time, the switches retain the device MAC addresses in the table for a longer period of time before the age out.

Switch/Router Memory Utilization

- The following is sample output from the **show processes memory** command:

```
Router# show processes memory

Total: 5611448, Used: 2307548, Free: 3303900
  PID  TTY  Allocated      Freed    Holding    Getbufs    Retbufs Process
    0    0     199592       1236    1907220          0          0 *Init*
    0    0        400      76928        400          0          0 *Sched*
    0    0    5431176    3340052     140760     349780          0 *Dead*
    1    0        256        256       1724          0          0 Load Meter
    2    0        264          0       5032          0          0 Exec
    3    0          0          0       2724          0          0 Check heaps
    4    0      97932          0       2852      32760          0 Pool Manager
    5    0        256        256       2724          0          0 Timers
    6    0         92          0       2816          0          0 CXBus hot stall
    7    0          0          0       2724          0          0 IPC Zone Manager
    8    0          0          0       2724          0          0 IPC Realm Manager
    9    0          0          0       2724          0          0 IPC Seat Manager
   10    0        892        476       3256          0          0 ARP Input
   11    0         92          0       2816          0          0 SERIAL A'detect
   12    0        216          0       2940          0          0 Microcode Loader
   13    0          0          0       2724          0          0 RFSS watchdog
   14    0   15659136   15658584       3276          0          0 Env Mon
...
   77    0        116          0       2844          0          0 IPX-EIGRP Hello
                                    2307224 Total
```

Interface/Bandwidth Utilization

What is the bandwidth?

- Bandwidth is the maximum amount of data that an object can transfer within a given amount of time. It is object-specific. Two different objects may have similar or different bandwidths. It depends on many factors such as the object's capacity, environment, configuration, etc.

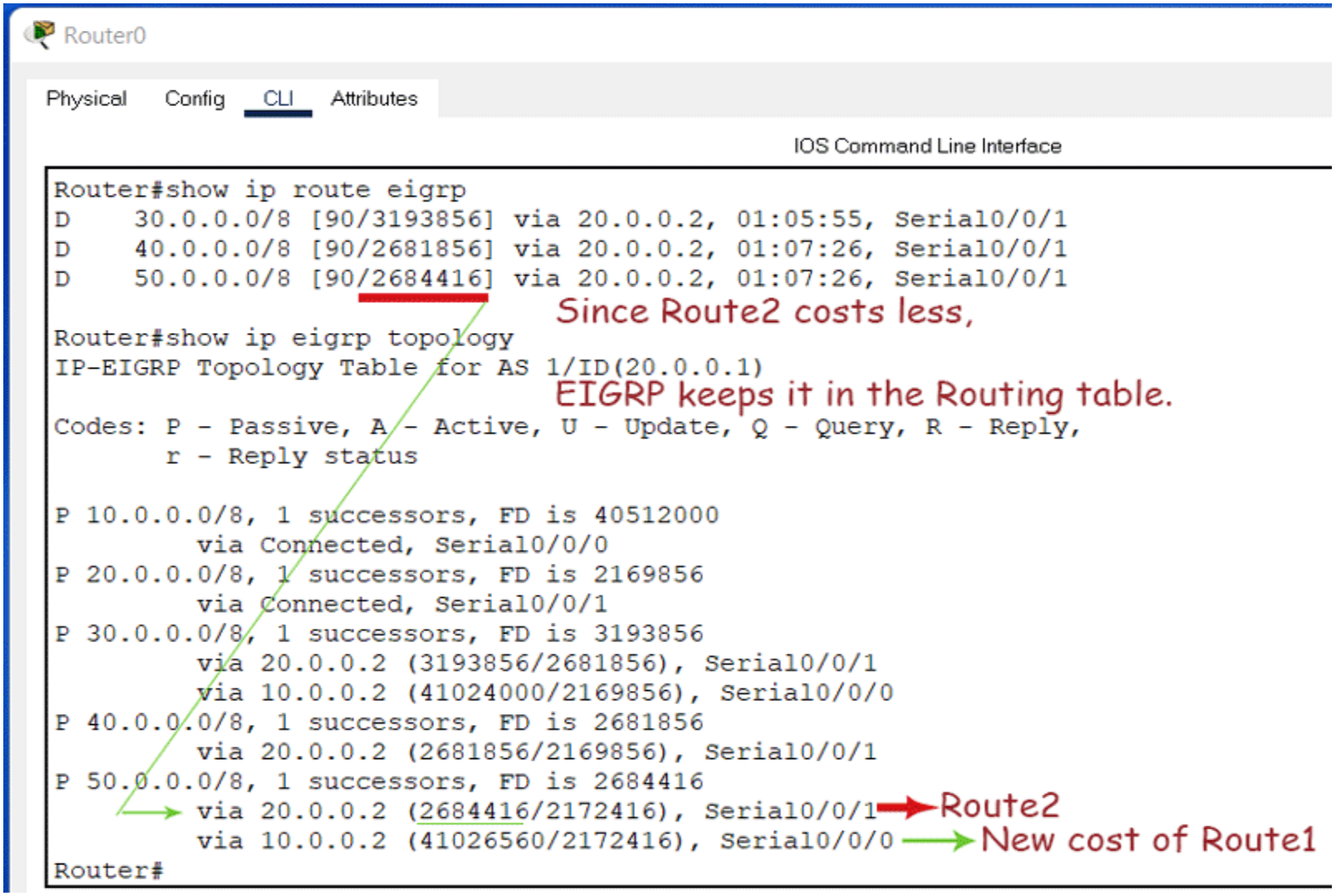
Interface/Bandwidth Utilization

Using the **bandwidth** command to influence a routing protocol's metric

- Some routing protocols such as EIGRP and OSPF use the interface's bandwidth to calculate the metric of each route. We can use the **bandwidth** command to influence their metric calculation. For example, EIGRP uses the interface's bandwidth in the metric calculation formula.

- By changing an interface's bandwidth, we can force EIGRP to select the route we want for a particular destination without making any change in the physical layout of the network.

Interface/Bandwidth Utilization



Q & A

E.R. Ramesh, M.C.A., M.Sc., M.B.A.,
98410 59353, 98403 50547
rameshvani@gmail.com

Question Bank

1. .....
2. .....
3. .....
4. .....
5. .....
6. .....
7. .....
8. .....