**APEX CAMPUS NETWORK**

**INTRODUCTION**

In today’s technology-driven world, organizations across various sectors rely heavily on robust and efficient communication networks to support their operations.

Campus networks, often referred to as corporate or enterprise networks, play a crucial role in enabling seamless connectivity and collaboration within educational institutions, corporate offices, and other large-scale facilities. These networks serve as backbone of communications infrastructure, providing a foundation for essential services such as data sharing, file transfer, internet access, and application deployment.

A campus network encompasses a collection of interconnected local area networks (LANs) that operate within a confined geographical area, typically encompassing a college campus, corporate headquarters or industrial complex. These networks are designed to cater to diverse connectivity needs of a large number of users, facilitating efficient communication and resource sharing among employees, students, and other stakeholders.

**FUNCTIONAL LAYERS OF CAMPUS NETWORKS**

* **ACCESS LAYER:**

The access consists of devices that directly connect end-user devices, such as computers, laptops, and smartphones to the network.

* **DISTRIBUTION LAYER:**

The distribution layer aggregates traffic from multiple access layer devices and provides routing and segmentation within the network.

* **CORE LAYER:**

The core layer forms the backbone of the network, providing high speed connectivity and handling the bulk of data traffic.

**BENEFITS OF CAMPUS NETWORKS**

1. **Enhanced Communication and Collaboration:**

Campus network facilitate seamless communication and collaboration among employees, students, and other stakeholders, enabling efficient information sharing and task management.

1. **Resource Sharing:**

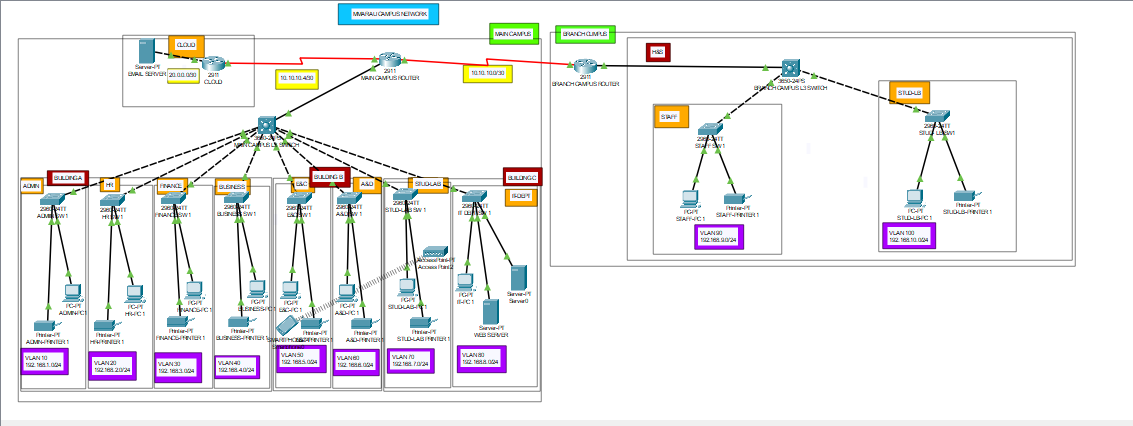
Campus networks provide a platform for sharing resources, such as printers, file servers, and application servers, minimizing resource utilization and reducing costs.

1. **Centralized Management:**

Campus networks enable centralized management of network devices, policies, and security measures, simplifying network administration and enhancing security posture.

1. **Scalability:**

Campus networks can be seamlessly scaled to accommodate growing user bases and evolving network demands, ensuring that the network infrastructure remains adaptable to future needs.



WIRED AND WIRELESS

Above is our network for campus network, The network is a Wide Area Network that has been implemented in the campus set up due t the large number of students. The Above network is both wired and wireless network, due to students and visitors connectivity the network had to wireless as well to cater for the needs of the students with smartphones and laptops to access internet via the various access points in the school of hotspot for the students. There are various cables that were used in implementing the above to ensure that network is operational such as

**Ethernet Cables (Twisted Pair):**

Category 6 (Cat6): Offers higher data transfer rates and better performance than Cat5 hence suitable for this network in the university set up where users of the network are many.

**Copper Backbone Cables:**

Cat6 : Used for high-speed connections between network switches and core networking equipment.

Coaxial Cables:

RG-6 and RG-11: Sometimes used for cable television (CATV) distribution within campus buildings.

Coaxial Cables:

RG-6 and RG-11: Sometimes used for cable television (CATV) distribution within campus buildings.

**Fiber Optic Cables:**

Multimode Fiber (MMF): Suitable for shorter distances and offers various bandwidth options. OM3 and OM4 are common types for high-speed applications.

USB and HDMI Cables:

Used for connecting peripherals, displays, and other devices.

**ENCODING**

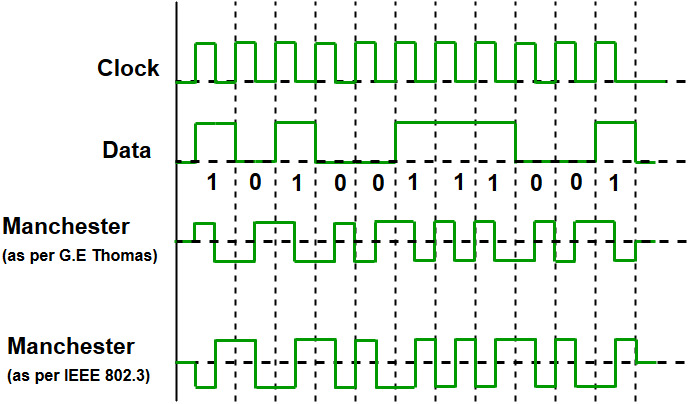
**Manchester Encoding in Campus Network**

Manchester encoding is a synchronous clock encoding technique used by the physical layer of the Open System Interconnection [OSI] to encode the clock and data of a synchronous bit stream. The idea of RZ and the idea of-L are combined in Manchester.

Different encoding techniques are used in data communication to ensure data security and transmission speed. Manchester encoding is an example of digital encoding. Because each data bit length is defined by default, it differs from other digital encoding schemes. The bit state is defined by the direction of the transition. Bit status is represented in various ways by different systems, although most systems use 1 bit for low to high transitions and 0 bit for high to low transitions.

In manchester duration of a bit is divided into two halves. The voltage remains the same at one level during the first half & moves to the other level. The transition at the middle of the bit provides synchronization. Differential Manchester, on the other hand, combines the idea of RZ and NRZ-I. There is always a transition at the middle of the bit, but the bit values are determined at the beginning of the bit. If next bit is zero there is transition if next bit is 1 there is none.

**Note:** Manchester encoding’s main advantage is signal synchronization.



The binary data to be transmitted over the cable are not sent as NRZ [Non-return-to-zero].

**Non-return-to-zero [NRZ] –**

NRZ code’s voltage level is constant during a bit interval. When there is a long sequence of 0s and 1s, there is a problem at the receiving end. The problem is that the synchronization is lost due to a lack of transmissions.

It is of 2 types:

**NRZ-level encoding –**

The polarity of signals changes when the incoming signal changes from ‘1’ to ‘0’ or from ‘0’ to ‘1’. It considers the first bit of data as polarity change.

**NRZ-Inverted/ Differential encoding –**

In this, the transitions at the beginning of the bit interval are equal to 1 and if there is no transition at the beginning of the bit interval is equal to 0.

**Characteristics of Manchester Encoding –**

A logic 0 is indicated by a 0 to 1 transition at the center of the bit and logic 1 by 1 to 0 transition.

The signal transitions do not always occur at the ‘bit boundary’ but there is always a transition at the center of each bit.

The Differential Physical Layer Transmission does not employ an inverting line driver to convert the binary digits into an electrical signal. And therefore the signal on the wire is not opposite the output by the encoder.

**The following are the properties of Manchester encoding:**

Each bit is sent at a predetermined rate.

When a high to low transition happens, a ‘1’ is recorded; when a low to high transition occurs, a ‘0’ is recorded.

At the mid-point of a period, the transition that is utilized to precisely note 1 or 0 happens.

The Manchester Encoding is also called Biphase code as each bit is encoded by a positive 90 degrees phase transition or by negative 90 degrees phase transition.

The Digital Phase Locked Loop (DPLL) extracts the clock signal and deallocates the value and timing of each bit. The transmitted bitstream must contain a high density of bit transitions.

The Manchester Encoding consumes twice the bandwidth of the original signal.

The advantage of the Manchester code is that the DC component of the signal carries no information. This makes it possible that standards that usually do not carry power can transmit this information.

It is a self-clocking protocol, meaning that the receiver can determine the clock frequency from the incoming data.

The Manchester encoding ensures a constant transition density, making it easier to detect the start and end of a data frame.

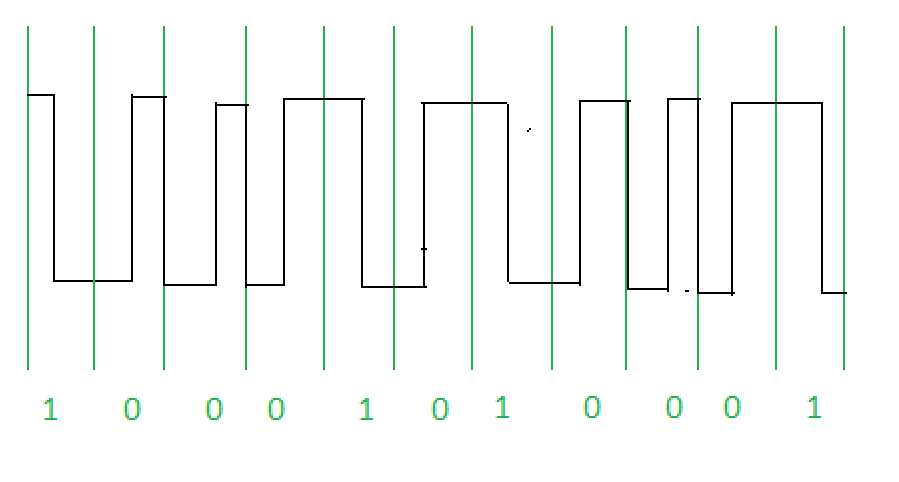
It provides a simple and reliable way to detect errors in the data transmission by checking for a violation of the encoding rules.

The encoding process adds a redundant bit to the data, enabling error correction in some applications.

Manchester encoding can also be used for multi-level signaling, where multiple voltage levels are used to represent different data states.

Only drawback is the signal rate. The signal rate is manchester and differential is double that for NRZ. The reason is that there is always one transition at the middle of the bit and maybe one transition at the end of each bit.

Another example to find out the bits by seeing the transitions.



**Advantages of Manchester Encoding:**

**Self-clocking**: Manchester encoding is self-clocking, which means that the receiver can synchronize its clock with the transmitter’s clock. This ensures that the data is transmitted and received at the same rate, and there is no need for a separate clock signal.

**Reduced DC component:** Manchester encoding eliminates the DC component in the transmitted signal, which reduces the risk of errors due to interference from external sources.

**Error detection:** Manchester encoding provides a mechanism for detecting errors in the transmitted data. Any change in the voltage level within a time interval indicates a bit error, which can be detected and corrected.

**Simplicity:** Manchester encoding is a relatively simple encoding scheme that can be implemented using simple digital circuits.

**Disadvantages of Manchester Encoding:**

**Lower data rate:** Manchester encoding has a lower data rate than other encoding schemes, such as non-return-to-zero (NRZ) encoding, which means that it takes more time to transmit the same amount of data.

**Higher bandwidth requirement:** Manchester encoding requires a higher bandwidth than other encoding schemes, as each bit requires two voltage transitions within each time interval.

**Clock synchronization:** Although Manchester encoding is self-clocking, it still requires the receiver to synchronize its clock with the transmitter’s clock, which can be a challenge in some situations.

**Reduced transmission distance:** Manchester encoding has a reduced transmission distance compared to other encoding schemes, as the signal loses strength over long distances due to the need for frequent voltage transitions.

**FRAMING**

**What are frames?**

A frame is a simple network message in systems that use packet switching. In other word a frame is a repeating framework that enables time-division multiplexing. It typically includes a series of symbols or bits that provide frame synchronization advantages. In the bits and symbols sequence it gets, it displays the beginning and end of the payload data. At the moment a frame is broadcast when a receiver is connected to the system. Until it discovers a new frame coordination sequence, it stays away from the information.

**Parts of frame**

A frame generally has the following parts:

* ***Frame header:***  It contains the source and destination address of the frame.
* ***Payload field:*** It will contain the message which is needed to be delivered.
* ***Trailer:*** It contains the error correction and error detection bits.
* ***Flag:*** It marks the beginning and the end of the frame.

**What is framing?**

Framing is a process of dividing a stream of data into smaller, more manageable units called frames. The frames are the transmitted over the network and reassembled at the receiving end to recreate the original data stream. Framing is important in computer network since it helps in ensuring data integrity and security by allowing the receiver to detect errors and prevent unauthorized access.

**How framing works?**

It is done in computer network by combining hardware and software. Hardware-level network devices like switches and routers divide the data stream into frames using specialized processors. Then, using a system like Ethernet, these frames are transmitted across the network.

Framing is usually dealt with at the program level by a network protocol like the Point-To-Point Protocol (PPP) or the High-Level Data Link Control (HDLC). The source and target identifiers, error-checking codes, and other control information are added as headers and trailers by these protocols to each frame.

The same protocol and hardware are used to put the frames back together into the initial data stream after they have been delivered to the target. The receiving device checks each frame for errors and drops any frames that fail the error-checking process.

**Types of framing in computer network**

There are mainly two types of framing. They include;

* ***Fixed sized framing***

Fixed-sized framing involves dividing the data into frames of a predetermined, fixed size. This approach is commonly used in network such as Ethernet, where each frame is exactly 1500bytes long. Its advantage is that it is simple and effective, as all frames are of the same size. This makes it easy for network devices to split the data stream into frames, and for the receiving device to know how much data is in each frame.

It also makes it easier to manage network resources, as it ensures that each frame takes up the same amount of bandwidth. This is important in high-speed networks where a large amount of data is being transmitted simultaneously. Furthermore, fixed-size framing is suitable for data that can be easily divided into smaller units, such as text files or structured data.

Its disadvantage is that it may not be suitable for all types of data. For example, video or audio files may not fit neatly into fixed-size frames, as their size and complexity may vary. It also can introduce additional overhead as some frames may contain unused space if the data being transmitted does not fill the entire frame.

* ***Variable size framing***

Variable size framing involves dividing the data into frames of varying sizes. This approach is used in network where the data being transmitted does not fit neatly into fixed-size frames, such as video or audio streaming. In variable size framing, each frame contains a header that specifies the length of the payload, allowing the receiving device to know how much data is in each frame.

Its advantage is that it provides more flexibility than fixed-size framing. Frames can be sized to fit the data being transmitted, which can help to reduce overhead and increase efficiency. This is important in applications where data may be of varying sizes, such as multimedia streaming.

Its disadvantage is that it can be more complex to implement, as each frame must contain a header specifying the length of the payload. This increases the overhead of each frame, which can reduce overall network efficiency. It also can introduce delay, as the receiver must wait for the entire frame to be received before processing it.

**Approaches of framing in computer network**

There are two main type of framing approaches used in computer networks. They include;

* ***Byte-oriented framing***

Byte-oriented framing divides data into fixed-length bytes, which are then encapsulated into frames. The frame contains a header, a payload and a trailer. The header and trailer provide control information such as the source and destination addresses, error-checking codes and other control information.

Byte-oriented framing is widely used in network protocols such as Ethernet and TCP/IP. It is also used in file transfer protocol such as FTP and HTTP.

* ***Bit-oriented framing / character-oriented framing***

Bit-oriented framing divides data into variable-length units called characters. Each character is then encapsulated into frames, which contain a header, a payload and a trailer.

It is less common but is still used in some network protocols such as the Synchronous Data Link Control (SDLC) protocol used by IBM mainframes.

**Advantages / importance of framing**

Framing provides the following services;

* ***Data integrity ;***

It provides error detection and error correction mechanism which in turn ensure the integrity of the transmitted data over the network.

* ***Security ;***

Framing also helps in ensuring network security by preventing unauthorized access to data.

* ***Efficient Data Transmission ;***

By dividing the total data into smaller frames the framing makes the data transmission more efficient and low network congestion with improved overall performance.

**Disadvantages of framing**

* ***Overhead ;***

Framing adds overhead to the main data stream which in turn reduces the content of actual data that can be transmitted over the network.

* ***Complexity ;***

We need to use both hardware and software mechanisms to implement framing which increases the complexity.

* ***Delay ;***

Framing sometimes leads to delay in large networks, as multiple frames are transferred simultaneously.

**Framing type to be used in our network and why?**

Since our network is a local area network we will use ***variable-size framing*** since the data to be transmitted in our network could be of different size, therefore variable-size will be more efficient to implement due to not having fixed size framing and also for compactible of different data type and their respective sizes.

Under variable-size framing i will use ***High-Level Data Link Control*** due to our network being a LAN and also HDLC provides various operations like framing, data transparency, error detection and control and even flow control therefore being easily to manage our network efficiently.

***HDLC*** is a group of protocols or rules for transmitting data between network points.

***HDLC works in the manner that*** data is organized into units called frames and then being sent across a network destination that verifies its successful arrival. It is a bit-oriented protocol that is applicable for both point-to-point and multipoint communication.

The HDLC protocol also manages the flow or pacing at which data is sent.

**HDLC Transfer mode**

HDLC supports two types of transfer modes namely;

* ***Normal Response Mode (RNM);***

Here, two types of stations are there; ***primary station***; that send command and ***secondary station*** that can respond to received commands. It is used in both point-to-point and multipoint communications.

* ***Asynchronous Balanced Mode (ABM);***

Here, the configuration is balanced, that is each station can both send commands and respond to commands. It is used for only point-to-point communications.

**HDLC Frame**

HDLC contains up to six fields namely;

* ***Flag*** that marks the beginning and end of the frame in 8-bit sequence
* ***Address*** that contains address of the receiver
* ***Control*** that control flow and error in the data
* ***Payload*** that carries data from the network
* ***Frame check sequence*** for error detection

**Types of HDLC Frames**

* ***I-frame / information frame;***

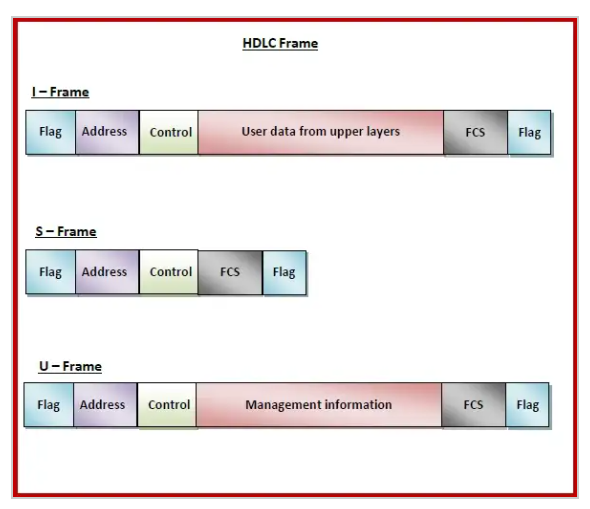
It carries user data from the network layer. It also includes flow and error control information that is piggybacked on user data. The first bit of i-frame is 0.

* ***S-frame / supervisory frame;***

It does not contain information field. It is used for flow and error control when piggybacking is not required. The first two bits of s-frame are 10.

* ***U-frame / un-numbered frame* ;**

It is used for myriad miscellaneous functions like link management. It may contain an information field, if required. The first two bits of control field of u-frame are 11.



Therefore there are two ways to define delimiters in variable sized framing which are;

* ***Length field ;***

Here, a length field is used to determine the size of the frame. It is used in Ethernet (IEEE 802.3).

* ***End Delimiter ;***

Here, a pattern is used as a delimiter to determine the size of frame. It is used in Token Rings. If the pattern occurs in the message, then two approaches are used to avoid the situations-

* ***Byte – stuffing ;***

A byte is stuffed in the message to differentiate from the delimiter. This is also called character-oriented framing.

* ***Bit – stuffing ;***

A pattern of bits of arbitrary length is stuffed in the message to differentiate from the delimiter. This is also called bit-oriented framing.

**Framing in Data Link Layer**

In the physical layer, data transmission involves synchronized transmission of bits from the source to the destination.

The Data-Link Layer packs these bits into frames. Data-link layer takes the packet from the network layer and encapsulates them into frames. If the frame size becomes too large, then the packet may be divided into small sized frames.

At receiver end, data link layer picks up signals from hardware and assembles them into frames.

**ERROR CONTROL**

**Error Control in a campus network**

**Introduction:**

Error control involves identifying, correcting, and preventing errors during data transmission. To achieve this, it is crucial to implement effective error control mechanisms within the network infrastructure. Cisco, a leading networking solutions provider, offers a comprehensive set of tools and protocols to address errors and ensure the smooth functioning of a campus network.

**Error Types in a Campus Network:**

It is essential to understand the types of errors that can occur in a campus network. Common errors include packet loss, latency, collisions, and corrupted data. These issues can arise due to various factors such as network congestion, hardware failures, or electromagnetic interference.

Below is a detailed step-by-step approach to implementing error control in a campus network, focusing on each OSI model layer

**Physical Layer (Layer 1):**

At the physical layer, where the actual transmission of bits occurs, error control is primarily concerned with minimizing signal degradation and electromagnetic interference. Cisco employs technologies such as Ethernet switches with auto-negotiation and error-detection capabilities. By using quality cabling, properly configuring switch ports, and ensuring devices operate within specified signal strength parameters, the physical layer contributes to error-free data transmission.

**Data Link Layer (Layer 2):**

The data link layer is crucial for error detection and correction. Cisco switches implement mechanisms like cyclic redundancy checks (CRC) to identify errors in received frames. In the event of an error, the switch can request retransmission using the Automatic Repeat reQuest (ARQ) protocol. Additionally, the Spanning Tree Protocol (STP) prevents broadcast storms and ensures loop-free topologies, minimizing the risk of collisions and enhancing data link layer stability.

**Network Layer (Layer 3):**

Error control at the network layer involves routing protocols and packet integrity. Cisco routers utilize protocols such as OSPF or EIGRP to dynamically adapt to network changes and reroute traffic in the case of link failures. To address packet loss or corruption, the network layer leverages ICMP for error reporting and diagnosis. Packet loss statistics can be monitored using tools like Cisco's NetFlow to identify and troubleshoot issues promptly.

**Transport Layer (Layer 4):**

The transport layer plays a significant role in error control through protocols like Transmission Control Protocol (TCP). Cisco devices utilize TCP's sliding window mechanism for flow control, ensuring efficient and reliable data transfer. In the event of packet loss or corruption, TCP triggers the retransmission of specific segments, guaranteeing the accurate delivery of data.

**Application Layer (Layer 7):**

While the application layer is primarily concerned with end-user interactions, error control at this layer involves implementing application-level protocols with error-handling capabilities. For instance, Cisco's VoIP solutions often use the Real-Time Transport Protocol (RTP) for voice transmission, which includes mechanisms for error recovery and retransmission.

***ERROR MANAGEMENT***

***SIGNIFICANCE OF ERROR MANAGEMENT***

In Campus networks, data integrity plays a pivotal role in ensuring the seamless and accurate exchange of information between various devices and systems. Errors can disrupt communication, compromise data security, and impede the smooth operation of academic and administrative activities. Effective error management, therefore, becomes crucial to safeguard the integrity and efficiency of the campus network.

***TYPES OF ERRORS AND THEIR SOURCES***

Errors can originate from various sources during data transmission across the network:

1. **Noise:** Electromagnetic interference, caused by electrical devices or environmental factors, can distort or corrupt data signals.
2. **Hardware Failures:** Defective data components, such as routers, switches, or cables, can introduce errors into data packets.
3. **Software Issues:** Bugs or malfunctions in network protocols or applications can also lead to data corruption.
4. **Denial-of-Service Attacks:** Malicious actors can intentionally inject errors into the network to disrupt communication or steal data.

***ERROR DETECTION MECHANISMS: ENSURING ACCURACY***

To protect data integrity, various error detection mechanisms are employed:

1. **Parity Checking:** This method adds a redundant bit to check data block, ensuring that the total number of 1s is either even or odd. Upon arrival, the receiver checks the parity count to detect any errors.
2. **Checksum Calculations:** A checksum, a unique value derived from the data content, is appended to each data packet. Upon receipt, the receiver recalculates the checksum to compare it against the received value. Discrepancies indicate an error.
3. **Cyclic-Redundancy Check (CRC):** This algorithm generates a more sophisticated checksum incorporating polynomial arithmetic to error detection capabilities.
4. **Frame Check Sequence (FCS):** Used in protocols like Ethernet, an FCS is calculated based on the data content and appended to the frame. The receiver verifies the FCS to detect any errors.

***ERROR CORRECTION STRATEGIES: RESTORING DATA INTEGRITY***

Once an error is detected, error correction mechanisms are activated to recover the original data:

1. **Retransmission:** The data is sent again from the sender, ensuring that an error-free copy reaches the receiver. This is the most common error correction method.
2. **Forward Error Correction (FEC):** ECC codes introduce additional redundant bits to the data, allowing for the correction of single-bit errors without the need for retransmission. This method is particularly efficient for applications with strict latency requirements.
3. **Hybrid Error Correction:** A combination of retransmission and FEC can be employed to handle both single-bit and multi-bit errors, maximizing error recovery and network efficiency.

***ERROR MANAGEMENT AT DIFFERENT LAYERS***

Error management strategies should be implemented across various layers of the network architecture:

1. **Link Layer:** Data link protocols like Ethernet and Wi-Fi incorporate error detection and correction mechanisms at the physical and data link layers to ensure reliable data transmission.
2. **Network Layer:** Network protocols like IP and TCP provide mechanisms for retransmission, error handling, and congestion control to maintain data integrity and reliability in the network layer.
3. **Transport Layer:** Transport protocols like UDP and TCP offer additional error handling capabilities particularly for ensuring reliable data delivery in applications like file transfers and voice calls.
4. **Application Layer:** Applications like file transfer protocols, messaging systems, and video streaming services incorporate their own error handling mechanisms to protect against specific error types and ensure data integrity for specific applications.

***IMPLEMENTING COMPREHENSIVE ERROR MANAGEMEN***

By implementing comprehensive error management strategies across all layers of the network, the campus network can achieve:

1. **High Reliability:** Errors are detected and correctly quickly, ensuring that data is delivered accurately and without disruptions.
2. **High Efficiency:** Error management mechanisms are optimized to minimize network overhead and maximize data throughout.
3. **Enhanced Security:** Data corruption caused by errors is prevented, reducing the risk of data loss, security breaches, and denial of service attacks.
4. **Seamless Communication:** Users experience a seamless and reliable experience across the campus network, enabling effective communication and collaboration among various devices and systems.

**RELIABLE TRANSMISSION**

**Sliding window algorithm**

The sliding window is a technique for sending multiple frames at a time. It controls the data packets between the two devices where reliable and gradual delivery of data frames is needed. It is also used in TCP (Transmission Control Protocol).

In this technique, each frame has sent from the sequence number. The sequence numbers are used to find the missing data in the receiver end. The purpose of the sliding window technique is to avoid duplicate data, so it uses the sequence number.

**Working of the Sliding Window algorithm**

The working of the sliding window protocol can be divided into two steps sender steps, and the receiver steps and also some important values are needed in a network model for smooth transmission of the data frames are:

Sender and the receiver side

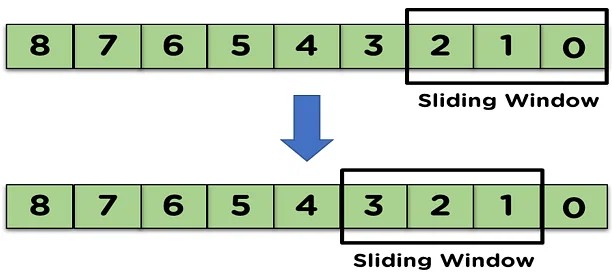
Window Size

The total data frames to be transmitted

Proper sequencing of the frames

**Steps for the Sender Side**

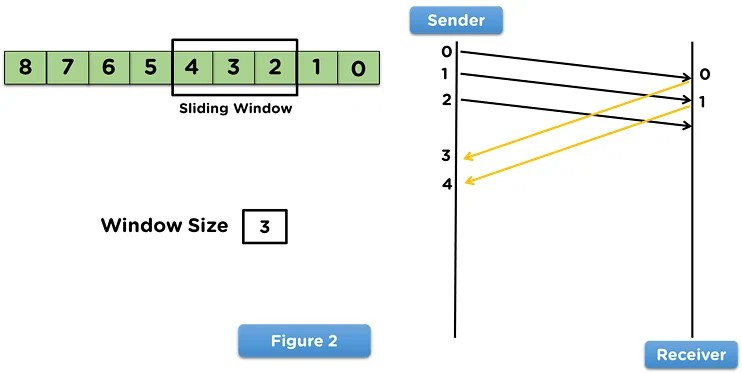
**Sliding\_window\_algorithm\_sender\_side**

* To begin with, the sender side will share data frames with the receiver side per the window size assigned to the model.
* The sliding window will appear on the frames transmitted over to the receiver side.
* Then the sender will wait for an acknowledgment from the receiver side for the shared frames. As shown in this figure.
* When the receiver transmits the acknowledgment of the first transmitted frame, the sliding window will shift from the acknowledged frame.

**Steps for the Receiver Side**

**Sliding\_window\_algorithm\_receiver\_side.**

* On receiving the data frames from the sender side, the receiver will use the frames in the network model.
* The receiver uses the frame, it will transmit the acknowledgement to the sender side for that data frame.
* Then, the receiver side will receive the next data frame from the sender side, as shown in the figure.



This process continues until all the frames are transmitted from the sender side to the receiver side, and the receiver side transmits the acknowledgment of all the received frames.

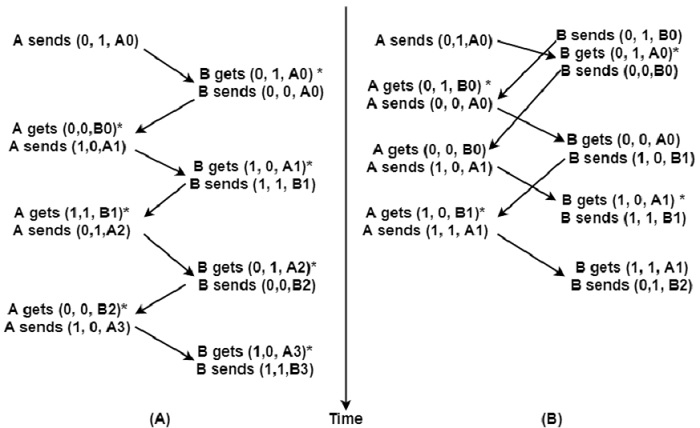
**Go Back-n Protocol**

Go-Back-N Automatic Repeat Query (ARQ) protocol is also referred to as Go-Back-N Automatic Repeat Request. It is a data link layer protocol that helps a sliding window method. In this, if any frame is manipulated or lost, all subsequent frames have to be sent again.

For example, in GO- Back –N, the N is the sender’s window size; if it is GO-Back-5, the sender will send frame 1 to 5 before receiving the knowledge of frame 1.

All the frames are numbers to deal with the most and duplicate frames. If the sender does not receive the receiver’s acknowledgement, then all the frames available in the current window will be retransmitted.

The design of the Go-Back-N protocol is shown below –



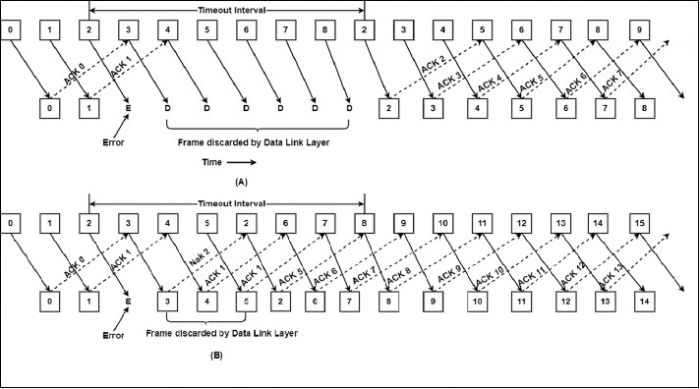
**Selective Repetitive ARQ**

Selective Repeat ARQ is also referred to as the Selective Repeat Automatic Repeat Request. It is a data link layer protocol that facilitates a sliding window method. The Go back-N ARQ protocol operates well if it has fewer errors.

In this protocol, the sender window size is always similar to the size of the receiver window. The size of the sliding window is continually greater than 1.

If the receiver obtains a corrupt frame, it does not directly remove it. It sends a negative acknowledgement to the sender. The sender sends that frame again immediately, receiving a negative acknowledgement. There is no waiting for any time-out to share that frame.

The structure of the Selective Repeat ARQ protocol is demonstrated below –

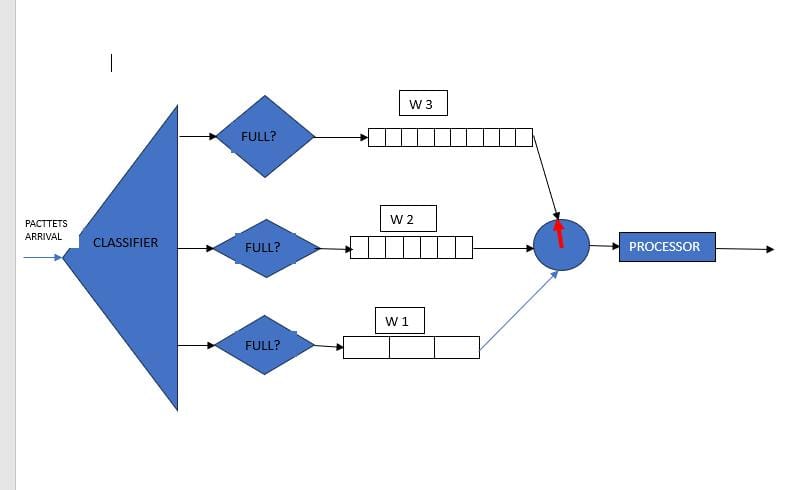
**Advantages and Disadvantages of Sliding Window algorithm**

**Advantages**

* In this algorithm, a sender can share multiple frames and then wait for the acknowledgment.
* This algorithm has much better efficiency in comparison, with low time delay.
* This algorithm requires sorting for increased efficiency and applies full-duplex transmission.

**Disadvantages**

* In case the sender does not receive acknowledgement from the receiver side, the network model becomes inefficient.
* Loss and wastage of bandwidth due to sharing multiple frames simultaneously.

**WEIGHTED FAIR QUEUING ALGORITHM**

Weighted fair queuing algorithm is used since the in considers both priority of the packets in the queue and the and also uses the round robin fashion that allows all packets from all the packets in the queue to be. As the packets arrive they are classified depending on their weight and then placed in their respective queues where the switch that applies round robin algorithm selects packets from the queue and processed according to their priority.