Lect. 4 - Study of Digital Transmission

Digital Transmission - is the transmission of signals that vary discretely with time between two values of some physical quantity, on value representing binary 0 and 1.

Two Categories:

• **Digital Data** – digital data is assigned to one voltage level to binary 1 and another for binary 0.

• **Analog Data** – Analog data such as video and voice are often digitized to be able to use digital transmission facilities.

Digital-to-Digital encoding is the representation of digital information by a digital signal.

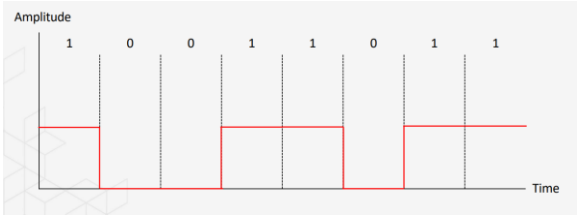
Three Categories of Digital-to-Digital Encoding:

• **Unipolar** – in this scheme, all the signal levels are either above or below the axis.

• **Polar** – the voltage are on the both sides of the axis.

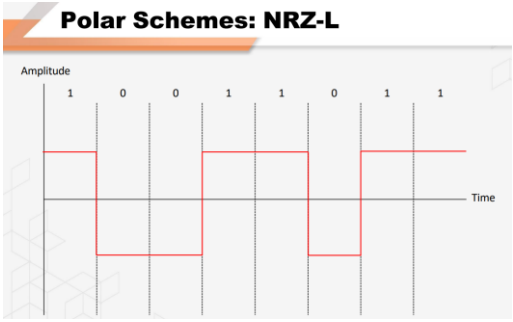
• **Bipolar** – there are **three voltage levels: positive, negative, and zero.** Voltage level for one data element is at zero, while voltage level for the other element alternates between positive and negative.

Unipolar Encoding – positive voltage defines bit 1 and zero voltage defines bit 0.



Non Return to Zero-Level (NRZ-L) – the level of signal depends on the type of bit that it represents; if a bit is 0 or 1, then their voltage will be positive and negative respectively.

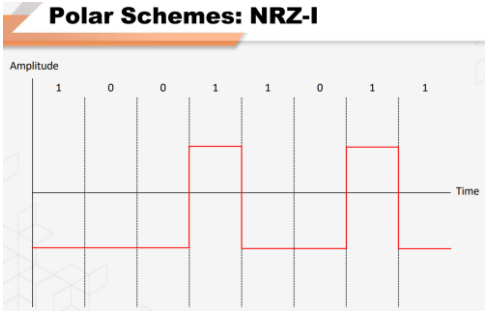
• Generally, **Positive Voltage represents 1, and Negative Voltage represents 0.**



Non Return to Zero-Inverted (NRZ-I) – Inversion of the voltage level that represents 1 bit.

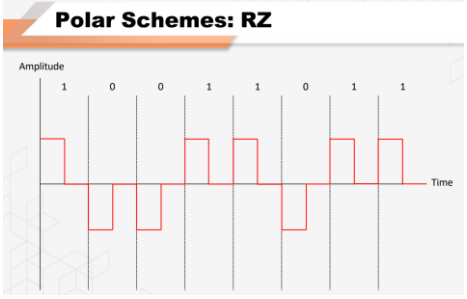
• In NRZ-I, voltage changes when 1 bit is encountered.

• In this scheme, **0 bit represents no change and 1 bit represents a change in voltage level.**



Return to Zero (RZ) – Signal changes between bits. RZ uses three voltage levels:

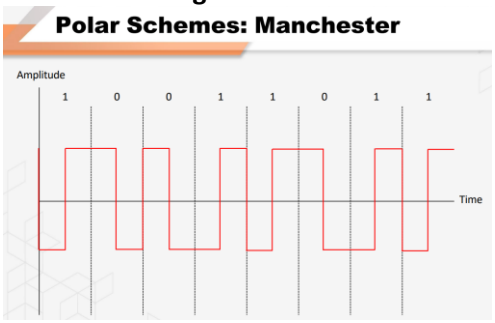
• 1 – Positive Voltage
• 0 – Negative Voltage
• Zero – None



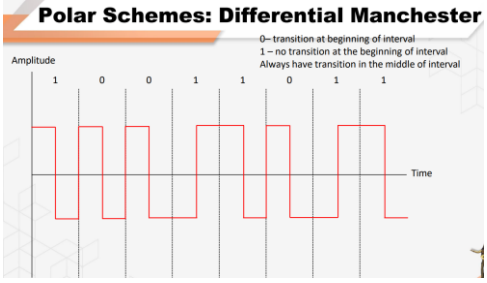
Biphase – an encoding scheme in which signal changes at the middle of the bit interval but does not return to zero.

• Biphase is implemented in two different ways:
    1. Manchester
    2. Differential Manchester

Manchester – this encoding scheme is a combination of RZ and NRZ-L.
• Changes the signal at the middle of the bit interval but does not return to zero for synchronization.
• Negative to Positive transition – 1 bit
• Positive to Negative transition – 0 bit

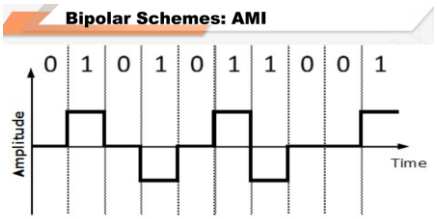


Differential Manchester – this encoding scheme is a combination of RZ and NRZ-I.
• Changes in the middle of the bit but changes phase only when 1 is encountered.
• Transition at the beginning of interval– 0 bit
• No Transition at the beginning of interval – 1 bit
• Always a transition in the middle of interval (middle of bit)

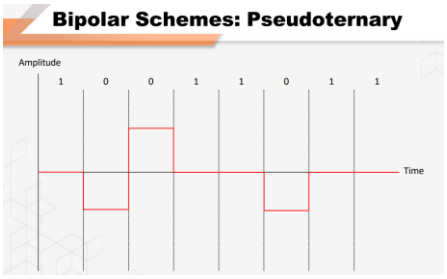


Bipolar encoding scheme represents three voltage levels: positive, negative, and zero.
• 0 bit – Zero Level, no change
• 1 bit – alternating positive and negative voltages.
• Two types: **Alternate Mark Inversion (AMI) and Pseudoternary**

Alternate Mark Inversion (AMI) – a neutral zero voltage represents binary 0. Binary 1's are represented by alternating positive and negative voltages.



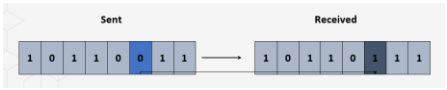
Pseudoternary – Bit 1 is encoded as zero voltage and the bit 0 is encoded as alternating positive and negative voltages.



Lect. 5 - Error Detection

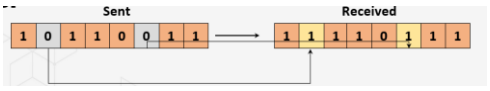
Error is a condition where the receiver's information does not match with the sender's information.

During transmission, digital **signals suffer from noise that can introduce errors** in the binary bits travelling from sender to receiver.

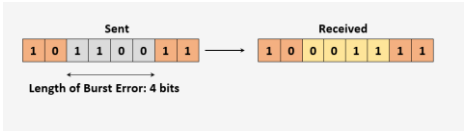


Bit Error (Single Bit Error)
- Only 1 bit in the data unit has been changed.

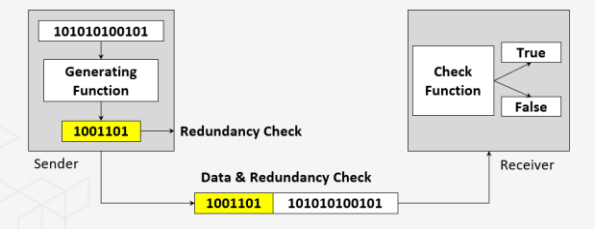
Multiple Bits Error
- Data Unit is received with more than one bits in corrupted state.



Burst Error
- 2 or more bits in the data unit have changed.

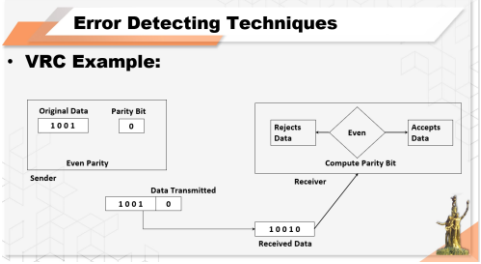


Error Detection – the detection of errors caused by noise or other impairments during transmission from the transmitter to receiver.



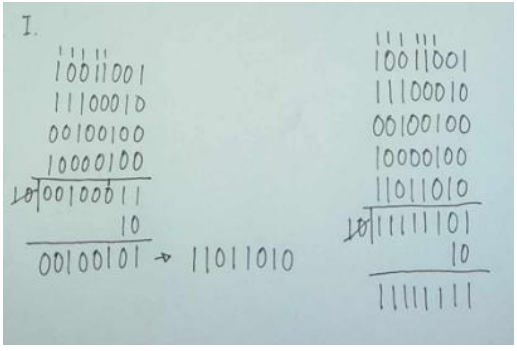
Vertical Redundancy Check (Parity Check)

- VRC is the simplest technique and inexpensive to detect the errors.
- A single bit error is detected by VRC.



Checksum – is generated at the sender's side.

Ex:
10011001 11100010 00100100 10000100



Lect. 6 - Network Devices

Network Devices are the devices that interconnect networks.

• These devices are also known as **connectivity devices**, because they connect network entities.

• These physical devices are required for communication and interaction between hardware on a computer network.

Repeater operates at the **physical layer**. Its job is to regenerate the signal over the same network before the signal becomes too weak or corrupted so as to extend the length to which the signal can be transmitted over the same network.

• A repeater **copies the signal bit by bit and regenerate it at the original strength.**

A **hub** is a multiport repeater. Hubs are devices to link several computers together.

• **A hub has no intelligence** – it sends all data received on any port to all the other ports. It means every devices connected through a hub will receive everything that the other devices send, whether or not it was meant for them. This process is called **broadcasting.**

Types of Hub:

- **Active Hub** – these are hubs which have their own power supply and can clean, boost, and relay the signal along with the network. It serves both as a repeater as well as wiring center. These are **used to extend the maximum distance between nodes.**

- **Passive Hub** – these are the hubs which collect wiring from nodes and power supply from active hub. These hubs **relay signals onto the network without cleaning and boosting them and can't be used to extend the distance between nodes.**

- **Intelligent Hub** - It work like **active hubs and include remote management capabilities.** They also provide flexible data rates to network devices. It also enables an administrator to monitor the traffic passing through the hub and to configure each port in the hub.

Bridge

• A network device that connects two similar network segments together. The primary function of a bridge is **to keep traffic separated on both side of the bridge.**

Switch

• A switch is a **multiport bridge** with a buffer and a design that can boost its efficiency and performance.
• Switches read the source and destination MAC addresses in the frames and therefore **can keep track of who is where, and who is talking to whom, and send data only where it needs to go.**

Routers

• A router is a device like a switch that routes data packets based on their IP Addresses.
• Routers **allow devices on different LANs to communicate with each other and with distant devices.** For example, devices that is connected through the Internet.

Routing is the process of forwarding the packets from source to the destination.

Routing Protocol is a routing that provides the best path from the source to the destination. The best path that has the least-cost path from source to the destination.

Classification of Routing Algorithm:

- **Adaptive Routing Algorithm**
    - An adaptive routing algorithm is also known as **dynamic routing algorithm**.
    - This algorithm makes the routing decisions **based on the topology and network traffic.**
- **Non-Adaptive Routing Algorithm**
    - Non Adaptive routing algorithm is also known as a **static routing algorithm**.
    - When booting up the network, the routing information stores to the routers.
    - Non-Adaptive routing algorithms **do not take the routing decision based on the network topology or network traffic.**

Classification of Adaptive Routing Algorithm:

1. **Centralized Algorithm**
    - It is also known as **global routing algorithm** as it computes the least-cost path between source and destination by using complete and global knowledge about the network.
    - a centralized algorithm is like having one person or entity in charge of making decisions for a group. It's a way of organizing tasks or solving problems where all the information and decision-making power are concentrated in a single location or authority.
2. **Isolation Algorithm**
    - it is an algorithm that obtains the routing information by using local information rather than gathering information from other nodes.
3. **Distributed Algorithm**
    - It is also known as **decentralized algorithm** as it computes the least-cost path between source and destination in an iterative and distributed manner.
    - A distributed algorithm is like organizing a group of individuals (nodes or computers) to work together on a task. They communicate, divide the work, and often have strategies to handle challenges, making them resilient and effective in solving problems in a collaborative way.

Classification of Non-Adaptive Routing Algorithms:

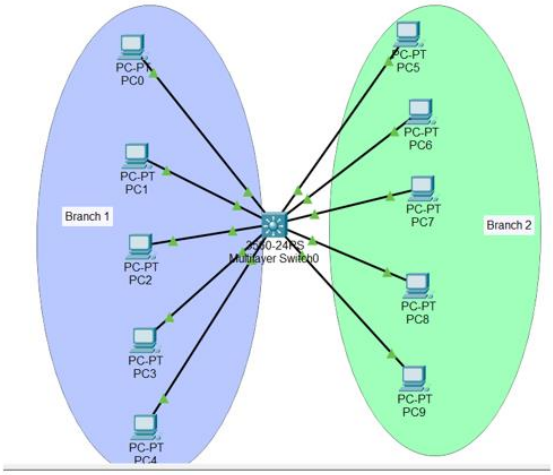
Flooding

- refers to a communication or broadcasting technique where data is sent from one node in a network to all other nodes.

Random walks

- means incorporating randomness into the algorithm's decisions, allowing it to explore different possibilities or paths while still operating within the constraints of a predefined plan.

Laboratory 5: VLAN connection



Topology:

- Layer 3 Switch (e.g., Cisco 3560 or similar)
- PCs 1 to 5 - Connected to VLAN 10 (Branch 1)
- PCs 6 to 10 - Connected to VLAN 20 (Branch 2)

Instructions:

1. **Create VLANs on the Layer 3 switch:**
    - Click on the switch and enter CLI.

Switch> enable
Switch# configure terminal
Switch(config)# vlan 10
Switch(config-vlan)# name Branch1
Switch(config-vlan)# exit

Switch(config)# vlan 20
Switch(config-vlan)# name Branch2
Switch(config-vlan)# exit

2. **Assign ports to VLANs.** Assign the ports connecting to PCs in Branch 1 to VLAN 10 and ports connecting to PCs in Branch 2 to VLAN 20.

Switch(config)# interface range fa0/1 - 5
Switch(config-if- range)# switchport mode access
Switch(config-if- range)# switchport access vlan 10
Switch(config-if-range)# exit

Switch(config)# interface range fa0/6 - 10
Switch (config-if-range)# switchport mode access
Switch(config-if-range)# switchport access vlan 20
Switch(config-if-range)# exit

3. **Enable ip routing on the switch**

Switch(config)# ip routing

4. **Create virtual interfaces (SVIs) for each VLAN and assign IP addresses to them.**

Switch(config)# interface vlan 10
Switch(config-if)# ip address 192.168.1.1 255.255.255.0

Switch(config-if)# no shutdown
Switch(config-if)# exit

Switch(config)# interface vlan 20
Switch(config-if)# ip address 192.168.2.1 255.255.255.0

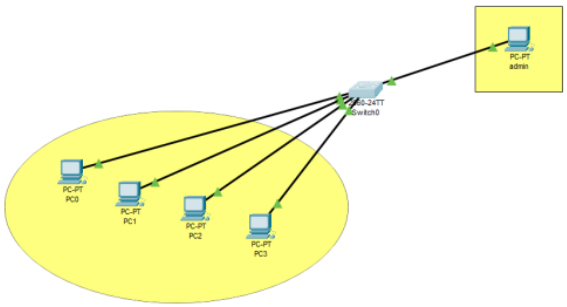
Switch(config-if)# no shutdown
Switch(config-if)# exit

5. **Assign IP Addresses to PCs:**
    - Click on each PC, go to the "Desktop" tab, and assign IP addresses according to the VLANs.
        - PCs in Branch 1 (PC1 to PC5): IP addresses in the range of 192.168.1.2 to 192.168.1.6 with a subnet mask of 255.255.255.0.
        - PCs in Branch 2 (PC6 to PC10): IP addresses in the range of 192.168.2.2 to 192.168.2.6 with a subnet mask of 255.255.255.0.

6. **Test Connectivity:** Try pinging between PCs in the same branch. For example, from PC1, ping PC2, PC3, PC4, and PC5. You should be able to ping successfully. Repeat the process for PCs in Branch 2 (PC6 to PC10).

By using a Layer 3 switch and configuring IP routing on the switch itself, you can achieve inter-VLAN communication without the need for an external router. This provides isolation between Branch 1 and Branch 2.

Laboratory #5: Cisco IOS Basic Network and Security Configuration



Topology:

- 4 pcs for user
- 1 pc name it admin
- 1 switch 2960-24tt

Instructions:

• In CLI, Create local username and password (username is your surname and password is 123)

• Assign IP address on switch using vlan. (Switch-192.168.1.1)

• Configure virtual connection / VTY 0 15

• Set IP address on admin PC – 192.168.1.2, you don't need to set IP addresses on the user PCs.

• Access Telnet on Admin PC, (telnet the address set on the switch) configure terminal and shutdown PC2 and PC0.

Guide:

- What is telnet - Telnet is a network protocol used for remote access to network devices, such as routers and switches.
- Telnet allows a user to connect to a device over a network and access its command-line interface (CLI) for configuration and management purposes.
- Why do we need to set a password? – To access the executive mode so an admin pc can use the CLI features.

Setting up VLAN connection in switch:

We assign an IP address to the VLAN interface of the switch so that we can Telnet the switch from the pc using this address.

```
Switch(config)#interface vlan 1
Switch(config-if)#ip address 192.168.1.1 255.255.255.0
Switch(config-if)#no shutdown
Switch(config-if)#exit
```

Setting up password:

```
Switch(config)#username cisco password password123
Switch(config)#
```

Configure virtual connection /VTY 0 15:

This password is configured on VTY lines. VTY means Virtual Terminal. Before you can manage the switch remotely via Telnet, you'll have to provide this password. We can establish up to 16 telnet connections to the switch at the same time. That's what '0 15' means.

```
Switch(config)#line vty 0 15
Switch(config-line)#login local
Switch(config-line)#exit
```

Shutting down PC via the admin:

Now that we can access the admin PC we can do so as shutting down even the PC that is connected to network. To do this, just state the interface of the PC you want to shutdown and then shutdown. To open it again just type no shutdown.

Switch(config-if)#interface fastethernet 0/3
Switch(config-if)#shutdown

NOTE:

When you type 'enable' in the admin pc and says no password set. Just go to CLI in the switch and type enable password "your chosen set password".