

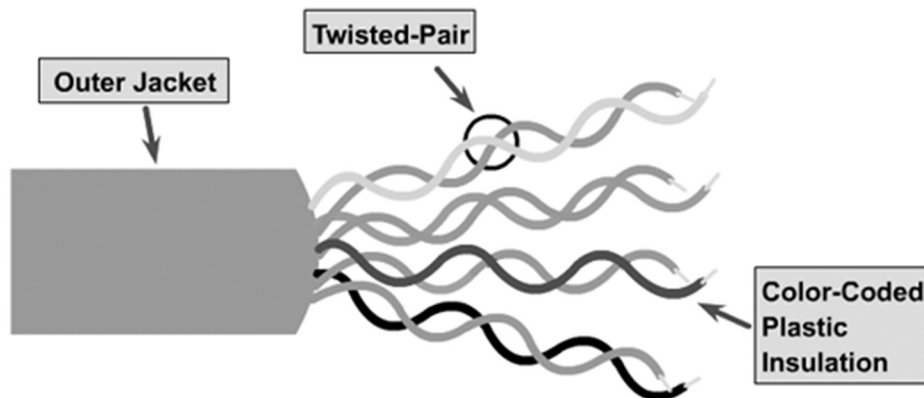
Experiment 1

Aim: To study different types of network cables and practically implement the cross wired cable and straight through cable using clamping tool.

Apparatus: RJ 45 connector, clamping tool, twisted pair cable.

Theory:

Twisted pair cables represent a prevalent category of electrical cables with versatile applications, mainly in telecommunications and networking. These cables are constructed by pairing insulated copper wires and subsequently twisting them together. The act of twisting is a critical design feature aimed at minimizing the negative impacts of electromagnetic interference (EMI) and crosstalk on signal quality, a factor of paramount importance in ensuring the efficient transmission



of data.

Two primary categories of twisted pair cables exist:

1. Unshielded Twisted Pair (UTP):

- Common Usage: UTP cables find widespread application in networking, serving as the go-to choice for Ethernet and telephone connections.

- Shielding: Remarkably, UTP cables lack additional shielding measures against interference; instead, they rely on their inherent twisted pair structure to mitigate electromagnetic interference (EMI).

- Variety: UTP cables are available in multiple categories, encompassing Cat 5e, Cat 6, Cat 6a, Cat 7, and Cat 8, each category tailored to specific requirements concerning data transmission speed and



bandwidth capacity.

Shielded Twisted Pair (STP) cables are distinguished by their additional layer of shielding, typically composed of metal foil or braided wire mesh, which complements the inherent twisted pair design. This shielding plays a vital role in countering electromagnetic interference (EMI), rendering STP cables particularly apt for environments teeming with interference or where **electromagnetic compatibility (EMC)**

stands as a critical concern. They are a prevalent choice in industrial settings and select specialized networking applications.

Twisted pair cables, broadly used to interconnect computers, telephones, and various devices within residences, offices, and data centers, offer flexibility and adaptability. The choice between **Unshielded Twisted Pair (UTP)** and STP hinges upon the unique demands of the application and the extent of EMI pervading the environment.

Regarding network cables, they serve as the conduits for data transmission within **Local Area Networks (LANs)** and for establishing wired internet connections. These cables facilitate the seamless exchange of data, encompassing internet traffic, among a spectrum of devices like computers, routers, switches, and printers. Diverse types and categories of network cables exist, each tailored to distinct characteristics and use cases.

Ethernet Cable (RJ-45):

Ethernet cables represent the predominant type in networking. They employ RJ-45 connectors, the industry-standard for Ethernet connections. These cables exist in various categories, including Cat 5e, Cat 6, Cat 6a, Cat 7, and Cat 8, each endowed with distinct data transmission speeds and capabilities.

Coaxial Cable (Coax):

Coaxial cables, often affiliated with cable television (CATV) and some legacy broadband internet setups, consist of a central conductor encased in insulating material, enveloped by a metallic shield, and further insulated externally.

The selection of the appropriate network cable hinges on multifaceted considerations, including the network's speed requisites, the distance amid devices, and the specific networking apparatus in use. While Ethernet cables (e.g., Cat 5e and Cat 6) are frequently preferred for high-speed LAN connections within homes and offices, fiber optic cables may take precedence in scenarios necessitating extended distances and immunity to electrical interference.

Crucially, prioritizing the selection of the suitable cable ensures the reliable and efficient transmission of data within the network, underlining the pivotal role of these cables in modern communication and connectivity.

Fiber Optic Cable: Fiber optic cables employ strands of either glass or plastic fibers to transmit data via light signals. Renowned for their high-speed data transmission capabilities, these cables are a staple in long-distance and high-bandwidth applications, notably serving as the backbone of the internet and in data centers.

USB Cable: Universal Serial Bus (USB) cables serve as the linchpin for connecting a diverse array of devices, spanning from computers and printers to external storage peripherals. Although not conventionally employed for Local Area Network (LAN) connections, USB cables are indispensable for interfacing with and integrating peripherals into computers and other devices.

The judicious selection of a network cable hinges on a multitude of factors, encompassing the network's speed requisites, the spatial separation between devices, and the specific network equipment in deployment. For instance, Ethernet cables (e.g., Cat 5e, Cat 6, etc.) are the go-to choice for furnishing high-speed LAN connections within homes and offices. Conversely, situations demanding extended distances or those fraught with concerns about electrical interference may propel fiber optic cables to the forefront.

The precision of your network cable choice is paramount, as it determines the reliability and efficacy of data transmission within your network, underscoring the pivotal role these cables play in modern communication and connectivity.

Regarding Cat5 and Cat6, these categories of twisted pair Ethernet cables serve as stalwarts in the realm of networking. They proffer distinct attributes and capacities, with Cat6 generally outshining Cat5 in performance. To illustrate the differentiation:

Cat5 Cable:

- **Category:** Cat5 is an earlier standard, sometimes referred to as Cat5e (Cat5 Enhanced), representing an improved iteration of the original Cat5 cable.
- **Maximum Data Rate:** Cat5e can sustain data rates of up to 1000 Mbps (1 Gbps) with a maximum bandwidth of 100 MHz.
- **Typical Use:** Cat5e cables are well-suited for most home and small office networking needs, adept at linking computers, printers, and assorted devices to a network.
- **Crosstalk:** Cat5e cables offer modest crosstalk resistance, contributing to signal integrity.

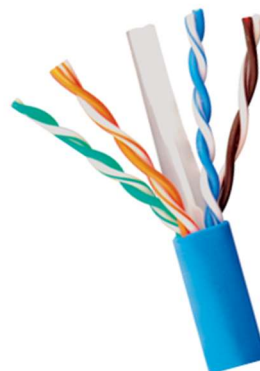
Cat6 Cable:

- **Category:** Cat6 is a later standard architected to deliver enhanced performance and higher data rates relative to Cat5e.
- **Maximum Data Rate:** Cat6 can facilitate data rates of up to 10 Gbps, accompanied by a maximum bandwidth of 250 MHz.
- **Typical Use:** Cat6 cables find common application in more extensive and demanding networking environments, such as data centers and business installations necessitating high-speed data transfer.
- **Crosstalk:** Cat6 cables are meticulously crafted with stringent specifications that minimize crosstalk, affording superior performance, especially in environments rife with interference.

Cat-5



Cat-6



In sum, the choice between Cat5e and Cat6 cables should be appraised in light of your particular networking requirements, budget considerations, and the devices that will be interconnected. In many instances, Cat5e cables suffice for standard home and small office setups, while Cat6 cables shine in demanding contexts or when preparing for potential network upgrades.

Cat5 Cable:

Category: Cat5 is an older standard and is sometimes referred to as Cat5e (Cat5 Enhanced), which is an improved version of the original Cat5 cable.

Maximum Data Rate: Cat5e can support data rates up to 1000 Mbps (1 Gbps) with a maximum bandwidth of 100 MHz.

Typical Use: Cat5e cables are suitable for most home and small office networking needs. They work well for connecting computers, printers, and other devices to a network.

Crosstalk: Cat5e cables have some resistance to crosstalk (interference between adjacent wires), which helps maintain signal integrity.

Cat6 Cable:

Category: Cat6 is a more recent standard designed to provide improved performance and higher data rates compared to Cat5e.

Maximum Data Rate: Cat6 can support data rates up to 10 Gbps with a maximum bandwidth of 250 MHz.

Typical Use: Cat6 cables are commonly used in larger and more demanding network environments, such as data centers, businesses, and installations where high-speed data transmission is crucial.

Crosstalk: Cat6 cables are engineered with stricter specifications for reduced crosstalk, offering better performance in environments with higher levels of interference.

Key Differences:

1.	Cat6 for High-Speed Applications: <ul style="list-style-type: none">Cat6 cables are engineered to handle higher data transmission rates, making them optimal for bandwidth-intensive applications such as high-definition video streaming, large file transfers, and online gaming. Their capability to sustain 10 Gbps speeds over short distances ensures smooth data flow in demanding scenarios.
2.	Improved Interference Resistance: <ul style="list-style-type: none">Cat6 cables exhibit superior resistance to electromagnetic interference (EMI) and crosstalk, which enhances signal quality and reliability, especially at higher data rates. This makes them ideal for environments where interference is a concern.
3.	Cost-Effective Cat5e for Standard Needs: <ul style="list-style-type: none">Cat5e cables offer a cost-effective solution for basic home and small office networking requirements. They can capably support most everyday tasks like web browsing, email, and general data transfer, making them suitable for standard usage.
4.	Consider Specific Needs and Budget: <ul style="list-style-type: none">When selecting between Cat5e and Cat6 cables, it's essential to evaluate your specific networking needs, budget constraints, and the equipment you plan to connect. Cat6 provides the headroom for future network growth and performance demands but may involve a higher upfront cost.
5.	Future-Proofing with Cat6: <ul style="list-style-type: none">Opting for Cat6 cables can be a strategic choice for future-proofing your network. As technology advances and network demands increase, having Cat6 infrastructure in place can save you from the need for cable upgrades down the line.

Ultimately, the choice between Cat5e and Cat6 cables hinges on a balance between current requirements and potential future needs. While Cat5e suffices for many standard applications, Cat6 offers the assurance of robust performance in more demanding scenarios and can serve as an investment in the long-term stability and speed of your network.

Clamping tool (crimping tool):

This is a tool used to attach connectors to the ends of network cables. It typically has a mechanism that allows it to strip the outer insulation of the cable and crimp the connector onto the exposed wires, creating a secure connection. Clamping tools are essential for creating custom Ethernet cables and terminating the ends of network cables with RJ-45 connectors.



Using a clamping tool properly depends on the type of clamp you are working with and the specific task at hand. Here are some general steps on how to use a common C-clamp as an example:

Materials you'll need:

- **C-clamp**
- **Work piece (the item you want to clamp)**
- **Surface (a stable platform or workbench to attach the clamp to)**

Steps:

Using a C-Clamp:

1. Select the Right C-Clamp:

- Begin by selecting a C-clamp that matches the size and weight of your workpiece and is appropriate for the available workspace.

2. Prepare the Workpiece:

- Position your workpiece on the work surface in the desired location. Ensure it is aligned correctly and securely before proceeding.

3. Position the C-Clamp:

- Place the C-clamp over the workpiece in the desired location. The fixed jaw of the clamp should be on one side of the workpiece, and the movable jaw should be on the opposite side.

4. Adjust the Movable Jaw:

- Rotate the threaded screw handle on the movable jaw (the open end of the C-clamp) clockwise to move the movable jaw toward the workpiece. Ensure that the jaw is centered and aligned with the workpiece.

5. Apply Adequate Pressure:

- Continue turning the screw handle clockwise until the movable jaw makes contact with the workpiece. Apply enough pressure to securely hold the workpiece in place. You can use your hand or a wrench to turn the handle, depending on the clamp's size and the pressure required.

6. Verify Alignment:

- Ensure that the workpiece is correctly aligned and positioned as needed. Make any necessary adjustments to achieve the desired alignment.

7. Tighten the Clamp:

- Keep turning the screw handle clockwise until the clamp securely holds the workpiece. Be cautious not to over-tighten, as excessive pressure can damage either the workpiece or the clamp.

8. Perform Your Task:

- With the workpiece securely clamped in place, you can now proceed with your intended task, such as cutting, drilling, sanding, welding, or assembly.

9. Release the Clamp:

- Once your task is completed or if you need to reposition the workpiece, loosen the clamp by turning the screw handle counterclockwise. You can use your hand or a wrench for this purpose.

10. Remove the Clamp:

- After sufficiently loosening the clamp, lift it away from the workpiece and the work surface.

11. Store and Maintain the Clamp:

- Return the C-clamp to its storage location, if applicable, and ensure it is well-maintained for future use.

Remember that various types of clamps exist, and specific instructions may vary depending on the type. Always adhere to the manufacturer's guidelines for the specific clamp you are using, and prioritize safety by wearing appropriate protective gear when necessary for the task at hand.

Terminating RJ-45 Connectors:

1. Prepare the Cable:

- Begin by stripping off approximately 2 inches of the plastic jacket from the end of the network cable. Be extremely careful during this step to avoid damaging the wires inside, as this could compromise the cable's performance.

2. Maintain Twisted Pairs:

- Carefully spread apart the cable's wires while ensuring that you hold onto the base of the jacket with your other hand. Avoid letting the wires become untwisted beyond the recommended limits.

3. Arrange Wires for Termination:

- Depending on the type of cable you are creating (straight-through or crossover), arrange the wires inside the cable according to the correct wiring pattern for your specific cable type.
4. **Insert Wires into RJ-45 Connector:**
 - Gently insert the correctly arranged wires into the RJ-45 connector, ensuring each wire reaches the end of the connector and aligns with the respective pin slots. Double-check the alignment and make any necessary adjustments for proper placement.
 5. **Crimp the Connector:**
 - Place the connector into the appropriate slot on the crimping tool, ensuring it is fully seated.
 6. **Secure the Connector:**
 - Squeeze the crimping tool's handle firmly to secure the connector onto the wires. This typically involves crimping down the connector's pins onto the wires, creating a stable connection. Ensure the connector is securely attached.
 7. **Testing (Optional but Recommended):**
 - To verify proper termination and functionality, consider using a cable tester to check for continuity and correct wiring. This step helps identify any wiring errors or connectivity issues that may require correction.
 8. **Label or Mark the Cable (Optional):**
 - For organizational purposes, you can label or mark the cable ends for easy identification, especially if you are working with multiple cables.
 9. **Practice Good Cable Management:**
 - Implement proper cable management practices by securing the cable along its route, avoiding sharp bends or kinks, and using cable ties or clips to keep it organized and tidy.
 10. **Finalize and Use:**
 - Once you have successfully terminated both ends of the cable and, if applicable, tested it, you can use the cable for your network connections, whether it's connecting computers, routers, switches, or other networking devices.

Procedure:

1. To do these practical following steps should be done. 1. Start by stripping off about 2 inches of the plastic jacket off the end of the cable. Be very careful at this point, as to not nick or cut into the wires, which are inside. Doing so could alter the characteristics of your cable, or even worse render is useless. Check the wires, one more time for nicks or cuts. If there are any, just whack the whole end off, and start over.

2. Spread the wires apart, but be sure to hold onto the base of the jacket with your other hand. You do not want the wires to become untwisted down inside the jacket. Category 5 cable must only have 1/2 of an inch of 'untwisted' wire at the end; otherwise it will be 'out of spec'. At this point, you obviously have ALOT more than 1/2 of an inch of un-twisted wire.

3. You have 2 end jacks, which must be installed on your cable. If you are using a pre-made cable, with one of the ends whacked off, you only have one end to install - the crossed over end. Below are two diagrams, which show how you need to arrange the cables for each type of cable end. Decide at this point which end you are making and examine the associated picture below.

Diagram shows you how connection PC to prepare straight through wired

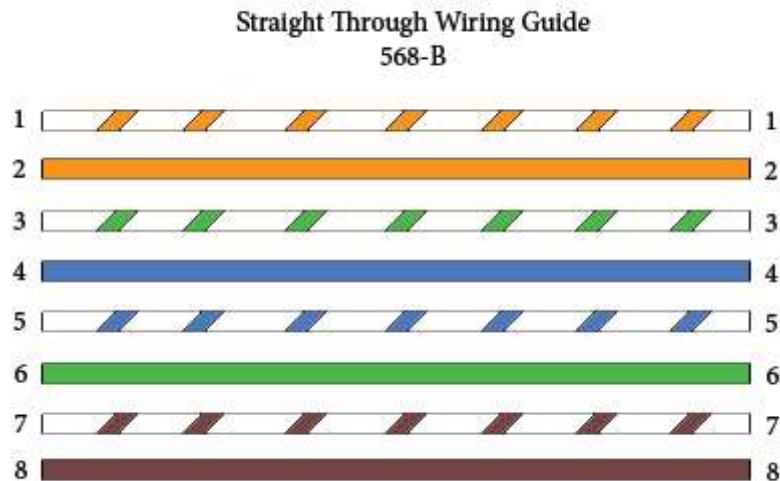
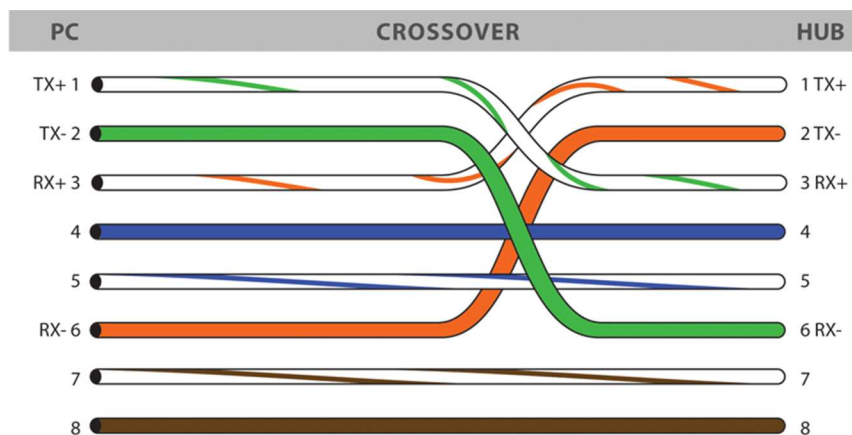


Diagram shows you how connection PC to prepare straight through wired



▪ Ethernet Cable Tips:

- A straight-thru cable has identical ends.
- A crossover cable has different ends. A straight-thru is used as a patch cord in Ethernet connections.
- A crossover is used to connect two Ethernet devices without a hub or for connecting two hubs. A crossover has one end with the Orange set of wires switched with the Green set.
- Odd numbered pins are always striped; even numbered pins are always solid coloured.
- Looking at the RJ-45 with the clip facing away from you, Brown is always on the right, and pin 1 is on the left.
- No more than 1/2" of the Ethernet cable should be untwisted

- A crossover has one end with the Orange set of wires switched otherwise it will be susceptible to crosstalk.
- Do not deform, do not bend, do not stretch, do not staple, do not run parallel with power cables, and do not run Ethernet cables near noise inducing components.

Experiment 2

Aim: To study different Network Devices like Hub, Bridge, Switch, Router, Repeater, Gateways etc. in Detail.

Hub – A hub, in the context of networking, refers to a basic network device that connects multiple devices in a local area network (LAN). It operates at the physical layer (Layer 1) of the OSI model and is primarily used for the purpose of signal amplification and signal distribution. Hubs are considered outdated and have largely been replaced by more advanced networking equipment like switches.

Here are some key characteristics and limitations of hubs:

1. **Signal Amplification:** Hubs regenerate and broadcast incoming data packets to all connected devices. This means that when a data packet arrives at a hub, it is amplified and sent to all connected devices, regardless of the intended recipient.
2. **Collision Domain:** Hubs create a single collision domain, which means that all devices connected to the hub share the same network segment. This can lead to network congestion and collisions, especially in larger networks.
3. **Broadcasting:** Hubs rely on broadcasting to send data to all devices in the network. This broadcasting approach can lead to inefficiencies as all devices receive the data, even if it's intended for just one.
4. **No Intelligence:** Hubs lack intelligence and do not have the ability to make forwarding decisions based on MAC addresses. They lack the sophistication of more advanced networking devices like switches.
5. **Limited Scalability:** Due to their limitations, hubs are not suitable for larger or more complex networks. They are best suited for small, simple networks with minimal traffic.
6. **Obsolete Technology:** Hubs have become obsolete in modern networking environments. They have been largely replaced by network switches, which provide better performance, improved security, and the ability to create separate collision domains.

In summary, a hub is a basic networking device that connects multiple devices in a network. However, due to its limitations, including broadcasting and creating a single collision domain, hubs are not recommended for modern network setups. Instead, network switches are the preferred choice as they offer better performance and efficiency.

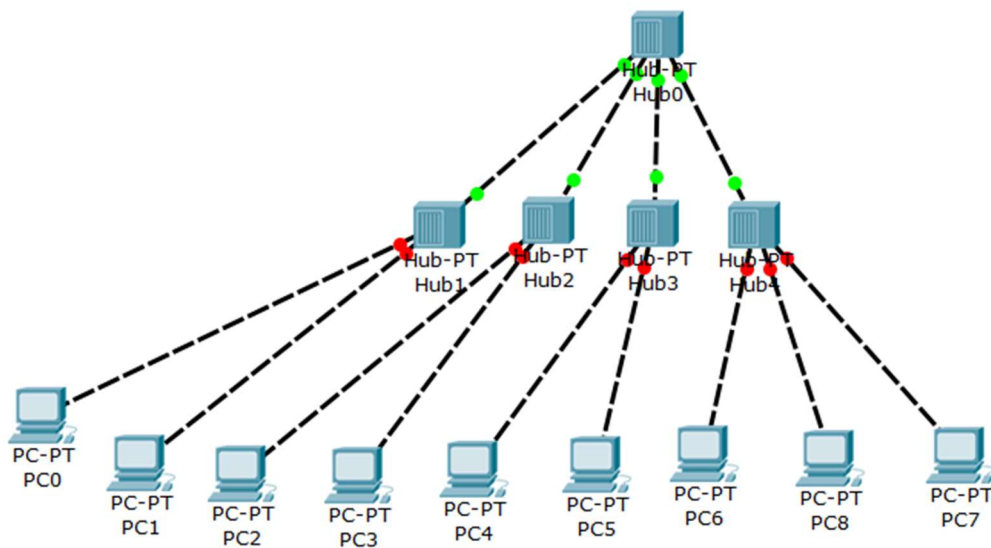
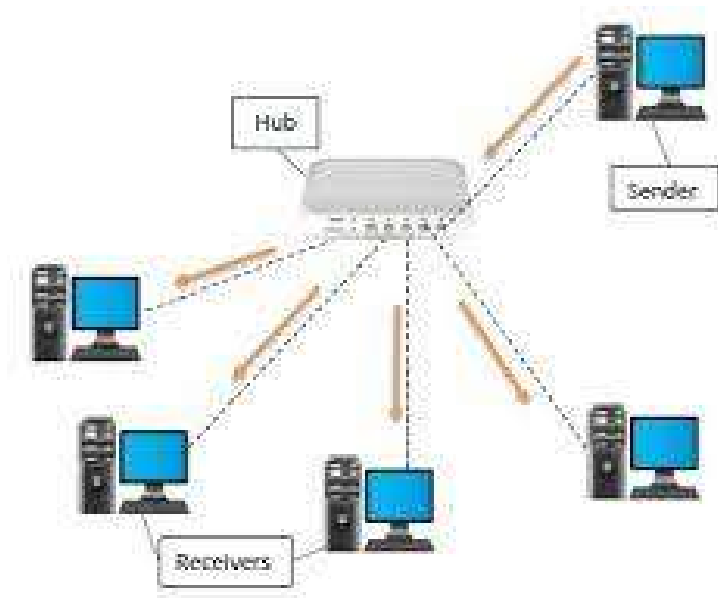


Figure Hub as a multi-port repeater can be connected in a hierarchical manner to form a single LAN with many nodes.

Bridge –

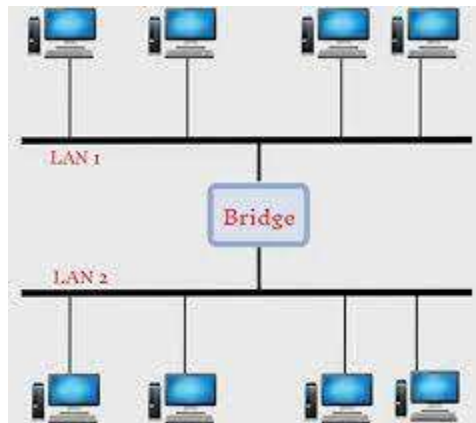
A bridge, in networking, is a device that operates at the data link layer (Layer 2) of the OSI model and is used to connect and filter traffic between two or more network segments, effectively creating a single logical network. Bridges are designed to enhance network performance, security, and segmentation.

Key functions of a bridge include:

1. **Segmentation:** Bridges divide a larger network into smaller segments, reducing collision domains and enhancing overall network efficiency. Each segment operates as a separate collision domain, reducing the chances of network collisions.
2. **Filtering:** Bridges can filter traffic based on Media Access Control (MAC) addresses. By examining the source and destination MAC addresses in data frames, bridges determine whether to forward or discard a frame, which improves network security and bandwidth utilization.
3. **Traffic Isolation:** Bridges help isolate traffic, preventing broadcast storms and other network issues from affecting the entire network. This enhances network reliability and stability.

4. **Extending Network Reach:** Wireless bridges enable the extension of network connectivity over long distances without the need for physical cables.
5. **Security:** Bridges can be configured to enhance network security by controlling which devices are allowed to communicate across network segments.

In modern networks, bridges are often implemented as a feature within more advanced networking devices such as switches and routers. However, they remain valuable tools for optimizing network performance and security in certain situations, such as connecting different network technologies or extending network reach.



Router -

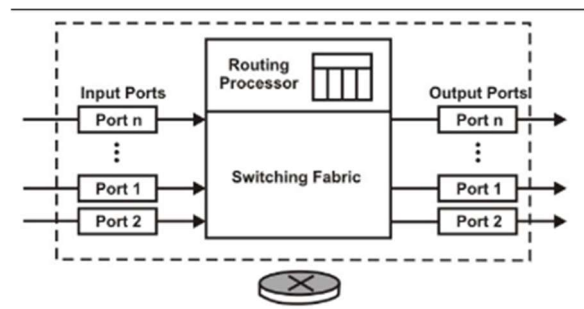
A router is a networking device that operates at the network layer (Layer 3) of the OSI model. Its primary function is to forward data packets between different networks, making routing decisions based on network addresses, typically IP addresses. Routers are key components of modern networking and are used to connect different networks, including local area networks (LANs) and wide area networks (WANs), and to facilitate data communication between devices.

Now, let's briefly explain the routing protocols you mentioned:

1. **IS-IS (Intermediate System to Intermediate System):** IS-IS is a link-state routing protocol used primarily in larger and more complex networks, including internet service provider (ISP) networks. It operates at the network layer and is capable of routing both IP and non-IP protocols. IS-IS uses a hierarchical structure and is often used in conjunction with IPv4 and IPv6 to enable efficient routing.
2. **IPX (Internetwork Packet Exchange):** IPX was a network layer protocol primarily used in Novell NetWare networks. It was designed for communication in early local area networks (LANs) and provided services like addressing and routing for NetWare devices. However, IPX has largely been replaced by IP (Internet Protocol) in modern networks.
3. **NLSP (NetWare Link Services Protocol):** NLSP is a routing protocol associated with Novell NetWare networks. It was used to exchange routing information in IPX-based networks, similar to how OSPF and IS-IS function in IP networks. Like IPX, NLSP has become less relevant as IP has become the dominant networking protocol.
4. **RIP (Routing Information Protocol):** RIP is one of the oldest and simplest routing protocols used for routing IP packets. It falls into the category of distance-vector routing protocols and is used primarily in small to medium-sized networks. RIP routers exchange routing information, and RIP's algorithm calculates the best paths based on hop count. RIP has limited scalability and is less suitable for larger and more complex networks compared to modern routing protocols like OSPF and BGP.

In summary, routers are networking devices that forward data packets between different networks, while the mentioned routing protocols (IS-IS, IPX, NLSP, and RIP) are specific protocols used for routing and

managing network traffic in different types of networks. Some of these protocols, like IS-IS and RIP, are still in use, while others, like IPX and NLSP, have become obsolete in favor of modern IP-based networking.



Schematic Diagram Of Router

Switch-

A switch is a networking device that operates at the data link layer (Layer 2) of the OSI (Open Systems Interconnection) model. Its primary function is to connect devices within a local area network (LAN) and forward data frames between them based on their Media Access Control (MAC) addresses. Switches are essential for creating efficient and scalable network infrastructures.

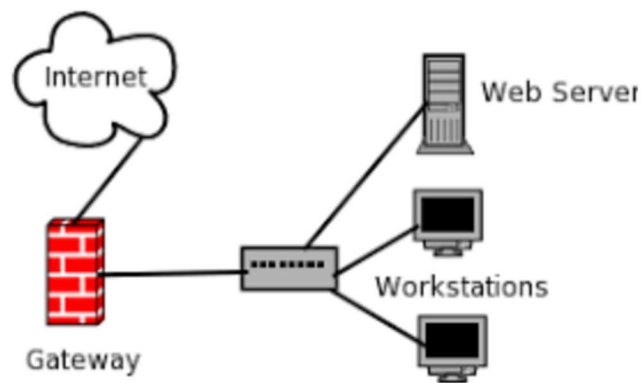
Here are the common types of switches:

1. **Ethernet Switch:** Ethernet switches are the most common type of network switches. They are used to connect devices like computers, printers, servers, and other Ethernet-enabled devices within a LAN. Ethernet switches operate at different speeds, including 10/100/1000/10000 Mbps (megabits per second), depending on the network's requirements.
2. **Managed Switch:** Managed switches provide administrators with greater control and configurability over their network. They allow for features like VLAN (Virtual LAN) support, Quality of Service (QoS) configuration, security settings, and remote management. Managed switches are commonly used in medium to large-sized networks.
3. **Unmanaged Switch:** Unmanaged switches are plug-and-play devices that do not offer the same level of configuration options as managed switches. They are typically used in small home or office networks and require minimal setup. Unmanaged switches automatically forward network traffic without any user intervention.
4. **PoE (Power over Ethernet) Switch:** PoE switches provide power to connected devices over Ethernet cables, eliminating the need for separate power sources. They are often used to power devices like IP cameras, VoIP phones, and wireless access points.

Gateway-

A gateway is a network device or software component that serves as a bridge or interface between different networks, protocols, or communication systems. Its primary function is to facilitate communication and data transfer between networks that use different communication protocols or have different network architectures. Gateways are crucial for enabling interoperability and routing data between networks that would otherwise be incompatible.

Here are some common types of gateways:



1. Unidirectional Gateway:

- A unidirectional gateway allows data to flow in only one direction, typically from a more secure network to a less secure one. It is often used in scenarios where data needs to be transmitted securely without the risk of information flowing back.

2. Bidirectional Gateway:

- A bidirectional gateway allows data to flow in both directions, between two networks or communication systems. It enables communication and data exchange in both directions, unlike a unidirectional gateway.

3. Network Gateway:

- A network gateway, in a general sense, is a device or software component that connects two different networks, facilitating communication between them. It can encompass various types of gateways, including routers and security gateways.

4. Cloud Storage Gateway:

- A cloud storage gateway is a device or software application that connects on-premises data storage systems to cloud-based storage services. It allows organizations to extend their data storage and backup solutions to the cloud.

5. IoT Gateway:

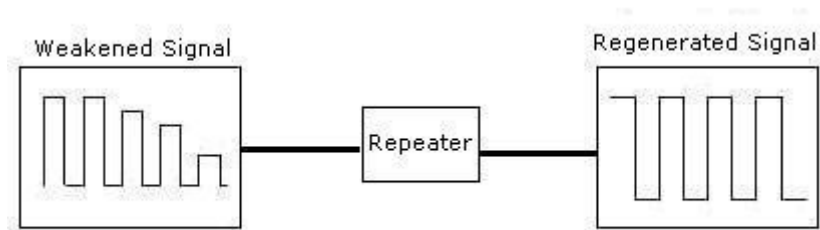
- An IoT gateway connects Internet of Things (IoT) devices to a network, often acting as an intermediary between IoT devices and cloud platforms. It collects, processes, and transmits data from IoT sensors and devices to the cloud for analysis.

6. VoIP Gateway:

- A VoIP gateway (Voice over Internet Protocol gateway) converts traditional analog or digital telephone signals into IP packets and vice versa. It enables the integration of legacy phone systems with IP-based telephony networks.

Repeater-

A basic repeater, often referred to as a signal repeater or simply a repeater, is a device that receives an incoming signal, amplifies it, and retransmits it at the same frequency or within a similar frequency range. Repeaters are commonly used in various communication systems to extend the range of signals, such as in radio and cellular networks.



Types Of Signal Repeater :-

1. Analog Repeater:

- An analog repeater is specifically designed to amplify and retransmit analog signals. It's commonly used in analog communication systems like older radio systems, analog television broadcasting, and some two-way radio systems.

2. Digital Repeater:

- A digital repeater is designed to amplify and retransmit digital signals. It is used in digital communication systems like digital radio, DVB (Digital Video Broadcasting), and digital cellular networks (e.g., 4G and 5G). Digital repeaters can help improve the quality and coverage of digital signals.

3. Wired Repeater:

- A wired repeater, also known as a signal booster or signal amplifier, is used in wired communication systems like Ethernet networks. It receives weak electrical signals, boosts their strength, and retransmits them over wired connections to extend the network's reach.

4. Wireless Repeater:

- A wireless repeater, also called a Wi-Fi repeater or range extender, is used in wireless networks, such as Wi-Fi networks. It receives wireless signals from a router or access point, amplifies them, and retransmits them to cover areas with weak or no wireless coverage, effectively extending the wireless network's range.

EXPERIMENT-3

AIM: To study Network IP Address. Classification of IP Addresses (Classful and Classless) along with Subnetting and Super netting.

NETWORK IP ADDRESS:

An IP address is the identifier that enables your device to send or receive data packets across the internet. It holds information related to your location and therefore making devices available for two-way communication. The internet requires a process to distinguish between different networks, routers, and websites. Therefore, IP addresses provide the mechanism of doing so, and it forms an indispensable part in the working of the internet. You will notice that most of the IP addresses are essentially numerical. Still, as the world is witnessing a colossal growth of network users, the network developers had to add letters and some addresses as internet usage grows. An IP address is represented by a series of numbers segregated by periods(.). They are expressed in the form of four pairs - an example address might be 255.255.255.255 wherein each set can range from 0 to 255. IP addresses are not produced randomly. They are generated mathematically and are further assigned by the IANA (Internet Assigned Numbers Authority), a department of the ICANN. ICANN stands for Internet Corporation for Assigned Names and Numbers. It is a non-profit corporation founded in the US back in 1998 with an aim to manage Internet security and enable it to be available by all.

Classful Addressing

In its initial days, IP addresses use the concept of classful addressing which splits the available address space into five classes A, B, C, D&E. IPv4 addresses are represented using 32-bit addresses. The 32-bit IPv4 address is also referred to as the 4-byte address or 4-octet address. So, we can conclude that the address space of IPv4 is 232 which is equal to 4,294,967,296.



Generally, the IPv4 addresses are expressed using the binary notation or dotted decimal notation or hexadecimal notation. The first few bits of binary notation of IPv4 addresses recognises the class of the address whereas, in dotted-decimal notation of IPv4 address the value of the first byte recognises the class of the address. As you can see the image below, the first byte of each class denotes the range of addresses in each class.

The classful addressing concepts divide the address space into a fixed number of blocks and each block has a fixed number of hosts. In IPv4 addresses of class A, B&C the first part of the address is considered as net-id (Network id) and the second part of the address is called host-id. The size of these parts varies with the classes.

Net-id: The net-id denotes the address of the network.

Host-id: The host-id denotes the address of the host attached to the corresponding network.

In Class A, the net-id is defined by the first byte of the address. and the rest 3 bytes defines the host-id.

In Class B, the first two bytes of the address defines the network address and the rest two bytes defines the host-id.

In Class C the first three bytes defines the network address and the last byte defines the host-id.

Classes of Classful address

Class A

The network id of class A is defined by the first byte of the 32-bit IPv4 address. In class A, the first bit of the net-id stays '0' to define that the IPv4 address belongs to the class A and the other 7 bits of the net-id can be changed to defines different blocks in class A. As the first bit is preserved the remaining seven bits calculate the number of blocks in the class A i.e. $2^7 = 128$ blocks. There are 128 blocks in class A, as the addressing would start from 0 the range of blocks will be from 0-127.

The host-id in class A is defined by the remaining three bytes of the IPv4 address which is equal to 24 bits. So, we can calculate the number of hosts for each block as $2^{24} = 16,777,216$. So, we conclude that we can assign 128 blocks from class A to 128 organisations where each organisation can have 16,777,216 hosts connected to the network.

Now, as we have calculated the number of blocks and the number of addresses in each block of class A. Let us count the total number of addresses in class A which can be calculated as follow: As we have seen above addresses of class A stays '0'. addresses can be changed to Ai.e. $2^{31} = 2,147,483,648$.

Class B

The network id or the net-id of class B is defined using the first two bytes of the IPv4 address. The first two bits of net-id stay '10' to define that the IPv4 address belongs to the class B and the remaining 14 bits of net-id can be changed to calculate the number of blocks in class B. i.e. $2^{14} = 16,384$.

The next two bytes of the IPv4 address denote the host id in class B which is 16 bits. The number of hosts can be calculated as $2^{16} = 65,536$. So, we conclude that we can assign 16,384 blocks from class B to 16,384 organisations where each organisation can have 65,536 hosts connected to the network.

Now, as we have calculated the number of blocks and the number of addresses in each block of class B. Let us count the total number of addresses in class B which can be calculated as follows: As we have seen above the first two bits of the entire 32-bit addresses of class B stay '10' to define the class. The remaining 30 bits of the entire 32-bit addresses can be changed to define the address space of class B. i.e. $2^{30} = 1,073,741,824$.

Class C

In class C the network id is defined by the first 3 bytes of the IPv4 address. The first 3 bits in the network id stay '110' to define the class and the remaining 21 bits define the number of blocks in class C. The number of blocks can be calculated as $2^{21} = 2,097,152$.

The last byte of the IPv4 address in class C defines the host-id. The number of hosts can be calculated as $2^8 = 256$. So, we conclude that we can assign 2,097,152 blocks from class C to 2,097,152 organisations where each organisation can have 256 hosts connected to the network.

Now, as we have calculated the number of blocks and the number of addresses in each block of class C. Let us count the total number of addresses in class C which can be calculated as follows: As we have seen above the first three bits of the entire 32-bit addresses of class C stay '110' to define the class. The remaining 29 bits of the entire 32-bit addresses can be changed to define the address space of class C. i.e. $2^{29} = 536,870,912$.

Class D

Like class A, B&C, class D does not divide IPv4 into net-id and host-id. All the addresses of class D are of one single block. The class D addresses are designed for multicasting. The first four-bit of entire 32-bit addresses of class D stays 1110' to define the class.

The remaining 28 bits from the 32-bit addresses of class D can be changed to define the address space of class D. So, the number of addresses in class D is $2^{28}=2,68,435,456$.

Class E

Like class D, Class E addresses are one block addresses. The addresses in class E are not split into net-id and host-id. The addresses in class E are reserved for future use. The first four bits of entire 32-bit IPv4 addresses of class E stays 1111'. The remaining 28-bit changes to define the number of addresses in class E i.e. $2^{28}=2,68,435,456$.

Subnetting and Super-netting

To overcome the flaws of classful addressing, these two solutions were introduced to compensate for the wastage of addresses. Let us discuss them one by one.

Subnetting

As class blocks of A&B are too large for any organisation. So, they can divide their large network into smaller subnetworks and share them with other organisations. This whole concept is subnetting.

Super-netting

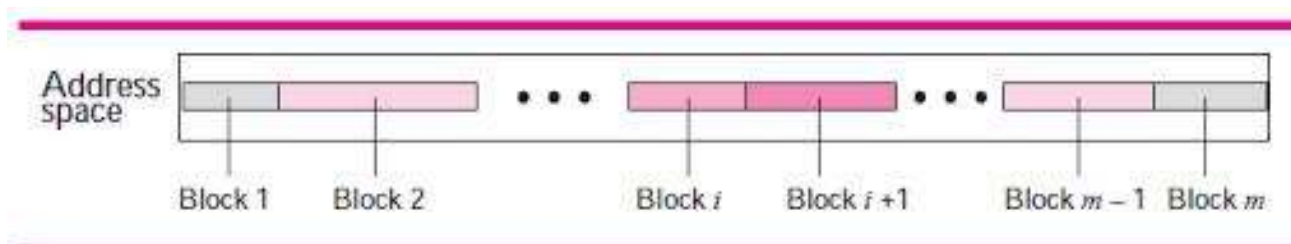
As the blocks in class A and B were almost consumed so, new organisations consider class C. But, the block of class C is too small then the requirement of the organisation. In this case, the solution which came out is super netting which grants to join the blocks of class C to form a larger block which satisfies the address requirement of the organisation.

CLASSLESS ADDRESSING

The address depletion issue was not fully resolved by classful addressing's subnetting and supernetting techniques. As the Internet expanded, it became obvious that a bigger address space was required as a long-term fix. However, the expanded address space necessitates that IP addresses should be longer as well, necessitating a change in IP packet syntax. The short-term solution, which uses the same address space but modifies the distribution of addresses to deliver a fair amount to each business, was developed despite the fact that the long-term solution, known as IPv6, has already been developed. Classless addressing is the temporary fix, which nevertheless makes use of IPv4 addresses. In order to make up for address depletion, the class privilege was taken out of the distribution.

The entire address space is partitioned into blocks of varying lengths with classless addressing. An address's prefix designates the block (network); its suffix designates the node (device). We are capable of having a block of 20, 21, 22, .., 232 addresses, theoretically. One of the limitations is that a block of addresses must have a power of two addresses. One address block may be given to an organisation. The given figure demonstrates the non-overlapping block

segmentation of the entire address space.

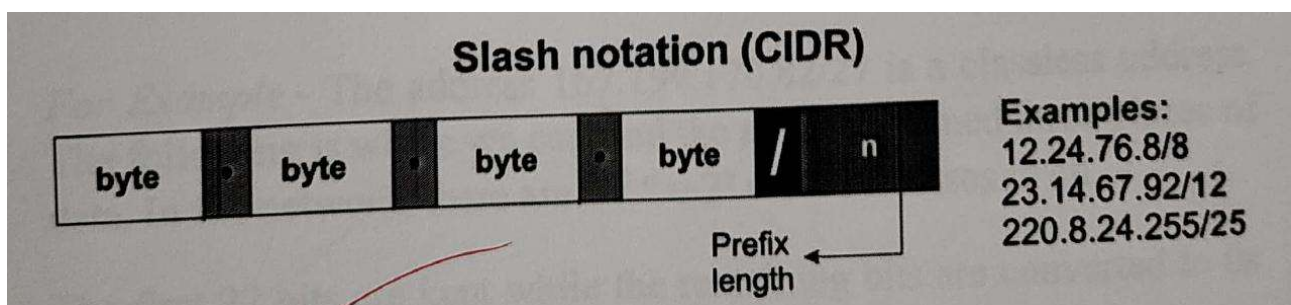


In contrast to classful addressing, classless addressing allows for varying prefix lengths. Prefix lengths that vary from 0 to 32 are possible. The length of the prefix has an inverse relationship with network size. A smaller network has a large prefix; a larger one has a small prefix.

We must stress that classful addressing is just as easily adaptable to the concept of classless addressing. Consider an address in class A as a classless address with a prefix length of 8. Class B addresses can be viewed as classless addresses with the prefix 16 and so on. Putting it another way, classless addressing is a specific instance of classful addressing.

Prefix Length - Slash Notation

In classless addressing, the first issue that needs to be resolved is how to determine the prefix length if an address is provided. We must individually provide the prefix length because it is not a property of the address. The address is inserted in this scenario, followed by a slash, and the prefix length, n . Slash notation is the colloquial name for the notation, while classless inter domain routing, or CIDR (pronounced cider) method, is the official name. An address in classless addressing can thus be expressed as illustrated in the figure below.



To put it in another way, we must also provide the prefix length in classless addressing because an address does not automatically define the block or network to which it belongs.

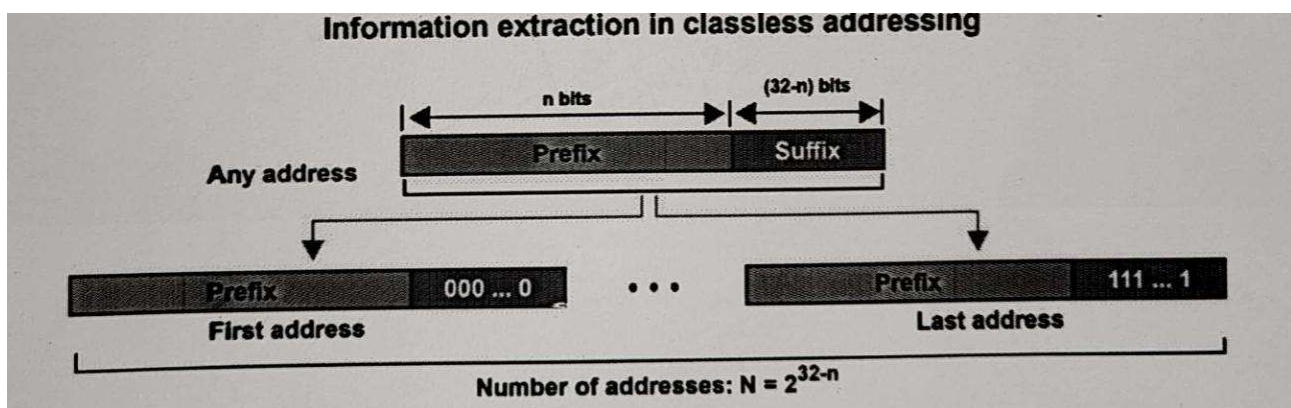
Extracting Information from an Address

With respect to any given address in the block, we typically like to know three things: the number of addresses in the block, the start address in the block, and the last address. These three pieces of information, which are depicted in the picture below, are simple to locate because the prefix length, n , is known.

• •

The block has $N = 2^{32-n}$ addresses, according to the calculation. The n leftmost bits are kept, and the $(32 - n)$ rightmost bits are all set to zeroes to determine the first address.

The n leftmost bits are kept, while the $(32 - n)$ rightmost bits are all set to 1s to determine the last address.



For Example - The address 167.199.170.82/27 is a classless address. The following is where we can find the aforementioned three pieces of data. In the network, there are $2^{32-n} = 2^{32-27} = 2^5 = 32$ addresses in all.

The first 27 bits are kept while the remaining bits are converted to 0s to determine the first address.

Address: 167.199.170.82/27	10100111 11000111
10101010 01010010	
First address: 167.199.170.64/27.	10100111 11000111
10101010 01000000	

Keeping the first 27 bits and turning the remaining bits to 1s will allow you to determine the last address.

Address: 167.199.170.82/27

10100111 11000111

10101010 01011111

Last address: 167.199.170.95/27

10100111 11000111

10101010 01011111

Experiment-4

Study Basic Router Configuration Commands.


Commands:

->User prompt

Router>

->View list of commands that can be entered in user mode

Router>?



The screenshot shows a window titled "Router1" with tabs for "Physical", "Config", and "CLI". The "CLI" tab is active, displaying the "IOS Command Line Interface". The text in the window includes:

```
Rights clause at FAR sec. 52.227-19 and subparagraph
(c) (1) (ii) of the Rights in Technical Data and Computer
Software clause at DFARS sec. 252.227-7013.

    cisco Systems, Inc.
    170 West Tasman Drive
    San Jose, California 95134-1706

Cisco Internetwork Operating System Software
IOS (tm) C2600 Software (C2600-I-M), Version 12.2(28), RELEASE SOFTWARE (fc5)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2005 by cisco Systems, Inc.
Compiled Wed 27-Apr-04 19:01 by miwang

Cisco 2621 (MPC860) processor (revision 0x200) with 253952K/8192K bytes of memory
.
Processor board ID JAD05190MTZ (4292891495)
M860 processor: part number 0, mask 49
Bridging software.
X.25 software, Version 3.0.0.
2 FastEthernet/IEEE 802.3 interface(s)
32K bytes of non-volatile configuration memory.
63488K bytes of ATA CompactFlash (Read/Write)

    --- System Configuration Dialog ---

Continue with configuration dialog? [yes/no]: no

Press RETURN to get started!

Router>?
Exec commands:
<1-99>      Session number to resume
connect     Open a terminal connection
disable     Turn off privileged commands
disconnect  Disconnect an existing network connection
enable      Turn on privileged commands
exit        Exit from the EXEC
logout      Exit from the EXEC
ping        Send echo messages
resume      Resume an active network connection
show        Show running system information
ssh         Open a secure shell client connection
telnet      Open a telnet connection
terminal    Set terminal line parameters
traceroute  Trace route to destination
Router>
```

At the bottom right of the window, there are "Copy" and "Paste" buttons.

->Enter privileged mode

Router>enable

Router#

->View list of commands that can be entered in privileged mode

Router#?


```

Router>enable
Router#configure
Configuring from terminal, memory, or network [terminal]? terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#?
Configure commands:
  aaa                Authentication, Authorization and Accounting.
  access-list        Add an access list entry
  banner             Define a login banner
  boot               Modify system boot parameters
  cdp                Global CDP configuration subcommands
  class-map          Configure Class Map
  clock              Configure time-of-day clock
  config-register     Define the configuration register
  crypto             Encryption module
  do                 To run exec commands in config mode
  enable             Modify enable password parameters
  end                Exit from configure mode
  exit               Exit from configure mode
  hostname           Set system's network name
  interface          Select an interface to configure
  ip                 Global IP configuration subcommands
  key                Key management
  line               Configure a terminal line
  logging            Modify message logging facilities
  no                 Negate a command or set its defaults
  ntp                Configure NTP
  policy-map         Configure QoS Policy Map
  priority-list       Build a priority list
  privilege           Command privilege parameters
  queue-list         Build a custom queue list
  radius-server       Modify Radius query parameters
  router             Enable a routing process
  service            Modify use of network based services
  snmp-server         Modify SNMP engine parameters
  tacacs-server       Modify TACACS query parameters
  username           Establish User Name Authentication
Router(config)#
Router(config)#

```

->Exit privileged mode

Router# disable Router>

->Enter configuration mode

Router>enable

Router# configure terminal

Router>enable

Router(config)#

->Configure Hostname

Router(config)#hostname 2621.1

2621.1(config)#

->View list of valid parameters to be used with enable commands

Configure an enable password of 'dcnlab' that will not be encrypted when viewing the router configuration file

Configuration an enable password of 'it3' that will be encrypted

2621.1(config)#enable?

2621.1(config)#enable passwords 123

2621.1(config)#enable secret 12

->Configure an IP Address for ethernet and activate it

2621.1(config)#interface fastethernet 0/1

2621.1(config-if)# ip address 192.168.1.1 255.255.255.0

2621.1(config-if)#no shut

->Configure an IP Address for a serial interface and activate it

2621.1(config-if)# interface serial 0/1

2621.1(config-if)# ip address 192.168.1.1 255.255.255.0

2621.1(config-if)# no shut

->Exit configuration mode

2621.1(config-if)# ctrl+z

2621.1#

->Exit command-line interface

2621.1#exit

->Prompt for password entry in privileged mode

2621.1>enable

Password: 123

2621.1#

```

    --- System Configuration Dialog ---
Continue with configuration dialog? [yes/no]: no

Press RETURN to get started!

Router>
Router>enable
Router#hostname 2621.1
      ^
% Invalid input detected at '^' marker.

Router#configure terminal
      ^
% Invalid input detected at '^' marker.

Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname 2621.1
2621.1(config)#enable password 123
2621.1(config)#enable secret 12
2621.1(config)#interface fastethernet 0/1
2621.1(config-if)#ip address 192.168.1.1 255.255.255.0
2621.1(config-if)#no shut

2621.1(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up

2621.1(config-if)#interface serial 0/1
%Invalid interface type and number
2621.1(config)#interface serial 0/1
%Invalid interface type and number
2621.1(config)#ip address 1992.168.1.1 255.255.255.0
      ^
% Invalid input detected at '^' marker.

2621.1(config)#no shut
      ^
% Invalid input detected at '^' marker.

2621.1(config)#logout
      ^
% Invalid input detected at '^' marker.

2621.1(config)#exit
2621.1#
%SYS-5-CONFIG_I: Configured from console by console

```

->Summary of interfaces

2621.1# show ip interface brief

->Detailed Interface information

2621.1 #show interfaces

```

2621.1>enable
Password:
Password:
Password:
% Bad secrets

2621.1>show ip interface brief
Interface                IP-Address      OK? Method Status      Protocol

FastEthernet0/0          unassigned      YES unset  administratively down down
FastEthernet0/1          192.168.1.1     YES manual up           down

2621.1>show interfaces
FastEthernet0/0 is administratively down, line protocol is down (disabled)
  Hardware is Lance, address is 000d.bdl4.c801 (bia 000d.bdl4.c801)
  MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  ARP type: ARPA, ARP Timeout 04:00:00,
  Last input 00:00:08, output 00:00:05, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0 (size/max/drops); Total output drops: 0
  Queueing strategy: fifo
  Output queue :0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
    0 packets input, 0 bytes, 0 no buffer
    Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
    0 input packets with dribble condition detected
    0 packets output, 0 bytes, 0 underruns
    0 output errors, 0 collisions, 1 interface resets
    0 babbles, 0 late collision, 0 deferred
    0 lost carrier, 0 no carrier
    0 output buffer failures, 0 output buffers swapped out
FastEthernet0/1 is up, line protocol is down (disabled)
  Hardware is Lance, address is 000d.bdl4.c802 (bia 000d.bdl4.c802)
  Internet address is 192.168.1.1/24
  MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  ARP type: ARPA, ARP Timeout 04:00:00,
  Last input 00:00:08, output 00:00:05, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0 (size/max/drops); Total output drops: 0
  Queueing strategy: fifo
  Output queue :0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
    0 packets input, 0 bytes, 0 no buffer
    Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort

```

->View active configuration in DRAM

2621.1#show running-config

```
Router>enable
Router#show running-config
Building configuration...

Current configuration : 484 bytes
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Router
!
!
!
!
!
!
!
ip cef
no ipv6 cef
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
interface FastEthernet0/0
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface FastEthernet0/1
 no ip address
 duplex auto
 speed auto
 shutdown
!
shutdown
:
ip classless
:
ip flow-export version 9
:
:
:
:
:
line con 0
:
line aux 0
:
line vty 0 4
 login
:
:
:
--More-- |
```

EXPERIMENT-5

Study advanced router configuration commands.

->View Router 1 flash memory

Router1# show flash

View history table and previously entered commands (ctrl+p)

Router1#sow history Router1#Ctrl+p

```
Press RETURN to get started!
```

```
Router>enable
```

```
Router#show flash
```

```
System flash directory:
```

```
File Length Name/status
```

```
3 5571584 c2600-i-mz.122-28.bin
```

```
2 28282 sigdef-category.xml
```

```
1 227537 sigdef-default.xml
```

```
[5827403 bytes used, 58188981 available, 64016384 total]
```

```
63488K bytes of processor board System flash (Read/Write)
```

```
Router#show history
```

```
enable
```

```
show flash
```

```
show history
```

```
Router#
```

->Configure interface

Router1#configure terminal

Router1(config)#interface s0/0

Router1(config-if)# bandwidth 64

Router1(config-if)# clock rate 64000

Router1(config-if)#Ctrl+z

Router1# show interfaces serial 0/0

->Add description to interface to serial 0/0

Router1(config)#interface serial 0/0

Router1(config-if)# description Serial Link to Router2

Router1(config-if)# exit

Router1(config)#exit

Router1#show interfaces serial 0/0

```
Router>show interfaces s0/1
%Invalid interface type and number
Router>enable
Router#show interfaces s0/1
%Invalid interface type and number
Router#show interfaces
FastEthernet0/0 is administratively down, line protocol is down (disabled)
  Hardware is Lance, address is 0001.c717.2c01 (bia 0001.c717.2c01)
  MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  ARP type: ARPA, ARP Timeout 04:00:00,
  Last input 00:00:08, output 00:00:05, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0 (size/max/drops); Total output drops: 0
  Queueing strategy: fifo
  Output queue :0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
    0 packets input, 0 bytes, 0 no buffer
      Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
    0 input packets with dribble condition detected
    0 packets output, 0 bytes, 0 underruns
    0 output errors, 0 collisions, 1 interface resets
    0 babbles, 0 late collision, 0 deferred
    0 lost carrier, 0 no carrier
    0 output buffer failures, 0 output buffers swapped out
--More--
```

Experiment – 6

Aim: Host to Host communication using IP Addressing.

Lab Scenario:

Host A: IP address: 192.168.101.2/24, Default gateway: 192.168.101.1

Host B: IP address: 192.168.100.2/24, Default gateway: 192.168.100.1

Router R1: Ethernet interface: IP address: 192.168.101.1/24, Serial interface: IP address: 192.168.1.1/24, DCE cable connected

Router R2: Ethernet interface: IP address: 192.168.100.1/24, Serial interface: IP address: 192.168.1.2/24

REQUIREMENTS:

Host A with appropriate IP address settings

Host B with appropriate IP address settings

Router R1 and R2 with appropriate IP address settings

DCE cable for connecting Router R1

Ethernet cables for connecting hosts and routers

Console cables for configuring routers

Terminal emulator software (such as PuTTY or HyperTerminal)

8Appropriate networking equipment (switches, hubs, etc.) as required

PROCEDURE:

Setup Host A with the IP address 192.168.101.2/24 and default gateway 192.168.101.1. Verify the settings.

Setup Host B with the IP address 192.168.100.2/24 and default gateway 192.168.100.1. Verify the settings.

Configure Router R1 with the Ethernet interface IP address

192.168.101.1/24 and the Serial interface IP address 192.168.1.1/24.
Connect the DCE cable to Router R1.

Configure Router R2 with the Ethernet interface IP address

192.168.100.1/24 and the Serial interface IP address 192.168.1.2/24.

Connect Host A and Host B to the respective Ethernet interfaces of Router R1 and Router R2 using Ethernet cables.

Connect the Serial interfaces of Router R1 and Router R2 using the DCE cable.

Configure the host names of Router R1 and Router R2 as per lab requirements.

Configure the interfaces of Router R1 and Router R2 with appropriate settings, including the clock rate on the DCE interface.

Save the configurations on Router R1 and Router R2.

Test the connectivity between Host A and Host B by pinging each other's IP addresses.

Test the connectivity between Host A and Router R1, and Host B and Router R2 by pinging the respective interface IP addresses.

Document the process, including the configurations made, any observations, and results obtained.

Router R1 Configuration: -

Router Con0 is now available
Press RETURN to get started!

```
Router>ena
ble
Router#con
fig t
```

Enter configuration commands, one per line. End with CNTL/Z

```
Router(config)#hostname R1
```

```
R1(config)#interface f0/0
```

```
R1(config-if)#ip address 192.168.101.1
255.255.255.0 R1(config-if)#no shut
```

```
03:47:46 %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up
```

```
03:47:46 %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed
state to up
```

```
R1(config-if)#interface s0/0
```

```
R1(config-if)#ip address 192.168.1.1 255.255.255.0
```

```
R1(config-if)#clock rate
64000 R1(config-if)#no
shut
```

03:48:43 %LINK-3-UPDOWN: Interface Serial0/0, changed state to up

03:48:43 %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0, changed state to up R1(config-if)#

Router R2 Configuration:

- Router Con0 is now available Press RETURN to get started!

Router>enable

Router#config t

Enter configuration commands, one per line. End with CNTL/Z

Router(config)#hostname R2

R2(config)#interface f0/0

R2(config-if)#ip address 192.168.100.1 255.255.255.0

R2(config-if)#no shut

03:51:11 %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up

03:51:11 %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up

R2(config-if)#interface s0/0

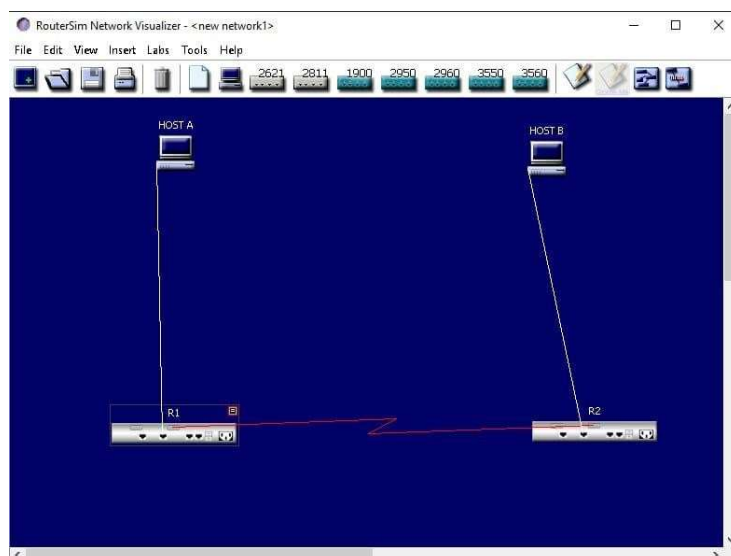
R2(config-if)#ip address 192.168.1.2

255.255.255.0 R2(config-if)#no shut

03:52:02 %LINK-3-UPDOWN: Interface Serial0/0, changed state to up

03:52:02 %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0, changed state to up R2(config-if)#exit

R2(config)#



Console for R2

File Edit View Tools Help

Net Detective

Press RETURN to get started

```
Router>enable
Router#config t
Enter configuration commands, one per line. End with CNTL/Z
Router(config)#hostname R2
R2(config)#interface f0/0
R2(config-if)#ip address 192.168.100.1 255.255.255.0
R2(config-if)#no shut
03:51:11 %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up
03:51:11 %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up

R2(config-if)#interface s0/0
R2(config-if)#ip address 192.168.1.2 255.255.255.0
R2(config-if)#no shut
03:52:02 %LINK-3-UPDOWN: Interface Serial0/0, changed state to up
03:52:02 %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0, changed state to up

R2(config-if)#exit
R2(config)#
```

Console for R1

File Edit View Tools Help

Net Detective

```
Router>enable
Router#config t
Enter configuration commands, one per line. End with CNTL/Z
Router(config)#hostname R1
R1(config)#interface f0/0
R1(config-if)#ip address 192.168.101.1 255.255.255.0
R1(config-if)#no shut
03:47:46 %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up
03:47:46 %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up

R1(config-if)#interface s0/0
R1(config-if)#ip address 192.168.1.1 255.255.255.0
R1(config-if)#clock rate 64000
R1(config-if)#no shut
03:48:43 %LINK-3-UPDOWN: Interface Serial0/0, changed state to up
03:48:43 %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0, changed state to up

R1(config-if)#exit
R1(config)#exit
```

EXPERIMENT-7

AIM-To define a static route between two routers so that all the devices can ping any other device.

LAB SCENARIO:

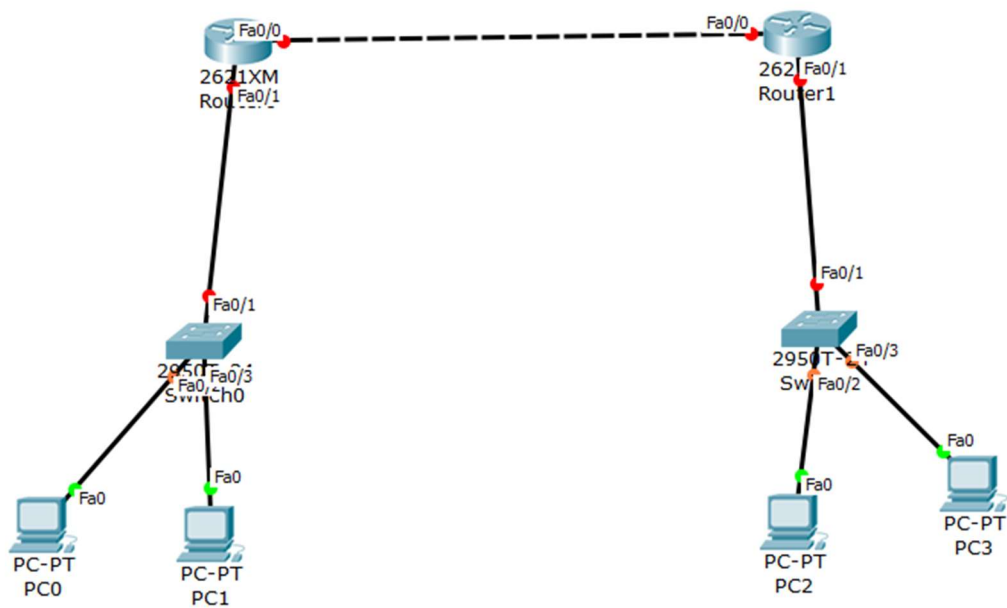
Devices IP address | Subnet Mask | Default gateway |

Interfaces

1.Router 1	192.168.1.1	255.255.255.0	Gigabit Ethernet 0/0
2.Router 1	10.0.0.1	255.0.0.0	Serial 0/0
3.Router 2	192.168.2.1	255.255.255.0	Gigabit Ethernet 0/0
4.Router 2	10.0.0.2	255.0.0.0	Serial 0/0
5.PC 0	192.168.1.5	255.255.255.0	192.168.1.1 Ethernet
6.PC 1	192.168.1.10	255.255.255.0	192.168.1.1 Ethernet
7.PC 2	192.168.2.5	255.255.255.0	192.168.2.1 Ethernet
8.PC 2	192.168.2.10	255.255.255.0	192.168.2.1 Ethernet

PROCEDURE:

1. Take two Cisco Routers Model 2911, two Ethernet Switches, and four generic PCs.
- 2.Connect them using the appropriate cables.
- 3.Use RJ 45 copper straight cable for connecting router LAN interface (Gigabit Ethernet Port) with Switch Fast Ethernet port and switch to PC as shown in the diagram.
- 4.Use Serial Cable to connect the serial interface of the two routers for point to point connection.
- 5.The serial interface is not integrated with the router, hence it has to be fitted externally. Insert the serial card (here we are taking HWIT- 2T)to the appropriate serial card slot. Please be sure that the router is off while inserting the card to the slot.
6. While configuring serial interface between two routers, please keep in mind that one end will be the DCE (Data Communication Equipment) and the other end will be DTE (Data Terminal Equipment).
7. We have to assign a clock rate or the bandwidth to the DCE end. The clock rate is written in bit per sec. Suppose, we have to assign channel bandwidth of 1Mbps, the clock rate is set as 1000000.



PC1

Physical Config Desktop Custom Interface

IP Configuration X

IP Configuration

☐ DHCP ☒ Static

IP Address 192.168.1.10

Subnet Mask 255.255.255.0

Default Gateway 192.168.1.1

DNS Server 0.0.0.0

host a

Physical Config Desktop Custom Interface

IP Configuration X

IP Configuration

☐ DHCP ☒ Static

IP Address 192.168.1.5

Subnet Mask 255.255.255.0

Default Gateway 192.168.1.1

DNS Server

host c

Physical Config Desktop Custom Interface

IP Configuration X

IP Configuration

☐ DHCP ☒ Static

IP Address 192.168.2.5

Subnet Mask 255.255.255.0

Default Gateway 192.168.2.1

DNS Server

PC3

Physical Config Desktop Custom Interface

IP Configuration X

IP Configuration

☐ DHCP ☒ Static

IP Address 192.168.2.10

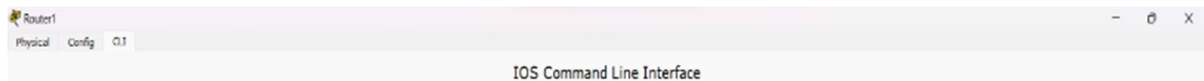
Subnet Mask 255.255.255.0

Default Gateway 192.168.2.1

DNS Server



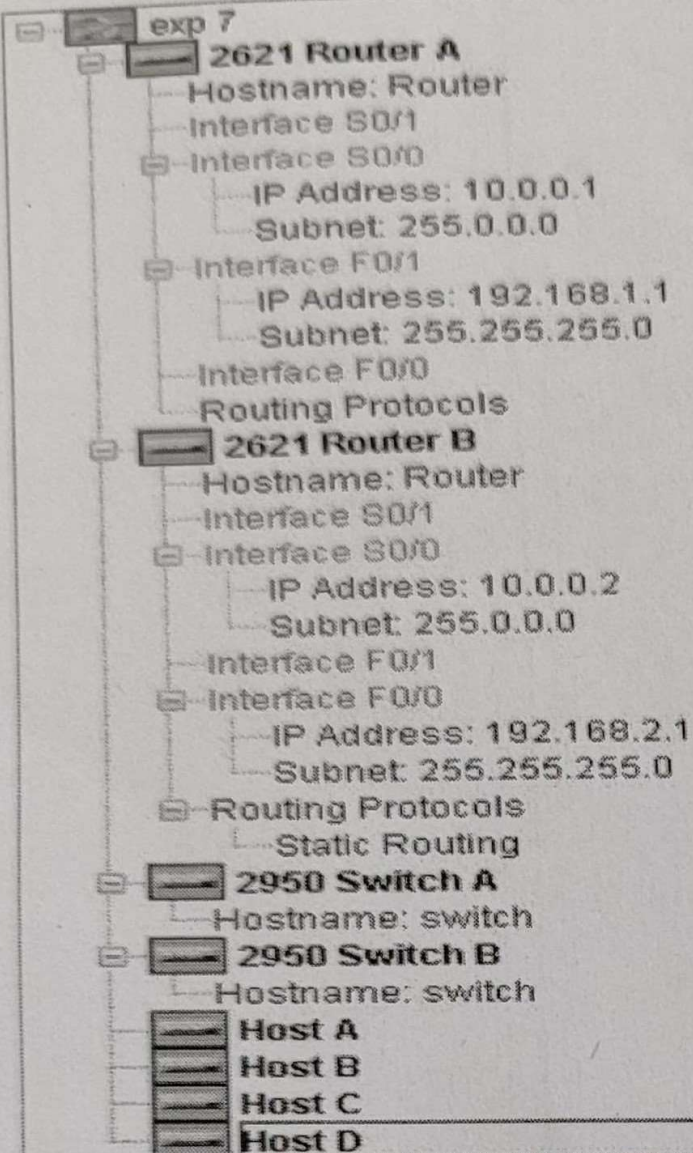
```
Router0
Router0#
Router0#enable
Router0#configure terminal
Enter configuration commands, one per line. End with CTRL/Z
Router0(config)#interface Gigabit Ethernet 0/0
Invalid input detected at marker. Router0(config)#interface Gigabit Ethernet 0/0
Invalid input detected at marker.
Router0(config)#interface FastEthernet0/1 Router0(config-if)#ip address
192.168.1.1 255.255.255.0
Router0(config-if)#no shutdown
16:52:36 LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to up 16:52:36
LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to
up
Router0(config-if)#exit
Router0(config)#interface serial 0/0/0
Invalid input detected at marker.
Router0(config)#interface serial 0/0
Router0(config-if)#ip address 10.0.0.1 255.0.0.0
Router0(config-if)#clock rate 1000000
Router0(config-if)#no shutdown
16:54:42 LINK-3-UPDOWN: Interface Serial0/0, changed state to up
16:54:42 LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0, changed state
to up
Router0(config-if)#exit
Router0(config)#ip route 192.168.2.0 255.255.255.0 10.0.0.2
Router0(config)#exit
Translating "site"... domain server (255.255.255.255) Unknown command or
computer name, or unable to find computer address
Router0#write
Router0#write
Building configuration...
[OK]
Router0#
```



```
Router1
Router1#
Router1#enable
Router1#configure terminal
Enter configuration commands, one per line. End with CTRL/Z
Router1(config)#interface FastEthernet 0/0 Router1(config-if)#ip address
192.168.2.1 255.255.255.0
Router1(config-if)#no shutdown
16:57:41 LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up
16:57:41 LINEPROTO-3-UPDOWN: Line protocol on Interface FastEthernet0/0,
changed state to up
Router1(config)#
Router1(config)#interface serial 0/0
Router1(config-if)#ip address 10.0.0.2 255.0.0.0
Router1(config-if)#no shutdown
Invalid input detected at
Router1(config-if)#no shutdown
16:58:31 LINK-3-UPDOWN: Interface Serial0/0, changed state to up 16:58:31
LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0, changed state to up
Router1(config-if)#exit
Router1(config)#ip route 192.168.1.0 255.255.255.0 10.0.0.1
Router1(config)#
Building configuration...
Router1#
```

NET CONFIGS:

Net Configs



EXPERIMENT-8

8.To define a default route between two routers so that all the devices can ping any other devices.

LAB SCENARIO:

Devices IP address | Subnet Mask | Default gateway |
Interfaces

1.Router 1 192.168.1.1 | 0.0.0.0 Gigabit Ethernet 0/0

2.Router 1 0.0.0.0 | 255.0.0.0 Serial 0/0

3.Router 2 192.168.2.1 | 255.255.255.0 Gigabit Ethernet 0/0

4.Router 2 10.0.0.2 | 255.0.0.0 Serial 0/0

5.PC 0 192.168.1.5 | 255.255.255.0 | 192.168.1.1 Ethernet

6.PC 1 192.168.1.10 255.255.255.0 | 192.168.1.1 Ethernet

7.PC 2 192.168.2.5 | 255.255.255.0 192.168.2.1 Ethernet

8.PC 2 192.168.2.10 255.255.255.0 | 192.168.2.1 Ethernet

PROCEDURE:

1. Take two Cisco Routers Model 2911, two Ethernet Switches, and four generic PCs.

2.Connect them using the appropriate cables.

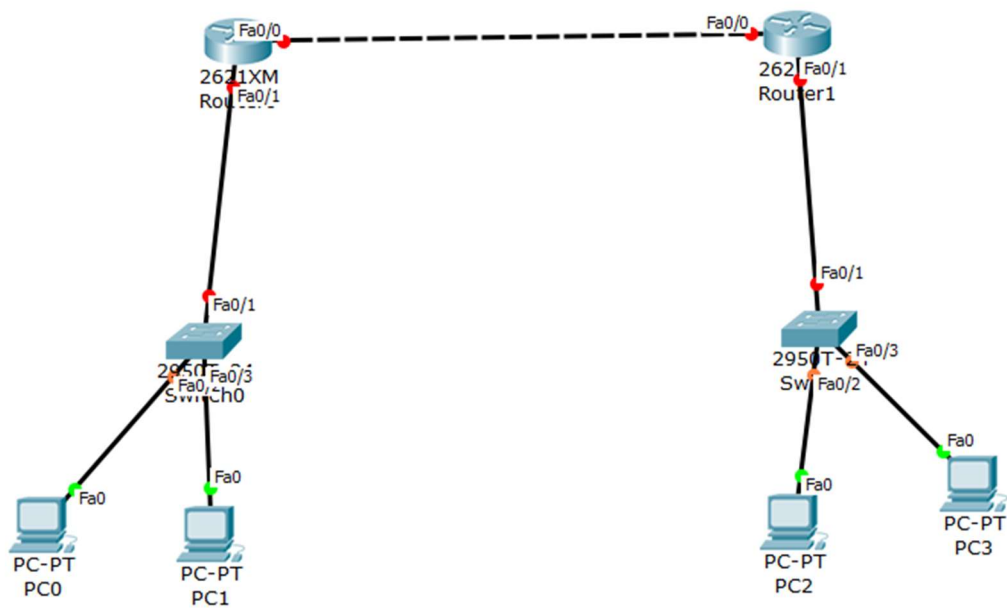
3. Use RJ 45 copper straight cable for connecting router LAN interface (Gigabit Ethernet Port) with Switch Fast Ethernet port and switch to PC as shown in the diagram.

4. Use Serial Cable to connect the serial interface of the two routers for point to point connection.

5. The serial interface is not integrated with the router, hence it has to be fitted externally. Insert the serial card (here we are taking HWIT- 2T) to the appropriate serial card slot. Please be sure that the router is off while inserting the card to the slot.

6. While configuring serial interface between two routers, please keep in mind that one end will be the DCE (Data Communication Equipment) and the other end will be DTE (Data Terminal Equipment).

7. We have to assign a clock rate or the bandwidth to the DCE end. The clock rate is written in bit per sec. Suppose, we have to assign channel bandwidth of 1Mbps, the clock rate is set as 1000000.



PC1

Physical Config Desktop Custom Interface

IP Configuration

IP Configuration

☐ DHCP ☒ Static

IP Address 192.168.1.10

Subnet Mask 255.255.255.0

Default Gateway 192.168.1.1

DNS Server 0.0.0.0

host a

Physical Config Desktop Custom Interface

IP Configuration

IP Configuration

☐ DHCP ☒ Static

IP Address 192.168.1.5

Subnet Mask 255.255.255.0

Default Gateway 192.168.1.1

DNS Server

host c

Physical Config Desktop Custom Interface

IP Configuration

IP Configuration

☐ DHCP ☒ Static

IP Address 192.168.2.5

Subnet Mask 255.255.255.0

Default Gateway 192.168.2.1

DNS Server

PC3

Physical Config Desktop Custom Interface

IP Configuration

IP Configuration

☐ DHCP ☒ Static

IP Address 192.168.2.10

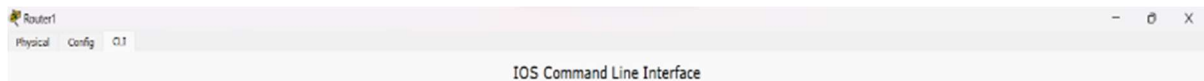
Subnet Mask 255.255.255.0

Default Gateway 192.168.2.1

DNS Server



```
Router Cond is now available
Press RETURN to get started!
Router enable Router config
Enter configuration commands, one per line. End with CHTL/2
Router(config)#interface Gigabit Ethernet 0/0.
Invalid input detected at marker. Router(config)#interface Gigabit Ethernet0/0
Invalid input detected at marker.
Router(config)#interface FastEthernet0/1 Router(config-if)#ip address
192.168.1.1 255.255.255.0
Router(config-if)#no shutdown
16:52:36 LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to up 16:52:36
LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to
up
Router(config-if)#exit
Router(config)#interface serial 0/0/0
Invalid input detected at marker.
Router(config)#interface serial 0/0
Router(config-if)#ip address 10.0.0.1 255.0.0.0
Router(config-if)#clock rate 1000000
Router(config-if)#no shutdown
16:54:42 LINK-3-UPDOWN: Interface Serial0/0, changed state to up
16:54:42 LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0, changed state
to up
Router(config-if)#exit
Router(config)#ip route 192.168.2.0 255.255.255.0 10.0.0.2
Router(config)#exit
Translating "site"... domain server (255.255.255.255) Unknown command or
computer name, or unable to find computer address
Router wite
Router write
Building configuration...
[OK]
Routers
```



```
Routez Cong is nov available
Prese RETURN to get atasted!
Routes-enable Fouter config t
Enter configuration coanande, one per line. End with CRTL/2
Router(config)#interface FastEthernet 0/0 Router(config-if)#ip address
192.168.2.1 255.255.255.0
Router(config-if)#ie shutdown
16:57:41 LINK-3-UPDOWN: Interface FastEthernet0/0. changed state to up
16:57:41 ALINEPROTO-3-UPDOWN: Line protocol an Interface FastEthernet0/0,
changed state to up
Routes (config-
Routez (config)#interface serial 0/0
Router(config-if)#ip address 10.0.0.2 255.0.0.0
Router(config-if)#no shutduon
Invalid Input detected at
Router(config-if)#no shutdown
16:58:31-3-o: Interface Secial0/0, changed state to up 16:58:31
LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0, duanged state to up
Router(config-if)#exit
Router(config)#ip route 192.168.1.0 255.255.259.0 10.0.0.1
Router(omfig)#e
Building configuratim...
Router
```