**[](http://www.bing.com/images/search?q=dehradun+institute+of+technology&view=detail&id=3269210848E4EAFFD1E2A3153403263A57F010D5&first=0&FORM=IDFRIR)**

INDUSTRIAL TRAINING:

ROUTING

MECHANISMS

**SUBMITTED TO:** **SUBMITTED BY:**

MR. RP ARORA GURLEEN SINGH (09070101043) CS 3RD YR

COMPUTER SCIENCE (HOD) ANKIT BALYAN (09070101012) CS 3RD YR

ANKIT BHADOLA (09070101013) CS 3RD YR

**ACKNOWLEDGEMENT**

This project has been made successful under the guidance of our teacher MR. RP ARORA (HOD-CS) who not only helped us in the completion of the project but also extended his full support for it.

We owe a great thanks to MR. ZAHID KHAN -CCNP (Cisco certified network Professional) and the instructor of the project who guided us in the making of the project and taught us internetworking concepts and routing mechanisms.

Our special thanks to Ms. DIMPLE BAJAJ for her guidance and support.

Thanks and appreciation to the helpful people at my institution for their support.

**INDEX**

1. Introduction
   1. Internetworking
2. Networking Devices
   1. Network Interface Card
   2. Hubs
   3. Bridges
   4. Switches
   5. Routers
3. Ethernet Cables
4. Networking Models
   1. OSI model
   2. DOD model
5. IP Addressing
   1. IP Addresses
   2. Class-full Address
   3. Network Masks
   4. Subnetting
6. IP Routing
   1. Types of Rooting
   2. Protocols
   3. RIP Routing Information Protocol
7. Project Description
   1. Network Designing
   2. Configuring of Routing
   3. Routing Mechanism
      1. Static Routing
      2. Dynamic Routing Using RIP
8. Conclusion

INTRODUCTION

* 1. ***Internetworking***

***Internetworking*** is the practice of connecting a computer network with other networks through the use of gateways that provide a common method of routing information packets between the networks. The resulting system of interconnected networks is called an internetwork, or simply an ***internet***.

It can also be defined as the art of connecting individual local-area networks (LANs) to create wide-area networks (WANs) , and connecting WANs to form even larger WANs. Internetworking can be extremely complex because it generally involves connecting networks that use different protocols. Internetworking is accomplished with routers, bridges, and gateways.

The most notable example of internetworking is the Internet, a network of networks based on many underlying hardware technologies, but unified by an internetworking protocol standard, the Internet Protocol Suite, often also referred to as TCP/IP.

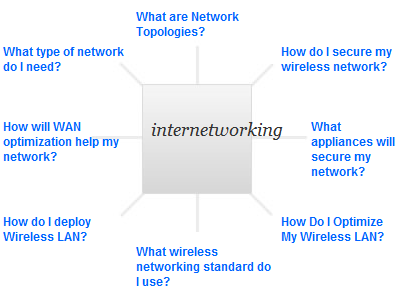


Fig 1.1) Breaking up of a internetwork

Internetworking started as a way to connect disparate types of networking technology, but it became widespread through the developing need to connect two or more local area networks via some sort of wide area network. The original term for an internetwork was catenet.

Today the interconnecting gateways are called Internet routers. Another type of interconnection of networks often occurs within enterprises at the Link Layer of the networking model, i.e. at the hardware-centric layer below the level of the TCP/IP logical interfaces. Such interconnection is accomplished with network bridges and network switches.

But, there were no. of things which cause LAN Traffic Congestion. Some of those things are:-

* Too many hosts in a Broadcast Domain.
* Broadcast Storms.
* Multicasting.
* Low Bandwidth.
* Adding hubs for connectivity to the network.
* A bunch of ARP or IPX Traffic.

**Q) What are LAN and WAN?**

**A) LAN (local area network)** supplies networking capability to a group of computers in close proximity to each other such as in an office building, a school, or a home. A LAN in turn often connects to other LANs, and to the Internet or other WAN. Most local area networks are built with relatively inexpensive hardware such as Ethernet cables, network adapters, and hubs.

**Useful for:**

* Sharing files
* Sharing printer
* LAN party; playing games over a network

**Causes of LAN traffic congestion:**

* + Too many hosts in a broadcast domain
  + Broadcast storms
  + Multicasting
  + Low bandwidth
  + Adding hubs for connectivity to the network
  + A bunch of ARP or IPX traffic (IPX is a Novell protocol that is like IP, but really, really chatty. Typically not used in today’s networks.)

**WAN (wide area network)** is a computer network that spans a relatively large geographical area. Typically, a WAN consists of two or more local-area networks (LANs).Computers connected to a wide-area network is often connected through public networks, such as the telephone system. They can also be connected through leased lines or satellites. The largest WAN in existence is the Internet.

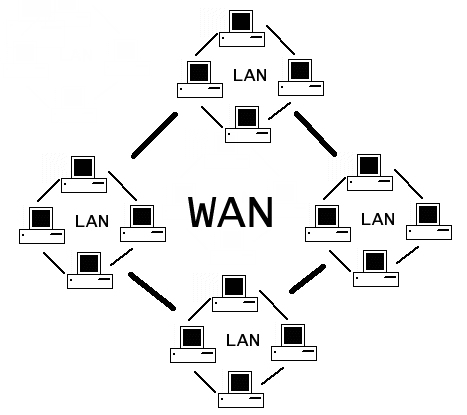


Fig 1.2) Interconnection of LAN networks to form a WAN network

**Networking Devices**

**Computer networking devices** are units that mediate data in a computer network. Computer networking devices are also called network equipment, Intermediate Systems (IS) or Inter Working Unit (IWU). Units which are the last receiver or generate data are called hosts or data terminal equipment.

* 1. ***Network Interface Card***

A network card, network adapter, or NIC (network interface card) is a piece of computer hardware designed to allow computers to physically access a networking medium. It provides a low-level addressing system through the use of **MAC addresses**.

Each Ethernet network interface has a unique MAC address which is usually stored in a small memory device on the card, allowing any device to connect to the network without creating an address conflict. Ethernet MAC addresses are composed of six octets. Uniqueness is maintained by the **IEEE**, which manages the Ethernet address space by assigning 3-octet prefixes to equipment manufacturers. The list of prefixes is publicly available.

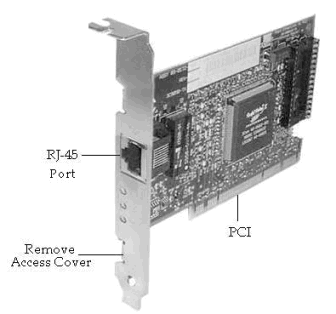


Fig 2.1) A Network Interface Card

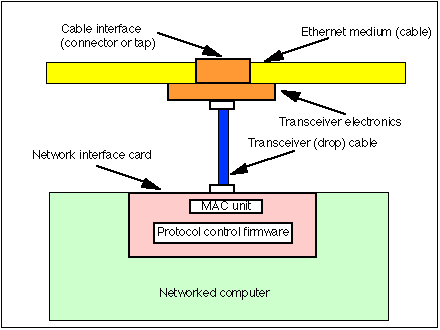


Fig 2.2) Topology showing working of a NIC

* 1. ***HUBS***

The term ‘hub’ is sometimes used to refer to any piece of network equipment that connects PCs together, but it actually refers to a multi-port repeater. This type of device simply passes on (repeats) all the information it receives, so that all devices connected to its ports receive that information.

Hubs repeat everything they receive and can be used to extend the network. However, this can result in a lot of unnecessary traffic being sent to all devices on the network. Hubs pass on traffic to the network regardless of the intended destination; the PCs to which the packets are sent use the address information in each packet to work out which packets are meant for them. In a small network repeating is not a problem but for a larger, more heavily used network, another piece of networking equipment (such as a switch) may be required to help reduce the amount of unnecessary traffic being generated.

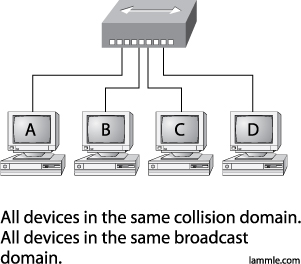


Fig 2.3) A hub in a network

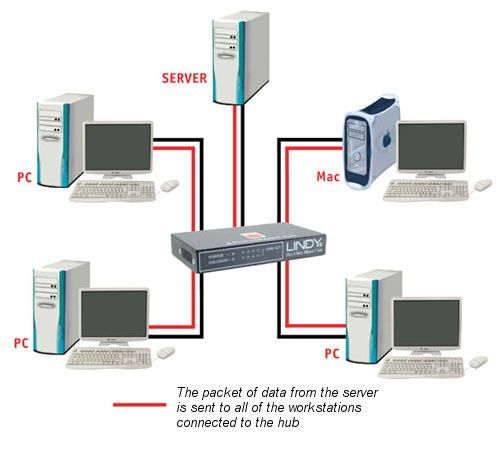


Fig 2.4) How a packet passes through a network on a hub.

**Q) What is a Broadcast Domain?**

**A)** A **broadcast domain** is a logical division of a computer network, in which all nodes can reach each other by broadcast at the data link layer. A broadcast domain can be within the same LAN segment or it can be bridged to other LAN segments.

Any computer connected to the same hub or switch is a member of the same broadcast domain. Further, any computer connected to the same set of inter-connected switches/hub is a member of the same broadcast domain. Routers and other higher-layer devices form boundaries between broadcast domains.

**Q) What is a collision Domain?**

**A)** A **collision domain** is a section of a network where data packets can collide with one another when being sent on a shared medium or through hubs, in particular. A network collision occurs when more than one device attempts to send a packet on a network segment at the same time. Collisions are resolved using carrier sense multiple access.

In this only one device in the collision domain may transmit at any one time, and the other devices in the domain listen to the network in order to avoid data collisions. Because only one device may be transmitting at any one time, total network bandwidth is shared among all devices. Collisions also decrease network efficiency on a collision domain; if two devices transmit simultaneously, a collision occurs, and both devices must retransmit at a later time.

*Collision domains are found in a hub environment where each host segment connects to a hub that represents only one collision domain and only one broadcast domain.*

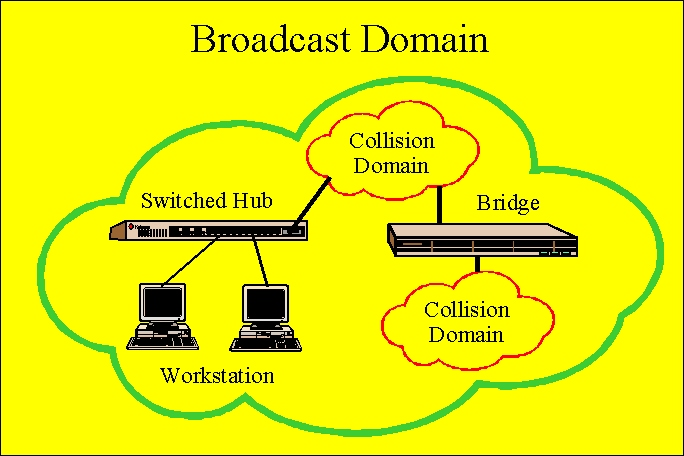


Fig 2.5) Representation of Broadcast and Collision domain

* + 1. ***Uses of Hub***

## Historically, the main reason for purchasing hubs rather than switches was their price. This motivator has largely been eliminated by reductions in the price of switches, but hubs can still be useful in special circumstances:

* When a switch is accessible for end users to make connections, for example, in a conference room, an inexperienced or careless user can bring down the network by connecting two ports together, causing a loop. This can be prevented by using a hub, where a loop will break other users on the hub, but not the rest of the network.
* A hub with a 10BASE2 port can be used to connect devices that only support 10BASE2 to a modern network. The same goes for linking in an old 10BASE5 network segment using an AUI port on a hub.
  1. ***Bridges***

A network bridge connects multiple network segments at the data link layer . Bridges broadcast to all ports except the port on which the broadcast was received. However, bridges do not promiscuously copy traffic to all ports, as hubs do, but learn which MAC addresses are reachable through specific ports.

Once the bridge associates a port and an address, it will send traffic for that address to that port only. Bridges learn the association of ports and addresses by examining the source address of frames that it sees on various ports. Once a frame arrives through a port, its source address is stored and the bridge assumes that MAC address is associated with that port. The first time that a previously unknown destination address is seen, the bridge will forward the frame to all ports other than the one on which the frame arrived.

*Bridges serve a similar function as switches that also operate at Layer 2. Traditional bridges, though, support one network boundary, whereas switches usually offer four or more hardware ports. Switches are sometimes called "multi-port bridges" for this reason.*

**Bridges come in three basic types:**

* Local bridges: Directly connect local area networks (LANs)
* Remote bridges: Can be used to create a wide area network (WAN) link between LANs.
* Wireless bridges: Can be used to join LANs or connect remote stations to LANs.

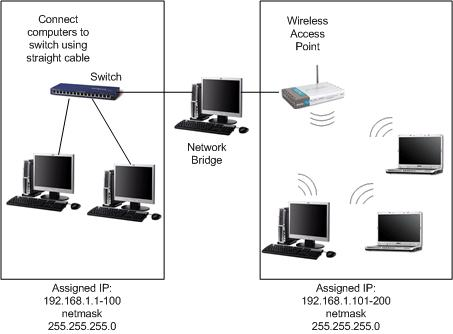


Fig 2.6) Working of a Bridge

* 1. ***Switches***

Switches control the flow of network traffic based on the address information in each packet. A switch learns which devices are connected to its ports (by monitoring the packets it receives), and then forwards on packets to the appropriate port only. This allows simultaneous communication across the switch, improving bandwidth. The switch works by learning the MAC addresses of the systems attached to it and storing it in a switching table.

This switching operation reduces the amount of unnecessary traffic that would have occurred if the same information had been sent from every port (as with a hub).

Switches and hubs are often used in the same network; the hubs extend the network by providing more ports, and the switches divide the network into smaller, less congested sections.

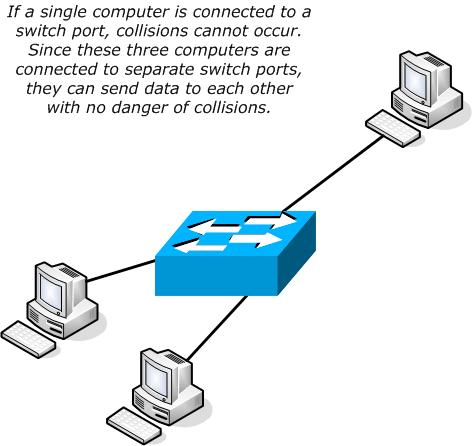
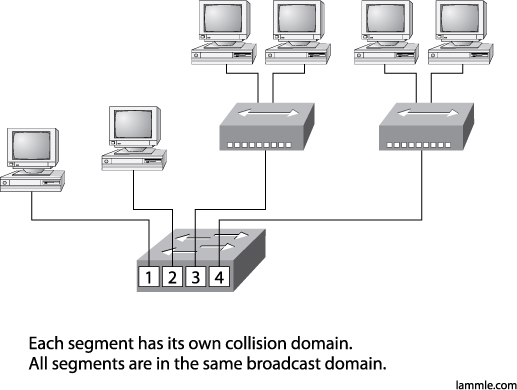


Fig 2.7) A Switch at work



**PORTS**

**SWITCH**

**HUBS**

Fig 2.8) A switch breaking collision domain in a network

**Q) When Should I Use a Hub or Switch?**

**A)** In a small network (less than 30 users), a hub (or collection of hubs) can easily cope with the network traffic generated and is the ideal piece of equipment to use for connecting the users.

When the network gets larger (about 50 users), you may need to use a switch to divide the groups of hubs, to cut down the amount of unnecessary traffic being generated.

* 1. ***Routers***

A router is used to route data packets between two networks. It reads the information in each packet to tell where it is going. If it is destined for an immediate network it has access to, it will strip the outer packet, readdress the packet to the proper Ethernet address, and transmit it on that network.

If it is destined for another network and must be sent to another router, it will re-package the outer packet to be received by the next router and send it to the next router.

The section on routing explains the theory behind this and how routing tables are used to help determine packet destinations. Routing occurs at the network layer of the OSI model.

They can connect networks with different architectures such as Token Ring and Ethernet. Although they can transform information at the data link level, routers cannot transform information from one data format such as TCP/IP to another such as IPX/SPX.

Routers do not send broadcast packets or corrupted packets. If the routing table does not indicate the proper address of a packet, the packet is discarded.

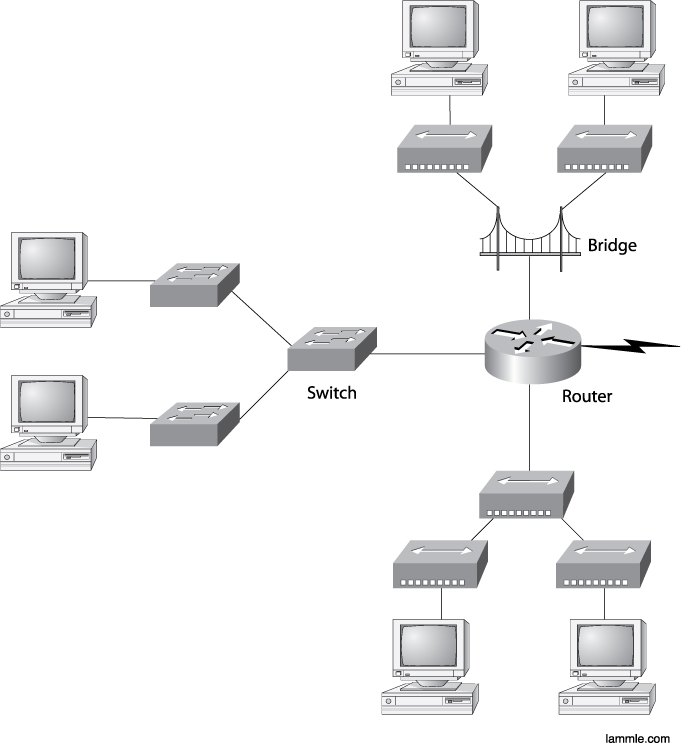
### D:\CCNA PROJECT\Network_Connection_With_Routers.jpg

Fig 2.9) A router in action

* + 1. ***Gateways***

A gateway can translate information between different network data formats or network architectures. It can translate TCP/IP to AppleTalk so computers supporting TCP/IP can communicate with Apple brand computers. Most gateways operate at the application layer, but can operate at the network or session layer of the OSI model. Gateways will start at the lower level and strip information until it gets to the required level and repackage the information and work its way back toward the hardware layer of the OSI model. To confuse issues, when talking about a router that is used to interface to another network, the word gateway is often used. This does not mean the routing machine is a gateway as defined here, although it could be.

***---SUMMARY---***



**D**

**C**

**B**

**A**

Fig 2.10) A segmented network containing of Hubs, Switches and a Router. (A)=A bridge and two hubs. (B)=Three switches. (C)=Three hubs. (D)=Network Interface Cards (NIC) of computers

The above diagram gives a complete overview about how network devices work together to form a network and communicate with each other.

Ethernet Cables

***There are 3 types of Ethernet Cables:-***

* 1. ***Straight Through Cable***

It is used to connect

* Host to Switch or Hub
* Router to Switch or Hub

Four wires are used in it to connect Ethernet Devices. It is relatively simple to create this type as below:

1

1

3

3

2

2

6

6

* 1. ***Crossover Cable***

The crossover cable can be used to connect:

* Switch to Switch
* Hub to Hub
* Host to Host
* Hub to Switch
* Router direct to Host

The same 4 wires are used in this cable. Different pins are connected together.

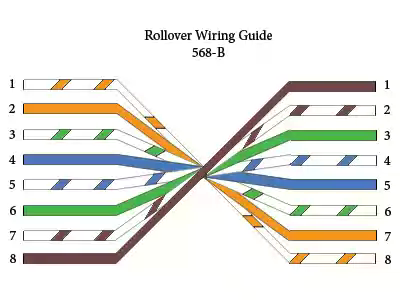


Fig 3.1) Rollover Cable

* 1. ***Rolled cable***

It is used to connect a host to a router console serial communication port.8 wires are used in this cable to connect serial devices, although not all 8 are used to send information.

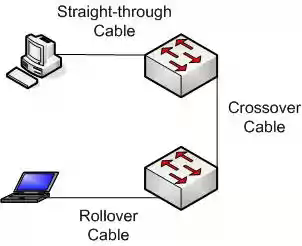


Fig 3.2) A network containing all the three cables

Networking models

* 1. ***OSI Model***

Work on a layered model of network architecture was started by the International Organization for Standardization (ISO) and OSI framework architecture was developed in the late 1970’s. The concept of a 7 layer model was provided by the work of Charles Bachman, Honeywell Information Services.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | **Data unit** | **Layer** | **Function** | |  |
| **Host layers** | * **Data** | ***7.*** *Application* | | Network process to application |  |
| ***6.*** *Presentation* | | Data representation, encryption and decryption, convert machine dependent data to machine independent data |  |
| ***5.*** *Session* | | Inter host communication |  |
| * **Segments** | ***4.*** *Transport* | | End-to-end connections and reliability, flow control |  |
| **Media layers** | * **Packet/Datagram** | ***3.*** *Network* | | Path determination and logical addressing |  |
| * **Frame** | ***2.*** *Data Link* | | Physical addressing |  |
| * **Bit** | ***1.*** *Physical* | | Media, signal and binary transmission |  |

Fig 4.1) OSI model 7 layers

* + 1. ***Layer 1: Physical Layer***

The Physical Layer defines electrical and physical specifications for devices. In particular, it defines the relationship between a device and a transmission medium, such as a copper or optical cable. This includes the layout of pins, voltages, cable specifications, hubs, repeaters, network adapters and more.

The major functions and services performed by the Physical Layer are:

**1.** Establishment and termination of a connection to a communications medium.

**2.** Modulation that is conversion between the representation of digital data in user equipment and the corresponding signals transmitted over a communications channel.

* + 1. ***Layer 2: Data Link Layer***

Data Link Layer provides both error correction and flow control by means of a selective repeat Sliding Window Protocol. It is responsible for the following:

1. Physical Addressing-It ensures that messages are delivered to the proper device on a LAN using hardware addresses.
2. It formats the message into pieces called a data frame and adds a customized header consisting of destination and source hardware address.
   * 1. ***Layer 3: Network Layer***

The Network Layer provides the functional and procedural means of transferring variable length data sequences from a source host on one network to a destination host on a different network, while maintaining the quality of service requested by the Transport Layer (in contrast to the data link layer which connects hosts within the same network).

The Network Layer performs network routing functions, and might also perform fragmentation and reassembly, and report delivery errors.

### *Layer 4: Transport Layer*

The Transport Layer provides transparent transfer of data between end users, providing reliable data transfer services to the upper layers. The Transport Layer controls the reliability of a given link through flow control, segmentation/ de-segmentation, and error control. Some protocols are connection-oriented. This means that the Transport Layer can keep track of the segments and retransmit those that fail. The Transport layer also provides the acknowledgement of the successful data transmission and sends the next data if no errors occurred.

### *Layer 5: Session Layer*

The Session Layer controls the dialogues (connections) between computers. It establishes, manages and terminates the connections between the local and remote application. It provides for full-duplex, half-duplex, or simplex operation, and establishes check pointing, adjournment, termination, and restart procedures. The OSI model made this layer responsible for graceful close of sessions, which is a property of the Transmission Control Protocol, and also for session check pointing and recovery, which is not usually used in the Internet Protocol Suite.

### 

### *Layer 6: Presentation Layer*

The Presentation Layer establishes context between Application Layer entities, in which the higher-layer entities may use different syntax and semantics if the presentation service provides a mapping between them.

This layer provides independence from data representation (e.g., encryption) by translating between application and network formats. The presentation layer transforms data into the form that the application accepts. This layer formats and encrypts data to be sent across a network. It is sometimes called the syntax layer.

### *Layer 7: Application Layer*

The Application Layer is the OSI layer closest to the end user, which means that both the OSI application layer and the user interact directly with the software application. This layer interacts with software applications that implement a communicating component.

# *DOD Model*

The **Department of Defense** created TCP/IP to ensure and preserve date integrity. The DOD model is a condensed version of the OSI model and only has four layers.

|  |  |
| --- | --- |
| **Corresponding Layers** | |
| **DoD Model** | **OSI Model** |
| * **Process Application Layer** | * **Application** |
| * **Presentation** |
| * **Session** |
| * **Host-to-Host Layer** | * **Transport** |
| * **Internet Layer** | * **Network** |
| * **Network Access Layer** | * **Data Link** |
| * **Physical** |

Fig 4.2) DOD Model compares to OSI model

* + 1. ***Process Application Layer***

Defines protocols for node-to-node application communication and also controls user interface specifications. It consists of a set of services that provide regular and consistent access to all types of networks. Applications utilize the services to communicate with other devices and remote applications.

* + 1. ***Host-to-Host Layer***

This layer shields the upper layers from the process of sending data. Also provides an end-to-end connection between two devices during communication by performing sequencing, acknowledgments, checksums, and flow control. Applications using services at this layer can use two different protocols: TCP and UDP.

* + - 1. ***TCP Overview (Transmission control Protocol)***

Before data is sent, the transmitting host contacts the receiving host to set up a connection known as a virtual circuit. This makes TCP *connection-oriented.* During the handshake the two hosts agree upon the amount of information to be sent before an acknowledgment is needed (Windowing). TCP takes the large blocks of data from the upper layers and breaks them up into segments that it numbers and sequences. TCP will the pass the segments to the network layer, which will route them through the Internetwork. The receiving TCP can put the segments back into order. After packets are sent, TCP waits for an acknowledgment from the receiving end of the virtual circuit. If no acknowledgment is received then the sending host will retransmit the segment.

#### UDP (User Datagram Protocol)

UDP transports information that doesn't require reliable delivery; therefore it can have less overhead than TCP as no sequencing or acknowledgments are used. NFS and SNMP use UDP for their session; the applications have their own methods to ensure reliability. UDP receives blocks of information from the upper layers, which it breaks into segments. It gives each segment a number, sends it, and then forgets about it. No acknowledgments, no virtual circuits, *connectionless protocol*.

* + 1. ***Internet Layer***

The Internet Layer exists for routing and providing a single network interface to the upper layers. IP provides the single network interface for the upper layers.

**IP (Internet Protocol):** The Internet Protocol (IP) is a network-layer (Layer 3) protocol that contains addressing information and some control information that enables packets to be routed.  IP has two primary responsibilities: providing connectionless, best-effort delivery of datagrams through an internetwork; and providing fragmentation and reassembly of datagrams.

* + 1. ***Network Access Layer***

The Network Access Layer monitors the data exchange between the host and the network. Oversees MAC addressing and defines protocols for the physical transmission of data.



**So if all binary bits are a one, the decimal equivalent would be 255 as shown here:**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **128** | **64** | **32** | **16** | **8** | **4** | **2** | **1** |
| **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** |

***(128+64+32+16+8+4+2+1=255)***

**Here is a sample octet conversion when not all of the bits are set to 1.**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **128** | **64** | **32** | **16** | **8** | **4** | **2** | **1** |
| **0** | **1** | **0** | **0** | **0** | **0** | **0** | **1** |

***(0+64+0+0+0+0+0+1=65)***

Decimal Equivalent= 65;

**And this is sample shows an IP address represented in both binary and decimal.**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ***DECIMAL*** | **10.** | **1.** | **23.** | **19** |
| ***BINARY*** | **00001010.** | **00000001.** | **00010111.** | **00010011** |

These octets are broken down to provide an addressing scheme that can accommodate large and small networks. There are five different classes of networks, A to E.

* 1. ***CLASSFULL ADDRESSING***

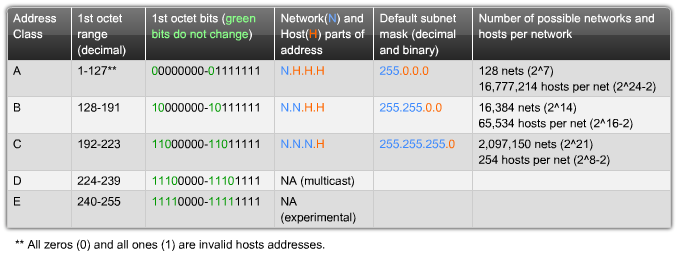


Fig 5.1) Class full addresses, Class A to E ranging from 0.0.0.0 to 255.255.255.255

Fig 5.2) Percentage (%) share of the 5 classes in 42258256025 IP Addresses

***CLASS A, B, C IP Addresses description***

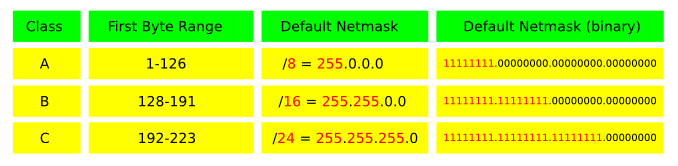


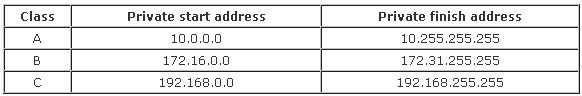
Fig 5.3) Generally used A, B, C classes IP Addresses and default subnet

* In a **Class A** address, the first octet is the network portion, so the Class A example in [Figure](http://www.cisco.com/en/US/tech/tk365/technologies_tech_note09186a00800a67f5.shtml) (5.3) has a major network address of 1.0.0.0 - 127.255.255.255. Octets 2, 3, and 4 (the next 24 bits) are for the network manager to divide into subnets and hosts as he/she sees fit. Class A addresses are used for networks that have more than 65,536 hosts (actually, up to 16777214 hosts!).
* In a **Class B** address, the first two octets are the network portion, so the Class B example in [Figure](http://www.cisco.com/en/US/tech/tk365/technologies_tech_note09186a00800a67f5.shtml) (5.3) has a major network address of 128.0.0.0 - 191.255.255.255. Octets 3 and 4 (16 bits) are for local subnets and hosts. Class B addresses is used for networks that have between 256 and 65534 hosts.
* In a **Class C address**, the first three octets are the network portion. The Class C example in [Figure](http://www.cisco.com/en/US/tech/tk365/technologies_tech_note09186a00800a67f5.shtml) (5.3) has a major network address of 192.0.0.0 - 233.255.255.255. Octet 4 (8 bits) is for local subnets and hosts - perfect for networks with less than 254 hosts.
  + 1. ***Private Network***

In the Internet addressing architecture, a **private network** is a network that uses private IP address space, following the standards set by *RFC 1918* and *RFC 4193*. These addresses are commonly used for home, office, and enterprise local area networks (LANs), when globally routable addresses are not mandatory, or are not available for the intended network applications. Private IP address spaces were originally defined in an effort to delay IPv4 address exhaustion, but they are also a feature of the next generation Internet Protocol, IPv6.

These addresses are characterized as private because they are not globally delegated, meaning they are not allocated to any specific organization, and IP packets addressed by them cannot be transmitted onto the public Internet. Anyone may use these addresses without approval from a regional Internet registry (RIR). If such a private network needs to connect to the Internet, it must use either a network address translator (NAT) gateway, or a proxy server.

**Private IPv4 address spaces:**

****

## *Network Masks*

A network mask helps you know which portion of the address identifies the network and which portion of the address identifies the node. Class A, B, and C networks have default masks, also known as natural masks, as shown here:

1. **Class A: *255.0.0.0***
2. **Class B: *255.255.0.0***
3. **Class C: *255.255.255.0***

An IP address on a Class A network that has not been subnetted would have an address/mask pair similar to: 8.20.15.1 255.0.0.0. To see how the mask helps you identify the network and node parts of the address, convert the address and mask to binary numbers.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 8.20.15.1 | 00001000. | 00010100. | 00001111. | 00001111. |
| **255.0.0.0** | **11111111.** | **00000000.** | **00000000.** | **00000000** |

Once you have the address and the mask represented in binary, then identifying the network and host ID is easier. Any address bits which have corresponding mask bits set to 1 represent the network ID. Any address bits that have corresponding mask bits set to 0 represent the node ID.

|  |  |  |
| --- | --- | --- |
| **NETID** | **00001000** | **8** |
| **HOST ID** | **00010100.00001111.00000001** | **20.15.1** |

* 1. ***Subnetting***

**Subnetting** allows you to create multiple logical networks that exist within a single Class A, B, or C network. If you do not subnet, you are only able to use one network from your Class A, B, or C network, which is unrealistic.

Each data link on a network must have a unique network ID, with every node on that link being a member of the same network. If you break a major network (Class A, B, or C) into smaller sub networks, it allows you to create a network of interconnecting sub networks. Each data link on this network would then have a unique network/sub network ID. Any device, or gateway, connecting *n* networks/sub networks has *n* distinct IP addresses, one for each network / sub network that it interconnects. In order to subnet a network, extend the natural mask using some of the bits from the host ID portion of the address to create a sub network ID.

**For example, given a Class C network of 204.17.5.0 which has a natural mask of 255.255.255.0, you can create subnets in this manner:**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 204.17.5.0 | 11001100. | 00010001. | 00000101. | 00000000 |
| 255.255.255.224 | **11111111.** | **11111111.** | **11111111.** | **11100000** |

By extending the mask to be 255.255.255.224, you have taken three bits (indicated by "sub") from the original host portion of the address and used them to make subnets. With these three bits, it is possible to create eight subnets. With the remaining five host ID bits, each subnet can have up to 32 host addresses, 30 of which can actually be assigned to a device *since host ids of all zeros or all ones are not allowed*. So these subnets have been created.

***Note:*** *The new subnet mask provided for an IP address or a network address to be more precise, should always be greater than the default network mask of the given class full IP / Network address. A IP Address with a new subnet mask defined for it, comes into the category of class less IP address.*

**The table on the next page describes the hosts range with the network address and subnet mask of 255.255.255.224 for each subnet created in the network 204.17.5.0.**

No. of Host Network Address Subnet Mask

**EXAMPLE 2**

In this example, two address/mask combinations are given written within the prefix/length notation, which have been assigned to two devices. The task is to determine if these devices are on the same subnet or on different subnet. One can do this by using the address and mask of each device to determine to which subnet each address belongs.

|  |  |
| --- | --- |
| DEVICE A | 172.16.17.30/20 |
| DEVICE B | **172.16.28.15/20** |

**Determining the Subnet for Device A:**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **IP Address** | *172.16.17.30* | 10101100. | 00010000. | 00010001. | 00011110 |
| **Subnet Mask** | *255.255.240.0* | 11111111. | 11111111. | 11110000. | 00000000 |
| **Sub netted Network Address** | ***172.16.16.0*** | ***10101100.*** | ***00010000.*** | ***00010000.*** | ***00000000*** |

***NOTE:*** *Looking at the address bits that have a corresponding mask bit set to one, and setting all the other address bits to zero (this is equivalent to performing a logical "AND" between the mask and address), shows you to which subnet this address belongs. In this case, Device A belongs to subnet 172.16.16.0.*

**Determining the Subnet for Device B:**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **IP Address** | *172.16.28.15* | 10101100. | 00010000. | 00011100. | 00001111 |
| **Subnet Mask** | *255.255.240.0* | 11111111. | 11111111. | 11110000. | 00000000 |
| **Sub netted Network Address** | ***172.16.16.0*** | ***10101100.*** | ***00010000.*** | ***00010000.*** | ***00000000*** |

**From these determinations, Device A and Device B have addresses that are part of the same subnet.**

## *CIDR*

Classless Inter domain Routing (CIDR) was introduced to improve both address space utilization and routing scalability in the Internet. It was needed because of the rapid growth of the Internet and growth of the IP routing tables held in the Internet routers.

CIDR moves way from the traditional IP classes (Class A, Class B, Class C, and so on). In CIDR, an IP network is represented by prefixes, which are an IP address and some indication of the length of the mask. Length means the number of left-most contiguous mask bits that are set to one. So network 172.16.0.0 255.255.0.0 can be represented as 172.16.0.0/16. CIDR also depicts a more hierarchical Internet architecture, where each domain takes its IP addresses from a higher level. This allows for the summarization of the domains to be done at the higher level. For example, if an ISP owns network 172.16.0.0/16, then the ISP can offer 172.16.1.0/24, 172.16.2.0/24, and so on to customers. Yet, when advertising to other providers, the ISP only needs to advertise 172.16.0.0/16.

**IP ROUTING**

The term routing is used for taking a packet from one device and sending it through the network to another device on a different network. Routers choose best path to each network.

The logical network address of the destination host is used to get packets to a network through a routed network, and then the hardware address of the host is used to deliver the packet from a router to the correct destination host.

Routers route traffic to all the networks in your network. *To route packets router must know the following:*

* Destination address.
* Neighbor routers from which it can learn about remote networks.
* Possible routes to all remote networks.
* The best route to each network.
* How to maintain and verify routing information.

The router learns about remote networks from neighbor routers or from an administrator. Then router builds a routing table that describes how to find the remote networks.

If a network is directly connected, then the router already knows how to get it and if it isn't then the router must use one of the two ways to learn how to get to the remote network. Following are the two ways:

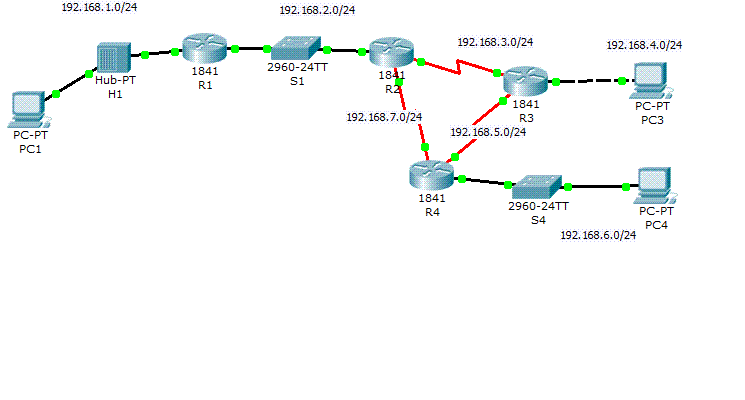


Fig 6.1) IP Routing taking place over a network

* 1. ***TYPES OF ROUTING***

1. *Static routing.*
2. *Dynamic routing.*
   * 1. ***Static routing***

It is responsible for updating all the changes by hand into all routers. It occurs when we manually add routes in each routers routing table.

**BENEFITS:**

* There is no overhead on the router CPU, meaning a cheap router can work.
* No bandwidth usage between routers that means money can be saved on wan links.
* It adds security.

**DISADVANTAGES:**

* The administrator must understand the internetwork and how each router is connected in order to configure the routers correctly.
* Not feasible for large networks.
* If a network is added to the network the administrator has to add routes to all the routers by hand.
  + 1. ***Dynamic Routing***

In dynamic routing a protocol on one router communicates with the same protocol running on the neighbor router. The routers then update each other about all the networks they know about and place this information into the routing table. If a change occurs in the network, the dynamic routing protocols automatically inform all the routers about the event.

**BENEFIT:**

* This is easier than static routing since it does not require any manual handling of the routers.

**DISADVANTAGES:**

* It costs in terms of router CPU processes and bandwidth on the network links.
  1. ***PROTOCOLS***

Protocols are the rules that are used in internetworking between different networks.

**THREE CLASSES OF ROUTING PROTOCOLS**

1. **Distance vector routing protocols:** Finds the best path to a remote network by judging distance.
2. **Link state routing protocol (shortest path first protocol):** Creates three separate tables. One keeps track of directly attached neighbors, one determines topology another used as a routing table.
3. **Hybrid routing protocol:** Use aspects of both distance vector and link state routing.

**Protocols used in dynamic routing are:**

* RIP (ROUTING INFORMATION PROTOCOL)
* IGRP(INTERIOR GATEWAY ROUTING PROTOCOL)
* OSPF(OPEN SHORTEST PATH FIRST)
* BGP(BORDER GATEWAY PROTOCOL)
* EGP(EXTERIOR GATEWAY PROTOCOL)

***In this project RIP v1 is the protocol that is used in configuring the routers under dynamic routing.***

* 1. ***RIP: (ROUTING INFORMATION PROTOCOL)***
* True distance vector routing protocol.
* Sends the complete routing table out to all active interfaces every 30 seconds.
* Uses hop count to determine the best way to a remote network.
* Maximum allowable hop count of 15 by default, meaning that 16 is deemed unreachable.
* RIP v1 uses only class full routing, which means that all devices in the network must use the same subnet mask.

## *Versions*

There are three versions of the Routing Information Protocol: *RIPv1*, *RIPv2*, and *RIPng*.

### RIP version 1

The original specification of RIP uses [classful](http://en.wikipedia.org/wiki/Classful_address) routing. The periodic routing updates do not carry subnet information, lacking support for variable length subnet masks (VLSM). This limitation makes it impossible to have different-sized subnets inside of the same network class. In other words, all subnets in a network class must have the same size. There is also no support for router authentication, making RIP vulnerable to various attacks.

### RIP version 2

Due to the deficiencies of the original RIP specification, RIP version 2 (RIPv2) was developed in 1993 and last standardized in 1998. It included the ability to carry subnet information, thus supporting Classless Inter-Domain Routing (CIDR). To maintain backward compatibility, the hop count limit of 15 remained. RIPv2 has facilities to fully interoperate with the earlier specification if all *Must Be Zero* protocol fields in the RIPv1 messages are properly specified. In addition, a *compatibility switch* feature allows fine-grained interoperability adjustments.

In an effort to avoid unnecessary load on hosts that do not participate in routing, RIPv2 *multicasts* the entire routing table to all adjacent routers at the address 224.0.0.9, as opposed to RIPv1 which uses broadcast. Unicast addressing is still allowed for special applications

### RIPng

RIPng (RIP next generation), is an extension of RIPv2 for support of IPv6, the next generation Internet Protocol. The main differences between RIPv2 and RIPng are:

* Support of IPv6 networking.
* While RIPv2 supports RIPv1 updates authentication, RIPng does not. IPv6 routers were, at the time, supposed to use IP sec for authentication.
* RIPv2 allows attaching arbitrary tags to routes, RIPng does not;
* RIPv2 encodes the next-hop into each route entries; RIPng requires specific encoding of the next hop for a set of route entries.

**RIP TIMERS:**

* Route update timer: 30 seconds
* Route invalid timer: 180 seconds
* Hold down timer: default is 180 seconds
* Route flush timer: 240 seconds

**Q) How RIP works?**

**A)** What makes RIP work is a routing database that stores information on the fastest route from computer to computer, an update process that enables each router to tell other routers which route is the fastest from its point of view, and an update algorithm that enables each router to update its database with the fastest route communicated from neighboring routers:

* **Database.** Each RIP router on a given network keeps a database that stores the following information for every computer in that network:
  + **IP Address.** The Internet Protocol address of the computer.
  + **Gateway.** The best gateway to send a message addressed to that IP address.
  + **Distance.** The number of routers between this router and the router that can send the message directly to that IP address.
  + **Route change flag.** A flag that indicates that this information has changed, used by other routers to update their own databases.
  + **Timers.** Various timers.

## *Limitations*

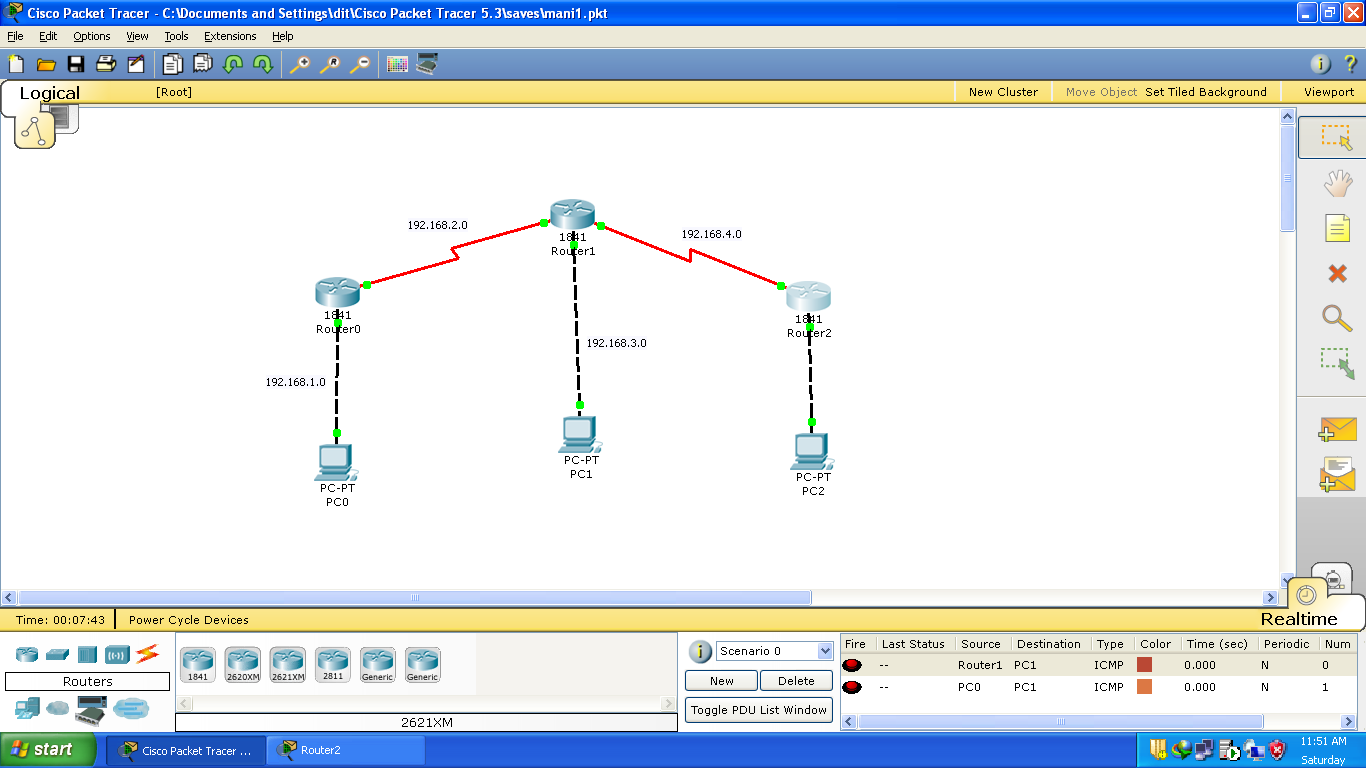
* Without using RMTI, Hop count cannot exceed 15, in the case that it exceeds this limitation, it will be considered invalid.
* Most RIP networks are flat. There is no concept of areas or boundaries in RIP networks.
* Variable Length Subnet Masks were not supported by RIP version 1.
* Without using RMTI, RIP has slow convergence and count to infinity problems.

Project Description

The laying, designing and configuration of the networks are performed on **CISCO PACKET TRACER**. *Packet Tracer* is a Cisco router simulator that is utilized in training and education, but also in research for simple computer network simulations. The version that we have worked on is Packet Tracer5.3.2.

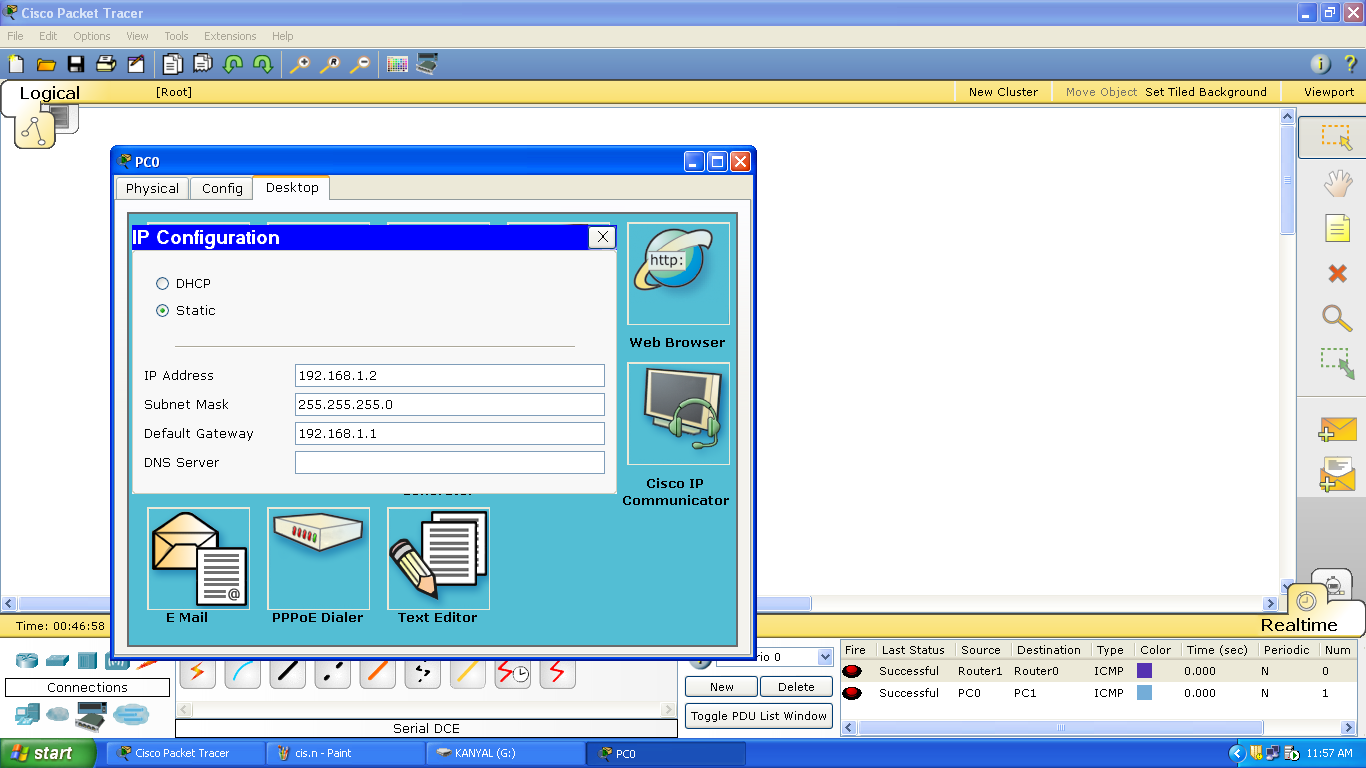
Configuration of routers is done using commands that are mentioned in the following pages. We have performed Static routing and dynamic routing using RIP.

* 1. ***NETWORK DESIGNING AND CONFIGURATION***
     1. ***STATIC ROUTING***



**CONFIGURATION**

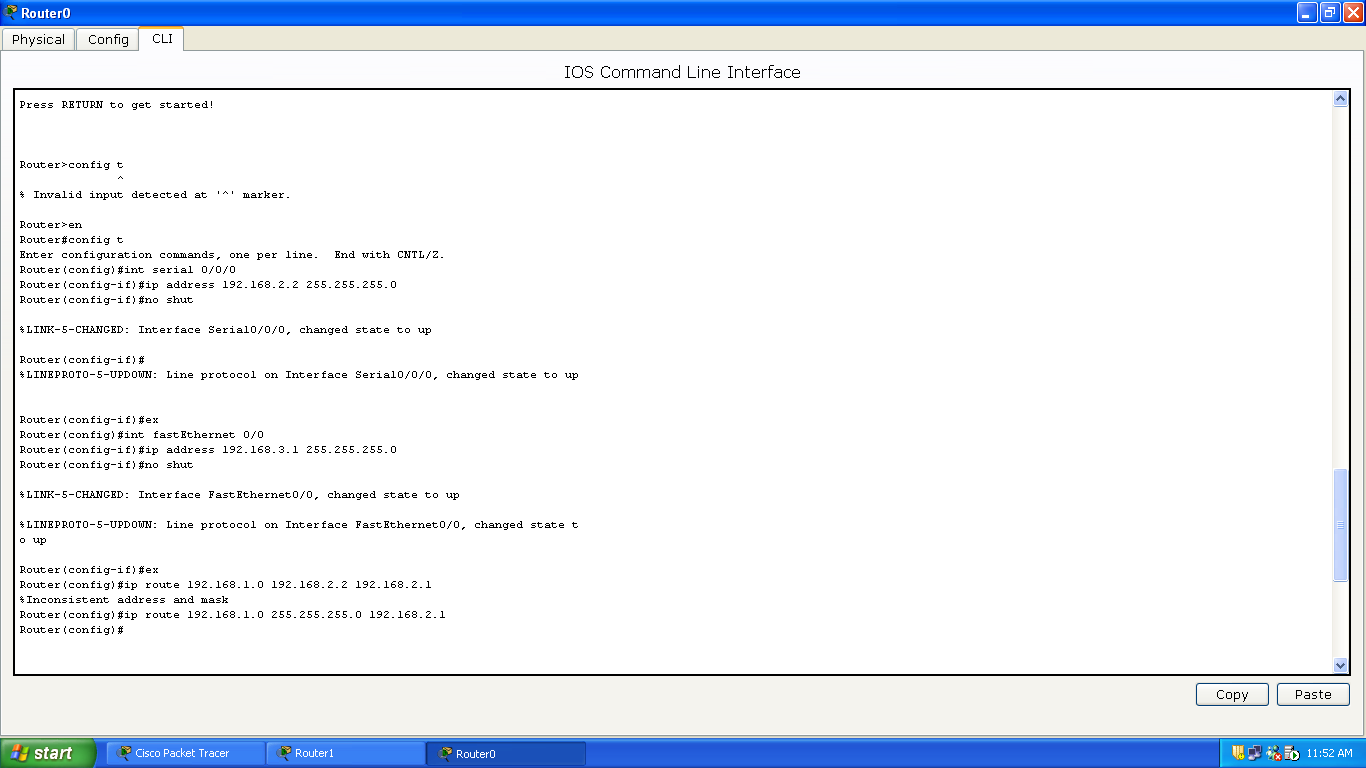
**1.** Communicating device-PC



This shows the configuration of PC. The IP address, subnet mask and gateway address is assigned to the communicating device. It is connected to the router using crossover cable through fast Ethernet port.

**2.** Router

The commands are written in CLI which is IOS Command Line Interface in this case.



**Commands:**

1. Router>en
2. Router#config t
3. Enter configuration commands, one per line. End with CNTL/Z.
4. Router(config)#int serial 0/0/0
5. Router(config-if)#ip address 192.168.2.2 255.255.255.0
6. Router(config-if)#no shut

%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up

1. Router(config-if)#

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up

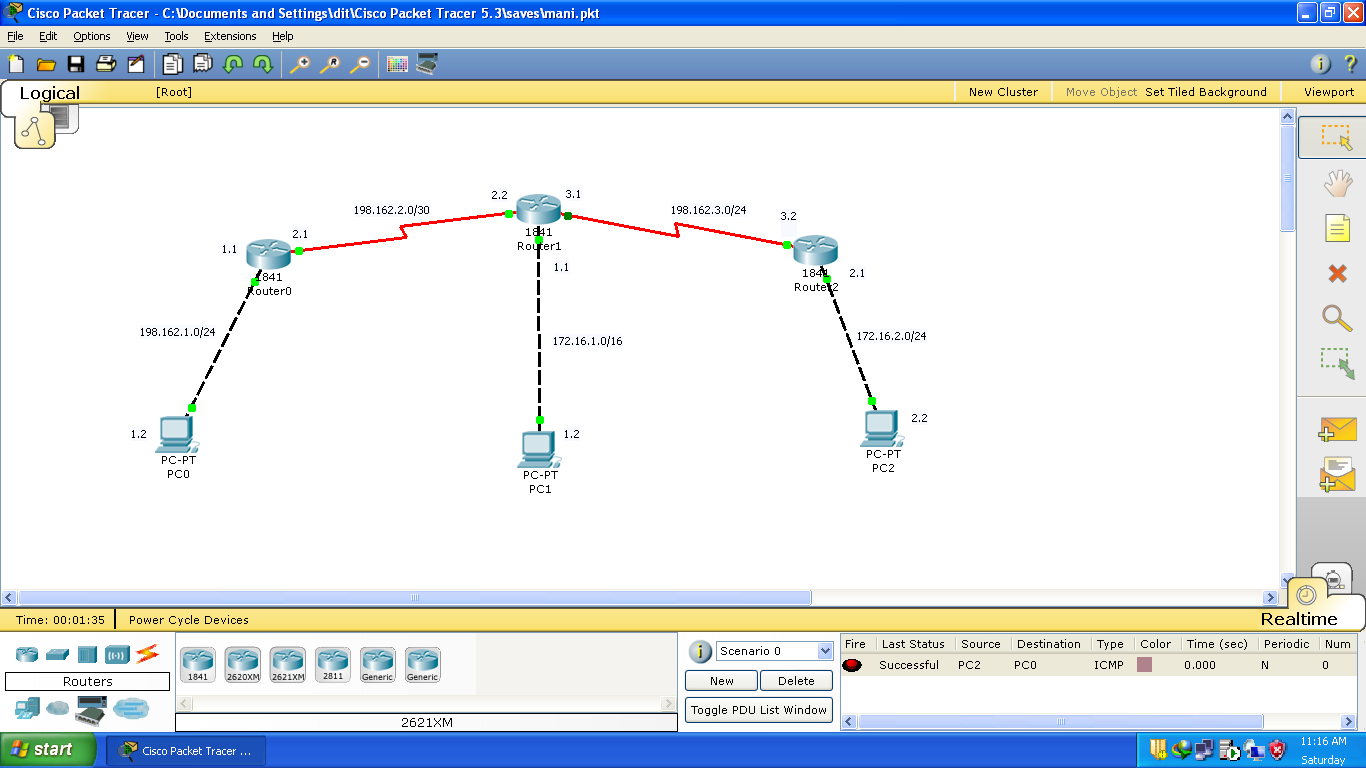
1. Router(config-if)#ex
2. Router(config)#int fastEthernet 0/0
3. Router(config-if)#ip address 192.168.3.1 255.255.255.0
4. Router(config-if)#no shut

%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

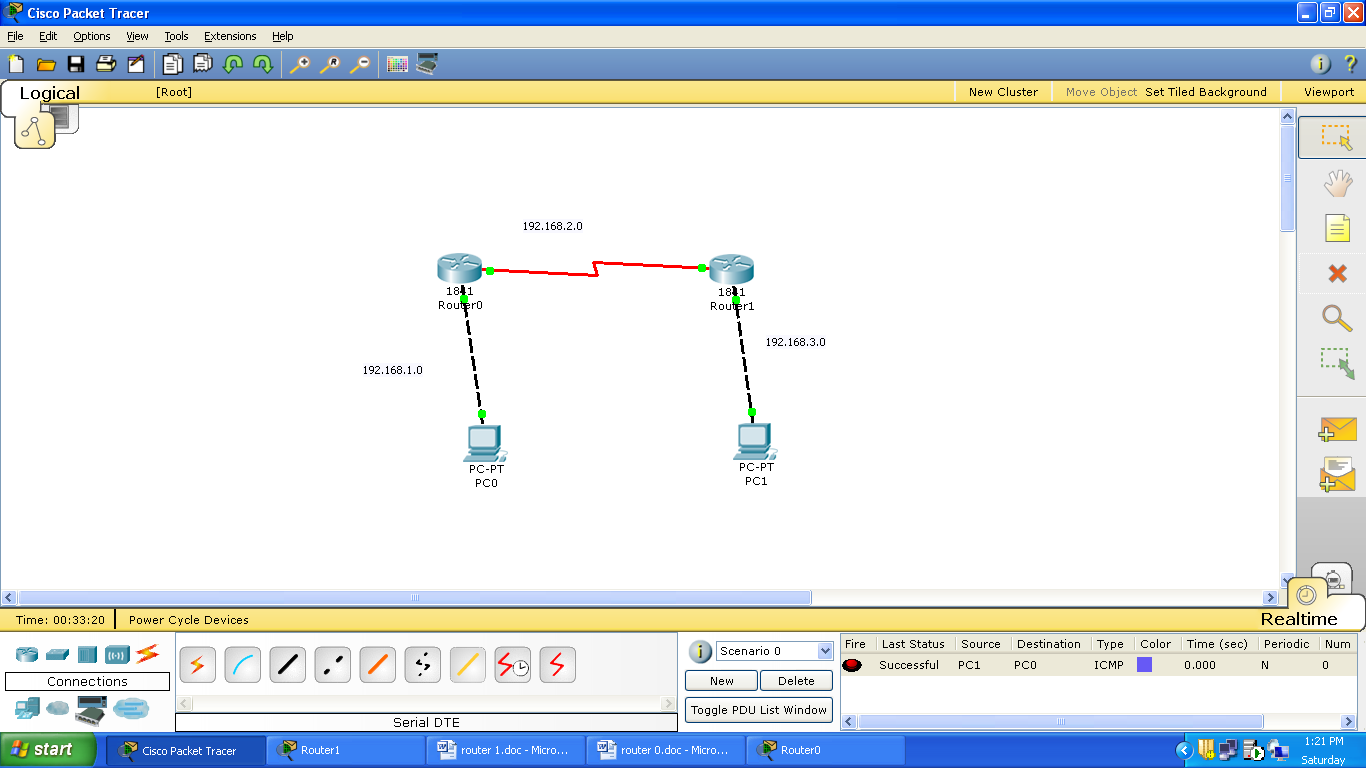
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up

1. Router(config-if)#ex
2. Router(config)#ip route 192.168.1.0 192.168.2.2 192.168.2.1
3. %Inconsistent address and mask
4. Router(config)#ip route 192.168.1.0 255.255.255.0 192.168.2.1
5. Router(config)#
   * 1. ***Dynamic Routing***

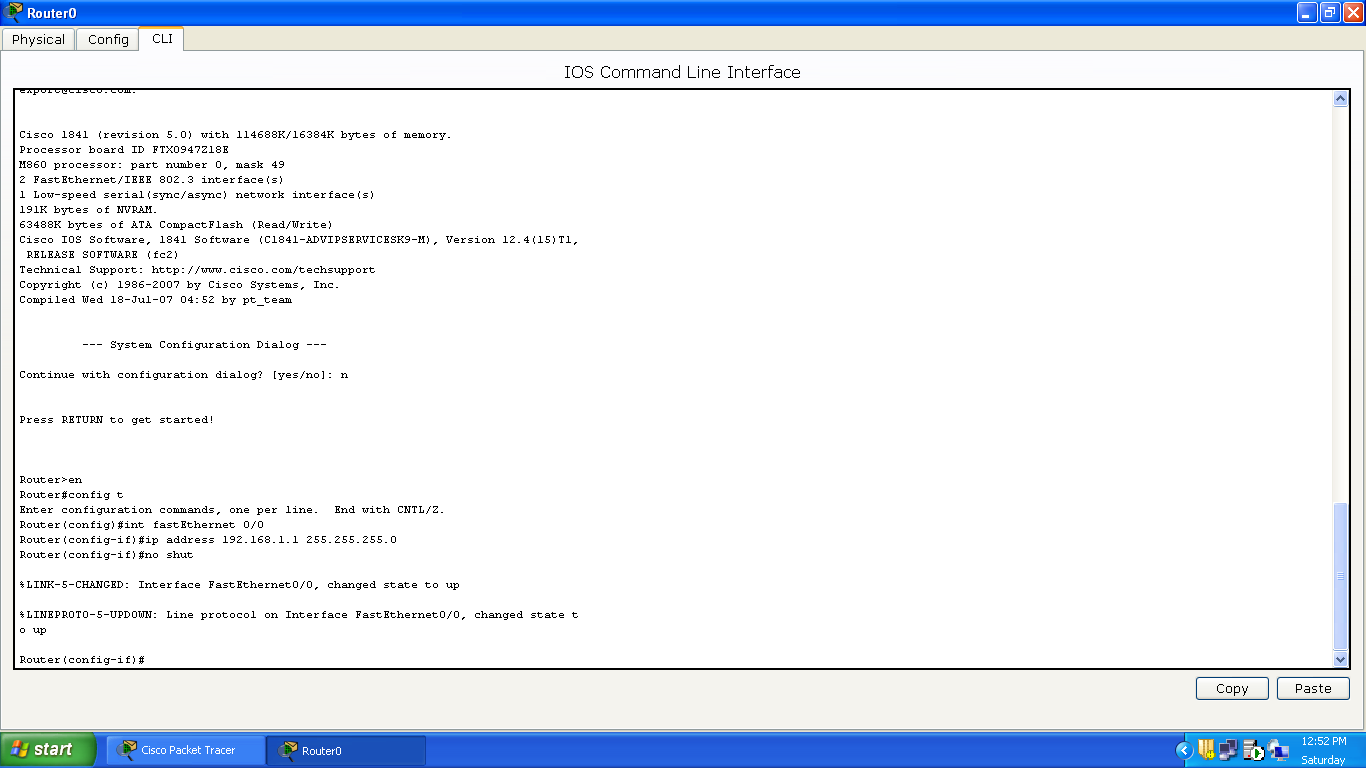
In dynamic routing a protocol on one router communicates with the same protocol running on the neighbor router. The routers then update each other about all the networks they know about and place this information into the routing table. If a change occurs in the network, the dynamic routing protocols automatically inform all the routers about the event.



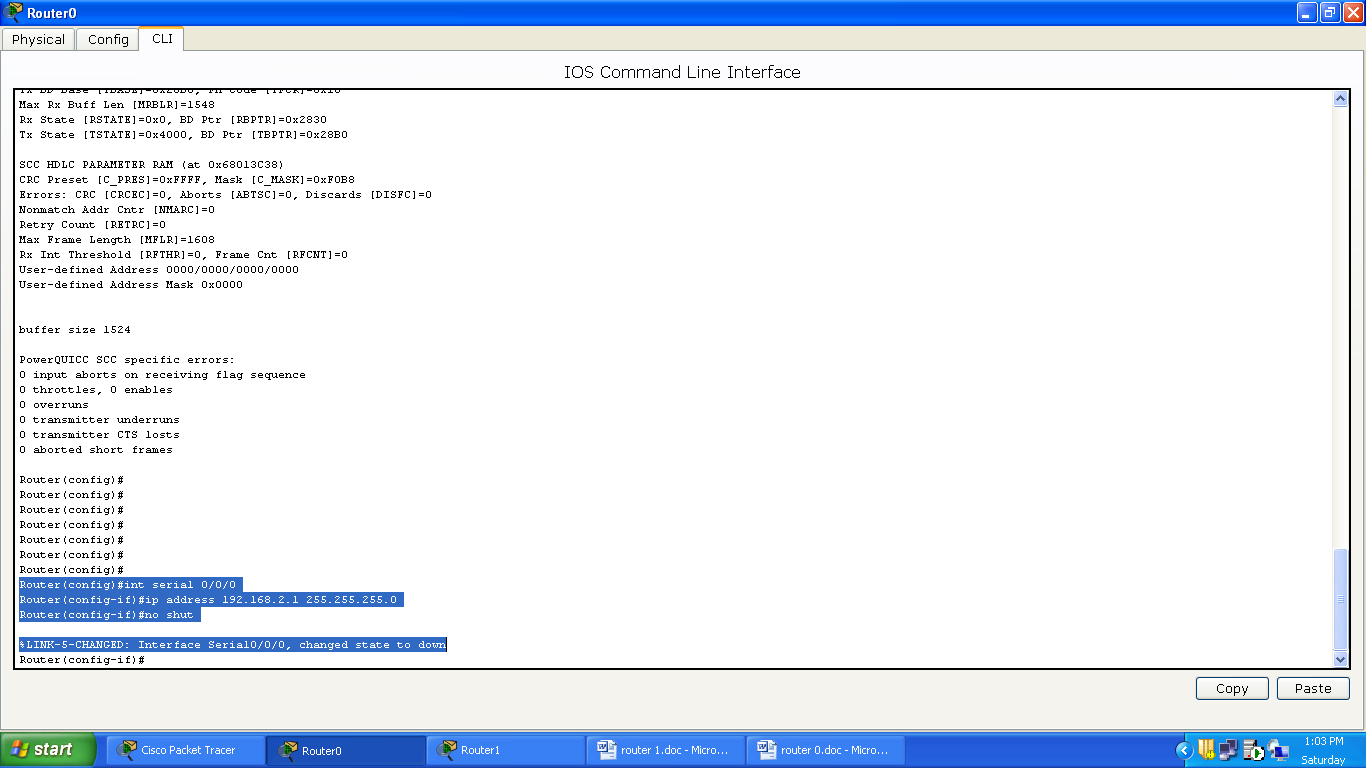
**The Configuration of Router in this case (using RIP can be shown as:**



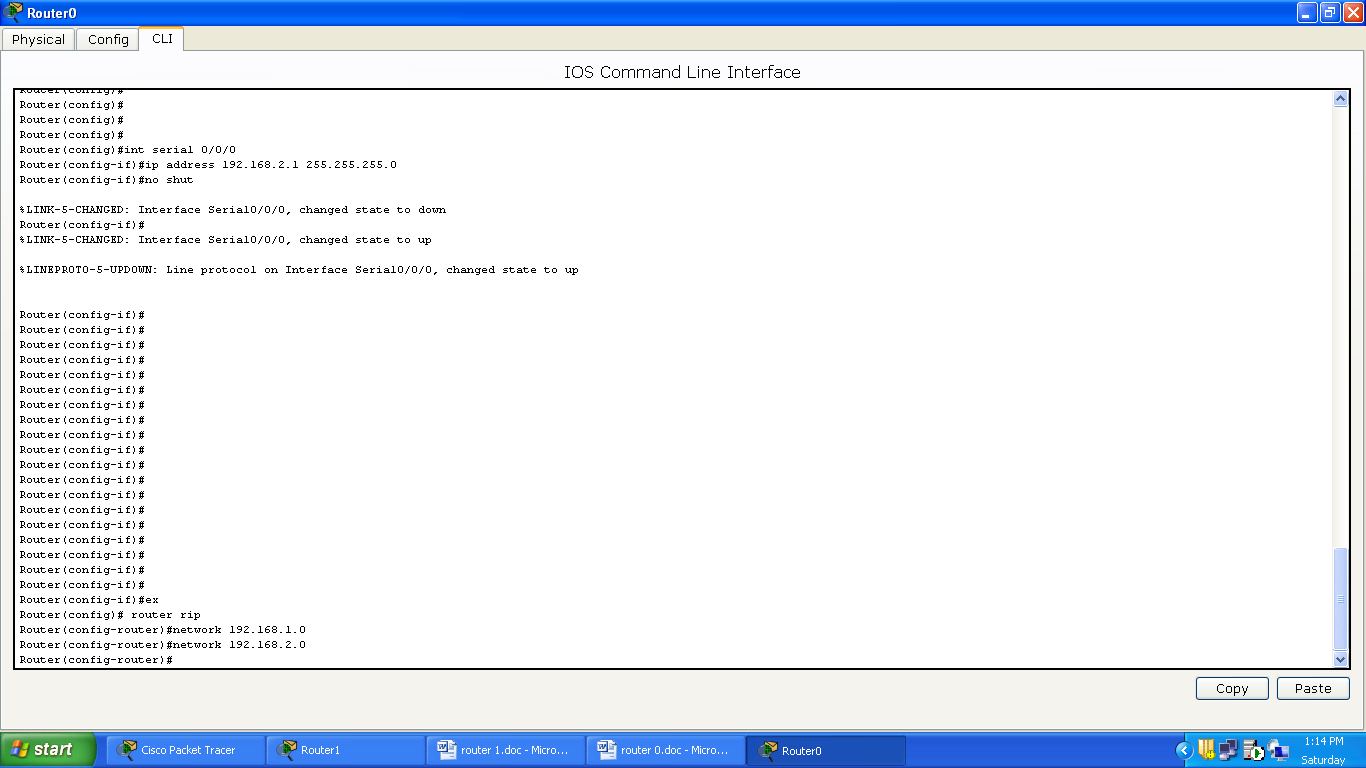
**1)** Assigning IP address to routers to communicate with PC.



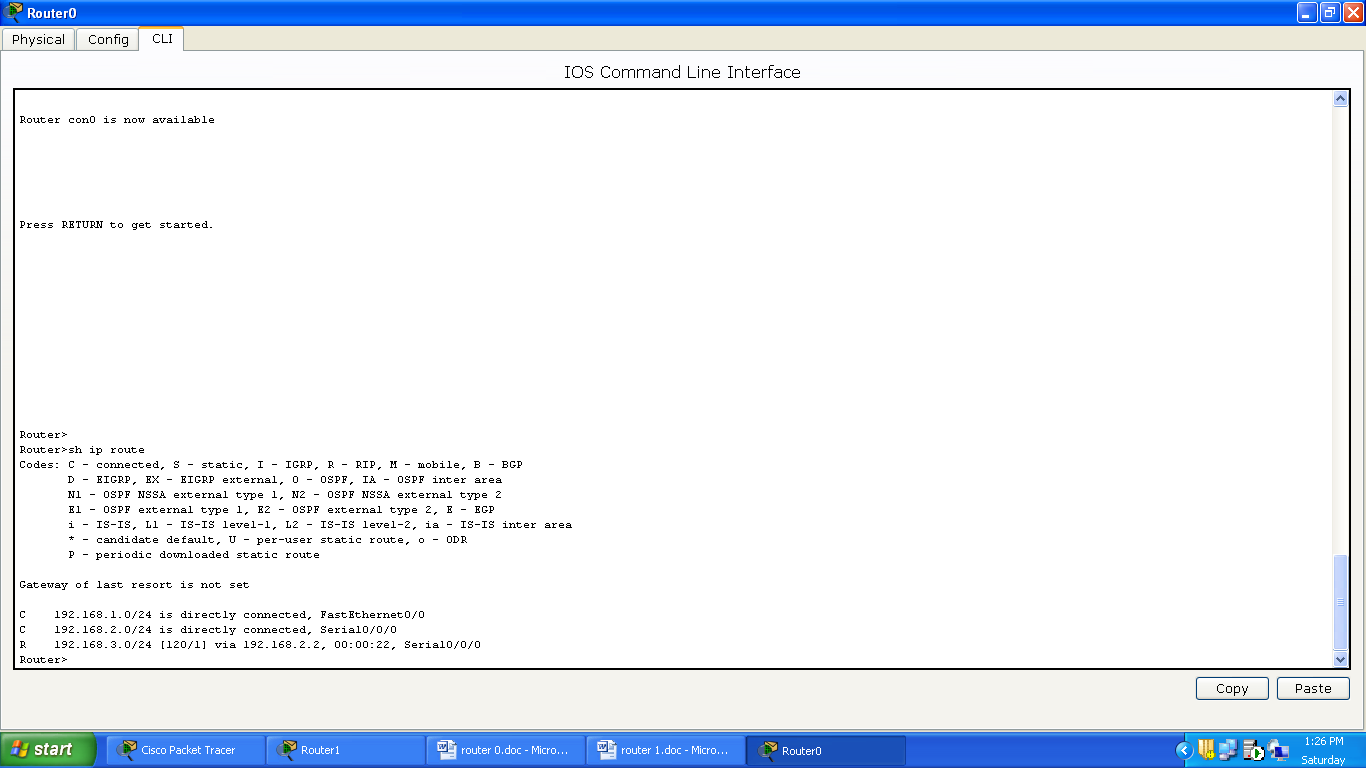
**2)** Connection between routers through serial port:



**3)** Routing between two networks



***THE ROUTING TABLE IS BUILT AS:***



**COMMANDS:**

1. Router>en
2. Router#config t
3. Enter configuration commands, one per line. End with CNTL/Z.
4. Router(config)#int fastEthernet 0/0
5. Router(config-if)#ip address 192.168.1.1 255.255.255.0
6. Router(config-if)#no shut

%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

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

1. Router(config)#int serial 0/0/0
2. Router(config-if)#ip address 192.168.2.1 255.255.255.0
3. Router(config-if)#no shut

%LINK-5-CHANGED: Interface Serial0/0/0, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up

1. Router(config-if)#ex
2. Router(config)# router rip
3. Router(config-router)#network 192.168.1.0
4. Router(config-router)#network 192.168.2.0
5. Router(config-router)#ex
6. Router(config)#ex
7. Router>sh ip route

**---Routing Table---**

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP

D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area

N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2

E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP

i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area

\* - candidate default, U - per-user static route, o - ODR

P - Periodic downloaded static route

Gateway of last resort is not set

C 192.168.1.0/24 is directly connected, FastEthernet0/0

C 192.168.2.0/24 is directly connected, Serial0/0/0

R 192.168.3.0/24 [120/1] via 192.168.2.2, 00:00:22, Serial0/0/0

**CONCLUSION**

The problems that a LAN network faced were removed using switches, hubs, repeaters, bridges and gateways. The drawbacks of RIP are such that, pinhole congestion makes it less efficient than IGRP when different bandwidths are used.

Thus, Static routing has some enormous advantages over dynamic routing. Chief among these advantages is predictability. Because the network administrator computes the routing table in advance, the path a packet takes between two destinations is always known precisely, and can be controlled exactly. With dynamic routing, the path taken depends on which devices and links are functioning, and how the routers have interpreted the updates from other routers.