Advances in Computer Science and Information Technology (ACSIT)
p-ISSN: 2393-9907; e-ISSN: 2393-9915; Volume 4, Issue 5; October-December, 2017, pp. 285-291
© Krishi Sanskriti Publications
http://www.krishisanskriti.org/Publication.html

Implementation of a Company Network Scenario Module by using Cisco Packet Tracer Simulation Software

Ashish Kumar

*U.G. Student, Delhi Technical Campus Sunshine Education and Development Society,
29/1 Knowledge Park - III, Greater Noida (Affiliated to GGSIPU University, Delhi)
E-mail: singh.ashish.kr96@gmail.com*

Abstract—*The enterprise network is the lifeblood of any Small to Medium Enterprise (SME) with more than one site or supply chain partner. It enables access to business information and allows for profitable and effective communication flows between employees in different enterprise sites. Network enterprise network equipment is mature and ubiquitous, but the quality of services provided by similar networks varies from city to city and from country to country. In particular, the quality variation gap between most of the cities in some developing nations and their counterparts in advanced nations is very wide. This is due to the lack in developing nations of an adequate IT infrastructure, which is taken for granted in developed nations. This study briefly discusses the architecture of an enterprise network. It examines the barriers to planning, designing and implementing an enterprise network. This study also covers the methods to implement enterprise level networks. A basic router configuration is used for covering the Routing technologies which route data between branches. After that we have implement Wide Area Network (WAN) and Frame-relay is considered a good choice because it connects multiple location using single interface of router and reduce the hardware costs. For Internet connectivity we are also using frame relay. In this setup Network Address Translation (NAT) is very essential in which we have translate live Internet Protocol (IP) into local and vice-versa.*

Index Terms*: Routing technologies, NAT, SME, IP, Frame relay, WAN.*

1. INTRODUCTION

Implementing a company network scenario is totally network based. IT is a secured network often used in big organizations and other institutions to make a secured communication and sharing's of their documents, files, etc. should also be secured. As we know that there are many departments in an organization. So we desire that these departments should be separate for their good output. Then this project also includes this feature. This type of network avoids the unauthorized access it authenticate the authorized users or hosts. Implementation of logical network topology has been done. All the routers have their password to access them by any user. This network connects the different department of a company or many companies and combines them in a single network. And the implementations of router are very accurate, that they should select the excellent path for the packets and make the communication fast and secure. In the developed scenario adaptive bitrate technology has been used. Adaptive bitrate streaming is a technique used in streaming multimedia over computer networks. A distance vector protocol is implemented in the project and the routers are password protected for security purpose.

In this setup Network Address Translation (NAT) [1] is very essential in which we have translate live Internet Protocol (IP) into local and vice-versa. The fundamental purpose of designing this scenario is to provide security in your network to secure your private data and make a reliable and excellent communication in a WAN connection and reduce the organization dependency on floppy disks etc. Organizations that share data through the use of floppy disks follow a non-efficient or cost-effective method. The issue is that the business by using this method to share data leads to duplication of data which effects the growth of the business. Using this method leads to a major issue i.e. Lack of communication- all details are not possible to be conveyed at the required time. The scope of creating company network scenario is to have a secure WAN network for the communication purpose of an company that eradicate data redundancy from the grass root level which shows smooth functioning of a network.

2. OVERVIEW

2.1 ROUTING INFORMATION PROTOCOL (RIP)

The Routing Information Protocol (RIP) is one of the oldest distance-vector routing protocols which employ the hop count as a routing metric. RIP prevents routing loops by implementing a limit on the number of hops allowed in a path from source to destination. The maximum number of hops allowed for RIP is 15, which limits the size of networks that RIP can support. A hop count of 16 is considered an infinite distance and the route is considered unreachable. RIP implements the split horizon, route poisoning & hold down mechanisms to prevent incorrect routing information from being propagated.

Originally, each RIP router transmitted full updates every 30 seconds. In the early deployments, routing tables were small enough that the traffic was not significant. As networks grew in size, however, it became evident there could be a massive traffic burst every 30 seconds, even if the routers had been initialized at random times. It was thought, as a result of random initialization, the routing updates would spread out in time, but this was not true in practice. [2] Sally Floyd and Van Jacobson showed in 1994that, without slight randomization of the update timer, the timers synchronized over time.In most networking environments, RIP is not the preferred choice for routing as its time to converge and scalability are poor compared to EIGRP, OSPF, or IS-IS. However, it is easy to configure, because RIP does not require any parameters unlike other protocols. [3] RIP uses the User Datagram Protocol (UDP) as its transport protocol, and is assigned the reserved port number 520.

Features: -RIP is a distance vector routing protocol (DVR). The maximum reachable hop-count is 15 the 16 Hop is considered unreachable. In RIP metric is HOP COUNT. periodic update after every 30 seconds takes place in this protocol. It supports equal path load balancing and works at application layer.

RIP Timers: -RIP uses different kinds of timers to regulate its performance:-

Route update timer: Sets the interval (typically 30 seconds) between periodic routing updates, in which the router sends a complete copy of its routing table out to all neighbours.

Route invalid timer: Determines the length of time that must elapse (180 seconds) before a router determines that a route has become invalid. It will come to this conclusion if it hasn't heard any updates about a particular route for that period. When that happens, the router will send out updates to all its neighbours letting them know that the route is invalid.

Hold down timer: This sets the amount of time during which routing information is suppressed. Routes will enter into the hold down state when an update packet is received that indicated the route is unreachable. This continues until either an update packet is received with a better metric or until the hold down timer expires. The default is 180 seconds.

Route flush timer: Sets the time between a route becoming invalid and its removal from the routing table (240 seconds). Before it's removed from the table, the router notifies its neighbours of that route's impending demise. The value of the route invalid timer must be less than that of the route flush timer. This gives the router enough time to tell its neighbours about the invalid route before the local routing table is updated.

2.2 LAN SWITCHING

Switches are a fundamental part of most networks [4]. They let multiple users communicate directly with each other. As such, they offer the potential for collision-free, high-speed networking. In essence, switches create a system of simultaneous, parallel, point-to-point connections between pairs of devices. Benefits of LAN switches:

Increased network scalability:-The network can expand easily as the business grows.

Improved bandwidth performance for each network user:- This is important in environments where users operate multimedia applications or conduct frequent client/server database interactions.

Multiple simultaneous connections:-Many simultaneous data transfers can take place between pairs of devices connected to switch ports. This is not possible with hub-based networks.

Reduced congestion and information transmission delay:- This translates to more efficient business application access. Remember that network segmentation is used to minimize the number of users contending for LAN bandwidth on each segment (switch port).

No single point of failure:-With proper network design, there are fewer chances for network failure.

Improved manageability and security through the use of virtual LANs (VLANs):-VLANs group individual users into logical workgroups with common interests or business functions. Data broadcasts are restricted to designated members of the group (also called the *broadcast domain*). This functionality gives companies the flexibility to move employees around physically yet still maintain their functional ties via the VLAN without network reconfiguration. VLANs are discussed in more depth later in this chapter.

A small-medium business can choose from a variety of switch types. The most popular options are the following:

Layer 2 switches:-Also called desktop or workgroup switches.

Layer 3 switches:-Also called routing switches or multilayer switches.

2.2.1 VLAN (Virtual LAN)

VLAN provides Virtual Segmentation of Broadcast Domain in the network. The devices, which are member of same Vlan, are able to communicate with each other. The devices of different Vlan may communicate with each other with routing. So that different Vlan devices will use different network addresses. A virtual LAN (VLAN) is any broadcast domain thatis partitioned and isolated in a computer network at the data link layer (OSI layer 2)[5-6]. LAN is the abbreviation for local area network and in this context virtual refers to a physical object recreated and altered by additional logic. Vlanprovides following advantages:

Security:-Groups that have sensitive data are separated from the rest of the network, decreasing the chances of confidential information breaches.

Cost reduction:-Cost savings result from less need for expensive network upgrades and more efficient use of existing bandwidth and uplinks. Some of the savings are reduced by administrative costs needed for IT staff to configure VLANs into switches.

Higher performance:-Dividing flat Layer 2 networks into multiple logical workgroups (broadcast domains) reduces overall network utilization and boosts performance.

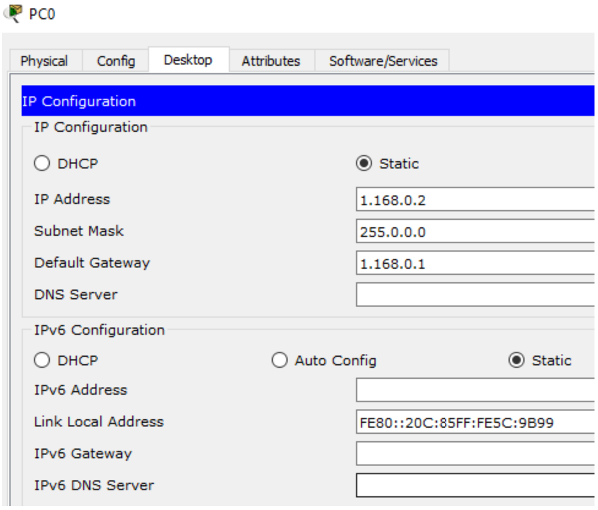
Broadcast storm mitigation:-Dividing a network into smaller logical networks results in lower susceptibility to broadcast storms.

Simpler project or application management:-VLANs bring together all required players in a way that makes managing a project or working with a specialized application easier.

Improved IT staff efficiency:-Moves, adds, and changes are easier and less expensive to perform. Network administrators' time is freed up for proactive network management.

2.3 IP Addresses

An Internet Protocol address (IP address) is a numerical label assigned to each device connected to a computer network that uses the Internet Protocol for communication.[7] An IP address serves two principal functions: host or network interface identification and location addressing.



PC0

Physical | Config | Desktop | Attributes | Software/Services

IP Configuration

IP Configuration

○ DHCP ● Static

IP Address: 1.168.0.2

Subnet Mask: 255.0.0.0

Default Gateway: 1.168.0.1

DNS Server:

IPv6 Configuration

○ DHCP ○ Auto Config ● Static

IPv6 Address:

Link Local Address: FE80::20C:85FF:FE5C:9B99

IPv6 Gateway:

IPv6 DNS Server:

Figure I: Assigning IP address and Default gateway to a PC

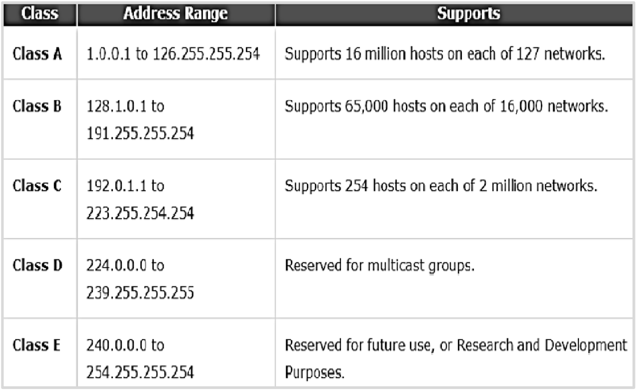
An IP address serves two principal functions:

- It identifies the host, or more specifically its network interface.
- It provides the location of the host in the network, and thus the path required to communicate with that host.

The role of the address has been characterized in context as follows: "A name indicates what we seek. An address indicates where it is. A route indicates how to get there [8]."

The header of each IP packet contains the IP address of the sending host, and that of the destination host. A host may use geolocation software to deduce the geolocation of its communicating peer [9].

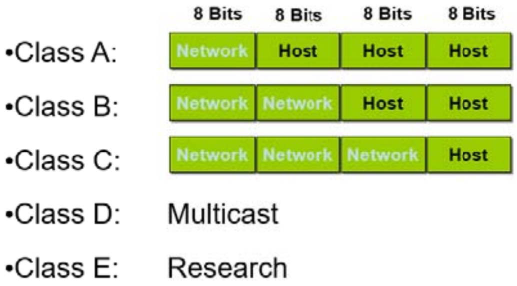
Table 1: Showing address range for different Class IP addresses



Class	Address Range	Supports
Class A	1.0.0.1 to 126.255.255.254	Supports 16 million hosts on each of 127 networks.
Class B	128.1.0.1 to 191.255.255.254	Supports 65,000 hosts on each of 16,000 networks.
Class C	192.0.1.1 to 223.255.254.254	Supports 254 hosts on each of 2 million networks.
Class D	224.0.0.0 to 239.255.255.255	Reserved for multicast groups.
Class E	240.0.0.0 to 254.255.255.254	Reserved for future use, or Research and Development Purposes.

IPv4 Address Formats

IP addressing is accompanied by a two-tiered network address, consisting of the network's address and a host address.



	8 Bits	8 Bits	8 Bits	8 Bits
•Class A:	Network	Host	Host	Host
•Class B:	Network	Network	Host	Host
•Class C:	Network	Network	Network	Host
•Class D:	Multicast			
•Class E:	Research			

Figure II: Host and Network Bits allocation

Class A Addresses

The Class A IPv4 address was designed to support extremely large networks. As the need for very large-scale networks was perceived to be minimal, architecture was developed that maximized the possible number of host addresses but severely limited the number of possible Class A networks that could be defined.A Class A IP address uses only the first octet to indicate the network address. The remaining three octets enumerate host addresses. The first bit of a Class A address is always a 0. This mathematically limits the possible range of the Class A address to 127, which is the sum of 64 + 32 + 16 + 8 + 4 + 2 + 1. The leftmost bit's decimal value of 128 is absent from this equation. Therefore, there can only ever be 127 possible Class A IP networks.

The last 24 bits of a Class A address represent possible host addresses. The range of possible Class A network addresses is from 1.0.0.0 to 126.0.0.0.

Class B Addresses

The Class B addresses were designed to support the needs of moderate- to large-sized networks. The range of possible Class B network addresses is from 128.1.0.0 to 191.254.0.0. The mathematical logic underlying this class is fairly simple. A Class B IP address uses two of the four octets to indicate the network address. The other two octets enumerate host addresses. The first 2 bits of the first octet of a Class B address are 10. The remaining 6 bits may be populated with either 1s or 0s.This mathematically limits the possible range of the Class B address space to 191, which is the sum of 128 + 32 + 16 + 8 + 4 + 2 + 1. The last 16 bits (two octets) identify potential host addresses. Each Class B address can support 65,534 unique host addresses.

Class C Addresses

The Class C address space is, by far, the most commonly used of the original IPv4 address classes. This address space was intended to support a lot of small networks. This address class can be thought of as the inverse of the Class A address space. Whereas the Class A space uses just one octet for network numbering, and the remaining three for host numbering, the Class C space uses three octets for networking addressing and just one octet for host numbering.The first 3 bits of the first octet of a Class C address are 110. The first 2 bits sum to a decimal value of 192 (128 + 64). This forms the lower mathematical boundary of the Class C address space. The third bit equates to a decimal value of 32. Forcing this bit to a value of 0 establishes the upper mathematical boundary of the address space. Lacking the capability to use the third digit limits the maximum value of this octet to 255 - 32, which equals 223. Therefore, the range of possible Class C network addresses is from 192.0.1.0 to 223.255.254.0.

The last octet is used for host addressing. Each Class C address can support a theoretical maximum of 256 unique host addresses (0 through 255), but only 254 are usable because 0 and 255 are not valid host numbers. There can be 2,097,150 different Class C network numbers.

Class D Addresses

The Class D address class was created to enable multicasting in an IP network. The Class D multicasting mechanisms have seen only limited usage. A multicast address is a unique network address that directs packets with that destination address to predefined groups of IP addresses. Therefore, a single station can simultaneously transmit a single stream of datagram’s to multiple recipients. The need to create separate streams of datagram’s, one for each destination, is eliminated. Routers that support multicasting would duplicate the datagram and forward as needed to the predetermined end systems. Multicasting has long been deemed a desirable feature in an IP network because it can substantially reduce network traffic.

The Class D address space, much like the other address spaces, is mathematically constrained. The first 4 bits of a Class D address must be 1110. Pre-setting the first 3 bits of the first octet to 1s means that the address space begins at 128 + 64 + 32, which equals 224. Preventing the fourth bit from being used means that the Class D address is limited to a maximum value of 128 + 64 + 32 + 8 + 4 + 2 + 1, or 239.Therefore, the Class D addresses space ranges from 224.0.0.0 to 239.255.255.254.This range may seem odd because the upper boundary is specified with all four octets. Ordinarily, this would mean that the octets for both host and network numbers are being used to signify a network number. There is a reason for this. The Class D address space isn't used for internetworking to individual end systems or networks. Class D addresses are used for delivering multicast datagram’s within a private network to groups of IP-addressed end systems. Therefore, there isn't a need to allocate octets or bits of the address to separate network and host addresses. Instead, the entire address space can be used to identify groups of IP addresses (Classes A, B, or C).

Class E Addresses

A Class E address has been defined, but is reserved by the IETF for its own research. Therefore, no Class E addresses have been released for use in the Internet. The first 4 bits of a Class E address are always set to 1s; therefore, the range of valid addresses is from 240.0.0.0 to 255.255.255.255.

2.4 NETWORK TOPOLOGY

Network topology is the arrangement of the various elements (links, nodes, etc.) of a communication network.[10-11]

Network topology is the topological[12] structure of a network and may be depicted physically or logically. Physical topology is the placement of the various components of a network, including device location and cable installation, while logical topology illustrates how data flows within a network. Distances between nodes, physical interconnections, transmission rates, or signal types may differ between two networks, yet their topologies may be identical.

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

3. SCENARIO DESIGNED

This project consist of 5 routers the main router is the Delhi Router which is further connected to Nirman Vihar and Vaishali router which are connected to Dwarka and Ghaziabad router respectively. The main Delhi Router is Password protected and it is assumed that headquarter of the company is located there. The other offices of the company are located at different places like: Dwarka, NirmanVihar, Ghaziabad and Vaishali.

Further to keep this project simple use of limited number of Computers and Laptops are there for the easy understanding to the users. Copper straight-through and copper cross over cables are used to connect routers with switches and switches with PCs. laptops are connected to the network with the help of wireless routers. Serial DTE (Data Terminal Equipment) cable is used to connect routers together.

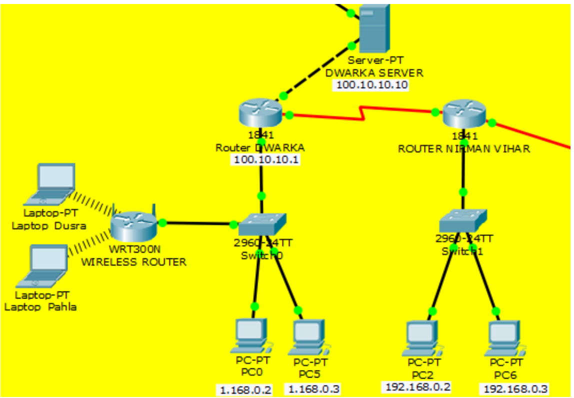


Figure III: Dwarka& Nirman Vihar Router

The above figure 1 shows Router DWARKA and Router NIRMAN VIHAR which are connected to each other with the help of Serial DTE cable. These routers are further connected to 2960-24TT switches and then the corresponding end devices like computer are connected to these switches.

Note: Every PC connected in a different network has a specific class IP. No IP addresses are repeated.

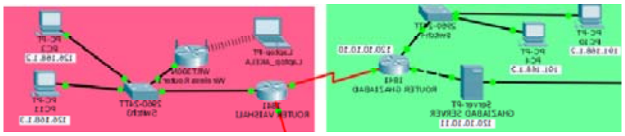


Figure IV: Ghaziabad and Vaishali Router

The above figure 2 shows Router (1841) GHAZIABAD and Router (1841) VAISHALI which are connected to each other with the help of Serial DTE cable. Just like Dwarka and Nirman vihar here also the routers are connected to 2960-24TT switches and then the corresponding end devices like computer are connected to these switches. In the Vaishali network a Wireless Router (WRT300N) is also connected to the switch making the end device like laptop to get attach to the network via Wireless medium.

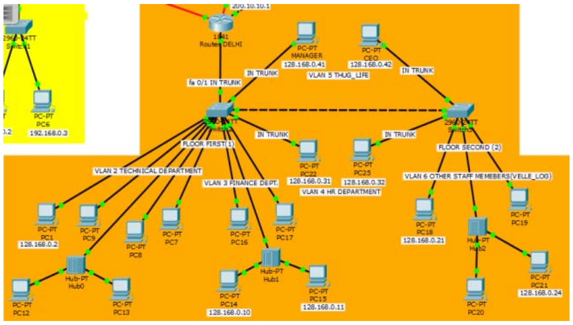
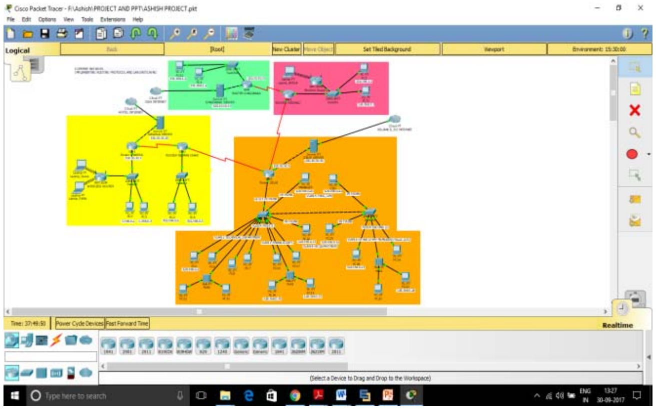


Figure V: Delhi Router (The Assumed Headquarter of the Company)

The above figure 3 shows Router (1841) Delhi that is assumed to be the main headquarter of the company. It comprises of various departments like: Technical department, HR department, Finance department and other staff members which can do there respected work in there PCs arranged (the person can be anyone who can work here- might be of a particular department or other people like trainee and interns). The headquarter as assumed to have two floors the manager CEO and HR department representatives are in Trunk in the network so then can communicate and share files in there network. Security features are added in this network separate VLANs are created for particular department so that a person in technical department cannot access the data that is present in the finance department. Different class IP Address is present in this network.

4. RESULT


Cisco Packet Tracer - F:\Ashish\PROJECT AND PPT\ASHISH PROJECT.pkt
File Edit Options View Tools Extensions Help
Logical
Root
New Cluster
Move Object
Set Tiled Background
Viewport
Realtime
Type here to search

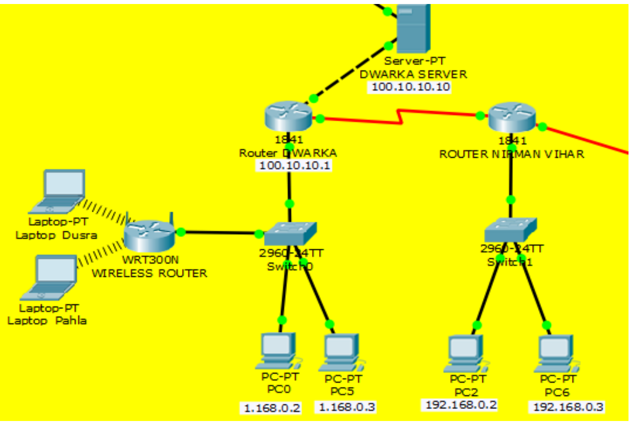
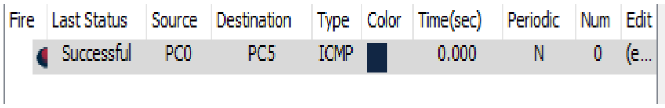
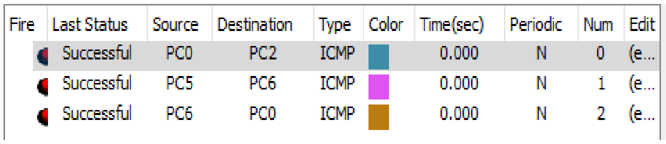


Figure VI: Communicating in same Network



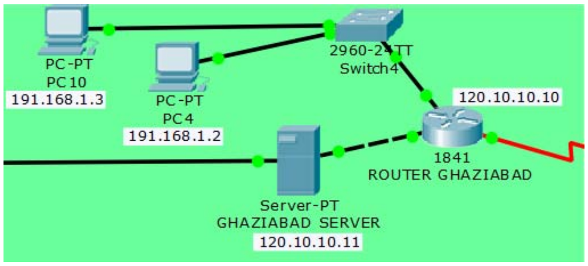
Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit
●	Successful	PC0	PC5	ICMP	🟦	0.000	N	0	(e...

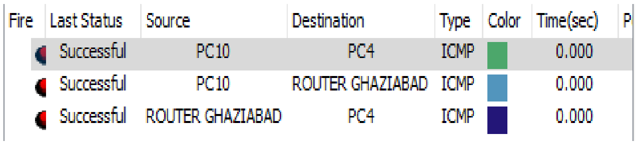
Figure VII: Communicating in different Network



Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit
●	Successful	PC0	PC2	ICMP	🟦	0.000	N	0	(e...
●	Successful	PC5	PC6	ICMP	🟪	0.000	N	1	(e...
●	Successful	PC6	PC0	ICMP	🟫	0.000	N	2	(e...

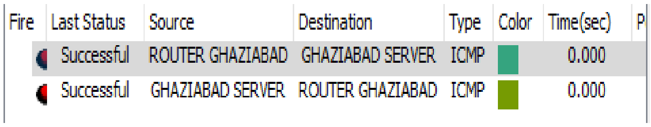
Figure VIII: Another Network Showing PC communicating to Router and Router to PC and PC to PC





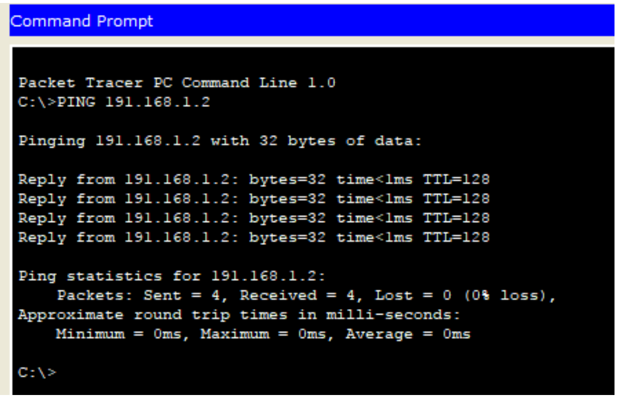
Fire	Last Status	Source	Destination	Type	Color	Time(sec)	P
●	Successful	PC10	PC4	ICMP	🟩	0.000	
●	Successful	PC10	ROUTER GHAZIABAD	ICMP	🟦	0.000	
●	Successful	ROUTER GHAZIABAD	PC4	ICMP	🟦	0.000	

Figure IX: Ghaziabad Router Communicating With Ghaziabad Serverand Vice Versa



Fire	Last Status	Source	Destination	Type	Color	Time(sec)	P
●	Successful	ROUTER GHAZIABAD	GHAZIABAD SERVER	ICMP	🟩	0.000	
●	Successful	GHAZIABAD SERVER	ROUTER GHAZIABAD	ICMP	🟩	0.000	

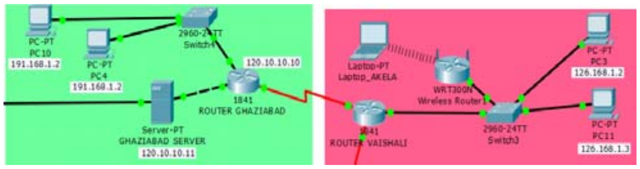
FIGURE X: Ping 191.168.1.2 from 191.168.1.3 (PC 10 to PC 4)

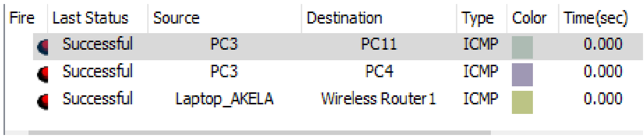


Command Prompt

```
Packet Tracer PC Command Line 1.0
C:\>PING 191.168.1.2

Pinging 191.168.1.2 with 32 bytes of data:

Reply from 191.168.1.2: bytes=32 time<1ms TTL=128
Reply from 191.168.1.2: bytes=32 time<1ms TTL=128
Reply from 191.168.1.2: bytes=32 time<1ms TTL=128
Reply from 191.168.1.2: bytes=32 time<1ms TTL=128

Ping statistics for 191.168.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

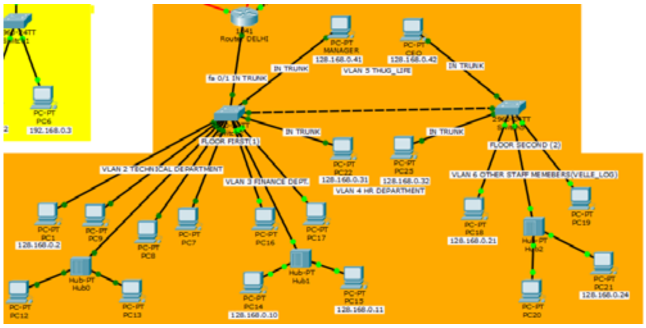
Figure XI: Different Networks Communicatingtoeach other andLaptop Connected to Wireless Router

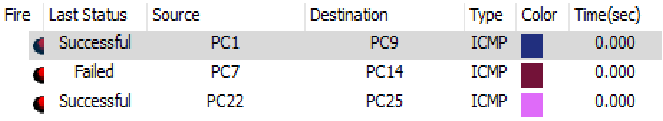




Fire	Last Status	Source	Destination	Type	Color	Time(sec)
●	Successful	PC3	PC11	ICMP	⬜	0.000
●	Successful	PC3	PC4	ICMP	🟪	0.000
●	Successful	Laptop_AKELA	Wireless Router1	ICMP	🟩	0.000

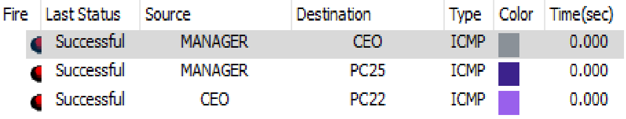
Figure XII: Same VLAN's are able to Communicate





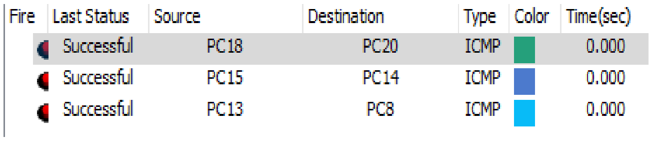
Fire	Last Status	Source	Destination	Type	Color	Time(sec)
●	Successful	PC1	PC9	ICMP	🟦	0.000
●	Failed	PC7	PC14	ICMP	🟥	0.000
●	Successful	PC22	PC25	ICMP	🟪	0.000

Figure XII: Managerand CEO Communicating with each other and with HR Department



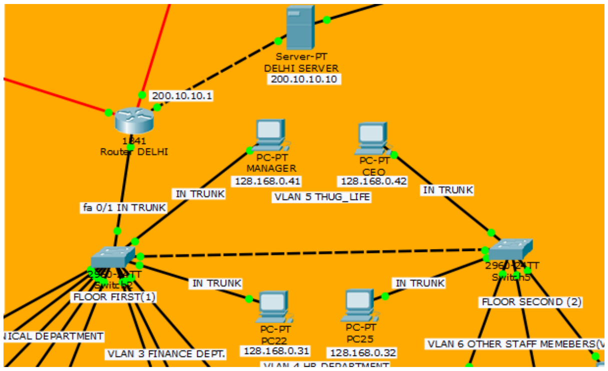
Fire	Last Status	Source	Destination	Type	Color	Time(sec)
●	Successful	MANAGER	CEO	ICMP	⬜	0.000
●	Successful	MANAGER	PC25	ICMP	🟦	0.000
●	Successful	CEO	PC22	ICMP	🟪	0.000

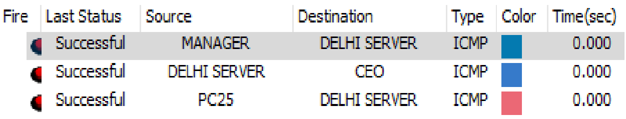
Figure XIV: PCs connected with help of HUB'sable to communicate in Network



Fire	Last Status	Source	Destination	Type	Color	Time(sec)
●	Successful	PC18	PC20	ICMP	🟩	0.000
●	Successful	PC15	PC14	ICMP	🟦	0.000
●	Successful	PC13	PC8	ICMP	🟦	0.000

Figure XV: Managerand CEOable to communicate with Delhi's Server





Fire	Last Status	Source	Destination	Type	Color	Time(sec)
●	Successful	MANAGER	DELHI SERVER	ICMP	🟦	0.000
●	Successful	DELHI SERVER	CEO	ICMP	🟦	0.000
●	Successful	PC25	DELHI SERVER	ICMP	🟥	0.000

REFERENCES

[1]Comer, Douglas (2000). *Internetworking with TCP/IP:Principles, Protocols, and Architectures – 4th ed.* Upper Saddle River, NJ: Prentice Hall. p. 394. ISBN 0-13-018380-6.

[2] S. Floyd & V. Jacobson,"The Synchronization of Periodic Routing Messages", April 1994

[3] "PORT *NUMBERS", The Internet Assigned Numbers Authority (IANA).May 2008*

[4] "*Network Security Basics*", 7 May 2004 by Robyn Aber

[5] IEEE 802.1Q-2011, *1. Overview*

[6] IEEE 802.1Q-2011, *1.4 VLAN aims and benefits*

[7] RFC 760, *DOD Standard Internet Protocol* (January 1980)

[8] *Internet Protocol*-DARPA Internet Program Protocol Specification. September 1981. p. 7. RFC 791.

[9] *"NetAcuity Edge Offers Hyper-local IP targeting"*Retrieved 2011-12-10.

[10] *Groth, David; Toby Skandier (2005). Network+ Study Guide, Fourth Edition. Sybex, Inc.* ISBN 0-7821-4406-3.

[11] *ATIS committee PRQC. "mesh topology". ATIS Telecom Glossary 2007.* Alliance for Telecommunications Industry Solutions. Retrieved 2008-10-10.

[12] *Chiang, Mung; Yang, Michael (2004). "Towards Network X-ities From a Topological Point of View: Evolvability and Scalability". Proc. 42nd Allerton Conference.*