International Journal of Enhanced Research in Science Technology & Engineering, ISSN: 2319-7463
Vol. 2 Issue 7, July-2013, pp: (123-133), Available online at: www.erpublications.com

# Company Network Architecture

Haris Mahmood Ansari[1], Harsh Singh Bhal[2]
Department of Electronics and Communication, Jamia Millia Islamia University, New Delhi, India

**Abstract: The project “Company Network Architecture” is a scenario of a company which has its branches spread across India. Through this project we have configured five branches of a company with their respective headquarters. In the North region we have configured two branches i.e. Delhi and Chandigarh with their headquarters named, the North Headquarter. In the South region we have configured three branches i.e. Bangalore, Chennai and Pune with their headquarters named, the South Headquarter.**

**Sub Netting has been done across all the branches which relieve us if purchasing new IP addresses for all the branches. This will help in the reduction of cost. All the branches are divided into three departments that are: Marketing, Sales and Finance. Virtual Private Network (VPN) connectivity is applied in order to conduct private data communication which uses the public network like the Internet rather than rely on private leased lines. We have also configured the Virtual LAN as a security measure. VLAN (Virtual LAN) will allow only the same departments of different branches to communicate with each other. It makes sure that no person from one department accesses the other department, thus providing security. We have also configured the Access Control List (ACL) which denies the services mentioned in the list.**

**Keywords: Network Protocols; Routing; Virtual Local Area Network (VLAN); Virtual Private Network (VPN); Access Control List (ACL); Open Shortest Path First (OSPF)**

## I. INTRODUCTION

In modern era, computer communication networks are growing rapidly day by day. Communication technology facilitates users by providing user friendly services such as file transferring, pint sharing, video streaming and video conferencing. Internet is a global system of interconnected computer networks. Today Internet is playing a vital role in communication networks. Computer communication networks are based on a technology that provides the technical infrastructure, where routing process and its protocols are used to transmit packets across the Internet.

### A. Routing

Routing is the process of selecting paths in a network along which to send network traffic. Routing is performed for many kinds of networks, including the telephone network (Circuit Switching) electronic data networks (such as the Internet), and transportation networks.

In packet switching networks, routing directs packet forwarding, the transit of logically addressed packets from their source toward their ultimate destination through intermediate nodes, typically hardware devices called routers, bridges, gateways, firewalls, or switches. The routing process usually directs forwarding on the basis of routing tables which maintain a record of the routes to various network destinations. Thus, constructing routing tables, which are held in the router’s memory, is very important for efficient routing. Most routing algorithms use only one network path at a time, but multipath routing techniques enable the use of multiple alternative paths.

Routing schemes differ in their delivery semantics:

- **Unicast** delivers a message to a single specified node.
- Broadcast delivers a message to all nodes in the network.
- **Multicast** delivers a message to a group of nodes that have expressed interest in receiving the message.
- **Anycast** delivers a message to any one out of a group of nodes.
- **Geocast** delivers a message to a geographic area.

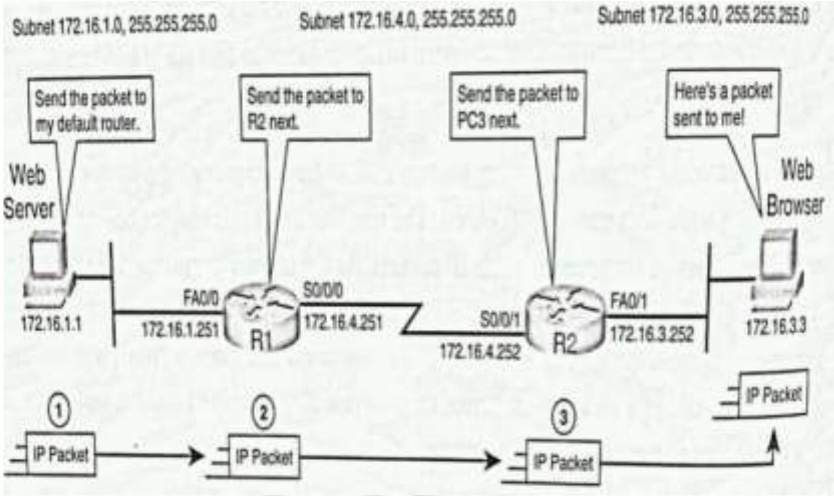

Subnet 172.16.1.0, 255.255.255.0
Subnet 172.16.4.0, 255.255.255.0
Subnet 172.16.3.0, 255.255.255.0
Send the packet to my default router.
Send the packet to R2 next.
Send the packet to PC3 next.
Here's a packet sent to me!
Web Server
Web Browser
172.16.1.1
FA0/0
172.16.1.251
R1
S0/0/0
172.16.4.251
S0/0/1
172.16.4.252
R2
FA0/1
172.16.3.252
172.16.3.3
1
2
3
IP Packet
IP Packet
IP Packet
IP Packet

Figure 1: How router works

Routing involves two basic activities: determining optimal routing paths and transporting information groups (typically called packets) through an internetwork. A metric is a standard of measurement, such as path length, that is used by routing algorithms to determine optimal path to a destination. To aid the process of path determination, routing algorithms initialise and maintain routing tables, which contain route information. Routers communicate with one another and maintain their routing tables through the transmission of a variety of messages. The routing update message is one such message that generally consists of all or a portion of routing table

### B. Routing Protocols

A routing protocol is a protocol that specifies how routers communicate with each other, disseminating information that enables them to select routes between any two nodes on a computer network, the choice of the route being done by routing algorithms. Each router has a prior knowledge only of networks attached to it directly. A routing protocol shares this information first among immediate neighbours, and then throughout the network. This way routers gain knowledge of the topology of the network. The term routing protocol may refer specifically to one operating at layer three of the OSI model, which similarly disseminates topology information between routers.

#### 1. Interior Gateway Protocols (IGPs)

Interior Gateway Protocols (IGPs) handle routing within an Autonomous System (one routing domain). IGP’s figure out how to get from place to place between the routers you own. These dynamic routing protocols keep track of paths used to move data from one end system to another inside a network or set of networks that you administrate.

IGP’s fall into two categories:

- Distance Vector Protocols – These are of two types
- Routing Information Protocol (RIP)
- Interior Gateway Routing Protocol (IGRP)

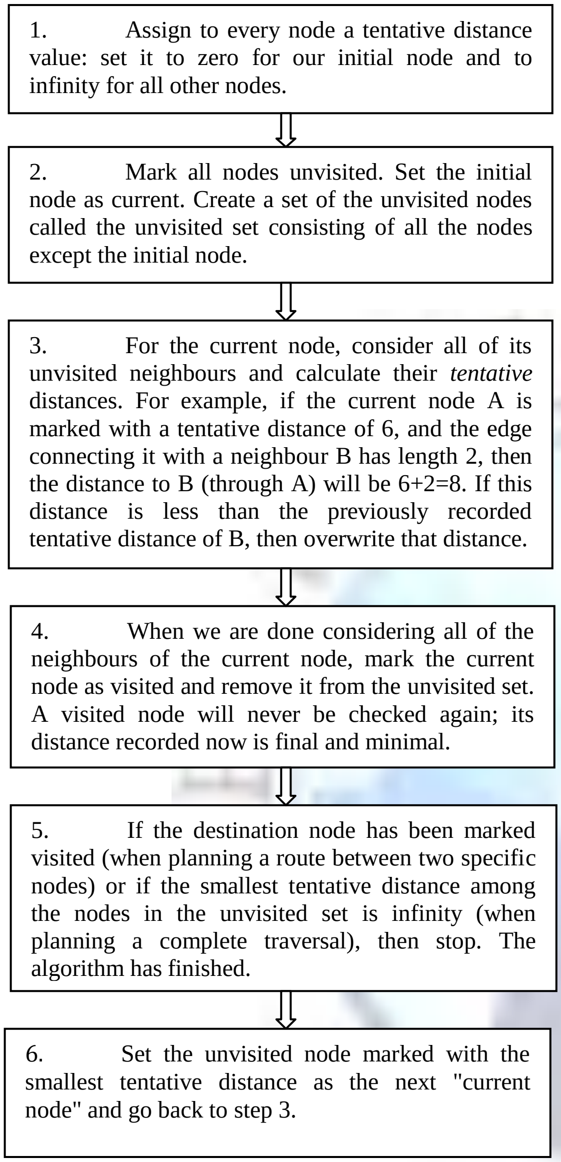
- Link State Protocols – These can also be further classified into two categories
- Open Shortest Path First (OSPF)
- Intermediate System to Intermediate System (IS-IS)

#### 2. Exterior Gateway Protocols (EGPs)

To get from place to place outside your network(s), i.e. on the Internet, you must use an Exterior Gateway Protocol. EGP handle routing outside an Autonomous System and get you from your network, through your Internet provider’s network and onto any other network. Border Gateway Protocol is used by many companies with more than one Internet provider to allow them to have redundancy and load balancing of their data transported to and from the Internet.

### C. Open Shortest Path First (OSPF)

#### 1. Basic Algorithm



1. Assign to every node a tentative distance value: set it to zero for our initial node and to infinity for all other nodes.

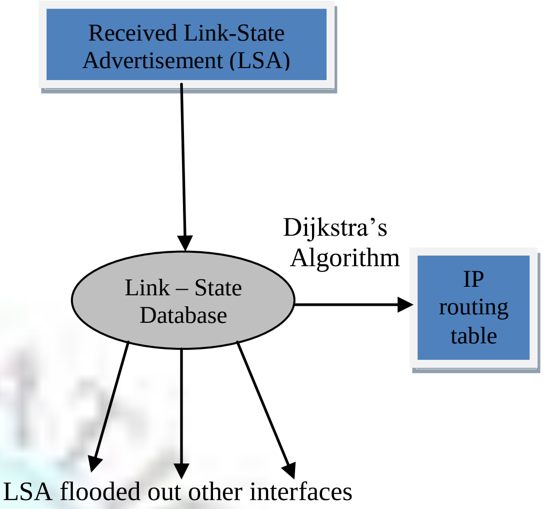
2. Mark all nodes unvisited. Set the initial node as current. Create a set of the unvisited nodes called the unvisited set consisting of all the nodes except the initial node.

3. For the current node, consider all of its unvisited neighbours and calculate their *tentative* distances. For example, if the current node A is marked with a tentative distance of 6, and the edge connecting it with a neighbour B has length 2, then the distance to B (through A) will be 6+2=8. If this distance is less than the previously recorded tentative distance of B, then overwrite that distance.

4. When we are done considering all of the neighbours of the current node, mark the current node as visited and remove it from the unvisited set. A visited node will never be checked again; its distance recorded now is final and minimal.

5. If the destination node has been marked visited (when planning a route between two specific nodes) or if the smallest tentative distance among the nodes in the unvisited set is infinity (when planning a complete traversal), then stop. The algorithm has finished.

6. Set the unvisited node marked with the smallest tentative distance as the next "current node" and go back to step 3.


Received Link-State Advertisement (LSA)
Dijkstra's Algorithm
Link – State Database
IP routing table
LSA flooded out other interfaces

### D. Virtual LAN (VLANs)

A virtual local area network, virtual LAN, is a group of hosts with a common set of requirements that communicate as if they were attached to the same broadcast domain, regardless of their physical location. A VLAN has the same attributes as a physical local area network (LAN), but it allows for end stations to be grouped together even if they are not located on the same network switch.

To physically replicate the functions of a VLAN, it would be necessary to install a separate, parallel collection of network cables and equipments which are kept separate from the primary network. However, unlike a physically separate network, It visualizes VLAN behaviors (configuring switch ports, tagging frames when entering VLAN, lookup MAC table to switch/flood frames to trunk links, and untagging when exit from VLAN)

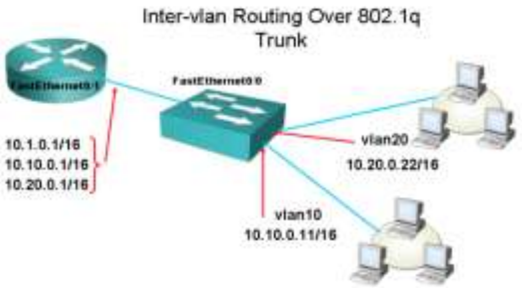


Figure 2: VLAN

The protocol most commonly used today in configuring VLANs is IEEE 802.1Q. The IEEE committee defined this method of multiplexing VLANs is an effort to provide multivendor VLAN support. Prior to the introduction of the 802.1Q standard, several proprietary protocols existed, such as Cisco's ISL (Inter Switch Link) and 3Com's VLT (Virtual LAN Trunk).

VLANs operate at Layer 2 (the data link layer) of the OSI model. Administrators often configure a VLAN to map directly to an IP network, or subnet, which gives the appearance of involving Layer 3 (the network layer). In the context of VLANs, the term "trunk" denotes a network link carrying multiple VLANs, which are identified by labels (or "tags") inserted into their packets. Such trunks must run between "tagged ports" of VLAN-aware devices, so they are often switch-to-switch or switch-to-router links rather than links to hosts.

### E. Access Control List (ACL)

An access control list (ACL), with respect to a computer file system, is a list of permissions attached to an object. An ACL specifies which users or system processes are granted access to objects, as well as what operations are allowed on given objects. Each entry in a typical ACL specifies a subject and an operation.
When a subject requests an operation on an object in an ACL-based security model the operating system first checks the ACL for an applicable entry to decide whether the requested operation is authorized. A key issue in the definition of any ACL-based security model is determining how access control lists are edited, namely which users and processes are granted ACL-modification access. Access control lists can generally be configured to control both inbound and outbound traffic, and in this context they are similar to firewalls.

An access control list (ACL) is a table that tells a computer operating system which access rights each user has to a particular system object, such as a file directory or individual file. Each object has a security attribute that identifies its access control list. The list has an entry for each system user with access privileges. The most common privileges include the ability to read a file (or all the files in a directory), to write to the file or files, and to execute the file (if it is an executable file, or program).

There are two types of ACL:

#### 1. Standard ACL

Standard IP access list provides basic packet filtering abilities, based on the source IP address of a packet only. As a general rule, apply standard IP access lists close to the destination network to which you wish to permit or deny access. In standard access-list we can filter the packet after routing and it will be applied on destination router it depends only on source IP address. Standard IP access lists fall into the numerical range 1-99.

#### 2. Extended ACL

Extended IP access lists allow filtering not only on source addresses, but also on destination addresses, protocols, and even applications, based on their port number. Extended IP access lists are identified through their use of the 100-199 numerical range. Extended IP access lists allow a much more granular level of control.

### F. Virtual Private Network (VPN)

A virtual private network (VPN) is a network that uses primarily public telecommunication infrastructure, such as the Internet, to provide remote offices or travelling users access to a central organizational network.

VPNs typically require remote users of the network to be authenticated, and often secure data with encryption technologies to prevent disclosure of private information to unauthorized parties.

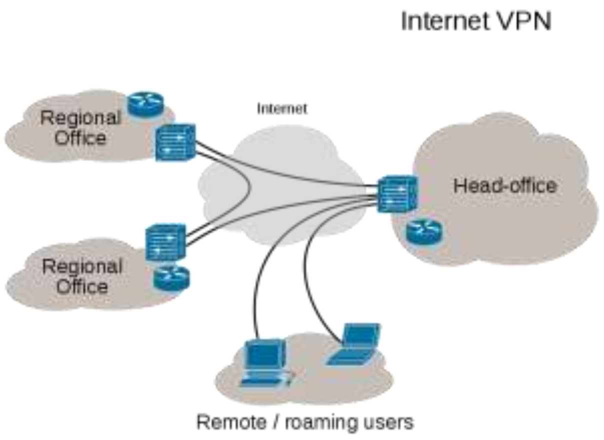


Figure 3: VPN

VPNs may serve any network functionality that is found on any network, such as sharing of data and access to network resources, printers, databases, websites, etc. A VPN user typically experiences the central network in a manner that is identical to being connected directly to the central network. VPN technology via the public Internet has replaced the need to requisition and maintain expensive dedicated leased-line telecommunication circuits once typical in wide-area network installations. VPN offers two main advantages over alternative technologies: cost savings, and network scalability.

## II. Sub-Netting for IPv4

Sub-netting is a set of techniques that you can use to efficiently divide the address space of a unicast address prefix for allocation among the subnets of an organization network. The fixed portion of a unicast address prefix includes the bits up to and including the prefix length that have a defined value. The variable portion of a unicast address prefix includes the bits beyond the prefix length that are set to 0. Sub-netting is the use of the variable portion of a unicast address prefix to create address prefixes that are more efficient (that waste fewer possible addresses) for assignment to the subnets of an organization network.

### A. Subnet Mask

Sub-netting for IPv4 was originally defined to make better use of the host bits for Class A and Class B IPv4 public address prefixes. Sub-netting for IPv4 produces a set of sub-netted address prefixes and their corresponding ranges of valid IPv4 addresses. By assigning sub-netted address prefixes that contain an appropriate number of host IDs to the physical and logical subnets of an organization's IPv4 network, network administrators can use the available address space in the most efficient manner possible.

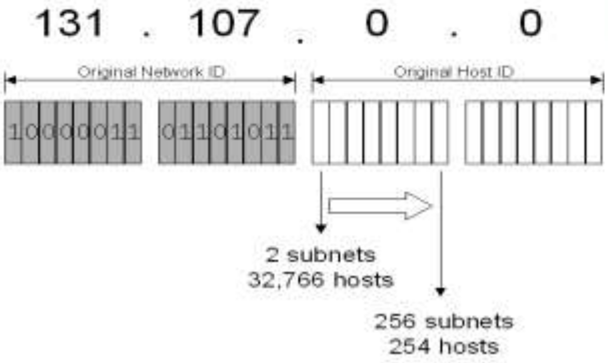


Figure 4: Tradeoffs between number of subnets and number of hosts per subnet.

Subnet masks, like IP addresses, are represented in the dotted decimal format like 255.255.255.0. Although subnet masks use the same format as IP addresses, they are not IP addresses themselves. Each subnet mask is 32-bit long, divided into four octets, and is usually represented in dotted-decimal notation like IP addresses. In their binary representation, subnet masks have all 1s in the network and sub-network portions, and have all 0s in the host portion.

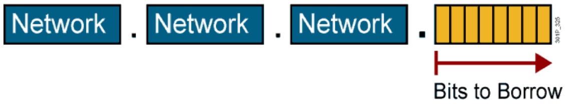


Figure 5: Class C Network

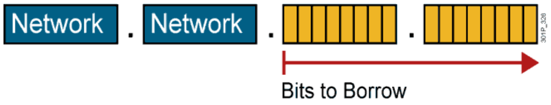


Figure 6: Class B Network

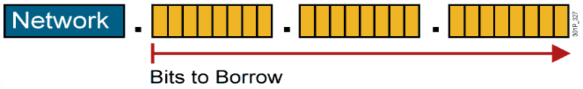


Figure 7: Class A Network

TABLE I

| Subnet | Decimal Octet of Sub-netted Octet | Sub-netted Address prefix |
|---|---|---|
| 1 | 0 | 192.168.0.0/19 |
| 2 | 32 | 192.168.32.0/19 |
| 3 | 64 | 192.168.64.0/19 |
| 4 | 96 | 192.168.96.0/19 |
| 5 | 128 | 192.168.128.0/19 |
| 6 | 160 | 192.168.160.0/19 |
| 7 | 192 | 192.168.192.0/19 |
| 8 | 224 | 192.168.224.0/19 |

## III. HARDWARE AND SOFTWARE REQUIREMENTS

### Hardware Specification

| | |
|---|---|
| Microprocessor: | Pentium-IV & above |
| RAM: | 512 MB of RAM |
| Hard Disk: | 2.5 GB on installation drive |

### Software Specification

| | |
|---|---|
| Operating System: | Windows XP, Windows 7. |
| Simulator Used: | Packet Tracer 5.0 |

And with these requirements we are going to configure the company network architecture using OSPF, VPN and ACL.

## IV. DESIGN AND DEVELOPMENT

### A. Simulator

Packet Tracer 5.0 is comprehensive networking technology teaching and learning software and is an integral part of the Networking Academy's CCNA Discovery and CCNA Exploration curriculum. It provides powerful simulation, visualization, authority, assessment, and collaboration capabilities and makes teaching and learning net-working technology easier by visually stimulating virtual networking environments.

Now, the company's network has been designed and virtually stimulated on the **Cisco Packet Tracer 5.0.**

### B. Network Design

We have designed company network architecture. In this we have two headquarters of the company present at north and south location. Corresponding to both the headquarters, we have some branches of the company. Our aim is to communicate to all the branches by configuring the routing protocol OSPF and also provide a private connectivity by using VPN. The security measures are provided by implementing ACL.

The figure below shows the head quarter of the south network from where we have configured three working stations that are as under:

- Bangalore
- Chennai
- Pune

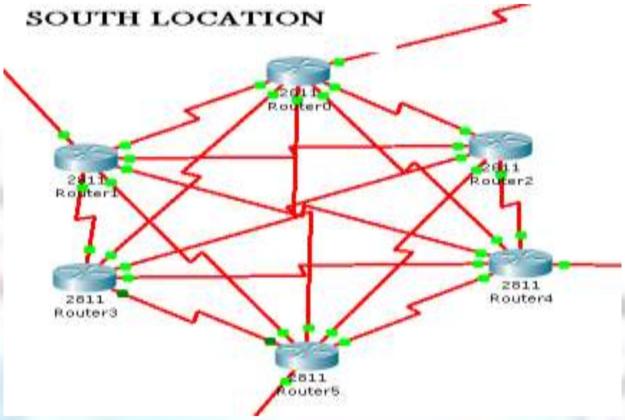


Figure 8: South Location

This is the model of Bangalore which has been configured with OSPF and sub-netting has been done throughout network. We have also configured access control list (ACL) and implemented VPN. The company's network
has been divided into three fields that are: Marking, Sales, Finance.

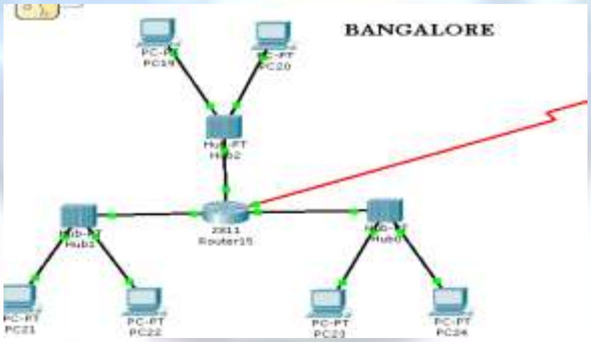


Figure 9: Bangalore Network

The other two sub networks have also been configured with the same scenario. The Pune sub-network is shown below:

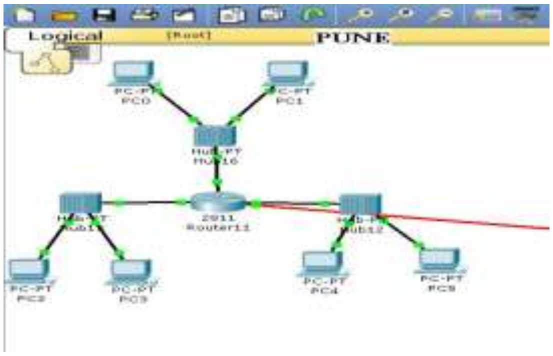


Figure 10: Pune Network

The Chennai sub-network is shown below:

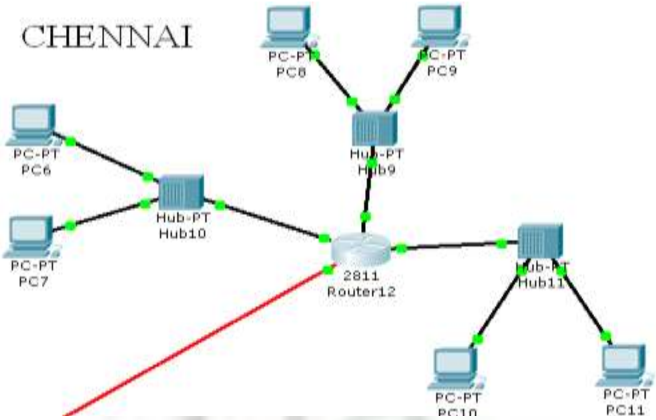


Figure 11: Chennai Network

The figure below shows the head quarter of the north network from where we have configured two working stations that are as under:

- ➢ Delhi
- ➢ Chandigarh

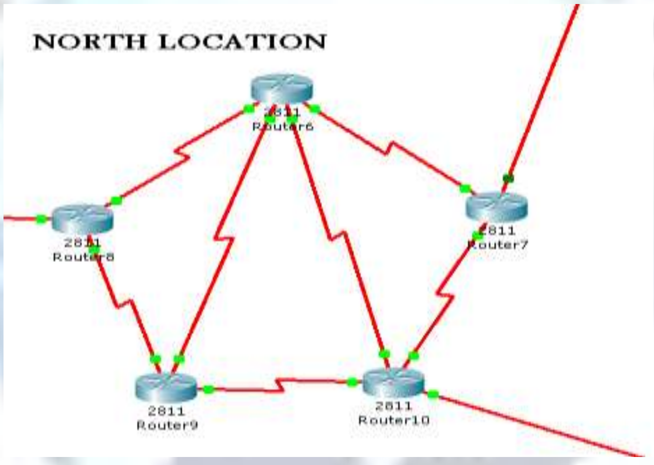


Figure 12: North Location

This is the model of Chandigarh which has been configured with OSPF and sub-netting has been done throughout the network. We have also configured VPN and access control list (ACL). The company's network has been divided into three fields that are: Marketing, Sales, and Finance.

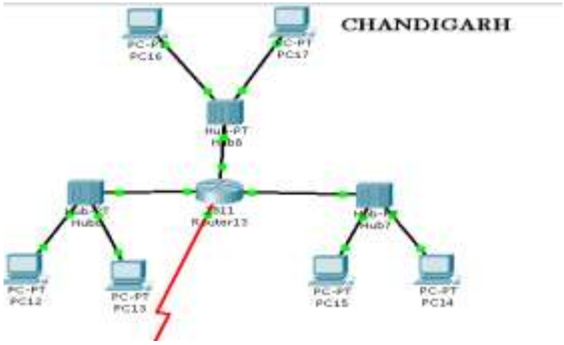


Figure 13: Chandigarh Network

The other sub-network is also been configured with the same scenario which is shown below:

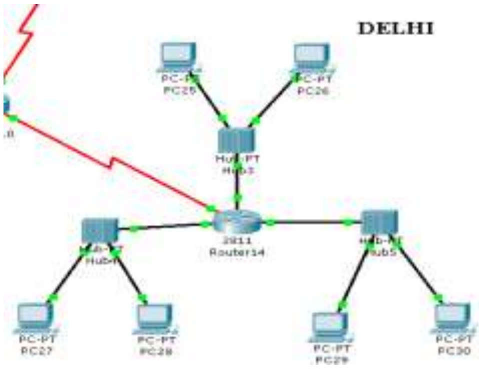
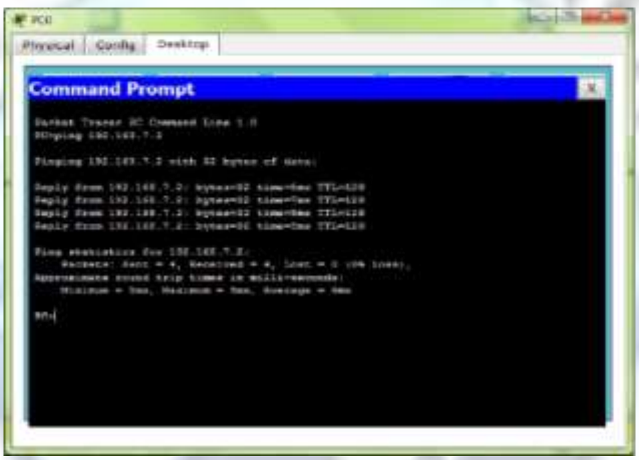


Figure 14: Delhi Network

## V. CONCLUSION

### A. Result

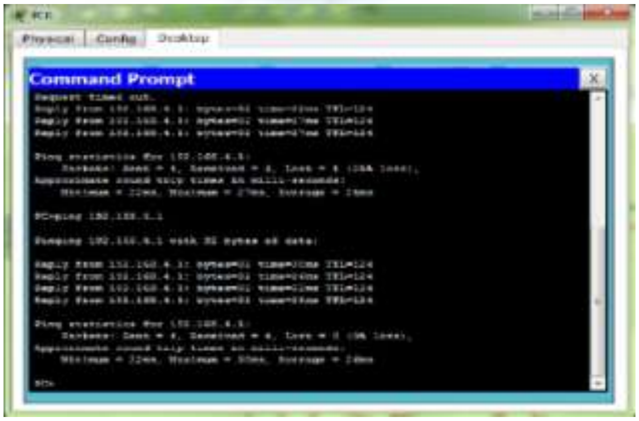
Now to show the output of VLAN, we ping from one host to other host of same department. As both the host belongs to same department in the same branch therefore they can communicate and send the data to each other.



```
Packet Tracer PC Command Line 1.0
PC>ping 192.168.7.2

Pinging 192.168.7.2 with 32 bytes of data:

Reply from 192.168.7.2: bytes=32 time=[illegible] TTL=128
Reply from 192.168.7.2: bytes=32 time=[illegible] TTL=128
Reply from 192.168.7.2: bytes=32 time=[illegible] TTL=128
Reply from 192.168.7.2: bytes=32 time=[illegible] TTL=128

Ping statistics for 192.168.7.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = [illegible], Maximum = [illegible], Average = [illegible]

PC>
```

Figure 15

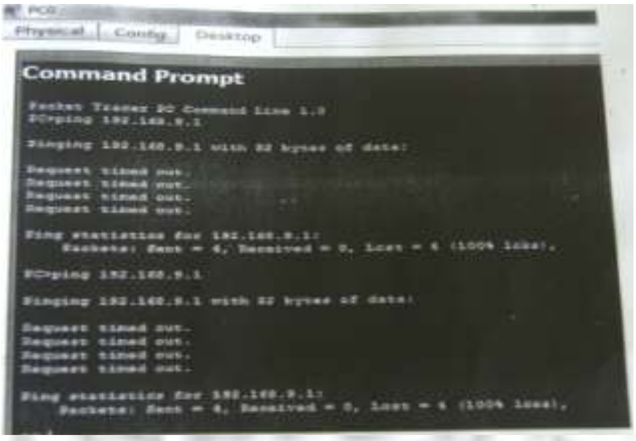
This is the output of Pune location from where we ping the pc0 to pc1. They communicate with each other as both the host belongs to the same department. Now we show the output of hosts belongs to same department but different branch. They should communicate with each other and can send the data.



```
Request timed out.
Reply from 192.168.4.1: bytes=32 time=[illegible] TTL=124
Reply from 192.168.4.1: bytes=32 time=[illegible] TTL=124
Reply from 192.168.4.1: bytes=32 time=[illegible] TTL=124

Ping statistics for 192.168.4.1:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = [illegible], Maximum = [illegible], Average = [illegible]

PC>ping 192.168.4.1

Pinging 192.168.4.1 with 32 bytes of data:

Reply from 192.168.4.1: bytes=32 time=[illegible] TTL=124
Reply from 192.168.4.1: bytes=32 time=[illegible] TTL=124
Reply from 192.168.4.1: bytes=32 time=[illegible] TTL=124
Reply from 192.168.4.1: bytes=32 time=[illegible] TTL=124

Ping statistics for 192.168.4.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = [illegible], Maximum = [illegible], Average = [illegible]

PC>
```

Figure 16

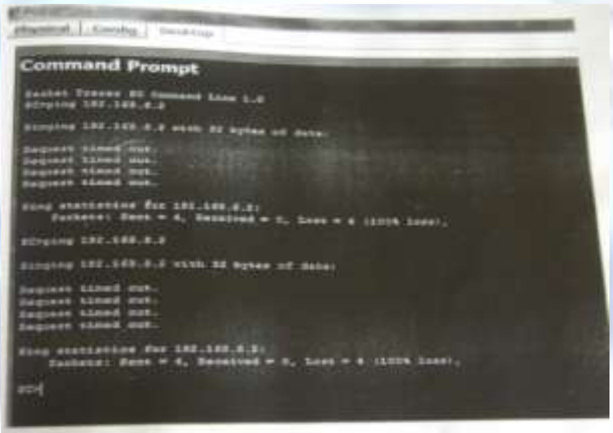
This is the output of host located in Pune location communicate with the host located in the Chennai location. They can access and send the data to each other even they don't belong to same branch but they belong to the same department. Now we show the output of hosts belongs to same branch but in different department. They can't communicate with each other.



```
Packet Tracer PC Command Line 1.0
PC>ping 192.168.9.1

Pinging 192.168.9.1 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.9.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

PC>ping 192.168.9.1

Pinging 192.168.9.1 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.9.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Figure 17

This is the output of hosts located in Pune location which can't communicate with each other as both the host belongs to the different department. They can't access and send the data. Now we show the output of hosts belongs to different department and in different branch. They should not communicate with each other and can't send the data.



```
Packet Tracer PC Command Line 1.0
PC>ping 192.168.[illegible].2

Pinging 192.168.[illegible].2 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.[illegible].2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

PC>ping 192.168.[illegible].2

Pinging 192.168.[illegible].2 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.[illegible].2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

PC>
```

Figure 18

This is the output of host located in Pune location which can't communicate with the host located in the Bangalore location. They can't access and send the data to each other as they don't belong to same department. For communication, both the hosts belong to the same department even they belong to the same branch.

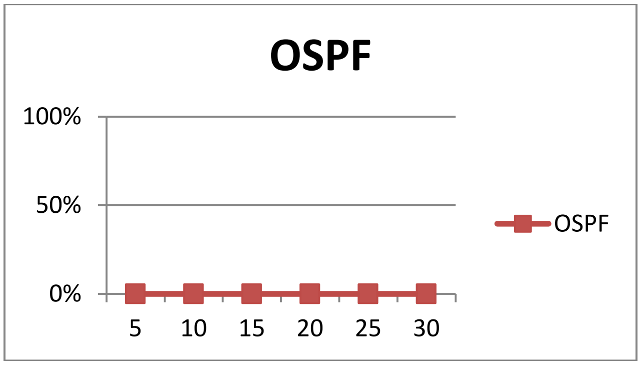


Figure 19: Output Graph

The output graph above is the graph for percentage of packet loss during the transmission of data in the form of packets. This graph shows that there is no packet loss during transmission of data from one host to another host. Therefore, the network configured with OSPF has zero percentage of packet loss.

### B. Advantages

VLANs are configured as the security measure in the company which concludes that there is no unauthorized access to the data from any of the department. The Access Control List (ACL) denies the services mentioned in the list. This will conclude that the authorized person will decide which services are used by which department or group of hosts.

In this we have also achieved cost reduction by applying sub-netting as single IP address is very costly and further more making the data available for all user of every branch of the company. We have also achieved time saving by not doing same task again and again and results can be fetched. By configuring OSPF routing protocol we have concluded that there is no loss of the data during the transmission from one host to another host.

### C. Future Prospects

The Company Network Architecture is scenario of the company which has its branches across India with their respective headquarters. We have implemented Interior Gateway Protocols such as OSPF. These protocols allow us to communicate within single autonomous system such as a single company to communicate with all its branches across India.

Further, we can implement the Exterior Gateway Protocols such as BGP (Border Gateway Protocol) which allow us to communicate with other autonomous system such as company has to communicate with another company.

## REFERENCES

[1]. Lamely Todd, CCNA, BPB Publications 4th Edition.
[2]. Forouzan B.H, Data Communication and Networking, TMH Publications 4th Edition.
[3]. Computer Networks: A Systems Approach, Larry L. Peterson, Bruce S. Davie.
[4]. Enabling Grid Computing over IPv6 within a Campus Network, “Parallel Architectures, Algorithms and Programming, International Symposium” By Jun Chen,You Zou, Zhongyu Liu, Qing Wu, pp. 285-288.
[5]. Security Problems and Countermeasures with Commercial Banking Computer Networks, “Computational Intelligence and Security, International Conference”, by YunCheng Liu, Xingchun Sun, Xiaoqin Mao, pp. 821-825.
[6]. A Dynamic VPN Architecture for Private Cloud Computing, “Utility and Cloud Computing, IEEE International Conference” By Wen-Hwa Liao, Shuo-Chun, pp. 409-414.