TNC Transactions on Networks and Communications
SOCIETY FOR SCIENCE AND EDUCATION UNITED KINGDOM
VOLUME 2, ISSUE 5
ISSN: 2054 - 7420

Enhancing the competence of enterprise network using contemporary networking paradigms

Aditya Ahuja, Kamal Dewan, Nikita Gupta and Meenakshi Sood
ECE Department, Jaypee University of Information Technology, Waknaghat Solan, India;
adityaahuja2005@gmail.com; kdewan9495@gmail.com; nikita92gupta@yahoo.com;
meenakshi.sood@juit.ac.in

ABSTRACT

Networking has traversed from days where networks were considered a background component of businesses to today's electronic age, where networks are an imperative resource, and directly determine revenue generation for an organization. In today's dynamic arena of networking, the crafting of networks has escalated from using just an elemental set of features, to consolidating modernistic technologies and services, in an effort to come up with state of the art networks which can meet the aim of connectivity, security, scalability, simplicity of operation, and flexible accommodation of new trends and technologies. The roots of this paper lie in the Enterprise network, and while adhering to the need of the hour in corporate sector, we propose architecture for Enterprise network, using avant-garde technologies such as Frame Relay, Port Security, Access Control Lists (Firewalling), VoIP, VPN, Ether Channel, Redistribution of Routing Protocols and ISP Redundancy. The network architecture has been designed on Cisco's network simulation software: Cisco Packet Tracer. The principle behind the proposed network architecture can be applied in designing the networks of a host of other campuses.

Keywords: Frame Relay, Port Security, ACL (Access Control List), Ether Channels, VoIP (Voice over Internet Protocol), VPN (Virtual Private Network).

1 Introduction

The designing of networks has evolved and matured from merely applying a basic set of techniques, to incorporating multiple technologies and services, in an effort to support the vastly disparate end to end communication requirements.

In the past, network designers had a very limited number of options in terms of hardware devices, protocols and media, and thus network designing was relatively easier, with very little scope of mistake, but with limited efficiency and flexibility. Whereas, today's networks are based on complex environments, which are an amalgamation of multiple protocols, media and interconnections to networks outside any single organization's dominion of control, thus giving rise to computationally efficient networks, which can scale, and flexibly accommodate upgrades without an entire revamp of the design. Networks are broadly classified as *LAN (Local Area Network)*, and *WAN (Wide Area Network)*. LANs, which persist over a relatively shorter distance are designed to allow personal computers to share resources, which can include hardware (e.g., a printer), software (e.g., an application program), or data.

DOI: 10.14738/tnc.25.565
Publication Date: 31rd October, 2014
URL: http://dx.doi.org/10.14738/tnc.25.565

A WAN, is an amalgamation of LANs which are spread over large geographical areas. WAN provides transmission of data over large distances that may encompass a country, a continent, or even the whole world [1].

This paper resides on the Enterprise Network, which is a building or a group of buildings, all connected into one central network that consists of many LANs. In enterprises today, more business is conducted electronically and deals are closed rapidly. Thus, in today's digital age, company operations have undergone a sea-change, and 24*7 connectivity has never been more imperative than it is today. Therefore, it is apt to say that the enterprise network has matured from an inert business element to a very active and visible asset that today's organizations rely on to support their day-to-day functions. It is seen as a critical resource, which directly supports revenue generation. When the network is going to interface with the internet, its security is also an important aspect, thus, today's networks must be open and pervasive, yet remain secure and controlled [2]. Moreover, the demand for mobile computing has increased in today's business environment, thus the networks must also be accessible remotely [3]. Therefore, new enterprise network designs are needed, as heirloom solutions and techniques cannot meet the new requirements, nor reduce the costs and streamline the operations [2].

This paper focuses on designing a state of the art enterprise network, by effectively blending a plethora of new technologies such as VoIP, VPN, Frame Relay, Port Security, Ether Channel, Access Control Lists (Firewalling), Redistribution of Routing Protocols and ISP Redundancy. The proposed architecture has been implemented and tested on Cisco's Network Simulation Program: *"Cisco Packet Tracer"*.

The rest of the paper is organized as follows: section 2 presents a brief insight into the technologies incorporated in the proposed design. Section 3 demonstrates the proposed network architecture, as designed on Cisco Packet Tracer. Section 4 presents the results and discussions along with demonstration of some of the results.

2 Technologies Incorporated

2.1 LAN Framework Design

The present scenario in the corporate world demands networks that can support high-speed business solutions such as voice, video, wireless, and mission-critical data applications. This calls for highly dependable and security-centred network designs. Using the principles of hierarchical design fulfils the requirements for building such efficient networks. The hierarchical design rests upon a building block approach. It consists of various independent distribution blocks which are attached to a high-speed routed core network layer [4].

The hierarchical design incorporates three layers, the *access* layer, *distribution* layer and the *core* layer. The Access Layer is where the end users are allowed in to the network. The Distribution Layer will contain switches and routers capable of VLAN switching and allow defining departmental workgroups and multicast domains. The Core Layer is capable of switching packets as fast as possible.

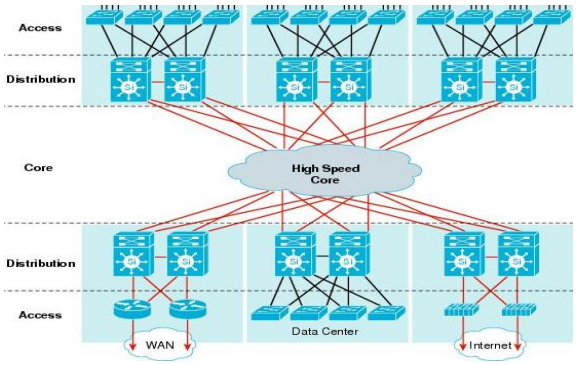

Figure 1: Hierarchical Model of LAN design

This design approach splits the functions of the network into various building blocks to provide reliability, flexibility, scalability, and fault isolation, thus making it a cluster of multiple smaller, more manageable hierarchical blocks. With the advancement in technology, the focus was highly on network convergence. The basic hierarchical model was modified to adapt itself with the active development of new services such as Voice over Internet Protocol (VoIP), Virtual Private Network (VPN), Frame Relay, Ether Channel, Port Security, etc. Myriads of such features, which the authors have also incorporated in their proposed design, have been discussed below.

Virtual Private Network (VPN) is a network that normally uses internet to establish connection between two branches of an enterprise. The security and protection of the shared information is maintained using special tunneling protocols and complex encryption procedures, hence the new connection so established is a dedicated point-to point connection. Besides costing significantly lesser as compared to privately owned or leased services, the service also provides data integrity, thus making it a private network virtually.

Voice over Internet Protocol (VoIP) is a rapidly surfacing technology that merges the voice and data networks for voice communication, using the all-pervasive IP-based networks to deploy VoIP client devices such as IP phones, mobile VoIP-enabled handheld devices, and VoIP gateways. Conventional telecommunications systems, even Private Branch Exchanges (PBX) are rapidly being replaced by IP-based systems (IP PBX) and thus, Voice over IP is extensively entering the enterprise networks [8].

Frame Relay is a packet-switched technology, which allows multiple sites of an organization, located within a few kilometers, to connect. All the locations plug into the frame relay “cloud”, which is usually a conglomeration of dozens or hundreds of Frame-Relay switches and routers. Unlike Ethernet switches, which make decisions based on MAC addresses, Frame Relay switches make decisions based on Data Link Connection Interfaces (DLCI). For communication to occur between locations, virtual circuits (VC) must be created, which is a one-way path through the Frame-Relay cloud. Virtual circuits are identified with DLCIs. Frame-relay circuits can either be permanent, or switched. A Switched Virtual Circuit (SVC) is created only when traffic needs to be sent, and is torn down when communication is complete. The authors have incorporated Permanent Virtual Circuit (PVC) in their designed network, which is always kept active, and is the most common virtual circuit. PVCs are software defined, so they can be created, altered or dismantled in a matter of hours. Networks working on the principle of frame relay have the higher speed and lower delay qualities of circuit switching without the need for dedicated full-time devices and circuits and wasted time slots when no data is being transmitted [9]. Also, Frame relay

networks are considered private because each customer's individual traffic is separated into a predetermined path, the PVC. Every PVC has an associated Committed Information Rate (CIR) that defines the amount of bandwidth a customer is provided on the shared network facility. However, customers have the ability to transmit data on their PVC at rates up to the full port speed [10].

Ether Channel technology, built upon standards-based 802.3 full-duplex Fast Ethernet, has emerged as a reliable, high-speed solution for the campus network backbone. It allows grouping of multiple ports into a single logical transmission path between a switch and a router, server, or another switch [11]. Besides making fair distribution of traffic between the channels, the technology also provides redundancy in the event of link failure. If a link is cut in an Ether Channel, traffic is rerouted to one of the other links in less than a few milliseconds [5].

Port security is a mechanism available on switches to restrict access to the devices that can connect via a particular port of the switch. Port security activated on a switch port only allows machines with a MAC address belonging to the range configured on it to connect to the switch's network. The MAC address of a frame arriving on the switch port is compared with the MAC addresses configured in its allowed list. The packet is allowed to pass through if its MAC address matches. If the MAC address is not a member of the configured list, the port either drops the packet or shuts itself down for a considerable amount of time [6].

Firewall is either hardware or software based security mechanism in a network. A hardware based firewall is a dedicated device with its own operating system on a specialized platform, whereas a software-based firewall or *Access Control List (ACL)* is an additional program loaded on a network device like a router to inspect data or network traffic. As a check point gateway, it analyses the IP packets and decides whether to allow through or not, based on the preconfigured rules. An ACL also determines which information or services to be accessed from outside as well as from inside and by whom. The authors have implemented firewall in the form of ACL in their proposed architecture.

2.2 Routing Protocols Used

Routing is an integral part of IP network design because it is the mechanism that provides accessibility for the applications. The communicating devices need to agree on a common set of rules to share the information. Such set of rules are known as protocols.

Routing Information Protocol (RIP) is a distance-vector routing protocol. This protocol has the feature of sending out the complete routing table to all active interfaces regularly and whenever the network topology changes. When a router receives a routing update that includes changes to an existing stored entry, it updates its routing table incorporating the new route. The protocol uses *hop count* to measure the distance between the source and destination network. It prevents routing loops from continuing indefinitely by limiting the number of hops allowed in a path to *15*. RIP version 1 uses classful routing, which means that the same subnet mask is used by all devices in the network. In the designed network, the authors have used RIP version 2 which utilizes classless routing. *Open Shortest Path First (OSPF)* is an open link-state routing protocol. It sends out link-state advertisements (LSAs) on attached interfaces, to all other routers within the same hierarchical area. After the link-state information has been accumulated, they use the Shortest Path First algorithm to calculate the shortest path to each node of the network. *Enhanced Interior Gateway Routing Protocol (EIGRP)* incorporates the capabilities of link-

state protocols into distance vector protocols. Under this protocol, no periodic updates are carried out. Upon the detection of a route change, partial updates are sent out. Partial updates are sent only to those routers that need the information. Fast convergence is another factor that distinguishes the protocol from other routing protocols. A router running EIGRP stores all its neighbors' routing tables so that it can quickly adapt to alternate routes [7]. EIGRP is apt for very large networks, having a maximum hop count of 255. As in the network architecture proposed in the paper, redistribution is the requirement of a network running different routing protocols. While running a single routing protocol throughout the entire IP internetwork is desirable, multi-protocol routing may be an outcome of company mergers, multiple departments being managed by multiple network administrators, or multi-vendor environments.

3 Proposed Architecture

The proposed network architecture has been depicted in Fig. 2.The different departments of the organisation, namely IT Operations, Marketing, Human Resource, and Finance, are located in Block 1 and Block 2. Each of the departments is under different VLANs. Each department has been provided an IP phone. Block 3 houses the organisation’s server room, which is the area where all the servers supporting the organisation’s network have been placed. Separate servers have been provided for the organisation’s website, data storage and for DNS service. Block 4 is the area where the Research and Development (R&D) department is located. To increase bandwidth and provide link redundancy, ether channels have been implemented in this area. For employees’ recreation, Cafeteria 1 and Cafeteria 2 have been designed, and Wi-Fi access has been provided. In response to a situation of the link to the primary ISP breaking down, the network incorporates a link from a secondary ISP, which has been administratively turned down. In case the primary ISP fails, the secondary ISP can be pushed into service. Another feature of the network is the application of Frame Relay, to interconnect all the offices of the organisation in the same city or state, those located within smaller distances. Site to site VPN over the internet has been created, to interconnect the organisation’s offices located at larger distances.

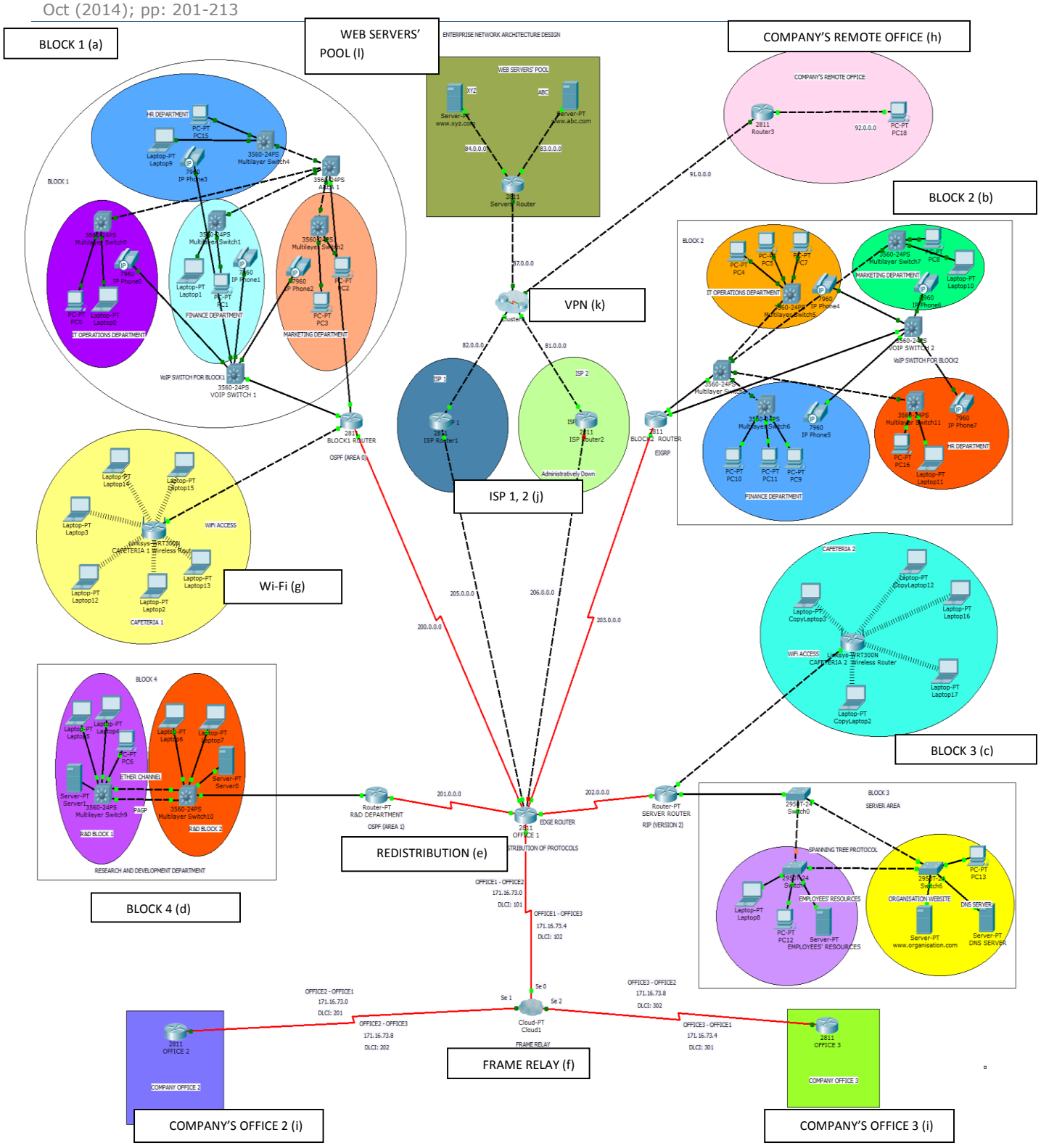

Figure 2: Proposed Network Architecture

4 Results and Discussions

The proposed network is *DHCP* (Dynamic Host Configuration Protocol) enabled. The programming modules prepared for different parts of the network are shown in Fig. 3-9.

Block 1, as shown in Fig. 2(a) is the area where one leg of all the different departments, namely, IT Operations, Marketing, Human Resource, and Finance, are placed. A separate switch for VoIP facility has been used, to which the IP phones for each department are connected. Configuration for VoIP has been depicted in Fig. 3. *Cafeteria 1* is located next to Block 1, and Wi-Fi access has been provided here, as shown in Fig. 2(g) for conducting informal meetings and for employee recreation. OSPF (Open Shortest Path First) routing protocol has been implemented in these areas. Block 1 and Cafeteria 1 are under OSPF area 0.

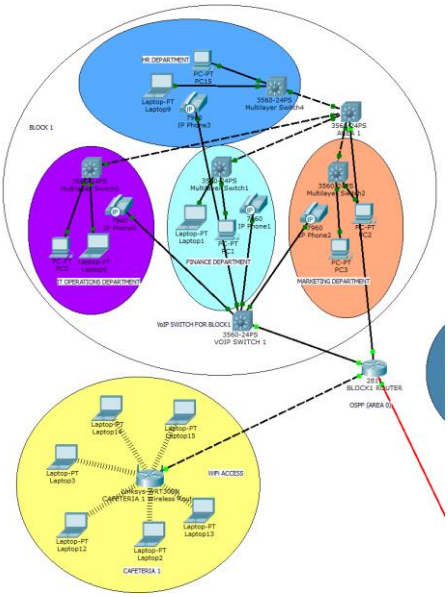

Figure 2(a): Block 1

Block 2, shown in Fig. 2(b) is the area where the second leg of the organisation's departments, along with VoIP Phones, has been placed. *Cafeteria 2* has been designed next to Block 2. *EIGRP (Enhanced Interior Gateway Routing Protocol)* has been implemented in these areas.

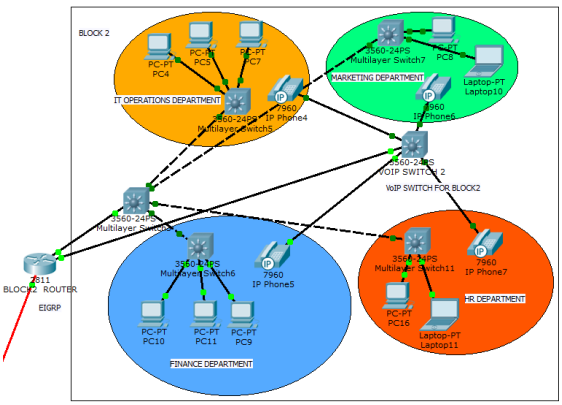

Figure 2(b): Block 2

The servers supporting the organisation's network are present in *Block 3*, which is the *Server Area*, running on *RIPv2* (Routing Information Protocol version 2), depicted by Fig. 2(c). One server is the Employees' resources server, second is the DNS server, and third is the organisation's website server. To provide undeterred access to the servers even in situations where any one of the paths goes down, a redundant path has been provided which has been automatically blocked by *STP (Spanning Tree Protocol)*, to avoid loop formation.

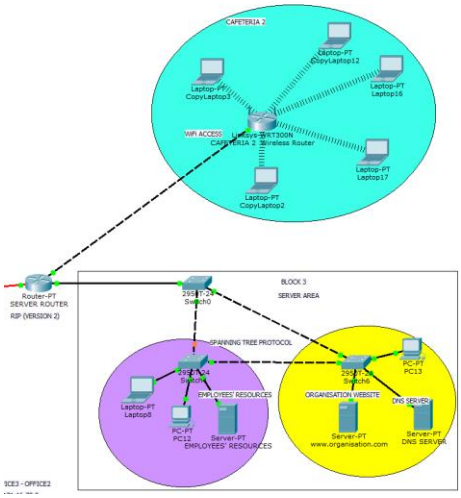

Figure 2(c): Block 3

Block 4, shown in Fig. 2(d) houses the *R&D* (*Research and Development) Department* of the organisation. This area has further been divided into R&D Block 1 and R&D Block 2. In order to shield the organisation's R&D activities from leaking out, ACL has been deployed on the R&D department router, as shown in Fig. 4. Block 4 is thus secured, as neither a user from within the R&D department can reach any other part of the organisation's network or the internet, nor vice versa. Moreover, *Port Security* has been implemented on the switches in the R&D department, as depicted by Fig. 5. The MAC addresses of the verified users' computers have been configured on the ports of the switches, so that an alien user cannot connect to the switch. Also, *Ether Channels* have been deployed between the two switches, i.e. two individual Ethernet links have been bundled into a single logical link. If a segment within an Ether Channel fails, traffic previously carried over the failed link switches to the second segment within the Ether Channel. This has been done to guarantee greater bandwidth as well as uninterrupted communication between the members of the two blocks. The Ether Channels have been configured using the *Port Aggregation Control Protocol (PAgP)*. The configuration has been shown by Fig. 6. Block 4 is running on OSPF and is a part of Area 1.

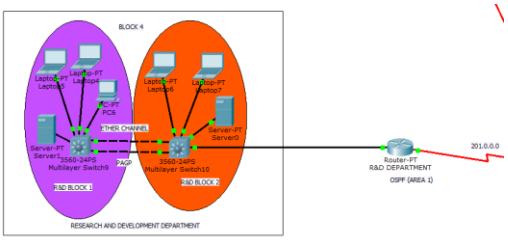

Figure 2(d): Block 4

As the design is an amalgamation of multiple protocols, *redistribution* is necessary, and has been implemented on the edge router, shown in Fig. 2(e), to enable inter-protocol communication between the three protocols, i.e. OSPF, EIGRP and RIPv2.

```
Router#conf t
Router(config)#telephony-service //activating telephony services on the router
Router(config-telephony)#no auto-reg-ephone
Router(config-telephony)#ip source-address 10.0.0.1 port 2000
Router(config-telephony)#max-ephones 10
Router(config-telephony)#max-dn 100
Router(config-telephony)#create cnf-files
Router(config-telephony)#exit
Router(config)#ephone-dn 1 //creating a telephone number for an IP Phone
Router(config-ephone-dn)#number 1000
Router(config-ephone-dn)#exit
Router(config)#ephone-dn 1
Router(config-ephone-dn)#exit
Router(config)#ephone 1
Router(config-ephone)#mac-address 0009.7C08.C930 //registering the telephone number to a particular IP Phone
Router(config-ephone)#exit
Router(config)#dial-peer voice 1 voip //enabling inter-network calls on IP Phones
Router(config-dial-peer)#destination-pattern ....
Router(config-dial-peer)#session target ipv4:200.0.0.1
Router(config-dial-peer)#exit
Router(config)#router ospf 1 //adding the networks of IP Phones to their respective routing configurations
Router(config-router)#network 10.0.0.0 0.0.0.255 area 0
Router(config-router)#network 20.0.0.0 0.0.0.255 area 0
Router(config-router)#network 30.0.0.0 0.0.0.255 area 0
Router(config-router)#exit
```

Figure 3: Configuration of VoIP on Block 1 Router

```
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#access-list 10 deny any //defining an access control list to deny every network
Router(config)#int f0/0
Router(config-if)#ip acc
Router(config-if)#ip access-group 10 out //applying the ACL to the interface connecting R&D department
Router(config-if)#exit
```

Figure 4: Configuration of Access Control List

```
Switch#conf t
Switch(config-if)#switchport mode access
Switch(config-if)#switchport port-security
Switch(config-if)#switchport port-security maximum 1 //defines the maximum number of devices which can be attached
Switch(config-if)#switchport port-security mac-address sticky //adds currently attached device's MAC address to list
Switch(config-if)#switchport port-security violation shutdown
Switch(config-if)#exit
```

Figure 5: Configuration of Port Security in R&D Department

```
Switch(config)#interface  port-channel 3 //configuring the Ether Channels
Switch(config-if)#switchport  trunk encapsulation dot1q
Switch(config-if)#switchport  mode trunk
Switch(config-if)#exit
Switch(config)#interface  range f0/3-4
Switch(config-if-range)#channel-protocol  pagp
Switch(config-if-range)#channel-group  3 mode desirable
Switch(config-if-range)#exit
//The corresponding channel is completed by configuring the same on the opposite switch
```

Figure 6: Configuration of Ether Channels in R&D Department

```
Router#conf t //Redistribution of EIGRP with RIP and OSPF
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#router eigrp 2
Router(config-router)#redistribute rip metric 1000 10 255 255 100
Router(config-router)#redistribute ospf 3 metric 1000 10 255 255 100
Router(config-router)#exit
Router(config)#
//Redistribution of OSPF with EIGRP and RIP, and RIP with OSPF and EIGRP is also carried out
```

Figure 7: Redistribution of routing protocols on edge router

It has been assumed that offices 1, 2 and 3 of the organisation are situated in the city A, with other offices in far-away states and countries. To connect the three offices in the same city, the authors have used *Frame Relay*, shown in Fig. 2(f), as this would lead to cost savings as well as provide high bandwidth according to the *CIR* (Committed Information Rate). *PVCs* have thus been created between each of the three offices, therefore guaranteeing secure and fast transmission of data between the offices. The cloud represents the Frame Relay network and the organisation's offices 2 and 3 have each been depicted by a router, for representational purpose. The configuration has been illustrated in Fig. 8(a)-(b).

```
Router#conf t
Router(config)#int s1/7
Router(config-if)#no ip address
Router(config-if)#encapsulation frame-relay
Router(config-if)#int s1/7.1 point-to-point  //creating sub-interface
Router(config-subif)#frame-relay interface-dlci 101 //providing DLCI to the sub-interface
Router(config-subif)#ip address 171.16.73.1 255.255.255.252 //assigning IP address to the sub-interface
Router(config-subif)#int s1/7.2 point-to-point
Router(config-subif)#frame-relay interface-dlci 102
Router(config-subif)#ip address 171.16.73.5 255.255.255.252
Router(config-subif)#exit
```

Figure 8(a): Configuration for Frame Relay

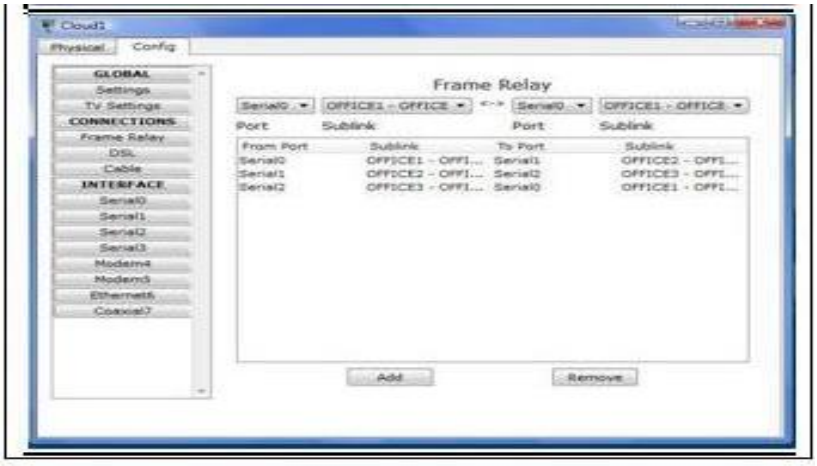

Figure 8(b): Configuration for Frame Relay

ISP (Internet Service Provider) *1* and *ISP 2*, as shown in Fig. 2(j), represent the internal networks of the two Internet Service Providers for the organisation. The link to ISP 2 has been kept in shut-down mode

administratively, and would be activated only in case of the link to the primary ISP shutting down. The network incorporates a connection to the (redundant) secondary ISP, to guarantee uninterrupted internet access for the organisation.

```
Router#configure terminal //configuring VPN tunnel from remote office (Router 3)
Router(config)#interface FastEthernet0/0
Router(config-if)#ip address 91.0.0.2 255.0.0.0
Router(config-if)#exit
Router(config)#router rip
Router(config-router)#version 2
Router(config-router)#network 92.0.0.0
Router(config-router)#network 91.0.0.0
Router(config-router)#exit
Router(config)#crypto isakmp policy 10
Router(config-isakmp)#authentication pre-share
Router(config-isakmp)#encryption aes 256
Router(config-isakmp)#group 2
Router(config-isakmp)#lifetime 86400
Router(config-isakmp)#exit
Router(config)#crypto isakmp key toor address 91.0.0.1
Router(config)#crypto ipsec transform-set TSET esp-aes esp-sha-hmac
Router(config)#access-list 101 permit ip 92.0.0.0 0.255.255.255 82.0.0.0
0.255.255.255
Router(config)#crypto map CMAP 10 ipsec-isakmp
Router(config-crypto-map)#set peer 91.0.0.1
Router(config-crypto-map)#match address 101
Router(config-crypto-map)#set transform-set TSET
Router(config-crypto-map)#exit
Router(config)#int f0/0
Router(config-if)#crypto map CMAP
*Jan 3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
//Configuration of VPN tunnel is also carried out on the Block 1 Router as well as
all the intermediate routers.
```

Figure 9: Configuration for VPN

The *Web Servers' Pool*, shown in Fig. 2(l), represents the servers of two websites, namely, *www.xyz.com* and *www.abc.com*. This area is running on RIPv2.

Company's Remote Office, as shown in Fig. 2(h), represents one of the offices of the organisation, in a different region or country. A *site-to-site VPN*, shown in Fig. 2(k), has been established between the remote office and the office under consideration, configuration as shown by Fig. 9. A secure *IPSec tunnel* has been set up starting from the remote office's router to the Block 1 router, for representational purposes. Traffic between the two offices is transmitted over the internet at best effort. Therefore, remote offices of the organisation are connected to each other as though they are a part of the same network.

4.1 Demonstration

The network, when simulated on Cisco Packet Tracer, produced the following results:

(a). On trying to ping a member of the R&D Department from another part of the network, the result "Destination Host Unreachable" gets displayed. The result has been illustrated in Fig. 10(a).

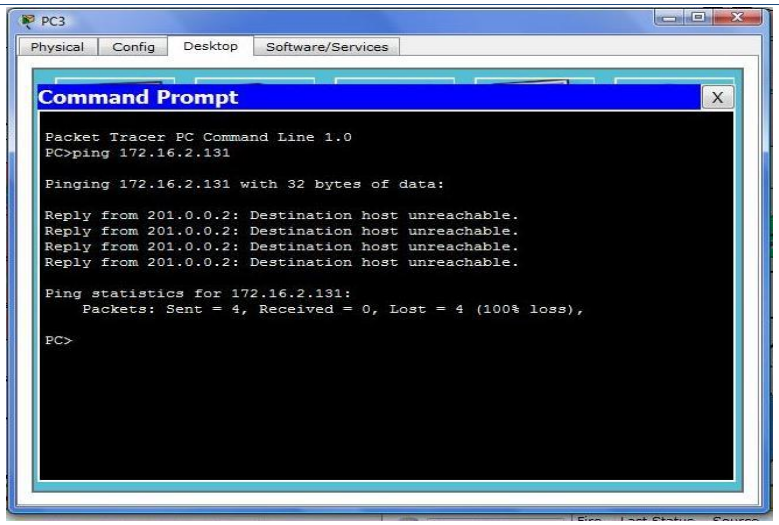

Figure 10(a): Unreachable host of R&D Department

(b). When a member of the R&D Department tries to ping a member of say, Block 1, "Request Timed out" gets displayed, as depicted by Fig. 10(b).

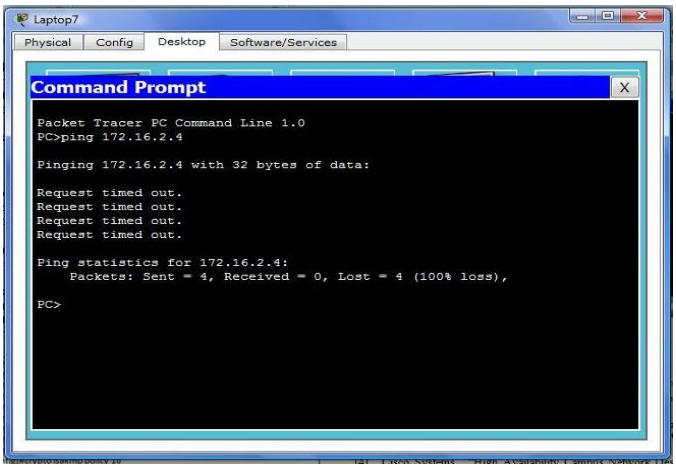

Figure 10(b): Host of another Block inaccessible from R&D Block

Thus, it can be concluded that the R&D Department has been well shielded from the outside network by the ACL.

Thus, winding up in a nutshell, the fact that nowadays in an organization, peer-to-peer communication is a more important part of Local Area Networks than client-server communication, led to the incorporation of Voice over Internet Protocol in the proposed design. Moreover, VoIP is advantageous as it leads to cost savings and poses no geographical boundaries. In case of the connection to the primary ISP breaking down, a redundant connection to a secondary ISP has been provisioned to guarantee 24*7 internet connectivity. The R&D department in the designed network has been supplied with Ether Channel technology to guarantee the best availability of resources and its functionality under the most severe circumstances. The isolation of R&D department from the other parts of the organization and the exterior world could be possible due to implementation of software firewall in the form of Access Control List. The sensitive company data on the servers of R&D department has been

secured by incorporation of Port Security in the area, which will prevent anyone to disconnect the presently connected computers, connect any unauthorized device and hack the data. Also, established as a network of privately owned equipment, Frame Relay is able to connect multiple offices of the organization in the same city. Site to site VPN is able to utilize the flexibility and ubiquity of the Internet in connecting remote offices of the organisation, for the holistic working and growth of the entire enterprise.

REFERENCES

[1]. Andrew S. Tanenbaum, 2003, Computer Networks, Prentice Hall PTR

[2]. Campus LAN Design Guide: Design Considerations for the High-Performance LAN, Juniper Networks, Inc., 2009

[3]. Martin W. Murhammer, Kok-Keong Lee, Payam Motallebi, Paolo Borghi, Karl Wozabal, IP Network Design Guide, IBM Corporation, 1999

[4]. Cisco Systems, "High Availability Campus Network Design--Routed Access Layer using EIGRP or OSPF", 2007

[5]. Qutaiba Ali, Salah Alabady, and Yehya Qasim, "Applying reliability solutions to a cooperative network," International Arab Journal of e-Technology, Vol. 1, No. 2, pp. 9-17, June 2009

[6]. Saadat Malik, Network Security Principles and Practices: Expert solutions for securing network infrastructures and VPNs, Cisco Press, 2003

[7]. Cisco Systems, Internetworking Technology Handbook, 2012

[8]. T-Systems, White paper- "Voice over Internet Protocol (VoIP)"

[9]. Hewlett Packard – "Frame Relay Networks", Digital Technical Journal, Vol. 5, No. 1, Winter 1993

[10]. Sprint, White paper- "Frame Relay vs. IP VPNs"

[11]. Cisco Systems, "Scaling Networks Companion Guide", 2014

