METRO ETHERNET RING AT MCS

By

Muhammad Sohaib Hassan

Ahmed Altaf

Ihsan Afzal

Directing Staff

Lt. Col. Imran Rasheed

Submitted to the Faculty of Department of Electrical Engineering
Military College of Signals, National University of Sciences and Technology, Islamabad
in partial fulfillment for the requirements of a B.E Degree in Telecom Engineering

June 2013

CERTIFICATE OF CORRECTNESS AND APPROVAL

Certified that work contained in this thesis “Metro Ethernet Ring at MCS”, was carried out by Muhammad Sohaib Hassan, Ahmed Altaf and Ihsan Afzal under the supervision of Lt. Col. Imran Rasheed for partial fulfillment of Degree of Bachelor of Telecommunication Engineering, is correct and approved.

Approved by

____

(Lt. Col. Imran Rasheed)
Project Directing Staff (DS)
Military College of Signals (MCS)

Dated: _____ June 2013

ABSTRACT

Ethernet has been the indisputable technology of choice for local area networks (LANs) for more than 30 years. Its attractiveness is due to its flexibility, plug and play features and low cost. Despite its popularity it is still restricted to local area networks, and is not ready to become a carrier grade technology for wide areas. Metro Ethernet Network (MEN) is a switched high bandwidth layer-2 technology that connects or bridges geologically segregated LANs.

Metro Ethernet Network is also capable of managing broadband applications of voice, video and data services. This unification of services and their convergence to a single network reduces the equipment cost, eases administrative work, a single line requirement to access all services and most importantly provides efficient utilization of bandwidth. This capability of unifying services and their convergence to a single network is a concept of Next Generation Network (NGN).

Military College of Signals (MCS) decided to initiate work on Metro Ethernet Networks to enable the advantage of productivity-enhancing IP communication such as IP video calling, video conferencing, instant messaging, streaming and broadcast video in its departments that are difficult to implement on TDM network of PASCOM. It was also decided to give emphasis on the integration of Metro Ethernet Network with PASCOM to remain connect with PASCOM users. To connect all departments we utilized optical fiber which covers the departments in the form of rings, so called Metro Ethernet Ring.

Accepting this challenge of installing a Metro Ethernet Network in our college we in a group of three students started work on this project to providing IP video calling facility over EE and CS Department and its LABs and integration of this network with PASCOM. Also we have to implement security features over this network to prevent any kind of foreign intrusion.

DEDICATED TO OUR BELOVED FAMILIES

ACKNOWLEDGEMENTS

We are grateful to our Project Supervisor Lt. Col. Imran Raheed who supervised the project in a very encouraging and helpful manner. As supervisor, his support and guidance has always been a valuable asset for our project. We are really thankful to his worthless contributions in our project work.

It is true to say, most of the things in our work would not have been possible without their mature and professional support. They have been a true guidance in difficult times and always providing insightful comments. We would like to pay all our gratitude to the staff NGN-Lab at Military College of Signals for providing us a congenial environment. We are obliged to their support in understanding official procedures. We have found people here very cooperative and fun to work with.

Heartfelt thanks and appreciation must also go to our beloved parents for their financial and moral support throughout the project. We are also grateful to the whole staff of the Department of Electrical Engineering for their support in all forms.

Contents

Table of Figures

List of Tables

LIST OF SYMBOLS/ABBREVIATIONS

TDM	Time division Multiplexing
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
SIP	Session Initiation Protocol
MGCP	Media Gateway Control Protocol
SCCP	Skinny Client Control Protocol
GW	Gateway
UAC	User Agent Client
UAS	User Agent Server
QoS	Quality of Service
VoIP	Voice over Internet Protocol
LAN	Local Area Network
WAN	Wide Area Network
MEN	Metro Ethernet Network
MCS	Military College of Signals
VLAN	Virtual LAN
NGN	Next Generation Network
CUCM	Cisco Unified Communication Manager
STP	Spanning Tree Protocol
STA	Spanning Tree Algorithm

Chapter: 1

INTRODUCTION

1.1 Problem Statement

Network carriers today are not only email or voice communications. They are much more than that and involves real-time communication capabilities including voice, instant messaging, video conferencing and data sharing, as well as non-real-time functionality such as email, voicemail, unified messaging and fax. These services are difficult to implement on TDM networks because of limited bandwidth or processing resources. Also, due to missing ingredients of bandwidth, speed, QoS, and scalability these services cannot be provided on already installed packet switched network in MCS. Also there was a critical need of inter-LAN communication to keep departments and members of MCS in touch regardless of where they are located and a centralized mechanism is required to monitor and control all these services.

1.2 Background

MCS has its own packet switched network for data communication and for Internet access. For voice communication MCS is being using TDM based circuit switched network of PASCOM, which is Pakistan Army's own telephony network operating along the whole country. So, there was a limitation of keeping both networks and infrastructures together for data and voice communication. Also MCS has already installed optical fiber which connects its departments in the form of rings.

MCS decided back in 2009 to develop a network in their college (utilizing these optical fiber rings) which could carry voice and data traffic along with video communication. As convergence of these services best suited to an IP based network, so integration of PASCOM with this new IP based network was also added to plan. Accepting this challenge of establishment of Metro Ethernet Network in our college we in a group of three students started work on this project.

1.3 Solution

Metro Ethernet Networks is the answer to these missing ingredients. Metro Ethernet Network is a switched, flexible, easy-to-use and high bandwidth Layer-2 technology that enables enterprises to converged voice, data, and video services on a single network such as IP telephony, video streaming and data storage. Metro Ethernet Rings allow us to connect multiple departments of MCS segregated by their physical locations within a service area supporting transmission speeds as low as 3 Megabits per second (Mbps) and up to 1 Gigabits per second (Gbps). This allows for flexible growth and permits us to choose a bandwidth profile that fits our real-time traffic needs. Also we can integrate already deployed TDM network of MCS to remain in touch with PASCOM's users.

1.4 Objectives

Following were the tasks and objectives defined by MCS for this project.

i. Design a Metro Ethernet Ring of ME-switches over optical fiber to cover EE-Department, CS-Department and NGN-LAB, which includes:
   a. Establishment of Core Network in NGN-LAB.
   b. Attachment of EE and CS-Department with NGN-LAB.
   c. Deployment of Router and Switches over this network
   d. Installation of Voice/Video supported versions of IOS on devices
   e. Enable and efficient configuration of desired routing and switching protocols in this network

ii. Enabling Voice/Video services in Metro Ethernet Network which includes:
   a. Installation of a Call manager (server) to monitor and control Voice/Video services
   b. Creating database for users, registering them and assign directory numbers to users
   c. Install a backup server for this call manager

iii. Integration of PASCOMs with this ME network

iv. Implement security features which includes installation of firewall device, enabling campus based security and MAC-base security.

Chapter: 2

NETWORK ARCHITECHTURE

2.1 Introduction

In this project of Metro Ethernet Network our main focus is to provide IP voice/video calling facility in MCS and the integration with PASCOM with this IP network. To complete these tasks we divided our network into three main logical parts/layers based on functions, roles and classification of devices involved in the project [1].

Core
Distribution
Access

Figure2.1 Layer Based Hierarchy of Metro Ethernet Network

2.2 Core Layer

This layer consist of all network controlling agents/devices e.g. call manager, firewall, and voice gateway router. We established Core Network in NGN-LAB. Here voice gateway router installed for the connectivity with PASCOM, firewall to implement security and call manager which is the call-processing and controlling component of IP telephony.

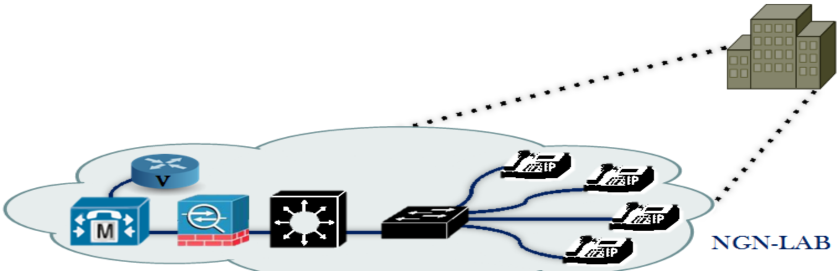


Figure 2.2 Core Layer of Metro Ethernet Network

2.2.1 Voice Gateway

Voice gateways are devices that communicate with other voice gateways, gatekeepers, their respective endpoints, and call control agents, such as Cisco Unified Communications Manager or a PBX via voice signaling and media protocols which include MGCP, H.323, SIP, SCCP and RTP. In VoIP networks, the primary purpose of voice gateways is to provide an interface between the VoIP network and the Public Switched Telephone Network (PSTN) [2]. This traditional use of voice gateways is illustrated in figure2.3.

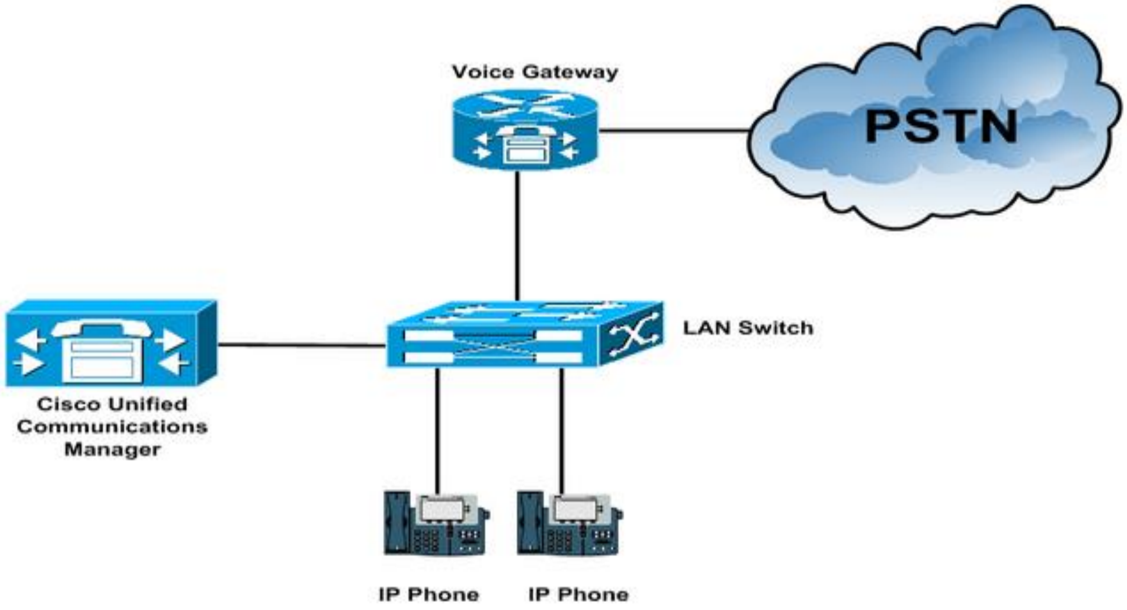


Figure2.3 Basic VoIP Network Integrated with PSTN

As illustrated in the diagram above, the voice gateway is connected to both the VoIP network and the PSTN. The gateway interfaces with the IP network and the PSTN and supports IP signaling control protocols used in Voice over IP, and Time Division Multiplexing (TDM) control protocols used on the PSTN.

2.2.2 Call Manager

Call Manager extends enterprise telephony features and functions to packet telephony network devices. These packet telephony network devices include Cisco IP Phones, media-processing devices, VoIP gateways, and multimedia applications as shown in figure2.3. It provide additional data, voice and video services such as converged messaging, multimedia conferencing, voice mail, call parking call transfer and all services that interact with the IP telephony [3].

Main functions of Call Manager are:

Call processing: Call processing refers to the complete process of originating, routing, and terminating calls, including any billing and statistical collection processes.

Signaling and device control: Call manager sets up all the signaling connections between call endpoints and directs devices such as phones, gateways, and conference bridges to establish and tear down streaming connections. Signaling is also referred to as call control and call setup/call teardown.

Dial plan administration: The dial plan is a set of configurable lists that CUCM uses to perform call routing. CUCM is responsible for digit analysis of all calls. CUCM enables users to create scalable dial plans.

Phone feature administration: CUCM extends services such as hold, transfer, forward, conference, speed dial, redial, call park, and many other features to IP phones and gateways.

Directory services: CUCM uses its own database to store user information. User authentication is performed locally or against an external directory. Directory synchronization allows for centralized user management. Directory synchronization allows CUCM to leverage users already configured in a corporate-wide directory.

Backup and restore tools: CUCM provides a Disaster Recovery System (DRS) to back-up and restore the CUCM configuration database. The DRS system also backs up call details records (CDR), call management records (CMR), and the CDR Analysis and Reporting (CAR) database.

2.2.3 Firewall

A firewall is a set of related programs, located at a network gateway server that protects the resources of a private network from users from other networks. An enterprise with an intranet that allows its workers access to the wider Internet installs a firewall to prevent outsiders from accessing its own private data resources and for controlling what outside resources its own users have access to.

Cisco firewall can operate either in transparent mode or routed mode which work on layer 2 and layer 3 respectively [4].

Transparent Mode:

Firewall acts as a bridge, mean it decides on basis of MAC addresses. It does not mean that it does not IP at all. It mean whether packet is to be forwarded or not is based on MAC addresses but all the inspections and all security features is based on IP address information. Figure 2.4 is a simple example in which a user attached to its gateway (multi-layer switch here) via firewall.

As firewall act as a transparent Ethernet bridge, it sends packet in or out on basis of MAC addresses and we can see that in and out interfaces have same subnet and IP given to fire wall also from same subnet so it is nothing more than a same user on the same segment. So in transparent mode only one interface will get an IP address and this is the management interface.

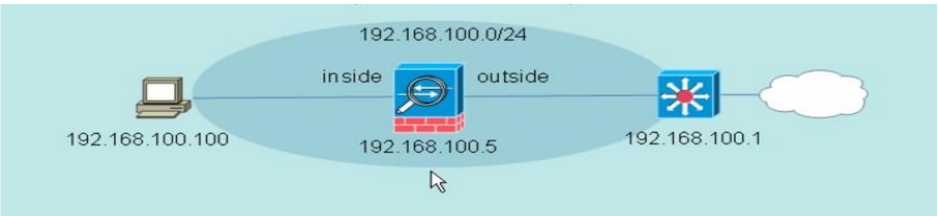


Figure2.4: Firewall in Transparent Mode

Routed Mode

In routed mode firewall works on layer 3 mean packets forward and all security features are implemented on basis of IP address information. Now firewall acts as a layer three boundary and inside users must use fire wall as a gateway.

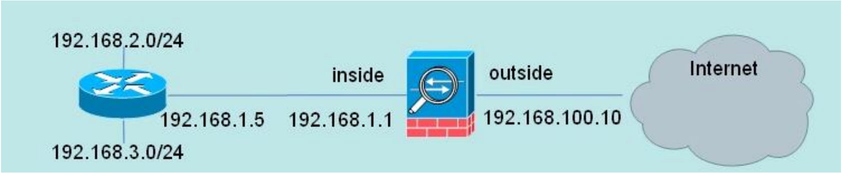


Figure2.5: Firewall in Routed Mode

Mean inside and outside interface are two separate subnets and firewall has one IP address for inside and one for outside interface.

2.3 Distribution Layer

Distribution layer includes LAN-based routers and layer-3 switches. This layer ensures that packets are properly routed between subnets and VLANs in your enterprise. This layer is also called the Workgroup layer. It is responsible to distribute services of voice video and data from core network to among LANs of an Enterprise.

Devises on this layer can be used for many other services. We used layer-3 switch to perform

- DHCP configuration
- Inter-VLAN routing
- Formation of access-control lists

A Layer 3 switch works much like a router because it has the same IP routing table for lookups and it forms a broadcast domain. However, the “switch” part of “Layer 3 switch” is there because:

1. The layer-3 switch looks like a switch. It has 24+ Ethernet ports and *no* WAN interfaces.
2. The layer-3 switch will act like a switch when it is connecting devices that are on the same network.
3. The layer-3 switch is the same as a switch with the router’s IP routing intelligence built in.
4. It works very quickly to switch or route the packets.

In other words, the Layer 3 switch is really like a high-speed router without the WAN connectivity.

We use layer-3 switch to perform distribution layer function as:

1. To Increase scalability: Number of Ethernet ports in layer-3 switch are greater than a router, which can be used to connect access nodes later. Also router is more expensive as layer-3 switch.
2. We can enable spanning tree to create a redundant path

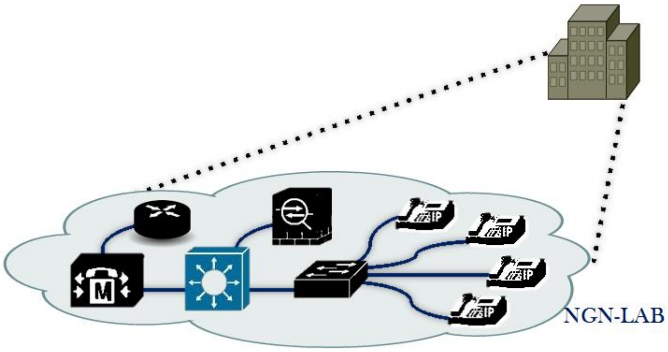


Figure2.6: Distribution Layer of Metro Ethernet Network

2.4 Access Layer

This layer consists of devices or media that provide connection of voice/video and data clients to our ME network like switches. This layer is also called the desktop layer because it focuses on connecting client nodes, such as workstations or IP phones to the network. This layer ensures that packets are delivered to end user or clients.

In our project this Layer consists of two main components:

- Optic fiber media.
- Layer two/Access switches (ME-3400)

Optical fiber media installed in MCS cover it’s departments is the form of loops as shown in figure2.7. It a single mode fiber and we are using SFPs supporting 1330nm wavelength in half duplex links.

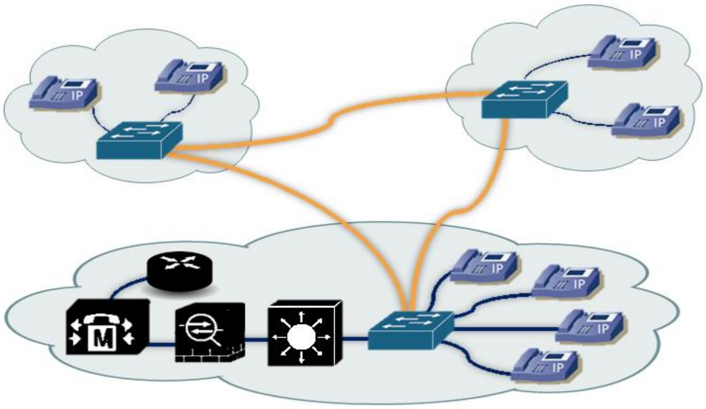


Figure2.7: Access Layer of Metro Ethernet Ring

If we look switches are connected via optical fiber ring (shown in orange color in above figure2.7). So, there might be a possibility of loop formation in our network. So we configured spanning tree protocol in our network to avoid formation of loops.

2.5 Spanning Tree Protocol (STP)

The Spanning tree protocol is a data link layer protocol that ensures a loop-free topology for any local area network [5].

As spanning tree gives a loop-free topology, it allows a network engineer to include spare (redundant) links to provide backup paths. These redundant links automatically made active by STP without the need for manual enabling/disabling of these backup paths. STP uses *spanning-tree algorithm* to create first a topology database and then search out and disables redundant links. STP uses spanning-tree algorithm (STA). STA form a topology database first and then locate the redundant links.

2.5.1 Spanning-Tree Algorithm (STA)

1. **Root Bridge:** It is the focal point for all the switches in a STP environment. All switches selects best/single path towards that root bridge.
2. **BPDU:** This is the packet that switches exchanges. This packet has many fields include several parameters. These parameters used in the selection of Root Bridge and subsequent configuration of switches. This packet is called Bridge Protocol Data Unit (BPDU).

3. **Bridge ID:** Bridge ID is the combination of two major fields of BPDU, first is the *Priority* and the other is *MAC address*. Bridge ID is used in selection of Root Bridge. Priority is from 0 to 61,440 (32,768 by default on all CISCO switches). Switch having the lowest bridge ID is designated as Root Bridge.
4. **Non-root Bridge:** These are the switches that are not Root Bridge.

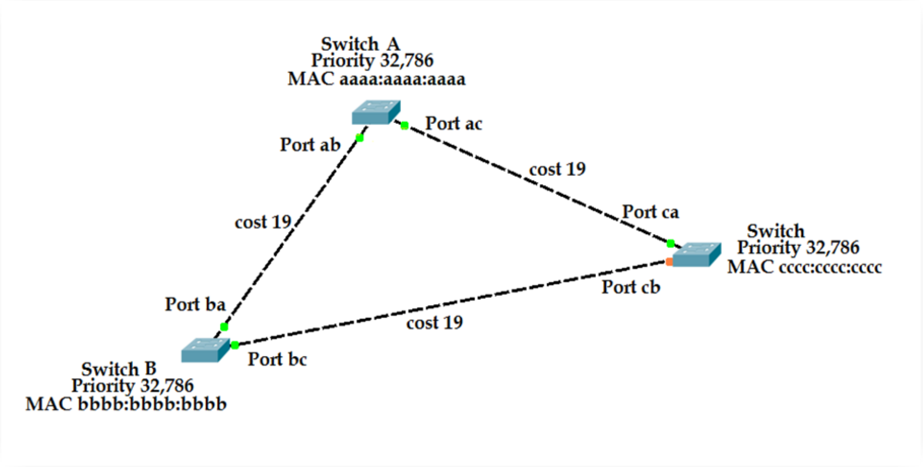


Figure2.8: Basic Spanning Tree Diagram

5. **Port cost:** It is also a field of BPDU. A decimal value assigned to a link on basis of its bandwidth. Port cost against bandwidth given in table 2.1.
6. **Port types:**
   a) **Root port:** The ports used by Nonroot Bridges to reach Root Bridge. In figure 2.8 *port ba* and *port ca* are also root ports as they are used by switch B and C to reach Root Bridge (switch A) respectively.
   b) **Forwarding port:** A port that forwards frames. It can be a Root Port or a Designated Port.
   c) **Blocked port:** A port which is not shutdown but only logically down, mean it do not forwards frames in order to prevent loops.
   d) **Designated port:** A Forwarding port, **one per link**. In the link between switch A and B of figure 2.8 *port ba* and *port ca* are the *Root Ports* and *port ab* and *port ac* are Designated Ports as it is used for forwarding frames and also not a Root Port. So ports of Root Bridge can never ever be Root Ports and are Designated Ports.

e) **Nondesignated port:** A port having cost higher then Designated Port. These are the ports that are left over after Root Ports and Designated Port have been determined. Nondesignated Ports are put in blocked mode i.e. they are not Forwarding Ports. In figure 2.8 *port cb* is a Nondesignated or Blocked port.

2.5.2 Spanning Tree Operation

As Spanning Tree Protocol job is to identify and disable any redundant link in the network. It does this by first electing a Root Bridge. In this election all switches participate. They exchange their BPDUs for the polling of Root Bridge. Switch having lowest Bridge ID wins the election and becomes Root Bridge. For lowest bridge ID first the priority is checked. If the priorities of all switches are different, then the switch having lowest priority would be elected as *Root Bridge*. If the priorities of all switches are equal, then the decision would be taken on the basis of MAC address (lowest). In figure 2.9 all switches have equal priority. So, switch A which has lowest MAC is the Root Bridge in this network**.** In next step Nonroot Bridges starts locating best path towards Root Bridge. For this selection they consider cost field of BPDU. In figure 2.9 Switch B have two paths to reach switch A. First path is the direct one (shown by red color) having cost 19 (100 Mbps link). Second path (shown by blue color) is through switch C and has total cost of 38 (19+19). So first path would be selected having lowest cost and second path is

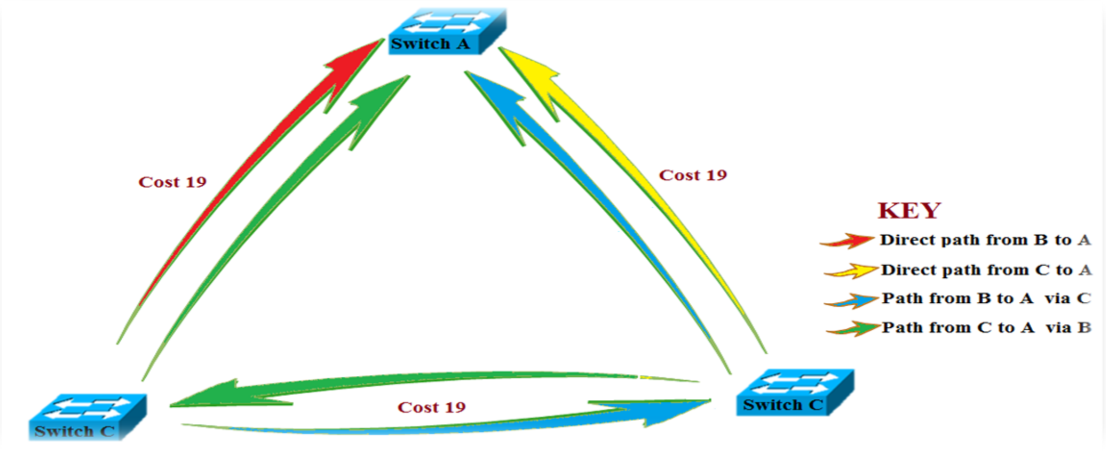


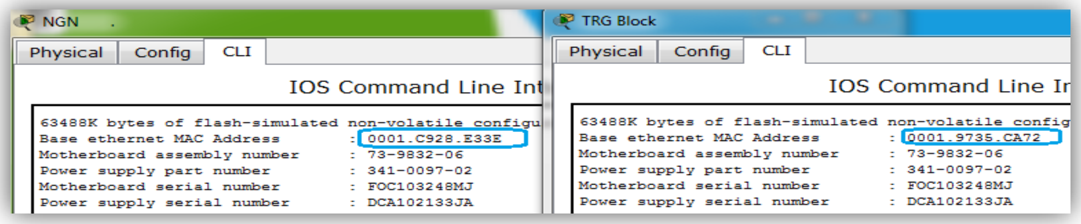
Figure2.9: Spanning Tree Operation

been considered as redundant path. If cost of two paths to root switch is equal then the decision is based on best Bridge ID.

Link Speed	Cost (Revised by IEEE Spec)
10 Gbps	2
1Gbps	4
10oMbps	19
10Mbps	100

Table1: Path cost based on the rated bandwidth of different links

Both port of redundant link are not kept in blocked mode. In fact one port is forwarding port and other is blocked. This is because when a link is down in a network, switch with forwarding port (of redundant link) send a request to the blocked port. Blocked port which is logically down (cannot send the frame), but it can receive frames. In response to this specific request it changes its status from blocked port to forwarding port. Switch having best Bridge ID would keep its port forwarding in a redundant link.



```
63488K bytes of flash-simulated non-volatile configu
Base ethernet MAC Address          : 0001.C928.E33E
Motherboard assembly number        : 73-9832-06
Power supply part number           : 341-0097-02
Motherboard serial number          : FOC103248MJ
Power supply serial number         : DCA102133JA
```

```
63488K bytes of flash-simulated non-volatile config
Base ethernet MAC Address          : 0001.9735.CA72
Motherboard assembly number        : 73-9832-06
Power supply part number           : 341-0097-02
Motherboard serial number          : FOC103248MJ
Power supply serial number         : DCA102133JA
```

Figure2.10: MAC-Based Decision in Spanning Tree

In figure 2.10 there is a redundant link between NGN switch and Cadet Wing switch. As both switches have equal priority, so switch having lowest MAC should have best Bridge ID which is Cadet Wing switch (shown in figure 2.8). So port of NGN switch is blocked

Chapter: 3

CONNECTING IP PHONES TO LAN INTERFACES

3.1 Introduction

When an IP phone connects to an Ethernet switchport and powered on, the Cisco switch delivers voice VLAN information to the IP phone. When IP phone know its VLAN it should use it sends a DHCP request asking for an IP address on its voice VLAN. The layer -3 device connecting to the voice VLAN receives this DHCP request. The DHCP server responds with an IP for IP phone and also carries an option field (150). This option includes the IP of TFTP server. Once the Cisco IP phone has the IP address of the TFTP server, it contacts the TFTP server and downloads its configuration file. Included in the configuration file is a list of valid call processing agents (such as Cisco Unified Communications Manager or CME agents).

Following this hierarchy let start with VLANs

3.2 VLANs

When VLANs were introduced a number of years ago, the concept was so radical and beneficial that it was immediately adopted into the industry. Nowadays, it is rare to find any reasonably sized network that is not using VLANs in some way [6].

Switched networks can be broken up into distinct broadcast domains or virtual LANs (VLANs). A network with a single broadcast domain can be simple to implement and manage. However, flat network topology is not scalable (A fully Layer 2 switched network is referred to as a flat network topology). Instead, the network can be divided into segments using VLANs, while Layer 3 routing protocols manage inter-VLAN communication.

Consider a network design in figure3.1 that consists of Layer 2 devices. For example, this design could be a single Ethernet segment, an Ethernet switch with many ports. A flat network is a single broadcast domain, such that every connected device sees every broadcast packet that is transmitted. As the number of stations on the network increases, so does the number of broadcasts.

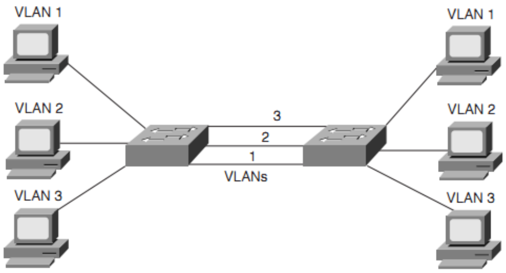


Figure 3.1: One Inter-switch link per VLAN

A switched environment offers the technology to overcome flat network limitations. Switched networks can be subdivided into virtual LANs (VLANs). By definition, a VLAN is a single broadcast domain. All devices connected to the VLAN receive broadcasts from other VLAN members. However, devices connected to a different VLAN will not receive those same broadcasts.

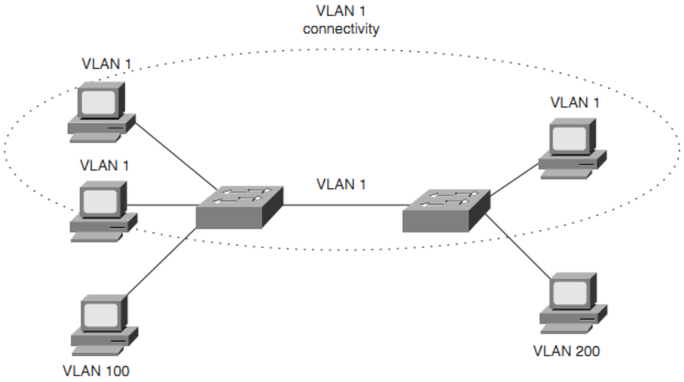


Figure 3.2: No Inter- VLAN Broadcast and Inter-switch trunks

Layer 2 switches are configured with a VLAN mapping and provide the logical connectivity between the VLAN members. Figure3.2 shows how a VLAN can provide logical connectivity between switch ports. Two workstations on the left of switch are assigned to VLAN 1, while a third workstation is assigned to VLAN 100. In this example, there can be no communication between VLAN 1 and VLAN 100. One workstation on the right side is also assigned to VLAN 1. Because there is end-to-end connectivity of VLAN 1, any of the workstations on VLAN 1 can communicate as if they were connected to a physical network segment.

3.22 VLAN Trunks

At the access layer, end user devices connect to switch ports that provide simple connectivity to a single VLAN each. The attached devices are unaware of any VLAN structure and simply attach to what appears to be a normal physical network segment. Remember, sending information from an access link on one VLAN to another VLAN is not possible without layer 3 device.

Inter-VLAN communication is possible by providing separate physical links for each VLAN N with layer 3 device. A trunk link, however, can transport more than one VLAN through a single switch port. Trunk links are most beneficial when switches are connected to other switches or switches are connected to routers. A trunk link is not assigned to a specific VLAN. Instead, one, many, or all active VLANs can be transported between switches using a single physical trunk link.

To distinguish between traffic belonging to different VLANs on a trunk link, the switch must have a method of identifying each frame with the appropriate VLAN. Frame identification, or tagging, assigns a unique user-defined ID to each frame transported on a trunk link. This ID can be thought of as the VLAN number or VLAN "color," as if each VLAN was drawn on a network diagram in a unique color. As each frame is transmitted over a trunk link, a unique identifier is placed in the frame header. As each switch along the way receives these frames, the identifier is examined to determine to which VLAN the frames belong. Identifier is attached at sending interface (trunk port) and removed at the receiver side.

3.3 Understanding Voice VLANs

It is a common and recommended practice to separate voice and data traffic by using VLANs. Separating voice and data traffic using VLANs provides a solid security boundary, keeping data applications from reaching the voice traffic. It also gives you a simpler method to deploy QoS, prioritizing the voice traffic over the data.

One initial difficulty you will encounter when separating voice and data traffic is the fact that PCs are often connected to the network using the Ethernet port on the back of a Cisco IP phone. Because you can assign a switchport to only a single VLAN, it initially seems impossible to separate voice and data traffic. That is, until you see that Cisco IP phones support 802.1Q tagging.

The switch built into Cisco IP phones has much of the same hardware that exists inside of a full Cisco switch. The incoming switchport is able to receive and send 802.1Q tagged packets. This gives you the capability to establish a trunk connection between the Cisco switch and IP phone, as shown in figure3.3.

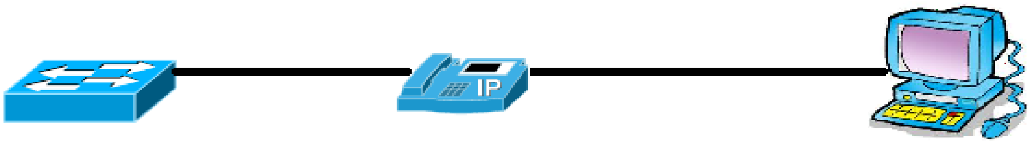


Figure 3.3: IP Phone act as a Switch Port for Data User

You might call the connection between the switch and IP phone a “mini-trunk” because a typical trunk passes a large number of VLANs (if not all VLANs). In this case, the IP phone tags its own packets with the correct voice VLAN. Because the switch receives the tagged packets on a port configured as a trunk (or a mini-trunk in our case), the switch can read the tag and place the data in the correct VLAN. The data packets pass through the IP phone and into the switch untagged. The switch assigns these untagged packets to whatever VLAN you have configured on the switchport for data traffic.

3.4 Configuring DHCP Server

IP phones in a network need IP addresses and TFTP server information. We have three options to configure DHCP server. Call Manager, voice gateway and layer-3 switch. But we configured DHCP on layers-3 switch because it is the only device that deals with both data and voice traffic, as we have to form two DHCP pools in our network. One pool for VOICE enabled clients and one for data users.

3.4.1 Reason of using DHCP

DHCP can minimizes configuration errors caused by manual IP address configuration, such as typographical errors, or address conflicts caused by the assignment of an IP address to more than one computer at the same time [7]. Thus we include DHCP configuration in our network design because of its following features:

- ❑ Centralized and automated IP configuration.
- ❑ The ability to define IP configurations from a central location.
- ❑ Isolate gateway or administrator IPs from being assigned to users. This is done by excluding that IPs from DHCP pool.
- ❑ To synchronize our user with configuration or design changes in our network.
- ❑ The ability to utilize efficiently full range of IPs.
- ❑ The efficient handling of complete IP subnet by assigning IPs to only enabled clients.

<u>DHCP pools</u>

In this we have assigned subnet 192.168.1.200/24 to 192.168.1.254/24 for our IP phones and VOICE services. Here we reserved 1st 50 IPs for administrative purposes.

For data user we have configured subnet 172.23.16.51/24 to 172.23.16.200. Here again 1st 50 IPs are reserved for administrative purposes.

TFTP in our project is call manager which is responsible for providing IP phone with initial configuration.

Chapter: 4

PROCESSING OF VOICE TO PACKETS

4.1 Introduction

Telephone equipment can accurately transmit understandable human conversation by sending only a limited range of frequencies. The telephone channel frequency range (300–3400 Hz) gives you enough sound quality to identify the remote caller and sense their mood. According to Nyquist criteria we can reproduce an audio signal by sampling at twice the highest frequency. It would mean sampling approximately 8000 times every second [8].

4.2 Sampling

In the voice realm, a sample is a numeric value that consumes a single byte of information. As Figure4.1, illustrates that during the process of sampling, the sampling device puts an analog waveform against a Y-axis lined with numeric values.

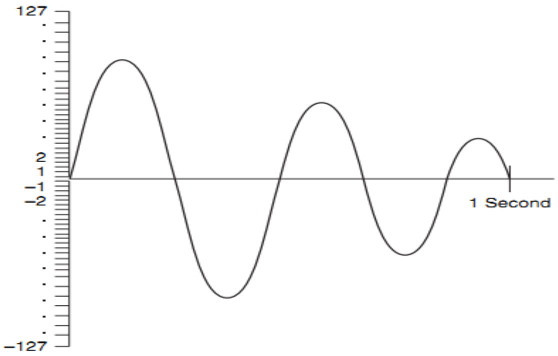


Figure 4.1: Sampling and Quantization of Voice

4.3 Quantization

This process of converting the analog wave into digital, numeric values is known as quantization. Because 1 byte of information is only able to represent values 0–255, the quantization of the voice scale is limited to values measuring a maximum peak of +127 and a maximum low of –127.

4.4 Uncompressed Codec

Now, remember, the Nyquist theorem dictates that you need to take 8000 of those samples every single second. Doing the math, figure 8000 samples in a second times the 8 bits in each sample, and you get 64,000 bits per second. It’s no coincidence that uncompressed audio (including the G.711 audio codec) consumes 64 kbps. Once the sampling device assigns numeric values to all these analog signals, a router can place them into a packet and send them across a network.

4.5 Compressed Codec

The last and optional step in the digitization process is to apply compression measures. Advanced codecs, such as G.729 [9], allow you to compress the number of samples sent and thus use less bandwidth. This is possible because sampling human voice 8000 times a second produces many samples that are very similar or identical. For example, say the word “cow” takes about a second to say. There’s the very distinguished “k” sound that starts the word, then you have the “ahhhhhh” sound in the middle, followed by the “wa” sound at the end. Most compressed codecs use to compress this audio is to send a sound sample once and simply tell the remote device to continue playing that sound for a certain time interval. Using this process, G.729 is able to reduce bandwidth down to 8 kbps for each call which is a fairly massive reduction in bandwidth. Bandwidth comparison of some codecs is shown in table 2.

Codec	Bandwidth Consumed
G.711	64 kbps
iLBC	15.2 kbps
G.729	8 kbps
G.726	32 kbps
G.729a	8 kbps
G.728	16 kbps

Table 2 Bandwidth Comparisons of Codecs

4.6 Choosing a voice codec

When selecting a voice codec for your network, you should ask the following questions regarding the codec:

- Is the codec supported on all VoIP devices in my network?
- How much bandwidth does the codec consume?
- Does the codec meet quality levels for my network for all audio types?
- How does the codec handle packet loss?

How many Digital Signal Processor (DSP) resources does it take to code audio using the codec?

4.7 Calculating Codec bandwidth requirement

Before we deploy VoIP over your network, we try to estimate how much bandwidth the codec we are using will consume [10]. For this we have taken several factors into account such as sample size, header information, and link-efficiency mechanisms.

Step-1: Required audio bandwidth for the audio codec itself.

To find the amount of bandwidth required for the audio codec, we determine the size (in bytes) of audio contained in each packet. For most audio codecs, the sample size is 20 milliseconds. Increasing the sample size gives you a bandwidth savings benefit because the router sends fewer packets overall (and fewer packets mean less header information). We use following formula to determine the voice payload size:

$$Bytes\ per\ packet = \frac{Sample\ size\ X\ Codec\ bandwidth}{8}$$

G.711 call uses a 20-ms sample size, the formula would calculate like this:

$$Bytes\ per\ packet = \frac{.02\ X\ 64000}{8} = 120$$

G.729 call uses a 20-ms sample size:

$$Bytes\ per\ packet = \frac{.02\ X\ 8000}{8} = 20$$

Step 2: Determine Data Link, Network, and Transport Layer Overhead

After we had found the amount of voice contained in each packet, we calculated the amount of data contained in the header in each packet. Because every voice packet uses RTP, UDP, and IP, they add 40 bytes of data per packet (RTP=12 bytes, UDP= 8 bytes and IP=20 bytes).

Step 3: Add It All Together

We add values from the first two steps together in a final equation:

$$Total\ Bandwidth = Packet\ size\ X\ Packets\ per\ second$$

So, first we add together the values from Steps 1 and 2 to form the packet size like for G.729 and G.711 as:

$$Packet\ size = Voice\ payload + IP\ header + UDP\ header + RTP\ header + Ethernet\ Header$$

$$Packet\ size = 20 + 20 + 8 + 12 + 20 = 80\ bytes\ per\ packet(G.729)$$

$$Packet\ size = 120 + 20 + 8 + 12 + 20 = 180\ bytes\ per\ packet(G.729)$$

For number of packets per second, some simple reasoning came into play. Each packet contains a 20-ms sample size, and 1 second is 1000 milliseconds. So, if you take 1000 ms / 20 ms = 50 ms, this helps you find that it will take 50 packets per second to generate the full second of audio. This now give you all the pieces you need to find the final amount of bandwidth per call:

$$Total\ bandwidth = Packet\ size\ X\ Packet\ per\ second$$

$$Total\ bandwidth = 80\ bytes\ X\ 50\ Packet\ per\ second$$

$$Total\ bandwidth = 4000\ bytes\ per\ second\ (G.729)$$

$$Total\ bandwidth = 9000\ bytes\ per\ second\ (G.711)$$

So a single call take about (4000X8=32000) 32kbps of bandwidth for G.729 and 72kbps for G.711.

Step 4: Subtract Bandwidth Savings Measures

In the realm of VoIP, there are two primary bandwidth savings measures that we can enable to improve the efficiency of your voice network. They are Voice Activity Detection (VAD) and RTP header compression.

VAD allows the router to detect the “sound of silence” in a VoIP conversation. By default, the routers will send RTP data, even if no one is talking. Through many studies, findings show that on average, 35–40 percent of a phone call is silence. By enabling VAD, you are able to recoup this bandwidth back into your budget.

4.8 The Role of Digital Signal Processors

Moving into the realm of VoIP, the network now requires the router to convert loads of voice into digitized, packetized transmissions. This task would easily overwhelm the resources you have on the router. This is where Digital Signal Processors (DSPs) come into play. DSPs offload the processing responsibility for voice-related tasks from the processor of the router [11]. This is very similar to the idea of purchasing an expensive video card for a PC to offload the video processing responsibility from the PC’s processor. Specifically, a DSP is a chip that performs all the sampling, encoding, and compression functions on audio coming into your router. If you were to equip your router with voice interface cards (VIC), allowing it to connect to the PSTN or analog devices, but did not equip your router with DSPs, the interfaces would be worthless. The interfaces would be able to actively connect to the legacy voice networks, but would not have the power to convert any voice into packetized form. All codecs are not created equal. Some codecs consume more DSP resources to pass through the audio conversion process than other codecs consume. Table 3 shows the codecs complexity.

Medium Complexity	High Complexity
G.711 (a-law and µ-law)	G.728
G.726	G.723
G.729a, G.729ab	G.729, G.729b
——	iLBC

Table 3 Complexity comparison of Codec

Chapter: 5

INTEGRATION OF PASCOM

5.1 Introduction

For connection with PASCOM we needed a voice gateway router. The router used to translate the legacy voice world to the VoIP world, and vice versa. In order to make the connection to the PASCOM, we equipped the voice gateway router with traditional telephony interfaces. The interfaces we used are analog connections but this could be done with digital connections.

5.2 Understanding Analog Connections

Analog connections are single-connection circuits. A router typically uses Foreign Exchange Station (FXS) analog interfaces to connect to analog devices such as telephones, fax machines, and modems. Foreign Exchange Office (FXO) analog interfaces are used to connect to the PSTN central office (CO) or to a legacy PBX system. So we used FXO interface to integrate PASCOM with our Metro Ethernet Network. There also exist another type of analog connection you can use is an Ear and Mouth (E&M) interface. E&M signaling is designed to connect directly to a PBX system that also supports E&M interfaces. Figure 5.1 illustrates a voice gateway router supporting analog voice connections [12].

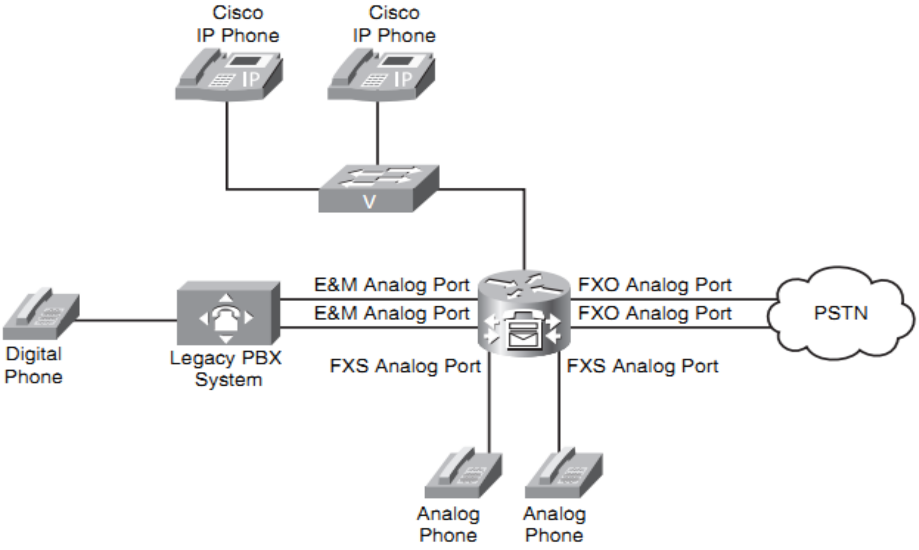


Figure 5.1: Integration of Voice Gateway with PSTN

FXS, FXO ports and DSP resources shown in Figure --- do the job of converting the analog audio coming from the port into VoIP packets, and vice versa.

5.3 Understanding Digital Connections

There is a possibility that our user in MCS increases to an extent where analog connectivity might be cumbersome, expensive and insufficient. In this scenario digital connections allow multiple conversations to share a single circuit. The digital channels are built using DS0 channels as "building blocks." Depending on the interface we are using to connect to the PASCOM or PSTN service provider, we can support a different number of DS0 channels. Each DS0 provides a 64-kbps channel, which supports a single audio call. The following are the available digital ports we can use in our voice gateway router:

- Channel associated signaling (CAS) T1/E1: CAS interfaces attempt to "squeeze" signaling (which provides features such as caller ID, ring, off-hook, and so on) into the same channel as the audio. By doing this, we are able to support 24 DS0 audio channels out of a T1 interface (used primarily in the United States, Japan, and Korea). E1 interfaces (typically used outside of the United States, Japan, and Korea) support 30 channels.
- Common channel signaling (CCS) or Primary Rate Interface (PRI) T1/E1: CCS/PRI interfaces separate the audio signaling into a dedicated channel, leaving the full 64kbps of each DS0 for audio only. Because of this, a T1 using CCS uses only 23 DS0 audio channels (because the 24th is dedicated to signaling). PRI describes the ISDN implementation of CCS, which is more commonly used by PSTN COs and PBX vendors. Because of its architecture, E1 still provides 30 channels with CCS signaling.
- Basic Rate Interface (BRI): Each BRI interface provides two DS0 channels and a small signaling channel.

5.4 Dial Plan

A dial plan in a network is a set of rules or pattern that allows how telephony users connect with each when they dial a number. Telephone terminals are dump devices they don't know any information about their network, its topology and even directory number assigned to it. So some guide and control mechanism must be there to route their traffic/call within and outside the network at the voice gateway.

It is very similar to data routing in which all routers forward packet they received by checking their routing table. If destination IP address matched with any entry in the routing table, they forward the packet according to matched entry. Else it acts as a black hole mean it starts discarding packets with unknown destination IP address. In same way we have to have a routing table for our voice. This routing table for voice is called dial plan saved on voice gateways [13].

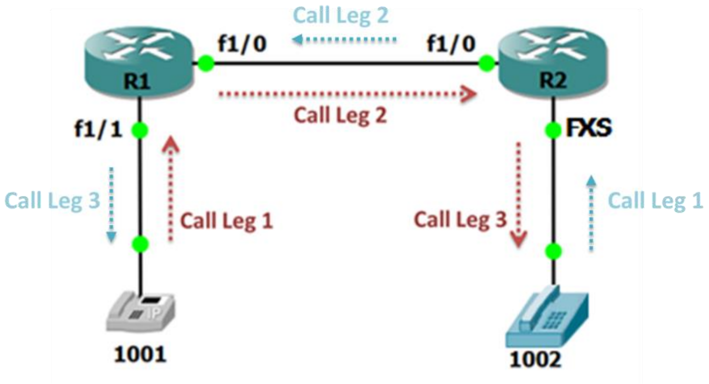


Figure 5.2: Call legs between Voice Gateways

For example in figure 5.2 if IP phone dials 1002, gateway must establish a connection. For this gateway must do two things. First it must have the information to resolve this DN (directory number) 1002 into an IP address. Second it must know the location of dialed number so that it can establish a connection.

Dial plan consists of two elements to perform establish a successful call:

i. Call Leg
ii. Dial Peers

5.41 Call Leg

It is a virtual connection or link between voice gateways or between voice gateway and telephony end terminal which are the segments of a complete call connection.

Cisco defined call leg as *every hop or link to reach IP telephony or any sort of telephony*. In figure5.2 router R1 and R2 are gateways both are connected to IP phone and analog phone respectively. According to above definition there are three call legs (segments) for the connection from phone 1001 to 1002 shown in red color. Similarly in the connection from phone (DN) 1002 to 1001 also includes three call legs shown in blue color. But these two pairs of call legs are different from each other as one for IP and other for analog phone respectively. So, on the basis of telephone terminal call legs are of following main types:

i. POTS Call Leg
ii. VoIP Call Leg

POTS Call Leg

All terminals which don't have an IP address are called POTS (Plain Old Telephone System) and call legs associated with them are called POTS call leg. This may be an analog phone, a fax machine, an E1 connected to PBX, modem etc.

VoIP Call Leg

Devices which have an IP address or any device which can communicate over an IP network are VoIP terminals and call legs associated with them are called VoIP call legs.

5.42 Dial Peers

Dial peers are the set of rules or instruction how these dial peers would be connected to complete a call connection. For example when R2 receiver a call of IP phone 1001 via R1, it can forward this call towards FXS port (analog phone 1002) or towards FXO port (PSTN). Dial peers helps R2 in routing this call toward correct destination or call leg. It uses information about IP addresses, directory number and ports type/number to join these call legs.

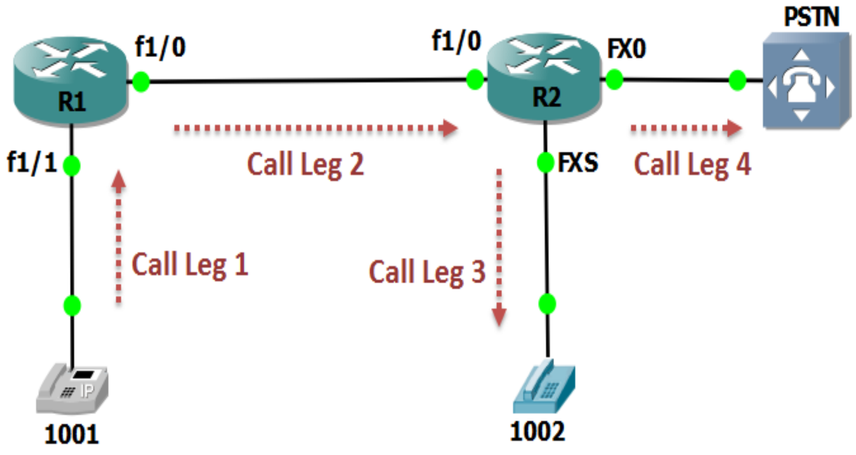


Figure 5.3: Dial peers between voice gateway and PSTN

Now these call legs are matched with inbound and outbound. Let IP phone dials 1002 it first goes to R1 and call leg from IP phone to R1 is called inbound call leg. After processing R1 routes this call towards R2 and this call leg between R1 and R2 is outbound for R1. So in short information about how these legs are joined must be known to gateway and this information is called dial peers. For example R1 connects call leg 1 and 2 according to information stored in R1 in form of dial peer.

5.5 Trunking CME to Other VoIP Systems

As VoIP becomes more popular, businesses will prefer to use interoffice connectivity over data networks rather than the PSTN, due to long-distance cost savings and bandwidth efficiency (VoIP calls can use less bandwidth than traditional PSTN). The single office CME deployment will need to connect with other offices or providers over the VoIP network, as illustrated in Figure5.4.

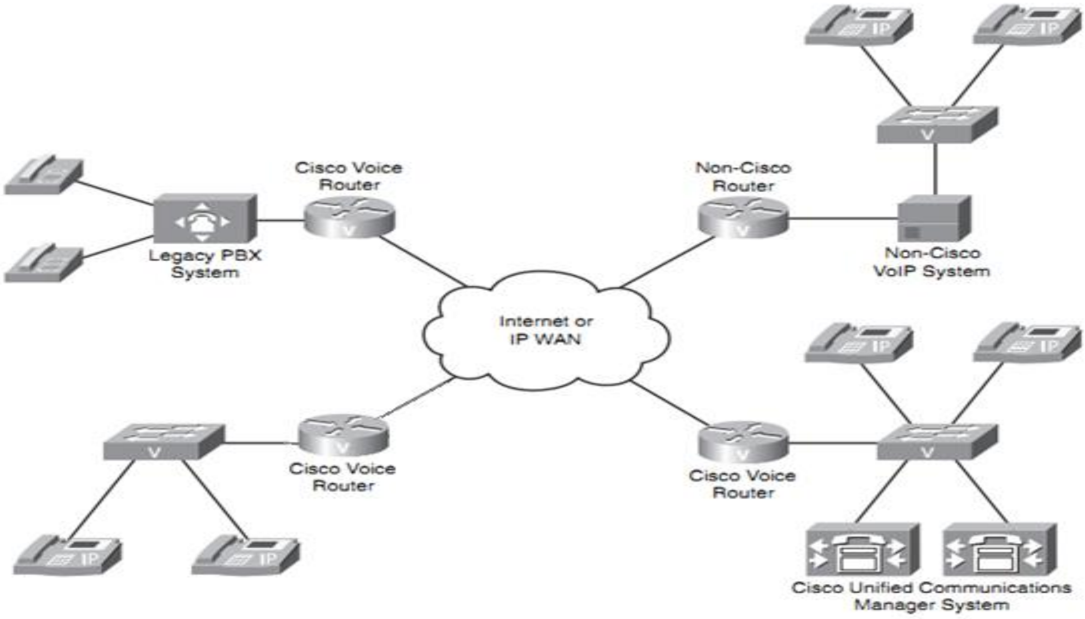


Figure 5.4: A complete Integrated IP and TDM Network

To communicate with these other VoIP systems, voice gateway router needs a common VoIP communication protocol. This is very similar to the world of data communications. Because all devices now support the TCP/IP protocol, they can all communicate over the network regardless of manufacturer. The voice world also needs a protocol, not so much for voice communication (because this is the job of RTP), but rather for voice signaling. Voice signaling includes call setup messages, call maintenance messages, relaying dialed digits, and so on. While the data realm has settled on TCP/IP as the protocol of choice, the voice world still has multiple signaling protocols you can use. The following list provides an overview of each of these protocols:

5.51 H.323

H.323 was the first of the four voice signaling protocols and definitely has maturity on its side. The International Telecommunication Union, Telecommunication Standardization Sector (ITU-T) originally created H.323 to allow simultaneous voice, video, and data to transmit across ISDN connections. It has since been adapted to work over LAN environments. It is a peer-to-peer protocol that allows every device running H.323 to be completely independent from other devices. This allows you to configure each H.323 device uniquely and prevent reliance on any other device for normal operation [14].

It is a signaling or communication protocol that is responsible for setting up the call, making sure that call remain established or terminating or teardown the call and for exchanging features. H.323 is the oldest of all signaling or communication protocols. It may sound bad but actually it is the most widely adopted or widely supported protocol because is was actually designed for multimedia communication like voice conferencing, interoperatability with PSTN etc.

Protocol break down shown in figure5.5 are the components which make H.323. In this figure the components H.255 call signaling, H.245 and H.225 RAS are core components of H.323 which define the standard for other components e.g. they interface with all other audio codec and video codecs. They support data applications like windows net meeting, instant messaging etc.

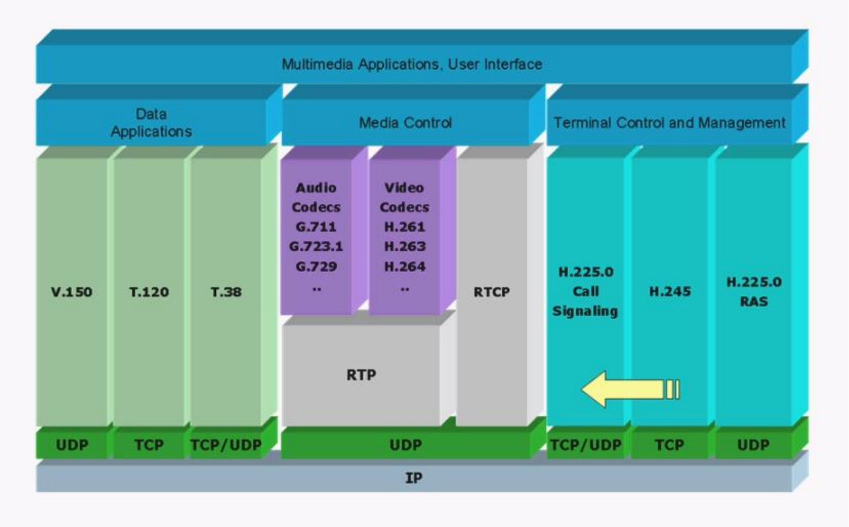

Multimedia Applications, User Interface
Data Applications
Media Control
Terminal Control and Management
V.150
T.120
T.38
Audio Codecs G.711 G.723.1 G.729 ..
Video Codecs H.261 H.263 H.264 ..
RTP
RTCP
H.225.0 Call Signaling
H.245
H.225.0 RAS
UDP
TCP
TCP/UDP
UDP
TCP/UDP
TCP
UDP
IP

Figure 5.5: Components of H.323

So these are core components and some interfaces of H.323. H.325 call signalling is resposible for call setup and teardown. H.245 is for feature exchange and it is the most important function of H.323. Feature exchange mean when two phones are calling what protocols they want to use. H.245 RAS (Regitartion addmission and status) is used only for the gatekeeper to form a centralized Route plan and bandwidth control.

5.5.2 H.323 Call Setup

Suppose we have two phones with directory number (DN) 1000 and 2000 connected with separate gateways (GW). When DN-1000 wants to make a call towards DN-2000, GW-1 uses H.225 is used to setup the call toward GW-2. Then GW-2 send an acknowledgement in response which is quickely followed by allerting message that DN-2000 has been provided with a ringtone. After receiving allerting message GW-1 also sends an alerting tone to DN-1000. When DN-2000 pickup the call, GW-2 sends H.225 connect message towards GW-1.

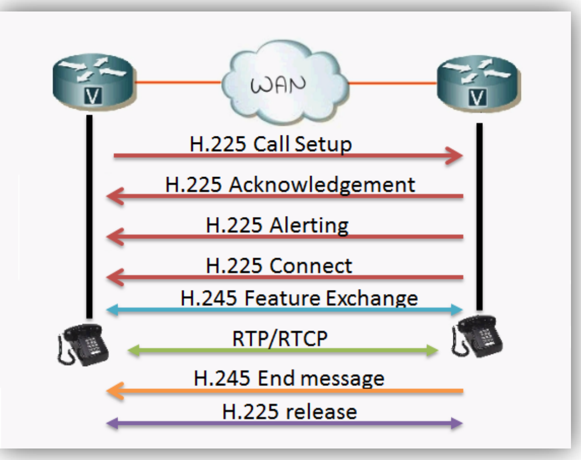


Figure 5.6: Call setup of H.323

After H.225 coonect message, H.245 come into action and start exchanging features like what codec should be used. In next step RTP strats voice streaming and RTCP for statistical analysis of RTP. When any of the DN hangup the phone respective GW sends H.245 end message to disconnect streaming channel of RTP and at the last H.225 release is used to completely teardown the call.

But System mentioned above has a serious problem which might be the single point of failure in the network. For example we dial a DN, bell rings at called DN but as soon as he pickup the call and both side connected, our call disconnects. This is due to codec miss match. For example GW-1 and 2 exchanges information about codecs but both not agreed to use a single codec as in our project we are using G.711 or G.729 in our Metro Ethernet Network but PASCOM using G.711a-law, so we also had the same issue of codec miss-match. To solve this issue we form a virtual interface at the gateway for transcoding or codec inter-conversion (rememnber transcoding could not be performed at call manager).

5.5.3 Session Initiation Protocol (SIP)

SIP is often called the "next generation" of H.323 developed by the Internet Engineering Task Force (IETF), SIP is a much more light-weight and scalable protocol than H.323. It is an evolving standard that does not currently support many of the advanced features of VoIP networks. As SIP becomes more mature and robust, it is poised to become the primary VoIP signaling standard used worldwide (similar to the way data networks use TCP/IP today) [15].

5.5.4 SIP Architechture

SIP is really just a signalling protocol. As its name show session initiation protocol, it starts and end sessions. Most people use it to start and end audio sessions or video sessions, but SIP is not only limited to it. We may use it to start and end data transfer, to start and end a television conversasion etc.

To discuss the general architechture of SIP I start with discussing with its signallingobjectives as:

- Determine Location: It determine the location of end terminal
- Determine Media capabilities: What codecs should be used between end terminals
- Determine Availability: Is called user is available or not
- Establish Session: Establish the session between end terminals
- Manage Termination/Transfer: Terminating a call or forwarding or transfering a call

To manage this there are many servers in SIP architechture as:

- Location Server: It is has the database of the location of all end points
- Redirect Server: It takes the incomming call and redirect to the whatever you want to connect. So it need very limited resources and very low capacity because it is not taking any responsablity of address provided by lacatio server.
- Registrar Server: It registers the end point credentials like DN, IP addresses and MAC

These three server works together to perform SIP operations. But it is very dificult to form three different databases for three different servers. So we may use a segmented server which could perform above mentioned functionalities. It is the proxy server such as call manager which we used in our project.

5.5.5 SIP Call Setup

Every SIP client is broken into two pieces. First user agent client (UAC), a clients is one who always initiate a cause [16], makes a request or initiate a call/calling party. Second user agent server (UAS), it is actually the called party.

Suppose DN-1000 wants to call DN-2000. Now 1st gateway (GW-1) is UAC and GW-2 is UAS. UAC sends an invitation to UAS to start a session. UAS replied with an 100 trying message. Actually 1xx are the messages to exchange informations. Immediately after 100 trying UAS sends 180 ringing message mean DN-2000 has been given a request tone. When DN-200 pickup the call UAS sends 200 ok message that called agent is ready. Then an acknowledged message is send by UAC and then RTP voice stream starts.

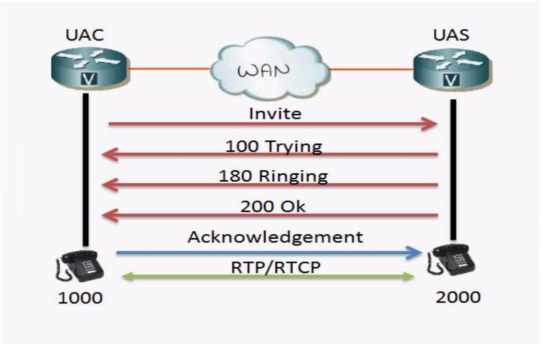


Figure 5.7: Call setup of SIP

5.6 Media Gateway Control Protocol (MGCP)

MGCP is the first true “client/server” VoIP signaling protocol. If you are using MGCP, you will perform the vast majority of your gateway configuration from a centralized system known as a call agent. Because this is a newer IETF standard, it is not as widely supported as H.323 or SIP.

Anytime the MGCP gateway interacts with the voice network, it relies on the call agent for its intelligence. The call agent tells the gateway how to process digits, where to send the calls, what codec it should be using, and so on. Using MGCP is like turning your voice gateway into a dumb terminal, where the call agent is now the mainframe. The gateway does not have any intelligence in itself; it receives everything from the centralized call agent system [17].

Consider an example. An analog phone connected to the FXS port of an MGCP gateway goes off-hook. The MGCP gateway immediately sends a message to the call agent that says, “Call agent, a phone just went off-hook. What should I do?” The call agent responds, “Play a dial tone.” After the MGCP gateway sends a dial tone to the phone, the phone user dials the digit 9. Once again, the MGCP gateway sends a message to the call agent that says, “Call agent, the phone just dialed the digit 9. What should I do?” The call agent responds, “Stop the dial tone and play a beep,” which the MGCP gateway then does. This process continues for each step of the voice call. The router basically becomes a “dumb terminal” interfacing with the call agent “mainframe.” The beauty of MGCP is in its centralized configuration. As you manage more VoIP gate-ways and devices in a growing voice network, you will appreciate having a centralized place of configuration rather than equipping each device with its own configuration. This is also a benefit for managed voice service provider environments. Corporations pay these service providers to manage their entire voice network. If the service provider uses MGCP, it can centralize the configuration in its call agents; the equipment that it installs at the customer premises will have minimal local configuration.

5.7 Skinny Client Control Protocol (SCCP)

SCCP is the only Cisco-proprietary VoIP protocol currently in use. Although SCCP is not specifically designed for gateway signaling and control, a limited number of Cisco gateways do support it. The primary goal of SCCP is to provide a signaling protocol between the Cisco Unified Communications Manager and Cisco IP phones [17].

Similar to MGCP, the SCCP devices report every action to the Communications Manager server, which then responds with the action the device should take.

SCCP (more often called “Skinny”), the only Cisco-proprietary protocol of the four signaling protocols, is used to control Cisco IP phones and other Cisco endpoint devices (such as the ATA 186/188). Skinny functions as a stimulus/response protocol similar to MGCP. Any interaction with a Cisco IP phone (such as lifting the handset, dialing a digit, and so on) causes the IP phone to send Skinny messages to the call processing software, which then responds with a Skinny message instructing the device with the action to take.

The main advantage of the Skinny protocol is also its main weakness: it is proprietary. By using a proprietary protocol to control Cisco IP phones, Cisco can deploy new features and capabilities for the IP phones without requiring major revisions to an industry-standard protocol. Of course, the drawback of using a proprietary protocol is that Cisco IP phones will only work with Cisco call processing software (such as Cisco Unified CME or Cisco Unified Communications Manager) by default. Cisco IP phones can also use SIP (and MGCP in some cases) by downloading a replacement

Chapter: 6

Campus based Security

Securing an IP-based network can be a difficult task, largely because the Internet is based on open standards. Because nonproprietary technologies such as IP are so well known, their bugs and their limitations are well publicized and often easily exploited. You can deal with risk in four ways: you accept it, you reduce it, you ignore it or transfer it. In network security, you seek to reduce risk with the help of sound technologies and policies. In this chapter I focus on reducing risk by using security technologies available in campus network design to mitigate vulnerabilities and treats [18].

We would secure our Metro Ethernet Ring Network by applying following firewalls, controls and devices e.g. Port base and mode based security, access control lists and cisco firewall device.

6.1 Port Security

Controlling users in a network by enabling security on interfaces of the network devices (ports) and allow/restrict them on basis of their MAC addresses [19].

We must identify a set of allowed MAC addresses so that the port can grant them access.

Port Security with Dynamically Learned and Static MAC Addresses

We can statically configure all secure MAC addresses by using the **switch port port-security MAC-address** MAC_address interface configuration command.

- We can allow the port to dynamically configure secure MAC addresses with the MAC addresses of connected devices.
- We also statically configure a number of addresses and allow the rest to be dynamically configured.

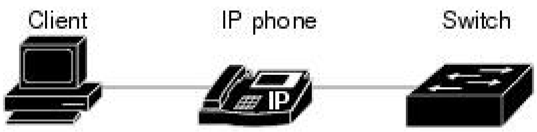
Port Security with Sticky MAC Addresses

Port security with sticky MAC addresses provides many of the same benefits as port security with static MAC addresses, but sticky MAC addresses can be learned dynamically. Port security with sticky MAC addresses retains dynamically learned MAC addresses during a link-down (shutdown) condition.

If you enter a **write memory** or **copy running-config startup-config** command, then port security with sticky MAC addresses saves dynamically learned MAC addresses in the startup-config file and the port does not have to learn addresses from ingress traffic after boot up or a restart.

Port Security with IP Phones

Figure below shows an application in which a device connects to the switch through the data port of an IP phone.



Because the device is not directly connected to the switch, the switch cannot physically detect a loss of port link if the device is disconnected.

In this situation a Cisco IP phones send a packet to switch. Packet includes Cisco Discovery Protocol (CDP) with type length value (TLV) to notify the switch about changes in the attached device's port link state. Upon receiving a host presence TLV notification of a link down on the IP phone's data port, port security removes from the address table all static, sticky, and dynamically learned MAC addresses. The removed addresses are added again only when the addresses are learned dynamically or configured.

6.2 Access control lists

Access control lists (ACLs) perform packet filtering to control which packets move through the network and where. Thus access list is essentially a list of conditions that categorizes packets.

Such control can be very useful to restrict the access of users and devices to the network providing a measure of security and can save network resources by reducing traffic. Access lists provide diverse benefits, depending on how they are used [20].

Some ACL decision points are:

- ❑ IP source address
- ❑ IP destination addresses
- ❑ UDP or TCP protocols
- ❑ upper-layer (TCP/UDP) port numbers

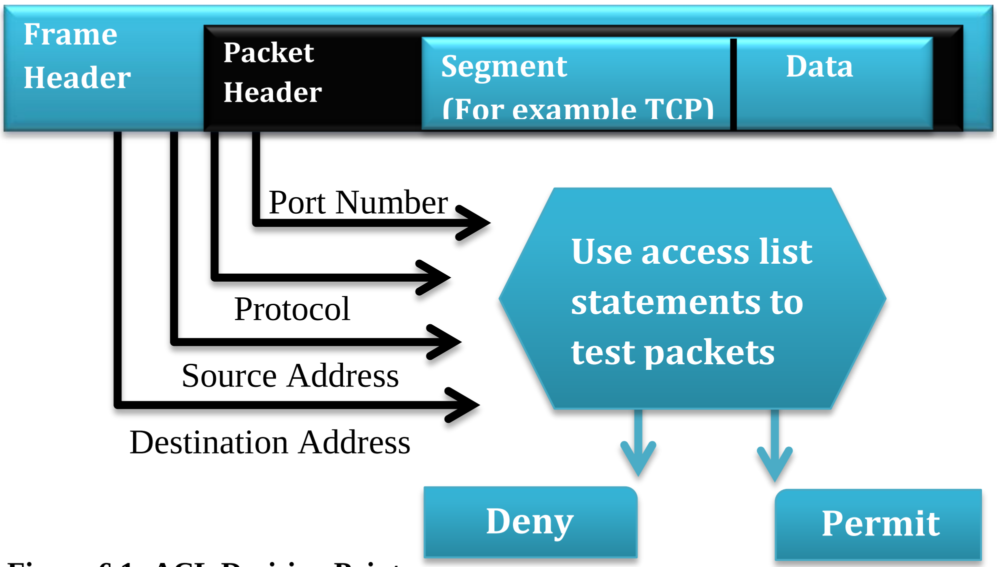


Figure 6.1: ACL Decision Points

Creating access lists is really a lot like programming a series of if-then statements. If a given condition is met, then a given action is taken. If a condition isn't met, nothing happens and the next statement is evaluated. Once the lists have built, they can be applied to either inbound or outbound traffic on any interface. When access list is applied, traffic that crosses that interface is checked in specified direction and appropriate action is taken.

6.2.1 Rules Access Lists follow in Filtering Traffic

Access lists are read from top to bottom.

- □ When the packet matches a condition on a given line of the access list, the packet is acted upon and no action takes place.
- □ Once a packet doesn't match the condition on any of the line of access list, the packet will be discarded.
- □ Its mean there is an implicit deny at the end of access lists.

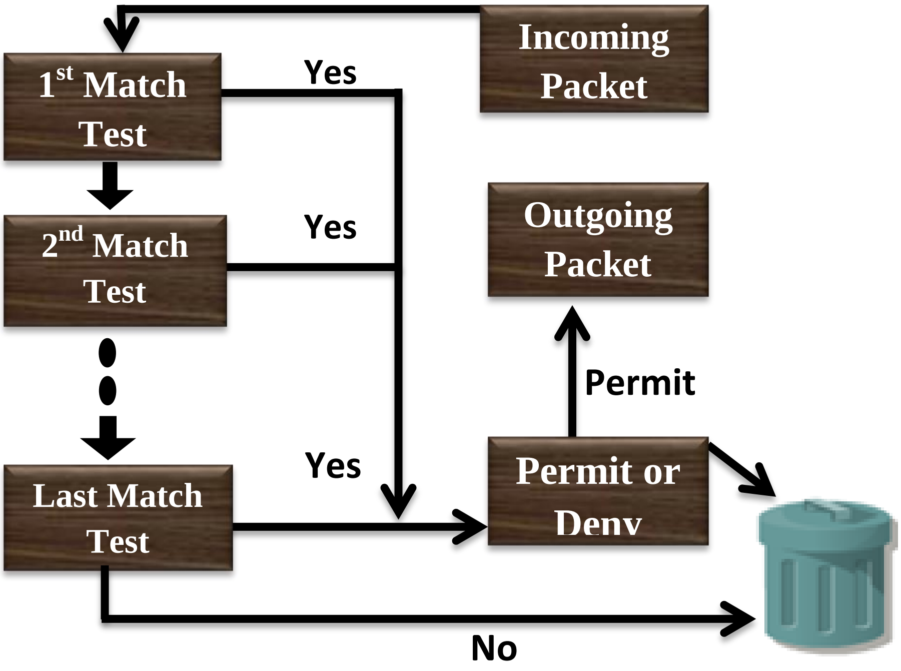


Figure 6.2: ACL Test Rule Diagram

6.2.2 Types of Access Lists

There are two types of IP access lists.

- □ **Standard**
  - ○ Checks source address
  - ○ Permits or denies entire protocol suite

They only use source IP address in an IP Packet as the condition test. All decisions are made based on source IP address. This means that standard access lists basically permit or deny an entire suit of protocols. They don’t distinguish between any of the many IP traffic such as Web, Telnet, UDP, and so on.

- □ **Extended**
    - Checks source and destination address
    - Generally permits or denies specific protocols

Extended access lists can evaluate many of the other fields in the layer 3 and layer 4 headers of an IP packet. They can evaluate source and destination IP addresses, the Protocol field in the Network layer Header and the port number at the Transport layer header. This gives extended access list the ability to make more granular decisions when controlling traffic.

Once you have created an access list, it’s not really going to do anything until it is applied. But where is to apply access list is still a question. To use access list as a packet filter, you need to apply it to an interface on the router where you want the traffic filtered and direction also. Different access lists can be used for inbound and outbound traffic on a single interface:

6.2.3 Reasons to Create ACLs

The following are some of the primary reasons to create ACLs:

□ Limit network traffic and increase network performance.

□ Provide traffic flow control.

□ Provide a basic level of security for network access.

□ Decide which types of traffic are forwarded or blocked at the router interfaces

□ For example: Permit e-mail traffic to be routed, but block all telnet traffic.

□ If ACLs are not configured on the router, all packets passing through the router will be allowed onto all parts of the network.

□ Restricting communication between unconcerned/unauthorized departments.

□ Use of port base and mode base security.

CONCLUSION

A complete IP video calling network is designed and deployed between different departments of MCS-NUST. Media of communication used is optical fiber which connects all departments in the form of ring. Server used for call monitoring and controlling is CUCM (CISCO Unified Communication Manager). Switches (ME-3400 and 2960) are used to form LAN environment in each departments. These switches are bridged together using a layer-3 switch (for inter-VLAN communication and applying access control lists for security and management purposes). A VOICE gateway (3845-router) is used for integration with PASCOM via an analog line. Firewall is also used to secure this VoIP network from foreign intrusion.

BIBLIOGRAPHY

BIBLIOGRAPHY

[1] CISCO three layered hierarchal model for LAN and WAN networks http://www.mcmcse.com/cisco/guides/hierarchical_model.shtml

[2] Cisco Voice official Exam Certification Guide by Jeremy Cioara, chapter 1

[3] Cisco Unified Communications Manager Administration Guide, Release 7.0

[4] Firewalls and Internet Security, Repelling the Wily Hacker, first edition

[5] CISCO Certified Network Associate Study Guide, 7th edition, chapter 10

[6] CISCO Certified Network Associate Study Guide, 7th edition, chapter 11

[7] The DHCP Handbook, Understanding, Deploying and Managing Automated Configuration Services by Ralph E.Droms and Ted Lemon

[8] Scilab Code for Digital Communication by Simon Haykin, chapter 4

[9] A Practical Guide to Video and Audio Compression by Cliff Wootton, chapter 2

[10] Standard Codecs, Image Processing to Advance video coding by Muhammad Ghanbari, chapter 3

[11] Voice over IP by Jason Sinclair and Michael E.Flannagan, chapter 4

[12] Voice over IP by Jason Sinclair and Michael E.Flannagan chapter 5

[13] CCNA Voice certification Guide by Michael J. Cavanaugh and Kris A. Krake, chapter 8

[14] IP Telephony with H.323, Architectures for Unified Network and Integrated Services by Vineet Kumar

[15] Understanding Session Initiation Protocol by Alan B. Johnston, Chapter 2

[16] Understanding Session Initiation Protocol by Alan B. Johnston, Chapter 3

[17] Implementing CISCO Communication Manager, (CITP1), chapter 9

[18] Campus Network Design Fundamntals by Diane Teare and Catherine Paquet, chapter

[19] CISCO Certified Network Associate Study Guide, 7th edition, chapter 10

[20] Access Control, Authentication and Public Key Infrastructure by Bill Ballad, Tricia Ballad and Erin Bank