इ रि से ट

IRISET

TCS-6

IP TELEPHONY & NGN

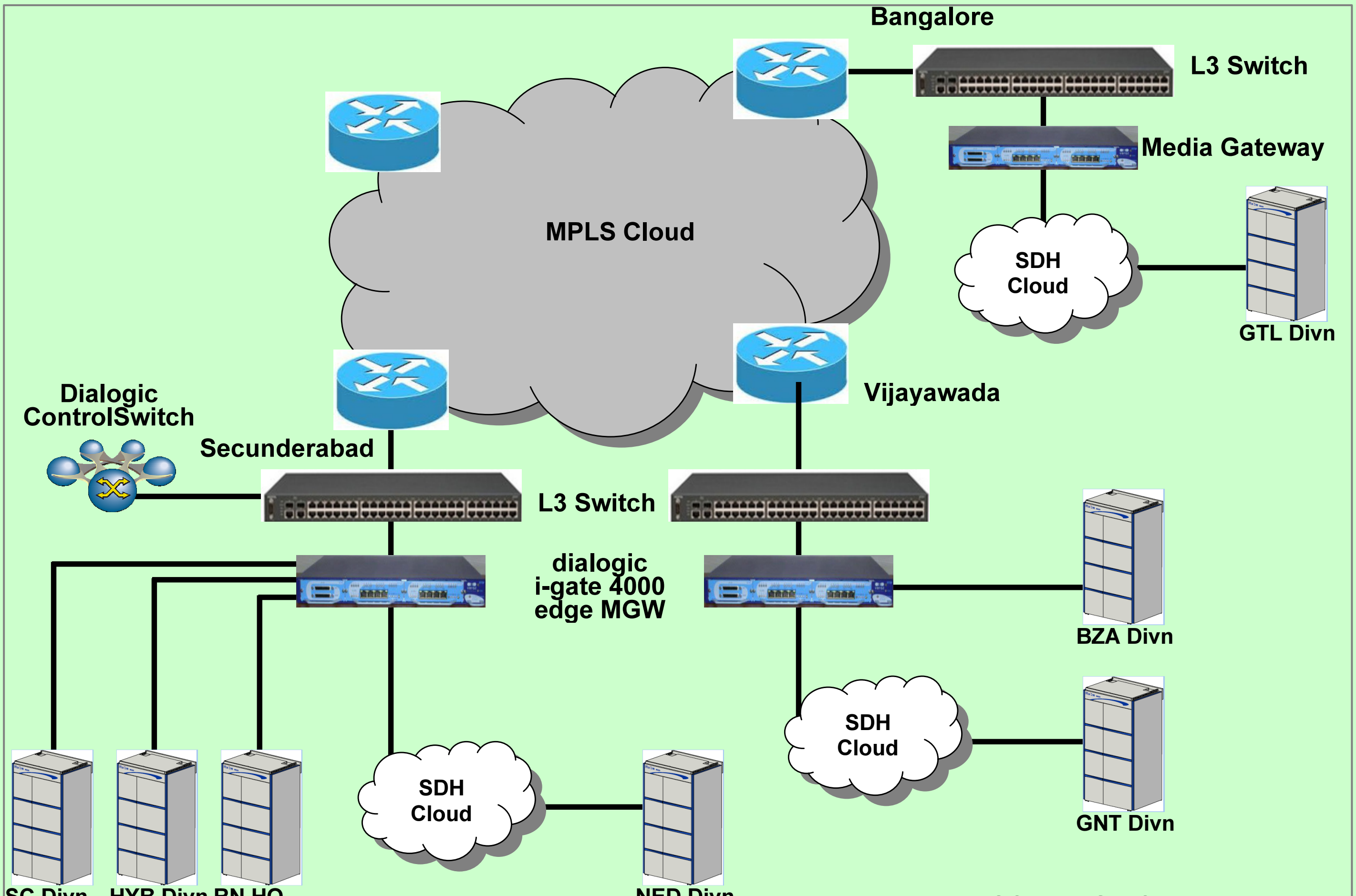


Fig. SCRly NGN Connectivity

Indian Railways Institute Of Signal Engineering & Telecommunications
Tarnaka Road, Secunderabad - 500 017 (A. P.)

TCS 6

IP TELEPHONY & NGN

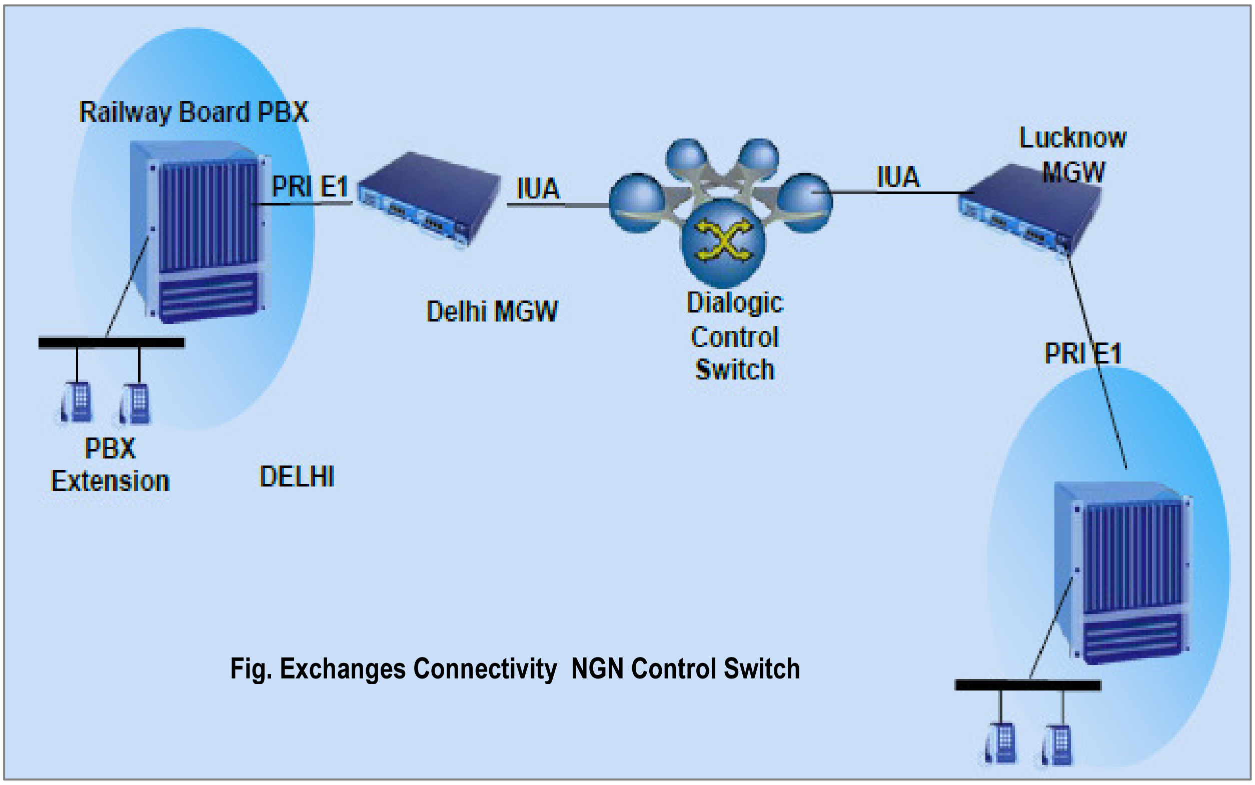


Fig. Exchanges Connectivity NGN Control Switch

Indian Railways Institute Of Signal Engineering & Telecommunications
Tarnaka Road, Secunderabad 500 017 (A. P.)

TCS 6

IP TELEPHONY & NGN

CONTENTS

1. VoIP Fundamentals 01
2. VoIP Protocols 15
3. Asterisk Based PBX 31
4. NGN 36
5. NGN Protocols 45
6. Dialogic Control Switch System 52

- Prepared By .... **M. Umapathy, Instructor Telecom**
- Checked By .... **S.M. Hafeez Ali, Lecturer Telecom**
- Approved By .... **C.K. Prasad, Professor Telecom**
- DTP & Drawings .... **M. Umapathy, Instructor Telecom**
- Date Of Issue .... **May 2013**
- Edition .... **First**
- No. Of Pages **72**

May 2013 : First Edition

CHAPTER 1

VoIP FUNDAMENTALS

Introduction

VoIP Voice Over Internet Protocol is a revolutionary technology that allows you to make calls using your internet broadband connection instead of your regular phone line. It is generally used to make international calls.

Benefits

Cheap International rates: VoIP calls are known to be much cheaper than equivalent services offered by traditional phone companies. A single broadband network is used to carry both voice and data. This substantial cost saving occurs because the technology allows the network to carry several calls in the same amount of space that normally carries a single call in a traditional phone network. Also, the data is compressed allowing more space and thus, lower rates.

Convenience: It is easy to operate using one of two options: Using a computer to make calls or using a special broadband phone to make calls rather than a PC.

Receive Calls anywhere: You can also receive incoming calls on your VoIP phone if you take it along on a trip. All you have to do is to plug it into the network.

Call centre on the move: Call centre agents can work easily from anywhere as long as they have a good Internet connection. There are also advanced call service options available from some carriers. These features use caller ID information to allow you to make a choice about how calls from a particular number are handled.

The above mentioned services can either be free as a part of your billing plan or it can even be chargeable as you subscribe to them so it is always better to check with the provider before you subscribe.

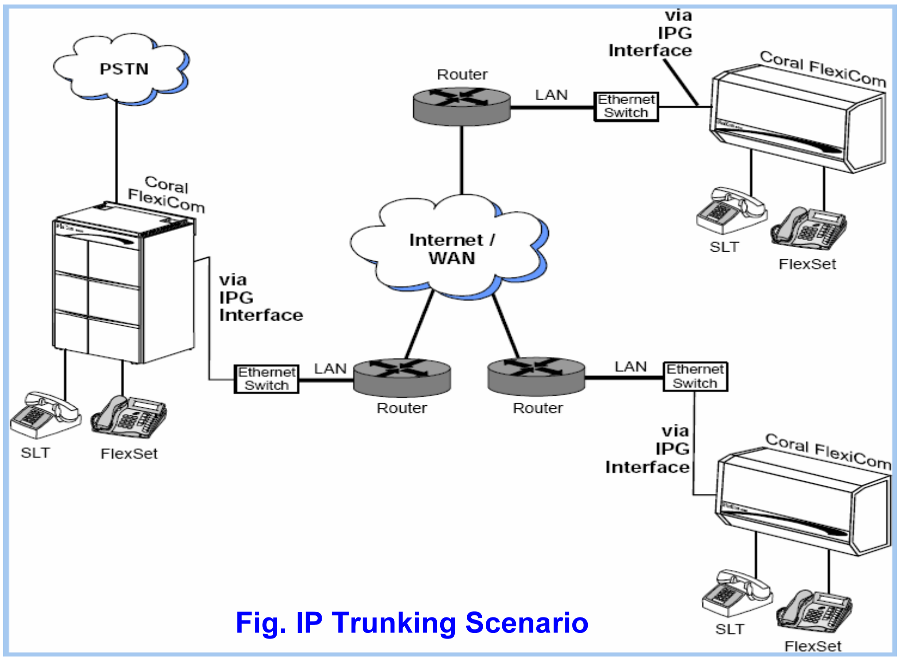


Fig. IP Trunking Scenario

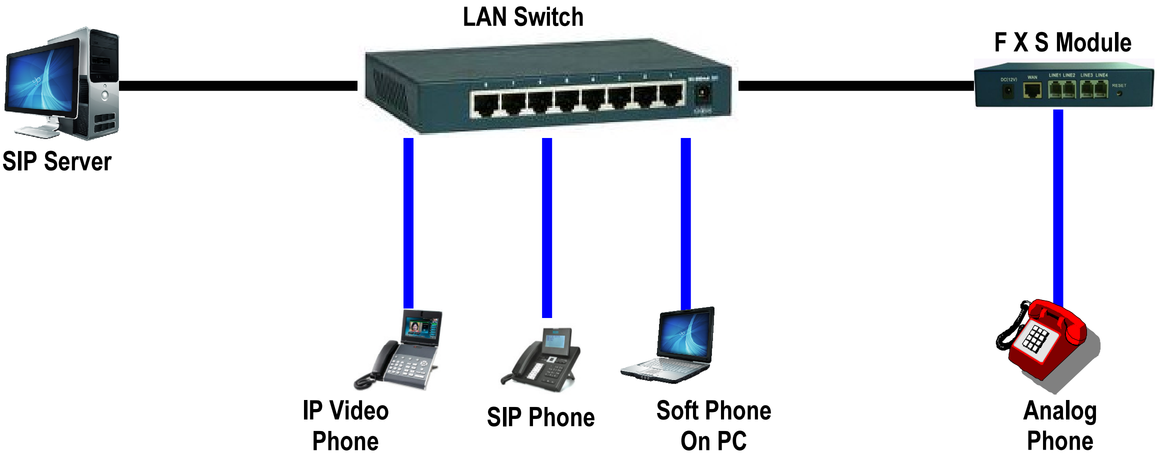


Fig. SIP Server Implementation

Technology

Traditional phone networks use circuit switching to connect calls. When you speak, the circuit is continuously open whether you are talking or not. This wastes a lot of network space and time. When you disconnect, the circuit closes. Nowadays, the system has been digitized so that fiber optic cables are used (for most of the connection, not all the way) which carry several calls at the same time. Calls are transmitted at a fixed rate per second.

VoIP uses packet switching technology to connect calls. Unlike circuit switching, this network does not waste any space. If you are talking it means that the other person is listening. This is not a full connection. It can be likened to using only half the connection at a given time. Also, dead air time, when nobody is speaking, is not used in the connection. Removing all this from the connection brings down the space used. So signals are sent only when it is needed, that is, when the connection is being used at a given point of time. Hence there is no wastage. Since the data is chopped up into packets, it is called packet switching.

The voice is converted to data on sending which goes like an email. The packets contain information on where they are to go. Several routers along the way receive and send the packets along until the final one reassembles the packets according to the instructions in it and converts it back to voice.

Limitations

You may not be able to emergency and dial toll free services such as 1 800 numbers or other free services. The Internet connection must be of a reasonable quality and speed for a clear and smooth connection. VoIP being dependant on the broadband line is susceptible to all the limitations of the Internet. It is also susceptible to computer issues such as processor specifications. Also, the quality of a call may be affected if you are using the computer for an intensive application while on a VoIP call.

Dialing Options

ATA Analog Telephone Adaptor

The ATA allows you to use a standard phone to make VoIP calls. The ATA is an analog to digital converter. It takes the analog signal from your traditional phone and converts it into digital data for transmission over the Internet. You simply crack the ATA out of the box, plug the cable from your phone (that would normally go in the wall socket) into the ATA, and you're ready to make VoIP calls.

IP Phones

These specialized phones look just like normal phones with a handset, cradle and buttons. But instead of having the standard RJ11 phone connectors, IP phones have an RJ45 Ethernet connector. IP phones connect directly to your router/modem and have all the hardware and software necessary right onboard to handle the VoIP call. Wi Fi phones allow subscribing callers to make VoIP calls from any Wi Fi hot spot.

Soft Phones

A small software applet known as soft phone installed on to a PC can be used to make and receive calls. With headset one can communicate.

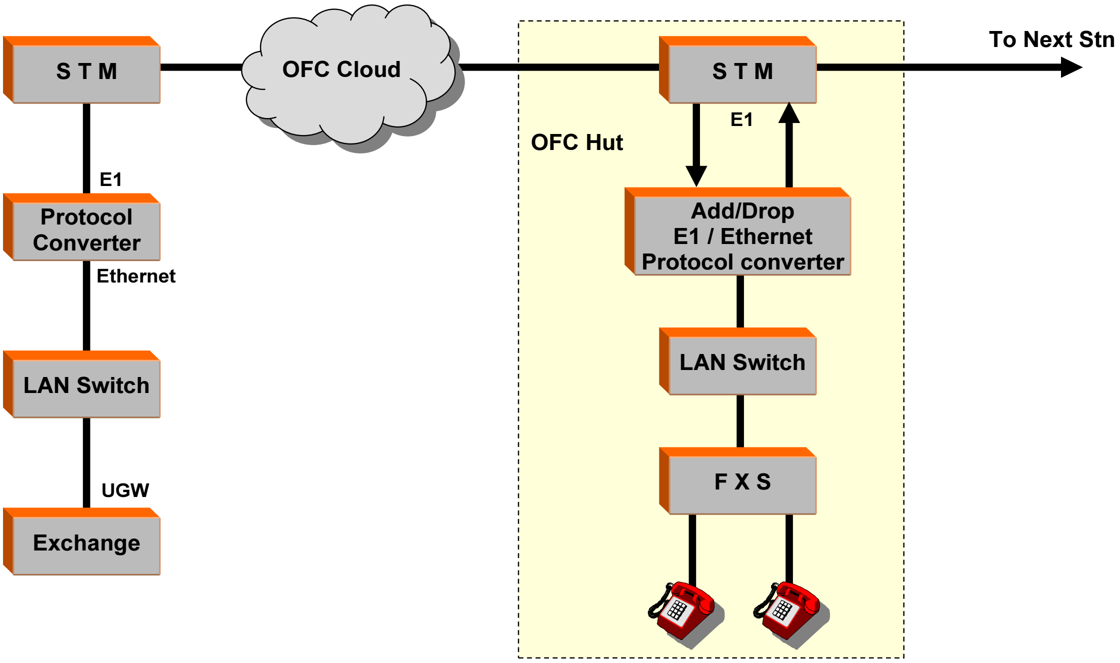


Fig. VoIP Implementation At Way Station

Voice over IP (VoIP) can be described as the ability to make telephone calls and send faxes over IP based data networks with a suitable Quality of Service (QoS). The voice information is sent in digital form using discrete packets rather than via dedicated connections as in the circuit switched Public Switched Telephone Network (PSTN).

Currently, there are two major international groups defining standards for VoIP:

International Telecommunications Union, Telecommunications Standardization Sector (ITU T) and Internet Engineering Task Force (IETF).

The H.323 recommendation was developed in the mid 1990s and is a mature protocol. SIP (Session Initiation Protocol) is an emerging protocol for setting up telephony, conferencing, multimedia, and other types of communication sessions on the Internet.

H.323 Overview

The H.323 specification is an umbrella specification for the implementation of packet based multimedia over IP networks that cannot guarantee Quality of Service (QoS). This section discusses the following topics about H.323:

- H.323 Entities
- H.323 Protocol Stack
- Codecs
- Basic H.323 Call Scenario
- Registration with a Gatekeeper
- H.323 Call Scenario via a Gateway

H.323 Entities

The H.323 specification defines the entity types in an H.323 network including:

Terminal

An endpoint on an IP network that supports the real time, two way communication with another H.323 entity. A terminal supports multimedia coders/decoders (codecs) and setup and control signaling.

Gateway

Provides the interface between a packet based network (for example, an IP network) and a circuit switched network (for example, the PSTN). A gateway translates communication procedures and formats between networks. It handles call setup and teardown and the compression and packetization of voice information.

Gatekeeper

Manages a collection of H.323 entities in an H.323 zone controlling access to the network for H.323 terminals, Gateways, and MCUs and providing address translation. A zone can span a wide geographical area and include multiple networks connected by routers and switches. Typically there is only one gatekeeper per zone, but there may be an alternate gatekeeper for backup and load balancing. Typically, endpoints such as terminals, gateways, and other gatekeepers register with the gatekeeper.

Multipoint Control Unit (MCU)

An endpoint that supports conferences between three or more endpoints. An MCU can be a stand alone unit or integrated into a terminal, gateway, or gatekeeper. An MCU consists of:

- Multipoint Controller (MC) – handles control and signaling for conferencing support
- Multipoint Processor (MP) – receives streams from endpoints, processes them, and returns them to the endpoints in the conference

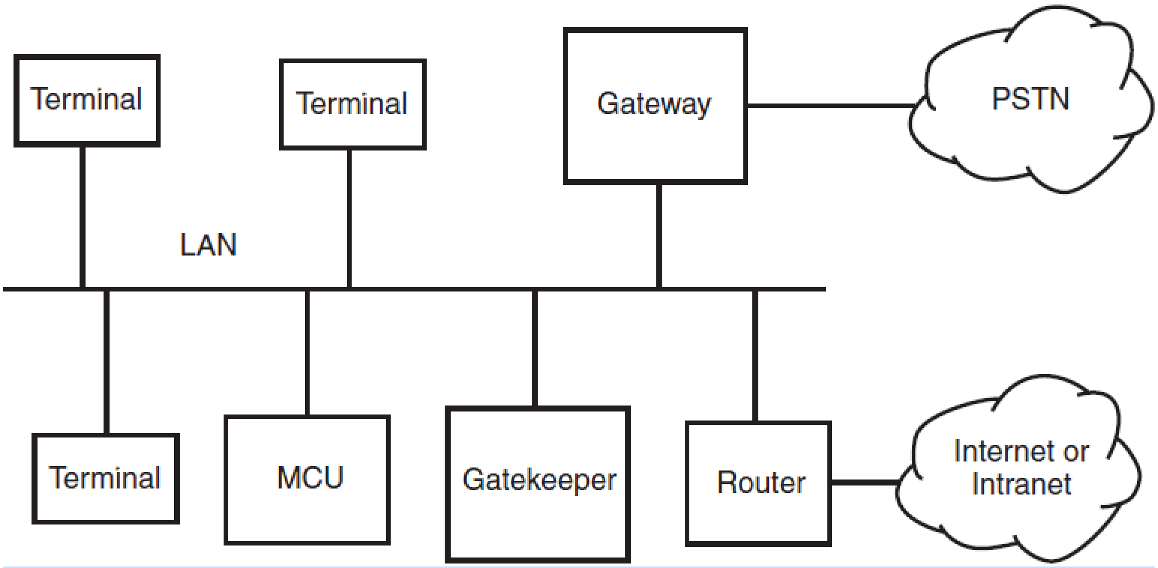


Fig. VoiP Scenerio In A Network

Call Setup

Establishing a call between two endpoints nominally requires two TCP connections between the endpoints:

- one TCP connection for the call setup (Q.931/H.225 messages)
- one TCP connection for capability exchange and call control (H.245 messages)

In practice, the H.245 channel may not be required thanks to two additional features of the H.323 protocol. H.323 version 2 defines a Fast Start mode that accomplishes the endpoint capability exchange through the use of Fast Start Elements (FSEs) which are “piggy backed” on Q.931/H.225 call setup messages rather than waiting for an H.245 channel to be established.

It is also possible to encapsulate H.245 media control messages within Q.931/H.225 signaling messages using a technique known as H.245 tunneling. If tunneling is enabled, one less TCP port is required for incoming connections.

The caller at endpoint A connects to the callee at endpoint B on a well known port, typically port 1720, and sends the call Setup message as defined in the H.225.0 specification. The Setup message includes:

- message type; in this case, Setup
- bearer capability, which indicates the type of call; for example, audio only
- called party number and address
- calling party number and address
- Protocol Data Unit (PDU), which includes an identifier that indicates which version of H.225.0 should be used along with other information When endpoint B receives the Setup message, it responds with one of the following messages:
- Release Complete
- Alerting
- Connect
- Call Proceeding

In this case, endpoint B responds with the Alerting message. Endpoint A must receive the Alerting message before its setup timer expires. After sending this message, the user at endpoint B must either accept or refuse the call with a predefined time period. When the user at endpoint B picks up the call, a Connect message is sent to endpoint A and the next phase of the call scenario, capability exchange, can begin.

Capability Exchange

Call control and capability exchange messages, as defined in the H.245 standard, are sent on a second TCP connection. Endpoint A opens this connection on a dynamically allocated port at the endpoint B after receiving the address in one of the following H.225.0 messages:

- Alerting
- Call Proceeding
- Connect

This connection remains active for the entire duration of the call. The control channel is unique for each call between endpoints so that several different media streams can be present. An H.245 TerminalCapabilitySet message that includes information about the codecs supported by that endpoint is sent from one endpoint to the other. Both endpoints send this message and wait for a reply which can be one of the following messages:

- TerminalCapabilitySetAck accept the remote endpoints capability
- TerminalCapabilitySetReject reject the remote endpoints capability

The two endpoints continue to exchange these messages until a capability set that is supported by both endpoints is agreed. When this occurs, the next phase of the call scenario, call initiation, can begin.

Call Initiation

Once the capability setup is agreed, endpoint A and B must set up the voice channels over which the voice data (media stream) will be exchanged. The scenario described here assumes a slow start connection procedure.

To open a logical channel at endpoint B, endpoint A sends an H.245 OpenLogicalChannel message to endpoint B. This message specifies the type of data being sent, for example, the codec that will be used.

For voice data, the message also includes the port number that endpoint B should use to send RTCP receiver reports. When endpoint B is ready to receive data, it sends an OpenLogicalChannelAck message to endpoint A. This message contains the port number on which endpoint A is to send RTP data and the port number on which endpoint A should send RTCP data.

Endpoint B repeats the process above to indicate which port endpoint A will receive RTP data and send RTCP reports to. Once these ports have been identified, the next phase of the call scenario, data exchange, can begin.

Data Exchange

Endpoint A and endpoint B exchange information in RTP packets that carry the voice data. Periodically, during this exchange both sides send RTCP packets, which are used to monitor the quality of the data exchange. If endpoint A or endpoint B determines that the expected rate of exchange is being degraded due to line problems, H.323 provides capabilities to make adjustments. Once the data exchange has been completed, the next phase of the call scenario, call termination, can begin.

Call Termination

To terminate an H.323 call, one of the endpoints, for example, endpoint A, hangs up. Endpoint A must send an H.245 CloseLogicalChannel message for each channel it has opened with endpoint B. Accordingly, endpoint B must reply to each of those messages with a CloseLogicalChannelAck message. When all the logical channels are closed, endpoint A sends an H.245

End Session Command, waits until it receives the same message from endpoint B, then closes the channel. Either endpoint (but typically the endpoint that initiates the termination) then sends an H.225.0 ReleaseComplete message over the call signaling channel, which closes that channel and ends the call.

Registration with a Gatekeeper

In a H.323 network, a gatekeeper is an entity that can manage all endpoints that can send or receive calls. Each gatekeeper controls a specific zone and endpoints must register with the gatekeeper to become part of the gatekeeper's zone. The gatekeeper provides call control services to the endpoints in its zone. The primary functions of the gatekeeper are:

- address resolution by translating endpoint aliases to transport addresses
- admission control for authorizing network access
- bandwidth management
- network management (in routed mode)

Endpoints communicate with a gatekeeper using the Registration, Admission, and Status (RAS) protocol. A RAS channel is an unreliable channel that is used to carry RAS messages (as described in the H.255 standard). The RAS protocol covers the following:

- Gatekeeper Discovery
- Endpoint Registration
- Endpoint Deregistration
- Endpoint Location
- Admission, Bandwidth Change and Disengage

Note: The RAS protocol covers status request, resource availability, nonstandard registration messages, unknown message response and request in progress that are not described in any detail in this overview. See ITU T Recommendation H.225.0 (09/99) for more information.

Gatekeeper Discovery

An endpoint uses a process called gatekeeper discovery to find a gatekeeper with which it can register. To start this process, the endpoint can multicast a GRQ (gatekeeper request) message to the well known discovery multicast address for gatekeepers. One or more gatekeepers may respond with a GCF (gatekeeper confirm) message indicating that it can act as a gatekeeper for the endpoint.

If a gatekeeper does not want to accept the endpoint, it returns GRJ (gatekeeper reject). If more than one gatekeeper responds with a GCF message, the endpoint can choose which gatekeeper it wants to register with. In order to provide redundancy, a gatekeeper may specify an alternate gatekeeper in the event of a failure in the primary gatekeeper. Provision for the alternate gatekeeper information is provided in the GCF and RCF messages.

Endpoint Registration

An endpoint uses a process called registration to join the zone associated with a gatekeeper. In the registration process, the endpoint informs the gatekeeper of its transport, alias addresses, and endpoint type. Endpoints register with the gatekeeper identified in the gatekeeper discovery process described above. Registration can occur before any calls are made or periodically as necessary. An endpoint sends an RRQ (registration request) message to perform registration and in return receives an RCF (registration confirmation) or RRJ (registration reject) message.

Endpoint Deregistration

An endpoint may send an URQ (unregister request) in order to cancel registration. This enables an endpoint to change the alias address associated with its transport address or vice versa. The gatekeeper responds with an UCF (unregister confirm) or URJ (unregister reject) message. The gatekeeper may also cancel an endpoint's registration by sending a URQ (unregister request) to the endpoint. The endpoint should respond with an UCF (unregister confirm) message. The endpoint should then try to reregister with a gatekeeper, perhaps a new gatekeeper, prior to initiating any calls.

Endpoint Location

An endpoint that has an alias address for another endpoint and would like to determine its contact information may issue a LRQ (location request) message. The LRQ message may be sent to a specific gatekeeper or multicast to the well known discovery multicast address for gatekeepers. The gatekeeper to which the endpoint to be located is registered will respond with an LCF (location confirm) message. A gatekeeper that is not familiar with the requested endpoint will respond with LRJ (location reject).

Admission, Bandwidth Change and Disengage

The endpoint and gatekeeper exchange messages to provide admission control and bandwidth management functions. The ARQ (admission request) message specifies the requested call bandwidth. The gatekeeper may reduce the requested call bandwidth in the ACF (admission confirm) message. The ARQ message is also used for billing purposes, for example, a gatekeeper may respond with an ACF message just in case the endpoint has an account so the call can be charged. An endpoint or the gatekeeper may attempt to modify the call bandwidth during a call using a BRQ (bandwidth change request) message. An endpoint will send a DRQ (disengage request) message to the gatekeeper at the end of a call.

H.323 Call Scenario via a Gateway

The IP addresses of both endpoints were defined to be known in the example, while most Internet Service Providers (ISPs) allocate IP addresses to subscribers dynamically. This section describes the fundamentals of a more realistic example that involves a gateway.

A gateway provides a bridge between different technologies; for example, an H.323 gateway (or IP gateway) provides a bridge between an IP network and the PSTN. Figure 3 shows a configuration that uses a gateway. User A is at a terminal, while user B is by a phone connected to the PSTN.

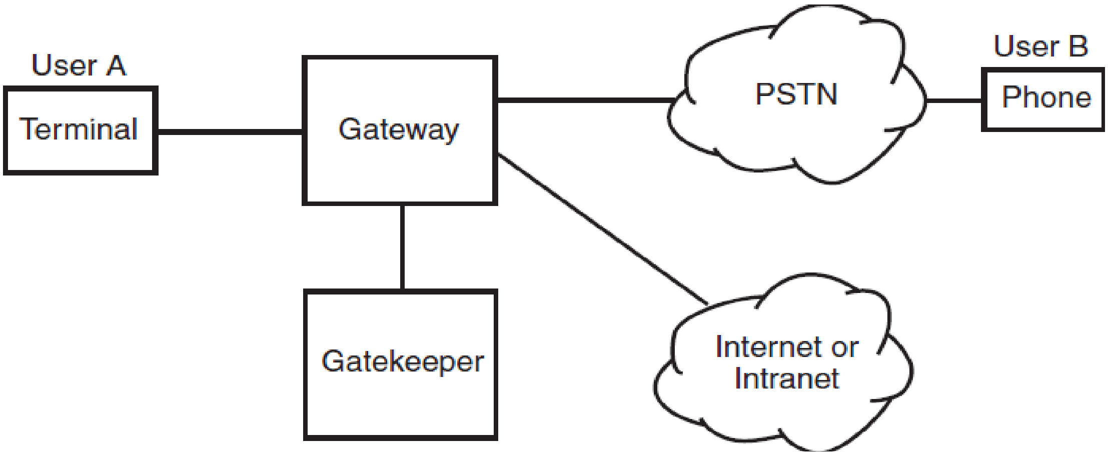


Fig. Typical VoIP Call In A Network

The gatekeeper provides network services such as Registration, Admission, and Status (RAS) and address mapping. When a gatekeeper is present, all endpoints managed by the gatekeeper must register with the gatekeeper at startup. The gatekeeper tracks which endpoints are accepting calls. The gatekeeper can perform other functions also, such as redirecting calls. For example, if a user does not answer the phone, the gatekeeper may redirect the call to an answering machine.

The call scenario in this example involves the following phases:

- Establishing Contact with the Gatekeeper
- Requesting Permission to Call
- Call Signaling and Data Exchange
- Call Termination

Establishing Contact with the Gatekeeper

The user at endpoint A attempts to locate a gatekeeper by sending out a Gatekeeper Request (GRQ) message and waiting for a response. When it receives a Gatekeeper Confirm (GCF) message, the endpoint registers with the gatekeeper by sending the Registration Request (RRQ) message and waiting for a Registration Confirm (RCF) message. If more than one gatekeeper responds, endpoint A chooses only one of the responding gatekeepers. The next phase of the call scenario, requesting permission to call, can now begin.

Requesting Permission to Call

After registering with the gatekeeper, endpoint A must request permission from the gatekeeper to initiate the call. To do this, endpoint A sends an Admission Request (ARQ) message to the gatekeeper. This message includes information such as:

- a sequence number
- a gatekeeper assigned identifier
- the type of call; in this case, point to point
- the call model to use, either direct or gatekeeper routed
- the destination address; in this case, the phone number of endpoint B
- an estimation of the amount of bandwidth required. This parameter can be adjusted later by a Bandwidth Request (BRQ) message to the gatekeeper. If the gatekeeper allows the call to proceed, it sends an Admission Confirm (ACF) message to endpoint A.
- The ACF message includes the following information:
- the call model used
- the transport address and port to use for call signaling (in this example, the IP address of the gateway)
- the allowed bandwidth

All setup has now been completed and the next phase of the scenario, call signaling and data exchange, can begin.

Call Signaling and Data Exchange

Endpoint A can now send the Setup message to the gateway. Since the destination phone is connected to an analog line (the PSTN), the gateway goes off hook and dials the phone number using dual tone multi frequency (DTMF) digits. The gateway therefore is converting the H.225.0 signaling into the signaling present on the PSTN. Depending on the location of the gateway, the number dialed may need to be converted.

For example, if the gateway is located in Europe, then the international dial prefix will be removed.

As soon as the gateway is notified by the PSTN that the phone at endpoint B is ringing, it sends the H.225.0 Alerting message as a response to endpoint A. As soon as the phone is picked up at endpoint B, the H.225.0 Connect message is sent to endpoint A. As part of the Connect message, a transport address that allows endpoint A to negotiate codecs and media streams with endpoint B is sent.

The H.225.0 and H.245 signaling used to negotiate capability, initiate and call, and exchange data are the same as that described in the basic H.323 call scenario. In this example the destination phone is analog, therefore, it requires the gateway to detect the ring, busy, and connect conditions so it can respond appropriately.

Call Termination

As in the basic H.323 call scenario example, the endpoint that hangs up first needs to close all the channels that were open using the H.245 CloseLogicalChannel message. If the gateway terminates first, it sends an H.245 EndSessionCommand message to endpoint A and waits for the same message from endpoint A. The gateway then closes the H.245 channel.

When all channels between endpoint A and the gateway are closed, each must send a DisengageRequest (DRQ) message to the gatekeeper. This message lets the gatekeeper know that the bandwidth is being released. The gatekeeper sends a DisengageConfirm (DCF) message to both endpoint A and the gateway.

SIP Overview

Session Initiation Protocol (SIP) is an ASCII based, peer to peer protocol designed to provide telephony services over the Internet. The SIP standard was developed by the Internet Engineering Task Force (IETF) and is one of the most commonly used protocols for VoIP implementations. This section discusses the following topics about SIP:

- Advantages of Using SIP
- SIP User Agents and Servers
- Basic SIP Operation
- Basic SIP Call Scenario
- SIP Messages

Advantages of Using SIP

Some of the advantages of using SIP include:

- The SIP protocol stack is smaller and simpler than other commonly used VoIP protocols, such as H.323.
- SIP based systems are more easily scalable because of the peer to peer architecture used. The hardware and software requirements for adding new users to SIP based systems are greatly reduced.
- Functionality is distributed over different components. Control is decentralized. Changes made to a component have less of an impact on the rest of the system.
- 1.3.2 SIP User Agents and Servers

User agents (UAs) are appliances or applications, such as SIP phones, residential gateways and software that initiate and receive calls over a SIP network. Servers are application programs that accept requests, service requests and return responses to those requests. Examples of the different types of servers are:

Location Server

Used by a SIP redirect or proxy server to obtain information about the location of the called party.

Proxy Server

An intermediate program that operates as a server and a client and which makes requests on behalf of the client. A proxy server does not initiate new requests, it interprets and possibly modifies a request message before forwarding it to the destination.

Redirect Server

Accepts a request from a client and maps the address to zero or more new addresses and returns the new addresses to the client. The server does not accept calls or generate SIP requests on behalf of clients.

Registrar Server Accepts REGISTER requests from clients. Often, the registrar server is located on the same physical server as the proxy server or redirect server.

Basic SIP Operation

Callers and callees are identified by SIP addresses. When making a SIP call, a caller first locates the appropriate server and then sends a SIP request. The most common SIP operation is the invitation request. Instead of directly reaching the intended callee, a SIP request may be redirected or may trigger a chain of new SIP requests by proxies. Users can register their location(s) with SIP servers.

Basic SIP Call Scenario

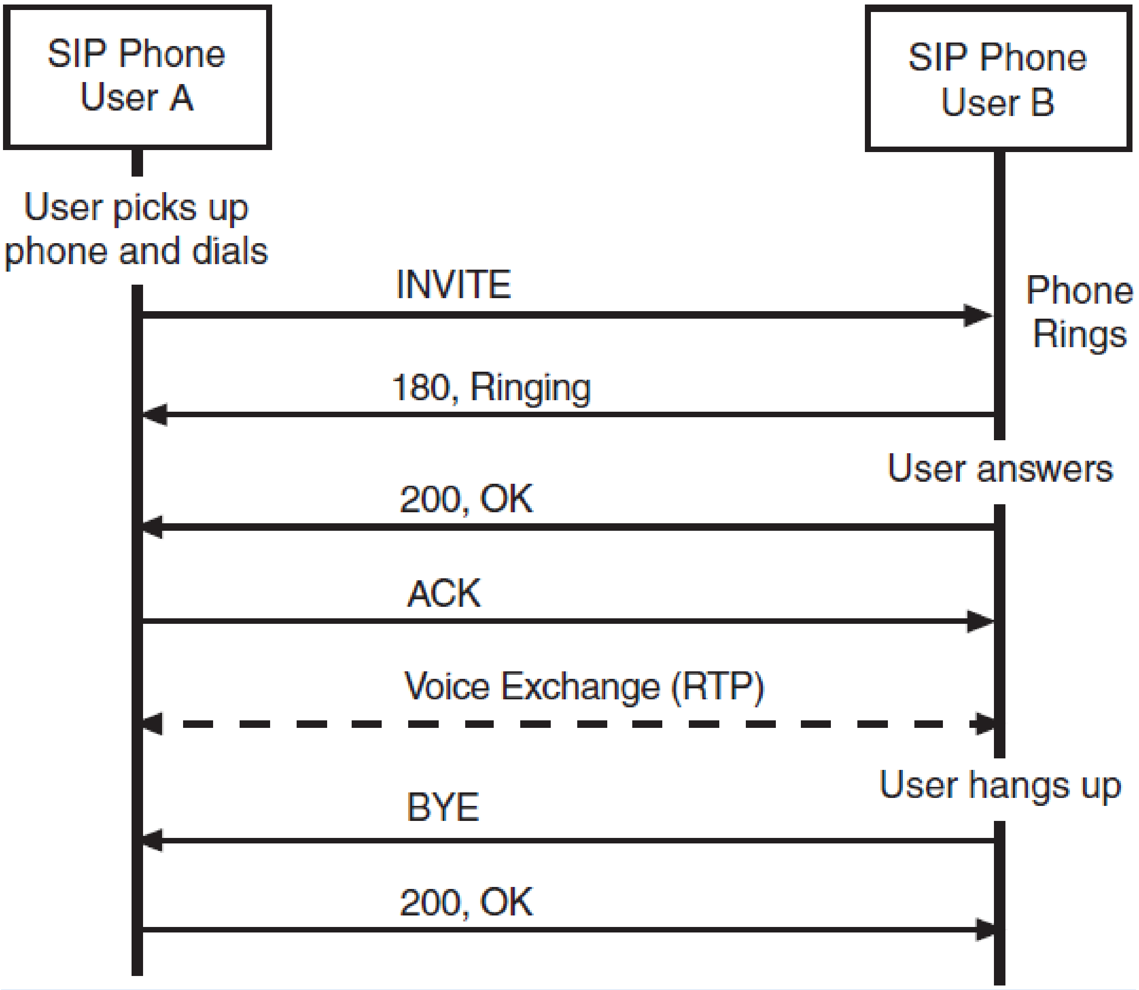


Fig. SIP Call Process Sequence

SIP Messages

In SIP, there are two types of messages:

- SIP Request Messages
- SIP Response Messages

SIP Request Messages

The most commonly used SIP request messages are:

- INVITE
- ACK
- BYE
- REGISTER
- CANCEL
- OPTIONS

For more information on specific SIP request types, see RFC 3261 at http://ietf.org/rfc/rfc3261.txt.

SIP Response Messages

SIP response messages are numbered. The first digit in each response number indicates the type of response. The response types are as follows:

- 1xx Information responses; for example, 180 Ringing
- 2xx Successful responses; for example, 200 OK
- 3xx Redirection responses; for example, 302 Moved Temporarily
- 4xx Request failure responses; for example, 402 Forbidden
- 5xx Server failure responses; for example, 504 Gateway Timeout
- 6xx Global failure responses; for example, 600 Busy Everywhere

For more information on SIP response messages, see RFC 3261 at the URL given above.

Basic Call Control Scenarios When Using IP Technology

This section provides details of the basic call control scenarios when using IP technology. The scenarios include:

- Basic Call Setup When Using H.323 or SIP
- Basic Call Teardown When Using H.323 or SIP
- Call Setup Scenarios for Early Media

Basic Call Setup When Using H.323 or SIP

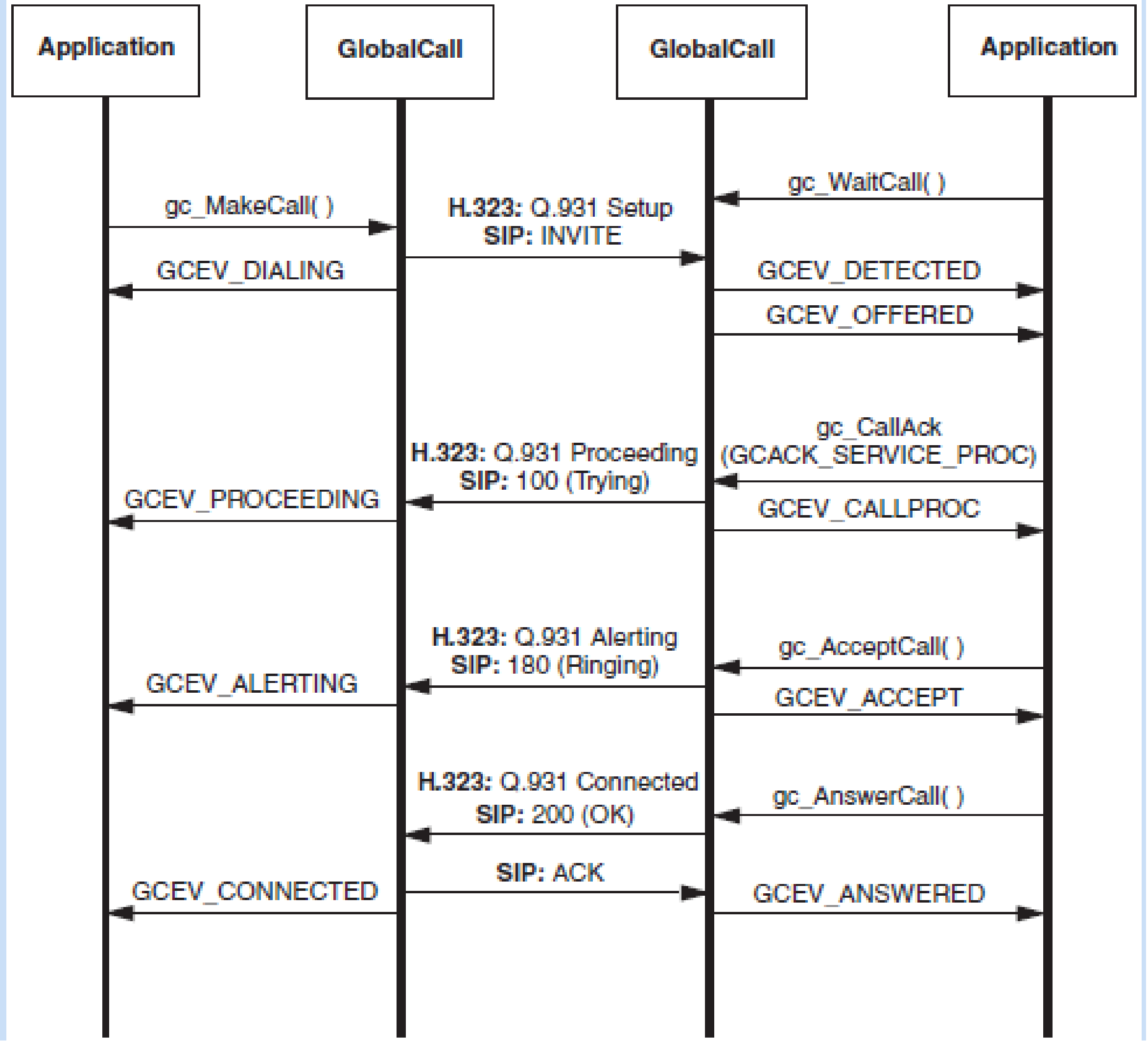


Fig. SIP Call Setup Sequence

CHAPTER 2
VOIP PROTOCOLS

The telecommunications industry spans over 100 years, and Asterisk integrates most, if not all, of the major technologies that it has made use of over the last century. To make the most out of Asterisk, you need not be a professional in all areas, but understanding the differences between the various codecs and protocols will give you a greater appreciation and understanding of the system as a whole.

This chapter explains Voice over IP and what makes VoIP networks different from the traditional circuit switched voice networks that were the topic of the last chapter. We will explore the need for VoIP protocols, outlining the history and potential future of each. We'll also look at security considerations and these protocols' abilities to work within topologies such as Network Address Translation (NAT). The following VoIP protocols will be discussed:

- IAX
- SIP
- H.323
- MGCP
- Skinny/SCCP
- UNISTIM

Codecs are the means by which analog voice can be converted to a digital signal and carried across the Internet. Bandwidth at any location is finite, and the number of simultaneous conversations any particular connection can carry is directly related to the type of codec implemented. In this chapter, we'll also explore the differences between the following codecs in regards to bandwidth requirements (compression level) and quality:

- G.711
- G.726
- G.723.1
- G.729A
- GSM
- iLBC
- Speex
- MP3

We will then conclude the chapter with a discussion of how voice traffic can be routed reliably, what causes echo and how to minimize it, and how Asterisk controls the authentication of inbound and outbound calls.

The Need for VoIP Protocols

The basic premise of VoIP is the packetization* of audio streams for transport over Internet Protocol–based networks. The challenges to accomplishing this relate to the manner in which humans communicate. Not only must the signal arrive in essentially the same form that it was transmitted in, but it needs to do so in less than 300 milliseconds. If packets are lost or delayed, there will be degradation in the quality of the communications experience.

The transport protocols that collectively are called "the Internet" were not originally designed with real time streaming of media in mind. Endpoints were expected to resolve missing packets by waiting longer for them to arrive, requesting retransmission, or, in some cases, considering the information to be gone for good and simply carrying on without it. In a typical voice conversation, these mechanisms will not serve. Our conversations do not adapt well to the loss of letters or words, nor to any appreciable delay between transmittal and receipt.

The traditional PSTN was designed specifically for the purpose of voice transmission, and it is perfectly suited to the task from a technical standpoint. From a flexibility standpoint, however, its flaws are obvious to even people with a very limited understanding of the technology. VoIP holds the promise of incorporating voice communications into all the other protocols we carry on our networks, but due to the special demands of a voice conversation, special skills are needed to design, build, and maintain these networks.

The problem with packet based voice transmission stems from the fact that the way in which we speak is totally incompatible with the way in which IP transports data. Speaking and listening consist of the relaying of a stream of audio, whereas the Internet protocols are designed to chop everything up, encapsulate the bits of information into thousands of packages, and then deliver each package in whatever way possible to the far end. Clearly, some sort of bridge was required.

The mechanism for carrying a VoIP connection generally involves a series of signaling transactions between the endpoints (and gateways in between), culminating in two persistent media streams (one for each direction) that carry the actual conversation. There are several protocols in existence to handle this. In this section, we will discuss some of those that are important to VoIP in general and to Asterisk specifically.

IAX (The "Inter Asterisk eXchange" Protocol)

The test of your Asteriskness comes when you have to pronounce the name of this protocol. Newbies say "eye ay ex"; those in the know say "eeks." IAX* is an open protocol, meaning that anyone can download and develop for it, but it is not yet a standard of any kind.

In Asterisk, IAX is supported by the chan_iax2.so module.

History

The IAX protocol was developed by Digium for the purpose of communicating with other

Asterisk servers (hence "the Inter Asterisk eXchange protocol"). IAX is a transport protocol (much like SIP) that uses a single UDP port (4569) for both the channel signaling and Realtime Transport Protocol (RTP) streams. As discussed below, this makes it easier to firewall and more likely to work behind NAT.

IAX also has the unique ability to trunk multiple sessions into one dataflow, which can be a tremendous bandwidth advantage when sending a lot of simultaneous channels to a remote box. Trunking allows multiple data streams to be represented with a single datagram header, to lower the overhead associated with individual channels. This helps to lower latency and reduce the processing power and bandwidth required, allowing the protocol to scale much more easily with a large number of active channels between endpoints.

Future

Since IAX was optimized for voice, it has received some criticism for not better supporting video but in fact, IAX holds the potential to carry pretty much any media stream desired. Because it is an open protocol, future media types are certain to be incorporated as the community desires them.

Security considerations

IAX includes the ability to authenticate in three ways: plain text, MD5 hashing, and RSA key exchange. This, of course, does nothing to encrypt the media path or headers between endpoints. Many solutions include using a Virtual Private Network (VPN) appliance or software to encrypt the stream in another layer of technology, which requires the endpoints to preestablish a method of having these tunnels configured and operational. In the future, IAX may be able to encrypt the streams between endpoints with the use of an exchanged RSA key, or dynamic key exchange at call setup, allowing the use of automatic key rollover. This would be very attractive for creating a secure link with an institution such as your bank. The various law enforcement agencies, however, are going to want some level of access to such connections.

IAX and NAT

The IAX2 protocol was deliberately designed to work from behind devices performing NAT. The use of a single UDP port for both signaling and transmission of media also keeps the number of holes required in your firewall to a minimum. These considerations have helped make IAX one of the easiest protocols (if not the easiest) to implement in secure networks.

SIP

The Session Initiation Protocol (SIP) has taken the world of VoIP by storm. Originally considered little more than an interesting idea, SIP now seems poised to dethrone the mighty H.323 as the VoIP protocol of choice certainly at the endpoints of the network. The premise of SIP is that each end of a connection is a peer, and the protocol negotiates capabilities between them. What makes SIP compelling is that it is a relatively simple protocol.

History

SIP was originally submitted to the Internet Engineering Task Force (IETF) in February of 1996 as “draft ietf mmusic sip 00.” The initial draft looked nothing like the SIP we know today and contained only a single request type: a call setup request. In March of 1999, after 11 revisions, SIP RFC 2543 was born.

At first, SIP was all but ignored, as H.323 was considered the protocol of choice for VoIP transport negotiation. However, as the buzz grew, SIP began to gain popularity, and while there may be a lot of different factors that accelerated its growth, we’d like to think that a large part of its success is due to its freely available specification.

Future

SIP has earned its place as the protocol that justified VoIP. All new user and enterprise products are expected to support SIP, and any existing products will now be a tough sell unless a migration path to SIP is offered. SIP is widely expected to deliver far more than VoIP capabilities, including the ability to transmit video, music, and any type of real time multimedia. SIP is poised to deliver the majority of new applications over the next few years.

Security considerations

SIP uses a challenge/response system to authenticate users. An initial INVITE is sent to the proxy with which the end device wishes to communicate. The proxy then sends back a 407 Proxy Authorization Request message, which contains a random set of characters referred to as a “nonce.” This nonce is used along with the password to generate an MD5 hash, which is then sent back in the subsequent INVITE. Assuming the MD5 hash matches the one that the proxy generated, the client is then authenticated.

Denial of Service (DoS) attacks are probably the most common type of attack on VoIP communications. A DoS attack can occur when a large number of invalid INVITE requests are sent to a proxy server in an attempt to overwhelm the system. These attacks are relatively simple to implement, and their effects on the users of the system are immediate. SIP has several methods of minimizing the effects of DoS attacks, but ultimately they are impossible to prevent.

SIP implements a scheme to guarantee that a secure, encrypted transport mechanism (namely Transport Layer Security, or TLS) is used to establish communication between the caller and the domain of the callee. Beyond that, the request is sent securely to the end device, based upon the local security policies of the network. Note that the encryption of the media (that is, the RTP stream) is beyond the scope of SIP itself and must be dealt with separately. More information regarding SIP security considerations, including registration hijacking, server impersonation, and session teardown, can be found in Section 26 of SIP RFC 3261.

SIP and NAT

Probably the biggest technical hurdle SIP has to conquer is the challenge of carrying out transactions across a NAT layer. Because SIP encapsulates addressing information in its data frames, and NAT happens at a lower network layer, the addressing information is not modified, and thus the media streams will not have the correct addressing information needed to complete the connection when NAT is in place. In addition to this, the firewalls normally integrated with NAT will not consider the incoming media stream to be part of the SIP transaction, and will block the connection.

H.323 Protocol Stack

The H.323 specification is an umbrella specification for the many different protocols that comprise the overall H.323 protocol stack. Figure 2 shows the H.323 protocol stack.

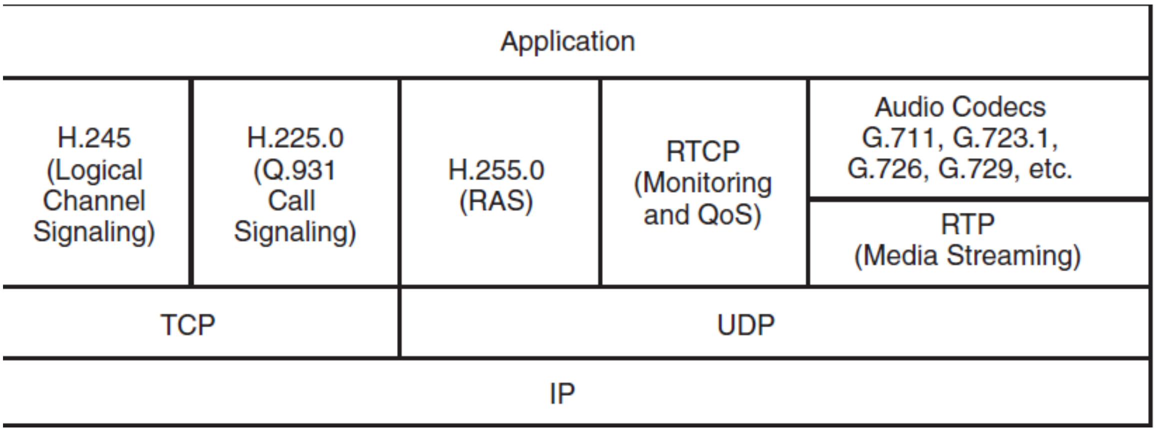

Application
H.245 (Logical Channel Signaling)
H.225.0 (Q.931 Call Signaling)
H.255.0 (RAS)
RTCP (Monitoring and QoS)
Audio Codecs G.711, G.723.1, G.726, G.729, etc.
RTP (Media Streaming)
TCP
UDP
IP

Fig. H.323 Protocol Stack

The purpose of each protocol is summarized briefly as follows:

H.245

Specifies messages for opening and closing channels for media streams, and other commands, requests, and indications.

Q.931

Defines signaling for call setup and call teardown.

H.225.0

Specifies messages for call control, including signaling, the packetization and synchronization of media streams, and Registration, Admission, and Status (RAS).

Real Time Protocol (RTP)

The RTP specification is an IETF draft standard (RFC 1889) that defines the end to end transport of real time data. RTP does not guarantee quality of service (QoS) on the transmission. However, it does provides some techniques to aid the transmission of isochronous data, including:

- information about the type of data being transmitted
- time stamps
- sequence numbers

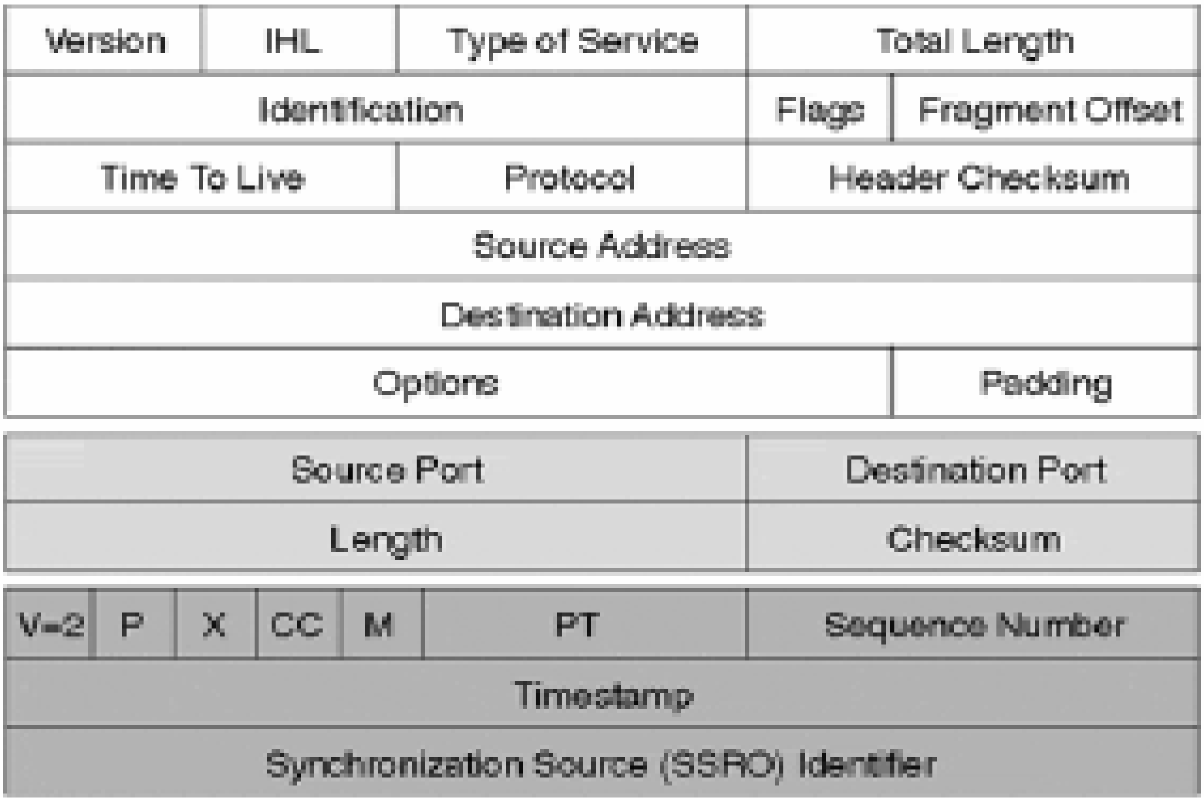
Real Time Control Protocol (RTCP)

RTCP is part of the IETF RTP specification (RFC 1889) and defines the end to end monitoring of data delivery and QoS by providing information such as:

- jitter, that is, the variance in the delays introduced in transmitting data over a wire average packet loss

The H.245, Q.931, and H.225.0 combination provide the signaling for the establishment of a connection, the negotiation of the media format that will be transmitted over the connection, and call teardown at termination. As indicated in Figure 2, the call signaling part of the H.323 protocol is carried over TCP, since TCP guarantees the in order delivery of packets to the application.

The RTP and RTCP combination is for media handling only. As indicated in Figure 2, the media part of the H.323 protocol is carried over UDP and therefore there is no guarantee that all packets will arrive at the destination and be placed in the correct order.

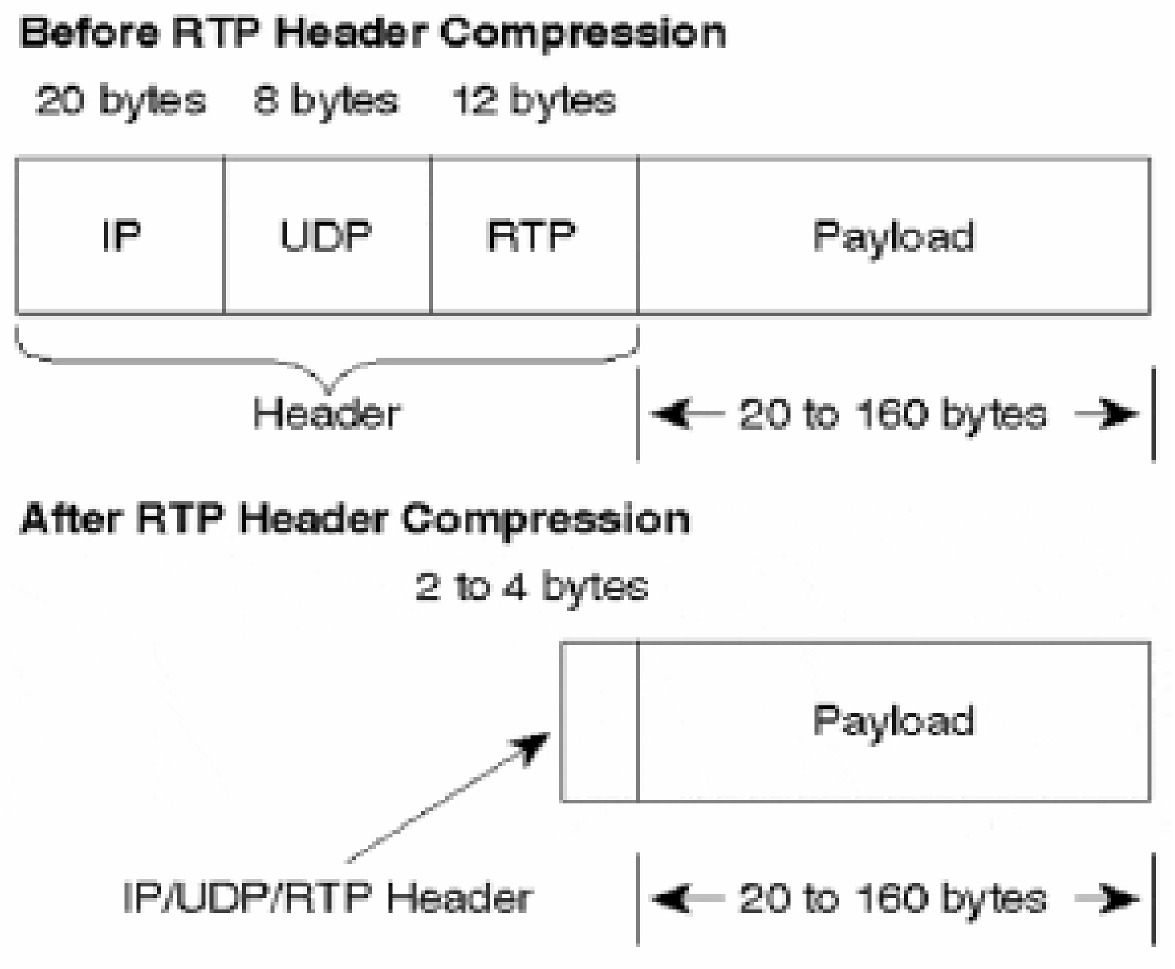


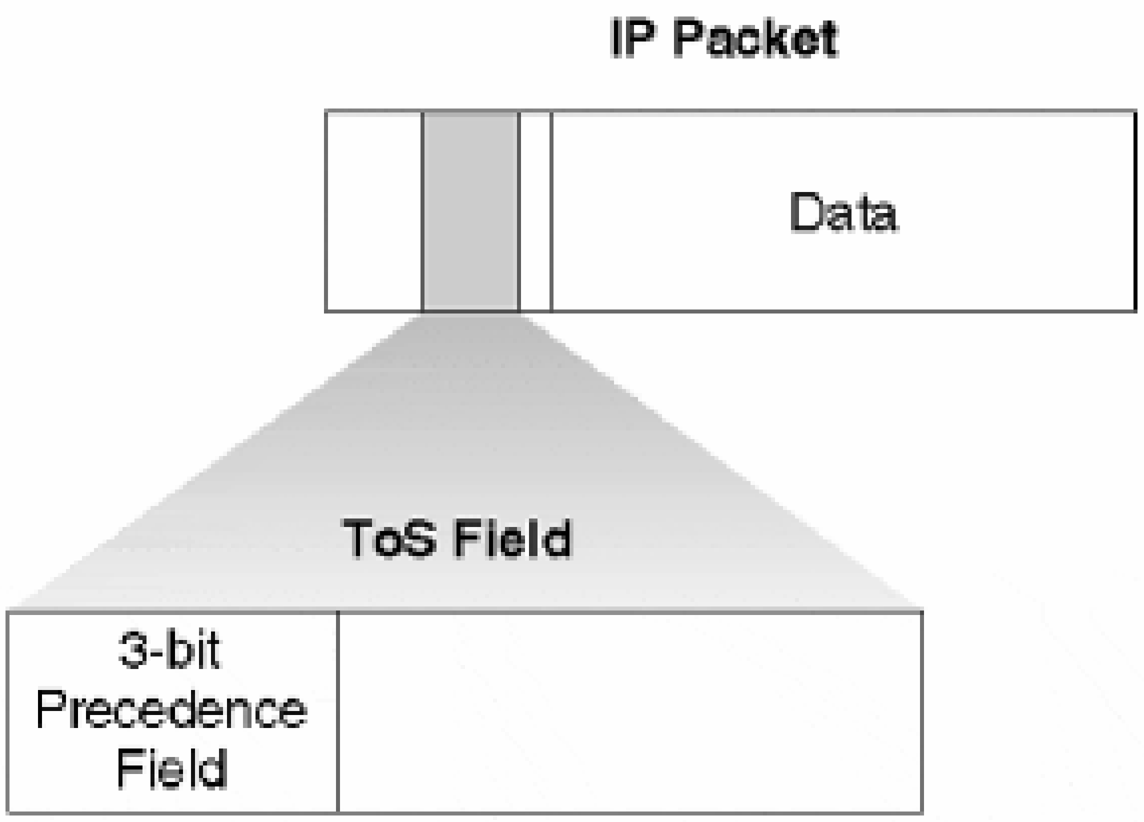
Version	IHL	Type of Service	Total Length
Identification		Flags	Fragment Offset
Time To Live		Protocol	Header Checksum
Source Address			
Destination Address			
Options			Padding

Source Port	Destination Port
Length	Checksum

V=2	P	X	CC	M	PT	Sequence Number
Timestamp						
Synchronization Source (SSRC) Identifier						

Fig. Real Time Transport Header


Before RTP Header Compression
20 bytes
8 bytes
12 bytes
IP
UDP
RTP
Payload
Header
20 to 160 bytes
After RTP Header Compression
2 to 4 bytes
Payload
IP/UDP/RTP Header
20 to 160 bytes


IP Packet
Data
ToS Field
3-bit Precedence Field

Codecs

RTP and RTCP data is the payload of a User Datagram Protocol (UDP) packet. Analog signals coming from an endpoint are converted into the payload of UDP packets by codecs (coders/decoders). The codecs perform compression and decompression on the media streams.

Different types of codecs provide varying sound quality. The bit rate of most narrow band codecs is in the range 1.2 kbps to 64 kbps. The higher the bit rate the better the sound quality. Some of the most popular codecs are:

G.711

Provides a bit rate of 64 kbps.

G.723.1

Provides bit rates of either 5.3 or 6.4 kbps. Voice communication using this codec typically exhibits some form of degradation.

Codec Type and Sample Size Effects on Bandwidth

Codec	Bandwidth Consumed	Bandwidth Consumed	Sample Latency
G. 729 w/ one 10 ms sample/frame	40 kbps	9.6 kbps	15ms
G.729 w/four 10 ms samples/frame	16 kbps	8.4 kbps	45ms
G.729 w/two 10 ms samples/frame	24 kbps	11.2 kbps	25ms
G.711 w/one 10 ms sample/frame	112 kbps	81.6 kbps	10ms
G.711 w/two 10 ms samples/frame	96 kbps	80.8 kbps	20ms

G.729

Provides a bit rate of 8 kbps. This codec is very popular for voice over frame relay and for V.70 voice and data modems.

Frames per Packet (G.729)			
G.729 Samples per Frame	IP/RTP/UDP Header	Bandwidth Consumed	Latency*
Default (two samples per frame)	40 bytes	24,000 bps	25 ms
Satellite (four samples per frame)	40 bytes	16,000 bps	45ms
Low Latency (one sample per frame)	40 bytes	40,000 bps	15 ms
*Compression and packetization delay only			

GSM

Provides a bit rate of 13 kbps. This codec is based on a telephony standard defined by the European Telecommunications Standards Institute (ETSI). The 13 kbps bit rate is achieved with little degradation of voice grade audio.

Basic H.323 Call Scenario

A simple H.323 call scenario can be described in five phases:

- Call Setup
- Capability Exchange
- Call Initiation
- Data Exchange
- Call Termination

Calls between two endpoints can be either direct or routed via a gatekeeper. This scenario describes a direct connection where each endpoint is a point of entry and exit of a media flow. The scenario described in this section assumes a slow start connection procedure. The example in this section describes the procedure for placing a call between two endpoints, A and B, each with an IP address on the same subnet.

H.323

This International Telecommunication Union (ITU) protocol was originally designed to provide an IP transport mechanism for video conferencing. It has become the standard in IP based video conferencing equipment, and it briefly enjoyed fame as a VoIP protocol as well. While there is much heated debate over whether SIP or H.323 (or IAX) will dominate the VoIP protocol world, in Asterisk, H.323 has largely been deprecated in favour of IAX and SIP. H.323 has not enjoyed much success among users and enterprises, although it is still the most widely used VoIP protocol among carriers.

The two versions of H.323 supported in Asterisk are handled by the modules chan_h323.so (supplied with Asterisk) and chan_oh323.so (available as a free addon).

History

H.323 was developed by the ITU in May of 1996 as a means to transmit voice, video, data, and fax communications across an IP based network while maintaining connectivity with the PSTN. Since that time, H.323 has gone through several versions and annexes (which add functionality to the protocol), allowing it to operate in pure VoIP networks and more widely distributed networks.

Future

The future of H.323 is a subject of hot debate. If the media is any measure, it doesn't look good for H.323; it hardly ever gets mentioned (certainly not with the regularity of SIP). H.323 is commonly regarded as technically superior to SIP, but, as with so many other technologies, that ultimately might not matter. One of the factors that makes H.323 unpopular is its complexity although many argue that the once simple SIP is starting to suffer from the same problem.

H.323 still carries by far the majority of worldwide carrier VoIP traffic, but as people become less and less dependent on traditional carriers for their telecom needs, the future of H.323 becomes more difficult to predict with any certainty. While H.323 may not be the protocol of choice for new implementations.

Security considerations

H.323 is a relatively secure protocol and does not require many security considerations beyond those that are common to any network communicating with the Internet. Since H.323 uses the RTP protocol for media communications, it does not natively support encrypted media paths. The use of a VPN or other encrypted tunnel between endpoints is the most common way of securely encapsulating communications. Of course, this has the disadvantage of requiring the establishment of these secure tunnels between endpoints, which may not always be convenient (or even possible). As VoIP becomes used more often to communicate with financial institutions such as banks, we're likely to require extensions to the most commonly used VoIP protocols to natively support strong encryption methods.

H.323 and NAT

The H.323 standard uses the Internet Engineering Task Force (IETF) RTP protocol to transport media between endpoints. Because of this, H.323 has the same issues as SIP when dealing with network topologies involving NAT. The easiest method is to simply forward the appropriate ports through your NAT device to the internal client.

To receive calls, you will always need to forward TCP port 1720 to the client. In addition, you will need to forward the UDP ports for the RTP media and RTCP control streams (see the manual for your device for the port range it requires). Older clients, such as MS Netmeeting, will also require TCP ports forwarded for H.245 tunneling (again, see your client's manual for the port number range).

If you have a number of clients behind the NAT device, you will need to use a gatekeeper running in proxy mode. The gatekeeper will require an interface attached to the private IP subnet and the public Internet. Your H.323 client on the private IP subnet will then register to the gatekeeper, which will proxy calls on the clients' behalf. Note that any external clients that wish to call you will also be required to register with the proxy server.

At this time, Asterisk can't act as an H.323 gatekeeper. You'll have to use a separate application, such as the open source OpenH323 Gatekeeper (http://www.gnugk.org).

MGCP

The Media Gateway Control Protocol (MGCP) also comes to us from the IETF. While MGCP deployment is more widespread than one might think, it is quickly losing ground to protocols such as SIP and IAX. Still, Asterisk loves protocols, so naturally it has rudimentary support for it.

It was designed to make the end devices (such as phones) as simple as possible, and have all the call logic and processing handled by media gateways and call agents. Unlike SIP, MGCP uses a centralized model. MGCP phones cannot directly call other MGCP phones; they must always go through some type of controller.

Asterisk supports MGCP through the chan_mgcp.so module, and the endpoints are defined in the configuration file mgcp.conf. Since Asterisk provides only basic call agent services, it cannot emulate an MGCP phone (to register to another MGCP controller as a user agent, for example).

If you have some MGCP phones lying around, you will be able to use them with Asterisk. If you are planning to put MGCP phones into production on an Asterisk system, keep in mind that the community has moved on to more popular protocols, and you will therefore need to budget your software support needs accordingly. If possible (for example, with Cisco phones), you should upgrade MGCP phones to SIP.

Proprietary Protocols

Finally, let's take a look at two proprietary protocols that are supported in Asterisk.

Skinny/SCCP

The Skinny Client Control Protocol (SCCP) is proprietary to Cisco VoIP equipment. It is the default protocol for endpoints on a Cisco Call Manager PBX. Skinny is supported in Asterisk, but if you are connecting Cisco phones to Asterisk, it is generally recommended that you obtain SIP images for any phones that support it and connect via SIP instead.

UNISTIM

Support for Nortel's proprietary VoIP protocol, UNISTIM, has recently been added to Asterisk. This remarkable milestone means that Asterisk is the first PBX in history to natively support proprietary IP terminals from the two biggest players in VoIP, Nortel and Cisco.

Codecs

Codecs are generally understood to be various mathematical models used to digitally encode (and compress) analog audio information. Many of these models take into account the human brain's ability to form an impression from incomplete information. We've all seen optical illusions; likewise, voice compression algorithms take advantage of our tendency to interpret what we believe we should hear, rather than what we actually hear.* The purpose of the various encoding algorithms is to strike a balance between efficiency and quality.

Codec quick reference

Codec	Data bitrate (kbps)	Licence required ?
G.711	64 kbps	No
G.726	16, 24, or 32 kbps	No
G.723.1	5.3 or 6.3 kbps	Yes(no for passthrough)
G.729A	8 kbps	Yes(no for passthrough)
GSM	13 kbps	No
iLBC	13.3 kbps (30 ms frames) or 15.2 kbps (20 ms	No
Speex	Variable (between 2.15 and 22.4 kbps)	No

G.711

G.711 is the fundamental codec of the PSTN. In fact, if someone refers to PCM (discussed in the previous chapter) with respect to a telephone network, you are allowed to think of G.711. Two companding methods are used: μ law in North America and A law in the rest of the world. Either one delivers an 8 bit word transmitted 8,000 times per second. If you do the math, you will see that this requires 64,000 bits to be transmitted per second.

Many people will tell you that G.711 is an uncompressed codec. This is not exactly true, as companding is considered a form of compression. What is true is that G.711 is the base codec from which all of the others are derived.

On an audio CD, quality is far more important than bandwidth, so the audio is quantized at 16 bits (times 2, as it's stereo), with a sampling rate of 44,100 Hz. Considering that the CD was invented in the late 1970s, this was quite impressive stuff. The telephone network does not require this level of quality (and needs to optimize bandwidth), so telephone signals are encoded using 8 bits, at a sampling frequency of 8,000 Hz.

G.726

This codec has been around for some time (it used to be G.721, which is now obsolete), and it is one of the original compressed codecs. It is also known as Adaptive Differential Pulse Code Modulation (ADPCM), and it can run at several bitrates. The most common rates are 16 kbps, 24 kbps, and 32 kbps. As of this writing, Asterisk currently supports only the ADPCM32 rate, which is far and away the most popular rate for this codec. G.726 offers quality nearly identical to G.711, but it uses only half the bandwidth. This is possible because rather than sending the result of the quantization measurement, it sends only enough information to describe the difference between the current sample and the previous one. G.726 fell from favor in the 1990s due to its inability to carry modem and fax signals, but because of its bandwidth/CPU performance ratio it is now making a comeback. G.726 is especially attractive because it does not require a lot of computational work from the system.

G.723.1

Not to be confused with G.723 (which is another obsolete version of ADPCM), this codec is designed for low bitrate speech. It has two data bitrate settings: 5.3 kbps and 6.3 kbps. G.723.1 is one of the codecs required for compliance with the H.323 protocol (although other codecs may be employed by H.323). It is currently encumbered by patents and thus requires licensing if used in commercial applications. What this means is that while you can switch two G.723.1 calls through your Asterisk system, you are not allowed to decode them without a license.

G.729A

Considering how little bandwidth it uses, G.729A delivers impressive sound quality. It does this through the use of Conjugate Structure Algebraic Code Excited Linear Prediction (CS ACELP).* Because of patents, you can't use G729A without paying a licensing fee; however, it is extremely popular and is thus well supported on many different phones and systems.

To achieve its impressive compression ratio, this codec requires an equally impressive amount of effort from the CPU. In an Asterisk system, the use of heavily compressed codecs will quickly bog down the CPU. G.729A uses 8 kbps of bandwidth.

GSM

GSM is the darling codec of Asterisk. This codec does not come encumbered with a licensing requirement the way that G.723.1 and G.729A do, and it offers outstanding performance with respect to the demand it places on the CPU. The sound quality is generally considered to be of a lesser grade than that produced by G.729A, but as much of this comes down to personal opinion, be sure to try it out. GSM operates at 13 kbps.

iLBC

The Internet Low Bitrate Codec (iLBC) provides an attractive mix of low bandwidth usage and quality, and it is especially well suited to sustaining reasonable quality on lossy network links. Naturally, Asterisk supports it (and support elsewhere is growing), but it is not as popular as the ITU codecs and thus may not be compatible with common IP telephones and commercial VoIP systems. IETF RFCs 3951 and 3952 have been published in support of iLBC, and iLBC is on the IETF standards track. Because iLBC uses complex algorithms to achieve its high levels of compression, it has a fairly high CPU cost in Asterisk.

While you are allowed to use iLBC without paying royalty fees, the holder of the iLBC patent, Global IP Sound (GIPS), wants to know whenever you use it in a commercial application. The way you do that is by downloading and printing a copy of the iLBC license, signing it, and returning it to them. If you want to read about iLBC and its license, you can do so at http://www.ilbcfreeware.org. iLBC operates at 13.3 kbps (30 ms frames) and 15.2 kbps (20 ms frames).

Speex

Speex is a Variable Bitrate (VBR) codec, which means that it is able to dynamically modify its bitrate to respond to changing network conditions. It is offered in both narrowband and wideband versions, depending on whether you want telephone quality or better. Speex is a totally free codec, licensed under the Xiph.org variant of the BSD license. An Internet draft for Speex is available, and more information about Speex can be found at its home page (http://www.speex.org). Speex can operate at anywhere from 2.15 to 22.4 kbps, due to its variable bitrate

MP3

Sure thing, MP3 is a codec. Specifically, it's the Moving Picture Experts Group Audio Layer 3 Encoding Standard.* With a name like that, it's no wonder we call it MP3! In Asterisk, the MP3 codec is typically used for Music on Hold (MoH). MP3 is not a telephony codec, as it is optimized for music, not voice; nevertheless, it's very popular with VoIP telephony systems as a method of delivering Music on Hold.

Be aware that music cannot usually be broadcast without a license. Many people assume that there is no legal problem with connecting a radio station or CD as a Music on Hold source, but this is very rarely true.

TCP, UDP, and SCTP

If you're going to send data on an IP based network, it will be transported using one of the three transport protocols discussed here.

Transmission Control Protocol

The Transmission Control Protocol (TCP) is almost never used for VoIP, for while it does have mechanisms in place to ensure delivery, it is not inherently in any hurry to do so. Unless you have an extremely low latency interconnection between the two endpoints, TCP is going to tend to cause more problems than it solves.

The purpose of TCP is to guarantee the delivery of packets. In order to do this, several mechanisms are implemented, such as packet numbering (for reconstructing blocks of data), delivery acknowledgment, and re requesting lost packets. In the world of VoIP, getting the packets to the endpoint quickly is paramount but 20 years of cellular telephony has trained us to tolerate a few lost packets.

TCP's high processing overhead, state management, and acknowledgment of arrival work well for transmitting large amounts of data, but it simply isn't efficient enough for real time media communications.

User Datagram Protocol

Unlike TCP, the User Datagram Protocol (UDP) does not offer any sort of delivery guarantee. Packets are placed on the wire as quickly as possible and released into the world to find their way to their final destinations, with no word back as to whether they get there or not. Since UDP itself does not offer any kind of guarantee that the data will arrive,† it achieves its efficiency by spending very little effort on what it is transporting.

TCP is a more "socially responsible" protocol, because the bandwidth is more evenly distributed to clients connecting to a server. As the percentage of UDP traffic increases, it is possible that a network could become overwhelmed.

Stream Control Transmission Protocol

Approved by the IETF as a proposed standard in RFC 2960, SCTP is a relatively new transport protocol. From the ground up, it was designed to address the shortcomings of both TCP and UDP, especially as related to the types of services that used to be delivered over circuit switched telephony networks.

Some of the goals of SCTP were:

- Better congestion avoidance techniques (specifically, avoiding Denial of Service attacks)
- Strict sequencing of data delivery
- Lower latency for improved real time transmissions

By overcoming the major shortcomings of TCP and UDP, the SCTP developers hoped to create a robust protocol for the transmission of SS7 and other types of PSTN signaling over an IP based network.

Differentiated Service

Differentiated service, or DiffServ, is not so much a QoS mechanism as a method by which traffic can be flagged and given specific treatment. Obviously, DiffServ can help to provide QoS by allowing certain types of packets to take precedence over others. While this will certainly increase the chance of a VoIP packet passing quickly through each link, it does not guarantee anything.

Guaranteed Service

The ultimate guarantee of QoS is provided by the PSTN. For each conversation, a 64 kbps channel is completely dedicated to the call the bandwidth is guaranteed. Similarly, protocols that offer guaranteed service can ensure that a required amount of bandwidth is dedicated to the connection being served. As with any packetized networking technology, these mechanisms generally operate best when traffic is below maximum levels. When a connection approaches its limits, it is next to impossible to eliminate degradation.

MPLS

Multiprotocol Label Switching (MPLS) is a method for engineering network traffic patterns independent of layer 3 routing tables. The protocol works by assigning short labels (MPLS frames) to network packets, which routers then use to forward the packets to the MPLS egress router, and ultimately to their final destinations. Traditionally, routers make an independent forwarding decision based on an IP table lookup at each hop in the network. In an MPLS network, this lookup is performed only once, when the packet enters the MPLS cloud at the ingress router.

The packet is then assigned to a stream, referred to as a Label Switched Path (LSP), and identified by a label. The label is used as a lookup index in the MPLS forwarding table, and the packet traverses the LSP independent of layer 3 routing decisions. This allows the administrators of large networks to finetune routing decisions and to make the best use of network resources. Additionally, information can be associated with a label to prioritize packet forwarding.

RSVP

Reservation protocol, MPLS contains no method to dynamically establish LSPs, but you can use the Reservation protocol (RSVP) with MPLS. RSVP is a signaling protocol used to simplify the establishment of LSPs and to report problems to the MPLS ingress router. The advantage of using RSVP in conjunction with MPLS is the reduction in administrative overhead. If you don't use RSVP with MPLS, you'll have to go to every single router and configure the labels and each path manually.

Using RSVP makes the network more dynamic by distributing control of labels to the routers. This enables the network to become more responsive to changing conditions, because it can be set up to change the paths based on certain conditions, such as a certain path going down (perhaps due to a faulty router). The configuration within the router will then be able to use RSVP to distribute new labels to the routers in the MPLS network, with no (or minimal) human intervention.

CHAPTER 3

ASTERISK BASED PBX

Introduction

Asterisk is an open source software implementation of a Private Branch Exchange (PBX). The software was originally created in 1999 by Mark Spence of Digium Corporation in the United States. Digium is primary developer for the Asterisk software package as well as a range of associated software and hardware products. Asterisk was designed for the Linux operating system and can be installed on either PC servers and compatible embedded hardware. Asterisk is available in a range of different formats and licenses.

As a pure software product it is available as:

Downloadable GPL licensed open source software for end user install. Asterisk can be downloaded free of charge from the website www.asterisk.org. The download version of Asterisk supports most functions except for components that have intellectual property restrictions such as G.729 Codec's, fax and echo cancellation. These components can be purchased for additional cost from Digium and other suppliers.

Commercial Licensing is also available for Asterisk. Commercial Licensing charges are intended to be used by OEM manufacturers and large scale solution providers and are priced accordingly.

Prepackaged systems are also available from Digium and other vendors which provide ready to run distributions that simplify the installation and configuration of the system. Prepackaged distributions include 'Asterisk Now' from Digium. This package is available free of charge as a community supported product. If commercial support is required, Digium provides a range of commercial support options. Prepackaged distributions are also available from other vendors and are typically not supplied as free downloadable products.

Asterisk is also available as preconfigured hardware/software complete solution from Digium and other manufacturers. These products are similar to proprietary PBX products and include support for TDM and Analog buses, VoIP and Analog handsets. The Digium manufactured turnkey Asterisk system is SwitchVox. The turnkey products typically include capabilities and ease of use features that are not included in the downloaded products.

Features of Asterisk PBX:

Many of the features of modern PBX systems are available in an Asterisk PBX. Enhanced functionality that extends these features is also available from Digium and other suppliers.

- CTI
- Audio codecs ADPCM, G.711, G.722, G.72 & GSM
- VoIP Protocols SIP, IAX & MGCP
- Traditional Telephony Protocols E&M, FXS, FXO, Loop start, MF and DTMF
- ISDN Protocols AT&T, Euro ISDN BRI/PRI, Lucent SESS, Nortel DMS100, QSig

Performance of an Asterisk System

Asterisk can run on most recent PC server hardware that supports the Linux operating system. Under specified system, will result in performance shortcomings such as audio quality, distortion, echo, call delays and dropped calls. With increase in load, system will have difficulty in maintaining the reliable operation.

The following factors will affect the performance of the Asterisk PBX.

Number Of Concurrent Calls

The more concurrent calls that exist, the more load that is created on the system. Load is caused by DSP functionality, Codec Coding, Protocol parsing and IP data transfer.

Call Establishment Rate

The system can only handle a specific number of calls being presented to or originating from the system within a short time period before delays and dropped calls will start to occur. VoIP load testing tools need to be employed to establish these limits.

Use of complex codec's such as G729, G723.1 and GSM

A system that might handle 50 concurrent call using G.711 codec, may only be able to support 10 concurrent calls with G 729 codec. Therefore the transcoding functions must be transferred to external gateways.

Echo Cancellation

Echo cancellation may be required on any call where existing TDM exchange interface is involved. Since echo cancellation is a mathematical function, the more of it the system has to perform, the higher the load on the CPU will be. Therefore the echo cancellation task should be shifted to end terminals like IP phones and gateways.

Hardware for Analog connections:

Asterisk connects with analog telephony connections through either a gateway card that is installed in the host computer or through an external gateway device. External gateways connect with Asterisk over the LAN. If internal gateway cards are used, transcoding and echo cancellation shall be done by Asterisk, thereby loading the CPU and thus affecting the performance. If external gateways are used, these functions shall be transferred to external gateways, thereby reducing the load on the server.

Features provided

More features like IVR (voice menu), text to speech, voice mail, speech recognition, recording etc. increase the load on server.

Reliability and Scalability requirement

These factors are affected by redundancy, type of computer system/server selected, capacity of the server, type of environment provided etc.

Underlying LAN/IP Network

Factors like speed, QoS support, provision of VLAN, Power over Ethernet will affect the voice quality and reliability of the system.

Implementation Guide Lines

Asterisk is available in versions 1.4, 1.6.x & 1.8.x version 1.8 is the most recent and being planned for NGN/Video support. It is recommended to use latest Asterisk Version 1.8.x.
with SIP as signaling protocol.

Implementation should have a web based interface for adding and configuring users. G.711 codec should be used to provide good voice quality and to reduce latency. However it will increase the bandwidth requirement. The bandwidth requirement is about 87 kbps per channel. Whereas the bandwidth requirement with other codec's (G.729, ILBC, GSM) is generally less than half of this. Use of G.711/G.722 codec is recommended. Use of G.729 requires licensing. This can be avoided by using same codec for all the SIP telephones connected to the server. This codec may be G.711 or G.729a. G.729a is very efficient codec but there may be issues regarding voice quality.

Using external gateways with the DSP with G.729a and G.711 codec's, thereby the transcoding functions for inter exchange communication and analog to SIP phone communication getting transferred to external gateways. Disable unused USB, serial and parallel ports of the server to avoid the CPU consumption due to unnecessary interrupt.

For large implementation of more than 500 subscribers, MySQL based database to be used for user/extension management.

External gateways are recommended for analog extension and E1 trunk, so that the echo cancellation and transcoding is not done by Asterisk, thereby increasing the call handling capacity of the system. therefore external gateways with DSP are to be used.

GUI Interface

Almost all the features which are required for an enterprise PBX are available with Asterisk PBX. All the necessary features as per local requirements may be provided. For centralized management, configuration, fault analysis etc. Network management system for SIP telephones and gateways should also be procured and installed including necessary spares. Installation and configuration of Asterisk shall require knowledge of Linux, scripting and telephony. GUI based interface should be there to configure Asterisk. GUIs which could be used are Free PBX or Asterisk GUI. The default interface of these GUIs is suitable to use Asterisk as a PBX for typical telecom needs. Moreover, the configurations not provided by a GUI can be done manually by Asterisk traditional configuration ways.

Server Specifications For 100 Lines

- Server should be suitable for 24x7 operations.
- Server should be from reputed brand like Dell, IBM and HP.
- Server should be installed in 1+1 redundancy.
- Processor should be Intel Atom dual core with minimum 1.8 GHz, 2 GB RAM, 256 MB cache with RAID1 dual HDD 250 GB minimum.
- Operating system should be recent standard Linux distribution.
- Server should work on 48V DC or 230V AC supply.
- Server should have dual Ethernet interfaces.

Server Specifications For 1000 Lines

- Server should be suitable for 24x7 operations.
- Server should be from reputed brand like Dell, IBM and HP.
- Processor should be quad core Xeon processor with minimum 8 GB RAM, 512 MB Cache, RAIDs HDD 500 GB Minimum.
- Server should be installed in 1+1 redundancy. The second server may be provided at geographically different location.
- Operating system should be recent standard Linux distribution.
- Server should work on 48V DC or 230V AC supply.
- Server should have dual Ethernet interfaces.

Analog gateways

These devices are with FXS/FXO ports.

Trunk gateways are with E&M/E1/PRI ports for inter exchange connectivity.

Analog gateway Specifications

- It should be an IP to TDM gateway.
- It should work both in registration and point to point mode.
- It should support SIP protocol with RFC 3261, RFC 3262, RFC 3263 & RFC 3264.
- It should support encryption of signaling like TLS and SRTP.
- It should support protocols like G.711, GSM, G.729, iLBC, G.722 codec's
- It should support protocols like T.38, T.30 for fax operations.
- It should have dual Ethernet interfaces.
- It should have GUI based configuration option.

Trunk Gateway Specifications

- It should be with four RJ45 slots on a single chassis.
- It should be managed by telnet, serial or web.
- It should have dual Ethernet interfaces.
- It should support protocols like SIP, SS7 and QSig.
- It should support protocols like G.711, GSM, G.729a/b, iLBC,G.722 codecs.
- It should support protocols like T.38, T.30 for fax operations.

SIP phones Specifications

- SIP phones should be as per TEC GR No.TEC/GR/SW/TER/SIP/02/Mar'2010.

Telephone connectivity

- Subscriber having LAN access are provided with IP telephones.
- Analog telephones/fax are provided through analog gateways.
- Remote locations are connected on WAN or E1 link.
- Remote locations not having IP or LAN connectivity are connected with FXO/FXS pairs on PDH/SDH Mux.

Inter exchange connectivity

- TDM exchanges are connected on E1/PRI interface with suitable gateways.
- IP exchanges are connected on IP trunk interface over a WAN or Ethernet link.

Network requirements

To ensure best possible voice quality and reliability, following is recommended.

- Guaranteed bandwidth to be provided for voice traffic or priority to voice traffic should be established using QoS tools. This QoS tool can also be integrated in MPLS network by assigning MPLS labels.
- VLAN's should be used to separate unnecessary broadcasts in the voice network.
- LAN should have sufficient redundancy so that failure of any single switch does not isolate very important telephones or the sever. Very important telephones and the Asterisk server should have redundancy at the access layer also i.e., they should have connection to two different switches.
- Switches should have PoE to avoid separate power supply for each IP telephone.

Security Considerations

- TLS and SRTP should be used for signaling and media security.
- Voice network should be provided with firewalls and VLANs. A mechanism to allow VoIP traffic through firewalls is required.
- Only authentic devices should be allowed to access the network.
- Unnecessary software should be removed from server.
- Unnecessary services should be disabled.
- Keep operating system up to date.
- User Accounts should have very strong passwords.
- Only the required network ports should be opened.
- Regular backups should be made.
- Ensure physical server security.

CHAPTER 4
NGN NEXT GENERATION NETWORK

Introduction

What is NGN

- NGN is a broad term to describe key evolutions in telecommunications for core and access network .The idea behind the NGN is that one network transports all information and services (voice ,data ,and all sorts of media such as video) by encapsulating these packets as on the internet .
- NGNs are commonly built around the Internet Protocol , therefore the term ' all IP " is commonly used to describe the transformation towards NGN .

Why NGN is required

- Revenue loss on Fixed Line users .
- New features & Value Added Services are IP based.
- Integrated Network for Voice and Data.
- Demand for Broadband by SP and EP.
- Reduced cost for Infrastructure.
- MPLS Network offered by ISP Service Provider

Problems of existing network

- Slow to develop new features and capabilities.
- Expensive upgrades and operating expenses.
- Large power and cooling requirements.
- Large Real Estate Space requirements.
- Limited migration strategy to new tech

Changing telecom trends

- Fixed line usages is reducing and revenue drivers are enterprise networks .
- Mobile use is increasing steadily with high penetration .
- Broadband Internet deployment shows a rapid growth trend .
- As per a statistical result IP traffic increases 10 fold every year while voice traffic is relatively flat

Convergence

- In other words convergence of voice and data network gave birth to NGN or Next Generation

How NGN will be used

- NGN is a collection of technologies which shall provide convergence for voice , data and video services . Voice shall also be transported through packet switching .
- NGN is a framework of services for next four to five years which shall use packet switching as the core transport and shall be access agnostic i.e. all types of access like fixed, wireless, IP, CDMA, GSM all can be used .

Advantages of NGN

- One network supports transmission of voice, data and video.
- No need to maintain two types networks viz., one for voice and one for data.
- Maintenance costs are less as no need to go for a variety of devices.
- Configuration process is simple can be done from a central location
- Quick deployment of new services.
- Supports all existing PSTN services like call forwarding and do not disturb.
- Number portability, phone number can be retained while changing ISP.
- Supports IP TV a growing business trend.
- One backbone for voice and data services instead of two parallel ones.
- No maintenance of proprietary switching systems.
- Fewer call controlling entities in the network so less capital and operating cost.

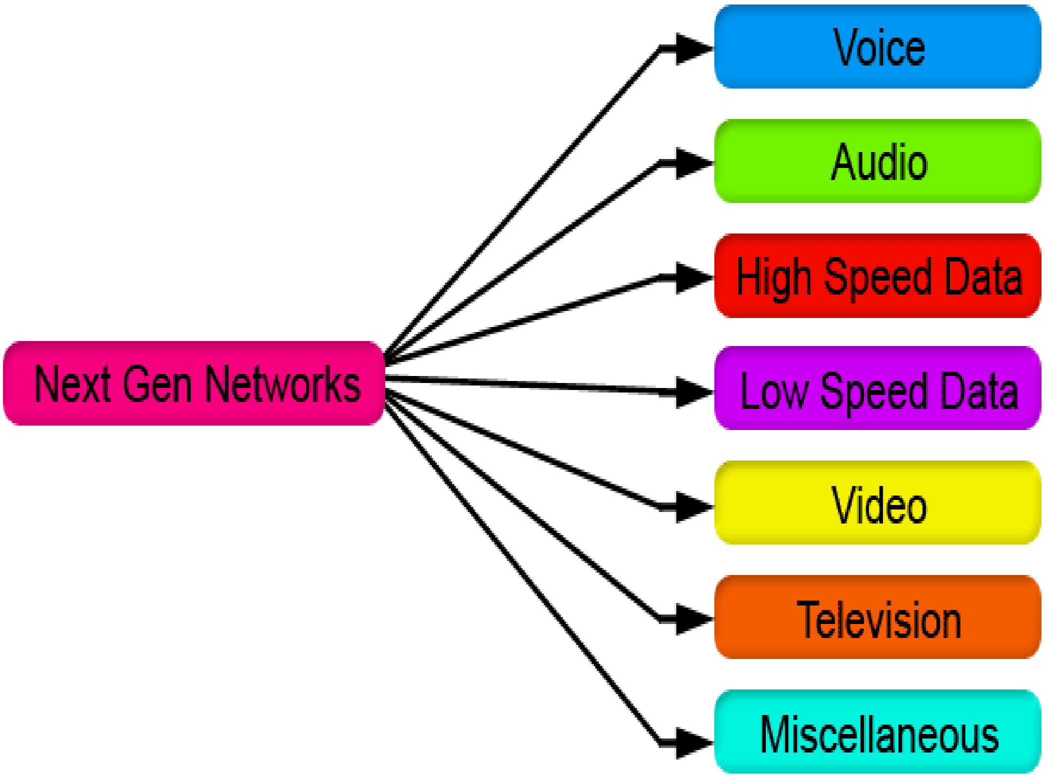


Fig. NGN Next Generation Network

- **VOICE TELEPHONE SERVICES** : NGN supports all existing [STN/PLMN voice telephony services like call forwarding, call waiting, centrex services, various IN services and value added services .
- **MULTIMEDIA SERVICES** : These services allow consumers to converse with each other while displaying visual information .
- **DATA SERVICES** : These include file transfer , www ,applications sharing interactivity etc .
- **MESSAGING SERVICES** : NGN supports both real time and non real time messaging services for fixed and mobile networks .

- **PUSH TO TALK SERVICE** : Push operation refers to service initiated data transmission to member of a group .
- **NUMBER PORTABILITY** : It provides end user to retain the phone number while changing the service provider .
- **VIRTUAL PRIVATE NETWORK** : Most common features used by the large organization to combine these enterprise private network at multiple location .
- **BROADCAST /MULTICAST /UNICAST** : Features used especially for video services using IPTV or presence .

International Telecommunication Union (ITU) in its recommendation Y.2001 has defined NGN, as a packet network able to provide telecommunication services. It uses broadband and QoS enabled transport technologies. In NGN service related functions are independent off transport related technologies.

At present separate networks exist for voice, data, mobile and Internet etc. Over the years, network operators have been looking for a service independent network architecture which can facilitate rapid and economical introduction of new services. The explosion of the Internet and popularity of Internet multimedia services emphasized the need to shift towards packet based core networks from the present circuit switched networks.

NGN is envisaged to facilitate the convergence of voice, data and video networks into a single unified packet based multiservice network. Converging voice, data and video services onto a common network infrastructure is a boon to the network operators.

NGN supports PSTN/ISDN replacement.

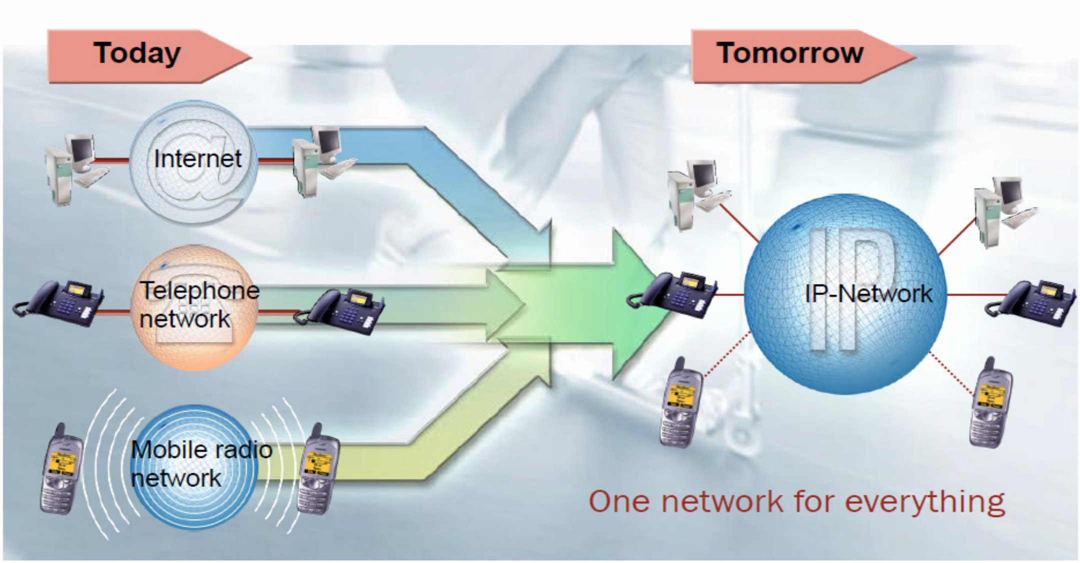
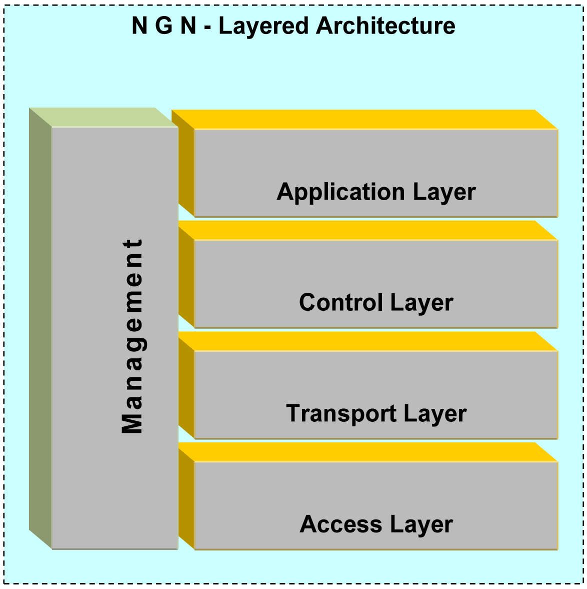


Fig. NGN Implementation

NGN ARCHITECTURE



Support for multiple access technologies

The NGN architecture offers the configuration flexibility needed to support multiple access technologies.

Distributed control

NGN supports distributed processing of packet based networks and support location transparency for distributed computing.

Open control

The NGN control interface is open to support service creation, service updating, and incorporation of service logic provision by third parties.

Independent service provisioning

The service provisioning process is separated from transport network operation by using the above mentioned distributed, open control mechanism. Support for services in a converged network. This is needed to generate flexible, easy to use multimedia services, by tapping the technical potential of the converged, fixed mobile functional architecture of the NGN.

Enhanced security and protection

This is the basic principle of an open architecture. It is imperative to protect the network infrastructure by providing mechanisms for security and survivability.

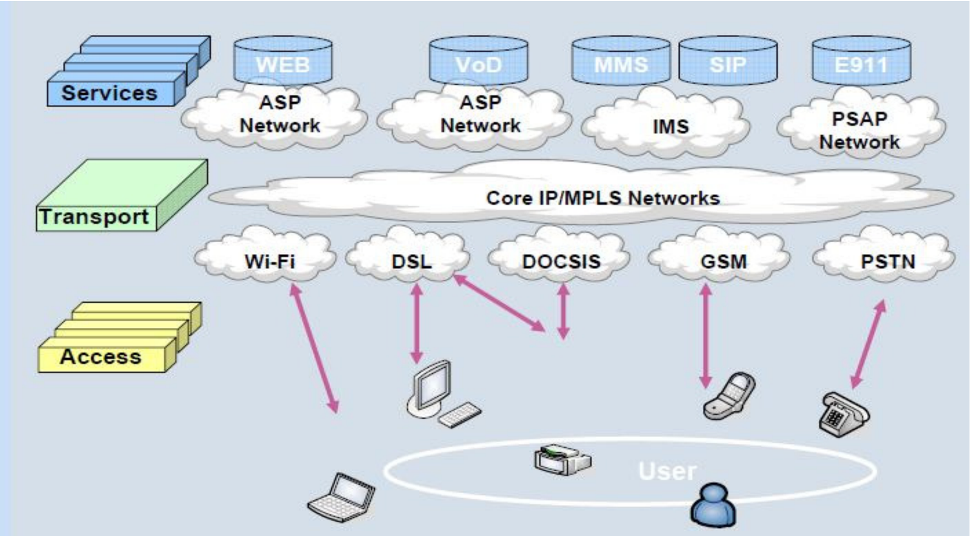


Fig. NGN Layered

Functional entity characteristics

Functional entities may not be distributed over multiple physical units but may have multiple instances. Functional entities have no direct relationship with the layered architecture.

One of the main characteristics of NGN is the decoupling of services and networks.

Decoupling can provide the advantage of services to be offered separately and to evolve independently. It is horizontally layered network architecture instead of the present vertically separated networks for each service. It uses Internet Protocol (IP) based transport for all services including voice.

Access Layer

Connects subscribers (Legacy/IP based), AN & PABX and trunks from PSTN, ISDN, and PLMN etc. Converting the format of information (circuit to packet or packet to circuit) before transmitting it.

Access Layer Components

IP terminals

The IP terminals refer to IP phones, IP PBX and software phones. They are typically intelligent terminals based on either H.323 or SIP protocol. IP terminals do not require to convert media as the voice already digitalized with IP terminals.

Integrated access device (IAD)

It is a device used to access subscribers (Analog, ADSL, IP) in the NGN. It accesses data of the subscriber terminals, voice services and video services to the packet network.

Access Layer (AL)

It acts as the line side interface to the core IP network and connects subscribers with analog subscriber access, integrated services digital network (ISDN) subscriber access, V5 subscriber access, PABX and x digital subscriber line (xDSL) access.

Access Network (AN)

The access network provides connectivity between the customer premises equipment and the access gateways in the service provider’s network. The access network includes access technology dependent functions, e.g., for WCDMA technology and xDSL access.

SIP phone

It is a multimedia device working in the Session Initiation Protocol (SIP).

H.323 phone

It is a multimedia device working in the H.323 protocol.

Signaling gateway (SG)

The SG provides the signaling interface between the IP network and the PSTN signaling network. It terminates SS7 links and provides Message Transport Part (MTP) Level 1 and Level 2 functionality. Each SG communicates with its associated circuit switch (CS) to support the end to end signaling for calls.

Trunk Media gateway (TMG)

It resides between the circuit switched (CS) network and the IP network. It converts format between pulse code modulation (PCM) signal flow and IP media flow. It supports functions such as packetization, echo control etc It can have integrated signaling gateway functionality also. The MGW can connect with devices, such as the PSTN exchange, private branch exchange (PBX), access network devices and base station controller (BSC).

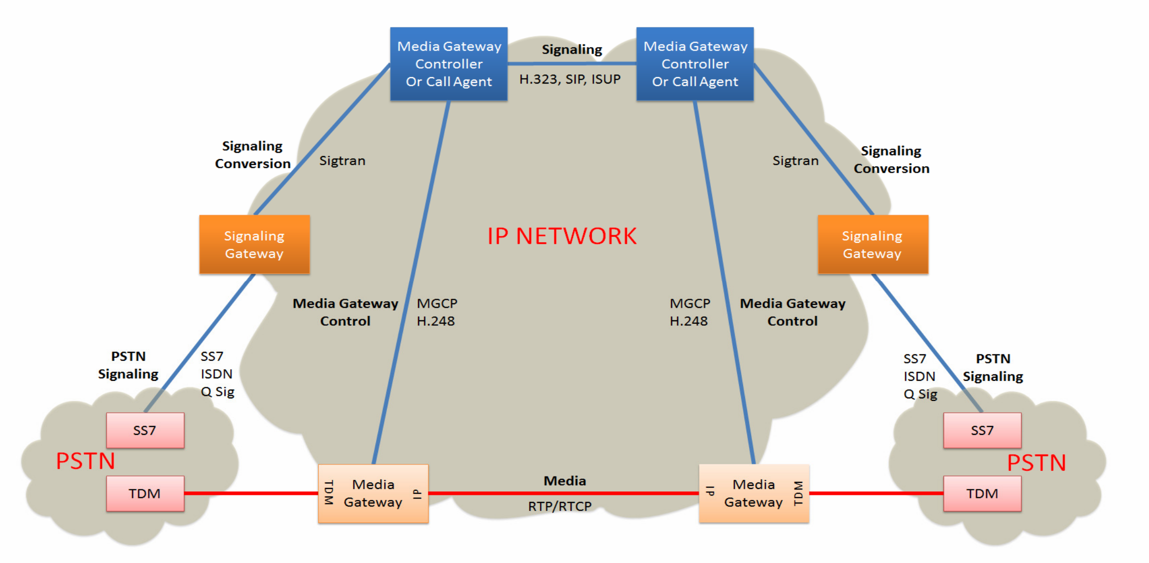


Fig. Media Gateways Connectivity

Session Border Controller (SBC)

Session Border Controller is located at the administrative boundary of an IP network for enforcing policy on multimedia sessions. Session policy may be defined to manage security, service level agreements, network device resources, network bandwidth, interworking and protocol interoperability between networks.

Session Border Controller (SBC) provides following functions:

- Interworking
- Security
- Management of service level agreements
- Overload control
- Network Address Translation and Firewall Traversal
- Lawful Interception
- Quality of Service (QoS) management
- Protocol Translation
- Call accounting

Session Border Controller functions can be logically split into two types, signaling related functions and media related functions.

Transport Layer

The transport functions provide the connectivity for all components and physically separated functions within the NGN. These functions provide support for the transfer of media information, as well as the transfer of control and management information. The transport layer is composed of devices, such as routers and layer 3 switches that are located in the backbone network and in the MAN. The primary function of the IP core network is to provide routing and transport of IP packets. It adopts the packet switching technology and provides subscribers with a common, integrated platform of data transport The network control layer adopts the software switching or soft switching technology to achieve primary real time call control Connection control.

The soft switch, also known as Media Gateway Controllers (MGC), Call Servers (CS) and Call Agents is the core device in the NGN. The Soft switch is located in the service provider's network and handles call control and signaling functions, typically maintaining call state for every call in the network. A Soft switch interacts with Application Servers to provide services that are not directly hosted on Soft switch. Important functions of Soft switch are:

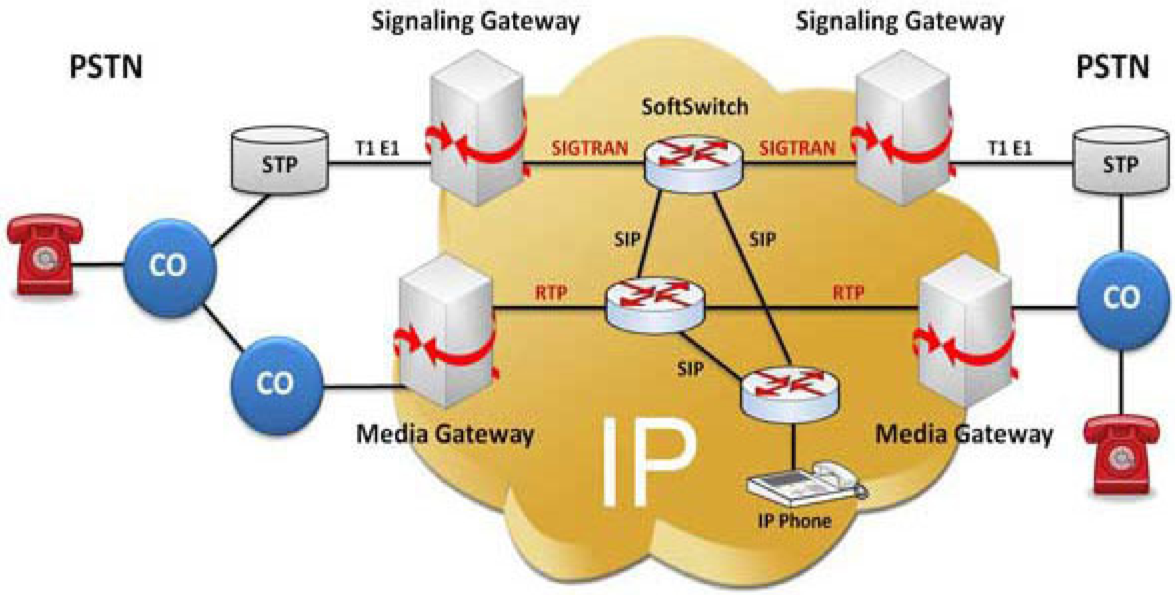


Fig. NGN Signaling Gateway

Call control

- Media gateway access control
- Signaling Gateway Control
- Border Gateways control
- Resource allocation
- Protocol processing
- Routing
- Authentication Charging

Soft switches also act as Signaling Switching Point (SSP) to provide access to IN services to SIP users. It supports basic voice and Multimedia services.

Service Layer

The service layer provides value added services and operation support functions.

Service Layer Components

OSS (Operation Support System)

It includes an integrated charging system, and network operation & management system, which conducts centralized management on the NGN components.

Application server

It produces and manages logics of value added services and intelligent network (IN) services, providing a platform for a third party to develop services through open APIs. The application server is the result of separating service from call control. It helps to develop supplementary services.

Media Server (MS)

It processes media streams in the basic and enhanced services. It provides functions of service tone playing, conference service,
interactive voice response (IVR), recorded announcement and advanced tone service.

Service control point (SCP)

It is the core component in the traditional IN, which is used to store subscriber data and service logics. The SCP starts a service logic based on the call events reported from the service switching point (SSP). It then, queries the service database and the subscriber database using the started service logic and sends proper call control instructions to the SSP on the next action. This helps to realize various intelligent calls, which is the main function of SCP. Video server It schedules and manages video conferences, and provides video conferences to NGN users.

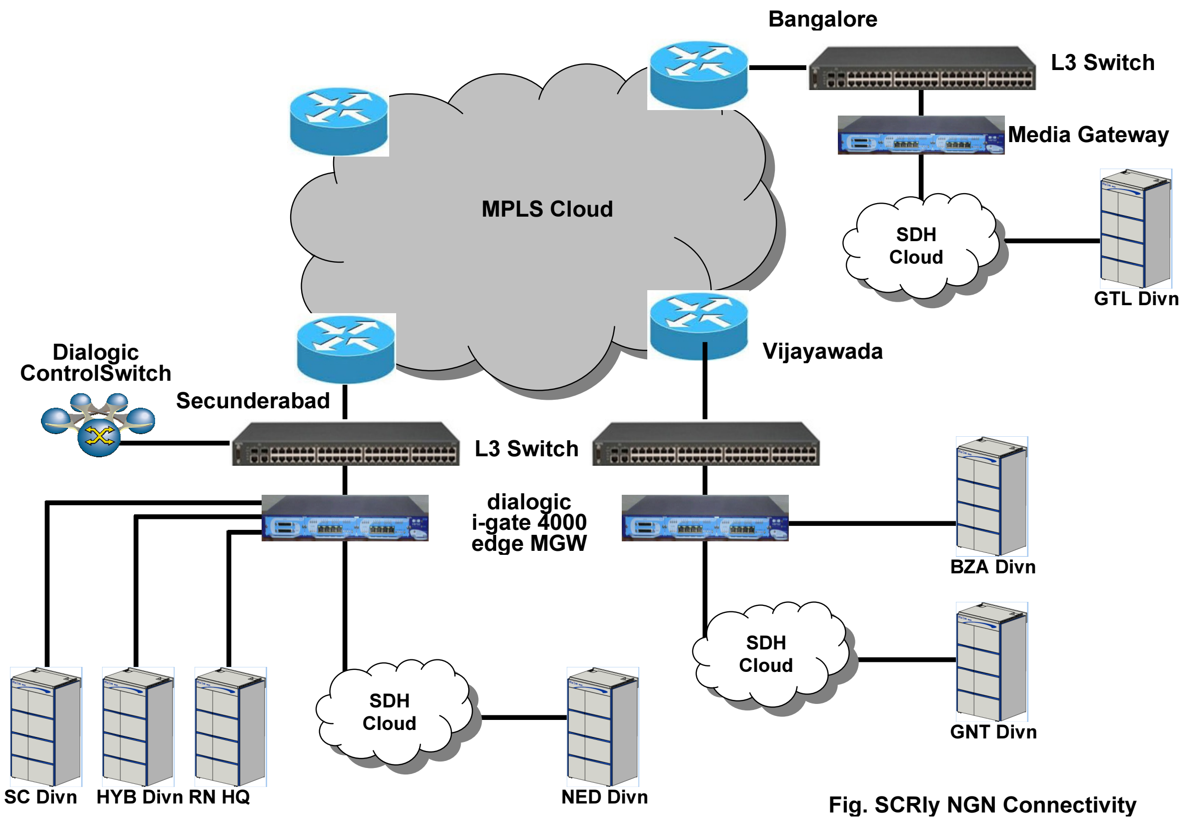


Fig. SCRly NGN Connectivity

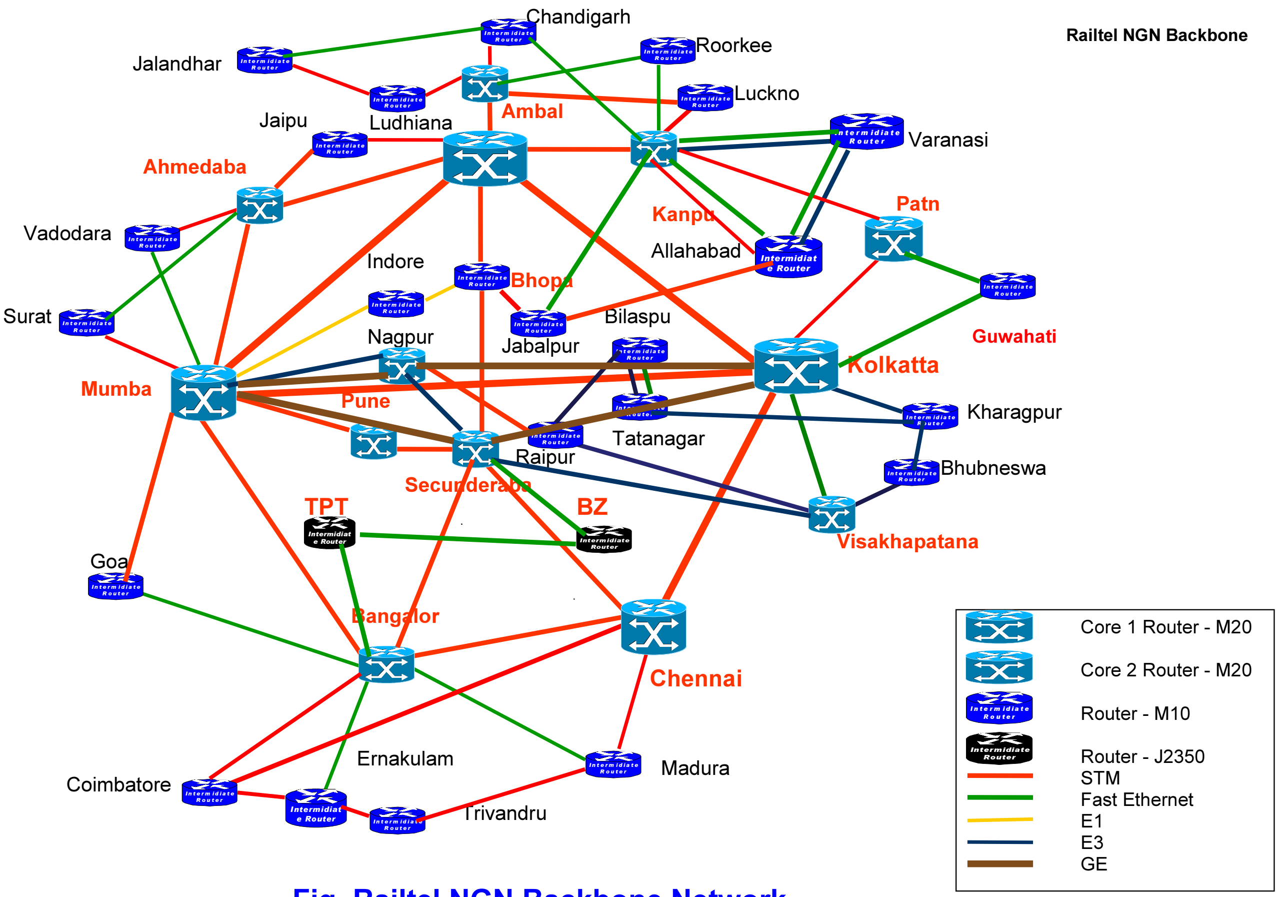


Fig. Railtel NGN Backbone Network

CHAPTER 5
NGN PROTOCOLS

Introduction

A protocol is a standard by which communication takes place between network devices. The following white paper attempts to explain in the simplest terms the protocols used by your Iomega network device.

TCP/IP

Transmission Control Protocol/Internet Protocol. TCP/IP is one of the core network protocols on top of which most other protocols are built. TCP watches network traffic to detect problems and ensure that data is safely transfered between network devices.

UDP

User Datagram Protocol (also Universal Datagram Protocol). Controls traffic between network devices, but does not attempt any error correction. It is used for protocols where speed is more important than accuracy or error correction is handled by the client software.

SMB/CIFS

Server Message Block/Common Internet File System. SMB is the File transfer protocol commonly used by Windows computers. Mac OS X and Linux/UNIX now commonly include an implementation of SMB known as Samba. This protocol uses TCP port 445.

AFP

Apple Filing Protocol. AFP is the file transfer protocol commonly used by Macintosh computers. This protocol is preferred for Mac transfers since it supports Unicode file names, resource forks, and other Mac OS specific attributes. This protocol uses TCP ports 548 and/or 427.

NFS

Network File System. NFS is the file transfer protocol commonly used by UNIX/Linux computers. Due to its UNIX roots, Mac OS X also supports NFS. This protocol uses TCP port 1025.

HTTPS

Hypertext Transfer Protocol Secure. This protocol is most commonly used for websites and combines HTTP (see below) transfers with SSL or TLS encryption. Iomega’s remote access features relies on HTTPS to transfer file lists, downloads, and uploads securely accross the Internet. The StorCenter ix Series will also use HTTPS for its web base configuration if security is enabled. HTTPS requires a certificate that verifies that the server operator is who they claim to be. Most web browsers will issue a warning if the HTTPS server’s certificate cannot be verified. Remote Access users can receive a HTTPS certificate for a nominal fee. HTTPS (Iomega Remote Access) typically uses TCP port 443.

FTP

File Transfer Protocol. FTP is a common Internet protocol used for file transfers. Although FTP is a very common protocol, it still may require special client software in some situations. For example, the Mac OS X finder supports FTP, but is read only you will need special software to use FTP to upload files. This protocol uses TCP port 21.

BitTorrent

BitTorrent is a common peer to peer (P2P) file sharing protocol used on the Internet. Torrents require special software clients such as the software builtin to the StorCenter ix Series. This file sharing method requires .torrent files that are downloaded from a torrent tracker — a special server that tracks which peers are sharing a file. The torrent tracker does not actually host a copy of the files that are being shared. Each peer shares portions of the torrent once it has been downloaded. File transfer rates increase as more peers participate in the download. This protocol uses TCP ports 6881 & 6999, however many Internet Service Providers (ISPs) throttle traffic on these ports. Some torrent trackers require that you use a port in the 49152 & 65535 (unassigned) range.

HTTP

Hypertext Transfer Protocol. This is the protocol used for most web traffic. Your iomega network device uses either this protocol or HTTPS (see above) to host the configuration interface. It will not allow you to host other websites on the device. This protocol usually uses TCP port 80, but may use 8008, 8080, 16080, etc.

Bluetooth

Bluetooth is a wireless transfer protocol that is used to transfer small files such as calendars, photos, and contacts over short distances (using OBEX or Object Exchange Protocol). It is also used to control devices such as mice wirelessly.

NTP

Network Time Protocol. NTP synchronizes the time between a client and a time server.
This protocol uses UDP port 123.

SMTP

Simple Mail Transfer Protocol. SMTP is a simple email protocol. SMTP is usually only used for outbound emails such as email notifications sent by your iomega network device. By default, this protocol uses UDP port 123.

UPnP

Universal Plug and Play. UPnP is a set of peer to peer network protocols that assistwith the discovery and control of network devices. Iomega network devices useUPnP to automatically configure network routers for port forwarding and servemultimedia files. DLNA and Microsoft Rally (see below) are both based on UPnP.

DLNA

Digital Living Network Alliance. DLNA is not technically a protocol, but is aseries of guidelines that define protocols, etc. necessary for network devicesto seamlessly share media files, such as movies, photos, and music. YourIomega network device uses DLNA for its media server.

DAAP/iTunes

Digital Audio Access Protocol. DAAP is a media sharing protocol developed by Apple forits iTunes software. DAAP uses Bonjour (see below) to announce and discover media files. This protocol uses TCP port 3689 by default.

Bonjour

Bonjour (formerly known as Rendezvous) is Apple's implementation of Zeroconf which isused to discover network resources. Bonjour announces your Iomega network device'sabilities as a file server, iTunes media server, and print server to client computers. Thisprotocol uses UDP port 5353.

Windows Rally

Rally is used to discover network resources. Rally announces your Iomega networkdevice's abilities as a file server, media server, and print server to client computers. Rallyis based on UPnP.

SNMP

Simple Network Management Protocol. SNMP is used to manage diverse networkresources using a single interface. StorCenter ix Series servers can be configured usingSNMP client software. This protocol uses UDP port 161.

A **Protocol Converter** is a device used to convert standard or proprietary protocol of one device to the protocol suitable for the other device or tools to achieve the interoperability. Protocols are software installed on the routers, which convert the data formats, data rate and protocols of one network into the protocols of the network in which data is navigating. There are varieties of protocols used in different fields like Power Generation, Transmission & Distribution, Oil & Gas, Automaton, Utilities, AMR, and Remote Monitoring applications. The major protocol translation messages involve conversion of data messages, events, commands and time synchronization.

A Media Gateway is a translation device or service that converts digital media streams between disparate telecommunications networks such as PSTN, SS7, Next Generation Networks (2G, 2.5G and 3G radio access networks) or PBX. Media gateways enable multimediacommunications across Next Generation Networks over multiple transport protocols such as Asynchronous Transfer Mode (ATM) andInternet Protocol (IP). Because the media gateway connects different types of networks, one of its main functions is to convert between different transmission and coding techniques (see also Transcode).

Media streaming functions such as echo cancellation, DTMF, and tone sender are also located in the media gateway.

Media Gateway Controller which provides the call control and signaling functionality. Communication between media gateways and Call Agents is achieved by means of protocols such as MGCP or Megaco(H.248) or Session Initiation Protocol (SIP). Modern media gateways used with SIP are often stand alone units with their own call and signaling control integrated and can function as independent, intelligent SIP end points. Voice over Internet Protocol (VoIP) media gateways perform the conversion between TDM voice to a media streaming protocol (usually Real time Transport Protocol, RTP), as well as a signaling protocol used in the VoIP system. Mobile access Media Gateways connect the radio access networks of a public land mobile network PLMN to a Next Generation Core network.

Media Gateway Definition

A Media Gateway acts as a translation unit between disparate telecommunications networks such as PSTN; Next Generation Networks; 2G, 2.5G and 3G radio access networks or PBX. Media Gateways enable multimedia communications across Next Generation Networks over multiple transport protocols such as ATM and IP. VoIP Media Gateways perform the conversion between TDM voice, to VoIP.

As the Media Gateway connects different types of networks, one of its main functions is to convert between the different transmission and coding techniques. Media streaming functions such as echo cancellation, DTMF, and tone sender are also located in the Media Gateways. Media Gateways are controlled by a Media Gateway Controller which provides the call control and signaling functionality. Communication between Media Gateways and Call Agents is achieved by means of protocols such as MGCP, MEGACO/H.248 or SIP.

Media Gateway Synonyms

VoIP Gateway; Voice Gateway; VoIP Media Gateway; PSTN Gateway, MGW; Voice IP Gateway; VoIP SIP Gateway; SIP VoIP Gateway; VoIP Telephone Gateway; VoIP Telephony Gateway; VoIP to PSTN Gateway; Access Gateway VoIP; Gateway Voice over IP; VoIP Gateways; Gateway VoIP; VoIP Internet Telephony Gateway

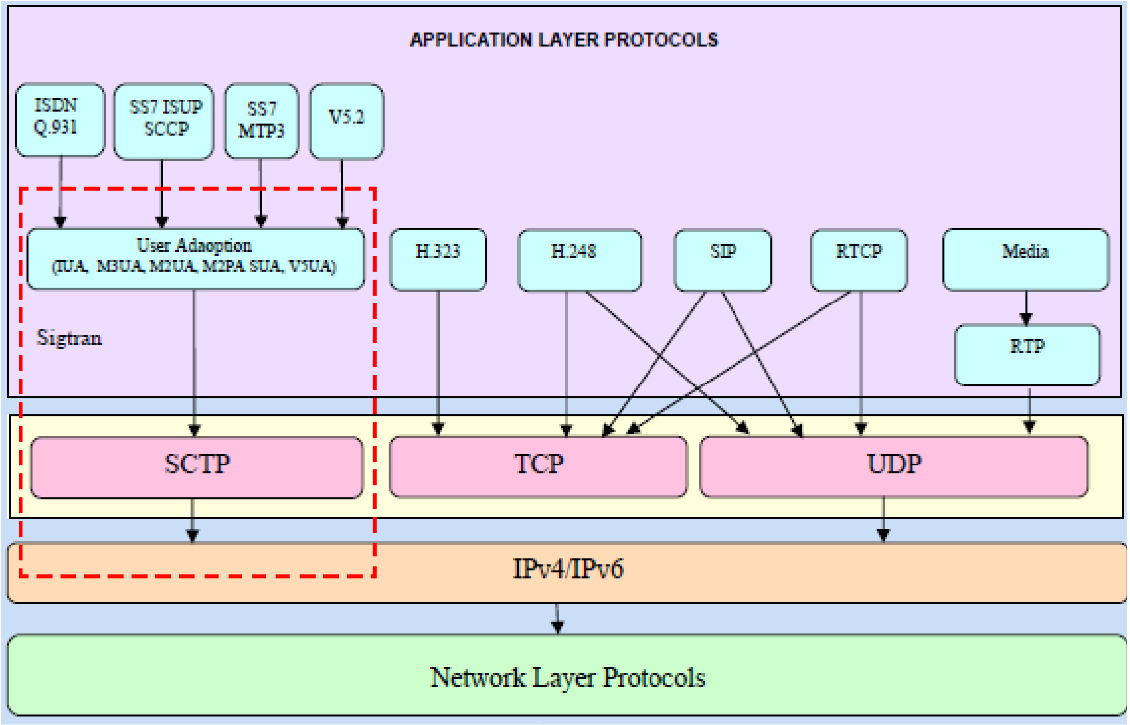


Fig. NGN Protocols

The figure shows the control and media streams in NGN environment. The media streams consist of audio, video or data, or a combination of any of them. Media stream conveys user or application data (i.e., a payload) but not control data. It is transported through RTP/RTCP. Control signaling messages are transported by control streams using signaling protocols like SIGTRAN, H.248, H.323, SIP etc.

H.323

H.323 is an ITU Recommendation that defines "packet based multimedia communications systems." It defines a distributed architecture for creating multimedia applications, including VoIP. The H.323 protocol is best known as the original call signaling protocol that made real time voice and video over IP possible. Being the first solution to work, H.323 is the most widely deployed protocol in the market.

SIP Session Initiation Protocol

SIP is an application layer control protocol for multimedia communication over IP network. It is used for creating, modifying and terminating two party sessions, multiparty sessions and multicast sessions. These sessions include audio, video and data for multimedia conferences, instant messaging, Internet telephone calls, distance learning, telemedicine, multiparty real time games etc.

Sip defines telephone numbers as URLs (Uniform Resource Locators), so that web pages can contain them. This allows a click on a link to initiate a telephone call. These addresses take the form of user@host, similar to email addresses. The user part, which is left of the “@” sign, may be user name or a telephone number and host part, which is right of the “@” sign, is a domain name or IP address. SIP addresses may be obtained out of band, learned via media gateways, recorded during earlier conversations, or guessed (since they're often similar to email addresses. SIP may be used in conjunction with other call setup & signaling protocols and has a verity of other features like caller reach ability, call screening, encryption and authentication etc.

MGCP Media Gateway Control Protocol

(MGCP) is a control protocol that uses text or binary format messages to setup, manage, and terminate multimedia communication sessions in a centralized communications system. This differs from other multimedia control protocol systems (such as H.323 or SIP) that allow the end points in the network to control the communication session. MGCP is specified in RFC 2705. MGCP is, in essence, a master/slave protocol, where the MGs are expected to execute commands sent by the MGCs.

H.248

H.248 is an ITU Recommendation that defines 'Media Gateway Control Protocol'. It is the result of a joint collaboration between the ITU and the IETF. It is also referred to as IETF RFC 2885 (MEGACO), which defines a centralized architecture for creating multimedia applications, including VoIP. In many ways, H.248 builds on and extends MGCP. It is used as a media gateway control protocol between a Media Gateway Controller (MGC) and a Media Gateway (MG). The ITU T, the IETF, the International Soft switch Consortium (ISC), and other standardization organizations are optimizing the H.248 protocol currently. Telecommunication equipment vendors are investing much in the development and application of the H.248 protocol. Compared to the MGCP protocol, the H.248 protocol is more flexible and can support more types of access technologies and mobility of terminations.

4. IP MULTIMEDIA SUBSYSTEM (IMS)

The IP Multimedia Subsystem (IMS) is a global, access independent and standard based IP connectivity and service control architecture that enables various types of multimedia services to end users using common Internet based protocols. IMS is envisaged to be the heart of NGN.

IMS allows applications in IP enabled devices to establish peer to peer and peer to content connections easily and securely. Once established, the IP connection can be used to exchange all types of communication media, including voice, video, content and more. The IMS provides a full suite of network capabilities for authentication of clients, network to network interfaces and administrative functions such as charging. SIP is a signaling protocol that handles the setup, modification and tear down of multimedia sessions and RTP provides transport of media streams.

Understanding Network Protocols

A protocol is a standard by which communication takes place between network devices. The following white paper attempts to explain in the simplest terms the protocols used by your Iomega network device.

SUMMARY

- NGN supports transportation of multi format data across the network.
- NGN offers multi services to the users, like IPTV, VoD and Video conferencing.
- NGN consists of three layers, viz, access layer, transport layer and control layer.
- NGN offers seamless connectivity the users.

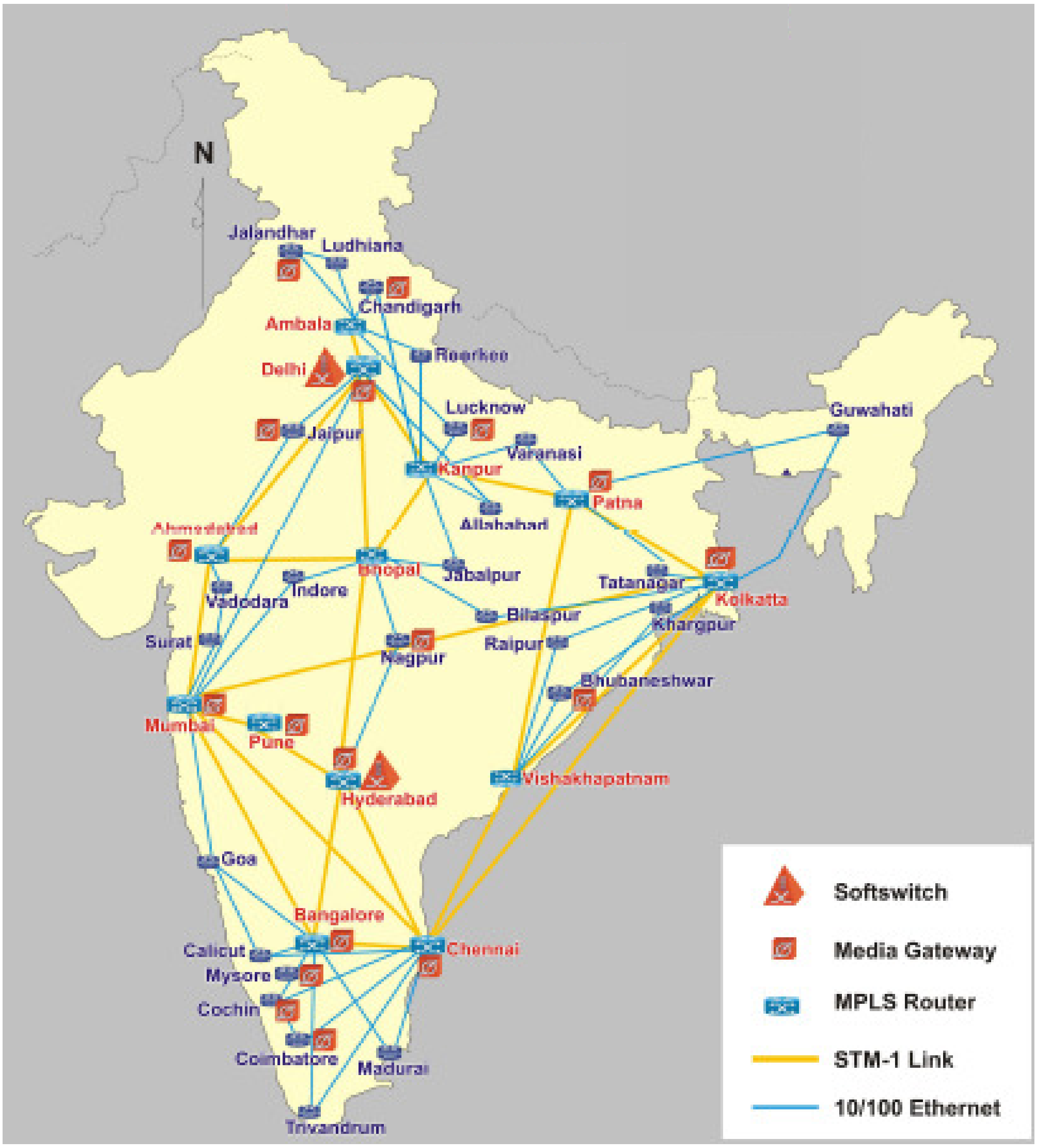


Fig. Railtel MPLS Network

CHAPTER 6

DIALOGIC® CONTROLSWITCH™ SYSTEM

Programmable Soft switch and Service Delivery Platform

The Dialogic® Control Switch™ System is an IP soft switch that provides a smooth migration path from existing TDM voice networks to the Next Generation Network/IP Multimedia Subsystem (NGN/IMS) by enabling the interconnection of a mix of traditional and IP based voice networks. The Control Switch System is built around an advanced modular, programmable, distributed, highly scalable, and high availability architecture with open interfaces to media devices, application servers, and back office systems.

Features

- Seamless connectivity between TDM, VoIP, and IMS networks, enables convergence of disparate networks and multi protocol support.
- Supports network wide deployments.
- Geographic redundancy Provides high availability and disaster recovery.
- Integrated security solution Allows secure VoIP interconnects.
- Gateway Mobile Switching Center (MSC) functionality Enables optimal routing in environments that include wireless networks.
- Designed to avoid forklift upgrades Provides investment protection.

Handling Packet Protocols

The ability of the Control Switch System to mediate between various packet protocols (such as MGCP, H.323, SIP, and H.248) and global PSTN signaling protocols (SS7, PRI, CAS R1/R2) and variants gives service providers the flexibility to fully utilize existing resources and deliver a wide variety of enhanced services via any type of network. Additionally, Dialogic provides a gradual migration strategy that leverages existing service investment and provides a clear path to an all IP based IMS network.

Deploying New Services on a Single Platform

The open standards, multi protocol, multi services Control Switch System platform enables new services to be implemented dynamically throughout the entire network; that is, service providers can deploy new services and solutions without the overhead of running multiple disparate networks or incurring downtime to reconfigure the network. Additional processing capacity is added using Common Off the Shelf (COTS) computing platforms. The Control Switch System includes a service delivery platform based on programmable, configurable, and dynamic loading of XML service scripts. This empowers customers to design, develop, deploy, activate, and tailor their service offerings on the fly, thus gaining control of their market differentiation. The rapid creation of a wide range of differentiated enhanced services can be delivered from both the Control Switch System and third party application servers.

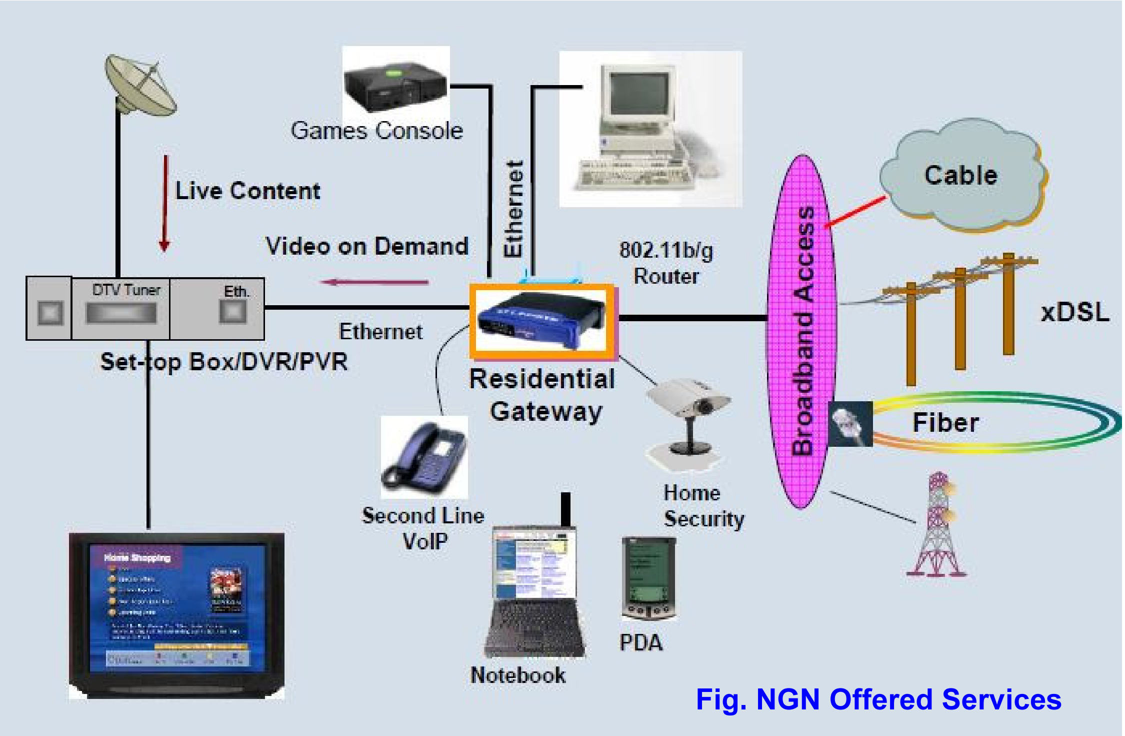


Fig. NGN Offered Services

A Multi Tiered Reference Model with a Single Point of Management

The Control Switch System provides an unparalleled solution set for meeting the requirements of the next generation multi tiered reference model. The Control Switch System design allows for high scalability in granular increments yielding an optimized solution for both initial and large scale deployments. For instance, service providers can choose to centralize system management, billing subsystem, service logic, and routing, and distribute call control and signaling to various regional centers. In this way, an additional investment to support traffic growth is aligned with revenue growth without confronting scalability limits. Regardless of the distribution of Control Switch System elements across multiple locations, Dialogic provides a single point of management for configuration, provisioning, and system monitoring, including real time alarms, performance statistics, and traffic reports. In addition, the Control Switch System provides a single view of Call Detail Records (CDR) and provides end to end call tracing as an invaluable troubleshooting tool. Various elements of the Control Switch System can be distributed geographically for scaling and redundancy a primary element may be located in a city and can be backed up by the secondary element located in a different switching center even in a different city.

Open and Flexible Solutions

The Control Switch System has proven openness at all interface layers to enable service providers to rapidly interoperate with new vendors of media hardware and application servers. Additionally, the Control Switch System is a core element in solutions that incorporate products from Dialogic partners. Dialogic offers numerous field deployed solutions interoperable with specialized products from its partners. Therefore, service providers can quickly exchange traffic with other service providers and deploy services from Dialogic and its partners to increase their revenue.

Real Time Collection of Detailed Statistics

The Control Switch System incorporates the real time collection of detailed statistics used for VoIP traffic prioritization and bandwidth utilization control. The network and application layer statistics collection system in combination with the Policy Engine enable advanced Quality of Service (QoS) Management and Service Level Agreements (SLAs) design. SLAs can be customized per customer, per interconnection partner, per service, etc. The QoS element enables carriers network wide and in real time to automatically obtain feedback and take corrective action to maintain custom SLAs.

Dashboard Functionality

The Control Switch element management system offers a dashboard into the service provider's network. However, for service providers with a large investment in existing back office systems including provisioning, billing, and network operations, the Control Switch System offers many open interfaces including PL/SQL and XML for provisioning, SNMP for network management and text based CDRs for billing. Control Switch can also be deployed with back office traffic monitoring systems that require call status tracking in real time. Alternately, this application can also be used by operators wishing to record traffic patterns in real time.

Security Features

The Control Switch System provides security features to enable service providers to prevent malicious attacks on their network and ensure that their customers' assets are fully protected. These features include topology hiding to hide internal network and customer details, access control lists, and "denial of service" attack prevention, and far end and near end NAT traversal to avoid NAT/Firewall complications.

Specific Economic and Functional Requirements

Based on its open architecture, the Control Switch System provides ubiquitous, simultaneous multi function capability across a broad range of applications. Because the call control and application elements of the Control Switch System are independent from the actual switching hardware, solutions deployment and implementation can be tailored according to a service provider's specific economic and functional requirements. This represents a significant departure from traditional solutions that employ embedded control and applications software with limited flexibility. The Control Switch System is a fundamental component of Dialogic IMS compliant solution, which enables the coexistence of legacy and IP networks and flawless migration of service provider customers to a full IMS NGN.

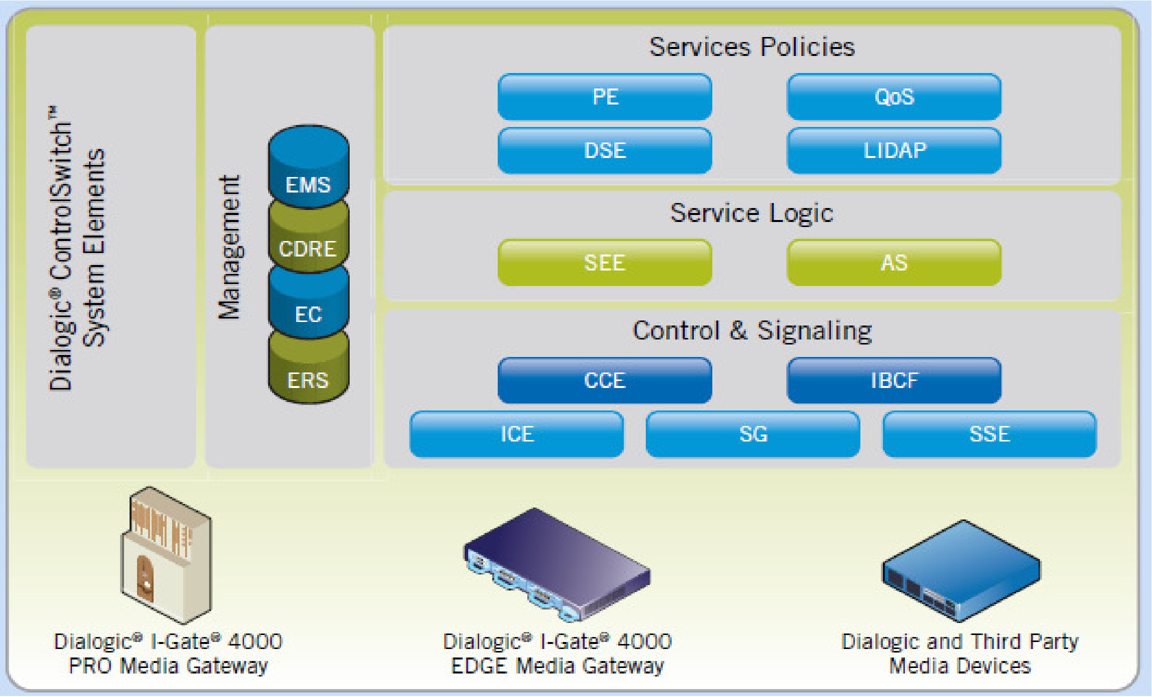

Dialogic® ControlSwitch™ System Elements
Management
EMS
CDRE
EC
ERS
Services Policies
PE
QoS
DSE
LIDAP
Service Logic
SEE
AS
Control & Signaling
CCE
IBCF
ICE
SG
SSE
Dialogic® I-Gate® 4000 PRO Media Gateway
Dialogic® I-Gate® 4000 EDGE Media Gateway
Dialogic and Third Party Media Devices

Fig. Dialogic Control Switch Block Diagram

Dialogic® Control Switch™ System Elements

The Control Switch System is a multi tiered, highly scalable, distributed software system that executes on commercial Oracle servers, interconnected over an underlying IP data network. A service provider can elect to start with a small system and grow it to a very large one, spanning multiple geographic centers, by adding components as the traffic and end user volume increase. At a high level, the Control Switch System can be described as a distributed, IP network based system providing traditional switch functions of call control, call routing, signaling gateway, and media device control in addition to back office functions in support of provisioning, billing, and network operations.

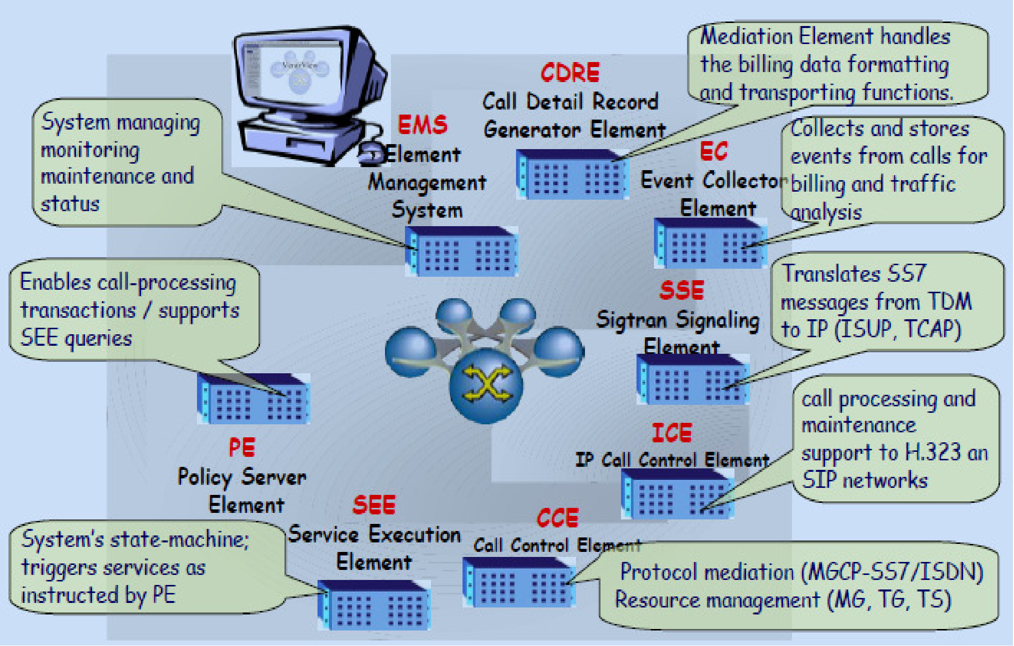

Mediation Element handles the billing data formatting and transporting functions.
CDRE
Call Detail Record Generator Element
System managing monitoring maintenance and status
EMS
Element Management System
EC
Event Collector Element
Collects and stores events from calls for billing and traffic analysis
Enables call-processing transactions / supports SEE queries
SSE
Sigtran Signaling Element
Translates SS7 messages from TDM to IP (ISUP, TCAP)
PE
Policy Server Element
ICE
IP Call Control Element
call processing and maintenance support to H.323 an SIP networks
SEE
Service Execution Element
CCE
Call Control Element
System's state-machine; triggers services as instructed by PE
Protocol mediation (MGCP-SS7/ISDN)
Resource management (MG, TG, TS)

Fig. Dialogic Control Switch Elements

Element Descriptions

1. Element Management System (EMS)

The EMS provisions all Control Switch System components and enables the modular and distributed network solution to be easily managed from a single switch. It proactively monitors the status of the system's elements. It provides call tracing, diagnostics, performance statistics, traffic reports, and browsing of call detail records stored in the CDR manager.

2. CDR Element (CDRE)

The CDRE is responsible for the Control Switch System billing and data analysis functions. It centralizes the billing data formatting and transport functions. The CDRE is responsible for generating one single billing record for one call.

3. Events Collector (EC)

The EC collects and stores billing and call related events from the various Control Switch System elements for subsequent processing of reports and CDRs.

Event Relay Server (ERS)

The ERS enables the Control Switch System to integrate with the third party Operational Support Systems (OSS) such as event monitoring applications and fraud management systems in a deployed Control Switch System network. It relays events in real time to the clients in an open and standard XML format for ease of integration with the customized event processing and monitoring applications.

4. Policy Element (PE)

The PE delivers unmatched flexibility with policies combining approximately a hundred and sixty parameters. It responds to service policy queries with treatments based on a database of provisioned policies. It supports a growing variety of service policies including routing, screening, announcement, IN service triggers, QoS, registration, and authentication. Its customized policy creation and provisioning are GUI based and a real time in memory hierarchical database enables an extremely high throughput.

Quality of Service (QoS) Server

The QoS Server provides a mechanism for feedback based reporting and routing to assure service and guarantee SLAs. It monitors pre established concurrent calls and imposes limitations based on Trunk Groups, Prefixes, Customer Interaction Center (CIC), and Telephone and Networking Services (TNS).

Directory Service Engine (DSE)

The DSE provides support for directory lookups and number translations natively via an optimized large directory query solution. For large directory applications such as Local Number Portability (LNP) or carrier ENUM, the DSE can scale up to four hundred million entries.

Legal Intercept Data Access Point (LIDAP)

The LIDAP performs legal interception provisioning functionality. It communicates with a mediation device for the assignment of target information into a database and replies to queries from the Service Execution Element (SEE) to determine whether the call will be tagged for interception or not.

5. Service Execution Element (SEE)

The SEE allows for the rapid delivery of enhanced user services. Because it operates as a protocol agnostic engine, the SEE enables service creation, regardless of the underlying framework. The SEE executes the service logic within the Control Switch System and can serve as a service broker when coordination is required across multiple external application platforms. Flexible adapters enable SEE services to combine resources residing in Control Switch System elements as well as external application systems such as Intelligent Network (IN) systems and SIP based application servers. Rapid services creation, deployment, and activation are enabled via XML scripting. SEE is based on the Services Logic Execution Environment (SLEE) and is developed in C++. Some of the services provided are announcements, postpaid, account codes, toll free, collect call, IVR services, and IN services.

Application Server (AS)

Value added services can be implemented easily and quickly via third party application servers or natively via the Control Switch System SEE. Value added services (such as calling cards [prepaid/postpaid/travel], conferencing, call center, messaging, VoIP VPN, account codes, premium number with IVR, call block, collect call) are in service today on the Control Switch System.

6. Call Control Element (CCE)

The CCE supports protocol specific call control and protocol mediation between PSTN facing (SS7/C7, ISDN PRI, CAS) and generic call processing protocols and resource management (Trunk Gateways [TGs], channels, Gateways [GWs]) using MGCP/H.248.

Interconnect Border Control Function (IBCF)

The IBCF enables global carrier IP peering, protects the carrier network against malicious attacks, and provides key security features including topology hiding, access control lists for “denial of service” attack prevention, and far end and near end Network Address Translation (NAT) traversal to avoid NAT/firewall complications.

7. IP Call Element (ICE)

The ICE supports SIP and H.323 protocol specific processing, protocol mediation between VoIP protocols (SIP and H.323), Control Switch System generic call processing protocols, resource management (IP Trunk Groups, IP Gateways, Gatekeepers), and SIP I and SIP T protocols.

Distributed Signaling Gateway (DSG)

The DSG, built on the Dialogic® I Gate® 4000 EDGE Media Gateway, allows the Control Switch System to connect to the SSP, STP, and SCP resources of the SS7/C7 network for PSTN call signaling and for intelligent networking services.

8. SIGTRAN Signaling Element (SSE)

The SSE supports MTP level 3 User Adaptation (M3UA) that is defined within the SIGTRAN protocol suite. It uses the Stream Control Transport Protocol (SCTP) and Internet Protocol (IP) as its underlying transport, enables service providers to take advantage of the IP transport network, and offers additional features.

Features

Service Policies

- Highly flexible, policy based routing engine
- Rapid development and deployment of customized policies
- Multi tiered routing
- Multiple numbering plans: international, national, and private
- Advanced call screening
- Re routing/route advance
- Virtual Private Networks support
- Combination of TDM and IP routes
- Over 160 routing/screening parameters
- Signaling attributes
- System attributes
- Dynamic attributes
- Other Service Policies
- account codes, personal pin, security pin, and authentication

Security

Provides security and NAT functions for signaling and media planes Offers defenses against Denial of Service (DoS) and other IP layer attacks Supports all H.323 and SIP peering traffic Network wide scalability Resides in the network core or in distributed Points Of Presence (POP) as per service provider needs.

Technical Specifications

Service Level Assurance/QoS

Real time event/statistics driven routing and policy enforcement.

Programmable concurrent calls limitation and monitoring.

ASR/ACD based routing.

Statistics database and report.

Directory Services

Supports directory lookups and number translations natively.

Scales up to 400 million entries.

Legal Intercept

Provides mediation device with two interfaces.

TDM based loop via the Third Party Mediation Device for call delivery.

IP based interface for provisioning of interception targets.

Element Management

Unified management of distributed systems.

Web based GUI with local and remote interfaces.

End to end real time call tracing capabilities for both PSTN and VoIP signaling.

Dynamic modification to parameters during operation.

Circuit switch COT test support.

Configuration and provisioning of all Control Switch System elements, SS7 network parameters, trunk groups, media gateway parameters, routing policies, and dial plans.

Fault management

Control Switch System alarm management, media gateway alarm management, network element monitoring, and SS7 monitoring and audit reports.

CDR Generation and Searching

FTP transport, text based CDR, BAF format, Flexible CDR Query.

Generates text based CDRs for billing mediation systems.

Raw call events for billing and traffic analysis.

Configurable persistent storage for call event data.

Generates Bellcore AMA Format (BAF) CDRs.

Coexistence with Open Settlement Protocol Clearinghouse.

Event Collection and Relay

Collects and stores billing and call related events and QoS statistics.

SLAs established per customer, per interconnection partner, per service, etc.

Easing the integration with the customized event processing.

Monitoring and fraud management applications, etc.

Protocol Support

MGCP, H.248, ANSI/ITU/ETSI ISUP, AIN/INAP/MAP, ISDN Q.931 (PRI): NI 2 and ETSI SIP, H.323, SIGTRAN, SCTP, M3UA and IUA, CAS (E&M, R1.5, R2), CAS MF and DTMF, SNMP and OSP.

Recommended Platform

NEBS Level 3 compliant Sun Netra platforms running Sun Solaris operating system.

Software runs on other SUN platforms running Sun Solaris operating system.

Approval Compliances and Standards

ITU, ANSI, ETSI, IETF, TISPAN, IMS and MSF.

Installation and Configuration

Pre loaded and preconfigured on the system.

Scalability and Performance

Scales to five million Busy Hour Call Attempts (BHCAs) across multiple media gateways on a SUN platform distributed, modular architecture provides scalability through addition of SUN platforms.

Fault Tolerance and Reliability

Automatic failover of any Control Switch System element to active backups distributed on one or more machines. Auto diagnostic and recovery mechanisms for any hardware, software, signaling link, or network fault. SCTP Protocol for messaging between Control Switch System elements and network level redundancy. Events collector and CDR Manager disk mirroring. High availability. Geographic redundancy. Routing database replication. CPU overload protection. SS7 link redundancy.

Call Processing

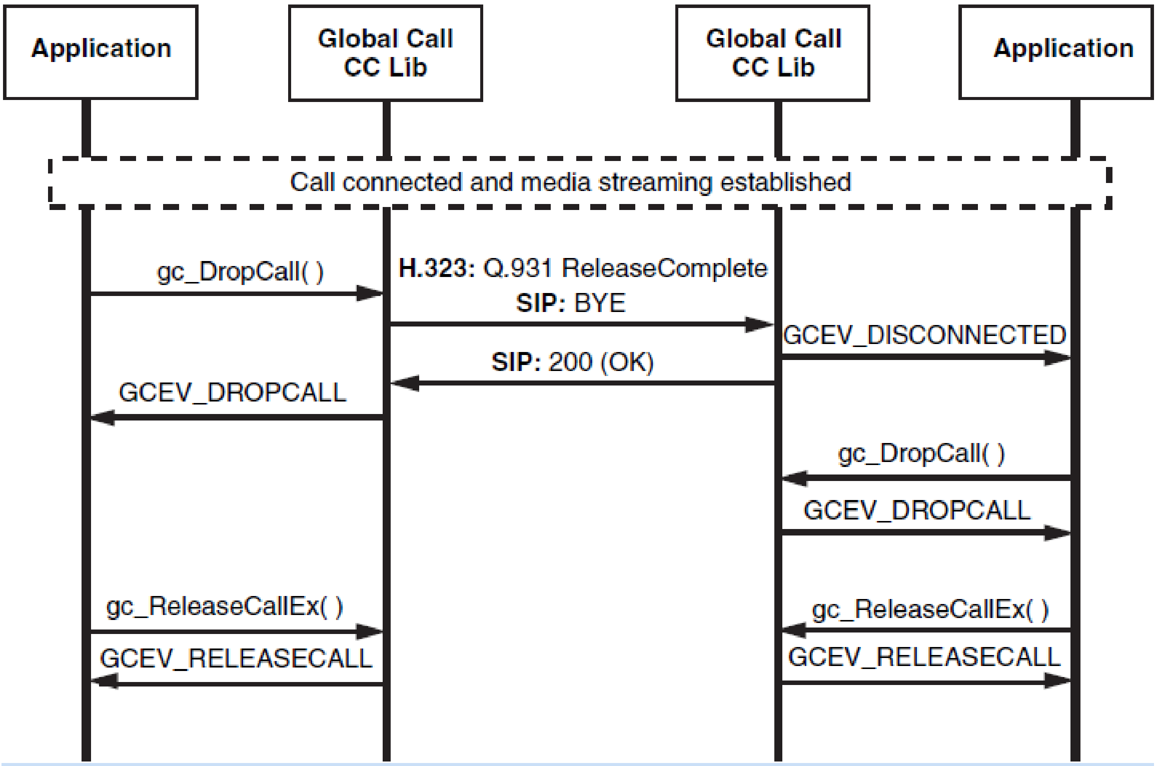


Fig. Call Process Sequence

Call Setup Scenarios for Early Media

When using IP technology, the establishment of RTP media streaming is normally one of the final steps in establishing and connecting a call. This is in contrast to the public switched telephone network (PSTN), where call progress signaling is commonly provided to the calling party via audible, in band call progress tones, such as ring back, busy signal, and SIT tones. When implementing a VoIP gateway, it often imperative to initiate media (RTP) streaming from the local endpoint to the calling party before the call is connected. This capability is commonly referred to as early media.

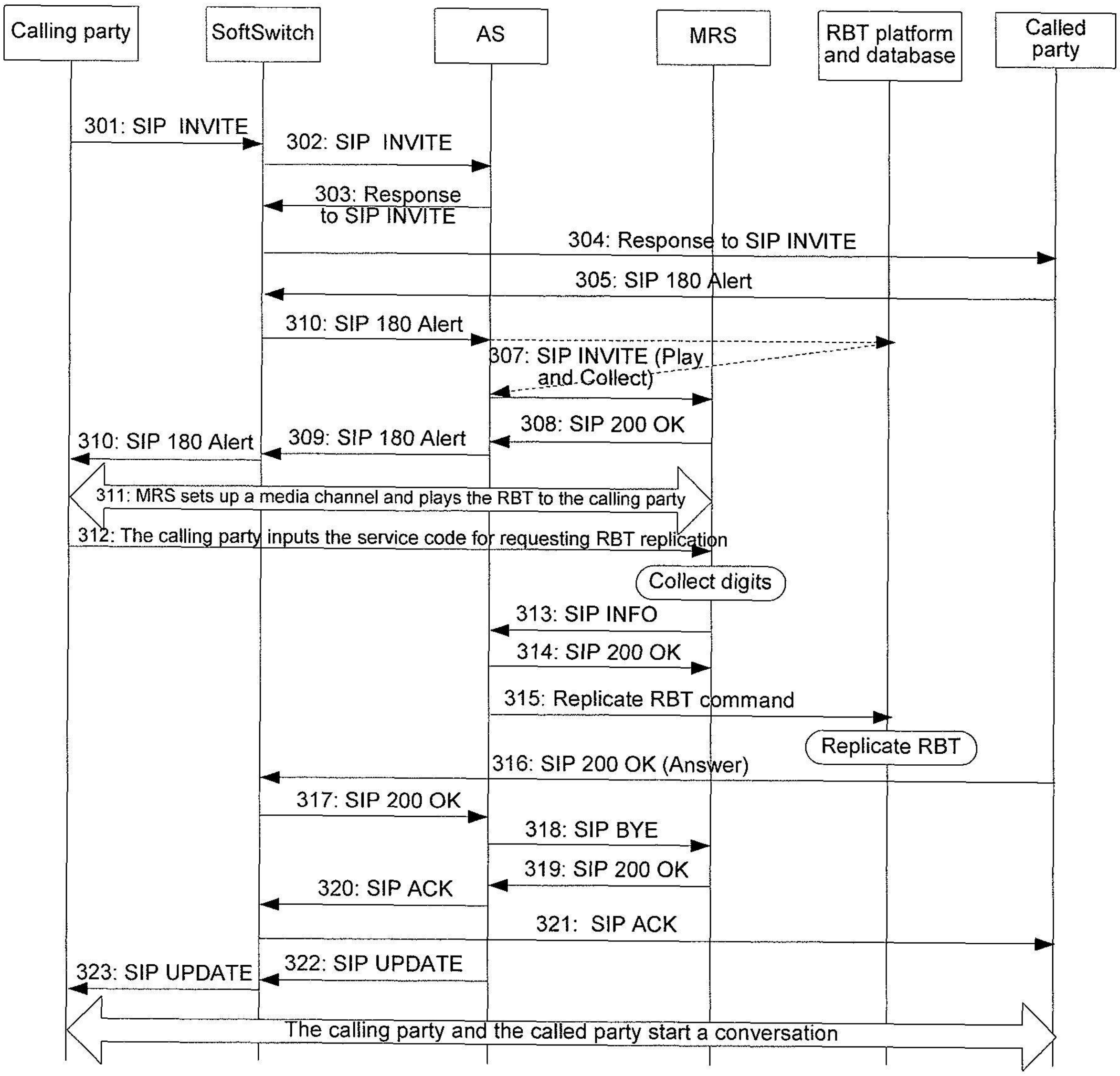

Calling party
SoftSwitch
AS
MRS
RBT platform and database
Called party
301: SIP INVITE
302: SIP INVITE
303: Response to SIP INVITE
304: Response to SIP INVITE
305: SIP 180 Alert
310: SIP 180 Alert
307: SIP INVITE (Play and Collect)
308: SIP 200 OK
310: SIP 180 Alert
309: SIP 180 Alert
311: MRS sets up a media channel and plays the RBT to the calling party
312: The calling party inputs the service code for requesting RBT replication
Collect digits
313: SIP INFO
314: SIP 200 OK
315: Replicate RBT command
Replicate RBT
316: SIP 200 OK (Answer)
317: SIP 200 OK
318: SIP BYE
319: SIP 200 OK
320: SIP ACK
321: SIP ACK
323: SIP UPDATE
322: SIP UPDATE
The calling party and the called party start a conversation

Fig. SIP Call Process Sequence

The Global Call IP call control library automatically enables media streaming at the earliest possible point in the pre connect process. This is generally the earliest point at which the remote endpoint provides the remote RTP/RTCP transport addresses and media capabilities. The precise point at which media can be enabled is dependant on a large number of factors, and the following figures illustrate some common best case scenarios. Each figure illustrates the Dialogic® Global Call API library’s behavior from the application’s perspective, either in the calling party role or in the called party role.

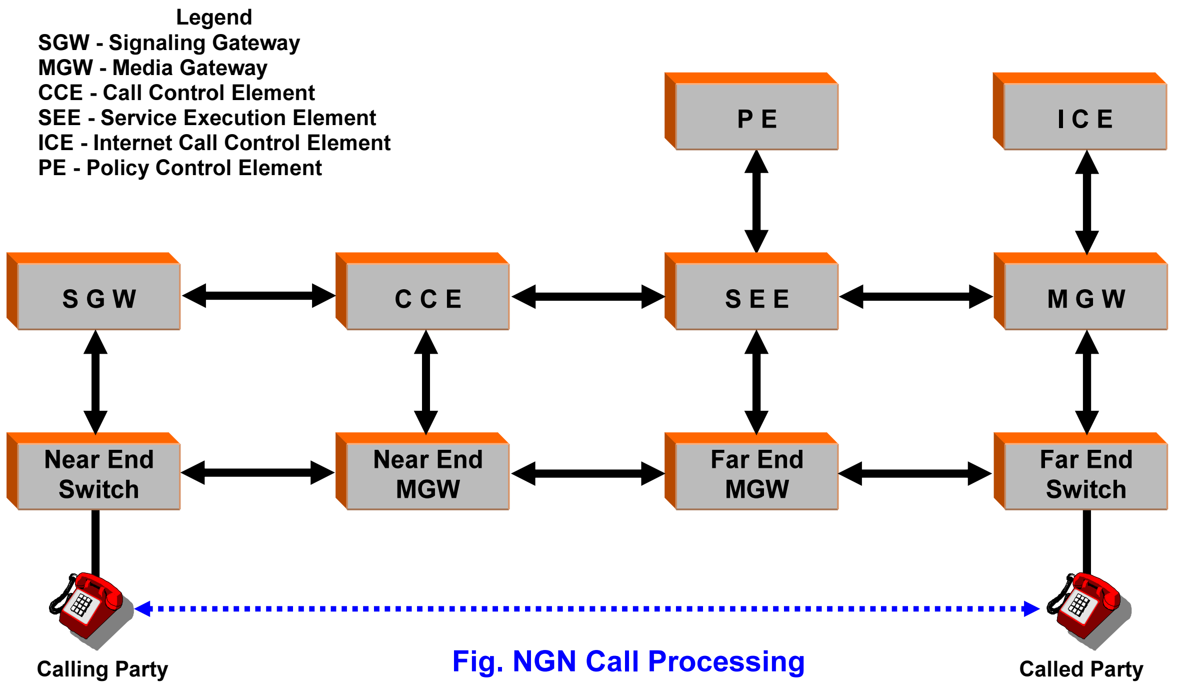


Fig. NGN Call Processing

Virtual Mesh Tandem Switching

The market for mobile voice services is characterized by growth and constant churn in the customer base. To support this, wholesale network service providers and/or wireless service providers need to frequently add tandem switching and trunk capacity to connect new and existing Mobile Switching Centers (MSCs) and Gateway MSCs (G MSCs) with each other. The investment required by traditional TDM solutions to support this need is disproportionately high and is not realistically sustainable in a market with declining prices and margins. The Control Switch System provides a next generation solution to this problem by delivering a highly efficient, distributed "virtual mesh" tandem switching solution, along with substantial bandwidth savings and toll quality voice over packet networks.

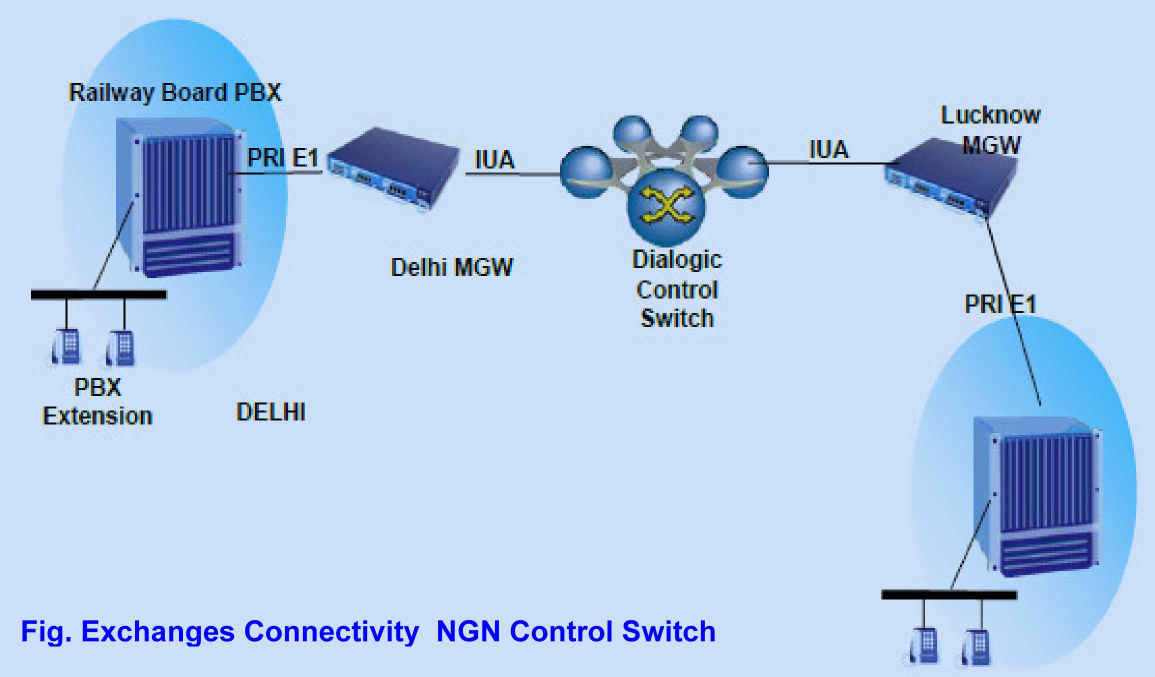


Fig. Exchanges Connectivity NGN Control Switch

5. CONCLUSION

With the gradual evolution towards NGNs, the time and direction of change will have to be regulated with well defined specifications and with NGN legacy threshold point. Service providers are making strategies to begin rolling out NGN based networks to take advantage of fast & flexible service creation and provisioning capabilities, while also providing for legacy networking and combinational services that make use of most of the existing investments. Operators can then build networks toward the all IP vision offering rich multi access multimedia services.

IMS provides business focused evolution options for delivering attractive, easy to use, reliable and profitable multimedia services. It also enables operators to achieve Fixed Mobile Convergence (FMC).

IP/ISDN Telephone Exchanges Network On OFC Over Secunderabad Division Of SCRly

Secunderabad division has introduced VoIP telephone system by using Softswitch. Tadiran Telecom make Sea Soft Switch is installed and commissioned in Test Room/ Secunderabad to enable to extend auto telephones on VoIP technology to each and every way station in SC division. This VoIP integrates with the other services available with internet, like video, message transfer etc. The VoIP services are fully secured.

The VoIP installed in SC division consists of the following equipments:

1. Tadiran made Sea Soft Switches.
2. Allied Tellisis made Core Routers AR 745
3. Allied Tellisis made Edge Routers AR 750
4. Grand stream made FXS Gateways

All the above equipments are connected with e 1 in OFC transmission in ring topology for full redundancy.

Soft Switch: This is a DELL Server working on Linux platform with Internet Protocol. Manufactured by M/s Tadiran Telecom, Israel, this is supplied and installed by M/S BPL Telecom. The Soft Switch is connected to the Core Router via Ethernet port. Soft Switches provision in other locations in ring will provide total redundancy. Due to this, OFC communication failure shall not interrupt any Soft Switch functionality. By using the soft switch with IP, the band width can be utilized efficiently. 20,000 subscribers may be configured, but presently 600 subscribers' authorization is available in soft switch. 300 no. of telephones will be extended to way stations of the SC division, which are programmed and stored in the soft switch. The Soft Switch in SC Test Room will be connected to Rail Nilayam Exchange through IP Universal gate way with IP authorization. This works on 230 V AC supply. The NMS associated with the soft switch will be utilized for programming and fault diagnostics.

Core Router: The core routers are provided at 13 ISDN exchange locations. All the core routers are connected in ring topology. The core routers provide connection to all edge routers. These core routers are integrated with ISDN exchanges and work on 230 V AC power supply. These 13 number of core routers are installed and commissioned at the following locations:

1.Test Room/SC 2. Hyderabad 3.Sanatnagar 4.Vikarabad 5.Kazipet 6.Warangal 7. Dornakal 8.Madhira 9.Bhadrachalam Road 10. Ramagundam 11.Bellampalli 12.Sirpurkaghaznagar 13.Manikgarh14. Bidar

Edge Routers: Edge Routers will be provided at 70 way stations to enable to connect the FXS Gate Ways at the required locations. At present 67 way stations are provided with 67 number of edge routers. All the way side telephone equipments are located in the corresponding OFC shelter. These edge routers are connected in serial connection. The edge routers works on 48 V DC.

FXS GATE WAYS: To extend an auto telephone in remote location from Soft Switch, FXS Gate Way is required and located along with the edge router at the way station location. The connectivity between Edge Router and FXS Gate Way is through Ethernet. The FXS gate way has 4 to 24 ports. The functionality of the FXS Gate Way can be monitored from NMS of the Soft Switch since the IP address of the FXS gate Way is registered in the soft switch. The first port of the FXS gate way is allotted for way station auto telephone. Subsequently, the other ports will be allocated to the required offices at the way station. This FXS Gate Way works on 230V AC and 48/12 V DC. Through this gate way, a simple auto phone or VoIP telephone can be provided. As on today, 181 number of auto telephones are extended from FXS gate ways at 67 way stations in the division.

PRI Connectivity: All the ISDN Telephone exchanges and Soft Switches are networked on IP/PRI trunking. At present the exchanges are connected with IP trunking with PRI back up. Soft Switch to Rail Nilayam exchange connectivity will be with Universal Gate Way card and the PRI connectivity between Rail Nilayam exchange and the 4 important exchanges i.e, KZJ,BPA,DKJ & VKB , are provided for back up during link failure or busy hour traffic. The telephone exchanges in SC division comes under the unified numbering scheme of 80000 to 82999, which provides the access of other exchange numbers with out dialing any access codes.

GLOSSARY

3GPP2	Third Generation Partnership Project 2
ACK	Acknowledgement
ADC	Analog To Digital Converter
ADM	Adaptive Delta Modulation
ADPCM	Adaptive Differential Pulse Code Modulation
ADSL	Asymmetric Digital Subscriber Line
AGI	Asterisk Gateway Interface
AGW	Access Gateway
AN	Access Node
AP	Access Point
API	Application Programming Interface
AS	Application Server
ASAP	As Soon As Possible
ATA	Analog Telephone Adaptor
ATM	Asynchronous Transfer Mode
BAS	Broadband Access Server
BICC	Bearer Independent Call Control
BRI	Basic Rate Interface
CAPEX	Capital Expenditure
CATV	Cable Television
CCF	Call Control Function
CDMA	Code Division Multiple Access
CME	Circuit Multiplication Equipment
CODEC	Compression / De compression
CS ACELP	Conjugate Structure Algebraic Code Excited Linear Prediction
CPE	Customer Premises Equipment
DAC	Digital To Analog Converter
DFFSERV	Differentiated Services
DNS	Domain Name System
DoS	Denial Of Service
DPCM	Differential Pulse Code Modulation
DS	Denial Of Service
DSL	Digital Subscriber Line
DSLAM	Digital Subscriber Line Access Multiplexer
DTH	Direct To Home
EDGE	Enhanced Data Rates for GSM Evolution
ETSI	European Telecommunications Standards Institute
FTP	File Transfer Protocol
FTTH	Fiber To The Home
FXO	Foreign Exchange Office
FXS	Foreign Exchange Subscriber
GPL	General Public License
GPRS	General Packet Radio Service

GSM	Global System for Mobile Communication
GW	Gateway
HTTP	Hyper Text Transfer Protocol
HTTPS	Hyper Text Transfer Protocol Secure
IDS	Intrusion Detection System
IETF	Internet Engineering Task Force
IIS	Internet Information Services
iLBC	Internet Low Bitrate Codec
IMS	IP Multimedia Subsystem
IN	Intelligent Network
INAP	Intelligent Network Application Part
INTSERV	Integrated Services
IP	Internetworking Protocol
IPS	Intrusion Prevention System
IPTN	IP Telephony Network
IPTV	Internet Protocol Television
ISDN	Integrated Services Digital Network
ISP	Internet Service Provider
ISUP	ISDN User Part
ITSP	Internet Telephony Service Provider
ITU	International Telecommunications Union
IUA	ISDN User Access
IVR	Interactive Voice Response
JAIN	Java API for Integrated Networks
LAN	Local Area Network
LEX	Local Exchange
LMC	Last Mile Connectivity
LMDS	Local Multipoint Distribution System
LSP	Label Switched Path
MEGACO	Media Gateway Control (an IETF Workgroup)
MGCP	Media Gateway Control Protocol
MGW	Media Gateway
MoH	Music On Hold
MOS	Mean Opinion Score
MP3	MPEG Audio Layer 3 Encoding Standard
MPEG	Motion Picture Expert Group
MPLS	Multi Protocol Label Switching (an IETF W.G.)
MUX	Multiplexing
NACK	Negative Acknowledgement
NAS	Network Access Server
NAT	Network Address Translation
NGN	Next Generation Network
NIC	Network Interface Card
NT	Network Termination

OPEX	Operational Expenditure
OSA	Open Service Access
OSI	Open Systems Interconnection
PABX	Private Automatic Branch Exchange
PC	Personal Computer
PCM	Pulse Code Modulation
PDA	Personal Digital Assistant
PDH	Plesiochronous Digital Hierarchy
PINT	PSTN Internet Interworking
PKI	Public Key Infrastructure
PoP	Point Of Presence
PoS	Point Of Sale
POTS	Plain Old Telephony Service
PRI	Primary Rate Interface
PSTN	Public Switched Telephone Network
QoS	Quality of Service
RFC	Request For Comments
RGW	Residential Gateway
RSVP	Reservation Protocol
RTCP	Real time Transmission Control Protocol
RTP	Real time Transport Protocol
SCCP	Signaling Connection Control Part
SCN	Switched Circuits Network
SCP	Signaling Control Point
SCTP	Stream Control Transmission Protocol
SDH	Synchronous Digital Hierarchy
SIGTRAN	Signaling Transport (an IETF W.G, PSTN over IP))
SIP	Session Initiation Protocol
SLA	Service Level Agreement
SLS	Service Level Specification
SONET	Synchronous Optical Network
SPIRIT	Service PSTN/IN Requesting Internet Services (IETF W.G)
SRTP	Secure Real time Transport Protocol
SS7	Signallling System No. 7
STP	Signaling Transfer Point
TAPI	Telephony Application Programming Interface
TCAP	Transaction Capabilities Application Part
TCP	Transmission Control Protocol
TDM	Time Division Multiplexing
TEX	Transit Exchange
TGW	Trunking Gateway
TLS	Transmission Level Security
UDP	User Datagram Protocol
UMT	Unified Threat Management

UNISTIM	Unified Networks IP Stimulus
URI	Universal Resource Identification
VBR	Variable Bit Rate
VoD	Video On Demand
VoDSL	Voice over Digital Subscriber Line
VoIP	Voice over IP
VPN	Virtual Private Network
VSAT	Very Small Aperture Terminal
WAN	Wide Area Network
WAP	Wireless Access Point
WCDMA	Wideband Code Division Multiple Access
WLAN	Wireless Local Area Network
WWW	World Wide Web
xDSL	Digital Subscriber Line (Any type)

Question Bank

Subjective

1. Write short notes on VoIP ?
2. Write short notes on NGN ?
3. What are the advantages of VoIP ?
4. What are the advantages of NGN ?
5. Draw a typical VoIP connection diagram ?
6. Write short notes on various types of codecs used in NGN ?
7. Draw a typical NGN connectivity diagram of a division ?
8. What are the basic components involved in Railtel NLD Network ?
9. Write short notes on H.323 and SIP ?
10. What is the importance of QoS in VoIP?

REFERENCES

Books

1. Asterisk 1.4 The Professional Guide, by Colman Carpenter & David Duffett First Edition Dec' 2009 Packt Publishers.
2. Asterisk 1.6, by David Merel & Barrie Dempster First Edition Jan' 2010 Packt Publishers.
3. Open SIPs 1.6, by Flavio E. Goncalves First Edition May' 2010 Packt Publishers.
4. The 3CX IP PBX Tutorial, by Matthew M. Landis & Robert Lloyd First Edition Oct' 2010 Packt Publishers.

Websites

1. http://www.asterisk.org
2. http://www.asteriskdocs.org
3. http://www.voip info.org
4. http://www.3cx.com
5. http://www.freeswitch.org
6. http://www.opensips.org
7. http://www.officesip.com
8. http://www.teksip.com

*** feedback on this book may be given to:**

Lecturer Telecom, email: smhafeezali@gmail.com

Instructor Telecom, email: m.umapathy@yahoo.com

Indian Railways Institute Of Signal Engineering & Telecommunications
Tarnaka Road, Secunderabad - 500 017 (A. P.)

http://www.iriset.indianrailways.gov.in