



VoIP Protocols

An explanation and comparison of the key VoIP protocols

An L1 Associates Technology Whitepaper

For more information on VoIP please visit www.L1Associates.com

Please direct any comments or questions about this whitepaper to enquiries@L1Associates.com

Contents

SCOPE	3
INTRODUCTION	3
H.323 STANDARD	4
H.323 INTRODUCTION	4
EQUIPMENT & ARCHITECTURE	4
HISTORY	5
H.225 REGISTRATION ADMISSION & STATUS (RAS)	5
H.225 (Q.931)	5
H.245	6
BASIC CALL SIGNALLING & ROUTING	6
H.323 SIGNALLING EXAMPLE	7
SESSION INITIATION PROTOCOL (SIP) OVERVIEW	8
SIP INTRODUCTION	8
EQUIPMENT & ARCHITECTURE	8
HISTORY	9
SIP MESSAGES	9
SESSION DESCRIPTION PROTOCOL (SDP)	10
BASIC CALL SIGNALLING & ROUTING	10
SIP REGISTRATION EXAMPLE	11
SIP PROXY EXAMPLE	11
SIP REDIRECT EXAMPLE	11
MGCP AND MEGACOP/H.248	12
MEDIA GATEWAY CONTROL PROTOCOL AND MEGACOP/H.248 INTRODUCTION	12
EQUIPMENT & ARCHITECTURE	12
HISTORY	13
BASIC CALL SIGNALLING	13
MGCP COMMANDS	14
MEGACOP/H.248 COMMANDS	15
MGCP SIGNALLING EXAMPLE	15
COMPARISON OF PROTOCOLS	16
GENERAL	16
PEER TO PEER VS MASTER/SLAVE	16
COMPLEXITY	16
SUITABILITY FOR VOICE	17
ADDRESSING	17
SUITABILITY FOR MULTIMEDIA	18
EXTENSIBILITY & DEVELOPMENT	18
CLIENT SUPPORT	18
SECURITY	19
SCALABILITY	19
SUMMARY	20
CONCLUSION	20

Scope

Anyone approaching IP Telephony (IPT) or Voice over IP (VoIP) for the first time will be bombarded with a plethora of protocols, messages, acronyms and abbreviations. It is sometimes difficult, even for experts, to track maturity of established protocols and which of those emerging protocols are being adopted in any great anger by the industry.

This whitepaper identifies the major protocols that have been adopted by the industry, how they are used in various architectures and what their relative merits are in comparison to each other.

Introduction

In order for telephone systems to facilitate calling between two or more parties they must perform certain tasks:

- authenticate the user to ensure that they are a valid user
- ensure that the user is authorised to invoke the service being requesting
- establish the call, maintain the call, and clear the call down gracefully
- during the call connect in other parties or specialised resources (e.g. voice recognition)
- generate call records for billing or performance purposes at the end of the call

In order to support these tasks a set of rules or 'protocols' are defined usually defined by industry or international standards bodies. Based on certain conditions and events these rules invoke message exchanges or 'signals' between devices or 'end points' in the telephony system.

In traditional telephone systems signalling protocols such as Signalling System No.7 (SS7) and Primary Rate Interface (PRI) are common for performing the tasks mentioned above. Although these two protocols have similarities they differ in one important way. One is a peer-to-peer protocol (SS7) and the other is a master/slave protocol (PRI) and it this difference in their models that distinguishes the functions that they perform and how they are used.

Key to the classical voice switched circuit network (SCN) is the voice switch. The concept of distributing voice switching functions across separate computing platforms is not new but the advent of VoIP in the mid 1990s allowed the bearer or media (trunks & lines), the call control, and service control functions to be elegantly separated into physically separate entities. Around 1996 industry standards bodies started to ratify early protocol standards that specified how these various entities should communicate and interact with each other.

Today there are many protocols that exist within the IPT arena not just for voice but for also for video telephony. This whitepaper introduces four key IPT protocols: H.323, SIP, MGCP and H.248/Megacop. A good measure of the maturity of a protocol or its strategic importance to the industry is the extent to which equipment suppliers develop products based on that protocol and it is these four protocols that have the majority of shipped IPT products in the market today.

One question asked by many companies is which of these protocol should they use for their particular application. The reality is that multiple VoIP protocols and architectures have been deployed today and will exist for some time. As a result networks will utilise one or more of these protocols and likely have to interoperate with other protocols.

The question companies should ask is "What are our business and services requirements?". It is from this question that the correct protocol, architecture or equipment supplier is determined. The unique nature of every business means that no two answers to this question or network implementations will ever be the same.

H.323 Standard

H.323 Introduction

Developed by Study Group 16 of the ITU-T, H.323 is an umbrella standard encompassing many subcomponent standards and annexes for transmitting multimedia (voice, video and data) across packet based networks.

The two main subcomponent protocols are H.225 (call control), & H.245 (bearer control and capabilities exchange). H.225 consists of two main parts Q.931 (basic call control as used in ISDN SCN networks) and RAS (Registration, Admission & Status). H.323 also references other standards such as Real Time Protocol (RTP), G.xxx audio codecs, H.26x video codecs and T.120 real time data conferencing protocol.

Equipment & Architecture

H.323 itself includes the equipment descriptions. Control messages & procedures define how components communicate within administrative domains or 'zones'. Entities of an H.323 system include:

Terminals: endpoint on a LAN that supports real-time, 2-way communications with another H.323 entity. Must support voice (audio codecs) and signalling (Q.931, H.245, RAS). Optionally supports video and data (e.g., PC phone or videophone, Ethernet phone).

Gateway (GW): provides interoperability between different networks, converts signalling and media (e.g. IP/PSTN gateway).

Gatekeeper (GK): manages a zone (collection of H.323 devices). Required functionality: address translation, admissions control, bandwidth control, zone management. Optional functionality: call control signalling, call authorization, bandwidth management, call management, alias address modification, dialled digit translation.

Multipoint Control Units (MCU): supports conferences between 3 or more endpoints. Contains multi-point controller (MC) for signalling & may contain multi-point processor (MP) for media stream processing. Can be stand-alone or integrated into GW, GK or terminal.

These component are shown in a reference H.323 network below:

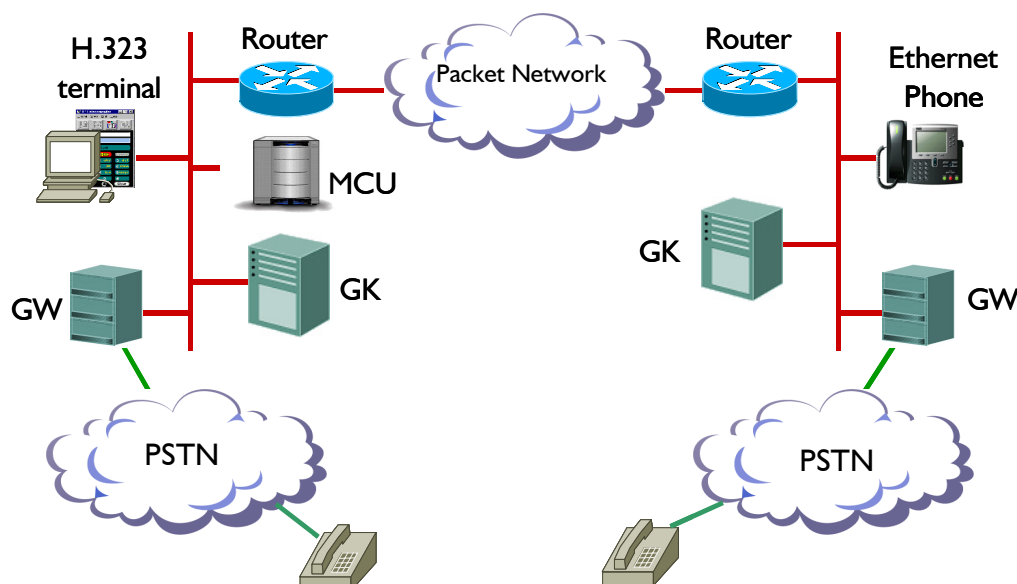


Figure 3.2

History

H.323 is a relatively mature, stable standard with continuing work in progress:

Version 1, ratified (or 'decided') in Oct 1996, was relatively basic and was heavily weighted towards multimedia communications in a LAN environment.

Version 2, decided Jan 1998, introduced communication between PC-based phones and the traditional SCN. It also introduced Fast call setup (triggered by Q.931 Fast Start message that contains basic capabilities), H.235 for security & authentication (GK registration passwords), H.450.x supplementary services (e.g. call transfer, forwarding), ability to specify alternative GKs to endpoints, and better integration of T.120 (opened like any H.323 channel).

Version 3, decided Sep 99, introduced modest but powerful changes that included the ability to reuse signalling connections (improved performance for GWs that may have thousands of calls running), better end point handling of H.245 messages, caller ID, Annex G/H.225.0 for communication between Administrative Domains and several new H.450 supplementary services such as call hold, call park & pickup, message waiting indication, & call waiting.

Version 4, decided Nov 00, introduced significant new functionality. Key was the joint IETF work approving H.248 (or Megacop in IETF) decomposed GW enabling larger, more scalable GW solutions for carriers. Other notable introductions were multiplexing audio & video together to help endpoint synchronisation and Alternate GKs providing for GK redundancy.

Version 5, due to be decided 03, is addressing a number of areas including v2 of Annex G/ H.225, Local Number Portability, and additional supplementary services.

H.225 Registration Admission & Status (RAS)

RAS is used between H.323 endpoints (terminals & GWs) and GKs. Messages are carried on unreliable channel, and may use timeouts and retry counts. Its key functions are:

Gatekeeper Discovery: process used by endpoints to determine the GK with which it must register. GK discovery can be static or dynamic. In static discovery, the endpoint knows the transport address of its GK. In the dynamic method, the endpoint multicasts a GK Request message on the GK's discovery multicast address: "Who is my GK?" One or more GKs may respond with a GK Confirm message: "I can be your GK."

Endpoint Registration: endpoint joins a zone and informs the GK of its transport and alias addresses. All endpoints register with a GK as part of their configuration.

Endpoint Location: Endpoint location is a process by which the transport address of an endpoint is determined and given its alias name or E.164 address.

Other Control: The RAS channel is also used for admission control (to restrict the entry of an endpoint into a zone), bandwidth control (negotiates bandwidth for call), disengagement control (endpoint is disassociated from a GK and its zone), and Access Tokens (providing privacy of an endpoint's address and to ensure proper routing of calls).

H.225 (Q.931)

H.225 call signalling based on ITU Q.931 is used to set up connections between H.323 endpoints (terminals and gateways), over which the real-time data can be transported. Call signalling involves the exchange of H.225 protocol messages over a reliable call signalling channel (H.225 protocol messages are carried over TCP in an IP based H.323 network).

H.245

H.245 is an end-to-end control signalling exchange between endpoints, carried over permanently open control channels (unlike media channels). Its key functions are:

Capabilities Exchange process to provide transmit & receive capabilities to the peer endpoint. Transmit capabilities describe terminal's ability to transmit media streams. Receive capabilities describe a terminal's ability to receive and process incoming media streams.

Logical Channel Signalling carries information from one endpoint to another or multiple endpoints. H.245 provides messages to open or close a logical channel; a logical channel is unidirectional.

Other Functions include Master Slave Determination messages, Multiplex Table signalling messages, Request Mode messages, Round Trip Delay messages, Maintenance Loop messages, Communication Mode Messages, Conference Request and Response Messages, Terminal ID, Commands and Indications.

Basic Call Signalling & Routing

The signalling of H.323 communication is made in the following steps:

- Step 1 RAS (optional step)
- Step 2 Call setup (H.225)
- Step 3 Initial communication and capability exchange (H.245)
- Step 4 Establishment of audiovisual communication (H.245)
- Step 5 Call services (H.225 & H.245)
- Step 6 Call termination (H.225 & H.245)

Many options exist in H.323 for call signaling & routing, and the following principles apply:

- In network environments that do not have a GK, the RAS signalling channel is not used, and H.225 (Q.931) & H.245 messages are exchanged between the endpoints.
- When a GK exists, the H.225 (Q.931) & H.245 messages are exchanged either directly between the endpoints or between the endpoints indirectly via routing through the GK. The first case is direct call signalling, the second is called GK-routed call signalling. The method is decided by the GK during RAS admission message exchange.
- The more messages that are routed via the GK, the more the load and responsibility (more information and more control).
- Media never passes through the GK function.

Figure 3.7 below shows three common models for call signalling and routing using a GK.

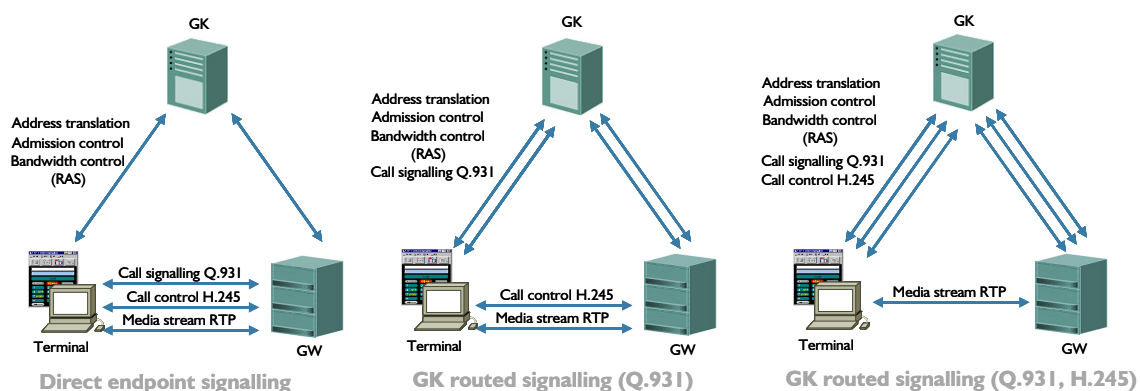


Figure 3.7

H.323 Signalling Example

Two endpoints (Clients A & B), RAS, GK routed Q.931, H.245 direct between endpoints

1. **Register with GK (RAS)** Client notifies GK of its address and aliases
 - Client transmits GK Registration Request
 - GK responds with either Registration Confirmation or Registration Rejection
2. **Call Admission (RAS)** Client initiates Admission Request (can I make this call?); the packet includes a maximum bandwidth requirement for the call
 - GK responds with Admission Confirmation
 - Bandwidth for call is either confirmed or reduced
 - Call signalling channel address of GK is provided
3. **Call Setup through GK (Q.931)**
 - Client A sends call setup message to GK
 - GK routes message to client B
 - If client B accepts, admission request with GK is initiated
 - If call accepted by GK, client B sends a connect message to client A specifying the H.245 call control channel for capabilities exchange
4. **Capabilities Exchange (H.245)** Clients exchange call capabilities with Terminal Capability Set message that describes each client's ability to transmit media streams, i.e. audio/video codec capabilities of each client
 - If conferencing, determination of MCU is negotiated during this phase
 - After capabilities exchange, clients have a compatible method for transmitting media streams; multimedia communication channels can be opened
5. **Establish Multimedia Communication** To open a logical channel for transmitting media streams, the calling client transmits an Open Logical Channel message (H.245)
 - Receiving client responds with Open Logical Channel Acknowledgement message (H.245)
 - Media streams are transmitted over an unreliable channel; control messages are transmitted over a reliable channel
 - Once channels established, either client or GK can request call services, i.e. client or GK can initiate increase or decrease of call bandwidth
6. **Call Termination (either party can terminate)**
 - Client A completes transmission of media and closes logical channels used to transmit media
 - Client A transmits End Session Command (H.245)
 - Client B closes media logical channels and transmits End Session Command
 - Client A closes H.245 control channel
 - If call signalling channel is still open, a Release Complete message (Q.931) is sent between clients to close this channel

Session Initiation Protocol (SIP) Overview

SIP introduction

Developed by IETF, SIP is a mechanism to initiate, terminate & modify sessions in an IP network. It uses a client / server architecture and the protocol is request-response based. It enables personal mobility by tracking down users and delivering calls to an endpoint.

It is a lightweight, text-based protocol and reuses much of the construct of other internet protocols such as HTTP and SMTP. SIP does not know about the underlying details of a session and relies on IETF protocol Session Description Protocol (SDP) to describe the session. It also interworks with other IETF protocols such as the Megacop (for controlling gateways to the SCN), RTP, RTSP, RSVP and SAP.

Equipment & Architecture

SIP defines a number of entities & describes their functions such as:

UA (user agent): Logical entity that initiates, receives and terminates calls:

UAC (user agent client): Logical entity that initiates and sends SIP requests. This role lasts only for the duration of that transaction (i.e. if it receives a request later, it assumes the role of a user agent server).

UAS (user agent server): Logical entity that that generates a response to a SIP request (accepts, rejects or redirects the request). This role lasts only for the duration of that transaction (i.e. if it generates a request later, it assumes the role of a user agent client).

Registrar: A server that accepts requests to register an endpoint and places the information it receives into the Location Service for the domain it handles. It is typically co-located with a Proxy or Redirect server and is the front end to the Location Service for a domain.

Location Service: Stores information about a callee's possible location(s) from information gathered by Registrar. It also then provides this information to Redirect and Proxy servers.

Proxy or Proxy Server: An intermediary entity that acts as both a server and a client (UAS & UAC) for the purpose of making requests on behalf of other clients. It plays the role of routing, by sending a request to one (or more) clients or next-hop servers "closer" to the targeted user. It can also enforce policy (e.g. ensuring a user is allowed to make a call). It interprets, and if necessary, rewrites specific parts of a request message before forwarding it.

Redirect Server: A user agent server that accepts SIP requests, maps the address into zero or more new addresses and directs the client to contact an alternate set of addresses. It does not initiate SIP requests or accept calls.

These component are shown in a reference SIP network below:

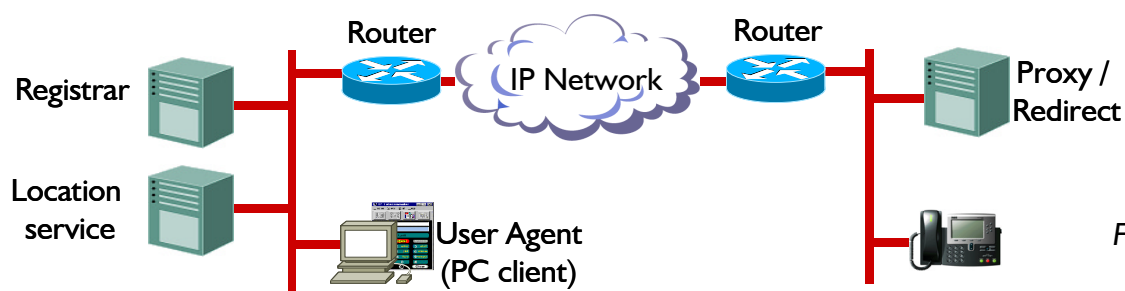


Figure 4.2

History

SIP originates from Mbone (multicast backbone) set of utilities & protocols, an early multicast network layered on top of the Internet to act as a multimedia delivery network. An initial draft of SIP was submitted to the IETF as early as February 1996 and went through many revisions until it was published as a 'standard' by the IETF MMUSIC working group three years later in March 1999 as RFC (Request For Comment) 2543. In June 2002 RFC 2543 was made obsolete when a number of improvements resulted in a group of new SIP RFCs:

- RFC 3261 SIP: Session Initiation Protocol
- RFC 3262 Reliability of Provisional Responses in SIP
- RFC 3263 Locating SIP Servers
- RFC 3264 Offer/Answer Model with SDP
- RFC 3265 SIP-Specific Event Notification
- RFC 3266 Support for IPv6 in SDP

Today SIP is a relatively mature, stable standard with continuing work on the RFC itself and many related areas.

SIP Messages

Request messages (or Methods):

- **INVITE** Invites a user to a call
- **ACK** confirms receipt of final response to an INVITE
- **BYE** Terminates a connection between users or declines a call
- **CANCEL** Terminates a request, or search, for a user
- **OPTIONS** Solicits information about a server's capabilities
- **REGISTER** Registers a user's current location
- **INFO** Used for mid-session signalling

Response types:

- **Provisional (1xx class)** informational responses used by the server to indicate progress, they do not terminate SIP transactions
- **Final (2xx, 3xx, 4xx, 5xx, 6xx classes)** responses terminate SIP transactions.

Response Classes:

- **1xx** provisional, searching, ringing, queuing etc.
- **2xx** success
- **3xx** redirection, forwarding
- **4xx** request failure (client mistakes)
- **5xx** server failures
- **6xx** global failure (busy, refusal, not available everywhere)

Examples of common response messages:

- | | |
|--------------------------------|------------------------------------|
| • 100 Trying | • 484 Address Incomplete |
| • 180 Ringing | • 500 Server Internal Error |
| • 200 OK | • 503 Service Unavailable |
| • 301 Moved Permanently | • 603 Decline |
| • 404 Not Found | • 606 Not Acceptable |

Session Description Protocol (SDP)

SDP (RFC 2327) is not part of the SIP protocol but is an important part of the establishment of SIP sessions. SDP describes multimedia sessions for session announcement, session invitation, and other forms of multimedia session initiation. It delivers a description of the session that the user is involved in and is usually included in an INVITE request (describes callers receive parameters), a 200 OK response (describes called party's receive session parameters), and an ACK (optionally describes callers transmit session parameters). SDP packets usually include the following information:

Session information

- Session name and purpose
- Time(s) the session is active
- Information about the bandwidth to be used by the session
- Contact information for the person responsible for the session

Media information

- Type of media (e.g. video and audio)
- Transport protocol (e.g. RTP/UDP/IP)
- Media format (e.g. H.261 video, MPEG video, G.711 voice etc.)
- Multicast address and transport port for media (IP multicast session)
- Remote address for media and transport port for contact address (IP unicast session)

Basic Call Signalling & Routing

The process for establishing communication with SIP usually occurs in six steps:

- Step 1 Registering, initiating and locating the user
- Step 2 Determine the media to use (using SDP)
- Step 3 Determine willingness of called party to communicate
- Step 4 Call setup
- Step 5 Call modification or handling (optional)
- Step 6 Call termination

Addressing: SIP gives a globally reachable address and callees 'bind' to this address using the REGISTER method. Addresses are in a URL format such as sip:user@host. It must include the host, and may include the user name, port number & other parameters (e.g. transport). For example sip:bob@office.com or sip:voicemail@siteA.com?subject=returnmycall

Registration: Each time a UA is enabled it creates an address mapping in the 'Location Service' explicitly by sending a **REGISTER** request to the 'Registrar'. The Registrar reads & writes mappings to location service based on the contents of **REGISTER** requests.

Proxy & Redirection: The Proxy server acts as a rendezvous point at which all callees are globally reachable. It performs the routing function i.e. to which hop (UA / Proxy / Redirect) the request is relayed to. The request may be forked whereby several destinations may be tried sequentially or in parallel. A Proxy server can be 'stateful' when it keeps state during a transaction and discards information about the transaction when it is complete. The Redirection server differs in that it only returns a mapped address back to the UA (i.e. instructs the UA to initiate a request elsewhere). Unlike a Proxy server it does not initiate its own SIP request. Unlike a UAS it does not accept or terminate calls.

SIP Registration Example

User's address bob@office.com is bound to user's current location 197.63.48.169.

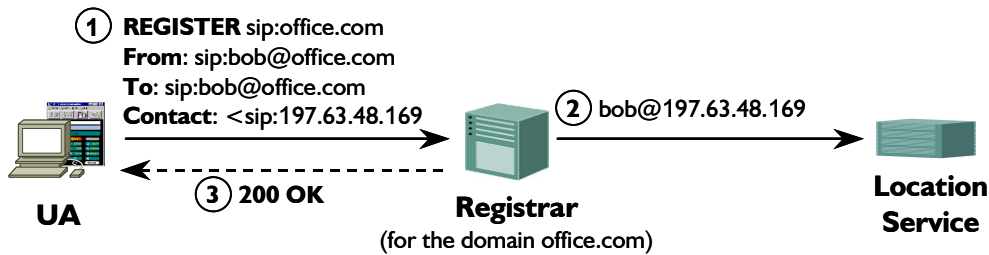
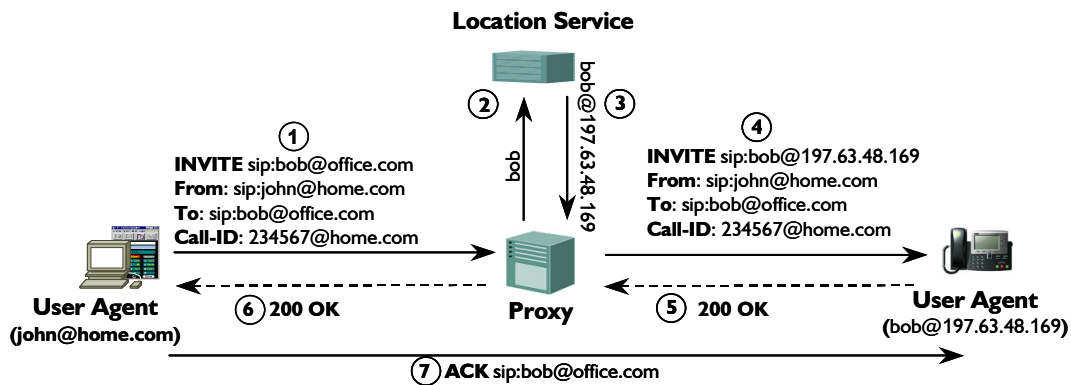


Figure 4.7



SIP Proxy Example

1. Proxy server accepts the INVITE request
2. It then contacts the location service with all or parts of the address
3. And obtains a more precise location
4. Proxy server issues an INVITE request to the address(es) returned by the location service
5. The user agent server alerts the user and returns a success indication to the proxy server
6. The proxy server then returns the success result to the original caller
7. The caller confirms receipt to the callee using ACK message (with a response returned)

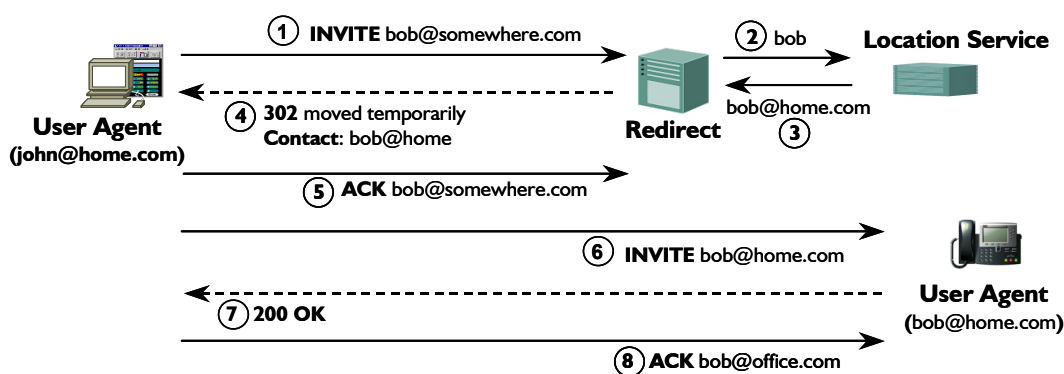


Figure 4.8

SIP Redirect Example

1. The redirect server accepts the INVITE request
2. It then contacts the location service as before
3. And obtains a more precise location
4. Instead of contacting the newly found address itself, returns the address to the caller
5. Caller confirms receipt to the Redirect Server using ACK (with a response returned)
6. The caller issues a new request (with a new call-ID) to the address returned by the server
7. The callee returns a success indication to the caller
8. The caller and callee complete the handshake with an ACK

MGCP and Megacop/H.248

Media Gateway Control Protocol and Megacop/H.248 introduction

MGCP & Megacop/H.248 are relatively low level, master/slave protocols used between call control devices called 'call agents' and media gateways (MGs). MGCP is not officially a standard but does exist as an informational RFC (RFC 3435). Megacop (IETF RFC 3015) & H.248 (ITU Rec.) are the same protocol developed by an IETF and ITU collaboration. It is derived from, and draws heavily from MGCP but adds several new enhancements.

Equipment & Architecture

MGCP and Megacop/H.248 operate in a distributed architecture, known as the 'decomposed multimedia GW' architecture defined by the ETSI TIPHON body. The MG in the decomposed GW architecture is less complex in comparison to H.323 in that the signalling function (e.g. SS7) and much of the intelligence is removed to other devices such as Signalling Gateways (SGs) and call agents.

Although the exact models of MGCP and Megacop/H.248 differ, they do have similarities in that they both contain MGs and call agents (as per the decomposed GW). In Megacop/H.248 the call agent is termed a Media Gateway Controller (MGC):

Media Gateway (MG): Converts media (audio, video & T.120) from one type of network to the format required in another type of network.

Call Agent (CA) or Media Gateway Controller (MGC): Controls the parts of the call state that pertain to connection control for media channels in a MG.

In the MGCP model the CA handles the signalling function (e.g. SS7 or PRI) and refers to the CA implementing the 'signalling' layers of H.323 for this function. In the Megacop/H.248 a dedicated Signalling Gateway (SG) is specified for this function:

SCN SG: This function contains the SCN Signalling Interface that terminates SS7, ISDN or other signalling links.

These component are shown as they would exist in a decomposed GW architecture:

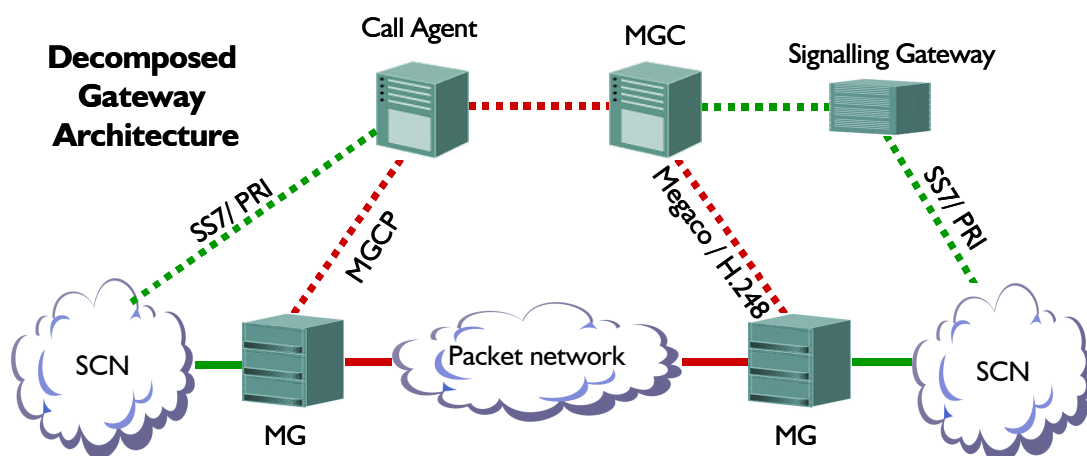


Figure 5.2

History

Early 98: Level 3, Cisco & Bellcore (now Telecordia) develop the Simple Gateway Control Protocol (SGCP) using BellCore's original gateway decomposition. Consortium (led by Level 3, with Xcom & Nortel) proposed IP Device Control (IPDC) similar in function to SGCP.

Mid 98: IETF formed MEGACO working group to produce a protocol between MGC & MG.

Late 98: MGCP (version 0.1) was formed from SGCP & IPDC. Lucent develop Media Device Control Protocol (MDCP) and went into the IETF and causes changes to MGCP (version 1). Lucent and Level 3 form Soft Switch Consortium and take MGCP version 1 with them.

Early 99: MEGACO design group produced Megacop using ETSI TIPHON requirements. ITU SG 16 adopts Megacop and now work in collaboration with IETF.

June 00: ITU Rec. H.248 decided (originally referred to as H.GCP). IETF lead on the requirements specification and ITU lead on drafting recommendation.

Today: Soft Switch Consortium & PacketCable are now maintaining MGCP. In IETF MGCP remains an informational RFC.

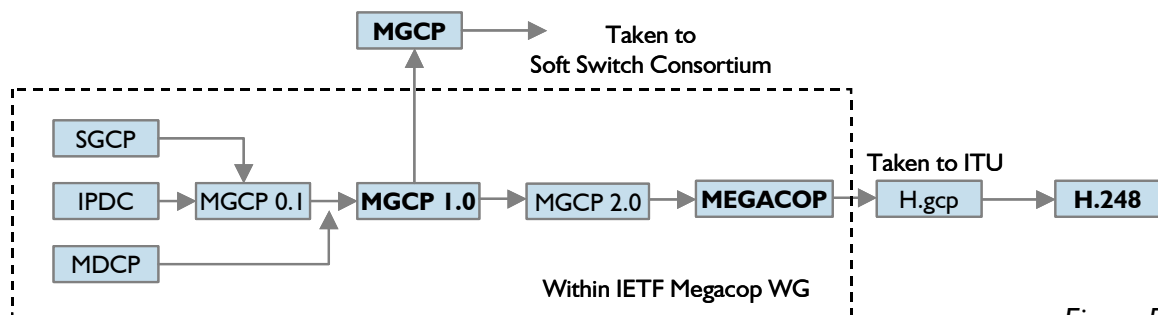


Figure 5.3

Basic Call Signalling

Call signalling in this case defines the interaction between the CA and the MG for the control of calls and both MGCP and Megacop/H.248 support the following interactions:

- Creating, modifying and deleting connections involving bearer terminations. The bearer terminations may be circuit switched or packet switched.
- Detecting events and applying signals to media streams. Upon detecting an event the CA specifies the MG's actions such as reporting it or applying another signal.
- Digit collection according to the dial plan or 'digit map' specified by the CA. The MG may collect digits according to the predetermined dial plan before reporting them to the CA.
- Adding or subtracting media streams throughout the session, providing conferencing services, and IVR type services such as playing announcements.
- Reporting statistics collected for the call such as Quality Of Service (QoS) measurements.

MGs contain 'endpoints' on which the CAs can create, modify and delete 'connections' in order to establish and control media sessions with other multimedia endpoints. In Megacop terminology the MGCP endpoint is a 'termination' & the MGCP connection is a 'context'.

The Call Agent instructs the endpoints to detect certain events and generate signals. The endpoints automatically communicate changes in service state to the Call Agent. Furthermore, the Call Agent can audit endpoints as well as the connections on endpoints.

MGCP Commands

EndpointConfiguration: CA to GW, instructing the GW about the coding characteristics expected by the "line-side" of the endpoint.

NotificationRequest: CA to a GW, instructing the GW to watch for specific events such as hook actions or DTMF tones on a specified endpoint

Notify: GW to inform the CA when the requested events occur.

CreateConnection: CA to create a connection that terminates in an "endpoint" inside GW.

ModifyConnection: CA to change parameters associated to a previously established connection.

DeleteConnection: CA to delete an existing connection or number of connections. May also be used by a GW to indicate that a connection can no longer be sustained.

AuditEndpoint and **AuditConnection:** CA to audit the status of an "endpoint" and any connections associated with it. Network management beyond the capabilities provided by these commands are generally desirable (through SNMP and definition of a MIB).

RestartInProgress: GW to notify CA that GW, or group of endpoints managed by the GW, is being taken out of service or is being placed back in service.

All MGCP commands are acknowledged with a return code or error code:

- values between 000 and 099 indicate a response acknowledgement
- values between 100 and 199 indicate a provisional response
- values between 200 and 299 indicate a successful completion
- values between 400 and 499 indicate a transient error
- values between 500 and 599 indicate a permanent error
- values between 800 and 899 are package specific response codes.

Megacop/H.248 Commands

Add: Adds a termination to a context. Context is created on first Termination.

Modify: Modifies the properties, events and signals of a termination.

Subtract: Disconnects a Termination from its Context & returns statistics on Termination's participation in Context. Context deleted on last Termination.

Move: Moves a Termination to another context

AuditValue: Returns current state of properties, events, signals & statistics of Terminations

AuditCapabilities: Returns all values for Termination properties, events & signals allowed by MG.

Notify: allows MG to inform MGC of the occurrence of events in the MG.

ServiceChange: Allows MG to notify MGC of Termination (or group) to be taken out of service or has just returned to service. Also used to announce MG availability to MGC (registration), & to notify MGC of impending or completed MG restart. Also MGC to announce handover to MG and to instruct MG to take a Termination (or group) in or out of service.

MGCP Signalling Example

User1 connected to Media Gateway1 (MG1) initiating and then terminating a call to User2 connected to MG2 with the call controlled by the CA.

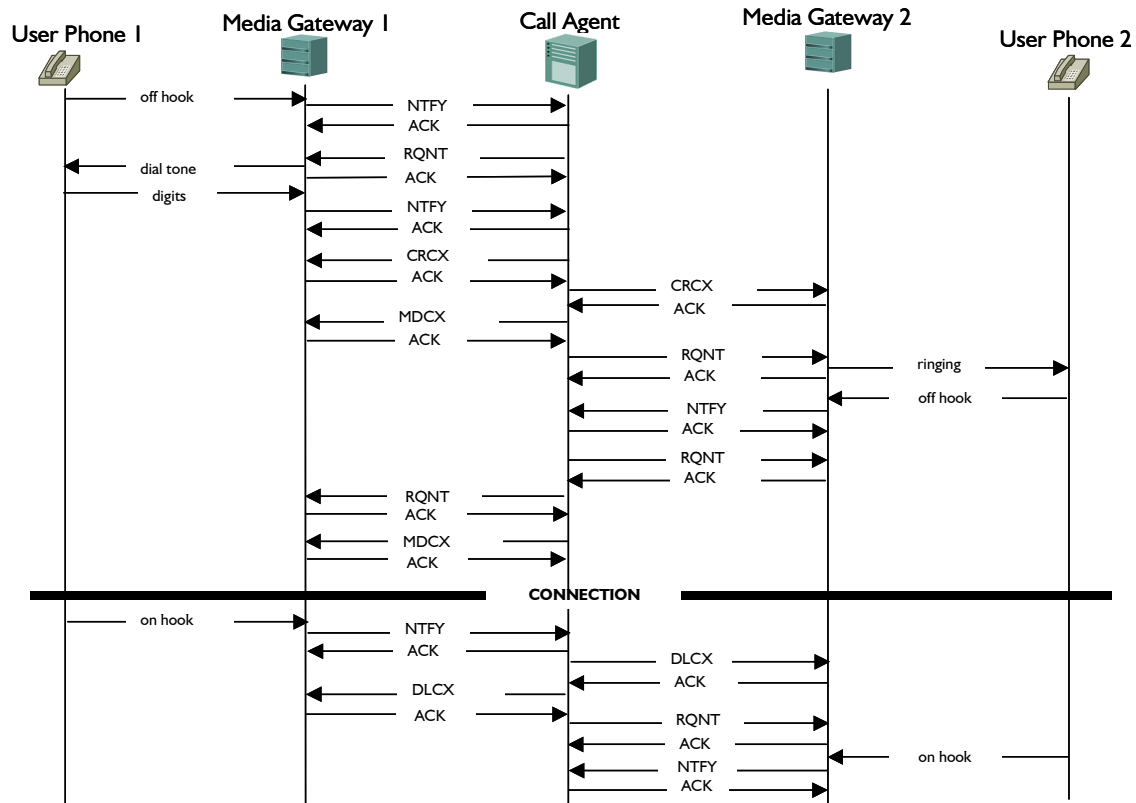


Figure 5.7

Connection Creation

1. NTFY (Notify) from MG1 to CA, informing that User1 has gone off hook [assumes CA had previously sent RQNT (NotificationRequest) requesting notification of off hook from User1].
2. RQNT from CA to MG1, requests MG1 to notify CA when User1 goes on-hook, provide dialtone, and collect digits according to the digit map.
3. NTFY from MG1 to CA, informing CA of digits dialed from User1.
4. CRCX (Create Connection) from CA to MG1, requests a new connection on MG1 with the specified local connection options (e.g. packetisation period, codec, send/receive mode). The ACK in response to this message contains the SDP (Session Description Protocol) information specifying the preferred session parameters from MG1.
5. CRCX from CA to MG2, requests a new connection on MG2 and includes the session description from MG1 such that a two-way connection can be initiated. The ACK in response contains the SDP information specifying the preferred session parameters from MG2.
6. MDCX (Modify Connection) from CA to MG1, requests MG1 to modify the existing connection and to use the session description returned by MG2 (assumes differences exist).
7. RQNT from CA to MG2 to provide ringing to User2 and to notify when User2 goes offhook.
8. NTFY from MG2 to CA that User2 has gone offhook.
9. RQNT of on-hook from CA to MG2.
10. RQNT of on-hook from CA to MG1.
11. MDCX from CA to MG1. This modifies the existing connection to sendrecv such that a full duplex connection is initiated.

Connection Deletion

1. NTFY from MG1 to CA that User1 has gone on-hook.
2. DLCX (Delete Connection) from CA to MG2 requests MG2 to delete the connection.
3. DLCX from CA to MG1 requests MG1 to delete the connection.
4. RQNT from CA to MG2 requests MG2 to notify CA in the event of an off-hook.
5. RQNT from CA to MG1 requests MG1 to notify CA in the event of an off-hook.

Comparison of Protocols

General

H.323 is the most mature of the protocols described and gained the earliest momentum in the IP Telephony market. It is a well specified protocol originally designed for the requirements of multimedia communication (voice, video and data conferencing) over IP. It takes advantage of traditional SCN protocols, for example the call establishment protocol H.225 is based on ISDN Q.931 and the H.450 series of standards define the support of ISDN like supplementary services.

SIP based solutions have been around for many years but recent enhancements and an increasing adoption by the marketplace have seen a more widespread take up and it is forecast that SIP shall ultimately replace H.323 as the peer protocol of choice for most IP Telephony applications. It was designed originally to set up and terminate calls (i.e. a session with media streams) between two parties. Its model has many close similarities with the Internet in that the protocol reuses much of HTTP & SMTP, and the addressing scheme is URL based.

Media gateway control protocols such as MGCP and Megacop/H.248 evolved to satisfy deficiencies in the gateway models and the current development activity around them is much less than that of H.323 and SIP. Whilst H.323 and SIP contrast substantially as peer protocols, there are fewer differences between MGCP and Megacop/H.248. These similarities stem from the fact that they perform the same architecture function of media gateway control, and that Megacop/H.248 has its roots in MGCP.

Peer to Peer vs Master/Slave

It is important to differentiate the four key protocols in terms of the function they perform in any network architecture. H.323 & SIP are peer-to-peer protocols since they define the protocols for communication between call control devices (e.g. GK to GK or SIP server to SIP server). MGCP & Megacop/H.248 are exclusively master/slave protocols (i.e. call agent to gateway) and they rely on other peer-to-peer protocols for communication between call agents.

H.323 & SIP also exhibit master/slave signalling functions since they include the control of gateway & endpoint devices. However the end-to-end nature of H.323 & SIP makes it difficult to directly compare them to MGCP and Megacop/H.248. This paper therefore mainly compares H.323 to SIP and MGCP to Megacop/H.248.

Complexity

H.323 is traditionally thought to be a more complex standard than SIP and this is certainly true when comparing the extensive H.323 specifications and its many annexes to the half dozen or so RFCs describing SIP. For example H.323 includes within its remit areas that SIP leaves to other standards such as bearer control (H.323 specifies H.245, SIP relies on SDP) and interconnecting to traditional SCNs. However when you include all the development and approved documentation pertaining to SIP it most likely exceeds H.323 in terms of functionality and documentation.

In both cases interoperability and version control problems exist. Many of H.323's several protocol components and annexes have their own development life cycle and change independently of the versions of H.323. Similarly for SIP it is difficult to know which of the related documents are informational, optional or required.

Comparing the message formats themselves, H.323 uses ASN.1 (Abstract Syntax Notation) a standardised, low level, precise structural notation. Messages are encoded in binary format suitable for narrowband and broadband transmission. SIP uses an ABNF syntactical notation (RFC 2234) and messages are encoded in ASCII text format which are easier for humans to read and understand. This is countered by the fact that textual messages are typically larger in comparison to their equivalent binary format and potential message size problems can materialise (e.g. large SIP messages can breach the MTU of a network and could require fragmentation).

Generally MGCP and Megacop/H.248 have the constructs to achieve the same tasks and as such there is very little difference in their messages structure. However since Megacop/H.248 has refined and extended many of the MGCP functions, it has the edge when comparing complexity.

Suitability for Voice

H.323 was designed from the outset to support voice, video and data conferencing. The use of Q.931 as the call signalling protocol gave it many advantages in supporting voice services. Today H.323 is used heavily for international (& national) voice toll bypass and is widespread in enterprise networks in particular for the majority of IP PBX implementations. H.323 also has strong conferencing capabilities with the definition of the MTU and H.245 bearer negotiation. It also has good support of business features such as call forward and transfer through the many H.450 standards.

SIP has its origins in the Mbone which was a set of utilities and protocols over the Internet and was basically a session initiation protocol. Soon after its origination it was adopted for use in voice applications. Like H.323 it is well suited for voice applications and supports as many services as H.323 including conferencing, call forward, and transfers. SIP has excellent mobility built in to its operation allowing users to be found regardless of their location. This operation also facilitates call 'forking' whereby multiple endpoints are targeted either sequentially or in parallel to find the user.

Since H.323 borrowed PSTN protocols it is more suited than SIP for supporting PSTN & ISDN services. SIP has very little commonality with the PSTN and does not handle ISDN at all gracefully. Both H.323 and SIP have significant limitations for supporting the PSTN SS7 signalling system, although there has been much recent work on this subject in both protocols. H.323 terminates the signalling channel on the MG and H.225 Q.931 is not suited to mapping or transparently transferring all SS7 signalling messages. Similarly SIP was just not designed to support this type of complex voice signalling system. The decomposed GW architecture helped to solve this problem by separating the complex SS7 signalling function out to dedicated devices such as Signalling GWs. Where H.323 and SIP architectures are to interwork with SS7 networks then an interworking function is required and this is usually implemented by a device known as 'softswitch'. The softswitch also allows H.323 and SIP to work in conjunction with MGCP or Megacop/H.248.

Addressing

H.323 has a more inherent flexible addressing mechanism in that it supports both URLs and E.164 numbers. H.323 endpoints may have one or more 'alias addresses' that can be private or public (E.164) numbers, H.323 IDs (alphanumeric strings representing names, or e-mail like addresses) & URLs. H.323 endpoints rely on the GK to perform address resolution and the GK may use a number of protocols to identify the destination address of the callee including communication with other GKs, H.225 Annex G (for inter domain), DNS, TRIP or ENUM.

SIP uses a URL style address format and the SIP Proxy or Redirect server is responsible for resolving the address or identifying a nearer location that will ultimately identify the location of the callee. The Proxy may use various protocols to identify the destination address of the callee including DNS, TRIP or ENUM.

Suitability for Multimedia

H.323 included the support of video and data conferencing from its outset whilst SIP focused initially on voice. H.323 defined the H.245 capabilities exchange that provided the ability to negotiate voice, video and data conferencing sessions between endpoints, particularly important for video where a large number of parameters may need to be agreed before a session can be established.

SIP, MGCP & Megacop/H.248 all rely on SDP which was not originally intended to provide capability negotiation. However as the need for this has become increasingly important IETF work has begun on a 'next generation SDP' (SDPng) that supports both session description and capability negotiation. SDPng is not intended to be backwards compatible with SDP and work is currently ongoing.

Extensibility & Development

As telephony features evolve it is important to be able to build in extensions whilst ensuring compatibility amongst versions.

H.323 provides extensibility by giving messages and fields placeholders where proprietary extensions can be added. A 'nonstandardParam' field is located in various places in the ASN.1 notation. This can be limited since extensions are only available to those places where a non standard parameter has been added. Additionally there is a very limited mechanism for endpoints to exchange information about which extensions each supports and the values are not self explanatory. This can be a problem for interworking products from different manufacturers.

SIP reuses many of the lessons from HTTP & SMTP and builds in extensibility and compatibility functions. SIP headers are extended by adding new lines that are in textual format and therefore usually self explanatory. Unknown headers and values are ignored by default and numerical error codes are hierarchically organised as in HTTP. Feature negotiation is available through the REQUIRE header.

SIP is generally considered to be easier to develop than H.323. H.323 requires special ASN.1 compilers or code generators to parse or requires an expert understanding of ASN.1. Since SIP encodes its messages in text it is easier to parse and generate messages.

Client Support

Microsoft Netmeeting is an H.323 client and Microsoft Messenger client is based on SIP. Since both are predominantly intended for use on PCs it is not too important for them to have small memory and processing requirements. To consider reducing the client 'footprint' typically invokes discussion about the location of intelligence, whether in the network (telephony model) or in the endpoints (Internet model). However generally H.323 is considered to be a 'thick' protocol and SIP a 'thin' protocol. SIP therefore lends itself to deployment on low performance devices such as Personal Digital Assistants (PDAs) and mobile terminals. This influenced the 3rd Generation mobile standards bodies to adopt SIP as its peer protocol of choice for packet telephony communication.

The MGCP and Megacop/H.248 have a low complexity connection model and their command structure is simple with a low messaging overhead which provides for a thin client. MGCP and Megacop/H.248 are not normally deployed as voice or multimedia clients due to the function the protocols perform but their low footprint facilitates their use in low cost low complexity residential gateways and IP phones.

Security

Both SIP and H.323 have some degree of security mechanisms. H.323 specifies its own security procedures in H.235 which are independent of the underlying IP network and can also use SSL for transport layer security. SIP utilises existing security measures including HTTP for authentication, SSL for encryption and PGP or S/MIME for end-to-end encryption & authentication.

Both H.323 & SIP require protocol aware firewalls. In both cases it may be necessary for the firewall to locate the called or calling party address and difficulties arise in both cases since SIP uses variable length fields and H.323 can use the FastStart procedure which encapsulates the required information within other H.323 messages.

MGCP supports IPsec in the underlying transport for securing signaling information and Megacop/H.248 adds the option providing an authentication header. Both also support encryption and authentication of the source address to prevent source address spoofing.

Scalability

Scalability can be measured in a number of ways and there are differences in the scalability of H.323 & SIP. The first releases of H.323 were designed for operation on a single LAN, and later the principle of administrative domains or zones was defined for identifying user location and general interoperation between domains (H.225 Annex G). This allows GKs to perform address resolution, pricing exchange, and least-cost delivery of calls in a scalable manner for large networks. It is also possible to use a third party, called a 'clearinghouse', to perform these functions between service providers who do not have prearranged service agreements. However for networks with a large number of domains loop detection can be a problem.

A SIP call traversing servers and GWs can be either stateful or stateless. In the stateless model the server forgets about the call once it has been processed. In H.323 the GK must retain state for all calls it has processed for the duration of the calls. For large IPT networks the number of calls being handled by a large server can be significant increasing the performance requirements of the server.

Similarly the server must process the signalling messages for a call and the simpler the signalling the faster it can be processed. Typically SIP is simpler to process and would support a greater number of calls per second for the same server specification.

H.323 has the ability to load balance endpoints across a number of alternate GKs for increased flexibility when scaling local points of presence. Endpoints can also report their load so that calls may be best distributed across a number of gateways when load problems materialise. SIP does not have any notable concept of load balancing.

Summary

H.323, SIP, MGCP, & Megacop are all protocols widely deployed in IPT networks. H.323 & SIP are peer-to-peer protocols and MGCP & Megaco/H.248 are master slave protocols. H.323's approach follows a more telephony model whilst SIP uses many concepts from the internet model.

There is a significant amount of development work around H.323 and SIP and both protocols are evolving rapidly. H.323 gained the earliest momentum in the IPT and VoIP industry with many supplier products on the market today particularly for enterprise and multimedia applications. SIP is gaining ground and is ultimately likely to become the major peer protocol.

As SIP becomes more prevalent there shall be circumstances where both protocols shall co-exist with interworking provided by specialised devices and a base set of services shall be transparent across both network types.

MGCP is not undergoing any significant development work but is still widely used particularly by the Soft Switch Consortium & PacketCable bodies. Megacop & H.248 are the same protocol and were developed collaboratively between the IETF and the ITU respectively. Derived from MGCP, it is the official industry protocol for interfacing between external call agents (MGCs) and MGs.

The decomposed GW architecture in which both MGCP & Megacop/H.248 operate, is designed to make the MG less complex, less expensive & more scalable by moving the complex signalling function (e.g. SS7) and much of the intelligence out of the MG. Megacop/H.248 is being increasingly adopted and is playing a key strategic role particularly for low cost MGs and for interworking to PSTN networks.

Conclusion

Many businesses are increasingly embracing IP Telephony as they discover the benefits and opportunities that it can deliver. IPT is becoming an important part of many communication strategies and business plans and fundamental to the successful implementation of the business plan is the correct choice of protocol. It is also important to understand exactly how that protocol resides within the overall architecture for the provision and interworking of services.

This paper has introduced four of the main IPT protocols, but of course there are many more standards, protocols, RFCs and industry bodies, performing their own specialised functions for IPT networks.

For carriers, enterprises and equipment suppliers the choice of protocol is one of many issues they shall encounter as they seek to gain competitive advantage. What is also clear is that we are entering a new era in communications and the evolution of industry protocols, as they have always been, are crucial to its success.
