Scientific Atlanta
A CISCO COMPANY

VoIP: Architectural Differences of SIP and MGCP/NCS Protocols and What It Means in Real World VoIP Service

Marcin Godlewski
Lead Engineer
Scientific Atlanta, a Cisco Company

Charles Moreman
Director of Engineering
Scientific Atlanta, a Cisco Company

Abstract

Voice over Internet Protocol (VoIP) is growing in popularity around the world and provides a tremendous opportunity for extracting more value from existing cable networks. Pressure to effectively compete with new players in the voice, video and data delivery marketplace continues to mount.

For the cable operator, VoIP represents opportunities that include:

- **Increased Revenue – Bundled services provide new opportunities to increase revenue, paired with greater scalability and flexibility for future growth**
- **Bandwidth Efficiency - VoIP extracts more revenue from the network by sharing bandwidth between voice and data**
- **Customer Appeal – Multiple services from one vendor simplifies bill paying and service calls for customers**
- **Competitive Advantage – Increase the value of cable service, build subscriber loyalty and attract new customers**

Most VoIP deployments today use one of two protocols:

- **Session Initiation Protocol (SIP)**
- **Media Gateway Control Protocol/Network Control Signaling (MGCP/NCS)**

These call control protocols are used to setup, maintain and tear down VoIP calls. This paper will explore the advantages and disadvantages of each. It will also cover the underlying architectural differences and how this relates to real world VoIP services, as well as establishing a foundation for future services.

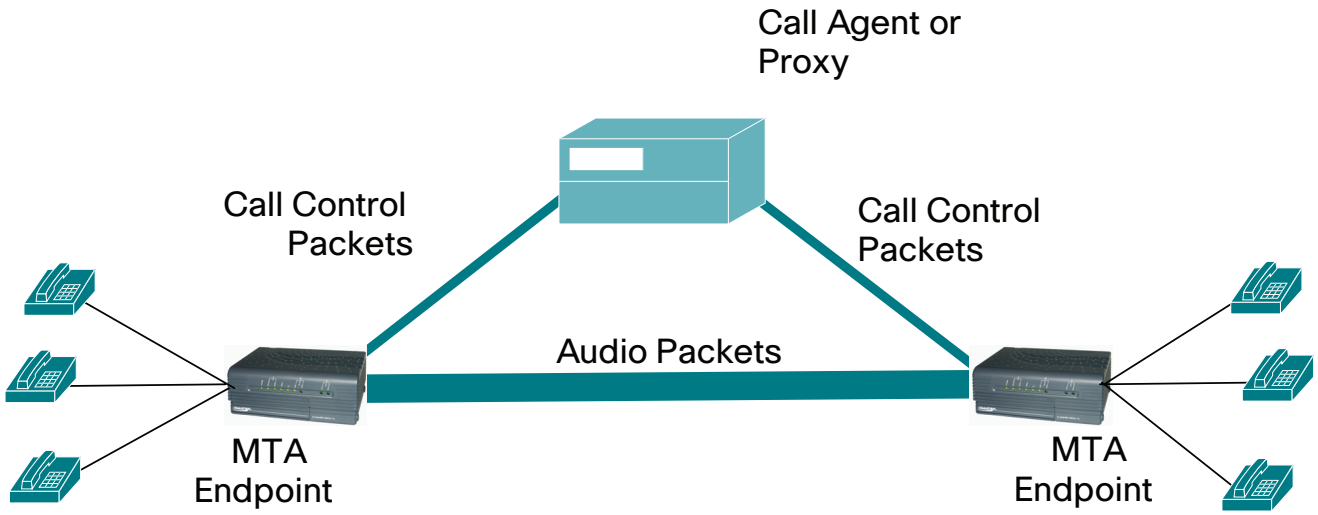
VoIP BACKGROUND

VoIP Packet Flows

Unlike calls in traditional PSTN (Public Switched Telephone Networks), a VoIP call is not a single, continuous end-to-end connection, but instead is made up of many individual IP "packets." With VoIP, voice packets travel across IP networks intermixed with millions of other data packets. Each call is made up of both signaling packets and media packets — signaling packets contain information required to connect and then disconnect callers, while media packets contain the actual voice conversation.

Because UDP/IP (User Datagram Protocol over IP) is mainly used for VoIP applications, it does not provide a mechanism to ensure that data packets are delivered in sequential order, or provide Quality of Service guarantees, VoIP implementations can face challenges dealing with latency and varying delays (otherwise known a "jitter"). The receiving node must restructure IP packets that may be out of order, delayed or missing, while ensuring that the audio stream maintains a proper time consistency.

Signaling packets go to the call agent or proxy, setting up, changing or deleting calls. This is because service providers need control over calls being made. Once call is set up, the media packets go directly between VoIP endpoints (phones). The signaling and media paths may be different, using separate resources, either physical, logical or both.



Signaling packets go to the call agent or proxy, setting up, changing or deleting calls. This is because service providers need control over calls being made. Once call is set up, the media packets go directly between VoIP endpoints (phones). The signaling and media paths may be different, using separate resources, either physical, logical or both.

Audio Quality

In a successful VoIP deployment, customers need to receive the same quality of audio transmission they receive with traditional telephone services –meaning high-quality voice transmissions on a consistent basis. For VoIP transmissions to be intelligible to the receiver, voice packets should not be dropped, excessively delayed or suffer jitter.

Factors that affect VoIP audio quality include: CODEC choice, network packet loss, special considerations including echo, analog modem and FAX calls and home security systems, and analog losses and noise, as compared to the PSTN.

End to End Audio Delay

Latency is also a critical factor in VoIP call quality. From a technical perspective, end to end audio delay should meet acceptable standards to achieve optimal performance and meet end user expectations. As one would expect, smaller delays are always better, as they enable more natural sounding phone calls. Typical PSTN delays are <20mS round trip. Typical VoIP service provider delay goals are approximately 150 to 200mS round trip. Delay sources vary and can be caused by the following:

- CODEC delays - 2mS to 40mS
- Packetization delays - 10mS to 30mS
- Network delays - <1mS to 20mS
- Jitter buffer delays – 5mS to 100mS

To minimize latency, dynamic adaptive jitter buffer approaches work best, allowing the service provider to resize jitter buffers upward and downward. The best implementations are able to adjust in 5mS increments.

Security

The Internet universe continues to expand, and with that growth, harmful computer viruses and hacker activity have also grown. Security is vital for successful VoIP deployments over public IP networks, and service providers must keep their customers safe, with consideration in mind for:

Theft of Service Prevention

- User authentication – Only authorized users (for example phone numbers) can access the VoIP network and make calls
- Device authentication – Only authorized devices can access the VoIP network and make calls. This is important for VoIP service providers to minimize hardware types to have easier support
- Call control to setup only authorized calls – Only the calls that originate from valid devices and users should be accepted
- Collection of per call billing records – Important for the providers to earn money on the VoIP serverice
- Prevention of unauthorized network QOS – Only authorized devices and users can get quality of service (QoS) for VoIP calls.

Privacy

In the PSTN it is difficult to learn about calls as the calls are carried by networks that have very limited access. VoIP calls can be part of Internet traffic and are more vulnerable to others seeking access to it. To make sure the privacy is met, these elements have to be considered:

- Encryption of Call Control Data

  - Phone numbers dialed and received – only the parties in a call and the operator's switch should be able to see this information

  - Call duration and call time - gaining information about call time and duration can reveal the intentions of conversations so this information has to be protected

- Encryption of Audio Content - it is important to make sure that nobody can evesdrop on a VoIP conversation.

CALEA - Communications Assistance for Law Enforcement Act

- Call Detail Reporting

VoIP Call Control Protocols – Features

Almost all VoIP call control protocols support similar features:

Setup new phone calls

- Pass information to other network resources regarding each new phone call.
- Pass information needed to setup the CODEC type and other call parameters (commonly using the Session Description Protocol – SDP)

Maintain phone calls

- Pass information regarding changes in call status, mid-call CODEC changes, etc.

Tear down phone calls

- Notify other network resources regarding call completion
- Needed to free up network resources

VoIP Call Control Protocols – Approaches

When it comes to VoIP call control protocol, there are three primary approaches. With the master/slave approach, endpoints notify a call agent when an "event" happens. The call agent makes all relative decisions and then sends commands back to the endpoints. In turn, endpoints act on the commands to play tones, etc.

With the peer to peer approach, "smart" endpoints locate other "smart" endpoints, and the endpoints setup and tear down calls directly. All traffic passes directly between users, not to a service provider.

With a peer to peer approach with proxy agents, the proxy Agents are inserted to act as a mediator between endpoints. The proxy agents are under the control of a service provider and maintain control to prevent theft of service and collect billing information. Proxy Agents can also enforce CODEC choices, packetization rates and other parameters.

Examples of VoIP call control protocols include H.323, Session Initiation Protocol (SIP), Media Gateway Control Protocol (MGCP) and MGCP Network Control Signaling (MGCP/NCS).

Cable operators must keep in mind that call control protocols are used to setup, maintain and tear down VoIP calls, but are not used to pass audio content

MGCP/NCS Protocol

Background

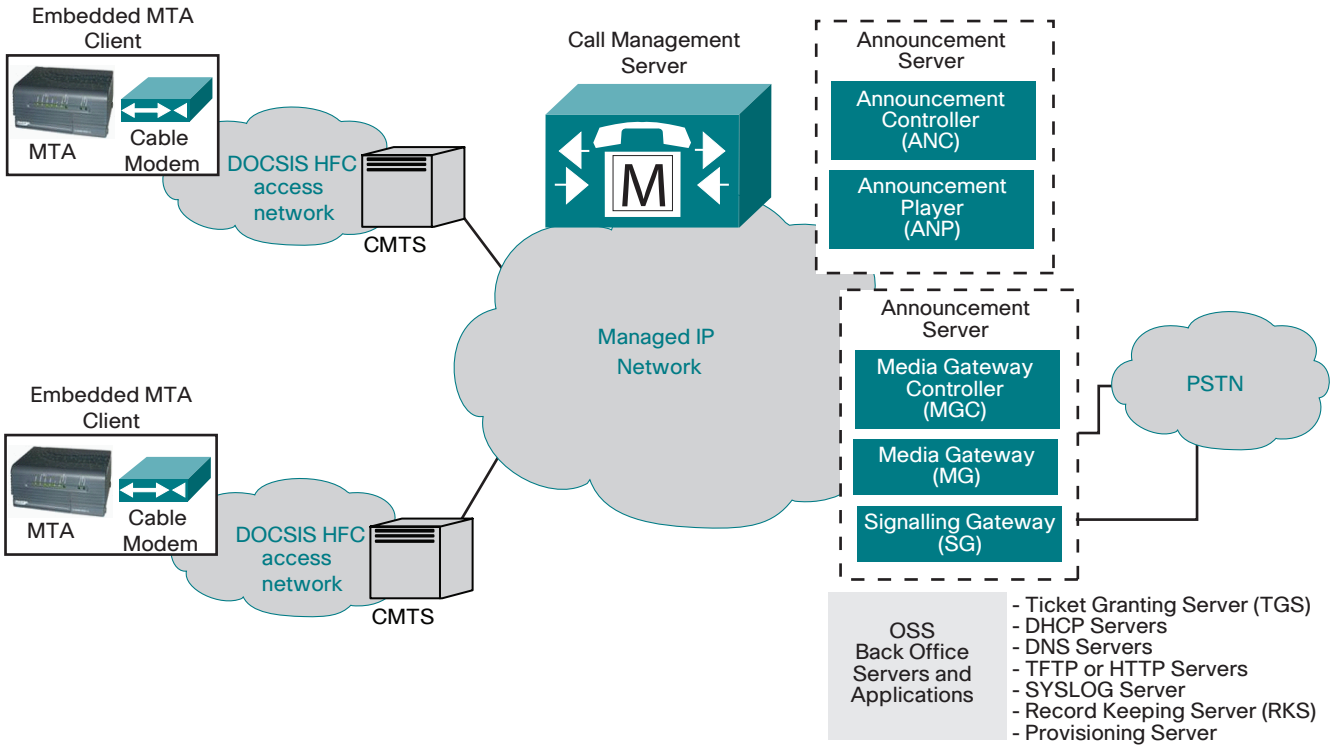
MGCP was created from two other protocols – Internet Protocol Device Control (IPDC) and Simple Gateway Control Protocol (SGCP). This protocol emerged in the Internet Engineering Task Force (IETF) in the late 1990s. In 2000, CableLabs® released its initial PacketCable™ specifications for MGCP/NCS, specifically created to enable cable operators to launch VoIP-based phone service over cable.

NCS includes much of MGCP, but there are differences as some items were added, some were deleted and some were changed. This being the case, MGCP/NCS is best thought of as the NCS profile of MGCP.

Standards

In 2003, the IETF announced RFC 3435, which made an earlier definition in RFC 2705 obsolete, and defined the base MGCP standard. PacketCable defines MGCP/NCS – the latest draft is PKT-SP-NCS1.5-I02-050812. Additionally, PacketCable defines many other specifications used to deploy VoIP services, such as device provisioning, common open policy service (COPS), dynamic quality of service (DQoS), security, management information bases (MIBs) and CODECs. MGCP/NCS is also supported for EuroPacketCable™ applications.

MGCP/NCS Network Diagram



MGCP/NCS Paradigm

The MGCP/NCS protocol is a master/slave-based protocol. Being such, it assumes an intelligent control point known as a call management server (CMS), or also referred to as a "softswitch." The CMS is operated under the control of a VoIP service provider, makes most of the decisions centrally and works with relatively non-intelligent endpoint devices

The CMS requests that endpoints notify the CMS if certain "events" are detected, such as off hook transitions, dialed digits (DTMF or pulse) and on hook transitions. If the endpoint detects the requested events, it sends "notify" messages to the CMS. The CMS then makes decisions and may instruct the endpoint to:

- Play signals (dial tone, caller ID, etc.)
- Create connections (setup audio packet streams with remote endpoints)
- Modify or delete connections

Common Uses

MGCP/NCS is used by the majority of cable-based phone service providers to provide VoIP phone service, and most Cable VoIP phone service providers use MGCP/NCS on embedded multimedia terminal adapter (EMTA) devices with integrated DQoS support. EMTAs are being deployed today in large numbers in North America and Europe, as well as other parts of the world.

The MGCP/NCS VoIP protocol is supported through CableLabs PacketCable and tComLabs EuroPacketCable.

SIP Protocol

SIP protocol origins began in academia, at Columbia University, in the 1990s and gained notoriety in 1996 when it was adopted by the IETF working group Multiparty Multimedia Session Control (MMUSIC).

SIP was originally intended to create a mechanism for inviting people to large-scale multiparty, multimedia conferences on the Internet Multicast Backbone (Mbone).

Today, SIP is used as a call signaling protocol for VoIP telephony, as well as many other applications.

SIP is a request-response protocol modeled after two Internet protocols – the Hyper Text Transfer Protocol (HTTP) and Simple Mail Transfer Protocol (SMTP). SIP is still maturing and evolving and is being nurtured by efforts from working groups within the IETF.

The standard SIP protocol is IETF RFC 3261, obsoleting RFC 2543. Other SIP RFCs which have been widely adopted by the vendor and operator community include: 2976, 3262, 3265, 3311, 3323, 3326, 3372, 3428, 3486, 3515, 3665, 3666, 3824, 3840, 3841, 3842, 3856, 3891, 3892, 3903, 3911, 3960, 4028 etc.

SIP Paradigm – Original Approach

Unlike MGCP/NCS, the SIP protocol is a user oriented protocol. But, like MGCP/NCS, SIP can be used in VoIP telephony applications to setup, maintain and tear down phone calls.

MGCP/NCS Call Flow - Simplified

User 1 phone	EMTA 1	CMS	EMTA 2	User 2 phone
offhook ->	NTFY ->			
		<- ack		
<- dialtone		<- RQNT		
	ack ->			
digits ->	NTFY ->			
		<- ack		
		<- RQNT		
	ack ->			
<- recvonly		<- CRCX		
	ack (sdp1) ->			
		CRCX(sdp1) ->		inactive ->
			<- ack (sdp2)	
<- recvonly		<- MDCX(sdp2)		
	ack ->			
<- ringback		<- RQNT		
	ack ->			
		RQNT ->		ringing ->
			<- ack	
			<- NTFY	<- offhook
		ack ->		
		RQNT ->		
			<- ack	
		<- RQNT		
	ack ->			
<- sendr ecv		<- MDCX		
	ack ->			
		MDCX->		sendrecv ->
			<- ack	

SIP is flexible and allows users to log on from any point on the Internet, while SIP applications allow users to log on from any device type or platform, without being tied to a particular piece of hardware. SIP was originally intended as a "peer to peer" protocol with direct communications between end users – for complete flexibility and control and no concerns about a service provider monitoring, controlling or billing for services.

This does, however, create a problem for service providers, as they often do need to:

- Monitor calls (the CALEA has strict governmental requirements for monitoring and reporting under court order)
- Monitor service demand vs. network capacity in order to ensure good quality service
- Control the network to setup DQoS to prioritize network access
- Control the network to prevent theft of service
- Bill for service in order to remain in business

SIP Paradigm – VoIP Telephony Approach

In light of these needs, most VoIP phone service providers prevent direct user peer to peer access by directing all access through a SIP proxy server. The proxy server (together with registration servers and application servers, as appropriate):

- Receives all SIP messages from endpoint devices
- Monitors traffic to meet CALEA requirements and balance service demands vs. available network capacity
- Controls network access

  - Allows only authorized users network access, eliminating theft of service

  - Authorized users can be provided with DQoS and other means of high priority access to help ensure good quality

  - Allows the service provider to trade off network bandwidth and call quality – the proxy server negotiates CODEC assignments, packetization intervals, etc.

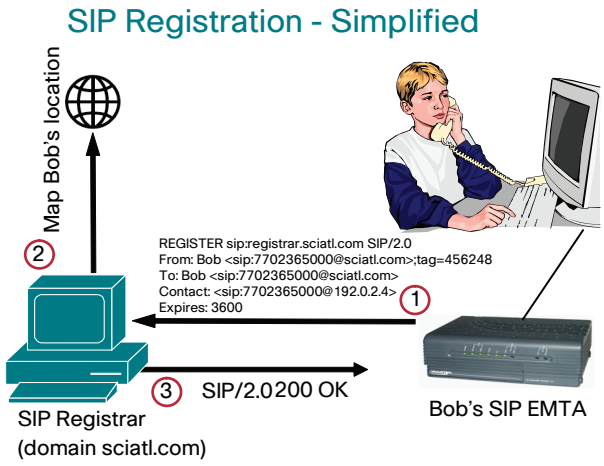
- Allows the service provider to bill for service

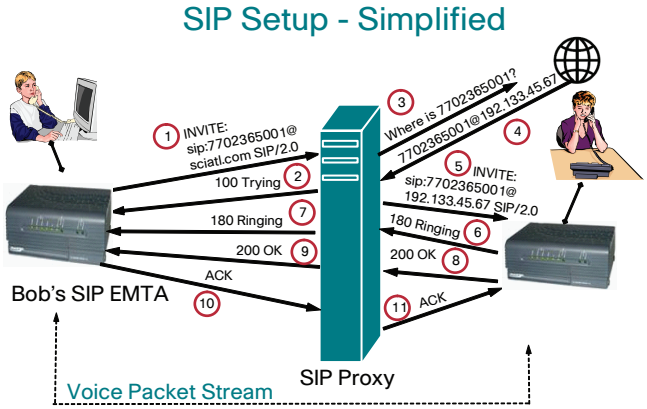
  - Per call charges have mostly disappeared in the United Sates, but remain common in Europe

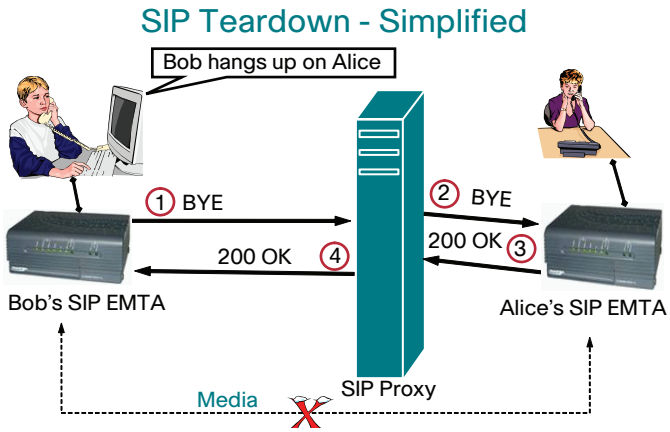
  - Almost all service providers charge for international calls to PSTN phone numbers

Some VoIP phone service providers limit user access only from within their own network. Cable based VoIP phone service providers and other "network based" providers often require that the VoIP subscriber be on the operator's network. This helps prevent theft of service, and enables the operator to provide good service by using DQoS, monitoring network capacity and adding bandwidth and PSTN access ports when "demand approaches capacity."

Non-Cable-based VoIP telephony service providers and other "non-network based" providers typically allow the service to be used anywhere. This results in several pitfalls – no "home" network, no ability to provide DQoS since the provider doesn't own or control the network and no ability to scale the network when demand increases







VoIP telephony service providers often tie users to a particular (unique) hardware device(s), resulting in several positive results. This helps prevent theft of service, as a particular device with unique embedded "keys" or certificates is required, and these unique keys or certificates are linked to the user's account. Furthermore, only the user can only access the service though this device meaning fraudulent users must actually take physical possession of the device to gain access to the service.

Tying the user to a unique device also results in improved support. Help desk support is faster, more efficient and requires less training for customer service representative if the CSR knows what device is being used by the consumer. This also means the CSR works with a limited number of device types to leverage training and familiarity with each type.

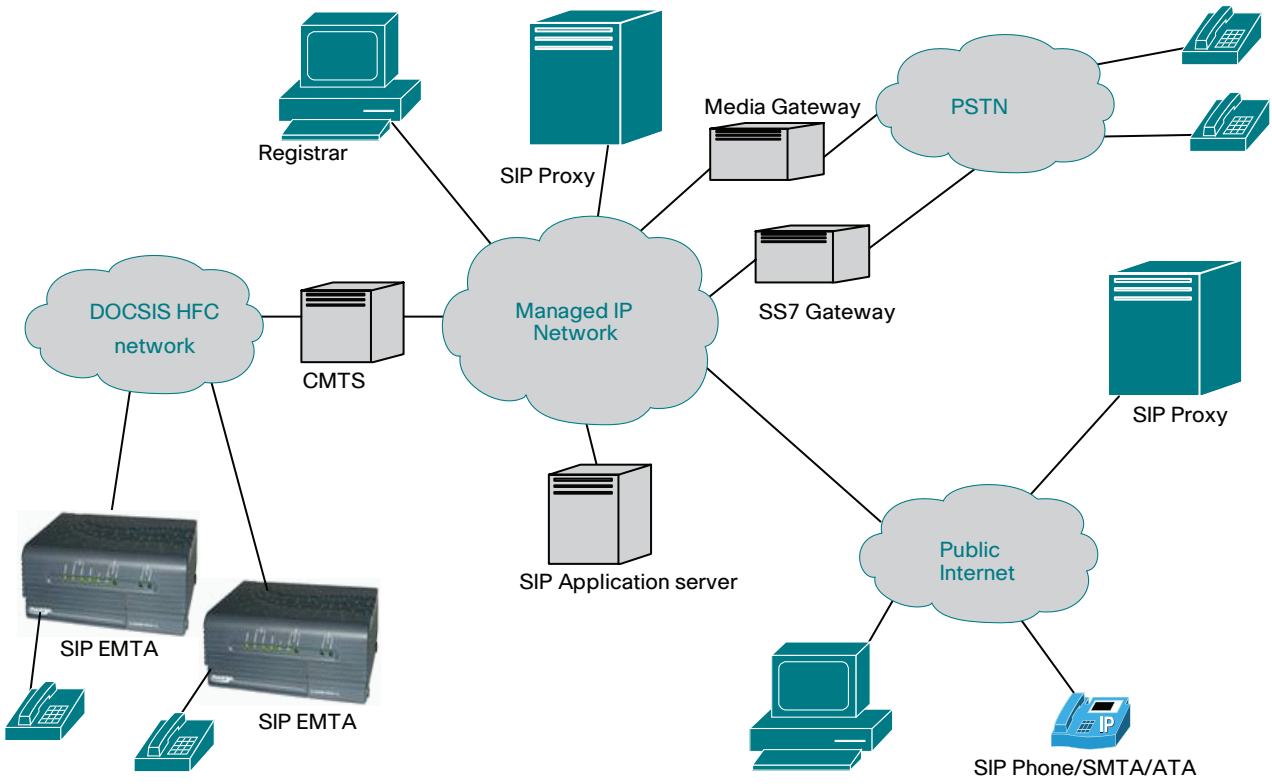
Common Uses

SIP is actively used by cable based phone service providers to provide VoIP phone service. To enable VoIP service, most cable VoIP providers use EMTA devices with integrated DQoS support to enable robust transport for voice packets. Currently, most SIP EMTA deployments are in Europe, and several hundred thousand SIP EMTAs are in active service. Additionally, PacketCable 2.0 committees are fully engaged with SIP.

SIP is also used by "non-network based" service providers worldwide. Most non-network based service providers use standalone multimedia terminal adapter (SMTA) or analog telephony adapter (ATA) type devices. And, PacketCable MultiMedia (PCMM) implementations promise to provide service providers with DQoS for these type devices on cable networks.

Of course SIP is not limited to VoIP, and SIP infrastructure could be leveraged in fixed and mobile networks for applications like instant messaging (IM), presence, video conferencing, voicemail, unified messaging, network games, push-to-talk, 3GPP IMS and much more.

SIP – Example VoIP Network Diagram



Advantages for Both Protocols

MGCP/NCS Advantages

MGCP/NCS features are controlled by a central CMS server. One advantage to a CMS server is that all users can receive a feature upgrade when the CMS is upgraded. Another advantage is that there is no need to upgrade software on all users' endpoint devices to add new features.

On another note, MGCP/NCS is a more mature platform for VoIP phone services. Because of this, it has been fully integrated into PacketCable and EuroPacketCable specifications. It also has the advantage of being designed from the beginning to specifically implement VoIP phone service.

As the mature platform, it is also fully integrated with secure network DQoS, billing applications, device provisioning tools and network management MIBs.

MGCP/NCS security is well defined and widely used. NCS has well defined and strong security mechanisms within the PacketCable specifications, and NCS security is increasingly deployed. As the more nascent protocol, SIP security is not yet widely used and not as well defined.

SIP Advantages

A major advantage of SIP over MGCP/NCS is that SIP may be more scalable as networks grow. Attributes contributing to this scalability include: use of less processing power on central servers,

more decision making distributed to the endpoint devices, and the fact that networks can scale by adding more processing power when more endpoint devices are added.

Another primary advantage is that SIP is inherently mobile and location independent. While SIP allows users to log on from anywhere and this flexibility may make the network more vulnerable to theft of service, tying the service to a physical device with unique certificates makes the service more secure.

SIP is also more extensible to other applications and services, with SIP software available on a wide variety of hardware platforms and client devices.

Defined as a generic "Session Initiation Protocol," SIP is not tied directly to VoIP phone service or any other application, therefore establishing a framework that many applications can use. Standards and specifications for new applications and services must evolve for multi-vendor networks to exist.

Conclusion

As evident, both SIP and MGCP/NCS protocols have certain advantages over the other. However, EMTA devices support both protocols today, and VoIP phone service providers can be successful with either protocol.

Service providers should be cognizant that while MGCP/NCS may be more fully integrated today, SIP may be more flexible for future applications. Service providers should also work carefully with equipment vendors to make sure that products fully support the service provider's business requirements, whether choosing an MGCP/NCS or SIP protocol.

Scientific Atlanta SIP EMTA

Scientific Atlanta's SIP EMTA offers service providers the features and flexibility they need to successfully deploy VoIP.

The Scientific Atlanta SIP EMTA

- Uses the same provisioning modes as NCS version
- Uses DQoS for calls to minimize audio latency and dropped packets
- Uses Scientific Atlanta MIB objects to configure endpoints and enable specific features
- Supports configuration file encryption
- Supports advanced call features
- Supports T.38 fax relay
- Interoperates with many RFC compliant SIP devices

Scientific Atlanta
A CISCO COMPANY

G1631A