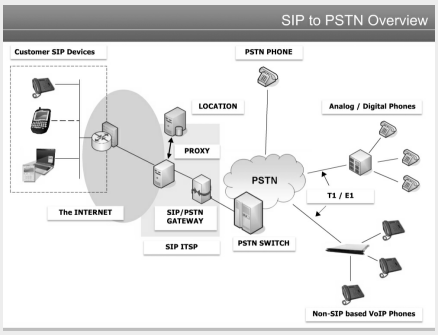
PSTN

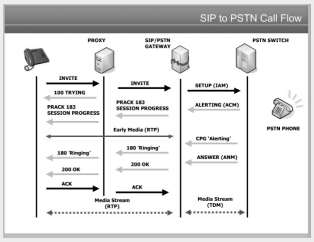


SIP to PSTN Overview

SIP devices communicate across an IP network connection such as the Internet to the Proxy at their ITSP

When the ITSP needs to direct calls to the PSTN, it forwards the calls to a SIP/ PSTN gateway that converts the signaling and voice media to the format the PSTN is expecting

SIP to PSTN call flow



SIP to PSTN call flow

SIP device dials the number of a PSTN device

The proxy sends the INVITE on to the SIP/PSTN gateway that will in turn send the appropriate SETUP message to the PSTN switch and onto the telephone

SIP to PSTN call flow (cont)

A provisional acknowledgement - 183 - informs the SIP device of the progress of the call setup and setup an early media channel

Once the phone starts ringing, the 'alerting' and '180 ringing' messages are sent back to the SIP device

When answered, the 'answer' and '200' messages are answered

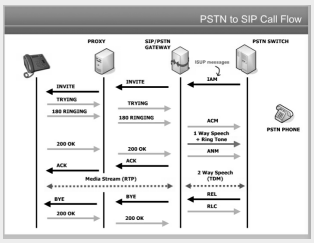
The media stream starts to flow after the SIP device sent it acknowledgements

The gateway convert RTP media to TDM media for the PSTN and vice versa

Both proxy and gateway can be used ambiguous depending on where they're being used and by whom, but ... A proxy generally talks SIP only (i.e. on both sides), and acts as a router for inbound and outbound requests (just like a web proxy). This might be required for security, NAT traversal or other reasons.

A gateway generally talks something other than SIP as well, such as a PSTN gateway which allows calls to and from the public switched telephone network which is based on TDM protocols such as ISDN or SS7.

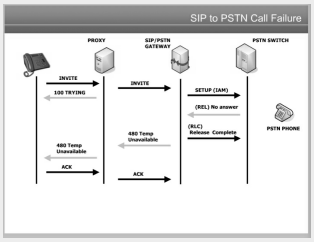
PSTN to SIP call flow



PSTN to SIP call flow

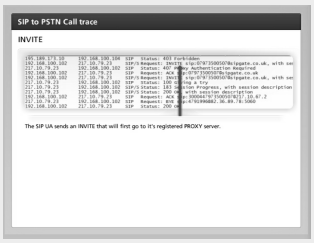
ACM	alerting
REL no answer	Release no answer
RLC	release complete
CPG	alerting, Call Progress (CPG) messages
ANM	answer
PRACK	provisional acknowledgement
ISUP	Integrated services digital network user part
IAM	Initial address message
NPI	numbering plan indicator, eg E.164

SIP to PSTN call failure

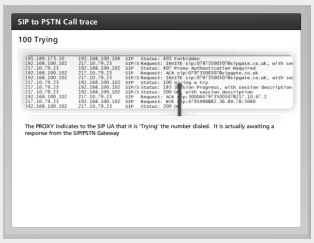


If a SIP device tries to call a PSTN phone and there is no answer, a Release No answer message is returned to the SIP gateway from the PSTN switch which acknowledges with a Release complete message. A 480 temporarily unavailable message is sent to the SIP device.

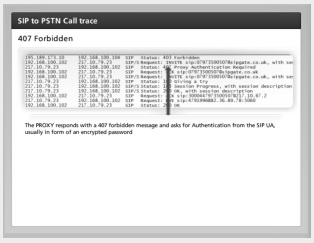
SIP to PSTN call trace



SIP to PSTN call trace

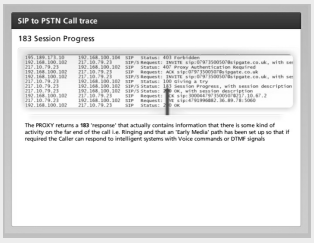


SIP to PSTN call trace

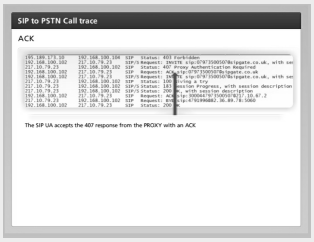


The proxy sent a 407 forbidden message that ask for Authentication from the SIP UA

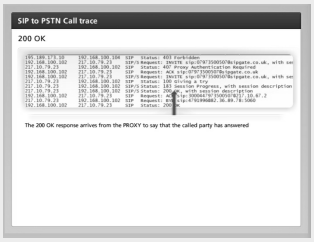
SIP to PSTN call trace



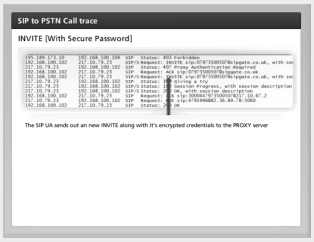
SIP to PSTN call trace



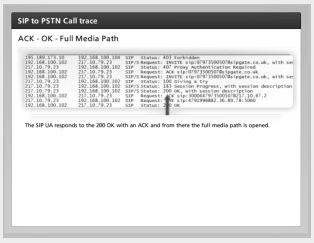
SIP to PSTN call trace



SIP to PSTN call trace



SIP to PSTN call trace



Early Media

To overcome a few problems that arise due to two different systems such as SIP and the PSTN trying to work together, a concept called Early Media has been introduced

Early media is not required on standard PSTN calls as when a number is dialed a media channel is established so the caller can hear the ringing tone of the remote device.

Early media gives companies the opportunity to replace ringing media with corporate messages or other instructions for the caller before they speak to a real person

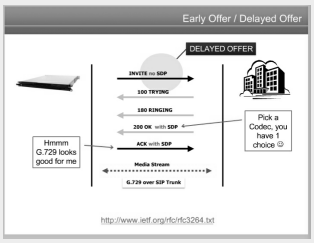
Clipping is a problem where if a person using a PSTN phone answers their phone and starts talking straight away, without Early Media the SIP phone that is calling them will miss the first part of the converstation as it hasn't yet received a 200 OK message to enable it to set up the RTP media path.

Early media also allow busy tone and other announcements to be played to the caller even though the called phone has not been picked up.

Early Offer

Early offer - the calling SIP device send an INVITE with the SDP body that includes contact info and a range of codecs that the SIP device supports. The receiving SIP device can then select a codec to use from the list offered, usually, the nearest one to the top and then the call is setup.

Delayed Offer



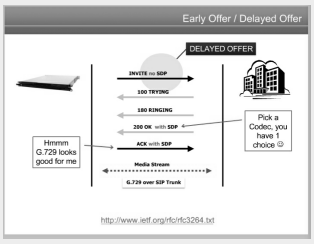
Maybe used in SIP trunk scenarios - the PBX sends an INVITE without an SDP body to the ITSP. The ITSP may only want the PBX to use the G.729 codec, si it lists only that codec in the 200OK. The PBX has only one choice and will then use G.729 for media across the SIP trunk.

Mini Quizlet

If you see a 407 error 'returned' from a Proxy Server to a SIP UA, what is the Proxy asking the SIP UA for ?

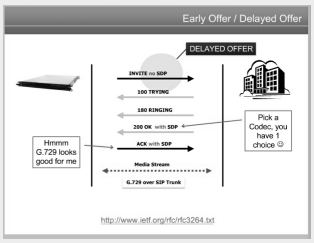
> The proxy sent a 407 forbidden message that ask for Authentication from the SIP UA

Default Gateway



A customer's default gateway is actually a default router.

Gateway



The SIP/PSTN gateway to the PSTN is to provide signalling and media conversion between the SIP and PSTN networks. When the SIP/SDP messages hit the signaling gateway it converts it to ISDN/ISUP signalling for the PSTN. RTP/RTCP media and control packets hit the media gateway for conversion to TDM for the PSTN
A single server may be running Gateway, proxy, location, registration services on it

TRIP - Gateway location and routing with TRIP

TRIP or telephony routing over IP intends to make it easy to find telephone number destinations and is achieved by using location servers that can advertise to each other their knowledge of gateways and the telephone numbers that these gateways support.

TRIP is protocol independent in that it can be used not only with SIP but also other protocols such as H.323

Gateways advertise their PSTN number range to a Location server, using TRIP protocol, that then advertises this range to other location servers.

The gateway tells the Location server of the numbers or routes that they can get to and their own contact details

TRIP - Gateway location and routing with TRIP (cont)

The Location servers then use Inter-domain routing updates to converge this info around to the other LS servers.

When a SIP client calls a number in another part of the world, the INVITE goes to the proxy. The Proxy may use ENUM to see if the number has a SIP location. If not, the Proxy forwards the SIP INVITE to the gateway. The gateway will check with the Location server to see which is the best Gateway to breakout to the PSTN. The Location server looks at its table and returns the relevan info to the Gateway. This then contacts the gateway at the remote end and the call is setup via that local gateway

TRIP is an emerging protocol that promises to do for SIP what BGP did for the internet in making it easy for SIP calls to be connected to most appropriate Gateway

Mini Quizlet

TRIP can help make it easy for gateways to find other gateways on a network thus enabling on-net communications. What does the R in TRIP stands for?

> routing

SIP-T SIP for telephones

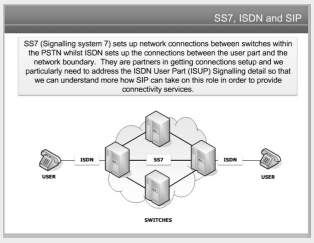
SIP-T is a framework that can enable SIP networks to carry legacy telephone signals across an IP based network to another legacy network.

The legacy SS7 ISUP messages have to be interrogated by the SIP/PSTN gatway and then the info that will help SIP proxies to route the SIP message is built into the SIP header while other ISUP info is added as a MIME message body. This message can be encrypted.

SIP INFO is another SIP-T approach or method that is used for in-call ISUP signaling across an IP network

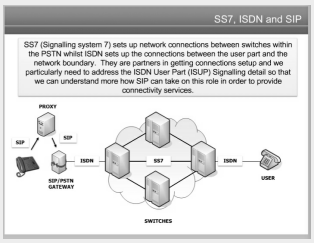
SIP-I (SIP with encapsulated ISUP) was developed by the ITU, not the IETF for SIP-T. It is more accurate than SIP-T

SS7

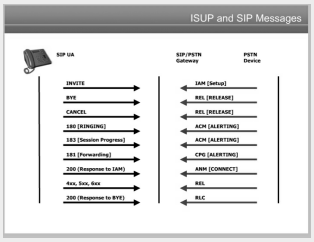


SS7, signalling system 7, sets up network connections between switches within the PSTN. ISDN sets up the connections between the user part and the network boundary.

SS7, ISDN, and SIP



SIP to ISUP messages



SIP to ISUP messages

INVITE	IAM , setup
BYE	REL, release
CANCEL	REL, release
180 ringing	ACM, alerting
183 session progress	ACM, alerting
181 forwarding	CPG, alerting
200 response to IAM	ANM, connect
4xx, 5xx, 6xx	REL
200 response to BYE	RLC

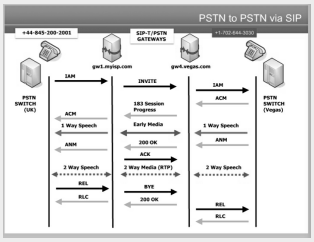
ISDN User part (ISUP) to SIP mapping

ISUP Event Code	SIP Message
1: Alerting	180: Ringing
2: Progress	183: Session progress
3: In-band information	183: Session progress

ISDN User part (ISUP) to SIP mapping (cont)

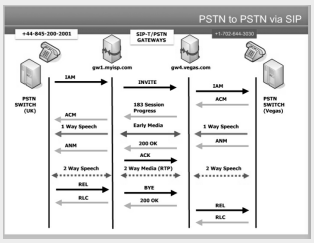
4: Call forward; Line Busy	181: Call is being Forwarded
5: Call forward; No Reply	181: Call is being Forwarded
6: Call forward; unconditional	181: Call is being Forwarded
ISUP Cause Code	**SIP Message**
1: Unallocated number	404: Not Found
2: no route to network	404: Not Found
17: User busy	486: Busy here
18: No user responding	408: Request timeout
21: Call rejected	403: Forbidden
28: Address Incomplete	484: Address Incomplete
34: No circuit available	503: Service unavailable
38: Network out of order	502: Service unavailable

PSTN to PSTN via SIP



PSTN to PSTN call via SIP is also known as SIP bridging

ISUP encapsulation



INVITE

ISUP encapsulation

VIA

ISUP encapsulation

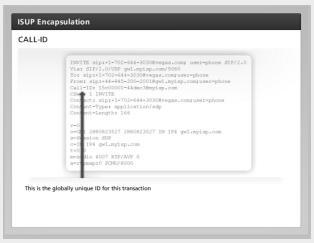
TO / FROM

To: shows who is being called
From: shows the detail of the caller's telephone number

ISUP encapsulation

CSeq used to identify and order the transactions

ISUP encapsulation



CALL- ID is the globally unique ID for this transaction.

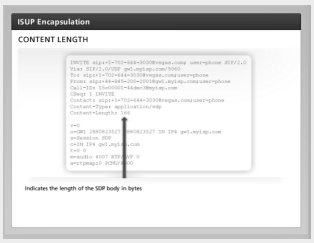
ISUP encapsulation

CONTACT gives info on who is being called

ISUP encapsulation

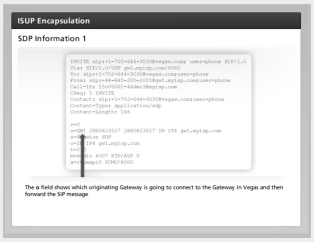
CONTENT-TYPE shows us that the SIP body is of the type SDP, session description protocol

ISUP encapsulation



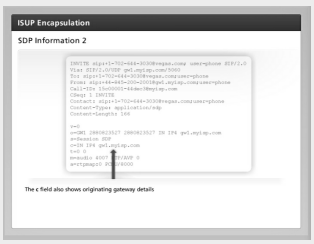
CONTENT LENGTH

ISUP encapsulation



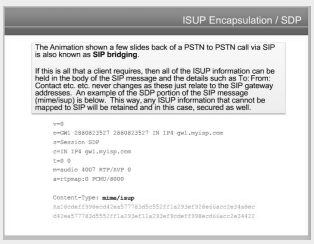
o shows originating Gateway

ISUP encapsulation



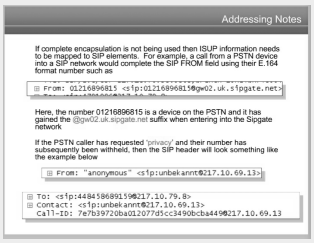
SDP **c** field also show originating gateway details.

ISUP encapsulation



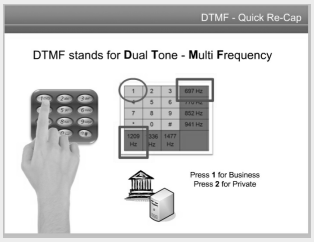
SDP content-type - any ISUP info that cannot be mapped to SIP will be retained, and in this case secured

Incomplete Encapsulation



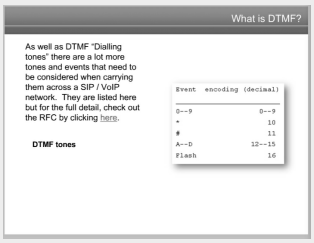
unbekannt means unknown in German
In anonymous PSTN calls, the transaction Call-ID will help the gateway to separate this session from other anonymous calls.

DTMF



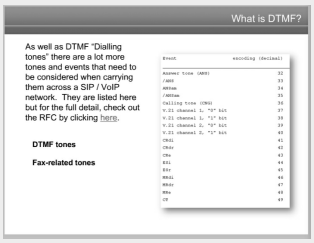
DTMF - dual tone - multi frequency
When you press the buttons on a telephone keypad, a connection is made that generates two tone at a time, a row tone and a column tone.

Tones over a SIP/VoIP network



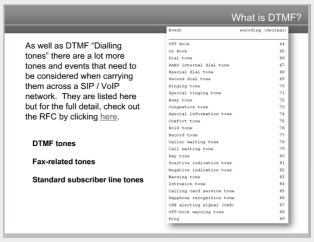
DTMF tones

Tones over a SIP/VoIP network



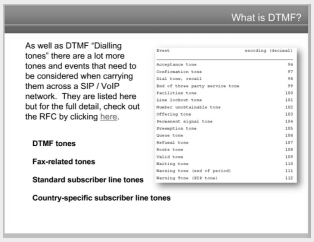
Fax-related tones

Tones over a SIP/VoIP network



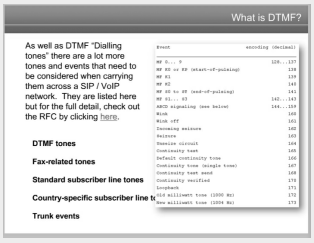
Standard subscriber line tones

Tones over a SIP/VoIP network



Country-specific subscriber line tones

Tones over a SIP/VoIP network



Trunk events

DTMF Transport methods

Inband	DTMF is transmitted in the same RTP stream as the media is.
	Some tones will be heard by parties in the conversation
	Only works when using G.711 codec or better. Compression codecs such as G.729, G723 may make tones unintelligible.
Out of band RFC 2833	Is an out of band method that takes DTMF out of the RTP stream and into its own RTP packets.
	DTMF codes can survive ok even if the main stream is compressed.
	The out of band RTP packets hold the various event codes and the tone is regenerated by an appropriate gateway or SIP UA
RFC 4733	build on and supersedes RFC 2833

DTMF Transport methods (cont)

	Requires that devices don't have to support every tone and event there is, just advertise what they do support when setting up a connection.
RFC 4734	updates 4733 with more event codes for modem, fax, and text telephony signals that get carried in the RTP payload
SIP INFO	method is used to carry session control info along the SIP signaling path during an existing session.
	SIP proxies can see and act upon SIP INFO messages and not DTMF Inband or RFC 2833 packets.
	Eg- a phone call to a bank, the session is established but you may get asked to type in an account number. SIP INFO carries the digits you type without changing the characteristics of the SIP session. RFC 6086

Module Quiz

The main purpose of a PSTN Gateway is to provide signaling and media translation services between SIP and the PSTN

> True

Which SIP method is used to carrying 'in-call' ISUP signaling acress an IP network

> INFO

Signaling paths

An

Voice over IP

In a VoIP system, all calls run over a shared network, this is known as packet switching. All voice calls are converted from analog signals to digital ones and transmitted over the network just like other data from PCs and servers.

Main transport protocols - TCP and UDP

TCP - transmission control protocol breaks data into packets, lebel them and send them out in order. On receipt the destination will acknowledge arrival. If an acknowledgment is not received within a set time data is resent. This guarentees delivery but can slow thing down a little

UDP - user datagram protocol is used to carry voice. There are no acknowledgements and no resends. This is the protocol of choice for real time applications such as video and voice.

Voice over IP (cont)

SIP RFC 3261 - all SIP elements must implement UDP and TCP. SIP elements may implement other protocols.

UDP is becoming obsolete because a lot of SIP products now produce headers that are too big for UDP. TCP is being used more because it has the ability to break up messages, re-assemble them at the destination and cope with packet loss with retransmissions.

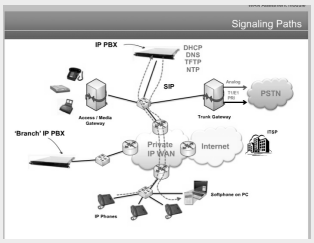
Microsoft's Skype for Business only support TCP for signaling.

Layer 5 Session - SIP messages

Layer 4 Transport - TCP segments

TCP segments has a maximum segment size of 1500 bytes.

Signaling paths



Signaling paths

An IP PBX consists of a call server/ manager that controls the calls

Usually the network supporting all the components of ah IP PBX is an Ethernet LAN. In some cases, the components can be remotely located over a WAN

Signaling paths (cont)

An access gateway is needed for supporting legacy phones, fax machines and other analog devices

Trunk gateway are useful for connecting to the PSTN/POTS network.

IP phones and softphones connect directly to the LAN or WAN

A router can be used to connect to other IP PBXs over an IP LAN or even SIP trunks of VoIP service

The calling device contacts the call server/manager which in turn the called device. This signaling path can operate with SIP or older standard H.323 or vendor's proprietary signaling protocol.

Signaling path does NOT carry the voice call.

All components of an IP PBX use IP addresses, the call server/manager or other servers must include DHCP and DNS functions.

TFTP is used to download software and configuration information to the IP phones, softphones and gateways.

A network time protocol (NTP) server sets the time clock for all the supported VoIP devices.

Speech paths

Once the call server/manager has determined that call call proceed, it established a peer-to-peer connection between the two endpoints, eg IP phone, softphone, gateways

This connecton uses the real time protocol (RTP) to carry the voice packets between devices

Speech paths (cont)

The call path is a point-to-point connection bypassing the call server/ manager.

IP PBX advantages

Single cable infrastructure	PC can connect into an IP phone and share the LAN connection
Flexibility in moving devices	Reconnect your phone to any other wall point and your number moves with you

Integration with IP applications

Integrated voicemail / auto attendant

Integration with unified messaging systems	For speech to text and text to speech conversion
SIP trunking	ability to migrate from PSTN connectivity to SIP trunking using VoIP

Encoding

Encoding is all about taking an analogue waveform, converting it into digital information before it is sent to the intended recipient

Encoding converts the orginal analogue signal into a binary data stream.

The encoder is set to take a reading of the wave - 8 thousand times a second, so 1 millisecond is going to be read or 'sampled' 8 times.

Encoding (cont)

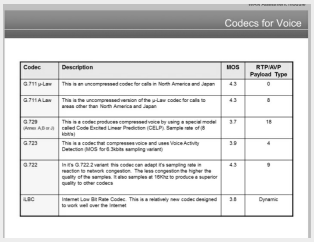
Digital telephony requires 64000 bits per second for normal speech quality

A codec that produces binary data at a rate of 64Kbps is usually working to the G.711 specification

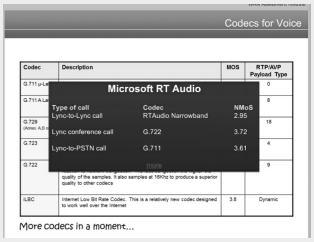
G.711 - uncompressed voice

G.729 - compressed voice (annex A/B/J)

Codecs of voice



Codecs for voice RTP payload type



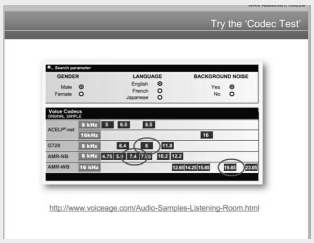
Codecs for voice

MOS - mean opinion scores	is used to get an idea of which codec sounds the best

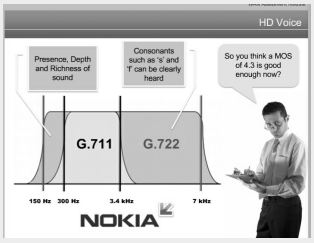
Codecs for voice (cont)

MOS	is a system of grading the voice quality of telephone connections. With MOS, a wide range of listeners judge the quality of a voice sample on a scale of 1(bad) to 5(excellent). The scores are averaged to provide the MOS for the codec.
G.729 codec	compresses voice so that it is possible to use less bandwidth for each call
RTP/AVP payload type	Value that is used with the body of a SIP and SDP message in negotiation between SIP system to decide which codecs they support and are then going to use for that voice session.
Microsoft Lync	supports standard codecs. However, it has its own real time (RT) audio.
Network mean opinion	Microsoft uses a measurement called network mean opinion scores

Codec test

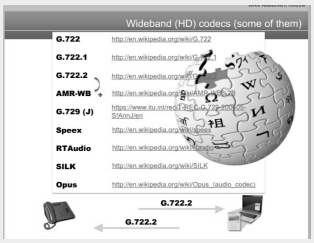


HD Voice



G.722 samples a much larger or wider frequency range to catch depth of voice and also at the higher end. Constants such a 's' and 'f'can be hard to catch with a narrow band codec.

Wideband HD codecs



Wideband HD codecs

G.722	Range from G.722 to G.722.2. Also know as adaptive multi-rate wideband

Wideband HD codecs (cont)

ARM-WB+	Proliferating in many VoIp phones from companies such as Polycom, Avaya, Snom, Mitel
G.729 (J)	G.729 with annex J is now a scalable wideband codec
Speex	Popular wideband codec because of being open source
RTAudio	Microsoft owned
SILK	Skype ultra wideband codec is now available as open source
Opus	is open source and gaining in popularity. It is the preferred codec for WebRTC

Opus

Opus is a new codec for interactive speech and audio transmission over the Internet.

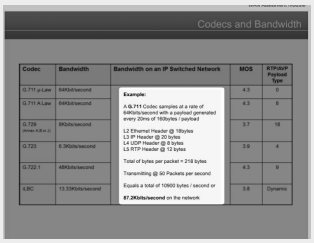
It is designed by the IETC codec working group and incorporates technology from the Skype 'Silk' codec and Xiph.org CELT codec technology

The OPUS codec is designed to handle a wide range of interactive audio applications, including Voice over IP, videoconferencing, and even remote live music performances

Implementing OPUS in VoIP will allow interoperability with new WebRTC enabled browsers and devices without any transcoding required

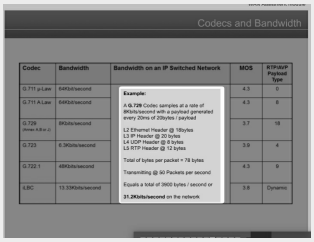
OPUS can change bandwidth and bitrate seamlessly without any glitch

Codecs and Bandwidth



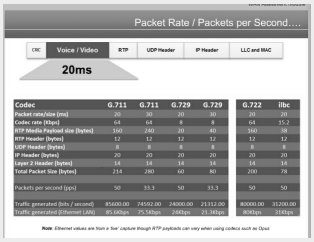
G.711 generates 87.2 Kbps on the network

Codecs and Bandwidth



G.729 generates 31.2 Kbps on the network

Packet Rates / packets per second



Packet Rates / packets per second

Codecs are responsible for breaking up the voice stream into chucks for packaging in RTP packets. The size of these chunks is know as Packet Rate

Most installations use packet rate or size of 20ms for the voice or video element when sending a stream of data

Packet Rates / packets per second (cont)

You sometime have the option of selecting a different rate, ie 30ms. The effect of increasing this size of the voice/video element is clear as it increases the size of the overall packet. This means that less packets will be required to deliver the same amount of data to the recipient.

Reducing the packet rate means that less work needs to be done on routers when it comes to analyzing IP addresses, checking QoS settings. It does also mans that packet loss can be more apparent to users as there is more information in a larger packet which if lost, results in a larger gap in a voice stream.

If you are using a codec such as OPUS, you may see in Wireshark traces that the packet sizes vary from pakcet to packet. This is because the codec is adapting to network conditions. This is known as variable bit-rate codec

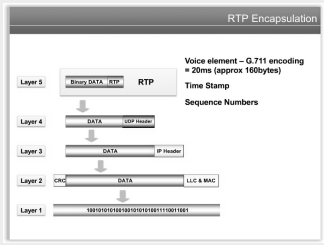
RTP

RTP	is designed to support real-time traffic such as voice and video that is time sensitive
	It can work with both Unicast and Multicast applications

RTP (cont)

It provides services that include info such as	Payload type identications
	Sequence numbering
	Timestamps
	Delivery information
RTP	runs over UDP because TCP is not good for real time operation
RTP	does not provide any service that guarantees timely delivery of the payload
	does not provide any quality of service guarantees
	does rely on other protocols to provide these extra services

RTP Encapulation



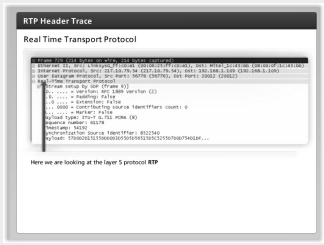
RTP Encapsulation

RTP	orginally designed to support video conferences with multiple, geopraphically dispersed participants and is now commonly used in Internet telephony applications
	does not guarantee real-time delivery of multimedia data since this is dependent on network characteristics.
	provide infomation that receiving devices can utilize in recontructing data received.
	Information in the RTP header tells the receiver how to reconstuct the data and describes which codecs are being used along with the very useful timestamp and sequence number
Layer routing - layer 4 & 5	RTP is sent to UDP
Layer 3	Then IP for addressing

RTP Encapsulation (cont)

Layer 1 and 2	Then Ethernet layer for more addressing before being sent out onto the network

RTP header trace



RTP Header Trace

Layer 5 protocol RTP

The first two bits of the RTP header donate the version of RTP. ie version 2

The next bit donotes is there is padding at the end of the payload. Sometimes padding is needed in order for things like encryption to work

The next bit is the extension bit. If it is enabled then RTP header is followed by one extra header extension

The next 4 bits are used to denote how many contributing sources there are. Useful for mixers at the receiving end if multiple streams of RTP are arriving. Usually set to 0 in a single VoIP call

The next bit is the marker bit which is used when events such as DTMF tones, volumes and other states that will effect the RTP stream need to be carried in the payload. eg 911 call

RTP Header Trace (cont)

The 7 bits denote the paylad type, the type of codec being used. ie G.711 type 8

The sequence number is used by the receiving device to detect if there is any packet loss and to put received packets in order. The initial value in a session is random and for each RTP packet it is incremented by one.

The timestamp is used to place the received audio in the correct timing order. A timestamp initial value is random and in the case of G.711, 20ms x 8kHz = 160 sampling instances per RTP packet. eg. the timestamp will increment by 160 for each RTP packet. In this stream, the next RTP header will show 54352

32 bits are used to identify the synchronization source. It is a random value with the intention that no two synchronization sources within the same RTP session will enven have the same SSRC id.

Payload of the encoded voice element

Real Time control protocol

The real time control protocol (RTCP) can be used alongside RTP in order to provide informaiton on the session and participants

Real Time control protocol (cont)

RTCP carries an ID for a device that is transmitting the RTP data and this is called a canonical name of CNAME, alias. If the synchronization source changes, such as when another stream is beingin introduced from the same device or machine, the CNAME remains the same. This helps to identify participants in a session and is useful as these participants can join and leave sessions dynamically

RTCP XR is a VoIP managment protocol that defines a set of metrics that contain information for assessing VoIP call quality and diagnosing problems.

RTCP XR is used defined in RFC 3411

RTCP XR messages containing key call-quality related metrics are exchanged periodically between IP phones and gateways and this allows analyzing equipment to monitor these metrics to assist in call quality analysis and troubleshooting

The protocol measures VoIP call quality using these following key metrics:

1. Packet loss and discard rate and the distribution of lost and discarded packets

2. Round-trip delay

3. Signal, noise and echo levels

4. Call quality in terms of estimated R factor or mean opinion score (MOS)

5. Configuration data such as jitter buffer size and configuration, and the type of packet loss concealment algorithm in use.

Real Time Control Protocol

Real Time Control Protocol (RTCP) can be used alongside RTP in order to provide information on the session and the participants

Types of RTCP packet are:

SR- this is the sender report. Showing statistics on transmission and reception for the participants in the session that are actively sending data

RR- this is the receiver report and it shows the reception statistics from participants that are not actively sending data in the session

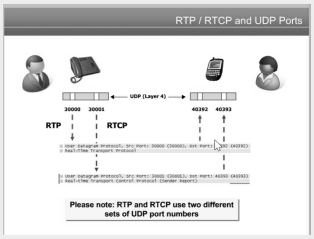
SDES - the source description items including identifying information such as CNAME and allows the binding of an SSCR value with an actual id of the user.

GOODBYE - this indicates end of participation in a session

APP - this denotes Application specific functions that will effect/interact with the session

XR - an RTCP extension that can help provide a 'rich set' of data for voice management - if it is implemented VoIP devices

RTP / RTCP and UDP Ports



RTP use dynamically allocated UDP ports to send and receive traffic across. Ex. the sending port is 30,000,, the receiving port is 40392. RTCP will use UDP ports dynamically as well, but actually resulting in the RTP port value plus 1.

QOS quality of service

QoS is not a single mechanism, it can be achieved if all the elements in the network WAN provided network recognize real time communication streams and give them the treatment or priority they need in order to get to their destination on time.

Quizlet - quality

The system that evaluates 'voice quality' gives you a value known as the MOS. What does the MOS stand for?

> mean opinion score

QoS Issues

Within the LAN and WAN, voice quality is dependent on four components:

Delay - one way end to end voice delay should be no more than 150ms

Delay will be different for every site dependent on the network installed.

The International Telecommunication Union Telecommunication Standardization Sector (ITU-T) G.114 recommendation specifies that for good voice quality, no more than 150ms of one-way, end-to-end delay or latency should occur.

Most manufacturers recommend that end to end delay be no more than 200ms. Of this 200 ms up to 80ms when an IP set is connected through an IP PBX. Allowing for up to 40ms delay in the PSTN without echo cancellation leaves 80ms available for use in the customer's network.

QoS Issues (cont)

Jitter - no more than 30ms

Packet loss

Bandwidth

Test for delay and jitter with Ping -l; eg pinng -l 218 134.199.192.1 G.711 voice frame 238 bytes

Network delay happens in various locations such as:

1. Hardware delays through the network

2. Variable delays, eg router queues

3. transmit delays- the time to traverse network

4. processing delay in the end devices

Jitter is the variation in delay from the expected value.

Jitter can occur from many of the network problems that cause delay like router queues, over utilized devices, poor cablings

IP phones are able to manage around 30ms of jitter

A packet of data leaves a phone at exactly 20 ms intervals using G.729 an on average they arrive at the destination phone every 20 ms. A jitter buffer at the receiving end copes with irregularities of the network. This is a buffer that holds each packet just long enough to allow packets to emerge at precisely 30 millisecond intervals

Packet loss means that a voice packet was sent, lost in transit and the far end never received it. Speech quality is usually not affect if packet loss stays below 5%

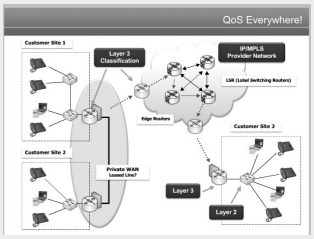
QoS Issues (cont)

http://www.voiptroubleshooter.com/problems/jitter.html

General VoIP acceptance criteria

Green - good quality
Amber - caution, may need to make adjustments on the network
Red - poor quality

Qos



Voice packets reaching a LAN switch can be seperated from Data traffic by utilizing VLANs and giving priority across uplinks using layer 2 classification.

At the router, layer 3 classification needs to be implemented to prioritize real time traffic.

Providers use MPLS to prioritize traffic within their network.

802.1Q - vlans

Benefits of configuring VLANs:

1. separate traffic for securitiy

2. separate traffic for broadcast and traffic control

3. separate traffic due to different characteristics, ie data and voice

802.1Q VLAN tagging ensures that while a frame is within the switch infrastructure it stays within its own VLAN

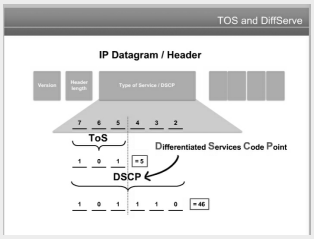
The switch will tag the frame with a VLAN ID and priority value for its life with the switched network.

The priority value 802.1P value ensures that frames can get priority over less important frames when faced with interswitch, shared link.

802.1P - L2 Classification

Layer 2 classifications is at the output or egress port of a LAN switch.

TOS and diffserve



When an IP datagram hits a router, the layer 2 classification is lost and the router has to rely on Layer 3 classification.

Older routers only recognize the first three bits in the 'type of service' field of the IP header. Newer systems recognize 6 of the bits known as the diffserve or differentiated service code point setting.

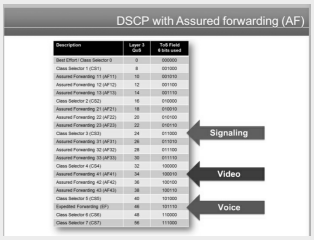
Layer 3 classification

Default for all differentiated service value IP datagram is 0.

A lot of VoIP manufacturers set their IP phones voice datagram value to 46, high priority RTP traffic

At the router, traffic is classified based on the diffserve value. RTP traffic goes into high priority EF or expedited forwarding queue.

DSCP with assured forwarding (AF)



Routers use assured forwarding to identify packets for forwarding.

DSCP with Assured Forwarding (AF)

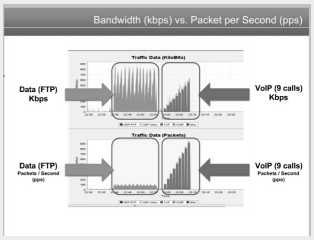
Class selectors are useful because even if a packet hits a router that only sees the 1st 3 bits of the DSCP string, the packet can still be classified and allocated to a queue.

eg Class 4 (CS4) you see that AF41 means Assured forwarding, Class 4 with a drop precedence of 1

1 means its the most important within its own class so packets marked with AF42 would get dropped first.

Class 4 is higher than class 3. Packets marked AF43 would take priority over packets marked AF31

Bandwidth (kbps) vs packet per second (pps)



Extra bandwidth is not always the answer.

Ex. the equipment cannot handle the number of packets that needs attention first.

The top diagram shoes that data traffic consumes a lot of bandwidth in a bursty nature. VoIP traffic consumes bandwidth in a constant fashion.

The bottom diagram shows that VoIP calls create the majority of packets on the network. The router needs to process all these packets in real time.

Port assignment

HTTP	port 80
RTMP (flash)	port 1935
BitTorrent	port 6999
HTTPS	port 443

Issues that can affect QoS

WAN router/ firewall congestion due to packet load / not enough packet handling capacity

Bandwidth hogs causing poor VoIP quality

Packet loss due to cabling or poorly configured issues at T1/DSL router

Poor quality wiring network deployed over a number of years. Can cause issues such as delay, packet loss

Issues that can affect QoS (cont)

Old firmware on IP phones. Phones sitting in warehouse, 1 or 2 versions behind.

DNS performance issues. Critical for VoIP as used for call setup

Switch duplex mismatch. Full duplex for IP phones and inter switch connections

Router flaps are where constant changes in route path of a call stream results in jitter. This could be caused by traffic engineering in place for load balancing.

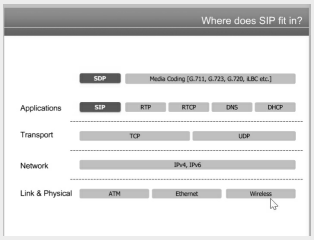
to determine how many SIP trunks over a trunk
http://voiptest.8x8.com/

Quizlet

Using DSCP values to manage voice traffic across a network device- usually a router, is known as

> Layer 3 classification

SIP SDP and VoIP



SIP INVITE Analysis

In order for RTP to work properly it needs the devices in the session to organize themselves regarding UDP ports, codec selection and other factors relating to the impending session.

SIP INVITE Analysis (cont)

Port 5060 is the default UDP port for SIP communication

The **sendrec** attribute specifies that the SIP devices should start off in send and receive mode.

SDP wireshark eg audio 20016 - media is audio and the UDP port is 20016 that the device is advertising to receive Voice or RTP packets. Another media type is video

SDP wireshark eg RTP/AVP 0 8 18 96 - the real time protocol / audio video profile element is included so that a device can inform a receiving device of the codecs it supports. The first listed is the default.

SDP wireshark eg rtpmap:8 PCMA/8000- The rtpmap element describes a little more detail of the codecs being advertised. 8 is the G.711 Alaw codec samples at 8000Hz

SDP wireshark eg rtpmap:96 telephone-event/8000 - the rtpmap is a dynamic value. It is offered as an extra stream alongside the audio stream used for telephone events - usually DTMF digits.

The offical format of rtpmap is [a=rtpmap: <payload type> <encoding name>/<clock rate> {/<encoding parameters>

SIP SDP 200 OK analysis

200 OK is a positive message saying that all is ready to go with the session

eg audio 56828 - the remote SIP device advertises the UDP port that it want to receive RTP audio on.

SIP SDP 200 OK analysis (cont)

eg RTP/AVP 8 0 18 96 - RTP/AVP codecs are listed and 8 is the first one listed, this will be the one that is now used for this session

8 is G.711 ALaw

eg fmtp:18 annexb=no - the fmtp attribute allows parameters that are specific to a particular format to be conveyed in a way that SDP doesnt have to understand them.

SDP doesn't have to understand fmtp:18 annexb=no, it simply passes the information between SIP devices and hopes that they understand.

eg fmtp:96 0 -16 - fmtp-entry shows that the SIP device supports up to 16 DTMF digits. If this entry is not present it is assumed that only 15 digits are supported

SIP devices do not have to send RTP packets if there is nothing to send. eg silence in a conversation

eg silenceSupp:off - turning off silence suppression means that RTP packets are sent even for those silent moments. Off is also the choice is transmitting other data such as Fax over IP

The nortprpoxy attribute tells us if the remote SIP device is using an RTP Proxy.

eg nortpproxy:yes - no proxy is being used.

Streaming video and video - 1 way tranmission

RTSP- real time streaming protocol - is the protocol used to carry video

RTSP runs over UDP, therefore there is not mechanism to compensate for packet loss

RTSP at the receiving end has a large buffer what can store several seconds of video. The buffer can compensate for the IP network impairments but it will cause a startup delay in the transmission.

High packet loss over 5% can cause noticeable picture distortion. Lost packets can also affect the sound quality.

Some implementations have implemented RTSP over TCP to compensate for packet loss. This delays the transmission and makes the TCP based devices incompatible with the rest of the RTSP implementations. RTSP running over TCP will very likely be blocked by firewalls.

Two-way conferencing with RTP

Video conferencing is a real time two way conversation. There cannot be a significant delay added by jitter buffers at each end of the call.

Smaller jitter buffers will force IP network designers to keep jitter in check on the network.

Once jitter exceeds 60msec, the receiving device will probably not be able to compensate and therefore the end device will discard packets thereby affecting the video quality.

Two-way conferencing with RTP (cont)

A larger jitter buffer could solve the problem but add more end-to-end delay which is not acceptable.

Video codecs - H.263, H.264, H.265 licensed

Video codecs - VP8, VP9 free

Frame rates - 15fps, 30fps, 60fps

Resolution - standard, HD=1920x1080, ultra HD, 4K

Better quality usually means more bandwidth

QoS tagging video is important

Video bitrate calculator - https://toolstud.io/

m:audio for voice, eg codecs Opus, SILK

m:video for video eg codecs offered VP8 , H263

Assured SIP (AS-SIP) services

Assured SIP services	is an open standard published by the IETF developed by a US Defense organization
AS-SIP	includes all the standard functions of SIP but with the added functionality of data packets being prioritized over other traffic on an netowrk
	all packets are encrypted

Assured SIP (AS-SIP) services (cont)

Service provider architecture	UA sends its calls to a proxy that takes care of all the calls for all the UAs in a particular domain.
	The proxy is acting as a servic provider and adding the specific AS-SIP features of security
	Prioritization of traffic is handled by another device called an access router
Assured SIP services	requires TLS to secure all SIP signaling and SRTP to encrypt all media.
Assured SIP services defines a network architecture that is	built to carry secure signalling and media within a domain or area
	with MLPP defines how important calls can get through
	using Priority - user defined /Network defined

Assured SIP (AS-SIP) services (cont)

SIP is extended with the use of the Resource priority header

accept priority header

Reason header for pre-emption

open standard

Proxy and Access router functions

Proxy functions

processing authentication requests

maintaining the state information of all existing sessions including their priority which exists on all UAs under the proxies control

Understanding / maintaining other services being used by the UA which might need to be taken into consideration when applying AS-SIP capabilities

Verifying originating UA is actually allowed to establish the session at the re:Precedence/priority level requested

Working with the access router - establish permission at the access router for it to handle the precedence marked packets from the UA

When to pre-empt - deciding when to preempt the end user and sending the appropriate pre-empt messages to the other party.

Maintain all records of the service, whether for accounting, auditing, or other purposes.

Access Router under control of the proxy

Proxy and Access router functions (cont)

Transfer packets - decides which packets are to be transported between networks or domains. If access is not granted, the access router will throw these packets away

Packets, pass or stop? - sometimes a live packet stream must be stopped. Since the assured service may not be able to rely on the UA to stop the flow, it may be necessary for the access router, under the control of the proxy, to stop carrying a particular flow of traffic.

AS-SIP network Resource-priority calling

For resource priority to work, the Require header in the SIP message should state that resource-priority be used. eg INVITE message Require: resource-priority

Resource-priority header contains namespace and priority known as the r-priority values.

eg Resource-priority:dsn.flash -the namespace is dsn, which was defined by a US government network called "the defense switched network". Within this namespace there are five priority levels defined.

Namespace

DSN	Defense Switch Network
(lowest)	dsn.routine
	dsn.priority
	dsn.immediate
	dsn.flash
(highest)	dsn.flash-override

Namespace (cont)

DRSN	Defense RED Switch Network
(lowest)	drsn.routine.drsn.priority
	drsn.immediate
	drsn.flash
	drsn.flash-override
(highest)	drsn.flash-override-override
q735 namespace	Commercial equivalent of the DSN namespace for Multi-level precedence and pre-emption (MLPP)
	Is used by signaling system 7 (SS7) networks based on ITU q.735.3 and thus can be mapped between IP and ISDN networks
(lowest)	q735.4
	q735.3
	q735.2
	q735.1
(highest)	q735.0
ETS	name of the US government telecommunications service called "Government Emergency Telecommunications Service"
(lowest)	ets.4
	ets.3
	ets.2
	ets.1
(highest)	ets.0

Namespace (cont)

WPS	Wireless priority service defined in GSM and other wireless technologies
(lowest)	wps.4
	wps.3
	wps.2
	wps.1
(highest)	wps.0

Namespaces detailed in RFC 4412

200OK Accept-Resource Priority

Response to a resource priority header

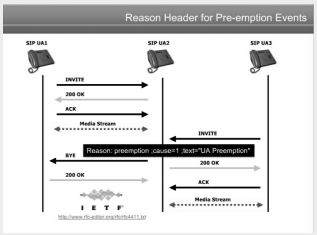
200 OK message will have Accept-Resource-Priority along with the namespace and r-priority value

If the called party does not support the proposed resource priority details, it can respond with a 417 unknown resource priority message with different namespace and values.

eg Accept-Resource-Priority: q735.0, q.735.1, q.735.2, q.735.3, q.735.4.

The calling party has a choice to accept and resend a q735 value in a new INVITE or decide that it cannot or will not work outside of it's own namespace.

Reason header for pre-emption events



Reason header can help the phone inform the user by a message or a tone that the call has been dropped. eg UA2 sends a BYE message to UA1 which includes a 'Reason' code to indicate why the call was dropped.

AS-SIP proxy

Proxy receives SIP messages from SIP UAs

-Proxy receives message

-Doesn't recognize namespace defined in message, it will ignore,drop the message

-Does recognizes and authorized it uses the priority levels. If it does not know the namespace and the UA has been authorized it will use the priority levels in the message

-Not authorized, it is ignored. If the UA is not authorized, the message is rejected.

-If UA doesn't have a priority level set, the proxy can assign a default

-If auth and resources are all ok and available to send the message, then the message treats as normal and sent.

-If auth and resource not available- priority is utilized.

-Proxy maintains state of all sessions.

MLPP Multi-level pre-emption and precedence

The principle of MLPP or multi-level pre-emption and precedence is that more important calls override less important calls.

MLPP is built as proactive system in which callers must assign a precedence level at call initiation, this precedence level cannot be changed throughout that call.

If there is end to end capacity to place a call, any call may be placed at any time.

MLPP Multi-level pre-emption and precedence (cont)

When any trunk configuration reaches its capacity, a choice must be made as to which call can continue.

The system will seize the trunks or bandwidth necessary to place the more important calls by pre-empting an existing call of lower precedence to permit a higher recedence call to be placed.

The main elements of MLPP are: A VoIP implementation of an MLPP service must provide these characteristics.

Call admission/pre-emption policy. If a call is in place with lower priority than a newer call, it must make way for the newer call, it must make way for the new call according to the policy/procedures defined for the network.

All callers that have been pre-empted to make way for the new call must be informed that their call has been pre-empted, and have to make way for the higher precedence call.

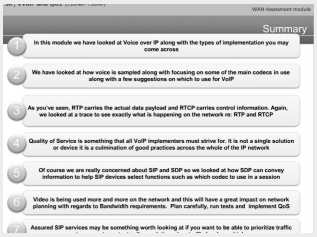
Bandwidth admission policy Many calls could be active but bandwidth available may change. There must be a bandwidth policy in place that will manage the bandwidth available based on the levels of precedence marked in the message.

MLPP Multi-level pre-emption and precedence (cont)

Authorization of call placed Calls can be made using a higher level of priority by either inputting a specific priority code before a number or setting variable on the SIP UA via policies so that the caller always has a minimum priority level

Defined user interface If a call is pre-empted, the caller and callee are notified via a defined signal, visual message or tone, to that they know that their call has been pre-empted and there is no bandwidth available

SIP VVoIP QoS summary



Quiz

Causes of jitter

> over utilized LAN switch trunking ports; poor cabling;

Packet carrying actual voice are transported using UDP

> UDP

RTP stands for

Which codecs have a MOS of 4.3

> G.711 Alaw; G.722; G.711 U-law

Quiz (cont)

layer 2 classification is something routers will use to prioritize VoIP packets across a WAN link

false

Packetization rate is always fixed regardless of ITSP providing your service

false

What is the default port for SIP messaging

5060

what kind of info would rtcp generate on a network

sender report; application specific functions for a RTP session

G.711 uLaw

64Kbps

G.729a

8Kbps

iLBC

13.33Kbps

G.722.1

48Kbps

How many bits can be used with a layer 3 DSCP

6 bits

Which port number the SIP device wants to receive RTP packets - audio 20016 RTP/AVP 0 8 18 96

20016

Which signaling protocol would allow a cisco ip phone to commuincate with a mitel pbx

SIP

Which is the 802 specification for vlans

802.1Q

Quiz (cont)

EF stands for enhanced forwarding when implemented on a route for re:QOS configuration

false - expedited forwarding

G.711 uLaw

0

G.729

18

G.722

9

iLBC

dynamic