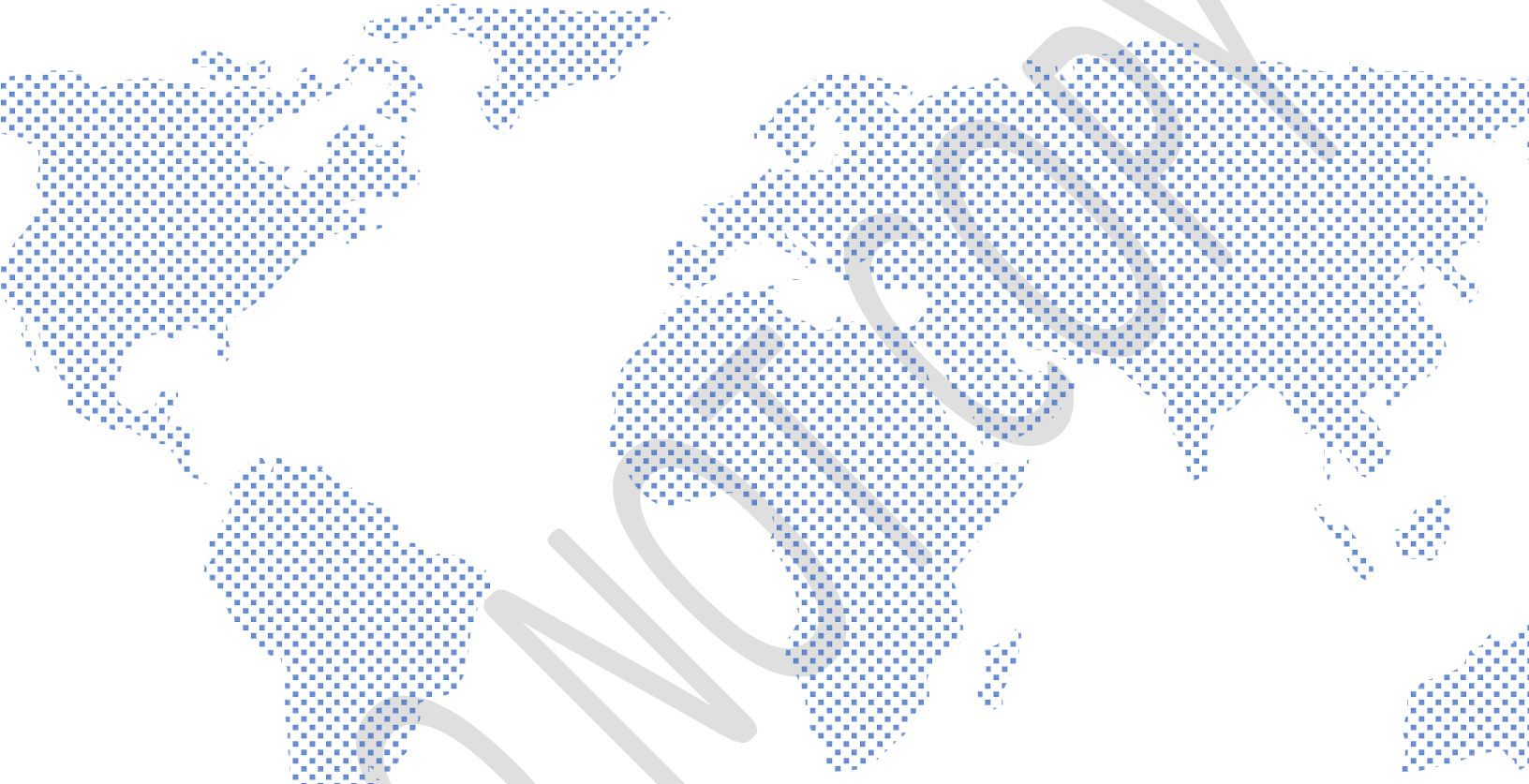
PART 3

Unified Communications – VoIP Assessment



Daniel Cortez

ID: 9849909

Unified Communications – VoIP Assessment Part 3

About this assessment:

These assessment tasks provide an opportunity to demonstrate the competencies covered in the VoIP - Unified Communications subject.

- You are allowed to refer to your text books, notes and the Internet during the Assessment.
- The documentation and research work must be entirely your own.
- By commencing this assessment you confirm that you have read and agree to abide by the ACIT Academic Honesty Policy

Successful completion of this assessment contributes towards attaining competency in the following:

ICTTEN512	Design and implement an enterprise voice over internet protocol and a unified communications network
ICTNWK610	Design and build integrated VoIP networks
ICTPMG611	Prepare a detailed design brief
ICTTEN611	Produce an ICT network architecture design
ICTNWK529	Install and manage complex ICT networks

There are 3 parts to this assessment

1. Design and planning
2. Deployment
3. Question and answer

These assessment tasks provide an opportunity for you to demonstrate the competencies required to design, plan and deploy unified communications solutions.

Part 3 - Question and Answer

Question 1

Start Wireshark Network Protocol Analyzer and open the capture file named 'Wireshark Capture VoIP Assessment'. This file is located in the student materials folder.

Examine line number 255.

1. Describe what is happening here - what is this packet doing?
2. What is the application layer protocol?
3. What are the IP addresses and names/numbers of the endpoints involved?
4. What are the source and destination port numbers?

1. The SIP INVITE request is the message sent by the calling party, inviting the recipient for a session. The SIP headers included in this SIP INVITE request provide information about the message. In other words, invite to start the session.

2. The application layer protocol is SIP with SDP used to describe media session.

3. source Ip address 10.10.100.50 from sip: 901@10.10.100.9 , destination ip address 10.10.100.9 to: sip:903@10.10.100.9

4. source port: 63612, destination port 5060

Question 2

Using the same capture file from the question above.

Examine line number 262.

1. Describe what is happening here - what is this packet doing?
2. What is the application layer protocol?
3. What are the IP addresses and names/numbers of the endpoints involved?
4. What are the source and destination port numbers?

1. The called phone starts ringing a response 180 – Ringing- is sent back

2. The application layer protocol is SIP.

3. source Ip address 10.10.100.9 from sip: 901@10.10.100.9 , destination ip address 10.10.100.50 to: sip:903@10.10.100.9

4. source port: 5060, destination port 63612

Question 3

Using the same capture file from the question above.

Examine line number 282.

1. Describe what is happening here - what is this packet doing?
2. What is the application layer protocol?
3. What are the IP addresses and names/numbers of the endpoints involved?
4. What are the source and destination port numbers?

1. The caller picks up the phone, the called phone sends a response 200 - ok

2. The application layer protocol is SIP with SDP used to describe media session.

3. source Ip address 10.10.100.9 from sip: 901@10.10.100.9 , destination ip address 10.10.100.50 to: sip:903@10.10.100.9

4. source port: 5060, destination port 63612

Question 4

Using the same capture file from the question above.

Examine line number 284.

1. Describe what is happening here - what is this packet doing?
2. What is the application layer protocol?
3. What are the IP addresses and names/numbers of the endpoints involved?
4. What are the source and destination port numbers?

1. The calling phone responds with ACK – acknowledgement. The ack confirms the other user has responded to a request, means confirmation of 200 ok packet delivery. and the phone call is established

2. The application layer protocol is SIP.

3. Source Ip address 10.10.100.50 from sip: 901@10.10.100.9 , destination ip address 10.10.100.9 to: sip:903@10.10.100.9

4. source port: 63612, destination port 5060

Question 5

Using the same capture file from the question above.

Examine line number 286.

1. Describe what is happening here - what is this packet doing?
2. What is the application layer protocol?
3. What are the IP addresses and names/numbers of the endpoints involved?
4. What are the source and destination port numbers?

1. Now the actual conversation is transmitted as data via RTP.

2. The application layer protocol is RTP.

3. Source Ip address 10.10.100.50, destination ip address 10.10.100.9.

4. source port: 60470, destination port 19756.

Question 6

Using the same capture file from the question above.

Examine line number 479.

1. Describe what is happening here - what is this packet doing?
2. What is the application layer protocol?
3. What are the IP addresses and names/numbers of the endpoints involved?
4. What are the source and destination port numbers?

1. When the person calling hungs up, a **BYE** request is sent to the calling phone.

2. The application layer protocol is SIP.

3. Source Ip address 10.10.100.50 from sip: 901@10.10.100.9 , destination ip address 10.10.100.9 to: sip:903@10.10.100.9

4. source port: 63612, destination port 5060.

Question 7

Using the table below, fill in the missing information for Bandwidth (Incl. Overhead), Bandwidth for 15 Concurrent Calls, and Quality.

Ref: http://kb.kerio.com/product/kerio-operator/server-configuration-kerio-operator/bandwidth-used-by-the-different-codecs-1107.html

Codec	Name	Bandwidth (Incl. Overhead)	Bandwidth For 15 Concurrent Calls	Quality
G.711 a/u-law	PCM	80 kbit/s	1536 kbit/s	ISDN
G.729	CSA-CELP	32 kbit/s	600 kbit/s	good
iLBC	iLBC	32 kbit/s	600 kbit/s	good
G.723.1	MP-MLQ	21 kbit/s	330 kbit/s	average
G.723	A-CELP	15 kbit/s	240 kbit/s	average
GSM fullrate	GSM	13 kbit/s	240 kbit/s	average
G.726	AD-PCM	55 kbit/s	1158 kbit/s	GSM
SpeeX	SpeeX	4 – 15 kbit/s	75 – 240 kbit/s	Variable

Question 8

Describe the impact that the choice of codec will have on network performance.

One of the major challenges facing VoIP deployment is achieving and maintaining acceptable voice quality. The user-perceivable voice quality within a VoIP network has to match that of conventional circuit-based networks. This perceived voice quality is affected by many factors including delay, jitter, packet loss and used voice codec systems. Most of these factors depend on the bandwidth capacity and other characteristics of the network links. Thus, network monitoring/management techniques covering bandwidth, jitter, delay and packet loss should be employed to properly handle VoIP traffic. In addition, since call loads vary significantly with the sampling rates provided by

different codec systems, such as G.711, G729 and ilbc, correct selection and usage of a VoIP codec system are crucial to voice quality.

How Codecs Affect Call Quality

The reason VoIP codecs affect call quality is that VoIP codecs typically use lossy compression. Lossy compression discards some audio data to compress the data as much as possible. Discarding a little bit of audio data enables a lossy compression codec to reduce audio data to one eighth or one tenth of the original size. That´s why VoIP codecs use lossy compression.

However, even with lossy compression, you can still get very high-quality VoIP call audio. In fact, most people can´t tell the difference between music compressed with lossy compression and uncompressed music.

The key is that the VoIP codec does a good job of carefully selecting which audio data gests discarded during compression, and doesn´t discard too much audio data.

There´s a method for selecting which audio data gets discarded. Those will get covered a little further on. For now, just understand that you want a VoIP codec that reduces your bandwidth requirements as much as possible, while retaining clear voice quality. Generally speaking, the more the VoIP codec compresses the audio data, the more audio quality it´ll lose. A codec that reduces audio data to one fourteenth of the original size will sacrifice more audio quality than a codec that reduces the data to one eighth of the original size.

If your VoIP codec discards too much audio data or does a poor job of selecting which audio data can be safely left out, it´ll get grainy, distorted voice calls. This can have a huge negative impact on any business.

Therefore, a weak VoIP codec could cost big bucks. Before select an audio codec, it´s important to know how much bandwidth have and how much it will need. That way uses a codec with more compression that is really needed, can be avoided, because with more compression, less quality but more bandwidth available.

Using the G.723 codec low bit rate can be processed a large number of calls with low-bandwidth, so it is G.723 the best option for managing traffic. Using the G.729 codec, which is characterized by low bit rate, but also a high degree of compression, also can process more calls than using G.711 codec. However, it must be stated with much less voice quality as G.729 has the highest value of the packetization delay. On the other hand, the G.711 codec that provides the desired high-quality voice with no delay or with a small value of delay and no packet loss, except in the case of multiple calls when necessary to have a large bandwidth for a large number of packages.

Question 9

Compare H.264 and H.265. Describe what these codecs do. Select which one is better and explain why.

What is H.264?

When we talk about video compression, the codec that often comes to mind is **H.264 (MPEG-4 Part 10 Advanced Video Codec** (MPEG-4 AVC)). This industry standard for video compression technology was originally developed by ITU, the International Telecommunications Union, and ISO, the International Organization for Standardization. First published in 2003, it is based on the concept of MPEG-2 and MPEG-4.

Some of the best features about this video codec are:

. Good quality compressed video output
. Good flexibility in transmitting and preserving the video
. Good quality image at the compressed bitrate

In H.264 the video encoder initializes multiple processes such as prediction, transform, and encoding in order to create an H.264 bitstream. It uses a block-oriented standard with motion compensation to process video frames. The resulting macroblocks are 16 x 16 pixel samples, subdivided into transform and then prediction blocks. The video decoder processes the inverse transform and reconstruction to create a decoded video sequence for distribution.

Some of the main applications of this video codec are:

. High definition DVDs, such as HD-DVD and Blu-Ray.
. High definition TV broadcasting, especially in Europe.
. Apple products
. NATO and US department of Defense video applications.
. Mobile TV broadcasting.
. Internet sources (iTunes, Youtube, for example).
. Video conferencing.

What is H.265?

H.265 is also referred to as High-Efficiency Video Coding (HEVC) and delivers higher quality video at the same bitrate as H.264. It has the potential to support resolutions of 8192 x 4320 pixels (bear in mind that 8K UHD is 7680 x 4320). H.265 was developed by the Joint Collaborative Team on Video Coding (JCT-VC), and collaboration between the ISO/IEC MPEG and ITU-T VCEG

Best features of H.265

. It provides higher and much better compression ratio compared to H.264
. It is also used in high-resolution movies say 2K or 4K
. It is also helpful in reducing the bandwidth with larger resolutions.

This codec uses a different macroblock-encoding method. **Coding Tree Units.** CTU processes information with greater coding efficiency (the lowest bitrate while maintaining video quality) and supports 64 x 64 macroblocks.

Applications:

. H.265 supports different color spaces such as generic film, NTSC, PAL, Rec. 601. Rec 709, Rec.2020, Rec.2100, SMPTE 170M, SMPTE 240M, Srgn, Sycc and xvYCC
. Next-generation HDTV displays and content capture systems.

What´s the difference between H.264 and H.265?

. The compression ratio of H.265 is almost double that of H.264

. H.264 provides support for 16 x 16 pixel macroblocks whereas H.265 provides support for 64 x 64 pixel macroblocks

. Video compression is highly dependent upon prediction between frames. H.265 offers significant improvements in prediction motion compared to H.264

. The intraframe prediction function of H.265 is more descriptive than H.264. This means H.265 can allow for 33 directions of motion whereas H.264 only allows for nine directions of motion.

. H.265 implements separate tiles and slices which are decoded independently

. H.265 provides support for resolutions up to 8192 x 4320 pixels (including 8K UHD) whereas H.264 does not provide support for such resolutions.

. H.265 requires much less bandwidth as compared to H.264 codecs. For instance, H.264 requires 32 mbps internet speed to broadcast 4K video while HEVC can easily do the same in just 15 mbps.

In conclusion H.265 is more advanced than H.264 because of various reasons. The biggest difference is that H.265/HEVC allows for even lower file sizes of the live video streams. This significantly lowers the required bandwidth.

Question 10

What is the purpose of the ITU-T E.164-numbering scheme?

E.164 is a global public switched telephone network (PSTN) and data network standard that prescribes how telephone numbers shoud be arranged for successful routing. It is officially referred to as ITU-T Recommendation. The standars is governed by the Telecommunication Standardization Sector (ITU-T), an arm of the International Telecommunication Union (ITU), which is the United Nations agency responsible for handling information and telecommunication technology (ICT) issues.

The E.164 standard establishes a common framework that every country can use to create international phone numbers. The standard limits the number of digits that a telephone number can have to 15, excluding the international call prefix.

The first part of a phone number is the country code, which can have anywhere between one to three digits. The second part is the national destination code (NDC or NXX), which denotes specific jurisdictions in countries that allocate telephone numbers by region. The national destination code is sometimes called an area code, international city code, or a number plan area.

The last part of a telephone number is the subscriber number (SN). Combined, the NDC and the SN are referred to as the national or significant number. Every country in the world is at liberty to decide how many digits should be in the national number, within the 15-digit limit that E.164 imposes. The limit may seem restrictive at first blush, but it actually allows for around 100 trillion permutations, enough for each person on earth to have thousands of telephone numbers.

E.164 numbers can also be mapped to a uniform resource identifier (URI) or internet portal (IP) addresses using special DNS record types. The most common way of mapping E.164 numbers in this manner is by using the E.164 Number to URI Mapping (ENUM) standard. This mapping makes it possible to use E.164 numbers for internet telephony.

E.164 has several benefits. It makes dialing much easier, a particular benefit for globetrotters and large corporations with offices around the world. An example may better save to elucidate this point.

Individuals making international calls from North America typically dial an access code followed by 011, the international code, and then punch in the country code and the subscriber number. However, if said callers move to another part of the world, that sequence will not work because every country has its own codes for international calls. This means callers would have to learn and remember the specific sequence for every country they visit – a hard, if not impossible, feat. With E.164, all callers require is the country code and subscriber number of the person they want to reach.

E.164 is designed to adapt the public telephone numbering plan to the demands of the internet age. It makes dialing easier, among other benefits. Plans are already underway to expand E.164 into an expanded protocol, dubbed Telephone Number Mapping, or ENUM.

Question 11

What is the purpose of ENUM?

ENUM – The bridge between the switched telephony network and the Internet

ENUM (E.164 Number to URI Mapping) translates telephone numbers into Internet addresses. You can dial a telephone number and reach a SIP, H.323 or any other Internet Telephony user. This all happens in the background; you do need to do anything special while calling someone.

A server with ENUM support will lookup a dialed telephone number in the ENUM tree of the DNS to see if there are alternate ways to set up the call instead of just calling out on the PSTN telephone line. ENUM may contain a reference to a SIP URI, a telephone number to dial, a web page or an e-mail address.

ENUM is already supported by SIP Proxies like SER, Kamailio, OpenSIPS or SNOM 4S, VoIP gateways like Asterisk, Swyx, and SIP phones (SNOM).

Enum uses DNS NAPTE resource records.

ENUM RFC 6116 is a protocol developed by the IETF that uses the Internet DNS system to translate E.164 telephone numbers into IP addressing schemes (like SIP, H.263 or Email.

Question 12

Provide an example configuration for an ENUM lookup in an Asterisk dialplan.

REF: Asterisk- The Definitive Guide, 4th Edition, Ch 12.

Asterisk can perform lookups against ENUM databases using either the ENUMLOOKUP function or a combination of the ENUMQUERY and ENUMRESULT dialplan functions. ENUMLOOKUP only returns a single value back from the lookup, and is useful when you know there is likely to only be one return value (such as the SIP URI you want the system to dial), or if you simply want to get the number of records available.

An ENUM lookup in the dialplan might look like this:

```
exten => _X.,1,Set(CurrentExten=${FILTER(0-9,${EXTEN})})
   same => n,Set(LookupResult=${ENUMLOOKUP(${CurrentExten},sip,,,e164.arpa)})
   same => n,GotoIf($[${EXISTS(${LookupResult})}]?HaveLocation,1)
   same => n,Set(LookupResult=${ENUMLOOKUP(${CurrentExten},sip,,,e164.org)})
   same => n,GotoIf($[${ISNULL(${LookupResult})}]?NormalCall,1:HaveLocation,1)

exten => HaveLocation,1,Verbose(2,Handle dialing via SIP URI returned)
    exten => ...

exten => NormalCall,1,Verbose(2,Handle dialing via standard PSTN route)
    exten => ...
```

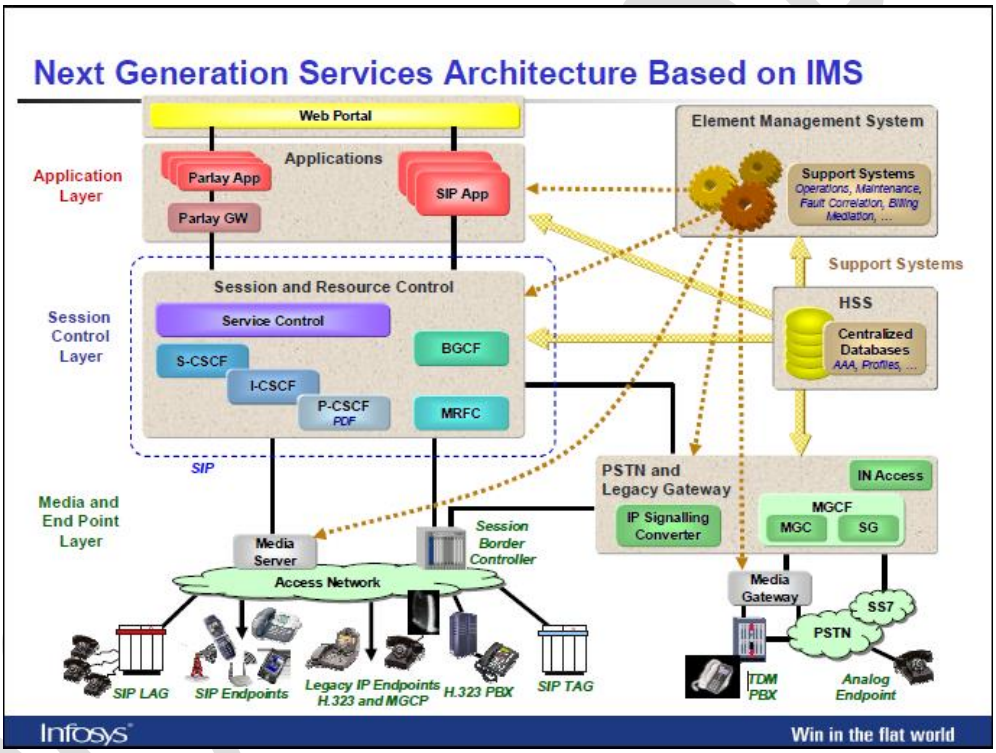
The dialplan code we just looked at will take the number dialed and pass it to the ENUMLOOKUP function. It requests the method type to be sip (we want the SIP URI returned) and the lookup to be performed first against the listings in DNS found in the e164.arpa zone, and next against the records found a at http://www.e164.org.

Outside the countries that have implemented it, there is little uptake of ENUM. As such, many ENUM queries will not return any results. This is not expected to change in the near future, and ENUM will remain a curiosity until more widely implemented.

Question 13

Describe 3 potential benefits that could be provided via the IMS IP-Multimedia Subsystem standards

IMS-IP



_True converged Wireline/Wireless architecture

. Access agnostic with roaming between domains

. Home control allows service differentiation and promotes roaming

_ Investment protection

. Walled session control avoids becoming a bit pipe

_ Managed network provides product and service differentiation

. Highly adaptable bandwidth management and security

. Guaranteed and adjustable QoS to meet individual customers needs

_ Common multi-market segment applications and databases
. Same applications and customers data available regardless of access method

_ Fosters and promotes the introduction of new services
. Common IMS network for voice and data allows for integrated multimedia services
. Allows the integration of disparate applications by carrier instead of supplier

Question 14

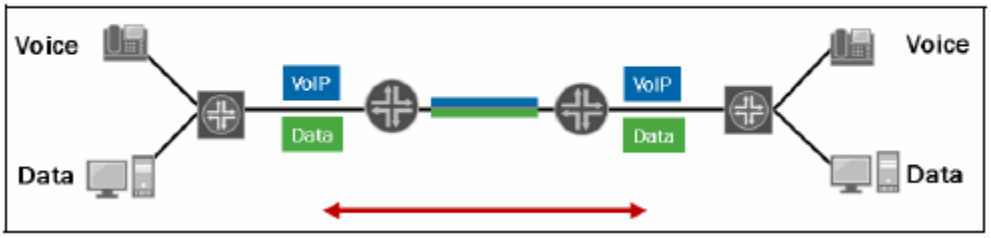
Describe possible network congestion solutions that would enable quality of service (QoS) requirements to be met during periods of network congestion. REF: JNAA-JRE-12.a_SG, Appendix A

By default, devices running the Junos operating system treat all transit traffic equally. The software handles all traffic entering the device on a first-come first-served basis. The device mixes together all traffic transiting the system and places it in the same input and output queues, which means the traffic is subject to the same potential for delays and drops. We refer to this method as best-effort traffic processing.

The CoS features available to devices running the Junos OS allow differentiated services to network traffic where best-effort traffic processing is insufficient. Several components to the CoS tool kit exist. First, tools exist that allow the systema to place traffic into different categories (named forwarding classes) where the system provides the same services. Second, certain components allow the system to treat traffic for each forwarding class in a unique manner. Finally, additional tools allow the system to mark packets with their category so that other devices in the network know how to categorize them.4

CoS allows you to treat traffic differently by providing a minimum bandwidth guarantee, low latency, low packet loss, or a combination of these things for categories of traffic. Consequently, deploying CoS can make some applications perform better. However, it cannot increase the total bandwidth of a link or decrease latency beyond the minimum limits imposed by the speed of light. CoS cannot eliminate congestion within a network. CoS can, however, help you control how this congestion affects different types of traffic.

Meeting the Requirements

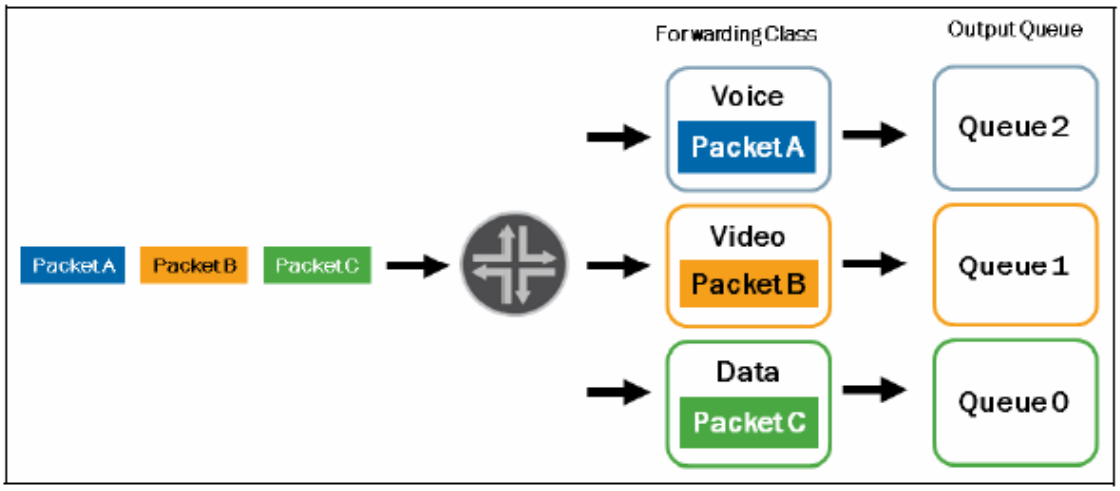


You can use CoS to control the order in which traffic is forwarded through devices running the Junos OS. Even in the networks that are not fully utilizing the capacity on all their network links, instantaneous contention for transmission to the wire can occur. If two packets arrive arrive at an output interface at the same time, the system transmits one packet and adds the other to a queue. The delay in the queue might be minimal in a generally uncongested network; however, even a brief delay can be significant for latency-

sensitive traffic-such as voice over IP (VoIP). You can use traffic prioritization to ensure that latency-sensitive traffic transmits before other traffic. Prioritization also controls the way that extra bandwidth is allocated after all bandwidth guarantees have been met.

You can also configure devices running the Junos OS to guarantee certain levels of bandwidth to traffic classes. This configuration ensures that the device meets minimum bandwidth guarantees during periods of congestion. In this way, it is possible to ensure that certain types of traffic receive a guaranteed minimum level of bandwidth on each link.

Forwarding Classes



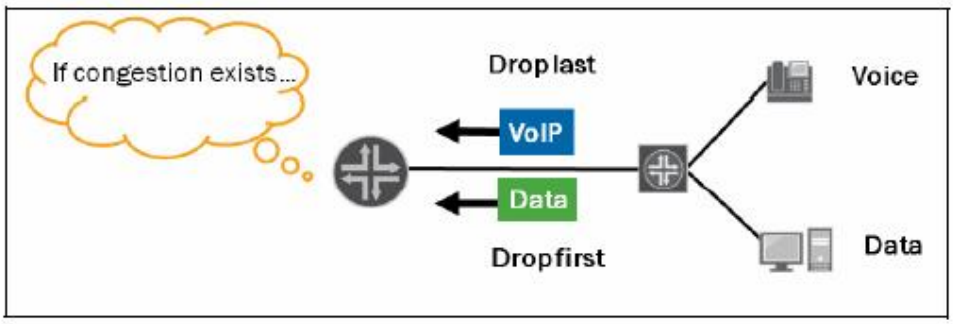
A forwarding class is an abstract concept devices running the Junos OS use to identify traffic that should receive common treatment. The devices associates traffic with a forwarding class during the classification process. During output, the system assigns traffic to a particular output queue based on forwarding class en rewrites behavior aggregate markers based on forwarding class.

Prioritise VoIP traffic with Class of Service

```
switch-options {
    voip {
        interface access-ports {
            vlan Voip;
            forwarding-class expedited-forwarding;
```

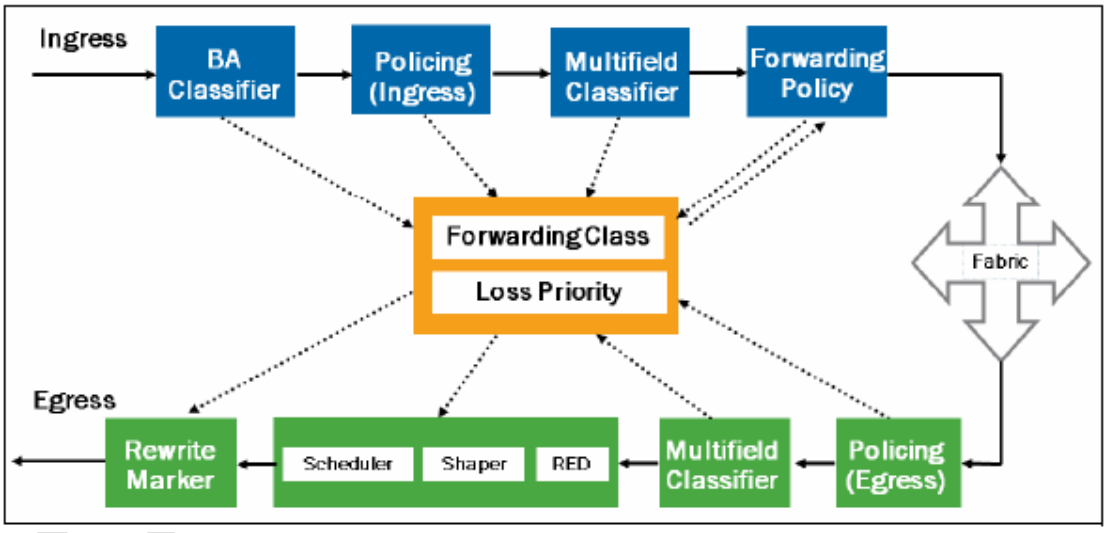
Expedited – forwarding delivers assured bandwidth, low loss, low delay, and low delay variation (jitter) end – to- end for packets in this service class. RFC 3246

Loss Priority



You can associate a loss priority with a packet to tell the system which priority it should give ti dropping this packet during congestion. If you choose to configure RED, you can choose different drop probabilities for traffic with different loss priorities.

CoS Processing



The graphic provides an overview of the way that CoS processing occurs in the Junos OS. The arrwheads indicate the flow of information. Thus, if a process sets the forwarding class and loss priority, the arrow points towards the forwarding class and loss priority box. If the process uses the forwarding class and loss priority as input values, the arrow points away from the forwarding class and loss priority box. The CoS processing chart illustrated in the graphic relates to some packet-based Junos routing devices. The actual processing flow varies between platforms.

Question 15

Make a copy of the text file named 'ooh323.conf'. This file is located in the student materials folder. Edit this file to configure an Asterisk PBX to act as a H.323 gateway and connect with a H.323 gatekeeper at 10.10.100.100.

Question 16

Write an Asterisk dial plan to facilitate emergency calls from VoiP handsets in Australia.

REF: Asterisk- The Definitive Guide, 4th Edition, Ch 7.

```
    [emergency-services]

exten => 000,1,Goto(dialpsap,1)
exten => 9000,1,Goto(dialpsap,1) ; some people will dial '9' because
                                 ; they're used to doing that from the PBX
exten => 000,1,Goto(dialpsap,1)
exten => 112,1,Goto(dialpsap,1)

exten => dialpsap,1,Verbose(1,Call initiated to PSAP!)
same => n,Dial(${LOCAL}/000) ; REPLACE 911 HERE WITH WHATEVER
                             ; IS APPROPRIATE TO YOUR AREA
[internal]
include => emergency-services ; you have to have this in any context
                              ; that has users in it
```

In context where you know the users are not onsite (for example, remote users with their laptops), something like this might be best instead:

```
[no-emergency-services]
exten => 000,1,Goto(nopsap,1)
exten => 9000,1,Goto(nopsap,1) ; for people who dial '9' before external calls
exten => 999,1,Goto(nopsap,1)
exten => 112,1,Goto(nopsap,1)

exten => nopsap,1,Verbose(1,Call initiated to PSAP!)
      same => n,Playback(no-emerg-service) ; you'll need to record this prompt

[remote-users]
include => no-emergency-services
```

Question 17

You need to allow the SIP protocol through your firewall. What port number would you open?

Port 5060

Question 18

Read the following post about a PBX security breach. http://forums.whirlpool.net.au/archive/1740551

What measures could be taken in Asterisk to prevent this from happening? Describe 3 measures that could be taken. REF: Asterisk- The Definitive Guide, 4th Edition, Ch 26.

1. Use non-numeric usernames for your VoIP accounts to make them harder to guess. We can use the MAC address of a SIP phone as its account name in Asterisk.

2. Set ***alwaysauthreject*** to ***yes*** in the [general] section of /etc/asterisk/sip.conf. This option tells Asterisk to respond as if every account is valid, which makes scanning for valid usernames useless. Luckily, this is the default setting for this option.

3. Use strong passwords. There are countless resources available on the internet that help define what constitutes a strong password. There are also many strong password generators available.

4. If you are using IAX2, use key-based authentication. This is a much stronger authentication method than the default MD5-based, challenge-response method. For further enhanced security with IAX2, use the option to encrypt the entire call. If you are using SIP, use TLS to encrypt the SIP signaling. This will prevent an attacker from capturing a successful authentication exchange with the server.

Submission requirements

You are required to submit the following as evidence for this assessment:

1. Written tasks should be completed on a word processor
2. The edited 'ooh323.conf' file must be submitted
3. You must click the submit button