Avaya IP Office QoS Third Party Router Interoperation

Introduction

This document provides a description of the VoIP QoS implementation for low speed PPP links on IP Office. The document describes the configuration of QoS on IP Office and the configuration requirements of 3rd party routers used in conjunction with IP Office. All results herein have been obtained from tests done by Avaya Labs.

The table below the details the hardware and software version used in all test.

<table>
<thead>
<tr>
<th>Equipment</th>
<th>Software version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco 2620</td>
<td>12.2(10)</td>
</tr>
<tr>
<td>Cisco 1750</td>
<td>12.2(7b)</td>
</tr>
<tr>
<td>IP Office IP403</td>
<td>1.2(14)</td>
</tr>
<tr>
<td>IP Office IP 406</td>
<td>1.2(14)</td>
</tr>
<tr>
<td>IP Office WAN 3</td>
<td>1.2(14)</td>
</tr>
</tbody>
</table>

Operation

The diagram below illustrates the operation of Avaya’s IP Office QoS mechanism for slow speed WAN links.

Voice packets are transmitted with a fixed length and intervals (1x20ms) and must not be delayed through the interface.
The illustration shows voice packets (V1, V2 and V3) and non-voice packet D1 arriving to the PPP interface. The non-voice packet D1 is made to fit into the interval between successive voice packets. This is accomplished by processing large non-voice packets through PPP Multilink. The Multilink process “fragments” the larger non-voice packet (D1) into smaller components (D1-1 and D1-2) for serialization to the PPP link. Voice packets are not fragmented in this way. Layer 3 (call control) packets are fragmented and inserted when bandwidth is available in the same way as non-voice packets.

**Elements of IP Office QoS**

The elements of IP Office QoS are described in this section.

**VPN Line Control**

QoS policies on routers protect delay sensitive VoIP traffic from non-voice traffic on slow speed WAN links. Such QoS policies do not generally restrict the actual sum of voice calls (i.e. not RTP session based); usually a portion of the available bandwidth is simply set aside for VoIP traffic under link congestion.

For this reason it is necessary to apply a level of strict access control to the available WAN link for the amount of concurrent VoIP calls.

IP Office controls access to the available WAN bandwidth for voice traffic using the VPN Line configuration. The VPN Line configuration governs the number of concurrent VoIP calls the IP Office system will allocate on the link. The quantity and type of call can be controlled in both incoming and outgoing directions.

**IP Header Compression**

IP Header Compression (IPHC) reduces the IP/UDP/RTP headers to two bytes for most packets in the case where no UDP checksums are being sent, or four bytes with checksums. IPHC therefore significantly reduces WAN bandwidth requirements per voice call.

IP Office applies IPHC to all traffic types i.e. voice signalling/traffic and data. However, some IP protocols yield a better compression ratio.

IPHC imposes process overheads which can become counter-productive at higher WAN speeds. It is for this reason that IP Office will not perform IP Header compression at speeds above 1024Kbps.

**Interface queue**

Traffic outbound to an interface is associated to one of two queue types; Voice Traffic/Signalling (call set-up) or Normal. The Voice Traffic/Signalling queue has priority over the Normal (data traffic) queue. IP Office identifies and prioritises voice traffic by the configured Differentiated Services Code Point (DSCP) value and is transparent to UDP port numbers. Voice Signalling is identified by the TCP port number 1720; this option is not configurable.

The DSCP value is configured on the System/Gatekeeper form and is a global parameter. For most applications the default setting of the DSCP 0xA0 and mask 0xFF is suitable for most applications.
The value set for the DSCP parameter serves two functions;

- The value is used by IP Office to mark the TOS field (DiffServ) in the IP Header.
- The value is used by IP Office to identify Voice traffic for prioritisation to a WAN link

For advance users the mask allows IP Office to identify more than one DiffServ value; use the mask to identify specific bits in the TOS field.

**Multilink Fragmentation**

Large non-voice packets can adversely affect the smaller voice packets and reduce voice quality. This effect of non-voice packets on voice packet is sometimes referred to as serialisation delay. To minimise the effect of serialisation delay the large non-voice packets are fragmented so as not to delay voice packets; the fragmented non-voice packets are interleaved with the VoIP packets thereby reducing jitter and delay.

The size of non-voice packets changes with respect to the speed of the link and the number of established VoIP calls occupying the link. IP Office dynamically calculates the size of a non-voice packet fragments on the “fly”. The calculation is based on the configured WAN speed and the number of established Voice calls on the link.

IP Office supports the Multi-class option (RFC2686) of the PPP Multi-link protocol (RFC1990).

**The PPP link**

IP QoS is “enabled” on a link when the PPP protocol options IPHC and Multilink are successful negotiated on an established PPP link. The WAN port must also be configured with the correct operational WAN speed.

**General Configuration Guidelines**

In order to configure QoS on an IP Office there are three Mandatory requirements as shown below:

1. IP Header Compression set on the WAN service type.
2. Multilink set on the service.
3. The WAN link is correctly configured for the WAN port speed.
4. An appropriate DSCP value system/gatekeeper tab

In the following section a simple example is shown with details of the configuration tasks.

**QoS configuration for IP Office**

The following diagram and configuration task list provides an example of QoS configuration between two IP Office systems. IP Office may however be configured to interoperable with 3rd party routers. Third party router interoperation relies on the successful negotiation of PPP protocol options IPHC and Multilink. Once the PPP protocol options are agreed on the link both routers are then able to apply QoS policies to their respective ends of the link using fragmentation interleave and IP Header compression.
The table below details the basic configuration of the simple network shown above.

<table>
<thead>
<tr>
<th>Configuration Steps</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Attach WAN cable, reboot unit and obtain configuration.</td>
</tr>
</tbody>
</table>

In order to configure the WAN interface IP Office requires the WAN cable to be attached at boot up.

<table>
<thead>
<tr>
<th><strong>Step 2</strong></th>
<th>Define a WAN service type</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Name = wan_link1</td>
</tr>
<tr>
<td></td>
<td>Account name = wan_link1</td>
</tr>
<tr>
<td></td>
<td>All password field = blank</td>
</tr>
</tbody>
</table>

If running a WAN3 the word “WAN” (upper case) must be added in the Service Dial In tab as a Dial In Source number.

<table>
<thead>
<tr>
<th><strong>Step 2</strong></th>
<th>On the PPP tab of the service configured in the previous step select the following configuration Items</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>PPP head comp</td>
</tr>
<tr>
<td></td>
<td>Multilink</td>
</tr>
</tbody>
</table>

Multilink and IPHC are mandatory configuration items for IP Office QoS.

<table>
<thead>
<tr>
<th><strong>Step 3</strong></th>
<th>On the WAN port form configure the operational speed of the WAN link in bits/second.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>E.g. 128000</td>
</tr>
</tbody>
</table>

IP Office uses the configured WAN speed to dynamically calculate PPP link fragment size.

<table>
<thead>
<tr>
<th><strong>Step 4</strong></th>
<th>Apply above settings (Steps 1-3) for the remote IP Office.</th>
</tr>
</thead>
</table>

**3rd Party Routers interoperation with IP Office**

IP Office QoS is fully compliant with 3rd party router manufacturers that support Link Fragmentation using PPP Multilink and IPHC (RFC 2507 and RFC 2508).
All vendors that support a QoS mechanism on their routers will present their own method of voice traffic prioritisation to a slow speed WAN links. The operation of such QoS mechanisms is “local” to a system but require that the enabling PPP protocols be negotiated on the link. IP Office will interoperate with any vendors QoS as long as the “enabling protocols” are agreed on the established link.

The “enabling protocols” for low speed WAN links is the PPP options for IP Header Compression (RFC 2508) and PPP Multilink (RFC1990). As long as these options are agreed on the PPP link then each router can “locally” apply QoS to their respective end of the link.

### Debugging IP Office QoS and VoIP

Using the IP Office System Monitor application options it is possible to debug all aspects of the IP Office function and features. Generally outputs are associated directly to the any related standard. PPP monitor outputs will, for example, reference RFC terms relating to the PPP protocol.

The following table describes monitor options that may be useful for debugging QoS issues on IP Office.

<table>
<thead>
<tr>
<th>Function</th>
<th>Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>Queue drops</td>
<td>Default monitor option shows the Voice and non-voice queue drops</td>
</tr>
<tr>
<td></td>
<td>15604mS PRN: Discards – Norm 2 Voice 0</td>
</tr>
<tr>
<td></td>
<td>16601mS PRN: Discards – Norm 2 Voice 0</td>
</tr>
<tr>
<td></td>
<td>17619mS PRN: Discards – Norm 2 Voice 0</td>
</tr>
<tr>
<td></td>
<td>Norm = drops from the non-voice queue</td>
</tr>
<tr>
<td></td>
<td>Voice = drops from the voice queue</td>
</tr>
<tr>
<td></td>
<td>Notes (2) A well designed network should not experience any voice packets drops.</td>
</tr>
<tr>
<td></td>
<td>2. The message is generated only when there are discards to the link.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Multilink</th>
<th>This output is taken using the following Monitor option</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fragmentation</td>
<td>• PPP/LCP Tx</td>
</tr>
<tr>
<td></td>
<td>• PPP/LCP Rx</td>
</tr>
<tr>
<td></td>
<td>The highlighted text indicates the PPP Multilink option; the negotiation is successful</td>
</tr>
<tr>
<td></td>
<td>97104mS PPP LCP Tx: v=cisco1750</td>
</tr>
<tr>
<td></td>
<td>PPP LCP Config-Req(1) id=2 len=33</td>
</tr>
<tr>
<td></td>
<td>MagicNum=00102152</td>
</tr>
<tr>
<td></td>
<td>Protocol field compression</td>
</tr>
<tr>
<td></td>
<td>Address and control field compression</td>
</tr>
<tr>
<td></td>
<td>MRRU=1500</td>
</tr>
<tr>
<td></td>
<td>ShortSeq</td>
</tr>
<tr>
<td></td>
<td>EndPointDiscrim=mac 00e07003f20</td>
</tr>
<tr>
<td></td>
<td>MultiClass=6 Classes=4</td>
</tr>
<tr>
<td></td>
<td>97106mS SERVICE:2002/6/511:30,”cisco1750”,0,0</td>
</tr>
<tr>
<td></td>
<td>97120mS PPP LCP Rx: v=cisco1750</td>
</tr>
<tr>
<td></td>
<td>PPP LCP Config-Req(1) id=196 len=31</td>
</tr>
<tr>
<td></td>
<td>AuthProt=c223 Algorithm=5</td>
</tr>
<tr>
<td></td>
<td>MagicNum=1de9b16a</td>
</tr>
<tr>
<td></td>
<td>MRRU=1524</td>
</tr>
<tr>
<td></td>
<td>EndPointDiscrim=local 636973636f31373530</td>
</tr>
<tr>
<td></td>
<td>97121mS PRN: LCPAutomatic.:ParseAutomaticPacket</td>
</tr>
<tr>
<td></td>
<td>97121mS PPP LCP Tx: v=cisco1750</td>
</tr>
<tr>
<td></td>
<td>PPP LCP Config-Ack(2) id=196 len=31</td>
</tr>
<tr>
<td></td>
<td>AuthProt=c223 Algorithm=5</td>
</tr>
<tr>
<td></td>
<td>MagicNum=1de9b16a</td>
</tr>
<tr>
<td></td>
<td>MRRU=1524</td>
</tr>
<tr>
<td></td>
<td>EndPointDiscrim=local 636973636f31373530</td>
</tr>
<tr>
<td></td>
<td>97122mS PPP LCP Rx: v=cisco1750</td>
</tr>
</tbody>
</table>
### Function | Method
---|---
PPP LCP Config-Rej(4) id=2 len=10
  *ShortSeq*
  *MultiClass=6 Classes=4*
  97122ms PRN: LCPAutomaton::ParseAutomatonPacket
  97122ms PPP LCP Tx: v=cisco1750
  PPP LCP Config-Req(1) id=3 len=27
  MagicNum=00102164
  Protocol field compression
  Address and control field compression
  **MRUU=1500**
  **EndPointDiscrim=mac 00e007003f20**
  97130ms SERVICE:2002/6/511:30,"cisco1750",0,0
  97138ms PPP LCP Rx: v=cisco1750
  PPP LCP Config-Ack(2) id=3 len=27
  MagicNum=00102164
  Protocol field compression
  Address and control field compression
  **MRUU=1500**
  **EndPointDiscrim=mac 00e007003f20**
  97153ms PRN: LCPAutomaton::UpLink()
  97153ms PRN: LCPAutomaton::UpLink() checking link_state
  97154ms PRN: ppplink start NetworkControlProtocols
  97154ms PRN: stack start NetworkControlProtocols

### VPN line
The following options are useful for debugging call setup issue.
- Call/Line Send
- Call/Line Receive
- Call/Targetting

The Highlighted text from the CMTARGET output shows the number received on ISDN line (5) is resolved to Line 2 (GROUP 2).

The CMLine TX=2 is the resulting call setup on a VPN Line 2. These output show the negotiated UDP port numbers

29505ms CMLineRx: v=5
  CMSetup
  Line: type=Q931Line 5 Call: lid=5 id=6 in=2
  **Called[8400]** Type=SubscriberNumber (4) Calling[01442404001] Type=SubscriberNumber (4)
  BC: CMTC=Speech CMTM=Circuit CMTR=64 CMST=Default CMU1=Alaw
  Bchan: slot=0 chan=2

29506ms CMTARGET: LOOKUP CALL ROUTE:41872 type=4 called_party=8400 sub=8400
calling=01442404001 in=2 complete=0
29507ms CMTARGET: ADD TARGET:41872 number=8400 type=4 depth=1 nobar=1 setorig=1
29508ms CMTARGET: SYS SC:41872 8400 2 400 sc=type=31 code=8N, num=.
29508ms CMTARGET: DIAL LINE:41872 GROUP=2 SUCCESS=1
29508ms CMTARGET: LOOKUP CALL ROUTE:41872 returned 1
29511ms CMLineTx: v=2
  CMSetup
  Line: type=VPN 2 Call: lid=0 id=42875 in=0
  **Called[8400]** Type=SubscriberNumber (4) Calling[01442404001] Type=SubscriberNumber (4)
  BC: CMTC=Speech CMTM=Circuit CMTR=64 CMST=Default CMU1=Alaw
  Bchan: slot=250 chan=9868
  IE CMIETxChannelAudio (1) comptype=G729A8K (6) pktsize=20 ipaddr=192.168.42.99 port=0
  IE CMIERxChannelAudio (2) comptype=G729A8K (6) pktsize=20 ipaddr=192.168.123.98
  port=51138
  Display [01442404001]
  Cause=16, Normal
  Locale: eng

29680ms CMLineRx: v=2
  CMProceeding
  Line: type=VPN 2 Call: lid=0 id=42875 in=0
  Bchan: slot=250 chan=9868
  IE CMIETxChannelAudio (1) comptype=G729A8K (6) pktsize=20 ipaddr=192.168.42.99
  port=49178
  IE CMIERxChannelAudio (2) comptype=G729A8K (6) pktsize=20 ipaddr=192.168.123.98
  port=51138
  Display [400]

29681ms CMLineTx: v=5
### Function | Method
---|---
CMProceeding | Line: type=Q931Line 5 Call: lid=5 id=6 in=2
Called[8400] Type=SubscriberNumber (4)
Bchan: slot=0 chan=2
IE CMITxChannelAudio (1) comptype=G729A8K (6) pktsize=20 ipaddr=192.168.42.99 port=49178
IE CMIERxChannelAudio (2) comptype=G729A8K (6) pktsize=20 ipaddr=192.168.123.98
| Display [8400]
30785m$ CMLineRx: v=2
CMConnect | Line: type=VPN 2 Call: lid=0 id=42875 in=0
BC: CMTC=Speech CMTM=Circuit CMT=64 CMST=Default CMU1=Alaw
Display [400]
30787m$ CMLineTx: v=5
CMConnect | Line: type=Q931Line 5 Call: lid=5 id=6 in=2
Called[8400] Type=SubscriberNumber (4)
Bchan: slot=0 chan=2
Display [8400]
30815m$ CMLineRx: v=5
CMConnectAck | Line: type=Q931Line 5 Call: lid=5 id=6 in=2

**Header compression (IPHC)**

This output is taken using the following Monitor option
- PPP/IPCP Tx
- PPP/IPCP Rx

The output shows the successful negotiation of an IP address 192.168.168.100 by the remote and the IPHC. The IPHC is negotiation is accepted by both local and remote. (Config-Ack received and transmitted)

| 47458m$ PRN: stack start NetworkControlProtocols | 47459m$ PPP IPCP Tx: v=cisco1750
PPP IPCP Config-Req(1) id=1 len1=20
IPHC |
| 0000 00 10 00 10 01 00 00 05 00 a8 01 02 | ............ |
| 47473m$ PPP IPCP Rx: v=cisco1750
PPP IPCP Config-Req(1) id=14 len1=26
IPHC |
| 0000 00 10 00 14 01 00 00 05 00 a8 01 02 | ............ |
| IP-Address 192.168.168.100 | 47473m$ PPP IPCP Tx: v=cisco1750
PPP IPCP Config-Ack(2) id=14 len1=26
IPHC |
| 0000 00 10 00 14 01 00 00 05 00 a8 01 02 | ............ |
| IP-Address 192.168.168.100 | 47847m$ PRN: Wed 5/6/2002 11:09:19 FreeMem=7084108 CMMsg=3 (3) Buff=100 554 500 1392
48337m$ PRN: Wed 5/6/2002 11:09:19 FreeMem=7085224 CMMsg=3 (3) Buff=100 555 500 1391
50464m$ PPP IPCP Tx: v=cisco1750
PPP IPCP Config-Req(1) id=2 len1=20
IPHC |
| 0000 00 10 00 14 01 00 00 05 00 a8 01 02 | ............ |
| 50474m$ PPP IPCP Rx: v=cisco1750
PPP IPCP Config-Ack(2) id=2 len1=20
IPHC |
| 0000 00 10 00 14 01 00 00 05 00 a8 01 02 | ............ |